NETGEAR®

User Manual

24-Port and 48-Port Gigabit Ethernet PoE+ Smart Managed Essentials Switch with 2 or 4 Dedicated SFP Ports

GS324TPv2
GS348TPv2

December 2025
202-12897-01

NETGEAR, Inc.
3553 N. 1st St,
San Jose, CA 95134, USA

Support and Community

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

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

Regulatory and Legal

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

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

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

See the regulatory compliance document before connecting the power supply.

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

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

This product is designed and warranted for indoor use only. Do not use this device outdoors. The PoE source is intended for intra building connection only.

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
202-12897-01	December 2025	First publication of the user manual.

Contents

Chapter 1 Get Started

Available publications and online help..... 17
Manage the switch by using the device UI..... 17
Device UI buttons and user-defined fields..... 17
Interface naming conventions..... 18
Save your changes in the device UI..... 19
Context-sensitive help..... 19
About on-network and off-network access..... 19
Access the switch on-network and connected to the Internet.... 20
Use a Windows-based computer to access the switch on-network and connected to the Internet..... 21
Use the NETGEAR Discovery Tool to discover the switch when it is connected to the Internet..... 22
Use other options to discover the switch IP address..... 24
Access the switch on-network when you know the switch IP address..... 24
Access the switch off-network and not connected to the Internet..... 26
Register the switch..... 27
Register and access the switch on-network with your NETGEAR account..... 27
Register the switch with your NETGEAR account and get a registration key for offline access..... 28
Access the switch with a registration key..... 29
Access the switch off-network and enter the registration key before you log in..... 30
Access the switch on-network and enter the registration key after you log in..... 31
Change the language of the device UI..... 32
Change the theme of the device UI..... 32
Configure ports using the Device View..... 33
Access the NETGEAR support website..... 34
Access the user manual online..... 35

Chapter 2 Configure Switch System Settings

Dashboard..... 37
Display VLAN membership..... 37
Display switch device details..... 37
Display port utilization and port connections..... 38

Configure and display general switch system information..... 40
Display information about switch hardware components and firmware..... 41
Display the power supply information..... 41
Display the boot and software version..... 42
Display the temperature sensor information..... 43
Display the status of the fans..... 44
IP network settings for management access..... 45
Configure the IPv4 management interface..... 45
Change the management VLAN..... 46
Configure an IPv6 management interface through autoconfiguration or a DHCPv6 server..... 48
Manage a static IPv6 address for the IPv6 management interface..... 49
Display IPv6 network interface neighbors..... 51
Time and SNTP settings..... 52
Set the time manually..... 52
Configure SNTP for the time settings and configure the global SNTP settings..... 53
Display the global SNTP status..... 55
SNTP servers..... 57
Add an SNTP server..... 58
Change the settings for an SNTP server..... 59
Remove an SNTP server..... 60
Display the status of the SNTP servers..... 61
Configure daylight saving time settings..... 62
Display the daylight saving time status..... 65
Domain Name System..... 66
Configure the global DNS settings and add a DNS server..... 66
Remove a DNS server..... 68
Map host names to DNS server IP addresses and display dynamic host mappings..... 69
Add an entry to the static DNS host mapping table..... 69
Change an entry in the static DNS host mapping table..... 70
Remove an entry from the static DNS host mapping table. 70
Display or clear the dynamic DNS host mapping entries.... 71
Manage switch discovery protocols..... 72
Display USB device information..... 73
LLDP and LLDP-MED settings for the switch..... 74
Configure the LLDP and LLDP-MED settings..... 75
Display the LLDP-MED network policy for an interface..... 76
Display the LLDP local device information..... 77
Display the LLDP neighbor information..... 79
Simple Network Management Protocol..... 82
Manage SNMPv1 and SNMPv2 communities..... 83

Add an SNMPv1 and SNMPv2 community..... 83
Change an existing SNMPv1 and SNMPv2 community..... 84
Delete an SNMPv1 and SNMPv2 community..... 85
Manage the SNMPv1 and SNMPv2 trap settings..... 86
Add an SNMPv1 or SNMPv2 trap configuration for a host.. 86
Change an SNMPv1 or SNMPv2 trap configuration for a host..... 87
Delete an SNMPv1 or SNMPv2 trap configuration for a host..... 88
Configure SNMPv1 and SNMPv2 trap flags..... 89
Display the supported MIBs..... 90
Configure the SNMPv3 user account..... 90
Configure HTTPS access settings..... 92
HTTPS management access..... 93
Configure HTTPS access settings..... 93
Manage the SSL certificate for HTTPS access..... 94
Generate an SSL certificate..... 95
Transfer an SSL certificate from a TFTP server to the switch..... 95
Delete the SSL certificate..... 97
Browser security message with HTTPS access..... 98
SSH management access..... 98
Configure the SSH access settings..... 99
Manage the RSA key for SSH access..... 100
Generate an RSA key..... 100
Transfer an RSA key from a computer to the switch..... 101
Delete the RSA key..... 102
Configure inbound Telnet settings..... 102
DHCP snooping..... 103
Enable DHCP snooping for the switch..... 104
Enable DHCP snooping for a VLAN..... 105
Configure DHCP snooping interface settings..... 105
Add a static DHCP snooping binding..... 107
Change a static DHCP snooping binding..... 108
Remove a static DHCP snooping binding..... 109
Display or clear dynamic DHCP snooping bindings..... 110
Configure DHCP snooping persistent settings..... 111
Display the DHCP snooping statistics..... 112
DHCP Layer 2 relay..... 113
Configure the global DHCP L2 relay settings..... 113
Configure the DHCP L2 relay VLAN settings..... 114
Configure a DHCP L2 relay interface..... 115
Display or clear the DHCP L2 relay interface statistics..... 117

Chapter 3 Manage VLANs

Manage the VLAN configuration on the switch..... 120
About VLANs..... 120
Add a VLAN..... 121
Configure membership interfaces for a VLAN..... 122
Change a VLAN 124
Delete one or more VLANs..... 125
Reset the entire VLAN configuration to default setting..... 126
Change the port VLAN ID (PVID) settings..... 127
Configure a voice VLAN..... 129
Auto-VLANs 131
Configure the OUI-based properties..... 132
Configure the OUI-based interface settings..... 133
Manage the OUI table..... 134
Add an OUI..... 135
Remove an OUI..... 136
Configure the global protocol-based VoIP prioritization and class..... 137
Configure VoIP protocol-based interface settings..... 138
Display the Auto-VoIP status..... 139
Configure a MAC-based VLAN..... 140
Add a MAC-based VLAN configuration..... 141
Delete a MAC-based VLAN configuration..... 141
Configure a protocol-based VLAN group..... 142
Add a protocol-based VLAN group..... 143
Configure membership interfaces for a protocol-based VLAN group..... 144
Change a protocol-based VLAN group..... 145
Delete a protocol-based VLAN group..... 146
Configure Generic Attribute Registration Protocol..... 147
Configure the GARP switch settings 147
Configure GARP interface settings..... 148
Private VLANs..... 149
Overview of the tasks for private VLAN configuration..... 150
Assign a private VLAN type to a VLAN..... 151
Configure a private VLAN association with a primary and secondary VLAN..... 152
Remove an existing private VLAN association..... 154
Configure the private VLAN port mode..... 154
Private VLAN host interface: Assign the interface to primary and secondary VLANs..... 156
Private VLAN host interface: Remove the interface from primary and secondary VLANs..... 157

Private VLAN promiscuous interface: Assign the interface to primary and secondary VLANs..... 159
Private VLAN promiscuous interface: Remove the interface from primary and secondary VLANs..... 160
Protect ports..... 161

Chapter 4 Configure Switching

LLDP and LLDP-MED settings for interfaces..... 164
Configure LLDP interface settings..... 164
Configure LLDP-MED interface settings..... 166
Power over Ethernet..... 168
PoE concepts..... 168
Power allocation and power budget concepts..... 169
Configure global PoE settings..... 170
Configure PoE settings for the ports..... 171
Power cycle PoE ports..... 175
PoE timer schedules..... 175
Add a new PoE timer schedule with an absolute entry or add a new absolute entry to an existing timer schedule..... 176
Add a new PoE timer schedule with a periodic entry or add a new periodic entry to an existing timer schedule..... 177
Change the settings for an entry of a timer schedule..... 179
Remove an entry from a timer schedule..... 180
Remove a timer schedule..... 181
Green Ethernet settings..... 182
Configure the global green Ethernet settings..... 182
Configure green Ethernet interface settings..... 183
Link aggregation groups..... 185
Configure a LAG..... 185
Configure the port members for a LAG..... 187
Set the LACP system priority..... 188
Set the LACP priority and time-out period for a port..... 189
Configure the port settings and maximum frame size..... 190
Spanning Tree Protocol..... 193
Configure the global STP settings and display the STP status. 194
Configure the CST settings and display the MSTP status..... 196
Configure the CST interface settings..... 198
Display the CST interface status..... 201
Display the Rapid STP interface status..... 203
Manage MST instances..... 204
Add an MST instance and display the MST status..... 204
Change an MST instance..... 206
Delete an MST instance 207

Configure and display the interface settings for an MST instance..... 207
Display the STP interface statistics..... 210
MAC address table..... 211
Set the dynamic MAC address aging interval..... 211
View, search, or clear the MAC address table..... 212
Add a static MAC address to the MAC address table..... 213
Remove a static MAC address from the MAC address table. 214
DHCP snooping..... 215
Enable DHCP snooping for the switch..... 216
Enable DHCP snooping for a VLAN..... 217
Configure DHCP snooping interface settings..... 217
Add a static DHCP snooping binding..... 219
Remove a static DHCP snooping binding..... 220
Configure DHCP snooping persistent settings..... 221
Display the DHCP snooping statistics..... 222
DHCP Layer 2 relay..... 223
Configure the global DHCP L2 relay settings..... 223
Configure the DHCP L2 relay VLAN settings..... 224
Configure a DHCP L2 relay interface..... 225
Display or clear the DHCP L2 relay interface statistics..... 227
Dynamic ARP inspection..... 228
Configure the global DAI settings..... 228
Configure DAI VLANs..... 229
Configure a DAI interface..... 231
DAI ACLs..... 232
Add a DAI access control list..... 232
Configure a rule for an existing DAI ACL..... 233
Remove a rule from a DAI ACL..... 234
Remove a DAI access control list 235
Display the DAI statistics..... 236

Chapter 5 Configure Multicast

Display the entries in the multicast forwarding database..... 239
Display the multicast forwarding database statistics..... 240
Internet Group Management Protocol snooping 241
Enable IGMP snooping and configure IP header validation. 242
Display entries in the IGMP snooping table..... 243
Display IGMP snooping statics and VLANs..... 244
Configure the IGMP snooping settings for an interface..... 245
Configure IGMP snooping for a VLAN..... 247
Configure an IGMP multicast router interface..... 249
Configure an IGMP multicast router VLAN..... 250
IGMP snooping querier overview..... 251

Enable the IGMP snooping querier and configure the global settings..... 251
Add an IGMP snooping querier for a VLAN..... 252
Change an IGMP snooping querier for a VLAN..... 254
Remove the IGMP snooping querier settings from a VLAN.. 254
Display the status of the IGMP snooping querier for all VLANs..... 255
Enable IGMP snooping on the Auto-Video VLAN..... 257
Multicast Listener Discovery snooping..... 258
Enable MLD snooping..... 258
Configure the MLD snooping settings for an interface..... 259
Add MLD snooping for a VLAN..... 261
Change the MLD snooping settings for a VLAN..... 262
Remove the MLD snooping settings from a VLAN..... 263
Configure an MLD multicast router interface..... 264
Enable or disable MLD multicast router mode for a VLAN.... 265
MLD snooping querier overview..... 266
Enable the MLD snooping querier and configure the global settings..... 267
Add an MLD snooping querier for a VLAN and display the status..... 268
Change an MLD snooping querier for a VLAN..... 269
Remove the MLD snooping querier settings from a VLAN.... 270
Multicast VLAN registration..... 271
Enable MVR and configure the global settings..... 272
Add an MVR group..... 273
Remove an MVR group..... 274
Configure an MVR interface..... 275
Configure the members of an MVR group..... 276
Display the MVR statistics..... 277

Chapter 6 Configure Quality of Service

Quality of Service concepts..... 280
Class of Service..... 280
CoS configuration concepts..... 280
Configure the CoS trust mode settings globally..... 281
Configure the CoS trust mode, shaping rate, and ingress rate for an interface..... 282
Configure CoS queue settings for an interface..... 284
Map 802.1p priorities to queues..... 285
Map DSCP values to queues 286
Differentiated Services..... 288
Defining DiffServ..... 288

Configure the DiffServ mode and display the entries in the DiffServ private MIB tables..... 289
Configure a DiffServ class..... 290
Add and configure a DiffServ class..... 290
Change the criteria for an existing DiffServ class..... 294
Change the name for an existing DiffServ class..... 295
Remove a DiffServ class..... 296
Configure an IPv6 DiffServ class..... 296
Add and configure an IPv6 DiffServ class..... 297
Change the criteria for an existing IPv6 DiffServ class..... 299
Change the name for an existing IPv6 DiffServ class..... 300
Remove an IPv6 DiffServ class..... 301
Configure a DiffServ policy..... 302
Add and configure a DiffServ policy..... 302
Change the attributes for an existing DiffServ policy..... 305
Remove a DiffServ policy..... 305
Attach a DiffServ policy to an interface..... 306
Remove a DiffServ policy from an interface..... 308
Display DiffServ service statistics..... 308

Chapter 7 Manage Switch Security

Change the device admin password..... 311
RADIUS servers..... 312
Configure the global RADIUS server settings..... 312
RADIUS authentication servers..... 313
Add a RADIUS authentication server..... 314
Change the settings for a RADIUS authentication server.. 315
Remove a RADIUS authentication server from the switch. 316
Display the RADIUS authentication server statistics..... 317
RADIUS accounting server..... 318
Configure a RADIUS accounting server..... 318
Display or clear the RADIUS accounting server statistics.. 319
TACACS+ servers..... 321
Configure the global TACACS+ settings..... 321
Add a TACACS+ server..... 322
Change the settings for a TACACS+ server..... 323
Remove a TACACS+ server from the switch 324
Authentication lists..... 325
Configure the HTTP authentication list..... 325
Configure the HTTPS authentication List..... 326
Configure the Dot1x authentication list..... 328
Management access profiles and rules..... 329
Add an access profile..... 329
Add a rule to the access profile..... 330

Activate the access profile..... 331
Display the access profile rules and the number of filtered packets..... 332
Change a rule for the access profile..... 333
Deactivate the access profile..... 334
Remove a rule from the access profile..... 335
Remove the access profile..... 336
Port authentication..... 336
Configure the global 802.1X authentication settings..... 337
Configure the 802.1X authentication settings for a port..... 339
Initialize 802.1X on a port..... 342
Restart 802.1X authentication on a port..... 343
Display the port summary..... 344
Display the client summary..... 346
MAC filters for traffic control..... 347
Create a MAC filter for a MAC address..... 347
Delete a MAC filter..... 349
Display the MAC filter summary..... 349
Storm control..... 350
Configure the global storm control settings..... 351
Configure the storm control settings for a port..... 352
Port security..... 354
Configure the global port security mode..... 354
Configure a port security interface..... 355
Display learned MAC addresses and convert them to static addresses..... 357
Display port security violations..... 358
Loop protection..... 359
Configure the global loop protection settings..... 360
Configure the loop protection settings for interfaces and display the loop protection state..... 362
Denial of service..... 363
Configure Auto-DoS..... 363
Configure individual denial of service attack options..... 364

Chapter 8 Configure Access Control Lists

About access control lists..... 369
ACL Wizard..... 369
Use the ACL Wizard to create a simple ACL..... 369
Change an ACL rule that you created with the ACL Wizard.. 373
Remove an ACL that you created with the ACL Wizard..... 375
MAC ACLs..... 376
Add a MAC ACL..... 376
Change the name of a MAC ACL..... 377

Remove a MAC ACL..... 378
MAC ACL rules..... 379
Add a rule for a MAC ACL..... 379
Change the match criteria for a MAC ACL rule..... 382
Remove a rule from a MAC ACL..... 383
MAC ACL bindings..... 384
Configure a MAC ACL interface binding..... 384
Display or delete MAC ACL bindings..... 385
IPv4 ACLs..... 387
Add an IPv4 ACL..... 387
Change the number or name of an IPv4 ACL..... 389
Remove an IPv4 ACL..... 390
Standard IPv4 ACL rules..... 390
Add a rule for a standard IPv4 ACL..... 391
Change the match criteria for a standard IPv4 ACL rule..... 393
Remove a rule from a standard IPv4 ACL..... 394
Extended IPv4 ACL rules..... 395
Add a rule for an extended IPv4 ACL..... 396
Change the match criteria for an extended IPv4 ACL rule.... 402
Remove a rule from an extended IPv4 ACL..... 403
IPv6 ACLs..... 404
Add an IPv6 ACL..... 404
Change the name of an IPv6 ACL..... 405
Remove an IPv6 ACL..... 406
IPv6 ACL rules..... 407
Add a rule for an IPv6 ACL..... 407
Change the match criteria for an IPv6 ACL rule..... 413
Remove a rule from an IPv6 ACL..... 414
IP ACL bindings..... 415
Configure an IP ACL interface binding..... 415
Display or delete IP ACL bindings..... 416
Display the existing ACLs and associated rules..... 417
VLAN ACL bindings..... 419
Configure a VLAN ACL binding..... 419
Display or delete VLAN ACL bindings..... 420

Chapter 9 Maintenance and Troubleshooting

Reboot the switch from the device UI..... 423
Reset the switch to factory default settings..... 424
Export the configuration file or log files from the switch 425
Export a file from the switch to a TFTP server..... 425
Export a file from the switch to a computer or USB storage device..... 427

Export a file from the switch to a directly-attached USB storage device..... 428
Update the switch software..... 429
Update the switch software through the device UI..... 430
Download the switch software from a TFTP server and update the switch..... 431
Update the switch software through the device UI..... 433
Download the switch software from a computer or USB storage device and update the switch..... 435
Download the switch software from a directly-attached USB storage device and update the switch..... 437
Download a file to the switch..... 439
Download a file from a TFTP server to the switch..... 439
Download a file from a computer or USB storage device to the switch..... 441
Download a text configuration file from a directly-attached USB storage device to the switch..... 443
Download and install an SSL security certificate file on the switch..... 444
Manage software images..... 446
Change the software image that loads when the switch starts. 446
Display the dual image configuration and add image descriptions..... 447
Copy a software image from one flash sector to another..... 448
Delete a software image..... 449
Diagnostics and troubleshooting..... 450
Ping an IPv4 address..... 450
Ping an IPv6 address..... 452
Send an IPv4 traceroute..... 453
Send an IPv6 traceroute..... 455
Enable the secure diagnostic mode..... 457
You cannot log in to the switch..... 458

Chapter 10 Monitor the Switch and Network

Switch, port, and EAP packet statistics..... 460
Display or clear switch statistics..... 460
Display or clear port statistics..... 462
Display or clear detailed statistics for a port..... 463
Display or clear EAP and EAPoL statistics..... 469
Perform a cable test..... 471
Logs..... 472
Message log format..... 472
Manage and display the memory log..... 473
Manage and display the flash log..... 475

Syslog and log server host settings..... 477
Configure the syslog settings..... 477
Add a syslog server..... 478
Change the settings for a syslog server..... 480
Delete the settings for a syslog server..... 480
Trap log..... 481
Port mirroring..... 482
Set up a port mirroring configuration..... 482
Remove a port mirroring probe..... 484
Switch CPU..... 485
Display the system CPU memory status and CPU utilization. 485
Configure the CPU thresholds..... 486

Appendix A Configuration Examples

Virtual Local Area Networks (VLANs)..... 489
VLAN example configuration..... 490
Access control lists (ACLs)..... 493
MAC ACL example configuration..... 494
Standard IP ACL sample configuration..... 497
Differentiated Services (DiffServ)..... 500
DiffServ classes..... 501
DiffServ traffic classes..... 502
DiffServ policies..... 502
DiffServ traffic conditioning policy..... 502
DiffServ example configuration..... 504
802.1X port access control 507
802.1X example configuration..... 509
Multiple Spanning Tree Protocol..... 511
MSTP example configuration..... 513

Appendix B Software Default Settings and Hardware Specifications

Access default settings for the switch device UI..... 520
System features default settings..... 520
VLAN features default settings..... 524
Switching features default settings..... 526
Multicast features default settings..... 529
QoS features default settings..... 532
Security features default settings..... 535
ACL features default settings..... 538
Monitoring features default settings..... 539
Hardware technical specifications..... 540

1

Get Started

This user manual describes how you can use the device user interface (UI) to configure and operate the following NETGEAR 8-Port, 24-Port and 48-Port Gigabit Ethernet PoE+ Smart Switches with 2 or 4 SFP Ports and Optional Remote/Cloud Management:

- **GS324TPv2**: NETGEAR 24-Port Gigabit Ethernet PoE+ Smart Managed Essentials Switch with 2 Dedicated SFP Ports. This model provides a PoE power budget of 190W.
- **GS348TPv2**: NETGEAR 48-Port Gigabit Ethernet PoE+ Smart Managed Essentials Switch with 4 Dedicated SFP Ports. This model provides a PoE power budget of 380W.

The manual describes the software configuration procedures and explains the options that are available within those procedures.

The chapter contains the following sections:

- Available publications and online help
- Manage the switch by using the device UI
- About on-network and off-network access
- Access the switch on-network and connected to the Internet
- Access the switch off-network and not connected to the Internet
- Register the switch
- Change the language of the device UI
- Change the theme of the device UI
- Configure ports using the Device View
- Access the NETGEAR support website
- Access the user manual online

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

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

Available publications and online help

You can download the following publications and more for your switch by visiting netgear.com/support/download and entering your model number in the search box.

- Installation Guide
- User Manual (this manual)
- Lite CLI manual

When you are logged in to the device UI, you can access documentation online by selecting **Help** and clicking the link in the User Manual section.

In addition, context-sensitive online help is available in the device UI.

Manage the switch by using the device UI

This manual describes how to use the device UI to manage and monitor the switch.

Device UI buttons and user-defined fields

The following table shows the *general* buttons that are used on the pages in the device UI. (Some pages have unique buttons.)

Table 1. Device UI buttons

Button	Function
Apply	Click the **Apply** button on a device UI page to save configuration changes, which take effect immediately and are retained when you reboot the switch.
Save	Click the **Save** button in a device UI pop-up window to save configuration changes, which take effect immediately and are retained when you reboot the switch.
Add	Click the **Add** button in a device UI pop-up window to add and save a configuration, which takes effect immediately and is retained when you reboot the switch.
Add New	Click the **Add New** button to add a new item to the configuration.
Edit	Click the **Edit** button to change a selected item.

Table 1. Device UI buttons (Continued)

Button	Function
Delete	Click the **Delete** button to remove a selected item.
Refresh	Click the **Refresh** button to update the page with the latest information from the switch.
Cancel	Click the **Cancel** button to cancel your configuration changes on a device UI page or pop-up window.
Back	Click the **back** button to return to the previous page or the main page for a feature.
Clear	Click the **Clear** button to reset statistics on the page.
Logout	Click the **Logout** button to end the device UI session.

User-defined fields can contain alphanumeric and special characters except for the following special characters (unless specifically noted for a feature on a device UI page):

Table 2. 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 Ethernet interfaces and Gigabit fiber interfaces, which are numbered on the front panel. You configure the logical interfaces.

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

Table 3. Naming conventions for interfaces

Interface	Description	Example
Physical Ethernet interfaces	Gigabit Ethernet interfaces, which also support 100 Mbps and 10 Mbps	g1, g2, g3, and so on
Physical fiber interfaces	SFP or SFP+ ports, in which you can install 1G transceiver modules. Depending on the model, you can also insert 10G transceiver modules.	g25 and g26
Link aggregation group (LAG)	A LAG interface is a logical interface (channel) that aggregates two or more physical ports.	ch1 with LAG ID l1, ch2 with LAG ID l2, ch3 with LAG ID l3, and so on

Table 3. Naming conventions for interfaces (Continued)

Interface	Description	Example
Routing VLAN interfaces	This is an interface used for routing functionality.	VLAN 1, VLAN 2, VLAN 3, and so on
CPU management interface	This is the internal switch interface c/1 responsible for the switch base MAC address. This interface is not configurable and is always listed in the MAC address table.	c1

Save your changes in the device UI

When you click the **Apply** button in the device UI, your changes are saved and are retained when you restart the switch. That is, your changes are saved to both the running configuration and the startup configuration of the switch.

Context-sensitive help

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

About on-network and off-network access

You can access the switch either on-network or off-network:

- **On-network and connected to the Internet**: When you use the device UI, for easiest access, we recommend that you cable the switch to a network that is connected to the Internet and that includes 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 to connect to the device UI. We refer to this setup as on-network.

  For more information, see Access the switch on-network and connected to the Internet on page 20.
- **Off-network and not connected to the Internet**: You can also configure the switch connected directly only to the computer that you are using to configure it. That is,

the switch is not connected to the network and the Internet. We refer to this setup as off-network or offline. If your network does not include a DHCP server (or a router that functions as a DHCP server), you must access the switch off-network.

For more information, see Access the switch off-network and not connected to the Internet on page 26.

Note: We recommend that you register the switch to activate your warranty. For more information, see Register the switch on page 27.

Access the switch on-network and connected to the Internet

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

If the switch is on-network, connected to a DHCP server, and connected to the Internet, you can use a Windows-based computer to access the device UI. We also recommend that you register the switch with NETGEAR to activate your warranty. For more information about accessing the device UI, see Use a Windows-based computer to access the switch on-network and connected to the Internet on page 21.

If you use a Mac, or if you do not know the IP address of the switch, use one of the following tools to discover the IP address of the switch on the network:

- **NETGEAR Discovery Tool (NDT)**: If you use a Mac or a Windows-based computer, you can use the NDT to discover the switch on your network. See Use the NETGEAR Discovery Tool to discover the switch when it is connected to the Internet on page 22.
- **Other tools**: You can also get the IP address of the switch from the DHCP server in the network or use an IP scanner utility. See Use other options to discover the switch IP address on page 24.

When you know the IP address, you can configure and manage the switch using the device UI. For configuration of all switch features, see Access the switch on-network when you know the switch IP address on page 24.

Use a Windows-based computer to access the switch on-network and connected to the Internet

For the following procedure, the network must provide Internet access.

To use a Windows-based computer to determine the switch IP address and access the switch on-network and connected to the Internet:

1. Cable the switch to a network with a router or DHCP server that manages IP addresses.
2. Power on the switch.

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

   You can use a WiFi or wired network connection.
4. Open File Explorer.
5. Click the **Network** link.
6. If prompted, enable the Network Discovery feature.
7. Under Network Infrastructure, locate the switch model number.
8. Double-click **XXmodel-YYYYYY**, in which XXmodel is the model number of your switch and YYYYYY represents the last six digits of the switch MAC address.

   The page that displays depends on whether your browser is connected to the Internet, whether the switch is connected to the Internet, and whether you registered the switch.
9. Enter your credentials, which depend on the page that displays:
   - **Registration options page displays**: If you did not yet activate your warranty, a page with the following options displays:
     - **Register to Activate Your Warranty**: To activate your warranty, click the **>** button, and follow the directions onscreen to register the switch with your email address and password. After you activate your warranty, you are no longer prompted to register the switch.

       If you do not have a NETGEAR account, you can create one.
     - **Enter Registration Key**: If you obtained a registration key, enter it in the **Registration Key** field, and click the **Submit** button. For more information,

see Register the switch with your NETGEAR account and get a registration key for offline access on page 28.

- **Skip Registration & Access the UI**: To access the device UI without activating your warranty, click the **>** button, and log in. You do not need to register the switch to activate your warranty, but if you do not activate your warranty within 30 days of purchase, your warranty entitlement might be affected.

  If you do not activate your warranty, the registration options page continues to display when you log in.

- **Device Admin Password page displays**: If you previously registered the switch with NETGEAR to activate your warranty, the Device Admin Password page displays. Enter the device admin password. The default device admin password is **password**. The first time that you enter the default device admin password, the Change Default Password page displays, requiring you to customize the device admin password for greater security.

10. If you enter a password, click the **Login** button.
11. If the Change Default Password page displays, specify and confirm a new device admin password, click the **Submit** button, and log in again with your new password.

    The Dashboard page displays. You can now configure the switch.

Use the NETGEAR Discovery Tool to discover the switch when it is connected to the Internet

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

The NETGEAR Discovery Tool (NDT) lets you discover the switch in your network and access the device UI of the switch from a Mac or a Windows-based computer.

To install the NDT and discover the IP address of the switch in your network when the switch is connected to the Internet:

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

   Depending on the computer that you are using, download either the Mac version or the version for a Windows-based computer.
2. Temporarily disable the firewall, Internet security, antivirus programs, or all of these on the computer that you use to configure the switch.

3. Unzip the NDT files, and click or double-click the **.exe** file to install the program on your computer.

   You might see the tool icon appear on your Mac dock or Windows desktop.
4. Reenable the security services on your computer.
5. Power on the switch.

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

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

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

   The initial page displays a menu and a button.
8. From the **Choose a connection** menu, select the network for this switch.
9. Click the **Start Searching** button.

   The NDT displays the IP addresses of the switches that it discovers.
10. Click the **ADMIN PAGE** button next to your switch.

    The page that displays depends on whether you registered the switch.
11. Enter your credentials, which depend on the page that displays:
    - **Registration options page displays**: If you did not yet activate your warranty, a page with the following options displays:
      - **Register to Activate Your Warranty**: To activate your warranty, click the **>** button, and follow the directions onscreen to register the switch with your email address and password. After you activate your warranty, you are no longer prompted to register the switch.

        If you do not have a NETGEAR account, you can create one.
      - **Enter Registration Key**: If you obtained a registration key, enter it in the **Registration Key** field, and click the **Submit** button. For more information, see Register the switch with your NETGEAR account and get a registration key for offline access on page 28.
      - **Skip Registration & Access the UI**: To access the device UI without activating your warranty, click the **>** button, and log in. You do not need to register the switch to activate your warranty, but if you do not activate your warranty within 30 days of purchase, your warranty entitlement might be affected.

If you do not activate your warranty, the registration options page continues to display when you log in.

- **Device Admin Password page displays**: If you previously registered the switch with NETGEAR to activate your warranty, the Device Admin Password page displays. Enter the device admin password. The default device admin password is **password**. The first time that you enter the default device admin password, the Change Default Password page displays, requiring you to customize the device admin password for greater security.

12. If you enter a password, click the **Login** button.
13. If the Change Default Password page displays, specify and confirm a new device admin password, click the **Submit** button, and log in again with your new password.

    The Dashboard page displays. You can now configure the switch.

Use other options to discover the switch IP address

If the switch is on-network, you can use one of the following options to determine the switch IP address:

- **Access the DHCP server**: You can access the DHCP server (or router that functions as a DHCP server) in your network and view the IP address that is assigned to the switch. For more information, see the documentation for your DHCP server (or router).
- **IP scanner utility**: IP scanner utilities are available free of charge on the Internet. An IP scanner utility lets you discover the IP address that is assigned to the switch.

For information about how to access the device UI of the switch, see Access the switch on-network when you know the switch IP address on page 24.

Access the switch on-network when you know the switch IP address

If the switch is on-network and you know the switch IP address, you can access the device UI.

For the following procedure, the network must provide Internet access.

To access the switch on-network when you know the switch IP address:

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

The page that displays depends on whether your browser is connected to the Internet, whether the switch is connected to the Internet, and whether you registered the switch.

3. Enter your credentials, which depend on the page that displays:
   - **Registration options page displays**: If you did not yet activate your warranty, a page with the following options displays:
     - **Register to Activate Your Warranty**: To activate your warranty, click the **>** button, and follow the directions onscreen to register the switch with your email address and password. After you activate your warranty, you are no longer prompted to register the switch.

       If you do not have a NETGEAR account, you can create one.
     - **Enter Registration Key**: If you obtained a registration key, enter it in the **Registration Key** field, and click the **Submit** button. For more information, see Register the switch with your NETGEAR account and get a registration key for offline access on page 28.
     - **Skip Registration & Access the UI**: To access the device UI without activating your warranty, click the **>** button, and log in. You do not need to register the switch to activate your warranty, but if you do not activate your warranty within 30 days of purchase, your warranty entitlement might be affected.

       If you do not activate your warranty, the registration options page continues to display when you log in.
   - **Device Admin Password page displays**: If you previously registered the switch with NETGEAR to activate your warranty, the Device Admin Password page displays. Enter the device admin password. The default device admin password is **password**. The first time that you enter the default device admin password, the Change Default Password page displays, requiring you to customize the device admin password for greater security.
4. If you enter a password, click the **Login** button.
5. If the Change Default Password page displays, specify and confirm a new device admin password, click the **Submit** button, and log in again with your new password.

   The Dashboard page displays. You can now configure the switch.

Access the switch off-network and not connected to the Internet

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 off-network must be in the same subnet as the default IP address of the switch.

To access the switch off-network and enter the registration key before you log in to the device UI:

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

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

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

   - **Windows-based computer**: See the following article: kb.netgear.com/27476
   - **Mac**: See the following article, which is written for an access point but is also valid for a switch: kb.netgear.com/000037250
2. Connect your computer to the switch using an Ethernet cable.
3. Power on the switch by connecting its power cord.
4. Open a web browser, and enter **http://192.168.0.239**.

   This is the default IP address of the switch. If you already disabled the DHCP client and assigned a static IP address to the switch, enter the static IP address of the switch.

   The registration options page displays.
5. Do one of the following:

   - **Enter a registration key**: If you obtained a registration key, type or paste the key in the **Registration Key** field, and click the **Submit** button.

     For more information, see Register the switch with your NETGEAR account and get a registration key for offline access on page 28.
   - **Do not register at this time and access the device UI**: Do the following:

     a. In the Skip Registration & Access the UI section, click the **>** button, and log in.

The Device Admin Password page displays.

b. Enter the device admin password. The default device admin password is **password**. The first time that you enter the default device admin password, the Change Default Password page displays, requiring you to customize the device admin password for greater security.

c. Click the **Login** button.

6. If the Change Default Password page displays, specify and confirm a new device admin password, click the **Submit** button, and log in again with your new password.

   The Dashboard page displays. You can now configure the switch.

7. 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 and use the switch on-network.

Register the switch

You can register the switch online or offline to activate your warranty, after which you are no longer prompted to activate your warranty when you log in:

- **Online registration for on-network access**: If your switch is on-network or connected to the Internet, you can register the switch with your NETGEAR account credentials and activate your warranty. During the registration process, the switch contacts a NETGEAR server. For more information, see Register and access the switch on-network with your NETGEAR account on page 27.
- **Registration for off-network access**: You can register your switch from any device that is connected to the Internet and get a registration key. If the switch is off-network or not connected to the Internet, you can enter the registration key. After you do so, the Register to activate your warranty page no longer displays when you log in. For more information, see Register the switch with your NETGEAR account and get a registration key for offline access on page 28.

Register and access the switch on-network with your NETGEAR account

For initial registration and access with your NETGEAR account, the switch must be connected to the Internet so that it can communicate with a NETGEAR server.

If you do not have a free NETGEAR account, you can create one during the registration process.

To register and access the switch on-network over the device UI with your NETGEAR account:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and enter the registration key before you log in on page 30.

   The registration options page displays.

3. In the Register to Activate Your Warrant section, click the **>** button and follow the directions onscreen to register the switch with your email address and password and activate the warranty.

   You are only prompted to do this once to confirm registration of your switch.

   If you did not yet create a NETGEAR account, click the **Create account** link, follow the directions onscreen to create an account, and register the switch with your email address and password.

4. If the Change Default Password page displays, specify and confirm a new device admin password, click the **Submit** button, and log in again with your new password.

   The Dashboard page displays. You can now configure the switch.

Register the switch with your NETGEAR account and get a registration key for offline access

Note: If you register your switch with your NETGEAR account and then access the switch connected to the Internet, you do not need a registration key because the Device Admin Password page displays. That is, you are no longer prompted to activate your warranty.

After you register your switch with your NETGEAR account, you can get a registration key, access the switch offline or not connected to the Internet, and either before or after you log in to the device UI, enter the registration key. After you enter the registration key, you are no longer prompted to activate your warranty. Instead, the Device Admin Password page displays.

You can visit my.netgear.com, log in to your NETGEAR account, register the switch using its serial number, and get a registration key.

To register the switch with your NETGEAR account and get a registration key:

1. From a computer or mobile device that is connected to the Internet, go to my.netgear.com.
2. Log in to your NETGEAR account.

   If you do not have a free NETGEAR account, you can create one.

   The Your Registered Products page displays.
3. Click the **REGISTER NEW PRODUCT** button.
4. In the **SERIAL NUMBER** field, type the serial number of your switch.

   The serial number is 13 digits long. It is printed on the switch label.
5. From the **PURCHASE DATE** menus, select the date that you purchased the switch.
6. Click the **REGISTER** button.

   Your switch is registered to your NETGEAR account.

   A confirmation email is sent to your NETGEAR account email address.
7. On the YOUR REGISTERED PRODUCTS page, click **VIEW PRODUCT** button for the switch that you just registered.

   The Registration Key field displays the registration key for your switch. You can use this key to access the switch offline.

Access the switch with a registration key

After you get a registration key, you can access the switch either off-network or on-network and enter the registration key. For more information, see one of the following sections:

- Access the switch off-network and enter the registration key before you log in on page 30
- Access the switch on-network and enter the registration key after you log in on page 31

After you enter the registration key, you are no longer prompted to activate your warranty when you log in. Instead, the Device Admin Password page displays.

Access the switch off-network and enter the registration key before you log in

For information about getting a registration key, see Register the switch with your NETGEAR account and get a registration key for offline access on page 28.

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 off-network must be in the same subnet as the default IP address of the switch.

To access the switch off-network and enter the registration key before you log in to the device UI:

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

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

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

   - **Windows-based computer**: See the following article: kb.netgear.com/27476
   - **Mac**: See the following article, which is written for an access point but is also valid for a switch: kb.netgear.com/000037250

2. Connect your computer to the switch using an Ethernet cable.
3. Power on the switch by connecting its power cord.
4. Open a web browser, and enter **http://192.168.0.239**.

   This is the default IP address of the switch. If you already disabled the DHCP client and assigned a static IP address to the switch, enter the static IP address of the switch.

   The registration options page displays.
5. Type or paste the key
6. Click the **Submit** button.
7. If the Change Default Password page displays, specify and confirm a new device admin password, click the **Submit** button, and log in again with your new password.

   The Dashboard page displays. You can now configure the switch.
8. 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 and use the switch on-network.

Access the switch on-network and enter the registration key after you log in

For information about getting a registration key, see Register the switch with your NETGEAR account and get a registration key for offline access on page 28.

To access the switch on-network and enter the registration key after you log in to the device UI:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and enter the registration key before you log in on page 30.

   The registration options page displays.

3. In the Skip Registration & Access the UI section, click the **>** button, and log in.

   The Device Admin Password page displays.

4. Enter the device admin password. The default device admin password is **password**. The first time that you enter the default device admin password, the Change Default Password page displays, requiring you to customize the device admin password.

5. Click the **Login** button.

   The Dashboard page displays.

6. Select **Maintenance > Registration Key**.

   The Registration Key page displays.

7. In the field, type or paste the registration key.

8. Click the **Submit** button.

   The registration takes effect on the switch and you are no longer prompted to activate your warranty when you log in.

   After successful registration, the **Maintenance > Registration Key** menu option and Registration Key page are hidden in the device UI.

Change the language of the device UI

You can set the language of the device UI to a specific one.

To change the language of the device UI:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. At the top right of the page, to the left of the Logout button, click the language button.

   The Select Language pop-up menu displays.
6. Select the radio button for a language.
7. Click the **Apply** button.

   You are logged out. The language of the device UI is set to the language that you selected.

   To continue configuring the switch, log in again.

Change the theme of the device UI

You can set the theme of the device UI to a specific one.

To change the theme of the device UI:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. At the top right of the page, to the left of the language button, click the theme button.

   The Select Theme pop-up menu displays.

6. Select the radio button for a theme.
7. Click the **Apply** button.

   You are logged out. The theme of the device UI is set to the theme that you selected.

   To continue configuring the switch, log in again.

Configure ports using the Device View

The Device View in the device UI displays the ports on the switch. This graphic tool provides an alternate way to navigate to port configuration and monitoring options.

To configure ports using 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   (If you are already logged into the device UI, select **Dashboard**.)

   The Dashboard page displays. The Device View pane shows the ports of the switch.
5. To display a port menu that shows the configuration and monitoring options, click a port.

   A pop-up menu displays.
6. Select a menu item.

   The associated page displays, allowing you to configure or monitor the port.

Access the NETGEAR support website

From the device UI, you can access the NETGEAR support website at netgear.com/support.

To access the NETGEAR support website from the device UI:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Help**.

The Online Help page displays.

6. In the Support section, click the link.

   The NETGEAR support website opens.

Access the user manual online

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

To access the user manual online from the device UI:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Help**.

   The Online Help page displays.

6. In the User Manual section, click the link.

   The NETGEAR Download Center website opens.

7. Enter the model number of the switch and select the model from the menu.

   The page displays the documentation that is available for your model, including the user manual.

2

Configure Switch System Settings

This chapter covers the following topics:

- Dashboard
- Display port utilization and port connections
- Configure and display general switch system information
- Display information about switch hardware components and firmware
- IP network settings for management access
- Time and SNTP settings
- Domain Name System
- Manage switch discovery protocols
- Display USB device information
- LLDP and LLDP-MED settings for the switch
- Simple Network Management Protocol
- Configure HTTPS access settings
- HTTPS management access
- SSH management access
- Configure inbound Telnet settings
- DHCP snooping
- DHCP Layer 2 relay

Dashboard

The information that is displayed on the dashboard is mostly self-explanatory.

Display VLAN membership

The Dashboard displays information about VLAN membership on the switch.

To display information about 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

The VLAN Membership section displays the number of member interfaces for each configured VLAN. If you did not configure any custom VLANs, the section displays only the following preconfigured VLANs: default, Auto-WiFi, Auto-Camera, Auto-VoIP, and Auto-Video.

For more information about VLANs, see Manage VLANs on page 119.

Display switch device details

The Dashboard displays switch device details.

To display switch device details:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

The following table describes the information that displays in the Device Details section,

Field	Description
Name	The system name that you configured, if any. For more information, see Configure and display general switch system information on page 40.
Serial Number	The serial number of the switch. This field is fixed.
Model	The model number of the switch. This field is fixed.
MAC Address	The MAC address of the switch. This field is fixed.
Uptime	The period in days, hours, minutes, and seconds since the switch was last started.
IP Address	The management IP address at which you can access the device UI. For more information, see IP network settings for management access on page 45.
Date & Time	The current date and time. For more information, see Time and SNTP settings on page 52.
Firmware Version	The active main firmware version of the switch (see Manage software images on page 446).

Display port utilization and port connections

The Dashboard displays port utilization and port connections.

To display port utilization and port connections:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

The following table describes information about port utilization.

Field	Description
Connected	The total number of connected ports, excluding ports that are connected to a powered device (PD) that is receiving any level of power over Ethernet (PoE) from the switch
Disabled	The total number of disabled ports
Connected and Powered	The total number of ports that are connected to a PD that is receiving any level of PoE from the switch
Available	The total number of available ports, including ports that are not connected to a device and excluding SFP and SFP+ fiber ports in which no SFP transceiver module is inserted

For more information about ports, see Configure the port settings and maximum frame size on page 190.

The following table describes information about the port connections in the Device View section.

Field	Description
Connected	The port is connected to a device that is powered up. The port is not connected to a PD that is receiving any level of PoE from the switch.
Disabled	The port is disabled.
Connected and Powered	The port is connected to a PD that is receiving any level of PoE from the switch.
Available	The port is not connected to a device but is available.
1G SFP Fiber Port	The port is a 1G SFP fiber port that can accept an SFP transceiver module.

(Continued)

Field	Description
PoE	The port is a PoE port. Depending on the switch model, the port can provide PoE+ or both PoE+ and PoE++. For more information, see Power over Ethernet on page 168.
Blocked	The port is blocked. That is, STP blocked the port to prevent a loop. For more information, see Configure the port settings and maximum frame size on page 190 and Loop protection on page 359.
Link Disabled	The port is administratively down. For more information, see Configure the port settings and maximum frame size on page 190.

For information about how you can use the Device View to configure the ports and the switch, see Configure ports using the Device View on page 33.

Configure and display general switch system information

You can configure the switch system name, location, and contact and display general switch information.

To configure and display general system information:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Management > System Information**.

   The System Information page displays.

6. Optionally, configure the following fields:
   - **System Name**: Type a name to identify this switch.
   - **System Location**: Type the location for this switch.
   - **System Contact**: Type the name of a contact person for this switch.

   For each field, you can use up to 255 alphanumeric characters.
7. Click the **Apply** button.

   Your settings are saved.

The following table describes the system information on the page.

Table 4. System information

Field	Description
Product Name	The product and model name of the switch
System Up Time	The time in days, hours, and minutes since the switch was restarted
Base MAC Address	Universally assigned network address
Date & Time	The current date and time, including the time zone
Serial Number	The serial number of the switch
System Object OID	The base object ID for the enterprise MIB of the switch

Display information about switch hardware components and firmware

You can display information about switch hardware components such as power supplies, temperature sensors, and fans, and information about the boot version and software version on the switch.

Display the power supply information

You can view information about the power supplies.

To display the power supply 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

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

   The System Information page displays.

The following table describes the view-only power supply information.

Table 5. Power supply information

Field	Description
Power supply	The ID number, which is always 1
Description	The description is always PS-1
Type	The type is always Fixed
Operational	The status of the power supply in the switch is always Operational. (If the power supply failed, you would not be able to access the device UI.)

Display the boot and software version

You can display the boot and software (firmware) versions that are running on the switch.

To display the boot and 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Management > System Information**.

   The System Information page displays.

The following table describes the version information.

Table 6. Version information

Field	Description
Model Name	The model number of the switch
Boot Version	The version of the boot code that is in the flash memory to load the software into the memory
Software Version	The release, version, and maintenance number of the software that is running on the switch. For example, if the release is 1, the version is 2.0, and the maintenance number is 3.5, the format is 1.2.0.3.5.

Display the temperature sensor information

You can view the current temperature of different system sensors using the Temperature Status table.

To display the temperature sensor 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Management > System Information**.

   The System Information page displays.
6. To refresh the page, click the **Refresh** button.

   The following table describes the view-only Temperature Status information.

Table 7. Temperature Status information

Field	Description
Sensor	The ID of the sensor
Description	The description of the sensor (System or MAC)
Temp (C)	The current temperature of the sensor in Celsius
State	Indicates if the sensor is operating normally
Max Temp (C)	The maximum temperature in Celsius that the sensor detected

Display the status of the fans

The fans remove the heat generated by the power, CPU, and other chipsets, and allow the chipsets work normally.

To display the status of the fans:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.

4. Click the **Login** button.
   The Dashboard page displays.
5. Select **System > Management > System Information**.
   The System Information page displays.

The following table describes the fan information.

Table 8. Fan information

Field	Description
FAN	The ID of the fan
Description	The description of the fan, such as Fan-1
Type	The type of fan is always Fixed
Speed	The speed of the fan
Duty Level (%)	The duty level of the fan in percentage
State	The status of the fan: • **Operational**: The fan is running normally. • **Failure**: The fan failed. • **Stop**: The fan stopped because the switch temperature is low. The fan will start if the switch temperature rises.

IP network settings for management access

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

Configure the IPv4 management interface

You can restrict IPv4 management to one specific interface. You can use any of the interfaces as an IPv4 management interface.

To configure an IPv4 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

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

   The IP Network Configuration page displays.

6. Select a radio button for the configuration of the switch management interface:

   - **Static IP Address**: You must manually configure the IP address, subnet mask, and default gateway. Enter this information in the fields below the radio buttons.
   - **Dynamic IP Address (BOOTP)**: The switch must obtain the IP address through a BootP server.
   - **Dynamic IP Address (DHCP)**: The switch must obtain the IP address through a DHCP server. This is the default setting.

7. If you selected 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.
   - **Subnet Mask**: The IP subnet mask for the interface.
   - **Default Gateway**: The default gateway for the IP interface.

8. Click the **Apply** button.

   Your settings are saved.

Change 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. By default, the management

VLAN ID is 1, which allows an IP connection to be established through any port. If this configuration works well for your network, you do not need to change the management VLAN.

If you change the management VLAN, you can make an IP connection only through a port that is a member of the management VLAN. Also, the port VLAN ID (PVID) of the port that you use to connect to the 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 Add a VLAN on page 121 and Change the port VLAN ID (PVID) settings on page 127.

The following applies to the management VLAN:

- Only one management VLAN can be active at a time.
- If you change the management VLAN, connectivity through the existing management VLAN is lost.
- You might need to reconnect the computer that you use to access the switch to another port that is a member of the new management VLAN.

To change 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The IP Network Configuration page displays.
6. In the **Management VLAN** field, type the new management VLAN ID of the switch.

You can type an ID in the range of 1 to 4093, but make sure that the new management VLAN exists.

Caution: After you click the **Apply** button, your connection might be lost and you might need to reconnect your computer to another port that is a member of the new management VLAN.

7. Click the **Apply** button.

   Your settings are saved.

Configure an IPv6 management interface through autoconfiguration or a DHCPv6 server

You can restrict IPv6 management to one specific interface. You can use any of the interfaces as an IPv6 management interface and configure the IPv6 address through autoconfiguration or a DHCPv6 server.

To configure an IPv6 management interface through autoconfiguration or a DHCPv6 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

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

   The IPv6 Network Configuration page displays.

6. Click the **Allow IPv6 Network** toggle to enable management of the switch over IPv6:

- **The toggle is gray and positioned to the left**: Management over IPv6 is disabled.
- **The toggle is purple and positioned to the right**: Management over IPv6 is enabled. This is the default setting.

7. Click the **IPv6 Address Auto Configuration Mode** toggle to allow the switch to autoconfigure its IPv6 address:
   - **The toggle is gray and positioned to the left**: IPv6 address autoconfiguration is disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: IPv6 address autoconfiguration is enabled.

   When this mode is enabled, the network interface can acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of router advertisement messages. When this mode is disabled, the network interface does not use the native IPv6 address auto-configuration features to acquire an IPv6 address. Use auto-configuration only if you do not use a DHCPv6 server.
8. To enable the DHCPv6 client mode, which allows the switch to receive an IPv6 address from a DHCPv6 server in your network, select the **DHCPv6** radio button.

   If the DHCPv6 client mode is enabled, the network interface attempts to acquire network information from a DHCPv6 server. By default, the None radio button is selected, and the DHCPv6 client mode is disabled.
9. If you enable the DHCPv6 client mode, in the **IPv6 Gateway** field, type the IPv6 address of the IPv6 gateway.

   The gateway address must be in IPv6 global or link-local address format.
10. Click the **Apply** button.

    Your settings are saved.

Manage a static IPv6 address for the IPv6 management interface

You can add a static IPv6 address that is specific to the IPv6 management interface. You can also change an existing IPv6 address or remove an IPv6 address that you no longer need for the IPv6 management interface.

When you add a static IPv6 address, you need to configure an IPv6 prefix and prefix length, and you need to enable or disable the Extended Unique Identifier (EUI).

IPv6 addresses are denoted by eight groups of hexadecimal quartets that are separated by colons. You can reduce any four-digit group of zeros within an IPv6 address to a single zero or omit it. The following errors invalidate an IPv6 address:

- More than eight groups of hexadecimal quartets
- More than four hexadecimal characters in a quartet
- More than two colons in a row

To add, change, or remove an IPv6 address for the IPv6 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Management > IP Network > IPv6 Network Configuration**.

   The IPv6 Network Configuration page displays.
6. To add an IPv6 address, in the IPv6 Network Interface Configuration section, do the following:
   a. Click the **Add New** button.

      The Add IPv6 Network Interface Configuration pop-up window displays.
   b. In the **IPv6 Prefix/Prefix Length** field, type the IPv6 address.
   c. From the **EUI64** menu, select to enable or disable the EUI:
      - **True**: The IPv6 management interface uses its MAC address to generate a unique 64-bit interface ID.
      - **False**: The EUI is not used.
   d. Click the **Save** button.

      Your settings saved.
7. To change an IPv6 address, do the following:
   a. Select the check box for the IPv6 address.
   b. Click the **Edit** button.

      The Edit IPv6 Network Interface Configuration pop-up window displays.

c. Change the settings as needed.
d. Click the **Save** button.

   Your settings saved.

8. To remove an IPv6 address, do the following:
   a. Select the check box for the IPv6 address.
   b. Click the **Delete** button.

      Your settings saved and the IPv6 address is removed.

Display IPv6 network interface neighbors

You can display the IPv6 neighbors to which the IPv6 network interface is connected in the network.

To display the IPv6 network interface neighbors:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Management > IP Network > IPv6 Network Neighbor**.

   The IPv6 Network Neighbor page displays.
6. To refresh the page, click the **Refresh** button.

The IPv6 Network Interface Neighbor table displays the following view-only fields.

Table 9. IPv6 network interface neighbor information

Field	Description
IPv6 Address	The IPv6 address of the neighboring device
MAC Address	The MAC address of the neighboring device
isRtr	Indicates if the neighboring device is a router (True) or not (False)
Neighbor State	The state of the neighboring device: • **Reachable**: The switch can reach the neighboring device. • **Stale**: Information about the neighboring device is scheduled to be deleted. • **Delay**: The switch did not receive information from the neighboring device during the delay period. • **Probe**: The switch is attempting to probe for the neighboring device. • **Unknown**: The status is not known.
Last Update	The last time that the information for the neighboring device was updated

Time and SNTP settings

The switch supports the Simple Network Time Protocol (SNTP). As its name suggests, it is a less complicated version of Network Time Protocol (NTP), 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.

Set the time manually

You can view and adjust date and time settings.

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

To set the time manually:

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

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

   The Time Configuration page displays.
6. Select the Clock Source **Local** radio button.

   The default is Local.
7. In the **Date** field, type the current date in months, days, and years (MM/DD/YYYY).
8. In the **Time** field, type the current time in hours, minutes, and seconds (HH/MM/SS).
9. In the **Time Zone Name** field, type the name or acronym of the time zone.

   In the **Offset Hours** and **Offset Minutes** fields, you can also specify the number of hours and number of minutes that the time zone differs from the Coordinated Universal Time (UTC). The time zone can affect the display of the current system time, for which the default is UTC.

   - **Offset Hours**: Set the number of hours that the time zone differs from the UTC.

     The range is from –12 to 13 hours. The default is 0 hours
   - **Offset Minutes**: Set the number of minutes that the time zone differs from the UTC.

     The range is from 0 to 59 minutes. The default is 0 minutes.
10. Click the **Apply** button.

    Your settings are saved.

Configure SNTP for the time settings and configure the global SNTP settings

Before you configure SNTP for the time settings, add at least one SNTP server (see Add an SNTP server on page 58) that the switch can contact for time keeping.

To configure SNTP for the time settings and configure the global SNTP settings:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

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

   The Time Configuration page displays.

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

   The default setting is Local.

7. In the **Time Zone Name** field, type the name or acronym of the time zone.

   In the **Offset Hours** and **Offset Minutes** fields, you can also specify the number of hours and number of minutes that the time zone differs from the Coordinated Universal Time (UTC). The time zone can affect the display of the current system time, for which the default is UTC.

   - **Offset Hours**: Set the number of hours that the time zone differs from the UTC.

     The range is from –12 to 13 hours. The default is 0 hours

   - **Offset Minutes**: Set the number of minutes that the time zone differs from the UTC.

     The range is from 0 to 59 minutes. The default is 0 minutes.

   The following steps refer to the SNTP Global Configuration section.

8. Select a Client Mode radio button to set the operation mode of the SNTP client on the switch:

   - **Unicast**: SNTP operates in a point-to-point mode. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the round-trip delay and local clock offset

relative to the server. For information about adding an SNTP server, see Add an SNTP server on page 58.

- **Broadcast**: SNTP operates uses a local broadcast address instead of a multicast address. The broadcast address has a single subnet scope while a multicast address has an Internet wide scope. Broadcast is the default setting.

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

   The port number is 123 or in a range from 1025 to 65535. The default is 123. When the default value is configured, the actual client port value used in SNTP packets is assigned by the operating system.

10. In the **Unicast Poll Interval** field, type the number of seconds between unicast poll requests expressed as a power of 2.

    The range is from 6 to 10. The default is 6.

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

    Broadcast messages received prior to the expiration of this interval are discarded. The range is from 6 to 10. The default is 6.

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

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

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

    The range is from 0 to 10. The default is 1.

14. Click the **Apply** button.

    Your settings are saved.

Display the global SNTP status

You can display the global SNTP status on the switch

To display the global SNTP 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

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

   The Time Configuration page displays.
6. Select the Clock Source **SNTP** radio button.

   The default setting is Local.
7. Scroll down to the SNTP Global Status section.
8. To refresh the page, click the **Refresh** button.

The SNTP Global Status section displays the following view-only fields.

Table 10. SNTP global status information

Field	Description
Version	The SNTP version that the client on the switch supports (version 4)
Supported Mode	The SNTP modes that the client on the switch supports (Unicast and Broadcast)
Last Update Time	The local date and time (UTC) that the response from the SNTP server was used to update the system clock
Last Attempt Time	The local date and time (UTC) that the SNTP server was last queried
Last Attempt Status	The status of the last SNTP request to the SNTP server: • **Success**: The SNTP operation was successful and the system time was updated. • **Request Timed Out**: A directed SNTP request timed out without receiving a response from the SNTP server. • **Bad Date Encoded**: The time provided by the SNTP server is not valid. • **Version Not Supported**: The SNTP version supported by the server is not compatible with the version supported by the client. • **Server Unsynchronized**: The SNTP server is not synchronized with its peers. This is indicated in the leap indicator field in the SNTP message. • **Other**: None of the previous status option applies.
Server IP Address	The IP address of the SNTP server for the last received valid packet
Address Type	The address type of the SNTP server address for the last received valid packet

Table 10. SNTP global status information (Continued)

Field	Description
Server Stratum	The claimed stratum of the server for the last received valid packet
Reference Clock ID	The reference clock identifier of the server for the last received valid packet
Server Mode	The mode of the server for the last received valid packet
Unicast Server Max Entries	The maximum number of unicast server entries that can be configured on the client on the switch
Unicast Server Current Entries	The number of current valid unicast server entries that are configured for the client on the switch
Broadcast Count	The number of received valid broadcast packets

SNTP servers

SNTP assures accurate time synchronization for network device clocks, up to the millisecond. Time synchronization is performed by a network SNTP server. The switch operates as an SNTP client only and does not provide time services to other devices.

Time sources are established by stratums. Stratums define the accuracy of the reference clock. The higher the stratum (zero is the highest), the more accurate the clock. The switch receives time from stratum 1 or stratum 0 devices because the switch itself is a stratum 2 device.

The following are examples of stratums:

- **Stratum 0**: A real-time clock is used as the time source, for example, a GPS system.
- **Stratum 1**: A server that is directly linked to a stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.
- **Stratum 2**: The time source is distanced from the stratum 1 server over a network path. For example, a stratum 2 server receives the time over a network link, 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 switch can poll unicast server types for the server time. The switch polls for unicast information to detect a server for which the IP address is known. SNTP servers that you configure on the switch are the only ones that are polled for synchronization information. T1 through T4 are used to determine the 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 that are configured on the switch.

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

Add an SNTP server

The switch can support three SNTP servers, and might be preconfigured with SNTP servers. If three SNTP server are preconfigured, you must delete a preconfigured server before you can add a custom 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The SNTP Server Configuration page displays.
6. Click the **Add New** button.

   The Add SNTP Server Configuration pop-up window displays.
7. From the **Server Type** menu, select the type of SNTP address to enter in the Address field.

   The address can be an IPv4 address, IPv6 address, or host name (DNS).
8. In the **Address** field, type the IP address or the host name of the SNTP server.

The entry can be either an IP address or a text string of up to 64 characters, containing the encoded IP address or host name of an SNTP server. Unicast SNTP requests are sent to this address. If the address is a DNS host name, the host name is resolved into an IP address each time an SNTP request is sent to it.

9. In the **Port** field, type the port number.

   This is the UDP port on the SNTP server to which SNTP requests are sent. The range is from 1 to 65535. The default is 123.

10. In the **Priority** field, type the priority order in which the switch must query the servers.

    The SNTP client on the switch continues to send SNTP requests to different servers until a successful response is received, or all servers were tried. The priority indicates the order in which the switch must query the servers. The switch first sends a request to an SNTP server with a priority of 1, then to a server with a priority of 2, and so on. If any servers are assigned the same priority, the SNTP client contacts the servers in the order that they are listed in the table. The priority range is from 1 to 3. By default, the first server that you add gets priority 1, the second server priority 2, and the third server priority 3.

11. In the **Version** field, type the NTP version that is supported by the switch.

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

12. Click the **Save** button.

    Your settings are saved and the SNTP server is added.

Change the settings for an SNTP server

You can change the settings for an existing SNTP server.

To change the settings for 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

The Dashboard page displays.

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

   The SNTP Server Configuration page displays.
6. Select the check box for the SNTP server.
7. Click the **Edit** button.

   The Edit SNTP Server Configuration pop-up window displays.
8. Change the settings as needed.

   For more information, see Add an SNTP server on page 58.
9. Click the **Save** button.

   Your settings are saved.

Remove an SNTP server

You can remove an SNTP server that you no longer need in your network.

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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

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

   Your settings are saved and the SNTP server is removed.

Display the status of the SNTP servers

You can display the status of the SNTP servers that are configured on the switch.

To display the status of the SNTP servers:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The SNTP Server Configuration page displays.
6. To refresh the page, click the **Refresh** button.

The SNTP Server Status table displays the following view-only fields.

Table 11. SNTP server status information

Field	Description
Address	The IP address of the SNTP server
Last Update Time	The local date and time (UTC) that the response from the server was used to update the system clock
Last Attempt Time	The local date and time (UTC) that the SNTP server was last queried

Table 11. SNTP server status information (Continued)

Field	Description
Last Attempt Status	The status of the last NTP request to the server: • **Other**: No packet was received from the server. • **Success**: The SNTP operation was successful and the system time was updated. • **Request Timed Out**: A directed SNTP request timed out without receiving a response from the SNTP server. • **Bad Date Encoded**: The time provided by the SNTP server is not valid. • **Version Not Supported**: The SNTP version supported by the server is not compatible with the version supported by the client. • **Server Unsynchronized**: The SNTP server is not synchronized with its peers. This is indicated through the leap indicator field on the SNTP message. • **Server Kiss Of Death**: The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.
Requests	The number of SNTP requests made to the server since the last reboot
Failed Requests	The number of failed SNTP requests made to the server since the last reboot

Configure daylight saving time settings

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

To configure the daylight saving time settings:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.

4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Management > Time > Daylight Saving Configuration**.

   The Daylight Saving Configuration page displays.
6. Select one of the following Daylight Saving (DST) radio buttons:

   - **Disable**: Disables daylight saving time. This is the default setting.
   - **Recurring**: Daylight saving time occurs at the same time every year. You must manually configure the start and end times and dates for the time shift.

     Configure the settings that are described in Step 7.
   - **Recurring EU**: The system clock uses the standard recurring summer time settings used in countries in the European Union. With this option, the rest of the applicable fields on the page are automatically populated and you cannot change them.

