



Hewlett Packard
Enterprise

HPE OfficeConnect 1920S 8G/24G/48G Switch Series Management and Configuration Guide

Abstract

Use this guide to assist in managing the following HPE OfficeConnect 1920S switches:

- HPE OfficeConnect 1920S 8G Switch (JL380A)
- HPE OfficeConnect 1920S 24G Switch (JL381A)
- HPE OfficeConnect 1920S 48G Switch (JL382A)
- HPE OfficeConnect 1920S 8G PPOE+ (65W) Switch (JL383A)
- HPE OfficeConnect 1920S 24G PPOE+(185W) Switch (JL384A)
- HPE OfficeConnect 1920S 24G PoE+(370W) Switch (JL385A)
- HPE OfficeConnect 1920S 48G PPOE+ (370W) Switch (JL386A)

© Copyright 2018 by Hewlett Packard Enterprise Development LP

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

Microsoft®, Windows®, and Windows NT® are US registered trademarks of Microsoft Corporation.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

Revision History

Revision #: 2	Date: November 2018
Revision #: 1	Date: December 2017
Revision #: Initial Release	Date: March 2017

Open Source Code Notice

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To receive the CD, HPE charges a small fee in order to cover the actual costs of manufacturing and shipping the CD.

Requests for Open Source Software should be emailed to HPN_SMB_FOSS_code_request@hpe.com.

Please specify the product and version for which you are requesting source code.

Warranty

For the software end user license agreement and the hardware limited warranty information for HPE Networking products, visit <http://www.hpe.com/support/Networking-Warranties>.

Applicable Products

HPE OfficeConnect 1920S 8G Switch	JL380A
HPE OfficeConnect 1920S 24G Switch	JL381A
HPE OfficeConnect 1920S 48G Switch	JL382A
HPE OfficeConnect 1920S 8G PPoE+ (65W) Switch	JL383A
HPE OfficeConnect 1920S 24G PPoE+(185W) Switch	JL384A
HPE OfficeConnect 1920S 24G PoE+(370W) Switch	JL385A
HPE OfficeConnect 1920S 48G PPoE+ (370W) Switch	JL386A

Contents

Preface	10
About This Document	10
Audience	10
About Your Switch Manual Set	10
Supported Features	11
1 Getting Started	12
Connecting the Switch to a Network	12
Operating System and Browser Support	13
Getting Started With the Web Interface	13
Logging On	13
Interface Layout and Features	14
Common Page Elements	15
Saving Changes	15
Graphical Switch	15
Port Configuration and Summary	16
System LEDs	16
Port Status Indicator	16
2 System Dashboard	17
Dashboard	17
3 Setup Network	19
Get Connected	19
HTTPS Configuration	22
System Time Pages	24
System Time	24
Time Configuration	25
Time Zone Configuration	27
Daylight Saving Time Configuration	28
User Accounts	30
Configuration	30
Adding a User Account	31
Changing User Account Information	32
Removing a User Account	32
Sessions	33
Password Manager	34

4 Switching Features	36
Port Configuration	36
Port Status	36
Modifying Interface Settings	39
Port Summary Statistics	40
Port Mirroring	41
Port Mirroring Configuration	41
Configuring a Port Mirroring Session	42
Configuring a Port Mirroring Source	43
Configuring the Port Mirroring Session Destination	44
Removing Source Ports from a Session	44
Port Mirroring Summary	45
Flow Control	46
Spanning Tree	47
Spanning Tree Switch Configuration	47
Spanning Tree MSTP Summary	49
Spanning Tree MSTP Port Summary	50
Viewing MSTP Port Details or Editing MSTP Port Settings	51
CST Configuration	54
CST Port Summary	56
Viewing CST Port Details or Editing CST Port Settings	57
Spanning Tree Statistics	61
Loop Protection	62
Loop Protection Status	62
Loop Protection Configuration	63
Configuring Loop Protection Settings on Interfaces	64
IGMP Snooping	66
IGMP Snooping Global Configuration	66
IGMP Snooping Interface Configuration	67
Configuring IGMP Snooping Settings on Interfaces	68
Multicast Router Configuration	68
Configuring Multicast Router Settings on Interfaces	69
IGMP Snooping VLAN Configuration	70
Enabling IGMP Snooping on a VLAN	71
Modifying IGMP Snooping Settings on a VLAN	71
Disabling IGMP Snooping on a VLAN	72
Multicast Router VLAN Configuration	72
SNMP	74

SNMP v1 and v2	74
SNMP v3	74
SNMP Community Configuration	75
Adding an SNMP Community or Community Group.....	76
Removing an SNMP Community or Community Group.....	76
SNMP v1/v2 Trap Receivers.....	77
Adding an SNMP v1/v2 Trap Receiver	78
Removing an SNMP v1/v2 Trap Receiver	78
SNMP 3 Trap Receivers	78
Adding an SNMP v3 Trap Receiver.....	79
Removing an SNMP v3 Trap Receiver.....	80
Access Control Group	80
Adding an SNMP Access Control Group	81
Removing an SNMP Access Control Group	82
User Security Model	82
Adding an SNMP v3 User.....	83
Removing an SNMP v3 User.....	83
SNMP View Entry.....	84
Adding an SNMP View	85
Removing an SNMP View	85
Auto Recovery Configuration.....	86
5 Virtual LAN	89
Viewing VLAN Status and Adding VLANs	89
Adding VLANs.....	90
Changing a VLAN Name.....	91
Configuring Interfaces as VLAN Members	91
VLAN Port Configuration	93
Auto Voice VLAN Configuration.....	94
6 Trunks	96
Trunk Overview.....	96
Trunk Configuration	97
Modifying Trunk Settings.....	98
Trunk Statistics	99
7 Link Layer Discovery Protocol (LLDP and LLDP-MED)	100
LLDP Global Configuration	100
LLDP Local Device Summary.....	102
Displaying Port Details	103

LLDP Remote Device Summary	104
LLDP Global Statistics	105
LLDP-MED Global Configuration	107
LLDP-MED Local Device Summary	109
LLDP-MED Remote Device Summary	110
Displaying Remote Device Details	111
8 Power Over Ethernet.....	113
PoE Capabilities	113
PoE Configuration.....	114
PoE Port Configuration	115
Modifying Port PoE Settings	116
Viewing PoE Port Details	117
PoE Port Schedule	118
Configuring an Absolute Time Period	119
Adding a Periodic Time Period.....	120
9 Routing	121
Routing Configuration	121
Routing IP Interface Summary	121
Global Routing IP Configuration.....	123
Routing IP VLAN/Interface Configuration.....	125
Routing IP Statistics	127
IPv4 Routing	130
IP Route Summary	130
Configured Route Summary.....	131
Adding a Static Route	132
Removing a Route	132
Route Table.....	133
DHCP Relay	134
DHCP Relay Global Configuration	134
Adding a DHCP Server.....	135
Removing a DHCP Server.....	135
DHCP Relay VLAN/Interface Configuration	135
Adding a DHCP Server.....	136
Removing a Relay Interface	136
DHCP Relay Statistics	137
Configuring ARP	138
ARP Table Summary	139

Adding a Static ARP Entry	140
Removing an ARP Entry	140
ARP Table Configuration	141
ARP Table Statistics	142
10 Quality of Service (QoS)	143
Configuring Access Control Lists	143
Access Control List Summary	143
Adding an ACL	144
Removing an ACL	145
Access Control List Configuration	145
Adding a Rule to a Standard IPv4 ACL	146
Adding a Rule to an Extended or Named IPv4 ACL	148
Adding a Rule to an Extended MAC ACL	151
Access Control List Interface Summary	154
Associating an ACL with an Interface	155
Removing an Association Between an ACL and an Interface	155
Access Control List VLAN Summary	156
Associating an ACL with a VLAN	157
Removing an Association Between an ACL and a VLAN	157
Access Control List Statistics	158
Configuring Class of Service	160
802.1p CoS Mapping Configuration	160
Configuring 802.1p CoS Mapping on an Interface	161
DSCP CoS Global Mapping Configuration	162
CoS Trust Configuration	163
Configuring the Trust Mode and Shaping Rate on an Interface	163
CoS Interface Queue Configuration	164
Configuring CoS Queue Settings	165
11 Security	166
Advanced Security Configuration	166
RADIUS Settings	168
RADIUS Configuration	168
Adding a RADIUS Server	170
Changing RADIUS Server Settings	170
Removing a RADIUS Server	171
RADIUS Server Statistics	171
RADIUS Accounting Server Status	173

Adding a RADIUS Accounting Server.....	174
Changing RADIUS Accounting Server Settings	174
Removing a RADIUS Accounting Server.....	175
RADIUS Accounting Server Statistics	175
Port Access Control	177
Port Access Control Configuration	177
Configuring Port Access Control on an Interface.....	180
Viewing Per-port 802.1X Details.....	184
Port Access Control Statistics	184
Port Access Control Client Summary	186
Port Access Control History Log Summary	187
Port Security	188
Port Security Global Administration	188
Port Security Interface Status	189
Port Security Static MAC Addresses.....	190
Port Security Dynamic MAC Addresses.....	191
Convert Dynamic MAC Addresses to Static MAC Addresses	192
Protected Ports	193
Protected Ports Configuration	193
Creating a Protected Ports Group	194
Editing a Protected Ports Group.....	194
Removing a Protected Ports Group	194
Storm Control.....	195
12 Green Features	196
Green Features Configuration	196
EEE Status	197
13 Diagnostics.....	198
Buffered Log	198
Crash Log.....	199
Log Configuration	200
Ping.....	202
Ping IPv4.....	202
Ping IPv6.....	203
Traceroute	205
Traceroute IPv4.....	205
Traceroute IPv6.....	207
Reboot Switch.....	209

Factory Defaults.....	210
Support File	211
Locator.....	213
MAC Table.....	213
14 Maintenance Pages	215
Dual Image Configuration	215
Backup and Update Manager	216
Backing Up Files	216
Updating Files	218
Configuration Files.....	222
A Support and other resources	223
Accessing Hewlett Packard Enterprise Support.....	223
Accessing updates	223
Websites	224
Customer self repair	224
Remote support	224
Documentation feedback.....	225
B Warranty information	226
Warranty information	226

Preface

About This Document

The HPE OfficeConnect 1920S Switch Series provides reliable, plug-and-play Gigabit network connectivity. The HPE OfficeConnect 1920S switches are ideal for open offices that require silent operation or businesses making the transition from unmanaged to managed networks.

The HPE OfficeConnect 1920S switches can be managed in-band from a remote network station using a web-based graphical user interface (GUI), and its configuration may also be viewed using the SNMP manager. This guide describes how to configure and view the software features using the web GUI.

Audience

The information in this guide is primarily intended for system administrators and support providers who are responsible for configuring, operating, or supporting a network using HPE OfficeConnect 1920S switch software. An understanding of the software specifications for the networking device platform, and a basic knowledge of Ethernet and networking concepts, are presumed.

About Your Switch Manual Set

The switch manual set includes the following:

- **HPE OfficeConnect 1920S Switch Series Quick Setup Guide and Safety/Regulatory Information** - a printed guide shipped with your switch. Provides illustrations for basic installation and setup. Also includes product specifications, as well as safety and regulatory statements and standards supported by the switch.
- **HPE OfficeConnect 1920S Switch Series Installation and Getting Started Guide** - (HPE website only). Provides detailed installation guide for your switch, including physical installation on your network, basic troubleshooting, product specifications, supported accessories, Regulatory and Safety information.
- **HPE OfficeConnect 1920S Switch Series Management and Configuration Guide** - This guide describes how to manage and configure switch features using a web browser interface.
- **Release Notes** - (HPE website only). Provides information on software updates. The Release Notes describe new features, fixes, and enhancements that become available between revisions of the above guides.

NOTE:

For the latest version of all HPE documentation, visit the HPE website at www.hpe.com/support/manuals. Then select your switch product.

Supported Features

HPE OfficeConnect 1920S switches include support for the following features:

Feature	HPE OfficeConnect 1920S Series Switch
HTTP and HTTPS sessions	4 each, 8 total
SNMPv1/v2c/v3 (r/w community)	1
MAC table	16382 entries
SNTP server configuration	1
Time zones count	91
Jumbo frame size	9216 bytes
Soft session web session timeout	1 min–60 min
Hard session web session timeout	1 Hr–168 Hrs
Trunk configuration (8 port switch)	4
Trunk configuration (24 port switch)	8
Trunk configuration (48 port switch)	16
Trunk membership ports (8 port switch)	4
Trunk membership ports (24 port switch)	4
Trunk membership ports (48 port switch)	8
VLANs	256
VLAN IDs	1-4093
VLAN priority levels	0–7
ACLs (IPv4 and MAC)	50
Configurable rules per list	2
ACL rules per interface	10
CoS queues per port	4
IEEE 802.1p traffic classes	4
Static routes	32
ARP entries	509
Syslog servers	1
Buffered logs	200 (total storage 10K)
Maintenance users	1
Password length	8 chars–64 chars
Images	2

1 Getting Started

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

Connecting the Switch to a Network

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

NOTE:

- 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 device 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 by using the default IP address:

1. Connect the switch to the management PC or to the network using any of the available network ports.
2. Power on the switch.
3. Set the IP address of the management PC's network adapter to be in the same subnet as the switch.

For example, set it to IP address 192.168.1.2, mask 255.255.255.0.

4. Enter the IP address 192.168.1.1 in the web browser. See [page 13](#) for web browser requirements.

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

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

Operating System and Browser Support

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

Operating System	Browser
Windows 7	Internet Explorer 9, 10 Firefox 38.2.1, 40.0.3, 41.0.b1 (beta) Chrome 44.0.2403, 45.0.2454, 46.0 (beta)
Windows 8/8.1	Internet Explorer 11 (included in base OS 8.1) Firefox 38.2.1, 40.0.3, 41.0.b1 (beta) Chrome 44.0.2403, 45.0.2454, 46.0 (beta)
Windows 10	Internet Explorer 11 (included in base OS) Chrome 44.0.2403, 45.0.2454 (beta)
MacOS X	Firefox 38.2.1, 40.0.3, 41.0.b1 (beta)
MacOS X 10.6 and later	Safari 7, Chrome 44.0.2403, 45.0.2454, 46.0 (beta)

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

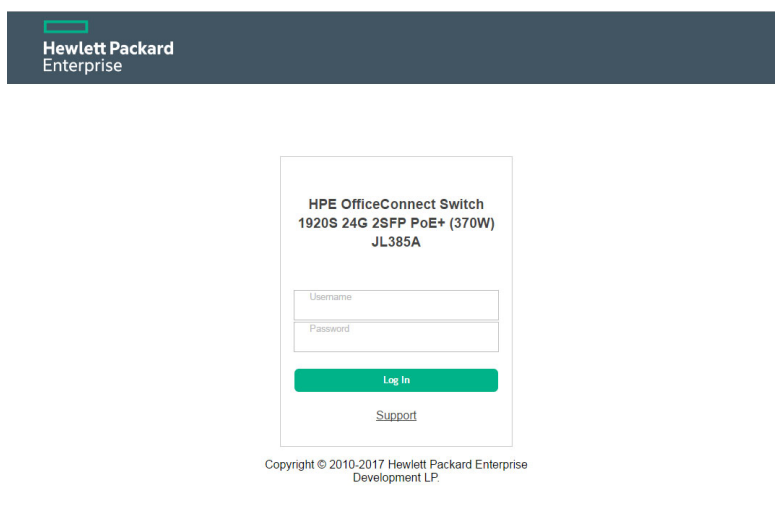
Follow these steps to log on through the web interface:

1. Open a web browser and enter the IP address of the switch in the web browser address field.
2. On the Login page, enter the username and password (if one has been set), and then click **Log In**.
By default, the username is **admin** and there is no password. After the initial log on, the administrator may configure a password.

NOTE:

To set the password or change the username, see [“Password Manager” on page 34](#).

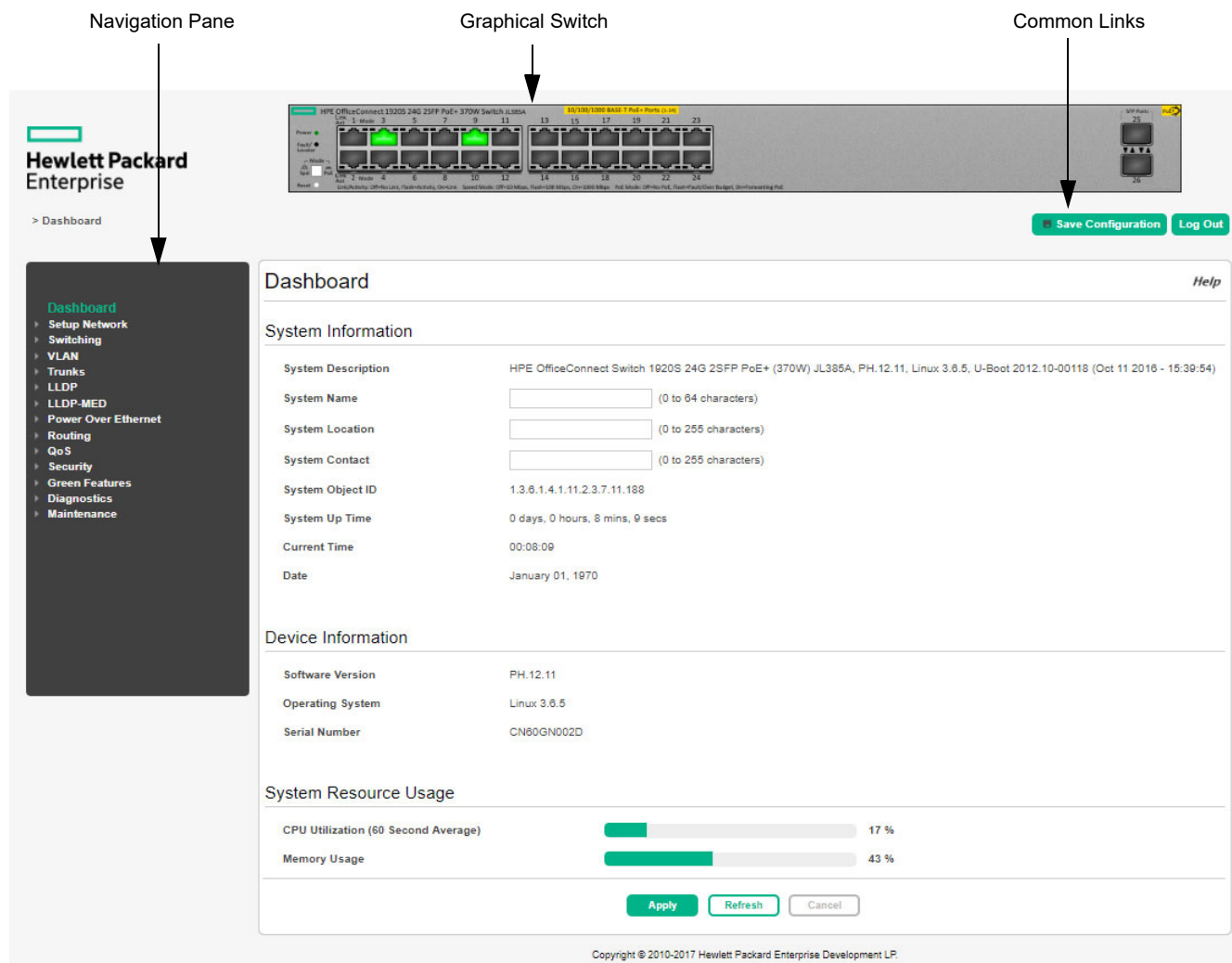
Figure 1. Login Page



Interface Layout and Features

Figure 2 shows the initial view.

Figure 2. Interface Layout and Features



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

The Dashboard page displays when you first log on and when you click **Dashboard** in the navigation pane. See [“System Dashboard” on page 17](#) 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” on page 19](#) for more information.

The graphical switch displays summary information for the switch LEDs and port status. For information on this feature see [“Graphical Switch” on page 15](#).

Common Page Elements

Most pages contain a common set of buttons that include one or more of the following:

- Click *Help* on any page to display a help panel that explains the fields and configuration options on the page.
- Click to send the updated configuration to the switch. Applied changes update the device running configuration and take effect immediately. If you want the device to retain these changes across a reboot, you must first save the configuration. See [“Saving Changes” on page 15](#).
- Click to refresh the page with the latest information from the switch.
- Click to clear any configurations changes that have not yet been applied on a page.
- Click to end the current management session.

Saving Changes

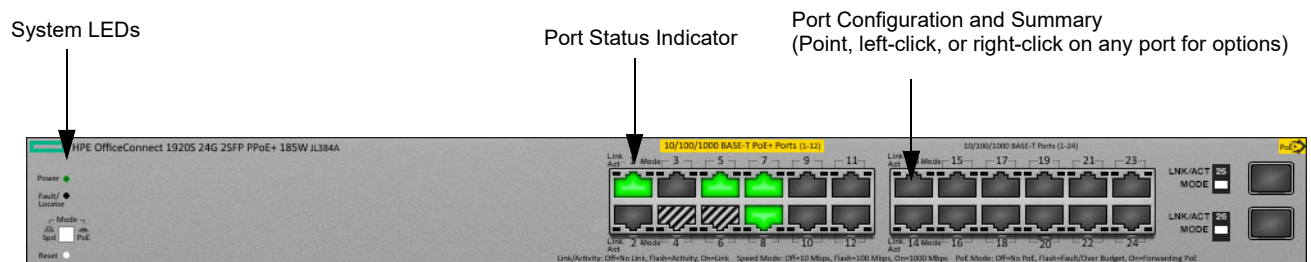
When you click , changes are saved to the running configuration file in RAM. Unless you save them to system flash memory, the changes will be lost if the system reboots. To save them permanently, click on the upper right side of the page. Note that when there are unsaved changes, the button displays a file image (). A page displays to confirm that you want to save, followed by a page that confirms that the operation was completed successfully.

Graphical Switch

The graphical switch, shown in [Figure 3](#), displays at the top of the page as a representation of the physical switch to provide status information about individual ports. The graphical switch enables easy system configuration and web-based navigation.

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

Figure 3. Graphical Switch



Port Configuration and Summary

You can point to any port to display the following information about the port:

- Port description
- The link status (up or down).
- Auto negotiation status.
- The maximum transmission unit (MTU), which is the largest packet size that can be transmitted on the port.

You can left-click a port to display the Port Status page.






System LEDs

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

- Power (Green)
 - On—The switch is receiving power.
 - Blinking—The switch is receiving power through its Power Over Ethernet (PoE) port.
 - Off—The switch is powered off or is NOT receiving power.
- Fault/Locator (Orange)
 - Blinking rapidly—A fault has occurred, other than during self-test.
 - Blinking slowly—The locator function has been enabled to help physically locate the switch.
 - On—If continuously on, no firmware was detected upon boot-up.
 - Off—The locator function is disabled and the switch is operating properly.

Port Status Indicator

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

Port State	Image	Description
Active		The port is connected, enabled, and the link is up.
Disabled		The port has been administrative disabled. This image is also used for “dead” ports that may exist physically on the device but have no internal connection.
Error		The port has an error condition and may or may not be active.
Inactive		The port is connected and enabled, but the link is down (likely because no cable is connected).
Sourcing Power		For a PoE port, this image is overlaid on the port when it is providing power.

2 System Dashboard

The switch includes a dashboard that displays basic information about the system and allows you to configure a name, location, and description for the system.

Dashboard

The Dashboard page displays basic information such as the configurable switch name and description, the IP address for management access, and the software and operating system versions. This page also shows resource usage statistics.

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

Figure 4. Dashboard Page

Dashboard

Help

System Information

System Description

HPE OfficeConnect Switch 1920S 24G 2SFP PoE+ (370W) JL385A, P12.12.13, Linux 3.6.5, U-Boot 2012.10-00118 (Oct 11 2016 - 15:39:54)

System Name

dhcp-10-27-36-198

(0 to 64 characters)

System Location

(0 to 255 characters)

System Contact

(0 to 255 characters)

System Object ID

1.3.6.1.4.1.11.2.3.7.11.188

System Up Time

0 days, 2 hours, 32 mins, 27 secs

Current Time

02:32:27

Date

January 01, 1970

Device Information

Software Version

P12.12.13

Operating System

Linux 3.6.5

Serial Number

CN80GN002D

System Resource Usage

CPU Utilization (60 Second Average)

28 %

Memory Usage

43 %

Logged In Users

Display

All

rows

Showing 1 to 2 of 2 entries

Filter:

Username	Connection From	Idle Time	Session Time
admin	10.27.65.210	00:00:01	00:03:30
admin	10.27.65.210	00:00:08	00:00:12

First

Previous

1

Next

Last

Apply

Refresh

Cancel

NOTE:

The Logged In Users fields display only if more than one user is logged into the system.

If you update the name, location, or contact information, 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 1. Dashboard Page Fields

Field	Description
System Information	
System Description	A description of the switch hardware, including the hardware type, software version, operating system version, and boot loader (U-Boot) version.
System Name	Enter the preferred name to identify this switch. A maximum of 64 alpha-numeric characters including hyphens, commas and spaces are allowed. This field is blank by default. The user configurable switch name will appear in the login screen banner.
System Location	Enter the location of this switch. A maximum of 255 alpha-numeric characters including hyphens, commas, and spaces are allowed. This field is blank by default.
System Contact	Enter the name of the contact person for this switch. A maximum of 255 alpha-numeric characters including hyphens, commas, and spaces are allowed. This field is blank by default.
System Object ID	The base object ID for the switch's enterprise MIB.
System Up Time	The time in days, hours and minutes since the last switch reboot.
Current Time	The current time in hours, minutes, and seconds as configured (24- or 12-hr AM/PM format) by the user.
Date	The current date in month, day, and year format.
Device Information	
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.
System Resource Usage	
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.
Logged In Users—These fields display only when more than one user is logged into the management utility.	
Username	The username of each logged in user.
Connection From	The IP address from which the user logged in.
Idle Time	The time that has elapsed since the last user activity.
Session Time	The amount of time the user session has been active.

3 Setup Network

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

Get Connected

Use the Get Connected page to configure settings for the network interface. The network interface is defined by an IP address, subnet mask, and gateway. Any one of the switch's front-panel ports can be selected as the management port for the network interface. The configuration parameters associated with the switch's network interface do not affect the configuration of the front-panel ports through which traffic is switched or forwarded except that, for the management port, the port VLAN ID (PVID) will be the management VLAN.

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


In the example configuration in [Figure 5](#), the switch is configured to acquire its IP address through DHCP, which is the default setting. Access to the management software is restricted to members of VLAN 1.

Figure 5. Get Connected Page

The screenshot shows the 'Get Connected' configuration page with the following sections:

- Get Connected** (Title bar with 'HTTPS Connection' tab and 'Help' link)
- Network Details**
 - Internet Protocol Address: ☒ IPv4, ☐ IPv6
 - Protocol Type: ☐ Static, ☒ DHCP, ☐ (P)
 - IP Address: (x.x.x.x)
 - Subnet Mask: (x.x.x.x)
 - Gateway Address: (x.x.x.x)
 - MAC Address: 1C:98:EC:7C:8E:40
- HTTP Management Access**
 - HTTP Admin Mode: ☒ Enabled, ☐ Disabled
 - HTTP Port: (1025 to 65535, 80 = Default)
 - HTTP Session Soft Time Out (Minutes): (1 to 60)
 - HTTP Session Hard Time Out (Hours): (1 to 168)
 - Maximum Number of HTTP Sessions: (1 to 4)
- Management VLAN**
 - Management VLAN ID:
 - Management Port:
- Buttons:** Apply, Refresh, Cancel

Table 2. Get Connected Fields

Field	Description
Network Details	
Internet Protocol Address	Select whether to configure the IPv4 or IPv6 information for the switch. The rest of the fields in the Network Details section depend on the option you select.
IPv4 Network Details	
Protocol Type	<p>Select the type of network connection:</p> <ul style="list-style-type: none"> • Static—Select this option to enable the IP address, subnet mask, and gateway fields for data entry. • DHCP—Select this option to enable the switch to obtain IP information from a DHCP server on the network. If the DHCP server responds, then the assigned IP address is used. If DHCP is enabled but the DHCP server does not respond, the default static IP address 192.168.1.1 is used. DHCP operation is enabled by default. <p>When a DHCP server assigns an IP address to the switch, it specifies the time for which the assignment is valid. After the time expires, the server may reclaim the address for assignment to another device. When DHCP is enabled, you can click  to send a request to the DHCP server to renew the lease.</p> <p>Only a user-configured static IP address is saved to flash.</p> <p>CAUTION: Changing the protocol type or IP address discontinues the current connection; you can log on again using the new IP information.</p>
IP Address	<p>The IPv4 address for the switch.</p> <p>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.</p> <p>Note: A broadcast, multicast, or network IP address should not be entered in this field.</p>
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.
MAC Address	The hardware MAC address of this switch.
IPv6 Network Details	
IPv6 Mode	Enables or disables the IPv6 administrative mode on the network interface.
Network Configuration Protocol	Specify whether the device should attempt to acquire network information from a DHCPv6 server. Selecting None disables the DHCPv6 client on the network interface.
IPv6 Stateless Address AutoConfig Mode	<p>Sets the IPv6 stateless address autoconfiguration mode on the network interface.</p> <ul style="list-style-type: none"> • Enabled – The network interface can acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of Router Advertisement messages. • Disabled – The network interface will not use the native IPv6 address autoconfiguration features to acquire an IPv6 address.
Static IPv6 Addresses	Specify the IPv6 address to add to the interface.
Dynamic IPv6 Addresses	Lists the IPv6 addresses on the network interface that have been dynamically configured through IPv6 autoconfiguration or DHCPv6.
EUI Flag	Select this option to enable the Extended Universal Identifier (EUI) flag for IPv6 address, or clear the option to omit the flag.
DHCPv6 Client DUID	The client identifier used by the DHCPv6 client (if enabled) when sending messages to the DHCPv6 server.
IPv6 Gateway	Specify the default gateway for the IPv6 network interface.

Field	Description
HTTP Management Access	
HTTP Admin Mode	Enables or disables the HTTP administrative mode. When enabled, the device can be accessed through a web browser using the HTTP protocol.
HTTP Port	<p>The TCP port number on which the HTTP server listens for requests. Existing HTTP login sessions are closed whenever this value is changed. All new HTTP sessions must use the new port number.</p> <p>Note: Before changing this value, check your system to make sure the desired port number is not currently being used by any other service.</p>
HTTP Session Soft Time Out (Minutes)	HTTP session inactivity timeout value. A logged-in user that does not exhibit any HTTP activity for this amount of time is automatically logged out of the HTTP session.
HTTP Session Hard Time Out (Hours)	HTTP session hard timeout value. A user connected to the device via an HTTP session is automatically logged out after this amount of time regardless of the amount of HTTP activity that occurs.
Maximum Number of HTTP Sessions	The maximum number of HTTP sessions that may be connected to the device simultaneously.
Management VLAN	
Management VLAN ID	<p>Access to the management software is controlled by the assignment of a management VLAN ID. Only ports that are members of the management VLAN allow access to the management software.</p> <p>By default, the management VLAN ID is 1. The management VLAN can be any value between 1 and 4093. All ports are members of VLAN 1 by default; the administrator may want to create a different VLAN to assign as the management VLAN and associate it with a management port (see the next field).</p> <p>A VLAN that does not have any member ports (either tagged or untagged) cannot be configured as the management VLAN.</p> <p>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.</p>
Management Port	<p>Access to the management software can also be controlled by the selection of a management port. The selected management port is auto-configured to be an untagged member of the management VLAN and is excluded from any other untagged VLANs.</p> <p>When the switch boots with the default configuration, any port can be used as management port and this field is configured as None.</p> <p>You can configure a management port to ensure that a port always remains an untagged member of the configured management VLAN; this helps to ensure management connectivity in case of an accidental change in VLAN membership.</p> <p>If no management port is specified, then all ports that are members of the management VLAN provide access to the switch management interface. If a management port is configured, access to the switch is restricted to that port. For example, if VLAN 1 is the management VLAN and port 10 is the management port, other ports that are members of VLAN 1 will not provide access to the switch management interface.</p> <p>The features that utilize the management port include the following:</p> <ul style="list-style-type: none"> • DHCP • SNMP • SNT • TFTP

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**.

NOTE:

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 [“Factory Defaults” on page 210](#)).

NOTE:

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

HTTPS Configuration

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

To access the HTTPS Configuration page, click **Setup Network > Get Connected** in the navigation menu, and then click the **HTTPS Connection** tab.

Figure 6. HTTPS Management Access Page

Get Connected **HTTPS Connection**

HTTPS Management Access Help

HTTPS Admin Mode ☐ Enabled ☒ Disabled

TLS Version 1 ☐ Enabled ☒ Disabled

HTTPS Port (1025 to 65535, 443 = Default)

HTTPS Session Soft Time Out (Minutes) (1 to 60)




HTTPS Session Hard Time Out (Hours) (1 to 168)

Maximum Number of HTTPS Sessions (1 to 4)

Certificate Status

Apply **Refresh** Cancel

Table 3. HTTPS Management Access Fields

Field	Description
HTTPS Admin Mode	Enables or disables the HTTPS administrative mode. When this mode is enabled, the device can be accessed through a web browser using the HTTPS protocol.
TLS Version 1	Enables or disables Transport Layer Security Version 1.0. When this option is enabled, communication between the web browser on the administrative system and the web server on the device is sent through TLS 1.0.
HTTPS Port	The TCP port number that HTTPS uses.
HTTPS Session Soft Time Out (Minutes)	HTTPS session inactivity timeout value. A logged-in user that does not exhibit any HTTPS activity for this amount of time is automatically logged out of the HTTPS session.
HTTPS Session Hard Time Out (Hours)	HTTPS session hard timeout value. A user connected to the device via an HTTPS session is automatically logged out after this amount of time regardless of the amount of HTTPS activity that occurs.
Maximum Number of HTTPS Sessions	The maximum number of HTTPS sessions that can be connected to the device simultaneously.
Certificate Status	The status of the SSL certificate generation process. <ul style="list-style-type: none">• Present – The certificate has been generated and is present on the device• Absent – Certificate is not available on the device• Generation In Progress – An SSL certificate is currently being generated.
Download Certificates (Button) 	Allows you to download an SSL certificate file from a remote system to the device. Note that to download SSL certificate files, SSL must be administratively disabled.
Generate Certificate (Button) 	Generates an SSL certificate to use for secure communication between the web browser and the embedded web server on the device.
Delete Certificates (Button) 	Deletes the SSL certificate. This button is available only if an SSL certificate is present on the device.

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**.

System Time Pages

You click **Setup Network > System Time** to display the web pages for configuring the system clock, SNTP client functionality, system time zone, and daylight saving time settings.

System Time

The System Time page displays the current time, time zone, and Daylight Saving Time settings, and enables you to configure the time display format. To display the System Time page, click **Setup Network > System Time** in the navigation pane, and ensure that the **Clock** tab is selected.

Figure 7. System Time Page

ClockTimeTime ZoneDaylight Saving Time

System Time

Help

Current Time

Time

02:45:23

Date

January 01, 1970

Time Source

No Time Source

Time Format

☒ 24 Hour

☐ 12 Hour

Time Zone

Time Zone

(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Acronym

Daylight Saving Time

Daylight Saving Time

No Daylight Saving Time

Apply

Refresh

Cancel

Table 4. System Time Fields

Field	Description
Current Time	
Time	The current time. This value is determined by an SNTP server. When SNTP is disabled, the system time increments from 00:00:00, 1 Jan 1970, which is set at bootup.
Date	The current date.
Time Source	The source from which the time and date is obtained: <ul style="list-style-type: none">• SNTP—The time has been acquired from an SNTP server.• No Time Source—The time has been either manually configured or not configured at all. This is the default selection.
Time Format	Select 24 Hour (“military” time, the default) or 12 Hour to specify the time display format.

Field	Description
Time Zone	
Time Zone	The currently set time zone. 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 (e.g., PST, EDT).
Daylight Saving Time	
Daylight Saving Time	<p>Shows whether Daylight Saving Time (DST) is enabled and the mode of operation:</p> <ul style="list-style-type: none"> • No Daylight Saving Time—No clock adjustment will be made for DST. This is the default. • Recurring Every Year—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 (i.e., they will not carry forward to subsequent years). <p>If DST is enabled and the current time is within the configured DST period, then “(On DST)” displays following this field value.</p>

For instructions on configuring the system time, see [“Time Configuration” on page 25](#), [“Time Zone Configuration” on page 27](#), and [“Daylight Saving Time Configuration” on page 28](#).

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 device 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.

To display the Time Configuration page, click **Setup Network > System Time** in the navigation pane and click the **Time** tab.

Figure 8. Time Configuration Page

The screenshot shows the 'Time Configuration' page with the 'Time' tab selected. At the top, there are tabs for 'Clock', 'Time', 'Time Zone', and 'Daylight Saving Time'. The 'Time' tab is active, displaying a 'Time Configuration' header with a 'Help' link. Below the header, there are two radio buttons for 'Set System Time': 'Using Simple Network Time Protocol (SNTP)' and 'Manually'. The 'Manually' option is selected. Under the 'SNTP Configuration' section, there are several fields: 'SNTP Client' with radio buttons for 'Enabled' and 'Disabled' (selected), 'SNTP/NTP Server' with a text input field and a placeholder '(x.x.x.x)', 'Server Port' with a text input field containing '123' and a range '(1 to 65535)', 'Last Update Time' with a timestamp 'Jan 1 00:00:00 1970', 'Last Attempt Time' with a timestamp 'Jan 1 00:00:00 1970', 'Last Attempt Status' with the text 'Other', 'Requests' with the value '0', and 'Failed Requests' with the value '0'. Below this is the 'Manual Time Configuration' section, which includes a 'Time' field with a text input '02:46:51' and a range '(00:00:00 to 23:59:59)', and a 'Date' field with a text input 'January 1, 1970' and a calendar icon. At the bottom, there are three buttons: 'Apply', 'Refresh', and 'Cancel'.

Table 5. Time Configuration Fields

Field	Description
Set System Time	Select Using Simple Network Time Protocol (SNTP) 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 Manually to disable SNTP and configure the time manually. When selected, only the Manual Time Configuration fields are available for configuration.
SNTP Configuration	
SNTP Client	Select Enabled or Disabled (default) to configure the SNTP client mode. When disabled, the system time increments from 00:00:00, 1 Jan 1970, which is set at bootup.
SNTP/NTP Server	Specify the IPv4 address of the SNTP server to which requests should be sent.
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.

Field	Description
Last Update Status	The status of the last update request to the SNTP server, which can be one of the following values: <ul style="list-style-type: none"> Other—None of the following values apply or no message has been received. Success—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. Bad Date Encoded—The time provided by the SNTP server is not valid. Version Not Supported—The SNTP protocol version supported by the server is not compatible with the version supported by the switch client. Server Unsynchronized—The SNTP server is not synchronized with its peers. This is indicated via the leap indicator field in the SNTP message. Blocked—The SNTP server indicated that no further requests were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from the server.
Requests	The number of requests made to the SNTP sever since the switch was rebooted.
Failed Requests	The number of failed SNTP requests made to this server since last reboot.
Manual Time Configuration	
Time	Specify the current time in HH:MM:SS format.
Date	Click the date field to display a calendar and select the current date.

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**.

Time Zone Configuration

The Time Zone Configuration page is used to configure your local time zone.

To display this page, click **Setup Network > System Time** in the navigation pane and click the **Time Zone** tab.

Figure 9. Time Zone Configuration Page

Table 6. Time Zone Configuration Fields

Field	Description
Time Zone	Select the time zone for your location. The default is (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London.
Acronym	Specify an acronym for the time zone. The acronym can have up to four alphanumeric characters and can contain dashes, underscores, and periods.

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**.

Daylight Saving Time Configuration

The Daylight Saving Time Configuration page 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 Time page, click **Setup Network > System Time** in the navigation pane and click the **Daylight Saving Time** tab.

Figure 10. Daylight Saving Time Configuration Page

The screenshot shows the 'Daylight Saving Time Configuration' page. At the top, there are four tabs: 'Clock', 'Time', 'Time Zone', and 'Daylight Saving Time'. The 'Daylight Saving Time' tab is selected. Below the tabs, the page title 'Daylight Saving Time Configuration' is displayed, along with a 'Help' link. The main configuration area is divided into three sections: 'Daylight Saving Time', 'Date Range', and 'Recurring Date'. In the 'Daylight Saving Time' section, there is a dropdown menu currently set to 'Disable'. The 'Date Range' section contains four fields: 'Start Date' (with a calendar icon), 'Starting Time of Day' (with a time range '(00:00 to 23:59)'), 'End Date' (with a calendar icon), and 'Ending Time of Day' (with a time range '(00:00 to 23:59)'). The 'Recurring Date' section contains eight fields: 'Start Week' (dropdown set to 'First'), 'Start Day' (dropdown set to 'Sunday'), 'Start Month' (dropdown set to 'January'), 'Starting Time of Day' (with a time range '(00:00 to 23:59)'), 'End Week' (dropdown set to 'First'), 'End Day' (dropdown set to 'Sunday'), 'End Month' (dropdown set to 'January'), and 'Ending Time of Day' (with a time range '(00:00 to 23:59)'). At the bottom of the page, there are three buttons: 'Apply' (green), 'Refresh' (green), and 'Cancel' (gray).

Table 7. Daylight Saving Time Configuration Fields

Field	Description
Daylight Saving Time	<p>Select how DST will operate:</p> <ul style="list-style-type: none">• Disable—No clock adjustment will be made for DST. This is the default selection.• Recurring—The settings will be in effect for the upcoming period and subsequent years.• EU—The system clock uses the standard recurring daylight saving time settings used in countries in the European Union.• USA—The system clock uses the standard recurring daylight saving time settings used in the United States.• Non-Recurring—The settings will be in effect only for a specified period during the year (that is, they will not carry forward to subsequent years). <p>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.</p>
Date Range	<p>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:</p> <ul style="list-style-type: none">• Start/End Date—Use the calendar to set the day, month, and year when the change to/from DST occurs. Or, enter the hours and minutes in 24-hour format (HH:MM).• Starting Time of Day—Set the hour and minutes when the change to/from DST occurs.
Recurring Date	<p>When Recurring is selected as the DST mode, the following fields display:</p> <ul style="list-style-type: none">• Start/End Week—Set the week of the month, from 1 to 5, when the change to/from DST occurs. The default is 1 (the first week of the month).• Start/End Day—Set the day of the week when the change to/from DST occurs.• Start/End Month—Set the month when the change to/from DST occurs.• Starting/Ending Time of Day—Set the hour and minutes when the change to/from DST occurs.

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

User Accounts

By default, the switch contains only the *admin* user account, which has read/write privileges.

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

Configuration

If you log on to the switch with a user account with read/write privileges (i.e., as admin), you can use the **User Accounts Configuration** page to assign passwords and set security parameters for the default accounts. You can also add up to five read-only accounts. You can delete all accounts except for the Read/Write account.

To display this page, click **Setup Network > User Accounts** in the navigation pane.

Figure 11. User Accounts Configuration Page

Username	Access Level	Lockout Status	Password Override	Password Expiration
admin	Read/Write	False	Disabled	

Table 8. User Accounts Configuration 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: <ul style="list-style-type: none">Read Write - The user can view and modify the configuration.Read Only - The user can view the configuration but cannot modify any fields.Suspended - The user exists but is not permitted to log on to the device.
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 Override	Identifies the password override complexity status for this user. <ul style="list-style-type: none">Enable - The system does not check the strength of the password.Disable - When configuring a password, it is checked against the Strength Check rules configured for passwords.
Password Expiration	Indicates the current expiration date (if any) of the password.

From this page, use the available buttons to add or remove users, or to edit the settings for an existing user.

Adding a User Account

To add a new user account:

1. From the User Accounts Configuration page, click **Add**.
2. Configure the settings for the new user.

Field	Description
User Name	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.) User names are up to 32 alphanumeric characters in length and are not case sensitive. Valid characters include all the alphanumeric characters and the dash ('-') and underscore ('_') characters. User name <i>default</i> is not valid.
Password	Enter the optional new or changed password for the account. It will not display as it is typed, only asterisks (*) or dots(.) will show based on the browser used. 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: <ul style="list-style-type: none">• Read Write - The user can view and modify the configuration.• Read Only - The user can view the configuration but cannot modify any fields.• Suspended - The user exists but is not permitted to log on to the device.
Password Override	Identifies the password override complexity status for this user. <ul style="list-style-type: none">• Enable - The system does not check the strength of the password.• Disable - When configuring a password, it is checked against the Strength Check rules configured for passwords.
Password Strength	Shows the status of password strength check.
Encrypt password	Select this option to encrypt the password before it is stored on the device.

