

HPE Networking Instant On 1940 Switch Series

Management and Configuration Guide

Instant On

Hewlett Packard Enterprise

Copyright Information

© Copyright 2026 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at https://myenterpriselicense.hpe.com/cwp-ui/software but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd, Spring, TX 77389
United States of America



Edition 1.0 | July 2026

Contents

Contents 3

About This Document 15

Applicable Products 15

Related Documents 15

Supported Features 16

1 Getting Started 18

Connecting the Switch to a Network 18

Browser Support 19

Selecting Local Web Management Mode 19

2 Getting Started With the Web Interface 20

Logging On 20

GUI Interface Layout and Features 21

Common Page Elements 22

Saving Changes 23

Latest Events Panel 23

Configuration Wizards 24

Getting Started Wizard 24

VLAN Configuration Wizard 25

ACL Configuration Wizard 26

Device View 27

Port Information 27

Port Status Indicator 28

System LEDs, Console Port, and Reset Pin 28

3 Dashboard 30

Dashboard Page 30

Device View 30

System Information 30

System Time 31

Device Information 32

System Health Status 32

System Resource Usage 33

Device LEDs 33
Active Users 34
4 Management 35
Network Settings 35
IPv4 Setup Tab 35
IPv6 Setup Tab 36
HTTP/S Management Settings 38
Management VLAN Settings 39
Telnet Settings 39
SSH Settings 40
System Time 41
Time Configuration 41
Daylight Saving Configuration 43
User Management 45
Logged In Sessions 45
User Accounts 46
Adding a User Account 47
Changing User Account Information 48
Removing a User Account 48
Account Security Settings 49
Password Keyword Exclusion 50
Password Strength Rules 51
Schedule Configuration 52
Adding a Schedule 53
Removing a Schedule 54
HTTPS Certificate 55
HTTPS Certificate Settings 55
Generate a Self-Signed Certificate 56
Using a Certificate Signed by a Certificate Authority 57
View a Certificate 58
Delete a Certificate 58
SSH Key Management 59
SNMP 60
SNMP v1 and v2 60
SNMP v3 60
Global Configuration 61
Community Configuration 62
Adding an SNMP Community or Community Group 63
Removing an SNMP Community or Community Group 63

SNMP v1/v2 Trap Receivers 64
Adding an SNMP v1/v2 Trap Receiver 65
Removing an SNMP v1/v2 Trap Receiver 65
SNMP v3 Trap Receivers 66
Adding an SNMP v3 Trap Receiver 67
Removing an SNMPv3 Trap Receiver 67
SNMP Filter Configuration 68
Adding an SNMP Filter 68
Removing an SNMP Filter 69
SNMP Access Control Group Configuration 69
Adding an SNMP Access Control Group 70
Removing an SNMP Access Control Group 70
SNMP User Configuration 71
Adding an SNMP v3 User 72
Removing an SNMP v3 User 72
SNMP View Configuration 73
Adding an SNMP View 74
Removing an SNMP View 74
Remote Engine ID Configuration 74
Adding a Remote Engine ID 75
Removing an Remote Engine ID 75
Management Access List Configuration 76
Profile Configuration 76
Profile Rule Configuration 77
Adding a Profile Rule 78
Editing a Profile Rule 78
Removing a Profile Rule 78
5 Switching Features 79
Port Configuration 79
Device View 79
Global Configuration 79
Interface Configuration 81
Modifying Interface Settings 83
Port Summary Statistics 85
Flow Control 86
Port Mirroring 88
Global Configuration 88
Session Configuration 89
Mirroring Sessions Configuration 90

Configuring a Port Mirroring Session 91
Removing Source Ports from a Session 92
Loop Protection 92
Global Configuration 93
Interface Configuration 94
IGMP Snooping 95
Global Configuration 95
IPv4 Unregistered Multicast 96
IGMP Snooping VLAN Configuration 97
Configuring IGMP Snooping on a VLAN 98
IGMP Snooping Multicast Router Interface Configuration 99
Configuring Multicast Router Settings on Interfaces 99
Multicast Forwarding Database 100
IGMPv3 Multicast Forwarding Database 101
Interface Auto Recovery 101
Global Configuration 102
Suspended Interfaces 104
Link Aggregation 105
Device View 106
Global Configuration 106
Link Aggregation 107
Modifying Trunk Settings 108
EEE Configuration 109
Global Configuration 109
Global Status 110
Interface Status 111
Device Tracking **112**
Device Tracking Global Configuration 112
Device Tracking Summary 113
Device Tracking Interface Configuration 114
Device Tracking Statistics 115
UDLD **116**
UDLD Configuration 116
UDLD Interface Configuration 117
6 Spanning Tree **119**
Global Settings 119
Global Configuration 119
Global Settings 121
Spanning Tree Statistics 122

CST Configuration 123
CST Port Configuration 123
Additional Actions on CST Ports 124
MSTP Configuration 128
MSTP Configuration 128
Adding, Editing or Removing an MSTP Configuration 129
MSTP Port Configuration 130
Editing MSTP Port Settings and Viewing MSTP Port Details 131
7 Virtual LAN 134
VLAN Configuration 134
Device View 134
VLAN Configuration 135
Adding, Editing, and Removing VLANs 136
VLAN Membership 137
VLAN Membership - By Interface Tab 137
VLAN Membership - By VLAN Tab 138
VLAN Interface Configuration 140
Voice VLAN Configuration 141
Global Configuration 142
Telephony OUI Configuration 143
Voice VLAN Interface Settings 144
Auto VLAN Configuration 146
Auto-Wifi Global Configuration 146
Auto-Camera Global Configuration 147
Auto-Wifi OUI Configuration 147
Auto-Camera OUI Configuration 148
Auto VLAN Interface Settings 149
Auto VLAN Interface Summary 150
8 Neighbor Discovery 151
LLDP 151
LLDP Global Configuration 152
LLDP Global Information 153
Interface Configuration 154
Remote Device Information 156
Local Device Information 157
LLDP Statistics 159
LLDP-MED Global Configuration 160
LLDP-MED Global Configuration 160
LLDP Global Information 161

LLDP-MED Interface Configuration 162
LLDP-MED Remote Device Summary 164
9 Power over Ethernet 166
PoE Configuration 167
Device View 167
Activity 167
Priority 167
Class 168
Global Configuration 168
Status 169
PoE Port Configuration 170
Modifying Port PoE Settings 171
Viewing PoE Port Details 173
Power Consumption History 174
10 Routing 175
IPv4 Routing 175
Global Configuration 175
Port IP and VLAN IP 176
Static Routing/Route Table Tile 180
Static Routing Tab 180
Adding a Static Route 181
Route Table Tab 182
IP Routing Statistics/ICMP Statistics Tile 183
IP Routing Statistics Tab 183
ICMP Statistics Tab 185
DHCP Relay 186
Global Configuration 186
Server Configuration 187
DHCP Relay Interfaces 188
ARP Table 189
Global Configuration 190
Static ARP Table 191
Adding a Static ARP Entry 191
Removing a Static ARP Entry 192
ARP Table Summary 192
ARP Table Statistics 193
11 Quality of Service 194
Access Control Lists 194

Access Control Lists 194
Adding an ACL 195
Removing an ACL 195
IPv4 ACL Rules and MAC ACL Rules Tile 196
IPv4 ACL Rules and MAC ACL Rules 196
Adding a Rule to an IPv4 ACL 197
Adding a Rule to an MAC ACL 200
Interface and VLAN Configuration Tile 202
Interface Configuration Tab and VLAN Configuration Tab 202
Associating an ACL with an Interface or VLAN 204
Removing an Association Between an ACL and an Interface or VLAN 204
Class of Service 205
General Settings 205
802.1p Priority Mapping 206
Configuring 802.1p Priority Mapping 207
DSCP CoS Mapping 208
Configuring DSCP CoS Mapping 209
Queue Configuration 210
Configuring CoS Queue Settings 211
Interface CoS Configuration 212
Configuring CoS on an Interface 213
12 Security 214
AAA Configuration 214
Management Authentication Order 214
Port Access Control Authentication Order 215
RADIUS Configuration 216
Global Configuration 217
RADIUS Server Configuration 218
Adding a RADIUS Server 219
Changing RADIUS Server Settings 220
Removing a RADIUS Server 220
RADIUS Accounting Server Configuration 221
Adding a RADIUS Accounting Server 221
Changing RADIUS Accounting Server Settings 222
Removing a RADIUS Accounting Server 222
RADIUS Server Statistics 223
RADIUS Accounting Server Statistics 224
TACACS+ Configuration 225
TACACS+ Configuration 225

TACACS+ Server Configuration 227
Adding, Editing, and Removing a TACACS+ Server 227
Port Access Control 228
Global Configuration 228
MAC Authentication Settings 229
Port Configuration 230
Configuring Port Access Control on an Interface 231
Authenticating and Initializing Port Authentication 234
Viewing Per-port 802.1X Details 235
Local MAC Authentication Clients 235
Access Control Client Information 236
Port Access Control Statistics 237
Port Security 239
Port Security Configuration 239
Static/Dynamic MAC Addresses 241
Static MAC Addresses Tab 241
Dynamic MAC Addresses 243
Protected Ports 244
Protected Ports Configuration 244
DHCP Snooping and IP Source Guard 245
DHCP Snooping Configuration 246
DHCP Snooping VLAN Configuration 246
DHCP Snooping Interface Configuration 247
Binding Database 248
ARP Attack Protection 249
Global Configuration 249
Interface Settings 250
ARP Access Control Rules 251
VLAN Settings 252
Denial of Service 253
TCP Settings 253
ICMP Settings 255
13 Diagnostics 256
Logging 256
Unexpected Restart Information 256
Global Log Settings 257
Remote Log Server 258
Trap Configuration 259
Buffered Log, Log File, and Trap Log 260

Buffered Log Tab 260
Log File Tab 262
Trap Log Tab 263
Ping 264
IPv4/IPv6 264
IPv4 Tab 264
IPv6 Tab 265
Ping Results 266
Traceroute 267
IPv4/IPv6 267
IPv4 Tab 267
IPv6 Tab 269
Traceroute Results 270
Support File **271**
Cable Test **273**
MAC Table 275
Global Configuration 275
MAC Address Table 276
Clear Dynamic FDB Entries 277
RMON 278
RMON Statistics 278
History Collectors/Log 280
History Collectors 280
History Log 282
RMON Events/Event Log 283
RMON Events Tab 283
Event Log Tab 284
RMON Alarms 284
IP Address Conflict **287**
Status 287
History 287
Email Alerts 288
Email Alert Global Configuration 288
Email Alert Statistics 289
Email Alert Server Configuration 290
Email Alert Subject Configuration 291
Email Alert To Address Configuration 292
14 Maintenance Pages 293
Dual Image Configuration 293

Backup and Update Files 294
Backing Up and Updating Files 294
InstantOn Provisioning 297
Configuration File Operations **299**
Reset **300**
Reboot Device 300
Reset to Factory Defaults 301
Reset Configuration 301
A Managing the Device from Direct Ops Commands 302
Command Summary 302
Command Details 305
boot autoinstall 305
boot host 305
boot system 306
clear config 307
clear counters 307
clear logging buffered 308
clear logging email statistics 308
clear mbuf stats 309
clock set 309
clock summer-time 309
clock timezone 310
configure 311
copy 311
crypto certificate 315
crypto dhparam size 317
crypto key generate 317
crypto key {encrypt | decrypt} write 317
crypto key pubkey-chain ssh 318
enable 319
enable password 319
exit 320
help 321
interface 321
ip http 322
ip routing 323
ip scp server enable 323
ip ssh 324
ip ssh {client | server} algorithm encryption 324

ip ssh {client | server} algorithm hostkey 325
ip ssh {client | server} algorithm kex 326
ip ssh {client | server} algorithm mac 327
ip telnet 327
logging 328
logout 328
network ipv6 329
network ip6 address 329
network mac-address 330
network mac-type 330
network mgmt_vlan 331
network parms 331
network protocol 332
ping 332
ping ipv6 334
release dhcp 335
reload 335
renew dhcp 336
script 337
set clibanner 338
show backup-config 339
show bootvar 340
show clibanner 340
show clock 341
show crypto certificate 341
show crypto dhparam 342
show crypto key 343
show error 344
show interface 344
show interface counters 345
show interface ethernet 345
show ip address-conflict 346
show ip http 347
show ip ssh 347
show ip vlan 348
show logging 349
show network 351
show network ipv6 351
show port 352
show running-config 354

show spanning-tree 355
show spanning-tree interface 356
show spanning-tree mst detailed 357
show spanning-tree mst port 358
show spanning-tree root-history 359
show ssh 359
show startup-config 360
show sysinfo 361
show tech-support 361
show telnet 363
show telnetcon 363
show version 363
show vlan 364
snmp-server 366
telnet 366
traceroute 367
update bootcode 368
vlan 368
vlan database 369
vlan name 369
write memory 370

B Support 371

Websites 371
Accessing HPE Networking Support 371
Accessing Updates 372
Warranty Information 372
Regulatory Information 372
Additional Regulatory Information 372
Documentation Feedback 373

The HPE Instant On 1940 Switch Series switches are designed to meet the needs of small business network environments—simple to set up and manage and are secure and reliable. Instant On switch deployments can be managed through a mobile application supported on iOS and Android, through a cloud portal that is accessible through a web browser, or using a local web GUI. Basic setup, configuration and troubleshooting can be performed from the Direct Ops interface accessed through the USB-C console port or via SSH/ Telnet.

This manual details using the web GUI to manage the switch.

Applicable Products

This guide applies to these products:

- HPE Networking Instant On Switch 8p Gigabit CL6 PoE 2p SFP 124W 1940
- HPE Networking Instant On Switch 8p SR10 4p CL6 PoE 2p SFP+ 120W 1940
- HPE Networking Instant On Switch 20p Gigabit CL4 4p SR2.5G CL6 PoE 4p SFP+ 370W 1940
- HPE Networking Instant On Switch 24p Gigabit 4p SFP+ 1940
- HPE Networking Instant On Switch 24p Gigabit CL4 PoE 4p SFP+ 240W 1940
- HPE Networking Instant On Switch 40p Gigabit CL4 8p SR2.5G CL6 PoE 4p SFP+ 600W 1940
- HPE Networking Instant On Switch 48p Gigabit 4p SFP+ 1940
- HPE Networking Instant On Switch 48p Gigabit CL4 PoE 4p SFP+ 370W 1940

Related Documents

The switch manual set includes the following:

- **HPE Instant On 1940 Switch Series Quick Setup Guide and Safety/Regulatory Information**—a printed guide shipped with your switch. Provides illustrations for basic installation and setup. Also includes product specifications, as well as safety and regulatory statements and standards supported by the switch.
- **HPE Instant On 1940 Switch Series Installation and Getting Started Guide**—(HPE website only). Provides detailed installation guide for your switch, including physical installation on your network, basic troubleshooting, product specifications, supported accessories, Regulatory and Safety information.
- **HPE Instant On 1940 Switch Series Management and Configuration Guide**—This guide describes how to manage and configure switch features using a web browser interface.
- **Release Notes**—(HPE website only). Provides information on software updates. The Release Notes describe new features, fixes, and enhancements that become available between revisions of the above guides.

Supported Features

The HPE Instant On 1940 Switch Series includes support for the following features:

- IEEE 802.3 10BASE-T
- IEEE 802.3u 100BASE-TX
- IEEE 802.3ab 1000BASE-T
- IEEE 802.3bz 2.5GBASE-T
- IEEE 802.3bz 5GBASE-T
- IEEE 802.3an 10GBASE-T
- Cable Test
- Concurrent management sessions – 5 total for any combination of supported methods:
  - HTTP
  - HTTPS
  - Telnet
  - SSH
- Power over Ethernet
  - IEEE 802.3af
  - IEEE 802.3at
  - IEEE 802.3bt
- IEEE 802.3x: Flow control
- IEEE 802.1Q: VLANs
- IEEE 802.1p: Priority Code Point
- ACLs (named ACL - IPv4 and MAC). Up to 100 ACLs.
- Access Control Entries (ACEs) – up to 2048
- Management Access Control and Administration List (MACAL)
- IEEE 802.1D: Spanning Tree Protocol
- IEEE 802.1W: Rapid Spanning Tree Protocol
- IEEE 802.1S: Multiple Spanning Tree Protocol supporting 8 MST instances
- IEEE 802.1AB: Link Layer Discovery Protocol (LLDP and LLDP-MED)
- IEEE 802.3ad Link Aggregation (LACP), Static/Dynamic:
  - 8 port units: up to 4 LAGs – up to 4 active port members in each
  - 24 port units: up to 8 LAGs – up to 4 active port members in each
  - 48 port units: up to 16 LAGs – up to 8 active port members in each
- Jumbo packet support (9216 bytes)
- Auto-MDI/MDIX
- Storm Control (global)
- Ingress Rate Limiting (per port)
- Port Mirroring (RSPAN)
- IGMP Snooping v1/v2/v3
- Global time scheduler (4 schedules)
  - Port Admin mode
  - PoE Admin mode
  - Access Control List (time-based ACLs)
  - LED Green Mode
- Static IPv4 address assignment – up to 32 interfaces
- Static IPv6 address assignment – on the management interface

- DHCP client
- DHCP fallback
- User accounts (up to 6, Read/Write, Read Only)
- Password management (aging, lockout, strength check, key word exclusion)
- SNMPv1/v2c/v3
- RMON (groups: Alarm, Event, History, and Statistics)
- RADIUS (up to 2 combined RADIUS authentication/accounting servers)
- RADIUS Accounting
- RADIUS assigned VLANs
- RADIUS MAC authentication (MAB)
- TACACS+ (primary and backup servers – 5 total)
- 802.1X port-based access control
- 802.1X Guest VLAN
- 802.1X authentication (EAP-MD5 supported)
- 802.1X MAC authentication (configurable username and password)
- Port Security
- Protected Ports
- ARP Attack Protection
- DoS Protection
- NTP
- Loop Protection
- Interface auto recovery
- Unidirectional Link Detection (UDLD)
- IEEE 802.3az: Energy Efficient Ethernet
- Routing (VLAN, Interface)
- Routing table – 992 entries
- Multicast groups – up to 1K
- DHCP relay (IPv4)
- DHCP snooping
- ARP table – 509 entries
- 802.1p/DSCP priority to queue mapping
- Number of egress queues (traffic priority) – 4
- Auto Voice VLAN
- Auto-WiFi/Auto-Camera VLAN
- Ping (IPv4/IPv6)
- Traceroute (IPv4/IPv6)
- Dual image support
- Email alerts
- Firmware update over HTTP, HTTPS, TFTP, SFTP, FTP, and SCP
- Configuration file backup and restore
- Syslog Log (local and remote)
  - 1 remote syslog server
  - Up to 200 entries on Buffered log
  - Up to 200 in Log file (Flash)

Chapter 1
Getting Started

This chapter describes how to make the initial connections to the switch and provides an overview of the web interface.

Connecting the Switch to a Network

To enable remote management of the switch through a web browser, the switch must be connected to the network. By default, the switch is configured to acquire an IP address from a DHCP server on the network. If the switch does not obtain an address from a DHCP server, the switch will be assigned the IP address 192.168.1.1.



The IP address of the switch can be determined by:

- Referencing the DHCP server.
- Accessing the Direct Ops interface via the USB-C console port.
- Using LLDP (Link Layer Discovery Protocol) through a connected neighbor switch.

To access the web interface on the switch by using the default IP address:

1. Connect the switch to the management PC or to the network using any of the available network ports.
2. Power on the switch.
3. Set the IP address of the management PC's network adapter to be in the same subnet as the switch. For example, set it to IP address 192.168.1.2, mask 255.255.255.0.
4. Enter the IP address 192.168.1.1 in the web browser. See Browser Support for web browser requirements.

Thereafter, use the web interface to configure a different IP address or configure the switch as a DHCP client so that it receives a dynamically assigned IP address from the network.

After the switch is able to communicate on your network, enter its IP address into your web browser's address field to access the switch management features.

Browser Support

The following browsers, with JavaScript enabled, are supported:

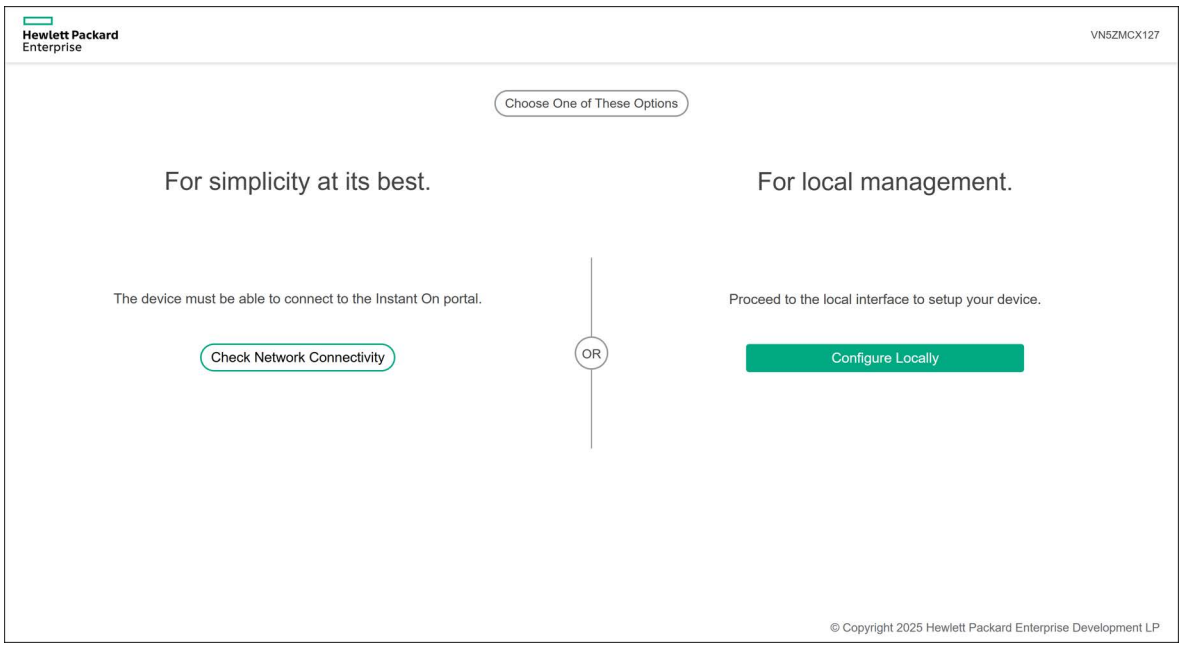
Table 1. Browser Support

Operating System	Browser
Firefox	145.0 146.0
Chrome	142143
Safari	18.6 26.2
Edge	139.0 143.0

Selecting Local Web Management Mode

Upon first connecting directly to the switch, you are presented with a welcome page indicating the choice to manage the switch locally using the web interface (detailed in this guide). The welcome page additionally provides an optional Network Connectivity interface designed to establish Internet access and facilitate connection to the Instant On cloud portal. Simply follow the instructions provided in the links to create, activate, and connect your switch to the cloud portal.

Figure 1. Selecting the Management Mode



NOTE

The screen captures shown in this document were taken from a sample system, with sample values.

Select **Configure Locally** to manage the switch locally using the web interface and continue on in this guide. If you would rather use the HPE Instant On Cloud Portal to manage the switch, see the *HPE Instant On 1940 Switch Series Installation and Getting Started Guide* and the *HPE Instant On User Guide*.

Chapter 2
Getting Started With the Web Interface

This chapter describes how to log on to the switch and provides information about the page layout.

Logging On

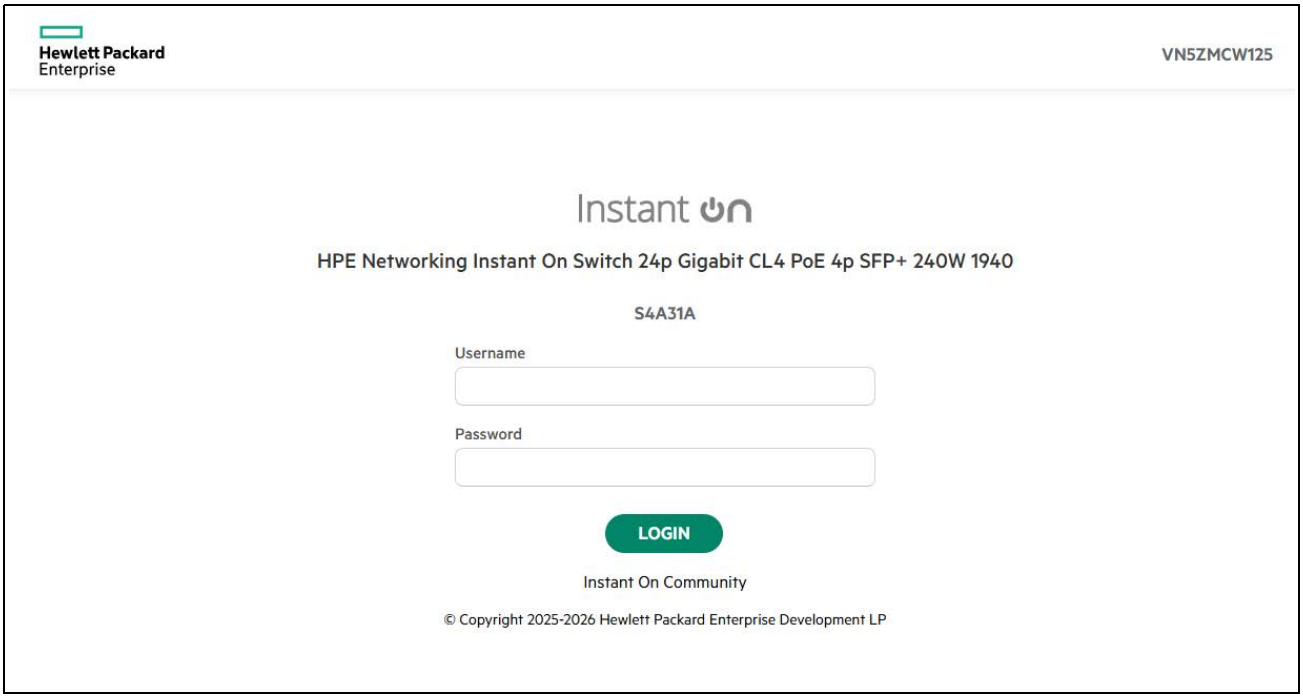
Follow these steps to log on through the web interface:

1. Open a web browser and enter the IP address of the switch in the web browser address field.
2. On the Login screen, enter the username and password (if one has been set), and then click **LOGIN**. On the initial login, the username is **admin** and there is no password.
3. Following the initial login, you are prompted to update the username and password.
4. Once the username and password are updated, you are required to login again using the newly configured username and password.

NOTE

To set the password or change the username, see User Accounts.

Figure 2. Login Screen



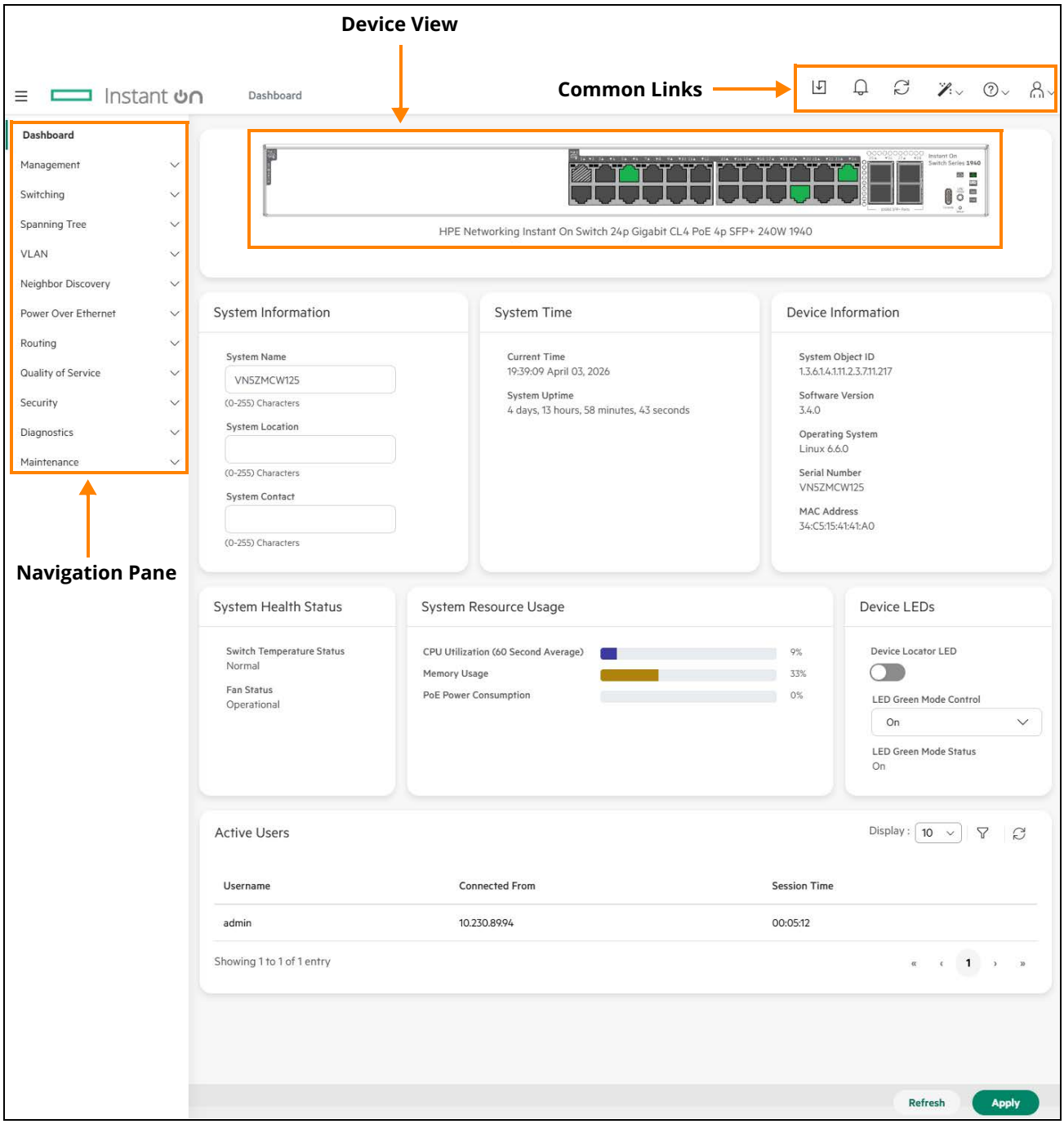
GUI Interface Layout and Features

The **Dashboard** displays when you first log on and when you click **Dashboard** in the navigation pane. See Dashboard for more information.

You can click the **Management** link beneath **Dashboard** to display the **Network Settings** page, which you use to set up a management connection to the switch. See Network Settings for more information.

The graphical switch displays summary information for the switch LEDs and port status. For information on this feature see Figure 9, Device View.

Figure 3. Interface Layout and Features

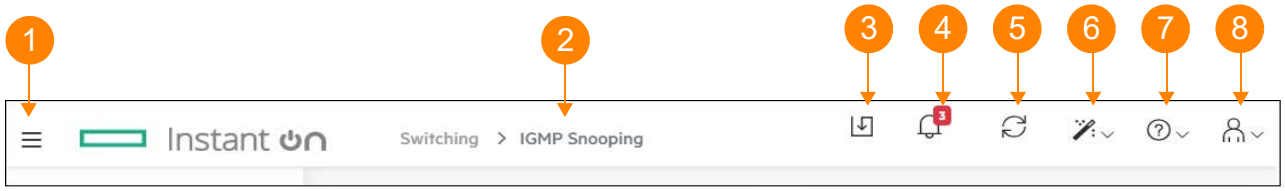


Click on any topic in the navigation pane to display related configuration options.

Common Page Elements

The upper panel includes the following buttons that are common to all the screens:

Figure 4. Upper Panel



Use the buttons to do the actions the following table describes.

Table 2. Upper Panel Components

Field	Description
1	Click **Show Navigation** ☰ to toggle the navigation pane that shows all the screens that are available for the switch.
2	This shows the current screen.
3	Click **Save Configuration** to save the current configuration. This icon appears only when there are unsaved changes.
4	Click **Notification** to view the latest notifications on the system in a panel that appears on the right side of the screen. Click again to close the panel. The notification has the following modes: · Grey: If there are no unread logs of severity Warning or higher. · Orange: If there are unread logs of severity Warning, but no unread logs of a higher severity. · Red: If there are unread logs of severity Error or higher.
5	Click **Refresh** to refresh the screen.
6	Click **Wizard** to use the Wizard to access the Getting Started Wizard, VLAN Configuration Wizard, or ACL Configuration Wizard. See Configuration Wizards.
7	Click **Help** on any page to display a help panel that explains the fields and configuration options on the page.
8	Click **Profile** to view your profile information, or to log out.

NOTE

If there is a recovery from an unexpected restart, an ⓘ icon appears in the upper panel. Click the icon to go to the logging page, which should provide additional information on the crash.

The bottom of the screen includes the following buttons:

- Click Apply to send the updated configuration to the switch. Applied changes update the switch running configuration and take effect immediately. If you want the switch to retain these changes across a reboot, you must first save the configuration.
- Click Refresh to refresh the page with the latest information from the switch.

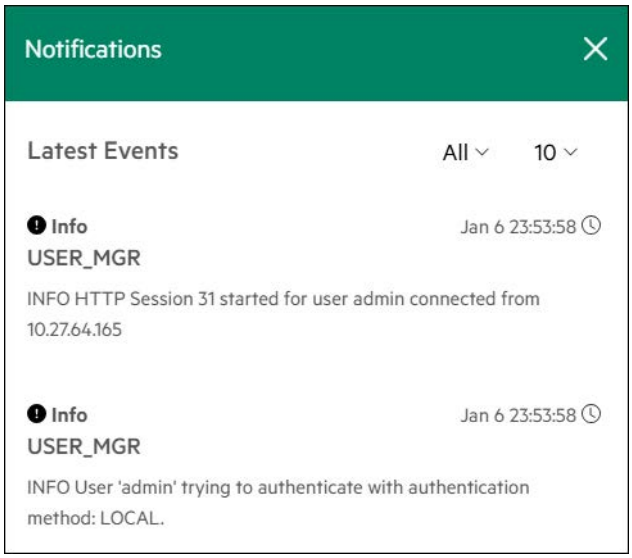
Saving Changes

When you click Apply, changes are saved to the running configuration file in RAM. Unless you save them to system flash memory, the changes will be lost if the system reboots. To save them permanently, click (**Save**) on the upper right side of the page.

Latest Events Panel

To view the Latest Events panel, click the Notification icon in the upper panel. The panel appears on the right side of the screen. Click again to close the panel.

Figure 5. Latest Events Panel



The Latest Events panel contains, by default, the most recent 10 logs in descending chronological order (the most recent event appears first). When a new event occurs, it will appear at the top of the panel, pushing the rest of the events down.

The Latest Events view can be configured to display events based on their severity. Click the All drop-down arrow to select event severities you want to see and filter unwanted events.

To set the number of displayed events (10, 20, 50), click the 10 drop-down icon at the top of the list, and select the appropriate setting.

Each event display has the following components:

- The name of the severity level.
- Date and time of the event.
- Text of the event.

Click the **Show More** button at the bottom of the list, to open the **Diagnostics > Logging** page with the full information on the events logged by the switch. For more information, see Logging.

Configuration Wizards

The HPE Networking Instant On 1940 Switch Series provides the following wizards:

- Getting Started Wizard
- VLAN Configuration Wizard
- ACL Configuration Wizard

To access the wizards, click (**Wizards**) near the top-right side of the screen.

Getting Started Wizard

Click **Wizards > Getting Started** Wizard to open the Getting Started Wizard that walks you through the stages of initial configuration of the basic management features of the HPE Networking Instant On 1940 Switch Series.

Figure 6. Getting Started Wizard



These are the steps that the wizard takes you through.

- Step 1—Introduction screen. Click the NEXT button to proceed with the configuration wizard.
- Step 2—Device Information, enter a System Name, System Location and System Contact information to help identify the device.

  Click **Next** to go to the next screen in the configuration wizard.
- Step 3—IP Address. Set up the IP interface. For more information on the fields in this screen, see Table 87, VLAN Configuration Fields, and Table 13, IPv4 Setup Fields.

  Click **Next** to go to the next screen in the configuration wizard.
- Step 4—System Time. Set up the device clock. For more information on the fields in this screen, see Table 19, Time Configuration Fields.

  Click **Next** to go to the next screen in the configuration wizard.
- Step 5—Summary. This screen details the changes that were configured. Click **Apply** to apply the changes to the next session.

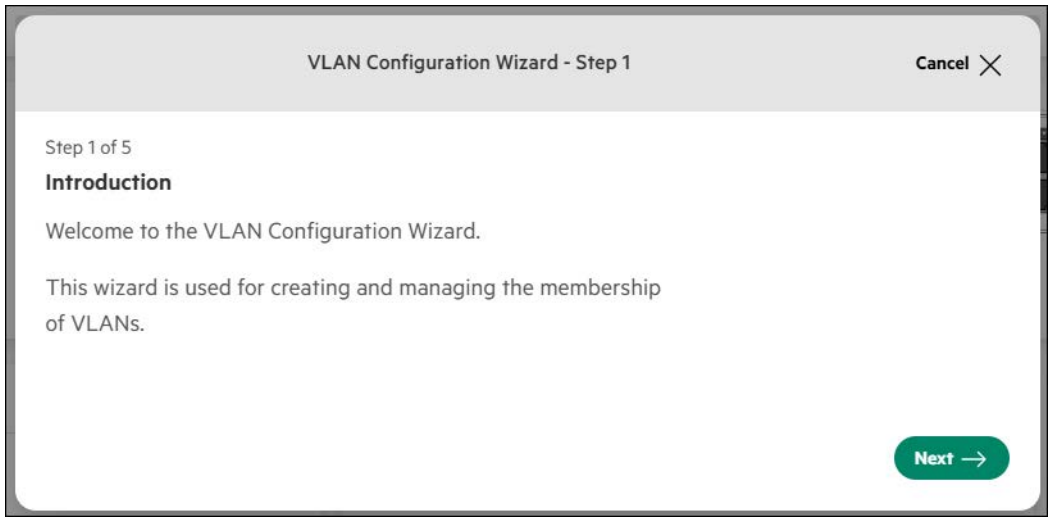
  Click **Next** to close the wizard.

The next screen shows that all the steps were taken and the configuration is successful.

VLAN Configuration Wizard

Click **Wizards > VLAN Configuration Wizard** to open the VLAN Configuration Wizard that walks you through the stages of initial configuration of a Virtual Local Area Network (VLAN) on the HPE Networking Instant On 1940 Switch Series.

Figure 7. VLAN Configuration Wizard



These are the steps that the wizard takes you through.

- Step 1—Introduction screen. Click the **Next** button to proceed with the configuration wizard.
- Step 2—VLAN. Select the VLAN type that you would like to create. If you create a new VLAN, you can enter a name for your VLAN. If you want to manage an existing VLAN, select it from the drop-down.

  Click **Next** to go to the next screen in the configuration wizard.
- Step 3—Untagged Interfaces. Select the interfaces that should be untagged. Use Ctrl-click to select specific interfaces, use Shift-click to select a range of interfaces. The selected interfaces are listed at the bottom of the screen. For more information on tagged and untagged interfaces, see Table 89, VLAN Membership - By VLAN Fields.

  Click **Next** to go to the next screen in the configuration wizard.
- Step 4—Tagged Interfaces. Select the interfaces that should be tagged. Use Ctrl-click to select specific interfaces, use Shift-click to select a range of interfaces. The selected interfaces are listed at the bottom of the screen.

  Click **Next** to go to the next screen in the configuration wizard.
- Step 5—Summary. This screen details the VLAN ID, and the untagged/tagged members of the VLAN. Click **Apply** to apply the changes to the next session.

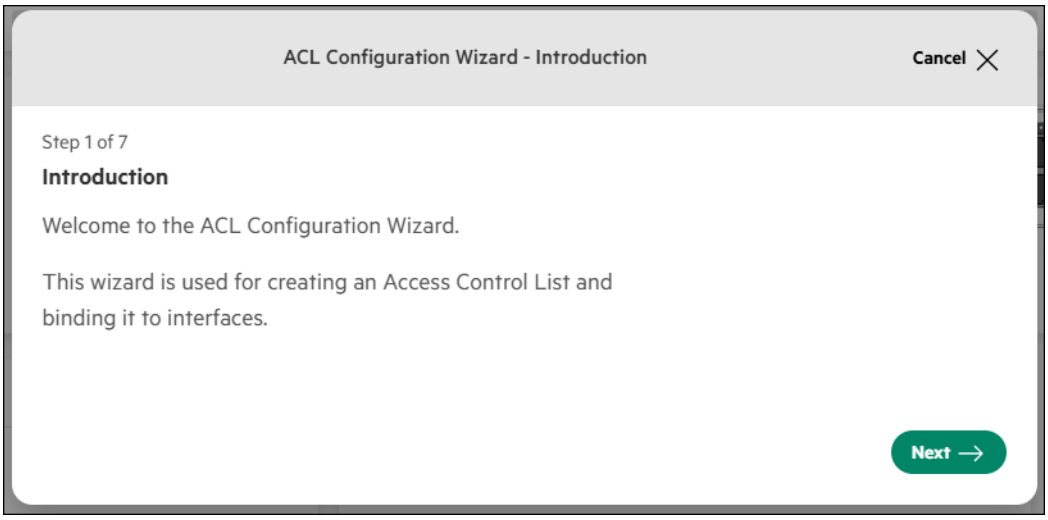
  Click **Close** to close the wizard.

The next screen shows that all the steps were taken and the configuration is successful. To view the changes, go to **VLAN > VLAN Configuration**.

ACL Configuration Wizard

Click the **ACL Configuration Wizard** button to open the ACL Configuration Wizard that walks you through the stages of initial configuration of an Access Control List (ACL) on the HPE Networking Instant On 1940 Switch Series switches.

Figure 8. ACL Configuration Wizard



These are the steps that the wizard takes you through.

- Step 1—Introduction screen. Click the **Next** button to proceed with the configuration wizard.
- Step 2—ACL Identifier. Select the ACL type that you would like to create. If you create a new ACL, you can enter a name for your ACL. If you want to manage an existing ACL, select it from the drop-down.

  Click **Next** to go to the next screen in the configuration wizard.
- Step 3—Traffic. Specify whether to configure the ACL to apply to all traffic or to specific packets.

  Click **Next** to go to the next screen in the configuration wizard.
- Step 4—Action. If the ACL applies to specific packets, configure the criteria to identify the traffic. Traffic can be identified by the source IP address in the packet, the destination IP address in the packet, or both.

  For traffic with the specified criteria, select the action to take when a packet matches the configured criteria. If you selected All Traffic in Step 3, select the action to take for all traffic. Select the interfaces that should be tagged. The action can be to either permit the traffic to flow toward its destination or deny the packet from continuing toward the destination.

  Click **Next** to go to the next screen in the configuration wizard.
- Step 5—Interface bindings. Use Ctrl-click to select specific interfaces where the ACL is applied. Use Shift-click to select a range of interfaces. Use the > and < arrows to move the selected interfaces into the appropriate field.

  Click **Next** to go to the next screen in the configuration wizard.
- Step 6—VLAN bindings. Use Ctrl-click to select specific VLANs where the ACL is applied. Use Shift-click to select a range of interfaces. Use the > and < arrows to move the selected interfaces into the appropriate field.
- Step 5—Summary. This screen details the ACL identifier, the match criteria (if the ACL applies to specific packets instead of all traffic), the action, and the interfaces and/or VLANs to which the ACL is applied. Click **Finish Wizard** to apply the changes to the next session.

  Click **Close** to close the wizard.

The next screen shows that all the steps were taken and the configuration is successful. To view the changes, go to **Quality of Service > Access Control Lists**.

Device View

The device view, shown below, displays at the top of some pages as a representation of the front panel of the physical switch to provide status information about individual ports. The device view enables easy system configuration and web-based navigation.

Figure 9. Device View

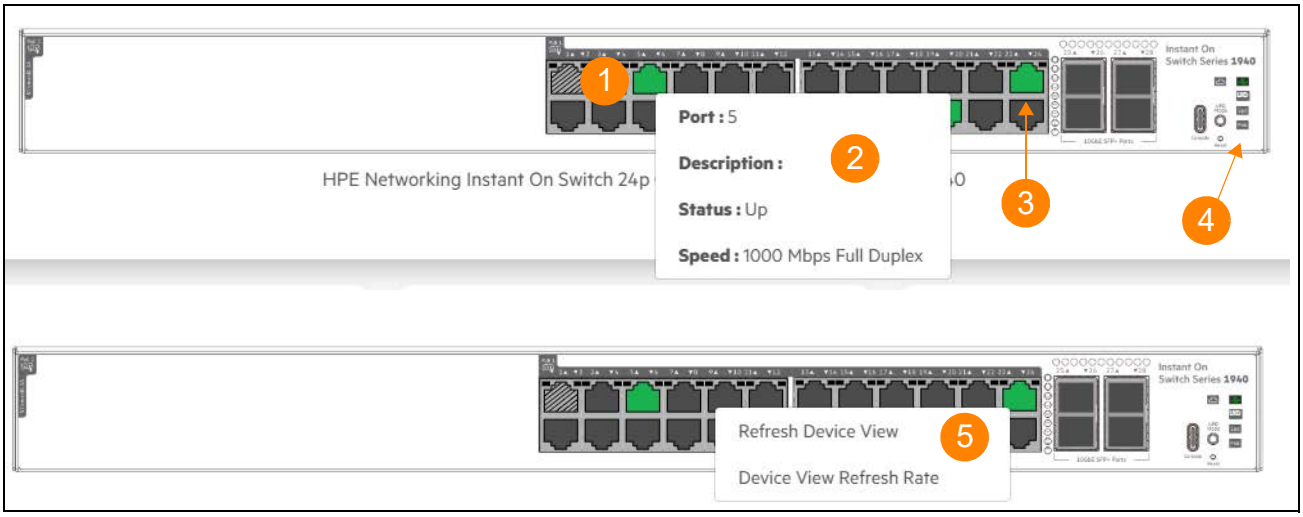


Table 3. Device View Components

Label	Description
1	Click any port to navigate to the **Switching > Port Configuration** page. For information about this page, see Port Configuration.
2	Port information. Hover over a port to display summary information about the port.
3	Port status indicator.
4	System LEDs, console port, and reset pin.
5	Right-click any port to display a menu with options to refresh the graphic display and to set the automatic refresh rate.

Port Information

You can hover the mouse on any port in the Device View to display the following information about the port:

- Port name. If the port is a trunk member, the trunk ID of the trunk is appended to the port name (for example: Port: 30 (TRK 7))
- Description. The description of the port, or the trunk if the port is a trunk member.
- The link status. Up, Down, Disabled, or Suspended. If the port is a trunk member, the status should be that of the trunk.
- Speed. The current speed of the port This field is only displayed for ports or trunks that are up. If the port is a trunk member, the speed is that of the trunk.

Port Status Indicator

Each port in the device view is visually represented by one of four different state images.

Port State	Image	Description
Up		The port is connected, enabled, and the link is up. This state image also applies to stack links in the Active state.
Down		The port is connected and enabled, but the link is down (likely because no cable is connected).
Disabled		The port has been administratively disabled. This state image also applies to stack links in the Inactive state.
Suspended		The port has an error condition and may or may not be active.

System LEDs, Console Port, and Reset Pin

Figure 10. System LEDs



NOTE

Some of the indications are visible only on the LED on the front panel and not in the GUI representation of the LED.

Table 4. System LED Indicators

Indicator	Color	Image	Description
Power	Green/ Orange		· On (green)—The switch is receiving power. This is an indication of normal operating condition. · Off—The switch is powered off or is NOT receiving power. · Slow flash (orange) o Self-test and initialization is in progress (boot-up). o A fault or self-test failure has occurred on the switch, one of the switch ports, the PSU, or the fan. The Status LED for the component with the fault will blink simultaneously.
UID (Locator)	Blue		· Blinking slowly—The locator function has been enabled to help physically locate the standalone unit, stack or a specific unit within the stack. · Off— Locator function was not activated by user, or if activated, the function was manually disabled by user, or the Locator function timer has expired.
Speed Mode	Green		· On—Speed Mode has been selected and port LEDs are used to indicate port speed information. · Off—Speed Mode is not selected.

Indicator	Color	Image	Description
PoE Mode	Green/ Orange		· On solid green—PoE Mode has been selected and port LEDs are used to indicate PoE information. · On solid orange—PoE Mode is selected, and a port has an internal PoE hardware failure. The specific port LED with fault also flashes in this case. · Slow flash orange—PoE Mode has NOT been selected, but a port has an internal PoE hardware failure. **NOTE**: In this case, the specific Port LED will NOT flash. · LED is off—PoE mode is not selected, and there are no PoE hardware failures on ports.
Cloud LED	Green/ Orange		Indicates the Cloud status of the switch: · Slow flash green—the switch is in the process of establishing a connection, to the cloud portal. · On green—the switch has successfully completed the "on-boarding process/procedure" and is fully operational, in cloud managed mode (connected to cloud portal). · On orange—The switch has detected an error/fault, and cannot connect to the cloud portal **NOTE**: The Global Status LED does not flash. · Alternating between green/orange—The switch is connected to the cloud portal, and ready for setup, through the App/Portal · This is a temporary state, which occurs while the switch is connected to the cloud portal, but not fully on-boarded yet.
LED Mode	—		This button determines the Port LED indication. Press this button to change to a different mode. The supported modes are: · Link/activity—this is the default mode of device operation. There is no indication for this mode (speed and PoE Mode LEDs are off). The LED Mode will switch back to the link/activity state 10 minutes after selecting a non-default mode (speed or PoE) · Speed · PoE (for units that support PoE) The speed and PoE LED modes have specific global LED indicating the selected mode.

In addition to the system LEDs, the front-panel also includes a console port and reset pin, as the following table describes.

Table 5. Console Port and Reset Pin

Port State	Image	Description
Console Port		USB-C console port used to access the Direct Ops command line interface.
Reset Pin		Reset the system. Gently insert a small, stiff tool (such as a straightened paperclip or SIM eject tool) into the circular opening until the reset button in the opening is pressed, then immediately remove the tool to reset the switch. Press and hold for 5 seconds or longer to reset the switch to factory defaults.

The Dashboard page provides key information, including a graphical representation of the switch, the configurable switch name and description, system time, and switch details such as software and operating system versions. It also displays resource-usage statistics and allows you to manage LED behavior through the Locator LED and LED Green Mode features.

The Dashboard is composed of multiple tiles, each presenting specific information about the switch. Each tile is described in this chapter.

Dashboard Page

The Dashboard page is displayed when you first log on, or when you click **Dashboard** in the navigation pane.

Device View

The top of the Dashboard page shows a graphical representation of the switch front panel. This panel view has a display of the ports, each with its current status.

Click a port in this screen, to open the **Switching > Port Configuration** page. For more information, see Device View.

The values that appear in the figures in this document are example values.

System Information

Figure 11. System Information Tile

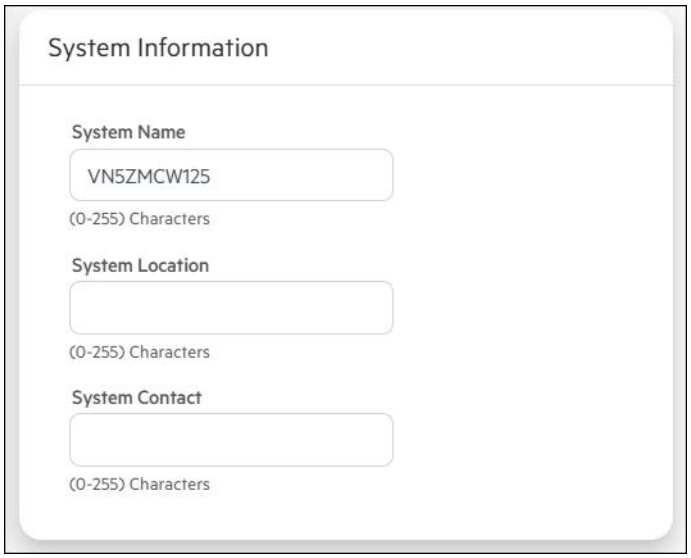


Table 6. System Information Fields

Field	Description
System Name	Enter the preferred name to identify this switch. A maximum of 255 alpha-numeric, case-sensitive characters is allowed. The system name must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. The user-configurable switch name will appear in the login screen banner. The default value is the switch serial number.
System Location	Enter the location of this switch. A maximum of 255 alpha-numeric, case-sensitive characters is allowed, including special characters (!, #, $, %, &, ', (,), *, +, -, ., /, :, ;, <, =, >, ?, @, [,], \, ^, _, `, {, } , ~, and space). This field is blank by default.
System Contact	Enter the name of the contact person for this switch. A maximum of 255 alpha-numeric, case-sensitive characters is allowed, including special characters (!, #, $, %, &, ', (,), *, +, -, ., /, :, ;, <, =, >, ?, @, [,], \, ^, _, `, {, } , ~, and space). This field is blank by default.

System Time

Figure 12. System Time Tile

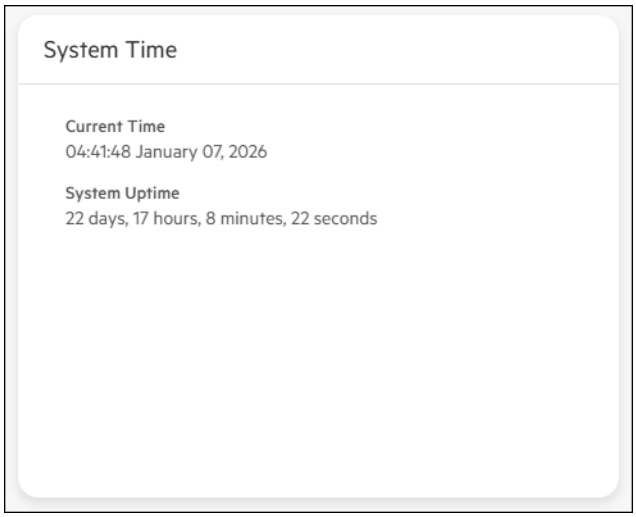


Table 7. System Time Fields

Field	Description
Current Time	The current time in hours, minutes, and seconds as configured (24-hr format), and the current date in month, day, and year format.
System Uptime	The time in days, hours, minutes, and seconds since the last switch reboot.

Device Information

Figure 13. Device Information Tile

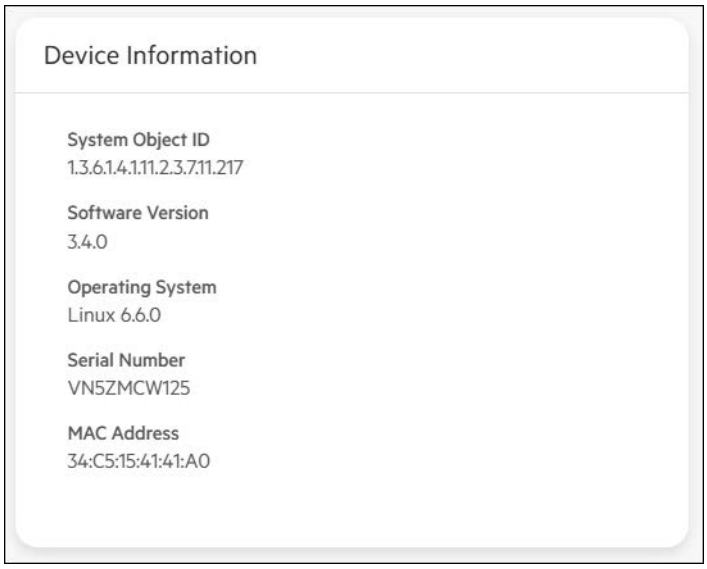


Table 8. Device Information Fields

Field	Description
System Object ID	The base object ID for the switch's enterprise MIB.
Software Version	The version of the code running on the switch.
Operating System	The version of the operating system running on the switch.
Serial Number	The unique serial number assigned to the switch.
MAC Address	Device base MAC address.

System Health Status

Figure 14. System Health Status Tile

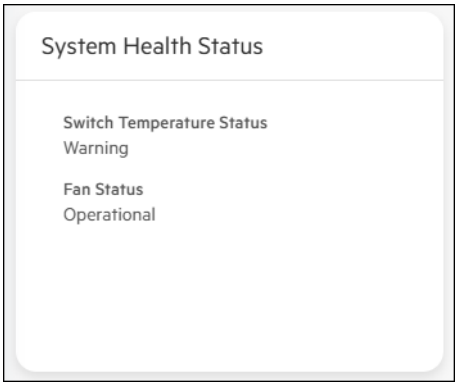


Table 9. System Health Status Fields

Field	Description
Switch Temperature Status	The general temperature of the switch. · Normal: The temperature is less than or equal to 40°C. · Warning: The temperature is greater than 40°C and less than or equal to 50°C. · Critical: The temperature is greater than 50°C.
Fan Status	The status of the fan. · Operational: All the fans are working. · Failed: At least one of the fans has failed.

System Resource Usage

Figure 15. System Resource Usage Tile

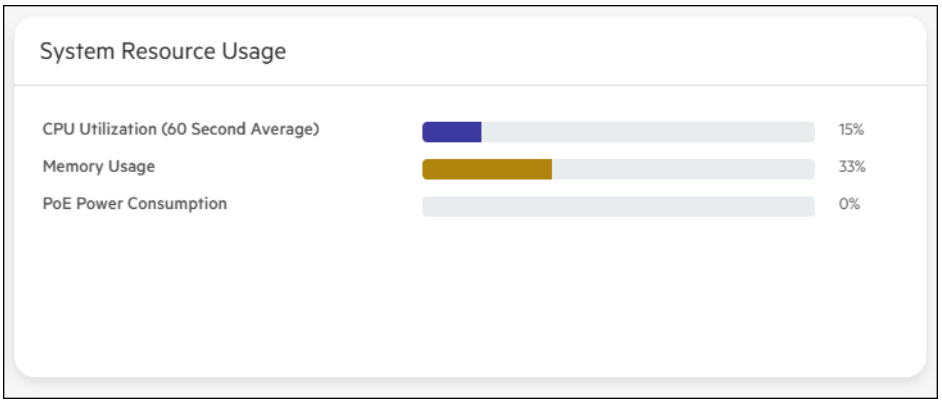


Table 10. System Resource Usage Fields

Field	Description
CPU Utilization	The percentage of CPU utilization for the entire system averaged over the past 60 seconds.
Memory Usage	The percentage of total available system memory (RAM) that is currently in use.
PoE Power Consumption	Current PoE power consumption as a percentage of total available PoE power budget.

Device LEDs

Figure 16. Device LEDs Tile

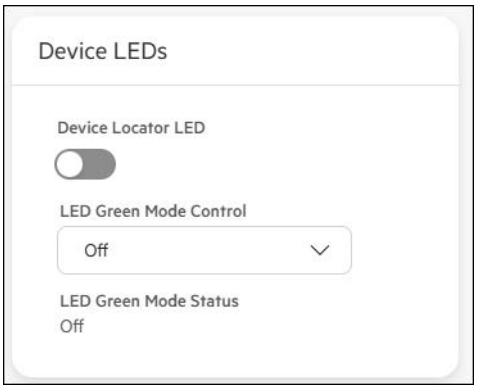


Table 11. Device LEDs Fields

Field	Description
Device Locator LED	Enable this feature to start flashing the physical device locator LED. After 30 minutes, the LED will automatically turn off if it has not been turned off manually. · —Disabled · —Enabled
LED Green Mode Control	Configure the switch LEDs (On/Off) or associate them with an absolute or periodic schedule to turn them on and off for specified periods. Turning the LEDs off can reduce switch power consumption.
LED Green Mode Status	Shows the status of the port LEDs (On/Off).

Active Users

The Active Users shows details about all current management sessions.

Figure 17. Active Users Tile



Table 12. Active Users Fields

Field	Description
Username	The username of each logged in user.
Connected From	The IP address from which the user logged in. If the user is connect through the console port, the field displays EIA-232.
Session Time	The amount of time the user session has been active, in hours, minutes, and seconds.

You can use the Management pages to set how a management computer connects to the switch, configure system time, manage user accounts and schedules, and secure management access.

Network Settings

Use the Network Settings page to configure the switch's management interface, which is defined by its IP address, subnet mask, and gateway. These settings apply only to management access and do not affect the front-panel switching ports, except that the management VLAN ID (PVID) determines which VLAN is used for management traffic.

To display the Network Settings page, click **Management > Network Settings**.

IPv4 Setup Tab

To view the IPv4 Setup options shown in Figure 18, click on the IPv4 Setup tab in the tile.

In the example configuration in Figure 18, the switch is configured to acquire its IPv4 address through DHCP, which is the default setting. By default, access to the management software is restricted to members of the management VLAN, which is VLAN 1 by default.

Figure 18. IPv4 Setup Tab

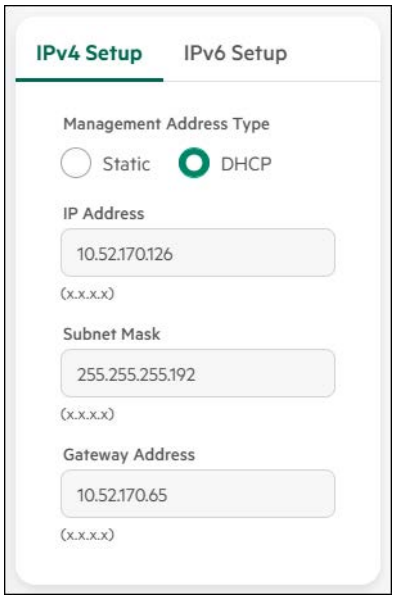


Table 13. IPv4 Setup Fields

Field	Description
Management Address Type	Select the type of network connection: · Static—Select this option to enable the IP address, subnet mask, and gateway fields for data entry. · DHCP—Select this option to enable the switch to obtain IP information from a DHCP server on the network. If the DHCP server responds, then the assigned IP address is used. If DHCP is enabled but the DHCP server does not respond, the default static IP address 192.168.1.1 is used. DHCP operation is enabled by default. When a DHCP server assigns an IP address to the switch, it specifies the time for which the assignment is valid. After the time expires, the server may reclaim the address for assignment to another device. When DHCP is enabled, you can click to send a request to the DHCP server to renew the lease. Only a user-configured static IP address is saved to flash. **CAUTION:** Changing the protocol type or IP address discontinues the current connection; you can log on again using the new IP information.
IP Address	The IPv4 address for the switch. If the Protocol Type is set to DHCP, this field displays the IP address assigned by the DHCP server. If the Protocol Type is set to Static, the IP address can be manually configured in this field. The default IP address is 192.168.1.1.
Subnet Mask	The IPv4 subnet address to be used. The default IP subnet address is 255.255.255.0.
Gateway Address	The IPv4 gateway address to be used. When in doubt, set this to be the same as the default gateway address used by your PC.

IPv6 Setup Tab

To view the IPv6 Setup options, click on the IPv6 Setup tab in the tile.

Figure 19. IPv6 Setup Tab

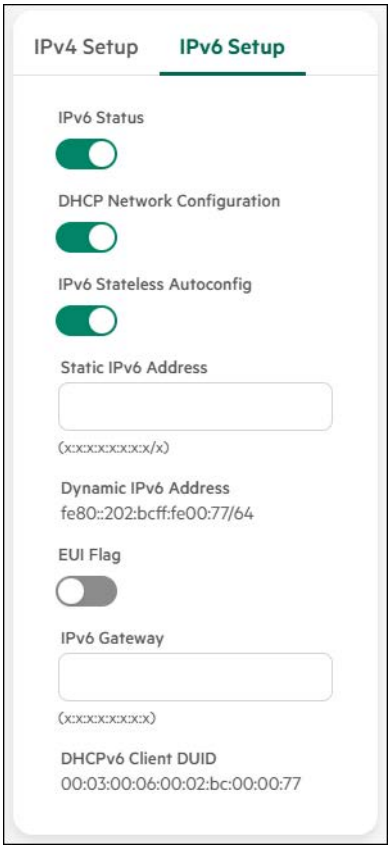


Table 14. IPv6 Setup Fields

Field	Description
IPv6 Status	Enables or disables the IPv6 administrative mode on the network interface.
DHCP Network Configuration	Specify whether the device should attempt to acquire network information from a DHCPv6 server. Selecting **None** disables the DHCPv6 client on the network interface.
IPv6 Stateless Autoconfig	Sets the IPv6 stateless address autoconfiguration mode on the network interface. · Enabled—The network interface can acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of Router Advertisement messages. · Disabled—The network interface will not use the native IPv6 address autoconfiguration features to acquire an IPv6 address.
Static IPv6 Addresses	Specify the IPv6 address to add to the interface.
Dynamic IPv6 Addresses	Lists the IPv6 addresses on the network interface that have been dynamically configured through IPv6 autoconfiguration or DHCPv6.
EUI Flag	Select this option to enable the Extended Universal Identifier (EUI) flag for IPv6 address, or clear the option to omit the flag.
IPv6 Gateway	Specify the default gateway for the IPv6 network interface.
DHCPv6 Client DUID	The client identifier used by the DHCPv6 client when sending messages to the DHCPv6 server.

HTTP/S Management Settings

Use this tile to view and modify the HTTP or Secure HTTP (HTTPS) settings on the switch. HTTPS increases the security of web-based management by encrypting communication between the administrative system and the switch.

To set HTTP management, click on the **HTTP Management** tab, to set HTTPS management, click the **HTTPS Management** tab.

Figure 20. HTTP/S Management Settings Tabs

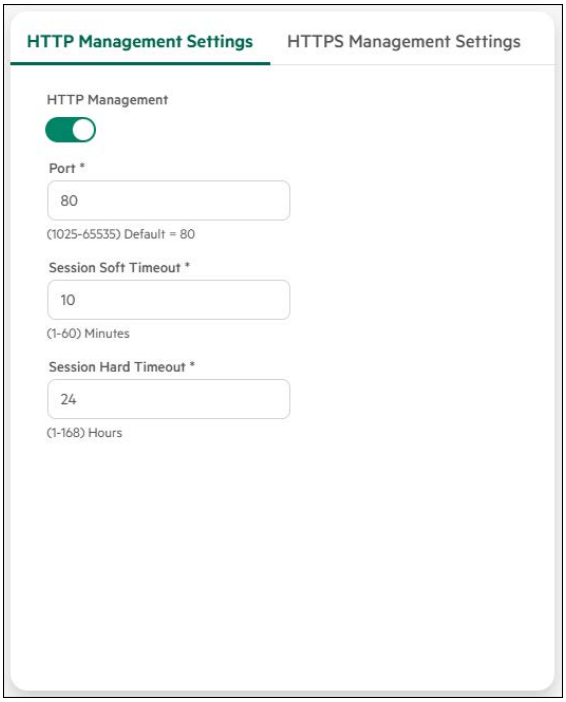


Table 15. HTTP/S Management Settings Fields

Field	Description
HTTP/S Management	Enables or disables the HTTP or HTTPS administrative mode. When enabled, the switch can be accessed through a web browser using the HTTP/S protocol. By default HTTP and HTTPS management are both enabled. · —Disabled · —Enabled
Port	The TCP port number on which the HTTP/S server listens for requests. Existing HTTP and HTTPS login sessions are closed whenever this value is changed. All new HTTP and HTTPS sessions must use the new port number. **Note:** Before changing this value, check your system to make sure the desired port number is not currently being used by any other switch service. For HTTP the default is 80, for HTTPS the default is 443. The valid range for this port number is 1025-65535.
Session Soft Timeout	Session inactivity timeout value, in minutes. A logged-in user that does not exhibit any HTTP/S activity for this amount of time is automatically logged out of the HTTP/S session. By default, the timeout is 10 minutes. The valid range is 1-60.

Field	Description
Session Hard Timeout	Session hard timeout value, in hours. A user connected to the switch through an HTTP/S session is automatically logged out after this amount of time regardless of the amount of HTTP/S activity that occurs. By default, the timeout is 24 hours. The valid range is 1-168.

Management VLAN Settings

Use this tile to view and modify the management VLAN settings on the switch.

Figure 21. Management VLAN Settings Tile

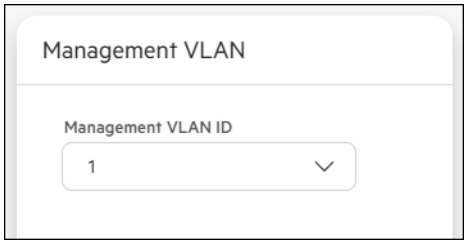


Table 16. Management VLAN Settings Field

Field	Description
Management VLAN ID	The Management IP address configured on this tile is applied to the Management VLAN. By default, the management VLAN ID is 1. The management VLAN can be any value between 1 and 4092. All ports are members of VLAN 1 by default; the administrator may want to create a different VLAN to assign as the management VLAN. In this case, the IP address is applied to the other VLAN configured by the user. A VLAN that does not have any member ports (either tagged or untagged) should not be configured as the management VLAN. When the network protocol is configured to be DHCP, any change in the configured management VLAN ID may cause disruption in connectivity because the switch acquires a new IP address when the management subnet is changed. To reconnect to the switch, the user must determine the new IP address by viewing the log on the DHCP server.

Telnet Settings

This page displays the current value of the telnet configuration parameters for the device.

Figure 22. Telnet Session Configuration Tile

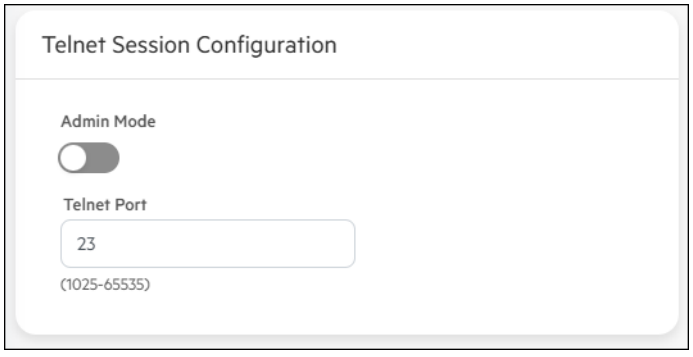


Table 17. Telnet Session Configuration Field

Field	Description
Admin Mode	Enables or disables the telnet administrative mode. When enabled, the device may be accessed through the telnet port (23). Disabling this setting disconnects all existing telnet connections and shuts down the telnet port in the device. Telnet admin mode is disabled by default.
Telnet Port	The TCP port number on which the telnet server listens for requests. Existing telnet login sessions are not affected by a change in this value, although establishment of any new telnet sessions must use the new port number.

NOTE

Before changing this value, check your system (for example, using netstat) to make sure the desired port number is not currently being used by any other service.

SSH Settings

Use this page to view and modify the Secure Shell (SSH) server settings on the device. SSH is a network protocol that enables access to the CLI management interface by using an SSH client on a remote administrative system. SSH is a more secure access method than Telnet because it encrypts communication between the administrative system and the device.

Figure 23. SSH Configuration Tile



Table 18. SSH Configuration Field

Field	Description
SSH Admin Mode	Enables or disables the SSH administrative mode. When enabled, the device may be accessed through the SSH port (22) by using an SSH client on a remote system. Disabling this setting disconnects all existing SSH connections and shuts down the SSH port in the device. SSH admin mode is enabled by default. · —Disabled · —Enabled
SSH Port	The TCP port number on which the SSH server listens for requests. Existing SSH login sessions are not affected by a change in this value, although establishment of any new SSH sessions must use the new port number.

NOTE

Before changing this value, check your system (for example, using netstat) to make sure the desired port number is not currently being used by any other service.

Click **Apply** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.



A power cycle does not reset the IP address to its factory-default value. If the configured IP address is unknown, you can perform a manual reset to factory defaults to regain access to the switch (see Reset to Factory Defaults).



Changing the management port from the default configuration not only restricts access to the web UI but also impacts the following protocols: DHCP, SNMP, NTP, and TFTP.

System Time

Click **Management > System Time** to configure the system clock, NTP client functionality, system time zone, and daylight saving time settings.

Time Configuration

You can configure the system time manually or acquire time information automatically from a Network Time Protocol (NTP) server. Using NTP ensures accurate network switch clock time synchronization up to the millisecond. Time synchronization is performed by an NTP server. The software operates only as an NTP client and cannot provide time services to other systems.

Figure 24. Time Configuration Tile

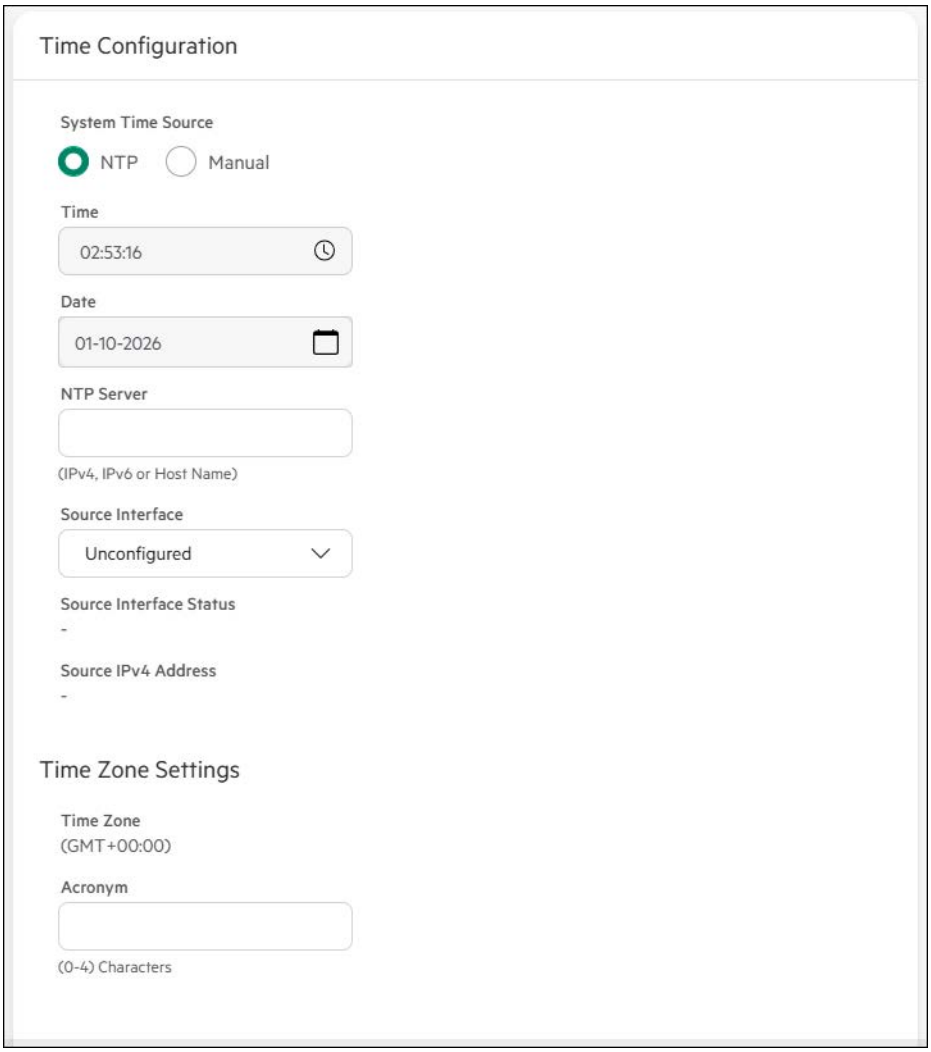


Table 19. Time Configuration Fields

Field	Description
System Time Source	Select **NTP** (Network Time Protocol) to configure the switch to acquire its time settings from an SNTP server. When selected, only the SNTP Configuration fields are available for configuration. Select **Manual** to disable SNTP and configure the time manually. You can manually set the date and time in the fields mentioned below.
Time	The current time. This value is determined by an NTP server. When NTP is disabled, the system time increments from the active image creation time stamp. You can also configure the time manually.
Date	The current date. This value is determined by an SNTP server. When SNTP is disabled, the system time increments the active image creation time stamp.
NTP Server	Specify the address of the NTP server to which requests should be sent. The address can be one of the following: · IPv4 address · IPv6 global address, in the format of X:X:X:X::X · IPv6 link local address (with zone), in the format of X:X:X:X::X · Hostname—Specify the server hostname

Field	Description
Source Interface	Configure the type of interface used as the source for outgoing NTP packets. This physical or logical interface is used as the NTP client source interface. When an IP address is configured on the source interface, this address is used for all NTP communications between the local NTP client and the remote NTP server. The IP address of the designated source interface is used in the IP header of NTP management protocol packets. This allows security devices, such as firewalls, to identify all source packets coming from a specific device. The available options are: · Unconfigured—The primary IP address of the originating (outbound) interface is used as the source address. · Network Port—The Network port source IP is used as the source address.
Source Interface Status	Indicates the current link status of the selected source interface. The possible values are: · Link up. · Link down.
Source IPv4 Address	Displays the primary IPv4 address associated with the selected source interface.
Time Zone Settings	
Time Zone	The currently set time zone. The default is (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London. **Note:** Click the **Edit Time Zone** button to configure the time zone.
Acronym	The acronym for the time zone, if one is configured on the system (for example, PST, EDT).

Daylight Saving Configuration

The Daylight Saving Configuration tile is used to configure if and when Daylight Saving Time (DST) occurs within your time zone. When configured, the system time adjusts automatically one hour forward at the start of the DST period, and one hour backward at the end.

To display the Daylight Saving Configuration tile, click **Management > System Time** in the navigation pane.

Figure 25. Daylight Saving Configuration Tile

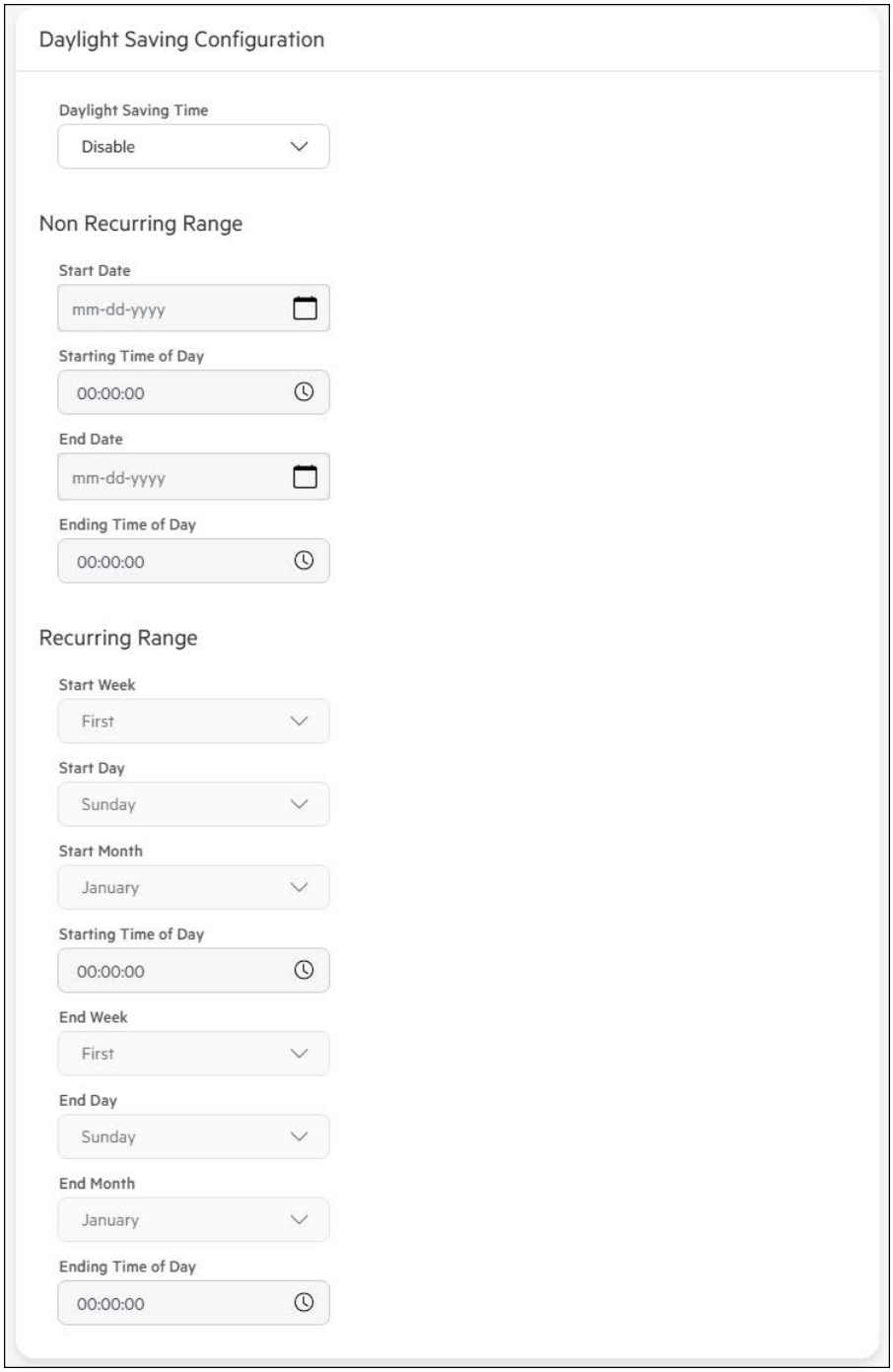


Table 20. Daylight Saving Time Configuration Fields

Field	Description
Daylight Saving Time	Select how DST will operate: · Disable—No clock adjustment will be made for DST. This is the default selection. · Recurring—The settings will be in effect for the upcoming period and subsequent years. · EU—The system clock uses the standard recurring daylight saving time settings used in countries in the European Union. · USA—The system clock uses the standard recurring daylight saving time settings used in the United States. · Non-Recurring—The settings will be in effect only for a specified period during the year (that is, they will not carry forward to subsequent years). When a DST mode is enabled, the clock will be adjusted one hour forward at the start of the DST period and one hour backward at the end.
Non Recurring Range	Set the following to indicate when the change to DST occurs and when it ends. These fields are editable when Non-Recurring is selected as the DST mode: · Start Date—Use the calendar to set the day, month, and year when the change to DST occurs. · Starting Time of Day—Set the hour and minutes when the change to DST occurs. Or, enter the hours and minutes in 12-hour format (HH:MM). · End Date—Use the calendar to set the day, month, and year when the change from DST occurs. · Ending Time of Day—Set the hour and minutes when the change from DST occurs. Or, enter the hours and minutes in 12-hour format (HH:MM).
Recurring Range	When Recurring is selected as the DST mode, the following fields display: · Start/End Week—Set the week of the month, from 1 to 5, when the change to/from DST occurs. The default is 1 (the first week of the month). · Start/End Day—Set the day of the week when the change to/from DST occurs. · Start/End Month—Set the month when the change to/from DST occurs. · Starting/Ending Time of Day—Set the hour and minutes when the change to/from DST occurs.

Click **Apply** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

User Management

By default, the switch contains only the *admin* user account, which has read/write privileges. Upon first login, you are prompted to change the default username and password.

Click **Management** > **User Management** to display the web pages to add switch management users, change user settings, or remove users.

Logged In Sessions

The Logged In Sessions tile identifies the users that are logged in to the management interface of the switch. The tile also provides information about their connections.

Figure 26. Logged In Sessions Tile



Table 21. Logged In Sessions Fields

Field	Description
User Name	The name that identifies the user account.
Connected From	Identifies the administrative system that is the source of the connection. For remote connections, this field shows the IP address of the administrative system.
Session Time	Shows the amount of time in hours, minutes, and seconds since the user logged onto the system.
Session Type	Shows the type of session, which can be Serial Port, Telnet, SSH, HTTP or HTTPS.

User Accounts

If you log on to the switch with a user account with read/write privileges (such as admin), you can use the User Accounts tile to assign passwords and set security parameters for the User accounts. The maximum number of user accounts can be 6. You can delete all accounts except for one Read/Write account.

Figure 27. User Accounts Tile

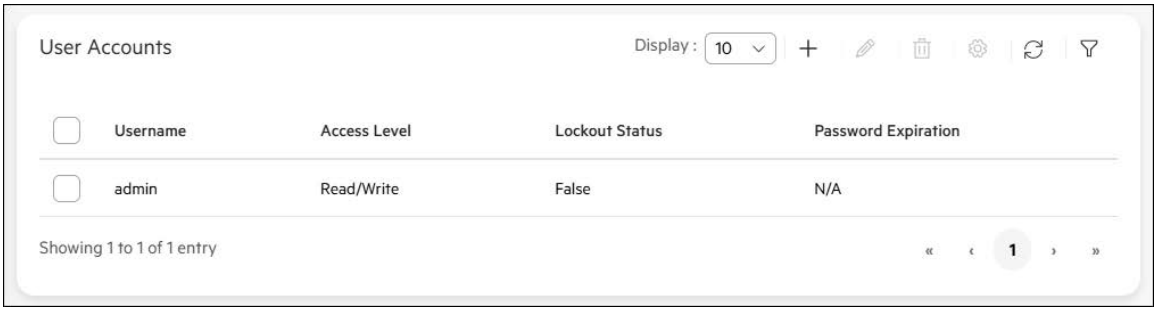


Table 22. User Accounts Fields

Field	Description
Username	A unique ID or name used to identify this user account.
Access Level	Indicates the access or privilege level for this user. The options are: · Read Write—The user can view and modify the configuration. · Read Only—The user can view the configuration but cannot modify any fields.
Lockout Status	Provides the current lockout status for this user. If the lockout status is True, the user cannot access the management interface even if the correct username and password are provided. The user has been locked out of the system due to a failure to supply the correct password within the configured number of login attempts.
Password Expiration	Indicates the current expiration date (if any) of the password.

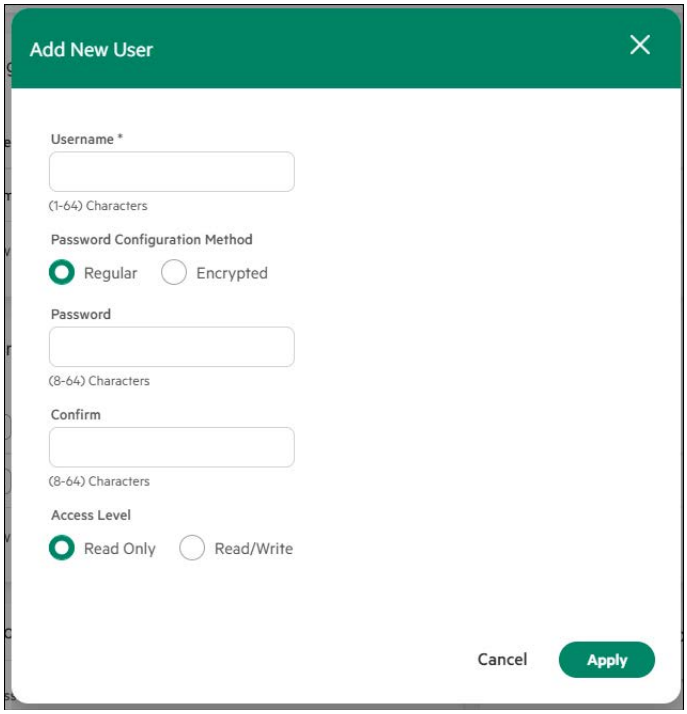
From this page, use the available buttons to add or remove users, or to edit the settings for an existing user. Use the ⚙ (**Unlock Account)** button to unlock a user account.

Adding a User Account

To add a new user account:

1. From the User Accounts tile, click + (**Add**).
   The Add New User dialog box displays.

Figure 28. Add New User Dialog



2. Configure the settings for the new user.

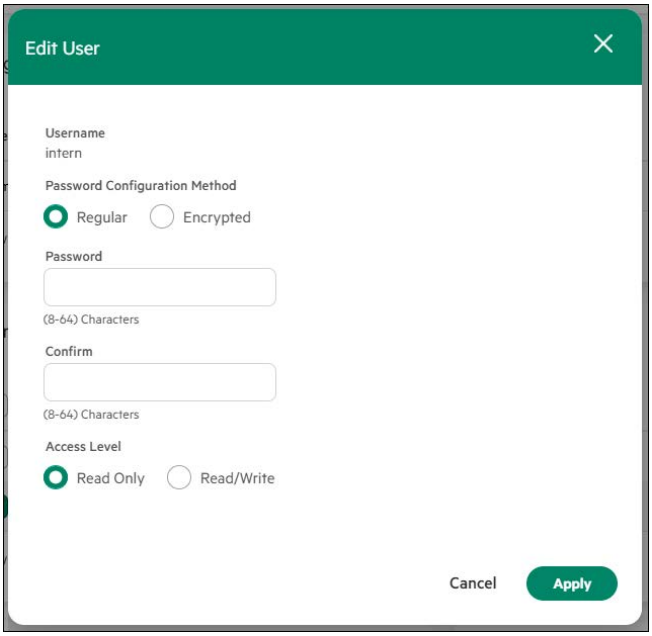
Field	Description
Username	Enter the name you want to give to the new account. (You can only enter data in this field when you are creating a new account.) Usernames are up to 64 alphanumeric characters in length and are not case sensitive. Valid characters include all the alphanumeric characters and the dash ('-') and underscore ('_') characters.
Password Configuration Method	Specify Regular for unencrypted passwords, or Encrypted to enter a password that is already encrypted. This option is usually used when the password is copied from an existing configuration file.
Password	Enter the password for the account. It will not display as it is typed, only asterisks (*) or dots (.) will show based on the browser used. By default, passwords must be greater than or equal to eight characters and can be up to 64 characters in length, and are case sensitive.
Confirm	Enter the password again, to confirm that you entered it correctly. This field will not display, but will show asterisks (*) or dots (.), based on the browser you use.
Access Level	Indicates the access or privilege level for this user. The options are: · Read Write—The user can view and modify the configuration. · Read Only—The user can view the configuration but cannot modify any fields.

3. Click **Apply**.

Changing User Account Information

You cannot change the name of an existing user, but you can change the password, privilege, and password settings. To change user information, select the username with the information to change and click the (**Edit**) button. Update the fields as needed, and click **Apply**.

Figure 29. Edit Existing User Dialog



Removing a User Account

To remove any of the user accounts, select one or more users to remove. Click the **(Remove) button** to delete the selected users. You must confirm the action before the user is deleted.

Account Security Settings

Use this tile to configure rules for locally-administered passwords.

Figure 30. Account Security Settings Tile

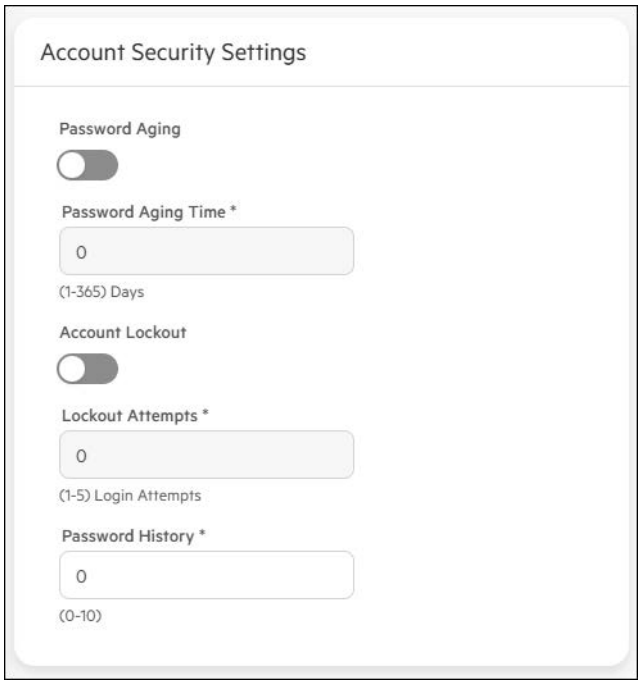


Table 23. Account Security Settings Fields

Field	Description
Password Aging	Activate this control to enable setting a maximum age for a user password. Users will need to change their password before the maximum age.
Password Aging Time	Set the amount of days that the password can be used before it is changed to a new password.
Account Lockout	Activate this control to enable setting a maximum number of password attempts before the account is locked.
Lockout Attempts	After a user fails to log in this number of times, the user is locked out until the password is reset by the administrator.
Password History	The number of previous passwords that are retained to prevent password reuse. This helps to ensure that a user does not attempt to reuse the same password too often.

Password Keyword Exclusion

Use the Keyword Exclusion configuration option to add keywords that are not allowed as part of a password. Up to three excluded keyword names are allowed.

Figure 31. Password Keyword Exclusion Tile



Table 24. Password Keyword Exclusion Fields

Field	Description
Keyword	The list of keywords that a valid password must not contain. Excluded keyword checking is case-insensitive. Additionally, a password cannot contain the backwards version of an excluded keyword. For example, if pass is an excluded keyword, passwords such as 23passA2c, ssapword, and PAsSwoRD are prohibited. Use the plus and minus buttons to perform the following tasks: · To add a keyword to the list, click the + (**Add**) button, type the word to exclude in the Keyword field, and click **Apply**. · To remove one or more keywords from the list, select each keyword to delete and click the (Remove) button.

Password Strength Rules

The rules you set determine the strength of local passwords that switch users can associate with their usernames. The strength of a password is a function of length, complexity, and randomness.

Figure 32. Password Strength Rules Tile

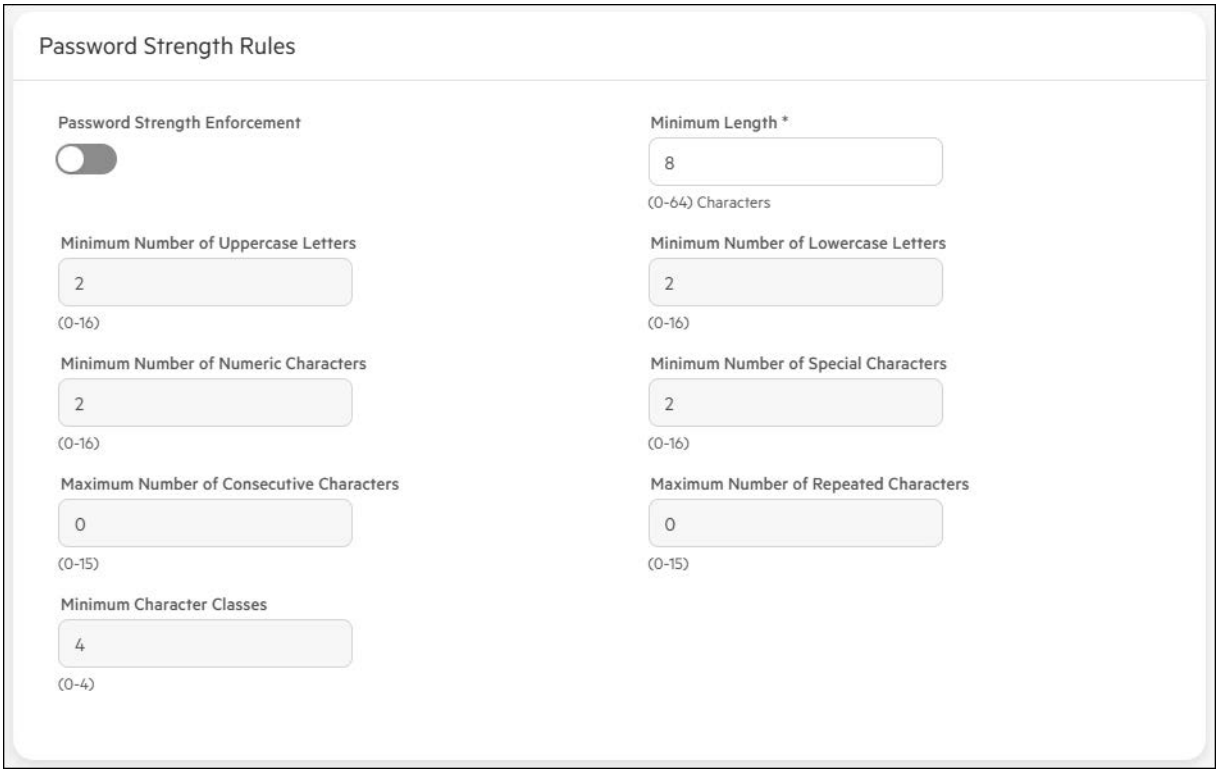


Table 25. Password Strength Rules Fields

Field	Description
Password Strength Enforcement	Enable or disable the password strength check feature. Enabling this feature forces the user to configure passwords that comply with the strong password configuration specified in the following fields.
Minimum Length	Passwords must have at least this many characters (0 to 64).
Minimum Number of Uppercase Letters	The minimum number of upper-case letters that a valid password must contain.
Minimum Number of Lowercase Letters	The minimum number of lower-case letters that a valid password must contain.
Minimum Number of Numeric Characters	The minimum number of numeric characters that a valid password must contain.
Minimum Number of Special Characters	The minimum number of special characters (such as the keyboard symbols @, $, &) that a valid password must contain.
Maximum Number of Consecutive Characters	The maximum number of characters belonging to a sequence that are allowed to occur in a valid password. Consecutive characters are defined as a sequential pattern of case-sensitive alphabetic or numeric characters, such as “2345” or “def” or “YZ”.
Maximum Number of Repeated Characters	The maximum number of characters of any type that are allowed to repeat in a valid password. Repetition is defined as the same character occurring in succession anywhere within the password, such as “11” or “%%%” or “EEEE”.

Field	Description
Minimum Character Classes	Specify the minimum number of character classes a password must contain. There are four character classes: · Uppercase · Lowercase · Numbers · Special Characters

Click **Apply** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Schedule Configuration

The switch provides four schedules. When a schedule is applied to a feature or setting, the feature is enabled when the schedule is active and disabled when the schedule is inactive.

Each schedule can have one absolute schedule and multiple periodic schedules. Schedules can be applied to these features:

- PoE—Set the time ranges when PoE power is provided.
- Port Admin status—Set the time ranges when the port is operationally enabled.
- LED Green Mode—Set the time ranges when front-panel LEDs are disabled (OFF).
- ACLs—Set the time ranges when the ACL is active.

Click **Management > Schedule Configuration** to view or configure the schedules.

Figure 33. Schedules Tile



Table 26. Schedules Fields

Field	Description
Schedule	Select Schedule-1, Schedule-2, Schedule-3, or Schedule-4 to add, edit, or remove time periods for the schedule or to display information about time periods configured for the schedule, if any.

Field	Description
Type	The type of time period entry, which is one of the following: · Absolute—A single time period that occurs once or has an undefined start or end period. The duration of an absolute entry can be hours, days, or even years. Each time entry configuration can have only one entry. · Periodic—A recurring entry that takes place at fixed intervals. This type of entry occurs at the same time on one or more days of the week.
Starts	For an absolute entry, this field indicates the time, day, month, and year that the entry begins. If this field is blank, the absolute entry became active when it was configured. For a periodic entry, this field indicates the time and day(s) of the week that the entry begins.
Ends	For an absolute entry, indicates the time, day, month, and year that the entry ends. If this field is blank, the absolute entry does not have a defined end. For a periodic entry, this field indicates the time and day(s) of the week that the entry ends.

NOTE

To configure a new time entry for a schedule, click the ＋ (**Add**) button

Schedules require setting the system clock manually or via NTP. Using NTP provides better accuracy and synchronizes the time setting across reboots.

To view or configure a schedule, go to the **Schedule Name** drop-down and select the schedule.

Adding a Schedule

To add a schedule, from the Schedules tile, click the ＋ (**Add**) button and configure the settings.

Figure 34. Add Schedule Dialog Box - Absolute Schedule

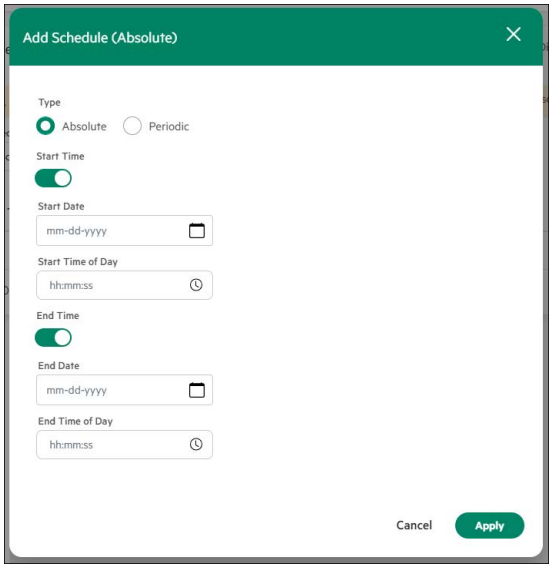


Figure 35. Add Schedule Dialog Box - Periodic Schedule

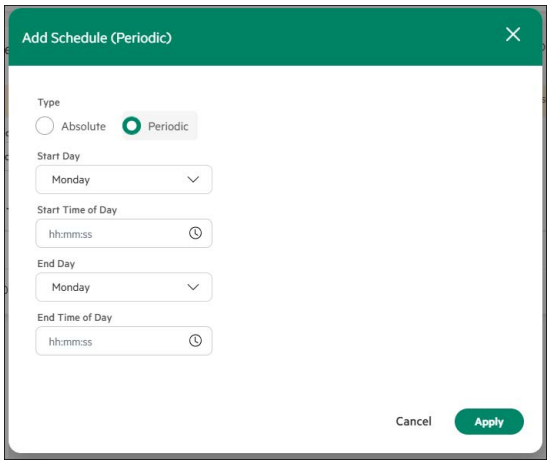


Table 27. New Schedule Configuration Fields

Field	Description
Type	The type of schedule. Can be one of the following: · Absolute. There can be only one absolute schedule in each schedule. The absolute schedule does not repeat. · Periodic. Each schedule can have multiple periodic schedules. A periodic schedule occurs at the same time every day or on one or more days of the week.
Absolute Schedule Fields	
Start Time	Enable the Start Time setting to apply the schedule Start Date. If the Start Time is disabled, the schedule Start Date will be active at the time of configuration.
Start Date	Select the start date from the calendar.
Start Time of Day	Set the time of day to start the schedule.
End Time	Activate this field to enable setting the End point of the schedule. If End Time is not activated, the schedule continues indefinitely.
End Date	Select the end date from the calendar.
End Time of Day	Set the time of day to end the schedule.
Periodic Schedule Fields	
Start Day	Select the day of the week to start the schedule, from the drop-down list.
Start Time of Day	Set the time of day to start the schedule.
End Day	Select the day of the week to end the schedule, from the drop-down list.
End Time of Day	Set the time of day to end the schedule.

Removing a Schedule

To remove a schedule, you must remove all ACL and port-related schedule configurations (port state, or PoE). Once the schedule is not in use by any ACL, port state or PoE configuration, select it in the Schedules tile, and click the (**Remove)** button.

HTTPS Certificate

Secure HTTP (HTTPS) enables the transmission of HTTP over Transport Layer Security (TLS) connection. Using HTTPS ensures that the web based management session is protected from unwanted eavesdropping.

Information encryption and decryption are performed by a pair of public and private keys.

- Data encrypted with the public key can only be decrypted with the private key.
- The public key is shared between server and clients, while the private key is never given out.

The certificate used for HTTPS sessions is also used to prove the identity of the server (the switch) to clients (management stations). Certificates are issued and signed by well known Certificate Authorities (CAs) trusted by the management station. A signed certificate stores data about the site (IP address/URL, Company name, Country, etc.). The browser inspects the signature and only if the signature is correctly verified the certificate is trusted, otherwise it notifies the user that the certificate is unsigned by a well-known authority.

The switch supports generation of a single certificate and exporting to CA for signing and allows the import of the signed certificate for use by the switch for HTTPS sessions.

To enable users to benefit from a secured connectivity, without the need to have a certificate signed by a CA, the switch also supports the use of unsigned certificates (also known as self-signed certificates). Although self-signed certificates do not prove the switch identity to the browser, they do enable securing the management session using the public and private key.

The certificate and key pairs are stored as part of the switch configuration file. If the switch startup file does not include a certificate then a self-signed certificate will be generated automatically as part of the switch boot sequence.

To access the HTTPS Configuration page, click **Management > HTTPS Certificate** in the navigation menu.

HTTPS Certificate Settings

The HTTPS Certificate Settings tile displays the current certificate details and provides several buttons at the bottom of the page to perform actions relating to HTTPS certification.



The fields that display on the page depend on whether a certificate is present. If a certificate has been generated, the page also displays the fields configured in the Generate Certificate Dialog Box (see Figure 37).

The following figure shows the HTTPS Certificate Settings Tile with no certificates.

Figure 36. HTTPS Certificate Settings Tile



Table 28. HTTPS Certificate Settings Fields

Field	Description
Common Name	Specifies the fully qualified switch URL or IP address.
Valid Dates	The start and end dates for the certificate.

Click **Apply** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Use the buttons at the bottom of the page to perform actions relating to HTTPS certification.

Generate a Self-Signed Certificate

Generating a new certificate overrides any previous certificate used. You can delete a self-signed certificate that you created. In this case, the switch will auto generate a self-signed certificate.

To generate a self-signed certificate, click the **Generate Certificate** button to view the dialog box.