     Configure the settings that are described in Step 8.
   - **Recurring USA**: The system clock uses the standard recurring daylight saving time settings used in the United States. With this option, the rest of the applicable fields on the page are automatically populated and you cannot change them.

     Configure the settings that are described in Step 8.
   - **Nonrecurring**: Daylight saving time settings are in effect only between the start date and end date of the specified year. With this option, the summer time settings do not repeat on an annual basis.

     Configure the settings that are described in Step 9.
7. If you select the **Recurring** radio button, configure the fields that are shown in the following table.

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

8. If you select the **Recurring EU** or **Recurring USA** radio button, configure the fields that are shown in the following table.

Field	Description
Offset	Configure recurring offset in minutes. The range is from 1 to 1440 minutes.
Zone	Configure the time zone.

9. If you select the **Nonrecurring** radio button, configure the fields that are shown in the following table.

Field	Description
Begins At	These fields are used to configure the start values of the date and time. • **Month**: Configure the start month. • **Date**: Configure the start date. • **Year**: Configure the start year. • **Hours**: Configure the start hours. • **Minutes**: Configure the start minutes.
Ends At	These fields are used to configure the end values of date and time. • **Month**: Configure the end start date. • **Date**: Configure the end date. • **Year**: Configure the end year. • **Hours**: Configure the end hours. • **Minutes**: Configure the end minutes.
Offset	Configure the non-recurring offset in minutes. The range is from 1 to 11440 minutes.
Zone	Configure the time zone.

10. Click the **Apply** button.

    Your settings are saved.

Display the daylight saving time status

You can display information about the daylight saving time settings and whether the time shift is currently in effect.

To view the daylight saving time status:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.

4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Management > Time > Daylight Saving Configuration**.

   The Daylight Saving Configuration page displays.
6. To refresh the page, click the **Refresh** button.

The following table displays the view-only daylight saving (DST) status information.

Table 12. Daylight saving status information

Field	Description
Daylight Saving (DST) Status	The configured daylight saving mode: Disable, Recurring, Recurring EU, Recurring USA, or Nonrecurring
Begins At	The date and time when daylight saving time begins
Ends At	The date and time when daylight saving time ends
Offset (in Minutes)	The offset time in minutes
Zone	The zone acronym. The zone is not displayed when daylight saving time is disabled.
Daylight Saving (DST) in Effect	Displays whether daylight saving time is in effect

Domain Name System

You can configure information about Domain Name System (DNS) servers that the network uses and how the switch operates as a DNS client.

Configure the global DNS settings and add a DNS server

You can configure the global DNS settings and add up to eight DNS servers.

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

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

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

   The DNS Configuration page displays.
6. Click the **DNS Status** toggle to enable the switch to reach a DNS server:
   - **The toggle is gray and positioned to the left**: DNS is disabled and the switch cannot reach a DNS server.
   - **The toggle is purple and positioned to the right**: DNS is enabled and the switch can reach a DNS server. This is the default setting.
7. In the **DNS Default Name** field, enter the name that must be included in DNS queries.

   When the switch looks up on an unqualified host name, this field provides the domain name. For example, if the default domain name is netgear.com and you enter *test*, then test is changed to test.netgear.com to resolve the name). The maximum length of the name is 255 characters.
8. Click the **Apply** button.

   Your settings are saved.
9. To add a DNS server to which the switch sends DNS queries, do the following in the DNS Server Configuration section:

   a. Click the **Add New** button.

      The Add DNS Server Configuration pop-up window displays.

   b. In the **DNS Server** field, type an IPv4 or IPv6 address.

   c. Click the **Save** button.

      Your settings are saved and the DNS server is added

      The server is added to the table. You can specify up to eight DNS servers. The precedence is set in the order that you add the servers.

The following table displays the view-only DNS server information.

Table 13. DNS server configuration information

Field	Description
ID	The sequence number of the DNS server.
Preference	The preference of the DNS server. The preference is determined by the order in which you add the servers.

Remove a DNS server

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

To remove a DNS server:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The DNS Configuration page displays.
6. In the DNS Server Configuration table, select the check box for the DNS server.
7. Click the **Delete** button.

   Your settings are saved and the DNS server is removed.

Map host names to DNS server IP addresses and display dynamic host mappings

You can manually map host names to DNS server IP addresses and view dynamic host mappings.

Add an entry to the static DNS host mapping table

You can add an entry to the static DNS host mapping table.

To add an entry to the static DNS 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The Host Configuration page displays.
6. Click the **Add New** button.

   The Add DNS Host Configuration pop-up window displays.
7. In the **Host Name** field, type the static host name.

   The maximum length of the name is 255 characters.
8. In the **IPv4/IPv6 Address** field, enter the IPv4 or IPv6 address that is associated with the host name.
9. Click the **Save** button.

   Your settings are saved and the entry is added to the DNS Host Configuration table.

Change an entry in the static DNS host mapping table

You can change the IP address for an existing entry in the static DNS host mapping table.

To change the IP address for an entry in the static DNS 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The Host Configuration page displays.
6. Select the check box for the entry.
7. Click the **Edit** button.

   The Edit Host Configuration pop-up window displays
8. Change the IPv4 or IPv6 address.
9. Click the **Save** button.

   Your settings are saved.

Remove an entry from the static DNS host mapping table

If you no longer need an entry in the static DNS host mapping table, you remove the entry from the table.

To remove an entry from the static DNS 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

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

   The Host Configuration page displays.

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

   Your settings are saved and the entry is removed.

Display or clear the dynamic DNS host mapping entries

You can display or clear the dynamic DNS host mapping entries.

To display or clear the dynamic DNS host mapping 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

The Dashboard page displays.

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

   The Host Configuration page displays.

6. To clear all entries in the Dynamic Host Mapping table, click the **Clear** button.

The dynamic host mapping table shows DNS host name-to-IP address entries that the switch learned. The following table describes the dynamic host fields.

Table 14. Dynamic host mapping information

Field	Description
Host	The host name that the switch learned
Total	The time since the dynamic entry was first added
Elapsed	The time since the dynamic entry was last updated
Type	The type of the dynamic entry (IPv4 or IPv6)
IPv4/IPv6 Address	The IP address that the switch learned and this is associated with the host name

Manage switch discovery protocols

By default, Universal Plug and Play (UPnP) is enabled on the switch. UPnP allows the switch to be discovered in your network. For greater security, you can disable UPnP.

To manage switch discovery protocols:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **System > Management > Switch Discovery**.

   The Switch Discovery page displays.
6. In the UPnP Configuration section, click the **Allow Discovery** toggle to enable or disable UPnP:
   - **The toggle is gray and positioned to the left**: UPnP is disabled.
   - **The toggle is purple and positioned to the right**: UPnP is enabled. This is the default setting.

     Note: You must enable the UPnP toggle to discover the switch using the NETGEAR Discovery Tool or the Windows File Explorer network scan.
7. Click **Apply**.

Display USB device information

To display 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Management > USB Device Information**.

   The USB Device Information page displays.

   The Device Status field displays the current status of the device. The status is one of the following:

- **Active**: The device is USB plugged in and recognized by the switch.
- **Inactive**: The device is not mounted.
- **Invalid**: The device is not present or an invalid device is plugged in.

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

   The following table describes the information in the USB Memory Statistics section.

   Table 15. USB Memory Statistics information

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

   The following table describes the information in the USB Directory Details section.

   Table 16. USB Directory Details information

Field	Description
File Name	The name of the file stored in the USB flash drive
File Size	The size of the file stored in the USB flash drive in bytes
Modification Time	The last modification time of the file stored in the USB flash drive

LLDP and LLDP-MED settings for the switch

This section describes the global Link Layer Discovery Protocol (LLDP) and LLDP-Media Endpoint Discovery (LLDP-MED) settings for the switch. For information about the LLDP and LLDP-MED settings for interfaces, see LLDP and LLDP-MED settings for interfaces on page 164.

LLDP, which is defined in IEEE 802.1AB, lets devices on a LAN advertise major capabilities and physical descriptions. You can view this information to identify the system topology and detect problematic configurations in the LAN.

LLDP is a one-way protocol without request and response sequences. Information is advertised by devices that are configured to transmit LLDP and is received and processed by devices that are configured to receive LLDP.
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 you to track your network devices and determine their characteristics (manufacturer, software and hardware versions, and serial or asset number).

Configure the LLDP and LLDP-MED settings

You can configure the LLDP and LDDP-MED settings that are globally applied to the switch.

To configure the LLDP and LDDP-MED 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > LLDP > LLDP Configuration**.

   The LLDP Configuration page displays.
6. In the **TLV Advertised Interval** field, enter the interval in seconds at which the switch transmits LLDP frames.

   The range is from 5 to 32768 secs. The default is 30 seconds.
7. In the **Hold Multiplier** field, enter the multiplier for the value that you enter in the **TLV Advertised Interval** field, which determines the time-to-live (TTL) for LLDP notifications.

   The range is from 2 to 10 secs. The default value is 4.

As an example, if the value that you enter in the **TLV Advertised Interval** field is 30 and the value that you enter in the **Hold Multiplier** field is 4, the TTL for LLDP notifications is 120 seconds.

8. In the **Reinitializing Delay** field, enter the delay before reinitialization starts.

   The range is from 1 to 10 secs. The default is 2 seconds.

9. In the **Transmit Delay** field, enter the interval in seconds at which notifications are transmitted.

   The range is from 5 to 3600 secs. The default is 5 seconds.

10. In the **Fast Start Duration** field of the LLDP-MED Configuration section, enter the number of LLDP packets that are transmitted per second when LLDP-MED Fast Start is initialized.

    Fast Start is initialized when a new endpoint device links with the switch. The range is from 1 to 10 packets per second. Default is 3 packets per second.

11. Click the **Apply** button.

    Your settings are saved.

Display the LLDP-MED network policy for an interface

You can display the LLDP-MED policy information for an interface.

For information about configuring LLDP and LLDP-MED for interfaces, see LLDP and LLDP-MED settings for interfaces on page 164.

To display the LLDP-MED 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

The Dashboard page displays.

5. Select **System > LLDP > LLDP-MED Network Policy**.
   The LLDP-MED Network Policy page displays.
6. From the **Interface** menu, select the interface.
   The page adjusts.
7. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 17. LLDP-MED network policy information

Field	Description
Network Policy Number	The network policy number, if any is transmitted
Application	The application type that is transmitted. The type can be one of the following: • unknown • voice signaling • guest voice • guest voice signaling • soft phone voice • videoconferencing • streaming video • video signaling Each application type that is transmitted includes the VLAN ID, VLAN type, user priority, and DSCP.
VLAN ID	The VLAN ID that is transmitted
VLAN Type	The VLAN type that is transmitted (tagged or untagged)
User Priority	The user priority that is transmitted
DSCP	The DSCP that is transmitted

Display the LLDP local device information

You can display LLDP local device information, which is information that the switch itself, or an interface of the switch, advertises.

For information about configuring LLDP and LLDP-MED for interfaces, see LLDP and LLDP-MED settings for interfaces on page 164.

To display LLDP local 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

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

   The Local Information page displays.

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

The following table describes the view-only fields on the page.

Table 18. LLDP local device information

Field	Description
Device Information	
Chassis ID Subtype	The switch identifier is the MAC address of the switch (see the following field)
Chassis ID	The MAC address of the switch
System Name	The system name, if any, of the switch
System Description	The description of the switch
System Capabilities	The capabilities of the switch, which is *bridge* by default
Port Information	
Interface	The number of the physical interface
Port ID Subtype	The port ID subtype is always *Local*
Port ID	The port ID is identical to the number of the interface
Port Description	The configured description of the port, if any
Advertisement	Indicates if LLDP information is being advertised by the port (Enable or Disable)

Display the LLDP neighbor information

LLDP neighbor information is the information that LLDP detects in the network. A neighbor is also referred to as a remote device.

To display the LLDP neighbor information:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The Neighbors Information page displays.
6. To refresh the page, click the **Refresh** button.

   The following table describes the view-only fields on the page.

   Table 19. LLDP neighbor information

Field	Description
MSAP Entry	The detected Media Service Access Point (MSAP) entry of the neighbor
Local Port	The number of the physical interface on the switch that receives the information
Chassis ID Subtype	The chassis ID subtype of the neighbor, for example, MAC address
Chassis ID	The chassis ID of the neighbor, for example, the MAC address of the device
Port ID Subtype	The type of the port identifier on the neighbor (Local or MAC address)

Table 19. LLDP neighbor information (Continued)

Field	Description
Port ID	The number of the Ethernet adapter or the MAC address of the port on the neighbor
System Name	The system name, if any, of the neighbor

7. To display detailed information for an MSAP entry, click the entry, which is a link.
   The Neighbor Information pop-up window displays.

The following table describes the view-only fields in the pop-up window.

Table 20. Detailed LLDP neighbor information

Field	Description
Port Details	
Local Port	The local switch port that detects the neighbor information that is displayed
MSAP Entry	The number of the MSAP entry for which information is displayed
Basic Details	
Chassis ID Subtype	The chassis ID subtype of the neighbor, for example, MAC address
Chassis ID	The chassis ID of the neighbor, for example, the MAC address of the device
Port ID Subtype	The type of the port identifier on the neighbor (Local or MAC address)
Port ID	The number of the Ethernet adapter or the MAC address of the port on the neighbor
Port Description	The LLDP description of the port on the neighbor. This information can include manufacturer, product name, hardware version, and software version.
System Name	The system name, if any, of the neighbor.
System Description	The LLDP description of the neighbor. This information can include the system hardware type and version, operating system, and network software.
System Capabilities	The system capabilities that are supported on the neighbor and its primary function. For example, "Bridge, WLAN access point."
Managed Address	
Address SubType	The managed address subtype of the neighbor. For example, MAC or IPv4.
Address	The managed address of the neighbor
Interface SubType	The port subtype (for the managed address) of the neighbor

Table 20. Detailed LLDP neighbor information (Continued)

Field	Description
Interface Number	The port number (for the managed address) of the neighbor
MAC/PHY Details	
Autonegotiation Supported	Displays if the neighbor supports autonegotiation (True or False)
Autonegotiation Enabled	Displays if autonegotiation is enabled on the neighbor (True or False)
Autonegotiation Advertised Capabilities	The autonegotiation capabilities. For example, 1000BASE-T half duplex mode, 100BASE-TX full duplex mode.
Operational MAU Type	The Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interface collision detection and bit injection into the network. For example, 100BASE-TX full duplex mode.
MED Details	
Capabilities Supported	The system capabilities that are supported on the neighbor
Current Capabilities	The system capabilities that are enabled on the neighbor
Device Class	The device class that is advertised by the neighbor. The device class can be Generic, Media, Communication, or Network Connectivity.
PoE Device Type	The type of PoE device that the neighbor is. For example, Powered.
PoE Power Source	The type of power source of the neighbor
PoE Power Priority	The power priority on the neighbor
PoE Power Value	The power in watts that the neighbor advertises that it can transmit
Hardware Revision	The hardware version of the neighbor
Firmware Revision	The firmware version of the neighbor
Software Revision	The software version of the neighbor
Serial Number	The serial number of the neighbor
Model Name	The model name of the neighbor
Asset ID	The asset ID of the neighbor
Location Information	
Civic	The neighbor's civic or street address location. For example, 123 45th St E.
Coordinates	The neighbor's location map coordinates (latitude, longitude, and altitude)

Table 20. Detailed LLDP neighbor information (Continued)

Field	Description
ECS ELIN	The neighbor's Emergency Call Service (ECS) Emergency Location Identification Number (ELIN)
Unknown	The neighbor's unknown location information.
Network Policies	
Application Type	The application type of the neighbor, which can be one of the following: • unknown • voice signaling • guest voice • guest voice signaling • soft phone voice • videoconferencing • streaming video • video signaling Each application type that is received includes the VLAN ID, VLAN type, user priority, and DSCP value. An interface can receive one or many such application types. This information is displayed only if a network policy TLV is received.
VLAN ID	The VLAN ID of the neighbor
VLAN Type	The type of VLAN of the neighbor
User Priority	The user priority of the neighbor
DSCP	The DSCP value of the neighbor
LLDP Unknown TLVs	
Type	The unknown TLV type of the neighbor
Value	The unknown TLV value of the neighbor

Simple Network Management Protocol

You can configure SNMP settings for SNMPv1, SNMPv2, 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.

Manage SNMPv1 and SNMPv2 communities

By default, no SNMP communities exist. The communities that you define can access the switch using SNMPv1 and SNMPv2. Only those communities with read/write level access can be used to change the configuration using SNMP.

Add an SNMPv1 and SNMPv2 community

You can add an SNMPv1 and SNMPv2 community, which grants both SNMPv1 and SNMPv2 access.

To add an SNMPv1 and SNMPv2 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > SNMP > Community Configuration**.

   The Community Configuration page displays.
6. Click the **Add New** button.

   The Add Community Configuration pop-up window displays.
7. In the **Management Station IP** field, type the IP address of the SNMP management station, also referred to as the SNMP client.
8. In the **Management Station IP Mask** field, type the IP subnet mask of the SNMP management station.

The client IP address and client IP mask together denote a range of IP addresses from which SNMP clients can use the community to access the switch.

If either the client IP address or client IP mask is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's IP address is *ANDed* with the mask, as is the client IP address. If the values are equal, access is allowed.

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

9. In the **Community String** field, type the name for the community.

   The name can be up to 16 characters.

10. From the **Access Mode** menu, select the access level for the community, which is either **Read/Write** or **Read Only**.
    - **ReadOnly**: The community can only ready information.
    - **ReadWrite**: The community can both read and write (save) information.
11. From the **Status** menu, select to enable or disable the community:
    - **Disabled**: The community is disabled. You can configure a community and temporarily disable it.
    - **Enabled**: The community is enabled.
12. Click the **Save** button.

    Your settings are saved and the community is added.

Change an existing SNMPv1 and SNMPv2 community

You can change an existing SNMPv1 and SNMPv2 community.

To change an existing SNMPv1 and SNMPv2 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > SNMP > Community Configuration**.

   The Community Configuration page displays.
6. Select the check box for the community.
7. Click the **Edit** button.

   The Edit Community Configuration pop-up window displays.
8. Change the settings as needed.

   For more information about the settings, see Add an SNMPv1 and SNMPv2 community on page 83.
9. Click the **Save** button.

   Your settings are saved.

Delete an SNMPv1 and SNMPv2 community

You can delete an SNMPv1 and SNMPv2 community that you no longer need.

To delete an SNMPv1 and SNMPv2 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > SNMP > Community Configuration**.

   The Community Configuration page displays.

6. Select the check box for the community.
7. Click the **Delete** button.

   Your settings are saved and the community is deleted.

Manage the SNMPv1 and SNMPv2 trap settings

For each SNMP community, you can specify the source interface that must be used on the switch, the community name, the associated IP address, and other settings.

Add an SNMPv1 or SNMPv2 trap configuration for a host

You can add a trap configuration for a host, enabling the host to receive SNMPv1 or SNMPv2 traps.

To add an SNMPv1 or SNMPv2 trap configuration for a 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > SNMP > Trap Configuration**.

   The Trap Configuration page displays.
6. Click the **Add New** button.

   The Add Trap Configuration pop-up window displays.
7. In the **Recipients IP** field, enter the IP address of the device (that is, the host) that must receive the traps.

8. From the **Version** menu, select the SNMP version that is used by the host:
   - **SNMPv1**: The switch uses SNMPv1 to send traps to the receiver. This the default setting.
   - **SNMPv2**: The switch uses SNMPv2 to send traps to the receiver.
9. In the **Community String** field, type the name of the SNMP community that includes the host.

   For information about communities, see Add an SNMPv1 and SNMPv2 community on page 83.
10. From the **Status** menu, select to enable or disable the trap configuration:
    - **Disabled**: The trap configuration is disabled. You can add a trap configuration and temporarily disable it.
    - **Enabled**: The trap configuration is enabled.
11. Click the **Save** button.

    Your settings are saved and the trap configuration is added.

Change an SNMPv1 or SNMPv2 trap configuration for a host

You can change an existing SNMPv1 or SNMPv2 trap configuration for a host.

To change an SNMPv1 or and SNMPv2 trap configuration for a 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > SNMP > Trap Configuration**.

   The Trap Configuration page displays.

6. Select the check box for the trap configuration.
7. Click the **Edit** button.

   The Edit Trap Configuration pop-up window displays.
8. Change the settings as needed.

   For more information about the settings, see Add an SNMPv1 or SNMPv2 trap configuration for a host on page 86.
9. Click the **Save** button.

   Your settings are saved.

Delete an SNMPv1 or SNMPv2 trap configuration for a host

You can delete an SNMPv1 or SNMPv2 trap configuration that you no longer need for a host.

To delete an SNMPv1 or SNMPv2 trap configuration for a 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > SNMP > Trap Configuration**.

   The Trap Configuration page displays.
6. Select the check box for the trap configuration.
7. Click the **Delete** button.

   Your settings are saved and the trap configuration is deleted.

Configure SNMPv1 and SNMPv2 trap flags

You can enable or disable specific traps. When the condition that is identified by an active trap occurs on the switch, a trap message is sent to any enabled SNMP trap receivers (also referred to as hosts), 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > SNMP > Trap Flags**.

   The Trap Flags page displays.

   By default, all of the following trap flags are enabled, and their associated toggles are purple and positioned to the right:

   - **Authentication**: When enabled, SNMP traps are sent when events involving authentication occur, such as when a user attempts to access the device UI but does not provide a valid user name and password.
   - **Link Up/Down**: When enabled, SNMP traps are sent when the administrative or operational state of a physical or logical interface link changes.
   - **Spanning Tree**: When enabled, SNMP traps are sent when various spanning tree events occur.
   - **PoE**: When enabled, SNMP traps are sent when various PoE events occur.
   - **Fan Failure**: When enabled, SNMP traps are sent when a fan fails.
6. To disable a trap flag, click the associated toggle.

   The toggle is gray and positioned to the left.
7. Click the **Apply** button.

Your settings are saved.

Display the supported MIBs

To display the MIBs that are supported by 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > SNMP > Supported MIBs**.

   The Supported MIBs page displays.

   The Name field displays the RFC number, if applicable, and the name of the MIB.

   The Description field displays the RFC title or MIB description.

   Note: A Request for Comments (RFC) is a document from the Internet Engineering Task Force (IETF).

Configure the SNMPv3 user account

Any user can connect to the switch using the SNMPv3 protocol, but for authentication and encryption, the switch supports only one user, which is the admin user. Therefore, you can configure only one SNMPv3 profile.

To configure authentication and encryption settings for the SNMPv3 admin 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **System > Protocols > SNMP > SNMP V3**.

   The SNMP V3 page displays.

   The SNMPv3 access privileges for the admin account are Read Write. You cannot change this access privilege.

6. If you need to disable SNMPv3 access, from the **SNMP V3 Access Mode** menu, select **Disable**.

   By default, SNMPv3 access is enabled.

7. To change authentication, select an Authentication Protocol radio button:
   - **MD5**: Message Digest 5 (MD5) is the authentication protocol.
   - **SHA**: Secure Hash Algorithm (SHA) is the authentication protocol. SHA provides stronger security than MD5.
   - **SHA-256**: A secure hash algorithm that is compatible with many devices. SHA-256 provides stronger security than SHA.
   - **SHA-512**: A secure hash algorithm that is superior to SHA-256. This is the default type.

   With any selection of authentication protocol, the admin login password for the device UI is used as the SNMPv3 authentication password.

8. To enable encryption, do the following:
   a. Select an Encryption Protocol button:
      - **DES**: SNMPv3 are encrypted using the DES encryption protocol.
      - **AES-256**: SNMPv3 packets are encrypted using the AES-256 protocol, which provides stronger security than DES.

By default, encryption is not enabled, and the None button is selected.

b. In the **Encryption Key** field, enter an encryption code of eight or more alphanumeric characters.

9. Click the **Apply** button.

   Your settings are saved.

Configure HTTPS access settings

Secure HTTP (HTTPS) enables the transmission of HTTP over an encrypted Secure Sockets Layer (SSL) connection. When you manage the switch over the device UI, HTTPS can help ensure that communication between the management system and the switch is protected from eavesdroppers and man-in-the-middle attacks.

To configure HTTPS access settings:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **System > Protocols > HTTPS**.

   The HTTPS page displays.

6. Click the **Allow HTTPS** toggle to enable or disable HTTPS access:
   - **The toggle is gray and positioned to the left**: You cannot access the switch device UI from an HTTPS session over a web browser.
   - **The toggle is purple and positioned to the right**: You can access the switch device UI from an HTTPS session over a web browser. This is the default setting.
7. In the **HTTPS Port** field, type the HTTPS port number.

The range is from 1025 to 65535. The default port number is 443.

8. In the **HTTPS Session Soft Timeout** field, type the number of minutes an HTTPS session can be idle before a time-out occurs.

   The range is from 0 to 60 minutes. The default is 5 minutes.

9. In the **HTTPS Session Hard Timeout** field, type the hard time-out for HTTPS sessions.

   This time-out is unaffected by the activity level of the session. The range is from 0 to 168 hours. The default is 24 hours.

10. In the **Maximum Number of HTTPS Sessions** field, type the maximum number of HTTPS sessions that are allowed simultaneously.

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

11. Click the **Apply** button.

    Your settings are saved.

HTTPS management access

You can configure secure HTTP (HTTPS) access to the device UI.

Configure HTTPS access settings

Secure HTTP (HTTPS) enables the transmission of HTTP over an encrypted Secure Sockets Layer (SSL) connection. When you manage the switch over the device UI, HTTPS can help ensure that communication between the management system and the switch is protected from eavesdroppers and man-in-the-middle attacks.

To configure HTTPS access settings:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > HTTPS**.

   The HTTPS page displays.
6. Click the **Allow HTTPS** toggle to enable or disable HTTPS access:
   - **The toggle is gray and positioned to the left**: You cannot access the switch device UI from an HTTPS session over a web browser. This is the default setting.
   - **The toggle is purple and positioned to the right**: You can access the switch device UI from an HTTPS session over a web browser.
7. In the **HTTPS Port** field, type the HTTPS port number.

   The range is from 1025 to 65535. The default port number is 443.
8. In the **HTTPS Session Soft Timeout** field, type the number of minutes an HTTPS session can be idle before a time-out occurs.

   The range is from 0 to 60 minutes. The default is 5 minutes.
9. In the **HTTPS Session Hard Timeout** field, type the hard time-out for HTTPS sessions.

   This time-out is unaffected by the activity level of the session. The range is from 0 to 168 hours. The default is 24 hours.
10. In the **Maximum Number of HTTPS Sessions** field, type the maximum number of HTTPS sessions that are allowed simultaneously.

    The range is from 1 to 4. The default is 4.
11. Click the **Apply** button.

    Your settings are saved.

Manage the SSL certificate for HTTPS access

For the switch to accept HTTPS connections from a device, the switch requires a public key certificate. The switch is preconfigured with a self-signed SSL certificate for HTTPS access. The switch supports a single certificate.

You can generate a new certificate on the switch. You can also generate a certificate externally (for example, offline) or obtain a certificate authority (CA)-signed certificate and transfer it to the switch.

Generate an SSL certificate

The switch is preconfigured with a self-signed SSL certificate. You can let the switch generate a new certificate, for example, in the unlikely situation that the key of the existing certificate is compromised. The new certificate replaces the existing certificate.

Note: Before you can generate a certificate, you must disable HTTPS (see Configure HTTPS access settings on page 93) and log back in to the device UI over an HTTP session. After you generate the certificate, you can reenable HTTPS and log back in to the device UI over an HTTPS session.

To let the switch generate an SSL certificate:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > HTTPS**.

   The HTTPS page displays.
6. In the Certificate Management section, select the **Generate Certificates** radio button.
7. Click the **Apply** button.

   The switch generates an SSL certificate.

   The Certificate Generation Status field shows if certificate generation is in process.

   The Certificate Present field shows Yes, indicating that the certificate is present.

Transfer an SSL certificate from a TFTP server to the switch

You can transfer an SSL certificate file from a TFTP server to the switch. The transferred certificate replaces the existing certificate on the switch.

Note: For information about downloading and installing an SSL certificate over an HTTP session, see Download and install an SSL security certificate file on the switch on page 444.

Before you transfer a file from a server to the switch, be sure that the following conditions are true:

- The file that you transfer from a server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch contains a path to the server.

Note: Before you can transfer a certificate, you must disable HTTPS (see Configure HTTPS access settings on page 93) and log back in to the device UI over an HTTP session. After you transfer the certificate, you can reenable HTTPS and log back in to the device UI over an HTTPS session.

To transfer an SSL certificate 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > HTTPS**.

   The HTTPS page displays.

   The following steps refer to the Certificate Upload section.
6. From the **File Type** menu, select the type of SSL certificate to download:

   - **SSL Trusted Root Certificate PEM File**: SSL Trusted Root Certificate file (PEM Encoded)
   - **SSL Server Certificate PEM File**: SSL Server Certificate File (PEM Encoded)

- **SSL DH Weak Encryption Parameter PEM File**: SSL Diffie-Hellman Weak Encryption Parameter file (PEM Encoded)
- **SSL DH Strong Encryption Parameter PEM File**: SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded)

7. Click the **Browse** button to upload the file you want to update. The factory default is blank.
8. Click the **Start File Transfer** toggle to enable the file transfer.
   - **The toggle is gray and positioned to the left**: The file transfer is disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: The file transfer is enabled. The file transfer starts after you click the **Apply** button.

   A status message displays during the transfer and upon successful completion of the transfer.
9. Click the **Apply** button.

   The certificate is downloaded from the server to the switch. After the file transfer starts, wait until the page refreshes. The page displays information about the progress of the file transfer.

Delete the SSL certificate

Note: Before you can delete the SSL certificate, you must disable HTTPS (see Configure HTTPS access settings on page 93) and log back in to the device UI over an HTTP session. After you delete the certificate, you can reenable HTTPS and log back in to the device UI over an HTTPS session.

To delete the SSL certificate:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.

4. Click the **Login** button.
   The Dashboard page displays.
5. Select **System > Protocols > HTTPS**.
   The HTTPS page displays.
6. In the Certificate Management section, select **Delete Certificates** radio button.
7. Click the **Apply** button.
   The certificate is removed.

Browser security message with HTTPS access

After you enable HTTPS access (see Configure HTTPS access settings on page 93) and you attempt to access the device UI, your browser might display a security warning because of the self-signed certificate on the switch. This is expected behavior. You can proceed, or add an exception for the security warning.

To proceed with a security warning or add an exception for a security warning:

- **Google Chrome**: Click the **ADVANCED** link. Then, click the **Proceed to x.x.x.x (unsafe)** link, in which x.x.x.x represents the domain name or IP address of the device.
- **Apple Safari**: Click the **Show Details** button. Then, click the **visit this website** link. If a warning pop-up window displays, click the **Visit Website** button. If another pop-up window displays to let you confirm changes to your certificate trust settings, enter your Mac user name and password and click the **Update Setting** button.
- **Mozilla Firefox**: Click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that displays, click the **Confirm Security Exception** button.
- **Microsoft Edge**: Select **Details > Go on to the webpage**.
- **Microsoft Internet Explorer**: Click the **Continue to this website (not recommended)** link.

Note: For information about installing a specific security certificate on the switch, see Manage the SSL certificate for HTTPS access on page 94 and Download and install an SSL security certificate file on the switch on page 444.

SSH management access

You can display and modify the Secure Shell (SSH) server settings on the switch. SSH is a network protocol that enables access to the CLI management interface by using an SSH client on a remote administrative device. SSH is a more secure access method than

Telnet because it encrypts communication between the administrative system and the device. You can download or generate SSH host keys for secure CLI-based management.

Configure the SSH access settings

You can configure the Secure Shell (SSH) access settings. By default, the switch uses SSH version 2.

To configure the SSH access settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > SSH**.

   The SSH page displays.
6. Click the **Allow SSH** toggle to enable or disable SSH access:
   - **The toggle is gray and positioned to the left**: You cannot access the switch from an SSH session.
   - **The toggle is purple and positioned to the right**: You can access the switch from an SSH session. This is the default setting.
7. In the **SSH Port** field, type the SSH port number.

   The range is from 1025 to 65535. The default port number is 22.
8. In the **SSH Session Timeout** field, type the number of minutes an SSH session can be idle before a time-out occurs.

   The range is from 0 to 60 minutes. The default is 5 minutes. If you enter 0, the session does not time out.

9. In the **Maximum Number of SSH Sessions** field, type the maximum number of SSH sessions that are allowed simultaneously.

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

10. Click the **Apply** button.

    Your settings are saved.

Manage the RSA key for SSH access

For the switch to accept SSH connections from a device, the switch requires a Rivest-Shamir-Adelman (RSA) key. The switch is preconfigured with an RSA key for SSH access. The switch supports a single RSA key.

You can generate a new RSA key on the switch. You can also generate an RSA key externally (for example, offline) or obtain an RSA key and transfer it to the switch.

Generate an RSA key

The switch is preconfigured with an RSA key. You can let the switch generate a new RSA key, which replaces the existing key.

Note: To generate an RSA key file, SSH must be disabled (see Configure the SSH access settings on page 99).

To generate an RSA key:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **System > Protocols > SSH**.

The SSH page displays.

6. In the RSA Keys Management section, select the **Generate RSA Keys** radio button.
7. Click the **Apply** button.

   The switch generates an RSA key.

   The Key Generation In Progress field shows if key generation is in process.

   The Key Present field shows Yes, indicating that the key is present.

Transfer an RSA key from a computer to the switch

You can transfer an RSA key file from a computer to the switch. The transferred RSA key replaces the existing key on the switch.

Note: To transfer an RSA key file to the switch, SSH must be disabled (see Configure the SSH access settings on page 99).

To transfer an RSA key 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > SSH**.

   The SSH page displays.

   The following steps refer to the Host Key Update section.

   The only option from the **File Type** menu is **SSH-2 RSA Key PEM File**.
6. Click the **Browse** button and locate and select the file that you want to download to the switch.
7. Click the **Apply** button.

The file transfer starts. The Transfer Status field displays a status message during the transfer and upon successful completion of the transfer.

Delete the RSA key

Note: To delete the RSA key file, SSH must be disabled (see Configure the SSH access settings on page 99).

To delete the RSA key:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > SSH**.

   The SSH page displays.
6. In the RSA Keys Management section, select the **Delete RSA Keys** radio button.
7. Click the **Apply** button.

   The RSA key is removed.

Configure inbound Telnet settings

If you enable the inbound Telnet session capability, an authorized user can establish a Telnet session to the switch.

To configure the inbound Telnet 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > Telnet**.

   The Telnet page displays.
6. Click the **Allow Telnet** toggle to enable or disable Telnet access:
   - **The toggle is gray and positioned to the left**: You cannot access the switch from a Telnet session. This is the default setting.
   - **The toggle is purple and positioned to the right**: You can access the switch from a Telnet session
7. Click the **Apply** button.

   Your settings are saved.

DHCP snooping

DHCP snooping is a 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 correspond 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 messages only from within the network.

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

Enable DHCP snooping for the switch

You can globally enable DHCP snooping for the switch.

To globally enable DHCP snooping for 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The Global Configuration page displays.
6. Click the **DHCP Snooping Mode** toggle:
   - **The toggle is gray and positioned to the left**: The DHCP Snooping Mode is globally disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: The DHCP Snooping Mode is globally enabled.
7. Click the **MAC Address Validation** toggle:
   - **The toggle is gray and positioned to the left**: MAC address validation is disabled.
   - **The toggle is purple and positioned to the right**: MAC address validation is enabled. This is the default setting.

     When MAC address validation is enabled, the switch 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 switch drops the packet.
8. Click the **Apply** button.

   Your settings are saved.

Enable DHCP snooping for a VLAN

To enable DHCP 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The Global Configuration page displays.

   The following steps refer to the VLAN Configuration section.
6. Select the check box for the VLAN.
7. Click the **Edit** button.

   The Edit VLAN Configuration pop-up window displays.
8. From the **DHCP Snooping Mode** menu, select the DHCP snooping mode for the VLAN:
   - **Disable**: DHCP snooping is disabled for the VLAN. This is the default setting.
   - **Enable**: DHCP snooping is enabled for the VLAN.
9. Click the **Save** button.

   Your settings are saved.

Configure DHCP snooping interface settings

You can display 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The Interface Configuration page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit DHCP Snooping Interface Configuration pop-up window displays.
9. From the **Trust Mode** menu, select the trust mode:
   - **Disabled**: The interface is considered to be untrusted and could potentially be used to launch a network attack. This is the default setting.

     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 are dropped.
  - DHCP messages are dropped if the MAC address is in the snooping database but the binding's interface is different from the interface where the message was received.
  - DHCP packets are dropped if the source MAC address does not match the client hardware address and if MAC address validation is globally enabled.
- **Enabled**: The interface is considered to be trusted and forwards DHCP server messages without validation.

10. From the **Invalid Packets** menu, select the packet logging mode:
    - **Disabled**: DHCP snooping does not generate log messages. This is the default setting.
    - **Enabled**: DHCP snooping generates a log message when an invalid packet is received and dropped by the interface.
11. In the **Rate Limit (pps)** field, type the rate limit value for DHCP snooping purposes.

    If the incoming rate of DHCP packets per second exceeds the configured burst interval per second, the port shuts down. If the rate limit is None (which is the default), the burst interval is also not applicable, and rate limiting is disabled.
12. In the **Burst Interval (secs)** field, type the burst interval in seconds for rate limiting on the interface.

    If the rate limit is N/A, the burst interval is not applicable.
13. Click the **Save** button.

    Your settings are saved.

Add a static DHCP snooping binding

You can add a static binding to the DHCP snooping bindings database.

To add a static DHCP snooping binding:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

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

   The Binding Configuration page displays.
6. In the Static Binding Configuration section, click the **Add New** button.

   The Add Static Binding Configuration pop-up window displays.
7. From the **Interface** menu, select the interface.
8. In the **MAC Address** field, type the MAC address for the binding to be added.

   This is the key to the binding database.
9. From the **VLAN ID** menu, select the ID of the VLAN.
10. In the **IP Address** field, type the IP address for the binding to be added.
11. Click the **Save** button.

    Your settings are saved. The DHCP snooping binding entry is added to the database.

Change a static DHCP snooping binding

You can change an existing static DHCP snooping.

To change a static DHCP snooping binding:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

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

   The Binding Configuration page displays.
6. In the Static Binding Configuration section, select the check box for the interface binding configuration.
7. Click the **Edit** button.

   The Edit Static Binding Configuration pop-up window displays.
8. Change the settings as needed.

   For more information about the settings, see Add a static DHCP snooping binding on page 107.
9. Click the **Save** button.

   Your settings are saved.

Remove a static DHCP snooping binding

You can remove a static binding from the DHCP snooping bindings database.

To remove a static DHCP snooping binding:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The Binding Configuration page displays.
6. In the Static Binding Configuration table, select the check box for the static binding.
7. Click the **Delete** button.

   The DHCP snooping binding entry is removed from the database.

Display or clear dynamic DHCP snooping bindings

You can display or clear the dynamic DHCP snooping bindings.

To display or clear the dynamic DHCP snooping 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The Binding Configuration page displays.

   The Dynamic Binding Configuration section shows information about the DHCP bindings that were learned on each interface on which DHCP snooping is enabled.
6. To clear the dynamic DHCP snooping bindings, clear the **Clear** button.
7. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields in the Dynamic Binding Configuration section.

Table 21. Dynamic binding 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

Table 21. Dynamic binding configuration information (Continued)

Field	Description
IP Address	The IP address assigned to the client by the DHCP server
Lease Time	The remaining IP address lease time for the client

Configure DHCP snooping persistent settings

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

To configure DHCP snooping persistent settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The Persistent Configuration page displays.
6. Select where the DHCP snooping bindings database is located.
   - **Local**: The binding table is stored locally on the switch.
   - **Remote**: The binding table is stored on a remote TFTP server.

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

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

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

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

8. Click the **Apply** button.

   Your settings are saved.

Display the DHCP snooping statistics

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

To display the DHCP snooping statistics:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

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

   The DHCP Snooping Statistics page displays.

6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**All**).
7. To refresh the page, click the **Refresh** button.

The following table describes the DHCP snooping statistics.

Table 22. DHCP Snooping Statistics information

Field	Description
Interface	The interface for which statistics are displayed
MAC Verify Failures	The number of DHCP messages that were dropped because the source MAC address and client hardware address did not match. MAC address verification is performed only if it is globally enabled.
Client Ifc Mismatch	The number of packets that were dropped by DHCP snooping because the interface and VLAN on which the packet was received do not match the client's interface and VLAN information stored in the binding database
DHCP Server Messages	The number of DHCP server messages that were dropped on an untrusted port

DHCP Layer 2 relay

If you enable and configure a DHCP relay agent on the switch, some Layer 2 (L2) devices do not need to connect to a DHCP server on the physical network. A relay agent automatically populates the gateway IP address (giaddr) field and adds the Relay Agent Information option to DHCP messages. A DHCP server uses this option for IP addresses and other assignment policies. A DHCP relay agent is usually an IP routing-aware device, which is also referred to as a Layer 3 relay agent. In some network configurations, L2 devices must append the Relay Agent Information option because they are closer to the end hosts.

An L2 device can operate as a bridge only for a network and might not include an IPv4 address on the network. If an L2 device lacks an IPv4 source address, the device cannot relay packets directly to a DHCP server that is located on another network. In that situation, the L2 device can append the Relay Agent Information option and broadcast the DHCP message.

Configure the global DHCP L2 relay settings

To configure the global DHCP L2 relay 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > DHCP Services > DHCP L2 Relay > DHCP L2 Relay Global Configuration**.

   The DHCP L2 Relay Global Configuration page displays.
6. Click the **Admin Mode** toggle:
   - **The toggle is gray and positioned to the left**: DHCP L2 Relay is globally disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: DHCP L2 Relay is globally enabled.
7. Click the **Apply** button.

   Your settings are saved.

Configure the DHCP L2 relay VLAN settings

You can enable or disable the DHCP L2 relay VLAN settings and circuit ID suboption of DHCP Option-82, and set a remote ID string.

To configure the DHCP L2 relay 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > DHCP Services > DHCP L2 Relay > DHCP L2 Relay Global Configuration**.

   The DHCP L2 Relay Global Configuration page displays.

   The following steps refer to the DHCP L2 Relay VLAN Configuration section.
6. Select the check box for the VLAN.
7. Click the **Edit** button.

   The Edit DHCP L2 Relay VLAN Configuration pop-up window displays.
8. From the **Admin Mode** menu, select the DHCP L2 relay mode for the VLAN:
   - **Disabled**: DHCP L2 relay is disabled for the VLAN.
   - **Enabled**: DHCP L2 relay is enabled for the VLAN. This is the default setting.
9. From the **Circuit ID Mode** menu, select the circuit ID option for the VLAN:
   - **Disabled**: The circuit ID suboption of DHCP Option-82 is disabled for the VLAN. This is the default setting.
   - **Enabled**: The circuit ID suboption of DHCP Option-82 is enabled for the VLAN.
10. In the **Remote ID String** field, type the remote ID.

    The remote ID applies if the circuit ID suboption is enabled.
11. Click the **Save** button.

    Your settings are saved.

Configure a DHCP L2 relay interface

You can enable a DHCP L2 relay on an interface.

To configure DHCP L2 relay 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > DHCP Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration**.

   The DHCP L2 Relay Interface Configuration page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit DHCP L2 Relay Configuration pop-up window displays.
9. From the **Admin Mode** menu, select the DHCP L2 relay mode for the interface:
   - **Disabled**: DHCP L2 relay is disabled for the interface.
   - **Enabled**: DHCP L2 relay is enabled for the interface. This is the default setting.
10. From the **82 Option Trust Mode** menu, select to enable or disable the interface as a trusted interface for the Relay Agent Information option (Option 82):
    - **Disabled**: The interface is not a trusted interface. This is the default setting.
    - **Enabled**: The interface is a trusted interface
11. Click the **Save** button.

    Your settings are saved.

Display or clear the DHCP L2 relay interface statistics

To display or clear the DHCP L2 relay interface 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > DHCP Services > DHCP L2 Relay > DHCP L2 Relay Interface Statistics**.

   The DHCP L2 Relay Interface Statistics page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**All**).
7. To clear the statistics, click the **Clear** button.
8. To refresh the information on the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 23. DHCP L2 relay interface statistics information

Field	Description
Interface	The interface from which the DHCP message is received
Untrusted Server Messages With Opt82	The number of DHCP messages with Option 82 received from an untrusted server
Untrusted Client Messages With Opt82	The number of DHCP messages with Option 82 received from an untrusted client

Table 23. DHCP L2 relay interface statistics information (Continued)

Field	Description
Trusted Server Messages Without Opt82	The number of DHCP messages without Option 82 received from a trusted server
Trusted Client Messages Without Opt82	The number of DHCP messages without Option 82 received from a trusted client

3

Manage VLANs

This chapter covers the following topics:

- Manage the VLAN configuration on the switch
- Auto-VLANs
- Configure a MAC-based VLAN
- Configure a protocol-based VLAN group
- Configure Generic Attribute Registration Protocol
- Private VLANs
- Protect ports

Note: For more information about VLANs and a configuration example, see Virtual Local Area Networks (VLANs) on page 489.

Manage the VLAN configuration on the switch

You can add, change, and delete VLANs, or reset the entire VLAN configuration on the switch to defaults.

About VLANs

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

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

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

You can define VLAN groups stored in the VLAN membership table. Each switch can support up to 256 VLANs. VLAN 1 is created by default and is the default VLAN of which all ports are members.

The following VLANs are preconfigured on the switch and you cannot delete them although you can change the VLAN IDs (except for VLAN 1):

- **VLAN 1**: The default VLAN of which all interfaces and LAGs are members.
- **VLAN 4086**: The Auto-WiFi VLAN. An interface or LAG that is connected to a detected WiFi device such as an access point automatically becomes a member of the Auto-WiFi VLAN.
- **VLAN 4087**: The Auto-Camera VLAN. An interface or LAG that is connected to a detected camera automatically becomes a member of the Auto-Camera VLAN.
- **VLAN 4088**: The Auto-VoIP VLAN. An interface or LAG that is connected to a detected VoIP device automatically becomes a member of the Auto-VoIP VLAN.
- **VLAN 4089**: The Auto-Video VLAN. An interface or LAG that is connected to a detected video device automatically becomes a member of the Auto-Video VLAN.

By default, none of the four Auto VLANs include as members any interfaces or LAGs. Interfaces and LAGs are added automatically upon device detection.

Add a VLAN

You can add multiple VLANs to customize the switch for you network.

A VLAN is reserved by a port-based routing interface and invisible to the end user. After a VLAN is allocated by the port-based routing interface, the VLAN cannot be assigned to a routing VLAN interface.

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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > VLAN Management**.

   The VLAN Management page displays.
6. Click the **Add New** button.

   The Add VLAN Configuration pop-up window displays.
7. In the **VLAN ID** field, type the identifier for the new VLAN.

   The range of the VLAN ID can be from 2 to 4093, excluding 4086, 4087, 4088 and 4089, all of which are preconfigured Auto VLANs. If you change the VLAN ID for an Auto VLAN (see Configure the OUI-based properties on page 132), you can re-use the preconfigured VLAN ID.
8. In the **VLAN Name** field, type a name for the new VLAN.

   The name can be up to 32 characters, including blanks.
9. Click the **Save** button.

Your setting are saved and the VLAN is added.

Note: When you add a VLAN manually (as in this procedure), the VLAN Type field always shows Static. A VLAN that is created by GVRP registration initially uses a type of dynamic but you can change it to static (see Change a VLAN on page 124).

Configure membership interfaces for a VLAN

You can add ports, LAGs, or both to a VLAN.

To configure membership interfaces 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The VLAN Configuration (Basic) page displays.
6. From the **VLAN ID** menu, select the VLAN ID.

   The following steps refer to the Port Membership section.
7. To add and configure or remove *individual* ports or LAGs, do the following:
   a. In the Ports table or LAG table, select the ports or LAGs that you want to add to the VLAN or exclude from the VLAN by doing the following:

- **Select**: Click an excluded port or LAG once. A selected port or LAG displays blue.
- **Exclude**: Click a selected port or LAG once. An excluded port or LAG displays blank.

b. To configure the selected ports or LAGs, click the following buttons as needed under the Ports table or the LAG table:

- **Untag Port**: The selected ports or LAGs are added as untagged members of the VLAN. These ports or LAGs display a "U."
- **Tag Port**: The selected ports or LAGs are added as tagged members of the VLAN. These ports or LAGs display a "T."
- **PVID**: The VLAN is assigned as the PVID for the selected ports or LAGs. These ports or LAGs display a "P."
- **Clear**: The configuration is removed from the port or LAG. The port or LAG does not display a "U," "T," or "P."

8. To add and configure or remove *all ports or LAGs simultaneously*, click the following buttons as needed under the Ports table or the LAG table:

- **Select All**: All ports or LAGs are included in the VLAN. All ports or LAGs display blue.

  After you click the Select All button, the button changes to the Unselect All button.
- **Unselect All**: All ports or LAGs are excluded from the VLAN. All ports or LAGs display blank.

  After you click the Unselect All button, the button changes to the Select All button.
- **Untag Port**: First click the **Select All** button and then the **Untag Port** button to add all ports or LAGs as untagged members of the VLAN. All ports or LAGs display a "U."
- **Tag Port**: First click the **Select All** button and then the **Tag Port** button to add all ports or LAGs as tagged members of the VLAN. All ports or LAGs display a "T."
- **PVID**: First click the **Select All** button and then the **PVID** button to assign the VLAN as the port VLAN ID (PVID) for all ports or LAGs. All ports or LAGs display a "P."
- **Clear**: First click the **Select All** button and then the **Clear** button to remove the configuration from all ports or LAGs. All ports or LAGs display blank.

9. Click the **Apply** button.

   Your settings are saved.

The following table describes the view-only fields on the page.

Table 24. VLAN Configuration (Basic)

Field	Definition
VLAN Name	The name for the VLAN
VLAN Type	The type of the VLAN you selected: • **Default** (VLAN ID = 1): Always present • **Static**: A VLAN that you added manually or the Auto-WiFi, Auto-Camera, Auto-VoIP, or Auto-Video VLAN • **Dynamic**: A VLAN that was created through GVRP registration and that you did not convert to static, and that GVRP can therefore remove

Change a VLAN

You can change the name for a statically or dynamically added VLAN.

Note: For a dynamically added VLAN (for example, a VLAN that is created by GVRP registration), you cannot change the VLAN type to static, but you can add a new VLAN with the same VLAN ID (see Add a VLAN on page 121), which effectively changes the dynamic VLAN to a static VLAN.

To change 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > VLAN Management**.

   The VLAN Management page displays.
6. Select the check box that is associated with the VLAN.

7. Click the **Edit** button.

   The Edit VLAN Configuration pop-up window displays.
8. To change the VLAN name, in the **VLAN Name** field, type a name for new VLAN.

   The name can be up to 32 characters, including blanks.
9. Click the **Save** button.

   You changes are saved.

Delete one or more VLANs

You can delete one or more VLANs that you no longer need. You cannot delete the default VLAN (VLAN 1) and the preconfigured Auto-WiFi, Auto-Camera, Auto-VoIP, and Auto-Video VLANs.

To delete one or more VLANs:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > VLAN Management**.

   The VLAN Management page displays.
6. In the VLAN Configuration section, select the check boxes for the VLAN IDs.
7. Click the **Delete** button.

   Your settings are saved and the VLANs are deleted.

Reset the entire VLAN configuration to default setting

You can reset all VLAN configuration settings on the switch to factory default settings, with the exception of the default VLAN (VLAN 1) and the preconfigured Auto VLANs (VLANs 4086, 4087, 4088, and 4089). The factory default values are as follows:

- All ports are assigned to the default VLAN of 1.
- All ports are configured with a PVID of 1.
- All ports are configured to admit all frames.
- All ports are configured with ingress filtering disabled.
- All ports are configured to transmit only untagged frames.
- GVRP is disabled on all ports and all dynamic entries are cleared.

To reset the entire VLAN configuration to 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > VLAN Management**.

   The VLAN Management page displays.
6. Click the **Reset Configuration** toggle.

   A warning pop-up window displays.
7. Click the **OK** button.

   The toggle is now purple and positioned to the right.

Warning: If you click the Apply button, all VLAN configuration settings on the switch are reset to their factory default values.

8. Click the **Apply** button.

   Your settings are saved. All VLANs, except for the default VLAN and the Auto VLANs, are deleted.

Change the port VLAN ID (PVID) settings

By default, each interface is assigned a port VLAN ID (PVID) of 1 because it is associated with the default VLAN, VLAN ID 1.

If you want to change the PVID for an interface, the interface must be a member of at least one other VLAN in addition to the default VLAN.

In addition to the PVID, you can configure other PVID-related settings.

To configure the PVID and PVID-related 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

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

   The VLAN Configuration (Advanced) page displays.

6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit PVID Configuration pop-up window displays.

9. In the **PVID** field, type the VLAN ID to assign to untagged or priority-tagged frames received on this interface.

   The default is 1.

10. In the **VLAN Member** field, type the VLAN ID or list of VLANs of a member interface.

    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.

11. In the **VLAN Tag** field, type the VLAN ID or list of VLANs of a tagged interface.

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

12. From the **Acceptable Frame** menu, select the types of frames that can be received on the interface:

    - **Admit All**: Untagged frames and priority-tagged frames received on the interface are accepted and assigned the value of the port VLAN ID for the interface. VLAN-tagged frames are forwarded in accordance to the 802.1Q VLAN specification. This is the default setting.
    - **VLAN Only**: Untagged frames and priority-tagged frames received on the interface are discarded. VLAN-tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
    - **Admit Untagged Only**: Untagged frames received on the interface are accepted. VLAN-tagged frames are forwarded in accordance to the 802.1Q VLAN specification.

13. From the **Ingress Filtering** menu, select one of the following options:

    - **Disabled**: All frames are forwarded in accordance with the 802.1Q VLAN bridge specification. This is the default setting.
    - **Enabled**: The frame is discarded if the interface 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 of the interface that receives this frame.

14. In the **Port Priority** field, set the default 802.1p priority assigned to untagged packets arriving at the port.

    You can enter a number from 0 (the lowest priority) to 7 (the highest priority).

15. Click the **Save** button.

    Your settings are saved.

The following table describes the view-only fields on the page.

Table 25. PVID configuration information

Field	Description
Interface	The interface for which information is displayed
Current Ingress Filtering	Indicates whether ingress filtering is enabled for the interface
Untagged VLANs	The ID or IDs of the untagged VLANs of which the interface is a member
Tagged VLANs	The ID or IDs of the tagged VLANs of which the interface is a member
Forbidden VLANs	The ID or IDs of the forbidden VLANs of which the interface is a member
Dynamic VLANs	The ID or IDs of the dynamically added VLANs of which the interface is a member

Configure a voice VLAN

Voice over Internet Protocol (VoIP) enables telephone calls over a data network. Because voice traffic is typically more time-sensitive than data traffic, a voice VLAN helps provide a classification mechanism for voice packets so that they can be prioritized above data packets in order to provide better Quality of Service (QoS).

For example, you can enable a voice VLAN on an interface that is connected to IP phones. A voice VLAN can ensure that the sound quality of IP phone traffic remains good when data traffic on the same interface is high.

To configure a voice VLAN:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > Voice VLAN Configuration**.

   The Voice VLAN Configuration page displays.
6. In the Voice VLAN Global Admin section, click the **Admin Mode** toggle to enable the global voice VLAN mode on the switch.

   The toggle is purple and positioned to the right. By default, the global voice VLAN mode is disabled and the toggle is gray and positioned to the left.

   The following steps refer to the Voice VLAN Configuration section.
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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit Voice VLAN Configuration pop-up window displays.
9. From the **Interface Mode** menu, select the voice VLAN mode:
   - **Disable**: Voice VLAN mode is disabled for the interface. This is the default setting.
   - **None**: A telephone that is connected to the interface can use its own configuration to send untagged voice traffic.
   - **VLAN ID**: A telephone that is connected to the interface must be configured to send tagged voice traffic.
   - **Dot1p**: Configure voice VLAN 802.1p priority tagging for voice traffic.

     If you select this mode, enter the dot1p value in the **Value** field. You can enter a value from 0 (the lowest priority) to 7 (the highest priority).
   - **Untagged**: A telephone that is connected to the interface must be configured to send untagged voice traffic.
10. From the **CoS Override Mode** menu, select if the 802.1p priority value is overridden:

- **Disabled**: The interface trusts the priority value in the received frame. This the default setting.
- **Enabled**: The interface ignores (that is, overrides) the 802.1p priority value in the Ethernet frames it receives from connected devices. The DSCP field overrides the CoS value.

11. From the **Authentication Mode** menu, select if an authorized interface is required for voice traffic:

    - **Disabled**: Voice traffic is allowed only an authorized voice VLAN interface, for which dot1x must be enabled (see Configure the 802.1X authentication settings for a port on page 339).
    - **Enabled**: Voice traffic is allowed on an unauthorized voice VLAN interface. This the default setting.

12. In the **DSCP Value** field, type the DSCP value for the interface.

    The range is from 0 to 64. The default is 0.

13. Click the **Save** button.

    Your settings are saved.

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

Auto-VLANs

An Auto-VLAN allows a device to be automatically placed in a VLAN based on the type of device or the type of traffic that is typical for the device. For most Auto-VLANs, you can set the prioritization for the level of Quality of Service (QoS) that is suitable for the type of device that the VLAN supports.

The switch comes preconfigured with the following Auto-VLANs:

- **Auto-VoIP**: The switch places detected Voice over Internet Protocol (VoIP) devices in the Auto-VoIP VLAN.
- **Auto-WiFi**: The switch places detected WiFi devices in the Auto-WiFi VLAN.
- **Auto-Camera**: The switch places detected camera devices in the Auto-Camera VLAN.
- **Auto-Video**: The switch places detected video devices in the Auto-Video VLAN.

Except for the Auto-Video VLAN, prioritization is based on protocol-based organizationally unique Identifier (OUI) bits. For the Auto-Video VLAN, prioritization is based on detected multicast traffic.

Configure the OUI-based properties

With organizationally unique Identifier (OUI)–based Auto-VLANs, voice prioritization is provided based on OUI bits.

To configure the OUI-based properties for the Auto-VoIP VLAN, Auto-WiFi VLAN, or Auto-Camera 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > Auto-VLAN > OUI-based Auto-VLAN**.

   The OUI-based Auto-VLAN page displays.

   The following steps refer to the OUI-based Properties section.
6. Change the OUI-based properties for the Auto VLANs as needed:
   - **Auto-VoIP VLAN ID**:
     - To change the default VLAN ID 4088 to another ID, type the ID in the **Auto-VoIP VLAN ID** field.
     - In the associated **OUI-Based priority** field, enter a priority value from 0 (lowest priority) to 7 (highest priority). The default setting is 7.
   - **Auto-WiFi VLAN ID**
     - To change the default VLAN ID 4086 to another ID, type the ID in the **Auto-WiFi VLAN ID** field.
     - In the associated **OUI-Based priority** field, enter a priority value from 0 (lowest priority) to 7 (highest priority). The default setting is 7.
   - **Auto-Camera VLAN ID**

- To change the default VLAN ID 4087 to another ID, type the ID in the **Auto-Camera VLAN ID** field.
- In the associated **OUI-Based priority** field, enter a priority value from 0 (lowest priority) to 7 (highest priority). The default setting is 7.

7. Click the **Apply** button.

   Your settings are saved.

Configure the OUI-based interface settings

You can configure the OUI interface settings.

To configure the OUI-based 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > Auto-VLAN > OUI-based Auto-VLAN**.

   The OUI-based Auto-VLAN page displays.

   The following steps refer to the OUI Port Settings section.

6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit OUI Port Settings pop-up window displays.

9. From the **Auto VoIP Mode** menu, select the Auto VoIP mode for the interface:
   - **Disable**: The Auto VoIP mode is disabled. This is the default setting.
   - **Enable**: The Auto VoIP mode is enabled.
10. From the **Auto WiFi Mode** menu, select the Auto WiFi mode for the interface:
    - **Disable**: The Auto WiFi mode is disabled. This is the default setting.
    - **Enable**: The Auto WiFi mode is enabled.
11. From the **Auto Camera Mode** menu, select the Auto Camera mode for the interface:
    - **Disable**: The Auto Camera mode is disabled. This is the default setting.
    - **Enable**: The Auto Camera mode is enabled.
12. Click the **Save** button.

    Your settings are saved.

    In the OUI Port Settings section, the Auto-VLAN Mode fields show if the mode is enabled or disabled.

    The Operational Status fields show if the interface for which you enabled or disabled the Auto-VLAN mode is connected to a device or administratively enabled or disabled. For example, if you enabled the Auto-WiFi mode for interface g2 but that interface is not connected to a device or is administratively disabled, the Operational Status field shows Down.

Manage the OUI table

Device hardware manufacturers can include an organizationally unique identifier (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 VoIP phone manufacturer:

- 00:01:E3: SIEMENS
- 00:03:6B: CISCO1

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

You can add OUIs for VoIP phones, WiFi devices, and camera.

Each OUI lets a device be automatically placed in the associated Auto-VLAN. For example, a device that is identified by an OUI for a VoIP phone can be automatically placed in the Auto-VoIP VLAN.

Add an OUI

You can add a new OUI and description to identify a WiFi device, camera, or VoIP phone on the network. The switch supports up to 32 OUIs.

To add an OUI:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > Auto-VLAN > OUI-based Auto-VLAN**.

   The OUI-based Auto-VLAN page displays.
6. Scroll down to the OUI Table section.
7. Click the **Add New** button.

The Add OUI Table pop-up window displays.

8. In the **Telephony OUIs** field, type the OUI.

   The OUI must be in the format AA:BB:CC.

9. In the **Description** field, type a description of up to 32 characters.
10. From the **Auto-VLAN Type** menu, select the type of OUI:
    - **Auto-WiFi**: The OUI is for a WiFi device.
    - **Auto-Camera**: The OUI is for a camera.
    - **Auto-VoIP**: The OUI is for a VoIP phone.
11. Click the **Save** button.

    Your settings are saved and the OUI is added to the OUI Table section.

Remove an OUI

You can remove a preconfigured or custom OUI that you do not need.

To remove an OUI:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > Auto-VLAN > OUI-based Auto-VLAN**.

   The OUI-based Auto-VLAN page displays.

6. Scroll down to the OUI Table section.
7. Select the check box for the OUI.

   You can select more than one check box.

8. Click the **Delete** button.

Your settings are saved and the OUI is removed from the OUI Table section.

Configure the global protocol-based VoIP prioritization and class

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

To prioritize time-sensitive voice traffic over data traffic, protocol-based Auto-VoIP checks for packets carrying the Session Initiation Protocol (SIP) VoIP protocol. VoIP frames that are received on ports for which the Auto-VoIP feature is enabled are marked with the specified CoS traffic class value.

To configure the global protocol-based VoIP prioritization and 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > Auto-VLAN > Protocol-based VoIP**.

   The Protocol-based VoIP page displays.

   The following steps refer to the Protocol-Based Global Settings section.
6. From the **Prioritization Type** menu, select the prioritization type:

- **Traffic Class**: Incoming traffic is assigned the CoS class value that you select in the following step.
- **Remark**: Outgoing traffic is assigned the CoS class value that you select in the following step.

7. In the **Class Value** menu, select the CoS class value to be reassigned for packets that the voice VLAN receives.

   You can select a value in the range from 0 to 7. The default setting is 7, which is the highest priority.

8. Click the **Apply** button.

   Your settings are saved.