3. Click **Apply**.

Figure 12. Add New User Page

Add new user

Username (1 to 64)

Password (8 to 64 characters)

Confirm (8 to 64 characters)

Access Level ☐ None ☐ Read Only ☐ Read/Write

Password Override ☐

Password Strength Disabled

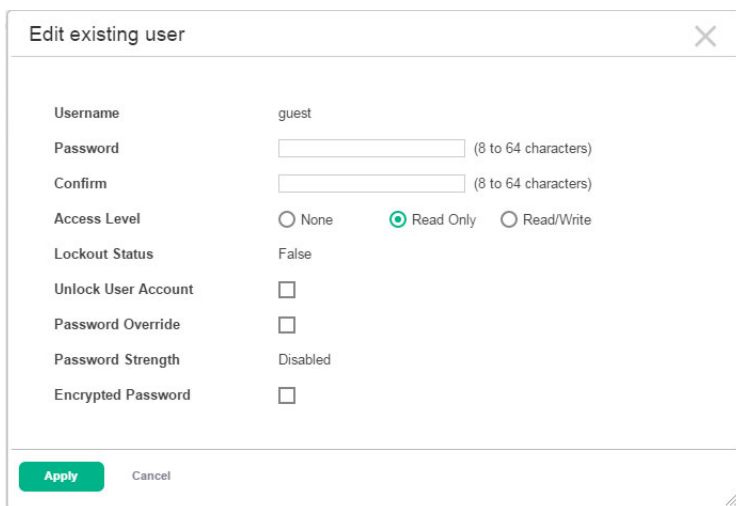
Encrypted Password ☐

Apply Cancel

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 **Edit**. Update the fields as needed, and click **Apply**.

Figure 13. Edit Existing User Page



The screenshot shows a dialog box titled "Edit existing user" with a close button (X) in the top right corner. The dialog contains the following fields and options:

Username	guest
Password	<input type="text"/> (8 to 64 characters)
Confirm	<input type="text"/> (8 to 64 characters)
Access Level	<input type="radio"/> None <input checked="" type="radio"/> Read Only <input type="radio"/> Read/Write
Lockout Status	False
Unlock User Account	<input type="checkbox"/>
Password Override	<input type="checkbox"/>
Password Strength	Disabled
Encrypted Password	<input type="checkbox"/>

At the bottom of the dialog, there are two buttons: "Apply" (highlighted in green) and "Cancel".

Removing a User Account

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

Sessions

The Sessions page identifies the users that are logged in to the management interface of the device. The page also provides information about their connections.

To display this page, click **Setup Network > User Accounts** in the navigation pane and click the **Sessions** tab.

Figure 14. Logged In Sessions Page

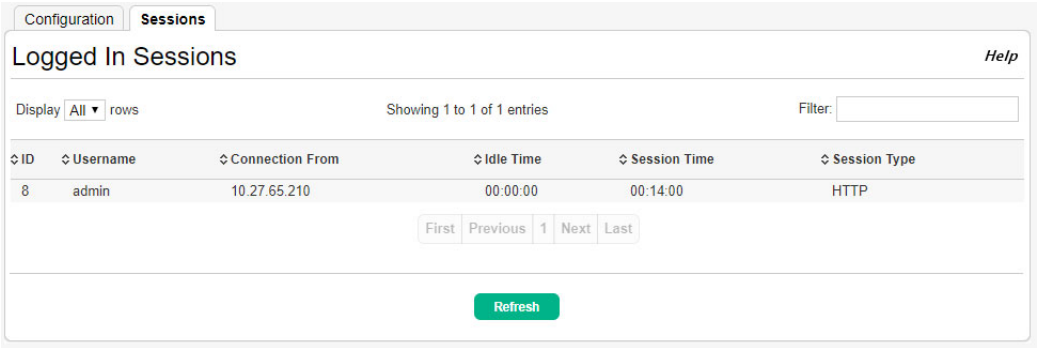


Table 9. Logged In Sessions Fields

Field	Description
ID	The unique ID of the session.
User Name	The name that identifies the user account.
Connection From	Identifies the administrative system that is the source of the connection. This field shows the IP address of the administrative system.
Idle Time	Shows the amount of time in hours, minutes, and seconds that the logged-on user has been inactive.
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.

Password Manager

Use this page to configure rules for locally-administered passwords. The rules you set determine the strength of local passwords that device users can associate with their usernames. The strength of a password is a function of length, complexity, and randomness. To display the Password Manager page, click **Setup Network > Password Manager** in the navigation menu.

Figure 15. Password Manager Page

Password Manager [Help](#)

Rules Configuration

Minimum Length: (0 to 64)

Aging (Days): (1 to 365, 0 = Default, 0 = Disable)

History: (0 to 10)

Lockout Attempts: (0 to 5, 0 = Default, 0 = Disable)

Password Complexity

Strength Check: ☐ Enabled ☒ Disabled

Minimum Number of Uppercase Letters: (0 to 16, 2 = Default, 0 = Disable)

Minimum Number of Lowercase Letters: (0 to 16, 2 = Default, 0 = Disable)

Minimum Number of Numeric Characters: (0 to 16, 2 = Default, 0 = Disable)

Minimum Number of Special Characters: (0 to 16, 2 = Default, 0 = Disable)

Maximum Number of Repeated Characters: (0 to 15, 0 = Default, 0 = Disable)

Maximum Number of Consecutive Characters: (0 to 15, 0 = Default, 0 = Disable)

Minimum Character Classes: (0 to 4, 4 = Default, 0 = Disable)

Keyword Exclusion

Display: rows Showing 0 to 0 of 0 entries Filter:

☐ Exclude Keyword Name

Table is Empty

First Previous Next Last

Table 10. Password Manager Fields

Field	Description
Rules Configuration	
Minimum Length	Passwords must have at least this many characters (0 to 64).
Aging (days)	The number of days that a user password is valid from the time the password is set. Once a password expires, the user is required to enter a new password at the next login.
History	The number of previous passwords that are retained to prevent password reuse. This helps to ensure that a user does not attempt to reuse the same password too often.

Field	Description
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 Complexity	
Strength Check	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 Number of Uppercase Letters	Specify the minimum number of uppercase letters a password must include.
Minimum Number of Lowercase Letters	Specify the minimum number of lowercase letters a password must include.
Minimum Number of Numeric Characters	Specify the minimum number of numbers a password must include.
Minimum Number of Special Characters	Specify the minimum number of special characters (non-alphanumeric, such as # or &) a password must include.
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> .
Maximum Number of Consecutive Characters	Specify the maximum number of consecutive characters a password is allowed to include. An example of four consecutive characters is <i>abcd</i>
Minimum Character Classes	Specify the minimum number of character classes a password must contain. There are four character classes: <ul style="list-style-type: none"> • Uppercase • Lowercase • Numbers • Special Characters
Keyword Exclusion	
Exclude Keyword Name	<p>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:</p> <ul style="list-style-type: none"> • To add a keyword to the list, click Add, type the word to exclude in the Exclude 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**.

4 Switching Features

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 pages to display port status, configure port settings, and view statistics on packets transmitted on the port.

Port Status

The Port Status page displays the operational and administrative status of each port and enables port configuration. To view this page, click **Switching** > **Port Configuration** in the navigation pane.

Figure 16. Port Status Page

StatusStatistics

Port Status

Help

Display 10 rows

Showing 1 to 10 of 34 entries

Filter:

<input type="checkbox"/>	Interface	Port Description	Type	Admin Mode	Physical Mode	Physical Status	Auto Negotiate Capabilities	STP Mode	LACP Mode	Link Status	MTU
<input type="checkbox"/>	1		Normal	Enabled	Auto	Unknown	10h 10f 100h 100f 1000f	Disabled	Enabled	Link Down	1500
<input type="checkbox"/>	2		Normal	Enabled	Auto	Unknown	10h 10f 100h 100f 1000f	Disabled	Enabled	Link Down	1500
<input type="checkbox"/>	3		Normal	Enabled	Auto	1000 Mbps	10h 10f 100h 100f 1000f	Disabled	Enabled	Link Up	1500
<input type="checkbox"/>	4		Normal	Enabled	Auto	Unknown	10h 10f 100h 100f 1000f	Disabled	Enabled	Link Down	1500
<input type="checkbox"/>	5		Normal	Enabled	Auto	Unknown	10h 10f 100h 100f 1000f	Disabled	Enabled	Link Down	1500
<input type="checkbox"/>	6		Normal	Enabled	Auto	Unknown	10h 10f 100h 100f 1000f	Disabled	Enabled	Link Down	1500
<input type="checkbox"/>	7		Normal	Enabled	Auto	Unknown	10h 10f 100h 100f 1000f	Disabled	Enabled	Link Down	1500
<input type="checkbox"/>	8		Normal	Enabled	Auto	Unknown	10h 10f 100h 100f 1000f	Disabled	Enabled	Link Down	1500
<input type="checkbox"/>	9		Normal	Enabled	Auto	1000 Mbps	10h 10f 100h 100f 1000f	Disabled	Enabled	Link Up	1500
<input type="checkbox"/>	10		Normal	Enabled	Auto	Unknown	10h 10f 100h 100f 1000f	Disabled	Enabled	Link Down	1500

First

Previous

1

2

3

4

Next

Last

Refresh

Edit

Table 11. Port Status Fields

Field	Description
Interface	The port or trunk ID.
Port Description	The current description, if any, associated with the interface to help identify it.

Field	Description
Type	<p>The interface type, which can be one of the following:</p> <ul style="list-style-type: none"> • Normal—The port is a normal port, which means it is not a Link Aggregation Group (LAG) member or configured for port mirroring. All ports are normal ports by default. • Trunk Member—The port is a member of a trunk. • Mirrored—The port is configured to mirror its traffic (ingress, egress, or both) to another port (the probe port). • Probe—The port is configured to receive mirrored traffic from one or more source ports.
Admin Mode	<p>The administrative mode of the interface. If a port or trunk is administratively disabled, it cannot forward traffic.</p> <ul style="list-style-type: none"> • Enabled: Administratively enabled. • Disabled: Administratively disabled. • D-Disabled: Automatically disabled by the system due to error conditions. For example, an interface may be disabled if it exceeded its rate limit. Please see error logs for more information.
Physical Mode	<p>The port speed and duplex mode. If the mode is Auto, the port's maximum capabilities are advertised, and the duplex mode and speed are set from the auto-negotiation process. The physical mode for a trunk is reported as "LAG."</p>
Physical Status	<p>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.</p>
Auto Negotiate Capabilities	<p>Indicates the list of configured capabilities for a port when Auto Negotiate is on. The Capability status for a trunk is not reported</p>
STP Mode	<p>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:</p> <ul style="list-style-type: none"> • Enable - Spanning tree is enabled for this port. • Disable - Spanning tree is disabled for this port.
LACP Mode	<p>Indicates the Link Aggregation Control Protocol administration state. The mode must be enabled in order for the port to participate in Link Aggregation. This field can have the following values:</p> <ul style="list-style-type: none"> • Enable: Specifies that the port is allowed to participate in a port channel (LAG), which is the default mode. • Disable: Specifies that the port cannot participate in a port channel (LAG). • N/A: For LAG ports.
Link Status	<p>Indicates whether the Link is up or down.</p>
MTU	<p>Indicates the Maximum Transmission Unit (MTU) of the interface, which is the largest frame size that can be transmitted on the port.</p> <p>The size does not include the Source MAC, the Destination MAC, the Ethernet Encapsulation, or the Ethernet FC.</p>
Edit Port Configuration Page (Additional Fields)	
Link Trap	<p>The physical speed (Mbps) at which the port is operating. If no link is present, this field is empty.</p>
Port Description	<p>The current description, if any, associated with the interface to help identify it.</p>

Field	Description
Storm Control Limits	
Broadcast Storm Recovery Level	<p>Specifies the broadcast storm control mode and threshold for the port. Broadcast storm control 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. Limits are defined as percentages or Packets Per Second (pps).</p> <p>The menu specifies the broadcast storm recovery action to take if a broadcast storm is detected on the interface. The options are:</p> <ul style="list-style-type: none"> • Shutdown: The interface which receives broadcast packets at a rate which is above the threshold is diagnostically disabled. • Trap: Sends trap messages at approximately every 30 seconds until broadcast storm control recovers. • None: No action is taken.
Multicast Storm Recovery Level	<p>Specifies the multicast storm control mode and threshold for the port. Multicast storm control 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. Limits are defined as percentages or Packets Per Second (pps).</p> <p>The menu specifies the multicast storm recovery action to take if a multicast storm is detected on the interface. The options are:</p> <ul style="list-style-type: none"> • Shutdown: The interface which receives multicast packets at a rate which is above the threshold is diagnostically disabled. • Trap: Sends trap messages at approximately every 30 seconds until multicast storm control recovers. • None: No action is taken.
Unicast Storm Recovery Level	<p>Specifies the unicast storm control mode and threshold for the port. Unicast storm control limits the amount of 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. Limits are defined as percentages or Packets Per Second (pps).</p> <p>The menu specifies the unicast storm recovery action to take if a unicast storm is detected on the interface. The options are:</p> <ul style="list-style-type: none"> • Shutdown: The interface which receives unicast packets at a rate which is above the threshold is diagnostically disabled. • Trap: Sends trap messages at approximately every 30 seconds until unicast storm control recovers. • None: No action is taken.

Modifying Interface Settings

To change the port configuration of one or more interfaces, select one or more interfaces and click **Edit**.

Figure 17. Edit Port Configuration Page

The screenshot shows the 'Edit Port Configuration' dialog box. It contains the following settings:

- Interface:** 3, 5
- Admin Mode:** ☒ Enabled ☐ Disabled
- Physical Mode:** Auto Negotiate (dropdown menu)
- STP Mode:** ☒ Enabled ☐ Disabled
- LACP Mode:** ☒ Enabled ☐ Disabled
- Link Trap:** ☒ Enabled ☐ Disabled
- MTU:** 1500 (range: 1500 to 9198)
- Port Description:** (empty text box, range: 0 to 64)

Storm Control Limits

Storm Type	Enabled	Disabled	Level	Unit	Action
Broadcast Storm Recovery Level	<input type="radio"/>	<input checked="" type="radio"/>	5	<input checked="" type="radio"/> Percent (%) <input type="radio"/> Packets (pps)	Shutdown
Multicast Storm Recovery Level	<input type="radio"/>	<input checked="" type="radio"/>	5	<input checked="" type="radio"/> Percent (%) <input type="radio"/> Packets (pps)	Shutdown
Unicast Storm Recovery Level	<input type="radio"/>	<input checked="" type="radio"/>	5	<input checked="" type="radio"/> Percent (%) <input type="radio"/> Packets (pps)	Shutdown

At the bottom, there are two buttons: **Apply** (highlighted in green) and **Cancel**.

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

Port Summary Statistics

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

To display the Port Summary Statistics page, click **Switching > Port Configuration** in the navigation pane and select the **Statistics** tab.

Figure 18. Port Summary Statistics Page

Interface	Received Packets w/o Error	Received Packets with Error	Broadcast Received Packets	Transmitted Packets w/o Error	Transmitted Packets with Error	Collisions	Transmitted Pause Frames	Received Pause Frames
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	49	0	5	1292	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	4255	0	55	3787	0	0	0	0
10	0	0	0	0	0	0	0	0

Table 12. Port Summary 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.
Transmitted Packets w/o Error	The number of packets transmitted out of that port without any packet errors.
Transmitted Packets with Error	The number of packets transmitted out of the port with packet errors.
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.)

Click **Clear All Counters** to reset all statistics to zero.

Port Mirroring

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



CAUTION:

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

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

Port Mirroring Configuration

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

Figure 19. Port Mirroring Page

The screenshot shows the 'Port Mirroring' configuration page. At the top, there are two tabs: 'Configuration' and 'Summary'. The 'Configuration' tab is active. Below the tabs, the page title 'Port Mirroring' is displayed on the left, and a 'Help' link is on the right. The main configuration area includes three fields: 'Session ID' with a dropdown menu showing '1', 'Mode' set to 'Disabled', and 'Destination Port' set to 'None'. Below these fields, there is a 'Display' dropdown set to 'All' and a 'Showing 0 to 0 of 0 entries' status. To the right of this is a 'Filter:' input field. Below the filter is a table header with a checkbox for 'Source Port(s)' and a 'Direction' dropdown. The table body is empty, displaying 'Table is Empty'. Below the table are navigation buttons: 'First', 'Previous', 'Next', and 'Last'. At the bottom of the page, there are five buttons: 'Refresh' (highlighted in green), 'Configure Session', 'Configure Destination', 'Configure Source', and 'Remove Source'.

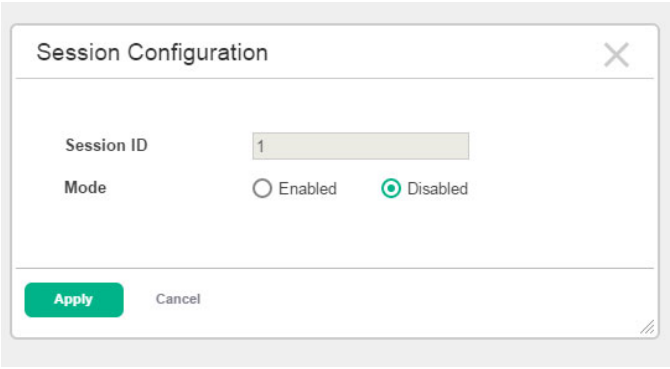
Table 13. Port Mirroring Fields

Field	Description
Session ID	The port mirroring session ID. Up to four port mirroring sessions are allowed.
Mode	The administrative mode for the selected port mirroring session. If the mode is disabled, the configured source is not mirroring traffic to the destination.
Destination Port	The switch port to which packets will be mirrored. Typically, a network protocol analyzer is connected to this port. <ul style="list-style-type: none">• Interface – If port configured as a interface or probe port. This port receives traffic from all configured source ports.• None – The destination is not configured.
Source Port(s)	The ports or VLAN configured to mirror traffic to the destination. You can configure multiple source ports or one source VLAN per session. The source VLAN can also be a remote VLAN.
Direction	The direction of traffic on the source port (or source ports) or VLAN that is sent to the specified destination. A source VLAN mirrors RX traffic only. Possible values for source ports are: <ul style="list-style-type: none">• Tx/Rx – Both ingress and egress traffic.• Rx – Ingress traffic only.• Tx – Egress traffic only.

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**.

Configuring a Port Mirroring Session

1. From the Port Mirroring page, select the Session ID for of the port mirroring session to configure.
2. Click **Configure Session** to display the **Session Configuration** page.

Figure 20. Configure Port Mirroring Session

The screenshot shows a 'Session Configuration' dialog box. It has a title bar with a close button. Inside, there is a 'Session ID' label followed by a text input field containing the number '1'. Below that is a 'Mode' label followed by two radio buttons: 'Enabled' and 'Disabled'. The 'Disabled' radio button is selected, indicated by a green dot. At the bottom of the dialog, there are two buttons: 'Apply' (in green) and 'Cancel'.

3. Enable or disable the selected port mirroring session.
4. Click **Apply** to apply the changes to the system.

Configuring a Port Mirroring Source

NOTE:

If an interface participates in some VLAN and is a LAG member, this VLAN cannot be assigned as a source VLAN for a Monitor session. At the same time, if an interface participates in some VLAN and this VLAN is assigned as a source VLAN for a Monitor session, the interface can be assigned as a LAG member.

1. From the Port Mirroring page, select the Session ID for of the port mirroring session to configure.
2. Click **Configure Source** to display the **Source Configuration** page.

Figure 21. Configure Port Mirroring Session Source

Source Configuration

Session ID: 1

Type: ☐ None ☐ VLAN ☒ Interface

VLAN ID: (1 to 4093)

Available Source Port(s): 1, 2, 3, 4, 5

Direction: ☒ Tx/Rx ☐ Rx ☐ Tx

Apply Cancel

3. Configure the following fields:

Field	Description
Type	The type of interface to use as the source: <ul style="list-style-type: none">• None – The source is not configured.• VLAN – Traffic to and from a configured VLAN is mirrored. In other words, all the packets sent and received on all the physical ports that are members of the VLAN are mirrored.• Interface – Traffic is mirrored from one or more physical ports on the device.
VLAN ID	The VLAN to use as the source. Traffic from all physical ports that are members of this VLAN is mirrored. This field is available only when the selected Type is VLAN.
Available Source port(s)	The physical port or ports to use as the source. To select multiple ports, CTRL + click each port. This field is available only when the selected Type is Interface.
Direction	The direction of traffic on the source port (or source ports) or VLAN that is sent to the specified destination. A source VLAN mirrors all received and transmitted packets to the destination. Possible values for source ports are: <ul style="list-style-type: none">• Tx/Rx – Both ingress and egress traffic.• Rx – Ingress traffic only.• Tx – Egress traffic only.

4. Click **Apply** to apply the changes to the system.

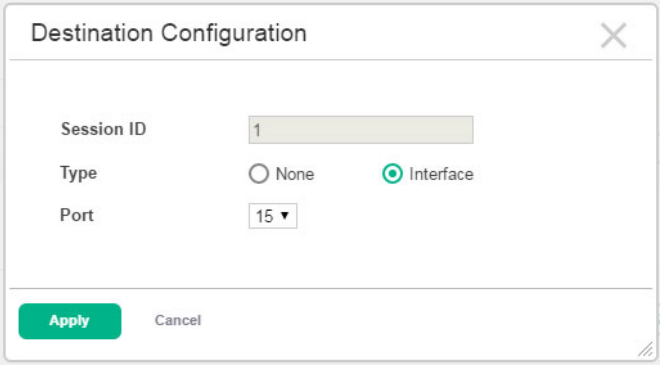
Configuring the Port Mirroring Session Destination

NOTE:

A port will be removed from a VLAN or LAG when it becomes a destination mirror.

1. From the Port Mirroring page, select the Session ID for of the port mirroring session to configure.
2. Click **Configure Destination** to display the **Destination Configuration** page.

Figure 22. Configure Port Mirroring Session Destination

A screenshot of a web-based configuration window titled "Destination Configuration". The window has a close button (X) in the top right corner. It contains three fields: "Session ID" with a text input containing the number "1"; "Type" with two radio buttons, "None" and "Interface", where "Interface" is selected; and "Port" with a dropdown menu showing "15". At the bottom, there are two buttons: "Apply" (highlighted in green) and "Cancel".

Session ID	1
Type	<input type="radio"/> None <input checked="" type="radio"/> Interface
Port	15 ▼
Apply Cancel	

3. To configure a port that receives the mirrored traffic, select **Interface** in the **Type** field, or select **None** to remove the configuration from a port.
4. If **Interface** is selected from the **Type** field, specify the port number of the interface to receive mirrored traffic.
5. Click **Apply** to apply the changes to the system.

Removing Source Ports from a Session

1. From the Port Mirroring page, select the Session ID for of the port mirroring session to configure.
2. Select one or more source ports to remove from the session.
3. Click **Remove Source**.

The source ports are removed from the port mirroring session, and the device is updated.

Port Mirroring Summary

The Port Mirroring Summary page displays summary information for all port mirroring sessions. To display the Port Mirroring Summary page, click **Switching** > **Port Mirroring** in the navigation pane and click the **Summary** tab.

Figure 23. Port Mirroring Summary Page

Configuration

Summary

Multiple Port Mirroring Summary

Help

Display

All

rows

Showing 1 to 4 of 4 entries

Filter:

↕ Session ID	↕ Admin Mode	↕ Probe Port	↕ Src VLAN	↕ Mirrored Port	↕ Direction
1	Enabled	16		19	Tx/Rx
1	Enabled	16		20	Tx/Rx
2	Disabled	3		4	Tx/Rx
3	Disabled				
4	Disabled				

First

Previous

1

Next

Last

Refresh

Table 14. Port Mirroring Summary Fields

Field	Description
Session ID	The port mirroring session ID. The number of sessions allowed is platform specific.
Admin Mode	The administrative mode for the selected port mirroring session. If the mode is disabled, the configured source is not mirroring traffic to the destination.
Probe Port	The interface that receives traffic from all configured source ports.
Src VLAN	The VLAN configured to mirror traffic to the destination. You can configure one source VLAN per session. The source VLAN can also be a remote VLAN.
Mirrored Port	The ports configured to mirror traffic to the destination. You can configure multiple source ports per session.
Direction	The type of traffic on the source port (or source ports) or VLAN that is sent to the specified destination. A source VLAN mirrors all received and transmitted packets to the destination. Possible values for source ports are: <ul style="list-style-type: none">Tx and Rx – Both ingress and egress traffic.Rx – Ingress traffic only.Tx – Egress traffic only.

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.

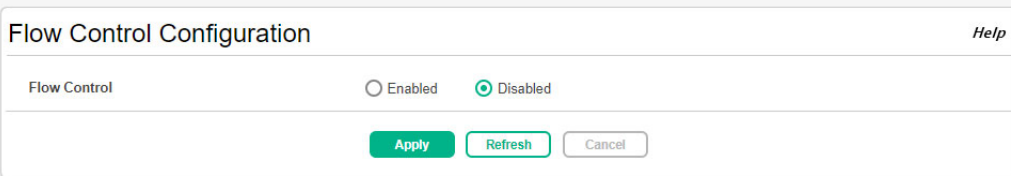
NOTE:

Flow control works well when the link speed is auto-negotiated. 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.

Use the Flow Control page to enable or disable this functionality. It is disabled by default and can be enabled globally on all switch ports.

To display the Flow Control page, click **Switching** > **Flow Control** in the navigation pane.

Figure 24. Flow Control Page

A screenshot of the 'Flow Control Configuration' web page. The page has a title bar with 'Flow Control Configuration' on the left and a 'Help' link on the right. Below the title bar, there is a section labeled 'Flow Control' with two radio buttons: 'Enabled' and 'Disabled'. The 'Disabled' radio button is selected, indicated by a green dot. At the bottom of the configuration area, there are three buttons: 'Apply' (green), 'Refresh' (green), and 'Cancel' (grey).

Select **Enabled** to use flow control on the switch. If you change this setting, click **Apply** to update the switch configuration. The change takes effect immediately but is not retained across a switch reset unless you click **Save Configuration**.

Spanning Tree

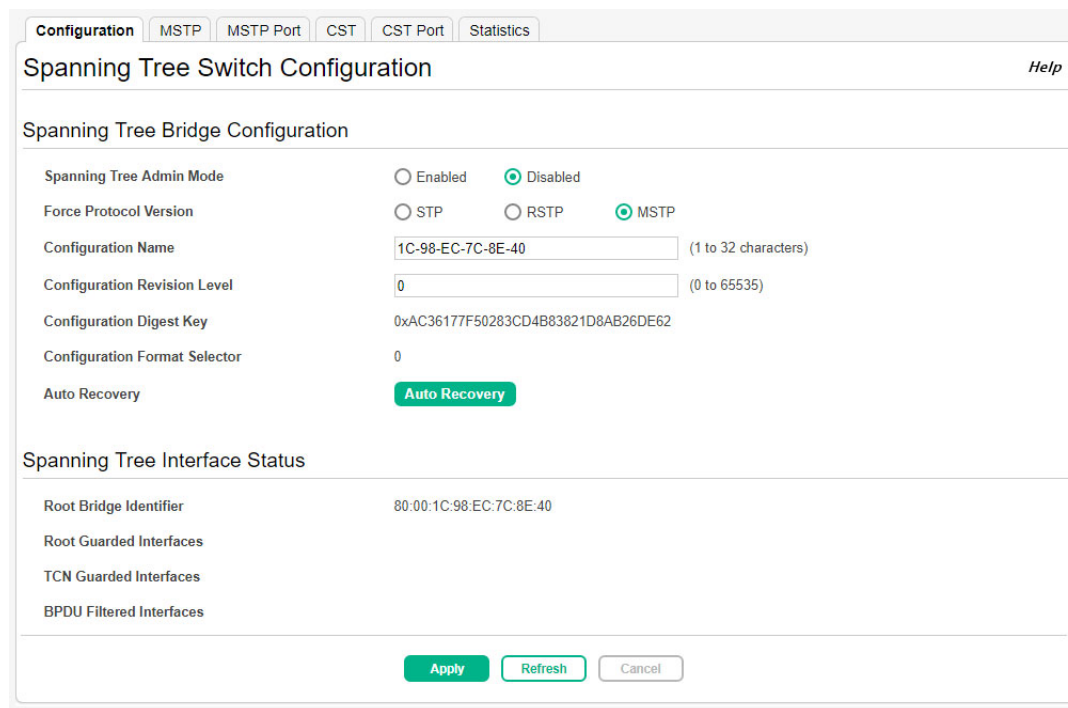
Spanning Tree Protocol (STP) is a Layer 2 protocol that provides a tree topology for switches on a bridged LAN. STP allows a network to have redundant paths without the risk of network loops. STP uses the spanning-tree algorithm to provide a single path between end stations on a network. When STP is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

HPE OfficeConnect 1920S series switches support STP versions IEEE 802.1D (STP), and 802.1w (Rapid STP, or RSTP). 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 interoperate with switches running the STP protocol by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

Spanning Tree Switch Configuration

To display the Spanning Tree Switch Configuration page, click **Switching > Spanning Tree** in the navigation pane, and make sure the **Configuration** tab is selected. This page includes information about global STP settings and interface status information.

Figure 25. Spanning Tree Switch Configuration Page



Configuration | MSTP | MSTP Port | CST | CST Port | Statistics

Spanning Tree Switch Configuration Help

Spanning Tree Bridge Configuration

Spanning Tree Admin Mode: ☐ Enabled ☒ Disabled

Force Protocol Version: ☐ STP ☐ RSTP ☒ MSTP

Configuration Name: (1 to 32 characters)

Configuration Revision Level: (0 to 65535)

Configuration Digest Key:

Configuration Format Selector:

Auto Recovery: [Auto Recovery](#)

Spanning Tree Interface Status

Root Bridge Identifier:

Root Guarded Interfaces

TCN Guarded Interfaces

BPDU Filtered Interfaces

[Apply](#) [Refresh](#) [Cancel](#)

Table 15. Spanning Tree Switch Configuration Fields

Field	Description
Spanning Tree Bridge Configuration	
Spanning Tree Admin Mode	The administrative mode of STP on the device. When enabled, the device 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.
Force Protocol Version	The STP version the device uses, which is one of the following: <ul style="list-style-type: none"> • 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. • 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.
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.
Configuration Digest Key	The 16 byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID-to-MST ID mapping).
Configuration Format Selector	The version of the configuration format being used in the exchange of BPDUs.
Auto Recovery	Click Auto Recovery to redirect your browser to the Auto Recovery Configuration page. For more information about the Auto Recovery feature, see “Auto Recovery Configuration” on page 86 .
Spanning Tree Interface Status	
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.
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.

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**.

Spanning Tree MSTP Summary

Multiple Spanning Tree Protocol (MSTP) allows the creation of MSTIs based upon a VLAN or groups of VLANs. Configuring MSTIs 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 Summary page, click **Switching** > **Spanning Tree** in the navigation pane, and then click the **MSTP** tab.

Figure 26. Spanning Tree MSTP Summary Page

⚙ MSTP ID ⚙	⚙ Priority ⚙	⚙ # of Associated VLANs ⚙	⚙ Bridge Identifier ⚙	⚙ Time Since Topology Change ⚙	⚙ Designated Root ⚙	⚙ Root Path Cost ⚙	⚙ Root Port ⚙
1	20480	3	50:01:1C:98:EC:7C:8E:40	0d:00:03:59	50:01:1C:98:EC:7C:8E:40	0	00:00

Table 16. Spanning Tree MSTP Summary Fields

Field	Description
MSTP ID	The number that identifies the MST 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 device 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**.

Spanning Tree MSTP Port Summary

To display the Spanning Tree MSTP Port Summary page, click **Switching** > **Spanning Tree** in the navigation pane, and then click the **MSTP Port** tab.

Figure 27. Spanning Tree MSTP Port Summary Page

Configuration MSTP **MSTP Port** CST CST Port Statistics

Spanning Tree MSTP Port Summary Help

MSTP ID: 1

Display 10 rows Showing 11 to 20 of 34 entries Filter:

<input type="checkbox"/>	Interface	Port Role	Port Forwarding State	Port Priority	Port Path Cost
<input type="checkbox"/>	11	Disabled	Disabled	128	0
<input type="checkbox"/>	12	Disabled	Disabled	128	0
<input type="checkbox"/>	13	Disabled	Disabled	128	0
<input type="checkbox"/>	14	Disabled	Disabled	128	0
<input type="checkbox"/>	15	Disabled	Disabled	128	0
<input type="checkbox"/>	16	Disabled	Manual Forwarding	128	0
<input type="checkbox"/>	17	Disabled	Disabled	128	0
<input type="checkbox"/>	18	Disabled	Disabled	128	0
<input type="checkbox"/>	19	Disabled	Disabled	128	0
<input type="checkbox"/>	20	Disabled	Disabled	128	0

First Previous 1 2 3 4 Next Last

Refresh Edit Details

Table 17. Spanning Tree MSTP Port Summary Fields

Field	Description
MSTP ID	The menu contains the ID of each MST instance that has been created on the device.
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: <ul style="list-style-type: none">• 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.
Port Forwarding State	<ul style="list-style-type: none">• 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 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.

From the Spanning Tree MSTP Port Summary page, you can view additional details about the MSTP settings on a port or configure additional settings for one or more ports.

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. 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**.

The fields on the Edit MSTP Port page and Details of MSTP Port Entry page are the same.

Figure 28. Edit MSTP Port Page

Edit MSTP Port Entry

MSTP ID

1

Interface

3

Port Priority

128

Port Path Cost

0

(0 to 200000000)

Auto-calculate Port Path Cost

Enabled

Port ID

80:03

Port Up Time Since Counters Last Cleared

0d:00:10:59

Port Mode

Enabled

Disabled

Port Forwarding State

Disabled

Port Role

Disabled

Designated Root

80:01:9C:DC:71:AE:00:F4

Designated Cost

0

Designated Bridge

80:01:9C:DC:71:AE:00:F4

Designated Port

00:00

Loop Inconsistent State

False

Transitions Into Loop Inconsistent State

0

Transitions Out Of Loop Inconsistent State

0

Apply

Cancel

Table 18. Spanning Tree MSTP Port Edit and 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.
Port Up Time Since Counters Last Cleared	The amount of time that the port has been up since the counters were cleared.
Port Mode	The administrative mode of spanning tree on the port.
Port Forwarding State	<ul style="list-style-type: none"> • 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	<p>The role of the port within the MST, which is one of the following:</p> <ul style="list-style-type: none"> • 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.
Loop Inconsistent State	Identifies whether the interface is currently in a loop inconsistent state. An interface transitions to a loop inconsistent state if loop guard is enabled and the port stops receiving BPDUs. In this state, the interface does not transmit frames.
Transitions Into LoopInconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out Of LoopInconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

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**.

CST Configuration

Use the Spanning Tree CST Configuration page to configure the Common Spanning Tree (CST) settings. The settings and information on this page define the device within the spanning tree topology that connects all STP/RSTP bridges and MSTP regions.

To display the CST Configuration page, click **Switching** > **Spanning Tree** in the navigation pane, and then click the **CST** tab.

Figure 29. Spanning Tree CST Configuration Page

Configuration MSTP MSTP Port **CST** CST Port Statistics

Spanning Tree CST Configuration [Help](#)

Bridge Priority 32768 ▼

Bridge Max Age 20 (6 to 40)

Bridge Hello Time 2

Bridge Forward Delay 15 (4 to 30)

Spanning Tree Maximum Hops 20 (6 to 40)

BPDU Guard ☐

BPDU Filter ☐

Spanning Tree Tx Hold Count 6 (1 to 10)

Bridge Identifier 80:00:1C:98:EC:7C:8E:40

Time Since Topology Change 0d:00:17:06

Topology Change Count 0

Topology Change False

Designated Root 80:00:1C:98:EC:7C:8E:40

Root Path Cost 0

Root Port 00:00

Max Age 20

Forward Delay 15

Hold Time 6

CST Regional Root 80:00:1C:98:EC:7C:8E:40

CST Path Cost 0

[Apply](#) [Refresh](#) [Cancel](#)

Table 19. Spanning Tree CST Configuration Fields

Field	Description
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.
Bridge Max Age	The amount of time a bridge waits before implementing a topological change.
Bridge Hello Time	The amount of time the root bridge waits between sending hello BPDUs.
Bridge Forward Delay	The amount of time a bridge remains in a listening and learning state before forwarding packets.
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.

Field	Description
BPDU Guard	When enabled, BPDU Guard can disable edge ports that receive BPDU packets. This prevents a new device from entering the existing STP topology. Thus devices that were originally not a part of STP are not allowed to influence the STP topology.
BPDU Filter	When enabled, this feature filters the BPDU traffic on the edge ports. When spanning tree is disabled on a port, BPDU filtering allows BPDU packets received on that port to be dropped.
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 device was last reset.
Topology Change Count	The number of times the topology of the spanning tree has changed.
Topology Change	Indicates whether a topology change is in progress on any port assigned to the CST. If a change is in progress the value is True; otherwise, it is False.
Designated Root	The bridge identifier of the root bridge for the CST. 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 the CST. Traffic from a connected device 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 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.

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**.

CST Port Summary

Use the CST Port Summary page to view and configure the Common Spanning Tree (CST) settings for each interface on the device. 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 display the Spanning Tree CST Port Configuration/Status page, click **Switching > Spanning Tree** in the navigation pane, and then click the **CST Port** tab.

Figure 30. Spanning Tree CST Port Summary Page

Configuration	MSTP	MSTP Port	CST	CST Port	Statistics
Spanning Tree CST Port Summary					Help
Display 10 rows		Showing 11 to 20 of 34 entries		Filter: <input type="text"/>	
<input type="checkbox"/>	Interface	Port Role	Port Forwarding State	Port Priority	Port Path Cost
<input type="checkbox"/>	11	Disabled	Disabled	128	0
<input type="checkbox"/>	12	Disabled	Disabled	128	0
<input type="checkbox"/>	13	Disabled	Disabled	128	0
<input type="checkbox"/>	14	Disabled	Disabled	128	0
<input type="checkbox"/>	15	Disabled	Disabled	128	0
<input type="checkbox"/>	16	Root	Forwarding	128	20000
<input type="checkbox"/>	17	Disabled	Disabled	128	0
<input type="checkbox"/>	18	Disabled	Disabled	128	0
<input type="checkbox"/>	19	Disabled	Disabled	128	0
<input type="checkbox"/>	20	Disabled	Disabled	128	0
First Previous 1 2 3 4 Next Last					
Refresh Edit Details					

Table 20. Spanning Tree CST Port Summary 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	<p>The role of the port within the CST, which is one of the following:</p> <ul style="list-style-type: none">• 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.
Port Forwarding State	<ul style="list-style-type: none">• 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 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 port to the root bridge.

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**.

Viewing CST Port Details or Editing CST Port Settings

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

The fields on the Edit CST Port Entry page and Details of CST Port Entry page are the same.

Figure 31. Edit CST Port Entry Page

Edit CST Port Entry

Interface

3

Port Priority

128

Admin Edge Port

☐

Port Path Cost

0

(0 to 200000000; 0 for Auto)

Auto-calculate Port Path Cost

Enabled

Hello Timer

2

External Port Path Cost

20000

(0 to 200000000; 0 for Auto)

Auto-calculate External Port Path Cost

Disabled

BPDU Filter

☐

BPDU Guard Effect

Disabled

Port ID

80:03

Port Up Time Since Counters Last Cleared

0d:00:03:37

Port Mode

☒ Enabled ☐ Disabled

Port Forwarding State

Forwarding

Port Role

Designated

Designated Root

80:00:E0:07:1B:52:91:80

Designated Cost

0

Designated Bridge

80:00:E0:07:1B:52:91:80

Designated Port

80:03

Topology Change Acknowledge

False

Auto Edge

☒

Edge Port

Enabled

Point-to-point MAC

True

Root Guard

☐

Loop Guard

☐

TCN Guard

☐

CST Regional Root

80:00:E0:07:1B:52:91:80

CST Path Cost

0

Loop Inconsistent State

False

Transitions Into Loop Inconsistent State

0

Transitions Out Of Loop Inconsistent State

0

Apply

Cancel

Table 21. Spanning Tree CST Port Edit and 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.
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.
Admin Edge Port	Select this option administratively configure the interface as an edge port. An edge port is an interface that is directly connected to a host and is not at risk of causing a loop.
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).
Hello Timer	The amount of time the port waits between sending hello BPDUs.
External Port Path Cost	The cost of the path from the port to the CIST root. This value becomes important when the network includes multiple regions.
Auto-calculate External Port Path Cost	Shows whether the path cost from the port to the CIST root 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 edge ports. Edge ports do not need to participate in the spanning tree, so BPDU filtering allows BPDU packets received on edge ports to be dropped.
BPDU Guard Effect	Shows the status of BPDU Guard Effect on the interface. When enabled, BPDU Guard Effect can disable edge ports that receive BPDU packets. This prevents a new device from entering the existing STP topology. Thus devices that were originally not a part of STP are not allowed to influence the STP topology.
Port ID	A unique value that is automatically generated based on the port priority value and the interface index.
Port Up Time Since Counters Last Cleared	The amount of time that the port has been up since the counters were cleared.
Port Mode	The administrative mode of spanning tree on the port.
Port Forwarding State	<ul style="list-style-type: none"> • 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	<p>The role of the port within the CST, which is one of the following:</p> <ul style="list-style-type: none"> • 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.

Field	Description
Designated Bridge	The bridge ID of the bridge with the designated port.
Designated Port	The port ID of the designated port.
Topology Change Acknowledge	Indicates whether the next BPDU to be transmitted for this port will have the topology change acknowledgment flag set.
Auto Edge	When enabled, Auto Edge allows the interface to become an edge port if it does not receive any BPDUs within a given amount of time.
Edge Port	Indicates whether the interface is configured as an edge port (Enabled).
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 device from changing. The port gets put into discarding state and does not forward any frames.
Loop Guard	When enabled, Loop Guard prevents an interface from erroneously transitioning from blocking state to forwarding when the interface stops receiving BPDUs. The port is marked as being in loop-inconsistent state. In this state, the interface does not forward 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.
Loop Inconsistent State	Identifies whether the interface is currently in a loop inconsistent state. An interface transitions to a loop inconsistent state if loop guard is enabled and the port stops receiving BPDUs. In this state, the interface does not transmit frames.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out Of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

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**.

Spanning Tree Statistics

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

To display the Spanning Tree Statistics page, click **Switching** > **Spanning Tree** in the navigation pane, and click the **Statistics** tab.

Figure 32. Spanning Tree Statistics Page

ConfigurationMSTMSTP PortCSTCST PortStatistics

Spanning Tree StatisticsHelp

Display 10 rowsShowing 11 to 20 of 34 entriesFilter:

Interface	STP BPDUs Rx	STP BPDUs Tx	RSTP BPDUs Rx	RSTP BPDUs Tx	MSTP BPDUs Rx	MSTP BPDUs Tx
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	47	0	0	5
17	0	0	0	0	0	0
18	0	0	0	0	0	0
19	0	0	0	0	0	0
20	0	0	0	0	0	0

FirstPrevious1234NextLast

Refresh

Table 22. Spanning Tree Statistics Fields

Field	Description
Interface	The port or trunk associated with the rest of the data in the row.
STP BPDUs Rx	The number of classic STP (IEEE 802.1d) BPDUs received by the interface.
STP BPDUs Tx	The number of classic STP BPDUs sent by the interface.
RSTP BPDUs Rx	The number of RSTP (IEEE 802.1w) BPDUs received by the interface.
RSTP BPDUs Tx	The number of RSTP BPDUs sent by the interface.
MSTP BPDUs Rx	The number of MSTP (IEEE 802.1s) BPDUs received by the interface.
MSTP BPDUs Tx	The number of MSTP BPDUs sent by the interface.

Loop Protection

Loops on a network consume resources and can degrade network performance. Detecting loops manually can be very cumbersome and time consuming. The HPE OfficeConnect 1920S series switch software provides an automatic loop protection feature.

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. When an interface receives a loop protection PDU, it compares the source MAC address with its own. If the MAC addresses match, a loop is detected and a configured action is taken, which may include shutting down the port for a specified period.

An interface can be configured to receive and take action in response to loop protection PDUs, but not to send out the PDUs itself.

Ports on which loop protection is disabled drop the loop protection packets silently.

Loop Protection Status

Use the Loop Protection Status page to display the status of this feature on each port. To display this page, click **Switching > Loop Protection** in the navigation pane.

