

Aruba Instant On 1960 Switch Series Management and Configuration Guide



Published: 2022
Edition: 0.5

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

IEEE 802.3af[™], IEEE 802.3at[™], and IEEE 802.3bt[™] are trademarks of the Institute of Electrical and Electronics Engineers.

All other trademarks and registered trademarks are owned by their respective owners.

Chapter 1: About This Document	9
Applicable Products.....	9
Latest Version Available Online.....	9
Related Documents.....	9
Supported Features	9
Chapter 2: Getting Started	13
Connecting the Switch to the Network.....	13
Operating System and Browser Support.....	13
Selecting Local Web Management Mode	14
Getting Started With the Web Interface.....	15
Logging On.....	15
GUI Interface Layout and Features.....	15
Common Page Elements	16
Saving Changes.....	17
Latest Events Panel	17
Switch Panel View.....	18
Port State Indicator	19
Port Information	19
System LEDs	20
Chapter 3: Dashboard	23
Graphical Display	23
System Information	23
System Time	24
Device Information	25
System Resource Usage	25
Device Locator	26
Configuration Wizards.....	26
Getting Started Wizard.....	26
VLAN Configuration Wizard	27
Active Users	29
Chapter 4: Setup Network	30
Get Connected.....	30
IPv4 Setup Options	30
IPv6 Setup Options	31
HTTP/S Management Settings	33
Management VLAN Settings.....	34

System Time	35
Time Configuration	35
Daylight Saving Configuration	37
User Management	39
Logged In Sessions	39
User Accounts	40
Adding a User Account	40
Changing User Account Information	42
Removing a User Account	42
Account Security Settings	42
Password Strength Rules	43
Password Keyword Exclusion	44
DHCP Server	45
Global Configuration	45
Address Pool Tab	46
Adding an Address Pool	47
Static Assignment Tab	48
Adding a Static Assignment	48
DHCP Common Options Tab	50
DHCP Custom Options Tab	51
Adding a Custom DHCP Option	52
Excluded Addresses Tile	53
Adding an Excluded Address Range	53
Leased Addresses Tile	54
Schedule Configuration	55
Schedules	55
Adding a Schedule	56
Removing a Schedule	59
DNS Configuration	59
Global Configuration	60
DNS Servers	60
Manual Host Mapping	61
DNS Resolutions	62
Stacking Configuration	62
Stacking LAG	63
Global Settings	64
Unit Numbering	65
Stacking Port Configuration	66
Chapter 5: Switching Features	68
Port Configuration	68
Graphical Display	68
Global Configuration	68
Interface Configuration	70
Modifying Interface Settings	71

Interface Statistics	74
Port Mirroring and Remote Port Mirroring	75
Global Configuration	77
Mirroring Sessions	77
Configuring a Port Mirroring Session	78
Loop Protection	79
Global Configuration	80
Interface Configuration	80
Loop Protection Configuration	81
IGMP Snooping	82
Global Configuration	82
IPv4/IPv6 Unregistered Multicast	83
IGMP Snooping VLAN Configuration	84
IGMP Snooping Multicast Router Interface Configuration	89
Configuring Multicast Router Settings on Interfaces	89
Multicast Forwarding Database	90
MLD Snooping	91
Global Configuration	91
IPv4/IPv6 Unregistered Multicast	93
MLD Snooping VLAN Configuration	93
Modifying MLD Snooping VLAN Configuration Settings	94
MLD Snooping Multicast Router Interface Configuration	96
Configuring Multicast Router Settings on Interfaces	97
IPv6 Multicast Forwarding Database	98
SNMP	98
Global Configuration	99
Community Configuration	100
Adding an SNMP Community or Community Group	101
Removing an SNMP Community or Community Group	101
SNMP Trap Receivers v1/v2	102
Adding an SNMP v1/v2 Trap Receiver	102
Removing an SNMP v1/v2 Trap Receiver	103
SNMP Trap Receivers v3	103
Adding an SNMP v3 Trap Receiver	104
Removing an SNMP v3 Trap Receiver	105
SNMP Access Control Group Configuration	105
Adding an SNMP Access Control Group	106
Removing an SNMP Access Control Group	107
SNMP User Configuration	107
Adding an SNMP User	108
Removing an SNMP User	110
SNMP View Configuration	110
Adding an SNMP View	110
Removing an SNMP View	111

Remote Engine ID Configuration	111
Adding a Remote Engine ID Configuration	111
Removing a Remote Engine ID Configuration	112
Interface Auto Recovery	112
Global Configuration	113
Suspended Interfaces	114
Trunk Configuration	115
Graphical Display	116
Global Configuration	116
Trunk Configuration	117
Modifying Trunk Settings	118
EEE Configuration	120
Global Configuration	120
Global Status	121
Interface Status	121
Chapter 6: Spanning Tree	123
Global Configuration	123
Global Settings	125
Spanning Tree Statistics	126
CST Configuration	127
CST Port Configuration	128
Additional Actions on CST Ports	129
MSTP Configuration	132
MSTP Configuration	133
Adding, Editing or Removing an MSTP Configuration	133
MSTP Port Configuration	134
Viewing MSTP Port Details or Editing MSTP Port Settings	136
Chapter 7: Virtual LAN	139
VLAN Configuration	139
Graphical Display	139
VLAN Configuration	140
VLAN Membership	142
VLAN Membership - By Interface Tab	142
VLAN Membership - By VLAN Tab	143
VLAN Interface Configuration	144
Voice VLAN Configuration	145
Global Configuration	146
Telephony OUI Configuration	147
Voice VLAN Interface Settings	148
Chapter 8: Neighbor Discovery	150
LLDP	150
LLDP Global Configuration	151
LLDP Global Information	151

Interface Configuration	152
Remote Device Information.....	155
Local Device Information.....	156
LLDP Statistics.....	158
LLDP-MED	159
LLDP-MED Global Configuration	159
LLDP Global Information.....	160
Interface Configuration	160
Remote Device Information.....	162
Displaying Remote Device Details	163
Chapter 9: Power over Ethernet	165
PoE Configuration.....	165
Graphical Display	166
Activity.....	166
Priority.....	166
Class	166
Status	167
Consumption History	168
Port Configuration	168
Edit Port PoE Configuration	170
PoE Port Details.....	170
Chapter 10: Routing	173
Routing Configuration	173
Global Configuration	173
Static Routing.....	179
Adding a Static Route	179
Route Table.....	181
IP Routing Statistics/ICMP Statistics.....	181
IP Routing Statistics.....	182
ICMP Statistics.....	183
IPv6 Routing	184
Global Configuration	185
IPv6 Routes.....	191
Neighbor Discovery	193
DHCP Relay.....	199
Global Configuration	199
Server Configuration	200
DHCP Relay Interfaces	200
Adding a DHCP Server	201
Removing a Relay Interface.....	202
DHCPv6 Relay.....	202
Global Destinations	202
Interface Destinations	203

ARP Table	204
Global Configuration	205
ARP Table	205
Adding a Static ARP Entry	206
Removing an ARP Entry	206
Chapter 11: Quality of Service (QoS)	207
Access Control Lists	207
Access Control Lists	207
Adding an ACL	208
IPv4 ACL Rules	209
IPv6 ACL Rules	211
MAC ACL Rules	213
Interface Configuration	215
Associating an ACL with an Interface	217
VLAN Configuration	217
Associating an ACL with a VLAN	218
Class of Service	219
General Settings	219
802.1p Priority Mapping	220
Configuring 802.1p CoS Mapping	220
Queue Configuration	221
DSCP CoS Mapping	222
Interface CoS Configuration	223
Configuring the CoS on an Interface	224
Queue Statistics	225
Chapter 12: Security	226
Overview	226
RADIUS Configuration	226
Global Configuration	226
Radius Server Configuration	228
Adding a RADIUS Server	228
Changing RADIUS Server Settings	229
Port Access Control	230
Global Configuration	230
MAC Authentication Settings	232
Port Configuration	233
Configuring Port Access Control on an Interface	234
Viewing Per-port 802.1X Details	237
VLAN Authentication	237
Supplicant Credentials	238
Access Control Client Information	238
Access Control Statistics	239
Access Control Details	240

Port Security	242
Port Security Configuration	242
Static MAC Addresses	243
Dynamic MAC Addresses	244
Convert Dynamic MAC Addresses to Static MAC Addresses	245
Protected Ports	245
Protected Ports Configuration	246
DHCP Snooping and IPSG	247
Global Configuration	247
VLAN Settings	248
Interface Settings	249
Binding Database	250
ARP Attack Protection	252
Global Configuration	252
Interface Settings	253
ARP Access Control Rules	254
VLAN Settings	255
Denial of Service Protection	257
Global Settings	257
SYN Attack Status Tab	258
Interface Settings Tab	259
HTTPS Certificate	260
HTTPS Certificate Settings	261
Generate a Self-Signed Certificate	262
Using a Certificate Signed by a Certificate Authority	263
View a Certificate	264
Chapter 13: Diagnostics	266
Unexpected Restart Information	266
Global Log Settings	266
Remote Log Server	267
Buffered Log	269
Log File	270
Ping	271
IPv4 Tab	271
IPv6 Tab	273
Ping Results	274
IPv4/IPv6	274
IPv4 Tab	274
IPv6 Tab	276
Traceroute Results	277
Support File	277
Cable Test	280
Interface Configuration	280
MAC Table	281

Global Configuration	281
MAC Address Table	282
RMON	283
RMON Statistics	283
History Collectors	285
History Log	287
RMON Events	288
Event Log	289
RMON Alarms	290
Chapter 14: Maintenance	292
Backup and Update Files	293
Secure Copy Protocol (SCP) Usage	293
Configuration File Operations	295
Reset	296
Reboot Device	296
Reset to Factory Defaults	297
Chapter 15: Support	299
Websites	299
Accessing Aruba Support	299
Accessing Updates	299
Warranty Information	300
Regulatory Information	300
Additional Regulatory Information	300
Documentation Feedback	301

The Aruba Instant On 1960 Switch Series are designed to meet the needs of small business network environments — simple to set up and manage and are secure and reliable. Aruba Instant On 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. This manual details using the web GUI to manage the switch.

Applicable Products

This guide applies to these products:

- Aruba Instant On 1960 24G 2XGT 2SFP+ Switch
- Aruba Instant On 1960 24G 20p Class4 4p Class6 PoE 2XGT 2SFP+ 370W Switch
- Aruba Instant On 1960 48G 2XGT 2SFP+ Switch
- Aruba Instant On 1960 48G 40p Class4 8p Class6 PoE 2XGT 2SFP+ 600W Switch
- Aruba Instant On 1960 12XGT 4SFP+ Switch

Latest Version Available Online

Updates to this document can occur after initial publication. For the latest versions of product documentation, see the links provided in the Websites chapter of this document or visit the Aruba Instant On Support site at:

<https://community.arubainstanton.com>

Related Documents

- *Aruba Instant On 1960 Installation and Getting Started Guide*
- *START HERE: Installation, Safety, and Regulatory Information for the Aruba Instant On 1960 Switches*
- *Aruba Instant On User Guide*

Supported Features

Aruba Instant On 1960 Switch Series switches include support for the following:

- IEEE 802.3 10BASE-T

- IEEE 802.3u 100BASE-TX
- IEEE 802.3ab 1000BASE-T
- IEEE 802.3ae 10Gb/s Ethernet (Aruba Instant On 1960 Switch Series)
- Cable Test
- HTTP and HTTPS sessions (5 sessions total)
- 16,384 MAC entries
- MAC aging (configurable)
- IEEE 802.2af: Power over Ethernet
- IEEE 802.3at
- IEEE 802.3bt
- IEEE 802.3x: Flow control
- IEEE 802.1Q: VLANs
 - o Access SKUs - up to 256 VLANs
 - o Aggregate SKUs - up to 512 VLANs
 - o Hybrid Stack - up to 256 VLANs
- IEEE 802.1p
- ACLs (named ACL - IPv4, IPv6 and MAC). Up to 100 ACLs. No limit to number of ACLs per interface
- Access Control Entries (ACEs) -
 - o Access SKUs – 960 ACEs
 - o Aggregate SKUs – 1024 ACEs
 - o Hybrid Stack – 960 ACEs
- 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)
- Trunk (LAG) support
 - o LAGs: up to 16 LAGs with up to 8 active port members
 - o IEEE 802.3ad: Link aggregation (LACP). Up to 16 candidate ports.
 - o Static Trunks
- Jumbo packet support (10240 bytes)
- Auto-MDI/MDIX
- Storm Control (global)
- Ingress Rate Limiting (per port)
- Port Mirroring
- Stacking
 - o Up to 4 switches in Native or Hybrid stack configuration
- IGMP Snooping v1/v2/v3
 - o IGMP Snooping querier
- MLD Snooping v1/v2
 - o MLD Snooping querier
- Unregistered Multicast handling (IPv4 and IPv6)

- Global time scheduler (3 schedules)
 - o PoE
 - o Port shutdown
 - o Access Control Entries (ACE)
- Static IPv4 address assignment - 32 interfaces
- Static IPv6 address assignment - 32 interfaces
- DHCP client
- DHCP fallback
- DHCPv4 Server
- DNS Client
- User Accounts (up to 5, Read/write, Read only)
- Password management (aging, lockout, strength check, key word exclusion)
- SNMPv1/v2c/v3
- RMON (groups: Alarm, Event, History & Statistics)
- RADIUS (up to 4 combined RADIUS authentication / accounting servers)
- RADIUS Accounting
- RADIUS assigned VLANs
- RADIUS MAC authentication (EAP equivalent to "RADIUS", MD5)
- 802.1x port based access control
- 802.1x Guest VLAN
- 802.1x configurable username and password
- Port Security
- Protected Ports
- ARP Attack Protection
- IP Source Guard
- DoS Protection
- SNTP (RFC 2030)
- Loop Protection
- IEEE 802.3az: Energy Efficient Ethernet
- IPv4 Static Routing
 - o Access SKU: 32 Static routes
 - o Aggregate SKU: 512 Static routes
 - o Hybrid Stack: 32 Static routes
- IPv6 Static Routing
 - o Access SKU: 32 Static routes
 - o Aggregate SKU: 256 Static routes
 - o Hybrid Stack: 32 Static routes
- Routing (VLAN, Interface)
- DHCP Relay (IPv4 and IPv6)
- DHCP snooping
- ARP table – 508 entries
- 802.1p/DSCP priority to queue mapping

- Number of egress queues (traffic priority) – 8
- 802.1p port based priority
- Auto Voice VLAN
- Ping (IPv4/IPv6)
- Traceroute (IPv4/IPv6)
- Dual image support
- Firmware Update over HTTP, HTTPS, TFTP, SCP
- Config File backup / restore
- File copy (upload/download)
- Syslog Log (local & remote)
 - o 1 remote syslog server
 - o Up to 1000 entries on Buffered log
 - o Up to 200 in Log file (Flash)

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

Connecting the Switch to the 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.



To use DHCP for IP network configuration, the switch must be connected to the same network as the DHCP server. You will need to access your DHCP server to determine the IP address assigned to the switch.

The switch supports LLDP (Link Layer Discovery Protocol), allowing discovery of its IP address from a connected switch or management station.

If DHCP is used for configuration and the switch fails to be configured, the IP address 192.168.1.1 is assigned to the switch interface.

To access the web interface on the switch, 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 **Operating System and 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 tool, interface or features.

Operating System and Browser Support

The following operating systems and browsers, with JavaScript enabled, are supported:

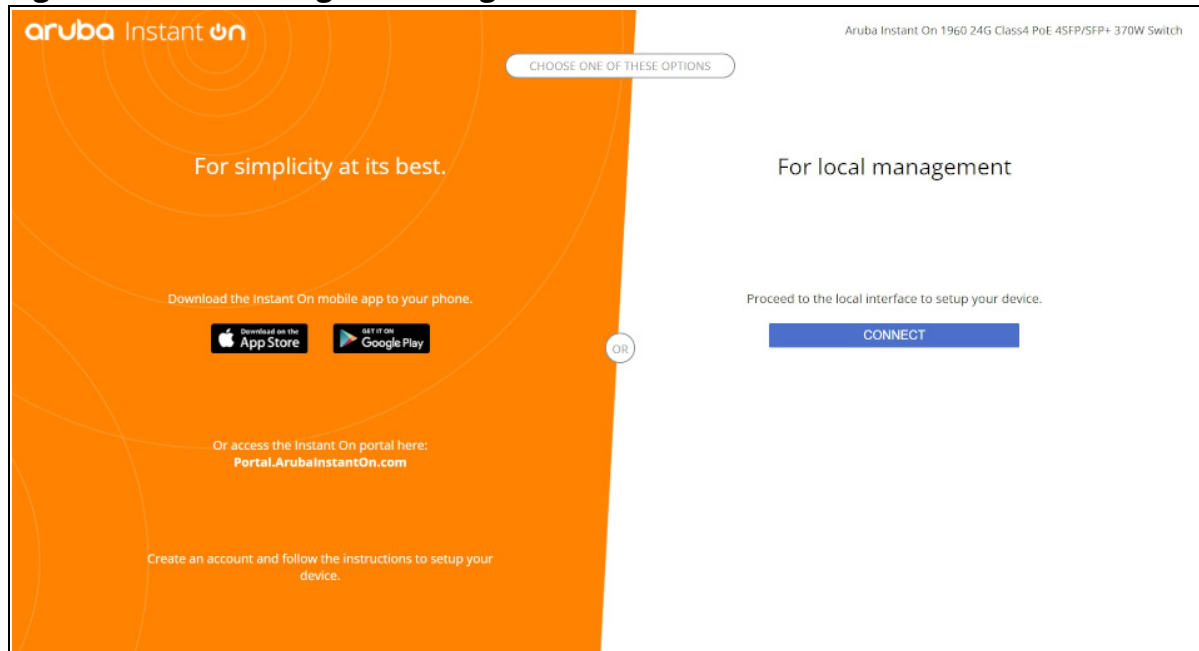
Table 1. Operating System and Browser Support

Operating System	Browser
Windows 7	Chrome version 87 or higher Firefox version 84 or higher
Windows 10	Chrome version 87 or higher Firefox version 84 or higher
MAC OS X 10.15	Safari version 14 or higher Chrome version 87 or higher Firefox version 84 or higher
Linux OS 2.6, 3.11	Chrome version 87 or higher Firefox version 84 or higher

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). In addition the welcome page outlines instructions to create and configure a portal account. 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



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

Select CONNECT to manage the switch locally using the web interface and continue on in this guide. If you would rather use the Aruba Instant On Cloud Portal to manage the switch, see the *Aruba Instant On 1960 Switch Series Installation and Getting Started Guide* and the *Aruba Instant On User Guide*.

Getting Started With the Web Interface

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

Logging On

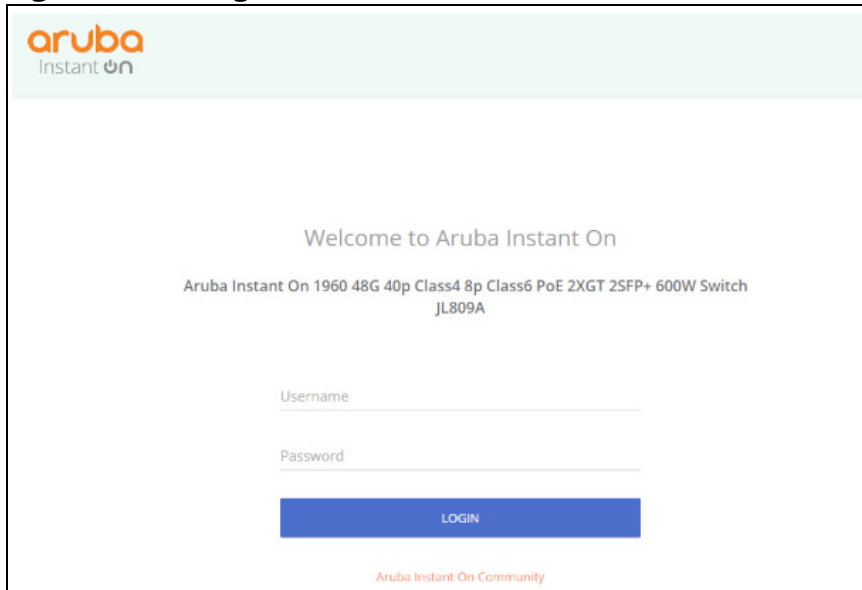
Follow these steps to log on through the web interface:

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 **Log In**.
On the initial login, the username is **admin** and there is no password.
3. Following the initial login, the administrator is prompted to update the username and password.



To set the password or change the username, see [User Management](#).

Figure 2. Login Screen



The login screen features the Aruba Instant On logo at the top left. The main heading is "Welcome to Aruba Instant On". Below this, the switch model "Aruba Instant On 1960 48G 40p Class4 8p Class6 PoE 2XGT 25FP+ 600W Switch JL809A" is displayed. There are two input fields: "Username" and "Password". A blue "LOGIN" button is positioned below the password field. At the bottom right, there is a link to the "Aruba Instant On Community".

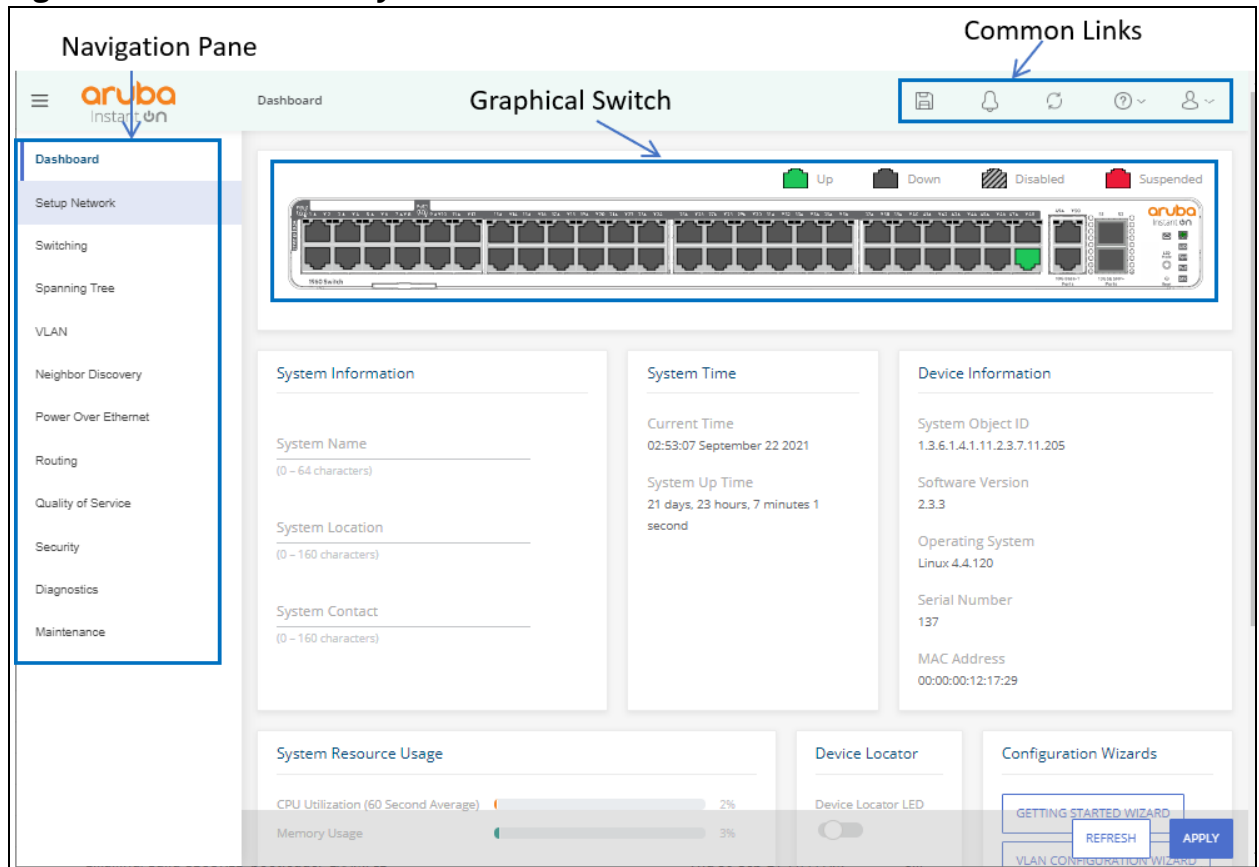
GUI Interface Layout and Features

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 **Setup Network** link beneath **Dashboard** to display the **Get Connected** page, which you use to set up a management connection to the switch. See [Get Connected](#) for more information.

The graphical switch displays summary information for the switch LEDs and port status. For information on this feature see [Switch Panel View](#).

Figure 3. Interface Layout and Features

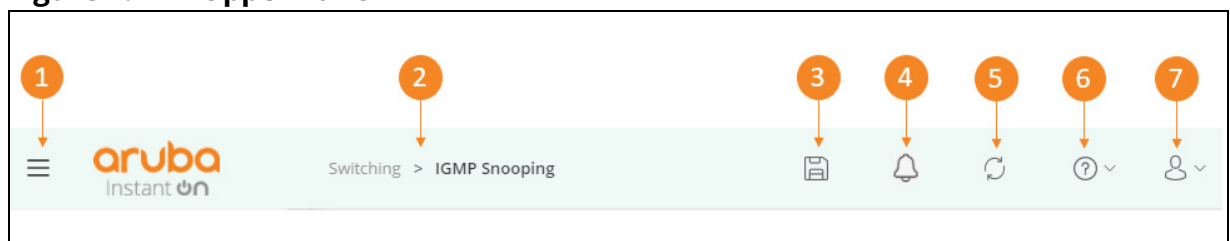


Click on any topic in the navigation pane to display related configuration options.

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 following:

Table 2. Upper Panel Components

Label	Description
1	Click Show Navigation  to toggle the navigation pane that shows all the screens that are available for the switch.

Label	Description
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 Help  on any page to display a help panel that explains the fields and configuration options on the page.
7	Click Profile  to view your profile information, or to log out.



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  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  to refresh the page with the latest information from the switch.

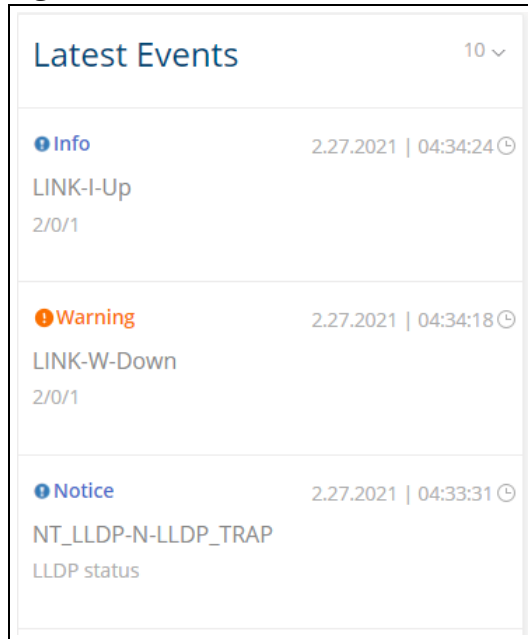
Saving Changes

When you click , 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  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.

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

Each event display has the following components:

- Severity indication: This indication is displayed as an icon and the name of the severity level in a color based on the severity:
 - o Blue - Severity lower than Warning
 - o Orange - Severity of Warning
 - o Red - Severity higher than Warning
- 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** panel with the full information on the events logged by the switch.

Switch Panel View

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

You can right-click anywhere on the view and select from the menu to display the product and port information on the Dashboard page, to refresh the graphic display, and to set the automatic refresh rate.

Figure 6. Switch Panel View

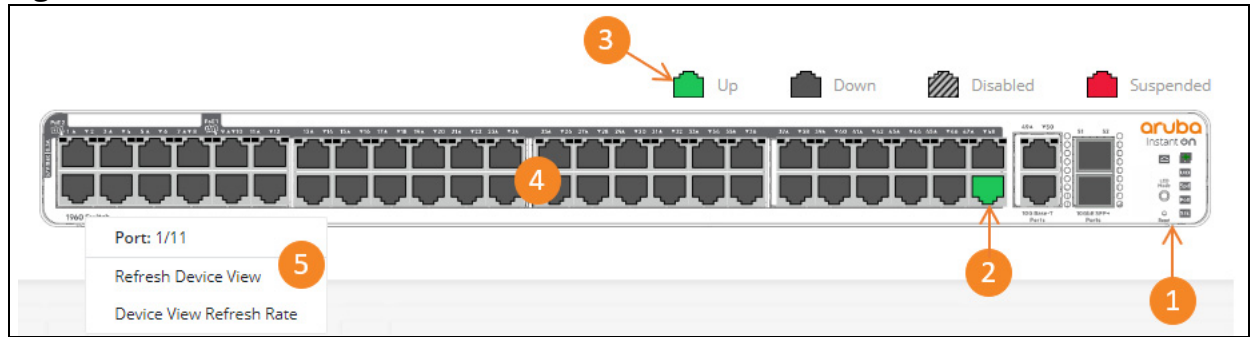


Table 3. Switch Panel Components

Label	Description
1	System LEDs
2	Port status indicator
3	Legend. The Legend shows port status for different features.
4	Port configuration and summary. Point or click on any port for options.
5	Right-click options, available from anywhere on the panel view,

Port State Indicator

Each port in the switch view is visually represented by one of the following state images.

Table 4. Port State Indicators

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.

Port Information

You can hover the mouse on any port in the Switch Panel 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.

You can right-click a port to refresh the switch view, display and configure the switch refresh rate.

System LEDs

The following System LEDs reflect the status of the actual LEDs on the switch:

Figure 7. System LED Indicators



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

Table 5. 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) - Self-test and initialization is in progress (boot-up). - 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 – 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.
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.

Indicator	Color	Image	Description
Stack Mode	Green/ Orange		The stack mode LED can be used, in conjunction with stacking interface LEDs, to indicate: - Stack conductor unit. - Stacking interfaces on all stack units. - Stacking and stack interface faults.
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 "onboarding 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, stacking 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, stacking or PoE) - Speed - Stacking - PoE (for units that support PoE) The speed, stacking and PoE LED modes have specific global LED indicating the selected mode.
Reset button			Reset the system. Press and release to reset the switch. Press and hold for 5 seconds or longer, to reset the switch to factory defaults.

The following table summarizes LED indication for stack and stack interfaces

Table 6: Stack Mode LED

Stack Mode LED State	Stack LED Indication	Stack Interface LED Indication
Off	Stacking mode is not selected and no stacking fault conditions exist.	According to the current LED mode (speed, PoE, Link activity).
On green	Stacking mode is selected and unit role is Conductor.	Green - stack that ports are up and active, no faults. Off - not a stack port or a stack port with no link up or a stack port that is in standby state.
Slow flash Green	Stacking mode is selected and unit role is Member.	Green - stack ports that are up and active, no faults. Off - not a stack port or a stack port with no link up or a stack port that is in standby state.
On orange	Stacking mode is selected and active. Unit role is Conductor or Member. One or more stacking ports are in a fault state. OR Member unit that is not connected to a stack conductor. NOTE: Global Status LED - slow flash (orange).	Slow flash (orange) - Configured Stack Port which is in a fault state. Green - stack ports that are up and active, no faults. Off - not a stack port or a stack port with no link up or a stack port that is in standby state. Stack port fault state - - link up but not connected to stack interface link partner. - Other issue with stack protocol with link partner which prevents establishing a stack link (but does not include a stack link in standby state).

Stack Mode		
LED State	Stack LED Indication	Stack Interface LED Indication
Slow flash orange	Stacking mode is NOT selected. Unit role is Conductor or Member. One or more stacking ports are in a fault state. OR Member unit that is not connected to a stack conductor NOTE: Global Status LED - slow flash (amber). Optionally, flash simultaneously with stacking LED	According to the current LED mode (speed, PoE, Link activity)
Slow flash orange	Together with port LED indication on the right - Duplicate Unit ID (Conductor or Member)	All port LEDs flash orange.



In stack LED mode, non-stacking interface LEDs are always off.

You can use the Dashboard page to display and configure basic information about the system, and to use device configuration wizards.

The Dashboard page displays basic information such as the graphical display of switch, configurable switch name and description, System time and Switch information including the software and operating system versions. This page also shows resource usage statistics, and allows you to enable the switch locator LED.

The page also supports the following configuration wizards:

- Getting started Wizard
- VLAN configuration Wizard

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

The Dashboard is made up of various tiles, each of which contain various information about the switch. Each tile is described here.

Graphical Display

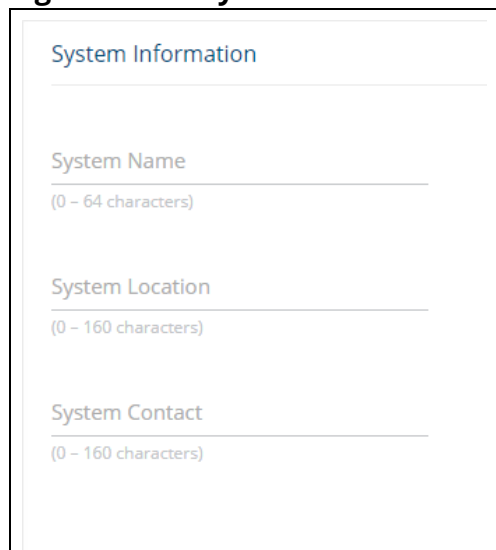
The top of the Dashboard page shows a graphical representation of the switch front panel. This panel view has a display of the ports, each with its current status.

Click a port in this screen, to open the **Switching > Port Configuration** page.

For more information, see [Switch Panel View](#).

System Information

Figure 8. System Information Tile



System Information

System Name
(0 - 64 characters)

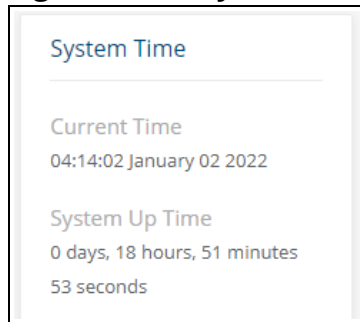
System Location
(0 - 160 characters)

System Contact
(0 - 160 characters)

Table 7. System Information Fields

Field	Description
System Name	Enter the preferred name to identify this switch. A maximum of 63 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.
System Location	Enter the location of this switch. A maximum of 160 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 160 alpha-numeric, case-sensitive characters is allowed, including special characters (!, ", #, \$, %, &, ', (,), *, +, ,, -, ., /, :, ;, <, =, >, ?, @, [,], \, ^, _ ` , {, }, ~, and space). This field is blank by default..

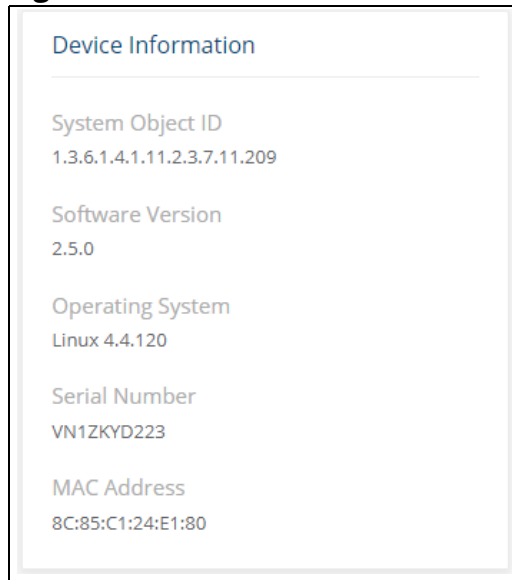
System Time

Figure 9. System Time Tile**Figure 10. 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 Up Time	The time in days, hours, minutes, and seconds since the last switch reboot.

Device Information

Figure 11. Device information Tile



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

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 Resource Usage

Figure 12. System Resource Usage Tile

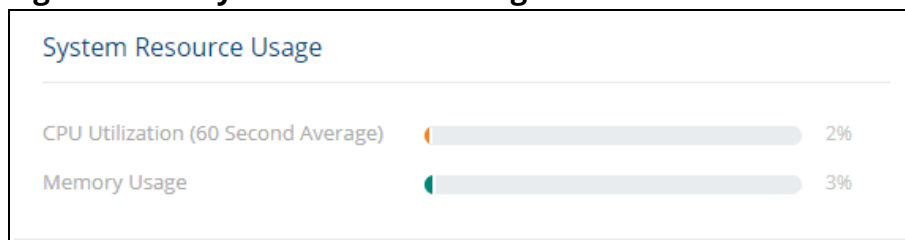


Table 9. System Resource Usage Fields

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 system memory (RAM) currently in use.

Device Locator

Figure 13. Device Locator Tile

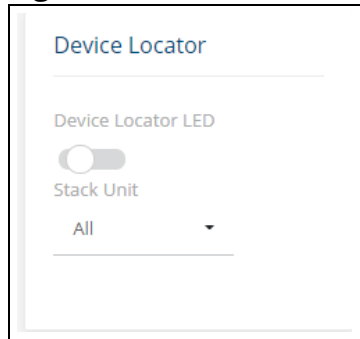


Table 10. Device Locator Field

Field	Description
Device Locator LED	Enable this feature to start flashing the physical device locator LED for 30 minutes.
Stack Unit	Define which units in the stack should flash the Locator LED. Available settings: All and 1-4, default is to flash the Locator LED of all units in the stack.

Configuration Wizards

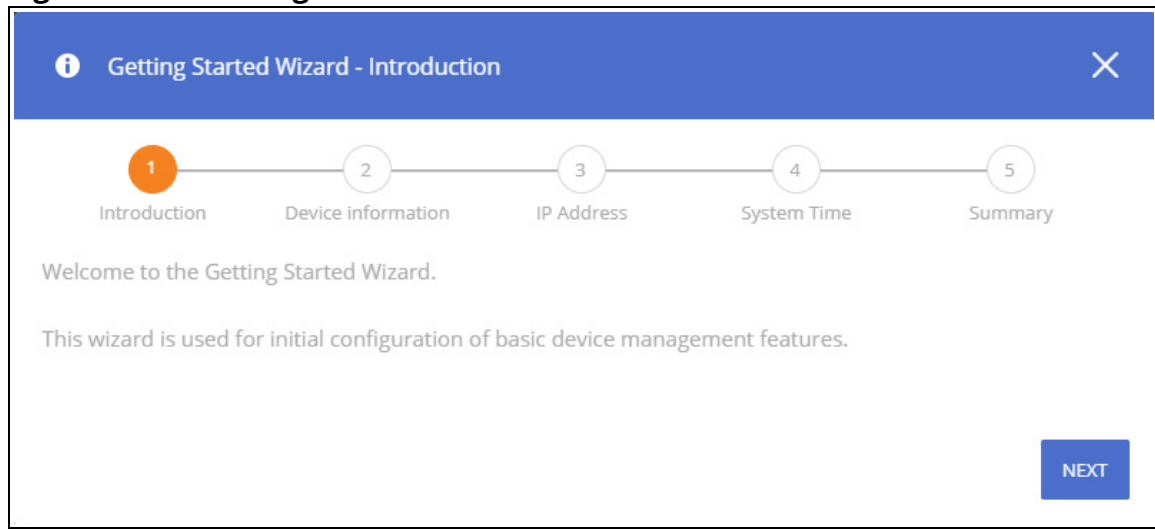
The Aruba Instant On 1960 provides the following wizards:

- Getting Started Wizard
- VLAN Configuration Wizard

Getting Started Wizard

Click the **GETTING STARTED WIZARD** button to open the Getting Started Wizard that walks you through the stages of initial configuration of the basic management features of the Aruba Instant On 1960 Switch Series.

Figure 14. Getting Started Wizard



These are the steps that the wizard takes you through.

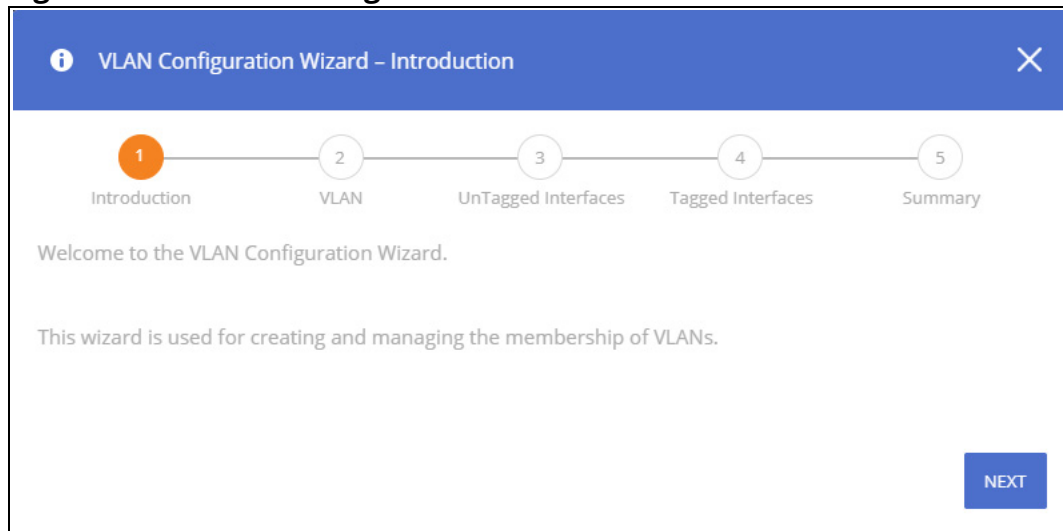
- Step 1 - Introduction screen. Click the **NEXT** button to proceed with the configuration wizard.
- Step 2 - Device Information, enter a System Name, System Location and System Contact information to help identify the device.
Click **NEXT** to go to the next screen in the configuration wizard.
- Step 3 - IP Address. Set up the IP interface. For more information on the fields in this screen, see [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 [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 **CLOSE** to close the wizard.

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

VLAN Configuration Wizard

Click the **VLAN CONFIGURATION WIZARD** button to open the VLAN Configuration Wizard that walks you through the stages of initial configuration of the a Virtual Local Area Network (VLAN) on the Aruba Instant On 1960 Switch Series.

Figure 15. 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 untagged and tagged interfaces, see [“VLAN Membership - By VLAN Tab 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.

To view the changes, go to **VLAN > VLAN Configuration**.

Active Users

Figure 16. Active Users Tile

Active Users			Display:
Username	Connected From	Session Time	
AIQUser1	10.5.229.216	27:51	
AIQUser1	*	01:03	
			< 1 >



The Active Users tile displays only if more than one user is logged into the system.

Table 11. Active Users Fields

Field	Description
Username	The username of each logged in user.
Connected From	The IP address from which the user logged in.
Session Time	The amount of time the user session has been active, in hours, minutes, and seconds.

You can use the Setup Network pages to configure how a management computer connects to the switch, to set up system time settings, and to manage switch administrator accounts and passwords.

Get Connected

Use the **Get Connected** page to configure settings for the switches management interface. The management interface is defined by an IP address, subnet mask, and gateway.

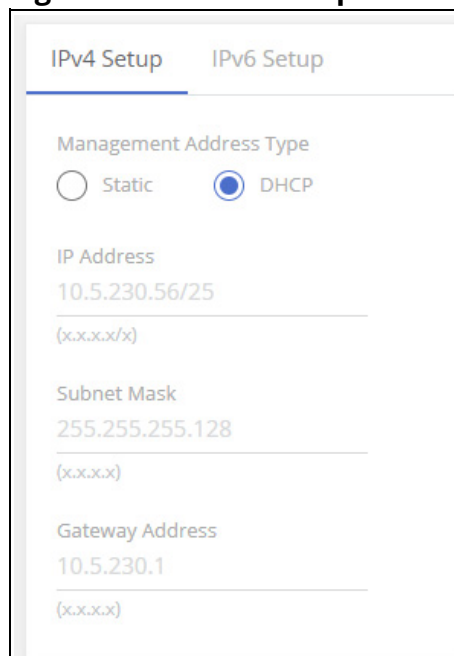
To display the Get Connected page, click **Setup Network** > **Get Connected**.

The following sections explain the various tiles and the configuration options within each tile.

IPv4 Setup Options

To view the IPv4 Setup options, click on the **IPv4 Setup** tab in the tile.

Figure 17. IPv4 Setup Tab



The screenshot shows the IPv4 Setup tab with the following configuration options:

- Management Address Type:** Two radio buttons are present. 'Static' is unselected, and 'DHCP' is selected (indicated by a blue dot).
- IP Address:** The value '10.5.230.56/25' is entered in the text field. Below the field is a placeholder '(x.x.x.x/x)'.
- Subnet Mask:** The value '255.255.255.128' is entered in the text field. Below the field is a placeholder '(x.x.x.x)'.
- Gateway Address:** The value '10.5.230.1' is entered in the text field. Below the field is a placeholder '(x.x.x.x)'.



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**)

Table 12. IPv4 Setup Fields

Field	Description
Management Address Type	Select the type of network connection: • Static—Select this option to configure the IP address, subnet mask, and gateway fields for data entry. • DHCP—Select this option to configure 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. 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 address 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 Options

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

Figure 18. IPv6 Setup Tab

IPv4 Setup **IPv6 Setup**

IPv6 Status
☒

DHCP Network Configuration
☒

IPv6 Stateless Autoconfig
☒

Static IPv6 Address

Dynamic IPv6 Address
51::103/128
51::200:16ff:fe05:2019/64

EUI Flag
☐

IPv6 Gateway

DHCPv6 Client DUID
00:03:00:01:00:00:16:05:20:19



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.

Table 13. IPv6 Setup Fields

Field	Description
IPv6 Status	Enables or disables the IPv6 administrative mode on the management interface.
DCHP Network Configuration	Specify whether the switch should attempt to acquire network information from a DHCPv6 server. Set as Disabled to disable the DHCPv6 client on the management interface.
IPv6 Stateless Autoconfig	Sets the IPv6 stateless address autoconfiguration mode on the management interface. • Enabled – The management interface can acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of Router Advertisement messages. • Disabled – The management interface will not use the native IPv6 address auto-configuration to acquire an IPv6 address.

Field	Description
Static IPv6 Address	Specify the IPv6 address to add to the interface.
Dynamic IPv6 Address	Lists the IPv6 addresses on the management 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 management 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 19. HTTP/S Management Settings Tabs

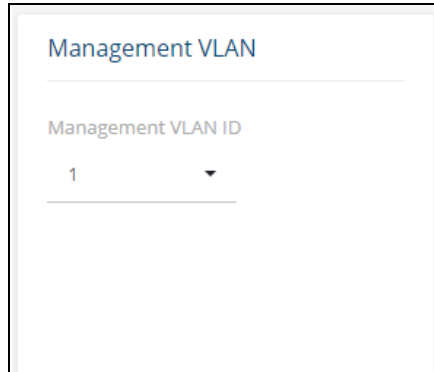
The screenshot shows the 'HTTP Management Settings' tab selected. The 'HTTP Management' toggle is turned on. Below it, the 'Port' is set to 80, with a range of 1025 – 59999; Default = 80. The 'Session Soft Timeout' is set to 10, with a range of 1 – 60 Minutes. The 'Session Hard Timeout' is set to 24, with a range of 1 – 168 Hours.

Table 14. 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/s management is enabled.
Port	The TCP port number on which the HTTP/S server listens for requests. Existing HTTP/S login sessions are closed whenever this value is changed. All new HTTP 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 service. For HTTP the default is 80, for HTTPS the default is 443. The valid range for this port number is 1025-59999.
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.
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

Figure 20. Management VLAN Tile



The figure shows a configuration tile titled "Management VLAN". Below the title is a label "Management VLAN ID" followed by a dropdown menu. The dropdown menu currently displays the value "1".

Table 15. Management VLAN Fields

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) cannot 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.

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

System Time

Click **Setup Network > System Time** to configure the system clock, SNTP 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 Simple Network Time Protocol (SNTP) server. Using SNTP ensures accurate network switch clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The software operates only as an SNTP client and cannot provide time services to other systems.

Figure 21. Time Configuration Tile

Time Configuration

System Time Source

☒ SNTP ☐ Manual

Time

21:21 

Date

Aug 01 2019 

SNTP Server

(x.x.x.x)

Server Port

123

(1 - 65535)

Last Update Time

N/A

Last Attempt Time

N/A

Last Attempt Status

Unknown

Time Zone Settings

Time Zone GMT 00:00 

Table 16. Time Configuration Fields

Field	Description
System Time Source	Select SNTP (Simple 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 SNTP server. When SNTP 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.

Field	Description
SNTP Server	Specify the address of the SNTP 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 • IPv6 link local address (with zone), in the format of X:X:X:X::X • Hostname - specify the server hostname
Server Port	Specify the server's UDP port for SNTP. The range is 1 to 65535 and the default is 123.
Last Update Time	The date and time (GMT) when the SNTP client last updated the system clock.
Last Attempt Time	The date and time (GMT) of the last SNTP request or receipt of an unsolicited message.
Last Attempt Status	The status of the last update request to the SNTP server, which can be one of the following values: • Unknown — None of the following values apply or no message has been received. • Up— The SNTP operation was successful and the system time was updated. • Request Timed Out— A SNTP request timed out without receiving a response from the SNTP server. • Down—Connection not established with SNTP server. • In Process—currently establishing connection with SNTP server.
Time Zone Settings	
Time Zone	The currently set time zone. To edit, click the Edit button  The default is (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London.
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 **Setup Network** > **System Time** in the navigation pane.

Figure 22. Daylight Saving Configuration Tile

Daylight Saving Configuration

Daylight Saving Time

Recurring

Non Recurring Range

Start Date

Jul 28 2019

Starting Time of Day

End Date

Ending Time of Day

Recurring Range

Start Week

Last

Start Day

Sunday

Start Month

Table 17. Daylight Saving 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. - 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. - Recurring—The settings will be in effect for the upcoming period and subsequent years. - 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.

Field	Description
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 24-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 24-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. 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 **Setup Network > User Management** 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 23. Logged In Sessions Tile

Logged In Sessions				Display: 10
Username	Connected From	Session Time	Session Type	
guest	10.4.82.2	39:07	HTTP	
1				

Table 18. Logged In Sessions Fields

Field	Description
Username	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 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. You can add up to five accounts. You can delete all accounts except for one Read/Write account.

Figure 24. User Accounts Tile

User Accounts								
☐	Username	▲ Access Level	Lockout Status	Password Expiration				
☐	admin	Read/Write	False	N/A				

Table 19. User Accounts Fields

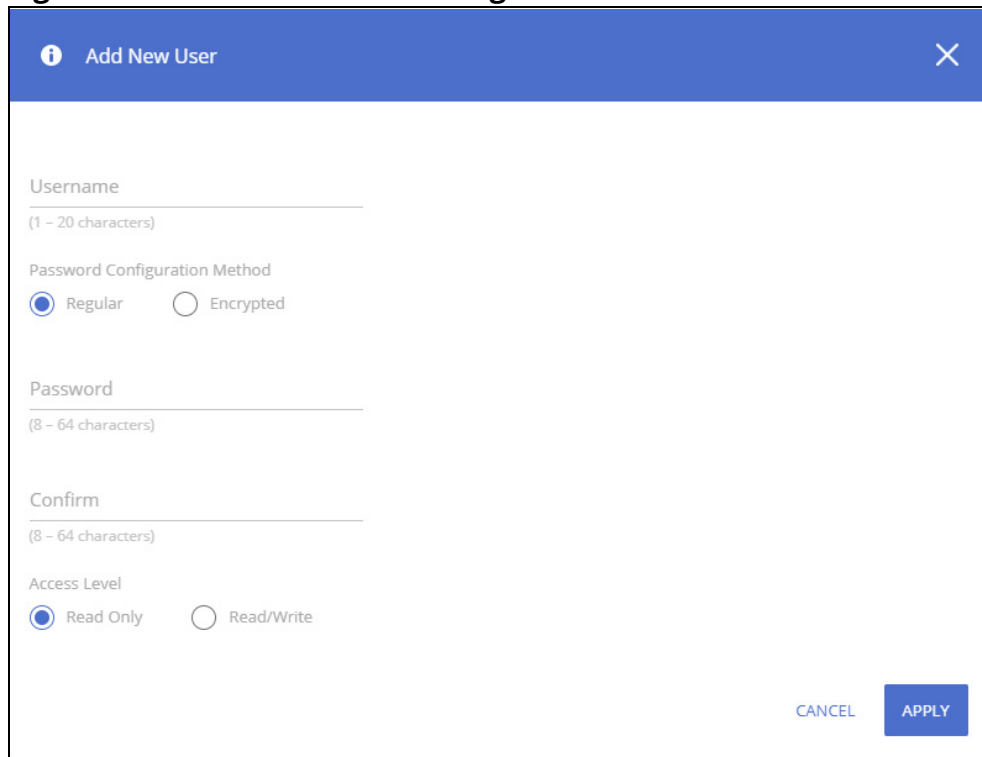
Field	Description
Username	A unique ID or name used to identify this user account.
Access Level	Indicates the access or privilege level for this user. The options are: - Read/Write - The user can view and modify the configuration. - Read Only - The user can view the configuration but cannot modify any 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 tile, 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, from the User Accounts tile, click the **Add Entry** button and configure the settings.

Figure 25. Add New User Dialog Box

The image shows a 'Add New User' dialog box with a blue header bar containing an information icon and a close button. The form fields include: 'Username' (1-20 characters), 'Password Configuration Method' (radio buttons for 'Regular' and 'Encrypted'), 'Password' (8-64 characters), 'Confirm' (8-64 characters), and 'Access Level' (radio buttons for 'Read Only' and 'Read/Write'). At the bottom right are 'CANCEL' and 'APPLY' buttons.

Add New User

Username
(1 – 20 characters)

Password Configuration Method
☒ Regular ☐ Encrypted

Password
(8 – 64 characters)

Confirm
(8 – 64 characters)

Access Level
☒ Read Only ☐ Read/Write

CANCEL APPLY

Configure the settings for the new user.

