24-Port Gigabit (Hi-Power) PoE+ Ethernet Smart Managed Pro Switch with 2 SFP Ports and Cloud Management

GS724TPv2
GS724TPP
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.

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

<table>
<thead>
<tr>
<th>Publication Part Number</th>
<th>Publish Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>202-12036-03</td>
<td>May 2021</td>
<td>We changed Chapter 1, Get Started to document the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The new device UI login options for initial access to the device UI. (HTTP rather than HTTPS is now the default protocol for access to the device UI.) See Access the switch on-network and connected to the Internet, Access the switch off-network and not connected to the Internet, and Credentials for the device UI.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The new options to register the switch to activate your warranty. See Register the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The new requirements to change the management mode. See Change the management mode of the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We changed the login steps in all tasks in the manual to document the new device UI login options.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We changed the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure the time settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure Green Ethernet settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure SNMPv1 and SNMPv2 trap flags</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure LLDP-MED port settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure DHCP snooping interface settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Set up PoE timer schedules</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Manage the Smart Control Center</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure HTTP access settings</td>
</tr>
</tbody>
</table>
We added the following sections:

- Manage switch discovery with UPnP and SSDP
- Browser security warning with HTTPS access
- We made multiple minor changes, including changes in terminology.

We changed Reboot the switch.

We changed Reset the switch to its factory default settings and added the following sections:

- Reset the switch to factory default settings but maintain the registration status
- Reset the switch to factory default settings and reset the registration status

We made the following major changes:

- We added support for model GS724TPP.
- We changed the login procedures for all tasks. After you register and access the switch with your NETGEAR account, you can access the switch with the device admin password.

The switch now supports management through the NETGEAR Insight app and Insight Cloud portal.

We reorganized the information in Chapter 1, Get Started and added or revised the following sections:

- Available publications
- Switch management options and default management mode
- About on-network and off-network access
- Access the switch on-network and connected to the Internet
- Access the switch off-network and not connected to the Internet
- Credentials for the device UI
- Register the switch
- Change the language of the device UI
- Change the management mode of the switch

In other chapters, we added the following sections:

- PoE concepts
- Device class power requirements
- Power allocation and power budget concepts
- Hardware technical specifications

Throughout the manual, we did the following:

- We added or revised many standard sections.
- We made many other minor changes and improvements.

We published the manual in a new format.
202-11765-02  May 2018  We made the following major changes:
• Added the DHCPv6 option to Configure the IPv6 network interface on page 57
• Added Configure Layer 2 loop protection on page 199
• Added Configure DiffServ IPv6 class settings on page 223
• Revised Manage port authentication on individual ports on page 277
• Added View the client summary on page 284
• Revised Use the ACL Wizard to create a simple ACL on page 299
• Added Configure an IPv6 ACL on page 331
• Added Configure rules for an IPv6 ACL on page 334
In addition we made multiple minor changes.

202-11765-01  June 2017  First publication
Chapter 1 Get Started

Available publications .......................................................... 13
Switch management options and default management mode ........ 14
Manage the switch by using the device UI ......................... 15
  Software requirements to use the device UI ................. 15
  Supported web browsers .................................................. 15
  Navigation tabs, configuration menus, and page menu .......... 16
  Configuration and status options ................................. 17
  Buttons in the device UI ................................................. 17
  User-defined fields ...................................................... 18
  Context-sensitive help .................................................... 18
About on-network and off-network access ................................ 18
Access the switch on-network and connected to the Internet .... 19
  Use a Windows-based computer to access the switch on-network and connected to the Internet .................. 20
  Use the NETGEAR Insight mobile app to discover the IP address of the switch ........................................ 21
  Use the NETGEAR Switch Discovery Tool to discover the switch when it is connected to the Internet .............. 22
  Discover the switch in a network with a DHCP server using the Smart Control Center .......................... 24
  Use other options to discover the switch IP address .......... 25
  Access the switch on-network and connected to the Internet when you know the switch IP address ................. 25
Access the switch off-network and not connected to the Internet .. 27
Credentials for the device UI ............................................... 28
Register the switch ...................................................... 30
  Register the switch with your NETGEAR account and access the switch online ........................................ 30
  Register the switch with your NETGEAR account and get a registration key for offline access ....................... 31
  Access the switch offline with a registration key ............. 32
Change the language of the device UI ............................... 34
Change the management mode of the switch ....................... 35
  About changing the management mode ......................... 35
  Change the management mode to NETGEAR Insight Mobile App and Insight Cloud Portal .................. 36
  Change the management mode back to Directly Connect to Web Browser Interface ................................ 37
Use the Device View of the device UI .................................. 40
Configure interface settings ............................................... 44
Chapter 2 Configure System Information

View or define switch system information ........................................ 51
View or define system information .............................................. 51
View the fan status ................................................................. 53
View the software versions ......................................................... 54
Configure the switch IP address settings ...................................... 55
Configure the IPv6 network interface .......................................... 57
View the IPv6 network neighbors ............................................... 58
Configure the time settings ......................................................... 60
Configure the time settings manually ........................................... 60
Configure the time settings with SNTP ........................................ 62
View the SNTP global status ...................................................... 65
Configure an SNTP server ......................................................... 67
Configure daylight saving time settings ....................................... 72
View the daylight saving time status ............................................ 75
Configure Denial of Service settings ............................................. 76
Configure Auto-DoS ................................................................. 76
Configure Denial of Service ....................................................... 77
Configure the DNS settings ....................................................... 79
Configure the global DNS settings .............................................. 79
Configure and view host name-to-IP address information .............. 81
Configure Green Ethernet settings .............................................. 84
Configure the Green Ethernet global settings ............................ 84
Configure the Green Ethernet interface settings ......................... 85
Manage switch discovery with UPnP and SSDP .......................... 87
Use the Device View ............................................................... 88
Configure Power over Ethernet .................................................. 88
PoE concepts ........................................................................ 88
Device class power requirements .............................................. 89
Power allocation and power budget concepts ............................. 89
Configure PoE trap settings and view PoE information ............... 91
Configure the PoE port settings .................................................. 92
Configure SNMP ................................................................. 95
Configure the SNMPv1 and SNMPv2 community ....................... 95
Configure SNMPv1 and SNMPv2 trap settings ......................... 98
Configure SNMPv1 and SNMPv2 trap flags ............................. 101
View the supported MIBs ......................................................... 103
Configure SNMPv3 users ......................................................... 103
Configure LLDP ................................................................. 105
Configure LLDP global settings ............................................... 105
Configure LLDP port settings ................................................. 107
View LLDP-MED network policy information ........................... 108
Configure LLDP-MED port settings .......................................... 110
View local LLDP information ................................................... 111
View LLDP neighbors information .............................................. 114
Configure DHCP snooping ..................................................... 117
Configure the global DHCP snooping settings ......................... 118
Enable DHCP for all interfaces in a VLAN ......................... 119
Configure DHCP snooping interface settings ...................... 120
Configure static DHCP bindings ........................................... 121
Set up PoE timer schedules ................................................. 123
Create a PoE timer schedule .............................................. 123
Specify the settings for an absolute PoE timer schedule ........ 124
Specify the settings for a recurring PoE timer schedule ........ 126
Change the settings for a recurring PoE timer schedule entry 128
Delete a PoE timer schedule entry .................................. 129
Delete a PoE timer schedule ............................................. 130

Chapter 3 Configure Switching

Configure the port settings and maximum frame size .............. 132
Configure link aggregation groups ..................................... 135
Configure LAG settings .................................................. 135
Configure LAG membership .................................................. 137
Set the LACP system priority ........................................... 138
Set the LACP port priority settings .................................. 139
Configure VLANs .......................................................... 141
Configure VLAN settings ................................................. 141
Configure VLAN membership .......................................... 145
View the VLAN status ...................................................... 147
Configure the port PVID settings ...................................... 148
Configure a voice VLAN .................................................. 150
Configure Auto-VoIP ....................................................... 152
Configure the Auto-VoIP protocol-based settings ................ 152
Configure the Auto-VoIP OUI-based properties .................. 154
Configure the OUI-based port settings ............................... 155
Manage the OUI table ..................................................... 157
Display the Auto-VoIP status ........................................... 159
Configure Spanning Tree Protocol .................................... 160
Configure the STP settings and view the STP status ............ 161
Configure the CST settings ............................................... 163
Configure the CST port settings ....................................... 165
View the CST port status ................................................ 167
View the Rapid STP information ...................................... 169
Manage the MST settings ............................................... 170
Configure and view the port settings for an MST instance .... 173
View the STP statistics .................................................. 176
Configure multicast ......................................................... 177
View, search, or clear the MFDB table ............................... 177
View the MFDB statistics ............................................... 179
Manage IGMP snooping .................................................. 180
Configure IGMP snooping ................................................ 180
Configure IGMP snooping for interfaces ............................ 182
View, search, or clear the IGMP snooping table .................. 184
Configure IGMP snooping for VLANs .......................... 185
Modify IGMP snooping settings for a VLAN .................. 187
Disable IGMP snooping on a VLAN ............................ 187
Configure one or more IGMP multicast router interfaces .... 188
Configure an IGMP multicast router VLAN .................... 190
IGMP snooping querier overview .............................. 191
Configure an IGMP snooping querier ......................... 191
Configure an IGMP snooping querier for a VLAN ............ 192
Display the status of the IGMP snooping querier for VLANs .. 193
View, search, and manage the MAC address table .......... 195
View, search, or clear the MAC address table ............... 195
Set the dynamic address aging interval ..................... 197
Add a static MAC address to the MAC address table ...... 198
Configure Layer 2 loop protection ............................ 199
Configure global Layer 2 loop protection .................... 200
View and configure Layer 2 loop protection on a port ...... 201
Chapter 4Configure Quality of Service
Quality of Service concepts ........................................ 205
Manage Class of Service .......................................... 205
CoS configuration concepts ....................................... 205
Configure the global CoS settings .............................. 206
Configure the CoS settings for an interface .................. 207
Configure the CoS queue settings for an interface ........ 209
Map 802.1p priorities to queues ............................... 211
Map DSCP values to queues ..................................... 212
Manage Differentiated Services ................................. 214
Defining DiffServ .................................................. 214
Configure the DiffServ mode and display the entries in the DiffServ private MIB tables ......................... 215
Configure a DiffServ class ....................................... 216
Configure DiffServ IPv6 class settings ....................... 223
Configure a DiffServ policy ..................................... 228
Configure the DiffServ service interface .................... 234
View DiffServ service statistics ............................... 237
Chapter 5 Manage Device Security
Change the device admin password for the device UI ........ 240
Manage the RADIUS settings .................................... 241
Configure the global RADIUS server settings ............... 241
Configure a RADIUS authentication server on the switch . 243
Configure a RADIUS accounting server ..................... 247
Configure the TACACS+ settings ............................... 251
Configure a TACACS+ server on the switch ................ 252
Modify the settings for a TACACS+ server on the switch ... 253
Remove a TACACS+ server from the switch ........................................ 254
Configure authentication lists ....................................................... 255
Configure the dot1x authentication list ......................................... 258
Manage the Smart Control Center ..................................................259
Configure management access ....................................................... 260
Configure HTTP access settings .................................................... 260
Configure HTTPS access settings ................................................... 262
Browser security warning with HTTPS access ............................... 263
Manage certificates for HTTPS access ............................................ 264
Control access with profiles and rules .......................................... 268
Add an access profile ............................................................... 268
Add a rule to the access profile .................................................... 270
Activate the access profile .......................................................... 271
Display the access profile summary and the number of filtered packets ........................................................................ 272
Deactivate an access profile ......................................................... 274
Remove an access profile ............................................................. 274
Configure port authentication ......................................................... 275
Configure the global 802.1X settings .............................................. 276
Manage port authentication on individual ports ............................. 277
View the port summary ............................................................... 282
View the client summary ............................................................ 284
Set up traffic control ..................................................................... 285
Manage MAC filtering ................................................................... 285
Configure storm control settings .................................................... 289
Configure port security ............................................................... 293
Configure protected ports ............................................................ 297
Configure access control lists ......................................................... 298
Use the ACL Wizard to create a simple ACL ................................. 299
Configure a MAC ACL ................................................................. 305
 Configure MAC ACL rules ............................................................. 308
Configure MAC bindings ............................................................. 312
View or delete MAC ACL bindings in the MAC binding table ....... 314
Configure a basic or extended IPv4 ACL ........................................ 315
Configure rules for a basic IPv4 ACL ............................................. 319
Configure rules for an extended IPv4 ACL ..................................... 323
Configure an IPv6 ACL ............................................................... 331
Configure rules for an IPv6 ACL .................................................... 334
Configure IP ACL interface bindings ............................................. 341
View or delete IP ACL bindings in the IP ACL binding table ........ 343
Configure VLAN ACL bindings .................................................... 344

Chapter 6  Monitor the System

Monitor the switch and the ports ................................................... 348
View or clear switch statistics ....................................................... 348
View port statistics ................................................................. 351
View and manage detailed port statistic ........................................ 354
View or clear EAP and EAPoL statistics ....................................... 360
Chapter 7 Maintain or Troubleshoot the Switch

Perform a cable test ............................................. 362
Configure and view the logs .................................... 364
Manage and view the memory log .............................. 364
Manage and view the flash log ................................. 366
Manage the server log ........................................... 367
View or clear the trap logs and the counter .................. 371
Configure port mirroring ....................................... 372

Reboot the switch ............................................... 376
Reset the switch to its factory default settings ............... 377
Reset the switch to factory default settings but maintain the
registration status .............................................. 377
Reset the switch to factory default settings and reset the
registration status .............................................. 378
Export a file from the switch ................................... 380
Use TFTP to export a file from the switch to a TFTP server .. 380
Use HTTP to export a file from the switch to a computer .... 382
Download a file to the switch or update the software ....... 383
Use TFTP to download a file to the switch or update the
software image .................................................. 383
Use HTTP to download a file to the switch or update the
software image .................................................. 386
Use an HTTP session to download and install an SSL
security certificate file on the switch ......................... 388
Manage software images ....................................... 389
Copy a software image ......................................... 390
Configure dual image settings ................................ 391
View the dual image status ..................................... 393
Perform diagnostics and troubleshooting ...................... 394
Ping an IPv4 Address .......................................... 394
Ping an IPv6 address .......................................... 395
Send an IPv4 traceroute ....................................... 397
Send an IPv6 traceroute ....................................... 400
Enable remote diagnostics .................................... 402

Appendix A Configuration Examples

Virtual Local Area Networks (VLANs) .......................... 404
VLAN configuration examples ................................. 405
Access control lists (ACLs) .................................... 406
MAC ACL example configuration .............................. 406
Basic IPv4 ACL example configuration ....................... 407
Differentiated Services (DiffServ) .............................. 408
Class .............................................................. 409
DiffServ traffic classes ........................................ 410
Creating policies ................................................ 410
DiffServ example configuration ............................... 411
# Appendix B Specifications and Default Settings

- **802.1X access control** .................................................. 413
- **802.1X example configuration** .................................. 414
- **Multiple Spanning Tree Protocol** ................................. 415
- **MSTP example configuration** ..................................... 417

## Switch default settings .................................................. 421
## General feature default settings ................................. 422
## System setup and maintenance settings .................. 428
## Port characteristics ................................................... 428
## Traffic control settings ............................................. 429
## Quality of Service Settings ....................................... 429
## Security settings ...................................................... 430
## System management settings .................................... 430
## Settings for other features ....................................... 431
## Hardware technical specifications ............................... 431
  - Model GS724TPv2 hardware technical specifications  ......... 432
  - Model GS724TPP hardware technical specifications .......... 433
Get Started

This user manual describes how you can use the device user interface (UI) to configure and operate the following NETGEAR Smart Managed Pro switches:

- **GS724TPv2.** NETGEAR 24-Port Gigabit PoE+ Ethernet Smart Managed Pro Switch with 2 SFP Ports and Cloud Management. This model provides a PoE power budget of 190W.
- **GS724TPP.** NETGEAR 24-Port Gigabit Hi-Power PoE+ Ethernet Smart Managed Pro Switch with 2 SFP Ports and Cloud Management. This model provides a PoE power budget of 380W.

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

This chapter contains the following sections:

- Available publications
- Switch management options and default management mode
- Manage the switch by using the device UI
- About on-network and off-network access
- Access the switch on-network and connected to the Internet
- Access the switch off-network and not connected to the Internet
- 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 both 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 app and Insight Cloud portal, 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 app on a smartphone or tablet or from the Insight Cloud portal that is available from a web browser on your Windows-based computer, Mac, 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.

- **NETGEAR Insight app and Insight Cloud portal.** 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:
  - **NETGEAR Insight app.** As an Insight Premium or Insight Pro subscriber, you can use the NETGEAR Insight app to discover the switch on the network and add the switch to a NETGEAR Insight network location. You can then set up the switch in the network and manage and monitor the switch remotely from your smartphone or tablet. You can choose from four methods to add the switch to the NETGEAR Insight app: You can scan your network for the switch, scan the QR code or the barcode of the switch, or add the serial number of the switch. A free trial is available for new customers.
  - **Insight Cloud portal.** As an Insight Premium or Insight Pro subscriber, you can use the NETGEAR Insight Cloud portal to set up the switch in the network, perform advanced remote setup, configuration, and management, monitor the switch, analyze the switch and network usage, and, if necessary, troubleshoot the switch and the network. A free trial is available for new customers.

For more information about NETGEAR Insight, visit [netgear.com/insight](http://netgear.com/insight) and [netgear.com/support/product/Insight.aspx](http://netgear.com/support/product/Insight.aspx). For knowledge base articles about NETGEAR Insight, visit [netgear.com/support](http://netgear.com/support).

To use the NETGEAR Insight app or Insight Cloud portal methods, you must change the management method to NETGEAR Insight Mobile App and Insight Cloud Portal. After you do so, you can also change the management 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 35](#).
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 using the NETGEAR Insight app and Insight Cloud portal to manage the switch, visit netgear.com/insight and netgear.com/support/product/Insight.aspx. For knowledge base articles about NETGEAR Insight, visit netgear.com/support.

Software requirements to use the device UI

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

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

Supported web browsers

The following browsers were tested and support the device UI. If later browser versions are not stated, it means that they were not tested but might function fine. The supported web browsers include the following:

- Microsoft Internet Explorer (IE) version 10 and later versions
- Mozilla Firefox version 35 and later versions
- Chrome version 33 and later versions
- Safari (on MAC OS) version 10 and later versions
Navigation tabs, configuration menus, and page menu

The following figure shows the System Information page for model GS724TPP.

![System Information Page](image)

**Figure 1. Switch navigation tabs, configuration menus, and page menu**

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

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

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

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

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

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>
<thead>
<tr>
<th>Button</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Clicking the Add button adds the new item configured in the heading row of a table.</td>
</tr>
<tr>
<td>Apply</td>
<td>Clicking the Apply button sends the updated configuration to the switch. Your settings are saved and configuration changes take effect immediately.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Clicking the Cancel button cancels the configuration on the page and resets the data on the page to the previous values of the switch.</td>
</tr>
<tr>
<td>Clear</td>
<td>Clicking the Clear button clears all the counters and resets the switch summary and detailed statistics to default values.</td>
</tr>
<tr>
<td>Delete</td>
<td>Clicking the Delete button removes the selected item.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Clicking the Refresh button refreshes the page with the latest information from the device.</td>
</tr>
<tr>
<td>Logout</td>
<td>Clicking the Logout button ends the session.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Invalid characters for user-defined fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
</tr>
</tbody>
</table>

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 or online.
  
  For more information, see **Access the switch on-network and connected to the Internet on page 19).**

- **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 27.**

---

**Note:** We recommend that you register the switch to activate your warranty.

For more information, see **Register the switch on page 30.**
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 of the switch and register the switch with NETGEAR. For more information, see Use a Windows-based computer to access the switch on-network and connected to the Internet on page 20.

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 app.** You can install the NETGEAR Insight app on an iOS or Android mobile device and discover the IP address of the switch. See Use the NETGEAR Insight mobile app to discover the IP address of the switch on page 21.
- **NETGEAR Switch Discovery Tool (NSDT):** If you use a Mac or a Windows-based computer, you can use the NSDT to discover the switch on your network. See Use the NETGEAR Switch Discovery Tool to discover the switch when it is connected to the Internet on page 22.
- **NETGEAR Smart Control Center (SCC):** You can install the SCC on a Windows-based computer. See Discover the switch in a network with a DHCP server using the Smart Control Center on page 24.
- **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 25.

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 and connected to the Internet when you know the switch IP address on page 25.
- **NETGEAR Smart Control Center (SCC):** For configuration of a limited number of switch features, use the SCC on a Windows-based computer. By default, you can use the SCC to discover the IP address of the switch, but you cannot use the SCC to perform any actions on the switch. However, if you enable the configuration option of the SCC, you can use it to configure the switch. See Manage the Smart Control Center on page 259.

For more information about the SCC, visit netgear.com/support/product/SCC.

- **NETGEAR Insight app and Insight Cloud portal.** You can change the management mode of the switch so that you can use the NETGEAR Insight app and Insight Cloud portal to manage the switch remotely. For more information, see Change the management mode of the switch on page 35.
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.
8. Double-click GSmodel-XXXXXX, in which GSmodel represents the model number of the switch and XXXXX represents the last six digits of the switch MAC address.
   The page that displays depends on whether your browser is connected to the Internet, whether the switch is connected to the Internet, and whether you activated the warranty.
9. Enter your credentials, which depend on the page that displays:
   • **Register to activate your warranty page displays**: If you did not yet activate your warranty, the Register to activate your warranty page displays.
     - **Register Your Device**: To activate your warranty, click the Register Your Device button, and follow the directions onscreen to register the switch with your email address and password. After you activate your warranty, you are no longer prompted to register the switch.

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

     - **Enter Registration Key**: If you obtained a registration key, enter it. For more information, see Register the switch with your NETGEAR account and get a registration key for offline access on page 31.

     - **Skip Registration & Access the UI**: You do not need to register the switch to activate your warranty, but if you do not activate your warranty within 30 days of purchase, your warranty entitlement might be affected.

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

   • **Device UI login page displays**: If you previously registered the switch with NETGEAR to activate your warranty, the Device UI login page displays. Enter one of the following credentials:
- **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 28](#).

10. Click the Go button.

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

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

### Use the NETGEAR Insight mobile 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 app or the Insight Cloud Portal 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 36](#)). 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 mobile device, go to the app store, search for NETGEAR Insight, and download the latest version of 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 mobile 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 switch IP address.
   You can use this IP address to access the switch directly from a web browser. For information about how to access the device UI of the switch, see Access the switch on-network and connected to the Internet when you know the switch IP address on page 25.

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

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


   Depending on the computer that you are using, download either the Mac version or the version for a Windows-based computer.

2. Temporarily disable the firewall, Internet security, antivirus programs, or all of these on the computer that you use to configure the switch.
3. Unzip the NSDT files, and click or double-click the .exe file (for example, NSDT-1.2.102.exe) to install the program on your computer.

You might see the tool icon appear on your Mac dock or Windows desktop.

4. Reenable the security services on your computer.

5. Power on the switch.

The DHCP server assigns the switch an IP address.

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

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

7. Open the Switch Discovery Tool.

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

The initial page displays a menu and a button.

8. From the Choose a connection menu, select the network for this switch.

9. Click the Start Searching button.

The NSDT displays the IP addresses of the switches that it discovers.

10. To access the switch from the NSDT, do the following:

a. Click the ADMIN PAGE button next to your switch.

The page that displays depends on whether you activated the warranty.

b. Enter your credentials, which depend on the page that displays:

   • Register to activate your warranty page displays: If you did not yet activate your warranty, the Register to activate your warranty page displays.

      - Register Your Device: To activate your warranty, click the Register Your Device button, and follow the directions onscreen to register the switch with your email address and password. After you activate your warranty, you are no longer prompted to register the switch.

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

      - Enter Registration Key: If you obtained a registration key, enter it. For more information, see Register the switch with your NETGEAR account and get a registration key for offline access on page 31.

      - Skip Registration & Access the UI: You do not need to register the switch to activate your warranty, but if you do not activate your warranty within 30 days of purchase, your warranty entitlement might be affected.

      If you do not activate your warranty, the Register to activate your warranty page continues to display when you log in.
• **Device UI login page displays**: If you previously registered the switch with NETGEAR to activate your warranty, the Device UI login page displays. Enter one of the following credentials:
  - **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.
  - **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 28.

  c. If you enter a password, click the **Go** button; If you enter a registration key, click the **Submit** button.
  d. If the Change Default Password page displays, specify and confirm a new device admin password, click the **Submit** button, and log in again with your new password.

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

**Discover the switch in a network with a DHCP server using the Smart Control Center**

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

For information about the SCC, visit https://www.netgear.com/support/product/SCC.

---

**Note**: By default, you can use the SCC to discover the IP address of the switch, but you cannot use the SCC to perform any actions on the switch. However, if you enable the configuration option of the SCC, you can use it to configure the switch (see Manage the Smart Control Center on page 259).

---

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

1. Connect the switch to a network with a DHCP server.
2. Power on the switch by connecting its power cord.
3. Install the SCC on your computer.
4. Start the SCC.
5. Click the **Discover** button for the SCC to discover all the devices in the subnet.
6. Write down the switch IP address assigned by the DHCP server.

For information about how to access the device UI of the switch, see Access the switch on-network and connected to the Internet when you know the switch IP address on page 25.

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).

• **Use an 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 and connected to the Internet when you know the switch IP address on page 25.

Access the switch on-network and connected to the Internet 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 and connected to the Internet when you know the switch IP address:

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

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

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

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

     - **Enter Registration Key**: If you obtained a registration key, enter it. For more information, see Register the switch with your NETGEAR account and get a registration key for offline access on page 31.

     - **Skip Registration & Access the UI**: You do not need to register the switch to activate your warranty, but if you do not activate your warranty within 30 days of purchase, your warranty entitlement might be affected.

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

   - **Device UI login page displays**: If you previously registered the switch with NETGEAR to activate your warranty, the Device UI login page displays. Enter one of the following credentials:

     - **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 28.

4. Click the Go button.

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

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

   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.

**Note:** If you prefer to use the Smart Control Center (SCC) to configure the switch, you must access the switch off-network as described in the following procedure and then enable the configuration option of the SCC (see Manage the Smart Control Center on page 259).

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:

   • **Mac.** See the following article:
     https://kb.netgear.com/000037250/Setting-a-static-IP-address-on-your-network-a
dapter-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](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 Enter Registration Key page displays.

6. Do one of the following:
   • **Enter a registration key.** If you obtained a registration key, do the following:
     a. Type or paste the key.
For more information, see Register the switch with your NETGEAR account and get a registration key for offline access on page 31.

b. Click the Submit button.

• **Do not register at this time and access the device UI:** Do the following:
  
a. Click the **Skip Registration & Access the UI** button.
  
The Device UI login page displays.

b. Enter one of the following credentials:

- **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.

- **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 28**.

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

   The 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 Insight app and Cloud portal.

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

- **NETGEAR account credentials:**

  You can register the switch online to activate your warranty by entering your NETGEAR account credentials (see Register the switch with your NETGEAR account and access the switch online on page 30). If you do not have a NETGEAR account, you can create one.
Alternatively, you can obtain a registration key and enter the key when the switch is offline so that you are no longer prompted to activate your warranty (see Register the switch with your NETGEAR account and get a registration key for offline access on page 31).

- **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 app and Insight Cloud portal to manage the switch remotely (see Change the management mode of the switch on page 35), 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>
<thead>
<tr>
<th>Management mode in the device UI</th>
<th>Added to an Insight network</th>
<th>Credentials</th>
<th>Device UI menu</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default mode: Direct Connect Web Browser Interface (Local LAN Only)</td>
<td>No</td>
<td>Device admin password</td>
<td>Full device UI menu</td>
</tr>
<tr>
<td></td>
<td>Yes¹</td>
<td>Insight network password</td>
<td></td>
</tr>
<tr>
<td>NETGEAR Insight Mobile App and Insight Cloud Portal (Cloud/Remote)</td>
<td>No</td>
<td>Device admin password</td>
<td>Limited device UI menu. Managed through NETGEAR Insight.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Insight network password</td>
<td>Limited device UI menu. Not managed through NETGEAR Insight.</td>
</tr>
</tbody>
</table>

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

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

- **Online registration for on-network access:** If your switch is on-network or connected to the Internet, you can register the switch with your NETGEAR account credentials and activate your warranty. During the registration process, the switch contacts a NETGEAR server. For more information, see Register the switch with your NETGEAR account and access the switch online on page 30.

- **Registration for off-network access:** You can register your switch from any device that is connected to the Internet and get a registration key. If the switch is off-network or not connected to the Internet, you can enter the registration key. After you do so, the Register to activate your warranty page no longer displays when you log in. For more information, see Register the switch with your NETGEAR account and get a registration key for offline access on page 31.

Register the switch with your NETGEAR account and access the switch online

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

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

**To register and access the switch online over the device UI with your NETGEAR account:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   For information about finding the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   
   The Register to activate your warranty page displays.

4. Click the **Register Your Device** button and follow the directions onscreen to register the switch with your email address and password and activate the warranty.

   You are only prompted to do this once to confirm registration of your switch.
If you did not yet create a NETGEAR account, click the **Create account** link, follow the directions onscreen to create an account, and register the switch with your email address and password.

For information about the credentials, see **Credentials for the device UI on page 28**.

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

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

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

---

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

---

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

You can visit [mynetgear.com](http://mynetgear.com), log in to your NETGEAR account, register the switch using its serial number, and get a registration key.

You can also use the NETGEAR Insight app to get a registration key. NETGEAR Insight Premium or Pro subscribers can use the Insight Cloud Portal to get a registration key. For information about how the registration key functions with Insight, visit [netgear.com/support/product/Insight.aspx](http://netgear.com/support/product/Insight.aspx). For knowledge base articles about NETGEAR Insight, visit [netgear.com/support](http://netgear.com/support).

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

1. From a computer or mobile device that is connected to the Internet, go to [mynetgear.com](http://mynetgear.com).

2. Log in to your NETGEAR account.
   
   If you do not have a free NETGEAR account, you can create one.

3. From the menu on the left, select **Register a Product**.
   
   The page adjusts.

4. In the **Serial Number** field, enter the serial number of the switch.
   
   The serial number consists of 13 digits. The serial number is usually printed on a label on the bottom or the back panel of the switch.

5. Click the **Register** button.
The switch is registered with NETGEAR.

6. If the My Products page does not display, select My Products from the menu. The page adjusts.

7. Select the radio button for the newly registered switch, and click the Get Registration Key button.

The registration key is displayed, and an email with the registration key is sent to your NETGEAR account email address.

Access the switch offline with a registration key

After you get a registration key, you can access the switch offline and enter the registration key. For more information, see one of the following sections:

- Access the switch offline and enter the registration key before you log in on page 32
- Access the switch offline and enter the registration key after you log in on page 33

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

Access the switch offline and enter the registration key before you log in

If you obtain a registration key, you can access the switch offline and enter the key before you log in to the device UI.

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

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

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

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

   - Windows-based computer: See the following article: 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 Enter Registration Key page displays.
6. Enter the registration key.
7. Click the Submit button.
   The registration takes effect on the switch and you are no longer prompted to activate your warranty when you log in.
   The Device UI login page displays.
8. Enter one of the following credentials:
   • **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.
   • **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.)
9. Click the Go button.
10. If the Change Default Password page displays, specify and confirm a new device admin password, click the Submit button, and log in again with your new password.
   The System Information page displays. You can now configure the switch.
11. 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.

Access the switch offline and enter the registration key after you log in
If you access the switch offline and obtain a registration key afterwards, you can enter the key on a page in the device UI.

**To access the switch offline and enter the registration key after you log in to the device UI:**
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

The Register to activate your warranty page displays.

4. Click the Skip Registration & Access the UI button.
   The Device UI login page displays.

5. Enter one of the following credentials:
   - 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.
   - 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.)

6. Click the Go button.

7. If the Change Default Password page displays, specify and confirm a new device admin password, click the Submit button, and log in again with your new password.
   The System Information page displays. You can now configure the switch.

8. Select Maintenance > Registration Key.
   The Registration Key page displays.

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

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

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 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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.

8. 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 app or the Insight Cloud portal.
  • If you previously added the switch to a network location on the Insight app or Insight Cloud portal, 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 app or the Insight Cloud portal, 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.

- **Changing back to Directly Connect to Web Browser Interface mode.**

  After you change the management mode, back up your configuration. Then, reset the switch to factory defaults. Finally, restore your configuration and reboot the switch. For more information, see [Change the management mode back to Directly Connect to Web Browser Interface on page 37](#).