Figure 37. Generate Certificate Dialog Box

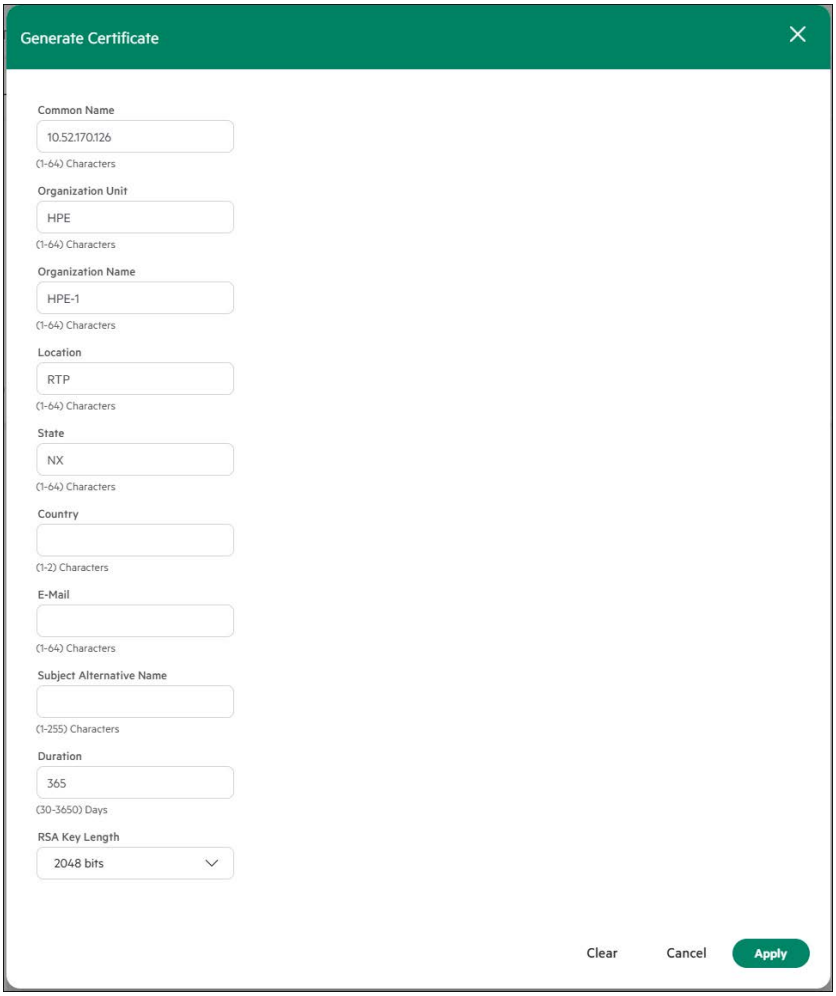


Table 29. Generate Certificate Fields

Field	Description
Common Name	Enter the fully qualified switch URL or IP address. If unspecified, defaults to the lowest IP address of the switch at time of generation.
Organization Unit	Enter the organization unit or department name. If unspecified, field is left empty.
Organization Name	Enter the organization name. If unspecified, field is left empty.
Location	Enter the location or city name. If unspecified, field is left empty.
State	Enter the state or province name. If unspecified, field is left empty.
Country	Enter the country name abbreviation. If unspecified, field is left empty.
E-Mail	Enter the email address. If unspecified, the field is left empty.
Subject Alternative Name	Enter the subject alternative name in the format of DNS:<hostname> or IP:<x.x.x.x>. If unspecified, the field is left empty.
Duration	Enter the number of days that the certificate is valid. If unspecified, the duration is set to 365 days (1 year).
RSA Key Length	Select the preferred key length. By default, key length is 2048.

Using a Certificate Signed by a Certificate Authority

To use a certificate that is signed by a Certificate Authority (CA), you need to complete the fol-lowing steps:

1. Generate a certificate request: Click **Generate Certificate Request** and enter the fields as defined in Generate a Self-Signed Certificate.



NOTE

The Duration and RSA Key Regeneration fields do not appear in the certificate request because they are not required. If new keys are needed, generate a self-signed certificate before generating a certificate request.

2. Export the certificate for signing: Under the **Certificate Request** box that appears, click **Copy To Clipboard** to copy the generated certificate request to a file, and send the file to the CA for signing.
3. After the Certificate is signed by a CA, import it back to the device. The certificate needs to be imported as a PEM encoding/file type. Import the signed certificate: Click **Import Certificate** and copy the certificate, and optionally RSA keys and the Public Key that you received from the CA to the dialog box fields.

   If keys are imported together with the certificate, the public key found in the certificate must match the imported key.

   If keys are not imported with the certificates, the public key found in the certificate must match the public key stored on the switch.
4. After copying the keys, click **Apply**.

   Importing a CA signed certificate overrides the certificate currently used on the switch.

Figure 38. Import Certificate Dialog Box

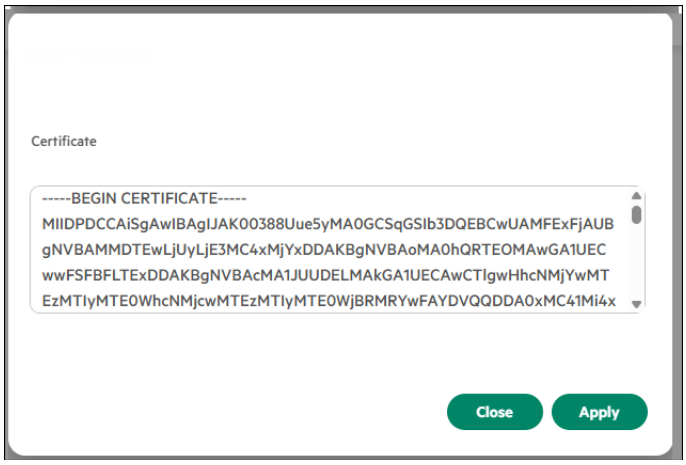


Table 30. Import Certificate Fields

Field	Description
Certificate	Paste the signed certificate into this text box.

View a Certificate

To view the current certificate details, click the **View Certificate Details** button.

Figure 39. Certificate Details

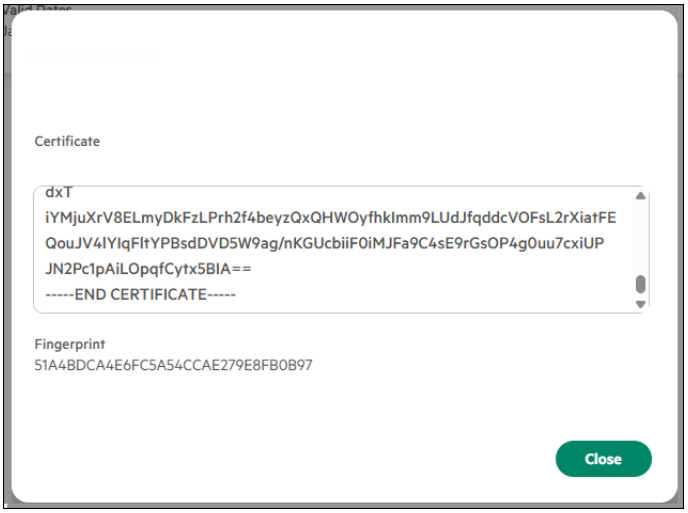


Table 31. Certificate Details Fields

Field	Description
Certificate	Non-editable text box with the certificate.
Fingerprint	The public key fingerprint.

Delete a Certificate

To delete the current certificate, click the **Delete Certificate** button.

SSH Key Management

The SSH Key Management page helps to view and modify the Secure Shell (SSH) keys on the device. SSH is a network protocol that enables access to the CLI management interface by using an SSH client on a remote administrative system. SSH is a more secure access method than Telnet because it encrypts communication between the administrative system and the device. This page also allows you to generate and delete SSH host keys for secure CLI-based management.

The SSH Keys Status tile shows the status of SSH keys.

Whenever SSH mode is enabled, a default auto key is generated if the key does not already exist in the system.

Figure 40. SSH Keys Status Tile



Table 32. SSH Key Status Fields

Field	Description
RSA Key Status	The status of the SSH-1 Rivest-Shamir-Adleman (RSA) key file or SSH-2 RSA key file (PEM Encoded) on the device, which might be Present, Absent, or Generation in Progress.
RSA Key Length	The length of the SSH-1 Rivest-Shamir-Adleman (RSA) key used to generate the PEM Encoded key file on the device, if present.
ECDSA Key Status	The status of the SSH-2 Elliptic Curve Digital Signature Algorithm (ECDSA) key file (PEM Encoded) on the device, which might be Present, Absent, or Generation in Progress.
ECDSA Key Length	The length of the SSH-2 Elliptic Curve Digital Signature Algorithm (ECDSA) key used to generate the PEM Encoded key file on the device, if present.
DHParam Key Length	The length of the Diffie-Hellman Parameter (DHParam) Key determines the strength of the key exchange used to establish a secure communication channel. The default length for the DHParam Key length is 1024.

To Generate the SSH Keys:

1. Click the **Generate Keys** button.
2. Select the type of the SSH keys.
3. Choose the length of the keys, and click **Generate** to generate the keys.

To Delete the SSH Keys:

1. Click on the **Delete Keys** button.
2. Select the type of the SSH keys to delete.
3. Click the **Delete** button to delete the keys.



Applied changes update the device running configuration. If you want the device to retain these changes across a reset, you must first save the configuration.

SNMP

Simple Network Management Protocol (SNMP) provides a method for managing network devices. The device supports SNMP version 1, SNMP version 2, and SNMP version 3.

SNMP v1 and v2

The SNMP agent maintains a list of variables, which are used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB presents the variables controlled by the agent. The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agent are controlled by access strings (also called community strings).

SNMP v3

SNMP v3 also applies access control and a new trap mechanism to SNMPv1 and SNMPv2 PDUs. In addition, the User Security Model (USM) is defined for SNMPv3 and includes:

- **Authentication:** Provides data integrity and data origin authentication.
- **Privacy:** Protects against disclosure of message content. Cipher-Block-Chaining (CBC) is used for encryption. Either authentication is enabled on an SNMP message, or both authentication and privacy are enabled on an SNMP message. However privacy cannot be enabled without authentication.
- **Timeliness:** Protects against message delay or message redundancy. The SNMP agent compares an incoming message to the message time information.
- **Key Management:** Defines key generation, key updates, and key use.

The switch supports SNMP notification filters based on Object IDs (OID). OIDs are used by the system to manage switch features. SNMP v3 supports the following features:

- Security
- Feature Access Control
- Traps

Authentication or Privacy Keys are modified in the SNMPv3 User Security Model (USM).

Global Configuration

Use the Global Configuration tile to globally enable SNMP and optionally configure the source interface.

Figure 41. SNMP v3 Global Configuration Tile



Table 33. SNMP v3 Global Configuration Fields

Field	Description
Admin Mode	Controls the administrative status of SNMP: · —Disabled · —Enabled
Source Interface	Configures the physical or logical interface to use as the SNMP client source interface. When an IP address is configured on the source interface, this address is used for all SNMP communications between the local SNMP client and the remote SNMP server. The IP address of the designated source interface is used in the IP header of SNMP management protocol packets. This allows security devices, such as firewalls, to identify all source packets coming from a specific device. · Unconfigured—The primary IP address of the originating (outbound) interface is used as the source address. · Network Port—The Network port source IP is used as the source address. · Interface—Based on the selected physical port to use as the source interface, the primary IP address of that physical port is used as the source address. · VLAN ID—Based on the selected VLAN to use as the source interface, the primary IP address of that VLAN routing interface is used as the source address.
Source Interface Status	Indicates the current link status of the selected source interface. The possible values are: · Link up. · Link down.
Source IPv4 Address	Displays the primary IPv4 address associated with the selected source interface.

Community Configuration

Access rights are managed by defining communities on the SNMP Community Configuration page. When the community names are changed, access rights are also changed. SNMP Communities are defined only for SNMP v1 and SNMP v2.

Use the SNMP Community Configuration tile to enable SNMP and Authentication notifications.

Figure 42. SNMP Community Configuration Tile



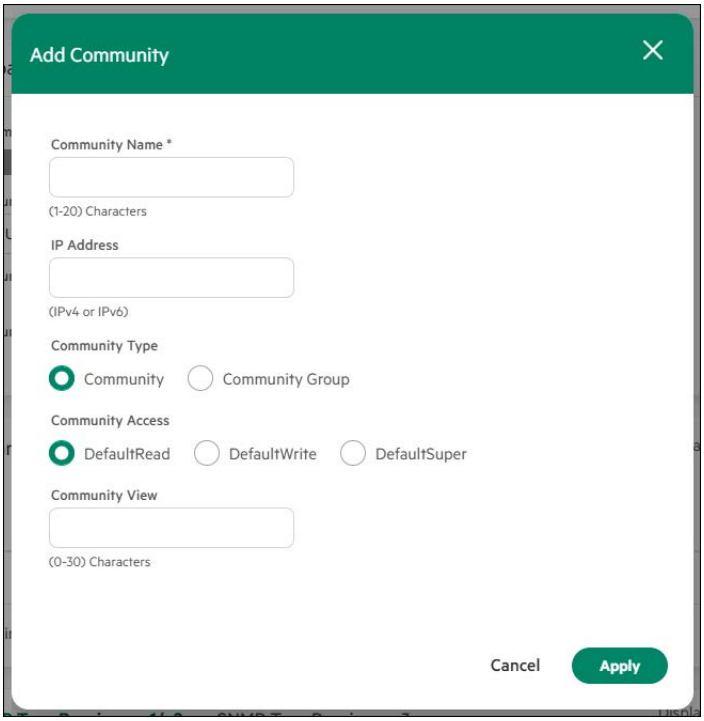
Table 34. SNMP Community Configuration Fields

Field	Description
Community Name	Community name used in SNMPv1/v2 packets. This is configured in the client and identifies the access the user may connect with.
IP Address	Specifies the IP address that can connect with this community. The address can be an IPv4 address or IPv6 address with prefix.
Community Type	The type of community, which is either Community or Community Group. When Community is selected as the type, both community access and a view name must be specified. When Community Group is selected, a group name can be chosen instead.
Community Access	Specifies the access control policy for the community. The default access privileges are as follows: · DefaultRead: Access to the entire MIB tree except to SNMP configuration objects. · DefaultWrite: Access to the entire MIB tree except to SNMP configuration objects. · DefaultSuper: Access to the entire MIB tree. For more information about controlling access to objects, see Table 41, SNMP View Configuration Fields.
Community View	Specifies the community view for the community. If the value is empty, then no access is granted. A view is used to restrict or grant access to specific MIB trees. For example, it is possible to define a view to grant access to the mib-2 tree but deny access to the RMON MIB subtree, or a view could allow access to only the RADIUS Accounting and Authentication MIBs. In this way, it is possible to define a community that has access rights of a (restricted) view.
Group Name	Identifies the Group associated with this Community entry. This is available only for Community Groups.

Adding an SNMP Community or Community Group

To add a new SNMP community or community group, click the + (**Add**) button on the SNMP Community Configuration tile. The **Add Community** dialog box appears.

Figure 43. Add SNMP Community Dialog Box



Configure the relevant fields and click **Apply**.

Removing an SNMP Community or Community Group

To remove an SNMP community or community group, select each item to delete and click the (**Remove)** button on the SNMP Community Configuration tile.

SNMP v1/v2 Trap Receivers

Use the SNMP v1/v2 Trap Receivers tile to configure settings for each SNMPv1 or SNMPv2 management host that will receive notifications about traps generated by the device. The SNMP management host is also known as the SNMP trap receiver.

Figure 44. SNMP v1/v2 Trap Receivers Tile

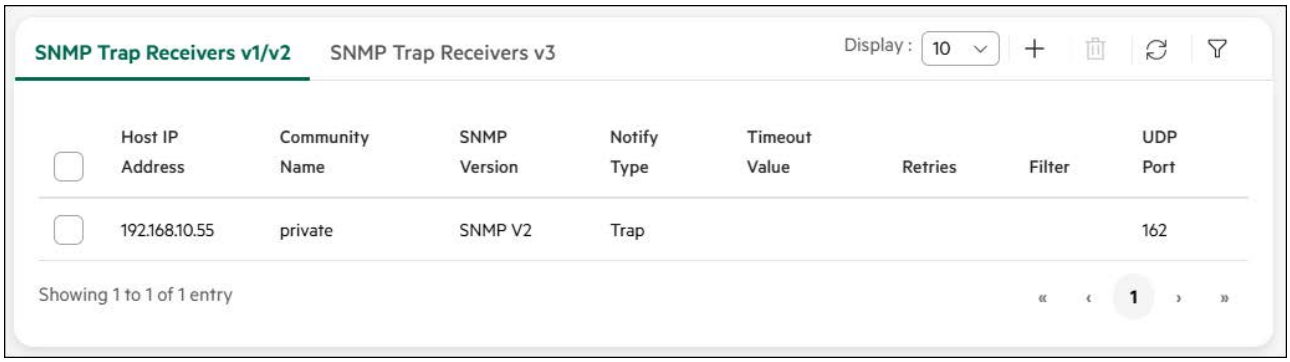


Table 35. SNMP v1/v2 Trap Receivers Fields

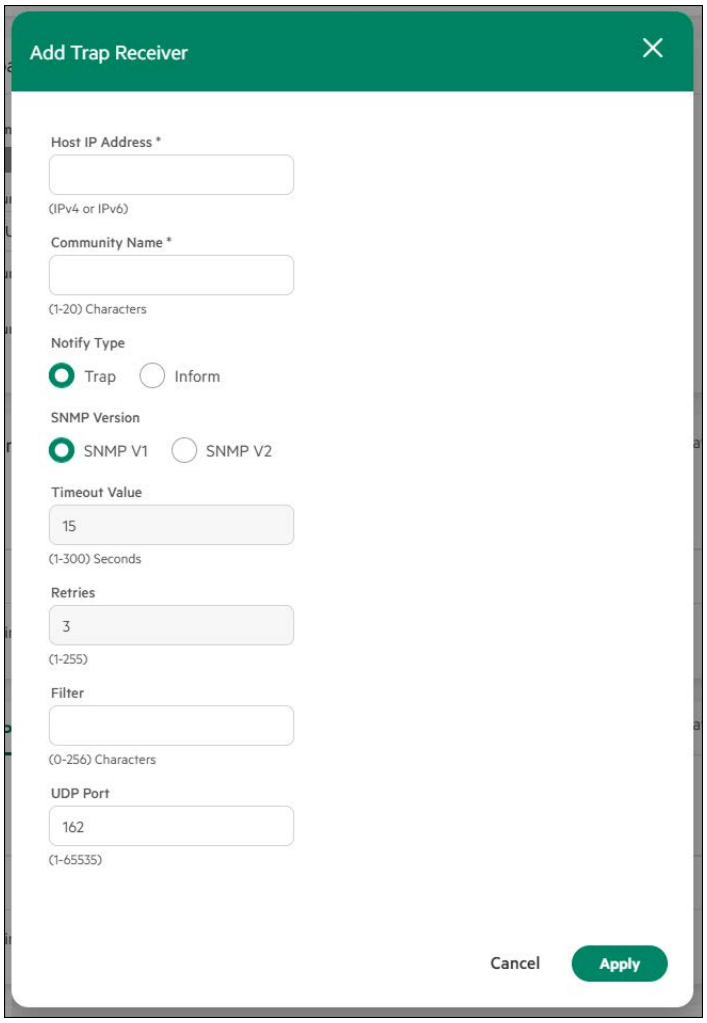
Field	Description
Host IP Address	The IP address of the SNMP management host that will receive traps generated by the device.
Community Name	The name of the SNMP community that includes the SNMP management host and the SNMP agent on the device.
Notify Type	The type of SNMP notification to send the SNMP management host: · Inform—An SNMP message that notifies the host when a certain event has occurred on the device. The message is acknowledged by the SNMP management host. This type of notification is not available for SNMPv1. · Trap—An SNMP message that notifies the host when a certain event has occurred on the device. The message is not acknowledged by the SNMP management host.
SNMP Version	The version of SNMP to use, which is either SNMPv1 or SNMPv2.
Timeout Value	The number of seconds to wait for an acknowledgment from the SNMP management host before resending an inform message.
Retries	The number of times to resend an inform message that is not acknowledged by the SNMP management host.
Filter	The name of the filter for the SNMP management host. The filter defines which MIB objects to include or exclude from the view. This field is optional.
UDP Port	The UDP port on the SNMP management host that will receive the SNMP notifications. If no value is specified when configuring a receiver, the default UDP port value is used.

Click **Apply** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Adding an SNMP v1/v2 Trap Receiver

To add an SNMP v1/v2 trap receiver, click the + (**Add**) button on the SNMP Trap Receivers tile. The **Add Trap Receiver** dialog box appears.

Figure 45. Add SNMP v1/v2 Trap Receiver Dialog Box



Configure the required fields and click **Apply**. The Retries and Timeout Value fields are available only if the selected Notify Type is Inform.

Removing an SNMP v1/v2 Trap Receiver

To remove an SNMP v1/v2 trap receiver, select each item to delete and click the (**Remove)** button on the SNMP Trap Receivers tile.

SNMP v3 Trap Receivers

Use the SNMP v3 Trap Receivers page to configure settings for each SNMPv3 management host that will receive notifications about traps generated by the device. The SNMP management host is also known as the SNMP trap receiver. You can configure up to 8 SNMP trap receivers in this tab.

To access the Trap Receiver v3 Configuration page, click **Switching > SNMP in the** navigation pane, and then click the **Trap Receiver V3** tab.

Figure 46. SNMP v3 Trap Receivers Tile



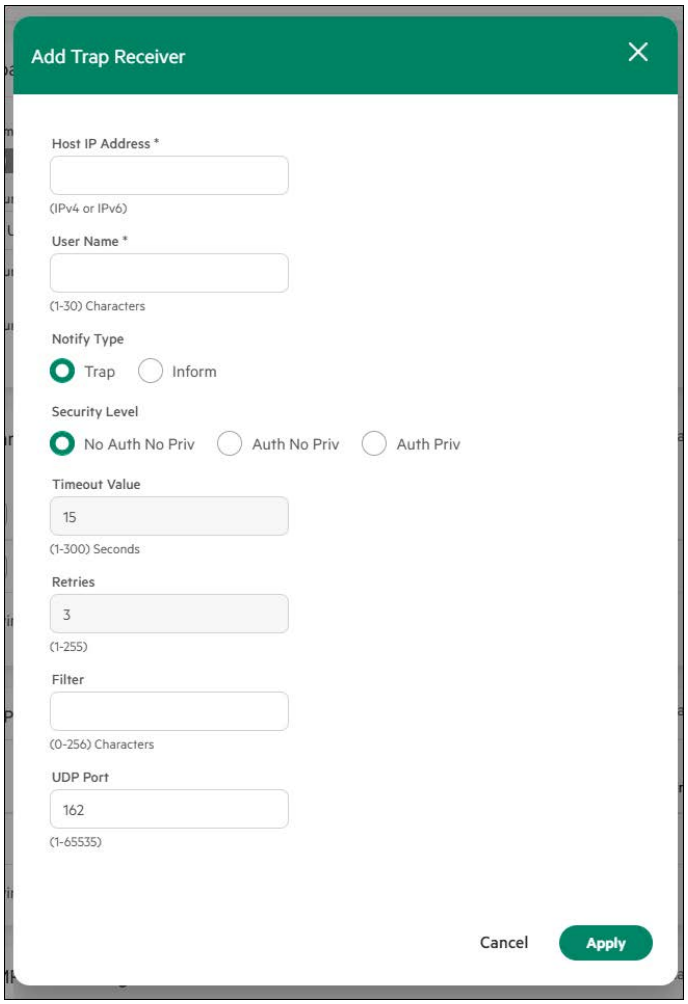
Table 36. SNMP v3 Trap Receivers Fields

Field	Description
Host IP Address	The IP address of the SNMP management host that will receive traps generated by the switch.
Username	The name of the SNMP user that is authorized to receive the SNMP notification.
Notify Type	The type of SNMP notification to send the SNMP management host: · Inform—An SNMP message that notifies the host when a certain event has occurred on the device. The message is acknowledged by the SNMP management host. · Trap—An SNMP message that notifies the host when a certain event has occurred on the device. The message is not acknowledged by the SNMP management host.
Security Level	This field is available on the Add Trap Receiver page. The security level associated with the SNMP user, which is one of the following: · No Auth No Priv—No authentication and no data encryption (no security). · Auth No Priv—Authentication, but no data encryption. With this security level, users send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption. · Auth Priv—Authentication and data encryption. With this security level, users send an MD5 key/password for authentication and a DES key/password for encryption.
Timeout Value	The number of seconds to wait for an acknowledgment from the SNMP management host before resending an inform message.
Retries	The number of times to resend an inform message that is not acknowledged by the SNMP management host.
Filter	The name of the filter for the SNMP management host. The filter defines which MIB objects to include or exclude from the view. This field is optional.
UDP Port	The UDP port on the SNMP management host that will receive the SNMP notifications. If no value is specified when configuring a receiver, the default UDP port value is used.

Adding an SNMP v3 Trap Receiver

To add an SNMP v3 trap receiver, click the + (**Add**) button on the SNMP Trap Receivers tile. The **Add Trap Receiver** dialog box appears.

Figure 47. Add SNMP v3 Trap Receiver Dialog Box



Configure the required fields and click **Apply**.

Removing an SNMPv3 Trap Receiver

To remove an SNMP v3 trap receiver, select each item to delete and click the (**Remove)** button on the SNMP Trap Receivers tile.

SNMP Filter Configuration

The SNMP Filter Configuration tile enables you to configure SNMP notification filters. An SNMP filter defines Object IDs (OIDs) that are included or excluded from the filter.

After defining a notification filter, it can be attached to an SNMP receiver using the SNMP Trap Receivers tile (V1/2 or V3 receiver).

Figure 48. SNMP Filter Configuration Tile

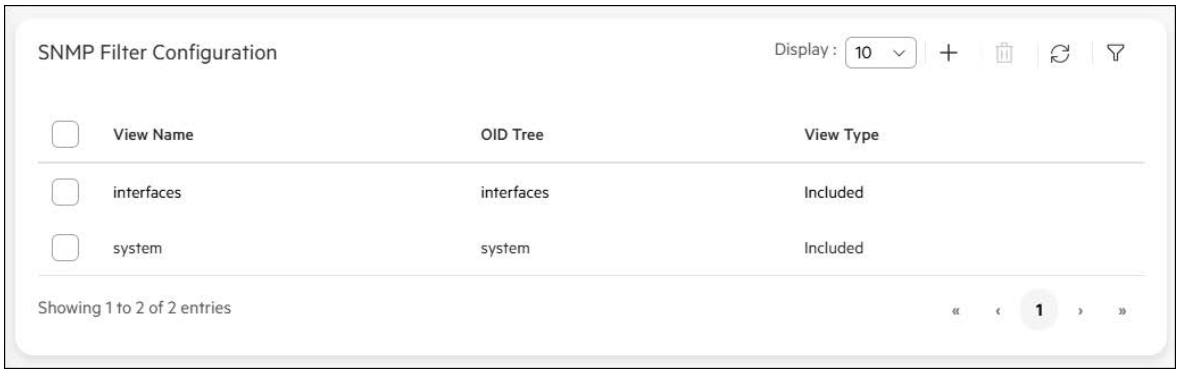


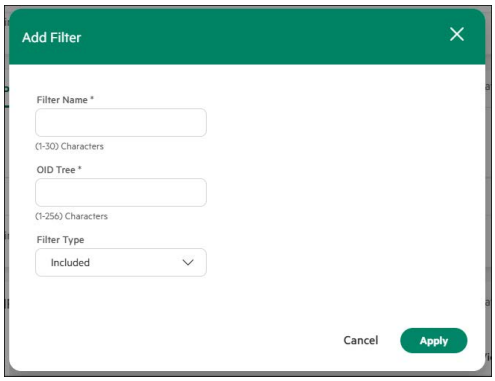
Table 37. SNMP Filter Configuration Fields

Field	Description
Filter Name	The name of the filter configuration name.
OID	The node in the MIB tree that is included or excluded in this SNMP filter.
Filter Type	The type of SNMP filter: · Excluded—Notifications are not sent for this OID · Included—Notifications are sent for this OID.

Adding an SNMP Filter

To add a new SNMP filter, click the + (**Add**) button in the SNMP Filter Configuration tile. The **Add Filter** dialog box appears.

Figure 49. Add Filter Dialog Box



Configure the relevant fields and click **Apply**.

Removing an SNMP Filter

To remove an SNMP filter, select each item to delete and click the (**Remove)** button in the SNMP Filter Configuration tile.

SNMP Access Control Group Configuration

Use this tile to configure SNMP access control groups. These SNMP groups allow network managers to assign different levels of authorization and access rights to specific device features and their attributes.

The SNMP group can be referenced by the SNMP community to provide security and context for agents receiving requests and initiating traps as well as for management systems and their tasks. An SNMP agent will not respond to a request from a management system outside of its configured group, but an agent can be a member of multiple groups at the same time to allow communication with SNMP managers from different groups. Several default SNMP groups are preconfigured on the system.

Figure 50. SNMP Access Control Group Configuration Tile

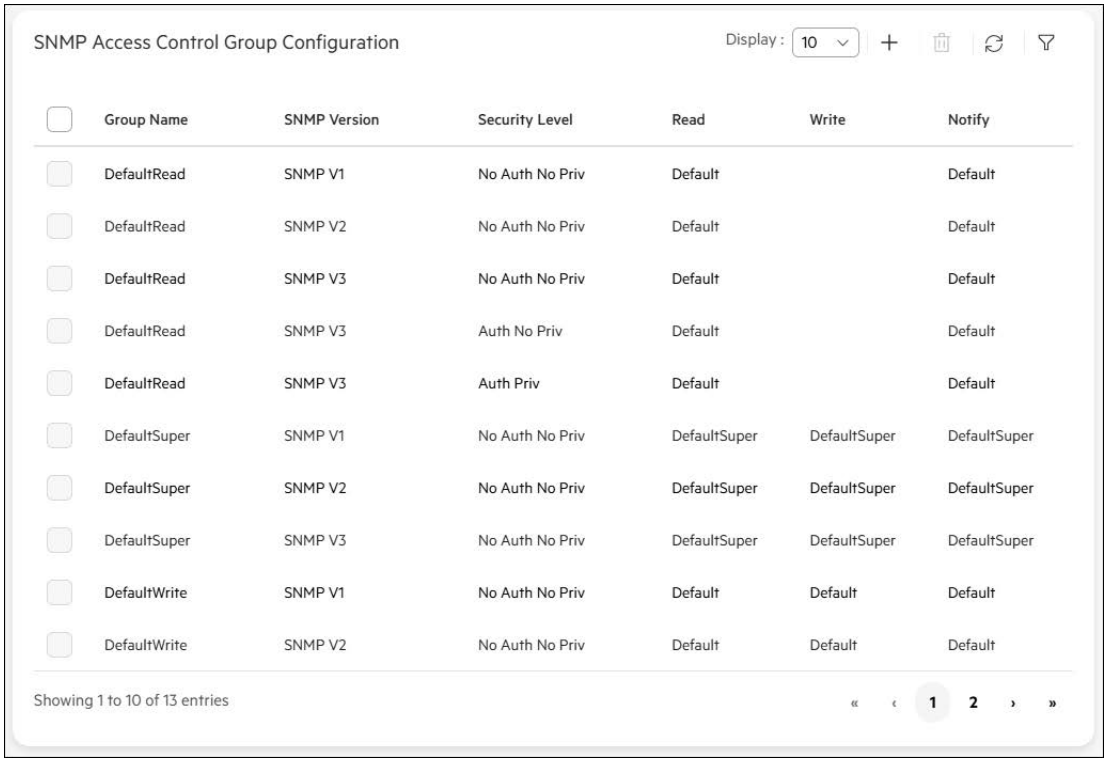


Table 38. SNMP Access Control Group Configuration Fields

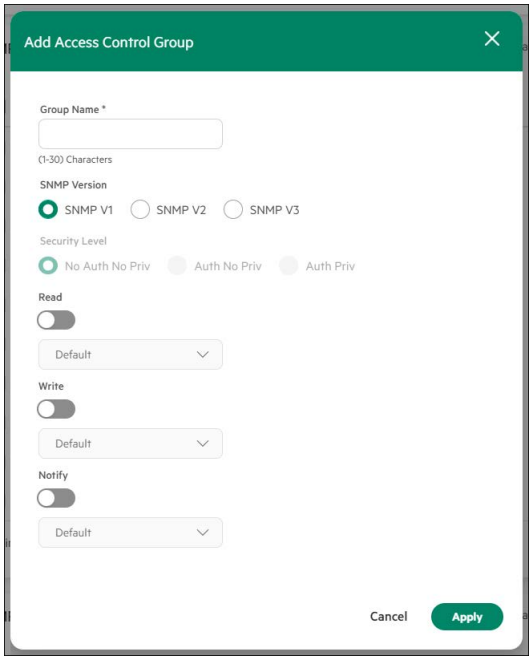
Field	Description
Group Name	The name that identifies the SNMP group.
SNMP Version	The SNMP version associated with the group.

Field	Description
Security Level	The security level associated with the group, which is one of the following: · No Auth No Priv—No authentication and no data encryption (no security). This is the only Security Level available for SNMPv1 and SNMPv2 groups. · Auth No Priv—Authentication, but no data encryption. With this security level, users send SNMP messages that use an MD5 or SHA key/password for authentication, but not a DES key/password for encryption. · Auth Priv—Authentication and data encryption. With this security level, users send an MD5 or SHA key/password for authentication and a DES key/password for encryption.
Read	The level of read access rights for the group. The menu includes the available SNMP views. When adding a group, select the check box to allow the field to be configured, then select the desired view that restricts management access to viewing the contents of the agent.
Write	The level of write access rights for the group. The menu includes the available SNMP views. When adding a group, select the check box to allow the field to be configured, then select the desired view that permits management read-write access to the contents of the agent but not to the community.
Notify	The level of notify access rights for the group. The menu includes the available SNMP views. When adding a group, select the check box to allow the field to be configured, then select the desired view that permits sending SNMP traps or informs.

Adding an SNMP Access Control Group

To add an SNMP access control group click the + (**Add**) button in the SNMP Access Control Group tile. The **Add Access Control Group** dialog box appears.

Figure 51. Add Access Control Dialog Box



Configure the required fields and click **Apply**

Removing an SNMP Access Control Group

To remove an SNMP access control group, select each item to delete and click the (**Remove)** button in the SNMP access control group tile.

SNMP User Configuration

The SNMP User Configuration tile provides the capability to configure the SNMP v3 user accounts.

To access the User Configuration tile, click **Switching > SNMP** and scroll down to the SNMP User Configuration tile.

Figure 52. SNMP User Configuration Tile



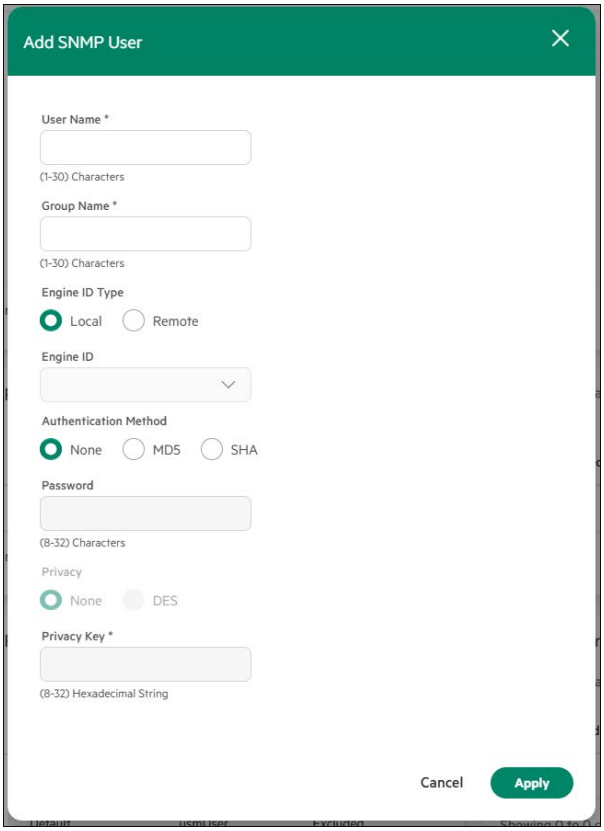
Table 39. SNMP User Configuration Fields

Field	Description
User Name	Specifies the name of the SNMP user being added for the User-based Security Model (USM). Each user name must be unique within the SNMP agent user list. A user name cannot contain any leading or embedded blanks
Group Name	An SNMP group is a group to which hosts running the SNMP service belong. A group name parameter is simply the name of that group by which SNMP communities are identified. The use of a group name provides some security and context for agents receiving requests and initiating traps and does the same for management systems and their tasks. An SNMP agent won't respond to a request from a management system outside its configured group, but an agent can be a member of multiple groups at the same time. This allows for communications with SNMP managers from different groups.
Engine ID	Each SNMPv3 agent has an engine ID that uniquely identifies the agent in the device. If given this entry will be used only for packets whose engine id is this. This field takes a hexadecimal string in the form 0102030405.
Authentication Method	The authentication protocol to be used on authenticated messages on behalf of the user. · None—No authentication will be used for this user. · MD5—MD5 protocol will be used. This option requires a password of 8 to 32 ASCII or hexadecimal characters. · SHA—SHA protocol will be used. This option requires a password of 8 to 32 ASCII or hexadecimal characters.
Privacy	Specifies the privacy protocol to be used on encrypted messages on behalf of the specified user. This parameter is only valid if the value in the Authentication Method field is not None. · None—No privacy protocol will be used. · DES—DES protocol will be used. This option requires an authentication key of 8-32 hexadecimal characters.

Adding an SNMP v3 User

To add an SNMP user, click the + (**Add**) button in the SNMP User Configuration tile. The **Add SNMP User** dialog box appears.

Figure 53. Add SNMP User Dialog Box



In addition to the fields listed in Table 39, the fields in the following table are available in the Add SNMP User dialog box.

Table 40. Add SNMP User Fields

Field	Description
Engine ID Type	Specify whether the engine ID for the SNMP v3 agent is local or remote. If the agent is local, the engine ID is automatically generated. If the agent is remote, you must specify the engine ID.
Password	If the Authentication Method is MD5 or SHA, use this field to specify the password used to generate the key to be used in authenticating messages on behalf of this user. If the Authentication Method is MD5-Key or SHA-Key, use this field to specify the pregenerated MD5 or SHA authentication key.
Privacy Key	This field is available on the Add New SNMP User dialog box. Specifies the password used to generate the key to be used in encrypting messages to and from this user. This parameter must be specified if the value in the Privacy field is not None.

Configure the required fields and click **Apply**

Removing an SNMP v3 User

To remove one or more SNMP v3 users, select each user to delete and click the 🗑 (**Remove)** button in the SNMP User Configuration tile.

SNMP View Configuration

Use the SNMP View Configuration tile to configure SNMP views. These SNMP views allow network managers to control access to different parts of the MIB hierarchy permitting or denying access to objects. Once configured, views are associated to access control groups to complete access privileges.

To access the SNMP View Configuration tile, click **Switching > SNMP** and scroll down to the SNMP View Configuration tile.

Figure 54. SNMP View Configuration Tile

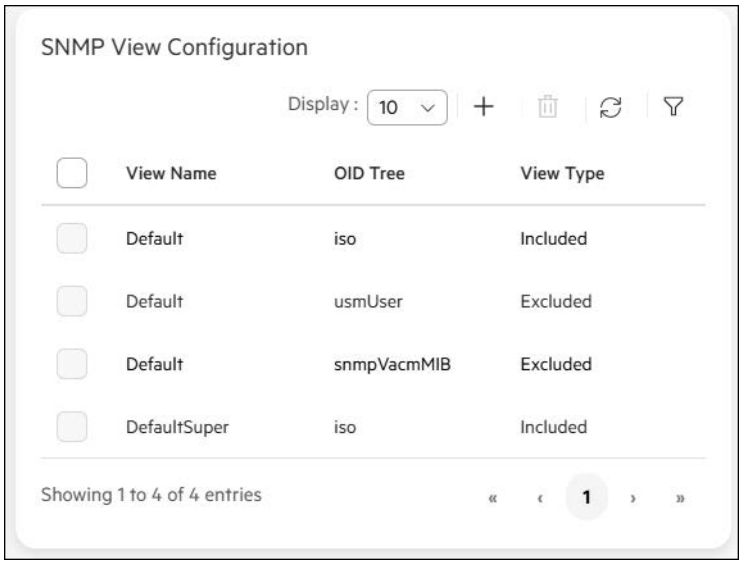


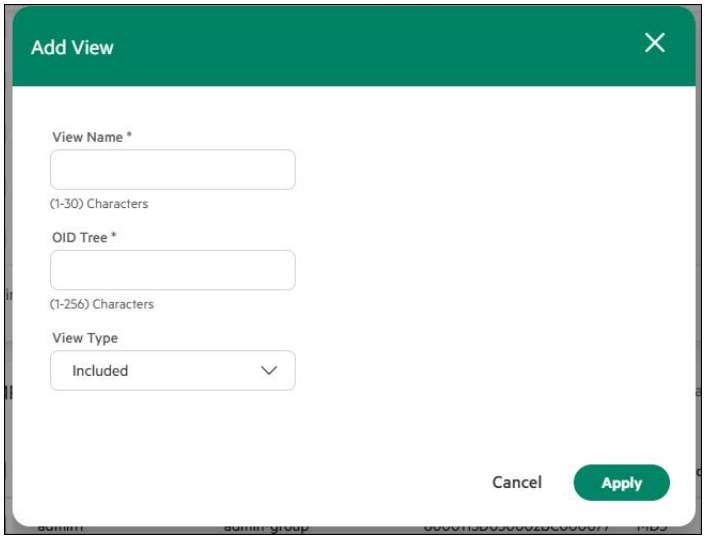
Table 41. SNMP View Configuration Fields

Field	Description
View Name	The name that identifies the SNMP view.
OID Tree	The ASN.1 subtree to be included or excluded from the view.
View Type	Type of access granted to the specified ASN.1 subtree: · Included—Access is granted to this subtree. · Excluded—Access is denied to this subtree.

Adding an SNMP View

To add an SNMP view, click the + (**Add**) button in the SNMP View Configuration tile. The **Add View** dialog box appears.

Figure 55. Add View Dialog Box



Configure the required fields and click **Apply**

Removing an SNMP View

To remove one or more SNMP views, select each view to delete and click the (**Remove)** button in the SNMP View Configuration tile. Only user-configured views can be removed.

Remote Engine ID Configuration

To use SNMPv3, an engine ID must be specified for the SNMP Agent. The engine ID must be unique within an administrative domain. The switch uses a Local Engine ID. The Local Engine ID is not configurable and is auto generated based on switch MAC address.

For remote SNMP Agents, Receiving informs or traps, a unique SNMP engine ID needs to be configured. Use this dialog box to configure the remote Engine ID for specific hosts.

Figure 56. Remote Engine ID Configuration Tile

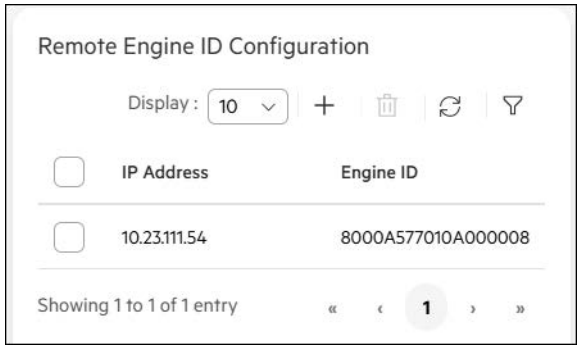


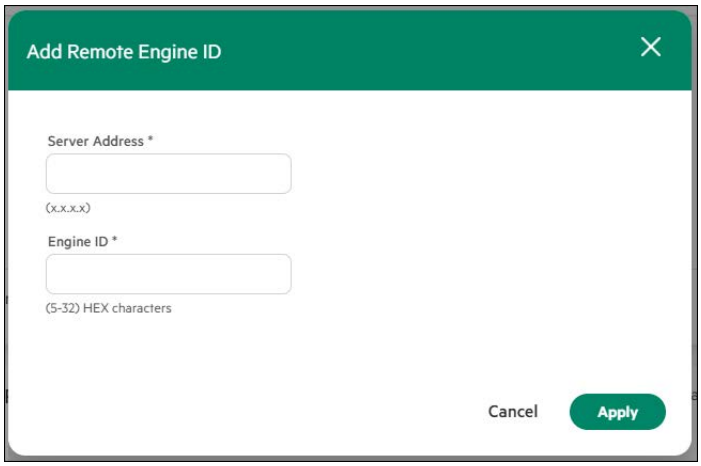
Table 42. Remote Engine ID Configuration Fields

Field	Description
IP Address	The IP Address of the remote SNMP agent
Engine ID	The engine ID of the remote agent. The engine ID is a concatenated hexadecimal string (10-64 HEX digits).

Adding a Remote Engine ID

To add an Remote Engine ID, click the + (**Add**) button in the Remote Engine ID Configuration tile. The **Add Remote Engine ID** dialog box appears.

Figure 57. Add Remote Engine ID Dialog Box



Configure the required fields and click **Apply**

Removing an Remote Engine ID

To remove one or more Remote Engine IDs, select each ID to delete and click the (**Remove)** button in the Remote Engine ID Configuration tile.

Management Access List Configuration

Use the Management Access List Configuration page to configure management access control and administration lists (MACALs). This page allows the configuration of rules, services and profiles to manage the switch management access via TCP/IP.

Profile Configuration

Use the Profile Configuration tile to configure the Management Access Control and Administration List, use the following buttons to perform the tasks: APPLY.

Figure 58. Profile Configuration Tile



Table 43. Profile Configuration Fields

Field	Description
Access Profile	Profile name for the management ACL. One user-defined access profile can be created.
Active Profile	Shows the currently active access profile used to control management access. This drop-down menu provides the following options: · None—No access profile is currently active. · Access Profile Name—This option activates the configured access profile and applies its settings for management access control.
Packets Filtered	The number of packets filtered.

Profile Rule Configuration

Use the Profile Rule Configuration tile to configure rules to associate with the MACAL. Rules can be created only if an access profile exists.

Figure 59. Profile Rule Configuration Tile



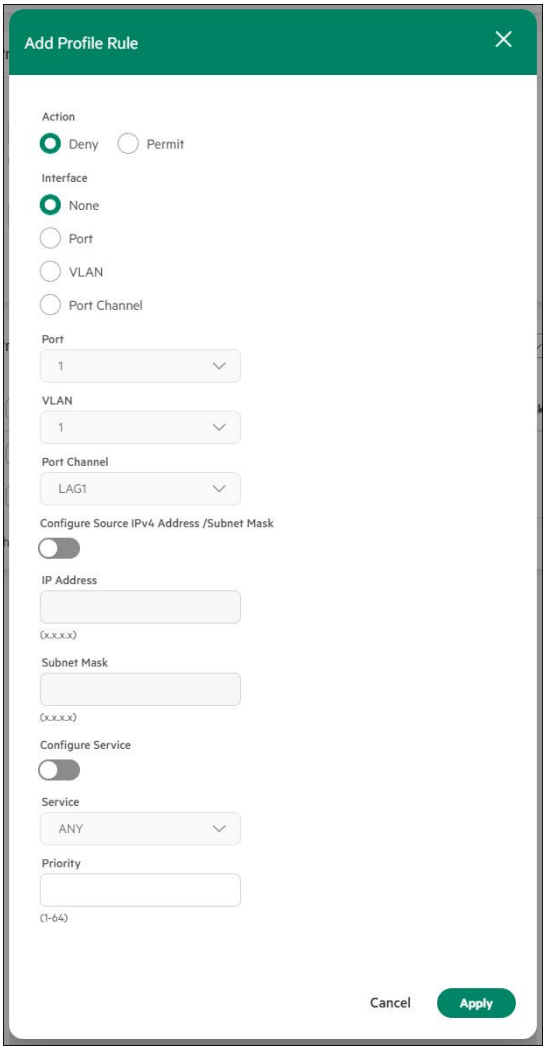
Table 44. Profile Rule Configuration Fields

Field	Description
Interface	Specifies the physical or logical interface associated with the management access configuration. The available types include: · None—No interface is currently configured. · Port—Refers to physical Ethernet ports on the device. · VLAN ID—Used to identify VLAN-tagged traffic that should be permitted to access the management interface. · Port Channel—Refers to a Link Aggregation Group (LAG), which combines multiple physical ports into a single logical interface.
Management Method	The following types of action can be taken on access control list. · Permit—To allow conditions for the management access list. · Deny—To deny conditions for the management access list.
Source IPv4 Address	IPv4 address of the device to be permitted or denied in the management access list.
Subnet Mask	Specifies the network mask of the source IPv4 address.
Service	Indicates service type. Can be one of the following. · ANY · TELNET · HTTP · HTTPS · SNMP · SSH · TFTP · NTP
Priority	The priority for the profile rule. Duplicate priorities are not allowed. If the priority is not specified during rule creation, the rule is automatically assigned the first free priority before adding it to the management access list. The rules are displayed based on their priority within the management access list.

Adding a Profile Rule

To add a profile rule, click the + (**Add**) button in the Profile Rule Configuration tile. The **Add Profile Rule** dialog box appears. Rules can be created only if an access profile exists.

Figure 60. Add Profile Rule Dialog Box



Configure the required fields and click **Apply**

Editing a Profile Rule

To edit an existing profile rule from the access profile, select the rule to edit and click the (**Edit**) button in the Profile Rule Configuration tile.

Removing a Profile Rule

To remove one or more profile rule from the access profile, select each rule to delete and click the (**Remove)** button in the Profile Rule Configuration tile.

Use the Switching pages to configure port operation and various Layer 2 features and capabilities.

Port Configuration

From the Port Configuration page, you can view port status information, configure global and individual port settings, and view statistics on packets transmitted on each port.

To view this page, click **Switching** > **Port Configuration** in the navigation pane.

Device View

The top of the Port Configuration page shows a graphical representation of the switch front panel. This panel view has a display of the ports, each with its current status.

Click a port on the device view (graphical display) to open the **Edit Port Configuration** dialog box for the port. For more information about port configuration, see Modifying Interface Settings.

For more information about the device view, see Device View.

Global Configuration

The following figure and table describe the global configuration options that you can set.

Figure 61. Port Settings Global Configuration Tile

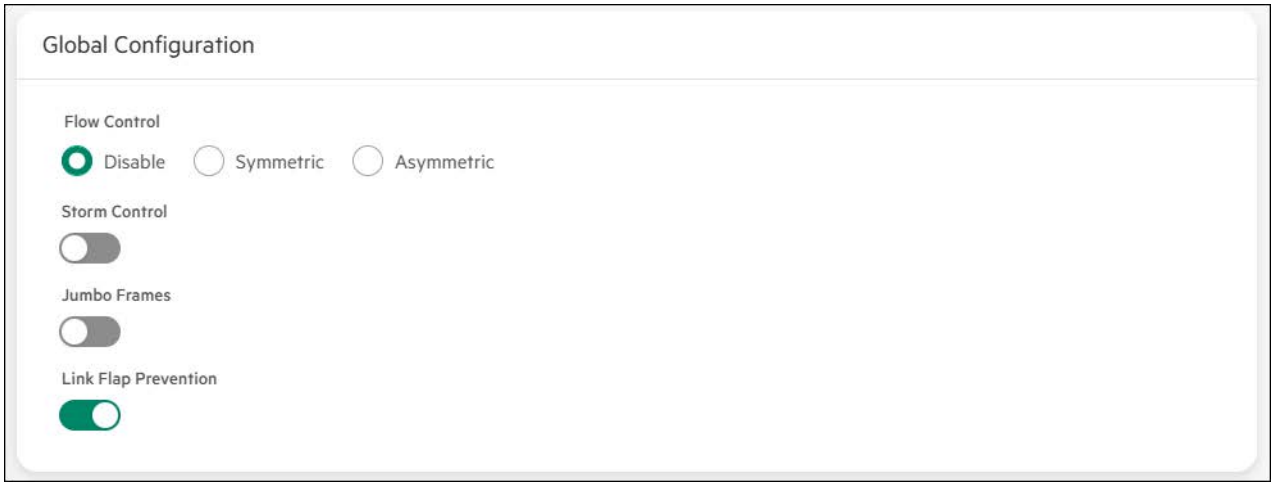


Table 45. Port Settings Global Configuration Fields

Field	Description
Flow Control	When a port becomes congested, it may begin dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss. When 802.3x flow control is enabled, a lower-speed switch can communicate with a higher-speed switch by requesting that the higher-speed switch refrain from sending packets. Transmissions are temporarily halted to prevent buffer overflows. The Flow Control Mode on the Interface. The possible values are: · Disable—To disable the flow control on the interface. · Symmetric—To configure symmetric flow control on the interface. It means a device sends and receives PAUSE frames in both directions to manage traffic flow. · Asymmetric—To configure Asymmetric flow control on the interface. The device is configured to send PAUSE frames in one direction
Storm Control	The switch supports both Global and per interface storm control settings. This is the global storm control setting. For information on per interface storm control, see Modifying Interface Settings. By default, global storm control is disabled. The Storm Control feature protects against conditions where incoming packets flood the LAN, causing network performance degradation. The software includes Storm Control protection for unicast traffic with an unknown destination, and for broadcast and multicast traffic.
Link Flap Prevention	A link-flap event is triggered if an interface changes its link state (link-up or link-down event) 5 or more times per second—for 10 seconds or longer. By default, link flap prevention mode is enabled. In such a case, the port is d-disabled. A port that is d-disabled by link flap prevention can be recovered by one of the following: · If auto-recovery is enabled for link flap prevention, after the timeout expires, the port attempts to recover. · If auto-recovery is disabled, you can attempt to manually recover the port in the Suspended Interface tile on the **Switching > Interface Auto Recovery** page.
Jumbo Frames	Sets both MTU (Maximum Transmission Unit) and MRU (Maximum Receive Unit) values · If disabled, frame size is limited to 1518 bytes · If enabled: o For bridging, the frame size is limited to 9216 bytes. o For Routing, the frame size is limited to 9000 bytes.



Flow control requires link speed to be set to auto-negotiate. If auto-negotiation is OFF or if the port speed was configured manually, then flow control is not negotiated with or advertised to the peer. Additionally, the flow control PAUSE frame configuration may be lost if the auto-negotiation is disabled on the port.



1) Interface storm control settings override the Global storm control settings. This means that if an interface has a specific setting for a certain storm type, the interface will use those settings and not the global setting.

2) The storm control threshold percentage is translated to a packets-per-second value that is used by the switch hardware to rate-limit the incoming traffic. This translation assumes a 512 byte packet size to determine the packets-per-second threshold based on the port speed. For example, the 5% threshold applied to a 1 Gbps port equates to approximately 11748 packets-per-second, regardless of the actual packet sizes received by the port.

Interface Configuration

The Interface Configuration tile displays the operational and administrative status of each port and enables port configuration.

Figure 62. Interface Configuration Tile

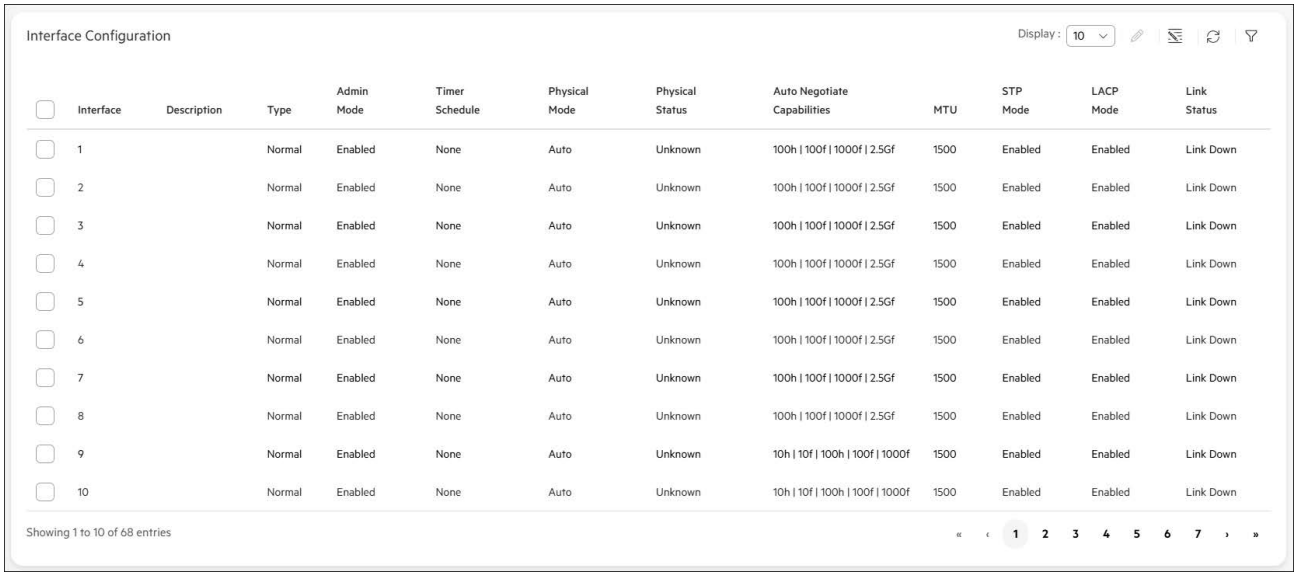


Table 46. Interface Configuration Fields

Field	Description
Interface	The port or trunk ID.
Description	The current description, if any, associated with the interface to help identify it.
Type	The interface type, which can be one of the following: · Normal—The port is a normal port, which means it is not a Link Aggregation Group (LAG) member or configured for port mirroring. All ports are normal ports by default. · Trunk Member—The port is a member of a trunk. · Mirrored—The port is configured to mirror its traffic (ingress, egress, or both) to another port (the probe port). · Probe—The port is configured to receive mirrored traffic from one or more source ports.
Admin Mode	The administrative mode of the interface. If a port or trunk is administratively disabled, it cannot forward traffic. · Enabled—Administratively enabled. · Disabled—Administratively disabled. · Diag Disabled (User cannot configure this value). · Not Applicable (User cannot configure this value).
Schedule	The schedule for activation of certain switch features. See Schedule Configuration.
Physical Mode	The port speed and duplex mode. The modes are: · Auto—The duplex mode and speed are set from the auto-negotiation process, based on the advertised capabilities. · Manual—The speed and duplex mode are those set manually by the user.
Physical Status	Indicates the port speed and duplex mode for physical interfaces. The physical status for a trunk is not reported. When a port is down, the physical status is unknown.
Auto Negotiate Capabilities	Indicates the list of configured capabilities for a port when Auto Negotiate is on. The Capability status for a trunk is not reported

Field	Description
MTU	Indicates the Maximum Transmission Unit (MTU) of the interface, which is the largest frame size that can be transmitted on the port. The size does not include the Source MAC, the Destination MAC, the Ethernet Encapsulation, or the Ethernet FC.
STP Mode	The Spanning Tree Protocol (STP) Administrative Mode associated with the port or LAG. STP is a layer 2 protocol that provides a tree topology for switches on a bridged LAN. STP allows a network to have redundant paths without the risk of network loops. by providing a single path between end stations on a network. The possible values for STP mode are: · Enable—Spanning tree is enabled for this port. · Disable—Spanning tree is disabled for this port.
LACP Mode	Indicates the Link Aggregation Control Protocol administration state. The mode must be enabled for the port to participate in Link Aggregation. This field can have the following values: · Enable—Specifies that the port is allowed to participate in a port channel (LAG), which is the default mode. · Disable—Specifies that the port cannot participate in a port channel (LAG). · N/A—For LAG ports.
Link Status	Indicates whether the Link is up or down.

Modifying Interface Settings

To change the port configuration of one or more interfaces, select the check the box to the left of one or more interfaces and click (**Edit**). To edit all the interfaces at the same time, click (**Edit All**).

Figure 63. Edit Port Configuration Dialog Box

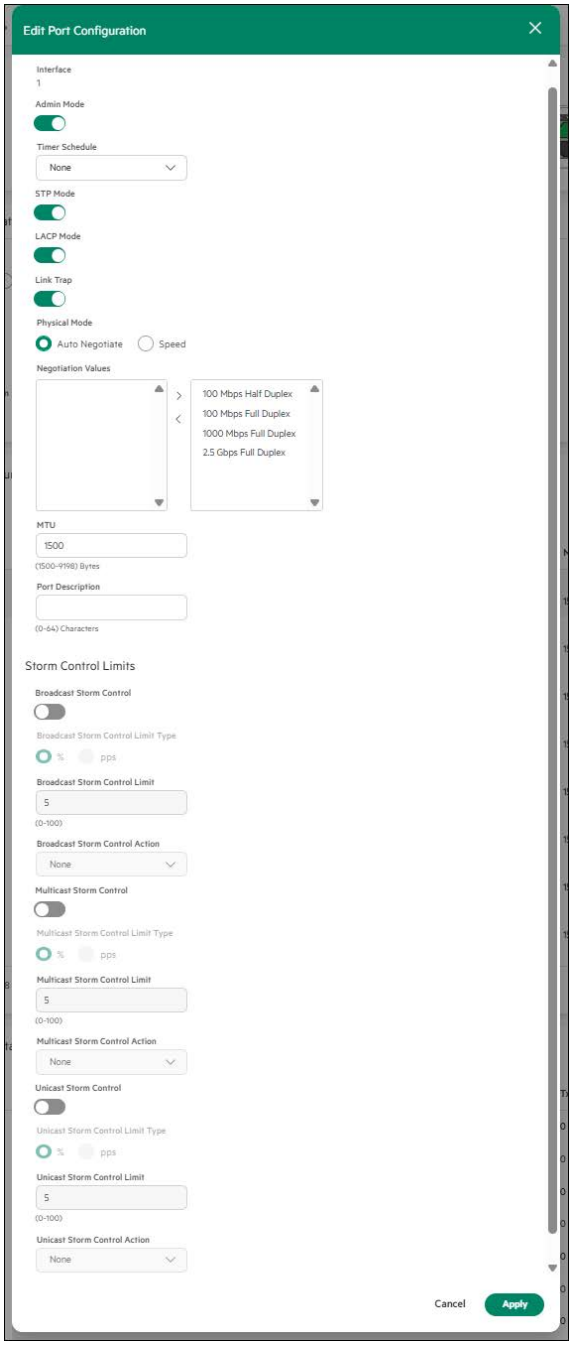


Table 47. Edit Port Configuration Fields

Field	Description
Interface	Indicates the interface(s) that were selected for configuration.
Admin Mode	Enable or disable the port.

Field	Description
Schedule	Select one of the previously defined schedules. See Schedule Configuration for more information on schedules.
STP Mode	Enable or disable STP on the interface.
LACP Mode	Enable or disable the Link Aggregation Control Protocol (LACP) administrative mode. This field can have the following values: · Enabled—The port uses LACP for dynamic LAG configuration. When LACP is enabled, the port sends and receives LACP PDUs with its link partner to confirm that the external switch is also configured for link aggregation. · Disabled—The port supports static LAG configuration only. This mode might be used when the port is connected to a device that does not support LACP. When a port is added to a LAG as a static member, it neither transmits nor receives LACP PDUs. · N/A—The port type is LAG.
Link Trap	Enable or disable generating a trap when the interface link status (up/down) changes.
Physical Mode	Set the port speed and duplex to either auto-negotiation or one of the available options.
Negotiation Values	Determines the link speed settings advertised by the switch during the auto-negotiation.
MTU	Configure the maximum transmission unit (MTU) size for the interface. The valid range is 1500 to 9198 bytes. The default value is 1500 bytes.
Port Description	Describe the interface to help identify it. Up to 64 alphanumeric characters are allowed.
Storm Control Limits	
Broadcast Storm Control	Enable or disable Broadcast Storm Control. If enabled, this feature limits the amount of broadcast frames accepted and forwarded by the port. If the broadcast traffic on the Ethernet port exceeds the configured threshold, the system blocks (discards) the broadcast traffic.
Broadcast Storm Control Limit Type	Select Percent or Rate for the type of broadcast storm control.
Broadcast Storm Control Limit	Set the threshold for broadcast storm control. Limits are defined as percentage, or rate of kilobits per second. Valid values are 0-100. The default is 0.
Broadcast Storm Control Action	Storm control packets that exceed the threshold limit are dropped. This control specifies the additional actions to take if a broadcast storm is detected on the interface. The available options are: · None: No additional action is taken. · Trap: In addition to dropping exceeding traffic, a syslog message and an SNMP trap is sent approximately every 30 seconds until the broadcast storm recovers. · Shutdown: The interface which receives broadcast packets at a rate which is above the threshold is suspended.
Multicast Storm Control	Enable or disable Multicast Storm Control. If enabled, this feature limits the amount of multicast frames accepted and forwarded by the port. If the multicast traffic on the Ethernet port exceeds the configured threshold, the system blocks (discards) the multicast traffic.
Multicast Storm Control Limit Type	Select Percent or Rate for the type of multicast storm control.
Multicast Storm Control Limit	Set the threshold for multicast storm control. Limits are defined as percentage, or rate of kilobits per second. Valid values are 0-100. The default is 0.

Field	Description
Multicast Storm Control Action	Storm control packets that exceed the threshold limit are dropped. This control specifies the additional actions to take if a multicast storm is detected on the interface. The available options are: · None: No additional action is taken. · Trap: In addition to dropping exceeding traffic, a syslog message and an SNMP trap is sent approximately every 30 seconds until multicast storm recovers. · Shutdown: The interface which receives multicast packets at a rate which is above the threshold is suspended.
Unicast Storm Control	Enable or disable Unicast Storm Control. If enabled, this feature limits the amount of unknown unicast frames accepted and forwarded by the switch. If the unicast traffic on the Ethernet port exceeds the configured threshold, the system blocks (discards) the unicast traffic.
Unicast Storm Control Limit Type	Select Percent or Rate for the type of unicast storm control.
Unicast Storm Control Limit	Set the threshold for unicast storm control. Limits are defined as percentage, or rate of kilobits per second. Valid values are 0-100. The default is 0.
Unicast Storm Control Action	Storm control packets that exceed the threshold limit are dropped. This control specifies the additional actions to take if a unicast storm is detected on the interface. The available options are: · None: No additional action is taken. · Trap: In addition to dropping exceeding traffic, a syslog message and an SNMP trap is sent approximately every 30 seconds until unicast storm control recovers. · Shutdown: The interface which receives unicast packets at a rate which is above the threshold is suspended.

Click **Apply** to save the changes for the current switch configuration. The changes take effect immediately and are applied to each of the selected interfaces. The changes are not retained across a switch reset unless you click **Save Configuration**.

Port Summary Statistics

The Port Summary Statistics page displays statistics on packets transmitted and received on each port or trunk. These statistics can be used to identify potential problems with the switch. The displayed values are the accumulated totals since the last clear operation.

To display the Port Summary Statistics page, click **Switching** > **Port Configuration** in the navigation pane and scroll down to the **Port Summary Statistics** tile.

Figure 64. Port Summary Statistics Tile

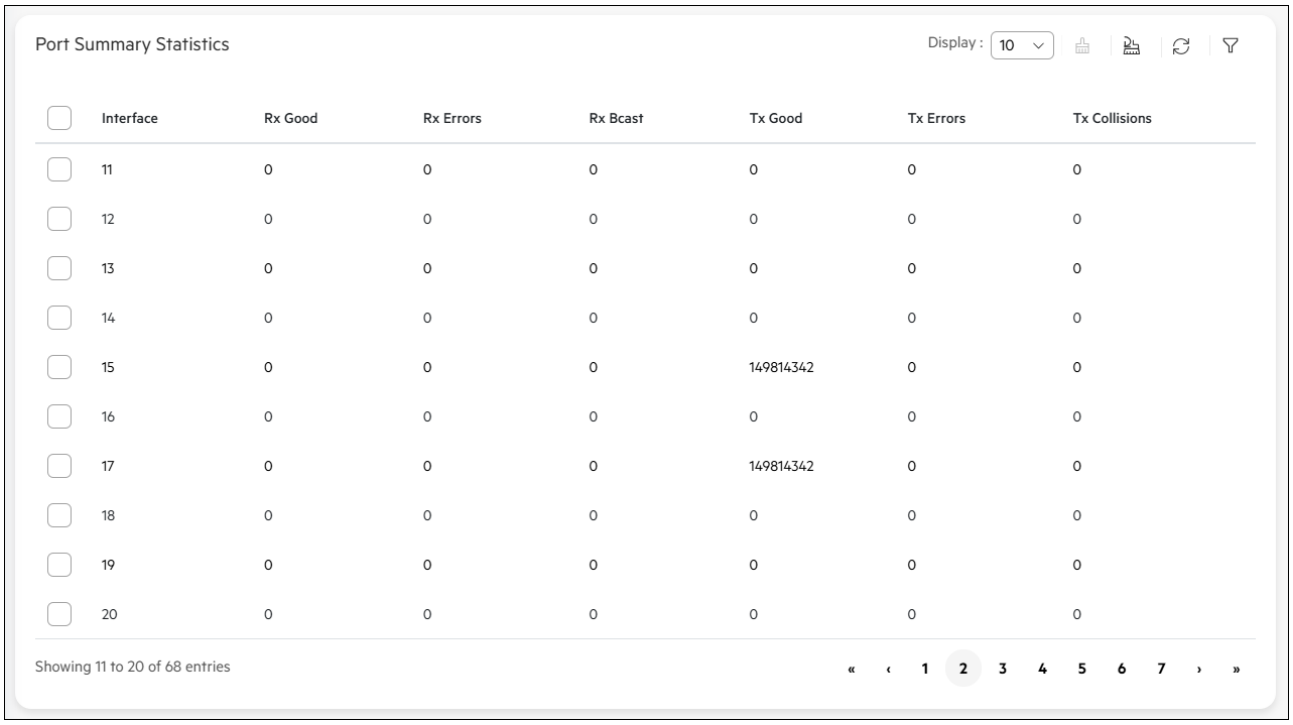


Table 48. Port Summary Statistics Fields

Field	Description
Interface	The port or trunk ID.
Rx Good	The total number of inbound packets received by the interface without errors.
Rx Errors	The number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol.
Rx Broadcast	The total number of good packets received that were directed to the broadcast address. Note that this number does not include multicast packets.
Tx Good	The total number of outbound packets transmitted by the interface to its Ethernet segment without errors.
Tx Errors	The number of outbound packets that could not be transmitted because of errors.
Tx Collisions	The number of packet collisions.

Select a row and click (**Clear**) to reset the row counters to zero. Click click (**Clear All**) to reset all counters to zero.

Flow Control

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period. This Flow Control Configuration table display the IEEE 802.3 Annex 31B flow control settings and status for all interfaces. along with 802.3 Tx and Rx pause counts. If the port is enabled for priority flow control, operational flow control status is displayed as Inactive.

Figure 65. Flow Control Tile

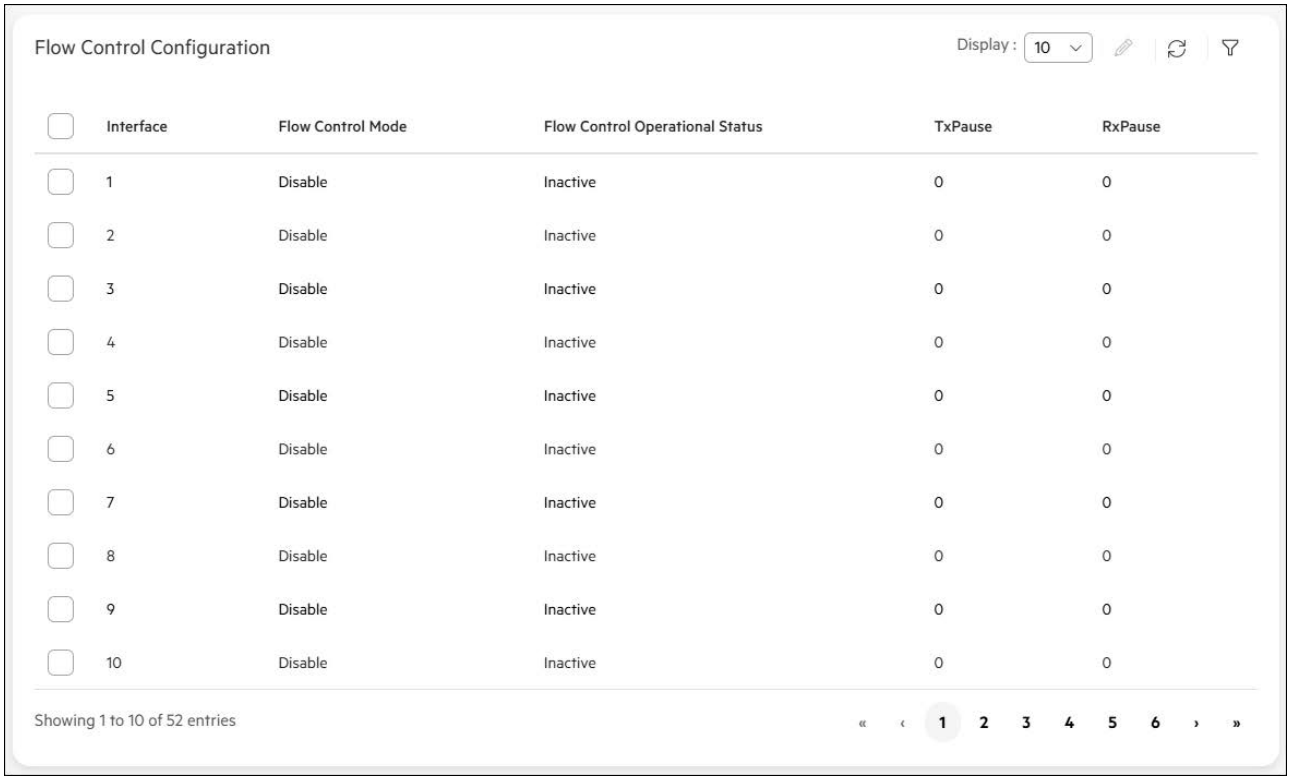


Table 49. Flow Control Fields

Field	Description
Interface	The port ID.
Flow Control Mode	The Flow Control Mode on the Interface. The possible values are: · Disable—To disable the flow control on the interface. · Symmetric—To configure symmetric flow control on the interface. It means a device sends and receives PAUSE frames in both directions to manage traffic flow. · Asymmetric—To configure Asymmetric flow control on the interface. The device is configured to send PAUSE frames in one direction.
Flow Control Operational Status	Indicates the current operational status of flow control on the interface. It reflects whether the flow control mechanism is actively working, based on factors like link status and configuration settings. This status helps to verify if flow control is functioning as expected.
TxPause	It shows the count of TxPause Frames. Occurs when a device receives a pause frame (RX pause) from its peer. It then sends a pause frame back to the peer, acknowledging the pause request and temporarily stopping its own data transmission.
RxPause	It shows the count of RxPause Frames. Occurs when a device receives too much data and its buffer fills up. The device sends a pause frame to the sender, asking them to slow down or stop sending packets.

Select one or more rows and click (**Edit**) to configure flow control on the selected interfaces.

Port Mirroring

Port Mirroring is used to monitor the network traffic that one or more ports send and receive. The Port Mirroring feature creates a copy of the traffic that the source interface handles and sends it to a destination port. All traffic from the source port or ports can be mirrored and sent to the destination port. When the destination is a port on the local device, a network protocol analyzer is typically connected to the port. Multiple switch ports can be configured as source ports, with each port mirrored to the same destination.

To display the Port Mirroring page, click **Switching** > **Port Mirroring** in the navigation pane.

CAUTION

When configuring port mirroring, avoid oversubscribing the destination port to prevent the loss of mirrored data.

While a port is used as the destination port for mirrored data, the port cannot be used for any other purpose; the port will not receive and forward traffic.

Global Configuration

Use the Global Configuration tile to enable or disable port mirroring on the switch and to select the remote mirroring VLAN.

Figure 66. Port Mirroring Global Configuration Tile

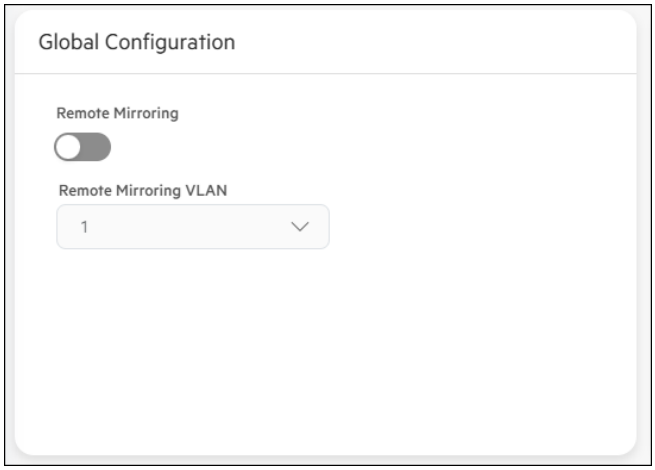


Table 50. Port Mirroring Global Configuration Fields

Field	Description
Remote Mirroring	Toggle the control to enable or disable remote mirroring on the device. · —Disabled · —Enabled
Remote Mirroring VLAN	Select the VLAN of the device to use for remote mirroring.

Click **Apply** to update the switch configuration.

Session Configuration

Use the Session Configuration tile to enable or disable each port mirroring session and associate ACLs with the sessions.

Figure 67. Session Configuration Tile

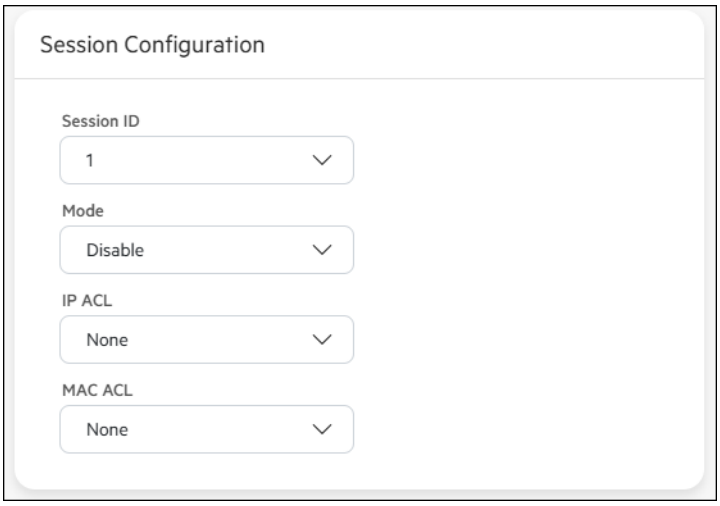


Table 51. Session Configuration Fields

Field	Description
Session ID	The port mirroring session ID. Up to four port mirroring sessions are allowed.
Mode	The administrative mode for the selected port mirroring session. If the mode is disabled, the configured source is not mirroring traffic to the destination. **NOTE:** Enable the mode only after configuring the source and destination.
IP ACL	The ID of the IP ACL to apply to traffic from the source. Only traffic that matches the rules in the ACL is mirrored to the destination.
MAC ACL	The ID of the MAC ACL to apply to traffic from the source. Only traffic that matches the rules in the ACL is mirrored to the destination.

Click **Apply** to update the switch configuration.

Mirroring Sessions Configuration

Use the Mirroring Sessions tile to enable or disable each port mirroring session and associate ACLs with the sessions.

Figure 68. Mirroring Sessions Tile



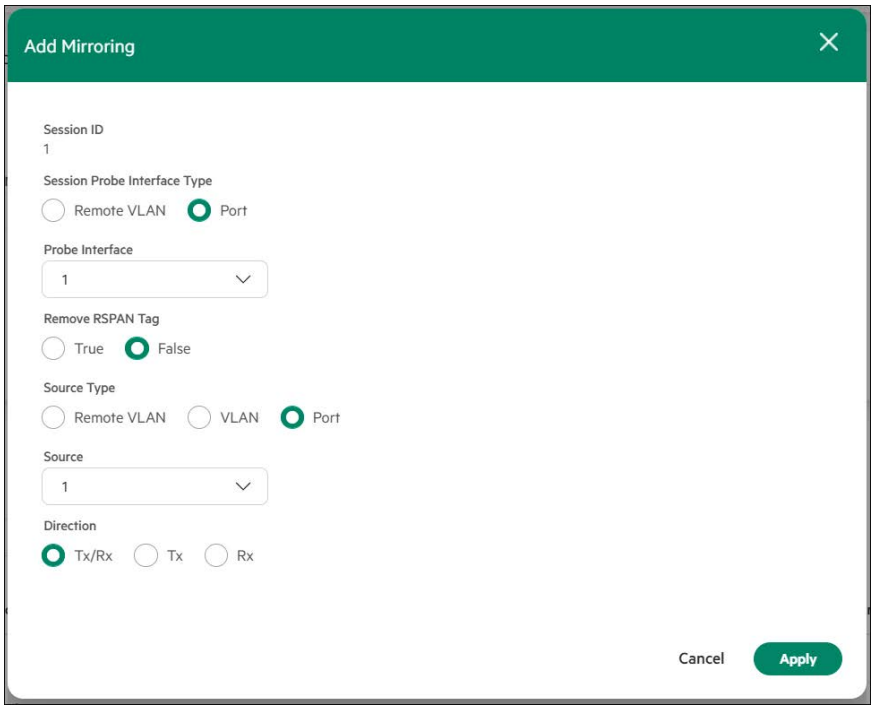
Table 52. Mirroring Sessions Fields

Field	Description
Session ID	The port mirroring session ID. Up to four port mirroring sessions are allowed.
Probe Interface	The switch port to which packets will be mirrored. Typically, a network protocol analyzer is connected to this port. If the port is configured as an interface or probe port, it receives traffic from all configured source ports.
Source	The ports or VLAN configured to mirror traffic to the destination. You can configure multiple source ports or one source VLAN per session. The source VLAN can also be a remote VLAN.
Direction	The direction of traffic on the source port (or source ports) that is sent to the specified destination. A source VLAN mirrors RX traffic only. Possible values for source ports are: · Tx/Rx—Both ingress and egress traffic. · Rx—Ingress traffic only. · Tx—Egress traffic only.

Configuring a Port Mirroring Session

To configuring a port mirroring session, select the Session ID to which the rule applies and click + (**Add**) in the Mirroring Sessions tile. The **Add Mirroring** dialog box appears.

Figure 69. Add Mirroring Dialog Box



Configure the required fields and click **Apply**.

Table 53. Add Mirroring Fields

Field	Description
Session ID	The identifier for the session being configured. For a new session, the ID is New Session.
Session Probe Interface Type	The type of probe interface to use for the session: · Remote VLAN via Port—Set this to monitor traffic via a remote VLAN using the specified port. · Port—The physical port to use as the source probe port to which traffic will be mirrored.
Probe Interface	The probe interface to use for the session.
Remove RSPAN Tag	The packets received at RSPAN destination port are double tagged. Enable this option to remove RSPAN VLAN ID tag for mirroring session.
Source Type	The type of interface to use as the source: · Remote VLAN—Traffic to a configured remote VLAN is mirrored. · VLAN—Traffic to a configured VLAN is mirrored. In other words, all the packets received on all the physical ports that are members of the VLAN are mirrored. VLAN can be specified as source only if the session ID is 1. · Port—Traffic is mirrored to and/or from a physical port on the switch.
Source	Specify the source interfaces for mirrored traffic. Interface type depends on the value set in the Source Type field.

Field	Description
Direction	The direction of traffic on the source port (or source ports) that is sent to the specified destination. A source VLAN mirrors RX traffic only. Possible values for source ports are: · Tx/Rx—Both ingress and egress traffic. · Rx—Ingress traffic only. · Tx—Egress traffic only.

NOTE

A port will be removed from a VLAN when it becomes a destination (probe) port.

NOTE

A port cannot be defined as a destination (probe) port if it is configured as a member of a LAG.

Removing Source Ports from a Session

To remove one or more source ports from a port mirroring session, select the appropriate session ID, select each source port to delete, and click (**Remove)** in the Mirroring Sessions tile.

Loop Protection

Loops on a network consume resources and can degrade network performance. Detecting loops manually can be very cumbersome and time consuming. The HPE Networking Instant On 1940 Switch Series software provides an automatic loop protection feature.

This feature allows loop detection in the network for switches that do not run spanning tree, or on which STP feature is disabled.

When loop protection is enabled on the switch and on one or more interfaces (ports or trunks), the interfaces send loop protection protocol data units (PDUs) to the multicast destination address 09:00:09:09:13:A6, using the switch's base MAC address as the source address.

If STP is enabled on switch the interface will send PDUs only if STP is in the forwarding state.

When an interface receives a loop protection PDU, it compares the source MAC address with switch base MAC address and if there is a match a loop state is detected. Upon detection of a loop, the port is disabled. Once a port is disabled, for the duration of one second, other ports will not process loop protection PDUs. This is to allow the network to stabilize, following disabling the port.

A port that is disabled by loop protection can be recovered by one of the following:

- If auto-recovery is enabled for loop protection, after the timeout expires, the port attempts to recover.
- If auto-recovery is disabled, you can attempt to manually recover the port in the Suspended Interface tile on the **Switching > Interface Auto Recovery** page.

Global Configuration

Use the Global Configuration tile to enable or disable loop protection globally on the switch and to configure the PDU transmission interval.

Figure 70. Loop Protection Global Configuration Page

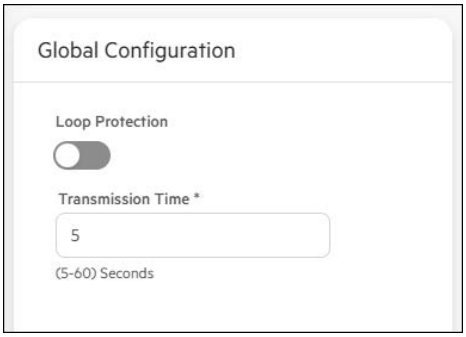


Table 54. Loop Protection Global Configuration Fields

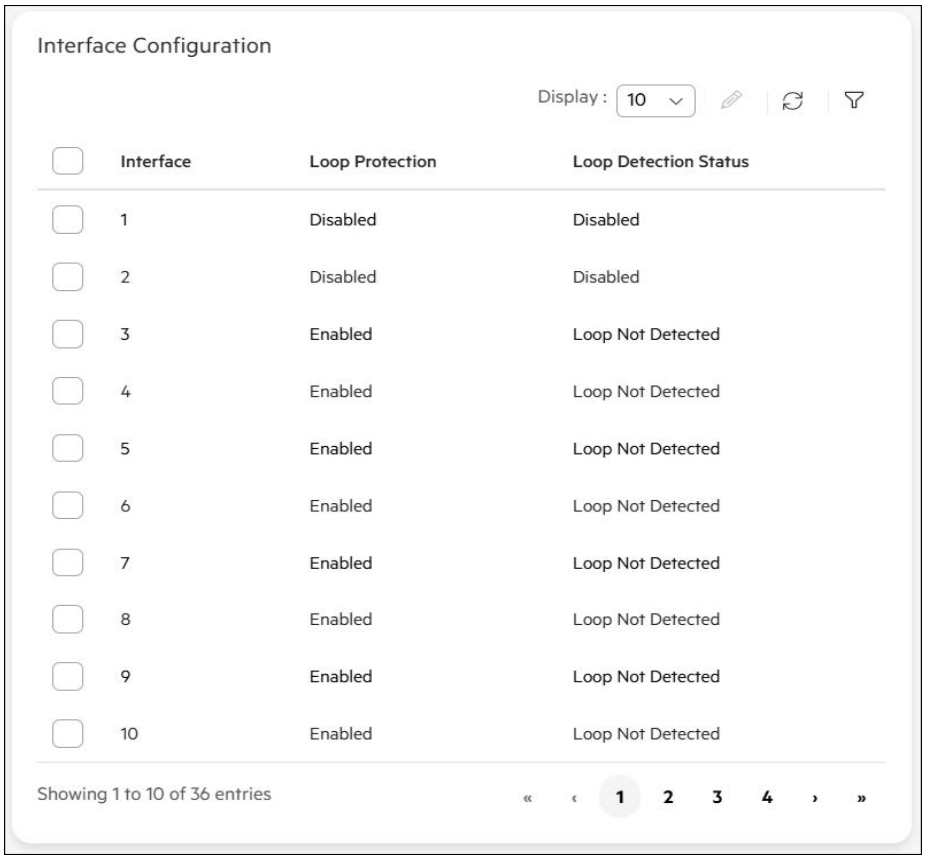
Field	Description
Loop Protection	Toggle the control to administratively enable or disable this feature globally on the switch. Loop protection is disabled by default. · —Disabled · —Enabled
Transmission Time	The interval at which the switch sends loop protection PDUs on interfaces on which Loop Protection is enabled. The range is 5 to 60 seconds and the default is 10 seconds.

If you modify these settings, click **Apply** to save the changes for the current switch configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save** on the top-right side of the page.

Interface Configuration

Use the Interface Configuration tile to enable or disable loop protection on one or more interfaces on the switch.

Figure 71. Interface Configuration Page



To configure loop protection on one or more interfaces, select each interface to configure and click (**Edit**). The same settings are applied to all selected interfaces.

Table 55. Interface Configuration Fields

Field	Description
Interface	Identifies the selected interface or interfaces.
Loop Protection	Toggle the control to enable or disable this feature on the interface. Loop protection is disabled by default on all interfaces. · —Disabled · —Enabled
Loop Detection Status	The current loop status of the port. · Disabled—Loop detection is disabled. · Loop Detected—This status displays under the following conditions: o Loop protection is enabled on the port, the operational status is up, and a loop is detected. o The operational status is down and the port is diag-disabled due to loop protection. · Loop Not Detected—Loop protection is enabled on the port, and no loop detected.

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows a switch to forward multicast traffic intelligently. Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports, which could affect network performance.

The device also supports IGMP Snooping Querier. The IGMP Snooping Querier is used to support L2 multicast domain of snooping switches in the absence of a multicast router. A typical example is a local network where the multicast content is provided from a local server, and the router (if one exists) for that network does not support multicast.

The local IGMP Snooping Querier uses the configurable parameters of the IGMP Snooping when it is building the General Query message. The network administrator can configure an IGMP snooping switch to be an IGMP Snooping Querier of a VLAN.

If a VLAN is shared by more than one IGMP snooping switch, the user should verify that only one switch is configured as the IGMP Querier of a VLAN.

When enabled, the switch supports IGMPv1, IGMPv2.

If you change any settings on the page, click **Apply** to save the changes for the current boot session. The changes take effect immediately but are not retained across a switch reset unless you click **Save**.

Global Configuration

To enable IGMP snooping and view global status information, click **Switching** > **IGMP Snooping** in the navigation pane.

Figure 72. IGMP Snooping Global Configuration Tile

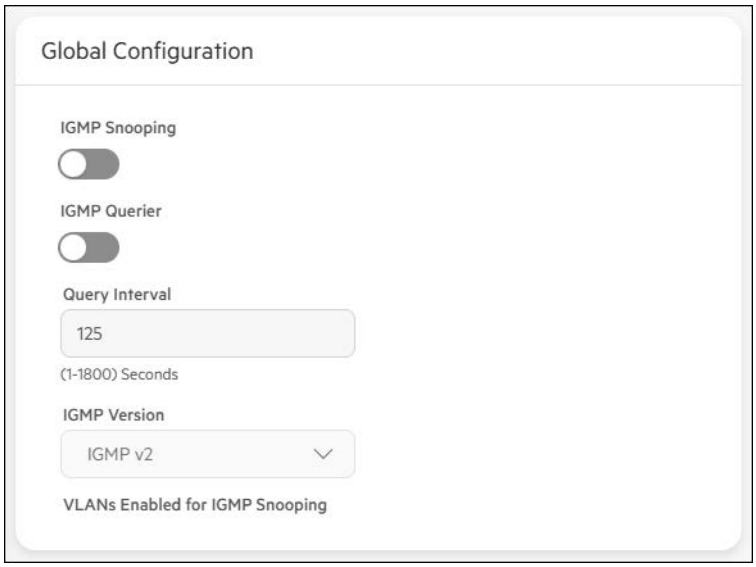


Table 56. IGMP Snooping Global Configuration Fields

Field	Description
IGMP Snooping	Set as enabled to globally enable IGMP snooping on the switch. This feature is disabled by default. · —Disabled · —Enabled
IGMP Querier	Set as enabled to globally enable IGMP querying on the switch. This feature is disabled by default. · —Disabled · —Enabled
Query Interval (Seconds)	The amount of time the IGMP snooping querier on the device should wait between sending periodic IGMP queries.
IGMP Version	The IGMP protocol version used in periodic IGMP queries.
VLANs Enabled for IGMP Snooping	Identifies the VLAN ID of each VLAN on which IGMP snooping is administratively enabled. If IGMP snooping is not enabled on any VLANs, this field shows None.

IPv4 Unregistered Multicast

The IPv4 Unregistered Multicast feature enables configuring the handling of Multicast frames that belong to unregistered Multicast groups. Unregistered Multicast groups are the groups that are not known to the switch. The Multicast switch (when it operates as an L2 switch) learns about Multicast groups through IGMP Snooping or through static configuration.

Normally, Multicast frames are always flooded to all ports in the VLAN. If IGMP Snooping is enabled, the switch learns about the existence of Multicast groups and keeps track of which ports have joined which Multicast group. This enables the switch to forward the Multicast frames (from a registered Multicast group) only to ports that are registered to that Multicast group.

All unregistered Multicast frames, i.e. the Multicast frames that do not belong to a registered Multicast group, are still flooded to all ports on the VLAN. The IPv4 Unregistered Multicast feature allows you to configure whether to forward these Multicast frames to all ports or to filter (drop) them.

Figure 73. IPv4 Unregistered Multicast Tile



Table 57. IPv4 Unregistered Multicast Fields

Field	Description
Forwarding	Use the toggle button enable or disable forwarding unknown multicast traffic to all ports. · —Disabled · —Enabled

IGMP Snooping VLAN Configuration

Use the IGMP Snooping VLAN Configuration tile to configure IGMP snooping settings on specific VLANs.

Figure 74. IGMP Snooping VLAN Configuration Tile

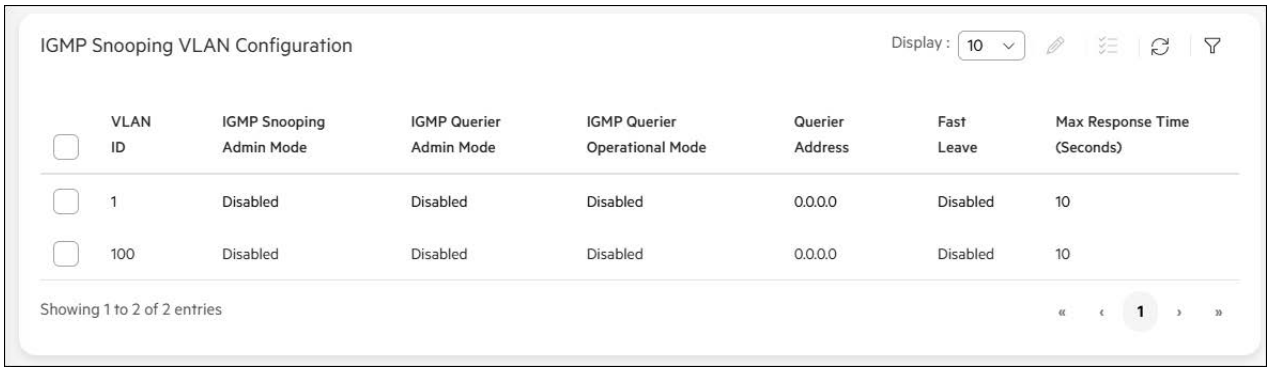


Table 58. IGMP Snooping VLAN Configuration Fields (Tile)

Field	Description
VLAN ID	The VLAN interface associated with the rest of the data in the row.
IGMP Snooping Admin Mode	The administrative mode of IGMP snooping on the VLAN interface. IGMP snooping must be enabled globally and on an VLAN interface to be able to snoop IGMP packets and determine which segments should receive multicast packets directed to the group address.
IGMP Querier Admin Mode	The administrative mode of IGMP querier on the VLAN interface. IGMP querier must be enabled globally and on a VLAN interface to be able to send IGMP query packets.
IGMP Querier Operational Mode	The operational state of the IGMP Snooping Querier on a VLAN, which is one of the following: · Querier—The snooping switch is the querier in the VLAN. The snooping switch will send out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch sees a better querier (numerically lower) in the VLAN, it moves to non-querier mode. · Non-Querier—The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch moves into querier mode. · Disabled—The snooping querier is not operational on the VLAN. The snooping querier moves to the disabled mode when IGMP snooping is not operational on the VLAN, when the querier address is not configured, or the network management address is not configured.
Querier Address	The address of the querier.
Fast Leave	The administrative mode of Fast Leave on the VLAN interface. If Fast Leave is enabled, the VLAN interface can be immediately removed from the Layer 2 forwarding table entry upon receiving an IGMP leave message for a multicast group without first sending out MAC-based general queries.
Max Response Time (Seconds)	The maximum number of seconds a host can wait before sending a group report once it receives a membership query. The specified value should be less than the Group Membership Interval.

Configuring IGMP Snooping on a VLAN

To configure IGMP snooping on a VLAN, select one or more VLANs configured on the switch, click (**Edit**), configure the required settings, and click **Apply**.

Figure 75. IGMP Snooping VLAN Configuration (Dialog Box)

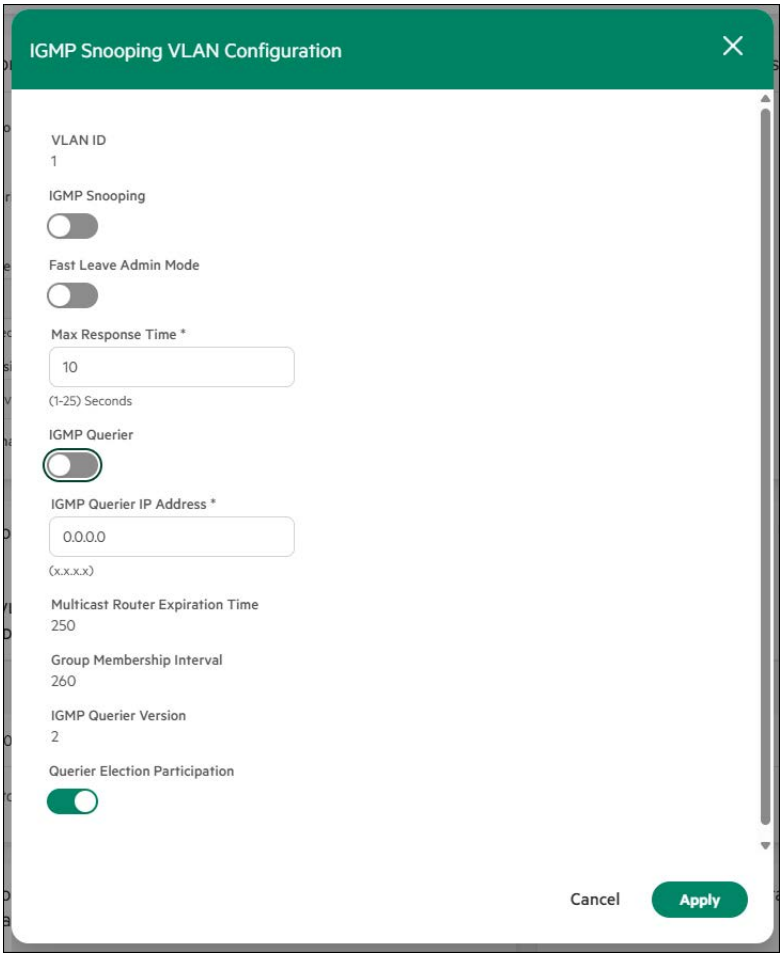


Table 59. IGMP Snooping VLAN Configuration Dialog Box Fields

Field	Description
VLAN ID	The VLAN interface(s) that are being configured.
IGMP Snooping	The administrative mode of IGMP snooping on the VLAN interface. IGMP snooping must be enabled globally and on an VLAN interface to be able to snoop IGMP packets and determine which segments should receive multicast packets directed to the group address.
Fast Leave	The administrative mode of Fast Leave on the VLAN interface. If Fast Leave is enabled, the VLAN interface can be immediately removed from the Layer 2 forwarding table entry upon receiving an IGMP leave message for a multicast group without first sending out MAC-based general queries.
Max Response Time	The maximum number of seconds a host can wait before sending a group report once it receives a membership query. The specified value should be less than the Group Membership Interval. The valid range is 1 to 25 seconds. The default is 10 seconds.
IGMP Querier	The administrative mode of IGMP querier on the VLAN interface. IGMP querier must be enabled globally and on a VLAN interface to be able to send IGMP query packets.
IGMP Querier IP Address	The IPv4 address of the IGMP querier.

Field	Description
Multicast Router Expiration Time	The number of seconds after which a multicast router entry is timed out. This value is not configurable. The default value is 250 seconds.
Group Membership Interval	The interval that must pass before the router decides that no members of a group or source exist on the network. This value is not configurable. The default is 260 seconds.
IGMP Querier Version	The IGMP protocol version used in periodic IGMP queries. This is a global configuration.
IGMP Querier Election	Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.

IGMP Snooping Multicast Router Interface Configuration

Use the IGMP Snooping Multicast Router Interface Configuration tile to manually configure an interface within a VLAN as an IGMP snooping multicast router interface.

If a multicast router is attached to the switch, its existence can be learned dynamically. You can also statically configure one or more VLANs on each interface to act as a multicast router interface, which is an interface that faces a multicast router or IGMP querier and receives multicast traffic.

Figure 76. IGMP Snooping Multicast Router Interface Configuration Tile

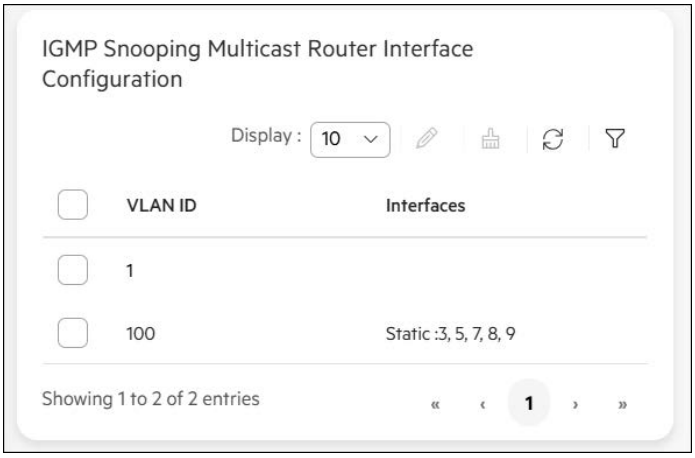


Table 60. IGMP Snooping Multicast Router Interface Configuration Fields

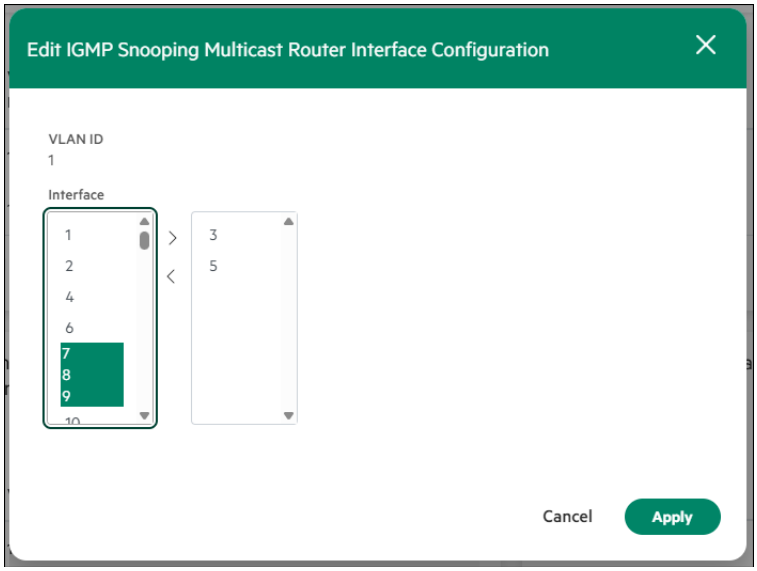
Field	Description
VLAN ID	The ID of the VLAN configured as enabled for multicast routing on the associated interface.
Interface	The statically configured multicast router ports associated with the VLAN.

Configuring Multicast Router Settings on Interfaces

To configure an interface within a VLAN as an IGMP snooping multicast router interface, select one or more VLANs configured on the switch and click (**Edit**).

In the Edit IGMP Snooping Multicast Router Configuration dialog box, select one or more interfaces that you want to configure as IGMP snooping multicast router interfaces and click the right arrow. To remove an interface from the list on the right, select it and press the left arrow. Click **Apply** to save the changes for the current switch configuration.

Figure 77. Edit IGMP Snooping Multicast Router Configuration Dialog Box



Multicast Forwarding Database

The Multicast Forwarding Database tile displays the Multicast group addresses learned from IGMP. Interface membership is displayed for each VLAN.

Figure 78. Multicast Forwarding Database Tile

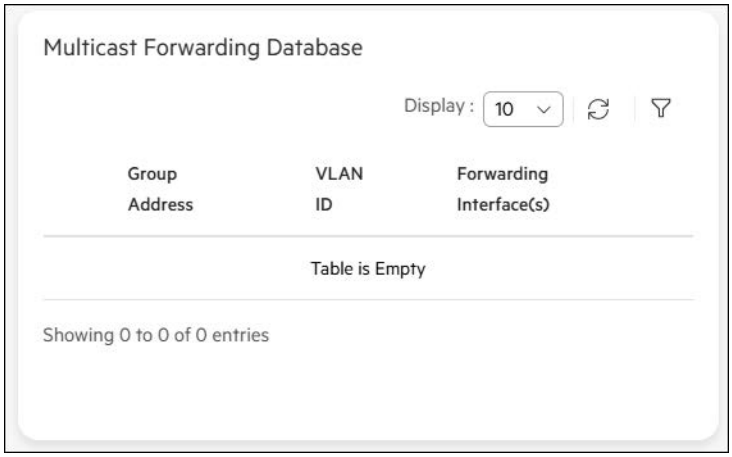


Table 61. Multicast Forwarding Database Fields

Field	Description
Group Address	The Multicast Address group for which information is displayed.
VLAN ID	The ID of the VLANs on which multicast groups were registered.
Forwarding Interfaces	Interfaces that are registered to this group.

IGMPv3 Multicast Forwarding Database

The IGMPv3 Multicast Forwarding Database tile displays the entries in the multicast forwarding database (MFDB) for source-specific multicast that were added because they were discovered by the IGMP Snooping feature.

Figure 79. IGMPv3 Multicast Forwarding Database Tile



Table 62. IGMPv3 Multicast Forwarding Database Fields

Field	Description
Type	Type of snooping. The value can be IGMP Snooping.
VLAN ID	The ID of the VLANs on which the entry has been learned.
Group	The multicast group address.
Source	The source address.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group.
Interfaces	Specifies the list of interfaces on which an incoming packet is forwarded.

Interface Auto Recovery

Several features on the switch can set the port to a suspended state when defined error conditions are met. The auto recover feature enables a suspended port to exit this suspended state after a period of time.