Table 20. New User Configuration Fields

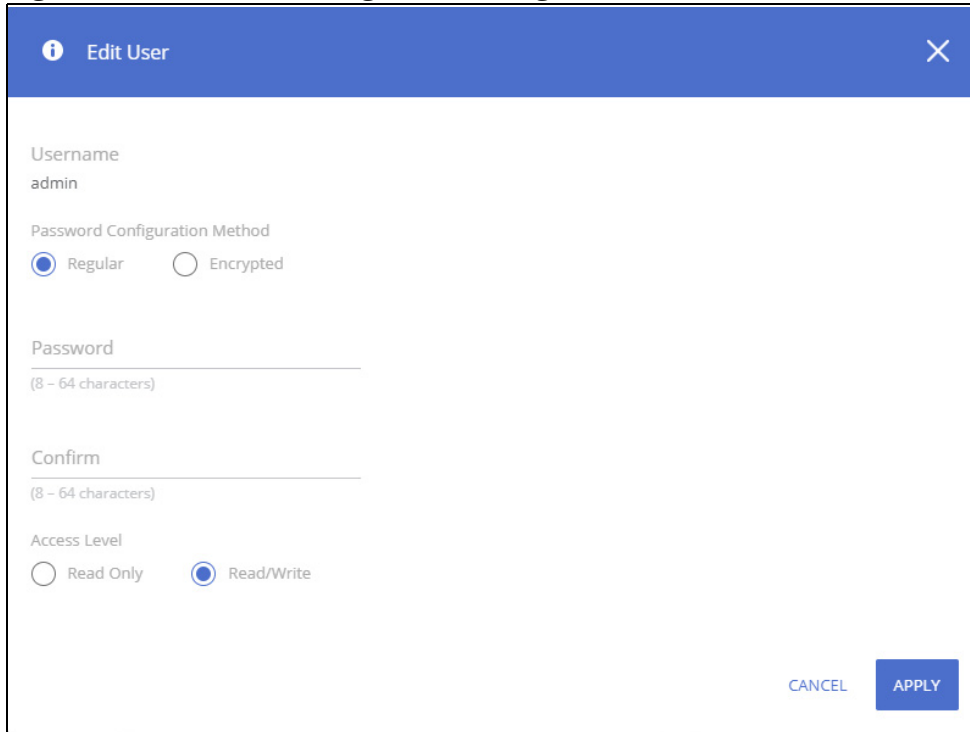
Field	Description
Username	Enter the name you want to give to the new account. (You can only enter data in this field when you are creating a new account.) Usernames are up to 20 alphanumeric characters in length and are not case sensitive. Valid characters include all the alphanumeric characters and the dash ('-') and underscore ('_') characters. Username <i>default</i> is not valid.
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 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 Only - The user can view the configuration but cannot modify any fields. - Read/Write - The user can view and modify the configuration.

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 26. Edit Existing User Dialog Box



The dialog box is titled "Edit User" with a blue header bar containing an information icon and a close button. The main content area is white and contains the following fields and options:

- Username:** A text field with the value "admin".
- Password Configuration Method:** Two radio buttons: "Regular" (selected) and "Encrypted".
- Password:** A text field with a placeholder "(8 - 64 characters)".
- Confirm:** A text field with a placeholder "(8 - 64 characters)".
- Access Level:** Two radio buttons: "Read Only" and "Read/Write" (selected).

At the bottom right, there are two buttons: "CANCEL" and "APPLY".

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 27. Account Security Settings Tile

The screenshot shows a configuration interface titled "Account Security Settings". It contains four settings:

- Password Aging:** A toggle switch that is turned on (blue).
- Password Aging Time:** A numeric input field set to "1", with a range of "(1 - 365) Days" indicated below it.
- Account Lockout:** A toggle switch that is turned on (blue).
- Lockout Attempts:** A numeric input field set to "1", with a range of "(1 - 5) Login Attempts" indicated below it.

Table 21. Account Security Settings Fields

Field	Description
Password Aging	Activate this 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 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 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 28. Password Strength Rules Tile

Password Strength Rules

Password Strength Enforcement

☒

Minimum Length

8

(0 - 64 characters)

Character Repetition Enforcement

☒

Maximum Number of Repeated Characters

1

(1 - 16)

Minimum Character Classes

0

(0 - 4)

Table 22. 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).
Character Repetition Enforcement	Enable or disable the character repetition enforcement feature. Enabling this feature limits the number of repeated characters allowed in the password.
Maximum Number of Repeated Characters	Specify the maximum number of repeated characters a password is allowed to include. An example of four repeated characters is <i>aaaa</i> .
Minimum Character Classes	Specify the minimum number of character classes a password must contain. There are four character classes: • Uppercase • Lowercase • Numbers • Special Characters

Password Keyword Exclusion

Use the Keyword Exclusion configuration option to add keywords that are not allowed as part of a password

Figure 29. Password Exclusion Tile

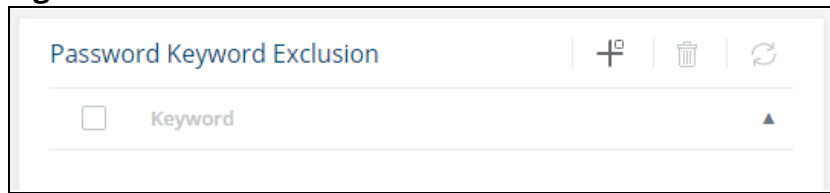


Table 23. Password Exclusion Field

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 Add, type the word to exclude in the Keyword Name field, and click APPLY. • To remove one or more keywords from the list, select each keyword to delete and click Remove.

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**.

DHCP Server

DHCP server is used for centralized control and automatic assignment of IP addresses to attached hosts. The DHCP server provides information on the IP address allocation, the DNS server address, default router, WINS server, and domain name.

The DHCP server can also provide a configuration file name and the IP address of the corresponding TFTP/SCP server so that this configuration file can be automatically downloaded to the station to which the IP Address is assigned.

Click **Setup Network > DHCP Server** to view or configure the DHCP server.

Global Configuration

A switch can operate as either a DHCP client (obtaining its own IP from a DHCP server), or as a DHCP server (allocate IP Addresses to stations). A switch with support for IP routing can operate as a DHCP Relay when the DHCP Server feature is disabled.

The DHCP server is configured with a predetermined pool of IP addresses from which it allocates IP addresses to DHCP clients.

The DHCP server supports DHCP options (0-254).

Figure 30. Global Configuration

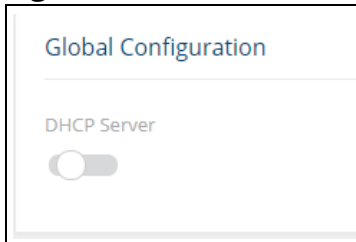


Table 24. Global Configuration Field

Field	Description
DHCP Server	Select Enabled or Disabled to administratively enable or disable this feature globally on the switch. A DHCP server cannot be enabled if DHCP client is enabled on any of the device interfaces. This feature is disabled by default.

If you modify these settings, click **APPLY** to update the switch configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Address Pool and Static Assignment Tile

This tile has two tabs:

- Address Pool - for configuring an address range or network mask of DHCP clients.
- Static Assignment - for manually binding IP addresses, based on hardware-address (MAC address) or on a client identifier.

To display these tabs, click **Setup Network > DHCP Server** in the navigation pane, and click on the appropriate tab.

Address Pool Tab

Use the Address Pool tab to configure the IP address pools for allocation.

Figure 31. Address Pool Tab

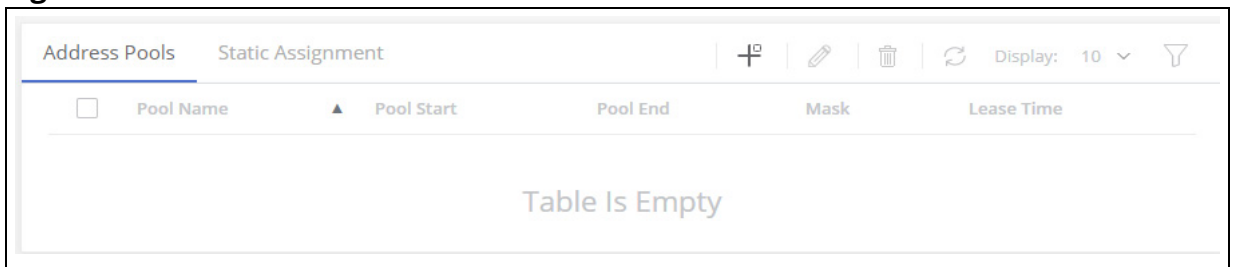
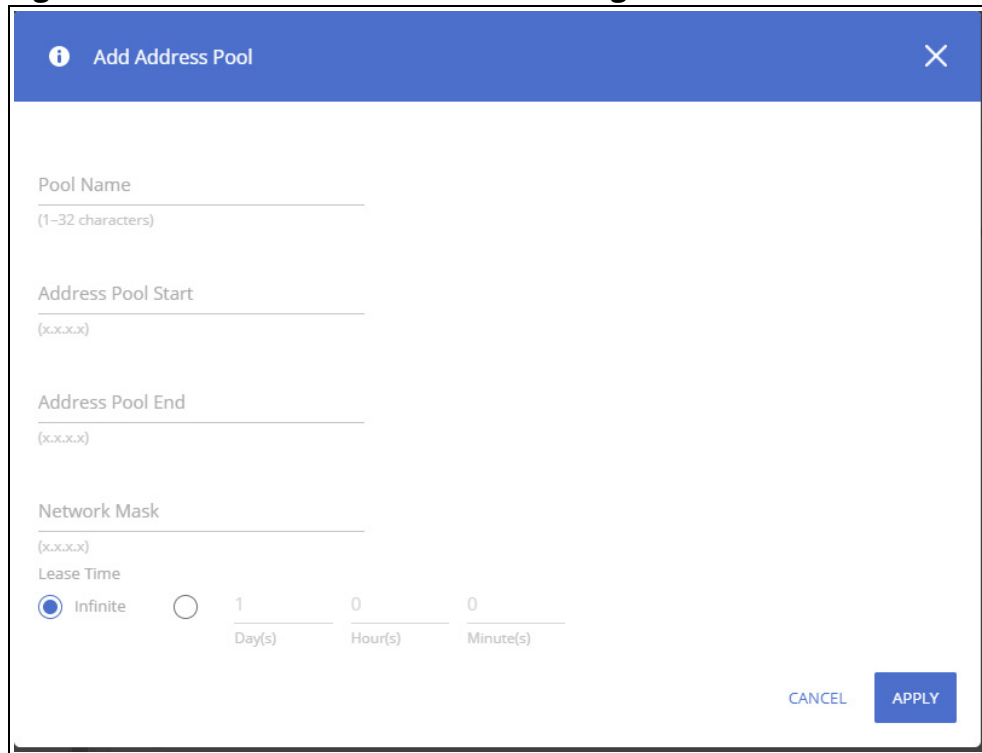


Table 25. Address Pool Tab Fields

Field	Description
Pool Name	The pool name.
Pool Start	The IP address of the first address in the pool.
Pool End	The IP address of the last address in the pool.
Mask	The network mask of the IP addresses.
Lease Time	The amount of time that the IP address is allocated.

Adding an Address Pool

To add a new address pool, from the Address Pool tab, click the **Add Entry** button  and configure the settings.

Figure 32. Add New Address Pool Dialog Box


The dialog box titled "Add Address Pool" contains the following fields and controls:

- Pool Name:** A text input field with a placeholder "(1-32 characters)".
- Address Pool Start:** A text input field with a placeholder "(x.x.x.x)".
- Address Pool End:** A text input field with a placeholder "(x.x.x.x)".
- Network Mask:** A text input field with a placeholder "(x.x.x.x)".
- Lease Time:** A section with a radio button for "Infinite" (which is selected) and a time picker for "Day(s)", "Hour(s)", and "Minute(s)". The time picker shows values of 1, 0, and 0 respectively.
- Buttons:** "CANCEL" and "APPLY" buttons at the bottom right.

Table 26. New Address Pool Configuration Fields

Field	Description
Pool Name	Enter a meaningful name for the Address Pool.
Address Pool Start	Enter the address of the first IP address in the address pool.
Address Pool End	Enter the address of the last IP address in the address pool.

Field	Description
Network Mask	Enter the network mask for the address pool.
Lease Time	Set either Infinite - for an unlimited lease time, or set the number of days, hours and minutes to limit the lease time.

Static Assignment Tab

Use the Static Assignment tab to configure static assignments for the DHCP address allocation.

Figure 33. Static Assignment Tab

Address Pools	Static Assignment					Display: 10	
☐	IP Address	Mask	ID Type	Identifier	Client Name		
Table Is Empty							

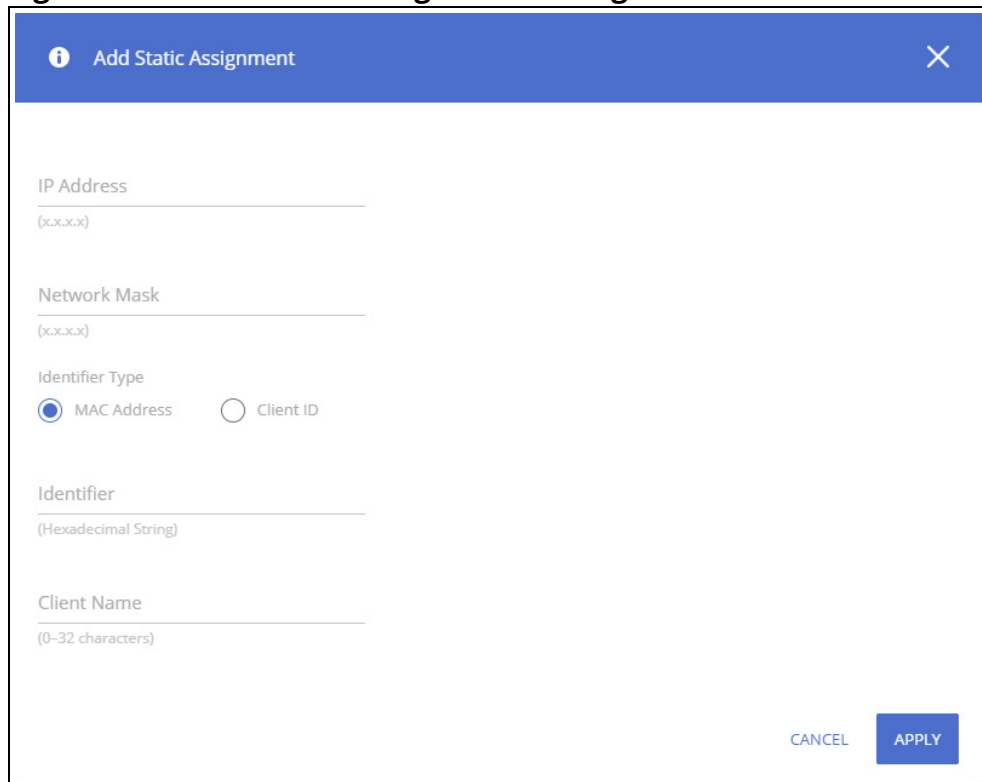
Table 27. Static Assignment Tab Fields

Field	Description
IP Address	The IP Address to assign to the DHCP client.
Mask	The network mask of the IP address.
ID Type	The type of identifier used for the client: hardware-address (MAC address), or client identifier.
Identifier	The Identifier of the client (value depends on the ID type).
Client Name	The name of the DHCP client.

Adding a Static Assignment

To add a new assignment, from the Static Assignment tab, click the **Add Entry** button and configure the settings.

Figure 34. Add Static Assignment Dialog Box



The dialog box is titled "Add Static Assignment" with an information icon on the left and a close icon on the right. It contains five input fields: "IP Address" with a placeholder "(x.x.x.x)", "Network Mask" with a placeholder "(x.x.x.x)", "Identifier Type" with two radio buttons labeled "MAC Address" (selected) and "Client ID", "Identifier" with a placeholder "(Hexadecimal String)", and "Client Name" with a placeholder "(0-32 characters)". At the bottom right are "CANCEL" and "APPLY" buttons.

Table 28. New Static Assignment Configuration Fields

Field	Description
IP Address	Enter the IP Address to assign to the DHCP client.
Network Mask	Enter the network mask for the IP address.
Identifier Type	Select MAC address, or Client ID
Identifier	Enter either the MAC address or the Client ID of the DHCP client.
Client Name	Enter a name for the client

DHCP Common Options and DHCP Custom Options Tile

This tile has two tabs:

- DHCP Common Options - for configuring the common options for a DHCP address pool. Common options are options that are frequently used and referenced by name.
- DHCP Custom Options - for configuring custom options. Custom options are referenced by Option ID.

To display these tabs, click **Setup Network > DHCP Server** in the navigation pane, scroll down and click on the appropriate tab.

DHCP Common Options Tab

Use the DHCP Common Options tab to configure the common options for the DHCP servers.

Figure 35. DHCP Common Options Tab

The screenshot shows the 'DHCP Common Options' tab, which is the active tab, with 'DHCP Custom Options' as a secondary tab. The configuration area includes several fields and a radio button group. The 'Pool Name' is set to 'new pool'. The 'Domain Name' field is empty, with a note '(0-32 characters)'. The 'Auto Gateway' toggle is turned on. The 'Gateway(s)', 'DNS Server(s)', 'SNTP Server(s)', and 'WINS Server(s)' fields are all empty, each with a note '(x.x.x.x)'. The 'NetBIOS Node Type' is set to 'Broadcast' via a selected radio button, with other options being 'Peer to Peer', 'Mixed', and 'Hybrid'. The 'File Server Address' and 'File Server Host Name' fields are empty, with notes '(x.x.x.x)' and '(0-64 characters)' respectively. The 'Boot File Name' field is empty, with a note '(0-128 characters)'.

DHCP Common Options	DHCP Custom Options
Pool Name new pool	
Domain Name (0-32 characters)	
Auto Gateway ☒	
Gateway(s) (x.x.x.x)	
DNS Server(s) (x.x.x.x)	
SNTP Server(s) (x.x.x.x)	
WINS Server(s) (x.x.x.x)	
NetBIOS Node Type ☒ Broadcast ☐ Peer to Peer ☐ Mixed ☐ Hybrid	
File Server Address (x.x.x.x)	
File Server Host Name (0-64 characters)	
Boot File Name (0-128 characters)	

Table 29. DHCP Common Options Tab Fields

Field	Description
Pool Name	The pool name.
Domain Name	The domain of the address pool.
Auto Gateway	If a default-gateway was not configured for the pool, this setting enables automatic transmission of the interface IP address as the default-gateway.
Gateways(s)	Configures the default router list for the DHCP client. Up to 8 default routers can be specified. The router IP address should be on the same subnet as the client subnet.
DNS Servers(s)	Specifies the Domain Name System (DNS) IP server list available to a DHCP client. Up to 8 servers are supported.
WINS Servers(s)	Specifies the NetBIOS Windows Internet Naming Service (WINS) server list that is available to Microsoft DHCP clients. Up to 8 servers are supported.
NetBIOS Node Type	Set the the NetBIOS node type for Microsoft DHCP clients. Available types are: • Broadcast • Peer-to-peer • Mixed • Hybrid (the default)
File Server Address	The address of the next server (siaddr) in the boot process of the DHCP client.
File Server Host Name	The name of the next server (siaddr) in the boot process of a DHCP client.
Boot File Name	The file name of the boot image file for the DHCP client.

DHCP Custom Options Tab

Use the DHCP Custom Options tab to configure the custom options for the DHCP address pool.

Figure 36. DHCP Custom Options Tab

DHCP Common Options		DHCP Custom Options			+ edit delete refresh Display: 10	
☐ Pool Name	▲ Option Code	Type	Value	Description		
Table Is Empty						

Table 30. DHCP Custom Options Tab Fields

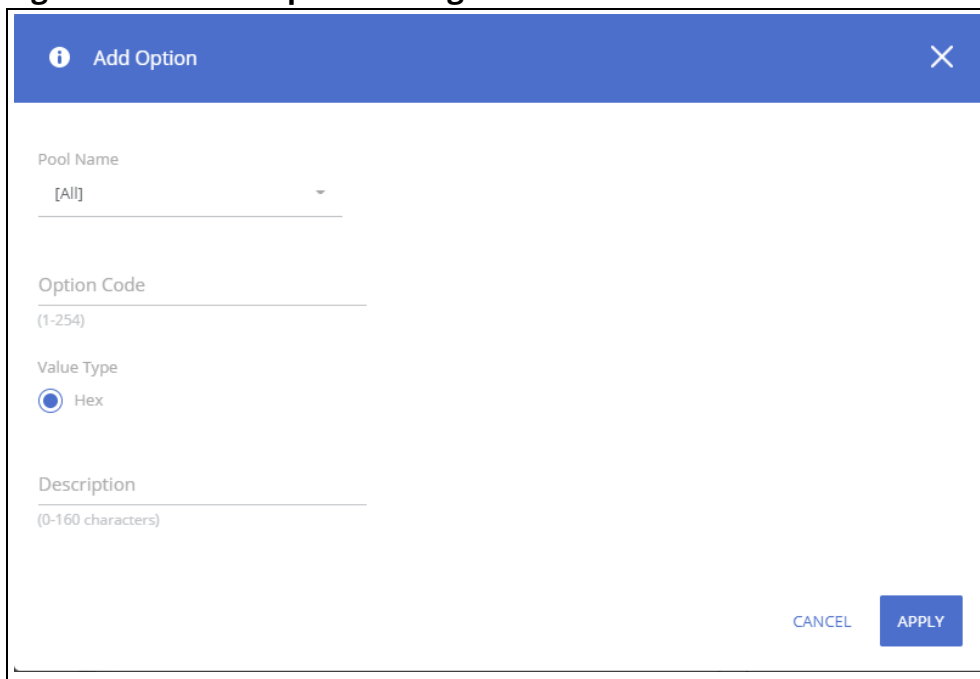
Field	Description
Pool Name	The DHCP address pool name.
Option Code	The DHCP Option code, range 1-254, except for the following: 1, 3-4, 6, 12, 15, 44, 46, 50-51, 53-54, 56, 66-67, 82, and 255.

Field	Description
Value Type	The type of option. Available DHCP option types: • boolean: 19, 20, 27, 29-31, 34, 36 and 39 • integer: 2, 13, 22-26, 35, 37-38, 132-134, and 211 The switch checks the value range and builds the value field of the size defined by the option code. • ascii: 14, 17-18, 40, 64, 130, 209, and 210 • ip: 16, 28, 32, 128-129, 131, 135, and 136 • ip-list: 5, 7-11, 33, 41, 42, 45, 48, 49, 65, 68-76, and 150. Up to 8 IP addresses can be configured • hex: 1-254 except for the following: 1, 3-4, 6, 12, 15, 44, 46, 50-51, 53-54, 56, 66-67, 82, and 255. The switch does not validate the syntax of an option defined by this format.
Value	The value to set for this option.
Description	A description of the custom option.

Adding a Custom DHCP Option

To add a new custom DHCP custom option, from the DHCP Custom Options tab, click the **Add Entry** button  and configure the settings.

Figure 37. Add Option Dialog Box



The dialog box titled "Add Option" has a blue header bar with an information icon and a close button. It contains four input fields: "Pool Name" with a dropdown menu showing "[All]", "Option Code" with a range of "(1-254)", "Value Type" with radio buttons for "Hex" (selected) and "Integer", and "Description" with a range of "(0-160 characters)". At the bottom right, there are "CANCEL" and "APPLY" buttons.

Table 31. Add Option Configuration Fields

Field	Description
Pool Name	Select a pool name from the drop-down list.

Field	Description
Option Code	The DHCP Option code. range 1-254, except for the following: 1, 3-4, 6, 12, 15, 44, 46, 50-51, 53-54, 56, 66-67, 82, and 255
Value Type	The type of option. The selected type is based on the value entered in the option code, according to the following: - boolean: 19, 20, 27, 29-31, 34, 36 and 39 - integer: 2, 13, 22-26, 35, 37-38, 132-134, and 211 The switch checks the value range and builds the value field of the size defined by the option code. - ascii: 14, 17-18, 40, 64, 130, 209, and 210 - ip: 16, 28, 32, 128-129, 131, 135, and 136 - ip-list: 5, 7-11, 33, 41, 42, 45, 48, 49, 65, 68-76, and 150. Up to 8 IP addresses can be configured - hex: 1-254 except for the following: 1, 3-4, 6, 12, 15, 44, 46, 50-51, 53-54, 56, 66-67, 82, and 255. The switch does not validate the syntax of an option defined by this format.
Value	Enter an appropriate value for the option type.
Description	A description of the custom option.

Excluded Addresses Tile

Use the Excluded Addresses tile to list IP addresses that a DHCP server must not assign to DHCP clients.

Figure 38. Excluded Addresses Tile



Table 32. Excluded Addresses Fields

Field	Description
Address range	The address range that a DHCP server must not assign to DHCP clients.

Adding an Excluded Address Range

To add an excluded address range entry to the list, from the Excluded Addresses Tile, click the **Add Entry**  button, and configure the settings.

Figure 39. Add Excluded Address Range Dialog Box

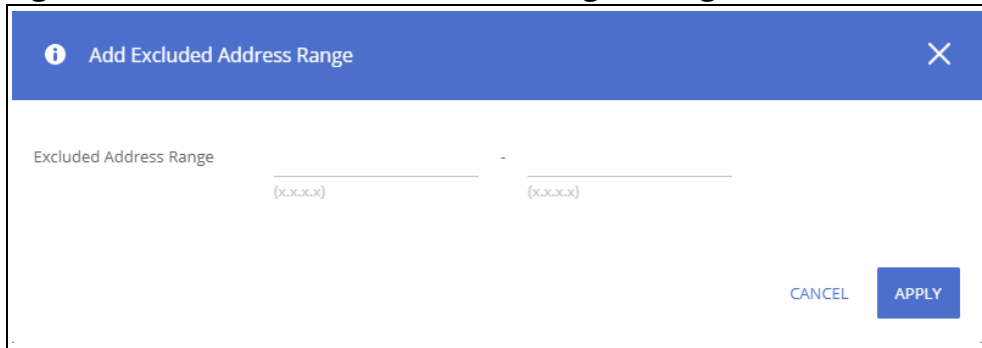
A dialog box titled "Add Excluded Address Range" with a blue header bar containing an information icon and a close button. The main area has a label "Excluded Address Range" followed by two input fields separated by a hyphen. Below each input field is a placeholder "(x.x.x.x)". At the bottom right are "CANCEL" and "APPLY" buttons.

Table 33. Add Excluded Address Range Configuration Fields

Field	Description
Excluded Address Range	Enter the start and end of the range of addresses a DHCP server must not assign to DHCP clients.

To remove an excluded address range entry to the list, select the entry and click **Remove**  .

Leased Addresses Tile

The Leased Addresses tile list addresses that are leased by the DHCP server to DHCP clients.

Figure 40. Leased Addresses Tile

A screenshot of the "Leased Addresses" tile. It has a title bar with a trash icon, a refresh icon, and a "Display: 10" dropdown. Below the title bar is a table header with columns: Address, Client ID, Expiration, Type, and Status. The table body is empty, and the text "Table Is Empty" is displayed in the center.

Table 34. Leased Addresses Fields

Field	Description
Address	The address that is leased.
Client ID	The client ID of the DHCP client.
Expiration	The date and time of the lease expiration.
Type	The manner in which the IP address was assigned to the host. (Dynamic, Static or Automatic)
Status	The status of the IP address allocation (allocated, expired, declined and pre-allocated)

Schedule Configuration

The switch provides three 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 - to set the time ranges when PoE power is provided.
- Port Admin status - to set the time ranges when the port is operationally enabled.
- ACEs - to set the time ranges when the ACE is active.

Click **Setup Network > Schedule** to view or configure the schedules.

Schedules

Figure 41. Schedules Tile

Schedules

The system time is currently set manually. It is recommended to use SNTP to set the system time when using the scheduling feature.

Schedule Name
Schedule-1

Type	Start	Ends
☐ Absolute	08:00 June 08, 2021	20:00 June 08, 2021
☐ Periodic	07:00 Mon	08:00 Mon

Table 35. Schedule Fields

Field	Description
Schedule Name	Select the schedule to view from the drop-down list to display information on time periods configured for the schedule, if any.
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. • 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.
Start	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.

Field	Description
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.

To configure a new time entry for a schedule, click **Add**  .



Schedules require setting the system clock manually, or via SNTP. SNTP provides better accuracy.

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 Entry** button  and configure the settings.

Figure 42. Add Schedule Dialog Box - Absolute Schedule

 Add Schedule (Absolute) 

Type

☒ Absolute ☐ Periodic

Start Time

☐

Start Date



Start Time of Day



End Time

☐

End Date



End Time of Day



CANCEL

APPLY

Figure 43. Add Schedule Dialog Box - Periodic Schedule

Add Schedule (Periodic)

Type

☐ Absolute ☒ Periodic

Start Day

Monday

Start Time of Day

08:00

End Day

Thursday

End Time of Day

10:00

CANCEL APPLY

Table 36. New Schedule Configuration Fields

Field	Description
Type	The type of schedule. Can be one of the following: - Absolute. There can 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.

Field	Description
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  .

DNS Configuration

The DNS protocol controls the Domain Name System (DNS), by which host names can be mapped to IP addresses. When DNS is configured on a switch, the host name can be substituted for the IP address with all IP commands. The DNS client retrieves this information from a DNS server.

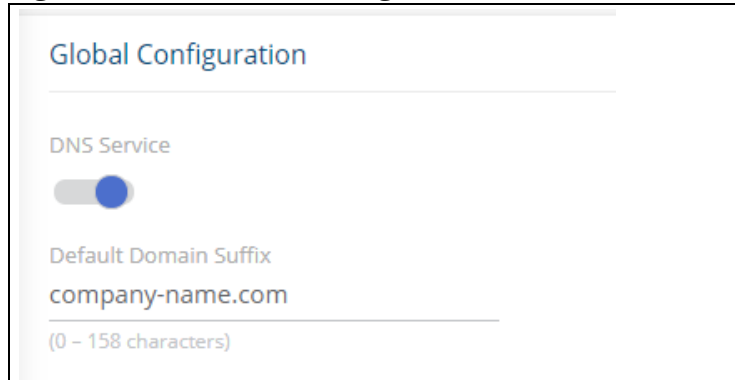
A default domain name can be configured either statically, or by using DHCP. The system can store up to eight DNS servers. Servers can be learned dynamically by DHCP client or configured statically. DNS will send a query to all reachable servers, the first server to provide a valid answer is inserted into the cache (and returned to the user). The rest are discarded.

Queried names are saved to a local DNS cache. Cache size is 64 entries. You can statically map a DNS hostname to 4 IPv4 or IPv6 addresses.

Click **Setup Network > DNS Configuration** to view or configure the DNS.

Global Configuration

Figure 44. Global Configuration



Global Configuration

DNS Service

☒

Default Domain Suffix

company-name.com

(0 - 158 characters)

Table 37. Global Configuration Fields

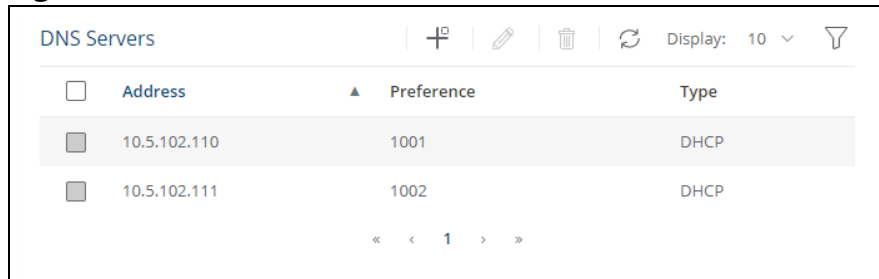
Field	Description
DNS Service	Select Enabled or Disabled to administratively enable or disable this feature globally on the switch. This feature is enabled by default.
Default Domain Suffix	The default domain suffix is appended to host names that do not include a dot. The device supports Domain Name Lookup for all applications and servers such as ping, trace route, TACACS server, RADIUS server, SNMP server, Syslog server, TFTP server, and DHCP server.

If you modify these settings, click **APPLY** to update the switch configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

DNS Servers

Use the DNS Servers tile to configure up to 8 DNS servers. To display this tile, click **Setup Network > DNS Configuration** in the navigation pane.

Figure 45. DNS Servers Tile



DNS Servers

Display: 10

☐	Address	Preference	Type
☒	10.5.102.110	1001	DHCP
☒	10.5.102.111	1002	DHCP

« < 1 > »

Table 38. DNS Server Fields

Field	Description
Address	The address of the DNS server.
Preference	The priority of the DNS server.
Type	The type of DNS server. Valid types are: - DHCP - Static

To add a DNS server, click **Add** .

To edit an existing DNS server, click the check box to the left of the DNS server entry and click **Edit** .

To remove an existing session, click the check box to the left of the DNS server entry and click **Remove** .

Manual Host Mapping

Use the Manual Host Mapping tile to statically map up to four IPv4 or IPV6 addresses per host. This mapping is kept in the local host and not in the remote server and limited to 64 mappings.

To display this tile, click **Setup Network > DNS Configuration** in the navigation pane.

Figure 46. Manual Host Mapping Tile

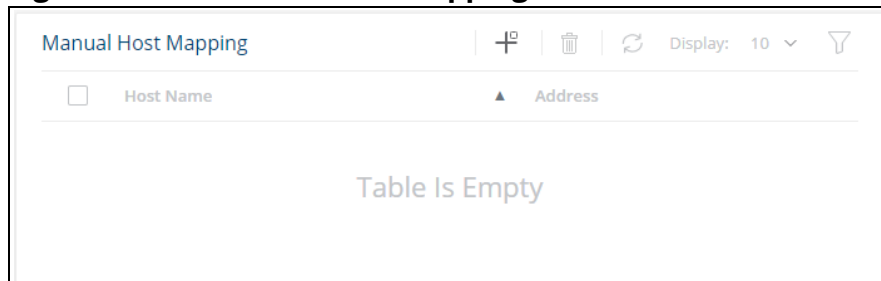


Table 39. Manual Host Mapping Fields

Field	Description
Host Name	The name of the host.
Address	The IPv4 or IPv6 address of the host.

To add a host mapping, click **Add** .

To remove an existing mapping, click the check box to the left of the mapping entry and click **Remove** .

DNS Resolutions

Use the DNS Resolutions tile to view the DNS resolutions.

To display this tile, click **Setup Network > DNS Configuration** in the navigation pane.

Figure 47. DNS Resolutions Tile



The screenshot shows a web interface titled "DNS Resolutions". It features a table with five columns: "Host Name", "Address", "Type", "TTL", and "Status". The table is currently empty, and the text "Table Is Empty" is displayed in the center. Above the table, there are icons for refresh, print, and a filter icon, along with a "Display: 10" dropdown menu.

Table 40. DNS Resolutions Fields

Field	Description
Host Name	The name of the host.
Address	The IPv4 or IPv6 address of the host.
Type	IPv4 or IPv6 address.
TTL	Time until the entry expires.
Status	The status of the DNS resolution.

To clear dynamic resolutions, click **Clear Dynamic** .

Stacking Configuration

Stacking enables connecting multiple physical devices, through stack ports, to one logical device. All units in the stack are managed as one logical device:

- One management session for all units
- All ports and units are configured as a single entity
- Stack capacity (ports and units) can be changed dynamically

The stacking feature supports the following attributes and settings:

- Stack model based on a single conductor, optionally a conductor backup unit and multiple stack member units
- Up to 4 units in a stack (unit ID 1-4)
- Automatic, or user-defined unit ID
- Up to 4 stacking interfaces on each unit.
- Stacking interface can have multiple members (Stacking LAG)
- Native or hybrid mode

- Chain or ring topology

Click **Setup Network > Stacking Configuration** to view or configure the stack.

By default, switch ports are not configured as stacking interfaces. Configuring a switch port as a stacking interface requires unit reload. Any switch port can be configured as stacking interface - 10G ports and also 1G ports on the access switch. Stack interfaces are functional only if connected to a same speed link partner (1G to 1G or 10G to 10G).

Up to 4 switch ports can be configured as stacking interfaces. If two devices are connected by both 10G and 1G stacking interfaces, then the 10G stack interface are active stacking links and the 1G interfaces are in standby. The 1G interfaces will become active stack links only if all the 10G interfaces are disconnected, or down.

Stacking interfaces are not treated as regular switch ports. These ports are not visible in the tiles for configuring trunk group members, network trunk members, or VLAN members.

If a configuration is applied to a switch port and then the switch port is set as a stack interface - the switch port settings are retained in the running configuration, but are inactive. These settings will become active once the switch port is removed from stacking interface list.

Stacking LAG

The switch supports connecting multiple stacking interfaces between two units in the stack. This is referred to as stack LAG. These are the advantages of stacking LAG:

- Increasing the stack bandwidth between stack members.
- Improved redundancy of the stack connection.

When two neighboring units are connected, the stacking interfaces connecting them are automatically assigned to a stack LAG.

There can be up to two stack LAGs on each unit:

- One LAG for the uplink device
- One LAG for the downlink device

Once multiple stacking interfaces are connected between units, the physical topology is detected automatically, and the stack LAG is formed accordingly. The stack interfaces are automatically assigned to stack lags according to unit uplink/downlink connectivity.

The LAG implements traffic load-balancing between its ports, using the same algorithm as the algorithm set for the standard switch LAG. When a stack interface fails, traffic is redistributed between remaining ports.

Only one LAG is used between any two directly connected units. A stack LAG must contain ports of the same speed.



Star topology is not supported - only two stack LAGs can be active on each stack unit.

A stack interface can be in one of the following states:

- Down port - operational status is down

- Active-stack port - port was added to a stack LAG
- Standby-stack port - operational status is up but the port cannot be added to a stack LAG, and the port does not pass traffic. This can happen due to the following:
 - o Stack ports with different speeds connect to a single neighbor
 - o More than two stack members are connected to the same unit

When connecting more than two stack members to a single unit, only two stack LAGs are active, the rest of the stacking ports are in "standby" state. The criteria that is used to choose the stack LAG that is active (by order of appearance):

1. Unit is connected to the Conductor unit.
2. Unit is connected to the backup unit.
3. Maximum bandwidth.
4. Unit is connected to the unit with lowest MAC address.

Disconnecting one of the active neighbor units enables a stack LAG in "standby" state, to become active and for the "new" unit to connect to the stack.

Global Settings

Figure 48. Global Configuration

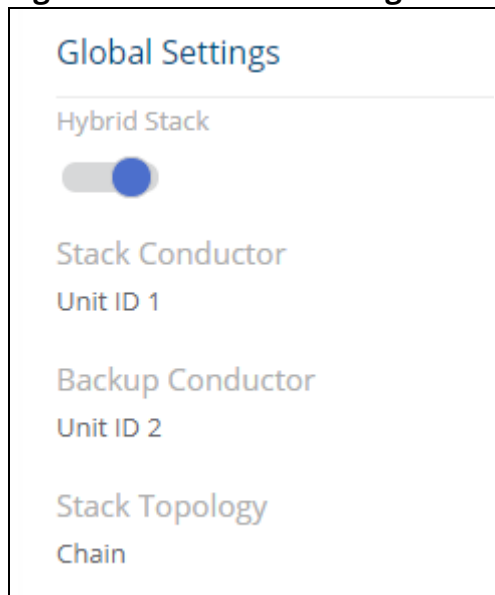


Table 41. Global Settings Fields

Field	Description
Hybrid Stack	Enable this feature if you need to mix both switch types in the stack: • Access switches - 24 or 48 1G network interfaces with 4 10G uplink interfaces • Aggregate switches - 16 10G interfaces When using this feature, each unit in the stack must be set to "Hybrid" mode stack. Non-hybrid units are shutdown and do not join the stack. Table sizes and other settings of the Hybrid stack are based on the lowest denominator between the two SKUs (in most cases the Access switch parameters). Setting this feature requires device reboot and automatically erases device/stack configuration. Deselecting this feature requires reboot but does not require removal of device configuration. By default, this setting is disabled.
Stack Conductor	Indicates if unit 1 or 2 is the stack Conductor.
Backup Conductor	Indicates if unit 1 or 2 is the stack Backup Conductor, or if the stack does not include a backup conductor .
Stack Topology	Indicates the stack topology - either ring or chain.

Unit Numbering

This tile enables setting the unit IDs after reset.

Figure 49. Unit Numbering

The screenshot shows a configuration page titled "Unit Numbering". It contains four sections, each with a label and a dropdown menu:

- Unit 1 ID After Reset**: The dropdown menu shows the value "1".
- Unit 2 ID After Reset**: The dropdown menu shows the value "2".
- Unit 3 ID After Reset**: The dropdown menu shows the value "3".
- Unit 4 ID After Reset**: The dropdown menu shows the value "4".

Table 42. Unit Numbering Fields

Field	Description
Unit 1 ID after Reset	Select from the drop-down list. The available values are Auto and 1-4. A specific unit ID can be configured for only 1 unit.
Unit 2 ID after Reset	
Unit 3 ID after Reset	
Unit 4 ID after Reset	

Stacking Port Configuration

This tile enables configuring the stack ports.

Figure 50. Stacking Port Configuration

Stacking Port Configuration				
Unit ID	Role	Current Stacking Ports	Stacking Ports After Reset	
☐ 1	Conductor	49,50,51,52	49,50,51,52	
☐ 2	Backup	25,26	25,26	
☐ 3	Member	15,16	15,16	
☐ 4	Member	25,26,27,28	25,26,27,28	

Table 43. Stacking Port Configuration Fields

Field	Description
Unit ID	Indicates the unit ID of the unit (1-4).
Role	The role of the unit (Conductor, Backup or Member)
Current Stacking Ports	The stacking links currently configured for use.
Stacking Ports After Reset	The stacking links configured for use after device reset.

To edit a stacking port(s), select the unit(s) to edit and click the **Edit** button  and edit the configuration.

Figure 51. Edit Stacking Ports Dialog Box

Unit ID
2

Stacking Ports

Left List	Right List
1	25
2	26
3	
4	
5	
6	
7	
8	

CANCEL APPLY

Table 44. Edit Stacking Ports Fields

Field	Description
Unit ID	The ID(s) of the selected unit(s)
Stacking Ports	Move ports that should be stacking ports to the list on the right. Move ports that should not be stacking ports to the list on the left. A unit in a stack must have 2, 3, or 4 stacking ports.

You can use the Switching pages to configure port operation and various Layer 2 features and capabilities.

Port Configuration

You can use the Port Configuration tiles to display port status, configure port settings, and view statistics on packets transmitted on the port.

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

Graphical Display

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 in this screen, to open the **Switching > Port Configuration** page. If the port is a trunk member, the **Switching > Trunk Configuration** appears.

For more information, see [Switch Panel View](#).

Global Configuration

These are the global configuration options that you can set:

Figure 52. Global Configuration

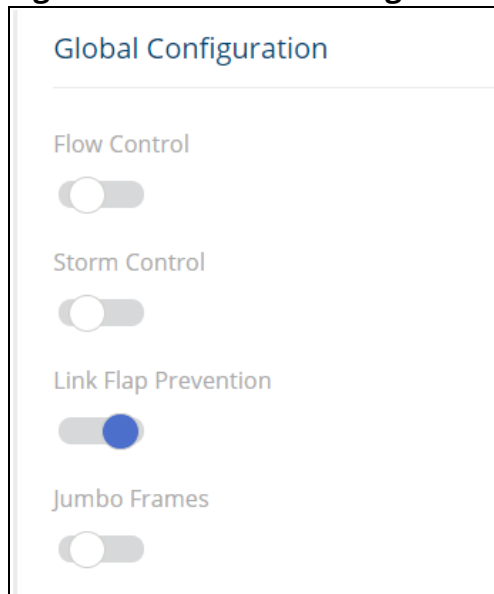


Table 45. Global Configuration Fields

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.
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. When enabled, the following storm control settings are applied to all switch interfaces: • Storm Control rate limit - 5% of interface speed. The limit is applied separately to each type of storm control - unicast (including unknown unicast), multicast or broadcast. • Packets that exceed the threshold limits are dropped.
Link Flap Prevention	A link-flap event is triggered if an interface changes its link state (link-up or link-down event) 3 or more times a second - for 10 seconds or more. In such a case, the port is suspended and the following syslog message and SNMP trap are generated: %LINK-W-PORT_SUSPENDED: Port <port number> suspended by link-flapping Where <port number> is the number of the port that was suspended. A port that is suspended 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 may attempt to manually recover the port in the Suspended Interface tile on the Switching > Interface Auto Recovery page.

Field	Description
Jumbo Frames	Sets both MTU and MRU values • If disabled - frame size is limited to 1518 bytes • If enabled - - For bridging: frame size is limited to 10240 bytes. - For Routing: frame size is limited to 9000 bytes Changing this setting requires saving the configuration and rebooting the switch. The new setting is applied only after reboot.



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.



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.



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 53. Interface Configuration Tile

Interface Configuration										
☐ Interface ▲	Description	Type	Admin Mode	Schedule	Physical Mode	Physical Status	Auto Negotiation Capabilities	STP Mode	LACP Mode	Link Status
☐ 1		Normal	Enabled	None	Auto	Unknown	10h 10f 100h 100f 1000f	Enabled	N/A	Link Down
☐ 2		Normal	Enabled	None	Auto	Unknown	10h 10f 100h 100f 1000f	Enabled	N/A	Link Down
☐ 3		Normal	Enabled	None	Auto	Unknown	10h 10f 100h 100f 1000f	Enabled	N/A	Link Down
☐ 4		Normal	Enabled	None	Auto	Unknown	10h 10f 100h 100f 1000f	Enabled	N/A	Link Down

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 (also known as Trunk), 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. The possible values are: - Enabled: Administratively enabled. - Disabled: Administratively disabled.
Schedule	The schedule for activation of certain switch features, as defined in Schedule Configuration .
Physical Mode	The port speed and duplex mode. If the mode is Auto, all the port capabilities are advertised, and the duplex mode and speed are set from the auto-negotiation process.
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 Negotiation Capabilities	Indicates the list of configured capabilities for a port when Auto Negotiate is enabled. The Capability status for a trunk is not reported.
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: - Enabled - Spanning tree is enabled for this port. - Disabled - Spanning tree is disabled for this port.
LACP Mode	Indicates the Link Aggregation Control Protocol administration state. This field can have the following values: - Enabled: The port is a Trunk member. Trunk is an LACP Trunk. - Disabled: The port is a Trunk member. Trunk is a Static Trunk (not LACP). - N/A: The port is not a member of a Trunk, or port type is Trunk (TRK).
Link Status	Indicates the link status of the port. The possible values are: - Link up. - Link down. - Suspended: Automatically disabled by the system due to schedule configurations, or error conditions. For example, an interface may be disabled by the switch due to an error condition. See the error logs for more information.

Modifying Interface Settings

To change the port configuration of one or more interfaces, 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 54. Edit Port Configuration Dialog Box

Edit Port Configuration

Interface
1/1

Admin Mode
☒

Schedule
None

STP Mode
☒

Link Trap
☒

Physical Mode
Auto Negotiate

Negotiation Values
☒ 10M ☒ 100M ☒ 1G

Description
(0 - 64 characters)

Storm Control Limits

Broadcast Storm Control
☒

Broadcast Storm Control Limit Type
☒ Percent ☐ Rate

Broadcast Storm Control Limit
5
(1 - 100)

Broadcast Storm Control Action
None

Multicast Storm Control
☒

Multicast Storm Control Limit Type

CANCEL APPLY

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**.

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.
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.
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.
Description	Describe the interface to help identify it.
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 kbits per second. Valid values are 1-100. The default is 5.
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 kbits per second. Valid values are 1-100. The default is 5.
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.

Field	Description
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 kbits per second. Valid values are 1-100. The default is 5.
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.

Interface Statistics

The Interface Statistics tile 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 Interface Statistics tile, click **Switching** > **Port Configuration** in the navigation pane and scroll down to the **Interface Statistics** tile.

Figure 55. Interface Statistics Tile

☐ Interface ▲	Received Packets w/o Error	Received Packets with Error	Broadcast Received Packets	Transmitted Packets	Collisions	Transmitted Pause Frames	Received Pause Frames
☐ 1	2	0	0	61187	0	0	0
☐ 2	2	0	0	61187	0	0	0
☐ 3	61187	0	5881	2	0	0	0
☐ 4	2	0	0	61187	0	0	0
☐ 5	2	0	0	61187	0	0	0

Table 48. Interface Statistics Fields

Field	Description
Interface	The port or trunk ID.
Received Packets w/o Error	The count of packets received on the port without any packet errors.
Received Packets with Error	The count of packets received on the port with errors.
Broadcast Received Packets	The count of broadcast packets received on the port.

Field	Description
Transmitted Packets	The number of packets transmitted out of the port.
Collisions	The number of packet collisions.
Transmitted Pause Frames	The number of Ethernet pause frames transmitted. This information is collected for ports but not for trunks.
Received Pause Frames	The number of Ethernet pause frames received. This information is collected for ports but not for trunks.

Select a row and click **Clear**  to reset the row counters to zero.

Click **Clear All**  to reset all counters to zero.

Port Mirroring and Remote 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 probe port (also known as destination port).

All traffic from the source interfaces can be mirrored and sent to the probe port. A network protocol analyzer is typically connected to the destination port. Multiple switch ports can be configured as source interfaces, with each port mirrored to the same probe port.

Remote Port Mirroring (RSPAN) enables mirroring packets to a monitor VLAN, and flow over the network to a remote device to which the monitor station is connected.

RSPAN works by mirroring the traffic from the source ports of an RSPAN session onto a VLAN that is dedicated for the RSPAN session. This VLAN is then trunked to other switches, allowing the RSPAN session traffic to be transported across multiple switches. On the switch that contains the destination port for the session, traffic from the RSPAN session VLAN is simply mirrored out the destination port.

There are three switch functionalities in the RSPAN setup:



The RSPAN VLAN must be the same on all switches (source, intermediary and destination).
All traffic into a RSPAN VLAN is tagged and MAC learning is disabled in a RSPAN VLAN.

Source Switch

The switch on which traffic is captured/mirrored. The RSPAN session in the source switch consists up to 8 source interfaces and a single remote destination session.

The source session defines one port/LAG and the traffic type (Tx, Rx, or both) that should be mirrored, or the source VLAN to be mirrored.



The VLAN - RSPAN VLAN cannot be a source Mirrored VLAN.

The remote destination session defines the RSPAN VLAN_ID and reflector port through that the mirrored traffic is sent to the RSPAN VLAN.



The reflector port cannot be a member of the remote VLAN.
The reflector port is configured to also pass network/VLAN traffic in addition to traffic capture.
Other ports on the switch can be members of Remote VLAN, but only as a tagged member.

Destination Switch

The destination switch to which the monitoring station is connected

The RSPAN session in the destination switch consists of up to 8 sources (including remote VLANs) and one destination session with the same session number. The source session defines the RSPAN VLAN from which traffic should be mirrored to the destination port.

Source ports (for mirrored traffic) must be members of RSPAN VLAN. The destination session defines the destination port.



It is recommended not to configure the destination port as a member of the RSPAN VLAN.

Intermediate Switch

All the switches in the network between the Source Switch and Destination Switch.

The RSPAN settings need to be configured on all the intermediate switches creating the "path" between source and destination switch.

You need to define at least two ports that are tagged members of the RSPAN VLAN. One port will be connected "towards" the source switch, the other port "towards" the destination switch. Traffic will pass through the switch via the RSPAN VLAN.



It is recommended to remove RSPAN VLAN membership from all ports that are not part of the RSPAN topology.

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



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

Figure 56. Global Configuration Tile

Global Configuration

Remote Mirroring

Remote Mirroring VLAN

Table 49. Global Configuration Fields

Field	Description
Remote Mirroring	When enabled, remote mirroring is enabled on the device
Remote Mirroring VLAN	Enter the VLAN of the device to use for remote mirroring.

Mirroring Sessions

To display the Mirroring Sessions tile, click **Switching** > **Port Mirroring** in the navigation pane. The Mirroring Sessions tile appears.

Figure 57. Mirroring Sessions Tile

Mirroring Sessions

Display: 10

Session ID	Probe Interface	Source	Direction
------------	-----------------	--------	-----------

Table 50. 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. NOTE: You can configure multiple source ports or one source VLAN per session. VLANs can be defined as sources only in Session ID 1.

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.

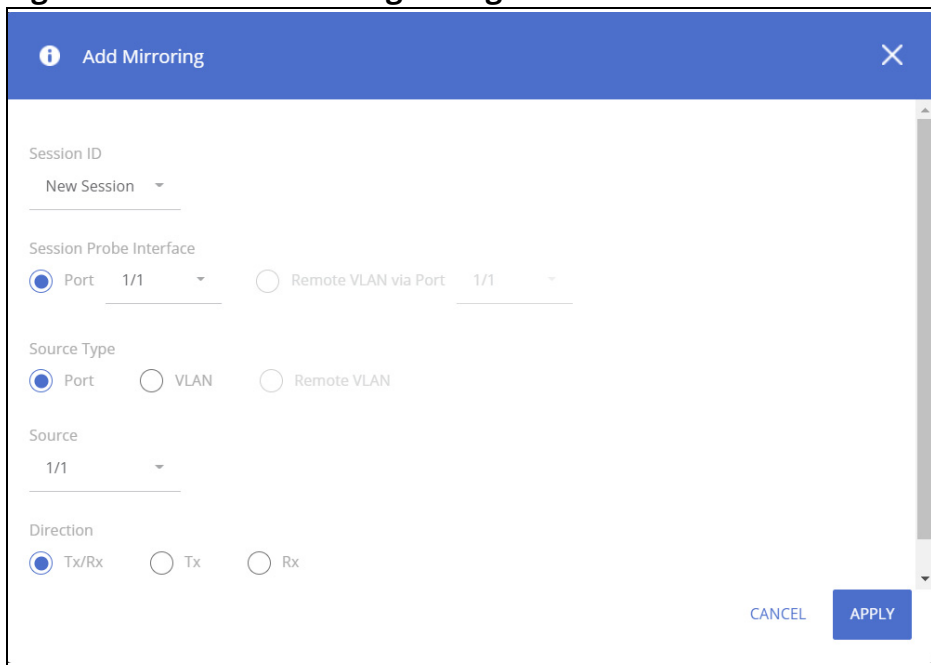
Configuring a Port Mirroring Session

To add a session in the **Mirroring Sessions** pane, click **Add** .