  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 not 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**

1. **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 19](#) or [Access the switch off-network and not connected to the Internet on page 27](#).

      The Device UI login page displays.

      If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see [Register the switch on page 30](#).

   4. Enter one of the following passwords:

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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 app or Insight Cloud portal, 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 mobile app or Insight Cloud portal.

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.

Change the management mode back to Directly Connect to Web Browser Interface

To 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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go 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 380.
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 **Reset configuration to factory default (EXCEPT registered device status), and clear device logs** radio button.
       This option resets the switch to its factory default settings but does not change its registration status with NETGEAR.
   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 19 or **Access the switch off-network and not connected to the Internet** on page 27.

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 383.

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 19** or **Access the switch off-network and not connected to the Internet on page 27**.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see **Register the switch on page 30**.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.

6. Select **System > Device View**.

The following table describes the system LEDs in the Device View.

<table>
<thead>
<tr>
<th>System LED</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power LED</td>
<td>Solid green</td>
<td>Power is supplied to the switch and the switch is operating normally.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The physical Power LED on the switch can also light solid amber. Solid amber does not apply to the Device View. (If the switch is off or booting, you cannot access the Device View.)</td>
</tr>
<tr>
<td>Fan LED</td>
<td>Off</td>
<td>The internal fan is operating normally</td>
</tr>
<tr>
<td></td>
<td>Solid yellow</td>
<td>The internal fan failed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> In this situation, the physical Fan LED on the switch lights solid amber rather than yellow.</td>
</tr>
<tr>
<td>PoE Max LED</td>
<td>Off</td>
<td>Sufficient (more than 7W of) PoE power is available on the switch</td>
</tr>
<tr>
<td></td>
<td>Solid yellow</td>
<td>Less than 7W of PoE power is available on the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> In this situation, the physical PoE Max LED on the switch lights solid amber rather than yellow.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
</tbody>
</table>

For each Ethernet port and for the two SFP fiber ports in the Device view, colors indicate the link status of the port. In addition, each Ethernet port also provides two port LEDs, which are located on the left. For each port, an upper port LED indicates the port speed status and a lower port LED indicates the port PoE status.
The following table describes the ports and port LEDs in the Device View.

<table>
<thead>
<tr>
<th>Port or port LED</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet port</td>
<td>Black</td>
<td>No Ethernet link is established.</td>
</tr>
<tr>
<td></td>
<td>Solid green</td>
<td>An Ethernet link is established.</td>
</tr>
<tr>
<td></td>
<td>Solid red</td>
<td>An error occurred on the port or the port is administratively disabled.</td>
</tr>
<tr>
<td>Upper Ethernet port LED</td>
<td>Solid dark green</td>
<td>No Ethernet link is established.</td>
</tr>
<tr>
<td></td>
<td>Solid green</td>
<td>A 1000 Mbps Ethernet link is established.</td>
</tr>
<tr>
<td></td>
<td>Blinking green</td>
<td>The port is transmitting or receiving packets at 1000 Mbps.</td>
</tr>
<tr>
<td></td>
<td>Solid yellow</td>
<td>A 10 Mbps or 100 Mbps Ethernet link is established.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: In this situation, the physical upper port LED on the switch lights solid amber rather than yellow.</td>
</tr>
<tr>
<td></td>
<td>Blinking yellow</td>
<td>The port is transmitting or receiving packets at 10 Mbps or 100 Mbps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: In this situation, the physical upper port LED on the switch blinks amber rather than yellow.</td>
</tr>
<tr>
<td>Lower Ethernet port LED</td>
<td>Solid dark green</td>
<td>The port is not delivering PoE.</td>
</tr>
<tr>
<td></td>
<td>Solid green</td>
<td>The port is delivering PoE.</td>
</tr>
<tr>
<td></td>
<td>Solid yellow</td>
<td>A PoE fault occurred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: In this situation, the physical lower port LED on the switch lights solid amber rather than yellow.</td>
</tr>
<tr>
<td>SPF fiber port</td>
<td>Black</td>
<td>No SFP module link is established.</td>
</tr>
<tr>
<td></td>
<td>Solid green</td>
<td>A 1000 Mbps link is established.</td>
</tr>
<tr>
<td></td>
<td>Blinking green</td>
<td>The SFP fiber port is transmitting or receiving packets at 1000 Mbps.</td>
</tr>
</tbody>
</table>

7. Click a port to open a menu that displays statistics and configuration options.
   You can select a menu option to access the page that contains the configuration or monitoring options.
   If you right-click the graphic, but do not right-click a specific port, the main menu displays. This menu contains the same options as the navigation tabs at the top of the page.
Right-click the specific port that you want to view or configure to see a menu that displays statistics and configuration options. Select the menu option to access the page that contains the configuration or monitoring options.
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

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

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

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

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

Use these links as follows:

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

The procedures in this section describe how to select the ports and LAGs to configure. The procedures assume that you are already logged in to the switch. If you do not know how to
log in to the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

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

1. Ensure that the page is displaying all ports, and not only the LAGs.
2. In the **Go To Interface** field, type the port number, for example g3.
   
   For more information, see Configure interface settings on page 44.
3. Click the **Go** button.

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

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

   Your settings are saved.

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

1. Click the **LAG** link or the **All** link to display the LAGs.
2. In the **Go To Interface** field, type the LAG number, for example l3.
   
   For information, see Configure interface settings on page 44.
3. Click the **Go** button.

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

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

   Your settings are saved.

To configure a single port:

1. Ensure that the page is displaying all ports, and not only the LAGs.
2. Select the check box next to the port number.
The row for the selected interface is highlighted, and the interface number appears in the heading row.

3. Configure the desired settings.
4. Click the **Apply** button.
   
   Your settings are saved.

**To configure a single LAG:**

1. Click the **LAG** link or the **All** link to display the LAGs.
2. Select the check box next to the LAG number.
   
   The row for the selected interface is highlighted, and the interface number appears in the heading row.

3. Configure the desired settings.
4. Click the **Apply** button.
   
   Your settings are saved.

**To configure multiple ports:**

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

3. Configure the desired settings.
4. Click the **Apply** button.
   
   Your settings are saved.

**To configure multiple LAGs:**

1. Click the **LAG** link or the **All** link to display the LAGs.
2. Select the check box next to each LAG to configure.
   
   The check box associated with each interface is selected, and the row for each selected interface is highlighted.
3. Configure the desired settings.
4. Click the **Apply** button.
   
   Your settings are saved.

**To configure all ports:**

1. Ensure that the page is displaying only ports, and not LAGs.
2. Select the check box in the heading row.
   
   The check box associated with every port is selected, and the rows for all ports are highlighted.

![Interface Configuration]

3. Configure the desired settings.
4. Click the **Apply** button.
   
   Your settings are saved.

**To configure all LAGs:**

1. Click the **LAG** link to display only the LAG interfaces.
2. Select the check box in the heading row.
   
   The check box associated with every LAG is selected, and the rows for all LAGs are highlighted.

3. Configure the desired settings.
4. Click the **Apply** button.
   
   Your settings are saved.

**To configure multiple ports and LAGs:**

1. Click the **All** link to display all ports and LAGs.
2. Select the check box associated with each port and LAG to configure.
The rows for the selected ports and LAGs are highlighted.

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

Your settings are saved.

To configure all ports and LAGs:
1. Click the All link to display all ports and LAGs.
2. Select the check box in the heading row.
   The check box associated with every port and LAG is selected, and the rows for all ports and LAGs are highlighted.
3. Configure the desired settings.
4. Click the Apply button.

Your settings are saved.

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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
The System Information page displays.

   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. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   The User Guide page displays.

7. To access the NETGEAR download center, click the Apply button.

8. Enter the model number of the switch.
2 Configure System Information

This chapter contains the following sections:

- View or define switch system information
- Configure the switch IP address settings
- Configure the IPv6 network interface
- Configure the time settings
- Configure Denial of Service settings
- Configure the DNS settings
- Configure Green Ethernet settings
- Use the Device View
- Configure Power over Ethernet
- Configure SNMP
- Configure LLDP
- Configure DHCP snooping
- Set up PoE timer schedules
View or define switch system information

You can view or define system information, view temperature information, view fan information, and view software information.

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Name</td>
<td>The product name of this switch.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number of the switch.</td>
</tr>
<tr>
<td>System Object OID</td>
<td>The base object ID for the switch's enterprise MIB.</td>
</tr>
<tr>
<td>Date &amp; Time</td>
<td>The current date and time.</td>
</tr>
</tbody>
</table>
View the fan status

The fans remove the heat generated by the power, CPU, and other components, and allow the switch to function normally.

Model GS724TPv2 integrates two fans. Model GS724TPP integrates three fans. You can view the fan status.

**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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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 nonconfigurable temperature and fan status information.

**Table 5. Fan status**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAN</td>
<td>The fan index used to identify the fan for the switch.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the fan temperature sensor.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies whether the fan module is fixed or removable.</td>
</tr>
<tr>
<td>Speed</td>
<td>The fan speed.</td>
</tr>
<tr>
<td>Duty level (%)</td>
<td>The duty level of the fan.</td>
</tr>
<tr>
<td>State</td>
<td>Specifies whether the fan is operational.</td>
</tr>
</tbody>
</table>

**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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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 nonconfigurable information displayed in the Versions section of the System Information page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Name</td>
<td>The model name of the switch.</td>
</tr>
<tr>
<td>Boot Version</td>
<td>The version of the bootloader software of the switch.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The version number of the code currently running on the switch.</td>
</tr>
</tbody>
</table>

**Configure the switch IP address settings**

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 configuration parameters associated with the switch’s network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

**To configure the IP address and management VLAN information 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

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

   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.

   The IP Configuration page displays.

7. Select the appropriate radio button to specify how to configure the network information for
   the switch device UI:
   - **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 is 192.168.0.239.
     Each part of the IP address must start with a number other than zero. For example, IP
     addresses 001.100.192.6 and 192.001.10.3 are not valid.
   - **Subnet Mask.** The IP subnet mask for the interface. The default is 255.255.255.0.
   - **Default Gateway.** The default gateway for the IP interface. The default is
     192.168.0.254.

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 141.

   The following requirements apply to the management VLAN:
   - Only one management VLAN can be active at a time.
When a new management VLAN is configured, connectivity through the existing management VLAN is lost.

The management station must be reconnected to the port in the new management VLAN.

10. Click the **Apply** button.
Your settings are saved.

Configure the IPv6 network interface

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

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

To access the switch over an IPv6 network, you must initially configure the switch with IPv6 information (IPv6 prefix, prefix length, and default gateway). You can configure IPv6 using any 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 interface 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** 19 or **Access the switch off-network and not connected to the Internet on page** 27.
   
   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see **Register the switch on page** 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


The IPv6 Network Global Configuration page displays.

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

8. Determine how the switch acquires an IPv6 address:
   - IPv6 Address Auto Configuration Mode. Select the Enable radio button to enable the network interface to acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of router advertisement messages. If you select the Disable radio button (which is the default selection), the network interface does not use the native IPv6 address auto-configuration features to acquire an IPv6 address. Auto-configuration functions only if DHCPv6 is not enabled on the management interface.
   - DHCPv6. Next to Current Network Configuration Protocol, select the DHCPv6 radio button to enable the DHCPv6 client on the management interface. The switch attempts to acquire network information from a DHCPv6 server. If you select the None radio button (which is the default selection), the DHCPv6 client on the network interface is disabled. If 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 device UI, do the following:
    a. In the IPv6 Address/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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


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

   Table 6. IPv6 network interface neighbor table information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 address</td>
<td>The IPv6 address of a neighbor switch visible to the network interface.</td>
</tr>
<tr>
<td>MAC address</td>
<td>The MAC address of a neighbor switch.</td>
</tr>
</tbody>
</table>
   | IsRtr   | • true (1). The neighbor machine is a router.  
   |         | • false (2). The neighbor machine is not a router. |
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 settings manually

You can view and adjust the date and time settings.

To manually configure the time setting:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

---

**Table 6. IPv6 network interface neighbor table information (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor State</td>
<td>The state of the neighboring switch:</td>
</tr>
<tr>
<td></td>
<td>• <strong>reachable</strong> (1). The neighbor is reachable by this switch.</td>
</tr>
<tr>
<td></td>
<td>• <strong>stale</strong> (2). Information about the neighbor is scheduled for deletion.</td>
</tr>
<tr>
<td></td>
<td>• <strong>delay</strong> (3). No information was received from the neighbor during the delay period.</td>
</tr>
<tr>
<td></td>
<td>• <strong>probe</strong> (4). The switch is attempting to probe for this neighbor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>unknown</strong> (5). Unknown status.</td>
</tr>
</tbody>
</table>

| Last Updated  | The last sysUpTime that this neighbor was updated.                           |
For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button. The System Information page displays.


7. Select the Clock Source Local radio button.

8. In the Date field, specify the current date by entering the month, day, and year (MM/DD/YYYY).

9. In the Time field, specify the current time by entering in hours, minutes, and seconds (HH:MM:SS).

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

10. In the Time Zone Name field, specify the acronym for a time zone. You can also specify the number of hours and number of minutes that the time zone is different from the Coordinated Universal Time (UTC). The time zone can affect the display of the current system time. The default value is UTC.

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

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

    For more information see the description for Time Zone Name in Step 10. The allowed range is –12 to 13. The default value is 0.

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

    For more information see the description for Time Zone Name in Step 10. The allowed range is 0 to 59. The default value is 0.

13. Click the Apply button. Your settings are saved.
Configure the time settings with SNTP

To configure the time by using SNTP:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   The Time Configuration page displays.

7. Select the Clock Source SNTP radio button.
The local clock can be set to SNTP only if the following two conditions are met:

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

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 67.

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clock Source</td>
<td>Local @ SNTP</td>
</tr>
<tr>
<td>Date</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>Time</td>
<td>HH:MM:SS</td>
</tr>
<tr>
<td>Time Zone Name</td>
<td></td>
</tr>
<tr>
<td>Offset Hours</td>
<td>-12 to 13</td>
</tr>
<tr>
<td>Offset Minutes</td>
<td>0 to 59</td>
</tr>
<tr>
<td>Client Mode</td>
<td>Unicast, Broadcast</td>
</tr>
<tr>
<td>Port</td>
<td>123</td>
</tr>
<tr>
<td>Unicast Poll Interval</td>
<td>6 (6 to 10)</td>
</tr>
<tr>
<td>Broadcast Poll Interval</td>
<td>6 (6 to 10)</td>
</tr>
<tr>
<td>Unicast Poll Timeout</td>
<td>5 (1 to 30)</td>
</tr>
<tr>
<td>Unicast Poll Retry</td>
<td>1 (0 to 10)</td>
</tr>
</tbody>
</table>
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 range is from 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 range is from 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 range is from 0 to 10. The default value is 1.

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

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

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

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

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

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

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

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

16. Click the **Apply** button.

   Your settings are saved.
View the SNTP global status

If you configure the time settings with SNTP, you can view information about the switch’s SNTP client and the global SNTP status.

To view information about the switch’s SNTP client and the SNTP global status:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   Make sure that the Clock Source SNTP radio button is selected.
   The SNTP Global Status section displays below the SNTP Global Configuration section.
7. Click the **Refresh** button to update the page with the latest information about the switch.

The following table displays the nonconfigurable SNTP Global Status information.

**Table 7. SNTP Global Status information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>The SNTP version that the client supports.</td>
</tr>
<tr>
<td>Supported Mode</td>
<td>The SNTP modes that the client supports. Multiple modes can be supported by a client.</td>
</tr>
<tr>
<td>Last Update Time</td>
<td>The local date and time (UTC) that the SNTP client last updated the system clock.</td>
</tr>
<tr>
<td>Last Attempt Time</td>
<td>The local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.</td>
</tr>
<tr>
<td>Last Attempt Status</td>
<td>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 <strong>Other</strong> is displayed. These values are appropriate for all operational modes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Other</strong>. The status of the last request is unknown.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Success</strong>. The SNTP operation was successful and the system time was updated.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Request Timed Out</strong>. After an SNTP request was sent to an SNTP server, the response timer expired before a response from the server was received.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bad Date Encoded</strong>. The time provided by the SNTP server is not valid.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Version Not Supported</strong>. The SNTP version supported by the server is not compatible with the version supported by the client.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Server Unsynchronized</strong>. The SNTP server is not synchronized with its peers. This is indicated by the leap indicator field in the SNTP message.</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>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.</td>
</tr>
<tr>
<td>Address Type</td>
<td>The address type of the SNTP server address for the last received valid packet.</td>
</tr>
<tr>
<td>Server Stratum</td>
<td>The claimed stratum of the server for the last received valid packet.</td>
</tr>
</tbody>
</table>
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

Table 7. SNTP Global Status information (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference Clock ID</td>
<td>The reference clock identifier of the server for the last received valid packet.</td>
</tr>
<tr>
<td>Server mode</td>
<td>The mode of the server for the last received valid packet.</td>
</tr>
<tr>
<td>Unicast Server Max Entries</td>
<td>The maximum number of unicast server entries that can be configured on this client.</td>
</tr>
<tr>
<td>Unicast Server Current Entries</td>
<td>The number of current valid unicast server entries configured for this client.</td>
</tr>
<tr>
<td>Broadcast Count</td>
<td>The number of unsolicited broadcast SNTP messages that were received and processed by the SNTP client since the last reboot.</td>
</tr>
</tbody>
</table>
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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   The SNTP Server Configuration page displays.

7. From the Server Type menu, select the type of SNTP address to enter in the address field.
   The address can be either an IP address (IPv4 or IPv6) or a host name (DNS). The default 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 is 123.

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

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

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

    The range is 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 fields in the SNTP Server Status

**Table 8. SNTP Server Status information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>All the existing server addresses. If no server configuration exists, a message stating that no SNTP server exists displays on the page.</td>
</tr>
<tr>
<td>Last Update Time</td>
<td>The local date and time (UTC) that the response from this server was used to update the system clock.</td>
</tr>
<tr>
<td>Last Attempt Time</td>
<td>The local date and time (UTC) that this SNTP server was last queried.</td>
</tr>
</tbody>
</table>
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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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. Specify new values in the available fields.

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

6. Select **System > Management > Time > Daylight Saving Configuration**.
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 that are described in the following table are visible on the page only if the DayLight Saving (DST) **Recurring**, **Recurring EU**, or **Recurring USA** radio button is selected.

### Table 9. Daylight saving setting is Recurring, Recurring EU, or Recurring USA

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Begins At</td>
<td>These fields are used to configure the start values of the date and time.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Week</strong>. Configure the start week.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Day</strong>. Configure the start day.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Month</strong>. Configure the start month.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hours</strong>. Configure the start hours.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Minutes</strong>. Configure the start minutes.</td>
</tr>
</tbody>
</table>

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

### Table 10. Daylight saving setting is Non Recurring

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Begins At</td>
<td>These fields are used to configure the start values of the date and time.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Week</strong>. Configure the start week.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Day</strong>. Configure the start day.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Month</strong>. Configure the start month.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hours</strong>. Configure the start hours.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Minutes</strong>. Configure the start minutes.</td>
</tr>
</tbody>
</table>

| 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 | 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

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

7. To refresh the page, click the **Refresh** button.
The following table displays the nonconfigurable information on the page.

Table 11. Daylight Saving (DST) Status information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daylight Saving (DST)</td>
<td>The Daylight Saving value, which is one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Disable</td>
</tr>
<tr>
<td></td>
<td>• Recurring</td>
</tr>
<tr>
<td></td>
<td>• Recurring EU</td>
</tr>
<tr>
<td></td>
<td>• Recurring USA</td>
</tr>
<tr>
<td></td>
<td>• Non Recurring</td>
</tr>
<tr>
<td>Begins At</td>
<td>Displays when the daylight saving time begins. This field is not displayed</td>
</tr>
<tr>
<td></td>
<td>when daylight saving time is disabled.</td>
</tr>
<tr>
<td>Ends At</td>
<td>Displays when the daylight saving time ends. This field is not displayed</td>
</tr>
<tr>
<td></td>
<td>when daylight saving time is disabled.</td>
</tr>
<tr>
<td>Offset (in Minutes)</td>
<td>The offset value in minutes. This field is not displayed when daylight</td>
</tr>
<tr>
<td></td>
<td>saving time is disabled.</td>
</tr>
<tr>
<td>Zone</td>
<td>The zone acronym. This field is not displayed when daylight saving time</td>
</tr>
<tr>
<td></td>
<td>is disabled.</td>
</tr>
<tr>
<td>Daylight Saving (DST) in Effect</td>
<td>Displays whether daylight saving time is in effect.</td>
</tr>
</tbody>
</table>

Configure Denial of Service settings

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

Configure Auto-DoS

The Auto-DoS Configuration page lets you automatically enable all the DoS features available on the switch, except for the L4 Port attack. For information about the types of DoS attacks the switch can monitor and block, see Configure Denial of Service on page 77.

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 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   The Auto-DoS Configuration page displays.

7. Next to Auto-DoS Mode, select the Enable radio button.

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

8. Click the Apply button.

   Your settings are saved.

Configure Denial of Service

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

To configure individual DoS settings:

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

2. Launch a web browser.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.
If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.

6. Select System > Management > Denial of Service > Denial of Service Configuration.

7. Select the types of DoS attacks for the switch to monitor and block and configure any associated values:
   • Denial of Service ICMPv4. Enabling ICMPv4 DoS prevention causes the switch to drop ICMPv4 packets with a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv4 packet size.
   • Denial of Service Max ICMPv4 Packet Size. Specify the maximum ICMPv4 packet size allowed. If ICMPv4 DoS prevention is enabled, the switch drops IPv4 ICMP ping packets with a size greater than the configured value.
   • Denial of Service ICMPv6. Enabling ICMPv6 DoS prevention causes the switch to drop ICMPv6 packets with a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv6 packet size.
   • Denial of Service Max ICMPv6 Packet Size. Specify the maximum IPv6 ICMP packet size allowed. If ICMPv6 DoS prevention is enabled, the switch drops IPv6 ICMP ping packets with a size greater than the configured maximum ICMPv6 packet size.

8. Click the Apply button.

Your settings are saved.
Configure the 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

You can configure global DNS settings and DNS server information.

To configure the global DNS settings:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information 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. To remove a DNS server from the list, select its check box and click the Delete button.
    If you click the Delete button without selecting a DNS server, all the DNS servers are deleted.

12. Click the Apply button.
    Your settings are saved.

13. To refresh the page, click the Refresh button.
The following table describes the fields that are shown in the DNS Server Configuration table.

Table 12. DNS Server Configuration information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The identification of the DNS Server.</td>
</tr>
<tr>
<td>Preference</td>
<td>Shows the preference of the DNS server. The preferences are determined by the order in which they were entered.</td>
</tr>
</tbody>
</table>

Configure and view host name-to-IP address information

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

Add a static entry to the dynamic host mapping table

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

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

2. Launch a web browser.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

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 IP address to associate with the host name.

9. Click the **Add** button.
   
The entry displays in the list on the page.

Remove an entry from the dynamic host mapping table

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

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see **Access the switch on-network and connected to the Internet** on page 19 or **Access the switch off-network and not connected to the Internet** on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the **Register to activate your warranty** page displays. For more information, see **Register the switch** on page 30.

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

   For information about the credentials, see **Credentials for the device UI** on page 28.

5. Click the **Go** 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.

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

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

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** 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 13. Dynamic Host Mapping information

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

Configure Green Ethernet settings

Using the Green Ethernet feature allows for power consumption savings.

Configure the Green Ethernet global settings

You can configure Green Ethernet features.

To configure the Green Ethernet settings:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the **Go** 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 the load is light.
   Transition to low power mode does not change the link status. Frames in transit are not
dropped or corrupted in transition to and from low power mode. Transition time is
   transparent to upper layer protocols and applications.

9. Click the **Apply** button.
   Your settings are saved.

**Configure the Green Ethernet interface settings**

You can configure per-port Green Ethernet settings.

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

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and
   connected to the Internet on page 19 or Access the switch off-network and not
   connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page
displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information 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 (for example, g1) in the Go To Interface field and click the Go button.
   • To configure multiple interfaces with the same settings, select the check box associated with each interface.
   • To configure all interfaces with the same settings, select the check box in the heading row.

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

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

The default is Disable.

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

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

10. Click the **Apply** button.
Your settings are saved.

**Manage switch discovery with UPnP and SSDP**

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

You cannot manage the settings for these protocols independently.

**To manage switch discovery with UPnP and SSDP:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see **Access the switch on-network and connected to the Internet** on page 19 or **Access the switch off-network and not connected to the Internet** on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see **Register the switch** on page 30.

4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see **Credentials for the device UI** on page 28.

5. Click the **Go** button.
   The System Information page displays.

6. Select **System > Management > Switch Discovery > UPnP / SSDP**
   The UPnP / SSDP page displays.
7. Select the **Enable** or **Disable** radio button.
   By default, the **Enable** radio button is selected so that both UPnP and SSDP are enabled and the switch can be discovered in the network.

8. Click the **Apply** button.
   Your settings are saved.
   The UPnP / SSDP Administrative Mode field shows the status of UPnP and SSDP.

## Use the Device View

For device view information, see *Use the Device View of the device UI on page 40.*

## 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 following table shows the PoE+ capacity for each model.

<table>
<thead>
<tr>
<th>Model</th>
<th>Maximum Power Budget Across All Active PoE+ Ports</th>
<th>Maximum PoE Power Per Individual Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>GS724TPv2</td>
<td>190W</td>
<td>30W PoE+ (IEEE 802.3at)</td>
</tr>
<tr>
<td>GS724TPP</td>
<td>380W</td>
<td></td>
</tr>
</tbody>
</table>

By default, supplied power is prioritized in ascending port order, up to the total power budget of the device. 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 15. PoE and PoE+ device class power allocation

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

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 88.)

An example for model GS724TPv2:
Port 1 delivers 4.4W to a PD. The available power budget is 185.6W (190W–4.4W).

An example for model GS724TPP:
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 359.1W (380W–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 19 or Access the switch off-network and not connected to the Internet on page 27.
   - The Device UI login page displays.
   - If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   - After registration, enter the device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   - For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   - The System Information page displays.
6. Select System > PoE > Advanced > PoE Port Configuration.
The delivered power is stated in the Output Power (Watt) column.

Configure PoE trap settings and view PoE information

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

To configure the PoE trap settings and view PoE information:

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   - The Device UI login page displays.
   - If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   - After registration, enter the device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   - For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   - The System Information page displays.
6. Select System > PoE > Basic > PoE Configuration.

7. From the Traps menu, select Enable or Disable.
   - The default is Enable. Selecting Disable deactivates the PoE traps.
8. Click the Apply button.
   - Your settings are saved.
The following table describes the nonconfigurable fields on the page.

Table 16. PoE Configuration fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware Version</td>
<td>The firmware version of the PoE firmware component.</td>
</tr>
<tr>
<td>Power Status</td>
<td>The power status.</td>
</tr>
<tr>
<td>Nominal Power</td>
<td>The maximum amount of power in watts that the switch can deliver to all ports.</td>
</tr>
<tr>
<td>Threshold Power Watts</td>
<td>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.</td>
</tr>
<tr>
<td>Consumed Power Watts</td>
<td>The total amount of power in watts that is being delivered to all ports.</td>
</tr>
</tbody>
</table>

Configure the PoE port settings

You can configure PoE settings for individual PoE ports.

To configure the PoE port settings:

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   - The Device UI login page displays.
   - If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   - After registration, enter the device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   - For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   - The System Information page displays.
6. Select System > PoE > Advanced > PoE Port Configuration.
7. Select one or more ports by taking one of the following actions:
   • To configure a single port, select the check box associated with the port, or type the port number (for example, g1) in the **Go To Interface** field and click the **Go** button.
   • To configure multiple ports with the same settings, select the check box associated with each interface.
   • To configure all ports with the same settings, select the check box in the heading row.

8. From the **Admin Mode** menu, select the administrative PoE mode of the port:
   • **Enable**. The port’s capacity to deliver power is enabled. This is the default setting.
   • **Disable**. The port’s capacity to deliver power is disabled.

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 **High Power Mode** menu, select the PoE mode that the port must function in:
    • **802.3af**. The port is powered in and limited to the IEEE 802.3af mode. A PD that requires IEEE 802.3at does not receive power if the port functions in IEEE 802.3af mode.
    • **Legacy**. The port is powered using high-inrush current, which is used by legacy PDs that require more than 15W to power up.
    • **Pre-802.3at**. The port is initially powered in the IEEE 802.3af mode and, before 75 msec pass, is switched to the high-power IEEE 802.3at mode. Select this mode if the PD does not perform Layer 2 classification or if the switch performs 2-event Layer 1 classification.
    • **802.3at**. The port is powered in the IEEE 802.3at mode and is backward compatible with IEEE 802.3af. The 802.3at mode is the default mode. In this mode, if the switch detects that the attached PD requests more power than IEEE 802.3af but is not an IEEE 802.3at Class 4 device, the PD does not receive power from the switch.
11. From the Detection Type menu, select how the port detects the attached PD:
   • pre-ieee. The port performs legacy detection.
   • ieee auto. The port performs a 4-point resistive detection. This is the default setting.
   • auto. The port performs a 4-point resistive detection, and if required, continues with legacy detection.

12. 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 123.

13. Click the Apply button.
    Your settings are saved.

The following table describes the nonconfigurable fields on the page.

Table 17. PoE Port Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Power</td>
<td>All ports supports high-power mode.</td>
</tr>
<tr>
<td>Max Power</td>
<td>The maximum power in milliwatts that can be provided by the port.</td>
</tr>
</tbody>
</table>
| 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: 0.44–12.95W                                                            |
|               | • 1: 0.44–3.83W                                                             |
|               | • 2: 0.44–6.48W                                                             |
|               | • 3: 0.44–12.95W                                                            |
|               | • 4: 0.44–25.5W                                                             |
| Output Voltage| The voltage that is delivered to the PD in volts.                           |
| Output Current| The current that is delivered to the PD in mA.                              |
| Output Power  | The power that is delivered to the PD in watts.                             |
Configure SNMP

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

The switch uses both standard public MIBs for standard functionality and private MIBs that support additional switch functionality. The main object for interface configuration is in the NetgearSmartSwitch-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 to the switch using the SNMP V1 and SNMP V2 protocols. Only those communities with read/write level access can be used to change the configuration using SNMP.
Add an SNMP community:

**To add an SNMP community:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

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

   As an example, the previous figure shows one community configuration.

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 address and management station IP mask parameters are 192.168.1.0/255.255.255.0, any client with an IP address
from one 192.168.1.0 through 192.168.1.255 (inclusive) is allowed access. To allow access from only one station, use a management station IP mask value of 255.255.255.255, and use that machine’s IP address for client address.

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 **Read/Write** or **Read Only**.

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

   • After registration, enter the device admin password.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** 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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

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

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:
   
   • **SNMPv1**. The switch uses SNMPv1 to send traps to the receiver. The default setting is SNMPv1.
   
   • **SNMPv2**. The switch uses SNMPv2 to send traps to the receiver.

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. From the **Status** menu, select **Enable** to send traps to the receiver or select **Disable** to prevent the switch from sending traps to the receiver.
11. Click the **Add** button.
   
The receiver configuration is added.

Modify information about an existing SNMP recipient

**To modify information about an existing SNMP recipient:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   
   • After registration, enter the device admin password.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** 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 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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go 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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

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

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 switch device UI 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.
   - **PoE.** When enabled, SNMP traps are sent when the PoE status changes. The default is Enable.
   - **Fan Failure.** When enabled, SNMP traps are sent when a fan failure occurs. The default is Enable.

8. Click the Apply button.
   Your settings are saved.
View the supported MIBs

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

To view the supported MIBs:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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 nonconfigurable information on the page.

   Table 18. SNMP supported MIBs

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The RFC number if applicable and the name of the MIB.</td>
</tr>
<tr>
<td>Description</td>
<td>The RFC title or MIB description.</td>
</tr>
</tbody>
</table>

Configure SNMPv3 users

Any user can connect to the switch using the SNMPv3 protocol, but for authentication and encryption, the switch supports only one user (admin). Therefore, you can create or modify only one profile.
To configure authentication and encryption settings for the SNMPv3 admin profile by using the web interface:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.
   The User Configuration page displays.
   The SNMPv3 Access Mode field is a read-only field that shows the access privileges for the user account. Access for the admin account is always Read Write. Access for all other accounts is Read Only.
7. To enable authentication, select an Authentication Protocol radio button.
   You can select the MD5 radio button or the SHA radio button. With either of these options, the user login password is used as SNMPv3 authentication password. For information about how to configure the login password, see Change the device admin password for the device UI on page 240.
8. To enable encryption:
   a. Next to Encryption Protocol, select the DES radio button to encrypt SNMPv3 packets using the DES encryption protocol.
   b. In the Encryption Key field, enter an encryption code of eight or more alphanumeric characters.
9. Click the Apply button.
   Your settings are saved.
Configure LLDP

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

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

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

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

Configure LLDP global settings

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

To configure global LLDP settings:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


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

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

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

9. Click the Apply button.

   Your settings are saved.
Configure LLDP port settings

You can specify per-interface LLDP settings.