The following list describes the features supported by Auto Recovery and the error conditions that cause a port to be placed into the suspended state:

- BPDU Guard: If a port that has the BPDU Guard feature enabled receives a BPDU, the port state is set to Suspended.
- Storm Control: Interface-level storm control setting includes a “shutdown” action. If this action is selected and the incoming rate of unicast (with unknown destination), multicast, or broadcast packets exceeds a set threshold, the port moves to the Suspended state.
- Port Security: If a port that has the Violation Shutdown Mode feature enabled receives unknown MAC addresses after the MAC limit is reached, the port moves to the Suspended state.
- Loop Protection: If a loop is detected on an interface with loop protection enabled, the port state is set to Suspended.
- Link Flap Prevention: If excessive link flapping is detected on an interface on which link flap prevention is enabled, the port state is set to Suspended.
- BPDU Storm: If a port that has the BPDU Storm feature enabled receives flood of BPDUs, the port state is set to Suspended.
- DHCP Rate Limit: If a port exceeded the allowed rate for DHCP requests with DHCP Rate Limit enabled, the port state is set to Suspended.

- Denial of Service: If a port that has Denial of Service (DoS) feature enabled experiences abnormal traffic patterns suggesting a DoS attack, the port state is set to Suspended.
- Authentication Manager: If a port that has Authentication Manager feature enabled detects unknown MAC Address attempts to connect to it, the port state is set to Suspended.
- UDLD: If a port detects that the link is unidirectional instead of bidirectional on which UDLD Auto recovery feature is enabled, the port state is set to Suspended.
- ARP Inspection: If a port that has ARP Inspection feature enabled detects that the rate of incoming ARP packets exceeds the configured limit, the port state is set to Suspended.

When a port has been placed into a Suspended state, the port is shutdown, and no traffic is sent or received on the port until it is either manually enabled by the administrator or re-enabled by the Auto Recovery feature.

The Auto Recovery feature automatically re-enables a suspended port when the error conditions that caused the port to be disabled are no longer detected. The switch uses a configurable Auto Recovery timer to periodically check the error condition at set intervals. If the error condition is no longer present, the port is re-enabled. The administrator can manually override the timer setting by re-enabling a port at any time.

Auto Recovery is disabled by default for all conditions except Link Flap Prevention. If Auto Recovery is disabled after ports have been placed in a suspended state, they will remain disabled until an administrator manually enables them.

To display this page, click **Switching > Interface Auto Recovery**.

Global Configuration

Use the Global Configuration tile to configure Auto Recovery settings for each supported feature and to set how often the switch checks the error condition.

For all features, toggle the control to enable or disable Auto Recovery:

- —Disabled
- —Enabled

Figure 80. Auto Recovery Global Configuration Tile

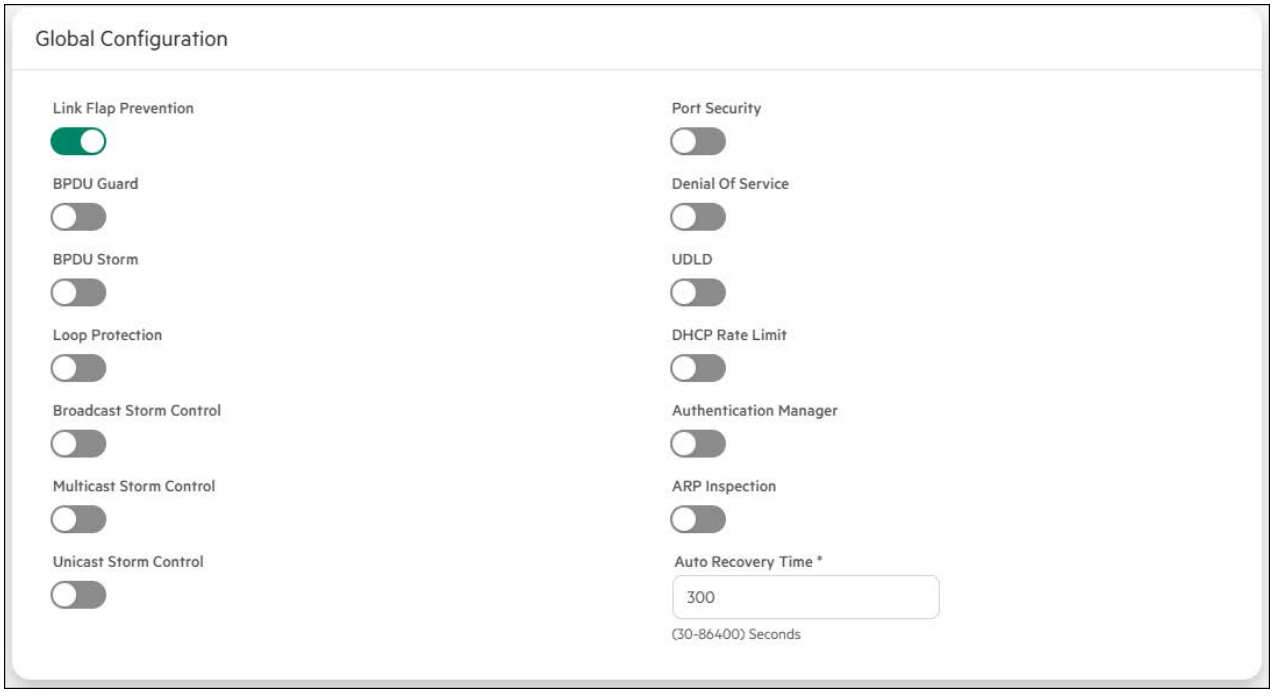


Table 63. Auto Recovery Global Configuration Fields

Field	Description
BPDU Guard	When BPDU Guard Auto Recovery is enabled, the port will be enabled once the configured Recovery Time expires. If the port receives another BPDU, it will be disabled again. If the BPDU Guard Auto Recovery mode is disabled, a port that has received a BPDU and has been placed in the suspended state will remain in that state until an administrator manually enables it. BPDU Guard Auto Recovery is disabled by default.
Unicast Storm Control	If the incoming rate of unicast (with unknown destination) packets exceeds a set threshold, the port moves to the suspended state. When Unicast Storm Control Auto Recovery is enabled, the port will be enabled once the configured Recovery Time expires. If the port continues to receive unicast (with unknown destination) packets exceeding the set threshold, that port will be disabled again. Unicast Storm Control Auto Recovery is disabled by default.
Multicast Storm Control	If the incoming rate of multicast packets exceeds a set threshold, the port moves to the suspended state. When Multicast Storm Control Auto Recovery is enabled, the port will be enabled once the configured Recovery Time expires. If the port continues to receive multicast packets exceeding the set threshold, that port will be disabled again. Multicast Storm Control Auto Recovery is disabled by default.
Broadcast Storm Control	If the incoming rate of broadcast packets exceeds a set threshold, the port moves to the suspended state. When Broadcast Storm Control Auto Recovery is enabled, the port will be enabled once the configured Recovery Time expires. If the port continues to receive broadcast packets exceeding the set threshold, that port will be disabled again. Broadcast Storm Control Auto Recovery is disabled by default.
Port Security	If a port that has the Violation Shutdown Mode feature enabled receives unknown MAC addresses after the MAC limit is reached, the port moves to the suspended state. When Port Security Auto Recovery is enabled, the port will be enabled once the configured Recovery Time expires. If the port continues to receive unknown MAC addresses after the MAC limit is reached, the port will be disabled again. Port Security Auto Recovery is disabled by default.
Loop Protection	If a loop is detected on an interface with loop protection enabled, the port state is set to Suspended. Loop Protection is disabled by default.
Link Flap Prevention	If excessive link flapping is detected on an interface on which link flap prevention is enabled, the port state is set to Suspended. Link Flap Prevention is enabled by default.
BPDU Storm	When BPDU Storm Control Auto Recovery is enabled, a port disabled due to excessive BPDUs will be enabled after the Recovery Time. If the storm continues, it will be disabled again. BPDU Storm is disabled by default.
DHCP Rate Limit	When DHCP Rate Limit Auto Recovery is enabled, the port will be re-enabled after the Recovery Time elapses if it was disabled due to excessive DHCP messages. If the high rate of DHCP messages continues, it will be disabled again. DHCP Rate Limit is disabled by default.
Denial Of Service	When Denial Of Service is enabled, the port will be suspended if it detects suspicious activity (such as abnormal traffic patterns or excessive broadcast/multicast packets), and will be re-enabled after the Recovery Time expires. Denial Of Service is disabled by default.
Authentication Manager	If Authentication Manager Auto Recovery is enabled, the port will be suspended if a device with an unknown MAC address attempts to connect to it. Authentication Manager is disabled by default.

Field	Description
UDLD	Port will be suspended if it detects that the link is unidirectional instead of bidirectional, when UDLD Auto Recovery is enabled, and will be re-enabled after the Recovery Time expires. UDLD Auto recovery is disabled by default.
ARP Inspection	When ARP Inspection Auto Recovery is enabled, port will get suspended if it detects that the rate of incoming ARP packets exceeds the configured limit. ARP Inspection Auto recovery is disabled by default.
Auto Recovery Time	Configurable time interval (in seconds) for auto recovery. Default is 300 seconds, range from 30 to 86400 seconds.

If you modify these settings, click **Apply** to save the changes for the current switch configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save**.

Suspended Interfaces

The Suspended Interfaces tile displays interfaces suspended due to one of the conditions specified in the Interface Auto Recovery Global Configuration Fields and the time to recover (if enabled).

Figure 81. Suspended Interfaces Tile



Table 64. Suspended Interfaces Fields

Field	Description
Interface	The interface that is suspended. If no interfaces are in the suspended state, the table is blank.
Reason	If the switch detects an error condition for an interface, the switch puts the interface in the suspended state, meaning that it has been intentionally disabled because it has encountered errors. The reasons that the interface can go into a suspended state include the following: · ARP Inspection · Authentication Manager · BPDU Guard · BPDU Storm · Denial Of Service · DHCP Rate Limit · Link Flap Prevention · Loop Protection · Multicast Storm · Port Security · Unicast Storm · UDLD
Time to Recover	When Auto Recovery is enabled and the interface is placed in the suspended state, then a recovery timer starts for that interface. Once this timer expires, the switch checks if the interface is in the suspended state. If yes, then the switch enables the interface.

To re-enable one or more interfaces select them from the Suspended Interface table and click (**Recover Interface**).

NOTE

If the error condition still exists on the interface it may be shutdown again due to this condition.

Link Aggregation

Link aggregation enables combining multiple full-duplex Ethernet links into a single logical link known as a Link Aggregation Group (LAG). Network devices treat the aggregation as if it were a single link, which increases fault tolerance and throughput by providing load sharing capability.

NOTE

LAGs are also referred to as trunks or port-channels.

A LAG interface can be either static or dynamic:

- Dynamic: Dynamic LAG use the Link Aggregation Control Protocol (LACP, IEEE standard 802.3ad). An LACP-enabled port automatically detects the presence of other directly attached switches supporting LACP and exchanges Link Aggregation Control Protocol Data Units (LACPDUs) with links in the LAG. The PDUs contain information about each link and enable the LAG to maintain them.
- Static: Static LAG are assigned to a trunk group by the administrator. Members do not exchange LACPDUs. A static LAG does not require a partner system to be able to aggregate its member ports. This is the default LAG type.

All members of a LAG must participate in the same protocols. A static LAG interface does not require a partner system to be able to aggregate its member ports.

From a system perspective, a LAG is treated as a physical port. A LAG and a physical port use the same configuration parameters for parameters such as: administrative enable/disable, port priority, and path cost.

A LAG failure of one or more of the links does not stop traffic. Upon failure, the traffic mapped to a link is dynamically reassigned to the remaining links of the LAG. Similarly when links are added to a LAG, existing traffic may automatically shift to a different link member within the LAG. Before shifting traffic, the system ensures reordered frames do not exist.

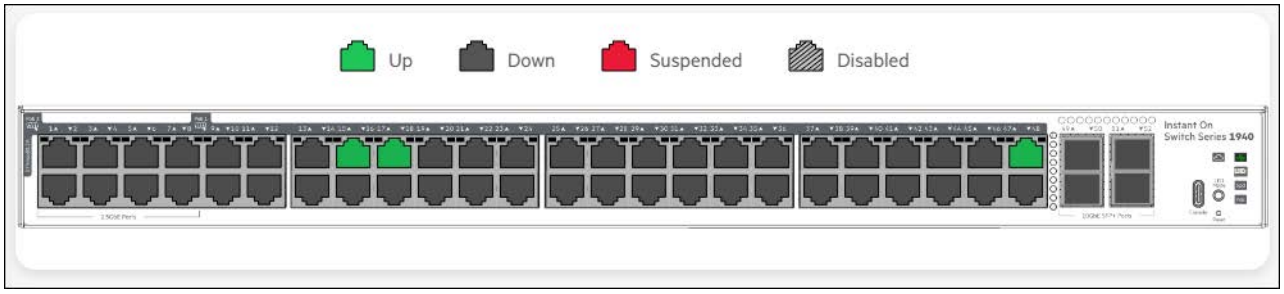
When a link is added to a LAG, it retains its configuration. However this configuration is not active. Once the link is removed from the LAG, all the interface-configured settings become active.

The number of LAGs supported and ports per LAG depends on the HPE Networking Instant On 1940 Switch Series model.

Device View

The top of the Link Aggregation page shows a graphical representation of the switch front panel. This panel view has a display of the ports, each with its current status. The LAG ports also show the LAG ID.

Figure 82. Device View



For more information about the device view, see Device View.

Global Configuration

You can use the Global Configuration tile to select the hashing algorithm used to distribute traffic load among the physical ports of the LAG while preserving the per-flow packet order. The hashing algorithm uses various packet attributes to determine the outgoing physical port. This setting is global and effects all system LAGs.

Figure 83. Link Aggregation Global Configuration Tile

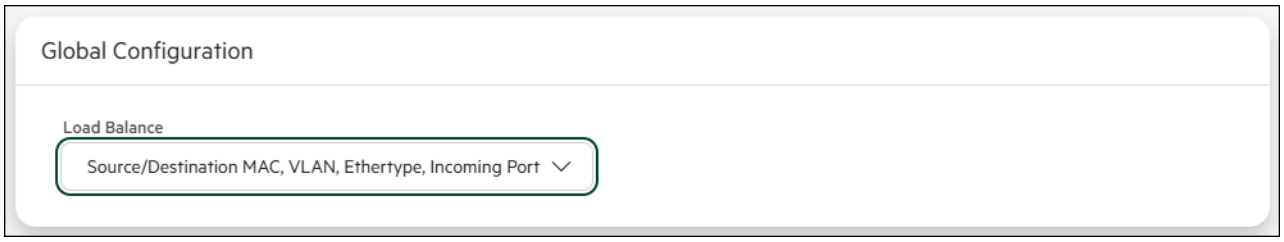


Table 65. Link Aggregation Global Configuration Field

Field	Description
Load Balance	The following sets of packet attributes can be used to compute the hashing algorithm: · Source MAC, VLAN, EtherType, Incoming Port · Destination MAC, VLAN, EtherType, Incoming Port · Source/Destination MAC, VLAN, EtherType, Incoming Port (default) · Source IP and Source TCP/UDP Port Fields · Destination IP and Destination TCP/UDP Port Fields · Source/Destination IP and TCP/UDP Port Fields

Link Aggregation

You can use the Link Aggregation tile to view and edit trunks. The number of trunks on the system is fixed, and by default there are no port members in trunks. You can enable, disable, and edit settings for each trunk.

Figure 84. Link Aggregation Tile

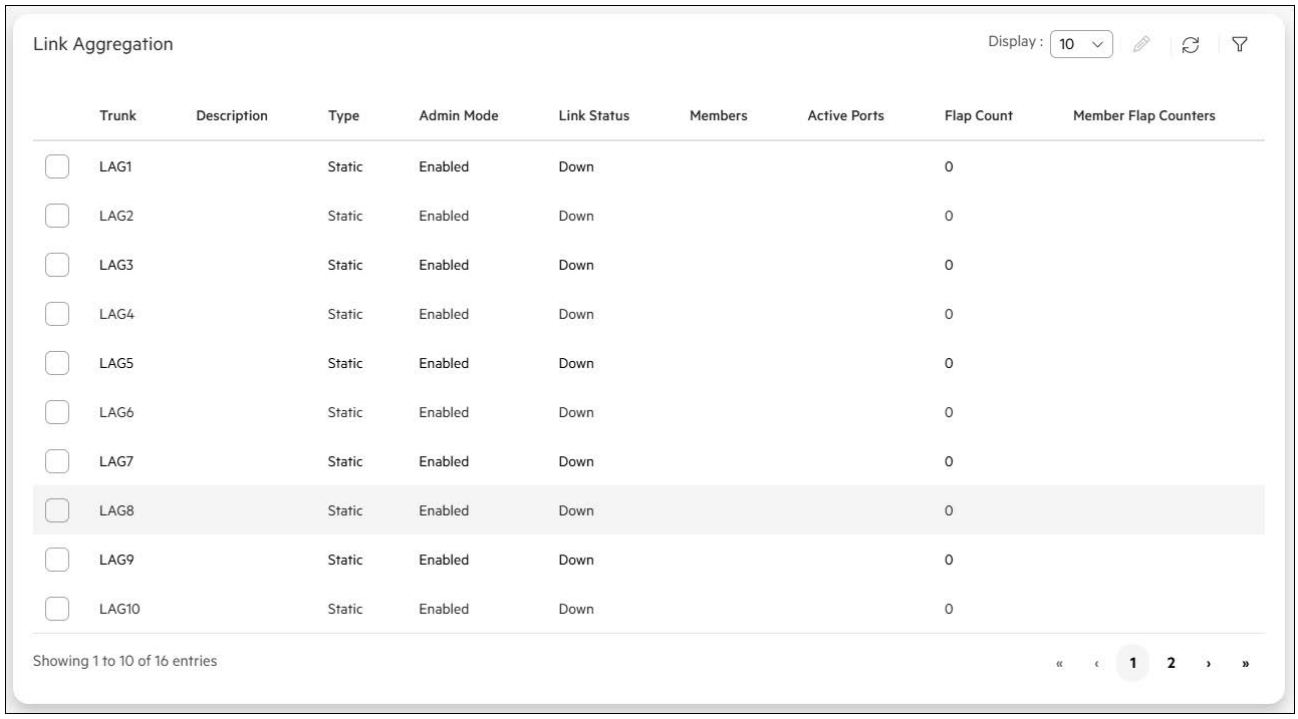


Table 66. Link Aggregation Fields

Field	Description
Trunk	The trunk ID.
Description	The trunk description, if any, associated with the interface to help identify it.
Type	Trunks can be either dynamic or static, but not both: · LACP—Link Aggregation Control Protocol (LACP, IEEE standard 802.3ad). An LACP-enabled port automatically detects the presence of other aggregation-capable network devices in the system and exchanges Link Aggregation Control Protocol Data Units (LACPDUs) with links in the trunk. The PDUs contain information about each link and enable the trunk to maintain them. · Static—Static trunks are assigned to a bundle by the administrator. Members do not exchange LACPDUs. A static trunk does not require a partner system to be able to aggregate its member ports. This is the default port type.
Admin Mode	Whether the trunk is administratively enabled or disabled. This feature is enabled by default.
Link Status	Indicates the operational status of the trunk interface: Up, Up (SFP) for ports with SFP transceivers, or Down.
Members	The ports that are members of the trunk. By default, no ports belong to any trunk.
Active Ports	The ports that are actively participating members of a trunk. A member port that is operationally or administratively disabled or does not have a link is not an active port.

Field	Description
Flap Count	The number of times the interface has gone down. The counter for a member port is incremented when the physical port is either manually shut down by the administrator or when its link state is down. When a port channel is administratively shut down or all active member ports of a port channel are down the flap counter for the port channel is incremented.
Member Flap Counters	The Member Flap Counter tracks the number of times an individual port within a port-channel (EtherChannel) goes down and comes back up. This can occur due to physical link failures, administrative shutdowns, or other disruptions affecting the specific member port. Each member port in the port-channel has its own flap counter, which helps monitor the stability of individual links.

Modifying Trunk Settings

To modify a trunk, select it and click (**Edit**). The Edit Trunk Configuration dialog box displays.

Figure 85. Edit Existing Trunk Dialog Box

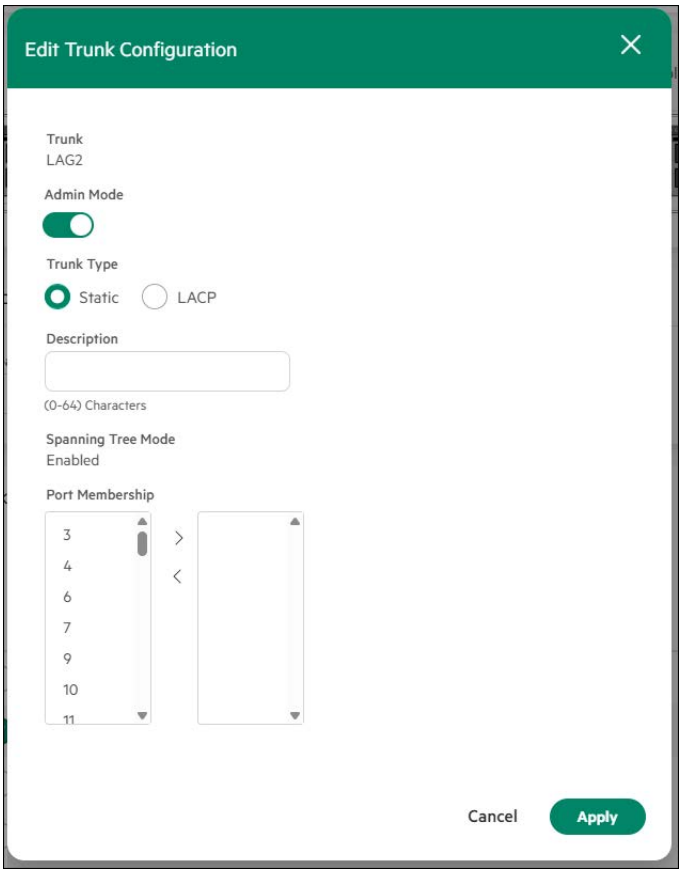


Table 67. Additional Trunk Configuration Fields

Field	Description
Trunk	The trunk ID.
Admin Mode	Administratively enable or disable the trunk.
Description	Enter a description for the trunk.

Field	Description
STP Mode	The spanning tree protocol (STP) mode of the trunk. When enabled, the trunk participates in the STP operation to help prevent network loops. This is a read-only field. Use the CST Configuration tile to set the TRUNK STP mode. By default, the STP mode is enabled.
Port Membership	The list on the left shows ports that are not members of the trunk. The list on the right shows the ports that are members of the trunk. Use the arrows to move ports between the lists.
Trunk Type	Choose **Static** for a static trunk. Choose **LACP** for a dynamic trunk using Link Aggregation Control Protocol.

Note the following considerations when configuring trunks and trunk members:

- All ports in a trunk must have the same full-duplex speed.
- A port that is added to a trunk retains its VLAN configuration as a “shadow” configuration, meaning the port VLAN configuration is not active while the port is a member of the trunk. When the port is removed from the trunk, the port VLAN configuration becomes active.
- When ports are members of a trunk, they take on the STP configuration for the trunk. When ports are removed from a trunk, they take on their earlier configured STP states.

Click **Apply** to save any changes to the currently selected trunk. The changes take effect immediately.

EEE Configuration

The green features on the switch are Energy Efficient Ethernet (EEE) technologies, as defined by the IEEE 802.3az task force. These features are designed to reduce per-port power usage by shutting down ports when no link is present or when activity is low.

Global Configuration

Use the Global Configuration tile to enable or disable the Auto Port Power-Down and Low Power Idle (EEE) modes on the switch. Both features are enabled by default.

Figure 86. EEE Global Configuration Tile



Table 68. EEE Global Configuration Fields

Field	Description
Auto Port Power-Down	When this feature is enabled and the port link is down, the PHY automatically goes down for a short period of time. The port wakes up when it senses activity on the link. This feature enables saving power consumption when no link partner is present. This feature is enabled by default.

Field	Description
Low-Power Idle (EEE)	When this feature is enabled and there is not traffic on the port, the port enters a low-power mode, to reduce power consumption. The EEE feature works on ports in auto-negotiation mode, where the port is negotiated to either 100 Mbps full duplex, 1 Gbps (1000 Mbps) full duplex, 2.5Gbps (2500 Mbps) full duplex, or 10Gbps Copper interfaces. The EEE feature is enabled by default. **NOTE**: EEE is active only if port auto-negotiation mode is enabled.

Click **Apply** to save any changes for the current boot session. The changes take effect immediately but are not retained across a switch reset unless you click **Save**.

Global Status

When EEE is enabled, the Global Status tile shows the estimated power savings and power consumption information.

Figure 87. Global Status Tile



Table 69. Global Status Fields

Field	Description
Estimated Energy Savings	The estimated cumulative energy saved on the device (in watts x hours) due to the Energy Efficient Ethernet feature.
Estimated Power Savings	The estimated percentage of power conserved on all ports due to the Energy Efficient Ethernet feature. For example, 10% means that the device required 10% less power.
Current Power Consumption	The estimated power consumption by all ports.

Interface Status

This tile displays EEE status information for each interface.

Figure 88. Interface Status Tile

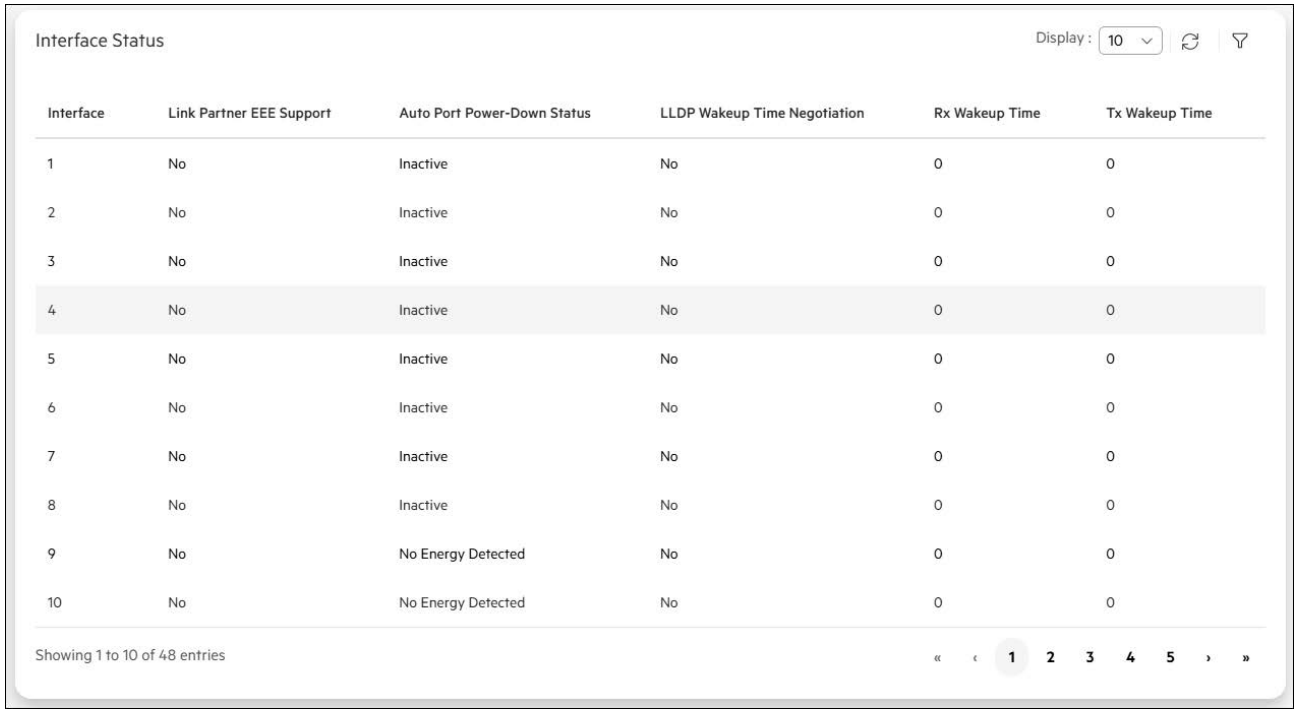


Table 70. Interface Status Fields

Field	Description
Interface	The interface ID.
Link Partner EEE Support	Displays Yes if the interface has received EEE messages (called Type-Length Values, or TLVs) from a link partner, or No if it has not.
Auto Port Power-Down Status	The current operational state of Auto Port Power-Down mode.
LLDP Wakeup Time Negotiation	Indicates whether the EEE wakeup time is negotiated with the link partner (Yes or No).
Rx Wakeup time	The Rx wakeup time in effect for the port, if negotiated by LLDP (otherwise, 0).
Tx Wakeup time	The Tx wakeup time in effect for the port, if negotiated by LLDP (otherwise, 0).

Device Tracking

The IP Device Tracking (IPDT) feature enables the network administrator to track IPv4 hosts that are attached to the physical and logical interfaces on the switch. The DHCP Snooping feature already provides mapping from a host IP address to the physical port on the switch for the IP address acquired via DHCP, but it can neither track the statically configured hosts nor can it detect the movement of the hosts in a VLAN. The IPDT feature snoops the Address Resolution Protocol (ARP) packets exchanged in a VLAN and populates the tracking table with the host information including its IP address, MAC address, VLAN, and Interface.

Device Tracking Global Configuration

Use the Device Tracking Global Configuration tile to configure Device Tracking settings that apply globally to the switch and to all interfaces.

Figure 89. Device Tracking Global Configuration Tile

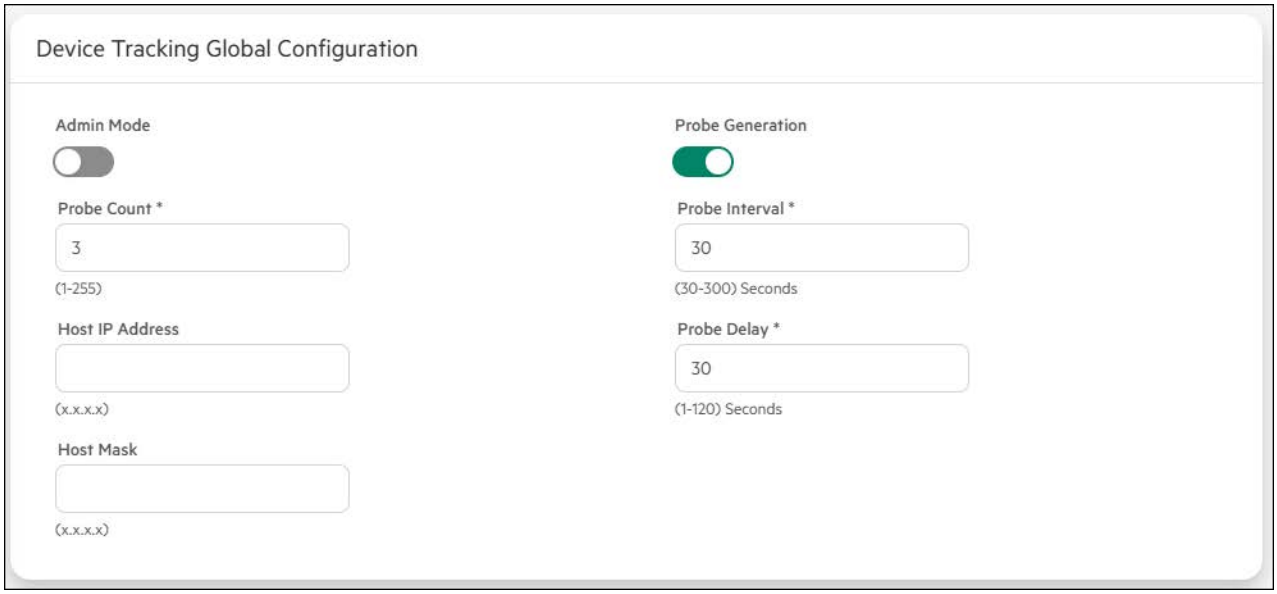


Table 71. Device Tracking Global Configuration Fields

Field	Description
Admin Mode	The administrative mode of the IPDT feature on the device. Disabling the administrative mode clears all the entries in the IPDT table.
Probe Generation	The ARP probe generation mode for the entries in the IPDT table. For each device entry in the IPDT table, an ARP probe is sent periodically to check the reachability of the device. If there are no ARP responses received for the configured number of retransmit ARP probes, the device entry is marked inactive.
Probe Count	The number of probes sent to the device, without any response from the device, before the device is declared as inactive in the IPDT table.
Probe Interval	The number of seconds IPDT should wait before sending an ARP probe to the device entries in the IPDT table.
Probe Delay	The number of seconds to delay sending the first ARP probe to the IPDT table entries, when the interface associated with the device entry moves from the non-forwarding state to the forwarding state.

Field	Description
Host IP Address / Mask	The source IP address and mask in the ARP probes generated by IPDT and sent to the device entries in the IPDT table on non-routing interfaces.

Device Tracking Summary

The Device Tracking Summary tile shows information about the device entries in the IPDT table that were learned on the IPDT enabled interfaces.

Figure 90. Device Tracking Summary Tile

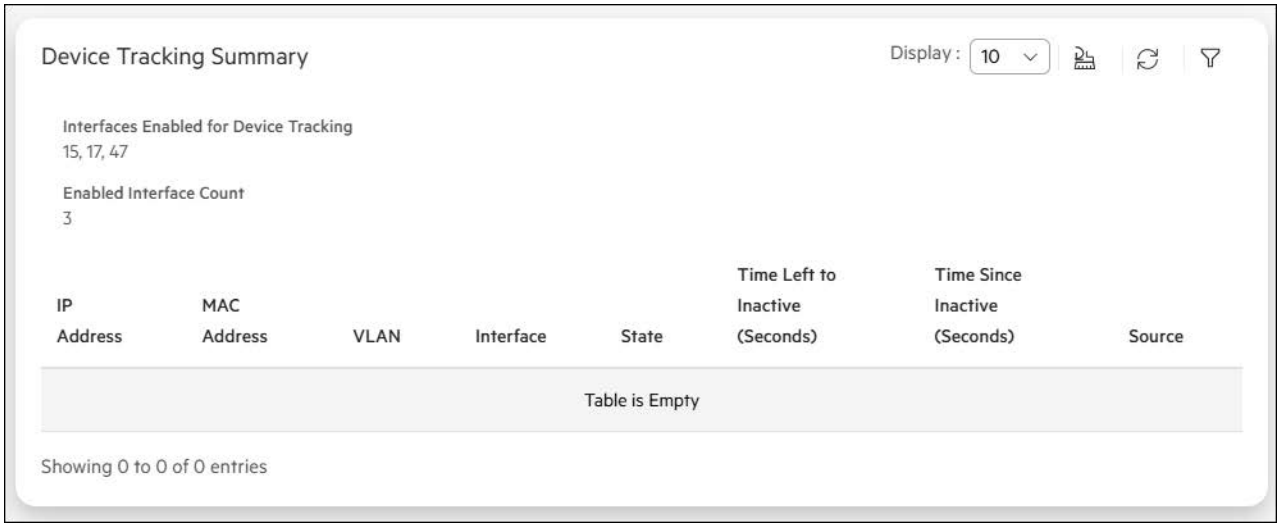


Table 72. Device Tracking Summary Fields

Field	Description
Interfaces Enabled for Device Tracking	The list of interfaces that are enabled for IPDT.
Enabled Interface Count	The total number of IPDT enabled interfaces.
IP Address	The learned IP address of the device.
MAC Address	The MAC address associated with the learned IP address of the device.
VLAN	The VLAN ID associated with the interface on which the device is learned.
Interface	The interface on which the device is learned.
State	The state of the learned device in the IPDT table, which can be one of the following: · Active—The device is reachable and responding to the ARP probes sent. · Inactive—The device is not reachable.
Time Left to Inactive	The number of seconds remaining before an active device in the IPDT table is marked inactive.
Time Since Inactive	The number of seconds elapsed since the inactive device in the IPDT table was last reachable.
Source	The source of the learned device in the IPDT table, which can be one of the following: · ARP—ARP snooping detected new devices. · DHCP—DHCP snooping detected DHCP client devices.

To remove all entries from the IPDT table, click (**Clear All**). The table is repopulated as new devices are learned by the IPDT feature.

Device Tracking Interface Configuration

Use the Device Tracking Interface Configuration tile to configure IPDT settings on specific interfaces. To configure the settings for one or more interfaces, select each entry to modify and click (**Edit**) and specify the maximum number of learned entries that can be added to the IPDT table. The same IPDT settings are applied to all selected interfaces.

Figure 91. Device Tracking Interface Configuration Tile

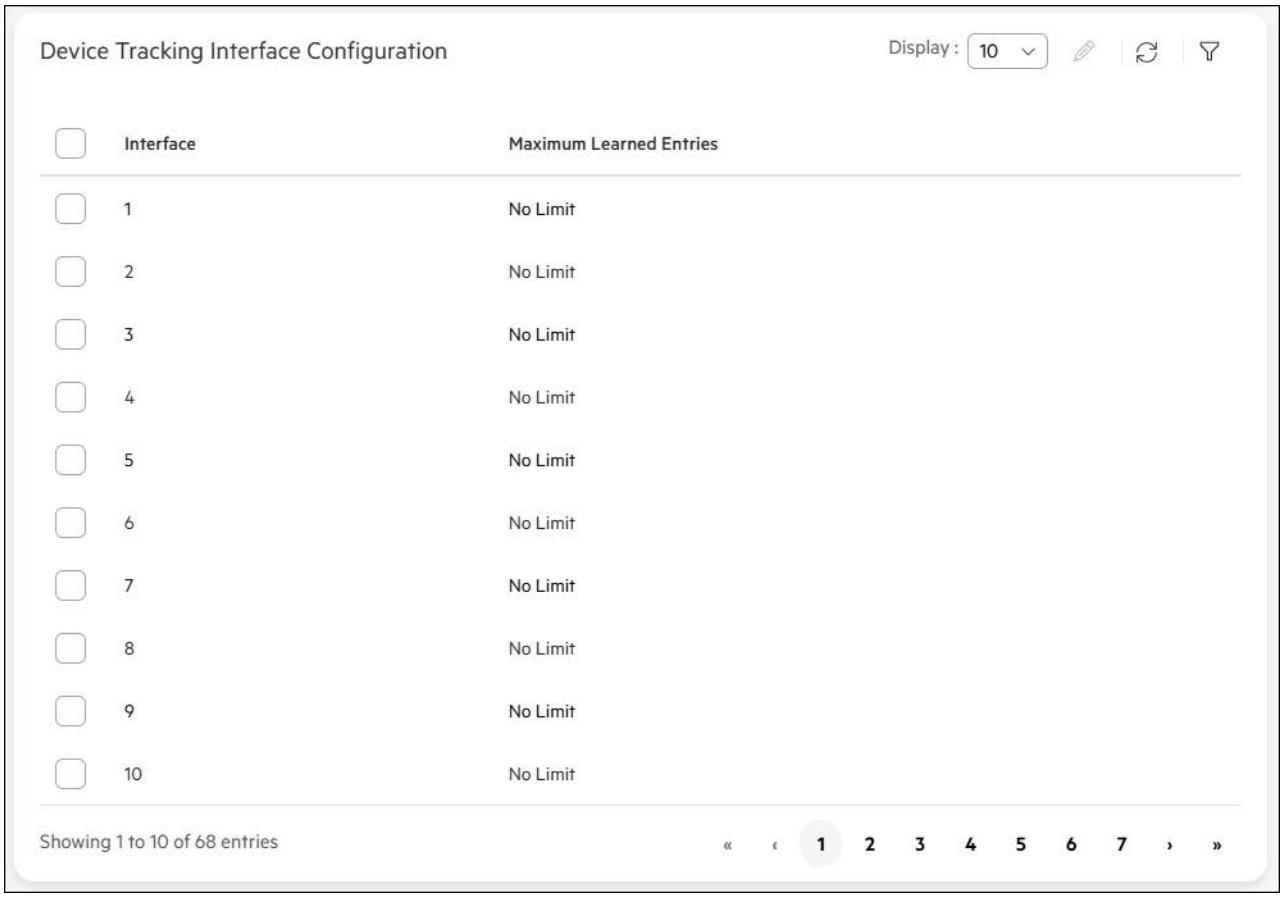


Table 73. Device Tracking Interface Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring IPDT settings, this field identifies the interface(s) that are being configured.
Maximum Learned Entries	The maximum number of learned entries that can be added to the IPDT table per interface. If the maximum limit configured on an interface is zero, then IPDT is effectively disabled on that interface. If the current number of entries learned on an interface is already more than the maximum limit configured on the interface, then all the entries associated with the interface are deleted from the IPDT table and ARP probes are sent again to the devices previously learned on that interface. By default, there is no limit on the number of entries that can be learned per interface.

Device Tracking Statistics

The Device Tracking Statistics tile displays information about the number and type of learned entries in the IPDT table.

Figure 92. Device Tracking Statistics Tile



Table 74. Device Tracking Statistics Fields

Field	Description
ARP Entries	The number of device entries learned by ARP snooping.
DHCP Entries	The number of client devices learned by DHCP snooping.
Active Entries	The number of device entries that are currently in an active state.
Inactive Entries	The number of device entries that are currently in an inactive state.
Total Entries	The total number of device entries in the IPDT table.

UDLD

The Unidirectional Link Detection (UDLD) feature detects unidirectional links on physical ports by exchanging packets containing information about neighboring devices. The purpose of the UDLD feature is to detect and avoid unidirectional links. A unidirectional link is a forwarding anomaly in a Layer 2 communication channel in which a bidirectional link stops passing traffic in one direction.

NOTE

The UDLD feature is not available on all models in the HPE Networking Instant On 1940 Switch Series.

UDLD Configuration

Use the UDLD Configuration tile to configure the global UDLD settings on the device.

Figure 93. UDLD Configuration Tile

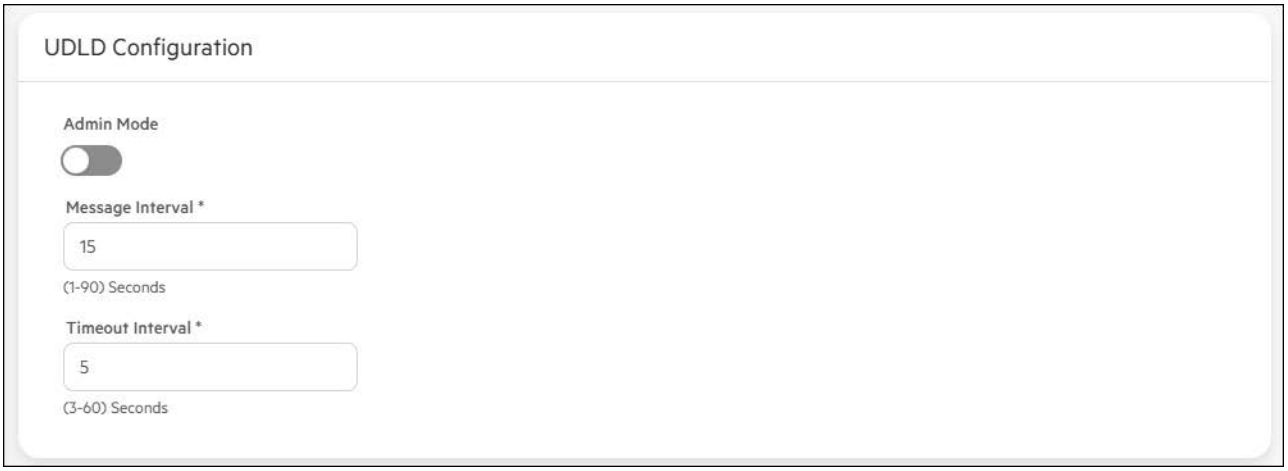


Table 75. UDLD Configuration Fields

Field	Description
Admin Mode	The administrative mode of UDLD on the device. UDLD must be administratively enabled on the device and on an interface for that interface to send UDLD messages. Additionally, UDLD must be enabled on the both sides of the link for the device to detect a unidirectional link.
Message Interval (Seconds)	The amount of time to wait between sending UDLD probe messages on ports that are in the advertisement phase.
Timeout Interval (Seconds)	The amount of time to wait to receive a UDLD message before considering the UDLD link to be unidirectional.

UDLD Interface Configuration

Use the UDLD Configuration tile to configure the per-port UDLD settings.

Figure 94. UDLD Interface Configuration Tile

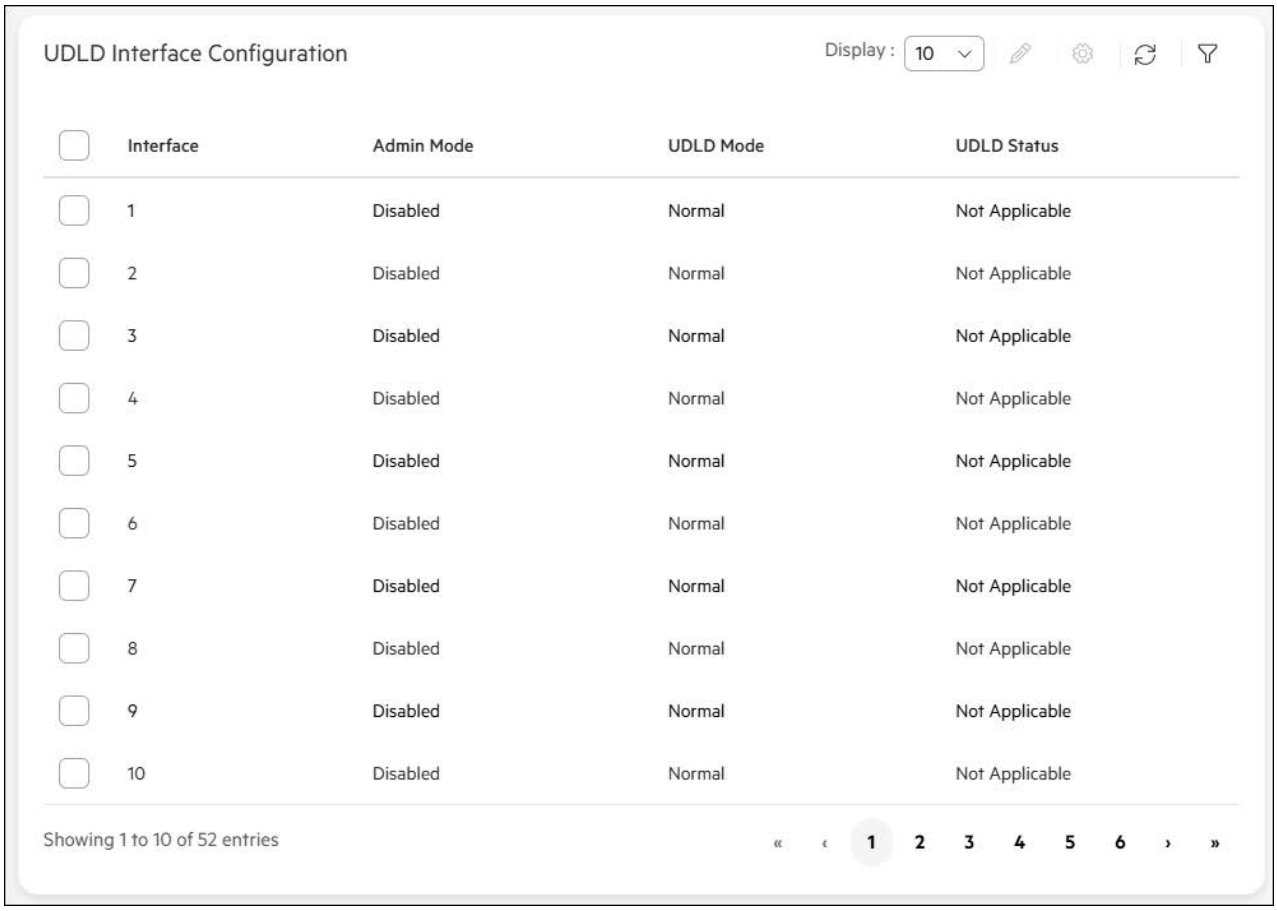


Table 76. UDLD Interface Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. In the Edit UDLD Interface Configuration window, this field identifies each interface that is being configured.
Admin Mode	The administrative mode of UDLD on the port.
UDLD Mode	The UDLD mode for the port, which is one of the following: · Normal—The state of the port is classified as Undetermined if an anomaly exists. An anomaly might be the absence of its own information in received UDLD messages or the failure to receive UDLD messages. An Undetermined state has no effect on the operation of the port. The port is not disabled and continues operating. When operating in UDLD normal mode, a port will be put into a disabled (Shutdown) state only in the following situations: o The UDLD PDU received from a partner does not have its own details (echo). o When there is a loopback, and information sent out on a port is received back exactly as it was sent. · Aggressive—The port is put into a disabled state for the same reasons that it occurs in normal mode. Additionally, a port in UDLD aggressive mode can be disabled if the port does not receive any UDLD echo packets even after bidirectional connection was established. If a bidirectional link is established, and packets suddenly stop coming from partner device, the UDLD aggressive-mode port assumes that link has become unidirectional.

Field	Description
UDLD Status	The UDLD status on the port, which is one of the following: · Not Applicable—The administrative status of UDLD is globally disabled or disabled on the interface. · Bidirectional—UDLD has detected a bidirectional link. · Shutdown—UDLD has detected a unidirectional link, and the port is in a disabled state. To clear the disabled state, click UDLD Port Reset. · Undetermined—UDLD has not collected enough information to determine the state of the port. · Unknown—The port link has physically gone down, but it is not because it was put in a disabled state by the UDLD feature.

To configure UDLD settings for one or more interfaces, select each interface to configure and click (**Edit**). The same settings are applied to all selected interfaces.

To reset all UDLD ports that have a UDLD Status of Shutdown, click (**UDLD Port Reset**). If the global and interface UDLD administrative mode is enabled and the port link is up, the port restarts the exchange of UDLD messages with its link partner. The UDLD port status is Shutdown if UDLD has detected an unidirectional link and has put the port in a disabled state.

Spanning Tree Protocol (STP) is a Layer 2 protocol that provides a tree topology for switches on a bridged LAN. STP allows a network to have redundant paths without the risk of network loops. STP uses the spanning-tree algorithm to provide a single path between end stations on a network. When STP is enabled, bridges on a network exchange bridge protocol data units (BPDUs) to communicate changes in the network topology and to provide information that helps determine the optimal paths between network segments.

HPE Networking Instant On 1940 Switch Series supports STP versions IEEE 802.1d (STP), 802.1w (Rapid STP, or RSTP) and 802.1s Multiple spanning tree (MSTP) with up to 8 instances. RSTP reduces the convergence time for network topology changes to about 3 to 5 seconds from the 30 seconds or more for the IEEE 802.1d STP standard. RSTP is intended as a complete replacement for STP, but can still inter-operate with switches running the STP protocol by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

Global Settings

To display the Spanning Tree Switch Global Settings page, click **Spanning Tree** in the navigation panel.

Global Configuration

Use the Global Configuration tile to set the global settings for STP.

Figure 95. STP Global Configuration Tile

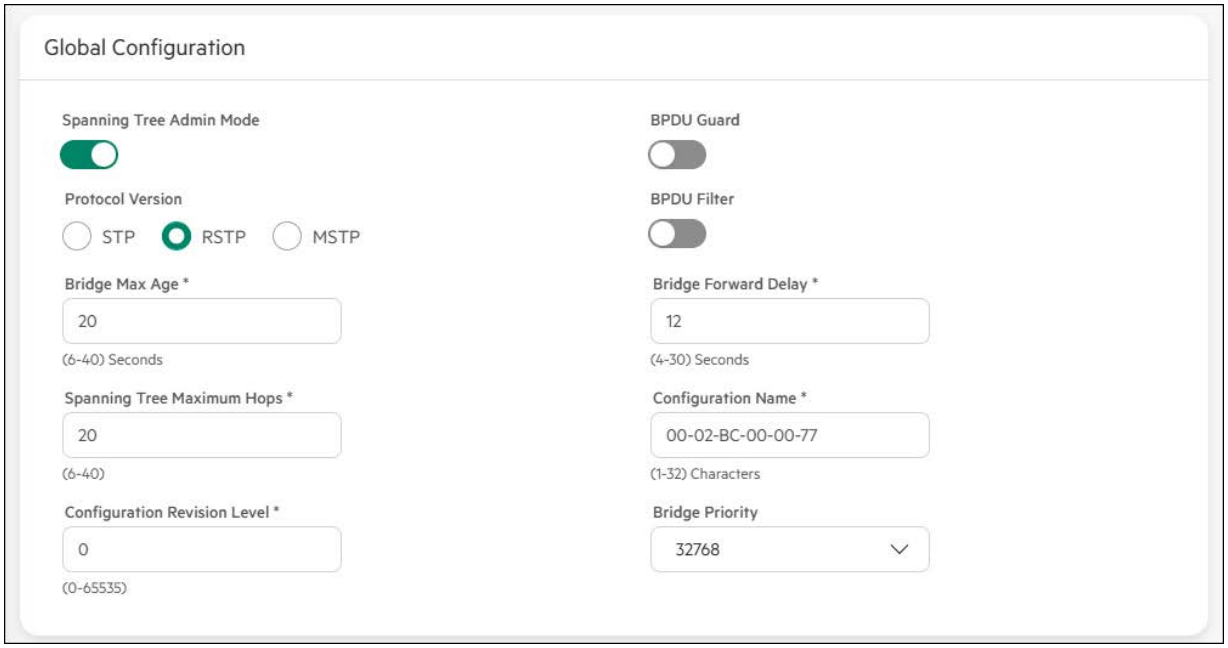


Table 77. STP Global Configuration Fields

Field	Description
Spanning Tree Admin Mode	The administrative mode of STP on the switch. When enabled, the switch participates in the root bridge election process and exchanges Bridge Protocol Data Units (BPDUs) with other switches in the spanning tree to determine the root path costs and maintain topology information. By default, Admin Mode is enabled.
Protocol Version	The STP version the device uses, which is one of the following: · STP (IEEE 802.1d)—Classic STP provides a single path between end stations, avoiding and eliminating loops. · RSTP (IEEE 802.1w)—Rapid Spanning Tree Protocol (RSTP) behaves like classic STP but also has 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 Notifications. This is the default protocol. · MSTP (IEEE 802.1s)—Multiple Spanning Tree Protocol (MSTP) includes all the advantages of RSTP and also supports multiple spanning tree instances to efficiently channel VLAN traffic over different interfaces. MSTP is compatible with both RSTP and STP.
Bridge Max Age	The amount of time a bridge waits before implementing a topological change. The default is 20 seconds. The valid range is 6-40 seconds.
Spanning Tree Maximum Hops	The maximum number of hops a Bridge Protocol Data Unit (BPDU) is allowed to traverse within the spanning tree region before it is discarded.
Configuration Revision Level	The revision number of the MSTP region. This number must be the same on all switches that participate in the MSTP region.
BPDU Guard	When enabled, BPDU Guard can disable edge ports that receive BPDU packets. This prevents a new device from entering the existing STP topology. Thus devices that were originally not a part of STP are not allowed to influence the STP topology.
BPDU Filter	When enabled, this feature filters the BPDU traffic on ports when spanning tree is disabled. When disabled, BPDU traffic is flooded on all ports.
Bridge Forward Delay	The amount of time a bridge remains in a listening and learning state before forwarding packets. The default is 15. The valid range is 4-30.
Configuration Name	The name of the MSTP region. Each switch that participates in the same MSTP region must share the same Configuration Name, Configuration Revision Level, and MST-to-VLAN mappings.
Bridge Priority	The value that helps determine which bridge in the spanning tree is elected as the root bridge during STP convergence. A lower value increases the probability that the bridge becomes the root bridge.

Global Settings

Use the Global Settings tile to view the global STP settings on the switch.

Figure 96. Global Settings Tile

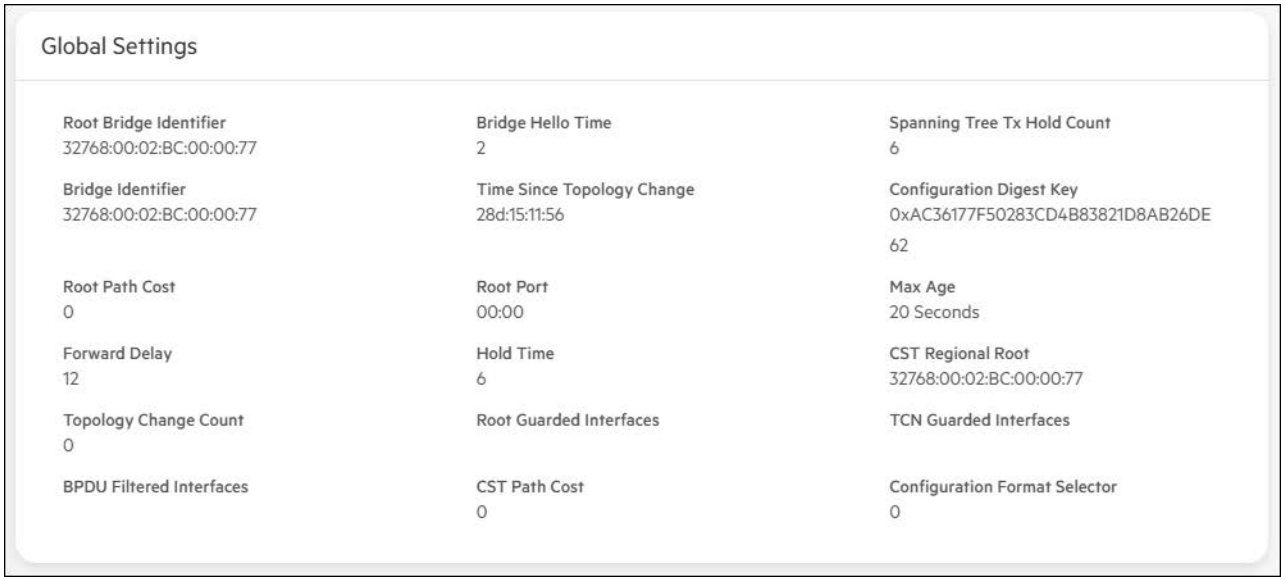


Table 78. Global Settings Fields

Field	Description
Root Bridge Identifier	The bridge identifier of the root bridge for the spanning tree. The identifier is made up of the bridge priority and the base MAC address. When electing the root bridge for the spanning tree, if the bridge priorities for multiple bridges are equal, the bridge with the lowest MAC address is elected as the root bridge.
Bridge Hello Time	The amount of time the root bridge waits between sending hello BPDUs.
Spanning Tree Tx Hold Count	The maximum number of BPDUs that a bridge is allowed to send within a hello time window.
Bridge Identifier	A unique value that is automatically generated based on the bridge priority value and the base MAC address of the bridge. When electing the root bridge for the spanning tree, if the bridge priorities for multiple bridges are equal, the bridge with the lowest MAC address is elected as the root bridge.
Time Since Topology Change	The amount of time that has passed since the topology of the spanning tree has changed since the switch was last reset.
Configuration Digest Key	The 16-byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID-to-MST ID mapping). Use this field to compare between devices and determine if they have the same MSTP global configuration.
Root Path Cost	The path cost to the designated root for the CST (Common Spanning Tree). Traffic from a connected switch to the root bridge takes the least-cost path to the bridge.
Root Port	The port on the bridge with the least-cost path to the designated root for the CST.
Max Age	The amount of time a bridge waits before implementing a topological change.
Forward Delay	The forward delay value for the root port bridge.
Hold Time	The minimum amount of time between transmissions of Configuration BPDUs.
CST Regional Root	The bridge identifier of the CST regional root. The identifier is made up of the priority value and the base MAC address of the regional root bridge.
Topology Change Count	The number of topology changes that occurred since last time the device reloaded.

Field	Description
Root Guarded Interfaces	A list of interfaces currently having the Root Guard parameter set.
TCN Guarded Interfaces	A list of interfaces currently having the TCN Guard parameter set.
BPDU Filtered Interfaces	A list of interfaces currently having the BPDU Filter parameter set.
CST Path Cost	The path cost to the CST (Common Spanning Tree) tree regional root.
Configuration Format Selector	The version of the configuration format being used in the exchange of BPDUs.

Spanning Tree Statistics

Use the Spanning Tree Statistics tile to view information about the number of bridge protocol data units (BPDUs) transmitted and received on each port.

To view the Spanning Tree Statistics tile, click **Spanning Tree > Global Settings** in the navigation pane, and scroll down to the Spanning Tree Statistics tile.

Figure 97. Spanning Tree Statistics Tile

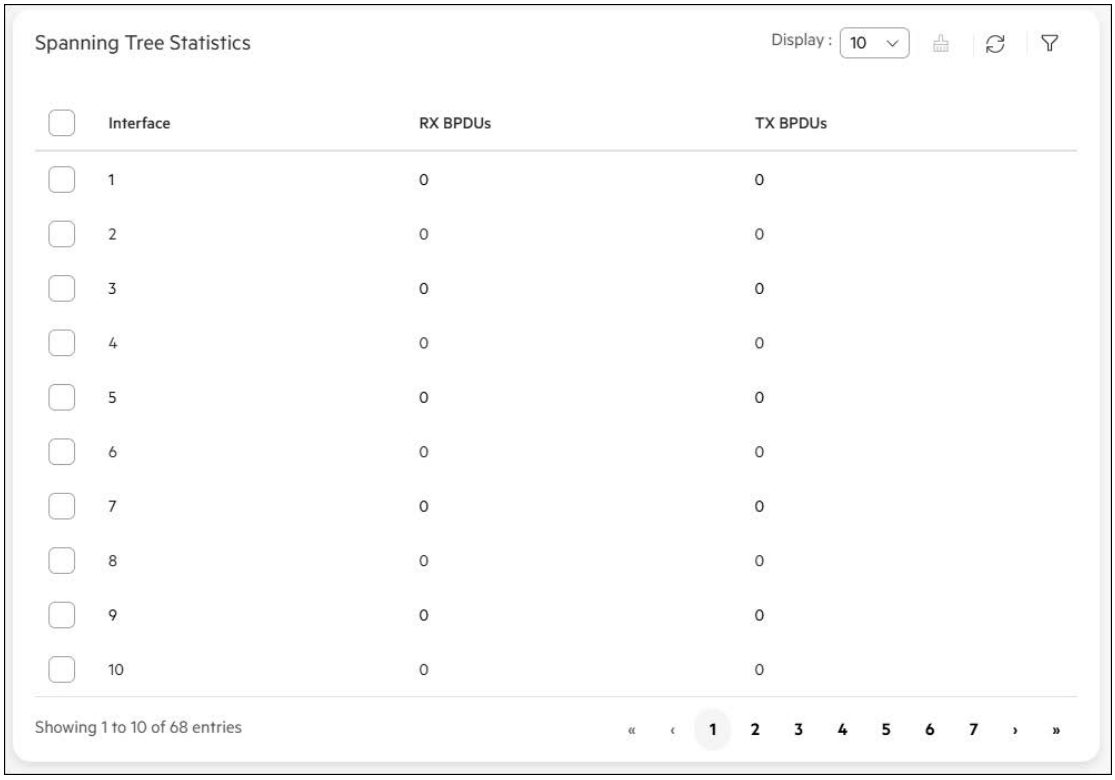


Table 79. Spanning Tree Statistics Fields

Field	Description
Interface	The port or trunk associated with the rest of the data in the row.
RX BPDUs	The Received BPDUs are the combined total of STP, RSTP BPDUs received by the interface.
TX BPDUs	The Transmitted BPDUs are the combined total of STP, RSTP BPDUs sent by the interface.

To clear the data in the Statistics table, click (**Clear All**).

To refresh the data shown in the Statistics table, click (**Refresh**).

To filter the data shown in the Statistics table, click (**Filter**). A filter box appears below the headers. you can select the interface that you want to view, or sort by the BPDU values (highest to lowest, or vice versa).

CST Configuration

Use the CST Configuration page to view and configure the Common Spanning Tree (CST) settings for each interface on the switch.

CST Port Configuration

To configure CST settings for an interface and to view additional information about the interface's role in the CST topology, select each interface to view or configure and click (**Edit**). The same settings are applied to all selected interfaces.

Figure 98. CST Port Configuration Tile

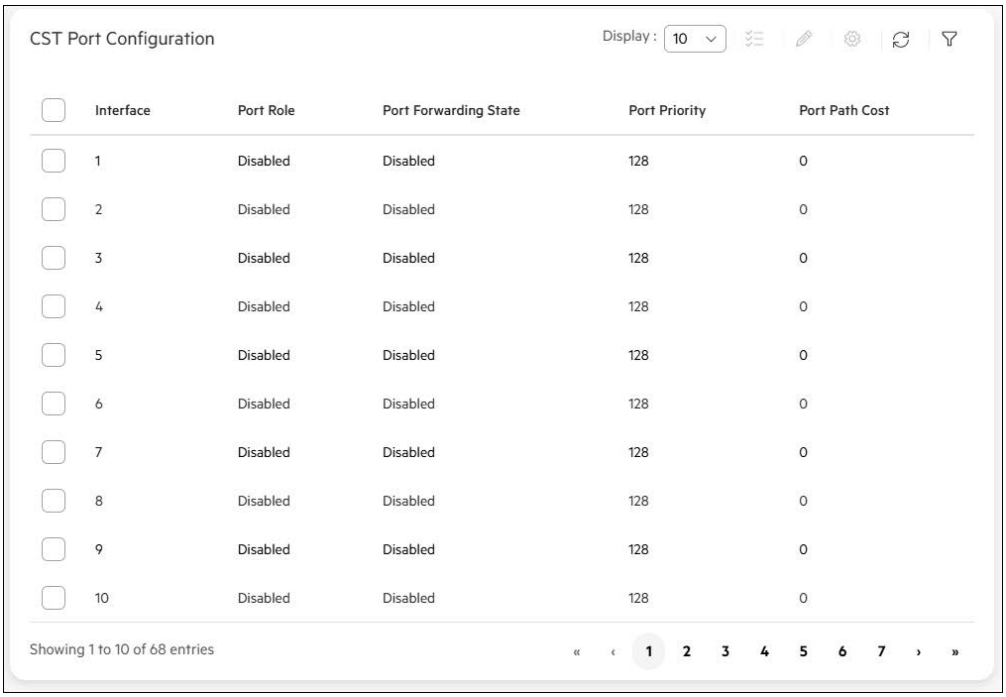


Table 80. CST Port Configuration Fields

Field	Description
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring CST settings for an interface, this field identifies the interface being configured.

Field	Description
Port Role	The role of the port within the CST, which is one of the following: · Root—A port on the non-root bridge that has the least-cost path to the root bridge. · Designated—A port that has the least-cost path to the root bridge on its segment. · Alternate—A blocked port that has an alternate path to the root bridge. · Backup—A blocked port that has a redundant path to the same network segment as another port on the bridge. · Master—The port on a bridge within an MST instance that links the MST instance to other STP regions. · Disabled—The port is physically down, or administratively disabled and is not part of the spanning tree.
Port Forwarding State	The traffic forwarding state of the port, which is one of the following: · Blocking—The port discards user traffic and receives, but does not send, BPDUs. During the election process, all ports are in the blocking state. The port is blocked to prevent network loops. · Listening—The port sends and receives BPDUs and evaluates information to provide a loop-free topology. This state occurs during network convergence and is the first state in transitioning to the forwarding state. · Learning—The port learns the MAC addresses of frames it receives and begins to populate the MAC address table. This state occurs during network convergence and is the second state in transitioning to the forwarding state. · Forwarding—The port sends and receives user traffic. · Disabled—The port is physically down, or administratively disabled and is not part of the spanning tree.
Port Priority	The priority for the port within the CST. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost from the assigned port to this port.

Additional Actions on CST Ports

The following actions are available when you select one or more CST Ports:

- View Details—Select a single port and click (**Details**) This option is available if you have a single port selected. For more information, see CST Port Details Fields.
- Edit CST Settings—Select one or more ports and click (**Edit**). The same settings are applied to all selected interfaces. For more information, see Edit CST Port Fields.
- Clear Detected Protocols—Select one or more ports and click (**Clear Detected Protocols**). Clicking this button restarts the STP migration process with the link partner. This forces STP mode renegotiation with the link partner.

Figure 99. Edit CST Port Settings Dialog Box

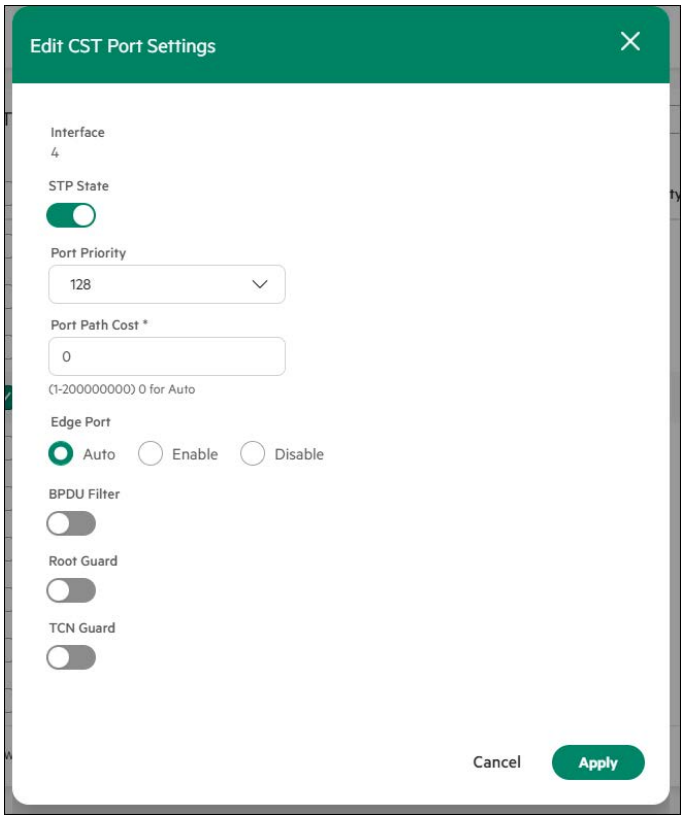


Table 81. Edit CST Port Configuration Fields

Field	Description
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring CST settings for an interface, this field identifies the interface being configured.
STP State	The port STP state. If enabled, the port will be part of the spanning tree topology. If disabled, the port will not participate in spanning tree topology. The default state is enabled.
Port Priority	The priority for the port within the CST. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost associated with this port. If set to 0 cost will be determined based on port speed (auto).
Edge Port	Indicates whether the interface is configured as an edge port the following settings are supported: · Auto—Enables edge port on switch, but only following a few seconds delay after port is up (this is the default) · Enable—Edge port is enabled on interface · Disable—Edge port is disabled on interface.
BPDU Filter	When enabled, this feature filters the BPDU traffic on the port, if STP is administratively disabled on the interface. This feature requires BPDU filtering to be enabled globally.
Root Guard	When enabled, Root Guard allows the interface to discard any superior information it receives to prevent the root bridge from changing. The port gets put into discarding state and does not forward any frames.
TCN Guard	When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.

To view additional information about an interface's role in the CST topology, select the interface to view, and then click (**Details**) This option is available only if you have a single port selected.

Figure 100. CST Port Details Dialog Box

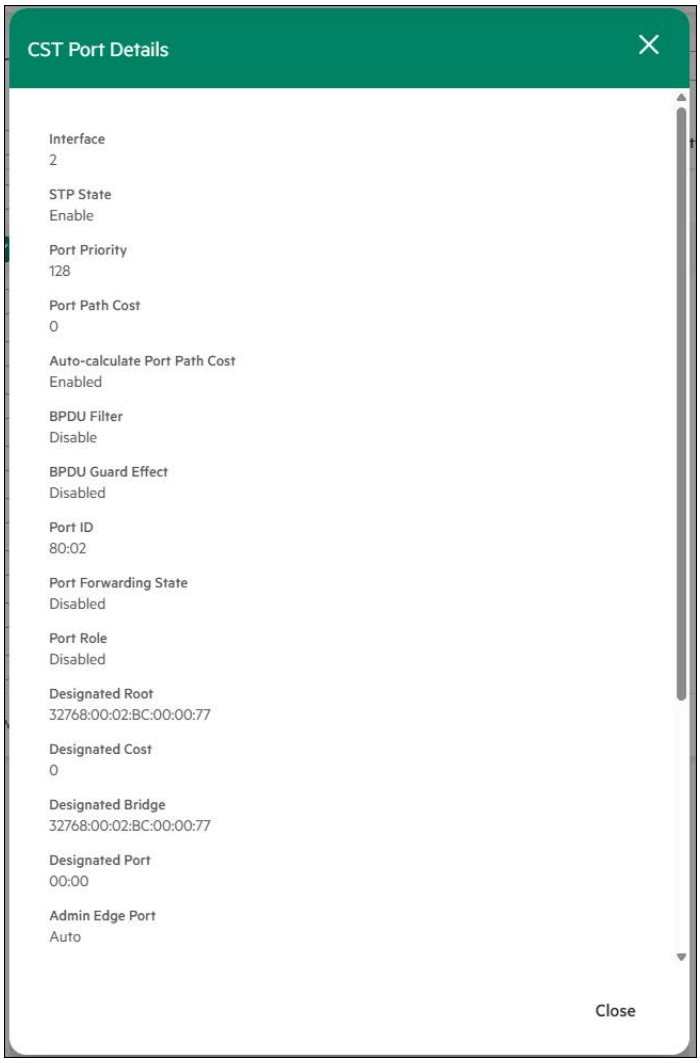


Table 82. CST Port Details Fields

Field	Description
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring CST settings for an interface, this field identifies the interface being configured.
STP State	The port STP state. If set to enabled, the port will be part of the spanning tree topology. If set to disable, the port will not participate in spanning tree topology. The default state is enabled.
Port Priority	The priority for the port within the CST. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost associated with this port. If set to 0 cost will be determined based on port speed (auto).
Auto-Calculate Port Path Cost	Shows whether the path cost from the port to the root bridge is automatically determined by the speed of the interface (Enabled) or configured manually (Disabled).

Field	Description
BPDU Filter	When enabled, this feature filters the BPDU traffic on the port, if STP is administratively disabled on interface. This feature requires BPDU filtering to be enabled globally.
BPDU Guard Effect	When enabled, BPDU Guard can disable edge ports that receive BPDU packets. This prevents a new switch from entering the existing STP topology. Thus devices that were originally not a part of STP are not allowed to influence the STP topology.
Port ID	A unique value that is automatically generated based on the port priority value and the interface index.
Port Forwarding State	The forwarding state of the selected port, which can be one of the following: · Blocking—The port discards user traffic and receives, but does not send, BPDUs. During the election process, all ports are in the blocking state. The port is blocked to prevent network loops. · Listening—The port sends and receives BPDUs and evaluates information to provide a loop-free topology. This state occurs during network convergence and is the first state in transitioning to the forwarding state. · Learning—The port learns the MAC addresses of frames it receives and begins to populate the MAC address table. This state occurs during network convergence and is the second state in transitioning to the forwarding state. · Forwarding—The port sends and receives user traffic. · Disabled—The port is physically down, or administratively disabled and is not part of the spanning tree.
Port Role	The role of the port within the CST, which is one of the following: · Root—A port on the non-root bridge that has the least-cost path to the root bridge. · Designated—A port that has the least-cost path to the root bridge on its segment. · Alternate—A blocked port that has an alternate path to the root bridge. · Backup—A blocked port that has a redundant path to the same network segment as another port on the bridge. · Master—The port on a bridge within an MST instance that links the MST instance to other STP regions. · Disabled—The port is physically down, or administratively disabled and is not part of the spanning tree.
Designated Root	The bridge ID of the root bridge for the CST.
Designated Cost	The path cost offered to the LAN by the designated port.
Designated Bridge	The bridge ID of the bridge with the designated port.
Designated Port	The port ID of the designated port.
Admin Edge Port	The edge port setting on port—Auto, Enabled or Disabled.
Edge Port	Indicates if edge port is Active or Inactive on the interface.
Point-to-point MAC	Indicates whether the link type for the interface is a point-to-point link.
Root Guard	When enabled, Root Guard allows the interface to discard any superior information it receives to prevent the root bridge from changing. The port gets put into discarding state and does not forward any frames.
TCN Guard	When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.
CST Regional Root	The bridge ID of the bridge that has been elected as the root bridge of the CST region.
CST Path Cost	The path cost from the interface to the CST regional root.

MSTP Configuration

Multiple Spanning Tree Protocol (MSTP) allows the creation of spanning tree instances based on a VLAN or groups of VLANs. Configuring spanning tree instances creates an active topology with a better distribution of network traffic and an increase in available bandwidth when compared to classic STP.

MSTP Configuration

Use the MSTP Configuration tile to create a new MSTP instance or to change the priority of or VLANs associated with an existing MSTP instance.

Figure 101. MST Configuration Tile

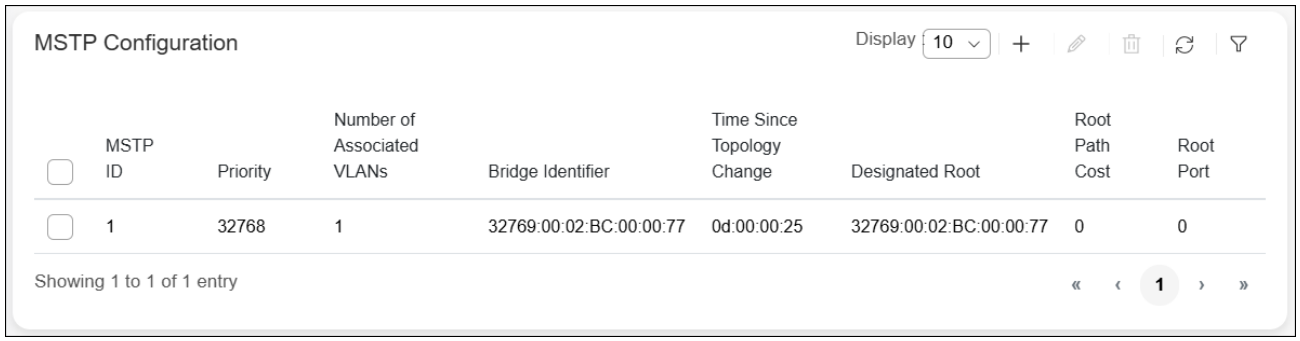


Table 83. MSTP Configuration Fields

Field	Description
MSTP ID	The number that identifies the MSTP instance.
Priority	The bridge priority for the spanning-tree instance. This value affects the likelihood that the bridge is selected as the root bridge. A lower value increases the probability that the bridge is selected as the root bridge.
Number of Associated VLANs	The number of VLANs that are mapped to the MSTI. This number does not contain any information about the VLAN IDs that are mapped to the instance.
Bridge Identifier	A unique value that is automatically generated based on the bridge priority value of the MSTI and the base MAC address of the bridge. When electing the root bridge for an MST instance, if the bridge priorities for multiple bridges are equal, the bridge with the lowest MAC address is elected as the root bridge.
Time Since Topology Change	The amount of time that has passed since the topology of the MSTI has changed.
Designated Root	The bridge identifier of the root bridge for the MST instance. The identifier is made up of the bridge priority and the base MAC address.
Root Path Cost	The path cost to the designated root for this MST instance. Traffic from a connected switch to the root bridge takes the least-cost path to the bridge. If the value is 0, the cost is automatically calculated based on port speed.
Root Port	The port on the bridge with the least-cost path to the designated root for the MST instance.

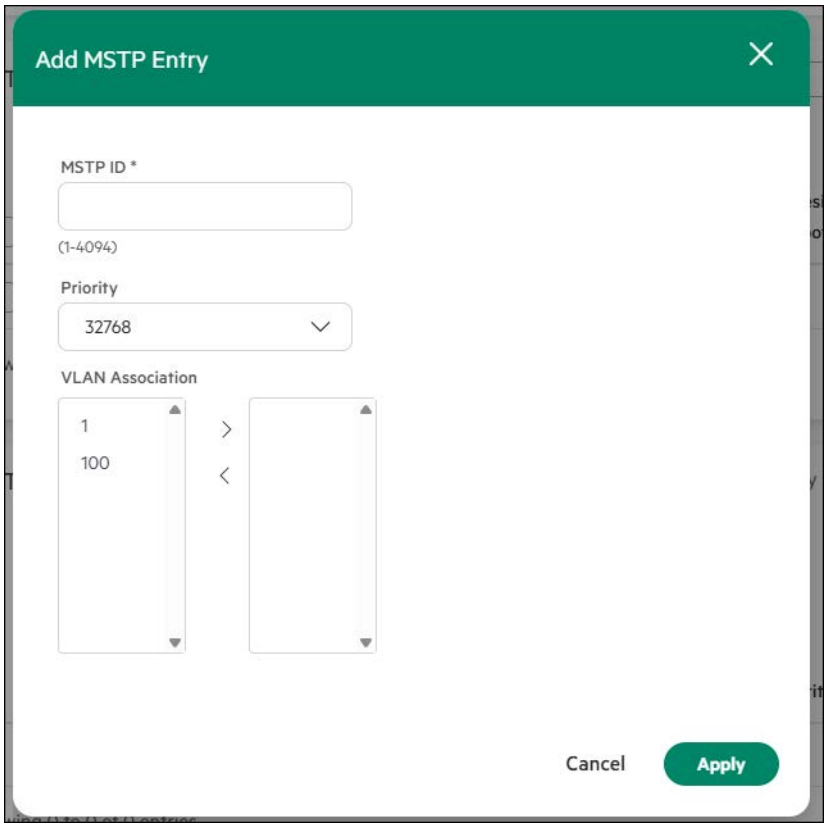
Adding, Editing or Removing an MSTP Configuration

To add an MSTP instance, click + (**Add)**.

To change the configuration for an MSTP instance, select the check box to the left of the entry and click (**Edit**).

To delete an MSTP instance, select the check box to the left of the entry and click (**Remove**).

Figure 102. Add MSTP Instance Dialog Box



MSTP Port Configuration

Use the MSTP Port Configuration tile to view details about the MSTP settings on a port or configure additional settings for one or more ports.

Figure 103. MSTP Port Configuration Tile

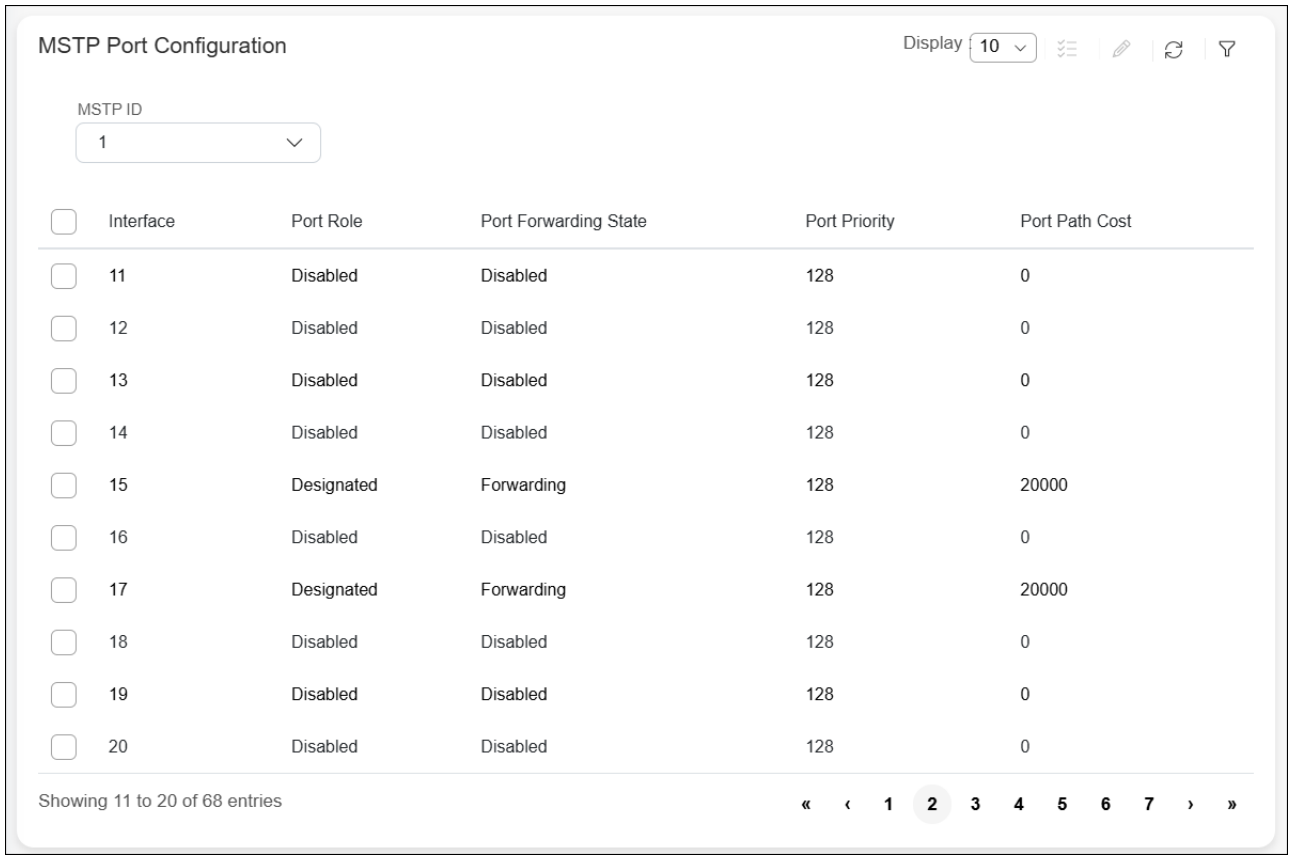


Table 84. MSTP Port Configuration Fields

Field	Description
MSTP ID	The menu contains the ID of each MST instance that has been created on the switch. The menu will display an instance only if there are port members in one of the VLANs mapped to this instance. Select a certain Instance ID to view and configure interface setting for that instance.
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring MST settings for an interface, this field identifies the interface being configured.
Port Role	The role of the port within the MST, which is one of the following: · Root—A port on the non-root bridge that has the least-cost path to the root bridge. · Designated—A port that has the least-cost path to the root bridge on its segment. · Alternate—A blocked port that has an alternate path to the root bridge. · Backup—A blocked port that has a redundant path to the same network segment as another port on the bridge. · Master—The port on a bridge within an MST instance that links the MST instance to other STP regions. · Disabled—The port is physically down, or administratively disabled and is not part of the spanning tree.

Field	Description
Port Forwarding State	The traffic forwarding state of the port, which is one of the following: · Blocking—The port discards user traffic and receives, but does not send, BPDUs. During the election process, all ports are in the blocking state. The port is blocked to prevent network loops. · Listening—The port sends and receives BPDUs and evaluates information to provide a loop-free topology. This state occurs during network convergence and is the first state in transitioning to the forwarding state. · Learning—The port learns the MAC addresses of frames it receives and begins to populate the MAC address table. This state occurs during network convergence and is the second state in transitioning to the forwarding state. · Forwarding—The port sends and receives user traffic. · Disabled—The port is physically down, or administratively disabled and is not part of the spanning tree.
Port Priority	The priority for the port within the MSTI. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost associated to this port, for this instance.

Editing MSTP Port Settings and Viewing MSTP Port Details

To configure MST settings for one or more interfaces, first select the appropriate MST instance from the MSTP ID menu. Then, select the interfaces to configure and click (**Edit**). The same settings are applied to all selected interfaces.

Figure 104. Edit MSTP Port Settings Dialog Box

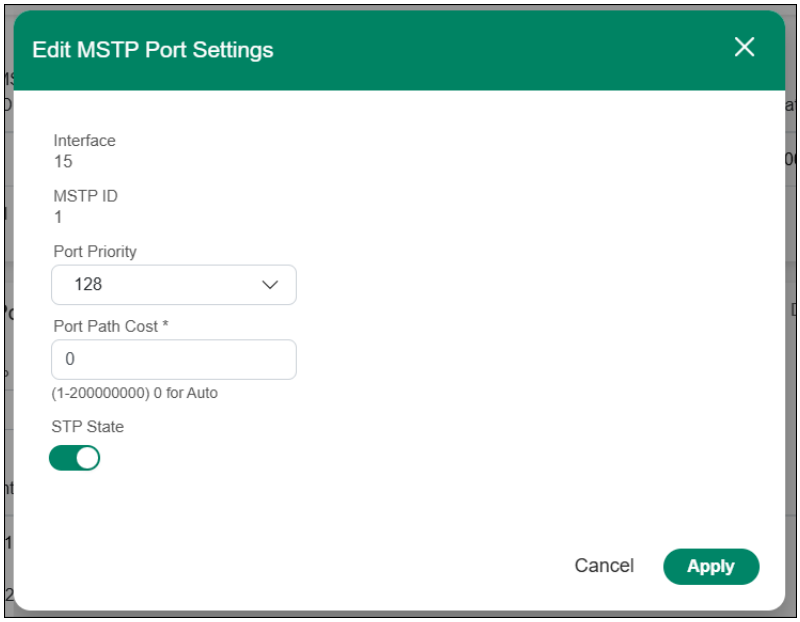


Table 85. Edit MSTP Port Settings Fields

Field	Description
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring CST settings for an interface, this field identifies the interface being configured.
MSTP ID	The ID of each MST instance this port is associated with.

Field	Description
Port Priority	The priority for the port within the MSTI. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost associated to this port within the MSTI.
STP State	Spanning tree state of this interface. Can be Enabled or Disabled, Disabled is the default.

If you modify any MSTP port settings, click **Apply** to save the changes for the current boot session. The changes take effect immediately but are not retained across a switch reset unless you click **Save**.

To view additional information about an interface's role in the MSTP topology, select the interface to view, and then click (**Details**). This option is available only if you have a single port selected.

Figure 105. MSTP Port Details Dialog Box

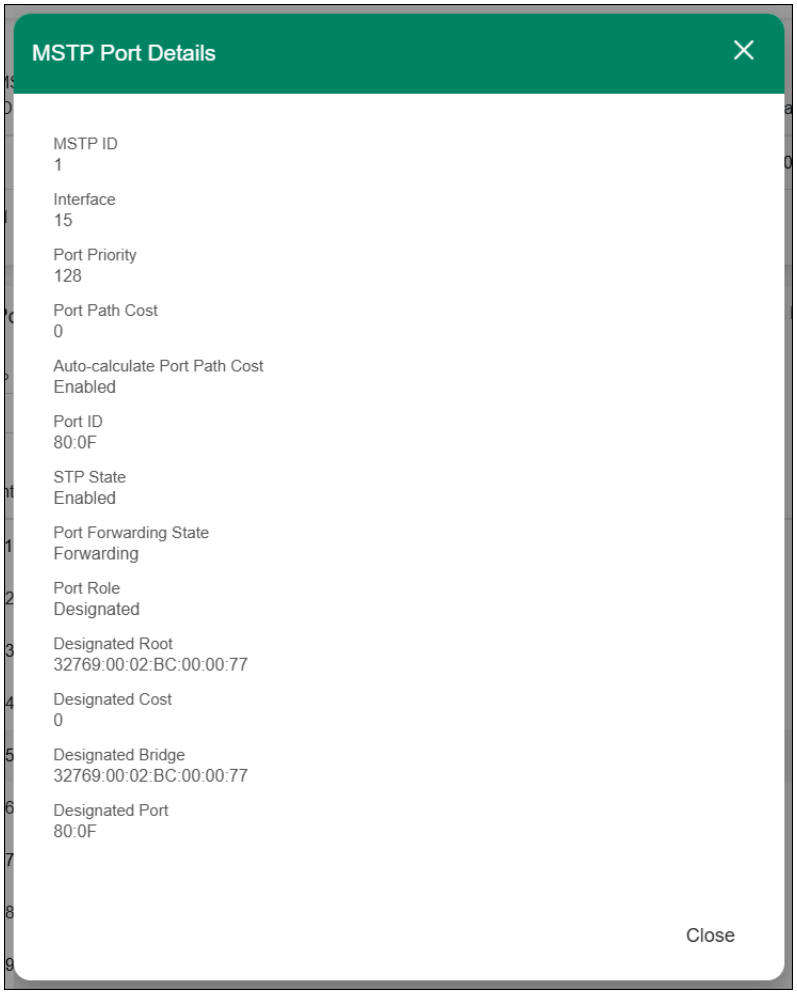


Table 86. MSTP Port Details Fields

Field	Description
MSTP ID	The ID of each MST instance this port is associated with.
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring CST settings for an interface, this field identifies the interface being configured.

Field	Description
Port Priority	The priority for the port within the MSTI. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost associated to this port within the MSTI.
Auto-Calculate Port Path Cost	Shows whether the path cost from the port to the root bridge is automatically determined by the speed of the interface (Enabled) or configured manually (Disabled).
Port ID	A unique value that is automatically generated based on the port priority value and the interface index.
STP State	Spanning tree state of this interface. Can be Enabled or Disabled, Disabled is the default.
Port Forwarding State	The forwarding state of the selected port, which can be one of the following: · Blocking—The port discards user traffic and receives, but does not send, BPDUs. During the election process, all ports are in the blocking state. The port is blocked to prevent network loops. · Listening—The port sends and receives BPDUs and evaluates information to provide a loop-free topology. This state occurs during network convergence and is the first state in transitioning to the forwarding state. · Learning—The port learns the MAC addresses of frames it receives and begins to populate the MAC address table. This state occurs during network convergence and is the second state in transitioning to the forwarding state. · Forwarding—The port sends and receives user traffic. · Disabled—The port is administratively disabled and is not part of the spanning tree.
Port Role	The role of the port within the MST, which is one of the following: · Root—A port on the non-root bridge that has the least-cost path to the root bridge. · Designated—A port that has the least-cost path to the root bridge on its segment. · Alternate—A blocked port that has an alternate path to the root bridge. · Backup—A blocked port that has a redundant path to the same network segment as another port on the bridge. · Master—The port on a bridge within an MST instance that links the MST instance to other STP regions. · Disabled—The port is administratively disabled and is not part of the spanning tree.
Designated Root	The bridge ID of the root bridge for the MST instance.
Designated Cost	The path cost offered to the LAN by the designated port.
Designated Bridge	The bridge ID of the bridge with the designated port.
Designated Port	The port ID of the designated port.

On a Layer 2 switch, Virtual LAN (VLAN) support offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header. Like a router, a VLAN switch partitions the network into logical segments. Partitioning the network provides better administration, security, and multicast traffic management.

A VLAN is a set of end stations and the switch ports that connect them. Many reasons exist for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

Each VLAN in a network has an associated VLAN ID, which is displayed in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station may omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet may either reject it or insert a tag using its default VLAN ID. A given port may handle traffic for more than one VLAN, but it can only support one default VLAN ID.

HPE Networking Instant On 1940 Switch Series supports up to 256 VLANs.

VLAN Configuration

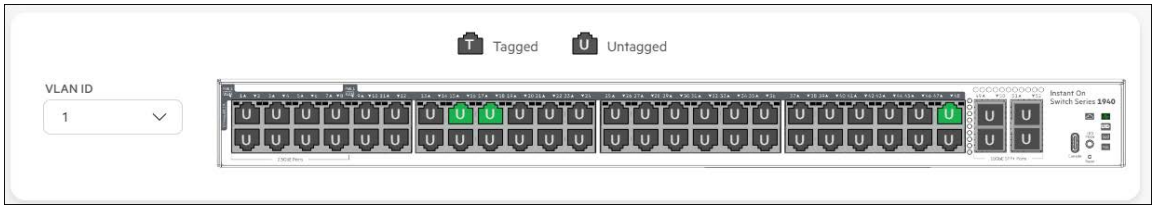
Use the VLAN Configuration page to view information about VLANs currently defined on the switch and to add and edit VLAN information.

Device View

The top of the VLAN Configuration page shows a graphical representation of the switch front panel. This panel view has a display of the ports, each with its current status.

Select the VLAN ID to view from the drop-down on the left side of the display.

Figure 106. VLAN Switch Panel View



The VLAN Switch Panel View shows the tagging behavior for each port in this VLAN:

- Tagged-The port is a tagged member of the selected VLAN. When frames in this VLAN are for-warded on this port, the VLAN ID will be included in the frame's Ethernet header.
- Untagged-The port is an untagged member of the selected VLAN. When frames in this VLAN are forwarded on this port, the VLAN ID will not be included in the frame's Ethernet header.

If there is no indication, this means that the port is not a member of a VLAN. For more information, see Device View.

Click on a port to open the **Edit VLAN Membership** dialog box. The content of the dialog depends on the currently active VLAN Membership tab.

VLAN Configuration

Use the VLAN Configuration tile to create new VLANs on the switch and edit or delete existing VLANs.

By default, VLAN 1 is defined on the switch and designated as the default VLAN. VLAN 1 cannot be modified or deleted. All ports are members of VLAN 1 by default.

VLAN 1 is also the default management VLAN, which identifies the VLAN that management users must be a member of. The administrator can configure a different VLAN as the management VLAN.

Figure 107. VLAN Configuration Tile

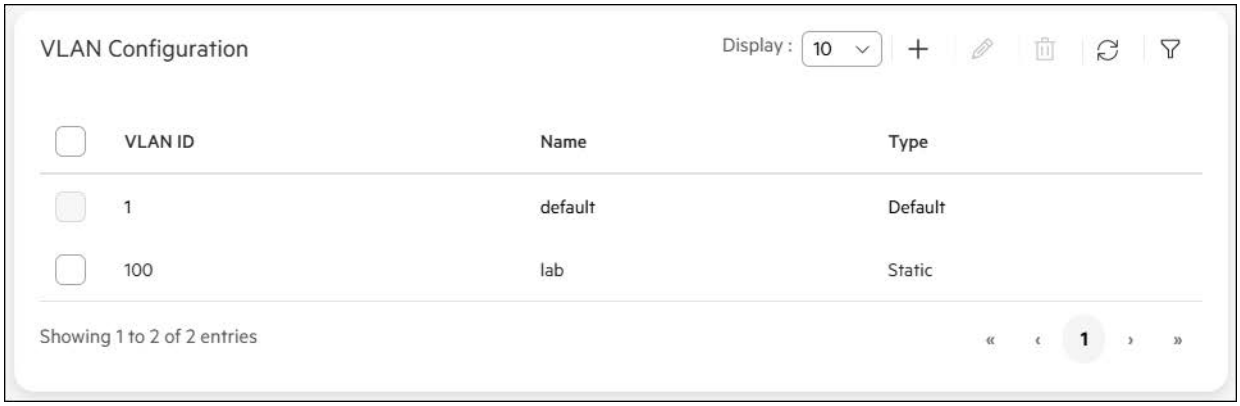


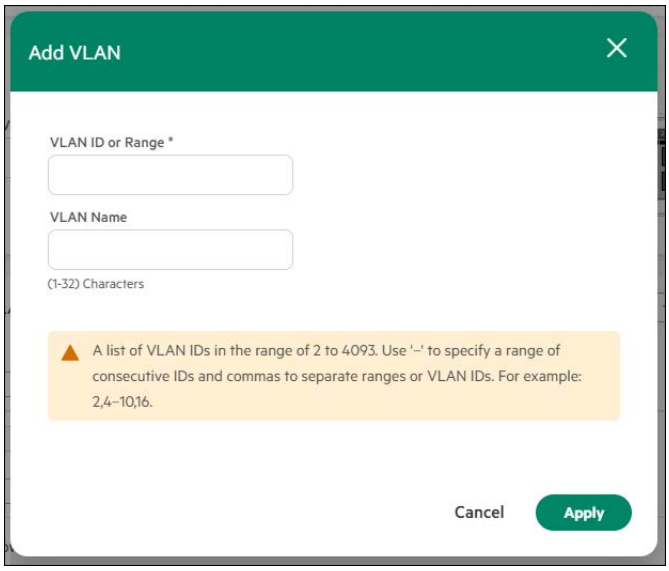
Table 87. VLAN Configuration Fields

Field	Description
VLAN ID	The numerical VLAN identifier (VID) assigned to the VLAN, from 1 to 4092. **Note:** VLAN 0 (VID = 0x000 in a frame) is reserved and is used to indicate that the frame does not belong to any VLAN. In this case, the 802.1Q tag specifies only a priority and the value is referred to as a priority tag.
Name	A user-configurable name that identifies the VLAN.
Type	The type of VLAN, which can be one of the following: · Default—The default VLAN. This VLAN is always present, and the VLAN ID is 1. · RADIUS—A VLAN created by a RADIUS VLAN assignment. · Static—A user-configured VLAN.

Adding, Editing, and Removing VLANs

To add a VLAN, click ＋ (**Add**).

Figure 108. Add VLAN Dialog Box



In the VLAN ID or Range field, specify one or more VLAN IDs in the range 2 to 4092.

NOTE

VLAN 4093 and 4094 are reserved for internal system use.

To create a range of VLANs, specify the beginning and ending VLAN IDs, separated by a dash. Option-ally you can define a name for the VLAN in the VLAN Name field.

To create multiple non-sequential VLANs, separate each VLAN ID with a comma. You can create up to 256 VLANs.

After entering the VLAN IDs, ranges, or both, click **Apply**.

To change the name of a VLAN, click (**Edit**), specify the new name, and click **Apply**.

To remove one or more VLANs, select the check box associated with each VLAN to delete and click (**Remove**).

VLAN Membership

By default, all ports and trunks are assigned membership in the default VLAN (VLAN 1). If you create additional VLANs, you can add interfaces as members of the new VLANs and configure VLAN tagging settings for the interfaces. You can also modify interface memberships in VLAN 1.

This tile has two tabs:

- VLAN Membership - By Interface—This tab is for configuring the interface to VLAN membership for one or more VLANs.
- VLAN Membership - By VLAN—This tab is for configuring VLAN membership participation for one or more interfaces.

VLAN Membership - By Interface Tab

Use the VLAN Membership - By Interface tab to view the tagging behavior of each interface in the VLAN.

Figure 109. VLAN Membership - By Interface Tab

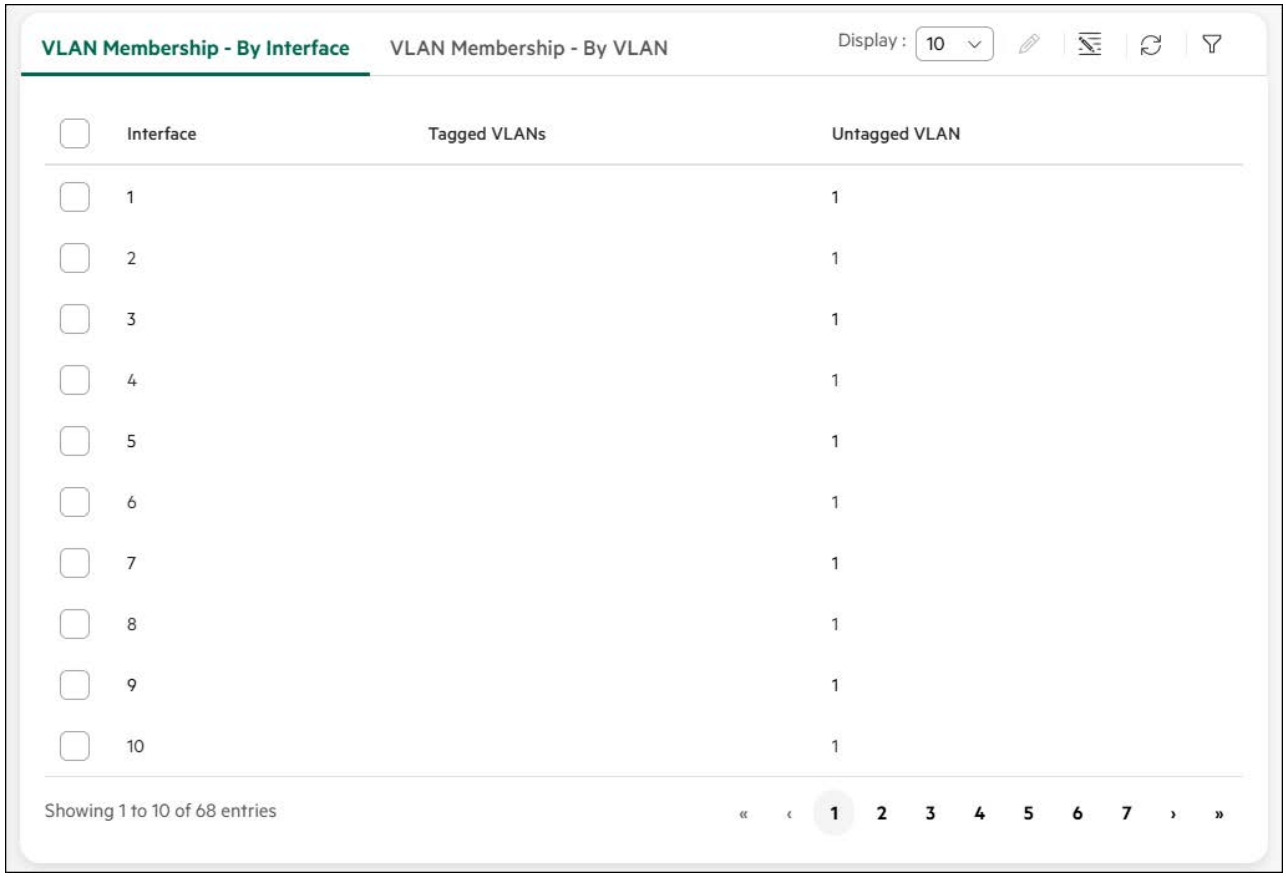


Table 88. VLAN Membership - By Interface Fields

Field	Description
Interface	The port or trunk ID.
Tagged VLANs	The port is a tagged member of the specified VLAN(s). When frames in these VLANs are forwarded on this port, the VLAN ID will be included in the frame's Ethernet header.
Untagged VLAN	The port is an untagged member of the specified VLAN. When frames in this VLAN are forwarded on this port, the VLAN ID will not be included in the frame's Ethernet header.

To configure VLAN membership by interface, select the check the box to the left of one or more ports and click (**Edit**). To configure all ports at the same time with the same settings, click (**Edit All**).

VLAN Membership - By VLAN Tab

Use the VLAN Membership - By VLAN tab to configure the participation mode of each interface in the VLAN.