Configure VoIP protocol-based interface settings

To prioritize time-sensitive voice traffic over data traffic, protocol-based Auto-VoIP determines if packets carry the following VoIP protocols:

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

VoIP packets that come in on an interface on which Auto-VoIP is enabled are marked with the specified CoS traffic class value.

To configure VoIP protocol-based settings for 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

The Dashboard page displays.

5. Select **Switching > VLAN > Auto-VLAN > Protocol-based VoIP**.

   The Protocol-based VoIP page displays.

   The following steps refer to the Protocol-Based Port Settings section.

6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit Protocol-Based Port Settings pop-up window displays.

9. From the **Auto VoIP Mode** menu, select the Auto VoIP mode for the interface.
   - **Disable**: The Auto VoIP mode is disabled. This is the default setting.
   - **Enable**: The Auto VoIP mode is enabled.
10. Click the **Save** button.

    Your settings are saved.

    The Operational Status field shows if the interface is up or down.

Display the Auto-VoIP status

To display the Auto-VoIP status:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > Auto-VLAN > Auto-VoIP Status**.

   The Auto-VoIP Status page displays.
6. To refresh the page, click the **Refresh** button.

   The following table describes the view-only fields on the page.

Table 26. Auto-VoIP status information

Field	Description
Auto-VoIP VLAN ID	The Auto-VoIP VLAN ID (By default, 4088)
Maximum Number of Voice Channels Supported	The maximum number of voice channels supported
Number of Voice Channels Detected	The number of VoIP channels prioritized successfully

Configure a MAC-based VLAN

A MAC-based VLAN allows incoming untagged packets to be assigned to a VLAN and classifies 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 defined by its source MAC address and a VLAN ID. MAC–to–VLAN configurations are shared across all interfaces (that is, there is a system-wide table 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 switch attempts to find the source MAC address of the packet: If the switch finds an entry, 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. You must manually configure a MAC-address–to–VLAN-ID mapping.

Add a MAC-based VLAN configuration

To add a MAC-based VLAN configuration:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > MAC-based VLAN**.

   The MAC-based VLAN page displays.
6. Click the **Add New** button.

   The Add MAC-based VLAN Configuration pop-up window displays.
7. In the **MAC Address** field, type a MAC address that must be bound to a VLAN ID.
8. In the **VLAN ID** field, type the VLAN ID in the range of 1 to 4093.
9. Click the **Save** button.

   Your settings are saved and the MAC-based VLAN configuration is added.

Delete a MAC-based VLAN configuration

To delete a MAC-based VLAN configuration:

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > MAC-based VLAN**.

   The MAC-based VLAN page displays.
6. Select the check box for the MAC-based VLAN configuration.
7. Click the **Delete** button.

   The MAC-based VLAN configuration is deleted.

Configure a protocol-based VLAN group

You can use a protocol-based VLAN to define filtering criteria for untagged packets. By default, if you do not configure a port-based (IEEE 802.1Q) or protocol-based VLAN, untagged packets are assigned to VLAN 1. You can override this behavior by defining port-based VLANs, 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 an interface to a protocol-based VLAN for a specific protocol, untagged frames received on the interface for that protocol are assigned the protocol-based VLAN ID. Untagged frames received on the interface for other protocols are assigned the Port VLAN ID, either the default PVID (1) or a PVID you specifically assigned to the interface (see Change the port VLAN ID (PVID) settings on page 127).

You define a protocol-based VLAN by creating a group. Each group has a one-to-one relationship with a VLAN ID, can include one to three protocol definitions, and can include multiple interfaces. When you create a group, you specify a name. A group ID is assigned automatically.

Add a protocol-based VLAN group

You can add a protocol-based VLAN group.

To add 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > Protocol-based VLAN**.

   The Protocol-based VLAN page displays.
6. Click the **Add New** button.

   The Add Protocol-based VLAN Group pop-up window displays.
7. In the **Group ID** field, type a numerical ID.

   You can enter an ID in the range from 1 to 128.
8. In the **Group Name** field, type a name for the new group.

   You can enter up to 16 characters.
9. In the **Protocol** field, type one or more of the following protocols to be associated with the group:

   - **IP**: IP is a network layer protocol that provides a connectionless service for the delivery of data.
   - **ARP**: Address Resolution Protocol (ARP) is a low-level protocol that dynamically maps network layer addresses to physical medium access control (MAC) addresses.
   - **IPX**: The internetwork packet exchange (IPX) is a connectionless datagram network-layer protocol that forwards data over a network.

Separate protocols by a comma (,). For example, to specify all three protocols, enter the following: ip,arp,ipx

You can also enter hexadecimal or decimal values in the range of 0x0600(1536) to 0xFFFF(65535).

10. In the **VLAN ID** field, type the VLAN ID.

    The ID must be a number in the range of 1 to 4093. An interface in the group assigns this VLAN ID to untagged packets that the interface receives for the protocols that you include in this group.

11. Click the **Save** button.

    Your settings are saved and the protocol-based VLAN group is added.

    The Ports field displays the interfaces that belong to the group.

Configure membership interfaces for a protocol-based VLAN group

For a protocol, an interface can belong to one protocol-based VLAN group only. If you already added an interface to a group for IP, you cannot add the interface to another group that also includes IP, but you *can* add it to a new group for IPX.

To configure membership interfaces for 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > VLAN > Protocol-based VLAN**.

   The Protocol-based VLAN page displays.

The following steps refer to the Protocol-based VLAN Group Membership section.

6. From the **Group ID** menu, select the protocol-based VLAN group ID.

   The Group Name field shows the name for the protocol-based VLAN that you select.

7. In the Ports table, click the ports that you want to add to the VLAN.

   Click once to select a port. A selected port displays blue.

   Click again to deselect an already selected port. An excluded port displays blank.

8. In the LAG table, click the LAGs that you want to add to the VLAN.

   Click once to select a LAG. A selected LAG displays blue.

   Click again to deselect an already selected LAG. An excluded LAG displays blank.

9. Click the **Apply** button.

   Your settings are saved.

   The Current members field displays the ports and LAGs that are members of the selected VLAN group.

Change a protocol-based VLAN group

You can change an existing protocol-based VLAN group.

To change 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > VLAN > Protocol-based VLAN**.

   The Protocol-based VLAN page displays.

6. Select the check box for the group ID.

7. Click the **Edit** button.

   The Edit Protocol-based VLAN Group pop-up window displays.
8. Change the settings as needed.

   For more information, see Add a protocol-based VLAN group on page 143.
9. Click the **Save** button.

   Your settings are saved.

Delete a protocol-based VLAN group

You can delete a protocol-based VLAN group that you no longer need.

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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > Protocol-based VLAN**.

   The Protocol-based VLAN page displays.
6. Select the check box for the group ID.
7. Click the **Delete** button.

   The protocol-based VLAN group is deleted.

Configure Generic Attribute Registration Protocol

Generic Attribute Registration Protocol (GARP) allows network devices to share information such as VLAN IDs and multicast group membership across a bridged LAN. That is, GARP participants can register and deregister attribute values within the LAN. When a GARP participant declares or withdraws an attribute, the attribute value is recorded for that attribute and for the interface from which the declaration or withdrawal was made.

The following applies to GARP:

- Registration occurs only on interfaces that receive a GARP PDU with a declaration or withdrawal.
- Deregistration occurs only if all GARP participants that are connected to the same LAN segment as the interface withdraw the declaration.

Configure the GARP switch settings

You can globally enable GARP VLAN registration protocol (GVRP) on the switch. If GVRP is enabled, the switch can share VLAN IDs with devices in the network.

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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > GARP VLAN**.

The GARP VLAN page displays.

6. In the GARP Switch Configuration section, click the **GVRP Mode** toggle to enable the GVRP mode for the switch.

   The toggle is purple and positioned to the right. By default, the GVRP mode is disabled and the toggle is gray and positioned to the left.

7. Click the **Apply** button.

   Your settings are saved.

Configure GARP interface settings

You can configure GARP settings for individual interfaces. These settings take effect only if the GVRP mode is enabled on the switch.

To configure GARP settings 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > VLAN > GARP VLAN**.

   The GARP VLAN page displays.

   The following steps refer to the GARP Port Configuration section.

6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit GARP Port Configuration pop-up window displays.

9. From the **GVRP Mode** menu, select to enable or disable GVRP mode for the interface:
   - **Disabled**: The GVRP mode is disabled for the interface. The join timer, leave timer, and leave all timer options are without any effect. This is the default setting.
   - **Enabled**: The GVRP mode is enabled for the interface.
10. In the **Join Timer** field, type the time in centiseconds between the transmission of GARP PDUs registering 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).

11. In the **Leave Timer** field, type the time in centiseconds that the interface must 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).

12. In the **Leave All Timer** field, type how frequently 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 * 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).

13. Click the **Save** button.

    Your settings are saved.

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.

A private VLAN separates a regular VLAN domain into two or more subdomains. Each subdomain is defined (represented) by a primary VLAN and a secondary VLAN:

- **Primary VLAN**: The primary VLAN ID is the same for all subdomains that belong to a private VLAN.
- **Secondary VLAN**: The secondary VLAN ID differentiates subdomains from each other and provides Layer 2 isolation between ports of the same private VLAN.

Within a private VLAN, three types of VLANs can exist:

- **Primary VLAN**: The VLAN forwards traffic from promiscuous ports to isolated ports, community ports, and other promiscuous ports in the same private VLAN. In a private VLAN, you can configure only one primary VLAN. All ports in a private VLAN share the same primary VLAN.
- **Isolated VLAN**: The VLAN is a secondary VLAN that carries traffic from isolated ports to promiscuous ports. In a private VLAN, you can configure one isolated VLAN only.
- **Community VLAN**: The VLAN is a secondary VLAN that forwards traffic between ports that belong to the same community and to the promiscuous ports. In a private VLAN, you can configure multiple community VLANs.

Within a private VLAN, the switch supports two types of special port designations:

- **Host port**: The port is a host port that is a member of a community VLAN or an isolated VLAN, both of which are secondary VLANs within the private VLAN. Two host port subtypes exist:
  - **Community port**: The port is a member of a community VLAN. A community port can communicate with other community ports and promiscuous ports.
  - **Isolated port**: The port is a member of an isolated VLAN. An isolated port can communicate with promiscuous ports.
- **Promiscuous port**: The port is a member of a primary VLAN (within the private VLAN) and can communicate with all types of ports in the private VLAN, including other promiscuous ports, community ports, and isolated ports.

Overview of the tasks for private VLAN configuration

To set up a private VLAN that allows for communication between switches in a network, perform the tasks that are described in the following sections:

1. Assign a private VLAN type to a VLAN on page 151.

By default, a VLAN is a regular VLAN, so you must assign a private VLAN type to a VLAN.

2. Configure a private VLAN association with a primary and secondary VLAN on page 152.

   A private VLAN must consist of a single primary VLAN and one or more secondary VLANs.

3. Configure the private VLAN port mode on page 154.

   A port must be in the correct port mode to participate in a private VLAN. For example, to make a port a member of an isolated VLAN or community VLAN, you must first configure the port as a host port.

4. Private VLAN host interface: Assign the interface to primary and secondary VLANs on page 156.

   For a port that you configured to function in host mode, configure a single primary VLAN and a single secondary VLAN.

5. Private VLAN promiscuous interface: Assign the interface to primary and secondary VLANs on page 159.

   For a port that you configured to function in promiscuous mode, configure a single primary VLAN and one or more secondary VLANs.

Assign a private VLAN type to a VLAN

To each VLAN, you can assign a private VLAN type, which can be Primary, Isolated, or Community. By default, a VLAN is a regular VLAN and assigned the private VLAN type Unconfigured.

To assign a private VLAN type to 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.

4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > Private VLAN > VLAN Type Configuration**.

   The VLAN Type Configuration page displays.
6. Select the check box for the VLAN.
7. Click the **Edit** button.

   The Edit Private VLAN Type Configuration pop-up window displays.
8. From the **Private VLAN Name** menu, select the type of private VLAN:

   - **Unconfigured**: The VLAN is not a private VLAN but a regular VLAN. This is the default setting.
   - **Primary**: The VLAN is a primary VLAN that forwards traffic from promiscuous ports to isolated ports, community ports, and other promiscuous ports in the same private VLAN. In a private VLAN, you can configure only one primary VLAN. All ports in a private VLAN share the same primary VLAN.
   - **Isolated**: The VLAN is a secondary VLAN that carries traffic from isolated ports to promiscuous ports. In a private VLAN, you can configure only one isolated VLAN.
   - **Community**: The VLAN is a secondary VLAN that forwards traffic between ports that belong to the same community and to the promiscuous ports. In a private VLAN, you can configure multiple community VLANs.
9. Click the **Save** button.

   Your settings are saved.

Configure a private VLAN association with a primary and secondary VLAN

You can configure a private VLAN by associating a single primary VLAN with one or more secondary VLANs.

To configure a private VLAN association with a primary and secondary 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > Private VLAN > VLAN Association Configuration**.

   The VLAN Association Configuration page displays.
6. Select the check box for a primary private VLAN.

   The page displays only the VLANs that you configured as primary private VLANs (see Configure the private VLAN port mode on page 154).
7. Click the **Edit** button.

   The Edit Private VLAN Association pop-up window displays.
8. In the **Secondary VLANs** field, type one or more secondary VLANs for the private VLAN.

   This selection sets secondary VLANs (isolated VLANs, community VLANs, or a combination of both) within the private VLAN. The secondary VLANs are associated with the primary VLAN in the private VLAN.

   You can specify a single VLAN ID, a range of VLAN IDs, or a combination of both in sequence separated by a comma (,):

   - You can type an individual VLAN ID, such as 10.
   - You can type the VLAN range values separated by a hyphen, for example, 10-13.
   - You can type the combination of both separated by commas, for example: 12,15,40–43,1000–1005, 2000.

   For information about configuring an isolated or community VLAN for the private VLAN, see Assign a private VLAN type to a VLAN on page 151.
9. Click the **Save** button.

   Your settings are saved.

The following table describes the view-only fields on the page.

Table 27. Private VLAN Association

Field	Description
Isolated VLAN	The single isolated VLAN associated with the selected primary VLAN
Community VLANs	The list of community VLANs associated with the selected primary VLAN

Remove an existing private VLAN association

You can remove a private VLAN association that you no longer need.

To remove a 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > Private VLAN > VLAN Association Configuration**.

   The VLAN Association Configuration page displays.
6. Select the check box for the private VLAN association.
7. Click the **Delete** button.

   Your settings are saved. The private VLAN association is removed.

Configure the private VLAN port mode

A port must be in the correct port mode to participate in a private VLAN.

The private VLAN port mode determines if a port (or LAG) can function in Host mode for a primary or secondary VLAN (within a private VLAN) or in Promiscuous mode for a promiscuous VLAN (within a private VLAN).

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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > VLAN > Private VLAN > VLAN Port Mode Configuration**.

   The VLAN Port Mode Configuration page displays.

6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit Private VLAN Port Mode Configuration pop-up window displays.

9. From the **Port VLAN Mode** menu, select the private VLAN port mode:
   - **General**: The port functions in general mode and not as a port in a private VLAN. This is the default setting.
   - **Host**: The port functions in host mode in a private VLAN. In this mode, the port can be member of a community VLAN or isolated VLAN:

- **Community VLAN**: The port is a member of a secondary VLAN (within the private VLAN) and can communicate with other community ports and promiscuous ports.
- **Isolated VLAN**: The port is a member of a secondary VLAN (within the private VLAN) and can communicate only with promiscuous ports.

To configure a host port to be a member of specific VLANs, see Private VLAN host interface: Assign the interface to primary and secondary VLANs on page 156.

- **Promiscuous**: The port functions in promiscuous mode in a private VLAN. In this mode, the port can communicate with all types of ports in the private VLAN, including other promiscuous ports, community ports, and isolated ports.

  To configure a promiscuous port to be a member of specific VLANs, see Private VLAN promiscuous interface: Assign the interface to primary and secondary VLANs on page 159.

10. Click the **Save** button.

    Your settings are saved.

Private VLAN host interface: Assign the interface to primary and secondary VLANs

If you configure the private VLAN port mode of an interface as Host (see Configure the private VLAN port mode on page 154), you can assign the interface to a single primary VLAN and a single secondary VLAN.

To assign a private VLAN host interface to a primary and secondary 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

The Dashboard page displays.

5. Select **Switching > VLAN > Private VLAN > VLAN Host Interface Configuration**.

   The VLAN Host Interface Configuration page displays.

6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.

   The interface that you select must be configured in Host mode (see Configure the private VLAN port mode on page 154).
8. Click the **Edit** button.

   The Edit Private VLAN Host Interface Configuration pop-up window displays.
9. In the **Host Primary VLAN** field, type a primary VLAN ID.

   You must select a VLAN for which you configured the type as Primary (see Assign a private VLAN type to a VLAN on page 151).
10. In the **Host Secondary VLAN** field, type a secondary VLAN ID.

    You must select a VLAN for which you configured the type as Isolated or Community, both of which are secondary VLAN types within a private VLAN (see Assign a private VLAN type to a VLAN on page 151).
11. Click the **Save** button.

    Your settings are saved.

    The Operational VLANs fields shows the primary and secondary VLANs that operate on the host interface.

Private VLAN host interface: Remove the interface from primary and secondary VLANs

You can remove a private VLAN host interface from primary and secondary VLANs.

To remove a private VLAN host interface from primary and secondary VLANs:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > VLAN > Private VLAN > VLAN Host Interface Configuration**.

   The VLAN Host Interface Configuration page displays.

6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.

   The interface that you select must be configured in Host mode (see Configure the private VLAN port mode on page 154).

8. Click the **Delete** button.

   Your settings are saved. The interface is removed from the primary and secondary VLANs.

Private VLAN promiscuous interface: Assign the interface to primary and secondary VLANs

If you configure the private VLAN port mode of an interface as Promiscuous (see Configure the private VLAN port mode on page 154), you can assign the interface to a single primary VLAN and to one or more secondary VLANs.

To assign a private VLAN promiscuous interface to a primary VLAN and secondary VLANs:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > Private VLAN > VLAN Promiscuous Interface Configuration**.

   The VLAN Promiscuous Interface Configuration page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.

   The interface that you select must be configured in Promiscuous mode (see Configure the private VLAN port mode on page 154).

8. Click the **Edit** button.

   The Edit Private VLAN Promiscuous Interface Configuration pop-up window displays.
9. In the **Promiscuous Primary VLAN** field, specify a primary VLAN ID.

   You can select a VLAN for which you configured the type as Primary (see Assign a private VLAN type to a VLAN on page 151).
10. In the **Promiscuous Secondary VLAN** field, specify one or more secondary VLAN IDs.

    You can specify VLANs for which you configured the type as Isolated or Community, both of which are secondary VLAN types within a private VLAN (see Assign a private VLAN type to a VLAN on page 151).

    You can specify a single 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 a combination of both separated by commas, for example: 12,15,40–43,1000–1005, 2000.
11. Click the **Save** button.

    Your settings are saved.

    The Operational VLANs fields shows the primary and secondary VLANs that operate on the promiscuous interface.

Private VLAN promiscuous interface: Remove the interface from primary and secondary VLANs

You can remove a private VLAN promiscuous interface from primary and secondary VLANs.

To remove a private VLAN promiscuous interface from primary and secondary VLANs:

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > Private VLAN > VLAN Promiscuous Interface Configuration**.

   The VLAN Promiscuous Interface Configuration page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.

   The interface that you select must be configured in Promiscuous mode (see Configure the private VLAN port mode on page 154).
8. Click the **Delete** button.

   Your settings are saved.

   Your settings are saved. The interface is removed from the primary and secondary VLANs.

Protect 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. You can configure ports as protected. A port that is not configured as protected is an unprotected port.

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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > VLAN > Protected Port**.

   The Protected Port page displays.

6. In the Ports table, select the ports that must be protected ports:
   - Click once to select a port. A selected port displays blue. Selected ports become members of the protected port group.
   - Click again to deselect an already selected port. An excluded port displays blank. By default, no ports are selected.
   - Click the **Select All** button to select all ports.
7. Click the **Apply** button.

   Your settings are saved.

4

Configure Switching

This chapter covers the following topics:

- LLDP and LLDP-MED settings for interfaces
- Power over Ethernet
- Green Ethernet settings
- Link aggregation groups
- Configure the port settings and maximum frame size
- Spanning Tree Protocol
- MAC address table
- DHCP snooping
- DHCP Layer 2 relay
- Dynamic ARP inspection

LLDP and LLDP-MED settings for interfaces

This section describes the global Link Layer Discovery Protocol (LLDP) and LLDP-Media Endpoint Discovery (LLDP-MED) settings for interfaces. For information about the global LLDP and LLDP-MED settings, see LLDP and LLDP-MED settings for the switch on page 74.

LLDP, which is defined in IEEE 802.1AB, lets devices on a LAN advertise major capabilities and physical descriptions. You can view this information to identify the system topology and detect problematic configurations in the LAN.

LLDP is a one-way protocol without request and response sequences. Information is advertised by devices that are configured to transmit LLDP and is received and processed by devices that are configured to receive LLDP. You can enable and disable the transmit and receive functions separately per interface. By default, both transmit and receive functions are disabled on all interfaces.

LLDP-MED is an enhancement to LLDP with support for the following features:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 priority, and DiffServ settings), which allows for plug-and-play networking
- Device location discovery, which allows for the creation of location databases
- Extended and automated power management of Power over Ethernet endpoints
- Inventory management, which lets you track your network devices and determine their characteristics, such as manufacturer, software and hardware versions, and serial or asset numbers

Configure LLDP interface settings

You can specify LLDP settings that are applied to one or more interfaces.

To configure LLDP 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Ports > LLDP > LLDP Port Configuration**.

   The LLDP 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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit LLDP Port Configuration pop-up window displays.
8. From the **Admin Status** menu, select the status for transmitting and receiving LLDP packets:
   - **Tx Only**: Enables transmitting of LLDP PDUs only.
   - **Rx Only**: Enables receiving of LLDP PDUs only.
   - **Tx and Rx**: Enable both transmitting and receiving of LLDP PDUs. This is the default setting.
   - **Disabled**: No LLDP PDUs are transmitted or received,
9. From the **Management IP Address** menu, select if the interface advertises the management IP address:
   - **Auto Advertise**: The interface advertises the management IP address. This is the default setting.
   - **Stop Advertise**: The interface does not advertise the management IP address.
10. From the **Notification** menu, select if the interface initiates traps for remote data changes:
    - **Disabled**: The interface does not initiate traps. This is the default setting.
    - **Enabled**: The interface initiates traps.

11. From the **Optional TLVs** menu, select if the interface transmits optional type-length value (TLV) information.
    - **Disabled**: The interface does not transmit optional TLV information.
    - **Enabled**: The interface transmits optional TLV information. This is the default setting.

    The optional TLV information includes the system name, system description, system capabilities, and port description.
12. Click the **Save** button.

    Your settings are saved.

Configure LLDP-MED interface settings

You can specify LLDP-MED settings that are applied to one or more interfaces.

To configure LLDP-MED 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Ports > LLDP > LLDP-MED Port Configuration**.

   The LLDP-MED 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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit LLDP-MED Port Configuration pop-up window displays.

8. From the **LLDP-MED Status** menu, select if LLDP-MED is enabled on the interface.
   - **Disabled**: LLDP-MED is disabled on the interface.
   - **Enabled**: LLDP-MED is enabled on the interface. This is the default setting.
9. From the **Notification** menu, select if the interface initiates traps for remote data changes:
   - **Disabled**: The interface does not initiate traps. This is the default setting.
   - **Enabled**: The interface initiates traps.
10. From the **MED Capabilities** menu, select if the interface transmits capabilities type length values (TLVs), which advertise the Intermediate System - Intermediate System (IS-IS) capabilities of the switch:
    - **Disabled**: The interface does not transmit capabilities TLVs.
    - **Enabled**: The interface transmits capabilities TLVs. This is the default setting.
11. From the **Network Policy** menu, select if the interface transmits network policy TLVs, which advertise network information such as information about VLANs:
    - **Disabled**: The interface does not transmit network policy TLVs.
    - **Enabled**: The interface transmits network policy TLVs. This is the default setting.
12. From the **Extended MDI-PSE** menu, select if the interface transmits extended media dependent interface (MDI) power sourcing equipment (PSE) TLVs, which advertise PoE information:
    - **Disabled**: The interface does not transmit extended MDI-PSE TLVs. This is the default setting.
    - **Enabled**: The interface transmits extended MDI-PSE TLVs.
13. Click the **Save** button.

    Your settings are saved.

Power over Ethernet

You can configure the global Power over Ethernet (PoE) configuration settings and the PoE settings for each port.

PoE concepts

Depending on the model, the port capacities and budgets are described in the following table.

Table 28. PoE port capacities and budgets

Model	Number of PoE+ Ports	Maximum Power Budget Across All Active PoE+ Ports	Maximum Power Per Individual Port
GS324TPv2	24	190W	30W (802.3at)
GS348TPv2	48	380W	30W (802.3at)

Supplied power is prioritized according to the port order, up to the total power budget of the device. Port 1 receives the highest PoE priority, while port 8 is relegated to the lowest PoE priority.

If the power requirements for attached powered devices (PDs) exceed the total power budget of the switch, the PoE power to the device on the highest-numbered active PoE port is disabled to make sure that the devices connected to the higher-priority, lower-numbered PoE ports are supported first.

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

The following table shows the standard power ranges, calculated with the maximum cable length of 328 feet (100 meters). If a device receives insufficient PoE power from the switch, consider using a shorter cable.

Table 29. PoE classes and PoE power allocations

Device Class	Compatible PoE Standard	Range of Power Delivered to the PD	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

Table 29. PoE classes and PoE power allocations (Continued)

Device Class	Compatible PoE Standard	Range of Power Delivered to the PD	Minimum Output at PoE Switch Port (Minimum Allocated)	Maximum Output at PoE Switch Port (Maximum Allocated)
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 concepts

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 concepts on page 168.)

To determine the power that a port delivers:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Ports > POE > POE**.

   The PoE Configuration page displays.

   In the PoE Port Configuration section, the power that a port delivers is stated in the Output Voltage (Volts) column.

Configure global PoE settings

You can configure global PoE settings that apply to the switch, as opposed to settings that apply to individual ports.

To configure 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Ports > POE > POE**.

   The POE page displays.
6. In the PoE Configuration section, click the check box for the PoE firmware version.
7. Click the **Edit** button.

   The Edit PoE Configuration pop-up window displays.
8. In the **System Usage Threshold** field, type a percentage number from 1 to 99 to set the threshold level at which a trap is sent if the consumed power exceeds the threshold power.

The default is 95 percent.

9. From the **Power Management mode** menu, select the power management algorithm that the switch uses to deliver power to the requesting PDs:
   - **Static**: Specifies that the power allocated for each port depends on the type of power threshold that is configured on the port.
   - **Dynamic**: Specifies that the power consumption on each port is measured and calculated in real time. This is the default setting.
10. To set the traps, in the PoE Trap Configuration section, select one of the following radio buttons:
    - **Enable**: Enables the transmission of PoE traps. This is the default setting.
    - **Disable**: Disables the transmission of PoE traps.
11. Click the **Save** button.

    Your settings are saved.

The following table describes the view-only fields in the PoE Configuration section.

Table 30. PoE configuration information

Field	Description
Firmware Version	The firmware version of the PoE software
Power Status	The power status
Total Power Available (Watts)	The maximum power in watts that the switch can deliver to all ports
Threshold Power (Watts)	If the consumed power is below the threshold power, the switch can power up another port. The consumed power can be between the nominal and threshold power. The threshold power is displayed in watts. **Note**: The threshold power value is determined by the value that you enter in the System Usage Threshold field.
Consumed Power (Watts)	Total power in watts that is being delivered to all ports

Configure PoE settings for the ports

To configure PoE settings for the 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Ports > POE > POE**.

   The POE page displays.

   The following steps refer to the PoE Port Configuration section on the page.
6. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the interface, or type the interface number (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit PoE Port Configuration pop-up window displays.
8. From the **Port Power** menu, select the administrative PoE mode of the port:
   - **Enable**: The port's capacity to deliver power is enabled. This is the default setting.
   - **Disable**: The port's capacity to deliver power is disabled.
9. From the **Port Priority** menu, select the priority for the port in relation to other ports if the total power that the switch is capable of delivering exceeds the total power budget:
   - **Low**: Low priority. This is the default setting.
   - **Medium**: Medium priority.
   - **High**: High priority.
   - **Critical**: Critical priority.

   The port priority determines which ports can still deliver power after the total power delivered by the switch exceeds the total power budget. (In such a situation, the

switch might not be able to deliver power to all connected devices.) If the same priority applies to two ports, the lower-numbered port receives higher priority.

10. From the **Power Mode** menu, select the PoE mode that the port must function in:

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

    Note: The Power Limit (mW) menu is masked because the limit is set at the port's maximum capacity.

11. From the **Power Limit Type** menu, select how the port controls the maximum power that it can deliver:

    - **None**: The port draws up to Class 0 maximum power in low power mode and up to Class 4 maximum power in high power mode.
    - **Class**: The port power limit is equal to the class of the attached PD.
    - **User**: The port power limit is equal to the value that you specify in the **Power Limit (mW)** field. This is the default setting.

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

12. If you select **User** from the **Power Limit Type** menu, in the **Power Limit (mW)** field, type the maximum power limit in milliwatt.
13. From the **Detection Type** menu, select how the port detects the attached PD:

- **IEEE 802**: The port performs a 4-point resistive detection. This is the default setting.
- **4ptdotaf+legacy**: The port performs a 4-point resistive detection, and if required, continues with legacy detection.
- **Legacy**: The port performs legacy detection.

14. From the **Longer Detection Time** menu, if PD is not powering up correctly, enable this option for devices that require a longer detection time (DC disconnects with 500ms delay):
    - **Enable**: A longer detection time is enabled.
    - **Disable**: A longer detection time is disabled. This is the default setting.
15. From the **Timer Schedule** menu, select a timer schedule or select **None**, which is the default selection.

    For information about setting up and configuring PoE timer schedules, see PoE timer schedules on page 175.
16. Click the **Save** button.

    Your settings are saved.

The following table describes the view-only fields on the page.

Table 31. PoE port information

Field	Description
High Power	All ports supports high power mode
Max Power (mW)	The maximum power in milliwatts (mW) that can be provided by the port
Class	The class defines the range of power that a powered device (PD) is drawing from the switch. The class definitions are as follows: • **0**: 0.44W–16.2W • **1**: 0.44W–4.2W • **2**: 0.44W–7.4W • **3**: 0.44W–16.2W • **4**: 0.44W–31.6W • **Unknown**: The class cannot be detected, or no PD is attached to the port
Output Voltage (Volts)	The voltage that is delivered to the PD in volts

Power cycle PoE ports

You can power-cycle one or more PoE ports to forcibly reset the PoE delivery of the ports.

To power cycle 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Ports > POE > POE**.

   The PoE 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 (for example, g3) in the **Search** 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. Click the **Power Cycle Port(s)** button.

   PoE is reset on the selected ports.

PoE timer schedules

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

After you create a timer schedule, you can associate it with one or more PoE ports (see Configure PoE settings for the ports on page 171). You can also use a separate timer schedule for each PoE port.

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

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

Add a new PoE timer schedule with an absolute entry or add a new absolute entry to an existing timer schedule

An absolute PoE timer schedule applies to specific dates and times. The schedule does not recur.

Note: A timer schedule can contain both absolute and periodic entries.

To add a new PoE timer schedule with a periodic entry or add a new periodic entry to an existing 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Ports > POE > Timer Schedule**.

   The Timer Schedule page displays.
6. Click the **Add New** button.

   The Add Timer Schedule pop-up window displays.

7. Do one of the following:
   - **Add a new timer schedule**: Do the following:
     a. From the **Name** menu, select **New Entry**.
     b. In the **New Entry** field, type a name for the timer schedule.

        The name can be a maximum of 31 characters.
   - **Add a new entry to an existing timer schedule**: From the **Name** menu, select the name of the existing timer schedule.

   The following steps add an entry to the timer schedule.
8. From the **Type** menu, select **Absolute**.

   The default setting is Absolute.
9. Click in the **Start Date** field to display the pop-up calendar, and select the date on which the schedule must start.
10. In the **Start Time** field, type the time (minutes and seconds, separated by a colon) at which the schedule must start, and then click the **AM** or **PM** button.
11. Click in the **End Date** field to display the pop-up calendar, and select the date on which the schedule must end.
12. In the **End Time** field, type the time (minutes and seconds, separated by a colon) at which the schedule must end, and then click the **AM** or **PM** button.
13. Click the **Save** button.

    Your settings are saved.

    Either the new timer schedule and entry are added to the Timer Schedule table, or the new *entry* is added to the existing timer schedule in the Timer Schedule table.

Add a new PoE timer schedule with a periodic entry or add a new periodic entry to an existing timer schedule

A periodic PoE timer schedule recurs on a daily, weekly, or monthly basis.

Note: A timer schedule can contain both periodic and absolute entries.

To add a new PoE timer schedule with a periodic entry or add a new periodic entry to an existing 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Ports > POE > Timer Schedule**.

   The Timer Schedule page displays.
6. Click the **Add New** button.

   The Add Timer Schedule pop-up window displays.
7. Do one of the following:
   - **Add a new timer schedule**: Do the following:
     a. From the **Name** menu, select **New Entry**.
     b. In the **New Entry** field, type a name for the timer schedule.

        The name can be a maximum of 31 characters.
   - **Add a new entry to an existing timer schedule**: From the **Name** menu, select the name of the existing timer schedule.

   The following steps add an entry to the timer schedule.
8. From the **Type** menu, select **Periodic**.

   The window adjusts.
9. Click in the **Date Start** field to display the pop-up calendar, and select the date on which the schedule must start.
10. In the **Time Start** field, type the time (minutes and seconds, separated by a colon) at which the schedule must start, and then click the **AM** or **PM** button.
11. Optionally, to set an end date for the schedule, do the following:
    a. Click the **Date End** toggle so that the toggle displays purple and is positioned at the right.

       By default, the Date End toggle display gray and is positioned at the left, the Date End field is masked, and the periodic schedule continues indefinitely.
    b. Click in the **Date End** field to display the pop-up calendar, and select the date on which the schedule must end.

12. In the **Time End** field, type the time (minutes and seconds, separated by a colon) at which the schedule must end, and then click the **AM** or **PM** button.
13. From the **Recurrence Pattern** menu, select the pattern:
    - **Daily**: The timer schedule works with daily recurrence.

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

      In the latter case, the schedule is triggered every specified number of days. If the number of days is not specified, or if you enter 0, then the schedule is triggered only once.
    - **Weekly**: The timer schedule works with weekly recurrence. The fields adjust.

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

      Select a single **Week Day** check box, multiple check boxes, or all check boxes to specify the day or days of the week that the schedule must operate.
    - **Monthly**: The timer schedule works with monthly recurrence. The fields adjust.

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

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

    Your settings are saved.

    Either the new timer schedule and entry are added to the Timer Schedule table, or the new *entry* is added to the existing timer schedule in the Timer Schedule table.

Change the settings for an entry of a timer schedule

You can change the settings for an existing timer schedule entry.

To change the settings for an entry of a 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Ports > POE > Timer Schedule**.

   The Timer Schedule page displays.
6. Click the name of the timer schedule to which the existing entry is associated.

   The name of the timer schedule is a hyperlink.

   The entries that are associated with the timer schedule display.
7. Select the check box for the entry.

   The entries are identified by an ID number. An absolute (continuous) entry and a periodic entry can receive the same ID number because the timer schedule tracks continuous and periodic entries separately.
8. Click the **Edit** button.

   The Edit Timer Schedule pop-up window displays.
9. Change the settings as needed.

   For more information, see Add a new PoE timer schedule with an absolute entry or add a new absolute entry to an existing timer schedule on page 176 or Add a new PoE timer schedule with a periodic entry or add a new periodic entry to an existing timer schedule on page 177, depending om the type of schedule that you are changing.
10. Click the **Save** button.

    Your settings are saved.

Remove an entry from a timer schedule

You can remove an entry from a timer schedule.

To remove an entry from a 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > Ports > POE > Timer Schedule**.

   The Timer Schedule page displays.

6. Click the name of the timer schedule to which the existing entry is associated.

   The name of the timer schedule is a hyperlink.

   The entries that are associated with the timer schedule display.

7. Select the check box for the entry.

   The entries are identified by an ID number. An absolute (continuous) entry and a periodic entry can receive the same ID number because the timer schedule tracks continuous and periodic entries separately.

8. Click the **Delete** button.

   Your settings are saved and the entry is removed.

Remove a timer schedule

You can remove a timer schedule that you no longer need. When you do so, all entries that are associated with the timer schedule are also removed.

To remove a 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Ports > POE > Timer Schedule**.

   The Timer Schedule page displays.
6. Select the check box for the timer schedule.
7. Click the **Delete** button.

   Your settings are saved and the schedule is removed.

Green Ethernet settings

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

Configure the global green Ethernet settings

You can configure the global green Ethernet settings.

To configure the global 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Ports > Green Ethernet**.

   The Green Ethernet page displays.
6. Click the **Auto Power Down Mode** toggle:
   - **The toggle is gray and positioned to the left**: Auto Power Down Mode is disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: Auto Power Down Mode is enabled. If a port link is down, the underlying physical layer goes down for a short period and then checks for port link pulses again so that auto-negotiation remains possible. In this way, the switch saves power when no link partner is present for the port.
7. Click the **EEE Mode** toggle:
   - **The toggle is gray and positioned to the left**: Energy Efficient Ethernet (EEE) Mode is disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: EEE Mode is enabled. EEE combines the MAC address of a port with a family of physical layers that support operation in a low power mode. (EEE is defined by the IEEE 802.3az standard.) Lower power mode lets both the send and receive sides of the link 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.
8. Click the **Apply** button.

   Your settings are saved.

Configure green Ethernet interface settings

You can configure green Ethernet settings for individual interfaces.

To configure the green Ethernet interface settings:

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Ports > Green Ethernet**.

   The Green Ethernet page displays.

   The following steps refer to the Green Ethernet Interface Configuration section.
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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit Green Ethernet Interface Configuration pop-up window displays.
8. From the **Auto Power Down Mode** menu, select to enable or disable this option for the interface:
   - **Disable**: Auto Power Down Mode is disabled for the interface. This is the default setting.
   - **Enable**: Auto Power Down Mode is enabled for the interface. If the interface link is down, the underlying physical layer goes down for a short period and then checks for interface link pulses again so that auto-negotiation remains possible. In this way, the switch saves power when no link partner is present for the interface.
9. From the **EEE mode** menu, select to enable or disable this option for the interface:
   - **Disable**: EEE is disabled for the interface. This is the default setting.
   - **Enable**: EEE is enabled for the interface. EEE combines the MAC address of the interface with a family of physical layers that support operation in a low power mode. (EEE is defined by the IEEE 802.3az standard.) Lower power mode lets both the send and receive sides of the link 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.

10. Click the **Save** button.

    Your settings are saved.

Link aggregation groups

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

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

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

The switch supports 16 LAGs with names ch1 through ch16.

Configure a LAG

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

To configure the 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > LAG > LAG Configuration**.

   The LAG Configuration page display.
6. Select one or more LAGs (channels) by taking one of the following actions:

   - To configure a single LAG, select the check box associated with the LAG, or type the LAG number (for example, ch3) in the **Search** field and click the **Go** button.
   - 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. Click the **Edit** button.

   The Edit LAG Configuration pop-up window displays.
8. To change the default name of the LAG, in the **LAG Name** field, enter the name to be assigned to the LAG.

   By default, the names are ch1, ch2, ch3, and so on. You can enter a name of up to 15 characters.
9. In the **Description** field, enter an optional description for the LAG.

   A description is for identification only.
10. From the **Admin Mode** menu, select to enable or disable the administrative mode for the LAG.
    - **Disabled**: The LAG is administratively disabled. When the LAG is disabled, no traffic flows, and LACPDUs are dropped, but the links that form the LAG are not released.
    - **Enabled**: The LAG is administratively enabled. This is the default setting.
11. From the **Hash Mode** menu, select the hash mode (that is, the load-balancing mode) for the LAG:

    - **1 Src/Dest MAC, incoming port**: This mode uses the source and destination MAC addresses and incoming port that are associated with the packet. This is the default mode.
    - **2 Src/Dest IP and TCP/UDP Port fields**: This mode uses the source and destination IP addresses and the source and destination TCP or UDP port values that are associated with the packet.

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

12. From the **STP Mode** menu, select to enable or disable the Spanning Tree Protocol (STP) administrative mode for the LAG.
    - **Disable**: STP is disabled for the LAG.
    - **Enable**: STP is enabled for the LAG. This is the default setting.
13. From the **Link Trap** menu, select to enable or disable the transmission of a trap when the LAG link status changes.
    - **Disable**: No trap is sent when the LAG link status changes. This is the default setting.
    - **Enable**: A trap is sent when the LAG link status changes.
14. From the **LAG Type** menu, select to enable or disable the LAG as a static LAG.
    - **Static**: Disables Link Aggregation Control Protocol (LACP) on the LAG. You must configure the LAG manually on each device. This is the default setting.
    - **LACP**: Enables LACP on the LAG. If both devices support LACP, the LAG can be configured automatically between the devices.
15. Click the **Save** button.

    Your settings are saved.

The following table describes the view-only fields on the page.

Table 32. LAG configuration information

Field	Description
LAG ID	The LAG ID (l1, l2, l3, and so on)
Active Ports	The ports that are members of the LAG
LAG State	Indicates if the LAG link is up (Link Up) or down (Link Down)

Configure the port members for a LAG

You can configure a single LAG and add physical interfaces as members to the LAG.

To configure a single LAG and its 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > LAG > LAG Membership**.

   The LAG Membership page display.
6. From the **LAG ID** menu, select the LAG.
7. To change the default name of the LAG, in the **LAG Name** field, enter the name to be assigned to the LAG.

   By default, the names are ch1, ch2, ch3, and so on. You can enter a name of up to 15 characters.
8. In the Ports table, click each port that you want to make a member of the LAG.

   Selected ports display blue in the Ports table.
9. Click the **Apply** button.

   Your settings are saved.

   The Current members field displays the ports that are members of the selected LAG.

Set the LACP system priority

You can set the Link Aggregation Control Protocol (LACP) system priority that applies to all LAGs on the switch.

To set the LACP system priority:

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > LAG > LACP Configuration**.

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

   A higher value indicates a lower priority. You can change the value of the setting globally by setting a priority from 1 to 65535. The default priority is 32768.
7. Click the **Apply** button.

   Your settings are saved.

Set the LACP priority and time-out period for a port

You can set the Link Aggregation Control Protocol (LACP) priority LACP time-out period for a port.

To set the LACP priority and time-out period 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > LAG > LACP Configuration**.

   The LACP System Priority page display.

   The following steps refer to the LACP Port Priority section.
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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit LACP Port Priority pop-up window displays.
8. In the **LACP Priority** field, enter the LACP priority for the interface.

   The priority sets the interface's link aggregation priority relative to the device at the other end of the link on which link aggregation is enabled. A higher value indicates a lower priority. The range is 1 to 65535. The default priority is 128.
9. From the **Timeout** menu, select the time-out period for LACP:
   - **Long**: The time-out period is long. This is the default setting.
   - **Short**: The time-out period is short.

   If the switch does not receive a LACP protocol data unit (PDU) before the time-out period expires, the LAG is terminated.
10. Click the **Save** button.

    Your settings are saved.

Configure the port settings and maximum frame size

You can configure and display the information for the physical ports on the switch. Some settings that apply to physical ports do not apply to LAGs.

Note: If you change the autonegotiation, speed, or duplex mode for a physical port, the switch might be inaccessible for a number of seconds while the new settings take effect.

To configure and display the 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

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

   The Port Configuration page display.

6. To set the global frame size, in the **Frame Size** field, specify the maximum Ethernet frame size that any interface can support. The frame size includes Ethernet header, CRC, and payload.

   The range is from 1522 to 10000 bytes. The default maximum frame size is 1522 bytes. You cannot set the frame size for individual interfaces. The frame size is defined in IEEE 802.3 and calculated with the Layer 2 Ethernet frame and the optional IEEE 802.1Q VLAN/QoS tag.

7. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**All**).
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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit Port Configuration pop-up window displays.

10. In the **Description** field, enter an optional description for the port.

    A description is for identification only.

11. From the **Admin Mode** menu, select to enable or disable the administrative mode for the port.

    - **Disable**: The port is administratively disabled.
    - **Enable**: The port is administratively enabled. This is the default setting.

    For the port or LAG to participate in the network, you must select **Enable**.

12. To manually set the speed for the port, in the **Speed** field, type one of the following options:

    - **Auto**: The speed is set by the auto-negotiation process. This is the default setting..
    - **10MB Half duplex**: The speed is limited to 10 Mbits/second at half duplex operation.
    - **100MB Half duplex**: The speed is limited to 100 Mbits/second at half duplex operation.
    - **10MB Full duplex**: The speed is limited to 10 Mbits/second at full duplex operation.
    - **100MB Full duplex**: The speed is limited to 100 Mbits/second at full duplex operation.

    For you to set the auto-negotiation speed, the selection from the **Autonegotiation** menu must be **Enable**.

    Note: You can set the speed for Ethernet ports. For SFP ports, the speed is automatically detected and you cannot change it.

13. From the **Link Trap** menu, select to enable or disable the option to send a trap when the port or LAG link status changes.

    - **Disable**: No trap is sent when the port or LAG link status changes.
    - **Enable**: A trap is sent when the port or LAG link status changes. For ports, the default is Enable. For LAGs, the default is Disable.

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

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

      Flow control helps to prevent data loss when the port cannot keep up with the number of frames being switched. When you enable flow control, the switch can

send a pause frame to stop traffic on the port if the amount of memory used by the packets on the port exceeds a preconfigured threshold and responds to pause requests from partner devices. The paused port does not forward packets for the time that is specified in the pause frame. When the pause frame time elapses, or the utilization returns to a specified low threshold, the switch enables the port to again transmit frames. The switch also honors incoming pause frames by temporarily halting transmission.

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

15. Click the **Save** button.

    Your settings are saved.

The following table describes the view-only fields on the page.

Table 33. Port configuration information

Field	Description
Port Type	For normal ports this field is blank. Otherwise the possible values are: • **Trunk Member**: The port is a member of a link aggregation trunk. • **Mirrored**: The port is a mirrored port. • **Probe**: The port is a monitoring port.
Physical Status	The port speed and duplex mode
Link Status	Indicates if the port or LAG link is up or down
Frame Size	The maximum Ethernet frame size the interface supports in the range from 1522 to 10000. The default maximum frame size is 1522.
MAC Address	The MAC address that is assigned to the interface
PortList Bit Offset	The bit offset value that corresponds to the port when the MIB object type PortList is used to manage in SNMP. The PortList Bit Offset is identical to the interface number.
ifindex	The ifIndex of the interface table entry. The ifIndex is identical to the interface number.

Spanning Tree Protocol

The Spanning Tree Protocol (STP) provides a tree topology for any arrangement of network devices. STP also provides one path between end stations on a network, eliminating loops. STP (also referred to as “classic” STP) provides a single path between end stations, avoiding and eliminating loops. For information about configuring the

global STP settings for the switch, see Configure the global STP settings and display the STP status on page 194.

The switch support the following spanning tree versions:

- **CST**: Common STP. For information about configuring CST, see Configure the CST settings and display the MSTP status on page 196 and Configure the CST interface settings on page 198.
- **MSTP**: Multiple Spanning Tree Protocol (MSTP, also referred to as MST) supports multiple instances of spanning tree to efficiently channel VLAN traffic over different interfaces. For information about configuring MSTP, see Add an MST instance and display the MST status on page 204 and Configure and display the interface settings for an MST instance on page 207.

  Note: For more information about MSTP and a configuration example, see Multiple Spanning Tree Protocol on page 511.
- **RSTP**: Rapid STP. Each instance of the spanning tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree (RSTP), with slight modifications in the working but not the end effect (the main effect is the rapid transitioning of the port to the forwarding state). For information about RSTP, see Display the Rapid STP interface status on page 203.

  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 messages. These features are represented by the 'pointtopoint' and 'edgeport' parameters. MSTP is compatible with both RSTP and STP. It behaves in a way that is appropriate for STP and RSTP bridges. An MSTP bridge can be configured to behave entirely as an RSTP bridge or an STP bridge.

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

Configure the global STP settings and display the STP status

You can configure the Spanning Tree Protocol (STP) settings and display the STP status on the switch.

To configure the STP settings and display the STP status:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > STP > STP**.

   The STP page displays.

   In the Global Settings section, make sure that the **Spanning Tree State** toggle is purple and positioned to the right. This indicates that STP is enabled on the switch, which is the default setting.

6. If the **Spanning Tree State** toggle is gray and positioned to the left, which indicates that STP is disabled on the switch, click the **Spanning Tree State** toggle to enable the STP for the switch.

   The toggle is purple and positioned to the right.

7. Select one of the following radio buttons to set the STP operation mode:
   - **STP**: "Classic" Spanning Tree Protocol (STP).
   - **RSTP**: Rapid STP. This is the default setting.
   - **MSTP**: Multiple Spanning Tree Protocol (MSTP).
8. In the **Configuration Name** field either leave the default identifier or type a new identifier that is used to identify the configuration currently being used.

   The identifier can be up to 32 alphanumeric characters.

9. In the **Configuration Revision Level** field, either leave the default level value or type a new level value.

   The value can be between 0 and 65535. The default setting is 0.

10. To enable the forwarding of bridge protocol data units (BPDUs) while STP is disabled on the switch, click the **Forward BPDU while STP Disabled** toggle.

The toggle is purple and positioned to the right. By default, this setting is disabled, and the toggle is gray and positioned to the left.

11. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only fields on the page.

Table 34. STP configuration and status information

Field	Description
Global Settings	
Configuration Digest Key	The key that identifies the configuration currently being used
STP Status	
Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	The time in day, hour, minute, and 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	Indicates if a topology change is in progress on any port assigned to the CST: True or False
Designated Root	The bridge identifier of the root bridge. It is based on the bridge priority and the base MAC address of the bridge.
Root Path Cost	The path cost to the designated root for the CST
Root Port	The port through which the designated root for the CST is accessed
Max Age (secs)	The time in seconds that passes before a bridge port saves its configuration BPDU information. The default is 20 seconds.
Forward Delay (secs)	The derived value of the Root Port Bridge Forward Delay setting. The default is 15 seconds.
Hold Time (secs)	The minimum time in seconds between the transmission of configuration BPDUs. The default is 6 seconds.
CST Regional Root	The priority and base MAC address of the CST regional root
CST Path Cost	The path cost to the CST tree regional root

Configure the CST settings and display the MSTP status

You can configure common spanning tree (CST) and display the MSTP status on the switch.

To configure the CST settings and display the MSTP 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > STP > Common Settings > CST Configuration**.

   The CST Configuration page displays.

   The following steps refer to the CST Configuration section.

6. In the **Bridge Priority** field, specify the bridge priority value for the common spanning tree (CST) and common and internal spanning tree (CIST).

   The range is from 0 to 61440. The bridge priority is a multiple of 4096. The default priority is 32768.

   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. 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 a value between 0 and 4095, it is automatically set to 0.

7. In the **Bridge Max Age** field, specify the period in seconds that a bridge waits before implementing a topological change.

   The range is from 6 to 40 seconds, and the value must be less than or equal to the following: (2 * Bridge Forward Delay) – 1 and greater than or equal to 2 * (Bridge Hello Time +1).

   The default is 20 seconds.

   Note: The Bridge Hello Time (secs) field shows the fixed period in seconds that a root bridge waits between configuration messages. The fixed period is 2 seconds.

8. In the **Bridge Forward Delay** field, specify the period in seconds that a bridge remains in a listening and learning state before forwarding packets.

   The period is from 4 to 30 seconds, and the value must be greater than or equal to the following: (Bridge Max Age / 2) + 1.

   The default is 15 seconds.
9. In the **Spanning Tree Maximum Hops** field, specify the maximum number of bridge hops that the information for a particular CST instance can travel before being discarded.

   The range is from 6 to 40 hops. The default is 20 hops.
10. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only fields on the page.

Table 35. MSTP status information

Field	Description
MST ID	The MST instances (including the CST) and the corresponding VLAN IDs (VIDs) associated with each one of them
VID	The VIDs and the corresponding Filtering ID (FID) associated with each one of them
FID	The FIDs and the corresponding VIDs associated with each once of them

Configure the CST interface settings

You can configure a common spanning tree (CST) and internal spanning tree on a specific interface on the switch.

An interface can become diagnostically disabled (D-Disable) when a severe error condition occurs for DOT1S. The most common cause is when BPDU flooding occurs. The flooding criteria are such that DOT1S receives more than 15 BPDUs in a 3-second interval. (Other causes for a DOT1S D-Disable condition are very rare.)

To configure the CST 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > STP > Common Settings > CST Port Configuration**.

   The CST Port Configuration page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit CST Port Configuration pop-up window displays.
9. From the **STP Status** menu, select to enable or disable STP for the interface:
   - **Disabled**: STP is disabled for the interface.
   - **Enabled**: STP is enabled for the interface. This is the default setting.
10. From the **Fast Link** menu, select if the interface functions as an edge port within the CST:
    - **Disabled**: The interface does not function as an edge port. This is the default setting.
    - **Enabled**: The interface functions as an edge port.
11. From the **BPDU Filter** menu, select one of the following options:
    - **Disable**: The BPDU Filter feature is disabled, which is the default setting.
    - **Enable**: The BPDU Filter feature is enabled and applies to all operational edge ports. An edge port in an operational state connects to hosts that typically drop BPDUs. If an operational edge port receives a BPDU, it loses its operational status.

If a port on which BPDU filtering is enabled receives BPDUs, the port drops the BPDUs and remains operational.

12. From the **BPDU Forwarding** menu, select if Bridge Protocol Data Unit (BPDU) forwarding is enabled for the interface:
    - **Disabled**: The interface does not forward BPDUs. This is the default setting.
    - **Enabled**: The interface forwards BPDUs even when STP is disabled on the interface.
13. From the **BPDU Guard** menu, select one the following options:
    - **Disable**: The BPDU guard feature is disabled, which is the default setting.
    - **Enable**: The BPDU guard feature is enabled and enforces the STP domain borders to keep the active topology consistent and predictable. Switches behind edge ports on which STP BPDU guard is enabled do not affect the overall STP topology. At the reception of BPDUs, the port on which BPDU guard is enabled transitions into disabled state.
14. From the **Auto Edge** menu, select if the interface can become an edge port:
    - **Disabled**: The interface cannot become an edge port if it does not receive BPDUs for a period.
    - **Enabled**: The interface can become an edge port even if it does not receive BPDUs for a period. This is the default setting.
15. In the **Path Cost** field, type the path cost for the interface in the CIST.

    The value can be in the range from 1 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.
16. In the **Priority** field, type the priority for the interface in the CIST.

    The port priority is set in multiples of 16. For example if you attempt to set the priority to any value between 0 and 15, it is set to 0. If you try to set it to any value between 16 and (2*16 – 1), it is set to 16, and so on. The range is 0 to 240. The default value is 128.
17. In the **External Port Path Cost** field, type an external path cost for the interface in the CIST.

    The value can be in the range from 1 to 200000000. The default is 0.
18. Click the **Save** button.

    Your settings are saved.

The following table describes the view-only fields on the page.

Table 36. CST port configuration information

Field	Description
Port State	Indicates the current STP state of the interface. 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 interface. The interface forwards traffic while learning MAC addresses. • **Blocking**: The interface is currently blocked and cannot be used to forward traffic or learn MAC addresses. • **Listening**: The interface is currently in the listening mode. The interface cannot forward traffic nor can it learn MAC addresses. • **Learning**: The interface is currently in the learning mode. The interface cannot forward traffic. However, it can learn new MAC addresses. • **Forwarding**: The interface is currently in the forwarding mode. The interface can forward traffic and learn new MAC addresses • **Manual forwarding**: The interface is currently in the manual forwarding mode. The interface can forward traffic and learn new MAC addresses
Port ID	The port identifier for the interface in the CST. The identifier is based on the port priority and the interface number.
Hello Timer	The setting of the Hello Timer for the CST. By default, the setting is 2.

Display the CST interface status

You can display the Common Spanning Tree (CST) status information for interfaces on the switch.

To display the CST interface 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

The Dashboard page displays.

5. Select **Switching > STP > Common Settings > CST Port Status**.

   The CST Port Status page displays.

6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**All**).
7. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 37. CST interface status information

Field	Description
Interface	The physical interface or LAG that is associated with the CST
Port Role	Each MST bridge port that is enabled is assigned a port role for each spanning tree. The port role is one of the following: Root, Designated, Alternate, Backup, Master, or Disabled.
Designated Root	The root bridge for the CST, which is created from the bridge priority and the base MAC address of the bridge
Designated Cost	The path cost offered to the LAN by the designated port
Designated Bridge	The bridge identifier of the bridge with the designated port. This identifier is created from the bridge priority and the base MAC address of the bridge.
Designated Port	The port identifier on the designated bridge that offers the lowest cost to the LAN. This identifier is created from the port priority and the interface number of the port.
Topology Change Acknowledge	Indicates if the topology change acknowledgement flag is set for the next BPDU to be transmitted on the port (True or False)
Edge port	Indicates if the port is enabled as an edge port
Point-to-Point MAC	The point-to-point status, which indicates is the port's link is a point-to-point link (True) or not or (False)
CST Regional Root	The bridge identifier of the CST regional root. This identifier is created from the bridge priority and the base MAC address of the bridge.

Table 37. CST interface status information (Continued)

Field	Description
CST Path Cost	The path cost to the CST regional root
Port Forwarding State	Indicates the current STP state of the interface. 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 interface. The interface forwards traffic while learning MAC addresses. • **Blocking**: The interface is currently blocked and cannot be used to forward traffic or learn MAC addresses. • **Listening**: The interface is currently in the listening mode. The interface cannot forward traffic nor can it learn MAC addresses. • **Learning**. The interface is currently in the learning mode. The interface cannot forward traffic. However, it can learn new MAC addresses. • **Forwarding**: The interface is currently in the forwarding mode. The interface can forward traffic and learn new MAC addresses. • **Manual forwarding**: The interface is currently in the manual forwarding mode. The interface can forward traffic and learn new MAC addresses

Display the Rapid STP interface status

You can display the Rapid Spanning Tree (RSTP) status information for interfaces on the switch.

To display the RSTP interface 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > STP > RSTP**.

   The RSTP page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**All**).
7. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 38. RSTP interface status information

Field	Description
Interface	The physical interface or LAG that is associated with a VLAN that is 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, Designated, Alternate, Backup, Master, or Disabled.
Mode	The spanning tree operation mode: STP, RSTP, or MSTP
Fast Link	Indicates if the interface is enabled as an edge port
Status	Indicates the current state of the interface. 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 interface. The interface forwards traffic while learning MAC addresses. • **Blocking**: The interface is currently blocked and cannot be used to forward traffic or learn MAC addresses. • **Listening**: The interface is currently in the listening mode. The interface cannot forward traffic nor can it learn MAC addresses. • **Learning**. The interface is currently in the learning mode. The interface cannot forward traffic. However, it can learn new MAC addresses. • **Forwarding**: The interface is currently in the forwarding mode. The interface can forward traffic and learn new MAC addresses. • **Manual forwarding**: The interface is currently in the manual forwarding mode. The interface can forward traffic and learn new MAC addresses

Manage MST instances

You can add, change, or delete Multiple Spanning Tree (MST) instances on the switch. The MST instance consists of an ID, a priority value, and a VLAN ID.

Add an MST instance and display the MST status

You can add an MST instance and display the MST status.

The configuration includes one preconfigured MST with ID 0 that includes all VLANs.

To add an MST instance and display the MST 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > STP > MSTP > MST Configuration**.

   The MST Configuration page displays.

6. Click the **Add New** button.

   The Add MST Configuration pop-up window displays.

7. In the **MST ID** field, type the ID of the MST.

   The ID can be in the range from 1 to 4094.

8. In the **Priority** field, type the bridge priority value for the MST instance.

   When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if you set the priority to any value between 0 and 4095, the switch automatically sets the value to 0. The range is from 0 to 61440. The default is 32768.

9. From the **VLAN ID** menu, select the VLAN that must be associated with the MST instance.
10. Click the **Save** button.

    Your settings are saved and the MST is added.

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

    The following table describes the view-only fields on the page.

Table 39. MST configuration information

Field	Description
Bridge Identifier	The bridge identifier for the MST instance, which is created by using the bridge priority and the base MAC address of the bridge
Last TCN	The time in seconds since the topology of the MST instance changed
Topology Change Count	The number of times the topology changed for the MST instance
Topology Change	This field shows if a topology change is in progress on an interface in the MST (True or False)
Designated Root	The bridge identifier of the root bridge, which is created by using the bridge priority and the base MAC address of the bridge
Root Path Cost	The path cost to the designated root for the MST instance
Root Port	The port through which the designated root for the MST instance can be accessed

Change an MST instance

You can change an existing MST instance.

To change an existing 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > STP > MSTP > MST Configuration**.

   The MST Configuration page displays.
6. Select the check box that is associated with the MST instance.
7. Click the **Edit** button.

   The Edit MST Configuration pop-up window displays.

8. Change the settings as needed.

   For more information, see Add an MST instance and display the MST status on page 204.

9. Click the **Save** button.

   Your settings are saved.

Delete an MST instance

You can delete an MST instance that you no longer need.

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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > STP > MSTP > MST Configuration**.

   The MST Configuration page displays.

6. Select the check box that is associated with the MST instance.
7. Click the **Delete** button.

   The MST instance is deleted.

Configure and display the interface settings for an MST instance

You can configure and display the interface settings for a Multiple Spanning Tree (MST) instance.

To configure and display the interface settings for an MST instance:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > STP > MSTP > MST Port Configuration**.

   The MST Port Configuration page displays.
6. From the **Select MST** menu, select an MST instance.

   For information about adding MST instances, see Add an MST instance and display the MST status on page 204.
7. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**All**).
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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit MST Port Configuration pop-up window displays.
10. In the **Port Priority** field, type the priority for the interface in the MST instance.

    The port priority is set in multiples of 16. If you specify a value that is not a multiple of 16, the priority is automatically set to the next lowest priority that is a multiple of 16. For example, if you set a value between 0 and 15, the priority is set to 0. If you

specify a number between 16 and 31, the priority is set to 16. Specify a value in the range from 0 to 240. The default is 128.

11. In the **Port Path Cost** field, type the path cost in the range from 0 to 200000000.

    The default cost depends on the interface.

12. Click the **Save** button.

    Your settings are saved.

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

    The following table describes the view-only fields on the page.

Table 40. MST interface configuration information

Field	Description
Auto Calculated Port Path Cost	Indicates if the path cost is automatically calculated (Enable) or not (Disable). If enabled, the path cost is calculated based on the link speed of the port if the configured value for Port Path Cost is zero.
Port ID	The port identifier for the port in the MST instance, which is created by using the port priority and the interface number
Port Up Time Since Counters Last Cleared	The time since the counters were cleared
Port Mode	Indicates if STP is enabled for the interface
Port Forwarding State	The current STP state of the interface. 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 interface. The interface forwards traffic while learning MAC addresses. • **Blocking**: The interface is currently blocked and cannot be used to forward traffic or learn MAC addresses. • **Listening**: The interface is currently in the listening mode. The interface cannot forward traffic nor can it learn MAC addresses. • **Learning**: The interface is currently in the learning mode. The interface cannot forward traffic. However, it can learn new MAC addresses. • **Forwarding**: The interface is currently in the forwarding mode. The interface can forward traffic and learn new MAC addresses. • **Manual forwarding**: The interface is currently in the manual forwarding mode. The interface 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.
Designated Root	The bridge identifier of the root bridge, which is created by using the bridge priority and the base MAC address of the bridge
Designated Cost	The path cost offered to the LAN by the designated port

Table 40. MST interface configuration information (Continued)

Field	Description
Designated Bridge	The bridge identifier of the bridge with the designated port. This identifier is created from the bridge priority and the base MAC address of the bridge.
Designated Port	The port identifier on the designated bridge that offers the lowest cost to the LAN. This identifier is created from the port priority and the interface number of the port.