To edit an existing session, click the check box to the left of the session entry and click **Edit** .

To remove an existing session, click the check box to the left of the session entry and click **Remove** .

Figure 58. Add Mirroring Dialog Box



The dialog box titled "Add Mirroring" contains the following fields and options:

- Session ID:** A dropdown menu with "New Session" selected.
- Session Probe Interface:** Two radio buttons. "Port" is selected with a dropdown menu showing "1/1". "Remote VLAN via Port" is unselected with a dropdown menu showing "1/1".
- Source Type:** Three radio buttons. "Port" is selected. "VLAN" and "Remote VLAN" are unselected.
- Source:** A dropdown menu showing "1/1".
- Direction:** Three radio buttons. "Tx/Rx" is selected. "Tx" and "Rx" are unselected.
- Buttons:** "CANCEL" and "APPLY" buttons at the bottom right.

Figure 59.

Table 51: Add Mirroring Dialog Box Fields

Field	Description
Session ID	The identifier for the session being configured. For a new session, the ID is New Session.
Session Probe Interface	The physical port to use as the source probe port to which traffic will be mirrored.
Remote VLAN via Port	Set this to monitor traffic via remote VLAN using the specified port.

Field	Description
Source Type	The type of interface to use as the source: - Port – Traffic is mirrored to and/or from a physical port on the switch. - 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. - Remote VLAN - Traffic to a configured remote VLAN is mirrored.
Source	Specify the source interfaces for mirrored traffic. interface type depends on the value set in the Source Type field.
Direction	The direction of traffic on the source port (or source ports) that is sent to the specified destination. A source VLAN mirrors only received packets. Possible values for source ports are: - Tx/Rx – Both ingress and egress traffic. - Tx – Egress traffic only. - Rx – Ingress traffic only.

Click **APPLY** to apply the changes to the system.



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



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

Loop Protection

Loops on a network consume resources and can degrade network performance. Detecting loops manually can be very cumbersome and time consuming. The Aruba Instant On 1960 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:

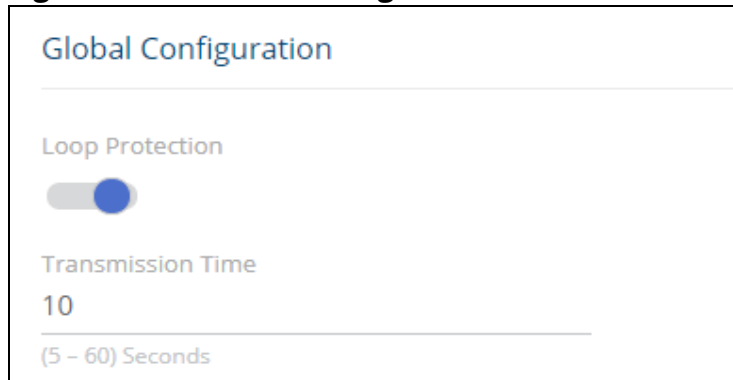
- If auto-recovery is enabled for loop protection- after the timeout expires, the port attempts to recover.

- If auto-recovery is disabled - you may attempt to manually recover the port in the **Suspended Interface** tile on the **Switching > Interface Auto Recovery** page.

To view this page, click **Switching > Loop Protection** in the navigation pane.

Global Configuration

Figure 60. Global Configuration



The screenshot shows the 'Global Configuration' page. It has a title 'Global Configuration' at the top. Below it, there is a section for 'Loop Protection' with a toggle switch that is currently turned on (blue). Underneath, there is a 'Transmission Time' field with the value '10' and a range '(5 - 60) Seconds' indicated below it.

Table 52. Global Configuration Fields

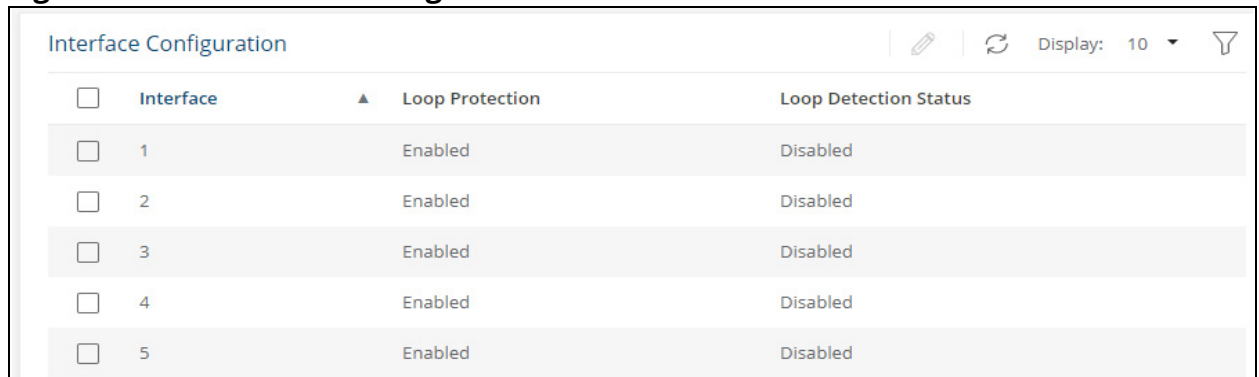
Field	Description
Loop Protection	Select Enabled or Disabled to administratively enable or disable this feature globally on the switch. This feature is disabled by default.
Transmission Time	The interval at which the switch sends loop protection PDUs on interfaces on which Loop Protection is enabled. 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 Configuration**.

Interface Configuration

Use the Interface Configuration tile enable Loop Detection and to display the status of this feature on each port. To display this tile, click **Switching > Loop Protection** in the navigation pane.

Figure 61. Interface Configuration Tile



☐	Interface	▲ Loop Protection	Loop Detection Status
☐	1	Enabled	Disabled
☐	2	Enabled	Disabled
☐	3	Enabled	Disabled
☐	4	Enabled	Disabled
☐	5	Enabled	Disabled

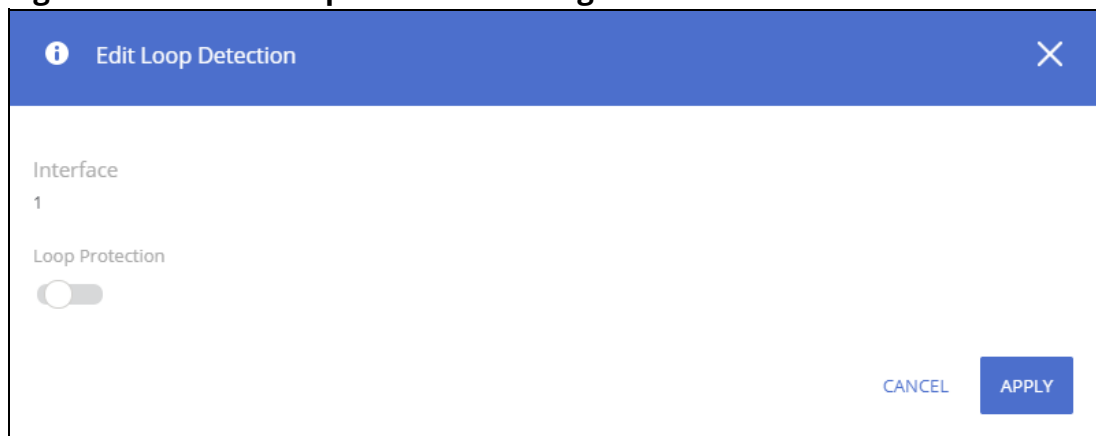
Table 53. Loop Protection Interface Configuration Fields

Field	Description
Interface	The port or trunk ID.
Loop Protection	Indicates whether the feature is administratively enabled or disabled on the port. Loop Protection is disabled by default.
Loop Detection Status	The current loop protection status of the port. • Enabled - no loop present • Disabled - Loop detection is disabled, or the port is down • Loop detected - Loop has been detected and port disabled • Inactive - Loop detection operational state is disable for the port

Loop Protection Configuration

To configure loop protection for a specific interface, select the checkbox to the left of the interface entry and click **Edit** .

Figure 62. Edit Loop Detection Dialog Box



 Edit Loop Detection 

Interface

1

Loop Protection



CANCEL

APPLY

Table 54. Edit Loop Protection Fields

Field	Description
Interface	The port or ports that are being configured.
Loop Protection	Enable or Disable to administratively enable or disable this feature on the selected interfaces. By default, this feature is disabled on all interfaces.

Click **APPLY** to save the changes for the current switch configuration. Your changes take effect immediately. The changes are not retained across a switch reset unless you click **Save Configuration**.

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 it exists) of 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 and IGMPv3.

Global Configuration

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

Figure 63. Global Configuration Tile

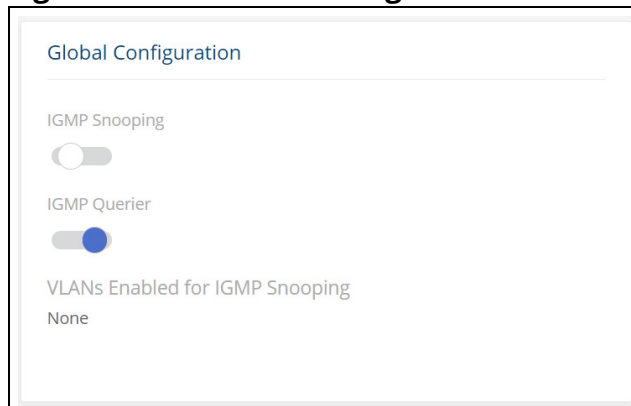


Table 55. Global Configuration Fields

Field	Description
IGMP Snooping	Set as Enabled to globally enable IGMP snooping on the switch. This feature is disabled by default.
IGMP Querier	Set as Enabled to globally enable IGMP querying on the switch. This feature is enabled by default.
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 .

If you change the Admin Mode, 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 Configuration**.

IPv4/IPv6 Unregistered Multicast

The IPv4/IPv6 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 by IGMP Snooping, MLD Snooping or by static configuration.

Normally, Multicast frames are always flooded to all ports in the VLAN. If IGMP Snooping or MLD Snooping is enabled, the switch learns about the existence of Multicast groups and keeps track of which ports joined to 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/IPv6 Unregistered Multicast** feature enables to configure whether to flood (ON) or to filter (Off) these Multicast frames.

This configuration is done per egress port. Once an egress port has been set to filter/forward then this port's configuration is valid for any VLAN it is member of or will be member of.

Figure 64. IPv4/IPv6 Unregistered Multicast Tile

The tile is titled "IPv4/IPv6 Unregistered Multicast". It contains two main sections: "Forwarding" and "Filtering". The "Forwarding" section has a list of ports: 1/1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, and 1/8. The "Filtering" section is currently empty. There are arrow buttons between the two lists to move items.

Table 56. IPv4/IPv6 Unregistered Multicast Fields

Field	Description
Forwarding	This box lists the ports from which unregistered multicast addresses are forwarded to all the ports on the VLAN. The setting applies to all VLANs on the interface which are MLD snooping enabled. Use the arrow buttons to move addresses to or from this list.
Filtering	This box lists the ports from which unregistered multicast addresses are filtered. Setting applies to all VLANs on the interface which are MLD snooping enabled. Use the arrow buttons to move addresses to or from this list.

IGMP Snooping VLAN Configuration

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

To access the tile, click **Switching** > **IGMP Snooping** in the navigation pane.

Figure 65. IGMP Snooping VLAN Configuration Tile

The tile is titled "IGMP Snooping VLAN Configuration". It features a table with columns for VLAN ID, IGMP Snooping Admin Mode, IGMP Snooping Operational Mode, IGMP Querier Admin Mode, IGMP Querier Operational Mode, Querier Address, Fast Leave, Query Interval (Seconds), and Max Response Time (Seconds). The table shows settings for VLAN 1.

☐	VLAN ID	IGMP Snooping Admin Mode	IGMP Snooping Operational Mode	IGMP Querier Admin Mode	IGMP Querier Operational Mode	Querier Address	Fast Leave	Query Interval (Seconds)	Max Response Time (Seconds)
☐	1	Disabled	Disabled	Disabled	Disabled	255.255.255.255	Disabled	125	10

Table 57. IGMP Snooping VLAN Configuration Fields

Field	Description
VLAN ID	The VLAN interface associated with the rest of the data in the row. When configuring IGMP snooping settings, this field identifies the VLAN interface(s) that are being configured.
IGMP Snooping Admin Mode	The administrative mode of IGMP snooping on the VLAN interface. IGMP snooping must be enabled globally and on a VLAN interface to be able to snoop IGMP packets and determine which segments should receive multicast packets directed to the group address.
IGMP Snooping Operational Mode	Indicates whether IGMP snooping is operational on this VLAN. To be operational, IGMP snooping needs to be enabled globally and on the VLAN.
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	Indicates whether IGMP querier is operational on this VLAN. To be operational, IGMP snooping needs to be operational and IGMP querier must be enabled globally and on the VLAN, and there is a valid IGMP querier address.
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.
Query Interval (Seconds)	The expected Frequency, in seconds, at which IGMP query messages are forwarded on this VLAN interface.
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.

To change the snooping VLAN configuration, check the box to the left of one or more interfaces and click **Edit**  .

Figure 66. Edit IGMP Snooping VLAN Configuration Dialog Box

Edit IGMP Snooping VLAN Configuration

VLAN ID
1

IGMP Snooping
☒

IGMP Querier
☐

IGMP Querier Version
☒ v2 ☐ v3

IGMP Querier Election
☒

IGMP Querier IP Address
☒ Auto ☐ (x.x.x.x)

Forwarding Method
☒ IP ☐ Source and IP

Query Robustness
2
(1 - 7)

CANCEL APPLY

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**.

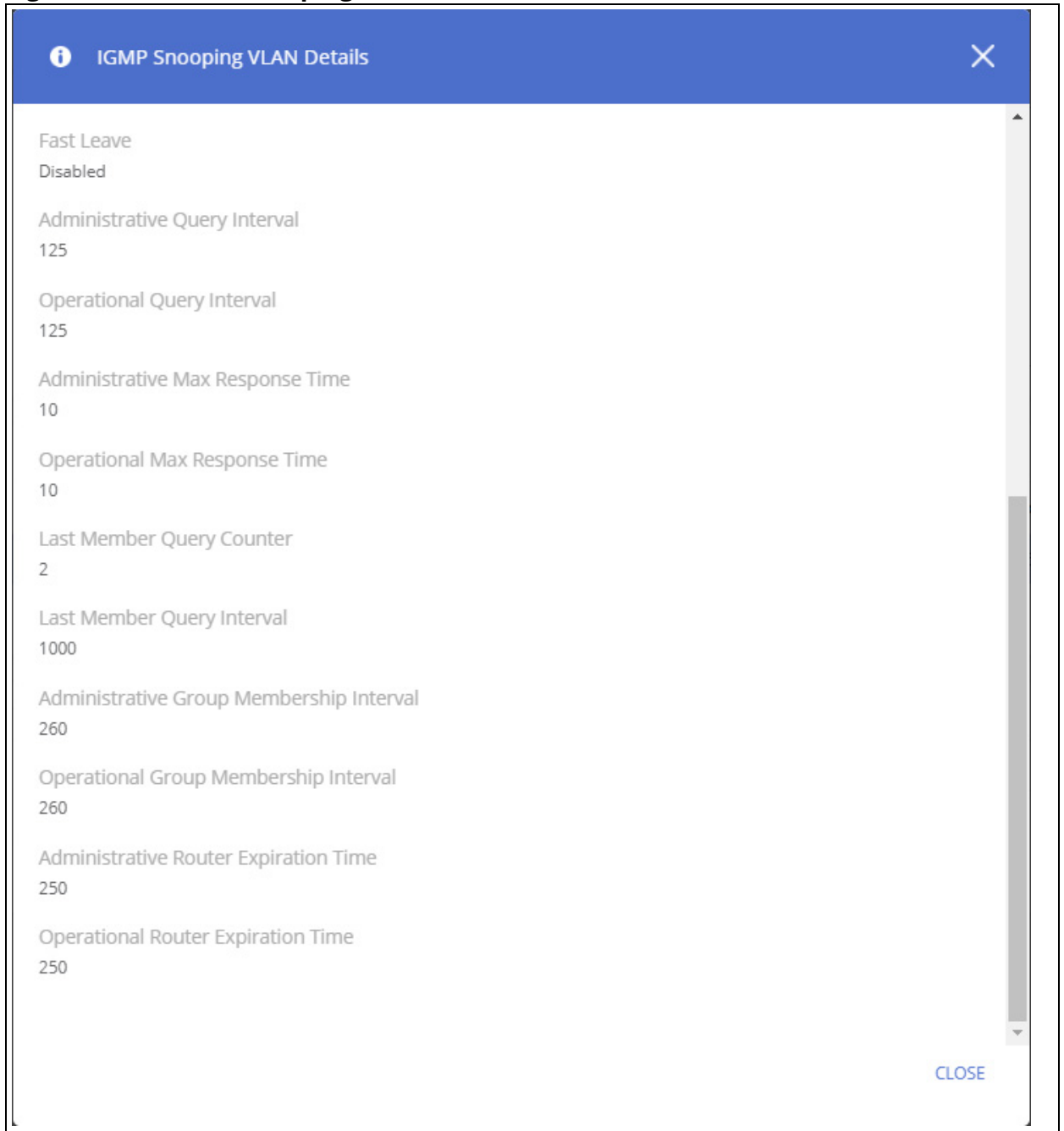
Table 58. Edit IGMP Snooping VLAN Configuration Fields

Field	Description
VLAN ID	The VLAN interface(s) that are being configured.
IGMP Snooping	The administrative mode of IGMP snooping on the VLAN interface. To be operational, IGMP snooping needs to be enabled globally and on the VLAN.
IGMP Querier	The administrative mode of IGMP querier on the VLAN interface. IGMP snooping must be enabled globally and on an VLAN interface to be able to query IGMP packets.
IGMP Querier Version	Select the IGMP version. Available options are: v2 (IGMPv2) or v3 (IGMPv3). The default is v2.
IGMP Querier Election	Enable or disable IGMP querier election on the VLAN. Default is enabled. If enabled, the IGMP snooping querier supports the standard IGMP querier election mechanism specified in RFC2236 and RFC3376. If disabled, IGMP snooping querier delays sending General Query messages for 60 seconds from the time it was enabled. During this time, if the switch did not receive an IGMP query from another Querier - it starts sending General Query messages. Once the switch acts as a Querier - it will stop sending General Query messages if it detects another Querier on the VLAN.
IGMP Querier IP Address	Define the source IP address to use for IGMP query packets sent by the querier. If Auto is selected, the IP address configured on the VLAN is used. If an IP is not specified on the VLAN, the querier on this VLAN is inactive.

Field	Description
Forwarding Method	Select IP , or Source and IP . If IP is selected the multicast forwarding method is based on Multicast IP destination address information. This is the default. If Source and IP is selected, the multicast forwarding is based on multicast IP destination and the source IP address information.
Query Robustness	Set the query robustness value for the IGMP querier. The default is 2.
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 group-based general queries.
Query Interval	The expected Frequency, in seconds, at which IGMP query messages are sent on this VLAN interface.
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.
Last Member Query Counter	Set the number of times that group- or group-source-specific queries are sent upon receipt of a message indicating a leave. The default is 2.
Last Member Query Interval	Set the interval, in milliseconds, at which the IGMP group-specific host query messages are sent on the interface. The default is 1000 milliseconds.
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.
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.

The **Details**  button displays the **IGMP Snooping VLAN Configuration** fields and the operational values related to IGMP snooping timers on the interface.

Figure 67. IGMP Snooping VLAN Details



These are the additional fields that are shown in the **Details** dialog box.

Table 59. IGMP Snooping VLAN Details Fields

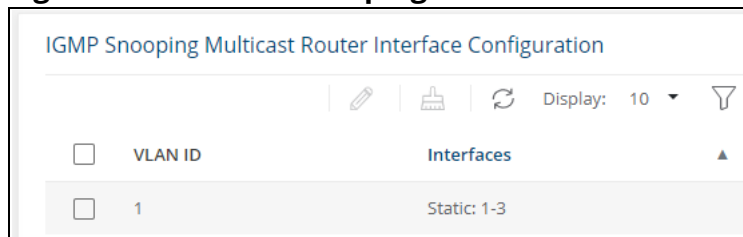
Field	Description
IGMP Querier Version	The IGMP version detected on the VLAN. If the IGMP querier is operational, the selected querier version is displayed. If not the version is determined based on the active IGMP router connected the VLAN.
Operational Query Interval	Indicates the operational value of the querier Interval parameter.
Operational Max Response Time	Indicates the operational value of the Max Response Time parameter.
Operational Group Membership Interval	The operational value of the Group Membership Interval parameter.
Operational Router Expiration Time	The operational value of the Router expiration Time parameter.

IGMP Snooping Multicast Router Interface Configuration

Use this tile to manually configure an interface within a VLAN as a 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 an interface as a multicast router interface, which is an interface that faces a multicast router or IGMP querier and receives multicast traffic.

To access the tile, click **Switching > IGMP Snooping** in the navigation pane.

Figure 68. IGMP Snooping Multicast Router Configuration Tile**Table 60. IGMP Snooping Multicast Router Configuration Fields**

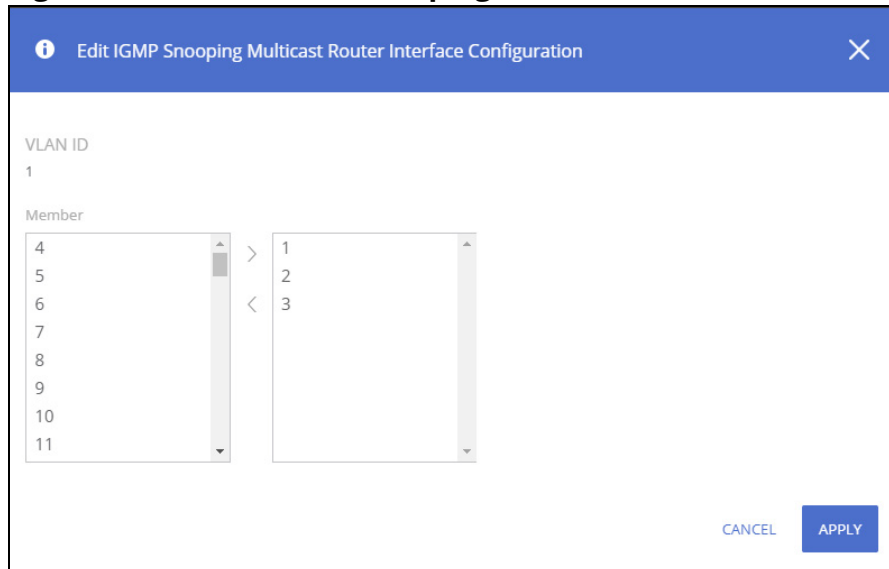
Field	Description
VLAN ID	The VLAN ID associated with the rest of the data in the row. When configuring the IGMP snooping multicast router settings, this field identifies the VLAN(s) that are being configured
Interfaces	List the ports in this VLAN which are Multicast Router interfaces. Membership can be dynamic or static.

Configuring Multicast Router Settings on Interfaces

To remove a static entry, click **Remove Static**  .

To change the multicast router membership for one or more interfaces, select each entry (that is, VLAN) you wish to modify and click **Edit**  .

Figure 69. Edit IGMP Snooping Multicast Router Interface 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.

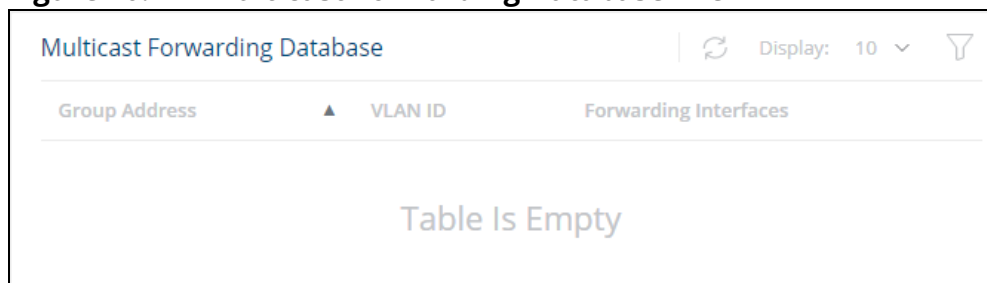
Click **APPLY** to save the changes for the current switch configuration. The changes take effect immediately and are applied to each of the selected interfaces. The changes are not retained across a switch reset unless you click **Save Configuration**.

Multicast Forwarding Database

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

To access the tile, click **Switching > IGMP Snooping** in the navigation pane.

Figure 70. Multicast Forwarding Database Tile



To refresh the list, click **Refresh**  .

To filter the list, click **Filter**  .

Table 61. Multicast Forwarding Database Fields

Field	Description
Group Address	The Multicast 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.

MLD Snooping

Multicast Listener Discovery (MLD) snooping is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (hosts wishing to receive IPv6 multicast packets) on its directly attached links and to discover which multicast packets are of interest to neighboring hosts. MLD is derived from IGMP; MLD version 1 (MLDv1) is equivalent to IGMPv2 and MLD version 2 (MLDv2) is equivalent to IGMPv3.

The switch supports two versions of MLD snooping:

- MLDv1 snooping detects MLDv1 control packets and sets up traffic bridging based on IPv6 destination multicast addresses.
- MLDv2 uses control packets to set up traffic forwarding based on source IPv6 address and destination IPv6 multicast address.

IPv6 multicast frames are snooped as they are forwarded by the switch from hosts to an upstream multicast router and vice versa. This snooping allows a switch to conclude the following:

- Which ports might be interested in joining a specific multicast group
- Which multicast routers are sending multicast frames

This information is used to exclude ports on which no hosts have registered to receive a specific multicast stream from forwarding incoming multicast frames.

There are 2 port types:

- Host port - a port which is connected to a host (end-node) running an IGMP/MLD (multicast communication) application.
- Multicast Router (mrouter) port - a port that connects a multicast router port to the switch. This port receives all IGMP/MLD control packets (reports and queries) as well as all multicast data traffic associated with dynamic multicast groups.

Global Configuration

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

Figure 71. Global Configuration Tile

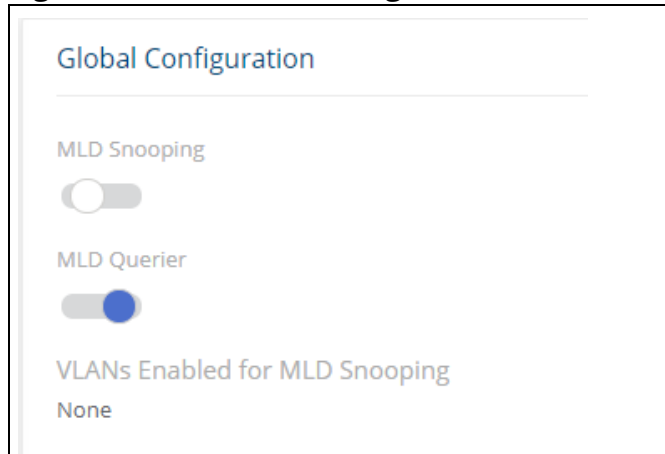


Table 62. Global Configuration Fields

Field	Description
MLD Snooping	Select Enabled to globally enable MLD snooping on the switch. This feature is disabled by default.
MLD Querier	Select Enabled to globally enable MLD querier on device. This feature is enabled by default.
VLANs Enabled for MLD Snooping	Identifies the VLAN ID of each VLAN on which MLD snooping is administratively enabled. If MLD snooping is not enabled on any VLANs, this field shows None .

If you change the global configuration, click **APPLY** to save the changes for the current switch configuration.

IPv4/IPv6 Unregistered Multicast

Figure 72. IPv4/IPv6 Unregistered Multicast Tile

IPv4/IPv6 Unregistered Multicast

Action	Forwarding	Filtering
	1/1	
	1/2	
	1/3	
	1/4	
	1/5	
	1/6	
	1/7	
	1/8	

Table 63. IPv4/IPv6 Unregistered Multicast Fields

Field	Description
Forwarding	This box lists the ports from which unregistered multicast addresses are forwarded to all the ports on the VLAN. The setting applies to all VLANs on the interface which are MLD snooping enabled. Use the arrow buttons to move addresses to or from this list.
Filtering	This box lists the ports from which unregistered multicast addresses are filtered. Setting applies to all VLANs on the interface which are MLD snooping enabled. Use the arrow buttons to move addresses to or from this list.

MLD Snooping VLAN Configuration

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

To access the tile, click **Switching > MLD Snooping** in the navigation pane.

Figure 73. MLD Snooping VLAN Configuration Tile

MLD Snooping VLAN Configuration							
☐	VLAN ID ▲	MLD Snooping Admin Mode	MLD Snooping Operational Mode	MLD Querier Admin Mode	MLD	Fast Leave	Query Interval (Seconds)
☐	1	Disabled	Disabled	Disabled	Disabled	Disabled	125
« < 1 > »							

Table 64. MLD Snooping VLAN Configuration Fields

Field	Description
VLAN ID	The VLAN interface associated with the rest of the data in the row. When configuring MLD snooping settings, this field identifies the VLAN interface(s) that are being configured.
MLD Snooping Admin Mode	The administrative mode of MLD snooping on the VLAN interface. MLD snooping must be enabled globally and on a VLAN interface to be able to snoop MLD packets and determine which segments should receive multicast packets directed to the group address.
MLD Snooping Operational Mode	The operational mode.
MLD Querier Admin Mode	The expected Frequency, in seconds, at which MLD query messages are forwarded on this VLAN interface.
MLD Querier Operational Mode	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.
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.
Query Interval (Seconds)	The expected frequency, in seconds, at which MLD query messages are forwarded on this VLAN interface.
Max Response Time (Seconds)	The number of seconds the VLAN interface should wait to receive a query before it is removed from the list of VLAN interfaces with multicast routers attached. This field is read-only.

The **Details**  button displays the **MLD Snooping VLAN Configuration** fields and the operational values related to MLD snooping timers on the interface.

Modifying MLD Snooping VLAN Configuration Settings

To change the MLD VLAN configuration of one or more interfaces, check the box to the left of one or more interfaces and click **Edit**  .

Figure 74. Edit MLD VLAN Configuration Dialog Box

Edit MLD VLAN Configuration

VLAN ID
1

MLD Snooping
☐

MLD Version
☐ v1 ☒ v2

MLD Querier
☐

MLD Querier Version
☐ v1 ☒ v2

MLD Querier Election
☒

MLD Querier IP Address
255.255.255.255

MLD Querier IP Address

Forwarding Method
☐ IP ☒ Source and IP

CANCEL APPLY

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**.

Table 65. Edit Port Configuration Fields

Field	Description
VLAN ID	Indicates the VLAN ID that was selected for configuration.
MLD Snooping	Enable or disable MLD snooping on the VLAN port.
MLD Querier	Enable or disable MLD querying on the VLAN port
MLD Querier Version	Select v1 or v2 for MLD querying on the VLAN port.

Field	Description
MLD Querier Election	Enable or disable MLD query election on the VLAN port. When enabled, the MLD Snooping querier supports the standard MLD Querier election mechanism specified in RFC2236 and RFC3376. When disabled, the MLD Snooping Querier delays sending General Query messages for 60 seconds from the time it was enabled. During this time, if the switch did not receive an MLD query from another Querier - it starts sending General Query messages. it will stop sending General Query messages if it detects another Querier on the VLAN.
Forwarding Method	Select the forwarding method: - IP - select this method for forwarding that is based only on Multicast IP destination address information - Source and IP - select this method for forwarding that is based on multicast IP destination and source IP address information.
Query Robustness	Set the robustness level for the query. Valid values are 1-7. The default is 2
Fast Leave	Enable or disable fast leave mode
Query Interval	Set the query interval in seconds. Valid values are 30-18000. The default is 125.
Max Response Time	Set the maximum response time in seconds. Valid values are 5-20. The default is 10.
Last Member Query Counter	Configure the number of times that group- or group-source-specific queries are sent upon receipt of a message indicating a leave. Valid values are 1-7. The default is 2.
Last Member Query Interval	Set the interval, in milliseconds, at which MLD group-specific host query messages are sent on the interface. Valid values are: 100-25500 ms. The default is 1000 ms.
Group Membership Interval	This is not configurable.
Multicast Router Expiration Time	This is not configurable.

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**.

MLD Snooping Multicast Router Interface Configuration

Use this tile to manually configure an interface within a VLAN as a MLD snooping multicast router interface.

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

To access the tile, click **Switching** > **MLD Snooping** in the navigation pane.

Figure 75. MLD Snooping Multicast Router Configuration Tile

MLD Snooping Multicast Router Interface Configuration

Display: 10

VLAN ID	Interfaces
1	

Table 66. MLD Snooping Multicast Router Configuration Fields

Field	Description
VLAN ID	The VLAN ID associated with the rest of the data in the row. When configuring the MLD snooping multicast router settings, this field identifies the VLAN(s) that are being configured.
Interface	List the ports in this VLAN which are Multicast Router interfaces. Membership can be dynamic or static.

Configuring Multicast Router Settings on Interfaces

To change the multicast router membership for one or more interfaces, select each entry (that is, VLAN) you wish to modify and click **Edit** .

Figure 76. Edit MLD Snooping Multicast Router Interface Configuration Dialog Box

Edit MLD Snooping Multicast Router Interface Configuration

VLAN ID
1

Member

1/1	>	
1/2		
1/3	<	
1/4		
1/5		
1/6		
1/7		
1/8		

CANCEL APPLY

Select one or more interfaces that you want to configure as MLD 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.

For interfaces that have static interfaces set, you can remove the static interface setting by selecting the interface and clicking the **Remove Static**  button.

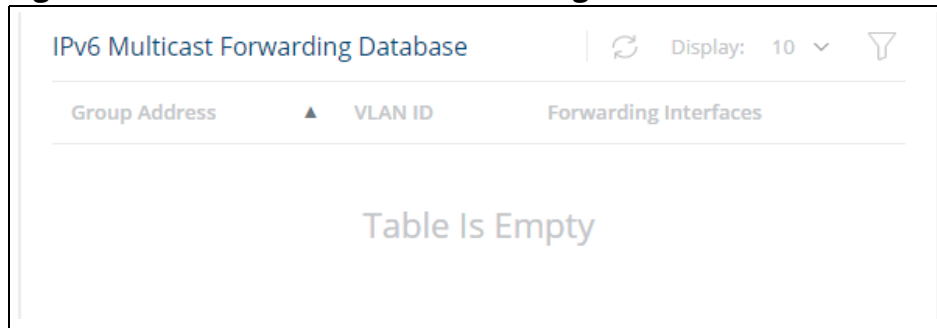
Click **APPLY** to save the changes for the current switch configuration. The changes take effect immediately and are applied to each of the selected interfaces. The changes are not retained across a switch reset unless you click **Save Configuration**.

IPv6 Multicast Forwarding Database

This tile displays the Multicast group addresses learned from MLD. Interface membership is displayed per each VLAN

To access the tile, click **Switching > MLD Snooping** in the navigation pane.

Figure 77. IPv6 Multicast Forwarding Database Tile



To refresh the list, click **Refresh** .

To filter the list, click **Filter** .

Table 67. Multicast Forwarding Database Fields

Field	Description
Group Address	The Multicast 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.

SNMP

Simple Network Management Protocol (SNMP) provides a method for managing network devices. The switch 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 switch. 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 traps 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:

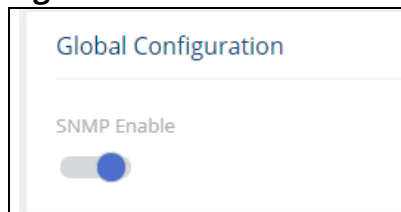
- Security
- Feature Access Control
- Traps

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

Global Configuration

To globally enable SNMP, set **SNMP Enable** in the **Global Configuration** section:

Figure 78. Global SNMP



Community Configuration

Access rights are managed by defining communities on the Community Configuration tile. 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 add SNMP communities and community groups.

To display the Community Configuration tile, click **Switching** > **SNMP** in the navigation pane.

Figure 79. Community Configuration Tile

Community Configuration						
☐	Community Name	IP Address	Community Type	Access	View	Group Name
☐	comg1	0.0.0.0	Community Group			DefaultRead

Table 68. Community Configuration Fields

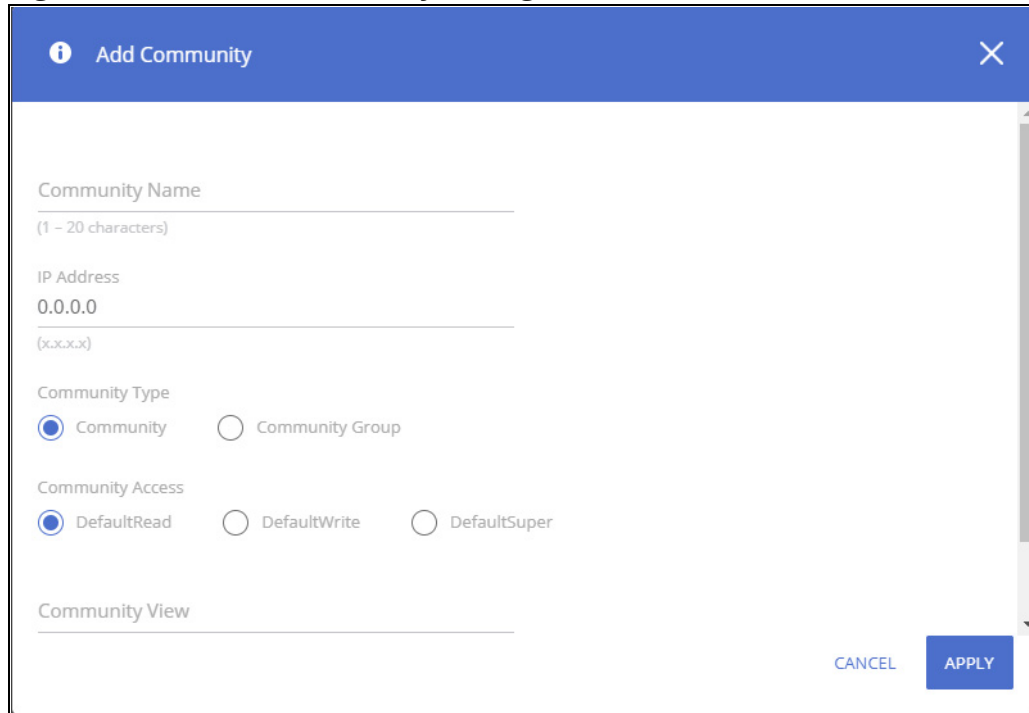
Field	Description
Community Name	Community name used in SNMPv1/v2 packets. This is configured in the client and identifies the access the user may connect with.
IP Address	Specifies the IP address that can connect with this community. The address can be one of the following: - IPv4 address. - IPv6 global 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%<ID> - Hostname - specify the server hostname
Community Type	This is either Community or Community Group .
Access	Specifies the access control policy for the community. The default access privileges are as follows: - DefaultRead: Read access to the entire MIB tree except to SNMP configuration objects. - DefaultWrite: Write access to the entire MIB tree except to SNMP configuration objects. - DefaultSuper: Read and Write access to the entire MIB tree.
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.

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

Adding an SNMP Community or Community Group

To add a new SNMP community, click **Add** . The **Add Community** dialog box appears.

Figure 80. Add Community Dialog Box



The dialog box titled "Add Community" has a blue header bar with an information icon and a close button. The main area contains the following fields and options:

- Community Name:** A text input field with a placeholder "(1 – 20 characters)".
- IP Address:** A text input field with the value "0.0.0.0" and a placeholder "(x.x.x.x)".
- Community Type:** Two radio buttons: "Community" (selected) and "Community Group".
- Community Access:** Three radio buttons: "DefaultRead" (selected), "DefaultWrite", and "DefaultSuper".
- Community View:** A text input field.
- Buttons:** "CANCEL" and "APPLY" buttons at the bottom right.

Configure the community 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 **Remove** . You must confirm the action before the entries are removed.

SNMP Trap Receivers

The SNMP Trap Receivers tile includes two tabs:

- SNMP Trap Receivers v1/v2
- SNMP Trap Receivers v3.

To access the Trap Receiver v1/v2 Configuration tile, click **Switching** > **SNMP** in the navigation pane. The **SNMP Trap Receivers v1/v2** tab is selected by default.

SNMP Trap Receivers v1/v2

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

You can configure up to 8 SNMP trap receivers in this tab.

Figure 81. SNMP Trap Receivers v1/v2 Tab

SNMP Trap Receivers v1/v2		SNMP Trap Receivers v3						Display: 10		
☐	Host IP Address	Community Name	Notify Type	SNMP Version	Timeout (Sec)	Retries	Filter	UDP Port		
☐	1.1.1.1	Trap1	Traps	v1				162		

Table 69. SNMP Trap Receivers v1/v2 Fields

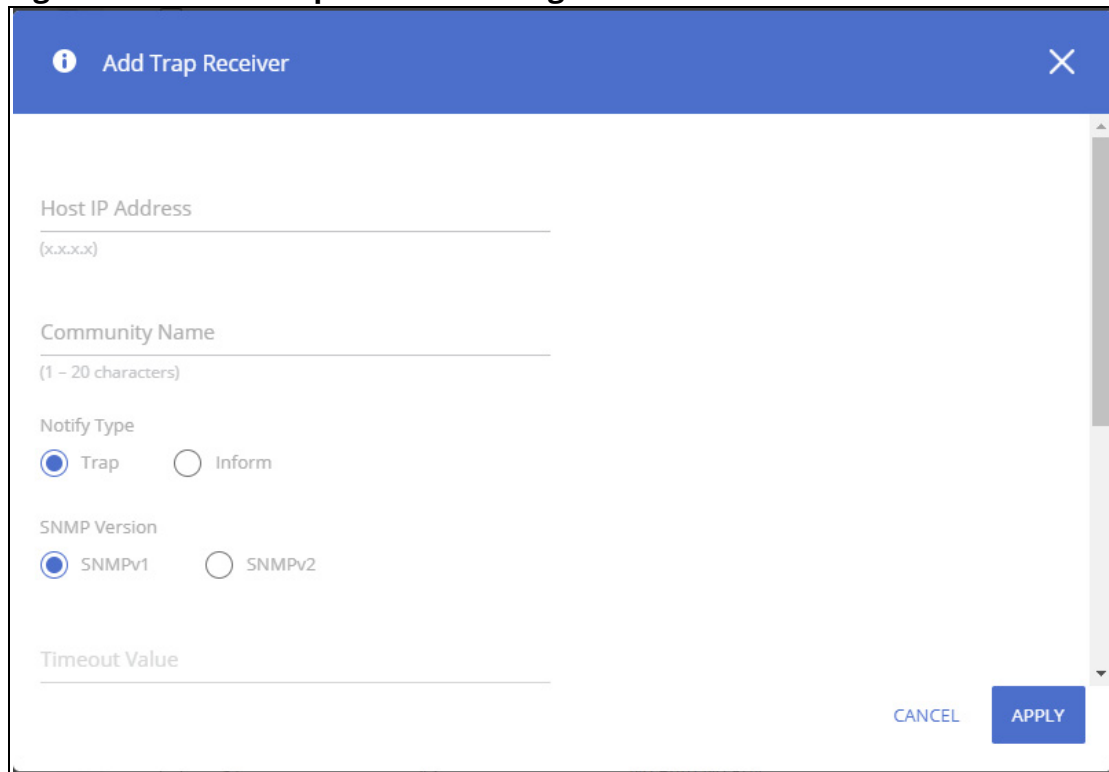
Field	Description
Host IP Address	The IP address of the SNMP management host that will receive traps generated by the switch.
Community Name	The name of the SNMP community that includes the SNMP management host and the SNMP agent on the switch.
Notify Type	The type of SNMP notification to send the SNMP management host: • Inform – An SNMP message that notifies the host when a certain event has occurred on the switch. 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 switch. 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 (Sec)	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 save the changes for the current 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 a SNMP v1/v2 trap receiver, click **Add** . The **Add Trap Receiver** dialog box appears.

Figure 82. Add Trap Receiver Dialog Box

The image shows a dialog box titled "Add Trap Receiver" with a blue header bar containing an information icon and a close button. The main area is white and contains several form fields: "Host IP Address" with a placeholder "(x.x.x.x)", "Community Name" with a placeholder "(1 - 20 characters)", "Notify Type" with two radio buttons, "Trap" (selected) and "Inform", "SNMP Version" with two radio buttons, "SNMPv1" (selected) and "SNMPv2", and "Timeout Value". At the bottom right, there are two buttons: "CANCEL" and "APPLY".

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

To edit an existing trap receiver, select it in the table, click **Edit** , and edit the fields as needed.

Removing an SNMP v1/v2 Trap Receiver

To remove an SNMP v1/v2 trap receiver, select each item to delete and click **Remove** . You must confirm the action before the entries are removed.

SNMP Trap Receivers v3

Use the SNMP Trap Receivers v3 tab to configure settings for each SNMPv3 management host that will receive notifications about traps generated by the switch. 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 tab, click **Switching** > **SNMP** in the navigation pane, and then click the **SNMP Trap Receivers v3** tab.

Figure 83. SNMP v3 Trap Receivers Tab

SNMP Trap Receivers v1/v2		SNMP Trap Receivers v3						Display: 10		
☐	Host IP Address	▲	Username	Notify Type	Security Level	Timeout (Sec)	Retries	Filter	UDP Port	
☐	1.1.1.1		admin	Traps	No Auth No Priv				162	

Table 70. SNMP Trap Receivers v3 Fields

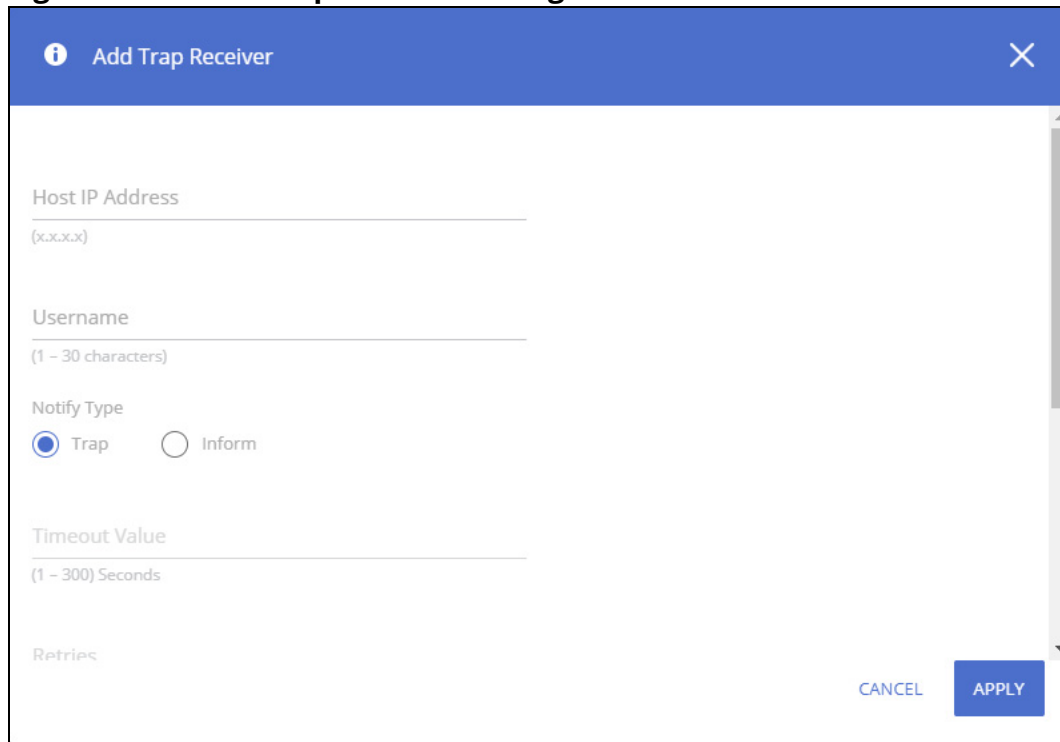
Field	Description
Host IP Address	The IP address of the SNMP management host that will receive traps generated by the switch.
Username	The name of the SNMP user that is authorized to receive the SNMP notification.
Notify Type	The type of SNMP notification to send the SNMP management host: • Inform – An SNMP message that notifies the host when a certain event has occurred on the switch. 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 switch. The message is not acknowledged by the SNMP management host.
Security Level	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 (sec)	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 save the changes for the current switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Adding an SNMP v3 Trap Receiver

To add a SNMP v3 trap receiver, click **Add** . The **Add Trap Receiver** dialog box appears.

Figure 84. Add Trap Receiver Dialog Box

The image shows a dialog box titled "Add Trap Receiver" with a blue header bar containing an information icon and a close button. The main area is white and contains several input fields: "Host IP Address" with a placeholder "(x.x.x.x)", "Username" with a placeholder "(1 - 30 characters)", "Notify Type" with two radio buttons labeled "Trap" (selected) and "Inform", "Timeout Value" with a placeholder "(1 - 300) Seconds", and "Retries". At the bottom right, there are two buttons: "CANCEL" and "APPLY".

Configure the required fields and click **APPLY**. Note that the Reties and Timeout Value fields are available only if the selected Notify Type is Inform.

To edit an existing trap receiver, select it in the table, click **Edit** , and edit the fields as needed.

Removing an SNMP v3 Trap Receiver

To remove an SNMP v3trap receiver, select each item to delete and click **Remove** . You must confirm the action before the entries are removed.

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 switch 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.

To access the SNMP Access Control Group Configuration tile, click **Switching** > **SNMP** in the navigation pane.

Figure 85. SNMP Access Control Group Configuration Tile

SNMP Access Control Group Configuration										Display: 10 ▾	
☐	Group Name ▲	SNMP Version	Security Level	Read	Write	Notify					
☐	DefaultRead	v3	No Auth No Priv	Default		Default					
☐	DefaultSuper	v1	No Auth No Priv	DefaultSuper	DefaultSuper	DefaultSuper					
☐	DefaultWrite	v3	No Auth No Priv	Default	Default	Default					

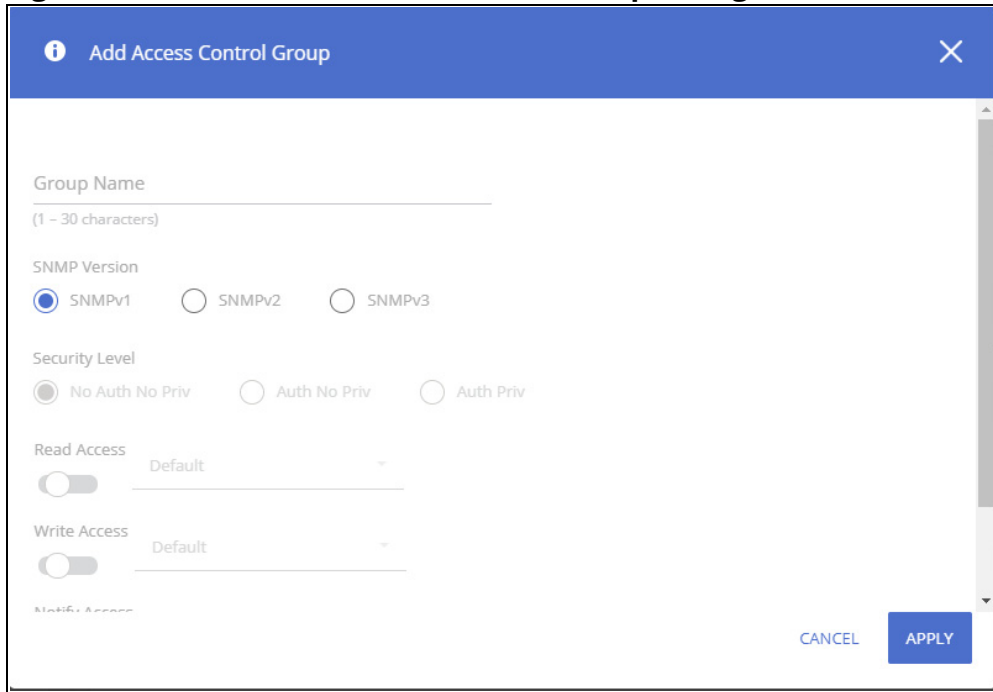
Table 71. SNMP Access Control Group Configuration Fields

Field	Description
Group Name	The name that identifies the SNMP group.
SNMP Version	The SNMP version associated with the group.
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 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.
Read	The level of read access rights for the group. The menu includes the available SNMP views. When adding a group, enable this setting 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, enable this setting to allow the field to be configured, then select the desired view that permits management read-write access to viewing the contents of the agent, but not to the community.
Notify	The level of notify access rights for the group.

Adding an SNMP Access Control Group

To add a SNMP access control group click **Add** . The **Add new Access Control Group** dialog box appears.

Figure 86. Add New Access Control Group Dialog Box



The dialog box is titled "Add Access Control Group" with an information icon and a close button. It contains the following fields and options:

- Group Name:** A text input field with a placeholder "(1 - 30 characters)".
- SNMP Version:** Three radio buttons: ☒ SNMPv1, ☐ SNMPv2, and ☐ SNMPv3.
- Security Level:** Three radio buttons: ☒ No Auth No Priv, ☐ Auth No Priv, and ☐ Auth Priv.
- Read Access:** A toggle switch (currently off) and a dropdown menu set to "Default".
- Write Access:** A toggle switch (currently off) and a dropdown menu set to "Default".
- Notify Access:** A partially visible field at the bottom.

