NETGEAR®

User Manual

8-Port Gigabit Ethernet High-Power PoE+ Smart Switch with 2 Dedicated SFP Ports (190W)

GS510TPP

December 2024
202-12816-01

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

Support and Community

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

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

Regulatory and Legal

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

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

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

See the regulatory compliance document before connecting the power supply.

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

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

Do not use this device outdoors. The PoE source is intended for intra building connection only.

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

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
202-12697-01	December 2024	First publication for model GS510TPP with NETGEAR Insight support.

Contents

Chapter 1 Get Started

Available publications 13
Switch management options and default management mode 14
Manage the switch by using the device UI 15
Navigation tabs, configuration menus, and page menu 15
Configuration and Status Options 15
Buttons in the device UI 16
User-defined fields 16
Context-sensitive help 16
About on-network and off-network access 16
Access the switch on-network and connected to the Internet 17
Use a Windows-based computer to access the switch on-network and connected to the Internet 18
Use the NETGEAR Insight app to discover the IP address of the switch 19
Use the NETGEAR Discovery Tool to discover the switch when it is connected to the Internet 20
Use other options to discover the switch IP address 21
Access the switch on-network when you know the switch IP address . 21
Access the switch off-network and not connected to the Internet 22
Credentials for the device UI 23
Register the switch 24
Change the language of the device UI 25
Change the management mode of the switch 26
About changing the management mode 26
Change the management mode to NETGEAR Insight Mobile App and Insight Cloud Portal 27
Permanently change the management mode back to Directly Connect to Web-browser Interface 28
Use the Device View of the device UI 31
Configure interface settings 32
Access the NETGEAR support website 33
Access the user manual online 34

Chapter 2 Configure System Information

View or define system information 37
View the fan status 38
View the power supply information 39
View the software versions 40
View the system CPU status 41

Configure the CPU thresholds. 42
Configure the IP network settings for management access 43
Configure the IPv4 network and VLAN settings for the device UI 43
Configure the IPv6 network settings for the local browser interface 45
View the IPv6 network neighbors 47
Configure the time settings. 48
Configure the time setting manually 48
Configure the time settings with SNTP and configure the global SNTP settings. 49
View the SNTP global status 51
Configure an SNTP server 53
Configure daylight saving time settings 57
View the daylight saving time status 59
Configure denial of service settings 60
Configure Auto-DoS 60
Configure denial of service 61
Configure DNS settings 64
Configure the global DNS settings and add a DNS server. 64
Remove a DNS server 65
Configure and view host name-to-IP address information 66
Manage UPnP switch discovery 69
Configure green Ethernet settings 70
Configure the global green Ethernet settings 70
Configure green Ethernet interface settings. 71
Configure and display detailed green Ethernet settings for an interface 72
Display green Ethernet information for the link partner of an interface 74
Display the green Ethernet statistics summary. 75
Configure and display the green Ethernet EEE LPI history for an interface 77
Use the Device View 78
Configure Power over Ethernet 79
PoE concepts 79
Device class power requirements. 79
Power allocation and power budget concepts. 80
Configure the global PoE settings 81
Configure the PoE port settings 82
Configure SNMP 86
Configure the SNMPv1 and SNMPv2 community 86
Configure SNMPv1 and SNMPv2 trap settings. 89
Configure SNMPv1 and SNMPv2 trap flags 91
View the supported MIBs 92
Configure SNMPv3 users 93
Configure Link Layer Discovery Protocol 96
Configure LLDP global settings 96

Configure LLDP port settings 97
View the LLDP-MED network policy 99
Configure the LLDP-MED port settings 100
Display the LLDP-MED neighbors information 101
View the local information advertised through LLDP 104
View the LLDP neighbors information 106
Configure a DHCP L2 relay 110
Enable the DHCP L2 relay 110
Configure a DHCP L2 relay interface 111
View DHCP L2 relay interface statistics 112
Configure DHCP snooping 114
Configure the global DHCP snooping settings 114
Enable DHCP for all member interfaces of a VLAN 115
Configure DHCP snooping interface settings 116
Configure static DHCP bindings 117
Display or clear dynamic DHCP snooping bindings 120
Configure DHCP snooping persistent settings 121
View or clear DHCP snooping statistics 122
Configure Dynamic ARP Inspection 124
Configure the global DAI settings 124
Configure DAI on a VLAN 125
Configure DAI on an interface 127
Configure a DAI access control list and DAI rules 128
View DAI statistics per VLAN 131
Set up PoE timer schedules 132
Create a PoE timer schedule 133
Specify the settings for an absolute PoE timer schedule 134
Specify the settings for a recurring PoE timer schedule 135
Change the settings for a recurring PoE timer schedule entry 137
Delete a PoE timer schedule entry 138
Delete a PoE timer schedule 139

Chapter 3 Configure Switching

Configure the port settings and maximum frame size 141
Configure link aggregation groups 144
Configure LAG settings 144
Configure LAG membership 146
Set the LACP switch priority 147
Set the LACP port priority settings 148
Configure VLANs 149
Configure VLAN settings 149
Configure VLAN membership 152
View the VLAN status 154
Configure the PVID settings 155
Configure a MAC-based VLAN 157
Configure protocol-based VLAN groups 159
Configure protocol-based VLAN group membership 162
Configure a voice VLAN 163

Configure GARP switch settings 165
Configure GARP ports 166
Configure Auto-VoIP 168
Configure the Auto-VoIP protocol-based settings 168
Configure the Auto-VoIP OUI-based properties 169
Configure the OUI-based port settings 170
Manage the OUI table 171
Display the Auto-VoIP status 173
Configure Spanning Tree Protocol 174
Configure the STP settings and view the STP status 175
Configure the CST Settings 177
Configure the CST port settings 178
View the CST port status 180
View the Rapid STP information 182
Manage the MST settings 183
Configure and view the port settings for an MST instance 186
View the STP Statistics 189
Configure multicast 190
View, search, or clear the MFDB table 190
View the MFDB statistics 191
Configure the auto-video multicast settings 192
Manage IGMP snooping 193
Configure IGMP snooping 194
Configure IGMP snooping for interfaces 195
View, search, or clear the IGMP snooping table 197
Configure IGMP snooping for VLANs 198
Configure one or more IGMP multicast router interfaces 199
Configure an IGMP multicast router VLAN 200
IGMP snooping querier overview 201
Configure an IGMP snooping querier 202
Configure an IGMP snooping querier for VLANs 203
Remove the IGMP snooping querier settings from a VLAN 204
Display the status of the IGMP snooping querier for VLANs 204
Manage MLD snooping 206
Enable MLD snooping 206
Configure MLD snooping for interfaces 207
Configure the MLD VLAN settings 209
Modify the MLD snooping settings for a VLAN 210
Remove MLD snooping from a VLAN 211
Configure one or more MLD multicast router interfaces 211
Configure an MLD multicast router VLAN 212
Configure an MLD snooping querier 213
Configure an MLD snooping querier for a VLAN 214
Remove the MLD snooping querier settings for a VLAN 216
Configure multicast VLAN registration 217
Configure the global MVR settings 217
Configure an MVR group 219
Remove an MVR group 220

Configure MVR group membership 221
Configure the MVR interface settings. 222
View the MVR statistics 223
View, search, and manage the MAC address table. 224
View, search, or clear the MAC address table. 224
Set the dynamic address aging interval. 226
Add a static MAC address to the MAC address table 227
Remove a static MAC address from the MAC address table 228
Configure Layer 2 loop protection. 228
Configure global Layer 2 loop protection. 229
View and configure Layer 2 loop protection on a port 230

Chapter 4 Configure Routing

Routing concepts. 233
Configure the routing mode. 233
Manage the global IPv4 routing settings. 233
View the IP routing statistics 234
Configure IPv6 routing. 238
Configure the global IPv6 routing settings 238
View the IPv6 route table 239
Configure the IPv6 VLAN interface settings 240
Configure an IPv6 prefix. 242
View the IPv6 routing statistics 244
View, search, or clear the IPv6 neighbor table 248
Configure an IPv6 static route 250
Configure IPv6 route preferences. 251
Configure VLAN routing 252
Create a routing interface with the VLAN Static Routing Wizard 253
Manage a VLAN routing interface. 254
Delete a VLAN routing interface 256
Configure router discovery for a VLAN routing interface. 257
Manage routes and view the routing table. 258
Manually add a route and view the routing table 258
Modify a route 260
Delete a route 261
Configure Address Resolution Protocol 262
View the ARP cache. 263
Manually add an entry to the ARP table. 264
Delete a static ARP entry 266
View or globally configure the ARP table 267
Remove ARP entries from the ARP cache 268

Chapter 5 Configure Quality of Service

Quality of Service concepts 270
Manage Class of Service 270
CoS configuration concepts 270
Configure the global CoS settings 271

Configure the CoS settings for an interface 272
Configure the CoS queue settings for an interface 273
Map 802.1p priorities to queue 275
Map DSCP values to queues 276
Manage Differentiated Services 277
Defining DiffServ 277
Configure the DiffServ mode and display the entries in the DiffServ private MIB tables 278
Configure a DiffServ class 279
Configure DiffServ IPv6 class settings 285
Configure a DiffServ Policy 289
Configure the DiffServ service interface 295
View DiffServ service statistic 298

Chapter 6 Manage Device Security

Change the device admin password for the device UI 301
Reset the device admin password for the device UI 302
Configure password lockout 303
Manage the RADIUS settings 304
Configure the global RADIUS server settings 304
Configure a RADIUS authentication server on the switch 306
Configure a RADIUS accounting server 309
Configure the TACACS+ settings 313
Configure the global TACACS+ settings 313
Configure a TACACS+ server on the switch 314
Modify the settings for a TACACS+ server on the switch 315
Remove a TACACS+ server from the switch 316
Configure authentication lists 317
Configure an HTTP authentication list 317
Configure an HTTPS authentication list 318
Configure the dot1x authentication list 320
Configure management access 321
Configure the HTTP settings 321
Configure the HTTPS settings 322
Browser security warning with HTTPS access 323
Manage certificates for HTTPS access 324
Transfer an existing certificate to the switch 326
Control access with profiles and rules 328
Add an access profile 328
Add a rule to the access profile 329
Activate the access profile 330
Display the access profile summary and the number of filtered packets 331
Deactivate an access profile 332
Remove an access profile 333
Configure port authentication 334
Configure global 802.1X settings 334

Manage port authentication on individual ports 336
View the port summary 341
View the client summary 342
Set up traffic control 344
Manage MAC filtering 344
Configure storm control settings 347
Manage port security 349
Configure protected ports 354
Manage private VLANs 354
Overview of the tasks for private VLAN configuration 355
Assign a private VLAN type to a VLAN 356
Configure a private VLAN association with a primary and secondary VLAN 357
Remove an existing private VLAN association 358
Configure the private VLAN port mode 359
Private VLAN host interface: Assign the interface to primary and secondary VLANs 361
Private VLAN host interface: Remove the interface from primary and secondary VLANs 362
Private VLAN promiscuous interface: Assign the interface to primary and secondary VLANs 363
Private VLAN promiscuous interface: Remove the interface from primary and secondary VLANs 365

Chapter 7 Manage Access Control Lists

About access control lists 368
Use the ACL Wizard to create an uncomplicated ACL 368
Use the ACL Wizard to create an ACL 368
Modify an ACL rule that you created with the ACL Wizard 371
Delete an ACL rule that you created with the ACL Wizard 372
Configure a MAC ACL 373
Add a MAC ACL 373
Change the name of a MAC ACL 374
Delete a MAC ACL 375
Configure MAC ACL rules 376
Add a rule to a MAC ACL 376
Change the match criteria for a MAC rule 378
Delete a rule for a MAC ACL 379
Configure MAC ACL interface bindings 380
Bind a MAC ACL to one or more interfaces 380
View or delete MAC ACL bindings 381
Configure a basic or extended IPv4 ACL 382
Add an IP ACL 383
Change the number or name of an IPv4 ACL 384
Delete an IP ACL 385
Configure rules for a basic IPv4 ACL 386
Add a rule for a basic IPv4 ACL 386
Modify the match criteria for a basic IPv4 ACL rule 388

Delete a basic IPv4 ACL rule 389
Configure rules for an extended IPv4 ACL 389
Add a rule for an extended IPv4 ACL 390
Modify the match criteria for an extended IPv4 ACL rule 395
Delete an extended IPv4 ACL rule 396
Configure an IPv6 ACL 396
Add an IPv6 ACL 397
Change the name of an IPv6 ACL 398
Delete an IPv6 ACL 399
Configure rules for an IPv6 ACL 400
Add a rule for an IPv6 ACL 400
Modify the match criteria for an IPv6 ACL rule 405
Delete an IPv6 ACL rule 405
Configure IP ACL interface bindings 406
Bind an IP ACL to one or more interfaces 406
View or delete an IP ACL binding 408
Configure VLAN ACL bindings 409
Add a VLAN ACL binding 409
Remove a VLAN ACL binding 410

Chapter 8 Monitor the Switch and the Traffic

Monitor the switch and the ports 413
View or clear switch statistics 413
View port statistics 415
View and manage detailed port statistics 418
View or clear EAP and EAPoL statistics 424
Perform a cable test 426
Configure and view the logs 427
Manage and view the memory logs 427
Manage and view the flash log 429
Manage the server log 431
View or clear the trap logs and the counters 434
View or clear the event logs 436
Configure port mirroring 437

Chapter 9 Maintain or Troubleshoot the switch

Reboot the switch 440
Reset the switch to its factory default settings 441
Export a file from the switch 442
Use TFTP to export a file from the switch to a TFTP server 442
Use HTTP to export a file from the switch to a computer 444
Download a file to the switch or update the software 445
Use TFTP to download a file to the switch or update the software image 445
Use HTTP to download a file to the switch or update the software image 448
Use an HTTP session to download and install an SSL

security certificate file on the switch 450
Manage software images 451
Copy a software image 452
Configure dual image settings 453
View the dual image status 455
Perform diagnostics and troubleshooting 456
Ping an IPv4 address 456
Ping an IPv6 address 457
Send an IPv4 traceroute 459
Send an IPv6 traceroute 461
Enable remote diagnostics 462
Configure remote SSH diagnostics 463
You cannot log in to the switch 467

Appendix A Configuration Examples

Virtual local area networks (VLANs) 469
VLAN configuration examples 470
Access control lists (ACLs) 471
MAC ACL example configuration 471
Basic IPv4 ACL example configuration 473
Differentiated Services (DiffServ) 474
Class 474
DiffServ traffic classes 475
Create policies 475
DiffServ example configuration 477
802.1X access control 478
802.1X example configuration 480
Multiple Spanning Tree Protocol 481
MSTP example configuration 482
VLAN routing interfaces 484

Appendix B Default Settings and Specifications

Access default settings for the switch device UI 487
System features default settings 487
Switching features default settings 492
Routing and multicast features default settings 498
QoS features default settings 500
Security features default settings 501
Monitoring features default settings 504
Hardware technical specifications 505

1

Get Started

This user manual describes how you can configure and operate the NETGEAR 8-Port Gigabit Ethernet High-Power PoE+ Smart Switch with 2 Dedicated SFP Ports (190W), model GS510TPP, by using the device user interface (UI).

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

This chapter contains the following sections:

- Available publications
- Switch management options and default management mode
- Manage the switch by using the device UI
- Access the switch on-network and connected to the Internet
- Access the switch off-network and not connected to the Internet
- Credentials for the device UI
- Register the switch
- Change the language of the device UI
- Change the management mode of the switch
- Use the Device View of the device UI
- Configure interface settings
- Access the NETGEAR support website
- Access the user manual online

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

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

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

Available publications

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

- *Installation Guide*
- *Hardware Installation Guide*

For information about the NETGEAR Insight Cloud Portal and Insight app, visit netgear.com/insight and netgear.com/support/product/Insight.aspx. For knowledge base articles about NETGEAR Insight, visit netgear.com/support.

Switch management options and default management mode

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

The switch provides administrative management options that let you configure, monitor, and control the network. The device UI is enabled by default, allowing you to configure the switch and the network from a web browser. If you are an Insight Premium or Pro subscriber, you can choose to manage the switch by using the NETGEAR Insight Cloud Portal that is available from a web browser on your Windows-based computer, Mac, or tablet or from the NETGEAR Insight app on a smartphone or tablet.

The switch provides the following management options that let you discover the switch on the network and configure, monitor, and control the switch:

- **Device UI**: By default, the management mode of the switch is set to Directly Connect to Web Browser Interface, which lets you access the device UI. In this mode, you can change all settings of the switch.

  Note: If you plan to use NETGEAR Insight to manage the switch, we recommend that you do not use the device UI to change settings that are *Insight manageable*. These settings would not be synchronized with Insight or to the network location to which you assigned the switch. We recommend that use the Insight Cloud Portal or Insight app to change *Insight manageable* settings.

- **NETGEAR Insight Cloud Portal and Insight app**: If you set the management mode of the switch to *NETGEAR Insight Mobile App and Insight Cloud Portal*, you can use the following applications to manage the switch remotely:
  - **Insight Cloud Portal**: As an Insight Premium or Insight Pro user, you can use the Insight Cloud Portal to set up the switch in the network; perform remote setup; configure, manage, and monitor the switch; analyze the switch and network usage; and, if necessary, troubleshoot the switch and the network.
  - **NETGEAR Insight app**: With the Insight app, you can discover the switch on the network and add it to a network location. You can then set up the switch in the network, and manage and monitor the switch remotely from your tablet or smartphone. You can choose from four methods to add the switch to the Insight app: You can scan your network for the switch, scan the QR code of the switch, scan the barcode of the switch, or add the serial number of the switch.

  For more information about NETGEAR Insight, visit netgear.com/insight. The Insight Cloud Portal and Insight app have embedded help and are documented in multiple knowledge base articles that you can access by visiting netgear.com/support.

To use the NETGEAR Insight Cloud Portal or NETGEAR Insight app management method, you must change the method to *NETGEAR Insight Mobile App and Insight Cloud Portal*. After

you do so, you can also change the method back to *Directly Connect to Web Browser Interface* and use the device UI. For more information, see Change the management mode of the switch on page 26.

Manage the switch by using the device UI

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

For information about how you can manage and monitor the switch with the Insight Cloud Portal and Insight app, visit netgear.com/business/services/insight. The Insight Cloud Portal and Insight app have embedded help and are documented in multiple knowledge base articles that you can access by visiting netgear.com/support/product/insight.

Navigation tabs, configuration menus, and page menu

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

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

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

Configuration and Status Options

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

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

Buttons in the device UI

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

Table 1. Command buttons in the device UI

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

User-defined fields

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

Table 2. Invalid characters for user-defined fields

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

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 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 17).

- **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 22.

Note: We recommend that you register the switch to activate your warranty. For more information, see Register the switch on page 24.

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 18.

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 Insight mobile app**: You can install the NETGEAR Insight mobile app on an iOS or Android mobile device and discover the IP address of the switch. See Use the NETGEAR Insight app to discover the IP address of the switch on page 19.
- **NETGEAR Discovery Tool (NDT)**: If you use a Mac, Linux-based computer, or 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 20.
- **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 21.

When you know the IP address, you can configure the switch in the following ways:

- **Device UI**: For configuration of all switch features, access the switch over the device UI. See Access the switch on-network when you know the switch IP address on page 21.
- **NETGEAR Insight app and Insight Cloud Portal**: You can change the management mode of the switch so that you can use the NETGEAR Insight Cloud Portal and Insight app to manage the switch remotely. For more information, see Change the management mode of the switch on page 26.

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 Windows Explorer.
5. Click the **Network** link.
6. If prompted, enable the Network Discovery feature.
7. Under Network Infrastructure, locate the switch model number.

   The model number is GS510TPP.
8. Double-click **GSmodel-XXXXXX**, in which GSmodel is the model number of your switch and XXXXXX represents the last six digits of the switch MAC address.

   The device UI login page displays.
9. Enter one of the following passwords:
   - **Device admin password**: 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.
   - **Insight network password**: If you previously logged in to the device UI, you changed the management mode to NETGEAR Insight, and you added the switch to an Insight network location, enter the Insight network password to access the device UI. (In such a situation, the Insight network password replaces the switch device admin password.)

   For information about the credentials, see Credentials for the device UI on page 23.

10. Click the **Login** button.

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

Use the NETGEAR Insight app to discover the IP address of the switch

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

If you do not use the NETGEAR Insight app to claim the switch by adding it to an Insight network location, the switch is not registered and your warranty is not activated.

Using the NETGEAR Insight app to discover the IP address of the switch in your network is not the same as managing the switch with the Insight app or the Insight Cloud Portal.

Note: The default management mode of the switch is the device UI. If you want to use the Insight Cloud Portal or the Insight app to manage the switch, you first must change the management mode (see Change the management mode to NETGEAR Insight Mobile App and Insight Cloud Portal on page 27). After you do so, you can manage the switch with Insight and add the switch to an Insight network location.

To use the NETGEAR Insight app to discover the IP address of the switch in your network when the switch is connected to the Internet:

1. On your iOS or Android mobile device, go to the app store, search for NETGEAR Insight, download the latest version of the app, and install the app.
2. Connect your mobile device to the WiFi network of the WiFi router or access point to which the switch is connected.
3. Open the NETGEAR Insight app.
4. If you did not set up a NETGEAR account, tap **Create NETGEAR Account** and follow the onscreen instructions.
5. Enter the email address and password for your account and tap **LOG IN**.

   After you log in to your account, the IP address of the switch displays in the device list.
6. Write down the IP address for future use.

   You can use this IP address to access the switch directly from a web browser. For information about how to do this, see Access the switch on-network when you know the switch IP address on page 21.

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 lets you discover the switch in your network and access the device UI of the switch from a Mac, Linux-based computer, or Windows-based computer.

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

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

   Depending on the computer that you are using, download either the Mac version, the version for a Linux-based computer, 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, Linux desktop, 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 Too**l icon on your desktop.

   The initial page displays a menu and a button.
8. From the **Choose a connection** menu, 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. To access the switch from the NDT, do the following:
    a. Click the **ADMIN PAGE** button next to your switch.

    The device UI login page displays.

11. Enter one of the following passwords:
    - **Device admin password**: 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.
    - **Insight network password**: If you previously logged in to the device UI, you changed the management mode to NETGEAR Insight, and you added the switch to an Insight network location, enter the Insight network password to access the device UI. (In such a situation, the Insight network password replaces the switch device admin password.)

    For information about the credentials, see Credentials for the device UI on page 23.
12. Click the **Login** button.

    The System Information 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 21.

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 device UI login page displays.
3. Enter one of the following passwords:
    - **Device admin password**: 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.

- **Insight network password**: If you previously logged in to the device UI, you changed the management mode to NETGEAR Insight, and you added the switch to an Insight network location, enter the Insight network password to access the device UI. (In such a situation, the Insight network password replaces the switch device admin password.)

For information about the credentials, see Credentials for the device UI on page 23.

4. Click the **Login** button.

   The System Information 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 not connected to the Internet:

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

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

2. Connect your computer to the switch using an Ethernet cable.
3. Power on the switch by connecting its power cord.
4. Launch a web browser.
5. 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 device UI login page displays.

6. Enter one of the following passwords:
   - **Device admin password**: 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.
   - **Insight network password**: If you previously logged in to the device UI, you changed the management mode to NETGEAR Insight, and you added the switch to an Insight network location, enter the Insight network password to access the device UI. (In such a situation, the Insight network password replaces the switch device admin password.)

   For information about the credentials, see Credentials for the device UI on page 23.
7. Click the **Login** button.

   The System Information 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.

Credentials for the device UI

The information in this section applies to accessing the switch device UI in either management mode. That is, it does *not* apply to accessing the NETGEAR Cloud Portal and Insight app.

To access the device UI, and depending on your situation, use one of the following credentials:

- **Device admin password**:

  You can access the device UI with your device admin password.

  The first time that you access the device UI, enter the default device admin password (**password**), after which you are required to customize the password for greater security. Subsequent times that you log in to the device UI, use your customized device admin password.
- **NETGEAR Insight network location password**:

  NETGEAR Insight can affect how you access the switch device UI. After you add the switch to an Insight network location and change the management mode of the switch so that you can use the NETGEAR Insight Cloud Portal and Insight app to manage the switch remotely (see Change the management mode of the switch on page 26), the

Insight network location password replaces the switch device admin password. To access the device UI, you must enter the Insight network location password.

Even if you *temporarily* change the management mode of the switch back to *Direct Connect Web Browser Interface*, for example to change settings that are not Insight-manageable or for debugging purposes, you must enter the Insight network location password.

For information about how the Insight network password functions, visit netgear.com/support/product/Insight.aspx. For knowledge base articles about NETGEAR Insight, visit netgear.com/support.

The following table lists the essential credential options for access to the device UI.

Table 3. Credentials for access to the device UI

Management mode in the device UI	Added to an Insight network	Credentials	Device UI menu
Default mode: Direct Connect Web Browser Interface (Local LAN Only)	No	Device admin password	Full device UI menu
	Yes[1]	Insight network password	
NETGEAR Insight Mobile App and Insight Cloud Portal (Cloud/Remote)	No	Device admin password	Limited device UI menu. *Not* managed through NETGEAR Insight.
	Yes	Insight network password	Limited device UI menu. Managed through NETGEAR Insight.

1. This situation occurs if you temporarily change the management mode of the switch from NETGEAR Insight Mobile App and Insight Cloud Portal back to Direct Connect Web Browser Interface.

Register the switch

Register your switch online to activate your warranty.

To register the switch:

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

   Note: 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.

Change the language of the device UI

By default, the language is set to Auto. You can set the language 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

   A confirmation pop-up window displays.
7. Click the **OK** 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 management mode of the switch

By default, the management mode on the switch is *Directly Connect to Web Browser Interface* (which is the same as the device UI). You can also change the management mode to *NETGEAR Insight Mobile App and Insight Cloud Portal*.

About changing the management mode

The following applies to changing the management mode:

- **Changing to the NETGEAR Insight Mobile App and Insight Cloud Portal mode**.
  - The first time that you enable this mode, the switch is reset to its factory default settings so that you can create the switch configuration and network topology using the Insight Cloud Portal or the Insight app.
  - If you previously added the switch to a network location on the Insight Cloud Portal or the Insight app, all Insight-manageable device settings are returned to the last configuration saved on the cloud server, including the switch device admin password (that is, the password is reset to the Insight network location password).
  - If you use the Insight Cloud Portal or the Insight app, you can temporarily change the management mode of the switch back to *Directly Connect to Web Browser Interface*. You can then access the device UI for settings that are not Insight-manageable, for complex tasks such as integrating with an existing network of devices that are not managed through Insight, and for debugging purposes. When you are done, you can change the management mode back to *NETGEAR Insight Mobile App and Insight Cloud Portal*.
- **Permanently changing back to Directly Connect to Web Browser Interface mode**.

  If you want to permanently change the management mode back to *Directly Connect to Web Browser Interface*, we recommend that after you change the management mode, you back up your configuration. Then, reset the switch to factory defaults. Finally, restore your configuration and reboot the switch. For more information, see Permanently change the management mode back to Directly Connect to Web-browser Interface on page 28.

  After you change the management mode, the follow occurs:

  - The *NETGEAR Insight Mobile App and Insight Cloud Portal* management mode is disabled and the current Insight-manageable device settings are saved to the cloud server.
  - Any changes that you make using the *Directly Connect to Web Browser Interface* management mode are no longer saved to the cloud server.
  - All configuration menus and options are available in the device UI.

Change the management mode to NETGEAR Insight Mobile App and Insight Cloud Portal

To change the management mode of the switch to NETGEAR Insight Mobile App and Insight Cloud Portal:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select the **NETGEAR Insight Mobile App and Insight Cloud Portal** radio button.

   An Alert pop-up window displays.

7. Read the text, and click the **OK** button.

   The pop-up window closes.

8. Click the **Apply** button.

   Another pop-up window displays.

9. Click the **OK** button.

   The pop-up window closes, the System Information page closes, and your settings are saved.

   The following occurs:

   - The first time that you enable this mode, the switch is reset to its factory default settings.
   - The switch connects to the cloud server.
   - If you previously added the switch to a network on the Insight Cloud Portal or Insight app, all Insight-manageable device settings are returned to the last configuration

saved on the cloud server, including the device admin password (that is, the password is reset to the Insight network password).

- The Device UI login page might display again. (You can close the page.)

You can now manage the switch using the Insight Cloud Portal or Insight app.

For more information about NETGEAR Insight, visit netgear.com/insight and netgear.com/support/product/Insight.aspx. For knowledge base articles about NETGEAR Insight, visit netgear.com/support.

Permanently change the management mode back to Directly Connect to Web-browser Interface

Note: If you use the Insight Cloud Portal or the Insight app, you can temporarily change the management mode of the switch back to *Directly Connect to Web Browser Interface*. You can then access the device UI for settings that are not Insight-manageable, for complex tasks such as integrating with an existing network of devices that are not managed through Insight, and for debugging purposes. When you are done, you can change the management mode back to *NETGEAR Insight Mobile App and Insight Cloud Portal*.

After you permanently change the management mode of the switch back to *Directly Connect to Web Browser Interface*, we recommend that you back up the configuration, reset the switch to factory default settings, restore the configuration that you just backed up, and then reboot the switch.

To permanently change the management mode of the switch back to Directly Connect to Web Browser Interface:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select the **Directly Connect to Web Browser Interface** radio button.

   An Alert pop-up window displays.

7. Read the text, and click the **OK** button.

   The pop-up window closes.

8. Click the **Apply** button.

   Another pop-up window displays.

9. Click the **OK** button.

   The pop-up window closes, the System Information page closes, and your settings are saved. Any current Insight-manageable device settings are saved to the cloud server.

   The device UI login page displays.

10. Log in again.

    The System Information page displays.

    Note: The following step uses an HTTP session to back up the configuration. For information about using a TFTP session, see Use TFTP to export a file from the switch to a TFTP server on page 442.

11. Back up the configuration:
    a. Select **Maintenance > Export > HTTP File Export**.

       The HTTP File Export page displays.

    b. From the **File Type** menu, select **Text Configuration**.
    c. Click the **Apply** button.

       A pop-up window displays.

    d. Navigate to a location on your computer and save the file.

       The file transfer begins. The page displays information about the file transfer progress.

12. Reset the switch to factory default settings:
    a. Select **Maintenance > Reset > Factory Default**.

       The Default Settings page displays.

    b. Select the check box.
    c. Click the **Apply** button.

An Alert pop-up window displays.

d. Click the **OK** button.

All configuration settings are reset to their factory default values. The DHCP client on the switch is enabled. Your device admin password is reset to the default password (**password**). This process takes about 135 seconds.

The device UI login page displays.

In the unlikely situation that the Device UI page does not display and you cannot log in, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

e. 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.

The System Information page displays.

Note: The following step uses an HTTP session to restore the configuration. For information about using a TFTP session, see Use TFTP to download a file to the switch or update the software image on page 445.

13. Restore the configuration that you saved in Step 11:

a. Select **Maintenance > Update > HTTP Firmware/File Update**.

The HTTP Firmware/File Update page displays.

b. From the **File Type** menu, select **Text Configuration**.

c. Click the **Browse** button and locate and select configuration file that you saved in Step 11.

d. Click the **Apply** button.

The file transfer begins. The page displays information about the progress of the file transfer. The switch applies the configuration automatically.

14. Reboot the switch:

a. Select **Maintenance > Reset > Device Reboot**.

The Device Reboot page displays.

b. Select the check box.

c. Click the **Apply** button.

An Alert pop-up window displays.

d. Click the **OK** button to confirm.

The switch reboots.

The device UI login page displays.

15. Log in again.

The System Information page displays. You can now configure the switch using all options in the device UI.

Use the Device View of the device UI

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

To use the Device View:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Device View**.

   The Device View page displays.

   The system LEDs display on the left side on the Device View page:

   - **Power LED**. A bicolor LED that serves as an indicator of power and diagnostic status. If the LED is solid green, the power is supplied to the switch and operating normally.
   - **Fan LED**. Indicates the following status:
     - **Off**. The fan is operating normally.
     - **Solid yellow**. The fan is faulty.
   - **PoE Max**. Indicates the following status:
     - **Off**. Sufficient (more than 7W of) PoE power is available on the switch.

- **Solid yellow**. Less than 7W of PoE power is available on the switch.

  In this situation, the physical PoE Max LED on the switch lights solid amber rather than yellow.

  The physical PoE Max LED on the switch can also blink amber, indicating that at least once during the previous two minutes, less than 7W of PoE power was available.

Depending upon the status of the port, the port color on the Device View page is either green, yellow, or black:

- **Green port color**: The port is linking up.
- **Yellow port color**: A PoE fault occurred on the port.

  In this situation, the physical lower port LED on the switch lights solid amber rather than yellow.

- **Black port color**: No link is present.

Each port also provides one LED on the Device View page to indicate the link status of the port:

- **Green LED**: The port is linking at a speed of 1 Gbps.
- **Yellow LED**: The port is linking at a speed of 10 Mbps or 100 Mbps.

7. To display a port menu that shows configuration and statistics options, click a port.

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

8. To display the main menu, right-click the switch graphic but do not right-click a specific port.

   The menu contains the same options as the navigation tabs at the top of the page. You can select a menu option to access the page that contains the configuration or monitoring options.

Configure interface settings

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

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

Table 4. Naming conventions for interfaces

Interface	Description	Example
Physical	The physical ports are Gigabit Ethernet interfaces and are numbered sequentially starting from 1.	g1, g2, g12
Link aggregation group (LAG)	LAG interfaces are logical interfaces that are used only for bridging functions.	l1, l2, l3
CPU management interface	This is the internal switch interface that determines the switch base MAC address. This interface is not configurable and is always listed in the MAC Address Table.	c1
Routing VLAN interfaces	This is an interface used for routing functionality.	VLAN 1, VLAN 2, VLAN 3

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

- A single port
- Multiple ports
- All ports
- A single LAG
- Multiple LAGs
- All LAGs
- Multiple ports and LAGs
- All ports and LAGs

Many of the pages that allow you to configure or view interface settings include links to display all ports, all LAGs, or all ports and LAGs on the page.

Access the NETGEAR support website

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

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

Access the user manual online

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

To access the user manual online from the 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. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
3. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
4. Click the **Login** button.

   The System Information page displays.

5. Select **Help > Online Help > User Manual**.

   The User Guide page displays.

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

   Enter the model number of the switch.

2

Configure System Information

This chapter contains the following sections:

- View or define system information
- Configure the IP network settings for management access
- Configure the time settings
- Configure denial of service settings
- Configure DNS settings
- Configure green Ethernet settings
- Use the Device View
- Configure Power over Ethernet
- Configure SNMP
- Configure Link Layer Discovery Protocol
- Configure a DHCP L2 relay
- Configure DHCP snooping
- Configure Dynamic ARP Inspection
- Set up PoE timer schedules

View or define system information

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

To view or define system information:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   Your settings are saved.

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

Table 5. System Information

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

View the fan status

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

To view the fan status:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Scroll down to the Fans section.
7. To refresh the page, click the **Refresh** button.

The following table describes the view-only fan status information.

Table 6. Fan status

Field	Description
FAN	The fan index used to identify the fan for the switch.
Description	The description of the fan.
Type	Specifies whether the fan module is fixed or removable.
Speed	The fan speed.
Duty level(%)	The duty level of the fan.
State	Specifies whether the fan is operational.

View the power supply information

You can view the status of the power supplies.

To view the power supplies status:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Scroll down to the Power supplies section.
7. To refresh the page, click the **Refresh** button.

The following table describes the view-only Power supplies information.

Table 7. Power supplies status

Field	Description
Power supply	The power supply index used for the unit.
Description	The description of the power supply.
Type	Specifies whether the power module is fixed or removable.
State	Specifies the state of the power module.

View the software versions

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

To view the software versions:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Scroll down to the Versions section.
7. To refresh the page, click the **Refresh** button.

The following table describes the view-only information displayed in the Versions section of the System Information page.

Table 8. Versions information

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

View the system CPU status

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

To view the system CPU status:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

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

The following table describes the view-only CPU memory status information.

Table 9. CPU Memory Status information

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

Configure the CPU thresholds

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

To configure the CPU thresholds:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

   The CPU Threshold page displays.
7. Specify the thresholds:
   - **Rising Threshold**. Notification is generated when the total CPU utilization exceeds this threshold value over the configured time period. The range is 1 to 100.
   - **Rising Interval**. This utilization monitoring time period can be configured from 5 to 86400 seconds in multiples of 5 seconds.

- **Falling Threshold**. Notification is triggered when the total CPU utilization falls below this level for a configured period of time.

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

8. Click the **Apply** button.

   Your settings are saved.

Configure the 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 network and VLAN settings for the device UI

You can configure the IPv4 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.

To configure the IPv4 network and VLAN settings for 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

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

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

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

Note: Make sure that the VLAN that must be the management VLAN exists. Also make sure that the PVID of at least one port in the VLAN is the same as the management VLAN ID. For information about creating VLANs and configuring the PVID for a port, see Configure VLANs on page 149.

The following requirements apply to the management VLAN:

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

10. Click the **Apply** button.

    Your settings are saved.

Configure the IPv6 network settings for the local browser interface

You can configure IPv6 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.

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

- IPv6 auto-configuration
- DHCPv6

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

To configure the IPv6 network settings for 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Management > IPv6 Network Configuration**.

   The IPv6 Network Global Configuration page displays.
7. Ensure that the Admin Mode **Enable** radio button is selected.
8. Determine how the switch acquires an IPv6 address:
   - **IPv6 Address Auto Configuration Mode**. When this mode is enabled, the network interface can acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of router advertisement messages. When this mode is disabled (the default setting), the network interface does not use the native IPv6 address auto-configuration features to acquire an IPv6 address. Auto-configuration can be enabled only when DHCPv6 is not enabled on any of the management interfaces.
   - **DHCPv6**. Next to Current Network Configuration Protocol, select the **DHCPv6** radio button to enable the DHCPv6 client on the interface. The switch attempts to acquire network information from a DHCPv6 server. Selecting the **None** radio button disables the DHCPv6 client on the network interface. When DHCPv6 is enabled, the DHCPv6 Client DUID field displays the client identifier used by the DHCPv6 client (if enabled) when sending messages to the DHCPv6 server.
9. In the **IPv6 Gateway** field, specify the default gateway for the IPv6 network interface.

   The gateway address is in IPv6 global or link-local address format.
10. To configure one or more static IPv6 addresses for the management interface, do the following:
    a. In the **IPv6 Prefix/Prefix Length** field, specify the static IPv6 prefix and prefix to the IPv6 network interface.

       The address is in the global address format.
    b. In the **EUI64** menu, select **True** to enable the Extended Universal Identifier (EUI) flag for IPv6 address, or select **False** to omit the EUI flag.
    c. Click the **Add** button.
11. Click the **Apply** button.

    Your settings are saved.

View the IPv6 network neighbors

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

To view the IPv6 Network Neighbor Table:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Management > IPv6 Network Neighbor**.

   The IPv6 Network Interface Neighbor Table page displays.

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

Table 10. IPv6 network interface neighbor table information

Field	Description
IPv6 address	The IPv6 address of a neighbor switch visible to the network interface.
MAC address	The MAC address of a neighbor switch.
IsRtr	• **true (1)**. The neighbor machine is a router. • **false (2)**. The neighbor machine is not a router.

Table 10. IPv6 network interface neighbor table information (continued)

Field	Description
Neighbor State	The state of the neighboring switch: • **reachable (1)**. The neighbor is reachable by this switch. • **stale (2)**. Information about the neighbor is scheduled for deletion. • **delay (3)**. No information was received from the neighbor during the delay period. • **probe (4)**. The switch is attempting to probe for this neighbor. • **unknown (5)**. Unknown status.
Last Updated	The last sysUpTime that this neighbor was updated.

Configure the time settings

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

Configure the time setting manually

You can view and adjust date and time settings.

To manually configure the time setting:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

The System Information page displays.

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

   The Time Configuration page displays.

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

   The page adjusts.

8. In the **Date** field, specify the current date in months, days, and years (MM/DD/YYYY).
9. In the **Time** field, specify the current time in hours, minutes, and seconds (HH:MM:SS).

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

10. Click the **Apply** button.

    Your settings are saved.

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

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

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

The Time Configuration page displays.

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

   If this button was not yet selected, the page refreshes and displays the SNTP Global Configuration section and the SNTP Global Status section.

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

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

8. Next to Client Mode, select the mode of operation of the SNTP client:
   - **Unicast**. SNTP operates in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the round-trip delay and local clock offset relative to the server.
   - **Broadcast**. SNTP operates in the same manner as multicast mode but uses a local broadcast address instead of a multicast address. The broadcast address provides a single-subnet scope while a multicast address provides an Internet-wide scope.

   The default value is Unicast.

9. If the SNTP client mode is **Unicast**, use the SNTP Server Configuration page to add the IP address or DNS name of one or more SNTP servers for the switch to poll.

   For more information, see Configure an SNTP server on page 53.

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

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

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

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

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

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

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

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

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

15. In the **Time Zone Name** field, specify a 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 is different from the Coordinated Universal Time (UTC). The time zone can affect the display of the current system time. There is no default value.

Note: When you use an SNTP time server, the time data that is received from the server is based on the UTC, which is the same as Greenwich Mean Time (GMT). This might not be the time zone in which the switch is located.

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

    The allowed range is –12 to 14. The default value is 0.

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

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

18. Click the **Apply** button.

    Your settings are saved.

View the SNTP global status

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

To view SNTP global status:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The Time Configuration page displays.

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

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

The following table displays the view-only SNTP Global Status information.

Table 11. SNTP Global Status information

Field	Description
Version	The SNTP version that the client supports.
Supported Mode	The SNTP modes that the client supports. Multiple modes can be supported by a client.
Last Update Time	The local date and time (UTC) that the SNTP client last updated the system clock.
Last Attempt Time	The local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.
Last Attempt Status	The status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message was received from a server, a status of **Other** is displayed. These values are appropriate for all operational modes. • **Other**. The status of the last request is unknown. • **Success**. The SNTP operation was successful and the system time was updated. • **Request Timed Out**. After an SNTP request was sent to an SNTP server, the response timer expired before a response from the server was received. • **Bad Date Encoded**. The time provided by the SNTP server is not valid. • **Version Not Supported**. The SNTP version supported by the server is not compatible with the version supported by the client. • **Server Unsynchronized**. The SNTP server is not synchronized with its peers. This is indicated by the leap indicator field in the SNTP message. • **Server Kiss Of Death**. The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.
Server IP Address	The IP address of the server for the last received valid packet. If no message was received from any server, an empty string is shown.
Address Type	The address type of the SNTP server address for the last received valid packet.
Server Stratum	The claimed stratum of the server for the last received valid packet.
Reference Clock ID	The reference clock identifier of the server for the last received valid packet.

Table 11. SNTP Global Status information (continued)

Field	Description
Server mode	The mode of the server for the last received valid packet.
Unicast Server Max Entries	The maximum number of unicast server entries that can be configured on this client.
Unicast Server Current Entries	The number of current valid unicast server entries configured for this client.
Broadcast Count	The number of unsolicited broadcast SNTP messages that were received and processed by the SNTP client since the last reboot.

Configure an SNTP server

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

Time sources are established by strata. Strata define the accuracy of the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock. The device receives time from Stratum 1 and above since it is itself a Stratum 2 device.

The following is an example of strata:

- **Stratum 0**. A real-time clock is used as the time source, for example, a GPS system.
- **Stratum 1**. A server that is directly linked to a Stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.
- **Stratum 2**. The time source is distanced from the Stratum 1 server over a network path. For example, a Stratum 2 server receives the time over a network link, through NTP, from a Stratum 1 server.

Information received from SNTP servers is evaluated based on the time level and server type.

SNTP time definitions are assessed and determined by the following time levels:

- **T1**. Time that the original request was sent by the client.
- **T2**. Time that the original request was received by the server.
- **T3**. Time that the server sent a reply.
- **T4**. Time that the client received the server's reply.

The device can poll unicast server types for the server time.

Polling for unicast information is used for polling a server for which the IP address is known. SNTP servers that were configured on the device are the only ones that are polled for synchronization information. T1 through T4 are used to determine server time. This is the preferred method for synchronizing device time because it is the most secure method. If this method is selected, SNTP information is accepted only from SNTP servers defined on the device using the SNTP Server Configuration page.

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

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

Add an SNTP server

To add an SNTP server:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

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

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

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

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

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

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

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

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

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

11. In the **Version** field, specify the SNTP version that is supported by the switch.

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

12. Click the **Add** button.

    The SNTP server entry is added.

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

    You can configure up to three SNTP servers.

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

Table 12. SNTP Server Status information

Field	Description
Address	All the existing server addresses. If no server configuration exists, a message stating that no SNTP server exists displays on the page.
Last Update Time	The local date and time (UTC) that the response from this server was used to update the system clock.
Last Attempt Time	The local date and time (UTC) that this SNTP server was last queried.
Last Attempt Status	The status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message was received from a server, a status of Other is displayed. These values are appropriate for all operational modes: • **Other**. The status of the last request is unknown, or no SNTP responses were received. • **Success**. The SNTP operation was successful and the system time was updated. • **Request Timed Out**. After an SNTP request was sent to an SNTP server, the response timer expired before a response from the server was received. • **Bad Date Encoded**. The time provided by the SNTP server is not valid. • **Version Not Supported**. The SNTP version supported by the server is not compatible with the version supported by the client. • **Server Unsynchronized**. The SNTP server is not synchronized with its peers. This is indicated by the leap indicator field on the SNTP message.
Requests	The number of SNTP requests made to this server since last agent reboot.
Failed Requests	The number of failed SNTP requests made to this server since the last reboot.

Change the settings for an existing SNTP server

To change the settings for an existing SNTP server:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

   The SNTP Server Configuration page displays.
7. Select the check box next to the configured server.
8. Change the settings.
9. Click the **Apply** button.

   Your settings are saved.

Remove an SNTP server

To remove an SNTP server:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

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

   The entry is removed, and the device is updated.

Configure daylight saving time settings

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

To configure the daylight saving time settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

The System Information page displays.

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

   The Daylight Savings Configuration page displays.

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

   Your settings are saved.

The fields in the following tables are visible only when the Daylight Saving (DST) **Recurring**, **Recurring EU**, or **Recurring USA** radio button is selected.

Table 13. Daylight saving setting is Recurring, Recurring EU, or Recurring USA

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

The fields in the following table are visible only when the DayLight Saving (DST) **Non Recurring** radio button is selected.

Table 14. Daylight saving setting is Non Recurring

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

View the daylight saving time status

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

To view the daylight saving time status:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The Daylight Savings Configuration page displays.

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

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

Table 15. Daylight Saving (DST) Status information

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

Configure denial of service settings

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

Configure Auto-DoS

You can automatically enable all the DoS features available on the switch, except for the L4 Port attack. For information about the types of DoS attacks the switch can monitor and block, see Configure denial of service on page 61.

To enable the Auto-DoS feature:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

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

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

   Your settings are saved.

Configure denial of service

You can select which types of denial of service (DoS) attacks the switch monitors and blocks.

To configure individual DoS settings:

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Management > Denial of Service > Denial of Service Configuration**.

   The Denial of Service Configuration page displays.
7. Select the types of DoS attacks for the switch to monitor and block and configure any associated values:
   - **Denial of Service Min TCP Header Size**. Specify the minimum allowed TCP header size. If you select the Denial of Service TCP Fragment **Enable** radio button, 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 255. The default value is 20.
   - **Denial of Service ICMPv4**. Enabling ICMPv4 DoS prevention causes the switch to drop ICMPv4 packets with a type set to ECHO_REQ (ping) and a size that exceeds the specified maximum allowed ICMP packet size. By default, this option is disabled.
   - **Denial of Service Max ICMPv4 Packet Size**. Specify the maximum allowed ICMP packet size. If you select the Denial of Service ICMPv4 **Enable** radio button, the switch drops ICMP ping packets that exceed the size that you specify. Enter a value in the range from 0 to 16376. The default value is 512.
   - **Denial of Service ICMPv6**. Enabling ICMPv6 DoS prevention causes the switch to drop ICMPv6 packets with a type set to ECHO_REQ (ping) and a size that exceeds the specified maximum allowed ICMPv6 packet size. By default, this option is disabled.
   - **Denial of Service Max ICMPv6 Packet Size**. Specify the maximum allowed ICMP packet size. If you select the Denial of Service ICMPv6 **Enable** radio button, the switch drops ICMPv6 ping packets that exceed the size that you specify. Enter a value in the range from 0 to 16376. The default value is 512.
   - **Denial of Service First Fragment**. Enabling First Fragment DoS prevention causes the switch to check DoS options on the first fragment IP packets when the switch is receiving fragmented IP packets. Otherwise, the switch ignores the first fragment IP packets.

- **Denial of Service ICMP Fragment**. Enabling ICMP Fragment DoS prevention causes the switch to drop fragmented ICMP packets. By default, this option is disabled.
- **Denial of Service SIP=DIP**. Enabling SIP=DIP DoS prevention causes the switch to drop packets with a source IP address that is equal to the destination IP address. By default, this option is disabled.
- **Denial of Service SMAC=DMAC**. Enabling SMAC=DMAC DoS prevention causes the switch to drop packets with a source MAC address that is equal to the destination MAC address. By default, this option is disabled.
- **Denial of Service TCP FIN&URG&PSH**. Enabling TCP FIN & URG & PSH DoS prevention causes the switch to drop packets for which the TCP FIN, URG, and PSH flags are set to 1 and for which the TCP sequence number is set to 0. By default, this option is disabled.
- **Denial of Service TCP Flag&Sequence**. Enabling TCP Flag DoS prevention causes the switch to drop packets for which the TCP control flags are set to 0 and the TCP sequence number is set to 0. By default, this option is disabled.
- **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 smaller than the minimum allowed TCP header size. By default, this option is disabled.
- **Denial of Service TCP Offset**. Enabling TCP Offset DoS prevention causes the switch to drop packets with a TCP header offset of 1. By default, this option is disabled.
- **Denial of Service TCP Port**. Enabling TCP Port DoS prevention causes the switch to drop packets with a TCP source port that is equal to the TCP destination port. By default, this option is disabled.
- **Denial of Service TCP SYN**. Enabling TCP SYN DoS prevention causes the switch to drop packets for which the TCP flag SYN is set to 1. By default, this option is disabled.
- **Denial of Service TCP SYN&FIN**. Enabling TCP SYN & FIN DoS prevention causes the switch to drop packets for which the TCP flags SYN and FIN are set to 1. By default, this option is disabled.
- **Denial of Service UDP Port**. Enabling UDP Port DoS prevention causes the switch to drop packets with a UDP source port that is equal to the UDP destination port. By default, this option is disabled.

8. Click the **Apply** button.

   Your settings are saved.

Configure DNS settings

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

Configure the global DNS settings and add a DNS server

You can configure the global DNS settings and DNS server information.

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

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

   When the system is performing a lookup on an unqualified host name, this field is provides the domain name (for example, if default domain name is netgear.com and the

user enters test, then test is changed to test.netgear.com to resolve the name). The name must not be longer than 255 characters.

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

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

    Your settings are saved.
12. To refresh the page, click the **Refresh** button.

The following table displays view-only DNS Server Configuration information.

Table 16. DNS Server Configuration information

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

Remove a DNS server

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

To remove a DNS server:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The DNS Configuration page display.

7. In the DNS Server Configuration table, select the check box for the DNS server.

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

8. Click the **Delete** button.

   The DNS server is removed.

Configure and view host name-to-IP address information

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

Add a static entry to the dynamic host mapping table

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

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The DNS Host Configuration page display.

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

   Its length cannot exceed 255 characters and it is a required field.
8. In the **IPv4/IPv6 Address** field, enter the IPv4 or IPv6 address to associate with the host name.
9. Click the **Add** button.

   The entry displays in the list on the page.

Change the host name or IP address in an entry of the dynamic host mapping table, view all entries, or clear all entries

To change the host name or IP address in an entry of the dynamic host mapping table, view all entries, or clear all entries:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

   The DNS Host Configuration page display.
7. Select the check box next to the entry to update.
8. Enter the new information in the appropriate field.
9. Click the **Apply** button.

   Your settings are saved.
10. To clear all the dynamic host name entries from the list, click the **Clear** button.

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

Table 17. Dynamic Host Mapping information

Field	Description
Host	Lists the host name that you assign to the specified IP address.
Total	Time since the dynamic entry was first added to the table.
Elapsed	Time since the dynamic entry was last updated.
Type	The type of the dynamic entry.
IPv4/IPv6 Addresses	Lists the IP address associated with the host name.

Remove an entry from the dynamic host mapping table

To remove an entry from the dynamic host mapping table:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

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

   The entry is removed.

Manage UPnP switch discovery

By default, Universal Plug and Play (UPnP) is enabled on the switch. UPnP allows the switch to be discovered in your network, for example on Windows-based computers and mobile devices on which the NETGEAR Insight app is installed. For greater security, you can disable UPnP.

To manage UPnP switch discovery:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Management > Switch Discovery**.

   The Switch Discovery page displays.
7. Select the UPnP Administrative Mode **Disable** or **Enable** radio button.

   By default, this mode is enabled.
8. Click the **Apply** button.

   Your settings are saved.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The Green Ethernet Configuration page displays.

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

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

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

   By default, this mode is disabled. Energy Efficient Ethernet (EEE) combines the MAC with a family of physical layers that support operation in a low power mode. It is defined by the IEEE 802.3az standard. Lower power mode enables both the send and receive sides of the link to disable some functionality for power savings when 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.

9. Click the **Apply** button.

   Your settings are saved.

Configure green Ethernet interface settings

You can configure green Ethernet settings for individual interfaces.

To configure the green Ethernet interface settings:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The Green Ethernet Interface Configuration page displays.