Display the STP interface statistics

You can display information about the number and type of bridge protocol data units (BPDUs) that are transmitted and received on each interface.

To display the STP interface 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > STP > STP Statistics**.

   The STP Statistics page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**All**).
7. To refresh the page, click the **Refresh** button.

   The following table describes the view-only fields on the page.

Table 41. STP interface statistics information

Field	Description
STP BPDUs Received	The number of STP BPDUs received on the interface
STP BPDUs Transmitted	The number of STP BPDUs transmitted from the interface
RSTP BPDUs Received	The number of RSTP BPDUs received on the interface
RSTP BPDUs Transmitted	The number of RSTP BPDUs transmitted from the interface
MSTP BPDUs Received	The number of MSTP BPDUs received on the interface
MSTP BPDUs Transmitted	The number of MSTP BPDUs transmitted from the interface

MAC address table

You can view or configure the MAC address table. This table contains information about static and dynamic unicast entries for which the switch holds forwarding or filtering information. This information lets the switch determine how an incoming frame must be propagated.

Set the dynamic MAC address aging interval

You can set the MAC address aging interval for the forwarding database. This is the time-out period in seconds for aging out dynamically learned forwarding information.

To set the dynamic MAC address aging interval:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

The Dashboard page displays.

5. Select **Switching > Address Table > Address Table**.

   The Address Table page displays.

6. In the **Address Aging Timeout** field, type the time-out period in seconds for aging out dynamically learned forwarding information.

   The period is from 10 to 1000000 seconds. The default is 300 seconds.

7. Click the **Apply** button.

   Your settings are saved.

View, search, or clear the MAC address table

If you clear the MAC address entries in the MAC address table, only the dynamic entries are removed.

To view, search, or clear the MAC address table:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > Address Table > Address Table**.

   The Address Table page displays.

6. From the **VLAN ID** menu, select how you want to perform a search, and in the **Search** field, enter the information associated with your search option:

- **VLAN ID**: In the **Search** field, enter the VLAN ID, for example, 100. Then, click the **Go** button.
- **MAC Address**: In the **Search** field, enter the 6-byte hexadecimal MAC address in two-digit groups separated by colons, for example, 01:23:45:67:89:AB. Then click the **Go** button.

  If the address exists, that entry is displayed as the first entry followed by the remaining (higher) MAC addresses. An exact match is required.
- **Interface**: In the **Search** field, enter the interface ID using the interface naming convention (for example, g5). Then, click the **Go** button.

7. To remove the dynamic entries from the MAC address table, click the **Clear** button.
8. To refresh the page, click the **Refresh** button.

   The following table describes the view-only fields on the page.

Table 42. MAC address table information

Field	Description
VLAN ID	The VLAN ID associated with the MAC address
MAC Address	The unicast MAC address for which the switch holds forwarding information, filtering information, or both forwarding and filtering information. The format is a 6-byte MAC address that is separated by colons, for example 01:23:45:67:89:AB. The table header for the MAC Address column shows the total number of MAC addresses in the table.
Interface	The interface on which the address was learned
Status	The status of this entry: • **Static**: The MAC address was added by the switch or a user and cannot be relearned • **Learned**: The MAC address was learned, and is being used • **Management**: The management MAC address

Add a static MAC address to the MAC address table

Static MAC address entries are the ones that you manually add to the MAC address table for a specific interface and VLAN.

To add a static MAC address to the MAC address table:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Address Table > Static MAC Address**.

   The Static MAC Address page displays.
6. From the **Interface** menu, select the interface or LAG.
7. Click the **Add New** button.

   The Add Static MAC Address pop-up window displays.
8. In the **Static MAC Address** field, type the MAC address.

   The MAC address must be in the 00:11:22:33:44:55 format.
9. From the **VLAN ID** menu, select the VLAN ID that must be associated with the MAC address.
10. Click the **Save** button.

    Your settings are saved and the static MAC address is added to the MAC address table.

Remove a static MAC address from the MAC address table

You can remove a static MAC address that you no longer need.

To remove a static MAC address from 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Address Table > Static MAC Address**.

   The Static MAC Address page displays.
6. From the **Interface** menu, select the interface or LAG.
7. Select the check box for the MAC address.
8. Click the **Delete** button.

   The static MAC address is removed from the MAC address table.

DHCP snooping

DHCP snooping is a 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 correspond 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 messages only from within the network.

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

Enable DHCP snooping for the switch

You can globally enable DHCP snooping for the switch.

To globally enable DHCP snooping for 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The Global Configuration page displays.
6. Click the **DHCP Snooping Mode** toggle:
   - **The toggle is gray and positioned to the left**: The DHCP Snooping Mode is globally disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: The DHCP Snooping Mode is globally enabled.
7. Click the **MAC Address Validation** toggle:
   - **The toggle is gray and positioned to the left**: MAC address validation is disabled.
   - **The toggle is purple and positioned to the right**: MAC address validation is enabled. This is the default setting.

     When MAC address validation is enabled, the switch 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 switch drops the packet.
8. Click the **Apply** button.

   Your settings are saved.

Enable DHCP snooping for a VLAN

To enable DHCP 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The Global Configuration page displays.

   The following steps refer to the VLAN Configuration section.
6. Select the check box for the VLAN.
7. Click the **Edit** button.

   The Edit VLAN Configuration pop-up window displays.
8. From the **DHCP Snooping Mode** menu, select the DHCP snooping mode for the VLAN:
   - **Disable**: DHCP snooping is disabled for the VLAN. This is the default setting.
   - **Enable**: DHCP snooping is enabled for the VLAN.
9. Click the **Save** button.

   Your settings are saved.

Configure DHCP snooping interface settings

You can display 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The Interface Configuration page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit DHCP Snooping Interface Configuration pop-up window displays.
9. From the **Trust Mode** menu, select the trust mode:
   - **Disabled**: The interface is considered to be untrusted and could potentially be used to launch a network attack. This is the default setting.

     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 are dropped.
  - DHCP messages are dropped if the MAC address is in the snooping database but the binding's interface is different from the interface where the message was received.
  - DHCP packets are dropped if the source MAC address does not match the client hardware address and if MAC address validation is globally enabled.
- **Enabled**: The interface is considered to be trusted and forwards DHCP server messages without validation.

10. From the **Invalid Packets** menu, select the packet logging mode:
    - **Disabled**: DHCP snooping does not generate log messages. This is the default setting.
    - **Enabled**: DHCP snooping generates a log message when an invalid packet is received and dropped by the interface.
11. In the **Rate Limit (pps)** field, type the rate limit value for DHCP snooping purposes.

    If the incoming rate of DHCP packets per second exceeds the configured burst interval per second, the port shuts down. If the rate limit is None (which is the default), the burst interval is also not applicable, and rate limiting is disabled.
12. In the **Burst Interval (secs)** field, type the burst interval in seconds for rate limiting on the interface.

    If the rate limit is N/A, the burst interval is not applicable.
13. Click the **Save** button.

    Your settings are saved.

Add a static DHCP snooping binding

You can add a static binding to the DHCP snooping bindings database.

To add a static DHCP snooping binding:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

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

   The Binding Configuration page displays.
6. In the Static Binding Configuration section, click the **Add New** button.

   The Add Static Binding Configuration pop-up window displays.
7. From the **Interface** menu, select the interface.
8. In the **MAC Address** field, type the MAC address for the binding to be added.

   This is the key to the binding database.
9. From the **VLAN ID** menu, select the ID of the VLAN.
10. In the **IP Address** field, type the IP address for the binding to be added.
11. Click the **Save** button.

    Your settings are saved. The DHCP snooping binding entry is added to the database.

Remove a static DHCP snooping binding

You can remove a static binding from the DHCP snooping bindings database.

To remove a static DHCP snooping binding:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

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

   The Binding Configuration page displays.
6. In the Static Binding Configuration table, select the check box for the static binding.
7. Click the **Delete** button.

   The DHCP snooping binding entry is removed from the database.

Configure DHCP snooping persistent settings

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

To configure DHCP snooping persistent settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

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

   The Persistent Configuration page displays.
6. Select where the DHCP snooping bindings database is located.
   - **Local**: The binding table is stored locally on the switch.
   - **Remote**: The binding table is stored on a remote TFTP server.

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

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

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

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

8. Click the **Apply** button.

   Your settings are saved.

Display the DHCP snooping statistics

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

To display the DHCP snooping statistics:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

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

   The DHCP Snooping Statistics page displays.

6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**All**).
7. To refresh the page, click the **Refresh** button.

The following table describes the DHCP snooping statistics.

Table 43. DHCP Snooping Statistics information

Field	Description
Interface	The interface for which statistics are displayed
MAC Verify Failures	The number of DHCP messages that were dropped because the source MAC address and client hardware address did not match. MAC address verification is performed only if it is globally enabled.
Client Ifc Mismatch	The number of packets that were dropped by DHCP snooping because the interface and VLAN on which the packet was received do not match the client's interface and VLAN information stored in the binding database
DHCP Server Messages	The number of DHCP server messages that were dropped on an untrusted port

DHCP Layer 2 relay

If you enable and configure a DHCP relay agent on the switch, some Layer 2 (L2) devices do not need to connect to a DHCP server on the physical network. A relay agent automatically populates the gateway IP address (giaddr) field and adds the Relay Agent Information option to DHCP messages. A DHCP server uses this option for IP addresses and other assignment policies. A DHCP relay agent is usually an IP routing-aware device, which is also referred to as a Layer 3 relay agent. In some network configurations, L2 devices must append the Relay Agent Information option because they are closer to the end hosts.

An L2 device can operate as a bridge only for a network and might not include an IPv4 address on the network. If an L2 device lacks an IPv4 source address, the device cannot relay packets directly to a DHCP server that is located on another network. In that situation, the L2 device can append the Relay Agent Information option and broadcast the DHCP message.

Configure the global DHCP L2 relay settings

To configure the global DHCP L2 relay 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > DHCP Services > DHCP L2 Relay > DHCP L2 Relay Global Configuration**.

   The DHCP L2 Relay Global Configuration page displays.
6. Click the **Admin Mode** toggle:
   - **The toggle is gray and positioned to the left**: DHCP L2 Relay is globally disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: DHCP L2 Relay is globally enabled.
7. Click the **Apply** button.

   Your settings are saved.

Configure the DHCP L2 relay VLAN settings

You can enable or disable the DHCP L2 relay VLAN settings and circuit ID suboption of DHCP Option-82, and set a remote ID string.

To configure the DHCP L2 relay 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > DHCP Services > DHCP L2 Relay > DHCP L2 Relay Global Configuration**.

   The DHCP L2 Relay Global Configuration page displays.

   The following steps refer to the DHCP L2 Relay VLAN Configuration section.
6. Select the check box for the VLAN.
7. Click the **Edit** button.

   The Edit DHCP L2 Relay VLAN Configuration pop-up window displays.
8. From the **Admin Mode** menu, select the DHCP L2 relay mode for the VLAN:
   - **Disabled**: DHCP L2 relay is disabled for the VLAN.
   - **Enabled**: DHCP L2 relay is enabled for the VLAN. This is the default setting.
9. From the **Circuit ID Mode** menu, select the circuit ID option for the VLAN:
   - **Disabled**: The circuit ID suboption of DHCP Option-82 is disabled for the VLAN. This is the default setting.
   - **Enabled**: The circuit ID suboption of DHCP Option-82 is enabled for the VLAN.
10. In the **Remote ID String** field, type the remote ID.

    The remote ID applies if the circuit ID suboption is enabled.
11. Click the **Save** button.

    Your settings are saved.

Configure a DHCP L2 relay interface

You can enable a DHCP L2 relay on an interface.

To configure DHCP L2 relay 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > DHCP Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration**.

   The DHCP L2 Relay Interface Configuration page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit DHCP L2 Relay Configuration pop-up window displays.
9. From the **Admin Mode** menu, select the DHCP L2 relay mode for the interface:
   - **Disabled**: DHCP L2 relay is disabled for the interface.
   - **Enabled**: DHCP L2 relay is enabled for the interface. This is the default setting.
10. From the **82 Option Trust Mode** menu, select to enable or disable the interface as a trusted interface for the Relay Agent Information option (Option 82):
    - **Disabled**: The interface is not a trusted interface. This is the default setting.
    - **Enabled**: The interface is a trusted interface
11. Click the **Save** button.

    Your settings are saved.

Display or clear the DHCP L2 relay interface statistics

To display or clear the DHCP L2 relay interface 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > DHCP Services > DHCP L2 Relay > DHCP L2 Relay Interface Statistics**.

   The DHCP L2 Relay Interface Statistics page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**All**).
7. To clear the statistics, click the **Clear** button.
8. To refresh the information on the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 44. DHCP L2 relay interface statistics information

Field	Description
Interface	The interface from which the DHCP message is received
Untrusted Server Messages With Opt82	The number of DHCP messages with Option 82 received from an untrusted server
Untrusted Client Messages With Opt82	The number of DHCP messages with Option 82 received from an untrusted client

Table 44. DHCP L2 relay interface statistics information (Continued)

Field	Description
Trusted Server Messages Without Opt82	The number of DHCP messages without Option 82 received from a trusted server
Trusted Client Messages Without Opt82	The number of DHCP messages without Option 82 received from a trusted client

Dynamic ARP inspection

Dynamic ARP inspection (DAI) is a security feature that rejects invalid and malicious Address Resolution Protocol (ARP) packets. DAI prevents a class of man-in-the-middle attacks where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The unfriendly station sends ARP requests or responses mapping another station's IP address to its own MAC address.

DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a bindings database of valid MAC addresses, IP addresses, VLAN interfaces, and so on.

If DAI is enabled and if a sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database, the switch drops the ARP packet. However, you can also create static mappings in the DHCP snooping bindings database. Static mappings are useful when hosts configure static IP addresses, the switch cannot run DHCP snooping, or other switches in the network do not run dynamic ARP inspection. A static mapping associates an IP address to a MAC address on a VLAN.

You can configure DAI VLANs, interfaces, and access control lists (ACLs) with associated rules.

Configure the global DAI settings

You can configure the global dynamic ARP inspection (DAI) settings.

To configure the global DAI 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Dynamic ARP Inspection > DAI Configuration**.

   The DAI Configuration page displays.
6. Click the **Validate Source MAC** toggle to set the source MAC validation mode for the switch:
   - **The toggle is gray and positioned to the left**: Source MAC addresses are not validated. This is the default setting.
   - **The toggle is purple and positioned to the right**: Source MAC addresses are validated for ARP packets.
7. Click the **Validate Destination MAC** toggle to set the destination MAC validation mode for the switch:
   - **The toggle is gray and positioned to the left**: Destination MAC addresses are not validated. This is the default setting.
   - **The toggle is purple and positioned to the right**: Destination MAC addresses are validated for ARP packets.
8. Click the **Validate IP** toggle to set the IP validation mode for the switch:
   - **The toggle is gray and positioned to the left**: IP addresses are not validated for the switch. This is the default setting.
   - **The toggle is purple and positioned to the right**: IP addresses are validated for ARP packets.
9. Click the **Apply** button.

   Your settings are saved.

Configure DAI VLANs

You can configure one or more dynamic ARP inspection (DAI) VLANs.

To configure a DAI 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > Dynamic ARP Inspection > DAI VLAN Configuration**.

   The DAI VLAN Configuration page displays.

6. Select the check box for the VLAN.
7. Click the **Edit** button.

   The Edit VLAN Configuration pop-up window displays.

8. From the **Admin Mode** menu, select the DAI mode for the VLAN.
   - **Disabled**: DAI is disabled for the VLAN. This is the default setting.
   - **Enabled**: DAI is enabled for the VLAN.
9. From the **Invalid Packets** menu, select if DAI logging is enabled for the VLAN:
   - **Disabled**: Logging of invalid ARP packets is disabled for the VLAN.
   - **Enabled**: Logging of invalid ARP packets is enabled for the VLAN. This is the default setting.
10. In the **ARP ACL Name** field, type a name of an existing ARP ACL (see Add a DAI access control list on page 232).

    The ARP ACL is used for ARP packet validation. To remove an existing ARP ACL name from the **ARP ACL Name** field, enter **N/A**.

11. From the **Static Flag** menu, select if an ARP packet must be validated using the DHCP snooping database if the ARP ACL rule does not match.
    - **Disabled**: An ARP packet is validated by the ARP ACL rule only. This is the default setting.
    - **Enabled**: An ARP packet is validated by the ARP ACL rule. If further validation is required, the ARP packet is validated using the DHCP snooping database.
12. Click the **Save** button.

Your settings are saved.

Configure a DAI interface

You can configure one or more dynamic ARP inspection (DAI) interfaces.

To configure a DAI 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Dynamic ARP Inspection > DAI Interface Configuration**.

   The DAI Interface Configuration page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit DAI Interface Configuration pop-up window displays.
9. From the **Trust Mode** menu, specify if the interface is trusted for DAI.

- **Disabled**: The interface is not trusted and ARP packets entering the interface are subjected to DAI. This is the default setting.
- **Enabled**: The interface is trusted and ARP packets entering the interface are forwarded without checking.

10. In the **Rate Limit (pps)** field, type the rate limit value for DAI.

    If the incoming rate of ARP packets exceeds the specified value for consecutive burst interval seconds, ARP packets are dropped. If you specify N/A, no limit exists. The range is from 0 to 300. The default is 15 packets per second (pps).

11. In the **Burst Interval (secs)** field, type the burst interval value for rate limiting on the interface.

    If you specify N/A, the burst interval is not effective. The range is from 1 to 15. The default is 1 second.

12. Click the **Save** button.

    Your settings are saved.

DAI ACLs

DAI relies on the information in the DHCP snooping bindings database to validate ARP packets. When hosts use static IP addresses, the DHCP snooping feature cannot build a bindings database. For networks that use static IP addresses and do not use DHCP, you can use DAI access control lists (ACLs) to statically map an IP address to a MAC address on a VLAN. DAI ACLs are also useful when other switches in the network do not use DAI.

DAI consults the static mappings configured in the DAI ACLs before it consults the DHCP snooping bindings database. In this way, static mappings receive precedence over DHCP snooping bindings. If the static flag is enabled on a VLAN, DAI consults the DAI ACL only and does not validate ARP information against the DHCP snooping bindings database.

Add a DAI access control list

You can add a dynamic ARP inspection (DAI) access control list (ACL) to which you then can add rules.

To add a DAI 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > Dynamic ARP Inspection > DAI ACL/Rule Configuration**.

   The DAI ACL/Rule Configuration page displays.

6. Click the **Add New** button.

   The Add DAI ACL/Rule Configuration pop-up window displays.

7. Select the **Add New ACL only** radio button.

   The window adjusts.

8. In the **Name** field, type a name of up to 31 characters.
9. Click the **Save** button.

   Your settings are saved and the DAI ACL is added.

Configure a rule for an existing DAI ACL

After you add a DAI ACL (see Add a DAI access control list on page 232), you can configure a rule for it. A DAI ACL rule consists of a binding between an IP address and a MAC address.

To configure a rule for an existing DAI 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Dynamic ARP Inspection > DAI ACL/Rule Configuration**.

   The DAI ACL/Rule Configuration page displays.
6. Click the **Add New** button.

   The Add DAI ACL/Rule Configuration pop-up window displays.
7. Select the **Add a Rule to an existing ACL** radio button.

   The window adjusts.
8. From the **Name** menu, select the DAI ACL for which you want to configure the rule.
9. In the **Source IP Address** field, type the source IP address that must be used as a match for the rule.
10. In the **Source MAC Address** field, type the source MAC address that must be used as a match for the rule.
11. Click the **Save** button.

    Your settings are saved and the rule is added.

Remove a rule from a DAI ACL

You can remove a rule from a DAI ACL if you no longer need the rule. When you remove a rule, the rule is deleted.

To remove a rule from a DAI 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Dynamic ARP Inspection > DAI ACL/Rule Configuration**.

   The DAI ACL/Rule Configuration page displays.
6. Click the name of the DAI ACL with which the rule is associated.

   The name of the DAI ACL is a hyperlink.

   The rules that are associated with the DAI ACL display.
7. Select the check box for the rule.
8. Click the **Delete** button.

   Your settings are saved and the rule is removed.

Remove a DAI access control list

You can delete a dynamic ARP inspection (DAI) access control list (ACL) that you no longer need. All rules that are associated with the ACL are also removed.

To remove a DAI 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Dynamic ARP Inspection > DAI ACL/Rule Configuration**.

   The DAI ACL/Rule Configuration page displays.
6. Select the check box for the ACL name.
7. Click the **Delete** button.

Your settings are saved and the DAI ACL is removed.

Display the DAI statistics

To display the DAI 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Dynamic ARP Inspection > DAI Statistics**.

   The DAI Statistics page displays.
6. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 45. DAI Statistics information

Field	Description
VLAN ID	The VLAN ID
DHCP Drops	The number of ARP packets that were dropped by DAI because no matching DHCP snooping binding entry exists
DHCP Permits	The number of ARP packets that were forwarded by DAI because a matching DHCP snooping binding entry exists
ACL Drops	The number of ARP packets that were dropped by DAI because no matching ARP ACL rule exists for the VLAN and the static flag is set on the VLAN
ACL Permits	The number of ARP packets that were permitted by DAI because a matching ARP ACL rule exists for the VLAN
Bad Source MAC	The number of ARP packets that were dropped by DAI because the sender MAC address in the ARP packets did not match the source MAC address in the Ethernet header

Table 45. DAI Statistics information (Continued)

Field	Description
Bad Dest MAC	The number of ARP packets that were dropped by DAI because the target MAC address in the ARP reply packets did not match the destination MAC address in the Ethernet header
Invalid IP	The number of ARP packets that were dropped by DAI because the sender IP address in the ARP packets or the target IP address in the ARP reply packets is invalid. Invalid addresses include 0.0.0.0, 255.255.255.255, IP multicast addresses, class E addresses (240.0.0.0/4), and loopback addresses (127.0.0.0/8).
Forwarded	The number of valid ARP packets forwarded by DAI
Dropped	The number of invalid ARP packets dropped by DAI

5

Configure Multicast

This chapter covers the following topics:

- Display the entries in the multicast forwarding database
- Display the multicast forwarding database statistics
- Internet Group Management Protocol snooping
- IGMP snooping querier overview
- Multicast Listener Discovery snooping
- MLD snooping querier overview
- Multicast VLAN registration

Display the entries in the multicast forwarding database

The multicast forwarding database (MFDB) holds the port membership information for all active multicast address entries. The key for an entry consists of a combination of a VLAN ID and a MAC address. Entries can contain data for more than one protocol.

To display the entries in the multicast forwarding database:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > Multicast Status**.

   The Multicast Status page displays.
6. To search for an entry, in the **MAC Address** field, enter a MAC address, and click the **Go** button.

   If the address exists, that entry is displayed. An exact match is required.
7. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields in IGMP Snooping Table section on the page.

Table 46. IGMP snooping 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

Table 46. IGMP snooping information (Continued)

Field	Description
Component	The component that is responsible for this entry in the MFDB. The component can be IGMP snooping, GMRP, Static Filtering, or MLD snooping.
Type	The type of the entry. Static entries are those that you configure. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The description of this multicast table entry. The description can be Management Configured, Network Configured, or Network Assisted.
Interfaces	The interfaces that are designated for forwarding (Fwd) and filtering (Flt)
Forwarding Interfaces	The forwarding list that is derived from combining all the forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces

Display the multicast forwarding database statistics

You can display the multicast forwarding database (MFDB) statistics for the switch.

To display 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > Multicast Status**.

The Multicast Status page displays.

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

The following table describes the MFDB Statistics section on the page.

Table 47. MFDB statistics information

Field	Definition
Max MFDB Table Entries	The maximum number of entries that the MFDB can hold
Most MFDB Entries Since Last Reset	The largest number of entries that were present in the MFDB since the switch was last reset
Current Entries	The current number of entries in the MFDB

Internet Group Management Protocol snooping

Internet Group Management Protocol (IGMP) snooping allows a switch to forward multicast traffic intelligently. Multicast IP traffic 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 into each of the remaining network segments in accordance with the IEEE MAC Bridge standard. Eventually, the packet is made accessible to all nodes connected to the network.

This approach works well for broadcast packets that are intended to be seen or processed by all connected nodes. In the case of multicast packets, however, this approach could lead to less efficient use of network bandwidth, particularly when the packet is intended for only a small number of nodes. Packets 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 during the period 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 solution to 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.

Enable IGMP snooping and configure IP header validation

You can enable IGMP snooping, which is used to build forwarding lists for IPv4 multicast traffic.

To enable IGMP snooping and configure IP header validation:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping**.

   The IGMP Snooping page displays.
6. Click the **IGMP Snooping Status** toggle to enable or disable IGMP snooping:
   - **The toggle is gray and positioned to the left**: IGMP snooping is disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: IGMP snooping is enabled.
7. Click the **Validate IGMP IP Header** toggle to enable or disable IP header validation:
   - **The toggle is gray and positioned to the left**: Validation of IP headers in IGMP snooping packets is disabled.
   - **The toggle is purple and positioned to the right**: Validation of IP headers in IGMP snooping packets is enabled. This validation is for ToS and TTL information in the packets. This is the default setting.
8. Click the **Apply** button.

   Your settings are saved.

Display entries in the IGMP snooping table

You can display entries in the IGMP snooping table.

To display 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping**.

   The IGMP Snooping page displays.
6. To search for an entry in the IGMP snooping table, in the **Search** field, enter a MAC address, and click the **Go** button.

   For example, enter a MAC as six two-digit hexadecimal numbers separated by colons, for example 00:01:23:43:45:67. If the address exists, that entry is displayed. An exact match is required.

The following table describes the information in the IGMP snooping table.

Table 48. IGMP snooping table information

Field	Description
MAC Address	The multicast MAC address for which the switch holds forwarding and/or filtering information. The format is six two-digit hexadecimal numbers that are separated by colons, for example, 01:00:5e:45:67:89.
VLAN ID	The VLAN ID for which the switch holds forwarding and filtering information.
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.

Table 48. IGMP snooping table information (Continued)

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

Display IGMP snooping statics and VLANs

You can display the IGMP statistics and VLANs that are enabled for IGMP snooping and IGMP snooping querier.

To display the IGMP statistics and VLAN 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping**.

   The IGMP Snooping page displays.

The following table describes the view-only fields on the page.

Table 49. IGMP snooping statistics

Field	Description
Multicast Control Frame Count	The number of multicast control frames that are processed by the switch
Interfaces Enabled for IGMP Snooping	The interfaces on which IGMP snooping is enabled

Table 49. IGMP snooping statistics (Continued)

Field	Description
VLAN IDs Enabled For IGMP Snooping	The VLANs on which IGMP snooping is enabled
VLAN IDs Enabled For IGMP Snooping Querier	The VLANs on which IGMP snooping querier is enabled

For information about displaying entries in the IGMP snooping table, see Display entries in the IGMP snooping table on page 243.

Configure the IGMP snooping settings for an interface

You can configure the IGMP snooping settings for an interface.

To configure the IGMP snooping 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping Interface Configuration**.

   The IGMP Snooping Interface Configuration page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit IGMP Snooping Interface Configuration pop-up window displays.

9. From the **Admin Mode** menu, select to enable or disable IGMP snooping for the interface:
   - **Disabled**: IGMP snooping is disabled for the interface. This is the default setting.
   - **Enabled**: IGMP snooping is enabled for the interface.
10. In the **Host Timeout** field, type the period that the switch must wait for a group report before it removes the interface as a member of the group.

    The range is from 1 to 3600 seconds. The default is 260 seconds.

11. In the **Max Response Time** field, type the period that the switch must wait after it sent a query on the interface because it did not receive a report from a group on that interface.

    The period must be 1 second or more but shorter than the period in the Host Timeout field. The default is 10 seconds.

12. In the **MRouter Timeout** field, type the period that the switch must wait to receive a query on the interface before it removes the interface from the list of interfaces with multicast routers attached.

    The range is from 0 to 3600 seconds. The default is 0 seconds, which means that the time-out is disabled and the switch waits indefinitely.

13. From the **Fast Leave Mode** menu, select to enable or disable the IGMP snooping Fast Leave mode for the interface:
    - **Disabled**: Fast Leave mode is disabled for the interface. This is the default setting.
    - **Enabled**: Fast Leave mode is enabled for the interface. If the switch receives an IGMP Leave message, the switch removes the interface immediately from the group without waiting for any further response.
14. Click the **Save** button.

    Your settings are saved.

Configure IGMP snooping for a VLAN

You can configure the settings for IGMP snooping for a VLAN, which are then used to build forwarding lists for multicast traffic.

To configure the settings for 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard 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 **Edit** button.

   The Edit IGMP Snooping VLAN Configuration pop-up window displays.
8. From the **Admin Mode** menu, select to enable or disable IGMP snooping for the VLAN:
   - **Disabled**: IGMP snooping is disabled for the VLAN. This is the default setting.
   - **Enabled**: IGMP snooping is enabled for the VLAN.
9. From the **Fast Leave Mode** menu, select to enable or disable the IGMP snooping Fast Leave mode for the VLAN:
   - **Disabled**: Fast Leave mode is disabled for the VLAN. This is the default setting.
   - **Enabled**: Fast Leave mode is enabled for the VLAN, allowing for automatic generation of fast-leave messages for the VLAN.
10. In the **Host Timeout** field, type the period that the switch must wait for a group report before it removes the VLAN as a member of the group.

The range is from 1 to 3600 seconds. The default is 260 seconds.

11. In the **Maximum Response Time** field, type the period for the maximum response time of IGMP snooping for the VLAN.

    The period must be 1 second or more but shorter than the period in the Host Timeout field. The default is 10 seconds.

12. In the **MRouter Timeout** field, type the period that the switch must wait to receive a query on the VLAN before it removes the VLAN from the list of VLANs with multicast routers attached.

    The range is from 0 to 3600 seconds. The default is 0 seconds, which means that the time-out is disabled and the switch waits indefinitely.

13. From the **Report Suppression Mode** menu, select to enable or disable the IGMP snooping report suppression mode for the VLAN:

    - **Disabled**: IGMP snooping report suppression mode is disabled for the VLAN. This is the default setting.
    - **Enabled**: IGMP snooping report suppression mode is enabled for the VLAN, and IGMP reports that are sent by multicast hosts are suppressed. The switch accomplishes this by building a Layer 3 membership table and sending only the essential reports to IGMP routers that must receive the multicast traffic.

14. From the **Querier Mode** menu, select to enable or disable the proxy querier for the VLAN:

    - **Disabled**: Query Mode is disabled for the VLAN. This is the default setting.

      If querier mode is disabled, the switch does not send IGMP queries and cannot determine if any active listeners exist on the network, nor does the switch reply to IGMP leave messages.

    - **Enabled**: Query Mode is enabled for the VLAN.

      If querier mode is enabled, the switch sends group-specific queries to determine if any hosts are interested in receiving traffic for the multicast group. If the switch receives an IGMP leave message, the switch sends an IGMP proxy query with the source IP address as 0.0.0.0.

15. In the **Query Interval** field, type the period for the IGMP query interval for the VLAN.

    The range is from 1 to 1800 seconds. The default is 60 seconds.

16. Click the **Save** button.

    Your settings are saved.

Configure an IGMP multicast router interface

You can configure an interface as the designated interface to which a multicast router is attached. All IGMP packets snooped by the switch are forwarded to the multicast router that is reachable from this interface. We refer to this interface as the multicast router.

In most situations, this configuration is not required because the switch automatically detects a multicast router and forwards IGMP packets accordingly. This configuration might be required in a complex network if you want to make sure that the multicast router always receives IGMP packets from the switch.

To configure an IGMP multicast router interface:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > IGMP Snooping > Multicast Router Configuration**.

   The Multicast Router Configuration page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit Multicast Router Configuration pop-up window displays.
9. From the **Multicast Router** menu, select to enable or disable the IGMP multicast router option for the interface:
   - **Disabled**: The IGMP multicast router option is disabled for the interface. This is the default setting.
   - **Enabled**: The IGMP multicast router option is enabled for the interface.
10. Click the **Save** button.

    Your settings are saved.

Configure an IGMP multicast router VLAN

You can configure a specific VLAN for a specific interface to forward snooped IGMP packets to the multicast router that is connected to the interface.

In most situations, this configuration is not required because the switch automatically detects a multicast router and forwards IGMP packets accordingly. This configuration might be required in a complex network if you want to make sure that the multicast router always receives IGMP packets from the switch.

To configure an IGMP multicast router VLAN:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > IGMP Snooping > Multicast Router VLAN Configuration**.

   The Multicast Router VLAN Configuration page displays.

6. From the **Interface** menu, select the interface.
7. Select the check box for the VLAN ID.
8. Click the **Edit** button.

   The Edit Multicast Router VLAN Configuration pop-up window displays.
9. From the **Multicast Router** menu, select to enable or disable the IGMP multicast router option for the VLAN:
   - **Disabled**: The IGMP multicast router option is disabled for the VLAN. This is the default setting.
   - **Enabled**: The IGMP multicast router option is enabled for the VLAN.
10. Click the **Save** button.

    Your settings are saved.

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 for IGMP snooping queriers on the network and, separately, on VLANs.

Enable the IGMP snooping querier and configure the global settings

You can enable the IGMP snooping querier on the switch and configure the global settings.

To enable the IGMP snooping querier and configure the 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > IGMP Snooping Querier > Querier Configuration**.

   The Querier Configuration page displays.
6. Click the **Querier Admin Mode** toggle to enable or disable the IGMP snooping querier:
   - **The toggle is gray and positioned to the left**: The IGMP snooping querier is disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: The IGMP snooping querier is enabled.
7. In the **Snooping Querier Address** field, type the snooping querier IPv4 address that must be used as the source address in periodic IGMP queries.

   This address is used when no address is configured on the VLAN on which queries are sent.
8. In the **IGMP Version** field, type the IGMP protocol version used in periodic IGMP queries.

   The version can be 1 or 2. The default is 2.
9. In the **Query Interval** field, type the period in seconds between periodic queries sent by the snooping querier.

   The range is from 1 to 1800 seconds. The default is 60 seconds.
10. In the **Querier Expiry Interval** field, type the period in seconds after which the last querier information is removed.

    The range is from 60 to 300 seconds. The default is 125 seconds.
11. Click the **Apply** button.

    Your settings are saved.

Add an IGMP snooping querier for a VLAN

You can add an IGMP querier for use with a VLAN on the network.

To add an IGMP snooping querier 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Configuration**.

   The Querier VLAN Configuration page displays.
6. Click the **Add New** button.

   The Add Querier VLAN Configuration pop-up window displays.
7. From the **VLAN ID** menu, select the ID for an existing VLAN.
8. From the **Querier Election Participate Mode** menu, select to enable or disable the querier election participate mode for IGMP snooping for the VLAN:

   - **Disabled**: If the switch detects another querier of the same version in the VLAN, the snooping querier moves to the non-querier state.
   - **Enabled**: The snooping querier participates in querier election, in which the lowest numbered IP address operates as the querier in that VLAN. The other querier moves to non-querier state.
9. In the **Snooping Querier VLAN Address** field, type the IPv4 address to be used as the source IP address in periodic IGMP queries that are sent on the VLAN.
10. Click the **Save** button.

    Your settings are saved.

Change an IGMP snooping querier for a VLAN

You can change an existing IGMP snooping querier for a VLAN.

To change an IGMP snooping querier 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Configuration**.

   The Querier VLAN Configuration page displays.
6. Select the check box for the VLAN.
7. Click the **Edit** button.

   The Edit Querier VLAN Configuration pop-up window displays.
8. Change the settings as needed.

   For more information, see Add an IGMP snooping querier for a VLAN on page 252.
9. Click the **Save** button.

   Your settings are saved.

Remove the IGMP snooping querier settings from a VLAN

You can remove the IGMP snooping querier settings from a VLAN.

To remove the IGMP snooping querier settings from 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Configuration**.

   The Querier VLAN Configuration page displays.
6. Select the check box for the VLAN.
7. Click the **Delete** button.

   Your settings are saved and the IGMP snooping querier settings are removed. (The VLAN itself is not deleted.)

Display the status of the IGMP snooping querier for all VLANs

You can display the status of the IGMP snooping querier for all VLANs.

To display the status of the IGMP snooping querier for all VLANs:

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Status**.

   The Querier VLAN Status page displays.
6. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 50. IGMP snooping group information

Field	Description
VLAN ID	The VLAN ID on which an IGMP snooping querier is enabled
Operational State	The operational state of the IGMP snooping querier on a VLAN. It can be in any of the following states: • **Querier**: The snooping switch is the querier in the VLAN. The snooping switch sends periodic queries with a time interval equal to the configured querier query interval. If the snooping switch finds a better querier in the VLAN, it moves to non-querier mode. • **Non-Querier**: The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch moves into querier mode. • **Disabled**: The snooping querier is not operational on the VLAN. The snooping querier moves to disabled mode when IGMP snooping is not operational on the VLAN or when the querier address is not configured or the network management address is also not configured.
Operational Version	The operational IGMP protocol version of the querier
Last Querier Address	The IP address of the last querier from which a query was snooped on the VLAN
Last Querier Version	The IGMP protocol version of the last querier from which a query was snooped on the VLAN
Operational Max Response Time (secs)	The maximum response time to be used in the queries that are sent by the snooping querier

Enable IGMP snooping on the Auto-Video VLAN

You can enable IGMP snooping on the Auto-Video VLAN.

To enable IGMP snooping on the Auto-Video 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > Auto-Video**.

   The Auto-Video page displays.

   The Auto-Video VLAN field displays the ID of the Auto Video VLAN. (By default, the ID is 4089.)
6. Click the **Auto-Video Status** toggle to enable or disable IGMP snooping on the Auto-Video VLAN:
   - **The toggle is gray and positioned to the left**: IGMP snooping is disabled on the Auto-Video VLAN. This is the default setting.
   - **The toggle is purple and positioned to the right**: IGMP snooping is enabled on the Auto-Video VLAN.
7. Click the **Apply** button.

   Your settings are saved.

Multicast Listener Discovery snooping

In IPv6 networks, Multicast Listener Discovery (MLD) snooping performs a similar function as IGMP in IPv4 networks. With MLD snooping, IPv6 multicast data is selectively forwarded to ports that are configured to receive the data instead of being flooded to all ports in a VLAN. The ports are determined by snooping IPv6 multicast control packets.

A multicast listener is a device that is configured to receive IPv6 multicast packets. MLD is used by IPv6 multicast routers to discover the presence of multicast listeners on its directly-attached links and to discover which multicast packets are of interest to neighboring devices.

The MLD protocol 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.

Enable MLD snooping

You can enable MLD snooping for the switch. MLD snooping is used to build forwarding lists for IPv6 multicast traffic.

To enable MLD snooping for 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > MLD Snooping > Configuration**.

The Configuration page displays.

6. Click the **MLD Snooping Admin Mode** toggle to enable or disable IGMP snooping:
   - **The toggle is gray and positioned to the left**: MLD snooping is disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: MLD snooping is enabled.
7. Click the **Apply** button.

   Your settings are saved.
8. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 51. MLD snooping configuration information

Field	Definition
Multicast Control Frame Count	The number of multicast control frames that were processed
Interfaces Enabled for MLD Snooping	The interfaces on which MLD snooping is enabled. MLD snooping must be enabled both globally (on the switch) and on an interface for the interface to be able to snoop MLD packets to determine which segments should receive multicast packets directed to the group address.
VLAN IDs Enabled For MLD Snooping	The VLANs on which MLD snooping is enabled

Configure the MLD snooping settings for an interface

You can configure the MLD snooping settings for an interface.

MLD snooping must be enabled both globally (on the switch) and on an interface for the interface to be able to snoop MLD packets to determine which segments should receive multicast packets directed to the group address.

To configure the MLD snooping 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > MLD Snooping > Interface Configuration**.

   The Interface Configuration page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit MLD Snooping Interface Configuration pop-up window displays.
9. From the **Admin Mode** menu, select to enable or disable MLD snooping for the interface:
   - **Disabled**: MLD snooping is disabled for the interface. This is the default setting.
   - **Enabled**: MLD snooping is enabled for the interface.
10. In the **Membership Interval** field, type the period that the switch must wait for a group report before it removes the interface as a member of the group.

    The range is from 1 to 3600 seconds. The default is 260 seconds.
11. In the **Max Response Time** field, type the period that the switch must wait after it sent a query on the interface because it did not receive a report from a group on that interface.

    The period must be 1 second or more but shorter than the period in the Host Timeout field. The default is 10 seconds.
12. In the **Expiration Time** field, type the period that the switch must wait to receive a query on the interface before it removes the interface from the list of interfaces with multicast routers attached.

The range is from 0 to 3600 seconds. The default is 0 seconds, which means that the time-out is disabled and the switch waits indefinitely.

13. From the **Fast Leave** menu, select to enable or disable the MLD snooping Fast Leave mode for the interface:
    - **Disabled**: Fast Leave mode is disabled for the interface. This is the default setting.
    - **Enabled**: Fast Leave mode is enabled for the interface, allowing for automatic generation of fast-leave messages for the interface.
14. Click the **Save** button.

    Your settings are saved.

Add MLD snooping for a VLAN

You can configure the settings for MLD snooping for a VLAN, which are then used to build forwarding lists for IPv6 multicast traffic.

To add 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > MLD Snooping > MLD VLAN Configuration**.

   The MLD VLAN Configuration page displays.
6. Click the **Add New** button.

   The Add MLD VLAN Configuration pop-up window displays.
7. From the **VLAN ID** menu, select the ID for an existing VLAN.
8. From the **Fast Leave** menu, select to enable or disable the MLD snooping Fast Leave mode for the VLAN:

- **Disabled**: Fast Leave mode is disabled for the VLAN. This is the default setting.
- **Enabled**: Fast Leave mode is enabled for the VLAN, allowing for automatic generation of fast-leave messages for the VLAN.

9. In the **Membership Interval** field, type the period that the switch must wait for a group report before it removes the VLAN as a member of the group.

   The range is from 2 to 3600 seconds.

10. In the **Maximum Response Time** field, type the period for the maximum response time of MLD snooping for the VLAN.

    The period must be 1 second or more but shorter than the period in the Membership Interval field.

11. In the **Multicast Router Expiry Time** field, type the period that the switch must wait to receive a query on the VLAN before it removes the VLAN from the list of VLANs with multicast routers attached.

    The range is from 0 to 3600 seconds. If you enter 0 seconds, the time-out is disabled and the switch waits indefinitely.

12. Click the **Save** button.

    Your settings are saved.

Change the MLD snooping settings for a VLAN

You can change the existing MLD snooping settings for a VLAN.

To change the existing MLD 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

The Dashboard page displays.

5. Select **Switching > Multicast > MLD Snooping > MLD VLAN Configuration**.

   The MLD VLAN Configuration page displays.
6. Select the check box for the VLAN.
7. Click the **Edit** button.

   The Edit MLD VLAN Configuration pop-up window displays.
8. Change the settings as needed.

   For more information, see Add MLD snooping for a VLAN on page 261.
9. Click the **Save** button.

   Your settings are saved.

Remove the MLD snooping settings from a VLAN

You can remove the MLD snooping settings from a VLAN.

To remove the MLD snooping settings from 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > MLD Snooping > MLD VLAN Configuration**.

   The MLD VLAN Configuration page displays.
6. Select the check box for the VLAN.
7. Click the **Delete** button.

Your settings are saved and the MLD snooping settings are removed. (The VLAN itself is not deleted.)

Configure an MLD multicast router interface

You can configure an interface as the designated interface to which a multicast router is attached. All MLD packets snooped by the switch are forwarded to the multicast router that is reachable from this interface. We refer to this interface as the multicast router.

In most situations, this configuration is not required because the switch automatically detects a multicast router and forwards MLD packets accordingly. This configuration might be required in a complex network if you want to make sure that the multicast router always receives MLD packets from the switch.

To configure an MLD multicast router interface:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > MLD Snooping > Multicast Router Configuration**.

   The Multicast Router Configuration page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit Multicast Router Configuration pop-up window displays.

9. From the **Multicast Router** menu, select to enable or disable the MLD multicast router option for the interface:
   - **Disabled**: The MLD multicast router option is disabled for the interface. This is the default setting.
   - **Enabled**: The MLD multicast router option is enabled for the interface.
10. Click the **Save** button.

    Your settings are saved.

Enable or disable MLD multicast router mode for a VLAN

You can use a VLAN for a specific interface to forward snooped MLD packets to the multicast router that is connected to the interface.

In most situations, this configuration is not required because the switch automatically detects a multicast router and forwards MLD packets accordingly. This configuration might be required in a complex network if you want to make sure that the multicast router always receives MLD packets from the switch.

To enable or disable MLD multicast router mode 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard 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 interface.
7. Select the **Add New** check box.

   The Add MLD Router VLAN Configuration pop-up window displays.
8. In the **VLAN ID** field, type the ID for an existing VLAN.
9. From the **Multicast Router** menu, select to enable or disable the MLD multicast router mode for the VLAN:
   - **Disabled**: The MLD multicast router mode is disabled for the VLAN. This is the default setting.
   - **Enabled**: The MLD multicast router mode is enabled for the VLAN.
10. Click the **Save** button.

    Your settings are saved.

MLD snooping querier overview

In IPv6 networks, a Multicast Listener Discovery (MLD) snooping querier performs a similar function as an IGMP snooping querier in IPv4 networks.

MLD 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 MLD querier. The MLD query responses, known as MLD 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 for MLD snooping queriers on the network and, separately, on VLANs.

Enable the MLD snooping querier and configure the global settings

You can enable the MLD snooping querier on the switch and configure the global settings.

To enable the MLD snooping querier and configure the 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > Multicast > MLD Snooping > Querier Configuration**.

   The Querier Configuration page displays.

6. Click the **Querier Admin Mode** toggle to enable or disable the MLD snooping querier:
   - **The toggle is gray and positioned to the left**: The MLD snooping querier is disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: The MLD snooping querier is enabled.
7. In the **Querier Address** field, specify the snooping querier IPv6 address that must be used as the source address in periodic MLD queries.

   This address is used when no address is configured on the VLAN on which queries are sent. The supported IPv6 formats are x:x:x:x:x:x:x:x and x::x.

   Note: The MLDP Version field always states MLD protocol version 1. This is the version that is used in periodic MLD queries.

8. In the **Query Interval** field, type the period in seconds between periodic queries sent by the snooping querier.

The range is from 1 to 1800 seconds. The default is 60 seconds.

9. In the **Querier Expiry Interval** field, type the period in seconds after which the last querier information is removed.

   The range is from 60 to 300 seconds. The default is 60 seconds.

10. Click the **Apply** button.

    Your settings are saved.

    The page displays the VLAN IDs enabled for MLD snooping querier.

Add an MLD snooping querier for a VLAN and display the status

You can add an MLD querier for use with a VLAN on the network.

To add an MLD snooping querier for a VLAN and display the 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > Multicast > MLD Snooping > Querier VLAN Configuration**.

   The Querier VLAN Configuration page displays.

6. Click the **Add New** button.

   The Add MLD Snooping Querier VLAN Configuration pop-up window displays.

7. From the **VLAN ID** menu, select the ID for an existing VLAN.
8. From the **Querier Election Participate Mode** menu, select to enable or disable the querier election participate mode for MLD snooping for the VLAN:

- **Disabled**. If the switch detects another querier of the same version in the VLAN, the snooping querier moves to the non-querier state.
- **Enabled**: The snooping querier participates in querier election, in which the lowest numbered IP address operates as the querier in that VLAN. The other querier moves to non-querier state.

9. In the **Querier VLAN Address** field, specify the IPv6 address to be used as the source address in periodic IGMP queries that are sent on the VLAN.
10. Click the **Save** button.

    Your settings are saved.

The following table describes the view-only fields on the page.

Table 52. MLD snooping querier VLAN configuration information

Field	Description
Operational State	The operational state of the MLD snooping querier on a VLAN: • **Querier**: The snooping switch is the querier in the VLAN. The snooping switch sends out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch finds a better querier in the VLAN, it moves to non-querier mode. • **Non-Querier**: The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch moves into querier mode. • **Disabled**: The snooping querier is not operational on the VLAN. The snooping querier moves to disabled mode when 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 IPv6 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

Change an MLD snooping querier for a VLAN

You can change an existing MLD snooping querier for a VLAN.

To change an MLD snooping querier 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > Multicast > MLD Snooping > Querier VLAN Configuration**.

   The Querier VLAN Configuration page displays.

6. Select the check box for the VLAN.
7. Click the **Edit** button.

   The Edit MLD Snooping Querier VLAN Configuration pop-up window displays.

8. Change the settings as needed.

   For more information, see Add an MLD snooping querier for a VLAN and display the status on page 268.

9. Click the **Save** button.

   Your settings are saved.

Remove the MLD snooping querier settings from a VLAN

You can remove the MLD snooping querier settings from a VLAN.

To remove the MLD snooping querier settings from 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > Multicast > MLD Snooping > Querier VLAN Configuration**.

   The Querier VLAN Configuration page displays.
6. Select the check box for the VLAN.
7. Click the **Delete** button.

   Your settings are saved and the MLD snooping querier settings are removed. (The VLAN itself is not deleted.)

Multicast VLAN registration

IGMP and MLD snooping help to limit multicast traffic when member ports are in the same VLAN. However, when ports belong to different VLANs, a copy of the multicast stream is sent to each VLAN with member ports in the multicast group. Multicast VLAN registration (MVR) eliminates the need to duplicate the multicast traffic when multicast group member ports belong to different VLANs.

MVR uses a dedicated multicast VLAN to forward multicast traffic over the L2 network. You can configure only one multicast source VLAN (MVLAN) on the switch. Such an MVLAN is used only for certain multicast traffic, such as traffic from an IPTV application, to prevent duplication of multicast streams for clients in different VLANs. Clients can dynamically join or leave the MVLAN without interfering with their membership in other VLANs.

MVR, like IGMP and MLD snooping, allows a Layer 2 switch to listen to IGMP and MLD messages to learn about multicast group membership.

You can configure global, group, interface, and group membership settings.

Enable MVR and configure the global settings

You can enable MVR and configure the global settings that apply to the switch.

To enable MVR and configure the 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > MVR > MVR Configuration**.

   The MVR Configuration page displays.
6. From the **MVR Running** menu, select to enable or disable MVR on the switch:
   - **Disable**: MVR is disabled on the switch. This is the default setting.
   - **Enable**: MVR is enabled on the switch.
7. In the **MVR Multicast VLAN** field, type the VLAN ID on which MVR multicast data must be received.

   All MVR source ports belong to this VLAN. The range is from 1 to 4093. The default is 1.
8. In the **MVR Global Query Response Time** field, type the period that the switch must wait for an IGMP group membership report from an interface before removing the interface as a member from the multicast group.

   This period applies only to the removal of the interface from the receiver port on the switch. When an IGMP query is sent from a receiver port, the switch waits for the default or configured MVR query time for an IGMP group membership report before removing the interface as a member from the multicast group. The period is measured

in a tenths of a second. The range is from 1 to 100 tenths. The default is 5 tenths (one half).

9. From the **MVR Mode** menu, select the MVR mode of operation:
   - **Compatible**: Blocks IGMP group membership reports on source ports. This is the default setting.
   - **Dynamic**: Allows IGMP group membership reports on source ports.
10. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only fields on the page.

Table 53. MVR configuration information

Field	Definition
MVR Max Multicast Groups	The maximum number of multicast groups that MVR supports
MVR Current Multicast Groups	The number of the MVR groups allocated

Add an MVR group

You can add an MVR group. After you configure interfaces for MVR (see Configure an MVR interface on page 275), you can add them as members to the MVR group (see Configure the members of an MVR group on page 276).

To add an MVR 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > MVR > MVR Group Configuration**.

The MVR Group Configuration page displays.

6. Click the **Add New** button.

   The Add MVR Group Configuration pop-up window displays.

7. In the **MVR Group IP** field, type the IP address for the MVR group.
8. In the **Count** field, type the number of contiguous MVR groups.

   The range is from 1 to 256.

   This number helps you to easily create multiple MVR groups. If the field is empty, clicking the Save button creates only one new MVR group. If you, for example, type 3, three MVR groups are created when you click the Save button.

9. Click the **Save** button.

   You settings are saved and the MVR group is added.

The following table describes the view-only fields on the page.

Table 54. MVR group configuration information

Field	Definition
Status	The status of the MVR group
Members	The list of interfaces that are members of the MVR group

Remove an MVR group

You can remove an MVR group that you no longer need.

To remove an MVR 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

The Dashboard page displays.

5. Select **Switching > MVR > MVR Group Configuration**.

   The MVR Group Configuration page displays.

6. Select the check box for the MVR group.
7. Click the **Delete** button.

   Your settings are saved and the MVR group is removed.

Configure an MVR interface

We recommend that you first configure an MVR interface before you add it as a member to an MVR group.

To configure an MVR 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > MVR > MVR Interface Configuration**.

   The MVR Interface Configuration page displays.

6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit MVR Interface Configuration pop-up window displays.

9. From the **Admin Mode** menu, select if MVR is enabled on the interface:
   - **Disabled**: MVR is disabled on the interface. This is the default setting.
   - **Enabled**: MVR is enabled on the interface.
10. From the **Type** menu, select the function, if any, for the interface in the multicast VLAN registration process:
    - **none**: The interface is neither an MVR source interface nor an MVR receiver interface. That is, the interface does not participate in the multicast VLAN registration process.
    - **source**: The interface functions as an MVR source interface.
    - **receiver**: The interface functions as an MVR receiver interface.
11. From the **Immediate Leave** menu, select if the Immediate Leave feature is enabled on the interface:
    - **Disabled**: The Immediate Leave feature is disabled on the interface. This is the default setting.
    - **Enabled**: The Immediate Leave feature is enabled on the interface, allowing the interface to immediately leave the MVR group that it is a member of after the interface receives a leave message.
12. Click the **Save** button.

    Your settings are saved.

Configure the members of an MVR group

You can add or remove interfaces as members of an MVR group.

For information about MVR groups, see Add an MVR group on page 273. For information about MVR interfaces, see Configure an MVR interface on page 275.

To configure the members of an MVR 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > MVR > MVR Group Membership**.

   The MVR Group Membership page displays.

6. From the **MVR Group IP** menu, select the IP address of the MVR group.
7. In the Ports table, click each port that you want to make a member of the MVR group.

   A selected port displays blue in the Ports table.

8. In the LAG table, click each LAG that you want to make a member of the MVR group.

   A selected LAG displays blue in the LAG table.

9. Click the **Apply** button.

   Your settings are saved.

Display the MVR statistics

You can display MVR statistics for the switch. These statistics are associated with IGMP.

To display the MVR 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > MVR > MVR Statistics**.

   The MVR Statistics page displays.
6. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 55. MVR statistics information

Field	Definition
IGMP Query Received	The number of received IGMP queries
IGMP Report V1 Received	The number of received IGMP V1 reports
IGMP Report V2 Received	The number of received IGMP V2 reports
IGMP Leave Received	The number of received IGMP leaves
IGMP Query Transmitted	The number of transmitted IGMP queries
IGMP Report V1 Transmitted	The number of transmitted IGMP V1 reports
IGMP Report V2 Transmitted	The number of transmitted IGMP V2 reports
IGMP Leave Transmitted	The number of transmitted IGMP leaves
IGMP Packet Receive Failures	The number of IGMP packet receive failures
IGMP Packet Transmit Failures	The number of IGMP packet transmit failures

6

Configure Quality of Service

This chapter covers the following topics:

- Quality of Service concepts
- Class of Service
- Differentiated Services

Quality of Service concepts

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

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

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.

At the queue (or port) level, you can configure CoS queue characteristics that affect queue mapping, such as minimum guaranteed bandwidth or transmission rate shaping.

The switch supports eight queues per port.

CoS configuration concepts

You can set the Class of Service trust mode for an interface. Each port on 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. 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 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 in situation in which 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 the CoS trust mode settings globally

A global CoS trust mode configuration setting is applied to all interfaces on the switch.

To configure the CoS trust mode 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > CoS > CoS Configuration**.

   The CoS Configuration page displays.
6. From the **Global Trust Mode** menu, select the trust mode:

- **Untrusted**: Do not trust any CoS packet marking at ingress.
- **802.1p**: The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of eight internal hardware priority queues. The default mode is 802.1p.
- **DSCP**: The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.

7. Click the **Apply** button.

   Your settings are saved.

Configure the CoS trust mode, shaping rate, and ingress rate for an interface

You can configure the CoS trust mode, shaping rate, and ingress rate for an interface.

To configure the CoS trust mode, shaping rate, and ingress rate 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **QoS > CoS > CoS Configuration**.

   The CoS Configuration page displays.

   The following steps refer to the CoS Interface Configuration section.

6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit CoS Interface Configuration pop-up window displays.

9. From the **Interface Trust Mode** menu, select one of the following trust mode options for ingress traffic on the interface:
   - **Untrusted**: Do not trust any CoS packet marking at ingress.
   - **802.1p**: The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of eight internal hardware priority queues. The default mode is 802.1p.
   - **DSCP**: The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.
10. In the **Interface Shaping Rate** field, specify the maximum outbound transmission rate bandwidth in percentage.

    This setting is used to shape the outbound transmission rate in increments of 1 percent in a range from 0 to 100 percent. This value is controlled independently of any per-queue maximum bandwidth configuration. It is effectively a second-level shaping mechanism. The default value is 0, which means that the maximum is unlimited.

11. In the **Interface Ingress Rate Limit** field, specify the maximum ingress bandwidth in percentage.

    This setting is used to shape the inbound transmission rate in increments of 1 percent in a range from 0 to 100 percent. The interface discards traffic that arrives at a bandwidth in excess of the specified limit. The default value is 0, which means that the maximum is unlimited.

12. Click the **Save** button.

    Your settings are saved.

Configure CoS queue settings for an interface

You can define what a particular queue does by configuring switch egress queues. You can control how much bandwidth is used by the queue, the queue depth during times of congestion, and the scheduling of packet transmission from all queues on a port. Each port contains its own CoS queue-related configuration.

To configure the CoS queue settings for an interface:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > CoS > Interface Queue Configuration**.

   The Interface Queue Configuration page displays.

   By default, the queue management type is TailDrop, which you cannot change. This means that when a queue is full, newly arriving packets are dropped. When space opens up again in the queue, packets are once again processed.
6. From the **Queue ID** menu, select the queue.

   You can select a queue from **0** to **7**.

   For information about queue priorities, see Map 802.1p priorities to queues on page 285.
7. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**All**).
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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit Interface Queue Configuration pop-up window displays.

10. From the **Scheduler Type** menu, select the type of scheduling that is used for the queue on the interface:

    - **Strict**: For the selected queue, the interface services traffic with the highest priority on a queue first.
    - **Weighted**: For the selected queue, the interface uses weighted round robin to associate a weight to each queue. This is the default setting.

    The setting applies only to the queue that you select from the **Queue ID** menu.

11. Click the **Save** button.

    Your settings are saved.

Map 802.1p priorities to queues

You can view or change which internal traffic classes are mapped to the 802.1p priority class values in Ethernet frames that the switch receives. 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.

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.

Table 56. Switch default values for 802.1p to queue mapping

802.1p priority	0	1	2	3	4	5	6	7
Default queue	1	0	0	1	2	2	3	3

The values under each 802.1p 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. For example, traffic that is assigned queue 7 is sent before traffic that is assigned queue 5.

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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > CoS > 802.1p to Queue Mapping**.

   The 802.1p to Queue Mapping page displays.
6. In the 802.1p to Queue Mapping section, select a check box for a queue.

   The 802.1p Priority row contains check boxes for each of the eight 802.1p priorities to be mapped.
7. From the **Queue** menu, select the queue from **0** to **7**.
8. Click the **Apply** button.

   Your settings are saved.

   For each 802.1p priority, you can select a queue value from the **Queue** menu.
9. To select and save a queue value for another 802.1p priority, repeat the previous three steps.

Map DSCP values to queues

The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits. The DSCP values go from 1 to 63. You can map each DSCP value to an internal traffic class.

You can view or change which internal traffic classes are mapped to the DSCP values in Ethernet frames that the switch receives. 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.

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 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. For example, traffic that is assigned queue 7 is sent before traffic that is assigned queue 5.

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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **QoS > CoS > DSCP to Queue Mapping**.

   The DSCP to Queue Mapping page displays.

6. From the **DSCP** menu, select a Per Hop Behavior (PHB) option or the Other DSCP Values option:
   - **Class Selector (CS) PHB**: These values are based on IP precedence.
   - **Assured Forwarding (AF) PHB**: These values define main levels to sort and manipulate some flows within the network.
   - **Expedited Forwarding (EF) PHB**: These values are used to prioritize traffic for real-time applications. In many situations, if the network exceeded traffic and you need some bandwidth guaranteed for an application, the EF traffic must receive this rate independently of the intensity of any other traffic attempting to transit the node.
   - **Other DSCP Values (Local/Experimental Use)**
7. Select a check box for a DSCP value.
8. From the **Queue** menu, select the queue from **0** to **7**.

9. Click the **Apply** button.

   Your settings are saved.

   For each DSCP value, you can select a queue value from the **Queue** menu.

10. To select and save a queue value for another DSCP value, repeat the previous four steps.

Differentiated Services

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

Standard IP-based networks provide best-effort data delivery service. Best-effort service implies that the network delivers the data in a timely fashion, although there is no guarantee. If congestion occurs, packets might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email and file transfers, a slight degradation in service is acceptable and in many cases unnoticeable. However, any degradation of service can negatively affect applications with strict timing requirements, such as voice and multimedia.

Note: For more information about DiffServ and a configuration example, see Differentiated Services (DiffServ) on page 500.

Defining DiffServ

To use DiffServ for QoS, you must first define the following categories and their criteria:

1. **Class**: Create a class and define class criteria (see Add and configure a DiffServ class on page 290 or Add and configure an IPv6 DiffServ class on page 297).
2. **Policy**: Create a policy, associate a class with the policy, and define policy attributes (see Add and configure a DiffServ policy on page 302).
3. **Service**: Add a policy to an inbound interface (see Attach a DiffServ policy to an interface on page 306).

Note the following about the DiffServ process:

- Packets are filtered and processed based on defined criteria. The filtering 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. 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. Next, the class is added to a policy. Finally, the policy is added to an interface.
- Packet processing begins by testing the match criteria for a packet. Each match criterion within a class must evaluate to true for a packet to match that class. A policy is applied to a packet when a class match within that policy is found.

Configure the DiffServ mode and display the entries in the DiffServ private MIB tables

You can enable or disable DiffServ and display the current and maximum number of rows in each of the main DiffServ private MIB tables.

To configure the DiffServ mode and display the entries in the DiffServ private MIB tables:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > DiffServ > DiffServ Configuration**.

   The DiffServ Configuration page displays.
6. Click the **DiffServ Admin Mode** toggle to enable or disable DiffServ:
   - **The toggle is gray and positioned to the left**: Differentiated services are disabled. This is the default setting.

An existing DiffServ configuration is retained and can be changed but is not active.

- **The toggle is purple and positioned to the right**: Differentiated services are enabled.