At the bottom right, there are "CANCEL" and "APPLY" buttons.

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

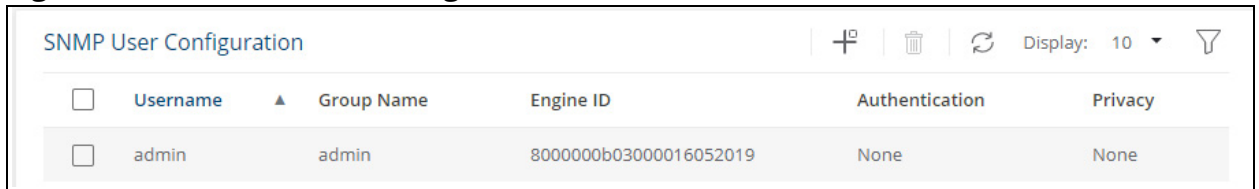
Removing an SNMP Access Control Group

To remove an SNMP Access Control Group receiver, select each item to delete and click **Remove** . You must confirm the action before the entries are removed.

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 87. SNMP User Configuration Tile



The tile shows a table of SNMP v3 user accounts. At the top right, there are icons for adding, deleting, and refreshing, along with a "Display: 10" dropdown and a filter icon.

☐	Username	Group Name	Engine ID	Authentication	Privacy
☐	admin	admin	8000000b03000016052019	None	None

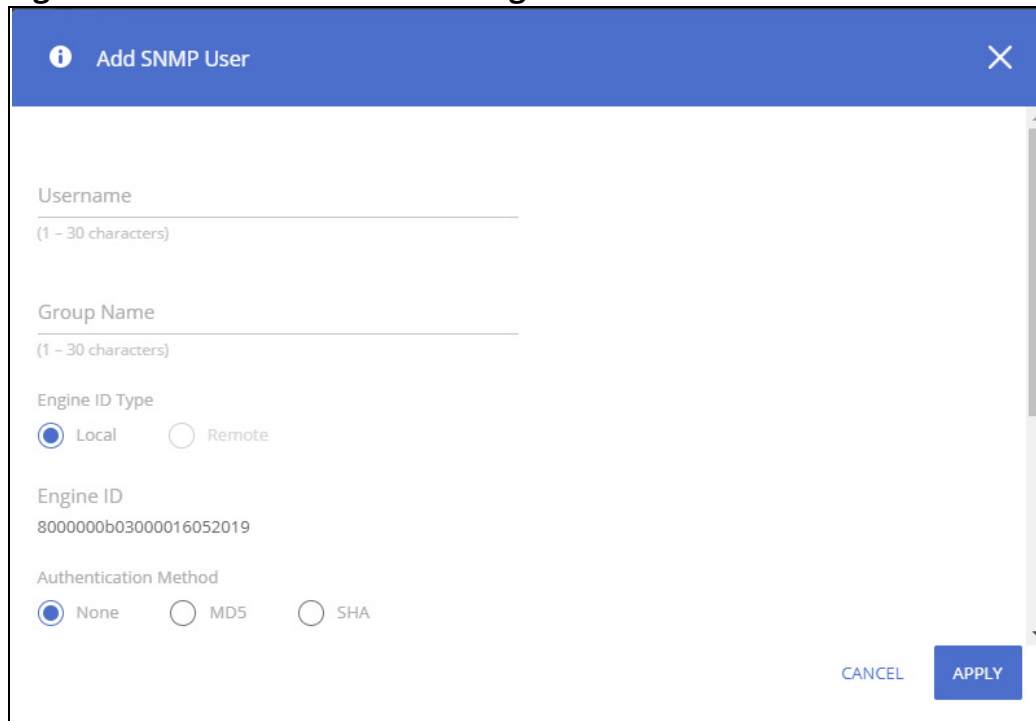
Table 72. SNMP User Configuration Fields

Field	Description
Username	Specifies the name of the SNMP user being added for the User-based Security Model (USM). Each Username must be unique within the SNMP agent user list. A Username cannot contain any leading or embedded blanks.
Group Name	A 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 network. This field takes an hexadecimal string in the form of 0102030405.
Authentication	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 1-32 hexadecimal characters. • SHA - SHA protocol will be used. This option requires a password of 1-32 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 1-32 hexadecimal characters.

Adding an SNMP User

To add an SNMP v3 user, click **Add**  . The **Add SNMP User** screen appears.

Figure 88. Add SNMP User Dialog Box

The image shows a web-based dialog box titled "Add SNMP User". It has a blue header bar with an information icon and a close button. The main content area is white and contains several fields: "Username" with a placeholder "(1 - 30 characters)", "Group Name" with a placeholder "(1 - 30 characters)", "Engine ID Type" with radio buttons for "Local" (selected) and "Remote", "Engine ID" with the value "8000000b03000016052019", and "Authentication Method" with radio buttons for "None" (selected), "MD5", and "SHA". At the bottom right, there are "CANCEL" and "APPLY" buttons.

The following fields appear in the configuration dialog, but are not described in **SNMP User Configuration Fields**.

Table 73. 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.
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 1-32 hexadecimal characters. • SHA - SHA protocol will be used. This option requires a password of 1-32 hexadecimal characters.
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 User

To remove one or more SNMP v3 users, select each user to delete and click **Remove** . You must confirm the action before the entries are removed.

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 89. SNMP View Configuration Tile

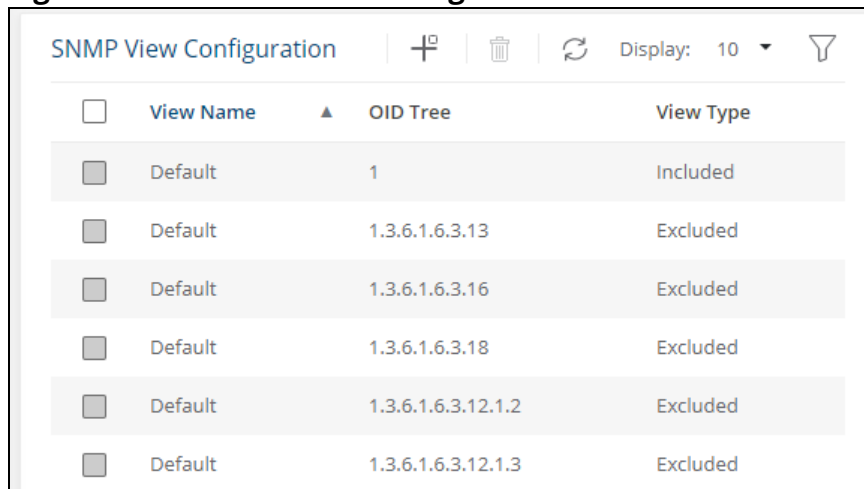
The screenshot shows the 'SNMP View Configuration' tile. At the top, there's a title bar with the title 'SNMP View Configuration', a plus icon, a trash icon, a refresh icon, and a 'Display: 10' dropdown with a filter icon. Below the title bar is a table with four columns: 'View Name', 'OID Tree', and 'View Type'. The first row has a checkbox, 'Default', '1', and 'Included'. The subsequent rows have checkboxes, 'Default', various OID trees (1.3.6.1.6.3.13, 1.3.6.1.6.3.16, 1.3.6.1.6.3.18, 1.3.6.1.6.3.12.1.2, 1.3.6.1.6.3.12.1.3), and 'Excluded'.

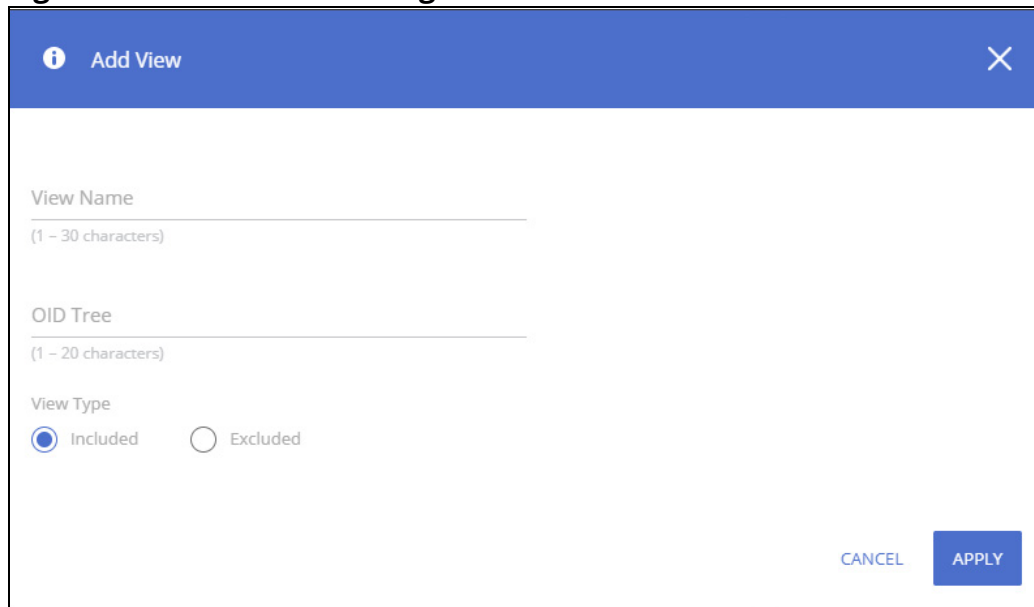
Table 74. SNMP View Entry Fields

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 **Add** . The **Add View** screen appears.

Figure 90. Add View Dialog Box

The image shows a dialog box titled "Add View" with a blue header bar containing an information icon and a close button. The main area is white and contains three input fields: "View Name" with a placeholder "(1 - 30 characters)", "OID Tree" with a placeholder "(1 - 20 characters)", and "View Type" with two radio buttons labeled "Included" (selected) and "Excluded". At the bottom right, there are two buttons: "CANCEL" and "APPLY".

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 **Remove** . Only user-configured views can be removed. You must confirm the action before the entries are 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.

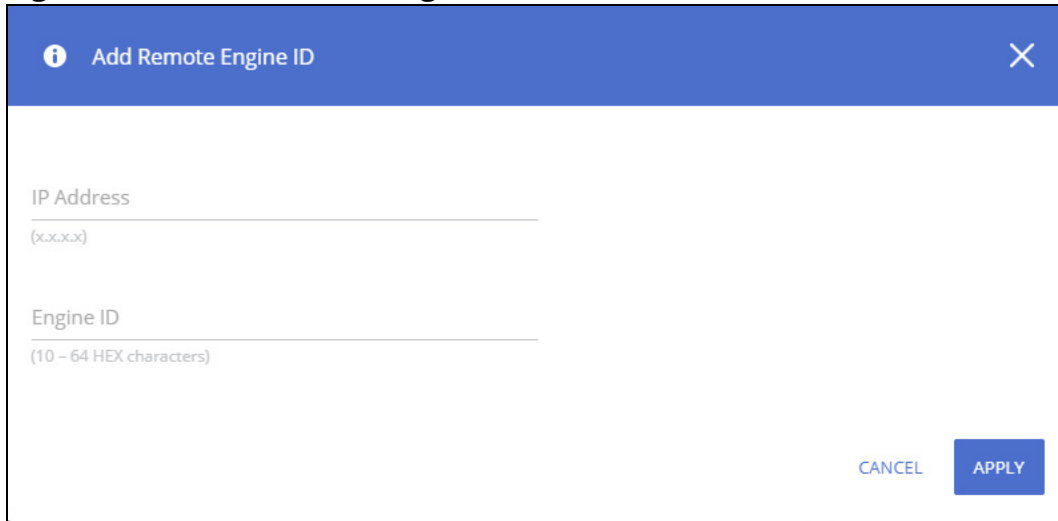
Table 75. Remote Engine ID Configuration Entry Fields

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 Configuration

To add a **Remote Engine ID Configuration**, click **Add** . The **Add Remote Engine ID** screen appears.

Figure 91. Add Remote Engine ID

A dialog box titled "Add Remote Engine ID" with a blue header bar containing an information icon and a close button. The main area is white and contains two input fields. The first field is labeled "IP Address" with a placeholder "(x.x.x.x)". The second field is labeled "Engine ID" with a placeholder "(10 - 64 HEX characters)". At the bottom right, there are two buttons: "CANCEL" and "APPLY".

IP Address
(x.x.x.x)

Engine ID
(10 - 64 HEX characters)

CANCEL APPLY

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

Removing a Remote Engine ID Configuration

To remove one or more remote engine IDs, select each engine to delete and click **Remove** . You must confirm the action before the entries are removed.

Interface Auto Recovery

A number of features on the switch may 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.

Features supported by Auto Recovery are listed below. Each feature is listed with 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. See **Modifying Interface Settings** for more information.
- 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.

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 utilizes 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.

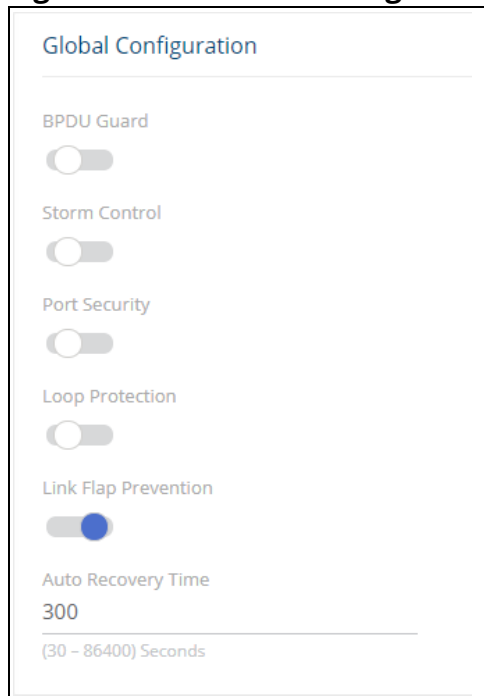
Use the **Auto Recovery Configuration** page to configure **Auto Recovery** settings for all the components.

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

Global Configuration

These are the global configuration options that you can set:

Figure 92. Global Configuration



The screenshot displays the 'Global Configuration' page with a list of network features and their status:

- BPDU Guard**: Disabled (toggle switch is grey)
- Storm Control**: Disabled (toggle switch is grey)
- Port Security**: Disabled (toggle switch is grey)
- Loop Protection**: Disabled (toggle switch is grey)
- Link Flap Prevention**: Enabled (toggle switch is blue)
- Auto Recovery Time**: 300 (range: 30 – 86400) Seconds

Table 76. Interface 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.
Storm Control	If the incoming rate of unicast (with unknown destination), multicast, or broadcast packets exceeds a set threshold, the port moves to the suspended state. When 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), multicast, or broadcast packets exceeding the set threshold, that port will be disabled again. 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.
Auto Recovery Time	This configures the Auto Recovery time interval, in seconds. The Auto Recovery time interval is common for all the components. The default value of the timer is 300 seconds and the range is 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 Configuration**.

Use the Auto Recovery Configuration page to configure Auto Recovery settings for all the components. To display this page, click **Switching > Interface Auto Recovery**.

Suspended Interfaces

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

Figure 93. Suspended Interfaces

Table 77. 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: • BPDU Guard • Storm Control • Port Security • Loop Protection • Link Flap Prevention
Time to Recover (seconds)	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 the **Recover Interface**  button.



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

Trunk Configuration

Trunks allow for the aggregation of multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and throughput by providing load sharing capability.

A trunk interface can be either static or dynamic:

- **Dynamic**—Dynamic trunks 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 trunk. The PDUs contain information about each link and enable the trunk to maintain them.

- **Static**—Static trunks are assigned to a trunk group 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 trunk type.

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

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

A trunk 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 trunk. Similarly when links are added to a trunk, existing traffic may automatically shift to a different link member within the trunk. Before shifting traffic, the system ensures reordered frames do not exist.

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

The device supports up to 16 LAGs with 8 port members for static LAG, and up to 16 port members for LACP LAG.

To display this page, click **Switching > Trunk Configuration**.

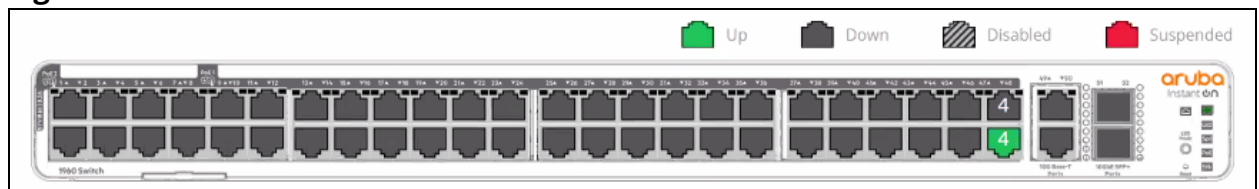


Trunks are sometimes referred to as link aggregation groups (LAGs) or port-channels.

Graphical Display

The top of the Trunk 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. The Trunk ports also show the Trunk ID.

Figure 94. Switch Panel View



Click a trunk member in this screen, to open the **Switching > Trunk Configuration** page.

For more information, see [Switch Panel View](#).

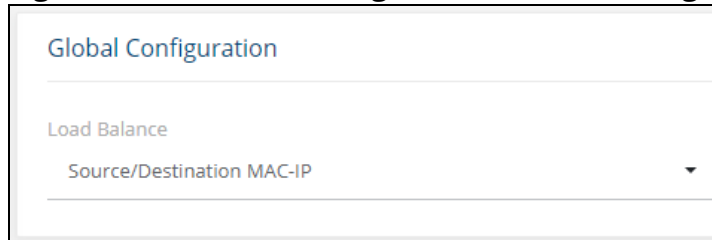
Global Configuration

You can use the Global Configuration page to select the hashing algorithm used to distribute traffic load among the physical ports of the trunk 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.

The following sets of packet attributes can be used to compute the hashing algorithm:

- Source and Destination MAC, IP and TCP/UDP Port fields
- Source and Destination MAC fields
- Source and Destination MAC and IP fields (this is the default)

Figure 95. Trunk Configuration Global Configuration Section



Global Configuration

Load Balance

Source/Destination MAC-IP

Table 78. Trunk Configuration Global Configuration Fields

Field	Description
Load Balance	These are the Load balance options: • Source/Destination MAC-IP-TCP/UDP Port • Source/Destination MAC • Source/Destination MAC-IP

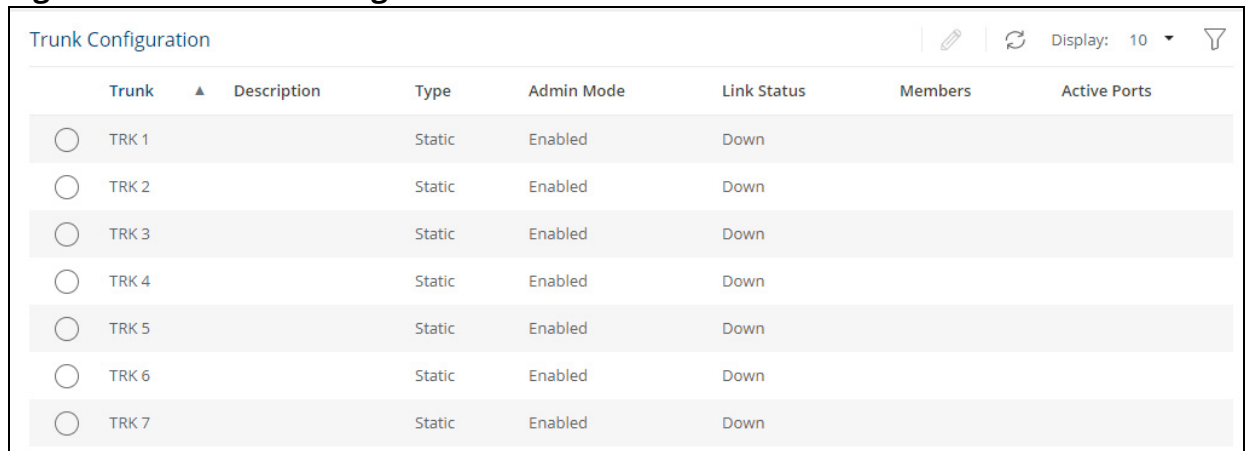
Click **APPLY** to update the trunk configuration.

Trunk Configuration

You can use the Trunk Configuration page 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.

To access the trunk configuration, click **Switching > Trunk Configuration** in the navigation pane.

Figure 96. Trunk Configuration



Trunk Configuration							
Trunk	Description	Type	Admin Mode	Link Status	Members	Active Ports	
☐ TRK 1		Static	Enabled	Down			
☐ TRK 2		Static	Enabled	Down			
☐ TRK 3		Static	Enabled	Down			
☐ TRK 4		Static	Enabled	Down			
☐ TRK 5		Static	Enabled	Down			
☐ TRK 6		Static	Enabled	Down			
☐ TRK 7		Static	Enabled	Down			

The following information is displayed for each trunk.

Table 79. Trunk Configuration 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 (LACPDU) 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 setting is enabled by default.
Link Status	Indicates the operational status of the trunk interface, which can be Up, Up (SFP) for ports with an installed SFP transceiver, 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.

Modifying Trunk Settings

To modify a trunk, select it and click **Edit** . The **Edit Trunk Configuration** page displays:

Figure 97. Edit Trunk Configuration Dialog Box

Edit Trunk Configuration

Trunk
Trunk 1

Admin Mode
☐

Description
(0 – 64 characters)

STP Mode
Enabled

Member Ports

2 3 4 | 1 5

CANCEL APPLY

Table 80. Edit Trunk Configuration Fields

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

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 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.

To display the EEE configuration page, click **Switching** > **EEE Configuration** in the navigation pane.

Global Configuration

Figure 98. Global Configuration

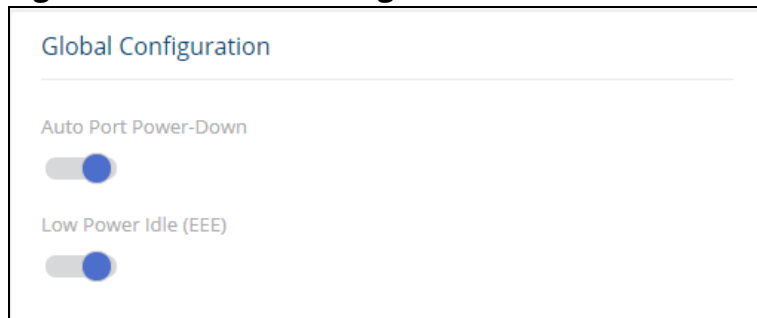


Table 81. Global Configuration Fields

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.
Low Power Idle (EEE)	EEE (Energy Efficient Ethernet) saves power by reducing power consumption on network ports that are not forwarding traffic. When Low Power Idle (EEE) is enabled, the ports will enter a low-power mode to reduce power consumption during periods there is no traffic on a network port. The EEE feature works on ports in auto-negotiation mode, where the port is negotiated to either 100 Mbps full duplex or 1 Gbps (1000 Mbps) full duplex. 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 switch configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Global Status

When EEE is enabled, you can use the EEE Status tile to view estimated power savings and power consumption information.

Figure 99. Global Status

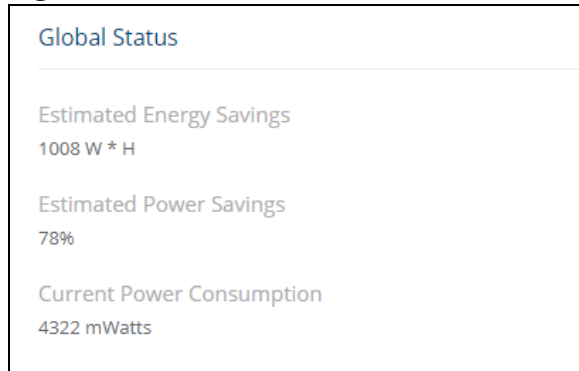


Table 82. Global Status Fields

Field	Description
Estimated Energy Savings	The estimated cumulative energy saved on the switch (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 switch required 10% less power.
Current Power Consumption	The estimated power consumption by all ports.

Interface Status

This page displays EEE status information for each interface.

To display the Interface Status page, click **Switching > EEE Configuration** in the navigation pane.

Figure 100. Interface Status Tile

Interface Status					
Interface ▲	Link Partner EEE Support	Auto Port Power-Down Status	LLDP Wakeup Time Negotiation	Rx Wakeup Time	Tx Wakeup Time
1	No	Active	No	0	0
2	Yes	Inactive	No	17	17
3	Yes	Inactive	No	17	17
4	Yes	Inactive	No	17	17
5	Yes	Inactive	No	17	17
6	Yes	Inactive	No	17	17
7	No	Active	No	0	0
8	Yes	Inactive	No	17	17
9	Yes	Inactive	No	17	17
10	No	Active	No	0	0

« < 1 2 3 4 5 6 > »

REFRESHAPPLY

Table 83. EEE 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).

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.

Aruba Instant On 1960 Switch Series series switches support 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.

To display the Spanning Tree General Settings page, click **Spanning Tree > General Settings** in the navigation pane.

Global Configuration

These are the global configurations for Spanning Tree Switch:

Figure 101. Spanning Tree Global Configuration Page

Global Configuration

Spanning Tree Admin Mode

☒

Spanning Tree Maximum Hops

20

(6 – 40)

Protocol Version

☐ STP ☒ RSTP ☐ MSTP

Configuration Name

00:00:00:12:17:29

(1 – 32 characters)

Bridge Priority

32768

Configuration Revision Level

0

(0 – 65535)

Bridge Max Age

20

(6 – 40) Seconds

BPDU Filter

☐

Bridge Forward Delay

15

(4 – 30) Seconds

Table 84. Spanning Tree 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 switch 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 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. The default priority is 32768. The valid range is 0-61440, in steps of 4096.
Bridge Max Age	The amount of time a bridge waits before implementing a topological change. The default is 20. The valid range is 6-40.

Field	Description
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.
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 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.
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 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.

If you modify any settings, Click **APPLY** to update the switch configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Global Settings

These are the Global Settings that you can view:

Figure 102. Spanning Tree Global Settings Page

Global Settings		
Root Bridge Identifier 32768:00:00:A1:A2:A3:A4	Root Path Cost 80000	Topology Change Count 2
Bridge Hello Time 2 Seconds	Root Port 23	Root Guard Interfaces N/A
Spanning Tree Tx Hold Count 3	Max Age 20 Seconds	TCN Guarded Interfaces 1-28,TRK1-TRK8
Bridge Identifier 32768:38:21:C7:CA:11:E6	Forward Delay 15 Seconds	BPDU Filtered Interfaces N/A
Time Since Topology Change 19:25:19	Hold Time 1 Seconds	CST Path Cost 0
Configuration Digest Key AC36177F50283CD4B83821D8AB26DE62	CST Regional Root 32768:38:21:C7:CA:11:E6	Configuration Format Selector 0

Table 85. Spanning Tree Global Settings Fields

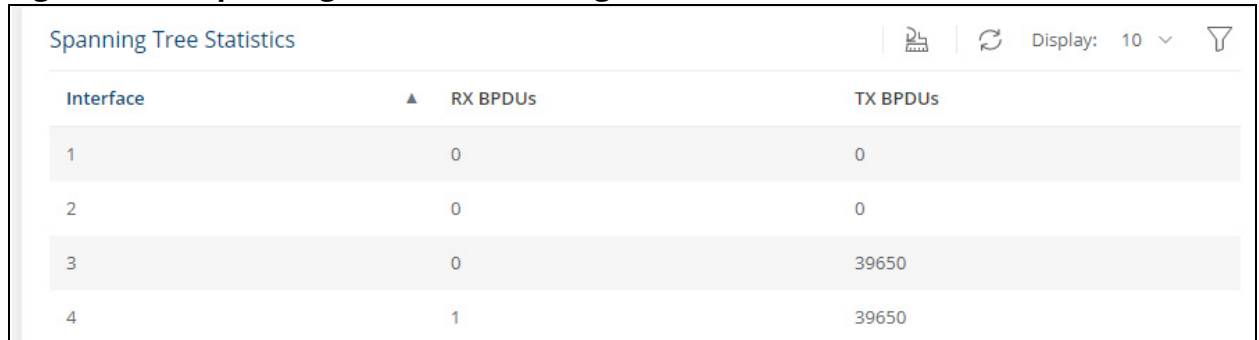
Field	Description
Root Bridge Identifier	The bridge identifier of the root bridge for the spanning tree. The identifier is made up of the bridge priority and the base MAC address. When electing the root bridge for the spanning tree, if the bridge priorities for multiple bridges are equal, the bridge 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. 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.
CST Path Cost	The path cost to the CST tree regional root.
TopologyChange Count	The number of topology changes that occurred since last time the device reloaded.
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.
Configuration Format Selector	The version of the configuration format being used in the exchange of BPDUs.

Spanning Tree Statistics

Use the Spanning Tree Statistics page 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 > General Setting** in the navigation pane, and scroll down to the **Spanning Tree Statistics** tile.

Figure 103. Spanning Tree Statistics Page



Interface	RX BPDUs	TX BPDUs
1	0	0
2	0	0
3	0	39650
4	1	39650

Table 86. Spanning Tree Statistics Fields

Field	Description
Interface	The port or trunk associated with the rest of the data in the row.
Rx BPDUs	The number of STP/RSTP/MSTP (IEEE 802.1d) BPDUs received by the interface.
Tx BPDUs	The number of STP/RSTP/MSTP 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 BPDUs 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. To configure CST settings for an interface and to view additional information about the interface's role in the CST topology, select the interface to view or configure and click **Edit**.

To view the CST Configuration page, click **Spanning Tree > CST Configuration** in the navigation pane.

CST Port Configuration

Figure 104. CST Port Configuration Tile

CST Port Configuration					
☐	Interface	▲ Port Role	Port Forwarding State	Port Priority	Port Path Cost
☐	1	Disabled	Disabled	128	2000000
☐	2	Disabled	Disabled	128	20000
☐	3	Designated	Forwarding	128	20000
☐	4	Designated	Forwarding	128	20000

Table 87. 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.
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	• 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**  . This option is available if you have a single port selected. For more information, see [CST Port Details Fields](#).
- **Edit CST Settings**  . This option is available if you select one or more ports. The same settings are applied to all selected interfaces. For more information, see [Edit CST Port Fields](#).
- **Clear Detected Protocols**  . This option is available if you select one or more ports. Click this button to restart the STP migration process with the link partner. This forces STP mode renegotiation with the link partner.

Figure 105. Edit CST Port Settings Page

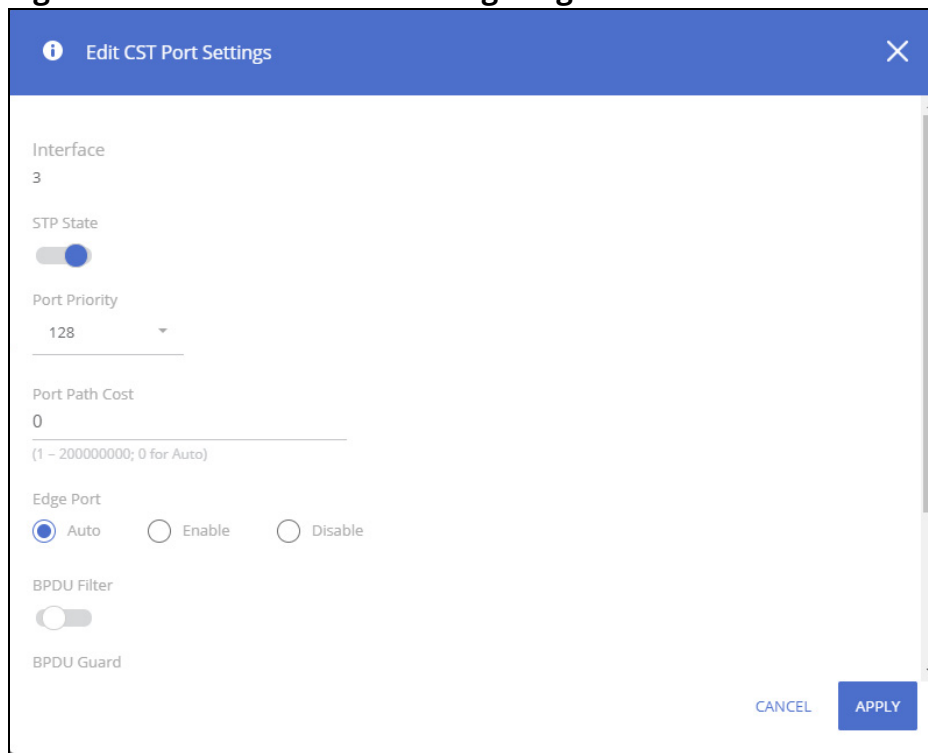


Table 88. Edit CST Port Fields

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.

Field	Description
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 interface. This feature requires BPDU filtering to be enabled globally.
BPDU Guard	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.
Root Guard	When enabled, Root Guard allows the interface to discard any superior information it receives to protect the root of the switch 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** 

Figure 106. CST Port Details Page

CST Port Details

Interface
1

STP State
Enabled

Port Priority
128

Port Path Cost
2000000

Auto-Calculate Port Path Cost
Enabled

BPDU Filter
Disabled

BPDU Guard Effect
Disabled

Port ID
128.1

Port Forwarding State
Disabled

CLOSE

The following table describes the fields in the **CST Port Details** dialog box.

Table 89. 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).
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.

Field	Description
Port ID	A unique value that is automatically generated based on the port priority value and the interface index.
Port Forwarding State	• 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 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 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 protect the root of the switch 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 upon 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.

To display the Spanning Tree MSTP Configuration page, click **Spanning Tree > MSTP Configuration** in the navigation pane.

MSTP Configuration

Figure 107. MSTP Configuration Tile

MSTP Configuration								
+ ✎ 🗑 ↺ Display: 10 ▼ 🔍								
☐ MSTP ID ▲	Priority	# of Associated VLANs	Bridge Identifier	Time Since Topology Change	Designated Root	Root Path Cost	Root Port	
☐ 1	4096	1	4096:00:00:44:44:55:88	23	4096:00:00:44:44:55:88	0	0	
« < 1 > »								

Table 90. 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.
# 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.

If you modify any settings, click **APPLY** to update the switch configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Adding, Editing or Removing an MSTP Configuration

To add an MSTP Instance configuration, click Add +.

To edit an existing configuration, click the check box to the left of the entry and click **Edit** ✎. The fields in the **Add** and **Edit** dialog boxes are the same.

To remove an existing MSTP Instance, click the check box to the left of the session entry and click **Remove**  .

Figure 108. Edit MSTP Entry

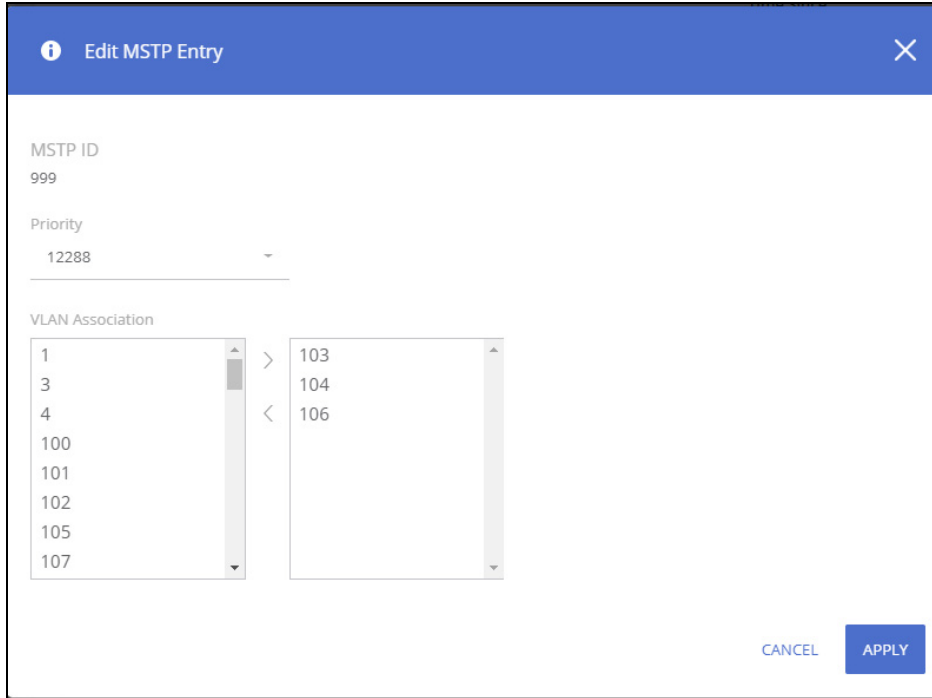


Table 91. Add/Edit MSTP Entry Fields

Field	Description
MSTP ID	Enter a unique number that identifies the MSTP instance. Valid values are 1-4094
Priority	Enter 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.
VLAN Association	Specify the VLANs to associate to this MSTP instance. the VLANs are specified by their VLAN ID.

MSTP Port Configuration

From the MSTP Port Configuration tile, you can view additional details about the MSTP settings on a port or configure additional settings for one or more ports.

To display the Spanning Tree MSTP Port Configuration tile, click **Spanning Tree > MSTP Configuration** in the navigation pane.

Figure 109. MSTP Port Configuration Tile

MSTP Port Configuration					
MSTP ID 1					
☐	Interface	Port Role	Port Forwarding State	Port Priority	Port Path Cost
☐	1	Disabled	Disabled	128	2000000
☐	2	Disabled	Disabled	128	20000
☐	3	Designated	Forwarding	128	20000
☐	4	Designated	Forwarding	128	20000

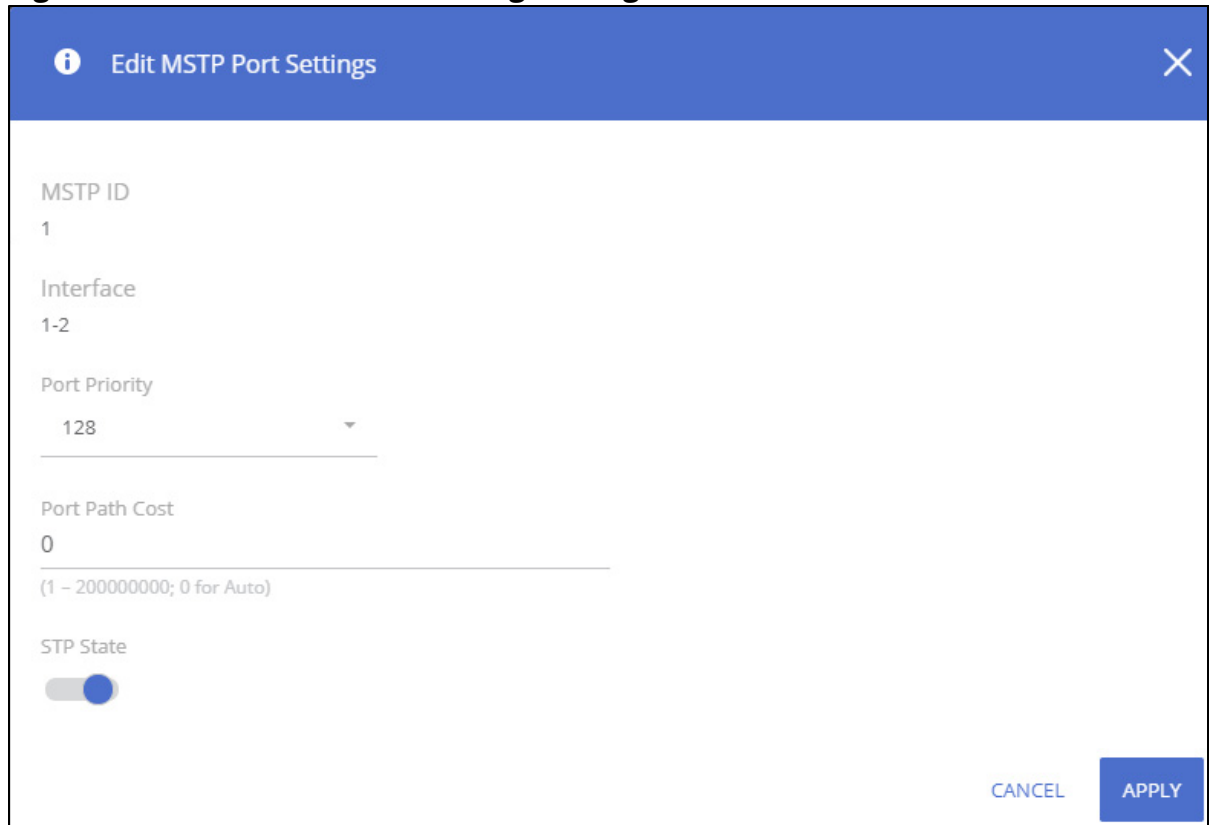
Table 92. MSTP Port Configuration Fields

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.
Port Forwarding State	- 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.

Viewing MSTP Port Details or Editing MSTP Port Settings

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 110. Edit MSTP Port Settings Dialog Box



The dialog box titled "Edit MSTP Port Settings" has a blue header bar with an information icon and a close button. The main area contains the following fields:

- MSTP ID:** A text field with the value "1".
- Interface:** A text field with the value "1-2".
- Port Priority:** A dropdown menu showing "128".
- Port Path Cost:** A text field with the value "0". Below it, a note reads "(1 - 200000000; 0 for Auto)".
- STP State:** A toggle switch that is currently turned on (blue).

At the bottom right, there are two buttons: "CANCEL" and "APPLY".

Table 93. Edit MSTP Port Settings Fields

Field	Description
MSTP ID	The ID of each MST instance this port is associated with.
Interface	Identifies the interface.
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 Enable or Disable, Disable is the default.

To view additional information about an interface's role in the MST topology, select the MST instance and the interface to view, and then click **Details**  .

Figure 111. MSTP Port Details

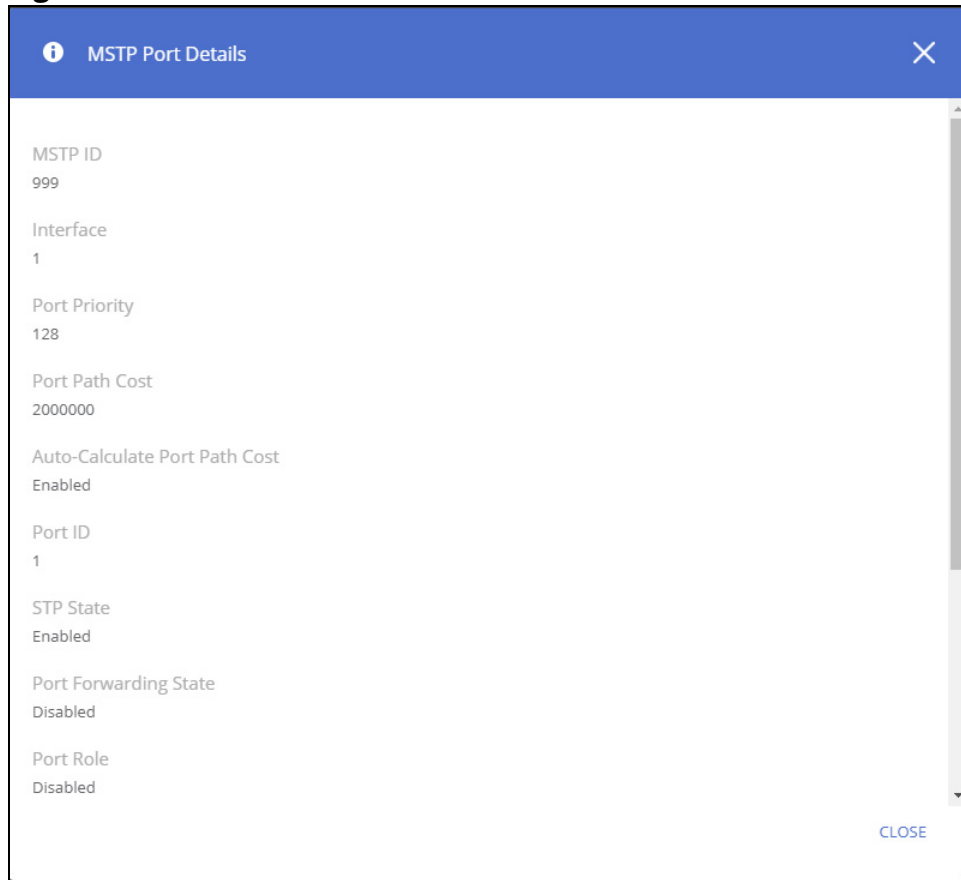


Table 94. MSTP Port Details Fields

Field	Description
MSTP ID	The ID of each MST instance this port is associated with.
Interface	Identifies the interface.
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 from the port to the root bridge.
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 Enable or Disable, Disable is the default.

Field	Description
Port Forwarding State	- 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 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.

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 Configuration**.

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 displays 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.

Aruba Instant On 1960 Switch Series switches support up to 512 VLANs.

- Access SKUs support up to 256 VLANs
- Aggregate SKUs support up to 512 VLANs
- Hybrid Mode stack supports up to 256 VLANs

VLAN Configuration

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

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

Graphical Display

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 112. 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 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.

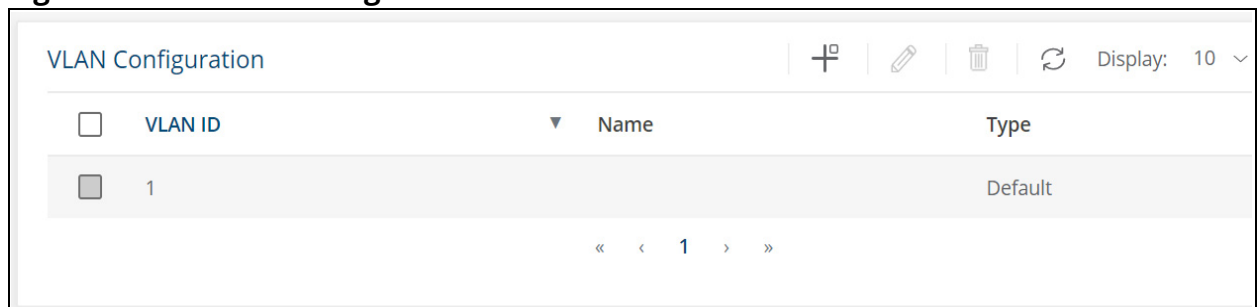
If there is no indication, this means that the port is not a member of a VLAN. For more information, see [Switch Panel View](#).

Double-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.

Click **APPLY** to save any changes for the currently selected VLAN interface.

VLAN Configuration

Figure 113. VLAN Configuration Tile



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. See [Management VLAN Settings](#) for additional information about the management VLAN.

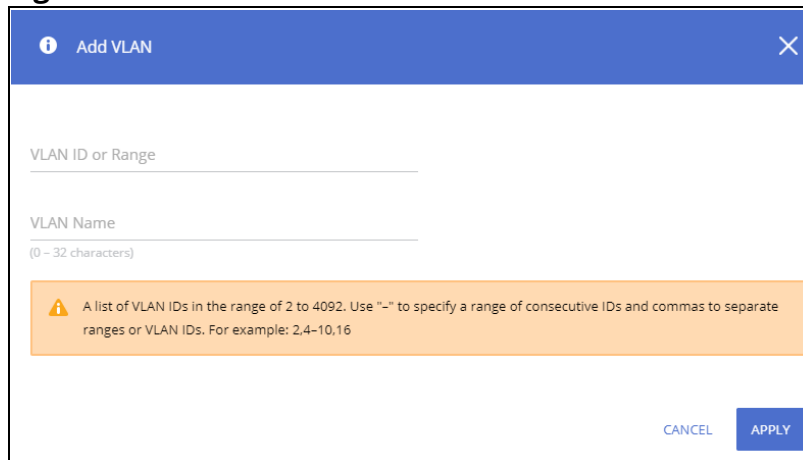
The following information is displayed for each VLAN:

Table 95. 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 <i>priority tag</i> .
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.

To add a VLAN, click **Add** .

Figure 114. Add VLAN

The dialog box has a blue header with an information icon, the title "Add VLAN", and a close button. It contains two text input fields: "VLAN ID or Range" and "VLAN Name" with a character count "(0 - 32 characters)". An orange warning box with an exclamation mark icon contains the text: "A list of VLAN IDs in the range of 2 to 4092. Use '-' to specify a range of consecutive IDs and commas to separate ranges or VLAN IDs. For example: 2,4-10,16". At the bottom right are "CANCEL" and "APPLY" buttons.

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



VLAN 4093 and 4094 are reserved for internal system use.

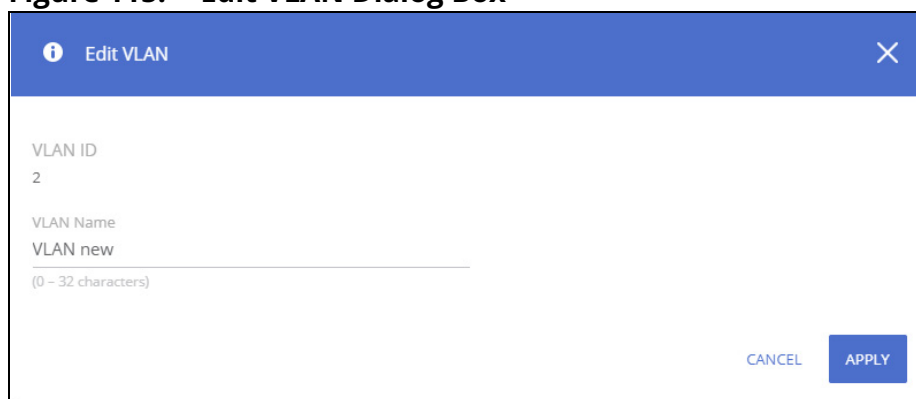
To create a range of VLANs, specify the beginning and ending VLAN IDs, separated by a dash. Optionally you can define a name for the VLAN in the **VLAN Name** field.

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

When you have entered the VLAN IDs and/or range(s) as needed, click **APPLY**.

To change the VLAN name, select it on the VLAN Configuration tile and click **Edit**  .

Figure 115. Edit VLAN Dialog Box

The dialog box has a blue header with an information icon, the title "Edit VLAN", and a close button. It contains two text input fields: "VLAN ID" with the value "2" and "VLAN Name" with the value "VLAN new" and a character count "(0 - 32 characters)". At the bottom right are "CANCEL" and "APPLY" buttons.

On the Edit VLAN Configuration page, specify the new name consisting of 0 to 32 alphanumeric characters and click **APPLY**.

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.

To configure interface VLAN memberships, click **VLAN > VLAN Configuration** in the navigation pane and scroll down to the VLAN Membership tile.

This tile has two tabs:

- VLAN Membership - By Interface - for configuring the interface to VLAN membership for one or more VLANs.
- VLAN Membership - By VLAN - 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 116. VLAN Membership - By Interface Tab

Interface	Tagged VLANs	Untagged VLAN
1	1	
2		1
3		1
4		1

Table 96. 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 one or more ports and click **Edit** . Or, click **Edit All** to configure all ports at the same time.

On the **Edit VLAN Membership** page, enter the **Tagged VLAN(s)** for this interface, you can enter a range, or comma-separated list.

In addition, you can enter a single Untagged VLAN. The untagged VLAN cannot be one of the Tagged VLANs.

VLAN Membership - By VLAN Tab

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

Figure 117. VLAN Membership - By VLAN Tab

Interface	Participation	Tagging
☐ 1	Included	Tagged
☐ 2	Included	Untagged
☐ 3	Included	Untagged

Table 97. VLAN Membership - By VLAN Tab Fields

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

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

On the **Edit VLAN Membership** page, 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.

Click **APPLY** to save any changes for the currently selected VLAN. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

VLAN Interface Configuration

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

To view this tile, click **VLAN > VLAN Configuration** in the navigation pane.

Figure 118. VLAN Interface Configuration Tile

VLAN Interface Configuration						
☐	Interface ▲	Port VLAN ID	Acceptable Frame Type	Ingress Filtering	Untagged VLAN	Tagged VLANs
☐	1	1	Tagged and Untagged	Enabled	1	1
☐	2	1	Tagged and Untagged	Enabled	1	1
☐	3	1	Tagged and Untagged	Enabled	1	1
☐	4	1	Tagged and Untagged	Enabled	1	1
☐	5	1	Tagged and Untagged	Enabled	1	1

Table 98. 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.

Field	Description
Acceptable Frame Type	Indicates how the interface handles untagged and priority tagged frames: • Tagged and Untagged– Untagged and priority 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	VLANs that are 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 these settings for one or more interfaces, select the interface and click **Edit**  . Or, click **Edit All**  to configure all interfaces at the same time.

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 OUI's.

The voice VLAN ID must be a manually configured through the switch's web interface and ports enabled to participate in the voice VLAN. When the switch receives a packet with a source MAC address matching to one of the configured telephony OUIs, the port is dynamically placed in the voice VLAN.

The switch supports up to 16 OUIs. You can manually add or remove OUIs. The switch also supports pre-defined OUIs that exist on the switch by default. If the switch is reset back to factory defaults, only the pre-defined OUIs are available.

These are the pre-defined OUIs:

- Siemens (00-01-e3)
- Avaya (00-09-6e)
- 3Com (00-0f-e2)
- H3C (00-60-b9)
- Cisco (00-03-6b)
- 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

Figure 119. Global Configuration

Global Configuration

Voice VLAN State

Voice VLAN ID

1

CoS/802.1p Handling

☒ Remap ☐ Remark

CoS/802.1p Value

6

(0 - 7)

Membership Aging Time

1 0 0

Day(s) Hour(s) Minute(s) (1 min - 30 days)

Table 99. Global Configuration Fields

Field	Description
Voice VLAN State	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.
Voice VLAN ID	Specify the VLAN that will carry voice traffic on enabled interfaces.
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 "CoS/802.1p Value" field. • remark - remap and remark the L2 field of incoming voice traffic to the CoS specified in the "CoS/802.1p Value" field.
CoS/802.1p Value	The CoS value to remap or remark to.
Membership Aging Time	Set the maximum duration (days, hours and minutes) that the enabled port will be a member of the voice VLAN, after receiving voice VLAN traffic.