Figure 33. Loop Protection Status Page

Status

Configuration

Loop Protection Status

Help

Display10▼rows

Showing 1 to 10 of 34 entries

Filter:

↕Interface	↕Loop Protection	↕Configured Action Taken	↕Tx Mode	↕Loop Count	↕Status	↕Loop	↕Time of Last Loop
1	Disabled	Shutdown Port	Enabled	0	Link Down		01/01/1970 00:00:00
2	Disabled	Shutdown Port	Enabled	0	Link Down		01/01/1970 00:00:00
3	Disabled	Shutdown Port	Enabled	0	Link Up		01/01/1970 00:00:00
4	Disabled	Shutdown Port	Enabled	0	Link Down		01/01/1970 00:00:00
5	Disabled	Shutdown Port	Enabled	0	Link Down		01/01/1970 00:00:00
6	Disabled	Shutdown Port	Enabled	0	Link Down		01/01/1970 00:00:00
7	Disabled	Shutdown Port	Enabled	0	Link Down		01/01/1970 00:00:00
8	Disabled	Shutdown Port	Enabled	0	Link Down		01/01/1970 00:00:00
9	Disabled	Shutdown Port	Enabled	0	Link Up		01/01/1970 00:00:00
10	Disabled	Shutdown Port	Enabled	0	Link Down		01/01/1970 00:00:00

First

Previous

1

2

3

4

Next

Last

Refresh

Table 23. Loop Protection Status 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.
Configured Action Taken	The action that is set to occur when a loop is detected on the port with loop protection enabled: <ul style="list-style-type: none"> Shutdown Port—The port will be shut down for the configured period. This is the default. Shutdown Port and Log—The event will be logged and the port is shut down for the configured period. Log Only—The event will be logged and the port remains operational.
Tx Mode	Indicates whether the interface is configured (Enabled) to send out loop protection protocol data units (PDUs) to actively detect loops. When disabled, the interface does not send out loop protection PDUs but can receive them from other ports. Tx Mode is enabled by default.
Loop Count	The number of loops detected on this interface since the last system boot or since statistics were cleared.
Status	The current loop protection status of the port. Link Up indicates the interface is operating normally. Link Down indicates that the port has been shut down due to the detection of a loop.
Loop	Whether a loop is currently detected on the port.
Time of Last Loop	The date and time of the last loop event detected.

Loop Protection Configuration

Use the Loop Protection Configuration page to configure this feature on one or more interfaces. To display this page, click **Switching > Loop Protection** in the navigation pane and select the **Configuration** tab.

Figure 34. Loop Protection Configuration Page

Status

Configuration

Loop Protection Configuration

Help

Loop Protection

☐ Enabled
☒ Disabled

Transmission Time (Seconds)

5 (1 to 10)

Shutdown Time (Seconds)

180 (0 to 604800)

Display 10 rows

Showing 1 to 10 of 34 entries

Filter:

<input type="checkbox"/>	↕ Interface	↕ Loop Protection	↕ Action	↕ Tx Mode	↕ Status	↕ Loop	↕ Time of Last Loop
<input type="checkbox"/>	1	Disabled	Shutdown Port	Enabled	Link Down		01/01/1970 00:00:00
<input type="checkbox"/>	2	Disabled	Shutdown Port	Enabled	Link Down		01/01/1970 00:00:00
<input type="checkbox"/>	3	Disabled	Shutdown Port	Enabled	Link Up		01/01/1970 00:00:00
<input type="checkbox"/>	4	Disabled	Shutdown Port	Enabled	Link Down		01/01/1970 00:00:00
<input type="checkbox"/>	5	Disabled	Shutdown Port	Enabled	Link Down		01/01/1970 00:00:00
<input type="checkbox"/>	6	Disabled	Shutdown Port	Enabled	Link Down		01/01/1970 00:00:00
<input type="checkbox"/>	7	Disabled	Shutdown Port	Enabled	Link Down		01/01/1970 00:00:00
<input type="checkbox"/>	8	Disabled	Shutdown Port	Enabled	Link Down		01/01/1970 00:00:00
<input type="checkbox"/>	9	Disabled	Shutdown Port	Enabled	Link Up		01/01/1970 00:00:00
<input type="checkbox"/>	10	Disabled	Shutdown Port	Enabled	Link Down		01/01/1970 00:00:00

First

Previous

1

2

3

4

Next

Last

Apply

Refresh

Edit

Edit All

Table 24. Loop Protection Configuration Global 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 that are enabled to send them. The range is 1 to 10 seconds and the default is 5 seconds.
Shutdown Time	The period that a port is shut down when a loop is detected. This setting applies only to ports that are configured to be shut down upon the detection of a loop. The range is 0 to 604800 seconds and the default is 180 seconds.

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**.

Configuring Loop Protection Settings on Interfaces

To configure loop protection settings on one or more interfaces, select the interfaces and click **Edit**.

Figure 35. Edit Loop Protection Port Configuration Page

The screenshot shows a dialog box titled "Edit Loop Protection Port Configuration" with a close button (X) in the top right corner. The dialog contains the following configuration options:

- Interface:** 4
- Loop Protection:** Two radio buttons are present: "Enabled" (unselected) and "Disabled" (selected).
- Action:** A dropdown menu showing "Shutdown Port".
- Tx Mode:** Two radio buttons are present: "Enabled" (selected) and "Disabled" (unselected).

At the bottom of the dialog, there are two buttons: "Apply" (highlighted in green) and "Cancel".

Table 25. Edit Loop Protection Port Configuration Fields

Field	Description
Interface	The port or ports that are being configured.
Loop Protection	Select Enabled or Disabled to administratively enable or disable this feature on the selected interfaces. By default, this feature is disabled on all interfaces. Note that loop protection can be enabled on static trunks, but cannot be enabled on trunks that are dynamically formed through LACP.
Action	Select the action to occur when a loop is detected on a port with loop protection enabled: <ul style="list-style-type: none">• Shutdown Port—The port will be shut down for the configured period. This is the default selection.• Shutdown Port and Log—The event will be logged and the port is shut down for the configured period.• Log Only—The event will be logged and the port remains operational.
Tx Mode	When set to Enabled (the default), the port actively sends out loop protection PDUs to other ports on which the loop protection feature is enabled. When set to Disabled , the port does not send loop protection PDUs but can receive them from other ports. Tx Mode is enabled by default.

Click **Apply** to update the 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 device 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.

When enabled, the switch supports IGMPv1 and IGMPv2.

IGMP Snooping Global Configuration

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

Figure 36. IGMP Snooping Page

Configuration | Interface Configuration | Multicast Router Configuration | VLAN Configuration | Multicast Router VLAN Configuration

IGMP Snooping Help

IGMP Snooping ☐ Enabled ☒ Disabled

Multicast Control Frame Count 0

Interfaces Enabled for IGMP Snooping 7, 8, 9

VLANs Enabled for IGMP Snooping 10

Apply Refresh Cancel

Table 26. IGMP Snooping Fields

Field	Description
IGMP Snooping	Select Enabled to globally enable IGMP snooping on the switch. This feature is disabled by default.
Multicast Control Frame Count	The number of multicast control frames that have been processed by the CPU since the switch was last reset.
Interfaces Enabled for IGMP Snooping	Identifies the interfaces on which IGMP snooping is administratively enabled. If IGMP snooping is not enabled on any interfaces, this field does not display a value. IGMP snooping must be enabled globally and on an interface for the interface to be able to snoop IGMP packets to determine which segments should receive multicast packets directed to the group address.
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 does not display a value.

If you change the Admin Mode, 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**.

IGMP Snooping Interface Configuration

Use the IGMP snooping **Interface Configuration** page to configure IGMP snooping settings on specific interfaces.

To access the page, click **Switching > IGMP Snooping** in the navigation pane and select the **Interface Configuration** tab.

Figure 37. IGMP Snooping Interface Configuration Page

Configuration Interface Configuration Multicast Router Configuration VLAN Configuration Multicast Router VLAN Configuration

IGMP Snooping Interface Configuration Help

Display rows Showing 1 to 10 of 68 entries Filter:

<input type="checkbox"/>	↕ Interface	↕ Admin Mode	↕ Group Membership Interval	↕ Max Response Time	↕ Multicast Router Expiration Time	↕ Fast Leave Admin Mode
<input type="checkbox"/>	1	Disable	260	10	0	Disable
<input type="checkbox"/>	2	Disable	260	10	0	Disable
<input type="checkbox"/>	3	Disable	260	10	0	Disable
<input type="checkbox"/>	4	Disable	260	10	0	Disable
<input type="checkbox"/>	5	Disable	260	10	0	Disable
<input type="checkbox"/>	6	Disable	260	10	0	Disable
<input type="checkbox"/>	7	Enable	260	10	0	Disable
<input type="checkbox"/>	8	Enable	260	10	0	Disable
<input type="checkbox"/>	9	Enable	260	10	0	Disable
<input type="checkbox"/>	10	Disable	260	10	0	Disable

First Previous 1 2 3 4 5 Next Last

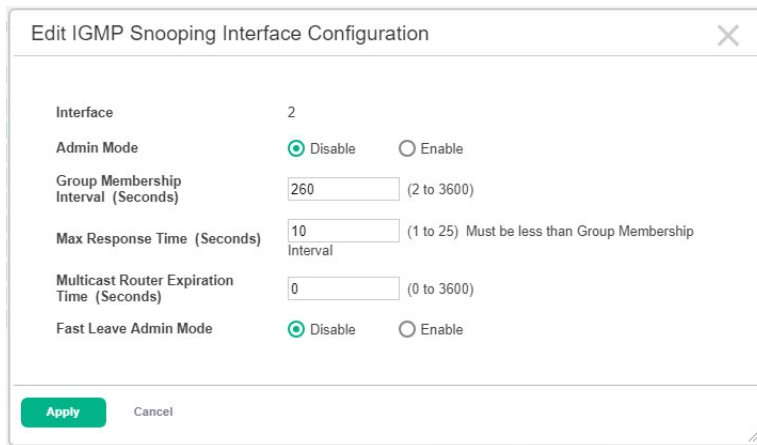
Table 27. IGMP Snooping Interface Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring IGMP snooping settings, this field identifies the interface(s) that are being configured.
Admin Mode	The administrative mode of IGMP snooping on the interface. IGMP snooping must be enabled globally and on an interface for the interface to be able to snoop IGMP packets to determine which segments should receive multicast packets directed to the group address.
Group Membership Interval	The number of seconds the interface should wait for a report for a particular group on the interface before the IGMP snooping feature deletes the interface from the group.
Max Response Time	The number of seconds the interface should wait after sending a query if it does not receive a report for a particular group. The specified value should be less than the Group Membership Interval.
Multicast Router Expiration Time	The number of seconds the interface should wait to receive a query before it is removed from the list of interfaces with multicast routers attached.
Fast Leave Admin Mode	The administrative mode of Fast Leave on the interface. If Fast Leave is enabled, the 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.

Configuring IGMP Snooping Settings on Interfaces

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

Figure 38. Edit IGMP Snooping Interface Configuration Page



The dialog box titled "Edit IGMP Snooping Interface Configuration" contains the following settings:

- Interface: 2
- Admin Mode: ☒ Disable ☐ Enable
- Group Membership Interval (Seconds): 260 (2 to 3600)
- Max Response Time (Seconds): 10 (1 to 25) Must be less than Group Membership Interval
- Multicast Router Expiration Time (Seconds): 0 (0 to 3600)
- Fast Leave Admin Mode: ☒ Disable ☐ Enable

Buttons: Apply, Cancel

Click **Apply** to save the changes for the current boot session. 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**.

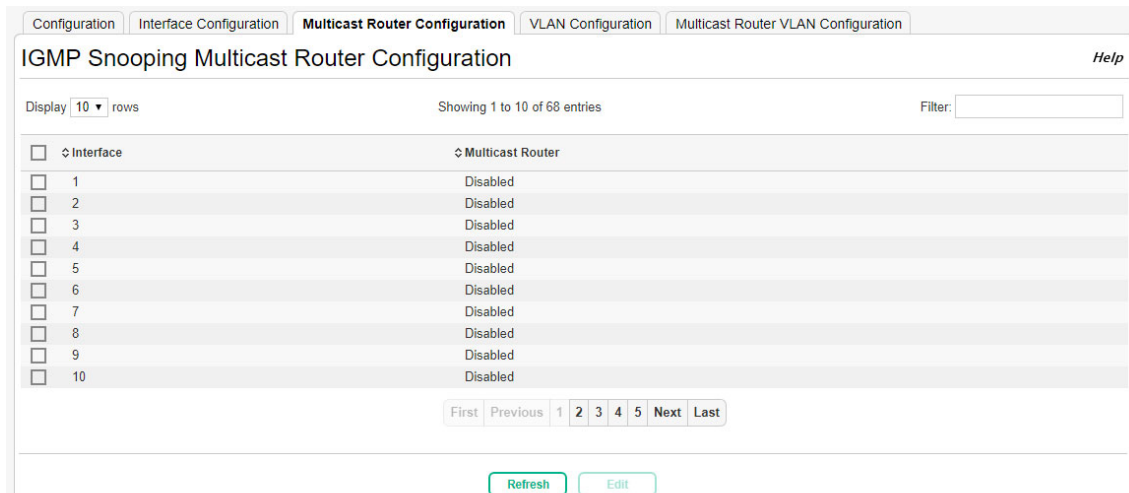
Multicast Router Configuration

Use this page to manually configure an interface as a static 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 page, click **Switching > IGMP Snooping** in the navigation pane and select the **Multicast Router Configuration** tab.

Figure 39. IGMP Snooping Multicast Router Configuration Page



The page shows the "Multicast Router Configuration" tab selected. It displays a table of interfaces and their multicast router status.

Interface	Multicast Router
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled

Buttons: Refresh, Edit

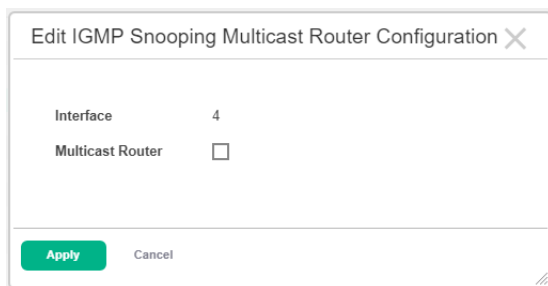
Table 28. IGMP Snooping Multicast Router Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When configuring the IGMP snooping multicast router settings, this field identifies the interface(s) that are being configured
Multicast Router	Indicates whether the interface is enabled or disabled as a multicast router interface.

Configuring Multicast Router Settings on Interfaces

To change the multicast router mode for one or more interfaces, select each entry to modify and click **Edit**.

Figure 40. Edit IGMP Snooping Multicast Router Configuration Page



Dialog box titled "Edit IGMP Snooping Multicast Router Configuration" with a close button (X). The dialog contains two fields: "Interface" with the value "4" and "Multicast Router" with an unchecked checkbox. At the bottom, there are "Apply" and "Cancel" buttons.

Click **Apply** to save the changes for the current boot session. 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**.

IGMP Snooping VLAN Configuration

Use the IGMP snooping **VLAN Status** page to enable or disable IGMP snooping on system VLANs and to view and configure per-VLAN IGMP snooping settings. Only VLANs that are enabled for IGMP snooping appear in the table.

To access the page, click **Switching > IGMP Snooping** in the navigation pane and select the **VLAN Configuration** tab.

Figure 41. IGMP Snooping VLAN Status Page

<input type="checkbox"/>	VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval (Seconds)	Max Response Time (Seconds)	Multicast Router Expiration Time (Seconds)	Report Suppression Mode
<input type="checkbox"/>	10	Enabled	Enabled	1024	10	0	Enabled

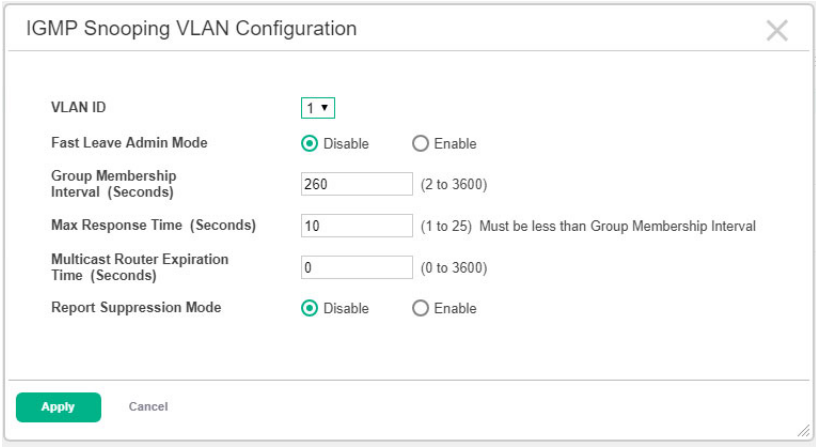
Table 29. IGMP Snooping VLAN Status Fields

Field	Description
VLAN	The VLAN associated with the rest of the data in the row. When enabling IGMP snooping on a VLAN, use this menu to select the desired VLAN. Only VLANs that have been configured on the system and are not already enabled for IGMP snooping appear in the menu. When modifying IGMP snooping settings, this field identifies the VLAN that is being configured.
Admin Mode	The administrative mode of IGMP snooping on the VLAN. IGMP snooping must be enabled globally and on a VLAN for the VLAN to be able to snoop IGMP packets to determine which network segments should receive multicast packets directed to the group address.
Fast Leave Admin Mode	The administrative mode of Fast Leave on the VLAN. If Fast Leave is enabled, the VLAN 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.
Group Membership Interval	The number of seconds the VLAN should wait for a report for a particular group on the VLAN before the IGMP snooping feature deletes the VLAN from the group.
Max Response Time	The number of seconds the VLAN should wait after sending a query if it does not receive a report for a particular group. The specified value should be less than the Group Membership Interval.
Multicast Router Expiration Time	The number of seconds the VLAN should wait to receive a query before it is removed from the list of VLANs with multicast routers attached.
Report Suppression Mode	<p>The IGMPv1 and IGMPv2 report suppression mode. The device uses IGMP report suppression to limit the membership report traffic sent to multicast-capable routers. When this mode is enabled, the device does not send duplicate reports to the multicast router. Note that this mode is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports. The options are as follows:</p> <ul style="list-style-type: none">• Enabled - Only the first IGMP report from all hosts for a group IGMP report is forwarded to the multicast routers.• Disabled - The device forwards all IGMP reports from all hosts in a multicast group to the multicast routers.

Enabling IGMP Snooping on a VLAN

To enable IGMP snooping on a VLAN, click **Add** and configure the settings in the available fields. Use the VLAN ID drop down to select the desired VLAN.

Figure 42. IGMP Snooping VLAN Configuration Page



The dialog box titled "IGMP Snooping VLAN Configuration" contains the following fields and controls:

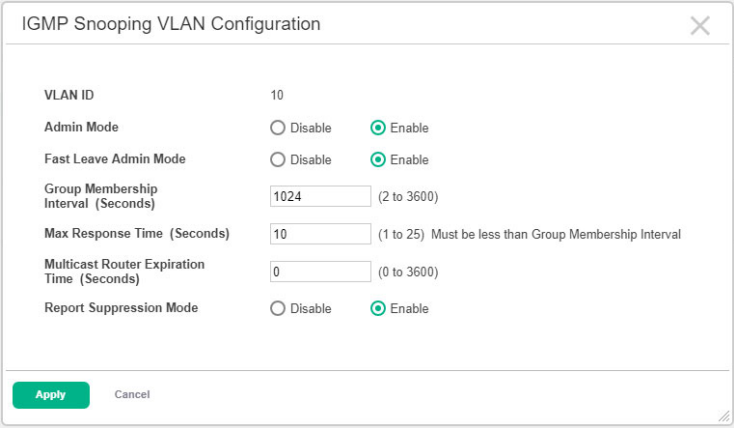
- VLAN ID:** A dropdown menu showing "1".
- Fast Leave Admin Mode:** Radio buttons for "Disable" (selected) and "Enable".
- Group Membership Interval (Seconds):** A text input field with "260" and a range "(2 to 3600)".
- Max Response Time (Seconds):** A text input field with "10" and a range "(1 to 25) Must be less than Group Membership Interval".
- Multicast Router Expiration Time (Seconds):** A text input field with "0" and a range "(0 to 3600)".
- Report Suppression Mode:** Radio buttons for "Disable" (selected) and "Enable".
- Buttons:** "Apply" (green) and "Cancel" (grey) at the bottom left.

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

Modifying IGMP Snooping Settings on a VLAN

To change the IGMP snooping settings for an IGMP-snooping enabled VLAN, select the entry with the settings to change and click **Edit**.

Figure 43. Edit IGMP Snooping VLAN Configuration Page



The dialog box titled "IGMP Snooping VLAN Configuration" contains the following fields and controls:

- VLAN ID:** A text input field showing "10".
- Admin Mode:** Radio buttons for "Disable" and "Enable" (selected).
- Fast Leave Admin Mode:** Radio buttons for "Disable" and "Enable" (selected).
- Group Membership Interval (Seconds):** A text input field with "1024" and a range "(2 to 3600)".
- Max Response Time (Seconds):** A text input field with "10" and a range "(1 to 25) Must be less than Group Membership Interval".
- Multicast Router Expiration Time (Seconds):** A text input field with "0" and a range "(0 to 3600)".
- Report Suppression Mode:** Radio buttons for "Disable" and "Enable" (selected).
- Buttons:** "Apply" (green) and "Cancel" (grey) at the bottom left.

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

Disabling IGMP Snooping on a VLAN

To disable IGMP snooping on one or more VLANs, select each VLAN to modify and click **Remove**. You must confirm the action before IGMP snooping is disabled on the selected VLANs. When IGMP snooping is disabled, the VLAN entry is removed from the table, but the VLAN itself still exists on the system.

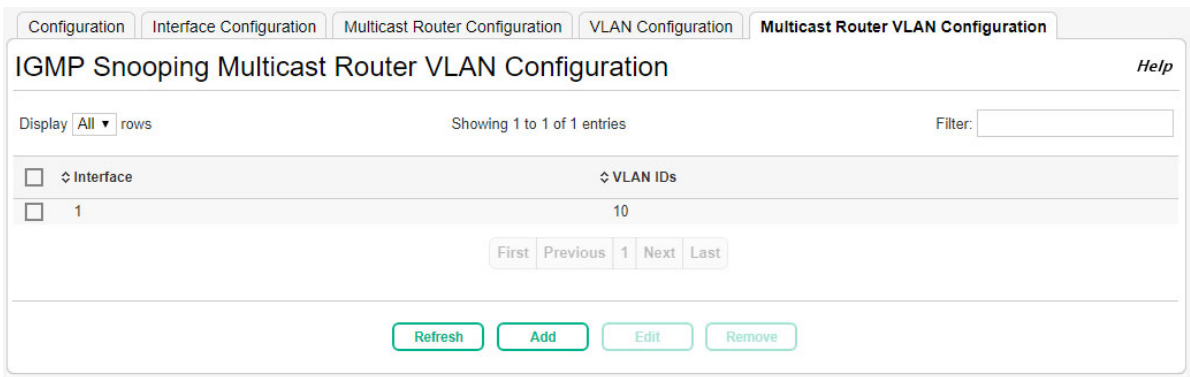
Multicast Router VLAN Configuration

Use this page to manually configure a specific VLAN as a multicast router interface for a physical port or LAG.

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

To access the page, click **Switching > IGMP Snooping** in the navigation pane and select the **Multicast Router VLAN Configuration** tab.

Figure 44. IGMP Snooping Multicast Router VLAN Configuration Page



Use the **Add** or **Edit** buttons to configure specific VLANs as multicast router interfaces for a physical port or LAG.

Figure 45. Add or Edit IGMP Snooping Multicast Router VLAN Configuration Page

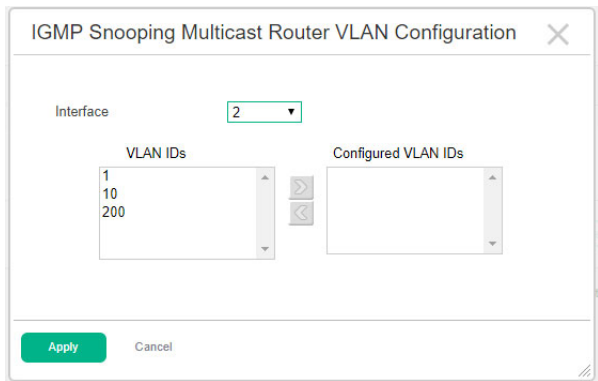


Table 30. IGMP Snooping Multicast Router VLAN Configuration Fields

Field	Description
Interface	The interface associated with the indicated VLANs. Only interfaces that are configured with multicast router VLANs appear in the table.
VLAN IDs	The ID of the VLANs configured and enabled for multicast routing on the associated interface.
Configured VLAN IDs	<p>This field is available when configuring a VLAN as a multicast router interface (after clicking Add or Edit).</p> <p>The VLANs that are enabled as multicast router interfaces on the selected port or LAG. To disable a VLAN as a multicast router interface, click the VLAN ID to select it (or CTRL + click to select multiple VLAN IDs). Then, click the appropriate arrow to move the selected VLAN or VLANs to the VLAN IDs window.</p>

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**.

SNMP

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

SNMP v1 and v2

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

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 device supports SNMP notification filters based on Object IDs (OID). OIDs are used by the system to manage device 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).

SNMP Community Configuration

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

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

To display the Community Configuration page, click **Switching** > **SNMP** in the navigation pane, and ensure that the **Community** tab is selected.

Figure 46. SNMP Community Configuration Page

Community Name	Security Name	Group Name	IP Address
private	private	DefaultWrite	0.0.0.0
public	public	DefaultRead	0.0.0.0

Table 31. SNMP Community Configuration Fields

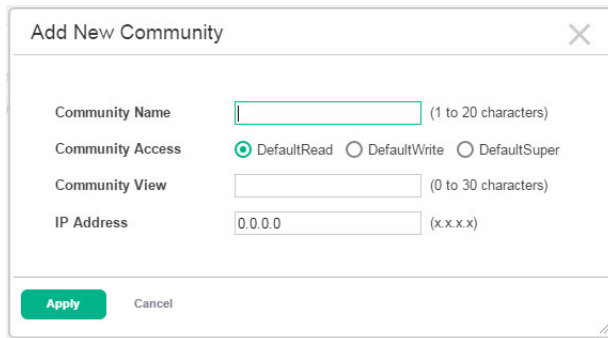
Field	Description
Community Name	Community name used in SNMPv1/v2 packets. This is configured in the client and identifies the access the user may connect with.
Security Name	Identifies the Security entry that associates Communities and Groups for a specific access type.
Group Name	Identifies the Group associated with this Community entry.
Community Access	<p>Specifies the access control policy for the community. The default access privileges are as follows:</p> <ul style="list-style-type: none">• DefaultRead: Access to the entire MIB tree except to SNMP configuration objects.• DefaultWrite: Access to the entire MIB tree except to SNMP configuration objects.• DefaultSuper: Access to the entire MIB tree. <p>For more information about controlling access to objects, see “SNMP View Entry” on page 84.</p>
Community View	<p>Specifies the community view for the community. If the value is empty, then no access is granted.</p> <p>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 (SNMPv2-SMI::mib-2.67.2.2 and SNMPv2-SMI::mib-2.67.1.2). In this way, it is possible to define a community that has access rights of a (restricted) view.</p>
IP Address	Specifies the IP address that can connect with this community.

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

Adding an SNMP Community or Community Group

To add a new SNMP community, click **Add Community**. The **Add New Community** screen appears.

Figure 47. Add SNMP Community Page



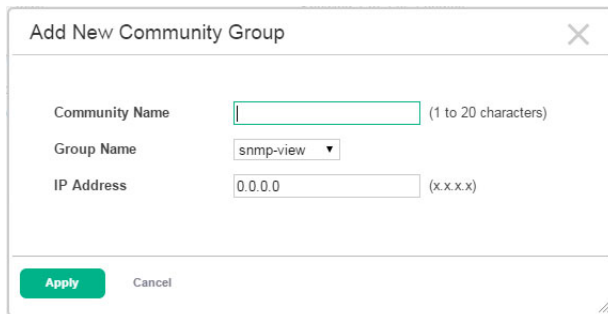
The 'Add New Community' dialog box contains the following fields and options:

- Community Name:** A text input field with a placeholder bar and a label '(1 to 20 characters)'.
- Community Access:** Three radio buttons labeled 'DefaultRead' (selected), 'DefaultWrite', and 'DefaultSuper'.
- Community View:** A text input field with a placeholder bar and a label '(0 to 30 characters)'.
- IP Address:** A text input field containing '0.0.0.0' and a label '(x.x.x.x)'.
- Buttons:** A green 'Apply' button and a 'Cancel' button.

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

To add a new SNMP community group, click **Add Community Group**. The **Add New Community Group** screen appears.

Figure 48. Add SNMP Community Group Page



The 'Add New Community Group' dialog box contains the following fields and options:

- Community Name:** A text input field with a placeholder bar and a label '(1 to 20 characters)'.
- Group Name:** A dropdown menu with 'snmp-view' selected.
- IP Address:** A text input field containing '0.0.0.0' and a label '(x.x.x.x)'.
- Buttons:** A green 'Apply' button and a 'Cancel' button.

Configure the community group 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 from the page.

SNMP v1/v2 Trap Receivers

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

To access the Trap Receiver v1/v2 Configuration page, click **Switching** > **SNMP** in the navigation pane, and then click the **Trap Receiver V1/V2** tab.

Figure 49. SNMP v1/v2 Trap Receivers Page

Community **Trap Receiver v1/v2** Trap Receiver v3 Access Control Group User Security Model View Entry

SNMP v1/v2 Trap Receivers Help

Display **All** rows Showing 0 to 0 of 0 entries Filter:

☐ Host IP Address Community Name Notify Type SNMP Version Timeout Value Retries Filter UDP Port

Table is Empty

First Previous Next Last

Refresh Add Remove

Table 32. SNMP v1/v2 Trap Receivers Fields

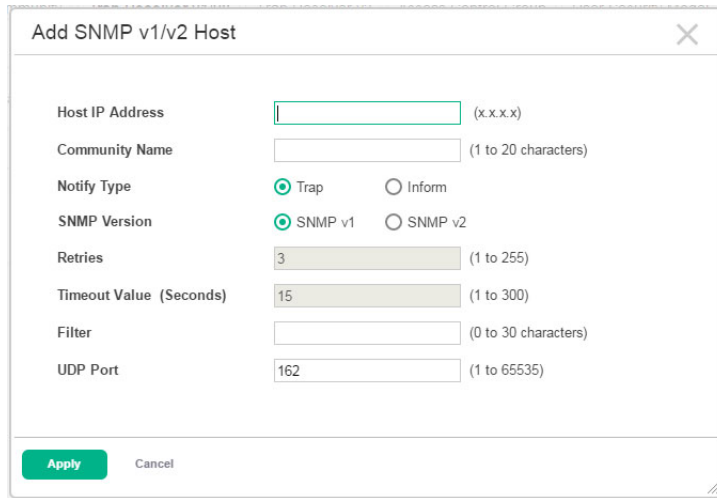
Field	Description
Host IP Address	The IP address of the SNMP management host that will receive traps generated by the device.
Community Name	The name of the SNMP community that includes the SNMP management host and the SNMP agent on the device.
Notify Type	The type of SNMP notification to send the SNMP management host: <ul style="list-style-type: none">• Inform – An SNMP message that notifies the host when a certain event has occurred on the device. The message is acknowledged by the SNMP management host. This type of notification is not available for SNMPv1.• Trap – An SNMP message that notifies the host when a certain event has occurred on the device. The message is not acknowledged by the SNMP management host.
SNMP Version	The version of SNMP to use, which is either SNMPv1 or SNMPv2.
Timeout Value	The number of seconds to wait for an acknowledgment from the SNMP management host before resending an inform message.
Retries	The number of times to resend an inform message that is not acknowledged by the SNMP management host.
Filter	The name of the filter for the SNMP management host. The filter defines which MIB objects to include or exclude from the view. This field is optional.
UDP Port	The UDP port on the SNMP management host that will receive the SNMP notifications. If no value is specified when configuring a receiver, the default UDP port value is used.

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

Adding an SNMP v1/v2 Trap Receiver

To add a SNMP v1/v2 trap receiver, click **Add**. The **Add SNMP v1/v2 Host** screen appears.

Figure 50. Add SNMP v1/v2 Host Page



The dialog box titled "Add SNMP v1/v2 Host" contains the following fields and options:

- Host IP Address: Text input field with placeholder (x.x.x.x)
- Community Name: Text input field with placeholder (1 to 20 characters)
- Notify Type: Radio buttons for ☒ Trap and ☐ Inform
- SNMP Version: Radio buttons for ☒ SNMP v1 and ☐ SNMP v2
- Retries: Spin box with value 3 and range (1 to 255)
- Timeout Value (Seconds): Spin box with value 15 and range (1 to 300)
- Filter: Text input field with placeholder (0 to 30 characters)
- UDP Port: Spin box with value 162 and range (1 to 65535)

At the bottom are **Apply** and **Cancel** buttons.

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.

Removing an SNMP v1/v2 Trap Receiver

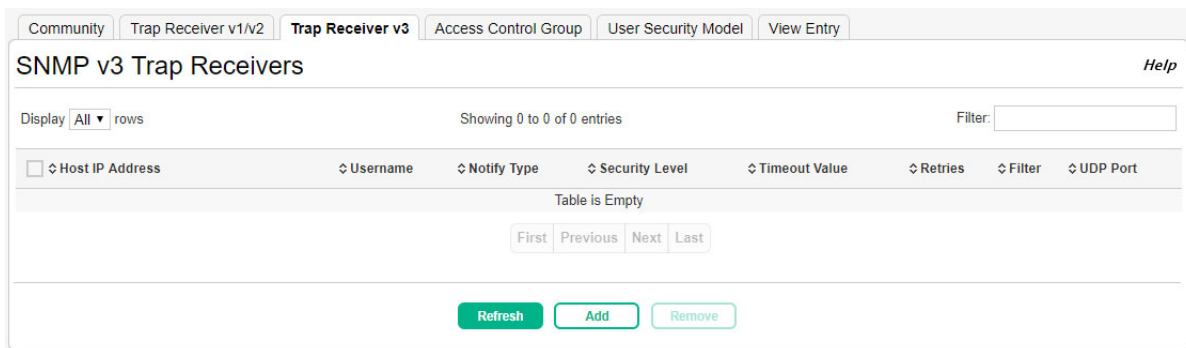
To remove an SNMP v1/v2 trap receiver, select each item to delete and click **Remove**. You must confirm the action before the entries are removed from the page.

SNMP 3 Trap Receivers

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

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

Figure 51. SNMP v3 Trap Receivers Page



The page shows tabs for **Community**, **Trap Receiver v1/v2**, **Trap Receiver v3** (selected), **Access Control Group**, **User Security Model**, and **View Entry**. The title is "SNMP v3 Trap Receivers" with a **Help** link.

Display: **All** rows. Showing 0 to 0 of 0 entries. Filter:

<input type="checkbox"/> Host IP Address	Username	Notify Type	Security Level	Timeout Value	Retries	Filter	UDP Port
Table is Empty							

Navigation: **First** **Previous** **Next** **Last**

Buttons: **Refresh** **Add** **Remove**

Table 33. SNMP v3Trap Receivers Fields

Field	Description
Host IP Address	The IP address of the SNMP management host that will receive traps generated by the device.
User Name	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: <ul style="list-style-type: none">• Inform – An SNMP message that notifies the host when a certain event has occurred on the device. The message is acknowledged by the SNMP management host. This type of notification is not available for SNMPv1.• Trap – An SNMP message that notifies the host when a certain event has occurred on the device. The message is not acknowledged by the SNMP management host.
Security Level	The security level associated with the SNMP user, which is one of the following: <ul style="list-style-type: none">• No Auth No Priv – No authentication and no data encryption (no security).• Auth No Priv – Authentication, but no data encryption. With this security level, users send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption.• Auth Priv – Authentication and data encryption. With this security level, users send an MD5 key/password for authentication and a DES key/password for encryption.
Timeout Value	The number of seconds to wait for an acknowledgment from the SNMP management host before resending an inform message.
Retries	The number of times to resend an inform message that is not acknowledged by the SNMP management host.
Filter	The name of the filter for the SNMP management host. The filter defines which MIB objects to include or exclude from the view. This field is optional.
UDP Port	The UDP port on the SNMP management host that will receive the SNMP notifications. If no value is specified when configuring a receiver, the default UDP port value is used.

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

Adding an SNMP v3 Trap Receiver

To add a SNMP v3 trap receiver, click **Add**. The **Add SNMP v3 Host** screen appears.

Figure 52. Add SNMP v3 Host Page

The screenshot shows a web-based configuration window titled "Add SNMP v3 Host". It contains the following fields and options:

- Host IP Address:** A text input field with a placeholder "(x.x.x.x)".
- Username:** A text input field with a placeholder "(1 to 30 characters)".
- Notify Type:** Two radio buttons: "Trap" (selected) and "Inform".
- Security Level:** Three radio buttons: "No Auth No Priv" (selected), "Auth No Priv", and "Auth Priv".
- Retries:** A numeric input field with the value "3" and a placeholder "(1 to 255)".
- Timeout Value (Seconds):** A numeric input field with the value "15" and a placeholder "(1 to 300)".
- Filter:** A text input field with a placeholder "(0 to 30 characters)".
- UDP Port:** A numeric input field with the value "162" and a placeholder "(1 to 65535)".

At the bottom of the window, there are two buttons: "Apply" (highlighted in green) and "Cancel".

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.

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 from the page.

Access Control Group

Use this page to configure SNMP access control groups. These SNMP groups allow network managers to assign different levels of authorization and access rights to specific device features and their attributes. The SNMP group can be referenced by the SNMP community to provide security and context for agents receiving requests and initiating traps as well as for management systems and their tasks. An SNMP agent will not respond to a request from a management system outside of its configured group, but an agent can be a member of multiple groups at the same time to allow communication with SNMP managers from different groups. Several default SNMP groups are preconfigured on the system.

To access the Access Control Group page, click **Switching > SNMP** in the navigation pane, and then click the **Access Control Group** tab.

Figure 53. Access Control Group Configuration Page

Community Trap Receiver v1/v2 Trap Receiver v3 **Access Control Group** User Security Model View Entry

SNMP Access Control Group Help

Display 10 rows Showing 1 to 10 of 13 entries Filter:

<input type="checkbox"/>	↕ Group Name	↕ Context Name	↕ SNMP Version	↕ Security Level	↕ Read	↕ Write	↕ Notify
<input type="checkbox"/>	DefaultRead		SNMP v1	No Auth No Priv	Default		Default
<input type="checkbox"/>	DefaultRead		SNMP v2	No Auth No Priv	Default		Default
<input type="checkbox"/>	DefaultRead		SNMP v3	No Auth No Priv	Default		Default
<input type="checkbox"/>	DefaultRead		SNMP v3	Auth No Priv	Default		Default
<input type="checkbox"/>	DefaultRead		SNMP v3	Auth Priv	Default		Default
<input type="checkbox"/>	DefaultSuper		SNMP v1	No Auth No Priv	DefaultSuper	DefaultSuper	DefaultSuper
<input type="checkbox"/>	DefaultSuper		SNMP v2	No Auth No Priv	DefaultSuper	DefaultSuper	DefaultSuper
<input type="checkbox"/>	DefaultSuper		SNMP v3	No Auth No Priv	DefaultSuper	DefaultSuper	DefaultSuper
<input type="checkbox"/>	DefaultWrite		SNMP v1	No Auth No Priv	Default	Default	Default
<input type="checkbox"/>	DefaultWrite		SNMP v2	No Auth No Priv	Default	Default	Default

First Previous 1 2 Next Last

Refresh Add Remove

Table 34. Access Control Group Configuration Fields

Field	Description
Group Name	The name that identifies the SNMP group.
Context Name	The SNMP context associated with the SNMP group and its views. A user or a management application specifies the context name to get the performance information from the MIB objects associated with that context name. The Context EngineID identifies the SNMP entity that should process the request (the physical router), and the Context Name tells the agent in which context it should search for the objects requested by the user or the management application.
SNMP Version	The SNMP version associated with the group.
Security Level	The security level associated with the group, which is one of the following: <ul style="list-style-type: none">• 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, select the check box to allow the field to be configured, then select the desired view that restricts management access to viewing the contents of the agent.
Write	The level of write access rights for the group. The menu includes the available SNMP views. When adding a group, select the check box to allow the field to be configured, then select the desired view that permits management read-write access to the contents of the agent but not to the community.
Notify	The level of notify access rights for the group. The menu includes the available SNMP views. When adding a group, select the check box to allow the field to be configured, then select the desired view that permits sending SNMP traps or informs.

Adding an SNMP Access Control Group

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

Figure 54. Add New Access Control Group Page

Add new Access Control Group

Access Control Group

Group Name (1 to 30 characters)

SNMP Version ☒ SNMP v1 ☐ SNMP v2 ☐ SNMP v3

Security Level ☒ No Auth No Priv ☐ Auth No Priv ☐ Auth Priv

Context Name (0 to 30 characters)

Group Access Rights

Read ☐ Default

Write ☐ Default

Notify ☐ Default

Apply Cancel

Configure the required fields and click **Apply**

Removing an SNMP Access Control Group

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 from the page.

User Security Model

The User Security Model page provides the capability to configure the SNMP V3 user accounts.

To access the User Security Model page, click **System > Advanced Configuration > SNMP > User Security Model** in the navigation menu.

Figure 55. SNMP User Security Model Page

Username	Group Name	Engine ID	Authentication	Privacy
User1	SNMP-RO	8000113D031C98EC7C8E40	None	None

Table 35. SNMP User Security Model Fields

Field	Description
User Name	Specifies the name of the SNMP user being added for the User-based Security Model (USM). Each user name must be unique within the SNMP agent user list. A user name cannot contain any leading or embedded blanks
Group Name	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 Type	This field is available on the Add New SNMP User page. 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.
Engine ID	Each SNMPv3 agent has an engine ID that uniquely identifies the agent in the device. If given this entry will be used only for packets whose engine id is this. This field takes an hexadecimal string in the form 0102030405.

Field	Description
Authentication Method	The authentication protocol to be used on authenticated messages on behalf of the user. <ul style="list-style-type: none"> • 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. • MD5-Key - MD5 protocol will be used. This option requires a pregenerated MD5 authentication key of 32 hexadecimal characters. • SHA-Key - SHA protocol will be used. This option requires a pregenerated SHA authentication key of 48 hexadecimal characters.
Password	This field is available on the Add New SNMP User page. 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	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. <ul style="list-style-type: 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. • DES-Key - DES protocol will be used. This option requires an authentication key of 32 characters if MD5 is selected or 48 characters if SHA is selected.
Authentication Key (Add New SNMP User page)	This field is available on the Add New SNMP User page. 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.

Adding an SNMP v3 User

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

Figure 56. Add New SNMP User Page

Configure the required fields and click **Apply**

Removing an SNMP v3 User

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

SNMP View Entry

Use the SNMP View Entry page 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 Entry page, click **System > Advanced Configuration > SNMP > View Entry** in the navigation menu.

Figure 57. SNMP View Entry Page

<input type="checkbox"/>	View Name	OID Tree	View Type
<input type="checkbox"/>	Default	1	Included
<input type="checkbox"/>	Default	1.3.6.1.6.3.16	Excluded
<input type="checkbox"/>	Default	1.3.6.1.6.3.15.1.2	Excluded
<input type="checkbox"/>	Default	1.3.6.1.6.3.18.1.1	Excluded
<input type="checkbox"/>	DefaultSuper	1	Included

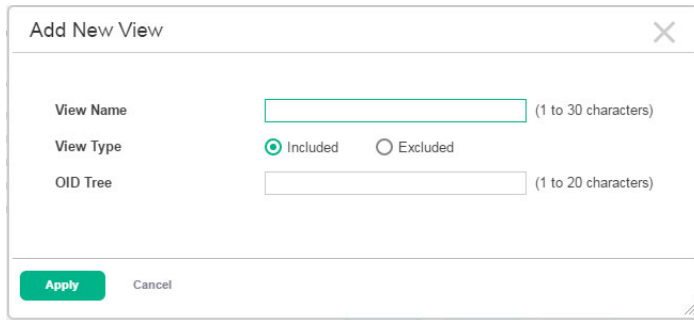
Table 36. SNMP View Entry Fields

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: <ul style="list-style-type: none">• 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 New SNMP User** screen appears.

Figure 58. Add New View

A dialog box titled "Add New View" with a close button (X) in the top right corner. It contains three input fields: "View Name" (1 to 30 characters), "View Type" (radio buttons for "Included" and "Excluded", with "Included" selected), and "OID Tree" (1 to 20 characters). At the bottom, there are "Apply" and "Cancel" buttons.