To configure the LLDP interface:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information 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.** 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 switch system information on page 51](#). For information about how to configure the port description, see [Configure the port settings and maximum frame size on page 132](#).

   9. Click the **Apply** button.

      Your settings are saved.

**View LLDP-MED network policy information**

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

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

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

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   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 nonconfigurable information on the page.

<table>
<thead>
<tr>
<th>Table 19. LLDP-MED network policy information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>Network Policy Number</td>
</tr>
<tr>
<td>Application</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>VLAN ID</td>
</tr>
</tbody>
</table>
Configure LLDP-MED port settings

You can enable LLDP-MED mode on an interface and configure its properties.

To configure LLDP-MED settings for a port:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   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 PSE TLV in LLDP frames.

9. Click the **Apply** button.
   Your settings are saved.

### View local LLDP information

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

**To view local LLDP information:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see *Access the switch on-network and connected to the Internet on page 19* or *Access the switch off-network and not connected to the Internet on page 27*.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see *Register the switch on page 30*.

4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see *Credentials for the device UI on page 28*.

5. Click the Go button.
   The System Information page displays.
6. Select System > LLDP > Advanced > Local Information.

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis ID Subtype</td>
<td>The type of information used to identify the switch in the Chassis ID field.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>The hardware platform identifier for the switch.</td>
</tr>
<tr>
<td>System Name</td>
<td>The user-configured system name for the switch.</td>
</tr>
<tr>
<td>System Description</td>
<td>The switch description, which includes information about the product model</td>
</tr>
<tr>
<td></td>
<td>and platform.</td>
</tr>
<tr>
<td>System Capabilities</td>
<td>The primary functions that the switch supports.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface associated with the rest of the data in the row.</td>
</tr>
<tr>
<td>Port ID Subtype</td>
<td>The type of information used to identify the interface in the Port ID field.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The port number.</td>
</tr>
<tr>
<td>Port Description</td>
<td>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 132.</td>
</tr>
<tr>
<td>Advertisement</td>
<td>The TLV advertisement status of the port.</td>
</tr>
</tbody>
</table>

7. To view additional details about a port, click the name of the port in the Interface column of the Port Information table.
The following table describes the detailed local information that displays for the selected port.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Managed Address</strong></td>
<td></td>
</tr>
<tr>
<td>Address SubType</td>
<td>The type of address the device UI uses, such as an IPv4 address.</td>
</tr>
<tr>
<td>Address</td>
<td>The address used to manage the device.</td>
</tr>
<tr>
<td>Interface SubType</td>
<td>The port subtype.</td>
</tr>
<tr>
<td>Interface Number</td>
<td>The number that identifies the port.</td>
</tr>
<tr>
<td><strong>MAC/PHY Details</strong></td>
<td></td>
</tr>
<tr>
<td>Auto Negotiation Supported</td>
<td>Indicates whether the interface supports port speed autonegotiation. The</td>
</tr>
<tr>
<td></td>
<td>possible values are True and False.</td>
</tr>
<tr>
<td>Auto Negotiation Enabled</td>
<td>The port speed autonegotiation support status. The possible values are True</td>
</tr>
<tr>
<td></td>
<td>(enabled) or False (disabled).</td>
</tr>
<tr>
<td>Auto Negotiation Advertised</td>
<td>The port speed autonegotiation capabilities such as 100BASE-T half-duplex</td>
</tr>
<tr>
<td>Capabilities</td>
<td>mode or 10BASE-TX full-duplex mode.</td>
</tr>
<tr>
<td>Operational MAU Type</td>
<td>The Medium Attachment Unit (MAU) type. The MAU performs physical layer</td>
</tr>
<tr>
<td></td>
<td>functions, including digital data conversion from the Ethernet interface</td>
</tr>
<tr>
<td></td>
<td>collision detection and bit injection into the network.</td>
</tr>
<tr>
<td><strong>MED Details</strong></td>
<td></td>
</tr>
<tr>
<td>Capabilities Supported</td>
<td>The MED capabilities enabled on the port.</td>
</tr>
<tr>
<td>Current Capabilities</td>
<td>The TLVs advertised by the port.</td>
</tr>
<tr>
<td>Device Class</td>
<td>Network Connectivity indicates that the device is a network connectivity</td>
</tr>
<tr>
<td></td>
<td>device.</td>
</tr>
<tr>
<td><strong>Network Policies</strong></td>
<td></td>
</tr>
<tr>
<td>Application Type</td>
<td>The media application type associated with the policy.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID associated with the policy.</td>
</tr>
<tr>
<td>VLAN Type</td>
<td>Specifies whether the VLAN associated with the policy is tagged or untagged.</td>
</tr>
<tr>
<td>User Priority</td>
<td>The priority associated with the policy.</td>
</tr>
<tr>
<td>DSCP</td>
<td>The DSCP associated with a particular policy type.</td>
</tr>
</tbody>
</table>
View LLDP neighbors information

You can view the data that a specific interface receives from other LLDP-enabled systems.

**To view LLDP information received from a neighbor device:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see [Access the switch on-network and connected to the Internet](#) on page 19 or [Access the switch off-network and not connected to the Internet](#) on page 27.
   
   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see [Register the switch](#) on page 30.

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

   For information about the credentials, see [Credentials for the device UI](#) on page 28.

5. Click the Go button.

   The System Information page displays.

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

   ![Neighbor Information](image)

   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.

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

7. 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Details</td>
<td></td>
</tr>
<tr>
<td>Local Port</td>
<td>The interface on the local system that received LLDP information from a remote system.</td>
</tr>
<tr>
<td>MSAP Entry</td>
<td>The Media Service Access Point (MSAP) entry number for the remote device.</td>
</tr>
<tr>
<td>Basic Details</td>
<td></td>
</tr>
<tr>
<td>Chassis ID Subtype</td>
<td>The type of data displayed in the Chassis ID field on the remote system.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>The remote 802 LAN device’s chassis.</td>
</tr>
<tr>
<td>Port ID Subtype</td>
<td>The type of data displayed in the remote system’s Port ID field.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The physical address of the port on the remote system from which the data was sent.</td>
</tr>
<tr>
<td>Port Description</td>
<td>The user-defined description of the port.</td>
</tr>
<tr>
<td>System Name</td>
<td>The system name associated with the remote device.</td>
</tr>
<tr>
<td>System Description</td>
<td>The description of the selected port associated with the remote system.</td>
</tr>
<tr>
<td>System Capabilities</td>
<td>The system capabilities of the remote system.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Managed Addresses</strong></td>
<td></td>
</tr>
<tr>
<td>Address SubType</td>
<td>The type of the management address.</td>
</tr>
<tr>
<td>Address</td>
<td>The advertised management address of the remote system.</td>
</tr>
<tr>
<td>Interface SubType</td>
<td>The port subtype.</td>
</tr>
<tr>
<td>Interface Number</td>
<td>The port on the remote device that sent the information.</td>
</tr>
<tr>
<td><strong>MAC/PHY Details</strong></td>
<td></td>
</tr>
<tr>
<td>Auto-Negotiation Supported</td>
<td>Specifies whether the remote device supports port-speed autonegotiation. The possible values are True or False.</td>
</tr>
<tr>
<td>Auto-Negotiation Enabled</td>
<td>The port speed autonegotiation support status. The possible values are True and False.</td>
</tr>
<tr>
<td>Auto Negotiation Advertised</td>
<td></td>
</tr>
<tr>
<td>Operational MAU Type</td>
<td></td>
</tr>
<tr>
<td>Capabilities</td>
<td>The port speed autonegotiation capabilities.</td>
</tr>
<tr>
<td><strong>MED Details</strong></td>
<td></td>
</tr>
<tr>
<td>Capabilities Supported</td>
<td>The supported capabilities that were received in MED TLV from the device.</td>
</tr>
<tr>
<td>Current Capabilities</td>
<td>The advertised capabilities that were received in MED TLV from the device.</td>
</tr>
<tr>
<td>Device Class</td>
<td>The LLDP-MED endpoint device class. The possible device classes are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Endpoint Class 1 Indicates a generic endpoint class, offering basic LLDP services.</td>
</tr>
<tr>
<td></td>
<td>• Endpoint Class 2 Indicates a media endpoint class, offering media streaming capabilities as well as all Class 1 features.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Hardware Revision</td>
<td>The hardware version advertised by the remote device.</td>
</tr>
<tr>
<td>Firmware Revision</td>
<td>The firmware version advertised by the remote device.</td>
</tr>
<tr>
<td>Software Revision</td>
<td>The software version advertised by the remote device.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number advertised by the remote device.</td>
</tr>
<tr>
<td>Model Name</td>
<td>The model name advertised by the remote device.</td>
</tr>
<tr>
<td>Asset ID</td>
<td>The asset ID advertised by the remote device.</td>
</tr>
</tbody>
</table>
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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


7. Next to DHCP Snooping Mode, select the Enable radio button.

8. To enable the verification of the sender’s MAC address for DHCP snooping, next to MAC Address Validation, select the Enable radio button.
When MAC address validation is enabled, the device checks packets that are received on an untrusted interface to verify that the MAC address and the DHCP client hardware address match. If the addresses do not match, the device drops the packet.

9. Click the **Apply** button.
   Your settings are saved.

Enable DHCP for all interfaces in a VLAN

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

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.

4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** 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 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

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

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.
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:
   - Disabled. The interface is considered to be untrusted and could potentially be used to launch a network attack. DHCP server messages are checked against the bindings database. On untrusted ports, DHCP snooping enforces the following security rules:
     - DHCP packets from a DHCP server (DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) are dropped.
     - DHCPRELEASE and DHCPDECLINE messages are dropped if the MAC address is in the snooping database but the binding’s interface is other than the interface where the message was received.
     - DHCP packets are dropped when the source MAC address does not match the client hardware address if MAC address validation is globally enabled.
   - Enabled. The interface is considered to be trusted and forwards DHCP server messages without validation.

10. From the Invalid Packets menu, select the packet logging mode.
    When enabled, the DHCP snooping feature generates a log message when an invalid packet is received and dropped by the interface.

11. In the Rate Limit (pps) field, specify the rate limit value for DHCP snooping purposes.
    The range is from 0 to 300. 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 also nonapplicable, and rate limiting is disabled.

12. In the Burst Interval (secs) field, specify the burst interval value for rate limiting purposes on the interface.
    The range is from 1 to 15. If the rate limit is N/A, then the burst interval is also nonapplicable, and the field displays N/A.

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 view or clear the dynamic bindings in the bindings table.
To configure static DHCP bindings:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information 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, select 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 dynamic bindings information.

### Table 20. DHCP Dynamic Configuration information

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

---

**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 92](#)). You can use a separate timer schedule for each PoE port.

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

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

**Create a PoE timer schedule**

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

**To create a PoE timer schedule:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


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 123).
   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-YYY format to specify when the timer schedule must start.
   d. Next to the Date End field, click the calendar icon and use the menus in the pop-up window to enter the date in the DD-Mon-YYY format to specify when the timer schedule must stop.

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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   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 123).
   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-YYY format to specify when the timer schedule must start.
   d. Either select the **No End Date** radio button or select the **End Date** radio button, and next to the **End Date** field, click the calendar icon and use the menus in the pop-up window to enter the date in the DD-Mon-YYY format to specify when the timer schedule must stop.
   e. From the **Recurrence Pattern** menu, select the pattern:
      • **Daily.** The timer schedule works with daily recurrence. The fields adjust.
        Either select the **Every Weekday** radio button to let the schedule operate from Monday through Friday or select the **Every Day(s)** radio button and enter a number from 0 to 255 in the field.
        In the latter case, the schedule is triggered every specified number of days. If the number of days is not specified, or if you enter 0, then the schedule is triggered only once.
      • **Weekly.** The timer schedule works with weekly recurrence. The fields adjust.
        In the **Every Week(s)** field, enter a number from 0 to 255 to specify that the schedule must be triggered every specified number of weeks. If the number of weeks is not specified, or if you enter 0, then the schedule is triggered only once.
        Select a single **Week Day** check box, multiple check boxes, or all check boxes to specify the day or days of the week that the schedule must operate.
      • **Monthly.** The timer schedule works with monthly recurrence. The fields adjust.
        In the **Day** field, enter a number from 1 to 31 to specify the day of the month when the schedule must be triggered.
        In the **Every Month(s)** field, enter a number from 0 to 99 to specify that the schedule must be triggered every specified number of months. If the number of months is not specified, or if you enter 0, then the schedule is triggered only once.

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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.
   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 126.
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.

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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.
   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 are part of the PoE timer schedule are also deleted.

To delete a PoE timer schedule:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • After registration, enter the device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   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 a voice VLAN
- Configure Auto-VoIP
- Configure Spanning Tree Protocol
- Configure multicast
- View, search, and manage the MAC address table
- Configure Layer 2 loop protection
Configure the port settings and maximum frame size

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

To configure the port settings and maximum frame size:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

6. Select Switching > Ports > Port Configuration.
7. In the Frame Size field, specify the maximum Ethernet frame size that each interface can support.
   The frame size includes the Ethernet header, CRC, and payload. The range is 1522 to 10000. The default maximum frame size is 1522.

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. In the Description field, enter the description string to be attached to a port.
    The string can be up to 64 characters in length.

11. 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.

12. 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.

13. In the Speed field, specify the speed value for the selected port.
    Possible field values are as follows:
    - Auto. All supported speeds. This is the default setting.
    - 10Mbps. 10 Mbits/second.
    - 100Mbps. 100 Mbits/second.
    - 1000Mbps. 1000 Mbits/second.
    
    The delimiter characters for setting different speed values are a comma (,), a period (.) and a space ( ). For you to set the autonegotiation speed, the autonegotiation mode must be set to Enable. The default is Auto.
    
    Note: After you change the speed value, the switch might be inaccessible for a number of seconds while the new settings take effect.
14. 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.

15. From the **Link Trap** menu, select whether to send a trap when link status changes.

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

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

The default is disabled. The switch does not send pause frames if the port buffers become full. Flow control helps to prevent data loss when the port cannot keep up with the number of frames being switched. When flow control is enabled, the switch can send a pause frame to stop traffic on a port if the amount of memory used by the packets on the port exceeds a preconfigured threshold and responds to pause requests from partner devices. The paused port does not forward packets for the period of time specified in the pause frame. When the pause frame time elapses, or the utilization returns to a specified low threshold, the switch enables the port to again transmit frames. For LAG interfaces, flow control mode is displayed as a blank field because flow control is not applicable.

17. Click the **Apply** button.

Your settings are saved.

The following table describes the nonconfigurable information on the page.

**Table 21. Port Configuration information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Type</td>
<td>For normal ports this field is blank. Otherwise, the possible values are as follows:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Mirrored.</strong> The port is a mirrored port on which all the traffic is copied to the probe port.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Probe.</strong> Use this port to monitor a mirrored port.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Trunk Member.</strong> The port is a member of a link aggregation trunk. Look at the LAG pages for more information.</td>
</tr>
<tr>
<td>Physical Status</td>
<td>Indicates the port speed and duplex mode.</td>
</tr>
<tr>
<td>Link Status</td>
<td>Indicates whether the link is up or down.</td>
</tr>
</tbody>
</table>
Configure link aggregation groups

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

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

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

Configure LAG settings

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

To configure LAG settings:

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

2. Launch a web browser.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

### Table 21. Port Configuration information (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Size (1522 to 10000)</td>
<td>The maximum Ethernet frame size that each interface can support. The frame size depends on your selection from the Frame Size menu above the table and applies to each interface.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Displays the physical address of the specified interface.</td>
</tr>
<tr>
<td>PortList Bit Offset</td>
<td>Displays the bit offset value that corresponds to the port when the MIB object type PortList is used to manage in SNMP.</td>
</tr>
<tr>
<td>ifIndex</td>
<td>The ifIndex of the interface table entry associated with this port.</td>
</tr>
</tbody>
</table>
If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.

6. Select Switching > LAG > Basic > LAG Configuration.

7. In the LAG Name field, enter the name to be assigned to the LAG.

You can enter any string of up to 15 alphanumeric characters. A valid name must be specified for you to create the LAG.

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

The description can be up to 64 characters in length.

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

When the LAG is disabled, no traffic flows and LACPDUs are dropped, but the links that form the LAG are not released. The default is Enable.

10. From the Hash Mode menu, select the load-balancing mode for a port channel (LAG):
   • 1 Src/Dest MAC, incoming port. This mode uses the source MAC address, destination MAC address, and incoming port that are associated with the packet.
   • 2 Src/Dest IP and TCP/UDP Port Fields. This mode uses the source and destination IP addresses and source and destination TCP or UDP port values that are associated with the packet.

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

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.** Disables LACP on the selected LAG. The LAG is configured automatically.

14. Click the **Apply** button.

Your settings are saved.

The following table describes the nonconfigurable information on the page.

### Table 22. LAG Configuration information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAG ID</td>
<td>Identification of the LAG.</td>
</tr>
<tr>
<td>Active Ports</td>
<td>Indicates the ports that are actively participating in the port channel.</td>
</tr>
<tr>
<td>LAG State</td>
<td>Indicates whether the link is up or down.</td>
</tr>
</tbody>
</table>

**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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.

6. Select Switching > LAG > Basic > LAG Membership.

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 system priority

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

To set the LACP system priority:

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

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


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

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

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.

   The System Information page displays.
6. Select Switching > LAG > Advanced > LACP Port Configuration.

   ![LACP Port Configuration](image)

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 0 to 255. The default 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 64 VLANs.

The following VLANs are preconfigured on the switch and you cannot delete them:
   - **VLAN 1.** The default VLAN of which all ports are members.
   - **VLAN 4088.** The default Auto-VoIP VLAN. By default, this VLAN does not include any members but you can manually add members.

Configure VLAN settings

You can configure the various VLAN settings.

Add a VLAN

**To add a VLAN:**

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

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

6. Select Switching > VLAN > Basic > VLAN Configuration.

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. (The default VLANs are 1 and 4088).

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.

9. The VLAN Type field displays the type of the VLAN that you are configuring.
   The VLAN name can be up to 32 alphanumeric characters long, including blanks. You cannot change the names of the default VLANs (that is, the VLANs with ID 1 and 4088).

10. The VLAN Type field displays the type of the VLAN that you are configuring.
    You cannot change the type of the default VLANs (that is, the VLANs with ID 1 and 4088). When you create a VLAN using this page, its type is always static. A VLAN that is created by the Generic VLAN Registration Protocol (GVRP) initially uses a type of dynamic. You can change the type of a dynamic VLAN to static.
11. Click the **Add** button.
    
    The VLAN is added to the switch.

Delete a VLAN

**To delete a VLAN from the switch:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see [Access the switch on-network and connected to the Internet on page 19](#) or [Access the switch off-network and not connected to the Internet on page 27](#).
   
   The Device UI login page displays.
   
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see [Register the switch on page 30](#).

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

   For information about the credentials, see [Credentials for the device UI on page 28](#).

5. Click the **Go** 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 2 to 4093. You cannot delete VLANs 1 and 4088, 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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. 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 19 or Access the switch off-network and not
   connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page
displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter
     the Insight network password for the last Insight network location.
     For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information 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 and LAGs that are members of the VLAN, tags are removed from all egress packets.
   - **Tag All**. For all ports and LAGs that are members of the VLAN, all egress packets are tagged.
   - **Remove All**. All ports and LAGs are removed from the VLAN, including the ports and LAGs that were dynamically registered through GVRP.

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)**. Selects the port as a tagged port in the VLAN. All frames transmitted on the port are tagged for this VLAN.
   - **U (Untagged)**. Selects the port as an untagged port in the VLAN. All frames transmitted on the port are untagged for this VLAN.
   - **Blank**. The port is excluded from the VLAN.

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)**. Selects the LAG as a tagged LAG in the VLAN. All frames transmitted on the LAG are tagged for this VLAN.
    - **U (Untagged)**. Selects the LAG as an untagged LAG in the VLAN. All frames transmitted on the LAG are untagged for this VLAN.
    - **Blank**. The LAG is excluded from the VLAN.

11. Click the **Apply** button.
    
    Your settings are saved.

The following table describes the nonconfigurable information on the page.

**Table 23. Advanced VLAN membership**

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Name</td>
<td>The name for the VLAN that you selected. It can be up to 32 alphanumeric characters long, including blanks. The names for the following VLANs are predefined:</td>
</tr>
<tr>
<td></td>
<td>• <strong>VLAN 1</strong>. Default.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VLAN 4088</strong>. Auto-VoIP.</td>
</tr>
<tr>
<td>VLAN Type</td>
<td>The type of the VLAN you selected:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong> (VLAN ID = 1). Always present.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Static</strong>. A VLAN that you configured.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dynamic</strong>. A VLAN that is created through GVRP registration, that you did not convert to a static VLAN, and that GVRP can therefore remove.</td>
</tr>
</tbody>
</table>
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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

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

   ![](image)

   The following table describes the nonconfigurable information on the page.

   **Table 24. VLAN status**

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>The VLAN identifier (VID) of the VLAN. The range of the VLAN ID is 1 to 4093.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>The name of the VLAN. VLAN ID 1 is always named Default.</td>
</tr>
</tbody>
</table>
Configure the port PVID settings

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

- By default, the PVID for each port is 1.
- If you do not specify another value, the default VLAN PVID is used.
- To change the port’s default PVID, you must first create a VLAN that includes the port as a member.

To configure PVID settings:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.
6. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

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. You can specify port tagging for the VLAN only if the port that you want to add as a tagged port is also member of the VLAN. To reset the VLAN tag configuration to the defaults, use the **None** keyword.

12. From the **Acceptable Frame** menu, specify one if the following types of frames that can be received on the port:
    - **Admit All**. Untagged frames or priority-tagged frames that are received on the port are accepted and assigned the value of the port VLAN ID for the port. This is the default selection.
    - **VLAN Only**. Untagged frames or priority-tagged frames that are received on the port are discarded.
    - **Admit Untagged Only**. Untagged frames that are received on the port are accepted.
With the Admit All and VLAN Only selections, VLAN-tagged frames are forwarded in accordance to the 802.1Q VLAN specification.

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 nonconfigurable fields on the page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Ingress Filtering</td>
<td>Indicates whether ingress filtering is enabled for the interface.</td>
</tr>
<tr>
<td>Untagged VLANs</td>
<td>The number of untagged VLANs for the interface.</td>
</tr>
<tr>
<td>Tagged VLANs</td>
<td>The number of tagged VLANs for the interface.</td>
</tr>
<tr>
<td>Forbidden VLANs</td>
<td>The number of forbidden VLANs for the interface.</td>
</tr>
<tr>
<td>Dynamic VLANs</td>
<td>The number of dynamically added VLANs for the interface.</td>
</tr>
</tbody>
</table>

Configure a voice VLAN

You can configure the settings for a voice VLAN.

**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 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


![Voice VLAN Configuration](image)

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. You must enter the VLAN ID in the **Value** field (see the next step).
   - **Dot1p.** Configure voice VLAN 802.1p priority tagging for voice traffic. You must enter the dot1p value in the **Value** field (see the next step).
   - **Untagged.** Configure the phone to send untagged voice traffic.

10. In the **Value** field, enter the VLAN ID or dot1p value.
    This field is enabled only if you select **VLAN ID** or **Dot1p** from the **Interface Mode** menu.

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 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 Auto-VoIP

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

### Configure 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   ![](image)

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

   This specifies the type of prioritization.
8. From the **Class Value** menu, specify the CoS tag value to be reassigned for packets received on the voice VLAN when Remark CoS is enabled.

9. 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.

10. Click the **Apply** button.
    
    Your settings are saved.
    
    The Operational Status field displays the current operational status of each 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   The OUI-Based Properties page displays.

7. In the Auto-VoIP VLAN ID field, enter the VoIP VLAN ID of the switch.

   The default Auto-VoIP VLAN ID is 4088. You can use that VLAN ID or create another VLAN ID for Auto-VoIP.

8. From the OUI-based priority menu, select the OUI-based priority of the switch, from 0 to 7.

   The default value is 7.

9. Click the Apply button.

   Your settings are saved.

Configure the OUI-based port settings

You can configure the OUI port settings.

To configure OUI-based port settings:

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

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

2. Launch a web browser.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** button.

The System Information page displays.

6. Select **Switching > Auto-VoIP > OUI-based > Port Settings**.

![Auto-VoIP OUI Port Settings](image)

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 the following OUIs that identify the IP phone manufacturer:

- 00:01:E3: SIEMENS
- 00:03:6B: CISCO1
- 00:12:43: CISCO2
- 00:60:B9: NITSUKO
- 00:D0:1E: PINTEL
- 00:E0:75: VERILINK
- 00:E0:BB: 3COM
- 00:04:0D: AVAYA1
- 00:1B:4F: AVAYA2

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

Configure the OUI table

**To configure the OUI table:**

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

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

2. Launch a web browser.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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 19](#) or [Access the switch off-network and not connected to the Internet on page 27](#).
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see [Register the switch on page 30](#).

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see [Credentials for the device UI on page 28](#).

5. Click the **Go** 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 19 or **Access the switch off-network and not connected to the Internet** on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see **Register the switch** on page 30.

4. Enter one of the following passwords:

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

   For information about the credentials, see **Credentials for the device UI** on page 28.

5. Click the **Go** 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 with the latest information about the switch, click the **Refresh** button.

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

**Table 26. Auto-VoIP status information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-VoIP VLAN ID</td>
<td>The Auto-VoIP VLAN ID.</td>
</tr>
<tr>
<td>Maximum Number of Voice Channels Supported</td>
<td>The maximum number of voice channels supported.</td>
</tr>
</tbody>
</table>
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 161.

The switch supports the following spanning tree versions:

- **CST.** Common STP. For information on configuring CST, see Configure the CST settings on page 163 and Configure the CST port settings on page 165.

- **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 170 and Configure and view the port settings for an MST instance on page 173.

- **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 169.

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

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

7. Configure the following global settings for the switch:
   
   a. **Spanning Tree State.** Enable or disable the spanning tree operation on the switch.
      
      By default, spanning tree operation is disabled.

   b. **STP Operation Mode.** Specify the STP version for the switch.
      
      The options are **STP**, **RSTP**, and **MSTP**. The default is RSTP.
c. **Configuration Name.** Specify a name to identify the STP, RSTP, or MSTP configuration.

   The name can be up to 32 alphanumeric characters.

d. **Configuration Revision Level.** Specify an identifier to identify the STP, RSTP, or MSTP configuration.

   The values can be from 0 to 65535. The default value is 0.

e. **Forward BPDU while STP Disabled.** Enable or disable the bridge protocol data unit (BPDU) flood.

   This setting specifies whether spanning tree BPDUs are forwarded while spanning tree is disabled on the switch.

8. Click the **Apply** button.

   Your settings are saved.

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

**Table 27. STP Configuration status**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Configuration Digest Key</td>
<td>The identifier used to identify the configuration currently being used.</td>
</tr>
<tr>
<td><strong>STP Status</strong></td>
<td></td>
</tr>
<tr>
<td>Bridge Identifier</td>
<td>The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.</td>
</tr>
<tr>
<td>Time Since Topology Change</td>
<td>The time in day-hour-minute-second format since the topology of the CST last changed.</td>
</tr>
<tr>
<td>Topology Change Count</td>
<td>The number of times that the topology changed for the CST.</td>
</tr>
<tr>
<td>Topology Change</td>
<td>The value of the topology change setting for the switch that indicates if a topology change is in progress on any port assigned to the CST. The option is True or False.</td>
</tr>
<tr>
<td>Designated Root</td>
<td>The bridge identifier of the root bridge. It consists of the bridge priority and the base MAC address of the bridge.</td>
</tr>
<tr>
<td>Root Path Cost</td>
<td>The path cost to the designated root for the CST.</td>
</tr>
<tr>
<td>Root Port</td>
<td>The port to access the designated root for the CST.</td>
</tr>
<tr>
<td>Max Age (secs)</td>
<td>The maximum age timer controls the maximum length of time in seconds that passes before a bridge port saves its configuration BPDU information.</td>
</tr>
<tr>
<td>Forward Delay (secs)</td>
<td>The derived value of the Root Port Bridge Forward Delay setting.</td>
</tr>
<tr>
<td>Hold Time (secs)</td>
<td>The minimum time in seconds between the transmission of configuration BPDUs.</td>
</tr>
</tbody>
</table>
Configure the CST settings

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

To configure CST settings:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CST Regional Root</td>
<td>The priority and base MAC address of the CST regional root.</td>
</tr>
<tr>
<td>CST Path Cost</td>
<td>The path cost to the CST tree regional root.</td>
</tr>
</tbody>
</table>
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 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 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.

- **Bridge Forward Delay (secs).** The bridge forward delay time, which indicates the time in seconds a bridge must remain in a listening and learning state before forwarding packets. The value must be greater or equal to (Bridge Max Age / 2) + 1. The time range is from 4 seconds to 30 seconds. The default is 15 seconds.

- **Spanning Tree Maximum Hops.** The maximum number of bridge hops the information for a particular CST instance can travel before being discarded. The range is from 6 to 40. The default is 20 hops.

8. Click the **Apply** button.

Your settings are saved.
Configure the CST port settings

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

A port can become diagnostically disabled (D-Disable) when DOT1S experiences a severe error condition. The most common cause is when the DOT1S software experiences BPDU flooding. The flooding criteria are such that DOT1S receives more than 15 BPDUs in a 3-second interval. The other causes for DOT1S D-Disable are extremely rare.

To configure CST port settings:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

6. Select Switching > STP > Advanced > CST Port Configuration.
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 that is associated with the port or port channel.
   The possible values are Enable and Disable. The default 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, Disable, and Auto. The default value is Auto, which specifies that the switch waits three seconds (with no BPDUs received on the interface) before placing the interface into the PortFast mode.

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 time.
    The option is Enable or 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 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 with the latest information about the switch, click the **Refresh** button.
The following table describes the nonconfigurable information on the page.

**Table 28. CST port configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port State</td>
<td>The forwarding state of this port. The default is Disabled.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The port identifier for the specified port within the CST. It is made up from</td>
</tr>
<tr>
<td></td>
<td>the port priority and the interface number of the port.</td>
</tr>
<tr>
<td>Hello Timer</td>
<td>The value of the parameter for the CST. The default is 2 seconds.</td>
</tr>
</tbody>
</table>

View the CST port status

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

**To view the CST port status:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see **Access the switch on-network and connected to the Internet on page 19** or **Access the switch off-network and not connected to the Internet on page 27**.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see **Register the switch on page 30**.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see **Credentials for the device UI on page 28**.

5. Click the **Go** button.
   The System Information page displays.

6. Select **Switching > STP > Advanced > CST Port Status**.
The CST Port Status 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 with the latest information about the switch, click the **Refresh** button.

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

**Table 29. CST port status**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The physical port or LAG that is associated with the CST.</td>
</tr>
<tr>
<td>Port Role</td>
<td>Each MST bridge port that is enabled is assigned a port role for each spanning tree. The port role can be Root, Designated, Alternate, Backup, Master, or Disabled.</td>
</tr>
<tr>
<td>Designated Root</td>
<td>The root bridge for the CST. It is made up using the bridge priority and the base MAC address of the bridge.</td>
</tr>
<tr>
<td>Designated Cost</td>
<td>The path cost offered to the LAN by the designated port.</td>
</tr>
<tr>
<td>Designated Bridge</td>
<td>The identifier of the bridge with the designated port. It is made up using the bridge priority and the base MAC address of the bridge.</td>
</tr>
<tr>
<td>Designated Port</td>
<td>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.</td>
</tr>
<tr>
<td>Topology Change Acknowledge</td>
<td>Identifies whether the topology change acknowledgement flag is set for the next BPDU to be transmitted for the port. It is either True or False.</td>
</tr>
<tr>
<td>Edge port</td>
<td>Indicates whether the port is enabled as an edge port. It is either Enabled or Disabled.</td>
</tr>
<tr>
<td>Point-to-Point MAC</td>
<td>The derived value of the point-to-point status.</td>
</tr>
<tr>
<td>CST Regional Root</td>
<td>The bridge identifier of the CST regional root. It is made up using the bridge priority and the base MAC address of the bridge.</td>
</tr>
<tr>
<td>CST Path Cost</td>
<td>The path cost to the CST regional root.</td>
</tr>
<tr>
<td>Port Forwarding State</td>
<td>The forwarding state of the port.</td>
</tr>
</tbody>
</table>
View the Rapid STP information

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

**To view information about RSTP:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

6. Select **Switching > STP > Advanced > RSTP**.

   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.