Telephony OUI Configuration

Use 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 120. Telephony OUI Configuration

Table 100. 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 restore the defaults, click **Restore Default** .

Click **APPLY** to save any changes for the currently selected configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Voice VLAN Interface Settings

Figure 121. Voice VLAN Interface Settings Page

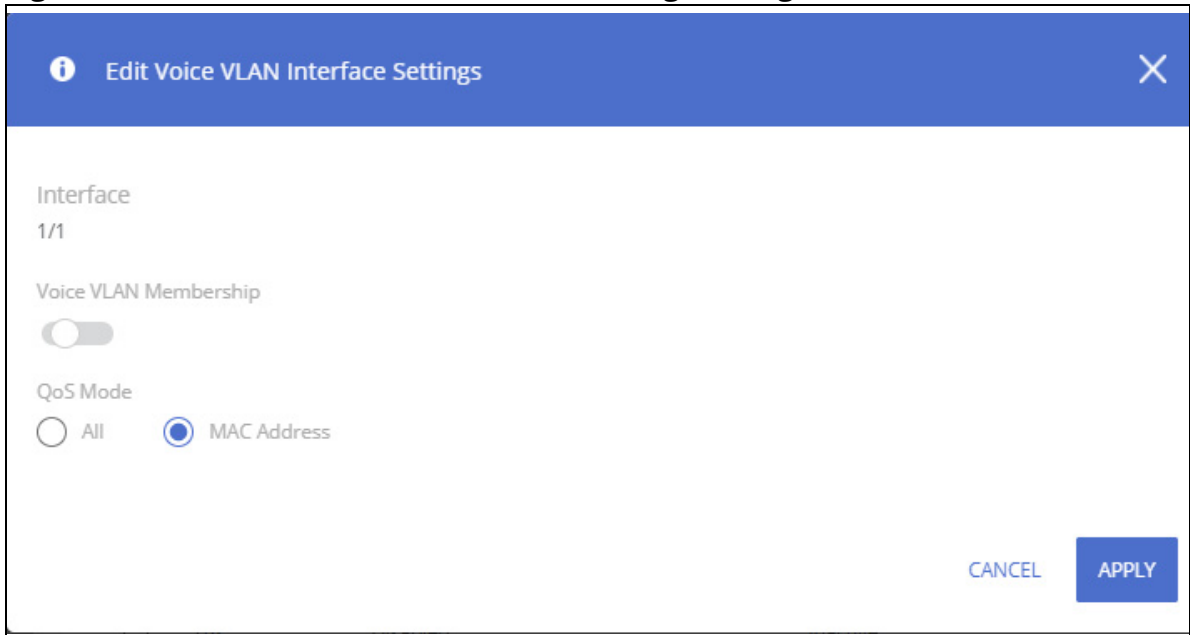
Voice VLAN Interface Settings				
☐	Interface	Admin Voice VLAN Membership	Operational Voice VLAN Membership	QoS Mode
☐	1	Disabled	Inactive	MAC Address
☐	2	Disabled	Inactive	MAC Address
☐	3	Disabled	Inactive	MAC Address
☐	4	Disabled	Inactive	MAC Address
☐	5	Disabled	Inactive	MAC Address

Table 101. 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 interface(s) that are being configured.
Admin Voice VLAN Membership	Click Enable or Disable to enable 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 window, the field name is Voice VLAN Membership.
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 will be 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 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.
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 modify these settings for one or more interfaces, select the interface and click **Edit**  . Or, click **Edit All**  to configure all interfaces at the same time.

Figure 122. Edit Voice VLAN Interface Settings Dialog Box



The dialog box has a blue header bar with the title "Edit Voice VLAN Interface Settings" and a close button (X) on the right. The main content area is white and contains the following settings:

- Interface**
1/1
- Voice VLAN Membership**
☐
- QoS Mode**
☐ All ☒ MAC Address

At the bottom right, there are two buttons: "CANCEL" and "APPLY".

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**.

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

Figure 123. LLDP Global Configuration Tile

LLDP Global Configuration

Transmit Interval

30

(5 – 32768) Seconds

Transmit Hold Multiplier

4

(2 – 10) Seconds

Re-Initialization Delay

2

(1 – 10) Seconds

Modification Interval

5

(5 – 3600) Seconds

You can configure the following global settings:

Table 102. LLDP Global Configuration Fields

Field	Description
Transmit Interval	Specify the time between transmission of LLDPDUs. The range is from 5 to 32768 seconds and 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 range is from 2 to 10 seconds, and the default is 4 seconds.
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.
Modification 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.

If you change these settings, 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

Use the LLDP Global Information tile to view the information that is included in the switch LLDP advertisement.

Figure 124. LLDP Global Information

LLDP Global Information

Chassis ID

00:00:B0:17:12:00

Chassis ID Subtype

MAC Address

Capabilities Supported

Bridge

Capabilities Enabled

Bridge

Table 103. 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

The following information is displayed for each LLDP interface.

Figure 125. Interface Configuration

Interface Configuration										Display: 10	
☐	Interface	▲	Link Status	Transmit	Receive	Notify	Transmit Management Information				
☐	1		Link Down	Enabled	Enabled	Enabled	Yes				
☐	2		Link Up	Enabled	Enabled	Enabled	Yes				
☐	3		Link Up	Enabled	Enabled	Enabled	Yes				
☐	4		Link Up	Enabled	Enabled	Enabled	Yes				
☐	5		Link Up	Enabled	Enabled	Enabled	Yes				

Table 104. 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 switch can receive LLDPDUs from other devices.
Notify	Enable to have LLDP generate a log file 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 interface settings, select one or more interfaces and click **Edit** to display the Edit LLDP Interface page. Or, click **Edit All**  to configure all interfaces at the same time.

Figure 126. Edit LLDP Interface

Edit LLDP Interface

Interface
1/1

Transmit ☒

Receive ☒

Notify ☒

Transmit Management Information ☒

LLDP/LLDP-MED Optional TLVs

802.3 MAC-PHY ☐

802.3 Power via MDI ☒

802.3 Link Aggregation ☐

802.3 Maximum Frame Size ☐

CANCEL APPLY

Move the toggle to the right to enable the associated feature. Move it to the left to disable it. The following additional options are configurable from the **Edit** dialog.

Table 105. Additional LLDP Interface Fields

Field	Description
802.3 MAC-PHY	Duplex and bit rate capability and the current duplex and bit rate settings of the sending device.
802.3 Power via MDI	This field appears for PoE devices. This TLV supports the following extensions. • Type 2 (12 octets) • Type 3 (29 octets) This option is enabled by default.

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.

Device Information Tile

This tile has two tabs:

- Remote Device Information - for the remote devices
- Local Device Information - for the local devices

To display the Device Information tabs, click **Neighbor Discovery > LLDP** in the navigation pane, and scroll down to the **Remote/Local Device Information** tile.

Remote Device Information

Use the Remote Device Information tab to view 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 127. Remote Device Information Tab

Remote Device Information								Local Device Information
								Display: 10  
Interface ▲	Remote ID	Chassis ID	Port ID	Port Description	System Name	Capabilities Supported	Capabilities Enabled	System ID
1/1	3	00:00:00:02:17:03	1/2	1/2		Bridge	Bridge	
« < 1 > »								

Table 106. 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. If the port description is not configured, the field may show the interface number of the remote port, or it may be blank.
System Name	The system description configured on the remote device. If the system description is not configured, the field is blank.

Field	Description
Capabilities Supported	The capabilities on the remote device. The possible capabilities include other, repeater, bridge, WLAN AP, router, telephone, DOCSIS cable device, and station.
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

Use the Local Device Information tab to view LLDP information for 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 128. Local Device Information Tab

Remote Device Information		Local Device Information					Display: 10	
Interface	Port ID	Port ID Subtype	Port Description					
☐ 1	1	Interface Name	1					
☐ 2	2	Interface Name	2					
☐ 3	3	Interface Name	3					
☐ 4	4	Interface Name	4					
☐ 5	5	Interface Name	5					

Table 107. Local Interface 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 129. LLDP Interface Information

LLDP Interface Information

Interface

1/1

Chassis ID Subtype

MAC Address

Chassis ID

00:00:00:12:17:29

Port ID Subtype

Interface Name

System Name

N/A

System Description

Aruba Instant On 1960 48G 40p Class4 8p Class6 PoE 2XGT 2SFP+ 600W Switch JL809A, InstantOn_1960_2.3.3.0 (56), Linux 4.4.120, U-Boot 2013.01 (V1.0.0.22)

Capabilities Supported

Bridge

Capabilities Enabled

Bridge

Management Address

N/A

Management Address Type

N/A

CLOSE

This page displays the following fields.

Table 108. LLDP Interface Information Fields

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. The system name is configured on the Dashboard page.
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.

Field	Description
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 Link Layer Discovery Protocol (LLDP) Statistics tile displays per-port information for LLDP and LLDP-MED frames transmitted and received on the switch.

To display the LLDP Statistics tile, click **Neighbor Discovery > LLDP** in the navigation pane.

Figure 130. LLDP Statistics Tile

LLDP Statistics							
Interface ▲	Transmitted Frames	Received Frames	Discarded Frames	Errors	Discarded TLVs	Unrecognized TLVs	Neighbor Ageouts
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0

Table 109. 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.

Click **Clear All**  to reset all statistics to 0.

LLDP-MED

Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) is an enhancement to LLDP that enables:

- Auto-discovery of LAN policies (such as VLAN and Layer 2 Priority settings) for VoIP phones and other network elements.
- Switch location discovery for creation of location databases. For example, this information is used during emergency calls to identify the location of the MED (for VoIP and enhanced 911 services).
- 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 Discovery > LLDP-MED** in the navigation pane.

LLDP-MED Global Configuration

Figure 131. LLDP-MED Global Configuration Tile

The screenshot shows a configuration tile titled "LLDP-MED Global Configuration". It contains two main sections: "Fast Start Repeat Counter" with a value of "3" and a range of "(1 - 10)", and "Device Class" with a value of "Network Connectivity".

The following global settings display:

Table 110. 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 Aruba Instant On 1960 Switch Series switch is classified as a Network Connectivity device.

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

Use the LLDP Global Information tile to view the information that is included in the switch LLDP advertisement.



The same tile appears in the LLDP page.

Figure 132. LLDP Global Information

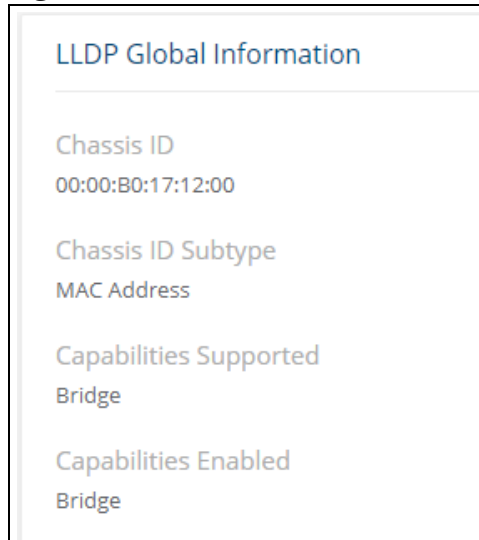


Table 111. LLDP Global Information Fields

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 the interfaces.

To view the Interface Configuration tile, click **Neighbor Discovery > LLDP-MED** in the navigation pane.

Figure 133. Interface Configuration Tile

Interface Configuration						
☐	Interface ▲	Link Status	MED Mode	Notification Status	Operational Status	Transmitted TLVs
☐	1	Link Down	Enabled	Disabled	Disabled	Capabilities, Network Policy
☐	2	Link Up	Enabled	Disabled	Disabled	Capabilities, Network Policy
☐	3	Link Up	Enabled	Disabled	Disabled	Capabilities, Network Policy
☐	4	Link Up	Enabled	Disabled	Disabled	Capabilities, Network Policy
☐	5	Link Up	Enabled	Disabled	Disabled	Capabilities, Network Policy

The following information is displayed for each port:

Table 112. 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 switch. The switch waits for the LLDP-MED switch 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 Aruba Instant On 1960 Switch Series switch, can transmit TLVs of the following types: • Capabilities • Network Policy • Power Sourcing Entity (PSE)

To enable or disable LLDP-MED on one or more interfaces, and to configure related features, select the interfaces and click **Edit** . Or, click **Edit All**  to configure all ports at the same time.

Figure 134. Edit LLDP-MED Interface

The screenshot shows a dialog box titled "Edit LLDP-MED Interface". Inside, under the heading "Interface 1", there are three toggle switches, all of which are currently turned on (indicated by a blue circle on the right). The switches are labeled "LLDP-MED", "Configuration Notification", and "Network Policy TLV Transmit". At the bottom right of the dialog, there are two buttons: "CANCEL" and "APPLY".

Table 113. 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 on interface sending topology change notifications. Default is Disabled.
Network Policy TLV Transmit	Enable/disable on interface sending Network policy TLV. Default is Enabled.

Remote Device Information

Use the LLDP-MED Remote Device Information page to view 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.

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

Figure 135. LLDP-MED Remote Device Information Page

Table 114. LLDP 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.

Field	Description
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.

Displaying Remote Device Details

To view additional information about a remote device, select the row including remote device information and click **Details**  .

The following fields appear on the LLDP-MED **Remote Device Information** page:

Table 115. LLDP Remote Device 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.
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.

Field	Description
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.

Power Over Ethernet (PoE) functionality is supported on certain Aruba Instant On 1960 Switch 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 three configurable PoE priority values (Critical, High, 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.

The 1960 Class 6 PoE switches support the IEEE 802.3af/at/bt standards providing 60W of power for Class 6 PD connections while maintaining backwards compatibility with IEEE 802.3af/at standards.

All PoE Class 6 switch ports are capable of delivering 60W per PoE port, up to the maximum power supply budget.

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



The information in this chapter relates to switches that support PoE. This page appears only when there is at least one unit in the stack that supports PoE.

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

Table 116. PoE Maximum Power per Model

Switch	PoE Support	Maximum Power
Aruba Instant On 1960 24G 20p Class 4 4p Class 6 PoE 2XGT 2SFP+370W Switch	20 ports class 4 PoE 4 ports class 6 PoE	370W
Aruba Instant On 1960 48G 40p Class 4 8p Class 6 PoE 2XGT 2SFP+ 600W Switch	40 ports class 4 PoE 8 ports class 6 PoE	600W

PoE Configuration

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

To view this page, click **Power Over Ethernet > PoE Configuration** in the navigation pane.

Graphical Display

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.

Activity

Click the **Activity** radio button to show which ports have the following conditions:

Activity 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.

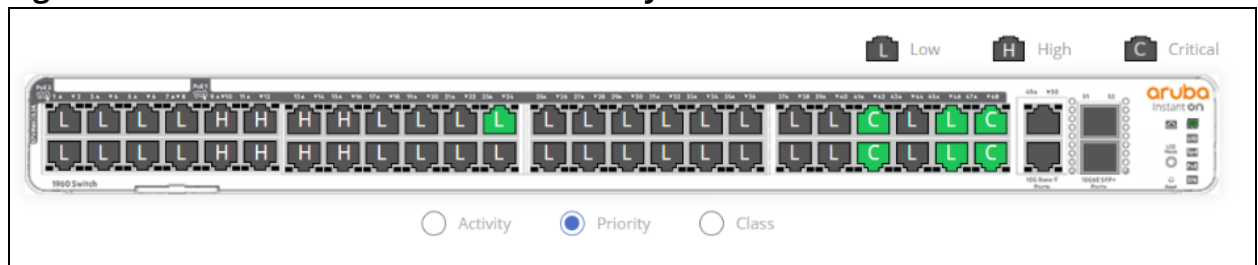
Priority

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

- L - this indicates Low priority
- H - this indicates High priority
- C - this indicates Critical priority

The following graphic shows the PoE Switch panel view with the Priorities showing on the ports.

Figure 136. PoE Switch Panel View - Priority



Class

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

- 0 - this indicates 0.44-12.95W
- 1 - this indicates 0.44-3.84W
- 2 - this indicates 3.84- 6.49W
- 3 - this indicates 6.49-12.95W
- 4 - this indicates 12.95-25.5W

Click a PoE port in this screen to open the **Edit Port PoE Configuration** page.
For more information, see [Switch Panel View](#).

Status

The Status tile displays PoE global information: the total power, actual power consumption, and PoE status.

Figure 137. Status Tile

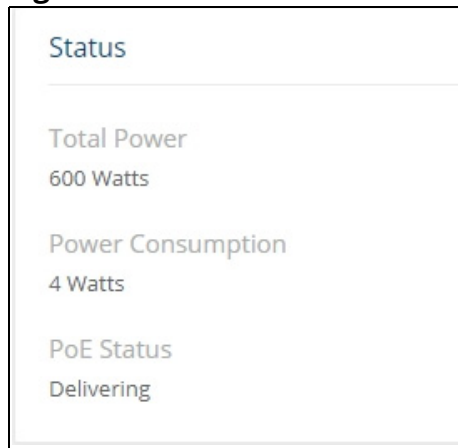


Table 117. Status Fields

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. • Idle—The PoE functionality is operational but no ports are delivering power, and no ports have errors. • Faulty—one or more ports is 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 is in PoE fault state. this does not include hardware-related fault states.



PoE Fault and Activity status is also indicated through the switch port and PoE LEDs. See [System LEDs](#) for more information.

Consumption History

The Consumption History tile provides information on average PoE consumption on the switch over the last hour, day and week. This information is useful for monitoring PoE trends and behavior.

The consumption history information is saved to the switch non-volatile memory so it is available after switch reboot.

Figure 138. Consumption History Tile

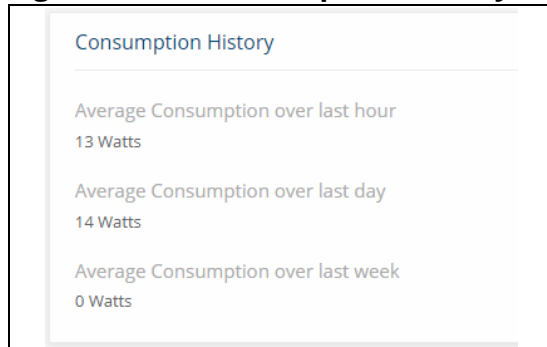


Table 118. Consumption History Fields

Field	Description
Average Consumption over last hour	The average power consumption by PDs attached to the switch, over the last hour (in units of watts).
Average Consumption over last day	The average power consumption by PDs attached to the switch, over the last day (in units of watts).
Average Consumption over last week	The average power consumption by PDs attached to the switch, over the last week (in units of watts).

Port Configuration

You can use the PoE Port Configuration page to administratively enable or disable PoE on ports and to view and configure the port priority and other settings.

To view this page, click **Power Over Ethernet > PoE Configuration** in the navigation pane.

Figure 139. PoE Port Configuration Tile

The figure shows a 'Port Configuration' tile with a title bar and a table of port settings. The table has columns for Interface, Admin Mode, Priority, Schedule, Class Limit, Status, Fault Status, Output Power, Power Management Mode, and Pre Standard Detection. There are three rows of data for interfaces 1, 2, and 3.

Interface	Admin Mode	Priority	Schedule	Class Limit	Status	Fault Status	Output Power	Power Management Mode	Pre Standard Detection
1	Enabled	Low	None	Unlimited	Delivering	None	14.8W (4)	Usage	Disabled
2	Enabled	High	None	Class 3	Searching	None	0	Class	Enabled
3	Enabled	Low	None	Unlimited	Searching	None	0	Usage	Disabled

The following settings are displayed.

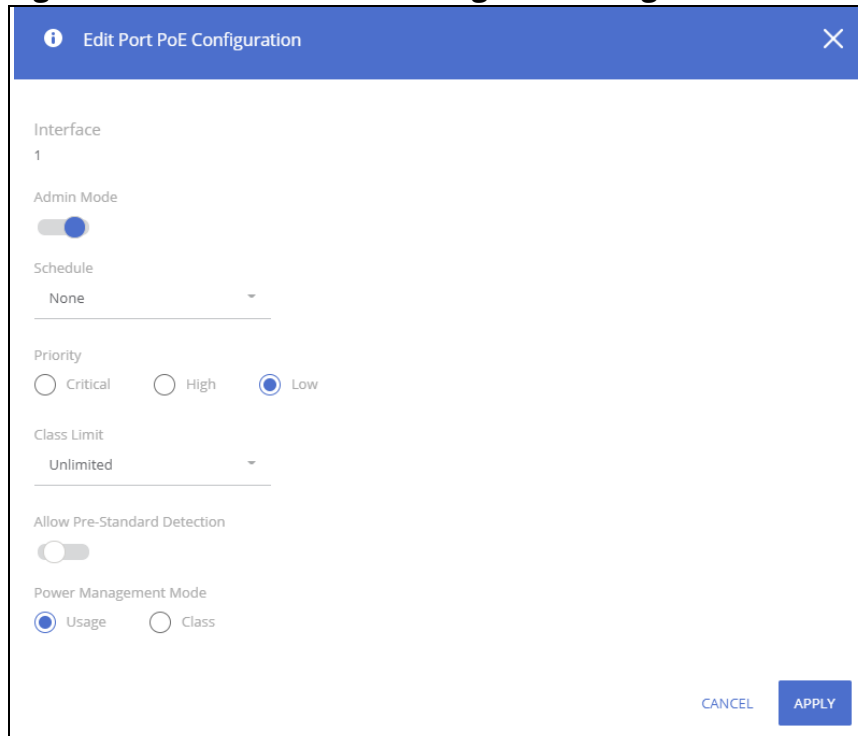
Table 119. PoE Port Configuration Fields

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.
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.
Schedule	The scheduled time when source power is available on this port. Options are: • None—Source power is available at all times. This is the default selection. • Schedule 1—Source power is available during the configured schedule in Schedule 1. • Schedule 2—Source power is available during the configured schedule in Schedule 2. • Schedule 3—Source power is available during the configured schedule in Schedule 3. You can configure schedules on the Schedule Configuration page in Setup Network.
Class Limit	By default, the power is not limited (BT ports can deliver up to class 6 and non-BT ports can deliver up to class 4) • The class limit of a BT port can be set to class 3, 4, or unlimited. • The class limit of a non-BT port can be set to class 3 or unlimited.
Pre-Standard Detection	Indicates whether Pre-Standard Detection is allowed. The 4-point detection scheme defined in IEEE 802.3 is used by default. If this mechanism fails to detect a connected PD, and pre-standard detection is allowed, then pre-standard detection is used.
Power Management Mode	Select the method by which the PoE controller determines supplied power. Possible values are: • 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. This is the default selection.
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 operational status of the PSE is disabled. • Delivering Power—The PSE is delivering power. • Fault—The PSE has experienced a fault condition. • Searching—The PSE is transitioning between states. • Recovering—the port is recovering from a previous condition of internal hardware fault.
Output Power	Power consumed on port, in watts.
Fault Status	Indicates the type of fault condition that exists on the port . Possible values are: • None - the port is not in fault condition. • Short - a Short fault condition exists on the port. • Overload - a PoE Overload fault condition exists on the port. • Power Denied - Power on port is denied due to power over-subscription condition on the switch. • Hardware Fault - a general Hardware fault occurred on the switch which prevents power on port • Internal HW Fault - a hardware fault occurred on the interface. • Other - a fault of a type not specified above occurred on the port. NOTE: This field is relevant only if the status of the port is Fault.

Edit Port PoE Configuration

To change PoE settings for a port, select the checkbox associated with it and click **Edit** . Or, click **Edit All**  to configure all PoE enabled ports at the same time.

Figure 140. Edit Port PoE Configuration Page



Interface
1

Admin Mode
☒

Schedule
None

Priority
☐ Critical ☐ High ☒ Low

Class Limit
Unlimited

Allow Pre-Standard Detection
☐

Power Management Mode
☒ Usage ☐ Class

CANCEL APPLY

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**.

PoE Port Details

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

Figure 141. PoE Port Details Page

 PoE Port Details

Interface

1/1

Class Limit

Unlimited

Assigned Class

-

Measured Class

-

Output Voltage

0 Volts

Output Current

0 mAmps

Negotiated Power

0 Watts

Output Power

0 Watts

Event Counters

Overloads

0

Denials

0

Absences

0

Invalid Signatures

0

CLEAR COUNTERS

CLOSE

Table 120. PoE Port Details Fields

Field	Description
Class Limit	Shows the class limit: • Unlimited • Class 3 • Class 4
Measured Class	The class of power requested by the powered device. Possible values are Unknown and Class 0 through Class 6. A higher class value indicates that the switch provides higher power. BT ports may provide power in dual signature mode. In this case, each channel has its own class, that appears in format of Alt-A class/Alt-B class.
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.
Negotiated Power	Power in watts negotiated between the port and connected switch.
Output Power	Power in watts being drawn by the 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 that 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.



The **Re-activate**  button appears when there is a disabled port due to a hardware failure. Ports that are in hardware fault state may recover automatically from this state, however, in some cases you may need to manually re-activate this port.

To manually re-activate the port, select the row with the hardware failure and click the **Re-activate**  button.

Routing provides a means of transmitting IPv4 packets between subnets on the network. Routing is disabled by default. Static routing means that routes need to be added by the system administrator and are not learned through a routing protocol.

The device supports:

- Up to 32 IPv4 interfaces:
 - o An IPv4 address can be configured on VLAN, LAG or Physical interface
 - o Single IPv4 address per interface
- IPv4 static routes:
 - o Access SKUs and aggregate SKUs in hybrid mode - up to 32 static routes
 - o Aggregate SKUs in aggregate mode - up to 512 static routes
 - o Hybrid Stack - up to 32 static routes
- Up to 32 IPv6 addresses - which can be configured on ports or VLAN interfaces
- IPv6 routes:
 - o Access SKUs and aggregate SKUs in hybrid mode- 32 static routes
 - o Aggregate SKUs in native mode: 256 routes

Routing configuration is necessary only if the switch is used as a Layer 3 switch that routes packets between subnets. If the switch is used as a Layer 2 switch that handles switching only, it typically connects to an external Layer 3 switch that handles the routing functions; therefore, routing configuration is not required on the Layer 2 switch.

You can use the Routing pages to configure Layer 3 features and capabilities.

Routing Configuration

Use the Routing Configuration page to configure Global 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** > **Routing Configuration** 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. Global Configuration Page

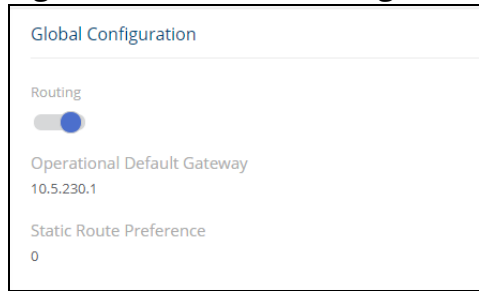


Table 121. Routing Configuration Fields

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 when using the CLI to configure a static route and no preference is specified. This field is not configurable and has a value of 1.

Port IP and VLAN IP Tile

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 following figure shows the Port IP tab. The Port IP and the VLAN IP tabs show the same fields.

These pages show summary information about the routing configuration for all interfaces.

Figure 143. Port IP Tile

Port IP		VLAN IP							Display: 10	
Interface ▲	Status	IP Address	Subnet Mask	Admin Mode	State	MAC Address	Proxy ARP			
☒ 1	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:00:44:44:55:89	Disabled			
☐ 2	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:00:44:44:55:8A	Disabled			
☐ 3	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:00:44:44:55:8B	Disabled			
☐ 4	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:00:44:44:55:8C	Disabled			
☐ 5	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	00:00:44:44:55:8D	Disabled			

Table 122. Port/VLAN IP Fields

Field	Description
Interface/VLAN ID	The interface 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 being viewed.
Status	It indicates whether the interface 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). NOTE: This field is only relevant to Port IP interfaces.
IP Address	The IP address of the interface.
Subnet Mask	The IP subnet mask for the interface (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, which is either Enabled or Disabled.
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

Edit Routing Interface Configuration

Interface
1/1

Status
Down

Routing Mode
☐

Admin Mode
☒

State
Inactive

Link Speed Data Rate
1000

IP Address Configuration Method
☒ None ☐ Manual ☐ DHCP

IP Address
0.0.0.0
(xxxx)

Subnet Mask
0.0.0.0
(xxxx)

Forward Net Directed Broadcasts
☐

Proxy ARP
☐

ICMP Redirects
☐

CANCEL APPLY

Table 123. Edit Routing Interface Configuration Fields

Field	Description
Interface/VLAN ID	The selected interface, or VLAN ID, that is being edited.

Field	Description
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). NOTE: For VLAN interfaces, routing mode is always enabled.
Routing Mode	The administrative mode of IP routing on the interface. NOTE: This setting is available only for IP port. for VLAN interfaces this setting is always enabled.
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. NOTE: 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.
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.

To view additional routing configuration information for an interface, select the radio button to the left of the interface and click **Details**  .

Figure 145. Routing Interface Settings Details

Routing Interface Settings Details

Interface
1

Status
Down

Routing Mode
Disabled

Admin Mode
Enabled

State
Inactive

MAC Address
00:00:44:44:55:89

Link Speed Data Rate
1000

IP Address Configuration Method
None

DHCP Client Identifier
N/A

[CLOSE](#)

The following information describes the fields in the **Details** window that are not displayed on the summary page.

Table 124. 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.

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**.

Static Routing/Route Table Tile

To display the Static Routing/Route Table tile, click **Routing > Routing Configuration** 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 **Routing Table** tab.

Static Routing

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

Figure 146. Static Routing Tab

Static Routing	Route Table				Display: 10	
☐	Network Address	▲ Subnet Mask	Next Hop IP Address	Next Hop Interface	Preference	
Table Is Empty						

Table 125. Static Routing Fields

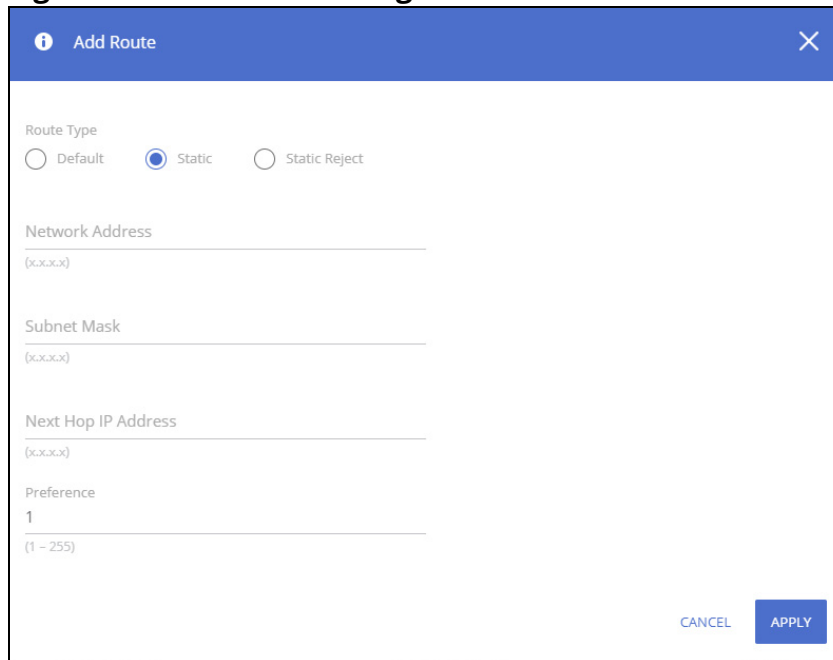
Field	Description
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Next Hop IP Address	The next hop router address to use when forwarding traffic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

Figure 147. Add Route Page



2. Enter the Route information:

Next to **Route Type**, select **Default** route, **Static** or **Static Reject** from the menu.

- o **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.
- o **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**.
- o **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

The route table manager collects routes from multiple sources: static routes and local routes. The route table manager may 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

Static Routing

Route Table

Display: 10

Network Address	Subnet Mask	Protocol	Next Hop IP Address	Next Hop Interface
0.0.0.0	0.0.0.0	Default	10.5.230.1	VLAN 1
10.5.230.0	255.255.255.128	Local	10.5.230.77	VLAN 1

«

<

1

>

»

Table 126. 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.

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

IP Routing Statistics/ICMP Statistics

To display the IP Routing/ICMP Statistics tile, click **Routing > Routing Configuration** 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.

IP Routing Statistics

Figure 149. IP Routing Statistics Tab

IP Routing Statistics		ICMP Statistics	
IpInReceives	74682	IpInDelivers	63968
IpInHdrErrors	9028	IpOutRequests	24913
IpInAddrErrors	10	IpOutDiscards	0
IpFowdDatagrams	0	IpOutNoRoutes	4
IpInUnknownProtos	0	IpReasmTimeout	10
IpInDiscards	0	IpReasmReqds	0
		IpReasmOKs	0
		IpReasmFails	0
		IpFragOKs	0
		IpFragFails	0
		IpFragCreates	0

Table 127. Routing IP 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.

ICMP Statistics

Table 128. 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.

Field	Description
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.
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.

IPv6 Routing

The device supports Internet Protocol version 6 (IPv6) routing. IPv6 is a protocol that provides identification for network-based devices. IPv6 is also used to route traffic across networks. In IPv6 the address size is 128-bit. This provides a great range and flexibility of address assignment.

IPv6 interface addresses can be configured manually, or automatically by a DHCPv6 server.

Global Configuration

Use the IPv6 Routing Global Configuration page to enable the IPv6 routing feature on the switch. To display the IPv6 Routing Global Configuration page, click **Routing** > **IPv6 Routing** in the navigation pane.

Figure 150. IPv6 Routing Global Configuration Page

Global Configuration

IPv6 Routing

ICMPv6 Rate Limit Interval

100

(0 - 2147483647) ms

ICMPv6 Bucket Size

10

(1 - 200)

IPv6 Hop Limit

64

(1 - 255)

DHCPv6 Client DUID

000300018c85c13c1000

Link Local Default Zone

None

Table 129. IPv6 Routing Global Configuration Fields

Field	Description
IPv6 Routing	Activate to enable IPv6 routing on the device.
ICMPv6 Rate Limit Interval	Set the interval for IPv6 ICMP error messages. Set 0 to disable ICMP rate limiting. The valid range is: 0 to 2147483647 ms. The default = 100ms.
ICMPv6 Bucket Size	Set the bucket size (that is, the maximum number of tokens stored in the bucket) for IPv6 ICMP error messages. The valid range is: 1-200. The default = 100.
IPv6 Hop Limit	Set the maximum number of hops used in all IPv6 packets that are originated by the router. This setting can be overridden by interface level setting. The valid range is:1-255. The default = 64
DHCPv6 Client DUID	Displays the device DHCP unique identifier (DUID) based on the Link-layer Address.

Field	Description
Link Local Default Zone	Click the dropdown to select an IPv6 interface to egress a link local packet that does not have a specified interface. The default is None.

IPv6 Interfaces/IPv6 Addresses

To view the IPv6 interface information, click the **IPv6 Interfaces** tab.

To view the IPv6 address information, click the **IPv6 Addresses** tab.

IPv6 Interfaces Tab

Figure 151. IPv6 Interfaces Tab

IPv6 Interfaces

IPv6 Addresses

Display: 10

☐ Interface ▲	Autoconfiguration	DAD Attempts	ICMPv6	IPv6 Redirects	MLD Version	DHCPv6
☐ VLAN1	Enabled	1	Enabled	Enabled	v2	Enabled
☐ VLAN3	Enabled	1	Disabled	Enabled	v2	Disabled

«

<

1

>

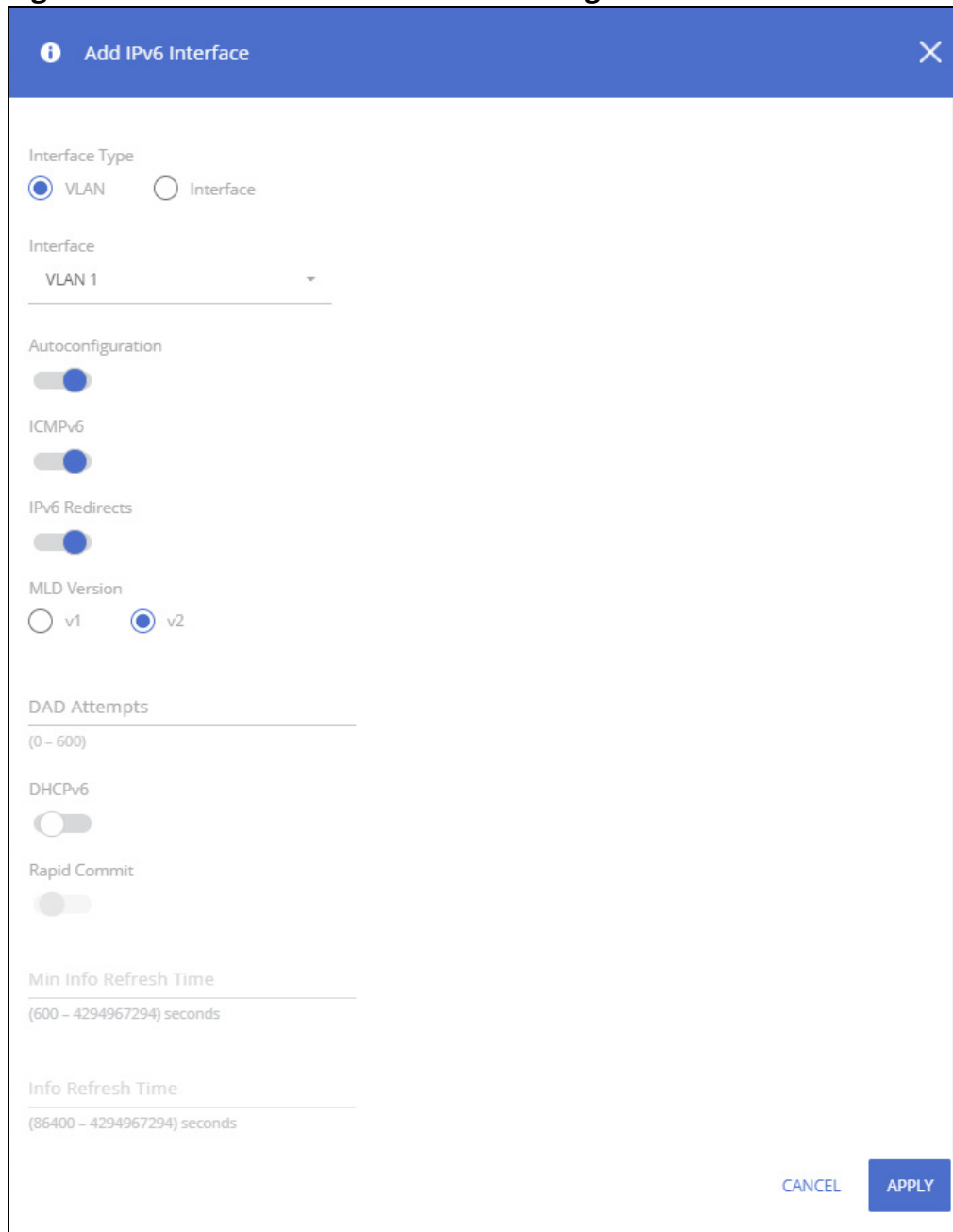
»

Table 130. IPv6 Interfaces Fields

Field	Description
Interface	The interface associated with the rest of the data in the row.
Autoconfiguration	When activated, the interface supports automatic configuration of IPv6 addresses, using stateless auto configuration on an interface. Addresses are configured depending on the prefixes received in Router Advertisement messages.
DAD Attempts	The number of consecutive neighbor solicitation messages that can be sent on an interface, while Duplicate Address Detection (DAD) is performed on the Unicast IPv6 addresses of the interface.
ICMPv6	Specifies if ICMPv6 is enabled or disabled on this interface.
IPv6 Redirects	When enabled, ICMP IPv6 redirect messages can re-send a packet through the same interface on which the packet was received.
MLD Version	The Multicast Listener Discovery Protocol (MLD) version that the interface uses.
DHCPv6	When enabled, the interface supports DHCP for an IPv6 client process and acquires an IPv6 address.

To configure a new IPv6 interface, click **Add** . To edit an interface, select the interface in the tile and then click **Edit** .

Figure 152. Add/Edit IPv6 Interface Dialog Box



The dialog box is titled "Add IPv6 Interface" with a close button (X) in the top right corner. It contains several configuration sections:

- Interface Type:** Two radio buttons, "VLAN" (selected) and "Interface".
- Interface:** A dropdown menu showing "VLAN 1".
- Autoconfiguration:** A toggle switch that is turned on.
- ICMPv6:** A toggle switch that is turned on.
- IPv6 Redirects:** A toggle switch that is turned on.
- MLD Version:** Two radio buttons, "v1" and "v2" (selected).
- DAD Attempts:** A text input field with the value "0" and a range "(0 - 600)".
- DHCPv6:** A toggle switch that is turned off.
- Rapid Commit:** A toggle switch that is turned off.
- Min Info Refresh Time:** A text input field with the value "600" and a range "(600 - 4294967294) seconds".
- Info Refresh Time:** A text input field with the value "86400" and a range "(86400 - 4294967294) seconds".

At the bottom right, there are two buttons: "CANCEL" and "APPLY".

Table 131. Edit IPv6 Interface Fields

Field	Description
Interface	The interface associated with the rest of the data in the row.

Field	Description
Autoconfiguration	Activate to enable the interface to automatically configure IPv6 addresses, using stateless auto configuration on an interface. Addresses are configured depending on the prefixes received in Router Advertisement messages. By default, this feature is enabled.
ICMPv6	Activate to enable ICMPv6 on this interface. By default, this feature is enabled.
IPv6 Redirects	Activate to enable ICMP IPv6 redirect messages to re-send a packet through the same interface on which the packet was received. By default, this option is enabled.
MLD Version	Define the Multicast Listener Discovery Protocol (MLD) version that the interface uses. Valid values: v1 or v2. The default is v2.
DAD Attempts	Set the number of consecutive neighbor solicitation messages that can be sent on an interface, while Duplicate Address Detection (DAD) is performed on the Unicast IPv6 addresses of the interface. The valid range is: 0-600. The default = 1.
DHCPv6	When enabled, the interface supports DHCP for an IPv6 client process and acquires an IPv6 address.
Rapid Commit	This feature is related to DHCP client. When enabled, it allows the two-message exchange method for address assignment and other configuration. The client includes the rapid-commit option in a solicit message. By default, this feature is disabled.
Min Info Refresh Time	Set the minimum acceptable refresh time on the specified interface, in seconds. The valid range is: 600-4294967294 seconds. The default is 86,400 seconds (24 hours).
Info Refresh Time	Set the refresh time for DHCPv6 client information on the interface, if the DHCPv6 server reply does not include the Information Refresh Time. The valid range is: 600-4294967294 seconds. The default is 86,400 seconds (24 hours).

To view additional information on an IPv6 interface, select the interface and click **Details**  .



IPv6 is active on a physical interface only if routing is enabled for that interface. To enable routing on an interface, go to **Routing Configuration** and enable the **Routing Mode** setting.

Figure 153. IPv6 Interface Settings Details

Interface
VLAN1

DHCP Operational Mode
Enabled

Stateful Service State
Available

Stateless Service State
Available

IPv6 Address IA NA

DHCP Server Address

DHCP Server DUID

DHCP Server Preference
0

Received Information Refresh Time
0 seconds

Remaining Information Refresh Time
0 seconds

Configuration Error

CLOSE

The following table lists the details that are not described in the **Edit** dialog:

Table 132. IPv6 Interface Details Fields

Field	Description
Interface	The IPv6 interface
DHCP operational mode	Indicates if DHCPv6 is operational on the interface
Stateful service state	In stateful mode the host gains the /64 prefix either from a DHCPv6 server, or from a user configuration.
Stateless service state	In stateless mode the router advertises the /64 prefix according to configured data.
IPv6 Address IANA	The vendor's registered Private Enterprise number as maintained by IANA.
DHCP Server Address	The DHCPv6 server from which the address was acquired.
DHCP Server DUID	Displays the device DHCP unique identifier (DUID) based on the Link-layer Address.
DHCP Server Preference	The preference of the DHCPv6 server that assigned an address to this interface.

Field	Description
Received Information Refresh Time	The refresh interval, in seconds, for the information received from the router.
Remaining Information Refresh Time	Time remaining until information refresh occurs.
Configuration Server	The address of the server used to download the configuration file.
Configuration Path	The path to the configuration file on the server.

IPv6 Addresses Tab

Figure 154. IPv6 Addresses Tab

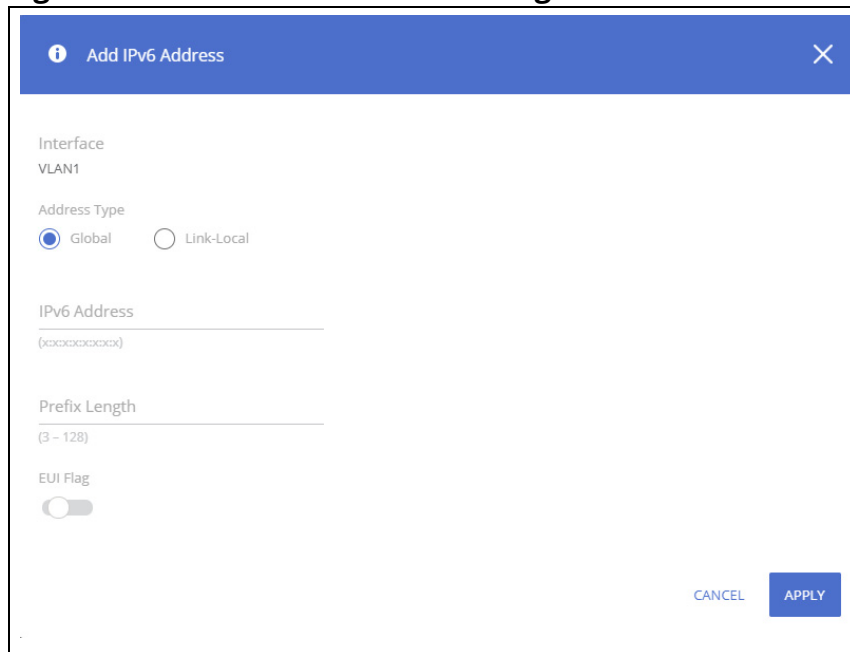
Address	Source	DAD Status	Preferred Lifetime (Sec)	Valid Lifetime (Sec)	Expiry Time (Sec)
25::8e85:c1ff:fe3c:1000	System	Preferred	2	1	
fe80::8e85:c1ff:fe3c:1000	System	Preferred	2	1	
ff02::1	System	Preferred	2	1	
ff02::1:ff3c:1000	System	Preferred	2	1	

Table 133. IPv6 Addresses Fields

Field	Description
IPv6 Interface	Select an interface from the drop-down menu, to show its related addresses in the tab.
Address	The address specified in hexadecimal using 16-bit values between double-colons.
Source	The source of the IPv6 address.
DAD Status	The status of the DAD.
Preferred Lifetime (sec)	The number of seconds that the that this prefix is preferred. That is, the time until deprecation.
Valid Lifetime (sec)	The number of seconds that the that this prefix is valid. That is, time until invalidation.
Expiry time (sec)	The number of seconds until this prefix expires.

To configure a new IPv6 address, click **Add**  .

Figure 155. Add IPv6 Address Dialog Box



The dialog box is titled "Add IPv6 Address" with a close button (X) in the top right corner. It contains the following fields and controls:

- Interface:** A text field with the value "VLAN1".
- Address Type:** Two radio buttons: "Global" (selected) and "Link-Local".
- IPv6 Address:** A text field with a placeholder "(XXXXXXXXXX)".
- Prefix Length:** A text field with a placeholder "(3 - 128)".
- EUI Flag:** A toggle switch currently turned off.
- Buttons:** "CANCEL" and "APPLY" buttons at the bottom right.

Table 134. Add IPv6 Address Fields

Field	Description
Interface	The interface that the address is added to.
Address Type	Select Global or Link-Local.
IPv6 Address	Enter the IPv6 address for the interface
Prefix length	This option is available for Global addresses, when the EUI flag is off. Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address) The valid range is: 3-128.
EUI Flag	Activate to enable the Extended Universal Identifier (EUI) for IPv6 addresses.

IPv6 Routes

Use this tile to display and configure entries in the IPv6 routes table.

Figure 156. IPv6 Routes Tile

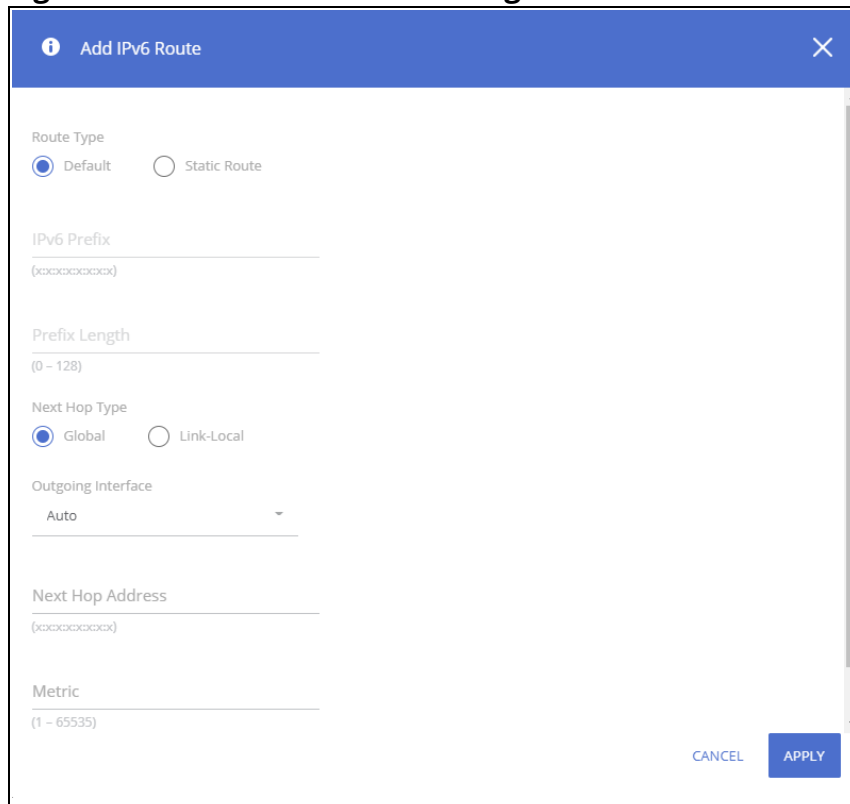
IPv6 Routes										Display: 10	
☐	IPv6 Prefix		Next Hop Address	Interface	Metric	Type	Lifetime (Sec)				
☐	25::		64	VLAN1	0	ND					
☐	Default Router		0	VLAN1	0						
☐	Default Router		0	VLAN1	0						

Table 135. IPv6 Routes Fields

Field	Description
IPv6 Prefix	The IPv6 network that is the destination of the static route. This field can also provide the host name when using static host routes.
Next Hop Address	The IPv6 address of the next hop that can be used to reach the specified network.
Interface	The outgoing IPv6 interface.
Metric	Static route metric.
Type	The route entry type. The possible values are: Static, ICMP, ND and Connected.
Lifetime (Sec)	Time, in seconds until the entry expires.

To configure a new IPv6 Route, click **Add**  .

Figure 157. Add IPv6 Route Dialog Box



The dialog box is titled "Add IPv6 Route" with a close button (X) in the top right corner. It contains the following fields and options:

- Route Type:** Two radio buttons, "Default" (selected) and "Static Route".
- IPv6 Prefix:** A text input field with a placeholder "(xxxxxxxx)".
- Prefix Length:** A text input field with a placeholder "(0 - 128)".
- Next Hop Type:** Two radio buttons, "Global" (selected) and "Link-Local".
- Outgoing Interface:** A dropdown menu with "Auto" selected.
- Next Hop Address:** A text input field with a placeholder "(xxxxxxxx)".
- Metric:** A text input field with a placeholder "(1 - 65535)".

At the bottom right, there are two buttons: "CANCEL" and "APPLY".

Table 136. Add IPv6 Route Fields

Field	Description
Route Type	Select Default, or Static Route.
IPv6 Prefix	Enter the IPv6 network that is the destination of the static route. Can also be a host name when static host routes are configured.
Prefix Length	Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address) The valid range is: 3-128.
Next Hop Type	Select Global or Link-Local.
Outgoing Interface	Select an interface from the drop-down.
Next Hop Address	Enter the address of the next hop. The valid options may require configuring an outgoing interface that is not Auto .
Metric	The static route metric. The valid range is: 1 to 65535. The default value is: 1.

Neighbor Discovery

Use this tile to display and configure neighbor discovery configuration.

Figure 158. Neighbor Discovery Tile

Neighbor Discovery

Display: 10

☐	IPv6 Address	MAC Address	Interface	Type	State	Aging (sec)
☐	fe80::244:44ff:fe44:4444	00:44:44:44:44:44	VLAN1	Dynamic	Stale	116777
☐	fe80::2ac7:ceff:fe7d:fb0	28:c7:ce:7d:fb:c0	VLAN1	Dynamic	Stale	187

<<

<

1

>

>>

Table 137. Neighbor Discovery Fields

Field	Description
IPv6 Address	The IPv6 address of the IPv6 neighbor.
MAC Address	The MAC address of the IPv6 neighbor.
Interface	Interface on which address was learned.
Type	Static (that is, added by the user) or Dynamic.
State	The state of the neighbor. Supported values are Reachable, Incomplete, Stale, Delay, Probe.
Aging (sec)	Time, in seconds until the entry expires.

To configure a new IPv6 Neighbor, click **Add** .