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

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

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

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

   By default, this mode is disabled. Energy Efficient Ethernet (EEE) combines the MAC with a family of physical layers that support operation in a low power mode. It is defined by the IEEE 802.3az standard. Lower power mode enables both the send and receive sides of the link to disable some functionality for power savings when 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 **Apply** button.

    Your settings are saved.

Configure and display detailed green Ethernet settings for an interface

You can select a single interface and configure and display detailed green Ethernet settings.

To configure and display detailed green Ethernet settings for a single interface:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **System > Management > Green Ethernet > Green Ethernet Detail**.

The Green Ethernet Details page displays.

7. From the **Interface** menu, select the interface.
8. From the **Energy Detect Admin Mode** menu, select to enable or disable this mode.

   By default, this mode is disabled for the interface. When a port link is down, the underlying physical layer goes down for a short period and then checks for port link pulses again so that auto-negotiation remains possible. In this way, the switch saves power when no link partner is present for the port.
9. From the **EEE Admin Mode** menu, select to enable or disable this mode.

   With Energy Efficient Ethernet (EEE) mode enabled, the port transitions to low power mode during a link idle condition. The default value is Disabled.
10. In the **EEE Transmit Idle Time** field, enter the period that the interface must remain idle (without receiving packets for transmission) before entering the low-power idle (LPI) state.

    The range is from 600 to 4294967295 seconds. The default is 600 seconds.
11. In the **EEE Transmit Wake Time** field, enter the period that the interface must remain in the LPI state before returning to the active state after it receives a packet for transmission.

    The range is from 8 to 65535 seconds. The default is 17 seconds.
12. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only fields.

Table 18. Green Ethernet local device information

Field	Description
Cumulative Energy Saved on this port due to Green mode(s) (Watts * Hours)	The cumulative energy saved on the port because of the green modes that are enabled on the port in watts * hours.
Energy Detect Operational Status	The operational state (Active or Inactive) of the Energy Detect mode.
Reason	The reason for the operational state that is displayed in the previous field.
Rx Low Power Idle Event Count	The total number of times that the port entered the low-power idle (LPI) state since the EEE counters were reset.
Rx Low Power Idle Duration (uSec)	The total period (in 10 us increments) that the port remained in the LPI state since the EEE counters were reset.
Tx Low Power Idle Event Count	The total number of times that the link partner of the port entered the LPI state since the EEE counters were reset.
Tx Low Power Idle Duration (uSec)	The total period (in 10 us increments) that the link partner of the port remained in the LPI state since the EEE counters were reset.
Tw_sys_tx (uSec)	The value of ‘Tw_sys’ that the port can support.
Tw_sys_tx Echo (uSec)	The link partner’s ‘transmit Tw_sys’ that the port uses to compute the ‘Tw_sys’ that it requests from its link partner.

Table 18. Green Ethernet local device information (continued)

Field	Description
Tw_sys_rx (uSec)	The value of 'Tw_sys' that the port requested from its link partner.
Tw_sys_rx Echo (uSec)	The link partner's 'receive Tw_sys' that the port uses to compute the 'Tw_sys' that it can support.
Fallback Tw_sys (uSec)	The value of the 'fallback Tw_sys' that the port requested from its link partner.
Tx_dll_enabled	The initialization status of the transmit EEE transmit Data Link Layer (DLL) function on the port.
Tx_dll_ready	The transmit DLL status, which indicates if the 'tx system' initialization is complete and if port is ready to receive or update LLDPDUs that contain EEE TLVs.
Rx_dll_enabled	The status of the EEE capability negotiation on the port.
Rx_dll_ready	The receive DLL status, which indicates if the 'rx system' initialization is complete and if port is ready to receive or update LLDPDUs that contain EEE TLVs.
Time Since Counters Last Cleared	The time since the counters were reset.

Display green Ethernet information for the link partner of an interface

The switch can detect green Ethernet information for the link partner of an interface, that is for the remote device.

To display the green Ethernet information for the link partner of an interface:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **System > Management > Green Ethernet > Green Ethernet Detail**.

   The Green Ethernet Detail page displays.

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

The following table describes the view-only fields.

Table 19. Green Ethernet remote device information

Field	Description
Remote ID	The identifier that is assigned to the link partner of the port.
Remote Tw_sys_tx (uSec)	The value of 'Tw_sys' that the link partner can support.
Remote Tw_sys_tx Echo (uSec)	The value of 'transmit Tw_sys' that the link partner returns to the port.
Remote Tw_sys_rx (uSec)	The value of 'Tw_sys' that the link partner requests from the port.
Remote Tw_sys_rx Echo (uSec)	The value of 'receive Tw_sys' that the link partner returns to the port.
Remote Fallback Tw_sys (uSec)	The value of 'fallback Tw_sys' that the link partner returns to the port.

Display the green Ethernet statistics summary

The green Ethernet statistics summary displays information about both the switch and the interfaces.

To display the green Ethernet statistics summary:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The Green Ethernet Statistics Summary page displays.

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

The following table describes the view-only fields in the Green Ethernet Statistics Summary section.

Table 20. Green Ethernet statistics summary information

Field	Description
Current Power Consumption (mW)	The power consumption by all ports on the switch in mWatts (mW).
Percentage Power Saving (%)	The percentage of power saved on all ports on the switch when green Ethernet mode is enabled.
Cumulative Energy Saving (W*H)	The cumulative energy saved on the switch in (watts * hour) when all green features are enabled.

The following table describes the view-only fields in the Green Ethernet Feature Summary section.

Table 21. Green Ethernet feature summary information

Field	Description
Unit	The unit is always 1.
Green Features supported on this unit	The green features that are supported on the switch: • Energy-Detect • EEE (Energy Efficient Ethernet) • LPI-History (EEE low power idle history) • LLDP-Cap-Exchg (EEE LLDP capability exchange) • Pwr-Usg-Est (Power usage estimates).

The following table describes the view-only fields in the Green Ethernet Interface Summary section.

Table 22. Green Ethernet interface summary information

Field	Description
Interface	The interface for which information is displayed.
Energy Detect Admin Mode	Indicates the status of the mode (Enable or Disable). If the mode is enabled and 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.
Energy Detect Operational Status	The operational state (Active or Inactive) of the Energy Detect mode.
EEE Admin mode	Indicates the status of the mode (Enable or Disable). If this mode is enabled, the port transitions to low power mode during a link idle condition.

Configure and display the green Ethernet EEE LPI history for an interface

You can configure and display the green Ethernet EEE low-power idle (LPI) history for an interface.

To configure and display the green Ethernet EEE LPI history for an interface:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.

6. Select **System > Management > Green Ethernet > Green Ethernet LPI History**.

   The Green Ethernet LPI History page displays.
7. From the **Interface** menu, select the interface.
8. In the **Sampling Interval** field, enter the interval at which EEE LPI data is collected.

   The range is from 30 to 36000 seconds.The default is 3600 seconds.
9. In the **Max Samples To Keep** field, enter the maximum number of samples to keep.

   The range is from 1 to 168.The default is 168.
10. Click the **Apply** button.

    Your settings are saved.

    The Percentage LPI time field displays the time that the interface was in LPI mode since the EEE counters were reset.
11. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields.

Table 23. Interface green mode EEE LPI history information

Field	Description
Sample No.	The sample index.
Time Since The Sample Was Recorded	The period that past since the sample was recorded.
Percentage Time spent in LPI mode since last sample	The percentage of time that the interface was in LPI mode since the last sample was recorded.
Percentage Time spent in LPI mode since last reset	The percentage of time that the interface was in LPI mode since the EEE counters were reset.

Use the Device View

For information about the device view, see Use the Device View of the device UI on page 31.

Configure Power over Ethernet

You can configure the global Power over Ethernet (PoE) configuration settings and the PoE settings for each port.

PoE concepts

The switch can provide up to 190W of PoE+ power. By default, supplied power is prioritized in ascending port order, up to the total power budget of the switch. If the power requirements for the attached devices exceed the total power budget of the switch, the power to the device on the highest-numbered PoE+ port is disabled to make sure that the devices connected to the higher-priority, lower-numbered PoE+ ports are supported first.

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

Device class power requirements

PoE and PoE+ use Ethernet cables to supply power to PoE-capable devices on the network, such as WiFi access points, IP cameras, VoIP phones, and switches. The switch is compliant with the IEEE 802.3at standard (PoE+) and backward compatible with the IEEE 802.3af standard (PoE). The switch can pass power through to any powered device (PD) that supports these standards. PoE and PoE+ let you power such devices without the need for a separate power supply.

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

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

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

Table 24. PoE and PoE+ device class power allocation

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

Table 24. PoE and PoE+ device class power allocation (continued)

Device Class	Standard	Range of Power Delivered to the Powered Device	Minimum Output at PoE Switch Port (Minimum Allocated)	Maximum Output at PoE Switch Port (Maximum Allocated)
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 79.)

An example:
Port 1 delivers 4.4W to a PD. The available power budget is 185.6W (190W–4.4W).

Another example:
A Class 4 PD is attached to Port 1, a Class 2 PD to Port 2, and another Class 4 PD to Port 3. However, the PDs consume less power than defined by their classes: The PD attached to Port 1 consumes 7.3W, the PD attached to Port 2 consumes 4.7W, and the PD attached to Port 3 consumes 8.9W. So even though the switch provides power to two Class 4 devices and one Class 3 device, if the default power adapter is installed, the available power budget is 169.1W (190W–7.3–4.7–8.9W).

To determine the delivered power by a PoE+ port:

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

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > PoE > Advanced > PoE Port Configuration**.

   The PoE Port Configuration page displays.

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

Configure the global PoE settings

To configure the global PoE settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > PoE > Basic > PoE Configuration**.

   The PoE Configuration page displays.

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

   Selecting the Traps **Disable** radio button deactivates the PoE traps. The default setting is Enable.
10. Click the **Apply** button.

    Your settings are saved.

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

Table 25. PoE Configuration fields

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

Configure the PoE port settings

To configure the PoE port settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > PoE > Advanced > PoE Port Configuration**.

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

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 is specified in the **Power Limit (W)** 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. In the **Power Limit (W)** field, enter the maximum power (in W) that the port can deliver.

    The range is 3–30 W. The default is 30 W.

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.
    - **4pt 802.3af + Legacy**. The port performs a 4-point resistive detection, and if required, continues with legacy detection.
    - **Legacy.** The port performs legacy detection.
14. From the **Timer Schedule** menu, select a timer schedule or select **None**, which is the default selection.

    For information about setting up and configuring PoE timer schedules, see Set up PoE timer schedules on page 132.

15. Click the **Apply** button.

    Your settings are saved.

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

Table 26. PoE Port Configuration

Field	Description
High Power	All ports supports high power mode.
Max Power (W)	The maximum power in Watts that can be provided by the port.

Table 26. PoE Port Configuration (continued)

Field	Description
Class	The class defines the range of power that a powered device (PD) is drawing from the switch. The class definitions are as follows: • **0**: 0.44–16.2W • **1**: 0.44–4.2W • **2**: 0.44–7.4W • **3**: 0.44–16.2W • **4**: 0.44–31.6W • **Unknown**. The class cannot be detected, or no PD is attached to the port.
Output Voltage (Volts)	The voltage that is delivered to the PD in volts.
Output Current (mA)	The current that is delivered to the PD in mA.
Output Power (W)	The power that is delivered to the PD in W.
Status	The operational status of the port. The possible values are as follows: • **Disabled**. No power is delivered. • **Delivering Power**. Power is being drawn by the PD. • **Requesting Power**. The port is requesting power. • **Fault**. A problem occurred with the power. • **Searching**. The port is not in one of the other states in this list.
Fault Status	The error description when the PoE port is in a fault state. The possible values are as follows: • **No Error**. The port is not in any error state and can provide power. • **MPS Absent**. The port detected the absence of the main power supply, preventing the port from providing power. • **Short**. The port detected a short circuit condition, preventing the port from providing power. • **Overload**. The PD that is connected to the port attempts to draw more power than allowed by the port's settings, preventing the port from providing power at all. • **Power Denied**. The port was denied power because of a shortage of power or because of an administrative condition. In this condition, the port does not provide power. • **Startup Failure**. The PD that is connected to the port failed to start up. In this condition, the port does not provide power. • **Over Voltage**. The port was denied power because of a over-voltage lockout. • **Under Voltage**. The port was denied power because of an under-voltage lockout. • **Thermal Shutdown**. The port detected a thermal temperature fault, preventing the port from providing power.

Configure SNMP

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

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

Configure the SNMPv1 and SNMPv2 community

Only the communities that you define can access the switch using the SNMPv1 and SNMPv2 protocols. Only those communities with read/write level access can be used to change the configuration using SNMP.

Add an SNMP community:

To add an SNMP community:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

   The Community Configuration page displays.
7. In the **Management Station IP** field, specify the IP address of the management station.

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

   Together, the management station IP and the management station IP mask denote a range of IP addresses from which SNMP clients can use that community to access this device. If either the management station IP or management station IP mask value is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's address is ANDed with the mask, as is the management station IP address. If the values are equal, access is allowed. For example, if the management station IP and management station IP mask settings are 192.168.1.0/255.255.255.0, then any client whose address is 192.168.1.0 through 192.168.1.255 (inclusive) is allowed access. To allow access from only one station, use a management station IP mask value of 255.255.255.255, and use that machine's IP address for client address.

9. In the **Community String** field, specify a community name.
10. From the **Access Mode** menu, select the access level for this community, which is either **ReadWrite** or **ReadOnly**.
11. From the **Status** menu, select to enable or disable the community.

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

12. Click the **Add** button.

    The selected community is added.

Modify an existing SNMP community

To modify an existing SNMP community:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

The System Information page displays.

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

   The Community Configuration page displays.

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

   Your settings are saved.

Delete an SNMP community

To delete an SNMP community:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The Community Configuration page displays.

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

   The community is removed.

Configure SNMPv1 and SNMPv2 trap settings

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

Add an SNMP trap receiver

To add an SNMP trap receiver:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

   The Trap Configuration page displays.
7. In the **Recipients IP** field, enter the IPv4 address in the x.x.x.x format to receive SNMP traps from this device.
8. From the **Version** menu, select the trap version to be used by the SNMP trap receiver:
   - **SNMP V1**. The switch uses SNMPv1 to send traps to the receiver. The default setting is SNMP V1.
   - **SNMP V2**. The switch uses SNMPv2 to send traps to the receiver.
9. In the **Community String** field, specify the name of the SNMP community that includes the SNMP management host and the SNMP agent on the device.

   This name can be up to 16 characters and is case-sensitive.
10. Click the **Add** button.

    The receiver configuration is added.

Modify information about an existing SNMP trap recipient

To modify information about an existing SNMP trap recipient:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

   The Trap Configuration page displays.
7. Select the check box next to the recipient.
8. Update the desired fields.
9. Click the **Apply** button.

   Your settings are saved.

Delete an SNMP trap recipient

To delete an SNMP trap recipient:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

   The Trap Configuration page displays.
7. Select the check box next to the recipient to remove.
8. Click the **Delete** button.

   The trap recipient is removed.

Configure SNMPv1 and SNMPv2 trap flags

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

To configure the trap flags:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.

6. Select **System > SNMP > SNMP V1/V2 > Trap Flags**.

   The Trap Flags page displays.

7. Enable or disable the following system traps:
   - **Authentication**. When enabled, SNMP traps are sent when events involving authentication occur, such as when a user attempts to access the device management interface and fails to provide a valid user name and password. The default is Enable.
   - **Link Up/Down**. When enabled, SNMP traps are sent when the administrative or operational state of a physical or logical link changes. The default is Enable.
   - **Spanning Tree**. When enabled, SNMP traps are sent when various spanning tree events occur. The default is Enable.
   - **ACL**. When enabled, SNMP traps are sent when an ACL is triggered. The default is Disable.
   - **PoE**. When enabled, SNMP traps are sent when a PoE event occurs. The default is Enable.
8. Click the **Apply** button.

   Your settings are saved.

View the supported MIBs

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

To view the supported MIBs:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

The System Information page displays.

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

   The Supported MIBs page displays.

The following table describes the view-only MIB status fields.

Table 27. SNMP supported MIBs

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

Configure SNMPv3 users

You can manage SNMPv3 user accounts and set up authentication and encryption.

Add an SNMPv3 user

By default, the admin user is an SNMPv3 user with read/write access.

To add an SNMPv3 user:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The User Configuration page displays.

7. In the **User Name** field, type a name for the user account.

   The name can up be up to characters.

8. From the **SNMP v3 Access Mode** menu, select **Read-Only** or **Read/Write** to specify the SNMPv3 access privileges for the user account.

   The SNMPv3 access privileges for the admin account are Read/Write.

   Note: The only option from the Authentication Protocol menu is SHA512. This is the default.

9. Specify an authentication password (key) in the **Authentication Key** field.

   The password can be up to 32 characters.

10. From the **Encryption Protocol** menu, select **None** or **AES128** for the encryption:
    - **None**: The information is not encrypted.
    - **AES128**: The information is encrypted and you must specify an encryption password for SNMPv3 access (see the following step).

11. If you select **AES128** from the **Encryption Protocol** menu, specify an encryption password (key) in the **Encryption Key** field.

    The password can be up to 32 characters.

12. Click the **Add** button.

    The SNMPv3 user is added.

Modify an SNMPv3 user

To modify information about an existing SNMPv3 user:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

The System Information page displays.

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

   The User Configuration page displays.

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

   Your settings are saved.

Delete an SNMPv3 user

To delete an SNMPv3 user:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The User Configuration page displays.

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

   The SBNPv3 user is removed.

Configure Link Layer Discovery Protocol

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

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

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

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

Configure LLDP global settings

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

To configure global LLDP settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The LLDP Configuration page displays.

7. In the **TLV Advertised Interval** field, enter the interval in seconds to transmit LLDP frames.

   The range is from 5 to 32768 secs. The default is 30 seconds.

8. 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.

9. In the **Reinitialization Delay** field, enter the delay before reinitialization starts.

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

10. In the **Transmit Delay** field, enter the number of seconds to wait between transmissions of remote data change notifications to one or more SNMP trap receivers configured on the switch.

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

11. in the **Fast Start Duration** field, enter a value for LLDP-MED.

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

    The range is from 1 to 10 times. The default is 3 times.

12. Click the **Apply** button.

    Your settings are saved.

Configure LLDP port settings

You can specify LLDP settings for a port.

To configure LLDP settings for a port:

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

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

2. Launch a web browser.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The LLDP Port Settings page displays.

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

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

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

     The default is Auto Advertise.

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

  For information about how to configure the system name, see View or define system information on page 37. For information about how to configure the port description, see Configure the port settings and maximum frame size on page 141.

9. Click the **Apply** button.

   Your settings are saved.

View the LLDP-MED network policy

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

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

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The LLDP-MED Network Policy page displays.

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

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

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

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

Table 28. LLDP-MED network policy information

Field	Description
Network Policy Number	The policy number.
Application	The media application type associated with the policy, which can be one of the following: • Unknown • Voice • Guest Voice • Guest Voice Signaling • Softphone Voice • Video Conferencing • Streaming Video • Video Signaling A port can receive multiple application types. The application information is displayed only if a network policy TLV was transmitted from the port.
VLAN ID	The VLAN ID associated with the policy.
VLAN Type	Indicates whether the VLAN associated with the policy is tagged or untagged.
User Priority	The priority associated with the policy.
DSCP	The DSCP associated with a particular policy type.

Configure the LLDP-MED port settings

You can enable LLDP-MED mode on a port and configure its properties.

To configure LLDP-MED settings for a port:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

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

   Your settings are saved.

Display the LLDP-MED neighbors information

You can display LLDP-MED neighbors device information, which is information that the device that is connected to an interface advertises.

To display the LLDP-MED neighbors device information:

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > LLDP > LLDP-MED Neighbors Information**.

   The LLDP-MED Neighbors Information page displays.
7. From the **Interface** menu, select an interface on which the reception of LLDP-MED frames is enabled.

   The Remote ID field displays the ID that is assigned to the remote device.
8. To refresh the page, click the **Refresh** button.

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

Table 29. LLDP-MED neighbors information

Field	Description
Capability Information Displays the supported capabilities that are received in LLDP-MED frames.	
Supported Capabilities	The system capabilities that are supported on the remote device.
Enabled Capabilities	The system capabilities that are enabled on the remote device.
Device Class	The device class that is advertised by the remote device. The device class can be Generic, Media, Communication, or Network Connectivity.

Table 29. LLDP-MED neighbors information (continued)

Field	Description
Network Policies Information Displays the network policies information that is received in LLDP-MED frames.	
Media Application Type	The application type of the remote device, 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, priority, DSCP, tagged bit status, and unknown bit status. 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 remote device.
Priority	The priority of the remote device.
DSCP	The DSCP of the remote device.
Unknown Bit Status	The unknown bit status of the remote device.
Tagged Bit Status	The tagged bit status of the remote device.
Inventory Information Displays the inventory information that is received in LLDP-MED frames.	
Hardware Revision	The hardware version of the remote device.
Firmware Revision	The firmware version of the remote device.
Software Revision	The software version of the remote device.
Serial Number	The serial number of the remote device.
Manufacturer Name	The manufacturers name of the remote device.
Model Name	The model name of the remote device.
Asset ID	The asset ID of the remote device.
Location Information Displays the location information that is received in LLDP-MED frames.	
Sub Type	The type of location information of the remote device.
Location Information	The location information of the remote device.

Table 29. LLDP-MED neighbors information (continued)

Field	Description
Extended PoE Displays if extended PoE information is received in LLDP-MED frames.	
Device Type	The PoE device type of the remote device.
Extended PoE PSE Displays if extended PoE Power Sourcing Equipment (PSE) information is received in LLDP-MED frames.	
Device Type	The type of PoE device that remote device is.
Power Source	The type of power source of that the remote device.
Power Priority	The type of power priority on the remote device.
Power Value	The power in watts that the remote device transmits, that is, the information is transmitted, not the actual power.
Extended PoE PD Displays if extended PoE Powered Device (PD information is received in LLDP-MED frames.	
Device Type	The type of PoE device that remote device is.
Power Source	The type of power source of that the remote device.
Power Priority	The type of power priority on the remote device.
Power Value	The power in watts that the remote device transmits, that is, the information is transmitted, not the actual power.

View the local information advertised through LLDP

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

To view the local LLDP information:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The Local Information page displays.

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

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

Field	Description
Device Information	
Chassis ID Subtype	The type of information used to identify the switch in the Chassis ID field.
Chassis ID	The hardware platform identifier for the switch.
System Name	The user-configured system name for the switch.
System Description	The switch description, which includes information about the product model and platform.
System Capabilities	The primary functions that the switch supports.
Port Information	
Interface	The interface associated with the rest of the data in the row.
Port ID Subtype	The type of information used to identify the interface in the Port ID field.
Port ID	The port number.
Port Description	The user-defined description of the port. For information about how to configure the port description, see Configure the port settings and maximum frame size on page 141.
Advertisement	The TLV advertisement status of the port.

8. To view additional details about a port, click the name of the port in the Interface column of the Port Information table.

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

Field	Description
Managed Address	
Address SubType	The type of address that the management interface (which includes the device UI) uses, such as an IPv4 address.

Field	Description
Address	The address used to manage the device.
Interface SubType	The port subtype.
Interface Number	The number that identifies the port.
MAC/PHY Details	
Auto Negotiation Supported	Indicates whether the interface supports port speed autonegotiation. The possible values are True and False.
Auto Negotiation Enabled	The port speed autonegotiation support status. The possible values are True (enabled) or False (disabled).
Auto Negotiation Advertised Capabilities	The port speed autonegotiation capabilities such as 1000BASE-T half-duplex mode or 100BASE-TX full-duplex mode.
Operational MAU Type	The Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interface collision detection and bit injection into the network.
MED Details	
Capabilities Supported	The MED capabilities enabled on the port.
Current Capabilities	The TLVs advertised by the port.
Device Class	Network Connectivity indicates that the device is a network connectivity device.
Network Policies	
Application Type	The media application type associated with the policy.
VLAN ID	The VLAN ID associated with the policy.
VLAN Type	Specifies whether the VLAN associated with the policy is tagged or untagged.
User Priority	The priority associated with the policy.
DSCP	The DSCP associated with a particular policy type.

View the LLDP neighbors information

You can view the data that a specific port received from other LLDP-enabled systems.

To view the LLDP information received from a neighbor device:

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Advanced > LLDP > Neighbor Information**.

   The Neighbor Information page displays.
7. To refresh the page, click the **Refresh** button.

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

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

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

8. To view additional information about the remote device, click the link in the MSAP Entry column.

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

The following table describes the information transmitted by the neighbor.

Field	Description
Port Details	
Local Port	The interface on the local system that received LLDP information from a remote system.
MSAP Entry	The Media Service Access Point (MSAP) entry number for the remote device.
Basic Details	
Chassis ID Subtype	The type of data displayed in the Chassis ID field on the remote system.
Chassis ID	The remote 802 LAN device's chassis.
Port ID Subtype	The type of data displayed in the remote system's Port ID field.
Port ID	The physical address of the port on the remote system from which the data was sent.
Port Description	The user-defined description of the port.
System Name	The system name associated with the remote device.
System Description	The description of the selected port associated with the remote system.
System Capabilities	The system capabilities of the remote system.
Managed Addresses	
Address SubType	The type of the management address.
Address	The advertised management address of the remote system.
Interface SubType	The port subtype.
Interface Number	The port on the remote device that sent the information.
MAC/PHY Details	
Auto-Negotiation Supported	Specifies whether the remote device supports port-speed autonegotiation. The possible values are N/A, True, and False.
Auto-Negotiation Enabled	The port speed autonegotiation support status. The possible values are N/A, True, and False.
Auto Negotiation Advertised Capabilities	The port speed autonegotiation capabilities. N/A, True, and False.
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. N/A, True, and False.
MED Details	
Capabilities Supported	The supported capabilities that were received in MED TLV from the device.
Current Capabilities	The advertised capabilities that were received in MED TLV from the device.

Field	Description
Device Class	The LLDP-MED endpoint device class. The possible device classes are as follows: • Endpoint Class 1 Indicates a generic endpoint class, offering basic LLDP services. • Endpoint Class 2 Indicates a media endpoint class, offering media streaming capabilities as well as all Class 1 features. • Endpoint Class 3 Indicates a communications device class, offering all Class 1 and Class 2 features plus location, 911, Layer 2 switch support, and device information management capabilities.
PoE Device Type	The type of PoE 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 advertised by the remote device.
Firmware Revision	The firmware version advertised by the remote device.
Software Revision	The software version advertised by the remote device.
Serial Number	The serial number advertised by the remote device.
Model Name	The model name advertised by the remote device.
Asset ID	The asset ID advertised by the remote device.
Location Information	
Civic	The physical location, such as the street address, that the remote device advertised in the location TLV, for example, 123 45th St. E. The field value length range is 6–160 characters.
Coordinates	The location map coordinates that the remote device advertised in the location TLV, including latitude, longitude, and altitude.
ECS ELIN	The Emergency Call Service (ECS) Emergency Location Identification Number (ELIN) that the remote device advertised in the location TLV. The field range is 10–25.
Unknown	The unknown location information for the remote device.
Network Policies	
Application Type	The media application type associated with the policy advertised by the remote device.
VLAN ID	The VLAN ID associated with the policy.
VLAN Type	Specifies whether the VLAN associated with the policy is tagged or untagged.
User Priority	The priority associated with the policy.
DSCP	The DSCP associated with a particular policy type.

Field	Description
LLDP Unknown TLVs	
Type	The unknown TLV type field.
Value	The unknown TLV value field.

Configure a DHCP L2 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 Layer 3 relay agent. In some network configurations, Layer 2 (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.

Enable the DHCP L2 relay

You can enable the DHCP L2 relay.

To enable the DHCP L2 relay:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Global Configuration**.

   The DHCP L2 Relay Global Configuration page displays.

7. Select the **Enable** radio button

   The default admin mode is disabled.

8. In the DHCP L2 Relay VLAN Configuration section, configure the following settings:
   - **VLAN ID**: The ID of the VLAN that is already configured on the switch.

     You cannot use this page to add a VLAN. For information about adding VLANs, see Configure VLANs on page 149.
   - **Admin mode**: Enable or disable the DHCP L2 relay on the VLAN.
   - **Circuit ID mode**: Enable or disable the circuit ID suboption of DHCP Option-82.
   - **Remote ID String**: Specify the remote ID if the Remote ID option is enabled.

9. Click the **Apply** button.

   Your settings are saved.

Configure a DHCP L2 relay interface

You can configure a DHCP L2 relay interface.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration**.

   The DHCP L2 Relay Configuration page displays.

7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. From the **Admin Mode** menu, select to enable or disable the DHCP L2 relay on the selected interface.

   The default is Disable.

10. From the **82 Option Trust Mode** menu, select to enable or disable an interface to be trusted for DHCP L2 Relay (Option-82) received.

    The default is Disable.

11. Click the **Apply** button.

    Your settings are saved.

View DHCP L2 relay interface statistics

You can view DHCP L2 relay interface statistics.

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Statistics**.

   The DHCP L2 Relay Interface Statistics page displays.
7. Select whether to display physical interfaces, LAGs, VLANs, or al by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Physical interfaces, VLANs, and LAGs are displayed.

   The following table describes the view-only data that is displayed.

Field	Description
Interface	The interface from which the DHCP message is received.
Untrusted Server Messages With Opt82	The number of DHCP message with option82 received from an untrusted server.
Untrusted Client Messages With Opt82	The number of DHCP message with option82 received from an untrusted client.
Trusted Server Messages Without Opt82	The number of DHCP message without option82 received from a trusted server.
Trusted Client Messages Without Opt82	The number of DHCP message without option82 received from a trusted client.

8. Click the **Refresh** button to refresh the page with the latest information about the switch.
9. Click the **Clear** button to reset the statistics.

Configure DHCP snooping

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

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

Configure the global DHCP snooping settings

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

To configure the global DHCP snooping settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

   The DHCP Snooping Global Configuration page displays.

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

   By default, the Disable radio button is selected.

8. To enable the verification of the sender's MAC address for DHCP snooping, select the MAC Address Validation **Enable** radio button.

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

   By default, the Enable radio button is selected.

9. Click the **Apply** button.

   Your settings are saved.

Enable DHCP for all member interfaces of a VLAN

To enable DHCP snooping for all member interfaces of a VLAN:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The DHCP Snooping Global Configuration page displays.

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

   Your settings are saved.

Configure DHCP snooping interface settings

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

To configure DHCP snooping interface settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Services > DHCP Snooping > Interface Configuration**.

   The DHCP Snooping Interface Configuration page displays
7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.

9. From the **Trust Mode** menu, select the desired trust mode:
   - **Disable**. The interface is considered to be untrusted and could potentially be used to launch a network attack. DHCP server messages are checked against the bindings database. On untrusted ports, DHCP snooping enforces the following security rules:
     - DHCP packets from a DHCP server (DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) are dropped.
     - DHCPRELEASE and DHCPDECLINE messages are dropped if the MAC address is in the snooping database but the binding's interface is other than the interface where the message was received.
     - DHCP packets are dropped when the source MAC address does not match the client hardware address if MAC address validation is globally enabled.
   - **Enable**. 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, specify the rate limit value for DHCP snooping purposes.

    If the incoming rate of DHCP packets per second exceeds the configured burst interval per second, the port shuts down. If the rate limit value is None, the burst interval is nonapplicable, and rate limiting is disabled.
12. In the **Burst Interval (secs)** field, specify the burst interval value for rate limiting purposes on this interface.

    If the rate limit is None, the burst interval is nonapplicable.
13. Click the **Apply** button.

    Your settings are saved.

Configure static DHCP bindings

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

Add a static DHCP binding

To configure static DHCP bindings:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Services > DHCP Snooping > Binding Configuration**.

   The Binding Configuration page displays.
7. From the **Interface** menu, select the interface on which the DHCP client is authorized.
8. In the **MAC Address** field, specify 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 the client is authorized to use.
10. In the **IP Address** field, specify the IP address of the client.
11. Click the **Add** button.

    The DHCP snooping binding entry is added to the database.

The Dynamic Binding Configuration table shows information about the DHCP bindings that were learned on each interface on which DHCP snooping is enabled. The following table describes the view-only dynamic bindings information.

Table 30. DHCP Dynamic Configuration information

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

Change a static DHCP binding

You can change an existing static DHCP binding.

To change a static DHCP bindings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Services > DHCP Snooping > Binding Configuration**.

   The Binding Configuration page displays.
7. In the Static Binding Configuration table, select the check box to the left of the binding configuration.
8. Change the settings.
9. Click the **Apply** button.

   Your settings are saved.

Remove a static DHCP binding

You can remove a static binding from the DHCP snooping bindings database.

To change a static DHCP bindings:

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Services > DHCP Snooping > Binding Configuration**.

   The Binding Configuration page displays.
7. In the Static Binding Configuration table, select the check box to the left of the binding configuration.
8. Click the **Delete** button.

   Your settings are saved. The binding is removed.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **System > 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.

7. To clear the dynamic DHCP snooping bindings, clear the **Clear** button.

   The DHCP snooping binding entry is added to the database.

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

The following table describes the view-only dynamic bindings information.

Table 31. DHCP Dynamic Configuration information

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

Configure DHCP snooping persistent settings

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

To configure DHCP snooping persistent settings:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

   The DHCP Snooping Persistent Configuration page displays.
7. Specify where the DHCP snooping bindings database is located.
   - **Local**. The binding table is stored locally on the switch.
   - **Remote**. The binding table is stored on a remote TFTP server.

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

     a. Specify the IP address of the TFTP server.
     b. Specify the file name of the DHCP snooping bindings database in which the bindings are stored.
8. In the **Write Delay** field, specify the time to wait between writing bindings information to persistent storage.

   The delay allows the device 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.
9. Click the **Apply** button.

   Your settings are saved.

View or clear DHCP snooping statistics

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

To view or clear the DHCP snooping statistics:

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Services > DHCP Snooping > Statistics**.

   The DHCP Snooping Statistics page displays.
7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Click the **Clear** button to clear all interfaces statistics.

The following table describes the view-only DHCP snooping statistics.

Table 32. DHCP Snooping Statistics information

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

Configure Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious 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 malicious attacker sends ARP requests or responses mapping another station's IP address to its own MAC address.

When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

When DAI is enabled on a VLAN, DAI is enabled on the interfaces (physical ports or LAGs) that are members of that VLAN. Individual interfaces are configured as trusted or untrusted. The trust configuration for DAI is independent of the trust configuration for DHCP snooping.

Configure the global DAI settings

If you configure the source MAC address validation option, DAI verifies that the sender MAC address in an ARP packet equals the source MAC address in the Ethernet header.
The Ethernet header includes a configurable option to verify that the target MAC address in the ARP packet equals the destination MAC address. This check applies only to ARP responses, since the target MAC address is unspecified in ARP requests. You can also enable IP address checking. When this option is enabled, DAI drops ARP packets with an invalid IP address. The following IP addresses are considered invalid:

- 0.0.0.0
- 255.255.255.255
- All IP multicast addresses
- All class E addresses (240.0.0.0/4)
- Loopback addresses (in the range 127.0.0.0/8)

The valid IP check is applied only on the sender IP address in ARP packets. In ARP response packets, the check is applied only on the target IP address.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Services > Dynamic ARP Inspection > DAI Configuration**.

   The Dynamic ARP Inspection Global Configuration page displays.
7. To let the switch validate the source MAC address in ARP packets, select the Validate Source MAC **Enable** radio button.

   By default, the Disable radio button is selected.
8. To let the switch validate the destination MAC address in ARP packets, select the Validate Destination MAC **Enable** radio button.

   By default, the Disable radio button is selected.
9. To let the switch validate IP addresses in ARP packets, select the Validate IP **Enable** radio button.

   By default, the Disable radio button is selected.
10. Click the **Apply** button.

    Your settings are saved.

    The additional ARP validations are performed on packets received on VLANs that are enabled for DAI and interfaces configured as untrusted.

Configure DAI on a VLAN

An example of DAI on a VLAN:
DAI is enabled on VLAN 1. Ports 1–4 connect end users to the network and are members of VLAN 1. These ports are configured to limit the maximum number of ARP packets with a rate limit of 10 packets per second. LAG 1, which is also a member of VLAN 1 and contains ports 5–6, is the trunk port that connects the switch to a data center, so it is configured as a trusted port.

To configure DAI on a VLAN:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **System > Services > Dynamic ARP Inspection > DAI VLAN Configuration**.

   The VLAN Configuration page displays.

7. In the VLAN ID column, select the check box next to the VLAN.
8. From the **Admin Mode** menu, select one of the following options:
   - Select **Enable** to enable Dynamic ARP inspection on the selected VLAN.
   - Select **Disable** to disable Dynamic ARP inspection on the selected VLAN.

   The default is Disable.

9. From the **Invalid Packets** menu, select one of the following options:
   - Select **Enable** to enable logging the invalid ARP packet information for the selected VLAN.
   - Select **Disable** to disable dynamic ARP inspection logging for the selected VLAN.

   The default is Enable.

10. In the **ARP ACL Name** field, enter the name of an ARP access list (ACL).

    A VLAN can be configured to use an ARP ACL that contains rules as the filter for ARP packet validation. For more information, see Configure a DAI access control list and DAI rules on page 128.

11. From the **Static Flag** menu, select whether ARP packets need validation by using the DHCP snooping database if the ARP ACL rules do not match:
    - Select **Enable** to enable validation of ARP packets by ARP ACL rules only.
    - Select **Disable** to enable validation of ARP packets using DHCP snooping entries.

    The default is Disable.

12. Click the **Apply** button.

    Your settings are saved.

Configure DAI on an interface

This section describes a configuration example.

To configure DAI on LAG1 as a trusted port and rate limiting for ports 1–10:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Services > Dynamic ARP Inspection > DAI Interface Configuration**.

   The DAI Interface Configuration page displays.
7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. From the **Trust Mode** menu, select **Enable** to set the interface to trusted.

The Trust Mode field indicates whether the interface is trusted for dynamic ARP inspection purposes. All interfaces are untrusted by default.

10. In the **Rate Limit (pps)** field, specify the rate limit value for dynamic ARP inspection purposes.

    If the incoming rate of ARP packets per second exceeds the configured burst interval per second, ARP packets are dropped. If this value is None (N/A), no limit exists. The value can be set to –1, which means N/A. The rate limit range is 0–300. The default is 15 packets per second (pps).

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

    If the rate limit is None, the burst interval is also nonapplicable and is displayed as N/A. The burst interval range is 1–15 seconds. The default is 1 second.

12. Click the **Apply** button.

    Your settings are saved.

Configure a DAI access control list and DAI rules

DAI relies on the information in the DHCP snooping bindings database to validate ARP packets. For networks that use static IP addresses and do not use DHCP, DAI access control lists (ACLs) can be used to statically map an IP address to a MAC address on a VLAN. When hosts use static IP addresses, the DHCP snooping feature cannot build a bindings database. DAI ACLs are also useful when other switches in the network do not run DAI.

DAI consults the static mappings configured in the DAI ACLs before it consults the DHCP snooping bindings database; thus 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 ACL, add rules, and associate the DAI ACL with a VLAN

To configure a DAI ACL, add one or more DAI ACL rules, and associate the DAI ACL with a VLAN:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Services > Dynamic ARP Inspection > DAI ACL Configuration**.

   The DAI ACL Configuration page displays.
7. In the **Name** field, specify a name for the ACL.
8. Click the **Add** button.

   The page displays the new ACL.
9. Click the ACL name.

   The ACL name is a hyperlink to the Rules page.
10. From the **ACL Name** menu, select the DAI ACL to configure.
11. In the **Source IP Address** field, specify the IP address of a host.
12. In the **Source MAC Address** field, specify the MAC address of the host that is statically mapped to the IP address specified in the Source IP Address field.
13. Click the **Add** button.

    The rule is added to the table.
14. Repeat Step 11 through Step 13 to add a second rule to the DAI ACL.

    You can add up to 20 static IP address–MAC address mappings to a DAI ACL.
15. To assign the DAI ACL to a VLAN, do the following:
    a. Select **System > Services > Dynamic ARP Inspection > DAI VLAN Configuration**.

       The VLAN Configuration page displays.
    b. Next to a VLAN, select the check box.
    c. In the **ARP ACL Name** field, specify the name of the DAI ACL to associate with the VLAN.
    d. Click the **Apply** button.

       Your settings are saved.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **System > Services > Dynamic ARP Inspection > DAI ACL Rule Configuration**.

   The Rules page displays.
7. From the **ACL Name** menu, select the DAI ACL.
8. In the DAI Rule Table, select the check box for the rule.
9. Click the **Delete** button.

   Your settings are saved. The rule is removed.

Remove a DAI ACL

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.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **System > Services > Dynamic ARP Inspection > DAI ACL Configuration**.

   The DAI ACL Configuration page displays.

7. In the table, select the check box for the ACL.
8. Click the **Delete** button.

   Your settings are saved. The ACL is removed.

View DAI statistics per VLAN

To view DAI statistics per VLAN:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

The System Information page displays.

6. Select **System > Services > Dynamic ARP Inspection > DAI Statistics**.

   The DAI Statistics page displays.

7. To refresh the page, click the **Refresh** button.
8. Click the **Clear** button to clear the DAI statistics.

   The following table describes the view-only DAI statistics information that is displayed.

Field	Description
VLAN	The enabled VLAN ID for which statistics are displayed.
DHCP Drops	The number of ARP packets that were dropped by DAI because no matching DHCP snooping binding entry was found.
DHCP Permits	The number of ARP packets that were forwarded by DAI because a matching DHCP snooping binding was entry found.
ACL Drops	The number of ARP packets that were dropped by DAI because no matching ARP ACL rule was found for this VLAN and the static flag is set on this VLAN.
ACL Permits	The number of ARP packets that were permitted by DAI because a matching ARP ACL rule was found for this VLAN.
Bad Source MAC	The number of ARP packets that were dropped by DAI as the sender MAC address in the ARP packet did not match the source MAC in the Ethernet header.
Bad Dest MAC	The number of ARP packets that were dropped by DAI as the target MAC address in the ARP reply packet did not match the destination MAC in the Ethernet header.
Invalid IP	The number of ARP packets that were dropped by DAI as the sender IP address in the ARP packet, or target IP address in the ARP reply packet, is not valid. 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.

Set up PoE timer schedules

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

After you create a timer schedule, you can associate it with one or more PoE ports (see Configure the PoE port settings on page 82). You can use a separate timer schedule for each PoE port.

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

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

Create a PoE timer schedule

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

To create a PoE timer schedule:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

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

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

Specify the settings for an absolute PoE timer schedule

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

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

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The Timer Schedule Configuration page displays.

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

      You can select only names of schedules that you created (see Create a PoE timer schedule on page 133).

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

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

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

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

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

   b. In the **Time End** field, enter the time of day in the HH:MM format to specify when the timer schedule must stop.
   c. Next to the **Date Start** field, click the calendar icon and use the menus in the pop-up window to enter the date in the DD-Mon-YYYY format to specify when the timer schedule must start.
   d. Next to the **Date End** field, click the calendar icon and use the menus in the pop-up window to enter the date in the DD-Mon-YYYY format to specify when the timer schedule must stop.
9. Click the **Add** button.

   The entry for the timer schedule is added.

Specify the settings for a recurring PoE timer schedule

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

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

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

   The Timer Schedule Configuration page displays.

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

      You can select only names of schedules that you created (see Create a PoE timer schedule on page 133).

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

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

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

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

8. In the Timer Schedule Configuration section, specify the recurrence pattern:
   a. In the **Time Start** field, enter the time of day in the HH:MM format to specify when the timer schedule must start.
   b. In the **Time End** field, enter the time of day in the HH:MM format to specify when the timer schedule must stop.
   c. Next to the **Date Start** field, click the calendar icon and use the menus in the pop-up window to enter the date in the DD-Mon-YYYY format to specify when the timer schedule must start.
   d. Either select the **No End Date** radio button or select the **End Date** radio button, and next to the **End Date** field, click the calendar icon and use the menus in the pop-up window to enter the date in the DD-Mon-YYYY format to specify when the timer schedule must stop.
   e. From the **Recurrence Pattern** menu, select the pattern:
      - **Daily**. The timer schedule works with daily recurrence. The fields adjust.

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

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

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

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

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

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

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

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

9. Click the **Add** button.

   The entry for the timer schedule is added.

Change the settings for a recurring PoE timer schedule entry

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

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

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The Timer Schedule Configuration page displays.

7. From the **Timer Schedule Name** menu, select the schedule name.
8. From the **Timer Schedule Type** menu, select the schedule type.
9. From the **Timer Schedule Entry** menu, select the schedule entry.
10. Make the changes to the schedule entry.

    For more information, see Specify the settings for a recurring PoE timer schedule on page 135.

11. Click the **Apply** button.

    Your settings are saved.

Delete a PoE timer schedule entry

You can delete a PoE timer schedule entry that you no longer need. The PoE timer schedule itself is not deleted.

To delete a PoE timer schedule entry:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

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

    The entry is deleted.

Delete a PoE timer schedule

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

To delete a PoE timer schedule:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

   The Timer Schedule Name page displays.
7. Select the check box for the schedule that you want to delete.
8. Click the **Delete** button.

   The schedule is deleted.

3

Configure Switching

This chapter contains the following sections:

- Configure the port settings and maximum frame size
- Configure link aggregation groups
- Configure VLANs
- Configure Auto-VoIP
- Configure Spanning Tree Protocol
- Configure multicast
- Manage IGMP snooping
- Manage MLD snooping
- Configure multicast VLAN registration
- View, search, and manage the MAC address table
- Configure Layer 2 loop protection

Configure the port settings and maximum frame size

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

To configure the port settings and maximum frame size:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

   The Port Configuration page displays.
7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.

- To configure all interfaces with the same settings, select the check box in the heading row.

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

   The string can be up to 64 characters in length.

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

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

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

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

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

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

    Possible field values are as follows:

    - **Auto**. All supported speeds.
    - **10**. 10 Mbits/second
    - **100**. 100 Mbits/second
    - **1000**. 1000 Mbits/second

    The delimiter characters for setting different speed values are a comma (,), a period (.) and a space ( ). The default is Auto.

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

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

    Possible values are as follows:

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

    The default is Auto.

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

14. Use the **Link Trap** menu to specify whether or not to send a trap when link status changes.

    The default is Enabled.

15. To set the frame size, in the **Frame Size** field, specify the maximum Ethernet frame size that the interface can support. The frame size includes the Ethernet header, CRC, and payload.

    The range is from 1500 to 9198 bytes. The default maximum frame size is 1500 bytes.

16. 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.
17. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only data that is displayed.

Table 33. Port Configuration information

Field	Description
Port Type	For normal ports this field is blank. Otherwise, the possible values are as follows: • **Mirrored**. The port is a mirrored port on which all the traffic is copied to the probe port. • **Probe**. Use this port to monitor a mirrored port. • **Trunk Member**. The port is a member of a link aggregation trunk. Look at the LAG pages for more information.
Physical Status	The port speed and duplex mode.
Link Status	Indicates whether the link is up or down.
MAC Address	The physical address (MAC address) of the port.
PortList Bit Offset	The bit offset value that corresponds to the port when the MIB object type PortList is used to manage in SNMP.
ifIndex	The ifIndex of the interface table entry associated with this port.

Configure link aggregation groups

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

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

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

The switch supports 16 LAGs.

Configure LAG settings

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

To configure LAG settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > LAG > Basic > LAG Configuration**.

The LAG Configuration page displays.

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

   You can enter any string of up to 15 alphanumeric characters. A valid name must be specified for you to create the LAG.

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

   The description can be up to 64 characters in length.

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

   When the LAG is disabled, no traffic flows and all LACPDUs are dropped, but the links that form the LAG are not released. The default is Enable.

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

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

11. From the **STP Mode** menu, select the Spanning Tree Protocol (STP) administrative mode associated with the LAG. The possible values are as follows:
    - **Disable**. Spanning tree is disabled for this LAG.
    - **Enable**. Spanning tree is enabled for this LAG. Enable is the default.

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

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

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

14. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only information displayed on the page.

Table 34. LAG Configuration information

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

Configure LAG membership

You can select two or more full-duplex Ethernet links to be aggregated together to form a link aggregation group (LAG), which is also known as a port channel. The switch can treat the port channel as a single link.

To configure LAG membership:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > LAG > Basic > LAG Membership**.

   The LAG Membership page displays.
7. From the **LAG ID** menu, select the LAG ID.

8. In the **LAG Name** field, enter the name to be assigned to the LAG.

   You can enter any string of up to 15 alphanumeric characters. A valid name must be specified for you to create the LAG.

9. In the Ports table, click each port that you want to include as a member of the selected LAG.

   A selected port is displayed by a check mark.

10. Click the **Apply** button.

    Your settings are saved.

Set the LACP switch priority

You can configure the LACP priority value for the switch.

To configure LACP port priority settings:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The LACP Configuration page displays.

7. In the **LACP System Priority** field, specify the LACP priority value for the switch.

   This value specifies the device's link aggregation priority relative to the devices at the other ends of the links on which link aggregation is enabled. A higher value indicates a lower priority. The range is 1 to 65535. The default value is 32768.

8. Click the **Apply** button.

   Your settings are saved.

Set the LACP port priority settings

You can configure the LACP priority value and administrative LACP time-out value for a port.

To configure LACP port priority settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

   The LACP Port Priority page displays.
7. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the interface, or type the interface number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
8. In the **LACP Priority** field, specify the LACP priority value for the selected interfaces.

   This value specifies the device's link aggregation priority relative to the devices at the other ends of the links on which link aggregation is enabled. A higher value indicates a lower priority. The range is 1 to 65535. The default value is 128.

9. In the **Timeout** field, configure the administrative LACP time-out value:
   - **Long**. Specifies a long time-out value.
   - **Short**. Specifies a short time-out value.
10. Click the **Apply** button.

    Your settings are saved.

Configure VLANs

Adding virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security, and management of multicast traffic.

By default, all ports on the switch are in the same broadcast domain. VLANs electronically separate ports on the same switch into separate broadcast domains so that broadcast packets are not sent to all the ports on a single switch. When you use a VLAN, users can be grouped by logical function instead of physical location.

Each VLAN in a network is assigned an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station can omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet can either reject it or insert a tag using its default VLAN ID. A given port can handle traffic for more than one VLAN, but it can support only one default VLAN ID.

You can define VLAN groups stored in the VLAN membership table. The switch supports 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:

- **VLAN 1**. The default VLAN of which all ports are members.
- **VLAN 4088**. The default Auto-VoIP VLAN. By default, this VLAN does not include any members but you can manually add members.
- **VLAN 4089**. The Auto-Video VLAN. By default, this VLAN does not include any members but you can manually add members

Configure VLAN settings

Add a VLAN

To add a VLAN:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > VLAN > Basic > VLAN Configuration**.

   The VLAN Configuration page displays.
7. In the **VLAN ID** field, specify the VLAN identifier for the new VLAN.

   The range of the VLAN ID can be from 2 to 4093, excluding 4088 and 4089. (The default VLANs are 1, 4088, and 4089).
8. In the **VLAN Name** field, specify a name for the VLAN.

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

   The **VLAN Type** field displays the type of the VLAN that you are configuring:
   - The type for VLAN ID 1 is always Default.
   - The type for VLAN ID 4088 is always Auto-VoIP.
   - The type for VLAN ID 4089 is always Auto-Video.

   When you create a VLAN on the VLAN Configuration page, by default, the type that is assigned is Static. A VLAN that is created through the GVRP registration process is assigned a type of Dynamic (GVRP). The type that is assigned to an Auto-Video VLAN is Auto-Video.
9. Click the **Add** button.

   The VLAN is added to the switch.
10. Click the **Apply** button.

    Your settings are saved.

Delete a VLAN

To delete a VLAN from the switch:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > VLAN > Basic > VLAN Configuration**.

   The VLAN Configuration page displays.
7. In the **VLAN ID** field, specify the VLAN identifier.

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

   Note: You cannot delete VLANs 1, 4088, and 4089, all of which are predefined.
8. Click the **Delete** button.

   The VLAN is removed.

Reset the VLAN configuration on the switch to the default settings

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

The VLAN default values are as follows:

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

- All ports are configured to an Acceptable Frame Types value of Admit All Frames.
- All ports are configured with ingress filtering disabled.
- All ports are configured to transmit only untagged frames.
- GVRP is disabled on all ports and all dynamic entries are cleared.

To reset the VLAN configuration on the switch to the default settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > VLAN > Basic > VLAN Configuration**.

   The VLAN Configuration page displays.
7. Select the **Reset Configuration** check box.
8. Click the **Apply** button.

   Your settings are saved.

   Your settings are saved. Except for the predefined default VLANs, all VLANs are deleted.

Configure VLAN membership

To configure VLAN membership:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The VLAN Membership page displays.

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

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

10. In the LAG table, click each LAG once, twice, or three times to configure one of the following modes or reset the LAG to the default settings:
    - **T (Tagged)**. Select the LAGs on which all frames transmitted for this VLAN are tagged. The LAGs that are selected are included in the VLAN.
    - **U (Untagged)**. Select the LAGs on which all frames transmitted for this VLAN are untagged. The LAGs that are selected are included in the VLAN.

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

11. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only information displayed on the page.

Table 35. Advanced VLAN membership

Field	Definition
VLAN Name	The name for the VLAN that you selected. It can be up to 32 alphanumeric characters long, including blanks. VLAN ID 1 always uses the name Default.
VLAN Type	The VLAN type: • **Default** (VLAN ID = 1). Always present. • **Auto-VoIP** (VLAN ID = 4088). Always present. • **Auto-VIdeo** (VLAN ID = 4089). Always present. • **Static**. A VLAN that you configured. • **Dynamic**. A VLAN created by GVRP registration that you did not convert to static, and that GVRP can therefore remove.