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

**Table 30. Rapid STP status information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The physical or port channel interfaces associated with VLANs associated with the CST.</td>
</tr>
<tr>
<td>Role</td>
<td>Each MST bridge port that is enabled is assigned a port role for each spanning tree. The port role can be Root, Designated, Alternate, Backup Master, or Disabled.</td>
</tr>
</tbody>
</table>
Manage the MST settings

You can configure Multiple Spanning Tree (MST) on the switch.

Configure an MST instance

To configure an MST instance:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information 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 64. This is visible only when the select option of the MST ID select box is selected. The switch supports up to four instances.
   - **Priority.** The bridge priority value for the MST. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if you set the priority to any value between 0 and 4095, the switch automatically sets the value to 0. The default is 32768. The valid range is 0–61440.
   - **VLAN ID** The menu includes all VLANs that are configured on the switch. You can select VLANs that must be associated with the MST instance or clear VLANs that are already associated with the MST instance.

8. Click the **Add** button.

   The MST is added.

The following table describes the nonconfigurable information on the page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge Identifier</td>
<td>The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.</td>
</tr>
<tr>
<td>Last TCN</td>
<td>The time in the format day:hour:minute:second since the topology of the selected MST instance last changed.</td>
</tr>
<tr>
<td>Topology Change Count</td>
<td>Number of times that the topology changed for the selected MST instance.</td>
</tr>
<tr>
<td>Topology Change</td>
<td>The value of the topology change settings for the switch, indicating if a topology change is in progress on any port assigned to the selected MST instance. It is either True or False.</td>
</tr>
<tr>
<td>Designated Root</td>
<td>The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.</td>
</tr>
<tr>
<td>Root Path Cost</td>
<td>The path cost to the designated root for this MST instance.</td>
</tr>
<tr>
<td>Root Port</td>
<td>The port to access the designated root for this MST instance.</td>
</tr>
</tbody>
</table>

**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 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


The MST Configuration page displays.

7. Select the check box next to the instance.

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


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 Multiple Spanning Tree (MST) settings on a specific port on the switch.

A port can become diagnostically disabled (D-Disable) when DOT1S experiences a severe error condition. The most common cause is when the DOT1S software experiences BPDU flooding. The flooding criteria is such that DOT1S receives more than 15 BPDUs in a 3-second interval. The other causes for DOT1S D-Disable are extremely rare.

To configure MST port settings:

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

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

2. Launch a web browser.

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

If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

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

For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.

6. Select Switching > STP > Advanced > MST Port Configuration.

![MST Port Configuration](image)

**Note:** If no MST instances are configured on the switch, the page displays a “No MSTs Available” message.

7. From the Select MST menu, select the MST instance.
   You can select only instances that you added to the switch (see Configure an MST instance on page 170).

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.

The following table describes the nonconfigurable information on the page.

<table>
<thead>
<tr>
<th>Table 32. MST port status information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Auto-calculated Port Path Cost</td>
</tr>
<tr>
<td>Port ID</td>
</tr>
<tr>
<td>Port Up Time Since Counters Last Cleared</td>
</tr>
<tr>
<td>Port Mode</td>
</tr>
<tr>
<td>Port Forwarding State</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Port Role</td>
</tr>
<tr>
<td>Designated Root</td>
</tr>
<tr>
<td>Designated Cost</td>
</tr>
<tr>
<td>Designated Bridge</td>
</tr>
<tr>
<td>Designated Port</td>
</tr>
</tbody>
</table>
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 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

6. Select **Switching > STP > Advanced > STP Statistics**.

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.
8. To refresh the page with the latest information about the switch, click the **Refresh** button.

The following table describes the nonconfigurable information on the page.

**Table 33. STP Statistics**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The physical port or LAG on the switch.</td>
</tr>
<tr>
<td>STP BPDUs Received</td>
<td>The number of STP BPDUs received at the selected port.</td>
</tr>
<tr>
<td>STP BPDUs Transmitted</td>
<td>The number of STP BPDUs transmitted from the selected port.</td>
</tr>
<tr>
<td>RSTP BPDUs Received</td>
<td>The number of RSTP BPDUs received at the selected port.</td>
</tr>
<tr>
<td>RSTP BPDUs Transmitted</td>
<td>The number of RSTP BPDUs transmitted from the selected port.</td>
</tr>
<tr>
<td>MSTP BPDUs Received</td>
<td>The number of MSTP BPDUs received at the selected port.</td>
</tr>
<tr>
<td>MSTP BPDUs Transmitted</td>
<td>The number of MSTP BPDUs transmitted from the selected port.</td>
</tr>
</tbody>
</table>

**Configure multicast**

Multicast IP traffic is traffic that is destined to a host group. Host groups for IPv4 multicast are identified by class D addresses, which range from 224.0.0.0 to 239.255.255.255.

**View, search, or clear the MFDB table**

The Multicast Forwarding Database (MFDB) holds the port membership information for all active multicast forwarding 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 19** or **Access the switch off-network and not connected to the Internet on page 27**.

   The Device UI login page displays.
If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

6. Select Switching > Multicast > MFDB > MFDB Table.

7. In the Search by MAC Address field, enter a MAC address.

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

8. Click the Go button.

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

The following describes the nonconfigurable information on the page.

Table 34. MFDB table information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>The multicast MAC address for which you requested data.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID to which the multicast MAC address is related.</td>
</tr>
<tr>
<td>Type</td>
<td>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.</td>
</tr>
<tr>
<td>Component</td>
<td>The component that is responsible for this entry in the Multicast Forwarding Database. The options are IGMP snooping, GMRP, Static Filtering, and MLD snooping.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description of this multicast table entry. The options are Management Configured, Network Configured, and Network Assisted.</td>
</tr>
<tr>
<td>Forwarding Interfaces</td>
<td>The resultant forwarding list is derived from combining all the forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.</td>
</tr>
</tbody>
</table>
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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   The MFDP Statistics page displays.

7. To refresh the page with the latest information about the switch, click the Refresh button.
The following table describes the MFDB Statistics fields.

Table 35. MFDB Statistics information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max MFDB Table Entries</td>
<td>The maximum number of entries that the Multicast Forwarding Database table can hold (256 entries).</td>
</tr>
<tr>
<td>Most MFDB Entries Since Last Reset</td>
<td>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.</td>
</tr>
<tr>
<td>Current Entries</td>
<td>The current number of entries in the Multicast Forwarding Database table.</td>
</tr>
</tbody>
</table>
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 parameters for IGMP snooping, which is used to build forwarding lists for multicast traffic.

To configure IGMP snooping:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.
If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


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

7. Select the IGMP Snooping Status Enable or Disable radio button.

   This selection 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 with the latest information about the switch, click the Refresh button.

    The following table describes the nonconfigurable information on the page.

**Table 36. IGMP Snooping Configuration Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast Control Frame Count</td>
<td>The number of multicast control frames that are processed by the switch.</td>
</tr>
<tr>
<td>Interfaces Enabled for IGMP Snooping</td>
<td>The interfaces that are enabled for IGMP snooping.</td>
</tr>
</tbody>
</table>
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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information 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 selection 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 option 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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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 entry in the MFDB table.
   Enter six two-digit hexadecimal numbers separated by colons, for example 01:00:5e:45:67:89.
Configure IGMP snooping for VLANs

To configure IGMP snooping settings for VLANs:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
The System Information page displays.

6. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping VLAN Configuration**.

   ![IGMP Snooping VLAN Configuration](image)

7. Select the check boxes for one or more VLANs.

   If you select the check box for a single VLAN, the VLAN ID displays in the VLAN ID field.

8. Configure the IGMP snooping values for the selected VLAN or VLANs:

   - **Admin Mode**. Enable or disable IGMP snooping for the specified VLAN ID. The default is Disable.
   - **Fast Leave Mode**. Enable or disable the IGMP snooping fast leave mode for the specified VLAN ID. The default is Disable.
   - **Host Timeout**. Set the value for group membership interval of IGMP snooping for the specified VLAN ID. The range is from the value for the Maximum Response Time plus 1 to 3600 seconds. The default is 260 seconds.
   - **Maximum Response Time**. Set the value for the maximum response time of IGMP snooping for the specified VLAN ID. The range is from 1 to the Host Timeout value minus 1. This value must be greater than group membership interval value. The default is 10 seconds.
   - **MRouter Timeout**. Set the value for multicast router expiry time of IGMP snooping for the specified VLAN ID. The range is from 0 to 3600 seconds. The default is 0 seconds.
   - **Report Suppression Mode**. Enable or disable IGMP snooping report suppression mode for the specified VLAN ID. IGMP snooping report suppression allows the suppression of the IGMP reports sent by the multicast hosts by building a Layer 3 membership table. The results is that only the most essential reports are sent to the IGMP routers so that the routers can continue to receive the multicast traffic. The default is Disable.
   - **Querier Mode**. Enable or disable the IGMP querier mode. The default is Disable.
   - **Query Interval**. Set the IGMP query interval for the specified VLAN ID. The range is from 1 to 1800 seconds. The default is 60 seconds.

9. Click the **Apply** button.

   Your settings are saved.
Modify IGMP snooping settings for a VLAN

To modify IGMP snooping settings for a VLAN:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.
   The IGMP Snooping VLAN Configuration page displays.
7. Select the check box next to the VLAN ID.
8. Update the values.
9. Click the Apply button.
   Your settings are saved.

Disable IGMP snooping on a VLAN

To disable IGMP snooping on a VLAN:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   The IGMP Snooping VLAN Configuration page displays.

7. Select the check box next to the VLAN ID.

8. From the Admin Mode menu, select Disable.

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 connected. All IGMP packets snooped by the switch are forwarded to the multicast router reachable from the interface. Configuring a multicast router interface is usually not required because the switch automatically detects the multicast router and forwards IGMP packets accordingly. This configuration is required only if you want to make sure that the multicast router always receives IGMP packets from the switch in a complex network.

To configure 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 19 or Access the switch off-network and not connected to the Internet on page 27.
The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information 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 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 connected to the interface. This configuration is usually not required because the switch automatically detects a multicast router and forwards the IGMP packets accordingly. This configuration is required only in a complex network if you want to make sure that the multicast router always receives IGMP packets from the switch.

To configure an IGMP multicast router VLAN:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information 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 queries all end-devices on the network to announce their multicast memberships. This central device is the IGMP querier. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it stops forwarding multicasts to the port where the end device is located.

You can configure and display information about IGMP snooping queriers on the network and, separately, on VLANs.

**Configure an IGMP snooping querier**

You can configure the settings for an IGMP snooping querier.

**To configure the settings for an IGMP snooping querier:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
    If you do not know the IP address of the switch, see **Access the switch on-network and connected to the Internet on page 19** or **Access the switch off-network and not connected to the Internet on page 27**.
    The Device UI login page displays.
    If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see **Register the switch on page 30**.

4. Enter one of the following passwords:
    • Enter your device admin password.
    • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
    For information about the credentials, see **Credentials for the device UI on page 28**.

5. Click the **Go** button.
    The System Information page displays.
6. Select **Switching > Multicast > IGMP Snooping Querier > Querier Configuration**.

![Querier Configuration](image)

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 in the range from 1 to 1800. The default value is 60 seconds.
   - **Querier Expiry Interval (secs)**. Specify the time interval in seconds after which the last querier information is removed. The querier expiry interval must be in the range from 60 to 300. The default value is 125 seconds.

8. Click the **Apply** button.
   
   Your settings are saved.

**Configure an IGMP snooping querier for a VLAN**

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.
If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information 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 must be enabled. You can select an existing VLAN only.
   • Querier Election Participate Mode. Enable or disable the querier mode:
     - Disable. Upon seeing another querier of the same version in the VLAN, the snooping querier moves to the non-querier state.
     - Enable. The snooping querier participates in querier election, in which the lowest IP address operates as the querier in that VLAN. The other querier moves to non-querier state.
   • Snooping Querier VLAN Address. Specify the snooping querier IP address to be used as the source address in periodic IGMP queries that are sent to the VLAN.

9. Click the Apply button.

Your settings are saved.

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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.
   
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID on which IGMP snooping querier is administratively enabled and the VLAN exists in the VLAN database.</td>
</tr>
<tr>
<td>Operational State</td>
<td>The operational state of the IGMP snooping querier on a VLAN. It can be in any of the following states:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>
7. To refresh the page with the latest information about the switch, click the Refresh button.
The following table describes the nonconfigurable information on the page.

Table 38. Querier VLAN Status information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.

6. Select Switching > Address Table > Basic > Address Table.

7. Use the Search menu and field to search for a MAC address, VLAN ID, or interface number:
   - **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.

   - **VLAN ID.** From the Search menu, select VLAN ID, and enter the VLAN ID, for example, 100. Then click the Go button.

   - **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.

8. To refresh the page with the latest information about the switch, click the Refresh button.

9. To clear all dynamic MAC address entries in the table, click the Clear button.

The following table describes the nonconfigurable information on the page.

**Table 39. MAC address table information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total MAC Addresses</td>
<td>The number of MAC addresses learned or configured.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID associated with the MAC address.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

6. Select Switching > Address Table > Advanced > Dynamic Addresses.
7. In the **Address Aging Timeout (seconds)** field, specify the time-out period in seconds for aging out dynamically learned forwarding information. The value can be any number between 10 and 1000000 seconds. The default is 300 seconds.

8. Click the **Apply** button. Your settings are saved.

### Add a static MAC address to the MAC address table

**To add a static MAC address to the MAC address table:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch. If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** button.
   The System Information page displays.

6. Select **Switching > Address Table > Advanced > Static MAC Address**.
7. From the **Interface** menu, select the interface.
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.

**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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information 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 Transmit 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 Disable Timer field, enter the time in seconds after which a port is disabled when a loop is detected.
    The range is from 0 to 604800 seconds. The default is 0 seconds.

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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information 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 Keep Alive menu, select Enable or Disable to specify whether keep-alives are enabled on an interface.
   The default is Enable.

10. 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.

11. Click the Apply button.
    Your settings are saved.

12. Click the Clear button to clear all the statistics in the table.

13. Click the Refresh button to update the page to show the latest information.
The following table describes the nonconfigurable information displayed on the page.

Table 40. L2 Loop Protection Interface Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loop Detected</td>
<td>Shows whether a loop is detected on the interface. If the interface is disabled and then reenabled, the status changes to No again.</td>
</tr>
<tr>
<td>Loop Count</td>
<td>The number of packets that were received after the loop was detected.</td>
</tr>
<tr>
<td>Time Since Last Loop</td>
<td>The time that elapsed since the loop was detected.</td>
</tr>
<tr>
<td>Port Status</td>
<td>The status of the interface (Enabled, Disabled, or D-Disabled, which stands for diagnostically disabled).</td>
</tr>
</tbody>
</table>
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 the 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

7. Either configure the same CoS trust mode settings for all CoS-configurable interfaces or configure CoS settings per interface:
   • To configure the same CoS trust mode settings for all CoS-configurable interfaces, do the following:
     a. Select the Global radio button.
     b. From the Global Trust Mode menu, select one of the following trust mode options for ingress traffic on the switch:
        - Untrusted. Do not trust any CoS packet marking at ingress.
        - 802.1p. The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of seven internal hardware priority queues. The default mode is 802.1p.
        - DSCP. The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.
   • To configure CoS settings per interface, do the following:
     a. Select the Interface radio button.
     b. From the Interface Trust Mode menu, select one of the following trust mode options:
        - Untrusted. Do not trust any CoS packet marking at ingress.
        - 802.1p. The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of seven internal hardware priority queues. The default mode is 802.1p.
        - DSCP. The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.

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 19 or Access the switch off-network and not connected to the Internet on page 27.
The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information 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 is 802.1p.
• **DSCP.** The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.

10. In the **Interface Shaping Rate** field, specify the maximum outbound transmission rate bandwidth in kbps.

   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.

   The expected shaping at egress interface is calculated as follows:
   
   \[ \text{frameSize} \times \frac{\text{shaping}}{\text{frameSize} + \text{IFG}} \]
   
   where IFG (Inter frame gap) is 20 bytes, frameSize is configured frame size, and shaping is configured traffic shaping.

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

11. In the **Interface Ingress Rate Limit** field, specify the maximum inbound transmission rate bandwidth in kbps.

   This setting is used to shape the inbound transmission rate in increments of 1 percent in a range of 0–100. The interface discards traffic that arrives at a bandwidth in excess of the specified limit.

12. 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 206.

**To configure the CoS queue settings for an interface:**

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

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

2. Launch a web browser.

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

   If you do not know the IP address of the switch, see [Access the switch on-network and connected to the Internet](#) on page 19 or [Access the switch off-network and not connected to the Internet](#) on page 27.

   The Device UI login page displays.
If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information 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 to be configured.
   You can select a queue from 0 to 7.
10. 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.

11. Click the **Apply** button.
    Your settings are saved.

    The Queue Management Type field displays the queue depth management technique that is used for queues on the interface. By default, this method is Taildrop, irrespective of your selection from the **Scheduler Type** menu.

Map 802.1p priorities to queues

You can view or change which internal traffic classes are mapped to the 802.1p priority class values in Ethernet frames that the device receives. The priority-to-traffic class mappings can be applied globally or per interface. The mapping allows the switch to group various traffic types (for example, data or voice) based on their latency requirements and give preference to time-sensitive traffic.

**To map 802.1p priorities to queues:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** button.
   The System Information page displays.

6. Select **QoS > CoS > Advanced > 802.1p to Queue Mapping**.
7. In the 802.1p to Queue Mapping table, map each of the eight 802.1p priorities to a queue (internal traffic class) from 0 to 7.

The 802.1p Priority row contains traffic class selectors for each of the eight 802.1p priorities to be mapped. The priority goes from low (0) to high (7). For example, traffic with a priority of 0 is for most data traffic and is sent using best effort. Traffic with a higher priority, such as 7, might be time-sensitive traffic, such as voice or video.

The values in the menu under each priority represent the traffic class. The traffic class is the hardware queue for a port. Higher traffic class values indicate a higher queue position. Before traffic in a lower queue is sent, it must wait for traffic in higher queues to be sent.

8. 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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the **Go** button.
   The System Information page displays.

6. Select **QoS > CoS > Advanced > DSCP to Queue Mapping**.

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, besides other DSCP experimental values, are as follows:
   - **Class Selector (CS) PHB**. These values are based on IP precedence.
   - **Assured Forwarding (AF) PHB**. These values define four main levels to sort and manipulate some flows within the network.
   - **Expedited Forwarding (EF) PHB**. These values are used to prioritize traffic for real-time applications. In many situations, if the network exceeded traffic and you need some bandwidth guaranteed for an application, the EF traffic must receive this rate independently of the intensity of any other traffic attempting to transit the node.

   The Other DSCP Values (Local/Experimental Use) section allows you to set non-default values for advanced settings.

8. Click the **Apply** button.
   Your settings are saved.
Manage Differentiated Services

The QoS feature contains Differentiated Services (DiffServ) support that allows traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors.

Standard IP-based networks provide best-effort data delivery service. Best-effort service implies that the network delivers the data in a timely fashion, although there is no guarantee. If congestion occurs, packets might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email and file transfers, a slight degradation in service is acceptable and in many cases unnoticeable. However, any degradation of service can negatively affect applications with strict timing requirements, such as voice and multimedia.

Defining DiffServ

To use DiffServ for QoS, you must first define the following categories and their criteria:

1. **Class.** Create classes and define class criteria.
2. **Policy.** Create policies, associate classes with policies, and define policy statements.
3. **Service.** Add a policy to an inbound interface.

Packets are classified and processed based on defined criteria. The classification criteria are defined by a class. The processing is defined by a policy’s attributes. Policy attributes can be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs. A policy can contain multiples classes. When the policy is active, the actions taken depend on which class matches the packet.

Note the following about the DiffServ process:

- Packets are filtered and processed based on defined criteria. The filtering criteria is defined by a class. The processing is defined by a policy's attributes. Policy attributes can be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs.
- The configuration process begins with defining one or more match criteria for a class. Then one or more classes are added to a policy. Policies are then added to interfaces.
- Packet processing begins by testing the match criteria for a packet. The **All** class type option specifies that each match criteria within a class must evaluate to true for a packet to match that class. The **Any** class type option specifies that at least one match criteria must evaluate to true for a packet to match that class. Classes are tested in the order in which they were added to the policy. A policy is applied to a packet when a class match within that policy is found.
Configure 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

6. Select QoS > DiffServ > Basic > DiffServ Configuration.
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 page.

**Table 41. DiffServ Status information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Table</td>
<td>The number of configured DiffServ classes out of the total allowed on the switch.</td>
</tr>
<tr>
<td>Class Rule table</td>
<td>The number of configured class rules out of the total allowed on the switch.</td>
</tr>
<tr>
<td>Policy table</td>
<td>The number of configured policies out of the total allowed on the switch.</td>
</tr>
<tr>
<td>Policy Instance Table</td>
<td>The number of configured policy class instances out of the total allowed on the switch.</td>
</tr>
<tr>
<td>Policy Attributes Table</td>
<td>The number of configured policy attributes (attached to the policy class instances) out of the total allowed on the switch.</td>
</tr>
<tr>
<td>Service Table</td>
<td>The number of configured services (attached to the policies on specified interfaces) out of the total allowed on the switch.</td>
</tr>
</tbody>
</table>

**Configure a DiffServ class**

You can add a new DiffServ class name or rename or delete an existing class. You can also define the criteria to associate with a DiffServ class. As packets are received, these DiffServ classes are used to prioritize packets. You can set up multiple match criteria in a class. The logic is a Boolean logical AND for this criteria. After creating a class, click the class link to the Class page.

**Add and configure a DiffServ class**

**To add and configure a DiffServ class:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see **Access the switch on-network and connected to the Internet on page 19** or **Access the switch off-network and not connected to the Internet on page 27**.
   The Device UI login page displays.
If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

6. Select QoS > DiffServ > Advanced > Class Configuration.

   The Class Name page displays.

7. In the Class Name field, enter a class name.

   The Class Name field also lists all existing DiffServ class names, from which you can select one for modification or deletion. The class name can be 1 to 31 alphanumeric characters in length.

   The switch supports only the class type value All, which means that all the various match criteria defined for the class are satisfied for a packet match. All signifies the logical AND statement of all the match criteria. For any class that you add, the class type is All.

8. Click the Add button.

   The new class is added.

9. After creating the class, click the class name.

   The class name is a hyperlink to the page on which you can define the class configuration.
10. Define the criteria that must be associated the DiffServ class by selecting one of the following radio buttons:

- **Match Every.** Select this radio button to add a match condition that considers all packets to belong to the class. The only selection from the Match Every menu is Any.

- **Reference Class.** Select this radio button to reference another class for criteria. The match criteria defined in the reference class function as match criteria in addition to the match criteria that you define for the selected class. After you select the radio button, the classes that can be referenced are displayed. Select the class to reference. A class can reference only one other class of the same type.

- **Class of Service.** Select this radio button to require the Class of Service (CoS) value in an Ethernet frame header to match the specified CoS value. This option lists all the values for the Class of Service match criterion in the range 0 to 7 from which you can select one.

- **VLAN.** Select this radio button to require a packet’s VLAN ID to match a VLAN ID. The VLAN value is in the range from 1 to 4093.
• **Ethernet Type.** Select this radio button to require the EtherType value in the Ethernet frame header to match the specified EtherType value. After you select the radio button, select the EtherType keyword from the menu of common protocols that are mapped to their Ethertype value. You can also select User Value from the menu and enter a value in the hexadecimal range from 600 to ffff.

• **Source MAC.** Select this radio button to require a packet’s source MAC address to match the specified MAC address. After you select this radio button, use the following fields to configure the source MAC address match criteria:
  - **Address.** The source MAC address to match. The source MAC address is specified as six two-digit hexadecimal numbers separated by colons.
  - **Mask.** The MAC mask, which specifies the bits in the source MAC address to compare against the Ethernet frame. Use Fs and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.

• **Destination MAC.** Select this radio button to require a packet’s destination MAC address to match the specified MAC address. After you select the radio button, use the following fields to configure the destination MAC address match criteria:
  - **Address.** The destination MAC address to match. The destination MAC address is specified as six two-digit hexadecimal numbers separated by colons.
  - **Mask.** The MAC mask, which specifies the bits in the destination MAC address to compare against an Ethernet frame. Use Fs and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.

• **Protocol Type.** Select this radio button to require a packet’s Layer 4 protocol to match the specified protocol, which you must select from the menu. You can also select Other from the menu and enter a protocol number from 0 to 255.

• **Source IP.** Select this radio button to require a packet’s source IP address to match the specified IP address. After you select the radio button, use the following fields to configure the source IP address match criteria:
  - **Address.** The source IP address format to match in dotted-decimal.
  - **Mask.** The bit mask in IP dotted-decimal format indicating which parts of the source IP address to use for matching against packet content.

• **Source L4 Port.** Select this radio button to require a packet’s TCP/UDP source port to match the specified protocol, which you must select from the menu. You can also select Other from the menu and enter a port number from 0 to 65535.

• **Destination IP.** Select this radio button to require a packet’s destination IP address to match the specified IP address.
After you select the radio button, use the following fields to configure the destination IP address match criteria:

- **Address.** The destination IP address format to match in dotted-decimal.
- **Mask.** The bit mask in IP dotted-decimal format indicating which parts of the destination IP address to use for matching against packet content.

**• Destination L4 Port.** Select this radio button to require a packet’s TCP/UDP destination port to match the specified protocol. You can also select **Other** from the menu and enter a port number from 0 to 65535.

**• IP DSCP.** Select this radio button to require the packet’s IP DiffServ Code Point (DSCP) value to match the specified IP DSCP keyword code, which you must select from the menu. You can also select **Other** from the menu and enter an IP DSCP value from 0 to 63. The DSCP value is defined as the high-order 6 bits of the Service Type octet in the IP header.

**• Precedence Value.** Select this radio button to require the packet’s IP precedence value to match the specified number from 0 to 7, which you must select from the menu. The IP Precedence field in a packet is defined as the high-order 3 bits of the Service Type octet in the IP header.

**• IP ToS.** Select this radio button to require the packet’s Type of Service (ToS) bits in the IP header to match the specified value. The IP ToS field in a packet is defined as all 8 bits of the service type octet in the IP header. After you select the radio button, use the following fields to configure the ToS match criteria:

- **Bits Value.** Enter a two-digit hexadecimal number octet value in the range from 00 to ff to match the bits in a packet’s ToS field.
- **Bit Mask.** Specify the bit positions that are used for comparison against the IP ToS field in a packet.

11. Click the **Apply** button.

Your settings are saved.

The following table describes the nonconfigurable information on the page.

**Table 42. DiffServ Class Configuration, Class Summary information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match Criteria</td>
<td>The configured match criteria for the specified class.</td>
</tr>
<tr>
<td>Values</td>
<td>The values of the configured match criteria.</td>
</tr>
</tbody>
</table>

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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
Configure Quality of Service

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

• Enter your device admin password.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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 19** or **Access the switch off-network and not connected to the Internet on page 27**.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see **Register the switch on page 30**.

4. Enter one of the following passwords:

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

   For information about the credentials, see **Credentials for the device UI on page 28**.

5. Click the **Go** button.

   The System Information page displays.

6. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.
The IPv6 Class Name 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.

The class name is a hyperlink to the page on which you can define the class configuration.

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 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 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 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.

- **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 nonconfigurable information that is displayed in the Class Summary section.

**Table 43. IPv6 DiffServ class configuration class summary**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match Criteria</td>
<td>The configured match criteria for the specified class.</td>
</tr>
<tr>
<td>Values</td>
<td>The values of the configured match criteria.</td>
</tr>
</tbody>
</table>
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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   The IPv6 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 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   The IPv6 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

   • Enter your device admin password.
If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location. For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   The IPv6 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 one or more 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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
     For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.
   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, 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.
    The policy name is a hyperlink to the page on which you can define the policy attributes.

11. Configure the policy attributes by selecting one of the following radio buttons:
    - **Assign Queue**. Select this radio button to specify that traffic must be assigned to a queue, which you must select from the menu. The queue is expressed as a value in the range from 0 to 7.
    - **Drop**. Select this radio button to require each inbound packet to be dropped.
    - **Mark VLAN CoS**. Select this radio button to specify the VLAN priority, which you must select from the menu. The VLAN priority is expressed as a value in the range from 0 to 7.
• **Mark IP Precedence.** Select this radio button to require packets to be marked with an IP precedence value before being forwarded. You must select an IP precedence value from 0 to 7 from the menu.

• **Mirror.** Select this radio button to require packets to be mirrored to an interface or LAG, one of which you must select from the menu.

• **Redirect.** Select this radio button to require packets to be redirected to an interface or LAG, one of which you must select from the menu.

• **Mark IP DSCP.** Select this radio button to require packet to be marked with an IP DSCP keyword code, which you must select from the menu. The DSCP value is defined as the high-order 6 bits of the Service Type octet in the IP header.

• **Simple Policy.** Select this radio button to define the traffic policing style for the class. By default, this simple policy is color blind, and color classes do not apply. A simple policy supports a single data rate and results in one of two outcomes: conform or violate. Packets that violate the policy are always dropped. That is, you cannot specify any other action for those packets. You must specify a policy action for packets that conform to the policy.
  - **Committed Rate.** Enter the committed rate that is applied to conforming packets by specifying a value in the range from 16 to 1000000 Kbps.
  - In the Conform Action section, select one of the following radio buttons:
    • **Send.** Packets are forwarded unmodified. This is the default confirming action.
    • **Drop.** Packets are dropped. This is the default (and only) violating action.
    • **Mark CoS.** Packets are marked by DiffServ with the specified CoS value before being forwarded. This selection requires that the Mark CoS field is set. You must select a CoS value from 0 to 7 from the menu.
    • **Mark IP Precedence.** These packets are marked by DiffServ with the specified IP Precedence value before being forwarded. This selection requires that the Mark IP Precedence field is set. You must select an IP precedence value from 0 to 7 from the menu.
    • **Mark IP DSCP.** Packets are marked by DiffServ with the specified DSCP value before being forwarded. This selection requires that the DSCP field is set. You must either select a DSCP code from the menu or enter an IP DSCP value from 0 to 63 in the field next to the menu. A value that you enter in the field overrides any selection from the menu. The DSCP value is defined as the high-order six bits of the Service Type octet in the IP header.

12. Click the **Apply** button.

   Your settings are saved.

**Rename an existing DiffServ policy**

**To rename an existing DiffServ policy:**

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

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.
   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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.

   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 from the Member Class menu.
   - To remove the class, select None, from the Member Class menu.

9. Click the Apply button.
   Your settings are saved.

Delete a DiffServ policy

To delete a DiffServ policy:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   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 assign (attach) a policy to an interface.

Attach a DiffServ policy to an interface

To attach a DiffServ policy to an interface:

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

2. Launch a web browser.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   ![Service Interface Configuration](image)

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.
Configure Quality of Service

24-Port Gigabit (Hi-Power) PoE+ Ethernet Smart Managed Pro Switch with 2 SFP Ports

- **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 In Name** menu, select a policy name.

10. Click the **Apply** button.
    
    Your settings are saved.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direction</td>
<td>Shows the traffic direction of this service interface, which is always inbound (In).</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Shows the operational status of this service interface (either Up or Down). The operational status is shown as Up if all of the following conditions are true: The attached class is valid and includes at least one matching rule. The attached policy is valid and includes at least one attribute. The port is enabled, that is, the physical link of the port is in the up state.</td>
</tr>
</tbody>
</table>

**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 19 or Access the switch off-network and not connected to the Internet on page 27.
   
   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.
   The Service Interface Configuration page displays.

6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   • 1 (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   • LAG. Only LAGs are displayed.
   • All. Both physical interfaces and LAGs are displayed.

7. Select the check box for the interface.

8. From the Policy In Name menu, select None.

9. Click the Apply button.
   Your settings are saved.

View DiffServ service statistics

You can display service-level statistical information about all interfaces to which DiffServ policies are attached.

To view the DiffServ service statistics:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
The System Information page displays.

6. Select **QoS > DiffServ > Advanced > Service Statistics**.

The Service Statistics page displays.