Figure 159. Add IPv6 Neighbor Dialog Box

 Add IPv6 Neighbor 

Interface

VLAN1

IPv6 Address

(xxxxxxxxxxxx)

MAC Address

(xxxxxxxxxxxxxx)

CANCEL

APPLY

Table 138. Add IPv6 Neighbor Fields

Field	Description
Interface	Select the interface to configure.

Field	Description
IPv6 Address	The IPv6 address of the IPv6 neighbor.
MAC Address	The MAC address of the IPv6 neighbor.

RA Prefixes/RA Settings

Use this tile to view or configure the Router Advertisement (RA) settings for an IPv6 enabled device.

To view the RA Prefixes information, click the **RA Prefixes** tab.

To view the RA Settings information, click the **RA Settings** tab.

RA Prefixes Tab

Figure 160. RA Prefixes Tab

RA Prefixes

RA Settings

+

✎

🗑

↺

Display: 10

⌵

⌵

☐	Interface	Prefix	Advertisement	Valid Lifetime (Sec)	Preferred Lifetime	Autoconfig	Type
☐	VLAN1	Default	Enabled	2592000	604800	Enabled	Onlink

«

<

1

>

»

Table 139. RA Prefixes Fields

Field	Description
Interface	The interface associated with the rest of the data in the row.
Prefix	The IPv6 network number to include in router advertisements.
Advertisement	Enable or disable advertising the prefix. The default is to advertise the prefix.
Valid Lifetime	Length of time, in seconds, that this prefix is valid. That is, time until invalidation.
Preferred Lifetime	Length of time, in seconds, that this prefix is preferred. That is, time until deprecation.
Autoconfig	If enabled, hosts on the local link are indicated that the specified prefix can be used for IPv6 autoconfiguration. The prefix is advertised with the A-bit set. The default is enabled.
Type	The RA prefix type: Onlink - This is the default, Offlink, or No Onlink.

To configure a new RA Prefix, click **Add** . To edit an interface, select the interface in the tile and then click **Edit** . The **Edit** dialog is identical to the **Add** dialog, except for the **Prefix Length** option that is not available in the **Edit** dialog box.

Figure 161. Add RA Prefix Dialog Box

Table 140. Add RA Prefix Fields

Field	Description
Interface	The interface associated with the rest of the data in the row.
IPv6 Prefix	The IPv6 network number to include in router advertisements.
Prefix Length	Length of the IPv6 prefix. Indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). The valid range is: 0-128.
Advertisement	Enable or disable advertising the prefix. The default is to advertise the prefix.
Valid Lifetime	Length of time, in seconds, that this prefix is valid. That is, time until invalidation. The address generated from an invalidated prefix should not appear as the destination or source address of a packet. The valid range is: 1- 4,294,967,295.
Preferred Lifetime	Length of time, in seconds, that this prefix is preferred. That is, time until deprecation. The Preferred Lifetime must not be larger than the Valid Lifetime. The address generated from a deprecated prefix should no longer be used as a source address in new communications, but packets received on such an interface are processed as expected. The valid range is: 1- 4,294,967,295

Field	Description
Autoconfig	If enabled, hosts on the local link will not use the specified prefix for IPv6 autoconfiguration. The prefix will be advertised with the A-bit clear. By default this is enabled.
Type	These are the available types: - Onlink - This is the default. - Offlink - The prefix is advertised with the L-bit clear. The prefix is not inserted into the routing table as a connected prefix. If the prefix is already present in the routing table as a connected prefix (for example, because the prefix was also configured as an ipv6 address on the interface), then it is removed. - No Onlink - The prefix is configured as not on-link. The prefix is advertised with the L-bit clear.

RA Settings Tab

Figure 162. RA Settings Tab

RA Prefixes

RA Settings

Display: 10

☐ Interface ▲	RA Halt	Max Sending Interval (sec)	Min Sending Interval (sec)	Advertisement Interval Option	Hop Limit	managed-address-flag	other-flag	Lifetime (Sec)	NS Retrans Interval (mS)	Nud Reachable Time (mS)	Preference
☐ VLAN1	False	600	198	Disabled	64	False	False	1800	1000	0	Medium

«

<

1

>

»

Table 141. RA Settings Fields

Field	Description
Interface	The interface associated with the rest of the data in the row.
RA Halt	When True , IPv6 router advertisement transmissions are suppressed on the interface.
Max Sending Interval (Sec)	The maximum interval between IPv6 RA transmissions, in seconds.
Min Sending Interval (Sec)	The minimum interval between IPv6 RA transmissions, in seconds.
Advertisement Interval Option	If enabled, the advertisement interval option is set in router advertisements (RAs)
Hop Limit	The maximum number of hops used in router advertisements on the interfaces.
managed-address-flag	If True, the managed address configuration flag in IPv6 router advertisements is sent on the interface.
other-flag	If True, the Other Stateful configuration flag in IPv6 router advertisements is sent on the interface.
Router Lifetime	The Router Lifetime value in IPv6 router advertisements on an interface.
NS Retransmit Interval	The interval between IPv6 neighbor solicitation retransmissions on an interface, in Milli seconds.
NUD Reachable Time	The amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred.

Field	Description
Preference	The default router preference (DRP) for the router on the interface.

To edit an RA Setting, select it and click **Edit** .

Figure 163. Edit RA Setting Dialog Box

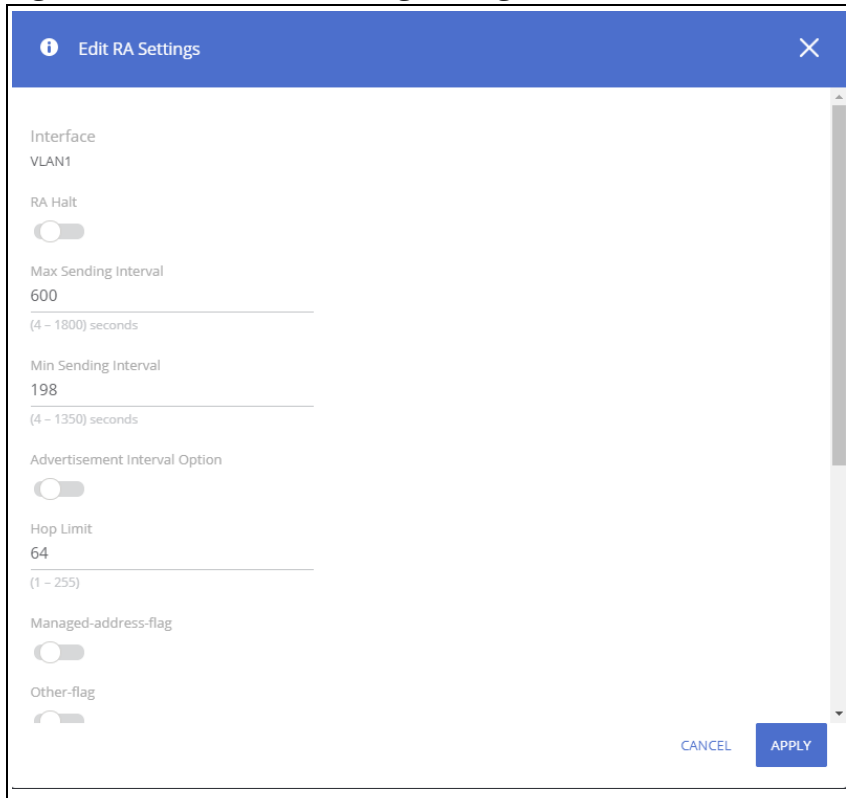


Table 142. Edit RA Settings Fields

Field	Description
Interface	The interface that the RA Settings are configured for.
RA Halt	Enable to suppress IPv6 router advertisement transmissions on the interface. By default, this is enabled.
Max Sending Interval (Sec)	Configure the maximum interval between IPv6 RA transmissions, in seconds. The valid range is: 4 -1800. The default is: 600
Min Sending Interval (Sec)	Configure the minimum interval between IPv6 RA transmissions, in seconds. The valid range is: 3 - 1350. The default is 0.33*maximum-secs
Advertisement Interval Option	Enable to set the advertisement interval option in router advertisements (RAs)

Field	Description
Hop Limit	Configure the maximum number of hops used in router advertisements on the interfaces. The valid range is: 1 - 255. The default value is either 64, or the global setting.
managed-address-flag	Enable to set the managed address configuration flag in IPv6 router advertisements sent on the interface.
other-flag	Enable to set the Other Stateful configuration flag in IPv6 router advertisements sent on the interface.
Router Lifetime	The Router Lifetime value in IPv6 router advertisements on an interface. The value needs to be equal or higher than the router advertisement interval. The valid values are 0, or from <Maximum RA Interval> to 9000 seconds. The default is 3*<Maximum RA Interval> seconds. When set to 0, the router is not considered a default router on this interface.
NS Retransmit Interval	The interval between IPv6 neighbor solicitation retransmissions on an interface, in Milli seconds. The valid range is: 1000 - 3600000 milliseconds. By default, 0 seconds (unspecified) is advertised in router advertisements, and the value 1000 milliseconds is used for neighbor discovery activity of the router itself.
NUD Reachable Time	The amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred. The valid range is: 0 - 3600000 milliseconds. By defaults, 0 milliseconds (unspecified) is advertised in router advertisements, and the value 30000 (30 seconds) is used for the neighbor discovery activity of the router itself.
Preference	The default router preference (DRP) for the router on the interface. Valid values are high, medium and low. The default setting is medium

DHCP Relay

Aruba Instant On 1960 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. 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.

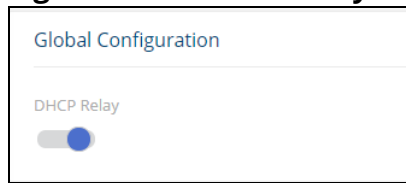
Global Configuration

Use the DHCP Relay Global Configuration page to enable the DHCP relay feature on the switch.

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

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**.

Figure 164. DHCP Relay Global Configuration Page



Server Configuration

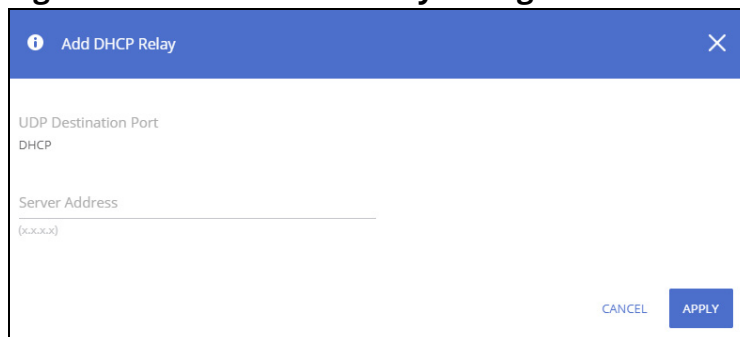
Use the Server Configuration tile view and configure information about DHCP servers where packets should be relayed.

Table 143. 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 165. Add DHCP Relay Dialog Box



To remove one or more configured DHCP servers, select each server to delete and click **Remove**  .

DHCP Relay Interfaces

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

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



DHCP relay is operational on a VLAN or interface, only if it is enabled for routing. To enable routing on an interface or VLAN, use the Port IP and VLAN tile.

Figure 166. DHCP Relay Interfaces Page

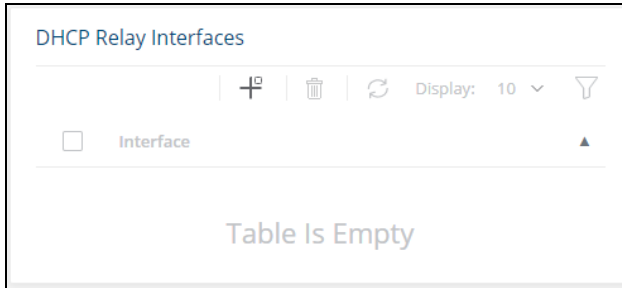


Table 144. DHCP Relay Interface Fields

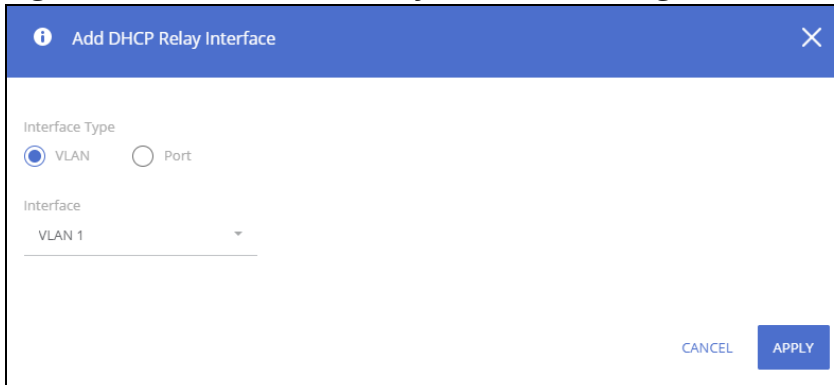
Field	Description
Interface	The routing interface that has the DHCP relay feature configured.

Adding a DHCP Server

To configure an interface or VLAN that can relay DHCP packets to a DHCP server:

1. Click **Add**  to open **Add DHCP Relay Interface** dialog box.

Figure 167. Add DHCP Relay Interface Dialog Box



2. Select the Interface type: VLAN or Port
3. Select the interface from the drop-down menu.
4. Click **APPLY**.

Removing a Relay Interface

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

DHCPv6 Relay

The device supports DHCPv6 Relay, as defined in RFC 3315, for relaying DHCPv6 messages to the DHCPv6 servers.

When a DHCPv6 client is not connected in the same subnet as the DHCPv6 Server, a DHCPv6 Relay agent to which this DHCPv6 client is directly connected is required. The DHCPv6 relay agent encapsulates the messages received from the directly connected DHCPv6 client, and forwards these encapsulated to the DHCPv6 server. In the opposite direction, the Relay Agent decapsulates the packets received from the central DHCPv6 Server and forwards them to the DHCPv6 client.

DHCPv6 relay requires IPv6 to be enabled on the interface.

You can create a global list of DHCPv6 servers and per-source-interface (interfaces connected to the DHCPv6 client) list of DHCPv6 servers.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays messages to a Multicast address, it sets the hop limit field in the IPv6 packet header to 32.

When a DHCPv6 packet is received on an interface, the DHCPv6 server list (if configured) for this interface DHCPv6 server's list is used first, and then the global list is used. Up to 10 addresses can be defined per one interface and up to 100 addresses can be defined per switch.

Global Destinations

Use the Global Destinations page to configure global relay destinations for the switch.

Figure 168. Global Destinations Tile

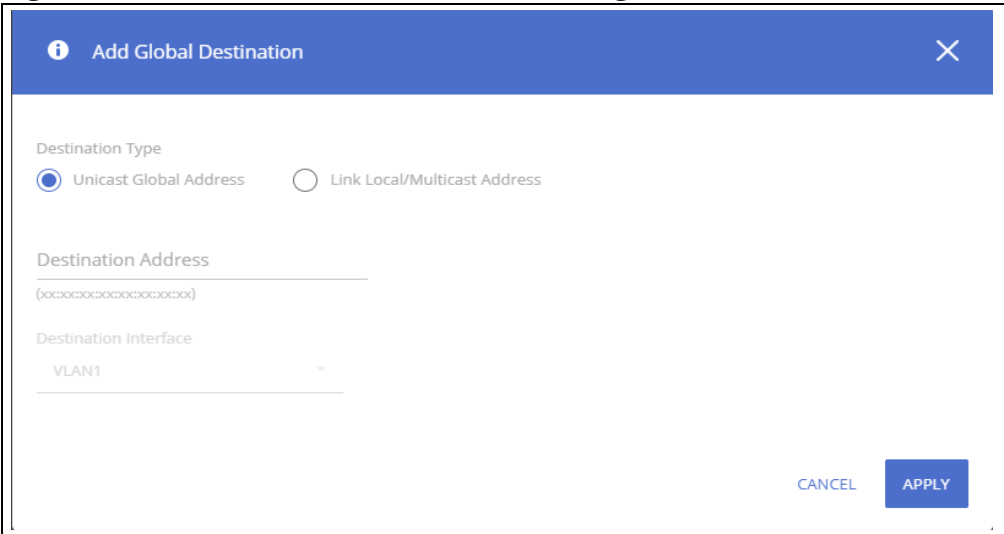


Table 145. Global Destinations Fields

Field	Description
Relay Destinations	The IPv6 address and interface for the relay destination.

To add a global destination click Add .

Figure 169. Add Global Destination Dialog Box



The dialog box is titled "Add Global Destination" with a close button (X) in the top right corner. It contains three main sections: "Destination Type" with two radio buttons, "Unicast Global Address" (selected) and "Link Local/Multicast Address"; "Destination Address" with a text input field containing a placeholder "(xxxxxxxxxxxxxxxxxx)"; and "Destination Interface" with a dropdown menu showing "VLAN1". At the bottom right are "CANCEL" and "APPLY" buttons.

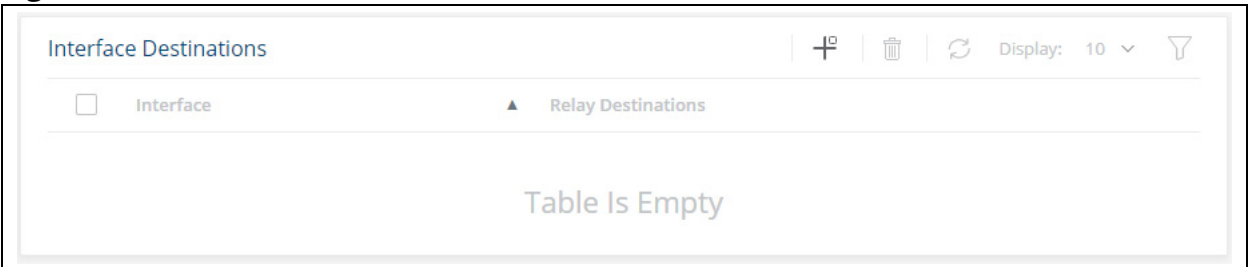
Table 146. Add Global Destination Fields

Field	Description
Destination Type	Select Unicast Global Address, or Link Local/Multicast Address.
Destination Address	Enter the IPv6 address for the destination.
Destination Interface	Select the interface to configure, from the drop-down list.

Interface Destinations

Use the Interface Destinations page to configure relay destinations for the interface.

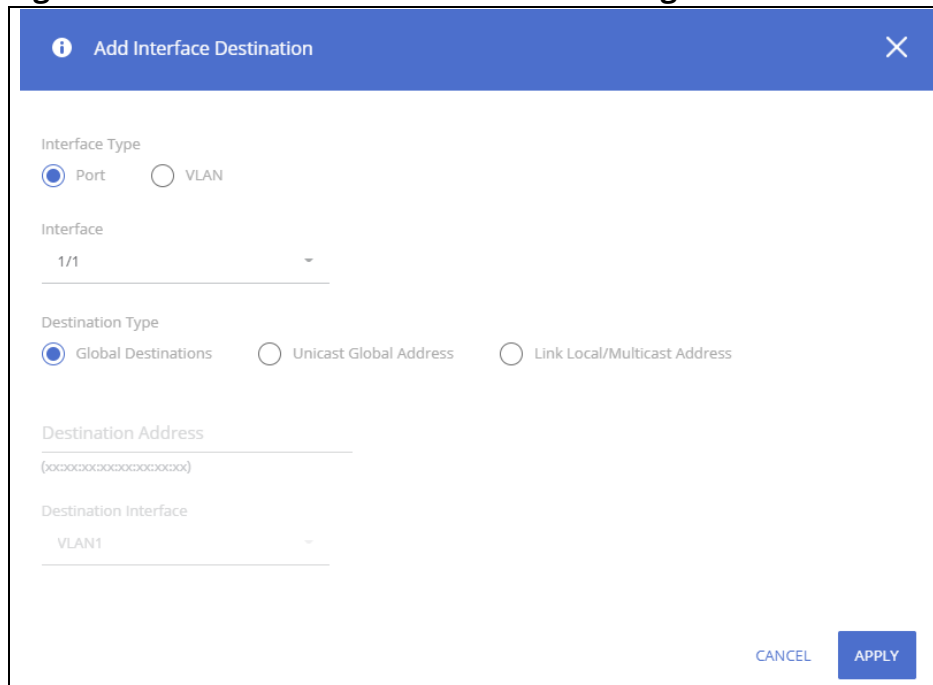
Figure 170. Interface Destinations Tile



The tile is titled "Interface Destinations" and includes action icons (Add, Delete, Refresh) and a "Display: 10" dropdown. Below the title is a toggle switch for "Interface" (unchecked) and "Relay Destinations" (checked). The main area contains the text "Table Is Empty".

To add an interface destination click **Add** .

Figure 171. Add Interface Destination Dialog Box



The dialog box is titled "Add Interface Destination" with an information icon and a close button. It contains the following fields:

- Interface Type:** Radio buttons for "Port" (selected) and "VLAN".
- Interface:** A dropdown menu showing "1/1".
- Destination Type:** Radio buttons for "Global Destinations" (selected), "Unicast Global Address", and "Link Local/Multicast Address".
- Destination Address:** A text field with a placeholder "(xxxxxxxxxxxxxxxx)".
- Destination Interface:** A dropdown menu showing "VLAN1".

At the bottom right are "CANCEL" and "APPLY" buttons.

Table 147. Add Interface Destination Fields

Field	Description
Interface Type	Select Port or VLAN as the interface type.
Interface	Select the interface to configure, from the drop-down list.
Destination Type	Select Unicast Global Address, or Link Local/Multicast Address, as the destination type.
Destination Address	Enter the IPv6 address for the destination.
Destination Interface	Select the destination interface to configure, from the drop-down list. NOTE: This option is required only if address type is multicast/link local. For a global address it is grayed out.

ARP Table

The Address Resolution Protocol (ARP) protocol associates a layer 2 MAC address with a layer 3 IPv4 address. Aruba Instant On 1960 Switch Series 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.

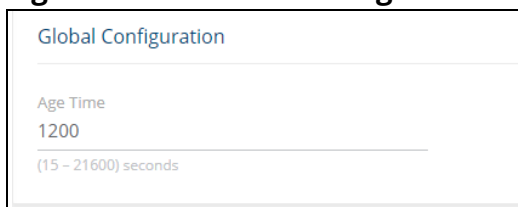
- If an entry related to a host station times out, it is removed from the table.
- If an entry related to a router or gateway ages out, the switch sends an ARP request for an entry IP address and only if there is no response, the entry is removed from the ARP table.

Global Configuration

Use this page to change the configuration parameters for the ARP Table.

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

Figure 172. Global Configuration



The screenshot shows the 'Global Configuration' page. It has a title bar 'Global Configuration'. Below it, there is a label 'Age Time' followed by a text input field containing '1200'. Below the input field, it says '(15 - 21600) seconds'.

Table 148. 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. Valid range is 15-21600. Default is 1200.

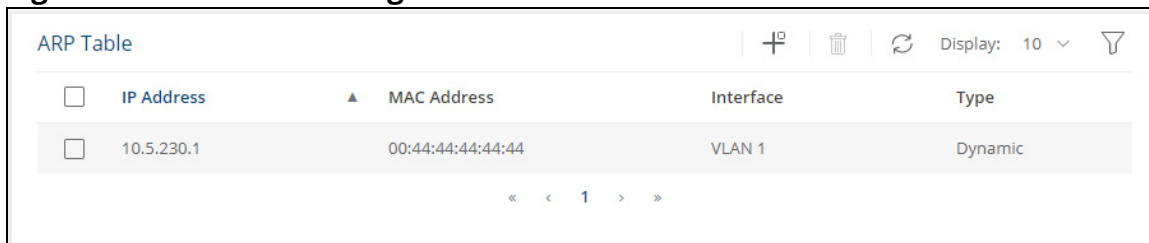
Click **APPLY** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

ARP Table

Use the ARP Table page to add an entry to the Address Resolution Protocol (ARP) table and to view existing entries.

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

Figure 173. ARP Table Page



The screenshot shows the 'ARP Table' page. It has a title bar 'ARP Table'. Below the title bar, there are icons for adding, deleting, and refreshing entries, and a 'Display: 10' dropdown menu. Below these, there is a table with the following columns: 'IP Address', 'MAC Address', 'Interface', and 'Type'. The table contains one entry: IP Address 10.5.230.1, MAC Address 00:44:44:44:44:44, Interface VLAN 1, and Type Dynamic. At the bottom of the table, there are navigation icons: '<<', '<', '1', '>', and '>>'.

Table 149. ARP Table Fields

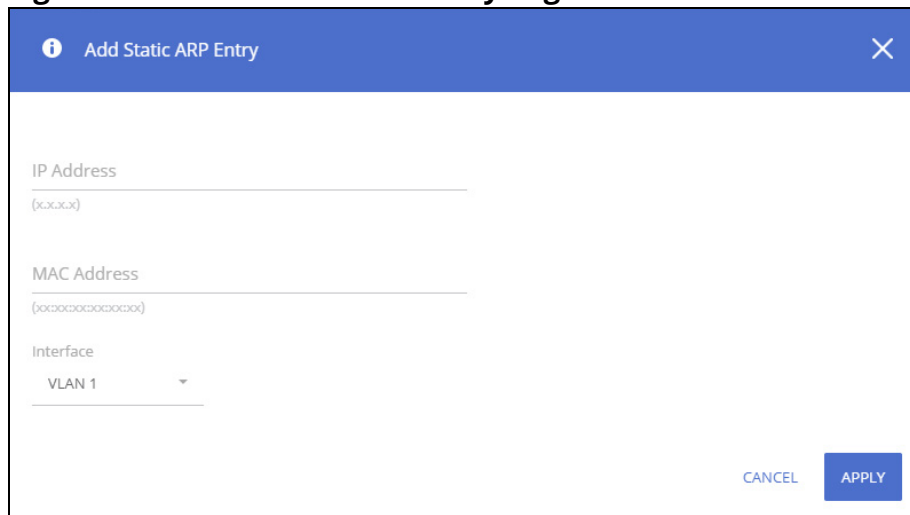
Field	Description
IP Address	The IP address of a network host on a subnet attached to one of the switch's routing interfaces. When adding a static ARP entry, specify the IP address for the entry after you click Add .
MAC Address	The unicast MAC address (hardware address) associated with the network host. 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: • Dynamic – An ARP entry that has been learned by the router • Static – 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 opens.

Figure 174. Add Static ARP Entry Page

The image shows a dialog box titled "Add Static ARP Entry" with a blue header bar containing an information icon and a close button. The main area is white and contains three input fields: "IP Address" with a placeholder "(x.x.x.x)", "MAC Address" with a placeholder "(xxxxxxxxxxxx)", and "Interface" with a dropdown menu showing "VLAN 1". At the bottom right, there are two buttons: "CANCEL" and "APPLY".

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 an ARP Entry

To delete one or more ARP entries, select each entry to delete and click **Remove** . Note that ARP entries designated as Local cannot be removed.

You can use the QoS pages to configure Access Control Lists (ACLs) and Class of Service (CoS).

Access Control Lists

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.

Aruba Instant On 1960 Switch Series switches support IPv4, IPv6, and MAC inbound ACLs. The maximum number of ACLs is 256.

- Access SKU: 960 MAX ACE entries available to user
- Aggregate SKUs in Native mode: 1024 Max ACE entries available to user

To configure an ACL:

1. Create an IPv4-, IPv6-, or MAC-based rule and assign a unique ACL ID. See [Access Control Lists](#) for more information.
2. Define the rules, which can identify protocols, source and destination IP and MAC addresses, and other packet-matching criteria. See [IPv4 ACL Rules](#) for more information.
3. Use the ID number to assign the ACL to a port or to a VLAN interface. See [Interface Configuration](#) for more information.

Access Control Lists

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

To display the Access Control Lists tile, click **QoS > Access Control Lists** in the navigation pane.

Figure 175. Access Control List Page

Access Control Lists						
			Display: 10			
☐	ACL Name	ACL Type	Rules	Bound Interfaces	Bound VLANs	
☐	ACL IPv4	IPv4	0			
☐	ACL MAC	MAC	0			
« < 1 > »						

Table 150. Access Control Lists Fields

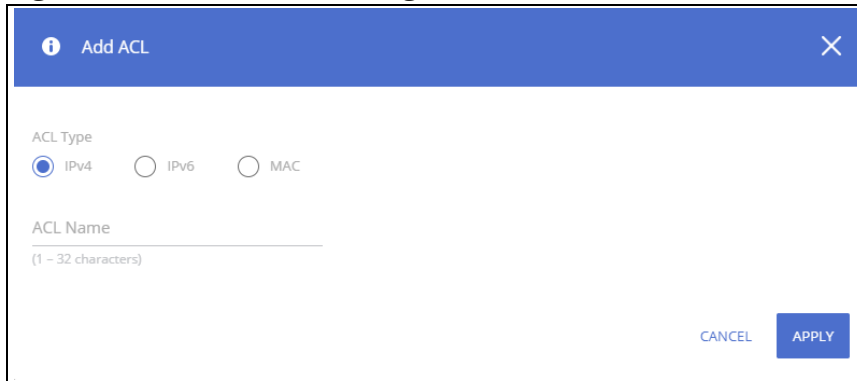
Field	Description
ACL Name	The name that identifies the ACL, 1-32 characters, case sensitive.
ACL Type	The type of ACL. The ACL type determines the criteria that can be used to match packets. These are the ACL types: • IPv4 – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv4 packets. • IPv6 – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv6 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.
Rules	The number of rules currently configured for the ACL.
Bound Interfaces	The interface(s) to which the ACL has been applied.
Bound VLANs	The VLAN(s) to which the ACL has been applied.

Adding an ACL

To add an ACL:

1. Click **Add**  to open the **Add ACL Entry** dialog box.

Figure 176. Add ACL Dialog Box

The image shows a dialog box titled "Add ACL" with a blue header bar containing an information icon and a close button. The main area is white and contains three radio buttons for "ACL Type": "IPv4" (selected), "IPv6", and "MAC". Below this is a text input field for "ACL Name" with a placeholder "(1 - 32 characters)". At the bottom right, there are two buttons: "CANCEL" and "APPLY".

2. Specify the type of ACL to add.
3. Assign a name.
4. Click **APPLY**.

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

IPv4 ACL Rules/IPv6 ACL Rules/MAC ACL Rules Tile

The **IPv4 ACL Rules/IPv6 ACL Rules/MAC ACL Rules** tile enables adding and editing rules to ACLs created by users.

To view the IPv4 ACL Rules click the **IPv4 ACL Rules** tab.

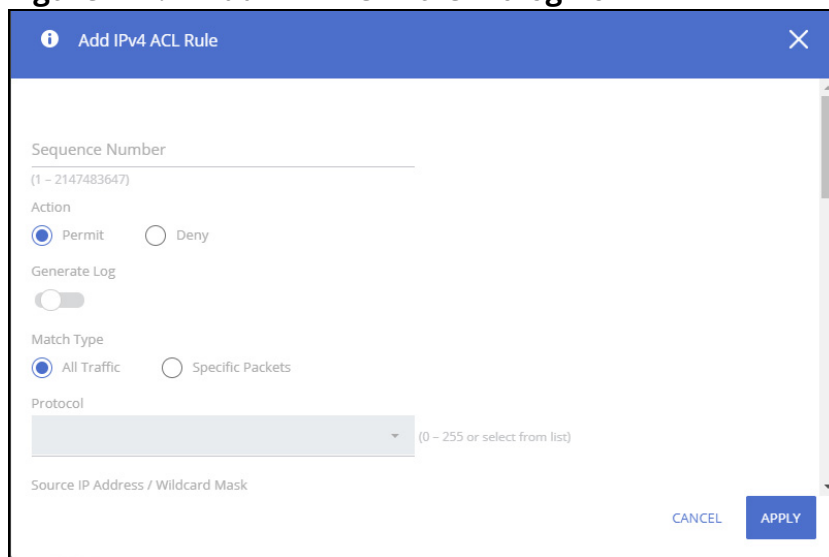
To view the IPv6 ACL Rules click the **IPv6 ACL Rules** tab.
 To view the MAC ACL Rules click the **MAC ACL Rules** tab.

IPv4 ACL Rules

To add a rule to an IPv4 ACL:

1. From the **IPv4 ACL Rules** tab, click the drop-down button next to the ACL Name list, select the name of the IPv4 ACL to configure.
2. Click **Add**  to open the **Add IPv4 ACL Rule** dialog box.

Figure 177. 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:
 - o Permit – The packet or frame is forwarded.
 - o Deny – The packet or frame is dropped.
5. To create a log of the ACL, set **Generate Log** to enable. If enabled, the switch sends an informational SYSLOG message if a receive packet matched the entry.
6. Select the appropriate **Schedule** from the drop-down list.
7. Specify the **Match Conditions** and rule attributes shown in **IPv4 ACL Match Criteria** below.
8. Click **APPLY**.

Table 151. IPv4 ACL Match Criteria

Field	Description
Match Type	• 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.

Field	Description
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. Wild card 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 protocol is either TCP or UDP. The following options are available: Equal to, Range, Greater than, and Less than. User can select port ID from the range 1-65535, 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 port IP address in the packet and destination IP wildcard mask (in the second field) to compare to the IP address in a packet header. Wild card masks determines which bits in the IP address are used and which bits are ignored. A wild card 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 protocol is either TCP or UDP. The following options are available: Equal to, Not Equal to, Greater than, and Less than. You can select a port ID from the range 1-65535, 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.
IGMP Type	IP ACL rule to match on the specified IGMP message type. This option is available only if the protocol is IGMP.
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. NOTE: This option is available only if the protocol is TCP.

Field	Description
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.

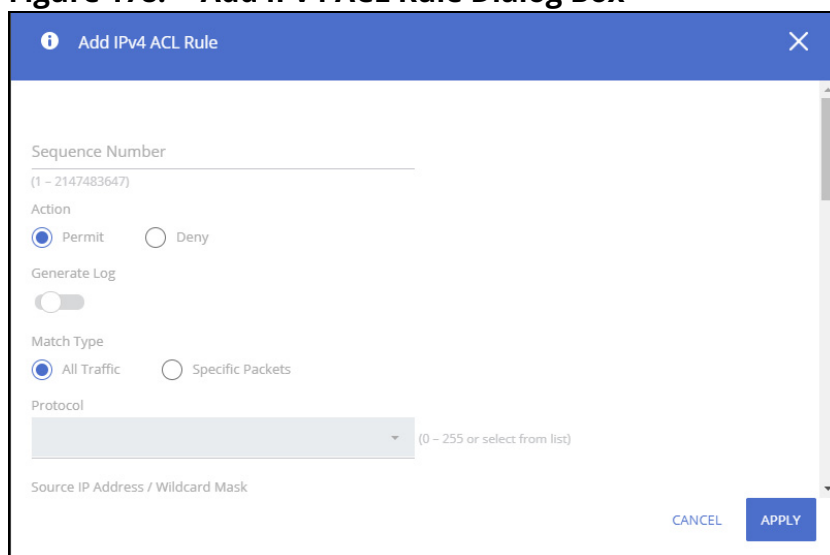
To remove a rule, select it in the list and click **Remove**  .

IPv6 ACL Rules

To add a rule to an IPv6 ACL:

1. From the **IPv6 ACL Rules** tab, click the drop-down button next to the ACL Name list, select the name of the IPv6 ACL to configure.
2. Click **Add**  to open the **Add IPv6 ACL Rule** dialog box.

Figure 178. Add IPv4 ACL Rule Dialog Box



The dialog box titled "Add IPv4 ACL Rule" contains the following fields and options:

- Sequence Number:** A text input field with a range indicator "(1 - 2147483647)".
- Action:** Two radio buttons: "Permit" (selected) and "Deny".
- Generate Log:** A toggle switch currently turned off.
- Match Type:** Two radio buttons: "All Traffic" (selected) and "Specific Packets".
- Protocol:** A dropdown menu with a range indicator "(0 - 255 or select from list)".
- Source IP Address / Wildcard Mask:** A text input field.
- Buttons:** "CANCEL" and "APPLY" buttons at the bottom right.

3. Specify a **Sequence Number** to indicate the position of a rule within the ACL.
4. Specify the **Action** for the rule:
 - o Permit – The packet or frame is forwarded.
 - o Deny – The packet or frame is dropped.
5. To create a log of the ACL, set **Generate Log** to enable. If enabled, the switch sends an informational SYSLOG message if a receive packet matched the entry.

6. Select the appropriate **Schedule** from the drop-down list.
7. Specify the **Match Conditions** and rule attributes shown in **IPv6 ACL Match Criteria** below.
8. Click **APPLY**

Table 152. IPv6 ACL Match Criteria

Field	Description
Match Type	- 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 IPv6 packet. You can also specify one of the keywords provided in the drop-down menu.
Source IP Address / Prefix	The source port IP address in the packet and source IP prefix (in the second field) to compare to the IP address in a packet header. The prefix determines which bits in the IP address are used and which bits are ignored. A prefix ff:ff:ff:ff:ff:ff indicates that no bit is important. A prefix of 00:00:00:00:00:00 indicates that all of the bits are important. Prefix masking for ACLs operates differently from a subnet mask. A prefix 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 prefix 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 IPv6 address. If not specified, this means any source IPv6.
Source L4 Port	The IPv6 TCP/UDP source port to match in the packet header. The Source L4 Port and Destination L4 port are configurable only if protocol is either TCP or UDP. The following options are available: Equal to, Range, Greater than, and Less than, with up to 4 ranges of either TCP or UDP ports supported You can select port ID from the range 1-65535, or select predefined protocols. These are the predefined protocols available for TCP: Echo, FTPdata, FTP, Telnet,SMTP,Domain,HTTP,POP2,POP3 or BGP. For UDP protocol: Echo, Time, Domain, TFTP, NTP, SNMP, WHO or RIP.
Destination IP Address / Prefix	The destination port IPv6 address in the packet and destination IP prefix (in the second field) to compare to the IP address in a packet header. The prefix determines which bits in the IP address are used and which bits are ignored. A prefix ff:ff:ff:ff:ff:ff indicates that no bit is important. A prefix of 00:00:00:00:00:00 indicates that all of the bits are important. Prefix masking for ACLs operates differently from a subnet mask. A prefix 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 prefix 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 IPv6 address.

Field	Description
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 protocol is either TCP or UDP. If left empty, this means any destination port. The following options are available: Equal to, Not Equal to, Greater than, and Less than, with up to 4 ranges of either TCP or UDP ports supported. You can select port ID from the range 1-65535, or select predefined protocols. These are the predefined protocols available for TCP: Echo, FTPdata, FTP, Telnet, SMTP, Domain, HTTP, POP2, POP3 or BGP. For UDP protocol: Echo, Time, Domain, TFTP, NTP, SNMP, WHO or RIP.
ICMP Type	IP ACL rule to match on the specified ICMP message type. This option is available only if the protocol is ICMP. If left empty, this means any ICMP code (any code is the default).
ICMP Code	IP ACL rule to match on the specified ICMP message code. This option is available only if the protocol is ICMP.
Flow Label	Specifies the IPv6 Flow Label value. The valid range is: 0-1048575, or any. The default is Any
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. If left empty, this means ignore flags. 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 IPv6 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. Valid range is: 0 - 63. • 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. Valid range is: 0 - 7.

To remove a rule, select it in the list and click **Remove**  .

MAC ACL Rules

To add a rule to an Extended MAC ACL:

1. From the **MAC ACL Rules** tab, click the drop-down button next to the ACL MAC list, select the ID of the extended MAC ACL. The ID is up to 32 alphanumeric characters.
2. Click **Add**  to open the **Add MAC ACL Rule** dialog box.

Figure 179. Add MAC ACL Page

Add MAC ACL Rule

Sequence Number
(1 - 2147483647)

Action
☒ Permit ☐ Deny

Generate Log
☐

Match Type
☒ All Traffic ☐ Specific Packets

CoS
(0 - 7)

Ethertype

CANCEL APPLY

3. Specify a **Sequence Number** to indicate the position of a rule within the ACL.
4. Specify the **Action** for the rule:
 - o Permit – The packet or frame is forwarded.
 - o Deny – The packet or frame is dropped.
5. To create a log of the ACL, set **Generate Log** to enable. If enabled, the switch sends an informational SYSLOG message if a receive packet matched the entry.
6. Select the appropriate Schedule from the drop-down list.
7. Specify the **Match Conditions** and rule attributes shown in **MAC ACL Match Criteria** below.
8. Click **APPLY**.

Table 153. MAC ACL Match Criteria

Field	Description
Match Type	• 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 0-7. The default is none.
Ethertype	The EtherType value to match in an Ethernet frame. Specify the number associated with the EtherType (range 600 - FFFF hex), or specify one of the keywords from the drop-down list.

Field	Description
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.

To remove a rule, select it in the list and click **Remove**  .

Interface and VLAN Configuration

Use this tile to bind an ACL to ports, LAGs or VLANs. Multiple ACLs can be configured on a port/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 display the Interface Configuration tab, click the **Interface Configuration** tab.

To display the VLAN Configuration tab, click the **VLAN Configuration** tab.

Interface Configuration

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.

Figure 180. Interface Configuration Tab

Interface Configuration

VLAN Configuration

+

🗑

↺

Display: 10

⌵

☐	Interface ▲	Direction	ACL Type	ACL Identifier	Sequence Number	Queue	Flow	Committed Rate	Burst Size
Table Is Empty									

Table 154. Interface Configuration Fields

Field	Description
Interface	The interface 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 (Inbound) or after it has been received, routed, and is ready to exit an interface (Outbound). Only the inbound direction is supported.
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. • IPv4 – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv4 packets. • IPv6 – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv6 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 menu contains the ID for each ACL that exists on the system. Before you add or remove a rule, you must select the ID 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.
Queue	The number (0-7) that identifies the hardware egress queue that handles all packets matching this rule.
Flow	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.
Committed Rate	The allowed transmission rate for frames on the interface. Range:100 – 10000000 kbits/sec.
Burst Size	The number of bytes allowed in a temporary traffic burst. Range: 3000 – 19173960 Bytes.

To add an interface configuration, click **Add**  and enter the values as needed.

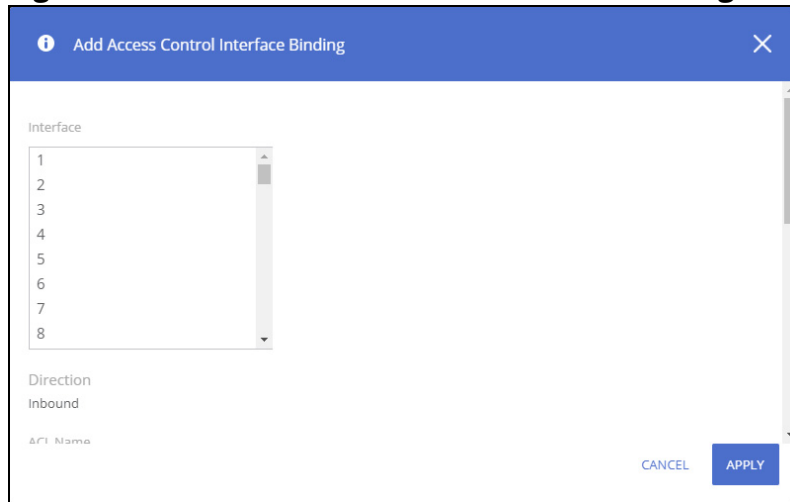
To remove a configuration, click the check box to the left of the session entry and click **Remove** .

Associating an ACL with an Interface

To apply an ACL to an interface:

1. In the Interface Configuration tab, click **Add**  .
The **Add Access Control List Interface Binding** dialog box appears.

Figure 181. Access Control List Interface Binding Dialog Box



2. Select one or more interfaces to associate with the ACL.
To select multiple interfaces, Ctrl + click each interface, or Shift + click a contiguous set of interfaces.
Only Inbound ACLs are supported.
3. Select the ACL name to associate with the interface or interfaces, from the drop-down list.
4. For the sequence number, select between **Auto** or specify a sequence number. If **Auto** is selected, the rule is automatically assigned a sequence number after it is successfully added to the ACL.
5. Under the **Actions** separator, enter values for **Assign Queue**, **Flow Action**, **Interface**, **Committed Rate**, and **Burst Size**. See details on the appropriate values in **Interface Configuration** Fields.
6. Click **APPLY**.

To remove one or more ACL-interface associations, select each entry to delete and click **Delete** .

VLAN Configuration

Use this page to associate one or more ACLs with one or more VLANs on the switch.

To display the VLAN Configuration tab, click **Quality of Service > Access Control Lists** and scroll down to **Interface/VLAN Configuration** tile, and click on the **VLAN Configuration** tab.

Figure 182. VLAN Configuration Tab

Interface Configuration		VLAN Configuration		+ - Refresh Display: 10 Filter	
☐	VLAN ID	▲	Direction	ACL Type	ACL Identifier
Table Is Empty					

Table 155. VLAN Configuration Fields

Field	Description
VLAN ID	The ID of the VLAN associated with the rest of the data in the row.
Direction	Indicates whether the packet is checked against the rules in an ACL when it is received on a VLAN (Inbound) or after it has been received, routed, and is ready to exit a VLAN (Outbound). Only the inbound direction is supported.
ACL Type	The type of ACL, which is either IPv4, IPv6, or MAC.
ACL Identifier	The name that identifies the ACL.

Associating an ACL with a VLAN

To apply an ACL to a VLAN:

1. Click **Add** + .
The Add Access Control VLAN Binding page appears.

Figure 183. Access Control VLAN Binding Dialog Box

Add Access Control VLAN Binding

VLAN ID

1

2

100

101

102

103

104

105

Direction

Inbound

ACL Name

CANCEL

APPLY

2. Select one or more VLANs to associate with the ACL.
To select multiple VLANs, Ctrl + click each VLAN, or Shift + click a contiguous set of VLANs.
3. Select the ACL name to associate with the VLAN or VLANs.

4. Click **APPLY**.

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

Class of Service

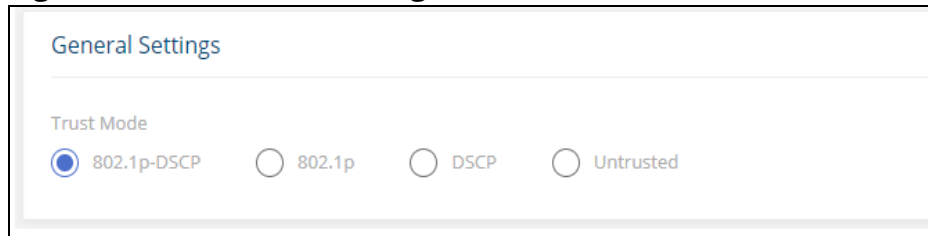
The Class of Service (CoS) queueing feature lets you directly configure certain aspects of switch queueing. This provides the desired QoS behavior for different types of network traffic when the complexities of DiffServ are not required. The priority of a packet arriving at an interface can be used to steer the packet to the appropriate outbound CoS queue through a mapping table. CoS queue characteristics that affect queue mapping, such as minimum guaranteed bandwidth, transmission rate shaping, etc., are user-configurable at the queue (or port) level.

To display the tile, click **QoS > Class of Service** in the navigation pane.

General Settings

Use the **General Settings** tile to configure the Trust Mode.

Figure 184. General Settings Tile



Trust mode is a global parameter that defines ingress traffic on all switch interfaces. Select one of the following:

- **802.1p-DSCP** - Classifies ingress packets with the packet IP DSCP values for IP packets. For other packet types, ingress traffic is classified with the packet 802.1p priority value encoded within the packet.
In the case that a frame is not an IP packet and is untagged, the frame is assigned to the queue associated with the default CoS value defined for the interface in the **Interface Configuration** tile.
- **802.1p** - Classifies ingress packets with the packet encoded 802.1 priority value.
For untagged packets, the frame is assigned to the queue associated with the default CoS value defined for the interface in the **Interface Configuration** tile.
- **DSCP** - Classifies ingress packets with the packet IP DSCP value.
If the frame is not an IP frame it is assigned to the queue associated with CoS value 0.
- **Untrusted** - The interface ignores any priority designations encoded in incoming packets.
Frames are assigned to the queue associated with CoS 0.

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

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.

To display the tile, click **QoS > Class of Service** in the navigation pane.

Figure 185. 802.1p Priority Mapping Tile

802.1p Priority	Traffic Class
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Table 156. 802.1p Priority Mapping Configuration Fields

Field	Description
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 CoS Mapping

To configure the 802.1p mapping for one or more interfaces:

1. Select the 802.1p Priority Mapping value to configure and select the traffic class to map to the 802.1p priority value for the interface from the drop-down button.
2. Repeat for any other 802.1p Priority Mapping you wish to configure.

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** page 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.

To display the Queue Configuration tile, click **Quality of Service > Class of Service**.

Figure 186. Queue Configuration Tile

Queue Configuration				
Queue	Scheduler Type		WRR Weight (1 - 255)	WRR Percentage
0	☒ WRR	☐ Strict Priority	2	40.00 %
1	☒ WRR	☐ Strict Priority	3	60.00 %
2	☐ WRR	☒ Strict Priority	1	
3	☐ WRR	☒ Strict Priority	1	

Table 157. Queue Configuration Fields

Field	Description
Queue	The queue to be configured.
Schedule Type	Select the type of queue processing per-queue. This enables creating the desired service characteristics for different types of traffic. • WRR: Weighted round robin associates a weight to each queue. • Strict Priority: Strict priority services traffic with the highest priority on a queue first By default, these are the settings, by queue: • Q7 - Strict Priority • Q6 - 20% of bandwidth to allocate to queue • Q5 - 15% of bandwidth to allocate to queue • Q4 - 15% of bandwidth to allocate to queue • Q3 - 15% of bandwidth to allocate to queue • Q2 - 30% of bandwidth to allocate to queue • Q1 - 3% of bandwidth to allocate to queue • Q0 - 2% of bandwidth to allocate to queue

Field	Description
WRR Weight	The weight assigned to queues that are configured to the Weighted Round Robin Scheduler Type. The valid range is 1-255. The default is according to the queue.
WRR Percentage	Displays the calculated percentage of traffic for this queue compare to all other queues that are set to WRR schedule. The ratio for each queue is defined as the queue weight divided by the sum of all queue weights (the normalized weight). This sets the bandwidth allocation of each queue. All queues participate in the WRR, excluding the expedite queues, whose corresponding weight is not used in the ratio calculation.

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.

To display the DSCP CoS Mapping tile, click **QoS > Class of Service** in the navigation pane, and scroll down to the **DSCP CoS Mapping** tile.

Figure 187. DSCP CoS Mapping Tile

DSCP CoS Mapping							
IP DSCP	Traffic Class	IP DSCP	Traffic Class	IP DSCP	Traffic Class	IP DSCP	Traffic Class
0 - be/cs0	0	16 - cs2	5	32 - cs4	6	48 - cs6	5
1	0	17	4	33	4	49	5
2	0	18 - af21	4	34 - af41	4	50	5
3	0	19	4	35	4	51	5
4	0	20 - af22	4	36 - af42	4	52	5
5	0	21	4	37	4	53	5
6	0	22 - af23	4	38 - af43	4	54	5
7	0	23	4	39	4	55	5
8 - cs1	0	24 - cs3	5	40 - cs5	5	56 - cs7	5
9	1	25	3	41	6	57	5
10 - af11	1	26 - af31	3	42	6	58	5
11	1	27	3	43	6	59	5

Table 158. DSCP CoS Mapping Configuration Fields

Field	Description
IP DSCP	Lists the IP DSCP values to which you can map an internal traffic class. The values range from 0-63.

Field	Description
Traffic Class	The traffic class is the hardware queue for a port. Higher traffic class values indicate a higher queue position. Before traffic in a lower queue is sent, it must wait for traffic in higher queues to be sent. Valid range is 0 to 7. The page displays the default values per each IP DSCP.

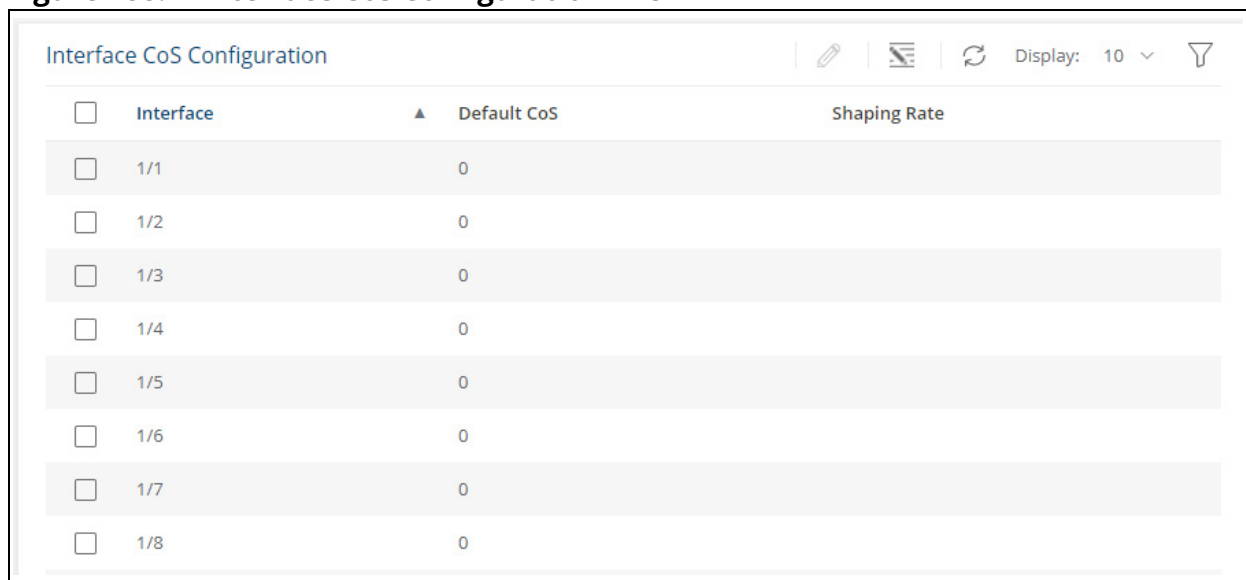
Click **APPLY** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Interface CoS Configuration

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

To display the **Interface Configuration** tile, click **QoS > Class of Service** in the navigation pane, and scroll down to the tile.