To configure VLAN Membership - By VLAN, select the VLAN to configure from the VLAN ID drop-down, then select one or more interfaces and click (**Edit**). To configure all ports at the same time with the same settings, click (**Edit All**).

Figure 110. VLAN Membership - By VLAN Tab

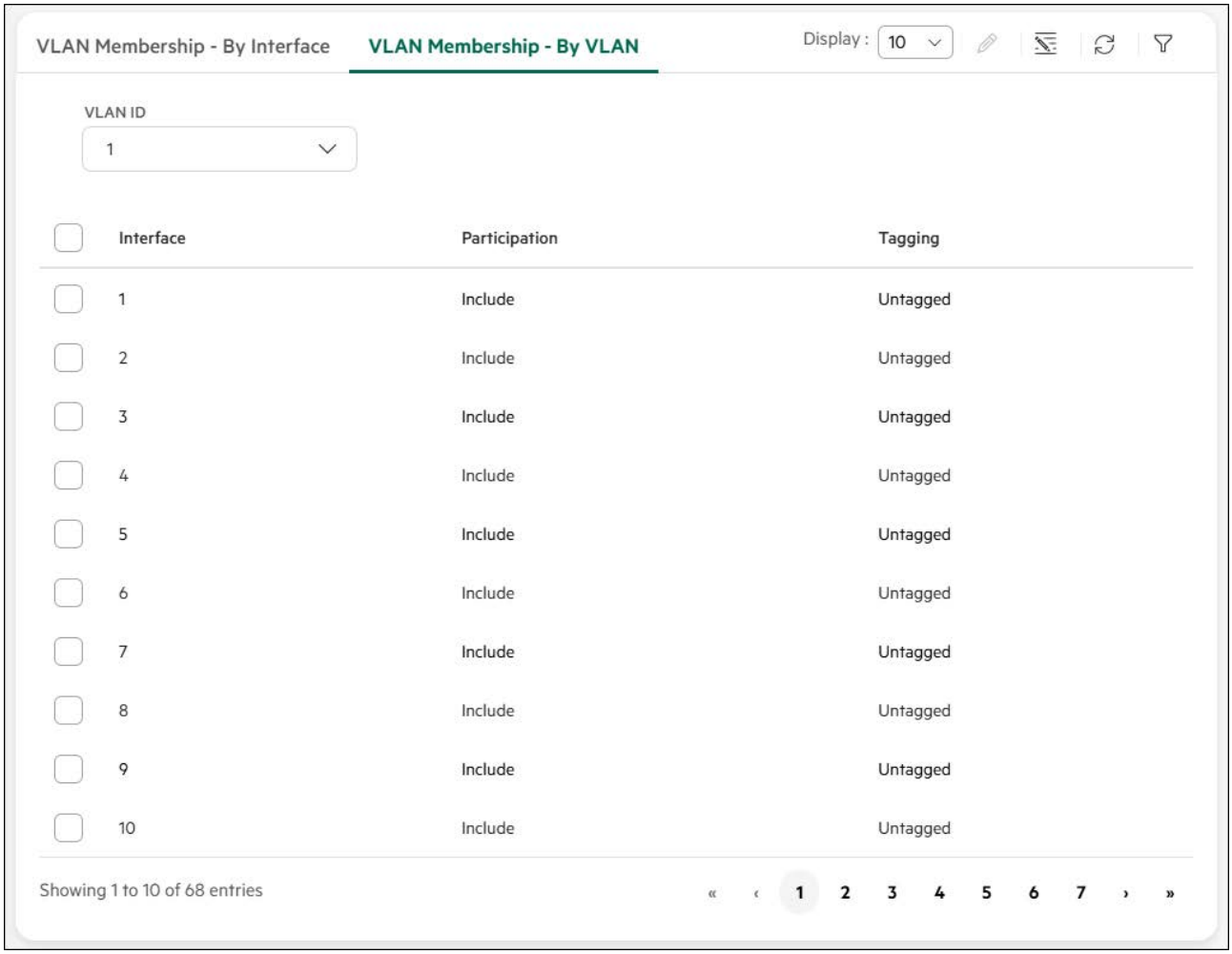


Table 89. VLAN Membership - By VLAN Fields

Field	Description
VLAN ID	Select the VLAN ID for which you want to view interface memberships.
Interface	The port or trunk ID.

Field	Description
Participation	The participation mode of the interface in the selected VLAN, which is one of the following: · Included—The port is a member of the selected VLAN. This mode is also equivalent to registration fixed in the IEEE 802.1Q standard. · Excluded—The port is not a member of the selected VLAN. This mode is also equivalent to registration forbidden in the IEEE 802.1Q standard.
Tagging	The tagging behavior for each port in this VLAN, which is one of the following: · Tagged—The port is a tagged member of the selected VLAN. When frames in this VLAN are forwarded on this port, the VLAN ID will be included in the frame's Ethernet header. · Untagged—The port is an untagged member of the selected VLAN. When frames in this VLAN are forwarded on this port, the VLAN ID will not be included in the frame's Ethernet header.

On the Edit VLAN Membership screen, configure the Participation and Tagging settings to specify whether the ports are excluded from the VLAN or are included as a tagged or untagged member.

Consider the following guidelines when editing VLAN port memberships and settings:

- A port can be an untagged member of only one VLAN.
- If you change the VLAN that a port is an untagged member of, then the port will be excluded from the VLAN where it was previously an untagged member.
- A port can be a tagged member of multiple VLANs.
- Every port must be a member of at least one VLAN, as either a tagged or an untagged member.
- You cannot exclude a port from a VLAN unless the port is a member of at least one other VLAN.
- If you exclude a port from the management VLAN, a computer connected to the switch through that port will be unable to access the switch management interface.
- Ports belonging to a trunk cannot be assigned membership in a VLAN, although the trunk itself can be a member of one or more VLANs. If VLAN configuration was applied to such a port before it was assigned to a trunk, this VLAN configuration will be retained as an inactive configuration and will not be displayed. When the port is removed from the trunk, the VLAN configuration will become active.

VLAN Interface Configuration

Use the VLAN Interface Configuration tile to configure the way interfaces handle VLAN-tagged, priority-tagged, and untagged traffic.

Figure 111. VLAN Interface Configuration Tile

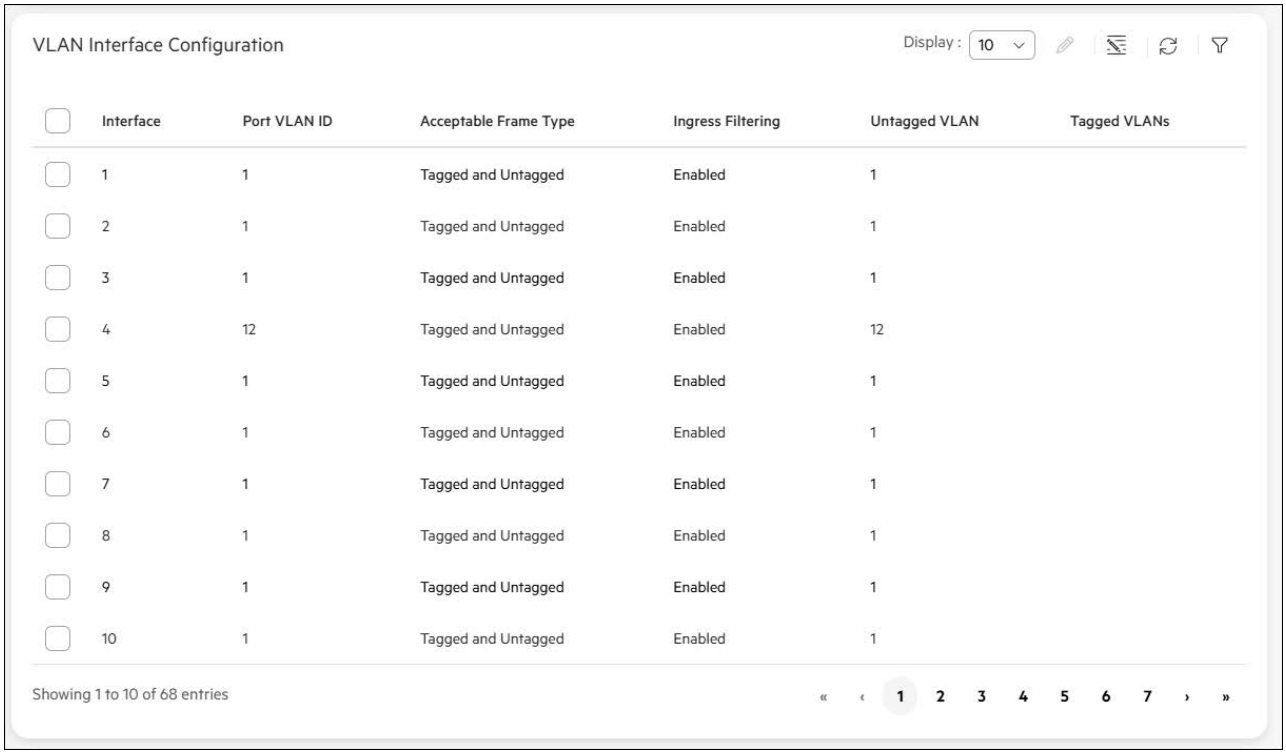


Table 90. VLAN Interface Configuration Fields

Field	Description
Interface	Identifies the physical interface or LAG associated with the rest of the data in the row.
Port VLAN ID	The VLAN ID assigned to untagged or priority-tagged frames received on this port. This value is also known as the Port VLAN ID (PVID). In a tagged frame, the VLAN is identified by the VLAN ID in the tag.
Acceptable Frame Type	Indicates how the interface handles untagged and priority-tagged frames: · All: Untagged, priority tagged and tagged frames received on the interface are accepted and assigned the value of the Port VLAN ID for this interface. · Tagged Only: The interface discards any untagged or priority-tagged frames it receives. · Untagged Only: The interface discards any tagged frames it receives. For all options, VLAN-tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN standard.
Ingress Filtering	Shows how the port handles tagged frames: · Enabled: A tagged frame is discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. This is the default setting · Disabled: All tagged frames are accepted.
Untagged VLAN	VLAN that is configured on the port to transmit egress packets as untagged.
Tagged VLANs	VLANs that are configured on the port to transmit egress packets as tagged.

To modify the VLAN interface settings, select the check the box next to the interfaces to configure and click (**Edit**). To configure all interfaces at the same time with the same settings, click (**Edit All**).

Voice VLAN Configuration

Use the Voice VLAN Configuration page to configure the global administrative mode of the Voice VLAN feature as well as the per-port settings. When Voice VLAN is configured on a port that receives both voice and data traffic, it can help ensure that the voice traffic has priority.

The switch supports OUI-based Voice VLAN with the ability to dynamically detect voice traffic based on telephony OUIs.

The switch also supports protocol-based Voice VLAN with the ability to process SIP, H.323, and SCCP protocol packets, set up a session, and prioritize the voice traffic for that session.

The voice VLAN ID must be manually configured through the switch's web interface and ports must be enabled to participate in the voice VLAN.

When the switch receives a packet with a source MAC address matching one of the configured telephony OUIs, the port is dynamically placed in the voice VLAN.

When the switch receives voice protocol packets in this VLAN, the call is set up and the call traffic gets prioritized.

The switch supports up to 32 OUIs. You can manually add or remove OUIs. The switch also supports predefined OUIs that exist on the switch by default. If the switch is reset to factory defaults, only the predefined OUIs are available.

These are the predefined OUIs:

- SIEMENS (00-01-e3)
- CISCO1 (00-03-6b)
- AVAYA3 (00-09-6e)
- H3C (00-0f-e2)
- NITSUKO (00-60-b9)
- SNOM (00-04-13)
- POLYCOM (64-16-7f)
- YEALINK (80-5E-0c)

To display the Voice VLAN Configuration page, click **VLAN > Voice VLAN Configuration** in the navigation pane.

Global Configuration

Use the options on the Global Configuration tile to control the Voice VLAN settings that apply to the switch and all interfaces that are enabled for Voice VLAN.

Figure 112. Voice VLAN Global Configuration Tile

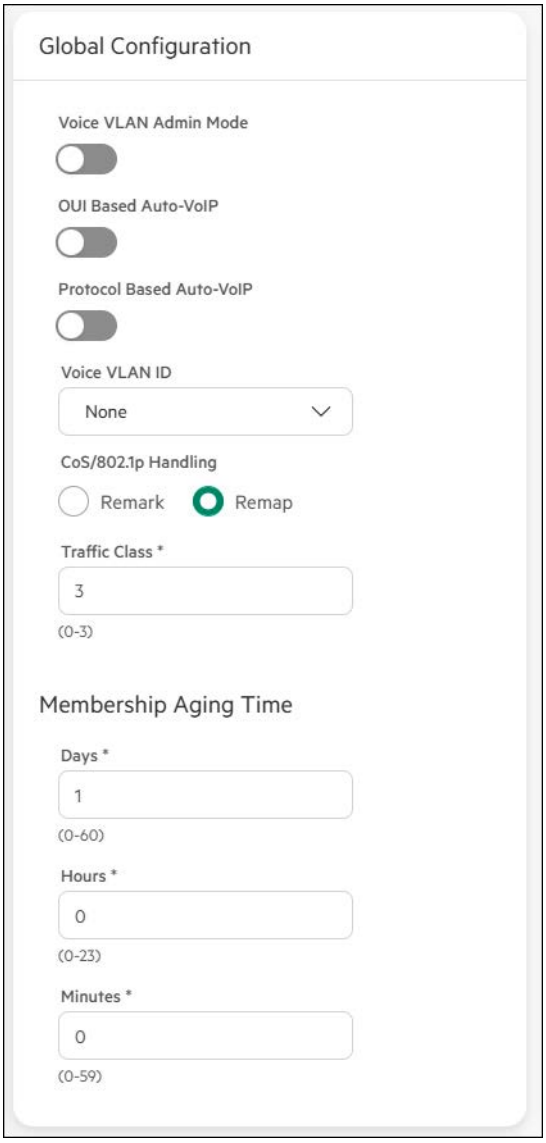


Table 91. Voice VLAN Global Configuration Fields

Field	Description
Voice VLAN Admin Mode	Set as Enabled to globally enable Voice VLAN operation. The Voice VLAN still needs to be enabled on the interface that requires the voice VLAN operation.
OUI Based Auto-VoIP	Enables automatic Voice over IP (VoIP) configuration based on OUI of connected devices. When enabled globally, the system recognizes VoIP devices by their OUI and applies optimized QoS settings automatically to prioritize voice traffic.
Protocol Based Auto-VoIP	Enables automatic detection and prioritization of Voice over IP (VoIP) traffic based on recognized signaling protocols (e.g., SIP, H.323). When enabled, the system identifies VoIP streams by protocol type and applies QoS policies to ensure optimal voice performance.

Field	Description
Voice VLAN ID	The VLAN used to separate VoIP traffic from other non-voice traffic. All VoIP traffic that matches a value in the known OUI list gets assigned to this VoIP VLAN. This VLAN ID information is advertised in the LLDP-MED messages. Voice devices sending traffic with this VLAN gets a defined priority over the data traffic. Remap and Remark settings are not applicable for this traffic. They are only applicable for Auto-VoIP.
CoS/802.1p Handling	Define the Class of Service (CoS) setting for the voice traffic received on enabled interfaces: · Remap—Remap incoming voice traffic to the CoS specified in the "Traffic Class" field. · Remark—Remap and remark the L2 field of incoming voice traffic to the CoS specified in the "Priority" field. Any changes are not applied to ongoing traffic.
Priority	Sets the priority value when the CoS/802.1p is set to Remark.
Traffic Class	Sets the Traffic Class value when the CoS/802.1p is set to Remap.
Membership Aging Time	The maximum duration (days, hours and minutes) that the voice VLAN traffic will get priority. Membership Aging is supported only for the Auto-VoIP OUI based.

Telephony OUI Configuration

Use the options on the Telephony OUI Configuration tile to add a MAC address prefix to the voice VLAN OUI table. The MAC prefixes in the OUI are used to identify voice traffic received on ports that are voice VLAN enabled.

Figure 113. Telephony OUI Configuration Tile

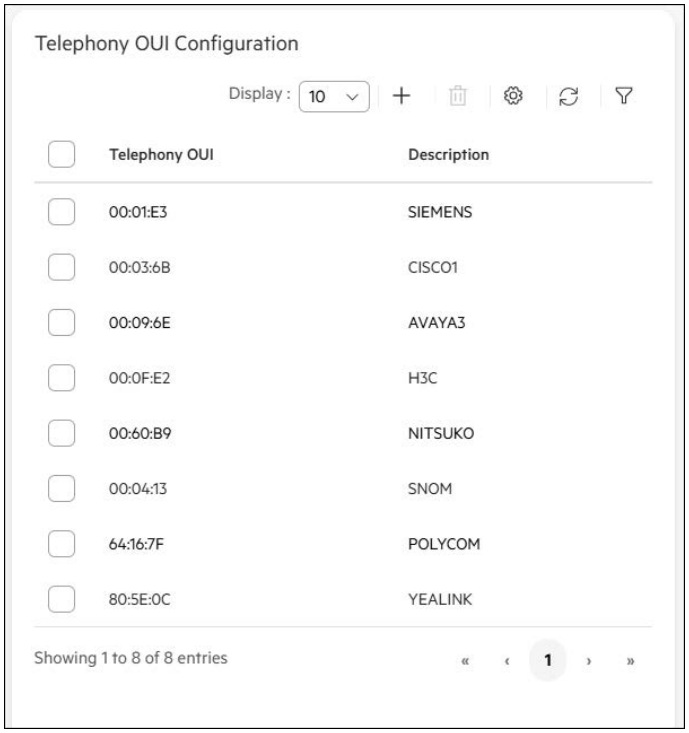


Table 92. Telephony OUI Configuration Fields

Field	Description
Telephony OUI	Specify the MAC address prefix which will be used to identify voice traffic.
Description	Description of the Telephony OUI.

To add a configuration, click + (**Add**).

To remove a configuration, select it and click (Remove).

To restore the defaults, click Restore Defaults.

Voice VLAN Interface Settings

Use Voice VLAN Interface Settings tile to configure Voice VLAN settings on one or more interfaces.

Figure 114. Voice VLAN Interface Settings Tile

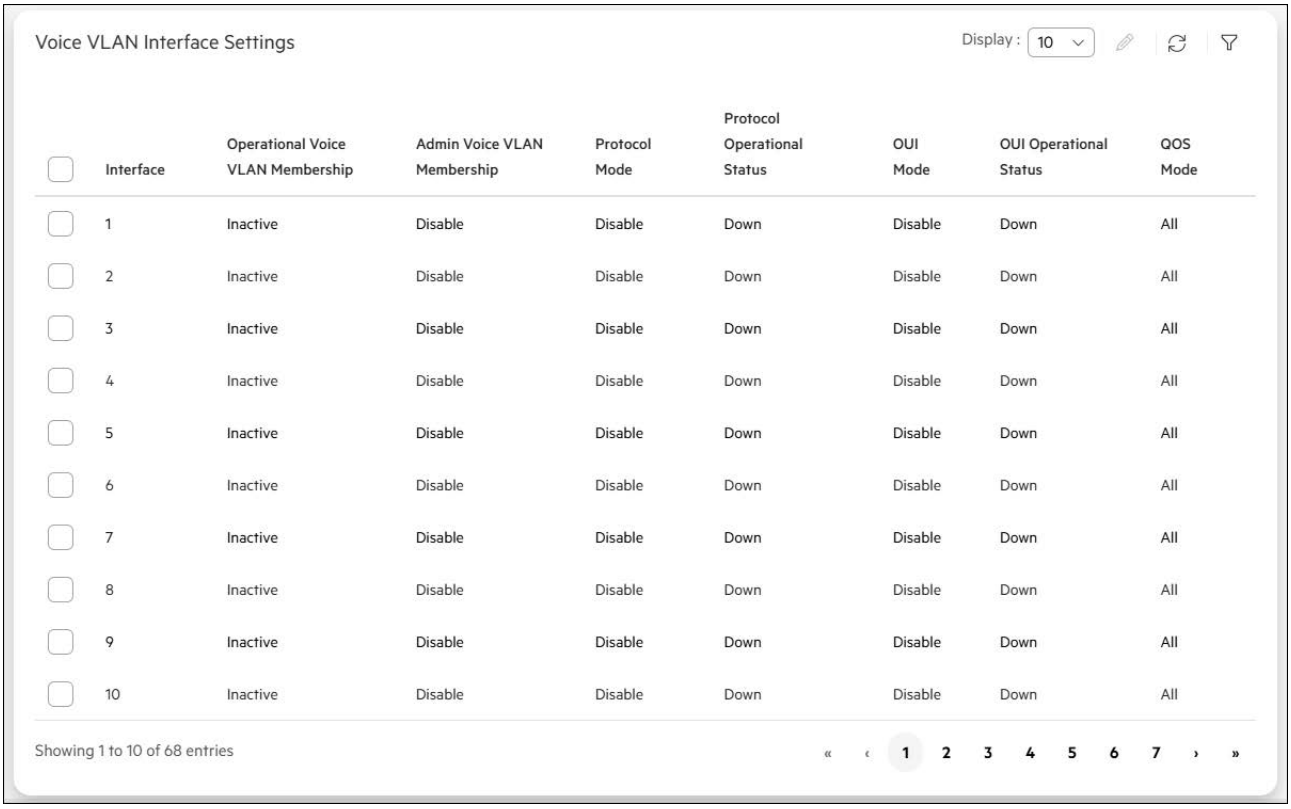


Table 93. Voice VLAN Interface Settings Fields

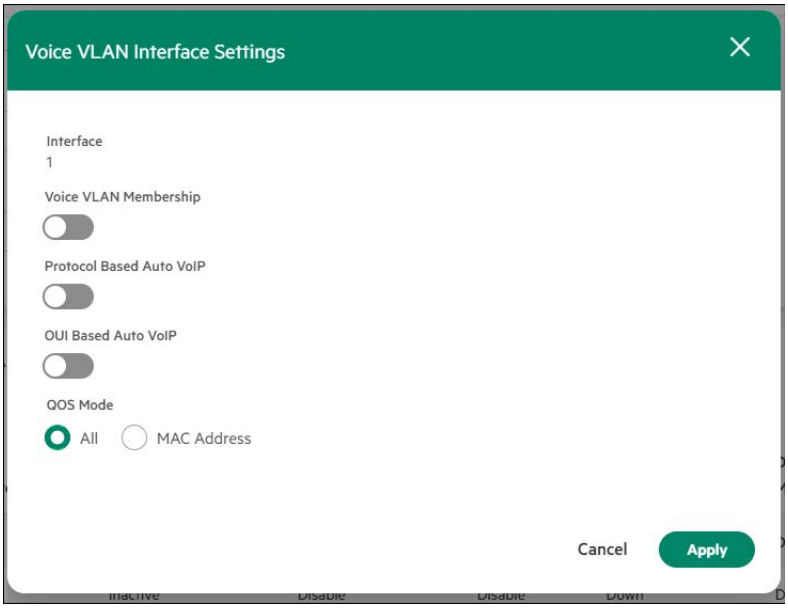
Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring the Voice VLAN Interface settings, this field identifies the interfaces that are being configured.
Operational Voice VLAN Membership	This is a read-only field that indicates the operational status of the Voice VLAN feature on the interface. The Interface Voice VLAN operational status is in the active state if all the following conditions exist: · Voice VLAN must be globally enabled and enabled on the interface. · The interface must be up. · The interface must have a link and be receiving traffic with matching voice protocol or with source OUI matching one of those in the Telephony OUI Configuration table. An example for active state is if interface receives a voice call with source MAC that equals one of the listed OUI. An example of Inactive state is if such a call ended and the OUI MAC entry aged out.

Field	Description
Admin Voice VLAN Membership	Enables or disables the Voice VLAN feature on the interface. When Voice VLAN is enabled globally and configured on interfaces that carry voice traffic, this feature can help ensure that the sound quality of an IP phone does not deteriorate when data traffic on the port is high. **Note**: In the edit page, the field name is Voice VLAN Membership.
OUI Mode	The administrative mode of OUI-based Auto-VoIP on the interface.
OUI Operational Status	The operational status of an interface. To be up, an interface must be administratively enabled and have a link.
Protocol Mode	The administrative mode of the Auto-VoIP feature on the interface: · Enable—The interface scans incoming traffic for the following call-control protocols: o Session Initiation Protocol (SIP). o H.323 o Skinny Client Control Protocol (SCCP). · Disable—The interface does not use the Auto-VoIP feature to scan for call-control protocols.
Protocol Operational Status	The operational status of an interface. Interface must be administratively enabled and have a link Up for the status to be Up.
QoS Mode	The Quality of Service override mode: · MAC Address—The voice VLAN QoS attributes will be applied only to packets with source MAC matching one of those in the OUI table. · All—The voice VLAN QoS attributes will be applied to all traffic forwarded on this port on the voice VLAN.

To add a configuration, click + (**Add**).

To modify these settings for one or more interfaces, select each interface to configure and click (**Edit**). To configure all interfaces at the same time with the same settings, click (**Edit All**).

Figure 115. Voice VLAN Interface Settings Dialog Box



Auto VLAN Configuration

The Auto VLAN feature allows dynamic assignment of VLANs to devices based on their MAC address prefix (OUI). This behavior simplifies network segmentation by automatically classifying and isolating devices like IP cameras, Wifi access points, and other devices into their respective VLANs, improving security and manageability.

Auto-Wifi Global Configuration

Use the Auto-Wifi Global Configuration tile to enable this figure and configure the global settings.

The Auto-Wifi feature automatically assigns Wifi-related devices (such as wireless access points or wireless controllers) to a predefined VLAN based on their OUI.

Figure 116. Auto-Wifi Global Configuration Tile

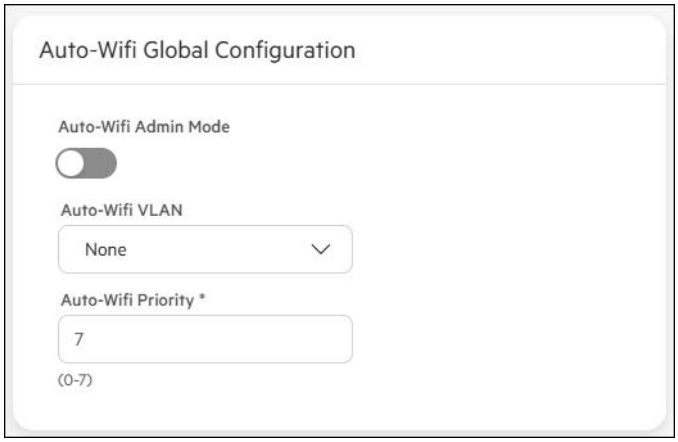


Table 94. Auto-Wifi Global Configuration Fields

Field	Description
Auto-Wifi Admin Mode	Set as Enabled to globally enable Auto-Wifi operation. The Auto-Wifi still needs to be enabled on the interface that requires the Auto-Wifi operation.
Auto-Wifi VLAN	Auto-Wifi VLAN automatically assigns Wifi-related devices (such as access points or wireless controllers) to a specific VLAN based on their MAC address prefix (OUI). This eliminates the need for manual VLAN tagging, streamlining the onboarding process for wireless infrastructure.
Auto-Wifi Priority	Auto-Wifi Priority allows the system to automatically prioritize traffic from Wifi devices on the selected interface or VLAN.

Auto-Camera Global Configuration

Use the Auto-Camera Global Configuration tile to enable this figure and configure the global settings.

The Auto-Camera feature automatically detects and places surveillance and IP camera devices into a designated VLAN using their MAC address OUI.

Figure 117. Auto-Camera Global Configuration Tile

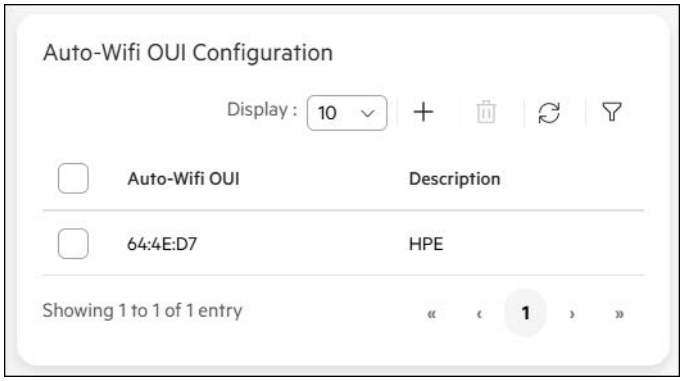


Table 95. Auto-Camera Global Configuration Fields

Field	Description
Auto-Camera Admin Mode	Set as Enabled to globally enable Auto-Camera operation. The Auto-Camera still needs to be enabled on the interface that requires the Auto-Camera operation.
Auto-Camera VLAN	Auto-Camera VLAN is used to automatically detect and segregate IP cameras into a designated VLAN based on their MAC OUI.
Auto-Camera Priority	Auto-Camera Priority automatically detects and prioritizes traffic from IP cameras on the network.

Auto-Wifi OUI Configuration

Use the options on the Auto-Wifi OUI Configuration tile to add MAC address prefixes to the Auto-Wifi VLAN OUI table. These MAC prefixes are used to identify Wifi devices based on their OUI. When untagged traffic from OUI matched devices is received on ports with Auto-Wifi VLAN enabled, it is automatically classified and placed into the Auto-Wifi VLAN.

Figure 118. Auto-Wifi OUI Configuration Tile

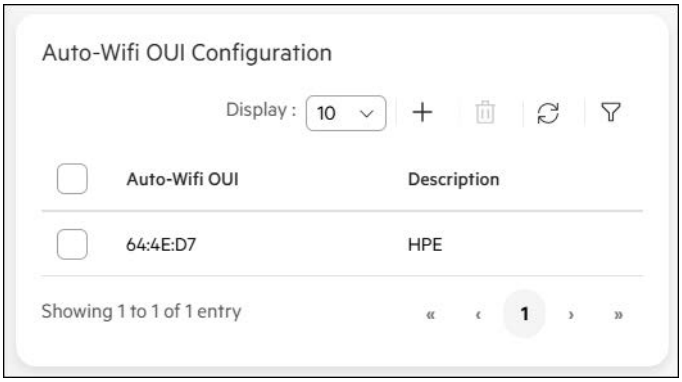


Table 96. Auto-Wifi OUI Configuration Fields

Field	Description
Auto-Wifi OUI	Specify the MAC address prefix which will be used to identify Wifi traffic.
Description	Description of the Wifi OUI.

To add a configuration, click + (**Add**).

To remove a configuration, select it and click (Remove).

Auto-Camera OUI Configuration

Use the options on the Auto-Camera OUI Configuration tile to add MAC address prefixes to the Auto-Camera VLAN OUI table. These MAC prefixes are used to identify camera devices based on their OUI. When untagged traffic from OUI matched devices is received on ports with Auto-Camera VLAN enabled, it is automatically classified and assigned to the Auto-Camera VLAN.

Figure 119. Auto-Camera OUI Configuration Tile

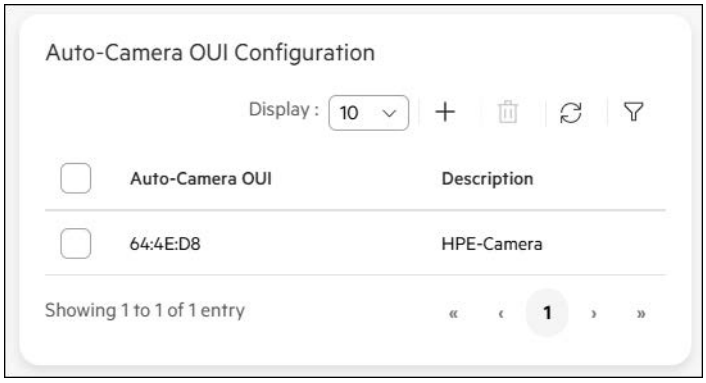


Table 97. Auto-Camera OUI Configuration Fields

Field	Description
Auto-Camera OUI	Specify the MAC address prefix which will be used to identify camera traffic.
Description	Description of the Auto-Camera OUI.

To add a configuration, click + (**Add**).

To remove a configuration, select it and click (Remove).

Auto VLAN Interface Settings

Use the options on the Auto VLAN Interface Settings tile to administratively enable or disable Auto-Wifi or Auto-Camera mode on interfaces.

Figure 120. Auto VLAN Interface Settings Tile

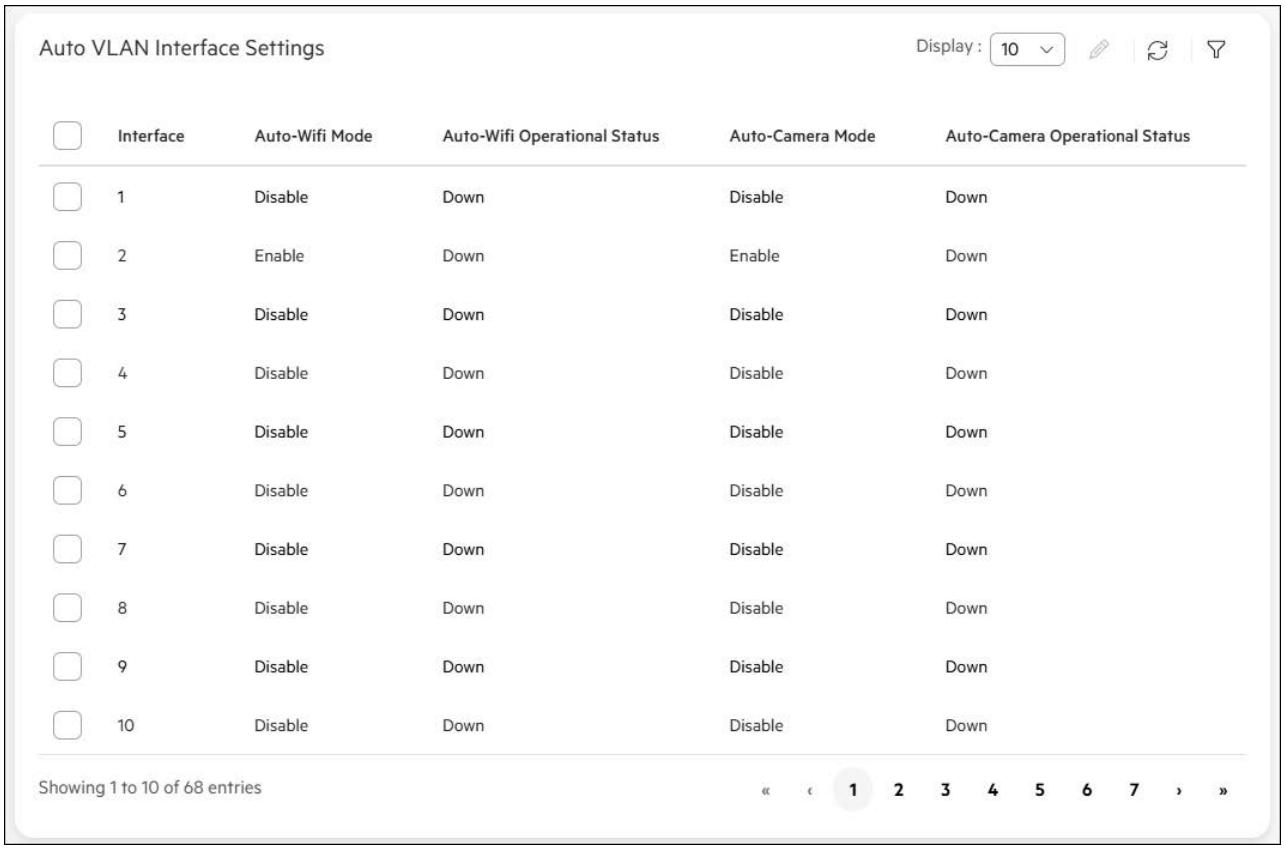


Table 98. Auto VLAN Interface Settings Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring the Auto-Wifi/Camera Interface settings, this field identifies the interface(s) that are being configured.
Auto-Wifi Mode	The administrative mode of Auto-Wifi on the interface.
Auto-Wifi Operational Status	The operational status of an interface. To be up, an interface must be administratively enabled and have a link.
Auto-Camera Mode	The administrative mode of Auto-Camera on the interface.
Auto-Camera Operational Status	The operational status of an interface. To be up, an interface must be administratively enabled and have a link.

To modify the settings for one or more interfaces, select each interface to configure and click + (**Edit**). The same settings are applied to all selected interfaces.

To remove a configuration, select it and click (Remove).

Auto VLAN Interface Summary

Use the options on the Auto VLAN Interface Settings tile to administratively enable or disable Auto-Wifi or Auto-Camera mode on interfaces.

Figure 121. Auto VLAN Interface Summary Tile



Table 99. Auto VLAN Interface Summary Fields

Field	Description
Interface	The physical or logical network port where the device was detected and assigned.
Auto VLAN Type	The type of Auto VLAN triggered for the device — e.g., Auto-Wifi, Auto-Camera
MAC Address	The MAC address of the detected device. Used to match against configured OUIs.

Chapter 8
Neighbor Discovery

Link Layer Discovery Protocol (LLDP) is a standard discovery protocol defined by IEEE 802.1AB. It allows stations residing on a LAN to advertise device capabilities, physical descriptions, and management information to other devices on the network. A network management system (NMS) can access and display this information.

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised in LLDP Protocol Data Units (LLDPDUs) by stations implementing the LLDP transmit function, and LLDPDUs are received and processed by stations implementing the receive function. The transmit and receive functions can be enabled and disabled separately per port. By default, both functions are enabled on all ports.

LLDP-MED is an extension of the LLDP standard. LLDP-MED uses LLDP's organizationally-specific Type-Length-Value (TLV) extensions and defines additional TLVs.

LLDP-MED can be utilized for many advanced features in a VoIP network environment. These features include basic configuration, network policy configuration, location identification (including for Emergency Call Service / E911), inventory management, and more.

LLDP-MED provides extensions to the IEEE 802.1AB base protocol to allow for these functions, and also provides behavioral requirements for devices implementing the extensions to enable correct multi-vendor inter-operation.

LLDP

Use the LLDP page to configure Global LLDP, to view LLDP Global Information, to configure the protocol on individual interfaces, and to view LLDP information and statistics.

To view the LLDP page, click **Neighbor Discovery > LLDP** in the navigation pane.

LLDP Global Configuration

Use the LLDP Global Configuration tile to specify the global LLDP parameters that apply to all LLDP-enabled interfaces.

Figure 122. LLDP Global Configuration Tile

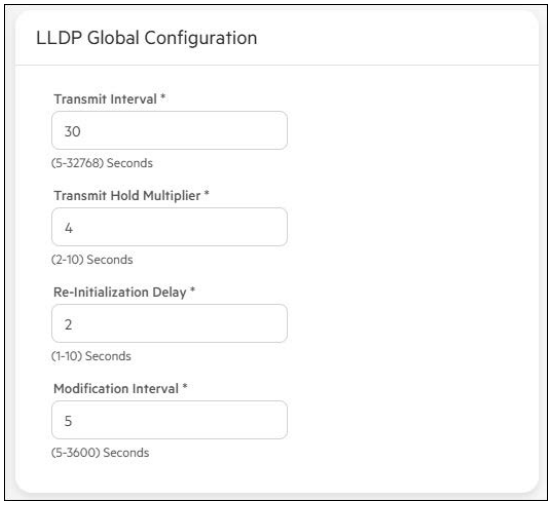


Table 100. LLDP Global Configuration Fields

Field	Description
Transmit Interval	Specify the time between transmission of LLDPDUs. The range is from 5 to 32768 seconds. The default is 30 seconds.
Transmit Hold Multiplier	Specify the multiplier value on the transmit interval, which is used to compute the time-to-live (TTL) value associated with LLDPDUs. The TTL = Transmit Interval × Transmit Hold Multiplier and determines how long the receiving neighbor should keep the information it has learned about a device before discarding it. The multiplier range is from 2 to 10, and the default is 4.
Re-Initialization Delay	Specify the number of seconds to wait before attempting to re-initialize LLDP on a port after the LLDP operating mode on the port changes. The range is from 1 to 10 seconds and the default is 2 seconds.
Notification Interval	Specify the minimum number of seconds to wait between transmissions of remote data change notifications. The range is from 5 to 3600 seconds and the default is 5 seconds.

LLDP Global Information

The LLDP Global Information tile displays the information that is included in the switch LLDP advertisement.

Figure 123. LLDP Global Information Tile

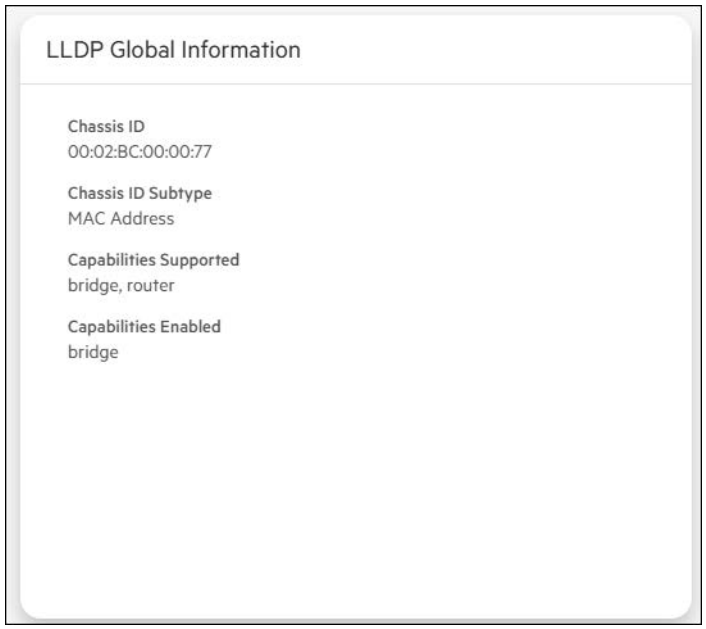


Table 101. LLDP Global Information Fields

Field	Description
Chassis ID	The hardware platform identifier for the switch.
Chassis ID Subtype	The type of information used to identify the chassis.
Capabilities Supported	The primary function(s) the switch supports.
Capabilities Enabled	The primary function(s) the switch supports that are enabled.

Interface Configuration

Use this tile to view and configure LLDP on the interfaces.

Figure 124. Interface Configuration Tile

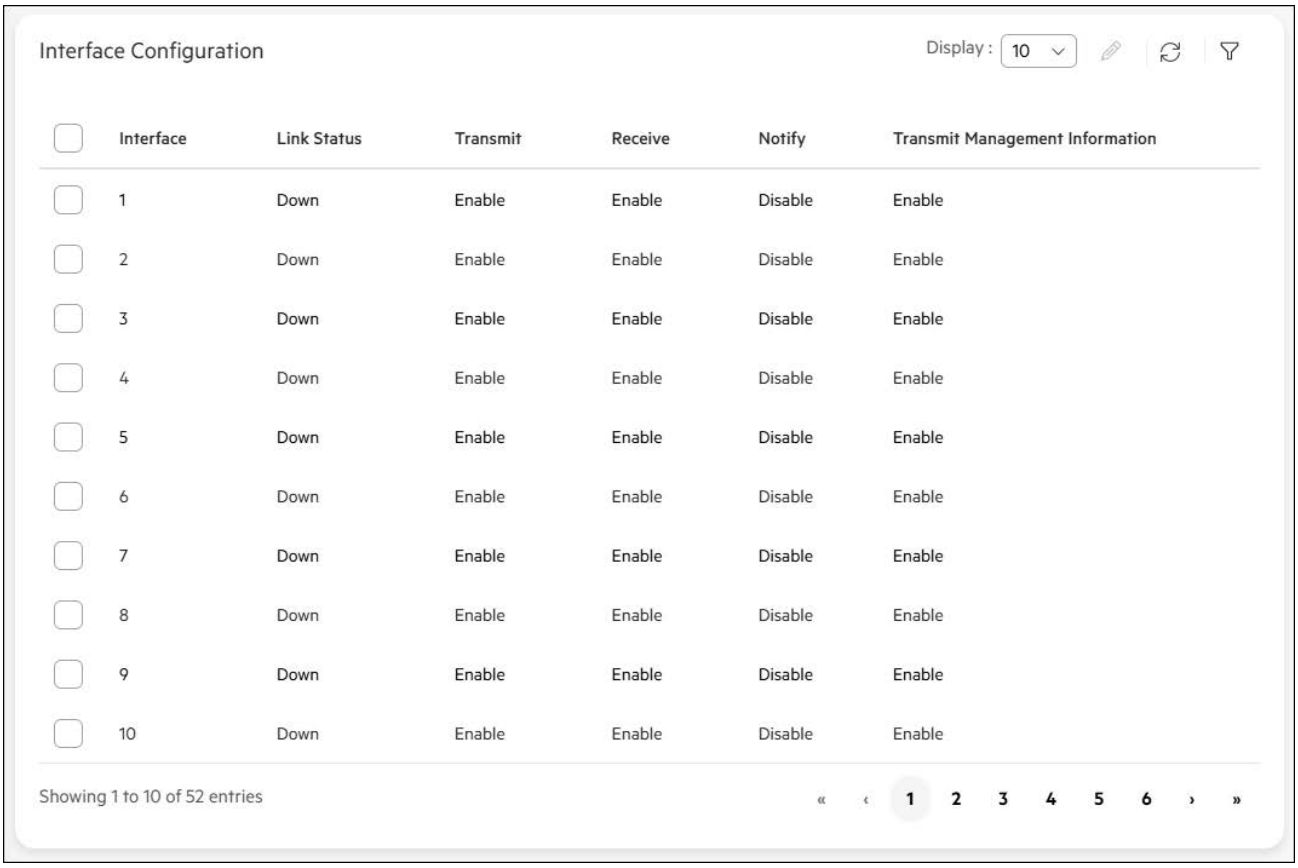


Table 102. Interface Configuration Fields

Field	Description
Interface	The port ID.
Link Status	The link status of the interface, which is either Up or Down. An interface that is down does not forward traffic.
Transmit	The LLDP advertise (transmit) mode on the interface. If the transmit mode is enabled, the interface sends LLDPDUs that advertise the mandatory TLVs that are enabled.
Receive	The LLDP receive mode on the interface. If the receive mode is enabled, the device can receive LLDPDUs from other devices.
Notify	Enable this option to have LLDP generate a log entry.
Transmit Management Information	Indicates whether management address information for the local switch is transmitted in LLDPDUs. Other remote managers can obtain information about the switch by using its advertised management address.

To modify the settings for one or more interfaces, select each interface to configure and click (**Edit**). The same settings are applied to all selected interfaces.

Figure 125. LLDP Interface Configuration Dialog Box



In addition to the controls described in Table 102, the LLDP interface configuration dialog box includes the LLDP/LLDP-MED Optional TLV settings the following table describes.

Table 103. Additional LLDP Interface Configuration Fields

Field	Description
802.3 Link Aggregation	Set to enable the link (associated with the port on which the LLDP PDU is transmitted) to be aggregated.
802.3 Maximum Frame Size	Maximum frame size capability of the MAC/PHY implementation.
802.3 Power via MDI	This TLV is applicable for PoE devices. This TLV supports the following extensions. · Type 2 (12 octets) · Type 3 (29 octets) This option is enabled by default and not configurable.

Remote Device Information

The Remote Device Information tab displays information about remote devices for which the switch has received LLDP information. Interfaces that have this option enabled display in this table only if they have received LLDP notifications from a remote device.

Figure 126. Remote Device Information Tab

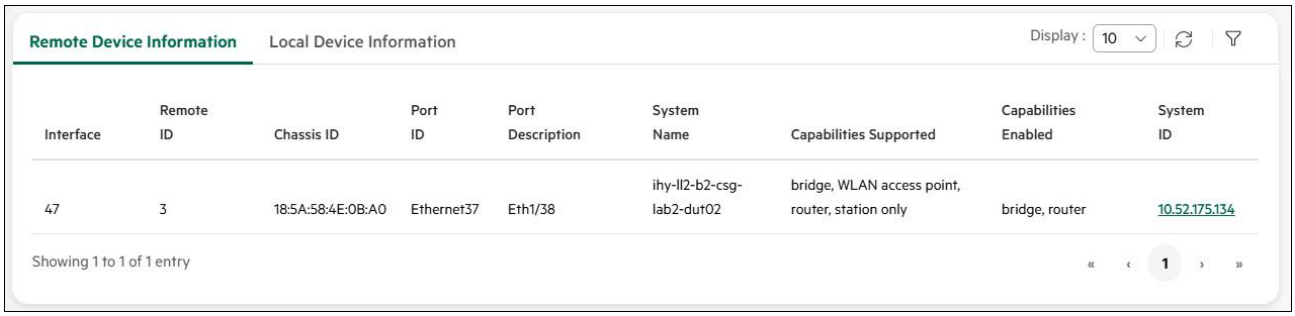


Table 104. Remote Device Information Fields

Field	Description
Interface	The device interface that received the LLDP data from the remote system.
Remote ID	The identifier assigned to the remote system that sent the LLDPDU.
Chassis ID	The hardware platform ID for the remote system.
Port ID	The physical address of the port on the remote device that sent the LLDP data.
Port Description	The port description configured on the remote device.
System Name	The system name configured on the remote device.
Capabilities Supported	The capabilities on the remote device (e.g., Repeater, Bridge, WLAN AP).
Capabilities Enabled	The capabilities on the remote device that are enabled.
System ID	The reported management IP or MAC addresses of the remote device.

Local Device Information

The Local Device Information tab displays LLDP information about the switch interfaces.

To display this tab, click **Neighbor Discovery > LLDP** in the navigation pane and click the **Local Device Information** tab (next to the **Remote Device Information** tab).

Figure 127. Local Device Information Tab

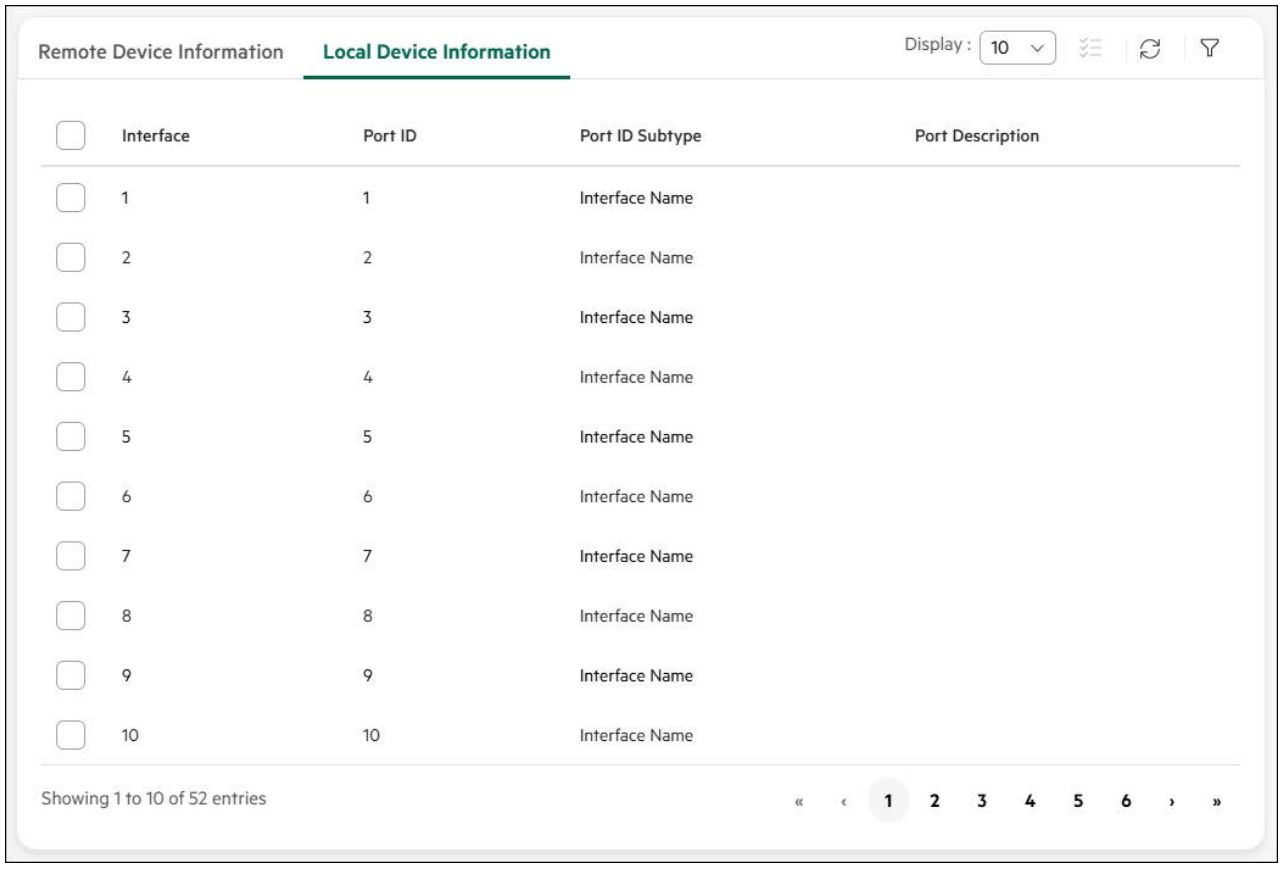


Table 105. Local Device Information Fields

Field	Description
Interface	The interface ID.
Port ID	The port identifier, which is the interface name.
Port ID Subtype	The type of information used to identify the interface.
Port Description	A description of the port.

To view additional information about an interface, select the interface row and click (**Details**).

Figure 128. LLDP Local Device Information Details

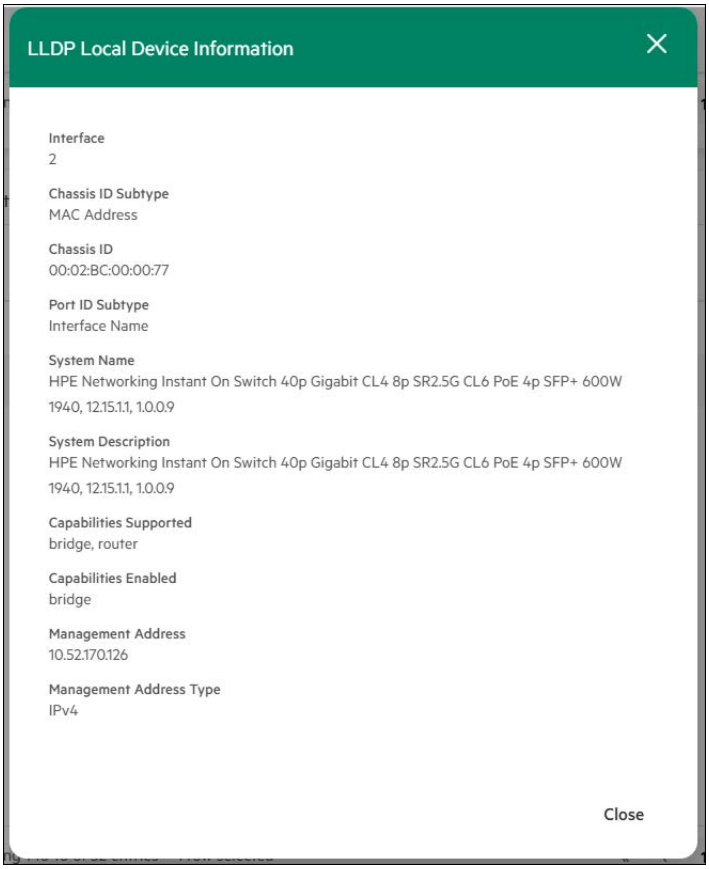


Table 106. LLDP Local Device Information Details

Field	Description
Interface	The interface ID.
Chassis ID Subtype	The type of information used to identify the chassis.
Chassis ID	The hardware platform identifier for the switch.
Port ID Subtype	The type of information used to identify the interface.
System Name	The user-configured system name for the switch.
System Description	The switch description which includes information about the product model and platform.
Capabilities Supported	The primary function(s) the switch supports.
Capabilities Enabled	The primary function(s) the switch supports that are enabled.
Management Address	The address, such as an IP address, associated with the management interface of the switch.
Management Address Type	The protocol type or standard associated with the management address.

LLDP Statistics

The LLDP Statistics tile displays per-port information for LLDP and LLDP-MED frames transmitted and received on the switch.

Figure 129. LLDP Statistics Tile

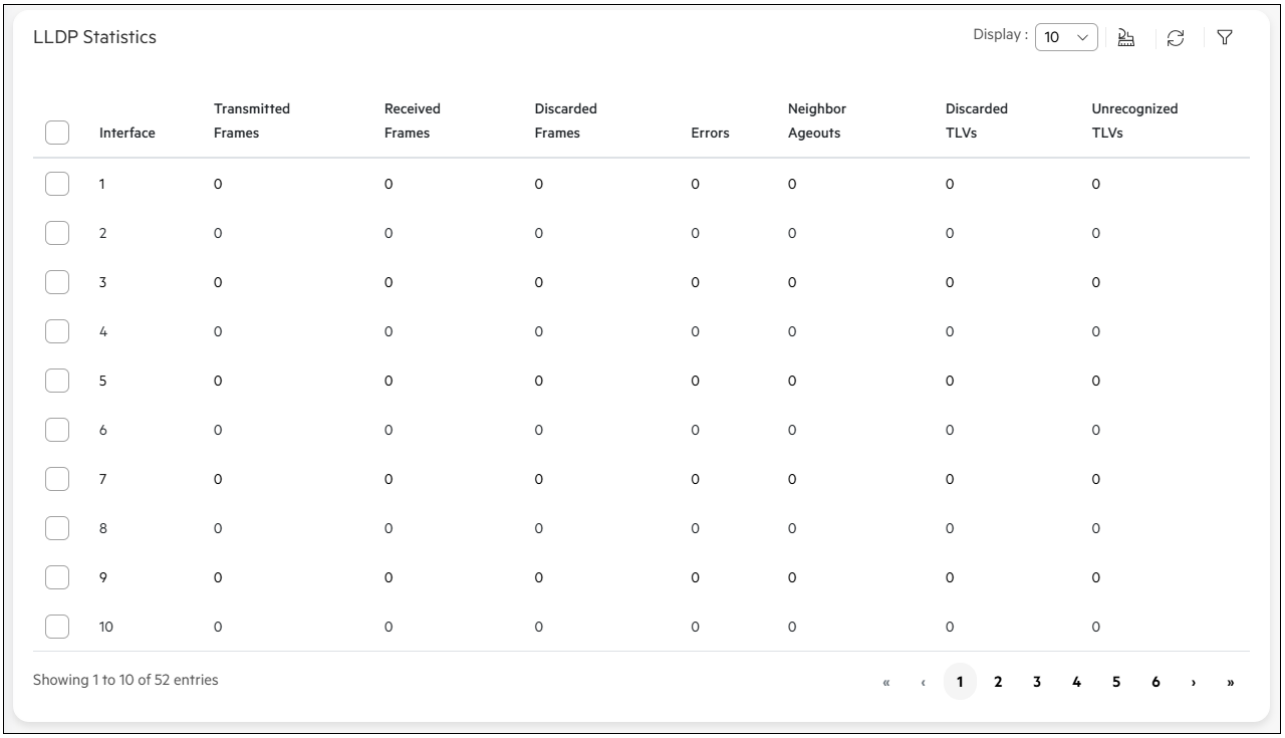


Table 107. LLDP Statistics Fields

Field	Description
Interface	The interface ID.
Transmitted Frames	The number of LLDP frames transmitted on the interface.
Received Frames	The number of LLDP frames received on the interface.
Discarded Frames	The number of LLDP frames the interface discarded for any reason.
Errors	The number of invalid LLDP frames received by the LLDP agent on the interface.
Discarded TLVs	The number of received LLDP TLVs that were discarded.
Unrecognized TLVs	The number of received LLDP TLVs that were not recognized.
Neighbor Ageouts	The number of LLDP neighbors that aged out on this interface.

To reset all statistics to 0, click (**Clear All**).

LLDP-MED Global Configuration

LLDP-MED is an enhancement to LLDP that enables:

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

To view and configure global Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) settings, click **Neighbor Discover** > **LLDP-MED** in the navigation pane.

LLDP-MED Global Configuration

Use the LLDP-MED Global Configuration tile to specify the global LLDP-MED parameters that apply to all LLDP-MED-enabled interfaces.

Figure 130. LLDP-MED Global Configuration Tile

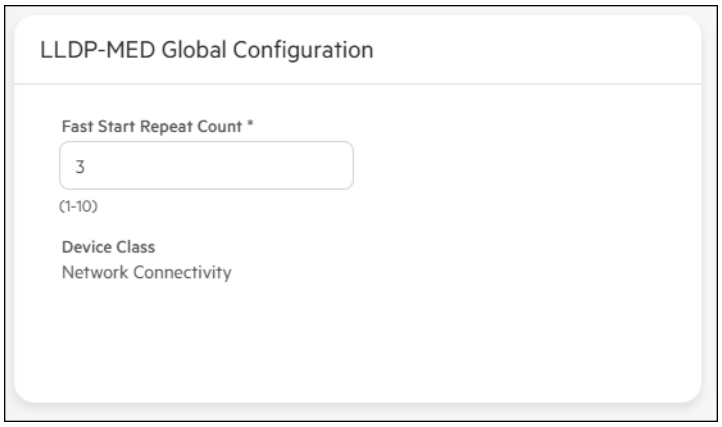


Table 108. LLDP-MED Global Configuration Fields

Field	Description
Fast Start Repeat Counter	The number of LLDP-MED Protocol Data Units (LLDPDUs) that are transmitted during the fast start period when LLDP-MED is enabled. The valid range is 1-10. The default is 3.
Device Class	The device's MED Classification. The HPE Networking Instant On 1940 Switch Series follows three classifications represent the actual endpoints: · Class I Generic (for example, IP Communication Controller) · Class II Media (for example, Conference Bridge) · Class III Communication (for example, IP Telephone) The fourth device is Network Connectivity Device, which is typically a device such as a LAN switch or router, IEEE 802.1 bridge, or IEEE 802.11 wireless access point.

If you change the Fast Start Repeat Counter value, click **Apply** to save any changes for the current boot session. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

LLDP Global Information

The LLDP Global Information tile displays the information that is included in the switch LLDP advertisement.

NOTE

The same tile appears in the LLDP page.

Figure 131. LLDP Global Information Tile



Table 109. LLDP Global Information Fields

Field	Description
Chassis ID	The hardware platform identifier for the switch.
Chassis ID Subtype	The type of information used to identify the chassis.
Capabilities Supported	The primary function(s) the switch supports.
Capabilities Enabled	The primary function(s) the switch supports that are enabled.

LLDP-MED Interface Configuration

Use this tile to view and configure LLDP-MED on the interfaces.

Figure 132. LLDP-MED Interface Configuration Tile

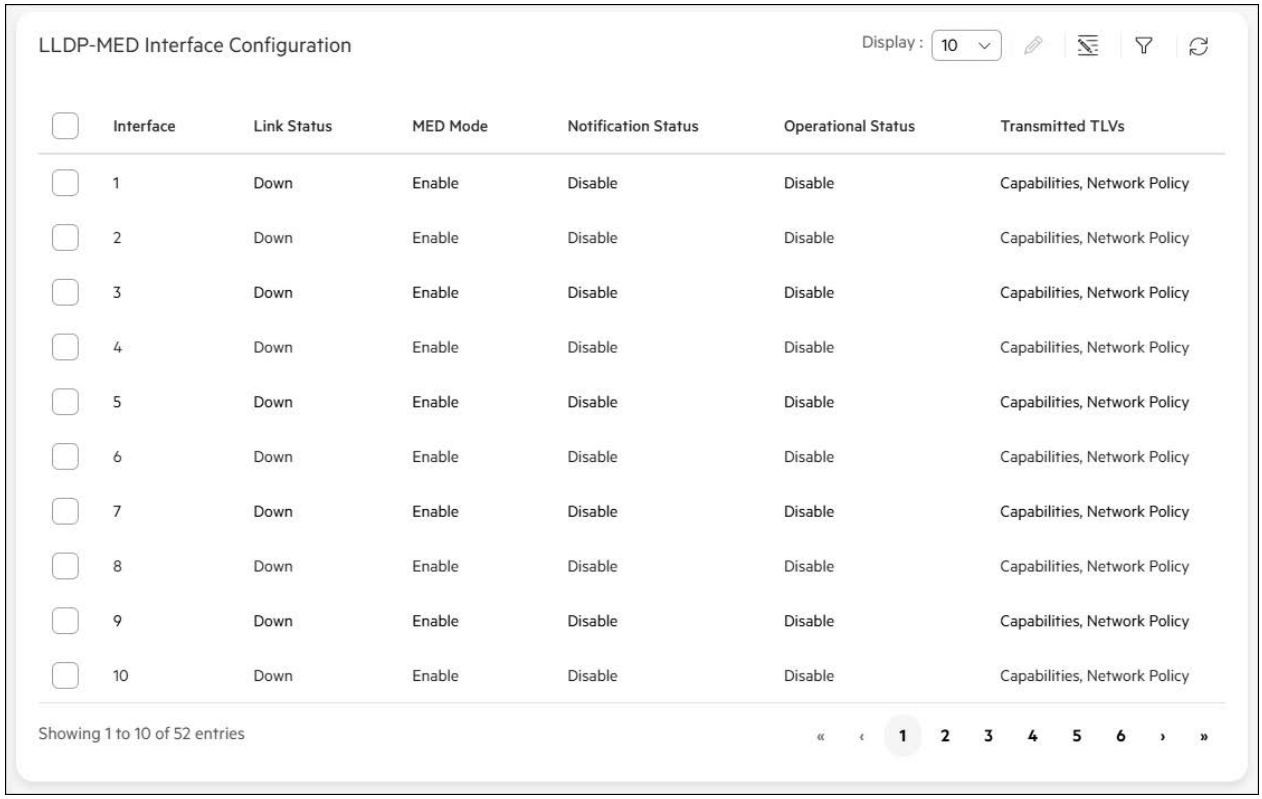


Table 110. LLDP-MED Interface Configuration Fields

Field	Description
Interface	The ID of the physical and trunk interfaces.
Link Status	The link status of the interface, which is either Up or Down. An interface that is down does not forward traffic.
MED Mode	The administrative status of LLDP-MED on the interface. When enabled, the LLDP-MED transmit and receive functions are effectively enabled on the interface. This feature is enabled by default.
Notification Status	Indicates whether LLDP-MED topology change notifications are enabled or disabled on the interface. This feature is disabled by default.
Operational Status	Indicates whether the interface is configured to transmit TLVs. To transmit TLVs, the interface must be enabled to receive and transmit LLDPDUs and must be connected to an LLDP-MED-capable device. The switch waits for the LLDP-MED device to advertise its information before the switch transmits its own LLDP-MED TLVs, at which point the operational status becomes enabled.
Transmitted TLVs	The LLDP-MED TLV(s) that the interface transmits. The HPE Networking Instant On 1940 Switch Series switches can transmit TLVs of the following types: · Capabilities · Network Policy · Power Sourcing Entity (PSE) on PoE-supported interfaces · 802.3 MAC-PHY is enabled by default and not configurable

To modify the settings for one interface, select the interface to configure and click (**Edit**). To configure all interfaces with the same settings, click (**Edit All**).

Figure 133. Edit LLDP-MED Interface Dialog Box

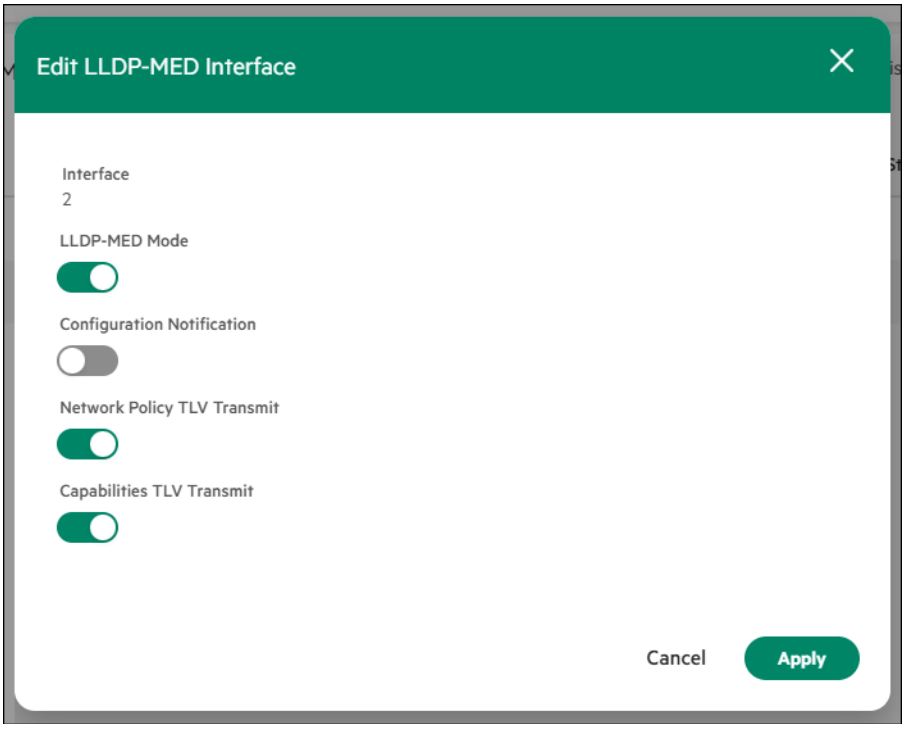


Table 111. Edit LLDP-MED Interface Fields

Field	Description
Interface	The port ID.
LLDP-MED	Enable/disable LLDP-MED on interface. Default is Enabled.
Configuration Notification	Enable/disable sending topology change notifications on the interface. Default is Disabled.
Network Policy TLV Transmit	Enable/disable on interface sending Network policy TLV. Default is Enabled.
Capabilities TLV Transmit	Enable/disable on interface sending Capabilities TLV. Default is Enabled.

LLDP-MED Remote Device Summary

The LLDP-MED Remote Device Summary tile displays information about the remote devices the local system has learned through the LLDP-MED data units received on its interfaces. Information is available about remote devices only if an interface receives an LLDP-MED data unit from a switch.

Figure 134. LLDP-MED Remote Device Summary Tile

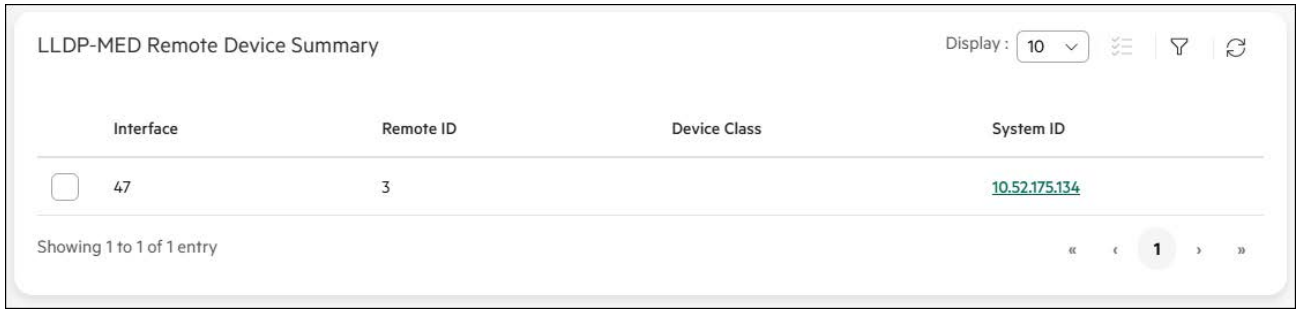


Table 112. LLDP-MED Remote Device Summary Fields

Field	Description
Interface	The local interface that has received LLDP-MED data units from remote devices.
Remote ID	The client identifier assigned to the remote system that sent the LLDP-MED data unit.
Device Class	The MED Classification advertised by the TLV from the remote device. The following three classifications represent the actual endpoints: · Class I Generic (for example, IP Communication Controller) · Class II Media (for example, Conference Bridge) · Class III Communication (for example, IP Telephone) The fourth device is Network Connectivity Device, which is typically a device such as a LAN switch or router, IEEE 802.1 bridge, or IEEE 802.11 wireless access point.
System ID	The reported management IP addresses of the remote device.

To view additional information about an interface, select the interface row and click (**Details**).

Table 113. LLDP-MED Remote Device Detailed Information Fields

Field	Description
Interface	The local interface that has received LLDP-MED data units from remote devices.
Remote ID	The client identifier assigned to the remote system that sent the LLDP-MED data unit.
System ID	The reported management IP addresses of the remote device.
Capabilities	
Capabilities Supported	The supported capabilities that were received in the MED TLV on this interface.
Capabilities Enabled	The supported capabilities on the remote device that are also enabled.
Device Class	The MED Classification advertised by the TLV from the remote device.
Inventory	
This section describes the information in the inventory TLVs received in the LLDP-MED frames on this interface.	
Hardware Revision	The hardware version advertised by the remote device.
Firmware Revision	The firmware version advertised by the remote device.
Software Revision	The software version advertised by the remote device.
Serial Number	The serial number advertised by the remote device.

Field	Description
Manufacturer Name	The name of the system manufacturer advertised by the remote device.
Model Name	The name of the system model advertised by the remote device.
Asset ID	The system asset ID advertised by the remote device.
Extended PoE	
This section describes whether the remote device is advertised as a PoE device.	
Device Type	If the remote device is a PoE device, this field identifies the PoE device type of the remote device connected to the port.
Extended PoE-PD	
This section describes the information about the remote PoE powered device.	
Required	If the remote device is a PoE device, this field details the remote ports PD power requirement in Watts.
Source	If the remote device is a PoE device, this field details the remote ports PoE PD power source.
Priority	If the remote device is a PoE device, this field details the remote ports PD power priority.
Network Policy Information	
This section describes the information in the network policy TLVs received in the LLDP-MED frames on this interface.	
Media Application Type	The media application type received in the TLV from the remote device. The application types are unknown, voice-signaling, guest-voice, guest-voice-signaling, soft-phone-voice, video-conferencing, streaming-video, video-signaling. Each application type that is transmitted has the VLAN ID, priority, DSCP, tagged bit status and unknown bit status. The port on the remote device may transmit one or many such application types. This information is displayed only when a network policy TLV has been received.
VLAN ID	The VLAN ID associated with a particular policy type.
Priority	The user priority associated with a particular policy type.
DSCP	The Differentiated Services Code Point value associated with a particular policy type.
Unknown Bit Status	The unknown bit associated with a particular policy type.
Tagged Bit Status	Identifies whether the network policy is defined for tagged or untagged VLANs.

Chapter 9
Power over Ethernet

Power over Ethernet (PoE) functionality is supported on certain HPE Networking Instant On Series switch models, enabling designated switch ports to provide power to connected devices. These PoE ports are referred to as power source equipment (PSE).

The devices receiving power through PoE are referred to as powered devices (PDs).

The PoE software supports two power modes to allocate power by Usage (default) or Class. The default usage mode reclaims unused power for use by new PD connections or increased power demand by existing powered PDs. The configurable class mode reserves the full PD requested class power from the total available power budget.

Ports are assigned one of four configurable PoE priority values (Critical, High, Medium and Low). When more power is requested than is available on the switch, the switch provides power to high priority ports before lower priority ports. Power allocation can be scheduled so that power is supplied only during that schedule time.

You can limit the power of a port using the Class Limit feature.

Always-on PoE is a new feature in the Instant On portfolio that enables continuous PoE delivery to connected PDs during system maintenance. This applies only to interfaces that were supplying power prior to the reboot. PoE will not be maintained if the switch experiences a power interruption.

Quick PoE is an additional PoE feature that enables the switch to provide power to connected PDs upon a warm reboot. When Quick PoE is enabled, disabling PoE on a port and PD demotion are not permitted. The feature must be enabled both globally and on each interface to take effect.



The information in this chapter is valid only for the switches that support PoE. The switches that do not have PoE ports do not include the web pages this chapter describes.

The following table shows the maximum power per SKU that the switch can provide to all PoE ports combined.

Table 114. PoE Ports and Power Capabilities

Switch	PoE Support	Maximum Power
HPE Networking Instant On Switch 8p Gigabit CL6 PoE 2p SFP 124W 1940	8 ports class 6 PoE	124W
HPE Networking Instant On Switch 8p SR10 4p CL6 PoE 2p SFP+ 120W 1940	4 ports class 6 PoE	120W
HPE Networking Instant On Switch 24p Gigabit CL4 PoE 4p SFP+ 240W 1940	24 ports class 4 PoE	240W
HPE Networking Instant On Switch 20p Gigabit CL4 4p SR2.5G CL6 PoE 4p SFP+ 370W 1940	20 ports class 4 and 4 ports class 6 PoE	370W
HPE Networking Instant On Switch 48p Gigabit CL4 PoE 4p SFP+ 370W 1940	48 ports class 4 PoE	370W
HPE Networking Instant On Switch 40p Gigabit CL4 8p SR2.5G CL6 PoE 4p SFP+ 600W 1940	40 ports class 4 and 8 ports class 6 PoE	600W

PoE Configuration

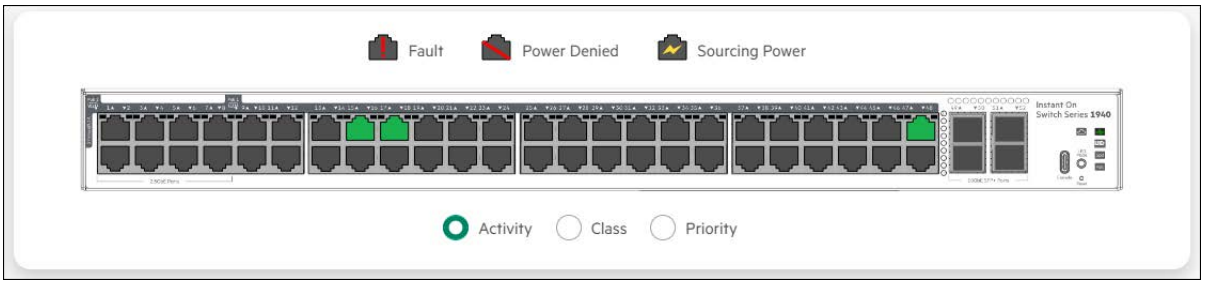
Use the PoE Configuration Page to view PoE status, consumption history, and port configuration.

Device View

The top of the PoE Configuration page shows a graphical representation of the switch front panel. This panel view can show the Activity status, Priority, and Class of the ports.

Click the radio buttons to show the related information. Click a PoE port in this screen to open the Edit Port PoE Configuration dialog box.

Figure 135. PoE Device View



Activity

Click the Activity radio button to show which ports have the conditions described in the following table.

Port State	Image	Description
Fault		There is a fault in the port activity.
Power Denied		Power is denied for this port.
Sourcing Power		This port is providing power.

Priority

Click the Priority radio button to show the priority of the ports on the switch.

- L —Indicates Low priority.
- M —Indicates Medium priority.
- H —Indicates High priority.
- C —Indicates Critical priority.

Class

Click the Class radio button to show the class of the ports on the switch.

- 0—Indicates 0.44-12.95W.
- 1—Indicates 0.44-3.84W.
- 2—Indicates 3.84- 6.49W.
- 3—Indicates 6.49-12.95W.
- 4 —Indicates 12.95-25.5W.
- 5 —Indicates 25.5-40W.
- 6 —Indicates 40-51W.

Global Configuration

Use the Global Configuration tile to configure the settings that impact all interfaces on the switch.

Figure 136. PoE Global Configuration Tile

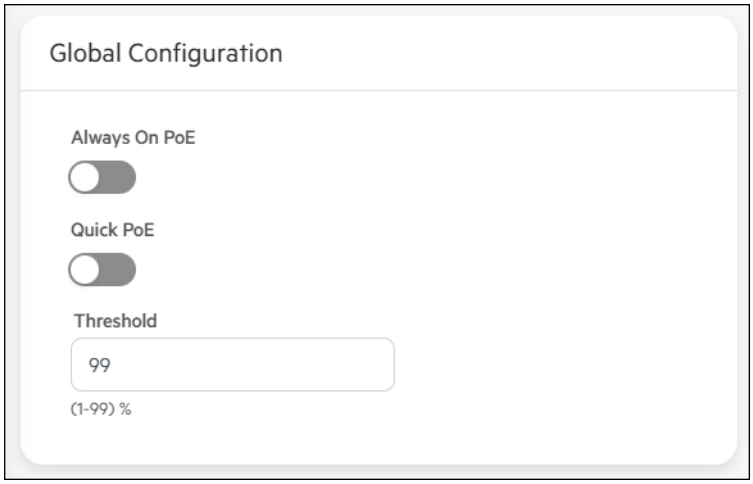


Table 115. PoE Global Configuration Fields

Field	Description
Always On PoE	Provides the user a mode that keeps PoE power active during system maintenance. By default, Always On PoE is globally disabled.
Quick PoE	Provides the user a mode to enable PoE power delivery quickly upon a warm reboot prior to the system coming online. By default, Quick PoE is disabled.
Threshold	A user-configurable threshold value as a percentage (%) of the total available power. Sets the threshold at which the system will send an excess power consumption notification trap and post a syslog message. Default value is 90%.

Status

The Status tile shows PoE global information, including the total power, actual power consumption, and PoE status.

Figure 137. PoE Status Tile

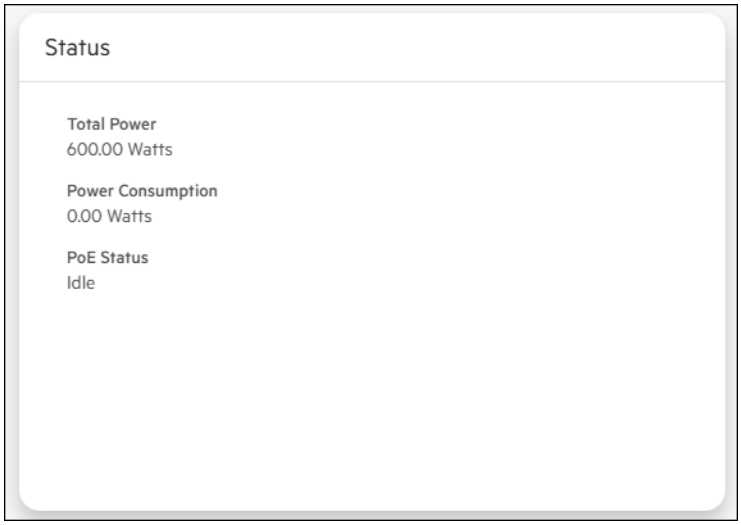


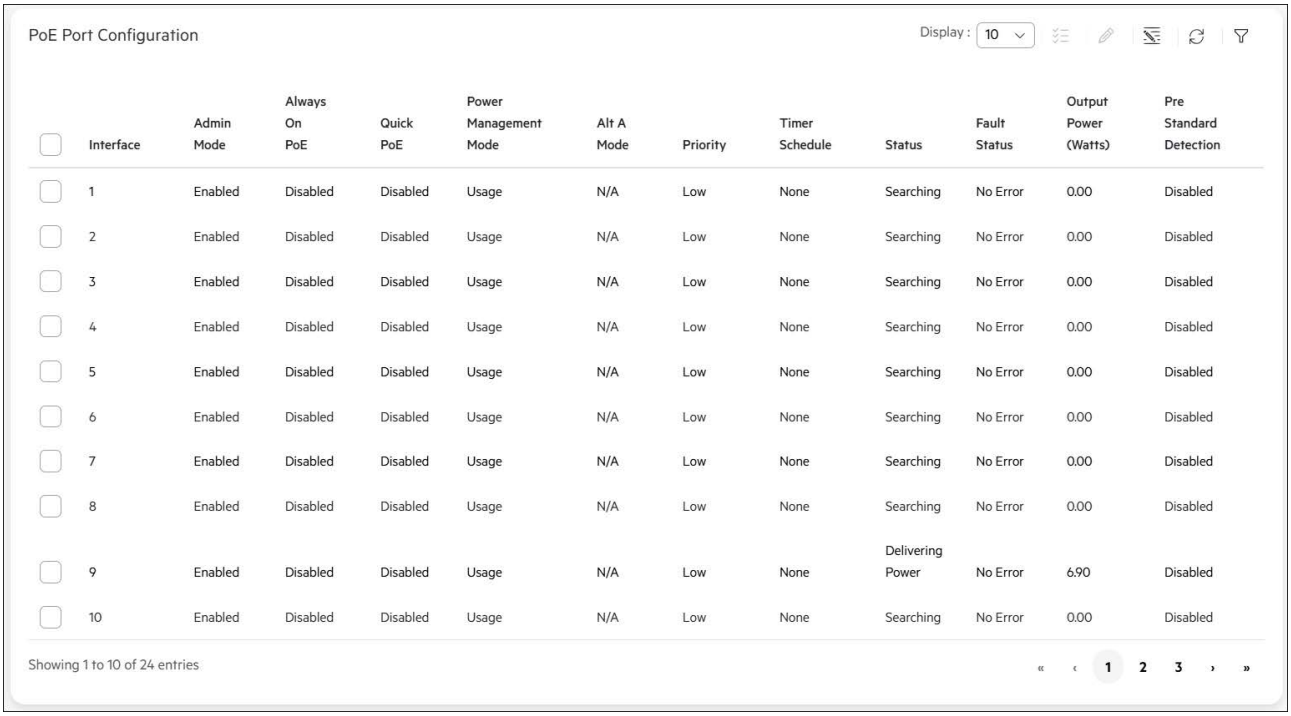
Table 116. PoE Status Fields

Field	Description
Total Power (Watts)	The total power in watts that can be provided by the switch.
Power Consumption (Watts)	The amount of power in watts currently being consumed by connected PoE devices (PD).
PoE Status	The current status of the switch PoE functionality. Possible values are: · Delivering—At least one port on the switch is delivering power to a connected switch, and no port is in Fault state. · Requesting Power—At least one port on the switch is requesting power to a connected switch, and no port is in Fault state. · Idle—The PoE functionality is operational but no ports are delivering power, and no ports have errors. · Faulty—One or more ports are not functioning due to a hardware fault or is in the hardware fault-recovery state. · Not Functional—PoE is not functional on switch due to a hardware failure. · Error—One or more ports are in a PoE fault state. This does not include hardware-related fault states.

PoE Port Configuration

Use the PoE Port Configuration tile to administratively enable or disable PoE on ports that support it and to configure the port priority and other settings.

Figure 138. PoE Port Configuration Tile



Interface	Admin Mode	Always On PoE	Quick PoE	Power Management Mode	Alt A Mode	Priority	Timer Schedule	Status	Fault Status	Output Power (Watts)	Pre Standard Detection
1	Enabled	Disabled	Disabled	Usage	N/A	Low	None	Searching	No Error	0.00	Disabled
2	Enabled	Disabled	Disabled	Usage	N/A	Low	None	Searching	No Error	0.00	Disabled
3	Enabled	Disabled	Disabled	Usage	N/A	Low	None	Searching	No Error	0.00	Disabled
4	Enabled	Disabled	Disabled	Usage	N/A	Low	None	Searching	No Error	0.00	Disabled
5	Enabled	Disabled	Disabled	Usage	N/A	Low	None	Searching	No Error	0.00	Disabled
6	Enabled	Disabled	Disabled	Usage	N/A	Low	None	Searching	No Error	0.00	Disabled
7	Enabled	Disabled	Disabled	Usage	N/A	Low	None	Searching	No Error	0.00	Disabled
8	Enabled	Disabled	Disabled	Usage	N/A	Low	None	Searching	No Error	0.00	Disabled
9	Enabled	Disabled	Disabled	Usage	N/A	Low	None	Delivering Power	No Error	6.90	Disabled
10	Enabled	Disabled	Disabled	Usage	N/A	Low	None	Searching	No Error	0.00	Disabled

The following settings display for each port that supports PoE.

Table 117. PoE Port Configuration Fields

Field	Description
Interface	The port number.
Admin Mode	Indicates whether PoE is administratively enabled or disabled on the port. This feature is enabled by default on ports that support PoE.
Always On PoE	Provides the user a mode that keeps PoE power active across soft reboots. Always On PoE is globally disabled by default. Always On PoE and Quick PoE are mutually exclusive and cannot be enabled at the same time on a port.
Quick PoE	Provides the user a mode to enable PoE power delivery quickly upon a soft reboot or power cycle prior to the system coming online. Quick PoE is globally disabled by default. Always On PoE and Quick PoE are mutually exclusive and cannot be enabled at the same time on a port.
Power Management Mode	The method by which the PoE controller determines supplied power, which can be one of the following: · Class—The power allocated to each port is reserved and is not available to any other port, even when less than the maximum allocation is being used. · Usage—The power allocated to each port is not reserved. Unused power may be allocated from one port to another as needed, up to the power limit defined for each port.

Field	Description
Alt A Mode	The Alt-A setting is available on Class 6 ports only. When enabled, the switch's PoE controller delivers power over 2 pairs (IEEE 802.3af/at) instead of 4 pairs (IEEE 803.2bt). The Alt-A setting is useful for legacy or non-compliant IEEE 802.3af/at PD devices unable to support IEEE 802.3bt standards.
Priority	The priority of the port when allocating available power. Power is delivered to the higher-priority ports when needed before providing it to the lower priority ports. Possible values are Critical, High and Low. Low is the lowest priority and the default for all ports.
Time Schedule	The scheduled time when source power is available on this port. You can configure schedules on the Schedule Configuration page.
Status	The status of the port as a provider of power over Ethernet. Such devices are referred to as power-sourcing equipment (PSE). Possible values are: · Disabled—The PSE is disabled. · Delivering Power—The PSE is delivering power. · Fault—The PSE has experienced a fault condition. · Test—The PSE is in test mode. · Other Fault—The PSE has experienced a variable error condition. · Searching—The PSE is transitioning between states. · Requesting Power—The PSE is currently not able to deliver power because power is unavailable to the port.
Output Power	Power consumed by the port, in Watts.
Fault Status	The fault status, if a fault occurred. Possible values are: · None—No faults have occurred. · Short—PSE port has detected a short circuit condition. · Overload—A connected PD has attempted to draw more than the allowed watts. · Power Denied—A PD requesting power on the port has been denied because of insufficient power available. · MPS Absent—PSE port has detected absence of main power supply. NOTE: This field is relevant only if the status of the port is Fault.
Pre Standard Detection	The protocol(s) that can be used to detect the presence of a PD when connected to a PoE port. The IEEE specification 802.3af (Dot3af) specifies various detection algorithms. Some PDs use legacy detection algorithms that were in place prior to the 802.3af standard, which can be one of the following: · Disabled—The switch uses the 802.3af 4-point detection scheme only. · Enabled—The switch uses the 802.3af 4-point detection scheme, followed by the legacy detection scheme.

Modifying Port PoE Settings

To change the PoE settings for one port, select each interface to configure and click (**Edit**). To configure all ports with the same settings, click (**Edit All**).

Figure 139. Edit Port PoE Configuration Dialog Box

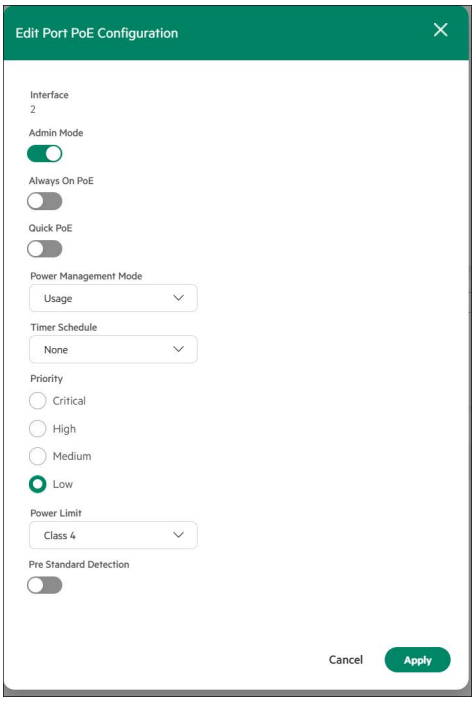


Table 118. Edit Port PoE Configuration Fields

Field	Description
Interface	The port number.
Admin Mode	Controls whether PoE is administratively enabled or disabled on the port. This feature is enabled by default.
Always On PoE	Provides the user a mode to keep PoE power active across soft reboots. Always On PoE is disabled by default. Always On PoE and Quick PoE are mutually exclusive and cannot be enabled at the same time on a port.
Quick PoE	Provides the user a mode to enable PoE power delivery quickly upon a soft reboot or power cycle prior to the system coming online. Quick PoE is globally disabled by default. Always On PoE and Quick PoE are mutually exclusive and cannot be enabled at the same time on a port.
Power Management Mode	The method by which the PoE controller determines supplied power, which can be one of the following: · Class—The power allocated to each port is reserved and is not available to any other port, even when less than the maximum allocation is being used. · Usage—The power allocated to each port is not reserved. Unused power may be allocated from one port to another as needed, up to the power limit defined for each port.
Alt A Mode	The Alt-A setting is available on Class 6 ports only. When enabled, the switch's PoE controller delivers power over 2 pairs (IEEE 802.3af/at) instead of 4 pairs (IEEE 803.2bt). The Alt-A setting is useful for legacy or non-compliant IEEE 802.3af/at PD devices unable to support IEEE 802.3bt standards. NOTE: Enabling Alt A Mode forces Power Limit to Class 4.
Timer Schedule	The scheduled time when source power is available on this port. You can configure schedules on the Schedule Configuration page.
Priority	The priority of the port when allocating available power. Power is delivered to the higher-priority ports when needed before providing it to the lower priority ports. Possible values are Critical, High, Medium and Low. Low is the lowest priority and the default for all ports.

Field	Description
Power Limit	The power limit for the port, the following values can be selected: · Class 6—Limit the power for dot3bt-type3 · Class 4—Limits the power for dot3at devices · Class 3—Limits the power for dot3af devices · Legacy—Allows higher inrush for legacy PDs
Pre Standard Detection	The protocol(s) that can be used to detect the presence of a PD when connected to a PoE port. The IEEE specification 802.3af (Dot3af) specifies various detection algorithms. Some PDs use legacy detection algorithms that were in place prior to the 802.3af standard, which can be one of the following: · Disabled: The switch uses the 802.3af 4-point detection scheme only. · Enabled: The switch uses the 802.3af 4-point detection scheme, followed by the legacy detection scheme.

Viewing PoE Port Details

To view additional PoE configuration information for a port, select the port row and click (**Details**).

Figure 140. PoE Port Details Dialog Box

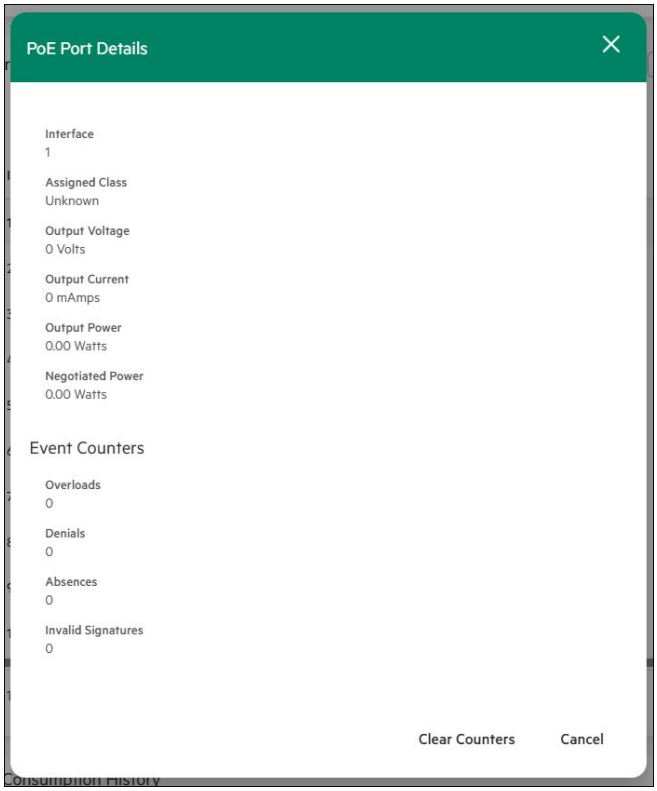


Table 119. PoE Port Details Fields

Field	Description
Interface	The port number.
Assigned Class	The class of power actually supplied to the powered device. This class may be lower than the measured class because of lack of available power or if the port does not support the measured class.
Output Voltage	The voltage being applied to the connected switch.
Output Current	The current, in milliamps, being drawn by the connected switch.

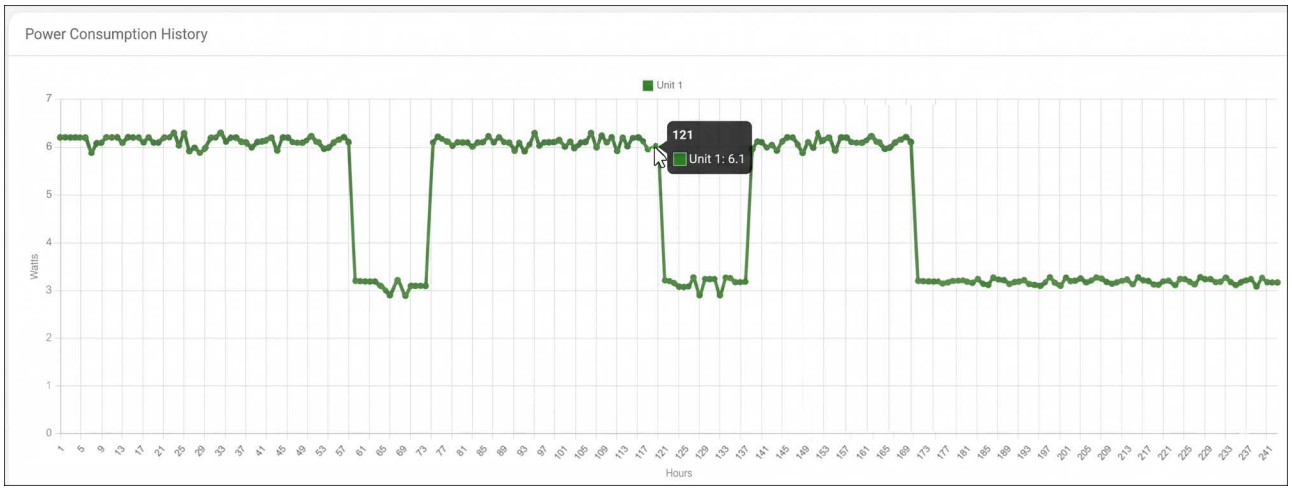
Field	Description
Output Power	Power in watts being drawn by the connected switch.
Negotiated Power	Power in watts negotiated between the port and connected switch.
Event Counters	
Overloads	The number of power overload events detected on the port.
Denials	The number of times that the powered device was denied power.
Absences	The number of times that power was stopped to the powered device, because the powered device was not detected.
Invalid Signatures	The number of times an invalid signature was received. Signatures are the means by which the powered device identifies itself to the PSE. Signatures are generated during powered device detection, classification, or maintenance.

To reset the Event Counters to 0, click **Clear Counters**.

Power Consumption History

The Power Consumption History tile presents a 10-day history of the switch's power usage, allowing you to track consumption trends over time. The information is displayed as a line graph. The Y-axis shows the power consumption in Watts, and the X-axis shows the time interval in Hours. If you hover over a plot point, the hour and Watt usage for that point are displayed.

Figure 141. Power Consumption History Tile



Use the Routing pages to configure Layer 3 features and capabilities.

IPv4 Routing

Use the IPv4 Routing page to configure global IPv4 Layer 3 features, view and edit Port IP and VLAN IP routing, static routing and route table, IP routing statistics and ICMP statistics.

To view the Routing Configuration page, click **Routing > IPv4 Routing** in the navigation pane.

Global Configuration

Use the Global Configuration page to configure global IPv4 routing settings on the switch. These are the global settings for Routing:

Figure 142. IPv4 Routing Global Configuration Tile



Table 120. IPv4 Routing Global Configuration Fields

Field	Description
Routing	The administrative mode of routing on the switch. The options are as follows: · Enable—The switch can act as a Layer 3 switch by routing packets between interfaces configured for IP routing. · Disable—The switch acts as a Layer 2 bridge and switches traffic between interfaces. The switch does not perform any internetwork routing.
Operational Default Gateway	The IP address of the default gateway for the switch. If the destination IP address in a packet does not match any routes in the routing table, the packet is sent to the default gateway. The gateway displayed in this field is the next hop on switch with the lowest metric.
Static Route Preference	The default distance (preference) for static routes. Lower route-distance values are preferred when determining the best route. The value configured for Static Route Preference is used to configure a static route and no preference is specified. Changing the Static Route Preference does not update the preference of existing static routes.

Port IP and VLAN IP

To view the Port IP interface information, click the Port IP tab. To view the VLAN IP interface information, click the VLAN IP tab.

The Port IP and the VLAN IP tabs show the same fields. These tabs show summary information about the routing configuration for all interfaces.

The following figure shows the Port IP tab.

Figure 143. Port IP Tab

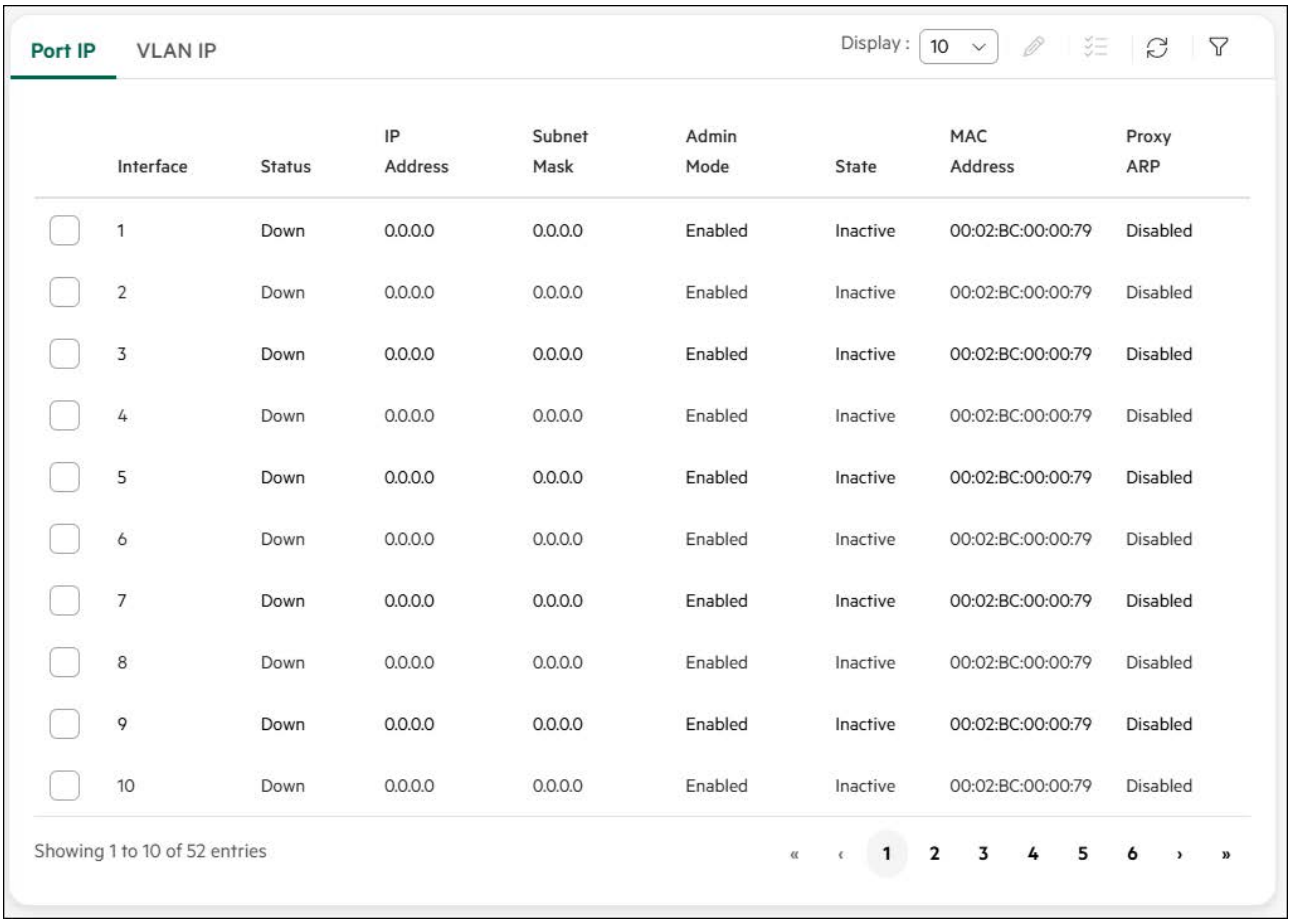


Table 121. Port/VLAN IP Fields

Field	Description
Interface/VLAN ID	The interface or VLAN associated with the rest of the data in the row. When viewing information about the routing settings for an interface, this field identifies the interface or VLAN being viewed.
Status	Indicates whether the interface or VLAN is capable of routing IP packets (Up) or cannot route packets (Down). For the status to be Up, the routing mode and administrative mode for the interface must be enabled. Additionally, the interface must have an IP address and be physically up (active link).
IP Address	The IP address of the interface or VLAN.
Subnet Mask	The IP subnet mask for the interface or VLAN (also known as the network mask or netmask). It defines the portion of the interface's IP address that is used to identify the attached network.
Admin Mode	The administrative mode of the interface or VLAN, which is either Enabled or Disabled.

Field	Description
State	This field is only available in the Port IP tab. The state of the interface, which is either Active or Inactive. An interface is considered active if the link is up, and the interface is in a forwarding state.
MAC Address	The burned-in physical address used for routing traffic on this interface. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
Proxy ARP	Indicates whether proxy ARP is enabled or disabled on the interface. When proxy ARP is enabled, the interface can respond to an ARP request for a host other than itself. An interface can act as an ARP proxy if it is aware of the destination and can route packets to the intended host, which is on a different subnet than the host that sent the ARP request.

To edit an interface, select the Port IP or VLAN IP in the tile and then click (**Edit**).