7. Click the **Refresh** button to refresh the page with the latest information about the switch.

The following table describes the information available on the Service Statistics page.

**Table 45. DiffServ Service Statistics information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>All valid port numbers on the switch with a DiffServ policy that is attached in the inbound direction.</td>
</tr>
<tr>
<td>Direction</td>
<td>The traffic direction of interface is inbound (In). This field shows only the direction for which a DiffServ policy is attached.</td>
</tr>
<tr>
<td>Policy Name</td>
<td>The name of the policy that is currently attached to the specified interface and direction.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The operational status of the policy that is attached to the specified interface and direction. The value is either Up or Down.</td>
</tr>
<tr>
<td>Member Classes</td>
<td>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.</td>
</tr>
</tbody>
</table>
5

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
- Manage the Smart Control Center
- Configure management access
- Control access with profiles and rules
- Configure port authentication
- Set up traffic control
- Configure access control lists
Change the device admin password for the device UI

You can change the device admin password for the user with the user name admin.

**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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   The Change Password page displays.

7. In the Current Password field, enter the current password.

   The default password is password. The password is displayed in dots.

8. In the New Password field, specify the new password.

   The password must be between 8 and 20 characters in length and must include at least one uppercase letter, one lowercase letter, and one number. The password is case-sensitive.

   The password is displayed in dots.

9. In the Confirm Password field, enter the password again to confirm that you entered it correctly.
The password is displayed in dots.

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 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


   ! CAUTION:

   The maximum delay in receiving a RADIUS response on the switch equals the maximum number of retransmissions multiplied by the time-out period multiplied by the number of configured RADIUS servers. If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the switch receives a RADIUS response.

   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 enable or disable RADIUS accounting on the server.
   The default is Disabled.

10. Click the **Apply** button.
    Your settings are saved.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Server IP Address</td>
<td>The IP address of the current server. This field is blank if no servers are configured.</td>
</tr>
<tr>
<td>Number of Configured Servers</td>
<td>The number of configured authentication RADIUS servers. The value can range from 0 to 3.</td>
</tr>
</tbody>
</table>

**Configure a RADIUS authentication server on the switch**

You view and configure various settings for a RADIUS server configured on the switch.

**Add a primary RADIUS authentication server to the switch**

**To add a primary RADIUS authentication server to the switch and view or reset the RADIUS authentication server statistics:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information 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 that the server uses to verify the RADIUS server authentication.

The 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 one that is configured on the RADIUS server.

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 nonconfigurable information in the Statistics table on the page.

**Table 47. RADIUS authentication server statistics information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
<td>The address of the RADIUS server or the name of the RADIUS server for which the statistics are displayed.</td>
</tr>
<tr>
<td>Round Trip Time</td>
<td>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.</td>
</tr>
<tr>
<td>Access Requests</td>
<td>The number of RADIUS access-request packets sent to this server. This number does not include retransmissions.</td>
</tr>
<tr>
<td>Access Retransmissions</td>
<td>The number of RADIUS access-request packets retransmitted to this server.</td>
</tr>
<tr>
<td>Access Accepts</td>
<td>The number of RADIUS access-accept packets, including both valid and invalid packets, that were received from this server.</td>
</tr>
<tr>
<td>Access Rejects</td>
<td>The number of RADIUS access-reject packets, including both valid and invalid packets, that were received from this server.</td>
</tr>
<tr>
<td>Access Challenges</td>
<td>The number of RADIUS access-challenge packets, including both valid and invalid packets, that were received from this server.</td>
</tr>
<tr>
<td>Malformed Access Responses</td>
<td>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.</td>
</tr>
<tr>
<td>Bad Authenticators</td>
<td>The number of RADIUS access-response packets containing invalid authenticators or signature attributes received from this server.</td>
</tr>
<tr>
<td>Pending Requests</td>
<td>The number of RADIUS access-request packets destined for this server that did not yet time out or receive a response.</td>
</tr>
<tr>
<td>Timeouts</td>
<td>The number of authentication time-outs to this server.</td>
</tr>
<tr>
<td>Unknown Types</td>
<td>The number of RADIUS packets of unknown type that were received from this server on the authentication port.</td>
</tr>
<tr>
<td>Packets Dropped</td>
<td>The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.</td>
</tr>
</tbody>
</table>

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 19 or *Access the switch off-network and not connected to the Internet* on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the *Register to activate your warranty* page displays. For more information, see *Register the switch* on page 30.

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

For information about the credentials, see *Credentials for the device UI* on page 28.

5. Click the **Go** 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 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 19 or *Access the switch off-network and not connected to the Internet* on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the *Register to activate your warranty* page displays. For more information, see *Register the switch* on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   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.

9. Click the Apply button.
   Your settings are saved.

Configure a RADIUS accounting server

You can view and configure various settings for a RADIUS accounting server on the network.

Add a RADIUS accounting server to the switch

To add a RADIUS accounting server to the switch and view or clear the RADIUS accounting server statistics:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.

The System Information page displays.


The previous figure does not show the Accounting Server Statistics section.

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 that the server uses to verify the RADIUS accounting server authentication.

   The default UDP port number is 1813.

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 Apply button.

   Your settings are saved.

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

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

   Table 48. RADIUS accounting server statistics information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Server Address</td>
<td>The accounting server associated with the statistics.</td>
</tr>
<tr>
<td>Round Trip Time (secs)</td>
<td>The time interval, in hundredths of a second, between the most recent accounting-response and the accounting-request that matched it from this RADIUS accounting server.</td>
</tr>
<tr>
<td>Accounting Requests</td>
<td>The number of RADIUS accounting-request packets sent not including retransmissions.</td>
</tr>
</tbody>
</table>
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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.

   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 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 19 or Access the switch off-network and not
   connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page
   displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   The Accounting Server Configuration page displays.

7. Remove the server IP address from the Accounting Server Address field.
   Leave the field blank.

8. Click the Apply button.
   Your settings are saved. The RADIUS accounting server is removed.
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 19 or Access the switch off-network and not connected to the Internet on page 27.
   - The Device UI login page displays.
   - If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   - For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** button.
   - The System Information page displays.

6. Select **Security > Management Security > TACACS+ > TACACS+ Configuration**.
7. In the **Key String** field, specify the authentication and encryption key for TACACS+ communications between the switch and the TACACS+ server.

The range is from 0 to 128. The key must match the key configured on the TACACS+ server.

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

9. Click the **Apply** button.

Your settings are saved.

---

**Configure a TACACS+ server on the switch**

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

**To configure a TACACS+ server on the switch:**

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

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

2. Launch a web browser.

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

   If you do not know the IP address of the switch, see [Access the switch on-network and connected to the Internet](#) on page 19 or [Access the switch off-network and not connected to the Internet](#) on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see [Register the switch](#) on page 30.

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

   For information about the credentials, see [Credentials for the device UI](#) on page 28.

5. Click the **Go** button.

   The System Information page displays.
6. Select **Security > Management Security > TACACS+ > TACACS+ Server Configuration**.

<table>
<thead>
<tr>
<th>TACACS+ Server</th>
<th>Priority (0 to 65535)</th>
<th>Port (0 to 65535)</th>
<th>Key String</th>
<th>Connection Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>49</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 range is from 0 to 65535.

9. In the **Port** field, specify the authentication port value for TACAS+ server sessions.

   The value must be in the range from 0 to 65535. If you do not specify a value, the switch uses the standard TCP port 49 for sessions with the server.

10. In the **Key String** field, specify the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server.

    The range is from 0 to 128. The key must match the key used on the TACACS+ server.

11. In the **Connection Timeout** field, specify the time that passes before the connection between the device and the TACACS+ server times out.

    The range is from 1 to 30. If you do not specify a value, the switch uses a default value of 5 seconds.

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 19* or *Access the switch off-network and not connected to the Internet on page 27*.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see *Register the switch on page 30*. 
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

   The System Information 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. This is the default method. This is the default selection for Method 1.

   - **RADIUS**. The user’s ID and password are authenticated using the RADIUS server. If you select **RADIUS** or **Tacacs+** as the first method and an error occurs during the authentication, the switch uses Method 2 to authenticate the user.

   - **Tacacs+**. The user’s ID and password are authenticated using the TACACS+ server. If you select **RADIUS** or **Tacacs+** as the first method and an error occurs during the authentication, the switch attempts user authentication Method 2.

   - **None**. The authentication method is unspecified, that is, no authentication is required.

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information 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. This is the default selection for Method 1.
• **RADIUS.** The user’s ID and password are authenticated using the RADIUS server. If you select RADIUS or Tacacs+ as the first method and an error occurs during the authentication, the switch uses Method 2 to authenticate the user.

• **Tacacs+.** The user’s ID and password are authenticated using the TACACS+ server. If you select RADIUS or Tacacs+ as the first method and an error occurs during the authentication, the switch attempts user authentication Method 2.

• **None.** The authentication method is unspecified, that is, no authentication is required.

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


The Dot1x Authentication List page displays.

7. Select the check box next to dot1xList.

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:

• Radius. The user’s ID and password are authenticated using the RADIUS server instead of locally.

• None. The user is not authenticated.

9. Click the Apply button.

Your settings are saved.

Manage the Smart Control Center

By default, the configuration option of the Smart Control Center (SCC) is disabled. You still can use the SCC to discover the IP address of the switch, but you cannot use the SCC to perform any actions on the switch. If you enable the configuration option of the SCC, you can use it to configure the switch.

For more information about the SCC, visit netgear.com/support/product/SCC.

Note: The device admin password is contained in many NETGEAR Switch Discovery Protocol (NSDP) packet. Therefore, to increase the switch security, the configuration option of the SCC is disabled by default.

To enable or disable the configuration option of the SCC:

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

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   The NETGEAR Smart Control Center (SCC) Utility page displays.

7. Select the one of the following SCC Admin Mode radio buttons:
   • Enable. The SCC can discover the switch and perform actions on the switch.
   • Disable. The SCC can discover the switch but cannot perform any actions on the switch. This is the default setting.

8. 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 HTTP access 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


7. Select the Admin Mode Enable or Disable radio button.

   This selection 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 from 0 to 60 minutes. The default value is 5 minutes.

   After the session is inactive for the configured time, you are automatically logged out and must reenter the password to access the 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 from 0 to 168 hours. A 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 range is from 1 to 4 sessions. The default is 4 sessions.
11. Click the **Apply** button.

Your settings are saved.

---

**Configure HTTPS access settings**

Secure HTTP (HTTPS) enables the transmission of HTTP over an encrypted Secure Sockets Layer (SSL) 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](#) or [Access the switch off-network and not connected to the Internet](#).

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see [Register the switch](#).

4. Enter one of the following passwords:

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

   For information about the credentials, see [Credentials for the device UI](#).

5. Click the **Go** button.

   The System Information page displays.

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

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

9. In the **HTTPS Session Soft Timeout (Minutes)** field, enter the inactivity time-out for HTTPS sessions.
   The range is from 1 to 60 minutes. The default value is 5 minutes.

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 range is from 1 to 168 hours. The default is 24 hours.

11. In the **Maximum Number of HTTPS Sessions** field, enter the maximum allowable number of HTTPS sessions.
    The range is from 1 to 4 sessions. The default is 4 sessions.

12. Click the **Apply** button.
    Your settings are saved.

### Browser security warning with HTTPS access

After you enable HTTPS access (see **Configure HTTP access settings on page 260**) and you attempt to access the device UI, your browser might display a security warning that your connection is not private or not secure, or that a problem with the security certificate occurred.

If such a security warning displays, you cannot proceed but must take one of the following actions, depending on the browser that you are using:

- **Google Chrome:** If Google Chrome displays a *Your connection is not private* warning, 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:** If Apple Safari displays a *This connection is not private* warning, 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:** If Mozilla Firefox displays a *Your connection is not secure* warning, click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that displays, click the **Confirm Security Exception** button.

- **Microsoft Internet Explorer:** If Microsoft Internet Explorer displays a *There is a problem with this website’s security certificate* warning, click the **Continue to this website (not recommended)**.
• **Microsoft Edge:** If Microsoft Edge displays a *There is a problem with this website’s security certificate* warning or a similar warning, select **Details > Go on to the webpage**.

For information about installing a specific security certificate on the switch, see Manage certificates for HTTPS access on page 264 and Use an HTTP session to download and install an SSL security certificate file on the switch on page 388.

## Manage certificates for HTTPS access

You can manage certificates for HTTPS access.

### Generate an SSL certificate

---

**Note:** Before you can generate a certificate, you must disable HTTPS (see Configure HTTPS access settings on page 262) 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 19** or **Access the switch off-network and not connected to the Internet on page 27**.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see **Register the switch on page 30**.

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

   For information about the credentials, see **Credentials for the device UI on page 28**.

5. Click the **Go** button.

   The System Information 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 progress information.

Delete an SSL certificate

---

**Note:** Before you can delete a certificate, you must disable HTTPS (see Configure HTTPS access settings on page 262) 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information 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 from a TFTP server to the switch

You can transfer a certificate file to the switch.

---

**Note:** For information about downloading and installing an SSL certificate over an HTTP session, see Use an HTTP session to download and install an SSL security certificate file on the switch on page 388.

---

For the switch to accept HTTPS connections from a device, the switch requires a public key certificate. You can generate a certificate externally (for example, offline) and transfer it to the switch.

Before you transfer a file from a TFTP server to the switch, the following conditions must be true:

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

---

**Note:** Before you can transfer a certificate, you must disable HTTPS (see Configure HTTPS access settings on page 262) 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 configure the certificate transfer settings for HTTPS sessions:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information 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 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. From the **Server Address Type** menu, select **IPv4** or **DNS** to indicate the format for the TFTP Server IP field.
   The default is IPv4.

9. In the **TFTP Server IP** field, specify the address or host name of the TFTP server.
   The address can be an IP address in standard x.x.x.x format or a host name. The host name must start with a letter of the alphabet.

10. 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.

11. 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.

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

13. 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 377).

### 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   ![Access Profile Configuration](image)

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

   The maximum length is 32 characters.

8. Click the Apply button.

   Your settings are saved. By default, the access profile is deactivated. After you add rules, you can activate the access profile.
Add a rule to the access profile

After you add the access profile, you can add one or more security access rules to the access profile.

If you access the switch from a computer, make sure that you add a permit rule for the type of service that you use (for example, HTTPS), your computer's IP address, and your computer's subnet mask.

⚠️ **CAUTION:**

You must add a permit rule for your device and access method, otherwise you are locked out from the switch after you activate the access profile. If that situation occurs, you must reset the switch to factory default settings (see Reset the switch to its factory default settings on page 377).

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information 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 from a device that matches the rule criteria. A Deny rule blocks a device 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. Possible access methods are **TFTP**, **HTTP**, **Secure HTTP (SSL)**, and **SNMP**.

9. In the **Source IP Address** field, enter the source IP address from which the management traffic originates.

10. In the **Mask** field, specify the subnet mask from which the management traffic originates.

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 rule are ignored. For example, if a source IP address 10.10.10.10 is configured with priority 1 to permit, and the same source IP address 10.10.10.10 is also configured with priority 2 to deny, then access is permitted if the profile is active, and the second rule is ignored.

12. Click the **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 377](#)).

**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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.
   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 19 or Access the switch off-network and not connected to the Internet on page 27.
The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


The Packets Filtered field displays the number of packets filtered (none in the previous figure).

7. To refresh the page with the latest information about the switch, click the Refresh button.

The following table describes the nonconfigurable data that is displayed.

**Table 49. Access profile configuration profile summary**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Type</td>
<td>The action performed when the rules match.</td>
</tr>
<tr>
<td>Service Type</td>
<td>The service type selected. The policy is restricted by the selected service type.</td>
</tr>
<tr>
<td>Source IP Address</td>
<td>The source IP address of the client originating the management traffic.</td>
</tr>
<tr>
<td>Mask</td>
<td>The subnet mask of the IP Address.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority of the rule.</td>
</tr>
</tbody>
</table>
Deactivate an access profile

You can 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   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 274).

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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.
   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 the global 802.1X settings

You can configure global port access control settings on the switch.

To globally enable all 802.1X features:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   
   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   
   The System Information page displays.


7. Configure the following port authentication settings:
   
   • **Port Based Authentication State.** This selection specifies the 802.1X administrative mode on the switch. The default value is Disable.
     
     * **Enabled.** If 802.1X is enabled, authentication is performed by a RADIUS server. This means that the primary authentication method must be RADIUS. To set the method, select Security > Management Security > Authentication List and select RADIUS as method 1 for defaultList. For more information, see Configure authentication lists on page 255.
- **Disabled.** When port-based authentication is globally disabled, the switch does not check for 802.1X authentication before allowing traffic on any ports, even if the ports are configured to allow only authenticated users.

- **VLAN Assignment Mode.** This selection specifies whether a port can be placed in a particular VLAN. The default value is Disable.

  When enabled, this feature allows a port to be placed into a particular VLAN based on the result of the authentication or type of 802.1X authentication a client uses when it accesses the device. The authentication server can provide information to the device about which VLAN to assign the supplicant.

- **Dynamic VLAN Creation Mode.** This selection specifies whether a VLAN can be dynamically created. The default value is Disable.

  If RADIUS-assigned VLANs are enabled, the RADIUS server includes the VLAN ID in the 802.1X tunnel attributes of its response message to the device. If dynamic VLAN creation is enabled on the device and the RADIUS-assigned VLAN does not exist, the assigned VLAN is dynamically created. This means that the client can connect from any port and is assigned to the appropriate VLAN. This feature gives flexibility for clients to move around the network without much additional configuration required.

- **EAPoL Flood Mode.** This selection specifies whether Extensible Authentication Protocol (EAP) over LAN (EAPoL) flood support is enabled on the switch. The default value is Disable.

  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 19 or Access the switch off-network and not connected to the Internet on page 27.

     The Device UI login page displays.

     If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter
     the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


The previous figure does not show all columns.

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.
• **MAB.** Specify whether to enable or disable MAC-based Authentication Bypass (MAB) for 802.1x-unaware clients at the specified port. MAB only functions if the port control mode is MAC-based. By default, MAB is disabled.

• **Guest VLAN ID.** Specify the VLAN ID for the guest VLAN. The range is from 0 to 4093. The default value is 0. Enter 0 to reset the guest VLAN ID on the interface. The guest VLAN allows the port to provide a distinguished service to unauthenticated users, after three authentication failures. This feature provides a mechanism to allow users access to hosts on the guest VLAN.

• **Guest VLAN Period.** Specify the time in seconds that the selected port remains in the quiet state following a failed authentication exchange. The guest VLAN time-out must be a value in the range from 1 to 300. The default value is 90 seconds.

• **Unauthenticated VLAN ID.** Specify the VLAN ID of the unauthenticated VLAN for the selected port. The range is from 0 to 4093. 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. If you select Disable, connected clients are not forced to reauthenticate periodically. 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 from 1 to 65535. The default value is 3600 seconds.

• **Quiet Period.** Specify the time in seconds that the port remains in the quiet state following a failed authentication exchange. While in the quiet state, the port does not attempt to acquire a supplicant. The quiet state period must be a value in the range from 0 to 65535. A value of 0 means that the port remains in the quiet state and never attempts to acquire a supplicant. The default value is 60 seconds.

• **Resending EAP.** Specify the EAP retransmit period for the selected port. The retransmit period is the time in seconds, after which an EAPoL EAP Request/Identify frame is resent to the supplicant. The retransmit period must be a value in the range from 1 to 65535. The default value is 30 seconds.

• **MAX EAP Requests.** Specify the maximum number of EAP requests for the selected port. The value is the maximum number of times an EAPoL EAP Request/Identity message is retransmitted before the supplicant times out. The maximum number of EAP requests must be a value in the range from 1 to 10. The default value is 2.

• **Supplicant Timeout.** Specify the supplicant time-out for the selected port. The supplicant time-out is the time in seconds after which the supplicant times out. The supplicant time-out period must be a value in the range from 1 to 65535. The default value is 30 seconds.

• **Server Timeout.** Specify the time in seconds that elapses before the switch resends a request to the authentication server. The server time-out period must be a value in the range from 1 to 65535. The default value is 30 seconds.

10. Click the **Apply** button.

Your settings are saved.
The following table describes the port authentication status information available on the page.

### Table 50. Port authentication status information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Direction</td>
<td>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).</td>
</tr>
<tr>
<td>Protocol Version</td>
<td>The protocol version associated with the selected port. The only possible value is 1, corresponding to the first version of the 802.1X specification.</td>
</tr>
<tr>
<td>PAE Capabilities</td>
<td>The port access entity (PAE) functionality of the selected port. The option is Authenticator or Supplicant.</td>
</tr>
</tbody>
</table>
| Authenticator PAE State | The current state of the authenticator PAE state machine. The options are as follows:  
  - Initialize  
  - Disconnected  
  - Connecting  
  - Authenticating  
  - Authenticated  
  - Aborting  
  - Held  
  - ForceAuthorized  
  - ForceUnauthorized  |
| Backend State | The current state of the backend authentication state machine. The options are as follows:  
  - Request  
  - Response  
  - Success  
  - Fail  
  - Timeout  
  - Initialize  
  - Idle  |

**Initialize 802.1X on a port**

**To initialize 802.1X on a port:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   The Port Authentication page displays.

7. Select the check box for the port.

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


The Port Authentication page displays.

7. Select the check box for the port.

8. Click the Reauthenticate button.

The selected port is forced to restart the authentication process. This button is available only if the control mode is auto. If the button is not selectable, it is grayed out. When you click this button, the action is immediate. You do not need to click the Apply button for the action to occur.

View the port summary

You can view summary information about the port-based authentication settings for each port.

To view the port summary:

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

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

2. Launch a web browser.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

   • Enter your device admin password.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
The System Information page displays.


![Port Summary Table]

7. To refresh the page with the latest information about the switch, click the Refresh button.

The following table describes the fields on the Port Summary page.

### Table 51. Port summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port whose settings are displayed in the current table row.</td>
</tr>
<tr>
<td>Control Mode</td>
<td>This field indicates the configured control mode for the port. The options are as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Force Unauthorized</strong>. The authenticator port access entity (PAE) unconditionally sets the</td>
</tr>
<tr>
<td></td>
<td>controlled port to unauthorized.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Force Authorized</strong>. The authenticator PAE unconditionally sets the controlled port to</td>
</tr>
<tr>
<td></td>
<td>authorized.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>. The authenticator PAE sets the controlled port mode to reflect the outcome of</td>
</tr>
<tr>
<td></td>
<td>the authentication exchanges between the supplicant, authenticator, and the authentication</td>
</tr>
<tr>
<td></td>
<td>server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>MAC Based</strong>. The authenticator PAE sets the controlled port mode to reflect the outcome</td>
</tr>
<tr>
<td></td>
<td>of authentication exchanges between a supplicant, an authenticator, and an authentication</td>
</tr>
<tr>
<td></td>
<td>server on a per supplicant basis.</td>
</tr>
<tr>
<td>Operating Control Mode</td>
<td>The control mode under which the port is actually operating. The options are as follows:</td>
</tr>
<tr>
<td></td>
<td>• ForceUnauthorized</td>
</tr>
<tr>
<td></td>
<td>• ForceAuthorized</td>
</tr>
<tr>
<td></td>
<td>• Auto</td>
</tr>
<tr>
<td></td>
<td>• MAC Based</td>
</tr>
<tr>
<td></td>
<td>• N/A: If the port is in detached state, it cannot participate in port access control.</td>
</tr>
<tr>
<td>Reauthentication Enabled</td>
<td>This field shows whether reauthentication of the supplicant for the specified port is allowed.</td>
</tr>
<tr>
<td></td>
<td>The option is True or False. If the value is True, reauthentication occurs. Otherwise,</td>
</tr>
<tr>
<td></td>
<td>reauthentication is not allowed.</td>
</tr>
<tr>
<td>Port Status</td>
<td>The authorization status of the specified port. The options are Authorized, Unauthorized,</td>
</tr>
<tr>
<td></td>
<td>and N/A. If the port is in detached state, the value is N/A because the port cannot</td>
</tr>
<tr>
<td></td>
<td>participate in port access control.</td>
</tr>
</tbody>
</table>
View the client summary

You can view 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   The following table describes the fields on the Client Summary page.

   Table 52. Client Summary information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port to be displayed.</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name representing the identity of the supplicant device.</td>
</tr>
<tr>
<td>Supplicant MAC Address</td>
<td>The supplicant’s device MAC address.</td>
</tr>
<tr>
<td>Session Time</td>
<td>The time since the supplicant logged in seconds.</td>
</tr>
</tbody>
</table>
Set up traffic control

You can configure MAC filters, storm control, port security, and protected port settings.

Manage MAC filtering

You can create MAC filters that limit the traffic allowed into and out of specified ports on the switch.

Create a MAC filter

If a packet with a MAC address and VLAN ID that you specify for a filter is received on a port that is not part of the inbound filter, the packet is dropped.

A packet with a MAC address and VLAN ID that you specify for a filter can be transmitted only from a port that is part of the outbound filter.

To create a MAC filter:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   
   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter ID</td>
<td>The policy filter ID assigned by the authenticator to the supplicant device.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID assigned by the authenticator to the supplicant device.</td>
</tr>
<tr>
<td>VLAN Assigned</td>
<td>The reason for the VLAN ID assigned by the authenticator to the supplicant device.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>The session time-out imposed by the RADIUS server on the supplicant device.</td>
</tr>
<tr>
<td>Termination Action</td>
<td>The termination action imposed by the RADIUS server on the supplicant device.</td>
</tr>
</tbody>
</table>
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

6. Select **Security > Traffic Control > MAC Filter > MAC Filter Configuration.**

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.
   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. A multicast filter is determined by the MAC address that you enter in the MAC Address field.

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 19* or *Access the switch off-network and not connected to the Internet on page 27*.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see *Register the switch on page 30*.

4. Enter one of the following passwords:

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

   For information about the credentials, see *Credentials for the device UI on page 28*.

5. Click the **Go** 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** button.

   The System Information page displays.

6. Select **Security > Traffic Control > MAC Filter > MAC Filter Summary**.

   The following table describes the information displayed on the page.

   **Table 53. MAC Filter Summary information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>The MAC address of the filter in the format XX:XX:XX:XX:XX:XX.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID used with the MAC address to fully identify packets you want filtered.</td>
</tr>
</tbody>
</table>
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 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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.
6. Select **Security > Traffic Control > Storm Control**.

![Storm Control Interface]

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** button.
   
   The System Information page displays.

6. Select **Security > Traffic Control > Storm Control.**
The default settings in the Port Settings section depends on the global storm control settings (see Configure global storm control settings on page 289), 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%.

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.
Configure 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information 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.

By default, port security is disabled for individual ports.

**Note:** After you enable port security for individual ports (see Configure a port security interface on page 294), you can return to this page and click the **Refresh** button to refresh the page with the latest information about the ports.

The Port Security Violations table shows information about violations that occurred on ports that are enabled for port security.

The following table describes the fields in the Port Security Violations table.

**Table 54. Port Security Violations information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The physical interface.</td>
</tr>
<tr>
<td>Last Violation MAC</td>
<td>The source MAC address of the last packet that was discarded at a locked port.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID corresponding to the last MAC address violation.</td>
</tr>
</tbody>
</table>

Configure a port security interface

A MAC address can be defined as allowed on a port by one of two methods: dynamically or statically. Both methods can occur concurrently when a port is locked.

Dynamic locking implements a first arrival mechanism for port security. You specify how many addresses can be learned on the locked port. If the limit is not reached, a packet with an unknown source MAC address is learned and forwarded normally. If the limit is reached, no more addresses are learned on the port. Any packets with source MAC addresses that were not already learned are dropped.

Static locking allows you to specify a list of MAC addresses that are allowed on a port. The behavior of packets is the same as for dynamic locking: only packets with an allowable source MAC address can be forwarded.

**To configure port security settings:**

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

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information 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 on the selected interfaces. The default is 4096. If you specify 0, the selected interfaces do not learn any MAC addresses.

• **Max Static MAC Address.** Specify the maximum number of statically locked MAC addresses on the selected interfaces. The default is 48.

• **Enable Violation Shutdown.** Enable or disable shutdown of the selected interfaces if a packet with a disallowed MAC address is received. The default value is No, which means that the option is disabled.

• **Enable Violation Traps.** Enable or disable the sending of new violation traps if a packet with a disallowed MAC address is received. The default value is No, which means that the option is disabled.

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 293) and enabled port security for specific interfaces (see Configure a port security interface on page 294), 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** button.
The System Information page displays.


![Port Security Settings](image)

7. From the **Port List** menu, select the individual interface.

Port security must be enabled on the selected interface.

The Dynamic MAC Address Table displays the MAC addresses and their associated VLANs that were learned on the selected port.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID corresponding to the MAC address.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC addresses learned on a specific port.</td>
</tr>
</tbody>
</table>

8. To convert the dynamically learned MAC address to a statically locked addresses, select the **Convert Dynamic Address to Static** check box.

9. Click the **Apply** button.

The dynamic MAC address entries are converted to static MAC address entries in a numerically ascending order until the static limit is reached.

The **Number of Dynamic MAC Addresses Learned** field displays the number of dynamically learned MAC addresses on a specific port.

10. To refresh the page with the latest information about the switch, click the **Refresh** button.

Configure protected ports

If you configure a port as protected, it does not forward traffic to any other protected port on the switch, but it does forward traffic to unprotected ports. You can configure the ports as protected or unprotected. By default, all ports are 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.

   In the Ports table, click each port that you want to configure as a protected port.

   Protected ports are marked with a check mark. No traffic forwarding is possible between two protected ports.
7. Click the Apply button.
   Your settings are saved.

Configure access control lists

Access control lists (ACLs) ensure that only authorized users can access specific resources while blocking any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents, decide which types of traffic are forwarded or blocked, and provide security for the network. The switch supports a total of 100 ACLs, which can be a combination of MAC ACLS, basic or extended IPv4 ACLs, and IPv6 ACLs.
To configure an ACL:

1. Create an IPv4-based, IPv6-based, or MAC-based ACL ID.
2. Create a rule and assign it to a unique ACL ID.
3. Define the rules, which can identify protocols, source, and destination IP and MAC addresses, and other packet-matching criteria.
4. Use the ID number to assign the ACL to a port or to a LAG.

To view ACL configuration examples, see Access control lists (ACLs) on page 406.

Use the ACL Wizard to create a simple ACL

The ACL Wizard helps you create a simple ACL and apply it to the selected ports easily and quickly. First, select an ACL type to use when you create an ACL. Then add an ACL rule to this ACL and apply this ACL on the selected ports.

---

**Note:** The steps in the following procedure describe how you can create an ACL based on the destination MAC address. If you select a different type of ACL (for example, an ACL based on a source IPv4), the page displays different information.

---

Use the ACL Wizard to create an ACL

**To use the ACL Wizard to create an ACL:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button. The System Information 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).

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.** Packets do not need to match the selected ACL and rule. With this selection, you can add a destination MAC address, destination MAC mask, and VLAN.
   - **True.** All packets must match the selected ACL and rule and are either permitted or denied. In this case, since all packets match the rule, the option of configuring other match criteria is not offered.

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 format is xx:xx:xx:xx:xx:xx. The BPDU keyword might be specified using a destination MAC address of 01:80:C2:xx:xx:xx.  
• **Destination MAC Mask.** Specify the destination MAC address mask, which represents the bits in the destination MAC address to compare against an Ethernet frame. The format is xx:xx:xx:xx:xx:xx. The BPDU keyword might be specified using a destination MAC mask of 00:00:00:ff:ff:ff.  
• **VLAN.** Specify the VLAN ID to match within the Ethernet frame.  
| Source MAC | • **Source MAC.** Specify the source MAC address to compare against an Ethernet frame. The format is xx:xx:xx:xx:xx:xx.  
• **Source MAC Mask.** Specify the source MAC address mask, which represents the bits in the source MAC address to compare against an Ethernet frame. The format is (xx:xx:xx:xx:xx:xx).  
• **VLAN.** Specify the VLAN ID to match within the Ethernet frame.  
| Destination IPv4 | • **Destination IP Address.** Specify the destination IP address.  
• **Destination IP Mask.** Specify the destination IP address mask.  
| Source IPv4 | • **Source IP Address.** Specify the source IP address.  
• **Source IP Mask.** Specify the source IP address mask.  
| 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.
12. As an example, the following steps describe how you can create an ACL based on the destination MAC address:

a. In the **Destination MAC** field, specify the destination MAC address that must be compared against the information in an Ethernet frame.


b. In the **Destination MAC Mask** field, specify the destination MAC address mask that must be compared against the information in an Ethernet frame.