View the VLAN status

You can view the status of all currently configured VLANs.

To view the VLAN status:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > VLAN > Advanced > VLAN Status**.

The VLAN Status page displays.

The following table describes the view-only information displayed on the page.

Table 36. VLAN status

Field	Definition
VLAN ID	The VLAN identifier (VID) of the VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	The name of the VLAN. VLAN ID 1 is always named Default.
VLAN Type	The VLAN type: • **Default** (VLAN ID = 1). Always present. • **Auto-VoIP** (VLAN ID = 4088). Always present. • **Auto-Video** (VLAN ID = 4089). Always present. • **Static**. A VLAN that you configured. • **Dynamic**. A VLAN created by GVRP registration that you did not convert to static, and that GVRP can therefore remove.
Routing Interface	The interface associated with the VLAN, in the case that VLAN routing is configured for this VLAN.
Member Ports	The ports that are included in the VLAN.

Configure the PVID settings

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

- You must define a PVID for all ports.
- If no other value is specified, the default VLAN PVID is used.
- To change the port's default PVID, you must first create a VLAN that includes the port as a member (see Configure VLAN membership on page 152).

To configure the PVID settings:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

   The PVID Configuration page displays.
7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. In the **PVID** field, specify the VLAN ID to assign to untagged or priority-tagged frames received on this port.

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

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

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

    The options are **Admit All**, **VLAN only**, **Admitted Untagged Only**:
    - **Admit All**. Untagged frames or priority-tagged frames received on the port are accepted and assigned the value of the port VLAN ID for this port. VLAN-tagged

frames are forwarded in accordance to the 802.1Q VLAN specification. This is the default setting.

- **VLAN only**. Untagged frames or priority-tagged frames received on the port are discarded.
- **Admitted Untagged Only**. Untagged frames are accepted on the port. Priority-tagged frames received on the port are discarded.

13. From the **Ingress Filtering** menu, select one of the following options:
    - **Enable**. The frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the port VLAN ID specified for the port that received this frame.
    - **Disable**. All frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The default is Disable.
14. In the **Port Priority** field, specify the default 802.1p priority assigned to untagged packets arriving at the port.

    You can enter a number from 0 to 7.
15. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only fields.

Table 37. View-only fields on the PVID Configuration page

Field	Description
Current Ingress Filtering	Indicates whether ingress filtering is enabled for the interface.
Untagged VLANs	The number of untagged VLANs for the interface.
Tagged VLANs	The number of tagged VLANs for the interface.
Forbidden VLANs	The number of forbidden VLANs for the interface.
Dynamic VLANs	The number of dynamically added VLANs for the interface.

Configure a MAC-based VLAN

The MAC-Based VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the source MAC address of the packet.

You define a MAC-to-VLAN mapping by configuring an entry in the MAC-to-VLAN table. An entry is specified through a source MAC address and the desired VLAN ID. The MAC-to-VLAN configurations are shared across all ports of the device (that is, a system-wide table exists with MAC address–to–VLAN ID mappings).

When untagged or priority-tagged packets arrive at the switch and entries exist in the MAC-to-VLAN table, the source MAC address of the packet is looked up. If an entry is found, the corresponding VLAN ID is assigned to the packet. If the packet is already priority tagged

it maintains this value. Otherwise, the priority is set to zero. The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues. Otherwise, the packet is dropped. This implies that the user is allowed to configure a MAC address mapping to a VLAN that was not created on the system.

Add a MAC-based VLAN

To add a MAC-based VLAN:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > VLAN > Advanced > MAC Based VLAN**.

   The MAC Based VLAN Configuration page displays.
7. In the **MAC Address** field, enter a valid MAC address that must be bound to a VLAN ID.
8. In the **VLAN ID** field, specify a VLAN ID in the range of 1 to 4093.
9. Click the **Add** button.

   The MAC address is added to the VLAN mapping.

Delete a MAC address from VLAN mapping

To delete a MAC address from VLAN mapping:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > VLAN > Advanced > MAC Based VLAN**.

   The MAC Based VLAN Configuration page displays.

7. In the table, select the check box for the MAC address.
8. Click the **Delete** button.

   The MAC address is removed from the VLAN mapping.

Configure protocol-based VLAN groups

You can use a protocol-based VLAN to define filtering criteria for untagged packets. By default, if you do not configure any port-based (IEEE 802.1Q) or protocol-based VLANs, untagged packets are assigned to VLAN 1. You can override this behavior by defining either port-based VLANs or protocol-based VLANs, or both. Tagged packets are always handled according to the IEEE 802.1Q standard and are not included in protocol-based VLANs.

If you assign a port to a protocol-based VLAN for a specific protocol, untagged frames received on that port for that protocol are assigned the protocol-based VLAN ID. Untagged frames received on the port for other protocols are assigned the port VLAN ID, either the default PVID (1) or a PVID you specifically assigned to the port using the Port VLAN Configuration page.

You define a protocol-based VLAN by creating a group. Each group forms a one-to-one relationship with a VLAN ID, can include one to three protocol definitions, and can include multiple ports. When you create a group, you specify a name and 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The Protocol Based VLAN Group Configuration page displays.

7. In the **Group ID** field, type an identifier for the new group.

   You can enter a number 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, enter one or more protocols that must be associated with the group.

   You can enter keywords such as arp, ip, and ipx. Separate keywords with a comma. You can also enter hexadecimal or decimal values in the range of 0x0600 (1536) to 0xFFFF (65535).

10. In the **VLAN ID** field, enter the VLAN ID.

    The ID can be any number in the range of 1 to 4093. All the ports in the group assign this VLAN ID to untagged packets received for the protocols that you included in this group.

11. Click the **Add** button.

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

The view-only Ports field displays all member ports that belong to the 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

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

   The Protocol Based VLAN Group Configuration page displays.
7. In the table, select the check box for the protocol-based VLAN group.
8. Change the settings.
9. Click the **Apply** button.

   Your settings saved.

Remove a protocol-based VLAN group

You can remove a protocol-based VLAN group that you no longer need.

To remove a protocol-based VLAN group:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The Protocol Based VLAN Group Configuration page displays.

7. In the table, select the check box for the protocol-based VLAN group.
8. Click the **Delete** button.

   Your settings saved. The group is removed.

Configure protocol-based VLAN group membership

To configure protocol-based VLAN group membership:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The Protocol Based VLAN Group Membership page displays.

7. From the **Group ID** menu, select the protocol-based VLAN group ID.

   The Group Name field shows the name that is associated with the group.

8. In the Ports table and LAG table, click each port and LAG that you want to include in the protocol-based VLAN group.

   A protocol-based VLAN group can include both port and LAGs. A selected port or LAG is displayed by a check mark.

9. Click the **Apply** button

   Your settings are saved.

10. To show the current numbers in the selected protocol-based VLAN group, click the **Current Members** button.

Configure a voice VLAN

You can configure the settings for a voice VLAN configuration.

To configure a voice VLAN:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > VLAN > Advanced > Voice VLAN Configuration**.

   The Voice VLAN Configuration page displays.

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

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

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

9. From the **Interface Mode** menu, select the voice VLAN mode for selected interfaces:
   - **Disable**. This is the default value.
   - **None**. Allow the IP phone to use its own configuration to send untagged voice traffic.
   - **VLAN ID**. Configure the phone to send tagged voice traffic.
   - **Dot1p**. Configure voice VLAN 802.1p priority tagging for voice traffic. When this is selected, enter the dot1p value in the **Value** field.
   - **Untagged**. Configure the phone to send untagged voice traffic.

10. In the **Value** field, enter the VLAN ID or Dot1p value.

    This field is enabled only when VLAN ID or Dot1p is selected as the interface mode.

11. In the **CoS Override Mode** field, select **Disable** or **Enable**.

    The default is Disable.

12. In the **Authentication Mode** field, select **Enable** or **Disable**.

    The default is Enable. When the authentication mode is enabled, voice traffic is allowed on an unauthorized voice VLAN port. When the authentication mode is disabled, devices are authorized through dot1x.

    Note: Authentication through Dot1x is possible only if Dot1x is enabled.

13. In the **DSCP Value** field, configure the Voice VLAN DSCP value for the port.

    The valid range is 0 to 64. The default value is 0.

14. Click the **Apply** button.

    Your settings are saved.

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

Configure GARP switch settings

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

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

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

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

To configure GARP switch settings:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The GARP Switch Configuration page displays.

7. Select the GVRP Mode **Disable** or **Enabl**e radio button.

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

8. Click the **Apply** button.

   Your settings are saved.

Configure GARP ports

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

To configure GARP ports:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

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

   The GARP Port Configuration page displays.

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

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

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

   This specifies the GARP VLAN registration protocol administrative mode for the port. If you select **Disable**, the protocol is not active and the join time, leave time, and leave all time options are without any effect. The default is Disable.
10. In the **Join Timer** field, specify the time in centiseconds between the transmission of GARP PDUs registering (or reregistering) membership for a VLAN or multicast group.

    Enter a number between 10 and 100 (0.1 to 1.0 seconds). The default is 20 centiseconds (0.2 seconds). An instance of this timer exists for each GARP participant for each port.
11. In the **Leave Timer** field, specify the time in centiseconds to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry.

    This allows time for another station to assert registration for the same attribute to maintain uninterrupted service. Enter a number between 20 and 600 (0.2 to 6.0 seconds). The default is 60 centiseconds (0.6 seconds). An instance of this timer exists for each GARP participant for each port.
12. In the **Leave All Timer field**, specify how frequently (in centiseconds) LeaveAll PDUs are generated.

    A LeaveAll PDU indicates that all registrations are to 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). An instance of this timer exists for each GARP participant for each port.
13. Click the **Apply** button.

    Your settings are saved.

Configure Auto-VoIP

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

Configure the Auto-VoIP protocol-based settings

To prioritize time-sensitive voice traffic over data traffic, protocol-based Auto-VoIP checks for packets carrying the Session Initiation Protocol (SIP) VoIP protocol.

VoIP frames that are received on ports that for which the Auto-VoIP feature is enabled are marked with the specified CoS traffic class value.

To configure the Auto-VoIP protocol-based settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Auto-VoIP > Protocol-based > Port Settings**.

   The Protocol Based Port Settings page displays.
7. In the Protocol Based Global Settings section, specify the following global settings:
   a. From the **Prioritization Type** menu, select **Traffic Class** or **Remark**.

      This specifies the type of prioritization.

b. From the **Class Value** menu, specify the CoS class value to be reassigned for packets that the voice VLAN receives.

8. In the Protocol Based Global Settings section, specify the Auto VoIP Mode settings:
   a. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
      - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
      - **LAG**. Only LAGs are displayed.
      - **All**. Both physical interfaces and LAGs are displayed.
   b. Select one or more interfaces by taking one of the following actions:
      - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
      - To configure multiple interfaces with the same settings, select the check box associated with each interface.
      - To configure all interfaces with the same settings, select the check box in the heading row.
   c. From the **Auto VoIP Mode** menu, select to enable or disable the Auto VoIP mode for the interface or interfaces.
9. Click the **Apply** button.

   Your settings are saved.

   The Operational State field displays the operational status of the interface.

Configure the Auto-VoIP OUI-based properties

With Organizationally Unique Identifier (OUI)–based Auto-VoIP, voice prioritization is provided based on OUI bits.

To configure the Auto-VoIP OUI-based properties:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > Auto-VoIP > OUI-Based > Properties**.

   The OUI-Based Properties page displays.

7. In the **Auto-VoIP VLAN ID** field, enter the VoIP VLAN ID for the switch.

   By default, an Auto-VoIP with VLAN ID 4088 exists.

8. From the **OUI-Based priority** menu, select the OUI-based priority of the switch.

   The default value is 7.

9. Click the **Apply** button.

   Your settings are saved.

Configure the OUI-based port settings

The port settings page allows you to configure the OUI port settings.

To configure the OUI-based port settings:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > Auto-VoIP > OUI-based > Port Settings**.

   The OUI Port Settings page displays.

7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. From the **Auto VoIP Mode** menu, select **Disable** or **Enable**.

   Auto-VoIP is disabled by default.

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

10. Click the **Apply** button.

    Your settings are saved.

Manage the OUI table

Device hardware manufacturers can include an OUI in a network adapter to help identify a hardware device. The OUI is a unique 24-bit number assigned by the IEEE registration authority. The switch comes preconfigured with OUIs that identify IP phone manufacturers.

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

Configure the OUI table

To configure the OUI table:

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

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Auto-VoIP > OUI-based > OUI Table**.

   The OUI Table page displays.
7. In the **Telephony OUI(s)** field, specify the VoIP OUI prefix to be added in the format AA:BB:CC.

   You can configure up to 32 OUIs.
8. In the **Description** field, enter the description for the OUI.

   The maximum length of description is 32 characters.
9. Click the **Add** button.

   The telephony OUI entry is added.

Delete one or more OUI prefixes from the OUI table

To delete one or more OUI prefixes from the OUI table:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > Auto-VoIP > OUI-based > OUI Table**.

   The OUI Table page displays.

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

   The telephony OUI entries are removed.

Display the Auto-VoIP status

You can display the Auto-VoIP status.

To view the Auto-VoIP status:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > Auto-VoIP > Auto-VoIP Status**.

   The Auto-VoIP Status page displays.

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

The following table describes the view-only Auto-VoIP status information.

Table 38. Auto-VoIP status

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

Configure Spanning Tree Protocol

The Spanning Tree Protocol (STP) provides a tree topology for any arrangement of network devices. STP also provides one path between end stations on a network, eliminating loops. STP (also referred to as “classic” STP) provides a single path between end stations, avoiding and eliminating loops. For information about configuring the global STP settings for the switch, see Configure the STP settings and view the STP status on page 175.

The switch support the following spanning tree versions:

- **CST**. Common STP. For information on configuring CST, see Configure the CST Settings on page 177 and Configure the CST port settings on page 178.
- **MSTP**. Multiple Spanning Tree Protocol (MSTP, also referred to as MST) supports multiple instances of spanning tree to efficiently channel VLAN traffic over different interfaces. For information on configuring MSTP, see Manage the MST settings on page 183 and Configure and view the port settings for an MST instance on page 186.
- **RSTP**. Rapid STP. Each instance of the spanning tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree (RSTP), with slight modifications in the working but not the end effect (chief among the effects is the rapid transitioning of the port to the forwarding state). For information on viewing the RSTP state, see View the Rapid STP information on page 182.

  The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full-duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to the forwarding state and the suppression of Topology Change Notification. These features are represented by the parameters pointtopoint and edgeport. MSTP is compatible with both RSTP and STP. It behaves in a way that is appropriate for STP and RSTP bridges. An MSTP bridge can be configured to behave entirely as an RSTP bridge or an STP bridge.

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

Configure the STP settings and view the STP status

You can configure the STP settings and view the STP status on the switch.

To configure the STP settings and view the STP status:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > STP > Basic > STP Configuration**.

   The Global Settings page displays.
7. Configure the following options:
   - **Spanning Tree State**. Enable or disable the spanning tree operation on the switch.
   - **STP Operation Mode**. Specify the STP version for the switch. The options are **STP**, **RSTP**, and **MSTP**.
   - **Configuration Name**. Specify an identifier for the configuration currently being used. It can be up to 32 alphanumeric characters. The default is the switch base MAC address.
   - **Configuration Revision Level**. Specify an number for the configuration currently being used. The value allowed is between 0 and 65535. The default value is 0.

- **Forward BPDU while STP Disabled**. Enable or disable the BPDU floods. This specifies whether spanning tree BPDUs are forwarded while spanning tree is disabled on the switch.

8. Click the **Apply** button.

   Your settings are saved.

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

Table 39. STP configuration status

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

Configure the CST Settings

You can configure a common spanning tree (CST) and internal spanning tree on the switch.

To configure the CST settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > STP > Advanced > CST Configuration**.

   The CST Configuration page displays.
7. Specify the CST options:
   - **Bridge Priority**. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. Specify the bridge priority value for the Common and Internal Spanning Tree (CST). The valid range is 0–61440. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if you set the priority to any value between 0 and 4095, the switch automatically sets the value to 0. The default value is 32768.
   - **Bridge Max Age (secs)**. The bridge maximum age time for the Common and Internal Spanning Tree (CST), which indicates the time in seconds a bridge must wait before implementing a topological change. The valid range is 6–40, and the value must be less than or equal to (2 * Bridge Forward Delay) – 1 and greater than or equal to 2 * (Bridge Hello Time +1). The default value is 20.
   - **Bridge Hello Time (secs)**. The bridge hello time for the Common and Internal Spanning Tree (CST), which indicates the time in seconds a root bridge must wait

between configuration messages. The value is fixed at 2 seconds. The value must be less than or equal to (Bridge Max Age / 2) – 1. The default hello time value is 2.

- **Bridge Forward Delay (secs)**. The bridge forward delay time, which indicates the time in seconds a bridge must remains in a listening and learning state before forwarding packets. The value must be greater or equal to (Bridge Max Age / 2) + 1. The time range is from 4 seconds to 30 seconds. The default value is 15 seconds.
- **Spanning Tree Maximum Hops**. The maximum number of bridge hops the information for a particular CST instance can travel before being discarded. The valid range is 6–40. The default is 20 hops.

8. Click the **Apply** button.

   Your settings are saved.

The following table describes the view-only MSTP status information that is displayed.

Table 40. STP advanced CST configuration, MSTP status

Field	Description
MST ID	Table consisting of the MST instances (including the CST) and the corresponding VLAN IDs associated with each of them.
VID ID	Table consisting of the VLAN IDs and the corresponding FID associated with each of them.
FID ID	Table consisting of the FIDs and the corresponding VLAN IDs associated with each of them.

Configure the CST port settings

You can configure a common spanning tree (CST) and internal spanning tree on a specific port on the switch.

A port can become diagnostically disabled (D-Disable) when DOT1S experiences a severe error condition. The most common cause is when the DOT1S software experiences BPDU flooding. The flooding criteria are such that DOT1S receives more than 15 BPDUs in a 3-second interval. The other causes for DOT1S D-Disable are extremely rare.

To configure the CST port settings:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > STP > Advanced > CST Port Configuration**.

   The Port Configuration page displays.
7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. From the **STP Status** menu, select the option to enable or disable the spanning tree administrative mode associated with the port or port channel.

   The possible values are Enable and Disable. The default value is Enable.
10. From the **Fast Link** menu, select whether the specified port is an edge port within the CST.

    The possible values are Enable and Disable. The default value is Disable.
11. From the **BPDU Forwarding** menu, configure BPDU forwarding.

    The possible values are Enable and Disable. The default value is Disable. When BPDU forwarding is enabled, the switch forwards the BPDU traffic arriving on this port when STP is disabled on this port.
12. From the **Auto Edge** menu, specify if the port is allowed to become an edge port if it does not detect BPDUs for some duration.

    The possible values are Enable and Disable. The default value is Enable.
13. In the **Path Cost** field, set the path cost to a new value for the specified port in the common and internal spanning tree.

Specify a value in the range of 0 to 200000000. The default is 0. When the path cost is set to 0, the value is updated with the external path cost from a received STP packet.

14. In the **Priority** field, specify the priority for a particular port within the CST.

    The port priority is set in multiples of 16. For example if you attempt to set the priority to any value between 0 and 15, it is set to 0. If you try to set it to any value between 16 and (2*16 – 1), it is set to 16, and so on. The range is 0 to 240. The default value is 128.

15. In the **External Port Path Cost** field, set the external path cost to a new value for the specified port in the spanning tree.

    The value range is 0 to 200000000. The default is 0.

16. Click the **Apply** button.

    Your settings are saved.

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

The following table describes the view-only information displayed on the page.

Table 41. CST port configuration

Field	Description
Port State	The forwarding state of this port. The default is Disabled.
Port Path Cost	The automatically calculated path cost, which is based on the link speed of the port if the configured value in the Path Cost field zero.
Port ID	The port identifier for the specified port within the CST. It is made up from the port priority and the interface number of the port.
Hello Timer	The value of the setting for the CST. The default is 2 seconds.

View the CST port status

You can display the common spanning tree (CST) and internal spanning tree for a specific port on the switch.

To view the CST port status:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > STP > Advanced > CST Port Status**.

   The CST Port Status field displays.
7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. To refresh the page, click the **Refresh** button.

The following table describes the view-only CST status information displayed on the page.

Table 42. CST port status

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

Table 42. CST port status (continued)

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

View the Rapid STP information

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

To view information about RSTP:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > STP > Advanced > RSTP**.

   The the Rapid STP page displays.
7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.

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

The following table describes the view-only Rapid STP status information displayed on the page.

Table 43. Rapid STP status information

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

Manage the MST settings

You can configure a multiple spanning tree (MST) on the switch.

Configure an MST instance

To configure an MST instance:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > STP > Advanced > MST Configuration**.

The MST Configuration page displays.

7. Configure the MST values:
   - **MST ID**. Specify the ID of the MST to create. The valid values for this are 1 to 4094. This is visible only when the select option of the MST ID select box is selected.
   - **Priority**. The bridge priority value for the MST. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if you set the priority to any value between 0 and 4095, the switch automatically sets the value to 0. The default value is 32768. The valid range is 0–61440.
   - **VLAN ID**. The menu includes all VLANs that are configured on the switch. You can select VLANs that must be associated with the MST instance or clear VLANs that are already associated with the MST instance.
8. Click the **Add** button.

   The MST is added.

For each configured instance, the view-only information described in the following table displays on the page.

Table 44. MST configuration

Field	Description
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Last TCN	The time in day:hour:minute:second format since the topology of the selected MST instance last changed.
Topology Change Count	Number of times that the topology changed for the selected MST instance.
Topology Change	The value of the topology change setting for the switch indicating if a topology change is in progress on any port assigned to the selected MST instance. It is either True or False.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge
Root Path Cost	Path cost to the designated root for this MST instance.
Root Port	Port to access the designated root for this MST instance.

Modify an MST instance

To modify an MST instance:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > STP > Advanced > MST Configuration**.

   The MST Configuration page displays.
7. Select the check box next to the instance.

   You can select multiple check boxes to apply the same setting to all selected ports.
8. Update the values.
9. Click the **Apply** button.

   Your settings are saved.

Delete an MST instance

To delete an MST instance:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > STP > Advanced > MST Configuration**.

   The MST Configuration page displays.
7. Select the check box for the instance.
8. Click the **Delete** button.

   The MST instance is removed.

Configure and view the port settings for an MST instance

You can configure and display the Multiple Spanning Tree (MST) settings on a specific port on the switch.

A port can become diagnostically disabled (D-Disable) when DOT1S experiences a severe error condition. The most common cause is when the DOT1S software experiences BPDU flooding. The flooding criteria is such that DOT1S receives more than 15 BPDUs in a 3-second interval. The other causes for DOT1S D-Disable are extremely rare.

To configure and view the port settings for an MST instance:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > STP > Advanced > MST Port Configuration**.

   The MST Port Configuration page displays.

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

---

7. From the **Select MST** menu, select an MST instance.
8. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
9. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
10. Configure the MST values for the selected interfaces:
    - **Port Priority**. The priority for a particular port within the selected MST instance. The port priority is set in multiples of 16. If you specify a value that is not a multiple of 16, the priority is set to the priority is automatically set to the next lowest priority that is a multiple of 16. For example, if you set a value between 0 and 15, the priority is set to 0. If you specify a number between 16 and 31, the priority is set to 16. Specify a value in the range of 0–240.
    - **Port Path Cost**. Set the path cost to a new value for the specified port in the selected MST instance. Specify a value in the range of 0–200000000.
11. Click the **Apply** button.

    Your settings are saved.

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

The following table describes the view-only MST port configuration information displayed on the Spanning Tree CST Configuration page.

Table 45. MST port status information

Field	Description
Operational Port Path Cost	The actual port path cost.
Auto-calculated Port Path Cost	Indicates whether the path cost is automatically calculated (Enabled) or not (Disabled). Path cost is calculated based on the link speed of the port if the configured value for Port Path Cost is zero.
Port ID	The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
Port Up Time Since Counters Last Cleared	The time since the counters were last cleared, displayed in days, hours, minutes, and seconds.
Port Mode	The Spanning Tree Protocol administrative mode that is associated with the port or port channel. The possible values are Enable and Disable.
Port Forwarding State	Indicates the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are as follows: • **Manual Forwarding**. STP is currently disabled on the port. The port forwards traffic while learning MAC addresses. • **Discarding**. The port is currently blocked. The port cannot forward traffic nor can it learn MAC addresses. • **Learning**. The port is currently in the learning mode. The port cannot forward traffic. However, it can learn new MAC addresses. • **Forwarding**. The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses
Port Role	Each MST bridge port that is enabled is assigned a port role for each spanning tree. The port role is one of the following: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.
Designated Root	The root bridge for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	The cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
Designated Bridge	The bridge identifier of the bridge with the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	The port identifier on the designated bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.

View the STP Statistics

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

To view the spanning tree statistics:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > STP > Advanced > STP Statistics**.

   The STP Statistics page displays.
7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. To refresh the page, click the **Refresh** button.

The following table describes the information available about the STP Statistics page.

Table 46. STP Statistics

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

Table 46. STP Statistics (continued)

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

Configure multicast

Multicast IP traffic is traffic that is destined to a host group. Host groups for IPv4 multicast are identified by class D addresses, which range from 224.0.0.0 to 239.255.255.255. Host groups for IPv6 multicast are identified by the prefix ff00::/8.

View, search, or clear the MFDB table

The Multicast Forwarding Database (MFDB) holds the port membership information for all active multicast address entries. The key for an entry consists of a VLAN ID and MAC address pair. Entries can contain data for more than one protocol.

To view, search, or clear the MFDB table:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

The System Information page displays.

6. Select **Switching > Multicast > MFDB > MFDB Table**.

   The MFDB Table page displays.

7. In the **Search by MAC Address** field, enter a MAC address.

   Enter six two-digit hexadecimal numbers separated by colons, for example 00:01:23:43:45:67.

8. Click the **Login** button.

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

Table 47. MFDB table information

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

View the MFDB statistics

To view the MFDB statistics:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > Multicast > MFDB > MFDB Statistics**.

   The MFDB Statistics page displays.

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

The following table describes the view-only MFDB statistics fields.

Table 48. MFDB Statistics information

Field	Description
Max MFDB Table Entries	The maximum number of entries that the Multicast Forwarding Database table can hold.
Most MFDB Entries Since Last Reset	The largest number of entries that were present in the Multicast Forwarding Database table since last reset. This value is also known as the MFDB high-water mark.
Current Entries	The current number of entries in the Multicast Forwarding Database table.

Configure the auto-video multicast settings

You can configure the auto-video settings.

To configure auto-video multicast settings:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > Multicast > Auto-Video**.

   The Auto-Video Configuration page displays.

7. Select one of the following radio buttons:
   - Select the **Disable** radio button to globally disable Auto-Video administrative mode for the switch.
   - Select the **Enable** radio button to globally enable Auto-Video administrative mode for the switch.

   The Auto-Video VLAN field shows the ID of the Auto-Video VLAN.

8. Click the **Apply** button.

   Your settings are saved.

Manage IGMP snooping

Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward IPv4 multicast traffic intelligently. Multicast IPv4 traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

A traditional Ethernet network can be separated into different network segments to prevent placing too many devices onto the same shared media. Bridges and switches connect these segments. When a packet with a broadcast or multicast destination address is received, the switch forwards a copy to each of the remaining network segments in accordance with the IEEE MAC Bridge standard. Eventually, the packet is made accessible to all nodes connected to the network.

This approach works well for broadcast packets that are intended to be detected or processed by all connected nodes. For multicast packets, this approach could lead to a less efficient use of the network bandwidth, particularly when the packets are intended for a small number of nodes only. Packets are flooded into network segments where no node is receptive to the packet. Although nodes rarely incur any processing overhead to filter packets addressed to unrequested group addresses, the nodes cannot transmit new packets onto the shared media while the multicast packets are being flooded. Such as waste of bandwidth is even worse when the LAN segment is not shared, for example in full-duplex links.

Allowing switches to snoop IGMP packets can solve this problem. While the IGMP packets are being forwarded throughout the network, the switch uses the information in the packets to determine which segments must receive packets that are directed to the group address.

Configure IGMP snooping

You can configure the settings for IGMP snooping, which is used to build forwarding lists for multicast traffic.

To configure IGMP snooping:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping Configuration**.

   The IGMP Snooping Configuration page displays.
7. Select the IGMP Snooping Status **Enable** or **Disable** radio button.

   This specifies the administrative mode for IGMP snooping for the switch. The default is Disable.
8. Select the Validate IGMP IP header **Enable** or **Disable** radio button.

   When IGMP IP header validation is enabled, any IGMP IP header must include the Router Alert, ToS, and TTL information. Otherwise, the IGMP packet is discarded. The default value is Enable.
9. Click the **Apply** button.

   Your settings are saved.
10. To refresh the page, click the **Refresh** button.

The following table displays the view-only information about the global IGMP snooping status and statistics on the page.

Table 49. IGMP Snooping Configuration information

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

Configure IGMP snooping for interfaces

To configure IGMP snooping for interfaces:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping Interface Configuration**.

   The IGMP Snooping Interface Configuration page displays.

7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. From the **Admin Mode** menu, select **Disable** or **Enable**.

   This specifies the interface mode for the selected interface for IGMP snooping for the switch. The default is Disable.
10. In the **Host Timeout** field, specify the time that the switch must wait for a report for a particular group on a particular interface before it deletes that interface from the group.

    Enter a value between 1 and 3600 seconds. The default is 260 seconds.
11. In the **Max Response Time** field, specify the time that the switch must wait after sending a query on an interface because it did not receive a report for a particular group on that interface.

    Enter a value greater or equal to 1 and less than the group membership interval in seconds. The default is 10 seconds. The configured value must be less than the group membership interval.
12. In the **MRouter Timeout** field, specify the time that the switch must wait to receive a query on an interface before removing it from the list of interfaces with multicast routers attached.

    Enter a value between 0 and 3600 seconds. The default is 0 seconds. A value of zero indicates an infinite time-out, that is, no expiration.
13. From the **Fast Leave Mode** menu, select whether fast leave mode is enabled.

    The options are **Enable** and **Disable**. The default is Disable.
14. Click the **Apply** button.

    Your settings are saved.

View, search, or clear the IGMP snooping table

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

To view, search, or clear the IGMP snooping table:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping Table**.

   The IGMP Snooping Table page displays.
7. In the **Search By MAC Address** field, specify the MAC address for which you want to view the MFDB table entry.

   Enter six two-digit hexadecimal numbers separated by colons, for example 00:01:23:43:45:67.
8. Click the **Login** button.

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

The following table describes the information in the IGMP snooping table.

Table 50. IGMP Snooping Table information

Field	Description
MAC Address	The multicast MAC address for which the switch holds forwarding and/or filtering information. The format is six two-digit hexadecimal numbers that are separated by colons, for example, 01:00:5e:45:67:89.
VLAN ID	The VLAN ID for which the switch holds forwarding and filtering information.

Table 50. IGMP Snooping Table information (continued)

Field	Description
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry. Possible values are Management Configured, Network Configured, and Network Assisted.
Interface	The interfaces that are designated for forwarding (Fwd) and filtering (Flt) for the associated address.

Configure IGMP snooping for VLANs

To configure IGMP snooping for VLANs:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping VLAN Configuration**.

   The IGMP Snooping VLAN Configuration page displays.
7. To enable IGMP snooping on a VLAN, in the **VLAN ID** field, enter the VLAN ID.
8. Configure the IGMP snooping settings for the VLAN:
   - **Admin Mode**. Enable or disable IGMP snooping for the specified VLAN ID. The default is Disable.
   - **Fast Leave Mode**. Enable or disable the IGMP snooping fast leave mode for the specified VLAN ID. The default is Disable.

- **Host Timeout**. Set the value for group membership interval of IGMP snooping for the specified VLAN ID. The valid range is Maximum Response Time + 1 to 3600 seconds. The default is 260 seconds.
- **Maximum Response Time**. Set the value for the maximum response time of IGMP snooping for the specified VLAN ID. The valid range is from 1 to 25 seconds. The default is 10 seconds. The configured value must be lower than the value that you specify in the Host Timeout field.
- **MRouter Timeout**. Set the value for multicast router expiry time of IGMP snooping for the specified VLAN ID. The valid range is 0 to 3600 seconds.
- **Report Suppression Mode**. Enable or disable IGMP snooping report suppression mode for the specified VLAN ID. IGMP snooping report suppression allows the suppression of the IGMP reports sent by the multicast hosts by building a Layer 3 membership table. The results is that only the most essential reports are sent to the IGMP routers so that the routers can continue to receive the multicast traffic.The default is Disable.
- **Querier Mode**. Enable or disable the IGMP querier mode for the specified VLAN ID. If proxy querier mode is disabled, an IGMP proxy query with source IP 0.0.0.0 is not sent in response to an IGMP leave packet. The default is Disable.
- **Query Interval**. Set the IGMP query interval for the specified VLAN ID. The valid range is 1 to 1800 seconds. The default is 60 seconds.

9. Click the **Apply** button.

   Your settings are saved.

Configure one or more IGMP multicast router interfaces

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 reachable from this interface. Configuring a multicast router interface is usually not required because the switch automatically detects the multicast router and forwards IGMP packets accordingly. It is required only if you want to make sure that the multicast router always receives IGMP packets from the switch in a complex network.

To configure one or more IGMP multicast router interfaces:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Multicast > IGMP Snooping > Multicast Router Configuration**.

   The Multicast Router Configuration page displays.
7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. In the **Multicast Router** field, select **Enable** or **Disable**.
10. Click the **Apply** button.

    Your settings are saved.

Configure an IGMP multicast router VLAN

You can configure an interface to forward only snooped IGMP packets from a specific VLAN to the multicast router attached to the interface. This configuration is usually not required because the switch automatically detects a multicast router and forwards the IGMP packets accordingly. It is required only if you want to make sure that the multicast router always receives IGMP packets from the switch in a complex network.

To configure a multicast router VLAN:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > Multicast > IGMP Snooping > Multicast Router VLAN Configuration**.

   The Multicast Router VLAN Configuration page displays.

7. From the **Interface** menu, select the interface.
8. In the **VLAN ID** field, enter the VLAN ID.
9. From the **Multicast Router** menu, select **Enable** or **Disable**.
10. Click the **Apply** 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 about IGMP snooping queriers on the network and, separately, on VLANs.

Configure an IGMP snooping querier

You can configure the settings for an IGMP snooping querier.

To configure the settings for an IGMP snooping querier:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Multicast > IGMP Snooping Querier > Querier Configuration**.

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

8. Click the **Apply** button.

   Your settings are saved.

Configure an IGMP snooping querier for VLANs

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

To configure IGMP snooping for a VLAN:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Configuration**.

   The Querier VLAN Configuration page displays.
7. From the **VLAN ID** menu, select **New Entry**.
8. Configure the following settings:
   - **VLAN ID**. The VLAN ID for which the IGMP snooping querier is to be enabled.
   - **Querier Election Participate Mode**. Enable or disable querier this mode:
     - **Disable**. Upon seeing another querier of the same version in the VLAN, the snooping querier moves to the non-querier state.
     - **Enable**. The snooping querier participates in querier election, in which the lowest IP address operates as the querier in that VLAN. The other querier moves to non-querier state.
   - **Snooping Querier VLAN Address**. Specify the snooping querier IP address to be used as the source address in periodic IGMP queries sent on the specified VLAN.

9. Click the **Apply** 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Configuration**.

   The Querier VLAN Configuration page displays.
7. From the **VLAN ID** menu, select the VLAN ID
8. Click the **Delete** button.

   Your settings saved. The IGMP snooping querier settings are removed from the VLAN. (The VLAN itself is not deleted.)

Display the status of the IGMP snooping querier for VLANs

To display the status of the IGMP snooping querier VLANs:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Status**.

   The Querier VLAN Status page displays.
7. To refresh the page, click the **Refresh** button.

The following table describes the view-only information displayed on the page.

Table 51. Querier VLAN Status information

Field	Description
VLAN ID	The VLAN ID on which IGMP snooping querier is administratively enabled and the VLAN exists in the VLAN database.
Operational State	The operational state of the IGMP snooping querier on a VLAN. It can be in any of the following states: • **Querier**. The snooping switch is the querier in the VLAN. The snooping switch sends out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch finds a better querier in the VLAN, it moves to non-querier mode. • **Non-Querier**. The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch moves into querier mode. • **Disabled**. The snooping querier is not operational on the VLAN. The snooping querier moves to disabled mode when IGMP snooping is not operational on the VLAN or when the querier address is not configured or the network management address is also not configured.
Operational Version	The operational IGMP protocol version of the querier.
Last Querier Address	The IP address of the last querier from which a query was snooped on the VLAN.

Table 51. Querier VLAN Status information (continued)

Field	Description
Last Querier Version	The IGMP protocol version of the last querier from which a query was snooped on the VLAN.
Operational Max Response Time	The maximum response time to be used in the queries that are sent by the snooping querier.

Manage MLD snooping

In IPv6 networks, Multicast Listener Discovery (MLD) snooping performs a similar function as IGMP does 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, which is used to build forwarding lists for multicast traffic.

To enable MLD snooping:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > Multicast > MLD Snooping > Configuration**.

   The MLD Snooping Configuration page displays.

7. Select the MLD Snooping Admin Mode **Enable** radio button.

   By default, the **Disable** radio button is selected.

8. Click the **Apply** button.

   Your settings are saved.

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

The following table describes the view-only MLD Snooping Configuration fields.

Table 52. MLD Snooping Configuration information

Field	Definition
Multicast Control Frame Count	The number of multicast control frames that were processed by the CPU.
Interfaces Enabled for MLD Snooping	The interfaces on which MLD snooping is administratively enabled. MLD snooping must be enabled globally and on an interface for the interface to be able to snoop MLD packets to determine which segments must receive multicast packets directed to the group address.
VLAN IDs Enabled For MLD Snooping	The VLANs on which MLD snooping is administratively enabled.

Configure MLD snooping for interfaces

To configure MLD snooping for interfaces:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Multicast > MLD Snooping > Interface Configuration**.

   The MLD Snooping Interface Configuration page displays.
7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. From the **Admin Mode** menu, select to enable or disable the interface mode for the selected interface for MLD snooping for the switch.

   The default is Disable.
10. In the **Membership Interval** field, specify the time that the switch must wait for a report for a particular group on a particular interface before it deletes that interface from the group.

    The valid range is from 2 to 3600 seconds. The configured value must be greater than the maximum response time. The default is 260 seconds.
11. In the **Max Response Time in seconds** field, specify the time that the switch must wait after sending a query on an interface because it did not receive a report for a particular group on that interface.

    Enter a value greater than or equal to 1 and less than the group membership interval in seconds. The default is 10 seconds. The configured value must be less than the group membership interval.
12. In the **Expiration Time** field, specify the time that the switch must wait to receive a query on an interface before removing the interface from the list of interfaces with multicast routers attached.

Enter a value between 0 and 3600 seconds. The default is 0 seconds. A value of zero indicates an infinite time-out, that is, no expiration.

13. From the **Fast Leave** menu, select to enable or disable Fast Leave on the interface.

    If Fast Leave is enabled, the interface can be immediately removed from the Layer 2 forwarding table when the switch receives an MLD leave message for a multicast group without first sending MAC-based general queries. The default is Disable.

14. Click the **Apply** button.

    Your settings are saved.

Configure the MLD VLAN settings

To configure the MLD VLAN settings:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > Multicast > MLD Snooping > MLD VLAN Configuration**.

   The MLD VLAN Configuration page displays.

7. In the **VLAN ID** field, specify the VLAN IDs for which MLD snooping is enabled.
8. From the **Fast Leave** menu, select to enable or disable the MLD snooping Fast Leave mode for the specified VLAN ID.
9. In the **Membership Interval** field, set the value for the group membership interval of MLD snooping for the specified VLAN ID.

   The valid range is Maximum Response Time + 1 to 3600.

10. In the **Maximum Response Time** field, set the value for the maximum response time of MLD snooping for the specified VLAN ID.

    The valid range is 1 to Group Membership Interval –1. This value must be less than the group membership interval value.

11. In the **Multicast Router Expiry Time** field, set the value for the multicast router expiration time of MLD snooping for the specified VLAN ID.

    The valid range is 0 to 3600.

12. Click the **Add** button.

    MLD snooping is enabled on the specified VLAN.

Modify the MLD snooping settings for a VLAN

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > Multicast > MLD Snooping > MLD VLAN Configuration**.

   The MLD VLAN Configuration page displays.

7. Select the check box next to the VLAN ID.
8. Change the settings.
9. Click the **Apply** button.

   Your settings are saved.

Remove MLD snooping from a VLAN

To remove MLD snooping 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Multicast > MLD Snooping > MLD VLAN Configuration**.

   The MLD VLAN Configuration page displays.
7. Select the check box next to the VLAN ID.
8. Click the **Delete** button.

   MLD snooping is removed from the VLAN.

Configure one or more MLD multicast router interfaces

To configure one or more MLD multicast router interfaces:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Multicast > MLD Snooping > Multicast Router Configuration**.

   The Multicast Router Configuration page displays.
7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. From the **Multicast Router** menu, select to enable or disable the multicast router for the selected interfaces.
10. Click the **Apply** button.

    Your settings are saved.

Configure an MLD multicast router VLAN

To configure an MLD multicast router VLAN:

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Multicast > MLD Snooping > Multicast Router VLAN Configuration**.

   The Multicast Router VLAN Configuration page displays.
7. From the **Interface** menu, select the interface for which you want the multicast router to be enabled.
8. In the **VLAN ID** field, specify the VLAN ID.
9. From the **Multicast Router** menu, select to enable or disable the multicast router for the VLAN ID.
10. Click the **Apply** button.

    Your settings are saved.

Configure an MLD snooping querier

You can configure the settings for an MLD snooping querier.

To configure an MLD snooping querier:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > Multicast > MLD Snooping > Querier Configuration**.

   The MLD Snooping Querier Configuration page displays.

7. Select the Querier Admin Mode **Enable** or **Disable** radio button to specify if MLD snooping is enabled for the switch.

   The default is Disable.

8. In the **Querier Address** field, specify the snooping querier IP 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 query is being 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.

9. In the **Query Interval (secs)** field, specify 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 (secs)** field, specify 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.

11. Click the **Apply** button.

    Your settings are saved.

    The page displays the VLAN IDs enabled for MLD snooping querier.

Configure an MLD snooping querier for a VLAN

You can configure an MLD querier for use with a VLAN on the network.

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Multicast > MLD Snooping > Querier VLAN Configuration**.

   The MLD Snooping Querier VLAN Configuration page displays.
7. In the **VLAN ID** field, either specify a new VLAN or change an existing VLAN:
   - **Specify a new VLAN**. In the **VLAN ID** field, enter the ID for a new VLAN.
   - **Change an existing VLAN**. Select the check box for an existing VLAN.
8. From the **Querier Election Participate Mode** menu, select to enable or disable the querier election participate mode:
   - **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 IPv6 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. Either add the new VLAN or save the settings for the existing VLAN:
    - **Add the new VLAN**: Click the **Add** button.

      The VLAN is added.
    - **Save the settings for the existing VLAN**: Click the **Apply** button.

      Your settings are saved.

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

Table 53. 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 IP address of the last querier from which a query was snooped on the VLAN.
Last Querier Version	The MLD protocol version of the last querier from which a query was snooped on the VLAN.
Operational Max Response Time	The maximum response time to be used in the queries that are sent by the snooping querier.

Remove the MLD snooping querier settings for a VLAN

You can remove the MLD snooping querier settings for a VLAN.

To remove the MLD snooping querier settings for a VLAN:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   • Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > Multicast > MLD Snooping > Querier VLAN Configuration**.

   The MLD Snooping Querier VLAN Configuration page displays.

7. Select the check box for the VLAN for which you want to remove the IGMP snooping querier settings.
8. Click the **Delete** button.

   Your settings are saved. (The VLAN itself is not deleted.)

Configure multicast VLAN registration

IGMP snooping helps 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. Only one multicast source VLAN (MVLAN) can be configured per switch, and it is used only for certain multicast traffic, such as traffic from an IPTV application, to avoid duplication of multicast streams for clients in different VLANs. Clients can dynamically join or leave the multicast VLAN without interfering with their membership in other VLANs.

MVR, like IGMP snooping, allows a Layer 2 switch to listen to IGMP messages to learn about multicast group membership.

You can configure basic, advanced, group, interface, or group membership settings.

Configure the global MVR settings

To configure the global MVR settings:

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

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > MVR > Basic > MVR Configuration**.

   The MVR Configuration page displays.
7. From the **MVR Running** menu, select **Enable** or **Disable**.

   The default is Disable.
8. In the **MVR Multicast VLAN** field, specify the VLAN on which MVR multicast data is received.

   All source ports belong to this VLAN. The value can be set in a range from 1 to 4093. The default value is 1.
9. In the **MVR Global Query Response Time** field, set the maximum time that the switch must wait for an IGMP group membership report before removing the port from the multicast group membership.

   This time applies only to receiver-port leave processing. 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 port from the multicast group membership. The value is equal to tenths of a second. The range is from 1 to 100 tenths. The default is 5 tenths or one-half.
10. From the **MVR Mode** menu, specify the MVR mode of operation.

    Select **compatible** (the default mode) to block IGMP group membership reports on source ports. Select **dynamic** to allow IGMP group membership reports on source ports.
11. Click the **Apply** button.

    Your settings are saved.
12. To refresh the page, click the **Refresh** button.

The following table describes the view-only information displayed on the page.

Table 54. 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 MVR groups allocated.

Configure an MVR group

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > MVR > Advanced > MVR Group Configuration**.

   The MVR Group Configuration page displays.
7. In the **MVR Group IP** field, specify the IP address for the new MVR group.
8. In the **Count** field, specify the number of contiguous MVR groups.

   This number helps you to create multiple MVR groups through a single click of the **Add** button. If the field is empty, then clicking the button creates only one new group. The field is displayed as empty for each particular group. The range is from 1 to 256.
9. Click the **Add** button.

   The MVR group is added.

The following table describes the view-only information displayed on the page.

Table 55. MVR Group Configuration

Field	Definition
Status	The status of the specific MVR group.
Members	The list of ports that participate in the specific 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > MVR > Advanced > MVR Group Configuration**.

   The MVR Group Configuration page displays.
7. Select the check box for the MVR group.
8. Click the **Delete** button.

   The MVR group is removed.

Configure MVR group membership

To configure MVR group membership:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > MVR > Advanced > MVR Group Membership**.

   The MVR Group Membership page displays.
7. From the **MVR Group IP** menu, select the IP multicast address of the MVR group.
8. In the Ports table, click each port that you want to make a member of the MVR group.

   A selected port is shown by a check mark.
9. In the LAG table, click each LAG that you want to make a member of the MVR group.

   A selected LAG is shown by a check mark.
10. Click the **Apply** button.

    Your settings are saved.

Configure the MVR interface settings

To configure the MVR interface setting:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > MVR > Advanced > MVR Interface Configuration**.

   The MVR Interface Configuration page displays.
7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. From the **Admin Mode** menu, specify whether MVR is enabled by selecting **Enable** or **Disable**.

   The default is Disable.

10. From the **Type** menu, specify whether the port is an MVR receiver or an MVR source by selecting **receiver** or a **source**.

    The default port type is none.

11. From the **Immediate Leave** menu, specify whether the Immediate Leave feature is enabled by selecting **Enable** or **Disable**.

    The default is Disable.

12. Click the **Apply** button.

    Your settings are saved.

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

    The Status field shows the status for each interface.

View the MVR statistics

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > MVR > Advanced > MVR Statistics**.

   The MVR Statistics page displays.

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

The following table describes the view-only information displayed on the page.

Table 56. 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.

View, search, and manage the MAC address table

You can view or configure the MAC address table. This table contains information about unicast entries for which the switch holds forwarding or filtering information. This information lets the transparent bridging function determine how an incoming frame must be propagated. If you clear the MAC address entries in the MAC address table, only the dynamic entries are removed.

View, search, or clear the MAC address table

To view, search, or clear the MAC address table:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Address Table > Basic > Address Table**.

   The MAC Address Table page displays.
7. Use the **Search** menu and field to search for a MAC address, VLAN ID, or interface number:
   - **Search by MAC Address**. From the **Search** menu, select **MAC Address**, and enter the 6-byte hexadecimal MAC address in two-digit groups separated by colons, for example, 01:23:45:67:89:AB. Then click the **Go** button.

     If the address exists, that entry is displayed as the first entry followed by the remaining (higher) MAC addresses. An exact match is required.
   - **Search VLAN ID**. From the **Search** menu, select **VLAN ID**, and enter the VLAN ID, for example, 100. Then click the **Go** button.
   - **Search Interface**. From the **Search** menu, select **Interface**, and enter the interface ID using the respective interface naming convention (for example, g1 or l1). Then click the **Go** button.

The following table describes the view-only information displayed on the page.

Table 57. MAC Address Table information

Field	Description
Total MAC Addresses	The number of total MAC addresses learned or configured.
VLAN ID	The VLAN ID associated with the MAC address.
MAC Address	The unicast MAC address for which the switch holds forwarding and/or filtering information. The format is a 6-byte MAC address that is separated by colons, for example 01:23:45:67:89:AB.
Interface	The interface upon which this address was learned.
Status	The status of this entry. The meanings of the values are as follows: • **Static**. The value of the corresponding instance was added by the system or a user and cannot be relearned. • **Learned**. The value of the corresponding instance was learned, and is being used. • **Management**. The value of the corresponding instance is also the value of an existing instance of dot1dStaticAddress.

Set the dynamic address aging interval

You can set the address aging interval for the forwarding database. This is the time-out period in seconds for aging out dynamically learned forwarding information.

To set the dynamic address aging interval:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Address Table > Advanced > Dynamic Address**.

   The Dynamic Address page displays.
7. In the **Address Aging Timeout (seconds)** field, specify the time-out period in seconds for aging out dynamically learned forwarding information.

   802.1D-1990 recommends a default of 300 seconds. The value can be any number between 10 and 1000000 seconds. The default is 300.
8. Click the **Apply** button.

   Your settings are saved.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > Address Table > Advanced > Static MAC Address**.

   The Static MAC Address page displays.
7. From the **Interface** menu, select the interface or LAG.
8. In the **Static MAC Address** field, enter the MAC address.
9. From the **VLAN ID** menu, select the VLAN ID that must be associated with the MAC address.
10. Click the **Add** button.

    The static MAC address is added to the switch.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Select **Switching > Address Table > Advanced > 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.

Configure Layer 2 loop protection

Loops inside a network are costly because they consume resources and reduce the performance of the network. Detecting loops manually can be cumbersome.

The switch can automatically identify loops in the network. You can enable loop protection per port or globally.

If loop protection is enabled, the switch sends predefined PDU packets to a Layer 2 broadcast destination address (FF:FF:FF:FF:FF:FF) on all ports for which the feature is enabled. You can selectively disable PDU packet transmission for loop protection on specific ports even while port loop protection is enabled. If the switch receives a packet with the previously mentioned broadcast destination address, the source MAC address in the packet

is compared with the MAC address of the switch. If the MAC address does not match, the packet is forwarded to all ports that are members of the same VLAN, just like any other broadcast packet. The packet is not forwarded to the port from which it was received.

If the source MAC address matches the MAC address of the switch, the switch can perform one of the following actions, depending on how you configure the action:

- The port is shut down.
- A log message is generated. (If a syslog server is configured, the log message can be sent to the syslog server.)
- The port is shut down and a log message is generated.

Loop protection is not intended for ports that serve as uplinks between spanning tree–aware switches. It is intended for unmanaged switches that drop spanning tree BPDUs. Loop protection detects physical and logical loops between Ethernet ports on a device. You must enable loop protection globally before you can enable and configure it at the interface level. Loop protection is supported on physical interfaces and static LAG interfaces, but not on dynamic LAG interfaces.

Configure global Layer 2 loop protection

To configure L2 loop protection globally:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Switching > L2 Loop Protection > L2 Loop Protection Configuration**.

   The Global L2 Loop Protection Configuration page displays.

7. To enable or disable loop protection feature, select the Admin Mode **Enable** or **Disable** radio button.

   By default, the Disable radio button is selected.

8. From the **TLV Advertised Interval** menu, select the time in seconds between transmission of loop packets.

   The default transmit interval is 5 seconds.

9. From the **Max PDU Receive** menu, select the maximum number of packets to be received before an action is taken.

   The default is 1.

10. In the **Recovery Timer** field, enter the time in seconds after which a port is disabled when a loop is detected.

    The range is from 0 to 604800 seconds. The default is 0 seconds, which means that the port is not reenabled until you manually reenable the port.

11. Click the **Apply** button.

    Your settings are saved.

View and configure Layer 2 loop protection on a port

To view and configure L2 loop protection on a port:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Switching > L2 Loop Protection > L2 Loop Protection Configuration**.

The Global L2 Loop Protection Configuration page displays.

7. Scroll down to the L2 Loop Protection Interface Configuration section.
8. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
9. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
10. From the **Keep Alive** menu, select **Enable** or **Disable** to specify whether keep-alives are enabled on an interface.

    The default is Disable.
11. From the **RX Action** menu, select the action that occurs when the switch detects a loop on an interface:
    - **Log**. The switch logs a message.
    - **Disable**. The switch disables the interface. This is the default action.
    - **Both**. The switch both logs a message and disables the interface.
12. Click the **Apply** button.

    Your settings are saved.
13. Click the **Clear** button to clear all the statistics in the table.
14. Click the **Refresh** button to refresh the page with the latest information about the switch.

    The following table describes the view-only information displayed on the page.