Figure 144. Edit Routing Interface Configuration Dialog Box

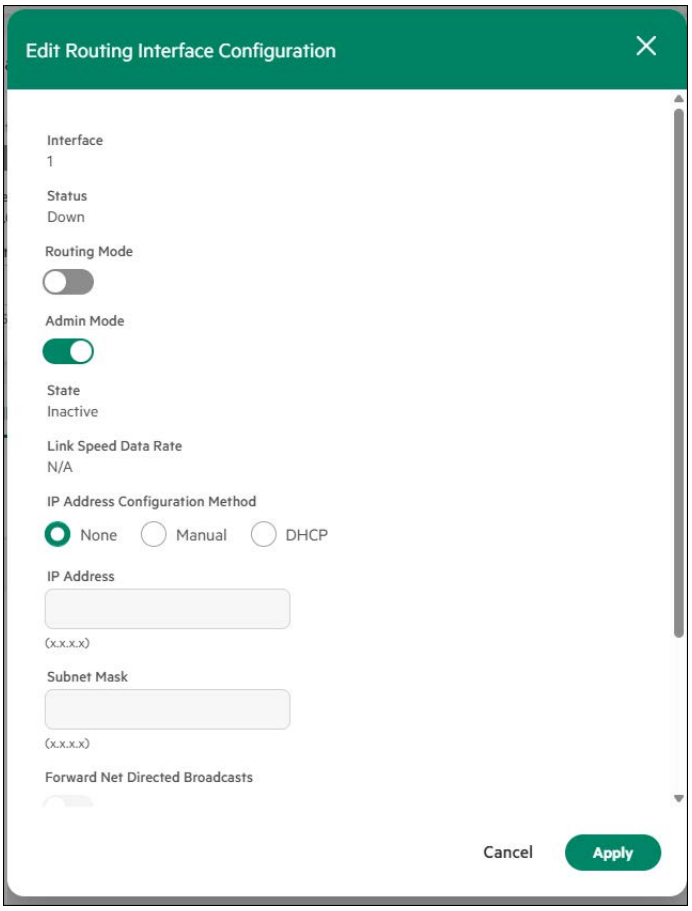


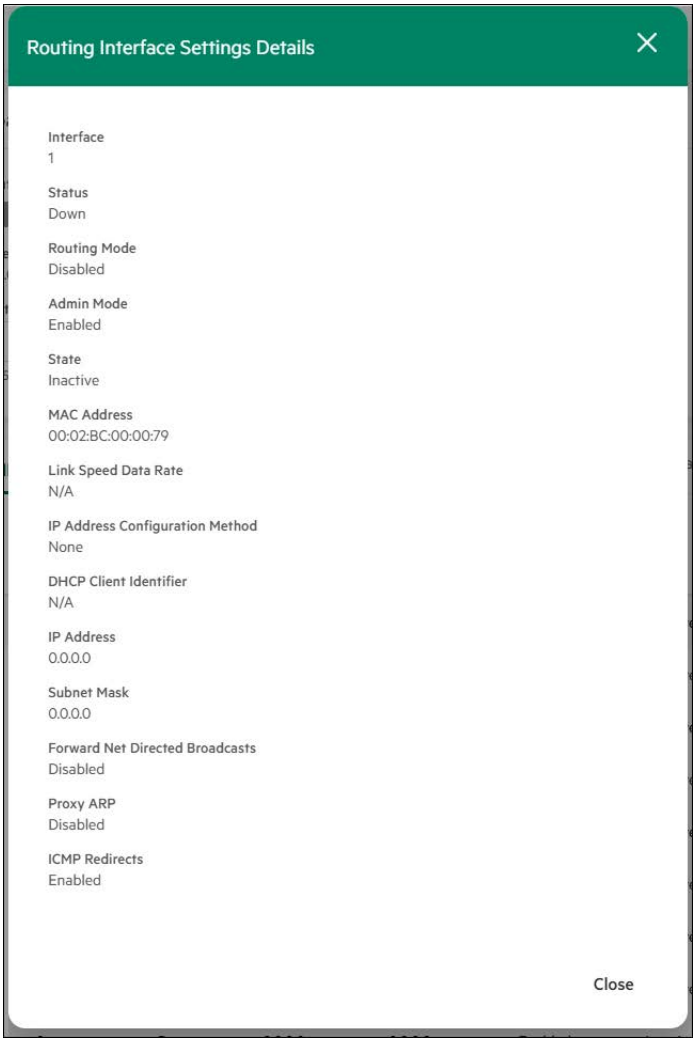
Table 122. Edit Routing Interface Configuration Fields

Field	Description
Interface/VLAN ID	The selected interface, or VLAN ID, that is being edited.
Status	Indicates whether the interface is currently capable of routing IP packets (Up) or cannot route packets (Down). For the status to be Up, the routing mode and administrative mode for the interface must be enabled. Additionally, the interface must have an IP address and be physically up (active link).
Routing Mode	The administrative mode of IP routing on the interface.

Field	Description
Admin Mode	The administrative mode of the interface. If a port interface is administratively disabled, it cannot forward traffic. If a VLAN interface is administratively disabled the VLAN forwards only L2 traffic.
State	Displays the state of the interface, which is either Active or Inactive. An interface is considered active if the link is up, and the interface is in a forwarding state. This field is not displayed for VLAN ID.
Link Speed Data Rate	Displays the physical link data rate of the interface.
IP Address Configuration Method	The method to use for configuring an IP address on the interface, which can be one of the following: · None—No address is to be configured. · Manual—The address is to be statically configured. When this option is active you can specify the IP address and subnet mask in the available fields. · DHCP—The interface will attempt to acquire an IP address from a network DHCP server.
IP Address	The IP address of the interface. This field can be configured only when the selected IP Address Configuration Method is Manual. If the method is DHCP, the interface attempts to lease an IP address from a DHCP server on the network, and the IP address appears in this field (read-only) after it is acquired. If this field displays IP address of 0.0.0.0, the IP Address Configuration Method might be None, or the method might be DHCP and the interface is unable to lease an address.
Subnet Mask	The IP subnet mask for the interface (also known as the network mask or netmask). This field can be configured only when the selected IP Address Configuration Method is Manual.
Forward Net Directed Broadcasts	Determines how the interface handles network-directed broadcast packets. A network-directed broadcast is a broadcast directed to a specific subnet. If this option is activated, network directed broadcasts are forwarded. If this option is clear, network directed broadcasts are dropped. This setting is available only if the IP Address Configuration Method is manual.
Proxy ARP	When this option is active, proxy ARP is enabled, and the interface can respond to an ARP request for a host other than itself. An interface can act as an ARP proxy if it is aware of the destination and can route packets to the intended host, which is on a different subnet than the host that sent the ARP request. This setting is available only if the IP Address Configuration Method is manual.
ICMP Redirects	When this option is active, the interface is allowed to send ICMP Redirect messages. An ICMP Redirect message notifies a host when a better route to a particular destination is available on the network segment. This setting is available only if the IP Address Configuration Method is manual.

To view additional routing configuration information for an interface or VLAN, select the option associated with the interface or VLAN and click (**Details**)

Figure 145. Routing Interface Settings Details



The following information describes the fields in the Details dialog box that are not displayed on the Edit Routing Interface Configuration dialog box.

Table 123. Routing Interface Settings Details Fields

Field	Description
MAC Address	The MAC address of the IP interface.
DHCP Client Identifier	The DHCP Client Identifier (Option 61) is used by DHCP clients to specify their unique identifier. DHCP servers use this value to index their database of address bindings. This value is expected to be unique for all clients in an administrative domain. The Client Identifier string is displayed beside the check box once DHCP is enabled on the port on which the Client identifier option is active. This setting is always enabled for an interface that used DHCP to acquire IP address.

Static Routing/Route Table Tile

To display the Static Routing/Route Table tile, click **Routing > IPv4 Routing** in the navigation pane, and scroll down to the **Static Routing/Route Table** tile.

To view the static routing information, click the **Static Routing** tab. To view the routing table information, click the **Route Table** tab.

Static Routing Tab

Use the Static Routing tab to create and display static routes.

Figure 146. Static Routing Tab



Table 124. Static Routing Fields

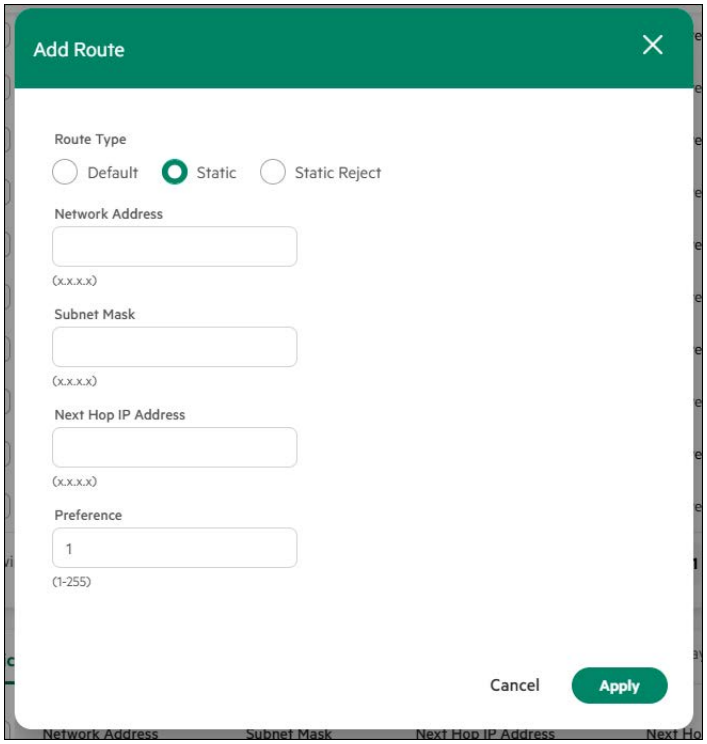
Field	Description
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Next Hop IP Address	The next hop router address to use when forwarding traffic to the destination.
Next Hop Interface	The outgoing interface to use when forwarding traffic to the destination.
Preference	The preferences configured for the added routes.

Adding a Static Route

To add a static route:

1. Click + (**Add**). The Add Route dialog box displays.

Figure 147. Add Route Dialog Box



2. Enter the Route information:
   Select the route type:
   - Default—Configures the gateway to remote networks when no other route in the table matches the destination IP subnet of the traffic. Enter the default gateway address in the Next Hop IP Address field and optionally change the Preference field.

     The Network Address and Subnet Mask fields are grayed out and will be updated with the value of 0.0.0.0 after clicking the APPLY button.
   - Static—Configures the Next Hop for traffic with a matching destination IP subnet. Enter values for Network Address, Subnet Mask, Next Hop IP Address, and Preference.
   - Static Reject—Packets to these destinations will be dropped.

   The route type you select determines the fields available on the page.
3. Click **Apply**.

The new route is added to the **Static Routing/Route Table** tab.

Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

To remove one or more configured routes, select each route to delete and click 🗑 (**Remove**).

Route Table Tab

The route table manager collects routes from multiple sources, including static routes and local routes. The route table manager might learn multiple routes to the same destination from multiple sources. The route table displays only the most preferred route to each destination.

To display the Route Table page, click **Routing > Routing Configuration** in the navigation pane, scroll down to the **Static Routing/Route Table** tile, and click the **Route Table** tab.

Figure 148. Route Table Tab



Table 125. Route Table Fields

Field	Description
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Protocol	This field tells which protocol created the specified route. The possibilities are one of the following: · Local · Static · Default
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly-attached network.
Next Hop Interface	The outgoing interface to use when forwarding traffic to the destination. For a static reject route, the next hop is Null.
Best Route	Indicates whether the route is the preferred route to the network. If the field is blank, a better route to the same network exists in the routing table.

Click (**Refresh**) to update the information on the screen.

IP Routing Statistics/ICMP Statistics Tile

To display the IP Routing/ICMP Statistics tile, click **Routing > IPv4 Routing** in the navigation pane, and scroll down to the IP Routing Statistics/ICMP Statistics tile.

To view the IP Routing Statistics, click the IP Routing Statistics tab. To view the ICMP Statistics, click the ICMP Statistics tab.

To reset all statistics to 0, click **Clear Counters**. Clicking this button clears the counters on the IP Routing and ICMP Statistics tabs.

IP Routing Statistics Tab

The IP Routing Statistics tab displays the IPv4 routing counter information the switch has collected since the counters were cleared or the switch was reset.

Figure 149. IP Routing Statistics Tab

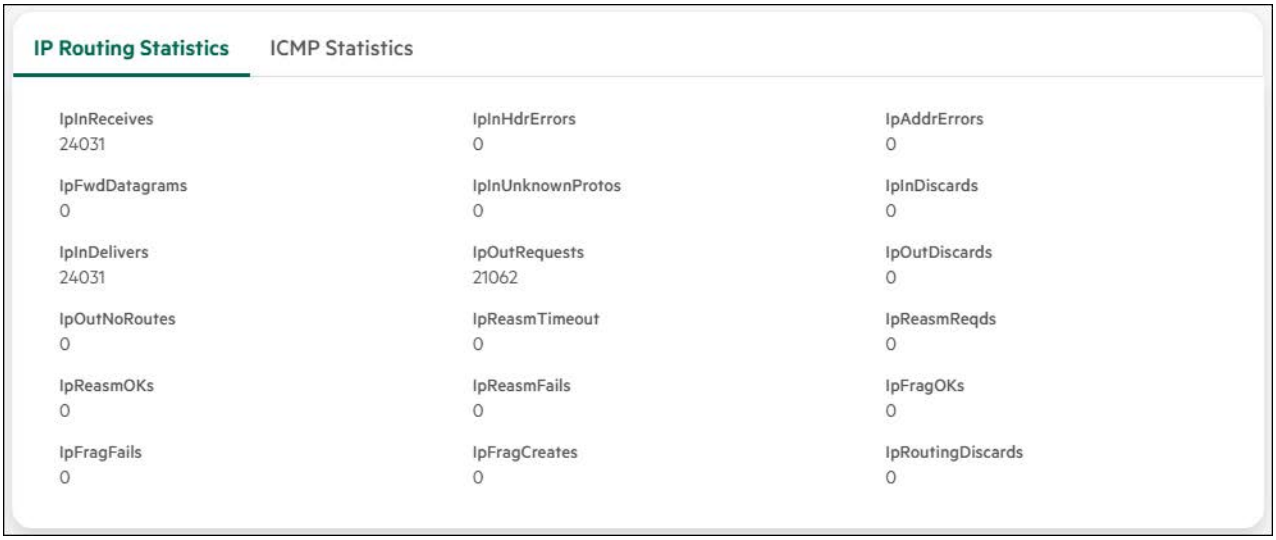


Table 126. IP Routing Statistics Fields

Field	Description
IpInReceives	The total number of input datagrams received from interfaces, including those received in error.
IpInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
IpInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
IpFowdDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter includes only those packets which were Source-Routed through this entity, and the Source-Route option processing was successful.
IpInUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

Field	Description
IpInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
IpInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
IpOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
IpOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
IpOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this `no-route' criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
IpReasmTimeout	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
IpReasmReqds	The number of IP fragments received which needed to be reassembled at this entity.
IpReasmOKs	The number of IP datagrams successfully re-assembled.
IpReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.
IpFragOKs	The number of IP datagrams that have been successfully fragmented at this entity.
IpFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.
IpFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
IpRoutingDiscards	The number of routing entries that were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.

ICMP Statistics Tab

The ICMP Statistics tab displays the ICMP counter information the switch has collected since the counters were cleared or the switch was reset.

Figure 150. ICMP Statistics Tab

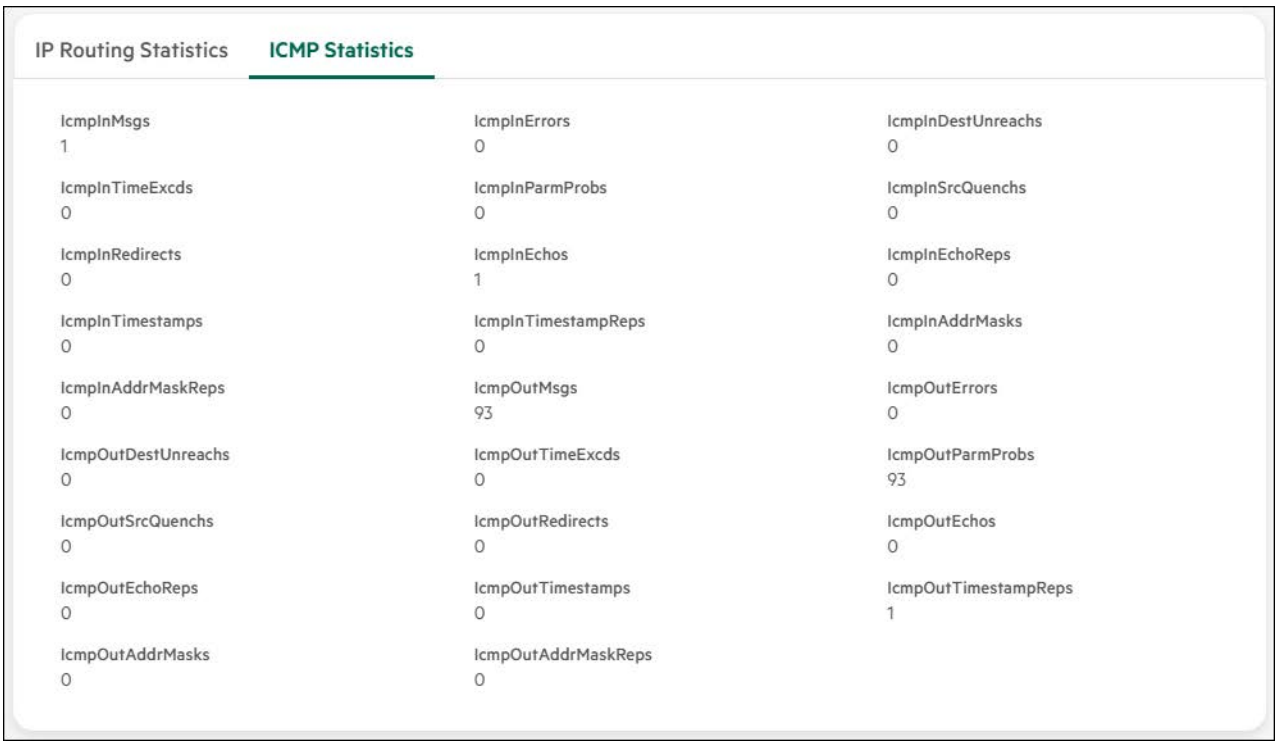


Table 127. ICMP Statistics Fields

Field	Description
IcmpInMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.
IcmpInErrors	The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
IcmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
IcmpInTimeExcds	The number of ICMP Time Exceeded messages received.
IcmpInParmProbs	The number of ICMP Parameter Problem messages received.
IcmpInSrcQuenchs	The number of ICMP Source Quench messages received.
IcmpInRedirects	The number of ICMP Redirect messages received.
IcmpInEchos	The number of ICMP Echo (request) messages received.
IcmpInEchoReps	The number of ICMP Echo Reply messages received.
IcmpInTimestamps	The number of ICMP Timestamp (request) messages received.
IcmpInTimestampReps	The number of ICMP Timestamp Reply messages received.
IcmpInAddrMasks	The number of ICMP Address Mask Request messages received.
IcmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
IcmpOutMsgs	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.

Field	Description
IcmpOutErrors	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
IcmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
IcmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
IcmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
IcmpOutSrcQuenchs	The number of ICMP Source Quench messages sent.
IcmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object is always zero, since hosts do not send redirects.
IcmpOutEchos	The number of ICMP Echo (request) messages sent.
IcmpOutEchoReps	The number of ICMP Echo Reply messages sent.
IcmpOutTimestamps	The number of ICMP Timestamp (request) messages.
IcmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
IcmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
IcmpOutAddrMasksReps	The number of ICMP Address Mask Reply messages sent.

DHCP Relay

HPE Networking Instant On 1940 Switch Series switches can be used to relay packets between a DHCP client and server on different subnets. The switch acts as an L3 relay agent and must have an IP interface on the client subnets and, if it does not have an IP interface on the server's subnet, it should be able to route traffic toward the server's subnet.

Use the DHCP Relay page to enable the DHCP relay feature on the switch and to view and configure information about DHCP servers where packets should be relayed.

To display the DHCP Relay page, click **Routing** > **DHCP Relay** in the navigation pane.

Global Configuration

Use the Global Configuration tab to administratively enable or disable DHCP relay on the switch.

Figure 151. DHCP Relay Global Configuration Tile

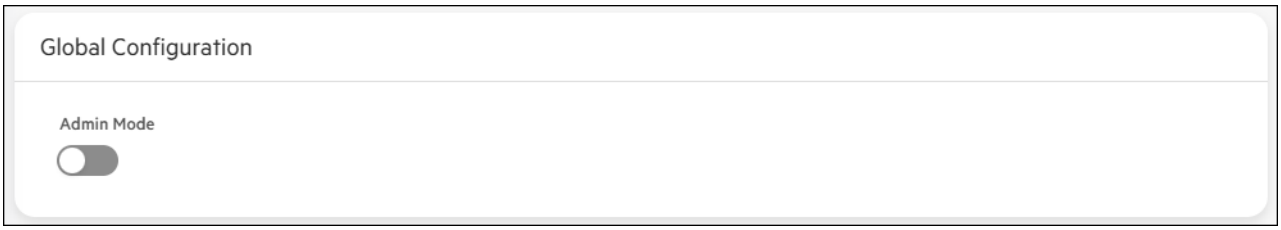


Table 128. DHCP Relay Global Configuration Field

Field	Description
Admin Mode	The global mode of DHCP L3 relay on the device.

If you change the administrative mode of the feature, click **Apply** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Server Configuration

Use the Server Configuration tile to view and configure information about DHCP servers where packets should be relayed.

Figure 152. Server Configuration Tile

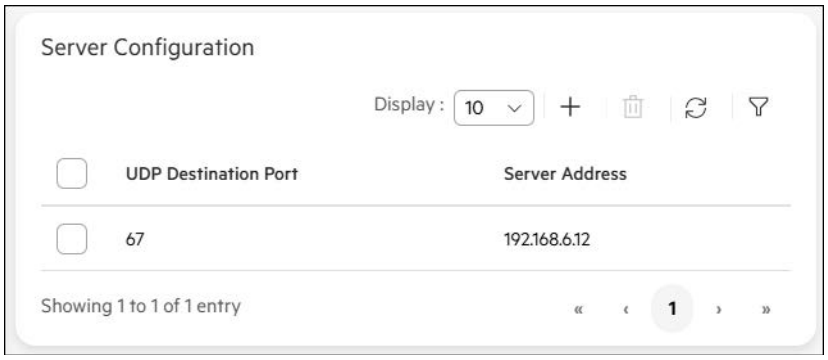
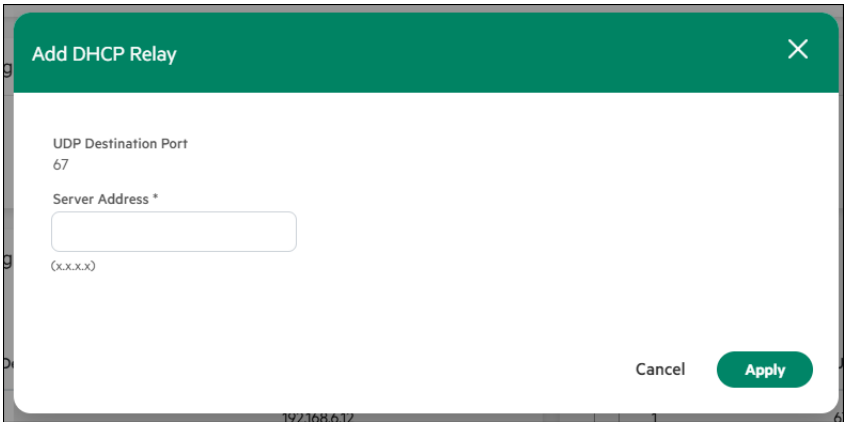


Table 129. Server Configuration Fields

Field	Description
UDP Destination Port	The destination UDP port number of UDP packets to be relayed.
Server Address	The IPv4 address of the server to which packets are relayed for the specific UDP Destination Port.

To add a DHCP server to which packets are relayed, click + (**Add**) to open the Add DHCP Relay dialog box, specify the IP address of the DHCP server, and click **Apply**.

Figure 153. Add DHCP Relay Dialog Box



To remove one or more configured DHCP relay servers, select each entry to remove and click (**Remove**).

DHCP Relay Interfaces

Use the DHCP Relay Interfaces tile to add, view, or delete the DHCP relay configuration on a selected routing interface.

NOTE

DHCP relay can be configured on an VLAN or interface only if it is enabled for routing. To enable routing on an interface or VLAN, see Port IP and VLAN IP.

Figure 154. DHCP Relay Interfaces Tile

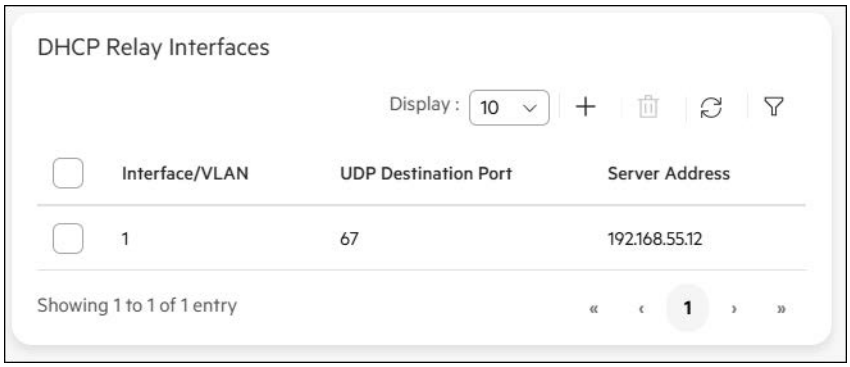
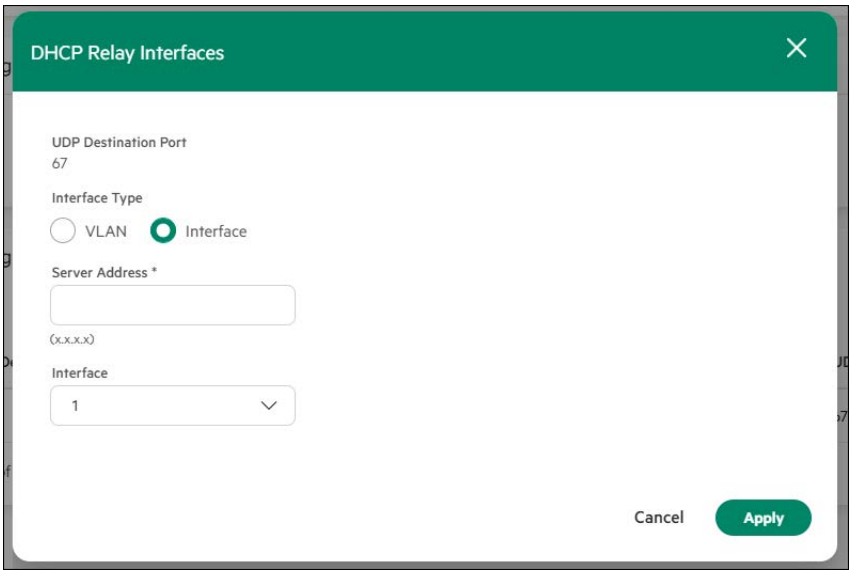


Table 130. DHCP Relay Interfaces Fields

Field	Description
Interface/VLAN	The routing interface or VLAN that has the DHCP relay feature configured.
UDP Destination Port	The destination UDP port number of UDP packets to be relayed.
Server Address	The IPv4 address of the server to which packets are relayed for the specific UDP Destination Port.

To configure an interface or VLAN that can relay DHCP packets to a DHCP server, click + (**Add**) to open the Add DHCP Relay Interface dialog box. Select the type of routing interface and specify the IP address of the DHCP server. Select the DHCP relay interface or VLAN from the drop-down menu. If no interfaces or VLANs or listed, then no interfaces or VLANs are enabled for routing, and click **Apply**.

Figure 155. Add DHCP Relay Dialog Box



To remove the DHCP relay capabilities from one or more VLANs or interfaces, select each entry to remove and click (**Remove**).

ARP Table

The Address Resolution Protocol (ARP) associates a layer 2 MAC address with a layer 3 IPv4 address.

Switch software features both dynamic and manual ARP configuration. With manual ARP configuration, you can add static entries into the ARP table.

If the ARP table is full, new entries are rejected, and an appropriate Syslog message is generated.

The number of supported ARP entries is 509. To dynamically add an ARP entry for a new station, the switch sends an ARP request. Up to 3 requests are sent with an interval of 3 seconds between them.

If an entry related to a host station times out, it is removed from the table.

If an entry related to a router or gateway ages out, the switch sends an ARP request for an entry IP address and only if there is no response, the entry is removed from the ARP table.

To display the ARP Table page, click **Routing** > **ARP Table** in the navigation pane.

Global Configuration

Use the Global Configuration tile to configure the global ARP table settings.

Figure 156. ARP Table Global Configuration Tile



Table 131. ARP Table Global Configuration Fields

Field	Description
Age Time	The amount of time, in seconds, that a dynamic ARP entry remains in the ARP table before aging out. The valid range is 15 to 21600. The default is 1200.
Response Time	The amount of time, in seconds, that the device waits for an ARP response to an ARP request that it sends.
Retries	The maximum number of times an ARP request will be retried after an ARP response is not received. The number includes the initial ARP request.
Cache Size	The maximum number of entries allowed in the ARP table. This number includes all static and dynamic ARP entries.
Dynamic Renew	When selected, this option allows the ARP component to automatically attempt to renew dynamic ARP entries when they age out.

Static ARP Table

Use the Static ARP Table tile to add static ARP entry to the ARP table and to view existing entries.

Figure 157. Static ARP Table Tile



Table 132. Static ARP Table Fields

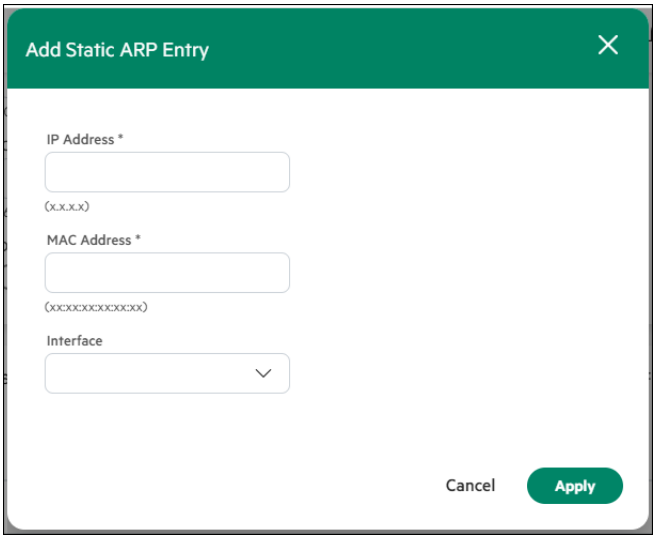
Field	Description
IP Address	The IP address of a network host on a subnet attached to one of the switch's routing interfaces. When adding a static ARP entry, specify the IP address for the entry after you click **Add**.
MAC Address	The unicast MAC address (hardware address) associated with the network host. When adding a static ARP entry, specify the MAC address to associate with the IP address in the entry.
Interface	The routing interface associated with the ARP entry. The network host is associated with the switch through this interface. When adding a static ARP entry, specify the interface to associate with this entry.
Type	The ARP entry type in this table is Static, which is an ARP entry configured by the user

Adding a Static ARP Entry

To add a static ARP entry:

1. Click + (**Add**) to open the Add Static ARP Entry dialog box.

Figure 158. Add Static ARP Entry Dialog Box



2. Specify the IP address and its associated MAC address.
3. Specify the interface (VLAN or Port) to associate to this static entry.
4. Click **Apply**.

Removing a Static ARP Entry

To delete one or more static ARP entries, select each entry to delete and click (**Remove**).

ARP Table Summary

The ARP Table Summary tile displays entries in the ARP table that are not statically configured.

Figure 159. ARP Table Summary Tile



Table 133. ARP Table Summary Fields

Field	Description
IP Address	The IP address of a network host on a subnet attached to one of the device's routing interfaces.
MAC Address	The unicast MAC address (hardware address) associated with the network host. When adding a static ARP entry, specify the MAC address to associate with the IP address in the entry.
Interface	The routing interface associated with the ARP entry. The network host is associated with the device through this interface.
Type	The ARP entry type: · Dynamic—An ARP entry that has been learned by the router · Local—An ARP entry associated with the MAC address of a routing interface on the device
Age	The age of the entry since it was last learned or refreshed. This value is specified for Dynamic or Gateway entries only (it is left blank for all other entry types).

ARP Table Statistics

The ARP Table Statistics tile displays information about the number and type of entries in the system ARP table. The ARP table contains entries that map IP addresses to MAC addresses.

Figure 160. ARP Table Statistics Tile

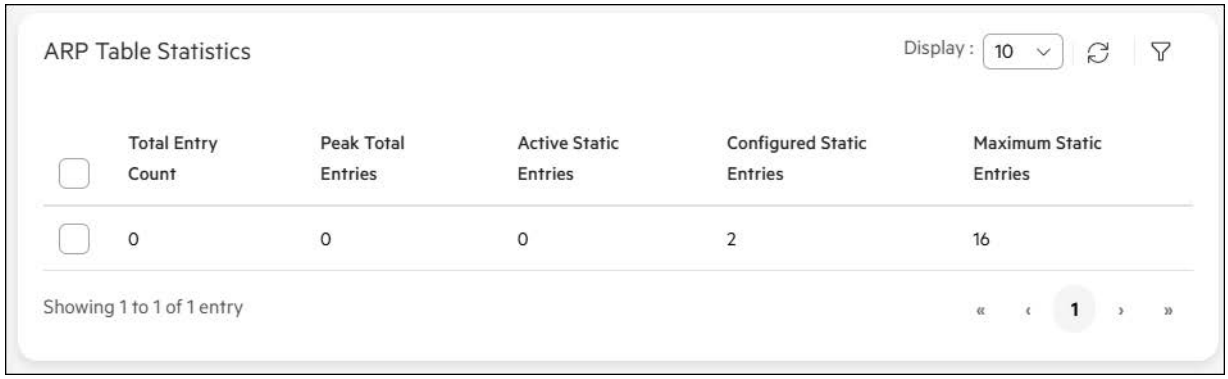


Table 134. ARP Table Statistics Fields

Field	Description
Total Entry Count	The total number of entries currently in the ARP table. The number includes both dynamically learned entries and statically configured entries.
Peak Total Entries	The highest value reached by the Total Entry Count. This value is reset whenever the ARP table Cache Size configuration parameter is changed.
Active Static Entries	The total number of active ARP entries in the ARP table that were statically configured. After a static ARP entry is configured, it might not become active until certain other routing configuration conditions are met.
Configured Static Entries	The total number of static ARP entries that are currently in the ARP table. This number includes static ARP entries that are not active.
Maximum Static Entries	The maximum number of static ARP entries that can be configured in the ARP table.

Use the Quality of Service (QoS) pages to configure Access Control Lists (ACLs) and Class of Service (CoS) on the switch.

Access Control Lists

ACLs ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and above all provide security for the network.

HPE Networking Instant On 1940 Switch Series switches support IPv4 and MAC ingress and egress ACLs. The maximum number of ACLs is 100. The maximum number of rules, known as access control entries (ACEs) is 2048.

To configure an ACL:

1. Create an IPv4-based or MAC-based rule and assign a unique ACL ID (see Access Control Lists).
2. Define the rules, which can identify protocols, source and destination IP and MAC addresses, and other packet-matching criteria (see IPv4 ACL Rules and MAC ACL Rules).
3. Use the ID number to assign the ACL to a port or to a VLAN interface (see Associating an ACL with an Interface or VLAN).

To display the Access Control List page, click **Quality of Service > Access Control Lists** in the navigation pane.

Access Control Lists

Use the Access Control Lists tile to add or remove ACLs, and to view information about the MAC and IP ACLs configured on the switch.

Figure 161. Access Control Lists Tile



Table 135. Access Control List Fields

Field	Description
ACL Name	The name that identifies the ACL, 1-255 characters, case sensitive.
ACL Type	The type of ACL. The ACL type determines the criteria that can be used to match packets. The type also determines which attributes can be applied to matching traffic. IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic, and MAC ACLs classify Layer 2 traffic. These are the ACL types: · IPv4 Named—Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv4 packets. · MAC—Match criteria can be based on the source and destination MAC addresses, 802.1p user priority, VLAN ID, and EtherType value within Ethernet frames
Direction	Indicates whether the packet is checked against the rules in an ACL when it is received on an interface (Inbound) or after it has been received, routed, and is ready to exit an interface (Outbound).
Rules	The number of rules currently configured for the ACL
Bound Interfaces	The interface(s) to which the ACL has been applied.
Bound VLANs	Each VLAN to which the ACL has been applied.

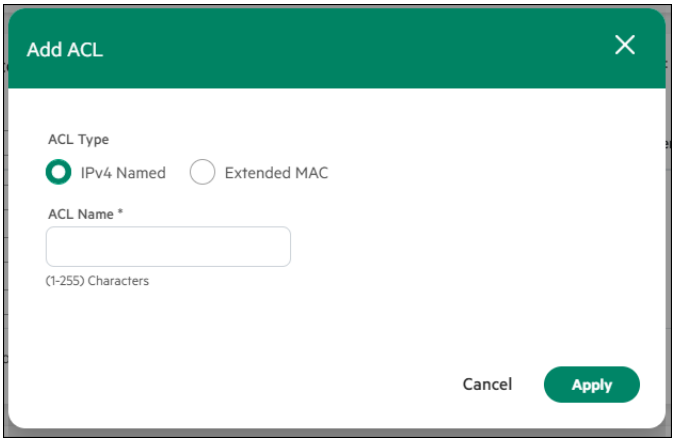
Click **Apply** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Adding an ACL

To add an ACL:

1. Click + (**Add**) to open the Add ACL dialog box.

Figure 162. Add ACL Dialog Box



2. Select the type of ACL to add.
3. Specify the name of the ACL.
4. Click **Apply**.

Removing an ACL

To delete one or more ACLs, select each entry to delete and click (**Remove**).

IPv4 ACL Rules and MAC ACL Rules Tile

The IPv4 ACL Rules/MAC ACL Rules tile enables adding and editing rules to ACLs created by users.

To view, add, or edit IPv4 ACL rules, click the **IPv4 ACL Rules** tab.

To view, add, or edit MAC ACL rules, click the **MAC ACL Rules** tab.

IPv4 ACL Rules and MAC ACL Rules

Use the IPv4 ACL Rules tab to configure rules for IPv4 ACLs on the system and to view summary information about the rules that have been added to an ACL. Use the MAC ACL Rules tab to configure rules for MAC ACLs on the system and to view summary information about the rules that have been added to an ACL.

Each ACL rule is configured to match one or more aspects of traffic on the network. When a packet matches the conditions in a rule, it is handled according to the configured action (permit or deny) and attributes. Each ACL can have multiple rules, but the final rule for every ACL is an implicit deny all rule. For each rule, a packet must match all the specified criteria in order for the specified rule action (Permit/ Deny) to take place.

Figure 163. IPv4 ACL Rules Tab



Table 136. IPv4 ACL Rules and MAC ACL Rules Fields

Field	Description
ACL Name	The menu contains the name of each ACL that exists on the system. Before you add or remove a rule, you must select the name of the ACL from the menu.
Sequence Number	The number that indicates the position of a rule within the ACL. The rules are displayed based on their position within the ACL, but can also be renumbered. Packets are checked against the rule criteria in order, from the lowest-numbered rule to the highest. When the packet matches the criteria in a rule, it is handled according to the rule action and attributes. If no rule matches a packet, the packet is discarded based on the implicit deny all rule, which is the final rule in every ACL.
Action	The action to take when a packet or frame matches the criteria in the rule: · Permit—The packet or frame is forwarded. · Deny—The packet or frame is dropped.
Match Conditions	The criteria used to determine whether a packet or frame matches the ACL rule.
Rule Attributes	Each action — beyond the basic Permit and Deny actions — to perform on the traffic that matches the rule.

Adding a Rule to an IPv4 ACL

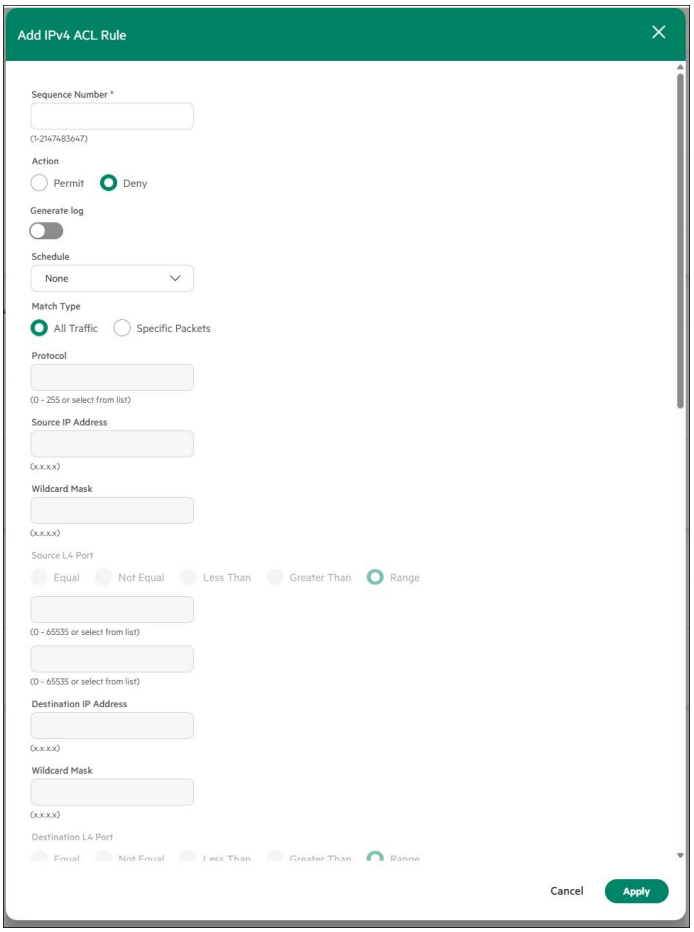
To add a rule to an IPv4 ACL:

1. From the IPv4 ACL Rules tab, click the ACL Name drop-down menu to select the IPv4 ACL to configure.
2. Click + (**Add**) to open the IPv4 ACL Rule dialog box.

NOTE

The following figure does not show all fields available in the Add IPv4 ACL Rule dialog box.

Figure 164. Add IPv4 ACL Rule Dialog Box



3. Specify a sequence number to indicate the position of a rule within the ACL.
4. Specify the action for the rule:
   - Permit—The packet or frame is forwarded.
   - Deny—The packet or frame is dropped.
5. To create a log of the ACL, enable the Generate Log option. If enabled, the switch sends an informational syslog message if an incoming packet matches the entry.
6. Select the appropriate schedule from the drop-down list.
7. Specify the match criteria and rule attributes shown in Table 137.
8. Click **Apply**.

Table 137. Add IPv4 ACL Rule Dialog Box with IPv4 ACL Match Criteria and Rule Attributes

Field	Description
Sequence Number	The number that indicates the position of a rule within the ACL. The rules are displayed based on their position within the ACL, but can also be renumbered. Packets are checked against the rule criteria in order, from the lowest-numbered rule to the highest. When the packet matches the criteria in a rule, it is handled according to the rule action and attributes. If no rule matches a packet, the packet is discarded based on the implicit deny all rule, which is the final rule in every ACL.
Action	The action to take when a packet or frame matches the criteria in the rule: · Permit—The packet or frame is forwarded. · Deny—The packet or frame is dropped.
Generate log	If enabled, the switch sends an informational SYSLOG message when an incoming packet matches the entry.
Schedule	Select the schedule to control the time ranges when the ACL is active. You can configure schedules on the Schedule Configuration page.
IPv4 ACL Match Criteria	
Match Type	Specify which traffic to match: · All Traffic—When this option is selected, all packets will match the rule and will be either permitted or denied. This option is exclusive to all other match criteria, so if All Traffic is selected, no other match criteria can be configured. · Specific Packets—Select this option to configure the match criteria on the ACL.
Protocol	The IANA-assigned protocol number to match within the IP packet. You can also specify one of the keywords provided in the drop-down menu.
Source IP Address / Wildcard Mask	The source IP address in the packet and source IP wildcard mask (in the second field) to compare to the IP address in a packet header. Wildcard masks determines which bits in the IP address are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that all bits are ignored. A wildcard of 0.0.0.0 indicates that no bit is ignored. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A '1' in a bit position of the ACL mask indicates the corresponding bit can be ignored. This field is required when you configure a source IP address.
Source L4 Port	The TCP/UDP source port to match in the packet header. The Source L4 Port and Destination L4 port are configurable only if the protocol is either TCP or UDP. User can select port ID from the range 0-65535, or select predefined protocols. These are predefined protocols available for TCP: BGP, Domain, Echo, FTP, FTP-Data, HTTP, SMTP, Telnet, POP2, or POP3. For UDP protocol: Domain, Echo, NTP, RIP, SNMP, TFTP, Time, or WHO.
Destination IP Address / Wildcard Mask	The destination IP address in the packet and destination IP wildcard mask (in the second field) to compare to the IP address in a packet header. Wildcard masks determines which bits in the IP address are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all of the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A 1 in a bit position of the ACL mask indicates the corresponding bit can be ignored. This field is required when you configure a destination IP address.
Destination L4 Port	The TCP/UDP destination port to match in the packet header. The Source L4 Port and Destination L4 port are configurable only if the protocol is either TCP or UDP. User can select port ID from the range 0-65535, or select predefined protocols. These are predefined protocols available for TCP: BGP, Domain, Echo, FTP, FTP-Data, HTTP, SMTP, Telnet, POP2, or POP3. For UDP protocol: Domain, Echo, NTP, RIP, SNMP, TFTP, Time, or WHO.

Field	Description
IGMP Type	IP ACL rule to match on the specified IGMP message type. This option is available only if the protocol is IGMP.
ICMP Message	IP ACL rule to match on the ICMP message type and code. Specify one of the following supported ICMP messages: Echo, Echo-Reply, Host-Redirect, Mobile-Redirect, Net-Redirect, Net-Unreachable, Redirect, Packet-Too-Big, Port-Unreachable, Source-Quench, Router-Solicitation, Router-Advertisement, Time-Exceeded, TTL-Exceeded, and Unreachable. This option is available only if the protocol is ICMP.
ICMP Type	IP ACL rule to match on the specified ICMP message type. This option is available only if the protocol is ICMP.
ICMP Code	IP ACL rule to match on the specified ICMP message code. This option is available only if the protocol is ICMP.
TCP Flags	IP ACL rule to match on the TCP flags. When a + flag is specified, a match occurs if the flag is set in the TCP header. When a - flag is specified, a match occurs if the flag is not set in the TCP header. These are the available options: FIN, SYN, RST, PSH, ACK, URG. This option is available only if the protocol is TCP.
Service Type	The service type to match in the IP header. The options in this menu are alternative ways of specifying a match condition for the same Service Type field in the IP header, but each service type uses a different user notation. After you select the service type, specify the value for the service type in the appropriate field. Only the field associated with the selected service type can be configured. The services types are as follows: · IP DSCP—Matches the packet IP DiffServ Code Point (DSCP) value to the rule. The DSCP value is defined as the high-order six bits of the Service Type octet in the IP header. · IP Precedence—Matches the IP Precedence value to the rule. The IP Precedence field in a packet is defined as the high-order three bits of the Service Type octet in the IP header.
IPv4 ACL Rule Attributes	
Assign Queue	The number (0 to 3) that identifies the hardware egress queue that handles all packets matching this rule.
Flow Action	The traffic flow action used: · Unchanged—The flow is unchanged. · Redirect—Allows traffic that matches a rule to be redirected to the selected interface instead of being processed on the original port. The redirect function and mirror function are mutually exclusive. · Mirror—Provides the ability to mirror traffic that matches a rule to the selected interface. Mirroring is similar to the redirect function, except that in flow-based mirroring a copy of the permitted traffic is delivered to the mirror interface while the packet itself is forwarded normally through the switch.
Interface	The interface to use for the flow action.
Committed Rate	The allowed transmission rate for frames on the interface. Range: 1 to 4294967295 kbit/s.
Burst Size	The number of bytes allowed in a temporary traffic burst. Range: 1 –128 Bytes.

To remove one or more rules from an ACL, select each entry to remove and click (**Remove**).

Adding a Rule to an MAC ACL

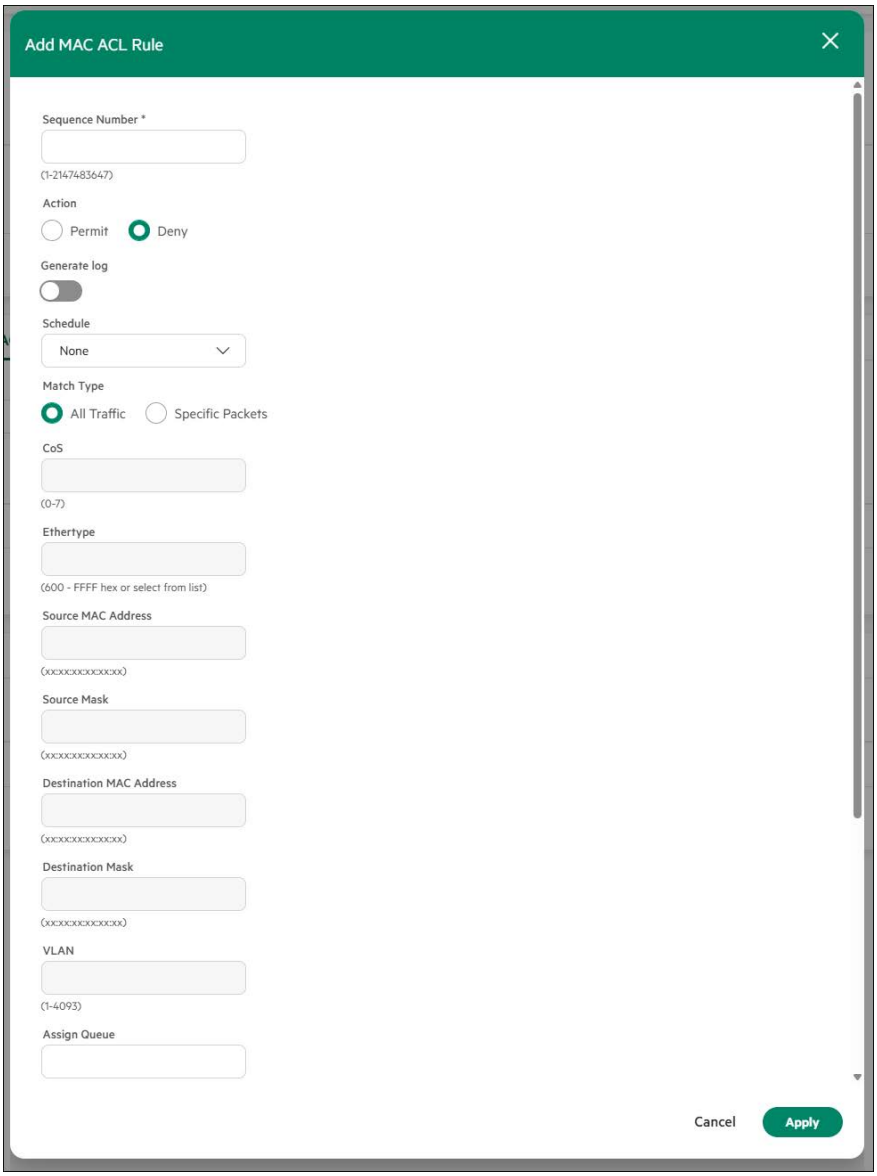
To add a rule to an MAC ACL:

1. From the MAC ACL Rules tab, click the ACL Name drop-down button and select the name of the MAC ACL to configure.
2. Click + (**Add**) to open the MAC ACL Rule dialog box.

NOTE

The following figure does not show all fields available in the Add MAC ACL Rule dialog box.

Figure 165. Add MAC ACL Rule Dialog Box



3. Specify a sequence number to indicate the position of a rule within the ACL.
4. Specify the action for the rule:
   - Permit—The packet or frame is forwarded.
   - Deny—The packet or frame is dropped.

5. To create a log of the ACL, enable Generate Log. If enabled, the switch sends an informational syslog message when an incoming packet matches the entry.
6. Select the appropriate Schedule from the drop-down list.
7. Specify the match criteria and rule attributes shown in Table 138.
8. Click **Apply**

Table 138. Add MAC ACL Rule and MAC ACL Match Criteria

Field	Description
Sequence Number	The number that indicates the position of a rule within the ACL. The rules are displayed based on their position within the ACL, but can also be renumbered. Packets are checked against the rule criteria in order, from the lowest-numbered rule to the highest. When the packet matches the criteria in a rule, it is handled according to the rule action and attributes. If no rule matches a packet, the packet is discarded based on the implicit deny all rule, which is the final rule in every ACL.
Action	The action to take when a packet or frame matches the criteria in the rule: · Permit—The packet or frame is forwarded. · Deny—The packet or frame is dropped.
Generate log	If enabled, the switch sends an informational SYSLOG message if an incoming packet matches the entry.
Schedule	Select the schedule to control the time ranges when the ACL is active. You can configure schedules on the Schedule Configuration page.
Match Criteria	
Match Type	The type of traffic for the rule to match: · All Traffic—When this option is selected, all packets will match the rule and will be either permitted or denied. This option is exclusive to all other match criteria, so if All Traffic is selected, no other match criteria can be configured. · Specific Packets—Select this option to configure the match criteria on the ACL.
CoS	The 802.1p user priority value to match within the Ethernet frame. The valid range is 0 to 7. The default is none.
EtherType	The EtherType value to match in an Ethernet frame. Select an option from the drop-down list or specify the number associated with the EtherType range from 600 to FFFF hex (0x0600 to 0xFFFF are also accepted),
Source MAC Address / Mask	The MAC address to match to an Ethernet frame's source port MAC address. If desired, enter the MAC Mask associated with the source MAC to match. The MAC address mask specifies which bits in the source MAC to compare against an Ethernet frame. Use F's and zeros in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a zero in a bit position means that the data must equal the value given for that bit. For example, if the MAC address is aa_bb_cc_dd_ee_ff, and the mask is 00_00_ff_ff_ff_ff, all MAC addresses with aa_bb_xx_xx_xx_xx result in a match (where x is any hexadecimal number).
Destination MAC Address / Mask	The MAC address to match to an Ethernet frame's destination port MAC address. If desired, enter the MAC Mask associated with the destination MAC to match. The MAC address mask specifies which bits in the destination MAC to compare against an Ethernet frame. Use F's and zeros in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a zero in a bit position means that the data must equal the value given for that bit. For example, if the MAC address is aa_bb_cc_dd_ee_ff, and the mask is 00_00_ff_ff_ff_ff, all MAC addresses with aa_bb_xx_xx_xx_xx result in a match (where x is any hexadecimal number).
VLAN	The VLAN ID to match within the Ethernet frame.
MAC ACL Rule Attributes	
Assign Queue	The number (0 to 3) that identifies the hardware egress queue that handles all packets matching this rule.

Field	Description
Flow Action	The traffic flow action used: · Unchanged—The flow is unchanged. · Redirect—Allows traffic that matches a rule to be redirected to the selected interface instead of being processed on the original port. The redirect function and mirror function are mutually exclusive. · Mirror—Provides the ability to mirror traffic that matches a rule to the selected interface. Mirroring is similar to the redirect function, except that in flow-based mirroring a copy of the permitted traffic is delivered to the mirror interface while the packet itself is forwarded normally through the switch.
Interface	The interface to use for the action.
Committed Rate	The allowed transmission rate for frames on the interface. Range: 1 to 4294967295 kbit/s.
Burst Size	The number of bytes allowed in a temporary traffic burst. Range: 1 –128 Bytes.

To remove one or more rules from an ACL, select each entry to remove and click (**Remove**).

Interface and VLAN Configuration Tile

Use this tile to bind an ACL to ports, LAGs or VLANs. Multiple ACLs can be configured on a port or LAG interface. In this case, a sequence number determines the order in which the ACL is applied to traffic, compared to other ACLs configured on the interface. The ACL with the lowest sequence number is applied first, and the other ACLs are applied in ascending numerical order.

To view and configure ACL-to-interface bindings, click the **Interface Configuration** tab.

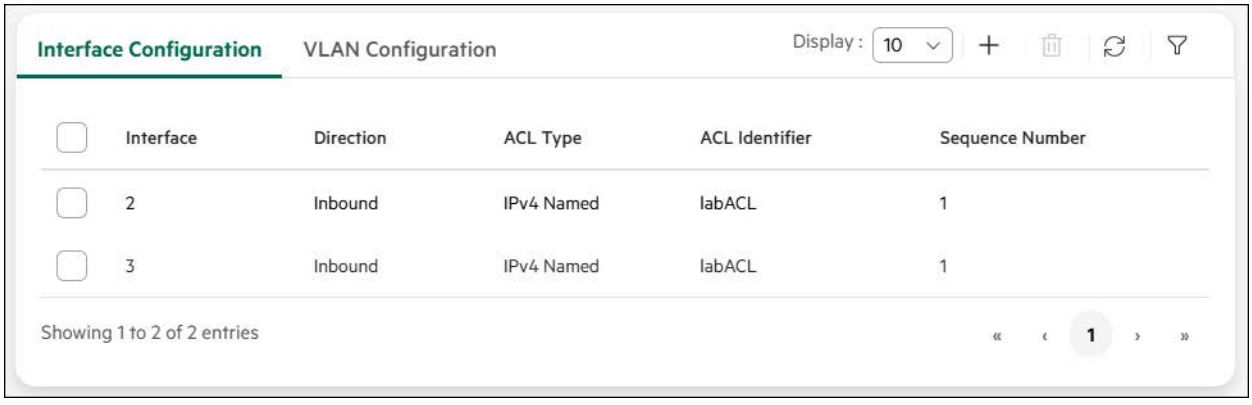
To view and configure ACL-to-VLAN bindings, click the **VLAN Configuration** tab.

Interface Configuration Tab and VLAN Configuration Tab

When binding an ACL to an interface, the user can specify additional Traffic Rule Attributes per each ACL. The Traffic Rule Attributes will be applied only to ACEs with the permit rule.

The following figure shows the Interface Configuration Tab with an IPv4 ACL bound to two interfaces.

Figure 166. Interface Configuration Tab



The following figure shows the VLAN Configuration Tab with a MAC ACL bound to one VLAN.

Figure 167. VLAN Configuration Tab

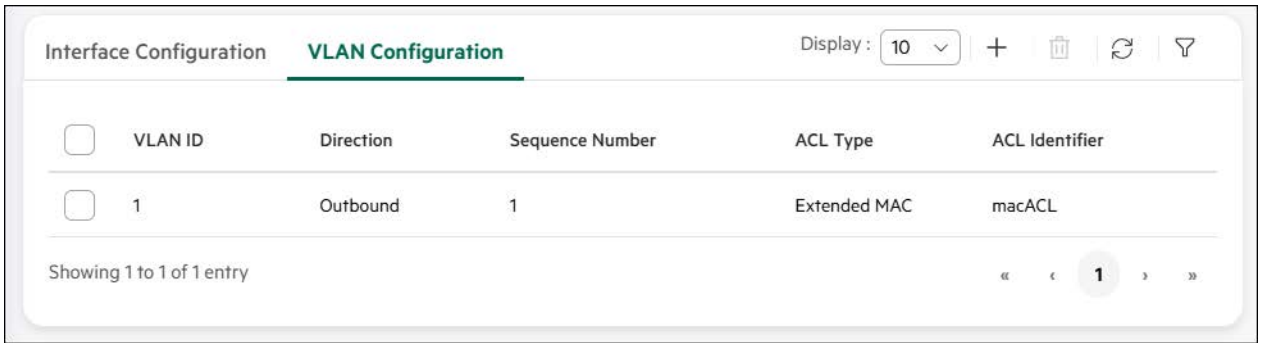


Table 139. Interface Configuration and VLAN Configuration Fields

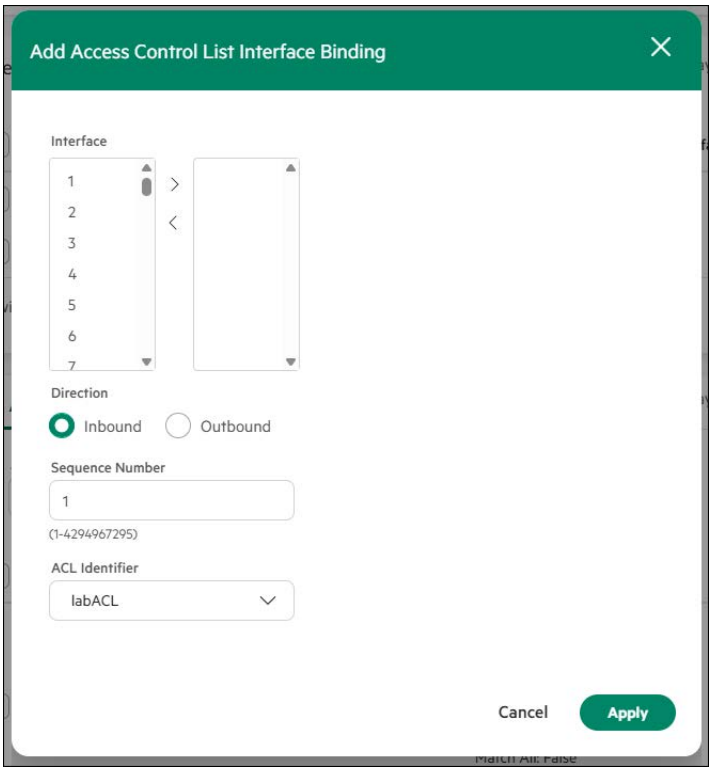
Field	Description
Interface / VLAN	The interface or VLAN that has an associated ACL.
Direction	Indicates whether the packet is checked against the rules in an ACL when it is received on an interface or VLAN (Inbound) or after it has been received, routed, and is ready to exit an interface or VLAN (Outbound).
ACL Type	The type of ACL. The ACL type determines the criteria that can be used to match packets and which attributes can be applied to matching traffic. IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic and MAC ACLs classify Layer 2 traffic. · IPv4 Named—Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv4 packets. · MAC—Match criteria can be based on the source and destination MAC addresses, 802.1p user priority, VLAN ID, and EtherType value within Ethernet frames.
ACL Identifier	The name of the ACL.
Sequence Number	The order the ACL is applied to traffic on the interface or VLAN relative to other ACLs associated with the interface or VLAN in the same direction. When multiple ACLs are applied to the same interface or VLAN in the same direction, the ACL with the lowest sequence number is applied first, and the other ACLs are applied in ascending numerical order.

Associating an ACL with an Interface or VLAN

To apply an ACL to an interface or VLAN:

1. Ensure the correct tab is selected:
   - To apply an ACL to an interface, select the Interface Configuration tab.
   - To apply an ACL to a VLAN, select the VLAN Configuration tab.
2. Click + (**Add**) to display the Add Access Control List Interface/VLAN Binding dialog box.

Figure 168. Access Control List Interface Configuration Dialog Box



3. Select one or more interfaces or VLANs to associate with the ACL.
   To select multiple interfaces or VLANs, Ctrl + click each interface/VLAN, or Shift + click a contiguous set of interfaces/VLANs.
4. Apply the ACL to traffic entering (inbound) the interface or VLAN.
5. Specify a sequence number or leave the field blank to let the switch assign the sequence number.
6. Select the ID of the ACL to associate with the interface or VLAN.
7. Click **Apply**.

Removing an Association Between an ACL and an Interface or VLAN

To remove one or more ACL-interface or ACL-VLAN associations, select each entry to delete and click (**Remove**).

Class of Service

The Class of Service (CoS) queuing feature lets you directly configure certain aspects of switch queuing. 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, transmission rate shaping, etc., are user-configurable at the queue (or port) level.

To display the Class of Service page, click **Quality of Service > Class of Service** in the navigation pane.

General Settings

Use the General Settings tile to configure the Trust Mode on the switch, which is a global parameter that defines ingress traffic on all switch interfaces.

Select one of the following Trust Mode options:

- untrusted—The interface ignores any priority designations encoded in incoming packets, and instead sends the packets to a traffic queue based on the ingress port's default priority.
- trust 802.1p—The port accepts at face value the 802.1p priority designation encoded within packets arriving on the port.
- trust ip-dscp—The port accepts at face value the IP DSCP priority designation encoded within packets arriving on the port.

If you change the settings, click **Apply** to update the configuration. Your changes take effect immediately but are not retained across a switch reset unless you click (**Save**).

Figure 169. CoS General Settings Tile



802.1p Priority Mapping

The IEEE 802.1p feature allows traffic prioritization at the MAC level. The switch can prioritize traffic based on the 802.1p tag attached to the L2 frame. Each port on the switch has multiple queues to give preference to certain packets over others based on the Class of Service (CoS) criteria you specify. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission.

Use the 802.1p Priority Mapping page to assign 802.1p priority values to various traffic classes. The setting is applied to all interfaces on the switch.

Figure 170. 802.1p Priority Mapping Tile

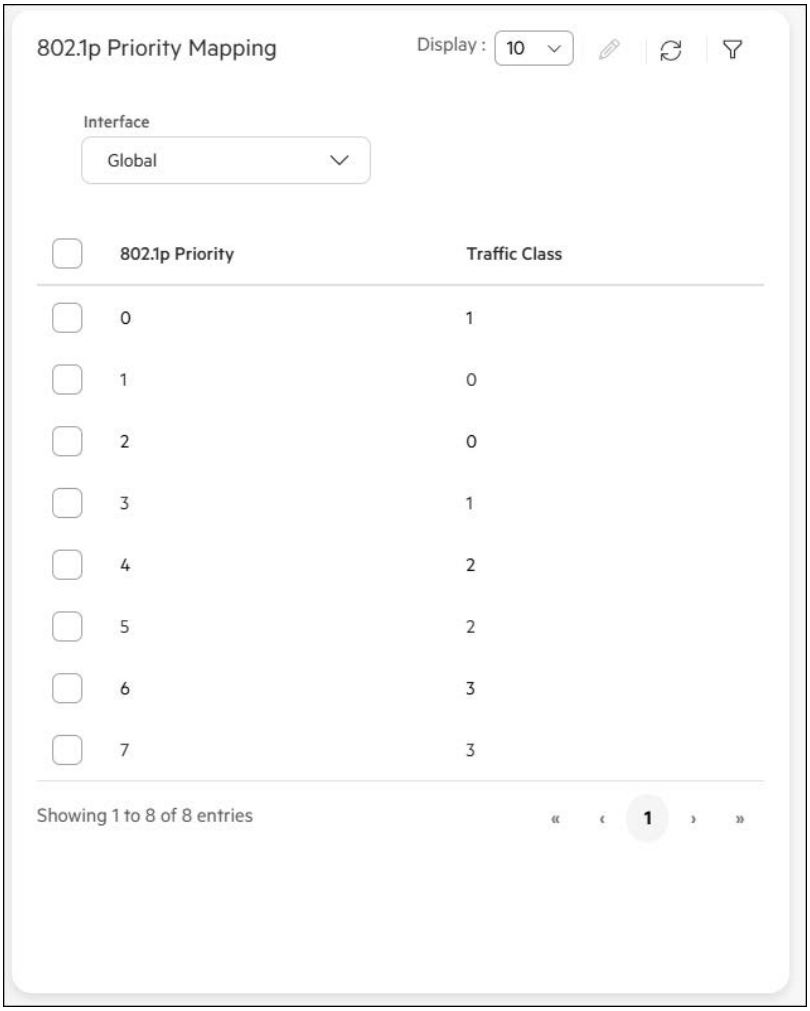


Table 140. 802.1p Priority Mapping Fields

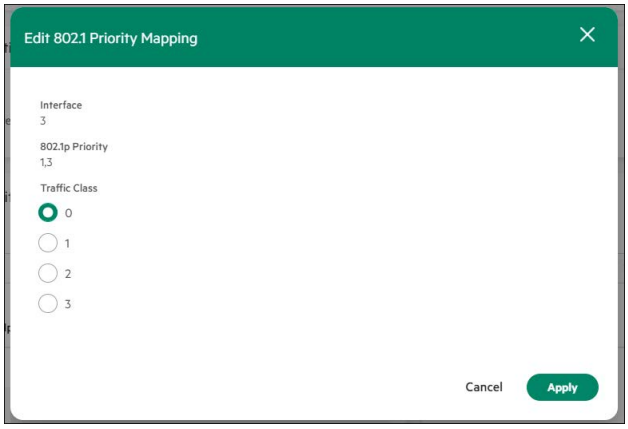
Field	Description
Interface	The interface to configure. To configure the same settings on all interfaces, select the Global menu option.
802.1p Priority	The 802.1p priority value to be mapped.
Traffic Class	The internal traffic class to which the corresponding 802.1p priority value is mapped. The default value for each 802.1p priority level is displayed for reference.

Configuring 802.1p Priority Mapping

To configure the 802.1p mapping:

1. From the Interface drop-down menu, select the interface to configure. To configure the same settings on all interfaces, select Global.
2. To map one or more 802.1p Priority values to a traffic class, select each 802.1p Priority value to configure and click (**Edit**). To map the same traffic class to all 802.1p priorities, select the check box in the 802.1p Priority heading row and click (**Edit**).
   The Edit 802.1 Priority Mapping dialog box appears.

Figure 171. Edit 802.1p Priority Mapping Dialog Box



3. Specify the traffic class to map to the 802.1p priority value(s) for the interface identified in the Interface field.
4. Click **Apply** to update the switch configuration.
   Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

DSCP CoS Mapping

Use the DSCP CoS Mapping tile to map an IP DSCP value to an internal traffic class.

Figure 172. DSCP CoS Mapping Tile

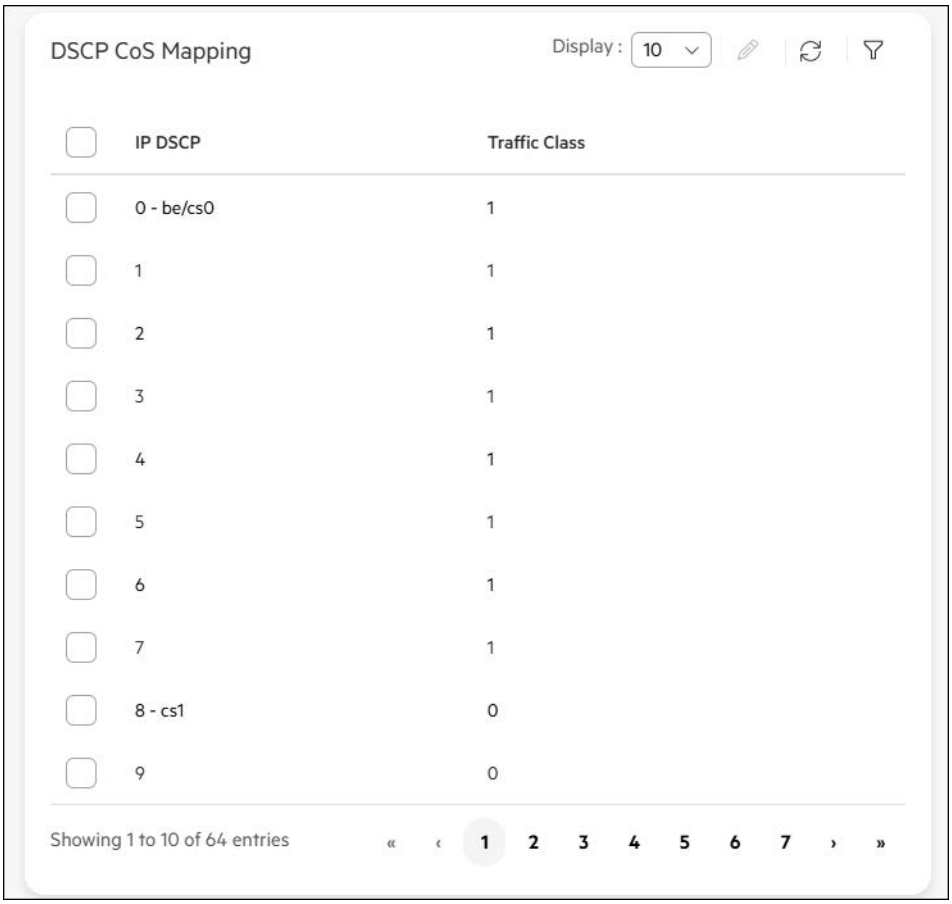


Table 141. DSCP CoS Mapping Fields

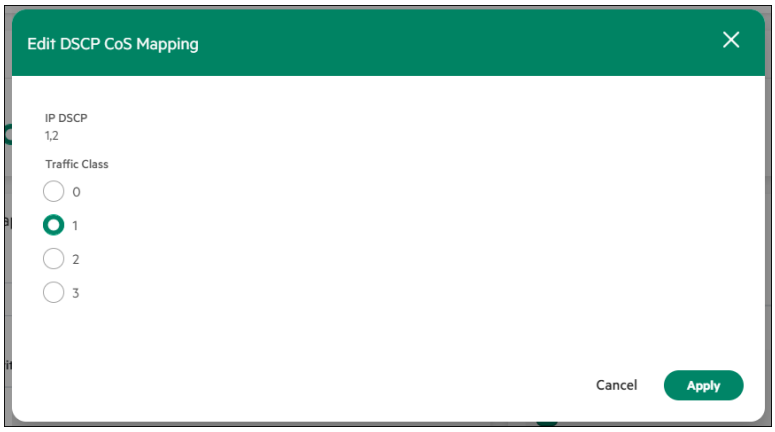
Field	Description
IP DSCP Values	The list of possible IP DSCP values the IP header can include.
Traffic Class	The internal traffic class to which the corresponding IP DSCP priority value is mapped. The higher the traffic class value, the higher its priority is for sending traffic.

Configuring DSCP CoS Mapping

To configure the DSCP CoS mapping:

1. To map one or more DSCP values to a traffic class, select each DSCP value to configure and click (**Edit**). To map the same traffic class to all IP DSCP values, select the check box in the IP DSCP heading row and click (**Edit**).
   The Edit DSCP CoS Mapping dialog box appears.

Figure 173. Edit DSCP CoS Mapping Dialog Box



2. Specify the traffic class to map to the IP DSCP value(s) for the interface identified in the Interface field.
3. Click **Apply** to update the switch configuration.
   Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Queue Configuration

Use the Queue Configuration tile to define what a particular queue does by configuring switch egress queues. User-configurable parameters control the amount of bandwidth used by the queue, the queue depth during times of congestion, and the scheduling of packet transmission from the set of all queues on a port.

Figure 174. Queue Configuration Tile

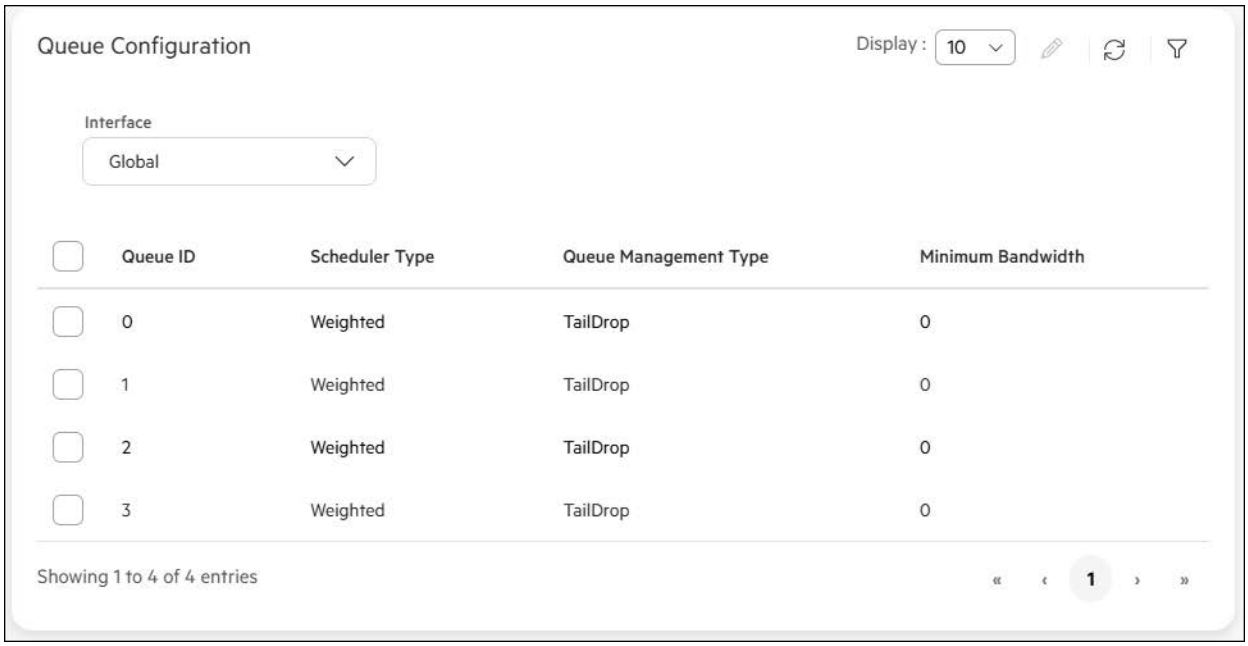


Table 142. Queue Configuration Fields

Field	Description
Interface	The interface to configure. To configure the same settings on all interfaces, select the Global menu option.
Queue ID	The queue to be configured.
Scheduler Type	The type of queue processing. Defining this value on a per-queue basis allows you to create the desired service characteristics for different types of traffic. The options are as follows: · Weighted—Uses weighted round robin to associate a weight to each queue. · Strict—Uses strict priority to service traffic with the highest priority on a queue first.
Queue Management Type	The type of queue depth management techniques used for all queues on this interface. Taildrop is the only option and means that all packets on a queue are safe until congestion occurs. At this point, any additional packets queued are dropped.
Minimum Bandwidth	The minimum guaranteed bandwidth allocated to the selected queue on the interface. Setting this value higher than its corresponding Maximum Bandwidth automatically increases the maximum to the same value. A zero value (0) means no guaranteed minimum. The sum of individual Minimum Bandwidth values for all queues in the selected interface cannot exceed defined maximum 100.

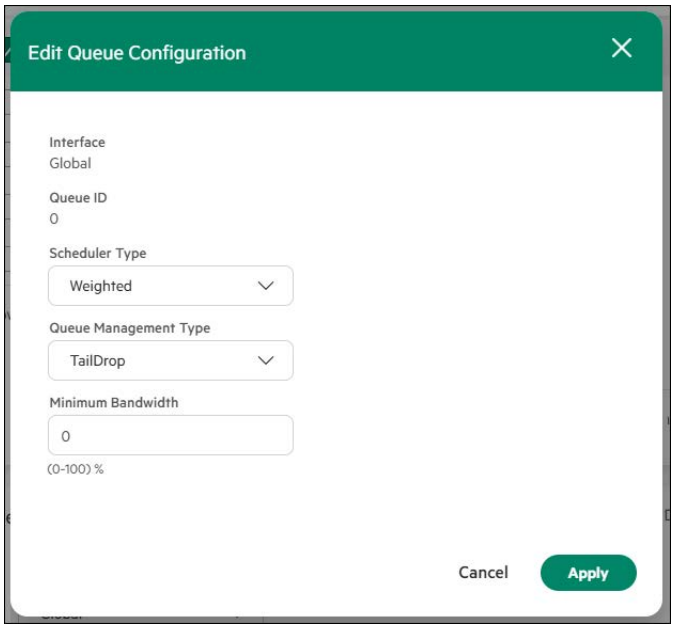
Configuring CoS Queue Settings

To define the behavior of the egress CoS queues on an interface:

1. From the Interface drop-down menu, select the interface to configure. To configure the same settings on all interfaces, select Global.
2. Select each queue to configure for the selected interface (or all interfaces) and click (**Edit**). If you select multiple queues, the same settings are applied to all selected queues.

   The Edit CoS Queue Configuration dialog box appears.

Figure 175. Edit Queue Configuration Dialog Box



3. Specify the scheduler type and minimum bandwidth for the interfaces identified in the Interface field and queues identified in the Queue ID field.
4. Click **Apply** to update the switch configuration.

   Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Interface CoS Configuration

Use the Interface CoS Configuration page to configure the Trust Mode and apply an interface shaping rate to all ports or to a specific port.

Figure 176. Interface CoS Configuration Tile

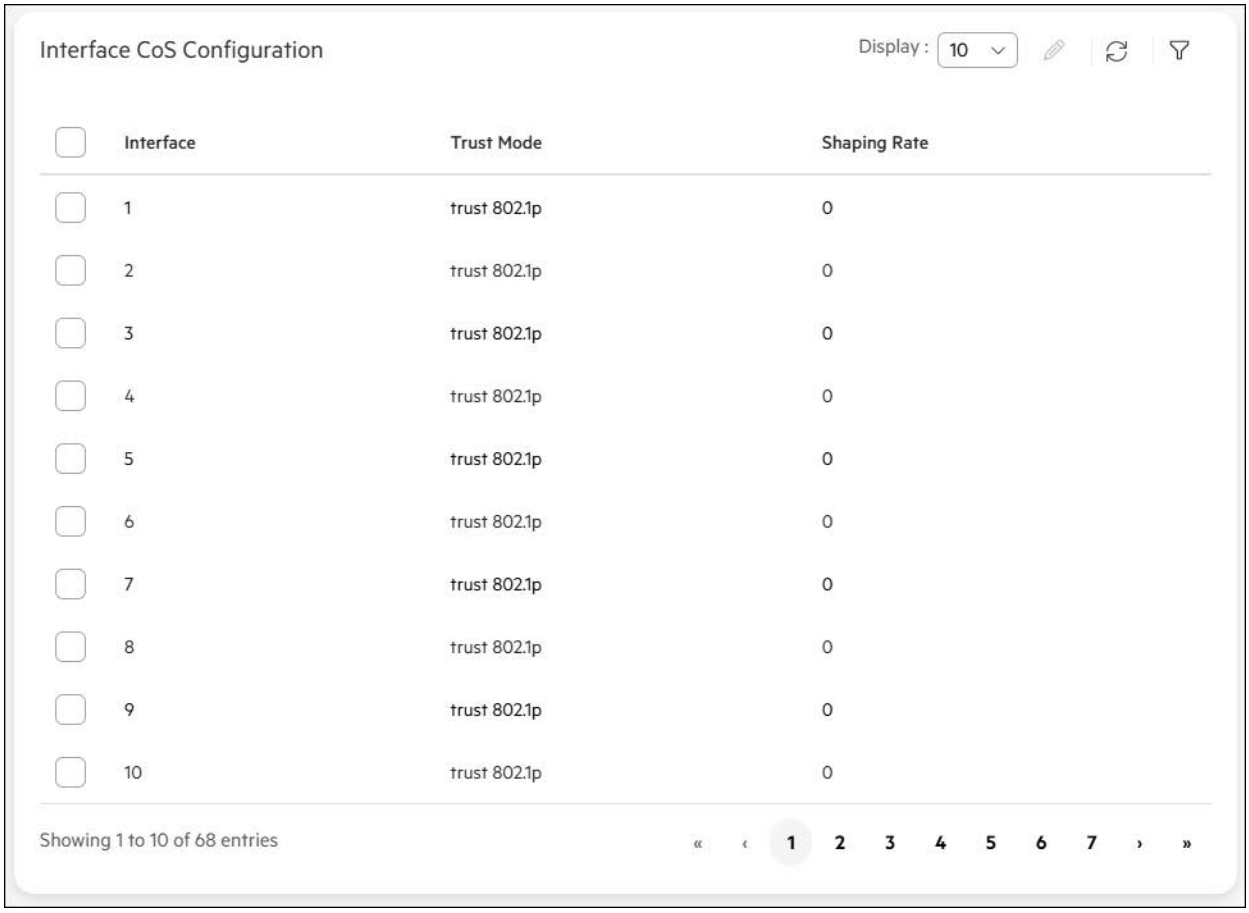


Table 143. Interface CoS Configuration Fields

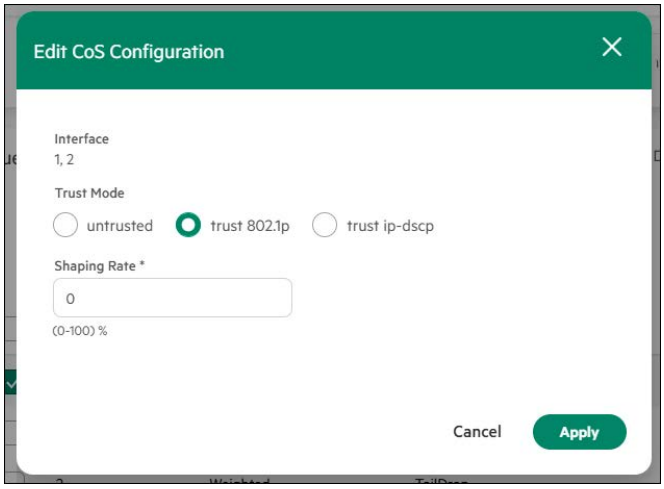
Field	Description
Interface	Selects the CoS configurable interface to be affected by the Interface Shaping Rate.
Trust Mode	The trust mode for ingress traffic on the interface, which is one of the following: · untrusted—The interface ignores any priority designations encoded in incoming packets, and instead sends the packets to a traffic queue based on the ingress port's default priority. · trust 802.1p—The port accepts at face value the 802.1p priority designation encoded within packets arriving on the port. · trust ip dscp—The port accepts at face value the IP DSCP priority designation encoded within packets arriving on the port.
Shaping Rate	Sets the limit on how much traffic can leave a port. The limit on maximum transmission bandwidth has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bound to the interface. Possible values for the rate: 0 to 100%.

Configuring CoS on an Interface

To configure the trust mode and shaping rate for one or more interfaces:

1. Select each interface to configure and click (**Edit**). If you select multiple interfaces, the same settings are applied to all selected interfaces.
   The Edit CoS Configuration dialog box appears.

Figure 177. Edit CoS Configuration Dialog Box



2. Specify the trust mode and shaping rate for all interfaces identified in the Interface field.
3. Click **Apply** to update the switch configuration.
   Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

The HPE Networking Instant On 1940 Switch Series series switch software includes a robust set of built-in security features to secure access to the switch management interface and to protect the network.

AAA Configuration

Authentication, Authorization, and Accounting (AAA) is a security framework used to manage network access and track user activity. It centralizes security functions, making it easier for administrators to control permissions and audit usage across multiple devices.

Use this page to view and configure the authentication lists used for both management access to the system and Port Access Control (802.1X) via RADIUS or TACACS+. An authentication list specifies the sequence of authentication methods to validate the credentials of a user accessing the device or a supplicant (client device) requesting network access via a switch port. For management access, the configured methods are applied through the system's login authentication list, while for 802.1X, they are enforced through the default dot1x authentication profile, which governs the order of operations during the authentication process.

If you change any settings on the page, click **Apply** to update the configuration. Your changes take effect immediately but are not retained across a switch reset unless you click (**Save**).

Management Authentication Order

Use the Management Authentication Order tile to configure the priority for management access to the switch.

The three priority drop-down menus show the configured method order for Management access.

Figure 178. Management Authentication Order Tile

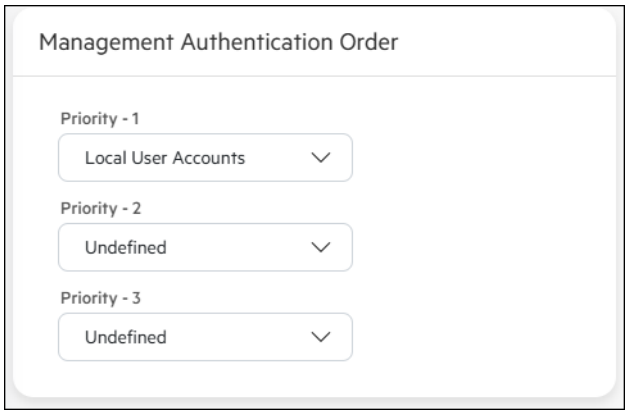


Table 144. Management Authentication Order Fields

Field	Description
Priority Options	The methods used to authenticate a user who attempts to access the management interface. These are the possible methods: · Local User Accounts — Uses the username and password in the Local User database to verify the user's credentials. · RADIUS — Sends the username and password to the configured RADIUS server to verify the user's credentials. · TACACS — Sends the username and password to the configured TACACS server to verify the user's credentials. · Undefined — No method is selected. To ensure reliable access to the system, at least one authentication method in the Management Authentication priority list must be set to Local User Accounts.

Port Access Control Authentication Order

Use the Port Access Control Authentication Order tile to configure the priority for users who access the network through the ports on the switch.

The three priority drop-down menus show the configured method order for port access.

Figure 179. Port Access Control Authentication Order Tile

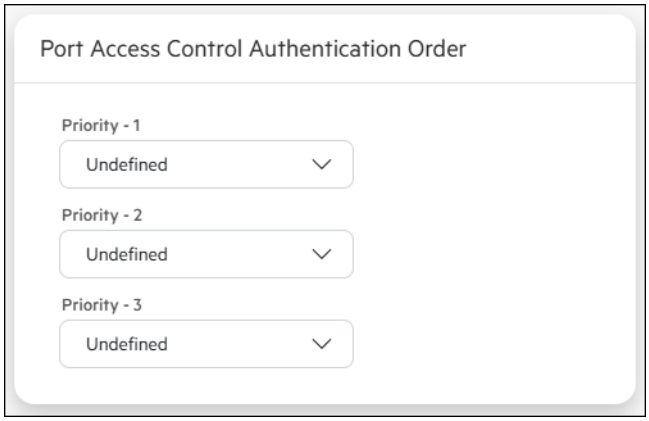


Table 145. Port Access Control Authentication Order Fields

Field	Description
Priority Options	The methods used to authenticate a user who attempts to access the network. These are the possible methods: · Local MacAuth DB — Uses the local MAC authentication clients database for 802.1X port-based authentication. To view or configure MAC authentication clients in the local MacAuth DB, see Local MAC Authentication Clients. · Local User Accounts — Uses the credentials stored in the Local User database to authenticate the supplicant attempting 802.1X port-based access. · RADIUS — Sends the client's credentials to the configured RADIUS server to authenticate the user as part of the 802.1X port-based authentication process. · Undefined — No method is selected.

RADIUS Configuration

Remote Authentication Dial-In User Service (RADIUS) servers provide additional security for networks. The HPE Networking Instant On 1940 Switch Series includes a RADIUS client that can contact one or more RADIUS servers for various authentication and accounting services. The RADIUS server maintains a centralized database that contains per-user information.

The switch can connect to up to 2 RADIUS servers. At each given time only 1 of these RADIUS servers is used for both authentication and authorization. The switch will send the RADIUS packets to the RADIUS server with the highest priority that is not in “dead-time” period.

A server is placed in a "dead-time" period if it did not respond to a switch request for "Max number of retransmits". The dead-time is 0-2000 minutes. If a server is placed in dead-time the switch will send the RADIUS frames to the RADIUS server with next highest priority. If the dead-time expired, the switch will try once again to send frames to the RADIUS server with higher priority.

To display the RADIUS Configuration page, click **Security** > **RADIUS Configuration** in the navigation pane.

RADIUS as a Device Management Authenticator

By default, the user accounts configured on the switch are used for device Management Authentication. However, the RADIUS server can be configured as the first device management authenticator. In this case, the user accounts are used as backup in case the configured RADIUS server is not reachable.

When configured as a device management authenticator, the RADIUS server receives the user credentials from the switch and looks up the entry in the RADIUS user database. The RADIUS server can reply with one of the following responses:

- Reject—User credentials do not match an entry in RADIUS Database. User is denied access to device management.
- Accept + RADIUS service-type attribute is set to 6 (Administrative)—The user is granted access with read/write permission.
- Accept + RADIUS service-type attribute is set to 7 (NAS Prompt)—The user is granted access with read-only permission.

Global Configuration

Use the Global Configuration tile to configure global settings for the RADIUS feature.

Figure 180. RADIUS Global Configuration Tile

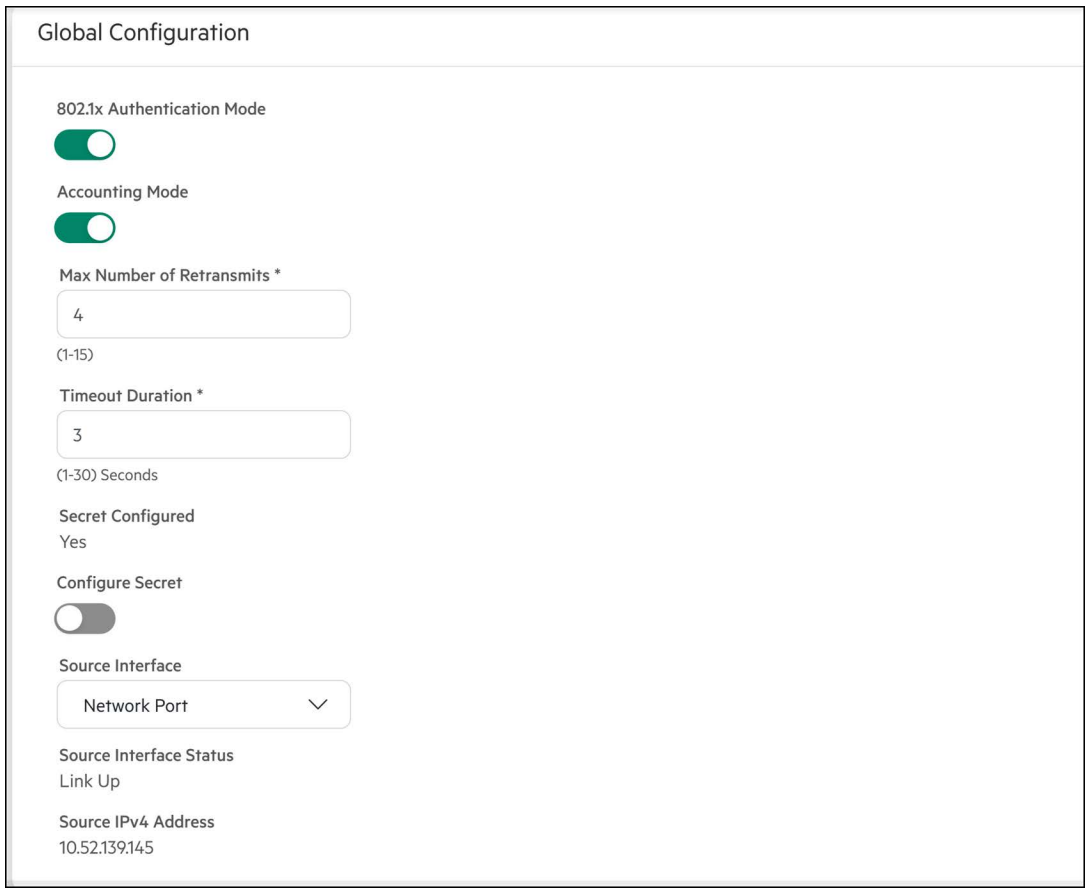


Table 146. RADIUS Global Configuration Fields

Field	Description
802.1X Authentication Mode	Specifies whether the IEEE 802.1X authentication mode on the switch relies on RADIUS services for 802.1x supplicant authentication. When this setting is selected, and port-based authentication is enabled for the switch, RADIUS will be used for the 802.1x authentication process. Specifically, the credentials presented by the authenticating station (the 802.1x supplicant) are sent to the configured RADIUS server(s) for verification.
Accounting Mode	Specifies whether the accounting mode on the switch is enabled or disabled. When this setting is selected, RADIUS is used for session accounting. Specifically, an accounting event is sent to the configured RADIUS server(s) at the start and end of each 802.1X session.
Max Number of Retransmits	The maximum number of times the RADIUS client on the switch will retransmit a request packet to a configured RADIUS server after a response is not received. If multiple RADIUS servers are configured, the max retransmit value will be exhausted on the first server before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS server equals the sum of (retransmit x timeout) for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the RADIUS application returns a response.

Field	Description
Timeout Duration	The number of seconds the RADIUS client waits for a response from the RADIUS server. Consideration to maximum delay time should be given when configuring RADIUS timeout and RADIUS max retransmit values.
Secret Configured	Specifies whether the global server secret on the switch is configured or not.
Configure Secret	When enabled, the Set Secret field is visible and allows to configure the global server secret.
Set Secret	To specify the global server secret. This field is visible only when Configure Secret is enabled.
Source Interface	Configures the physical or logical interface to use as the RADIUS client source interface. When an IP address is configured on the source interface, this address is used for all RADIUS communications between the local RADIUS client and the remote RADIUS server. The IP address of the designated source interface is used in the IP header of RADIUS management protocol packets. This allows security devices, such as firewalls, to identify all source packets coming from a specific device. The following options are available for the type of interface to use as the source for outgoing RADIUS packets: · Unconfigured—The primary IP address of the originating (outbound) interface is used as the source address. · Network Port—The Network port source IP is used as the source address. · Interface—Based on the selected physical port to use as the source interface, the primary IP address of that physical port is used as the source address. · VLAN ID—Based on the selected VLAN to use as the source interface, the primary IP address of that VLAN routing interface is used as the source address.
Source IPv4 Address	Displays the primary IPv4 address associated with the selected source interface.
Source Interface Status	Indicates the current link status of the selected source interface. These are the possible values: · Link up. · Link down.

RADIUS Server Configuration

Use the RADIUS Server Configuration tile to add one or two RADIUS servers for the switch to contact and to view information about the configured RADIUS servers.

Figure 181. RADIUS Server Configuration Tile

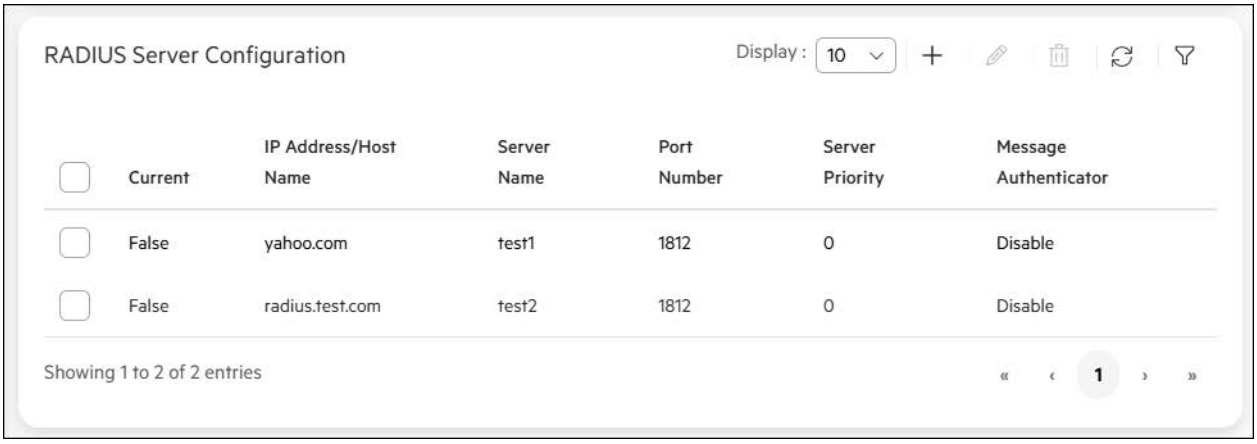


Table 147. RADIUS Server Configuration Fields

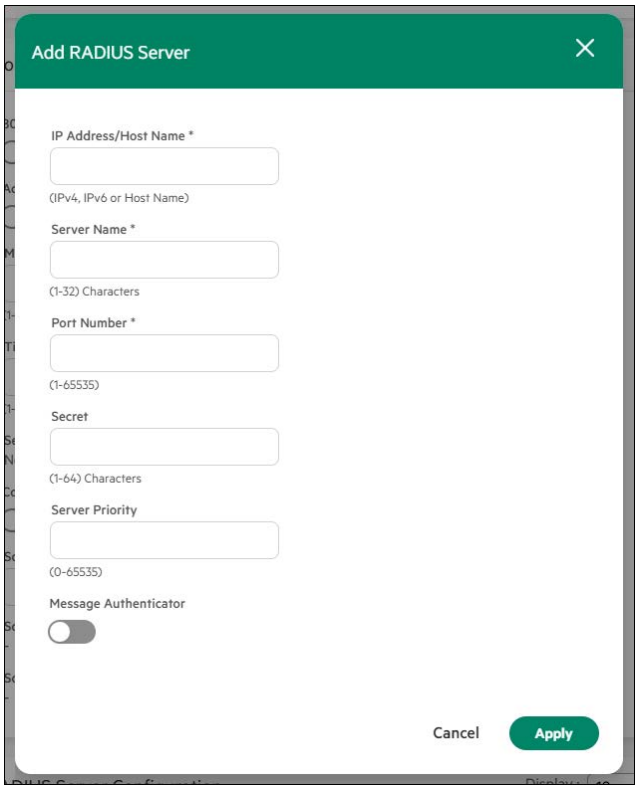
Field	Description
Current	Identifies whether the configured RADIUS server is the current server for the RADIUS Authentication server. · True—The server is the current server for the authentication. · False—The server is not the current server for authentication. When the switch sends a RADIUS request to the RADIUS server, the request is directed to the server selected as the current server. Initially the server with the highest priority (lowest number value in priority field) is selected as the current server. If the server with the highest priority fails, one of the other servers becomes the current server.
IP Address/Host Name	The IP address of the RADIUS server, which can be one of the following: · IPv4 address · IPv6 address (x:x:x:x:x:x:x:x) · IPv6 link local address (x:x:x:x::x) · Hostname—Host names must be resolvable by DNS and are composed of a series of labels separated by dots.
Server Name	The name of the RADIUS server.
Port Number	Identifies the authentication port the server uses for handling RADIUS authentication requests. The port is a UDP port.
Server Priority	Displays the RADIUS server priority. Lower value means server has a higher priority. The switch will use the RADIUS server with highest priority that is not in dead-time. Range: 0-65535
Message Authenticator	Indicates whether the RADIUS server requires the Message Authenticator attribute to be present. 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.

Adding a RADIUS Server

To add a RADIUS server to the switch configuration:

1. Click + (**Add**).
   The Add RADIUS Server dialog box appears.

Figure 182. Add RADIUS Server Dialog Box



2. Specify the IP address or hostname, server name, and port number associated with the RADIUS server.
3. Enter the Secret (1 to 64 characters), which is the shared secret text string used for authenticating and encrypting all RADIUS communications between the RADIUS client on the switch and the RADIUS server. The secret specified in this field must match the shared secret configured on the RADIUS server.
4. Specify the priority of the RADIUS server (0 is the highest priority).
5. Indicate whether the RADIUS server requires the Message Authenticator attribute to be present.
6. Click **Apply** to update the switch configuration.

   Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Changing RADIUS Server Settings

To change settings for an existing RADIUS server:

1. Select the RADIUS server to configure and click (**Edit**).
2. On the Edit RADIUS server dialog box, update the RADIUS server information as needed. The IP address of an existing RADIUS server cannot be changed.
3. Click **Apply** to update the switch configuration.

   Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Removing a RADIUS Server

To delete one or more RADIUS servers, select the check box associated with each entry to delete and click (**Remove**).

RADIUS Accounting Server Configuration

Use the RADIUS Accounting Server Configuration tile to add one or two RADIUS accounting servers for the switch to contact and to view information about the configured RADIUS accounting servers.

Figure 183. RADIUS Accounting Server Configuration Tile

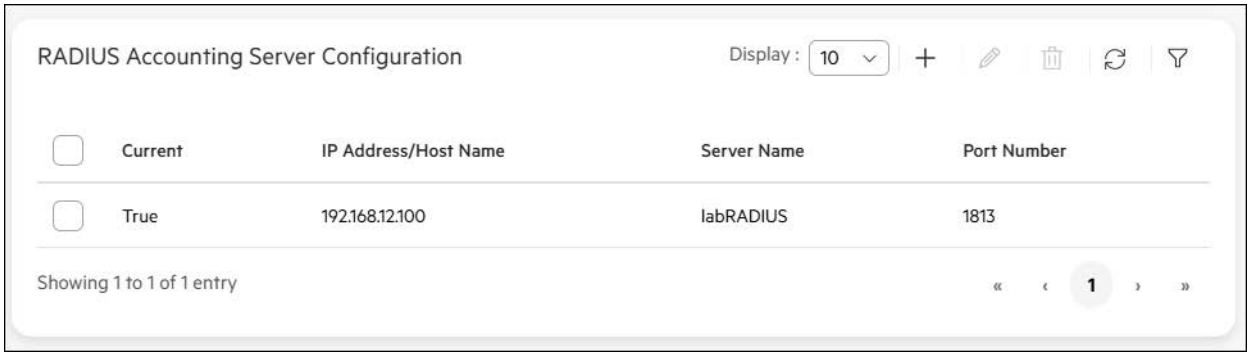


Table 148. RADIUS Accounting Server Configuration Fields

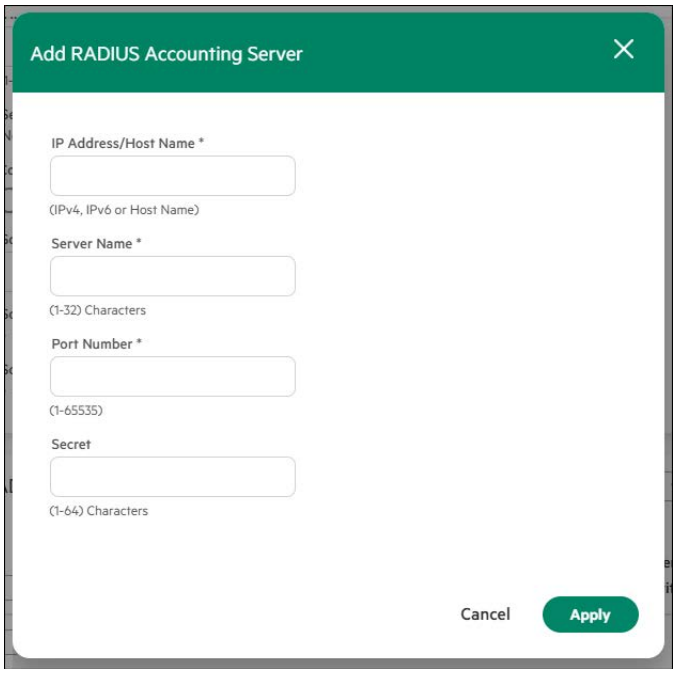
Field	Description
Current	Identifies whether the configured RADIUS accounting server is the current server for the RADIUS Authentication server. · True—The server is the current accounting server for the authentication. · False—The server is not the current accounting server for authentication. When the switch sends a RADIUS request to the RADIUS Accounting server, the request is directed to the server selected as the current server. When the current server becomes unavailable, the other server (if configured) becomes the current server.
IP Address/Host Name	The IP address or hostname of the RADIUS accounting server, which can be one of the following: · IPv4 address · IPv6 address (x:x:x:x:x:x:x:x) · IPv6 link local address (x:x:x:x::x) · Hostname—Host names must be resolvable by DNS and are composed of a series of labels separated by dots.
Server Name	The name of the RADIUS accounting server.
Port Number	Identifies the authentication port the server uses for handling RADIUS accounting requests. The port is a UDP port. The standard RADIUS accounting port number is 1813 (UDP).