Add New View

View Name (1 to 30 characters)

View Type ☒ Included ☐ Excluded

OID Tree (1 to 20 characters)

Apply Cancel

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 from the page.

Auto Recovery Configuration

The switch supports an Auto Recovery feature that allows ports to be placed in a diagnostically disabled state when defined error conditions are met. Features supported by Auto Recovery are BPDU Guard, BPDU Rate Limiting, Storm Control, and Port Security.

The error conditions that cause a port to be placed into the diagnostically disabled state are as follows:

- **BPDU Guard:** If a port that has the BPDU Guard feature enabled receives a BPDU, it is placed in the diagnostically disabled state.
- **BPDU Rate Limit:** When Spanning Tree is enabled, BPDU Rate Limiting is enabled by default to protect the switch from BPDU storms. The BPDU rate limit threshold is set to 12-17 BPDU packets per second for three consecutive seconds. If this threshold is exceeded on a port, the port moves to the diagnostically disabled state.
- **Storm Control:** If the incoming rate of unicast (with unknown destination), multicast, or broadcast packets exceeds a set threshold, the port moves to the diagnostically disabled state.
- **Port Security:** If a port that has the Violation Shutdown Mode feature enabled receives unknown MAC addresses after the MAC limit is reached, the port moves to the diagnostically disabled state.

When a port has been placed into a diagnostically disabled 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 diagnostically disabled 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. If Auto Recovery is disabled after ports have been placed in a diagnostically disabled state, they will remain disabled until an administrator manually enables them.

Use the Auto Recovery Configuration page to configure Auto Recovery settings for spanning-tree BPDU Guard, BPDU Rate Limit, Storm Control, and Port Security components. To display this page, click **Switching > Auto Recovery**.

Figure 59. Auto Recovery Configuration Page

Auto Recovery Configuration
Help

Auto Recovery Components

BPDU Guard

☐ Enabled
☒ Disabled

BPDU Rate Limit

☐ Enabled
☒ Disabled

Storm Control

☐ Enabled
☒ Disabled

Port Security

☐ Enabled
☒ Disabled

Auto Recovery Parameters

Recovery Time (Seconds)

(30 to 86400, 300 = Default)

Interface Status

Display All rows

Showing 0 to 0 of 0 entries

Filter:

Interface

Admin Mode

Port Status

Reason

Time to Recover

Table is Empty

First Previous Next Last

Apply

Refresh

Cancel

Table 37. Auto Recovery Configuration Fields

Field	Description
Auto Recovery Components	
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 diagnostically disabled state will remain in that state until an administrator manually enables it. BPDU Guard Auto Recovery is disabled by default.
BPDU Rate Limit	If a port receives BPDUs at a rate greater than or equal to 12-17 BPDUs per second for three consecutive seconds, that port will be placed in the diagnostically disabled state. When BPDU Rate Limit Auto Recovery is enabled, the port will be enabled once the configured Recovery Time expires. If the port continues to receive BPDUs at a rate greater than or equal to 12-17 BPDUs per second for three consecutive seconds, that port will be disabled again. BPDU Rate Limit 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 diagnostically disabled 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 diagnostically disabled 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.

Field	Description
Auto Recovery Parameters	
Recovery Time (Seconds)	This configures the Auto Recovery time interval. The Auto Recovery time interval is common for BPDU Guard, BPDU Rate Limit, Storm Control and Port Security. The default value of the timer is 300 seconds and the range is from 30 to 86400 seconds.
Interface Status	
Interface	The interface that is diagnostically disabled. If no interfaces are in the diagnostically disabled state, the table is blank.
Admin Mode	The administrative mode of the interface.
Port Status	Indicates whether the link is up or down. The link is the physical connection between the port or trunk and the interface on another device.
Reason	<p>If the switch detects an error condition for an interface, the switch puts the interface in the diagnostically disabled state, meaning that it has been intentionally disabled because it has encountered errors. The reasons that the interface can go into a diagnostically disabled state include the following:</p> <ul style="list-style-type: none"> • BPDU Guard • BPDU Storm • Storm Control • Port Security
Time to Recover	When Auto Recovery is enabled and the interface is placed in the diagnostically disabled state, then a recovery timer starts for that interface. Once this timer expires, the device checks if the interface is in the diagnostically disabled state. If yes, then the device enables the diagnostically disabled interface.

If you modify these 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**.

5 Virtual LAN

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.

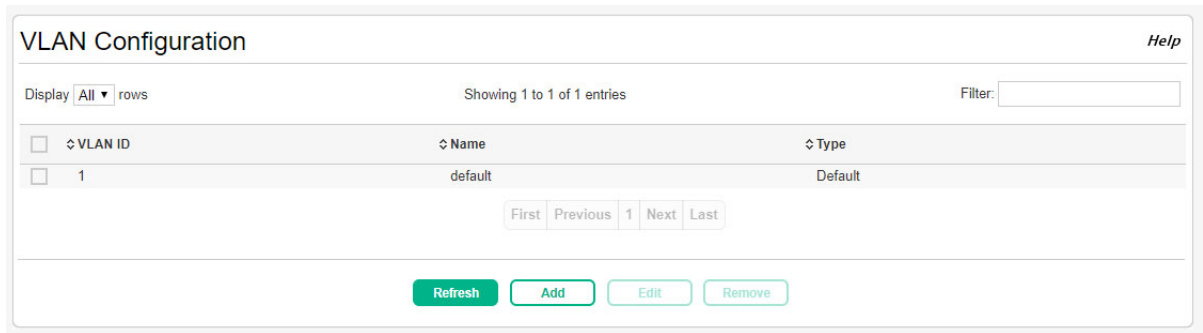
HPE OfficeConnect 1920S series switches support up to 256 VLANs.

Viewing VLAN Status and Adding VLANs

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

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

Figure 60. VLAN Configuration Page



By default, VLAN 1 is defined on the switch. It is designated as the default VLAN and 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 [Table 2 on page 20](#) for additional information about the management VLAN.

The following information displays for each VLAN:

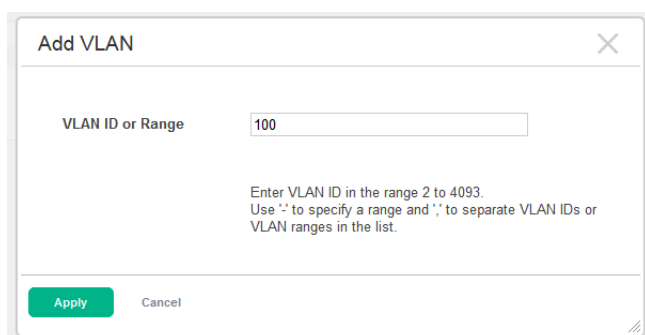
Table 38. VLAN Configuration Fields

Field	Description
VLAN ID	The numerical VLAN identifier (VID) assigned to the VLAN, from 1 to 4093. 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. If no name is specified, the name is VLANnnnn, where nnnn is the four-digit VLAN ID (including any leading zeros).
Type	The type of VLAN, which can be one of the following: <ul style="list-style-type: none">• Default—The default VLAN. This VLAN is always present, and the VLAN ID is 1.• Static—A user-configured VLAN.

Adding VLANs

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

Figure 61. Add VLAN

A screenshot of a web-based dialog box titled "Add VLAN" with a close button (X) in the top right corner. Inside the dialog, there is a label "VLAN ID or Range" followed by a text input field containing the number "100". Below the input field, there is a small block of instructional text: "Enter VLAN ID in the range 2 to 4093. Use '-' to specify a range and ',' to separate VLAN IDs or VLAN ranges in the list." At the bottom of the dialog, there are two buttons: a green "Apply" button and a grey "Cancel" button.

In the **VLAN ID or Range** field, specify one or more VLAN IDs in the range 2 to 4093, and click **Apply**.

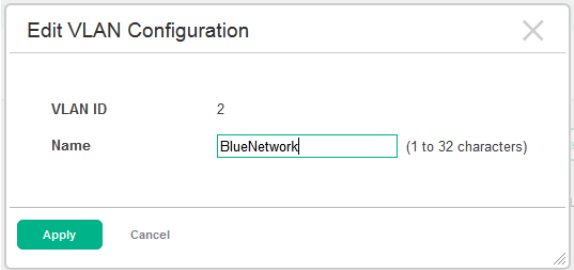
To create a range of VLANs, specify the beginning and ending VLAN IDs, separated by a dash. To create multiple non-sequential VLANs, separate each VLAN ID with a comma.

You can create up to 256 VLANs.

Changing a VLAN Name

When you create a VLAN, a default name is automatically assigned in the form VLANnnnn, where *nnnn* is the VLAN number with preceding zeros as needed. To change the VLAN name, select it on the VLAN Status page and click **Edit**.

Figure 62. Edit VLAN Page



The dialog box titled "Edit VLAN Configuration" has a close button (X) in the top right corner. It contains two fields: "VLAN ID" with the value "2" and "Name" with the value "BlueNetwork". The "Name" field has a placeholder "(1 to 32 characters)". At the bottom, there are two buttons: "Apply" (green) and "Cancel" (gray).

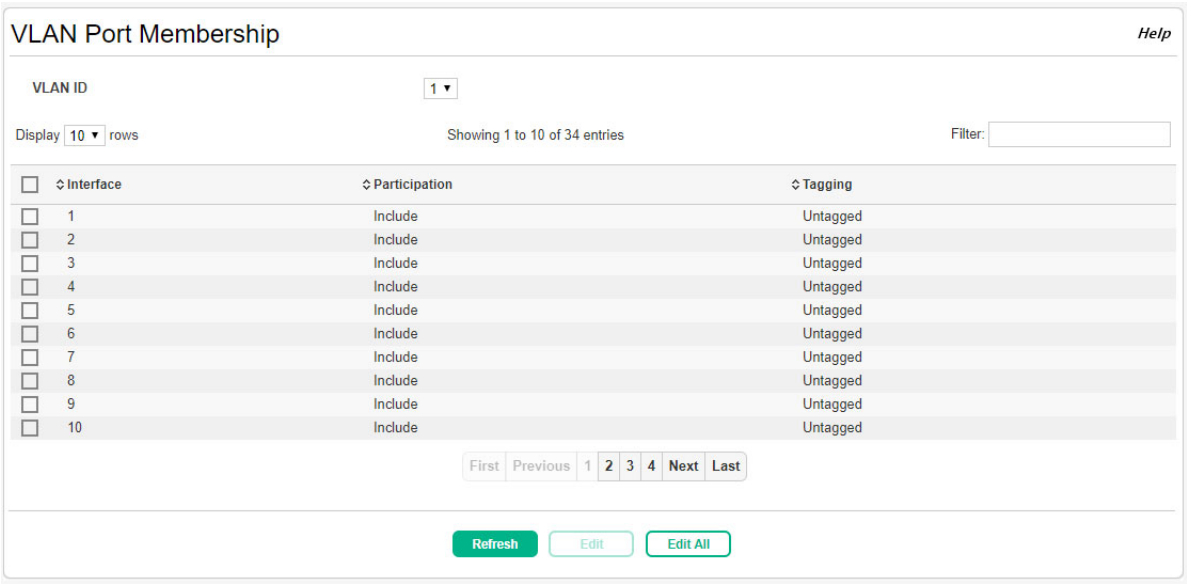
On the Edit VLAN Configuration page, specify the new name consisting of 0 to 32 alphanumeric characters and click **Apply**.

Configuring Interfaces as VLAN Members

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 > Port Membership** in the navigation pane.

Figure 63. VLAN Port Membership Page



The "VLAN Port Membership" page has a "Help" link in the top right corner. It features a "VLAN ID" dropdown menu set to "1". Below this, it says "Display 10 rows" and "Showing 1 to 10 of 34 entries". There is a "Filter:" input field. The main content is a table with three columns: "Interface", "Participation", and "Tagging". Each row has a checkbox in the "Interface" column. The table shows 10 rows of data, all with "Include" participation and "Untagged" tagging. At the bottom, there are navigation buttons: "First", "Previous", "1", "2", "3", "4", "Next", and "Last". Below the table, there are three buttons: "Refresh" (green), "Edit" (gray), and "Edit All" (gray).

<input type="checkbox"/> Interface	Participation	Tagging
<input type="checkbox"/> 1	Include	Untagged
<input type="checkbox"/> 2	Include	Untagged
<input type="checkbox"/> 3	Include	Untagged
<input type="checkbox"/> 4	Include	Untagged
<input type="checkbox"/> 5	Include	Untagged
<input type="checkbox"/> 6	Include	Untagged
<input type="checkbox"/> 7	Include	Untagged
<input type="checkbox"/> 8	Include	Untagged
<input type="checkbox"/> 9	Include	Untagged
<input type="checkbox"/> 10	Include	Untagged

Table 39. VLAN Port Membership 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: <ul style="list-style-type: none">• Include – The port is a member of the selected VLAN. This mode is also equivalent to registration fixed in the IEEE 802.1Q standard.• Exclude – 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: <ul style="list-style-type: none">• 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 port membership to the selected VLAN, select one or more ports and click **Edit**. Or, click **Edit All** to configure all ports at the same time.

On the **Edit VLAN Port 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.

NOTE:

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.
- All ports 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 via 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. When a member port is added to a trunk, it loses any previous VLAN memberships and acquires those of the trunk. When deleted from a trunk, a port loses the VLAN memberships of the trunk and acquires untagged membership in VLAN 1.

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 Port Configuration

Use the VLAN Port Configuration page to configure the way interfaces handle VLAN-tagged, priority-tagged, and untagged traffic. To view this page, click **VLANS > VLAN Port Configuration** in the navigation pane.

Figure 64. VLAN Port Configuration Page

The screenshot shows the 'VLAN Port Configuration' page with a table of 10 interfaces. Each row has a checkbox, an interface name, a Port VLAN ID, an Acceptable Frame Type, Ingress Filtering, Untagged VLANs, Tagged VLANs, and a Priority. The table is filtered to show 1 to 10 of 34 entries. Below the table are navigation buttons (First, Previous, 1, 2, 3, 4, Next, Last) and action buttons (Refresh, Edit, Edit All).

<input type="checkbox"/>	Interface	Port VLAN ID	Acceptable Frame Type	Ingress Filtering	Untagged VLANs	Tagged VLANs	Priority
<input type="checkbox"/>	1	1	Admit All	Enabled	1		0
<input type="checkbox"/>	2	1	Admit All	Enabled	1		0
<input type="checkbox"/>	3	1	Admit All	Enabled	1		0
<input type="checkbox"/>	4	1	Admit All	Enabled	1		0
<input type="checkbox"/>	5	1	Admit All	Enabled	1		0
<input type="checkbox"/>	6	1	Admit All	Enabled	1		0
<input type="checkbox"/>	7	1	Admit All	Enabled	1		0
<input type="checkbox"/>	8	1	Admit All	Enabled	1		0
<input type="checkbox"/>	9	1	Admit All	Enabled	1		0
<input type="checkbox"/>	10	1	Admit All	Enabled	1		0

Table 40. VLAN Port Configuration Fields

Field	Description
Interface	Identifies the physical interface associated with the rest of the data in the row.
Port VLAN ID	The VLAN ID assigned to untagged or priority tagged frames received on this port. This value is also known as the Port VLAN ID (PVID). In a tagged frame, the VLAN is identified by the VLAN ID in the tag.
Acceptable Frame Types	Indicates how the interface handles untagged and priority tagged frames: <ul style="list-style-type: none">Admit All – Untagged and priority tagged frames received on the interface are accepted and assigned the value of the Port VLAN ID for this interface.Only Tagged – The interface discards any untagged or priority tagged frames it receives.Only Untagged – 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. <ul style="list-style-type: none">Enable: A tagged frame is discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag.Disable: All tagged frames are accepted, which is the factory default.
Untagged VLANs	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.
Priority	Identifies the default 802.1p priority assigned to untagged packets arriving at the port.

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. 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**.

Auto Voice VLAN Configuration

The voice VLAN feature enables switch ports to carry voice traffic with defined settings so that voice and data traffic are separated when coming onto the port. A voice VLAN ensures that the sound quality of an IP phone is safeguarded from deterioration when data traffic on the port is high.

The inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network-attached clients cannot initiate a direct attack on voice components. A QoS protocol based on the IEEE 802.1P class-of-service (CoS) protocol uses classification and scheduling to send network traffic from the switch in a predictable manner. The system uses the source MAC of the traffic traveling through the port to identify the IP phone data flow.

Voice VLAN is enabled per-port basis. A port can participate only in one voice VLAN at a time. The Voice VLAN feature is disabled by default.

Use the Auto 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.

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

Figure 65. Auto Voice VLAN Configuration Page

Auto Voice VLAN Configuration Help

Voice VLAN Admin Mode ☐ Enabled ☒ Disabled

Display All rows Showing 0 to 0 of 0 entries Filter:

<input type="checkbox"/> Interface	Operational State	CoS Override Mode	Voice VLAN Interface Mode	Voice VLAN DSCP
Table is Empty				

First Previous Next Last

Apply Refresh Add Edit Remove Cancel

Table 41. Auto Voice VLAN Configuration Fields

Field	Description
Voice VLAN Admin Mode	Click Enable or Disable to administratively turn the Voice VLAN feature on or off for all ports. The administrative mode of the Voice VLAN feature. 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.
Interface	The interface associated with the rest of the data in the row. When adding a Voice VLAN configuration to a port, the Interface menu allows you to select the port to configure. Only interfaces that have not been configured with Voice VLAN settings can be selected from the menu.
Operational State	The operational status of the Voice VLAN feature on the interface. To be enabled, Voice VLAN must be globally enabled and enabled on the interface. Additionally, the interface must be up and have a link.

Field	Description
CoS Override Mode	The Class of Service override mode: <ul style="list-style-type: none"> Enabled – The port ignores the 802.1p priority value in the Ethernet frames it receives from connected devices. Disabled – The port trusts the priority value in the received frame.
Voice VLAN Interface Mode	Indicates how an IP phone connected to the port should send voice traffic: <ul style="list-style-type: none"> VLAN ID – Forward voice traffic in the specified voice VLAN. 802.1p – Tag voice traffic with the specified 802.1p priority value. None – Use the settings configured on the IP phone to send untagged voice traffic. Untagged – Send untagged voice traffic.
Voice VLAN Interface Value	When adding or editing Voice VLAN settings for an interface and either VLAN ID or Dot1p is selected as the Voice VLAN Interface Mode, specify the voice VLAN ID or the Dot1p priority value that the connected IP phone should use for voice traffic.
Voice VLAN DSCP	The IP DSCP value that voice traffic is tagged with.

Use the buttons to perform the following tasks:

- To configure Voice VLAN settings on a port, click **Add**. Select the interface to configure from the Interface menu, and then configure the desired settings.
- To change the Voice VLAN settings, select the interface to modify and click **Edit**.
- To remove the Voice VLAN configuration from one or more ports, select each entry 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**.

6 Trunks

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 provides load sharing capability.

Trunk Overview

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 aggregation-capable network devices in the system and exchanges Link Aggregation Control Protocol Data Units (LACPDUs) with links in the trunk. The PDUs contain information about each link and enable the trunk to maintain them.
- **Static**—Static trunks are assigned to a bundle by the administrator. Members do not exchange LACPDUs. A static trunk does not require a partner system to be able to aggregate its member ports. This is the default port type.

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 administrative enable/disable, port priority, and path cost.

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

When ports are added as members to a trunk, they are removed from all existing VLAN memberships and acquire the membership of trunk VLANs.

The 8-port switches support four trunks, the 24-port switches support eight trunks, and the 48-port switches support 16 trunks. On the 8-port and 24-port switches, each trunk can support up to four trunk members, and on the 48-port switches, each trunk can support up to eight members.

NOTE:

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

Trunk Configuration

You can use the Trunk Configuration page to view and edit trunks. The number of trunks on the system is fixed, and all trunks are disabled by default. You can enable, disable, and edit settings for each trunk. Click **Trunk > Trunk Configuration** in the navigation pane.

Figure 66. Trunk Configuration Page

Trunk	Name	Type	Admin Mode	Link Status	Members	Active Ports
<input type="checkbox"/> TRK 1	TRK1	Static	Enabled	Down		
<input type="checkbox"/> TRK 2	TRK2	Static	Enabled	Down		
<input type="checkbox"/> TRK 3	TRK3	Static	Enabled	Down		
<input type="checkbox"/> TRK 4	TRK4	Static	Enabled	Down		
<input type="checkbox"/> TRK 5	TRK5	Static	Enabled	Down		
<input type="checkbox"/> TRK 6	TRK6	Static	Enabled	Down		
<input type="checkbox"/> TRK 7	TRK7	Static	Enabled	Down		
<input type="checkbox"/> TRK 8	TRK8	Static	Enabled	Down		

The following information displays for each trunk.

Table 42. Trunk Configuration Fields

Field	Description
Trunk	The trunk ID.
Name	The configurable trunk name, which is the same as the trunk ID by default.
Type	<p>Trunks can be either dynamic or static, but not both:</p> <ul style="list-style-type: none">Dynamic—Dynamic trunks use the 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)s 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 LACPDU)s. A static trunk does not require a partner system to be able to aggregate its member ports. This is the default port type. <p>Note that the loop protection feature is not supported on dynamic trunks. If loop protection is enabled on a static trunk and the trunk is changed to a dynamic trunk, loop protection is disabled.</p>
Admin Mode	Whether the trunk is administratively enabled or disabled. This feature is enabled by default.
Link Status	Indicates the operational status of the trunk interface, 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 Existing Trunk page displays:

Figure 67. Edit Existing Trunk Page

The screenshot shows the 'Edit Existing Trunk' dialog box. It contains the following fields and options:

- Trunk Name:** A text input field with the value 'TRK3' and a character count '(1 to 15 characters)'.
- Admin Mode:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- STP Mode:** Radio buttons for 'Enabled' and 'Disabled' (selected).
- Static Mode:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Load Balance:** A dropdown menu with the selected option 'Source/Destination MAC, VLAN, Ethertype, Incoming Port'.
- Port List:** A list box containing ports 1, 4, 5, 6, 7, 8, 9, and 10.
- Members:** A list box containing ports 2 and 3.
- Buttons:** 'Apply' and 'Cancel' buttons at the bottom.

You can define the trunk name, administratively enable and disable the trunk, and select between static and dynamic mode, as described in [Table 42 on page 97](#). You can also configure the following additional settings:

Table 43. Additional Trunk Configuration Fields

Field	Description
STP Mode	The spanning tree protocol (STP) mode of the trunk. When enabled, the trunk participates in the STP operation to help prevent network loops. This feature is enabled on all trunks by default.
Static Mode	When enabled, the trunk is a static trunk. When disabled, the trunk type is Dynamic.
Load Balance	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. The following sets of packet attributes can be used to compute the hashing algorithm: <ul style="list-style-type: none">• Source MAC, VLAN, EtherType, Incoming Port• Destination MAC, VLAN, EtherType, Incoming Port• Source/Destination MAC, VLAN, EtherType, Incoming Port. This is the default selection.• Source IP and Source TCP/UDP Port Fields• Destination IP and Destination TCP/UDP Port Fields• Source/Destination IP and TCP/UDP Port Fields
Port List/Members	The Port List shows ports that are not members of the trunk, and the Members list shows the ports that are members. Use the arrows to move ports between the lists.

Note the following considerations when configuring trunks and trunk members:

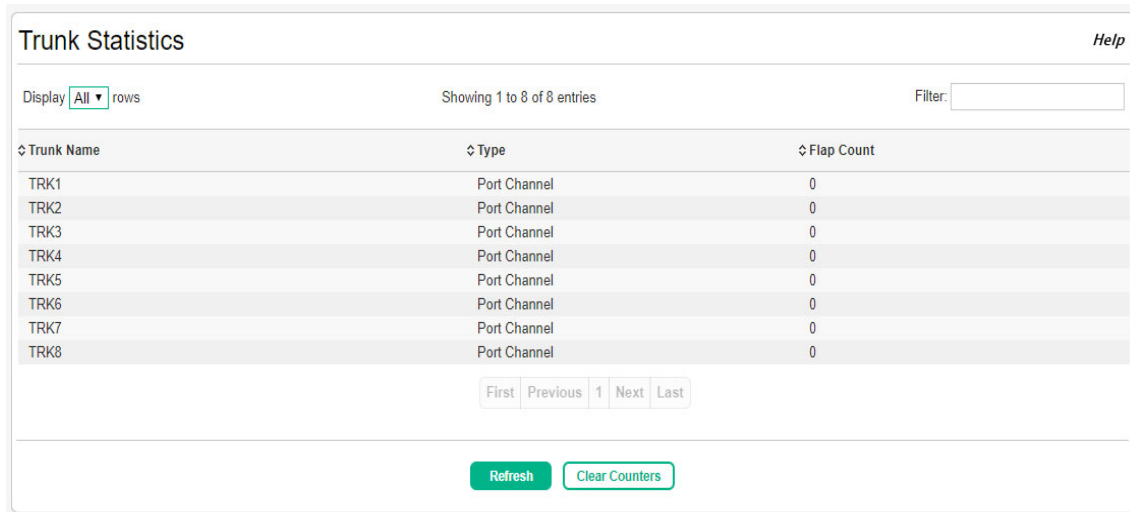
- All ports in a trunk must have the same full-duplex speed.
- Loop protection is supported on static trunks, but not on dynamic trunks. If loop protection is enabled on a static trunk that is now being changed to a dynamic trunk, loop protection will be disabled on the trunk.
- A port that is added to a trunk loses its port VLAN membership and is assigned the VLAN memberships configured for the trunk. Individual port VLAN memberships cannot be configured for ports that are members of a trunk. When the port is removed from a trunk, the port is made a member of the default VLAN.
- 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.

Trunk Statistics

The Trunk Statistics page displays the flap count for each trunk. A flap occurs when a trunk interface or trunk member port goes down. To display the Trunk page, click **Trunks > Statistics** in the navigation pane.

Figure 68. Trunk Statistics Page



Trunk Name	Type	Flap Count
TRK1	Port Channel	0
TRK2	Port Channel	0
TRK3	Port Channel	0
TRK4	Port Channel	0
TRK5	Port Channel	0
TRK6	Port Channel	0
TRK7	Port Channel	0
TRK8	Port Channel	0

Table 44. Trunk Statistics Fields

Field	Description
Trunk Name	The user-created name for the trunk.
Type	The interface type, which is either Port-Channel (a trunk) or Member Port (a physical port).
Flap Count	The number of times the interface has gone down. The counter for a member port is incremented when the physical port is either manually shut down by the administrator or when its link state is down. When a trunk is administratively shut down, the flap counter for the trunk is incremented, but the flap counters for its member ports are not affected. When all active member ports for a trunk are inactive (either administratively down or link down), then the trunk flap counter is incremented.

You can click **Clear Counters** to reset the flap count statistics to 0.

7 Link Layer Discovery Protocol (LLDP and LLDP-MED)

LLDP is a standardized discovery protocol defined by IEEE 802.1AB. It allows stations residing on a LAN to advertise major 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 Global Configuration

Use the LLDP Global Configuration page to specify global LLDP parameters and to configure the protocol on individual ports.

To display the LLDP Global Configuration page, click **LLDP > Configuration** in the navigation pane.

Figure 69. LLDP Global Configuration Page

LLDP Global Configuration

Help

Transmit Interval (Seconds)

30

(5 to 32768)

Transmit Hold Multiplier (Seconds)

4

(2 to 10)

Re-Initialization Delay (Seconds)

2

(1 to 10)

Notification Interval (Seconds)

5

(5 to 3600)

Display 10 rows

Showing 1 to 10 of 26 entries

Filter:

<input type="checkbox"/>	↕Interface	↕Link Status	↕Transmit	↕Receive	↕Notify	↕Transmit Management Information
<input type="checkbox"/>	1	Down	Enabled	Enabled	Enabled	Yes
<input type="checkbox"/>	2	Down	Enabled	Enabled	Enabled	Yes
<input type="checkbox"/>	3	Up	Enabled	Enabled	Enabled	Yes
<input type="checkbox"/>	4	Down	Enabled	Enabled	Enabled	Yes
<input type="checkbox"/>	5	Down	Enabled	Enabled	Enabled	Yes
<input type="checkbox"/>	6	Down	Enabled	Enabled	Enabled	Yes
<input type="checkbox"/>	7	Down	Enabled	Enabled	Enabled	Yes
<input type="checkbox"/>	8	Down	Enabled	Enabled	Enabled	Yes
<input type="checkbox"/>	9	Up	Enabled	Enabled	Enabled	Yes
<input type="checkbox"/>	10	Down	Enabled	Enabled	Enabled	Yes

First

Previous

1

2

3

Next

Last

Apply

Refresh

Edit

Edit All

Cancel

You can configure the following global settings:

Table 45. 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.
Notification Interval	Specify the minimum number of seconds to wait between transmissions of remote data change notifications. The range is from 5 to 3600 seconds and the default is 5 seconds.

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**.

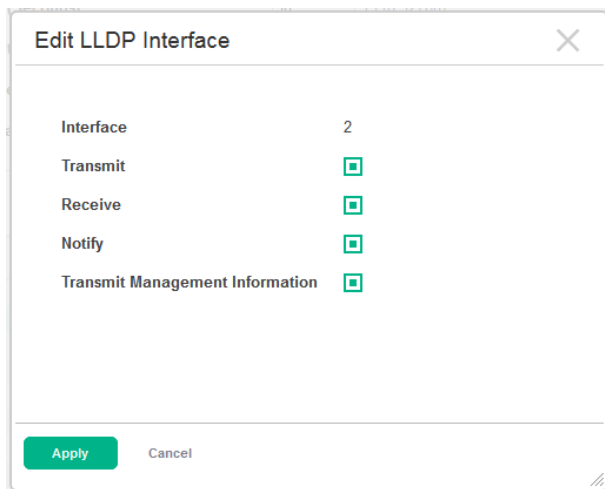
The following information displays for each interface:

Table 46. LLDP Global Configuration—Port Fields

Field	Description
Interface	The port or trunk ID.
Link Status	The link status of the interface, which is either Up or Down. An interface that is down does not forward traffic.
Transmit	The LLDP advertise (transmit) mode on the interface. If the transmit mode is enabled, the interface sends LLDPDUs that advertise the mandatory TLVs that are enabled.
Receive	The LLDP receive mode on the interface. If the receive mode is enabled, the device can receive LLDPDUs from other devices.
Notify	Enable to have LLDP generate a log file entry.
Transmit Management Information	The status of the LLDP remote data change notification on the interface. When enabled, the interface sends notifications when a link partner device is added or removed.

To modify interface settings, select one or more interfaces and click **Edit** to display the Edit LLDP Interface page.

Figure 70. Edit LLDP Interface



The 'Edit LLDP Interface' dialog box shows settings for interface 2. It includes checkboxes for Transmit, Receive, Notify, and Transmit Management Information, all of which are currently checked. At the bottom are 'Apply' and 'Cancel' buttons.

Interface	2
Transmit	<input checked="" type="checkbox"/>
Receive	<input checked="" type="checkbox"/>
Notify	<input checked="" type="checkbox"/>
Transmit Management Information	<input checked="" type="checkbox"/>

Apply Cancel

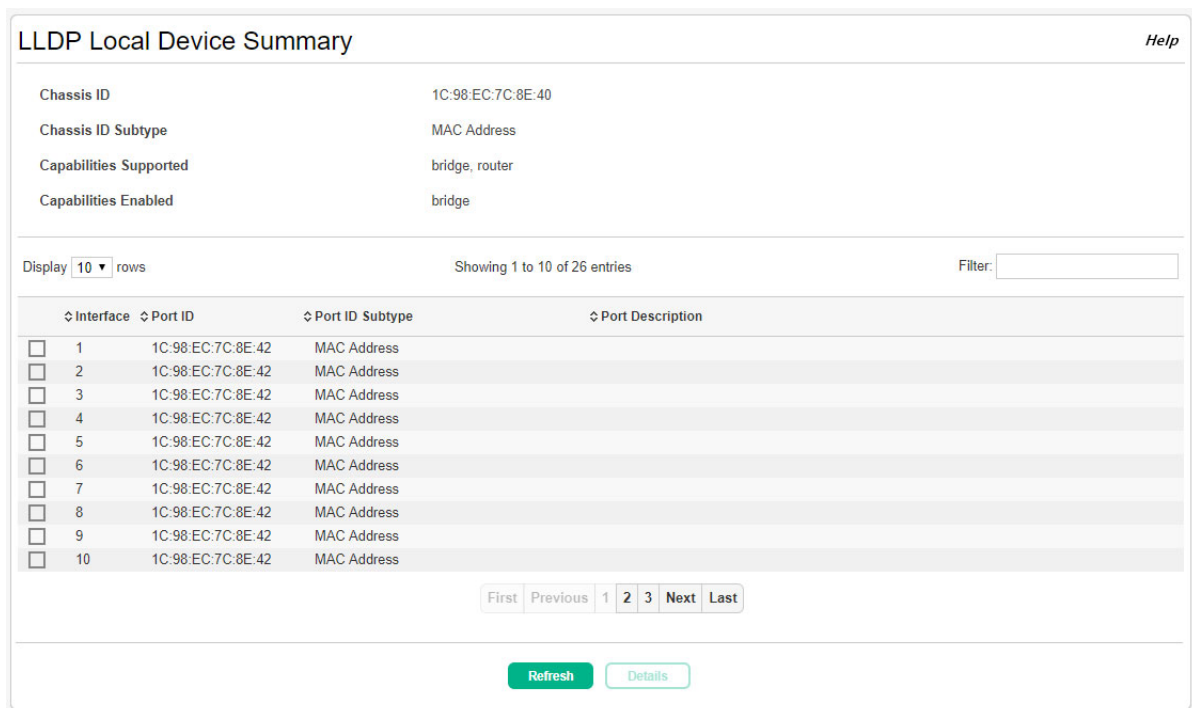
Select a box to enable the associated feature. Clear a box to disabled the associated feature.

To modify settings on all interfaces, click **Edit All**.

LLDP Local Device Summary

Use the LLDP Local Device Summary page to view LLDP information for switch interfaces. To display this page, click **LLDP > Local Devices** in the navigation pane.

Figure 71. LLDP Local Device Summary Page



The 'LLDP Local Device Summary' page displays device information and a table of interfaces. The summary section shows Chassis ID (1C:98:EC:7C:8E:40), Chassis ID Subtype (MAC Address), Capabilities Supported (bridge, router), and Capabilities Enabled (bridge). The table below lists 10 interfaces, all with the same MAC address and subtype. Navigation controls include a display count of 10 rows, a filter box, and pagination buttons (First, Previous, 1, 2, 3, Next, Last). At the bottom are 'Refresh' and 'Details' buttons.

LLDP Local Device Summary Help

Chassis ID 1C:98:EC:7C:8E:40
Chassis ID Subtype MAC Address
Capabilities Supported bridge, router
Capabilities Enabled bridge

Display 10 rows Showing 1 to 10 of 26 entries Filter:

	Interface	Port ID	Port ID Subtype	Port Description
<input type="checkbox"/>	1	1C:98:EC:7C:8E:42	MAC Address	
<input type="checkbox"/>	2	1C:98:EC:7C:8E:42	MAC Address	
<input type="checkbox"/>	3	1C:98:EC:7C:8E:42	MAC Address	
<input type="checkbox"/>	4	1C:98:EC:7C:8E:42	MAC Address	
<input type="checkbox"/>	5	1C:98:EC:7C:8E:42	MAC Address	
<input type="checkbox"/>	6	1C:98:EC:7C:8E:42	MAC Address	
<input type="checkbox"/>	7	1C:98:EC:7C:8E:42	MAC Address	
<input type="checkbox"/>	8	1C:98:EC:7C:8E:42	MAC Address	
<input type="checkbox"/>	9	1C:98:EC:7C:8E:42	MAC Address	
<input type="checkbox"/>	10	1C:98:EC:7C:8E:42	MAC Address	

First Previous 1 2 3 Next Last

Refresh Details

If all LLDP functions are disabled on an interface, then it does not appear in the table.

Table 47. LLDP Local Device Summary Fields

Field	Description
Local Device Summary	
Chassis ID	The hardware platform identifier for the device.
Chassis ID Subtype	The type of information used to identify the chassis.
Capabilities Supported	The primary function(s) the device supports.
Capabilities Enabled	The primary function(s) the device supports that are enabled.
Interface Description	
Interface	The interface ID.
Port ID	The port identifier, which is the physical address associated with the interface.
Port ID Subtype	The type of information used to identify the interface
Port Description	A description of the port. An administrator can configure this information on the Port Status page.

Displaying Port Details

To view additional LLDP information that the interface advertises, select the interface and click **Details**.

Figure 72. LLDP Local Device Information Page

In addition to the fields described in [Table 47 on page 103](#), this page displays the following fields.

Table 48. LLDP Local Device Information Fields

Field	Description
System Name	The user-configured system name for the device. The system name is configured on the Dashboard page.
System Description	The device description which includes information about the product model and platform.
Management Address	The address, such as an IP address, associated with the management interface of the device.
Management Address Type	The protocol type or standard associated with the management address.

LLDP Remote Device Summary

Use the LLDP Remote Device Summary page 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.

To display the Remote Device page, click **LLDP > Remote Devices** in the navigation pane.

Figure 73. LLDP Remote Device Summary Page

LLDP Remote Device Summary

Help

Display

All

 rows

Showing 1 to 5 of 5 entries

Filter:

↕Interface	↕Remote ID	↕Chassis ID	↕Port ID	↕Port Description	↕System Name	↕Capabilities Supported	↕Capabilities Enabled	↕System ID
1	61	00:1E:C9:AA:AD:F7	Gi1/0/18					001EC9AAADF7
4	174	9C:DC:71:AE:10:4C	9C:DC:71:AE:10:4E	4		bridge, router	bridge	10.130.174.158
5	177	9C:DC:71:AE:10:D8	9C:DC:71:AE:10:DA	5		bridge, router	bridge	10.130.173.157
6	175	9C:DC:71:AE:10:4C	9C:DC:71:AE:10:4E	6		bridge, router	bridge	10.130.174.158
8	72	9C:DC:71:AE:10:4C	9C:DC:71:AE:10:4E	8		bridge, router	bridge	10.130.174.158

First

Previous

1

Next

Last

Refresh

Table 49. LLDP Remote Device Summary Fields

Field	Description
Interface	The HPE OfficeConnect 1920S 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.
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.

LLDP Global Statistics

The Link Layer Discovery Protocol (LLDP) Statistics page displays summary and per-port information for LLDP and LLDP-MED frames transmitted and received on the switch.

To display the LLDP Global Statistics page, click **LLDP > Statistics** in the navigation pane.

Figure 74. LLDP Statistics Page

LLDP Global Statistics

Help

Insertions2

Deletions0

Drops0

Age Outs0

Time Since Last Update0 days 01:01:10

Display10▼ rows

Showing 1 to 10 of 26 entries

Filter:

↕ Interface	↕ Transmitted Frames	↕ Received Frames	↕ Discarded Frames	↕ Errors	↕ MED TLVs
1	0	0	0	0	0
2	0	0	0	0	0
3	121	121	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0
8	0	0	0	0	0
9	121	699	0	0	0
10	0	0	0	0	0

First

Previous

1

2

3

Next

Last

Refresh

Clear All Counters

Table 50. LLDP Global Statistics Fields

Field	Description
Global Statistics	
Insertions	The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into tables associated with the remote systems.
Deletions	The number of times the complete set of information advertised by a particular MSAP has been deleted from tables associated with the remote systems.
Drops	The number of times the complete set of information advertised by a particular MSAP could not be entered into tables associated with the remote systems because of insufficient resources.
Age Outs	The number of times the complete set of information advertised by a particular MSAP has been deleted from tables associated with the remote systems because the information timeliness interval has expired.
Time Since Last Update	Time when an entry was created, modified, or deleted in the tables associated with the remote system.
Interface Statistics	
Interface	The interface ID.
Transmitted Frames	The number of LLDP frames transmitted on the interface.
Received Frames	The number of valid 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.
MED TLVs	The total number of LLDP-MED TLVs received on the interface.

Click **Clear All Counters** to reset all statistics to their initial values.

LLDP-MED Global Configuration

LLDP-MED is an enhancement to LLDP that enables:

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

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

Figure 75. LLDP-MED Global Configuration Page

LLDP-MED Global Configuration Help

Fast Start Repeat Count (1 to 10)

Device Class

Display rows Showing 1 to 10 of 26 entries Filter:

<input type="checkbox"/>	↕ Interface	↕ Link Status	↕ MED Mode	↕ Notification Status	↕ Operational Status	↕ Transmitted TLVs
<input type="checkbox"/>	1	Down	Enabled	Disabled	Disabled	Capabilities, Network Policy
<input type="checkbox"/>	2	Down	Enabled	Disabled	Disabled	Capabilities, Network Policy
<input type="checkbox"/>	3	Up	Enabled	Disabled	Disabled	Capabilities, Network Policy
<input type="checkbox"/>	4	Down	Enabled	Disabled	Disabled	Capabilities, Network Policy
<input type="checkbox"/>	5	Down	Enabled	Disabled	Disabled	Capabilities, Network Policy
<input type="checkbox"/>	6	Down	Enabled	Disabled	Disabled	Capabilities, Network Policy
<input type="checkbox"/>	7	Down	Enabled	Disabled	Disabled	Capabilities, Network Policy
<input type="checkbox"/>	8	Down	Enabled	Disabled	Disabled	Capabilities, Network Policy
<input type="checkbox"/>	9	Up	Enabled	Disabled	Disabled	Capabilities, Network Policy
<input type="checkbox"/>	10	Down	Enabled	Disabled	Disabled	Capabilities, Network Policy

1 **2** 3

The following global settings display:

Table 51. LLDP-MED Global Configuration Fields

Field	Description
Fast Start Repeat Count	The number of LLDP-MED Protocol Data Units (LLDPDUs) that are transmitted during the fast start period when LLDP-MED is enabled. The default is 3.
Device Class	The device's MED classification. The HPE OfficeConnect 1920S switch is classified as a Network Connectivity device.

If you change the Fast Start Repeat Count, 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**.

The following information displays for each port:

Table 52. LLDP Global Configuration—Port 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 device. The switch waits for the LLDP-MED device to advertise its information before the switch transmits its own LLDP-MED TLVs, at which point the operational status becomes enabled.
Transmitted TLVs	The LLDP-MED TLV(s) that the interface transmits. The HPE OfficeConnect 1920S switch, can transmit TLVs of the following types: <ul style="list-style-type: none">• Capabilities• Network Policy

To enable or disable LLDP-MED on one or more interfaces, and to configure related features, select the interfaces and click **Edit**.

Figure 76. Edit LLDP-MED Interface

The screenshot shows a dialog box titled "Edit LLDP-MED Interface". Inside, the "Interface" is set to "4". The "LLDP-MED Mode" is set to "Enabled" with a selected radio button. The "Configuration Notification Mode" is set to "Disabled" with a selected radio button. Under the "Transmit TLVs" section, both "Capabilities" and "Network Policy" are checked with checkboxes. At the bottom, there are "Apply" and "Cancel" buttons.

To modify settings on all interfaces, click **Edit All**. The settings you configure are applied to all interfaces.

LLDP-MED Local Device Summary

Use the LLDP-MED Local Device Summary to view the information that is advertised by the switch interfaces when they are enabled for LLDP-MED. To display this page, click **LLDP-MED > Local Devices** in the navigation pane.

Figure 77. LLDP-MED Local Device Summary Page

LLDP-MED Local Device Summary

Help

Display 10 rows

Showing 1 to 10 of 26 entries

Filter:

Interface	Port ID
1	1C:98:EC:7C:8E:42
2	1C:98:EC:7C:8E:42
3	1C:98:EC:7C:8E:42
4	1C:98:EC:7C:8E:42
5	1C:98:EC:7C:8E:42
6	1C:98:EC:7C:8E:42
7	1C:98:EC:7C:8E:42
8	1C:98:EC:7C:8E:42
9	1C:98:EC:7C:8E:42
10	1C:98:EC:7C:8E:42

First

Previous

1

2

3

Next

Last

Refresh

Table 53. LLDP-MED Local Device Summary Fields

Field	Description
Interface	The trunk or port ID.
Port ID	The interface identifier, which is its physical address.

LLDP-MED Remote Device Summary

Use the LLDP-MED Remote Device Summary 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 device.

To display this page, click **LLDP-MED > Remote Devices** in the navigation pane.

Figure 78. LLDP-MED Remote Device Summary Page

Interface	Remote ID	Device Class	System ID
3	2	Not Defined	10.27.36.234
9	1	Not Defined	10.27.36.154

Table 54. 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.
Device Class	<p>The MED Classification advertised by the TLV from the remote device. The following three classifications represent the actual endpoints:</p> <ul style="list-style-type: none">• Class I Generic (for example, IP Communication Controller)• Class II Media (for example, Conference Bridge)• Class III Communication (for example, IP Telephone) <p>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.</p>
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 interface that received the LLDP-MED data and click **Details**.