Table 58. L2 Loop Protection Interface Information

Field	Description
Loop Detected	Shows whether a loop is detected on the interface. If the interface is disabled and then reenabled, the status changes to No again.
Loop Count	The number of packets that were received after the loop was detected.
Time Since Last Loop	The time that elapsed since the loop was detected.
Port Status	The status of the interface (Enabled, Disabled, or D-Disabled, which stands for diagnostically disabled).

4

Configure Routing

This chapter contains the following sections.

- Routing concepts
- Configure the routing mode
- Configure IPv6 routing
- Configure VLAN routing
- Configure router discovery for a VLAN routing interface
- Manage routes and view the routing table
- Configure Address Resolution Protocol

Routing concepts

The switch supports IP routing. When a packet enters the switch, the switch checks the destination MAC address to determine if it matches any of the configured routing interfaces. If it does, the switch searches the host table for a matching destination IP address. If a matching entry is found, the packet is routed to the host. If no matching entry is found, the switch performs a longest prefix match on the destination IP address. If a matching entry is found, the packet is routed to the next hop. If no matching entry is found, the packet is routed to the next hop that is specified in the default route. If no default route exists, the packet is are dropped.

The routing table can include static entries that you added manually. The host table can include static entries that were manually added and entries that were dynamically added through ARP.

Configure the routing mode

For information about how to configure the routing mode and display IP routing data, see the following sections:

- Manage the global IPv4 routing settings on page 233
- View the IP routing statistics on page 234

Manage the global IPv4 routing settings

You can enable routing and configure the routing settings for the switch.

The switch allows routing through any of its interfaces only after you enable routing on the switch. Separately, you can enable routing on VLANs (see Configure VLAN routing on page 252).

To enable routing on the switch:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > IP > IP Configuration**.

   The IP Configuration page displays.
7. Select the Routing Mode **Enable** radio button.

   You must enable routing for the switch before you can route through any of the interfaces. Routing is also enabled or disabled per VLAN interface. The default value is Disable.
8. Select the ICMP Redirects **Enable** or **Disable** radio button.

   The default is Disable. If you enable ICMP Redirects, the switch can forward ICMP Redirect messages.
9. Click the **Apply** button.

   Your settings are saved.

The following table describes the view-only IP configuration information displayed on the page.

Table 59. Global IP status information

Field	Description
Default Time to Live	The default value inserted into the Time-To-Live field of the IP header of datagrams originated by the switch, if a TTL value is not supplied by the transport layer protocol. The default value is 64.
Maximum Next Hops	The maximum number of hops supported by the switch. This is a compile-time constant. The default value is 1.

View the IP routing statistics

You can view the IP routing statistics as specified in RFC 1213.

To view the IP routing statistics:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Routing > IP > Statistics**.

   The IP Statistics page displays.

The following table describes the view-only information displayed on the page.

Table 60. IP Statistics information

Field	Description
IpInReceives	The total number of input datagrams received from interfaces, including those received in error.
IpInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
IpInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
IpForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities that do not act as IP gateways, this counter includes only those packets that were source-routed through this entity, and the source-route option processing was successful.
IpInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
IpInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but that were discarded (for lack of buffer space). This counter does not include any datagrams discarded while awaiting re-assembly.

Table 60. IP Statistics information (continued)

Field	Description
IpInDelivers	The total number of input datagrams successfully delivered to IP user protocols (including ICMP).
IpOutRequests	The total number of IP datagrams that local IP user protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in ipForwDatagrams.
IpOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that were discarded for reasons such as lack of buffer space. This counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
IpOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in ipForwDatagrams that meet this no-route criterion. This includes any datagrams that a host cannot route because all of its default gateways are down.
IpReasmTimeout	The maximum number of seconds for which received fragments are held while they are awaiting reassembly at this entity.
IpReasmReqds	The number of IP fragments received that were reassembled at this entity.
IpReasmOKs	The number of IP datagrams successfully reassembled.
IpReasmFails	The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so on). This is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.
IpFragOKs	The number of IP datagrams that were fragmented at this entity.
IpFragFails	The number of IP datagrams that were discarded because they needed to be fragmented at this entity but could not be, for reasons such as their Don't Fragment flag was set.
IpFragCreates	The number of IP datagram fragments that were generated as a result of fragmentation at this entity.
IpRoutingDiscards	The number of routing entries that were discarded even though they were valid. One possible reason for discarding such an entry could be to free up buffer space for other routing entries.
IcmpInMsgs	The total number of ICMP messages that the entity received. This counter includes all those counted by icmpInErrors.
IcmpInErrors	The number of ICMP messages that the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so on).
IcmpInDestUnreachs	The number of ICMP destination unreachable messages received.
IcmpInTimeExcds	The number of ICMP time exceeded messages received.
IcmpInParmProbs	The number of ICMP parameter problem messages received.

Table 60. IP Statistics information (continued)

Field	Description
IcmpInSrcQuenchs	The number of ICMP source quench messages received.
IcmpInRedirects	The number of ICMP redirect messages received.
IcmpInEchos	The number of ICMP echo (request) messages received.
IcmpInEchoReps	The number of ICMP echo reply messages received.
IcmpInTimestamps	The number of ICMP timestamp (request) messages received.
IcmpInTimestampReps	The number of ICMP timestamp reply messages received.
IcmpInAddrMasks	The number of ICMP address mask request messages received.
IcmpInAddrMaskReps	The number of ICMP address mask reply messages received.
IcmpOutMsgs	The total number of ICMP messages that this entity attempted to send. This counter includes all those counted by icmpOutErrors.
IcmpOutErrors	The number of ICMP messages that this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value does not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there might be no types of error that contribute to this counter's value.
IcmpOutDestUnreachs	The number of ICMP destination unreachable messages sent.
IcmpOutTimeExcds	The number of ICMP time exceeded messages sent.
IcmpOutParmProbs	The number of ICMP parameter problem messages sent.
IcmpOutSrcQuenchs	The number of ICMP source quench messages sent.
IcmpOutRedirects	The number of ICMP redirect messages sent. For a host, this is always zero, since hosts do not send redirects.
IcmpOutEchos	The number of ICMP echo (request) messages sent.
IcmpOutEchoReps	The number of ICMP echo reply messages sent.
IcmpOutTimestamps	The number of ICMP timestamp (request) messages.
IcmpOutTimestampReps	The number of ICMP timestamp reply messages sent.
IcmpOutAddrMasks	The number of ICMP address mask request messages sent.

Configure IPv6 routing

Note: IPv6 is supported on VLAN interfaces only, not on physical ports.

Configure the global IPv6 routing settings

You can configure the global IPv6 routing settings for the switch.

To enable IPv6 routing on the switch:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > IPv6 > Basic > Global Configuration**.

   The IPv6 Global Configuration page displays.
7. Click the IPv6 Unicast Routing **Enable** radio button or the **Disable** radio button to specify whether IPv6 unicast routing is globally enabled.
8. In the **Hop Limit** field, enter a value for the unicast hop count that is used in IPv6 packets originated by the node.

   The value is also included in router advertisements. The valid values for hops are 1 to 255, inclusive. The default is 64.
9. In the **ICMPv6 Rate Limit Error Interval** field, specify the number of ICMP error packets allowed per burst interval.

This value controls the ICMPv6 error packets. The default rate limit is 1000 mseconds. To disable ICMP rate limiting, set this field to 0. The valid rate interval must be in the range 0 to 2147483647 mseconds.

10. In the **ICMPv6 Rate Limit Burst Size** field, specify the number of ICMP error packets allowed per burst interval.

    This value controls the ICMP error packets. The default burst size is 100 packets. When the burst interval is 0, then the information in this field has not effect. The valid burst size is 1 to 200.

11. Click the **Apply** button.

    Your settings are saved.

View the IPv6 route table

To view the IPv6 route table:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Routing > IPv6 > Basic > Route Table**.

   The IPv6 Route Table page displays.

7. From the **Routes Displayed** menu, select one of the following options:
   - **All Routes**. Show all active IPv6 routes.
   - **Best Routes Only**. Show only the best active routes.
   - **Configured Routes Only**. Show only the manually configured routes.
8. To refresh the page with the latest information about the switch, click the **Refresh** button.

The following table describes the view-only data that is displayed.

Table 61. IPv6 Route Table information

Field	Description
Number of Routes	The total number of active routes in the route table.
IPv6 Prefix	The network prefix for the active route.
Prefix Length	The prefix length for the active route.
Protocol	The type of protocol for the active route.
Next Hop Interface	The interface over which the route is active. For a reject route, the next hop would be a *Null0* interface.
Next Hop IP Address	The next hop IPv6 address for the active route.
Preference	The route preference of the configured route.

Configure the IPv6 VLAN interface settings

To configure the IPv6 VLAN interface settings:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > IPv6 > Advanced > VLAN Configuration**.

   The VLAN Configuration page displays.
7. Select one or more interfaces by taking one of the following actions:

- To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
- To configure multiple interfaces with the same settings, select the check box associated with each interface.
- To configure all interfaces with the same settings, select the check box in the heading row.

8. From the **IPv6 Mode** menu, select **Enable** or **Disable**.

   When IPv6 mode is enabled, the interface is capable of IPv6 operation without a global address. In this case, an EUI-64-based link-local address is used.

9. From the **DHCPv6 Client Mode** menu, select to enable or disable the DHCPv6 client mode on an interface.

   Only one interface can function as a client.

10. From the **Stateless Address AutoConfig Mode** menu, select to enable or disable the stateless address autoconfiguration mode on an interface.
11. From the **Admin Mode** menu, select to enable or disable the IPv6 mode.

    When the IPv6 mode is enabled, the interface is capable of IPv6 operation without a global address. In this case, an EUI-64-based link-local address is used.

12. In the **MTU** field, specify the maximum transmit unit (MTU) for an interface.

    If you do not configure the IPv6 MTU, the switch uses the link MTU as the IPv6 MTU. The range of the MTU for the port routing interface is from 1280 to the link MTU. On a VLAN routing interface, you can set the IPv6 MTU as high as the highest-allowed jumbo frame. The range of MTU values for a VLAN routing interface is from 1280 to 9198.

    If the value is 0, the interface is not enabled for routing. Do not set the value to 0 if routing is enabled.

13. In the **Duplicate Address Detection Transmits** field, specify the number of duplicate address detection (DAD) transmits on an interface.

    The DAD transmits value must be in the range from 0 to 600.

14. In the **Life Time Interval** field, specify the router advertisement life time interval that is sent from the interface.

    This value must be greater than or equal to the maximum advertisement interval.
    0 means do not use the router as the default router. The range of router life time is from 0 to 9000.

15. In the **Adv NS Interval** field, specify the retransmission time field of router advertisements sent from the interface.

    A value of 0 means the interval is not specified for the router. The range of the neighbor solicit interval is from 1000 to 4294967295.

16. In the **Adv Reachable Interval** field, specify the router advertisement time.

    This is the time allocated to consider the neighbors reachable after ND confirmation. The range of reachable time is 0 to 3600000. The default is 0.

17. In the **Adv Interval** field, specify the maximum time allowed between sending router advertisements from the interface.

    The range of the maximum advertisement interval is 4 to 1800.

18. From the **Adv Managed Config Flag** menu, specify the setting for the router advertisement managed address configuration flag.

    When the selection is Enable, end nodes use DHCPv6. When the selection is Disable, end nodes autoconfigure addresses.

19. From the **Adv Other Config Flag** menu, select to enable or disable the router advertisement other stateful configuration flag.
20. From the **Router Preference** menu, specify the router preference advertisement on an interface.
21. From the **Adv Suppress Flag** menu, select to enable or disable the router advertisement suppression on an interface.
22. From the **Destination Unreachables** menu, select to enable or disable the mode for sending ICMPv6 destination unreachable messages on this interface.

    If this mode is disabled, the interface does not send ICMPv6 destination unreachable messages.

23. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only data that is displayed.

Table 62. IPv6 VLAN Configuration information

Field	Description
Routing Mode	The routing mode of an interface. The default is Disable.
Operational Mode	The operational state of an interface. The default value is Disable.
Link State	Indicates whether the link is up or down.

Configure an IPv6 prefix

For you to be able to configure these settings, you first must have configured a VLAN routing interface. For more information, see Create a routing interface with the VLAN Static Routing Wizard on page 253 or Manage a VLAN routing interface on page 254.

To configure an IPv6 prefix:

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

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

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

   The IPv6 Interface Selection page displays.
7. From the **Interface** menu, select the VLAN to be configured.

   When the selection is changed, the page refreshes, causing all fields to be updated for the newly selected VLAN.
8. In the **IPv6 Prefix** field, specify the IPv6 prefix for an interface.
9. In the **Prefix Length** field, specify the IPv6 prefix length for an interface.
10. From the **EUI64** menu, select **Enable** or **Disable** to indicate whether the specified 64-bit unicast prefix is enabled.
11. In the **Valid Life Time** field, specify the router advertisement per prefix time.

    This is the time allowed to consider the prefix valid for the purpose of on-link determination. The valid life time is 0 to 4294967295.
12. In the **Preferred Life Time** field, specify the router advertisement per prefix time.

    An autoconfigured address generated from this prefix is preferred. The preferred life time must be in the range 0 to 4294967295.
13. From the **Onlink Flag** menu, select **Enable** or **Disable** to specify whether the selected prefix can be used for on-link determination.
14. From the **Autonomous Flag** menu, select **Enable** or **Disable** to specify whether the selected prefix can be used for autonomous address configuration.
15. Click the **Add** button.

    The IPv6 address is added to the interface.

    The Current State field displays the state of the IPV6 address. The state is TENT if routing is disabled or DAD fails. The state is Active if the interface is active and DAD is successful.

View the IPv6 routing statistics

To view the IPv6 routing statistics:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > IPv6 > Advanced > Statistics**.

   The IPv6 Interface Selection page displays. The page also display the IPv6 Statistics section.
7. From the **Interface** menu, select the VLAN for which you want to display statistics.
8. To refresh the page with the latest information about the switch, click the **Refresh** button.

The following table describes the view-only IPv6 data that is displayed.

Table 63. IPv6 Statistics information

Field	Description
Total Datagrams Received	The total number of input datagrams received by the interface, including those received in error.
Received Datagrams Locally Delivered	The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed, which might not be the input interface for some of the datagrams.
Received Datagrams Discarded Due To Header Errors	The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, and so on.

Table 63. IPv6 Statistics information (continued)

Field	Description
Received Datagrams Discarded Due To MTU	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
Received Datagrams Discarded Due To No Route	The number of input datagrams discarded because no route could be found to transmit them to their destination.
Received Datagrams With Unknown Protocol	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed, which might not be the input interface for some of the datagrams.
Received Datagrams Discarded Due To Invalid Address	The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, ::0) and unsupported addresses (such as addresses with unallocated prefixes). For entities that are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Received Datagrams Discarded Dut To Truncated Data	The number of input datagrams discarded because datagram frame didn't carry enough data.
Received Datagrams Discarded Other	The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but that were discarded for reasons such as lack of buffer space. This counter does not include any datagrams discarded while awaiting reassembly.
Received Datagrams Reassembly Required	The number of IPv6 fragments received that needed to be reassembled at this interface. This counter is incremented at the interface to which these fragments were addressed, which might not be the input interface for some of the fragments.
Datagrams Reassembled	The number of IPv6 datagrams successfully reassembled. This counter is incremented at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the fragments.
Datagrams Failed To Reassemble	The number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, and so on). This is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed, which might not be the input interface for some of the fragments.
Datagrams Forwarded	The number of output datagrams that this entity received and forwarded to their final destinations. In entities that do not act as IPv6 routers, this counter includes only those packets that were source-routed through this entity, and the source-route processing was successful. For a successfully forwarded datagram the counter of the outgoing interface is incremented.
Datagrams Locally Transmitted	The number of datagrams that this entity successfully transmitted from this output interface.
Datagrams Transmit Failed	The number of datagrams that this entity failed to transmit successfully.

Table 63. IPv6 Statistics information (continued)

Field	Description
Datagrams Successfully Fragmented	The number of IPv6 datagrams that were fragmented at this output interface.
Datagrams Failed To Fragment	The number of output datagrams that could not be fragmented at this interface.
Datagrams Fragments Created	The number of output datagram fragments that were generated as a result of fragmentation at this output interface.
Multicast Datagrams Received	The number of multicast packets received by the interface.
Multicast Datagrams Transmitted	The number of multicast packets transmitted by the interface.

The following table describes the view-only ICMPv6 data that is displayed.

Table 64. ICMPv6 Statistics information

Field	Description
Total ICMPv6 Messages Received	The total number of ICMP messages received by the interface, which includes all those counted by IPv6IfIcmpInErrors. This interface is the interface to which the ICMP messages were addressed, which might not be the input interface for the messages.
ICMPv6 Messages With Errors Received	The number of ICMP messages that the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so on).
ICMPv6 Destination Unreachable Messages Received	The number of ICMP Destination Unreachable messages received by the interface.
ICMPv6 Messages Prohibited Administratively Received	The number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
ICMPv6 Time Exceeded Messages Received	The number of ICMP Time Exceeded messages received by the interface.
ICMPv6 Parameter Problem Messages Received	The number of ICMP Parameter Problem messages received by the interface.
ICMPv6 Packet Too Big Messages Received	The number of ICMP Packet Too Big messages received by the interface.
ICMPv6 Echo Request Messages Received	The number of ICMP Echo (request) messages received by the interface.
ICMPv6 Echo Reply Messages Received	The number of ICMP Echo Reply messages received by the interface.
ICMPv6 Router Solicit Messages Received	The number of ICMP Router Solicit messages received by the interface.
ICMPv6 Router Advertisement Messages Received	The number of ICMP Router Advertisement messages received by the interface.

Table 64. ICMPv6 Statistics information (continued)

Field	Description
ICMPv6 Neighbor Solicit Messages Received	The number of ICMP Neighbor Solicit messages received by the interface.
ICMPv6 Neighbor Advertisement Messages Received	The number of ICMP Neighbor Advertisement messages received by the interface.
ICMPv6 Redirect Messages Received	The number of ICMPv6 Redirect messaged received by the interface.
ICMPv6 Group Membership Query Messages Received	The number of ICMPv6 Group Membership Query messages received by the interface.
ICMPv6 Group Membership Response Messages Received	The number of ICMPv6 Group Membership Response messages received by the interface.
ICMPv6 Group Membership Reduction Messages Received	The number of ICMPv6 Group Membership Reduction messages received by the interface.
Total ICMPv6 Messages Transmitted	The total number of ICMP messages that this interface attempted to send. This counter includes all those counted by icmpOutErrors.
ICMPv6 Messages Not Transmitted Due To Error	The number of ICMP messages that this interface did not send due to problems discovered within ICMP such as a lack of buffers. This value does not include errors discovered outside the ICMP layer such as the inability of IPv6 to route the resultant datagram. In some implementations there might be no types of error that contribute to this counter's value.
ICMPv6 Destination Unreachable Messages Transmitted	The number of ICMP Destination Unreachable messages sent by the interface.
ICMPv6 Messages Prohibited Administratively Transmitted	Number of ICMP Destination Unreachable/Communication Administratively Prohibited messages sent.
ICMPv6 Time Exceeded Messages Transmitted	The number of ICMP Time Exceeded messages sent by the interface.
ICMPv6 Parameter Problem Messages Transmitted	The number of ICMP Parameter Problem messages sent by the interface.
ICMPv6 Packet Too Big Messages Transmitted	The number of ICMP Packet Too Big messages sent by the interface.
ICMPv6 Echo Request Messages Transmitted	The number of ICMP Echo (request) messages sent by the interface.
ICMPv6 Echo Reply Messages Transmitted	The number of ICMP Echo Reply messages sent by the interface.
ICMPv6 Router Solicit Messages Transmitted	The number of ICMP Neighbor Solicitation messages sent by the interface.
ICMPv6 Router Advertisement Messages Transmitted	The number of ICMP Router Advertisement messages sent by the interface.
ICMPv6 Neighbor Solicit Messages Transmitted	The number of ICMP Neighbor Solicitation messages sent by the interface.

Table 64. ICMPv6 Statistics information (continued)

Field	Description
ICMPv6 Neighbor Advertisement Messages Transmitted	The number of ICMP Neighbor Advertisement messages sent by the interface.
ICMPv6 Redirect Messages Transmitted	The number of Redirect messages sent.
ICMPv6 Group Membership Query Messages Transmitted	The number of ICMPv6 Group Membership Query messages sent.
ICMPv6 Group Membership Response Messages Transmitted	The number of ICMPv6 Group Membership Response messages sent.
ICMPv6 Group Membership Reduction Messages Transmitted	The number of ICMPv6 Group Membership Reduction messages sent.
ICMPv6 Duplicate Address Detects	The number of duplicate addresses detected by the interface.

View, search, or clear the IPv6 neighbor table

To view, search, or clear the IPv6 neighbor table:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > IPv6 > Advanced > Neighbor Table**.

   The IPv6 Neighbor Table page displays.

7. Use the **Search** menu and field to search for IPv6 routes by IPv6 address or interface number:
   - **Search by IPv6 address**. Select **IPv6 Address** from the **Search** menu. Enter the 128-byte hexadecimal IPv6 address in four-digit groups separated by colons, for example, 2001:231F:::1. Then click the **Go** button.

     If the address exists, the entry is displayed. An exact match is required.
   - **Search by Interface**. Select **Interface** from the **Search** menu. Enter the interface using the respective naming convention (for example, g1 or l1). Then click the **Go** button.

     If the address exists, the entry is displayed.
8. To clear the IPv6 neighbors on a selected interface or on all interfaces, click the **Clear** button.
9. To refresh the page with the latest information about the switch, click the **Refresh** button.

The following table describes the view-only data that is displayed.

Table 65. IPv6 Neighbor Table information

Field	Description
Interface	The interface whose settings are displayed in the current table row.
IPv6 Address	The IPv6 address of the neighbor or interface.
MAC Address	The MAC address associated with an interface.
isRtr	Indicates whether the neighbor is a router. If the neighbor is a router, the value is True. If the neighbor is not a router, the value is False.

Table 65. IPv6 Neighbor Table information (continued)

Field	Description
Neighbor State	The state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache: • **Incmp**. Address resolution is being performed on the entry. A neighbor solicitation message was sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message is not yet received. • **Reach**. Positive confirmation was received within the last Reachable Time milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent. • **Stale**. More than Reachable Time milliseconds elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent. • **Delay**. More than Reachable Time milliseconds elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE. • **Probe**. Seeks a reachability confirmation by resending neighbor solicitation messages every Retrans Timer milliseconds until a reachability confirmation is received.
Last Updated	The time since the address was confirmed to be reachable.

Configure an IPv6 static route

For you to be able to configure these settings, you first must have configured a VLAN routing interface. For more information, see Create a routing interface with the VLAN Static Routing Wizard on page 253 or Manage a VLAN routing interface on page 254.

To configure an IPv6 static route:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > IPv6 > Advanced > Static Route Configuration**.

   The Configuration Routes page displays.
7. In the **IPv6 Prefix** field, specify the IPv6 network prefix for the configured route.
8. In the **Prefix Length** field, specify the IPv6 prefix length for the configured route.
9. From the **Next Hop IPv6 Address Type** menu, select one of the following options:
   - **Global**. Select this option if the IPv6 address is a global IPv6 address.
   - **Link-Local**. Select this option if the next hop IPv6 address is a link-local IPv6 address. You must specify a next hop IPv6 address in the **Next Hop IPv6 Address** field.
   - **Static-Reject**. Select this option to create a static-reject route for a destination prefix. You do not need to specify a next hop IPv6 address.
10. If the selection from the **Next Hop IPv6 Address Type** menu is **Global** or **Link-Local**, enter the next hop IPv6 address in the **Next Hop IPv6 Address** field.
11. If the selection from the **Next Hop IPv6 Address Type** menu is **Link-Local**, from the **Interface** menu, select the interface that connects to the IPv6 next hop.
12. In the **Preference** field, specify the router preference.
13. Click the **Add** button.

    The route is added.

Note: For information about viewing routes in the IPv6 route table, see View the IPv6 route table on page 239.

Configure IPv6 route preferences

For you to be able to configure these settings, you first must have configured a VLAN routing interface. For more information, see Create a routing interface with the VLAN Static Routing Wizard on page 253 or Manage a VLAN routing interface on page 254.

You can configure the default preference for each protocol. These values are arbitrary values in the range of 1 to 255 and are independent of route metrics. Most routing protocols use a route metric to determine the shortest path known to the protocol, independent of any other protocol. The switch selects the route with the lowest preference value as the best route to a

destination. When multiple routes to a destination exist, the preference values are used to determine the preferred route. If these preference values routes are equal, the route with the best route metric is chosen. To avoid problems with mismatched metrics, you must configure different preference values for each of the protocols.

To configure IPv6 route preferences:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > IPv6 > Advanced > Route Preference**.

   The IPv6 Route Preference page displays.
7. In the **Static** field, specify the static route preference value for the router.

   The range is 1 to 255. The default value is 1.
8. Click the **Apply** button.

   Your settings are saved. The Local field displays the local preference.

Configure VLAN routing

You can configure the switch with some ports supporting VLANs and some ports supporting routing. You can also configure the switch to allow traffic on a VLAN to be treated as if the VLAN were a router port.

When a port is enabled for bridging (the default setting) rather than routing, all normal bridge processing is performed for an inbound packet, which is then associated with a VLAN. Its

MAC destination address (MAC DA) and VLAN ID are used to search the MAC address table. If routing is enabled for the VLAN, and the MAC DA of an inbound unicast packet is that of the internal bridge-router interface, the packet is routed. An inbound multicast packet is forwarded to all ports in the VLAN. If a routed VLAN receives the multicast packet, the packet is also forwarded on the internal bridge-router interface.

Because you can configure a port to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. You can use VLAN routing to allow more than one physical port to reside on the same subnet. You can also use VLAN routing if a VLAN spans multiple physical networks, or if you require additional segmentation or security. A port can either be a VLAN port or a router port, but not both. However, a VLAN port can be part of a VLAN that is itself a router port.

Create a routing interface with the VLAN Static Routing Wizard

The VLAN Static Routing Wizard lets you create a VLAN routing interface, configure the IP address and subnet mask for the interface, and add ports, LAGs, or both to the VLAN. With this wizard, you can do the following:

- Create a VLAN.
- Add ports to the newly created VLAN and remove selected ports from the default VLAN.
- Optionally, create a LAG, add ports to the LAG, then add the LAG to the newly created VLAN.
- Enable tagging on selected ports if the port is in another VLAN. Disable tagging if a selected port does not exist in another VLAN.
- Enable routing on the VLAN using the IP address and subnet mask entered.

To use the VLAN Static Routing Wizard:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Routing > VLAN > VLAN Routing Wizard**.

   The VLAN Static Routing Wizard page displays.

7. In the **VLAN ID** field, specify the VLAN ID that is associated with the VLAN.

   The range of the VLAN ID is 1 to 4093.

8. In the **IP Address** field, specify the IP address of the VLAN interface.
9. In the **Network Mask** field, specify the subnet mask of the VLAN interface.
10. In the Ports table, click each port once, twice, or three times to configure one of the following modes or reset the port to the default settings:
    - **T (Tagged)**. Select the ports on which all frames transmitted for this VLAN are tagged. The ports that are selected are included in the VLAN.
    - **U (Untagged)**. Select the ports on which all frames transmitted for this VLAN are untagged. The ports that are selected are included in the VLAN.

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

11. In the LAG table, click each LAG once, twice, or three times to configure one of the following modes or reset the LAG to the default settings:
    - **T (Tagged)**. Select the LAGs on which all frames transmitted for this VLAN are tagged. The LAGs that are selected are included in the VLAN.
    - **U (Untagged)**. Select the LAGs on which all frames transmitted for this VLAN are untagged. The LAGs that are selected are included in the VLAN.

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

12. Click the **Apply** button.

    Your settings are saved.

Manage a VLAN routing interface

You can add and manage an existing VLAN (see Configure VLAN settings on page 149) as a new VLAN routing interface. You can also manage an existing VLAN routing interface that you added with the wizard (see Create a routing interface with the VLAN Static Routing Wizard on page 253).

To add routing to a VLAN interface or change an existing VLAN routing interface:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > VLAN > VLAN Routing Configuration**.

   The VLAN Routing Configuration page displays.
7. From the **VLAN** menu, select the VLAN.

   This menu displays the IDs of all VLANs that are configured on the switch.
8. In the **IP Address** field, enter the IP address to be configured for the VLAN routing interface.
9. In the **Subnet Mask** field, enter the subnet mask to be configured for the VLAN routing interface.
10. In the **IP MTU** field, specify the maximum size of IP packets that can be sent on an interface.

    The range is from 68 bytes to the link MTU. When the IP MTU is not configured, the switch uses the link MTU as the IP MTU. The link MTU is the maximum frame size minus the length of the Layer 2 header.
11. From the **ICMP Redirects** menu, select **Enable** or **Disable**.

    If you enable ICMP Redirects, the switch can forward ICMP Redirect messages.
12. Click the **Add** button.

    The VLAN routing interface is added for the selected VLAN ID.

The following table describes the view-only information displayed on the page.

Table 66. VLAN Routing Configuration information

Field	Description
Port	The interface that is assigned to the VLAN for routing.

Table 66. VLAN Routing Configuration information (continued)

Field	Description
MAC Address	The MAC address that is assigned to the VLAN routing interface.
Routing Mode	Indicates whether routing is enabled for the VLAN routing interface.

Delete a VLAN routing interface

You can delete a VLAN routing interface that you no longer need.

To delete a VLAN routing interface:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > VLAN > VLAN Routing Configuration**.

   The VLAN Routing Configuration page displays.
7. Select the check box for the VLAN routing interface.
8. Click the **Delete** button.

   The VLAN routing interface is removed. The VLAN itself is not removed.

Configure router discovery for a VLAN routing interface

By default, a VLAN routing interface does not send router advertisements.You can enable the router advertisements for a VLAN routing interface and configure the setting for the router advertisements.

To configure router discovery for a VLAN routing interface:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > Router Discovery > Router Discovery Configuration**.

   The Router Discovery Configuration page displays.
7. Select the check box for a VLAN routing interface.

   If you did not yet configure a VLAN routing interface, none are displayed.
8. From the **Advertise Mode** menu, select **Enable** or **Disable**.

   If you select Enable, router advertisements are transmitted from the selected interface.
9. In the **Advertise Address** field, specify the IP address that must be advertised.
10. In the **Maximum Advertise Interval** field, enter the maximum time (in seconds) allowed between router advertisements sent from the interface.

    The default value is 600.

11. In the **Minimum Advertise Interval** field, enter the minimum time (in seconds) allowed between router advertisements sent from the interface.

    The value must be in the range of 3 to 1800. The default value is 450.

12. In the **Advertise Lifetime** field, enter the value (in seconds) to be used as the lifetime field in router advertisements sent from the interface.

    This is the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts. The default value is 1800.

13. In the **Preference Level** field, specify the preference level of the router as a default router relative to other routers on the same subnet.

    Higher numbered addresses are preferred. You must enter an integer. The default value is 0.

14. Click the **Apply** button.

    Your settings are saved.

Manage routes and view the routing table

The routing table collects routes from multiple sources: static routes and local routes. The routing table can learn multiple routes to the same destination from multiple sources. The routing table lists all routes.

Manually add a route and view the routing table

To manually add a default route or static route and view the routing table:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Routing > Routing Table > Route Configuration**.

   The Configure Routes page displays.

7. From the **Route Type** menu, select one of the following route types.
   - **Static**. Creates a static route. You must specify the network address, subnet mask, next hop address, and preference.
   - **Default Route**. Creates a default route. You must specify the next hop address and preference.
8. Depending on the type of route that you are creating, specify the following information:
   - In the **Network Address** field, specify the IP route prefix for the destination.
   - In the **Subnet Mask** field, specify the portion of the IP interface address that identifies the attached network.

     This is also referred to as the subnet/network mask.
   - In the **Next Hop IP Address** field, specify the outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

     The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.
   - In the **Preference** field, specify the preference, which is an integer value from 1 to 255.

     You can specify the preference value (sometimes called administrative distance) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you control whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.
   - In the **Description** field, enter a description for the route.

     The description must consist of alphanumeric, hyphen, or underscore characters and can be up to 31 characters in length.
9. Click the **Add** button.

   The static route is added to the switch.

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

The following table describes the view-only data that is displayed.

Table 67. Learned Routes information

Field	Description
Network Address	The IP route prefix for the destination.
Subnet Mask	The portion of the IP interface address that identifies the attached network (also referred to as the subnet or network mask).
Protocol	The protocol that created the specified route. The possibilities are one of the following: • Local • Static
Route Type	The route type can be Connected, Static, or Dynamic, depending on the protocol.
Next Hop Interface	The outgoing router interface to use when forwarding traffic to the destination.
Next Hop Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.
Preference	The preference is an integer value from 0 to 255. The user can specify the preference value (sometimes called *administrative distance*) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you control whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.
Metric	The administrative cost of the path to the destination. If no value is entered, the default is 1. The range is 0–255.

Modify a route

You can modify an existing route.

To modify an existing route:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > Routing Table > Route Configuration**.

   The Configure Routes page displays.
7. Select the check box for the route that you want to modify.
8. Modify the settings.

   For more information, see Manually add a route and view the routing table on page 258.
9. Click the **Apply** button.

   Your settings are saved.

Delete a route

You can delete a route that you no longer need.

To delete a route:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

The System Information page displays.

6. Select **Routing > Routing Table > Route Configuration**.

   The Configure Routes page displays.

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

   The route is deleted.

Configure Address Resolution Protocol

The Address Resolution Protocol (ARP) associates a Layer 2 MAC address with a Layer 3 IPv4 address. ARP is a part of the Internet Protocol (IP) and is used to translate an IP address to a media (MAC) address, defined by a LAN such as an Ethernet LAN.

The switch supports both dynamic and manual ARP configurations. With a manual ARP configuration, you can statically add entries to the ARP table.

A device that sends an IP packet must learn the MAC address of the IP destination, or, if the destination is not on the same subnet, of the next hop router. The device broadcasts an ARP request packet, to which the intended recipient responds with a unicast ARP reply that contains its MAC address. The device then uses the MAC address in the destination address field of the Layer 2 header that is prepended to the IP packet and sent to the recipient. Each device in a network maintains its ARP cache locally.

The switch learns ARP cache entries by examining the source information in the ARP packet payload fields, regardless of whether it is an ARP request or a response. In that way, when an ARP request is broadcast to all stations on a LAN segment or VLAN, each recipient can store the sender's IP and MAC address in its ARP cache. Normally, only the requestor receives an ARP response (a unicast message) and stores the sender's information in its ARP cache. The most recent information always replaces existing content in the ARP cache.

A device can be moved in a network, which means that the device's IP address that was associated with one MAC address is now associated with another MAC address. A device can also disappear from the network altogether (for example, it was reconfigured, disconnected, or powered off). These situations cause stale information in the ARP cache. Therefore, entries are updated or periodically refreshed to determine if an address still exists. If an entry was identified as a sender of an ARP packet, the entry can be removed from the ARP cache. You can configure an age-out interval that determines how long an entry that is not updated remains in the ARP cache.

View the ARP cache

You can view ARP entries in the ARP cache. The ARP cache is a table that lists the remote connections that were recently detected by the switch.

To view entries in the ARP cache:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > ARP > Basic > ARP Cache**.

   The Management VLAN ARP Cache page displays.
7. Navigate through the table by doing the following:
   - From the **Rows per page** menu, select how many table entries are displayed per page.

     Possible values are **20**, **50**, **100**, **200**, and **All**. If you select **All**, the browser might be slow to display the information.
   - Click the **<** button to display the previous page of the table data entries.
   - Click the **>** button to display the next page of the table data entries.
8. To refresh the page, click the **Refresh** button.

The following table describes the view-only information displayed on the page.

Table 68. ARP cache information

Field	Description
Management VLAN ARP Cache	
IP Address	The IP address associated with the system's MAC address. This must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.
Port	The associated interface ID of the connection.
MAC Address	The unicast MAC address of the device. The address is six two-digit hexadecimal numbers separated by colons, for example, 00:06:29:32:81:40.
Routing VLANs ARP Cache	
IP Address	The IP address. It must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.
Interface	The routing interface associated with the ARP entry.
MAC Address	The unicast MAC address of the device. The address is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
Type	The type of ARP entry. Possible values are as follows: • **Local**. An ARP entry associated with one of the switch's routing interface's MAC addresses. • **Gateway**. A dynamic ARP entry whose IP address is that of a router. • **Static**. An ARP entry configured by the user. • **Dynamic**. An ARP entry that was learned by the router.
Age	The time since the entry was last refreshed in the ARP table (in seconds).

Manually add an entry to the ARP table

You can manually add an entry to the ARP table.

To manually add an entry to the ARP table:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > ARP > Advanced > ARP Create**.

   The Static ARP Configuration page displays.
7. In the **IP Address** field, specify an IP address.

   This must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.
8. In the **MAC Address** field, specify the unicast MAC address of the device.

   Enter the address as six two-digit hexadecimal numbers separated by colons, for example, 00:06:29:32:81:40.
9. Click the **Add** button.

   The static ARP entry is added to the switch.

The following table describes the view-only information displayed on the page. You can navigate through the table by doing the following:

- From the **Rows per page** menu, select how many table entries are displayed per page.

  Possible values are **20**, **50**, **100**, **200**, and **All**. If you select **All**, the browser might be slow to display the information.
- Click the **<** button to display the previous page of the table data entries.
- Click the **>** button to display the next page of the table data entries.

Table 69. Routing VLANs ARP Cache information

Field	Description
IP Address	The IP address. It must be the IP address of a device on a subnet attached to one of the switch’s existing routing interfaces.
Interface	The routing interface associated with the ARP entry.
MAC Address	The unicast MAC address of the device. The address is six two-digit hexadecimal numbers separated by colons, for example, 00:06:29:32:81:40.

Table 69. Routing VLANs ARP Cache information (continued)

Field	Description
Type	The type of ARP entry. Possible values are as follows: • **Local**. An ARP entry associated with one of the switch's routing interface's MAC addresses. • **Gateway**. A dynamic ARP entry whose IP address is that of a router. • **Static**. An ARP entry configured by the user. • **Dynamic**. An ARP entry that was learned by the router.
Age	The time since the entry was last refreshed in the ARP table (in seconds).

Delete a static ARP entry

You can delete a static ARP entry that you no longer need.

To delete a static ARP entry:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > ARP > Advanced > ARP Create**.

   The Static ARP Configuration page displays.
7. Select the check box for the entry.
8. Click the **Delete** button.

   Your settings are saved. The entry is removed.

View or globally configure the ARP table

You can change the global settings for the ARP table.

To view or configure the ARP table:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > ARP > Advanced > Global ARP Configuration**.

   The Global ARP Configuration page displays.
7. In the **Age Time** field, enter the time in seconds that a dynamic ARP entry remains in the ARP table before aging out.

   The range is 15 to 21600 seconds. The default value is 1200 seconds.
8. In the **Response Time** field, enter the time in seconds that the device waits for an ARP response to an ARP request that it sends. The range for this field is 1 to 10 seconds. The default value is 1 second.
9. In the **Retries** field, enter the maximum number of times an ARP request is retried after an ARP response is not received.

   The number includes the initial ARP request. The range for this field is 0 to 10. The default value is 4.
10. In the **Cache Size** field, specify the maximum number of entries allowed in the ARP table.

    This number includes all IPv4 ARP and IPv6 Neighbor static and dynamic entries. The range for this field is 79 to 479. The default value is 479.
11. Select the Dynamic Renew **Enable** or **Disable** radio button.

When enabled, the ARP component automatically attempts to renew dynamic ARP entries when they age out. The default setting is Enable.

12. Click the **Apply** button.

    Your settings are saved.

Remove ARP entries from the ARP cache

You can remove entries from the ARP cache.

To remove entries from the ARP cache:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Routing > ARP > Advanced > ARP Entry Management**.

   The ARP Entry Management page displays.
7. From the **Remove From Table** menu, select the type of ARP entry to be deleted:
   - **All Dynamic Entries**
   - **All Dynamic and Gateway Entries**
   - **Specific Dynamic/Gateway Entry**. Lets you specify the IP address to be removed.
   - **Specific Static Entry**. Lets you specify the IP address to be removed.
8. If you select **Specific Dynamic/Gateway Entry** or **Specific Static Entry**, in the **Remove IP Address** field, enter the IP address to be removed.
9. Click the **Apply** button.

   Your settings are saved.

5

Configure Quality of Service

This chapter contains the following sections:

- Quality of Service concepts
- Manage Class of Service
- Manage Differentiated Services

Quality of Service concepts

In a switch, each physical port consists of one or more queues for transmitting packets on the attached network. Multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets are held in the queue until the scheduler authorizes the queue for transmission. As queues become full, packets can no longer be held for transmission and are dropped by the switch.

Quality of Service (QoS) is a means of providing consistent, predictable data delivery by distinguishing packets with strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given special treatment in a QoS-capable network. With this in mind, all elements of the network must be QoS capable. The presence of at least one node that is not QoS capable creates a deficiency in the network path, and the performance of the entire packet flow is compromised.

Manage Class of Service

The Class of Service (CoS) queueing feature lets you directly configure certain aspects of switch queueing. This provides the desired QoS behavior for different types of network traffic when the complexities of DiffServ are not required. The priority of a packet arriving at an interface can be used to steer the packet to the appropriate outbound CoS queue through a mapping table. CoS queue characteristics that affect queue mapping, such as minimum guaranteed bandwidth or transmission rate shaping, are user configurable at the queue (or port) level.

Eight queues per port are supported.

CoS configuration concepts

You can set the Class of Service trust mode for an interface. Each port in the switch can be configured to trust one of the packet fields (802.1p or IP DSCP), or to not trust any packet's priority designation (untrusted mode). If the port is set to a trusted mode, it uses a mapping table appropriate for the trusted field being used. This mapping table indicates the CoS queue to which the packet must be forwarded on the appropriate egress port. Of course, the trusted field must exist in the packet for the mapping table to be of any use. If this is not the case, default actions are performed. These actions involve directing the packet to a specific CoS level configured for the ingress port as a whole, based on the existing port default priority as mapped to a traffic class by the current 802.1p mapping table.

Alternatively, when a port is configured as untrusted, it does not trust any incoming packet priority designation and uses the port default priority value instead. All packets arriving at the

ingress of an untrusted port are directed to a specific CoS queue on the appropriate egress ports, in accordance with the configured default priority of the ingress port. This process is also used for cases where a trusted port mapping cannot be honored, such as when a non-IP packet arrives at a port configured to trust the IP DSCP value.

Configure the global CoS settings

A global configuration setting is automatically applied to all interfaces on the switch.

To configure CoS trust mode settings on all interfaces:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **QoS > CoS > Basic > CoS Configuration**.

   The Cos Configuration page displays.
7. Either configure the same CoS trust mode settings for all CoS-configurable interfaces or configure CoS settings per interface.

   By default, the Global radio button is selected.
   - To configure the same CoS trust mode settings for all CoS configurable interfaces, do the following:
     a. Select the **Global** radio button.
     b. From the **Global Trust Mode** menu, select one of the following trust mode options for ingress traffic on the switch:
        - **Untrusted**. Do not trust any CoS packet marking at ingress.

- **802.1p**. The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of seven internal hardware priority queues. The default mode is 802.1p.
- **DSCP**. The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.

- To configure CoS settings per interface, do the following:
  a. Select the **Interface** radio button.
  b. From the **Interface Trust Mode** menu, select one of the following trust mode options:
     - **Untrusted**. Do not trust any CoS packet marking at ingress.
     - **802.1p**. The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of seven internal hardware priority queues. The default mode is 802.1p.
     - **DSCP**. The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.

8. Click the **Apply** button.

   Your settings are saved.

Configure the CoS settings for an interface

You can configure the trust mode for one or more interfaces and apply an interface shaping rate to all interfaces or to a specific interface.

To configure CoS settings for an interface:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

The System Information page displays.

6. Select **QoS > CoS > Advanced > CoS Interface Configuration**.

   The CoS Interface Configuration page displays.

7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. From the **Interface Trust Mode** menu, select one of the following trust mode options for ingress traffic on the selected interfaces:
   - **Untrusted**. Do not trust any CoS packet marking at ingress.
   - **802.1p**. The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of seven internal hardware priority queues. The default value is 802.1p.
   - **DSCP**. The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.
10. In the **Interface Shaping Rate** field, specify the maximum egress bandwidth allowed.

    This setting is used to shape the outbound transmission rate in increments of 1 percent in a range of 0–100. This value is controlled independently of any per-queue maximum bandwidth configuration. It is effectively a second-level shaping mechanism. The default value is 0. The value 0 means that the maximum is unlimited.

11. Click the **Apply** button.

    Your settings are saved.

Configure the 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.

For information about configuring CoS queue settings globally, see Configure the global CoS settings on page 271.

To configure CoS queue settings for an interface:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **QoS > CoS > Advanced > Interface Queue Configuration**.

   The Interface Queue Configuration page displays.

7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. From the **Queue ID** menu, select the queue from 0 to 7 to be configured.
10. In the **Minimum Bandwidth** field, specify the minimum guaranteed bandwidth allotted to the queue on the interface.

    Setting this value higher than its corresponding maximum bandwidth automatically increases the maximum to the same value. The default value is 0. The range is from 0 to

100 in increments of 1. The value 0 means that no guaranteed minimum bandwidth is applied. The sum of the individual minimum bandwidth values for all queues on the selected interface cannot exceed the maximum (100).

The setting applies only to the queue that you select from the **Queue ID** menu.

11. From the **Scheduler Type** menu, select one of the following options:
    - **Strict**. The interface services traffic with the highest priority on a queue first.
    - **Weighted**. The interface uses weighted round robin to associate a weight to each queue. This is the default setting.

    The Queue Management Type field displays the queue depth management technique that is used for queues on the interface. By default, this method is Taildrop, irrespective of your selection from the **Scheduler Type** menu.
12. Click the **Apply** button.

    Your settings are saved.

Map 802.1p priorities to queue

You can view or change which internal traffic classes are mapped to the 802.1p priority class values in Ethernet frames that the device receives. The priority-to-traffic class mappings can be applied globally or per interface. The mapping allows the switch to group various traffic types (for example, data or voice) based on their latency requirements and give preference to time-sensitive traffic.

To map 802.1p priorities to queues:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.

6. Select **QoS > CoS > Advanced > 802.1p to Queue Mapping**.

   The 802.1p to Queue Mapping page displays.

7. Either configure the same CoS trust mode settings for all CoS-configurable interfaces or configure CoS settings per interface by selecting an interface from the **Interface** menu.

   By default, the Global radio button is selected, and your selection is applied to all interfaces.

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

   The 802.1p Priority row contains traffic class selectors for each of the eight 802.1p priorities to be mapped. The priority goes from low (0) to high (7). For example, traffic with a priority of 0 is for most data traffic and is sent using best effort. Traffic with a higher priority, such as 7, might be time-sensitive traffic, such as voice or video.

   The values in the menu under each priority represent the traffic class. The traffic class is the hardware queue for a port. Higher traffic class values indicate a higher queue position. Before traffic in a lower queue is sent, it must wait for traffic in higher queues to be sent.

9. Click the **Apply** button.

   Your settings are saved.

Map DSCP values to queues

You can map an internal traffic class to a DSCP value.

To map DSCP values to queues:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **QoS > CoS > Advanced > DSCP to Queue Mapping**.

   The DSCP to Queue Mapping page displays.

7. For each DSCP value, select from the corresponding **Queue** menu which internal traffic class must be mapped to the DSCP value.

   The traffic class is the hardware queue for a port. Higher traffic class values indicate a higher queue position. Before traffic in a lower queue is sent, it must wait for traffic in higher queues to be sent.

   The allowed Per Hop Behavior (PHBs) values, apart from other DSCP experimental values, are as follows:

   - **Class Selector (CS) PHB**. These values are based on IP precedence.
   - **Assured Forwarding (AF) PHB**. These values define four main levels to sort and manipulate some flows within the network.
   - **Expedited Forwarding (EF) PHB**. These values are used to prioritize traffic for real-time applications. In many situations, if the network exceeded traffic and you need some bandwidth guaranteed for an application, the EF traffic must receive this rate independently of the intensity of any other traffic attempting to transit the node.

8. Click the **Apply** button.

   Your settings are saved.

Manage Differentiated Services

Differentiated Services (DiffServ) support allows traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors.

Standard IP-based networks provide best-effort data delivery service. Best-effort service implies that the network delivers the data in a timely fashion, although there is no guarantee. If congestion occurs, packets might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email and file transfers, a slight degradation in service is acceptable and in many cases unnoticeable. However, any degradation of service can negatively affect applications with strict timing requirements, such as voice and multimedia.

Defining DiffServ

To use DiffServ for QoS, you must first define the following categories and their criteria:

1. **Class**. Create classes and define class criteria.
2. **Policy**. Create policies, associate classes with policies, and define policy statements.
3. **Service**. Add a policy to an inbound interface.

Packets are classified and processed based on defined criteria. The classification criteria are defined by a class. The processing is defined by a policy's attributes. Policy attributes can be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs. A policy can contain multiples classes. When the policy is active, the actions taken depend on which class matches the packet.

Note the following about the DiffServ process:

- Packets are filtered and processed based on defined criteria. The filtering criteria is defined by a class. The processing is defined by a policy's attributes. Policy attributes can be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs.
- The configuration process begins with defining one or more match criteria for a class. Then one or more classes are added to a policy. Policies are then added to interfaces.

Packet processing begins by testing the match criteria for a packet. The *All* class type option specifies that each match criteria within a class must evaluate to true for a packet to match that class. The *Any* class type option specifies that at least one match criteria must evaluate to true for a packet to match that class. Classes are tested in the order in which they were added to the policy. A policy is applied to a packet when a class match within that policy is found.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **QoS > DiffServ > Advanced > DiffServ Configuration**.

   The DiffServ Configuration page displays.

7. Select the administrative mode for DiffServ:
   - **Enable**. Differentiated services are active. This is the default setting.
   - **Disable**. The DiffServ configuration is retained and can be changed but is not active.

8. Click the **Apply** button.

   Your settings are saved.

The following table describes the information displayed in the Status table on the DiffServ Configuration page.

Table 70. 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 specified interfaces) out of the total allowed on the switch.

Configure a DiffServ class

You can add a new DiffServ class name, or rename or delete an existing class. You can also define the criteria to associate with a DiffServ class. As packets are received, these DiffServ classes are used to prioritize packets. You can set up multiple match criteria in a class. The logic is a Boolean logical AND for this criteria. After creating a class, click the class link to the Class page.

Add and configure a DiffServ class

To create and configure a DiffServ class:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **QoS > DiffServ > Advanced > Class Configuration**.

   The Class Configuration page displays.
7. In the **Class Name** field, enter a class name.

   The **Class Name** field also lists all the existing DiffServ class names, from which you can select one for modification or deletion. The class name can be 1 to 31 alphanumeric characters in length.
8. From the **Class Type** menu, select the class type.

   The switch supports only the class type value **All**, which means that all the various match criteria defined for the class are satisfied for a packet match. **All** signifies the logical AND statement of all the match criteria. You can select the class type only when you are creating a new class. After the class is created, the **Class Type** field becomes nonconfigurable.
9. Click the **Add** button.

   The new class is added.
10. After creating the class, click the class name, which is a hyperlink.

    The page on which you can define the class configuration displays.
11. Define the criteria that must be associated the DiffServ class:
    - **Match Every**. Select this radio button to add a match condition that considers all packets to belong to the class. The only selection from the **Match Every** menu is **Any**.
    - **Reference Class**. Select this radio button to reference another class for criteria. The match criteria defined in the reference class function as match criteria in addition to the match criteria that you define for the selected class. After you select the radio button, the classes that can be referenced are displayed. Select the class to reference. A class can reference at most one other class of the same type.

- **Class of Service**. Select this radio button to require the Class of Service (CoS) value in an Ethernet frame header to match the specified CoS value. This option lists all the values for the Class of Service match criterion in the range 0 to 7 from which one can be selected.
- **VLAN**. Select this radio button to require a packet's VLAN ID to match a VLAN ID or a VLAN ID within a continuous range. If you configure a range, a match occurs if a packet's VLAN ID is the same as any VLAN ID within the range. The VLAN value is in the range of 0–4093.
- **Ethernet Type**. Select this radio button to require the EtherType value in the Ethernet frame header to match the specified EtherType value. After you select the radio button, specify the EtherType keyword from the list of common protocols that are mapped to their Ethertype value.
- **Source MAC**. Select this radio button to require a packet's source MAC address to match the specified MAC address. After you select this radio button, use the following fields to configure the source MAC address match criteria:
  - **Address**. The source MAC address to match. The source MAC address is specified as six two-digit hexadecimal numbers separated by colons.
  - **Mask**. The MAC mask, which specifies the bits in the source MAC address to compare against the Ethernet frame. Use Fs and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.
- **Destination MAC**. Select this radio button to require a packet's destination MAC address to match the specified MAC address. After you select the radio button, use the following fields to configure the destination MAC address match criteria:
  - **Address**. The destination MAC address to match. The destination MAC address is specified as six two-digit hexadecimal numbers separated by colons.
  - **Mask**. The MAC mask, which specifies the bits in the destination MAC address to compare against an Ethernet frame. Use Fs and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.
- **Protocol Type**. Select this radio button to require a packet's Layer 4 protocol to match the specified protocol, which you must select from the menu. The menu includes **Other** as a selection, which lets you enter a protocol number from 0 to 255.
- **Source IP**. Select this radio button to require a packet's source IP address to match the specified IP address. After you select the radio button, use the following fields to configure the source IP address match criteria:
  - **Address**. The source IP address format to match in dotted-decimal.