   The format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC mask of 00:00:00:ff:ff:ff.

c. In the **VLAN ID** field, specify which VLAN must be compared against the information in an Ethernet frame.

   The range is from 1 to 4093. Either a VLAN range or VLAN can be configured.

13. In the Binding Configuration section, from the **Direction** menu, select the packet filtering direction for the ACL.

   Only the inbound direction is valid.

14. In the Ports and LAG tables in the Binding Configuration section, select the ports and LAGs to which the ACL must be applied.

15. Click the **Add** button.

   The rule is added to the ACL.

16. Click the **Apply** button.

   Your settings are saved.
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 19 or Access the switch off-network and not connected to the Internet on page 27.
   
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   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 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


The ACL Wizard page displays.

7. Select check box that is associated with the rule.

8. Click the Delete button.

   The rule is removed.

ACL Wizard Example

In the following figure, the ACL rule is configured to check for packet matches on ports 8, 10, 11, and 13 and on LAG 1. Only the Inbound option is valid. Packets that include a source address in the 192.168.3.0/16 network are forwarded by the interfaces. All other packets are dropped because every ACL includes an implicit deny all rule as the last rule.
For information about the ACL Wizard, see Use the ACL Wizard to create a simple ACL on page 299.

Configure a MAC ACL

A MAC ACL consists of a set of rules that are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit or Deny) is taken, and the additional rules are not checked for a match.

The following steps are involved in defining a MAC ACL and applying it to the switch:

1. Create a MAC ACL ID (see Configure a MAC ACL on page 305).
2. Create a MAC rule (see Configure MAC ACL rules on page 308).
3. Associate the MAC ACL with one or more interfaces (see Configure MAC bindings on page 312).

You can view or delete MAC ACL configurations in the MAC Binding table (see View or delete MAC ACL bindings in the MAC binding table on page 314).

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   
   The System Information page displays.

6. Select Security > ACL > Basic > MAC ACL.
The MAC ACL Table displays the number of ACLs currently configured in the switch and the maximum number of ACLs that can be configured. The current size is equal to the number of configured IPv4 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 19* or *Access the switch off-network and not connected to the Internet on page 27*.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see *Register the switch on page 30*.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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.
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 19* or *Access the switch off-network and not connected to the Internet on page 27*.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see *Register the switch on page 30*.

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

   For information about the credentials, see *Credentials for the device UI on page 28*.

5. Click the Go button.

   The System Information page displays.

6. Select **Security > ACL > Basic > MAC Rules**.
The previous figure does not show all columns.

7. From the **ACL Name** menu, select the MAC ACL.

8. In the **Sequence Number** field, enter a whole number in the range from 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 range for the queue ID is from 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 priority that must be compared against the information in an Ethernet frame.
    The range for the priority is from 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.

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 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 values are as follows:
    • **Apple Talk**
    • **IBM SNA**
18. If you select User Value from the EtherType Key menu, in the EtherType User Value field, specify the customized EtherType value that must be used.
   
   This value must be compared against the information in an Ethernet frame. The range is from 0x0600 to 0xFFFF.

19. In the Source MAC field, specify the source MAC address that must be compared against the information in an Ethernet frame.
   

20. In the Source MAC Mask field, specify the source MAC address mask that must be compared against the information in an Ethernet frame.
   

21. In the VLAN field, specify the VLAN ID that must be compared against the information in an Ethernet frame.
   
   The range is from 1 to 4093. You can configure either a single VLAN or a VLAN range.

22. From the Logging menu, select whether to enable or disable logging.
   
   If you select Enable, logging is enabled for this ACL rule (subject to resource availability on the switch).

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 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


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 bindings

When an ACL is bound to an interface, all the rules that are defined are applied to the selected interface. You can assign MAC ACLs to interfaces and LAGs.

To configure MAC bindings:

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

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

2. Launch a web browser.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information 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 the interface and direction is used. The range is from 1 to 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 columns in the Interface Binding Status table on the page.

Table 55.  Interface Binding Status table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface of the ACL assigned.</td>
</tr>
<tr>
<td>Direction</td>
<td>The selected packet filtering direction for the ACL.</td>
</tr>
<tr>
<td>ACL Type</td>
<td>The type of ACL assigned to the selected interface and direction.</td>
</tr>
<tr>
<td>ACL ID</td>
<td>The ACL name identifying the ACL assigned to the selected interface and direction.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.</td>
</tr>
</tbody>
</table>

View or delete MAC ACL bindings in the MAC binding table

You can view or delete the MAC ACL bindings in the MAC binding table.

To view or delete MAC ACL bindings:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

6. Select Security > ACL > Basic > MAC Binding Table.
The previous figure shows examples.

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 nonconfigurable information on the page.

Table 56. MAC Binding Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface of the ACL assigned.</td>
</tr>
<tr>
<td>Direction</td>
<td>The selected packet filtering direction for the ACL.</td>
</tr>
<tr>
<td>ACL Type</td>
<td>The type of ACL assigned to the selected interface and direction.</td>
</tr>
<tr>
<td>ACL ID</td>
<td>The ACL name identifying the ACL assigned to the selected interface and direction.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.</td>
</tr>
</tbody>
</table>

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 **Configure a basic or extended IPv4 ACL on page 315**).

   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 319 or Configure rules for an extended IPv4 ACL on page 323).

3. Associate the IPv4 ACL with one or more interfaces (see Configure IP ACL interface bindings on page 341).

You can view or delete IPv4 ACL configurations in the IP ACL Binding table (see View or delete IP ACL bindings in the IP ACL binding table on page 343).

Add an IPv4 ACL

To add an IPv4 ACL:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

6. Select Security > ACL > Advanced > IP ACL.
The previous figure shows an example.

The IP ACL page shows the current size of the ACL table compared to the maximum size of the ACL table. The current size is equal to the number of configured IPv4 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 extended IP ACL with a name string that is up to 31 alphanumeric characters in length. The name must start with an alphabetic character.

Each configured ACL displays the following information:
   • Rules. The number of rules currently configured for the IPv4 ACL.
   • Type. Identifies the ACL as a basic IP ACL (with ID from 1 to 99), extended IP ACL (with ID from 100 to 199 or a name).

8. Click the Add button.

   The IP ACL is added.

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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 IPv4 ACL

To delete 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
     For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.

![Image of IP Rules]

If no rules exist, the Basic ACL Rule Table might show the message *No rules were 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.

![Image of Standard ACL Rule Configuration]

9. Specify the following match criteria for the rule:
   - **Sequence Number**: Enter an ACL sequence number in the range from 1 to 2147483647 that is used to identify the rule. An IP ACL can contain up to 50 rules.
   - **Action**: Select the ACL forwarding action, which is one of the following:
     - **Permit**: Forward packets that meet the ACL criteria.
     - **Deny**: Drop packets that meet the ACL criteria.
   - **Logging**: If the selection from the **Action** menu is **Deny**, you can enable logging for the ACL by selecting the **Enable** radio button. (Logging is subject to resource availability on the switch.)
• **Match Every.** Select one of the radio buttons to specify whether all packets must match the selected IP ACL rule:
  - **Enable.** All packets must match the selected IP ACL rule and are either permitted or denied.
  - **Disable.** Not all packets need to match the selected IP ACL rule.
• **Interface.** Select one of the radio buttons to specify whether all packets must be mirrored or redirected:
  - **Mirror.** From the menu, select the specific egress interface to which the matching traffic stream must be copied, in addition to being forwarded normally by the switch.
  - **Redirect.** From the menu, select the egress interface to which the matching traffic stream must be redirected, bypassing any forwarding decision normally performed by the switch.
• **Source IP Address.** Enter an IP address using dotted-decimal notation to be compared to a packet’s source IP address as a match criterion for the selected IP ACL rule.
• **Source IP Mask.** Specify the IP mask in dotted-decimal notation to be used with the source IP address value.

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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. **Enter one of the following passwords:**
   • **Enter your device admin password.**
   • **If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.**
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the **Go** button.
The System Information page displays.

6. Select **Security > ACL > Advanced > IP Rules**.
The IP Rules page displays.

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 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 19 or [Access the switch off-network and not connected to the Internet](#) on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see [Register the switch](#) on page 30.

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

   For information about the credentials, see [Credentials for the device UI](#) on page 28.

5. Click the **Go** button.
The System Information page displays.

6. Select **Security > ACL > Advanced > IP Rules**.
The IP Rules page displays.

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 IPv4 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 19** or **Access the switch off-network and not connected to the Internet on page 27.**
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see **Register the switch on page 30.**

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

   For information about the credentials, see **Credentials for the device UI on page 28.**

5. **Click the **Go** button.**
   The System Information page displays.

6. **Select **Security > ACL > Advanced > IP Extended Rules.**
The previous figure does not show all columns on the page.

If no rules exist, the Extended ACL Rule Table might show the message *No rules were 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 100 to 199 or a name.

8. Click the **Add** button.

9. Configure the following match criteria for the rule:
   - **Sequence Number**. Enter a number in the range from 1 to 2147483647 that is used to identify the rule. An extended IP ACL can contain up to 50 rules.
   - **Action**. Select the ACL forwarding action, which is one of the following:
     - **Permit**. Forward packets that meet the ACL criteria.
     - **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 form the Action menu is Deny, you can enable logging for the ACL by selecting the Enable radio button. (Logging is subject to resource availability in the device.)

- **Interface.** For a Permit action, use either a mirror interface or a redirect interface:
  - Select the Mirror radio button and use the menu to specify the egress interface to which the matching traffic stream is copied, in addition to being forwarded normally by the device.
  - Select the Redirect radio button and use the menu to specify the egress interface to which the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device.

- **Match Every.** Select one of the radio buttons to specify whether all packets must match the selected IP ACL rule:
  - **False.** Not all packets need to match the selected IP ACL rule. You can configure other match criteria on the page.
  - **True.** All packets must match the selected IP ACL rule and are either permitted or denied. In this case, you cannot configure other match criteria on the page.

- **Protocol Type.** From the menu, select a protocol that a packet’s IP protocol must be matched against: IP, ICMP, IGMP, TCP, UDP, EIGRP, GRE, IPINIP, OSPF, PIM, or Other. If you select Other, enter a protocol number from 0 to 255.

- **Src.** In the Src field, enter a source IP address, using dotted-decimal notation, to be compared to a packet’s source IP address as a match criterion for the selected IP ACL rule:
  - If you select the IP Address radio button, enter an IP address or an IP address range. You can enter a relevant wildcard mask to apply this criteria. If this field is left empty, it means any.
  - If you select the Host radio button, the wildcard mask is configured as 0.0.0.0. If this field is left empty, it means any.

The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that none of the bits are important. A wildcard of 255.255.255.255 indicates that all of the bits are important.

- **Src L4.** The options are available only when the protocol is set to TCP or UDP. Use the source L4 port option to specify relevant matching conditions for L4 port numbers in the extended ACL rule.

You can select either the Port radio button or the Range radio button:

- **Port.** If you select the Port radio button, you can enter the port number yourself or select one of the following protocols from the menu:
  - The source IP TCP port protocols are domain, echo, ftp, ftpdata, www-http, smtp, telnet, pop2, pop3, and bgp.
  - The source IP UDP port protocols are domain, echo, snmp, ntp, rip, time, who, and tftp.

Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.
Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.

The only relevant matching condition for L4 port numbers is **Equal**. This means that an IP ACL rule matches only if the Layer 4 source port number is equal to the specified port number or port protocol.

- **Range**. 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 UDP port protocols are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **tftp**.

  Each of these values translates into its equivalent port number, which is used as both the start and end of the port range. Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.

  The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard of 255.255.255.255 indicates that *all* of the bits are important.

  - **Dst**. In the **Dst** field, enter a destination IP address, using dotted-decimal notation, to be compared to a packet’s destination IP address as a match criterion for the selected IP ACL rule:

    - If you select the **IP Address** radio button, enter an IP address with a relevant wildcard mask to apply this criteria. If this field is left empty, it means *any*.

    - If you select the **Host** radio button, the wildcard mask is configured as 0.0.0.0. If this field is left empty, it means *any*.

  The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard of 255.255.255.255 indicates that *all* of the bits are important.

  - **Dst L4**. The options are available only when the protocol is set to TCP or UDP. Use the destination L4 port option to specify relevant matching conditions for L4 port numbers in the extended ACL rule.
You can select either the **Port** radio button or the **Range** radio button:

- **Port.** 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 UDP port protocols are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **tftp**.

Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.

The only relevant matching condition for L4 port numbers is **Equal**. This means that an IP ACL rule matches only if the Layer 4 source port number is equal to the specified port number or port protocol.

- **Range.** 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 UDP port range names are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **tftp**.

  Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

  Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.

  The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard of 255.255.255.255 indicates that *all* of the bits are important.

- **IGMP Type.** If your selection from the **Protocol Type** menu is IGMP and you specify the IGMP type, the IP ACL rule matches the specified IGMP message type. The range is from 0 to 255. If this field is left empty, it means *any*. 
• **ICMP.** If your selection from the Protocol Type menu is ICMP, you can select either the Type or Message radio button:
  - If you select the Type radio button, note the following:
    • The Type and Code fields are enabled only if the protocol is ICMP. Use these fields to specify a match condition for ICMP packets:
      • If you specify information in the Type field, the IP ACL rule matches the specified ICMP message type. The type number can be from 0 to 255.
      • If you specify information in the Code field, the IP ACL rule matches the specified ICMP message code. The code can be from 0 to 255.
    • If these fields are left empty, it means any.
  - If you select the Message radio button, from the menu, select the type of the ICMP message to match with the selected IP ACL rule. Specifying a type of message implies that both the ICMP type and ICMP code are specified. The ICMP message is decoded into the corresponding ICMP type and ICMP code within the ICMP type.


• **Fragments.** Either select the Enable radio button to allow initial fragments (that is, the fragment bit is asserted) or leave the default Disable radio button selected to prevent initial fragments from being used.

This option is not valid for rules that match L4 information such as a TCP port number, because that information is carried in the initial packet.

• **Service Type.** Select a service type match condition for the extended IP ACL rule.

  The possible options are IP DSCP, IP precedence, and IP TOS, which are alternative methods to specify a match criterion for the same service type field in the IP header. Each method uses a different user notation. After you make a selection, you can specify the appropriate values:

  - **IP DSCP.** This is an optional configuration. Specify the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order 6 bits of the service type octet in the IP header. Enter an integer from 0 to 63. To select the IP DSCP, select one of the DSCP keywords from the menu. To specify a numeric value, select Other and a field displays in which you can enter numeric value of the DSCP.

  - **IP Precedence.** This is an optional configuration. The IP precedence field in a packet is defined as the high-order 3 bits of the service type octet in the IP header. Enter a number from 0 to 7.

  - **IP TOS.** This is an optional configuration. The IP ToS field in a packet is defined as all 8 bits of the service type octet in the IP header. The ToS bits value is a hexadecimal number that is composed of numbers 00 to 09 and AA to FF. The ToS mask value is a hexadecimal number that is composed of numbers 00 to FF.
The ToS mask denotes the bit positions in the ToS bits value that are used for comparison against the IP ToS field in a packet.

For example, to check for an IP ToS value for which bit 7 is set and is the most significant value, for which bit 5 is set, and for which bit 1 is cleared, use a ToS bits value of 0xA0 and a ToS mask of 0xFF.

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 existing 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   The IP Rules page displays.

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 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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   The IP Rules page displays.

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 331).
   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 334).

3. **Associate the IPv6 ACL with one or more interfaces** (see Configure IP ACL interface bindings on page 341).

You can view or delete IPv6 ACL configurations in the IP ACL Binding table (see View or delete IP ACL bindings in the IP ACL binding table on page 343).

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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

6. Select Security > ACL > Advanced > IPv6 ACL.
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 nonconfigurable information displayed on the page.

Table 57. IPv6 Configuration and IPv6 ACL Table information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Number of ACL</td>
<td>The current number of the IP ACLs configured on the switch.</td>
</tr>
<tr>
<td>Maximum ACL</td>
<td>The maximum number of IP ACLs that can be configured on the switch.</td>
</tr>
<tr>
<td>Rules</td>
<td>The number of the rules associated with the IP ACL.</td>
</tr>
<tr>
<td>Type</td>
<td>The type is IPv6 ACL.</td>
</tr>
</tbody>
</table>

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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.

6. Select Security > ACL > Advanced > IPv6 ACL.

   The IPv6 ACL 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

   • Enter your device admin password.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

The previous figure does not show all columns on the page.

If no rules exist, the IPv6 ACL Rule Table might show the message *No rules were configured for this ACL*. If one or more rules exist for the ACL, the rules display in the IPv6 Rules 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.

9. Configure the following match criteria for the rule:
   - **Action.** Select the ACL forwarding action by selecting one of the following radio buttons:
     - **Permit.** Forward packets that meet the ACL criteria.
     - **Deny.** Drop packets that meet the ACL criteria.
   - **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:
  - **False.** Not all packets need to match the selected IPv6 ACL rule. You can configure other match criteria on the page.
  - **True.** 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.

• **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 extended ACL rule.

  You can select either the **Port** radio button or the **Range** radio button:
  - **Port.** 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 UDP port protocols are domain, echo, snmp, ntp, rip, time, who, and tftp.

Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

Select Other from the menu to enter a port number. If you select Other from the menu but leave the field blank, it means any.

The only relevant matching condition for L4 port numbers is Equal. This means that an IPv6 ACL rule matches only if the Layer 4 source port number is equal to the specified port number or port protocol.

- Range. 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, ftpdata, www-http, smtp, telnet, pop2, pop3, and bgp.
- The source IP UDP port protocols are domain, echo, snmp, ntp, rip, time, who, and tftp.

Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

Select Other from the menu to enter 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 extended ACL rule.
You can select either the Port radio button or the Range radio button:

- **Port.** If you select the Port radio button, you can either enter the port number yourself or select one of the following protocols from the menu:
  - The destination IP TCP port protocols are `domain`, `echo`, `ftp`, `ftpdata`, `www-http`, `smtp`, `telnet`, `pop2`, `pop3`, and `bgp`.
  - The destination IP UDP port protocols are `domain`, `echo`, `snmp`, `ntp`, `rip`, `time`, `who`, and `tftp`.

Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

Select Other from the menu to enter a port number. If you select Other from the menu but leave the field blank, it means any.

The only relevant matching condition for L4 port numbers is Equal. This means that an IPv6 ACL rule matches only if the Layer 4 destination port number is equal to the specified port number or port protocol.

- **Range.** 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`, `ftpdata`, `www-http`, `smtp`, `telnet`, `pop2`, `pop3`, and `bgp`.
  - The destination IP UDP port protocols are `domain`, `echo`, `snmp`, `ntp`, `rip`, `time`, `who`, and `tftp`.

Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

Select Other from the menu to enter 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.


- **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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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.

**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 19** or **Access the switch off-network and not connected to the Internet on page 27**.
   
The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see **Register the switch on page 30**.

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

   For information about the credentials, see **Credentials for the device UI on page 28**.

5. Click the **Go** button.
   
The System Information page displays.

6. Select **Security > ACL > Advanced > IP Binding Configuration**.
7. From the **ACL ID** menu, select an existing IP ACL for which you want to add an IP ACL interface binding.

   The fixed selection from the **Direction** menu is **Inbound**, which means that 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 the interface and direction, the specified access list replaces the currently attached access list using that sequence number. If you do not specify the sequence number (meaning that the value is 0), a sequence number that is one number greater than the highest sequence number currently in use for the interface and direction is used. The range is from 1 to 4294967295.

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 nonconfigurable information on the page.

### Table 58. IP Binding Status table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The selected interface.</td>
</tr>
<tr>
<td>Direction</td>
<td>The selected packet filtering direction for the ACL, which is always Inbound.</td>
</tr>
<tr>
<td>ACL Type</td>
<td>The type of ACL assigned to the selected interface and direction.</td>
</tr>
<tr>
<td>ACL ID</td>
<td>The ACL number or name identifying the ACL assigned to the selected interface and direction.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>The sequence number signifying the order of specified ACL relative to other ACLs assigned to the selected interface and direction.</td>
</tr>
</tbody>
</table>

View or delete IP ACL bindings in the IP ACL binding table

You can view or delete bindings for basic IPv4, extended IPv4, and IPv6 ACLs.

**To view or delete IP ACL bindings:**

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

2. Launch a web browser.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

6. Select **Security > ACL > Advanced > Binding Table.**
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 fields in the IP ACL Binding Table on the page.

Table 59. IP ACL Binding Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface.</td>
</tr>
<tr>
<td>Direction</td>
<td>The selected packet filtering direction for the ACL, which is always Inbound.</td>
</tr>
<tr>
<td>ACL Type</td>
<td>The type of ACL assigned to the selected interface and direction.</td>
</tr>
<tr>
<td>ACL ID</td>
<td>The ACL number or name identifying the ACL assigned to the selected interface and direction.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.</td>
</tr>
</tbody>
</table>

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.
If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


7. In the VLAN ID field, enter the VLAN ID to which the binding must apply.

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 range is from 1 to 4294967295.

9. From the ACL Type menu, select the type of ACL.

   You can select a MAC ACL, IP ACL, or 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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   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.
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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

6. To view the switch statistics, select Monitoring > Ports > Switch Statistics.
7. Click the **Refresh** button to refresh the page with the latest information about the switch.

8. To clear all the statistics counters, click the **Clear** button.

Clearing resets all switch summary and detailed statistics to default values. However, the discarded packets count cannot be cleared.

The following table describes the switch statistics displayed on the page.

**Table 60. Switch statistics**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifIndex</td>
<td>The interface index of the interface table entry associated with the processor of this switch.</td>
</tr>
<tr>
<td>Octets Received</td>
<td>The total number of octets of data received by the processor (excluding framing bits, but including FCS octets).</td>
</tr>
<tr>
<td>Packets Received Without Errors</td>
<td>The total number of packets (including broadcast packets and multicast packets) received by the processor.</td>
</tr>
<tr>
<td>Unicast Packets Received</td>
<td>The number of subnetwork-unicast packets delivered to a higher-layer protocol.</td>
</tr>
<tr>
<td>Multicast Packets Received</td>
<td>The total number of packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.</td>
</tr>
<tr>
<td>Broadcast Packets Received</td>
<td>The total number of packets received that were directed to the broadcast address. This does not include multicast packets.</td>
</tr>
</tbody>
</table>
Table 60. Switch statistics (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive Packets Discarded</td>
<td>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.</td>
</tr>
<tr>
<td>Octets Transmitted</td>
<td>The total number of octets transmitted out of the interface, including framing characters.</td>
</tr>
<tr>
<td>Packets Transmitted Without Errors</td>
<td>The total number of packets transmitted out of the interface.</td>
</tr>
<tr>
<td>Unicast Packets Transmitted</td>
<td>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.</td>
</tr>
<tr>
<td>Multicast Packets Transmitted</td>
<td>The total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent.</td>
</tr>
<tr>
<td>Broadcast Packets Transmitted</td>
<td>The total number of packets that higher-level protocols requested be transmitted to the broadcast address, including those that were discarded or not sent.</td>
</tr>
<tr>
<td>Transmit Packets Discarded</td>
<td>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.</td>
</tr>
<tr>
<td>Most Address Entries Ever Used</td>
<td>The highest number of Forwarding Database Address Table entries that were learned by this switch since the most recent reboot.</td>
</tr>
<tr>
<td>Address Entries in Use</td>
<td>The number of learned and static entries in the Forwarding Database Address Table for this switch.</td>
</tr>
<tr>
<td>Maximum VLAN Entries</td>
<td>The maximum number of VLANs allowed on this switch.</td>
</tr>
<tr>
<td>Most VLAN Entries Ever Used</td>
<td>The largest number of VLANs that were active on this switch since the last reboot.</td>
</tr>
<tr>
<td>Static VLAN Entries</td>
<td>The number of active VLAN entries on this switch that were created statically.</td>
</tr>
<tr>
<td>VLAN Deletes</td>
<td>The number of VLANs on this switch that were created and then deleted since the last reboot.</td>
</tr>
<tr>
<td>Time Since Counters Last Cleared</td>
<td>The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.</td>
</tr>
</tbody>
</table>
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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   ![Port Statistics Table]

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 view a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   • To view multiple interfaces, select the check box associated with each interface.

The following table describes the per-port statistics displayed on the page.

**Table 61. Port statistics**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface or LAG.</td>
</tr>
<tr>
<td>Total Packets Received</td>
<td>The total number of packets received that were without errors.</td>
</tr>
<tr>
<td>Without Errors</td>
<td></td>
</tr>
<tr>
<td>Packets Received With Error</td>
<td>The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.</td>
</tr>
<tr>
<td>Broadcast Packets Received</td>
<td>The total number of good packets received that were directed to the broadcast address. This does not include multicast packets.</td>
</tr>
<tr>
<td>Packets Transmitted Without Errors</td>
<td>The number of frames without errors that were transmitted by the port.</td>
</tr>
<tr>
<td>Transmit Packet Errors</td>
<td>The number of outbound packets that could not be transmitted because of errors.</td>
</tr>
<tr>
<td>Collision Frames</td>
<td>The best estimate of the total number of collisions on this Ethernet segment.</td>
</tr>
<tr>
<td>Link Down Events</td>
<td>The total number of link down events on a physical port.</td>
</tr>
<tr>
<td>Time Since Counters Last Cleared</td>
<td>The elapsed time in days, hours, minutes, and seconds since the statistics for the port were last cleared.</td>
</tr>
</tbody>
</table>

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 19 or *Access the switch off-network and not connected to the Internet* on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see *Register the switch* on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   The Port Statistics page displays.

7. Select the check box in the heading of the table.

8. Click the Clear button.

   All counters are reset to 0.

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   The Port 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. Select one or more interfaces by taking one of the following actions:
   • To reset a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   • To reset multiple interfaces, select the check box associated with each interface.
9. Click the Clear button.
   The counters for the interface are reset to 0.

View and manage detailed port statistic

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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.
7. From the **Interface** menu, select the interface with the statistics to view.
8. From the **MST ID** menu, select the MST ID associated with the interface (if available).
9. To refresh the page with the latest information about the switch, click the **Refresh** button.
10. To clear all the counters, click the **Clear** button.

All statistics for the port are reset to the default values.

The following table describes the detailed port information that displays for a particular port.

**Table 62. Detailed port statistics**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifIndex</td>
<td>The interface or LAG.</td>
</tr>
</tbody>
</table>
| Port Type           | For normal ports, this field is displayed as blank. Otherwise, the options are as follows:  
|                     | • **Mirrored.** The port is a participating in port mirroring as a mirrored port.  
|                     | • **Probe.** The port is a participating in port mirroring as the probe port.  
|                     | • **Port Channel.** The port is a member of a LAG.                                                                                             |
| Port Channel ID     | If the port is a member of a port channel (LAG), the port channel’s interface ID and name are shown. Otherwise, Disable is shown.          |
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Role</td>
<td>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.</td>
</tr>
<tr>
<td>STP Mode</td>
<td>The Spanning Tree Protocol administrative mode that is associated with the port or port channel. The options are as follows: • <strong>Enable.</strong> Spanning tree is enabled for the port. • <strong>Disable.</strong> Spanning tree is disabled for the port.</td>
</tr>
<tr>
<td>STP State</td>
<td>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</td>
</tr>
<tr>
<td>Admin Mode</td>
<td>The port control administration state. The port must be enabled for it to be allowed into the network. The default is Enabled.</td>
</tr>
<tr>
<td>Flow Control Mode</td>
<td>Indicates whether flow control is enabled or disabled for the port. This field does not apply to LAGs.</td>
</tr>
<tr>
<td>LACP Mode</td>
<td>Indicates the Link Aggregation Control Protocol administrative state. The mode must be enabled for the port to participate in link aggregation.</td>
</tr>
<tr>
<td>Physical Mode</td>
<td>Indicates the port speed and duplex mode. In autonegotiation mode the duplex mode and speed are set from the autonegotiation process.</td>
</tr>
<tr>
<td>Physical Status</td>
<td>Indicates the port speed and duplex mode for physical interfaces.</td>
</tr>
<tr>
<td>Link Status</td>
<td>Indicates whether the link is up or down.</td>
</tr>
<tr>
<td>Link Trap</td>
<td>Indicates whether or not the port sends a trap when link status changes.</td>
</tr>
<tr>
<td>Packets RX and TX 64 Octets</td>
<td>The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets RX and TX 65-127 Octets</td>
<td>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).</td>
</tr>
<tr>
<td>Packets RX and TX 128-255 Octets</td>
<td>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).</td>
</tr>
<tr>
<td>Packets RX and TX 256-511 Octets</td>
<td>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).</td>
</tr>
</tbody>
</table>
## Table 62. Detailed port statistics (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets RX and TX 512-1023 Octets</td>
<td>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).</td>
</tr>
<tr>
<td>Packets RX and TX 1024-1518 Octets</td>
<td>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).</td>
</tr>
<tr>
<td>Octets Received</td>
<td>The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If you need greater precision, the <code>etherStatsPkts</code> and <code>etherStatsOctets</code> objects must be sampled before and after a common interval.</td>
</tr>
<tr>
<td>Packets Received 64 Octets</td>
<td>The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets Received 65-127 Octets</td>
<td>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).</td>
</tr>
<tr>
<td>Packets Received 128-255 Octets</td>
<td>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).</td>
</tr>
<tr>
<td>Packets Received 256-511 Octets</td>
<td>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).</td>
</tr>
<tr>
<td>Packets Received 512-1023 Octets</td>
<td>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).</td>
</tr>
<tr>
<td>Packets Received 1024-1518 Octets</td>
<td>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).</td>
</tr>
<tr>
<td>Packets Received &gt; 1518 Octets</td>
<td>The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.</td>
</tr>
<tr>
<td>Total Packets Received Without Errors</td>
<td>The total number of packets received that were without errors.</td>
</tr>
<tr>
<td>Unicast Packets Received</td>
<td>The number of subnetwork-unicast packets delivered to a higher-layer protocol.</td>
</tr>
<tr>
<td>Multicast Packets Received</td>
<td>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.</td>
</tr>
<tr>
<td>Broadcast Packets Received</td>
<td>The total number of good packets received that were directed to the broadcast address. This does not include multicast packets.</td>
</tr>
</tbody>
</table>
Table 62. Detailed port statistics (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive Packets Discarded</td>
<td>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.</td>
</tr>
<tr>
<td>Total Packets Received with MAC Errors</td>
<td>The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.</td>
</tr>
<tr>
<td>Jabbers Received</td>
<td>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.</td>
</tr>
<tr>
<td>Fragments Received</td>
<td>The total number of packets received that were less than 64 octets in length with ERROR CRC (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Undersize Received</td>
<td>The total number of packets received that were less than 64 octets in length with GOOD CRC (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Alignment Errors</td>
<td>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.</td>
</tr>
<tr>
<td>Rx FCS Errors</td>
<td>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.</td>
</tr>
<tr>
<td>Total Received Packets Not Forwarded</td>
<td>The number of valid frames received that were discarded (that is, filtered) by the forwarding process.</td>
</tr>
<tr>
<td>802.3x Pause Frames Received</td>
<td>The number of MAC control frames received on the interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.</td>
</tr>
<tr>
<td>Total Packets Transmitted (Octets)</td>
<td>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 you need greater precision, the etherStatsPkts and etherStatsOctets objects must be sampled before and after a common interval.</td>
</tr>
<tr>
<td>Packets Transmitted 64 Octets</td>
<td>The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets Transmitted 65-127 Octets</td>
<td>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).</td>
</tr>
<tr>
<td>Packets Transmitted 128-255 Octets</td>
<td>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).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Packets Transmitted 256-511 Octets</td>
<td>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).</td>
</tr>
<tr>
<td>Packets Transmitted 512-1023 Octets</td>
<td>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).</td>
</tr>
<tr>
<td>Packets Transmitted 1024-1518 Octets</td>
<td>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).</td>
</tr>
<tr>
<td>Packets Transmitted &gt; 1518 Octets</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Frame Size</td>
<td>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.</td>
</tr>
<tr>
<td>Total Packets Transmitted Successfully</td>
<td>The number of frames that were transmitted successfully by the port.</td>
</tr>
<tr>
<td>Unicast Packets Transmitted</td>
<td>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.</td>
</tr>
<tr>
<td>Multicast Packets Transmitted</td>
<td>The total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent.</td>
</tr>
<tr>
<td>Broadcast Packets Transmitted</td>
<td>The total number of packets that higher-level protocols requested be transmitted to the broadcast address, including those that were discarded or not sent.</td>
</tr>
<tr>
<td>Transmit Packets Discarded</td>
<td>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.</td>
</tr>
<tr>
<td>Total Transmit Errors</td>
<td>The sum of single, multiple, and excessive collisions.</td>
</tr>
<tr>
<td>Total Transmit Packets Discarded</td>
<td>The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.</td>
</tr>
<tr>
<td>Single Collision Frames</td>
<td>The number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.</td>
</tr>
<tr>
<td>Multiple Collision Frames</td>
<td>The number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.</td>
</tr>
<tr>
<td>Excessive Collision Frames</td>
<td>The number of frames for which transmission on a particular interface fails due to excessive collisions.</td>
</tr>
<tr>
<td>Dropped Transmit Frames</td>
<td>The number of transmit frames discarded at the selected port.</td>
</tr>
<tr>
<td>STP BPDUs Received</td>
<td>The number of STP BPDUs received at the selected port.</td>
</tr>
</tbody>
</table>
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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


The previous figure does not show all fields on the EAP Statistics page.