7. Click the **Apply** button.

   Your settings are saved.

The following table describes the view-only fields on the page.

Table 57. DiffServ status information

Field	Description
Class Table	The number of configured DiffServ classes out of the total allowed on the switch
Class Rule Table	The number of configured class rules out of the total allowed on the switch
Policy Table	The number of configured policies out of the total allowed on the switch
Policy Instance Table	The number of configured policy class instances out of the total allowed on the switch
Policy Attributes Table	The number of configured policy attributes (attached to the policy class instances) out of the total allowed on the switch
Service Table	The number of configured services (attached to the policies on specific interfaces) out of the total allowed on the switch

Configure a DiffServ class

You can add a new DiffServ class name or rename or delete an existing class. You can also define the criteria to associate with a DiffServ class. These DiffServ classes are used to prioritize packets as they are received. You can use multiple match criteria in a class. The logic is a Boolean logical-AND for these criteria.

Add and configure a DiffServ class

You can add a new DiffServ class and define the criteria that must be associated with the DiffServ class.

To add and configure a DiffServ class:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > DiffServ > Class Configuration**.

   The Class Configuration page displays.
6. Click the **Add New** button.

   The Add Class Configuration pop-up window displays.
7. In the **Class Name** field, type a class name.

   The class name must start with a letter and can be 1 to 31 alphanumeric characters in length.

   Note: The only option in the **Class Type** menu is **All**. You do not need to select this option because it is automatically applied. All means that all match criteria that you define for the class must be satisfied for a packet match. That is, All signifies the logical AND of all the match criteria. For example, if the class includes one criterion for an IP address and another criterion for a MAC address, the traffic must match both criteria.
8. Click the **Save** button.

   Your settings are saved and the new class is added.
9. After creating the class, click the class name, which is a hyperlink.

   The page adjusts and shows the Class Information section with the class name and the class type, and the DiffServ Class Configuration section.

   The following steps refer to the DiffServ Class Configuration section.
10. From the **Class Configuration** menu, select the criteria that must be associated with the DiffServ class:
    - **Match Every**: Adds a match condition that considers all packets to belong to the class. In the field below the Class Configuration menu, the automatic selection for this option is Any.
    - **Reference Class**: References another class for criteria. The match criteria defined in the reference class function as match criteria in addition to the match criteria that you define for the selected class.

From the menu below the Class Configuration menu, select the class to reference. A class can reference only one other class of the same type.

- **Class of Service**: Requires the Class of Service (CoS) value in an Ethernet frame header to match the specified CoS value.

  From the menu below the Class Configuration menu, select a match criterion in the range **0** to **7**.

- **VLAN**: Requires the packet's VLAN ID to match a VLAN ID that you set in the **VLAN** field. Type a VLAN ID in the range from 1 to 4093.
- **Ethernet Type**: Requires the EtherType value in the Ethernet frame header to match the protocol that you select from the **Ethernet Type** menu. You can also select **User Value** from the **Ethernet Type** menu and, in the field to the right, type a value in the hexadecimal range from 600 to ffff.
- **Source MAC**: Requires the packet's source MAC address to match the MAC address and mask that you type in the **Address** and **Mask** fields:
  - **Address**: The source MAC address that must match. The source MAC address is specified as six two-digit hexadecimal numbers separated by colons.
  - **Mask**: The MAC mask, which specifies the bits in the source MAC address to compare against the Ethernet frame. Use Fs and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.
- **Destination MAC**: Requires the packet's destination MAC address to match the MAC address and mask that you type in the **Address** and **Mask** fields:
  - **Address**: The destination MAC address that must match. The destination MAC address is specified as six two-digit hexadecimal numbers separated by colons.
  - **Mask**: The MAC mask, which specifies the bits in the destination MAC address to compare against an Ethernet frame. Use Fs and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.
- **Protocol Type**: Requires the packet's Layer 4 protocol to match the protocol that you select from the menu below the Class Configuration menu. To define an unnamed protocol, select **Other** from the menu and, in the field to the right, type a protocol number from **0** to **255**.

- **Source IP**: Requires a packet's source IP address to match the IP address and mask that you type in the **Address** and **Mask** fields:
  - **Address**: The source IPv4 address that must match, in dotted-decimal format.
  - **Mask**: The bit mask in IP dotted-decimal format indicating which parts of the source IPv4 address to use for matching against packet content.
- **Source L4 Port**: Requires the packet's TCP/UDP source port to match the protocol that you select from the menu below the **Class Configuration** menu. To define a port number, select **Other** from the menu. Then, in the field to the right, type the port number from **0** to **65535**.
- **Destination IP**: Requires the packet's destination IP address to match the IP address and mask that you type in the **Address** and **Mask** fields:
  - **Address**: The destination IPv4 address that must match, in dotted-decimal format.
  - **Mask**: The bit mask in IP dotted-decimal format indicating which parts of the destination IPv4 address to use for matching against packet content.
- **Destination L4 Port**: Requires the packet's TCP/UDP destination port to match the protocol that you select from the menu below the **Class Configuration** menu. To define a port number, select **Other** from the menu. Then, in the field to the right, type the port number from **0** to **65535**.
- **IP DSCP**: Requires the packet's IP DiffServ Code Point (DSCP) value to match the IP DSCP keyword code that you select from the menu below the **Class Configuration** menu. To define an IP DSCP value, select **Other** from the menu. Then, in the field to the right, type 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**: Requires the packet's IP precedence value to match the value that you select from the menu below the **Class Configuration** menu. You can select a value from **0** to **7**.

  The IP precedence field in a packet is defined as the high-order 3 bits of the service type octet in the IP header.
- **IP ToS**: Requires the packet's Type of Service (ToS) bits in the IP header to match the value that you type in the **Bit Value** and **Bit Type** fields:
  - **Bit Value**: Type a two-digit hexadecimal number octet value in the range from 00 to ff to match the bits in a packet's ToS field.
  - **Bit Mask**: Type the bit positions that are used for comparison against the IP ToS field in a packet.

  The IP ToS field in a packet is defined as all 8 bits of the service type octet in the IP header.

11. To add more criteria to the DiffServ class, repeat the previous step.

You can add multiple criteria to a single DiffServ class.

12. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only fields in the Class Summary section.

Table 58. DiffServ Class Configuration, Class Summary information

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

Change the criteria for an existing DiffServ class

You can change the criteria for an existing DiffServ class.

To change the criteria for an existing DiffServ class:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > DiffServ > 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. In the DiffServ Class Configuration section, change the class configuration as needed.

   For more information about the settings, see Add and configure a DiffServ class on page 290.
8. Click the **Apply** button.

Your settings are saved.

Change the name for an existing DiffServ class

You can change the name for an existing DiffServ class.

To change the name for an existing DiffServ class:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > DiffServ > Class Configuration**.

   The Class Configuration page displays.
6. Select the check box for the class name.
7. Click the **Edit** button.

   The Edit Class Configuration pop-up window displays.
8. Change the name in the **Class Name** field.

   The class name can be 1 to 31 alphanumeric characters in length. The name can be a number, a text, or a combination of both.

   Note: The only option in the **Class Type** menu is **All**. You do not need to select this option because it is automatically applied. All means that all match criteria that you define for the class must be satisfied for a packet match. That is, All signifies the logical AND of all the match criteria. For example, if the class includes one criterion for an IP address and another criterion for a MAC address, the traffic must match both criteria.
9. Click the **Apply** button.

   Your settings are saved.

Remove a DiffServ class

You can remove a DiffServ class that you no longer need.

To remove a DiffServ class:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > DiffServ > Class Configuration**.

   The Class Configuration page displays.
6. Select the check box for the class name.
7. Click the **Delete** button.

   Your settings are saved and the class is removed.

Configure an IPv6 DiffServ class

The switch supports DiffServ functionality for IPv6 by providing support for IPv6 packet classification. An IPv6 DiffServ class serves the same purpose as an IPv4 DiffServ class.

An Ethernet IPv6 packet is distinguished from an IPv4 packet by its unique Ethertype value, so all IPv6 classifiers include the Ethertype field, even though you cannot configure its value for an IPv6 class on the switch.

The destination and source IPv6 addresses use a prefix length value instead of an individual mask to qualify them as a subnet addresses or host addresses. Packets that match an IPv6 classifier can be marked with the IP DSCP field in the traffic class octet.

You can add a new DiffServ class name or rename or delete an existing class. As packets are received, these DiffServ classes are used to prioritize packets. You can use multiple match criteria in a class. The logic is a Boolean logical-AND for these criteria.

Add and configure an IPv6 DiffServ class

You can add a new IPv6 DiffServ class and define the criteria that must be associated the 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > DiffServ > IPv6 Class Configuration**.

   The IPv6 Class Configuration page displays.
6. Click the **Add New** button.

   The Add Class Configuration pop-up window displays.
7. In the **Class Name** field, type a class name.

   The class name must start with a letter and can be 1 to 31 alphanumeric characters in length.

   Note: The only option in the **Class Type** menu is **All**. You do not need to select this option because it is automatically applied. All means that all match criteria that you define for the class must be satisfied for a packet match. That is, All signifies the logical AND of all the match criteria. For example, if the class includes one criterion for an IP address and another criterion for a MAC address, the traffic must match both criteria.
8. Click the **Save** button.

   Your settings are saved and the new class is added.
9. After creating the class, click the class name, which is a hyperlink.

The page adjusts and shows the IPv6 Class Information section with the class name and the class type, and the IPv6 DiffServ Class Configuration section.

The following steps refer to the IPv6 DiffServ Class Configuration section.

10. From the **Class Configuration** menu, select the criteria that must be associated with the IPv6 DiffServ class:

- **Match Every**: Adds a match condition that considers all packets to belong to the class. In the field below the Class Configuration menu, the automatic selection for this option is Any.
- **Reference Class**: References another class for criteria. The match criteria defined in the reference class function as match criteria in addition to the match criteria that you define for the selected class.

  From the menu below the Class Configuration menu, select the class to reference. A class can reference only one other class of the same type.
- **Protocol Type**: Requires the packet's Layer 4 protocol to match the protocol that you select from the menu below the Class Configuration menu. To define an unnamed protocol, select **Other** from the menu and, in the field to the right, type a protocol number from **0** to **255**.
- **Source Prefix/Length**: Requires the packet's source prefix and prefix length to match the source IPv6 prefix and prefix length that you type in the fields below the menu.

  A 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**: Requires the packet's TCP/UDP source port to match the protocol that you select from the menu below the **Class Configuration** menu.

  To define a port number, select **Other** from the menu. Then, in the field to the right, type the port number from **0** to **65535**.
- **Destination Prefix/Length**: Requires the packet's destination prefix and prefix length to match the destination IPv6 prefix and prefix length that you type in the fields below the menu.

  A 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**: Requires the packet's TCP/UDP destination port to match the protocol that you select from the menu below the **Class Configuration** menu.

To define a port number, select **Other** from the menu. Then, in the field to the right, type the port number from **0** to **65535**.

- **IP DSCP**: Requires the packet's IP DiffServ Code Point (DSCP) value to match the IP DSCP keyword code that you select from the menu below the **Class Configuration** menu.

  To define an IP DSCP value, select **Other** from the menu. Then, in the field to the right, type 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.

11. To add more criteria to the IPv6 DiffServ class, repeat the previous step.

    You can add multiple criteria to a single IPv6 DiffServ class.

12. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only fields in the Class Summary section.

Table 59. IPv6 DiffServ class configuration class summary

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

Change the criteria for an existing IPv6 DiffServ class

You can 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.

4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > DiffServ > IPv6 Class Configuration**.

   The IPv6 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. In the IPv6 DiffServ Class Configuration section, change the class configuration as needed.

   For more information about the settings, see Add and configure an IPv6 DiffServ class on page 297.
8. Click the **Apply** button.

   Your settings are saved.

Change the name for an existing IPv6 DiffServ class

You can change the name for an existing IPv6 DiffServ class.

To change the name 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > DiffServ > IPv6 Class Configuration**.

   The Class IPv6 Configuration page displays.
6. Select the check box for the class name.
7. Click the **Edit** button.

   The Edit Class Configuration pop-up window displays.

8. Change the name in the **Class Name** field.

   The class name can be 1 to 31 alphanumeric characters in length.

   Note: The only option in the **Class Type** menu is **All**. You do not need to select this option because it is automatically applied. All means that all match criteria that you define for the class must be satisfied for a packet match. That is, All signifies the logical AND of all the match criteria. For example, if the class includes one criterion for an IP address and another criterion for a MAC address, the traffic must match both criteria.

9. Click the **Apply** button.

   Your settings are saved.

Remove an IPv6 DiffServ class

You can remove an IPv6 DiffServ class that you no longer need.

To remove 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **QoS > DiffServ > IPv6 Class Configuration**.

   The IPv6 Class Configuration page displays.

6. Select the check box for the class name.
7. Click the **Delete** button.

   Your settings are saved and the class is removed.

Configure a DiffServ policy

A DiffServ policy defines the action that must occur when packets match the criteria that are configured in one ore more classes.

Add and configure a DiffServ policy

You can add a new DiffServ policy, attach a DiffServ class or IPv6 DiffServ class to the policy, and define the attributes that must be associated the 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > DiffServ > Policy Configuration**.

   The Policy Configuration page displays.
6. Click the **Add New** button.

   The Add Policy Configuration pop-up window displays.
7. In the **Policy Name** field, type a policy name.

   The class name can be 1 to 31 alphanumeric characters in length. The name can be a number, a text, or a combination of both.
8. From the **Member Class** menu, select an existing DiffServ class or IPv6 DiffServ class that must be associated with the new policy.
9. Click the **Save** button.

   Your settings are saved and the new policy is added.
10. After creating the policy, click the policy name, which is a hyperlink.

The page adjusts and shows the Class Information section with the policy name, policy type (which is always *In* for inbound), and member class, and the Policy Attribute section.

The following steps refer to the Policy Attribute section.

11. From the **Policy Attribute** menu, select the attributes that must be associated with the policy:
    - **Assign Queue**: Requires that matching packets are assigned to a queue.

      From the menu below the Policy Attribute menu, select a queue in the range **0** to **7**.
    - **Drop**: Requires that matching packets are dropped.
    - **Mark VLAN CoS**: Requires that matching packets are marked with the VLAN priority.

      From the menu below the Policy Attribute menu, select a VLAN priority in the range from **0** to **7**.
    - **Mark IP Precedence**: Requires that matching packets are marked with an IP precedence value.

      From the menu below the Policy Attribute menu, select an IP precedence value in the range from **0** to **7**.
    - **Mirror**: Requires that matching packets are mirrored (copied) to another interface or LAG.

      From the menu below the Policy Attribute menu, select an interface or LAG.
    - **Redirect**: Requires that matching packets are redirected to another interface or LAG.

      From the menu below the Policy Attribute menu, select an interface or LAG.
    - **Mark IP DSCP**: Requires that matching packet are marked with an IP DSCP keyword code.

      From the menu below the Policy Attribute menu, select an IP DSCP keyword code. The DSCP value is defined as the high-order 6 bits of the Service Type octet in the IP header.
    - **Simple Policy**: Requires that matching packets are treated by a simple traffic policy, which is color blind and for which color classes do not apply:
      - A color-aware policy distinguishes between an action for packets that confirm to the policy, an action for packets that exceed the policy, and an action for packets that violate the policy. The switch does not support a color-aware policy.
      - A simple policy supports a single data rate and results in an action for packets that conform to the policy and an action for packets that violate the policy. You can configure the action for packets that conform to the policy, but the

action for packets that violate the policy is always Drop, that is, these packets are always dropped.

To configure a simply policy, do the following:

a. In the **Committed Rate** field, type the traffic rate for packets that conform to the simple policy.

   The traffic rate is a value in the range from 1 to 4294967295 Kbps. The committed rate is used to limit the arrival rate of conforming traffic.

b. From the **Conform Action** menu, select the action that must be associated with the simple policy:

   - **Send**: Requires that matching packets are forwarded unmodified. This is the default conforming action.
   - **Drop**: Requires that matching packets are dropped.

     Note that violating packets are also dropped.
   - **Mark CoS**: Requires that matching packets are marked with a CoS value.

     From the menu below the Conform Action menu, select a CoS value in the range from **0** to **7**.
   - **Mark IP Precedence**: Requires that matching packets are marked with an IP precedence value.

     From the menu below the Conform Action menu, select an IP precedence value in the range from **0** to **7**.
   - **Mark IP DSCP**: Requires that matching packet are marked with an IP DSCP keyword code.

     From the menu below the Conform Action menu, select an IP DSCP keyword code or type an IP DSCP value from 0 to 63 in the field to the right of the menu. A value that you type in the field overrides any IP DSCP keyword code selection from the menu.

12. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only fields on the page.

Table 60. DiffServ policy configuration, policy attributes

Field	Description
Policy Name	The name of the DiffServ policy
Policy Type	The type of the policy, which is always *In* for inbound
Member Class	The class that is associated within the policy

Change the attributes for an existing DiffServ policy

You can change the 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > DiffServ > 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. In the Policy Attribute section, change the attributes as needed.

   For more information about the settings, see Add and configure a DiffServ policy on page 302.
8. Click the **Apply** button.

   Your settings are saved.

Remove a DiffServ policy

You can remove a DiffServ policy that you no longer need.

Note: If you attached more than one class to the policy, a policy instance was created for each class. When you remove a policy, all instances of the policy are removed.

To remove 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **QoS > DiffServ > Policy Configuration**.

   The Policy Configuration page displays.

6. Select the check box for the policy name.

   If more than one instance of the same policy exists, select the first instance.

7. Click the **Delete** button.

   Your settings are saved and the policy is removed.

Attach a DiffServ policy to an interface

By attaching a DiffServ policy to an interface, you activate the policy on the interface, and traffic that enters through the interface is subject to the policy. You can attach only one 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > DiffServ > Service Configuration**.

   The Service Configuration page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit Service Interface Configuration pop-up window displays.
9. From the **Policy In Name** menu, select the name of a policy.
10. Click the **Save** button.

    Your settings are saved.

The following table describes the view-only fields on the page.

Table 61. Service Interface Configuration information

Field	Description
Direction	The traffic direction of the policy on the service interface. The direction is always *In* for inbound.
Operational Status	The operational status of this service interface (either Up or Down). The operational status is shown as Up if all of the following conditions are true: • The attached class is valid and includes at least one matching rule. • The attached policy is valid and includes at least one attribute. • The port is enabled, that is, the physical link of the port is in the *up* state.

Remove a DiffServ policy from an interface

You can remove a DiffServ policy from an interface.

To 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > DiffServ > Service Configuration**.

   The Service Configuration page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**All**).
7. Select the check box for the interface, or type the interface number (for example, g5) in the **Search** field and click the **Go** button.
8. Click the **Edit** button.

   The Edit Service Interface Configuration pop-up window displays.
9. From the **Policy In Name** menu, select **None**.
10. Click the **Save** button.

    Your settings are saved and the policy is removed from the interface.

Display DiffServ service statistics

You can display service information about the interfaces to which you attached DiffServ policies.

To display 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > DiffServ > Service Statistics**.

   The Service Statistics page displays.
6. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 62. DiffServ Service Statistics information

Field	Description
Interface	The interface with a DiffServ policy attached
Direction	The direction for which the DiffServ policies is attached. The direction is always *In* for inbound.
Policy Name	The name of the DiffServ policy. If more than one class is attached to the policy, each policy instance (with the same policy name) is displayed.
Operational Status	The operational status of the DiffServ policy (Up or Down). The status is displayed as Up if all of the following conditions are true: • The attached class is valid and includes at least one matching rule • The attached policy is valid and includes at least one attribute • The port is enabled, that is, the physical link of the port is in the *up* state
Member Classes	The DiffServ class that is a member of the policy. Different classes can be members of the same policy.

7

Manage Switch Security

The chapter covers the following topics:

- Change the device admin password
- RADIUS servers
- TACACS+ servers
- Authentication lists
- Management access profiles and rules
- Port authentication
- MAC filters for traffic control
- Storm control
- Port security
- Loop protection
- Denial of service

Change the device admin password

This device admin password is the password that you use to log in to the device UI of the switch.

The password must be 8 to 20 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. The password is case-sensitive.

To change the device admin password:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Management Security > User Configuration**.

   The User Configuration page displays.
6. In the **Current Password** field, enter the current (old) password.
7. In the **New Password** and **Confirm Password** fields, enter the same new password.
8. Click the **Apply** button.

   Your settings are saved. The next time that you log in to the switch, you must use the new password.

   If you forget the new password, you must reset the switch to factory default settings. Doing so restores the password to the default password (**password**).

RADIUS servers

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

- Web access
- Port access control (802.1X)

Configure the global RADIUS server settings

You can add information about one or more RADIUS servers on the network.

If you configure multiple RADIUS servers, consider the maximum delay time when you specify the maximum number of retransmissions (that is, the value that you enter in the **Max Number of Retransmits** field in the following procedure) and the time-out period (that is, the value that you enter in the **Timeout Duration** field in the following procedure) for RADIUS:

- For one RADIUS server, a retransmission does not occur until the configured time-out period expires without a response from the RADIUS server. In addition, the maximum number of retransmissions for one RADIUS server must pass before the switch attempts the next RADIUS server.
- Therefore, the maximum delay in receiving a RADIUS response on the switch equals the maximum number of retransmissions multiplied by the time-out period multiplied by the number of configured RADIUS servers. If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the switch receives a RADIUS response.

To configure the global RADIUS server settings:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Management Security > RADIUS > Global Configuration**.

   The Global Configuration page displays.
6. In the **Max Number of Retransmits** field, type the maximum number of times a request packet is retransmitted to the RADIUS server.

   The range is from 1 to 15. The default setting is 4.
7. In the **Timeout Duration** field, type the time-out value, in seconds, for request retransmissions.

   The range is from 1 to 30. The default setting is 5.
8. From the **Accounting Mode** menu, select to enable or disable the accounting mode on the current primary RADIUS server:
   - **Disable**: The accounting mode is disabled on the active (current) server. This is the default setting.
   - **Enable**: The accounting mode is enabled on the active (current) server.
9. Click the **Apply** button.

   Your settings are saved.

The following table describes the view-only fields on the page.

Table 63. Radius configuration information

Field	Description
Current Server IP Address	The IP address of the current RADIUS server. This field is blank if no servers are configured.
Number of Configured Servers	The number of configured RADIUS servers. The number can range from 0 to 3.

RADIUS authentication servers

You can configure and display settings for up to three RADIUS authentication servers in the network.

Add a RADIUS authentication server

You can add up to three RADIUS authentication servers. One server can be the primary server; other servers are secondary servers. If you first assign one server as the primary server and then assign another server as the primary server, the first server is automatically changed to a secondary server.

To add a RADIUS authentication 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Management Security > RADIUS > Server Configuration**.

   The Server Configuration page displays.
6. Click the **Add New** button.

   The Add Server Configuration pop-up window displays.
7. In the **Server Address** field, type the IP address of the RADIUS server.
8. In the **Authentication Port** field, type the UDP port number of the RADIUS authentication server.

   The range is from 1 to 65535.
9. From the **Secret Configured** menu, select if you want to enable or disable authentication and encryption for communication between the switch and the RADIUS server:
   - **No**: Authentication and encryption are disabled. A secret (password) is not required.
   - **Yes**: Authentication and encryption are enabled. A secret (password) is required.

10. If you enable authentication and encryption, in the **Secret** field, type the shared secret text string (password) that is used for authenticating and encrypting all RADIUS communications between the switch and the RADIUS server.

    This secret must match the one that is configured on the RADIUS server.
11. From the **Active** menu, select if the RADIUS server is a primary or secondary server:
    - **Primary**: The server functions as the primary RADIUS authentication server.
    - **Secondary**: The server functions as a secondary RADIUS authentication server.
12. Click the **Save** button.

    Your settings are saved and the server is added to the switch.

    The **Message Authenticator** attribute is automatically enabled, which adds protection to RADIUS messages by using an MD5 hash algorithm to encrypt each message. The shared secret is used as the key. If a message cannot be verified by the RADIUS server, it is discarded.

Change the settings for a RADIUS authentication server

You can change the settings for an existing RADIUS authentication server.

To change the settings for a RADIUS authentication 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Management Security > RADIUS > Server Configuration**.

   The Server Configuration page displays.
6. Select the check box for the RADIUS server.
7. Click the **Edit** button.

The Edit Server Configuration pop-up window displays.

8. Change the settings as needed.

   For more information about the settings, see Add a RADIUS authentication server on page 314.

   Note: If you change a secondary server to a primary server, the previous primary server is automatically changed to a secondary server.

9. Click the **Save** button.

   Your settings are saved.

Remove a RADIUS authentication server from the switch

You can remove a RADIUS server with which the switch no longer needs to communicate.

To remove a RADIUS authentication server from the switch:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > Management Security > RADIUS > Server Configuration**.

   The Server Configuration page displays.

6. Select the check box for the RADIUS server.
7. Click the **Delete** button.

   Your settings are saved and the RADIUS server is removed.

Display the RADIUS authentication server statistics

You can display the traffic statistics for the RADIUS authentication servers that you configure on the switch.

To display the traffic statistics for the RADIUS authentication servers:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Management Security > RADIUS > Server Configuration**.

   The Server Configuration page displays.

The following table describes the view-only fields on the page.

Table 64. RADIUS authentication server statistics information

Field	Description
Server Address	The address of the RADIUS server or the name of the RADIUS server for which the statistics are displayed
Round Trip Time	The interval, in hundredths of a second, between the most recent access-reply/access-challenge and the access-request that matched it from the RADIUS authentication server
Access Requests	The number of RADIUS access-request packets sent to the server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS access-request packets retransmitted to the server
Access Accepts	The number of RADIUS access-accept packets, including both valid and invalid packets, that were received from the server
Access Rejects	The number of RADIUS access-reject packets, including both valid and invalid packets, that were received from the server

Table 64. RADIUS authentication server statistics information (Continued)

Field	Description
Access Challenges	The number of RADIUS access-challenge packets, including both valid and invalid packets, that were received from the server
Malformed Access Responses	The number of malformed RADIUS access-response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included in malformed access-responses.
Bad Authenticators	The number of RADIUS access-response packets containing invalid authenticators or signature attributes received from the server
Pending Requests	The number of RADIUS access-request packets destined for the server that did not yet time out or receive a response
Timeouts	The number of authentication time-outs to the server
Unknown Types	The number of RADIUS packets of an unknown type that were received from the server
Packets Dropped	The number of RADIUS packets received from the server and then dropped

RADIUS accounting server

You can configure and display the settings for a single RADIUS accounting server on the network.

Configure a RADIUS accounting server

You can configure a single dedicated RADIUS accounting server for the switch.

To configure a RADIUS accounting 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Management Security > RADIUS > Accounting Server Configuration**.

   The Accounting Server Configuration page displays.
6. In the **Accounting Server Address** field, type the IP address of the RADIUS accounting server.
7. In the **Port** field, type the UDP port number of the RADIUS accounting server.

   The range is from 1 to 65535. The default port number is 1813.
8. From the **Secret Configured** menu, select if you want to enable or disable authentication and encryption for communication between the switch and the RADIUS server:
   - **No**: Authentication and encryption are disabled. A secret (password) is not required.
   - **Yes**: Authentication and encryption are enabled. A secret (password) is required.
9. If you enable authentication and encryption, in the **Secret** field, type the shared secret text string (password) that is used for authenticating and encrypting all RADIUS communications between the switch and the RADIUS server.

   This secret must match the one that is configured on the RADIUS server.
10. From the **Accounting Mode** menu, select to enable or disable the RADIUS accounting mode:
    - **Disable**: Accounting is disabled for the RADIUS server. This is the default setting.
    - **Enable**: Accounting is enabled for the RADIUS server.
11. Click the **Apply** button.

    Your settings are saved.

Display or clear the RADIUS accounting server statistics

You can display the traffic statistics for the RADIUS accounting server that you configure on the switch. You can also clear the counters.

To display or clear the RADIUS accounting server statistics:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > Management Security > RADIUS > Accounting Server Configuration**.

   The Accounting Server Configuration page displays.

6. To reset the statistics to their default values, click the **Clear Counters** button.
7. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 65. RADIUS accounting server statistics information

Field	Description
Accounting Server Address	The accounting server that is associated with the statistics
Round Trip Time	The time interval, in hundredths of a second, between the most recent accounting-response and the accounting-request that matched it from the RADIUS accounting server
Accounting Requests	The number of RADIUS accounting-request packets sent to the server. This number does not include retransmissions.
Accounting Retransmissions	The number of RADIUS accounting-request packets retransmitted to the server
Accounting Responses	The number of RADIUS packets received from the server
Malformed Accounting Responses	The number of malformed RADIUS accounting-response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS accounting-response packets that contained invalid authenticators received from this accounting server

Table 65. RADIUS accounting server statistics information (Continued)

Field	Description
Pending Requests	The number of RADIUS accounting-request packets sent to the server that did not yet time out or receive a response
Timeouts	The number of accounting time-outs to this server
Unknown Types	The number of RADIUS packets of an unknown type that were received from the server
Packets Dropped	The number of RADIUS packets received from the server and then dropped

TACACS+ servers

Terminal Access Controller Access Control System plus (TACACS+) provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. TACACS+ provides the following services:

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

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

Configure the global TACACS+ settings

You can configure the global TACACS+ settings for communication between the switch and a TACACS+ server.

To configure the global TACACS+ settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Management Security > TACACS+**.

   The TACACS+ page displays.
6. In the **Key String** field, type the authentication and encryption key for TACACS+ communications between the switch and a TACACS+ server.

   The range is from 0 to 128. The key must match the key configured on the TACACS+ server.
7. In the **Connection Timeout** field, type the maximum number of seconds allowed to establish a TCP connection between the switch and a TACACS+ server.

   The key can be from 1 to 30 seconds. The default is 5 seconds.
8. Click the **Apply** button.

   Your settings are saved.

Add a TACACS+ server

You can add up to two TACACS+ servers with which the switch can communicate.

To add a TACACS+ 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

The Dashboard page displays.

5. Select **Security > Management Security > TACACS+**.

   The TACACS+ page displays.

6. Click the **Add New** button.

   The Add TACACS+ Server Configuration pop-up window displays.

7. In the **TACACS+ Server** field, type the IP address of the TACACS+ server.
8. In the **Priority** field, type the priority for the TACACS+ server.

   The priority determines the order in which the TACACS+ servers are contacted when attempting to authenticate a user. A value of 0 is the highest priority. The range is from 0 to 65535.

9. In the **Port** field, type the authentication port number that is used by the TACAS+ server.

   The value must be in the range from 0 to 65535.

10. In the **Key String** field, type the authentication and encryption key for TACACS+ communications between the switch and the TACACS+ server.

    The key can be from 0 to 128 characters. The key must match the key that is used on the TACACS+ server. You can also leave this field empty, in which case the switch uses the global key string.

11. In the **Connection Timeout** field, type the time that passes before the connection between the switch and the TACACS+ server times out.

    The range is from 1 to 30 seconds. You can also leave this field empty, in which case the switch uses the global connection time-out setting.

12. Click the **Save** button.

    Your settings are saved and the TACACS+ server is added.

Change the settings for a TACACS+ server

You can change the settings for an existing TACACS+ server.

To change the settings for a TACACS+ 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Management Security > TACACS+**.

   The TACACS+ page displays.
6. Select the check box for the TACACS+ server.
7. Click the **Edit** button.

   The Edit TACACS+ Server Configuration pop-up window displays.
8. Change the settings as needed.

   For more information about the settings, see Add a TACACS+ server on page 322.
9. Click the **Save** button.

   Your settings are saved.

Remove a TACACS+ server from the switch

You can remove a TACACS+ server with which the switch no longer needs to communicate.

To remove a TACACS+ server from the switch:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Management Security > TACACS+**.

   The TACACS+ page displays.
6. Select the check box for the TACACS+ server.
7. Click the **Delete** button.

   Your settings are saved and the TACACS+ server is removed.

Authentication lists

An authentication login list specifies one or more authentication methods to validate switch or interface access for a user. Access can be HTTP or HTTPS access to the device UI, or Dot1x (IEEE 802.1x) access to an interface.

Configure the HTTP authentication list

You can configure the HTTP authentication list, which specifies the authentication methods to validate switch or port access through HTTP, for example, through a web browser session. A single HTTP authentication list exists, which, by default, uses local authentication.

To configure the HTTP 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

The Dashboard page displays.

5. Select **Security > Management Security > Authentication List > HTTP/HTTPS Authentication List**.

   The HTTP/HTTPS Authentication List page displays.

6. In the HTTP Authentication List section, click the **Edit** button.

   The Edit HTTP Authentication List pop-up window displays.

7. From the **1** menu, select the authentication method that must be used first in the selected authentication login list.

   If you select a method that does not time out as the first method, such as Local, no other method is tried, even if you specified more than one method. User authentication occurs in the order that you select the methods:

   - **Local**: The user's locally stored name and password are used for authentication. 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. This is the default selection for method 1.
   - **None**: The user is allowed access without authentication.
   - **RADIUS**: The user's name and password are authenticated using the RADIUS server instead of the local server.
   - **TACACS+**: The user's name and password are authenticated using the TACACS+ server instead of the local server.

8. From the **2**, **3**, and **4** menus, select the authentication methods, if any, that must be used in the selected authentication login list.

   If a previous method times out, the next method is used. For example, the authentication method that you select from the 2 menu is tried after the authentication method that select from the 1 menu in the previous step. Similarly, the authentication method that you select from the 3 menu is tried after the authentication method that you select from the 2 menu, and so on. If you select a method that does not time out, or you select None, the next method is not tried.

9. Click the **Save** button.

   Your settings are saved.

Configure the HTTPS authentication List

You can configure the HTTPS authentication list, which specifies the authentication methods to validate switch or port access through secure HTTP (HTTPS), for example, through a web browser session. A single HTTPS authentication list exists, which, by default, uses local authentication.

To configure the 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > Management Security > Authentication List > HTTP/HTTPS Authentication List**.

   The HTTP/HTTPS Authentication List page displays.

6. In the HTTPS Authentication List section, click the **Edit** button.

   The Edit HTTPS Authentication List pop-up window displays.

7. From the **1** menu, select the authentication method that must be used first in the selected authentication login list.

   If you select a method that does not time out as the first method, such as Local, no other method is tried, even if you specified more than one method. User authentication occurs in the order that you select the methods:

   - **Local**: The user's locally stored name and password are used for authentication. 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. This is the default selection for method 1.
   - **None**: The user is allowed access without authentication.
   - **RADIUS**: The user's name and password are authenticated using the RADIUS server instead of the local server.
   - **TACACS+**: The user's name and password are authenticated using the TACACS+ server instead of the local server.

8. From the **2**, **3**, and **4** menus, select the authentication methods, if any, that must be used in the selected authentication login list.

If a previous method times out, the next method is used. For example, the authentication method that you select from the 2 menu is tried after the authentication method that select from the 1 menu in the previous step. Similarly, the authentication method that you select from the 3 menu is tried after the authentication method that you select from the 2 menu, and so on. If you select a method that does not time out, or you select None, the next method is not tried.

9. Click the **Save** button.

   Your settings are saved.

Configure the Dot1x authentication list

You can configure the Dot1x authentication list, which specifies the authentication methods to validate interface access for users associated with the Dot1x list. A single Dot1x list exists, for which you can select a single access method only. By default, access to interfaces does not require authentication, so no default access method exists.

To configure the Dot1x authentication list:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > Management Security > Authentication List > Dot1x Authentication List**.

   The Dot1x Authentication List page displays.

6. Click the **Edit** button.

   The Edit Dot1x Authentication List pop-up window displays.

7. To enable the Dot1x list, select the **dotxList** check box.

   The menu options become available.

8. Select the authentication method that must be used:
   - **None**: The user is allowed access without authentication.
   - **RADIUS**: The user's name and password are authenticated using the RADIUS server.
9. Click the **Save** button.

   Your settings are saved.

Management access profiles and rules

Access control allows you to configure an access control profile and set rules for access to the device UI and access by SNMP stations, and client access to a TFTP server. We refer to an access control profile as an access profile. You can add a single access profile, which you can configure, activate, or deactivate.

Caution: If you configure a security access profile incorrectly and you activate the access profile, you might no longer be able to access the switch's device UI. If that situation occurs, you must reset the switch to factory default settings.

Add an access profile

You can set up a single security access profile with which you can associate an access rule configuration.

To add an access profile:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Protocol Access Control**.

   The Protocol Access Control page displays.
6. In the **Access Profile Name** field, enter the name of the access profile to be added.

   The maximum length is 32 characters.
7. Click the **Apply** button.

   Your settings are saved. By default, the access profile is deactivated. After you add rules, you can activate the access profile.

Add a rule to the access profile

After you add the access profile, you can add one or more security access rules to the access profile.

If you access the switch from a computer, make sure that you add a permit rule for the type of service that you use (for example, HTTPS), your computer's IP address, and your computer's subnet mask.

Caution: You must add a permit rule for your device and access method, otherwise you are locked out from the switch after you activate the access profile. If that situation occurs, you must reset the switch to factory default settings (see Reset the switch to factory default settings on page 424).

To add a rule to the access profile:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

The Dashboard page displays.

5. Select **Security > Protocol Access Control**.

   The Protocol Access Control page displays.

   The following steps refer to the Access Rule Configuration section.

6. Click the **Add New** button.

   The Add Access Rule Configuration pop-up window displays.

7. From the **Rule Type** menu, select to permit or deny access when the rule is a match:
   - **Permit**: Allows access from a device that matches the rule criteria.
   - **Deny**: Denies access to a device that matches the rule criteria.
8. From the **Service Type** menu, select the access method or protocol to which the rule applies:

   TFTP, **HTTP**, **Secure HTTP (SSL)**, **SNMP**, or **SSH**.

   Access over the protocol is either permitted or denied.

9. In the **Source IP Address** field, type the source IP address from which the management traffic originates.
10. In the **Mask** field, type the subnet mask from which the management traffic originates.
11. In the **Priority** field, type a priority number for the rule.

    The range is from 1 to 64.

    The rules are validated against the incoming management request in ascending order of their priorities. If a rule matches, the action is performed and subsequent rules below that rule are ignored. For example, if a source IP address 10.10.10.10 is configured with priority 1 to permit, and the same source IP address 10.10.10.10 is also configured with priority 2 to deny, then access is permitted if the profile is active, and the second rule is ignored.

12. Click the **Save** button.

    Your settings are saved and the access rule is added.

Activate the access profile

After you add rules to the access profile, you can activate the access profile.

To activate the access profile:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > Protocol Access Control**.

   The Protocol Access Control page displays.

6. Activate the access profile by clicking the **Access Profile** toggle.

   When the access profile is set to be enabled, the toggle is purple and positioned to the right.

   Caution: If you configure a security access profile incorrectly and you activate the access profile, you might no longer be able to access the switch's device UI. If that situation occurs, you must reset the switch to factory default settings (see Reset the switch to factory default settings on page 424).

7. Click the **Apply** button.

   Your settings are saved and the access profile is now active.

Display the access profile rules and the number of filtered packets

After you added rules to the active profile, you can display the rules. If the access profile is active, you can also display the number of filtered packets.

To display the access profile rules and the number of filtered packets:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > Protocol Access Control**.

   The Protocol Access Control page displays.

   The Packet Filtered field displays the number of number of filtered packets.

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

The following table describes the view-only fields on the page.

Table 66. Access rule configuration information

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

Change a rule for the access profile

You can change an existing security access rule for the access profile.

To change a rule for the access profile:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > Protocol Access Control**.

   The Protocol Access Control page displays.

6. In the Access Rule Configuration section, select the check box for the rule.
7. Click the **Edit** button.

   The Edit Access Rule Configuration pop-up window displays.

8. Change the settings for the rule as needed.

   For more information about the settings, see Add a rule to the access profile on page 330.

9. Click the **Save** button.

   Your settings are saved.

Deactivate the access profile

You can deactivate the access profile.

To deactivate the access profile:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Protocol Access Control**.

   The Protocol Access Control page displays.
6. Deactivate the access profile by clicking the **Access Profile** toggle.

   When the access profile is set to be disabled, the toggle is gray and positioned to the left.
7. Click the **Apply** button.

   Your settings are saved and the access profile is now deactivated.

Remove a rule from the access profile

You can remove a security access rule that you no longer need for the access profile.

To remove a rule from the access profile:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Protocol Access Control**.

   The Protocol Access Control page displays.

6. In the Access Rule Configuration section, select the check box for the rule.
7. Click the **Delete** button.

   Your settings are saved and the rule is removed.

Remove the access profile

You can remove the access profile if you no longer need it. Before you can remove the access profile, you must deactivate it (see Deactivate the access profile on page 334).

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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Protocol Access Control**.

   The Protocol Access Control page displays.
6. Click the **Remove Profile** button.

   A confirmation pop-up window displays.
7. Click the **Yes, Remove** button.

   The access profile is removed.

Port authentication

With port-based authentication, when 802.1X is enabled both globally and on the port, successful authentication of any one client device (supplicant) attached to the port

results in all users being able to use the port without restrictions. At any time, only one supplicant is allowed to attempt authentication on a port in this mode. Ports in this mode are under bidirectional control. 802.1X is the default authentication mode. 802.1X is also referred to as Dot1x.

Note: For port authentication, if we refer to a port, it means the same as a physical interface.

An 802.1X network includes three components:

- **Authenticator**: The switch port that is authenticated before access to system services is permitted.
- **Supplicant**: The client device or host that is connected to the authenticated port requesting access to the system services.
- **Authentication server**: The external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates if the supplicant is authorized to access system services.

Note: For more information about 802.1X and a configuration example, see 802.1X port access control on page 507.

Configure the global 802.1X authentication settings

You can enable 802.1X on the switch and configure the global 802.1X settings that apply to the switch.

If you enable 802.1X, authentication must be performed by a RADIUS server:

- **RADIUS server**: Configure a RADIUS server (see RADIUS servers on page 312).
- **Primary authentication method**: Set the primary authentication method to RADIUS, that is, RADIUS must be the first method for a login authentication list (see Authentication lists on page 325).

To configure the global 802.1X authentication 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Port Authentication > 802.1x Configuration**.

   The 802.1x Configuration page displays.
6. Click the **Port-Based Authentication State** toggle to enable or disable 802.1X port-based authentication:
   - **The toggle is gray and positioned to the left**: 802.1X port-based authentication is globally disabled on the switch. This is the default setting.

     The switch does not check for 802.1X authentication before allowing traffic on any ports, even if individual ports are configured to allow only authenticated users.
   - **The toggle is purple and positioned to the right**: 802.1X port-based authentication is globally enabled on the switch.
7. Click the **VLAN Assignment Mode** toggle to enable or disable automatic assignment of a port to a particular VLAN:
   - **The toggle is gray and positioned to the left**: A port is not assigned to a particular VLAN. This is the default setting.
   - **The toggle is purple and positioned to the right**: A port is assigned to a particular VLAN based on the result of the authentication that a client device (supplicant) uses when it accesses a resource that is attached to the port.

     The authentication server can provide information to the switch about which VLAN the client device must be assigned to.
8. Click the **Dynamic VLAN Creation Mode** toggle to enable or disable dynamic VLAN creation:
   - **The toggle is gray and positioned to the left**: A VLAN is not dynamically created. This is the default setting.
   - **The toggle is purple and positioned to the right**: A RADIUS-assigned VLAN that does not yet exist on the switch can be dynamically created.

     If RADIUS-assigned VLANs are enabled, the RADIUS server includes the VLAN ID in the 802.1X tunnel attributes of its response message to the switch. If dynamic VLAN creation is enabled on the switch and the RADIUS-assigned VLAN does not exist, the assigned VLAN is dynamically created. This means that the client device (supplicant) can connect from any port and is assigned to the appropriate

VLAN. This feature gives flexibility for client devices to move around the network without much additional configuration required.

9. Click the **EAPoL Flood Mode** toggle to enable or disable Extensible Authentication Protocol (EAP) over LAN (EAPoL) flood mode:
   - **The toggle is gray and positioned to the left**: A flood of EAPoL messages is rejected by the switch. This is the default setting.
   - **The toggle is purple and positioned to the right**: A flood of EAPoL messages with 802.1X authentication requests is accepted by the switch.
10. Click the **Apply** button.

    Your settings are saved.

Configure the 802.1X authentication settings for a port

You can configure 802.1X authentication settings for a port. These control access to the port.

To configure 802.1X authentication 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Port Authentication > Port Authentication**.

   The Port Authentication 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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit Port Authentication pop-up window displays.

8. From the **Port Control** menu, select an option:

   - **Auto**: Access is determined by the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server. This is the default setting.
   - **Authorized**: The port is unconditionally set to authorized. Supplicants do not need to be authorized.
   - **Unauthorized**: The port is unconditionally set to unauthorized. No supplicant can be authorized on the port.
   - **MAC Based**: Access is determined by the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server and the MAC address of the supplicant.

     This mode allows multiple supplicants that are connected to the same port to each authenticate individually. Each supplicant connected to the port must authenticate separately in order to gain access to the network. The supplicants are distinguished by their MAC addresses.

9. If you select **MAC Based** from the **Control Mode** menu, from the **MAB** menu, select to enable or disable MAC-based authentication bypass (MAB) for 802.1x-unaware client devices:

   - **Disabled**: MAB is disabled. This is the default setting.
   - **Enabled**: MAB is enabled. If a client device does not support 802.1x, it can still be authenticated.

10. In the **Guest VLAN ID** field, type the ID of the guest VLAN.

    After three authentication failures, an unauthenticated client device can be placed in the guest VLAN, which allows the port to provide a distinguished service to unauthenticated client devices.

    Enter an ID in the range from 2 to 4093. Type 0 if you do not use a guest VLAN or to reset the guest VLAN ID.

11. In the **Guest VLAN Period** field, type the period in seconds during which the port remains in the quiet state following a failed authentication exchange.

In the quiet state for the guest VLAN, the port does not accept authentication requests. Enter a period from 1 to 300 seconds. The default is 90 seconds.

12. In the **Unauthenticated VLAN ID** field, enter the ID for the unauthenticated VLAN.

    After three failed authentication attempts, a client device can be placed in a VLAN for unauthenticated clients. This VLAN might be configured with limited network access.

    Enter an ID in the range from 2 to 4093. Type 0 if you do not use an unauthenticated VLAN or to reset the unauthenticated VLAN ID.

13. From the **Periodic Reauthentication** menu, select to enable or disable periodic reauthentication:
    - **Disabled**: Periodic reauthentication is disabled. This is the default setting.
    - **Enabled**: Periodic reauthentication is enabled.
14. If you select **Enabled** from the **Periodic Reauthentication** menu, in the **Reauthentication Period** field, type the period in seconds after which the supplicant must be reauthenticated.

    Type a period from 0 to 65535 seconds. The default is 3600 seconds.

15. In the **Quiet Period** field, type the period in seconds that the port remains in the quiet state following a failed authentication exchange.

    In the quiet state, the port does not accept authentication requests. Type a period from 0 to 65535 seconds. The default is 60 seconds.

16. In the **Resending EAP** field, type the period in seconds for EAP retransmissions.

    The EAP retransmission is the period after which an EAPoL EAP Request/Identify frame is resent to the supplicant.

    Type a period from 0 to 65535 seconds. The default is 30 seconds.

17. In the **Max EAP Requests** field, type the maximum number of times that the port sends an EAPoL EAP Request/Identify frame to the supplicant before timing out the supplicant.

    Type a number from 1 to 10. The default is 2.

18. In the **Supplicant Timeout** field, type the period in seconds after which the port times out the supplicant, causing the authentication to fail.

    Type a period in the range from 0 to 65535 seconds. The default is 30 seconds.

19. In the **Server Timeout** field, enter the period after which the port times out the authentication server, causing the authentication to fail.

    Type a period in the range from 0 to 65535 seconds. The default is 30 seconds.

20. Click the **Save** button.

    Your settings are saved.

The following table describes the view-only fields on the page.

Table 67. Port authentication information

Field	Description
Control Direction	The control direction for the port, which is always Both. The control direction indicates how protocol exchanges take place between a 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 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 port (Authenticator or Supplicant)
Authenticator PAE State	The state of the authenticator PAE: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, or ForceUnauthorized
Backend State	The state of the backend authentication: Request, Response, Success, Fail, Timeout, Initialize, or Idle

Initialize 802.1X on a port

If you initialize a port, the port becomes unauthorized and then goes through the authentication procedure, causing traffic on the port to be blocked until the port is authorized successfully.

You can initialize a port only if the control mode setting is Auto. This is the default setting, in which port access is determined by the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.

To initialize 802.1X on a port:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Port Authentication > Port Authentication**.

   The Port Authentication page displays.
6. Select one or more ports (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 (for example, g3) in the **Search** 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. Click the **Initialize** button.

   802.1X is reset to the initialization state. Traffic sent to and from the port is blocked during the authentication process. When you click this button, the action is immediate.

Restart 802.1X authentication on a port

You can force a port to restart 802.1X authentication for an attached client device. During the authentication procedure, traffic continues to be forwarded and is not blocked.

You can restart 802.1X authentication only if the control mode setting is Auto. This is the default setting, in which port access is determined by the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.

To restart 802.1X authentication on a port:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Port Authentication > Port Authentication**.

   The Port Authentication page displays.
6. Select one or more ports (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 (for example, g3) in the **Search** 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. Click the **Reauthenticate** button.

   The port is forced to restart the authentication process. When you click this button, the action is immediate.

Display the port summary

You can display summary information about the port-based authentication settings for each port.

To display 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > Port Authentication > Port Summary**.
   The Port Summary page displays.
6. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 68. Port summary information

Field	Description
Port	The port for which settings are displayed
Control Mode	The *configured* control mode for the port: • **Auto**: Access is determined by the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server. • **Force Authorized**: The port is unconditionally set to authorized. Supplicants do not need to be authorized. • **Force Unauthorized**: The port is unconditionally set to unauthorized. No supplicant can be authorized on the port.
Operating Control Mode	The control mode under which the port is *actually operating*: • **Auto**: Access is determined by the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server. • **Force Authorized**: The port is unconditionally set to authorized. Supplicants do not need to be authorized. • **Force Unauthorized**: The port is unconditionally set to unauthorized. No supplicant can be authorized on the port. • **MAC Based**: Access is determined by the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server and by the MAC address of the supplicant. • **N/A**: The port cannot participate in port access control. This situation occurs if the port is in detached state.
Reauthentication Enabled	Indicates if reauthentication of the supplicant is allowed: • **True**: Reauthentication is allowed • **False**: Reauthentication is not allowed
Port Status	The authorization status of the port: • **Authorized**: The port is authorized • **Unauthorized**: The port is unauthorized • **N/A**: The port cannot participate in port access control. This situation occurs if the port is in detached state.

Display the client summary

You can display information about client devices (supplicants) that are connected to switch authenticator ports. Information is displayed only if active 802.1X sessions are present.

To display 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Port Authentication > Client Summary**.

   The Client Summary page displays.
6. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 69. Client summary information

Field	Description
Port	The port for which information is displayed
User Name	The name that represents the identity of the client device (supplicant)
Supplicant MAC Address	The MAC address of the supplicant
Filter ID	The policy filter ID assigned by the authenticator to the supplicant
VLAN ID	The VLAN ID assigned by the authenticator to the supplicant

Table 69. Client summary information (Continued)

Field	Description
VLAN Assigned	The type of VLAN that the authenticator assigned to the supplicant: • **Default Assigned VLAN**: The client was authenticated on the port default VLAN and the authentication server was not a RADIUS server. • **RADIUS Assigned VLAN**: RADIUS was used to authenticate the client. • **Unauthenticated VLAN:** The client was authenticated on the Unauthenticated VLAN. • **Guest VLAN**: The client was authenticated on the Guest VLAN. • **Voice VLAN**: The client was authenticated on the Voice VLAN. • **Monitor Mode VLAN**: The client was authenticated in Monitor mode and assigned by the RADIUS server to a monitor VLAN. • **Not Assigned**: The client was not assigned to any VLAN.
Session Timeout	The session time-out enforced by the RADIUS server for the supplicant
Termination Action	The termination action enforced by the RADIUS server for the supplicant

MAC filters for traffic control

You can create MAC filters that limit the traffic allowed into and out of specific ports on the switch. The traffic limitations are based on MAC addresses. You can limit the traffic from a MAC address, to a MAC address, or both by selecting one or more source ports and LAGs, one or more destination ports and LAGs, or a combination of both. Traffic from or to the MAC address is rejected on all ports and LAGs that are not defined in the MAC filter for the MAC address.

Note: You can include destination ports and LAGs in a multicast filter only. A multicast filter is determined by the type of MAC address.

Create a MAC filter for a MAC address

You can create MAC filters that limit the traffic allowed into and out of specific ports.

To create a MAC filter for a 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > Traffic Control > MAC Filter**.

   The MAC Filter page displays.

   The following steps refer to the MAC Filter Configuration section.

6. From the **MAC Filter** menu, select **Create Filter**.

   If you did not configure any filters, this is the only option available.

7. From the **VLAN ID** menu, select the VLAN that must be used with the MAC address.
8. In the **MAC Address** field, type the MAC address of the filter in the format XX:XX:XX:XX:XX:XX.

   You cannot define filters for the following MAC addresses:

   - 00:00:00:00:00:00
   - 01:80:C2:00:00:00 to 01:80:C2:00:00:0F
   - 01:80:C2:00:00:20 to 01:80:C2:00:00:21
   - FF:FF:FF:FF:FF:FF

9. In the Source Port Members section, in the Port and LAG tables, select the ports and LAGs that must be included in the inbound filter.

   If a packet with the MAC address and VLAN ID that you specify is received on a port that is not part of the inbound filter, the packet is dropped.

10. In the Destination Port Members section, in the Port and LAG tables, select the ports and LAGs that must be included in the outbound filter.

    A packet with the MAC address and VLAN ID that you specify can be transmitted only from a port that is part of the outbound filter.

Note: You can include destination ports in a multicast filter only. A multicast filter is determined by the MAC address that you enter in the MAC Address field.

11. Click the **Apply** button.

    Your settings are saved.

Delete a MAC filter

You can remove an existing MAC filter that you no longer need.

To delete a MAC filter:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Traffic Control > MAC Filter**.

   The MAC Filter page displays.

   The following steps refer to the MAC Filter Configuration section.
6. From the **MAC Filter** menu, select the MAC filter.
7. Click the **Delete** button.

   Your settings are saved and the MAC filter is removed.

Display the MAC filter summary

You can display the MAC filters that are configured on the switch.

To display the MAC filter summary:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Traffic Control > MAC Filter**.

   The MAC Filter page displays.

   The following information refers to the MAC Filter Summary section.
6. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 70. MAC filter summary information

Field	Description
MAC Address	The MAC address of the filter in the format XX:XX:XX:XX:XX:XX
VLAN ID	The VLAN ID used with the MAC address
Source Port Members	The ports and LAGs that are used to filter inbound packets
Destination Port Members	The ports and LAGs that are used to filter outbound packets for a multicast MAC address

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.

Configure the global storm control settings

The global storm control settings apply to all ports. After you configure the global settings, you can specify storm control settings for individual ports.

To configure the global storm control settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Traffic Control > Storm Control**.

   The Storm Control page displays.

   The following steps refer to the Storm Control section, in which you can globally enable or disable a type of packet to be rate-limited on all ports. For information about individual ports, see Configure the storm control settings for a port on page 352.
6. From the **Ingress Control Mode** menu, select to enable storm control for a specific packet type or disable storm control entirely:
   - **Disabled**: Strom control is disabled entirely. This is the default setting.
   - **Unknown Unicast**: If unknown unicast traffic on a port exceeds the configured threshold and you select **Enable** from the **Status** menu, the switch discards the unknown unicast traffic.

- **Multicast**: If multicast traffic on a port exceeds the configured threshold and you select **Enable** from the **Status** menu, the switch discards the multicast traffic.
- **Broadcast**: If broadcast traffic on a port exceeds the configured threshold and you select **Enable** from the **Status** menu, the switch discards the broadcast traffic.

7. From the **Status** menu, select to enable or disable storm control for the packet type that you select from the **Ingress Control Mode** menu:
   - **Enable**: Storm control for the selected packet type is enabled.
   - **Disable**: Storm control for the selected packet type is disabled. This is the default setting.

   If you disable storm control entirely, the Status menu is also disabled.
8. In the **Threshold** field, type the percentage of the available bandwidth above which a storm control event is triggered.

   Type a percentage from 1 to 100. The default is 5 percent. This means that a storm control event is triggered if more than 5 percent of the available bandwidth is used by traffic of the configured packet type.
9. From the **Control Action** menu, select which action occurs, if any, if a storm control event is triggered:
   - **None**: No further action is taken. This is the default setting.
   - **Trap**: An SNMP trap is sent.
   - **Shutdown**: The port is shut down.
10. Click the **Apply** button.

    Your settings are saved.

Configure the storm control settings for a port

You can specify storm control settings for one or more ports. These settings can override the global storm control settings (see Configure the global storm control settings on page 351).

To configure storm control 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Traffic Control > Storm Control**.

   The Storm Control page displays.

   The following steps refer to the Port Settings section, in which you can enable or disable the globally configured type of storm control for a specific port. For information about the global storm control settings, see Configure the global storm control settings on page 351.
6. Select one or more ports (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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit Storm Control pop-up window displays.
8. From the **Status** menu, select to enable or disable storm control for the packet type that is globally selected (see Configure the global storm control settings on page 351):
   - **Enable**: Storm control for the selected packet type is enabled on the port.
   - **Disable**: Storm control for the selected packet type is disabled on the port. This is the default setting.

   If you disable storm control entirely, the Status menu is also disabled.
9. In the **Threshold** field, type the percentage of the available bandwidth on the port above which a storm control event is triggered.

   Type a percentage from 1 to 100. The default is 5 percent. This means that a storm control event is triggered if more than 5 percent of the available bandwidth on the port is used by traffic of the configured packet type.

10. From the **Control Action** menu, select which action occurs on the port, if any, if a storm control event is triggered:
    - **None**: No further action is taken. This is the default setting.
    - **Trap**: An SNMP trap is sent.
    - **Shutdown**: The port is shut down.
11. Click the **Save** button.

    Your settings are saved.

Port security

Port security lets you lock one or more ports on the switch. When a port is locked, the port can only forward packets if the total number of dynamically learned MAC addresses and the total number of statically added MAC addresses are not exceeded. You can set the thresholds for these numbers. Once a threshold is exceeded, the port discards all other packets.

You can also convert dynamically learned MAC addresses to static MAC addresses and allow traffic from these MAC addresses on a port.

Configure the global port security mode

Before you can enable and configure port security for individual ports, you must globally enable the port security mode for the switch.

To configure the global port security mode:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.

4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Traffic Control > Port Security > Port Security Configuration**.

   The Port Security Configuration page displays.
6. Click the **Port Security Mode** toggle to enable or disable port security:
   - **The toggle is gray and positioned to the left**: Port security is globally disabled on the switch. This is the default setting.
   - **The toggle is purple and positioned to the right**: Port security is globally enabled on the switch.

   The Port Security Violations table shows information about violations that occurred on ports that are enabled for port security.

   Table 71. Port security violations information

Field	Description
Port	The port for which the violation is displayed
Last Violation MAC	The source MAC address of the last packet that was discarded on the locked port
VLAN ID	The VLAN ID corresponding to the last MAC address violation

7. Click the **Apply** button.

   Your settings are saved.

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 is not reached, a packet with an unknown source MAC address is learned and forwarded normally. If the limit is reached, no more addresses are learned on the port. Any packets with source MAC addresses that are not already learned are discarded. You can effectively disable dynamic locking by setting the number of allowable dynamic entries to zero.

Static locking allows you to specify a list of MAC addresses that are allowed on a port (see Display learned MAC addresses and convert them to static addresses on page 357). The behavior of packets is the same as for dynamic locking: only packets with an allowable source MAC address can be forwarded.

To configure port security settings:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > Traffic Control > Port Security > Interface Configuration**.

   The Interface Configuration page displays.

6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

   The Edit Interface Configuration pop-up window displays.

9. From the **Port Security** menu, select to enable or disable port security for the port:
   - **Disabled**: Port security is disabled for the port. This is the default setting.
   - **Enabled**: Port security is enabled for the port.
10. In the **Max Learned MAC Address** field, type the maximum number of MAC addresses that the port can learn dynamically.

    The range is from 0 to 4096. The default setting is 4096.

11. In the **Max Static MAC Address** field, type the maximum number of statically locked MAC addresses that the port can hold.

    The range is from 0 to 48. The default setting is 48.

12. From the **Enable Violation Shutdown** menu, select to enable or disable the shut down of the port if a violation occurs:
    - **No**: The port is not shut down if a violation occurs. This is the default setting.
    - **Yes**: The port is shut down if a violation occurs.

    An example of a violation is an incoming packet from a disallowed MAC address.
13. From the **Enable Violation Traps** menu, select to enable or disable the transmission of an SNMP trap if a violation occurs:
    - **No**: A trap is not sent if a violation occurs. This is the default setting.
    - **Yes**: A trap is sent if a violation occurs.
14. Click the **Save** button.

    Your settings are saved.

Display learned MAC addresses and convert them to static addresses

After you enable port security globally (see Configure the global port security mode on page 354) and enable port security for specific interfaces (see Configure a port security interface on page 355), you can convert a dynamically learned MAC address to a statically locked address.

To display learned MAC addresses for an individual port 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > Traffic Control > Port Security > Security MAC Address**.

   The Security MAC Address page displays.

6. To display the learned MAC addresses for a port or LAG, from the **Port List** menu, select the port or LAG.

   The Number of Dynamic MAC Addresses Learned field displays the number of dynamically learned MAC addresses on a specific port.

   The following table shows the MAC addresses and their associated VLANs learned on the selected port or LAG.

Field	Description
VLAN ID	The VLAN ID corresponding to the MAC address
MAC Address	The MAC addresses learned on port or LAG

7. To refresh the page, click the **Refresh** button.
8. To convert the dynamically learned MAC addresses on the port or LAG to statically locked addresses, click the **Convert Dynamic Address to Static** toggle:
   - **The toggle is gray and positioned to the left**: Address conversion is disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: Address conversion is enabled.
9. Click the **Apply** button.

   Your settings are saved.

   The dynamic MAC address entries are converted to static MAC address entries in a numerically ascending order until the static limit is reached.

Display port security violations

If you enable port security, you can display port security violations.

To display port security violations:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Traffic Control > Port Security > Port Security Configuration**.

   The Port Security Configuration page displays.
6. To refresh the page, click the **Refresh** button.

The Port Security Violations table shows information about violations that occurred on ports on which port security is enabled.

Table 72. Port security violations information

Field	Description
Port	The port for which the violation is displayed
Last Violation MAC	The source MAC address of the last packet that was discarded on the locked port
VLAN ID	The VLAN ID corresponding to the last MAC address violation

Loop protection

Loops inside a network are costly because they consume resources and reduce the performance of the network. Detecting loops manually can be cumbersome.

The switch can automatically identify loops in the network. You can enable loop protection per port or globally.

If loop protection is enabled, the switch sends predefined protocol data unit (PDU) packets to a Layer 2 multicast destination address (09:00:09:09:13:A6) on all ports for which the feature is enabled. You can selectively disable PDU packet transmission for loop protection on specific ports even while port loop protection is enabled. If the switch receives a packet with the previously mentioned multicast destination address, the source MAC address in the packet is compared with the MAC address of the switch. If the MAC address does not match, the packet is forwarded to all ports that are members of the same VLAN, just like any other multicast packet. The packet is not forwarded to the port from which it was received.