Figure 79. LLDP-MED Remote Device Information Page

LLDP-MED Remote Device Information

Interface 1

Remote ID 1

Capability Information

Supported Capabilities

Enabled Capabilities

Device Class

Network Policy Information

Media Application Type	VLAN ID	Priority	DSCP	Unknown Bit Status	Tagged Bit Status
------------------------	---------	----------	------	--------------------	-------------------

Inventory Information

Hardware Revision

Firmware Revision

Software Revision

Serial Number

Manufacturer Name

Model Name

Asset ID

Extended PoE

Device Type	PSE
-------------	-----

Extended PoE PD

Required	0 Watts
Source	Unknown
Priority	Unknown

Close

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

Field	Description
Capability Information	
Supported Capabilities	The supported capabilities that were received in the MED TLV on this interface.
Enabled Capabilities	The supported capabilities on the remote device that are also enabled.
Device Class	The MED Classification advertised by the TLV from the remote device.

Field	Description
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, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streamingvideo, vidoesignalling. 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.
Inventory Information	
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.
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.

8 Power Over Ethernet

NOTE:
The information in this chapter is valid only for the HPE OfficeConnect 1920S switches that support PoE. The switches that do not have PoE ports do not include the web pages this chapter describes.

Power Over Ethernet (PoE) functionality is supported on certain HPE OfficeConnect 1920S switch models, enabling designated switch ports to provide power to connected devices. The devices receiving power through PoE are referred to as powered devices (PDs).

The switch automatically detects the presence of a PD on a PoE-enabled port, and the switch can learn power requirements from LLDP messages from the PD. Power allocation can also be configured statically per port.

The PoE software supports sharing the available power among the PoE-enabled ports. Ports are assigned one of three configurable PoE priority values (High, Low, and None). When more power is requested than is available on the switch, the switch provides power to a high priority ports before lower priority ports.

Power allocation can be scheduled so that power is supplied only during periods when the PD is actually in use.

PoE Capabilities

The HPE OfficeConnect 1920S PoE-enabled switches support the original PoE specification (IEEE 802.3af) and the PoE Plus specification (IEEE 802.1at). IEEE 802.3af, enables providing up to 15.4W of power over a PoE port, whereas PoE Plus enables providing up to 30W of power.

Table 55 shows which ports on each switch support PoE and PoE Plus, along with the maximum power the switch can provide to all PoE ports combined.

Table 55. PoE Ports and Power Capabilities

Switch	Ports that Support PoE	Ports that Support PoE Plus	Maximum Power Available to All Ports
8-Port PoE Plus	Ports 1–4	Any 2 of Ports 1–4	65W
24-Port PoE Plus	Ports 1–12	Any 6 of Ports 1–12	185W
24-Port PoE Plus	Ports 1–24	Any 12 of Ports 1–24	370W
48-Port PoE Plus	Ports 1–24	Any 12 of Ports 1–24	370W

The maximum power that the switch can provide is configurable on a per-port basis.

PoE Configuration

Use the PoE Configuration page to view global PoE settings. To display this page, click **Power Over Ethernet > Configuration** in the navigation pane.

Figure 80. PoE Configuration Page

PoE Configuration

Help

PoE Power Status

Idle

Total Power (Watts)

390

Power Consumption (Watts)

0

Power Management Mode

Static

☒ Dynamic

Apply

Refresh

Cancel

Table 56. PoE Configuration Fields

Field	Description
PoE Power Status	The current status of the switch PoE functionality. Possible values are: <ul style="list-style-type: none">Delivering—At least one port on the switch is delivering power to a connected device.Idle—The PoE functionality is operational but no ports are delivering power.Faulty—The PoE functionality is not operational.
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.
Power Management Mode	Select the method by which the PoE controller determines supplied power. Possible values are: <ul style="list-style-type: none">Static—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.Dynamic—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. <p>Note: In either mode, High Power Mode must be enabled on the port when PoE+ functionality is required. See “PoE Port Configuration” on page 115.</p>

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 Configuration

You can use the PoE Port Configuration page to administratively enable or disable PoE on ports that support it and to configure the port priority and other settings. To display this page, click **Power Over Ethernet > Port Configuration** in the navigation pane.

Figure 81. PoE Port Configuration Page

PoE Port Configuration

Help

Display 10 rows

Showing 1 to 10 of 24 entries

Filter:

<input type="checkbox"/>	↕ Interface	↕ Admin Mode	↕ Priority	↕ Schedule	↕ High Power Mode	↕ Power Detect Type	↕ Power Limit Type	↕ Status	↕ Fault Status
<input type="checkbox"/>	1	Enabled	Low	None	Disabled	802.3af/at	Class	Searching	None
<input type="checkbox"/>	2	Enabled	Low	None	Disabled	802.3af/at	Class	Searching	None
<input type="checkbox"/>	3	Enabled	Low	None	Disabled	802.3af/at	Class	Searching	None
<input type="checkbox"/>	4	Enabled	Low	None	Disabled	802.3af/at	Class	Searching	None
<input type="checkbox"/>	5	Enabled	Low	None	Disabled	802.3af/at	Class	Searching	None
<input type="checkbox"/>	6	Enabled	Low	None	Disabled	802.3af/at	Class	Searching	None
<input type="checkbox"/>	7	Enabled	Low	None	Disabled	802.3af/at	Class	Searching	None
<input type="checkbox"/>	8	Enabled	Low	None	Disabled	802.3af/at	Class	Searching	None
<input type="checkbox"/>	9	Enabled	Low	None	Disabled	802.3af/at	Class	Searching	None
<input type="checkbox"/>	10	Enabled	Low	None	Disabled	802.3af/at	Class	Searching	None

First

Previous

1

2

3

Next

Last

Refresh

Edit

Edit All

Reset

Details

The following settings display for each port that supports PoE.

Table 57. PoE Port Configuration Fields

Field	Description
Interface	The port number.
Admin Mode	Indicates whether PoE is administratively enabled or disabled on the port. This feature is enabled by default on ports that support PoE.
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 High, Low, and None. None is the lowest priority and the default for all ports.
Schedule	The scheduled time, if any, when source power is available on this port. Options are: <ul style="list-style-type: none">None—Source power is available at all times (subject to the port priority). This is the default selection.Schedule 1—Source power is available during the configured first schedule.Schedule 2—Source power is available during the configured second schedule. You can configure schedules on the PoE Port Schedule page.
High Power Mode	When enabled, the port supports the original PoE standard and the PoE+ standard, which allows for providing up to 30W of power. When disabled, the port supports the original PoE standard, which allows for providing up to 15.4W of power, and supports Type-2 PSE 1-event classification. This is the default behavior. If PoE+ functionality is required, this setting can be enabled on the port, even when the switch is configured to operate in Dynamic Power Management mode (which is configured on the PoE Configuration page, see "PoE Configuration" on page 114). If LLDP negotiates to High Power Mode, the port will be placed in High Power Mode.

Field	Description
Power Detect Type	The PD detection mechanism performed by the PSE port. Possible value are: <ul style="list-style-type: none"> Dot3af/at—The 4-point detection scheme defined in IEEE 802.3af is used. This is the default option. Dot3af/at + Pre-Standard—The 4-point detection scheme defined in IEEE 802.3af is used. If this mechanism fails to detect a connected PD, Dot3af/at detection is used.
Power Limit Type	The type of power limiting used for the port. Possible values are: <ul style="list-style-type: none"> Class—The device class determines the power limit. The switch learns the class of the device through the receipt of LLDP messages. This is the default selection. User—The power limit is user-defined, overriding the LLDP information. When set to User, the specified power limit also displays next to this value. When High Power Mode is enabled, the maximum value is 30W. When High Power Mode is disabled, the maximum value is 15.4W. (The Power Limit field is available on the Edit PoE Port Configuration page.)
Status	The status of the port as a provider of power over Ethernet. Such devices are referred to as power-sourcing equipment (PSE). Possible values are: <ul style="list-style-type: none"> Disabled—The PSE is disabled. Delivering Power—The PSE is delivering power. Fault—The PSE has experienced a fault condition. Test—The PSE is in test mode. Other Fault—The PSE has experienced a variable error condition. Searching—The PSE is transitioning between states. Requesting Power—The PSE is currently not able to deliver power because power is unavailable to the port.
Fault Status	The fault status, if a fault occurred. Possible values are: <ul style="list-style-type: none"> None—No faults have occurred. Short—The switch provided insufficient current to a connected PD Overload—A connected PD has attempted to draw more than the allowed watts. Power Denied—A PD requesting power on the port has been denied because of insufficient power available.

Modifying Port PoE Settings

To change PoE settings for a port, select the checkbox associated with it and click **Edit**.

Figure 82. Edit PoE Port Configuration Page

NOTE: The values displayed are based on the first selected item from the table.

Interface: 5, 9

Admin Mode: ☒ Enabled ☐ Disabled

Schedule:

Priority: ☐ Critical ☐ High ☒ Low

High Power Mode: ☐ Enabled ☒ Disabled

Power Detect Type: ☒ 802.3af/at ☐ 802.3af/at + Pre-Standard

Power Limit Type: ☒ Class ☐ User

Power Limit (Watts):

Apply Cancel

To configure the same settings for all PoE-enabled ports, click **Edit All**.

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**.

Viewing PoE Port Details

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

Figure 83. PoE Port Details Page

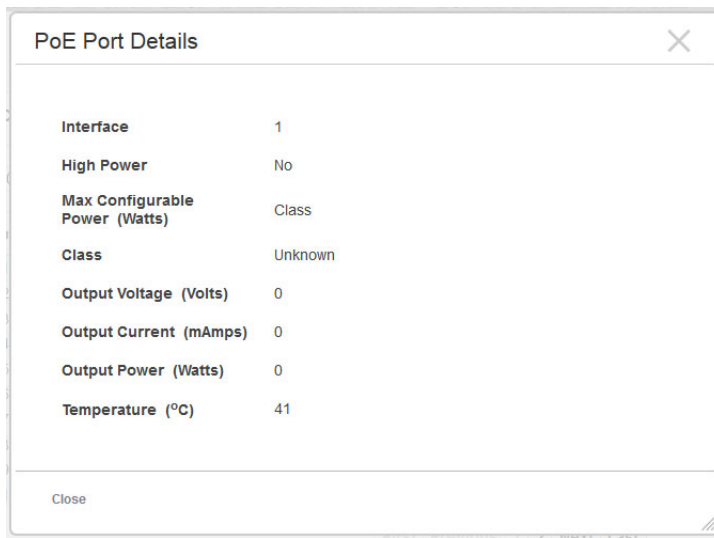


Table 58. PoE Port Details Fields

Field	Description
Interface	The port number.
High Power	Indicates whether high power mode is enabled or disabled. When enabled, the port supports the PoE+ power standard, which allows for providing up to 30W of power. When disabled, the port supports the original PoE standard only, which allows for providing up to 15.4W of power.
Max Configurable Power	If the Power Limit Type for the port is User (user-defined), this field displays the configured power limit. If the Power Limit type is set to Class, then Class displays.
Class	If the Power Limit Type is set to Class, this field displays the class of the connected device, as learned in LLDP messages. Possible values are Unknown and Class 0 through Class 4. A higher class value indicates that the device requires higher power.
Output Voltage	The voltage being applied to the connected device.
Output Current	The current in milliamps being drawn by the powered device.
Output Power	The power in watts being drawn by the connected device.
Temperature	The temperature measured at the PoE port.

PoE Port Schedule

You can configure schedules for the allocation of power to PoE ports. Two built-in schedules, Schedule 1 and Schedule 2, are available for configuration. Schedules consist of one or more time periods when PoE power is to be supplied.

Time periods can be periodic or absolute. A periodic entry occurs at the same time every day or on one or more days of the week. An absolute entry does not repeat. Each schedule can have multiple periodic entries but only one absolute entry. Up to 10 time periods can be configured per schedule.

To display the PoE Port Schedule page, click **Power Over Ethernet > Schedule** in the navigation pane.

Figure 84. PoE Port Schedule Page

PoE Port Schedule

Help

To customize one of the two available schedules for PoE select the schedule from the list below and add the scheduled time ranges in which PoE will be enabled. Each schedule allows a single absolute time range and multiple periodic time ranges.

Schedule

Schedule-1

Display All rows

Showing 1 to 2 of 2 entries

Filter:

<input type="checkbox"/>	Entry Type	Starts	Ends
<input type="checkbox"/>	Absolute	18:00 February 21, 2015	06:00 February 24, 2015
<input type="checkbox"/>	Periodic	00:01 Sunday, Saturday	23:59 Sunday, Saturday

First

Previous

1

Next

Last

Refresh

Add Absolute

Add Periodic

Remove

Table 59. PoE Port Schedule Fields

Field	Description
Schedule	Select Schedule-1 or Schedule-2 to display information on time periods configured for the schedule, if any.
Entry Type	The type of time period entry, which is one of the following: <ul style="list-style-type: none">Absolute—A single time period that occurs once or has an undefined start or end period. The duration of an absolute entry can be hours, days, or even years. Each time entry configuration can have only one entry.Periodic—A recurring entry that takes place at fixed intervals. This type of entry occurs at the same time on one or more days of the week.
Starts	For an absolute entry, this field indicates the time, day, month, and year that the entry begins. If this field is blank, the absolute entry became active when it was configured. For a periodic entry, this field indicates the time and day(s) of the week that the entry begins.
Ends	For an absolute entry, indicates the time, day, month, and year that the entry ends. If this field is blank, the absolute entry does not have a defined end. For a periodic entry, this field indicates the time and day(s) of the week that the entry ends.

To configure a schedule, select the schedule from the **Schedule** list, then click **Absolute** or **Periodic**. If the **Absolute** button is not available, an absolute entry already exists for the selected schedule.

Configuring an Absolute Time Period

To configure an absolute schedule, select the schedule from the **Schedule** list and click **Add Absolute**.

Figure 85. Add Absolute Time Period Page

Add Absolute Time Period

Note: The system clock is set by manual configuration.

Schedule: Schedule-1

Start Time: ☐

Start Date: February 21, 2015

Starting Time of Day: 18:00 (00:00 to 23:59)

End Time: ☐

End Date: February 24, 2015

Ending Time of Day: 06:00 (00:00 to 23:59)

Apply Cancel

Table 60. Add Absolute Time Period Fields

Field	Description
Schedule	The schedule to be configured.
Start Time	Select this option to configure values for the Start Date and the Starting Time of Day fields. If this option is not selected, the entry becomes active immediately. It is not selected by default.
Start Date	Click the calendar icon to select the day, month, and year when this entry becomes active. This field can be configured only when the Start Time option is selected.
Starting Time of Day	Specify the time of day that the entry becomes active by entering the information in the field or by using the scroll bar in the Choose Time window, which displays when you click the field. You can click Now to use the current time of day. Click Done to close the window.
End Time	Select this option to configure values for the End Date and Ending Time of Day fields. If this option is not selected, the entry does not have an end time; after the time period starts, it will remain active indefinitely.
End Date	Click the calendar icon to select the day, month, and year when this entry should no longer be active.
Ending Time of Day	Specify the time of day that the entry becomes inactive by entering the information in the field or by using the scroll bar in the Choose Time window, which displays when you click the field. Click Now to use the current time of day. Click Done to close the window.

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**.

Adding a Periodic Time Period

To configure a periodic schedule, select the schedule from the **Schedule** list and click **Add Periodic**.

NOTE:

Periodic time periods cannot overlap. Consecutive periodic time periods must be at least three minutes apart.

Figure 86. Add Periodic Time Period Page

Table 61. Add Periodic Time Period Fields

Field	Description
Schedule	The schedule to be configured.
Applicable Days	Select the days on which the periodic time range entry is active. If you select Days of Week , you can select multiple days from the Start Days list.
Start Days	Indicates the days on which the time period becomes active. The days are autoselected to correspond to your choice in the Applicable Days field. If you selected Days of Week , you can hold down the Ctrl key to select multiple days.
Starting Time of Day	Specify the time of day that the entry becomes active by entering the information in the field or by using the scroll bar in the Choose Time window, which displays when you click the field. You can click Now to use the current time of day. Click Done to close the window.
End Days	Indicates the days on which the time entry ends. The days are autoselected to correspond to your choice in the Applicable Days . If you selected Days of Week , the selected days correspond to your selections in the Start Days list.
Ending Time of Day	Specify the time of day that the entry becomes inactive by entering the information in the field or by using the scroll bar in the Choose Time window, which displays when you click the field. Click Now to use the current time of day. Click Done to close the window.

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**.

9 Routing

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

Routing Configuration

Use the pages under the Configuration link to view global routing status and statistics and to configure global routing settings and routing interfaces.

Routing IP Interface Summary

This page shows summary information about the routing configuration for all interfaces. To view additional routing configuration information for an interface, select the interface with the settings to view and click **Details**.

To display the Routing IP Interface Summary page, click **Routing > Configuration** in the navigation pane, and ensure that the **Status** tab is selected.

Figure 87. Routing IP Interface Summary Page

StatusGlobalVLAN/Interface ConfigurationStatistics

Routing IP Interface Summary

Help

Display 10 rowsShowing 1 to 10 of 26 entriesFilter:

	Interface	Status	IP Address	Subnet Mask	Admin Mode	State	MAC Address	Proxy ARP	IP MTU
<input type="checkbox"/>	1	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	1C:98:EC:7C:8E:42	Disabled	1500
<input type="checkbox"/>	2	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	1C:98:EC:7C:8E:42	Disabled	1500
<input type="checkbox"/>	3	Down	0.0.0.0	0.0.0.0	Enabled	Active	1C:98:EC:7C:8E:42	Disabled	1500
<input type="checkbox"/>	4	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	1C:98:EC:7C:8E:42	Disabled	1500
<input type="checkbox"/>	5	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	1C:98:EC:7C:8E:42	Disabled	1500
<input type="checkbox"/>	6	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	1C:98:EC:7C:8E:42	Disabled	1500
<input type="checkbox"/>	7	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	1C:98:EC:7C:8E:42	Disabled	1500
<input type="checkbox"/>	8	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	1C:98:EC:7C:8E:42	Disabled	1500
<input type="checkbox"/>	9	Down	0.0.0.0	0.0.0.0	Enabled	Active	1C:98:EC:7C:8E:42	Disabled	1500
<input type="checkbox"/>	10	Down	0.0.0.0	0.0.0.0	Enabled	Inactive	1C:98:EC:7C:8E:42	Disabled	1500

FirstPrevious123NextLast

RefreshDetails

Table 62. Routing IP Interface Summary Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When viewing details about the routing settings for an interface, this field identifies the interface being viewed.
Status	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).
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.

Field	Description
Admin Mode	The administrative mode of the interface, which is either Enabled or Disabled.
State	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 of the 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.
IP MTU	The largest IP packet size the interface can transmit, in bytes. The IP Maximum Transmission Unit (MTU) is the maximum frame size minus the length of the Layer 2 header.

To view additional information about an interface, select it and click **Details**. The following information describes the fields in the **Details** window that are not displayed on the summary page.

Table 63. Detailed Routing IP Interface Fields

Field	Description
Routing Mode	Indicates whether routing is administratively enabled or disabled on the interface.
Link Speed Data Rate	The physical link data rate of the interface.
IP Address Configuration Method	The source of the IP address, which is one of the following: <ul style="list-style-type: none"> • None – The interface does not have an IP address. • Manual – The IP address has been statically configured by an administrator. • DHCP – The IP address has been learned dynamically through DHCP. If the method is DHCP but the interface does not have an IP address, the interface is unable to acquire an address from a network DHCP server.
Bandwidth	The configured bandwidth on this interface. This setting communicates the speed of the interface to higher-level protocols.
Encapsulation Type	The link layer encapsulation type for packets transmitted from the interface, which can be either Ethernet or SNAP.
Forward Net Directed Broadcasts	Indicates how the interface handles network-directed broadcast packets. A network-directed broadcast is a broadcast directed to a specific subnet. The possible values are as follows: <ul style="list-style-type: none"> • Enabled – Network directed broadcasts are forwarded. • Disabled – Network directed broadcasts are dropped.
Local Proxy ARP	Indicates whether local proxy ARP is enabled or disabled on the interface. When local proxy ARP is enabled, the interface can respond to an ARP request for a host other than itself. Unlike proxy ARP, local proxy ARP allows the interface to respond to ARP requests for a host that is on the same subnet as the host that sent the ARP request. This feature is useful when a host is not permitted to reply to an ARP request from another host in the same subnet, for example when using the protected ports feature.
Destination Unreachables	Indicates whether the interface is allowed to send ICMP Destination Unreachable message to a host if the intended destination cannot be reached for some reason. If the status of this field is Disabled, this interface will not send ICMP Destination Unreachable messages to inform the host about the error in reaching the intended destination.
ICMP Redirects	Indicates whether the interface is allowed to send ICMP Redirect messages. The device sends an ICMP Redirect message on an interface only if ICMP Redirects are enabled both globally and on the interface. An ICMP Redirect message notifies a host when a better route to a particular destination is available on the network segment.

Global Routing IP Configuration

Use the Routing IP Configuration page to configure global routing settings on the device. Routing provides a means of transmitting IP packets between subnets on the network. Routing configuration is necessary only if the device is used as a Layer 3 device that routes packets between subnets. If the device is used as a Layer 2 device that handles switching only, it typically connects to an external Layer 3 device that handles the routing functions; therefore, routing configuration is not required on the Layer 2 device.

To display the Routing IP Configuration page, click **Routing > Configuration** in the navigation pane and click the **Global** tab.

Figure 88. Routing IP Configuration Page

The screenshot shows the 'Routing IP Configuration' page with the 'Global' tab selected. The 'Routing Mode' is set to 'Disabled'. 'ICMP Echo Replies' and 'ICMP Redirects' are enabled. The 'ICMP Rate Limit Interval' is 1000, 'ICMP Rate Limit Burst Size' is 100, 'Static Route Preference' is 1, 'Local Route Preference' is 0, 'Maximum Next Hops' is 1, 'Maximum Routes' is 64, and 'Global Default Gateway' is empty. The 'Apply', 'Refresh', and 'Cancel' buttons are at the bottom.

Table 64. Routing IP Configuration Fields

Field	Description
Routing Mode	The administrative mode of routing on the device. The options are as follows: <ul style="list-style-type: none">• Enable – The device can act as a Layer 3 device by routing packets between interfaces configured for IP routing.• Disable – The device acts as a Layer 2 bridge and switches traffic between interfaces. The device does not perform any internetwork routing.
ICMP Echo Replies	Select Enable or Disable from the drop-down menu. If you select Enable , then only the router can send ECHO replies. By default, ICMP Echo Replies are sent for echo requests.
ICMP Redirects	Select this option to allow the device to send ICMP Redirect messages to hosts. An ICMP Redirect message notifies a host when a better route to a particular destination is available on the network segment.
ICMP Rate Limit Interval	To control the ICMP error packets, you can specify the number of ICMP error packets that are allowed per burst interval. By default, the rate limit is 100 packets per second, i.e. the burst interval is 1000 milliseconds. To disable ICMP rate limiting, set this field to zero. The valid rate interval range is 0 to 2147483647 milliseconds.
ICMP Rate Limit Burst Size	To control the ICMP error packets, you can specify the number of ICMP error packets that are allowed per burst interval. By default, the burst size is 100 packets. When the burst interval is zero, then configuring this field is not a valid option. The valid burst size range is 1 to 200.

Field	Description
Static Route Preference	The default distance (preference) for static routes. Lower route-distance values are preferred when determining the best route. Changing the Static Route Preference does not update the preference of existing static routes.
Local Route Preference	The default distance (preference) for local routes.
Maximum Next Hops	The maximum number of hops supported by the switch. This is a read-only value.
Maximum Routes	The maximum number of routes (routing table size) supported by the switch.
Global Default Gateway	<p>The IP address of the default gateway for the device. 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 specified in this field is more preferred than a default gateway learned from a DHCP server. Use the icons associated with this field to perform the following tasks:</p> <ul style="list-style-type: none"> • To configure the default gateway, click the Edit icon and specify the IP address of the default gateway in the available field. • To reset the IP address of the default gateway to the factory default value, click the Reset icon associated with this field.

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**.

Routing IP VLAN/Interface Configuration

Use the Routing IP VLAN/Interface Configuration page to configure the IP routing settings for each interface.

To display the page, click **Routing > Configuration** in the navigation pane and click the **VLAN/Interface Configuration** tab.

Figure 89. Routing IP VLAN/Interface Configuration Page

The screenshot shows the 'Routing IP Interface Configuration' page. At the top, there are tabs: 'Status', 'Global', 'VLAN/Interface Configuration' (which is active), and 'Statistics'. Below the tabs is a title bar 'Routing IP Interface Configuration' with a 'Help' link on the right. The main configuration area is divided into two columns. The left column lists various settings, and the right column shows their current values or options. The settings include: 'Type' (radio buttons for 'VLAN' and 'Interface', with 'VLAN' selected), 'VLAN' (a dropdown menu showing 'VLAN 1'), 'Interface' (a dropdown menu showing '1'), 'Status' (text 'Down'), 'Routing Mode' (radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected), 'Admin Mode' (radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected), 'Link Speed Data Rate' (text field), 'IP Address Configuration Method' (radio buttons for 'None', 'Manual', and 'DHCP', with 'None' selected), 'DHCP Client Identifier' (checkbox), 'IP Address' (text field with placeholder '(x.x.x.x)'), 'Subnet Mask' (text field with placeholder '(x.x.x.x)'), 'MAC Address' (text field), 'IP MTU' (text field with value '1500' and range '(68 to 1500)'), 'Bandwidth' (text field with value '10000' and range '(1 to 10000000)'), 'Encapsulation Type' (radio buttons for 'Ethernet' and 'SNAP', with 'Ethernet' selected), 'Forward Net Directed Broadcasts' (checkbox), 'Proxy ARP' (checkbox), 'Local Proxy ARP' (checkbox), 'Destination Unreachables' (checkbox), and 'ICMP Redirects' (checkbox). At the bottom of the page are three buttons: 'Apply' (green), 'Refresh' (blue), and 'Cancel' (grey).

Table 65. Routing IP VLAN/Interface Configuration Fields

Field	Description
Type	The type of interface that can be configured for routing: <ul style="list-style-type: none">Interface – Enables list of all non-loopback interfaces that can be configured for routing.VLAN – Enables list of all VLANs that can be configured for routing.
VLAN	The menu contains all VLANs that can be configured for routing. To configure routing settings for a VLAN, select it from the menu and then configure the rest of the settings on the page.
Interface	The menu contains all non-loopback interfaces that can be configured for routing. To configure routing settings for an interface, select it from the menu and then configure the rest of the settings on the page.

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).
Routing Mode	The administrative mode of IP routing on the interface.
Admin Mode	The administrative mode of the interface. If an interface is administratively disabled, it cannot forward traffic.
State	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.
Link Speed Data Rate	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: <ul style="list-style-type: none"> • None – No address is to be configured. • Manual – The address is to be statically configured. When this option is selected 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.
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 will be displayed beside the check box once DHCP is enabled on the port on which the Client Identifier option is selected. This web page will need to be refreshed once this change is made.
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 is blank, 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.
MAC Address	The burned-in physical address of the interface. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
IP MTU	The largest IP packet size the interface can transmit, in bytes. The IP Maximum Transmission Unit (MTU) is the maximum frame size minus the length of the Layer 2 header.
Bandwidth	The configured bandwidth on this interface. This setting communicates the speed of the interface to higher-level protocols.
Encapsulation Type	The link layer encapsulation type for packets transmitted from the interface, which can be either Ethernet or SNAP.
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 selected, network directed broadcasts are forwarded. If this option is clear, network directed broadcasts are dropped.
Proxy ARP	When this option is selected, 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.
Local Proxy ARP	When this option is selected, local proxy ARP is enabled, and the interface can respond to an ARP request for a host other than itself. Unlike proxy ARP, local proxy ARP allows the interface to respond to ARP requests for a host that is on the same subnet as the host that sent the ARP request. This feature is useful when a host is not permitted to reply to an ARP request from another host in the same subnet, for example when using the protected ports feature.

Field	Description
Destination Unreachables	When this option is selected, the interface is allowed to send ICMP Destination Unreachable message to a host if the intended destination cannot be reached for some reason. If this option is clear, the interface will not send ICMP Destination Unreachable messages to inform the host about the error in reaching the intended destination.
ICMP Redirects	When this option is selected, the interface is allowed to send ICMP Redirect messages. The device sends an ICMP Redirect message on an interface only if ICMP Redirects are enabled both globally and on the interface. An ICMP Redirect message notifies a host when a better route to a particular destination is available on the network segment.

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**.

Routing IP Statistics

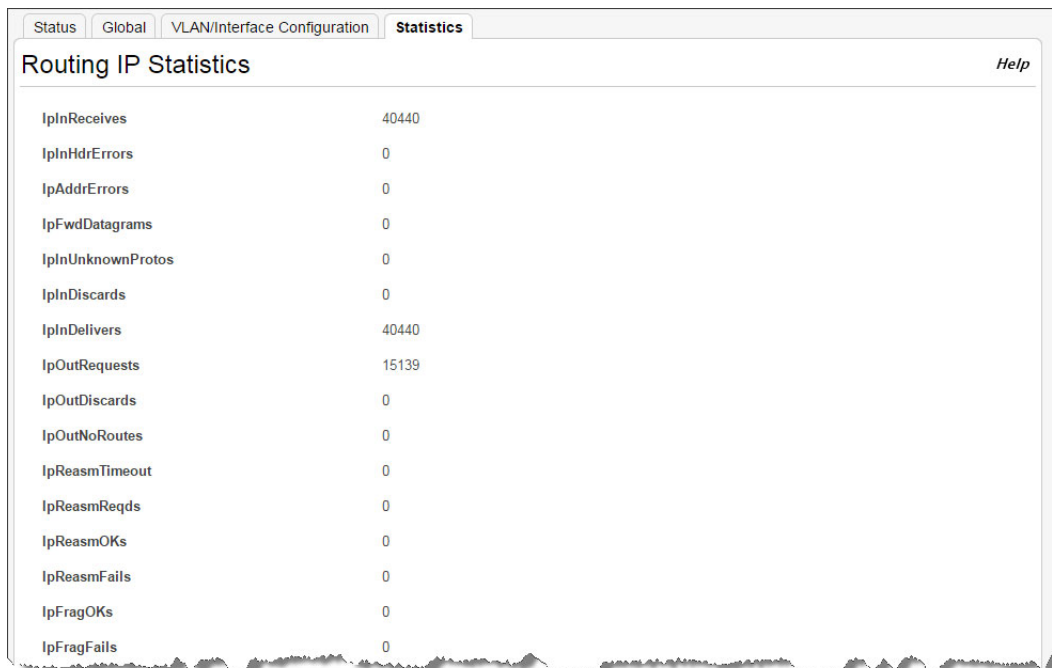
The statistics reported on the IP Statistics page are as specified in RFC 1213.

To display the Routing IP Statistics page, click **Routing > Configuration** in the navigation pane and click the **Statistics** tab.

NOTE:

[Figure 90](#) does not show all of the fields on the page.

Figure 90. Routing IP Statistics Page



Status	Global	VLAN/Interface Configuration	Statistics
Routing IP Statistics Help			
IpInReceives	40440		
IpInHdrErrors	0		
IpAddrErrors	0		
IpFwdDatagrams	0		
IpInUnknownProtos	0		
IpInDiscards	0		
IpInDelivers	40440		
IpOutRequests	15139		
IpOutDiscards	0		
IpOutNoRoutes	0		
IpReasmTimeout	0		
IpReasmReqds	0		
IpReasmOKs	0		
IpReasmFails	0		
IpFragOKs	0		
IpFragFails	0		

Table 66. 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.
IpFwdDatagrams	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 via this entity, and the Source-Route option processing was successful.
IpInUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
IpInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
IpInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
IpOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
IpOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
IpOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this 'no-route' criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
IpReasmTimeout	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
IpReasmReqds	The number of IP fragments received which needed to be reassembled at this entity.
IpReasmOKs	The number of IP datagrams successfully re-assembled.
IpReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.
IpFragOKs	The number of IP datagrams that have been successfully fragmented at this entity.
IpFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.
IpFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
IpRoutingDiscards	The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
IcmpInMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.

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

IPv4 Routing

The pages under the IPv4 Routing link allow you to configure and display route tables.

IP Route Summary

The IP Route Summary page displays summary information about the entries in the IP routing table. To display the IP Route Summary page, click **Routing > IPv4 Routing** in the navigation pane, and ensure that the **Status** tab is selected.

Figure 91. IP Route Summary Page

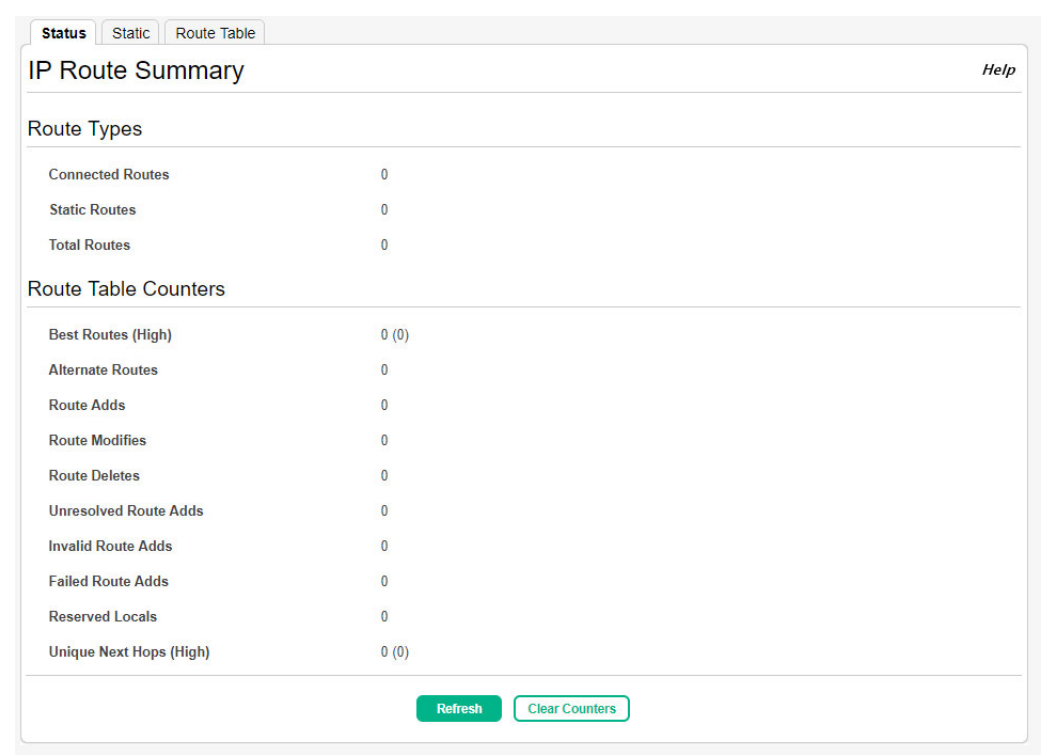


Table 67. IP Route Summary Fields

Field	Description
Route Types	
Connected Routes	The total number of connected routes in the IP routing table.
Static Routes	The total number of static routes in the IP routing table.
Total Routes	The total number of routes in the routing table.
Route Table Counters	
Best Routes (High)	The number of best routes currently in the routing table. This number only counts the best route to each destination.
Alternate Routes	The number of alternate routes currently in the routing table. An alternate route is a route that was not selected as the best route to its destination.

Field	Description
Route Adds	The number of routes that have been added to the routing table.
Route Modifies	The number of routes that have been changed after they were initially added to the routing table.
Route Deletes	The number of routes that have been deleted from the routing table.
Unresolved Route Adds	The number of route adds that failed because none of the route's next hops were on a local subnet. Note that static routes can fail to be added to the routing table at startup because the routing interfaces are not yet up. This counter gets incremented in this case. The static routes are added to the routing table when the routing interfaces come up.
Invalid Route Adds	The number of routes that failed to be added to the routing table because the route was invalid. A log message is written for each of these failures.
Failed Route Adds	The number of routes that failed to be added to the routing table because of a resource limitation in the routing table.
Reserved Locals	The number of routing table entries reserved for a local subnet on a routing interface that is down. Space for local routes is always reserved so that local routes can be installed when a routing interface bounces.
Unique Next Hops (High)	The number of distinct next hops used among all routes currently in the routing table. These include local interfaces for local routes and neighbors for indirect routes.
Routes with n Next Hops	The current number of routes with n , which represents a number, next hops. Note that this field is present only if there is at least one route with n next hops.

Use the **Clear Counters** button to reset the IPv4 routing table counters to zero. This only resets event counters. Counters that report the current state of the routing table, such as the number of routes of each type, are not reset

Configured Route Summary

Use the Configured Route Summary page to create and display static routes.

To display the IP Route Summary page, click **Routing > IPv4 Routing** in the navigation pane, and click the **Static** tab.

Figure 92. Configured Route Summary Page

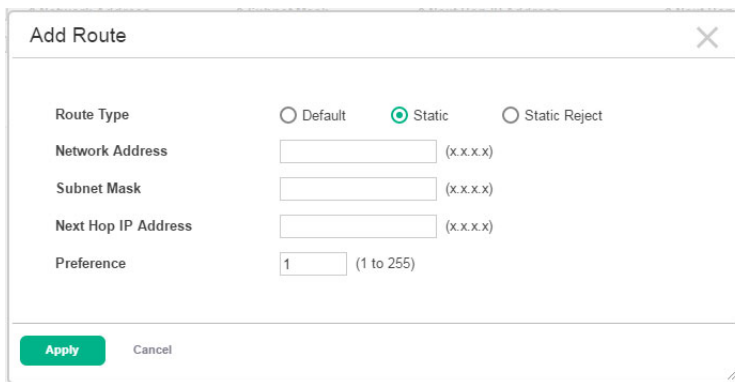
Table 68. Configured Route Summary Fields

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

1. From the Configured Route Summary page, click **Add**.
The **Add Route** page displays:

Figure 93. Add Route Page



2. Next to **Route Type**, select **Default** route, **Static** or **Static Reject** from the menu.
 - o **Default:** Enter the default gateway address in the **Next Hop IP Address** field.
 - o **Static:** Enter values for **Network Address**, **Subnet Mask**, **Next Hop IP Address**, and **Preference**.
 - o **Static Reject:** Packets to these destinations will be dropped.

NOTE:

The route type you select determines the fields available on the page.

3. Click **Apply**.

The new route is added, and you are returned to the Configured Routes page.

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

Removing a Route

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 lists all routes. The best routes table displays only the most preferred route to each destination.

To display the Route Table page, click **Routing > IPv4 Routing** in the navigation pane, and click the **Route Table** tab.

Figure 94. Route Table Page

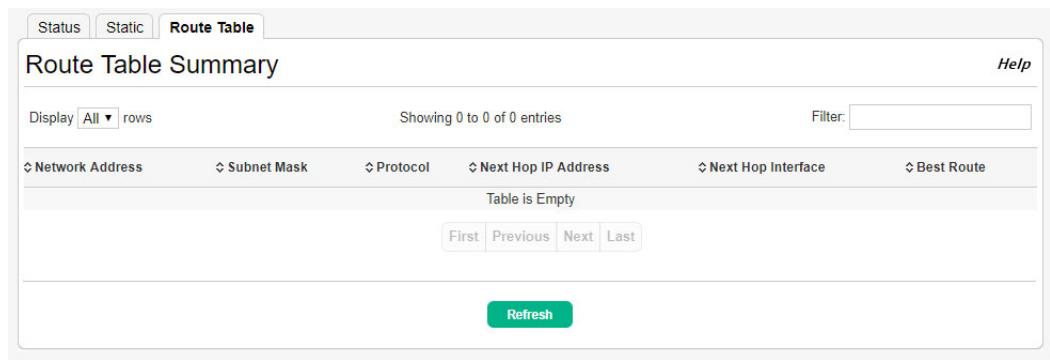


Table 69. Route Table Fields

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: <ul style="list-style-type: none">LocalStaticDefault
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly-attached network.
Next Hop Interface	The outgoing interface to use when forwarding traffic to the destination. For a static reject route, the next hop is Null.
Best Route	Indicates whether the route is the preferred route to the network. If the field is blank, a better route to the same network exists in the routing table.

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

DHCP Relay

HPE OfficeConnect 1920S switches can be used to relay packets between a DHCP client and server on different subnets. The switch acts as an L3 relay agent and must have an IP interface on the client subnets and, if it does not have an IP interface on the server's subnet, it should be able to route traffic toward the server's subnet.

DHCP Relay Global Configuration

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

To display the DHCP Relay Global Configuration page, click **Routing > DHCP Relay** in the navigation pane, and ensure that the **Global** tab is selected.

Figure 95. DHCP Relay Global Configuration Page

Table 70. DHCP Relay Global Configuration Fields

Field	Description
Admin Mode	The global mode of DHCP L3 relay on the device.
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.
Hit Count	The number of times a packet has been forwarded or discarded according to this entry.

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**.

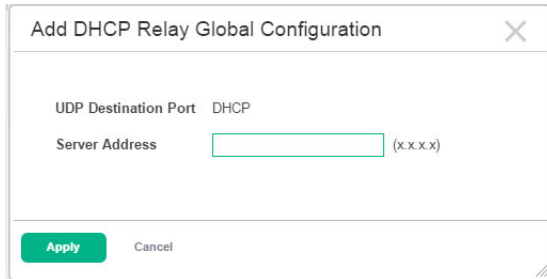
Adding a DHCP Server

To add a DHCP server to which packets are relayed:

1. Click **Add**.

The Add DHCP Relay Global Configuration page appears.

Figure 96. Add DHCP Relay Global Configuration Page



The dialog box titled "Add DHCP Relay Global Configuration" contains two input fields: "UDP Destination Port" with a dropdown menu set to "DHCP", and "Server Address" with a text input field and a placeholder "(x.x.x.x)". At the bottom, there are "Apply" and "Cancel" buttons.

2. Specify the IP address of the DHCP server.
3. Click **Apply**.

Removing a DHCP Server

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

DHCP Relay VLAN/Interface Configuration

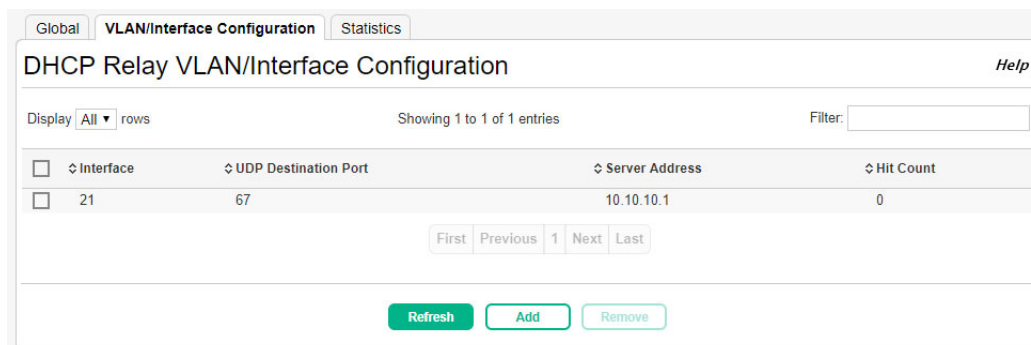
Use the DHCP Relay VLAN/Interface Configuration page to add, view, or delete the DHCP relay configuration on a selected routing interface.

To display the DHCP Relay VLAN/Interface Configuration page, click **Routing > DHCP Relay** in the navigation pane and click the **VLAN/Interface Configuration** tab.

NOTE:

DHCP relay can be configured on an VLAN or interface only if it is enabled for routing. If no interfaces or VLANs are enabled for routing, the page displays a message indicating this. To enable routing on an interface or VLAN, see [“Routing IP VLAN/Interface Configuration” on page 125](#).

Figure 97. DHCP Relay VLAN/Interface Configuration Page



The page shows the "DHCP Relay VLAN/Interface Configuration" tab selected. It includes a table with columns: Interface, UDP Destination Port, Server Address, and Hit Count. The table contains one entry for interface 21 with UDP Destination Port 67 and Server Address 10.10.10.1, with a Hit Count of 0. Below the table are navigation buttons: First, Previous, 1, Next, Last. At the bottom, there are "Refresh", "Add", and "Remove" buttons.