  - **Mask**. The bit mask in IP dotted-decimal format indicating which parts of the source IP address to use for matching against packet content.
- **Source L4 Port**. Select this radio button to require a packet's TCP/UDP source port to match the specified protocol, which you must select from the menu. The range is 0 to 65535. The menu includes **Other** as an option for unnamed ports.
- **Destination IP**. Select this radio button to require a packet's destination IP address to match the specified IP address. After you select the radio button, use the following fields to configure the destination IP address match criteria:
  - **Address**. The destination IP address format to match in dotted-decimal.
  - **Mask**. The bit mask in IP dotted-decimal format indicating which parts of the destination IP address to use for matching against packet content.
- **Destination L4 Port**. Select this radio button to require a packet's TCP/UDP destination port to match the specified protocol, which you must select from the menu. The range is 0 to 65535. The menu includes **Other** as an option for unnamed ports.
- **IP DSCP**. Select this radio button to require the packet's IP DiffServ Code Point (DSCP) value to match the specified IP DSCP keyword code, which you must select from the menu. The menu includes **Other** as a selection, which lets you enter an IP DSCP value from 0 to 63. The DSCP value is defined as the high-order 6 bits of the Service Type octet in the IP header.
- **Precedence Value**. Select this radio button to require the packet's IP precedence value to match the specified number from 0 to 7, which you must select from the menu. The IP Precedence field in a packet is defined as the high-order 3 bits of the Service Type octet in the IP header.
- **IP ToS**. Select this radio button to require the packet's Type of Service (ToS) bits in the IP header to match the specified value. The IP ToS field in a packet is defined as all 8 bits of the service type octet in the IP header. After you select the radio button, use the following fields to configure the ToS match criteria:
  - **Bits Value**. Enter a two-digit hexadecimal number octet value in the range from 00 to ff to match the bits in a packet's ToS field.
  - **Bit Mask**. Specify the bit positions that are used for comparison against the IP ToS field in a packet.

12. Click the **Apply** button.

Your settings are saved.

The following table describes the view-only information displayed in the Class Summary section at the bottom of the DiffServ Advanced Class Configuration page.

Table 71. DiffServ Class Configuration, Class Summary information

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

Rename an existing DiffServ class

To rename an existing DiffServ class:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **QoS > DiffServ > Advanced > Class Configuration**.

   The Class Name page displays.
7. Select the check box next to the class name.
8. In the **Class Name** field, specify the new name.
9. Click the **Apply** button.

   Your settings are saved.

Change the criteria for an existing DiffServ class

To change the criteria for an existing DiffServ class:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **QoS > DiffServ > Advanced > Class Configuration**.

   The Class Name page displays.
7. Click the class name, which is a hyperlink.

   The page on which you can change the class configuration displays.
8. Change the class configuration as needed.
9. Click the **Apply** button.

   Your settings are saved.

Delete a DiffServ class

To delete a DiffServ class:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.

6. Select **QoS > DiffServ > Advanced > Class Configuration**.

   The Class Name page displays.

7. Select the check box next to the class name.
8. Click the **Delete** button.

   The class is removed.

Configure DiffServ IPv6 class settings

The switch supports QoS ACL and DiffServ functionality for IPv6 by providing support for IPv6 packet classification. An IPv6 ACL serves the same purpose as an IPv4 ACL.

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 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 a host addresses. Packets that match an IPv6 classifier can be marked with the IP DSCP field in the traffic class octet.

You can also assign an IPv6 ACL with a DiffServ assignment to LAG interfaces.

Create and configure an IPv6 DiffServ class

To create and configure an IPv6 DiffServ class:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

The IPv6 Class Configuration page displays.

7. Enter a class name in the **Class Name** field.

   The **Class Name** field also lists all the existing IPv6 class names, from which one can be selected for modification or deletion.

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

   The switch supports only the class type value **All**, which means that all the various match criteria defined for the class are satisfied for a packet match. **All** signifies the logical AND statement of all the match criteria. You can select the class type only when you are creating a new class. After the class is created, the **Class Type** field becomes nonconfigurable.

9. Click the **Add** button.

   The new class is added.

10. After creating the class, click the class name, which is a hyperlink.

    The page on which you can define the class configuration displays.

11. Define the criteria that must be associated the IPv6 DiffServ class:
    - **Match Every**. Select this radio button to add a match condition that considers all packets to belong to the class. The only selection from the **Match Every** menu is **Any**.
    - **Reference Class**. Select this radio button to reference another class for criteria. The match criteria defined in the reference class function as match criteria in addition to the match criteria that you define for the selected class. After selecting this option, the classes that can be referenced are displayed. Select the class to reference. A class can reference at most one other class of the same type.
    - **Protocol Type**. Select this radio button to require a packet's Layer 4 protocol to match the specified protocol, which you must select from the menu. The menu includes **Other** as a selection, which lets you enter a protocol number from 0 to 255.
    - **Source Prefix/Length**. Select this radio button to require a packet's source prefix and prefix length to match the specified source IPv6 prefix and prefix length. Prefix must always be specified with the prefix length. The prefix can be in the hexadecimal range from 0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF and the prefix length can be in the range from 0 to 128.
    - **Source L4 Port**. Select this radio button to require a packet's TCP/UDP source port to match the specified protocol, which you must select from the menu. The range is 0 to 65535. The menu includes **Other** as an option for unnamed ports.
    - **Destination Prefix/Length**. Select this radio button to require a packet's destination prefix and prefix length to match the specified source IPv6 prefix and prefix length. Prefix must always be specified with the prefix length. The prefix can be in the hexadecimal range from 0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF and the prefix length can be in the range from 0 to 128.
    - **Destination L4 Port**. Select this radio button to require a packet's TCP/UDP destination port to match the specified protocol, which you must select from the menu. The range is 0 to 65535. The menu includes **Other** as an option for unnamed ports.

- **Flow Label**. Select this radio button to require a packet's flow label to match the specified flow label. The flow label is a 20-bit number that is unique to an IPv6 packet and that is used by end stations to signify QoS handling in routers. The flow label can be specified in the range from 0 to 1048575.
- **IP DSCP**. Select this radio button to require the packet's IP DiffServ Code Point (DSCP) value to match the specified IP DSCP keyword code, which you must select from the menu. The menu includes **Other** as a selection, which lets you enter an IP DSCP value from 0 to 63. The DSCP value is defined as the high-order 6 bits of the Service Type octet in the IP header.

12. Click the **Apply** button.

Your settings are saved.

The following table describes the view-only information that is displayed in the Class Summary section.

Table 72. 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.

Rename an existing IPv6 DiffServ class

To rename an existing IPv6 DiffServ class:

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

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

2. Launch a web browser.

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:

- Enter your device admin password.
- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

The System Information page displays.

6. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

The Class Name page displays.

7. Select the check box next to the class name.
8. In the **Class Name** field, specify the new name.
9. Click the **Apply** button.

   Your settings are saved.

Change the criteria for an existing IPv6 DiffServ class

To change the criteria for an existing IPv6 DiffServ class:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

   The Class Name page displays.
7. Click the class name, which is a hyperlink.

   The page on which you can change the class configuration displays.
8. Change the class configuration as needed.
9. Click the **Apply** button.

   Your settings are saved.

Delete an IPv6 DiffServ class

To delete an IPv6 DiffServ class:

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

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

   The Class Name page displays.
7. Select the check box next to the class name.
8. Click the **Delete** button.

   The class is removed.

Configure a DiffServ Policy

You can associate a collection of classes with one or more policies.

Create and configure a DiffServ policy

To create and configure a DiffServ policy:

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

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **QoS > DiffServ > Advanced > Policy Configuration**.

   The Policy Configuration page displays.
7. Enter a policy name in the **Policy Name** field.

   You cannot specify the policy type. By default, the policy type is In, indicating that the policy applies to ingress packets.
8. From the **Member Class** menu, optionally select an existing class that you want to associate with the new policy.
9. Click the **Add** button.

   The new policy is added.
10. After creating the policy, click the policy name, which is a hyperlink.

    The page on which you can define the policy attributes displays.
11. From the **Assign Queue** menu, select the queue to which packets of this policy class must be assigned.

    This is an integer value in the range 0 to 7.
12. Configure the policy attributes:
    - **Drop**. Select this radio button to require each inbound packet to be dropped.
    - **Mark VLAN CoS**. Select this radio button to specify the VLAN priority, which you must select from the menu. The VLAN priority is expressed as an integer value in the range from 0 to 7.
    - **Mark IP Precedence**. Select this radio button to require packets to be marked with an IP precedence value before being forwarded. You must select an IP precedence value from 0 to 7 from the menu.
    - **Mirror**. Select this radio button to require packets to be mirrored to an interface or LAG, one of which you must select from the menu.
    - **Redirect**. Select this radio button to require packets to be redirected to an interface or LAG, one of which you must select from the menu.
    - **Mark IP DSCP**. Select this radio button to require packet to be marked with an IP DSCP keyword code, which you must select from the menu. The menu includes **Other** as a selection, which lets you enter an IP DSCP value from 0 to 63. The DSCP value is defined as the high-order 6 bits of the Service Type octet in the IP header.

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

  a. To specify the traffic policing style for the class, select the **Simple Policy** radio button.

  By default, the Color Mode field is set to Color Blind. Color classes do not apply.

  b. Specify the traffic rate and bust size for packets that conform to the simple policy.

  - **Committed Rate**. Specify the committed rate that is applied to conforming packets by entering a value in the range from 1 to 4294967295 kilobits-per-second (Kbps). The committed rate is used to limit the arrival rate of conforming traffic.
  - **Committed Burst Size**. Specify the burst size that is applied to conforming packets by entering a value in the range from 1 to 128 KBytes (KB). The committed burst size is used to limit the amount of conforming traffic.

  c. Select the conforming action that the switch takes when a packet conforms to the policing metrics:

  - **Send**. Packets are forwarded unmodified. This is the default confirming action.
  - **Drop**. Packets are dropped.
  - **Mark CoS**. Packets are marked by DiffServ with the specified CoS value before being forwarded. This selection requires that the Mark CoS field is set. You must select a CoS value from 0 to 7 from the menu.
  - **Mark IP Precedence**. These packets are marked by DiffServ with the specified IP Precedence value before being forwarded. This selection requires that the Mark IP Precedence field is set. You must select an IP precedence value from 0 to 7 from the menu.
  - **Mark IP DSCP**. Packets are marked by DiffServ with the specified DSCP value before being forwarded. This selection requires that the DSCP field is set. You must select a DSCP code from the menu. The DSCP value is defined as the high-order six bits of the Service Type octet in the IP header.

  d. Select the violating action that the switch takes when a packet does not conform to the policing metrics:

  - **Send**. Packets are forwarded unmodified. This is the default violating action.
  - **Drop**. Packets are dropped.
  - **Mark CoS**. Packets are marked by DiffServ with the specified CoS value before being forwarded. This selection requires that the Mark CoS field is set. You must select a CoS value from 0 to 7 from the menu.
  - **Mark IP Precedence**. These packets are marked by DiffServ with the specified IP Precedence value before being forwarded. This selection requires that the Mark IP Precedence field is set. You must select an IP precedence value from 0 to 7 from the menu.
  - **Mark IP DSCP**. Packets are marked by DiffServ with the specified DSCP value before being forwarded. This selection requires that the DSCP field is set. You

must select a DSCP code from the menu. The DSCP value is defined as the high-order six bits of the Service Type octet in the IP header.

13. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only information displayed on the page.

Table 73. DiffServ policy configuration policy attribute

Field	Description
Policy Name	The name of the DiffServ policy.
Policy Type	The type of the policy, which is always inbound (In).
Member Class Name	The name of the class instance within the policy.

Rename an existing DiffServ policy

To rename an existing DiffServ policy:

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

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **QoS > DiffServ > Advanced > Policy Configuration**.

   The Policy Configuration page displays.
7. Select the check box next to the policy name.
8. In the **Policy Name** field, specify the new name.
9. Click the **Apply** button.

Your settings are saved.

Change the policy attributes for an existing DiffServ policy

To change the policy attributes for an existing DiffServ policy:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **QoS > DiffServ > Advanced > Policy Configuration**.

   The Policy Configuration page displays.
7. Click the policy name, which is a hyperlink.

   The page on which you can change the policy attributes displays.
8. Change the policy attributes as needed.
9. Click the **Apply** button.

   Your settings are saved.

Change or remove a class from an existing DiffServ policy

To change or remove a class from an existing DiffServ policy:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **QoS > DiffServ > Advanced > Policy Configuration**.

   The Policy Configuration page displays.
7. Select the check box next to the policy name.
8. Do one of the following:
   - To change the class, select another class rom the **Member Class** menu.
   - To remove the class, select **None**, from the **Member Class** menu.
9. Click the **Apply** button.

   The class is removed from the policy.

Delete a DiffServ policy

To delete a DiffServ policy:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **QoS > DiffServ > Advanced > Policy Configuration**.

   The Policy Configuration page displays.

7. Select the check box next to the policy name.
8. Click the **Delete** button.

   The policy is removed.

Configure the DiffServ service interface

You can activate a policy on an interface.

Attach a DiffServ policy to an interface

To attach a DiffServ policy to an interface:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **QoS > DiffServ > Advanced > Service Configuration**.

   The Service Interface Configuration page displays.

7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:

- **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
- **LAG**. Only LAGs are displayed.
- **All**. Both physical interfaces and LAGs are displayed.

8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. From the **Policy Name** menu, select a policy name.
10. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only information displayed on the page.

Table 74. Service Interface Configuration information

Field	Description
Direction	Shows the traffic direction of this service interface (either In or Out).
Operational Status	Shows the operational status of this service interface (either Up or Down).

Change the DiffServ policy for an interface

To change the DiffServ policy for an interface:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **QoS > DiffServ > Advanced > Service Configuration**.

   The Service Interface Configuration page displays.

7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select the check box for the interface.
9. From the **Policy In Name** menu, select another policy name.
10. Click the **Apply** button.

    Your settings are saved.

Remove a DiffServ policy from an interface

To remove a DiffServ policy from an interface:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **QoS > DiffServ > Advanced > Service Configuration**.

   The Service Interface Configuration page displays.

7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
8. Select the check boxes that are associated with the interfaces from which you want to remove the policy.
9. From the **Policy In Name** menu, select **None**.
10. Click the **Apply** button.

    Your settings are saved.

View DiffServ service statistic

You can display service-level statistical information about all interfaces to which DiffServ policies are attached.

To view the DiffServ service statistics:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **QoS > DiffServ > Advanced > Service Statistics**.

   The Service Statistics page displays.
7. To refresh the page, click the **Refresh** button.

The following table describes the information available on the Service Statistics page.

Table 75. DiffServ Service Statistics information

Field	Description
Interface	All valid port numbers on the switch with a DiffServ policy that is attached in the inbound direction.
Direction	The traffic direction of interface is inbound (In). This field shows only the direction for which a DiffServ policy is attached.
Policy Name	The name of the policy that is currently attached to the specified interface and direction.
Operational Status	The operational status of the policy that is attached to the specified interface and direction. The value is either Up or Down.
Member Classes	All DiffServ classes that are defined as members of the selected policy name. Select a member class name to display its statistics. If no class is associated with the selected policy, then the list is empty.

6

Manage Device Security

This chapter contains the following sections:

- Change the device admin password for the device UI
- Manage the RADIUS settings
- Configure the TACACS+ settings
- Configure authentication lists
- Configure management access
- Control access with profiles and rules
- Configure port authentication
- Set up traffic control

Change the device admin password for the device UI

You can change the device admin password for device UI.

To change the device admin password for 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Management Security > User Configuration > Change Password**.

   The Change Password page displays.
7. From the **Encryption Type** menu, select the encryption type for the password.

   The default encryption type is SHA512. You can also select SHA256, which is a weaker protocol than SHA512.
8. In the **Old Password** field, specify the current password for the account created by the user.

   The entered password is displayed in dots. Passwords are up to 20 alphanumeric characters in length, and are case sensitive.
9. In the **New Password** field, specify the optional new or changed password for the account.

   Use the following guidelines for a new password:
   - The minimum length of the password must be eight characters.
   - The password must include at least one uppercase letter, one lowercase letter, and one numeral.

- Although it is not required, we recommend that you include a special character in the password.

If the new password does not conform to the requirements, the switch rejects the password.

The entered password is displayed in dots. Passwords are up to 20 alphanumeric characters in length, and are case sensitive.

10. In the **Confirm Password** field, enter the password again to confirm that you entered it correctly.

    The entered password is displayed in dots.

11. Click the **Apply** button.

    Your settings are saved.

    The Lockout Status field indicates if the user account is locked (True or False).

Reset the device admin password for the device UI

You can reset the device admin password for device UI. The default password is **password**.

To reset the device admin password for 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Management Security > User Configuration > Change Password**.

   The Change Password page displays.

7. Select the **Reset Password** check box.
8. Click the **Apply** button.

   Your settings are saved.

   The Lockout Status field indicates if the user account is locked (True or False).

Configure password lockout

You can configure the password lockout settings. By default, if you type the wrong password five times, you are locked out for five minutes, after which you can try again. The you can change these settings.

To configure the password lockout settings:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Management Security > User Configuration > Password Configuration**.

   The Password Configuration page displays.

7. In the **Lockout Attempts** field, specify the number of times a user is allowed to fail a local authentication attempt before the user account is locked out.

   The default is 5, which means that a user account is locked after five failed attempts. You can select from 1 to 5 attempts. If you select **0**, the lockout feature is disabled.

8. In the **Lockout Attempts** field, specify the period during which a user account is locked.

   The default is 5, which means that a user account is locked for five minutes. You can select from 1 to 60 minutes.

9. Select the Unlock Timer Mode **Disable** or **Enable** radio button.

   By default, the Enable radio button is selected, and a user account is locked after failed local authentication attempts. You can disable this capability.

10. Click the **Apply** button.

    Your settings are saved.

Manage the RADIUS settings

RADIUS servers provide additional security for networks. The RADIUS server maintains a user database, which contains per-user authentication information. The switch passes information to the configured RADIUS server, which can authenticate a user name and password before authorizing use of the network. RADIUS servers provide a centralized authentication method for the following:

- Web access
- Access control port (802.1X)

Configure the global RADIUS server settings

You can add information about one or more RADIUS servers on the network.

If you configure multiple RADIUS servers, consider the maximum delay time when you specify the maximum number of retransmissions (that is, the value that you enter in the **Max Number of Retransmits** field) and the time-out period (that is, the value that you enter in the **Timeout Duration** field) for RADIUS:

For one RADIUS server, a retransmission does not occur until the configured time-out period expires without a response from the RADIUS server. In addition. the maximum number of retransmissions for one RADIUS server must pass before the switch attempts the next RADIUS server.

Therefore, the maximum delay in receiving a RADIUS response on the switch equals the maximum number of retransmissions multiplied by the time-out period multiplied by the number of configured RADIUS servers. If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the switch receives a RADIUS response.

To configure the global RADIUS server settings:

1. Connect your computer to the same network as the switch.

You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Management Security > RADIUS > Global Configuration**.

   The RADIUS Configuration page displays.

   The Current Server IP Address field is blank if no servers are configured (see Configure a RADIUS authentication server on the switch on page 306). The switch supports up to three RADIUS servers. If more than one RADIUS server is configured, the current server is the server configured as the primary server. If no servers are configured as the primary server, the current server is the most recently added RADIUS server.



CAUTION:

The maximum delay in receiving a RADIUS response on the switch equals the maximum number of retransmissions multiplied by the time-out period multiplied by the number of configured RADIUS servers. If the RADIUS request is generated by a user login attempt, all user interfaces are blocked until the switch receives a RADIUS response.

7. In the **Max Number of Retransmits** field, specify the maximum number of times a request packet is retransmitted to the RADIUS server.

   The range is from 1 to 15. The default value is 4.
8. In the **Timeout Duration** field, specify the time-out value, in seconds, for request retransmissions.

   The range is from 1 to 30. The default value is 5.
9. From the **Accounting Mode** menu, select to disable or enable RADIUS accounting on the server.

The default is Disable.

10. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only fields displayed on the page.

Table 76. RADIUS Configuration information

Field	Description
Current Server Address	The address of the current server. This field is blank if no servers are configured.
Number of Configured Authentication Servers	The number of configured authentication RADIUS servers. The value can range from 0 to 3.

Configure a RADIUS authentication server on the switch

You can configure various settings for a RADIUS authentication server.

Add a primary RADIUS authentication server to the switch

To add a primary RADIUS authentication server to the switch and view or reset the RADIUS authentication server statistics:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Management Security > RADIUS > Server Configuration**.

   The Server Configuration page displays.

7. In the **Server Address** field, specify the IP address of the RADIUS server.
8. In the **Authentication Port** field, specify the UDP port number the server uses to verify the RADIUS server authentication.

   The valid range is from 1 to 65535. The default value is 1812.
9. From the **Secret Configured** menu, select **Yes**.

   You must select **Yes** before you can configure the RADIUS secret. After you add the RADIUS server, this field indicates whether the shared secret for this server was configured.
10. In the **Secret** field, type the shared secret text string used for authenticating and encrypting all RADIUS communications between the switch and the RADIUS server.

    This secret must match the RADIUS encryption.
11. From the **Active** menu, select **Primary**.
12. From the **Message Authenticator** menu, select **Enable** or **Disable** to specify whether the message authenticator attribute for the selected server is enabled.

    The message authenticator adds protection to RADIUS messages by using an MD5 hash to encrypt each message. The shared secret is used as the key, and if the message fails to be verified by the RADIUS server, it is discarded.
13. Click the **Add** button.

    The server is added to the switch.
14. To reset the authentication server and RADIUS statistics to their default values, click the **Clear Counters** button.

    The following table describes the view-only statistics fields on the page.

Table 77. RADIUS authentication server statistics information

Field	Description
Server Address	The address of the RADIUS server or the name of the RADIUS server for which the statistics are displayed.
Round Trip Time	The time interval, in hundredths of a second, between the most recent access-reply/access-challenge and the access-request that matched it from this RADIUS authentication server.
Access Requests	The number of RADIUS access-request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS access-request packets retransmitted to this server.
Access Accepts	The number of RADIUS access-accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS access-reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS access-challenge packets, including both valid and invalid packets, that were received from this server.

Table 77. RADIUS authentication server statistics information (continued)

Field	Description
Malformed Access Responses	The number of malformed RADIUS access-response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included in malformed access-responses.
Bad Authenticators	The number of RADIUS access-response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS access-request packets destined for this server that did not yet time out or receive a response.
Timeouts	The number of authentication time-outs to this server.
Unknown Types	The number of RADIUS packets of unknown type that were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

Modify the settings for a RADIUS authentication server on the switch

To modify the settings for a RADIUS authentication server on the switch:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Management Security > RADIUS > Server Configuration**.

   The Server Configuration page displays.
7. Select the check box next to the server IP address.

8. Modify the configuration for the selected server.
9. Click the **Apply** button.

   Your settings are saved.

Remove a RADIUS authentication server from the switch

To a remove a RADIUS authentication server from the switch:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Management Security > RADIUS > Server Configuration**.

   The Server Configuration page displays.
7. Select the check box next to the IP address of the server to remove.
8. Click the **Delete** button.

   The RADIUS server is removed.

Configure a RADIUS accounting server

You can configure various settings for a RADIUS accounting server on the network.

Add a RADIUS accounting server to the switch

To add a RADIUS accounting server to the switch and view or clear the RADIUS accounting server statistics:

1. Connect your computer to the same network as the switch.

You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Management Security > RADIUS > Accounting Server Configuration**.

   The Accounting Server Configuration page displays.
7. In the **Accounting Server Address** field, specify the IP address of the RADIUS accounting server to add.
8. In the **Port** field, specify the UDP port number the server uses to verify the RADIUS accounting server authentication.
9. From the **Secret Configured** menu, select **Yes** to add a RADIUS secret in the next field.

   You must select **Yes** before you can configure the RADIUS secret. After you add the RADIUS accounting server, this field indicates whether the shared secret for this server was configured.
10. In the **Secret** field, type the shared secret to use with the specified accounting server.
11. From the **Accounting Mode** menu, select **Enable** to enable the RADIUS accounting mode.
12. Click the **Add** button.

    The server is added to the switch.
13. To reset the accounting server and RADIUS statistics to their default values, click the **Clear Counters** button.

The following table describes the view-only statistics fields on the page.

Table 78. RADIUS accounting server statistics information

Field	Description
Accounting Server Address	The address of the RADIUS server or the name of the RADIUS server for which the statistics are displayed.
Round Trip Time	The time interval, in hundredths of a second, between the most recent access-reply/access-challenge and the access-request that matched it from this RADIUS authentication server.
Access Requests	The number of RADIUS access-request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS access-request packets retransmitted to this server.
Access Responses	The number of RADIUS access-response packets, including both valid and invalid packets, that were received from this server.
Malformed Access Responses	The number of malformed RADIUS access-response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included in malformed access-responses.
Bad Authenticators	The number of RADIUS access-response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS access-request packets destined for this server that did not yet time out or receive a response.
Timeouts	The number of authentication time-outs to this server.
Unknown Types	The number of RADIUS packets of unknown type that were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

Modify the settings for a RADIUS accounting server on the switch

To modify the settings for a RADIUS accounting server on the switch:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Management Security > RADIUS > Accounting Server Configuration**.

   The Accounting Server Configuration page displays.
7. Select the check box next to the server IP address.
8. Modify the configuration for the selected accounting server.
9. Click the **Apply** button.

   Your settings are saved.

Remove a RADIUS accounting server from the switch

To a remove a RADIUS accounting server from the switch:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Management Security > RADIUS > Accounting Server Configuration**.

   The Accounting Server Configuration page displays.
7. Select the check box next to the IP address of the server to remove.

8. Click the **Delete** button.

   The RADIUS accounting server is removed.

9. Click the **Apply** button.

   Your settings are saved.

Configure the TACACS+ settings

TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. TACACS+ provides the following services:

- **Authentication**. Provides authentication during login and through user names and user-defined passwords.
- **Authorization**. Performed at login. When the authentication session is completed, an authorization session starts using the authenticated user name. The TACACS+ server checks the user privileges.

The TACACS+ protocol ensures network security through encrypted protocol exchanges between the device and TACACS+ server.

Configure the global TACACS+ settings

You can configure the global TACACS+ settings for communication between the switch and a TACACS+ server.

To configure the global TACACS+ settings:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Management Security > TACACS+ > TACACS+ Configuration**.

   The TACACS+ Configuration page displays.

7. In the **Key String** field, specify the authentication and encryption key for TACACS+ communications between the switch and the TACACS+ server.

   The valid range is 0–128. The key must match the key configured on the TACACS+ server.

8. In the **Connection Timeout** field, specify the maximum number of seconds allowed to establish a TCP connection between the switch and the TACACS+ server.

   The time-out period is from 1 to 30 seconds.

9. Click the **Apply** button.

   Your settings are saved.

Configure a TACACS+ server on the switch

You can configure up to five TACACS+ servers with which the switch can communicate.

To configure a TACACS+ server on the switch:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Management Security> TACACS+ > TACACS+ Server Configuration**.

The TACACS+ Server Configuration page displays.

7. In the **TACACS+ Server** field, enter the TACACS+ server IP address.
8. In the **Priority** field, specify the priority for the TACACS+ server.

   The priority determines the order in which the TACACS+ servers are contacted when attempting to authenticate a user. A value of 0 is the highest priority. The valid range is 0–65535.
9. In the **Port** field, specify the authentication port value for TACAS+ server sessions. It must be within the range 0–65535. If you do not specify a value, the switch uses the standard TCP port 49 for sessions with the server.
10. In the **Key String** field, specify the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server.

    The valid range is 0–128. The key must match the key used on the TACACS+ server.
11. In the **Connection Timeout** field, specify the time in seconds that passes before the connection between the device and the TACACS+ server times out.

    The range is 1–30. If you do not specify a value, the switch uses a default value of 5.
12. Click the **Add** button.

    The server is added to the switch.

Modify the settings for a TACACS+ server on the switch

To modify the settings for a TACACS+ server on the switch:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Management Security> TACACS+ > TACACS+ Server Configuration**.

   The TACACS+ Server Configuration page displays.
7. Select the check box next to the server IP address.
8. Modify the configuration for the selected TACACS+ server.
9. Click the **Apply** button.

   Your settings are saved.

Remove a TACACS+ server from the switch

To remove a TACACS+ server from the switch:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Management Security> TACACS+ > TACACS+ Server Configuration**.

   The TACACS+ Server Configuration page displays.
7. Select the check box next to the server IP address.
8. Click the **Delete** button.

   The TACACS+ server is removed.

Configure authentication lists

A login list specifies one or more authentication methods to validate switch or port access for the admin user. You can configure a default login list.

Note: The admin user is assigned to a preconfigured list that is named defaultList and that you cannot delete.

Configure an HTTP authentication list

You can configure the default HTTP login list.

To change the HTTP authentication method for the default list:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Management Security > Authentication List > HTTP Authentication List**.

   The HTTP Authentication List page displays.
7. Select the check box next to the httpList name.
8. From the menu in the 1 column, select the authentication method that must be used first in the selected authentication login list.

If you select a method that does not time out as the first method, such as **Local**, no other method is tried, even if you specified more than one method. User authentication occurs in the order the methods are selected. Possible methods are as follows:

- **Local**. The user's locally stored ID and password are used for authentication. Since the Local method does not time out, if you select this option as the first method, no other method is tried, even if you specified more than one method.
- **RADIUS**. The user's ID and password are authenticated using the RADIUS server. If you select **RADIUS** or **TACACS+** as the first method and an error occurs during the authentication, the switch uses Method 2 to authenticate the user.
- **TACACS+**. The user's ID and password are authenticated using the TACACS+ server. If you select **RADIUS** or **TACACS+** as the first method and an error occurs during the authentication, the switch attempts user authentication Method 2.
- **None**. The authentication method is unspecified. This option is available only for Method 2 and Method 3.

9. From the menu in the 2 column, select the authentication method, if any, that must be used second in the selected authentication login list.

   This is the method that is used if the first method times out. If you select a method that does not time out as the second method, the third method is not tried.

10. From the menu in the 3 column, select the authentication method, if any, that must be used third in the selected authentication login list.
11. From the menu in the 4 column, select the method, if any, that must be used fourth in the selected authentication login list.

    This is the method that is used if all previous methods time out.

12. Click the **Apply** button.

    Your settings are saved.

Configure an HTTPS authentication list

You can configure the default login list for secure HTTP (HTTPS).

To configure an HTTPS authentication list:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Management Security > Authentication List > HTTPS Authentication List**.

   The HTTPS Authentication List page displays.
7. Select the check box next to the httpsList name.
8. From the menu in the 1 column, select the authentication method that must be used first in the selected authentication login list.

   If you select a method that does not time out as the first method, such as **Local**, no other method is tried, even if you specified more than one method. This setting does not display when you first create a new login list. User authentication occurs in the order the methods are selected. Possible methods are as follows:
   - **Local**. The user's locally stored ID and password are used for authentication. Since the Local method does not time out, if you select this option as the first method, no other method is tried, even if you specified more than one method.
   - **RADIUS**. The user's ID and password are authenticated using the RADIUS server. If you select **RADIUS** or **TACACS+** as the first method and an error occurs during the authentication, the switch uses Method 2 to authenticate the user.
   - **TACACS+**. The user's ID and password are authenticated using the TACACS+ server. If you select **RADIUS** or **TACACS+** as the first method and an error occurs during the authentication, the switch attempts user authentication Method 2.
   - **None**. The authentication method is unspecified. This option is only available for Method 2 and Method 3.
9. From the menu in the 2 column, select the authentication method, if any, that must be used second in the selected authentication login list.

   This is the method that is used if the first method times out. If you select a method that does not time out as the second method, the third method is not tried.
10. From the menu in the 3 column, select the authentication method, if any, that must be used third in the selected authentication login list.
11. From the menu in the 4 column, select the method, if any, that must be used fourth in the selected authentication login list.

    This is the method that is used if all previous methods time out.
12. Click the **Apply** button.

    Your settings are saved.

Configure the dot1x authentication list

The dot1x authentication list defines the IEEE 802.1X authentication method used for the default list. The default list is dot1xList.

To configure the dot1x authentication list:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Management Security > Authentication List > Dot1x Authentication List**.

   The Dot1x Authentication List page displays.
7. Select the check box next to the dot1xList name.
8. From the menu in the 1 column, select the method that must be used first in the selected authentication login list.

   The options are as follows:
   - **Local**. The user's ID and password are locally authenticated.
   - **RADIUS**. The user's ID and password are authenticated using a RADIUS server.
   - **None**. The user is not authenticated.
9. Click the **Apply** button.

   Your settings are saved.

Configure management access

You can configure the global settings for HTTP and secure HTTP (HTTPS) access to the switch's device UI. You can also configure access control profiles and access rules.

Configure the HTTP settings

You can configure the HTTP access settings on the switch. If you access the switch device UI, HTTP is the default access method.

To configure the HTTP access settings:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Access > HTTP > HTTP Configuration**.

   The HTTP Configuration page displays.
7. Select the Admin Mode **Enable** or **Disable** radio button.

   This enables or disables HTTP. The default value is Enable.
8. In the **HTTP Session Soft Timeout** field, specify the number of minutes an HTTP session can be idle before a time-out occurs.

   The value must be in the range of 0–60 minutes. The default value is 5 minutes. The currently configured value is shown when the web page is displayed.

After the session is inactive for the configured time, you are automatically logged out and must reenter the password to access the device UI. A value of zero means that the session does not time out.

9. In the **HTTP Session Hard Timeout** field, specify the hard time-out for HTTP sessions.

   This time-out is unaffected by the activity level of the session. The value must be in the range of 0–168 hours. value of zero means that the session does not time out. The default value is 24 hours.

10. In the **Maximum Number of HTTP Sessions** field, specify the maximum number of HTTP sessions that can exist at the same time.

    The value must be in the range of 1 to 4. The default value is 4.

11. Click the **Apply** button.

    Your settings are saved.

Configure the HTTPS settings

Secure HTTP (HTTPS) enables the transmission of HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) 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. The hash algorithms that SSL uses are MD5 and SHA-1.

To configure HTTPS access settings:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Access > HTTPS > HTTPS Configuration**.

   The HTTPS Configuration page displays.

7. Select the Admin Mode **Enable** or **Disable** radio button.

   This selection enables or disables HTTPS. The default value is Disable.

   Note: You can download SSL certificates only when HTTPS is disabled.

8. In the **HTTPS Port** field, type the HTTPS port number.

   The value must be in the range of 1025 to 65535. Port 443 is the default value. The configured value is displayed.

9. In the **HTTPS Session Soft Timeout (Minutes)** field, enter the inactivity time-out for HTTPS sessions.

   The value must be in the range of 1 to 60 minutes. The default value is 5 minutes. The configured value is displayed.

10. In the **HTTPS Session Hard Timeout (Hours)** field, set the hard time-out for HTTPS sessions.

    This time-out is unaffected by the activity level of the session. The value must be in the range of 1 to 168 hours. The default value is 24 hours.

11. In the **Maximum Number of HTTPS Sessions** field, enter the maximum allowable number of HTTPS sessions.

    The value must be in the range of 0 to 4. The default value is 4.

12. Click the **Apply** button.

    Your settings are saved.

Browser security warning with HTTPS access

After you enable HTTPS access (see Configure the HTTPS settings on page 322) 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 IP address of the switch.
- **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.

  For information about installing a specific security certificate on the switch, see Manage certificates for HTTPS access on page 324 and Use an HTTP session to download and install an SSL security certificate file on the switch on page 450.

Manage certificates for HTTPS access

You can manage certificates.

Generate an SSL certificate

Note: Before you can generate a certificate, you must disable HTTPS (see Configure the HTTPS settings on page 322) 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 generate an SSL certificate:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Access > HTTPS > Certificate Management**.

   The Certificate Management page displays.

The Certificate Present field displays whether a certificate is present on the switch.

7. In the Certificate Management section, select the **Generate Certificates** radio button.
8. Click the **Apply** button.

   The switch generates an SSL certificate.

   The Certificate Generation Status field shows information about the progress.

Delete an SSL certificate

Note: Before you can delete a certificate, you must disable HTTPS (see Configure the HTTPS settings on page 322) 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 an SSL certificate:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security** > **Access > HTTPS** > **Certificate Management**.

   The Certificate Management page displays.
7. The Certificate Management page displays.

   The Certificate Present field displays Yes.
8. In the Certificate Management section, select **Delete Certificates** radio button.

9. Click the **Apply** button.

   The certificate is removed.

Transfer an existing certificate to the switch

You can transfer a certificate file to the switch.

For the switch to accept HTTPS connections from a device, the switch requires a public key certificate. You can generate a certificate externally (for example, offline) and transfer it to the switch.

Before you transfer a file from a TFTP server to the switch, the following conditions must be true:

- The file to download from the TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch contains a path to the TFTP server.

Note: Before you can transfer a certificate, you must disable HTTPS (see Configure the HTTPS settings on page 322) 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 a certificate 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

The System Information page displays.

6. Select **Security > Access > HTTPS > Certificate Download**.

   The Certificate Download page displays.

7. From the **File Type** menu, select the type of SSL certificate to download, which can be one of the following:
   - **SSL Trusted Root Certificate PEM File**. SSL Trusted Root Certificate file (PEM Encoded)
   - **SSL Server Certificate PEM File**. SSL Server Certificate File (PEM Encoded)
   - **SSL DH 1024 Encryption Parameter PEM File**. SSL Diffie-Hellman Weak Encryption Parameter file (PEM Encoded)
   - **SSL DH 2048 Encryption Parameter PEM File**. SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded)
8. From the **Transfer Mode** menu, specify the protocol that must be used to transfer the file to the server:
   - **SFTP**: Secure File Transfer Protocol. This selection requires you to specify a user name and password.
   - **TFTP**: Trivial File Transfer Protocol.
   - **SCP**: Secure Copy Protocol. This selection requires you to specify a user name and password.
9. From the **Server Address Type** menu, select **IPv4** or **DNS** to indicate the format of the Server Address field.

   The default is IPv4.

10. In the **TFTP Server IP** field, specify the address of the TFTP server.

    The address can be an IP address in standard x.x.x.x format or a host name. The host name must start with a letter of the alphabet. Make sure that the software image or other file to be downloaded is available on the TFTP server.

11. In the **Remote File Path** field, enter the path of the file to download.

    You can enter up to 96 characters. The default is blank.

12. In the **Remote File Name** field, enter the name of the file on the TFTP server to download.

    You can enter up to 32 characters. The default is blank.

13. If you select **SFTP** or **SCP** from **Transfer Mode** menu, specify the following settings:
    - **User Name**: Specify the user name for remote login to the server.
    - **Password**: Specify the password for remote login to the server.
14. Select the **Start File Transfer** check box.
15. Click the **Apply** button.

    The file transfer starts. A status message displays during the transfer and upon successful completion of the transfer.

Control access with profiles and rules

Access control allows you to configure an access control profile and set rules for access to the device UI, 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 (see Reset the switch to its factory default settings on page 441).

Add an access profile

You can set up a single security access profile with which you can associate an access rule configuration.

To add an access profile:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Access > Access Control > Access Profile Configuration**.

   The Access Profile Configuration page displays.

7. In the **Access Profile Name** field, enter the name of the access profile to be added.

   The maximum length is 32 characters.

   You do not need to select any check boxes if you are adding access profile.

8. Click the **Apply** button.

   Your settings are saved.

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 its factory default settings on page 441).

To add a rule to the access profile:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Access > Access Control > Access Rule Configuration**.

   The Access Rule Configuration page displays.

7. From the **Rule Type** menu, select **Permit** or **Deny** to permit or deny access when the selected rules are matched.

   A Permit rule allows access by traffic that matches the rule criteria. A Deny rule blocks traffic that matches the rule criteria.

8. From the **Service Type** menu, select the access method to which the rule is applied.

   The policy is restricted by the selected access method. You can select **TFTP**, **HTTP, Secure HTTP (SSL)**, or **SNMP**.

9. In the **Source IP Address** field, enter the source IP address of the client originating the management traffic.
10. In the **Mask** field, specify the subnet mask of the client that originates the management traffic.
11. In the **Priority** field, assign a priority to the rule.

    The rules are validated against the incoming management request in ascending order of their priorities. If a rule matches, the action is performed and subsequent rules below that are ignored. For example, if a source IP 10.10.10.10 is configured with priority 1 to permit, and source IP 10.10.10.10 is configured with priority 2 to deny, then access is permitted if the profile is active, and the second rule is ignored.

12. Click the **Add** button.

    The access rule is added.

Activate the access profile

After you add rules to the access profile, you can activate the access profile.



CAUTION:

If you configure a security access profile incorrectly and you activate the access profile, you might no longer be able to access the switch's device UI. If that situation occurs, you must reset the switch to factory default settings (see Reset the switch to its factory default settings on page 441).

To activate the access profile:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Access > Access Control > Access Profile Configuration**.

   The Access Profile Configuration page displays.

   The Deactivate Profile check box is selected.
7. Select the **Activate Profile** check box.
8. Click the **Apply** button.

   Your settings are saved and the access profile is now active.

Display the access profile summary and the number of filtered packets

After you added rules to the active profile, you can view the entries in the summary. If the access profile is active, you can also view the number of filtered packets.

To display the access profile summary and the number of filtered packets:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Access > Access Control > Access Profile Configuration**.

   The Access Profile Configuration page displays.

   The Packets Filtered field displays the number of packets filtered.

7. To refresh the page, click the **Refresh** button.

The following table describes the view-only data that is displayed.

Table 79. Access profile configuration profile summary

Field	Description
Rule Type	The action performed when the rules match.
Service Type	The service type selected. The policy is restricted by the selected service type.
Source IP Address	The source IP address of the client originating the management traffic.
Mask	The subnet mask of the IP Address.
Priority	The priority of the rule.

Deactivate an access profile

You can deactivate an access profile.

To deactivate an access profile:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Access > Access Control > Access Profile Configuration**.

   The Access Profile Configuration page displays.

   The Activate Profile check box is selected.

7. Select the **Deactivate Profile** check box.
8. Click the **Apply** button.

   Your settings are saved and the access profile is now deactivated.

Remove an access profile

You can remove an access profile that you no longer need. Before you can remove the access profile, you must deactivate it (see Deactivate an access profile on page 332).

To remove an access profile:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Access > Access Control > Access Profile Configuration**.

   The Access Profile Configuration page displays.

The Deactivate Profile check box is selected.

7. Select the **Remove Profile** check box.
8. Click the **Apply** button.

   The access profile is removed.

Configure port authentication

With port-based authentication, when 802.1X is enabled globally and on the port, successful authentication of any one supplicant attached to the port results in all users being able to use the port without restrictions. At any given time, only one supplicant is allowed to attempt authentication on a port in this mode. Ports in this mode are under bidirectional control. This is the default authentication mode.

An 802.1X network includes three components:

- **Authenticators**. The port that is authenticated before system access is permitted.
- **Supplicants**. The host connected to the authenticated port requesting access to the system services.
- **Authentication Server**. The external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the user is authorized to access system services.

Configure global 802.1X settings

You can configure global port access control settings on the switch.

To globally enable the 802.1X features:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Port Authentication > Basic > 802.1X Configuration**.

   The 802.1X Configuration page displays.

7. Select the Port Based Authentication State **Enable** radio button.

   This enables the 802.1X administrative mode on the switch. The default value is Disable.

   Note: If 802.1X is enabled, authentication is performed by a RADIUS server. This means that the primary authentication method must be RADIUS. To set the method, select **Security > Management Security > Authentication List** and select **RADIUS** as method 1 for defaultList. For more information, see Configure authentication lists on page 317.

   When port-based authentication is globally disabled, the switch does not check for 802.1X authentication before allowing traffic on any ports, even if the ports are configured to allow only authenticated users.

8. Select the VLAN Assignment Mode **Enable** radio button.

   The default value is Disable.

   When enabled, this feature allows a port to be placed into a particular VLAN based on the result of the authentication or type of 802.1X authentication a client uses when it accesses the device. The authentication server can provide information to the device about which VLAN to assign the supplicant.

9. Select the Dynamic VLAN Creation Mode **Enable** radio button.

   The default value is Disable.

   If RADIUS-assigned VLANs are enabled, the RADIUS server is expected to include the VLAN ID in the 802.1X tunnel attributes of its response message to the device. If dynamic VLAN creation is enabled on the device and the RADIUS-assigned VLAN does not exist, then the assigned VLAN is dynamically created. This implies that the client can connect from any port and can get assigned to the appropriate VLAN. This feature gives flexibility for clients to move around the network without much additional configuration required.

10. Select the EAPOL Flood Mode **Enable** radio button.

    The default value is Disable. Extensible Authentication Protocol (EAP) over LAN (EAPoL) flood support is enabled on the switch.

11. Click the **Apply** button.

    Your settings are saved.

Manage port authentication on individual ports

You can enable and configure port access control on one or more physical ports.

Configure 802.1X settings for a port

To configure 802.1X settings for a port:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Port Authentication > Advanced > Port Authentication**.

   The Port Authentication page displays.
7. Use the horizontal scroll bar at the bottom of the page to view all the fields.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. Specify the following settings:
   - **Port Control**. Defines the port authorization state. The control mode is set only if the link status of the port is link up. Select one of the following options:
     - **Auto**. The switch automatically detects the mode of the interface.

  - **Authorized**. The switch places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication.
  - **Unauthorized**. The switch denies the selected interface system access by moving the interface into unauthorized state. The switch cannot provide authentication services to the client through the interface.
  - **MAC based**. This mode allows multiple supplicants connected to the same port to each authenticate individually. Each host connected to the port must authenticate separately in order to gain access to the network. The hosts are distinguished by their MAC addresses.

- **Guest VLAN ID**. Specify the VLAN ID for the guest VLAN. The valid range is 0–4093. The default value is 0. Enter 0 to reset the guest VLAN ID on the interface. The guest VLAN allows the port to provide a distinguished service to unauthenticated users, after three authentication failures. This feature provides a mechanism to allow users access to hosts on the guest VLAN.
- **Guest VLAN Period**. Specify the number of seconds that the selected port remains in the quiet state following a failed authentication exchange. The guest VLAN time-out must be a value in the range of 1–300. The default value is 90.
- **Unauthenticated VLAN ID**. Specify the VLAN ID of the unauthenticated VLAN for the selected port. The valid range is 0–3965. The default value is 0. Hosts that fail the authentication might be denied access to the network or placed on a VLAN created for unauthenticated clients. This VLAN might be configured with limited network access.
- **Periodic Reauthentication**. Select **Enable** to allow periodic reauthentication of the supplicant for the specified port. The default is Disable.
- **Reauthentication Period**. Specify the time, in seconds, after which reauthentication of the supplicant occurs. The reauthentication period must be a value in the range of 1–65535. The default value is 3600. If this field is disabled, connected clients are not forced to reauthenticate periodically.
- **Reauthentication Period**. Specify the time, in seconds, after which reauthentication of the supplicant occurs. The reauthentication period must be a value in the range of 1–65535. The default value is 3600. If this field is disabled, connected clients are not forced to reauthenticate periodically.
- **Quiet Period**. Specify the number of seconds that the port remains in the quiet state following a failed authentication exchange. While in the quite state, the port does not attempt to acquire a supplicant.

  The period can be from 0 to 65535 seconds. The default is 60 seconds.
- **Resending EAP**. Specify the EAP retransmit period for the selected port. The transmit period is the value, in seconds, after which an EAPoL EAP Request/Identify frame is resent to the supplicant.

  The period can be from 0 to 65535 seconds. The default is 30 seconds.

- **Max EAP Requests**. Specify the maximum number of EAP requests for the selected port. The value is the maximum number of times an EAPoL EAP Request/Identity message is retransmitted before the supplicant times out.

  The range is from 1 to 20. The default is 2.
- **Supplicant Timeout**. Specify the supplicant time-out for the selected port. The supplicant time-out is the value, in seconds, after which the supplicant times out.

  The period can be from 0 to 65535 seconds. The default is 30 seconds.
- **Server Timeout**. Specify the time that elapses before the switch resends a request to the authentication server.

  The period can be from 0 to 65535 seconds. The default is 30 seconds.

10. Click the **Apply** button.

Your settings are saved.

The following table describes the view-only port authentication fields on the page.

Table 80. Port authentication status information

Field	Description
Control Direction	The control direction for the specified port, which is always Both. The control direction dictates the degree to which protocol exchanges take place between supplicant and authenticator.The unauthorized controlled port exerts control over communication in both directions (disabling both incoming and outgoing frames).
Protocol Version	The protocol version associated with the selected port. The only possible value is 1, corresponding to the first version of the 802.1X specification.
PAE Capabilities	The port access entity (PAE) functionality of the selected port. Possible values are Authenticator or Supplicant.
Authenticator PAE State	The current state of the authenticator PAE state machine. Possible values are as follows: Initialize Disconnected Connecting Authenticating Authenticated Aborting Held ForceAuthorized ForceUnauthorized

Table 80. Port authentication status information (continued)

Field	Description
Backend State	The current state of the backend authentication state machine. Possible values are as follows: Request Response Success Fail Timeout Initialize Idle

Initialize 802.1X on a port

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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Port Authentication > Advanced > Port Authentication**.

   The Port Authentication page displays.

7. Select the check box that is associated with the port that you want to initialize.
8. Click the **Initialize** button.

   802.1X on the selected interface is reset to the initialization state. Traffic sent to and from the port is blocked during the authentication process. This button is available only if the control mode is auto. When you click this button, the action is immediate. You do not need to click the **Apply** button for the action to occur.

Restart the 802.1X authentication process on a port

To restart the 802.1X authentication process on a port:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Port Authentication > Advanced > Port Authentication**.

   The Port Authentication page displays.
7. Select the check box associated with the port to reauthenticate.
8. Click the **Reauthenticate** button.

   The selected port is forced to restart the authentication process.If the button is not selectable, it is grayed out. When you click this button, the action is immediate. You do not need to click the **Apply** button for the action to occur.

View the port summary

You can view summary information about the port-based authentication settings for each port.

To view the port summary:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Port Authentication > Advanced > Port Summary**.

   The Port Summary page displays.
7. To refresh the page, click the **Refresh** button.

The following table describes the fields on the Port Summary page.

Table 81. Port summary

Field	Description
Port	The port whose settings are displayed in the current table row.
Control Mode	This field indicates the configured control mode for the port. Possible values are as follows: • **Force Unauthorized**. The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized. • **Force Authorized**. The authenticator PAE unconditionally sets the controlled port to authorized. • **Auto**. The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server. • **MAC Based**. The authenticator PAE sets the controlled port mode to reflect the outcome of authentication exchanges between a supplicant, an authenticator, and an authentication server on a per supplicant basis.
Operating Control Mode	The control mode under which the port is actually operating. Possible values are as follows: • ForceUnauthorized • ForceAuthorized • Auto • MAC Based • N/A: If the port is in detached state, it cannot participate in port access control.
Reauthentication Enabled	This field shows whether reauthentication of the supplicant for the specified port is allowed. The possible values are True and False. If the value is True, reauthentication occurs. Otherwise, reauthentication is not allowed.
Port Status	The authorization status of the specified port. The possible values are Authorized, Unauthorized, and N/A. If the port is in detached state, the value is N/A because the port cannot participate in port access control.

View the client summary

You can display information about supplicant devices that are connected to the local authenticator ports. If no active 802.1X sessions exist, the table is empty.

To view the client summary:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Port Authentication > Advanced > Client Summary**.

   The Client Summary page displays.
7. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields on the Client Summary page.

Table 82. Client Summary information

Field	Description
Port	The port to be displayed.
User Name	The user name representing the identity of the supplicant device.
Supplicant Mac Address	The supplicant's device MAC address.
Session Time	The time since the supplicant logged in seconds.
Filter ID	The policy filter ID assigned by the authenticator to the supplicant device.
VLAN ID	The VLAN ID assigned by the authenticator to the supplicant device.
VLAN Assigned	The reason for the VLAN ID assigned by the authenticator to the supplicant device.
Session Timeout	The session time-out imposed by the RADIUS server on the supplicant device.
Termination Action	The termination action imposed by the RADIUS server on the supplicant device.

Set up traffic control

You can configure MAC filters, storm control, port security, protected port, and private VLAN settings.

Manage MAC filtering

You can create MAC filters that limit the traffic allowed into and out of specified ports on the switch.

Create a MAC filter

If a packet with a MAC address and VLAN ID that you specify for a filter is received on a port that is not part of the inbound filter, the packet is dropped.

A packet with a MAC address and VLAN ID that you specify for a filter can be transmitted only from a port that is part of the outbound filter.

To create a MAC filter:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Traffic Control > MAC Filter > MAC Filter Configuration**.

   The MAC Filter Configuration page displays.
7. From the **MAC Filter** menu, select **Create Filter**.

   If you did not configure any filters, this is the only option available.

8. From the **VLAN ID** menu, select the VLAN that must be used with the MAC address.
9. In the **MAC Address** field, specify the MAC address of the filter in the format XX:XX:XX:XX:XX:XX.

   You cannot define filters for the following MAC addresses:

   - 00:00:00:00:00:00
   - 01:80:C2:00:00:00 to 01:80:C2:00:00:0F
   - 01:80:C2:00:00:20 to 01:80:C2:00:00:21
   - FF:FF:FF:FF:FF:FF
10. In the Port and LAG tables in the Source Port Members section, select the ports and LAGs that must be included in the inbound filter.

    If a packet with the MAC address and VLAN ID that you specify is received on a port that is not part of the inbound filter, the packet is dropped.
11. In the Port and LAG tables in the Destination Port Members section, select the ports and LAGs that must be included in the outbound filter.

    A packet with the MAC address and VLAN ID that you specify can be transmitted only from a port that is part of the outbound filter.