If the source MAC address matches the MAC address of the switch, the switch can perform one of the following actions, depending on how you configure the action:

- The port is shut down.
- A log message is generated. (If a syslog server is configured, the log message can be sent to the syslog server.)
- The port is shut down and a log message is generated.

If loop protection is disabled, the multicast packet is silently dropped.

Loop protection is not intended for ports that serve as uplinks between spanning tree–aware switches. Loop protection is designed for unmanaged switches that drop spanning tree bridge protocol data units (BPDUs).

You need to enable the feature globally before you can enable it at the port level so that the system policy filter can be installed.

Loop protection treats PDU packet transmission and spanning tree protocol in the following ways:

- **Loop protection and PDU packet transmission**: Loop protection sends loop protocol packets from all ports on which it is enabled. You can configure the interval (1 to 5 seconds) between two successive loop protection PDU packets. The default interval is 5 seconds. If the switch receives a loop protocol packet on a port for which the action is set to shut down the port, the port can no longer receive and send frames.

  Loop protection operates at a port level, regardless of VLAN assignment and membership, detecting loops across VLANs.
- **Loop protection and Spanning Tree Protocol**: Loop protection does not impact end nodes and is not intended for ports that serve as uplinks between spanning tree–aware switches. Loop protection can coexist with Spanning Tree Protocol (STP). You can enable both loop protection and STP on a port because these features function independently of each other. STP does not bring a port down when a loop is detected but keeps the port in blocking state. Because PDUs are allowed in a blocking state, loop protection packets are received and loop protection brings down the port that is involved in the loop (if the configured action is to shut down the port).

Configure the global loop protection settings

Before you can configure Layer 2 (L2) loop protection for individual ports (see Configure the loop protection settings for interfaces and display the loop protection state on page 362), you must globally enable and configure loop protection.

To globally configure loop protection:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > L2 Loop Protection**.

   The L2 Loop Protection page displays.

   The following steps refer to the Global L2 Loop Protection Configuration section.

6. Click the **L2 Loop Protection** toggle to enable or disable loop protection:
   - **The toggle is gray and positioned to the left**: Loop protection is globally disabled on the switch. This is the default setting.
   - **The toggle is purple and positioned to the right**: Loop protection is globally enabled on the switch.
7. From the **Transmit Interval** menu, select the interval between the transmissions of loop packets on a port.

   You can select from 1 to 10 seconds. The default setting is 5 seconds. The selected interval applies to all ports for which you enable loop protection.

8. From the **Max PDU Receive** menu, select the maximum number of packets that a port can receive before an action is taken.

   You can select from 1 to 10 packets. The default setting is 1 packet. The selected number of packets applies to all ports for which you enable loop protection.

9. In the **Disable Timer** field, type the period in seconds after which a port is disabled if a loop is detected.

   The range is from 0 to 604800 seconds. The default setting is 0 seconds, which means that a port is not disabled if a loop is detected.

10. Click the **Apply** button.

    Your settings are saved.

Configure the loop protection settings for interfaces and display the loop protection state

Before you can configure loop protection for individual ports, you must globally enable loop protection (see Configure the global loop protection settings on page 360).

To enable and configure loop protection for an interface and display the loop protection state 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > L2 Loop Protection**.

   The L2 Loop Protection page displays.
6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**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 (for example, g3) in the **Search** 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. Click the **Edit** button.

The Edit L2 Loop Protection Interface Configuration pop-up window displays.

9. From the **Keep Alive** menu, select to enable or disable loop protection on the port:
   - **Disabled**: Loop protection is disabled on the port. This is the default setting.
   - **Enabled**: Loop protection is enabled on the port.
10. From the **RX Action** menu, select the action that the switch takes when a loop is detected on the port:
    - **Log**: Logs a message when a loop is detected on the port.
    - **Disable**: Disables the port when a loop is detected. This is the default setting.
    - **Both**: Logs a message and disables the port when a loop is detected.
11. Click the **Save** button.

    Your settings are saved.
12. To clear the information in the L2 Loop Protection Interface Configuration table, click the **Clear** button.
13. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 73. Loop protection interface configuration information

Field	Description
Port	The port for which loop detection information is displayed
Loop Detected	Indicates (Yes or No) whether a loop is detected on the port
Loop Count	The number of packets that were received on the port after the loop was detected
Time Since Last Loop	The period since the loop was detected
Port Status	The status of the interface (Enabled or Disabled)

Denial of service

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

Configure Auto-DoS

You can automatically enable all denial of service (DoS) features that are supported on the switch, except for the TCP port and UDP port DoS features, which you must enable manually.

If the switch detects an attack, it shuts down the affected port and logs a warning message. After you have assessed the risk, you can then manually re-enable the port.

To configure Auto-DoS:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Denial of Service**.

   The Denial of Service page displays.
6. In the Auto-DoS Configuration section, click the **Auto-DoS Mode** toggle to enable or disable Auto-DoS:
   - **The toggle is gray and positioned to the left**: Auto-DoS is disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: Auto-DoS is enabled.
7. Click the **Apply** button.

   Your settings are saved.

Configure individual denial of service attack options

You can select which types of denial of service (DoS) attacks the switch monitors and blocks.

If the switch detects an attack, it shuts down the affected port and logs a warning message. After you have assessed the risk, you can then manually re-enable the port.

To configure individual DoS settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > Denial of Service**.

   The Denial of Service page displays.

   The following steps refer to the Denial of Service Configuration section.
6. In the **Denial of Service Min TCP Header Size** field, type the minimum TCP header size allowed.

   If you click the **Denial of Service TCP Fragment** toggle to enable that option, the switch first drops packets for which the first TCP fragments include the following TCP payload:

   `IP_Payload_Length - IP_Header_Size < Min_TCP_Header_Size`.

   Enter a value in the range from 0 to 31. The default setting is 20.
7. In the **Denial of Service Max ICMP Packet Size** field, type the maximum ICMP packet size allowed.

   If you click the **Denial of Service ICMPv4** toggle and **Denial of Service ICMPv6** toggle to enable these options, the switch drops ICMP and ICMPv6 ping packets that exceed the size that you specify. Enter a value in the range from 0 to 16376. The default setting is 512.
8. In the Denial of Service Configuration section, click each DoS option toggle to enable or disable the option:
   - **The toggle is gray and positioned to the left**: The option is disabled. This is the default setting. for all options.
   - **The toggle is purple and positioned to the right**: The option is enabled.

The switch lets you configure the following individual DoS options:

- **Denial of Service ICMPv4**: Enabling ICMPv4 DoS prevention causes the switch to drop ICMPv4 packets with a type set to ECHO_REQ (ping) and a size greater than the ICMPv4 packet size that you configured.
- **Denial of Service ICMPv6**: Enabling ICMPv6 DoS prevention causes the switch to drop ICMPv6 packets with a type set to ECHO_REQ (ping) and a size greater than the ICMPv6 packet size that you configured.
- **Denial of Service Ping of Death**: Enabling Ping of Death DoS prevention causes the switch to drop ICMP ping packet larger than 65535 bytes.
- **Denial of Service IPv6 Fragment**: Enabling IPv6 Fragment DoS prevention causes the switch to drop IPv6 packets for which the header is fragmented, the More flag is set to 1, and the payload length is smaller than 1240.
- **Denial of Service ICMP Fragment**: Enabling ICMP Fragment DoS prevention causes the switch to drop ICMP fragmented packets.
- **Denial of Service Smurf**: Enabling Smurf DoS prevention causes the switch to drop broadcast ICMP echo request packets.
- **Denial of Service SIP=DIP**: Enabling SIP=DIP DoS prevention causes the switch to drop packets with a source IP address equal to the destination IP address.
- **Denial of Service SMAC=DMAC**: Enabling SMAC=DMAC DoS prevention causes the switch to drop packets with a source MAC address equal to the destination MAC address.
- **Denial of Service TCP FIN&URG&PSH**: Enabling TCP FIN & URG & PSH DoS prevention causes the switch to drop packets with TCP flags FIN, URG, and PSH set and the TCP sequence number equal to 0.
- **Denial of Service TCP Flag&Sequence**: Enabling TCP Flag DoS prevention causes the switch to drop packets with TCP control flags set to 0 and the TCP sequence number set to 0.
- **Denial of Service TCP Fragment**: Enabling TCP Fragment DoS prevention causes the switch to drop packets with a TCP payload for which the IP payload length minus the IP header size is less than the minimum allowed TCP header size.
- **Denial of Service TCP Offset**: Enabling TCP Offset DoS prevention causes the switch to drop packets with a TCP header offset set to 1.
- **Denial of Service TCP Port**: Enabling TCP Port DoS prevention causes the switch to drop packets for which the TCP source port is equal to the TCP destination port.
- **Denial of Service TCP Source Port**: Enabling TCP Source Port DoS prevention causes the switch to drop packets when the number of the TCP source port is lower than 1024.

- **Denial of Service TCP SYN&FIN**: Enabling TCP SYN & FIN DoS prevention causes the switch to drop packets with TCP flags SYN and FIN set.
- **Denial of Service TCP SYN&RST**: Enabling TCP SYN & RST DoS prevention causes the switch to drop packets for which the TCP flags SYN and RST are set to 1.
- **Denial of Service UDP Port**: Enabling UDP Port DoS prevention causes the switch to drop packets for which the UDP source port is equal to the UDP destination port.

9. Click the **Apply** button.

   Your settings are saved.

8

Configure Access Control Lists

This chapter covers the following topics:

- About access control lists
- ACL Wizard
- MAC ACLs
- MAC ACL rules
- MAC ACL bindings
- IPv4 ACLs
- Standard IPv4 ACL rules
- Extended IPv4 ACL rules
- IPv6 ACLs
- IPv6 ACL rules
- IP ACL bindings
- Display the existing ACLs and associated rules
- VLAN ACL bindings

Note: For more information about access control lists (ACLs) and configuration examples, see Access control lists (ACLs) on page 493.

About access control lists

Access control lists (ACLs) ensure that only authorized users can access specific resources while blocking any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents, decide which types of traffic are forwarded or blocked, and provide security for the network. The switch supports a total of 100 ACLs, which can be a combination of MAC ACLs, basic IPv4 ACL, extended IPv4 ACLs, and IPv6 ACLs.

If you need a simple ACL, we recommend that you use the ACL Wizard (see ACL Wizard on page 369).

To manually configure an ACL, following these high-level steps:

1. Create a MAC ACL, IPv4 ACL, or IPv6 ACL.
2. For each ACL, create one or more rules, which can identify protocols, source, and destination IP and MAC addresses, and many other packet-matching criteria.
3. Bind the ACL to a port, LAG, or VLAN.

To view ACL configuration examples, see Access control lists (ACLs) on page 493.

ACL Wizard

The ACL Wizard can help you to create a simple ACL and apply it to physical ports, LAGs, or both.

The ACLs that you can create with the ACL Wizard can be based on source or destination MAC address, source or destination IPv4 or IPv6 address, or source or destination IPv4 or IPv6 Layer 4 port.

If you need ACLs with more complex rules, create them manually.

Use the ACL Wizard to create a simple ACL

The ACL Wizard can help you to 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.

To use the ACL Wizard to create a simple 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > ACL > ACL Wizard**.

   The ACL Wizard page displays

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. Click the **Add New** button.

   The Add ACL pop-up window display. The name of the window includes the type of ACL that you selected.

8. In the **Sequence Number** field, enter a number in the range from 1 to 2147483647 that is used to identify the rule.

   Note: The ACL Wizard automatically assignes a name to the ACL. The name includes the term *ACL_Wizard*.

9. From the **Action** menu, select the action that must occur if a packet matches the rule's criteria.
   - **Permit**: The packet is permitted and forwarded.
   - **Deny**: The packet is denied and dropped.

10. From the **Match Every** menu, select if packets must match the ACL and rule:
    - **False**: Packets do not need to match the selected ACL and rule. With this selection, you can add additional criteria for the rule.
    - **True**: All packets must match the selected ACL and rule and are either permitted or denied. With this selection, because all packets must match the rule, you cannot configure other match criteria for the rule.

11. If you select **False** from the **Match Every** menu, set the additional match criteria for the selected ACL type.

    The rule match criteria fields that display in the window 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**: Type the destination MAC address to compare against an Ethernet frame. The format is xx:xx:xx:xx:xx:xx. The BPDU keyword might be specified using a destination MAC address of 01:80:C2:xx:xx:xx. • **Destination MAC Mask**: Type the destination MAC address mask, which represents the bits in the destination MAC address to compare against an Ethernet frame. The format is xx:xx:xx:xx:xx:xx. The BPDU keyword might be specified using a destination MAC mask of 00:00:00:ff:ff:ff. • **VLAN**: Type the VLAN ID to match within the Ethernet frame.
Source MAC	• **Source MAC**: Type the source MAC address to compare against an Ethernet frame. The format is xx:xx:xx:xx:xx:xx. • **Source MAC Mask**: Type the source MAC address mask, which represents the bits in the source MAC address to compare against an Ethernet frame. The format is (xx:xx:xx:xx:xx:xx). • **VLAN**: Type the VLAN ID to match within the Ethernet frame.

(Continued)

ACL Based On	Fields
Destination IPv4	• **Destination IP Address**: Type the destination IP address. • **Destination IP Mask**: Type the destination IP address mask.
Source IPv4	• **Source IP Address**: Type the source IP address. • **Source IP Mask**: Type the source IP address mask.
Destination IPv6	• **Destination Prefix**: Type the destination prefix. • **Destination Prefix Length**: Type the destination prefix length.
Source IPv6	• **Source Prefix**: Type the source destination prefix. • **Source Prefix Length**: Type the source prefix length.
Destination IPv4 L4 Port	• **Destination L4 port (Protocol)**: Select the destination IPv4 L4 port protocol, or select **Other** and manually set the destination IPv4 L4 port value. • **Destination L4 port (Value)**: If you select **Other**, type the destination IPv4 L4 port value.
Source IPv4 L4 Port	• **Source L4 port (Protocol)**: Select the source IPv4 L4 port protocol, or select **Other** and manually set the source IPv4 L4 port value. • **Source L4 port (Value)**: If you select **Other**, type the source IPv4 L4 port value.
Destination IPv6 L4 Port	• **Destination L4 port (Protocol)**: Select the destination IPv6 L4 port protocol, or select **Other** and manually set the destination IPv6 L4 port value. • **Destination L4 port (Value)**: If you select **Other**, type the destination IPv6 L4 port value.
Source IPv6 L4 Port	• **Source L4 port (Protocol)**: Select the source IPv6 L4 port protocol, or select **Other** and manually set the source IPv6 L4 port value. • **Source L4 port (Value)**: If you select **Other**, type the source IPv6 L4 port value.

As an example, the following steps describe how you can create an ACL based on the destination MAC address:

a. In the **Destination MAC** field, type the destination MAC address that must be compared against the information in an Ethernet frame.

   The format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC address of 01:80:C2:xx:xx:xx.

b. In the **Destination MAC Mask** field, type the destination MAC address mask that must be compared against the information in an Ethernet frame.

The format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC mask of 00:00:00:ff:ff:ff.

c. In the **VLAN** field, type the VLAN ID against which the information in an Ethernet frame must be compared.

The range is from 1 to 4093. You can type an individual VLAN ID or a range of VLAN IDs.

12. Click the **Save** button.

The ACL and associated rule are saved and display on the ACL Wizard table.

Note: The ACL and associated rule display *only* while you remain on the page. If you go to another page and then return to the ACL Wizard page, the ACL and associated rule no longer display. To display rules that you created with the ACL Wizard, see Display the existing ACLs and associated rules on page 417.

13. In the Binding Configuration section, in the Ports and LAG tables, select the ports and LAGs to which the ACL must be bound.

A selected port or LAG displays blue. An excluded port or LAG displays blank.

Note: The selection from the **Direction** menu is always **Inbound**. You cannot change this selection. An ACL is always applied to incoming traffic only.

14. Click the **Apply** button.

Your settings are saved.

Change an ACL rule that you created with the ACL Wizard

For an ACL rule that you created with the ACL Wizard, you can do the following:

- Change the match criteria.
- Change the binding.

Note: An ACL and associated rule display *only* while you remain on the ACL Wizard page after you created the ACL. If you go to another page and then return to the ACL Wizard page, the ACL and associated rule no longer display, and you cannot change the rule on the ACL Wizard page. To display rules that you created with the ACL Wizard and for information about how to change the match criteria of a rule, see Display the existing ACLs and associated rules on page 417.

To change an ACL rule that you just created with the ACL Wizard while you remain on the ACL Wizard page:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > ACL Wizard**.

   The ACL Wizard page displays.
6. From the **ACL Type** menu, select the type of ACL.

   The page adjusts to display the ACLs that you created for the type of ACL.
7. To change the match criteria, do the following:
   a. Select the check box for the ACL.
   b. Click the **Edit** button.

      The Edit ACL pop-up window display. The name of the window includes the type of ACL that you selected.
   c. Change the setting as needed.

      For more information, see Use the ACL Wizard to create a simple ACL on page 369.
   d. Click the **Save** button.

      Your settings are saved.
8. To change the binding, do the following:
   a. Select the check box for the rule.
   b. In the Binding Configuration section, in the Ports and LAG tables, clear the ports and LAGs that you no longer want to use for the binding and select the new ports and LAGs to which the ACL must be bound.

A selected port or LAG displays blue. An excluded port or LAG displays blank.

Note: The selection from the **Direction** menu is always **Inbound**. You cannot change this selection. An ACL is always applied to incoming traffic only.

9. Click the **Apply** button.

   Your settings are saved.

Remove an ACL that you created with the ACL Wizard

You can remove an ACL that you no longer need.

Note: An ACL and associated rule display *only* while you remain on the ACL Wizard page after you created the ACL. If you go to another page and then return to the ACL Wizard page, the ACL and associated rule no longer display, and you cannot remove the rule on the ACL Wizard page. To display rules that you created with the ACL Wizard and for information about how to remove an ACL, see Display the existing ACLs and associated rules on page 417.

To remove an ACL that you just created with the ACL Wizard while you remain on the ACL Wizard page:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > ACL > ACL Wizard**.

   The ACL Wizard page displays.

6. From the **ACL Type** menu, select the type of ACL.

   The page adjusts to display the ACLs that you created for the type of ACL.
7. Select the check box for the ACL.
8. Click the **Delete** button.

   Your settings are saved and the ACL is removed.

MAC ACLs

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 applied, and any additional rules are not checked for a match. You must associate the MAC ACL with one or more interfaces.

Multiple steps are involved in defining a MAC ACL and applying it to the switch:

1. Create a MAC ACL (see Add a MAC ACL on page 376).
2. Create a MAC rule (see MAC ACL rules on page 379).
3. Bind (associate) the MAC ACL with one or more interfaces (see Configure a MAC ACL interface binding on page 384).

   You can display or delete MAC ACL binding configurations in the MAC binding table (see Display or delete MAC ACL bindings on page 385).

Add a MAC ACL

Configuring a MAC ACL is a two-step process: First, you add the MAC ACL. Then, you add rules to the 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > MAC ACL > MAC ACL/Rules**.

   The MAC ACL/Rules page displays.

   The MAC ACL Configuration section displays the total number of MAC ACLs, IPv4 ACLs, and IPv6 ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. Click the **Add New** button.

   The Add MAC ACL/Rule pop-up window displays.
7. Select the **Add New ACL only** radio button.
8. In the **ACL Name** field, type a name for the MAC ACL.

   The name string can include letters, numbers, hyphens, underscores, and spaces. The name must start with a letter.
9. Click the **Save** button.

   The MAC ACL is added. You can now add a rule for the MAC ACL (see Add a rule for a MAC ACL on page 379).

   Each configured MAC 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 is blank or Inbound. (If the ACL is not bound to an interface, the direction is blank.)

Change the name of a MAC ACL

You can change the name of an existing 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > MAC ACL > MAC ACL/Rules**.

   The MAC ACL/Rules page displays.

   The MAC ACL Configuration section displays the total number of MAC ACLs, IPv4 ACLs, and IPv6 ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. In the MAC ACL/Rule Table section, select the check box for the MAC ACL.
7. Click the **Edit** button.

   The Edit MAC ACL/Rule pop-up window displays.
8. In the **ACL Name** field, type a new name.
9. Click the **Save** button.

   Your settings are saved.

Remove a MAC ACL

You can remove a MAC ACL that you no longer need.

To remove 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > MAC ACL > MAC ACL/Rules**.

   The MAC ACL/Rules page displays.

   The MAC ACL Configuration section displays the total number of MAC ACLs, IPv4 ACLs, and IPv6 ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. In the MAC ACL/Rule Table section, select the check box for the MAC ACL.
7. Click the **Delete** button.

   Your settings are saved and the MAC ACL is removed.

MAC ACL rules

You can define rules for MAC-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

Note: An implicit “deny all” rule is included at the end of a list with ACL rules. 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 MAC ACL

Configuring a MAC ACL is a two-step process: After you add a MAC ACL, you can add rules to the 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > MAC ACL > MAC ACL/Rule**.

   The MAC ACL/Rule Table page displays.

   The MAC ACL Configuration section displays the total number of MAC ACLs, IPv4 ACLs, and IPv6 ACLs that *are* configured on the switch and the maximum number of ACLs that *can be* configured.
6. Click the **Add New** button.

   The Add MAC ACL/Rule pop-up window displays.
7. Select the **Add a Rule to existing ACL** radio button.

   The window adjusts.
8. From the **Name** menu, select the MAC ACL.
9. In the **Sequence Number** field, enter a number in the range from 1 to 2147483647 to identify the rule.
10. From the **Action** menu, select the action that must be taken if a packet matches the rule's criteria:

    - **Permit**: Forwards packets that meet the ACL criteria.
    - **Deny**: Drops packets that meet the ACL criteria.

    Note: In the following steps, configure the criteria that you need for the rule. You do not need to configure all criteria.
11. In the **Assign Queue ID** field, type the hardware egress queue ID that must be used to handle all packets matching this ACL rule.

    The range for the queue ID is from 0 to 7.
12. From the **Mirror Interface** menu, select the egress interface to which the matching traffic stream must be copied, in addition to being forwarded normally by the switch.

    This option is configurable only for a Permit action. A mirror interface and a redirect interface are mutually exclusive. Set either one or the other.
13. From the **Redirect Interface** menu, select the egress interface to which the matching traffic stream must be redirected, bypassing any forwarding decision normally performed by the switch.

    This option is configurable only for a Permit action. A redirect interface and a mirror interface are mutually exclusive. Set either one or the other.

14. From the **Match Every** menu, select if each Layer 2 MAC packet must be matched against the rule:
    - **False**: Not all packets need to match the ACL rule.
    - **True**: Each packet must match the ACL rule.
15. In the **CoS** field, type the 802.1p priority that must be compared against the information in an Ethernet frame.

    The range for the priority is from 0 to 7.
16. In the **Destination MAC** field, type the destination MAC address that must be compared against the information in an Ethernet frame.

    The format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC address of 01:80:C2:xx:xx:xx.
17. In the **Destination MAC Mask** field, type the destination MAC address mask that must be compared against the information in an Ethernet frame.

    The format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC mask of 00:00:00:ff:ff:ff.
18. From the **EtherType Key** menu, select the EtherType value that must be compared against the information in an Ethernet frame:
    - **Apple Talk**
    - **IBM SNA**
    - **IPv4**
    - **IPv6**
    - **IPX**
    - **MPLS Multicast**
    - **MPLS Unicast**
    - **NetBios**
    - **Novell**
    - **PPPOE**
    - **RARP**
    - **User Value**
19. If you select **User Value** from the **EtherType Key** menu, in the **EtherType User Value** field, type the customized EtherType value that must be used.

    This value must be compared against the information in an Ethernet frame. The range is from 0x0600 to 0xFFFF.

20. In the **Source MAC** field, type the source MAC address that must be compared against the information in an Ethernet frame.

    The format is xx:xx:xx:xx:xx:xx.

21. In the **Source MAC Mask** field, type the source MAC address mask that must be compared against the information in an Ethernet frame.

    The format is xx:xx:xx:xx:xx:xx.

22. In the **VLAN** field, type the VLAN ID that must be compared against the information in an Ethernet frame.

    The range is from 1 to 4093. You can type an individual VLAN ID or a range of VLAN IDs.

23. From the **Logging** menu, select to enable or disable logging for the ACL rule:
    - **Disabled**: Logging is disabled for this ACL rule.
    - **Enabled**: 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 five-minute report interval.

24. Click the **Save** button.

    The rule is added to the MAC ACL.

    Each ACL displays the following information:

    - **Rules**: The number of rules currently in place for the MAC ACL.
    - **Direction**: The direction of packet traffic affected by the MAC ACL, which is blank or Inbound. (If the ACL is not bound to an interface, the direction is blank.)

Change the match criteria for a MAC ACL rule

You can change the match criteria for an existing MAC ACL rule.

To change the match criteria for a MAC 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > MAC ACL > MAC ACL/Rules**.

   The MAC ACL/Rules page displays.

   The MAC ACL Configuration section displays the total number of MAC ACLs, IPv4 ACLs, and IPv6 ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. In the MAC ACL/Rule Table section, click the name of the MAC ACL with which the rule is associated.

   The name of the MAC ACL is a hyperlink.

   The rules that are associated with the MAC ACL display.
7. Select the check box for the rule.
8. Click the **Edit** button.

   The Edit MAC ACL/Rule pop-up window displays.
9. Change the settings as needed.

   For more information about the settings, see Add a rule for a MAC ACL on page 379.

   You cannot change the sequence number.
10. Click the **Save** button.

    Your settings are saved.

Remove a rule from a MAC ACL

You can remove a rule from a MAC ACL if you no longer need the rule. When you remove a rule, the rule is deleted.

To remove a rule from 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > MAC ACL > MAC ACL/Rules**.

   The MAC ACL/Rules page displays.

   The MAC ACL Configuration section displays the total number of MAC ACLs, IPv4 ACLs, and IPv6 ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. In the MAC ACL/Rule Table section, click the name of the MAC ACL with which the rule is associated.

   The name of the MAC ACL is a hyperlink.

   The rules that are associated with the MAC ACL display.
7. Select the check box for the rule.
8. Click the **Delete** button.

   Your settings are saved and the rule is removed.

MAC ACL bindings

When you bind a MAC ACL to an interface, all the rules that are defined for the ACL are applied to the selected interface.

Configure a MAC ACL interface binding

You can bind an MAC ACL to one or more interfaces, which can be physical ports, LAGs, or both.

To bind a MAC 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > MAC ACL > MAC Binding Configuration**.

   The MAC Binding Configuration page displays.
6. From the **ACL ID** menu, select the MAC ACL.

   Note: The selection from the **Direction** menu is always **Inbound**. The MAC ACL is applied to incoming traffic only.
7. In the **Sequence Number** field, type a number to define the order of the MAC ACL relative to other ACLs that are bound to the interface.

   A low number indicates a high precedence order. If a sequence number is already in use for the interface, the MAC ACL replaces the currently attached ACL using that sequence number. If you do not set the sequence number, a sequence number that is one number greater than the highest sequence number currently in use for the interface is used. The range is from 1 to 4294967295.
8. In the Ports table, LAG table, or both, click the ports and LAGs to which the MAC ACL must be bound.

   A selected port or LAG displays blue. An excluded port or LAG displays blank.
9. Click the **Apply** button.

   Your settings are saved.

Display or delete MAC ACL bindings

You can display or delete the MAC ACL bindings in the MAC binding table.

To display MAC ACL bindings or delete a MAC ACL binding:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > MAC ACL > Binding Table**.

   The 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 ACL Binding Table.

Table 74. Interface MAC ACL binding information

Field	Description
Interface	The interface to which the MAC ACL is bound
Direction	The packet filtering direction for the MAC ACL, which is always inbound
ACL Type	The type of ACL, which is always MAC ACL
ACL ID	The ACL name
Sequence Number	The sequence number signifying the order of the MAC ACL relative to other ACLs bound to the interface

IPv4 ACLs

An IPv4 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 applied, and the additional rules are not checked for a match. You must associate the IPv4 ACL with one or more interfaces.

The switch supports standard and extended IPv4 ACLs:

- **Standard IPv4 ACL**: Lets the switch permit or deny traffic from a source IP address.
- **Extended IPv4 ACL**: Lets the switch 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 much more granularity and filtering capabilities than the standard IPv4 ACL.

Multiple steps are involved in defining an IPv4 ACL and applying it to the switch:

1. Add an IPv4 ACL (see Add an IPv4 ACL on page 387):
   - **Numbered ACL from 1 to 99**: Creates a standard IPv4 ACL.
   - **Numbered ACL from 100 to 199**: Creates an extended IPv4 ACL.
   - **Named IP ACL**: Creates an extended IPv4 ACL with a name string that is up to 31 alphanumeric characters in length. The name must start with a letter.
2. Create an IPv4 rule (Add a rule for a standard IPv4 ACL on page 391 or Add a rule for an extended IPv4 ACL on page 396).
3. Bind (associate) the IPv4 ACL with one or more interfaces (see Configure an IP ACL interface binding on page 415).

   You can display or delete IPv4 ACL binding configurations in the IP ACL Binding table (see Display or delete IP ACL bindings on page 416).

Add an IPv4 ACL

You can add an IPv4 ACL and then add a rule later. The following procedure describes how to add an IPv4 ACL only. You can also add an IPv4 ACL and a rule together, as one task (see Add a rule for a standard IPv4 ACL on page 391 or Add a rule for an extended IPv4 ACL on page 396).

This procedure applies to standard and extended IPv4 ACLs.

To add an IPv4 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > ACL > IP ACL > IP ACL/Rules**.

   The IP ACL/Rules page displays.

   The IP ACL Configuration section displays the total number of IPv4 ACLs, IPv6 ACLs, and MAC ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.

6. Click the **Add New** button.

   The Add IP ACL/Rule pop-up window displays.

7. In the **Name** field, type a number or name for the IP ACL:

   - **Number from 1–99**: Creates a standard IP ACL, which allows you to permit or deny traffic from a source IP address.
   - **Number from 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.
   - **Name**: Creates an extended IP ACL with a name string that is up to 31 alphanumeric characters in length. The name must start with a letter.

8. Click the **Add** button.

   The IP ACL is added. You can now add a rule for the IPv4 ACL (see Add a rule for a standard IPv4 ACL on page 391 or Add a rule for an extended IPv4 ACL on page 396). Each configured IPv4 ACL displays the following information:

   - **Rules**: The number of rules currently configured for the IPv4 ACL.
   - **Type**: Identifies the ACL as a standard IP ACL (with an ID from 1 to 99), extended IP ACL (with an ID from 100 to 199), or named ACL (which is also an extended ACL).

Change the number or name of an IPv4 ACL

You can change the number or name of an existing IPv4 ACL.

This procedure applies to standard and extended IPv4 ACLs.

To change the number or name of an IPv4 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > IP ACL > IP ACL/Rules**.

   The IP ACL/Rules page displays.

   The IP ACL Configuration section displays the total number of IPv4 ACLs, IPv6 ACLs, and MAC ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. In the IP ACL/Rule Table section, select the check box for the IP ACL.
7. Click the **Edit** button.

   The Edit IP ACL/Rule pop-up window displays.
8. In the **Name** field, type a new number or name.

   - **Number from 1–99**: Applies to a standard IP ACL.
   - **Number from 100–199**: Applies to an extended IP ACL.
   - **IP ACL name**: Applies to an extended IP ACL with a name string that is up to 31 alphanumeric characters in length. The name must start with a letter.
9. Click the **Save** button.

   Your settings are saved.

Remove an IPv4 ACL

You can remove a standard or extended IPv4 ACL that you no longer need.

This procedure applies to standard and extended IPv4 ACLs.

To remove an IPv4 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > IP ACL > IP ACL/Rules**.

   The IP ACL/Rules page displays.

   The IP ACL Configuration section displays the total number of IPv4 ACLs, IPv6 ACLs, and MAC ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. In the IP ACL/Rule Table section, select the check box for the IP ACL.
7. Click the **Delete** button.

   Your settings are saved and the IP ACL is removed.

Standard IPv4 ACL rules

You can define rules for standard IPv4-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

Note: An implicit “deny all” rule is included at the end of a list with ACL rules. 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 standard IPv4 ACL

If you already added a standard IPv4 ACL, you can add a rule to the ACL. You can also add a standard IPv4 ACL and a rule together, as one task. The following procedure describes both options.

To add a rule for an existing or new standard IPv4 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > IP ACL > IP ACL/Rules**.

   The IP ACL/Rules page displays.

   The IP ACL Configuration section displays the total number of IPv4 ACLs, IPv6 ACLs, and MAC ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. Click the **Add New** button.

   The Add IP ACL/Rule pop-up window displays.
7. Select the **Add Rule to existing ACL or Add new ACL and Rule** button.

   The window adjusts.
8. Click the **Standard IP ACL** button.

   This button is selected by default.
9. Click the **Add** button.

   The window closes, and the Standard ACL Rule Configuration (1-99) section displays.
10. Do one of the following:

- **Add a rule to an existing standard IP ACL**: From the **ACL ID/Name** menu, select the ACL.
- **Add a rule to a new standard IP ACL**:
  a. From the **ACL ID/Name** menu, select **Add ACL**.

     The ACL Name field displays.

  b. In the **ACL Name** field, type a number in the range from 1 to 99 for a standard IP ACL.

11. In the **Sequence Number** field, enter a number in the range from 1 to 2147483647 to identify the rule.

    An IP ACL can contain up to 50 rules.

12. Select an Action radio button to set the action that must be taken if a packet matches the rule's criteria, and configure options that are available with your selection:

    - **Permit**: Forwards packets that meet the ACL criteria. You can configure an egress queue and you can let the switch mirror or redirect traffic to a specific interface. See the steps further down in this procedure.
    - **Deny**: Drops packets that meet the ACL criteria. You can enable logging. See the step further down in this procedure.

    Note: In the following steps, configure the criteria that you need for the rule. You do not need to configure all criteria.

13. (Optional) If you select the **Permit** Action radio button, select a hardware egress queue ID from the **Egress Queue** menu.

    This queue is used to handle all packets matching this IP ACL rule. The range for the queue ID is from 0 to 7.

14. (Optional) If you select the **Deny** Action radio button, click the **Logging** toggle to enable logging for the ACL rule:

    - **The toggle is gray and positioned to the left**: Logging is disabled for this ACL rule. This is the default setting.
    - **The toggle is purple and positioned to the right**: Logging is enabled for this ACL rule (subject to resource availability on the switch).

15. From the **Match Every** menu, select if all packets must match the IP ACL rule:

    - **Disable**: Not all packets need to match the ACL rule. You can configure the source IP address and mask. See the step further down in this procedure.
    - **Enable**: Each packet must match the ACL rule. You cannot configure the source IP address and mask.

16. (Optional) If you select the **Permit** Action radio button, select an Interface radio button to let the switch mirror or redirect traffic to a specific interface:

- **Mirror**: From the menu, select the egress interface to which the matching traffic stream must be copied, in addition to being forwarded normally by the switch.

  A mirror interface and a redirect interface are mutually exclusive.
- **Redirect**: From the menu, select the egress interface to which the matching traffic stream must be redirected, bypassing any forwarding decision normally performed by the switch.

  A redirect interface and a mirror interface are mutually exclusive.

17. If you select **Disable** from the **Match Every** menu, configure the source IP address and mask:
    - In the **Source IP Address** field, type the IP address that must be compared against the packet's source IP address.
    - In the **Source IP Mask** field, type the IP mask that must be compared against the packet's source IP mask.
18. Click one of the following buttons:
    - **Save**: To save your settings, click the **Save** button.

      The rule is added to the IP ACL.

      Each ACL displays the following information:
      - **Rules**: The number of rules for the IP ACL.
      - **Type**: The type of IP ACL (Standard IP ACL, Extended IP ACL, or Named IP ACL).
    - **Clear**: To clear the settings so that you can specify other settings before you save them, click the **Clear** button.
    - **Back**: To cancel the settings and return to the initial IP ACL/Rules page with the IP ACL/Rule Table section, click the **Back** button.

Change the match criteria for a standard IPv4 ACL rule

You can change the match criteria for an existing standard IPv4 ACL rule.

To change the match criteria for a standard IPv4 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > IP ACL > IP ACL/Rules**.

   The IP ACL/Rules page displays.

   The IP ACL Configuration section displays the total number of IPv4 ACLs, IPv6 ACLs, and MAC ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. In the IP ACL/Rule Table section, click the number of the IP ACL with which the rule is associated.

   The number of the IP ACL is a hyperlink.

   The rules that are associated with the IP ACL display.
7. Select the check box for the rule.
8. Click the **Edit** button.

   The page adjusts and displays the Standard ACL Rule Configuration (1-99) section.
9. Change the settings as needed.

   For more information about the settings, see Add a rule for a standard IPv4 ACL on page 391.

   You cannot change the ACL ID, name, or sequence number.
10. Click the **Save** button.

    Your settings are saved.

Remove a rule from a standard IPv4 ACL

You can remove a rule from a standard IPv4 ACL if you no longer need the rule. When you remove a rule, the rule is deleted.

To remove a rule from a standard IPv4 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > IP ACL > IP ACL/Rules**.

   The IP ACL/Rules page displays.

   The IP ACL Configuration section displays the total number of IPv4 ACLs, IPv6 ACLs, and MAC ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. In the IP ACL/Rule Table section, click the number of the IP ACL with which the rule is associated.

   The number of the IP ACL is a hyperlink.

   The rules that are associated with the IP ACL display.
7. Select the check box for the rule.
8. Click the **Delete** button.

   Your settings are saved and the rule is removed.

Extended IPv4 ACL rules

You can define rules for extended IPv4-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

Note: An implicit “deny all” rule is included at the end of a list with ACL rules. This means that if an ACL is applied to a packet and 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 IPv4 ACL

If you already added an extended IPv4 ACL, you can add a rule to the ACL. You can also add an extended IPv4 ACL and a rule together, as one task. The following procedure describes both options.

To add a rule for an existing or new extended IPv4 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > IP ACL > IP ACL/Rules**.

   The IP ACL/Rules page displays.

   The IP ACL Configuration section displays the total number of IPv4 ACLs, IPv6 ACLs, and MAC ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. Click the **Add New** button.

   The Add IP ACL/Rule pop-up window displays.
7. Select the **Add Rule to existing ACL or Add new ACL and Rule** button.

   The window adjusts.
8. Click the **Extended IP ACL** button.
9. Click the **Add** button.

   The window closes, and the Extended ACL Rule Configuration (100-199) section displays.
10. Do one of the following:

- **Add a rule to an existing extended IP ACL**: From the **ACL ID/Name** menu, select the ACL.
- **Add a rule to a new extended IP ACL**:
  a. From the **ACL ID/Name** menu, select **Add ACL**.

     The ACL Name field displays.

  b. In the **ACL Name** field, type a number in the range from 100 to 199 or a name of up to 31 characters for an extended IP ACL.

11. In the **Sequence Number** field, type a number in the range from 1 to 2147483647 to identify the rule.

    An IP ACL can contain up to 50 rules.

12. Select an Action radio button to set the action that must be taken if a packet matches the rule's criteria, and configure options that are available with your selection:

    - **Permit**: Forwards packets that meet the ACL criteria. You can configure an egress queue and you can let the switch mirror or redirect traffic to a specific interface. See the steps further down in this procedure.
    - **Deny**: Drops packets that meet the ACL criteria. You can enable logging. See the step further down in this procedure.

    Note: In the following steps, configure the criteria that you need for the rule. You do not need to configure all criteria.

13. (Optionally) If you select the **Permit** Action radio button, select a hardware egress queue ID from the **Egress Queue** menu.

    This queue is used to handle all packets matching this IP ACL rule. The range for the queue ID is from 0 to 7.

14. (Optionally) If you select the **Deny** Action radio button, click the **Logging** toggle to enable logging for the ACL rule:

    - **The toggle is gray and positioned to the left**: Logging is disabled for this ACL rule. This is the default setting.
    - **The toggle is purple and positioned to the right**: Logging is enabled for this ACL rule (subject to resource availability on the switch).

15. (Optionally) If you select the **Permit** Action radio button, select an Interface radio button to let the switch mirror or redirect traffic to a specific interface:

    - **Mirror**: From the menu, select the egress interface to which the matching traffic stream must be copied, in addition to being forwarded normally by the switch.

      A mirror interface and a redirect interface are mutually exclusive.

    - **Redirect**: From the menu, select the egress interface to which the matching traffic stream must be redirected, bypassing any forwarding decision normally performed by the switch.

A redirect interface and a mirror interface are mutually exclusive.

16. From the **Match Every** menu, select if all packets must match the IP ACL rule:

    - **False**: Not all packets need to match the ACL rule. You can configure other match criteria on the page.
    - **True**: Each packet must match the ACL rule. You cannot configure other match criteria on the page.

      If you select **True**, go to Step 26.

17. From the **Protocol Type** menu, select a protocol that a packet's IP protocol must be matched against:

    IP, **ICMP**, **IGMP**, **TCP**, **UDP**, **EIGRP**, **GRE**, **IPINIP**, **OSPF**, **PIM**, or **Other**.

    The protocol selection determines the options that are available on the page.

    If you select **Other**, type a protocol number from **0** to **255** in the **Other Protocol Type** field. Then, continue with Step 25.

18. In the Src (source) section, select to set an individual IP source address and subnet mask or a source IP host address:

    You can select the **IP Address** radio button or the **Host** radio button:

    - **IP Address**: In the **IP Address** field, type a source IP address. In the **Subnet Mask** field, type a source IP mask, type a relevant wildcard mask, or leave the field empty, which means *any*.

      The IP address and subnet mask are compared to a packet's source IP address and subnet mask.

    - **Host**: In the **IP Address** field, type a source host name.

      The host name (or the IP address associated with the name) is compared to a packet's source host name (or the IP address associated with the name).

19. If you select **TCP** or **UDP** from the **Protocol Type** menu, in the Src L4 (source Layer 4) section, select to set an individual port number or a range of port numbers:

    You can select the **Port** radio button or the **Range** radio button:

    - **Port**: Select one of the following protocols from the menu:
      - The source IP TCP port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **www-http**, **smtp**, **telnet**, **pop2**, **pop3**, and **bgp**. A selected protocol translates into its equivalent port number.
      - The source IP UDP port protocols are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **tftp**. A selected protocol translates into its equivalent port number.
      - Select **Other** to type a port number from 0 to 65535 in the rightmost field. The matching condition is always Equal (see the middle field).

The source port is compared to a packet's source port.

- **Range**: Define a range by selecting a protocol from the **Start Port** menu and a protocol from the **End Port** menu:
  - The source IP TCP port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **www-http**, **smtp**, **telnet**, **pop2**, **pop3**, and **bgp**. A selected protocol translates into its equivalent port number.
  - The source IP UDP port protocols are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **tftp**. A selected protocol translates into its equivalent port number.
  - Select **Other** to type a port number from 0 to 65535 in the rightmost field.

  The source port range is compared to a packet's source port range.

20. In the Dst (destination) section, select to set an individual IP destination address and subnet mask or a destination IP host address:

    You can select the **IP Address** radio button or the **Host** radio button:

    - **IP Address**: In the **IP Address** field, type a destination IP address. In the **Subnet Mask** field, type a destination IP mask, type a relevant wildcard mask, or leave the field empty, which means *any*.

      The IP address and subnet mask are compared to a packet's destination IP address and subnet mask.
    - **Host**: In the **IP Address** field, type a destination host name.

      The host name (or the IP address associated with the name) is compared to a packet's destination host name (or the IP address associated with the name).

21. If you select **TCP** or **UDP** from the **Protocol Type** menu, in the Dst L4 (destination Layer 4) section, select to set an individual port number or a range of port numbers:

    You can select the **Port** radio button or the **Range** radio button:

    - **Port**: Select one of the following protocols from the menu:
      - The destination IP TCP port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **www-http**, **smtp**, **telnet**, **pop2**, **pop3**, and **bgp**. A selected protocol translates into its equivalent port number.
      - The destination IP UDP port protocols are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **tftp**. A selected protocol translates into its equivalent port number.
      - Select **Other** to type a port number from 0 to 65535 in the rightmost field. The matching condition is always Equal (see the middle field).

      The destination port is compared to a packet's destination port.
    - **Range**: Define a range by selecting a protocol from **Start Port** menu and a protocol from the **End Port** menu:

- The destination IP TCP port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **www-http**, **smtp**, **telnet**, **pop2**, **pop3**, and **bgp**. A selected protocol translates into its equivalent port number.
- The destination IP UDP port protocols are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **tftp**. A selected protocol translates into its equivalent port number.
- Select **Other** to type a port number from 0 to 65535 in the rightmost field.

The destination port range is compared to a packet's destination port range.

22. If you select **IGMP** from the **Protocol Type** menu, set the IGMP message type.

    The range is from 0 to 255. If you leave the field empty, it means any IGMP message type.

    The IGMP message type is compared to a packet's IGMP message type.

23. If you select **ICMP** from the **Protocol Type** menu, select either the **Type** or **Message** radio button:

    - If you select the **Type** radio button, type a code in the left field. To set a range of codes, type a code in the left field and another code in the **Code** field (the right field).

      The range is from 0 to 255. If you leave the field empty, it means any ICMP type.

      The ICMP type is compared to a packet's ICMP type.

    - If you select the **Message** radio button, from the menu, select the type of the ICMP message:

      echo, **echo-reply**, **host-redirect**, **mobile-redirect**, **net-redirect**, **net-unreachable**, **redirect**, **packet-too-big**, **port-unreachable**, **source-quench**, **router-solicitation**, **router-advertisement**, **ttl-exceeded**, **time-exceeded**, or **unreachable**.

      Specifying a type of message implies that both the ICMP type and ICMP code are specified. That is, the ICMP message is decoded into the corresponding ICMP type and ICMP code within the ICMP type and compared to a packet's type of the ICMP message.

24. (Optionally) Click the **Fragments** toggle to allow initial fragments (that is, the fragment bit is asserted) or prevent initial fragments from being used:

    - **The toggle is gray and positioned to the left**: Initial fragments are not allowed. This is the default setting.
    - **The toggle is purple and positioned to the right**: Initial fragments are allowed.

    This option is not valid for rules that match L4 information such as a TCP port number, because that information is carried in the initial packet.

25. (Optionally) In the Service Type section, select the **IP DSCP**, **IP Precedence**, or **IP TOS** radio button to set a match criterion for the service type field in a packet's IP header.

    IP DSCP, IP precedence, and IP ToS are alternative methods to specify a match criterion for the same service type field in a packet's IP header. Each method uses a different user notation. After you make a selection, you can set a value.

    - **IP DSCP**: The IP DiffServ Code Point (DSCP) field in a packet is defined as the high-order 6 bits of the service type octet in the IP header. Select a keyword from the **IP DSCP** menu. If you select **Other**, type a number from 0 to 63 in the **Other IP DSCP** field.
    - **IP Precedence**: The IP precedence field in a packet is defined as the high-order three bits of the service type octet in the IP header. From the menu, select a number from 0 to 7.
    - **IP TOS**: The IP ToS field in a packet is defined as all 8 bits of the service type octet in the IP header. You can set two values:
        - **Left field**: The ToS bits value is a hexadecimal number from 0 to ff.
        - **Right field**: The ToS mask value is also a hexadecimal number from 0 to ff. The ToS mask denotes the bit positions in the ToS bits value that are used for comparison against the IP ToS field in a packet.

      For example, to check for an IP ToS value for which bit 7 is set (as the most significant value), for which bit 5 is set, and for which bit 1 is cleared, use a ToS bits value of 0xA0 and a ToS mask of 0xFF.

26. Click one of the following buttons:

    - **Save**: To save your settings, click the **Save** button.

      The rule is added to the IP ACL.

      Each ACL displays the following information:

        - **Rules**: The number of rules for the IP ACL.
        - **Type**: The type of IP ACL (Standard IP ACL, Extended IP ACL, or Named IP ACL).
    - **Clear**: To clear the settings so you can specify other settings before you save them, click the **Clear** button.
    - **Back**: To cancel the settings and return to the initial IP ACL/Rules page with the IP ACL/Rule Table section, click the **Back** button.

Change the match criteria for an extended IPv4 ACL rule

You can change the match criteria for an existing extended IPv4 ACL rule.

To change the match criteria for an extended IPv4 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > IP ACL > IP ACL/Rules**.

   The IP ACL/Rules page displays.

   The IP ACL Configuration section displays the total number of IPv4 ACLs, IPv6 ACLs, and MAC ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. In the IP ACL/Rule Table section, click the number or name of the IP ACL with which the rule is associated.

   The number or name of the IP ACL is a hyperlink.

   The rules that are associated with the IP ACL display.
7. Select the check box for the rule.
8. Click the **Edit** button.

   The page adjusts and displays the Extended ACL Rule Configuration (100-199) section.
9. Change the settings as needed.

   For more information about the settings, see Add a rule for an extended IPv4 ACL on page 396.

You cannot change the ACL ID, name, or sequence number.

10. Click the **Save** button.

    Your settings are saved.

Remove a rule from an extended IPv4 ACL

You can remove a rule from an extended IPv4 ACL if you no longer need the rule. When you remove a rule, the rule is deleted.

To remove a rule from an extended IPv4 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > ACL > IP ACL > IP ACL/Rules**.

   The IP ACL/Rules page displays.

   The IP ACL Configuration section displays the total number of IPv4 ACLs, IPv6 ACLs, and MAC ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.

6. In the IP ACL/Rule Table section, click the number or name of the IP ACL with which the rule is associated.

   The number or name of the IP ACL is a hyperlink.

   The rules that are associated with the IP ACL display.

7. Select the check box for the rule.
8. Click the **Delete** button.

   Your settings are saved and the rule is removed.

IPv6 ACLs

An 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 applied, and any additional rules are not checked for a match. You must associate the IPv6 ACL with one or more interfaces.

Multiple steps are involved in defining an IPv6 ACL and applying it to the switch:

1. Add an IPv6 ACL (see Add an IPv6 ACL on page 404).

   An IPv6 ACL must start with a name string that is up to 31 alphanumeric characters in length. The name must start with a letter.
2. Create an IPv6 rule (see IPv6 ACL rules on page 407).
3. Bind (associate) the IPv6 ACL to one or more interfaces (see Configure an IP ACL interface binding on page 415).

   You can display or delete IPv6 ACL binding configurations in the IP ACL Binding table (see Display or delete IP ACL bindings on page 416).

   Note: The process for binding an IPv6 ACL to an interface is the same process as binding an IPv4 ACL to an interface.

Add an IPv6 ACL

You can add an IPv6 ACL and then add a rule later. The following procedure describes how to add an IPv6 ACL only. You can also add an IPv6 ACL and a rule together, as one task (see Add a rule for an IPv6 ACL on page 407).

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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.

4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > IP ACL > IPv6 ACL/Rules**.

   The IPv6 ACL/Rules page displays.

   The IPv6 ACL Configuration section displays the total number of IPv6 ACLs, IPv4 ACLs, and MAC ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. Click the **Add New** button.

   The Add IPv6 ACL/Rule pop-up window displays.
7. In the **ACL Name** field, type a name.

   This is the IPv6 ACL name string, which includes up to 31 alphanumeric characters only. The name must start with a letter.
8. Click the **Add** button.

   The IP ACL is added. You can now add a rule for the IPv6 ACL (see Add a rule for an IPv6 ACL on page 407).
   Each configured IPv6 ACL displays the following information:
   - **Rules**: The number of rules configured for the IPv6 ACL.
   - **Type**: The type of ACL, which is always IPv6 ACL.

Change the name of an IPv6 ACL

You can change the name of an existing IPv6 ACL.

To change the name of 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

The Dashboard page displays.

5. Select **Security > ACL > IPv6 ACL/Rules**.

   The IPv6 ACL/Rules page displays.

   The IPv6 ACL Configuration section displays the total number of IPv6 ACLs, IPv4 ACLs, and MAC ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. In the IPv6 ACL/Rule Table section, select the check box for the IPv6 ACL.
7. Click the **Edit** button.

   The Edit IPv6 ACL/Rule pop-up window displays.
8. In the **ACL Name** field, type a new name.
9. Click the **Save** button.

   Your settings are saved.

Remove an IPv6 ACL

You can remove an IPv6 ACL that you no longer need.

To remove 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > IP ACL > IPv6 ACL/Rules**.

   The IPv6 ACL/Rules page displays.

The IPv6 ACL Configuration section displays the total number of IPv6 ACLs, IPv4 ACLs, and MAC ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.

6. In the IPv6 ACL/Rule Table section, select the check box for the IPv6 ACL.
7. Click the **Delete** button.

   Your settings are saved and the IPv6 ACL is removed.

IPv6 ACL rules

You can define rules for IPv6-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

Note: An implicit "deny all" rule is included at the end of a list with ACL rules. This means that if an ACL is applied to a packet and none of the explicit rules match, then the final implicit "deny all" rule applies and the packet is dropped.

Add a rule for an IPv6 ACL

If you already added an IPv6 ACL, you can add a rule to the ACL. You can also add an IPv6 ACL and a rule together, as one task. The following procedure describes both options.

To add a rule for an existing or new 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > ACL > IP ACL > IPv6 ACL/Rules**.

   The IPv6 ACL/Rules page displays.

   The IPv6 ACL Configuration section displays the total number of IPv6 ACLs, IPv4 ACLs, and MAC ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. Click the **Add New** button.

   The Add IPv6 ACL/Rule pop-up window displays.
7. Select the **Add Rule to existing ACL or Add new ACL and Rule** button.

   The window adjusts.
8. Click the **Add** button.

   The window closes, and the IPv6 ACL Rule Configuration section displays.
9. Do one of the following:
   - **Add a rule to an existing IPv6 ACL**: From the **ACL ID/Name** menu, select the ACL.
   - **Add a rule to a new IPv6 ACL**:
     a. From the **ACL ID/Name** menu, select **Add ACL**.

        The ACL Name field displays.
     b. In the **ACL Name** field, type a name.

        This is the IPv6 ACL name string, which includes up to 31 alphanumeric characters only. The name must start with an alphabetic character.
10. In the **Sequence Number** field, type a number in the range from 1 to 2147483647 to identify the rule.

    An IPv6 ACL can contain up to 50 rules.
11. Select an Action radio button to set the action that must be taken if a packet matches the rule's criteria, and configure options that are available with your selection:

    - **Permit**: Forwards packets that meet the ACL criteria. You can configure an egress queue and you can let the switch mirror or redirect traffic to a specific interface. See the steps further down in this procedure.
    - **Deny**: Drops packets that meet the ACL criteria. You can enable logging. See the step further down in this procedure.

    Note: In the following steps, configure the criteria that you need for the rule. You do not need to configure all criteria.
12. (Optionally) If you select the **Permit** Action radio button, select a hardware egress queue ID from the **Egress Queue** menu.

This queue is used to handle all packets matching this IPv6 ACL rule. The range for the queue ID is from 0 to 7.

13. (Optionally) If you select the **Deny** Action radio button, click the **Logging** toggle to enable logging for the ACL:
    - **The toggle is gray and positioned to the left**: Logging is disabled for this ACL rule. This is the default setting.
    - **The toggle is purple and positioned to the right**: Logging is enabled for this ACL rule (subject to resource availability on the switch).
14. (Optionally) If you select the **Permit** Action radio button, select an Interface radio button to let the switch mirror or redirect traffic to a specific interface:
    - **Mirror**: From the menu, select the egress interface to which the matching traffic stream must be copied, in addition to being forwarded normally by the switch.

      A mirror interface and a redirect interface are mutually exclusive.
    - **Redirect**: From the menu, select the egress interface to which the matching traffic stream must be redirected, bypassing any forwarding decision normally performed by the switch.

      A redirect interface and a mirror interface are mutually exclusive.
15. From the **Match Every** menu, select if all packets must match the IPv6 ACL rule:
    - **False**: Not all packets need to match the ACL rule. You can configure other match criteria on the page.
    - **True**: Each packet must match the ACL rule. You cannot configure other match criteria on the page.

      If you select **True**, go to Step 25.
16. From the **Protocol Type** menu, select a protocol that a packet's IP protocol must be matched against:

    IPv6, **ICMPv6**, **TCP**, **UDP**, or **Other**.

    The protocol selection determines the options that are available on the page.

    If you select **Other**, type a protocol number from **0** to **255** in the **Other Protocol Type** field. Then, continue with Step 24.
17. In the Src (source) section, select to set an individual IPv6 source address and prefix length or a source IPv6 host address:

    You can select the **IP Address** radio button or the **Host** radio button:
    - **IP Address**: In the **IPv6 Address** field, type a source IPv6 address. In the **Prefix Length** field, type a prefix length, type a relevant wildcard mask, or leave the field empty, which means *any*.

The IPv6 address and prefix length are compared to a packet's source IPv6 address and prefix length.

- **Host**: In the **IP Address** field, type a source host name.

  The host name (or the IPv6 address associated with the name) is compared to a packet's source host name (or the IPv6 address associated with the name).

The source IPv6 address must be in the form documented in RFC 2373,where the address is specified in hexadecimal numbers using 16-bit values between colons.

18. If you select **TCP** or **UDP** from the **Protocol Type** menu, in the Src L4 (source Layer 4) section, select to set an individual port number or a range of port numbers:

    You can select the **Port** radio button or the **Range** radio button:

    - **Port**: Select one of the following protocols from the menu:
      - The source IP TCP port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **www-http**, **smtp**, **telnet**, **pop2**, **pop3**, and **bgp**. A selected protocol translates into its equivalent port number.
      - The source IP UDP port protocols are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **tftp**. A selected protocol translates into its equivalent port number.
      - Select **Other** to type a port number from 0 to 65535 in the rightmost field. The matching condition is always Equal (see the middle field).

      The source port is compared to a packet's source port.
    - **Range**: Define a range by selecting a protocol from the **Start Port** menu and a protocol from the **End Port** menu:
      - The source IP TCP port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **www-http**, **smtp**, **telnet**, **pop2**, **pop3**, and **bgp**. A selected protocol translates into its equivalent port number.
      - The source IP UDP port protocols are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **tftp**. A selected protocol translates into its equivalent port number.
      - Select **Other** to type a port number from 0 to 65535 in the rightmost field.

      The source port range is compared to a packet's source port range.

19. In the Dst (destination) section, select to set an individual IPv6 destination address and prefix length or a destination IPv6 host address:

    You can select the **IP Address** radio button or the **Host** radio button:

    - **IP Address**: In the **IPv6 Address** field, type a destination IPv6 address. In the **Prefix Length** field, type a prefix length, type a relevant wildcard mask, or leave the field empty, which means *any*.

      The IPv6 address and prefix length are compared to a packet's destination IPv6 address and prefix length.
    - **Host**: In the **IP Address** field, type a destination host name.

The host name (or the IPv6 address associated with the name) is compared to a packet's destination name (or the IPv6 address associated with the name).

The destination IPv6 address must be in the form documented in RFC 2373,where the address is specified in hexadecimal numbers using 16-bit values between colons.

20. If you select **TCP** or **UDP** from the **Protocol Type** menu, in the Dst L4 (destination Layer 4) section, select to set an individual port number or a range of port numbers:

    You can select the **Port** radio button or the **Range** radio button:

    - **Port**: Select one of the following protocols from the menu:
      - The destination IP TCP port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **www-http**, **smtp**, **telnet**, **pop2**, **pop3**, and **bgp**. A selected protocol translates into its equivalent port number.
      - The destination IP UDP port protocols are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **tftp**. A selected protocol translates into its equivalent port number.
      - Select **Other** to type a port number from 0 to 65535 in the rightmost field. The matching condition is always Equal (see the middle field).

      The destination port is compared to a packet's destination port.
    - **Range**: Define a range by selecting a protocol from the **Start Port** menu and a protocol from the **End Port** menu:
      - The destination IP TCP port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **www-http**, **smtp**, **telnet**, **pop2**, **pop3**, and **bgp**. A selected protocol translates into its equivalent port number.
      - The destination IP UDP port protocols are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **tftp**. A selected protocol translates into its equivalent port number.
      - Select **Other** to type a port number from 0 to 65535 in the rightmost field.

      The destination port range is compared to a packet's destination port range.

21. If you select **ICMPv6** from the **Protocol Type** menu, select either the **Type** or **Message** radio button:

    - If you select the **Type** radio button, type a code in the left field. To set a range of codes, type a code in the left field and another code in the **Code** field (the right field).

      The range is from 0 to 255. If you leave the field empty, it means any ICMPv6 type.

      The ICMPv6 type is compared to a packet's ICMPv6 type.
    - If you select the **Message** radio button, from the menu, select the type of the ICMPv6 message:

destination-unreachable, **echo-reply**, **echo-request**, **header**, **hop-limit**, **mld-query**, **mld-reduction**, **mld-report**, **next-header**, **no-admin**, **no-route**, **packet-too-big**, **port-unreachable**, **router-solicitation**, **router-advertisement**, **router-renumbering**, **unreachable**, **time-exceeded**, **nd-na**, or **nd-ns**.

Specifying a type of message implies that both the ICMPv6 type and ICMPv6 code are specified. That is, the ICMPv6 message is decoded into the corresponding ICMPv6 type and ICMPv6 code within the ICMPv6 type and compared to a packet's type of the ICMPv6 message.

22. (Optionally) Click the **Fragments** toggle to allow initial fragments (that is, the fragment bit is asserted) or prevent initial fragments from being used:
    - **The toggle is gray and positioned to the left**: Initial fragments are not allowed. This is the default setting.
    - **The toggle is purple and positioned to the right**: Initial fragments are allowed.

    This option is not valid for rules that match L4 information such as a TCP port number, because that information is carried in the initial packet.
23. (Optionally) Click the **Routing** toggle to allow the routing extension header to be considered or ignored:
    - **The toggle is gray and positioned to the left**: The routing extension header in an incoming packet is ignored. This is the default setting.
    - **The toggle is purple and positioned to the right**: The routing extension header in an incoming packet is considered.
24. (Optionally) Select a keyword from the **IPv6 DSCP Service** menu to define that the IPv6 DiffServ Code Point (DSCP) field must be considered.

    If you select **Other**, type a number from 0 to 63 in the **Other IPv6 DSCP Service** field.

    The IPv6 DSCP field in a packet is defined as the high-order 6 bits of the service type octet in the IPv6 header. The IPv6 DSCP is compared to packet's IPv6 DSCP field.
25. Click one of the following buttons:
    - **Save**: To save your settings, click the **Save** button.

      The rule is added to the IPv6 ACL.

      Each ACL displays the following information:

      - **Rules**: The number of rules configured for the IPv6 ACL.
      - **Type**: The type of ACL, which is always IPv6 ACL.
    - **Clear**: To clear the settings so that you can specify other settings before you save them, click the **Clear** button.
    - **Back**: To cancel the settings and return to the initial IP ACL/Rules page with the IP ACL/Rule Table section, click the **Back** button.

Change the match criteria for an IPv6 ACL rule

You can change the match criteria for an existing IPv6 ACL rule.

To change 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > IP ACL > IPv6 ACL/Rules**.

   The IPv6 ACL/Rules page displays.

   The IPv6 ACL Configuration section displays the total number of IPv6 ACLs, IPv4 ACLs, and MAC ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. In the IPv6 ACL/Rule Table section, select the check box for the IPv6 ACL.

   The name of the IPv6 ACL is a hyperlink.

   The rules that are associated with the IPv6 ACL display.
7. Select the check box for the rule.
8. Click the **Edit** button.

   The page adjusts and displays the IPv6 ACL Rule Configuration section.
9. Change the settings as needed.

   For more information about the settings, see Add a rule for an IPv6 ACL on page 407.

   You cannot change the ACL name or the sequence number.
10. Click the **Save** button.

Your settings are saved.

Remove a rule from an IPv6 ACL

You can remove a rule from an IPv6 ACL if you no longer need the rule. When you remove a rule, the rule is deleted.