<input type="checkbox"/>	Interface	UDP Destination Port	Server Address	Hit Count
<input type="checkbox"/>	21	67	10.10.10.1	0

Table 71. DHCP Relay VLAN/Interface Configuration Fields

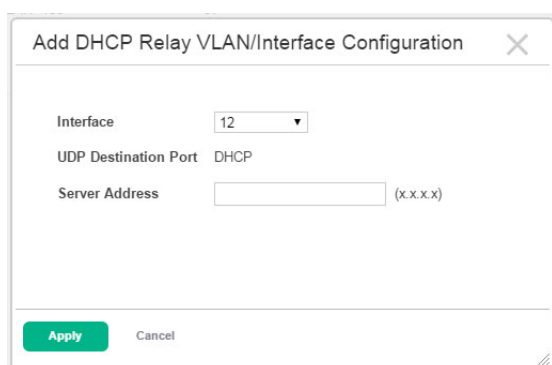
Field	Description
Interface	The routing interface that has the DHCP relay feature configured.
UDP Destination Port	The destination UDP port number of UDP packets to be relayed.
Server Address	The IPv4 address of the server to which packets are relayed for the specific UDP Destination Port.
Hit Count	The number of times a packet has been forwarded or discarded according to this entry.

Adding a DHCP Server

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

1. Click **Add**.

The Add DHCP Relay VLAN/Interface Configuration page appears.

Figure 98. Add DHCP Relay VLAN/Interface Configuration Page

2. Specify the IP address of the DHCP server to which the interface or VLAN should send packets.
3. 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**.

DHCP Relay Statistics

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

To display the DHCP Relay Statistics page, click **Routing > DHCP Relay** in the navigation pane and click the **Statics** tab.

Figure 99. DHCP Relay Statistics Page

Global

VLAN/Interface Configuration

Statistics

Table 72. DHCP Relay Statistics Fields

Field	Description
DHCP client messages received	The number of valid messages received from a DHCP client. The count is only incremented if DHCP relay is enabled globally, the ingress routing interface is up, and the packet passes a number of validity checks, such as having a TTL >1 and having valid source and destination IP addresses
DHCP client messages relayed	The number of DHCP client messages relayed to a server. If a message is relayed to multiple servers, the count is incremented once for each server.
DHCP server messages received	The number of DHCP responses received from the DHCP server. This count only includes messages that the DHCP server unicasts to the relay agent for relay to the client.
DHCP server messages relayed	Specifies the number of DHCP server messages relayed to a client.
UDP client messages received	The number of valid UDP packets received. This count includes DHCP messages and all other protocols relayed. Conditions are similar to those for the first statistic in this table.
UDP client messages relayed	The number of UDP packets relayed. This count includes DHCP messages relayed as well as all other protocols. The count is incremented for each server to which a packet is sent.
DHCP messages hop count exceeded max	The number of DHCP messages received whose hop count is larger than the maximum allowed. A log message is written for each such failure. The DHCP relay agent does not relay these packets.
DHCP message with secs field below min	The number of DHCP messages received whose secs field is less than the minimum value. A log message is written for each such failure. The DHCP relay agent does not relay these packets.

Field	Description
DHCP messages with giaddr as local address	The number of DHCP messages received whose gateway address, giaddr, is already set to an IP address configured on one of the relay agent's own IP addresses. In this case, another device is attempting to spoof the relay agent's address. The relay agent does not relay such packets. A log message gives details for each occurrence.
Pkts with expired TTL	The number of packets received with a time-to-live (TTL) of 0 or 1 that might otherwise have been relayed.

Configuring ARP

The ARP protocol associates a layer 2 MAC address with a layer 3 IPv4 address. HPE OfficeConnect 1920S software features both dynamic and manual ARP configuration. With manual ARP configuration, you can statically add entries into the ARP table.

ARP is a necessary part of the Internet protocol (IP) and is used to translate an IP address to a media (MAC) address, defined by a local area network (LAN) such as Ethernet. A station needing to send an IP packet must learn the MAC address of the IP destination, or of the next hop router, if the destination is not on the same subnet. This is achieved by broadcasting an ARP request packet, to which the intended recipient responds by unicasting an ARP reply containing its MAC address. Once learned, the MAC address is used in the destination address field of the layer 2 header prepended to the IP packet.

The ARP cache is a table maintained locally in each station on a network. ARP cache entries are learned by examining the source information in the ARP packet payload fields, regardless of whether it is an ARP request or response. Thus, when an ARP request is broadcast to all stations on a LAN segment or virtual LAN (VLAN), every recipient has the opportunity to store the sender's IP and MAC address in their respective ARP cache. The ARP response, being unicast, is normally seen only by the requester, who stores the sender information in its ARP cache. Newer information always replaces existing content in the ARP cache.

The number of supported ARP entries is platform-dependent.

Devices can be moved in a network, which means the IP address that was at one time associated with a certain MAC address is now found using a different MAC, or may have disappeared from the network altogether (i.e., it has been reconfigured, disconnected, or powered off). This leads to stale information in the ARP cache unless entries are updated in reaction to new information seen on the network, periodically refreshed to determine if an address still exists, or removed from the cache if the entry has not been identified as a sender of an ARP packet during the course of an age-out interval, usually specified via configuration.

ARP Table Summary

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

To display the ARP Table Summary page, click **Routing > ARP** in the navigation pane, and ensure that the **Status** tab is selected.

Figure 100. ARP Table Summary Page

The screenshot shows the 'ARP Table Summary' page in a web interface. At the top, there are three tabs: 'Status' (selected), 'Configuration', and 'Statistics'. The main heading is 'ARP Table Summary' with a 'Help' link on the right. Below the heading, there's a 'Display' dropdown menu set to 'All' rows, followed by the text 'Showing 0 to 0 of 0 entries' and a 'Filter:' input field. A table is displayed with the following headers: 'IP Address' (with a checkbox), 'MAC Address', 'Interface', 'Type', and 'Age'. The table body is empty, and the text 'Table is Empty' is centered. Below the table, there are four buttons: 'First', 'Previous', 'Next', and 'Last'. At the bottom of the page, there are three buttons: 'Refresh' (green), 'Add' (green), and 'Remove' (green).

Table 73. ARP Table Summary Fields

Field	Description
IP Address	The IP address of a network host on a subnet attached to one of the device's routing interfaces. 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 device through this interface.
Type	The ARP entry type: <ul style="list-style-type: none">• Dynamic – An ARP entry that has been learned by the router• Gateway – A dynamic ARP entry that has the IP address of a routing interface• Local – An ARP entry associated with the MAC address of a routing interface on the device• Static – An ARP entry configured by the user
Age	The age of the entry since it was last learned or refreshed. This value is specified for Dynamic or Gateway entries only (it is left blank for all other entry types).

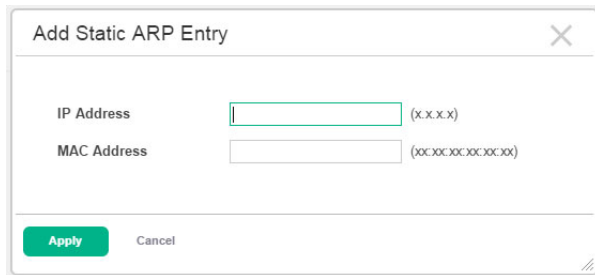
Adding a Static ARP Entry

To add a static ARP entry:

1. Click **Add**.

The Add Static ARP Entry dialog box opens.

Figure 101. Add Static ARP Entry Page

A screenshot of a dialog box titled "Add Static ARP Entry" with a close button (X) in the top right corner. The dialog contains two input fields: "IP Address" with a placeholder "(x.x.x.x)" and "MAC Address" with a placeholder "(xx:xx:xx:xx:xx:xx)". Below the fields are two buttons: "Apply" (highlighted in green) and "Cancel".

2. Specify the IP address and its associated MAC address.
3. 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.

ARP Table Configuration

Use this page to change the configuration parameters for the Address Resolution Protocol Table.

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

Figure 102. ARP Table Configuration Page

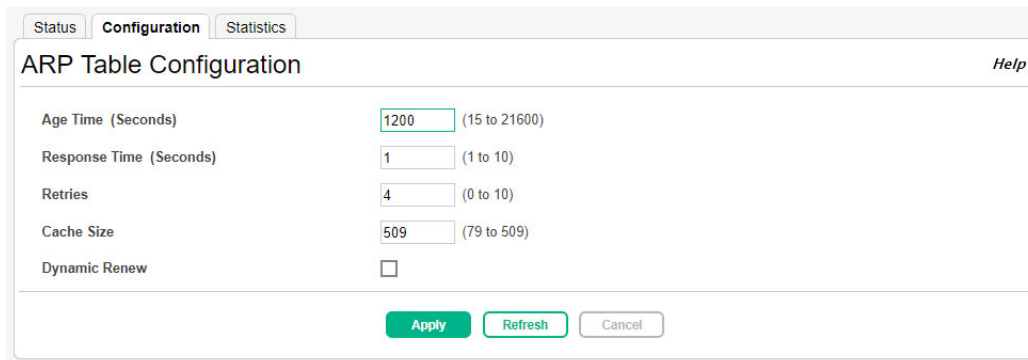


Table 74. ARP Table Configuration Fields

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

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 Statistics

Use this page to view information about the number and type of entries in the system ARP table. The ARP table contains entries that map IP addresses to MAC addresses.

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

Figure 103. ARP Table Statistics Page

Status

Configuration

Statistics

ARP Table Statistics

Help

Total Entry Count

0

Peak Total Entries

0

Active Static Entries

0

Configured Static Entries

0

Maximum Static Entries

32

Refresh

Table 75. ARP Table Statistics Fields

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

10 Quality of Service (QoS)

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

Configuring 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.

HPE OfficeConnect 1920S switches support IPv4 and MAC ACLs. The maximum number of ACLs (IPv4 and MAC) is 50. ACLs are applied per interface, and each interface supports a maximum of 10 rules.

To configure an ACL:

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

Access Control List Summary

Use the Access Control List Summary page to enable or disable ACL counters, to add or remove ACLs, and to view information about the MAC and IP ACLs configured on the switch.

To display the Access List Summary page, click **QoS > Access Control Lists** in the navigation pane, and ensure that the **Summary** tab is selected.

Figure 104. Access Control List Summary Page

Summary Configuration Interfaces VLANs Statistics					
Access Control List Summary Help					
Display All rows		Showing 1 to 2 of 2 entries		Filter: <input type="text"/>	
<input type="checkbox"/>	ACL Identifier	ACL Type	Rules Used	Direction	Interface
<input type="checkbox"/>	50	IPv4 Standard	1	Inbound	3
<input type="checkbox"/>	101	IPv4 Extended	1		
First Previous 1 Next Last					
Refresh Add Edit Remove					

Table 76. Access Control List Summary Fields

Field	Description
ACL Identifier	The name or number that identifies the ACL. The permitted identifier depends on the ACL type. Standard and Extended IPv4 ACLs use numbers within a set range, and Named IPv4 and MAC ACLs use alphanumeric characters.
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, IPv6 ACLs classify Layer 3 and Layer 4 IPv6 traffic, and MAC ACLs classify Layer 2 traffic. The ACL types are as follows: <ul style="list-style-type: none">• IPv4 Standard – Match criteria is based on the source address of IPv4 packets.• IPv4 Extended – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv4 packets.• IPv4 Named – Match criteria is the same as IPv4 Extended ACLs, but the ACL ID can be an alphanumeric name instead of a number.• Extended 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 Used	The number of rules currently configured for the 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).
Interface	The interface(s) to which the ACL has been applied.
VLAN	Each VLAN to which the ACL has been applied.

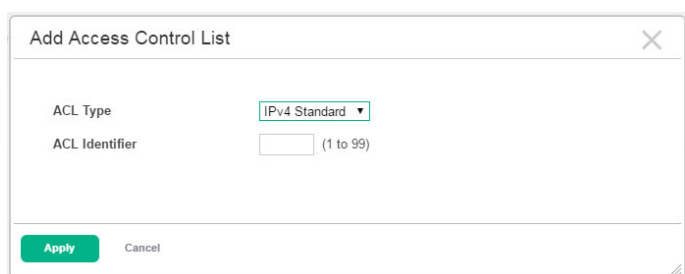
Click **Apply** to update the switch configuration. Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Adding an ACL

To add an ACL:

1. Click **Add**.

The Add Static ARP Entry dialog box opens.

Figure 105. Add Access Control List Page

2. Specify the type of ACL to add and the identifier.

The allowed identifier depends on the ACL type you select:

- IPv4 Standard: 1–99
- IPv4 Extended: 100–199
- IPv4 Named and Extended MAC: 1 to 31 alphanumeric characters

3. Click **Apply**.

Removing an ACL

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

Access Control List Configuration

Use this page to configure rules for the existing Access Control Lists (ACLs) on the system and to view summary information about the rules that have been added to an ACL. Each ACL rule is configured to match one or more aspects of traffic on the network. When a packet matches the conditions in a rule, it is handled according to the configured action (permit or deny) and attributes. Each ACL can have multiple rules, but the final rule for every ACL is an implicit deny all rule. For each rule, a packet must match all the specified criteria in order for the specified rule action (Permit/Deny) to take place.

To display the Access Control List Configuration page, click **QoS > Access Control Lists** in the navigation pane, and click the **Configuration** tab.

Figure 106. Access Control List Configuration Page

SummaryConfigurationInterfacesVLANsStatistics

Access Control List Configuration

Help

ACL Identifier

110

Display

All

 rows

Showing 1 to 1 of 1 entries

Filter:

<input type="checkbox"/>	Sequence Number	ACL Type	Status	Action	Match Conditions	Rule Attributes
<input type="checkbox"/>	10	IPv4 Extended	Active	Permit	Match All: False Protocol: 255 (IP) Source IP: 192.168.10.0 Source Mask: 0.255.255.255	

First

Previous

1

Next

Last

Refresh

Add Rule

Remove Rule

Resequence Rules

Table 77. Access Control List Configuration Fields

Field	Description
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. If the sequence number is not specified during rule creation, the rule is automatically assigned a sequence number after it is successfully added to 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.

Field	Description
ACL Type	<p>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. The ACL types are as follows:</p> <ul style="list-style-type: none"> • IPv4 Standard – Match criteria is based on the source address of IPv4 packets. • IPv4 Extended – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv4 packets. • IPv4 Named – Match criteria is the same as IPv4 Extended ACLs, but the ACL ID can be an alphanumeric name instead of a number. • Extended 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.
Status	<p>Indicates whether the ACL is active. If the ACL is a time-based ACL that includes a time range, the ACL is active only during the periods specified within the time range. If an ACL does not include a time range, the status is always active.</p>
Action	<p>The action to take when a packet or frame matches the criteria in the rule:</p> <ul style="list-style-type: none"> • Permit – The packet or frame is forwarded. • Deny – The packet or frame is dropped. <p>Note: When configuring ACL rules in the Add Access Control List Rule window, the selected action determines which fields can be configured. Not all fields are available for both Permit and Deny actions.</p>
Match Conditions	<p>The criteria used to determine whether a packet or frame matches the ACL rule.</p>
Rule Attributes	<p>Each action — beyond the basic Permit and Deny actions — to perform on the traffic that matches the rule.</p>

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

Adding a Rule to a Standard IPv4 ACL

To add a rule to a standard IPv4 ACL:

1. From the ACL identifier list, select the ID of the IPv4 standard ACL. The ID is a number from 1–99.
2. Click **Add Rule**.

The Add IPv4 ACL Rule page appears.

Figure 107. Add Standard IPv4 ACL Page

Add IPv4 ACL Rule

Sequence Number (1 to 2147483647)

Action ☐ Permit ☒ Deny

Match Criteria

Every ☐

Source IP Address / Wildcard Mask / (x.x.x.x)

Rule Attributes

Assign Queue (0 to 3)

Interface ☐ Redirect ☐ Mirror

Committed Rate / Burst Size (1 to 4294967295) (1 to 128)

Apply Cancel

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. Specify the match criteria and rule attributes shown in [Table 78](#).
6. Click **Apply**

Table 78. Standard IPv4 ACL Match Criteria

Field	Description
Match Criteria	
Every	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 Every is selected, no other match criteria can be configured. To configure specific match criteria, this option must be clear.
Source IP Address / Wildcard Mask	The source port 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 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 source IP address.
Rule Attributes	
Assign Queue	The number that identifies the hardware egress queue that will handle all packets matching this rule.
Interface	<p>The interface to use for the action:</p> <ul style="list-style-type: none"> • 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 device.
Committed Rate / Burst Size	The allowed transmission rate for frames on the interface (Committed Rate), and the number of bytes allowed in a temporary traffic burst (Burst Rate).

Adding a Rule to an Extended or Named IPv4 ACL

To add a rule to an Extended or Named IPv4 ACL:

1. From the ACL identifier list, select the ID of the IPv4 extended or named ACL. For an extended IPv4 ACL, the ID is a number from 100–199. For a named IPv4 ACL, the ID is up to 31 alphanumeric characters.
2. Click **Add Rule**.

The Add IPv4 ACL Rule page appears.

Figure 108. Add Extended or Named IPv4 ACL Page

Add IPv4 ACL Rule

Sequence Number: (1 to 2147483647)

Action: ☐ Permit ☒ Deny

Match Criteria

Every: ☐

Protocol: (0 to 255, or keyword) ?

Fragments: ☐

Source IP Address / Wildcard Mask: / (x.x.x.x)

Source L4 Port: ☒ Equal ☐ Not Equal ☐ Less Than ☐ Greater Than ☐ Range
 - (0 to 65535, or keyword) ?

Destination IP Address / Wildcard Mask: / (x.x.x.x)

Destination L4 Port: ☒ Equal ☐ Not Equal ☐ Less Than ☐ Greater Than ☐ Range
 - (0 to 65535, or keyword) ?

IGMP Type: (0 to 255)

ICMP Type: (0 to 255)

ICMP Code: (0 to 255)

ICMP Message:

TCP Flags: ☐
☐ +FIN ☐ -FIN ☐ +SYN ☐ -SYN ☐ +RST ☐ -RST ☐ +PSH ☐ -PSH

Service Type: ☐

IP DSCP: ☐ 0 - be/cso

IP Precedence: ☐ (0 to 7)

Apply Cancel

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. Specify the match criteria and rule attributes shown in [Table 79](#).
6. Click **Apply**

Table 79. Extended or Named IPv4 ACL Match Criteria

Field	Description
Match Criteria	
Every	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 Every is selected, no other match criteria can be configured. To configure specific match criteria, this option must be clear.
Protocol	The IANA-assigned protocol number to match within the IP packet. You can also specify one of the following keywords: EIGRP, GRE, ICMP, IGMP, IP, IPINIP, OSPF, PIM, TCP, or UDP.
Fragments	IP ACL rule to match on fragmented IP packets.
Source IP Address / Wildcard Mask	The source port 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 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 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. Equal to, Not Equal to, Greater than, and Less than options are available. For TCP protocol: BGP, Domain, Echo, FTP, FTP-Data, HTTP, SMTP, Telnet, WWW, 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. Equal to, Not Equal to, Greater than, and Less than options are available. For TCP protocol: BGP, Domain, Echo, FTP, FTP-Data, HTTP, SMTP, Telnet, WWW, 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.
ICMP Message	IP ACL rule to match on the ICMP message type and code. Specify one of the following supported ICMP messages: Echo, Echo-Reply, Host-Redirect, Mobile-Redirect, Net-Redirect, Net-Unreachable, Redirect, Packet-Too-Big, Port-Unreachable, Source-Quench, Router-Solicitation, Router-Advertisement, Time-Exceeded, TTL-Exceeded, and Unreachable. This option is available only if the protocol is ICMP.
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. When Established is specified, a match occurs if either RST or ACK bits are set in the TCP header. This option is available only if the protocol is TCP.

Field	Description
Service Type	<p>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:</p> <ul style="list-style-type: none"> • 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. • IP TOS Bits – Matches on the Type of Service (TOS) bits in the IP header. The IP TOS field in a packet is defined as all eight bits of the Service Type octet in the IP header. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a TOS Bits value of 0xA0 and a TOS Mask of 0xFF. <ul style="list-style-type: none"> ○ TOS Bits – Requires the bits in a packet's TOS field to match the two-digit hexadecimal number entered in this field. ○ TOS Mask – The bit positions that are used for comparison against the IP TOS field in a packet.
Rule Attributes	
Assign Queue	The number that identifies the hardware egress queue that will handle all packets matching this rule.
Interface	<p>The interface to use for the action:</p> <ul style="list-style-type: none"> • 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 device.
Committed Rate / Burst Size	The allowed transmission rate for frames on the interface (Committed Rate), and the number of bytes allowed in a temporary traffic burst (Burst Rate).

Adding a Rule to an Extended MAC ACL

To add a rule to an Extended MAC ACL:

1. From the ACL identifier list, select the ID of the extended MAC ACL. The ID is up to 31 alphanumeric characters.
2. Click **Add Rule**.

The Add MAC ACL Rule page appears.

Figure 109. Add MAC ACL Page

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. Specify the match criteria and rule attributes shown in [Table 80](#).
6. Click **Apply**

Table 80. Extended MAC ACL Match Criteria

Field	Description
Match Criteria	
Every	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 Every is selected, no other match criteria can be configured. To configure specific match criteria, this option must be clear.
CoS	The 802.1p user priority value to match within the Ethernet frame.
EtherType	The EtherType value to match in an Ethernet frame. Specify the number associated with the EtherType or specify one of the following keywords: AppleTalk, ARP, IBM SNA, IPv4, IPv6, IPX, MPLS, Unicast, NETBIOS, NOVELL, PPPoE, or RARP.

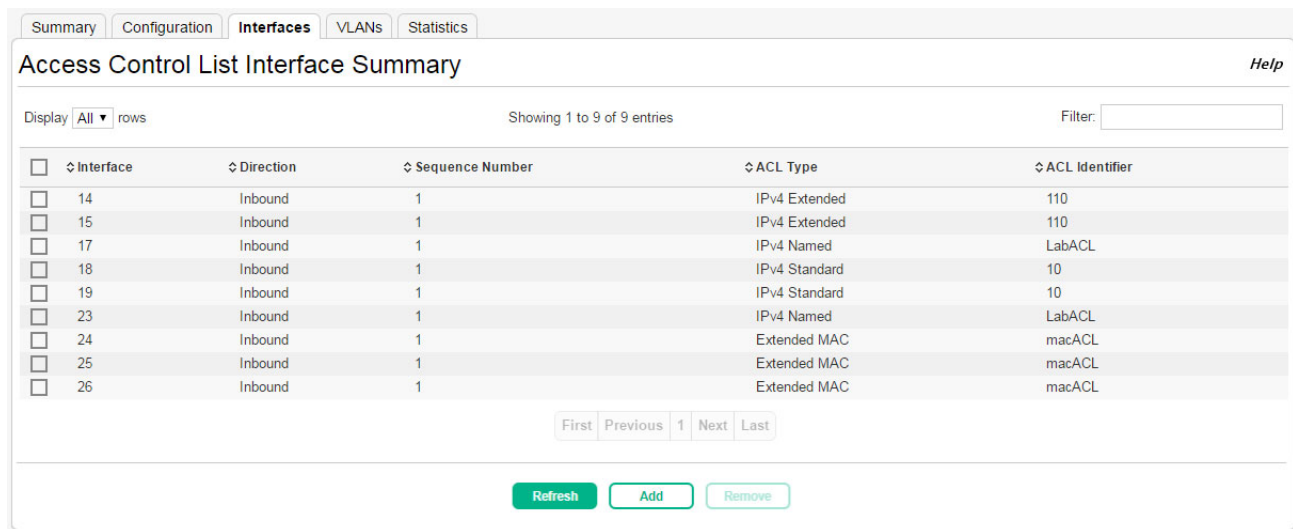
Field	Description
Source MAC Address / Mask	The MAC address to match to an Ethernet frame's source port MAC address. If desired, enter the MAC Mask associated with the source MAC to match. The MAC address mask specifies which bits in the source MAC to compare against an Ethernet frame. Use F's and zeros 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, 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.
Rule Attributes	
Assign Queue	The number that identifies the hardware egress queue that will handle all packets matching this rule.
Interface	<p>The interface to use for the action:</p> <ul style="list-style-type: none"> • 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 device.
Committed Rate / Burst Size	The allowed transmission rate for frames on the interface (Committed Rate), and the number of bytes allowed in a temporary traffic burst (Burst Rate).

Access Control List Interface Summary

Use this page to associate one or more ACLs with one or more interfaces on the device. When an ACL is associated with an interface, traffic on the port is checked against the rules defined within the ACL until a match is found. If the traffic does not match any rules within an ACL, it is dropped because of the implicit deny all rule at the end of each ACL.

To display the Access Control List Interface Summary page, click **QoS > Access Control Lists** in the navigation pane, and then click the **Interfaces** tab.

Figure 110. Access Control List Interface Summary Page



<input type="checkbox"/>	Interface	Direction	Sequence Number	ACL Type	ACL Identifier
<input type="checkbox"/>	14	Inbound	1	IPv4 Extended	110
<input type="checkbox"/>	15	Inbound	1	IPv4 Extended	110
<input type="checkbox"/>	17	Inbound	1	IPv4 Named	LabACL
<input type="checkbox"/>	18	Inbound	1	IPv4 Standard	10
<input type="checkbox"/>	19	Inbound	1	IPv4 Standard	10
<input type="checkbox"/>	23	Inbound	1	IPv4 Named	LabACL
<input type="checkbox"/>	24	Inbound	1	Extended MAC	macACL
<input type="checkbox"/>	25	Inbound	1	Extended MAC	macACL
<input type="checkbox"/>	26	Inbound	1	Extended MAC	macACL

Table 81. Access Control List Interface Summary 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).
Sequence Number	The order the ACL is applied to traffic on the interface relative to other ACLs associated with the interface in the same direction. When multiple ACLs are applied to the same interface in the same direction, the ACL with the lowest sequence number is applied first, and the other ACLs are applied in ascending numerical order.
ACL Type	The type of ACL, which is either IPv4, IPv6, or MAC.
ACL Identifier	The name or number that identifies the ACL. When applying an ACL to an interface, the ACL Identifier menu includes only the ACLs within the selected ACL Type.

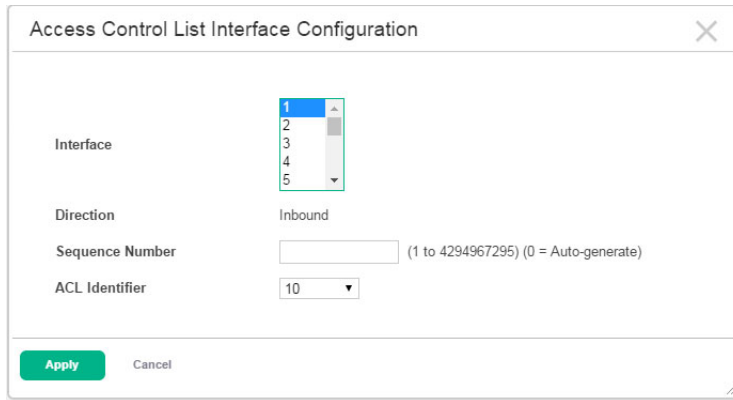
Associating an ACL with an Interface

To apply an ACL to an interface:

1. Click **Add**.

The Access Control List Interface Configuration page appears.

Figure 111. Access Control List Interface Configuration Page



The image shows a dialog box titled "Access Control List Interface Configuration" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Interface:** A list box showing a scrollable list of interface numbers: 1, 2, 3, 4, 5. Interface 1 is currently selected and highlighted in blue.
- Direction:** A text label followed by the value "Inbound".
- Sequence Number:** A text input field that is currently empty. To its right is a hint text: "(1 to 4294967295) (0 = Auto-generate)".
- ACL Identifier:** A dropdown menu showing the value "10".
- Buttons:** At the bottom left, there are two buttons: "Apply" (highlighted in green) and "Cancel".

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.
3. Specify a sequence number or leave the field blank to let the switch assign the sequence number.
4. Select the ID of the ACL to associate with the interface or interfaces.
5. Click **Apply**.

Removing an Association Between an ACL and an Interface

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

Access Control List VLAN Summary

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

To display the Access Control List VLAN Summary page, click **QoS > Access Control Lists > VLANs** in the navigation menu.

To display the Access Control List VLAN Summary page, click **QoS > Access Control Lists** in the navigation pane, and then click the **VLANs** tab.

Figure 112. Access Control List VLAN Summary Page

	↕ VLAN ID	↕ Direction	↕ Sequence Number	↕ ACL Type	↕ ACL Identifier
<input type="checkbox"/>	10	Inbound	1	IPv4 Extended	110
<input type="checkbox"/>	11	Inbound	1	IPv4 Extended	110
<input type="checkbox"/>	12	Inbound	1	IPv4 Extended	110

Table 82. Access Control List VLAN Summary Fields

Field	Description
VLAN ID	The ID of the VLAN associated with the rest of the data in the row. When associating a VLAN with an ACL, use this field to select the desired VLAN.
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).
Sequence Number	The order the ACL is applied to traffic on the VLAN relative to other ACLs associated with the VLAN in the same direction. When multiple ACLs are applied to the same VLAN in the same direction, the ACL with the lowest sequence number is applied first, and the other ACLs are applied in ascending numerical order.
ACL Type	The type of ACL, which is either IPv4, IPv6, or MAC.
ACL Identifier	The name or number that identifies the ACL. The permitted identifier depends on the ACL type. Standard and Extended IPv4 ACLs use numbers within a set range, and Named IPv4, IPV6, and MAC ACLs use alphanumeric characters.

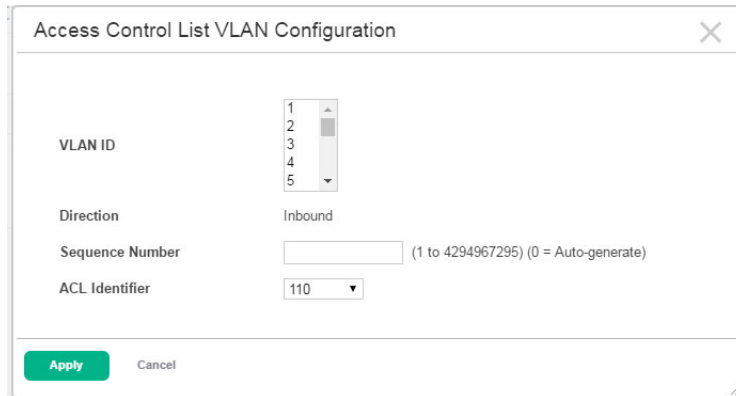
Associating an ACL with a VLAN

To apply an ACL to an interface:

1. Click **Add**.

The Access Control List VLAN Configuration page appears.

Figure 113. Access Control List VLAN Configuration Page



The image shows a dialog box titled "Access Control List VLAN Configuration" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- VLAN ID:** A list box showing a scrollable list of VLAN IDs: 1, 2, 3, 4, and 5. A vertical scrollbar is visible on the right side of the list.
- Direction:** A text field containing the word "Inbound".
- Sequence Number:** A text input field. To its right, there is a note: "(1 to 4294967295) (0 = Auto-generate)".
- ACL Identifier:** A dropdown menu currently showing the value "110".
- Buttons:** At the bottom left, there are two buttons: a green "Apply" button and a "Cancel" button.

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. Specify a sequence number or leave the field blank to let the switch assign the sequence number.
4. Select the ID of the ACL to associate with the VLAN or VLANs.
5. Click **Apply**.

Removing an Association Between an ACL and a VLAN

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

Access Control List Statistics

Use this page to display the statistical information about the packets forwarded or discarded by the port that matches the configured rules within an Access Control List (ACL). Each ACL rule is configured to match one or more aspects of traffic on the network. When a packet matches the conditions in a rule, the counter associated with the rule gets incremented, until it reaches the rollover value of the counter.

To display the Access Control List Statistics page, click **QoS > Access Control Lists** in the navigation pane, and then click the **Statistics** tab.

Figure 114. Access Control List Statistics Page

Access Control List Statistics Help

ACL Type: IPv4 Standard
ACL Identifier: 2

Display: All rows Showing 1 to 2 of 2 entries Filter:

<input type="checkbox"/>	Sequence Number	Action	Match Conditions	Rule Attributes	Hit Count
<input type="checkbox"/>	10	Deny	Match All: False Source IP: 192.168.1.2 Source Mask: 0.0.0.0		0
<input type="checkbox"/>	20	Permit	Match All: False Source IP: 10.130.65.96 Source Mask: 0.0.0.255		202189

[First](#) [Previous](#) [1](#) [Next](#) [Last](#)

[Refresh](#) [Clear Rule Hit Counter](#) [Clear ACL Counters](#)

Table 83. Access Control List Statistics Fields

Field	Description
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, IPv6 ACLs classify Layer 3 and Layer 4 IPv6 traffic, and MAC ACLs classify Layer 2 traffic. The ACL types are as follows: <ul style="list-style-type: none">• IPv4 Standard – Match criteria is based on the source address of the IPv4 packets.• IPv4 Extended – Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of the IPv4 packets.• IPv4 Named – Match criteria is the same as IPv4 Extended ACLs, but the ACL ID can be an alphanumeric name instead of a number.• Extended MAC – Match criteria can be based on the source and destination MAC addresses, 802.1p user priority, VLAN ID, and EtherType value within the Ethernet frames.
ACL Identifier	A list of ACL IDs that exist on the system for a given ACL type. To view the rule(s) within an ACL, you must select the ID of the ACL from the list. The ACL rules are not displayed when option All is selected. Option All lets you clear the hit count for an ACL type.
Sequence Number	The number that indicates the position of a rule within the ACL.
Action	The action to take when a packet or frame matches the criteria in the rule: <ul style="list-style-type: none">• Permit – The packet or frame is forwarded.• Deny – The packet or frame is dropped.
Match Conditions	The criteria used to determine whether a packet or frame matches the ACL rule.

Field	Description
Rule Attributes	Each action — beyond the basic Permit and Deny actions — to perform on the traffic that matches the rule.
Hit Count	Indicates the number of packets that match the configured rule in an ACL. If a rule is configured without rate limit, then the hit count is the number of matched packets forwarded or discarded by the port. If a rule is configured with rate limit, then if the sent traffic rate exceeds the configured rate, the hit count displays the matched packet count equal to the sent rate, despite packets getting dropped beyond the configured limit. If the sent traffic rate is less than the configured rate, the hit count displays only the matched packet count.

Use the buttons to perform the following tasks:

- To clear the hit count for one or more configured rules within an ACL, select the rule entry and click **Clear Rule Hit Counter**. You must confirm the action before the hit count is cleared for the selected rule(s).
- To clear the hit count for an ACL, select the ACL type from the ACL Type menu, select the ACL ID from the ACL Identifier menu, and then click **Clear ACL Counters**. You must confirm the action before the hit count is cleared for the selected ACL.

Configuring 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.

802.1p CoS Mapping Configuration

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 CoS Mapping Configuration page to assign 802.1p priority values to various traffic classes on one or more interfaces.

To display the page, click **QoS > Class of Service** in the navigation pane, and ensure that the **802.1p** tab is selected.

Figure 115. 802.1p CoS Mapping Configuration Page

802.1p CoS Mapping Configuration

Display 10 rows Showing 1 to 10 of 34 entries Filter:

<input type="checkbox"/>	Interface	Pri 0	Pri 1	Pri 2	Pri 3	Pri 4	Pri 5	Pri 6	Pri 7
<input type="checkbox"/>	1	1	0	0	1	2	2	3	3
<input type="checkbox"/>	2	1	0	0	1	2	2	3	3
<input type="checkbox"/>	3	1	0	0	1	2	2	3	3
<input type="checkbox"/>	4	1	0	0	1	2	2	3	3
<input type="checkbox"/>	5	1	0	0	1	2	2	3	3
<input type="checkbox"/>	6	1	0	0	1	2	2	3	3
<input type="checkbox"/>	7	1	0	0	1	2	2	3	3
<input type="checkbox"/>	8	1	0	0	1	2	2	3	3
<input type="checkbox"/>	9	1	0	0	1	2	2	3	3
<input type="checkbox"/>	10	1	0	0	1	2	2	3	3

First Previous 1 2 3 4 Next Last

Refresh Edit

Table 84. 802.1p CoS Mapping Configuration Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. The Global entry represents the common settings for all interfaces, unless specifically overridden individually.
Priority	The heading row lists each 802.1p priority value (0–7), and the data in the table shows which traffic class is mapped to the priority value. Incoming frames containing the designated 802.1p priority value are mapped to the corresponding traffic class in the device.
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 on an Interface

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

1. Select each interface to configure and click **Edit**. If you select multiple interfaces, the same settings are applied to all selected interfaces.

The Edit 802.1p Priority Mapping page appears.

Figure 116. Edit 802.1p Priority Mapping Page

Interface	5, 6
802.1p Priority	Traffic Class
0	1 (0 to 3, 1 = Default)
1	0 (0 to 3, 0 = Default)
2	0 (0 to 3, 0 = Default)
3	1 (0 to 3, 1 = Default)
4	2 (0 to 3, 2 = Default)
5	2 (0 to 3, 2 = Default)
6	3 (0 to 3, 3 = Default)
7	3 (0 to 3, 3 = Default)

Apply Cancel

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

DSCP CoS Global Mapping Configuration

Use the DSCP CoS Global Mapping Configuration page to map an IP DSCP value to an internal traffic class.

To display the DSCP CoS Global Mapping Configuration page, click **QoS > Class of Service** in the navigation pane, and then click the **DSCP** tab.

NOTE:
[Figure 117](#) does not show all of the fields on the page.

Figure 117. DSCP CoS Global Mapping Configuration Page

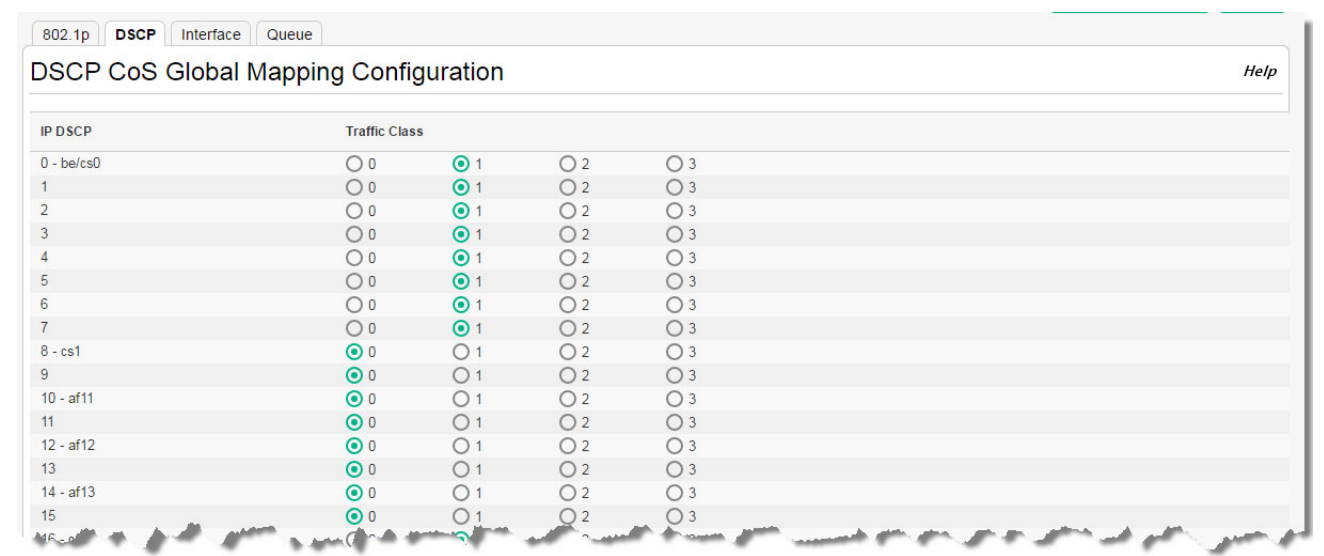


Table 85. DSCP CoS Global Mapping Configuration Fields

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

CoS Trust Configuration

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

To display the CoS Trust Configuration page, click **QoS > Class of Service** in the navigation pane, and then click the **Interfaces** tab.

Figure 118. CoS Trust Configuration Page

<input type="checkbox"/> ↕ Interface	↕ Trust Mode	↕ Shaping Rate
<input type="checkbox"/> 1	802.1p	0
<input type="checkbox"/> 2	802.1p	0
<input type="checkbox"/> 3	802.1p	0
<input type="checkbox"/> 4	802.1p	0
<input type="checkbox"/> 5	802.1p	0
<input type="checkbox"/> 6	802.1p	0
<input type="checkbox"/> 7	802.1p	0
<input type="checkbox"/> 8	802.1p	0
<input type="checkbox"/> 9	802.1p	0
<input type="checkbox"/> 10	802.1p	0

Table 86. CoS Trust Configuration Fields

Field	Description
Interface	Selects the CoS configurable interface to be affected by the Interface Shaping Rate. Select Global to apply a rate to all interfaces. Select an individual port to override the global setting.
Trust Mode	The trust mode for ingress traffic on the interface, which is one of the following: <ul style="list-style-type: none">• untrusted – The interface ignores any priority designations encoded in incoming packets, and instead sends the packets to a traffic queue based on the ingress port's default priority.• 802.1p – The port accepts at face value the 802.1p priority designation encoded within packets arriving on the port.• IP DSCP – The port accepts at face value the IP DSCP priority designation encoded within packets arriving on the port.
Shaping Rate	Sets the limit on how much traffic can leave a port. The limit on maximum transmission bandwidth has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. The specified value represents a percentage of the maximum negotiated bandwidth.

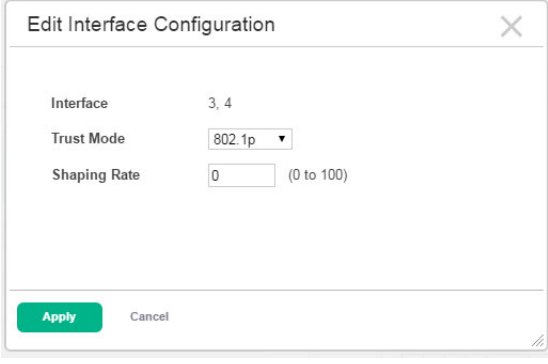
Configuring the Trust Mode and Shaping Rate on an Interface

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

1. Select each interface to configure and click **Edit**. If you select multiple interfaces, the same settings are applied to all selected interfaces.

The Edit Interface Configuration page appears.

Figure 119. Edit Interface Configuration Page



The dialog box titled "Edit Interface Configuration" contains the following fields:

- Interface: 3, 4
- Trust Mode: 802.1p (dropdown menu)
- Shaping Rate: 0 (input field) (0 to 100)

At the bottom, there are two buttons: "Apply" (green) and "Cancel".

2. Specify the trust mode and shaping rate for all interfaces identified in the Interface field.
3. Click **Apply** to update the switch configuration.

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

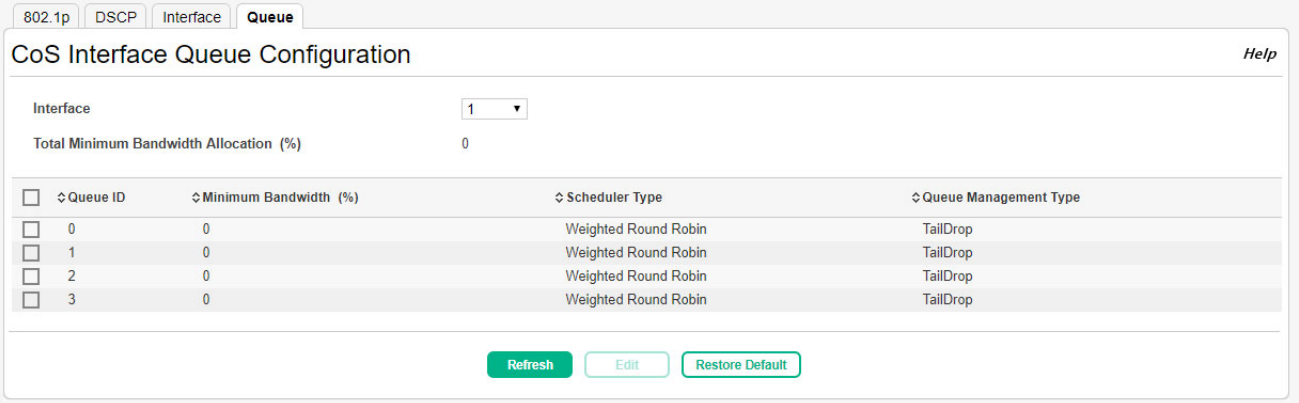
CoS Interface Queue Configuration

Use the CoS Interface 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. Each port has its own CoS queue-related configuration.

The configuration process is simplified by allowing each CoS queue parameter to be configured globally or per-port. A global configuration change is automatically applied to all ports in the system.