    Note: Destination ports can be included only in a multicast filter.
12. Click the **Apply** button.

    Your settings are saved.

Delete a MAC filter

To delete a MAC filter:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

The System Information page displays.

6. Select **Security > Traffic Control > MAC Filter > MAC Filter Configuration**.

   The MAC Filter Configuration page displays.

7. From the **MAC Filter** menu, select the filter.
8. Click the **Delete** button.

   The filter is removed.

View the MAC filter summary

You can view the MAC filters that are configured on the switch.

To view the MAC filter summary:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Traffic Control > MAC Filter > MAC Filter Summary**.

   The MAC Filter Summary page displays.

7. To refresh the page, click the **Refresh** button.

The following table describes the view-only fields displayed on the page.

Table 83. MAC Filter Summary information

Field	Description
MAC Address	The MAC address of the filter in the format XX:XX:XX:XX:XX:XX.
VLAN ID	The VLAN ID used with the MAC address to fully identify packets you want filtered.

Table 83. MAC Filter Summary information (continued)

Field	Description
Source Port Members	The ports to be used for filtering inbound packets.
Destination Port Members	The ports to be used for filtering outbound packets.

Configure storm control settings

A broadcast storm is the result of an excessive number of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses can overload network resources, cause the network to time out, or do both.

The switch measures the incoming packet rate per port for broadcast, multicast, unknown, and unicast packets and discards packets if the rate exceeds the defined value. You enable storm control per interface, by defining the packet type and the rate at which the packets are transmitted.

Configure global storm control settings

The global storm control settings apply to all ports. After you configure the global settings, you can specify storm control settings for one or more ports.

To configure global storm control settings:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Traffic Control > Storm Control**.

   The Storm Control page displays.

7. In the Storm Control section, from the **Ingress Control Mode** menu, select one of the following modes for storm control:
   - **Disabled**. Storm control is disabled. This is the default setting.
   - **Unknown Unicast**. If the rate of incoming unknown Layer 2 unicast traffic (that is, traffic for which a destination lookup failure occurs) increases beyond the configured threshold on an interface, the traffic is dropped.
   - **Multicast**. If the rate of incoming Layer 2 multicast traffic increases beyond the configured threshold on an interface, the traffic is dropped.
   - **Broadcast**. If the rate of incoming Layer 2 broadcast traffic increases beyond the configured threshold on an interface, the traffic is dropped.
8. If the selection from the **Ingress Control Mode** menu is *not* **Disabled**, specify whether the ingress control mode is enabled by selecting **Enable** or **Disable** from the **Status** menu.
9. In the **Threshold** field, specify the maximum rate at which unknown packets are forwarded.

   The range is a percent of the total threshold between 0 and 100%. The default is 5%.
10. From the **Control Action** mode menu, select one of the following options:
    - **None**. No action is taken. This is the default setting.
    - **Trap**. If the threshold of the configured broadcast storm is exceeded, a trap is sent.
    - **Shutdown**. If the threshold of the configured broadcast storm is exceeded, the port is shut down.
11. Click the **Apply** button.

    Your settings are saved.

Configure storm control settings for one or more ports

After you configure the global settings, you can specify storm control settings for one or more ports.

To configure storm control settings for one or more ports:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Traffic Control > Storm Control**.

   The Storm Control page displays.

   The default settings in the Port Settings section depends on the global storm control settings (see Configure global storm control settings on page 347), which apply to all ports.

7. In the Port Settings section, select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
8. From the **Status** menu, specify whether the ingress control mode is enabled for the port by selecting **Enable** or **Disable**.
9. In the **Threshold** field, specify the maximum rate at which unknown packets are forwarded for the port.

   The range is a percent of the total threshold between 0 and 100%. The default is 5%.

10. From the **Control Action** mode menu, select one of the following options for the port:
    - **None**. No action is taken.
    - **Trap**. If the threshold of the configured broadcast storm is exceeded, a trap is sent.
    - **Shutdown**. If the threshold of the configured broadcast storm is exceeded, the port is shut down.
11. Click the **Apply** button.

    Your settings are saved.

Manage port security

Port security lets you lock one or more ports on the switch. When a port is locked, the port can only forward packets with a source MAC addresses that you specifically allowed. The port discards all other packets.

Configure the global port security mode

To configure the global port security mode:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Traffic Control > Port Security > Port Security Configuration**.

   The Port Security Configuration page displays.
7. To enable port security on the switch, select the Port Security Mode **Enable** radio button.

   The default is Disable.
8. Click the **Apply** button.

   Your settings are saved.
9. To refresh the page, click the **Refresh** button.

The Port Security Violations table shows the view-only information about violations that occurred on ports that are enabled for port security.

The following table describes the fields in the Port Security Violations table.

Table 84. Port Security Violations information

Field	Description
Port	The physical interface.
Last Violation MAC	The source MAC address of the last packet that was discarded at a locked port.
VLAN ID	The VLAN ID corresponding to the last MAC address violation.

Configure port security settings for one or more interfaces

A MAC address can be defined as allowable by one of two methods: dynamically or statically. Both methods are used concurrently when a port is locked.

Dynamic locking implements a first arrival mechanism for port security. You specify how many addresses can be learned on the locked port. If the limit was not reached, then a packet with an unknown source MAC address is learned and forwarded normally. When the limit is reached, no more addresses are learned on the port. Any packets with source MAC addresses that were not already learned are discarded. You can effectively disable dynamic locking by setting the number of allowable dynamic entries to zero.

Static locking allows you to specify a list of MAC addresses that are allowed on a port. The behavior of packets is the same as for dynamic locking: only packets with an allowable source MAC address can be forwarded.

To configure port security settings 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Traffic Control > Port Security > Interface Configuration**.

   The Interface Configuration page displays.

7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.

8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. Specify the following settings:
   - **Port Security**. Enable or disable the port security feature for the selected interfaces The default is Disable.
   - **Max Learned MAC Address**: Specify the maximum number of dynamically learned MAC addresses. The default value is 4096. If you specify 0, the interface does not learn any MAC addresses.
   - **Max Static MAC Address**: Specify the maximum number of statically locked MAC addresses. The default value is 48.
   - **Enable Violation Shutdown**. Enable or disable shutdown of the selected interfaces if a packet with a disallowed MAC address is received. The default value is No, which means that the option is disabled.
   - **Enable Violation Traps**. Enable or disable the sending of new violation traps if a packet with a disallowed MAC address is received. The default value is No, which means that the option is disabled.
10. Click the **Apply** button.

    Your settings are saved.

View learned MAC addresses and convert them to static MAC addresses

After you enabled port security globally (see Configure the global port security mode on page 350) and enabled port security for specific interfaces (see Configure port security settings for one or more interfaces on page 351), you can convert a dynamically learned MAC address to a statically locked address.

To view learned MAC addresses for an individual interface or LAG and convert these MAC addresses to static MAC addresses:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Traffic Control > Port Security > Port Security Configuration**.

   The Port Security Configuration page displays.
7. Make sure that port security is globally enabled.

   For more information, see Configure the global port security mode on page 350.
8. Select **Security > Traffic Control > Port Security > Interface Configuration**.

   The Interface Configuration page displays.
9. Make sure that port security is enabled for the individual interface for which you want to view the dynamically learned MAC addresses.

   For more information, see Configure port security settings for one or more interfaces on page 351.
10. Select **Security > Traffic Control > Port Security > Security MAC Address**.

    The Port Security Configuration page displays.
11. In the Dynamic MAC Address Table section, from the **Port List** menu, select an individual interface.

    The Dynamic MAC Address Table displays the MAC addresses and their associated VLANs that were learned on the selected interface.

Field	Description
VLAN ID	The VLAN ID corresponding to the MAC address.
MAC Address	The MAC addresses learned on a specific port.

    In the Port Security Configuration section, the Number of Dynamic MAC Addresses Learned field displays the number of dynamically learned MAC addresses on the port.
12. To convert the dynamically learned MAC addresses to statically locked addresses, select the **Convert Dynamic Address to Static** check box.
13. Click the **Apply** button.

    The dynamic MAC address entries are converted to static MAC address entries in a numerically ascending order until the static limit is reached.
14. To refresh the page, click the **Refresh** button.

Configure protected ports

If a port is configured as protected, it does not forward traffic to any other protected ports on the switch, but it does forward traffic to unprotected ports. You can configure a port as protected or unprotected.

To configure protected ports:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Traffic Control > Protected Port**.

   The Protected Ports Membership page displays.
7. In the Ports table, click each port that you want to configure as a protected port.

   Protected ports are marked with a check mark. No traffic forwarding is possible between two protected ports.
8. Click the **Apply** button.

   Your settings are saved.

Manage private VLANs

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.

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.

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 one primary VLAN only. 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 five types of port designations:

- **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.
- **Community port**: The port is a host port that is a member of a community VLAN (a secondary VLAN within the private VLAN) and that can communicate with other community ports and promiscuous ports.
- **Isolated port**: The port is a host port that is a member of an isolated VLAN (a secondary VLAN within the private VLAN) and that can communicate with promiscuous ports only.

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 356.

   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 357.

   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 359.

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 configure port as a host port. However, a port that

4. Private VLAN host interface: Assign the interface to primary and secondary VLANs on page 361.

   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 363.

   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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Traffic Control > Private VLAN > Private VLAN Type Configuration**.

   The Private VLAN Type Configuration page displays.

7. Select the check box for the VLAN.

8. From the **Private VLAN Type** menu, select the type of private VLAN:
   - **Unconfigured**: The VLAN is not a private VLAN but a regular VLAN. This 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 one primary VLAN only. 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 one isolated VLAN only.
   - **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 **Apply** 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Traffic Control > Private VLAN > Private VLAN Association Configuration**.

   The Private VLAN Association Configuration page displays.

7. If you are changing an existing private VLAN association, select the check box for the private VLAN association.
8. Form the **Primary VLAN** menu, select the primary VLAN ID for the private VLAN.

   This selection specifies the primary VLAN within the private VLAN. You can associate secondary VLANs in the private VLAN with this primary VLAN.

   For information about configuring a primary VLAN for the private VLAN, see Assign a private VLAN type to a VLAN on page 356.

9. In the **Secondary VLANs** field, specify one or more secondary VLANs for the private VLAN.

   This selection specifies 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 specify individual VLAN ID, such as 10.
   - You can specify the VLAN range values separated by a hyphen, for example, 10-13.
   - You can specify the combination of both separated by commas, for example: 12,15,40–43,1000–1005, 2000.

   For information about configuring an isolated or community VLAN for the private VLAN, see Assign a private VLAN type to a VLAN on page 356.

10. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only information displayed on the page.

Table 85. Private VLAN Association

Field	Description
Isolated VLAN	The single isolated VLAN associated with the selected primary VLAN.
Community VLAN(s)	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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Traffic Control > Private VLAN > Private VLAN Association Configuration**.

   The Private VLAN Association Configuration page displays.
7. Select the check box for the private VLAN association.
8. 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 plan 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).

You can also configure a port (or LAG) to function as a promiscuous trunk for an uplink to a router or as an isolated trunk for a downlink to multiple devices. These types of private VLAN trunk ports can carry multiple private VLANs as well as regular VLANs.

To configure the private VLAN port mode:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Traffic Control > Private VLAN > Private VLAN Port Mode Configuration**.

   The Private VLAN Port Mode Configuration page displays.
7. 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 361.
   - **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 363.
8. Click the **Apply** 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 359), you can assign the interface to a single primary VLAN and 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Traffic Control > Private VLAN > Private VLAN Host Interface Configuration**.

   The Private VLAN Host Interface Configuration page displays.
7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch): Only physical interfaces are displayed. This is the default setting.
   - **LAG**: Only LAGs are displayed.
   - **All**: Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.

The interface that you select must be configured in Host mode (see Configure the private VLAN port mode on page 359).

9. In the **Host 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 356).

10. In the **Host Secondary VLAN** field, specify a secondary VLAN ID.

    You can 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 356).

11. Click the **Apply** button.

    Your settings are saved.

    The Operational VLAN(s) 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Traffic Control > Private VLAN > Private VLAN Host Interface Configuration**.

   The Private VLAN Host Interface Configuration page displays.

7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch): Only physical interfaces are displayed. This is the default setting.
   - **LAG**: Only LAGs are displayed.
   - **All**: Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.

   The interface that you select must be configured in Host mode (see Configure the private VLAN port mode on page 359).

9. 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 359), 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

- Enter your device admin password.
- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Traffic Control > Private VLAN > Private VLAN Promiscuous Interface Configuration**.

   The Private VLAN Promiscuous Interface Configuration page displays.

7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch): Only physical interfaces are displayed. This is the default setting.
   - **LAG**: Only LAGs are displayed.
   - **All**: Both physical interfaces and LAGs are displayed.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.

   The interface that you select must be configured in Promiscuous mode (see Configure the private VLAN port mode on page 359).
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 356).
10. In the **Promiscuous Secondary VLANs** 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 356).

    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 individual VLAN ID, such as 10.
    - You can specify the VLAN range values separated by a hyphen, for example, 10-13.
    - You can specify the combination of both separated by commas, for example: 12,15,40–43,1000–1005, 2000.

Note: The VLAN IDs that you specify overwrites the secondary VLANs that you configured on the Private VLAN Association Configuration page (see Configure a private VLAN association with a primary and secondary VLAN on page 357).

11. Click the **Apply** button.

    Your settings are saved.

    The Operational VLAN(s) 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > Traffic Control > Private VLAN > Private VLAN Promiscuous Interface Configuration**.

   The Private VLAN Promiscuous Interface Configuration page displays.
7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch): Only physical interfaces are displayed. This is the default setting.

- **LAG**: Only LAGs are displayed.
- **All**: Both physical interfaces and LAGs are displayed.

8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.

   The interface that you select must be configured in Promiscuous mode (see Configure the private VLAN port mode on page 359).
9. Click the **Delete** button.

   Your settings are saved.

   Your settings are saved. The interface is removed from the primary and secondary VLANs.

7

Manage Access Control Lists

This chapter contains the following sections:

- Use the ACL Wizard to create an uncomplicated ACL
- Configure a MAC ACL
- Configure MAC ACL rules
- Configure MAC ACL interface bindings
- Configure a basic or extended IPv4 ACL
- Configure rules for a basic IPv4 ACL
- Configure rules for an extended IPv4 ACL
- Configure an IPv6 ACL
- Configure rules for an IPv6 ACL
- Configure IP ACL interface bindings
- Configure VLAN ACL bindings

About access control lists

Access control lists (ACLs) ensure that only authorized users can access specific resources while blocking off any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and above all provide security for the network. The switch's software supports IPv4, IPv6, and MAC ACLs.

To configure an ACL:

1. Create an IPv4-based or IPv6-based or MAC-based ACL ID.
2. Create a rule and assign it to a unique ACL ID.
3. Define the rules, which can identify protocols, source, and destination IP and MAC addresses, and other packet-matching criteria.
4. Use the ID number to assign the ACL to a port or to a LAG.

To view ACL configuration examples, see Access control lists (ACLs) on page 471.

Use the ACL Wizard to create an uncomplicated ACL

The ACL Wizard helps you create an uncomplicated 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.

Note: The steps in the following procedure describe how you can create an ACL based on the destination MAC address. If you select a different type of ACL (or example, an ACL based on a source IPv4), the page displays different information.

Use the ACL Wizard to create an ACL

To use the ACL Wizard to create an ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > ACL Wizard**.

   The ACL Wizard page displays.
7. 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).

   You configure the following steps in the ACL Based on Destination MAC section.

8. In the **Sequence Number** field, enter a whole number in the range of 1 to 2147483647 that is used to identify the rule.
9. From the **Action** menu, select **Permit** or **Deny** to specify the action that must be taken if a packet matches the rule's criteria.
10. From the **Match Every** menu, select one of the following options:
    - **False**. Specifies that packets do not need to match the selected ACL and rule. With this selection, you can add additional criteria.

      For example, if you are setting up an ACL based on the destination MAC address, you can specify the destination MAC address, destination MAC mask, and VLAN ID.
    - **True**. Specifies that all packets must match the selected ACL and rule and are either permitted or denied. In this case, since all packets must match the rule, the option of configuring other match criteria is not available.
11. Specify the additional match criteria for the selected ACL type.

    The rest of the rule match criteria fields available for configuration depend on the selected ACL type. For information about the possible match criteria fields, see the following table.

ACL Based On	Fields
Destination MAC	• **Destination MAC**. Specify the destination MAC address to compare against an Ethernet frame. The valid format is xx:xx:xx:xx:xx:xx. The BPDU keyword might be specified using a destination MAC address of 01:80:C2:xx:xx:xx. • **Destination MAC Mask**. Specify the destination MAC address mask, which represents the bits in the destination MAC address to compare against an Ethernet frame. The valid format is xx:xx:xx:xx:xx:xx. The BPDU keyword might be specified using a destination MAC mask of 00:00:00:ff:ff:ff. • **VLAN**. Specify the VLAN ID to match within the Ethernet frame.
Source MAC	• **Source MAC**. Specify the source MAC address to compare against an Ethernet frame. The valid format is xx:xx:xx:xx:xx:xx. • **Source MAC Mask**. Specify the source MAC address mask, which represents the bits in the source MAC address to compare against an Ethernet frame. The valid format is (xx:xx:xx:xx:xx:xx). • **VLAN**. Specify the VLAN ID to match within the Ethernet frame.
Destination IPv4	• **Destination IP Address**. Specify the destination IP address. • **Destination IP Mask**. Specify the destination IP address mask.
Source IPv4	• **Source IP Address**. Specify the source IP address. • **Source IP Mask**. Specify the source IP address mask.
Destination IPv6	• **Destination Prefix**. Specify the destination prefix. • **Destination Prefix Length**. Specify the destination prefix length.
Source IPv6	• **Source Prefix**. Specify the source destination prefix. • **Source Prefix Length**. Specify the source prefix length.
Destination IPv4 L4 Port	• **Destination L4 port (protocol)**. Specify the destination IPv4 L4 port protocol. • **Destination L4 port (value)**. Specify the destination IPv4 L4 port value.

ACL Based On	Fields
Source IPv4 L4 Port	• **Source L4 port (protocol)**. Specify the source IPv4 L4 port protocol. • **Source L4 port (value)**. Specify the source IPv4 L4 port value.
Destination IPv6 L4 Port	• **Destination L4 port (protocol)**. Specify the destination IPv6 L4 port protocol. • **Destination L4 port (value)**. Specify the destination IPv6 L4 port value.
Source IPv6 L4 Port	• **Source L4 port (protocol)**. Specify the source IPv6 L4 port protocol. • **Source L4 port (value)**. Specify the source IPv6 L4 port value.

12. For this example procedure (in which an ACL based on the destination MAC address is created), configure the following settings:
    a. In the **Destination MAC** field, specify the destination MAC address that must be compared against the information in an Ethernet frame.

       The valid format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC address of 01:80:C2:xx:xx:xx.

    b. In the **Destination MAC Mask** field, specify the destination MAC address mask that must be compared against the information in an Ethernet frame.

       The valid format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC mask of 00:00:00:ff:ff:ff.

    c. In the **VLAN ID** field, specify which VLAN must be compared against the information in an Ethernet frame.

       Valid range of values is 1 to 4093. Either a VLAN range or VLAN can be configured.

    The fixed selection from the **Direction** menu is **Inbound**, which means that MAC ACL rules are applied to traffic entering the interface.
13. In the Ports and LAG tables in the Binding Configuration section, select the ports and LAGs to which the ACL must be applied.
14. Click the **Add** button.

    The rule is added to the ACL and is based on the destination MAC.

Modify an ACL rule that you created with the ACL Wizard

To modify an ACL rule that you created with the ACL Wizard:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > ACL Wizard**.

   The ACL Wizard page displays.
7. Select check box that is associated with the rule.
8. Update the match criteria as needed.
9. Click the **Apply** button.

   Your settings are saved.

Delete an ACL rule that you created with the ACL Wizard

To delete an ACL rule that you created with the ACL Wizard:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

The System Information page displays.

6. Select **Security > ACL > ACL Wizard**.

   The ACL Wizard page displays.

7. Select check box that is associated with the rule.
8. Click the **Delete** button.

   The rule is removed.

Configure a MAC ACL

A MAC ACL consists of a set of rules that are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit or Deny) is taken, and the additional rules are not checked for a match. Rules for the MAC ACL are created using the MAC ACL Rule Configuration page.

Multiple steps are involved in defining a MAC ACL and applying it to the switch:

1. Create the ACL ID (see Add a MAC ACL on page 373).
2. Create a MAC rule (see Configure MAC ACL rules on page 376).
3. Associate the MAC ACL with one or more interfaces (see Configure MAC ACL interface bindings on page 380).

You can view or delete MAC ACL configurations in the MAC Binding table (see View or delete MAC ACL bindings on page 381.

Add a MAC ACL

To add a MAC ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > ACL > Basic > MAC ACL**.

   The MAC ACL page displays.

   The MAC ACL Table displays the number of ACLs currently configured in the switch and the maximum number of ACLs that can be configured. The current size is equal to the number of configured IPv4 and IPv6 ACLs plus the number of configured MAC ACLs.

7. In the **Name** field, specify a name for the MAC ACL.

   The name string can include alphabetic, numeric, hyphen, underscore, or space characters only. The name must start with an alphabetic character.

8. Click the **Add** button.

   The MAC ACL is added.

   Each configured ACL displays the following information:

   - **Rules**. The number of rules currently configured for the MAC ACL.
   - **Direction**. The direction of packet traffic affected by the MAC ACL, which can be Inbound or blank.

Change the name of a MAC ACL

To change the name of a MAC ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > ACL > Basic > MAC ACL**.

   The MAC ACL page displays.

7. Select check box that is associated with the rule.
8. In the **Name** field, specify the new name.
9. Click the **Apply** button.

   Your settings are saved.

Delete a MAC ACL

To delete a MAC ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > ACL > Basic > MAC ACL**.

   The MAC ACL page displays.

7. Select check box that is associated with the rule.
8. Click the **Delete** button.

   The rule is removed.

Configure MAC ACL rules

You can define rules for MAC-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. A default *deny all* rule is the last rule of every list.

Add a rule to a MAC ACL

To add a rule to a MAC ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Basic > MAC Rules**.

   The MAC Rules page displays.
7. From the **ACL Name** menu, select the MAC ACL.
8. In the **Sequence Number** field, enter a number in the range of 1 to 2147483647 to identify the rule.
9. 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.
10. In the **Assign Queue** field, specify the hardware egress queue identifier that must be used to handle all packets matching this ACL rule.

The valid range of queue IDs is 0 to 7.

11. From the **Mirror Interface** menu, select the specific egress interface to which the matching traffic stream must be copied, in addition to being forwarded normally by the switch.

    This field cannot be set if a redirect interface is already configured for the ACL rule. This field is visible for a Permit action.

12. From the **Redirect Interface** menu, select the egress interface to which the matching traffic stream must be redirected, bypassing any forwarding decision normally performed by the switch.

    This field cannot be set if a mirror interface is already configured for the ACL rule.

13. From the **Match Every** menu, select whether each Layer 2 MAC packet must be matched against the rule:
    - **True**. Each packet must match the selected ACL rule.
    - **False**. Not all packets need to match the selected ACL rule.

14. In the **CoS** field, specify the 802.1p user priority that must be compared against the information in an Ethernet frame.

    The valid range of values is 0 to 7.

15. In the **Destination MAC** field, specify the destination MAC address that must be compared against the information in an Ethernet frame.

    The valid format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC address of 01:80:C2:xx:xx:xx.

16. In the **Destination MAC Mask** field, specify the destination MAC address mask that must be compared against the information in an Ethernet frame.

    The valid format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC mask of 00:00:00:ff:ff:ff.

17. From the **EtherType Key** menu, select the EtherType value that must be compared against the information in an Ethernet frame.

    The valid values are as follows:

    - **Appletalk**
    - **ARP**
    - **IBM SNA**
    - **IPv4**
    - **IPv6**
    - **IPX**
    - **MPLS multicast**
    - **MPLS unicast**
    - **NetBios**
    - **Novell**
    - **PPPoE**

- **RARP**
- **User Value**

18. In the **EtherType User Value** field, specify the customized EtherType value that must be used when you select **User Value** from the **EtherType Key** menu.

    This value must be compared against the information in an Ethernet frame. The valid range of values is 0x0600 to 0xFFFF.

19. In the **Source MAC** field, specify the source MAC address that must be compared against the information in an Ethernet frame.

    The valid format is xx:xx:xx:xx:xx:xx.

20. In the **Source MAC Mask** field, specify the source MAC address mask that must be compared against the information in an Ethernet frame.

    The valid format is xx:xx:xx:xx:xx:xx.

21. In the **VLAN** field, specify the VLAN ID that must be compared against the information in an Ethernet frame.

    The valid range of values is 1 to 4095. Either VLAN range or VLAN can be configured.

22. From the **Logging** menu, select whether to enable or disable logging.

    When set to **Enable**, logging is enabled for this ACL rule (subject to resource availability on the switch). If the access list trap flag is also enabled, periodic traps are generated, indicating the number of times the rule was evoked during the report interval. A fixed five-minute report interval is used for the switch. A trap is not issued if the ACL rule hit count is zero for the interval. This field is only supported for a deny action.

23. Click the **Add** button.

    The rule is added.

Change the match criteria for a MAC rule

To change the match criteria for a MAC rule:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Basic > MAC Rules**.

   The MAC Rules page displays.
7. Select the check box that is associated with the rule.
8. Modify the fields as needed.
9. Click the **Apply** button.

   Your settings are saved.

Delete a rule for a MAC ACL

To delete a rule for a MAC:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Basic > MAC Rules**.

   The MAC Rules page displays.

7. Select the check box that is associated with the rule.
8. Click the **Delete** button.

   The rule is removed.

Configure MAC ACL interface bindings

When an ACL is bound to an interface, all the rules that are defined are applied to the selected interface. You can assign MAC ACL lists to ACL priorities and interfaces.

Bind a MAC ACL to one or more interfaces

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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Basic > MAC Binding Configuration**.

   The MAC Binding Configuration page displays.
7. From the **ACL ID** menu, select an ACL.

   The fixed selection from the **Direction** menu is **Inbound**, which means that MAC ACL rules are applied to traffic entering the interface.
8. In the **Sequence Number** field, optionally specify a number to indicate the order of the access list relative to other access lists already assigned to the interface and direction.

A low number indicates high precedence order. If a sequence number is already in use for the interface and direction, the specified access list replaces the currently attached access list using that sequence number. If you do not specify the sequence number, a sequence number that is one number greater than the highest sequence number currently in use for this interface and direction is used. The valid range is 1–4294967295.

9. To add the selected ACL to a port or LAG, in the Ports table or LAG table, click the port or LAG so that a check mark displays.

   You can add the ACL to several ports and LAGs.

   The Ports and LAG tables display the available and valid interfaces for ACL binding. All nonrouting physical interfaces, VLAN interfaces, and interfaces participating in LAGs are listed.

10. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only information displayed in the Interface Binding Status table.

Table 86. Interface Binding Status table

Field	Description
Interface	The interface of the ACL assigned.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID	The ACL number (for an IP ACL) or ACL name (for a MAC ACL) identifying the ACL assigned to the selected interface and direction.
Sequence Number	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.

View or delete MAC ACL bindings

You can view or delete MAC ACL bindings from the MAC ACL binding table.

To view or delete MAC ACL bindings:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Basic > Binding Table**.

   The MAC Binding Table page displays.
7. To delete a MAC ACL-to-interface binding, do the following:
   a. Select the check box next to the interface.
   b. Click the **Delete** button.

   The binding is removed.

The following table describes the view-only information that is displayed in the MAC binding table.

Table 87. MAC Binding Table

Field	Description
Interface	The interface of the ACL assigned.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID	The ACL name identifying the ACL assigned to the selected interface and direction.
Sequence Number	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.

Configure a basic or extended IPv4 ACL

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 taken, and the additional rules are not checked for a match. You must specify the interfaces to which an IPv4 ACL applies, as well as whether it applies to inbound or outbound traffic.

Multiple steps are involved in defining an IPv4 ACL and applying it to the switch:

1. Add an IPv4 ACL ID (see Add an IP ACL on page 383).

   The differences between a basic IPv4 ACL and an extended IPv4 ACL are as follows:

   - **Numbered ACL from 1 to 99**. Creates a basic IPv4 ACL, which allows you to permit or deny traffic from a source IP address.
   - **Numbered ACL from 100 to 199**. Creates an extended IPv4 ACL, which allows you to permit or deny specific types of Layer 3 or Layer 4 traffic from a source IP address to a destination IP address. This type of ACL provides more granularity and filtering capabilities than the basic IP ACL.
   - **Named IP ACL**. Create an extended IPv4 ACL with a name string that is up to 31 alphanumeric characters in length. The name must start with an alphabetic character.
2. Create an IPv4 rule (see Configure rules for a basic IPv4 ACL on page 386 or Configure rules for an extended IPv4 ACL on page 389).
3. Associate the IPv4 ACL with one or more interfaces (see Configure IP ACL interface bindings on page 406).

You can view or delete IPv4 ACL configurations in the IP ACL Binding table (see View or delete an IP ACL binding on page 408.

Add an IP ACL

To add an IP ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Advanced > IP ACL**.

The IP ACL Configuration page displays.

The IP ACL page shows the current size of the ACL table compared to the maximum size of the ACL table. The current size is equal to the number of configured IPv4 and IPv6 ACLs plus the number of configured MAC ACLs. The maximum size is 100.

The Current Number of ACL field displays the current number of all ACLs configured on the switch.

The Maximum ACL field displays the maximum number of IP ACLs that can be configured on the switch.

7. In the **IP ACL ID** field, specify the ACL ID or IP ACL name, which depends on the IP ACL type. The IP ACL ID is an integer in the following range:
   - **1–99**. Creates a basic IP ACL, which allows you to permit or deny traffic from a source IP address.
   - **100–199**. Creates an extended IP ACL, which allows you to permit or deny specific types of Layer 3 or Layer 4 traffic from a source IP address to a destination IP address. This type of ACL provides more granularity and filtering capabilities than the standard IP ACL.
   - **IP ACL Name**. Create an IPv4 ACL name string that is up to 31 alphanumeric characters in length. The name must start with an alphabetic character.

   Each configured ACL displays the following information:

   - **Rules**. The number of rules currently configured for the IP ACL.
   - **Type**. Identifies the ACL as a basic IP ACL (with ID from 1 to 99), extended IP ACL (with ID from 100 to 199), or a named IP ACL.
8. Click the **Add** button.

   The IP ACL is added to the switch configuration.

Change the number or name of an IPv4 ACL

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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Advanced > IP ACL**.

   The IP ACL Configuration page displays.
7. Select the check box that is associated with the IP ACL.
8. In the **IP ACL** field, specify the new number or name.
9. Click the **Apply** button.

   Your settings are saved.

Delete an IP ACL

To delete an IP ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Advanced > IP ACL**.

   The IP ACL Configuration page displays.

7. Select the check box that is associated with the IP ACL.
8. Click the **Delete** button.

   The IP ACL is removed.

Configure rules for a basic IPv4 ACL

You can define rules for IP-based standard ACLs (basic ACLs). The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

Note: An implicit *deny all* rule is included at the end of an ACL list. This means that if an ACL is applied to a packet, and if none of the explicit rules match, then the final implicit *deny all* rule applies and the packet is dropped.

Add a rule for a basic IPv4 ACL

To add a rule for a basic 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Advanced > IP Rules**.

The IP Rules page displays and shows the Basic ACL Rule Table section.

If no rules exist, the Basic ACL Rule Table shows the message *No rules have been configured for this ACL*. If one or more rules exist for the ACL, the rules display in the Basic ACL Rule Table.

7. From the **ACL ID** menu, select the IP ACL for which you want to add a rule.

   For basic IP ACLs, this must be an ID in the range from 1 to 99.

8. Click the **Add** button.

   The Standard ACL Rule Configuration(1-99) page displays.

9. Specify the following match criteria for the rule:
   - **Sequence Number**. Enter an ACL sequence number in the range of 1 to 2147483647 that is used to identify the rule. An IP ACL can contain up to 50 rules.
   - **Action**. Select the ACL forwarding action, which is one of the following:
     - **Permit**. Forward packets that meet the ACL criteria.
     - **Deny**. Drop packets that meet the ACL criteria.
   - **Egress Queue**. If the selection form the **Action** menu is **Permit**, you can specify the hardware egress queue identifier that is used to handle all packets matching this IP ACL rule. The range of queue IDs is 0 to 7.
   - **Logging**. If the selection form the **Action** menu is **Deny**, you can enable logging for the ACL by selecting the **Enable** radio button. (Logging is subject to resource availability on the switch.)

     If the access list trap flag is also enabled, periodic traps are generated, indicating the number of times this rule was evoked during the report interval. A fixed five-minute report interval is used for the switch. A trap is not issued if the ACL rule hit count is zero for the current interval.
   - **Match Every**. Select whether all packets must match the selected IP ACL rule:
     - **Enable**. All packets must match the selected IP ACL rule and are either permitted or denied.
     - **Disable**. Not all packets need to match the selected IP ACL rule.
   - **Interface Mirror**. From the **Mirror** menu, select the specific egress interface to which the matching traffic stream must be copied, in addition to being forwarded normally by the switch.

     This field cannot be set if a redirect interface is already configured for the IP ACL rule. This field is visible for a Permit action.
   - **Interface Redirect**. From the **Redirect** menu, select the egress interface to which the matching traffic stream must be redirected, bypassing any forwarding decision normally performed by the switch.

     This field cannot be set if a mirror interface is already configured for the IP ACL rule.
   - **Src IP Address**. Enter an IP address using dotted-decimal notation to be compared to a packet's source IP address as a match criterion for the selected IP ACL rule.

- **Src IP Mask**. Specify the IP mask in dotted-decimal notation to be used with the source IP address value.

10. Click the **Apply** button.

    Your settings are saved.

Modify the match criteria for a basic IPv4 ACL rule

To modify the match criteria for a basic 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > ACL > Advanced > IP Rules**.

   The IP Rules page displays and shows the Basic ACL Rule Table section.

7. From the **ACL ID** menu, select the ACL that includes the rule that you want to modify.
8. In the Basic ACL Rule Table, click the rule.

   The rule is a hyperlink. The Standard ACL Rule Configuration(1-99) page displays.

9. Modify the basic IP ACL rule criteria.
10. Click the **Apply** button.

    Your settings are saved.

Delete a basic IPv4 ACL rule

To delete a basic 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Advanced > IP Rules**.

   The IP Rules page displays and shows the Basic ACL Rule Table section.
7. From the **ACL ID** menu, select the ACL that includes the rule that you want to modify.
8. In the Basic ACL Rule Table, select the check box that is associated with the rule.
9. Click the **Delete** button.

   The rule is removed.

Configure rules for an extended IPv4 ACL

You can define rules for extended IP-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

Note: An implicit *deny all* rule is included at the end of an ACL list. This means that if an ACL is applied to a packet and if none of the explicit rules match, then the final implicit *deny all* rule applies and the packet is dropped.

Add a rule for an extended IPv4 ACL

To add a rule for 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > ACL > Advanced > IP Extended Rules**.

   The IP Rules page displays and shows the Extended ACL Rule Table section.

   If no rules exists, the Extended ACL Rule Table shows the message *No rules have been configured for this ACL*. If one or more rules exist for the ACL, the rules display in the Extended ACL Rule Table.

7. From the **ACL ID/Name** menu, select the IP ACL for which you want to add a rule.

   For extended IP ACLs, this must be an ID in the range from 101 to 199 or a name.

8. Click the **Add** button.

   The Extended ACL Rule Configuration(100-199) page displays.

9. Configure the following match criteria for the rule:
   - **Sequence Number**. Enter a whole number in the range of 1 to 2147483647 that is used to identify the rule. An extended IP ACL can contain up to 50 rules.
   - **Action**. Select the ACL forwarding action, which is one of the following:
     - **Permit**. Forward packets that meet the ACL criteria.
     - **Deny**. Drop packets that meet the ACL criteria.

- **Egress Queue**. If the selection from the **Action** menu is **Permit**, select the hardware egress queue identifier that is used to handle all packets matching this IP ACL rule. The range of queue IDs is 0 to 7.
- **Logging**. If the selection from the **Action** menu is **Deny**, you can enable logging for the ACL by selecting the **Enable** radio button. (Logging is subject to resource availability in the device.)

  If the access list trap flag is also enabled, periodic traps are generated, indicating the number of times this rule was evoked during the report interval. A fixed five-minute report interval is used for the switch. A trap is not issued if the ACL rule hit count is zero for the current interval.
- **Interface**. For a Permit action, use either a mirror interface or a redirect interface:
  - Select the **Mirror** radio button and use the menu to specify the egress interface to which the matching traffic stream is copied, in addition to being forwarded normally by the device.
  - Select the **Redirect** radio button and use the menu to specify the egress interface to which the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device.
- **Match Every**. From the **Match Every** menu, select whether all packets must match the selected IP ACL rule:
  - **False**. Not all packets need to match the selected IP ACL rule. You can configure other match criteria on the page.
  - **True**. All packets must match the selected IP ACL rule and are either permitted or denied. In this case, you cannot configure other match criteria on the page.
- **Protocol Type**. From the menu, select a protocol that a packet's IP protocol must be matched against: **IP**, **ICMP**, **IGMP**, **TCP**, **UDP**, **EIGRP**, **GRE**, **IPINIP**, **OSPF**, **PIM**, or **Other**. If you select **Other**, specify enter a protocol number from 0 to 255.

  Note: The selection form the **Protocol Type** menu determines the configuration options that are available on the page.
- **Src**. In the **Src** field, enter a source IP address, using dotted-decimal notation, to be compared to a packet's source IP address as a match criterion for the selected IP ACL rule:
  - If you select the **IP Address** radio button, enter an IP address or an IP address range. You can enter a relevant wildcard mask to apply this criteria. If this field is left empty, it means *any*.
  - If you select the **Host** radio button, the wildcard mask is configured as 0.0.0.0. If this field is left empty, it means *any*.

  The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard of 255.255.255.255 indicates that *all* of the bits are important.
- **Src L4**. The options are available only when the protocol is set to TCP or UDP. Use the source L4 port option to specify relevant matching conditions for L4 port numbers in the extended ACL rule.

The default matching condition for L4 port numbers is **Equal**. That is, the IP ACL rule matches only if the Layer 4 source port number is equal to the specified port number or port protocol. You can also set **Not Equal**, **Less Than**, and **Greater Than**, and add values to compare against.

You can select either the **Port** radio button or the **Range** radio button:

- If you select the **Port** radio button, you can either enter the port number yourself or select one of the following protocols from the menu:
  - The source IP TCP port protocols are **Domain**, **Echo**, **FTP**, **FTP data**, **www-http**, **SMTP**, **Telnet**, **POP2**, **POP3**, and **BGP**.
  - The source IP UDP port protocols are **Domain**, **Echo**, **SNMP**, **NTP**, **RIP**, **Time**, **Who**, and **TFTP**.

  Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

  Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.
- If you select the **Range** radio button, the IP ACL rule matches only if the Layer 4 source port number is within the specified port range. The starting port, ending port, and all ports in between are a part of the Layer 4 port range.

  The **Start Port** and **End Port** fields identify the first and last ports that are part of the port range. The values can range from 0 to 65535.

  You can either enter the port range yourself or select one of the following protocols from the menu:

  - The destination IP TCP port protocols are **Domain**, **Echo**, **FTP**, **FTP data**, **www-http**, **SMTP**, **Telnet**, **POP2**, **POP3**, and **BGP**.
  - The destination IP UDP port protocols are **Domain**, **Echo**, **SNMP**, **NTP**, **RIP**, **Time**, **Who**, and **TFTP**.

  Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

  Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.

  The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard of 255.255.255.255 indicates that *all* of the bits are important.

- **Dst**. In the **Dst** field, enter a destination IP address, using dotted-decimal notation, to be compared to a packet's destination IP address as a match criterion for the selected IP ACL rule:
  - If you select the **IP Address** radio button, enter an IP address with a relevant wildcard mask to apply this criteria. If this field is left empty, it means *any*.
  - If you select the **Host** radio button, the wildcard mask is configured as 0.0.0.0. If this field is left empty, it means *any*.

The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard of 255.255.255.255 indicates that *all* of the bits are important.

- **Dst L4**. The options are available only when the protocol is set to TCP or UDP. Use the destination L4 port option to specify relevant matching conditions for L4 port numbers in the extended ACL rule.

  The default matching condition for L4 port numbers is **Equal**. That is, the IP ACL rule matches only if the Layer 4 destination port number is equal to the specified port number or port protocol. You can also set **Not Equal**, **Less Than**, and **Greater Than**, and add values to compare against.

  You can select either the **Port** radio button or the **Range** radio button:

  - If you select the **Port** radio button, you can either enter the port number yourself or select one of the following protocols from the menu.
    - The destination IP TCP port protocols are **Domain**, **Echo**, **FTP**, **FTP data**, **www-http**, **SMTP**, **Telnet**, **POP2**, **POP3**, and **BGP**.
    - The destination IP UDP port protocols are **Domain**, **Echo**, **SNMP**, **NTP**, **RIP**, **Time**, **Who**, and **TFTP**.

    Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

    Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.
  - If you select the **Range** radio button, the IP ACL rule matches only if the Layer 4 destination port number is within the specified port range. The starting port, ending port, and all ports in between are a part of the Layer 4 port range.

    The **Start Port** and **End Port** fields identify the first and last ports that are part of the port range. They values can range from 0 to 65535.

    You can either select the enter the port range yourself or select one of the following protocols from the menu:

    - The destination IP TCP port range names are **Domain**, **Echo**, **FTP**, **FTP data**, **www-http**, **SMTP**, **Telnet**, **POP2**, **POP3**, and **BGP**.
    - The destination IP UDP port range names are **Domain**, **Echo**, **SNMP**, **NTP**, **RIP**, **Time**, **Who**, and **TFTP**.

    Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

    Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.

    The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard of 255.255.255.255 indicates that *all* of the bits are important.

- **IGMP Type**. If you specify the IGMP type, the IP ACL rule matches the specified IGMP message type. Possible values are in the range 0 to 255. If this field is left empty, it means *any*.
- **ICMP**. Select either the **Type** or **Message** radio button:
  - If you select the **Type** radio button, note the following:
    - The **Type** and **Code** fields are enabled only if the protocol is ICMP. Use these fields to specify a match condition for ICMP packets:
    - The IP ACL rule matches the specified ICMP message type. Possible type numbers are in the range from 0 to 255.
    - If you specify information in the **Message** field, the IP ACL rule matches the specified ICMP message code. Possible values for the code can be in the range from 0 to 255.
    - If these fields are left empty, it means *any*.
  - If you select the **Message** radio button, select the type of the ICMP message to match with the selected IP ACL rule. Specifying a type of message implies that both the ICMP type and ICMP code are specified. The ICMP message is decoded into the corresponding ICMP type and ICMP code within the ICMP type.

    The IPv4 ICMP message types are **echo**, **echo-reply**, **host-redirect**, **mobile-redirect**, **net-redirect**, **net-unreachable**, **redirect**, **packet-too-big**, **port-unreachable**, **source-quench**, **router-solicitation**, **router-advertisement**, **ttl-exceeded**, **time-exceeded**, and **unreachable**.
- **Fragments**. Either select the **Enable** radio button to allow initial fragments (that is, the fragment bit is asserted) or leave the default Disable radio button selected to prevent initial fragments from being used.

  This option is not valid for rules that match L4 information such as a TCP port number, because that information is carried in the initial packet.
- **Service Type**. Select a service type match condition for the extended IP ACL rule.

  The possible options are **IP DSCP**, **IP Precedence**, and **IP TOS**, which are alternative methods to specify a match criterion for the same service type field in the IP header. Each method uses a different user notation. After you make a selection, you can specify the appropriate values:

  - **IP DSCP**. This is an optional configuration. Specify the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order 6 bits of the service type octet in the IP header. Enter an integer from 0 to 63. To select the IP DSCP, select one of the DSCP keywords from the menu. To specify a numeric value, select **Other** and a field displays in which you can enter numeric value of the DSCP.
  - **IP Precedence**. This is an optional configuration. The IP precedence field in a packet is defined as the high-order 3 bits of the service type octet in the IP header. Enter an integer from 0 to 7.
  - **IP TOS**. This is an optional configuration. The IP ToS field in a packet is defined as all 8 bits of the service type octet in the IP header. The ToS bits value is a hexadecimal number that is composed of numbers 00 to 09 and AA to FF. The

ToS mask value is a hexadecimal number that is composed of numbers 00 to FF. The ToS mask denotes the bit positions in the ToS bits value that are used for comparison against the IP ToS field in a packet.

For example, to check for an IP ToS value for which bit 7 is set and is the most significant value, for which bit 5 is set, and for which bit 1 is cleared, use a ToS bits value of 0xA0 and a ToS mask of 0xFF.

10. Click the **Apply** button.

    Your settings are saved.

Modify the match criteria for an extended IPv4 ACL rule

To modify 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > ACL > Advanced > IP Extended Rules**.

   The IP Rules page displays and shows the Extended ACL Rule Table section.

7. From the **ACL ID** menu, select the ACL that includes the rule that you want to modify.
8. In the Extended ACL Rule Table, click the rule.

   The rule is a hyperlink. The Extended ACL Rule Configuration(100-199) page displays.

9. Modify the extended IP ACL rule criteria.
10. Click the **Apply** button.

    Your settings are saved.

Delete an extended IPv4 ACL rule

To delete 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Advanced > IP Extended Rules**.

   The IP Rules page displays and shows the Extended ACL Rule Table section.
7. From the **ACL ID** menu, select the ACL that includes the rule that you want to delete.
8. In the Extended ACL Rule Table, select the check box that is associated with the rule.
9. Click the **Delete** button.

   The rule is removed.

Configure an IPv6 ACL

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 taken, and the additional rules are not checked for a match. You must specify the interfaces to which an IPv6 ACL applies, as well as whether it applies to inbound or outbound traffic.

Multiple steps are involved in defining an IPv6 ACL and applying it to the switch:

1. Add an IPv6 ACL ID (see Add an IPv6 ACL on page 397).

   An IPv6 ACL must start with a name string that is up to 31 alphanumeric characters in length. The name must start with an alphabetic character.
2. Create an IPv6 rule (see Configure rules for an IPv6 ACL on page 400).
3. Associate the IPv6 ACL with one or more interfaces (see Configure IP ACL interface bindings on page 406).

You can view or delete IPv6 ACL configurations in the IP ACL Binding table (see View or delete an IP ACL binding on page 408.

Add an IPv6 ACL

To add an IPv6 ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Advanced > IPv6 ACL**.

   The IPv6 Configuration page displays.
7. In the **IPv6 ACL** field, specify a name to identify the IPv6 ACL.

   This is the IPv6 ACL name string, which includes up to 31 alphanumeric characters only. The name must start with an alphabetic character.
8. Click the **Add** button.

   The IPv6 ACL is added.

The following table describes the view-only information displayed on the page.

Table 88. IPv6 Configuration and IPv6 ACL Table information

Field	Description
Current Number of ACL	The current number of the IP ACLs configured on the switch.
Maximum ACL	The maximum number of IP ACLs that can be configured on the switch.
Rules	The number of the rules associated with the IP ACL.
Type	The type is IPv6 ACL.

Change the name of an 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Advanced > IPv6 ACL**.

   The IPv6 Configuration page displays.
7. Select the check box that is associated with the IPv6 ACL.
8. In the **IPv6 ACL** field, specify the new name.
9. Click the **Apply** button.

   Your settings are saved.

Delete an IPv6 ACL

To delete an IPv6 ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Advanced > IPv6 ACL**.

   The IPv6 Configuration page displays.
7. Select the check box that is associated with the IPv6 ACL.
8. Click the **Delete** button.

   The IPv6 ACL is removed.

Configure rules for an IPv6 ACL

You can define rules for IPv6 ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

Add a rule for an IPv6 ACL

Add a rule for an ACL IPv6:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Advanced > IPv6 Rules**.

   The IP Rules page displays and shows the IPv6 ACL Rule Table section.

   If no rules exists, the IPv6 ACL Rule Table shows the message *No rules have been configured for this ACL*. If one or more rules exist for the ACL, the rules display in the IPv6 ACL Rule Table.
7. From the **ACL Name** menu, select the IPv6 ACL for which you want to add a rule.

   An IPv6 ACL can contain up to 50 rules.
8. Click the **Add** button.

   The IPv6 ACL Rule Configuration page displays.

9. Configure the following match criteria for the rule:
   - **Sequence Number**. Enter a whole number in the range of 1 to 2147483647 that is used to identify the rule.
   - **Action**. Select the ACL forwarding action by selecting one of the following radio buttons:
     - **Permit**. Forward packets that meet the ACL criteria.
     - **Deny**. Drop packets that meet the ACL criteria.
   - **Egress Queue**. If you select the **Permit** radio button, select the hardware egress queue identifier that is used to handle all packets matching this IPv6 ACL rule. The range of queue IDs is 0 to 7.
   - **Logging**. If you select the **Deny** radio button, you can enable logging for the ACL by selecting the **Enable** radio button. (Logging is subject to resource availability in the device.)

     If the access list trap flag is also enabled, periodic traps are generated, indicating the number of times this rule was evoked during the report interval. A fixed five-minute report interval is used for the switch. A trap is not issued if the ACL rule hit count is zero for the current interval.
   - **Interface**. For a Permit action, use either a mirror interface or a redirect interface:
     - Select the **Mirror** radio button and use the menu to specify the egress interface to which the matching traffic stream is copied, in addition to being forwarded normally by the device.
     - Select the **Redirect** radio button and use the menu to specify the egress interface to which the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device.
   - **Match Every**. Select whether all packet must match the selected IPv6 ACL rule:
     - **Disable**. Not all packets need to match the selected IPv6 ACL rule. You can configure other match criteria on the page.
     - **Enable**. All packets must match the selected IPv6 ACL rule and are either permitted or denied. In this case, you cannot configure other match criteria on the page.
   - **Protocol Type**. Specify the IPv6 protocol type in one of the following ways:
     - From the **Protocol Type** menu, select **IPv6**, **ICMPv6**, **TCP**, or **UDP**.
     - From the **Protocol Type** menu, select **Other**, and in the associated field, specify an integer ranging from 0 to 255. This number represents the IPv6 protocol.

     Note: The selection form the **Protocol Type** menu determines the configuration options that are available on the page.
   - **Src**. In the **Src** field, enter a source IPv6 address or source IPv6 address range to be compared to a packet's source IPv6 address as a match criterion for the selected IPv6 ACL rule:
     - If you select the **IPv6 Address** radio button, enter an IPv6 address or IPv6 range to apply this criteria. If this field is left empty, it means *any*.

- If you select the **Host** radio button, enter a host source IPv6 address to match the specified IPv6 address. If this field is left empty, it means *any*.

The source IPv6 address argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal numbers using 16-bit values between colons.

- **Src L4**. The options are available only when the protocol is set to TCP or UDP. Use the source L4 port option to specify relevant matching conditions for L4 port numbers in the IPv6 ACL rule.

  The default matching condition for L4 port numbers is **Equal**. That is, the IPv6 ACL rule matches only if the Layer 4 source port number is equal to the specified port number or port protocol. You can also set **Not Equal**, **Less Than**, and **Greater Than**, and add values to compare against.

  You can select either the **Port** radio button or the **Range** radio button:

  - If you select the **Port** radio button, you can either enter the port number yourself or select one of the following protocols from the menu:
    - The source IP TCP port protocols are **Domain**, **Echo**, **FTP**, **FTP data**, **www-http**, **SMTP**, **Telnet**, **POP2**, **POP3**, and **BGP**.
    - The source IP UDP port protocols are **Domain**, **Echo**, **SNMP**, **NTP**, **RIP**, **Time**, **Who**, and **TFTP**.

    Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

    Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.
  - If you select the **Range** radio button, the IPv6 ACL rule matches only if the Layer 4 source port number is within the specified port range. The starting port, ending port, and all ports in between are a part of the Layer 4 port range.

    The **Start Port** and **End Port** fields identify the first and last ports that are part of the port range. They values can range from 0 to 65535.

    You can either enter the port range yourself or select one of the following protocols from the menu:
    - The source IP TCP port protocols are **Domain**, **Echo**, **FTP**, **FTP data**, **www-http**, **SMTP**, **Telnet**, **POP2**, **POP3**, and **BGP**.
    - The source IP UDP port protocols are **Domain**, **Echo**, **SNMP**, **NTP**, **RIP**, **Time**, **Who**, and **TFTP**.

    Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

    Select **Other** from the menu to enter port numbers. If you select **Other** from the menu but leave the fields blank, it means *any*.

- **Dst**. In the **Dst** field, enter a destination IPv6 address to be compared to a packet's destination IPv6 address as a match criterion for the selected IPv6 ACL rule:
  - If you select the **IPv6 Address** radio button, enter an IPv6 address to apply this criteria. If this field is left empty, it means *any*.
  - If you select the **Host** radio button, enter a host source IPv6 address to match the specified IPv6 address. If this field is left empty, it means *any*.

  The source IPv6 address argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal numbers using 16-bit values between colons.
- **Dst L4**. The options are available only when the protocol is set to TCP or UDP. Use the destination L4 port option to specify relevant matching conditions for L4 port numbers in the IPv6 ACL rule.

  The default matching condition for L4 port numbers is **Equal**. That is, the IPv6 ACL rule matches only if the Layer 4 source port number is equal to the specified port number or port protocol. You can also set **Not Equal**, **Less Than**, and **Greater Than**, and add values to compare against.