7. To refresh the page with the latest information about the switch, click the Refresh button.

8. To clear the counters, which resets the EAP and EAPoL statistics to default values, take one of the following actions:
   - To clear the counters for a specific port, select the check box associated with the port, and click the Clear button.
   - To clear the counters for multiple ports, select the check boxes associated with the ports, and click the Clear button.
   - To clear all counters for all ports, select the check box in the row heading, and click the Clear button.

Clicking the button resets all statistics for all ports to default values.

The following table describes the EAP statistics displayed on the page.

**Table 63. EAP statistics**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port number.</td>
</tr>
<tr>
<td>EAPOL Frames Received</td>
<td>The number of valid EAPoL frames of any type that were received by this authenticator.</td>
</tr>
<tr>
<td>EAPOL Frames Transmitted</td>
<td>The number of EAPoL frames of any type that were transmitted by this authenticator.</td>
</tr>
<tr>
<td>EAPOL Start Frames Received</td>
<td>The number of EAPoL start frames that were received by this authenticator.</td>
</tr>
<tr>
<td>EAPOL Logoff Frames Received</td>
<td>The number of EAPoL logoff frames that were received by this authenticator.</td>
</tr>
<tr>
<td>EAPOL Last Frame Version</td>
<td>The protocol version number carried in the most recently received EAPoL frame.</td>
</tr>
<tr>
<td>EAPOL Last Frame Source</td>
<td>The source MAC address carried in the most recently received EAPoL frame.</td>
</tr>
</tbody>
</table>
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 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

   - If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

---

**Table 63. EAP statistics**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAPOL Invalid Frames Received</td>
<td>The number of EAPoL frames that were received by this authenticator in which the frame type is not recognized.</td>
</tr>
<tr>
<td>EAPOL Length Error Frames Received</td>
<td>The number of EAPoL frames that were received by this authenticator in which the frame type is not recognized.</td>
</tr>
<tr>
<td>EAP Response/ID Frames Received</td>
<td>The number of EAP response/identity frames that were received by this authenticator.</td>
</tr>
<tr>
<td>EAP Response Frames Received</td>
<td>The number of valid EAP response frames (other than resp/ID frames) that were received by this authenticator.</td>
</tr>
<tr>
<td>EAP Request/ID Frames Transmitted</td>
<td>The number of EAP request/identity frames that were transmitted by this authenticator.</td>
</tr>
<tr>
<td>EAP Request Frames Transmitted</td>
<td>The number of EAP request frames (other than request/identity frames) that were transmitted by this authenticator.</td>
</tr>
</tbody>
</table>
6. Select **Monitoring > Ports > Cable Test**.

7. Select one or more interfaces by taking one of the following actions:
   - To test 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 test multiple interfaces, select the check box associated with each interface.
   - To test all interfaces, select the check box in the heading row.

8. Select the check boxes that are associated with the physical ports for which you want to test the cables.

9. Click the **Apply** button.

   A cable test is performed on all selected ports. The cable test might take up to two seconds to complete. If the port forms an active link with a device, the cable status is always Normal. The test returns a cable length estimate if this feature is supported by the PHY for the current link speed. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter then the cable status might be Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded.

The following table describes the nonconfigurable information on the page.

**Table 64. Cable Test information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cable Status</strong></td>
<td>Indicates the cable status:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Normal</strong>. The cable is working correctly.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Open</strong>. The cable is disconnected or a faulty connector exists.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Short</strong>. An electrical short exists in the cable.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Cable Test Failed</strong>. The cable status could not be determined. The cable might in fact be working.</td>
</tr>
<tr>
<td></td>
<td>• <strong>No cable</strong>. The cable is not present or too short to test.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Untested</strong>. The cable is not yet tested.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Port Disabled</strong>. The port is disabled.</td>
</tr>
<tr>
<td><strong>Cable Length</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Failure Location</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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 log

The memory log stores messages in memory based upon the settings for message component and severity. You can set the administrative status and behavior of logs in the system buffer. These log messages are cleared when the switch reboots.

To manage and 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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.

   The Memory Log page displays.
7. Select one of the following Admin Status radio buttons:
   - **Enable.** Enable system logging. This is the default setting.
   - **Disable.** Prevent the system from logging messages.

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 Full.** When the buffer is full, the system stops logging new messages and preserves all existing log messages.

9. From the **Severity Filter** menu, select the logging level for messages that must be logged.
   Log messages with the selected severity level and all log messages of greater severity are logged. For example, if you select **Warning**, the logged messages include Warning, Error, Critical, Alert, and Emergency. The default severity level is Informational (6).

   The severity can be one of the following levels:
   - **Emergency (0).** System is unusable.
   - **Alert (1).** Action must be taken immediately.
   - **Critical (2).** Critical conditions.
   - **Error (3).** Error conditions.
   - **Warning (4).** Warning conditions.
   - **Notice (5).** Normal but significant conditions.
   - **Informational (6).** Informational messages. This is the default setting.
   - **Debug (7).** Debug-level messages.

   **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. Up to 450 of the most recent entries can be displayed.

    The rest of the page displays the Memory Log messages. The format of the log message is the same for messages that are displayed for the message log, persistent log, or console log. Messages logged to a collector or relay through syslog support the same format as well.

    The following example shows the standard format for a log message:

    *Jan 01 2018 00:00:18: AAA-5-CONNECT: New http connection for user admin, source 192.168.1.111 ACCEPTED*

    The message was generated by component AAA on January 1, 2018 at 00:00:18 a.m. with severity 5 (Notice). The message indicates that the administrator logged on to the HTTP management interface from a host with IP address 192.168.1.111.
11. To refresh the page with the latest information about the switch, 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, it 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** 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 logged.
Log messages with the selected severity level and all log messages of greater severity are logged. For example, if you select **Warning**, the logged messages include Warning, Error, Critical, Alert, and Emergency. The default severity level is Error (3).

The severity can be one of the following levels:

- **Emergency** (0). The highest warning level. If the device is down, or not functioning properly, an emergency log message is saved to the device.
- **Alert** (1). The second-highest warning level. An alert log message is saved if a serious device malfunction occurs, such as all device features being down. Action must be taken immediately.
- **Critical** (2). The third-highest warning level. A critical log message is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
- **Error** (3). A device error occurred, such as a port being offline. This is the default setting.
- **Warning** (4). The lowest level of a device warning.
- **Notice** (5). Normal but significant conditions. Provides the network administrators with device information.
- **Informational** (6). Provides device information.
- **Debug** (7). Provides detailed information about the device.

9. From the **Logs to be Displayed** menu, select one of the following options:

- **Current Logs**. The log messages for the current switch session are displayed. This is the default setting.
- **Previous Logs**. The previous log messages are displayed, that is, the log messages that are still in the flash memory from before the switch was rebooted.

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.

*Jan 01 2018 00:00:18: AAA-5-CONNECT: New http connection for user admin, source 192.168.1.111 ACCEPTED

The message was generated by component AAA on January 1, 2018 at 00:00:18 a.m. with severity 5 (Notice). The message indicates that the administrator logged on to the HTTP management interface from a host with IP address 192.168.1.111.

Manage the server log

You can let the switch send log messages to remote logging hosts. A remote log server is the same as a remote syslog host.

You must enable the server log on the switch and specify one or more remote syslog hosts.
Enable the server log and add a remote syslog host

**To enable the server log and add a remote syslog host:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see [Access the switch on-network and connected to the Internet on page 19](#) or [Access the switch off-network and not connected to the Internet on page 27](#).
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see [Register the switch on page 30](#).

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see [Credentials for the device UI on page 28](#).

5. Click the **Go** button.
   The System Information page displays.

6. Select **Monitoring > Logs > Server Log**.
   The Server Log page displays.

7. In the Server Log Configuration section, select one of the following Admin Status radio buttons:
   - **Enable**. Send log messages to all configured hosts (syslog collectors or relays) using the values configured for each host.
   - **Disable**. Stop logging to all syslog hosts. **Disable** means no messages are sent to any collector or relay.

8. Click the **Apply** button.
   Your settings are saved.

9. 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.
Monitor the System User Manual

- **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** (0). The highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
  - **Alert** (1). The second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
  - **Critical** (2). The third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
  - **Error** (3). A device error occurred, such as a port being offline.
  - **Warning** (4). The lowest level of a device warning.
  - **Notice** (5). Provides the network administrators with device information.
  - **Informational** (6). Provides device information.
  - **Debug** (7). Provides detailed information about the log.

10. Click the **Add** button.

   The remote syslog host is added.

   The Status field in the Server Configuration table shows whether the remote logging host is currently active.

**Modify the settings for a remote syslog host**

**To modify the settings for a remote syslog host:**

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

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

2. Launch a web browser.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


The Server Log Configuration page displays.

7. 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   The Server Log Configuration page displays.

7. 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 counter

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   ![Trap Logs Table]

7. To clear all counters, click the Clear button.

   All statistics for the trap logs are reset to their default values.
8. To refresh the page with the latest information about the switch, click the **Refresh** button.

9. To clear the messages from the trap logs in the memory and clear the counters, click the **Clear** button.

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

**Table 65. Trap Logs information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Traps Since Last</td>
<td>The number of traps that occurred since the switch last rebooted.</td>
</tr>
<tr>
<td>Reset</td>
<td></td>
</tr>
<tr>
<td>Trap Log Capacity</td>
<td>The maximum number of traps stored in the log. If the number of traps exceeds</td>
</tr>
<tr>
<td></td>
<td>the capacity, the entries overwrite the oldest entries.</td>
</tr>
<tr>
<td>Number of Traps since log</td>
<td>The number of traps that occurred since the traps were last displayed.</td>
</tr>
<tr>
<td>last viewed</td>
<td>Displaying the traps by any method (terminal interface display, web display,</td>
</tr>
<tr>
<td></td>
<td>upload file from switch, and so on) causes this counter to be cleared to 0.</td>
</tr>
<tr>
<td>Log</td>
<td>The sequence number of the trap.</td>
</tr>
<tr>
<td>System Up Time</td>
<td>The time when this trap occurred, expressed in days, hours, minutes, and</td>
</tr>
<tr>
<td></td>
<td>seconds, since the last reboot of the switch.</td>
</tr>
<tr>
<td>Trap</td>
<td>Information describing the trap.</td>
</tr>
</tbody>
</table>

**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 19 or Access the switch off-network and not connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.

6. Select Monitoring > Mirroring > Port Mirroring.

   ![Port Mirroring Configuration](image)

7. Select an Admin Mode radio button:
   • Disable. Port mirroring is disabled. This is the default setting.
   • Enabled. Port mirroring is enabled.

8. From the Destination Port menu, select the physical destination port to which port traffic must be copied.

   You can configure one destination port only. The port functions as a probe port and receives traffic from all configured source ports. If no port is configured, None is displayed. The default is None.

9. Click the Apply button.

   Your settings are saved.
In the Source Interface Configuration section, perform the following steps.

10. Select whether to display physical interfaces, LAGs, the CPU, or all by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **CPU**. Only the CPU is displayed.
   - **All**. The physical interfaces, LAGs, and CPU are displayed.

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

Traffic from the selected ports will be sent to the destination port.

12. From the **Direction** menu, specify the direction of the traffic that must be mirrored from the selected source ports:
   - **None**. No traffic direction is selected. This is the default setting.
   - **Tx and Rx**. Monitors both transmitted and received packets.
   - **Rx**. Monitors received (ingress) packets only.
   - **Tx**. Monitors transmitted (egress) packets only.

13. Click the **Apply** button.

Your settings are saved.

The Status field indicates the interface status. The destination port is listed as Probe. The source ports are listed as Mirrored.
7

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.

However, if you can physically access the switch, you can reboot the switch by pressing a button on the front panel:

- **Model GS724TPv2.** Press the single-function **Reset** button for more than one second.
- **Model GS724TPP.** Press the multi-function **Reset** button for less than 5 seconds. (Do not press the button for more than 5 seconds!)

**To reboot the switch 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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** 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 to confirm.

   The switch reboots.
Reset the switch to its factory default settings

You can reset the system configuration to the factory default values. All changes that you made are lost. If the IP address changes, your web session might disconnect.

---

**Note:** If you reset the switch to the default configuration, the IP address is reset to 192.168.0.239, and the DHCP client is enabled. If you lose network connectivity after you reset the switch to the factory defaults, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

---

If you reset the switch to factory default settings, you can select to either maintain the NETGEAR registration status or reset the NETGEAR registration status. In the latter situation, you must reregister the switch with NETGEAR.

Reset the switch to factory default settings but maintain the registration status

You can use the device UI to reset the switch to the factory default settings but maintain the registration status.

However, if you can physically access the switch, you can press a button on the front panel to reset the switch to factory default settings but maintain the registration status:

- **Model GS724TPv2.** Press the dual-function *Factory Defaults* button for more than one second but less than 10 seconds. (Do not press the button for more than 10 seconds!)
- **Model GS724TPP.** Press the multi-function *Reset* button for more than five seconds but less than 10 seconds. (Do not press the button for more than 10 seconds!)

**To use the device UI to reset the switch to the factory default settings but maintain the registration 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 19 or Access the switch off-network and not connected to the Internet on page 27.
connected to the Internet on page 27.

The Device UI login page displays.

If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information page displays.


The Default Settings page displays.

7. Select the Reset configuration to factory default (EXCEPT registered device status), and clear device logs radio button.

This option resets the switch to its factory default settings but does not change its registration status with NETGEAR.

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 erased, even if you saved the configuration. This process takes about 135 seconds.

Reset the switch to factory default settings and reset the registration status

This option can be useful if you want to register the switch under a different name or account. This option requires you to first contact NETGEAR support at netgear.com/support so that the NETGEAR registration status on the NETGEAR server can be reset. Then, you can use this option to erase all settings, reset the switch to factory defaults, go through the initial log-in process again, and reregister the switch with NETGEAR.

If you can physically access the switch, you can press a button on the front panel to reset the switch to factory default settings and reset the registration status:

• **Model GS724TPv2.** Press the dual-function Factory Defaults button for more than 10 seconds.

• **Model GS724TPP.** Press the multi-function Reset button for more than 10 seconds.
To use the device UI to reset the switch to factory default settings and reset the registration 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 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information page displays.
   The Default Settings page displays.
7. Select the Reset and erase everything including registered device status radio button.
   This option requires you to first contact NETGEAR support at netgear.com/support so that the NETGEAR registration status on the NETGEAR server can be reset.
   After the switch reboots, you can reregister the switch using your NETGEAR account credentials. If you previously obtained a registration key, you can reenter the registration key. For more information, see Register the switch on page 30.
   If you do not first contact NETGEAR, after you reset the switch to factory default settings, the Device UI login page displays rather than the Register to activate your warranty page. However, your device admin password is reset to the default password (password).
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 erased, even if you saved the configuration. This process takes about 135 seconds.
Export a file from the switch

You can export configuration (ASCII) or log (ASCII log) files from the switch to a file server by using TFTP or to a computer by using HTTP.

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:

   • Enter your device admin password.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information 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. This is the default setting.
   - **Trap Log.** The trap log with the switch trap records.
   - **Buffered Log.** The switch buffered (in-memory) log.
   - **Tech Support.** The tech support file is a text-base file that contains a variety of hardware, software, and configuration information that can assist in device and network troubleshooting.
   - **Crash Logs.** The switch crash logs, if any are available.

8. From the Server Address Type menu, select the format for the Server Address field:
   - **IPv4.** Indicates that the TFTP server address is an IP address in dotted-decimal format. This is the default setting.
   - **DNS.** Indicates that the TFTP server address is a host name.

9. In the Server Address field, enter the IP address of the server in accordance with the format indicated by the server address type.
   
The default is the IPv4 address 0.0.0.0.

10. In the Transfer File Path field, specify the path on the TFTP server where you want to save the file.
    
    You can enter up to 160 characters. Include the backslash at the end of the path. A path name with a space is not accepted. Leave this field blank to save the file to the root TFTP directory.

11. In the 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.

12. Select the Start File Transfer check box.

13. Click the Apply button.
    
    The file transfer begins.
    
    The page displays information about the file transfer progress. The page refreshes automatically when the file transfer completes.
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 19 or Access the switch off-network and not connected to the Internet on page 27.
   
   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   
   - Enter your device admin password.
   
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go 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 are available.

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 manually check for the latest software version (also referred to as firmware version) through the device UI of the switch, download the firmware, and upload the firmware to the switch. If firmware release notes are available with new firmware, read the release notes to find out if you must reconfigure the switch after updating.

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.

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 386 for additional information.

To download a file to the switch from a TFTP server:

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

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

2. Launch a web browser.

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

   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.

For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

The System Information 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. This is the default setting.
   • **Text Configuration.** A text-based configuration file enables you to edit a configured text file (`startup-config`) offline as needed. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name or IP address), and download it to that device.
   • **X.509 Public Certificate PEM.** SSL trusted root certificate file (PEM encoded).
   • **X.509 Certificate Private Key PEM.** SSL server certificate file (PEM encoded).
   • **SSL DH Weak Encryption Parameter PEM File.** SSL Diffie-Hellman weak encryption parameter file (PEM encoded).
   • **SSL DH Strong Encryption Parameter PEM File.** SSL Diffie-Hellman strong encryption parameter file (PEM encoded).

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 image1.
   • **Image2.** Select image2 to upload image2.
Note: We recommended that you do not overwrite the active image.

9. From the Server Address Type menu, select the format for the TFTP Server IP field:
   - IPv4. Indicates that the TFTP server address is an IP address in dotted-decimal format. This is the default setting.
   - DNS. Indicates that the TFTP server address is a host name.

10. In the TFTP Server IP field, enter the IP address of the TFTP server indicated by the server address type.
    The default is the IPv4 address 0.0.0.0.

11. In the Transfer File Path field, specify the path on the TFTP server where the file is located.
    Enter up to 160 characters. Include the backslash at the end of the path. A path name with a space is not accepted. Leave this field blank to save the file to the root TFTP directory.

12. In the Remote File Name field, specify the name of the file to download from the TFTP server.
    You can enter up to 32 characters. A file name with a space is not accepted.

13. Select the Start File Transfer check box to initiate the file upload.

14. 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.

15. 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 391).
   b. Reboot the switch (see Reboot the switch on page 376).
Use HTTP to download a file to the switch or update the software image

You can download a software (firmware) image, configuration files, and SSL files from a computer to the switch by using an HTTP session over a web browser.

To download a file to the switch using HTTP:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   - Enter your device admin password.
   - If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information 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, the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the nonactive
image. This is a safety feature for faults occurring during the boot upgrade process. This the default setting.

- **Text Configuration.** A text-based configuration file enables you to edit a configured text file (*startup-config*) offline as needed. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name, serial number, IP address), and download it to that device.


- **SSL 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 image1.
- **Image2.** Select image2 to upload image2.

**Note:** We recommended that you do not overwrite the active image.

9. Click the **Browse** button and locate and select 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 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 391).
   
   b. **Reboot the switch** (see Reboot the switch on page 376).
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:

- **X.509 Public Certificate PEM.** This the certificate file, which must be in the format `xxxxxCERTxxxxx.pem`.
- **X.509 Certificate Private Key PEM.** This is the key file, which must be in the format `xxxxxKEYxxxxx.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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** 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, select **X.509 Public Certificate PEM**.

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 **X.509 Certificate Private Key PEM**.

    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 (or if it fails).

**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.

Copy a software image

You can copy a software image from one location (primary or backup) to another.

To copy a software image:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information page displays.


   ![File Management](image)

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


   ![Dual Image Configuration](image.png)

7. As an option, specify a name for the selected image by entering one in the Image Description field.

8. Select the Activate Image check box.
9. Click the **Apply** button.  
Your settings are saved.

10. After activating the image, reboot the switch (see Reboot the switch on page 376).  
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 19 or Access the switch off-network and not connected to the Internet on page 27.
   
The Device UI login page displays.  
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:  
   • Enter your device admin password.  
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the **Go** 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 switch.

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 19 or Access the switch off-network and not connected to the Internet on page 27.

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.

   The System Information page displays.


The following table describes the nonconfigurable information on the page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image1 Ver</td>
<td>The version of the image1 file.</td>
</tr>
<tr>
<td>Image2 Ver</td>
<td>The version of the image2 file.</td>
</tr>
<tr>
<td>Current-active</td>
<td>The currently active image on this switch.</td>
</tr>
<tr>
<td>Next-active</td>
<td>The image to be used after the switch reboots.</td>
</tr>
<tr>
<td>Image1 Description</td>
<td>The description, if any, associated with the image1 file.</td>
</tr>
<tr>
<td>Image2 Description</td>
<td>The description, if any, associated with the image2 file.</td>
</tr>
</tbody>
</table>
Perform diagnostics and troubleshooting

You can send a ping or a traceroute, and you can perform a memory dump.

Ping an IPv4 Address

You can configure the switch to send a ping request to a specified IPv4 address. You can use this option to check whether the switch can communicate with a particular IPv4 device. When you send a ping, the switch sends a specified number of ping requests and the results are displayed.

If a reply to the ping is received, the following message displays:

PING x.y.z.w (x.y.z.w): size data bytes
size bytes from x.y.z.w: seq=0 ttl=xyz
--- x.y.z.w ping statistics ---
count packets transmitted, count packets received, x% packet loss

If a reply to the ping is not received, the following message displays:

PING x.y.z.w (x.y.z.w): size data bytes
--- x.y.z.w ping statistics ---
count packets transmitted, 0 packets received, 100% packet loss

To ping an IPv4 address:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

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

   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
The System Information 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. Click the Apply button
    The specified address is pinged. The results are displayed below the configurable data in the Results field.

### Ping an IPv6 address

You can configure the switch to send a ping request to a specified IPv6 address. You can use this option to check whether the switch can communicate with a particular IPv6 device. When you send a ping, the switch sends a specified number of ping requests and the results are displayed.

If a reply to the ping is received, the following message displays:

```
PING x:y::z:w (x:y::z:w): size data bytes
size bytes from x:y::z:w: seq=0 ttl=xyz
--- x:y::z:w ping statistics ---
count packets transmitted, count packets received, x% packet loss
```
If a reply to the ping is not received, the following message displays:

```
PING x:y::z:w (x:y::z:w): size data bytes
--- x:y::z:w ping statistics ---
count packets transmitted, 0 packets received, 100% packet loss
```

**To ping an IPv6 address:**

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see [Access the switch on-network and connected to the Internet on page 19](#) or [Access the switch off-network and not connected to the Internet on page 27](#).

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see [Register the switch on page 30](#).

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

   For information about the credentials, see [Credentials for the device UI on page 28](#).

5. Click the **Go** button.

   The System Information page displays.

6. Select **Maintenance > Troubleshooting > Ping IPv6**.
7. In the **IPV6 Address/Hostname** field, enter the IPv6 address or host name of the station that must be pinged.

   The format is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. The maximum number of characters is 255.

8. 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.

9. In the **Interval (secs)** field, enter the time in seconds between ping packets.

   The range is 1 to 60. The default value is 3.

10. In the **Size** field, enter the datagram size.

    The valid range is 0 to 13000. The default value is 0 bytes.

11. 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:

```
tracert route to x.y.z.w (x.y.z.w), maxTTL hops max, size byte packets
initTTL x.y.z.w (x.y.z.w) 0.000 ms * 0.000 ms
initTTL+1 x.y.z.w (x.y.z.w) 0.000 ms * 0.000 ms
initTTL+2 x.y.z.w (x.y.z.w) 0.000 ms * 0.000 ms
```
To send an IPv4 traceroute:

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

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.

4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.

5. Click the Go button.
   The System Information 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) for the destination.
   The default value is 30. The range is 1 to 255.

10. In the **Init TTL** field, enter the initial TTL 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 to 65535.

14. In the **Size** field, enter the size of the probe packets.
    The default value is 0. The range is 38 to 32768.

15. Click the **Apply** button.
A traceroute request is sent to the specified IP address or host name. The results are displayed below the configurable data in the Results field.

Send an IPv6 traceroute

You can configure the switch to send a traceroute request to a specified IPv6 address or host name. You can use this to discover the paths that packets take to a remote destination. When you send a traceroute, the switch displays the results below the configurable data.

If a reply to the traceroute is received, the following message displays:

```
traceroute to x:y::z:w (x:y::z:w), maxTTL hops max, size byte packets
initTTL x:y::z:w (x:y::z:w) 0.000 ms * 0.000 ms
initTTL+1 x:y::z:w (x:y::z:w) 0.000 ms * 0.000 ms
initTTL+2 x:y::z:w (x:y::z:w) 0.000 ms * 0.000 ms
```

To send an IPv6 traceroute:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Access the switch on-network and connected to the Internet on page 19 or Access the switch off-network and not connected to the Internet on page 27.
   The Device UI login page displays.
   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see Register the switch on page 30.
4. Enter one of the following passwords:
   • Enter your device admin password.
   • If you previously managed the switch through the Insight app or Cloud portal, enter the Insight network password for the last Insight network location.
   For information about the credentials, see Credentials for the device UI on page 28.
5. Click the Go button.
   The System Information 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) for the destination.
   
   The default value is 30. The range is 1 to 255.

10. In the **Init TTL** field, enter the initial TTL 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 to 65535.

14. In the **Size** field, enter the size of the probe packets.
    
    The default value is 38. The range is 38 to 32768.
15. Click the **Apply** button.

   A traceroute request is sent to the specified IP address or host name. The results are displayed below the configurable data in the Results field.

**Enable 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 19](#) or [Access the switch off-network and not connected to the Internet on page 27](#).

   The Device UI login page displays.

   If you did not yet activate your warranty, the Register to activate your warranty page displays. For more information, see [Register the switch on page 30](#).

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

   For information about the credentials, see [Credentials for the device UI on page 28](#).

5. Click the **Go** 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.
Configuration Examples

This appendix contains information about how to configure the following features.

The appendix contains the following sections:

- Virtual Local Area Networks (VLANs)
- Access control lists (ACLs)
- Differentiated Services (DiffServ)
- 802.1X access control
- Multiple Spanning Tree Protocol
Virtual Local Area Networks (VLANs)

A local area network (LAN) can generally be defined as a broadcast domain. Hubs, bridges, or switches in the same physical segment or segments connect all end node devices. End nodes can communicate with each other without the need for a router. Routers connect LANs together, routing the traffic to the appropriate port.

A virtual LAN (VLAN) is a local area network with a definition that maps workstations on some basis other than geographic location (for example, by department, type of user, or primary application). To enable traffic to flow between VLANs, traffic must go through a router, just as if the VLANs were on two separate LANs.

A VLAN is a group of computers, servers, and other network resources that behave as if they were connected to a single network segment—even though they might not be. For example, all marketing personnel might be spread throughout a building. Yet if they are all assigned to a single VLAN, they can share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specified individuals, depending on how the IT manager set up the VLANs.

VLANs present a number of advantages:

- It is easy to do network segmentation. Users who communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group’s traffic is contained largely within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.
- They are easy to manage. The addition of nodes, as well as moves and other changes, can be dealt with quickly and conveniently from a management interface rather than from the wiring closet.
- They provide increased performance. VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.
- They ensure enhanced network security. VLANs create virtual boundaries that can be crossed only through a router. So standard, router-based security measures can be used to restrict access to each VLAN.

Packets received by the switch are treated in the following way:

- When an untagged packet enters a port, it is automatically tagged with the port’s default VLAN ID tag number. Each port supports a default VLAN ID setting that is user configurable (the default setting is 1). The default VLAN ID setting for each port can be changed on the Port PVID Configuration page. See Configure the port PVID settings on page 148.
- 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 141), 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 145) 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 port PVID settings on page 148), 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 allows ACLs to be bound to physical ports and LAGs. The switch 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 305).

   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 308.

3. On the MAC Binding Configuration page, assign the Sales_ACL to the interface Gigabit ports 6, 7, and 8, and then click the Apply button. (See Configure MAC bindings on page 312.)

   You can assign an optional sequence number to indicate the order of this access list relative to other access lists if any are already assigned to this interface and direction.

4. The MAC Binding Table displays the interface and MAC ACL binding information. (See View or delete MAC ACL bindings in the MAC binding table on page 314.)

   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 315.)

   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
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 341.)
   
   By default, this IP ACL is bound on the inbound direction, so it examines traffic as it enters the switch.
7. Click the Apply button.
8. On the IP Binding Table page, view the interfaces and IP ACL binding information. (See View or delete IP ACL bindings in the IP ACL binding table on page 343)

The IP ACL in this example matches all packets with the source IP address and subnet mask of the Finance department’s network and deny it on the Ethernet interfaces 2, 3, and 4 of the switch. The second rule permits all non-Finance traffic on the ports. The second rule is required because an explicit deny all rule exists as the lowest priority rule.

**Differentiated Services (DiffServ)**

Standard IP-based networks are designed to provide *best effort* data delivery service. *Best effort* service implies that the network delivers the data in a timely fashion, although there is no guarantee that it does. During times of congestion, packets might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. However, any degradation of service can negatively affect applications with strict timing requirements, such as voice or multimedia.

Quality of Service (QoS) can provide consistent, predictable data delivery by distinguishing between packets with strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given special treatment in a QoS-capable network. With this in mind, all elements of the network must be QoS capable. If one node cannot meet the necessary timing requirements, this creates a deficiency in the network path and the performance of the entire packet flow is compromised.
Two basic types of QoS are supported:

- **Integrated Services.** Network resources are apportioned based on request and are reserved (resource reservation) according to network management policy (RSVP, for example).
- **Differentiated Services.** Network resources are apportioned based on traffic classification and priority, giving preferential treatment to data with strict timing requirements.

The switch supports DiffServ.

The DiffServ feature contains a number of conceptual QoS building blocks that you can use to construct a differentiated service network. Use these same blocks in different ways to build other types of QoS architectures.

You must configure three key QoS building blocks for DiffServ:

- Class
- Policy
- Service (the assignment of a policy to a directional interface)

**Class**

You can classify incoming packets at Layers 2, 3, and 4 by inspecting the following information for a packet:

- Source/destination MAC address
- EtherType
- Class of Service (802.1p priority) value (first/only VLAN tag)
- VLAN ID range (first/only VLAN tag)
- Secondary 802.1p priority value (second/inner VLAN tag)
- Secondary VLAN ID range (second/inner VLAN tag)
- IP Service Type octet (also known as: ToS bits, Precedence value, DSCP value)
- Layer 4 protocol (TCP, UDP and so on)
- Layer 4 source/destination ports
- Source/destination IP address

From a DiffServ point of view, two types of classes exist:

- DiffServ traffic classes
- DiffServ service levels/forwarding classes
DiffServ traffic classes

With DiffServ, you define which traffic classes to track on an ingress interface. You can define simple BA classifiers (DSCP) and a wide variety of multifield (MF) classifiers:

- Layer 2; Layers 3, 4 (IP only)
- Protocol-based
- Address-based

You can combine these classifiers with logical AND or OR operations to build complex MF-classifiers (by specifying a class type of all or any, respectively). That is, within a single class, multiple match criteria are grouped together as an AND expression or a sequential OR expression, depending on the defined class type. Only classes of the same type can be nested; class nesting does not allow for the negation (exclude option) of the referenced class.

To configure DiffServ, you must define service levels, namely the forwarding classes/PHBs identified by a given DSCP value, on the egress interface. You define these service levels by configuring BA classes for each.

Creating policies

Use DiffServ policies to associate a collection of classes that you configure with one or more QoS policy statements. The result of this association is referred to as a policy.

From a DiffServ perspective, two types of policies exist:

- **Traffic Conditioning Policy**. A policy applied to a DiffServ traffic class
- **Service Provisioning Policy**. A policy applied to a DiffServ service level

You must manually configure the various statements and rules used in the traffic conditioning and service provisioning policies to achieve the desired Traffic Conditioning Specification (TCS) and the Service Level Specification (SLS) operation, respectively.