To remove a rule from 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > IP ACL > IPv6 ACL/Rules**.

   The IPv6 ACL/Rules page displays.

   The IPv6 ACL Configuration section displays the total number of IPv6 ACLs, IPv4 ACLs, and MAC ACLs that are configured on the switch and the maximum number of ACLs that *can be* configured.
6. In the IPv6 ACL/Rule Table section, click the name of the IPv6 ACL with which the rule is associated.

   The name of the IPv6 ACL is a hyperlink.

   The rules that are associated with the IPv6 ACL display.
7. Select the check box for the rule.
8. Click the **Delete** button.

   Your settings are saved and the rule is removed.

IP ACL bindings

When you bind an IP ACL to an interface, all the rules that are defined for the ACL are applied to the selected interface.

The IP ACL can be a standard IPv4 ACL, extended IPv4 ACL, or IPv6 ACL.

Configure an IP ACL interface binding

You can bind an IP ACL (an IPv4 or IPv6 ACL) to one or more interfaces, which can be physical ports, LAGs, or both.

Note: You cannot bind both an IPv4 ACL and an IPv6 ACL to an interface. Either bind an IPv4 ACL or an IPv6 ACL.

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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > IP ACL > IP Binding Configuration**.

   The IP Binding Configuration page displays.
6. From the **ACL ID** menu, select the IP ACL.

   Note: The selection from the **Direction** menu is always **Inbound**. The IP ACL is applied to incoming traffic only.
7. In the **Sequence Number** field, type a number to define the order of the IP ACL relative to other ACLs that are bound to the interface.

A low number indicates a high precedence order. If a sequence number is already in use for the interface, the IP ACL replaces the currently attached ACL using that sequence number. If you do not set the sequence number, a sequence number that is one number greater than the highest sequence number currently in use for the interface is used. The range is from 1 to 4294967295.

8. In the Ports table, LAG table, or both, click the ports and LAGs to which the IP ACL must be bound.

   A selected port or LAG displays blue. An excluded port or LAG displays blank.

9. Click the **Apply** button.

   Your settings are saved.

Display or delete IP ACL bindings

You can display or delete bindings for standard IPv4, extended IPv4, and IPv6 ACLs.

To display IP ACL bindings or delete an IP ACL binding:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Security > ACL > IP ACL > Binding Table**.

   The 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 that is displayed in the IP ACL Binding Table.

Table 75. Interface IP ACL binding status information

Field	Description
Interface	The interface to which the IP ACL is bound
Direction	The packet filtering direction for the IP ACL, which is always inbound
ACL Type	The type of ACL, which is always IP ACL
ACL ID	The ACL number or name
Sequence Number	The sequence number signifying the order of the IP ACL relative to other ACLs bound to the interface

Display the existing ACLs and associated rules

Existing MAC ACLs, IPv4 ACLs, and IPv6 ACLs each display on a different page. You can also display the rules that are associated with an ACL.

To display the existing ACLs and associated rules:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Make one of the following selections, depending on the type of ACLs that you want to display:

- **MAC ACLs**: Select **Security > ACL > MAC ACL > MAC ACL/Rules**.

  The MAC ACL/Rules page displays.
- **IPv4 ACLs**: Select **Security > ACL > IP ACL > IP ACL/Rules**.

  The IP ACL/Rules page displays.
- **IPv6 ACLs**: Select **Security > ACL > IP ACL > IPv6 ACL/Rules**.

  The IPv6 ACL/Rules page displays.

The Current Number of ACLs field display the total number of configured MAC ACLs, IPv4 ACLs, and IPv6 ACLS on the switch.

The Maximum ACL field displays the maximum number of ACLs that *can be* configured on the switch.

6. To display the rules that are associated with an ACL, click the number or name of the ACL.

   The number or name of the ACL is a hyperlink.

   The rules that are associated with the ACL displays

The following table show the sections that provide information about changing or removing an ACL or rule.

Table 76. Sections that provide information about changing or removing an ACL or rule

Section
MAC ACLs
Change the name of a MAC ACL on page 377
Remove a MAC ACL on page 378
Change the match criteria for a MAC ACL rule on page 382
Remove a rule from a MAC ACL on page 383
IPv4 ACLs
Change the number or name of an IPv4 ACL on page 389
Remove an IPv4 ACL on page 390
Change the match criteria for a standard IPv4 ACL rule on page 393
Remove a rule from a standard IPv4 ACL on page 394
Change the match criteria for an extended IPv4 ACL rule on page 402
Remove a rule from an extended IPv4 ACL on page 403
IPv6 ACLs
Change the name of an IPv6 ACL on page 405
Remove an IPv6 ACL on page 406

Table 76. Sections that provide information about changing or removing an ACL or rule (Continued)

Section
Change the match criteria for an IPv6 ACL rule on page 413
Remove a rule from an IPv6 ACL on page 414

VLAN ACL bindings

You can associate a MAC ACL, any type of IPv4 ACL, or an IPv6 ACL with a VLAN. When you do so, the ACL is applied to all interfaces that are members of the VLAN.

The packet filtering direction for the ACL is always inbound.

Configure a VLAN ACL binding

When you bind an ACL to a VLAN, all the rules that are defined for the ACL are applied to all VLAN members (physical ports, LAGs, or both).

To bind an ACL to 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > VLAN ACL**.

   The VLAN ACL page displays.
6. Click the **Add New** button.

The Add VLAN Binding Configuration pop-up window displays.

7. In the **VLAN ID** field, type the VLAN ID to which the binding must apply.
8. In the **Sequence Number** field, type a number to define the order of the ACL relative to other ACLs that are bound to the VLAN.

   A low number indicates a high precedence order. If a sequence number is already in use for the VLAN, the ACL replaces the currently attached ACL using that sequence number. If you do not set the sequence number, a sequence number that is one number greater than the highest sequence number currently in use for the VLAN is used. The range is from 1 to 4294967295.
9. From the **ACL Type** menu, select the type of ACL.

   You can select **MAC ACL**, **IP ACL**, or **IPv6 ACL**.
10. From the **ACL ID** menu, select the ID or name of the ACL that must be bound to the VLAN.
11. Click the **Save** button.

    Your settings are saved.

Display or delete VLAN ACL bindings

You can display or delete the VLAN ACL bindings in the VLAN Binding Configuration table.

To display VLAN ACL bindings or delete a VLAN ACL binding:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > VLAN ACL**.

The VLAN ACL page displays.

6. To delete a VLAN-to-ACL binding, do the following:
   a. Select the check box for the VLAN ID.
   b. Click the **Delete** button.

      The binding is removed.

The following table describes the information that is displayed in the VLAN Binding Configuration table.

Table 77. Interface MAC ACL binding information

Field	Description
VLAN ID	The ID of the VLAN to which the ACL is bound
Direction	The packet filtering direction for the ACL, which is always inbound
Sequence Number	The sequence number signifying the order of the ACL relative to other ACLs bound to the VLAN
ACL Type	The type of ACL
ACL ID	The ACL number or name

9

Maintenance and Troubleshooting

This chapter covers the following topics:

- Reboot the switch from the device UI
- Reset the switch to factory default settings
- Export the configuration file or log files from the switch
- Update the switch software
- Download a file to the switch
- Manage software images
- Diagnostics and troubleshooting

Reboot the switch from the device UI

You can reboot the switch from the device UI.

Note: If you can physically access the switch, you can reboot the switch by pressing the multi-function **Reset** button on the front panel for less than 5 seconds. (Do not press the button for more than 5 seconds! Doing so resets the switch to factory default settings.)

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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Maintenance > Reset**.

   The Reset page displays.
6. Click the **Reboot Now** button.

   An Alert pop-up window displays.

   The switch reboots.
7. Click the **OK** button to close the window.

Reset the switch to factory default settings

You can reset the switch configuration to factory default values. All changes that you made are erased. If the IP address changes, your web browser session might disconnect. If you reset the switch to the default configuration, the management 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-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

Note: We recommend that you export and save the configuration file before you reset the switch to factory default settings. For more information, see Export the configuration file or log files from the switch on page 425.

To reset the switch to 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Maintenance > Reset**.

   The Reset page displays.

6. Do one of the following:

   - **Reset the configuration to factory defaults and clear device logs but keep the registered device status**: Click the **Factory Reset** button.

After the switch is reset, you will need to go through the initial login and setup process again.

- **Reset and erase everything, including registered device status**: Click the **Erase** button.

  After the switch is reset, you will need to enter a registration key or log in to your MyNETGEAR.com account and manually enter your device registration information, and then go through the initial login and setup process again.

A confirmation pop-up window displays.

The configuration is reset to the factory default settings.

7. Click the **OK** button to close the window.

Export the configuration file or log files from the switch

You can export the current configuration settings to create a back up configuration file, such as before performing a reset, when you want to reuse the settings to configure a second switch of the same model, or anytime you want to create a configuration baseline or fallback point. You can also export various types of log files from the switch, including the trap log, buffered (in-memory log), crash log, and files designed specifically for use when requesting assistance from NETGEAR customer support. The configuration and log files export in ASCII format and can be sent to a file server over a TFTP session, or to a computer or USB storage device over an HTTP session.

Export a file from the switch to a TFTP server

You can export (upload) the configuration or log files from the switch to a TFTP server on the network.

To export a file from the switch to a TFTP server:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard 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 that must be exported:

   - **Text Configuration**: A text-based configuration file enables you to edit a configured text file (`startup-config`) offline as needed. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline for another switch of the same model (for example, change the device name and IP address), and download it to the other switch. This is the default setting.
   - **Trap Log**: The trap log with the system trap records.
   - **Buffered Log**: The system buffered (in-memory) log.
   - **Tech Support**: The tech support file is a text-based file that contains a variety of hardware, software, and configuration information that can assist in device and network troubleshooting.
   - **Crash Logs**: The switch crash logs, if any are available.
7. From the **Server Address Type** menu, select the format for the **Server Address** field:

   - **IPv4**: The server address is an IPv4 address in dotted-decimal format. This is the default setting.
   - **DNS**: The server address is a host name.
8. In the **Server Address** field, type the IP address or host name of the server.

   The default is the IPv4 address 0.0.0.0.
9. In the **Transfer File Path** field, type the path on the server where you want to save the file.

   The path name can include letters, numbers, forward slashes, periods, and underscores characters only. You can type up to 160 characters.
10. In the **Transfer File Name** field, type a destination file name for the file to be exported.

    You can type up to 32 characters. The file name cannot include the following characters: ' / : * ? " < > | ' .

11. Click the **Start File Transfer** toggle to enable the file transfer:
    - **The toggle is gray and positioned to the left**: The file transfer is disabled. This is the default setting.
    - **The toggle is purple and positioned to the right**: The file transfer is enabled. The file transfer starts after you click the **Apply** button.
12. Click the **Apply** button.

    The file is exported to the server. The page displays information about the progress of the file transfer.

Export a file from the switch to a computer or USB storage device

You can export (upload) the configuration or log files from the switch to a computer or USB storage device through an HTTP session on your web browser. If you use a USB storage device, it must be attached to your computer.

To use HTTP to export a file from the switch to a computer or USB storage device that is attached to your computer:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Maintenance > Export > HTTP File Export**.

   The HTTP File Export page displays.
6. From the **File Type** menu, select the type of file that must be exported:

- **Text Configuration**: A text-based configuration file enables you to edit a configured text file (`startup-config`) offline as needed. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline for another switch of the same model (for example, change the device name and IP address), and download it to the other switch. This is the default setting.
- **Tech Support**: The tech support file is a text-based file that contains a variety of hardware, software, and configuration information that can assist in device and network troubleshooting.
- **Crash Logs**: The switch crash logs, if any are available.

7. Click the **Apply** button.

   The file is exported to the computer. The page displays information about the progress of the file transfer.
8. Depending on the type of browser and the browser configuration that you use, select a location on your computer or on a USB storage device that is attached to your computer, and save the file.

Export a file from the switch to a directly-attached USB storage device

You can upload (export) a text configuration file or license key to a USB storage device that is attached to the switch.

To export a file from the switch to a USB storage device:

1. Attach the USB storage device to the switch.
2. Connect your computer to the same network as the switch.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
4. Enter your device admin password.

5. Click the **Login** button.

   The Dashboard page displays.
6. Select **Maintenance > Export > Export File to USB**.

   The Export File to USB page displays.
7. From the **File Type** menu, select the type of file that must be exported:

   - **Text Configuration**: A text-based configuration file enables you to edit a configured text file (`startup-config`) offline as needed. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name or IP address), and download it to that device. This is the default setting.
   - **Buffered Log**: The system buffered (in-memory) log.
   - **Tech Support**: The tech support file is a text-based file that contains a variety of hardware, software, and configuration information that can assist in device and network troubleshooting.
   - **Crash Logs**: The switch crash logs, if any are available.
8. In the **File Path** field, type the path on the USB storage device.

   You can type up to 139 characters.
9. In the **USB File** field, type a name for the file.

   This is the name under which the file will be saved on the USB storage device. You can type up to 32 characters.
10. Click the **Apply** button.

    The file is exported (uploaded) to the USB storage device. The page displays information about the progress of the file transfer.

Update the switch software

You can check for the latest software (firmware) updates and upgrade the switch software directly through the device UI. You can also download software to the switch from a file server over a TFTP session, from a computer over an HTTP session, or from a USB storage device.

You can manually check for the latest firmware version, download the firmware to a server or computer, and then download the firmware to the switch. If firmware release notes are available with new firmware, read the release notes to find out if you must reconfigure the switch after updating.

In this context, downloading and installing a firmware update is also referred to as upgrading.

Update the switch software through the device UI

You can check for the latest software (firmware) images for the switch that are available, and update the software through the device UI.

To update the switch software through the device UI:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. In the Connectivity section on the Dashboard page, verify that the switch is online. A green connection indicates that the switch is online.
6. Do one of the following:
   - **Update the switch software through the Dashboard page:**
     a. In the Device Details section, click the **Check for Update** button.
     b. Click the **Update** button if a new software version is available.
     c. In the Firmware Update Confirmation window, read the upgrade information and click the software image you want to upgrade.
     d. Click the **Update** button.
     e. When the firmware download and update processes finish, click the **OK** button to reboot the switch.
   - **Update the switch software through the Update page:**

a. Select **Maintenance > Update > Online Firmware Update**.

   The Online Firmware Update page displays.

b. To check for the latest available firmware update, click the **Check For Update** button.

   The available firmware updates display under the current version of both the Active and Next Active images.

c. Click the **Update** button next to the new firmware version you want to use.

d. When the firmware download and update processes finish, click the **OK** button to reboot the switch.

7. After the switch completes its reboot, verify that the switch is online and runs the newly activated image. You can view the software version in the bottom right corner of the Login page or on the Dashboard page.

Download the switch software from a TFTP server and update the switch

You can download a software (firmware) image from a TFTP server on your network to the switch.

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

- The file that you want to download is on the server in an appropriate directory.
- The file is in the correct format.
- The switch has a path to the server.

To download the switch software from a TFTP server and update 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Maintenance > Update > TFTP Firmware/File Update**.

   The TFTP Firmware/File Update page displays.
6. From the **File Type** menu, select **Software**.

   This selection represents the switch software image, which is saved in one of two flash sectors called images (Image1 and Image2). The active image stores the active copy, while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the nonactive image. This is a safety feature for faults occurring during the boot upgrade process.
7. From the **Image Name**, select where the software image must be saved on the switch:

   - **Image1**: Uploads the software to flash sector image1.
   - **Image2**: Uploads the software to flash sector image2.

   Note: We recommended that you do not overwrite the active image.
8. From the **Server Address Type** menu, select the format for the **Server Address** field:

   - **IPv4**: The server address is an IPv4 address in dotted-decimal format. This is the default setting.
   - **DNS**: The server address is a host name.
9. In the **TFTP Server IP** field, type the IP address or host name of the server.

   The default is the IPv4 address 0.0.0.0.
10. In the **Transfer File Path** field, type the path on the server where the file is located.

    The path name can include letters, numbers, forward slashes, periods, and underscores only. You can type up to 160 characters.
11. In the **Remote File Name** field, type the file name for the file to be downloaded.

    You can type up to 32 characters. The file name cannot include the following characters: ' / : * ? " < > | ' .
12. Click the **Start File Transfer** toggle to enable the file transfer:
    - **The toggle is gray and positioned to the left**: The file transfer is disabled. This is the default setting.
    - **The toggle is purple and positioned to the right**: The file transfer is enabled. The file transfer starts after you click the **Apply** button.

13. Click the **Apply** button.

    The file is downloaded from the server to the switch. After the file transfer starts, wait until the page refreshes. The page displays information about the progress of the file transfer.

14. After you download the software image file, if you want the switch to run the new software image, do the following:

    a. Select **Maintenance > File Management**.

       The File Management page displays.

       The Dual Image Configuration section displays which software image is the active image.

       The Activate button displays for the image that is *not* currently the active image, but that you want the switch to run *after* it reboots.

    b. Click the **Activate** button.

       The Active Dual Image Configuration pop-up window displays.

    c. Click the **Activate & Reboot** button.

       The File Management page refreshes and displays the Reboot Now button.

    d. Click the **Reboot Now** button.

       The switch reboots.

    e. Click the **OK** button to close the window.

    f. After the switch completes its reboot, verify that the switch runs the newly activated image.

       On the Dashboard page, the Firmware Version field displays the firmware image that the switch runs.

Update the switch software through the device UI

You can check for the latest software (firmware) images for the switch that are available, and update the software through the device UI.

To update the switch software through the device UI:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. In the Connectivity section on the Dashboard page, verify that the switch is online. A green connection indicates that the switch is online.
6. Do one of the following:
   - **Update the switch software through the Dashboard page:**
     a. In the Device Details section, click the **Check for Update** button.
     b. Click the **Update** button if a new software version is available.
     c. In the Firmware Update Confirmation window, read the upgrade information and click the software image you want to upgrade.
     d. Click the **Update** button.
     e. When the firmware download and update processes finish, click the **OK** button to reboot the switch.
   - **Update the switch software through the Update page:**
     a. Select **Maintenance > Update > Online Firmware Update**.

        The Online Firmware Update page displays.
     b. To check for the latest available firmware update, click the **Check For Update** button.

        The available firmware updates display under the current version of both the Active and Next Active images.
     c. Click the **Update** button next to the new firmware version you want to use.
     d. When the firmware download and update processes finish, click the **OK** button to reboot the switch.
7. After the switch completes its reboot, verify that the switch is online and runs the newly activated image. You can view the software version in the bottom right corner of the Login page or on the Dashboard page.

Download the switch software from a computer or USB storage device and update the switch

You can download a software (firmware) image from a computer on your network to the switch, using an HTTP session on your web browser. The software can also be on a USB storage device attached to your computer.

To download the switch software from a computer or USB storage device and update 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Maintenance > Update > HTTP Firmware/File Update**.

   The HTTP Firmware/File Update page displays.

6. From the **File Type** menu, select **Software**.

   This selection represents the switch software image, which is saved in one of two flash sectors called images (Image1 and Image2). The active image stores the active copy, while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the nonactive image. This is a safety feature for faults occurring during the boot upgrade process.

7. From the **Image Name**, select where the software image must be saved on the switch:

- **Image1**: Uploads the software to flash sector image1.
- **Image2**: Uploads the software to flash sector image2.

Note: We recommended that you do not overwrite the active image.

8. Click the **Browse** button, navigate to the software file location, and select the file to download.

   You can select a file with a file name of up to 80 characters.

9. Click the **Apply** button.

   The file is downloaded from the computer or USB drive to the switch. After the file transfer starts, wait until the page refreshes. The page displays information about the progress of the file transfer.

10. After you download the software image file, if you want to upgrade the firmware on the switch with the new software image, do the following:

    a. Select **Maintenance > File Management**.

       The File Management page displays.

       The Dual Image Configuration section displays which software image is currently the active image.

       The Activate button displays for the new image that is *not* currently the active image but that you want the switch to run *after* it reboots.

    b. Click the **Activate** button.

       The Active Dual Image Configuration pop-up window displays.

    c. Click the **Activate & Reboot** button.

       The File Management page refreshes and displays the Reboot Now button.

    d. Click the **Reboot Now** button.

       The switch reboots.

    e. Click the **OK** button to close the window.

    f. After the switch completes its reboot, verify that the switch runs the newly activated image.

       On the Dashboard page, the Firmware Version field displays the firmware image that the switch runs.

Download the switch software from a directly-attached USB storage device and update the switch

You can download a software (firmware) image from a from a USB storage device to the switch.

To download the switch software from a USB storage device and update the switch:

1. Attach the USB storage device to the switch.
2. Connect your computer to the same network as the switch.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
4. Enter your device admin password.
5. Click the **Login** button.

   The Dashboard page displays.
6. Select **Maintenance > Update > USB Firmware/File Update**.

   The USB Firmware/File Update page displays.
7. From the **File Type** menu, select **Software**.

   This selection represents the switch software image, which is saved in one of two flash sectors called images (Image1 and Image2). The active image stores the active copy, while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the nonactive image. This is a safety feature for faults occurring during the boot upgrade process.
8. In the **File Path** field, type the path on the USB storage device.

   You can type up to 139 characters.
9. In the **USB File** field, type a name for the file.

This is the name under which the file will be saved on the USB storage device. You can type up to 32 characters.

10. From the **Image Name**, select where the software image must be saved on the switch:

    - **Image1**: Uploads the software to flash sector image1.
    - **Image2**: Uploads the software to flash sector image2.

    Note: We recommended that you do not overwrite the active image.

11. Click the **Apply** button.

    The file is downloaded from the USB storage device to the switch. After the file transfer starts, wait until the page refreshes. The page displays information about the progress of the file transfer.

12. After you download the software image file, if you want the switch to run the software image, do the following:

    a. Select **Maintenance > File Management**.

       The File Management page displays.

       The Dual Image Configuration section displays which software image is the active image.

       The Activate button displays for the image that is *not* the active image but that you want the switch to run *after* it reboots.

    b. Click the **Activate** button.

       The Active Dual Image Configuration pop-up window displays.

    c. Click the **Activate & Reboot** button.

       The File Management page displays again and displays the Reboot Now button.

    d. Click the **Reboot Now** button.

       The switch reboots.

    e. Click the **OK** button to close the window.

    f. After the switch completed its reboot, verify that the switch runs the newly activated image.

       On the Dashboard page, the Firmware Version field displays the firmware image that the switch runs.

Download a file to the switch

You can download software, configuration (ASCII), log (ASCII log), SSL, PEM, or other types of files to the switch from a file server over a TFTP session, from a computer over an HTTP session, or from a USB storage device.

For information about downloading software (firmware) and updating the switch firmware, see Update the switch software on page 429.

Note the following about SSH and SSL files:

- **SSH**: For you to be able to download SSH files to the switch, SSH must be administratively disabled and no active SSH sessions must occur.
- **SSL**: SSL files contain information to encrypt, authenticate, and validate HTTPS sessions. For you to be able to download SSL files to the switch, HTTPS must be administratively disabled.

Download a file from a TFTP server to the switch

You can download a software (firmware) image and configuration, SSL, PEM, or other types of files from a TFTP server on your network to the switch.

For information about downloading switch software from a TFTP server and updating the switch, see Download the switch software from a TFTP server and update the switch on page 431.

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

- The file to download is on the server in an appropriate directory.
- The file is in the correct format.
- The switch has a path to the server.

To download a file from a TFTP 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Maintenance > Update > TFTP Firmware/File Update**.

   The TFTP Firmware/File Update page displays.
6. From the **File Type** menu, select the type of file:

   - **Software**: For information about downloading switch software and updating the switch, see Download the switch software from a TFTP server and update the switch on page 431.
   - **Text Configuration**: A text-based configuration file enables you to edit a configured text file (`startup-config`) offline as needed. The most common usage of text-based configuration is to upload a working configuration from the switch, edit it offline to customize it for another switch of the same model (for example, change the device name and IP address), and download it to the second switch.
   - **X.509 Public Certificate PEM**: SSL Trusted Root Certificate File (PEM Encoded).
   - **X.509 Certificate Private Key PEM**: SSL Server Certificate File (PEM Encoded).
   - **SSL DH Weak Encryption Parameter PEM File**: SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).
   - **SSL DH Strong Encryption Parameter PEM File**: SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).
   - **SSH-2 RSA Key PEM File**: SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded).
7. From the **Server Address Type** menu, select the format for the **TFTP Server IP** field:

   - **IPv4**: The server address is an IPv4 address in dotted-decimal format. This is the default setting.
   - **DNS**: The server address is a host name.
8. In the **TFTP Server IP** field, type the IP address or host name of the server.
9. In the **Transfer File Path** field, type the path on the server where the file is located.

   The path name can include letters, numbers, forward slashes, periods, and underscores only. You can type up to 160 characters.
10. In the **Remote File Name** field, type the file name for the file to be downloaded.

You can type up to 32 characters. The file name cannot include the following characters: ' / : * ? " < > | ' .

11. Click the **Start File Transfer** toggle to enable the file transfer:
    - **The toggle is gray and positioned to the left**: The file transfer is disabled. This is the default setting.
    - **The toggle is purple and positioned to the right**: The file transfer is enabled. The file transfer starts after you click the **Apply** button.
12. Click the **Apply** button.

    The file is downloaded from the server to the switch. After the file transfer starts, wait until the page refreshes. The page displays information about the progress of the file transfer.

    Note: After you download a text configuration file, the switch applies the configuration automatically.

Download a file from a computer or USB storage device to the switch

You can download files of various types from a computer or to the switch through an HTTP session on your web browser. The file can also be on a USB storage device attached to your computer.

For information about downloading switch software from a computer and updating the switch, see Download the switch software from a computer or USB storage device and update the switch on page 435.

To download a file from a computer or USB storage device 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.

4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Maintenance > Update > HTTP Firmware/File Update**.

   The HTTP Firmware/File Update page displays.
6. From the **File Type** menu, select the type of file:

   - **Software**: For information about downloading switch software and updating the switch, see Download the switch software from a computer or USB storage device and update the switch on page 435.
   - **Text Configuration**: A text-based configuration file enables you to edit a configured text file (`startup-config`) offline as needed. The most common usage of text-based configuration is to upload a working configuration from the switch, edit it offline to customize it for another switch of the same model (for example, change the device name and IP address), and download it to the second switch.
   - **X.509 Public Certificate PEM**: SSL Trusted Root Certificate File (PEM Encoded).
   - **X.509 Certificate Private Key PEM**: SSL Server Certificate File (PEM Encoded).
   - **SSL DH Weak Encryption Parameter PEM File**: SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).
   - **SSL DH Strong Encryption Parameter PEM File**: SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).
   - **SSH-2 RSA Key PEM File**: SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded).
7. Click the **Browse** button, navigate to the file, and select the file to download.

   You can select a file with a file name of up to 80 characters.
8. Click the **Apply** button.

   The file is downloaded from the server to the switch. After the file transfer starts, wait until the page refreshes. The page displays information about the progress of the file transfer.

   Note: After you download a text configuration file, the switch applies the configuration automatically.

Download a text configuration file from a directly-attached USB storage device to the switch

You can download a text configuration file from a USB storage device to the switch.

For information about downloading switch software from a USB storage device and updating the switch, see Download the switch software from a computer or USB storage device and update the switch on page 435.

To download a text configuration file from a USB storage device to the switch:

1. Attach the USB storage device to the switch.
2. Connect your computer to the same network as the switch.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
4. Enter your device admin password.
5. Click the **Login** button.

   The Dashboard page displays.
6. Select **Maintenance > Update > USB Firmware/File Update**.

   The USB Firmware/File Update page displays.
7. From the **File Type** menu, select **Text Configuration**.

   This selection represents a text-based configuration. Such a file enables you to edit a configured text file (startup-config) offline as needed. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name or IP address), and download it to that device.
8. In the **File Path** field, type the path on the USB storage device.

   You can type up to 139 characters.
9. In the **USB File** field, type a name for the file.

This is the name under which the file will be saved on the USB storage device. You can type up to 32 characters.

10. Click the **Apply** button.

    The file is downloaded from the server to the switch. After the file transfer starts, wait until the page refreshes. The page displays information about the progress of the file transfer.

    Note: After you download a text configuration file, the switch applies the configuration automatically.

Download and install an SSL security certificate file on the switch

If you use HTTPS instead of HTTP to access the device UI, you are not required to obtain an SSL certificate. The security warning that might display in your browser prompts you to confirm that the self-signed certificate of the switch is valid. Once you do so, the browser warning might no longer display when you log in.

However, if you obtain an SSL security certificate from a certificate authority, you can download and install the SSL security certificate through an HTTP session using your web browser.

For an SSL security certificate, you must download two Privacy Enhanced Mail (PEM) files to the switch:

- **X.509 Public Certificate PEM**: The SSL trusted root certificate PEM file, which must be in the format `xxxxCERTxxxxx.pem`.
- **X.509 Certificate Private Key PEM**: The SSL server certificate PEM file (the key file), which must be in the format `xxxxKEYxxxxx.pem`.

Before you can download and install an SSL security certificate, you must temporarily disable HTTPS on the switch.

To disable HTTPS and use an HTTP session to download and install an SSL security certificate file 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **System > Protocols > HTTPS**.

   The HTTPS page displays.
6. Click the **Allow HTTPS** toggle to disable HTTPS access.

   The toggle is gray and positioned to the left.
7. Click the **Apply** button.

   Your settings are saved. Because you changed the access mode from HTTPS to HTTP, you are logged out of the switch.
8. Wait one minute, refresh your browser, and log back in to the switch.
9. Select **Maintenance > Update > HTTP Firmware/File Update**.

   The HTTP Firmware/File Update page displays.
10. From the **File Type** menu, select **X.509 Public Certificate PEM**.
11. Click the **Browse** button, navigate to the file, and select the file to download.

    This is the certificate file, which must be in the format `xxxxCERTxxxxx.pem`.
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.
13. From the **File Type** menu, select **X.509 Certificate Private Key PEM**.

    This is the key file, which must be in the format `xxxxKEYxxxxx.pem`.
14. Select the Select File **Browse** button and locate the file that you want to download.

    The file name can contain up to 80 characters.
15. Click the **Apply** button.

    The file is downloaded from the server to the switch. After the file transfer starts, wait until the page refreshes. The page displays information about the progress of the file transfer.

Manage software images

The switch maintains two versions of the switch software in permanent storage. One image is the active image, and the second image is the backup image. The active image is loaded when the switch starts or reboots. This feature reduces switch down time when you are upgrading the switch software.

Change the software image that loads when the switch starts

Because the switch can hold two software images, you can select which software image becomes the active image that next time that the switch reboots.

To change the image that loads during the boot process:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Maintenance > File Management**.

   The File Management page displays.

   The Dual Image Configuration section displays which software image is the active image.

   The Activate button displays for the image that is *not* the active image but that you want the switch to run *after* it reboots.
6. Click the **Activate** button.

The Active Dual Image Configuration pop-up window displays.

7. Do one of the following:
   - **Activate only**: Click the **Activate** button.

     The switch continues to run the image that is displayed as the currently active image until the next time that the switch reboots.
   - **Activate and reboot**: Do the following:
     a. Click the **Activate & Reboot** button.

        The File Management page displays again and displays the Reboot Now button.
     b. Click the **Reboot Now** button.

        The switch reboots.
     c. Click the **OK** button to close the window.
     d. After the switch completed its reboot, verify that the switch runs the newly activated image.

        On the Dashboard page, the Firmware Version field displays the firmware image that the switch runs.

Display the dual image configuration and add image descriptions

You can display the dual software image configuration and add descriptions to the images.

To display the dual image configuration and add image descriptions:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.

4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Maintenance > File Management**.

   The File Management page displays.

   The Dual Image Configuration section displays which software image is the active image.
6. To add descriptions to the image names, type a description in each **Image Description** field.

   You can type up to 255 characters in each field.
7. Click the **Apply** button.

   Your settings are saved.
8. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 78. Dual image configuration information

Field	Description
Image Name	The name of the image. By default, the image names are image1 and image2.
Image Version	The firmware version of the image.

Copy a software image from one flash sector to another

You can copy a software image from one flash sector (primary or backup) to another.

To copy a software image from one flash sector to another:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Maintenance > File Management**.

   The File Management page displays.

   The Dual Image Configuration section displays which software image is the active image.

   The following steps refer to the Copy section.
6. From the **Source image** menu, select **Image1** or **Image2** to specify the image to be copied.
7. From the **Destination image** menu, select **Image1** or **Image2** to specify the destination location.
8. Click the **Copy** button.

   The image is copied.

Delete a software image

You can delete a software image that you no longer need.

To delete a software image:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Maintenance > File Management**.

   The File Management page displays.

The Dual Image Configuration section displays which software image is the active image. You cannot delete the active image.

6. Click the **Delete Image** button for the image that is *not* the active image.

   Your settings are saved and the image is removed.

Diagnostics and troubleshooting

You can send a ping, trace a route, and perform a memory dump.

Ping an IPv4 address

You can configure the switch to send a ping request to a specified IPv4 address. You can use this option to check whether the switch can communicate with a particular IPv4 device. When you send a ping, the switch sends a specified number of ping requests and the results are displayed.

If a reply to the ping is received, the following message displays:

```
PING x.y.z.w (x.y.z.w): size data bytes
```

```
size bytes from x.y.z.w: seq=0 ttl=xyz
```

```
--- x.y.z.w ping statistics ---
```

```
count packets transmitted, count packets received, x% packet loss
```

If a reply to the ping is not received, the following message displays:

```
PING x.y.z.w (x.y.z.w): size data bytes
```

```
--- x.y.z.w ping statistics ---
```

```
count packets transmitted, 0 packets received, 100% packet loss
```

To ping an IPv4 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 and enter the IP address of the switch in the address field of your web browser.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Maintenance > Troubleshooting > Ping IPv4**.

   The Ping IPv4 page displays.
6. In the **IP Address/Hostname** field, type the IP address or host name of the device that must be pinged.

   The format is x.x.x.x. The maximum number of characters is 255.
7. In the **Count** field, type the number of echo requests that must be sent.

   The default setting is 3. The range is from 1 to 15.
8. In the **Interval** field, type the time between ping packets in seconds.

   The default setting is 3 seconds. The range is from 1 to 60.
9. In the **Size** field, type the size of the ping packet.

   The default setting is 0 bytes. The range is from 0 to 13000.
10. From the **Source** menu, as an option, you can select the IP address or interface that must be used to send echo request packets:

    - **None**: The source address of the ping packet is the address of the default egress interface.
    - **IP Address**: The source IP address that must be used when echo request packets are sent.

      With this selection, the **IP Address** field displays and you must type the IPv4 address that must be used as the source.
    - **Interface**: The interface that must be used when echo request packets are sent.

      With this selection, the **Interface** menu displays, and you must select a VLAN from the menu.
11. Click the **Apply** button.

    The specified address is pinged. The results are displayed below the configurable data in the Results field.

Ping an IPv6 address

You can configure the switch to send a ping request to a specified IPv6 address. You can use this option to check whether the switch can communicate with a particular IPv6 device. When you send a ping, the switch sends a specified number of ping requests and the results are displayed.

If a reply to the ping is received, the following message displays:

```
PING x:y::z:w (x:y::z:w): size data bytes
```

```
size bytes from x:y::z:w: seq=0 ttl=xyz
```

```
--- x:y::z:w ping statistics ---
```

```
count packets transmitted, count packets received, x% packet loss
```

If a reply to the ping is not received, the following message displays:

```
PING x:y::z:w (x:y::z:w): size data bytes
```

```
--- x:y::z:w ping statistics ---
```

```
count packets transmitted, 0 packets received, 100% packet loss
```

To ping an IPv6 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard 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 specific VLAN interface. With this selection, the **Interface** menu displays, and you must select a VLAN from the menu.
7. In the **IPv6 Address/Host Name** field, type the IPv6 address or host name of the device that must be pinged.

   The format is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. The maximum number of characters is 255.
8. In the **Count** field, type the number of echo requests that must be sent.

   The range is from 1 to 15. The default setting is 3.
9. In the **Interval** field, type the time in seconds between ping packets.

   The range is from 1 to 60. The default setting is 3 seconds.
10. In the **Datagram Size** field, type the datagram size.

    The valid range is from 0 to 13000. The default setting is 0 bytes.
11. From the **Source** menu, as an option, you can select the IP address or interface that must be used to send echo request packets:
    - **None**: The source address of the ping packet is the address of the default egress interface.
    - **IP Address**: The source IP address that must be used when echo request packets are sent.

      With this selection, the **IP Address** field displays and you must type the IPv6 address that must be used as the source.
    - **Interface**: The interface that must be used when echo request packets are sent.

      With this selection, the **Interface** menu displays, and you must select a VLAN from the menu.
12. Click the **Apply** button.

    The specified address is pinged. The results are displayed below the configurable data in the Results field.

Send an IPv4 traceroute

You can configure the switch to send a traceroute request to a specified IPv4 address or host name. You can use this to discover the paths that packets take to a remote

destination. When you send a traceroute, the switch displays the results below the configurable data.

If a reply to the traceroute is received, the following message displays:

```
traceroute to x.y.z.w (x.y.z.w), maxTTL hops max, size byte packets
```

```
initTTL x.y.z.w (x.y.z.w) 0.000 ms * 0.000 ms
```

```
initTTL+1 x.y.z.w (x.y.z.w) 0.000 ms * 0.000 ms
```

```
initTTL+2 x.y.z.w (x.y.z.w) 0.000 ms * 0.000 ms
```

To send an IPv4 traceroute:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Maintenance > Troubleshooting > Traceroute IPv4**.

   The Traceroute IPv4 page displays.
6. In the **IP Address/Hostname** field, type the IP address or host name of the device for which the path must be discovered.
7. In the **Probes Per Hop** field, type the number of probes per hop.

   The default setting is 3. The range is from 1 to 10.
8. In the **Max TTL** field, type the maximum time to live (TTL) for the destination.

   The default setting is 30. The range is from 1 to 255.
9. In the **Init TTL** field, type the initial TTL to be used.

   The default setting is 1. The range is from 1 to 255.

10. In the **MaxFail** field, type the maximum number of failures allowed in the session.

    The default setting is 5. The range is from 1 to 255.
11. In the **Interval** field, type the time between probes in seconds.

    The default setting is 3 seconds. The range is from 1 to 60.
12. In the **Port** field, type the UDP destination port for the probe packets.

    The default setting is 33434. The range is from 1 to 65535.
13. In the **Size** field, type the size of the probe packets.

    The default setting is 38. The range is from 38 to 32768.
14. From the **Source** menu, as an option, you can select the IP address or interface that must be used to send probe packets:

    - **None**: The source address of the ping packet is the address of the default egress interface.
    - **IP Address**: The source IP address that must be used when echo request packets are sent.

      With this selection, the **IP Address** field displays and you must type the IPv4 address that must be used as the source.
    - **Interface**: The interface that must be used when echo request packets are sent.

      With this selection, the **Interface** menu displays, and you must select a VLAN from the menu.
15. Click the **Apply** button.

    A traceroute request is sent to the specified IP address or host name. The results are displayed below the configurable data in the Results field.

Send an IPv6 traceroute

You can configure 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. When you send a traceroute, the switch displays the results below the configurable data.

If a reply to the traceroute is received, the following message displays:

```
traceroute to x:y::z:w (x:y::z:w), maxTTL hops max, size byte packets
```

```
initTTL x:y::z:w (x:y::z:w) 0.000 ms * 0.000 ms
```

```
initTTL+1 x:y::z:w (x:y::z:w) 0.000 ms * 0.000 ms
```

```
initTTL+2 x:y::z:w (x:y::z:w) 0.000 ms * 0.000 ms
```

To send an 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Maintenance > Troubleshooting > Traceroute IPv6**.

   The Traceroute IPv6 page displays.
6. In the **IPv6 Address/Host Name** field, type the IPv6 address or host name of the device for which the path must be discovered.
7. In the **Probes Per Hop** field, type the number of probes per hop.

   The default setting is 3. The range is from 1 to 10.
8. In the **Max TTL** field, type the maximum time to live (TTL) for the destination.

   The default setting is 30. The range is from 1 to 255.
9. In the **Init TTL** field, type the initial TTL to be used.

   The default setting is 1. The range is from 1 to 255.
10. In the **MaxFail** field, type the maximum number of failures allowed in the session.

    The default setting is 5. The range is from 1 to 255.

11. In the **Interval** field, type the time between probes in seconds.

    The default setting is 3 seconds. The range is from 1 to 60.

12. In the **Port** field, type the UDP destination port for the probe packets.

    The default setting is 33434. The range is from 1 to 65535.

13. In the **Size** field, type the size of the probe packets.

    The default setting is 38. The range is from 38 to 32768.

14. From the **Source** menu, as an option, you can select the IP address or interface that must be used to send probe packets:

    - **None**: The source address of the ping packet is the address of the default egress interface.
    - **IP Address**: The source IP address that must be used when echo request packets are sent.

      With this selection, the **IP Address** field displays and you must type the IPv6 address that must be used as the source.
    - **Interface**: The interface that must be used when echo request packets are sent.

      With this selection, the **Interface** menu displays, and you must select a VLAN from the menu.

15. Click the **Apply** button.

    A traceroute request is sent to the specified IP address or host name. The results are displayed below the configurable data in the Results field.

Enable the secure diagnostic mode

Secure diagnostics mode connects the switch to NETGEAR's diagnostic server, allowing support personnel to remotely diagnose your system. In this mode, changes to the default configuration are not saved.

To enable the secure diagnostic 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Maintenance > Troubleshooting > Secure Diagnostics**.

   The Secure Diagnostics page displays.
6. Click the **Secure Diagnostic Mode** toggle to enable the secure diagnostic mode:
   - **The toggle is gray and positioned to the left**: Secure diagnostic mode is disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: Secure diagnostic mode will be enabled after you click the **Apply** button.

     A confirmation pop-up window displays. Click the **OK** button to close the window.
7. Click the **Apply** button.

   Your settings are saved.

   After the connection to the server is established, the Port field displays the switch port that is connected to the server.

You cannot log in to the switch

After you enter the wrong password three times, your switch blocks further attempts to log in. The block lasts longer each time until you get the password right:

- After 3 times: 5 minutes
- After 6 times: 10 minutes
- After 9 times: 20 minutes
- After 12 times: 40 minutes
- After 15 times: 60 minutes
- After 18 times: 60 minutes

10

Monitor the Switch and Network

This chapter covers the following topics:

- Switch, port, and EAP packet statistics
- Perform a cable test
- Logs
- Port mirroring
- Switch CPU

Switch, port, and EAP packet statistics

You can view switch and port statistics, including detailed statistics, and Extensible Authentication Protocol (EAP) packets statistics.

Display or clear switch statistics

You can display statistical information about the traffic that the switch processes.

To display or clear 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Monitoring > Ports > Switch Statistics**.

   The Switch Statistics page displays.
6. To clear the counters, click the **Clear** button.
7. To refresh the page, click the **Refresh** button.

The following table describes the switch statistics on the page.

Table 79. Switch statistics information

Field	Description
Unicast Packets	
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol

Table 79. Switch statistics information (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	
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.
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
Octets	
Octets Received	The total number of octets of data received by the switch, excluding framing bits, but including FCS octets
Octets Transmitted	The total number of octets transmitted by the switch, including framing characters
Broadcast Packets	
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. This number does not include multicast packets.
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	
Most Address Entries Ever Used	The highest number of entries in the forwarding database address table that were learned by the switch since the most recent reboot
Address Entries in Use	The number of learned and static entries in the forwarding database address table for the switch
ifindex	
ifindex	The interface index of the interface table entry associated with the processor of the switch
Packets	
Receive Packets Discarded	The number of inbound packets that were discarded, even though no errors were detected, to prevent them from being delivered to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Transmit Packets Discarded	The number of outbound packets that were discarded, even though no errors were detected, to prevent them from being delivered to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Packets Received Without Errors	The total number of packets (including broadcast packets and multicast packets) received by the switch

Table 79. Switch statistics information (Continued)

Field	Description
Packets Transmitted Without Errors	The total number of packets transmitted by the switch
VLAN	
Maximum VLAN Entries	The maximum number of VLANs allowed on the switch
Most VLAN Entries Ever Used	The largest number of VLANs that were active on the switch since the last reboot
Static VLAN Entries	The number of active VLAN entries on the switch that were created statically
VLAN Deletes	The number of VLANs on the switch that were created and then deleted since the last reboot
Time Since Counters	
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for the switch were last cleared

Display or clear port statistics

You can display a summary of per-port traffic statistics on the switch and clear the statistics.

To view or clear 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Monitoring > Ports > Port Statistics**.

The Port Statistics page displays.

6. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**All**).
7. To find a single interface, select the check box associated with the interface, or type the port or LAG number in the **Search** field and click the **Go** button.
8. To clear counters, do one of the following:
   - To clear all the counters for all ports and LAGs on the switch, select the check box in the row heading and click the **Clear** button.
   - To clear the counters for a specific port or LAG, select the check box for the interface and click the **Clear** button.
9. To refresh the page, click the **Refresh** button.

The following table describes the per-port statistics on the page.

Table 80. Port statistics information

Field	Description
Interface	The port for which information is displayed
Total Packets Received Without Errors	The total number of packets that were received without errors
Packets Received With Errors	The number of inbound packets that contained errors, preventing them from being delivered to a higher-layer protocol
Broadcast Packets Received	The number of good packets received that were directed to the broadcast address. This does not include multicast packets.
Packets Transmitted Without Errors	The number of frames that were transmitted by this port to its segment
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors
Collision Frames	The best estimate of the total number of collisions on this Ethernet segment
Link Down Events	The total number of link down events on the port
Time since counters last cleared	The elapsed time in days, hours, minutes, and seconds since the statistics for this port were last cleared

Display or clear detailed statistics for a port

For a specific port, you can display a variety of per-port traffic statistics or clear the statistics.

To display and clear detailed statistics 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Monitoring > Ports > Port Detailed Statistics**.

   The Port Detailed Statistics page displays.
6. From the **Interface** menu, select the interface (a physical port or LAG) for which you want to display the statistics.
7. From the **MST ID** menu, select the MST ID associated with the interface (if available).
8. To clear all the counters, click the **Clear** button.

   All statistics for the port are reset to the default values.
9. To refresh the page, click the **Refresh** button.

The following table describes the detailed port statistics on the page.

Table 81. Port detailed statistics information

Field	Description
ifIndex	The ifIndex of the interface table entry associated with the port
Port Type	The port is either displayed blank for a normal port, or as one of the following types of ports: • **Mirrored**: The port is a mirrored port in a port mirroring configuration • **Probe**: The port is the probe port in a port mirroring configuration • **Port Channel**: The port is a member of a LAG
Port Channel ID	If the port is a member of a port channel, the port channel's interface ID and name display. Otherwise, Disable displays.
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 81. Port detailed statistics information (Continued)

Field	Description
STP Mode	The Spanning Tree Protocol administrative mode that is associated with the port or port channel. The options are Enable (spanning tree is enabled for the port) or Disable (spanning tree is disabled for the port).
STP State	The current spanning tree state of the port. This state controls what action a port takes on receipt of a frame. If the bridge detects a malfunctioning port it places that port into the broken state. The states are defined in IEEE 802.1D: • Disabled • Blocking • Listening • Learning • Forwarding • Broken
Admin Mode	The port control administration state. The port must be enabled for it to be allowed into the network. The default is Enable.
Flow Control Mode	Indicates if flow control is enabled or disabled for the port. This field does not apply to LAGs.
LACP Mode	The Link Aggregation Control Protocol (LACP) administrative state. The mode must be enabled for the port to participate in link aggregation.
Physical Mode	The port speed and duplex mode. In autonegotiation mode (Auto), the duplex mode and speed are set by the autonegotiation process.
Physical Status	The port speed and duplex mode
Link Status	Indicates if the link is up or down
Link Trap	Indicates if the port sends a trap when the link status changes
Packets RX and TX 64 Octets	The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets)
Packets RX and TX 65-127 Octets	The total number of packets (including bad packets) received or transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets)
Packets RX and TX 128-255 Octets	The total number of packets (including bad packets) received or transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets)
Packets RX and TX 256-511 Octets	The total number of packets (including bad packets) received or transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets)
Packets RX and TX 512-1023 Octets	The total number of packets (including bad packets) received or transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets)

Table 81. Port detailed statistics information (Continued)

Field	Description
Packets RX and TX 1024-1518 Octets	The total number of packets (including bad packets) received or transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets)
Octets Received	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects must be sampled before and after a common interval.
Packets Received 64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets)
Packets Received 65-127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Received 128-255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Received 256-511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Received 512-1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Received 1024-1518 Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Received > 1518 Octets	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed
Total Packets Received Without Errors	The total number of packets received that were without errors
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-Layer protocol
Multicast Packets Received	The total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. This does not include multicast packets.
Receive Packets Discarded	The number of inbound packets that were discarded, even though no errors were detected that would prevent the packets from being delivered to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

Table 81. Port detailed statistics information (Continued)

Field	Description
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 had either a bad frame check sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (alignment error). This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Fragments Received	The total number of packets received that were less than 64 octets in length with ERROR CRC (excluding framing bits but including FCS octets)
Undersize Received	The total number of packets received that were less than 64 octets in length with GOOD CRC (excluding framing bits but including FCS octets)
Alignment Errors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad frame check sequence (FCS) with a nonintegral number of octets
Rx FCS Errors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad frame check sequence (FCS) with an integral number of octets
Total Received Packets Not Forwarded	The number of valid frames received that were discarded (that is, filtered) by the forwarding process
802.3x Pause Frames Received	The number of MAC control frames received 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 (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects must be sampled before and after a common interval.
Packets Transmitted 64 Octets	The total number of packets (including bad packets) transmitted that were 64 octets in length (excluding framing bits but including FCS octets)
Packets Transmitted 65-127 Octets	The total number of packets (including bad packets) transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Transmitted 128-255 Octets	The total number of packets (including bad packets) transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Transmitted 256-511 Octets	The total number of packets (including bad packets) transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets)

Table 81. Port detailed statistics information (Continued)

Field	Description
Packets Transmitted 512-1023 Octets	The total number of packets (including bad packets) transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Transmitted 1024-1518 Octets	The total number of packets (including bad packets) transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets)
Packets Transmitted > 1518 Octets	The total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. This counter has a max increment rate of 815 counts per sec at 10 Mb/s.
Maximum Frame Size	The maximum Ethernet frame size that the interface supports or is configured to use, including the Ethernet header, CRC, and payload. The possible range is from 1522 to 10000. The default maximum frame size is 1522.
Total Packets Transmitted Successfully	The number of frames that the port transmitted to its segment
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the broadcast address, including those that were discarded or not sent
Transmit Packets Discarded	The total number of outbound packets that were discarded even though no errors were detected that would prevent the packets from being delivered to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Total Transmit Errors	The sum of single, multiple, and excessive collisions
Total Transmit Packets Discarded	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision
Multiple Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by more than one collision
Excessive Collision Frames	The number of frames for which transmission failed due to excessive collisions
Dropped Transmit Frames	The number of transmit frames discarded
STP BPDUs Received	The number of STP BPDUs received
STP BPDUs Transmitted	The number of STP BPDUs transmitted

Table 81. Port detailed statistics information (Continued)

Field	Description
RSTP BPDUs Received	The number of RSTP BPDUs received
RSTP BPDUs Transmitted	The number of RSTP BPDUs transmitted
MSTP BPDUs Received	The number of MSTP BPDUs received
MSTP BPDUs Transmitted	The number of MSTP BPDUs transmitted
802.3x Pause Frames Transmitted	The number of MAC control frames transmitted with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
GVRP PDUs Received	The number of GVRP PDUs received in the GARP Layer
GVRP PDUs Transmitted	The number of GVRP PDUs transmitted from the GARP Layer
GVRP Failed Registrations	The number of times attempted GVRP registrations could not be completed
EAPOL Frames Received	The number of valid EAPOL frames of any type that were received by the authenticator
EAPOL Frames Transmitted	The number of EAPOL frames of any type that were transmitted by the authenticator
Time Since Counters Last Cleared	The elapsed time in days, hours, minutes, and seconds since the statistics for the port were last cleared

Display or clear EAP and EAPoL statistics

You can display information about Extensible Authentication Protocol (EAP) and EAP over LAN (EAPoL) packets that are received on physical ports. You can also clear the statistics for individual ports.

To display or clear EAP and EAPoL statistics:

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

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

2. Launch a web browser and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Monitoring > Ports > EAP Statistics**.

   The EAP Statistics page displays.
6. To clear the counters, which resets the EAP and EAPoL statistics to default values, take one of the following actions:

   - To clear the counters for a specific port, select the check box associated with the port, and click the **Clear** button.
   - To clear the counters for multiple ports, select the check boxes associated with the ports, and click the **Clear** button.
7. To refresh the page, click the **Refresh** button.

The following table describes the EAP statistics on the page.

Table 82. EAP statistics information

Field	Description
Ports	The number of the port for which information is displayed
EAPOL	
Frames Received	The number of valid EAPOL frames of any type that were received by the authenticator
Frames Transmitted	The number of EAPOL frames of any type that were transmitted by the authenticator
Start Frames Received	The number of EAPOL start frames that were received by the authenticator
Logoff Frames Received	The number of EAPOL logoff frames that were received by the authenticator
Last Frame Version	The protocol version number carried in the most recently received EAPOL frame
Last Frame Source	The source MAC address carried in the most recently received EAPOL frame
Invalid Frames Received	The number of EAPOL frames that were received by the authenticator in which the frame type is not recognized
Length Error Frames Received	The number of EAPOL frames that were received by the authenticator in which the frame length is incorrect
EAP	
Response/ID Frames Received	The number of EAP response/identity frames that were received by the authenticator
Response Frames Received	The number of valid EAP response frames (other than resp/ID frames) that were received by the authenticator

Table 82. EAP statistics information (Continued)

Field	Description
Request/ID Frames Transmitted	The number of EAP request/identity frames that were transmitted by the authenticator
Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that were transmitted by the authenticator

Perform a cable test

You can test and display information about the cables that are connected to switch ports.

To perform a cable test:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard 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 the selected interface. The cable test might take up to two seconds to complete. If the port has an active link, the cable status is always Normal. The command returns a cable length estimate if this feature is supported by the PHY for the current link speed. Note that if the link is down and a cable is

attached to a 10/100 Ethernet adapter then the cable status might be Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded.

The following table describes the view-only fields on the page.

Table 83. Cable Test

Field	Description
Cable Status	Indicates the cable status: • **Normal**: The cable is working correctly. • **Open**: The cable is disconnected, or a faulty connector exists. • **Short**: An electrical short exists in the cable. • **Cable Test Failed**: The cable status could not be determined. The cable might in fact be working. • **Untested**: The cable is not yet tested. • **No Cable**: No cable is detected, or the cable length is too small to be tested accurately. • **Port Disabled**: The port is disabled, and the cable cannot be tested.
Cable Length	The estimated length of the cable in meters. The length is displayed as a range between the shortest estimated length and the longest estimated length. Unknown is displayed if the cable length could not be determined. The cable length is displayed only if the cable status is Normal.
Failure Location	The estimated distance in meters from the end of the cable to the failure location. The failure location is displayed only if the cable status is Open or Short.

Logs

The switch generates messages in response to events, faults, and errors as well as changes in the 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 (see Syslog and log server host settings on page 477). Local and remote configuration of the logging capability includes filtering of messages logged or forwarded based on severity and generating component.

Message log format

This topic applies to the format of all logged messages that are displayed for the message log, persistent log, or console log.

Messages logged to a collector or relay through syslog use an identical format:

- `<15>Aug 24 05:34:05 0.0.0.0-1 MSTP[2110]: mspt_api.c(318) 237%% Interface 12 transitioned to root state on message age timer expiry.`

  This example indicates a message with severity 7 (15 mod 8) (debug) on a switch and generated by component MSTP running in thread ID 2110 on Aug 24 05:34:05 by line 318 of file mstp_api.c. This is the 237th message logged with system IP 0.0.0.0 and task-ID 1.
- `<15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237%% Interface 12 transitioned to root state on message age timer expiry.`

  This example indicates a user-level message (1) with severity 7 (debug) on a system that is not a switch and generated by component MSTP running in thread ID 2110 on Aug 24 05:34:05 by line 318 of file mstp_api.c. This is the 237th message logged. Messages logged to a collector or relay through syslog use a format identical to the previous message.
- Total number of Messages: For the message log, only the latest 200 entries are displayed on the page.

Manage and display the memory log

The memory log stores messages in memory based upon the settings for message component and severity. You can set the administrative status and behavior of logs in the system buffer. These log messages are cleared when the switch reboots.

To manage and display the memory log:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Monitoring > Logs > Memory Log**.

   The Memory Log page displays.

   The following steps refer to the Memory Log Configuration section.

6. Click the **Memory Logging** toggle to enable or disable memory logging:
   - **The toggle is gray and positioned to the left**: Memory logging is disabled, which prevents the switch from logging default messages.
   - **The toggle is purple and positioned to the right**: Memory logging is enabled, which enables the switch to log default messages. This is the default setting.
7. From the **Behavior** menu, specify the behavior of the log when it is full:
   - **Wrap**: When the buffer is full, the oldest log messages are deleted as the system logs new messages.
   - **Stop on Full**: When the buffer is full, the system stops logging new messages and preserves all existing log messages.
8. From the **Severity Filter** menu, select the logging level for messages that must be logged.

   Log messages with the selected severity level and all log messages of greater severity are logged. For example, if you select Warning, the logged messages include Warning, Error, Critical, Alert, and Emergency. The default severity level is Informational (6).

   The severity can be one of the following levels:
   - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
   - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
   - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
   - **Error**: Level 3, a device error occurred, such as a port being offline.
   - **Warning**: Level 4, the lowest level of a device warning.
   - **Notice**: Level 5, provides the network administrators with device information.
   - **Informational**: Level 6, provides device information. This is the default setting.
   - **Debug**: Level 7, provides detailed information about the log.

   Note: A log records messages equal to or above a configured severity threshold.
9. Click the **Apply** button.

   Your settings are saved.

The Memory Log table displays in the Memory Log section.

The Total Number of Messages field displays the number of messages the system logged in memory. Up to 200 entries can be displayed on the page.

The rest of the page displays the Memory Log messages. The format of the log message is the same for messages that are displayed for the message log, persistent log, or console log. Messages logged to a collector or relay through syslog support the same format as well.

The following example shows the standard format for a log message:

```
<189> Jan 05 2023 00:00:18: AAA-5-CONNECT: New http connection
for user admin, source 192.168.1.111 ACCEPTED
```

The message was generated as severity 189 (Notice, level 5) on January 5, 2023 at 00:00:18 a.m. by component AAA. The message indicates that the administrator successfully logged on to the HTTP management interface from a host with IP address 192.168.1.111.

The severity number in the message is generated by a combination of the facility and the severity. In the previous example, the default facility of 23 is multiplied by 8 and the severity (5) is added: (23 * 8) + 5 = 189

10. To refresh the page, click the **Refresh** button.
11. To clear the log, click the **Clear** button.

Manage and display the flash log

The flash log is a persistent log, that is, is a log that is stored in persistent storage. Persistent storage survives across platform reboots. The first log type is the system startup log. The system startup log stores the first 32 messages received after system reboot. The second log type is the system operation log. The system operation log stores messages received during system operation.

To manage and display 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Monitoring > Logs > FLASH Log**.

   The FLASH Log page displays.

   The following steps refer to the FLASH Log Configuration section.
6. Click the **FLASH Logging** toggle to enable or disable flash logging:
   - **The toggle is gray and positioned to the left**: Flash logging is disabled, which prevents the switch from logging messages to flash memory. This is the default setting.
   - **The toggle is purple and positioned to the right**: Flash logging is enabled, which enables the switch to log messages to flash memory.
7. From the **Severity Filter** menu, select the logging level for messages that must be logged.

   Log messages with the selected severity level and all log messages of greater severity are logged. For example, if you select Warning, the logged messages include Warning, Error, Critical, Alert, and Emergency. The default severity level is Informational (6).

   The severity can be one of the following levels:
   - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
   - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
   - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
   - **Error**: Level 3, a device error occurred, such as a port being offline. This is the default setting.
   - **Warning**: Level 4, the lowest level of a device warning.
   - **Notice**: Level 5, provides the network administrators with device information.
   - **Informational**: Level 6, provides device information.
   - **Debug**: Level 7, provides detailed information about the log.

   Note: A log records messages equal to or above a configured severity threshold.

8. From the **Logs to be Displayed** menu, select one of the following options:
   - **Current Logs**: The log messages for the current switch sessions are displayed. This is the default setting.
   - **Previous Logs**: The previous log messages are displayed, that is, the log messages that are still in the flash memory from before the switch was rebooted.
9. Click the **Apply** button.

   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 maximum number of persistent log messages displayed on the switch is 64.

   The following example shows the standard format for a persistent log message:

   ```
   Jan 12 2023 00:00:18: AAA-5-CONNECT: New http connection for
   user admin, source 192.168.1.111 ACCEPTED
   ```

   The message was generated as severity 189 (Notice, level 5) on January 12, 2023 at 00:00:18 a.m. by component AAA. The message indicates that the administrator successfully logged on to the HTTP management interface from a host with IP address 192.168.1.111.

   The severity number in the message is generated by a combination of the facility and the severity. In the previous example, the default facility of 23 is multiplied by 8 and the severity (5) is added: (23 * 8) + 5 = 189
10. To refresh the page, click the **Refresh** button.

Syslog and log server host settings

You can let the switch send log messages to one or more servers, that is, to remote logging hosts. A remote log server is the same as a remote syslog host.

You must enable the server log on the switch and specify one or more remote syslog hosts.

Configure the syslog settings

You can globally enable or disable the syslog settings.

To configure the global syslog 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Monitoring > Logs > Server Log**.

   The Server Log page displays.

6. Click the **Server Logging** toggle to enable or disable server logging:
   - **The toggle is gray and positioned to the left**: Server logging is disabled, which prevents the switch from logging messages to a server. This is the default setting.
   - **The toggle is purple and positioned to the right**: Server logging is enabled, which enables the switch to log messages to a server.
7. Click the **Apply** button.

   Your settings are saved.

Add a syslog server

You can add multiple syslog servers.

To add a syslog 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Monitoring > Logs > Server Log**.

   The Server Log page displays.
6. Click the **Add New** button.

   The Add Server Configuration pop-up window displays.
7. From the **IP Address Type** menu, select type of IP address of the syslog server.

   You can select **IPv4**, **IPv6**, or **DNS**.
8. In **Host Address** field, depending on your selection from the **IP Address Type** menu, type the IPv4 address, IPv6 address, or DNS name of the syslog server.
9. In the **Port** field, type the port number that the syslog server uses.
10. From the **Severity Filter** menu, select the severity of the logs that must be sent to the syslog server.

    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.

    Select one of the following security levels:

    - **Emergency**: Level 0, the highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
    - **Alert**: Level 1, the second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
    - **Critical**: Level 2, the third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
    - **Error**: Level 3, a device error occurred, such as a port being offline.
    - **Warning**: Level 4, the lowest level of a device warning.
    - **Notice**: Level 5, provides the network administrators with device information.
    - **Informational**: Level 6, provides device information.
    - **Debug**: Level 7, provides detailed information about the log.
11. Click the **Save** button.

    Your settings are saved and the syslog server is added.

The Status field in the Server Configuration table shows whether the syslog server is currently active.

Change the settings for a syslog server

You can change the settings to an existing syslog server.

To change the settings for a syslog 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Monitoring > Logs > Server Log**.

   The Server Log page displays.
6. Select the check box for the syslog server.
7. Click the **Edit** button.