Adding a RADIUS Accounting Server

To add a RADIUS accounting server to the switch configuration:

1. Click + (**Add**).
   The Add RADIUS Server dialog box appears.

Figure 184. Add RADIUS Accounting Server Dialog Box



2. Specify the IP address or hostname, server name, and port number associated with the RADIUS accounting server.
3. Enter the Secret (1 to 64 characters), which is the shared secret text string used for authenticating and encrypting all RADIUS communications between the RADIUS client on the switch and the RADIUS accounting server. The secret specified in this field must match the shared secret configured on the RADIUS accounting server.
4. Click **Apply** to update the switch configuration.

   Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Changing RADIUS Accounting Server Settings

To change settings for an existing RADIUS accounting server:

1. Select the RADIUS accounting server to configure and click (**Edit**).
2. On the Edit RADIUS accounting server dialog box, update the RADIUS accounting server information as needed. The IP address of an existing RADIUS server cannot be changed.
3. Click **Apply** to update the switch configuration.

   Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Removing a RADIUS Accounting Server

To delete one or more RADIUS accounting servers, select the check box associated with each entry to delete and click (**Remove**).

RADIUS Server Statistics

Use this tile to view summary information about the number and type of RADIUS messages sent between the RADIUS client on the device and the configured RADIUS authentication servers.

Figure 185. RADIUS Server Statistics Tile

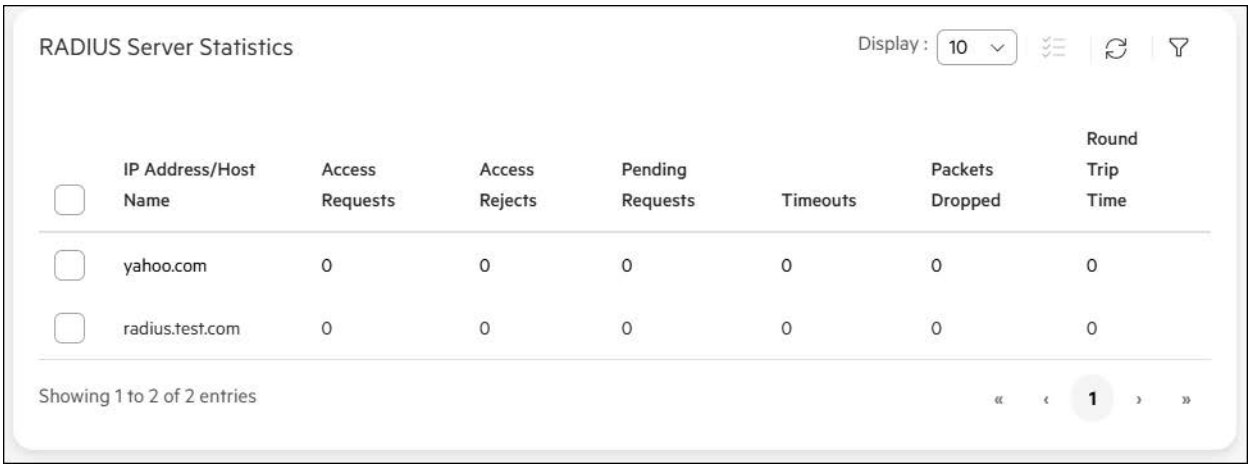


Table 149. RADIUS Server Statistics Fields

Field	Description
IP Address/Host Name	The IP address or host name of the RADIUS server associated with the rest of the data in the row. When viewing the detailed statistics for a RADIUS server, this field identifies the RADIUS server.
Access Requests	The number of RADIUS Access-Request packets sent to the server. This number does not include retransmissions.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from the server.
Pending Requests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response.
Timeouts	The number of times a response was not received from the server within the configured timeout value.
Packets Dropped	The number of RADIUS packets received from the server on the authentication port and dropped for some other reason.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Access-Reply/ Access-Challenge and the Access-Request that matched it from the RADIUS authentication server.

To view additional statistics, select the RADIUS server with the statistics to view and click (**Details**).

The following table describes the additional RADIUS server information that the RADIUS Server Detailed Statistics dialog box shows.

Table 150. RADIUS Server Detailed Statistics Fields

Field	Description
Access Retransmissions	The number of RADIUS Access-Request packets that had to be retransmitted to the server because the initial Access-Request packet failed to be successfully delivered.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from the server.

Field	Description
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from the server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators, signature attributes, and unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from the server.
Unknown Types	The number of RADIUS packets of unknown type which were received from the server on the authentication port.

RADIUS Accounting Server Statistics

Use the RADIUS Accounting Server Statistics tile to view statistical information for each RADIUS server configured on the system.

Figure 186. RADIUS Accounting Server Statistics Tile

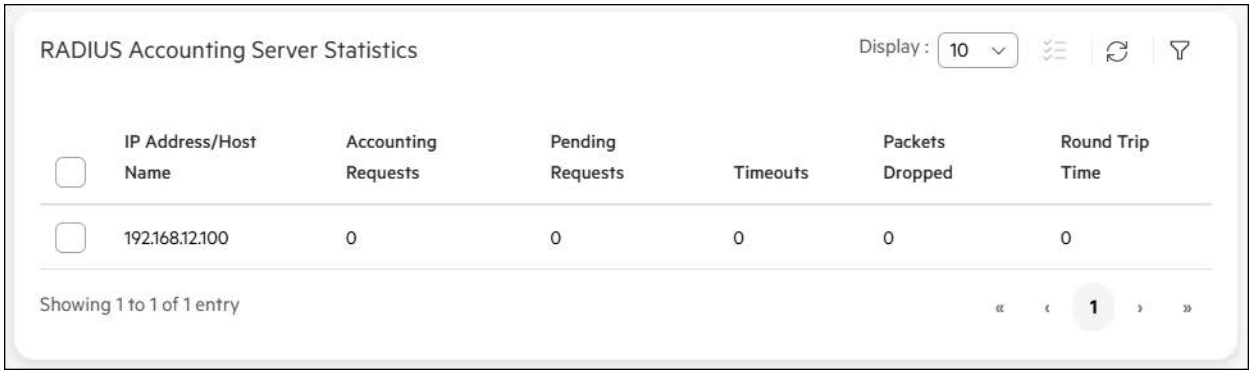


Table 151. RADIUS Accounting Server Statistics Fields

Field	Description
IP Address/Host Name	The IP address or host name of the RADIUS accounting server associated with the rest of the data in the row. When viewing the detailed statistics for a RADIUS accounting server, this field identifies the server.
Accounting Requests	The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.
Pending Requests	The number of RADIUS Accounting-Request packets destined for the server that have not yet timed out or received a response.
Timeouts	The number of times a response was not received from the server within the configured timeout value.
Packets Dropped	The number of RADIUS packets received from the server on the accounting port and dropped for some other reason.
Round Trip Time	Displays 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.

To view additional statistics, select the RADIUS accounting server with the statistics to view and click (**Details**).

The following table describes the additional RADIUS accounting server information that the RADIUS Accounting Server Detailed Statistics dialog box shows.

Table 152. RADIUS Accounting Server Detailed Statistics Fields

Field	Description
Accounting Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to the server.
Accounting Responses	The number of RADIUS packets received on the accounting port from the server.
Malformed Access Responses	The number of malformed RADIUS Accounting-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets that contained invalid authenticators received from the accounting server.
Unknown Types	The number of RADIUS packets of unknown type which were received from the server on the accounting port.

TACACS+ Configuration

TACACS provides access control for networked devices via one or more centralized servers. Similar to RADIUS, this protocol simplifies authentication by making use of a single database that can be shared by many clients on a large network. TACACS+ is based on the TACACS protocol (described in RFC1492) but additionally provides for separate authentication, authorization and accounting services. The original protocol was UDP based with messages passed in clear text over the network; TACACS uses TCP to ensure reliable delivery and a shared key configured on the client and daemon server to encrypt all messages. The switch can support up to 5 TACACS servers.

To display the TACACS+ Configuration page, click **Security** > **TACACS+ Configuration** in the navigation pane.

If you change any settings on the page, click **Apply** to update the switch configuration.

Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

TACACS+ Configuration

Use the TACACS+ Configuration tile to view and configure the TACACS+ global configuration.

Figure 187. TACACS+ Configuration Tile

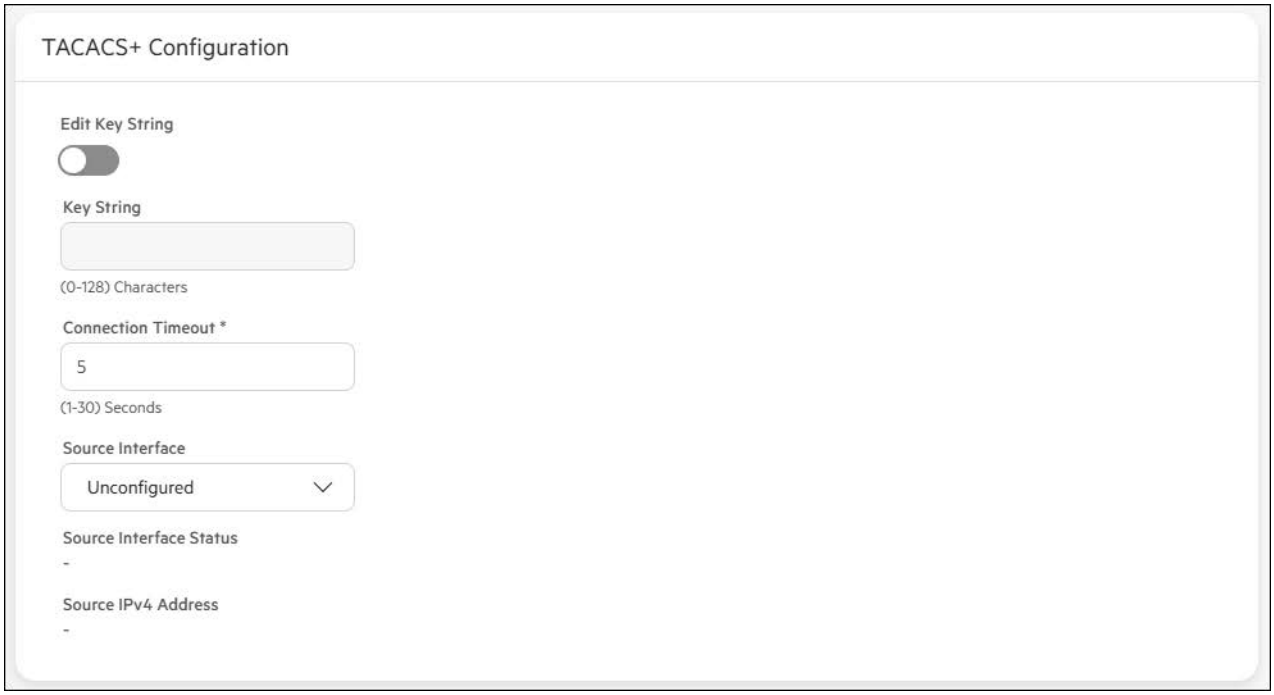


Table 153. TACACS+ Configuration Fields

Field	Description
Edit Key String	Toggle the control to the right to enable configuring or changing the global key string of the TACACS server.
Key String	Specifies the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The key must match the key configured on the TACACS+ server.
Connection Timeout	The maximum number of seconds allowed to establish a TCP connection between the device and the TACACS+ server.
Source Interface	Configures the physical or logical interface to use as the TACACS+ client source interface. When an IP address is configured on the source interface, this address is used for all TACACS+ communications between the local TACACS+ client and the remote TACACS+ server. The IP address of the designated source interface is used in the IP header of TACACS+ management protocol packets. This allows security devices, such as firewalls, to identify all source packets coming from a specific device. The following options are available for the type of interface to use as the source for outgoing TACACS+ packets: · Unconfigured—The primary IP address of the originating (outbound) interface is used as the source address. · Network Port—The Network port source IP is used as the source address. · Interface—Based on the selected physical port to use as the source interface, the primary IP address of that physical port is used as the source address. · VLAN ID—Based on the selected VLAN to use as the source interface, the primary IP address of that VLAN routing interface is used as the source address.
Source IPv4 Address	Displays the primary IPv4 address associated with the selected source interface.
Source Interface Status	Indicates the current link status of the selected source interface. These are the possible values: · Link up. · Link down.

TACACS+ Server Configuration

Use the TACACS+ Server Configuration tile to add up to five TACACS+ servers for the switch to contact and to view information about the configured TACACS+ servers.

Figure 188. TACACS+ Server Configuration Tile



Table 154. TACACS+ Server Configuration Fields

Field	Description
Server	The TACACS+ Server IP address or Hostname.
Priority	The order in which the TACACS+ servers are used. The lowest number has the highest priority.
Port Number	Identifies the authentication port the server uses for handling TACACS+ authentication requests. The default port number is 49, which is a TCP port.
Key String	The authentication and encryption key for TACACS+ communications between the switch and the TACACS+ server. The key must match the key configured on the TACACS+ server.
Connection Timeout	The amount of time that passes before the connection between the device and the TACACS+ server time out.

Adding, Editing, and Removing a TACACS+ Server

To add a TACACS+ server to the switch configuration, click + (**Add**) and configure the settings described in Table 154.

To change settings for an existing TACACS+ server, select the TACACS+ server to configure and click (**Edit**). Update the TACACS+ server information as needed. The IP address of an existing TACACS+ server cannot be changed.

To delete one or more TACACS+ servers, select the check box associated with each entry to delete and click (**Remove**).

Port Access Control

In port-based authentication mode, when 802.1X is enabled globally and on the port, successful authentication behavior depends on the configured access mode. In Multi-Domain Multi-Host mode, one voice client and one data client can be authenticated on the same port. Once the data client is authenticated, access is granted to all connected data clients on the port. Voice and data domains remain logically separated, allowing independent authentication for each. A typical use case includes an IP phone connected to the port and a Virtual Machine Controller (hosting multiple VMs) connected through the phone's hub port. Once the VM Controller is authenticated, all its hosted VMs can access the network without individual authentication. Ports in this mode are under bidirectional control. This is the default authentication mode.

The 802.1X network has three components:

- Authenticators: The port that is authenticated before permitting network access.
- Supplicants: The host connected to the authenticated port requesting access to the network 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 network services.

To display the Port Access Control Configuration page, click **Security** > **Port Access Control** in the navigation pane, and ensure that the **Configuration** tab is selected.

Global Configuration

Use the Global Configuration tile to configure the global Port Access Control settings on the switch. The port-based access control feature uses IEEE 802.1X to enable the authentication of system users through a RADIUS server. Only authenticated and approved network users can transmit and receive data. Supplicants (clients connected to authenticated ports that request access to the network) are authenticated using the Extensible Authentication Protocol (EAP). Also supported are PEAP, EAP-TTLS, and EAP-TLS.

Figure 189. Port Access Control Global Configuration Tile

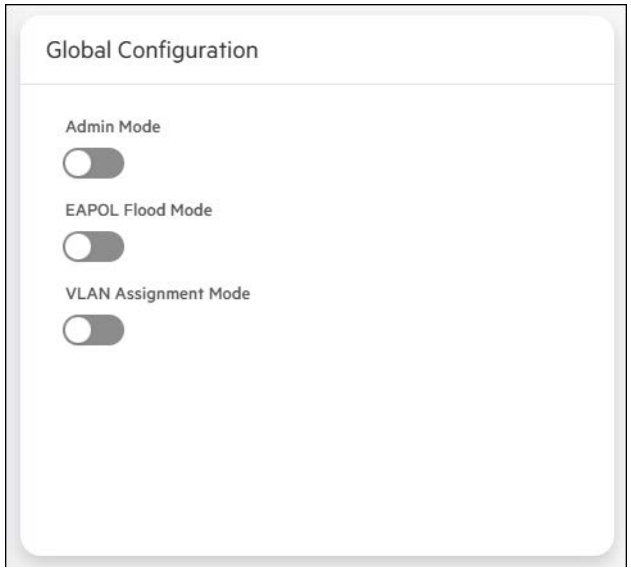


Table 155. Port Access Control Global Configuration Fields

Field	Description
Admin Mode	Toggle the control to enable or disable Authenticator admin mode on the switch. The default is Disable. This feature permits port-based authentication on the switch.
EAPOL Flood Mode	The administrative mode of the Extensible Authentication Protocol (EAP) over LAN (EAPOL) flood support on the device. EAPOL Flood Mode can be enabled when Admin Mode and Monitor Mode are disabled.
VLAN Assignment Mode	If enabled, when a supplicant is authenticated by a authentication server, the port that the supplicant is connected to is placed in a particular VLAN specified by the RADIUS server. VLAN Assignment mode controls if the switch is allowed to place a port in a RADIUS-assigned VLAN. A port's VLAN assignment is determined by the first supplicant that is authenticated on the port.

MAC Authentication Settings

Use the MAC Authentication Settings tile to customize the format in which MAC authentication requests are sent to the RADIUS server. MAC-based authentication 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. When accessing a port, the MAC address is the supplicant's username. This tile allows you to format the username, which must match the entries in the authentication server.

Figure 190. MAC Authentication Settings Tile

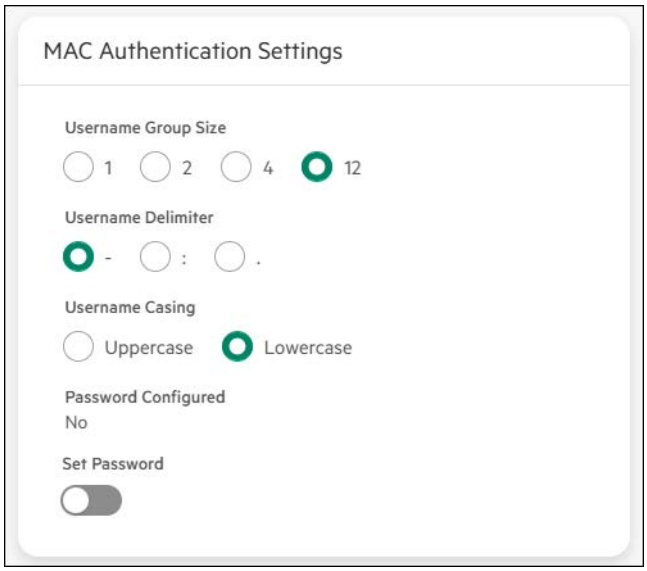


Table 156. MAC Authentication Settings Fields

Field	Description
Username Group Size	The number of characters per grouping between each delimiter. Available values are 1, 2, 4 and 12 (which indicates no delimiter). The default value is 12. An example of a username that uses the default values is aabbccddeeff.
Username Delimiter	Select the delimiter to use in username. These are the supported values: · Hyphen, for example aa-bb-cc-dd-ee-ff · Colon, for example aa:bb:cc:dd:ee:ff · Period, for example aa.bb.cc.dd.ee.ff The default delimiter is Hyphen ("-") In these examples, the username group size is 2.

Field	Description
Username Casing	Select Uppercase or Lowercase for the letters a-f of the MAC address. Default is Lowercase.
Password Configured	Indicates whether the password has been configured: · Yes—Password for MAC Authentication supplicants Configured. · No—Password for MAC Authentication supplicants not Configured.
Set Password	To set a password, enable the set password toggle control and enter the password.
Password	This password will be used for all MAC Authentication supplicants.

Port Configuration

Use the Port Configuration tile to configure port access control settings for each physical port on the switch.

Figure 191. Port Configuration Tile

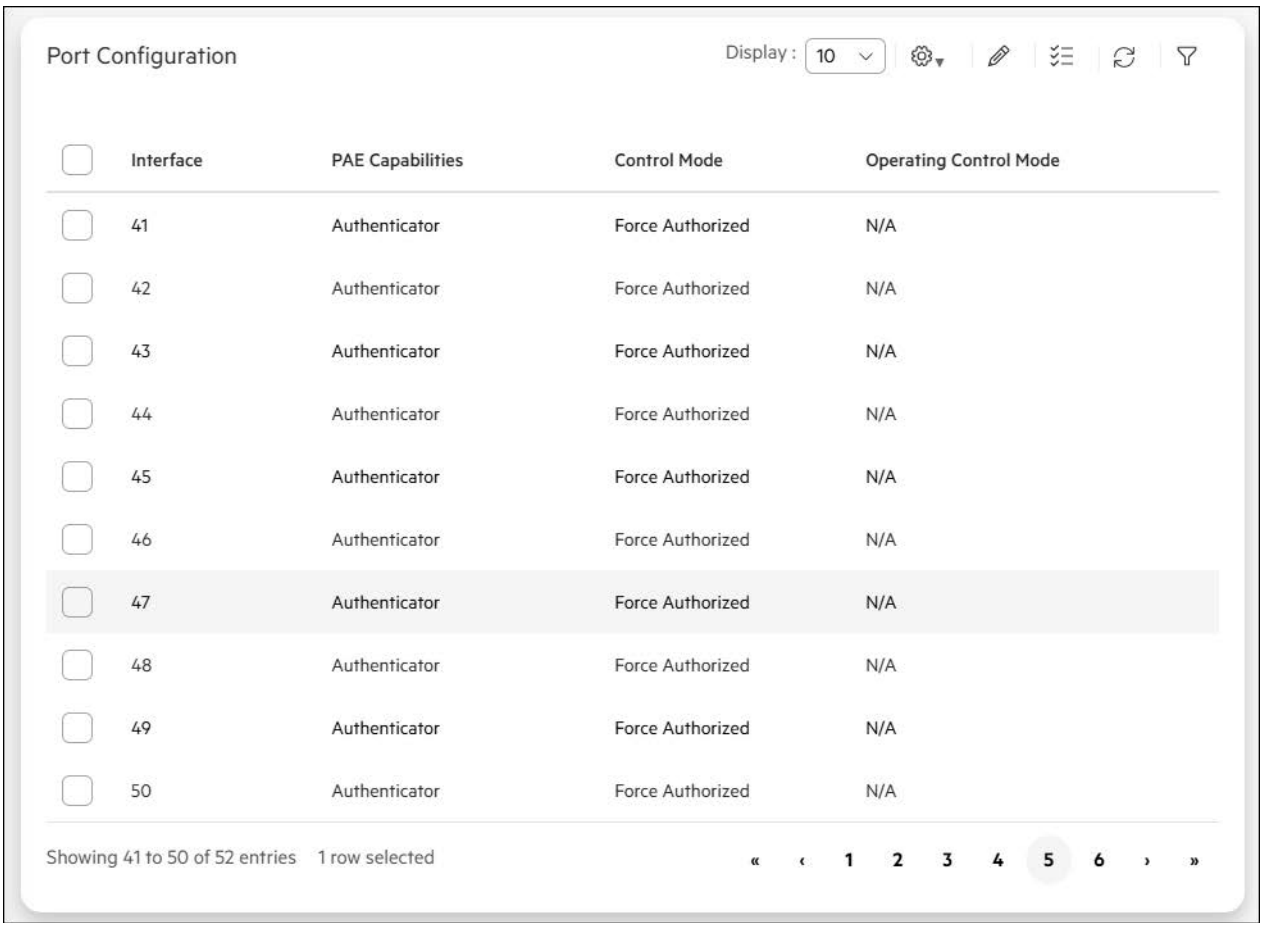


Table 157. Port Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row.

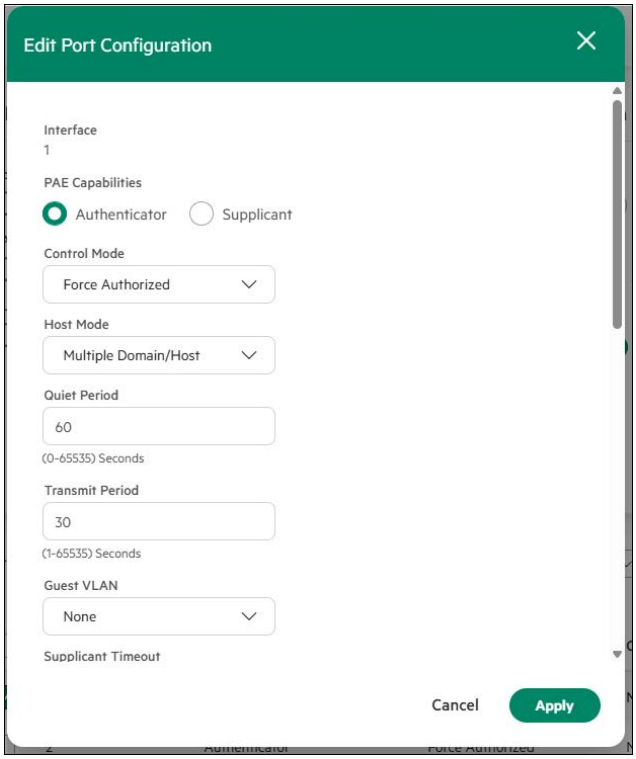
Field	Description
PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following: · Authenticator—The port enforces authentication and passes authentication information from a remote supplicant (similar to a client or host) to the authentication server. If the server successfully authenticates the supplicant, the port allows access. · Supplicant—The port must be granted permission by the authentication server before it can access the remote authenticator port.
Control Mode	The port-based access control mode configured on the port, which is one of the following: · Auto—The port is unauthorized until a successful authentication exchange has taken place. · Force Authorized—The port sends and receives normal traffic without client port-based authentication. · Force Unauthorized—The port ignores supplicant authentication attempts and does not provide authentication services to the client.
Operating Control Mode	The control mode under which the port is actually operating, which is one of the following: · Auto · Force Authorized · Force Unauthorized · N/A If the mode is N/A, port-based access control is not applicable to the port. If the port is in detached state it cannot participate in port access control. Additionally, if port-based access control is globally disabled, the status for all ports is N/A.

Configuring Port Access Control on an Interface

To configure the port access control settings on an interface:

1. Select the interface to configure.
2. Click (**Edit**) to open the Edit Port Configuration dialog box.
   The following figure does not show all available fields.

Figure 192. Edit Port Configuration Dialog Box



3. Update the port access control settings on the interface. Table 158 describes the fields on the page.
4. Click **Apply** to update the switch configuration.
   Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Table 158. Edit Port Configuration Fields

Field	Description
Interface	The interface with the settings to view or configure. If you have been redirected to this page, this field is read-only and displays the interface that was selected on the Port Access Control Port Summary page.
PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following: · Authenticator—The port enforces authentication and passes authentication information from a remote supplicant (client or host) to the authentication server. If the server successfully authenticates the supplicant, the port allows access. · Supplicant—The port is connected to an authenticator port and must be granted permission by the authentication server before it can send and receive traffic through the remote port.
Authenticator Options The fields in this section can be changed only when the selected port is configured as an authenticator port (that is, the PAE Capabilities field is set to Authenticator.	
Control Mode	The port-based access control mode on the port, which is one of the following: · Auto—The port is unauthorized until a successful authentication exchange has taken place. · Force Authorized—The port sends and receives normal traffic without client port-based authentication. · Force Unauthorized—The port ignores supplicant authentication attempts and does not provide authentication services to the client.

Field	Description
Host Mode	The mode determines the number of voice and data clients that can be authenticated and authorized on the ports. · Single Authentication: Only one data client. · Multiple Host: One data client authenticates and access is granted for all clients on that port. · Multiple Domain: One data client and one voice client are allowed to be authenticated. · Multiple Authentication: One voice and multiple data clients with independent authentication. · Multiple Domain/Host: One voice client in addition to multiple hosts mode.
Quiet Period	The number of seconds that the port remains in the quiet state following a failed authentication exchange.
Transmit Period	The value, in seconds, of the timer used by the authenticator state machine on the port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant.
Guest VLAN	The VLAN ID for the guest VLAN. The guest VLAN allows the port to provide a distinguished service to unauthenticated users. This feature provides a mechanism to allow users access to hosts on the guest VLAN.
Supplicant Timeout	The amount of time that the port waits for a response before retransmitting an EAP request frame to the client.
Server Timeout	The amount of time the port waits for a response from the authentication server.
Maximum Requests	The maximum number of times that the port sends an EAP request frame (assuming that no response is received) to the client before restarting the authentication process.
MAC Authentication Mode	The MAC Authentication mode of the port, which can be enabled or disabled. When MAC Authentication is enabled on the port (along with the Authenticator role and MAC-based control mode), stations connected to the port that do not support 802.1X can still be authenticated at the RADIUS server using the station's MAC address. Specifically, when the port detects a new, unauthorized station on the port, the switch first attempts to authenticate it using 802.1X. If the station does not respond, then after a time-out period, the switch extracts the station's MAC address from the detected packets and sends this to the RADIUS server for authentication. The RADIUS server responds with an authentication result, which is then applied to the port using the station's MAC address in MAC-based control mode.
MAC Authentication Type	MAC Authentication allows network access control based on a device's MAC address. It's commonly used for devices that do not support 802.1X (e.g., printers, IP phones, IoT devices). The switch or NAS sends the MAC address as a username and password to the RADIUS server for authentication. · EAP-MD5 (Extensible Authentication Protocol - Message Digest 5)—Uses a challenge-response mechanism to protect the password. Basic EAP method provides identity protection but does not support mutual authentication. It provides limited security and is not recommended for modern deployments. · PAP (Password Authentication Protocol)—Sends username and password in plain text. Least secure method, but widely supported. Should only be used in trusted or encrypted environments. · CHAP (Challenge-Handshake Authentication Protocol)—Uses a challenge-response mechanism to validate the client. Password is never sent over the wire directly. More secure than PAP, but not as flexible or extensible as EAP.
Re-Authentication Period	The amount of time that clients can be connected to the port without being reauthenticated. Values are 1 – 65535 Seconds, or 0. If this field is set to 0, connected clients are not forced to reauthenticate periodically.
Inactivity Period	The amount of time, after which an idle client is terminated. **NOTE:** Configuration of inactivity period is applicable for data clients in Single Authentication, Multiple Authentication and Multiple Domain modes.
Maximum Users	The maximum number of clients supported on the port if the Control Mode on the port is MAC-based 802.1X authentication. This field is configurable only if the control mode is set to MAC based.

Field	Description
Unauthenticated VLAN ID	The VLAN ID of the unauthenticated VLAN. 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 and is used to 802.1X aware clients only.
Supplicant Options The fields in this section can be changed only when the selected port is configured as a supplicant port (that is, the PAE Capabilities field is set to Supplicant).	
Control Mode	The port-based access control mode on the port, which is one of the following: · Auto—The port is in an unauthorized state until a successful authentication exchange has taken place between the supplicant port, the authenticator port, and the authentication server. · Force Authorized—The port is placed into an authorized state and does not require client port-based authentication to be able to send and receive traffic.
Guest VLAN	The VLAN ID for the guest VLAN. The guest VLAN allows the port to provide a distinguished service to unauthenticated users. This feature provides a mechanism to allow users access to hosts on the guest VLAN.
MAC Authentication Type	MAC Authentication allows network access control based on a device's MAC address. It's commonly used for devices that do not support 802.1X (e.g., printers, IP phones, IoT devices). The switch or NAS sends the MAC address as a username and password to the RADIUS server for authentication. · EAP-MD5 (Extensible Authentication Protocol - Message Digest 5)—Uses a challenge-response mechanism to protect the password. Basic EAP method provides identity protection but does not support mutual authentication. More secure than PAP or CHAP for MAC authentication. · PAP (Password Authentication Protocol)—Sends username and password in plain text. Least secure method, but widely supported. Should only be used in trusted or encrypted environments. · CHAP (Challenge-Handshake Authentication Protocol)—Uses a challenge-response mechanism to validate the client. Password is never sent over the wire directly. More secure than PAP, but not as flexible or extensible as EAP.
Unauthenticated VLAN ID	The VLAN ID of the unauthenticated VLAN. 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 and is used to 802.1X aware clients only.
Start Period	The amount of time the supplicant port waits for a response from the authenticator port after sending a Start packet. If no response is received, the supplicant retransmits the Start packet.
Held Period	The amount of time the supplicant port waits before contacting the authenticator port after an active 802.1X session fails.
Maximum Start Messages	The maximum number of Start packets the supplicant port sends to the authenticator port without receiving a response before it considers the authenticator to be 802.1X-unaware.
Username	Select the Username to use for port authentication from the drop down box.

Authenticating and Initializing Port Authentication

Select one or more ports and click the ⚙▾ (**Additional Options**) drop-down menu to initiate one of the following operations (this option works only when the port is an authenticator and the operating control mode is Auto):

- Reauthenticate: select this option to force the associated interface to restart the authentication process.
- Initialize: select this option to reset the 802.1X state machine on the associated interface to the initialization state. Traffic sent to and from the port is blocked during the authentication process.

Viewing Per-port 802.1X Details

To view the 802.1X configuration on an interface, select the interface and click (**Details**). See Table 158 for information about the fields the Port Access Control Port Details page displays.

The fields that display after you click Details depend on whether the port is configured with Authenticator or Supplicant PAE Capabilities.

Local MAC Authentication Clients

Use the Local MAC Authentication Clients tile to add clients to the local database and to view entries in the database. Local MAC Authentication allows a network device (typically a switch, wireless controller, or NAC system) to authenticate clients based on their MAC address before granting network access. This method is commonly used for devices that cannot support 802.1X authentication, such as IP phones, printers, or legacy devices.

Figure 193. Local MAC Authentication Clients Tile



Table 159. Local MAC Authentication Clients Fields

Field	Description
MAC Clients	Specifies devices authenticated using their MAC address. Commonly used for non-802.1X capable devices.

To add an entry to the Local MAC Authentication Clients database, click + (**Add**) and specify the MAC address of the client.

To delete one or more clients from the database, select the check box associated with each entry to delete and click (**Remove**).

To remove all Local MAC Authentication Clients, click (**Clear All**).

Access Control Client Information

The Access Control Client Information tile displays information about the supplicant devices that are connected to the local authenticator ports. If there are no active 802.1X sessions, the table is empty.

Figure 194. Access Control Client Information Tile



Table 160. Access Control Client Information Fields

Field	Description
Interface	The local interface associated with the rest of the data in the row.
Username	The name the client uses to identify itself as a supplicant to the authentication server.
Supplicant MAC Address	The MAC address of the supplicant that is connected to the port.
Authentication Method	Indicates if client was authenticated using 802.1x credentials or based only on supplicant MAC address.
Session Time	The amount of time that has passed since the connected supplicant was granted access to the network through the authenticator port.
VLAN ID	The ID of the VLAN the supplicant was placed in as a result of the authentication process.
VLAN Assigned Reason	The reason the VLAN identified in the VLAN ID field has been assigned to the port, which can be one of the following: · Default Assigned VLAN—Client is authenticated on the port in the default VLAN and the authentication server is not RADIUS. · RADIUS Assigned VLAN—RADIUS is used for authenticating the client. · Unauthenticated VLAN—Client is authenticated on the unauthenticated VLAN. · Guest VLAN—Client is authenticated on the guest VLAN. · Voice VLAN—Client is authenticated on the voice VLAN.

Port Access Control Statistics

The Port Access Control Statistics tile shows information about the EAPOL frames and EAP messages sent and received by the local interfaces.

Figure 195. Port Access Control Statistics Tile

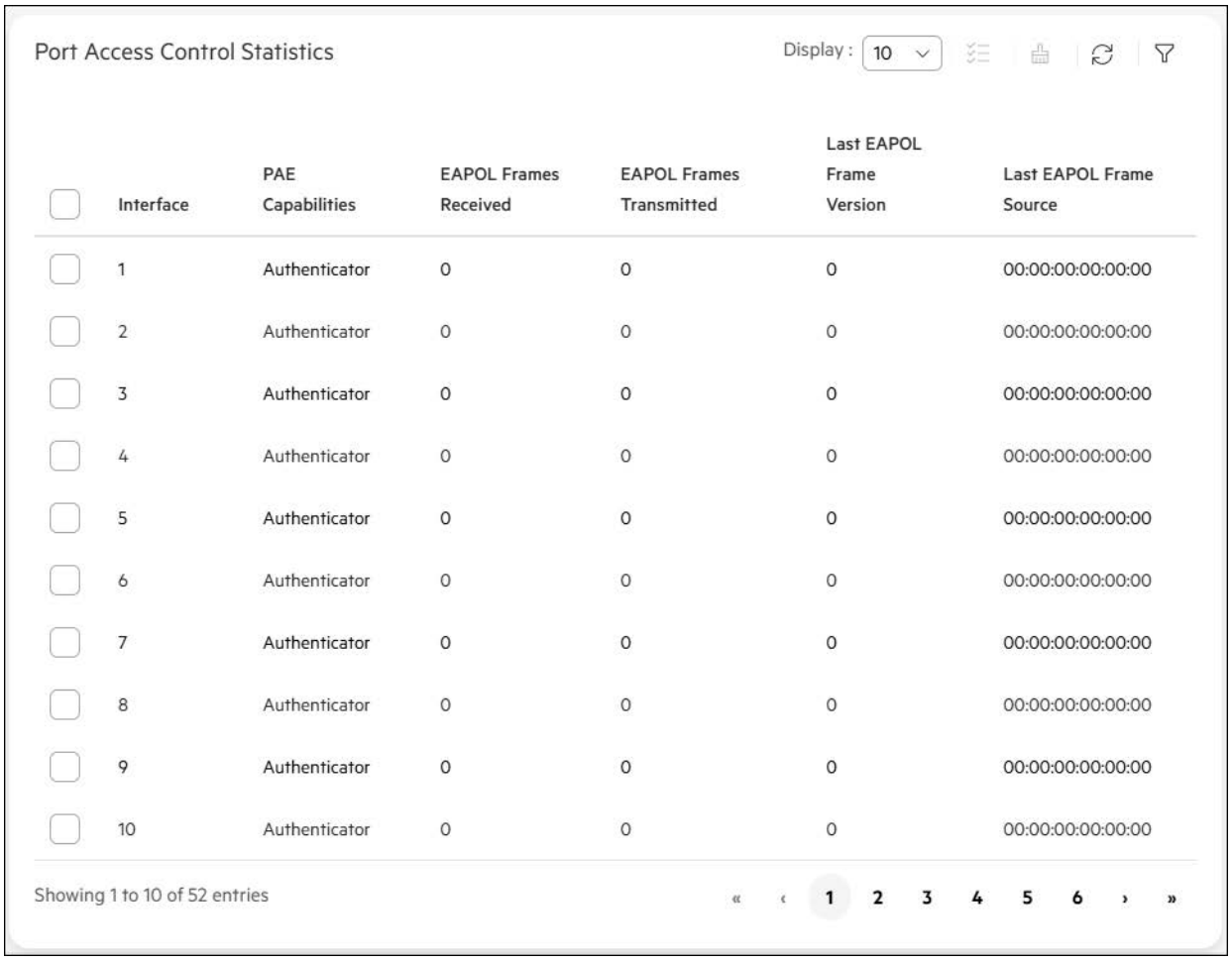


Table 161. Port Access Control Statistics Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When viewing detailed information for an interface, this field identifies the interface being viewed.
PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following: · Authenticator—The port enforces authentication and passes authentication information from a remote supplicant (similar to a client or host) to the authentication server. If the server successfully authenticates the supplicant, the port allows access. · Supplicant—The port must be granted permission by the authentication server before it can access the remote authenticator port.
EAPOL Frames Received	The total number of valid EAPOL frames received on the interface.
EAPOL Frames Transmitted	The total number of valid EAPOL frames sent by the interface.
Last EAPOL Frame Version	The protocol version number attached to the most recently received EAPOL frame.
Last EAPOL Frame Source	The Source MAC Address attached to the most recently received EAPOL frame.

To reset statistics counters to 0 for one or more interfaces, select each interface with the statistics to reset and click (**Clear**).

To view additional per-interface EAPOL and EAP message statistics, select the interface with the information to view and click (**Details**).

The following table describes the fields in the Port Access Control Statistics dialog box in addition to the fields described in Table 161. The fields that display depend on whether the interface is configured as an authenticator or supplicant.

Table 162. Port Access Control Statistics Detail Fields

Field	Description
Authenticator Fields The fields in this section are displayed only when the PAE Capabilities field for the selected port is configured as Authenticator.	
EAPOL Start Frames Received	The total number of EAPOL-Start frames received on the interface. EAPOL-Start frames are sent by a supplicant to initiate the 802.1X authentication process when it connects to the interface. This field is displayed only if the interface is configured as an authenticator.
EAPOL Logoff Frames Received	The total number of EAPOL-Logoff frames received on the interface. EAPOL-Logoff frames are sent by a supplicant to indicate that it is disconnecting from the network, and the interface can return to the unauthorized state. This field is displayed only if the interface is configured as an authenticator.
EAP Response/ID Frames Received	The total number of EAP-Response Identity frames the interface has received. EAP-Response Identity frames are sent by a supplicant to provide user information that is used to for authentication. This field is displayed only if the interface is configured as an authenticator.
EAP Response Frames Received	The total number of EAP-Response frames the interface has received. EAP-Response frames are sent from a supplicant to an authentication server during the authentication process. This field is displayed only if the interface is configured as an authenticator.
EAP Request/ID Frames Transmitted	The total number of EAP-Request Identity frames the interface has sent. EAP-Request Identity frames are sent from an authenticator to a supplicant to request user information that is used to for authentication. This field is displayed only if the interface is configured as an authenticator.
EAP Request Frames Transmitted	The total number of EAP-Request frames the interface has sent. EAP-Request frames are sent from an authentication server to the client to request authentication information. This field is displayed only if the interface is configured as an authenticator.
Invalid EAPOL Frames Received	The number of unrecognized EAPOL frames received on the interface.
EAPOL Length Error Frames Received	The number of EAPOL frames with an invalid packet body length received on the interface.
Supplicant Fields The fields in this section are displayed only when the PAE Capabilities field for the selected port is configured as Supplicant.	
EAPOL Start Frames Transmitted	The total number of EAPOL-Start frames the interface has sent to a remote authenticator. EAP OL-Start frames are sent by a supplicant to initiate the 802.1X authentication process when it connects to the interface. This field is displayed only if the interface is configured as a supplicant.
EAPOL Logoff Frames Transmitted	The total number of EAPOL-Logoff frames the interface has sent to a remote authenticator. EAPOL-Logoff frames are sent by a supplicant to indicate that it is disconnecting from the network, and the interface can return to the unauthorized state. This field is displayed only if the interface is configured as a supplicant.
EAP Response/ID Frames Transmitted	The total number of EAP-Response Identity frames the interface has sent. EAP-Response Identity frames are sent by a supplicant to provide user information that is used to for authentication. This field is displayed only if the interface is configured as a supplicant.

Field	Description
EAP Response Frames Transmitted	The total number of EAP-Response frames the interface has transmitted. EAP-Response frames are sent from a supplicant to an authentication server during the authentication process. This field is displayed only if the interface is configured as an supplicant.
EAP Request/ID Frames Received	The total number of EAP-Request Identity frames the interface has received. EAP-Request Identity frames are sent from an authenticator to a supplicant to request user information that is used to for authentication. This field is displayed only if the interface is configured as a supplicant.
EAP Request Frames Received	The total number of EAP-Request frames the interface has received. EAP-Request frames are sent from the authentication server to the supplicant during the authentication process. This field is displayed only if the interface is configured as a supplicant.
Invalid EAPOL Frames Received	The number of unrecognized EAPOL frames received on the interface.
EAPOL Length Error Frames Received	The number of EAPOL frames with an invalid packet body length received on the interface.

Port Security

Port security, also known as port MAC locking, allows you to limit the number of source MAC addresses that can be learned on a port. When port security is enabled on a port, learning of new MAC addresses are removed from the Layer-2 Forwarding Database. If a port reaches the configured limit, any other addresses beyond that limit are not learned, and the frames can be discarded. Frames with a source MAC address that have already been learned will be forwarded. Port security can help secure the network by preventing unknown devices from forwarding packets into the network.

To access the Port Security page, click **Security > Port Security** in the navigation pane.

Port Security Configuration

Use the Port Security Configuration tile to view and configure the port security settings for each interface.

To configure port security settings on one or more interfaces, select the interface or interfaces to configure, and click (**Edit**).

To configure all interfaces with the same settings, click (**Edit All**).

Figure 196. Port Security Configuration Tile

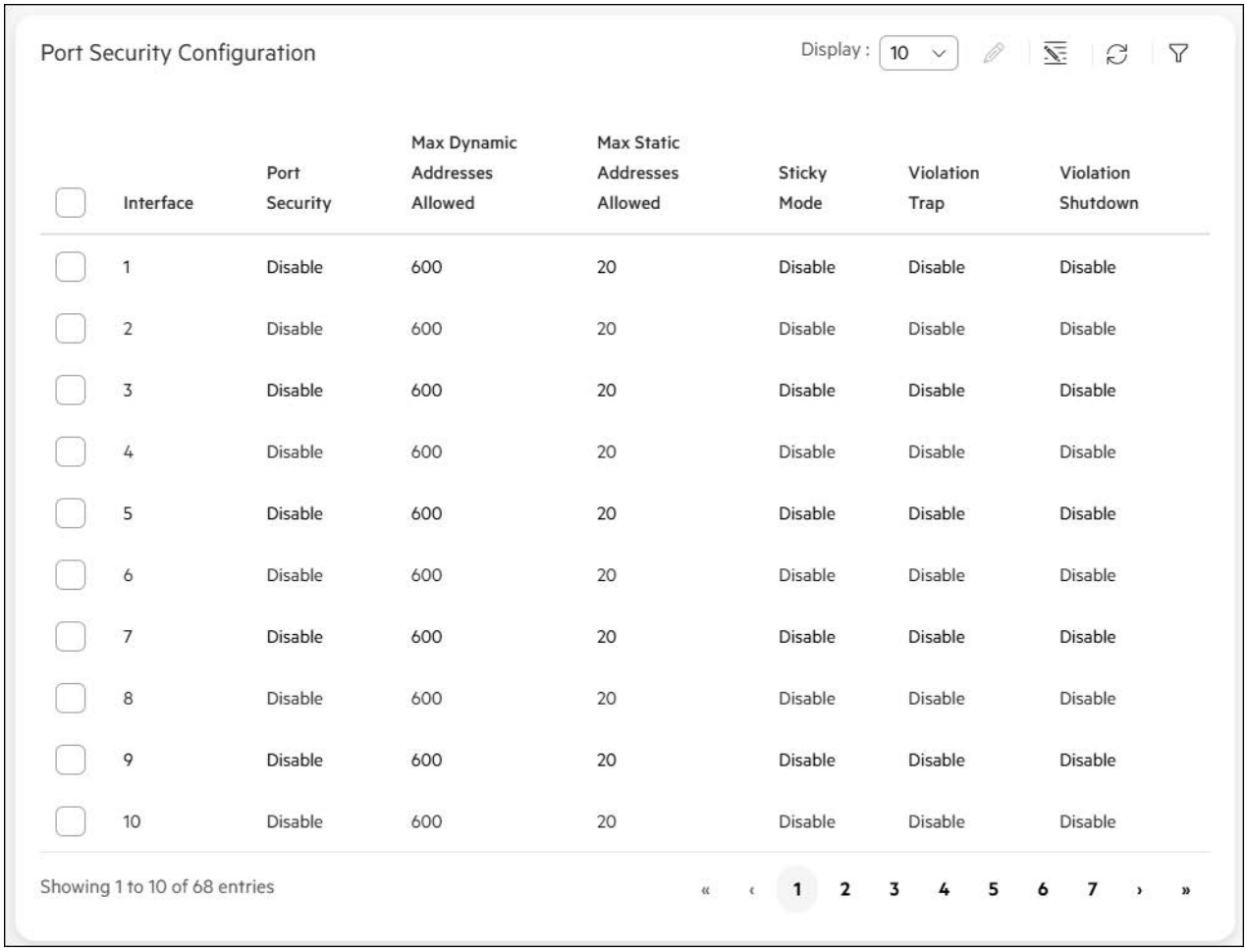


Table 163. Port Security Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring the port security settings for one or more interfaces, this field lists the interfaces that are being configured.
Port Security	The administrative mode of the port security feature on the interface.
Max Dynamic Addresses Allowed	The number of source MAC addresses that can be dynamically learned on an interface. If an interface reaches the configured limit, any other addresses beyond that limit are not learned, and the frames are discarded. Frames with a source MAC address that has already been learned will be forwarded. A dynamically-learned MAC address is removed from the MAC address table if the entry ages out, the link goes down, or the system resets. Note that the behavior of a dynamically-learned address changes if the sticky mode for the interface is enabled or the address is converted to a static MAC address.
Max Static Addresses Allowed	The number of source MAC addresses that can be manually added to the port security MAC address table for an interface. If the port link goes down, the statically configured MAC addresses remain in the MAC address table. The maximum number includes all dynamically-learned MAC addresses that have been converted to static MAC addresses.

Field	Description
Sticky Mode	The sticky MAC address learning mode is one of the following: · Enabled—MAC addresses learned or manually configured on this interface are learned in sticky mode. A sticky-mode MAC address is a MAC address that does not age out and is added to the running configuration. If the running configuration is saved to the startup configuration, the sticky addresses are saved to persistent storage and do not need to be relearned when the switch restarts. Upon enabling sticky mode on an interface, all dynamically learned MAC addresses in the MAC address table for that interface are converted to sticky mode. Additionally, new addresses dynamically learned on the interface will also become sticky. · Disabled—When a link goes down on a port, all of the dynamically learned addresses are cleared from the source MAC address table the feature maintains. When the link is restored, the interface can once again learn addresses up to the specified limit. If sticky mode is disabled after being enabled on an interface, the sticky-mode addresses learned or manually configured on the interface are converted to dynamic entries and are automatically removed from persistent storage.
Violation Trap	Indicates whether the port security feature sends a trap to the SNMP agent when a port is locked and a frame with a MAC address not currently in the table arrives on the port. A port is considered to be locked once it has reached the maximum number of allowed dynamic or static MAC address entries in the port security MAC address table.
Violation Shutdown	Indicates whether the port security feature shuts down the port when a port is locked and a frame with a MAC address not currently in the table arrives on the port. A port is considered to be locked once it has reached the maximum number of allowed dynamic or static MAC address entries in the port security MAC address table.

Static/Dynamic MAC Addresses

To view the static MAC address information and add static MAC addresses to the port security database, click the Static MAC Address tab.

To view the dynamic MAC address information, click the Dynamic MAC Address tab.

Static MAC Addresses Tab

Use the Static MAC Addresses tab to display, add, and remove the static MAC addresses of hosts that are allowed to send traffic to specific interfaces on the switch. The number of MAC addresses you can associate with each interface is determined by the maximum static MAC addresses allowed on a given interface.

The Static MAC Address tab lists the following type of MAC addresses learned on ports that are enabled for port security:

- MAC addresses learned on interfaces set to sticky mode disabled, which were converted to static addresses by users.
- MAC addresses learned dynamically by switch on interfaces that are sticky mode enabled.

Use the buttons to perform the following tasks:

To associate a static MAC address with an interface, click + (**Add**) and configure the settings in the available fields.

To remove one or more configured static MAC address entries, select each entry to delete and click (**Remove**).

Figure 197. Static MAC Addresses Tab



Table 164. Static MAC Addresses Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When adding a static MAC address entry, use the Interface menu to select the interface to associate with the permitted MAC address.
Static MAC Address	The MAC address of the host that is allowed to forward packets on the associated interface.
VLAN ID	The ID of the VLAN that includes the host with the specified MAC address.
Sticky Mode	Indicates whether the static MAC address entry is added in sticky mode. When adding a static MAC address entry, the Sticky Mode field can be selected only if it is enabled on the interface.

Dynamic MAC Addresses

The Dynamic MAC Addresses tab shows the dynamic MAC address entries that have been learned on interfaces set to sticky mode disable. From this page, you can also convert dynamic MAC address entries to static MAC address entries for a given interface.

Figure 198. Dynamic MAC Addresses Tab

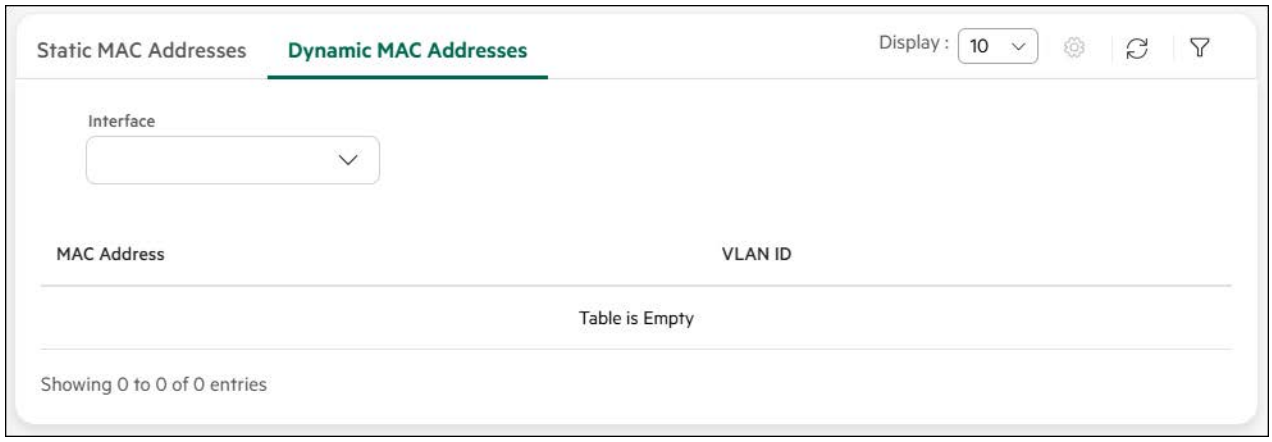


Table 165. Dynamic MAC Addresses Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. Use the Interface menu to select the interface to display. **NOTE:** Only interfaces that have Port Security enabled and Sticky Mode disabled are available for selection.
Dynamic MAC Address	The MAC address that was learned on the port. An address is dynamically learned when a frame arrives on the interface and the source MAC address in the frame is added to the MAC address table.
VLAN ID	The VLAN ID specified in the Ethernet frame received by the interface.

To convert dynamic MAC addresses to static MAC addresses, select the check box associated with each address to convert and click (**Convert to Static**) and then click **Apply**.

The converted dynamic MAC addresses can be viewed in the Static MAC Addresses tab. They are converted with Sticky mode Disabled.

Protected Ports

The Protected Ports feature provides L2 isolation between interfaces (Ethernet ports and LAGs) that share the same broadcast domain (VLAN) with other interfaces.

Ports can be defined to one of the following two modes:

- Protected ports: These ports can send traffic only to unprotected ports. Packets received on a protected port are filtered at the egress of the other protected ports.
- Unprotected ports: These ports send traffic to any port. This is the default setting of all interfaces.

Port Protection is independent from any and all other features and configuration settings. For example, a user can place two protected ports into a common VLAN, and they will not be able to communicate with each other. By the same token, a protected port will not be able to communicate with an unprotected port if the two ports are not in the same VLAN.

To access the **Protected Ports** page, click **Security > Protected Ports** in the navigation pane.

Protected Ports Configuration

Use the Protected Ports Configuration tile to configure and view protected ports groups.

Figure 199. Protected Ports Configuration Tile

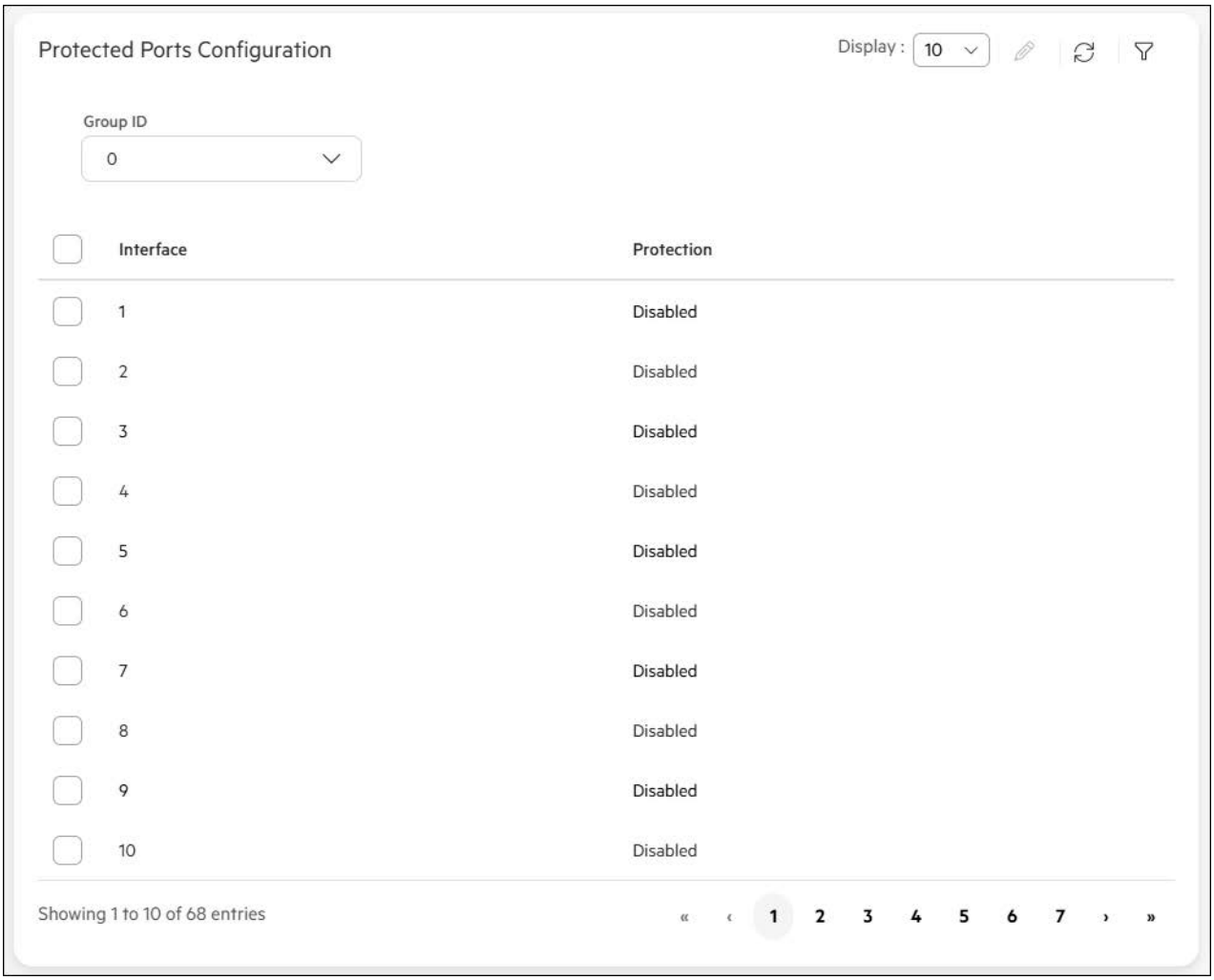


Table 166. Protected Ports Configuration Fields

Field	Description
Group ID	The Group ID for the protected port group.
Interface	The port or trunk ID.
Protection	Displays the Admin state of Port Protection on the interface: · Disabled—The port is an unprotected port. This is the default setting. · Enabled—The port is a protected port.

To change the Protection setting of an interface:

1. Select the ID of the protected port group to configure:
2. Select the check box associated with each interface to edit.
3. Click (**Edit**) to display the Edit Port Protection dialog box.
4. Toggle the control to enable or disable Port Protection as needed.
5. Click **Apply**.

DHCP Snooping and IP Source Guard

DHCP snooping provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, also referred to as a DHCP snooping binding table. DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. DHCP snooping differentiates between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

Interfaces are defined as trusted or untrusted by the administrator. Trusted interfaces are usually connected to DHCP servers or to switches/hosts that DHCP packet filtering is not required for them. Untrusted interfaces are connected to untrusted hosts, or to switches that are connected to untrusted hosts.

The database is updated by interception of DHCPACK, DHCPDECLINE and DHCPRELEASE packets.

The switch does not update the DHCP snooping database when a station moves to another interface.

When DHCP snooping is disabled for a VLAN the bindings that were collected for that VLAN are removed.

Periodically the Database is saved to the backup database on switch flash memory. This database is persistent across reboot. To ensure that the lease time in the database is accurate, backup to database will be active only if the system clock was set through NTP, DHCP on the switch, or manually by user. Backup to database is optional. You can enable or disabled the backup.

IP source guard (IPSG) is a security feature that restricts IP traffic on non-routed, Layer 2 interfaces by filtering traffic based on the DHCP snooping table, both snooped and manual entries, or statically configured IP source binding. Traffic from IP addresses that are not in the binding database is denied.

IPSG can be used to prevent traffic attacks caused when a host tries to use the IP address of its neighbor.

If DHCP snooping is enabled even on a single VLAN port is member of, then IPSG is active on all VLANs configured on the port.

The IPSG uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IPSG addresses are inactive because of a lack of TCAM resources.

Once every minute the software conducts a search for available space in the TCAM for the inactive IPSG addresses.

DHCP Snooping Configuration

Use the DHCP Snooping Configuration tile to configure the global DHCP snooping and IPSG options.

Figure 200. DHCP Snooping Configuration Tile



Table 167. DHCP Snooping Configuration Fields

Field	Description
DHCP Snooping	Enable or disable. By default, DHCP snooping is disabled. **NOTE:** DHCP snooping still needs to be enabled per VLAN to make it operational for that VLAN.
Verify MAC Address	Enable or disable. By default, MAC address verification is enabled. If enabled, the switch verifies that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address in the packet.

DHCP Snooping VLAN Configuration

Use the DHCP Snooping VLAN Configuration tile to view and configure the DHCP snooping mode on the VLANs configured on the switch.

Figure 201. DHCP Snooping VLAN Configuration Tile

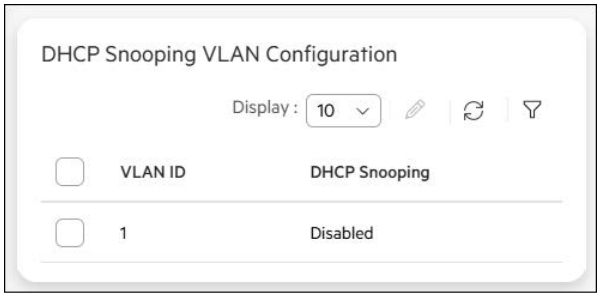


Table 168. DHCP Snooping VLAN Configuration Fields

Field	Description
VLAN ID	Identifier for the VLAN.
DHCP Snooping	Enable or disable. By default, DHCP snooping is disabled.

To change the DHCP Snooping setting on one or more VLANs:

1. Select the check box associated with each VLAN to configure
2. Click (**Edit**). The DHCP Snooping VLAN Configuration dialog box appears.
3. Toggle the control to enable or disable DHCP Snooping on the selected VLANs.
4. Click **Apply**.

DHCP Snooping Interface Configuration

Use the DHCP Snooping Interface Configuration tile to set ports to DHCP snooping trust mode enable or disable, and to enable or disable IP Source Guard.

Figure 202. DHCP Snooping Interface Configuration Tile

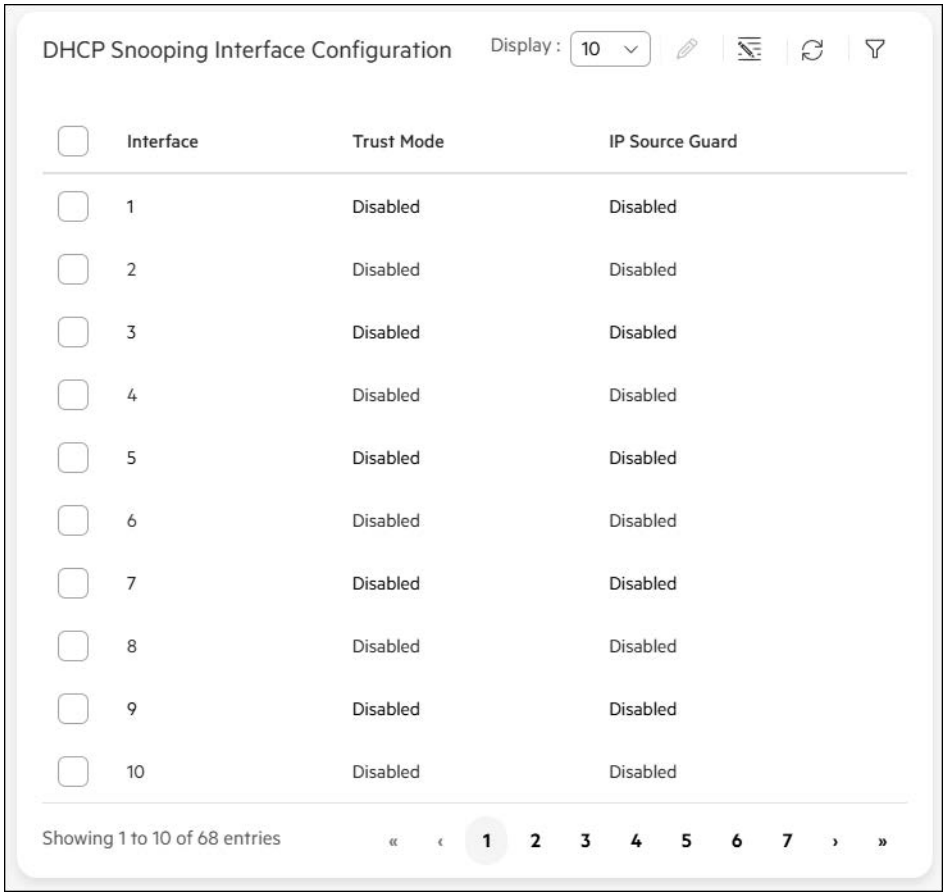


Table 169. DHCP Snooping Interface Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When editing the settings for one or more interfaces, this field lists the interfaces that are being configured.
Trust Mode	Enabled or Disabled. By default, Trust Mode is disabled.
IP Source Guard	Enabled or Disabled. By default, IP Source Guard is disabled.

1. Select the interface or interfaces to configure:
   - To change the DHCP Snooping setting on one or more interfaces, select the check box associated with each interface to configure and click (**Edit**).
   - To configure all interfaces with the same settings, click (**Edit All**)

   The DHCP Snooping Interface Configuration dialog box appears.
2. Toggle the controls to enable or disable Trust Mode and/or IP Source Guard on the selected Interfaces.
3. Click **Apply**.

Binding Database

Use the Binding Database tile to view the DHCP Snooping Binding table, which shows DHCP clients learned on untrusted ports. From this tile, you can also add static entries to the DHCP binding database.

Figure 203. Binding Database Tile



Table 170. Binding Database Fields

Field	Description
VLAN ID	The VLAN to which the DHCP client is connected.
MAC Address	DHCP client Source MAC address.
IP Address	DHCP client IP address.
Interface	Switch interface to which the DHCP client is connected.
Lease Time	DHCP address lease time. This field can be configured in the Add DHCP Snooping Binding dialog box if the Volatile option is set to Yes. Setting the lease time to 0 means that the lease does not expire.
Type	Binding entry type, which can be one of the following: · Static—The binding has been manually added to the database · Dynamic—The binding has been learned dynamically · Volatile—The binding is not saved if the switch reboots or if the lease time expires.
Volatile	This field is available when adding a static binding and has the following options: · Yes—The binding is removed from the database if the system reboots or if the lease time expires. · No—The binding persists across a system reboot and does not expire.

To add a static entry to the DHCP Snooping Binding table, click + (**Add**) and configure the fields described in Table 170.

To delete one or more clients from the database, select the check box associated with each entry to delete and click (**Remove**).

To clear all volatile entries in the Binding Database, click (**Clear All**).

ARP Attack Protection

The ARP attack protection security feature validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

The ARP inspection feature defines two types of interfaces: Trusted and Untrusted. ARP inspection is performed only on untrusted interface. The switch does not check ARP packets that are received on the trusted interface; it simply forwards the packets.

When a packet arrives on an untrusted interface the following logic is implemented:

- The VLAN that the packet arrived on has an ARP static binding list defined, then search that list.
  - If the IP address is found and the MAC address in the list matches the packet's MAC address, the packet is valid and is forwarded.
  - If the IP address is found and the MAC address in the list does not match the packet's MAC address, the packet is not valid and is dropped.
- If the packet's IP address was not found in the ARP static binding, and DHCP snooping is enabled for that VLAN, then search the DHCP snooping database for the packet's pair.
  - If the pair was found, and the MAC address and the interface in the database match the packet's MAC address and ingress interface, the packet is valid and is forwarded.
  - If the packet's IP address was not found in the ARP static binding and in the DHCP snooping, the packet is not valid and is dropped.
- If the ARP packet's header check is configured then, the following additional checks are performed:
  - Source MAC: Compare the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.
  - Destination MAC: Compare the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses.
  - IP addresses: Compare the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

Global Configuration

Use this tile to configure the global ARP Attack options

Figure 204. ARP Attack Global Configuration Tile

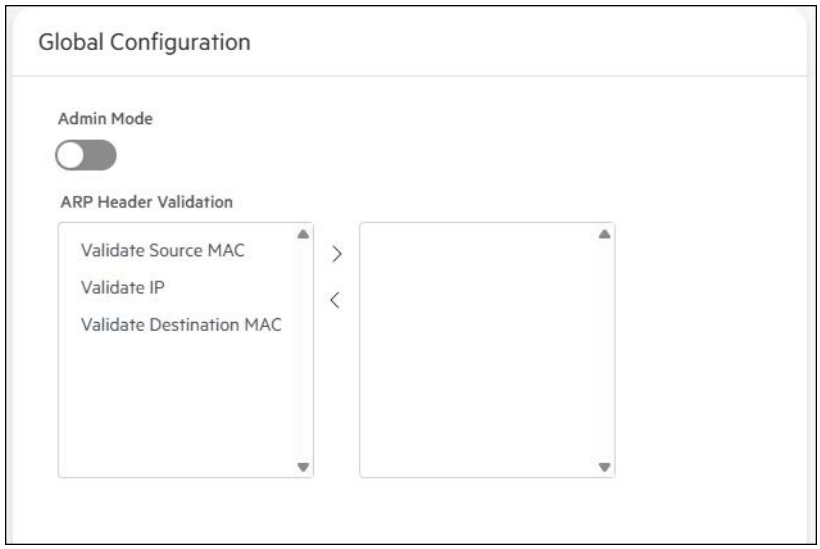


Table 171. ARP Attack Global Configuration Fields

Field	Description
Admin Mode	Enables or Disables the ARP attack protection administrative mode. When enabled, protects the Switch CPU from the DOS attacks with ARP messages.
ARP Header Validation	Enables (right panel) or disables (left panel) additional checks on the ARP packets header: · Validate Source MAC—When this option is selected, ARP attack protection verifies that the sender hardware address in the ARP packet equals the source MAC address in the Ethernet header. If the addresses do not match, the ARP packet is dropped. · Validate Destination MAC—When this option is selected, ARP attack protection verifies that the target hardware address in the ARP packet equals the destination MAC address in the Ethernet header. If the addresses do not match, the ARP packet is dropped. This check applies only to ARP responses because the target MAC address is unspecified in ARP requests. · Validate IP—When this option is selected, ARP attack protection drops ARP packets with an invalid IP address. The following IP addresses are considered invalid: o 0.0.0.0 o 255.255.255.255 o All IP multicast addresses o All class E addresses (240.0.0.0/4) o Loopback addresses (in the range 127.0.0.0/8)

Interface Settings

Use the Interface Settings tile to set the interface mode to Trusted or Untrusted:.

Figure 205. Interface Settings Tile

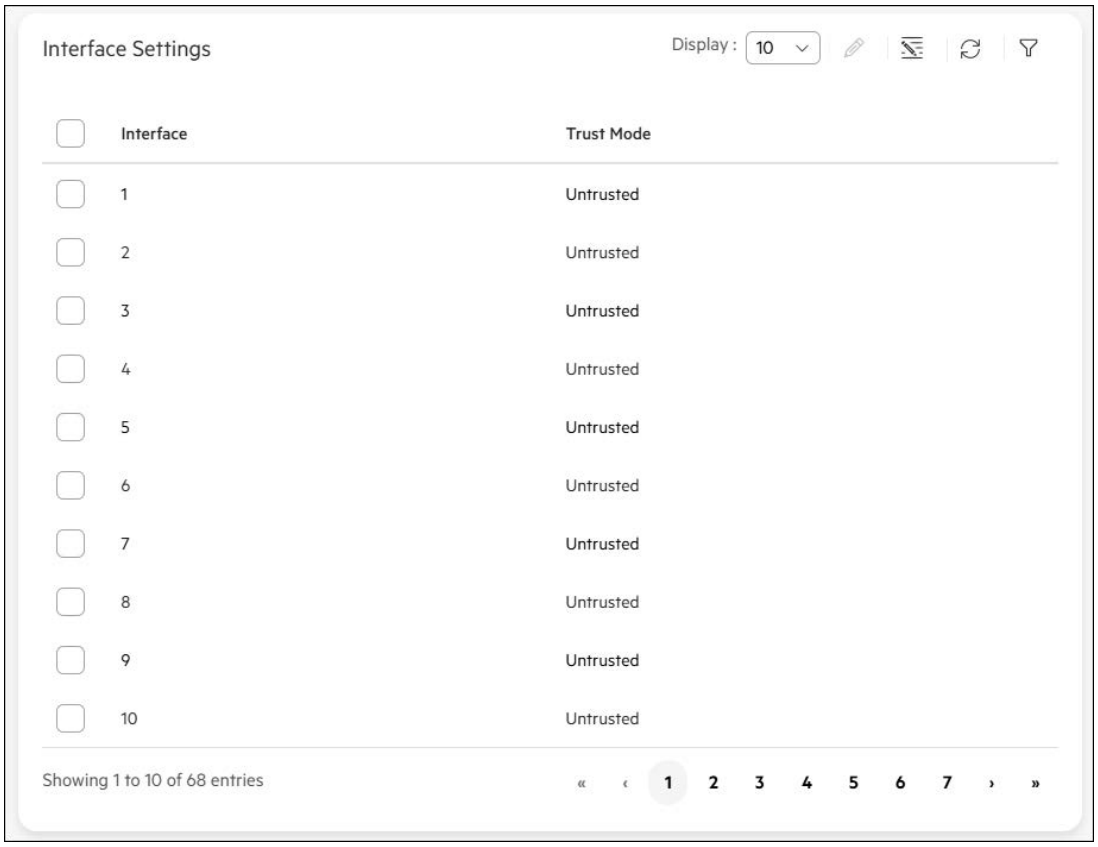


Table 172. Interface Settings Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When editing the settings for one or more interfaces, this field lists the interfaces that are being configured.
Trust Mode	Trusted or Untrusted. If Untrusted, ARP Protection validation is performed on the interface.

To change the ARP Attack Protection trust mode for one or more interfaces:

1. Select the interface or interfaces to configure:
   - To change the trust mode setting on one or more interfaces, select the check box associated with each interface to configure and click (**Edit**).
   - To configure all interfaces with the same settings, click (**Edit All**)

   The Edit ARP Protection Interface Settings dialog box appears.
2. Toggle the control to configure the selected interfaces as trusted or untrusted.
3. Click **Apply**.

ARP Access Control Rules

Use the ARP Access Control Rules tile to configure rules used to validate ARP frames.

Figure 206. ARP Access Control Rules Tile

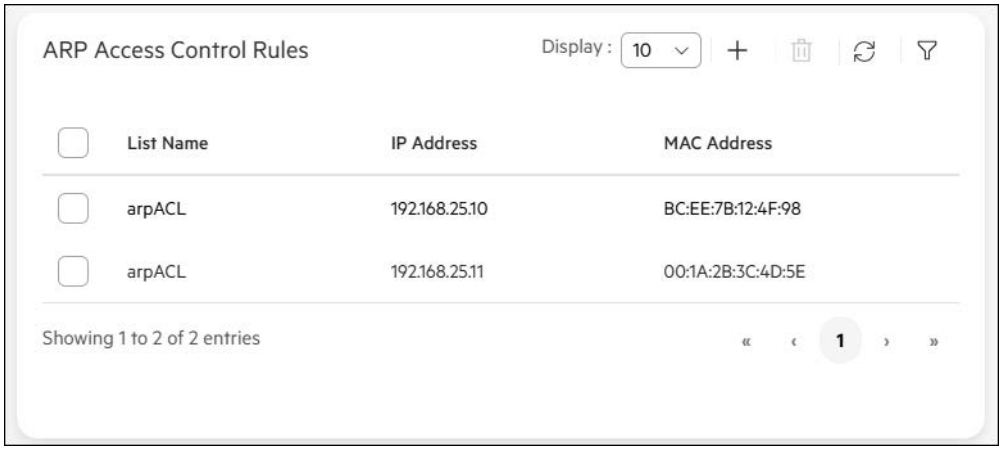


Table 173. ARP Access Control Rules Fields

Field	Description
List Name	The name of the list of access control rules.
IP Address	The IP address of a trusted ARP frame (associated to a MAC address in this row).
MAC Address	The MAC address of a trusted ARP frame (associated to an IP Address in this row).

To add a trusted ARP frame, click + (**Add**). For the List Type, select New List to create a new list with an access rule. To create an access rule on an existing list, click Existing List and select the list from the drop-down menu.

For either a new or existing list, specify the IP address and MAC address of the trusted frame in the available fields.

To remove one or more configured entries, select each entry to delete and click (**Remove**).

VLAN Settings

Use the VLAN Settings tile to enable or disable ARP protection on VLAN interfaces.

Figure 207. VLAN Settings Tile

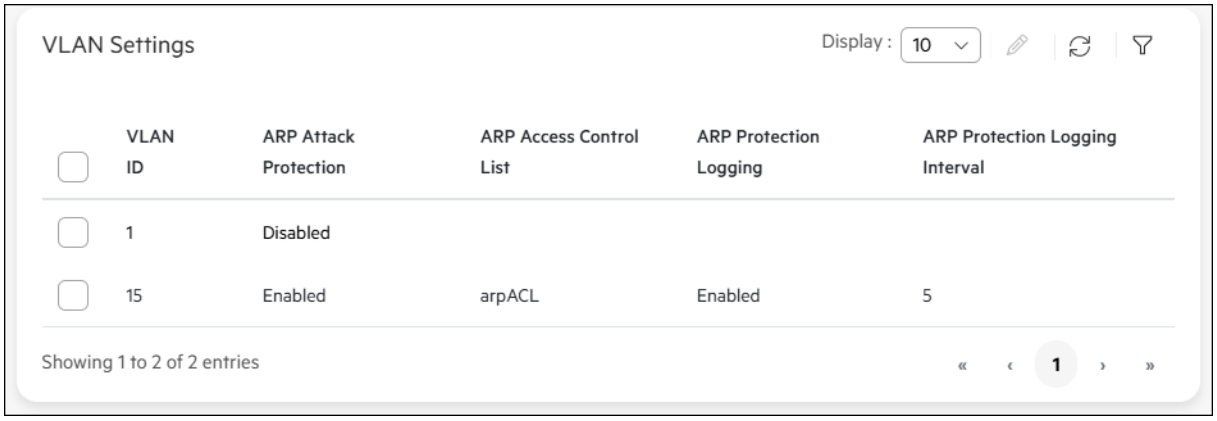


Table 174. VLAN Settings Fields

Field	Description
VLAN ID	The VLAN to which the ARP Attack Protection setting is connected.
ARP Attack Protection	Enable or disable. By default, ARP Protection is disabled.
ARP Access Control List	Association of the VLAN to an ARP Access control List created by user.
ARP Protection Logging	Enabled or disable. By default, ARP Protection Logging is enabled. If enabled, when an ARP attack occurs, a SYSLOG message is sent.
ARP Protection Logging Interval	If ARP Protection Logging is enabled, use this setting to define the interval between SYSLOG messages. By default, the interval is 5 minutes.

To change the ARP Attack Protection settings on one or more VLANs, select the check box associated with each VLAN to configure and click (**Edit**). If you enable ARP Attack Protection on the selected VLANs, you can also associate the protection with an ARP Access Control List.

Denial of Service

The HPE Networking Instant On 1940 Switch Series includes Denial-of-Service (DoS) and ICMP (ping) protection features to help protect against various high-volume traffic scenarios or malicious attacks.

A DoS attack is an attempt to saturate the switch or the network, with external communication requests to prevent the switch, or network from performing efficiently, or at all. You can enable DoS protection that prevents common types of DoS attacks.

The ICMP security options help prevent the switch and the network from attacks that involve issues with the ICMP echo request packets (pings) that the switch receives.

To display the Denial of Service page, click **Security > Denial of Service** in the navigation pane.

If you modify any settings on the page, click **Apply** to save any changes for the current boot session. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

TCP Settings

The options on the TCP Settings tile help prevent the device and the network from attacks that exploit the TCP header size or the information in the TCP or UDP headers of packets that the device receives.

Figure 208. TCP Settings Tile

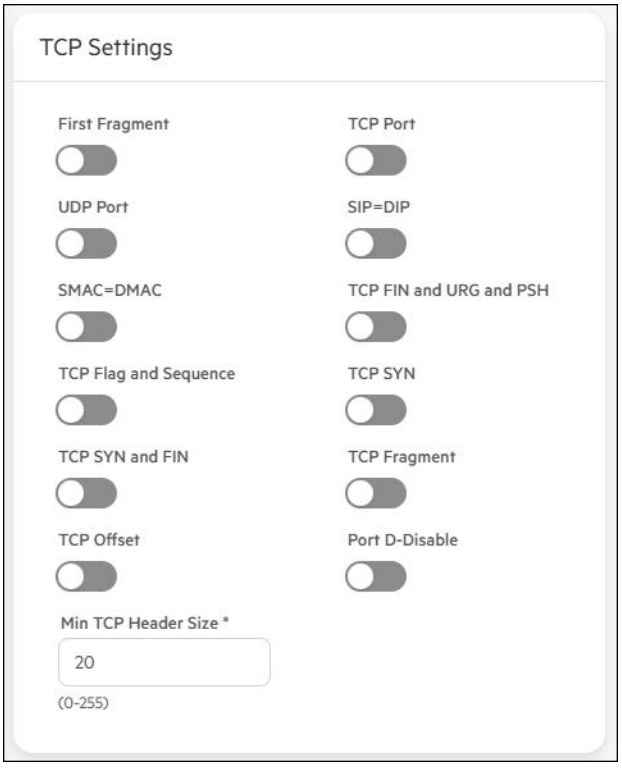


Table 175. TCP Settings Fields

Field	Description
First Fragment	When enabled, the device drops packets that have a TCP header smaller than the value configured in the Min TCP Header Size field.
TCP Port	When enabled, the device drops packets that have the TCP Source Port equal to the TCP destination port.

Field	Description
UDP Port	When enabled, the device drops packets that have the UDP Source Port equal to the UDP destination port.
SIP=DIP	When enabled, the device drops packets that have a source IP address equal to the destination IP address.
SMAC=DMAC	When enabled, the device drops packets that have a source MAC address equal to the destination MAC address.
TCP FIN and URG and PSH	When enabled, the device drops packets that have TCP Flags FIN, URG, and PSH set and a TCP Sequence Number equal to 0.
TCP Flag and Sequence	When enabled, the device drops packets that have TCP Flag SYN set and TCP Source Port less than 1024 or TCP Control Flags set to 0 and TCP sequence number set to 0 or TCP Flags FIN, URG, and PSH set and TCP sequence number set to 0 or both TCP Flags SYN and FIN set.
TCP SYN	When enabled, the device drops packets that have the TCP Flag SYN set and the Source Port is less than 1024.
TCP SYN and FIN	When enabled, the device drops packets that have TCP Flags SYN and FIN set.
TCP Fragment	When enabled, the device drops packets that have a TCP payload where the IP payload length minus the IP header size is less than the minimum allowed TCP header size.
TCP Offset	When enabled, the device drops packets that have a TCP header Offset set to 1.
Port D-Disable	When enabled, the device can diagnostically disable the interface if it might be exposed to DoS attacks.
Min TCP Header Size	The minimum TCP header size allowed. If First Fragment DoS prevention is enabled, the device will drop packets that have a TCP header smaller than this configured value.

ICMP Settings

The options on the ICMP Settings tile help prevent the device and the network from attacks that involve issues with the ICMP echo request packets (pings) that the device receives.

Figure 209. ICMP Settings Tile

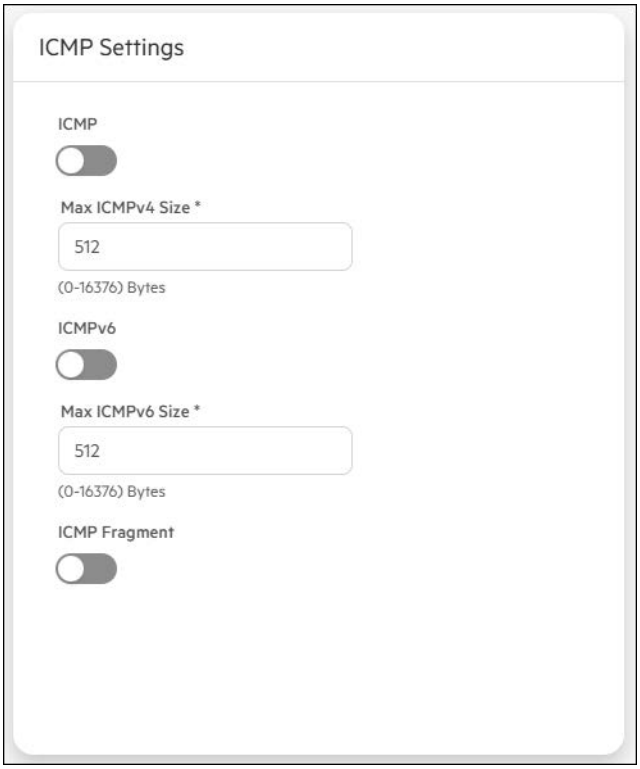


Table 176. ICMP Settings Fields

Field	Description
ICMP	Enable this option to allow the device to drop ICMP packets that have a type set to ECHO_REQ (ping) and a payload size greater than the ICMP payload size configured in the Max ICMPv4 Size field.
Max ICMPv4 Size	The maximum allowed ICMPv4 packet size. If ICMP DoS prevention is enabled, the device will drop ICMPv4 ping packets that have a size greater than this configured maximum ICMPv4 packet size.
ICMPv6	Enable this option to allow the device to drop ICMP packets that have a type set to ECHO_REQ (ping) and a payload size greater than the ICMP payload size configured in the Max ICMPv6 Size field.
Max ICMPv6 Size	The maximum allowed IPv6 ICMP packet size. If ICMP DoS prevention is enabled, the switch will drop IPv6 ICMP ping packets that have a size greater than this configured maximum ICMPv6 packet size.
ICMP Fragment	Enable this option to allow the device to drop fragmented ICMP packets.

Use the Diagnostics pages to help troubleshoot network issues, view log and configuration information, reboot the switch, and reset the HPE Networking Instant On 1940 Switch Series series switch to factory defaults.

Logging

The HPE Networking Instant On 1940 Switch Series includes system logging to maintain a record of events that occur within the hardware and software.

Beyond simple troubleshooting, logging can provide administrators with the following information:

- Audit Trails: Tracking who changed a configuration and when.
- Performance Monitoring: Identifying bandwidth bottlenecks or recurring errors.
- Security Analysis: Spotting patterns that might indicate a MAC spoofing attack or a loop in the network.

To configure log setting and display the Logging page, click **Diagnostics > Logging** in the navigation pane.

Unexpected Restart Information

The Unexpected Restart Information tile appears only if an unexpected restart that hasn't been cleared is registered on the switch. When an unexpected restart has occurred, a notification appears on the masthead. Click this notification icon to navigate to this page.

If there has been an unexpected restart of the switch, additional information is displayed near the top of the Logging page to alert the user of the event. The Crash Log text box displays information about the restart event, which may be helpful to technical support in diagnosing its cause. The crash log is part of the Log File entries. The file is stored in non-volatile memory so that it is preserved upon reboot.

When the switch is reset to factory defaults, all crash log information is erased.

To clear the unexpected restart alert, click Clear Unexpected Restart. This action clears the unexpected restart notification from the masthead and the Unexpected Restart Information tile. Click Save Crash Log to save the contents of the crash log to a text file using the browser save functionality.

Figure 210. Crash Log Information on Log Page



Global Log Settings

Use the Global Log Settings tile to define buffered logging settings. These log messages are not preserved across device reboots.

Figure 211. Global Log Settings Tile

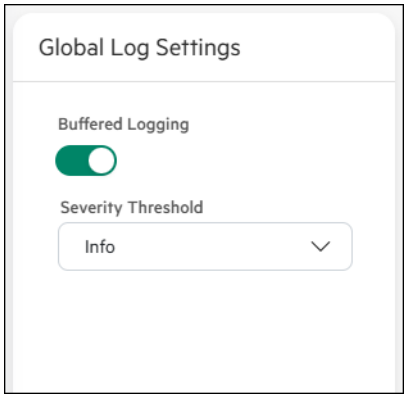


Table 177. Global Log Settings Fields

Field	Description
Buffered Logging	Enable or disable buffered logging.
Severity Threshold	Choose the appropriate severity threshold from the drop-down button. The severity can be one of the following (lowest to highest): · Debug—The switch is providing debug-level information. · Info—The switch is providing non-critical information. This is the default level. · Notice—The switch is experiencing normal but significant conditions. · Warning—The switch is experiencing conditions that require user attention. · Error—The switch is experiencing non-urgent failures. · Critical—The switch is experiencing primary system failures. · Alert—Action must be taken immediately. · Emergency—The switch is unusable. When selecting a certain severity threshold, the switch will provide logs with that severity and all higher severity levels.

Remote Log Server

Use the Remote Log Server tile to enable logging messages to a remote SYSLOG server, and to define the server address and other settings.

Figure 212. Remote Log Server Tile

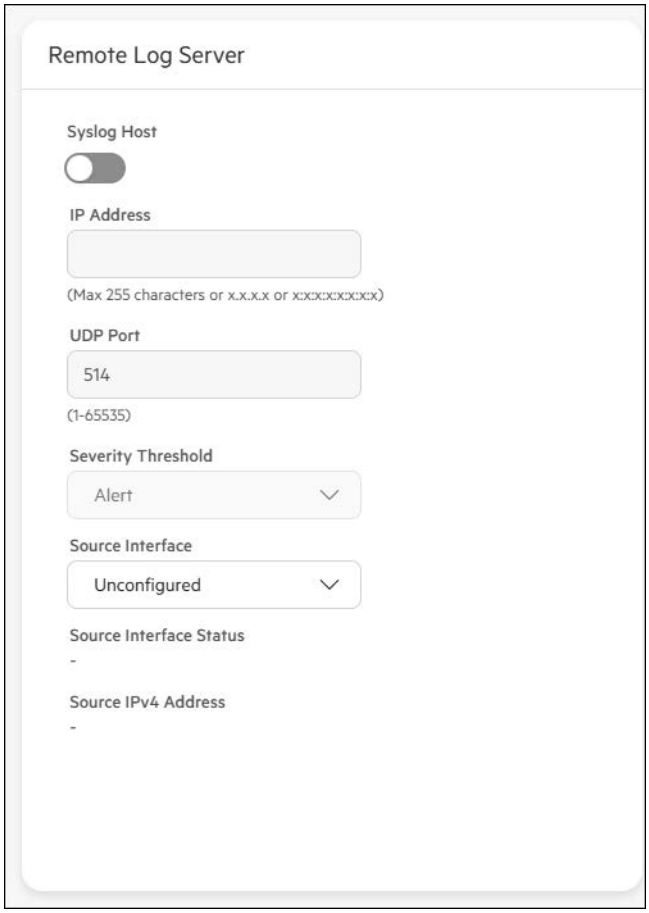


Table 178. Remote Log Server Fields

Field	Description
Syslog Host	Enables and disables logging to configured syslog host. When the syslog admin mode is disabled, the switch does not relay logs to syslog host. When enabled, messages are sent to configured host. This feature is disabled by default
Server Address	The IP address of the remote host that receives the log messages. The address can be one of the following options: · IPv4 address · IPv6 address · Hostname
UDP Port	The UDP port, on the logging host, to send syslog messages. The port ID can be any value from 1 to 65535. The default is 514
Severity Threshold	Choose the appropriate severity threshold from the drop-down button.

Field	Description
Source Interface	Configures the physical or logical interface to use as the logging (Syslog) client source interface. When an IP address is configured on the source interface, this address is used for all Syslog communications between the local logging client and the remote Syslog server. The IP address of the designated source interface is used in the IP header of Syslog management protocol packets. This allows security devices, such as firewalls, to identify all source packets coming from a specific device. The following options are available for the type of interface to use as the source for outgoing Syslog packets: · Unconfigured—The primary IP address of the originating (outbound) interface is used as the source address. · Network Port—The Network port source IP is used as the source address. · Interface—Based on the selected physical port to use as the source interface, the primary IP address of that physical port is used as the source address. · VLAN ID—Based on the selected VLAN to use as the source interface, the primary IP address of that VLAN routing interface is used as the source address.
Source IPv4 Address	Displays the primary IPv4 address associated with the selected source interface.
Source Interface Status	Indicates the current link status of the selected source interface. These are the possible values: · Link up. · Link down.

Trap Configuration

Use the Trap Configuration tile to specify which software features should generate SNMP traps. If the trap flag is enabled for a feature and a significant event occurs, the SNMP agent on the device sends a trap message to any enabled SNMP trap receivers and writes a message to the trap log.

Figure 213. Trap Configuration Tile

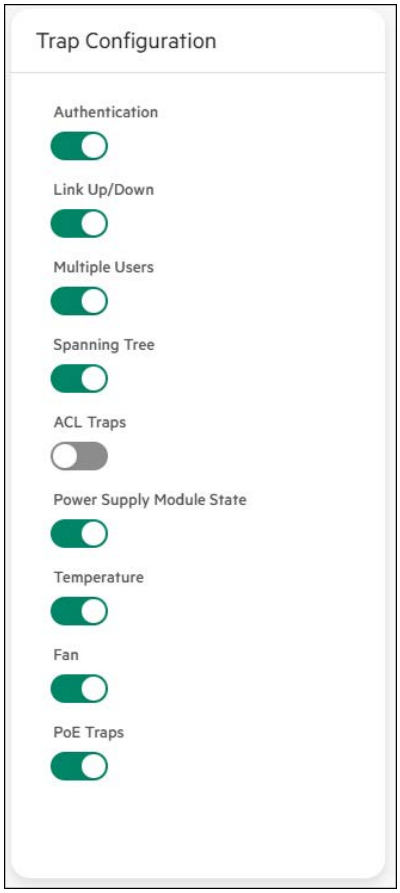


Table 179. Trap Configuration Fields

Field	Description
Authentication	Enables or disables SNMP notifications when events involving authentication occur, such as when a user attempts to access the device management interface and fails to provide a valid username and password.
Link Up/Down	Enables or disables SNMP notifications when the administrative or operational state of a physical or logical link changes.
Multiple Users	Enables or disables SNMP notifications when the same user ID is logged into the device more than once at the same time (either via telnet or the serial port).
Spanning Tree	Enables or disables SNMP notifications when various spanning tree events occur.
ACL Traps	Enables or disables SNMP notifications when a packet matches a configured ACL rule that includes ACL logging.
Power Supply Module State	Enables or disables SNMP notifications when power supply events occur.
Temperature	Enables or disables SNMP notifications when temperature events occur.
Fan	Enables or disables SNMP notifications when fan events occur.
PoE Traps	Enables or disables SNMP notifications when PoE events occur.

Buffered Log, Log File, and Trap Log

This tile includes three tabs:

- To view the Buffered Log information, click the Buffered Log tab.
- To view the Log File information, click the Log File tab.
- To view the Trap Log information, click the Trap Log tab.

Buffered Log Tab

The log messages that the switch generates in response to events, faults, errors, and configuration changes are stored locally on the switch in the RAM (cache). This collection of log files is called the buffered log. When the buffered log file reaches the maximum size, the oldest message is deleted from the RAM when a new message is added. If the system restarts, all messages are cleared. The Log page displays the 1000 most recent system messages, such as configuration failures and user sessions. The newest log entry, by default, is displayed at the top of the list.

Figure 214. Buffered Log Tab

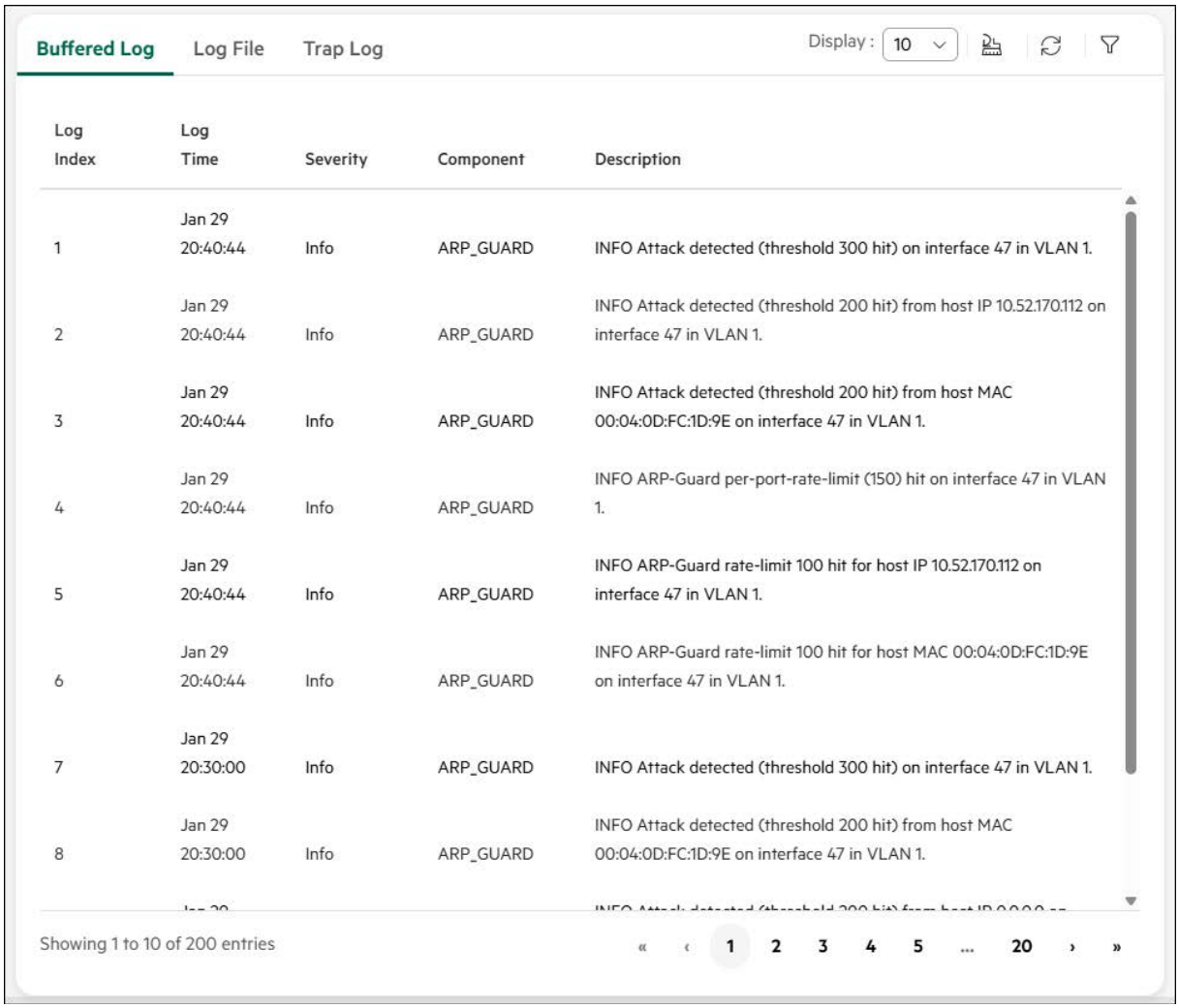


Table 180. Buffered Log Fields

Field	Description
Log Index	The log number.
Log Time	Time at which the log was entered in the table.
Severity	The severity level associated with the log message. The severity can be one of the following: · Debug—The switch is providing debug-level information. · Info—The switch is providing non-critical information. This is the default level. · Notice—The switch is experiencing normal but significant conditions. · Warning—The switch is experiencing conditions that require user attention. · Error—The switch is experiencing non-urgent failures. · Critical—The switch is experiencing primary system failures. · Alert—Action must be taken immediately. · Emergency—The switch is unusable.
Component	The system component that issued the log entry.
Description	A text description of the entry.

Click the column headings to sort the list by the column, in ascending or descending order.

To delete all buffered log messages, click (**Clear All**).

Log File Tab

The system sends logging messages to the local flash (Log file). When using this feature, all events with a severity level of Error and higher are logged to a flash Log file and will be available for viewing even after a system reboot.

When the log file reaches the maximum size, the oldest message is deleted from the flash when a new message is added.

Figure 215. Log File Tab

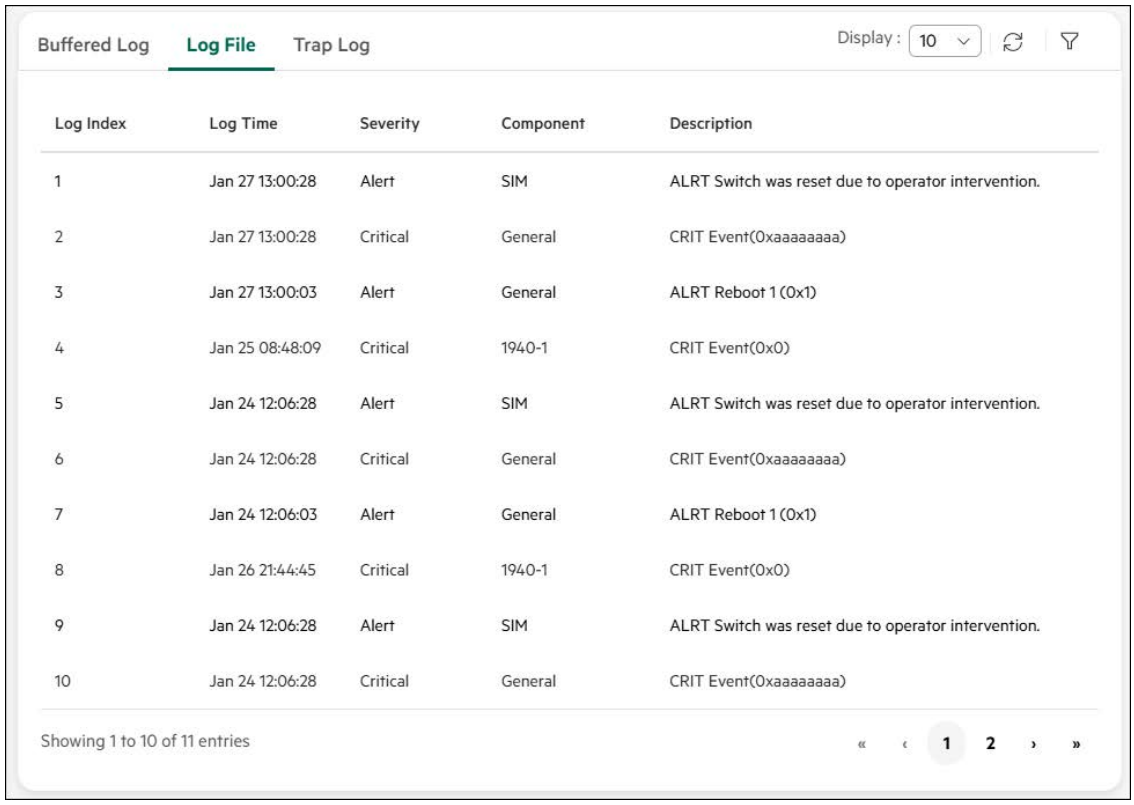


Table 181. Log File Tab Fields

Field	Description
Log Index	The log number.
Log Time	Time at which the log was created.
Severity	The severity level associated with the log message. The severity can be one of the following: · Debug—The switch is providing debug-level information. · Info—The switch is providing non-critical information. This is the default level. · Notice—The switch is experiencing normal but significant conditions. · Warning—The switch is experiencing conditions that require user attention. · Error—The switch is experiencing non-urgent failures. · Critical—The switch is experiencing primary system failures. · Alert—Action must be taken immediately. · Emergency—The switch is unusable.
Component	The system component that issued the log entry.
Description	A text description of the entry.

Trap Log Tab

The Trap Logs tab shows the SNMP traps the switch has generated.