To display the CoS Interface Queue Configuration page, click **QoS > Class of Service** in the navigation pane, and then click the **Queue** tab.

Figure 120. CoS Interface Queue Configuration Page



The page shows the "CoS Interface Queue Configuration" with tabs for "802.1p", "DSCP", "Interface", and "Queue". The "Queue" tab is active. Below the tabs, there is a "Help" link.

Interface: 1 (dropdown menu)

Total Minimum Bandwidth Allocation (%): 0

<input type="checkbox"/>	Queue ID	Minimum Bandwidth (%)	Scheduler Type	Queue Management Type
<input type="checkbox"/>	0	0	Weighted Round Robin	TailDrop
<input type="checkbox"/>	1	0	Weighted Round Robin	TailDrop
<input type="checkbox"/>	2	0	Weighted Round Robin	TailDrop
<input type="checkbox"/>	3	0	Weighted Round Robin	TailDrop

At the bottom, there are three buttons: "Refresh" (green), "Edit" (light blue), and "Restore Default" (light blue).

Table 87. CoS Interface Queue Configuration Fields

Field	Description
Interface	Specifies the interface (physical, LAG, or Global) to configure.
Total Minimum Bandwidth Allocation	Shows the sum of individual Minimum Bandwidth values for all queues in the interface. The sum cannot exceed the defined maximum of 100. This value is considered while configuring the Minimum Bandwidth for a queue in the selected interface.
Queue ID	The queue to be configured on the interface selected from the Interface menu.
Minimum Bandwidth	Specify the minimum guaranteed bandwidth allocated to the selected queue on the interface. Setting this value higher than its corresponding Maximum Bandwidth automatically increases the maximum to the same value. The default value is 0. The valid range is 0 to 100, in increments of 1. The value zero (0) means no guaranteed minimum. The sum of individual Minimum Bandwidth values for all queues in the selected interface cannot exceed defined maximum 100.
Scheduler Type	Selects the type of queue processing from the drop-down menu. Defining on a per-queue basis allows the user to create the desired service characteristics for different types of traffic. <ul style="list-style-type: none"> Weighted Round Robin: Weighted round robin associates a weight to each queue. This is the default. Strict Priority: Strict priority services traffic with the highest priority on a queue first
Queue Management Type	Displays the type of queue depth management techniques used for all queues on this interface. Queue Management Type can only be Taildrop. The default value is Taildrop. All packets on a queue are safe until congestion occurs. At this point, any additional packets queued are dropped.

Configuring CoS Queue Settings

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

1. Select the interface to configure from the Interface menu on the CoS Interface Queue Configuration page.
2. Select each queue to configure for the selected interface and click **Edit**. If you select multiple queues, the same settings are applied to all selected queues.

The Edit CoS Interface Queue Configuration page appears.

Figure 121. Edit CoS Interface Queue Configuration Page

The screenshot shows a dialog box titled "Edit CoS Interface Queue Configuration". It contains the following fields and values:

- Interface: 1
- Queue ID: 1
- Minimum Bandwidth (%): 0 (with a range of 0 to 100)
- Scheduler Type: Weighted Round Robin (dropdown menu)
- Queue Management Type: TailDrop

At the bottom of the dialog, there are two buttons: "Apply" (highlighted in green) and "Cancel".

3. Specify the trust mode and shaping rate for all interfaces identified in the Interface field.
4. Click **Apply** to update the switch configuration.

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

11 Security

The HPE OfficeConnect 1920S 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.

Advanced Security Configuration

The HPE OfficeConnect 1920S switches include Denial-of-Service (DoS) and ICMP (ping) protection features on the Advanced Security page to help protect against various high-volume traffic scenarios or malicious attacks.

A DoS attack is an attempt to saturate the switch with external communication requests to prevent the switch from performing efficiently, or at all. You can enable Auto DoS protection that prevents common types of DoS attacks.



CAUTION:

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 device and the network from attacks that involve issues with the ICMP echo request packets (pings) that the device receives.

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

Figure 122. Advanced Security Configuration Page

Table 88. Advanced Security Configuration Fields

Field	Description
Auto DoS Features	
Auto DoS	Enable this option to enable all the DoS prevention mechanisms with default values. Enabling this feature makes all the fields in the remainder of the table inaccessible (grayed-out). When disabled, you can individually turn on and off the DoS features and change their default values. This feature and all the individual DoS protections are disabled by default.
Prevent Land Attack	Enable this option to drop packets for which the source IP address equals the destination IP address.
Prevent TCP Blat Attack	Enable this option to drop packets for which the TCP source port equals the TCP destination port.
Prevent UDP Blat Attack	Enable this option to drop packets that have a UDP source port equal to the UDP destination port.
Prevent Invalid TCP Flags Attack	Enable this option to drop packets that have TCP Flags SYN and FIN set.
Prevent TCP Fragment Attack	Enable this option to drop IP packets that have an IP fragment offset equal to 1.
Check First Fragment Only	Enable this option to drop packets that have a TCP header smaller than the minimum TCP header size, which is hard-coded to 20 bytes.
Prevent Smurf Attack	Enable this option to drop ICMP Echo packets (ping) that are sent to a broadcast IP address.
Prevent Ping Flood Attack	Enable this option to prevent ping flooding by limiting the number of ICMP ping packets.
Prevent SYN Flood Attack	Enable this option to limit the rate of TCP connection requests so that they are not received faster than they can be processed.
ICMP Settings	
ICMP	Enable this option to allow the device to drop ICMP packets that have a type set to ECHO_REQ (ping) and a payload size greater than the ICMP payload size configured in the Max ICMPv4 Size or Max ICMPv6 Size fields.
Max ICMPv4 Size	The maximum allowed ICMPv4 packet size. If ICMP DoS prevention is enabled, the device will drop ICMPv4 ping packets that have a size greater than this configured maximum ICMPv4 packet size.
ICMPv6	Enable this option to allow the device to drop ICMP packets that have a type set to ECHO_REQ (ping) and a payload size greater than the ICMP payload size configured in the Max ICMPv6 Size field
Max ICMPv6 Size	The maximum allowed IPv6 ICMP packet size. If ICMP DoS prevention is enabled, the switch will drop IPv6 ICMP ping packets that have a size greater than this configured maximum ICMPv6 packet size.
ICMP Fragment	Enable this option to allow the device to drop fragmented ICMP packets.

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**.

RADIUS Settings

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. The HPE OfficeConnect 1920S 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.

RADIUS Configuration

Use the RADIUS 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 RADIUS Configuration page, click **Security > RADIUS** in the navigation pane, and ensure that the **Configuration** tab is selected.

Figure 123. RADIUS Configuration Page

Table 89. RADIUS Configuration Fields

Field	Description
Global RADIUS Settings	
802.1X Authentication Mode	Specifies whether the IEEE 802.1X authentication mode on the switch is enabled or disabled. When this setting is selected, and port-based authentication is enabled for the device, 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.

Field	Description
Max Number of Retransmits	The maximum number of times the RADIUS client on the device 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 will be 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.
NAS-IP Address	The network access server (NAS) IP address for the RADIUS server. To specify an address, click the Edit icon and enter the IP address of the NAS in the available field. The address should be unique to the NAS within the scope of the RADIUS server. The NAS IP address is used only in Access-Request packets. To reset the NAS IP address to the default value, click the Reset icon and confirm the action.

RADIUS Server Information

Current	<p>Identifies whether the configured RADIUS server is the current server for the authentication server group.</p> <ul style="list-style-type: none"> • True—The server is the current server for the authentication server group. • False—The server is a secondary server. <p>When the switch sends a RADIUS request to the named server, the request is directed to the server selected as the current server. Initially the primary server is selected as the current server. If the primary server fails, one of the other servers becomes the current server. If more than one RADIUS server is configured with the same name, the switch selects one of the servers to be the current server from the group of servers with the same name.</p>
RADIUS Server Name	Shows the RADIUS server name. Multiple RADIUS servers can have the same name. In this case, RADIUS clients can use RADIUS servers with the same name as backups for each other.
IP Address/Host Name	The IP address or DNS name of the RADIUS server.
Port Number	Identifies the authentication port the server uses to verify the RADIUS server authentication. The port is a UDP port.
Server Type	Shows whether the server is a Primary or Secondary server.
Secret Configured	Indicates whether the shared secret for this server has been configured. To reset the shared secret to an unconfigured state, click the reset icon. To set a new password for the RADIUS server, select the checkbox associated with the server and click Edit. Then, specify a shared secret in the Secret field.
Message Authenticator	Shows whether the message authenticator attribute for the selected server is enabled or disabled.
Secret	This field is available when you add or edit a RADIUS server. This is the shared secret text string used for authenticating and encrypting all RADIUS communications between the RADIUS client on the device and the RADIUS accounting server. The secret specified in this field must match the shared secret configured on the RADIUS accounting server.

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

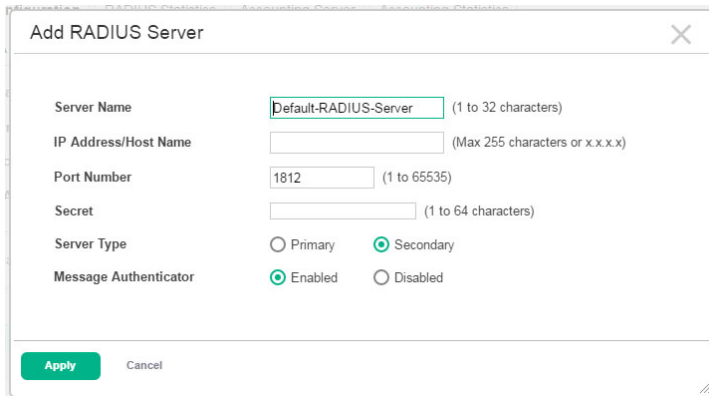
Adding a RADIUS Server

To add a RADIUS server to the switch configuration:

1. Click **Add**.

The Add RADIUS Server page appears.

Figure 124. Add RADIUS Server Page



The 'Add RADIUS Server' dialog box contains the following fields and options:

- Server Name:** Text field with 'Default-RADIUS-Server' and a note '(1 to 32 characters)'.
- IP Address/Host Name:** Text field with a note '(Max 255 characters or x.x.x.x)'.
- Port Number:** Text field with '1812' and a note '(1 to 65535)'.
- Secret:** Text field with a note '(1 to 64 characters)'.
- Server Type:** Radio buttons for 'Primary' and 'Secondary' (selected).
- Message Authenticator:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Buttons:** 'Apply' (green) and 'Cancel'.

2. Specify the required information about the RADIUS server.

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**.

Changing RADIUS Server Settings

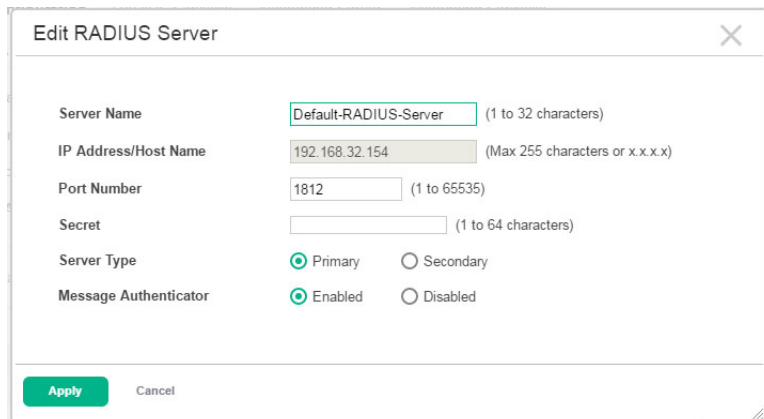
To change settings for an existing RADIUS server:

1. Select the RADIUS server to configure.

2. Click **Edit**.

The Edit RADIUS Server page appears.

Figure 125. Edit RADIUS Server Page



The 'Edit RADIUS Server' dialog box contains the following fields and options:

- Server Name:** Text field with 'Default-RADIUS-Server' and a note '(1 to 32 characters)'.
- IP Address/Host Name:** Text field with '192.168.32.154' and a note '(Max 255 characters or x.x.x.x)'.
- Port Number:** Text field with '1812' and a note '(1 to 65535)'.
- Secret:** Text field with a note '(1 to 64 characters)'.
- Server Type:** Radio buttons for 'Primary' (selected) and 'Secondary'.
- Message Authenticator:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Buttons:** 'Apply' (green) and 'Cancel'.

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**.

Removing a RADIUS Server

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

RADIUS Server Statistics

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

To access the RADIUS Server Statistics page, click **Security > RADIUS** in the navigation pane, and then click the **Statistics** tab.

Figure 126. RADIUS Server Statistics Page

IP Address/Host Name	Round Trip Time	Access Requests	Access Rejects	Pending Requests	Timeouts	Packets Dropped
192.168.32.154	0	0	0	0	0	0
192.168.55.173	0	0	0	0	0	0
192.168.20.124	0	0	0	0	0	0

Table 90. RADIUS Server Statistics Fields

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

To view additional information about a RADIUS server, select the server with the information to view and click **Details**. The following table describes the additional RADIUS server information that the RADIUS Server Detailed Statistics page shows.

Table 91. Detailed RADIUS Server Statistics Fields

Field	Description
Access Retransmissions	The number of RADIUS Access-Request packets that had to be retransmitted to the server because the initial Access-Request packet failed to be successfully delivered.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from the server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from the server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators, signature attributes, and unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from the server.
Unknown Types	The number of RADIUS packets of unknown type which were received from the server on the authentication port.

Click **Clear** to clear all RADIUS authentication and accounting server statistics. After you confirm the action, the statistics page will get reset. Click **Refresh** to update the page with the most current information.

RADIUS Accounting Server Status

The RADIUS Accounting Server Status page shows summary information about the accounting servers configured on the system.

To access the RADIUS Accounting Server Status page, click **Security > RADIUS** in the navigation pane, and then click the **Accounting Server** tab.

Figure 127. RADIUS Accounting Server Status Page

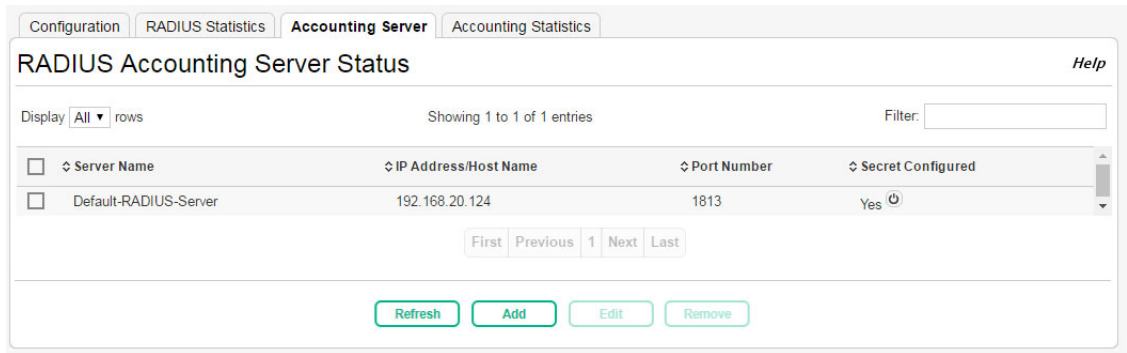


Table 92. RADIUS Accounting Server Status Fields

Field	Description
Server Name	The name of the RADIUS accounting server. RADIUS servers that are configured with the same name are members of the same named RADIUS server group. RADIUS accounting servers in the same group serve as backups for each other.
IP Address/Host Name	The IP address or host name of the RADIUS accounting server. Host names must be resolvable by DNS and are composed of a series of labels separated by dots.
Port Number	The UDP port on the RAIDUS accounting server to which the local RADIUS client sends request packets.
Secret Configured	Indicates whether the shared secret for this server has been configured. To reset the shared secret to an unconfigured state, click the reset icon. To set a new password for the RADIUS server, select the checkbox associated with the server and click Edit. Then, specify a shared secret in the Secret field.
Secret	This field is available when you add or edit a RADIUS accounting server. The shared secret text string used for authenticating and encrypting all RADIUS communications between the RADIUS client on the device and the RADIUS accounting server. The secret specified in this field must match the shared secret configured on the RADIUS accounting server.

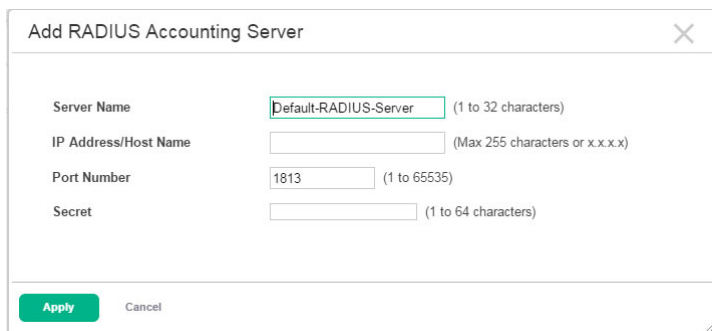
Adding a RADIUS Accounting Server

To add a RADIUS accounting server to the switch configuration:

1. Click **Add**.

The Add RADIUS Accounting Server page appears.

Figure 128. Add RADIUS Accounting Server Page



The dialog box titled "Add RADIUS Accounting Server" contains four input fields: "Server Name" with the value "Default-RADIUS-Server" and a character limit of "(1 to 32 characters)"; "IP Address/Host Name" with a character limit of "(Max 255 characters or x.x.x.x)"; "Port Number" with the value "1813" and a character limit of "(1 to 65535)"; and "Secret" with a character limit of "(1 to 64 characters)". At the bottom, there are "Apply" and "Cancel" buttons.

2. Specify the required information about the RADIUS accounting server.
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**.

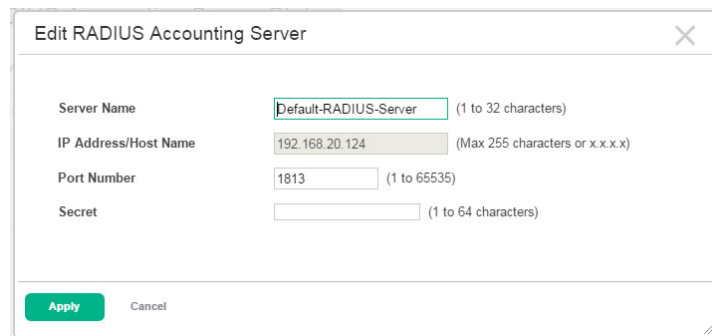
Changing RADIUS Accounting Server Settings

To change settings for an existing RADIUS accounting server:

1. Select the RADIUS accounting server to configure.
2. Click **Edit**.

The Edit RADIUS Accounting Server page appears.

Figure 129. Edit RADIUS Accounting Server Page



The dialog box titled "Edit RADIUS Accounting Server" contains four input fields: "Server Name" with the value "Default-RADIUS-Server" and a character limit of "(1 to 32 characters)"; "IP Address/Host Name" with the value "192.168.20.124" and a character limit of "(Max 255 characters or x.x.x.x)"; "Port Number" with the value "1813" and a character limit of "(1 to 65535)"; and "Secret" with a character limit of "(1 to 64 characters)". At the bottom, there are "Apply" and "Cancel" buttons.

3. Update the RADIUS accounting server information as needed. The IP address of an existing RADIUS accounting 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**.

Removing a RADIUS Accounting Server

To delete one or more RADIUS accounting servers, select each entry to delete and click **Remove**.

RADIUS Accounting Server Statistics

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

To access the RADIUS Accounting Server Statistics page, click **Security > RADIUS** in the navigation pane, and then click the **Accounting Statistics** tab.

Figure 130. RADIUS Accounting Server Statistics Page

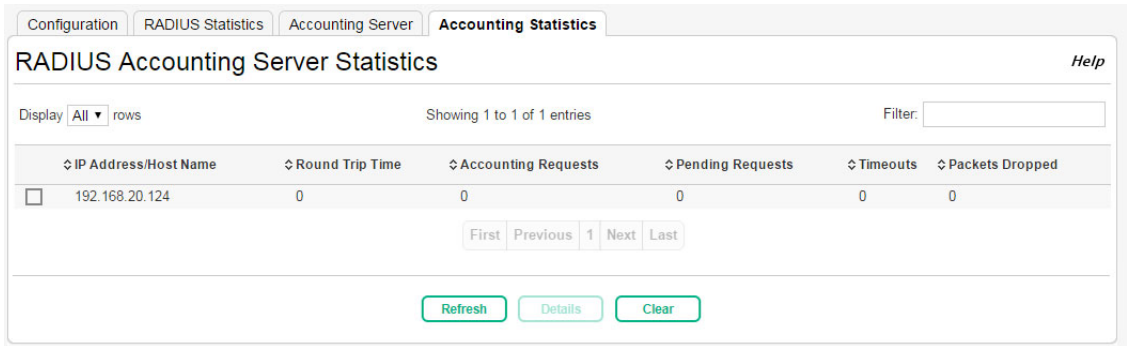


Table 93. RADIUS Accounting Server Statistics Fields

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

To view additional information about a RADIUS accounting server, select the server with the information to view and click **Details**. The following table describes the additional RADIUS accounting server information that the RADIUS Accounting Server Detailed Statistics page shows.

Table 94. Detailed RADIUS Accounting Server Statistics Fields

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

Click **Clear** to clear all RADIUS authentication and accounting server statistics. After you confirm the action, the statistics page will get reset. Click **Refresh** to update the page with the most current information.

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 system access.
- **Supplicants:** Specifies host connected to the authenticated port requesting access to the system 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 system services.

Port Access Control Configuration

Use this page to configure the global Port Access Control settings on the device. The port-based access control feature uses IEEE 802.1X to enable the authentication of system users through a local internal server or an external server. Only authenticated and approved system 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-TTL, EAP-TTLS, and EAP-TLS.

To display the Port Access Control Configuration page, click **Security > Port Access Control** in the navigation pane, and ensure that the **Configuration** tab is selected.

Figure 131. Port Access Control Configuration Page

Port Access Control Configuration Help

Admin Mode ☐ Enable ☒ Disable

VLAN Assignment Mode ☐ Enable ☒ Disable

Dynamic VLAN Creation Mode ☐ Enable ☒ Disable

Monitor Mode ☐ Enable ☒ Disable

EAPOL Flood Mode ☐ Enable ☒ Disable

Display **10** rows Showing 1 to 10 of 26 entries Filter:

	Interface	PAE Capabilities	Control Mode	Operating Control Mode	PAE State	Backend State	
<input type="checkbox"/>	1	Authenticator	Auto	N/A	Initialize	Initialize	<input type="button" value="⏻"/> <input type="button" value="⚙"/>
<input type="checkbox"/>	2	Authenticator	Auto	N/A	Initialize	Initialize	<input type="button" value="⏻"/> <input type="button" value="⚙"/>
<input type="checkbox"/>	3	Authenticator	Auto	N/A	Initialize	Initialize	<input type="button" value="⏻"/> <input type="button" value="⚙"/>
<input type="checkbox"/>	4	Authenticator	Auto	N/A	Initialize	Initialize	<input type="button" value="⏻"/> <input type="button" value="⚙"/>
<input type="checkbox"/>	5	Authenticator	Auto	N/A	Initialize	Initialize	<input type="button" value="⏻"/> <input type="button" value="⚙"/>
<input type="checkbox"/>	6	Authenticator	Auto	N/A	Initialize	Initialize	<input type="button" value="⏻"/> <input type="button" value="⚙"/>
<input type="checkbox"/>	7	Authenticator	Auto	N/A	Initialize	Initialize	<input type="button" value="⏻"/> <input type="button" value="⚙"/>
<input type="checkbox"/>	8	Authenticator	Auto	N/A	Initialize	Initialize	<input type="button" value="⏻"/> <input type="button" value="⚙"/>
<input type="checkbox"/>	9	Authenticator	Auto	N/A	Initialize	Initialize	<input type="button" value="⏻"/> <input type="button" value="⚙"/>
<input type="checkbox"/>	10	Authenticator	Auto	N/A	Initialize	Initialize	<input type="button" value="⏻"/> <input type="button" value="⚙"/>

First Previous 1 2 3 Next Last

Table 95. Port Access Control Configuration Fields

Field	Description
Global Port Access Control Fields	
Administrative Mode	Select Enable or Disable 802.1x mode on the switch. The default is Disable. This feature permits port-based authentication on the switch.
VLAN Assignment Mode	If enabled, when a supplicant is authenticated by an authentication server, the port that the supplicant is connected to is placed in a particular VLAN specified by the RADIUS server. VLAN Assignment mode controls if the switch is allowed to place a port in a RADIUS-assigned VLAN. A port's VLAN assignment is determined by the first supplicant that is authenticated on the port.
Dynamic VLAN Creation Mode	The administrative mode of dynamic VLAN creation on the device. If RADIUS-assigned VLANs are enabled, the RADIUS server is expected to include the VLAN ID in the 802.1X tunnel attributes of its response message to the device. If dynamic VLAN creation is enabled on the device and the RADIUS-assigned VLAN does not exist, then the assigned VLAN is dynamically created. This implies that the client can connect from any port and can get assigned to the appropriate VLAN. This feature gives flexibility for clients to move around the network without much additional configuration required.

Field	Description
Monitor Mode	The administrative mode of the Monitor Mode feature on the device. Monitor mode is a special mode that can be enabled in conjunction with port-based access control. Monitor mode provides a way for network administrators to identify possible issues with the port-based access control configuration on the device without affecting the network access to the users of the device. It allows network access even in cases where there is a failure to authenticate, but it logs the results of the authentication process for diagnostic purposes. If the device fails to authenticate a client for any reason (for example, RADIUS access reject from the RADIUS server, RADIUS timeout, or the client itself is 802.1X unaware), the client is authenticated and is undisturbed by the failure condition(s). The reasons for failure are logged and buffered into the local logging database for tracking purposes.
EAPOL Flood Mode	The administrative mode of the Extensible Authentication Protocol (EAP) over LAN (EAPOL) flood support on the device. EAPOL Flood Mode can be enabled when Admin Mode and Monitor Mode are disabled.

Interface Port Access Control Fields

Interface	The interface associated with the rest of the data in the row.
PAE Capabilities	<p>The Port Access Entity (PAE) role, which is one of the following:</p> <ul style="list-style-type: none"> • 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	<p>The port-based access control mode configured on the port, which is one of the following:</p> <ul style="list-style-type: none"> • Auto – The port is unauthorized until a successful authentication exchange has taken place. • Force Unauthorized – The port ignores supplicant authentication attempts and does not provide authentication services to the client. • Force Authorized – The port sends and receives normal traffic without client port-based authentication. • 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	<p>The control mode under which the port is actually operating, which is one of the following:</p> <ul style="list-style-type: none"> • Auto • Force Unauthorized • Force Authorized • MAC-Based • N/A <p>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.</p>
PAE State	<p>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:</p> <ul style="list-style-type: none"> • Initialize • Disconnected • Connecting • Authenticating • Authenticated • Aborting • Held • ForceAuthorized • ForceUnauthorized

Field	Description
Backend State	<p>The current state of the back-end authentication state machine, which is the 802.1X process that controls the interaction between the 802.1X client on the local system and the remote authentication server. The state can be one of the following:</p> <ul style="list-style-type: none"> • Request • Response • Success • Fail • Timeout • Initialize • Idle
Initialize (Icon)	Click the Initialize icon 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. This icon can be clicked only when the port is an authenticator and the operating control mode is Auto.
Re-Authenticate (Icon)	Click the Re-Authenticate icon to force the associated interface to restart the authentication process.

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**.

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 132. Edit Port Configuration Page

The screenshot shows the 'Edit Port Configuration' window. At the top, the 'Interface' is set to '2'. Under 'PAE Capabilities', the 'Authenticator' radio button is selected. The 'Authenticator Options' section includes fields for Control Mode (Auto), Quiet Period (60s), Transmit Period (30s), Guest VLAN ID (0), Guest VLAN Period (90s), Unauthenticated VLAN ID (0), Supplicant Timeout (30s), Server Timeout (30s), Maximum Requests (2), MAC Authentication Mode (unchecked), MAC Authentication Type (EAP-MD5), Re-Authentication Period (0s), and Maximum Users (32). The 'Supplicant Options' section includes Control Mode (Auto), Username (None), Authentication Period (30s), Start Period (30s), Held Period (60s), and Maximum Start Messages (3). At the bottom are 'Apply' and 'Cancel' buttons.

Section	Field	Value	Range/Notes
Authenticator Options	Control Mode	Auto	
	Quiet Period (Seconds)	60	(0 to 65535)
	Transmit Period (Seconds)	30	(1 to 65535)
	Guest VLAN ID	0	(0 to 4093, 0 = Default, 0 = Disable)
	Guest VLAN Period (Seconds)	90	(1 to 300)
	Unauthenticated VLAN ID	0	(0 to 4093, 0 = Default, 0 = Disable)
	Supplicant Timeout (Seconds)	30	(1 to 65535)
	Server Timeout (Seconds)	30	(1 to 65535)
	Maximum Requests	2	(1 to 10)
	MAC Authentication Mode	<input type="checkbox"/>	
	MAC Authentication Type	EAP-MD5	(PAP is also an option)
	Re-Authentication Period (Seconds)	0	(0 to 65535, 0 = Default, 0 = Disable)
	Maximum Users	32	(1 to 32)
	Supplicant Options	Control Mode	Auto
Username		None	
Authentication Period (Seconds)		30	(1 to 65535)
Start Period (Seconds)		30	(1 to 65535)
Held Period (Seconds)		60	(1 to 65535)
Maximum Start Messages		3	(1 to 10)

3. Update the 802.1X settings on the interface. [Table 96](#) 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 96. Per-Port Port Access Control 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	<p>The Port Access Entity (PAE) role, which is one of the following:</p> <ul style="list-style-type: none"> • 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. <p>To change the PAE capabilities of a port, click the Edit icon associated with the field and select the desired setting from the menu in the Set PAE Capabilities window.</p>
Authenticator Options	
The fields in this section can be changed only when the selected port is configured as an authenticator port (that is, the PAE Capabilities field is set to Authenticator).	
Control Mode	<p>The port-based access control mode on the port, which is one of the following:</p> <ul style="list-style-type: none"> • Auto – The port is unauthorized until a successful authentication exchange has taken place. • Force Unauthorized – The port ignores supplicant authentication attempts and does not provide authentication services to the client. • Force Authorized – The port sends and receives normal traffic without client port-based authentication. • 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.
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. When this field is 0, the guest VLAN facility is disabled.
Guest VLAN Period	The value, in seconds, of the timer used for guest VLAN authentication.
Unauthenticated VLAN ID	The VLAN ID of the unauthenticated VLAN. Hosts that fail the authentication might be denied access to the network or placed on a VLAN created for unauthenticated clients. This VLAN might be configured with limited network access. To set the unauthenticated VLAN ID, click the Edit icon associated with the field and specify the ID value in the available field. To reset the unauthenticated VLAN ID to the default value, click the Reset icon associated with the field and confirm the action.
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.

Field	Description
MAC Authentication Mode	The MAC Authentication mode of the port, which can be enabled or disabled. When MAC Authentication is enabled on the port (along with the Authenticator role and MAC-based control mode), stations connected to the port that do not support 802.1X can still be authenticated at the RADIUS server using the station's MAC address. Specifically, when the port detects a new, unauthorized station on the port, the switch first attempts to authenticate it using 802.1X. If the station does not respond, then after a time-out period, the switch extracts the station's MAC address from the detected packets and sends this to the RADIUS server for authentication. The RADIUS server responds with an authentication result, which is then applied to the port using the station's MAC address in MAC-based control mode. Note: MAC Authentication Mode cannot be enabled if Guest VLAN ID is non-zero, i.e., enabled.
MAC Authentication Type	The authentication type to be used for MAC-based access requests sent to the RADIUS server, which is one of the following: <ul style="list-style-type: none"> EAP-MD5 – The port uses EAP-MD5 authentication and sends the MD5 hash of the MAC address as the password in the EAP-Message (RADIUS attribute 79) to the authentication server. PAP – The port uses PAP authentication and sends the MAC address of the client as the password (clear text) in the User-Password (RADIUS attribute 2) to the authentication server.
Re-Authentication Period	The amount of time that clients can be connected to the port without being reauthenticated. If this field is disabled, connected clients are not forced to reauthenticate periodically. To change the value, click the Edit icon associated with the field and specify a value in the available field. To reset the reauthentication period to the default value, click the Reset icon associated with the field and confirm the action.
Maximum Users	The maximum number of clients supported on the port if the Control Mode on the port is MAC-based 802.1X authentication.

Supplicant Options

The fields in this section can be changed only when the selected port is configured as a supplicant port (that is, the PAE Capabilities field is set to Supplicant).

Control Mode	The port-based access control mode on the port, which is one of the following: <ul style="list-style-type: none"> 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 Unauthorized – The port is placed into an unauthorized state and is automatically denied system access. 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.
Username	The name the port uses to identify itself as a supplicant to the authenticator port. The menu includes the users that are configured for system management. When authenticating, the supplicant provides the password associated with the selected User Name.
Authentication Period	The amount of time the supplicant port waits to receive a challenge from the authentication server. If the configured Authentication Period expires, the supplicant retransmits the authentication request until it is authenticated or has sent the number of messages configured in the Maximum Start Messages field.
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.

Viewing Per-port 802.1X Details

To view the 802.1X configuration on an interface, select the interface and click **Details**. See [Table 96](#) 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.

Port Access Control Statistics

Use this page 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 Port Access Control Statistics page, click **Security > Port Access Control** in the navigation pane, and click the **Statistics** tab.

Figure 133. Port Access Control Statistics Page

Configuration

Statistics

Client Summary

History Log Summary

Port Access Control Statistics

Help

Display10rows

Showing 1 to 10 of 26 entries

Filter:

<input type="checkbox"/>	↕ Interface	↕ PAE Capabilities	↕ EAPOL Frames Received	↕ EAPOL Frames Transmitted	↕ Last EAPOL Frame Version	↕ Last EAPOL Frame Source
<input type="checkbox"/>	1	Authenticator	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	2	Authenticator	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	3	Authenticator	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	4	Authenticator	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	5	Authenticator	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	6	Authenticator	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	7	Authenticator	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	8	Authenticator	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	9	Authenticator	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	10	Authenticator	0	0	0	00:00:00:00:00:00

First

Previous

1

2

3

Next

Last

Refresh

Details

Clear

Table 97. Port Access Control Statistics Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When viewing detailed information for an interface, this field identifies the interface being viewed.
PAE Capabilities	The Port Access Entity (PAE) role, which is one of the following: <ul style="list-style-type: none">• 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.

Field	Description
Last EAPOL Frame Source	The protocol version number attached to the most recently received EAPOL frame.
Port Access Control Details	
The following information 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.	
EAPOL Start Frames Received	The total number of EAPOL-Start frames received on the interface. EAPOL-Start frames are sent by a supplicant to initiate the 802.1X authentication process when it connects to the interface. This field is displayed only if the interface is configured as an authenticator.
EAPOL Logoff Frames Received	The total number of EAPOL-Logoff frames received on the interface. EAPOL-Logoff frames are sent by a supplicant to indicate that it is disconnecting from the network, and the interface can return to the unauthorized state. This field is displayed only if the interface is configured as an authenticator.
EAP Response/ID Frames Received	The total number of EAP-Response Identity frames the interface has received. EAP-Response Identity frames are sent by a supplicant to provide user information that is used to for authentication. This field is displayed only if the interface is configured as an authenticator.
EAP Response Frames Received	The total number of EAP-Response frames the interface has received. EAP-Response frames are sent from a supplicant to an authentication server during the authentication process. This field is displayed only if the interface is configured as an authenticator.
EAP Request/ID Frames Transmitted	The total number of EAP-Request Identity frames the interface has sent. EAP-Request Identity frames are sent from an authenticator to a supplicant to request user information that is used to for authentication. This field is displayed only if the interface is configured as an authenticator.
EAP Request Frames Transmitted	The total number of EAP-Request frames the interface has sent. EAP-Request frames are sent from an authentication server to the client to request authentication information. This field is displayed only if the interface is configured as an authenticator.
EAPOL Start Frames Transmitted	The total number of EAPOL-Start frames the interface has sent to a remote authenticator. EAPOL-Start frames are sent by a supplicant to initiate the 802.1X authentication process when it connects to the interface. This field is displayed only if the interface is configured as a supplicant.
EAPOL Logoff Frames Transmitted	The total number of EAPOL-Logoff frames the interface has sent to a remote authenticator. EAPOL-Logoff frames are sent by a supplicant to indicate that it is disconnecting from the network, and the interface can return to the unauthorized state. This field is displayed only if the interface is configured as a supplicant.
EAP Response/ID Frames Transmitted	The total number of EAP-Response Identity frames the interface has sent. EAP-Response Identity frames are sent by a supplicant to provide user information that is used to for authentication. This field is displayed only if the interface is configured as a supplicant.
EAP Response Frames Transmitted	The total number of EAP-Response frames the interface has transmitted. EAP-Response frames are sent from a supplicant to an authentication server during the authentication process. This field is displayed only if the interface is configured as an supplicant.
EAP Request/ID Frames Received	The total number of EAP-Request Identity frames the interface has received. EAP-Request Identity frames are sent from an authenticator to a supplicant to request user information that is used to for authentication. This field is displayed only if the interface is configured as a supplicant.
EAP Request Frames Received	The total number of EAP-Request frames the interface has received. EAP-Request frames are sent from the authentication server to the supplicant during the authentication process. This field is displayed only if the interface is configured as a supplicant.
Invalid EAPOL Frames Received	The number of unrecognized EAPOL frames received on the interface.
EAPOL Length Error Frames Received	The number of EAPOL frames with an invalid packet body length received on the interface.

To reset all statistics counters to 0, select each interface with the statistics to reset and click **Clear**.

Port Access Control Client Summary

This page displays information about supplicant devices that are connected to the local authenticator ports. If there are no active 802.1X sessions, the table is empty. To view additional information about a supplicant, select the interface it is connected to and click **Details**.

To access the Port Access Control Client Summary page, click **Security > Port Access Control** in the navigation pane, and then click the **Client Summary** tab.

Figure 134. Port Access Control Client Summary Page

Configuration Statistics **Client Summary** History Log Summary

Port Access Control Client Summary Help

Display **All** rows Showing 0 to 0 of 0 entries Filter:

↕ Interface	↕ Logical Interface	↕ Username	↕ Supplicant MAC Address	↕ Session Time	↕ VLAN ID
Table is Empty					

[First](#) [Previous](#) [Next](#) [Last](#)

[Refresh](#) [Details](#)

Table 98. Port Access Control Client Summary Fields

Field	Description
Interface	The local 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.
Logical Interface	The logical port number associated with the supplicant that is connected to the port.
User Name	The name the client uses to identify itself as a supplicant to the authentication server.
Supp MAC Address	The MAC address of the supplicant that is connected to the port.
Session Time	The amount of time that has passed since the connected supplicant was granted access to the network through the authenticator port.
Filter ID	The policy filter ID assigned by the authenticator to the supplicant device.
VLAN ID	The ID of the VLAN the supplicant was placed in as a result of the authentication process.

Port Access Control Client Details

The following information describes the additional fields that appear in the Port Access Control Client Details window.

Session Timeout	The reauthentication timeout period set by the RADIUS server to the supplicant device.
Session Termination Action	The termination action set by the RADIUS server that indicates the action that will take place once the supplicant reaches the session timeout value.

Port Access Control History Log Summary

Use this page to grant or deny port access to users configured on the system. To change the access control privileges for one or more ports, select each interface to configure and click **Edit**. The same settings are applied to all selected interfaces.

To access the Port Access Control History Log Summary page, click **Security > Port Access Control** in the navigation pane, and click the **History Log Summary** tab.

Figure 135. Port Access Control History Log Summary Page

Configuration Statistics Client Summary **History Log Summary**

Port Access Control History Log Summary [Help](#)

Display **All** rows Showing 0 to 0 of 0 entries Filter:

↕ Interface	↕ Time Stamp	↕ VLAN Assigned	↕ VLAN Assigned Reason	↕ Supp MAC Address	↕ Auth Status	↕ Reason
Table is Empty						

First Previous Next Last

[Refresh](#) [Clear History](#)

Table 99. Port Access Control History Log Summary Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. Only interfaces that have entries in the log history are listed.
Time Stamp	The absolute time when the authentication event took place.
VLAN Assigned	The ID of the VLAN the supplicant was placed in as a result of the authentication process.
VLAN Assigned Reason	The reason why the authenticator placed the supplicant in the VLAN. Possible values are: <ul style="list-style-type: none">• RADIUS• Unauth• Default• Not Assigned
Supp MAC Address	The MAC address of the supplicant that is connected to the port.
Filter Name	The policy filter ID assigned by the authenticator to the supplicant device.
Auth Status	The authentication status of the client or port.
Reason	The reason for the successful or unsuccessful authentication.

To reset the history log, click **Clear History**.

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 Global Administration

Use this page to configure the global admin mode for Port Security.

To access the Port Security Global Administration page, click **Security > Port Security** in the navigation pane.

Figure 136. Port Security Global Administration Page

GlobalInterfaceStatic MACDynamic MAC

Port Security Global Administration

Help

Port Security Admin Mode

☒ Enable☐ Disable

Auto Recovery

Auto Recovery

Apply

Refresh

Cancel

Table 100. Port Security Global Administration Fields

Field	Description
Port Security Admin Mode	Enable or disable the global administrative mode for port security. The port security mode must be enabled both globally and on an interface to enforce the configured limits for the number of static and dynamic MAC addresses allowed on that interface.
Auto Recovery	Click Auto Recovery to redirect your browser to the Auto Recovery Configuration page. For more information about the Auto Recovery feature, see "Auto Recovery Configuration" on page 86 .

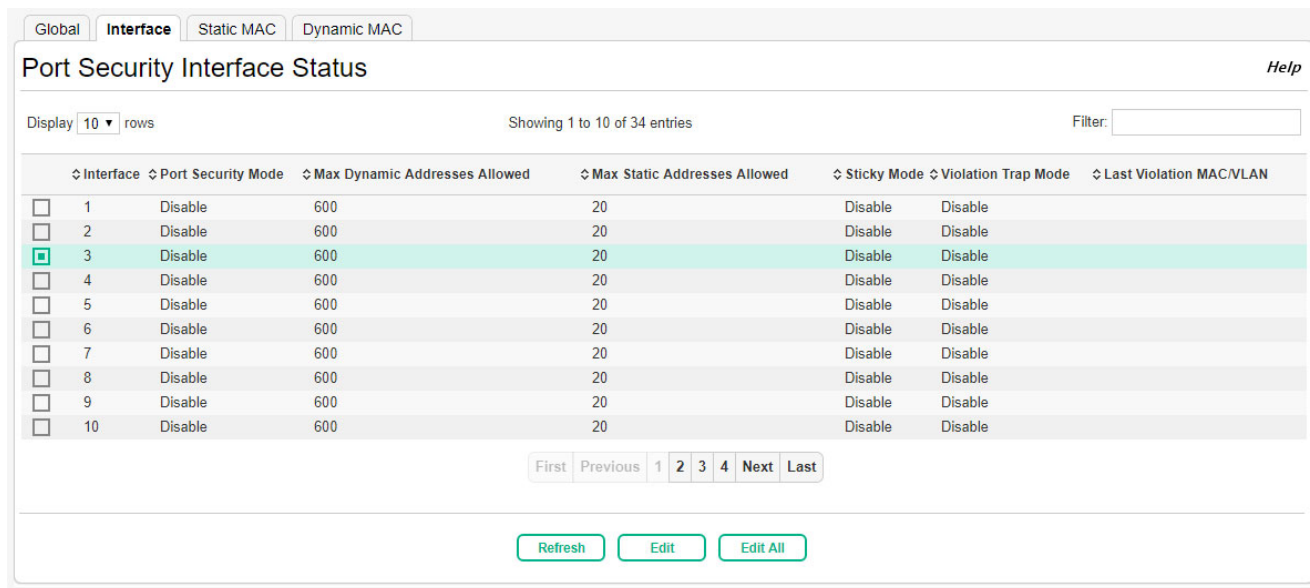
Click **Apply** to save any changes for the current boot session. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Port Security Interface Status

Use this page to view and configure the port security settings for each interface.

To access the Port Security Interface Status page, click **Security > Port Security** in the navigation pane, and then click the **Interface** tab.