  You can select either the **Port** radio button or the **Range** radio button:

  - If you select the **Port** radio button, you can either enter the port number yourself or select one of the following protocols from the menu:
    - The destination IP TCP port protocols are **Domain**, **Echo**, **FTP**, **FTP data**, **www-http**, **SMTP**, **Telnet**, **POP2**, **POP3**, and **BGP**.
    - The destination IP UDP port protocols are **Domain**, **Echo**, **SNMP**, **NTP**, **RIP**, **Time**, **Who**, and **TFTP**.

    Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

    Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.
  - If you select the **Range** radio button, the IPv6 ACL rule matches only if the Layer 4 destination port number is within the specified port range. The starting port, ending port, and all ports in between are a part of the Layer 4 port range.

    The **Start Port** and **End Port** fields identify the first and last ports that are part of the port range. They values can range from 0 to 65535.

    You can either enter the port range yourself or select one of the following protocols from the menu:

    - The destination IP TCP port protocols are **Domain**, **Echo**, **FTP**, **FTP data**, **www-http**, **SMTP**, **Telnet**, **POP2**, **POP3**, and **BGP**.
    - The destination IP UDP port protocols are **Domain**, **Echo**, **SNMP**, **NTP**, **RIP**, **Time**, **Who**, and **TFTP**.

    Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

Select **Other** from the menu to enter port numbers. If you select **Other** from the menu but leave the fields blank, it means *any*.

- **ICMPv6**. Select either the **Type** or **Message** radio button:
  - If you select the **Type** radio button, note the following:
    - The **Type** and **Message** fields are enabled only if the protocol is ICMPv6. Use these fields to specify a match condition for ICMPv6 packets.
    - The IPv6 ACL rule matches the specified ICMPv6 message type. Possible type numbers are in the range from 0 to 255.
    - If you specify information in the **Message** field, the IPv6 ACL rule matches the specified ICMPv6 message code. Possible values for code can be in the range from 0 to 255.
    - If these fields are left empty, it means *any*.
  - If you select the **Message** radio button, select the type of the ICMPv6 message to match with the selected IPv6 ACL rule. Specifying a type of message implies that both the ICMPv6 type and ICMPv6 code are specified. The ICMPv6 message is decoded into the corresponding ICMPv6 type and ICMPv6 code within the ICMP type.

    The ICMPv6 message types are **destination-unreachable**, **echo-reply**, **echo-request**, **header**, **hop-limit**, **mld-query**, **mld-reduction**, **mld-report**, **nd-na**, **nd-ns**, **next-header**, **no-admin**, **no-route**, **packet-too-big**, **port-unreachable**, **router-solicitation**, **router-advertisement**, **router-renumbering**, **time-exceeded**, and **unreachable**.
- **Fragments**. Either select the **Enable** radio button to allow initial fragments (that is, the fragment bit is asserted) or leave the default Disable radio button selected to prevent initial fragments from being used.

  This option is not valid for rules that match L4 information such as TCP port number, because that information is carried in the initial packet.
- **Routing**. Either select the **Enable** radio button to match packets that include a routing extension header or leave the default Disable radio button selected to ignore the routing extension headers in packets.
- **IPv6 DSCP Service**. Specify the IP DiffServ Code Point (DSCP) field. This is an optional configuration.

  The DSCP is defined as the high-order 6 bits of the service type octet in the IPv6 header. Enter an integer from 0 to 63. To select the IPv6 DSCP, select one of the DSCP keywords. To specify a numeric value, select **Other** and enter the numeric value of the DSCP.

10. Click the **Apply** button.

Your settings are saved.

Modify the match criteria for an IPv6 ACL rule

To modify the match criteria for an IPv6 ACL rule:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Advanced > IPv6 Rules**.

   The IPv6 Rules page displays.
7. From the **ACL Name** menu, select the ACL that includes the rule that you want to modify.
8. In the IPv6 ACL Rule Table, click the rule.

   The rule is a hyperlink. The IPv6 ACL Rule Configuration page displays.
9. Modify the IPv6 ACL rule criteria.
10. Click the **Apply** button.

    Your settings are saved.

Delete an IPv6 ACL rule

To delete an IPv6 ACL rule:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Advanced > IPv6 Rules**.

   The IPv6 Rules page displays.
7. From the **ACL Name** menu, select the ACL that includes the rule that you want to delete.
8. In the IPv6 ACL Rule Table, select the check box that is associated with the rule.
9. Click the **Delete** button.

   The rule is removed.

Configure IP ACL interface bindings

When you bind a basic IPv4, extended IPv4, or IPv6 ACL to an interface, all the rules that you defined for the IP ACL are applied to the selected interface.

If resources on the switch are insufficient, an attempt to bind an ACL to an interface fails.

Bind an IP ACL to one or more interfaces

To bind an IP ACL to one or more interfaces:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Advanced > IP Binding Configuration**.

   The IP Binding Configuration page displays.
7. From the **ACL ID** menu, select an existing IP ACL for you which you want to add an IP ACL interface binding.

   The fixed selection from the **Direction** menu is **Inbound**, which means that MAC ACL rules are applied to traffic entering the interface.
8. In the **Sequence Number** field, optionally specify a number to indicate the order of the access list relative to other access lists already assigned to this interface and direction.

   A low number indicates high precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If you do not specify the sequence number (meaning that the value is 0), a sequence number that is one number greater than the highest sequence number currently in use for this interface and direction is used. The valid range is 1–4294967295.
9. To add the selected ACL to a port or LAG, in the Ports table or LAG table, click the port or LAG so that a check mark displays.

   You can add the ACL to several ports and LAGs.

   The Ports and LAG tables display the available and valid interfaces for ACL binding. All nonrouting physical interfaces, VLAN interfaces, and interfaces participating in LAGs are listed.
10. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only information displayed on the page.

Table 89. IP Binding Status table

Field	Description
Interface	The selected interface.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.

Table 89. IP Binding Status table (continued)

Field	Description
ACL ID/Name	The ACL number (for an IP ACL) or ACL name (for a named IP ACL or IPv6 ACL) identifying the ACL assigned to the selected interface and direction.
Sequence Number	The sequence number signifying the order of specified ACL relative to other ACLs assigned to the selected interface and direction.

View or delete an IP ACL binding

You can view or delete IP ACL bindings from the IP ACL Binding table.

To view 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL > Advanced > Binding Table**.

   The IP ACL Binding Table page displays.
7. To delete an IP ACL-to-interface binding, do the following:
   a. Select the check box next to the interface.
   b. Click the **Delete** button.

      The binding is removed.

The following table describes the information displayed in the IP ACL Binding Table.

Table 90. IP ACL Binding Table

Field	Description
Interface	The interface.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID/Name	The ACL number (for an IP ACL) or ACL name (for a named IP ACL or IPv6 ACL) identifying the ACL assigned to the selected interface and direction.
Sequence Number	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.

Configure VLAN ACL bindings

You can associate a MAC ACL, 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.

Add a VLAN ACL binding

To add a VLAN ACL binding:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > ACL > Advanced > VLAN Binding Table**.

   The VLAN Binding Configuration page displays.

7. In the **VLAN ID** field, enter the VLAN ID to which the binding must apply.

   Note: The direction for packet filtering is always inbound.

8. In the **Sequence Number** field, enter an optional sequence number.

   You can specify an optional sequence number to indicate the order of this access list relative to other access lists that are already assigned to the VLAN ID and selected direction. A lower number indicates a higher precedence order. If a sequence number is already in use for the VLAN ID and selected direction, the specified access list replaces the currently attached ACL using that sequence number. If you do not specify a sequence number (the value is 0), a sequence number that is one greater than the highest sequence number currently in use for the VLAN ID and selected direction is used. The valid range is 1 to 4294967295.

9. From the **ACL Type** menu, select the type of ACL.

   Valid ACL types include IP ACL, MAC ACL, and IPv6 ACL.

10. From the **ACL ID** list, select the ID or name of the ACL that must be bound to the specified VLAN.
11. Click the **Add** button.

    The VLAN ACL binding is added.

Remove a VLAN ACL binding

To remove a VLAN ACL binding:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.
6. Select **Security > ACL> Advanced > VLAN Binding Table**.

   The VLAN Binding Configuration page displays.
7. Select the check box for the VLAN binding that you want to remove.
8. Click the **Delete** button.

   The VLAN ACL binding is removed.

8

Monitor the Switch and the Traffic

This chapter contains the following sections:

- Monitor the switch and the ports
- Configure and view the logs
- Configure port mirroring

Monitor the switch and the ports

You can view and clear port and switch statistics and perform a cable test.

View or clear switch statistics

You can view detailed statistical information about the traffic that the switch processes.

To view or clear the switch statistics:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Monitoring > Ports > Switch Statistics**.

   The Statistics page displays.
7. To refresh the page, click the **Refresh** button.
8. Click the **Clear** button to clear all the statistics counters, resetting all switch summary and detailed statistics to default values.

   The discarded packets count cannot be cleared.

The following table describes the view-only switch statistics.

Table 91. Switch statistics

Field	Description
ifIndex	The interface index of the interface table entry associated with the processor of this switch.
Octets Received	The total number of octets of data received by the processor (excluding framing bits, but including FCS octets).
Packets Received Without Errors	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. This does not include multicast packets.
Receive Packets Discarded	The number of inbound packets that were chosen to be discarded, even though no errors were detected, in order to prevent their being delivered to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted Without Errors	The total number of packets transmitted out of the interface.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets that were chosen to be discarded, even though no errors were detected, in order to prevent their being delivered to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that were learned by this switch since the most recent reboot.
Address Entries in Use	The number of learned and static entries in the Forwarding Database Address Table for this switch.
Maximum VLAN Entries	The maximum number of VLANs allowed on this switch.
Most VLAN Entries Ever Used	The largest number of VLANs that were active on this switch since the last reboot.

Table 91. Switch statistics (continued)

Field	Description
Static VLAN Entries	The number of active VLAN entries on this switch that were created statically.
VLAN Deletes	The number of VLANs on this switch that were created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

View port statistics

You can view a summary of per-port traffic statistics on the switch.

To view port statistics:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Monitoring > Ports > Port Statistics**.

   The Status page displays.
7. Select whether to display physical interfaces, link aggregation groups (LAGs), or both by clicking one of the following links above the table heading:
   - **1** (or the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only link aggregation groups are displayed.
   - **All**. Both physical interfaces and link aggregation groups are displayed.

8. To locate an interface quickly, type the interface number using the respective naming convention (for example, g1 or l1) in the **Go To Interface** field above or below the table and click the **Go** button.

   The entry corresponding to the specified interface is selected.

The following table describes the view-only per-port statistics.

Table 92. Port statistics

Field	Description
Interface	This object indicates the interface of the interface table entry that is associated with this port on an adapter.
Total Packets Received Without Errors	The total number of packets received that were without errors.
Packets Received With Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. This does not include multicast packets.
Packets Transmitted Without Errors	The number of frames that were transmitted by this port to its segment.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Collision Frames	The best estimate of the total number of collisions on this Ethernet segment.
Link Down Events	The total number of link down events on a physical port.
Time Since Counters Last Cleared	The elapsed time in days, hours, minutes, and seconds since the statistics for this port were last cleared.

Reset the counters for one or more interfaces

To reset the counters 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Monitoring** > **Ports > Port Statistics**.

   The Port Statistics page displays.

7. Select whether to display physical interfaces, link aggregation groups (LAGs), or both by clicking one of the following links above the table heading:
   - **1** (or the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only link aggregation groups are displayed.
   - **All**. Both physical interfaces and link aggregation groups are displayed.
8. To locate an interface quickly, type the interface number using the respective naming convention (for example, g1 or l1) in the **Go To Interface** field above or below the table and click the **Go** button.

   The entry corresponding to the specified interface is selected.

9. Click the **Clear** button.

   The counters for the interface or interfaces are reset to 0.

Reset the counters for all interfaces on the switch

To reset the counters for all interfaces on the switch:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Monitoring** > **Ports > Port Statistics**.

   The Status page displays.

7. Select the check box in the heading of the table.
8. Click the **Clear** button.

   All counters are reset to 0.

View and manage detailed port statistics

You can view a variety of per-port traffic statistics.

To view or clear detailed port statistics:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Monitoring > Ports > Port Detailed Statistics**.

   The Port Detailed Statistics page displays.

7. From the **Interface** menu, select the interface for which you want to view the statistics.
8. From the **MST ID** menu, select the MST ID associated with the interface (if available).
9. To refresh the page, click the **Refresh** button.
10. To clear all the counters, click the **Clear** button. This resets all statistics for this port to the default values.

The following table describes the detailed port information displayed on the page. To view information about a different port, select the port number from the **Interface** menu.

Table 93. Detailed port statistics

Field	Description
ifIndex	This object indicates the ifIndex of the interface table entry associated with this port on an adapter.
Port Type	For normal ports this field displays Normal. Otherwise, the possible values are as follows: • **Mirrored**. This port is a participating in port mirroring as a mirrored port. Look at the Port Mirroring pages for more information. • **Probe**. This port is a participating in port mirroring as the probe port. Look at the Port Mirroring pages for more information. • **Trunk Member**. The port is a member of a link aggregation trunk. Look at the Port Channel pages for more information.
Port Channel ID	If the port is a member of a port channel, the port channel's interface ID and name are shown. Otherwise, Disable is shown.
Port Role	Each MST bridge port that is enabled is assigned a port role for each spanning tree. The port role is one of the following values: Root, Designated, Alternate, Backup, Master, or Disabled.
STP Mode	The Spanning Tree Protocol administrative mode that is associated with the port or port channel. The possible values are as follows: • **Enable**. Spanning tree is enabled for this port. • **Disable**. Spanning tree is disabled for this port.
STP State	The port's current Spanning Tree state. This state controls what action a port takes on receipt of a frame. If the bridge detects a malfunctioning port, it places that port into the broken state. The states are defined in IEEE 802.1D: • Disabled • Blocking • Listening • Learning • Forwarding • Broken
Admin Mode	The port control administration state. The port must be enabled for it to be allowed into the network. The default is Enabled.
Flow Control Mode	Indicates whether flow control is enabled or disabled for the port. This field is not valid for LAG interfaces.
LACP Mode	Indicates the Link Aggregation Control Protocol administrative state. The mode must be enabled for the port to participate in link aggregation.
Physical Mode	Indicates the port speed and duplex mode. In autonegotiation mode the duplex mode and speed are set from the autonegotiation process.
Physical Status	Indicates the port speed and duplex mode.
Link Status	Indicates whether the link is up or down.

Table 93. Detailed port statistics (continued)

Field	Description
Link Trap	Indicates whether or not the port sends a trap when link status changes.
Packets RX and TX 64 Octets	The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
Packets RX and TX 65-127 Octets	The total number of packets (including bad packets) received or transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 128-255 Octets	The total number of packets (including bad packets) received or transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 256-511 Octets	The total number of packets (including bad packets) received or transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 512-1023 Octets	The total number of packets (including bad packets) received or transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1024-1518 Octets	The total number of packets (including bad packets) received or transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1519-2047 Octets	The total number of packets (including bad packets) received or transmitted that were between 1519 and 204 7octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 2048-4095 Octets	The total number of packets (including bad packets) received or transmitted that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 4096-9216 Octets	The total number of packets (including bad packets) received or transmitted that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
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).

Table 93. Detailed port statistics (continued)

Field	Description
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 to prevent their being delivered to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Total Packets Received with MAC Errors	The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Jabbers Received	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and included either a bad frame check sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (alignment error). This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Fragments Received	The total number of packets received that were less than 64 octets in length with ERROR CRC (excluding framing bits but including FCS octets).
Undersize Received	The total number of packets received that were less than 64 octets in length with GOOD CRC (excluding framing bits but including FCS octets).
Alignment Errors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but included a bad frame check sequence (FCS) with a nonintegral number of octets.

Table 93. Detailed port statistics (continued)

Field	Description
Rx FCS Errors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but included a bad frame check sequence (FCS) with an integral number of octets.
Overruns	The total number of frames discarded because this port was overloaded with incoming packets, and could not keep up with the inflow.
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 on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
Unacceptable Frame Type	The number of frames discarded from this port due to being an unacceptable frame type.
Total Packets Transmitted (Octets)	The total number of octets of data (including those in bad packets) transmitted on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects must be sampled before and after a common interval.
Packets Transmitted 64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Packets Transmitted 65-127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 128-255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 256-511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 512-1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 1024-1518 Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted > 1518 Octets	The total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. This counter supports a maximum increment rate of 815 counts per sec at 10 Mb/s.
Maximum Frame Size	The maximum Ethernet frame size the interface supports or is configured to use, including Ethernet header, CRC, and payload. The possible range is 1522 to 10000. The default maximum frame size is 1522.

Table 93. Detailed port statistics (continued)

Field	Description
Total Packets Transmitted	The number of frames that were transmitted by this port to its segment.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors were detected to prevent them from being delivered to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Total Transmit Errors	The sum of single, multiple, and excessive collisions.
Tx FCS Errors	The total number of transmitted packets with a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, and with a bad Frame Check Sequence (FCS) with an integral number of octets.
Total Transmit Packets Discarded	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
Single Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Excessive Collision Frames	The number of frames for which transmission on a particular interface fails due to excessive collisions.
Dropped Transmit Frames	The number of transmit frames discarded at the selected port.
STP BPDUs Received	The number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	The number of STP BPDUs transmitted from the selected port.
RSTP BPDUs Received	The number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	The number of RSTP BPDUs transmitted from the selected port.
MSTP BPDUs Received	The number of MSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	The number of MSTP BPDUs transmitted from the selected port.
802.3x Pause Frames Transmitted	The number of MAC control frames transmitted on this interface 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.

Table 93. Detailed port statistics (continued)

Field	Description
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 this authenticator.
EAPOL Frames Transmitted	The number of EAPoL frames of any type that were transmitted by this authenticator.
Time Since Counters Last Cleared	The elapsed time in days, hours, minutes, and seconds since the statistics for this port were last cleared.

View or clear EAP and EAPoL statistics

You can view information about Extensible Authentication Protocol (EAP) and EAP over LAN (EAPoL) packets that are received on physical ports.

To view or clear EAP and EAPoL statistics:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Monitoring > Ports > EAP Statistics**.

   The EAP Statistics page displays.
7. To locate an interface quickly, type the interface number using the respective naming convention (for example, g1 or l1) in the **Go To Interface** field above or below the table and click the **Go** button.

8. To refresh the page, click the **Refresh** button.
9. To clear the counters for a specific port, select the check box associated with the port and click the **Clear** button.
10. To clear all the EAP counters for all ports on the switch, select the check box in the row heading and click the **Clear** button.

    Clicking the button resets all statistics for all ports to default values.

The following table describes the view-only EAP statistics displayed on the page.

Table 94. EAP statistics

Field	Description
Port	The port number.
EAPOL Frames Received	The number of valid EAPoL frames of any type that were received by this authenticator.
EAPOL Frames Transmitted	The number of EAPoL frames of any type that were transmitted by this authenticator.
EAPOL Start Frames Received	The number of EAPoL start frames that were received by this authenticator.
EAPOL Logoff Frames Received	The number of EAPoL logoff frames that were received by this authenticator.
EAPOL Last Frame Version	The protocol version number carried in the most recently received EAPoL frame.
EAPOL Last Frame Source	The source MAC address carried in the most recently received EAPoL frame.
EAPOL Invalid Frames Received	The number of EAPoL frames that were received by this authenticator in which the frame type is not recognized.
EAPOL Length Error Frames Received	The number of EAPoL frames that were received by this authenticator in which the frame type is not recognized.
EAP Response/ID Frames Received	The number of EAP response/identity frames that were received by this authenticator.
EAP Response Frames Received	The number of valid EAP response frames (other than resp/ID frames) that were received by this authenticator.
EAP Request/ID Frames Transmitted	The number of EAP request/identity frames that were transmitted by this authenticator.
EAP Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that were transmitted by this authenticator.

Perform a cable test

You can test and view information about the cables that are connected to switch ports.

To perform a cable test:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Monitoring > Ports > Cable Test**.

   The Cable Test page displays.

7. Select the check boxes that are associated with the physical ports for which you want to test the cables.
8. Click the **Apply** button.

   A cable test is performed on all selected ports. The cable test might take up to two seconds to complete. If the port forms an active link with a device, the cable status is always Normal. The test returns a cable length estimate if this feature is supported by the PHY for the current link speed. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter then the cable status might be Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded.

The following table describes the view-only information displayed on the page.

Table 95. Cable Test information

Field	Description
Cable Status	Indicates the cable status: • **Normal**. The cable is working correctly. • **Open**. The cable is disconnected or a faulty connector exists. • **Short**. An electrical short exists in the cable. • **Cable Test Failed**. The cable status could not be determined. The cable might in fact be working. • **Untested**. The cable is not yet tested. • **Invalid cable type**. The cable type is unsupported. • **No cable**. The cable is not present.
Cable Length	The estimated length of the cable in meters. The length is displayed as a range between the shortest estimated length and the longest estimated length. Unknown is displayed if the cable length could not be determined. The cable length is displayed only if the cable status is Normal.
Failure Location	The estimated distance in meters from the end of the cable to the failure location. The failure location is displayed only if the cable status is Open or Short.

Configure and view the logs

The switch generates messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences. These messages are stored locally and can be forwarded to one or more centralized points of collection for monitoring purposes or long-term archival storage. Local and remote configuration of the logging capability includes filtering of messages logged or forwarded based on severity and generating component.

Manage and view the memory logs

The memory log stores messages in memory based upon the settings for message component and severity. You can set the administrative status and behavior of logs in the system buffer. These log messages are cleared when the switch reboots.

For the message log, only the latest 200 entries are displayed on the page.

To manage and view the memory log:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Monitoring > Logs > Memory Log**.

   The Memory Log Configuration page displays.

7. Select one of the following Admin Status radio buttons:
   - **Enable**. Enable system logging.
   - **Disable**. Prevent the system from logging messages.

8. From the **Behavior** menu, specify the behavior of the log when it is full.
   - **Wrap**. When the buffer is full, the oldest log messages are deleted as the system logs new messages.
   - **Stop on Ful**l. When the buffer is full, the system stops logging new messages and preserves all existing log messages.

9. From the **Severity Filter** menu, select one of the following severity levels:
   - **Emergency**. System is unusable. This is level 0.
   - **Alert**. Action must be taken immediately. This is level 1.
   - **Critical**. Critical conditions. This is level 2.
   - **Error**. Error conditions. This is level 3.
   - **Warning**. Warning conditions. This is level 4.
   - **Notice**. Normal but significant conditions. This is level 5.
   - **Informational**. Informational messages. This is level 6, the default setting.
   - **Debug**. Debug-level messages. This is level 7.

   Note: A log records messages equal to or above a configured severity threshold.

10. Click the **Apply** button.

    Your settings are saved.

    The Memory Log table displays on the Memory Log page.

The Total number of Messages field displays the number of messages the system logged in memory. Only the 200 most recent entries are displayed on the page.

The rest of the page displays the Memory Log messages. The format of the log message is the same for messages that are displayed for the message log, persistent log, or console log. Messages logged to a collector or relay through syslog support the same format as well.

The following example shows the standard format for a log message:

```
*Dec 01 2024 00:00:18: AAA-5-CONNECT: New http connection for user
admin, source 192.168.1.111 ACCEPTED
```

The message was generated by component AAA on December 1, 2024 at 00:00:18 a.m. with severity 5 (Notice). The message indicates that the administrator logged on to the HTTP management interface from a host with IP address 192.168.1.111.

11. To refresh the page, click the **Refresh** button.
12. To clear the messages from the buffered log in the memory, click the **Clear** button.

Manage and view 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 view the flash log:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

The System Information page displays.

6. Select **Monitoring > Logs > FLASH Log**.

   The FLASH Log Configuration page displays.

7. Select one of the following Admin Status radio buttons:
   - **Enable**. A log that is enabled logs messages.
   - **Disable**. A log that is disabled does not log messages.

8. From the **Severity Filter** menu, select the logging level for messages that must be sent to the logging host.

   Log messages with the selected severity level and all log messages of greater severity are sent to the host. For example, if you select **Error**, the logged messages include Error, Critical, Alert, and Emergency. The severity can be one of the following levels:

   - **Emergency**. The highest warning level. If the device is down, or not functioning properly, an emergency log message is saved to the device. This is level 0.
   - **Alert**. The second-highest warning level. An alert log message is saved if a serious device malfunction occurs, such as all device features being down. Action must be taken immediately. This is level 1, the default setting.
   - **Critical**. The third-highest warning level. A critical log message is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional. This is level 2.
   - **Error**. A device error occurred, such as a port being offline. This is level 3, the default setting.
   - **Warning**. The lowest level of a device warning. This is level 4.
   - **Notice**. Normal but significant conditions. Provides the network administrators with device information. This is level 5.
   - **Informational**. Provides device information. This is level 6.
   - **Debug**. Provides detailed information about the device. This is level 7.

9. 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.

10. Click the **Apply** button.

    Your settings are saved.

    The Total Number of Messages field shows is the total number of persistent log messages that are stored on the switch. The maximum number of persistent log messages displayed on the switch is 64.

    The following example shows the standard format for a persistent log message:

```
*Dec 01 2024 00:00:18: AAA-5-CONNECT: New http connection for user
admin, source 192.168.1.111 ACCEPTED
```

The message was generated by component AAA on December 1, 2024 at 00:00:18 a.m. with severity 5 (Notice). The message indicates that the administrator logged on to the HTTP management interface from a host with IP address 192.168.1.111.

Manage the server log

You can let the switch send log messages to remote logging hosts. A remote log server is the same as a remote syslog host.

You must enable the server log on the switch and specify one or more remote syslog hosts.

Enable the server log and add a remote syslog host

To enable the server log and add a remote syslog host:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Monitoring > Logs > Server Log**.

   The Server Log Configuration page displays.
7. Select one of the following Admin Status radio buttons:
   - **Enable**. Send log messages to all configured hosts (syslog collectors or relays) using the values configured for each host.
   - **Disable**. Stop logging to all syslog hosts. **Disable** means no messages are sent to any collector or relay.
8. In the **Local UDP Port** field, specify the port number that the switch uses to send log messages to the syslog servers.

The range is from 1 to 65535. The default port is 514.

9. Click the **Apply** button.

   Your settings are saved.

10. In the Server Configuration section, specify the following settings:
    - **IP Address Type**. Specify the IP address type of the host, which can be **IPv4**, **IPv6**, or **DNS**.
    - **Host Address**. Specify the IP address or host name of the syslog host.
    - **Port**. Specify the port on the host to which syslog messages must be sent. The default port number is 514.
    - **Severity Filter**. Use the menu to select the severity of the logs that must be sent to the logging host. Logs with the selected severity level and all logs of greater severity are sent to the host. For example, if you select **Error**, the logged messages include Error, Critical, Alert, and Emergency.

      The severity can be one of the following levels:

      - **Emergency**. The highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device. This is level 0.
      - **Alert**. The second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down. This is level 1.
      - **Critical**. The third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional. This is level 2.
      - **Error**. A device error occurred, such as a port being offline. This is level 3.
      - **Warning**. The lowest level of a device warning. This is level 4.
      - **Notice**. Normal but significant conditions. Provides the network administrators with device information. This is level 5.
      - **Informational** (6). Provides device information. This is level 6.
      - **Debug** (7). Provides detailed information about the log. This is level 7.

11. Click the **Add** button.

    The remote syslog host is added.

    The Status field in the Server Configuration table shows whether the remote logging host is currently active.

The following table describes the view-only fields in the Server Log Configuration section.

Table 96. Server Log Configuration information

Field	Description
Messages Received	The number of messages received by the log process. This includes messages that are dropped or ignored.
Messages Relayed	The number of syslog messages relayed.

Table 96. Server Log Configuration information (continued)

Field	Description
Messages Ignored	The number of syslog messages ignored.

Modify the settings for a remote syslog host

To modify the settings for a remote syslog host:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Monitoring > Logs > Server Log**.

   The Server Log Configuration page displays.
7. In the Server Configuration section, select the check box that is associated with the host.
8. Change the information as needed.
9. Click the **Apply** button.

   Your settings are saved.

Delete the settings for a remote syslog host

To delete the settings for a remote syslog host:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Monitoring > Logs > Server Log**.

   The Server Log Configuration page displays.
7. In the Server Configuration section, select the check box that is associated with the host.
8. Click the **Delete** button.

   The host is removed.

View or clear the trap logs and the counters

You can view information about the SNMP traps generated on the switch.

You can also display information about the traps that were sent.

To view or clear the trap logs and the counters:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.

- If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Monitoring > Logs > Trap Logs**.

   The Trap Logs page displays.

7. To refresh the page, click the **Refresh** button.
8. To clear all counters, click the **Clear** button.

   All statistics for the trap logs are reset to their default values.

The following table describes the view-only trap logs information that is displayed on the page.

Table 97. Trap Logs information

Field	Description
Number of Traps Since Last Reset	The number of traps that occurred since the switch last rebooted.
Trap Log Capacity	The maximum number of traps stored in the log. If the number of traps exceeds the capacity, the entries overwrite the oldest entries.
Number of Traps since log last viewed	The number of traps that occurred since the traps were last displayed. Displaying the traps by any method (terminal interface display, web display, upload file from switch, and so on) causes this counter to be cleared to 0.
Log	The sequence number of this trap.
System Up Time	The time when this trap occurred, expressed in days, hours, minutes, and seconds, since the last reboot of the switch.
Trap	Information identifying the trap.

View or clear the event logs

You can display and clear the event logs, which contains error messages from the switch.

Note: If you reset the switch to factory default settings, the event log is not cleared.

To display or clear the event logs:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Monitoring > Logs > Event Logs**.

   The Event Logs page displays.
7. To refresh the page, click the **Refresh** button.
8. To clear all information, click the **Clear** button.

The following table describes the view-only event logs information displayed on the page.

Table 98. Event logs information

Field	Description
Entry	The sequence number of the event.
Type	The type of the event.
File Name	The file in which the event originated.

Table 98. Event logs information (continued)

Field	Description
Line	The line number of the event.
Task Id	The task ID of the event.
Code	The event code.
Time	The time the event occurred.

Configure port mirroring

Port mirroring lets you select the network traffic of specific switch ports for analysis by a network analyzer. You can select many switch ports as source ports but a single switch port only as the destination port. You can configure how traffic is mirrored on a source port by selecting packets that are received, transmitted, or both.

A packet that is copied to the destination port is in the same format as the original packet on the wire. This means that if the mirror is copying a received packet, the copied packet is VLAN-tagged or untagged as it was received on the source port. If the mirror is copying a transmitted packet, the copied packet is VLAN-tagged or untagged as it is being transmitted on the source port.

To globally enable port mirroring, specify the destination port, and specify one or more source ports:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.

6. Select **Monitoring > Mirroring > Port Mirroring**.

   The Global Configuration page displays.

7. Select an Admin Mode radio button:
   - **True**. Port mirroring is enabled.
   - **False**. Port mirroring is disabled.

8. From the **Destination Port** menu, select the destination port to which port traffic must be copied.

   You can configure only one destination port on the switch. The port functions as a probe port and receives traffic from all configured source ports. If no port is configured, None is displayed. The default is None.

9. Click the **Apply** button.

   Your settings are saved.

   The following steps must be performed in the Source Interface Configuration section.

10. Use one of the following methods to narrow down the ports that are displayed:
    - Select **Unit ID** to display the physical ports of the selected unit.
    - Select **LAG** to display a list of LAGs only.
    - Select **CPU** to display a list of CPUs only.
    - Select **All** to display a list of all physical ports, LAGs, CPUs, and VLANs.

11. Use one of the following methods to select one or more source ports:
    - To select a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
    - To select multiple interfaces with the same settings, select the check box associated with each interface.

    Traffic from the selected ports is sent to the probe port.

12. From the **Direction** menu, specify the direction of the traffic that must be mirrored from the selected source ports:
    - **None**. The value is not configured. This is the default setting.
    - **Tx and Rx**. Monitors transmitted and received packets.
    - **Rx**. Monitors received (ingress) packets only.
    - **Tx**. Monitors transmitted (egress) packets only.

13. Click the **Apply** button.

    Your settings are saved.

    The Status field indicates the interface status.

9

Maintain or Troubleshoot the switch

This chapter contains the following sections:

- Reboot the switch
- Reset the switch to its factory default settings
- Export a file from the switch
- Download a file to the switch or update the software
- Manage software images
- Perform diagnostics and troubleshooting

Reboot the switch

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 single-function **Reset** button on the front panel for more than one second.

To reboot the switch:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Maintenance > Reset > Device Reboot**.

   The Device Reboot page displays.
7. Select the check box.
8. Click the **Apply** button.

   An Alert pop-up window displays.
9. Click the **OK** button.

   The switch reboots.

Reset the switch to its factory default settings

You can reset the system configuration to the factory default values. All changes that you made are lost. If the IP address changes, your web session might disconnect.

If you reset the switch to the default configuration, the IP address is reset to 192.168.0.239, and the DHCP client is enabled. If you lose network connectivity after you reset the switch to the factory defaults, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

Note: If you can physically access the switch, you can reset the switch to factory default settings by pressing the **Factory Defaults** button on the front panel. You must press the button for more than 10 seconds.

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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Maintenance > Reset > Factory Default**.

   The Default Settings page displays.
7. Select the check box.
8. Click the **Apply** button.

An Alert pop-up window displays.

9. Click the **OK** button.

   All configuration settings are reset to their factory default values. All changes that you made are lost, even if you saved the configuration.

Export a file from the switch

You can export configuration (ASCII or log ASCII) files from the switch to a file server by using TFTP, HTTP, or USB.

The following sections describe how you can export a file from the switch:

- Use TFTP to export a file from the switch to a TFTP server on page 442
- Use HTTP to export a file from the switch to a computer on page 444

Use TFTP to export a file from the switch to a TFTP server

You can upload (export) configuration (ASCII or log ASCII) files from the switch to a TFTP server on the network.

To export a file from the switch to a TFTP server:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Maintenance > Export > TFTP File Export**.

The TFTP File Export page displays.

7. From the **File Type** menu, select the type of file:
   - **Text Configuration**. A text-based configuration file enables you to edit a configured text file (`startup-config`) offline as needed. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name or IP address), and download it to that device.
   - **Error Log**. The log with the system errors.
   - **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-base file that contains a variety of hardware, software, and configuration information that can assist in device and network troubleshooting.
   - **Crash Logs**. The switch crash logs, if any.
8. From the **Transfer Mode** menu, specify the protocol that must be used to transfer the file to the server:
   - **SFTP**: Secure File Transfer Protocol. This selection requires you to specify a user name and password.
   - **TFTP**: Trivial File Transfer Protocol.
   - **SCP**: Secure Copy Protocol. This selection requires you to specify a user name and password.
   - **FTP**. File Transfer Protocol. This selection requires you to specify a user name and password.
9. From the **Server Address Type** menu, select the format for the **Server Address** field:
   - **IPv4**. Indicates that the server address is an IP address in dotted-decimal format. This is the default setting.
   - **DNS**. Indicates that the server address is a host name.
10. In the **Server Address** field, enter the IP address of the server in accordance with the format indicated by the server address type.

    The default is the IPv4 address 0.0.0.0.
11. In the **Transfer File Path** field, specify the path on the TFTP server where you want to save the file.

    You can enter up to 32 characters. Include the backslash at the end of the path. A path name with a space is not accepted. Leave this field blank to save the file to the root TFTP directory.
12. In the **Transfer File Name** field, specify a destination file name for the file to be uploaded.

    You can enter up to 32 characters. The transfer fails if you do not specify a file name.
13. If you select **SFTP**, **SCP**, or **FTP** from **Transfer Mode** menu, specify the following settings:
    - **User Name**: Specify the user name for remote login to the server.
    - **Password**: Specify the password for remote login to the server.

14. Select the **Start File Transfer** check box.
15. Click the **Apply** button.

    The file transfer begins.

    The page displays information about the file transfer progress. The page refreshes automatically when the file transfer completes.

Use HTTP to export a file from the switch to a computer

You can upload (export) files of various types from the switch to a computer through an HTTP session by using your web browser.

To export a file from the switch to a computer by using HTTP:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Maintenance > Export > HTTP File Export**.

   The HTTP File Export page displays.
7. From the **File Type** menu, select the type of file:
   - **Text Configuration**. A text-based configuration file enables you to edit a configured text file (`startup-config`) offline as needed. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name or IP address), and download it to that device.

- **Tech Support**. The tech support file is a text-base file that contains a variety of hardware, software, and configuration information that can assist in device and network troubleshooting.
- **Crash Logs**. The switch crash logs, if any.

8. Click the **Apply** button.

   The file transfer begins.

   The page displays information about the file transfer progress. The page refreshes automatically when the file transfer completes.

Download a file to the switch or update the software

You can download system files from a remote system to the switch by using either TFTP or HTTP. In this context, downloading is also referred to as updating.

The following sections describe how you can download a file to the switch:

- Use TFTP to download a file to the switch or update the software image on page 445
- Use HTTP to download a file to the switch or update the software image on page 448
- Use an HTTP session to download and install an SSL security certificate file on the switch on page 450

Note: Use one of these procedures to update the software (firmware) on the switch.

Use TFTP to download a file to the switch or update the software image

You can download a software (firmware) image, configuration files, and SSL files from a TFTP server to the switch.

Before you download a file to the switch, the following conditions must be true:

- The file to download from the TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch contains a path to the TFTP server.

You can also download files by using HTTP (see Use HTTP to download a file to the switch or update the software image on page 448).

To download a file to the switch from a TFTP server or update the software image from a TFTP server:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Maintenance > Update > TFTP Firmware/File Update**.

   The TFTP Firmware/File Update page displays.

7. From the **File Type** menu, select the type of file:
   - **Software**. The system software image, which is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy, while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the nonactive image. This is a safety feature for faults occurring during the boot upgrade process.
   - **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.
   - **SSH-2 RSA Key PEM File**. SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded).
   - **SSH-2 DSA Key PEM File**. SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded).
   - **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).

8. If the selection from the **File Type** menu is **Software**, the **Image Name** menu is displayed and you must select the software image that must be downloaded to the switch:
   - **Image1**. Select Image1 to upload image 1.
   - **Image2**. Select Image2 to upload image 2.

   Note: We recommended that you do not overwrite the active image.
9. From the **Transfer Mode** menu, specify the protocol that must be used to transfer the file to the server:
   - **SFTP**: Secure File Transfer Protocol. This selection requires you to specify a user name and password.
   - **TFTP**: Trivial File Transfer Protocol.
   - **SCP**: Secure Copy Protocol. This selection requires you to specify a user name and password.
   - **FTP**. File Transfer Protocol. This selection requires you to specify a user name and password.
10. From the **Server Address Type** menu, select the format for the selected transfer mode:
    - **IPv4**. Indicates that the server address is an IP address in dotted-decimal format. This is the default setting.
    - **DNS**. Indicates that the server address is a host name.
11. In the **TFTP Server IP** field, enter the IP address of the server indicated by the server address type.

    The default is the IPv4 address 0.0.0.0.
12. In the **Transfer File Path** field, specify the path on the server where the file is located.

    Enter up to 160 characters. Include the backslash at the end of the path. A path name with a space is not accepted. Leave this field blank to save the file to the root directory.
13. In the **Remote File Name** field, specify the name of the file to download from the server.

    You can enter up to 32 characters. A file name with a space is not accepted.
14. If you select **SFTP**, **SCP**, or **FTP** from **Transfer Mode** menu, specify the following settings:
    - **User Name**: Specify the user name for remote login to the server.
    - **Password**: Specify the password for remote login to the server.
15. Select the **Start File Transfer** check box to initiate the file upload.
16. Click the **Apply** button.

    The file transfer begins.

    The page displays information about the progress of the file transfer. The page refreshes automatically when the file transfer completes.

Note: After you download a text configuration file, the switch applies the configuration automatically.

17. After you download a software image file, if you want the switch to run the software image, do the following:
    a. Select the new software image file (see Change the software image that loads when the switch starts or reboots on page 453).
    b. Reboot the switch (see Reboot the switch on page 440).

Use HTTP to download a file to the switch or update the software image

You can download a software (firmware) image, configuration files, and SSL files from a computer to the switch by using an HTTP session over a web browser.

To download a file to the switch using HTTP or update the software image using HTTP:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Maintenance > Update > HTTP Firmware/File Update**.

   The HTTP Firmware/File Update page displays.
7. From the **File Type** menu, select the type of file:
   - **Software**. The system software image, which is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy, while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the

nonactive image. This is a safety feature for faults occurring during the boot upgrade process.

- **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.
- **SSH-2 RSA Key PEM File**. SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded).
- **SSH-2 DSA Key PEM File**. SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded).
- **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).

8. If the selection from the **File Type** menu is **Software**, the **Image Name** menu is displayed and you must select the software image that must be downloaded to the switch:
   - **Image1**. Select Image1 to upload image 1.
   - **Image2**. Select Image2 to upload image 2.

   Note: We recommended that you do not overwrite the active image.
9. Select the Select File **Browse** button and locate the file that you want to download.

   The file name can contain up to 80 characters.
10. Click the **Apply** button.

    The file transfer begins.

    The page displays information about the progress of the file transfer. After a file transfer is started, wait until the page refreshes. When the page refreshes, the option to select a file option is no longer available, indicating that the file transfer is complete.

    Note: After you download a text configuration file, the switch applies the configuration automatically.

11. After you download a software image file, if you want the switch to run the software image, do the following:
    a. Select the new software image file (see Change the software image that loads when the switch starts or reboots on page 453).
    b. Reboot the switch (see Reboot the switch on page 440).

Use an HTTP session to download and install an SSL security certificate file on the switch

Note: 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.

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:

- **SSL Trusted Root Certificate PEM File**. The SSL trusted root certificate PEM-encoded file, which must be in the format `xxxxCERTxxxxx.pem`.
- **SSL Server Certificate PEM File**. The SSL server certificate PEM-encoded file (the key file), which must be in the format `xxxxKEYxxxxx.pem`.

Before you can download and install an SSL security certificate, you must 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.

6. Select **Security > Access > HTTPS**.

   HTTPS Configuration page displays.

7. Select the Admin Mode **Disable** radio button.
8. 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.

9. Wait one minute, refresh your browser, and log back in to the switch (see steps 3 through 5).
10. Select **Maintenance > Update > HTTP Firmware/File Update**.

    The HTTP Firmware/File Update page displays.

11. From the **File Type** menu, **SSL Trusted Root Certificate PEM File**.
12. Select the Select File **Browse** button and locate the file that you want to download.

    This the certificate file, which must be in the format `xxxxCERTxxxxx.pem`.

13. Click the **Apply** button.

    The file transfer begins.

    The page displays information about the progress of the file transfer. The page refreshes automatically when the file transfer completes (or if it fails).

14. From the **File Type** menu, select **SSL Server Certificate PEM File**.

    This is the key file, which must be in the format `xxxxKEYxxxxx.pem`.

15. Select the Select File **Browse** button and locate the file that you want to download.

    The file name can contain up to 80 characters.

16. Click the **Apply** button.

    The file transfer begins.

The page displays information about the progress of the file transfer. The page refreshes automatically when the file transfer completes.

Manage software images

The switch maintains two versions of the switch software in permanent storage. One image is the active image, and the second image is the backup image. The active image is loaded when the switch starts or reboots. This feature reduces switch down time when you are updating the switch software.

Note: A switch that runs an older (legacy) software version might not load a configuration file that is created by a newer software version. In such a situation, the switch displays a warning.

The following sections describe how you can manage the software images:

- Copy a software image on page 452
- Configure dual image settings on page 453
- View the dual image status on page 455

Copy a software image

You can copy an image from one location (primary or backup) to another.

To copy a software image:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Maintenance > File Management > Copy**.

   The Copy page displays.
7. Select the Source Image **image1** or **image2** radio button to specify the image to be copied.
8. Select the Destination Image **image1** or **image2** radio button to specify the destination image.

9. Click the **Apply** button.

   Your settings are saved.

Configure dual image settings

The Dual Image feature allows the switch to retain two images in permanent storage. You can select which image must be loaded when the reboots, specify an image description, or delete an image. This feature reduces switch down time when you are upgrading or downgrading the software image.

Change the software image that loads when the switch starts or reboots

To change the image that loads during the boot process:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Maintenance > File Management > Dual Image Configuration**.

   The Dual Image Configuration page displays.
7. From the **Image Name** menu, select the image that is *not* the image displayed in the Current-active field.

   The Current-active field displays the name of the active image.
8. To specify a name for the selected image, enter one in the **Image Description** field.
9. Select the **Activate Image** check box.
10. Click the **Apply** button.

    Your settings are saved.

11. After activating the image, reboot the switch (see Reboot the switch on page 440).

    If you do not reboot the switch, it continues running the image shown in the Current-active field until the next time that the switch reboots.

Delete a software Image

To delete a software image:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Maintenance > File Management > Dual Image Configuration**.

   The Dual Image Configuration page displays.
7. From the **Image Name** menu, select the image that is *not* the image displayed in the Current-active field.

   The Current-active field displays the name of the active image. You cannot delete the active image.
8. Select the **Delete** Image check box.
9. Click the **Apply** button.

   The image is removed.

View the dual image status

You can view information about the active and backup images on the system.

To view dual image status information:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Maintenance > File Management > Dual Image > Dual Image Status**.

   The Dual Image Status page displays.

The following table describes the information available on the page.

Table 99. Dual Image Status information

Field	Description
Image1 Ver	The version of the image1 firmware file.
Image2 Ver	The version of the image2 firmware file.
Current-active	The currently active firmware image on this switch.
Next-active	The firmware image to be used on the next restart of this switch.
Image1 Description	The optional description associated with the image1 firmware file.
Image2 Description	The optional description associated with the image2 firmware file.

Perform diagnostics and troubleshooting

You can send a ping or a traceroute, and you can enable and configure remote diagnostics.

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 a.b.c.d (a.b.c.d): size data bytes
size bytes from a.b.c.d: seq=0 ttl=xyz
--- a.b.c.d 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 a.b.c.d (a.b.c.d): size data bytes
--- a.b.c.d 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.

6. Select **Maintenance > Troubleshooting > Ping IPv4**.

   The Ping Details page displays.

7. In the **IP Address/Host Name** field, enter the IP address or host name of the device that must be pinged.
8. In the **Count** field, enter the number of echo requests that must be sent.

   The default value is 3. The range is 1 to 15.

9. In the **Interval (secs)** field, enter the time between ping packets in seconds.

   The default value is 3 seconds. The range is 1 to 60.

10. In the **Size** field, enter the size of the ping packet. The default value is 0 bytes. The range is 0 to 13000.
11. From the **Source** menu, 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 IPv4 address that must be used when echo request packets are sent. With this selection, the **IP Address** field displays and you must enter the IP 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 the network interface or a VLAN as the source.
12. 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 a:b::c:d (a:b::c:d): size data bytes
size bytes from a:b::c:d: seq=0 ttl=xyz
--- a:b::c:d 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 a:b::c:d (a:b::c:d): size data bytes
--- a:b::c:d 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Maintenance > Troubleshooting > Ping IPv6**.

   The Ping IPv6 page displays.
7. From the **Ping** menu, select the type of ping:
   - **Global**. Pings a global IPv6 address.
   - **Link Local**. Pings a link-local IPv6 address over a specified interface. With this selection, the **Interface** menu displays, and you must select the interface.
8. In the **IPv6 Address/Hostname** field, enter the IPv6 address or host name of the station that must be pinged.

   The format is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. The maximum number of characters is 255.
9. In the **Count** field, enter the number of echo requests that must be sent.

   The range is 1 to 15. The default value is 3.
10. In the **Interval (secs)** field, enter the time between ping packets in seconds.

    The range is 1 to 60. The default value is 3.
11. In the **Datagram Size** field, enter the datagram size.

    The valid range is 0 to 13000. The default value is 0 bytes.