Figure 216. Trap Log Tab

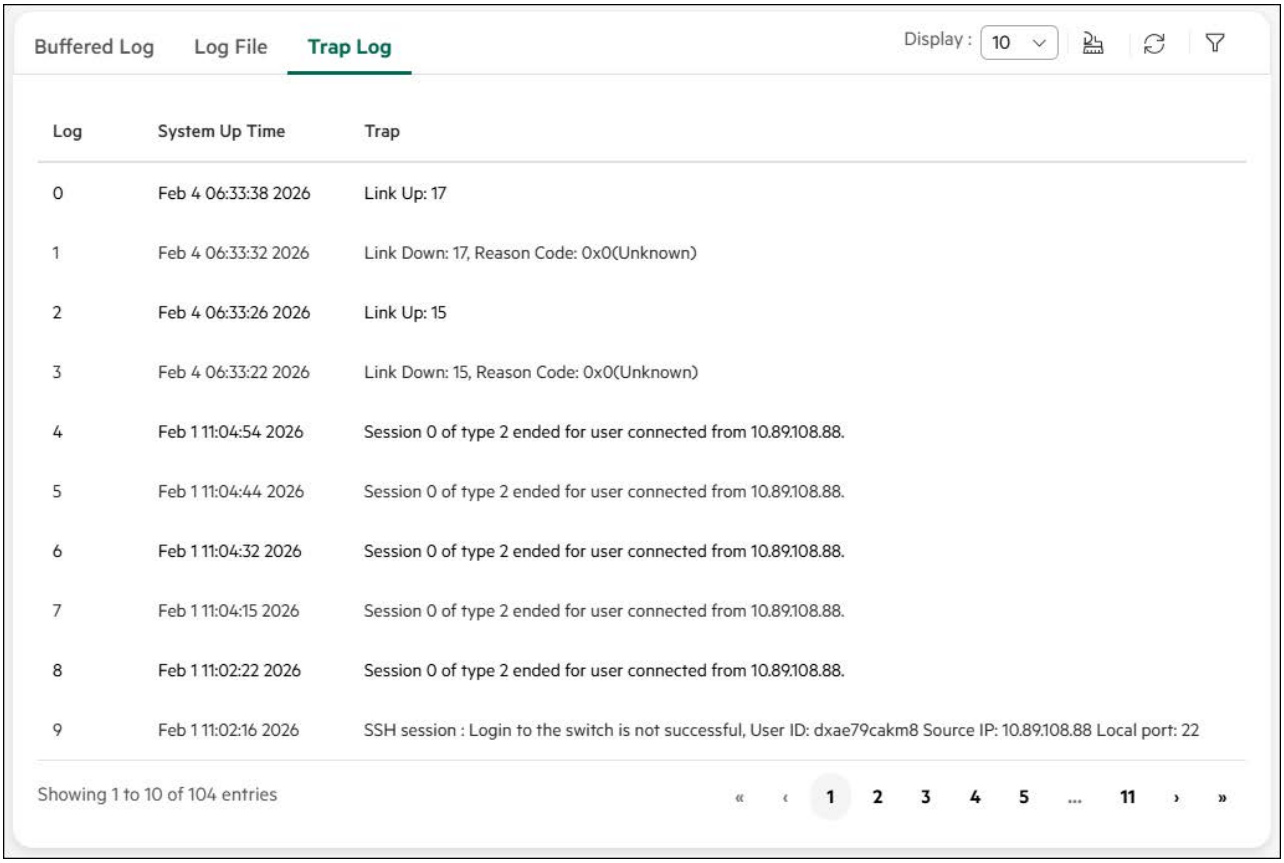


Table 182. Trap Log Fields

Field	Description
Log	The sequence number of this trap.
System Up Time	The time at which this trap occurred, expressed in days, hours, minutes and seconds since the device was last reset.
Trap	Provides information about the trap.

Click the column headings to sort the list by the column, in ascending or descending order.

To delete all trap log messages, click (**Clear All**).

Ping

A ping request is an Internet Control Message Protocol (ICMP) echo request packet. The switch supports both ICMP for sending ping requests to IPv4 addresses and ICMPv6 for sending ping requests to IPv6 addresses.

To display the Ping page, click **Diagnostics** > **Ping** in the navigation pane

IPv4/IPv6

This tile includes two tabs:

- To send a ping request to an IPv4 host, click the IPv4 tab.
- To send a ping request to an IPv6 host, click the IPv6 tab.

IPv4 Tab

Use the IPv4 tab to send one or more ping requests from the switch to a specified IPv4 address. You can use the ping request to check whether the switch can communicate with a particular host on an IP network. The information you enter on this page is not saved as part of the switch configuration.

Figure 217. IPv4 Tab

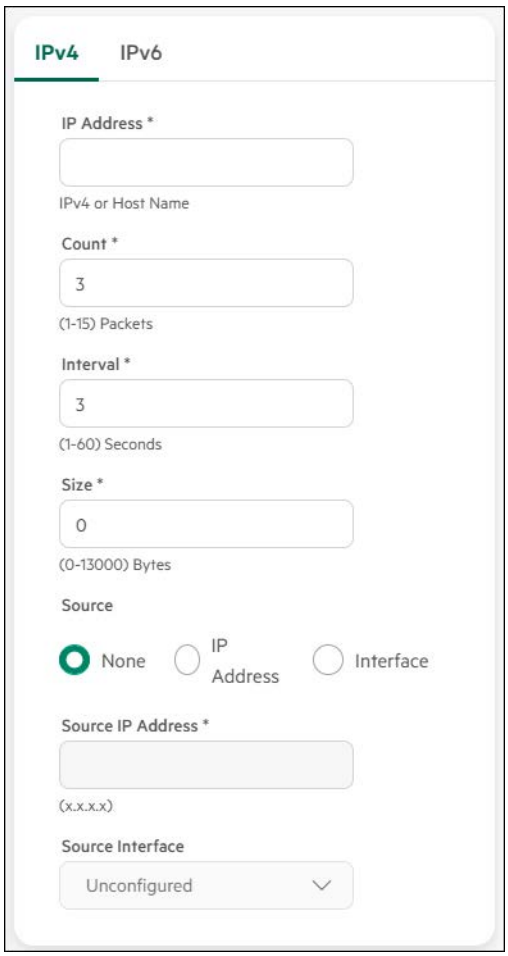


Table 183. IPv4 Fields

Field	Description
IP Address	Specify the IP address you want to reach.
Count	Specify the number of packets to send. The range is 1 to 15 packets and the default is 3 packets.
Interval	Specify the delay between ping packets. The range is from 1 to 60 seconds, and the default is 3 seconds.
Size	Specify the size of the ping packet to be sent. Changing the size allows you to troubleshoot connectivity issues with a variety of packet sizes, such as large or very large packets. The range is from 0 to 13000 bytes, and the default is 0 bytes.
Source	The source IP address or interface to use when sending a ping request. If source is not required, select None as the source option.
Source IP Address	The source IP address to use when sending a ping request. This field is enabled when IP Address is selected as the source option.
Source Interface	The interface to use when sending a ping request. This field is enabled when Interface is selected as the source option. The default interface to use is the network port.

Click **Ping** button to ping the specified host. Click Stop Ping to end a ping in progress. If you do not click Stop Ping, the pings continue until the number of pings specified in the Count field has been reached—even if you navigate away from the Ping page.

The results of the ping operation can be viewed in the Ping Results tile.

IPv6 Tab

Use the IPv6 page to send one or more ping requests from the switch to a specified IPv6 address. You can use the ping request to check whether the switch can communicate with a particular host on an IP network. The information you enter on this page is not saved as part of the device configuration.

Figure 218. IPv6 Tab

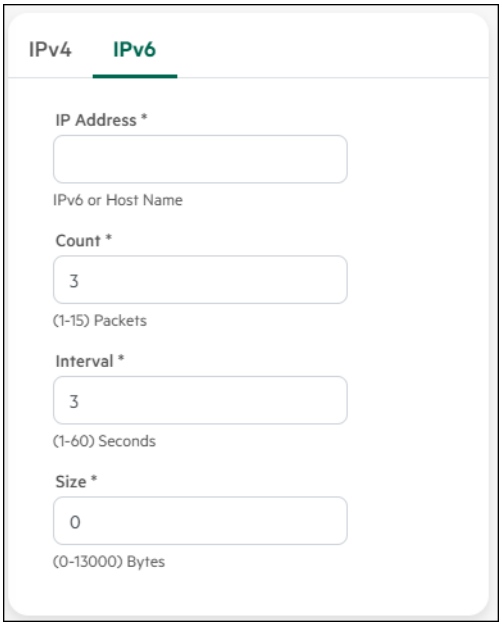


Table 184. IPv6 Fields

Field	Description
IPv6 Address	Enter the global or link-local IPv6 address to ping.
Count	Specify the number of packets to send. The range is 1 to 15 packets and the default is 3 packets.
Interval	Specify the delay between ping packets. The range is from 1 to 60 seconds, and the default is 3 seconds.
Size	Specify the size of the ping packet to be sent. Changing the size allows you to troubleshoot connectivity issues with a variety of packet sizes, such as large or very large packets. The range is from 0 to 13000 bytes, and the default is 0 bytes.

Click **Ping** button to ping the specified host. Click Stop Ping to end a ping in progress. If you do not click Stop Ping, the pings continue until the number of pings specified in the Count field has been reached—even if you navigate away from the Ping page.

The results of the ping operation can be viewed in the Ping Results tile.

Ping Results

The Ping Results tile shows the Ping status and results after you configure the fields in the IPv4 or IPv6 tab and click **Apply**.

Figure 219. Ping Results Tile

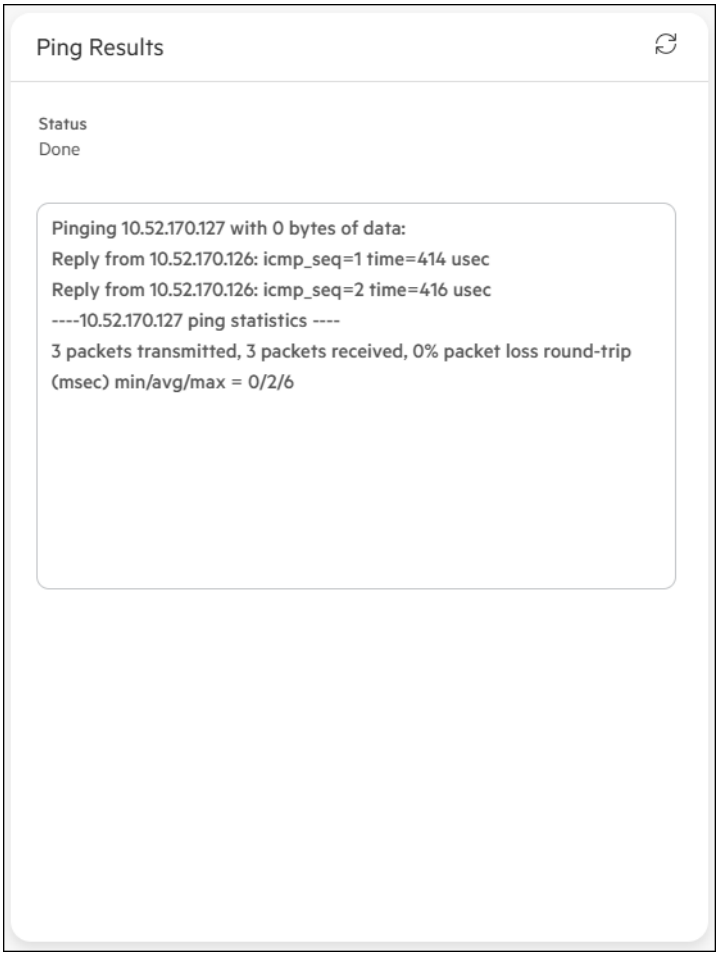


Table 185. Ping Results Fields

Field	Description
Status	The current status of the ping test, which can be one of the following: · Not Started—The ping test has not been initiated since viewing the page. · In Progress—The ping test has been initiated and is running. · Done—The test has completed, and information about the test is displayed in the Results area.
Results	The results of the ping test, which includes the following information: · The IP address of the switch that was pinged. · The Internet Control Message Protocol (ICMP) number of the packet, starting from 1. · The time it took to receive a reply, in microseconds. · The number of ping packets sent and received, the percent of packets that were lost, and the minimum, average, and maximum round-trip time for the responses in milliseconds.

Traceroute

Traceroute is a diagnostic tool that provides information about the route a packet takes from the switch to a specific IPv4 or IPv6 address as well as the amount of time it takes for the packet to reach its destination.

To display the Traceroute IPv4 page, click **Diagnostics** > **Traceroute** in the navigation pane.

IPv4/IPv6

This tile includes two tabs:

- To use traceroute to reach an IPv4 host, click the IPv4 tab.
- To use traceroute to reach an IPv6 host, click the IPv6 tab.

IPv4 Tab

Use this tab to determine the Layer 3 path a packet takes from the switch to a specific IP address. When you initiate the traceroute command by clicking the **Apply** button, the switch sends a series of traceroute probes toward the destination. The results list the IP address of each layer 3 switch a probe passes through until it reaches its destination—or fails to reach its destination and is discarded. The information you enter on this page is not saved as part of the switch configuration.

Figure 220. Traceroute IPv4 Tab

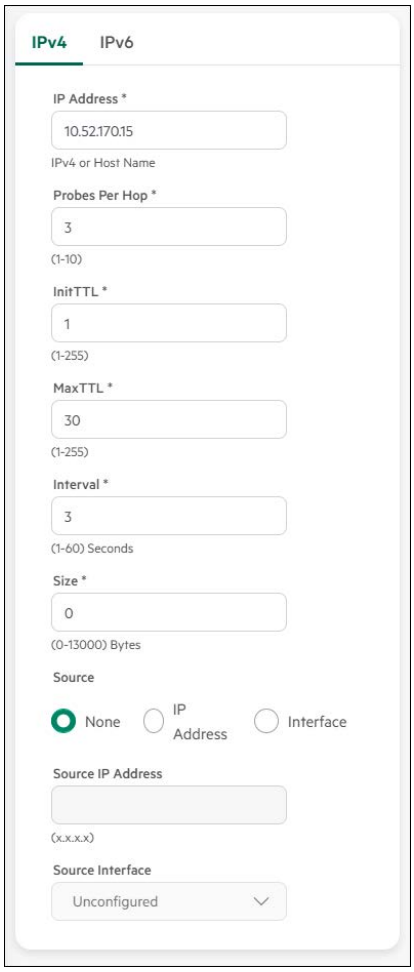


Table 186. Traceroute IPv4 Fields

Field	Description
IP Address	The IP address of the system to attempt to reach.
Probes Per Hop	Traceroute works by sending UDP packets with increasing Time-To-Live (TTL) values. Specify the number of probes sent with each TTL.
Init TTL	The initial Time-To-Live (TTL). This value controls the maximum number of layer 3 hops that the first set of probes may travel.
Max TTL	The maximum Time-To-Live (TTL). The traceroute terminates after sending probes that can be layer 3 forwarded this number of times. If the destination is further away, the traceroute will not reach it.
Interval	The number of Seconds to wait between sending probes.
Size	The size of probe payload in bytes.
Source	The source to use when sending the traceroute, which can be one of the following: · None—No specific source is required. · IP Address—Use the IP address specified in the Source IPv4 Address field as the source. · Interface—Use the specified switch interface as a source.
Source IP Address	The source IPv4 address to use when sending the traceroute. This field is enabled when IP Address is selected as source option.
Source Interface	The source interface to use when sending the traceroute. This field is enabled when Interface is selected as source option.

Click **Apply** to send the traceroute to the specified host. Click **Stop Traceroute** to end a traceroute in progress.

The Trace Operation status and results are displayed in the Traceroute Results pane.

IPv6 Tab

Use this tab to determine the Layer 3 path a packet takes from the switch to a specific IPv6 address. When you initiate the traceroute command by clicking the **Apply** button, the switch sends a series of traceroute probes toward the destination. The results list the IPv6 address of each Layer 3 switch a probe passes through until it reaches its destination—or fails to reach its destination and is discarded. The information you enter on this page is not saved as part of the switch configuration.

Figure 221. Traceroute IPv6 Page

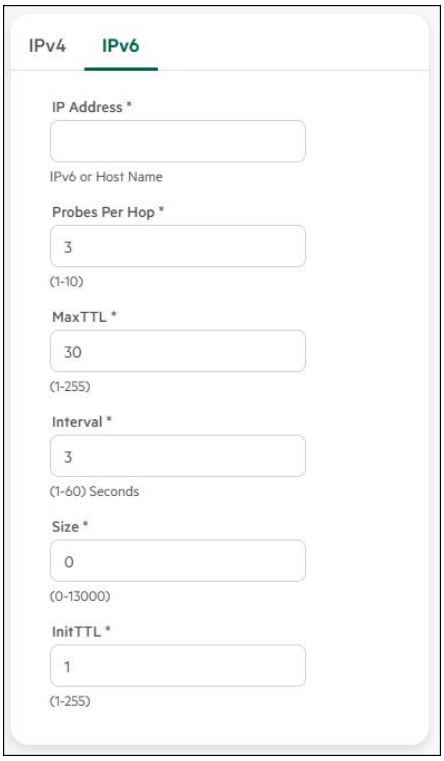


Table 187. Traceroute IPv6 Fields

Field	Description
IPv6 Address	The IPv6 address of the system to attempt to reach.
Probes Per Hop	Traceroute works by sending UDP packets with increasing Time-To-Live (TTL) values. Specify the number of probes sent with each TTL.
Max TTL	The maximum Time-To-Live (TTL). The traceroute terminates after sending probes that can be layer 3 forwarded this number of times. If the destination is further away, the traceroute will not reach it.
Interval	The number of Seconds to wait between sending probes.
Size	The size of probe payload in bytes.
InitTTL	The initial Time-To-Live (TTL). This value controls the maximum number of Layer 3 hops that the first set of probes may travel.

Click **Apply** to send the traceroute to the specified host.

Click **Stop Traceroute** to end a traceroute in progress.

Traceroute Results

The Traceroute Results tile shows the traceroute status and results after you configure the fields in the IPv4 or IPv6 tab and click **Apply**.

Figure 222. Traceroute Results Tile

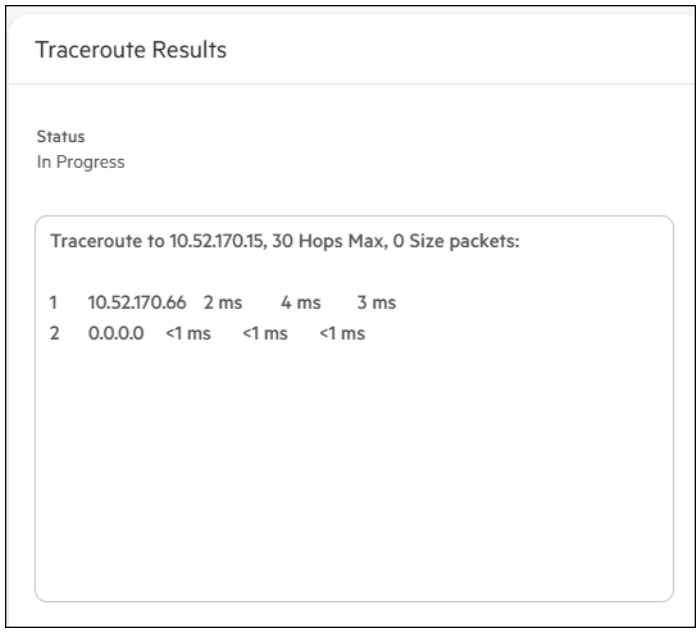


Table 188. Ping Results Fields

Field	Description
Status	The current status of the traceroute test, which can be one of the following: · Not Started—The traceroute test has not been initiated since viewing the page. · In Progress—The traceroute test has been initiated and is running. · Done—The test has completed, and information about the test is displayed in the Results area.
Results	The results of the traceroute are displayed. The output typically displays the following information for each hop: · Hop Number: The sequential order of the router in the path. If a destination is 12 hops away, you will see lines numbered 1 through 12. · IP Address: The specific interface IP of the router that handled your request · Round Trip Time (RTT): Usually displayed three times per hop (in milliseconds, ms). This is the time it takes for a “time exceeded” packet to return from that specific router. Multiple readings help show if there is latency jitter at a specific point.

Support File

Use the support file page to display summary information for the switch on a single page.

CAUTION

Generating the support file may take several minutes. During this time, switch management will not be available.

To display the Support File page, click **Diagnostics** > **Support File** in the navigation pane.

The page shows the following buttons:

- **VIEW SUPPORT INFORMATION—**Click this button to generate the tech support information.

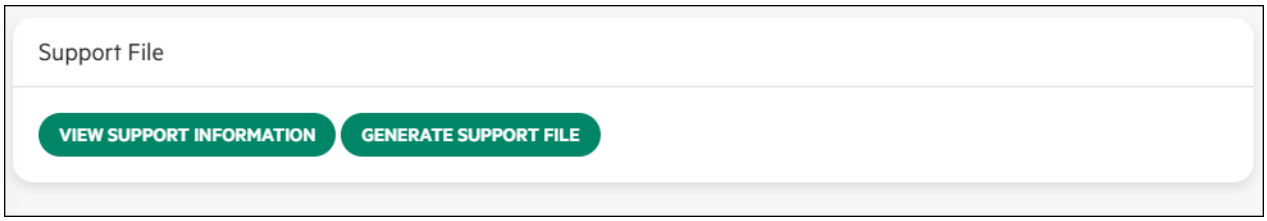
  After clicking this button, the View Support Information dialog box opens and indicates that the tech support generation takes a long time and will be generated in a new window. You might need to grant permission to allow browser pop-ups.

  After you click **Proceed** in the dialog box, a new browser tab or window opens with the support information.
- **GENERATE SUPPORT FILE—**Click this button to generate and download a text-based version of the support file.

  After clicking this button, the Generate and Download Tech Support dialog box opens and indicates that the tech support generation takes a long time and will be downloaded after it is generated

  After you click **Proceed** in the dialog box, the support information is generated and downloaded to the local system. Use any text editor to open and read the support file.

Figure 223. Support File Page



The support file includes the following information:

- System Information—A system description, name, location, and contact information, along with date and time information.
- System Time—Current Time and System Up Time.
- Device Information—Software and OS versions.
- System Resource Usage—CPU and memory usage data.
- Image Status and Image Description—The active and backup image status and versions.
- Buffered Log and Configuration—Messages and logging configuration details.
- Syslog Configuration—Syslog status and remote port and address information.
- Locator LED Configuration—Locator LED status.
- MAC Table—Address forwarding table and summary statistics.
- Time Configuration and Time Zone—NTP client status and time zone configuration.
- Daylight Saving Time—The daylight saving time mode on the system.
- Date Range and Recurring Date—Configuration of the date range or recurring date.
- Network Details—Switch IP and MAC addresses.
- Web Parameters and Management Access—Web session timeout, access port and management VLAN information.
- User Accounts and Passwords—User access, logged-in users, and password manager configuration.

- Port Status and Port Summary Statistics—Port and trunk configuration details, summary, and statistics.
- Port Mirroring Configuration—Enable/disable status, source and destination port configuration.
- Flow Control and Storm Control Configuration—Enable/disable status.
- Spanning Tree Switch Configuration—Global and per-port configuration, status, and statistics.
- Loop Protection Configuration and Status—Per interface configuration and statistics.
- IGMP Snooping—Enable/disable information and statistics.
- SNMP—SNMP v1/v2/v3 information.
- Auto Recovery Components and Configuration—Enable/disable status of auto recovery by supported features and recovery time.
- VLAN Configuration—Configured VLANs, VLAN port membership, and VLAN port configuration.
- Auto Voice VLAN Configuration—Voice VLAN settings.
- Link Aggregation and Statistics—Link Aggregation details and flap count statistics.
- LLDP and LLDP-MED Configuration—Global settings and per-port LLDP configuration and activity.
- DHCP Relay—Configuration and statistics.
- Access Control List—Configuration, summary (global, interface, and VLAN), and statistics.
- CoS—802.1p CoS mapping per interface, DSCP CoS global mapping configuration, CoS trust configuration, CoS interface queue configuration.
- Auto DoS Features—Enable/disable status.
- ICMP Settings—Global ICMP configuration.
- RADIUS—RADIUS authentication and accounting configuration, status, and statistics.
- Port Access Control—Global settings and per-port Authentication control and status.
- Port Security—Global enable/disable status, per-port status, and Static and Dynamic MAC addresses.
- Protected Ports Configuration—Configured groups and protected ports.
- Green Features (EEE) Configuration—Global and per-port enable/disable status and power consumption data.
- PoE Configuration—On switches that support PoE, global and per-port configuration and schedule settings.



Support file information can be saved and downloaded to the management system using the native browser file system.

Cable Test

This feature detects and reports potential cabling issues, such as cable opens or cable shorts, on copper links. This feature also provides the distance to the fault, if it exists, and the total cable length.

Cable length measurement is available when the link is up and the cable status is normal. The length is automatically detected. 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.

NOTE

Only short circuits across wires within a pair are reported. If there is a short circuit across wires not in a pair, it will not be reported.

Figure 224. Cable Test Tile

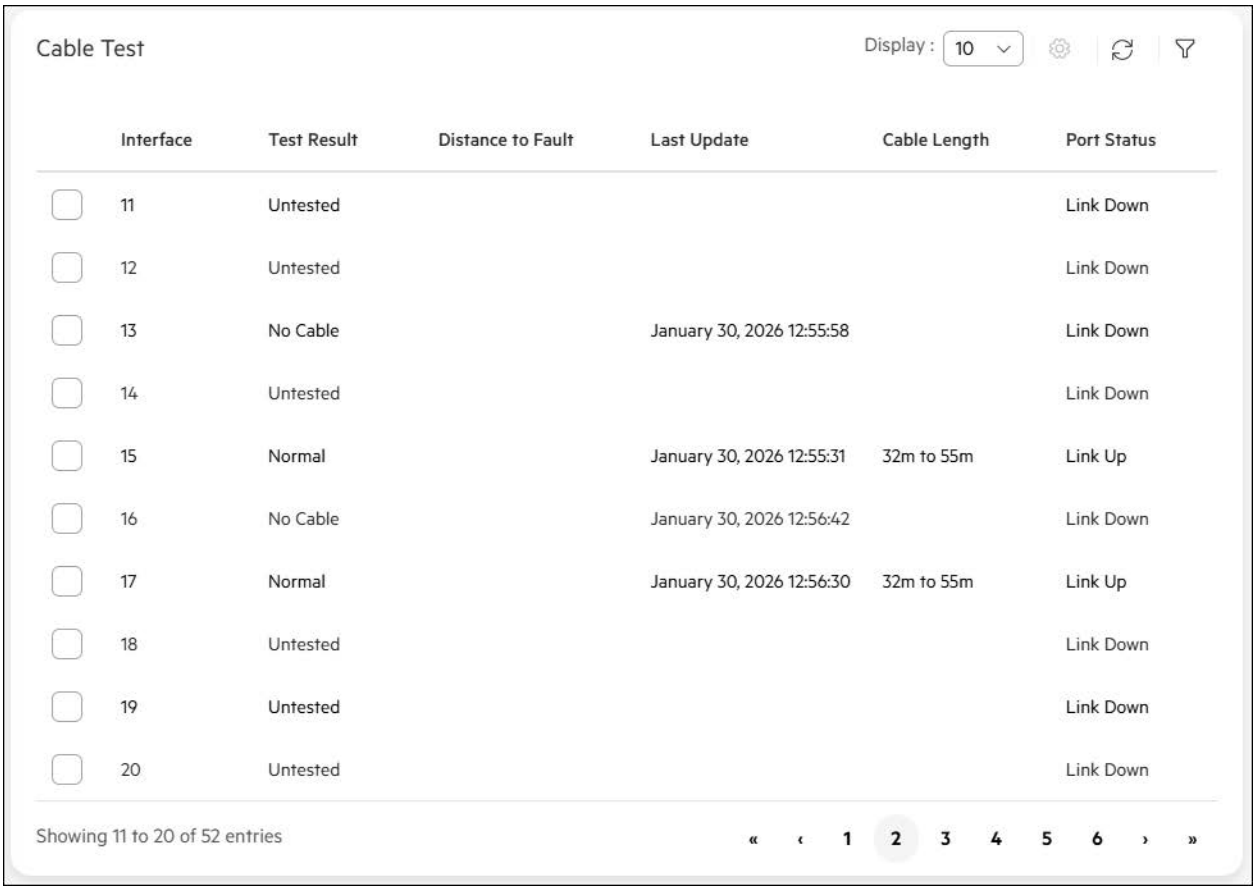


Table 189. Cable Test Fields

Field	Description
Interface	The interface ID.
Test Result	This field appears only after a test was run on the interface. These are the test result options: · Untested—The cable is not tested yet. · Normal—The cable is working correctly. · No Cable—No cable is connected to the interface. · Open—The cable is disconnected, or there is a faulty connector. · Short—There is an electrical short in the cable. · Open and Short—The cable is open and/or shorted. · Crosstalk—Crosstalk is a noise in cable that generally occurs due to a bad cable. · Cable status test failed—The cable status could not be determined. The cable may in fact be working.
Distance to Fault	This field appears only after a test was run on the interface. In the case of a fault, this column shows the distance to the fault.
Last Update	This field appears only after a test was run on the interface. It shows the last time a test was activated on this interface.
Cable Length	The estimated length of the cable in meters. The length is displayed as a range between the shortest estimated length and the longest estimated length. Unknown is displayed if the cable length could not be determined. Note: Cable length info is not available for interfaces with traffic rates below 1 Gbps.
Port Status	Displays the current port status.

To run the cable test on an interface, select the check box associated with the interface and click (**Test**). and then click **Apply**. The Interface Configuration dialog box appears and indicates that ports are briefly shut down. Click **Test** to run the cable test on the selected interface.



Activation of the test will cause link down state for a few milliseconds.

MAC Table

The MAC address table keeps track of the Media Access Control (MAC) addresses associated with each port. This table enables the switch to forward unicast traffic through the appropriate port. The MAC address table is sometimes called the bridge table or the forwarding database. The address table supports up to 16K MAC address entries for all the port devices.

To display the MAC Table page, click **Diagnostics > MAC Table** in the navigation pane.

Global Configuration

Use the Global Configuration tile to view the maximum number of entries the MAC table can maintain and to configure the MAC address aging interval.

Figure 225. MAC Table Global Configuration Tile



Table 190. MAC Table Global Configuration Fields

Field	Description
Maximum Addresses Supported	The maximum number of MAC address entries that can be learned on the switch.
MAC Address Aging Interval	The MAC address table (forwarding database) contains static entries, which never age out, and dynamically-learned entries, which are removed if they are not updated within a given time. Specify the number of seconds a dynamic address should remain in the MAC address table after it has been learned.

MAC Address Table

The MAC Address Table tile displays information about the MAC addresses in the MAC address table, which is also known as the forwarding database (FDB). You can also use this tile to remove MAC addresses that have been learned dynamically.

Figure 226. MAC Address Table Tile

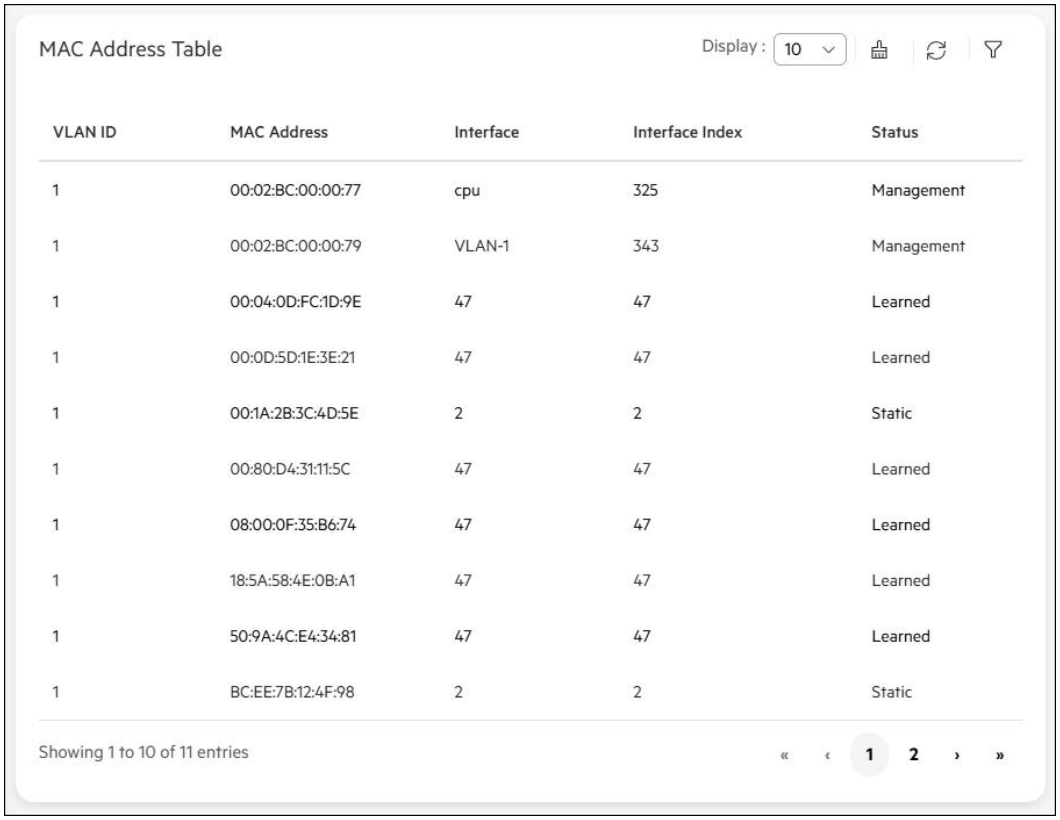


Table 191. MAC Address Table Fields

Field	Description
VLAN ID	The VLAN or VLANs with which the MAC address is associated.
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a six-byte MAC address, with each byte separated by colons.
Interface	The port where this address was learned. The port identified in this field is the port through which the MAC address can be reached. *CPU* is a special source port used for internal management on the switch.
Interface Index	The Interface Index of the MIB interface table entry associated with the source port. This value helps identify an interface when using SNMP to manage the switch.
Status	Provides information about the entry and why it is in the table. These are the possible values: · Learned—The address has been automatically learned by the switch and can age out when it is not in use. Dynamic addresses are learned by examining information in incoming Ethernet frames. · Management—The burned-in MAC address of the switch. · Static—The MAC address was added manually by the system administrator. · Self—The MAC address belongs to one of the device's physical interfaces. · Other—The address was added dynamically through an unidentified protocol or method. · Unknown—The device is unable to determine the status of the entry.

Clear Dynamic FDB Entries

To remove dynamically learned FDB entries, click (**Clear**). The Clear Dynamic FDB Entries dialog box appears.

Figure 227. Clear Dynamic FDB Entries Dialog Box.

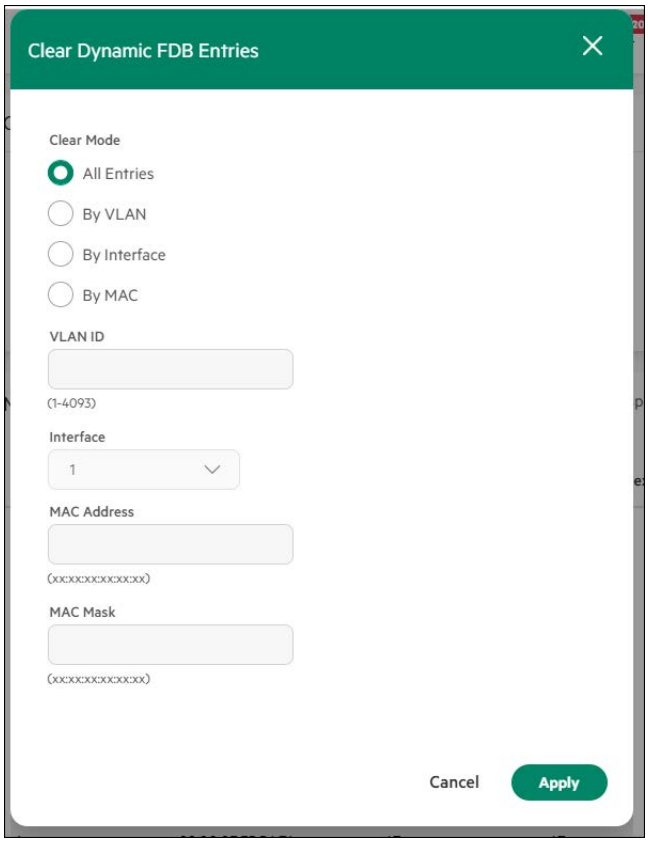


Table 192. Clear Dynamic FDB Entries Fields

Field	Description
Clear Mode	Determines how to specify which learned entries to clear: · All Entries—Select this option to clear all dynamically learned entries. · By VLAN—Select this option to clear all dynamic entries learned on a VLAN. · By Interface—Select this option to clear all dynamic entries learned on an interface. · By MAC—Select this option to clear a range of dynamic entries that match the MAC address and mask combination
VLAN ID	If the clear mode is By VLAN, specify the VLAN associated with the entries to clear.
Interface	If the clear mode is By Interface, select the interface associated with the entries to clear.
MAC Address	If the clear mode is By MAC, specify the MAC address associated with the entries to clear. When clearing a range of MAC addresses, the masked bits can be 0.
MAC Mask	If the clear mode is By MAC, specify the MAC mask, where f means the bit is significant, and 0 means the bit is ignored. For example, to clear all learned addresses for devices from a specific vendor (identified by the first 6 bits in the MAC address), the MAC address and mask fields could be aa:bb:cc:00:00:00 for the address and ff:ff:ff:00:00:00 for the mask.

RMON

Remote Monitoring (RMON) is an extension to the Simple Network Management Protocol (SNMP) that provides comprehensive network monitoring capabilities. In standard SNMP, the switch has to be queried to obtain information. RMON is proactive and can set alarms on a variety of traffic conditions, including specific types of errors. The RMON standard is an SNMP MIB definition described in RFC 1757 for Ethernet.

The following RMON groups are supported:

- RMON Statistics (Group 1)
- History (Group 2)
- Events (Group 9)
- Alarms (Group 3)

RMON Statistics

The RMON Statistics tile displays RMON (Ethernet) statistics, which includes counts of packets, octets (or bytes), broadcasts, multicasts and collisions on the local segment, as well as the number of occurrences of dropped packets by the agent.

Figure 228. RMON Statistics Tile

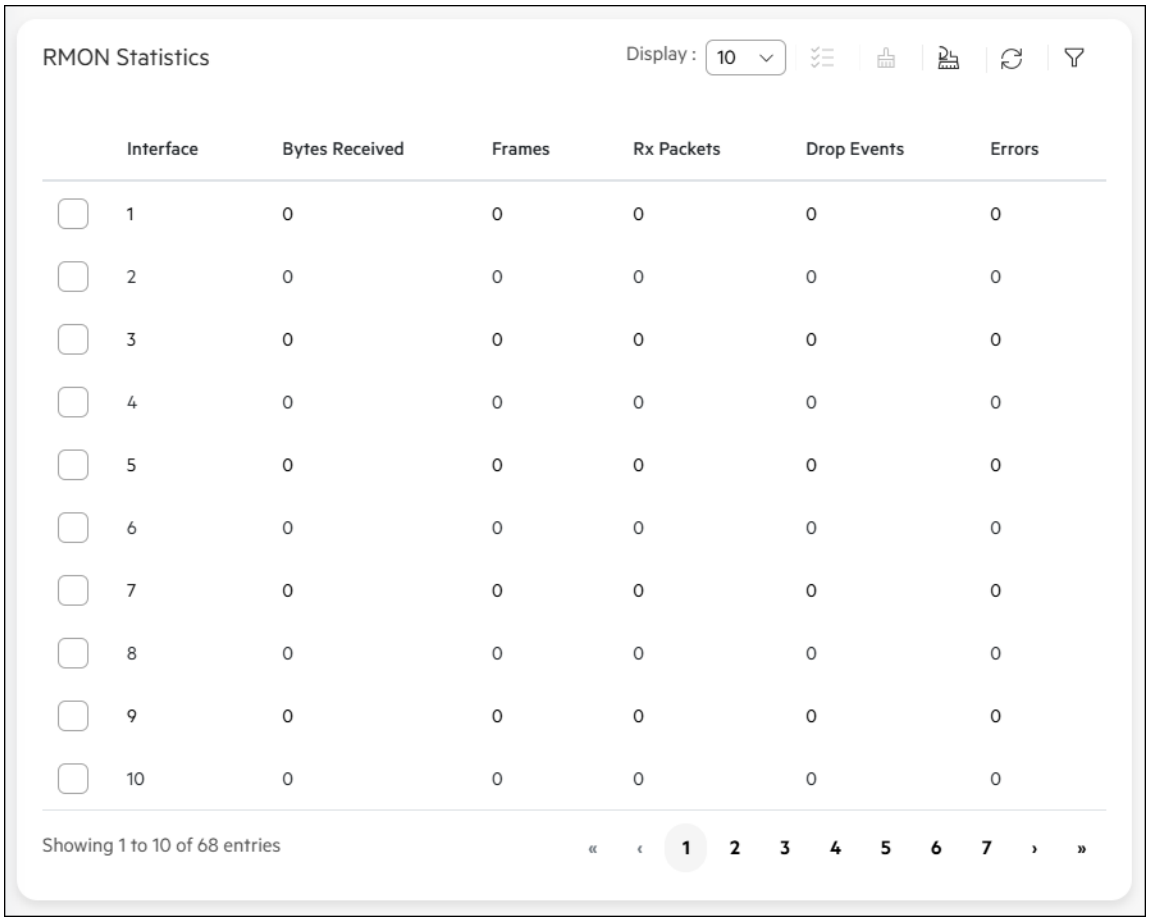


Table 193. RMON Statistics Fields

Field	Description
Interface	The interface identifier.
Bytes Received	Total number of octets of data (including those in bad packets) received on the interface (excluding framing bits but including FCS octets).
Frames	The total number of frames sent and received on the interface. The frame count includes only frames sizes of 64 bytes to max size allowed on interface (2048 bytes).
Packets Received	Total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Drop Events	Total number of events in which packets were dropped by the interface due to lack of resources. Note that this number is not necessarily the number of packets dropped. It is the number of times this condition was detected.
Errors	Total number of packets received on the interface with an Error.

To view additional RMON statistics for an interface, select the interface with the information to view and click (**Details**).

Table 194. RMON Statistics Details Fields

Field	Description
Interface	The interface identifier.
Bytes Received	Total number of octets of data (including those in bad packets) received on the interface (excluding framing bits but including FCS octets).
Drop Events	Total number of events in which packets were dropped by the interface due to lack of resources. Note that this number is not necessarily the number of packets dropped. It is the number of times this condition was detected.
Rx Packets	The number of packets of all types received on the interface during the sample time.
Rx Broadcast Packets	The number of Broadcast packets received on the interface during the sample time.
Rx Multicast Packets	The number of Multicast packets received on the interface during the sample time.
CRC/Align Errors	The number of packets with a CRC Align error received on the interface during the sample time.
Undersize Packets	The number of Undersize packets received on the interface during the sample time.
Oversize Packets	The number of Oversize packets received on the interface during the sample time.
Fragments	The number of fragment type packets received on the interface during the sample time.
Jabbers	The number of Jabber type packets received on the interface during the sample time.
Collisions	The estimated number of collisions which occurred on the interface during the sample time.
64 Byte Frames	Total number of packets (including bad packets) received that are 64 byte frames in length (excluding framing bits but including FCS byte frames).
65 - 127 Byte Frames	Total number of packets (including bad packets) received that are between 65 and 127 byte frames in length inclusive (excluding framing bits but including FCS byte frames).
128 - 255 Byte Frames	Total number of packets (including bad packets) received that are between 128 and 255 byte frames in length inclusive (excluding framing bits but including FCS byte frames).
256 - 511 Byte Frames	Total number of packets (including bad packets) received that are between 256 and 511 byte frames in length inclusive (excluding framing bits but including FCS byte frames).

Field	Description
512 - 1023 Byte Frames	Total number of packets (including bad packets) received that were between 512 and 1023 byte frames in length inclusive (excluding framing bits but including FCS byte frames).
1024 Byte or Larger Frames	Total number of packets (including bad packets) received that were between 1024 byte frames and the maximum frame size in length inclusive (excluding framing bits but including FCS byte frames).

To reset RMON and interface statistics counters to 0 for one or more interfaces, select each interface with the statistics to reset and click (**Clear**).

To reset RMON and interface statics for all interfaces, click (**Clear All**).

History Collectors/Log

The History group provides historical views of the statistics provided in the Statistics group, with the exception of frame size counters which are provided only on a real-time basis. Up to 300 entries can be displayed.

To view the History Collector information, click the **History Collectors** tab.

To view the History Log information, click the **History Log** tab.

History Collectors

Use the History Collectors tab to define the ID and parameters of the History info to view. Only Collector IDs that were defined in the History Collector tab are available.

Figure 229. History Collectors Tab

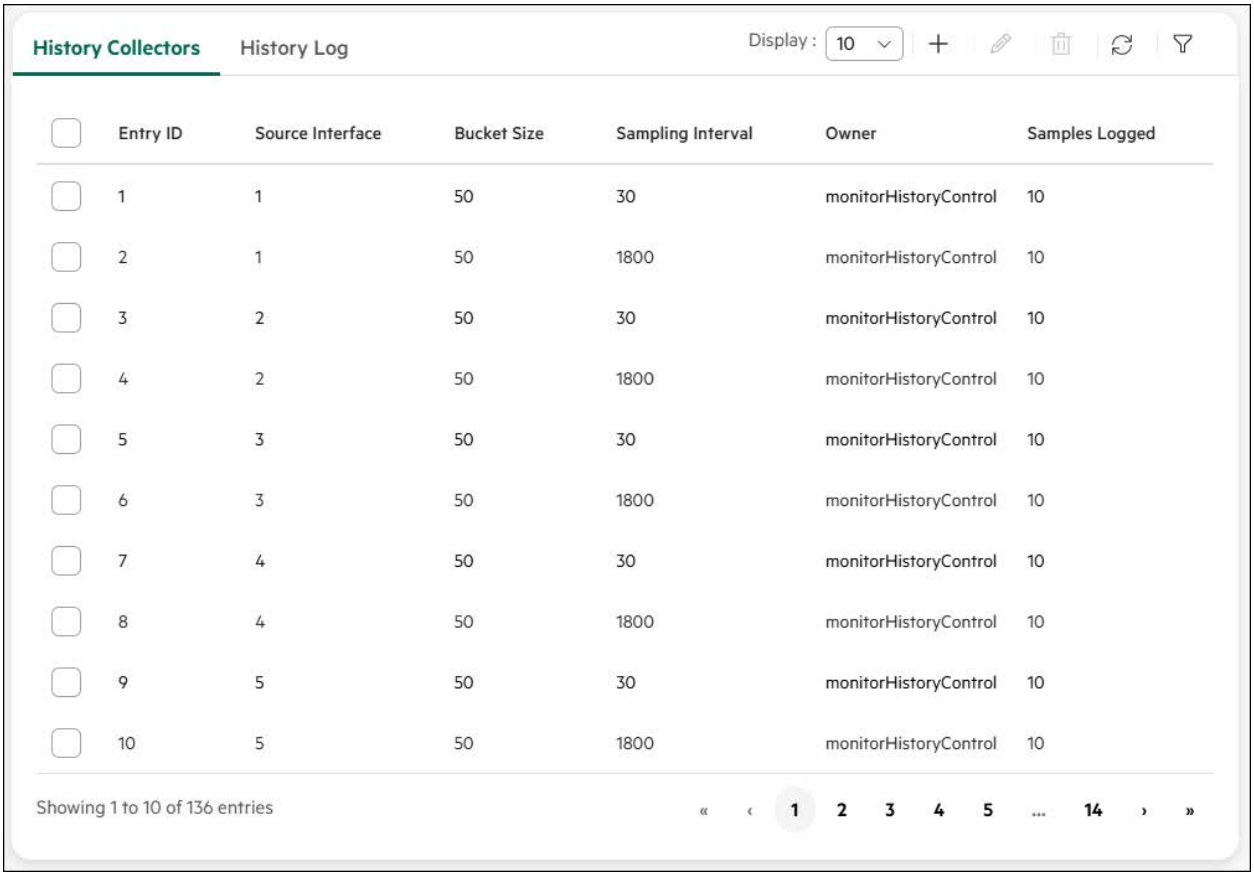
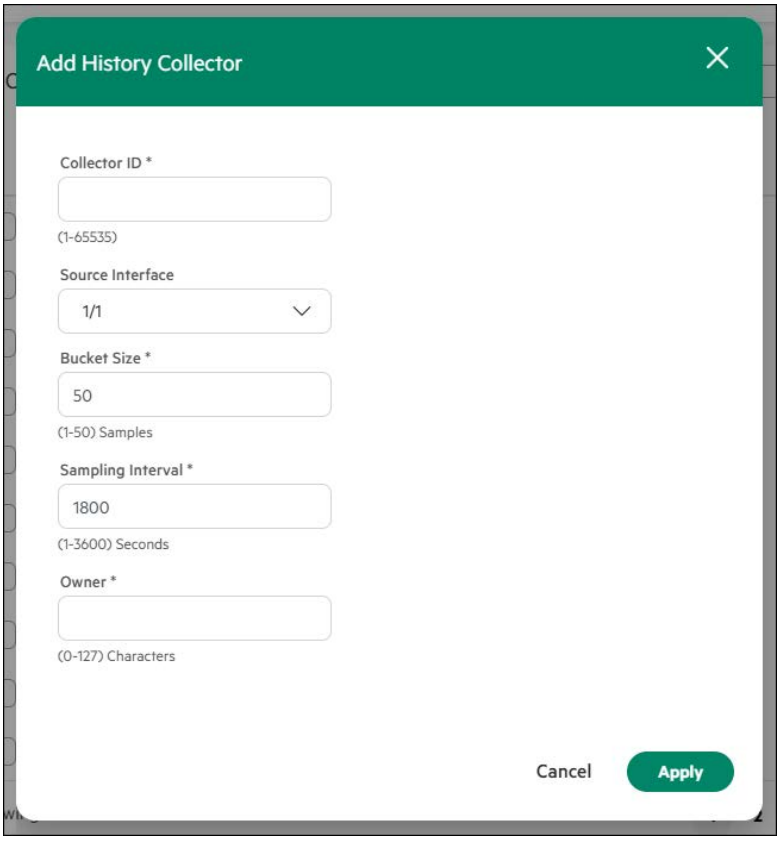


Table 195. History Collectors Fields

Field	Description
Entry ID	The entry identifier.
Source Interface	The source interface (port or LAG) to sample in this entry.
Bucket Size	The number of samples to store. Range: 1 - 50, default: 50
Sampling Interval	The number of seconds in each polling cycle. Range: 1-3600, default: 1800
Owner	The name of the owner of the RMON group of statistics. This parameter is optional and can be left empty.
Samples Logged	The granted number of samples to be saved. this field is updated by system and cannot be configured by the user.

To add a collector to the switch configuration, click + (**Add**). The Add History Collector dialog box appears. Configure the settings described in the previous table.

Figure 230. Add History Collector Dialog Box



To edit an existing collector, select the check box to the left of the collector entry and click (**Edit**). Update the fields in the Edit History Collector dialog box as needed. Only non-default History Collector entries can be modified.

To remove an existing collector, select the check box to the left of the collector entry and click (**Remove**).

History Log

The History Log tab displays the information itself (based on the definition in the History Collector tab).

Figure 231. History Log Tab



Table 196. History Log Fields

Field	Description
History Collector ID	The ID of the history collector. Click the drop-down to select the collector to view.
Sample Number	The ID of the sample related to info in this row.
Drops	The number of drop events which occurred on the interface during the sample time.
Rx Bytes	The number of bytes received on the interface during the sample time.
Rx Packets	The number of packets of all types received on the interface during the sample time.
Broadcast Packets	The number of broadcast packets received on the interface during the sample time.
Multicast Packets	The number of Multicast packets received on the interface during the sample time
CRC Align Errors	The number of packets with a CRC Align error received on the interface during the sample time.
Undersize Packets	The number of Undersize packets received on the interface during the sample time.
Oversize Packets	The number of Oversize packets received on the interface during the sample time.
Fragments	The number of fragment type packets received on the interface during the sample time.
Jabbers	The number of Jabber type packets received on the interface during the sample time.
Collisions	The estimated number of collisions which occurred on the interface during the sample time.
Utilization	Average port utilization during the sample time.

For more information on the log types, see Table 194, RMON Statistics Details Fields.

RMON Events/Event Log

The Events group provides the capability for users to generate events entries as logs, SNMP traps or both to the management station. Events can originate from a crossed threshold on any counter or administrative events from the agent, such as a power failure or reset. The trigger for each event is defined in the Alarm group (see RMON Alarms). The log includes the time of day for each event and a description of the event.

To view the RMON Events information, click the **RMON Events** tab.

To view the Events Log information, click the **Event Log** tab.

RMON Events Tab

Use the RMON Events tab to configure ID and settings of events (RMON Events).

Figure 232. RMON Events Tab

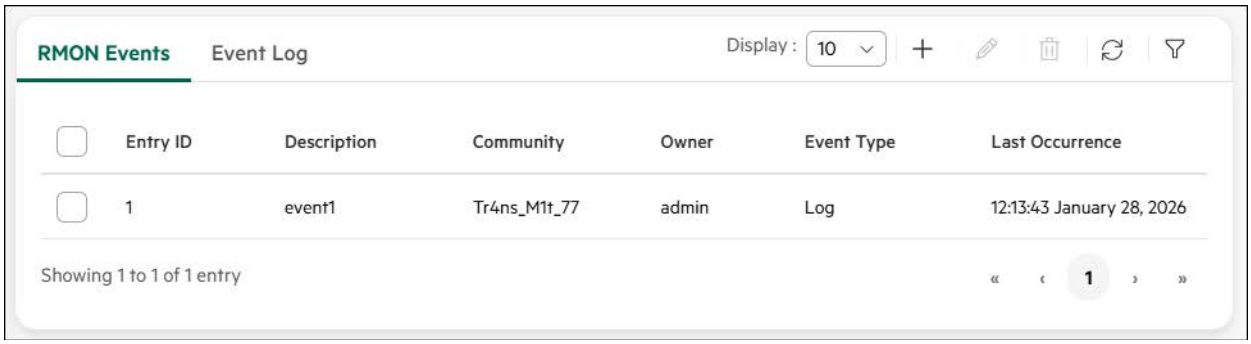


Table 197. RMON Events Fields

Field	Description
Entry ID	The entry identifier. Range is 1-65535
Description	A description of this event.
Community	The SNMP community string to be included when traps are sent to SNMP Manager.
Owner	The name of the owner of the RMON group of statistics. This parameter is optional and can be left empty.
Event Type	Identifies the type of RMON event: · None · Log · Trap · Trap Log
Last Occurrence	The last time an event defined by this entry occurred.

To add an event, click + (**Add**). The Add RMON Event dialog box appears. Configure the settings described in the previous table.

To edit an existing event, select the check box to the left of the event entry and click (**Edit**). Update the fields in the Edit RMON Event dialog box as needed.

To remove an event, select the check box to the left of the collector entry and click (**Remove**).

Event Log Tab

The Events group provides the capability for users to generate events entries as logs, SNMP traps or both to the management station. Events can originate from a crossed threshold on any counter or administrative events from the agent, such as a power failure or reset. The trigger for each event is defined in the Alarm group (see RMON Alarms). The log includes the time of day for each event and a description of the event.

The Event Log tab displays the log of RMON events (actions) that were triggered (occurred).

Figure 233. Event Log Tab



Table 198. Event Log Fields

Field	Description
Event ID	The ID of the event which is configured for the triggered alarm.
Log ID	The Log ID within the specific event.
Log Time	Time that the log entry occurred.
Description	Description of the alarm that triggered the event.

RMON Alarms

Use the RMON Alarms tile to configure and view RMON alarms on the system. The RMON Alarms provide a mechanism for setting thresholds and sampling intervals to generate events on any RMON counters or any other SNMP object counter maintained by the agent. Both the rising and falling thresholds must be configured. After a rising threshold is crossed, another rising event is not generated until the matching falling threshold is crossed. The alarm also indicates the action to be taken if the threshold is crossed.

Figure 234. RMON Alarms Tile

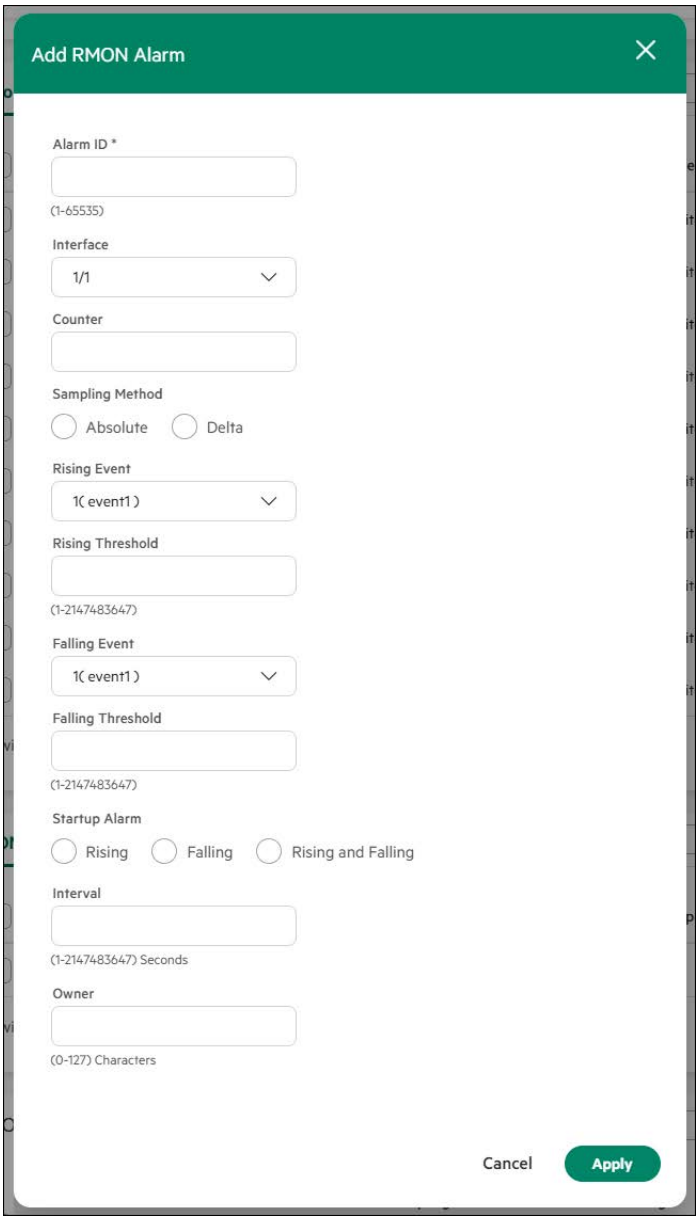


Table 199. RMON Alarms Fields

Field	Description
Alarm ID	The alarm identifier.
Interface	The switch interface on which the Alarm is applied.
Counter	Counter type (from list) to sample.
Sampling Method	The sampling method: · Absolute—Specifies that the selected variable value is compared directly with the threshold at the end of the sampling interval. · Delta—Specifies that the selected variable value of the previous sample is subtracted from the current value, and the difference is compared with the threshold.
Current Value	The current value of the counter.
Rising Threshold	Specifies the value which triggers the rising event Range: 1-2147483647
Rising Event	Specifies the ID of the event triggered when a rising threshold is crossed. The ID is displayed with the description configured for this event. Created events are available for selection or None.
Falling Threshold	Specifies the value which triggers the falling event. Range: 1-2147483647
Falling Event	Specifies the index of the event triggered when a rising threshold is crossed. The ID is displayed with the description configured for this event. Created events are available for selection or None.
Startup Alarm	Defines the type of event that will first trigger this alarm: · Rising and Falling (the default)—Either rising or falling event can first trigger this alarm · Rising—This event can be first triggered by the defined rising event · Falling—This event can be first triggered by the defined falling event
Interval	The interval in seconds during which the data is sampled and compared with rising and falling thresholds. Range: 1-2147483647 seconds.
Owner	The name of the owner of the RMON alarm. This parameter is optional and can be left empty.

To add an alarm, click + (**Add**). The Add RMON Alarm dialog box appears (see Figure 235). Configure the settings described in the previous table.

Figure 235. Add RMON Alarm Dialog Box



To edit an existing alarm, select the check box to the left of the alarm entry and click (**Edit**). Update the fields in the Edit RMON Alarm dialog box as needed.

To remove an alarm, select the check box to the left of the entry and click (**Remove**).

IP Address Conflict

Use IP Address Conflict page to determine whether an IP address configured on the device is the same as the IP address of another device on the same LAN (or on the Internet, for a routable IP address) and to help you resolve any existing conflicts.

An IP address conflict can make both this system and the system with the same IP address unusable for network operation.

Status

The Status tile shows whether an IP Address conflict has been detected since this status was last reset. These are the possible options:

- False—No conflict detected (the subsequent fields on this page display as N/A).
- True—Conflict was detected (the subsequent fields on this page show the relevant information).

Figure 236. Status Tile



To launch the IP address conflict feature, click the **Run Detection** button at the bottom of the screen.

History

The History tile displays the information corresponding to the last detected address conflict. If no conflict has been detected, the fields in this tile do not display any information.

Figure 237. History Tile

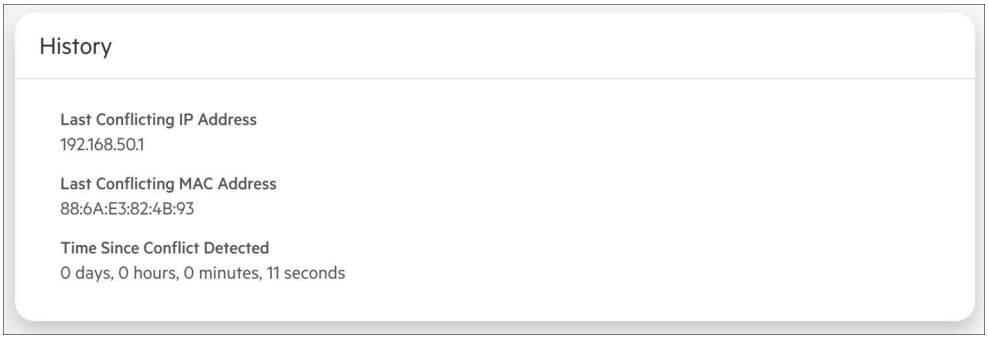


Table 200. IP Address Conflict History Fields

Field	Description
Last Conflicting IP Address	The device interface IP address that is in conflict. If multiple conflicts were detected, only the most recent occurrence is displayed.
Last Conflicting MAC Address	The MAC address of the remote host associated with the IP address that is in conflict. If multiple conflicts are detected, only the most recent occurrence is displayed.

Field	Description
Time Since Conflict Detected	The elapsed time (displayed in days, hours, minutes, and seconds) since the last address conflict was detected, provided the Clear History button has not yet been pressed.

To reset the IP address conflict detection status information, click the **Clear History** button at the bottom of the screen.

Email Alerts

Email Alerting allows the user to configure a set of destinations for log messages. This feature adds the email configuration, through which the log messages are sent to a configured SMTP server such that the administrators may receive the log in an e-mail account of their choice.

Click on Email Alert Test button which will open a modal page to verify that the email alert settings are configured properly. After you specify the settings on this page and click Apply, the device will use the configured SMTP server to send an email to the configured email addresses.

- Test Message Type—Specifies the type of message, which can be urgent, non urgent, or both, to test for email alert functionality.
- Test Message Body—Specifies the text contained in the body of the email alert test message.

To access the Email Alerts page, click **Diagnostics > Email Alerts** in the navigation pane.

Email Alert Global Configuration

Use the Email Alert Global Configuration tile to configure system-wide settings for the Email Alert feature, which allows the device to send log messages to one or more email addresses. You must configure information about the network Simple Mail Transport Protocol (SMTP) server for email to be successfully sent from the device.

Figure 238. Email Alert Global Configuration Tile

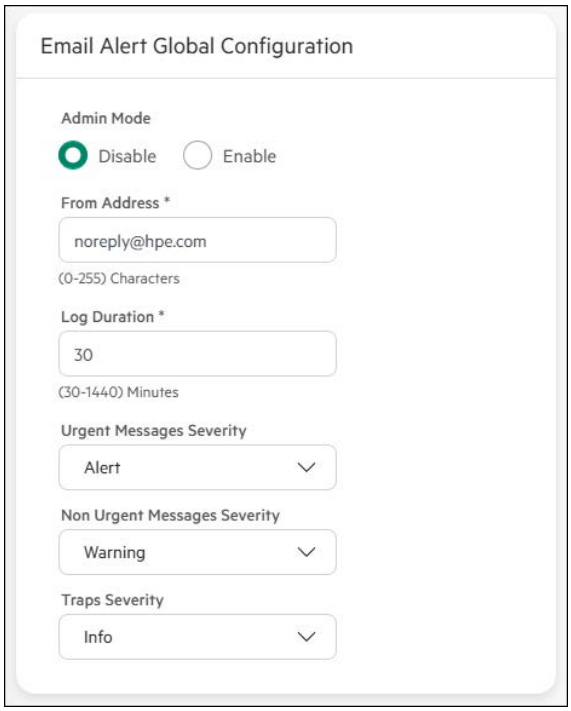


Table 201. Email Alert Global Configuration Fields

Field	Description
Admin Mode	Sets the administrative mode of the feature. · Enable—The device can send email alerts to the configured SMTP server. · Disable—The device will not send email alerts.
From Address	Specifies the email address of the sender (the device).
Log Duration	Determines how frequently the non critical messages are sent to the SMTP server.
Urgent Messages Severity	Configures the severity level for log messages that are considered to be urgent. Messages in this category are sent immediately. The severity level you select and all higher levels are considered to be urgent.
Non Urgent Messages Severity	Configures the severity level for log messages that are considered to be nonurgent. Messages in this category are collected and sent in a digest form at the time interval specified by the Log Duration field. The severity level you select and all levels up to, but not including the lowest Urgent Messages Severity level are considered nonurgent. Messages below the severity level you specify are not sent via email
Traps Severity	The severity level for trap log messages.

Email Alert Statistics

Use the Email Alert Statistics tile to view information about the email alerts the device has sent or attempted to send. The statistics are cleared when the system is reset.

Figure 239. Email Alert Statistics Tile

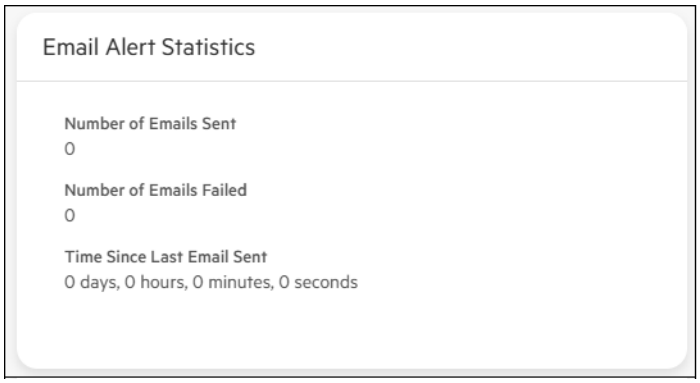


Table 202. Email Alert Statistics Fields

Field	Description
Number of Emails Sent	The number of email alerts that were successfully sent since the counters were cleared or the system was reset.
Number of Emails Failed	The number of email alerts that failed to be sent since the counters were cleared or system was reset.
Time Since Last Email Sent	The amount of time in days, hours, minutes, and seconds that has passed since the last email alert was successfully sent.

To reset all email alert statistics counters to zero, click the Clear Counters button at the bottom of the page.

Email Alert Server Configuration

Use the Email Alert Server Configuration tile to view information about the email alerts the device has sent or attempted to send. The statistics are cleared when the system is reset.

Figure 240. Email Alert Server Configuration Tile



Table 203. Email Alert Server Configuration Fields

Field	Description
Address	The IPv4/IPv6 address or host name of the SMTP server that handles email alerts that the device sends.
Port	The TCP port that email alerts are sent to on the SMTP server. The standard port number for TLSv1 Mail Server Security is 465. The standard port number for a mail server with no security is 25.
Security	The type of authentication to use with the mail server, which can be TLSv1 (SMTP over SSL) or None (no authentication is required).
User Name	If the Security is TLSv1, this field specifies the user name required to access the mail server. If the security is none, the user name is admin.
Password	This field is available in the Add/Edit Email Alert Server Configuration dialog box if the security is TLSv1. The password associated with the configured user name for mail server access. When adding or editing the server, you must retype the password to confirm that it is entered correctly.

To add an SMTP server, click + (**Add**). The Email Alert Server Configuration dialog box appears. Configure the settings described in the previous table.

To edit an existing SMTP server, select the check box to the left of the event entry and click (**Edit**). Update the fields in the Email Alert Server Configuration dialog box as needed.

To remove an SMTP server, select the check box to the left of the entry and click (**Remove**).

To send an email to the SMTP server to test the email alerting function, click the **Email Alert Test** button at the bottom of the page.

Email Alert Subject Configuration

Use the Email Alert Subject Configuration tile to view and edit the subject line of the urgent and non-urgent email alert messages sent from the device.

Figure 241. Email Alert Subject Configuration Tile

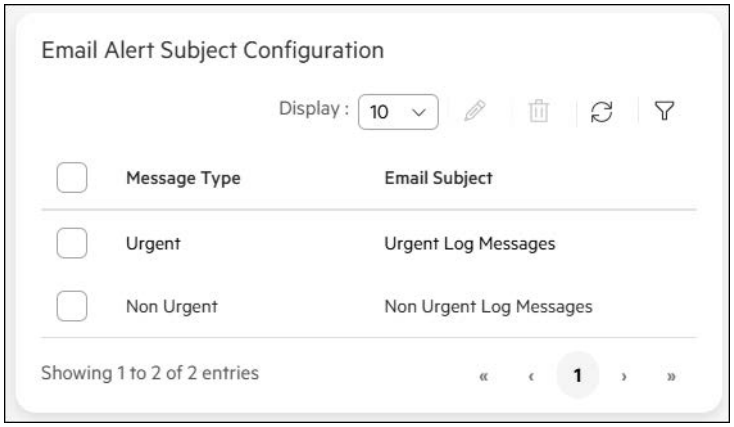


Table 204. Email Alert Subject Configuration Fields

Field	Description
Message Type	The message type, which is Urgent or Non Urgent. The log message severity levels classified as urgent and non-urgent are configured in the Email Alert Global Configuration tile.
Email Subject	The text displayed in the subject line of the email alert message for the message type. Some special characters are not allowed in the subject.

To edit the subject of the urgent or non-urgent message, select the check box to the left of the entry and click (**Edit**). Update the fields in the Email Alert Subject Configuration dialog box as needed.

To reset the subject line of a message type to the default value, select the check box associated with the entry and click (**Remove**).

Email Alert To Address Configuration

Use the Email Alert To Address Configuration tile to configure the email addresses to which email alert messages are sent. A maximum of 5 addresses can be added for each message type.

Figure 242. Email Alert To Address Configuration Tile

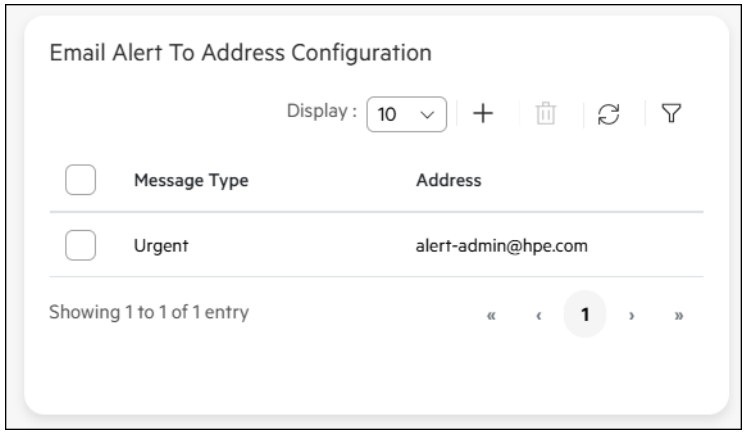


Table 205. Email Alert To Address Configuration Fields

Field	Description
Email Subject	The valid email address of an email alert recipient.
Message Type	The message type to send to the associated address. These are the options: · Urgent · Non Urgent · Both

To add an email address, click + (**Add**) and configure the fields in the dialog box.

To remove an email address, select the check box associated with the entry and click (**Remove**).

Use the maintenance pages to perform various switch maintenance tasks, including upgrading the software, managing system files, rebooting the switch, and resetting the switch configuration.

Dual Image Configuration

The switch can store up to two software images. One image is the active image and the other is the backup image (not actively running on the switch). You can select which image to load during the next boot cycle and add a description for each image on the switch.

To display the Dual Image Configuration page, click **Maintenance** > **Dual Image Configuration**.

Figure 243. Dual Image Configuration Page



Table 206. Dual Image Configuration Fields

Field	Description
Active Image Version	The version ID of the Active image
Active Image Description	Description of the Active image.
Backup Image Version	The version ID of the Backup image.
Backup Image Description	Description of the Backup image
Next Active Image	The firmware image that will become active the next time the switch is rebooted. To make the current backup image the active image, select Backup, then reboot the switch. When a new image is loaded to the Backup Image, the Backup Image automatically becomes the next active image.

Click **Apply** to save your changes to the switch.

Backup and Update Files

The Backup and Update page enables you to upload files from the device to a remote system and to download files from a remote system to the device.

Files can be backed up and updated using HTTP/S, TFTP, FTP, SCP or SFTP protocols.

Secure Copy Protocol (SCP) allows secure file transfer between hosts on the network. SCP runs over TCP port 22, and uses SSH for data transfer and authentication thereby ensuring confidentiality of transferred data.

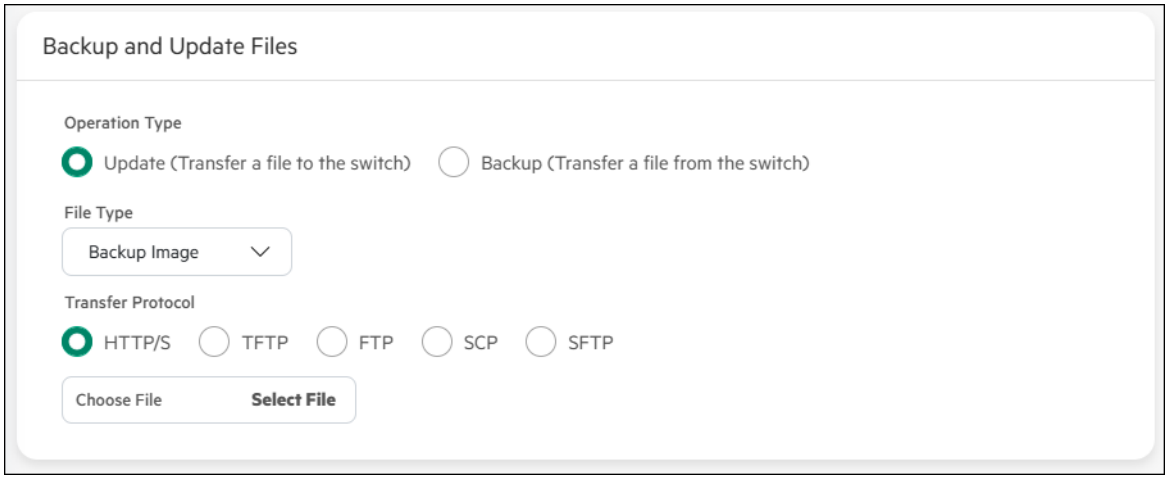
The switch acts as an SCP client and it can send or receive files to/from an SCP server. The switch uses username and password credentials to authenticate to the SCP server.

To display this page, click **Maintenance** > **Backup and Update Files** in the navigation pane.

NOTE

The fields available on the page depend on which options are selected.

Figure 244. Backup and Update Files Page



Backing Up and Updating Files

These are the steps for filling in the backup or update operation:

1. Select the Operation Type
   - Select Update to update the switch firmware or configuration files (transfer a file to the switch).
     NOTE: Firmware upgrades can only be performed on the backup image.
   - Select Backup to save a backup of the current image, configuration file or error log (transfer a file from the switch).
2. Select the file type from the drop-down menu.
   These are the available file types for Backup operation:

Field	Description
Active Image	Select this option to transfer an active image.
Backup Image	Select this option to transfer a backup image.
Running Configuration	Select this option to back up the running configuration file.
Startup Configuration	Select this option to transfer a copy of the stored startup configuration from the device to a remote system.

Field	Description
Backup Configuration	Select this option to transfer a copy of the stored backup configuration from the device to a remote system.
Script File	Select this option to transfer a custom text configuration script from the device to a remote system.
CLI Banner	Select this option to transfer the file containing the text to be displayed on the CLI before the login prompt to a remote system.
Crash Log	Select this option to transfer the system crash log to a remote system.
Local MacAuth DB	Select this option to transfer a local macAuth database file from the device to the remote system.
Operational Log	Select this option to transfer the system operational log to a remote system.
Startup Log	Select this option to transfer the system startup log to a remote system.
Trap Log	Select this option to transfer the system trap records to a remote system.
Factory Defaults	Select this option to transfer the factory default configuration file to a remote system.
Error Log	Select this option to transfer the system error (persistent) log, which is also known as the event log, to a remote system.
Buffered Log	Select this option to transfer the system buffered (in-memory) log to a remote system.
Technical Support Log	Select this option to transfer the technical support log to a remote system.

These are the available file types for Update operation:

Field	Description
Backup Image	Select this option to transfer a new image to the device. The image file is stored as the backup image. The Backup Image will be automatically activated once the update is successful.
Startup Configuration	Select this option to update the stored startup configuration file (startup-config). If the file has errors, the update will be stopped. Please be sure the configuration file matches the current switch model. Configuration files from dissimilar switches are incompatible and will result in a file transfer failure.
Backup Configuration	Select this option to update the stored backup configuration file (backup-config). If the file has errors, the update will be stopped. To apply backup-config as startup-config, first back up the stored file from the switch, to a server by selecting the file type as Backup Configuration and then update the startup-config by downloading file from the server to the switch by selecting file type as Startup Configuration.
Script File	Select this option to transfer a text-based configuration script to the device. You must use the command-line interface (CLI) to validate and activate the script.
CLI Banner	Select this option to transfer the CLI banner file to the device. This file contains the text to be displayed on the CLI before the login prompt.
Local MacAuth DB	Select this option to transfer a local macAuth database file to the device. The local macAuth database stores a list of MAC addresses for local port-based user authentication.
Factory Defaults	Select this option to transfer the factory default configuration file to the device. This file contains baseline configuration that the device uses when it is first powered on or reset to its original state.
SSH-1 RSA Key File	Select this option to transfer an SSH-1 Rivest-Shamir-Adleman (RSA) key file to the device. SSH key files contain information to authenticate SSH sessions for remote CLI-based access to the device.
SSH-2 RSA Key PEM File	Select this option to transfer an SSH-2 Rivest-Shamir-Adleman (RSA) key file (PEM Encoded) to the device.
SSH-2 DSA Key PEM File	Select this option to transfer an SSH-2 Digital Signature Algorithm (DSA) key file (PEM Encoded) to the device.

Field	Description
SSH-2 ECDSA Key PEM File	Select this option to transfer an SSH-2 Elliptic Curve Digital Signature Algorithm (ECDSA) key file (PEM Encoded) to the device.
CA Root Certificate	Select this option to transfer a CA certificate file to the device. This will be used as the root certificate for one of the syslog servers. Based on the index number the file will be named accordingly.
Client Key	Select this option to transfer a client certificate file to the device. This will be used as the client certificate for one of the syslog servers. Based on the index number the file will be named accordingly.
Client SSL Certificate	Select this option to transfer a client key file to the device. Based on the index number the file will be named accordingly.
SSL Trusted Root Certificate PEM File	Select this option to transfer an SSL Trusted Root Certificate file (PEM Encoded) to the device. SSL files contain information to encrypt, authenticate, and validate HTTPS sessions.
SSL Server Certificate PEM File	Select this option to transfer an SSL Server Certificate file (PEM Encoded) to the device.
SSL DH 1024 Encryption Parameter PEM File	Select this option to transfer an SSL Diffie-Hellman 1024 Encryption Parameter file (PEM Encoded) to the device.
SSL DH 2048 Encryption Parameter PEM File	Select this option to transfer an SSL Diffie-Hellman 2048 Encryption Parameter file (PEM Encoded) to the device.

3. Select the Transfer Protocol:
   - HTTP and HTTPS —These protocols do not require any additional fields.
   - TFTP —This protocol requires the Server Address and File Name.
   - FTP, SCP, and SFTP —These protocols require the Server Address, Username, Password, and File Name.
4. Enter any additional fields as required.

Field	Description
Server Address	(FTP/TFTP/SCP/SFTP only) Enter the IP address of the FTP/TFTP/SCP/SFTP server to use for file transfer (Update or Backup).
Username	For FTP, SCP or SFTP transfer, if the server requires authentication, specify the user name for remote login to the server that will receive the file.
Password	For FTP, SCP or SFTP transfer, if the server requires authentication, specify the password for remote login to the server that will receive the file.
File Name	For update operations using FTP, TFTP, SCP, or SFTP, enter the server path from which you want to upload the file, followed by the name for the file when saved. This can differ from the actual file name on the switch. The path can be 0 to 160 characters and the file name can be 1 to 32 characters. The file name can have ASCII printable characters, excluding the following: \, /, :, *, ?, ", <, >, | When backing up a script file, enter the name of the script file on the device, which can be 1 to 32 characters.
Destination File	For backup operations using FTP, TFTP, SCP, or SFTP, enter the path on the server where you want to put the file followed by the name to be applied to the file as it is saved. This name can differ from the actual file name on the switch. The path can be 0 to 160 characters, and the file name can be 1 to 32 characters. The file name can have ASCII printable characters, excluding the following: \, /, :, *, ?, ", <, >, | When updating a script file, enter the name of the script file. If the file name is not given, the script is saved with the source file name. The file name cannot include the symbols : ' ( ) * '

5. Click **Start File Transfer** to start the transfer.

   For a TFTP/SFTP/FTP/SCP backup, the switch begins the transfer to the specified location.

   For an HTTP/S update, browse to the location on your management station where the file you want to update to switch is located. For an HTTP/S backup, the file will be saved to the download folder specified by the browser.

NOTE

SSH key files can be downloaded, and SSH file types will be visible only when SSH is disabled and there are no active SSH sessions.

To download SSL related files, HTTPS must be administratively disabled.

CAUTION

Do not disturb the browser window while the transfer is in progress.

InstantOn Provisioning

Use the InstantOn Provisioning page to configure and run the AutoInstall feature, which can automatically obtain configuration information and install a new firmware image when the switch boots.

The process begins when the switch is initialized and no configuration file (startup-config) is found, or when the switch boots and loads a saved configuration that has AutoInstall enabled. If initiated, the AutoInstall feature allows the device to obtain an IP address from a network DHCP server and then is directed to a TFTP server in the DHCP response to obtain a predefined configuration file.

To configure a setting, select it, enter the configuration information, and click **Apply**.

To display the InstantOn Provisioning page, click **Maintenance** > **InstantOn Provisioning**.

Figure 245. AutoInstall Configuration Page



Table 207. AutoInstall Configuration Fields

Field	Description
Admin Mode	The current administrative mode of the AutoInstall feature: · Start — AutoInstall is enabled, and the feature will attempt to automatically configure the device during the next boot cycle. · Stop — AutoInstall is disabled. The automatic process will begin only if no configuration file is located during the next boot cycle.
Persistent Mode	If this option is selected, the settings you configure on this page are automatically saved to persistent memory in the startup-config file when you apply the changes. If this option is not selected, the device treats these settings like any other applied changes (i.e. the changes are not retained across a reboot unless you save the configuration).
AutoSave Mode	If this option is selected, the downloaded configuration is automatically saved to persistent storage. If this option is not selected, you must explicitly save the downloaded configuration in non-volatile memory for the configuration to be available for the next reboot.
AutoReboot Mode	If this option is selected, the switch automatically reboots after a new image is successfully downloaded and makes the downloaded image the active image. If this option is not selected, the device continues to boot with the current image. The downloaded image will not become the active image until the device reboots.
Retry Count	When attempting to retrieve the DHCP-specified configuration file, this value represents the number of times the TFTP client on the device tries to use unicast requests before reverting to broadcast requests.
Status	The current status of the AutoInstall process.

Configuration File Operations

Use the Configuration File Operations page to copy the information contained in one configuration file to another configuration file on the switch.

To display this page, click **Maintenance > Configuration File Operations** in the navigation pane.

Figure 246. Configuration File Operations Page



Table 208. Configuration File Operations Fields

Field	Description
Source File	Select the configuration file that will overwrite the contents in the selected destination file. The source file options are as follows: · Running Configuration—The file that contains the configuration that is currently active on the system. Copying the running configuration file to the startup configuration file is effectively the same as performing a Save. · Startup Configuration—The file that contains the configuration that loads when the system boots. · Backup Configuration—The file that is used to store a copy of the running or startup configuration. This option is available after you copy the running or startup configuration to backup.
Destination File	Select file to be overwritten by the contents in the selected source file. The destination file options are as follows: · Startup Configuration—The file that contains the configuration that loads when the system boots. · Backup Configuration—The file that is used to store a copy of the running or startup configuration.

After you specify the source file to copy and the destination file to overwrite, click **START FILE TRANSFER** to initiate the file transfer operation.

Reset

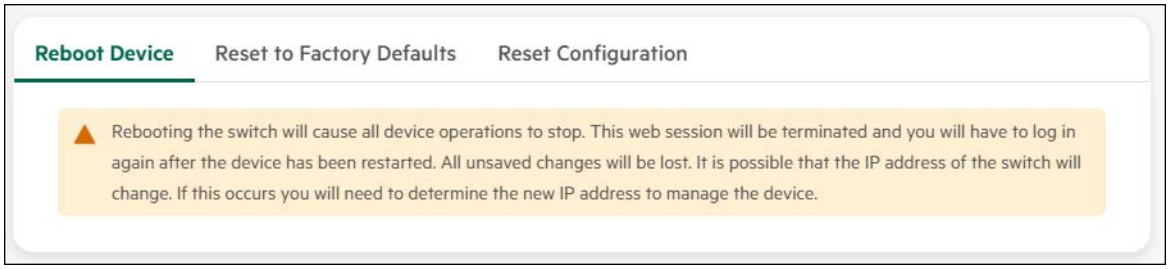
This page enables rebooting the switch, resetting the software to the factory default settings, and resetting all configuration parameters to the default values.

Reboot Device

Use this feature to perform a software reboot of the switch. If you applied configuration changes, click (**Save**) in the upper right of any page before rebooting. If the switch is configured to use DHCP to acquire its IP address, the address may change upon restart; you will need to determine the address before logging back in to the management utility.

To display the Reboot Switch page, click **Maintenance** > **Reset**, and make sure the Reboot Device tab is selected.

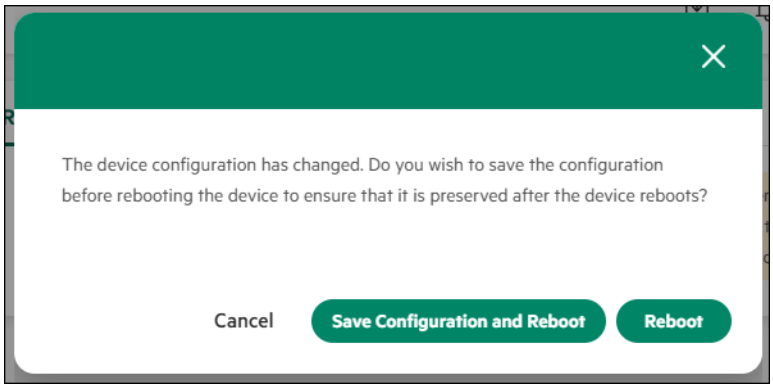
Figure 247. Reboot Device Tab



Click **Reboot** to reboot the switch.

If the device configuration has changed but has not been saved, the following window appears after you click Reboot. This window provides the opportunity to save the current configuration before rebooting the switch.

Figure 248. Save Before Reboot



To save the current configuration and reboot the switch, click **Save Configuration and Reboot**.

To continue the reboot without saving the current configuration, click **Reboot**.

Reset to Factory Defaults

Use the Reset to Factory Defaults tab to reboot the switch, restore all switch settings to their factory default values, and erase all entries in the switch log file stored in the non-volatile memory. After the switch reboots, all configuration changes, including those that were previously saved, are reset in the running system by this action.

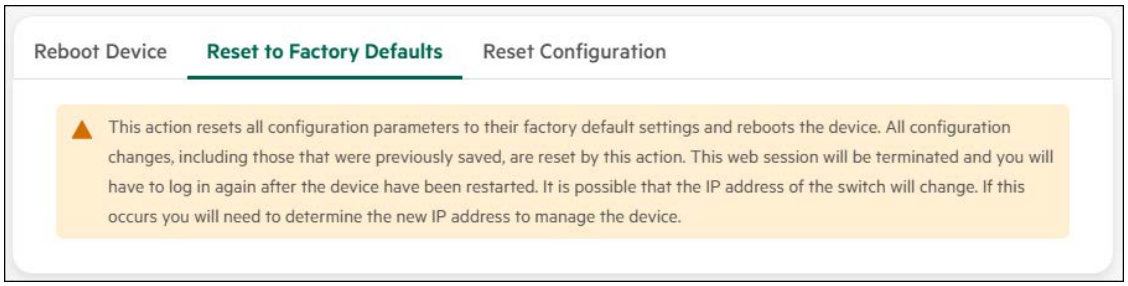
If the switch is configured to use DHCP to acquire its IP address, the address may change upon restart; you will need to determine the address before logging back in to the management utility.

To display the Reset to Factory Defaults tab, click **Maintenance > Reset**, and make sure the Reset to Factory Defaults tab is selected.

NOTE

It is recommended that you back up the current configuration file prior to restoring the factory defaults configuration. See Backup and Update Files for instructions.

Figure 249. Reset to Factory Defaults Tab



Click **Reset** to reboot the switch and restore the system to the default settings.

Reset Configuration

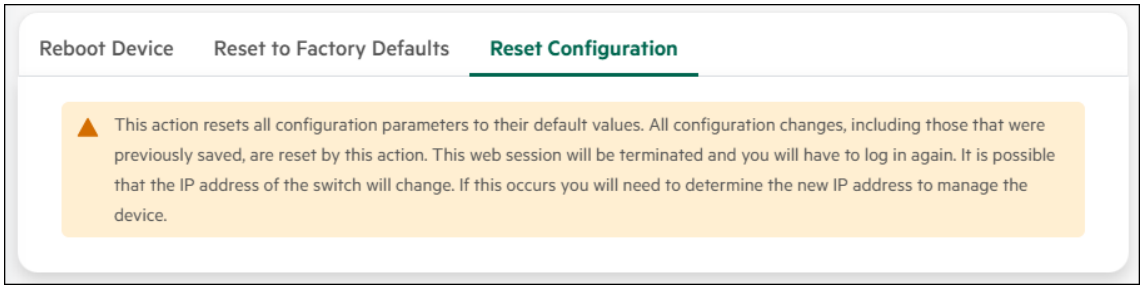
Use the Reset Configuration tab to restore all switch settings to their default values and to erase all entries in the switch log file stored in the non-volatile memory. Using the Reset Configuration option does not automatically reboot the switch. After the configuration is reset, all configuration changes, including those that were previously saved, are reset in the running system by this action.

If the switch is configured to use DHCP to acquire its IP address, the address may change the next time the switch reboots. You will need to determine the address before logging back in to the management utility.

NOTE

It is recommended that you back up the current configuration file prior to clearing the configuration. See Backup and Update Files for instructions.

Figure 250. Reset to Configuration Tab



Appendix A
Managing the Device from Direct Ops Commands

The HPE Networking Instant On 1940 Switch Series includes a Direct Ops Commands (DOCs) interface that allows you to perform basic device management when the Web interface is not available.

You can manage the device three ways when using the Direct Ops interface:

- USB-C console — Direct cable connection for local access.
- Telnet — Remote but unencrypted access.
- SSH — Remote, encrypted, and the recommended method.

You are placed in User mode immediately after you log in to the Direct Ops interface.

Command Summary

The following tables provide command summaries in each access level. The commands you can use depend on the access privileges you have.

From the User mode, you can reset the user account password, execute the ping command, and SSH or Telnet to another switch.

Table A-1. User Mode Command Summary

Command	Description
enable	Enter into Privilege mode.
help	Display help for various special keys.
logout	Exit this session. Any unsaved changes are lost.
password	Change an existing user's password.
ping	Send ICMP echo packets to a specified IP address.
show	Display CLI command options and settings. See the following table for additional `show` command information.
telnet	Telnet to a remote host

From User mode, you can view switch parameters such as the IP address, firmware version and basic feature status. The following table summarizes the `show` commands available in User mode.

Table A-2. User Mode Show Command Summary

Command	Description
show hosts	Display the default domain name, list of name server hosts, and static and cached list of host names and addresses
show port	Options are show port all or show interface range only)
show network	Display configuration for inband connectivity
show spanning-tree	Display spanning tree information
show vlan	Display VLAN configuration

Enter Privileged mode by typing the `enable` command. Privileged mode is password protected. Level 1 user accounts are prompted to enter a password. Level 2 user accounts transition directly to Privileged mode after entering `enable`.

Table A-3. Privilege Mode Command Summary

Command	Description
boot	Marks the given image as active for subsequent re-boots.
enable	Set the password for the enable privilege level.
clear	Reset the configuration to factory defaults. Options are available to clear the configuration, counters, or log files only.
configure	Enter into Global Config mode.
copy	Upload or download a file.
exit	Exit Privileged mode.
ip	Configure IP parameters. Options are available to enable, disable, or configure services including Telnet, SSH, and HTTP.
logout	Exit this session. Any unsaved changes are lost.
network	Configure in-band connectivity.
ping	Send ICMP echo packets to a specified IP address.
quit	Exit this session. Any unsaved changes are lost.
reload	Gracefully reload configuration or script file
renew dhcp	Renew an IPv4 address lease
script	Apply, delete, list, show, or validate configuration scripts.
show	Display switch options and settings. See the following table for additional `show` command information.
snmp-server	Configure SNMP server parameters, including port and trap receivers).
ssh	SSH to a remote host.
telnet	Telnet to a remote host.
traceroute	Trace the route to a destination.
update bootcode	Update the bootloader on the node from the activated image.
write	Save the current configuration to memory (`write mem`)
vlan database	Create a new VLAN. Use the `no vlan` command to delete an existing VLAN.

The following table summarizes the `show` commands available in Privileged mode.

Table A-4. Privilege Mode Show Command Summary

Command	Description
backup-config	Display the backup-configuration
bootvar	Display active and next active firmware information.
clibanner	Display banner configuration.
clock	Display the time and date from the system clock.
crypto	Display crypto certificates and public keys.
error	Display error statistics.
interface	Display IP interface information (remove dampening and switch port).

Command	Description
ip	Configure IP parameters for HTTP, Telnet, or SSH.
logging	Display logging parameters.
network	Display configuration for in-band connectivity.
port	Show information for a specified port, all ports, or a range of interfaces.
running-config	Display the running configuration.
ssh	Display SSH client configuration information.
telnet	Display outbound Telnet configuration information.
telnetcon	Display Telnet configuration information.
version	Display the switch description and hardware information.
startup-config	Display the startup-config.
spanning-tree	Display STP configuration information.
sysinfo	Display system information, including system up time, name, contact, location, and MIB support.
tech-support	Display switch information needed for trouble-shooting
vlan	Display VLAN configuration information.

Enter Global Configuration mode by typing the `config` command. The following table summarizes the commands available in Global Config mode.

Table A-5. Global Configuration Mode Command Summary

Command	Description
clock	Manage the system clock.
crypto	Generate and manage crypto certificates.
exit	Exit the mode and return to Privileged mode.
interface	Enter into Interface mode. From Interface mode, configure interface parameters including autonegotiation, speed and duplex mode, IP address parameters, spanning tree settings, and VLAN routing.
ip routing	Enable or disable routing.
logging	Configure buffered logging and logging to the console.
set	Configure the CLI banner.

Command Details

This section lists the Direct Ops commands in alphabetical order.

boot autoinstall

Use this command to operationally start or stop the AutoInstall process on the switch.

The command is non-persistent and is not saved in the startup or running configuration file.

Syntax

boot autoinstall {start | stop}

Default

Stopped

Mode

Privileged Exec

Usage guidelines

The AutoInstall feature enables the automatic update of the image and configuration of the switch. This feature enables touchless or low-touch provisioning to simplify switch configuration and imaging.

AutoInstall includes the following support:

- Downloading an image from TFTP server using DHCP option 125. The image update can result in a downgrade or upgrade of the firmware on the switch.
- Automatically downloading a configuration file from a TFTP server when the switch is booted with no saved configuration file.
- Automatically downloading an image from a TFTP server in the following situations:
  - When the switch is booted with no saved configuration found.
  - When the switch is booted with a saved configuration that has AutoInstall enabled.

When the switch boots and no configuration file is found, it attempts to obtain an IP address from a network DHCP server. The response from the DHCP server includes the IP address of the TFTP server where the image and configuration flies are located.

After acquiring an IP address and the additional relevant information from the DHCP server, the switch downloads the image file or configuration file from the TFTP server. A downloaded image is automatically installed. A downloaded configuration file is saved to non-volatile memory.

Example

```
(Switch)#boot autoinstall start
```

boot host

Use this command to configure the AutoInstall parameters on the switch.

Syntax

boot host {autoreboot | autosave | dhcp | retrycount <1–3>}

Defaults

autoreboot: Enabled

autosave: Disabled

DHCP: Enabled

retrycount: 3

Mode

Privileged Exec

Parameters

These are the boot host parameters:

- autoreboot: Allows the switch to automatically reboot after successfully downloading an image. When auto reboot is enabled, no administrative action is required to activate the image and reload the switch.
- autosave: Automatically saves the downloaded configuration file to the startup-config file on the switch. When autosave is disabled, you must explicitly save the downloaded configuration to non-volatile memory by using the `write memory` or `copy system:running-config nvram:startup-config` command. If the switch reboots and the downloaded configuration has not been saved, the AutoInstall process begins, if the feature is enabled.
- DHCP: Enables AutoInstall on the switch for the next reboot cycle. The command does not change the current behavior of AutoInstall and saves the command to NVRAM.
- retrycount: Sets the number of attempts to download a configuration file from the TFTP server. The supported range is 1 to 3.

Usage guidelines

See the guidelines in boot autoinstall.

Example

```
(Switch)#boot host autoreboot

(Switch)#boot host retrycount 2

(Switch)#boot host autosave
```

boot system

This command activates the specified image.

Syntax

boot system {active | backup}

Mode

Privileged Exec

Parameters

These are the boot system parameters:

- active: Load the active image on the next reboot.
- backup: Load the backup image on the next reboot. The backup image will become the active image.

Usage guidelines

The specified image will be the active-image for subsequent reboots and will be loaded by the boot loader. The current active-image is marked as the backup-image for subsequent reboots. If the specified image does not exist on the system, this command returns an error message.

Example

```
(Switch)#boot system backup
```

```
Activating image backup ..

(Switch)#show bootvar

Image Descriptions

 active :
 backup :

 Images currently available on Flash

 ----  ------------  ------------  -----------------  -----------------
 unit        active        backup     current-active        next-active
 ----  ------------  ------------  -----------------  -----------------
    1       3.4.0.7      3.31.1.1            3.4.0.7           3.31.1.1
```

clear config

This command resets the configuration to the factory defaults without powering off the switch.

Syntax

clear config

Mode

Privileged Exec

Usage guidelines

When you issue this command, a prompt appears to confirm that the reset should proceed. When you enter **y**, you automatically reset the current configuration on the switch to the default values. It does not reset the switch.

Example

```
(Switch)#clear config

Are you sure you want to clear the configuration? (y/n) n

Configuration Not Cleared!
```

clear counters

This command clears the statistics for a port, LAG, or VLAN, or it can clear all keepalive statistics.

Syntax

clear counters {*port-number* | all | keepalive | lag *lag-number* | vlan *vlan-id*}

Mode

Privileged Exec

Parameters

These are the parameters:

- *port-number*: Reset the statistics on the specified interface.
- all: Reset the statistics on all interfaces.

- keepalive: Reset the keepalive statistics associated with ports (for example, number of transmitted packets, received packets, and loop packets).
- lag *lag-number*: Reset the statistics on the specified LAG.
- vlan *vlan-id*: Reset the statistics on the specified routing VLAN.

Usage guidelines

You are prompted to confirm the action before executing the command. Enter **y** to continue clearing the specified counters, or enter **n** to cancel the command.

The `clear counters vlan` command is valid only for VLANs with the routing mode enabled.

Example

```
(Switch)#clear counters 3
Are you sure you want to clear the port stats? (y/n) y

Port Stats Cleared.
```

clear logging buffered

This command clears all buffered log entries.

Syntax

clear logging buffered

Mode

Privileged Exec

Usage guidelines

Executing this command clears all system startup and system operation logs.

Example

```
(Switch)#clear logging buffered

In-memory Logging Buffer cleared!
```

clear logging email statistics

This command resets the email alerting statistics.

Syntax

clear logging email statistics

Mode

Privileged

Example

```
(Switch)#clear logging email statistics
```

clear mbuf stats

This command clears the memory buffer statistics.

Syntax

clear mbuf stats

Mode

Privileged

Usage guidelines

You are prompted to confirm the action before executing the command. Enter **y** to continue clearing the memory buffer counters, or enter **n** to cancel the command.

Example

```
(Switch)#clear mbuf stats
Are you sure you want to clear mbuf statistics (y/n) y
```

clock set

This command sets the system time and date.

Syntax

clock set *hh:mm:ss*

clock set *mm/dd/yyyy*

Mode

Global Config

Parameters

These are the parameters:

- hh:mm:ss: Enter the current system time in 24-hour format in hours, minutes, and seconds. The range is hours: 0 to 23, minutes: 0 to 59, seconds: 0 to 59.
- mm/dd/yyyy: Enter the current system date the format month, day, year. The range for month is 1 to 12. The range for the day of the month is 1 to 31. The range for year is 2010 to 2079.

Example

```
(Switch)(Config)# clock set 03:17:00


(Switch)(Config)# clock set 04/16/2026
```

clock summer-time

Use the clock summer-time date command to set the summer-time offset to Coordinated Universal Time (UTC) and to set the summer-time recurring parameters.

Syntax

clock summer-time {date *date month year hh:mm month year hh:mm* | recurring {*week day month hh:mm week day month hh:mm* | EU | USA}} [offset *offset*] [zone acronym]

clock set *mm/dd/yyyy*

Mode

Global Config

Parameters

These are the parameters:

- date
  - *date*: Day of the month. Range is 1 to 31.
  - *month*: Month. The range is the first three letters by name (for example, Jan).
  - *year*: Year. The range is 2000 to 2097.
  - *hh:mm*: Time in 24-hour format in hours and minutes. The range is hours: 0 to 23, minutes: 0 to 59.
- recurring
  - EU: The system clock uses the standard recurring summer time settings used in countries in the European Union.
  - USA: The system clock uses the standard recurring daylight saving time settings used in the United States.
  - *week*: Week of the month. The range is 1 to 5, first, last.)
  - *day*: Day of the week. The range is the first three letters by name; sun, for example.
  - *month*: Month. The range is the first three letters by name; jan, for example.
  - *hh:mm*: Time in 24-hour format in hours and minutes. The range is hours: 0 to 23, minutes: 0 to 59.
- *offset*: The number of minutes to add during the summertime. The range is 1 to 1440.
- *acronym*: The acronym for the summer-time to be displayed when summertime is in effect. The range is up to four characters are allowed.

Example

```
(Switch) (Config)# clock summer-time date 8 mar 2026 2:00 1 nov 2026 2:00
(Switch) (Config)# clock summer-time recurring USA
```

clock timezone

Use this command to set the offset to Coordinated Universal Time (UTC).

Syntax

clock timezone {*hours*} [minutes *minutes*] [zone *acronym*]

Mode

Global Config

Parameters

These are the parameters:

- *hours*: Hours difference from UTC. The range is -12 to +14.
- *minutes*: Minutes difference from UTC. The range is 0 to 59.
- *acronym*: The acronym for the time zone. The range is up to four characters.

Example

```
(Switch)(Config)#clock timezone 5 minutes 30 zone INDA
```

configure

Use this command to enter Global Configuration mode from Privilege mode.

Syntax

configure

Mode

Privileged

Usage guidelines

You can also use the `configure terminal` or `config t` command to enter Global Config mode.

Afeter you enter Global Config mode, the prompt changes to include (Config) after the hostname.

Example

```
(Switch)#configure

(Switch)(Config)#
```

copy

Use this command transfer files to and from the switch using the following transfer protocols:

- HTTP
- HTTPS
- TFTP
- FTP
- SCP
- SFTP

You can also use the copy command to manage the dual images (active and backup) on the file system.

Syntax

copy *source destination* [source *option*]

Mode

Privileged

Parameters

These are the command parameters:

- *source*: The name of the source file to be copied. If the source file is not located on the switch, the source includes the URL and path to the source file. See the following table for more information
- *destination*: The name of the copied source file. When copying a file from the switch to a remote location, the destination includes a URL and path to identify where the source file is to be copied. See the following table for more information.
- source *option*: Specifies the source-interface or source IP address for the copy command. The selected source-interface IP address is to be used for filling the IP header of management protocol packets (SCP, SFTP, and TFTP). This allows security devices (firewalls) to identify the source packets coming from the specific switch. If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address. When the user selects the source interface for SCP, SFTP, or TFTP applications, it (re)binds the interface source IP address with the server. The source interface is not supported for HTTP/HTTPS protocols.

The *option* can be one of the following interfaces:

- *ip-address*: Specify the IP address of the source interface.
- *port-num*: Specify the port number of the source interface.
- network: Use the network IP address as the source interface.
- vlan *vlan-id*: Specify the VLAN ID of the source interface.

The following table lists the commands that copy a file from the switch to a remote system. In many cases, this action is useful when you want a backup copy of a file on the switch or want to analyze the data within the file.