Figure 188. Interface Cos Configuration Tile



☐ Interface	▲ Default CoS	Shaping Rate
☐ 1/1	0	
☐ 1/2	0	
☐ 1/3	0	
☐ 1/4	0	
☐ 1/5	0	
☐ 1/6	0	
☐ 1/7	0	
☐ 1/8	0	

Table 159. Interface CoS Configuration Fields

Field	Description
Interface	Selects the CoS configurable interface to be affected by the Interface Shaping Rate.
Default 802.1p Priority	Sets the default CoS for the interface. This is the default CoS value used for Global trust mode 802.1p, or 802.1p-DSCP.
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: 64 – 1000000 Kbits/Sec.

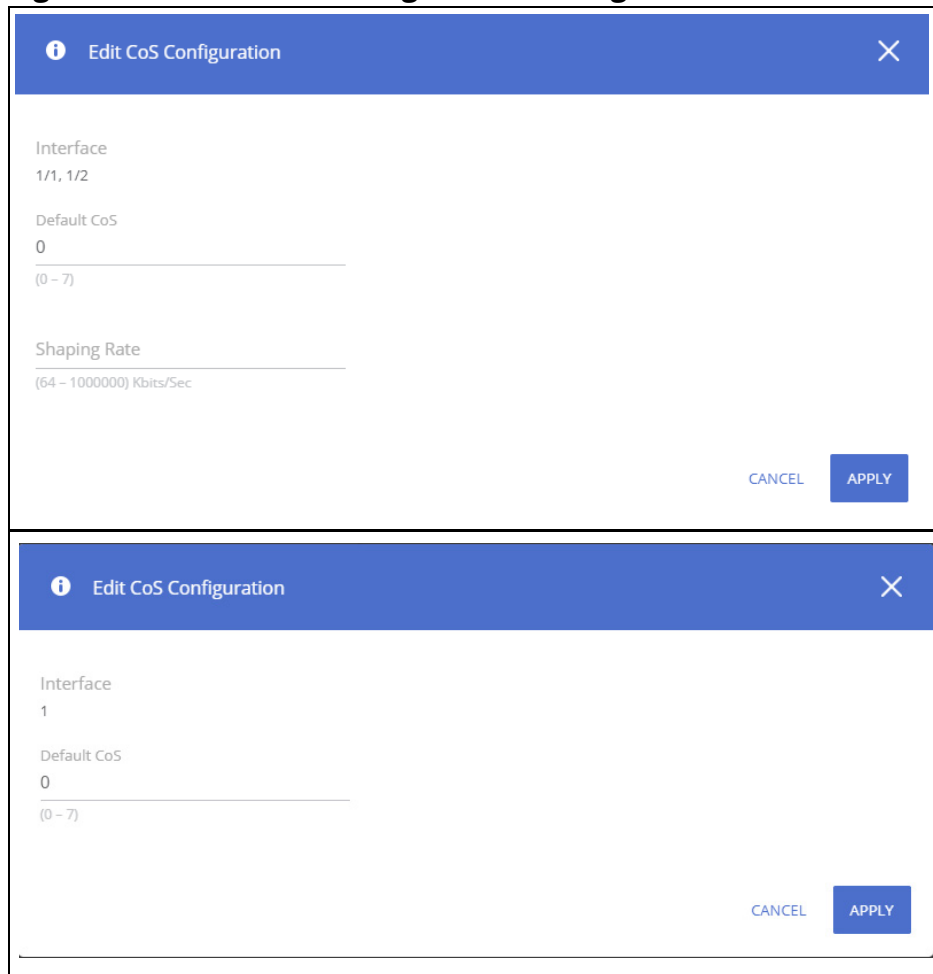
Configuring the CoS on an Interface

To configure the CoS for all the interfaces, click **Edit All** .

To configure the CoS for one or more interfaces:

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

Figure 189. Edit CoS Configuration Dialog Box



The figure displays two identical dialog boxes titled "Edit CoS Configuration". Each dialog box has a blue header bar with an information icon, the title, and a close button. The main content area contains three fields: "Interface" with the value "1/1, 1/2", "Default CoS" with the value "0", and "Shaping Rate" with the value "(64 - 1000000) Kbits/Sec". At the bottom right of each dialog box are two buttons: "CANCEL" and "APPLY".

2. Specify the Default 802.1p Priority value, and the shaping rate for all interfaces identified in the Interface field(s).

- 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 Statistics

Use the **Queue Statistics** tile to get information on the Queues.

To display the **Queue Statistics** tile, click **QoS > Class of Service** in the navigation pane, and scroll down to the tile.

Figure 190. Queue Statistics Tile

Queue Statistics 🏠 ↻ Display: 10 ▼ 🔍						
☐	Interface ▲	Queue	Transmitted Packets	Tail Dropped Packets	Transmitted Bytes	Tail Dropped Bytes
☐	1/1	0	0	0	0	0
☐	1/1	1	0	0	0	0
☐	1/1	2	0	0	0	0
☐	1/1	3	0	0	0	0
☐	1/1	4	0	0	0	0
☐	1/1	5	0	0	0	0

Table 160. Queue Statistics Fields

Field	Description
Interface	The interface identifier.
Queue	The specific queue to which the information relates.
Transmitted Packets	The number of packets that were transmitted on this queue.
Tail Dropped Packets	The number of packets that were tail dropped on this queue.
Transmitted Bytes	The number of bytes that were transmitted on this queue.
Tail Dropped Bytes	The number of bytes that were tail dropped on this queue.

Select an interface and click **Clear**  to clear the statistics from the Queues that are associated with the selected interface.

Overview

The Aruba Instant On 1960 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.

RADIUS Configuration

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. The Aruba Instant On 1960 Switch Series switch includes a RADIUS client that can contact one or more RADIUS servers for various Authentication and Accounting (AAA) services. The RADIUS server maintains a centralized database that contains per-user information.

The switch can connect to up to 4 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 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.

Global Configuration

Use the Global Configuration page to configure global settings for the Remote Authentication Dial-In User Service (RADIUS) feature and to configure one or more RADIUS servers for the switch to contact.

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

Figure 191. Global Configuration Tile

Global Configuration

802.1x Authentication Mode

☒

802.1x Accounting Mode

☒

Max Number of Retransmits

3

(1 - 15)

Timeout Duration

3

(1 - 30) Seconds

Table 161. 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.
802.1X Accounting Mode	Specifies whether the IEEE 802.1X 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 × 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.
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.

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**.

Radius Server Configuration

Figure 192. RADIUS Server Configuration Tile

RADIUS Server Configuration

☐ Current ▲ IP Address Authentication Port Accounting Port Server Priority

Table Is Empty

Table 162. RADIUS Server Configuration Fields

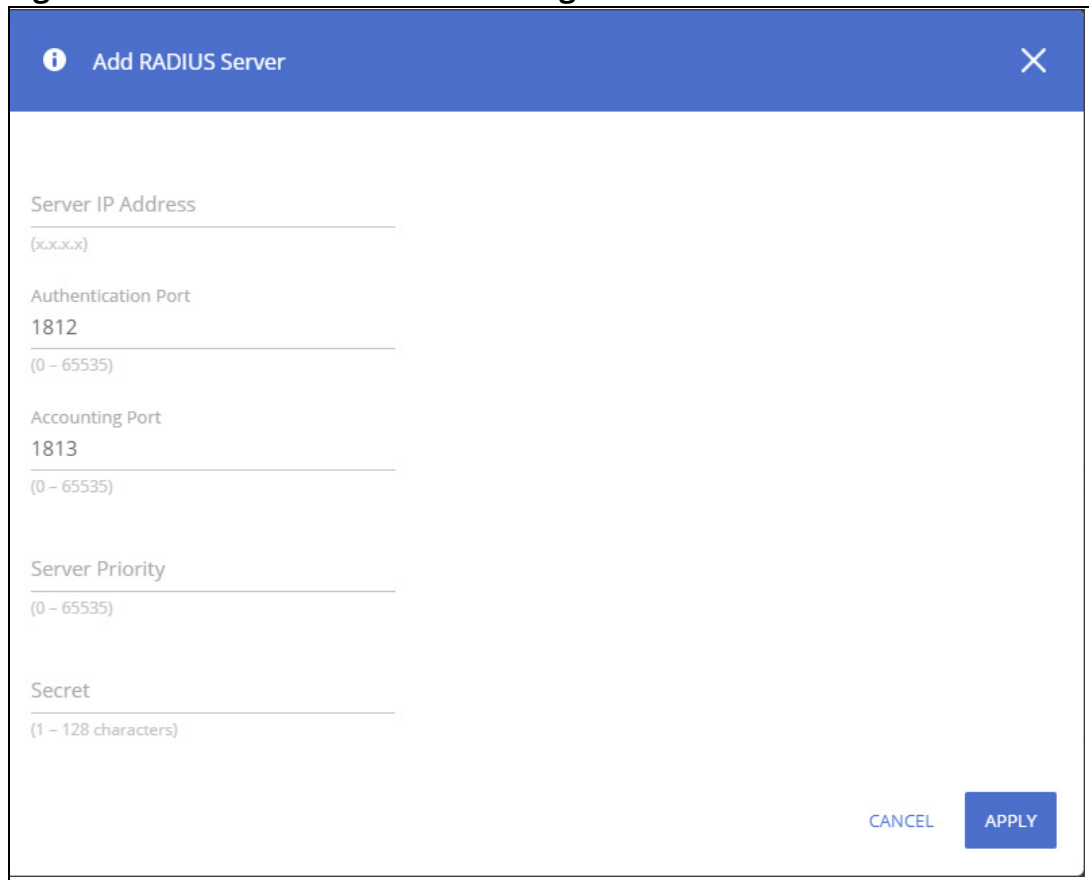
Field	Description
Current	Identifies whether the configured RADIUS server is the current server for the authentication server group. • True—The server is the current server for the authentication. • False—The server is not the current server for authentication. When the switch sends a RADIUS request 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	The IP address of the RADIUS server. 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%<ID> • Hostname - specify the server hostname
Authentication Port	Identifies the authentication port the server uses for handling RADIUS authentication requests. The port is a UDP port.
Accounting Port	Identifies the accounting port the server uses for handling RADIUS accounting packets. 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

Adding a RADIUS Server

To add a RADIUS server to the switch configuration:

1. Click Add . The **Add RADIUS Server** dialog box appears.

Figure 193. Add RADIUS Server Dialog Box



The dialog box is titled "Add RADIUS Server" with an information icon on the left and a close icon on the right. It contains five input fields with labels and placeholder text:

- Server IP Address**: Placeholder text "(x.x.x.x)".
- Authentication Port**: Value "1812", placeholder text "(0 - 65535)".
- Accounting Port**: Value "1813", placeholder text "(0 - 65535)".
- Server Priority**: Placeholder text "(0 - 65535)".
- Secret**: Placeholder text "(1 - 128 characters)".

At the bottom right, there are two buttons: "CANCEL" and "APPLY".

2. Specify the required information about the RADIUS server.
3. Enter the Secret (1-128 chars) - This 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. 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.
2. Click **Edit**  .
The Edit RADIUS Server page appears.
3. Update the RADIUS server information as needed. The IP address of an existing RADIUS server cannot be changed.
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**.

To delete one or more RADIUS servers, select 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 of any one supplicant attached to the port results in all users being able to use the port without restrictions. At any given time, only one supplicant is allowed to attempt authentication on a port in this mode. Ports in this mode are under bidirectional control. This is the default authentication mode.

The 802.1X network has three components:

- **Authenticators:** Specifies the port that is authenticated before permitting network access.
- **Supplicants:** Specifies host connected to the authenticated port requesting access to the network services.
- **Authentication Server:** Specifies 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.

Global Configuration

Use this 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.

To display the Global Configuration tile, click **Security > Port Access Control** in the navigation pane.

Figure 194. Global Configuration Tile

The image shows a 'Global Configuration' tile with the following settings:

- Admin Mode:** A toggle switch currently in the 'Off' position.
- EAPOL Flood Mode:** A toggle switch currently in the 'Off' position.
- Guest VLAN:** A toggle switch currently in the 'On' position (blue).
- Guest VLAN ID:** A dropdown menu with a downward arrow, currently showing an empty field.
- Guest VLAN Timeout:** Two radio buttons. The 'Immediate' option is selected (blue dot). The second option is an empty radio button with a text input field below it labeled '(30 - 180) Seconds'.

Table 163. Global Configuration Fields

Field	Description
Admin Mode	Select Enable or Disable 802.1x 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 switch. If flood mode is enabled, then the switch will bridge 802.1x PDUs received on switch interfaces. In flood mode the switch filters (drops) such PDUs. The default setting is disable. EAPOL Flood Mode can be enabled when Admin Mode and Monitor Mode are disabled.
Guest VLAN	Displays the admin mode of 802.1x guest VLAN. If enabled - guest VLAN can be enabled on ports using the guest VLAN ID. Default setting is disable.
Guest VLAN ID	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. NOTE: this field can be configured only if guest VLAN admin mode is set to enable.
Guest VLAN Timeout	Set Immediate or the number of seconds for the guest VLAN timeout. The Guest VLAN timeout specifies the time delay in seconds between enabling 802.1X (or port up) and adding the port to the guest VLAN. Set Immediate to apply the guest VLAN immediately.

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**.

MAC Authentication Settings

Use this tile to configure the MAC authentication settings. The MAC authentication settings enable you to customize the format in which MAC authentication requests are sent to the RADIUS server.

To display the Global Configuration tile, click **Security** > **Port Access Control** in the navigation pane.

Figure 195. MAC Authentication Settings Tile

The figure shows a configuration tile titled "MAC Authentication Settings". It contains several radio button options and a text input field. The "MAC Authentication Type" section has two options: "EAP-MD5" (selected) and "PAP". The "Username Group Size" section has four options: "1", "2", "4", and "12" (selected). The "Username Delimiter" section has three options: "-" (selected), ":", and ".". The "Username Casing" section has two options: "Uppercase" and "Lowercase" (selected). The "Password" section has two options: "Use username" (selected) and an empty text input field with a placeholder "(1 - 32 characters)".

Table 164. MAC Authentication Fields

Field	Description
MAC Authentication Type	Select EAP-MD5 or PAP.
Username Group Size	The number of characters between each delimiter. Available values are 1, 2 (the default) 4 and 12 (which indicates no delimiter).
Username Delimiter	Select the delimiter to use in username. Supported values are "-" (Hyphen), ":" (Colon) and . (period). The default is colon (":")
Username Casing	Select Uppercase or Lowercase for the letters a-f of the MAC address. Default is Lowercase.
Password	Select Use Username to use the MAC Authentication username (in its defined format) as the password. To use a different password, select the other radio button and enter the password. This password will be used for all MAC Authentication supplicants.

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**.

Port Configuration

To display the Port Configuration tile, click **Security > Port Access Control** in the navigation pane, and scroll down to the **Port Configuration** tile.

Figure 196. Port Configuration

Interface	PAE Capabilities	Control Mode	Operating Control Mode	PAE State
1	Authenticator	Force Authorized	N/A	Initialize
2	Authenticator	Force Authorized	N/A	Initialize
3	Authenticator	Auto	N/A	Initialize
4	Authenticator	Force Authorized	N/A	Initialize

Table 165. Port Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row.
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. - MAC-Based – This mode allows multiple supplicants connected to the same port to each authenticate individually. Each host connected to the port must authenticate separately in order to gain access to the network. The hosts are distinguished by their MAC addresses.
Operating Control Mode	The control mode under which the port is actually operating, which is one of the following: - Auto - Force Authorized - Force Unauthorized - MAC-Based - 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.

Field	Description
PAE State	The current state of the authenticator PAE state machine, which is the 802.1X process that controls access to the port. The state can be one of the following: • Initialize • Disconnected • Connecting • Authenticating • Authenticated • Aborting • Held • Force Authorized • Force Unauthorized

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**.
The Edit Port Configuration page appears.

Figure 197. Edit Port Configuration Page

Edit Port Configuration

Interface
1

PAE Capabilities
☒ Authenticator ☐ Supplicant

Control Mode
 Force Authorized ▼

Quiet Period
 60
 (10 – 65535) Seconds

Transmit Period
 30
 (30 – 65535) Seconds

CANCEL APPLY

3. Update the 802.1X settings on the interface. The following table 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 166. 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 are displayed and can be changed only when the PAE Capabilities field of the selected port is configured as 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. • MAC-Based – This mode allows multiple supplicants connected to the same port to each authenticate individually. Each host connected to the port must authenticate separately in order to gain access to the network. The hosts are distinguished by their MAC addresses. This control mode is required for MAC Authentication 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.
Monitor Mode	Enable this option to allow network access on the port even in cases where there is a failure to authenticate. However in such a case a log is generated with the results of the authentication process for diagnostic purposes. Monitor mode provides a way for network administrators to identify possible issues with the port-based access control configuration on the switch without affecting the network access to the users of the switch.

Field	Description
VLAN Assignment	The authentication server can provide information to the switch about which VLAN to assign the supplicant, and whether the port should be added as a tagged or untagged member of this VLAN. Enable this option to allow a port to be placed into a particular VLAN, based on the result of the authentication or type of 802.1X authentication. A client uses when it accesses the switch. Notes: • If the port is not already a member of the VLAN specified by the RADIUS reply, the port will join the specified VLAN as a tagged or un-tagged member, based on the information indicated by the RADIUS reply for the supplicant. • If the port is already a member of the VLAN specified by the RADIUS server (whether via user configuration or via 802.1x dynamic VLAN assignment), then the tagged indication provided by the RADIUS reply must match the tag status of the VLAN on the port. If this is not the case, the authentication for such a supplicant will fail. • If the port is already a static (configured by user) member of the VLAN returned by the RADIUS server for the supplicant, then: ◦ If the tag indication returned by the RADIUS server for the new supplicant matches that of the Static VLAN configured on the port, then the 802.1x authentication of the supplicant will succeed. ◦ If the tag indication returned by the RADIUS server for the new supplicant DOES NOT match that of the static VLAN configured on the port, then the 802.1x authentication for this supplicant will fail. • If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN as part of the authentication, the supplicant is accepted and classified based on regular VLAN rules. • If the RADIUS server authorized the supplicant with a VLAN ID that does not exist on switch, the switch will dynamically create the specified VLAN ID. If last supplicant with this VLAN ID assignment is removed from switch the VLAN will also be removed.
Guest VLAN	Enable guest VLAN operation on port.
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	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.
Re-Authentication Period	Specify the amount of time that clients can be connected to the port without being reauthenticated. Values are 300 – 4294967295 Seconds, or Never. If this field is set to Never, connected clients are not forced to reauthenticate periodically.
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
Supplicant Options The fields in this section are displayed and can be changed only when the PAE Capabilities field for the selected port is configured as 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.
Credentials	Select the credentials to use for port authentication from the drop down box. Supplicant credentials need to be created before they are available for selection in this control
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.

Select one or more rows and click the **Additional Option**   drop-down to initiate one of the following operations (This option is available 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.
- **Initiate:** 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

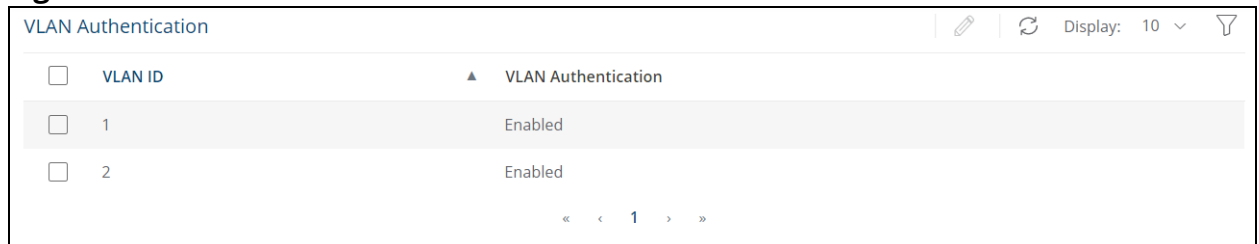
To view the detailed 802.1X configuration on an interface, select the interface and click **Details**. See **Configuring Port Access Control on an Interface** for information about the fields the Port Access Control Port Details page displays. Note that the fields that display after you click Details depend on whether the port is configured with Authenticator or Supplicant PAE Capabilities.

VLAN Authentication

This tile provides authentication configuration, and information on the VLANs.

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. Only tagged unauthenticated traffic is allowed on such VLANs. Authentication can be disabled on any VLAN created by the user but not on a Guest VLAN or the Default VLAN.

Figure 198. VLAN Authentication Tile



☐ VLAN ID	☐ VLAN Authentication
☐ 1	Enabled
☐ 2	Enabled

Select a VLAN ID and click **Edit**  to enable/disable the VLAN Authentication for the selected VLAN. The default for all VLANs is enable (Authentication is required on the VLAN).

Supplicant Credentials

This tile provides credential information on the supplicants.

Figure 199. Supplicant Credentials Tile



☐ Name	☐ Username	☐ Description
Table Is Empty		

Table 167. Supplicant Credentials Fields

Field	Description
Name	The supplicant credential name.
Username	The name the client uses to identify itself as a supplicant to the authentication server.
Description	Optional description of the credentials.

To add a supplicant to the list, click **Add**  and enter the appropriate fields. In addition to the fields in the table, you also need to enter the password that the client uses as credentials to identify as a supplicant to the authentication server.

To edit an existing supplicant, select it in the list, and click **Edit**  and edit the appropriate fields as needed.

To remove an existing supplicant, select it in the list, and **Remove** .

Access Control Client Information

This tile provides information on the supplicant devices that are connected to the local authenticator ports. If there are no active 802.1X sessions, the table is empty.

To access the Access Control Client Information tile, click **Security > Port Access Control** in the navigation pane, and then scroll down to the **Access Control Client Information** tile.

Figure 200. Access Control Client Information Tile

Access Control Client Information					
Interface	▲	Username	Supplicant MAC Address	Authentication Method	Session Time (HHH:MM:SS)
VLAN ID					
Table Is Empty					

Table 168. 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.

Access Control Statistics

Use this tile to view information about the Extensible Authentication Protocol over LAN (EAPOL) frames and EAP messages sent and received by the local interfaces. To view additional per-interface EAPOL and EAP message statistics, select the interface with the information to view and click **Details**.

To access the Access Control Statistics tile, click **Security > Port Access Control** in the navigation pane, and scroll down to the **Access Control Statistics** tile.

Figure 201. Access Control Statistics Tile

Access Control Statistics						
☐	Interface ▲	PAE Capabilities	EAPOL Frames Received	EAPOL Frames Transmitted	Last EAPOL Frame Version	Last EAPOL Frame Source
☐	1	Authenticator	2	0	0	00:00:00:00:00:00
☐	2	Authenticator	0	0	0	00:00:00:00:00:00
☐	3	Authenticator	4	0	0	00:00:00:00:00:00
☐	4	Authenticator	3	0	0	00:00:00:00:00:00

Table 169. Access Control Statistics Fields

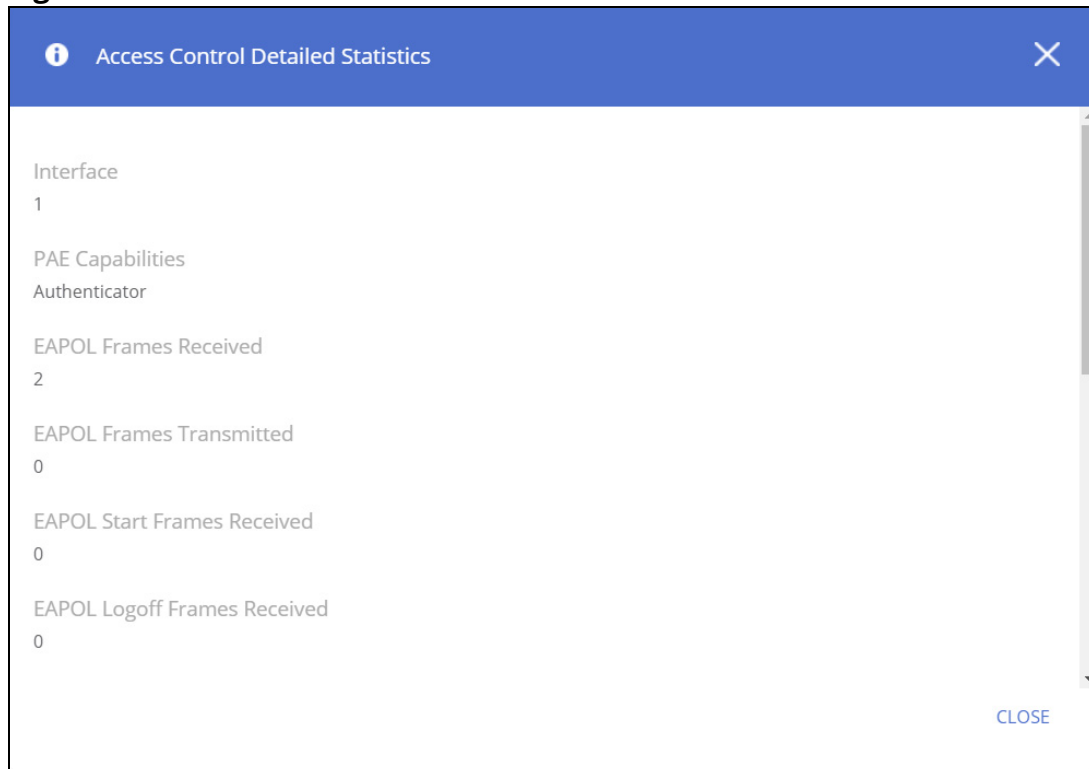
Field	Description
Interface	The interface associated with the rest of the data in the row. When viewing detailed information for an interface, this field identifies the interface being viewed.
PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following: • Authenticator – The port 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 all statistics counters to 0, select each interface with the statistics to reset and click **Clear**.

Access Control Details

To view Access Control Detailed Statistics, select an interface and click **Details** 

Figure 202. Access Control Detailed Statistics



The following table describes the additional fields that appear in the Details window. The fields this window displays depend on whether the interface is configured as an authenticator or supplicant, as noted in the applicable field descriptions.

Table 170. Access Control Statistics 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.
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.
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.
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.
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.

Field	Description
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.
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.	
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, that port's 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 are 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.

Port Security Configuration

Use this tile to view and configure the port security settings for each interface.

To view the Port Security Configuration tile, click **Security** > **Port Security** in the navigation pane,

Figure 203. Port Security Configuration Tile

Port Security Configuration										Display: 10	
☐	Interface	▲ Port Security	Max Addresses Allowed	Sticky Mode	Violation Trap	Violation Shutdown					
☐	1	Disabled	1	Disabled	Disabled	Disabled					
☐	2	Disabled	1	Disabled	Disabled	Disabled					
☐	3	Disabled	1	Disabled	Disabled	Disabled					
☐	4	Disabled	1	Disabled	Disabled	Disabled					

To configure port security settings on one or more interfaces, select the interface or interfaces to configure, and click **Edit** . To configure all interfaces at the same time, click **Edit All** .

Table 171. Port Security Interface Status 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 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 are 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: 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.
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, click the **Static MAC Address** tab.

To view the dynamic MAC address information, click the **Dynamic MAC Address** tab.

Static MAC Addresses

Use this 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 addressed learned on interfaces set to sticky mode disable, which were converted to static addresses by users.
- MAC addressed learned dynamically by switch on interfaces that are sticky mode enabled.

To display this tab, click **Security > Port Security** in the navigation pane, and then click the **Static MAC Addresses** tab.

Figure 204. Static MAC Addresses Tab

Interface	MAC Address	VLAN ID	Sticky Mode
Table Is Empty			

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** .

Table 172. 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.
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.

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

Dynamic MAC Addresses

Use this tab to view 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.

To display this tab, click **Security > Port Security** in the navigation pane, and then click the **Dynamic MAC Addresses** tab.

Figure 205. Port Security Dynamic MAC Addresses Tab

Table 173. Port Security 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.
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.
Type	The type of MAC address. The supported type is Learned .

Convert Dynamic MAC Addresses to Static MAC Addresses

To convert dynamic MAC addresses to static MAC addresses: Select the row(s) you wish to convert, 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 2 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.

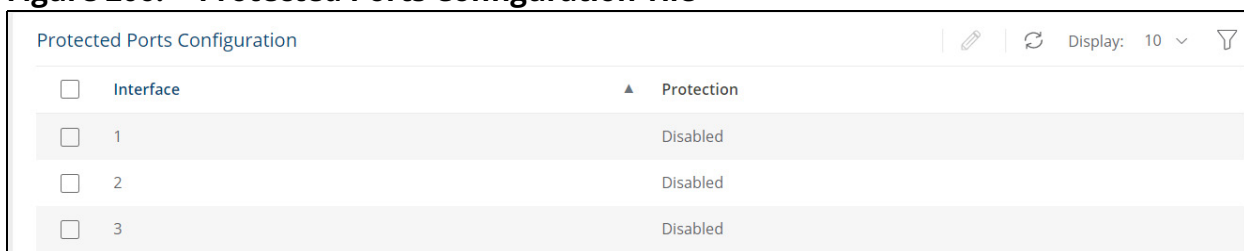
Port Protection is independent from any and all other features and configuration settings. For example: a user can place two protected ports into a common VLAN, and they will not be able to communicate with each other; By the same token, a protected port will not be able to communicate with an unprotected port, if the two ports are not in the same VLAN.

Protected Ports Configuration

Use this page to configure and view protected ports settings.

To view the Protected Ports Configuration tile, click **Security > Protected Ports** in the navigation pane.

Figure 206. Protected Ports Configuration Tile



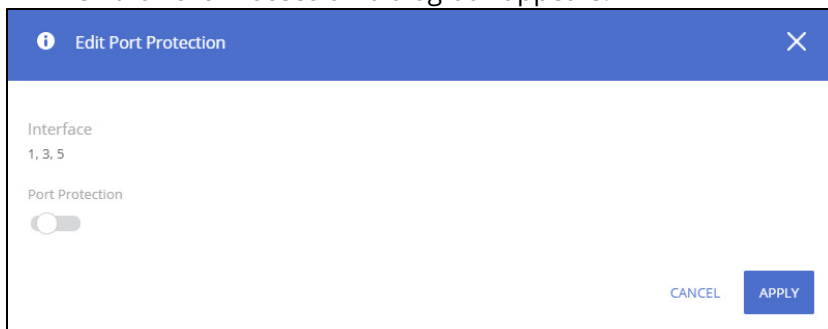
Interface	Protection
☐ 1	Disabled
☐ 2	Disabled
☐ 3	Disabled

Table 174. Protected Ports Configuration Fields

Field	Description
Interface	The port or trunk ID.
Protection	Displays the Admin state of Port Protection on the interface: - Disabled - port is an unprotected port. this is the default setting. - Enabled - port is a protected port

To change the Protection setting of an interface: create a protected ports group and add ports to the group:

1. Select the row(s) you wish to edit.
2. Click **Edit**  .
The **Edit Port Protection** dialog box appears.



3. Enable or disable Port Protection as needed.
4. Click **APPLY**.

DHCP Snooping and IPSG

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 other 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 SNTP, 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 data base 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.

Global Configuration

Use this tile to configure the global DHCP snooping and IPSG options:

Figure 207. Global Configuration Tile

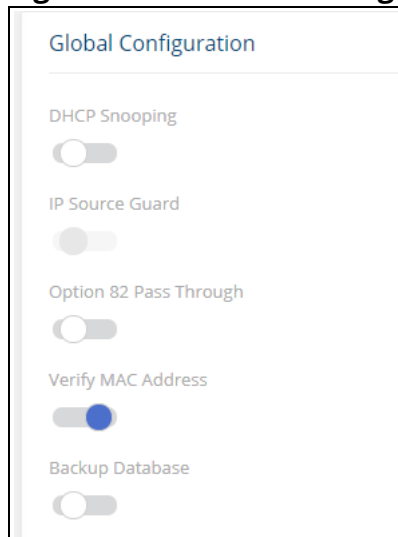


Table 175. Global Configuration Fields

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.
IP Source Guard	Enable or disable, This option is only available if DHCP Snooping is enabled.
Option 82 Pass Through	Enabled or disable. By default, option 82 pass through is disabled. • Disable - DHCP packets with option-82 information from an untrusted port are discarded. • Enable - DHCP packets with option-82 information from an untrusted port are forwarded.
Verify MAC Address	Enabled 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.
Backup Database	Enabled/ Disabled. By default, database backup is disabled. • Disable - DHCP snooping entries are not saved to a table on switch flash memory. • Enable - DHCP snooping entries are saved to a table on switch flash memory, and saved across reboots. To activate flash database update, you need to set the clock (manually or through SNTP).

VLAN Settings

Use the VLAN Settings tile to set enable DHCP Snooping on the required VLANs.

Figure 208. VLAN Settings Tile

The screenshot shows the 'VLAN Settings' tile. At the top, there's a title 'VLAN Settings' with edit, refresh, and filter icons. Below is a table with two columns: 'VLAN ID' and 'DHCP Snooping'. There are two rows: VLAN 1 and VLAN 2, both showing 'Disabled' for DHCP Snooping. A pagination bar at the bottom shows '1' as the current page.

VLAN ID	DHCP Snooping
1	Disabled
2	Disabled

Table 176. VLAN Settings Fields

Field	Description
VLAN ID	Identifier for the VLAN.
DHCP Snooping	Enabled or disable. By default, DHCP snooping is disabled.

To change the setting for DHCP snooping, select a VLAN and click **Edit**  .

Interface Settings

Use the Interface Settings tile to set ports to DHCP snooping trusted or untrusted state, and to enable or disable IP Source Guard.

Figure 209. Interface Settings Tile

The screenshot shows the 'Interface Settings' tile. At the top, there's a title 'Interface Settings' with edit, refresh, and filter icons. Below is a table with three columns: 'Interface', 'Trust Mode', and 'IP Source Guard'. There are four rows: 1/1, 1/2, 1/3, and 1/4. All rows show 'Untrusted' for Trust Mode and 'Disabled' for IP Source Guard. A pagination bar at the bottom shows '1' as the current page.

Interface	Trust Mode	IP Source Guard
1/1	Untrusted	Disabled
1/2	Untrusted	Disabled
1/3	Untrusted	Disabled
1/4	Untrusted	Disabled

Table 177. Interface Settings Fields

Field	Description
Interface	Identifier for the interface.
Trust Mode	Trusted or Untrusted. By default, DHCP snooping is untrusted.
IP Source Guard	Enabled or Disabled. By default IP Source Guard is disabled.

Select one or more interface(s) and click **Edit**  to toggle the trusted interface feature. Click **Edit All**  to configure all interfaces at the same time.

Figure 210. Edit DHCP Snooping Interface Settings Dialog

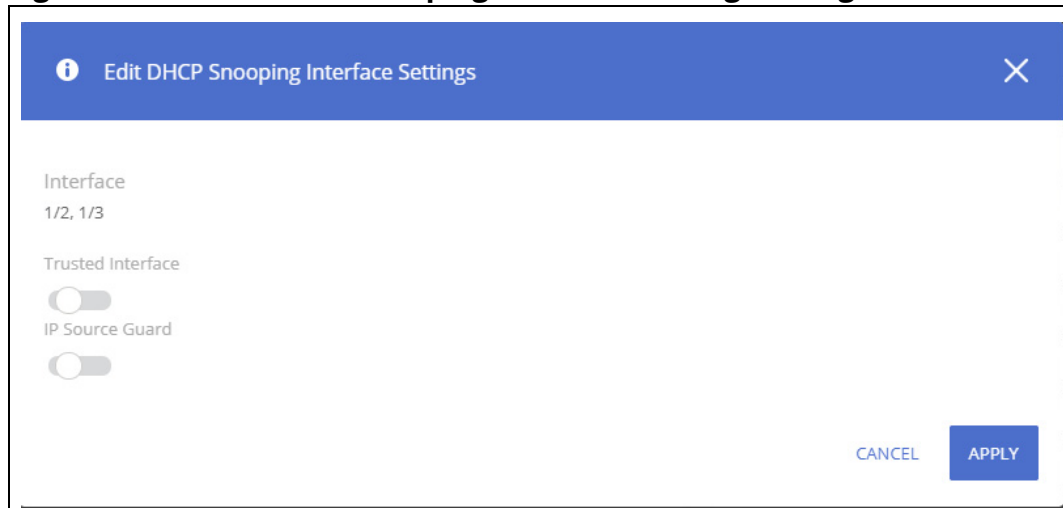


Table 178. Edit DHCP Snooping Interface Settings Fields

Field	Description
Interface	The interface(s) selected for editing.
Trusted Interface	Enable/disable as needed.
IP Source Guard	Enable/disable as needed.

Binding Database

Use the **Binding Database** setting tile to view the DHCP Snooping Binding table which show DHCP clients learned on untrusted ports.

Figure 211. Binding Database Tile

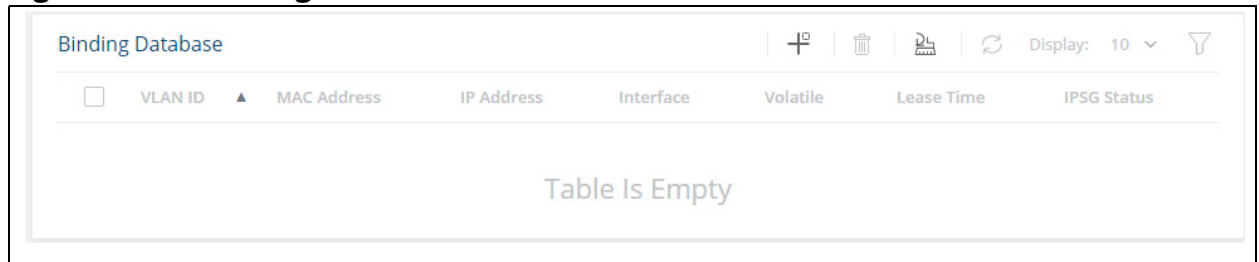


Table 179. Binding Database Fields

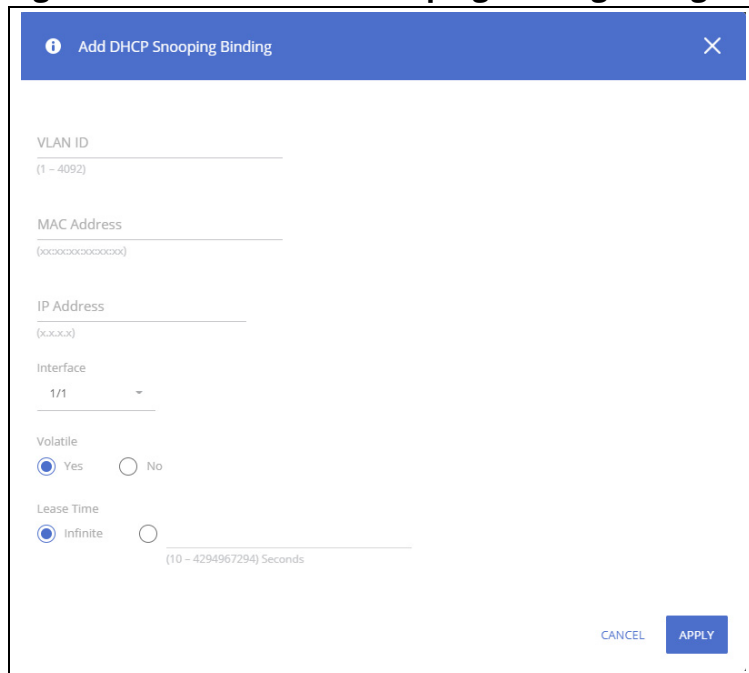
Field	Description
VLAN ID	The VLAN to which the DHCP client is connected
MAC Address	DHCP client Source MAC address.
IP Address	DHCP client IP address.
Interface	Switch interface to which the DHCP client is connected.
Volatile	Defines if the entry will be saved to device configuration file
Lease Time	DHCP address lease time. This may be configured for entries that are not volatile. Configure the entry lease-time or set it to infinite.
IPSG Status	The status of IP Source guard feature on this interface.

To remove a database, select it and click **Delete**  .

Click **Clear All**  to remove all entries in the database

To add a static DHCP binding database click **Add**  and enter the appropriate values for the binding database fields.

Figure 212. Add DHCP Snooping Binding Dialog Box



The dialog box titled "Add DHCP Snooping Binding" contains the following fields and controls:

- VLAN ID:** A text input field with a placeholder "(1 - 4092)".
- MAC Address:** A text input field with a placeholder "(xxxxxxxxxxxx)".
- IP Address:** A text input field with a placeholder "(xxxxx)".
- Interface:** A dropdown menu showing "1/1".
- Volatile:** Two radio buttons labeled "Yes" (selected) and "No".
- Lease Time:** Two radio buttons labeled "Infinite" (selected) and a text input field with a placeholder "(10 - 4294967294) Seconds".
- Buttons:** "CANCEL" and "APPLY" buttons at the bottom right.

ARP Attack Protection

ARP attack protection is a security feature that 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 interface:** The switch does not check ARP packets that are received on the trusted interface; it simply forwards the packets.
- **Untrusted interface.** ARP inspection is performed only on untrusted interfaces.

When a packet arrives on an untrusted interface the following logic is implemented:

If the VLAN that the packet arrived on has 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 <VLAN - IP address> pair.

- If the <VLAN - IP address> 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 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 213. Global Configuration Tile

Global Configuration

ARP Attack Protection

ARP Header Validation

ARP Protection Logging

ARP Protection Logging Interval

5

(0 – 86400) Seconds

Table 180. Global Configuration Fields

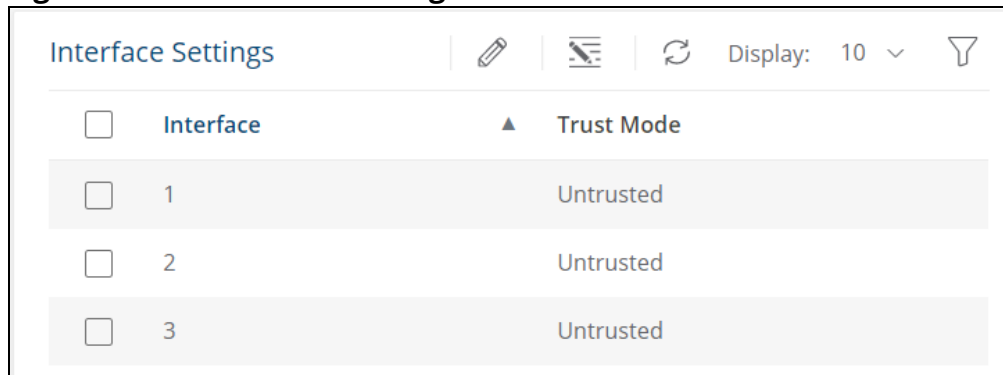
Field	Description
ARP Attack Protection	Enable or disable. By default, ARP Protection is disabled.
ARP Header Validation	Enabled or disable. By default, ARP Header Validation is disabled. • Disable - ARP header checks are not performed in addition to regular ARP protection validation. • Enable - ARP header checks are performed in addition to regular ARP protection validation.
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 seconds.

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 Settings

Use the **Interface Setting** tile to set the interface mode to Trusted or Untrusted:

Figure 214. Interface Settings Tile



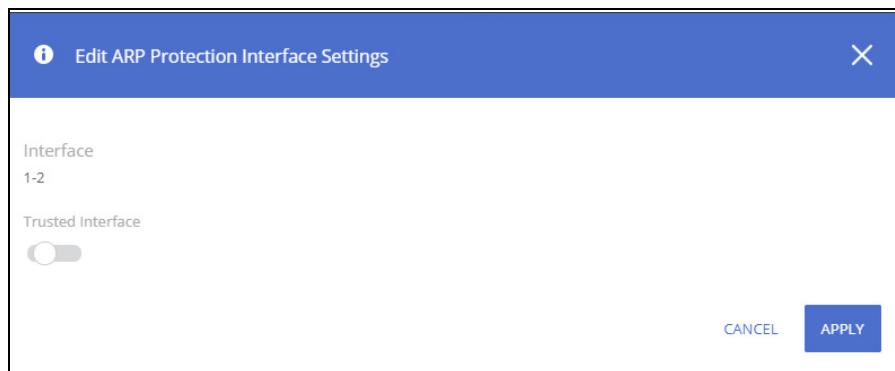
The screenshot shows a web interface titled "Interface Settings". At the top, there are icons for edit, list, and refresh, followed by a "Display: 10" dropdown and a filter icon. Below this is a table with two columns: "Interface" and "Trust Mode". The table contains three rows, each with a checkbox in the "Interface" column and the text "Untrusted" in the "Trust Mode" column. The rows are numbered 1, 2, and 3.

Interface	Trust Mode
☐ 1	Untrusted
☐ 2	Untrusted
☐ 3	Untrusted

Table 181. Interface Settings Fields

Field	Description
Interface	Identifier for the interface.
Trust Mode	Trusted or Untrusted. If Untrusted ARP Protection validation is performed on the interface

To change the trusted setting, select one or more interfaces and click **Edit** , or click **Edit All**  to configure all interfaces at the same time:



The screenshot shows a dialog box titled "Edit ARP Protection Interface Settings". It has a close button (X) in the top right corner. The dialog contains a section for "Interface 1-2" with a "Trusted Interface" toggle switch. The toggle switch is currently in the "off" position. At the bottom right of the dialog, there are two buttons: "CANCEL" and "APPLY".

ARP Access Control Rules

Use this tile to configure the ARP Access Controls rules. These rules are used for validation of ARP frames.

Figure 215. Access Control Rules Tile

ARP Access Control Rules

+ | | | Display: 10 |

☐ List Name ▲ IP Address MAC Address

Table Is Empty

Table 182. 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 an existing ARP Access Rule, click **Add** + and enter the values as required in the dialog box:

Figure 216. Add ARP Access Control Rule Dialog Box

Add ARP Access Control Rule

List Name
(1 - 32 characters)

IP Address
(x.x.x.x)

MAC Address
(xxxxxxxxxxxx)

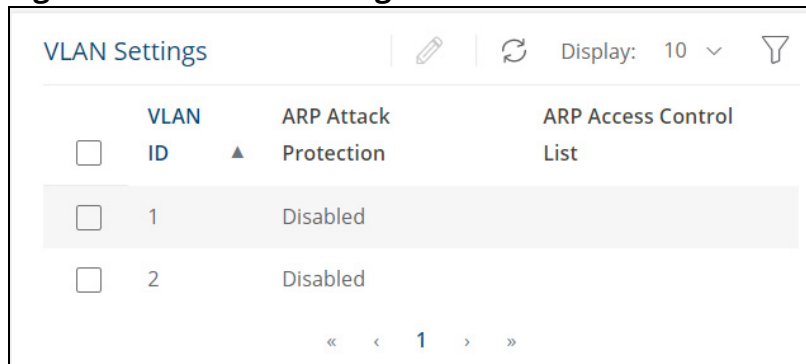
CANCEL APPLY

To remove a ARP Access Rule, select it and click **Delete** .

VLAN Settings

Use this tile to configure the enable or disable ARP protection on VLAN interfaces:

Figure 217. VLAN Settings Tile

A screenshot of the 'VLAN Settings' tile in a network management interface. The tile has a title bar with 'VLAN Settings', an edit icon, a refresh icon, and a 'Display: 10' dropdown. Below the title bar is a table with three columns: 'VLAN ID', 'ARP Attack Protection', and 'ARP Access Control List'. The table contains two rows: one for VLAN ID 1 with 'Disabled' protection and an empty list, and another for VLAN ID 2 with 'Disabled' protection and an empty list. At the bottom of the table are navigation arrows and a page number '1'.

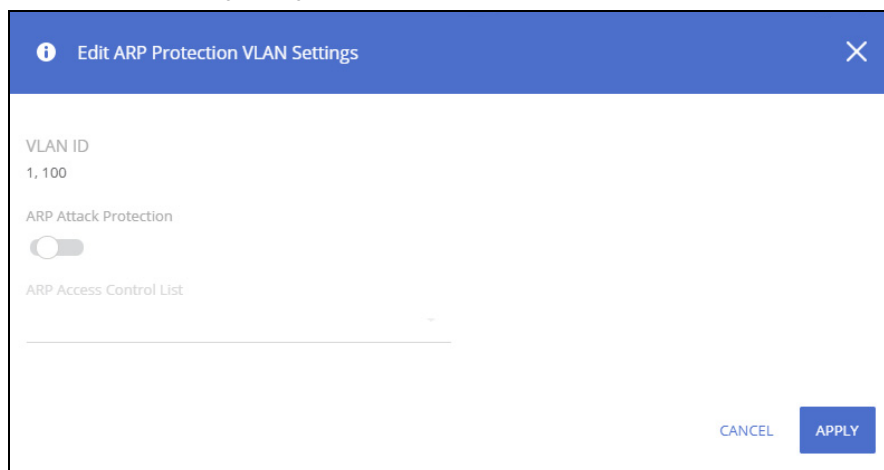
VLAN ID	ARP Attack Protection	ARP Access Control List
1	Disabled	
2	Disabled	

Table 183. 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

To edit one or more VLAN Settings entries, do the following:

1. Select the entry(ies) you wish to edit and click **Edit**  .

A screenshot of the 'Edit ARP Protection VLAN Settings' dialog box. The dialog has a blue header with an information icon, the title 'Edit ARP Protection VLAN Settings', and a close button. The main area contains three fields: 'VLAN ID' with a value of '1, 100', 'ARP Attack Protection' with a toggle switch currently turned off, and 'ARP Access Control List' with an empty text input field. At the bottom right are 'CANCEL' and 'APPLY' buttons.

Edit ARP Protection VLAN Settings

VLAN ID
1, 100

ARP Attack Protection
☐

ARP Access Control List

CANCEL APPLY

2. Enable or disable the ARP Attack Protection as needed.
3. If you enable ARP Attack Protection, you can also associate the protection with an ARP Access Control List.

Denial of Service Protection

The Aruba Instant On 1960 Switch Series switches include 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.



For some of the settings, the DoS feature does not generate notifications (such as error messages, SYSLOG messages, or SNMP traps) if a DoS attack occurs. The switch will simply drop DoS-related packets.

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 Global Settings tile, click **Security > Denial of Service Protection** in the navigation pane.

Global Settings

Figure 218. Global Settings

A screenshot of the 'Global Settings' configuration page for Denial of Service Protection. The page has a title 'Global Settings' at the top. Below it, there are several settings: 'Interface Level DoS Protection' with a toggle switch turned on; 'Block SYN-FIN Packets' with a toggle switch turned off; 'SYN Protection Mode' with three radio button options: 'Disabled', 'Log', and 'Log and Block' (which is selected); 'SYN Protection Threshold' with a numeric input field set to '80' and a range '(20 - 200) Packets per Second' below it; and 'SYN Protection Period' with a numeric input field set to '60' and a range '(10 - 600) Seconds' below it.

Global Settings

Interface Level DoS Protection

Block SYN-FIN Packets

SYN Protection Mode

☐ Disabled ☐ Log ☒ Log and Block

SYN Protection Threshold

80

(20 - 200) Packets per Second

SYN Protection Period

60

(10 - 600) Seconds

Table 184. Global Setting Fields

Field	Description
Interface Level DoS Protection	Enable this option to enable Interface level DoS settings (see SYN Attack Status Tab for more information). Interface level protection cannot be enabled if an Access Control List is attached to any switch interface.
Block SYN-FIN Packets	Enable this option to drop, on all interfaces, TCP packets in which both SYN and FIN flags are set.
SYN Protection Mode	Enables SYN Protection on the switch. SYN Protection detects TCP SYN traffic sent to the switch IP address(es) above the defined threshold and acts accordingly. Possible values are: • Disabled - SYN Protection is disabled on the switch. This is the default setting. • Log - SYN Protection is enabled on the switch. If the TCP SYN traffic rate on a certain interface is higher than the defined threshold, the violation is report through Syslog. • Log and Block - SYN Protection is enabled on the switch. If the TCP SYN traffic rate on a certain interface is higher than the defined threshold, the violation is reported through Syslog. In addition, all TCP SYN traffic on the interface is dropped for the specified duration.
SYN Protection Threshold	Defines The threshold applied to interface to activate SYN protection. Valid range is 20-200 Packets per second. Default is 80 Packets per second.
SYN Protection Period	The timeout (in seconds) after which an interface blocked by this feature gets unblocked. This setting is available only if SYN Protection mode is set to Log and Block. NOTE: If a SYN attack is still active on this interface it might become blocked again. Range is 10-600 seconds, default is 60 seconds.

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**.

Syn Attack Status/Interface Settings Tile

To view the SYN attack status, click the **SYN Attack Status** tab.

To view the Interface settings information, click the **Interface Settings** tab.

SYN Attack Status Tab

The SYN Attack Status tab displays the TCP SYN Protection status and last SYN attack on each interface.

Figure 219. SYN Attack Status Tab



Interface	Status	Last SYN Attack
1	Normal	
2	Normal	
3	Attacked	14-Dec-2021 07:07:16 Blocked and Logged
4	Normal	

Table 185. SYN Attack Status Fields

Field	Description
Interface	Interface identifier.
Status	Current status of the interface. Possible values are: • Normal - TCP SYN protection is not enabled or the interface is not under a TCP SYN attack. • Attacked - Interface is currently under a TCP SYN attack.
Last SYN Attack	The last time stamp in which the switch identified a SYN attack on this interface.