12. From the **Source** menu, 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.
    - **IPv6 Address**. The source IPv6 address that must be used when echo request packets are sent. With this selection, the **IPv6 Address** field displays and you must enter 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 the network interface or a VLAN as the source.
13. 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 a.b.c.d (a.b.c.d), maxTTL hops max, size byte packets
initTTL a.b.c.d (a.b.c.d) 0.000 ms * 0.000 ms
initTTL+1 a.b.c.d (a.b.c.d) 0.000 ms * 0.000 ms
initTTL+2 a.b.c.d (a.b.c.d) 0.000 ms * 0.000 ms
```

To send an IPv4 traceroute:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 23.

5. Click the **Login** button.

   The System Information page displays.

6. Select **Maintenance > Troubleshooting > Traceroute IPv4**.

   The Traceroute page displays.

7. In the **IP Address/Hostname** field, enter the IP address or host name of the device for which the path must be discovered.
8. In the **Probes Per Hop** field, enter the number of probes per hop.

   The default value is 3. The range is 1 to 10.

9. In the **Max TTL** field, enter the maximum time-to-live (TTL) period for the destination.

   The default value is 30. The range is 1 to 255.

10. In the **Init TTL** field, enter the initial TTL period to be used.

    The default value is 1. The range is 1 to 255.

11. In the **MaxFail** field, enter the maximum number of failures allowed in the session.

    The default value is 5. The range is 1 to 255.

12. In the **Interval (secs)** field, enter the time between probes in seconds.

    The default value is 3. The range is 1 to 60.

13. In the **Port** field, enter the UDP destination port for the probe packets.

    The default value is 33434. The range is 1–65535.

14. In the **Size** field, enter the size of the probe packets.

    The default value is 0. The range is 0 to 39936.

15. From the **Source** menu, select the IP address or interface that must be used to send echo request packets:
    - **None**. The source address for the traceroute is the address of the default egress interface.
    - **IP Address**. The source IP address that must be used for the traceroute. With this selection, the **IP Address** field displays and you must enter the IP address that must be used as the source.
    - **Interface**. The interface that must be used for the traceroute. With this selection, the **Interface** menu displays and you must select the network interface or a VLAN as the source.
16. 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 a:b::c:d (a:b::c:d), maxTTL hops max, size byte packets
initTTL a:b::c:d (a:b::c:d) 0.000 ms * 0.000 ms
initTTL+1 a:b::c:d (a:b::c:d) 0.000 ms * 0.000 ms
initTTL+2 a:b::c:d (a:b::c:d) 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.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

   The device UI login page displays.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Maintenance > Troubleshooting > Traceroute IPv6**.

   The Traceroute IPv6 Page displays.
7. In the **IPv6 Address/Host Name** field, enter the IPv6 address or host name of the device for which the path must be discovered.
8. In the **Probes Per Hop** field, enter the number of probes per hop.

   The default value is 3. The range is 1 to 10.
9. In the **Max TTL** field, enter the maximum time-to-live (TTL) period for the destination.

   The default value is 30. The range is 1 to 255.
10. In the **Init TTL** field, enter the initial TTL period to be used.

The default value is 1. The range is 1 to 255.

11. In the **MaxFail** field, enter the maximum number of failures allowed in the session.

    The default value is 5. The range is 1 to 255.

12. In the **Interval (secs)** field, enter the time between probes in seconds.

    The default value is 3. The range is 1 to 60.

13. In the **Port** field, enter the UDP destination port for the probe packets.

    The default value is 33434. The range is 1–65535.

14. In the **Size** field, enter the size of the probe packets.

    The default value is 0. The range is 0 to 39936.

15. From the **Source** menu, select the IP address or interface that must be used to send echo request packets:
    - **None**. The source address for the traceroute is the address of the default egress interface.
    - **IP Address**. The source IP address that must be used for the traceroute. With this selection, the **IPv6 Address** field displays and you must enter the IPv6 address that must be used as the source.
    - **Interface**. The interface that must be used for the traceroute. With this selection, the **Interface** menu displays and you must select the network interface or a VLAN as the source.

16. Click the **Apply** button.

    A traceroute request is sent to the specified IP address or host name. The results are displayed below the configurable data in the Results field.

Enable remote diagnostics

For enhanced security the remote diagnostic option is disabled by default. You can enable option to access the switch remotely. When remote access is enabled, you or technical support can perform remote diagnostics services.

To enable remote diagnostics:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 17 or Access the switch off-network and not connected to the Internet on page 22.

The device UI login page displays.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 23.
5. Click the **Login** button.

   The System Information page displays.
6. Select **Maintenance > Troubleshooting > Remote Diagnostics**.

   The Remote Diagnostics page displays.
7. Select the **Enable** radio button.
8. Click the **Apply** button.

   Your settings are saved.

Configure remote SSH diagnostics

You can view and modify the Secure Shell (SSH) server settings on the device. SSH is a network protocol that enables access to the CLI management interface by using an SSH client on a remote administrative system. SSH encrypts communication between an administrative system and the switch. You can download or generate SSH host keys for secure CLI-based management.

Configure SSH settings for remote SSH diagnostics

You can configure the SSH setting specifically for remote SSH diagnostics.

To configure SSH settings:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login window opens.
3. Enter the user name and password.

   The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
4. Click the **Login** button.

   The System Information page displays.
5. Select **Security > Access > SSH > SSH Configuration**.

   The SSH Configuration page displays.
6. Select the SSH Admin Mode **Disable** or **Enable** radio button.

This sets the SSH server administrative mode. When this mode is enabled, the switch can be accessed by using an SSH client on a remote system. The default is Disable.

7. In the **SSH Session Timeout** field, specify the SSH session inactivity time-out value for incoming SSH sessions to the switch.

   A connected user who does not actively uses SSH for the specified period is automatically disconnected from the switch. The range for is from 1 to 5 minutes. The default is 5 minutes.

8. In the **Maximum Number of SSH Sessions** field, specify the maximum number of inbound SSH sessions that can be connected to the switch simultaneously.

   The range is from is 0 to 5. The default is 2.

9. From the **Authentication List** menu, select an authentication list.

   This list is used to authenticate users who try to log in to the switch CLI.

10. From the **Enable Authentication List** menu, select an authentication list.

    This list is used to authenticate users who try to get *enable* level privilege in the CLI.

11. In the **SSH Port** field, specify the port that must be used for SSH connectivity.

    The port range is from 1 to 65535. The default is port 22.

12. Click the **Apply** button.

    Your settings are saved.

The following table describes the view-only fields that display on the page.

Table 100. SSH Configuration

Field	Description
SSH Version	The SSH server on the device can accept connections from an SSH client using protocol level 2 for SSH (SSH-2).
Current Number of SSH Sessions	The number of active SSH sessions between remote SSH clients and the SSH server on the switch.
Keys Present	Displays Yes or No to indicate if any of the following keys are present on the switch: • SSH-2 Rivest-Shamir-Adelman (RSA) key file (PEM encoded) • SSH-2 Digital Signature Algorithm (DSA) key file (PEM encoded)

Manage host keys for remote SSH diagnostics

You can generate or delete RSA and DSA keys.

Note: To generate SSH key files, SSH must be administratively disabled and no active SSH sessions can be present.

To generate or delete RSA or DSA host keys:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login window opens.
3. Enter the user name and password.

   The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
4. Click the **Login** button.

   The System Information page displays.
5. Select **Security > Access > SSH > Host Keys Management**.

   The Host Keys Management page displays.
6. To generate RSA or DSA keys, do the following:
   a. Select the **Generate RSA Keys** or **Generate DSA Keys** radio button.

      By default, the None radio button is selected.
   b. Click the **Apply** button.

      The host key file is generated.
7. To delete RSA or DSA keys, do the following:
   a. Select the **Delete RSA Keys** or **Delete DSA Keys** radio button.
   b. Click the **Apply** button.

      The host key file is deleted.

The following table describes the view-only fields that display on the page.

Table 101. RSA Key Management

Field	Description
Keys Present	Displays which of the following keys or both (if any) are present on the device: • SSH-2 Rivest-Shamir-Adelman (RSA) key file (PEM Encoded) • SSH-2 Digital Signature Algorithm (DSA) key file (PEM Encoded)
Key Generation In Progress	Displays which key is being generated (if any), RSA, DSA, or None.

Download host keys for remote SSH diagnostics

You can download an SSH-2 RSA or SSH-2 DSA key file from a remote system to the device.

Note: To download SSH key files, SSH must be administratively disabled and no active SSH sessions can be present.

To download host keys:

1. Launch a web browser.
2. In the address field of your web browser, enter the IP address of the switch.

   The login window opens.
3. Enter the user name and password.

   The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
4. Click the **Login** button.

   The System Information page displays.
5. Select **Security > Access > SSH > Host Keys Download**.

   The Host Keys Download page displays.
6. From the **File Type** menu, select the type of file to transfer:
   - **SSH-2 RSA Key PEM File**. SSH-2 Rivest-Shamir-Adelman (RSA) key file (PEM Encoded)
   - **SSH-2 DSA Key PEM File**. SSH-2 Digital Signature Algorithm (DSA) key file (PEM Encoded)
7. From the **Transfer Mode** menu, select the protocol that must be used to transfer the file:
   - **TFTP**: Trivial File Transfer Protocol.
   - **SFTP**: Secure File Transfer Protocol. This selection requires you to specify a user name and password.
   - **SCP**: Secure Copy Protocol. This selection requires you to specify a user name and password.
8. In the **Server Address Type** field, specify either **IPv4**, **IPv6**, or **DNS**.

   This specifies the format for the Server Address field. The default is IPv4.
9. In the **Server Address** field, enter the IPv4 address, IPv6 address, or DNS host name of the server.

   The default is the IPv4 address 0.0.0.0.
10. In the **Remote File Path** field, enter the path of the file to be downloaded.

    You can enter up to 96 characters.

11. In the **Remote File Name** field, enter the name of the file to be downloaded.

    You can enter up to 32 characters.

12. If you select **SFTP** or **SCP** from **Transfer Mode** menu, specify the following settings:
    - **User Name**: Specify the user name for remote login to the server.
    - **Password**: Specify the password for remote login to the server.
13. Click the **Apply** button.

    The host key file starts downloading.

You cannot log in to the switch

After you enter the wrong password three times, your switch blocks further attempts to log in. By default, 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

You can configure these settings (see Configure password lockout on page 303).

A

Configuration Examples

This appendix contains the following sections:

- Virtual local area networks (VLANs)
- Access control lists (ACLs)
- Differentiated Services (DiffServ)
- 802.1X access control
- Multiple Spanning Tree Protocol
- VLAN routing interfaces

Virtual local area networks (VLANs)

A local area network (LAN) can generally be defined as a broadcast domain. Hubs, bridges, or switches in the same physical segment or segments connect all end node devices. End nodes can communicate with each other without the need for a router. Routers connect LANs together, routing the traffic to the appropriate port.

A virtual LAN (VLAN) is a local area network with a definition that maps workstations on some basis other than geographic location (for example, by department, type of user, or primary application). To enable traffic to flow between VLANs, traffic must go through a router, just as if the VLANs were on two separate LANs.

A VLAN is a group of computers, servers, and other network resources that behave as if they were connected to a single network segment—even though they might not be. For example, all marketing personnel might be spread throughout a building. Yet if they are all assigned to a single VLAN, they can share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specified individuals, depending on how the IT manager set up the VLANs.

VLANs present a number of advantages:

- It is easy to do network segmentation. Users who communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group's traffic is contained largely within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.
- They are easy to manage. The addition of nodes, as well as moves and other changes, can be dealt with quickly and conveniently from a management interface rather than from the wiring closet.
- They provide increased performance. VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.
- They ensure enhanced network security. VLANs create virtual boundaries that can be crossed only through a router. So standard, router-based security measures can be used to restrict access to each VLAN.

Packets received by the switch are treated in the following way:

- When an untagged packet enters a port, it is automatically tagged with the port's default VLAN ID tag number. Each port supports a default VLAN ID setting that is user configurable (the default setting is 1). The default VLAN ID setting for each port can be changed on the Port PVID Configuration page. See Configure the PVID settings on page 155.
- When a tagged packet enters a port, the tag for that packet is unaffected by the default VLAN ID setting. The packet proceeds to the VLAN specified by its VLAN ID tag number.
- If the port through which the packet entered is not a member of the VLAN as specified by the VLAN ID tag, the packet is dropped.

- If the port is a member of the VLAN specified by the packet's VLAN ID, the packet can be sent to other ports with the same VLAN ID.
- Packets leaving the switch are either tagged or untagged, depending on the setting for that port's VLAN membership properties. A U for a given port means that packets leaving the switch from that port are untagged. Inversely, a T for a given port means that packets leaving the switch from that port are tagged with the VLAN ID that is associated with the port.

The example given in this section comprises numerous steps to illustrate a wide range of configurations to help provide an understanding of tagged VLANs.

VLAN configuration examples

This example demonstrates several scenarios of VLAN use and describes how the switch handles tagged and untagged traffic.

In this example, you create two new VLANs, change the port membership for default VLAN 1, and assign port members to the two new VLANs:

1. On the Basic VLAN Configuration page (see Configure VLANs on page 149), create the following VLANs:
   - A VLAN with VLAN ID 10.
   - A VLAN with VLAN ID 20.
2. On the VLAN Membership page (see Configure VLAN membership on page 152) specify the VLAN membership as follows:
   - For the default VLAN with VLAN ID 1, specify the following members: port 7 (U) and port 8 (U).
   - For the VLAN with VLAN ID 10, specify the following members: port 1 (U), port 2 (U), and port 3 (T).
   - For the VLAN with VLAN ID 20, specify the following members: port 4 (U), port 5 (T), and port 6 (U).
3. On the Port PVID Configuration page (see Configure the PVID settings on page 155), specify the PVID for ports g1 and g4 so that packets entering these ports are tagged with the port VLAN ID:
   - Port g1: PVID 10
   - Port g4: PVID 20
4. With the VLAN configuration that you set up, the following situations produce results as described:
   - If an untagged packet enters port 1, the switch tags it with VLAN ID 10. The packet can access port 2 and port 3. The outgoing packet is stripped of its tag to leave port 2 as an untagged packet. For port 3, the outgoing packet leaves as a tagged packet with VLAN ID 10.
   - If a tagged packet with VLAN ID 10 enters port 3, the packet can access port 1 and port 2. If the packet leaves port 1 or port 2, it is stripped of its tag to leave the switch as an untagged packet.

- If an untagged packet enters port 4, the switch tags it with VLAN ID 20. The packet can access port 5 and port 6. The outgoing packet is stripped of its tag to become an untagged packet as it leaves port 6. For port 5, the outgoing packet leaves as a tagged packet with VLAN ID 20.

Access control lists (ACLs)

ACLs ensure that only authorized users can access specific resources while blocking off any unwarranted attempts to reach network resources.

ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and provide security for the network. ACLs are normally used in firewall routers that are positioned between the internal network and an external network, such as the Internet. They can also be used on a router positioned between two parts of the network to control the traffic entering or exiting a specific part of the internal network. The added packet processing required by the ACL feature does not affect switch performance. That is, ACL processing occurs at wire speed.

Access lists are sequential collections of permit and deny conditions. This collection of conditions, known as the filtering criteria, is applied to each packet that is processed by the switch or the router. The forwarding or dropping of a packet is based on whether or not the packet matches the specified criteria.

Traffic filtering requires the following two basic steps:

1. Create an access list definition.

   The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. Additionally, you can assign traffic that matches the criteria to a particular queue or redirect the traffic to a particular port. A default *deny all* rule is the last rule of every list.

2. Apply the access list to an interface in the inbound direction.

The switch allow ACLs to be bound to physical ports and LAGs. The switch software supports MAC ACLs and IP ACLs.

MAC ACL example configuration

The following example shows how to create a MAC-based ACL that permits Ethernet traffic from the Sales department on specified ports and denies all other traffic on those ports.

1. On the MAC ACL page, create an ACL with the name Sales_ACL for the Sales department of your network (see Configure a MAC ACL on page 373).

   By default, this ACL is bound on the inbound direction, which means that the switch examines traffic as it enters the port.

2. On the MAC Rules page, create a rule for the Sales_ACL with the following settings:
   - **Sequence Number**. 1
   - **Action**. Permit
   - **Assign Queue ID**. 0
   - **Match Every**. False
   - **CoS**. 0
   - **Destination MAC**. 01:02:1A:BC:DE:EF
   - **Destination MAC Mask**. 00:00:00:00:FF:FF
   - **EtherType**. User Value.
   - **Source MAC**. 02:02:1A:BC:DE:EF
   - **Source MAC Mask**. 00:00:00:00:FF:FF
   - **VLAN ID**. 2

   For more information about MAC ACL rules, see Configure MAC ACL rules on page 376.
3. On the MAC Binding Configuration page, assign the Sales_ACL to the interface Gigabit ports 6, 7, and 8, and then click the **Apply** button. (See Configure MAC ACL interface bindings on page 380.)

   You can assign an optional sequence number to indicate the order of this access list relative to other access lists if any are already assigned to this interface and direction.
4. The MAC Binding Table displays the interface and MAC ACL binding information. (See View or delete MAC ACL bindings on page 381.)

The ACL named Sales_ACL looks for Ethernet frames with destination and source MAC addresses and MAC masks defined in the rule. Also, the frame must be tagged with VLAN ID 2, which is the Sales department VLAN. The CoS value of the frame must be 0, which is the default value for Ethernet frames. Frames that match this criteria are permitted on interfaces 6, 7, and 8 and are assigned to the hardware egress queue 0, which is the default queue. All other traffic is explicitly denied on these interfaces. To allow additional traffic to enter these ports, you must add a new Permit rule with the desired match criteria and bind the rule to interfaces 6, 7, and 8.

Basic IPv4 ACL example configuration

The following example shows how to create an IPv4-based ACL that prevents any IP traffic from the Finance department from being allowed on the ports that are associated with other departments. Traffic from the Finance department is identified by each packet's network IP address.

1. On the IP ACL page, create a new IP ACL with an IP ACL ID of 1. (See Configure a basic or extended IPv4 ACL on page 382.)
2. On the IP Rules page, create a rule for IP ACL 1 with the following settings:
   - **Sequence Number**. 1
   - **Action**. Deny
   - **Assign Queue ID**. 0 (optional: 0 is the default value)
   - **Match Every**. False
   - **Source IP Address**. 192.168.187.0
   - **Source IP Mask**. 255.255.0

   For additional information about IP ACL rules, see Configure rules for a basic IPv4 ACL on page 386.
3. Click the **Add** button.
4. On the IP Rules page, create a second rule for IP ACL 1 with the following settings:
   - **Sequence Number**. 2
   - **Action**. Permit
   - **Match Every**. True
5. Click the **Add** button.
6. On the IP Binding Configuration page, assign ACL ID 1 to the interface Gigabit ports 2, 3, and 4, and assign a sequence number of 1. (See Configure IP ACL interface bindings on page 406.)

   By default, this IP ACL is bound on the inbound direction, so it examines traffic as it enters the switch.
7. Click the **Apply** button.
8. Use the IP Binding Table page to view the interfaces and IP ACL binding information. (See View or delete an IP ACL binding on page 408)

The IP ACL in this example matches all packets with the source IP address and subnet mask of the Finance department's network and deny it on the Ethernet interfaces 2, 3, and 4 of the switch. The second rule permits all non-Finance traffic on the ports. The second rule is required because an explicit *deny all* rule exists as the lowest priority rule.

Differentiated Services (DiffServ)

Standard IP-based networks are designed to provide *best effort* data delivery service. *Best effort* service implies that the network delivers the data in a timely fashion, although there is no guarantee that it does. During times of congestion, packets might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. However, any degradation of service can negatively affect applications with strict timing requirements, such as voice or multimedia.

Quality of Service (QoS) can provide consistent, predictable data delivery by distinguishing between packets with strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given special treatment in a QoS-capable network. With this in mind, all elements of the network must be QoS capable. If one node cannot meet the necessary timing requirements, this creates a deficiency in the network path and the performance of the entire packet flow is compromised.

Two basic types of QoS are supported:

- **Integrated Services**. Network resources are apportioned based on request and are reserved (resource reservation) according to network management policy (RSVP, for example).
- **Differentiated Services**. Network resources are apportioned based on traffic classification and priority, giving preferential treatment to data with strict timing requirements.

The switch supports DiffServ.

The DiffServ feature contains a number of conceptual QoS building blocks that you can use to construct a differentiated service network. Use these same blocks in different ways to build other types of QoS architectures.

You must configure three key QoS building blocks for DiffServ:

- Class
- Policy
- Service (the assignment of a policy to a directional interface)

Class

You can classify incoming packets at Layers 2, 3, and 4 by inspecting the following information for a packet:

- Source/destination MAC address
- EtherType
- Class of Service (802.1p priority) value (first/only VLAN tag)
- VLAN ID range (first/only VLAN tag)

- Secondary 802.1p priority value (second/inner VLAN tag)
- Secondary VLAN ID range (second/inner VLAN tag)
- IP Service Type octet (also known as: ToS bits, Precedence value, DSCP value)
- Layer 4 protocol (TCP, UDP and so on)
- Layer 4 source/destination ports
- Source/destination IP address

From a DiffServ point of view, two types of classes exist:

- DiffServ traffic classes
- DiffServ service levels/forwarding classes

DiffServ traffic classes

With DiffServ, you define which traffic classes to track on an ingress interface. You can define simple BA classifiers (DSCP) and a wide variety of multifield (MF) classifiers:

- Layer 2; Layers 3, 4 (IP only)
- Protocol-based
- Address-based

You can combine these classifiers with logical AND operations to build complex MF-classifiers. That is, within a single class, multiple match criteria are grouped together as an AND expression. Only classes of the same type can be nested; class nesting does not allow for the negation (*exclude* option) of the referenced class.

To configure DiffServ, you must define service levels, namely the forwarding classes/PHBs identified by a given DSCP value, on the egress interface. You define these service levels by configuring BA classes for each.

Create policies

Use DiffServ policies to associate a collection of classes that you configure with one or more QoS policy statements. The result of this association is referred to as a policy.

From a DiffServ perspective, two types of policies exist:

- **Traffic Conditioning Policy**. A policy applied to a DiffServ traffic class
- **Service Provisioning Policy**. A policy applied to a DiffServ service level

You must manually configure the various statements and rules used in the traffic conditioning and service provisioning policies to achieve the desired Traffic Conditioning Specification (TCS) and the Service Level Specification (SLS) operation, respectively.

Traffic conditioning policy

Traffic conditioning pertains to actions performed on incoming traffic. Several distinct QoS actions are associated with traffic conditioning:

- **Dropping**. Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot coexist on the same interface.
- **Marking IP DSCP or IP Precedence**. Marking/re-marking the DiffServ code point in a packet with the DSCP value representing the service level associated with a particular DiffServ traffic class. Alternatively, the IP precedence value of the packet can be marked/re-marked.
- **Marking CoS (802.1p)**. Sets the 3-bit priority field in the first/only 802.1p header to a specified value when packets are transmitted for the traffic class. An 802.1p header is inserted if it does not already exist. This is useful for assigning a Layer 2 priority level based on a DiffServ forwarding class (such as the DSCP or IP precedence value) definition to convey some QoS characteristics to downstream switches that do not routinely look at the DSCP value in the IP header.
- **Policing**. A method of constraining incoming traffic associated with a particular class so that it conforms to the terms of the TCS. Packets that do not conform to the policy are always dropped (no other actions are available for such packets). The DiffServ feature supports the following types of traffic policing treatments (actions) for packets that confirm to the policy:
  - **drop**. The packet is dropped.
  - **mark cos**. The 802.1p user priority bits are (re)marked and forwarded.
  - **mark dscp**. The packet DSCP is (re)marked and forwarded.
  - **mark prec**. The packet IP Precedence is (re)marked and forwarded.
  - **send**. The packet is forwarded without DiffServ modification.
- **Counting**. Updating octet and packet statistics to keep track of data handling along traffic paths within DiffServ. In this DiffServ feature, counters are not explicitly configured by the user, but are designed into the system based on the DiffServ policy being created. For more information, see Monitor the switch and the ports on page 413.
- **Assigning QoS Queue**. Directs a traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.
- **Redirecting**. Forces a classified traffic stream to a specified egress port (physical or LAG). This can occur in addition to any marking or policing action. It can also be specified along with a QoS queue assignment.

DiffServ example configuration

To create a DiffServ class and policy and attach them to a switch interface, follow these steps:

1. On the QoS Class Configuration page, create a new class with the following settings:
   - **Class Name**. Class1
   - **Class Type**. All

   For more information about this page, see Configure a DiffServ class on page 279.
2. Click the **Class1** hyperlink to view the DiffServ Class Configuration page for this class.
3. Configure the following settings for Class1:
   - **Protocol Type**. UDP
   - **Source IP Address**. 192.12.1.0.
   - **Source Mask**. 255.255.255.0.
   - **Source L4 Port**. Other, and enter 4567 as the source port value.
   - **Destination IP Address**. 192.12.2.0.
   - **Destination Mask**. 255.255.255.0.
   - **Destination L4 Port**. Other, and enter 4568 as the destination port value.

   For more information about this page, see Configure a DiffServ class on page 279.
4. Click the **Apply** button.
5. On the Policy Configuration page, create a new policy with the following settings:
   - **Policy Selector**. Policy1
   - **Member Class**. Class1

   For more information about this page, see Configure a DiffServ Policy on page 289.
6. Click the **Add** button.

   The policy is added.
7. Click the **Policy1** hyperlink to view the Policy Class Configuration page for this policy.
8. Configure the Policy attributes as follows:
   - **Assign Queue**. 3
   - **Policy Attribute**. Simple Policy
   - **Color Mode**. Color Blind
   - **Committed Rate**. 1000000 Kbps
   - **Confirm Action**. Send
   - **Violate Action**. Drop

   For more information about this page, see Configure a DiffServ Policy on page 289.

9. On the Service Configuration page, select the check box next to interfaces g7 and g8 to attach the policy to these interfaces, and then click the **Apply** button. (See Configure the DiffServ service interface on page 295.)

All UDP packet flows destined to the 192.12.2.0 network with an IP source address from the 192.12.1.0 network that include a Layer 4 Source port of 4567 and Destination port of 4568 from this switch on ports 7 and 8 are assigned to hardware queue 3.

On this network, traffic from streaming applications uses UDP port 4567 as the source and 4568 as the destination. This real-time traffic is time sensitive, so it is assigned to a high-priority hardware queue. By default, data traffic uses hardware queue 0, which is designated as a best-effort queue.

Also the *confirmed action* on this flow is to send the packets with a committed rate of 1000000 Kbps. Packets that violate the committed rate are dropped.

802.1X access control

Local area networks (LANs) are often deployed in environments that permit unauthorized devices to be physically attached to the LAN infrastructure, or permit unauthorized users to attempt to access the LAN through equipment already attached. In such environments you might want to restrict access to the services offered by the LAN to those users and devices that are permitted to use those services.

Port-based network access control makes use of the physical characteristics of LAN infrastructures to provide a means of authenticating and authorizing devices attached to a LAN port with point-to-point connection characteristics. If the authentication and authorization process fails, access control prevents access to that port. In this context, a port is a single point of attachment to the LAN, such as a port of a MAC bridge and an association between stations or access points in IEEE 802.11 wireless LANs.

The IEEE 802.11 standard describes an architectural framework within which authentication and consequent actions take place. It also establishes the requirements for a protocol between the authenticator (the system that passes an authentication request to the authentication server) and the supplicant (the system that requests authentication), as well as between the authenticator and the authentication server.

The switch supports a guest VLAN, which allows unauthenticated users limited access to the network resources.

Note: You can use QoS features to provide rate limiting on the guest VLAN to limit the network resources that the guest VLAN provides.

Another 802.1X feature is the ability to configure a port to enable or disable EAPoL packet forwarding support. You can disable or enable the forwarding of EAPoL when 802.1X is disabled on the device.

The ports of an 802.1X authenticator switch provide the means by which it can offer services to other systems reachable through the LAN. Port-based network access control allows the operation of a switch's ports to be controlled to ensure that access to its services is permitted only by systems that are authorized to do so.

Port access control provides a means of preventing unauthorized access by supplicants to the services offered by a system. Control over the access to a switch and the LAN to which it is connected can be desirable when you restrict access to publicly accessible bridge ports or to restrict access to departmental LANs.

Access control is achieved by enforcing authentication of supplicants that are attached to an authenticator's controlled ports. The result of the authentication process determines whether the supplicant is authorized to access services on that controlled port.

A port access entity (PAE) is able to adopt one of two distinct roles within an access control interaction:

1. **Authenticator**. A port that enforces authentication before allowing access to services available through that port.
2. **Supplicant**. A port that attempts to access services offered by the authenticator.

Additionally, there exists a third role:

3. **Authentication server**. Performs the authentication function necessary to check the credentials of the supplicant on behalf of the authenticator.

All three roles are required for you to complete an authentication exchange.

The switch supports the authenticator role only, in which the PAE is responsible for communicating with the supplicant. The authenticator PAE is also responsible for submitting the information received from the supplicant to the authentication server for the credentials to be checked, which determines the authorization state of the port. The authenticator PAE controls the authorized/unauthorized state of the controlled port depending on the outcome of the RADIUS-based authentication process.

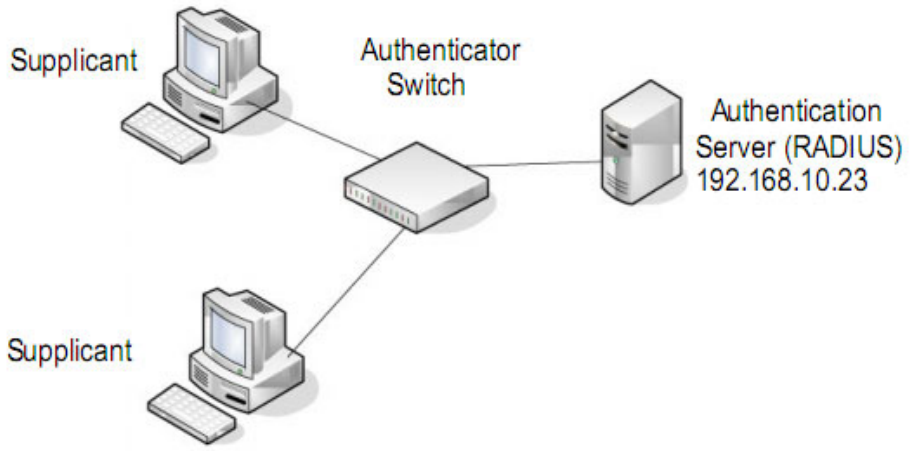


Figure 1. 802.1X authentication roles

802.1X example configuration

This example shows how to configure the switch so that 802.1X-based authentication is required on the ports in a corporate conference room (1/0/5–1/0/8). These ports are available to visitors and must be authenticated before access is granted to the network. The authentication is handled by an external RADIUS server. When the visitor is successfully authenticated, traffic is automatically assigned to the guest VLAN. This example assumes that a VLAN was configured with a VLAN ID of 150 and VLAN name of Guest.

1. On the Port Authentication page, select ports **1/0/5**, **1/0/6**, **1/0/7**, and **1/0/8**.
2. From the **Port Control** menu, select **Unauthorized**.

   The selection from the **Port Control** menu for all other ports on which authentication is not needed must be **Authorized**. When the selection from the **Port Control** menu is **Authorized**, the port is unconditionally put in a force-authorized state and does not require any authentication. When the selection from the **Port Control** menu is **Auto**, the authenticator PAE sets the controlled port mode.
3. In the **Guest VLAN** field for ports 1/0/5–1/0/8, enter **150** to assign these ports to the guest VLAN.

   You can configure additional settings to control access to the network through the ports. See Configure port security settings for one or more interfaces on page 351 for information about the settings.
4. Click the **Apply** button.
5. On the 802.1X Configuration page, set the port based authentication state and guest VLAN mode to **Enable**, and then the **Apply** button. (See Configure the global port security mode on page 350.)

   This example uses the default values for the port authentication settings, but you can configure several additional settings. For example, the **EAPOL Flood Mode** field allows you to enable the forwarding of EAPoL frames when 802.1X is disabled on the device.
6. On the RADIUS Server Configuration page, configure a RADIUS server with the following settings:
   - **Server Address**. 192.168.10.23
   - **Secret Configured**. Yes
   - **Secret**. secret123
   - **Active**. Primary

   For more information, see Manage the RADIUS settings on page 304.
7. Click the **Add** button.
8. On the Authentication List page, configure the default list to use RADIUS as the first authentication method. (See Configure authentication lists on page 317.)

This example enables 802.1X-based port security on the switch and prompts the hosts connected on ports g5-g8 for an 802.1X-based authentication. The switch passes the authentication information to the configured RADIUS server.

Multiple Spanning Tree Protocol

Spanning Tree Protocol (STP) runs on bridged networks to help eliminate loops. If a bridge loop occurs, the network can become flooded with traffic. IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) supports multiple instances of spanning tree to efficiently channel VLAN traffic over different interfaces. Each instance of the spanning tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree, with slight modifications in the working but not the end effect (chief among the effects is the rapid transitioning of the port to the forwarding state).

The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full-duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to the Forwarding state and the suppression of Topology Change Notification. These features are represented by the parameters pointtopoint and edgeport. MSTP is compatible to both RSTP and STP. It behaves in a way that is appropriate for STP and RSTP bridges.

An MSTP bridge can be configured to behave entirely as a RSTP bridge or an STP bridge. So, an IEEE 802.1s bridge inherently also supports IEEE 802.1w and IEEE 802.1D.

The MSTP algorithm and protocol provide simple and full connectivity for frames assigned to any given VLAN throughout a bridged LAN comprising arbitrarily interconnected networking devices, each operating MSTP, STP, or RSTP. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) regions composed of LANs and or MSTP bridges. These regions and the other bridges and LANs are connected into a single Common Spanning Tree (CST). (IEEE DRAFT P802.1s/D13)

MSTP connects all bridges and LANs with a single Common and Internal Spanning Tree (CIST). The CIST supports the automatic determination of each MST region, choosing its maximum possible extent. The connectivity calculated for the CIST provides the CST for interconnecting these regions, and an Internal Spanning Tree (IST) within each region. MSTP ensures that frames with a given VLAN ID are assigned to one and only one of the MSTIs or the IST within the region, that the assignment is consistent among all the networking devices in the region, and that the stable connectivity of each MSTI and IST at the boundary of the region matches that of the CST. The stable active topology of the bridged LAN with respect to frames consistently classified as belonging to any given VLAN thus simply and fully connects all LANs and networking devices throughout the network, though frames belonging to different VLANs can take different paths within any region, per IEEE DRAFT P802.1s/D13.

All bridges, whether they use STP, RSTP, or MSTP, send information in configuration messages through Bridge Protocol Data Units (BPDUs) to assign port roles that determine each port’s participation in a fully and simply connected active topology based on one or more spanning trees. The information communicated is known as the spanning tree priority vector. The BPDU structure for each of these different protocols is different. An MSTP bridge transmits the appropriate BPDU depending on the received type of BPDU from a particular port.

An MST region comprises of one or more MSTP bridges with the same MST configuration identifier, using the same MSTIs, and without any bridges attached that cannot receive and transmit MSTP BPDUs. The MST configuration identifier includes the following components:

1. Configuration identifier format selector
2. Configuration name
3. Configuration revision level
4. Configuration digest: 16-byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID to MSTID mapping)

Because multiple instances of spanning tree exist, an MSTP state is maintained on a per-port, per-instance basis (or on a per-port, per-VLAN basis, as any VLAN can be in one and only one MSTI or CIST). For example, port A can be forwarding for instance 1 while discarding for instance 2. The port states changed since IEEE 802.1D specification.

To support multiple spanning trees, configure an MSTP bridge with an unambiguous assignment of VLAN IDs (VIDs) to spanning trees. For such a configuration, ensure the following:

1. The allocation of VIDs to FIDs is unambiguous.
2. Each FID that is supported by the bridge is allocated to exactly one spanning tree instance.

The combination of VID to FID and then FID to MSTI allocation defines a mapping of VIDs to spanning tree instances, represented by the MST Configuration Table.

With this allocation we ensure that every VLAN is assigned to one and only one MSTI. The CIST is also an instance of spanning tree with an MSTID of 0.

VIDs might be not be allocated to an instance, but every VLAN must be allocated to one of the other instances of spanning tree.

The portion of the active topology of the network that connects any two bridges in the same MST region traverses only MST bridges and LANs in that region, and never bridges of any kind outside the region. In other words, connectivity within the region is independent of external connectivity.

MSTP example configuration

This example shows how to create an MSTP instance from the switch. The example network includes three different switches that serve different locations in the network. In this example, ports 1/0/1–1/0/5 are connected to host stations, so those links are not subject to network loops. Ports 1/0/6–1/0/8 are connected across switches 1, 2, and 3.

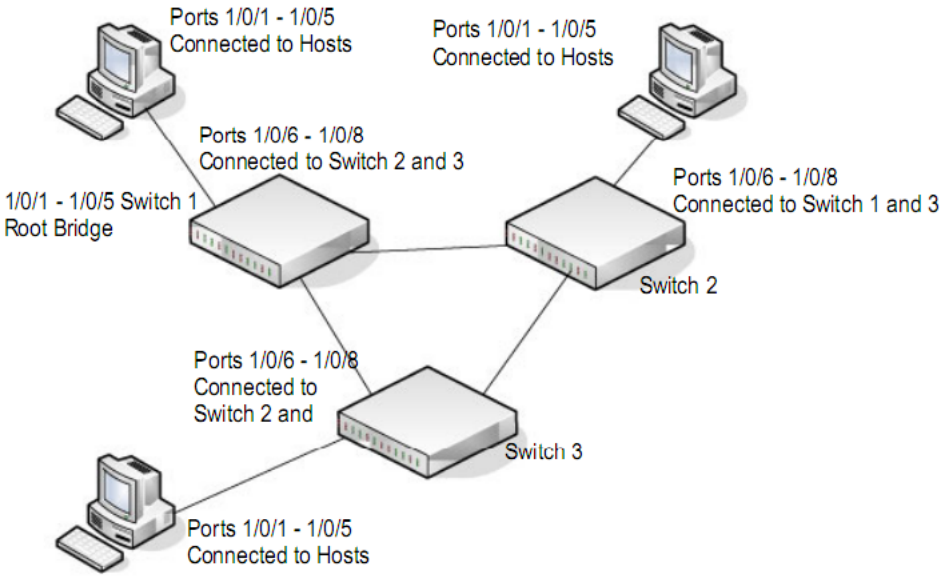


Figure 2. MSTP example configuration

Perform the following procedures on each switch to configure MSTP:

1. On the VLAN Configuration page, create VLANs 300 and 500 (see Configure VLAN settings on page 149).
2. On the VLAN Membership page, include ports 1/0/1–1/0/8 as tagged (T) or untagged (U) members of VLAN 300 and VLAN 500 (see Configure VLAN settings on page 149).
3. On the STP Configuration page, enable the Spanning Tree State option (see Configure the STP settings and view the STP status on page 175).

   Use the default values for the rest of the STP configuration settings. By default, the STP operation mode is MSTP and the configuration name is the switch MAC address.
4. On the CST Configuration page, set the bridge priority value for each of the three switches to force Switch 1 to be the root bridge:
   - **Switch 1**. 4096
   - **Switch 2**. 12288
   - **Switch 3**. 20480

   Note: Bridge priority values are multiples of 4096.

   If you do not specify a root bridge and all switches are assigned the same bridge priority value, the switch with the lowest MAC address is elected as the root bridge (see Configure the CST Settings on page 177).
5. On the CST Port Configuration page, select ports 1/0/1–1/0/8 and select **Enable** from the **STP Status** menu (see Configure the CST port settings on page 178).
6. Click the **Apply** button.
7. Select ports 1/0/1–1/0/5 (edge ports), and select **Enable** from the **Fast Link** menu.

Since the edge ports are not at risk for network loops, ports with Fast Link enabled transition directly to the forwarding state.

8. Click the **Apply** button.

   You can use the CST Port Status page to view spanning tree information about each port.

9. On the MST Configuration page, create a MST instances with the following settings:
   - **MST ID**. 1
   - **Priority**. Use the default (32768)
   - **VLAN ID**. 300

   For more information, see View the Rapid STP information on page 182.

10. Click the **Add** button.
11. Create a second MST instance with the following settings
    - **MST ID**. 2
    - **Priority**. 49152
    - **VLAN ID**. 500
12. Click the **Add** button.

In this example, assume that Switch 1 became the root bridge for the MST instance 1, and Switch 2 became the root bridge for MST instance 2. Switch 3 supports hosts in the sales department (ports 1/0/1, 1/0/2, and 1/0/3) and in the HR department (ports 1/0/4 and 1/0/5). Switches 1 and 2 also include hosts in the sales and HR departments. The hosts connected from Switch 2 use VLAN 500, MST instance 2 to communicate with the hosts on Switch 3 directly. Likewise, hosts of Switch 1 use VLAN 300, MST instance 1 to communicate with the hosts on Switch 3 directly.

The hosts use different instances of MSTP to effectively use the links across the switch. The same concept can be extended to other switches and more instances of MSTP.

VLAN routing interfaces

VLANs divide broadcast domains in a LAN environment. When hosts in one VLAN must communicate with hosts in another VLAN, the traffic must be routed between them. This is known as inter-VLAN routing. On the switch, it is accomplished by creating Layer 3 interfaces (switch virtual interfaces [SVI]).

When a port is enabled for bridging (the default) rather than routing, all normal bridge processing is performed for an inbound packet, which is then associated with a VLAN. Its MAC destination address (MAC DA) and VLAN ID are used to search the MAC address table. If routing is enabled for the VLAN, and the MAC DA of an inbound unicast packet is that of the internal bridge-router interface, the packet is routed. An inbound multicast packet is forwarded to all ports in the VLAN, plus the internal bridge-router interface, if it was received on a routed VLAN.

Since a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. VLAN routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when additional segmentation or security is required. A port can be either a VLAN port or a router port, but not both. However, a VLAN port can be part of a VLAN that is itself a router port.

Complete these steps to configure a switch to perform interVLAN routing:

1. Use the IP Configuration page to enable routing on the switch.

   For more information about this step, see Manage the global IPv4 routing settings on page 233.

2. Determine the IP addresses that you want to assign to the VLAN interface on the switch.

   For the switch to be able to route between the VLANs, the VLAN interfaces must be configured with an IP address. When the switch receives a packet destined for another subnet/VLAN, the switch looks at the routing table to determine where to forward the packet. The packet is then passed to the VLAN interface of the destination. It is then sent to the port where the end device is attached.

3. Use the VLAN Routing Wizard page to create a routing VLAN, configure the IP address and subnet mask, and add the member ports.

   For more information about this step, see Create a routing interface with the VLAN Static Routing Wizard on page 253.

B

Default Settings and Specifications

This appendix contains the following sections:

- Access default settings for the switch device UI
- System features default settings
- Switching features default settings
- Routing and multicast features default settings
- QoS features default settings
- Security features default settings
- Monitoring features default settings
- Hardware technical specifications

Note: Settings that you cannot change in the device UI are not included in the tables in this appendix but might be included in 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.

Table 102. Default settings for access to the switch device UI

Feature	Default
Management mode	Directly Connected To Web Browser Interface (Local LAN Only)
IP address	192.168.0.239
Subnet mask	255.255.255.0
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 new password.
Minimum length for password	Eight characters
Encryption type for the password	SHA512
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 103. System features default settings

Feature Name/Setting	Default
Time, Global	
Clock source	SNTP
SNTP client mode	Unicast

Table 103. System features default settings (continued)

Feature Name/Setting	Default
Port	123
Source interface	VLAN 1
Unicast poll interval	6
Broadcast poll interval	6
Unicast poll timeout	5
Unicast poll retry	1
Offset hours	0
Offset minutes	0
Time, SNTP Server	
Server type	DNS (for each default server)
Address	time-a.netgear.com time-b.netgear.com 0.openwrt.pool.ntp.org **Note:** Other servers might be default servers.
Port	123 (for each default server)
Priority	1 (for each default server)
Version	4 (for each default server)
Time, Daylight Saving	
Daylight saving	Disabled
Denial of Service	
Auto-DoS Configuration	Disabled
Denial of Service minimum TCP header size	20
Denial of Service ICMPv4	Disabled
Denial of Service maximum ICMPv4 packet size	512 (if maximum ICMPv4 packet size is enabled)
Denial of Service ICMPv6	Disabled
Denial of Service maximum ICMPv6 packet size	512 (if maximum ICMPv6 packet size is enabled)
Denial of Service first fragment	Disabled
Denial of Service ICMP fragment	Disabled
Denial of Service SIP=DIP	Disabled
Denial of Service SMAC=DMAC	Disabled

Table 103. System features default settings (continued)

Feature Name/Setting	Default
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 SYN	Disabled
Denial of Service TCP SYN & FIN	Disabled
Denial of Service UDP port	Disabled
DNS	
DNS status	Enabled
DNS server	8.8.8.8 **Note:** Another server might be the default server.
Switch Discovery	
UPnP Administrative Mode	Enabled
Green Ethernet, Global	
Auto Power Down mode	Disabled
EEE mode	Disabled
Green Ethernet, Interface	
Auto Power Down mode	Disabled
EEE mode	Disabled
Green Ethernet LPI History	
Sampling interval	3600
Maximum samples to keep	168
Green Ethernet Detail	
Energy Detect Admin Mode	Disabled (for all interfaces)
EEE Admin Mode	Disabled (for all interfaces)
EEE Transmit Idle Time	600
EEE Transmit Wake Time	17

Table 103. System features default settings (continued)

Feature Name/Setting	Default
PoE Configuration	
System usage threshold	95
Power management mode	Dynamic
PoE traps	Enabled
PoE Port Configuration	
Port power	Enabled
Port priority	Low
Power mode	802.3at
Power limit type	User
Power limit (W)	30.00
Detection type	IEEE 802
Timer schedule	None configured, none assigned
SNMPv1/v2	
Community configuration	None
Trap configuration	None
SNMPv1/v2 Trap Flags	
Authentication	Enabled
Link up/down	Enabled
Spanning tree	Enabled
ACL	Disabled
PoE	Enabled
SNMPv3	
User name	admin
SNMPv3 access mode	Read/Write
Authentication protocol	SHA512
Authentication key	password
Encryption protocol	AES128
Encryption key	password

Table 103. System features default settings (continued)

Feature Name/Setting	Default
LLDP, Global	
TLV advertised interval	30
Hold multiplier	4
Reinitializing delay	2
Transmit delay	5
LLDP, Interface	
Admin Status	TX and Rx
Management IP address	Auto Advertise
Notification	Disabled
Optional TLVs	Enabled
LLDP-MED, Global	
Fast start duration	3
LLDP-MED, Interface	
LLDP-MED status	Enabled
Notification	Enabled
Transmit optional TLVs, MED capabilities	Enabled
Transmit optional TLVs, Network policy	Enabled
DHCP L2 Relay, Global	
Admin mode	Enabled
DHCP L2 Relay, Interface	
Admin mode	Disabled
82 Option Trust mode	Disabled
DHCP Snooping, Global	
DHCP snooping mode	Disabled
MAC address validation	Enabled
DHCP Snooping, Interface	
Trust mode	Disabled
Invalid packets	Disabled
Rate limits	None

Table 103. System features default settings (continued)

Feature Name/Setting	Default
Burst interval	N/A
DHCP Snooping, Persistent Configuration	
Store	Local
Remote IP address	None
Remote file name	None
Write delay	300
Dynamic ARP Inspection, Global	
Validate source MAC	Disabled
Validate destination MAC	Disabled
Validate IP	Disabled
Dynamic ARP Inspection, VLAN	
Admin mode	Disabled
Invalid packets	Enabled
ARP ACL name	None
Static flag	Disabled
Dynamic ARP Inspection, Interface	
Trust mode	Disabled
Rate limit (pps)	15
Burst interval (secs)	1

Switching features default settings

The following table describes the default settings for the switching features that you can configure.

Table 104. Switching features default settings

Feature Name/Setting	Default
Ports	
Admin mode	Enabled
Autonegotiation	Enabled

Table 104. Switching features default settings (continued)

Feature Name/Setting	Default
Speed	Auto
Duplex mode	Auto
Link trap	Enabled
Frame size	1500
Flow control	Disabled
LAGs	
Admin mode	Enabled
Hash mode	3 Src/Dest MAC, VLAN, EType, incoming port
STP mode	Enabled
Link trap	Enabled
LAG type	Static
LACP Configuration	
LACP System Priority	32768
LACP Port Priority	
LACP priority	128
Timeout	Long
VLANs, Global	
Internal VLAN allocation base	1 to 4093
Default VLANs	1, Default (All ports are members) 4088, Auto-VoIP (no ports are members) 4089, Auto-Video (no ports are members)
Port PVIDs, Interface	
PVID	1
VLAN member	1
VLAN tag	None
Acceptable Frame	Admit All
Ingress filtering	Disabled
Port priority	0
Voice VLAN, Global	
Admin mode	Disabled

Table 104. Switching features default settings (continued)

Feature Name/Setting	Default
Voice VLAN, Interface	
Interface mode	Disabled
Value	0
Cos override mode	Disabled
Authentication mode	Enabled
DSCP value	0
GVRP, Global	
GVRP mode	Disabled
GVRP, Interface	
GVRP mode	Disabled
Join timer	20
Leave timer	60
Leave All timer	1000
Auto-VoIP Protocol-Based, Global	
Prioritization type	Traffic Class
Class value	7
Auto-VoIP Protocol-Based, Interface	
Auto-VoIP mode	Disabled
Auto-VoIP OUI-Based, Global	
Auto-VoIP VLAN ID	4088
OUI-based priority	7
Auto-VoIP OUI-based, Interface	
Auto-VoIP mode	Disabled

Table 104. Switching features default settings (continued)

Feature Name/Setting	Default
OUI table	00:01:E3 SIEMENS 00:03:6B CISCO1 00:12:43 CISCO2 00:0F:E2 H3C 00:60:B9 NITSUKO 00:D0:1E PINTEL 00:E0:75 VERILINK 00:E0:BB 3COM 00:04:0D AVAYA1 00:1B:4F AVAYA2 00:04:13 SNOM
STP, Global	
Spanning tree state	Enabled
STP operation mode	RSTP
Configuration name	MAC address
Configuration revision level	0
Forwarding of BPDUs while STP is disabled	Disabled
CST, Global	
Bridge priority	32768
Bridge maximum age	20
Bridge forward delay	15
Spanning tree maximum hops	20
CST, Interface	
STP status	Enabled
Fast link	Disabled
BPDU forwarding	Disabled
Auto edge	Enabled
Path cost	0
Priority	128
External port path cost	0
MST, Global	
MST ID	0
Priority	32768

Table 104. Switching features default settings (continued)

Feature Name/Setting	Default
VLAN ID	1, 4088-4089
Auto-Video Configuration	
Auto-Video status	Disabled
IGMP Snooping, Global	
IGMP snooping status	Disabled
Validate IGMP IP header	Enabled
IGMP Snooping, Interface	
Admin mode	Disabled
Host timeout	260
Maximum response time	10
Mrouter timeout	0
Fast leave mode	Disabled
IGMP Snooping, VLAN	
VLAN ID	1, 4088, 4089
Admin mode	Disabled
Fast leave mode	Disabled
Host timeout	260
Maximum response time	10
Mrouter timeout	0
Report suppression mode	Disabled
Query mode	Disabled
Query interval	60
IGMP Snooping, Multicast Router, Interface	
Multicast router	Disabled
IGMP Snooping, Querier, Global	
Querier admin mode	Disabled
Snooping querier address	None
IGMP version	2
Query interval	60

Table 104. Switching features default settings (continued)

Feature Name/Setting	Default
Querier expiry interval	125
IGMP Snooping, Querier, VLAN	
VLAN ID	None
Querier Election Participate mode	Disabled
Querier VLAN address	None
MLD Snooping, Global	
MLD snooping admin mode	Disabled
MLD Snooping, Interface	
Admin mode	Disabled
Membership interval	260
Maximum response time	10
Expiration time	0
Fast leave	Disabled
MLD Snooping, Multicast Router, Interface	
Multicast router	Disabled
MLD Snooping, Querier, Global	
Querier admin mode	Disabled
Querier address	None
Query interval	60
Querier expiry interval	60
MVR, Global	
MVR running	Disabled
MVR multicast VLAN	1
MVR global query response time	5
MVR mode	Compatible
MVR, Interface	
Admin mode	Disabled
Type	None
Immediate leave	Disabled

Table 104. Switching features default settings (continued)

Feature Name/Setting	Default
Address Table	
Address aging timeout	300
L2 Loop Protection Configuration, Global	
Admin mode	Disabled
TLV Advertised Interval	5
Max PDU Receive	1
Recovery Timer	0
L2 Loop Protection Configuration, Interface	
Keep alive	Disabled
RX action	Disabled

Routing and multicast features default settings

The following table describes the default settings for the routing and multicast features that you can configure.

Table 105. Routing and multicast features default settings

Feature Name/Setting	Default
IP, Global	
Routing mode	Disabled
ICMP redirects	Disabled
IPv6, Global Configuration	
IPv6 unicast routing	Disabled
Hop limit	64
ICMPv6 rate limit error interval	1000
ICMPv6 rate limit burst size	100

Table 105. Routing and multicast features default settings (continued)

Feature Name/Setting	Default
IPv6, VLAN Configuration	
IPv6 VLAN	An IPv6 VLAN configuration is automatically added after you add a routing VLAN, but the IPv6 mode is disabled for the routing VLAN.
IPv6 mode	Disabled
DHCPv6 client mode	Disabled
Stateless Address AutoConfig mode	Disabled
Admin mode	Enabled
MTU	1500
Duplicate address detection transmits	1
Life time interval	1800
Adv NS interval	0
Adv reachable interval	0
Adv interval	600
Adv managed config flag	Disabled
Adv other config flag	Disabled
Router preference	Medium
Adv suppress flag	Disabled
Destination unreachables	Enabled
IPv6, Prefix Configuration	
IPv6 prefix	None configured
IPv6, Static Route Configuration	
IPv6 route	None configured
IPv6, Route Preference	
Static	1
ARP, Global	
Age time	1200
Response time	1
Retries	4

Table 105. Routing and multicast features default settings (continued)

Feature Name/Setting	Default
Cache size	479
Dynamic renewal	Enabled

QoS features default settings

The following table describes the default settings for the QoS features that you can configure.

Table 106. QoS features default settings

Feature Name/Setting	Default
CoS, Global	
Global trust mode	802.1p
CoS, Interface	
Interface trust mode	802.1p
Interface shaping rate	0
CoS, Interface Queue	
Queue ID	0
Minimum bandwidth	0
Scheduler type	Weighted
Queue management type	Taildrop
CoS, 802.1p Queue Mapping	
802.1p priority (802.1p -> queue)	0 -> 1 1 -> 0 2 -> 0 3 -> 1 4 -> 2 5 -> 2 6 -> 3 7 -> 3
CoS, DSDCP to Queue Mapping	
See the device UI	

Table 106. QoS features default settings (continued)

Feature Name/Setting	Default
DiffServ, Global No default classes, policies, and services configured	
DiffServ admin mode	Enabled

Security features default settings

The following table describes the default settings for the security features that you can configure.

Table 107. Security features default settings

Feature Name/Setting	Default
Management Security, User Password	
Encryption type	SHA512
Password minimum length	8
Lockout attempts	5
Unlock time	5
Unlock timer mode	Enabled
Management Security, RADIUS, Global No RADIUS servers configured	
Maximum number of retransmits	4
Timeout duration	5
Accounting mode	Disabled
Management Security, TACAS+, Global No TACACS+ servers configured	
Connection timeout	5
Management Security, Authentication List	
httpList	Option 1 is Local, options 2 through 4 are N/A
httpsList	Option 1 is Local, options 2 through 4 are N/A
dot1xList	Disabled
Access, HTTP	
HTTP access	Enabled

Table 107. Security features default settings (continued)

Feature Name/Setting	Default
HTTP session soft timeout (minutes)	15
HTTP session hard timeout (hours)	24
Maximum number of HTTP sessions	4
Access, HTTPS	
HTTPS access	Disabled
HTTPS port	443
HTTPS session soft timeout (minutes)	15
HTTPS session hard timeout (hours)	24
Maximum number of HTTPS sessions	4
Access, Access Control, Access Profile No access profile configured	
Port Authentication, 802.1X, Global	
Port-based authentication state	Disabled
VLAN assignment mode	Disabled
Dynamic VLAN Creation mode	Disabled
EAPOL flood mode	Disabled
Port Authentication, 802.1X, Interface	
Port control	Auto
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
Traffic Control, MAC Filter No MAC filters configured	

Table 107. Security features default settings (continued)

Feature Name/Setting	Default
Traffic Control, Storm Control, Global	
Ingress control mode	Disabled
Traffic Control, Storm Control, Interfaces	
Status	Disabled
Threshold	5
Control action	None
Traffic Control, Port Security, Global	
Port security mode	Disabled
Traffic Control, Port Security, Interface	
Port security	Disabled
Maximum learned MAC addresses	4096
Maximum static MAC addresses	48
Enable violation shutdown	No
Enable violation traps	No
Protected Port None configured	
Private VLANs None configured All VLANs in General port VLAN mode	
ACL	
Total number of supported ACLs	100. This total number applies to all MAC ACLs, IPv4 ACLs, and IPv6 ACLs together.
MAC ACLs	None configured
IP 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.

Table 108. Monitoring features default settings

Feature	Default
Logs, Memory Log	
Admin status	Enabled
Behavior	Wrap
Severity filter	Informational
Logs, FLASH Log	
Admin status	Disabled
Severity filter	Alert
Logs to be displayed	Current logs
Logs, Server Log	
Admin status	Disabled
Local UDP port	514
Mirroring, Global	
Admin mode	False
Destination port	None
Mirroring, Interface	
Direction	None

Hardware technical specifications

The following table describes the main hardware technical specifications.

For additional hardware specifications, see the data sheet, which you can download by visiting netgear.com/support/download/.

Table 109. Hardware technical specifications

Feature	Descriptions
Network interfaces	Eight 10/100/1000BASE-T RJ-45 PoE+ copper ports
	Two dedicated 100/1000BASE-X fiber SFP ports
PoE+ power budget	190W
Maximum power consumption	225W with PoE 12.5W without PoE
Dimensions (W x D x H)	12.9 x 6.7 x 1.7 in. (328 x 169 x 43 mm
Weight	4.03 lb (1.83 kg)
Operating temperature	32º to 122ºF (0° to 50°C)
Operating humidity	90% maximum relative humidity, noncondensing
Maximum operating altitude	10,000 ft (3,000 m)
Storage temperature	–4° to 158°F (–20º to 70ºC)
Storage humidity	95% maximum relative humidity, noncondensing
Maximum storage altitude	10,000 ft (3,000 m)
Electromagnetic certifications and compliance	CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014, Class A, EN 61000-3-3:2013, EN 55024:2010
	VCCI: VCCI-CISPR 32:2016, Class A
	RCM: AS/NZS CISPR 32:2013 Class A
	CCC: GB4943.1-2011; YD/T993-1998; GB/T9254-2008 (Class A)
	FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014
	ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014
	BSMI: CNS 13438 Class A

Table 109. Hardware technical specifications (continued)

Feature	Descriptions
Safety certifications	CB report / certificate IEC 60950-1:2005 (ed.2) + A1:2009 + A2:2013
	UL listed (UL 1950)/cUL IEC 950/EN 60950
	CE LVD: EN 60950-1: 2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013
	RCM (AS/NZS) 60950.1:2015
	CCC (China Compulsory Certificate): GB4943.1-2011; YD/T993-1998; GB/T9254-2008 (Class A)
	BSMI: CNS 14336-1