Table A-6. Copy Command Options (from the Switch to a Remote System)

Source	Destination	Description
active	URL	Copy the active image to a remote system.
backup	URL	Copy the backup image to a remote system.
local-macAuth-db	URL	Copy the local MAC authentication database file from the device to the remote system.
nvram:application <sourcefilename>	URL	Copy the specified source application file to a remote system.
nvram:backup-config	URL	Copy the backup configuration to a remote system.
nvram:clibanner	URL	Copy the CLI banner to a remote system.
nvram:core-dump <filename>	URL	Copy the core dump file to a remote system.
nvram:cpu-pkt-capture.pcap	URL	Copy the CPU packet capture file to a remote system.
nvram:crash-log	URL	Copy the crash log to a remote system.
nvram:errorlog	URL	Copy the error log file to a remote system.
nvram:factory-defaults	URL	Copy the factory defaults file to a remote system.
nvram:fastpath.cfg	URL	Copy the binary config file to a remote system.
nvram:log	URL	Copy the log file to a server.
nvram:log-files	URL	Copy all startup and operational logs to a remote server at once.
nvram:operational-log [logfilename]	URL	Copy the operational log files or a specific operational log file to a remote system. To view the [logfilename] options, use the `show logging persistent log-files` command. Operational logs have the format ologlvl*.txt.
nvram:startup-config	URL	Copy the stored startup configuration file from the device to a remote system.
nvram:startup-log [logfilename]	URL	Copy the startup log files or a specific startup log file to a remote system. To view the [logfilename] options, use the `show logging persistent log-files` command. Operational logs have the format sloglvl*.txt.
nvram:tech-support	URL	Copy the technical support log to a remote system.
nvram:traplog	URL	Copy the trap log file to a remote system.
system:running-config	URL	Copy (backup) the running configuration file to a remote system.

The following table lists the commands that copy a file from a remote system to the switch. In many cases, this action is useful when you want to overwrite a file on the switch or upload certificate or key files to the switch.

Table A-7. Copy Command Options (from a Remote System to the Switch)

Source	Destination	Description
URL	backup	Copy an image from a remote server to switch as the backup image. This action overwrites any existing backup image on the switch.
URL	local-macAuth-db	Copy a MAC authentication database file to the switch. The macAuth database stores a list of MAC addresses for local port-based user authentication.
URL	nvram:application <destfilename>	Copies an application file to the switch with the specified filename.
URL	nvram:backup-config	Copy a configuration file from a remote server to the backup configuration file. This action overwrites the backup configuration file on the switch.
URL	nvram:ca-root [1-8]	Copy the CA certificate file to the switch and use the index number name in the copied file as CA[1-8].pem.
URL	nvram:clibanner	Copy a CLI banner file to the device. This file contains the text to be displayed on the CLI before the login prompt.
URL	nvram:client-key [1-8]	Copy a client certificate file to the switch. This file will be used as the client certificate for one of the syslog servers. Based on the index number the file will be named accordingly.
URL	nvram:client-ssl-cert [1-8]	Copy a client key file to the device. Based on the index number the file will be named accordingly.
URL	nvram:factory-defaults	Copy the factory default configuration file to the device. This file contains baseline configuration that the device uses when it is first powered on or reset to its original state.
URL	nvram:fastpath.cfg	Copy the binary config file to the switch.
URL	nvram:root-ca-certs	Copy root CA certificate files to the root-certificates directory on the switch.
URL	nvram:sshkey-ecdsa	Copy an SSH-2 ECDSA key file (PEM Encoded) to the switch.
URL	nvram:sshkey-rsa2	Copy an SSH-2 RSA key file (PEM Encoded) to the switch.
URL	nvram:sshkey-user-publickey <filename>	Copy the user SSH public key to the switch.
URL	nvram:sslpem-dh1024	Copy an SSL Diffie-Hellman 1024 Encryption Parameter file (PEM Encoded) to the switch.
URL	nvram:sslpem-dh2048	Copy an SSL Diffie-Hellman 2048 Encryption Parameter file (PEM Encoded) to the switch.
URL	nvram:sslpem-root	Copy an SSL Trusted Root Certificate file (PEM Encoded) to the switch.
URL	nvram:sslpem-server	Copy an SSL Server Certificate file (PEM Encoded) to the device.
URL	nvram:startup-config	Copy a configuration file from a remote server to the startup configuration file. This action overwrites the startup configuration file on the switch.
URL	nvram:tech-support-cmds	Copy the tech support commands file to the switch.

The following table lists the commands that copy (or overwrite) one file on the switch with another file on the switch.

Table A-8. Copy Command Options (Within the Switch)

Source	Destination	Description
active	backup	Copy the active image to the backup image.
backup	active	Copy the active image to the backup image.
nvram:backup-config	nvram:startup-config	Copy the backup configuration to the startup configuration.
system:running-config	nvram:factory-defaults	Copy the running configuration file to the factory default file.
system:running-config	nvram:startup-config	Copy the running configuration file to the startup configuration file.

Usage guidelines

The URL (including keywords for transfer type) is case-sensitive.

If the source or destination includes a URL, use one of the following values:

- tftp://{ipaddr | hostname | ipv6address}[:port]/filepath/filename [noval]
- sftp|scp://username@ipaddr | ipv6address/filepath/filename
- ftp://user@{ipaddr | hostname | ipv6addres}[:port]/filepath/filename
- http://user@url/[:port]/filepath/filename}
- https://user@url[:port]/filepath/filename

For FTP, TFTP, SFTP, and SCP, the parameters are as follows:

- ipaddr | hostname | ipv6address: The IP address, host name, or IPv6 address of the server.
- :port: The optional user-defined (non-default) port number for all transfer methods.
- filepath: The path to the file
- filename: The name of the file you want to upload or download.

Example

The following output shows an example of the command to copy the running config file to a remote system using TFTP.

```
(Switch) #copy system:running-config tftp://10.89.105.143:8009/run-cfg
Mode........................................... TFTP
Set Server IP.................................. 10.89.105.143
Set Server Port................................ 8009
Path........................................... ./
Filename....................................... run-cfg
Data Type...................................... Text Configuration
Source Filename................................ running-config

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the duration of the transfer. Please
wait...

File transfer operation completed successfully.
(Switch) #
```

The following commands show examples of copying SSL Diffie Hellman 1024 and 2048 PEM filetypes from a remote system to the switch using SCP.

```
copy scp://user@< ipaddr|hostname >/<path>/<filename> nvram:sslpem-dh2048
copy scp://admin@10.85.234.2/home/sk019490/dh2048.pem nvram:sslpem-dh2048

copy scp://user@< ipaddr|hostname >/<path>/<filename> nvram:sslpem-dh1024
copy scp://admin@10.85.234.2/home/sk019490/dh2048.pem nvram:sslpem-dh1024
```

crypto certificate

Use this command to manage keys and certificates.

Syntax

crypto certificate {1 | 2} {generate | request | import}

Mode

Global Config

Parameters

These are the parameters:

- 1 or 2: The certificate number.
- generate: Generate a self-signed certificate for HTTPS. This command enters the Crypto Certificate Generation mode.
- request: Generate and display a certificate request for HTTPS. This command enters the Crypto Certificate Request mode.
- Before generating a certificate request, you must first generate a self-signed certificate using the crypto certificate generate command in Global Configuration mode, to sign the certificate request. Make sure to re-enter the identical values in the certificate request fields as were entered in the self-signed certificate generated by the crypto certificate generate command.
- import: Import a signed certificate provided by the Certification Authority (CA).

Usage Guidelines

After entering Crypto Certificate Generate or Crypto Certificate Request mode, use the following parameters to configure the certificate.

- common-name: Specifies the common name, which is the fully qualified URL or IP address of the device. If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).
- country: Specifies the country name.
- duration: Specifies number of days a self-signed certification would be valid. If unspecified defaults to 365 day.
- email: Specifies the contact email address.
- exit: To generate certificate and exit from the mode.
- key-generate: Regenerate SSL RSA key.
- location: Specifies the location or city name.
- organization-name: Specifies the organization name
- organization-unit: Specifies the organization internal unit
- quit: To quit from the mode.
- state: Specifies the state or province name.
- subject-alternative-name: Specifies the Subject Alternative Name.

Enter the fields, such as key-generate, duration, location, and so on. The generated RSA key for SSL has a length specified by the key-generate field. The `exit` command attempts to generate the self-signed certificate. Use the `quit` command to exit Crypto Certificate Generation/Request mode without generating a certificate.

The certificate request that is generated using this command is sent to the Certification Authority for signing. The certificate request is generated in Base64-encoded X509 format.

When importing a certificate, enter an external certificate (signed by the Certification Authority) to the switch. To end the session, add a period on a separate line after the input, and press Enter. The signed certificate must contain the switch public key, match the RSA key on the switch, and must be in X509 PEM text format.

Examples

```
(Switch)(config)#crypto certificate 2 request

(Switch)(config-crypto-cert-req)#country US

(Switch)(config-crypto-cert-req)#location RTP

(Switch)(config-crypto-cert-req)#state NC

(Switch)(config-crypto-cert-req)#organization-name HPE

-----BEGIN CERTIFICATE REQUEST-----
MIICXTCCAUUCAQAwGDEWMBQGA1UEAwwNMTAuNTIuMTMxLjE3MDCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMjGcKvmMue6JqsZyMOnGcHmvm0KNkIQom7t
8BZrUJZBivcuEMpjAHI3H3FfE0drSzJQ4/VJk/ISwyqdcPmCYUqQXjB7ZFoTs5/5
KBoLL09P8jJ7lZ63+6ROcQpYDWGzFzJBgmKMShSUJi+g8SKt2JXDycJlYOrjxGY+
5CDrHo3lVqK0NUUu4aCbhA+mt3NuduVWvXfl4qSOEDFURCkqkCw/HJOkeESJgsMh
CGTaypbXyy4/u5PVA9Ivp0aeeWA1OEk0888rhi2HfGAjmC8e0fW9hXYTRZpszn/A
whc89uqiSHrviGoVA23LnizI1HptZyzEMZ8qf6KwTWHSHA7TjNMCAwEAAaAAMA0G
CSqGSIb3DQEBCwUAA4IBAQAGC36Bs/CMD4FVDGL7SJ+gAO8TNpkKPhPOmvItG//Q
TSSBSu26h+lio2bn/q5rFDvwbslnUCzR0GCB2yro9haMectXg38sxoFh3ow2PJYm
jpuOxSWPkKka2/jtXoBola8DUq3vqmcZoDuLsCM6AH4czi4MV8y8ajmv+CCykF4g
JzV+3qNGeJYqgib37tlfWsvkV33FJ0lLMPlYNs2dACPBpmlnmOwissEs94Kp6yMK
cQ8wNLWwP4QC1r/YzqMExBLv8NJaTwb5M90CpCUAWBKluslTpLykilwqVInX9zan
vVs6ZcfMKh2carOphsEr9vZP5hJX9DmOa39P+N+UdDjJ
-----END CERTIFICATE REQUEST-----
(Switch)(Config)#crypto certificate 1 import

Please paste the input now, add a period (.) on a separate line after the input, and press Enter.
-----BEGIN CERTIFICATE-----
MIIBrDCCARWgAwIBAgIJANi+zML5qmloMA0GCSqGSIb3DQEBCwUAMBgxFjAUBgNV
BAMMDTEwLjEzMC44Ni4yMTcwHhcNNzAwMTAxMDM0MzM3WhcNNzEwMTAxMDM0MzM3
WjAYMRYwFAYDVQQDDA0xMC4xMzAuODYuMjE3MIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQCZsOyuz2MlQ8ab+Y9vcRgqJdakeL8z4XLNRRDlAsNcOE6GXwskDrT8
hx0r7MywrO4J6bPfqG2t63ee3KUyPS+B6OdxwmNycRwbUZabxD87MmBwx9OtUULY
AkNCUKXG6I9kxUXry4CNbOmFtVpTHDr+xqWbmpQemRjB3VpUXOueewIDAQABMA0G
CSqGSIb3DQEBCwUAA4GBAHycAeQZv80Vxcw+hWFNsWePkD6VdM8o3ecV9kcCcFuV
SreKkICC6HBuPKVxqcoVoGbBiRSMGcDJ4XD9vEWWHZv1QiIn8Z1jy+OSpEAruIOi
myM3O5c1eG/4baIci1ccIJgWjwxZwAPd6kz+OtXHhWLn/+Y2akg3sev6oXTLTCsv
-----END CERTIFICATE-----
.

Certificate imported successfully
```

crypto dhparam size

Use this command to manage keys and certificates.

Syntax

crypto dhparam size {1024 | 2048}

Mode

Global Config

Parameters

These are the parameters:

- 1024: Diffie-Hellman 1024 bit key.
- 2048: Diffie-Hellman 2048 bit key.

Examples

```
(Switch)(config)#crypto dhparam size 2048
```

crypto key generate

Use this command to generate an RSA or ECDSA key pair for SSH. The new key files overwrite any existing generated or downloaded key files.

Syntax

crypto key generate {ecdsa | rsa} [*key-len*]

Mode

Global Config

Parameters

These are the parameters:

- ecdsa: ECDSA key pair for SSH.
- rsa: RSA key pair for SSH.
- *key-len*: The key length for the ECDSA or RSA key, in bits (ECDSA: 256, 384, or 521 bits. RSA: 1024, 2048, or 3072 bits).

Examples

```
(Switch)(Config)#crypto key generate ecdsa

ECDSA key generation started, this may take a few minutes....
ECDSA key generation complete.
```

crypto key {encrypt | decrypt} write

Use this command to encrypt or decrypt key files with a user-provided passphrase.

Syntax

crypto key {encrypt | decrypt} write {rsa | dsa | ecdsa | sslt-cert-key cert-num | sslt-client-cert-key client-key-num} passphrase *passphrase*

Mode

Global Config

Parameters

These are the parameters:

- rsa: RSA key pair for SSH.
- dsa: DSA key pair for SSH.
- ecdsa: ECDSA key pair for SSH.
- cert-num: The SSL certificate key.
- client-key-num: The SSL client certificate key.
- passphrase: The passphrase must be at least 8 characters long.

Usage guidelines

If an SSH key has not been generated, the command failes.

The key file to be encrypted is indicated by using an argument to the command. On successful encryption, the system configuration is saved to NVRAM automatically. The encrypted key file replaces the plain-text key file on flash.

Examples

```
(Switch)(Config)#crypto key encrypt write ecdsa passphrase this-is-my-passphrase

The key will be encrypted and saved on NVRAM.
This will result in saving all existing configuration also.
Do you want to continue? (y/n):y


(Switch)(Config)#
Config file 'startup-config' created successfully.
```

crypto key pubkey-chain ssh

Use this command to enter the Public Key Configuration mode to manually specify public keys for SSH clients or an individual user.

Syntax

crypto key pubkey-chain ssh user-key *user-name* {rsa | ecdsa}

Mode

Global Config

Parameters

These are the parameters:

- *user-name*: The key length for the ECDSA or RSA key, in bits (ECDSA: 256, 384, or 521 bits. RSA: 1024, 2048, or 3072 bits).
- ecdsa: ECDSA key pair for SSH.
- rsa: RSA key pair for SSH.

Usage guidelines

After executing the `crypto key pubkey-chain ssh` command, you enter Public Key Config mode. Enter the `key-string` command and paste the ECDSA or RSA key surrounded by quotation marks.

Enter `exit` to return to the previous command mode.

Examples

```
(Switch)(Config)#crypto key pubkey-chain ssh user-key admin rsa

(Switch)(config-pubkey-key)#key-string "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAvwova0rICLGoTJ46ZMRknjAk8pBEz3Y4DijzV7oim+wW7DI5mFUULI3cT111OcjGHeQF03
phufEDcK45Cr0nHCD37zDwjN5B2+YFtVq6h4dQGfBFJVnXvJ/PmqDt5iti/jAvRXn4NzHA03byn8/
yHUsrzI6Syd3FZfaBvD+Shxpgx+pZkkLRXHgZlL/s7uxOpu6aWwjhZEZFz5RJX//chT5J3uHn++W9Yt/
3CwEenZeF4oOwEji5DTnPfkTnHxm8s4NSWHpKYOsN8LW23ooEmU0moRU0KJx7/
Zeuw36fI6RvEIFbTmX6a59GRBPpaMh9bHBAGxDA4X9x5AXTrsqS1Q=="

(Switch)(config-pubkey-key)#exit
```

enable

Use this command in User mode to enter into Privileged Exec mode.

Syntax

enable

Mode

User

Usage guidelines

If the enable password is set, users must enter a password to access Privileged Exec mode. The command prompt changes in each command mode to help you identify the current mode.

Examples

```
(Switch)>enable

(Switch)#
```

enable password

Use this command to set a local password to control access to the privileged EXEC mode.

Syntax

enable password [encryption-type *encryption-type*] | [*password* [encryption-type *encryption-type*] encrypted]

Mode

Privileged Exec

Parameters

These are the command parameters:

- *password*: Specify the password for this level in encrypted format. Range: 8 to 64 characters.
- *encryption-type*: Specify the encryption algorithm type as MD5, AES, SHA256, or SHA512. The default value of encryption-type is AES.
- encrypted: The password entered or copied from another switch configuration, and is already encrypted. If specified in encrypted format, the *password* parameter must be exactly:
  - 128 hexadecimal characters for AES.
  - 34 characters for MD5 salt hash.
  - 63 characters for SHA256 salt hash.
  - 106 characters for SHA512 salt hash.

Usage guidelines

This command allows you to input the password in encrypted format, which aids in transferring the enable password between devices without having to know the password.

The command `enable password` does not accept plain text format. Specify the password in encrypted format.

This command displays the password in running-configuration in encrypted mode for the default encryption type. If the enable password is configured, `enable password password encryption-type encryption-type encrypted` is displayed in the running-configuration for both default and non-default encryption types.

Examples

The following example shows the command to configure the plain text password with AES encryption.

```
(Switch)#enable password encryption-type aes

Enter old password:********

Enter new password:********

Confirm new password:********
```

The following example shows the command to configure the encrypted password with AES encryption:

```
(Switching)#enable password
0a51d780be1a0240b8cc7c69fe0479dbf07644e1094b25fb43ebe2fa72f649e42ad9711bf5c33f9a7eb88efd8b9945347b
264e0c52b3a47db05f886caae9f42b encrypted
```

exit

Exit the current mode and return to the previous mode.

Syntax

exit

Mode

All command modes above User mode in the command mode hierarchy.

Usage guidelines

Issuing the exit command moves you back exactly one level at a time within the command mode hierarchy.

Examples

The following example starts in Interface Config mode and ends in User mode after exiting Global Config and Privileged modes.

```
(Switch)(Config)#interface 3

(Switch)(Interface 3)#exit

(Switch)(Config)#exit

(Switch)#exit

(Switch)>
```

help

Use this command to display help for various special keys.

Syntax

help

Mode

User

Examples

```
(Switch)>help

HELP:
Special keys:
  DEL, BS .... delete previous character
  Ctrl-A  .... go to beginning of line
  Ctrl-E  .... go to end of line
  Ctrl-F  .... go forward one character
  Ctrl-B  .... go backward one character
  Ctrl-C  .... cancel input and go to next line
  Ctrl-D  .... delete current character
  Ctrl-U, X .. delete to beginning of line
  Ctrl-K  .... delete to end of line
  Ctrl-W  .... delete previous word
  Ctrl-T  .... transpose previous character
  Ctrl-P  .... go to previous line in history buffer
  Ctrl-R  .... rewrites or pastes the line
  Ctrl-N  .... go to next line in history buffer
  Ctrl-Y  .... print last deleted character
  Ctrl-Q  .... enables serial flow
  Ctrl-S  .... disables serial flow
  Ctrl-Z  .... return to root command prompt
  Tab, <SPACE> command-line completion
  Exit    .... go to next lower command prompt
  ?       .... list choices
```

interface

Use this command to enter Interface mode for the specified interfaces.

Syntax

interface *intf-range*

Mode

Global Config

Interface

Parameters

The *intf-range* parameter can be a single interface, a contiguous range of interfaces, or non-contiguous set of interfaces. Use a comma between non-contiguous interfaces or a hyphen for ranges.

Usage guidelines

After entering the command, the command prompt changes and includes the interface numbers.

The following table lists the commands available in Interface mode. For more information about each command and its parameters, type **?** at the command prompt.

Table A-9. Interface Mode Command Summary

Command	Description
auto-negotiate	Enables/Disables automatic negotiation on a port.
autostate	Enables Auto-State for an interface, Use the no form to disable
description	Add description to the interface.
dhcp	Configure DHCP L2 Relay parameters.
exit	Exit from the mode.
interface	Enter into Interface Mode.
ip	Configure IP parameters.
poe	Configure PoE.
routing	Enables routing for an interface, Use the no form to disable
shutdown	Disable a port.
snmp	Configure SNMP options.
spanning-tree	Set the spanning tree operational mode.
speed	Sets the speed and duplex setting for the interface.
vlan	Configure VLAN parameters.

Examples

```
(Switch)(Config)#interface 3
(Switch)(Interface 3)#exit

(Switch)(Config)#interface 3,5,7-9
(Switch)(Interface 3,5,7-9)#
```

ip http

Use this command to configure web-based access to the switch.

Syntax

ip http {port *number* | server | secure-server | session {hard-timeout *hours* | soft-timeout *minutes* | maxsessions *sessions*}}

Mode

Privileged Exec

Parameters

These are the parameters:

- port *number*: The TCP port number on which the HTTP server listens for requests. For HTTP the default is 80, for HTTPS the default is 443. The valid range for this port number is 1025 - 65535.
- server: Configures whether users can log into the switch from the Web interface using HTTP.
- secure-server: Configures whether users can log into the switch from the Web interface using Secure HTTP (HTTPS).

- session: Configure the parameters for a use logged into the web interface.
  - hard-timeout *hours*: The amount of time the user remains logged into the web interface regardless of the amount of HTTP/S activity that occurs. By default, the timeout is 24 hours. The valid range is 1 to 168 hours.
  - soft-timeout *minutes*: The amount of time a user remains logged into the web interface without any HTTP/S activity. By default, the timeout is 10 minutes. The valid range is 1 to 60 minutes.
  - maxsessions *sessions*: The number of allowable un-secure HTTP sessions. The valid range is 0 to 5.

Usage guidelines

When HTTP/S access is enabled, the user can login to the switch from the Web interface. When access is disabled, the user cannot login to the switch's Web server. Disabling the Web interface takes effect immediately. All interfaces are affected.

Examples

```
(Switch)#ip http server

(Switch)#ip http session hard-timeout 100
```

ip routing

Use this command to administratively enable IPv4 routing on the switch.

Syntax

ip routing

Mode

Global Config

Usage guidelines

When routing is enabled, the switch can act as a Layer 3 switch by routing packets between interfaces configured for IP routing.

When routing is disabled, the switch acts as a Layer 2 bridge and switches traffic between interfaces. The switch does not perform any internetwork routing.

Examples

```
(Switch)(Config)#ip routing
```

ip scp server enable

This command enables SCP server functionality for SCP push operations on the switch, which allows files to be transferred from the host device to the switch using the SCP protocol.

Syntax

ip scp server enable

Mode

Privileged Exec

Usage guidelines

During an SCP file transfer operation, the management operations on the switch are blocked. After the completion of file download to the switch, the switch performs file validations.

To allow the SCP file transfers from the host system to the switch, the SCP server must be enabled on the switch.

Examples

```
(Switch)#ip scp server enable
```

ip ssh

Use this command to enable SSH access to the system and configure various SSH settings.

Syntax

ip ssh [authentication-retries *attempts* | port *tcp-port* | pubkey-auth |server {enable | test}]

Mode

Privileged Exec

Parameter

These are the parameters:

- authentication-retries *attempts*: Specify the maximum authentication retries allowed per SSH connection. The default value is 3. The range is 0 to 5.
- port *tcp-port*: The TCP port number on which the SSH server listens for requests. The default value is 22. Valid port numbers are from 1 to 65535.
- pubkey-auth: Enable public key authentication for incoming SSH sessions.
- server enable: Enable SSH access.
- server test: Check the validity of the configuration file and the sanity of the keys.

Usage guidelines

The `ip ssh` command with no options is the short form of the `ip ssh server enable` command.

The `ip ssh server test` command is equivalent to the Linux `sshd -t` command.

Examples

```
(Switch)#ip ssh
(Switch)#ip ssh authentication-retries 5
(Switch)#ip ssh server test

SSH server configuration file and keys validation passed.
```

ip ssh {client | server} algorithm encryption

Use this command to specify the encryption algorithms used to establish the SSH client-side or server-side connection.

Syntax

ip ssh {client | server} algorithm encryption {[aes128-ctr] [aes128-gcm@openssh.com] [aes192-ctr] [aes256-ctr] [aes256-gcm@openssh.com] [chacha20-poly1305@openssh.com]}

Mode

Privileged Exec

Parameters

These are the parameters:

- aes128-ctr: A symmetric encryption cipher using a 128-bit key in Counter (CTR) mode.
- aes128-gcm@openssh.com: A modern, high-performance mode that provides both encryption and data integrity (authentication) in one step using a 128-bit key.
- aes192-ctr: A symmetric encryption cipher using a 192-bit key in CTR mode.
- aes256-ctr: A symmetric encryption cipher using a 256-bit key in CTR mode.
- aes256-gcm@openssh.com: A modern, high-performance mode that provides both encryption and data integrity (authentication) in one step using a 256-bit key.
- chacha20-poly1305@openssh.com: A high-performance, secure Authenticated Encryption with Associated Data (AEAD) cipher used in OpenSSH, combining the ChaCha20 stream cipher and Poly1305-AES MAC.

Usage guidelines

The command also defines the order of the encryption algorithms.

Examples

```
(Switch)#ip ssh client algorithm encryption aes128-ctr aes192-ctr

(Switch)#ip ssh server algorithm encryption aes128-ctr aes192-ctr
```

ip ssh {client | server} algorithm hostkey

Use this command to specify the host key algorithms used to establish the SSH client-side or server-side connection.

Syntax

ip ssh {client | server} algorithm hostkey {[ecdsa-sha2-nistp256] [ecdsa-sha2-nistp384] [ecdsa-sha2-nistp521] [rsa-sha2-256] [rsa-sha2-512] [ssh-rsa]}

Mode

Privileged Exec

Parameters

These are the parameters:

- ecdsa-sha2-nistp256: Use the ECDSA standard with the 256-bit key and SHA-256 hashing.
- ecdsa-sha2-nistp384: Use the ECDSA standard with the 384-bit key with SHA-384 hashing.
- ecdsa-sha2-nistp521: Use the ECDSA standard with the 521-bit key and SHA-512 hashing.
- rsa-sha2-256: Use an RSA key with the SHA-256 hash function.
- rsa-sha2-512: Use an RSA key with the SHA-512 hash function.
- ssh-rsa: Use the SSH-RSA host key algorithm.

Usage guidelines

This command also defines the order of host key algorithms.

Examples

```
(Switch)#ip ssh client algorithm hostkey ecdsa-sha2-nistp256 ecdsa-sha2-nistp384

(Switch)#ip ssh server algorithm hostkey ecdsa-sha2-nistp256 ecdsa-sha2-nistp384
```

ip ssh {client | server} algorithm kex

Use this command to specify the key exchange algorithms used to establish the SSH client-side or server-side connection.

Syntax

ip ssh {client | server} algorithm kex {[curve25519-sha256] [curve25519-sha256@libssh.org] [diffie-hellman-group-exchange-sha256] [diffie-hellman-group14-sha1] [diffie-hellman-group14-sha256] [diffie-hellman-group16-sha512] [diffie-hellman-group18-sha512] [ecdh-sha2-nistp256] [ecdh-sha2-nistp384] [ecdh-sha2-nistp521] [mlkem768x25519-sha256] [sntrup761x25519-sha512] [sntrup761x25519-sha512@openssh.com]}

Mode

Privileged Exec

Parameters

These are the parameters:

- curve25519-sha256: The EC Diffie-Hellman key exchange method on Curve25519 with SHA2-256.
- curve25519-sha256@libssh.org: The EC Diffie-Hellman key exchange method on Curve25519 with SHA2-256 by libssh.
- diffie-hellman-group-exchange-sha256: The Diffie-Hellman group exchange algorithm using SHA2-256.
- diffie-hellman-group14-sha1: The Diffie-Hellman group14 algorithm using SHA1.
- diffie-hellman-group14-sha256: The Diffie-Hellman group14 algorithm using SHA2-256.
- diffie-hellman-group16-sha512:The Diffie-Hellman group16 algorithm using SHA2-512.
- diffie-hellman-group18-sha512: The Diffie-Hellman group18 algorithm using SHA2-512.
- ecdh-sha2-nistp256: The ECDH key exchange method with ephemeral keys generated on the nistp256 curve using SHA2.
- ecdh-sha2-nistp384: The ECDH key exchange method with ephemeral keys generated on the nistp384 curve using SHA2.
- ecdh-sha2-nistp521: The ECDH key exchange method with ephemeral keys generated on the nistp521 curve using SHA2.
- mlkem768x25519-sha256: Module-Lattice Key Enapsulation mechanism (ML-KEM) combined with X25519 ECDH key exchange method.
- sntrup761x25519-sha512: The hybrid Streamlined NTRUPrime + x25519 key exchange method IANA-assigned name.
- sntrup761x25519-sha512@openssh.com: The hybrid Streamlined NTRU Prime + x25519 key exchange method

Usage guidelines

This command also defines the order of the KEX algorithms.

Examples

```
(Switch)#ip ssh client algorithm kex curve25519-sha256 ecdh-sha2-nistp384


(Switch)#ip ssh server algorithm kex curve25519-sha256 ecdh-sha2-nistp384
```

ip ssh {client | server} algorithm mac

Use this command to specify the message authentication code (MAC) algorithms used to establish the SSH client-side or server-side connection.

Syntax

ip ssh {client | server} algorithm mac {[hmac-md5] [hmac-md5-96-etm@openssh.com] [hmac-md5-etm@openssh.com] [hmac-sha1] [hmac-sha1-96-etm@openssh.com] [hmac-sha1-etm@openssh.com] [hmac-sha2-256] [hmac-sha2-256-etm@openssh.com] [hmac-sha2-512] [hmac-sha2-512-etm@openssh.com]}

Mode

Privileged Exec

Parameters

These are the parameters:

- hmac-sha2-256: 256-bits of hash-based MAC using secure hash algorithm-2 (SHA-2).
- hmac-sha2-256-etm@openssh.com: 256-bits of hash-based Encrypt-then-MAC using SHA-2.
- hmac-sha2-512: 512-bits of hash-based MAC using SHA-2.
- hmac-sha2-512-etm@openssh.com: 512-bits of hash-based Encrypt-then-MAC using SHA-2.

Usage guidelines

The command also defines the order of the MAC algorithms.

Examples

```
(Switch)#ip ssh client algorithm mac hmac-md5-etm@openssh.com hmac-sha2-256 hmac-sha1


(Switch)#ip ssh server algorithm mac hmac-md5-etm@openssh.com hmac-sha2-256 hmac-sha1
```

ip telnet

Use this command to enable Telnet connections to the system and (optionally) configure the TCP port for Telnet connections.

Syntax

ip telnet {server enable | port *tcp-port*}

Mode

Privileged Exec

Parameters

These are the parameters:

- server enable: Enable the Telnet connection (open the Telnet listening port).
- port *tcp-port*: Configures the TCP port number on which the Telnet server listens for requests. The default port is 23. The valid range for a different port is 1025 to 65535.

Examples

```
(Switch)#ip telnet server enable


(Switch)#ip telnet port 1123
```

logging

This command configures logging to an in-memory log (buffered) or to the CLI console.

Syntax

logging {buffered | console} [*severity-level*]

Mode

Global Config

Parameters

These are the parameters:

- buffered: Configures the in-memory log.
- console: Configures logging to the CLI console.
- *severity-level*: Enter the logging severity level from 0 to 7. Logs at this severity level and above are sent to the buffered log or to the console.
  - 0: Emergency: 0
  - 1: Alert
  - 2: Critical
  - 3: Error
  - 4: Warning
  - 5: Notice
  - 6: Info
  - 7: Debug

Examples

```
(Switch)(Config)#logging console 3
```

logout

Use this command to exit this session.

Syntax

logout

Mode

Privileged Exec

User

Usage guidelines

Before exiting the current session, you are prompted to save any changes even if you have not made any changes to the configuration.

Examples

```
(Switch)#logout

The system has unsaved changes.
Would you like to save them now? (y/n) n
```

network ipv6

Use this command to enable IPv6 management mode, configure the IPv6 gateway, or configure the IPv6 neighbor.

Syntax

network ipv6 {enable | gateway *ipv6-address* | neighbor *ipv6-address mac-address*}

Mode

Privileged Exec

Parameters

These are the parameters:

- enable: Enable IPv6 administrative mode for system management.
- gateway: Configure the IPv6 gateway (default router) information for the management interface.
  - *ipv6-address*: IPv6 address in global or link-local address format.
- neighbor: Manually add IPv6 neighbors to the IPv6 neighbor table
  - *ipv6-address*: The IPv6 address of the neighbor or interface.
  - *mac-address*: The link-layer address.

Usage guidelines

Only a single IPv6 gateway address can be configured.

When configuring an IPv6 neighbor and it already exists in the neighbor table, the entry is automatically converted to a static entry. Static entries are not modified by the neighbor discovery process. They are, however, treated the same for IPv6 forwarding. Static IPv6 neighbor entries are applied to the kernel stack and to the hardware when the corresponding interface is operationally active.

Examples

```
(Switch)#network ipv6 gateway fe80::215:5dff:fe12:3456

(Switch)# ipv6 neighbor fe80::1 00ab.cdef.1234
```

network ip6 address

Use this command to configure a static IPv6 management address or enable dynamic configuration of the IPv6 management address.

Syntax

network ipv6 address {*prefix/prefix-length* [eui64] | autoconfig | dhcp}

Mode

Privileged Exec

Parameters

These are the parameters:

- *prefix*: IPv6 prefix in IPv6 global address format.
- *prefix-length*: IPv6 prefix length value.
- eui64: Formulate IPv6 address in eui64 address format.
- autoconfig: Enable stateless global address autoconfiguration.
- dhcp: Enable the DHCPv6 client protocol.

Usage guidelines

Use the command with *prefix/prefix-length* [eui64] to manually configure a static IPv6 address on the management port.

Use the autoconfig keyword to allow the management interface to acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of Router Advertisement messages.

Use the dhcp keyword to attempt to acquire network information from a DHCPv6 server.

Examples

```
(Switch)#network ipv6 address 2001:db8::/32 eui64
```

network mac-address

This command sets a locally administered MAC addresses.

Syntax

network mac-address *mac-addr*

Mode

Privileged Exec

Parameters

These *mac-addr* parameter is a twelve-character locally administered MAC address.

Usage guidelines

The following rules apply to the *mac-addr* parameter:

- Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (b'0') or locally administered (b'1').
- Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (b'0') or a group address (b'1').
- The second character, of the twelve character *mac-addr*, must be 2, 6, A, or E.

Examples

```
(Switch)#network mac-address 02:AA:BB:CC:DD:EE
```

network mac-type

This command specifies whether the switch uses the burned in MAC address or the locally administered MAC address.

Syntax

network mac-type {local | burnedin}

Mode

Privileged Exec

Parameters

- local: Use the locally administered MAC address. This is the default value.
- burnedin: Use the burned-in MAC address.

Examples

```
(Switch)#network mac-type local
```

network mgmt_vlan

This command specifies whether the switch uses the burned in MAC address or the locally administered MAC address.

Syntax

network mgmt_vlan *vlan-id*

Mode

Privileged Exec

Parameter

The *vlan-id* parameter is the ID of the management VLAN. The range is 1 to 4092. The default VLAN ID for the management VLAN is 1.

Usage guidelines

All ports are members of VLAN 1 by default. A VLAN that does not have any member ports (either tagged or untagged) should not be configured as the management VLAN.

When the network protocol is configured to be DHCP, any change in the configured management VLAN ID might cause a disruption in connectivity because the switch acquires a new IP address when the management subnet is changed. To reconnect to the switch, you must determine the new IP address by viewing the log on the DHCP server.

Examples

```
(Switch)#network mgmt_vlan 100
```

network parms

This command manually configures the IPv4 address, subnet mask and gateway of the device management interface.

Syntax

network parms {*ipaddr netmask* [gateway] | none}

Mode

Privileged Exec

Parameters

These are the parameters:

- *ipaddr*: The IP address of the management interface.
- *netmask*: The subnet mask associated with the IP address.
- *gateway*: The IP address of the default gateway.
- none: Resets IP address and gateway on management interface.

Usage guidelines

The IP address and the gateway must be on the same subnet.

Examples

```
(Switch)#network parms 10.50.125.20 255.255.255.0 10.50.125.1
```

network protocol

This command specifies the network configuration protocol to be used. If you modify this value, change is effective immediately.

Syntax

network protocol {dhcp [client-id] | bootp | none}

Mode

Privileged Exec

Parameters

These are the parameters:

- dhcp: Periodically send requests to a DHCP server until a response is received.
- client-id: Enable the DHCP client to specify the unique client identifier (option 61).
- bootp: Periodically send requests to a BootP server until a response is received
- none: Configure the network information for the switch manually.

Examples

```
(Switch)#network protocol dhcp client-id
```

ping

Use this command to determine whether another computer is on the network.

Syntax

ping {*address*| *hostname*} [count *count*] [interval 1-60] [size *size*] [source *address*| *if-number* | vlan 1-4093 | network}] [outgoing-interface {*if-number* | vlan 1-4093 | network}]

Mode

User

Privileged Exec

Parameter

These are the parameters.

- *address*: IPv4 or IPv6 address to ping.
- *hostname*: Ping the name of a host that resolves to an IPv4 address.
- count: The number of ping packets (ICMP Echo requests) that are sent to the destination address or hostname. The range is 1 to 15 requests. The default count is 3.
- size: The size, in bytes, of the payload of the Echo Requests sent. The range is 0 to 13000 bytes. The default size is 0 bytes.
- source: The source to use when sending the Echo requests packets:
  - *address*: IP or IPv6 address
  - *if-number*: The interface number.
  - vlan: The ID of the VLAN to use as the source. The range is 1 to 4093.
  - network: The network port on the switch.

- interval: The interval between Echo Request. The range is 1 to 60 seconds. The default interval is 3 seconds.
- outgoing-interface: The outgoing interface for multicast pings.

Usage guidelines

Ping provides a synchronous response when initiated from the CLI.

If you ping an IPv6 address and use the `source` keyword, the source options are an IPv6 address or `network` only. Similarly, if you ping an IPv6 address and use the `outgoing-interface` keyword, `network` is the only option.

To terminate a ping operation, press **Ctrl + C**.

Examples

Ping an IPv4 address (success_

```
(Routing) #ping 10.254.2.160 count 3 interval 1 size 255
Pinging 10.254.2.160 with 255 bytes of data:

Received response for icmp_seq = 0. time = 275268 usec
Received response for icmp_seq = 1. time = 274009 usec
Received response for icmp_seq = 2. time = 279459 usec

----10.254.2.160 PING statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms) min/avg/max = 274/279/276
```

Ping an IPv6 address (success)

```
(Routing) #ping 2001::1
 Pinging 2001::1 with 64 bytes of data:

Send count=3, Receive count=3 from 2001::1
Average round trip time = 3.00 ms
```

IPv4 ping failure (destination unreachable)

```
(Routing) # ping 192.168.254.222 count 3 interval 1 size 255
Pinging 192.168.254.222 with 255 bytes of data:
Received Response: Unreachable Destination
Received Response :Unreachable Destination
Received Response :Unreachable Destination
----192.168.254.222  PING statistics----
3 packets transmitted,3 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
```

IPv4 ping failure (request timed out)

```
(Routing) # ping 1.1.1.1 count 1 interval 3
Pinging 1.1.1.1 with 0 bytes of data:

----1.1.1.1 PING statistics----
1 packets transmitted,0 packets received, 100% packet loss
round-trip (ms) min/avg/max = 0/0/0
```

ping ipv6

Use this command to determine whether another system with an IPv6 or link-local IPv6 address is on the network.

Syntax

ping ipv6 {*ip6addr* | *hostname* | interface network *link-local-address*} [count *count*] [interval 1-60] [size *size*] [source {*ip6addr* | network}] [outgoing-interface network]

Mode

User

Privileged Exec

Parameter

These are the parameters.

- *address*: IPv4 or IPv6 address to ping.
- *hostname*: Ping the name of a host that resolves to an IPv6 address.
- interface *link-local-address*: Ping the specified link-local IPv6 address over an interface.
- count: The number of ping packets (ICMP Echo requests) that are sent to the destination address or hostname. The range is 1 to 15 requests. The default count is 3.
- interval: The interval between Echo Request. The range is 1 to 60 seconds. The default interval is 3 seconds.
- size: The size, in bytes, of the payload of the Echo Requests sent. The range is 0 to 13000 bytes. The default size is 0 bytes.
- source: The source to use when sending the Echo requests packets:
  - *ip6addr*: IPv6 address
  - network: The network port on the switch.
- outgoing-interface network: The outgoing interface for multicast pings, which is the network interface.

Usage guidelines

To terminate a ping operation, press **Ctrl + C**.

Examples

IPv6 ping success

```
(Routing) #ping ipv6 2001::1
 Pinging 2001::1 with 64 bytes of data:

Send count=3, Receive count=3 from 2001::1
Average round trip time = 3.00 ms
```

IPv4 ping failure (destination unreachable)

```
(Routing) # ping 192.168.254.222 count 3 interval 1 size 255
Pinging 192.168.254.222 with 255 bytes of data:
Received Response: Unreachable Destination
Received Response :Unreachable Destination
Received Response :Unreachable Destination
----192.168.254.222  PING statistics----
3 packets transmitted,3 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
```

IPv6 ping failure

```
(Routing) #ping ipv6 2001::4
```

```
 Pinging 2001::4 with 64 bytes of data:

Send count=3, Receive count=0 from 2001::4
Average round trip time = 0.00 ms
```

release dhcp

Use this command to force the DHCPv4 client to release the leased address from the specified interface.

Syntax

release dhcp {*interface* | vlan *vlan-id*}

Mode

Privileged Exec

Parameters

These are the parameters:

- *interface*: The number of the port with a DHCP-assigned IP address to release.
- vlan *vlan-id*: The VLAN ID of the VLAN with a DHCP-assigned IP address to release.

Usage guidelines

To successfully execute the command, the specified port or VLAN must have routing enabled and the IP address configuration method must be DHCP.

After issuing the command, the DHCP client sends a DHCP Release message telling the DHCP server that it no longer needs the IP address, and that the IP address can be reassigned to another interface.

Examples

```
(Switch)#release dhcp 5

Error! Routing is not enabled on this interface.

(Switch)#release dhcp 2
```

reload

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes.

Syntax

reload [configuration [*scriptname*]]

Mode

Privileged Exec

Parameters

These are the parameters:

- configuration: Gracefully reloads the configuration. If no configuration file is specified, the startup-config file is loaded.
- *scriptname*: The configuration file to load. The scriptname must include the extension.

Usage guidelines

The switch uses the stored configuration to initialize the switch. If the switch has unsaved changes, you are prompted to confirm whether to save the changes. You are also prompted to confirm that the reset should proceed with the reset.

Examples

```
(dhcp-10-52-131-173)#reload

The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully.


Configuration Saved!
Are you sure you would like to reset the system? (y/n)
```

renew dhcp

Use this command to force the DHCPv4 client to immediately renew an IPv4 address lease on the specified interface.

Syntax

renew dhcp {*interface* | vlan *vlan-id* | network}

Mode

Privileged Exec

Parameters

These are the parameters:

- *interface*: The number of the port with a DHCP-assigned IP address to renew.
- vlan *vlan-id*: The VLAN ID of the VLAN with a DHCP-assigned IP address to renew.
- network-port: Renew the DHCP-assigned IP address on the management port.

Usage guidelines

To successfully execute the command, the specified port or VLAN must have routing enabled and the IP address configuration method must be DHCP.

After issuing the command, the DHCP client sends a DHCP Release message telling the DHCP server that it no longer needs the IP address, and that the IP address can be reassigned to another interface.

Examples

```
(Switch)#release dhcp 5

Error! Interface does not have a DHCP originated address

(Switch)#renew dhcp 2
```

script

Use this command to manage configuration scripts on the switch.

Syntax

script {apply *scriptname* |delete {*scriptname* | all} | list | show *scriptname* | validate *scriptname*}

Mode

Privileged Exec

Parameters

These are the parameters:

- apply: Applies the commands in the script to the switch.
- delete: Deletes the specified script or all scripts on the switch.
- list: Lists all scripts present on the switch as well as the remaining available space.
- show: Displays the contents of the specified script file.
- validate: Validates a script file by parsing each line in the script file.
  The validate option is intended to be used as a tool for script development. Validation identifies potential problems. It might not identify all problems with a given script on any given device.
- *scriptname*: The name of the script to apply, delete, show, or validate.

Usage guidelines

Configuration Scripting allows you to generate text-formatted script files representing the current configuration of a system. You can upload these configuration script files to a PC or UNIX system and edit them. Then, you can download the edited files to the switch and apply the new configuration. You can apply configuration scripts to one or more switches with no or minor modifications.

Use the `show running-config` command to capture the running configuration into a script. Use the `copy` command to transfer the configuration script to or from the switch.

You should use scripts on systems with default configuration; however, you are not prevented from applying scripts on systems with non-default configurations.

Scripts must conform to the following rules:

- The file extension must be `.scr`.
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch shall not exceed 2048 KB.
- The maximum number of configuration file command lines is 2000.

You can type single-line annotations at the command prompt to use when you write test or configuration scripts to improve script readability. The exclamation point (!) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line, and all input following this character is ignored. Any command line that begins with the “!” character is recognized as a comment line and ignored by the parser.

The following lines show an example of a script:

```
! Script file for displaying management access

show telnet !Displays the information about remote connections

! Display information about direct connections

show serial

! End of the script file!
```

Examples

```
(Switch)#script list

Configuration Script Name        Size(Bytes)  Date of Modification(UTC)
-------------------------------  -----------  -------------------------
backup-config2.scr                       527   2026 04 15 21:40:46
lab-system.scr                           766   2026 04 15 21:35:02
lab-system2.scr                         1494   2026 04 15 21:36:16

3 configuration script(s) found.
2045 Kbytes free.
(Switch)#script apply backup-config2.scr

Are you sure you want to apply the configuration script? (y/n) y


The system has unsaved changes.
Would you like to save them now? (y/n) y


Config file 'startup-config' created successfully.
Configuration Saved!

<script contents>

Configuration script 'backup-config2.scr' applied.
```

set clibanner

Use this command to configure the prelogin CLI banner that displays before the login prompt.

Syntax

set clibanner *line*

Mode

Global Config

Parameters

The *line* parameter is the banner text where “” (double quote) is a delimiting character. The banner message can be up to 2000 characters.

Examples

```
(Switch)(Config)#set clibanner "++++++++++++++++++++++++++++++++++++++++++++++++++
+ This is the HPE Networking Instant On Switch    +
+ 24p Gigabit CL4 PoE 4p SFP+ 240W 1940           +
+ Please use caution when executing CLI commands. +
++++++++++++++++++++++++++++++++++++++++++++++++++"

(Switch)(Config)#
```

show backup-config

This command displays the content of text-based backup configuration file.

Syntax

show backup-config

Mode

Privileged Exec

Usage guidelines

The text-based configuration files (startup-config, backup-config, and factory-defaults) are saved compressed in flash. With this command, the files are decompressed while displaying their content.

Example

```
(Switch)#show backup-config

!Current Configuration:
!
!System Description "HPE Networking Instant On Switch 40p Gigabit CL4 8p SR2.5G CL6 PoE 4p SFP+ 600W
1940 S4A35A, F.6.29.1, 1.0.0.9"
!System Software Version "3.4.0.7"
!System Up Time          "16 days 3 hrs 34 mins 33 secs"
!Additional Packages     HPE QOS,HPE IPv6 Management
!Current System Time: Apr 15 10:12:00 2026
!
hostname "Switch"
network protocol dhcp
vlan database
vlan 777
exit
network mgmt_vlan 777
configure
dhcp client vendor-id-option-string "HPE Networking Instant On Switch 8p SR10 4p CL6 PoE 2p SFP+
120W 1940"
cloud-managed
no enable
exit
no logging console
username "admin" password
61649b8e2663441db045cb860439b973e5002167594d2e17a2f406579a1e2e65449eca8f677b5564db814ab5293f2458c1
2caecdc7f011c49d427335310f9a0f encryption-type aes level 15 encrypted
line console
serial timeout 60
exit
line telnet
exit
line ssh
exit
snmp-server sysname "dhcp-10-52-131-173"
!
interface 48
vlan pvid 777
vlan participation exclude 1
vlan participation include 777
exit
exit
```

show bootvar

This command displays the version information and the activation status for the current active and backup images on the switch. The command also displays any text description associated with an image.

Syntax

show bootvar

Mode

Privileged Exec

Examples

```
(Switch)#show bootvar

Image Descriptions

 active :
 backup :


 Images currently available on Flash

 ----  ------------  ------------  -----------------  -----------------
 unit        active        backup     current-active        next-active
 ----  ------------  ------------  -----------------  -----------------

    1    4.13.15.33       3.4.0.7         4.13.15.33         4.13.15.33
```

show clibanner

Use this command to display the configured prelogin CLI banner. The prelogin banner is the text that displays before displaying the CLI prompt.

Syntax

show clibanner

Mode

Privileged Exec

Examples

```
(Switch)#show clibanner

Banner Message configured :
=========================

++++++++++++++++++++++++++++++++++++++++++++++++++++
+ This is the HPE Networking Instant On Switch    +
+ 24p Gigabit CL4 PoE 4p SFP+ 240W 1940           +
+ Please use caution when executing CLI commands. +
++++++++++++++++++++++++++++++++++++++++++++++++++++
```

show clock

Use this command to display the time and date from the system clock.

Syntax

show clock

Mode

Privileged Exec

Examples

```
(Switch)#show clock

21:00:27 AB(UTC-1:02) Apr 15 2026
Time source is Local
```

show crypto certificate

Use this command to display the root-ca-certificate downloaded on the switch or the SSL certificates present on the switch.

Syntax

show crypto certificate {all | mycertificate [1-2]}

Mode

Privileged Exec

Parameters

These are the parameters:

- all: Display the root-ca-certificate.
- mycertificate: Display the SSL certificates on the switch.
- 1-2: Specify the SSL certificate instance.

Examples

```
(Switch)#show crypto certificate all

Root CA Certificate
Storage: nvram:ca_certs.pem
-----BEGIN CERTIFICATE-----
MIID+zCCAmOgAwIBAgIMY4CqkSlO9X3LTPA3MA0GCSqGSIb3DQEBCwUAMBkxFzAV
BgNVBAMTDkxEQVAgU2VydmVyIENBMB4XDTIyMTEyNTExNDQxN1oXDTIzMTEyNTEx
NDQxN1owGTEXMBUGA1UEAxMOTERBUCBTZXJ2ZXIgQ0EwggGiMA0GCSqGSIb3DQEB
AQUAA4IBjwAwggGKAoIBgQDGejUT5V32M6wMyy4XowLTmM95fT9JNW3uFXbsu0zA
goFk3B/3q8LN7JbyQRZlVIeKemuLwH59SVjN2OYe29Fv9VhEbeaP3vOHIvqP8nf+
J6bVTodNH+gK3NTwwdE3kqQJpBCnMgAIiWdBXErwPmEdRN4WAdTAujoQLI3t/Qzx
Gpu1PNsomjJn7EXs8aIaIPN5mwvL+dwtvUwA4Urd11nr+7orZ1vkeH5qzDp5GzeB
yYmorOAWGM3nHaP+AM//0Jx8xQJRe1Cun7GfFJchEVxMxNGqBLC9oYItNReKsKkn
yWRifQ1RibEzmrnomWVZSE5svnYF6GC/Sezg0GkZamgM4DZ/I0fMealtpSyi8S0p
LwfJF/bagFDquPbKANfW4mXq1SpXcxhPgtRoYUXqZgdmKg8TWx8EsNDJ+TNaaMxp
7R3eERBXklt6LVy1AxrItTL7wFJEroq1VigKpVHnsN5AF1X29H0dhxVV56E51aaR
Th7mWh+oux87BP4jDW2ApdkCAwEAAaNDMEEwDwYDVR0TAQH/BAUwAwEB/zAPBgNV
HQ8BAf8EBQMDBwQAMB0GA1UdDgQWBBQbARsw6CqSAH4APL6rRYsx+JSOMjANBgkq
hkiG9w0BAQsFAAOCAYEAJlUaMqURWQp8CbEKkcYeI3jJbxAvFJrB//9YLq838xeD
vnGidioJo/cCOjBQ8ykjjAur817MO1rJesUhA8u/3lFzXkCB1/zbxx9QQXTN7RKQ
```

```
6mmRIUkSWwf9nmAtol8SZ9Nb3+HaPUQLGy1b5OEruLWwUTOOGEqVh2RNrDal1W+G
d42+iXiZkTo/R8sOjlHSWbHqk7iaVV7l2iD3nSqJqu4hLgsF4Lzx/9Eel022lVS1
QPCbN1xVkBdNBXoweSBgtI4v5+TI9JFUSU5kJ5rEx1iH5zExFxqD7b0d9m08swsU
EKMLYjHF1vGkhEzbhLRCrayt1lgKfGvdA2Hw8WBWZmKlOx3OaTDcR+icl8Wm3UHL
VzTTq/3rTuY2fF1SDU9inDwseVMwtYCGFDWLiNWYoyCJ01sGU8NeYv79UJ+xZv2a
rSluB3nVmFG7P1hcx910BwkIv746Ox39LXDBV7ZgkCULGw1HPKshOCEWPB7qcpaZ
9sJHksAHZbgOAcVx9ubx
-----END CERTIFICATE-----
Issued by: LDAP Server CA
Valid from Nov 25 11:44:17 2022 GMT to Nov 25 11:44:17 2023 GMT
Subject: /CN=LDAP Server CA
Fingerprint: 786AF58AEDB04A750DF1154933812D0E

(Switch)#show crypto certificate mycertificate 1

-----BEGIN CERTIFICATE-----
MIICxjCCAa6gAwIBAgIJAI6dX/uCWOQcMA0GCSqGSIb3DQEBCwUAMBYxFDASBgNV
BAMMCzE5Mi4xNjguMS4xMB4XDTcwMDEwMTAwMDA1M1oXDTcxMDEwMTAwMDA1M1ow
FjEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDIxnCr5jLnuiarGcjDpxnB5r5tCjZCEKJu7fAWa1CWQYr3LhDKYwBy
Nx9xXxNHa0syUOP1SZPyEsMqnXD5gmFKkF4we2RaE7Of+SgaCy9PT/Iye5Wet/uk
TnEKWA1hsxcyQYJijEoUlCYvoPEirdiVw8nCZWDq48RmPuQg6x6N5VaitDVFLuGg
m4QPprdzbnblVr135eKkjhAxVEQpKpAsPxyTpHhEiYLDIQhk2sqW18suP7uT1QPS
L6dGnnlgNThJNPPPK4Yth3xgI5gvHtH1vYV2E0WabM5/wMIXPPbqokh674hqFQNt
y54syNR6bWcsxDGfKn+isE1h0hwO04zTAgMBAAGjFzAVMBMGA1UdJQQMMAoGCCsG
AQUFBwMBMA0GCSqGSIb3DQEBCwUAA4IBAQCixhA22PE1JCrzPkMs9behtnpSco1c
bp75tRnVNxJc0Cuh8OL3KSF8Azq+rgoTqWaa07x4neJ+R/LLmDdpDDKHrMYcByUC
K1Gyg/KIcWCdkM3appQlGF0gjOnoCY/huDK3MxHE4IHVzBA8y79x+MjFAnig/vkA
9ZUPXBA4lf3SMDcZFol0yoF9oKQ7Ekz4zA6DCdp8i9VvDvcVL5Z1NwvMTDNTrx6i
A83Um0UxB/F7PIiHVyDwvtHm8yjyytAUSP3wItiw0nFA942tRKaRAC9qqXCrrFEJ
Y8o5y349F9muDKfoKlAprGVFWxkCqc40vl6o/QUHLCYJakcDBiP1N2qG
-----END CERTIFICATE-----
Issued by: 192.168.1.1
Valid from Jan  1 00:00:53 1970 GMT to Jan  1 00:00:53 1971 GMT
Subject: /CN=192.168.1.1
Fingerprint: CA5B5A2E915B3E8252CFEB951ECA0291
```

show crypto dhparam

Use this command to display the Diffie Hellman parameter size used by the SSL tunnel.

Syntax

show crypto dhparam

Mode

Privileged Exec

Examples

```
(Switch)#show crypto dhparam

DH param size.................................. 2048
DH Parameter generation status................. Completed
```

show crypto key

Use this command to display the SSH public keys on the device or the client's public keys stored on the switch.

Syntax

show crypto key {mypubkey [{ecdsa | rsa}] | pubkey-chain ssh [username *user-name*] [finger-print {bubble-babble | hex}]}

Mode

Privileged Exec

Parameters

These are the parameters:

- mypubkey: Display the SSH public keys of the device.
  - ecdsa: Display the ECDSA key.
  - rsa: Display the RSA key.
- pubkey-chain ssh: Display the SSH client public keys.
  - username *user-name*: Display SSH public key for the given user.
  - finger-print: Display SSH user public key fingerprint.
    - bubble-babble: Show the data in bubble babble encoding.
    - hex: Show the data in hex encoding.

Examples

```
(Switch)#show crypto key mypubkey

RSA Key Data:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQD1xWi3s2eakSEsmMDoRIF748Q7pChNctFsSJOaD7esTIgGHhfFL3i2EPn9VOh2A+8tFg
2kXaiIzqWzy9kTbhmcn/tCtRyBkvmpLve2z+AKwdHQxO0ZzdLjtTv4/c4XTE4F6jg/
LBKdhFb4+qGr6PekbGbuMpp4rvJF76r8wXXlsw==
 Fingerprint (Hex):  MD5:ad:bb:2b:dd:c0:4b:8e:bc:f1:99:35:05:25:00:d5:cd
 Fingerprint (Bubble Babble):  xicag-duvek-fulir-lelab-sumyk-selar-suzys-fopum-cavis-gebyh-coxax

DSA Key Data:
ssh-dss AAAAB3NzaC1kc3MAAACBANrQifFkVewhGrGtOM8tzm1gig7vdp3zRY81jIiQF8ukS8x2f/
WDPAu1aZa+wf8pmt0y+nAv9rPmYTDnM0Ife8X+uu669xd15+FWkrSqe8B6c1NXVDJxDqJIgqOuNjxBj5W+hzwvQODTndVJm9L2
3hi+0zxt0DcWfvFVJILFNhjHAAAAFQC00qsPDniPrEn7wNUZH2r2mwGohwAAAIBECr5kreyIwwVBXq05yuSc+khzQ5aDdHBaEK
k4RIqgqXvPUMzyaH/
nR84TOX1syUcP5lxK1noo5ayVwUZKp9Gf43NC1KQmq4cI30VsNswvwn6tvm6+Brsw+DA2KcOxgeGjCZTEZOZXzsqD+OSndE5lo
6GBKQdA577NFoo3SzmffwAAAIEA04qsYl2WD1NBf86Ga7kX1EZYPVyNo8tmz3tk899P4VoZFRDw9BzrC/
j723Vdl27j0u8oddJKwliXWFSi4nbWg5NdiaSXtBH5v0nzs3GK59QIirXAJp3ZKMaTzn26PT1emLpw9zxwDpjRLmtpUIKG464K
ZQwIzSjhcWDJAgDmyVU=
 Fingerprint (Hex):  MD5:50:4e:c7:aa:ff:41:48:0f:f1:f6:46:4a:1e:db:e2:a7
 Fingerprint (Bubble Babble):  xomal-radyc-rebid-hodid-gelos-pekyn-voduz-cidom-damen-mogeb-hoxox
```

show error

Display error statistics.

Syntax

show error

Mode

Privileged Exec

Examples

```
(Switch)#show error

--------------------------------------------------------------------------------
 ports    Packets Without     Packets With        Packets             FCS
              Errors            Errors           Discarded          Errors
-------- ----------------- ----------------- ----------------- -----------------
            Tx       Rx       Tx       Rx       Tx       Rx       Tx       Rx
          -------- -------- -------- -------- -------- -------- -------- --------

1         0        0        0        0        0        0        0        0
2         0        0        0        0        0        0        0        0
3         0        0        0        0        0        0        0        0
4         0        0        0        0        0        0        0        0
5         293.1k   6.6k     0        0        0        0        0        0
6         0        0        0        0        0        0        0        0
7         0        0        0        0        0        0        0        0
8         0        0        0        0        0        0        0        0
9         0        0        0        0        0        0        0        0
10        0        0        0        0        0        0        0        0
11        0        0        0        0        0        0        0        0
12        0        0        0        0        0        0        0        0
13        0        0        0        0        0        0        0        0
14        0        0        0        0        0        0        0        0
15        0        0        0        0        0        0        0        0
```

show interface

This command displays a summary of statistics for a specific interface or a count of all CPU traffic based upon the argument.

Syntax

show interface {*port-num* | all | lag *lag-id* }

Mode

Privileged Exec

Parameters

These are the parameters:

- *port-num*: Display summary information for the specified port.
- all: Display summary information for all interfaces.
- lag *lag-id*: Display summary information for the specified LAG identifier.

Examples

```
(Switch)#show interface 5

Interface :................................ 5

Packets Received Without Error.................. 6665
Packets Received With Error..................... 0
Broadcast Packets Received...................... 0
Receive Packets Discarded....................... 0
Packets Transmitted Without Errors.............. 293612
Transmit Packets Discarded...................... 0
Transmit Packet Errors.......................... 0
Collision Frames................................ 0
Number of link down events...................... 0
Time Since Counters Last Cleared................ 2 day 7 hr 31 min 12 sec
```

show interface counters

This command displays a short summary of the statistics for all interfaces.

Syntax

show interface counters

Mode

Privileged Exec

Examples

```
(Switch)#show interface counters

Port              InOctets      InUcastPkts      InMcastPkts      InBcastPkts       InDropPkts        Rx Error
--------- ---------------- ---------------- ---------------- ---------------- ---------------- ---------------
1                        0                0                0                0                0               0
2                        0                0                0                0                0               0
3                        0                0                0                0                0               0
4                        0                0                0                0                0               0
5                  1551839                0             6664                0                0               0
6                        0                0                0                0                0               0
7                        0                0                0                0                0               0
8                        0                0                0                0                0               0
9                        0                0                0                0                0               0
10                       0                0                0                0                0               0
11                       0                0                0                0                0               0
12                       0                0                0                0                0               0
13                       0                0                0                0                0               0
14                       0                0                0                0                0               0
15                       0                0                0                0                0               0
16                       0                0                0                0                0               0
17                       0                0                0                0                0               0
18                       0                0                0                0                0               0
19                       0                0                0                0                0               0
20                26569670               98           266579            26880           186979               0
```

show interface ethernet

This command displays detailed statistics for a specific interface or for all CPU traffic based upon the argument.

Syntax

show interface ethernet {*port-num* | all | lag *lag-id* | switchport}

Mode

Privileged Exec

Parameters

These are the parameters:

- *port-num*: Display detailed information for the specified port.
- all: Display detailed information for all interfaces.
- lag *lag-id*: Display detailed information for the specified LAG identifier.
- switchport: Display detailed information for the management interface.

Examples

```
(Switch)#show interface ethernet switchport

Total Packets Received (Octets)..............  36611965
Packets Received Without Error...............  373349
Unicast Packets Received.....................  72691
Multicast Packets Received...................  273741
Broadcast Packets Received...................  26917
Receive Packets Discarded....................  0

Octets Transmitted...........................  150221462
Packets Transmitted Without Errors...........  338563
Unicast Packets Transmitted..................  118298
Multicast Packets Transmitted................  220253
Broadcast Packets Transmitted................  12
Transmit Packets Discarded...................  0

Packets forwarded by cpu.....................  0
IP Packets received without errors...........  484348

Most Address Entries Ever Used...............  9
Address Entries Currently in Use.............  7

Maximum VLAN Entries.........................  255
Most VLAN Entries Ever Used..................  2
Static VLAN Entries..........................  2
Dynamic VLAN Entries.........................  0
VLAN Deletes.................................  0
Time Since Counters Last Cleared.............  2 day 7 hr 36 min 41 sec
```

show ip address-conflict

This command displays the status information corresponding to the last detected address conflict.

Syntax

show ip address-conflict

Mode

Privileged Exec

Examples

```
(Switch)#show ip address-conflict

Address Conflict Detection Status.............  No Conflict Detected
```

show ip http

This command displays the HTTP settings for the switch.

Syntax

show ip http

Mode

Privileged Exec

Examples

```
(Switch)#show ip http

HTTP Mode (Unsecure)........................... Enabled
HTTP Port...................................... 80
Maximum Allowable HTTP Sessions................ 5
HTTP Session Hard Timeout...................... 100 hours
HTTP Session Soft Timeout...................... 60 minutes

HTTP Mode (Secure)............................. Enabled
HTTP Operational Mode (Secure)................. Enabled
Secure Port.................................... 443
Secure Protocol Level(s)....................... TLS1.2 TLS1.3
Maximum Allowable HTTPS Sessions............... 5
HTTPS session hard timeout..................... 24 hours
HTTPS session soft timeout..................... 10 minutes
Certificate Present............................ 1
User Selected Certificate...................... 1
Active Certificate............................. 1
Expired Certificate............................ Not Applicable (No NTP time source)
Certificate Generation In Progress............. None
DH Key Exchange................................ Enabled
Server Ciphersuite............................. aes-128-cbc-sha
                                                aes-256-cbc-sha
                                                dhe-aes-128-cbc-sha
                                                dhe-aes-cbc-sha2
                                                dhe-aes-gcm-sha2
                                                ecdhe-rsa-aes-cbc-sha2
                                                ecdhe-rsa-aes-gcm-sha2
                                                rsa-aes-cbc-sha2
                                                rsa-aes-gcm-sha2
                                                aes128-gcm-sha256
                                                aes256-gcm-sha384
                                                chacha20-poly1305-sha256
```

show ip ssh

This command displays the SSH settings for the switch.

Syntax

show ip ssh

Mode

Privileged Exec

Examples

```
(Switch)#show ip ssh

SSH Configuration

Administrative Mode: ......................... Enabled
Operational Mode:............................. Enabled
SSH Port: .................................... 22
Protocol Level: .............................. Version 2
SSH Sessions Currently Active: ............... 1
Max SSH Sessions Allowed: .................... 5
SSH Timeout (mins): .......................... 5
Keys Present: ................................ RSA(1024)

Key Generation In Progress: .................. None
SSH Public Key Authentication Mode: .......... Disabled
SCP server Administrative Mode: .............. Enabled
Max SSH authentication tries:................. 4
Encryption Algorithms:........................ aes128-ctr
                                               aes192-ctr
                                               aes256-ctr
                                               chacha20-poly1305@openssh.com
                                               aes128-gcm@openssh.com
                                               aes256-gcm@openssh.com

MAC Algorithms:............................... hmac-sha2-256
                                               hmac-sha2-512
                                               hmac-sha2-256-etm@openssh.com
                                               hmac-sha2-512-etm@openssh.com

KEX Algorithms:............................... curve25519-sha256
                                               curve25519-sha256@libssh.org
                                               ecdh-sha2-nistp256
                                               ecdh-sha2-nistp384
                                               ecdh-sha2-nistp521
                                               sntrup761x25519-sha512@openssh.com
                                               sntrup761x25519-sha512
                                               mlkem768x25519-sha256

HostKey Algorithms:........................... rsa-sha2-256
                                               rsa-sha2-512
                                               ecdsa-sha2-nistp256
                                               ecdsa-sha2-nistp384
                                               ecdsa-sha2-nistp521
```

show ip vlan

This command displays summary information about routing VLANs configured on the switch.

Syntax

show ip vlan

Mode

Privileged Exec

Examples

```
(Switch)#show ip vlan
```

```
MAC Address used by Routing VLANs:   34:C5:15:41:41:A2

           Logical
VLAN ID   Interface        IP Address       Subnet Mask
-------  -------------  ---------------   ---------------
100      VLAN-100        192.168.10.100    255.255.255.0
```

show logging

This command displays information about log files

Syntax

show logging [{buffered {[start *time date*] [end *time date*]} | email {config | statistics} | hosts | persistent {[start *time date*] [end *time date*]} [log-files | previous] | traplogs}]

Mode

Privileged Exec

Parameters

These are the parameters:

- buffered: Display log messages stored locally on the switch in the RAM (cache)
  - start *time date*: Display log messages timestamped after the specified time and date.
  - end *time date*: Display log messages timestamped before the specified time and date.
- email: View email alert information.
  - config: Display information about the email alert configuration.
  - statistics: Display the email alert statistics.
- hosts: Display information about remote SYSLOG server settings.
- persistent: Display messages stored in the flash Log file that are available for viewing even after system reboot.
  - start *time date*: Display log messages timestamped after the specified time and date.
  - end *time date*: Display log messages timestamped before the specified time and date.
  - log-files: Display the list of persistent log files existing in the system.
  - previous: Display persistent log entries from the last reboot.
- traplogs: Display traplog information.

Usage guidelines

When specifying a start or end time, the time is expressed in a 24-hour clock, in the form of hours:minutes. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.

The start and end dates are expressed in the format day month year. For example, 15 Apr 2026 is April 15, 2026. If the end time is not specified, the current time is used.

Examples

```
(Switch)#show logging

Logging Client Local Port           : 514
Logging Client Source Interface     : (not configured)
CLI Command Logging                 : disabled
Logging protocol                    : 0
Console Logging                     : disabled
Console Logging Severity Filter     : error
Buffered Logging                    : enabled
Buffered Logging Severity Filter    : info
Buffered Logging Threshold (%)      : 80
```

```
Persistent Logging                  : enabled
Persistent Logging Severity Filter  : error

Syslog Logging                      : disabled
Syslog Logging Facility             : local7

Duplicate Log Suppression Mode      : disabled
Duplicate Log Suppression Interval  : 300

Log Messages Received               : 1890
Log Messages Dropped                : 0
Log Messages Relayed                : 0

USB Logging Mode                    : overwrite-on-full
USB Logging Severity                : notice
USB Logging Operational Status      : Inactive

(Switch)#show logging buffered

Buffered (In-Memory) Logging        : enabled
Buffered Logging Wrapping Behavior  : On
Buffered Log Count                  : 750
Buffered Log Threshold (lines)      : 160

<190>Apr 15 22:48:29 switch-name USER_MGR[UtilTask]: user_mgr.c(7411) 1890 %% INFO Cleaned OpenSSH
stale child processes.
<189>Apr 15 22:47:08 switch-name SSHD[tRpcsrv.02002]: sftp-server.c(921) 1888 %% NOTE SFTP remote
file download operation is unsuccessful.
<190>Apr 15 22:47:05 switch-name USER_MGR[emWeb]: user_mgr.c(1875) 1887 %% INFO User 'admin' trying
to authenticate with authentication method: ENABLE.
<190>Apr 15 22:47:05 switch-name USER_MGR[tRpcsrv.01001]: user_mgr.c(1875) 1886 %% INFO User 'admin'
trying to authenticate with authentication method: LOCAL.
<189>Apr 15 22:47:03 switch-name TRAPMGR[trapTask]: traputil.c(853) 1885 %% NOTE Session 0 of type
3 started for user admin connected from 10.230.89.94.
<190>Apr 15 22:47:02 switch-name USER_MGR[tRpcsrv.01001]: user_mgr.c(1875) 1883 %% INFO User 'admin'
trying to authenticate with authentication method: LOCAL.
<190>Apr 15 22:25:27 switch-name USER_MGR[tRpcsrv.00001]: user_mgr_util.c(1648) 1882 %% INFO HTTP
Session 12 started for user admin connected from 10.230.89.94
<190>Apr 15 22:25:27 switch-name USER_MGR[tRpcsrv.00001]: user_mgr.c(1875) 1881 %% INFO User 'admin'
trying to authenticate with authentication method: LOCAL.
<189>Apr 15 22:22:16 switch-name TRAPMGR[trapTask]: traputil.c(853) 1880 %% NOTE Session 0 of type
3 ended for user admin connected from 10.230.89.94.
<190>Apr 15 22:22:16 switch-name CLI_WEB[UtilTask]: login_sessions.c(188) 1879 %% INFO SSH Session
0 ended for user admin connected from 10.230.89.94
<190>Apr 15 22:12:47 switch-name USER_MGR[tUISM]: user_mgr_util.c(1699) 1878 %% INFO HTTP Session
11 ended for user admin connected from 10.230.89.94


(Switch)#show logging traplogs

Number of Traps Since Last Reset.............. 136
Trap Log Capacity............................. 256
Number of Traps Since Log Last Viewed......... 1

Log System Up Time           Trap
--- ------------------------ ------------------------------------------------
  0 Apr 15 22:47:03 2026     Session 0 of type 3 started for user admin
                             connected from 10.230.89.94.
  1 Apr 15 22:22:16 2026     Session 0 of type 3 ended for user admin
                             connected from 10.230.89.94.
  2 Apr 15 21:59:49 2026     Session 0 of type 3 started for user admin
```

```
                          connected from 10.230.89.94.
  3 Apr 15 21:56:49 2026  Session 0 of type 3 ended for user admin
                          connected from 10.230.89.94.
  4 Apr 15 21:37:04 2026  Session 0 of type 3 started for user admin
                          connected from 10.230.89.94.
  5 Apr 15 21:26:06 2026  Session 0 of type 2 ended for user admin
                          connected from 10.52.133.225.
  6 Apr 15 21:26:03 2026  Session 0 of type 2 started for user admin
                          connected from 10.52.133.225.
  7 Apr 15 21:26:00 2026  Telnet session : Login to the switch is not
                          successful, User ID: admin Source IP:
```

show network

This command displays configuration settings associated with the switch's network interface.

Syntax

show network

Mode

Privileged Exec

User

Usage guidelines

The network interface is the logical interface used for in-band connectivity with the switch using 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. The network interface is always considered to be up, whether or not any member ports are up; therefore, the `show network` command will always show the interface status as up.

Example

```
(Switch)>show network

Interface Status.............................. Up
IP Address.................................... 10.52.131.170
Subnet Mask................................... 255.255.255.192
Default Gateway............................... 10.52.131.129
IPv6 Administrative Mode...................... Disabled
Burned In MAC Address......................... 34:C5:15:41:41:A0
Locally Administered MAC address.............. 00:00:00:00:00:00
MAC Address Type.............................. Burned In
Configured IPv4 Protocol...................... DHCP
Configured IPv6 Protocol...................... DHCP
DHCPv6 Client DUID............................
IPv6 AutoConfig Mode.......................... Enabled
Management VLAN ID............................ 1
```

show network ipv6

Use this command to display the information about the IPv6 neighbor entries cached on the network port or to view DHCPv6 client statistics.

Syntax

show network ipv6 {dhcp statistics | neighbors}

Mode

Privileged Exec

User

Example

```
(Switch)>show network ipv6 dhcp statistics

DHCPv6 Client Statistics
-----------------------------------------------
DHCPv6 Advertisement Packets Received..... 0
DHCPv6 Reply Packets Received................. 0
Received DHCPv6 Advertisement Packets Discard.. 0
Received DHCPv6 Reply Packets Discarded........ 0
DHCPv6 Malformed Packets Received.............. 0
Total DHCPv6 Packets Received................. 0
DHCPv6 Solicit Packets Transmitted............. 0
DHCPv6 Request Packets Transmitted............. 0
DHCPv6 Renew Packets Transmitted............... 0
DHCPv6 Rebind Packets Transmitted.............. 0
DHCPv6 Release Packets Transmitted............. 0
DHCPv6 Decline Packets Transmitted............. 0
DHCPv6 Confirm Packets Transmitted............. 0
Total DHCPv6 Packets Transmitted............... 0

(Switch) #show network ipv6 neighbors
                                                 Neighbor  Age
IPv6 Address             MAC Address       isRtr State    (Secs)      Type
------------------------ ----------------- ----- --------- ------     ------
FE80::5E26:AFF:FEBD:852C 5c:26:0a:bd:85:2c FALSE Reachable 0          Static
```

show port

This command displays port information.

Syntax

show port {*intf-range* | advertise [*port-number*] | all | description {*port-number* | lag *lag-id* | vlan *vlan-id*}

Mode

Privileged Exec

User

Parameters

These are the parameters:

- intf-range: The port or set of ports with the information to view. Use a comma for a list and hyphen for ranges.
- advertise: Show the auto negotiation advertisement information for the specified port.
- all: View summary information for all interfaces.
- description: Display interface description for the specified port, LAG, or VLAN routing interface.

Example

```
(Switch)#show port 5

                Admin     Physical   Physical   Link   Link    LACP   Flow
Intf      Type  Mode      Mode       Status     Status Trap    Mode   Mode
```

```
--------- ------ --------- ---------- ---------- ------ ------- ------ -------
5                Enable    Auto       1000 Full  Up     Enable  Enable Disable

(Switch)#show port description vlan 100

Interface....... VLAN-100
ifIndex......... 64
Description.....
MAC address..... 34:C5:15:41:41:A2
Bit Offset Val.. 64

(Switch)#show port advertise 5

Port: 5
Type: Gigabit - Level
Link State: Up
Auto Negotiation:Enabled
Clock:Auto

                                 10000f 1000f  1000h  100f   100h   10f    10h
                                 ------ ------ ------ ------ ------ ------ ------
Admin Local link Advertisement     no     yes    no     yes    yes    yes    yes
Oper Local link Advertisement      no     yes    no     yes    yes    yes    yes
Oper Peer Advertisement            no     yes    no     yes    yes    yes    yes
Priority Resolution                no     yes    no     no     no     no     no

(Switch)#show port advertise

 Intf     Type              Neg       Operational Link Advertisement
--------- ----------------  --------  -------------------------------------
1         Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
2         Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
3         Gigabit - Level   Disabled  -      -      -      -      -      -      -
4         Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
5         Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
6         Gigabit - Level   Disabled  -      -      -      -      -      -      -
7         Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
8         Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
9         Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
10        Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
11        Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
12        Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
13        Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
14        Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
15        Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
16        Gigabit - Level   Disabled  -      -      -      -      -      -      -
17        Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
18        Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
19        Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h
20        Gigabit - Level   Enabled   1000f, 100f, 100h, 10f, 10h

(Switch)#
```

show running-config

Use this command to display the current setting configured on the switch. This command displays commands with settings and configurations that differ from the default value.

Syntax

show running-config

Mode

Privileged Exec

Usage guidelines

Show running-config does not display the User Password, even if you set one different from the default.

The output is displayed in script format, which can be used to configure another switch with the same configuration.

If you issue the `show running-config` command from a serial connection, access to the switch through remote connections (such as Telnet) is suspended while the output is being generated and displayed.

If you use a text-based configuration file, the `show running-config` command only displays configured physical interfaces (that is, if any interface only contains the default configuration, that interface will be skipped from the show running-config command output). This is true for any configuration mode that contains nothing but default configuration. That is, the command to enter a particular config mode, followed immediately by its exit command, are both omitted from the `show running-config` command output (and hence from the startup-config file when the system configuration is saved.)

Use the following keys to navigate the command output.

- Key: Action
- Enter: Advance one line.
- Space Bar: Advance one page.
- q: Stop the output and return to the prompt.

Example

```
(Switch)#show running-config

!Current Configuration:
!
!System Description "HPE Networking Instant On Switch 24p Gigabit CL4 PoE 4p SFP+ 240W 1940,
4.13.15.33, 1.0.0.11"
!System Software Version "4.13.15.33"
!System Up Time          "2 days 11 hrs 53 mins 30 secs"
!Additional Packages     HPE QOS,HPE IPv6 Management,HPE Routing
!Current System Time: Apr 16 03:28:51 2026
!
hostname "dhcp-10-52-131-170"
network ipv6 address dhcp
network ipv6 address autoconfig
boot host autosave
boot host retrycount 2
snmp-server
vlan database
vlan 100
vlan routing 100 1
exit

ip http session hard-timeout 100
ip http session soft-timeout 60
```

```
ip telnet server enable
configure
dhcp client vendor-id-option-string "HPE Instant On;S4A31A;3.4.0.1;VN5ZMCW125"
clock timezone -1 minutes 2 zone "AB"
cloud-managed
no enable
exit
--More-- or (q)uit
```

show spanning-tree

This command displays spanning tree settings..

Syntax

show spanning-tree [{active | brief | summary}

Mode

Privileged Exec

User

Example

```
(Switch)#show spanning-tree

Bridge Priority.............................. 32768
Bridge Identifier............................ 80:00:34:C5:15:41:41:A0
Time Since Topology Change..................... 3 day 9 hr 39 min 33 sec
Topology Change Count........................ 1
Topology Change in progress.................. False
Designated Root.............................. 80:00:34:C5:15:41:41:A0
Root Path Cost............................... 0
Root Port Identifier......................... 00:00
Bridge Max Age............................... 20
Bridge Max Hops.............................. 20
Bridge Tx Hold Count......................... 6
Bridge Forwarding Delay...................... 15
Hello Time................................... 2
Bridge Hold Time............................. 6
CST Regional Root............................ 80:00:34:C5:15:41:41:A0
Regional Root Path Cost...................... 0

     Associated FIDs           Associated VLANs
     ---------------           ----------------
     1                         1
     20                        20
     25                        25
     30                        30
     31                        31
     32                        32
     33                        33
     34                        34
     35                        35
     100                       100
     200                       200

(Switch)#show spanning-tree active

Spanning Tree: Enabled    Portfast BPDU Filtering  : Disabled
Mode: rstp
```

```
CST Regional Root:        80:00:34:C5:15:41:41:A0
Regional Root Path Cost:  0


###### MST 0 Vlan Mapped:   1, 20, 25, 30-35, 100, 200
ROOT ID
              Priority        32768
              Address         34:C5:15:41:41:A0
              This Switch is the Root.
              Hello Time: 2s Max Age: 20s Forward Delay: 15s
Bridge ID
              Priority        32768
              Address         34:C5:15:41:41:A0
              Hello Time: 2s Max Age: 20s Forward Delay: 15s
Interfaces

Name      State    Prio.Nbr  Cost      Sts           Role  RestrictedPort
--------- -------- --------- --------- ------------- ----- --------------
5         Enabled  128.5     20000     Forwarding    Desg  No
20        Enabled  128.20    20000     Discarding    Bkup  No
23        Enabled  128.23    20000     Forwarding    Desg  No

(Switch)#show spanning-tree brief

Bridge Priority.............................. 32768
Bridge Identifier............................ 80:00:34:C5:15:41:41:A0
Bridge Max Age............................... 20
Bridge Max Hops.............................. 20
Bridge Hello Time............................ 2
Bridge Forward Delay......................... 15
Bridge Hold Time............................. 6

(Switch)#show spanning-tree summary

Spanning Tree Admin Mode.......... Enabled
Spanning Tree Version............. IEEE 802.1w
BPDU Guard Mode................... Disabled
BPDU Filter Mode.................. Disabled
Configuration Name................ 34-C5-15-41-41-A0
Configuration Revision Level...... 0
Configuration Digest Key.......... 0xac36177f50283cd4b83821d8ab26de62
Configuration Format Selector..... 0
No MST instances to display.
```

show spanning-tree interface

This command displays the settings and parameters for all interfaces, a specific switch port, or a specified LAG within the common and internal spanning tree.

Syntax

show spanning-tree interface {*port-num* | lag *lag-id* | all}

Mode

Privileged Exec

User

Example

```
(Switch)#show spanning-tree interface laG 1

Hello Time..................................... Not Configured
Port Mode...................................... Enabled
BPDU Guard Effect.............................. Disabled
Root Guard..................................... False
Loop Guard..................................... False
TCN Guard...................................... False
BPDU Filter Mode............................... Disabled
BPDU Flood Mode................................ Disabled
Auto Edge...................................... TRUE
Port Up Time Since Counters Last Cleared....... 3 day 9 hr 41 min 37 sec
STP BPDUs Transmitted.......................... 0
STP BPDUs Received............................. 0
RSTP BPDUs Transmitted......................... 0
RSTP BPDUs Received............................ 0
MSTP BPDUs Transmitted......................... 0
MSTP BPDUs Received............................ 0
SSTP BPDUs Transmitted......................... 0
SSTP BPDUs Received............................ 0
```

show spanning-tree mst detailed

This command displays the detailed settings for an MST instance or for all MST instances.

Syntax

show spanning-tree mst detailed {*mst-id* | all}

Mode

Privileged Exec

User

Example

```
(Switch)#show spanning-tree mst detailed all

MST Instance ID................................ 0
MST Bridge Priority............................ 32768
MST Bridge Identifier.......................... 80:00:34:C5:15:41:41:A0
Time Since Topology Change..................... 3 day 9 hr 43 min 21 sec
Topology Change Count.......................... 1
Topology Change in progress.................... False
Designated Root................................ 80:00:34:C5:15:41:41:A0
Root Path Cost................................. 0
Root Port Identifier........................... 00:00

     Associated FIDs           Associated VLANs
     ---------------           ----------------
     1                         1
     20                        20
     25                        25
     30                        30
     31                        31
     32                        32
     33                        33
     34                        34
     35                        35
```

```
100                         100
200                         200
```

show spanning-tree mst port

This command displays settings and parameters for a specific switch port within a particular multiple spanning tree instance.

Syntax

show spanning-tree mst port {detailed *mst-id* {*port-number* | lag *lag-id* } | summary *mst-id* {*port-number* | lag *lag-id* | active | all}}

Mode

Privileged Exec

User

Parameters

These are the parameters

- *mst-id*: A number that corresponds to the existing multiple spanning tree instance.
- *port-number*: The port with the MST information to view.
- lag *lag-id* : The LAG ID with the MST information to view.
- active: Display summary information for all active interfaces.
- all: Display summary information for all interfaces.

Example

```
(Switch)#show spanning-tree mst port detailed 0 5

Port Identifier.............................. 80:05
Port Priority................................ 128
Port Forwarding State........................ Forwarding
Port Role.................................... Designated
Auto-calculate Port Path Cost................ Enabled
Port Path Cost............................... 20000
Auto-Calculate External Port Path Cost....... Enabled
External Port Path Cost...................... 20000
Designated Root.............................. 80:00:34:C5:15:41:41:A0
Designated Port Cost......................... 0
Designated Bridge............................ 80:00:34:C5:15:41:41:A0
Designated Port Identifier................... 80:05
Topology Change Acknowledge.................. False
Hello Time................................... 2
Edge Port.................................... False
Edge Port Status............................. False
Point to Point MAC Status.................... TRUE
CST Regional Root............................ 80:00:34:C5:15:41:41:A0
CST Internal Root Path Cost.................. 0
Loop Inconsistent State...................... False
Transitions Into Loop Inconsistent State..... 0
Transitions Out Of Loop Inconsistent State..... 0

(Switch)#show spanning-tree mst port summary 0 active

            STP                  STP            Port
Interface   Mode   Type         State          Role       Desc
--------- -------- ------- ---------------- ---------- ----------
```

```
5          Enabled          Forwarding        Designated
20         Enabled          Discarding        Backup
23         Enabled          Forwarding        Designated
```

show spanning-tree root-history

Use the command with no optional parameters to display the root bridge changes in the topology for RSTP or STP.

Use the mst *mst-id* parameter to display settings for the specified MST instance.

Syntax

show spanning-tree root-history [{mst *mst-id* | all}]

Mode

Privileged Exec

User

Parameters

These are the parameters

- *mst-id*: Display the root bridge changes in the topology for a specific MST instance. This command displays root bridge changes for CIST when 0 is passed as MST identifier.
- mst all: Display the root bridge changes in the topology for all configured MST instances and the CIST.

Usage guidelines

A history of the root bridge changes in the network is maintained for STP, RSTP, and MSTP for a maximum of 32 root bridge changes. The root bridge identifier and the timestamp of the root device is stored. Beyond 32 root bridge changes, the oldest root bridge information is overwritten. Entries are available for display in the chronological order for ease of understanding about the root device election in the network topology. For MSTP mode, root bridge information is stored for up to 32 entries for each MST instance and 32 entries for CIST.

Example

```
(Switch)#show spanning-tree root-history

Root Changes Counter: 1
Root Bridge Id          Timestamp
----------------------- ------------------------
80:00:14:7E:19:48:61:A0 Mon Mar 30 06:38:18 2026
```

show ssh

Display the current SSH client settings.

Syntax

show ssh

Mode

Privileged Exec

Example

```
(Switch)#show ssh
```

```
Outbound SSH Admin Mode:..................... Enabled
Outbound SSH Login Timeout (minutes)........... 5
Maximum number of outbound SSH sessions allow.. 4
Number of Active outbound SSH sessions:........ 0
SSH Client Encryption Algorithms:.............. aes128-ctr
                                                aes192-ctr
                                                aes256-ctr
                                                chacha20-poly1305@openssh.com
                                                aes128-gcm@openssh.com
                                                aes256-gcm@openssh.com

SSH Client MAC Algorithms:..................... hmac-sha2-256
                                                hmac-sha2-512
                                                hmac-sha2-256-etm@openssh.com
                                                hmac-sha2-512-etm@openssh.com

SSH Client KEX Algorithms:..................... curve25519-sha256
                                                curve25519-sha256@libssh.org
                                                ecdh-sha2-nistp256
                                                ecdh-sha2-nistp384
                                                ecdh-sha2-nistp521
                                                diffie-hellman-group-exchange-sha256
                                                diffie-hellman-group16-sha512
                                                diffie-hellman-group18-sha512
                                                diffie-hellman-group14-sha256
                                                sntrup761x25519-sha512@openssh.com
                                                sntrup761x25519-sha512
                                                mlkem768x25519-sha256

SSH Client HostKey Algorithms:................. rsa-sha2-256
                                                rsa-sha2-512
                                                ecdsa-sha2-nistp256
                                                ecdsa-sha2-nistp384
                                                ecdsa-sha2-nistp521
```

show startup-config

This command displays the content of text-based startup configuration file. This configuration file is loaded when the switch reboots.

Syntax

show startup-config

Mode

Privileged Exec

Usage guidelines

The text-based configuration files (startup-config, backup-config, and factory-defaults) are saved compressed in flash. With this command, the files are decompressed while displaying their content.

Example

```
(dhcp-10-52-131-173)#show startup-config
```

show sysinfo

This command displays switch information. To suppress the supported MIB output, use the noMibs option.

Syntax

show sysinfo [noMibs]

Mode

Privileged Exec

Example

```
(Switch)#show sysinfo

System Description.............................. HPE Networking Instant On Switch 24p Gigabit CL4 PoE
4p SFP+ 240W 1940, 4.13.15.33, 1.0.0.11
System Name..................................... dhcp-10-52-131-170
System Location.................................
System Contact..................................
System Object ID................................ 1.3.6.1.4.1.11.2.3.7.11.217
System Up Time.................................. 3 days 10 hrs 3 mins 16 secs
Current Time.................................... Apr 17 00:36:37 2026 AB(UTC-1:02)

MIBs Supported:

DIFFSERV-DSCP-TC                    The Textual Conventions defined in this
                                    module should be used whenever a
                                    Differentiated Services Code Point is used
                                    in a MIB.
DISMAN-PING-MIB                     The Ping MIB (DISMAN-PING-MIB) provides the
                                    capability of controlling the use of the
                                    ping function at a remote host.
DISMAN-TRACEROUTE-MIB               The Traceroute MIB (DISMAN-TRACEROUTE-MIB)
                                    provides access to the traceroute capability
                                    at a remote host.
DNS-RESOLVER-MIB                    The MIB module for entities implementing the
                                    client (resolver) side of the Domain Name
                                    System (DNS) protocol.
--More-- or (q)uit
```

show tech-support

Use this command to display system and configuration information when you contact technical support.

Syntax

show tech-support [file]

Mode

Privileged Exec

Usage guidelines

The output of the `show tech-support` command combines the output of the various `show` commands and includes log history files from previous runs. Using the file keyword saves the output to the tech-support file, which you can upload to a remote system by using the `copy` command. See copy.

Example

```
(Switch)#show tech-support

*************** show version ***************


Switch: 1

System Description............................. HPE Networking Instant On Switch 24p Gigabit CL4 PoE
4p SFP+ 240W 1940, 4.13.15.33, 1.0.0.11
Machine Model.................................. S4A31A
Serial Number.................................. VN5ZMCW125
Burned In MAC Address.......................... 34:C5:15:41:41:A0
Software Version............................... 4.13.15.33
CPLD version................................... 0x3b
Board Revision................................. 0x10
Bootcode Version............................... 1.0.0.11
Current Time................................... Apr 17 00:46:41 2026 AB(UTC-1:02)


*************** show sysinfo ***************


System Description............................. HPE Networking Instant On Switch 24p Gigabit CL4 PoE
4p SFP+ 240W 1940, 4.13.15.33, 1.0.0.11
System Name.................................... dhcp-10-52-131-170
System Location................................
System Contact.................................
System Object ID............................... 1.3.6.1.4.1.11.2.3.7.11.217
System Up Time................................. 3 days 10 hrs 13 mins 20 secs
Current Time................................... Apr 17 00:46:41 2026 AB(UTC-1:02)

MIBs Supported:

DIFFSERV-DSCP-TC                  The Textual Conventions defined in this
                                  module should be used whenever a
                                  Differentiated Services Code Point is used
                                  in a MIB.
DISMAN-PING-MIB                   The Ping MIB (DISMAN-PING-MIB) provides the
                                  capability of controlling the use of the
                                  ping function at a remote host.
DISMAN-TRACEROUTE-MIB             The Traceroute MIB (DISMAN-TRACEROUTE-MIB)
                                  provides access to the traceroute capability
                                  at a remote host.
DNS-RESOLVER-MIB                  The MIB module for entities implementing the
                                  client (resolver) side of the Domain Name
                                  System (DNS) protocol.
DNS-SERVER-MIB                    The MIB module for entities implementing the
                                  server side of the Domain Name System (DNS)
                                  protocol.
--More-- or (q)uit
```

show telnet

This command displays the current outbound Telnet settings. In other words, these settings apply to Telnet connections initiated from the switch to a remote system

Syntax

show telnet

Mode

Privileged Exec

Example

```
(Switch)#show telnet

Outbound Telnet Login Timeout (minutes)........ 5
Maximum Number of Outbound Telnet Sessions..... 5
Allow New Outbound Telnet Sessions............. Yes
```

show telnetcon

This command displays the current inbound Telnet settings. In other words, these settings apply to Telnet connections initiated from a remote system to the switch.

Syntax

show telnetcon

Mode

Privileged Exec

Example

```
(Switch)#show telnetcon

Remote Connection Login Timeout (minutes)...... 5
Maximum Number of Remote Connection Sessions... 5
Allow New Telnet Sessions...................... Yes
Telnet Sessions currently active............... 0
Telnet Server Admin Mode....................... Enable
Telnet Server Port............................. 23
```

show version

This command displays inventory information for the switch.

Syntax

show version

Example

```
(Switch)#show version

Switch: 1

System Description............................. HPE Networking Instant On Switch 24p Gigabit CL4 PoE
4p SFP+ 240W 1940, 4.13.15.33, 1.0.0.11
```

```
Machine Model................................ S4A31A
Serial Number................................ VN5ZMCW125
Burned In MAC Address........................ 34:C5:15:41:41:A0
Software Version............................. 4.13.15.33
CPLD version................................. 0x3b
Board Revision............................... 0x10
Bootcode Version............................. 1.0.0.11
Current Time................................. Apr 16 23:38:10 2026 AB(UTC-1:02)
```

show vlan

Syntax

show vlan [{*vlan-id* | brief | internal usage | port {*port-num* | all} remote-span}]

Parameters

These are the parameters:

- *vlan-id*: Specify the ID of the VLAN to view. The valid range is 1 to 4093
- brief: Display summary information about all VLANs configured on the switch.
- internal usage: Show VLANs assigned to port-based routing interfaces
- port: Display 802.1Q port parameters.
  - *port-num*: Show parameters for the specified port.
  - all: Show parameters for all ports.
- remote-span: Display RSPAN VLAN information.

Mode

Privileged Exec

User

Example

```
(Switch)#show vlan 200

VLAN ID: 200
VLAN Name: lab-vlan
VLAN Type: Static

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1           Exclude   Autodetect   Untagged
2           Exclude   Autodetect   Untagged
3           Exclude   Autodetect   Untagged
4           Exclude   Autodetect   Untagged
5           Exclude   Autodetect   Untagged
6           Exclude   Autodetect   Untagged
7           Exclude   Autodetect   Untagged
8           Exclude   Autodetect   Untagged
9           Exclude   Autodetect   Untagged
10          Exclude   Autodetect   Untagged
11          Exclude   Autodetect   Untagged
12          Exclude   Autodetect   Untagged
13          Exclude   Autodetect   Untagged
14          Exclude   Autodetect   Untagged
15          Exclude   Autodetect   Untagged
16          Exclude   Autodetect   Untagged
```

```
(Switch)#show vlan brief

VLAN ID VLAN Name                         VLAN Type
------- -------------------------------- ------------------
1       default                          Default
20      marketing                        Static
25      engineering                      Static
30      VLAN0030                         Static
31      VLAN0031                         Static
32      VLAN0032                         Static
33      VLAN0033                         Static
34      VLAN0034                         Static
35      VLAN0035                         Static
100     VLAN0100                         Static
200     lab-vlan                         Static

(Switch)#show vlan internal

Command not found / Incomplete command. Use ? to list commands.

(Switch)#show vlan internal usage

Base VLAN ID:  4093
Allocation policy:  Descending


(Switch)#show vlan port 5

          Port       Port                  Ingress    Ingress
          VLAN ID    VLAN ID  Acceptable   Filtering  Filtering         Default
Interface Configured Current  Frame Types  Configured Current   GVRP    Priority
--------- ---------- -------- ------------ ---------- --------- ------- --------
5         1          1        Admit All    Enable     Enable    Disable 0

Protected Port ............................. False
Switchport mode: General Mode
Operating parameters:
Operational switchport mode: General Mode
Port 5 is member in:


VLAN    Name                             Egress rule   Type
----    -------------------------------- -----------   ------------------
1       default                          Untagged      Default

Static configuration:

Port 5 is statically configured to:

VLAN    Name                             Egress rule
----    -------------------------------- -----------

Forbidden VLANS:

VLAN    Name
----    --------------------------------
```

snmp-server

This command configures the UDP port number on which the SNMP server listens for requests or the SNMP default trap send port number.

Syntax

snmp-server {port | trapsend} *port-id*

Mode

Privileged Exec

Parameters

These are the parameters:

- port: Configure the SNMP server listen port number
- trapsend: Configure the SNMP default trap send port number.
- *port-id*: Enter the SNMP port number for the listening port (default is 161) or trap send (default is 162) port. The valid range is 1025 to 65535.

Example

```
(Switch)#snmp-server trapsend 10025
```

telnet

This command establishes a new outbound Telnet connection to a remote host.

Syntax

telnet {*ip-address* | *hostname*} [port] [debug] [line] [localecho]

Mode

Privileged Exec

User

Parameters

These are the parameters:

- *ip-address*: A valid IP address.
- *hostname*: A valid hostname.
- port: A valid decimal integer in the range of 0 to 65535, where the default value is 23.
- debug: Displays the current Telnet options that are enabled.
- line: Sets the outbound Telnet operational mode as linemode where, by default, the operational mode is character mode.
- localecho: Enable local echo.

Example

```
(Switch)#telnet 10.52.131.173
Trying 10.52.131.173...

Connected to 10.52.131.173


Connection closed by foreign host.
```

traceroute

Use the traceroute command to discover the routes that IPv4 or IPv6 packets actually take when traveling to their destination through the network on a hop-by-hop basis. Traceroute continues to provide a synchronous response when initiated from the CLI.

Syntax

traceroute {*ip-address* | [ipv6] {*ipv6-address* | *hostname*}} [initTtl *initTtl*] [maxTtl *maxTtl*] [maxFail *maxFail*] [interval *interval*] [count *count*] [port *port*] [size *size*] [source {*ip-address* | *ipv6-address* | *port-num* | network | vlan *vlan-id*}]

Mode

Privileged Exec

Parameters

These are the parameters:

- ip-address: A valid IP address.
- ipv6-address: A valid IPv6 address.
- hostname: A valid hostname.
- ipv6: The optional ipv6 keyword can be used before ipv6-address or hostname. Giving the ipv6 keyword before the hostname tries it to resolve to an IPv6 address.
- initTtl: The initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 0 to 255.
- maxTtl: The maximum TTL. Range is 1 to 255.
- maxFail: Terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 0 to 255.
- interval: Specify the time between probes, in seconds. If a response is not received within this interval, then traceroute considers that probe a failure (printing *) and sends the next probe. If traceroute does receive a response to a probe within this interval, then it sends the next probe immediately. Range is 1 to 60 seconds.
- count: Specify the number of probes to send for each TTL value. Range is 1 to 10 probes.
- port: Specify destination UDP port of the probe. This should be an unused port on the remote destination system. Range is 1 to 65535.
- size: Specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.
- source: Specify the source IP address or interface for the traceroute.

Usage guidelines

Traceroute works by sending packets that are expected not to reach their final destination, but instead trigger ICMP error messages back to the source address from each hop along the forward path to the destination. By specifying the source address, the user can determine where along the forward path there is no route back to the source address. Note that this is only useful if the route from source to destination and destination to source is symmetric.) It would be common, for example, to send a traceroute from an edge router to a target higher in the network using a source address from a host subnet on the edge router. This would test reachability from within the network back to hosts attached to the edge router. Alternatively, one might send a traceroute with an address on a loopback interface as a source to test reachability back to the loopback interface address.

In the CLI, the user can specify the source as an IPv4 address, IPv6 address, the network interface, or as a routing interface. When the source is specified as a routing interface, the traceroute is sent using the primary IPv4 address on the source interface. With SNMP, the source must be specified as an address.

Example

```
(Switch)#traceroute 10.10.1.115
```

```
 Traceroute to 10.10.1.115 ,30 hops max 0 byte packets:

1  10.52.131.130      1   ms    2   ms    1   ms
2  0.0.0.0            *         *         *
3  172.22.203.57      1   ms    1   ms    1   ms
4  172.22.203.217     1   ms    1   ms    2   ms
5  204.107.184.132    238 ms    237 ms    237 ms
6  172.20.218.2       238 ms    238 ms    238 ms
7  172.20.128.82      238 ms    237 ms    238 ms
8  172.20.219.140     238 ms    239 ms    238 ms
9  172.20.219.140     238 ms    238 ms    238 ms
10 0.0.0.0            *         *         *
11 0.0.0.0            *         *

Hop Count = 11 Last TTL = 11 Test attempt = 32 Test Success = 24
```

update bootcode

This command updates the bootcode (boot loader) on the switch. The bootcode is read from the active-image for subsequent reboots.

Syntax

update bootcode

Mode

Privileged Exec

Examples

```
(Switch)#update bootcode

Power to the device must be maintained.

Are you sure you want to update the bootcode(y/n)? n

Bootcode Update Canceled!
```

vlan

This command creates one or more VLANs.

Syntax

vlan *vlan-list*

Mode

VLAN Database

Parameters

The *vlan-list* is one or more VLAN IDs in the range 1 to 4093. Use - to specify a range, or , to separate VLAN IDs in a list. Spaces and zeros are not permitted.

Examples

```
(Switch)#vlan database

(Switch)(Vlan)#vlan 20,25,30-35,200
```

```
(Switch)(Vlan)#exit'
                                ^
% Invalid input detected at '^' marker.

(Switch)(Vlan)#exit

(Switch)#show vlan

VLAN ID VLAN Name                         VLAN Type
------- --------------------------------- ------------------
1       default                           Default
20      VLAN0020                          Static
25      VLAN0025                          Static
30      VLAN0030                          Static
31      VLAN0031                          Static
32      VLAN0032                          Static
33      VLAN0033                          Static
34      VLAN0034                          Static
35      VLAN0035                          Static
100     VLAN0100                          Static
200     VLAN0200                          Static
```

vlan database

This command gives you access to the VLAN Database mode, which allows you to configure VLAN characteristics

Syntax

vlan database

Mode

Privileged Exec

Usage guidelines

After entering VLAN Database mode, the command prompt changes to help you identify the current mode.

Examples

```
(Switch)#vlan database

(Switch)(Vlan)#
```

vlan name

This command changes the name of a VLAN.

Syntax

vlan name *vlan-id name*

Mode

VLAN Database

Parameters

These are the parameters:

- *vlan-id*: A valid VLAN identification number. ID range is 1 to 4093.
- *name*: An alphanumeric string of up to 32 characters

Examples

```
(Switch)(Vlan)#vlan name 20 marketing

(Switch)(Vlan)#vlan name 25 engineering

(Switch)(Vlan)#exit

(Switch)#show vlan

VLAN ID VLAN Name                         VLAN Type
------- --------------------------------- ------------------
1       default                           Default
20      marketing                         Static
25      engineering                       Static
30      VLAN0030                          Static
31      VLAN0031                          Static
32      VLAN0032                          Static
33      VLAN0033                          Static
100     VLAN0100                          Static
```

write memory

Use this command to save running configuration changes to NVRAM so that the changes you make will persist across a reboot.

Syntax

write memory [confirm]

Mode

Privileged Exec

Parameters

Use the optional confirm keyword to directly save the configuration to NVRAM without prompting for a confirmation.

Usage guidelines

This command is the same as `copy system:running-config nvram:startup-config`.

Examples

```
(Switch)#write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved!
```

Appendix B
Support

Websites

Main Instant On site:

https://instant-on.hpe.com/

Support:

https://instant-on.hpe.com/contact-support/

Support documents:

https://community.instant-on.hpe.com/support/instant-on-resources/support-documentation-wired

Instant On social forums and knowledge base:

https://community.instant-on.hpe.com/home

Security Bulletins:

https://support.hpe.com/connect/s/securitybulletinlibrary

HPE end-user license agreement— enterprise version:

https://instant-on.hpe.com/eula/

Instant On EOS Policy:

https://www.hpe.com/psnow/doc/a00156646enw

Accessing HPE Networking Support

To access HPE Networking Support, go to https://instant-on.hpe.com/contact-support/.

Be sure to collect the following information before contacting Support:

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing Updates

To download product updates, go to the Instant On Support Portal Instant-On - Community & Software Downloads

If you are unable to find your product in the Instant On Support Portal, you might need to search My Networking, where older networking products can be found:

My Networking www.hpe.com/networking/software

To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:

www.hpe.com/support/AccessToSupportMaterials



Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method. To subscribe to eNewsletters and alerts: www.hpe.com/support/e-updates

Warranty Information

To view warranty information for your product, go to https://www.hpe.com/support/Networking-Warranties.

Regulatory Information

To view the regulatory information for your product, view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional Regulatory Information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at: www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH: www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see: www.hpe.com/info/environment

Documentation Feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.