Traffic conditioning policy

Traffic conditioning pertains to actions performed on incoming traffic. Several distinct QoS actions are associated with traffic conditioning:

- **Dropping**. Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot coexist on the same interface.
- **Marking IP DSCP or IP Precedence**. Marking/re-marking the DiffServ code point in a packet with the DSCP value representing the service level associated with a particular DiffServ traffic class. Alternatively, the IP precedence value of the packet can be marked/re-marked.
- **Marking CoS (802.1p)**. Sets the 3-bit priority field in the first/only 802.1p header to a specified value when packets are transmitted for the traffic class. An 802.1p header is inserted if it does not already exist. This is useful for assigning a Layer 2 priority level based on a DiffServ forwarding class (such as the DSCP or IP precedence value)
definition to convey some QoS characteristics to downstream switches that do not routinely look at the DSCP value in the IP header.

- **Policing.** A method of constraining incoming traffic associated with a particular class so that it conforms to the terms of the TCS. Special treatment can be applied to out-of-profile packets that are either in excess of the conformance specification or are nonconformant. The DiffServ feature supports the following types of traffic policing treatments (actions):
  - **drop.** The packet is dropped.
  - **mark cos.** The 802.1p user priority bits are (re)marked and forwarded.
  - **mark dscp.** The packet DSCP is (re)marked and forwarded.
  - **mark prec.** The packet IP Precedence is (re)marked and forwarded.
  - **send.** The packet is forwarded without DiffServ modification.

**Color Mode Awareness.** Policing in the DiffServ feature uses either color blind or color aware mode. Color blind mode ignores the coloration (marking) of the incoming packet. Color aware mode takes into consideration the current packet marking when the switch determines the policing outcome. An auxiliary traffic class is used in conjunction with the policing definition to specify a value for one of the 802.1p, secondary 802.1p, IP DSCP, or IP precedence fields designating the incoming color value to be used as the conforming color. You can also specify the color of traffic that exceeds the threshold.

- **Counting.** Updating octet and packet statistics to keep track of data handling along traffic paths within DiffServ. In this DiffServ feature, counters are not explicitly configured by the user, but are designed into the system based on the DiffServ policy being created. For more information, see Monitor the switch and the ports on page 348.

- **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 216.

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 216.

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 228.

6. Click the **Add** button.

   The policy is added.

7. Click the **Policy1** hyperlink to view the Policy Class Configuration page for this policy.

8. Configure the Policy attributes as follows:
   • **Assign Queue.** 3
   • **Policy Attribute.** Simple Policy
   • **Color Mode.** Color Blind
   • **Committed Rate.** 10000 (which means 10000*16 kb/s).
   • **Confirm Action.** Send
   • **Violate Action.** Drop

   For more information about this page, see Configure a DiffServ policy on page 228.

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 234.)

All UDP packet flows destined to the 192.12.2.0 network with an IP source address from the 192.12.1.0 network that include a Layer 4 Source port of 4567 and Destination port of 4568 from this switch on ports 7 and 8 are assigned to hardware queue 3.

On this network, traffic from streaming applications uses UDP port 4567 as the source and 4568 as the destination. This real-time traffic is time sensitive, so it is assigned to a high-priority hardware queue. By default, data traffic uses hardware queue 0, which is designated as a best-effort queue.

Also the **confirmed action** on this flow is to send the packets with a committed rate of 1000000 Kbps. Packets that violate the committed rate and burst size are dropped.
802.1X access control

Local area networks (LANs) are often deployed in environments that permit unauthorized devices to be physically attached to the LAN infrastructure, or permit unauthorized users to attempt to access the LAN through equipment already attached. In such environments you might want to restrict access to the services offered by the LAN to those users and devices that are permitted to use those services.

Port-based network access control makes use of the physical characteristics of LAN infrastructures to provide a means of authenticating and authorizing devices attached to a LAN port with point-to-point connection characteristics. If the authentication and authorization process fails, access control prevents access to that port. In this context, a port is a single point of attachment to the LAN, such as a port of a MAC bridge and an association between stations or access points in IEEE 802.11 wireless LANs.

The IEEE 802.11 standard describes an architectural framework within which authentication and consequent actions take place. It also establishes the requirements for a protocol between the authenticator (the system that passes an authentication request to the authentication server) and the supplicant (the system that requests authentication), as well as between the authenticator and the authentication server.

The switch supports a guest VLAN, which allows unauthenticated users limited access to the network resources.

Note: You can use QoS features to provide rate limiting on the guest VLAN to limit the network resources that the guest VLAN provides.

Another 802.1X feature is the ability to configure a port to enable or disable EAPoL packet forwarding support. You can disable or enable the forwarding of EAPoL when 802.1X is disabled on the device.

The ports of an 802.1X authenticator switch provide the means by which it can offer services to other systems reachable through the LAN. Port-based network access control allows the operation of a switch's ports to be controlled to ensure that access to its services is permitted only by systems that are authorized to do so.

Port access control provides a means of preventing unauthorized access by supplicants to the services offered by a system. Control over the access to a switch and the LAN to which it is connected can be desirable when you restrict access to publicly accessible bridge ports or to restrict access to departmental LANs.

Access control is achieved by enforcing authentication of supplicants that are attached to an authenticator's controlled ports. The result of the authentication process determines whether the supplicant is authorized to access services on that controlled port.
A port access entity (PAE) is able to adopt one of two distinct roles within an access control interaction:

1. **Authenticator.** A port that enforces authentication before allowing access to services available through that port.

2. **Supplicant.** A port that attempts to access services offered by the authenticator.

Additionally, a third role exists:

3. **Authentication server.** Performs the authentication function necessary to check the credentials of the supplicant on behalf of the authenticator.

All three roles are required for you to complete an authentication exchange.

The switch supports the authenticator role only, in which the PAE is responsible for communicating with the supplicant. The authenticator PAE is also responsible for submitting the information received from the supplicant to the authentication server for the credentials to be checked, which determines the authorization state of the port. The authenticator PAE controls the authorized/unauthorized state of the controlled port depending on the outcome of the RADIUS-based authentication process.

![Figure 3. 802.1X authentication roles](image)

**802.1X example configuration**

This example shows how to configure the switch so that 802.1X-based authentication is required on the ports in a corporate conference room (g5–g8). These ports are available to visitors and must be authenticated before access is granted to the network. The authentication is handled by an external RADIUS server. When the visitor is successfully authenticated, traffic is automatically assigned to the guest VLAN. This example assumes that a VLAN was configured with a VLAN ID of 150 and VLAN name of Guest.

1. On the Port Authentication page (see Manage port authentication on individual ports on page 277), select ports g5, g6, g7, and g8.

2. From the Port Control menu, select Unauthorized.
The selection from the **Port Control** menu for all other ports on which authentication is not needed must be **Authorized**. When the selection from the **Port Control** menu is **Authorized**, the port is unconditionally put in a force-authorized state and does not require any authentication. When the selection from the **Port Control** menu is **Auto**, the authenticator PAE sets the controlled port mode.

3. In the **Guest VLAN** field for ports g5–g8, enter **150** to assign these ports to the guest VLAN.

   You can configure additional settings to control access to the network through the ports. See [Configure a port security interface on page 294](#) 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 293](#).)

   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 241](#).

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 255](#).)

   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.

![MSTP sample configuration](image-url)
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 141).
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 141).
3. On the STP Configuration page, enable the Spanning Tree State option (see Configure the STP settings and view the STP status on page 161).
   Use the default values for the rest of the STP configuration settings. By default, the STP operation mode is MSTP and the configuration name is the switch MAC address.
4. On the CST Configuration page (see Configure the CST port settings on page 165), set the bridge priority value for each of the three switch connections to force Switch 1 to be the root bridge:
   • Connection to Switch 1. 4096
   • Connection to Switch 2. 12288
   • Connection to Switch 3. 20480
   Note: Bridge priority values are multiples of 4096.
   If you do not specify a root bridge and all switches are assigned the same bridge priority value, the switch with the lowest MAC address is elected as the root bridge (see Configure the CST settings on page 163).
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 165).
6. Click the Apply button.
7. Select ports 1/0/1–1/0/5 (edge ports), and select Enable from the Fast Link menu.
   Since the edge ports are not at risk for network loops, ports with Fast Link enabled transition directly to the forwarding state.
8. Click the Apply button.
   On the CST Port Status page you can view spanning tree information about each port.
9. On the MST Configuration page (see Manage the MST settings on page 170), 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 169.
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.
This appendix describes the default settings for the switch and for its software features.

The appendix contains the following sections:

- Switch default settings
- General feature default settings
- System setup and maintenance settings
- Port characteristics
- Traffic control settings
- Quality of Service Settings
- Security settings
- System management settings
- Settings for other features
- Hardware technical specifications
Switch default settings

The following table describes the switch default settings.

Table 67. Switch default settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>192.168.0.239</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default gateway</td>
<td>192.168.0.254</td>
</tr>
<tr>
<td>Protocol</td>
<td>DHCP</td>
</tr>
<tr>
<td>Management VLAN ID</td>
<td>1</td>
</tr>
<tr>
<td>IPv6 admin mode</td>
<td>Enabled</td>
</tr>
<tr>
<td>IPv6 address auto configuration</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCPv6</td>
<td>Disabled</td>
</tr>
<tr>
<td>Minimum length for the device admin password</td>
<td>Eight characters</td>
</tr>
<tr>
<td>SNTP client</td>
<td>Disabled</td>
</tr>
<tr>
<td>Global logging</td>
<td>Enabled</td>
</tr>
<tr>
<td>Memory logging</td>
<td>Enabled (Severity level: informational and above)</td>
</tr>
<tr>
<td>Persistent (flash) logging</td>
<td>Disabled</td>
</tr>
<tr>
<td>DNS</td>
<td>Enabled (No servers configured)</td>
</tr>
<tr>
<td>SNMP traps</td>
<td>Enabled</td>
</tr>
<tr>
<td>Automatic saving to the startup configuration</td>
<td>Enabled, but you must click the Apply button to save changes that you make on a page.</td>
</tr>
<tr>
<td>TACACS+</td>
<td>No server configured</td>
</tr>
<tr>
<td>RADIUS</td>
<td>No server configured</td>
</tr>
<tr>
<td>Denial of service protection</td>
<td>Disabled</td>
</tr>
<tr>
<td>Dot1x authentication (IEEE 802.1X)</td>
<td>Disabled</td>
</tr>
<tr>
<td>MAC-based port security</td>
<td>All ports are unlocked</td>
</tr>
<tr>
<td>Access control lists (ACL)</td>
<td>Not configured</td>
</tr>
<tr>
<td>Protected ports</td>
<td>None</td>
</tr>
<tr>
<td>Advertised port speed</td>
<td>Maximum capacity</td>
</tr>
<tr>
<td>Broadcast storm control</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Table 67. Switch default settings (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC table address aging</td>
<td>300 seconds (dynamic addresses)</td>
</tr>
<tr>
<td>Default VLAN IDs and names</td>
<td>1. Default VLAN. 4088. Auto-VoIP VLAN</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> All ports are members of VLAN 1. No ports are members of the Auto-VoIP VLAN or the Auto-Video VLAN.</td>
</tr>
<tr>
<td>Multiple Spanning Tree</td>
<td>Disabled</td>
</tr>
<tr>
<td>Link aggregation</td>
<td>No link aggregation groups (LAGs) configured</td>
</tr>
<tr>
<td>LACP system priority</td>
<td>32768</td>
</tr>
<tr>
<td>DiffServ</td>
<td>Disabled</td>
</tr>
<tr>
<td>IGMP snooping</td>
<td>Disabled</td>
</tr>
<tr>
<td>IGMP multicast routing</td>
<td>Disabled</td>
</tr>
<tr>
<td>IGMP snooping querier</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

The following table describes the general feature default settings.

Table 68. General feature default settings

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual LAN (IEEE 802.1Q)</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Default VLANs                                 | • 1. Default VLAN. All ports are members.  
|                                               | • 4088. Auto-VoIP VLAN. No ports are members.              |
| PVID                                          | 1                                                            |
| Acceptable frame types                        | Admit All                                                    |
| Ingress filtering                             | Disabled                                                     |
| Port priority                                 | 0                                                            |
| **Jumbo Frames**                              |                                                              |
| Frame size                                    | 1522                                                         |
| **Flow Control**                              |                                                              |
| Admin mode                                    | Disabled                                                      |
### Table 68. General feature default settings (continued)

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>802.1X</strong></td>
<td></td>
</tr>
<tr>
<td>Port-based authentication state</td>
<td>Disabled</td>
</tr>
<tr>
<td>EAPOL flood mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port control</td>
<td>Auto</td>
</tr>
<tr>
<td>Periodic reauthentication</td>
<td>Disabled</td>
</tr>
<tr>
<td>Reauthentication period</td>
<td>3600</td>
</tr>
<tr>
<td>Quiet period</td>
<td>60</td>
</tr>
<tr>
<td>Number of EAP request resubmitted</td>
<td>30</td>
</tr>
<tr>
<td>Maximum number of EAP requests</td>
<td>2</td>
</tr>
<tr>
<td>Supplicant time-out</td>
<td>30</td>
</tr>
<tr>
<td>Server time-out</td>
<td>30</td>
</tr>
<tr>
<td><strong>STP/RSTP/MSTP, Global</strong></td>
<td></td>
</tr>
<tr>
<td>Spanning tree state</td>
<td>Enabled</td>
</tr>
<tr>
<td>STP operation mode</td>
<td>IEEE 802.1s RSTP</td>
</tr>
<tr>
<td>Configuration name</td>
<td>MAC address</td>
</tr>
<tr>
<td>Configuration revision level</td>
<td>0</td>
</tr>
<tr>
<td>Forwarding of BPDUs while STP is disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>CST bridge priority</td>
<td>32768</td>
</tr>
<tr>
<td>CST bridge maximum age</td>
<td>20</td>
</tr>
<tr>
<td>CST bridge hello time</td>
<td>2</td>
</tr>
<tr>
<td>CST bridge forward delay</td>
<td>15</td>
</tr>
<tr>
<td>CST spanning tree maximum number of hops</td>
<td>20</td>
</tr>
<tr>
<td>MST default instance ID</td>
<td>0</td>
</tr>
<tr>
<td>MST instance 0 priority</td>
<td>32768</td>
</tr>
<tr>
<td>MST instance 0 VLAN IDs</td>
<td>1, 4088</td>
</tr>
<tr>
<td><strong>STP/RSTP/MSTP, Interface</strong></td>
<td></td>
</tr>
<tr>
<td>CST STP status</td>
<td>Enabled</td>
</tr>
<tr>
<td>CST auto edge</td>
<td>Enabled</td>
</tr>
<tr>
<td>CST fast link</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
### Table 68. General feature default settings (continued)

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>CST BDPU forwarding</td>
<td>Disabled</td>
</tr>
<tr>
<td>CST path cost</td>
<td>0</td>
</tr>
<tr>
<td>CST priority</td>
<td>128</td>
</tr>
<tr>
<td>CST external path cost</td>
<td>0</td>
</tr>
<tr>
<td><strong>Link Aggregation</strong></td>
<td></td>
</tr>
<tr>
<td>Lag name</td>
<td>ch&lt;n&gt; where n is 1 to 8</td>
</tr>
<tr>
<td>Admin mode</td>
<td>Enabled</td>
</tr>
<tr>
<td>Hash mode</td>
<td>1 Src/Dest MAC, incoming port</td>
</tr>
<tr>
<td>STP mode</td>
<td>Enabled</td>
</tr>
<tr>
<td>Link trap</td>
<td>Enabled</td>
</tr>
<tr>
<td>LAG type</td>
<td>Static</td>
</tr>
<tr>
<td><strong>Local Link Discovery Protocol (LLDP), Global</strong></td>
<td></td>
</tr>
<tr>
<td>TLV advertised interval</td>
<td>30</td>
</tr>
<tr>
<td>Hold multiplier</td>
<td>4</td>
</tr>
<tr>
<td>Reinitializing delay</td>
<td>2</td>
</tr>
<tr>
<td>Transmit delay</td>
<td>5</td>
</tr>
<tr>
<td>Fast start duration</td>
<td>3</td>
</tr>
<tr>
<td><strong>Local Link Discovery Protocol (LLDP), Interface</strong></td>
<td></td>
</tr>
<tr>
<td>Admin status</td>
<td>Tx and Rx</td>
</tr>
<tr>
<td>Management IP address</td>
<td>Auto Advertise</td>
</tr>
<tr>
<td>Notification</td>
<td>Enabled</td>
</tr>
<tr>
<td>Optional TLVs</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>DHCP Snooping, Global</strong></td>
<td></td>
</tr>
<tr>
<td>Admin mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>MAC address validation</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>DHCP Snooping, Interface</strong></td>
<td></td>
</tr>
<tr>
<td>Trust mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>Logging invalid packets</td>
<td>Disabled</td>
</tr>
<tr>
<td>Rate limit</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Table 68. General feature default settings (continued)

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burst interval</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Persistent Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Store</td>
<td>Local</td>
</tr>
<tr>
<td>Write delay</td>
<td>300</td>
</tr>
<tr>
<td><strong>Differentiated Services (DiffServ)</strong></td>
<td></td>
</tr>
<tr>
<td>Admin mode</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Class of Service (CoS), Global</strong></td>
<td></td>
</tr>
<tr>
<td>Trust mode</td>
<td>802.1p</td>
</tr>
</tbody>
</table>

802.1p to queue mapping (802.1p -> queue)

<table>
<thead>
<tr>
<th>802.1p</th>
<th>Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>

Class Selector:

- (CS 0) 000000 -> 1
- (CS 1) 001000 -> 0
- (CS 2) 010000 -> 2
- (CS 3) 011000 -> 3
- (CS 4) 100000 -> 4
- (CS 5) 101000 -> 5
- (CS 6) 110000 -> 6
- (CS 7) 111000 -> 7

Assured Forwarding:

- (AF 11) 001010 -> 0
- (AF 12) 001100 -> 0
- (AF 13) 001110 -> 0
- (AF 21) 010010 -> 0
- (AF 22) 010100 -> 0
- (AF 23) 010110 -> 0
- (AF 31) 011010 -> 1
- (AF 32) 011100 -> 1
- (AF 33) 011110 -> 1
- (AF 41) 100010 -> 1
- (AF 42) 100100 -> 1
- (AF 43) 100110 -> 1
Table 68. General feature default settings (continued)

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
</table>
| DSCP to Queue Mapping (DSCP -> Queue) | Expedited Forwarding: (EF) 101110 -> 2  
Other:  
(1) 000001 -> 1  
(2) 000010 -> 1  
(3) 000011 -> 1  
(4) 000100 -> 1  
(5) 000101 -> 1  
(6) 000110 -> 1  
(7) 000111 -> 1  
(9) 001001 -> 0  
(11) 001011 -> 0  
(13) 001101 -> 0  
(15) 001111 -> 0  
(17) 010001 -> 0  
(19) 010011 -> 0  
(21) 010101 -> 0  
(23) 010111 -> 0  
(25) 011001 -> 1  
(27) 011011 -> 1  
(29) 011101 -> 1  
(31) 011111 -> 1  
(33) 100001 -> 2  
(35) 100011 -> 2  
(37) 100101 -> 2  
(39) 100111 -> 2  
(41) 101001 -> 2  
(43) 101011 -> 2  
(45) 101101 -> 2  
(47) 101111 -> 2  
(49) 110001 -> 3  
(50) 110010 -> 3  
(51) 110011 -> 3  
(52) 110100 -> 3  
(53) 110101 -> 3  
(54) 110110 -> 3  
(55) 110111 -> 3  
(57) 111001 -> 3  
(58) 111010 -> 3  
(59) 111011 -> 3  
(60) 111100 -> 3  
(61) 111101 -> 3  
(62) 111110 -> 3  
(63) 111111 -> 3 |
Table 68. General feature default settings (continued)

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Class of Service (CoS), Interface</strong></td>
<td></td>
</tr>
<tr>
<td>Trust mode</td>
<td>802.1p</td>
</tr>
<tr>
<td>Interface shaping rate</td>
<td>0</td>
</tr>
<tr>
<td>802.1p to queue mapping (802.1p -&gt; queue)</td>
<td>0 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>1 -&gt; 0</td>
</tr>
<tr>
<td></td>
<td>2 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>3 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>4 -&gt; 4</td>
</tr>
<tr>
<td></td>
<td>5 -&gt; 5</td>
</tr>
<tr>
<td></td>
<td>6 -&gt; 6</td>
</tr>
<tr>
<td></td>
<td>7 -&gt; 7</td>
</tr>
<tr>
<td>Queue minimum bandwidth</td>
<td>0</td>
</tr>
<tr>
<td>Queue scheduler type</td>
<td>Weighted</td>
</tr>
<tr>
<td><strong>Auto-VoIP, Protocol-Based</strong></td>
<td></td>
</tr>
<tr>
<td>Admin mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>Prioritization type</td>
<td>Traffic Class</td>
</tr>
<tr>
<td>Auto-VoIP traffic class</td>
<td>7</td>
</tr>
<tr>
<td><strong>Auto-VoIP, OUI-Based</strong></td>
<td></td>
</tr>
<tr>
<td>Admin mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>Auto-VoIP VLAN</td>
<td>0</td>
</tr>
<tr>
<td>OUI-based priority</td>
<td>7</td>
</tr>
<tr>
<td><strong>L2 Loop Protection</strong></td>
<td></td>
</tr>
<tr>
<td>Admin mode</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
System setup and maintenance settings

The following table describes the system setup and maintenance settings.

**Table 69. System setup and maintenance settings**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot code update</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>DHCP</td>
<td>1</td>
<td>Enabled</td>
</tr>
<tr>
<td>Static IP address</td>
<td>1</td>
<td>192.168.0.239</td>
</tr>
<tr>
<td>System name configuration</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration save/restore</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>Firmware upgrade</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>Restore defaults</td>
<td>1 (device UI and rear-panel button)</td>
<td>N/A</td>
</tr>
<tr>
<td>Dual image support</td>
<td>1</td>
<td>Enabled</td>
</tr>
<tr>
<td>Factory reset</td>
<td>1</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Port characteristics

The following table describes the port characteristics.

**Table 70. Port characteristics**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy Efficient Ethernet (EEE)</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td>Auto negotiating speed and full/half duplex</td>
<td>All ports</td>
<td>Auto negotiation</td>
</tr>
<tr>
<td>Auto MDI/MDIX</td>
<td>For cross over cables on all ports</td>
<td>Enabled</td>
</tr>
<tr>
<td>802.3x flow control/back pressure</td>
<td>1 (per system)</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port mirroring: TX, RX, Both</td>
<td>1</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port trunking (aggregation)</td>
<td>8</td>
<td>Preconfigured</td>
</tr>
<tr>
<td>802.1D spanning tree</td>
<td>1</td>
<td>Disabled</td>
</tr>
<tr>
<td>802.1w RSTP</td>
<td>1</td>
<td>Enabled</td>
</tr>
<tr>
<td>802.1s spanning tree</td>
<td>4 instances</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Traffic control settings

The following table describes the traffic control settings.

Table 71. Traffic control settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storm control</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td>Jumbo frame</td>
<td>All ports</td>
<td>1522 Max = 10,000 bytes</td>
</tr>
</tbody>
</table>

Quality of Service Settings

The following table describes the Quality of Service settings.

Table 72. Quality of Service settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of queues</td>
<td>8</td>
<td>N/A</td>
</tr>
<tr>
<td>802.1p</td>
<td>1</td>
<td>Enabled</td>
</tr>
<tr>
<td>DSCP</td>
<td>1</td>
<td>Disabled</td>
</tr>
<tr>
<td>Egress rate limiting</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Security settings

The following table describes the security settings.

Table 73. Security settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td>MAC ACLs</td>
<td>100 (shared with IPv4 and IPv6 ACLs)</td>
<td>All MAC addresses allowed</td>
</tr>
<tr>
<td>IPv4 ACLs</td>
<td>100 (shared with MAC and IPv6 ACLs)</td>
<td>All IPv4 addresses allowed</td>
</tr>
<tr>
<td>IPv6 ACLs</td>
<td>100 (shared with IPv4 ACL and MAC ACL)</td>
<td>All IPv6 addresses allowed</td>
</tr>
<tr>
<td>Password control access</td>
<td>1</td>
<td>Idle time-out = 5 mins.</td>
</tr>
<tr>
<td>Device admin password</td>
<td>1</td>
<td>Password = password</td>
</tr>
<tr>
<td>Management security</td>
<td>1 profile with 20 rules for HTTP/HTTPS/SNMP access to allow/deny an IP address/subnet</td>
<td>All IP addresses allowed</td>
</tr>
<tr>
<td>Port MAC lock down</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

System management settings

The following table describes the system management settings.

Table 74. System management settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-session web connections</td>
<td>4</td>
<td>Enabled</td>
</tr>
<tr>
<td>SNMPv1/v2</td>
<td>Max 5 community entries</td>
<td>Enabled (read, read/write communities)</td>
</tr>
<tr>
<td>SNMPv3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time control</td>
<td>1 (Local or SNTP)</td>
<td>Local Time enabled</td>
</tr>
<tr>
<td>LLDP/LLDP-MED</td>
<td>All ports</td>
<td>Enabled</td>
</tr>
<tr>
<td>Logging</td>
<td>3 (Memory/Flash/Server)</td>
<td>Memory log enabled</td>
</tr>
</tbody>
</table>
**Settings for other features**

The following table describes the settings for other features.

**Table 75. Settings for other features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP snooping v1/v2/v3</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td>EAPoL flooding</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td>BPDU flooding</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td>Multicast groups</td>
<td>256</td>
<td>Disabled</td>
</tr>
<tr>
<td>Filter multicast control</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td>Number of DHCP snooping bindings</td>
<td>256</td>
<td>N/A</td>
</tr>
<tr>
<td>Number of DHCP static entries</td>
<td>256</td>
<td>N/A</td>
</tr>
<tr>
<td>MAC address database size</td>
<td>16k</td>
<td>N/A</td>
</tr>
<tr>
<td>Number of IPv4/IPv6 static routes</td>
<td>32</td>
<td>N/A</td>
</tr>
<tr>
<td>Number of supported VLANs</td>
<td>64</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Hardware technical specifications**

The tables in the following sections describes the main hardware technical specifications for each model. For more hardware information, see the data sheet, which you can download by visiting [netgear.com/support/download/](http://netgear.com/support/download/).
Model GS724TPv2 hardware technical specifications

Table 76. Hardware technical specifications for model GS724TPv2

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network interfaces</td>
<td>Twenty-four 10/100/1000BASE-T RJ-45 PoE+ copper ports</td>
</tr>
<tr>
<td></td>
<td>Two dedicated 1000BASE-X fiber SFP ports</td>
</tr>
<tr>
<td>Switch PoE+ power budget</td>
<td>190W</td>
</tr>
<tr>
<td>Max.power consumption with PoE</td>
<td>228.53W</td>
</tr>
<tr>
<td>Max.power consumption without PoE</td>
<td>23.35W</td>
</tr>
<tr>
<td>Idle power consumption</td>
<td>13.86W</td>
</tr>
<tr>
<td>Dimensions (W x D x H)</td>
<td>17.3 x 8.0 x 1.7 in. (440 x 204 x 43 mm)</td>
</tr>
<tr>
<td>Weight</td>
<td>6.96 lb (3.15 kg)</td>
</tr>
<tr>
<td>Operating temperature</td>
<td>32º to 122ºF (0º to 50°C)</td>
</tr>
<tr>
<td>Operating humidity</td>
<td>95% maximum relative humidity, noncondensing</td>
</tr>
<tr>
<td>Maximum operating altitude</td>
<td>10,000 ft (3,000 m)</td>
</tr>
<tr>
<td>Storage temperature</td>
<td>–4º to 158ºF (~–20º to 70°C)</td>
</tr>
<tr>
<td>Storage humidity</td>
<td>95% maximum relative humidity, noncondensing</td>
</tr>
<tr>
<td>Maximum storage altitude</td>
<td>10,000 ft (3,000 m)</td>
</tr>
<tr>
<td>Electromagnetic certifications and compliance</td>
<td>CE:</td>
</tr>
<tr>
<td></td>
<td>EN 61000-3-2:2014, Class A</td>
</tr>
<tr>
<td></td>
<td>EN 61000-3-3:2013</td>
</tr>
<tr>
<td></td>
<td>EN 55024:2010</td>
</tr>
<tr>
<td></td>
<td>VCCI: VCCI-CISPR 32:2016, Class A</td>
</tr>
<tr>
<td></td>
<td>RCM: AS/NZS CISPR 32:2013 Class A</td>
</tr>
<tr>
<td></td>
<td>CCC: GB4943.1-2011, YD/T993-1998, GB/T9254-2008 (Class A)</td>
</tr>
<tr>
<td></td>
<td>BSMI: CNS 13438 Class A</td>
</tr>
<tr>
<td></td>
<td>KCC</td>
</tr>
</tbody>
</table>
### Model GS724TPP hardware technical specifications

#### Table 76. Hardware technical specifications for model GS724TPP (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>UL listed: UL/cUL 60950-1</td>
</tr>
<tr>
<td></td>
<td>RCM (AS/NZS) 60950.1:2015</td>
</tr>
<tr>
<td></td>
<td>CCC (China Compulsory Certificate): GB4943.1-2011; YD/T993-1998; GB/T9254-2008 (Class A)</td>
</tr>
<tr>
<td></td>
<td>BSMI: CNS 14336-1</td>
</tr>
</tbody>
</table>

#### Table 77. Hardware technical specifications for model GS724TPP

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network interfaces</td>
<td>Twenty-four 10/100/1000BASE-T RJ-45 PoE+ copper ports</td>
</tr>
<tr>
<td></td>
<td>Two dedicated 1000BASE-X fiber SFP ports</td>
</tr>
<tr>
<td>Switch PoE+ power budget</td>
<td>380W</td>
</tr>
<tr>
<td>Max.power consumption with PoE</td>
<td>446.70W</td>
</tr>
<tr>
<td>Max.power consumption without PoE</td>
<td>32.71W</td>
</tr>
<tr>
<td>Idle power consumption</td>
<td>24.70W</td>
</tr>
<tr>
<td>Dimensions (W x D x H)</td>
<td>17.3 x 8.0 x 1.7 in. (440 x 204 x 43 mm)</td>
</tr>
<tr>
<td>Weight</td>
<td>8.18 lb (3.7 kg)</td>
</tr>
<tr>
<td>Operating temperature</td>
<td>32º to 122ºF (0º to 50ºC)</td>
</tr>
<tr>
<td>Operating humidity</td>
<td>95% maximum relative humidity, noncondensing</td>
</tr>
<tr>
<td>Maximum operating altitude</td>
<td>10,000 ft (3,000 m)</td>
</tr>
<tr>
<td>Storage temperature</td>
<td>-4º to 158ºF (-20º to 70ºC)</td>
</tr>
<tr>
<td>Storage humidity</td>
<td>95% maximum relative humidity, noncondensing</td>
</tr>
<tr>
<td>Maximum storage altitude</td>
<td>10,000 ft (3,000 m)</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>- EN 61000-3-2:2014, Class A</td>
</tr>
<tr>
<td></td>
<td>- EN 61000-3-3:2013</td>
</tr>
<tr>
<td></td>
<td>- EN 55024:2010</td>
</tr>
<tr>
<td></td>
<td>- EN 55024:2010+AC1:2005</td>
</tr>
<tr>
<td></td>
<td>- EN 55035:2017</td>
</tr>
<tr>
<td></td>
<td>- VCCI: VCCI-CISPR 32:2016, Class A</td>
</tr>
<tr>
<td></td>
<td>- RCM: AS/NZS CISPR 32:2015 Class A</td>
</tr>
<tr>
<td></td>
<td>- CCC: GB4943.1-2011, YD/T993-1998, GB/T9254-2008 (Class A)</td>
</tr>
<tr>
<td></td>
<td>- BSMI: CNS 13438 Class A</td>
</tr>
<tr>
<td></td>
<td>- KCC</td>
</tr>
<tr>
<td></td>
<td>UL listed: vUL/cUL 62368-1</td>
</tr>
<tr>
<td></td>
<td>RCM (AS/NZS) 62368.1:2018</td>
</tr>
<tr>
<td></td>
<td>CCC (China Compulsory Certificate): GB4943.1-2011; YD/T993-1998; GB/T9254-2008 (Class A)</td>
</tr>
<tr>
<td></td>
<td>BSMI: CNS 14336-1</td>
</tr>
</tbody>
</table>