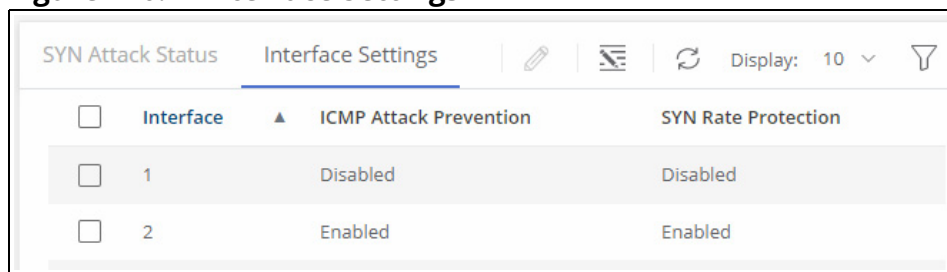
Interface Settings Tab

The Interface Settings tab enables configuring and provides information on the ICMP Attack Prevention and SYN Rate Protection settings for the interfaces.



The **Interface Setting** tab is enabled only if **Interface Level Dos Protection** state is enabled. Settings configured on interfaces are active only if the **Interface Level Dos Protection** setting is enabled.

Figure 220. Interface Settings



Interface	ICMP Attack Prevention	SYN Rate Protection
1	Disabled	Disabled
2	Enabled	Enabled

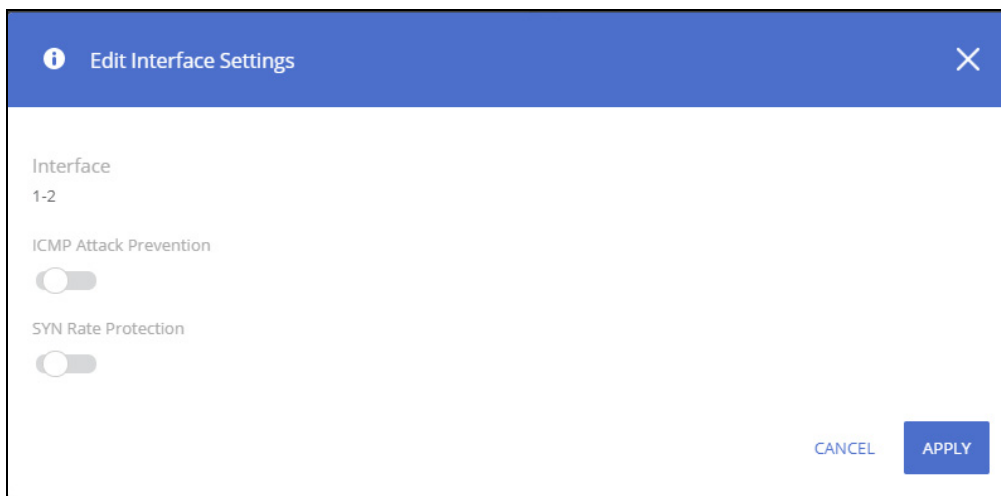
Table 186. Interface Settings Fields

Field	Description
Interface	Interface identifier.

Field	Description
ICMP Attack Prevention	Enabled or Disabled. If enabled, the interface will drop any ICMP request packet received on the interface. By default, ICMP Attack Prevention is disabled.
SYN Rate Protection	Enabled or Disabled. If enabled on an interface, this setting limits ingress TCP packets with the following flag settings to 250 packets per second: • SYN=1 • ACK=0 • FIN=0 Packets above the rate are dropped. By default Syn Rate Protection is disabled.

To change the setting for one or more interfaces, select it and click **Edit** . Or, click **Edit All**  to configure all interfaces at the same time.

The **Edit Interface Settings** dialog box appears. Set the **ICMP Attack Prevention** and the **SYN Rate Protection** as required, and click **APPLY**.



The dialog box titled "Edit Interface Settings" has a blue header bar with an information icon and a close button. Below the header, the "Interface" is listed as "1-2". There are two settings, each with a toggle switch: "ICMP Attack Prevention" and "SYN Rate Protection". Both toggle switches are currently in the "off" position. At the bottom right, there are two buttons: "CANCEL" and "APPLY".

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 a 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 importing of the signed certificate for use by the switch for HTTPS sessions.

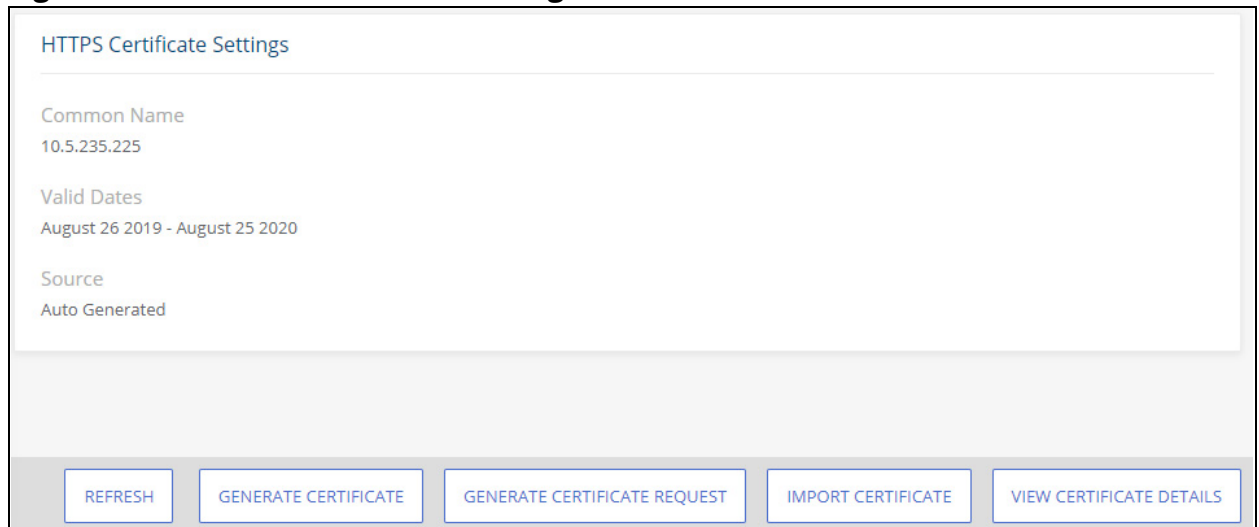
In order to enable users to benefit from a secured connectivity, without the need to sign a certificate by a CA - the switch also supports use of unsigned certificates (also known as self-signed certificates). While not useful for proving switch identity to the browser, the self-signed certificates enable 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.

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.

Figure 221. HTTPS Certificate Settings Tile



HTTPS Certificate Settings

Common Name
10.5.235.225

Valid Dates
August 26 2019 - August 25 2020

Source
Auto Generated

REFRESH GENERATE CERTIFICATE GENERATE CERTIFICATE REQUEST IMPORT CERTIFICATE VIEW CERTIFICATE DETAILS

Table 187. 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.
Source	Specifies whether the certificate was generated by the system (auto generated) or by the user (self defined).

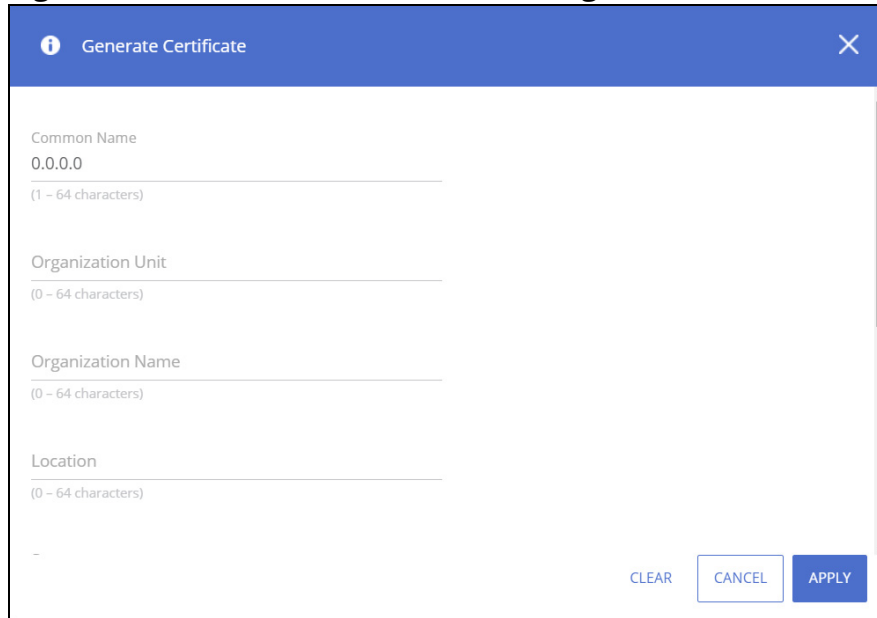
Use the buttons at the bottom of the page to perform actions relating to HTTPS certification:

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 222. Generate Certificate Dialog Box

The image shows a 'Generate Certificate' dialog box with a blue header bar containing an information icon and a close button. The main area has four text input fields: 'Common Name' (with '0.0.0.0' entered and '(1 - 64 characters)' below), 'Organization Unit' (with '(0 - 64 characters)' below), 'Organization Name' (with '(0 - 64 characters)' below), and 'Location' (with '(0 - 64 characters)' below). At the bottom right are three buttons: 'CLEAR', 'CANCEL', and 'APPLY'.

Enter the following fields:

Table 188. 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.
Duration	Enter the number of days that the certificate is valid. If unspecified, the duration is set to 365 days (1 year).

Field	Description
Regenerate RSA Key	Enable this feature to regenerate a pair of RSA keys. If disabled, the existing key set is used.
RSA Key Length	Select the preferred key length. By default, key length is 2048.

Using a Certificate Signed by a Certificate Authority

In order to use a certificate that is signed by a Certificate Authority (CA), you need to complete the following steps:

1. Generate a certificate request: Click **GENERATE CERTIFICATE REQUEST** and enter the fields as defined in [Generate a Self-Signed Certificate](#).



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

2. Export the certificate for signing: In 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 (see [Import Certificate Dialog Box](#)).
 - 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 223. Import Certificate Dialog Box

Import Certificate

Certificate

QA0N4KOva0Hmdhp8xDtWuXo6Buuuy/p0Nrd/IRgQtjRrkQRJ1GRKZA2DV55K8D/m
GppgYwJlQdsFgn6iaHfZ98vj77cLAdFn+jQ7xxYdHNC4JwOu1wo64rwZhYyYD04v
teWK/Xb5BnX8IA2wMFuOhmUT81IZx8922RLIWobTIE3EwpOmLW2UZFC752TPylya
4NnPBOq0jsyQPK4g17wTZ/MG0r9jNNUzH9GJUu896jo1mkvtABRs
-----END CERTIFICATE-----

Import RSA Keys

☒

Public Key

6GyM6Al/fhZ1JFcnTZWc6kpOw+JxVhTZsMQ5+Z4ZmNWZlJflbPcrALgeTtyqtOVKMIZiCm
L2f+WRlKCAh8TI/OgA1rwRULKCBryNDGvTOTH8ujzPhLzeCGk6oumC1NrFgCqmtRjkNO
DagQIDAQAB
-----END RSA PUBLIC KEY-----

Private Key

PVcg/1+xE3lgB8vv53nKrJwPZglwCE+t94e9xEggwGTfUFkpYR/7wmEN5X4p9I6e7pUfCK
R70FGTXEFvExAoGAbqw7uD+4eQabNWapt3AHk3bkFsIVN7FuBlZJ36Cd1jYCBwzZp11kx1
VbEk7e1TfOraV/J9P350awniv1TySHibPxvDd1X7g+OVM1xYMh0kCaTRHqT+D/qn513QsM
kinDV5GkeMa2IdAnGJeWu5xpG/SUcd5hf5P8aQ43YH25XkA=
-----END RSA PRIVATE KEY-----

CANCEL APPLY

Table 189. Import Certificate Fields

Field	Description
Certificate	Paste the signed certificate into this text box.
Import RSA Keys	Enable if you need to import RSA keys.
Public Key	If Import RSA Keys is enabled, paste the public key to this text box.
Private Key	If Import RSA Keys is enabled, paste the private key to this text box.

View a Certificate

To view the current certificate details, click the **VIEW CERTIFICATE DETAILS** button.

Figure 224. Certificate Details

Certificate Details

×

Certificate

-----BEGIN CERTIFICATE-----

MIIDITCCAqkCEE/C42KlvGFy1h7U0tIO2L4wDQYJKoZIhvcNAQELBQAwTzELMAkG
A1UEBhMCICAxCjAIBgNVBAGMASAxCjAIBgNVBACMASAxEDAQOBgNVBAMMBzAuMC4w
LjAxCjAIBgNVBAoMASAxCjAIBgNVBAsMASAwHhcNMTkxMjAyMDEzMTU2WhcNMjAx
MjAxMDEzMTU2WjBPMQswCQYDVQGEwlgIDEKMAgGA1UECAwBIDEKMAgGA1UEBwwB

Public Key

-----BEGIN RSA PUBLIC KEY-----

MIIBCgKCAQEAzE82ZcB/a0YaLnGWN8NbavFbpSpqebYrYMjqlvQ62J3A/nIYVK/sEdGtCEgiSjrCzXmo0Crc
N+q/Ok7hyRWcKmVLxjEHrLRBFZXgTZmMBHk4GfXs3vCb9aBBFPkCPFQby1aBPxh+HrCNK9/irvDOJZU
5EglP7wGe/6m24hh1QQDrDgDgKPTGHgCQ2w141YNmAiEegn3fYoZjkyLRqkrpfuVgR8/K1a3z8us1Wpr
R4LMNIOAqPDPI3LtjueJe/vlR3pVH/49wrlO/yrn6Bomwh/Y3JnHuO8jdbGSd53QnFBgVSuroov7dHWKtV

Private Key

-----BEGIN RSA PRIVATE KEY-----

MIIEpAIBAAKCAQEAzE82ZcB/a0YaLnGWN8NbavFbpSpqebYrYMjqlvQ62J3A/nIYVK/sEdGtCEgiSjrCzXmo
0CrcN+q/Ok7hyRWcKmVLxjEHrLRBFZXgTZmMBHk4GfXs3vCb9aBBFPkCPFQby1aBPxh+HrCNK9/irvD
OJZU5EglP7wGe/6m24hh1QQDrDgDgKPTGHgCQ2w141YNmAiEegn3fYoZjkyLRqkrpfuVgR8/K1a3z8us1
WprR4LMNIOAqPDPI3LtjueJe/vlR3pVH/49wrlO/yrn6Bomwh/Y3JnHuO8jdbGSd53QnFBgVSuroov7dH

Fingerprint

52:DD:41:26:51:37:7B:81:10:B8:68:13:25:33:70:E7:9B:16:F1:98

CLOSE

Table 190. Certificate Details Fields

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

You can use the Diagnostics pages to help troubleshoot network issues, view log and configuration information.

Logging

To configure log setting and display the Logging page, click **Diagnostics** > **Logging** in the navigation pane.

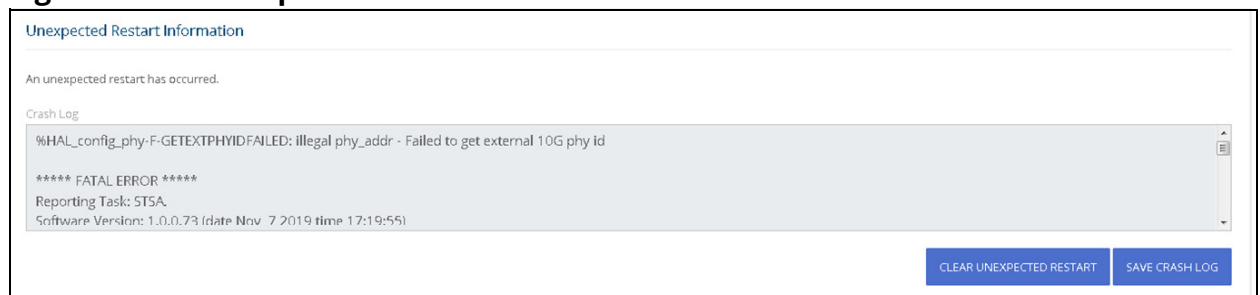
Unexpected Restart Information

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. When this notification icon is clicked, the application navigates 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 (see [Log File](#) for more information). The file stored into non-volatile memory so that it is preserved upon reboot.

When the switch is reset to factory defaults, all crash log information is erased.

Figure 225. Unexpected Restart Information Tile

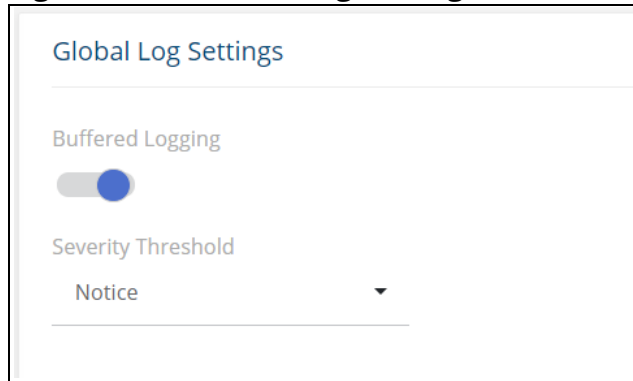


To clear the unexpected restart alert, click **Clear Unexpected Restart** this clears the unexpected restart notification from the masthead, and the **Unexpected Restart Information** tile. You can click **Save Crash Log** to save the contents of the crash log to a text file using the browser save functionality.

Global Log Settings

Use this tile to define buffered logging settings. These log messages are not preserved across device reboots.

Figure 226. Global Log Settings



Global Log Settings

Buffered Logging

Severity Threshold

Notice

Table 191. 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 that severity and all higher severity.

Remote Log Server

Use this tile to enable logging messages to a remote SYSLOG server, and to define the server address and other settings.

Figure 227. Remote Log Server

Remote Log Server

Syslog Host

☒

Server Address

(IPv4 or IPv6)

UDP Port

514

(1 - 65535)

Severity Threshold

Warning

Table 192. 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: - 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%<ID> - Hostname - specify the server 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. See descriptions for the available levels in Global Log Settings Fields

Buffered Log/Log File

To view the Buffered Log information, click the **Buffered Log** tab.

To view the Log File information, click the **Log File** tab.

Buffered Log

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 200 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.



If more than 1000 logs accumulate, their Log Index numbers continue to increment beyond 1000 and the oldest entries are deleted (for example, if 1400 log entries were generated since the system was last restarted or the log file was cleared, then the log file would display entries 1001 to 1400).

To view this tab, click **Diagnostics > Logging** in the navigation pane, and click the **Log File** tab in the **Buffered Log/Log File** Tile.

Figure 228. Buffered Log Tab

Buffered Log		Log File				
Index ▲	Log Time	Severity	Component	Description		
1	Oct 7 2021 01:08:25	Notice	SYSLOG-N-LOGGING	Logging started.		
2	Oct 7 2021 01:08:13	Info	BOOTP_DHCP_CL-I- DHCPCONFIGURED	The device has been configured on interface Vlan 1 , IP 10.5.227.151, mask 255.255.255.224, DHCP server 10.5.227.131		

Table 193. Buffered Log Tab Fields

Field	Description
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: • Emergency—The switch is unusable. • Alert—Action must be taken immediately. • Critical—The switch is experiencing primary system failures. • Error—The switch is experiencing non-urgent failures. • Warning—The switch is experiencing conditions that require user attention. • Notice—The switch is experiencing normal but significant conditions. • Info—The switch is providing non-critical information. • Debug—The switch is providing debug-level information.
Component	The system component that issued the log entry.
Description	A text description of the event.

Click **Clear**  to delete all log messages. You may be required to confirm the delete before the logs are removed.

For information on configuring log settings, see [Global Log Settings](#).

Log File

The system sends logging messages to the local flash (Log file). When using this feature, all events with error level and higher are logged to a flash Log file and will be available for viewing even after system reboot.

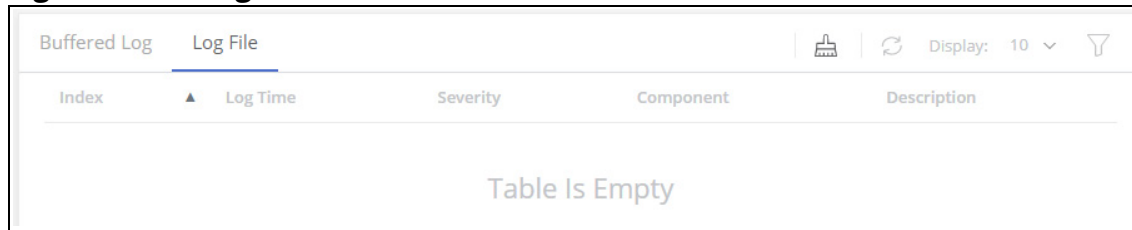
When the log file reaches the maximum size, the oldest message is deleted from the flash when a new message is added.



If more than 200 logs accumulate in flash, their Log Index numbers continue to increment beyond 200 and the oldest entries are deleted (for example, if 400 log entries were generated since log file was cleared, then the log file would display entries 201 to 400).

To view this tab, click **Diagnostics > Logging** in the navigation pane, and click the **Log File** tab in the **Buffered Log/Log File** Tile.

Figure 229. Log File Tab



Index	Log Time	Severity	Component	Description
Table Is Empty				

Table 194. Log File Tab Fields

Field	Description
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: - Emergency—The switch is unusable. - Alert—Action must be taken immediately. - Critical—The switch is experiencing primary system failures. - Error—The switch is experiencing non-urgent failures. - Warning—The switch is experiencing conditions that require user attention. - Notice—The switch is experiencing normal but significant conditions. - Info—The switch is providing non-critical information. - Debug—The switch is providing debug-level information.
Component	The system component that issued the log entry.
Description	A text description of the event.

Click **Clear**  to delete all log messages. You may be required to confirm the delete before the logs are removed.

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.

IPv4/IPv6

To view the IPv4 information, click the **IPv4** tab.

To view the IPv6 information, 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.

To display the IPv4 tab, click **Diagnostics > Ping** in the navigation pane, and ensure the **IPv4** tab is selected.

Figure 230. IPv4 Tab

The screenshot shows the IPv4 configuration tab. At the top, there are two tabs: 'IPv4' (selected) and 'IPv6'. Below the tabs, the configuration fields are as follows:

- IP Address:** A text input field with the placeholder '(x.x.x.x)'.
- Count:** A text input field with the value '3' and a range '(1 - 15)' below it.
- Interval:** A text input field with the value '3' and a range '(1 - 60) Seconds' below it.
- Size:** A text input field with the value '64' and a range '(64 - 1518) Bytes' below it.
- Source:** Three radio buttons: 'None' (selected), 'IP Address', and 'Interface'.
- Source IP Address:** A text input field with the placeholder '(x.x.x.x)'.

Table 195. 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. The range is from 0 to 1518 bytes, and the default is 64 bytes.
Source	The source IP address or interface to use when sending a ping request 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 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 **APPLY** 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 IPv4 page.

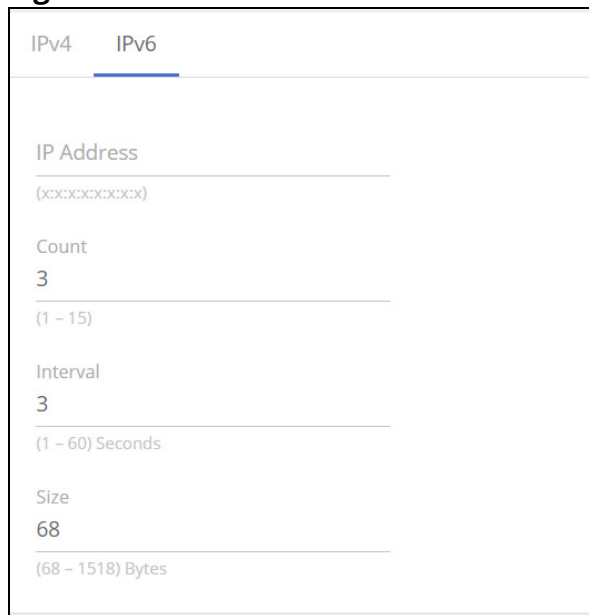
The results of the ping operation can be viewed in the [Ping Results](#) tile.

IPv6 Tab

Use the Ping IPv6 tab 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 IPv6 network. The information you enter on this page is not saved as part of the switch configuration.

To display the Ping IPv6 tab, click **Diagnostics > Ping** in the navigation pane, and then click the **IPv6** tab.

Figure 231. IPv6 Tab



The screenshot shows the IPv6 Tab interface. At the top, there are two tabs: 'IPv4' and 'IPv6', with 'IPv6' being the active tab. Below the tabs, there are four input fields: 'IP Address' with a placeholder '(xxxxxxxxxx)', 'Count' with a value of '3' and a range '(1 - 15)', 'Interval' with a value of '3' and a range '(1 - 60) Seconds', and 'Size' with a value of '68' and a range '(68 - 1518) Bytes'.

Table 196. IPv6 Fields

Field	Description
IP 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. The range is from 68 to 1518 bytes, and the default is 68 bytes.

Click **APPLY** 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 IPv4 page.

The results of the ping operation can be viewed in the [Ping Results](#) tile.

Ping Results

This tile shows the Ping status and results.

Table 197. 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.

IPv4/IPv6

To view the IPv4 information, click the **IPv4** tab.

To view the IPv6 information, 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.

To display the Traceroute IPv4 tab, click **Diagnostics > Traceroute** in the navigation pane, and ensure the **IPv4** tab is selected.

Figure 232. IPv4 Tab

IPv4

IPv6

IP Address

(x.x.x.x)

Probes Per Hop

3

(1 - 10)

Max TTL

30

(1 - 255)

Interval

3

(1 - 60) Seconds

Size

64

(64 - 1518) Bytes

Source

☒ None ☐ IP Address ☐ Interface

Table 198. 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.
Max TTL	The maximum 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 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 and **Stop Traceroute** to end a traceroute in progress.

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.

To display the Traceroute IPv6 tab, click **Diagnostics > Traceroute** in the navigation pane, and click the **IPv6** tab.

Figure 233. IPv6 Tab

The screenshot shows the IPv6 Traceroute configuration interface. At the top, there are two tabs: 'IPv4' and 'IPv6', with 'IPv6' being the active tab. Below the tabs, there are several input fields with their respective labels and ranges:

- IP Address:** A text input field with a placeholder '(xxxx:xxxx:xxxx:xxxx)'.
- Probes Per Hop:** A text input field with the value '3' and a range '(1 - 10)' below it.
- Max TTL:** A text input field with the value '30' and a range '(1 - 255)' below it.
- Interval:** A text input field with the value '3' and a range '(1 - 60) Seconds' below it.
- Size:** A text input field with the value '68' and a range '(68 - 1518) Bytes' below it.

Table 199. IPv6 Fields

Field	Description
IP 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 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.

Field	Description
Interval	The number of Seconds to wait between sending probes.
Size	The size of probe payload in bytes.

Click **APPLY** to send the traceroute to the specified host and **Stop Traceroute** to end a traceroute in progress.

Traceroute Results

Table 200. Traceroute Results Fields

Field	Description
Status	The current status of the traceroute, which can be: • Not Started – The traceroute has not been initiated since viewing the page. • In Progress – The traceroute has been initiated and is running. • Done – The traceroute has completed, and information about the traceroute is displayed in the Results area.
Results	The results of the traceroute are displayed.

Support File

Use the support file page to display summary information for the switch on a single page.

To display the Support File page, click **Diagnostics > Support File** in the navigation pane and click the **GENERATE SUPPORT INFORMATION** button. The **Support File Page** shows a partial view of the resulting information.



Generating the support file may take several minutes. During this time switch management will not be available.

Figure 234. Support File Page

The screenshot shows a web interface titled "Support File". At the top, there are two blue buttons: "GENERATE SUPPORT INFORMATION" and "DOWNLOAD AS TEXT". Below these buttons, the page is divided into two main sections. The first section, "System Information", contains three rows of data: "System Name" with the value "SwitchA", "System Location" with the value "AIO", and "System Contact" with the value "Admin". The second section, "System Time", contains two rows of data: "Current Time" with the value "11:00:30 January 03 2022" and "System Up Time" with the value "0 days, 20 hours, 46 minutes 31 seconds".

Support File	
GENERATE SUPPORT INFORMATION DOWNLOAD AS TEXT	
System Information	
System Name	SwitchA
System Location	AIO
System Contact	Admin
System Time	
Current Time	11:00:30 January 03 2022
System Up Time	0 days, 20 hours, 46 minutes 31 seconds

The support file page 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— SNTP 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 and 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 and 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 feature and recovery time
- VLAN Configuration —Configured VLANs, VLAN port membership, and VLAN port configuration.
- Auto Voice VLAN Configuration —Voice VLAN settings.
- Trunk Configuration and Trunk Statistics—Trunk configuration details and flap count statistics
- LLDP and LLDP-MED Configuration—Global settings and per-port LLDP configuration and activity
- Routing IP—Routing IP configuration, interface configuration, statistics, and IP route summary.
- DHCP Relay— Configuration and statistics.
- ARP Table—Summary, 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 management system using the native browser file system. The name of the downloaded file is SupportFile.htm.

To download the support file, click the **DOWNLOAD AS TEXT** button. This button is only displayed after the support information is gathered and shown in the screen.

Cable Test

This feature detects and reports potential cabling issues, such as cable opens, or cable shorts, on Copper Links. This feature also it provides distance to the fault if exists, and total length of cable.

Cable length measurement is available when link is up. Length is automatically detected. Length reports has a minimum Length of 50Meter and is provided with a 30 meter resolution (up to 50, 50 to 80, 80 to 110 etc)



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.

To display the Cable Test page, click **Diagnostics > Cable Test** in the navigation pane.

Interface Configuration

This tile shows the interface configuration of the cables. To run a test, select one or more interfaces and click the **Test**  button.

Figure 235. Interface Configuration

Interface Configuration				
☐	Interface	 Test Result	Distance to Fault	Last Update
☐	1			14-Dec-2021 07:43:30
☐	2			
☐	3	Ok		14-Dec-2021 07:43:31
☐	4			
☐	5	No Cable		14-Dec-2021 07:38:34
☐	6	No Cable		14-Dec-2021 07:38:42
☐	7	Short	11m	14-Dec-2021 07:38:50

Table 201. Interface Configuration 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: • Ok • No cable is connected • Open cable • Shorted cable • Unknown
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. The last time a test was activated on this interface.
Cable Length	Length reports has a minimum Length of 50Meter and provides a 30 meter resolution (up to 50, 50 to 80, 80 to 110, and so on) NOTE: Cable length info is not available for interfaces running in speeds lower than 1 Gbps.
Port Status	Displays the current port status.



Cable status test requires activation, per-interface by user. 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

This tile shows the MAC table global configuration. To configure a setting select it, enter the new configuration and click **APPLY**.

Figure 236. Global Configuration

Global Configuration

Maximum Addresses Supported

16384

MAC Address Aging Interval

300

(10 – 400) Seconds

Table 202. 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

Figure 237. MAC Address Table Tile

MAC Address Table					
VLAN ID	MAC Address	Interface	Interface Index	Status	
1	00:00:00:11:11:11	47	47	Learned	
1	00:00:44:44:55:88	CPU	0	Management	
1	00:22:12:52:03:77	47	47	Learned	

Table 203. MAC Address Table Fields

Field	Description
VLAN ID	The VLAN 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. <i>CPU</i> 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.

Field	Description
Status	Provides information about the entry and why it is in the table. Possible values are the following: • 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. • Other—The address was added dynamically through an unidentified protocol or method.

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)

Each group is detailed below.

RMON Statistics

The RMON (Ethernet) statistics are 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 238. RMON Statistics

RMON Statistics						
	Interface	▲ Bytes Received	Frames	Packets Received	Drop Events	Errors
☐	1	67388	1005459	485	0	0
☐	2	3353	1005001	26	0	0
☐	3	135441940	1005130	1005102	0	0

Table 204. 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.

Select an interface and click **Details**  to see a breakdown of the various types of frames by frame size, and error frames by error type.

Table 205. 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)

Field	Description
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).
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).

Select an interface and click **Clear**  to clear the RMON and interface statistics from the selected interface. Click **Clear All**  to clear the RMON and interface statistics from the all the interfaces.

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. Select the History Collector ID to view from the **History Collector ID** drop down box. Only Collector IDs that were defined in the History Collector tab are available.

Figure 239. History Collectors Tab

History Collectors

History Log

+

✎

🗑

↺

Display: 10 ▾

🔍

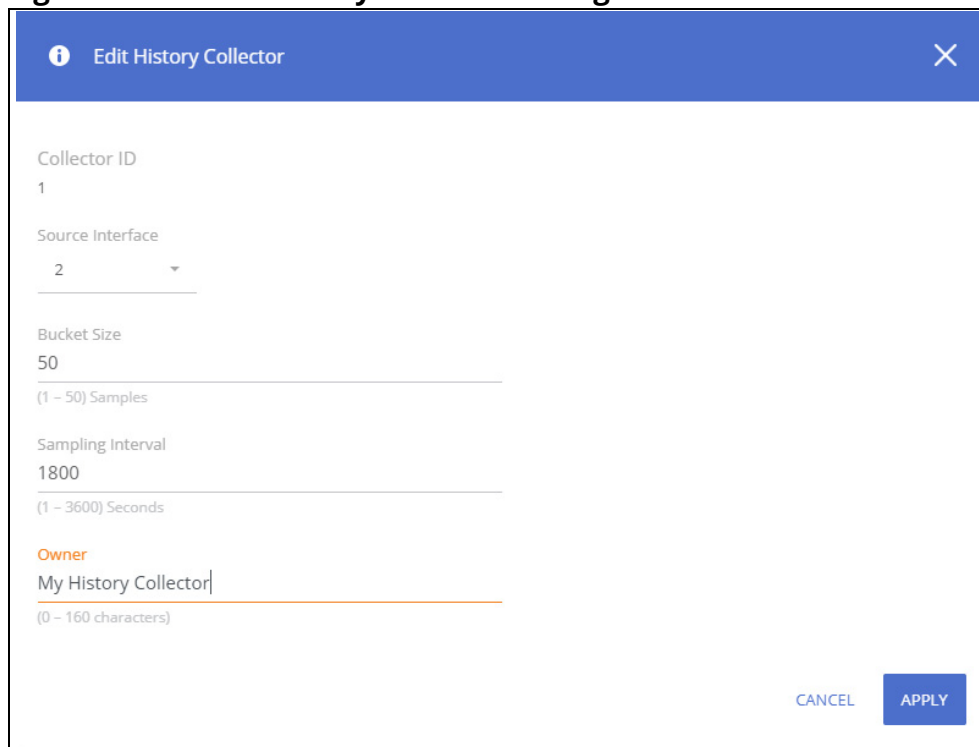
☐	Entry ID	▲	Source Interface	Bucket Size	Sampling Interval	Owner	Samples Logged
Table Is Empty							

Table 206. 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, click **Add** . The **Add History Collector** dialog box appears:

Figure 240. Edit History Collector Dialog Box



Edit History Collector

Collector ID
1

Source Interface
2

Bucket Size
50
(1 - 50) Samples

Sampling Interval
1800
(1 - 3600) Seconds

Owner
My History Collector
(0 - 160 characters)

CANCEL APPLY

Enter the appropriate fields as needed.

To edit an existing collector, click the check box to the left of the collector entry and click **Edit** . The **Edit History Collector** dialog box appears.

To remove an existing collector, click the check box to the left of the collector entry and click **Remove**



History Log

Use the History Log tab to view the information itself (based on the definition in the **History Collector** tab).

For more information on the log types, see [RMON Statistics](#).

Figure 241. History Log Tab

History Collectors		History Log											
		History Collector ID 1											
Sample Number	▲	Drops	Rx Bytes	Rx Packets	Broadcast Packets	Multicast Packets	CRC Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Utilization
42		0	0	0	0	0	0	0	0	0	0	0	0%
43		0	0	0	0	0	0	0	0	0	0	0	0%
44		0	0	0	0	0	0	0	0	0	0	0	0%

Table 207. 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.

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

Use the RMON Events tab to configure ID and settings of events (RMON Events).

Figure 242. RMON Events

RMON Events

Event Log

Display: 10

☐	Entry ID	▲	Description	Community	Owner	Log Event	Trap	Last Occurrence
--------------------------	----------	---	-------------	-----------	-------	-----------	------	-----------------

Table Is Empty

Table 208. 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.
Log Event	Enable or disable logging events. If set to enable, adds an entry to the RMON Event Log table when an alarm is triggered.
Trap	Enable or disable setting a trap. If set to enable, sends a trap to the remote log server and SNMP Manager when an alarm is triggered.
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:


Add RMON Event

×

Event ID
1
(1 – 65535)

Description
new RMON Event
(0 – 127 characters)

Community
2
(0 – 127 characters)

Owner
My Event
(0 – 160 characters)

Log Event
☒

Trap
☒

CANCEL

APPLY

Enter the appropriate fields as needed.

To edit an existing event, click the check box to the left of the event entry and click **Edit**  . The **Edit RMON Event** dialog box appears.

To remove an existing event, click the check box to the left of the event entry and click **Remove**  .

Event Log

Use the Event Log tab to view the event log. The Event Log displays the log of RMON events (actions) that were triggered (occurred).

Figure 243. RMON Event Log

RMON Events		Event Log			 Display: 10  	
Event ID ▲	Log ID	Log Time	Description			
1	2	Dec 11 2019 19:34:58	MIB Var.: 1.3.6.1.2.1.2.2.1.10.48 , Absolute , Rising , Actual Val: 66855353 , Thresh.Set:			
1	5	Dec 11 2019 19:43:23	MIB Var.: 1.3.6.1.2.1.2.2.1.16.48 , Absolute , Rising , Actual Val: 54945670 , Thresh.Set:			

Table 209. RMON 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

The Alarms group provides 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 244. RMON Alarms

RMON Alarms

Display: 10

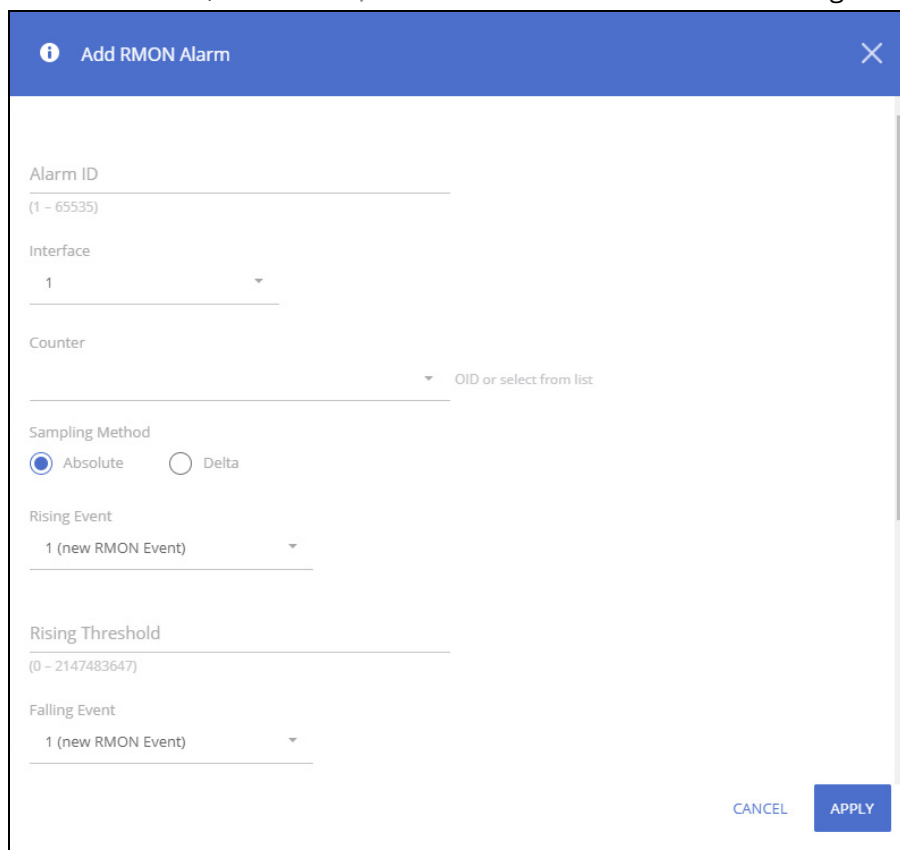
☐	Alarm ID ▲	Interface	Counter	Sampling Method	Current Value	Rising Threshold	Rising Event	Falling Threshold
Table Is Empty								

Table 210. 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. Range: 0-65535 - Only created events are available for selection.
Falling Threshold	Specifies the value which triggers the falling event. Range: 0-2147483647

Field	Description
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. Range: 1-65535 - Only created events are available for selection.
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 Event, click **Add**  . The **Add/Edit RMON Alarm** dialog box appears:



The dialog box titled "Add RMON Alarm" contains the following fields and controls:

- Alarm ID**: A text input field with a range of (1 - 65535).
- Interface**: A dropdown menu currently showing "1".
- Counter**: A dropdown menu with the text "OID or select from list" to its right.
- Sampling Method**: Two radio buttons, "Absolute" (selected) and "Delta".
- Rising Event**: A dropdown menu currently showing "1 (new RMON Event)".
- Rising Threshold**: A text input field with a range of (0 - 2147483647).
- Falling Event**: A dropdown menu currently showing "1 (new RMON Event)".
- Buttons**: "CANCEL" and "APPLY" buttons at the bottom right.

Enter the appropriate fields as needed.

To edit an existing alarm, click the check box to the left of the event entry and click **Edit**  . The **Add/Edit RMON Alarm** dialog box appears.

To remove an existing alarm, click the check box to the left of the alarm entry and click **Remove**  .

You can use the maintenance pages to upgrade software, save the switch configuration, and select which of two software images is the active image and which is the backup image.

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 245. Dual Image Configuration Page

The screenshot shows the 'Dual Image Configuration' page. It contains the following fields and options:

- Active Image Version:** 2.5.0
- Active Image Description:** (0 – 60 characters)
- Backup Image Version:** 2.5.0
- Backup Image Description:** (0 – 60 characters)
- Next Active Image:** Two radio buttons are shown: 'Active (2.5.0)' (which is selected) and 'Backup (2.5.0)'.

Table 211. 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.

Field	Description
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 save a backup of the switch's image, configuration files or error log (transfer a file from the switch), or update the switch firmware and configuration files (transfer a file to the switch), from a remote system.

Files can be backed up and updated using HTTP, TFTP, or SCP protocols.

Secure Copy Protocol (SCP) Usage

Secure Copy Protocol (SCP) is a protocol which 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. You need to use the **Next** > and **Back** < buttons to complete the various fields and start the transfer process. These are the steps for filling in the backup or update operation:

1. Select the Operation Type and then click **Next** >
 - o 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.
 - o Select **Backup** to save a backup of the current image, configuration file or error log (transfer a file from the switch).

Figure 246. Select Backup or Update

2. Select the **File Type** and then click **Next** .

These are the available file types:

File Type	Description	Available for Operation Type
Active Image	Select this option to backup/copy the active image file. The active image file is the one running currently on the switch.	Backup only
Backup Image	Select this option to transfer a new image to the switch. The code file is stored as the backup image. After updating the backup image, you can use the Dual Image Configuration page to make it the active image upon the next reboot. NOTE: You cannot directly update the active image.	Update and Backup
Startup Configuration	Select this option to update or backup the stored configuration file. In case of startup configuration update, if the copy operation resulted in an error (for example wrong configuration lines), the update is stopped.	Update and Backup
Running Configuration	Select this option to back up the running configuration file.	Backup only
Backup Configuration	Select this option to update or backup the stored backup configuration file. The backup configuration file is stored on the switch for future reference. It is not active unless copied to the running configuration.	Update only
Error Log	Select this option to backup the switch log file. The log file is the file on flash. It stores syslog messages, from level error and higher.	Backup only

3. Select the Transfer Protocol, and then click **Next** .

These are the available protocols:

- o HTTP - this protocol does not require any additional fields
- o TFTP - this protocol requires the Server Address and File Name
- o SCP - this protocol requires the Server Address, Username, Password, and File Name

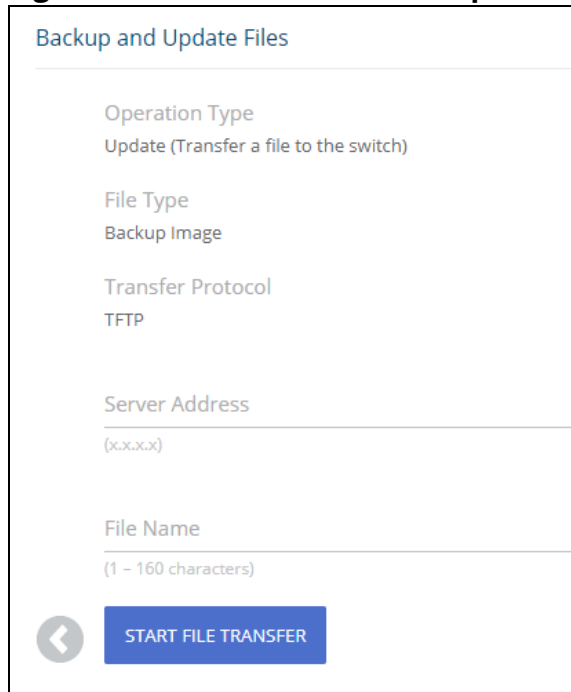
4. Enter any additional fields as required.

Field	Description
Server Address	(TFTP/SCP only) Enter the IP address of the TFTP/SCP server to use for file transfer (Update or Backup).
File Name	(TFTP/SCP only) 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 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: \\, /, :, *, ?, ", <, >,
Username	For SCP transfer, if the server requires authentication, specify the user name for remote login to the server that will receive the file.
Password	For SCP transfer, if the server requires authentication, specify the password for remote login to the server that will receive the file.

5. Click **START FILE TRANSFER** to start the transfer. For a TFTP or SFTP backup, the switch begins the

transfer to the specified location. For an HTTP update, browse to the location on your management station where the file you want to update to switch is located.
For HTTP backup - the file will be saved to the download folder specified by the browser.

Figure 247. File Transfer Example - TFTP Protocol



The screenshot shows a web interface titled "Backup and Update Files". It contains several configuration fields:

- Operation Type:** A dropdown menu with "Update (Transfer a file to the switch)" selected.
- File Type:** A dropdown menu with "Backup Image" selected.
- Transfer Protocol:** A dropdown menu with "TFTP" selected.
- Server Address:** A text input field with the placeholder "(x.x.x.x)".
- File Name:** A text input field with the placeholder "(1 - 160 characters)".

At the bottom left is a back arrow icon, and at the bottom right is a blue button labeled "START FILE TRANSFER".

Configuration File Operations

Use this 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 248. Configuration Files Operations Page

Configuration File Operations

Source File

Running Configuration ▼

Destination File

Startup Configuration ▼

Table 212. Configuration Files 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.
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

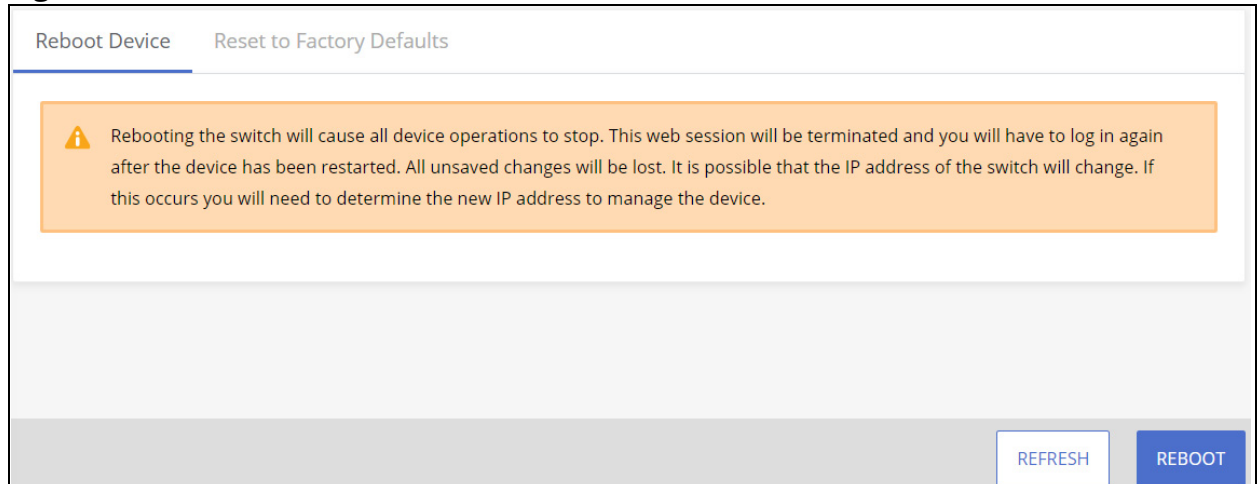
This page enables Rebooting the switch or Resetting to Factory Defaults.

Reboot Device

Use this feature to perform a software reboot of the switch. If you applied configuration changes, click the **Save Configuration** button 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 Device page, click **Maintenance > Reset**, and make sure the **Reboot Device** tab is selected.

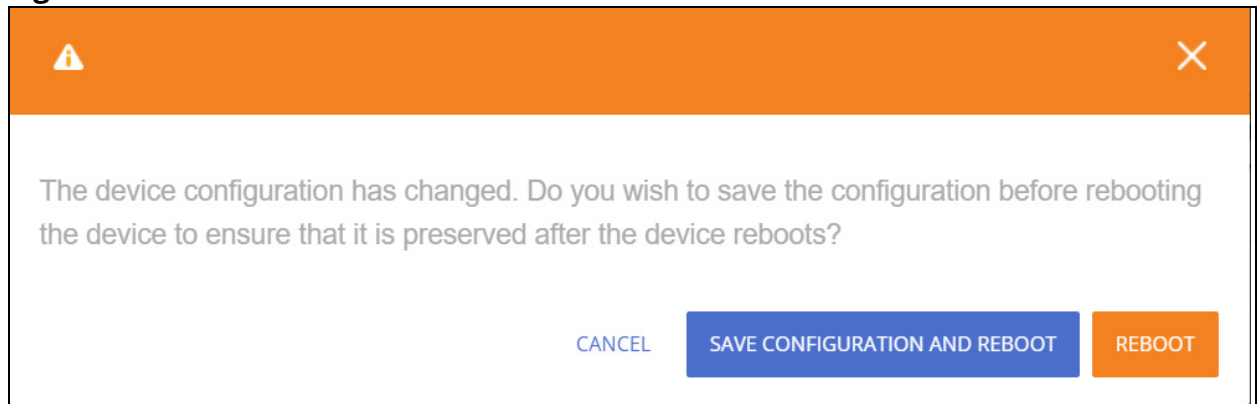
Figure 249. Reboot Device Tab



Click **REBOOT** to reboot the switch.

If the switch 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 250. Save Before Reboot



Reset to Factory Defaults

You can use the Reset To Factory Defaults page to reboot the switch and restore all switch settings to their factory default values and to erase all entries in the switch log file stored in the non-volatile memory. Following Reset to Factory default the switch will reset and all configuration changes, including those that were previously saved, are reset in the running system by this action.

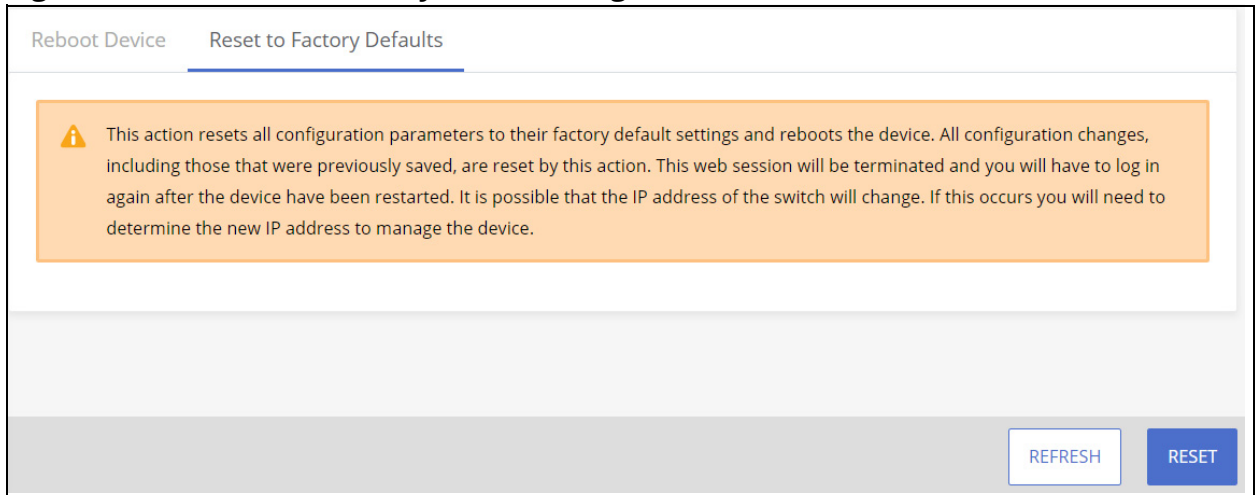
If the switch is configured to use DHCP to acquire its IP address, the address may change upon restart; you will need to determine the address before logging back in to the management utility.

To display the **Reset to Factory Defaults** page, click **Maintenance > Reset**, and make sure the **Reset to Factory Defaults** tab is selected.



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 251. Reset to Factory Defaults Page



Click **RESET** to reboot the switch and restore the system to the default settings.

Websites

Main Instant On site:

<https://www.arubainstanton.com/>

Support:

<https://support.arubainstanton.com/>

Instant On social forums and knowledge base:

<https://community.arubainstanton.com/>

Security Bulletins:

<https://www.arubanetworks.com/support-services/security-bulletins/>

End-user license agreement:

<https://www.arubainstanton.com/eula/>

Support contact numbers:

<https://www.arubainstanton.com/contact-support/>

Accessing Aruba Support

To access Aruba Support, go to <https://www.arubanetworks.com/support-services/>.

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:

- Aruba Support Portal asp.arubanetworks.com/downloads

If you are unable to find your product in the Aruba Support Portal, you may 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.