   The Edit Server Configuration pop-up window displays
8. Change the settings as needed.

   For more information about the settings, see Add a syslog server on page 478.
9. Click the **Save** button.

   Your settings are saved.

Delete the settings for a syslog server

You can delete the settings for a syslog server that you no longer need.

To delete the settings for a syslog 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Monitoring > Logs > Server Log**.

   The Server Log page displays.

6. Select the check box for the syslog server.
7. Click the **Delete** button.

   Your settings are saved and the syslog server is removed.

Trap log

The trap log includes information about the traps that the switch sent. You can display and clear the counters and entries in the trap log.

To display or clear the trap 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.

4. Click the **Login** button.
   The Dashboard page displays.
5. Select **Monitoring > Logs > Trap Logs**.
   The Trap Logs page displays.
6. To clear the counters and log, click the **Clear** button.
7. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 84. Trap log information

Field	Description
Number of Traps Since Last Reset	The number of traps that occurred since the switch last rebooted
Trap Log Capacity	The maximum number of traps stored in the log. If the number of traps exceeds the capacity, the new entries overwrite the oldest entries.
Number of Traps since log last viewed	The number of traps that occurred since the traps were last displayed
Log	The sequence number of this trap
System Up Time	The time when this trap occurred, expressed in days, hours, minutes and seconds, since the last reboot of the switch
Trap	Information about the trap

Port mirroring

Port mirroring lets you select the network traffic of specific switch ports for analysis by a network analyzer. You can select many switch ports as source ports but only a single switch port as the destination port.

A packet that is mirrored (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.

Set up a port mirroring configuration

You can mirror traffic of multiple physical ports and LAGs to a single destination port (the probe). The mirrored traffic can be incoming, outgoing, or both incoming and outgoing traffic.

To set up a port mirroring configuration:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Monitoring > Port Mirroring**.

   The Port Mirroring page displays.
6. Click the **Port Mirroring** toggle to enable or disable port mirroring:
   - **The toggle is gray and positioned to the left**: Port mirroring is disabled. This is the default setting.
   - **The toggle is purple and positioned to the right**: Port mirroring is enabled.
7. From the **Destination Port** menu, select the destination port to which traffic must be copied.

   You can select one destination port only.

   The following steps refer to the Source Interface Configuration section.
8. Click the **Apply** button.

   Your settings are saved.

   The Status field displays Probe for the destination port.
9. From the **Filter By** menu, select to display ports only (**Ports**), LAGs only (**LAG**), or both ports and LAGs (**All**).
10. Select one or more source ports, LAGs, or both by taking one of the following actions:
    - To select a single port or LAG, select the check box associated with the port, or type the port number (for example, g5) in the **Search** field and click the **Go** button.
    - To select multiple ports, LAGs, or both, select the check box associated with each port and LAG.

11. Click the **Edit** button.

    The Edit Source Interface Configuration pop-up window displays.
12. From the **Direction** menu, select the direction of the traffic that must be mirrored:
    - **None**: No direction is configured. This is the default.
    - **Tx and Rx**: Transmitted (Tx) and received (Rx) packets are copied to the destination port.
    - **Rx**: Received packets only are copied to the destination port.
    - **Tx**: Transmitted (Tx) packets only are copied to the destination port.
13. Click the **Save** button.

    Your settings are saved.

    The Status field displays Mirrored for the source port or ports.

Remove a port mirroring probe

You can remove a port mirroring probe that you no longer need.

To remove a port mirroring probe:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Monitoring > Port Mirroring**.

   The Port Mirroring page displays.
6. From the **Destination Port** menu, select **None**.
7. Click the **Apply** button.

Your settings are saved and the probe is removed.

Switch CPU

You can display information about the status of the switch CPU and set CPU thresholds that can generate notifications.

Display the system CPU memory status and CPU utilization

You can display information about the CPU memory status and CPU utilization on the switch.

To display the system CPU memory status and CPU 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 and enter the IP address of the switch in the address field of your web browser.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Monitoring > System CPU Status > System CPU Status**.

   The System CPU Status page displays.
6. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the page.

Table 85. System CPU status information

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

The CPU Utilization section displays the CPU utilization by the various processes on the switch.

Configure the CPU thresholds

You can configure CPU thresholds that trigger a notification if exceeded. The notification occurs through SNMP trap and syslog messages.

To configure the CPU thresholds:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Monitoring > System CPU Status > CPU Threshold**.

   The CPU Threshold page displays.
6. In the **Rising Threshold** field, type the rising threshold value.

   A notification is generated when the total CPU utilization exceeds this threshold value over the configured period. The range is a percentage from 1 to 100.
7. In the **Rising Interval** field, type the rising interval value.

   Configure this utilization monitoring period from 5 to 86400 seconds in multiples of 5 seconds.
8. In the **Falling Threshold** field, type the falling threshold.

A notification is triggered when the total CPU utilization falls below this level for a configured period.

The falling utilization threshold must be equal to or less than the rising threshold value. The falling utilization threshold notification is generated only if a rising threshold notification was generated previously. Configuring the falling utilization threshold and period is optional. If the falling CPU utilization values are not configured, they take the same value as the rising CPU utilization values. The range is a percentage from 1 to 100.

9. In the **Falling Interval** field, type the falling interval.

   You can configure the utilization monitoring period from 5 seconds to 86400 seconds in multiples of 5 seconds.

10. In the **Free Memory Threshold** field, type the CPU free memory threshold value in KB.
11. Click the **Apply** button.

    Your settings are saved.

A

Configuration Examples

This appendix contains information about how to configure the following features:

- Virtual Local Area Networks (VLANs)
- Access control lists (ACLs)
- Differentiated Services (DiffServ)
- 802.1X port access control
- Multiple Spanning Tree Protocol

Virtual Local Area Networks (VLANs)

A local area network (LAN) can generally be defined as a broadcast domain. Hubs, bridges, or switches in the same physical segment or segments connect all end node devices. End nodes can communicate with each other without the need for a router. Routers connect LANs together, routing the traffic to the appropriate port.

A virtual LAN (VLAN) is a local area network with a definition that maps workstations on some basis other than geographic location (for example, by department, type of user, or primary application). To enable traffic to flow between VLANs, traffic must go through a router, just as if the VLANs were on two separate LANs.

A VLAN is a group of computers, servers, and other network resources that behave as if they were connected to a single network segment—even though they might not be. For example, all marketing personnel might be spread throughout a building. Yet if they are all assigned to a single VLAN, they can share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specified individuals, depending on how the IT manager has set up the VLANs.

VLANs present a number of advantages:

- It is easy to do network segmentation. Users that communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group's traffic is contained largely within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.
- They are easy to manage. The addition of nodes, as well as moves and other changes, can be dealt with quickly and conveniently from a management interface rather than from the wiring closet.
- They provide increased performance. VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.
- They ensure enhanced network security. VLANs create virtual boundaries that can be crossed only through a router. So standard, router-based security measures can be used to restrict access to each VLAN.

Packets received by the switch are treated in the following way:

- When an untagged packet enters a port, it is automatically tagged with the port's default VLAN ID tag number. Each port supports a default VLAN ID setting that is configurable (the default setting is 1). For information about changing the default VLAN ID setting for a port, see Change the port VLAN ID (PVID) settings on page 127.
- 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 enters 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 (T) or untagged (U), depending on the setting for that port's VLAN membership properties. A U for a port means that packets leaving the switch from that port are untagged. A T for a port means that packets leaving the switch from that port are tagged with the VLAN ID that is associated with the port.

The example in this section comprises numerous steps to illustrate a wide range of configurations to help provide an understanding of tagged VLANs.

VLAN example configuration

This example demonstrates several scenarios of VLAN use and describes how the switch handles tagged and untagged traffic.

In this example, you do the following:

1. Create two new VLANs (VLAN ID 10 and VLAN ID 20).
2. Change the port membership for default VLAN 1.
3. Assign port members to the two new VLANs.
4. Change the PVIDs for certain ports in the new VLANs.

To configure the VLAN example:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.

5. Select **Switching > VLAN > VLAN Management**.

   The VLAN Management page displays.
6. Create the new VLAN IDs:
   - Create a VLAN with VLAN ID 10:
     a. Click the **Add New** button.

        The Add VLAN Configuration pop-up window displays.
     b. In the **VLAN ID** field, type 10.
     c. In the **VLAN Name** field, type a name for the new VLAN or leave the field blank.
     d. Click the **Save** button.

        Your setting are saved and the VLAN is added.
   - Create a VLAN with VLAN ID 20:
     a. Click the **Add New** button.

        The Add VLAN Configuration pop-up window displays.
     b. In the **VLAN ID** field, type 20.
     c. In the **VLAN Name** field, type a name for the new VLAN or leave the field blank.
     d. Click the **Save** button.

        Your setting are saved and the VLAN is added.
7. Select **Switching > VLAN > VLAN Configuration (Basic)**.

   The VLAN Configuration (Basic) page displays.
8. Configure the membership for each VLAN:
   - For the default VLAN with VLAN ID 1, configure ports g7 and g8 as untagged (U) ports:
     a. From the **VLAN ID** menu, select **1**.
     b. In the Ports table, click port **7** and port **8**, click the **Clear** button, and then click the **Untag Port** button.

        By default, all ports are untagged members of default VLAN 1 and are assigned PVID 1.
     c. Click the **Apply** button.

        Your settings are saved.
   - For the VLAN with VLAN ID 10, configure ports g1 and g2 as untagged (U) ports and port g3 as a tagged (T) port:

a. From the **VLAN ID** menu, select **10**.
b. In the Ports table, click port **1** and port **2** and then click the **Untag Port** button.
c. Click the **Apply** button.

   Your settings are saved.
d. In the Ports table, click port **3** and then click the **Tag Port** button.
e. Click the **Apply** button.

   Your settings are saved.

- For the VLAN with VLAN ID 20, configure ports g4 and g6 as untagged (U) ports and port g5 as a tagged (T) port:
  a. From the **VLAN ID** menu, select **20**.
  b. In the Ports table, click port **4** and port **6** and then click the **Untag Port** button.
  c. Click the **Apply** button.

     Your settings are saved.
  d. In the Ports table, click port **5** and then click the **Tag Port** button.
  e. Click the **Apply** button.

     Your settings are saved.

9. Select **Switching > VLAN > VLAN Configuration (Advanced)**.

   The VLAN Configuration (Advanced) page displays.
10. Set the PVID for port g1 to VLAN ID 10 and the PVID for port g4 to VLAN ID 20 so that packets entering these ports are tagged with the VLAN ID:
    - Set the PVID for port g1 to VLAN with VLAN ID 10:
      a. Select the check box for port g1.
      b. Select the **Edit** button.

         The Edit PVID Configuration pop-up window displays.
      c. In the **PVID** field, type 10 for VLAN ID 10.
      d. Click the **Save** button.

         Your settings are saved.
    - Set the PVID for port g4 to VLAN with VLAN ID 20:
      a. Select the check box for port g4.
      b. Select the **Edit** button.

         The Edit PVID Configuration pop-up window displays.
      c. In the **PVID** field, type 20 for VLAN ID 20.
      d. Click the **Save** button.

Your settings are saved.

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 a sequential collection of permit and deny conditions. This collection of conditions, known as the filtering criteria, is applied to each packet that is processed by the switch or the router. The forwarding or dropping of a packet is based on whether or not the packet matches the specified criteria.

Traffic filtering requires the following two basic steps:

1. Create an access list definition.

   The access list definition includes one or more 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.

MAC ACL example configuration

The following example shows how to create a MAC-based ACL that permits IPv4 traffic on the VLAN with ID 2 from a particular computer in the sales department (the computer is identified by its MAC address), sends the traffic to a specific queue on specific ports, and denies all other traffic on those ports.

In this example, you do the following:

1. Create a MAC ACL with the name Sales_ACL.
2. Create a rule with the following criteria:
   - **Sequence Number**: 1
   - **Action**: Permit
   - **Assign Queue ID**: 4
   - **Match Every**: No
   - **EtherType**: IPv4
   - **Source MAC address**: 02:02:1A:BC:DE:EF
   - **Source MAC Mask**: 00:00:00:00:FF:FF
   - **VLAN ID**: 2, which is the VLAN that is used for the sales department.
3. Bind the Sales_ACL to ports 6, 7, and 8.

To configure the MAC ACL example:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

The Dashboard page displays.

5. Select **Security > ACL > MAC ACL > MAC ACL/Rules**.

   The MAC ACL/Rules page displays.

6. Add a MAC ACL:
   a. Click the **Add New** button.

      The Add MAC ACL/Rule pop-up window displays.

   b. Leave the **Add New ACL only** radio button selected.

      This radio button is selected by default.

   c. In the **ACL Name** field, type **Sales_ACL**.
   d. Click the **Save** button.

      The MAC ACL is added. By default, an ACL is applied to the inbound direction, which means that the switch examines traffic as it enters the port.

      For more information about adding an IPv4 ACL, see Add a MAC ACL on page 376.

7. Click the **Add New** button.

   The Add MAC ACL/Rule pop-up window displays.

8. Select the **Add Rule to existing ACL** radio button.

   The window adjusts.

9. Create a rule for the MAC ACL with the name Sales_ACL with the following criteria:
   a. From the **Name** menu, select **Sales_ACL**.
   b. In the **Sequence Number** field, type **1**.
   c. From the **Action** menu, select **Permit**.

      This means that all packets are allowed.

   d. In the **Assign Queue ID** field, type **4**.

      This means that matching traffic is sent to queue 4.

   e. From the **Match Every** menu, select **False**.

      This means that not all packets need to match the ACL rule that permits the packets. You can configure additional criteria to refine the rule.

   f. From the **EtherType Key** menu, select **IPV4**.

      This means that the criteria apply to IPv4 traffic only.

   g. In the **Source Mask** field, type **01:02:1A:BC:DE:EF** and in the **Source MAC Mask** field, type **00:00:00:00:FF:FF**.

      This information identifies the computer in the Sales department.

   h. In the **VLAN** field, type **2**.

This means that the ACL applies to traffic on the VLAN with ID 2. (This VLAN must already exist on the switch.)

i. Click the **Save** button.

Your settings are saved and the rule is added.

For more information about adding a rule for a MAC ACL, see Add a rule for a MAC ACL on page 379.

10. Select **Security > ACL > MAC ACL > MAC Binding Configuration**.

The IP Binding Configuration page displays.

11. Bind the ACL with the name Sales_ACL to ports 6, 7, and 8, and assign a sequence number of 1:

a. From the **ACL ID** menu, select **Sales_ACL**.

b. In the **Sequence Number** field, type **1**

This number defines the order of the MAC ACL relative to other ACLs that are bound to the interface.

c. In the Ports table, click ports **6**, **7** and **8**.

The selected ports display blue.

d. Click the **Apply** button.

Your settings are saved.

By default, this MAC ACL is bound on the inbound direction, so it examines traffic as it enters the switch. For more information about binding a MAC IP ACL to an interface, see Configure a MAC ACL interface binding on page 384.

12. Select **Security > ACL > MAC ACL > Binding Table**.

The Binding Table page displays.

13. Verify that the ACL is bound to ports 6, 7, and 8.

For more information about MAC ACL bindings, see Display or delete MAC ACL bindings on page 385.

The MAC ACL with the name Sales_ACL looks for IPv4 packets with the source MAC address and MAC mask defined in the rule. Also, the packets must be tagged with VLAN ID 2.

Traffic that matches the criteria is permitted on ports 6, 7, and 8 and is assigned to queue 4. All other traffic is explicitly denied on these interfaces because an explicit *deny all* rule exists as the lowest priority rule. If you want to allow additional traffic to enter these ports, you must add a new Permit rule with the desired match criteria and bind the rule to interfaces 6, 7, and 8.

Standard IP ACL sample configuration

The following example shows how to create a standard IPv4 ACL that prevents any IP traffic from the finance department from being sent on ports 2, 3, and 4, which are associated with other departments. Traffic from the finance department is identified by each packet's network IP address.

In this example, you do the following:

1. Create a standard IPv4 ACL with number 1.
2. Create a first rule for the ACL with the number 1 with the following criteria:
   - **Sequence Number**: 1
   - **Action**: Deny
   - **Assign Queue ID**: 4
   - **Match Every**: No
   - **EtherType**: IPv4
   - **Source IP address**: 192.168.187.0
   - **Source IP Mask**: 255.255.0.0
3. Create a second rule for the ACL with the number 1 with the following criteria:
   - **Sequence Number**: 2
   - **Action**: Permit
   - **Match Every**: Yes
   - **EtherType**: IPv4
   - **Source IP address**: 192.168.187.0
   - **Source IP Mask**: 255.255.0.0
4. Bind the ACL with the number 1 to ports 2, 3, and 4.

To configure the standard IP ACL example:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.

3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Security > ACL > IP ACL > IP ACL/Rules**.

   The IP ACL/Rules page displays.
6. Add a standard IP ACL:
   a. Click the **Add New** button.

      The Add IP ACL/Rule pop-up window displays.
   b. Leave the **Add New ACL only** radio button selected.

      This radio button is selected by default.
   c. In the **Name** field, type **1**.
   d. Click the **Add** button.

      The standard IPv4 ACL is added. By default, an ACL is applied to the inbound direction, which means that the switch examines traffic as it enters the port.

      For more information about adding an IPv4 ACL, see Add an IPv4 ACL on page 387.
7. Click the **Add New** button.

   The Add IP ACL/Rule pop-up window displays.
8. Select the **Add Rule to existing ACL or Add new ACL and Rule** radio button.

   The window adjusts.
9. Click the **Standard IP ACL** button.

   This button is selected by default.
10. Click the **Add** button.

    The window closes, and the Standard ACL Rule Configuration (1-99) section displays.
11. Create a first rule for the IP ACL with number 1 with the following criteria:
    a. From the **ACL ID/Name** menu, select **1**.
    b. In the **Sequence Number** field, type **1**.
    c. Select the **Deny** Action radio button.

       This means that all packets are dropped.
    d. From the **Match Every** menu, select **Disable**.

This means that not all packets need to match the ACL rule that denies packets. You can configure the source IP address and mask for the packets that form an exception and are not dropped.

e. In the **Source IP Address** field, type **192.168.187.0** as the IP address that must be compared against the packet's source IP address.

f. In the **Source IP Mask** field, type **255.255.0.0** as the IP mask that must be compared against the packet's source IP mask.

g. Click the **Save** button.

Your settings are saved and the rule is added.

12. Click the **Add New** button.

The Add IP ACL/Rule pop-up window displays.

13. Select the **Add Rule to existing ACL or Add new ACL and Rule** radio button.

The window adjusts.

14. Click the **Standard IP ACL** button.

This button is selected by default.

15. Click the **Add** button.

The window closes, and the Standard ACL Rule Configuration (1-99) section displays.

16. Create a second rule for the IP ACL with number 1 with the following criteria:

a. From the **ACL ID/Name** menu, select **1**.

b. In the **Sequence Number** field, type **2**.

c. Select the **Permit** Action radio button.

This means that all packets are permitted.

d. From the **Match Every** menu, select **Enable**.

This means that all packets need to match the ACL rule. You cannot configure other options for this rule.

e. Click the **Save** button.

Your settings are saved and the rule is added.

For more information about adding a rule for a standard IP ACL, see Add a rule for a standard IPv4 ACL on page 391.

17. Select **Security > ACL > IP ACL > IP Binding Configuration**.

The IP Binding Configuration page displays.

18. Bind the ACL with ID 1 to ports 2, 3, and 4, and assign a sequence number of 1:

a. From the **ACL ID** menu, select **1**.

b. In the **Sequence Number** field, type **1**

This number defines the order of the IP ACL relative to other ACLs that are bound to the interface.

c. In the Ports table, click ports **2**, **3** and **4**.

The selected ports display blue.

d. Click the **Apply** button.

Your settings are saved.

By default, this IP ACL is bound on the inbound direction, so it examines traffic as it enters the switch. For more information about binding an IP ACL to an interface, see Configure an IP ACL interface binding on page 415.

19. Select **Security > ACL > IP ACL > Binding Table**.

The Binding Table page displays.

20. Verify that the ACL is bound to ports 2, 3, and 4.

For more information about IP ACL bindings, see Display or delete IP ACL bindings on page 416.

The IP ACL looks for traffic that matches all packets with the source IP address and subnet mask of the finance department's network and denies it on interfaces 2, 3, and 4 of the switch. The second rule permits all non-finance traffic on the ports. The second rule is required because an explicit *deny all* rule exists as the lowest priority rule.

Differentiated Services (DiffServ)

Standard IP-based networks are designed to provide *best effort* data delivery service. *Best effort* service implies that the network delivers the data in a timely fashion, although there is no guarantee that it does. During times of congestion, packets might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. However, any degradation of service can negatively affect applications with strict timing requirements, such as voice or multimedia.

Quality of Service (QoS) can provide consistent, predictable data delivery by distinguishing between packets with strict timing requirements and 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.

There are two basic types of QoS:

- **Integrated Services**: Network resources are apportioned based on request and are reserved (resource reservation) according to network management policy (RSVP, for example).
- **Differentiated Services**: Network resources are apportioned based on traffic classification and priority, giving preferential treatment to data with strict timing requirements.

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**: A class includes one or more rules with criteria that specify the traffic that must be inspected.
- **Policy**: A policy, to which you must attach a class, specifies the action that must occur for the traffic that matches the class criteria.
- **Service**: The assignment of a policy to a directional interface.

DiffServ classes

You can classify incoming packets at Layers 2, 3 and 4 by inspecting the following information for a packet:

- Source/destination MAC address
- EtherType
- Class of Service (802.1p priority) value (first/only VLAN tag)
- VLAN ID range (first/only VLAN tag)
- Secondary 802.1p priority value (second/inner VLAN tag)
- Secondary VLAN ID range (second/inner VLAN tag)
- IP Service Type octet (also known as: ToS bits, Precedence value, DSCP value)
- Layer 4 protocol (TCP, UDP and so on)
- Layer 4 source/destination ports
- Source/destination IP address

From a DiffServ point of view, there are two types of classes:

- DiffServ traffic classes
- DiffServ service levels/forwarding classes

DiffServ traffic classes

With DiffServ, you define which traffic classes to track on an ingress interface. You can define simple behavior aggregate (BA) classifiers (DSCP) and a wide variety of multifield (MF) classifiers:

- Layer 2; Layers 3, 4 (IP only)
- Protocol-based
- Address-based

You can combine these classifiers with logical AND operations to build complex MF-classifiers (by specifying a class type of *All*, which is the default and only option). That is, within a single class, multiple match criteria are grouped together as an AND expression.

You can define service levels, namely the forwarding classes/per-hop behaviors (PHBs) that are identified by a DSCP value, on the egress interface. You define these service levels by configuring BA classes for each.

DiffServ policies

Use DiffServ policies to associate a collection of classes that you configure with one or more QoS policy statements. The result of this association is referred to as a policy.

From a DiffServ perspective, there are two types of policies:

- **Traffic conditioning policy**: A policy applied to a DiffServ traffic class
- **Service provisioning policy**: A policy applied to a DiffServ service level

You must manually configure the various statements and rules used in the traffic conditioning and service provisioning policies to achieve the desired Traffic Conditioning Specification (TCS) and the Service Level Specification (SLS) operation, respectively.

DiffServ traffic conditioning policy

Traffic conditioning pertains to actions performed on incoming traffic. Several distinct QoS actions are associated with traffic conditioning:

- **Dropping**: Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot coexist on the same interface.
- **Marking IP DSCP or IP precedence**: Marking/re-marking the DiffServ code point in a packet with the DSCP value representing the service level associated with a

particular DiffServ traffic class. Alternatively, the IP Precedence value of the packet can be marked/re-marked.

- **Marking CoS (802.1p)**: Sets the three-bit priority field in the first/only 802.1p header to a specified value when packets are transmitted for the traffic class. An 802.1p header is inserted if it does not already exist. This is useful for assigning a Layer 2 priority level based on a DiffServ forwarding class (such as the DSCP or IP precedence value) definition to convey some QoS characteristics to downstream switches that do not routinely look at the DSCP value in the IP header.
- **Policing**: A method of constraining incoming traffic associated with a particular class so that it conforms to the terms of the TCS. Out-of-profile packets that are either in excess of the conformance specification or are non-conformant are dropped. That is, the only "violate" action is dropping the packets.

  The DiffServ feature supports the following types of traffic policing treatments (actions):

  - **Send**: The packet is forwarded without DiffServ modification.
  - **Drop**: The packet is dropped.
  - **Mark CoS**: The 802.1p user priority bits are (re)marked and forwarded.
  - **Mark DSCP**: The packet DSCP is (re)marked and forwarded.
  - **Mark IP precedence**: The packet IP Precedence is (re)marked and forwarded.
- **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 is used for handling packets belonging to the class.
- **Redirecting**. Forces a classified traffic stream to a specified egress port (physical or LAG). This can occur in addition to any marking or policing action. It can also be specified along with a QoS queue assignment.
- **Mirroring**. Copies a classified traffic stream to a specified egress port (physical or LAG). This can occur in addition to any marking or policing action. It can also be specified along with a QoS queue assignment.
- **Counting**: Updates the statistics for octets and packets 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 Switch, port, and EAP packet statistics on page 460.

DiffServ example configuration

The following example shows how to add and configure a DiffServ class, add and configure a policy of which the new class is a member, and then attach the policy to an interface.
In this example, network traffic from streaming applications uses UDP port 4567 as the source port and UDP port 4568 as the destination port. The traffic is real-time traffic that is time sensitive, so it must be assigned to a high-priority hardware queue. (By default, data traffic uses hardware queue 0, which is designated as a best-effort queue.)

In this example, you do the following:

1. Add a class with the following five criteria:
   - **Protocol type**: UDP
   - **Source IP address and mask**: 203.0.113.5 and 255.255.255.0
   - **Source L4 port**: 4567
   - **Destination IP address and mask**: 203.0.113.120 and 255.255.255.0
   - **Destination L4 port**: 4568
2. Add a policy and set the policy attribute to assign traffic that matches the class and criteria to queue 6.
3. Attach the policy to interfaces 7 and 8.

To configure the DiffServ example:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **QoS > DiffServ > Class Configuration**.

   The Class Configuration page displays.

6. Add the DiffServ class:
   a. Click the **Add New** button.

      The Add Class Configuration pop-up window displays.
   b. In the **Class Name** field, type **1** as the class name.

      Note: The only option from the **Class Type** menu is **All**. You do not need to select this option because it is automatically applied.
   c. Click the **Save** button.

      Your settings are saved and the new class is added.

   For more information about adding a class, see Add and configure a DiffServ class on page 290.
7. For class 1, configure the first set of criteria, which is for the protocol type:
   a. On the Class Configuration page, in the Class Name column, click **1** for the class that you just added.

      The page adjusts.
   b. From the **Class Configuration** menu, select **Protocol Type**.
   c. From the menu below the Class Configuration menu, select **UDP**.
   d. Click the **Apply** button.

      Your settings are saved and the first set of criteria is added to the Class Summary section.

   For more information about adding class criteria, see Add and configure a DiffServ class on page 290.
8. For class 1, configure the second set of criteria, which is for the source IP address:
   a. On the Class Configuration page, in the Class Name column, click **1**.

      The page adjusts.
   b. From the **Class Configuration** menu, select **Source IP**.
   c. In the **Address** field, type **203.0.113.5**.
   d. In the **Mask** field, type **255.255.255.0**.
   e. Click the **Apply** button.

      Your settings are saved and the second set of criteria is added to the Class Summary section.
9. For class 1, configure the third set of criteria, which is for the source port:
   a. On the Class Configuration page, in the Class Name column, click **1**.

      The page adjusts.
   b. From the **Class Configuration** menu, select **Source L4 Port**.

c. From the menu below the Class Configuration menu, select **Other**.
d. In the field next to the menu, type **4567** as the port number.
e. Click the **Apply** button.

   Your settings are saved and the third set of criteria is added to the Class Summary section.

10. For class 1, configure the fourth set of criteria, which is for the destination IP address:
    a. On the Class Configuration page, in the Class Name column, click **1**.

       The page adjusts.
    b. From the **Class Configuration** menu, select **Destination IP**.
    c. In the **Address** field, type **203.0.113.120**.
    d. In the **Mask** field, type **255.255.255.0**.
    e. Click the **Apply** button.

       Your settings are saved and the fourth set of criteria is added to the Class Summary section.
11. For class 1, configure the fifth set of criteria, which is for the destination port:
    a. On the Class Configuration page, in the Class Name column, click **1**.

       The page adjusts.
    b. From the **Class Configuration** menu, select **Destination L4 Port**.
    c. From the menu below the Class Configuration menu, select **Other**.
    d. In the field next to the menu, type **4568** as the port number.
    e. Click the **Apply** button.

       Your settings are saved and the fifth set of criteria is added to the Class Summary section.

    For more information about adding a class and class criteria, see Add and configure a DiffServ class on page 290 and Add and configure an IPv6 DiffServ class on page 297.
12. Select **QoS > DiffServ > Policy Configuration**.

    The Policy Configuration page displays.
13. Add the policy:
    a. Click the **Add New** button.

       The Add Policy Configuration pop-up window displays.
    b. In the **Policy Name** field, type **Policy1** as the class name.

c. From the **Member Class** menu, select **1**, which is the class that you just added and configured with five sets of criteria.
d. Click the **Save** button.

   Your settings are saved and the new policy is added.

14. Configure the policy:
    a. On the Policy Configuration page, in the Policy Name column, click **Policy1**.

       The page adjusts.
    b. From the **Policy Attribute** menu, select **Assign Queue**.
    c. From the menu below the Policy Attribute, select **6** for queue 6.
    d. Click the **Apply** button.

       Your settings are saved.

       For a single policy, you can configure a single attribute only.

    For more information about adding a policy, see Add and configure a DiffServ policy on page 302.
15. Select **QoS > DiffServ > Service Configuration**.

    The Service Configuration page displays.
16. Attach the policy to interfaces 7 and 8:
    a. Select the check boxes for interfaces 7 and 8.
    b. Click the **Edit** button.

       The Edit Service Interface Configuration pop-up window displays.
    c. From the **Policy In Name** menu, select **Policy1**, which is the name for the policy that you just added.
    d. Click the **Save** button.

       Your settings are saved.

    For more information about attaching a policy to an interface, see Attach a DiffServ policy to an interface on page 306.

All UDP packet flows that enter on switch interface 7 or 8, that have 203.0.113.5 as the source IP address and 203.0.113.120 as the destination IP address, and that include a Layer 4 source port of 4567 and a destination port of 4568 are assigned to queue 6.

802.1X port access control

Local Area Networks (LANs) are often deployed in environments that permit unauthorized devices to be physically attached to the LAN infrastructure, or permit unauthorized users

to attempt to access the LAN through equipment already attached. In such environments you might want to restrict access to the services offered by the LAN to those users and devices that are permitted to use those services.

Port-based network access control makes use of the physical characteristics of LAN infrastructures to provide a means of authenticating and authorizing devices attached to a LAN port with point-to-point connection characteristics. If the authentication and authorization process fails, access control prevents access to that port. In this context, a port is a single point of attachment to the LAN, such as a port of a MAC bridge and an association between stations or access points in IEEE 802.11 wireless LANs.

The IEEE 802.11 standard describes an architectural framework within which authentication and consequent actions take place. It also establishes the requirements for a protocol between the authenticator (the system that passes an authentication request to the authentication server) and the supplicant (the system that requests authentication), as well as between the authenticator and the authentication server.

The switch support a guest VLAN, which allows unauthenticated users limited access to network resources.

Note: You can use QoS features to provide rate limiting on the guest VLAN to limit the network resources the guest VLAN provides.

Another 802.1X feature is the ability to configure a port to enable 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 if you restrict access to publicly accessible bridge ports or 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.

In addition, an authentication server is required. This is a device that performs the authentication function necessary to check the credentials of the supplicant on behalf

of the authenticator. To complete an authentication exchange, an authenticator, supplicant, and authentication server are required.

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 or unauthorized state of the controlled port depending on the outcome of the RADIUS-based authentication process.

802.1X example configuration

This example shows how to configure the switch so that 802.1X-based authentication is required on the ports in a corporate conference room (g5 through g8). These ports are available to visitors and must be authenticated before access is granted to the network. The authentication is handled by an external RADIUS server. When a visitor is successfully authenticated, traffic is automatically assigned to a guest VLAN.

In this example, you do the following:

1. Set the port authentication for ports g5 through g8 to unauthorized and assign ports g5 through g8 to a guest VLAN with VLAN ID 150.
2. Globally enable 802.1X-based authentication and automatic assignment of a port to a particular VLAN.
3. Configure a RADIUS server.
4. Configure the Dot1x Authentication List to use RADIUS.

To configure the 802.1X example:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

The Dashboard page displays.

5. Select **Security > Port Authentication > Port Authentication**.

   The Port Authentication page displays.

6. Select the check boxes for ports **g5**, **g6**, **g7**, and **g8**.
7. Click the **Edit** button.

   The Edit Port Authentication pop-up window displays.

8. From the **Port Control** menu, select **Unauthorized**.

   The selection from the **Port Control** menu for all other ports on which authentication is not needed must be **Authorized**. When the selection from the **Port Control** menu is **Authorized**, the port is unconditionally put in a force-authorized state and does not require any authentication. When the selection from the **Port Control** menu is **Auto**, the authenticator PAE sets the controlled port mode.

9. In the **Guest VLAN** field, type **150** to assign the selected ports to a guest VLAN with VLAN ID 150.

   You can configure additional settings to control access to the network through the ports. For more information, see Configure the 802.1X authentication settings for a port on page 339.

10. Click the **Save** button.

    Your settings are saved.

11. Select **Security > Port Authentication > 802.1x Configuration**.

    The 802.1x Configuration page displays.

12. Click the **Port-Based Authentication State** toggle to enable 802.1X port-based authentication.

    The toggle is purple and positioned to the right.

13. Click the **VLAN Assignment Mode** toggle to enable automatic assignment of a port to a particular VLAN.

    The toggle is purple and positioned to the right.

    You can configure additional global settings for 802.1X-based authentication. For more information, see Configure the global 802.1X authentication settings on page 337.

14. Click the **Apply** button.

    Your settings are saved.

15. Select **Security > Management Security > RADIUS > Server Configuration**.

    The Server Configuration page displays.

16. Click the **Add New** button.

    The Add Server Configuration pop-up window displays.

17. Configure the settings for a RADIUS server:
    a. In the **Server Address** field, type the IP address of the RADIUS server.
    b. From the **Secret Configured** menu, select **Yes**.

       Authentication and encryption are enabled. A secret (password) is required.
    c. In the **Secret** field, type the shared secret text string (password) that is used for authenticating and encrypting all RADIUS communications between the switch and the RADIUS server.
    d. From the **Active** menu, select **Primary**.

       The server functions as the primary RADIUS authentication server.

    You can configure additional RADIUS setting. For more information, see Add a RADIUS authentication server on page 314.
18. Click the **Save** button.

    Your settings are saved and the server is added to the switch.
19. Select **Security > Management Security > Authentication List > Dot1x Authentication List**.

    The Dot1x Authentication List page displays.
20. Click the **Edit** button.

    The Edit Dot1x Authentication List pop-up window displays.
21. To enable the Dot1x list, select the **dotxList** check box.

    The menu options become available.
22. From the menu, select **RADIUS**.

    The user's name and password are authenticated using the RADIUS server instead of the local server.
23. Click the **Save** button.

    Your settings are saved.

This example enables 802.1X-based port security on the switch and prompts the devices that are connected on ports 5 through 8 for an 802.1X-based authentication. The switch passes the authentication information to the configured RADIUS server.

Multiple Spanning Tree Protocol

Spanning Tree Protocol (STP) runs on bridged networks to help eliminate loops. If a bridge loop occurs, the network can become flooded with traffic. IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) supports multiple instances of spanning tree to efficiently channel VLAN traffic over different interfaces. Each instance of the spanning tree behaves

in the manner specified in IEEE 802.1w, Rapid Spanning Tree, with slight modifications in the working but not the end effect (chief among the effects is the rapid transitioning of the port to the forwarding state).

The difference between RSTP and 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. So, an IEEE 802.1s bridge inherently also supports IEEE 802.1w and IEEE 802.1D.

The MSTP algorithm and protocol provide simple and full connectivity for frames assigned to any VLAN throughout a bridged LAN comprising arbitrarily interconnected networking devices, each operating with 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 the following:

- frames with a VLAN ID are assigned to one and only one of the MSTIs or the IST within the region
- the assignment is consistent among all the networking devices in the region
- 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 that are consistently classified as belonging to any VLAN thus simply and fully connects all LANs and networking devices throughout the network. Frames that belong 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:

- Configuration identifier format selector
- Configuration name
- Configuration revision level
- 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 the 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:

- The allocation of VIDs to FIDs is unambiguous.
- 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 describes how to create an MSTP instance on the switch (Switch 1) in a network in which two other switches (Switch 2 and Switch 3) participate in an MSTP configuration:

- Each switch is at a different location and connected to the other two switches through ports g6 and g7. (For consistency, each switch uses the same ports numbers.)
- Each switch has devices in the local sales department connected to ports g1, g2, and g3 and devices in the local HR department connected to ports g4 and g5. (For consistency, each switch uses the same port numbers.)
- The devices connected to Switch 1 use VLAN 300 to communicate with the devices connected to Switch 3.
- The devices connected to Switch 2 use VLAN 500 to communicate with the devices connected to Switch 3

In this example, you do the following *on each switch*:

1. Create a VLAN with VLAN ID 300 and another VLAN with VLAN ID 500.
2. Include ports 1 through 7 as tagged (T) members of VLAN 300 and VLAN 500.
3. Enable the Spanning Tree State and select MSTP as the STP operation mode.
4. Set the bridge priority value for each of the three switches in such a way that Switch 1 is forced to function as the root bridge.
5. Enable STP on ports 1 through 8.
6. Create MST instance 1 that is associated with VLAN 300
7. Create MST instance 2 that is associated with VLAN 500.

To configure the MSTP example:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 20 or Access the switch off-network and not connected to the Internet on page 26.

   The Device Admin Password page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 27.
3. Enter your device admin password.
4. Click the **Login** button.

   The Dashboard page displays.
5. Select **Switching > VLAN > VLAN Management**.

   The VLAN Management page displays.
6. Create the new VLAN IDs:

- Create a VLAN with VLAN ID 300:
  a. Click the **Add New** button.
     The Add VLAN Configuration pop-up window displays.
  b. In the **VLAN ID** field, type 300.
  c. In the **VLAN Name** field, type a name for the new VLAN or leave the field blank.
  d. Click the **Save** button.
     Your setting are saved and the VLAN is added.
- Create a VLAN with VLAN ID 500:
  a. Click the **Add New** button.
     The Add VLAN Configuration pop-up window displays.
  b. In the **VLAN ID** field, type 50.
  c. In the **VLAN Name** field, type a name for the new VLAN or leave the field blank.
  d. Click the **Save** button.
     Your setting are saved and the VLAN is added.

7. Select **Switching > VLAN > VLAN Configuration (Basic)**.
   The VLAN Configuration (Basic) page displays.
8. Configure the membership for each VLAN:
   - For the VLAN with VLAN ID 300, configure ports g1 through g7 as tagged (T) ports:
     a. From the **VLAN ID** menu, select **300**.
     b. In the Ports table, click port **1** through port **7**, and then click the **Tag Port** button.
     c. Click the **Apply** button.
        Your settings are saved.
   - For the VLAN with VLAN ID 500, configure ports g1 through g7 as tagged (T) ports:
     a. From the **VLAN ID** menu, select **500**.
     b. In the Ports table, click port **1** through port **7**, and then click the **Tag Port** button.
     c. Click the **Apply** button.
        Your settings are saved.
9. Select **Switching > STP > STP**.

The STP page displays.

Configure the following global settings:

a. If the Spanning Tree State toggle is gray and positioned to the left, which indicates that STP is disabled on the switch, click the **Spanning Tree State** toggle to enable the STP for the switch.

   The toggle is purple and positioned to the right.

b. Select the **MSTP** radio button to set the STP operation mode.

   For more information about the global STP settings, see Configure the global STP settings and display the STP status on page 194.

c. Click the **Apply** button.

   Your settings are saved.

10. Select **Switching > STP > Common Settings**.

    The CST Configuration page displays.

    In the CST Configuration section, configure the bridge priority value:

    a. In the **Bridge Priority** field, type **4096** as the bridge priority value for the common spanning tree (CST) and common and internal spanning tree (CIST).

       The bridge priority is a multiple of 4096. The default priority is 32768.

       4096 is the bridge priority for Switch 1, which forces Switch 1 to function as the root bridge.

       When you repeat this entire procedure to configure Switch 2, set the bridge priority for Switch 2 to 12288.

       When you repeat this entire procedure to configure Switch 3, set the bridge priority for Switch 3 to 20480.

       For more information, see Configure the CST settings and display the MSTP status on page 196.

    b. Click the **Apply** button.

       Your settings are saved.

11. Select **Switching > STP > CST Port Configuration**.

    The CST Port Configuration page displays.

    Enable STP for ports g1 through g7 and enable Fast Link for ports g1 through g5:

    a. Select the check boxes for ports g1 through g7.

    b. Click the **Edit** button.

       The Edit CST Port Configuration pop-up window displays.

    c. From the **STP Status** menu, select **Enable** to enable STP for the ports.

For information about the other settings in the pop-up window, see Configure the CST interface settings on page 198.

d. Click the **Save** button.

Your settings are saved.

e. Select the check boxes for ports g1 through g5.

f. Click the **Edit** button.

The Edit CST Port Configuration pop-up window displays again.

g. From the **Fast Link** menu, select **Enable** to let the ports functions as edge ports within the CST.

Because edge ports are not at risk for network loops, ports with Fast Link enabled transition directly to the forwarding state.

For information about the other settings in the pop-up window, see Configure the CST interface settings on page 198.

h. Click the **Save** button.

Your settings are saved.

12. Select **Switching > STP > MSTP > MST Configuration**.

The MST Configuration page displays.

Create MST instance 1 that is associated with VLAN 300 and MST instance 2 that is associated with VLAN 500:

a. Click the **Add New** button.

The Add MST Configuration pop-up window displays.

b. In the **MST ID** field, type **1**.

c. In the **Priority** field, type **32768** as the priority value for the MST instance.

This is the default setting.

d. From the **VLAN ID** menu, select **300** as the VLAN ID that must be associated with the MST instance.

e. Click the **Save** button.

Your settings are saved and the MST is added.

f. Click the **Add New** button.

The Add MST Configuration pop-up window displays again.

g. In the **MST ID** field, type **2**.

h. In the **Priority** field, type **49152** as the priority value for the MST instance.

This is the default setting.

i. From the **VLAN ID** menu, select **500** as the VLAN ID that must be associated with the MST instance.

j. Click the **Save** button.

Your settings are saved and the MST is added.

In this example, Switch 1 (with bridge priority 4096) became the root bridge for MST instance 1 (with priority 32768), and Switch 2 (with bridge priority 12288) became the root bridge for MST instance 2 (with priority 49152).

Each switch supports devices in their sales department (ports g1, g2, and g3) and in their HR department (ports g4 and g5).

The devices connected to Switch 1 use VLAN 300, MST instance 1, to communicate directly with the devices connected to Switch 3. The devices connected to Switch 2 use VLAN 500, MST instance 2, to communicate directly with the devices connected to Switch 3.

The devices use different MSTP instances to effectively use the links across the switch.

B

Software Default Settings and Hardware Specifications

This appendix contains the following sections:

- Access default settings for the switch device UI
- System features default settings
- VLAN features default settings
- Switching features default settings
- Multicast features default settings
- QoS features default settings
- Security features default settings
- ACL features default settings
- Monitoring features default settings
- Hardware technical specifications

Note: For more information about the switch specifications and capabilities, including the maximum settings for many features, see the data sheet, which you can download by visiting netgear.com/support/download/.

Access default settings for the switch device UI

The following table describes the default settings for access to the switch device UI.

Settings that you cannot change in the device UI are not included in the table but might be included in the data sheet, which you can download by visiting netgear.com/support/download/.

Table 86. Default settings for access to the switch device UI

Feature	Default
Management modes	Directly Connected To Web Browser Interface
IP address	192.168.0.239
Subnet mask	255.255.0.0
Default gateway	192.168.0.254
Management VLAN ID	1
Protocol	DHCP (client enabled)
User name	admin
Password	password (with lower case p) Upon first login, the admin user must set a password.
Minimum length for password	Eight characters
IPv6 network global configuration	Enabled
IPv6 address auto configuration	Disabled
DHCPv6	Disabled

System features default settings

The following table describes the default settings for the system features that you can configure.

Table 87. System features default settings

Feature Name/Setting	Default
Time Configuration	
Clock source	Local
SNTP time zone name	None configured
SNTP offset hours	0
SNTP offset minutes	0
SNTP client mode	Unicast
SNTP port	123
SNTP unicast poll interval	6
SNTP broadcast poll interval	6
SNTP unicast poll time-out	5
SNTP unicast poll retry	1
SNTP Server Configuration	
SNTP server	None configured
Port	123
Priority	1
Version	4
Daylight Saving Configuration	
Daylight saving	Disabled
DNS Configuration	
DNS status	Enabled
Host Configuration	
DNS status	None configured
Switch Discovery	
UPnP / SSDP	Enabled
Bonjour	Disabled
NSDP	Disabled
LLDP Configuration	
TLV advertised interval	30
Hold multiplier	4

Table 87. System features default settings (Continued)

Feature Name/Setting	Default
Reinitializing delay	2
Transmit delay	5
LLDP-MED fast start duration	3
SNMPv1/v2	
Community configuration	None configured
Trap configuration	None configured
Trap flag authentication	Enabled
Trap flag link up/down	Enabled
Trap flag spanning tree	Enabled
Trap flag PoE	Enabled
Trap fan failure	Enabled
SNMPv3	
SNMPv3 access mode	Read/Write
Authentication protocol	MD5
Authentication key	Same as admin user password
Encryption protocol	None
HTTP	
HTTP	Enabled
HTTP session soft timeout	5
HTTP session hard timeout	24
Maximum number of HTTP sessions	4
HTTPS	
HTTPS	Enabled
HTTPS port	443
HTTPS session soft timeout	5
HTTPS session hard timeout	24
Maximum number of HTTPS sessions	4
SSH	
SSH	Enabled

Table 87. System features default settings (Continued)

Feature Name/Setting	Default
SSH port	22
SSH session timeout	5
Maximum number of SSH sessions	4
Telnet	
Telnet	Disabled
DHCP Snooping Global Configuration	
DHCP snooping mode	Disabled
MAC address validation	Enabled
DHCP Snooping VLAN Configuration	
DHCP snooping mode	Disabled
DHCP Snooping Interface Configuration	
Trust mode	Disabled
Invalid packets	Disabled
Rate limit	None
Burst interval	N/A
DHCP Snooping Persistent Configuration	
Store	Local
Write delay	300
DHCP L2 Relay Global Configuration	
Admin mode	Disabled
DHCP L2 Relay VLAN Configuration	
Admin mode	Disabled
Circuit ID option mode	Disabled
Remote ID string	None
DHCP L2 Relay Interface Configuration	
Admin mode	Disabled
82 Option Trust mode	Disabled

Nonconfigurable settings are not included in the table but might be included in the data sheet, which you can download by visiting netgear.com/support/download/.

VLAN features default settings

The following table describes the default settings for the VLAN features that you can configure.

Settings that you cannot change in the device UI are not included in the table but might be included in the data sheet, which you can download by visiting netgear.com/support/download/.

Table 88. VLAN features default settings

Feature Name/Setting	Default
VLAN Management, preconfigured VLANs	
default	1 (All ports and LAGs are members)
Auto-WiFi	4086 (No members by default)
Auto-Camera	4087 (No members by default)
Auto-VoIP	4088 (No members by default)
Auto-Video	4089 (No members by default)
VLAN Configuration (interfaces)	
PVID	1
VLAN member	1
VLAN tag	None
Acceptable frame	Admit All
Ingress filtering	Disabled
Port priority	0
Voice VLAN Configuration	
Admin mode	Disabled
Value	0
Cos override mode	Disabled
Authentication mode	Enabled
DSCP value	0
Auto-VLAN, OUI-based Auto-VLAN	

Table 88. VLAN features default settings (Continued)

Feature Name/Setting	Default
Auto-VoIP VLAN ID	4088
Auto-VoIP OUI-based priority	7
Auto-WiFi VLAN ID	4086
Auto-WiFi OUI-based priority	7
Auto-Camera VLAN ID	4087
Auto-Camera OUI-based priority	7
OUI table	00:01:E3 SIEMENS 00:03:6B CISCO1 00:12:43 CISCO2 00:60:B9 NITSUKO 00:D0:1E PINTEL 00:E0:75 VERILINK 00:E0:BB 3COM 00:04:0D AVAYA1 00:1B:4F AVAYA2
Auto-VLAN, Protocol-based VoIP	
Prioritization class	Traffic Class
Class value	7
Auto-VoIP mode for an interface	Disabled
MAC-based VLAN	
MAC-based VLAN	None configured
Protocol-based VLAN	
Protocol-based VLAN	None configured
Private VLAN	
Private VLAN type	Unconfigured
Private VLAN association	None configured
Private VLAN port mode	General
Private VLAN host interface	None configured
Private VLAN promiscuous interface	None configured
Protected Port	
Protected port	None configured

Switching features default settings

The following table describes the default settings for the switching features that you can configure.

Table 89. Switching features default settings

Feature Name/Setting	Default
LLDP Port Configuration	
Admin status	Tx and Rx
Management IP address	Auto Advertise
Notification	Disabled
Optional TLVs	Enabled
LLDP-MED Port Configuration	
LLDP-MED status	Enabled
Notification	Enabled
MED capabilities	Enabled
Network policy	Enabled
Extended MDI-PSE	Disabled
PoE Configuration	
System usage threshold	95
Power management mode	Dynamic
Traps	Enabled
PoE Port Configuration	
Power power	Enabled
Port priority	Low
Power mode	802.3at
Power limit type	User
Detection type	IEEE 802
Timer schedule	None
Timer Schedule	
Timer schedule	None configured
Green Ethernet Configuration	

Table 89. Switching features default settings (Continued)

Feature Name/Setting	Default
Auto power down mode	Disabled
EEE mode	Disabled
Green Ethernet Interface Configuration	
Auto power down mode	Disabled
EEE mode	Disabled
Port Configuration	
Maximum frame size (global)	1522
Admin mode	Enabled
Autonegotiation	Enabled
Speed	Auto
Duplex mode	Auto
Link trap	Enabled
Flow control	Disabled
LAGs	
LAG name	ch<n> where n is 1 to 16
Admin mode	Enabled
Hash mode	1 Src/Dest MAC, incoming port
STP mode	Enabled
Link trap	Enabled
LAG type	Static
LAG membership	None configured
LACP system priority	32768
LACP port priority	128
Timeout	Long
STP	
Spanning tree state	Enabled
STP operation mode	RSTP
Configuration name	MAC address
Configuration revision level	0

Table 89. Switching features default settings (Continued)

Feature Name/Setting	Default
Forward BPDUs while STP disabled	Disabled
CST Configuration	
Bridge priority	32768
Bridge maximum age	20
Bridge hello time	2
Bridge forward delay	15
Spanning tree maximum hops	20
CST Port Configuration	
STP status	Enabled
Fast link	Enabled
BPDU forwarding	Disabled
Auto edge	Enabled
Path cost	0
Auto calculated port path cost	Enabled
Priority	128
External port path cost	0
MST Configuration	
MST ID	0 (All VLANs are included)
Priority	32768
VLAN ID	1
MST Port Configuration	
Port priority	128
Port path cast	20000
Address Table	
Address aging timeout	300
Static MAC address	None configured
DAI Configuration	
Validate source MAC	Disabled
Validate destination MAC	Disabled

Table 89. Switching features default settings (Continued)

Feature Name/Setting	Default
Validate IP	Disabled
DAI VLAN Configuration	
Admin mode	Disabled
Invalid packets	Enabled
Static flag	Disabled
DAI Interface Configuration	
Trust mode	Disabled
Rate limit (pps)	15
Burst interval(secs)	1
DAI ACL/Rule Configuration	
DAI ACL/Rule	None configured

Nonconfigurable settings are not included in the table but might be included in the data sheet, which you can download by visiting netgear.com/support/download/.

Multicast features default settings

The following table describes the default settings for the multicast features that you can configure.

Settings that you cannot change in the device UI are not included in the table but might be included in the data sheet, which you can download by visiting netgear.com/support/download/.

Table 90. Multicast features default settings

Feature Name/Setting	Default
IGMP Snooping	
Admin mode	Disabled
Validate IGMP IP header	Enabled
IGMP Snooping Interface Configuration	
Admin mode	Disabled
Host time-out	260

Table 90. Multicast features default settings (Continued)

Feature Name/Setting	Default
Maximum response time	10
Mrouter time-out	0
Fast leave mode	Disabled
IGMP Snooping VLAN Configuration	
Admin mode	Disabled
Fast leave mode	Disabled
Host time-out	260
Maximum response time	10
Mrouter time-out	0
Report suppression mode	Disabled
Query mode	Disabled
Query interval	60
Multicast Router Interface Configuration	
Multicast router	Disabled
Multicast Router VLAN Configuration	
Multicast router	Disabled
IGMP Snooping Querier Configuration	
Querier admin mode	Disabled
Snooping querier address	None
IGMP version	2
Query interval	60
Querier expiry interval	125
IGMP Snooping Querier VLAN Configuration	
Querier VLAN Configuration	None configured
Auto-Video	
Auto-Video status	Disabled
MLD Snooping Configuration	
MLD snooping admin mode	Disabled
MLD Snooping Interface Configuration	

Table 90. Multicast features default settings (Continued)

Feature Name/Setting	Default
Admin mode	Disabled
Fast leave	Disabled
Host time-out	260
Maximum response time	10
Mrouter time-out	0
MLD Snooping VLAN Configuration	
MLD VLAN	None configured
MLD Snooping Multicast Router Interface Configuration	
Multicast router	Disabled
MLD Snooping Multicast Router VLAN Configuration	
Multicast router	Disabled
MLD Snooping, Multicast Router, Interface	
Multicast router	Disabled
MLD Snooping Querier Configuration	
Querier admin mode	Disabled
Snooping querier address	None
MLD version	1
Query interval	60
Querier expiry interval	125
MLD Snooping Querier VLAN Configuration	
Querier VLAN	None configured
MVR Configuration	
MVR running	Disabled
MVR multicast VLAN	1
MVR global query response time	5
MVR mode	Compatible
MVR Group Configuration	
MVR group	None configured
MVR Interface Configuration	

Table 90. Multicast features default settings (Continued)

Feature Name/Setting	Default
Admin mode	Disabled
Type	None
Immediate leave	Disabled

QoS features default settings

The following table describes the default settings for the QoS features that you can configure.

Settings that you cannot change in the device UI are not included in the table but might be included in the data sheet, which you can download by visiting netgear.com/support/download/.

Table 91. QoS features default settings

Feature Name/Setting	Default
CoS Configuration	
Global trust mode	802.1p
CoS Interface Configuration	
Interface trust mode	802.1p
Interface shaping rate	0
Interface Queue Configuration	0
Queue ID	None configured
Scheduler type	Weighted
Queue management type	TailDrop (nonconfigurable)
802.1p to Queue Mapping	
802.1p priority (802.1p -> queue)	0 -> 1 1 -> 0 2 -> 0 3 -> 1 4 -> 2 5 -> 2 6 -> 3 7 -> 3

Table 91. QoS features default settings (Continued)

Feature Name/Setting	Default
DSCP to Queue Mapping	
Class Selector (CS) PHB	CS 0 -> 1 CS 1 -> 0 CS 2 -> 0 CS 3 -> 1 CS 4 -> 2 CS 5 -> 2 CS 6 -> 3 CS 7 -> 3
Assured Forwarding Selector (CS) PHB	AF 11 -> 0 AF 12 -> 0 AF 13 -> 0 AF 21 -> 0 AF 22 -> 2 AF 23 -> 0 AF 31 -> 1 AF 32 -> 1 AF 33 -> 1 AF 41 -> 2 AF 42 -> 2 AF 43 -> 2
Expedited Forwarding (EF) PHB	EF 0 -> 2

Table 91. QoS features default settings (Continued)

Feature Name/Setting	Default	
Other DSCP Values (Local/Experiment)	1 -> 1	39 -> 2
	2 -> 1	41 -> 2
	3 -> 1	42 -> 2
	4 -> 1	43 -> 2
	5 -> 1	44 -> 2
	6 -> 1	45 -> 2
	7 -> 1	47 -> 2
	9 -> 0	49 -> 3
	11 -> 0	50 -> 3
	13 -> 0	51 -> 3
	15 -> 0	52 -> 3
	17 -> 0	53 -> 3
	19 -> 0	54 -> 3
	21 -> 0	55 -> 3
	23 -> 0	57 -> 3
	25 -> 1	58 -> 3
	27 -> 1	59 -> 3
	29 -> 1	60 -> 3
	31 -> 1	61 -> 3
	33 -> 2	62 -> 3
	35 -> 2	63 -> 3
	37 -> 2	
DiffServ Configuration		
DiffServ admin mode	Enabled	
Class Configuration		
Class	None configured	
IPv6 Class Configuration		
IPv6 class	None configured	
Policy Configuration		
Policy	None configured	
Service Configuration		
Service	None configured	

Security features default settings

The following table describes the default settings for the security features that you can configure.

Settings that you cannot change in the device UI are not included in the table but might be included in the data sheet, which you can download by visiting netgear.com/support/download/.

Table 92. Security features default settings

Feature Name/Setting	Default
User Configuration	
Password length	8 to 20 characters
RADIUS Global Configuration	
Maximum number of retransmits	4
Time-out duration	5
Accounting mode	Disabled
RADIUS Server Configuration	
RADIUS server	None configured
RADIUS Accounting Server Configuration	
Accounting server address	Blank
Port	1813
Secret configured	No
Accounting mode	Disabled
TACAS+	
Key String	Blank
Connection timeout	5
TACAS+ Server Configuration	
TACACS+ server	None configured
HTTP Authentication List	
httpList	Enabled, option 1 is Local, options 2 through 4 are not configured
HTTPS Authentication List	
httpsList	Enabled, option 1 is Local, options 2 through 4 are not configured

Table 92. Security features default settings (Continued)

Feature Name/Setting	Default
Dot1x Authentication List	
dot1xList	Disabled
Protocol Access Control	
Access profile name	Blank
Access profile	Disabled
Access rules	None configured
802.1x Configuration	
Port-based authentication state	Disabled
VLAN assignment mode	Disabled
Dynamic VLAN creation mode	Disabled
EAPOL flood mode	Disabled
Port Authentication (interface)	
Port control	Auto
MAB	Disabled
MAB authentication type	N/A
Guest VLAN ID	0
Guest VLAN period	90
Unauthenticated VLAN ID	0
Periodic reauthentication	Disabled
Reauthentication period	3600
Quiet period	60
Resending EAP	30
Maximum EAP requests	2
Supplicant timeout	30
Server timeout	30
MAC Filter	
MAC filter	None configured
Storm Control	
Ingress control mode	Disabled

Table 92. Security features default settings (Continued)

Feature Name/Setting	Default
Status for any type of storm control	Disabled
Threshold for any type of storm control	5
Control action for any type of storm control	None
Storm Control Port Settings	
Status	Enabled
Threshold	5
Control action	None
Port Security Configuration	
Port security mode	Disabled
Port Security Interface Configuration	
Port security	Disabled
Maximum learned MAC addresses	4096
Maximum static MAC addresses	48
Enable violation shutdown	No
Enable violation traps	No
Security MAC Address	
Convert dynamic address to static	Disabled
Global L2 Loop Protection Configuration	
Transmit interval	5
Maximum PDU receive	1
Disable timer	0
L2 Loop Protection Interface Configuration	
Keep alive	Disabled
Rx action	Disabled
Auto-DoS Configuration	
Auto-DoS mode	Disabled
Denial of Service Configuration	
Denial of Service minimum TCP header size	Blank
Denial of Service maximum ICMPv4 packet size	Blank

Table 92. Security features default settings (Continued)

Feature Name/Setting	Default
Denial of Service ICMPv4	Disabled
Denial of Service ICMPv6	Disabled
Denial of Service Ping of Death	Disabled
Denial of Service IPv6 fragment	Disabled
Denial of Service ICMP fragment	Disabled
Denial of Service Smurf	Disabled
Denial of Service SIP=DIP	Disabled
Denial of Service SMAC=DMAC	Disabled
Denial of Service TCP FIN & URG & PSH	Disabled
Denial of Service TCP Flag & Sequence	Disabled
Denial of Service TCP fragment	Disabled
Denial of Service TCP offset	Disabled
Denial of Service TCP port	Disabled
Denial of Service TCP source port	Disabled
Denial of Service TCP SYN & FIN	Disabled
Denial of Service TCP SYN & RST	Disabled
Denial of Service UDP port	Disabled

ACL features default settings

The following table describes the default settings for the ACL features that you can configure.

Settings that you cannot change in the device UI are not included in the table but might be included in the data sheet, which you can download by visiting netgear.com/support/download/.

Table 93. ACL features default settings

Feature Name/Setting	Default
Total number of supported ACLs	100. This total number applies to all MAC ACLs, IP basic ACLs, IP extended ACLs, and IPv6 ACLs together.
MAC ACLs	None configured
IP basic ACLs	None configured
IP extended ACLs	None configured
IPv6 ACLs	None configured

Monitoring features default settings

The following table describes the default settings for the monitoring features that you can configure.

Settings that you cannot change in the device UI are not included in the table but might be included in the data sheet, which you can download by visiting netgear.com/support/download/.

Table 94. Monitoring features default settings

Feature	Default
Memory Log	
Memory logging	Enabled
Behavior	Wrap
Severity filter	Informational
Flash Log	
Severity filter	Error
Memory log	Current logs
Server Log	
Server logging	Disabled
Server	None configured
Port Mirroring	
Port mirroring	Disabled
Destination port	None

Hardware technical specifications

The following table shows the hardware technical specifications for models GS324TPv2 and GS348TPv2.

Table 95. Hardware technical specifications

Feature	Description	
	All Models	
Network interfaces	**GS324TPv2**: 24-Port Gigabit Ethernet PoE+ Smart Switch with 2 SFP Ports.	
	GS348TPv2: 48-Port Gigabit Ethernet PoE+ Smart Switch with 4 SFP Ports.	
	GS324TPv2	**GS348TPv2**
Switch PoE+ power budget	190W	380W
Max. power consumption with PoE	208.7W	431W
Max. power consumption without PoE	19.44W	45W
Idle power consumption	11.15W	23W
AC power input	100–240V ~ 50–60Hz, 4A	100–240V ~ 50-60Hz, 6A
Dimensions (W x D x H)	17.3 x 10.1 x 1.7 in. (440 x 257 x 43 mm)	17.3 x 12.1 x 1.7 in. (440 x 310 x 43 mm)
Weight	6.96 lb (3.15 kg)	10.86 lb (4.93 kg)
	All Models	
Operating temperature	32° to 122°F (0° to 50°C)	
Operating humidity	95% maximum relative humidity, noncondensing	
Maximum operating altitude	10,000 ft (3,000 m)	
Storage temperature	–4° to 158°F (–20° to 70°C)	
Storage humidity	95% maximum relative humidity, noncondensing	
Maximum storage altitude	10,000 ft (3,000 m)	
Electromagnetic emissions and immunity certifications	CE, FCC Class A, and ICES Class A	
Safety certifications	CB, CE, and UL	

For more hardware information, see the data sheet, which you can download by visiting netgear.com/support/download/.