Figure 137. Port Security Interface Status Page



	Interface	Port Security Mode	Max Dynamic Addresses Allowed	Max Static Addresses Allowed	Sticky Mode	Violation Trap Mode	Last Violation MAC/VLAN
<input type="checkbox"/>	1	Disable	600	20	Disable	Disable	
<input type="checkbox"/>	2	Disable	600	20	Disable	Disable	
<input checked="" type="checkbox"/>	3	Disable	600	20	Disable	Disable	
<input type="checkbox"/>	4	Disable	600	20	Disable	Disable	
<input type="checkbox"/>	5	Disable	600	20	Disable	Disable	
<input type="checkbox"/>	6	Disable	600	20	Disable	Disable	
<input type="checkbox"/>	7	Disable	600	20	Disable	Disable	
<input type="checkbox"/>	8	Disable	600	20	Disable	Disable	
<input type="checkbox"/>	9	Disable	600	20	Disable	Disable	
<input type="checkbox"/>	10	Disable	600	20	Disable	Disable	

To configure port security settings on one or more interfaces, select the interface or interfaces to configure, and then click **Edit**. To configure all interfaces at the same time, click **Edit All**.

Table 101. 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 Mode	The administrative mode of the port security feature on the interface. The port security mode must be enabled both globally and on an interface to enforce the configured limits for the number of static and dynamic MAC addresses allowed on that interface.
Max Dynamic Addresses Allowed	The number of source MAC addresses that can be dynamically learned on an interface. If an interface reaches the configured limit, any other addresses beyond that limit are not learned, and the frames are discarded. Frames with a source MAC address that has already been learned will be forwarded. A dynamically-learned MAC address is removed from the MAC address table if the entry ages out, the link goes down, or the system resets. Note that the behavior of a dynamically-learned address changes if the sticky mode for the interface is enabled or the address is converted to a static MAC address.
Max Static Addresses Allowed	The number of source MAC addresses that can be manually added to the port security MAC address table for an interface. If the port link goes down, the statically configured MAC addresses remain in the MAC address table. The maximum number includes all dynamically-learned MAC addresses that have been converted to static MAC addresses.

Field	Description
Sticky Mode	<p>The sticky MAC address learning mode is one of the following:</p> <ul style="list-style-type: none"> 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 device 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 Mode	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 Mode	Indicates whether the port security feature shuts down the port after the MAC limit is reached.
Last Violation MAC/VLAN	The source MAC address and, if applicable, associated VLAN ID of the last frame that was discarded at a locked port.

Port Security Static MAC Addresses

Use this page to add and remove the MAC addresses of hosts that are allowed to send traffic to specific interfaces on the device. The number of MAC addresses you can associate with each interface is determined by the maximum static MAC addresses allowed on a given interface.

To display this page, click **Security > Port Security** in the navigation pane, and then click the **Static MAC** tab.

Figure 138. Port Security Static MAC Addresses Page

Global Interface **Static MAC** Dynamic MAC

Port Security Static MAC Addresses Help

Display **All** rows Showing 1 to 2 of 2 entries Filter:

<input type="checkbox"/>	Interface	Static MAC Address	VLAN ID	Sticky Mode
<input type="checkbox"/>	1	00:01:02:03:04:05	1	Enable
<input type="checkbox"/>	1	00:01:02:03:04:06	1	Enable

First Previous 1 Next Last

Refresh Add Remove

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**. You must confirm the action before the entry is deleted.

Table 102. Port Security Static MAC Addresses Fields

Field	Description
Interface	The interface associated with the rest of the data in the row. When adding a static MAC address entry, use the Interface menu to select the interface to associate with the permitted MAC address.
Static MAC Address	The MAC address of the host that is allowed to forward packets on the associated interface.
VLAN ID	The ID of the VLAN that includes the host with the specified MAC address.
Sticky Mode	Indicates whether the static MAC address entry is added in sticky mode. When adding a static MAC address entry, the Sticky Mode field can be selected only if it is enabled on the interface. If a static MAC address is added in sticky mode, and sticky mode is disabled on the interface, the MAC address entry is converted to a dynamic entry and will age out and be removed from the running (and saved) configuration if it is not relearned.

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

Port Security Dynamic MAC Addresses

Use this page to view the dynamic MAC address entries that have been learned on each interface. From this page, you can also convert dynamic MAC address entries to static MAC address entries for a given interface. If the limit of statically-locked MAC addresses is less than the number of dynamically-locked MAC addresses to convert, then the addresses are converted in the order in which they were learned until the number of allowed static MAC address entries is reached.

To display this page, click **Security > Port Security** in the navigation pane, and then click the **Dynamic MAC** tab.

Figure 139. Port Security Dynamic MAC Addresses Page

Global Interface Static MAC Dynamic MAC		
Port Security Dynamic MAC Addresses Help		
Display All ▼ rows Showing 1 to 9 of 9 entries Filter: <input type="text"/>		
↕ Interface	↕ Dynamic MAC Address	↕ VLAN ID
16	00:1A:70:15:9A:FA	1
16	00:1B:21:AB:53:E7	1
16	00:1B:21:AB:54:37	1
16	00:40:9D:32:95:0B	1
16	00:FC:E3:90:01:93	1
16	00:FC:E3:90:01:95	1
16	30:8D:99:ED:70:AA	1
16	90:B1:1C:6A:76:65	1
16	E0:2F:6D:44:17:C1	1
First Previous 1 Next Last		
Refresh Convert to Static		

Table 103. Port Security Dynamic MAC Addresses Fields

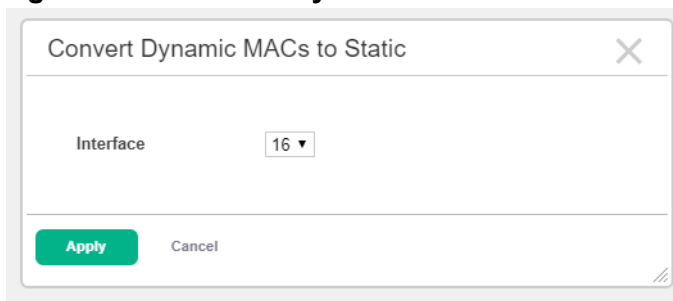
Field	Description
Interface	The interface associated with the rest of the data in the row. When converting dynamic addresses to static addresses, use the Interface menu to select the interface to associate with the MAC addresses.
Dynamic MAC Address	The MAC address that was learned on the device. An 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.
Convert to Static (Button)	Converts all MAC addresses learned on an interface to static MAC address entries. After you click the button, a window opens and allows you to select the interface associated with the MAC address entries to convert. A static MAC address entry is written to the running configuration file and does not age out.

Convert Dynamic MAC Addresses to Static MAC Addresses

To convert dynamic MAC addresses to static MAC addresses:

1. Click the **Convert to Static** button.

The Convert Dynamic MACs to Static window appears.

Figure 140. Convert Dynamic MACs to Static

2. In the Interface field, select the interface with the dynamically learned MAC addresses to convert.
3. Click **Apply**.

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

Protected Ports

A port that is a member of a protected ports group is a protected port. A port that is not a member of any protected ports group is an unprotected port. Each port can be a member of only one protected ports group. Ports in the same protected ports group cannot forward traffic to other protected ports within the group, even if they are members of the same VLAN. However, a port in a protected ports group can forward traffic to ports that are in a different protected ports group. A protected port can also forward traffic to unprotected ports. Unprotected ports can forward traffic to both protected and unprotected ports.

Protected Ports Configuration

Use this page to configure and view protected ports groups.

To access the Protected Ports Configuration page, click **Security > Protected Ports** in the navigation pane.

Figure 141. Protected Ports Configuration Page

Protected Ports Configuration

Help

Display

All

 rows

Showing 1 to 1 of 1 entries

Filter:

<input type="checkbox"/> ↕ Group Name	Protected Ports
<input type="checkbox"/> Lab1	5, 6, 7

First

Previous

1

Next

Last

Refresh

Add

Edit

Remove

Table 104. Protected Ports Configuration Fields

Field	Description
Group Name	This is the configured name of the protected ports group.
Protected Ports	The ports that are members of the protected ports group. When adding a port to a protected ports group, the Available Interfaces field lists the ports that are not already members of a protected ports group. To move an interface between the Available Interfaces and Selected Interfaces fields, click the port (or CTRL + click to select multiple ports), and then click the appropriate arrow to move the port(s) to the desired field.

Creating a Protected Ports Group

To create a protected ports group and add ports to the group:

1. Click **Add**.

The Add Group page appears.

Figure 142. Add Protected Port Group Page

The screenshot shows a window titled "Add Group" with a close button (X) in the top right corner. Inside the window, there is a "Group Name" label followed by a text input field and a hint "(1 to 32 characters)". Below this is a section titled "Protected Ports". Under "Protected Ports", there are two list boxes: "Available Interfaces" and "Selected Interfaces". The "Available Interfaces" list contains the numbers 1, 2, 3, 4, 8, 9, 10, and 11. The "Selected Interfaces" list is currently empty. Between the two list boxes are two arrow buttons: a right-pointing arrow (>) and a left-pointing arrow (<). At the bottom of the window, there are two buttons: a green "Apply" button and a "Cancel" button.

2. Specify a name for the protected ports group.
3. Select one or more available interface and click the > arrow to move the selected interface or interfaces to the Selected Interfaces field. To select multiple interfaces, Ctrl + click each interface or use Shift + click to select a contiguous range of interfaces.
4. Click **Apply**.

Editing a Protected Ports Group

To change the name or the port members for an existing group, select the group to update and click **Edit**.

Removing a Protected Ports Group

To remove one or more protected ports groups, select each entry to delete and click **Remove**. You must confirm the action before the entry is deleted.

Storm Control

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.

Storm control provides the possibility of disabling an interface on which a storm is detected to prevent unnecessary congestion in the network. When enabled, the storm control threshold is automatically set to 5% of port speed. If the incoming rate of unicast (with unknown destination), multicast, or broadcast packets exceeds this value, the port moves to the diagnostically disabled state and remains in that state until it is re-enabled by the Auto Recovery feature or re-enabled manually by enabling it in the Port Configuration Status page (see [“Port Status” on page 36](#)). If the interface continues to encounter excessive traffic, it may be placed back into the diagnostically disabled state, and the interface will be disabled (link down). Storm Control functionality is applicable only to the physical interfaces.

Use the Storm Control Configuration page to configure the storm control administrative mode and to access the Auto Recovery page, where you can configure the auto recovery settings for Storm Control.

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

NOTE:

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 nominal 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.

Figure 143. Storm Control Configuration

Storm Control Configuration

Help

Storm Control

☐ Enabled ☒ Disabled

Auto Recovery

Auto Recovery

Apply

Refresh

Cancel

Table 105. Storm Control Configuration Fields

Field	Description
Storm Control Features	
Storm Control	Enable or disable storm control on the switch.
Auto Recovery	Click Auto Recovery to redirect your browser to the Auto Recovery Configuration page. For more information about the Auto Recovery feature, see “Auto Recovery Configuration” on page 86 .

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**.

12 Green Features

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

Green Features Configuration

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

Figure 144. Green Features

Table 106. Green Features 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 disabled by default.
Low-Power Idle (EEE)	EEE (Energy Efficient Ethernet) is designed to save power by turning off network ports that are not passing traffic. When this features is enabled, the ports can enter a low-power mode to reduce power consumption during periods of low link utilization. EEE works for ports in auto-negotiation mode, where the port is negotiated to either 100 Mbps full duplex or 1 Gbps (1000 Mbps) full duplex. This feature is disabled by default. CAUTION: EEE is automatically disabled for a port if its auto-negotiation mode becomes disabled. To re-enable EEE for any port after enabling its auto-negotiation mode, the Low Power Idle (EEE) mode for the switch must be manually disabled and then enabled again.

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**.

EEE Status

When EEE is enabled, you can use the EEE status page to view estimated power savings and power consumption information. This page also displays status information for each interface.

To display the EEE status page, click **Green Features** > **EEE Status** in the navigation pane.

Figure 145. EEE Status Page

EEE Status

Help

Estimated Energy Savings (W * H)

0

Estimated Power Savings (%)

0

Current Power Consumption (mWatts)

6170

Display10▼ rows

Showing 1 to 10 of 24 entries

Filter:

Interface	Link Partner Supports EEE	Auto Port Power-Down Status	Wakeup Time Negotiated by LLDP	Rx Wakeup time	Tx Wakeup time
1	No	Inactive	No	-	-
2	No	Inactive	No	-	-
3	No	Inactive	No	-	-
4	No	Inactive	No	-	-
5	No	Inactive	No	-	-
6	No	Inactive	No	-	-
7	No	Inactive	No	-	-
8	No	Inactive	No	-	-
9	No	Inactive	No	-	-
10	No	Inactive	No	-	-

First

Previous

1

2

3

Next

Last

Refresh

Table 107. EEE Status Fields

Field	Description
Global Statistics	
Estimated Energy Savings	The estimated cumulative energy saved on the device (in watts x hours) due to the Energy Efficient Ethernet feature.
Estimated Power Savings	The estimated percentage of power conserved on all ports due to the Energy Efficient Ethernet feature. For example, 10% means that the device required 10% less power.
Current Power Consumption	The estimated power consumption by all ports.
Per-Port Status	
Interface	The interface ID. The table displays all interfaces that are enabled for EEE.
Link Partner Supports EEE	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.
Wakeup Time Negotiated by LLDP	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, a dash displays).
Tx Wakeup time	The Tx wakeup time in effect for the port, if negotiated by LLDP (otherwise, a dash displays).

13 Diagnostics

You can use the Diagnostics pages to help troubleshoot network issues, view log and configuration information, reboot the switch, and reset the HPE OfficeConnect 1920S series switch to factory defaults.

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 bottom of the list.

NOTE:

If more than 200 logs accumulate, their Log Index numbers continue to increment beyond 200 and the oldest entries are deleted (for example, if 400 log entries were generated since the system was last restarted or the log file was cleared, then the log file would display entries 301 to 400).

To display the Log page, click **Diagnostics > Log** in the navigation pane.

Figure 146. Buffered Log Page

Log					Help
Buffered Log					
Display 10 rows		Showing 1 to 10 of 58 entries		Filter:	
Log Index	Log Time	Severity	Component	Description	
1	Jan 2 00:12:17	Info	USER_MGR	HTTP Session 15 started for user admin connected from 10.27.65.210	
2	Jan 1 23:54:50	Info	USER_MGR	HTTP Session 14 ended for user admin connected from 10.27.65.210	
3	Jan 1 23:35:59	Info	USER_MGR	HTTP Session 14 started for user admin connected from 10.27.65.210	
4	Jan 1 02:29:46	Info	USER_MGR	HTTP Session 13 ended for user admin connected from 10.27.65.205	
5	Jan 1 02:24:42	Info	USER_MGR	HTTP Session 13 started for user admin connected from 10.27.65.205	
6	Jan 1 01:17:00	Info	USER_MGR	HTTP Session 12 ended for user admin connected from 10.27.65.210	
7	Jan 1 01:01:01	Info	USER_MGR	HTTP Session 11 ended for user admin connected from 10.27.65.205	
8	Jan 1 00:56:52	Info	USER_MGR	HTTP Session 12 started for user admin connected from 10.27.65.210	
9	Jan 1 00:55:38	Info	USER_MGR	HTTP Session 11 started for user admin connected from 10.27.65.205	
10	Jan 1 00:54:37	Info	USER_MGR	HTTP Session 10 ended for user admin connected from 10.27.65.210	
First Previous 1 2 3 4 5 Next Last					
Refresh Clear Log					

The following information displays in the Buffered Log table.

Table 108. Buffered Log Fields

Field	Description
Log Index	The log number.
Log Time	Time at which the log was entered in the table.
Severity	The severity level associated with the log message. The severity can be one of the following: <ul style="list-style-type: none">• Emergency—The device is unusable.• Alert—Action must be taken immediately.• Critical—The device is experiencing primary system failures.• Error—The device is experiencing non-urgent failures.• Warning—The device is experiencing conditions that could lead to system errors if no action is taken.• Notice—The device is experiencing normal but significant conditions.• Info—The device is providing non-critical information.• Debug—The device is providing debug-level information.
Component	The system component that issued the log entry.
Description	A text description of the entry.

- Click the arrows next to the column headings to sort the list by the column, in ascending or descending order.
- Click **Clear Log** to delete all log messages.

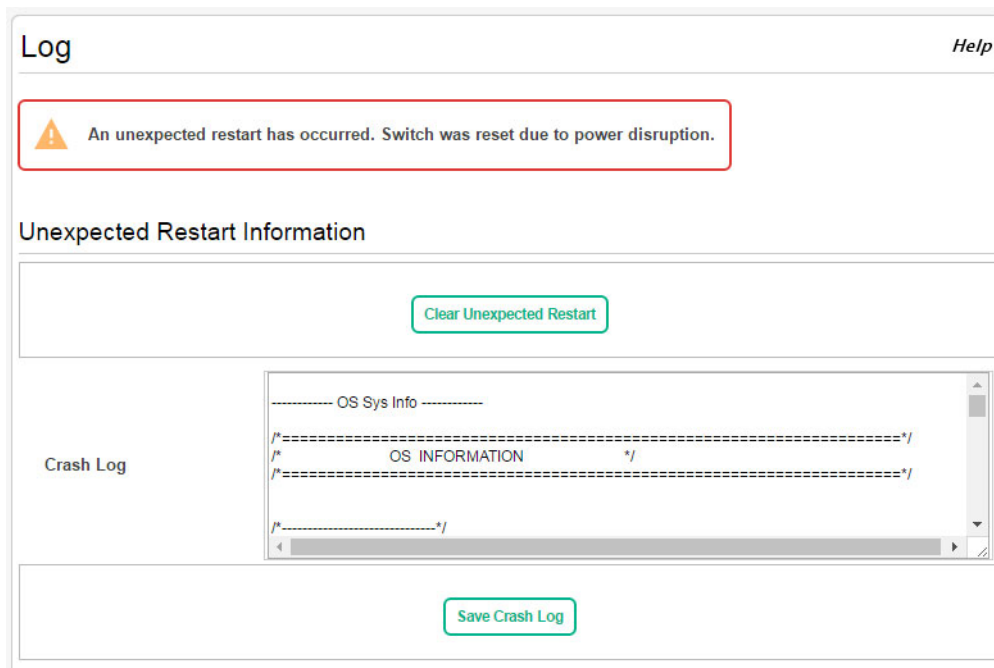
For information on configuring log settings, see [“Log Configuration” on page 200](#).

Crash Log

If there has been an unexpected restart of the switch, additional information displays near the top of the Log 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 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 147. Crash Log Information on Log Page



To clear the unexpected restart alert and the contents of the crash log, click **Clear Unexpected Restart**. You can click **Save Crash Log** to save the contents of the crash log to a file in tar.gz format (a compressed archive).

Log Configuration

The HPE OfficeConnect 1920S series switch software supports logging system messages to the buffered log file or forwarding messages over the network using the Syslog protocol. Syslog messages can be captured by a designated host on the network that is running a Syslog daemon. You can use the Log Configuration page to configure buffered log and Syslog settings.

To display the Log Configuration page, click **Diagnostics > Log Configuration** in the navigation pane.

Figure 148. Log Configuration Page

Log Configuration

Help

Buffered Log Configuration

Buffered Logging

☒ Enabled ☐ Disabled

Severity Filter

Info

Syslog Configuration

Syslog Host

☐ Enabled ☒ Disabled

UDP Port

514

(1 to 65535)

IP Address

(x.x.x.x or xxxxxxxx)

Severity Filter

Alert

Apply

Refresh

Cancel

Table 109. Log Configuration Fields

Field	Description
Buffered Log Configuration	
Buffered Logging	Enables or disables logging system events to the buffered log. This feature is enabled by default.
Severity Filter	<p>Specify type of system messages logged using the Buffered Logging Level setting:</p> <ul style="list-style-type: none">• Emergency—Alerts the user of the highest level of system error classified as urgent.• Alert—Alerts the user of a high level of system error.• Critical—Alerts the user of a high level of system error which must be immediately addressed.• Error—Alerts the user of an error in the system.• Warning—Warns the user of an impending system error of a specified operation.• Notice—Notifies the user of a system error.• Info—Provides the user with system information. This is the default filter level.• Debug—An internal note to reconcile programming code.
SysLog Configuration	
SysLog Host	Enables and disables logging to configured syslog hosts. When the syslog admin mode is disabled, the device does not relay logs to syslog hosts, and no messages are sent to any collector/relay. When enabled, messages are sent to configured collectors/relays using the values configured for each collector/relay. This feature is disabled by default.
UDP Port	The UDP port on the logging host to which syslog messages are sent. The port ID can be any value from 1 to 65535. The default is 514.
IP Address	The IP address of the remote host to receive log messages.
Severity Filter	The severity level threshold for log messages. All log messages with a severity level at and above the configured level are forwarded to the logging host. By default, messages designated as Alert and higher are forwarded to the Syslog host.

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**.

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.

Ping IPv4

Use the Ping IPv4 page 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 device configuration. To display the Ping IPv4 page, click **Diagnostics > Ping** in the navigation pane, and ensure the **IPv4** tab is selected.

Figure 149. Ping IPv4 Page

IPv4IPv6

Ping IPv4

Help

IP Address

10.27.36.234

(x.x.x.x)

Count

3

(1 to 15)

Interval (Seconds)

3

(1 to 60)

Size (Bytes)

0

(0 to 13000)

Source

☒ None☐ IP Address☐ Interface

Source IP Address

(x.x.x.x)

Interface

Network Port ▾

Status

Done

Results

Pinging 10.27.36.234 with 0 bytes of data:

Reply from 10.27.36.234: icmp_seq=0 time=6232 usec.

Reply from 10.27.36.234: icmp_seq=1 time=2763 usec.

Reply from 10.27.36.234: icmp_seq=2 time=2841 usec.

10.27.36.234 ping statistics----

3 packets transmitted, 3 packets received, 0% packet loss

round-trip (msec) min/avg/max = 2/3/6

Start

Stop

Table 110. Ping IPv4 Fields

Field	Description
IP Address	Specify the IP address you want to reach.
Count	Specify the number of packets to send. The range is 1 to 15 packets and the default is 3 packets.
Interval	Specify the delay between ping packets. The range is from 1 to 60 seconds, and the default is 3 seconds.
Size	Specify the size of the ping packet to be sent. Changing the size allows you to troubleshoot connectivity issues with a variety of packet sizes, such as large or very large packets. The range is from 0 to 13000 bytes, and the default is 0 bytes.
Source	The source IP address or interface to use when sending a ping request. If source is not required, select None as the source option.

Field	Description
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.
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.
Status	The current status of the ping test, which can be one of the following: <ul style="list-style-type: none"> Not Started—The ping test has not been initiated since viewing the page. In Progress—The ping test has been initiated and is running. Stopped—The ping test was interrupted because the user clicked the Stop button. 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: <ul style="list-style-type: none"> The IP address of the device that was pinged. The Internet Control Message Protocol (ICMP) number of the packet, starting from 0. 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.

Click **Start** to ping the specified host and **Stop** to end a ping in progress. If you do not click **Stop**, 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.

Ping IPv6

Use the Ping IPv6 page to send one or more ping requests from the switch to a specified IPv6 address. You can use the ping request to check whether the switch can communicate with a particular host on an IP network. The information you enter on this page is not saved as part of the device configuration.

To display the Ping IPv6 page, click **Diagnostics > Ping** in the navigation pane, and then click the **IPv6** tab.

Figure 150. Ping IPv6 Page

IPv4 IPv6

Ping IPv6 Help

Ping ☐ Global ☒ Link Local

IPv6 Address (xxxxxxxx)

Count (1 to 15)

Interval (Seconds) (1 to 60)

Size (Bytes) (0 to 13000)

Interface

Results

Send count=3, Receive count=0 from FE80::CE00:4FF:FE98:10

Table 111. Ping IPv6 Fields

Field	Description
Ping	Select either a global IPv6 address or a link local address to ping. A global address is routable over the Internet, while a link-local address is intended for communication only within the local network. Link local addresses have a prefix of fe80::/64.
IPv6 Address	Enter the global or link-local IPv6 address to ping.
Count	Specify the number of packets to send. The range is 1 to 15 packets and the default is 3 packets.
Interval	Specify the delay between ping packets. The range is from 1 to 60 seconds, and the default is 3 seconds.
Size	Specify the size of the ping packet to be sent. Changing the size allows you to troubleshoot connectivity issues with a variety of packet sizes, such as large or very large packets. The range is from 0 to 13000 bytes, and the default is 0 bytes.
Interface	The interface used to issue the Link Local ping request, which is the network port.
Results	The results of the ping test, which includes the following information: <ul style="list-style-type: none">• The IP address of the device that was pinged.• The Internet Control Message Protocol (ICMP) number of the packet, starting from 0.• 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.

Click **Start** to ping the specified host and **Stop** to end a ping in progress. If you do not click **Stop**, the pings continue until the number of pings specified in the Count field has been reached—even if you navigate away from the Ping IPv6 page.

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.

Traceroute IPv4

Use this page to determine the Layer 3 path a packet takes from the device to a specific IP address or hostname. When you initiate the traceroute command by clicking the Start button, the device sends a series of traceroute probes toward the destination. The results list the IP address of each layer 3 device 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 device configuration.

To display the Traceroute IPv4 page, click **Diagnostics > Traceroute** in the navigation pane, and ensure the **IPv4** tab is selected.

Figure 151. Traceroute IPv4 Page

IPv4 IPv6

Traceroute IPv4 Help

IP Address	<input type="text" value="10.27.36.234"/>	(x.x.x.x)
Probes Per Hop	<input type="text" value="3"/>	(1 to 10)
MaxTTL	<input type="text" value="30"/>	(1 to 255)
InitTTL	<input type="text" value="1"/>	(1 to 255)
MaxFail	<input type="text" value="5"/>	(1 to 255)
Interval (Seconds)	<input type="text" value="3"/>	(1 to 60)
Port	<input type="text" value="33434"/>	(1 to 65535)
Size (Bytes)	<input type="text" value="0"/>	(0 to 39936)
Source	<input checked="" type="radio"/> None <input type="radio"/> IP Address <input type="radio"/> Interface	
Source IP Address	<input type="text" value=""/>	(x.x.x.x)
Interface	<input type="text" value="Network Port"/>	
Status	Done	

Results

```
Traceroute to 10.27.36.234, 30 Hops Max, 0 Size packets:
 1  10.27.36.234  <1 ms  <1 ms  <1 ms

Hop Count=1, Last TTL=1, Test Attempt=3, Test Success=3
```

Table 112. Traceroute IPv4 Fields

Field	Description
IP Address	The IP address of the system to attempt to reach.
Probes Per Hop	Traceroute works by sending UDP packets with increasing Time-To-Live (TTL) values. Specify the number of probes sent with each TTL.
MaxTTL	The maximum Time-To-Live (TTL). The traceroute terminates after sending probes that can be layer 3 forwarded this number of times. If the destination is further away, the traceroute will not reach it.
InitTTL	The initial Time-To-Live (TTL). This value controls the maximum number of layer 3 hops that the first set of probes may travel.
MaxFail	The number of consecutive failures that terminate the traceroute. If the device fails to receive a response for this number of consecutive probes, the traceroute terminates.
Interval	The number of Seconds to wait between sending probes.
Port	The UDP destination port number to be used in probe packets. The port number should be a port that the target host is not listening on, so that when the probe reaches the destination, it responds with an ICMP Port Unreachable message.
Size	The size of probe payload in bytes.
Source	The source to use when sending the traceroute, which can be one of the following: <ul style="list-style-type: none"> • None – No source is required. • IP Address – Use the IP address specified in the Source IPv6 Address field as the source. • Interface – The interface to use as the 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.
Interface	The source interface to use when sending the traceroute. This field is enabled when Interface is selected as source option.
Status	The current status of the traceroute, which can be: <ul style="list-style-type: none"> • Not Started – The traceroute has not been initiated since viewing the page. • In Progress – The traceroute has been initiated and is running. • Stopped – The traceroute was interrupted by clicking the Stop button. • Done – The traceroute has completed, and information about the traceroute is displayed in the Results area.
Results	The results of the traceroute are displayed

Click **Start** to send the traceroute to the specified host and **Stop** to end a traceroute in progress.

Traceroute IPv6

Use this page to determine the Layer 3 path a packet takes from the device to a specific IPv6 address or hostname. When you initiate the traceroute command by clicking the Start button, the device sends a series of traceroute probes toward the destination. The results list the IP address of each Layer 3 device 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 device configuration.

To display the Traceroute IPv6 page, click **Diagnostics > Traceroute** in the navigation pane, and click the **IPv6** tab.

Figure 152. Traceroute IPv6 Page

IPv4IPv6

Traceroute IPv6

Help

IPv6 Address

2001:4860:4860::8844

(xxxxxxxx)

Probes Per Hop

3

(1 to 10)

MaxTTL

30

(1 to 255)

InitTTL

1

(1 to 255)

MaxFail

5

(1 to 255)

Interval (Seconds)

3

(1 to 60)

Port

33434

(1 to 65535)

Size (Bytes)

0

(0 to 39936)

Interface

Network Port

Results

Tracing route over a maximum of 30 hops

1 :: N N N

Hop Count = 1 Last TTL = 1 Test attempt = 3 Test Success = 0

Apply

Table 113. Traceroute IPv6 Fields

Field	Description
IPv6 Address	The IPv6 address of the system to attempt to reach.
Probes Per Hop	Traceroute works by sending UDP packets with increasing Time-To-Live (TTL) values. Specify the number of probes sent with each TTL.
MaxTTL	The maximum Time-To-Live (TTL). The traceroute terminates after sending probes that can be layer 3 forwarded this number of times. If the destination is further away, the traceroute will not reach it.
InitTTL	The initial Time-To-Live (TTL). This value controls the maximum number of layer 3 hops that the first set of probes may travel.
MaxFail	The number of consecutive failures that terminate the traceroute. If the device fails to receive a response for this number of consecutive probes, the traceroute terminates.
Interval	The number of Seconds to wait between sending probes.

Field	Description
Port	The UDP destination port number to be used in probe packets. The port number should be a port that the target host is not listening on, so that when the probe reaches the destination, it responds with an ICMP Port Unreachable message.
Size	The size of probe payload in bytes.
Interface	The source interface to use when sending the traceroute, which is the network port.
Results	The results of the traceroute are displayed

Click **Apply** to send the traceroute to the specified host.

Reboot Switch

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 Switch page, click **Diagnostics > Reboot Switch**.

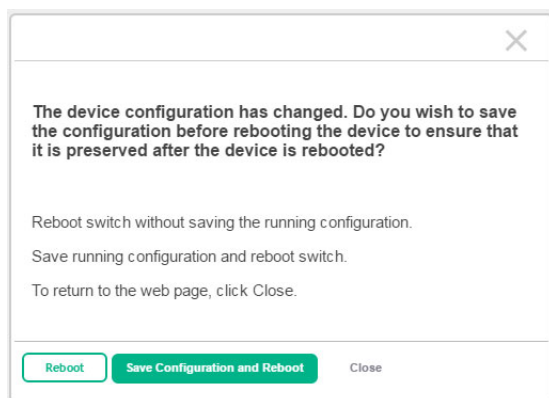
Figure 153. Reboot Switch Page



Click **Reboot** to reboot the switch.

If the device configuration has changed but has not been saved, the following window appears after you click Reboot. This window provides the opportunity to save the current configuration before rebooting the switch.

Figure 154. Save Before Reboot



Factory Defaults

You can use the Reset Configuration page to restore all settings to their factory default values. 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 Factory Defaults page, click **Diagnostics > Factory Defaults**.




CAUTION:

It is recommended that you back up the current configuration file prior to restoring the factory defaults configuration. See [“Dual Image Configuration” on page 215](#) for instructions.

Figure 155. Reset Configuration Page

Factory Defaults Help

 Initiates the action to reset all configuration parameters to their factory default settings after displaying a confirmation message. All configuration changes, including those that were previously saved, are reset in the running system by this action. It is possible that the IP address of the switch may change. If this occurs the user shall need to determine the new IP address to access the device using the web.

[Reset](#)

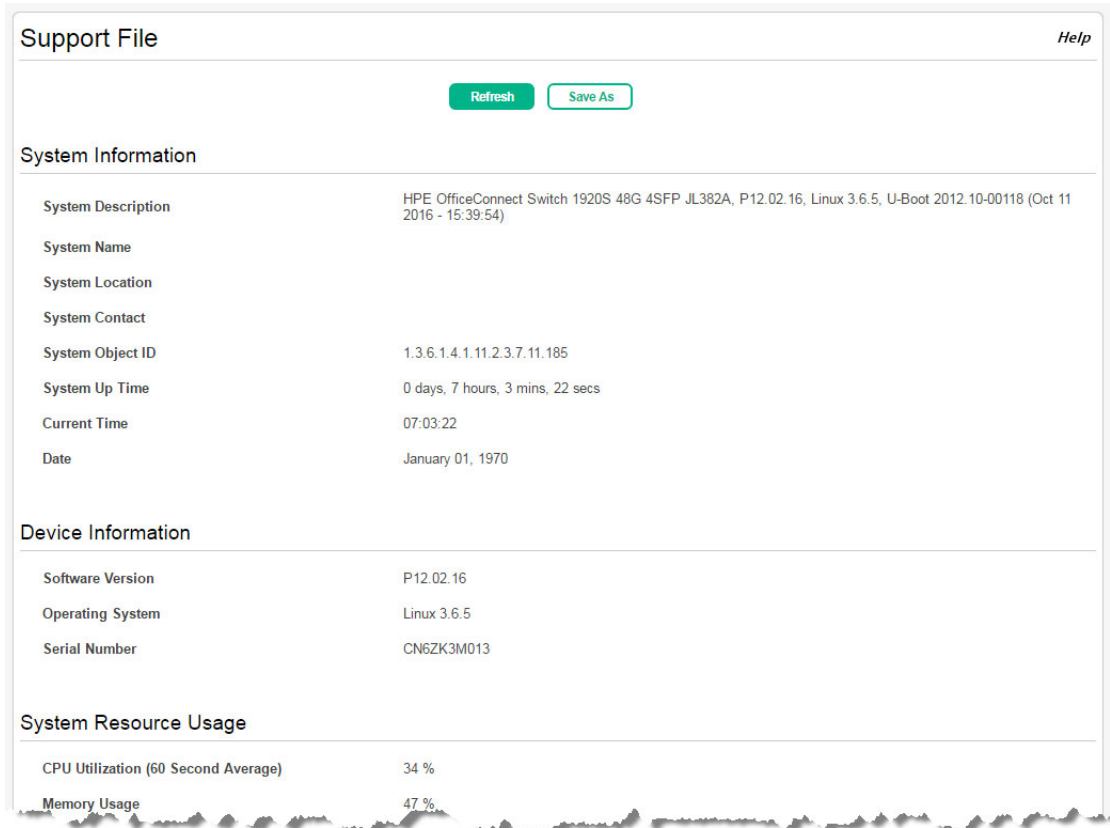
Click **Reset** to restore the system to the default settings.

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. [Figure 156](#) shows a partial view of the page.

Figure 156. Support File Page



The support file page includes the following information:

- System Information— A system description, name, location, and contact information, along with date and time information.
- 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.

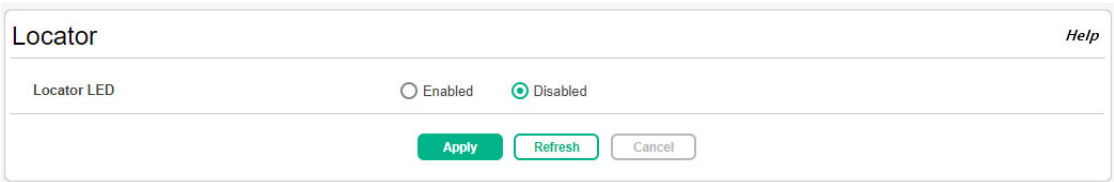
You can click **Save As** to save the Support File page content. The Support File page is saved as HTML and is named support_file.html by default.

Locator

When you need to physically locate the switch, you can use this page to activate a blinking LED on the switch. When enabled, the LED blinks for 30 minutes before being automatically turned off by switch software. You can also use this page to disable the LED if the switch has been located.

To display the Locator page, click **Diagnostics > Locator** in the navigation pane.

Figure 157. Locator Page



Select **Enabled** and click **Apply** to cause the Locator LED on the switch to blink for 30 minutes. The Locator System LED in the Device View is illuminated and blinks orange while this feature is active. This feature is disabled by default (see “[System LEDs](#)” on page 16).

Note that this setting is not stored with the system configuration, so clearing the configuration will not change this value. If the switch reboots, this value is reset to **Disabled**.

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.



IMPORTANT:

The address table supports up to 16K MAC address entries; however, the UI will display up to 500 entries. If the MAC address you want to view is not displayed, you can search for it by using the Filter option. You can enter a partial MAC address to view the first 500 addresses that match your entry.

To display the MAC Table page, click **Diagnostics > MAC Table** in the navigation pane.

Figure 158. MAC Table Page

MAC Table
Help

Maximum Entries Supported 16382

MAC Address Aging Interval (Seconds) (10 to 1000000)

Display rows Showing 1 to 10 of 14 entries Filter:

↕ VLAN ID	↕ MAC Address	↕ Interface	↕ Interface Index	↕ Status
1	00:1B:21:AB:53:E7	9	9	Learned
1	00:1B:21:AB:54:37	9	9	Learned
1	00:40:9D:32:95:0B	9	9	Learned
1	00:FC:E3:90:01:93	9	9	Learned
1	00:FC:E3:90:01:95	9	9	Learned
1	1C:98:EC:7C:8E:40	CPU	53	Management
1	30:8D:99:ED:70:A8	9	9	Learned
1	30:8D:99:ED:70:AA	9	9	Learned
1	30:8D:99:EE:C1:E8	3	3	Learned
1	30:8D:99:EE:C1:EA	3	3	Learned

First Previous 1 2 Next Last

Apply Refresh Cancel

Table 114. MAC Table Fields

Field	Description
Maximum Entries 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.
VLAN ID	The VLAN or VLANs with which the MAC address is associated.
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a six-byte MAC address, with each byte separated by colons.
Interface	The port where this address was learned. The port identified in this field is the port through which the MAC address can be reached. <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.
Status	Provides information about the entry and why it is in the table. Possible values are the following: <ul style="list-style-type: none"> 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. Self—The MAC address belongs to one of the physical interfaces on the switch. Other—The address was added dynamically through an unidentified protocol or method. Unknown—The switch is unable to determine the status of the entry.

14 Maintenance Pages

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 device.

!

IMPORTANT:
If you configure a description for the active and/or backup firmware image, the description will not be cleared if you reset the switch to the factory default settings.

To display the Dual Image Configuration page, click **Maintenance > Dual Image Configuration**.

Figure 159. Dual Image Configuration Page

Dual Image Configuration

Help

Image Status

Image	Version	Description
Active	PH.12.11	<div></div> <div>(0 to 255 characters)</div>
Backup	P12.12.13	<div></div> <div>(0 to 255 characters)</div>

Next Active

☒ Active (PH.12.11)

☐ Backup (P12.12.13)

Apply

Refresh

Cancel

Table 115. Dual Image Configuration Fields

Field	Description
Image Status	This section lists the current image status information.
Image	The type of image, which can be either Active or Backup.
Version	The software version of the image.
Description	Specify an optional description of the image selected.
Next Active	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.

Click **Apply** to save your changes to the switch.

Backup and Update Manager

The File Transfer page enables you to save a backup copy of the switch’s firmware image or configuration file on a local system or network directory and to update files on the switch by transferring newer files from a remote system. This is the page you use to update the switch firmware.

Files can be backed up and updated using HTTP, TFTP, or SFTP.

To display this page, click **Maintenance > Backup and Update Manager** in the navigation pane.

Figure 160. File Transfer Page

File Transfer			Help
Transfer Protocol	Backup Transfer a file from the switch	Update Transfer a file to the switch	
HTTP	⬇	⬆	
TFTP	⬇	⬆	
SFTP	⬇	⬆	

Backing Up Files

To back up a file, click ⬇ in the Backup column in the HTTP, TFTP, or SFTP row. The HTTP Backup File, TFTP Backup File, or SFTP File Upload page displays.

Figure 161. HTTP Backup File Page

HTTP Backup File

File Type

Active Code

Status

Begin Transfer

Close

Figure 162. TFTP Backup File Page

TFTP Backup File

File Type

Active Code

Server Address

File Name

Status

Begin Transfer

Close

Figure 163. SFTP Backup File Page

SFTP File Upload

File Type: Active Code

Server Address: (x.x.x.x)

File Name: (1 to 192 characters)

Username: (1 to 32 characters)

Password: (0 to 64 characters)

Status

Begin Transfer

Close


Configure the following settings:

Table 116. TFTP, HTTP, and SFTP Backup File Fields

Field	Description
File Type	Select the type of file to back up from the switch to a remote system. You can back up the active or backup image, the system configuration file, the backup configuration file, the error log in persistent memory (also referred to as the event log), and the buffered log in RAM.
Server Address	(TFTP/SFTP only) Enter the IP address of the TFTP server.
File Name	(TFTP/SFTP 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 SFTP transfer, if the server requires authentication, specify the user name for remote login to the server that will receive the file.
Password	For SFTP transfer, if the server requires authentication, specify the password for remote login to the server that will receive the file.
Status	Status information on the backup process.

Click **Begin Transfer** begin the backup process. For a TFTP or SFTP backup, the switch begins the transfer to the specified location. For an HTTP backup, browse to the location on your network where you want to save the file.

Updating Files

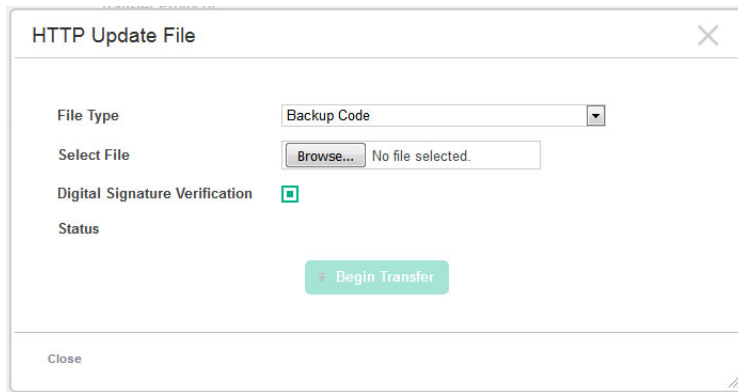
To transfer a file from a remote system to the switch using HTTP, TFTP, or SFTP click  in either row in the **Update** column. The HTTP Update, TFTP Update, or SFTP File Download page appears.

To update a file using HTTP, configure the following information and click **Begin Transfer**.

NOTE:

Firmware upgrades can be performed on the backup code only.

Figure 164. HTTP Update File Page



The screenshot shows a dialog box titled "HTTP Update File" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- File Type:** A dropdown menu currently showing "Backup Code".
- Select File:** A text input field with a "Browse..." button and the text "No file selected."
- Digital Signature Verification:** A checkbox that is currently checked.
- Status:** A section containing a green "Begin Transfer" button.
- Close:** A button in the bottom left corner.

Table 117. HTTP Update File Fields

Field	Description
File Type	<p>Select the type of file to update:</p> <ul style="list-style-type: none"> Backup Code—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. Startup Configuration—Select this option to update the stored configuration file. If the file has errors, the update will be stopped. Backup Configuration—Select this option to update the stored backup configuration file. If the file has errors, the update will be stopped. SSL Trusted Root Certificate PEM File—A PEM-encoded SSL certificate that has been digitally signed by a certificate authority. SSL Server Certificate PEM File—A PEM-encoded SSL certificate that has been signed by another server. SSL DH Weak/Strong Encryption Parameter PEM File—DH certificates provide the algorithms for encrypting key exchanges and are used independent of the certificate. The weak version uses a cipher strength of 512 bits and the strong version uses a cypher strength of 1024 bits. Browser settings determine which DH file parameters are requested at the start of the SSL session. Public Key Image—Select this option to transfer the public key file used for code image validation to the switch.
Select File	<p>Browse to the location on the network where the new file is located and select it.</p> <p>Note: The button in the Select File field varies depending on the browser. For example, it may say Browse or Choose File.</p>
Digital Signature Verification	<p>For the Backup Code, you can select this option to have the switch verify the file download with a digital signature.</p> <p>Digital signature verification is applied to backup code only.</p>
Status	Status information on the update process.

Figure 165. TFTP Update File Page

The screenshot shows a 'TFTP Update File' dialog box. It includes the following elements:

- Title Bar:** 'TFTP Update File' with a close button (X) on the right.
- File Type:** A dropdown menu currently showing 'Backup Code'.
- Server Address:** A text input field with a placeholder '(x.x.x.x)'.
- File Name:** A text input field with a placeholder '(1 to 192 characters)'.
- Digital Signature Verification:** A checkbox that is currently checked.
- Status:** A label for the status of the update process.
- Buttons:** A green 'Begin Transfer' button and a 'Close' button at the bottom left.

Figure 166. SFTP Update File Page

SFTP File Download

File Type

Backup Code

▼

Server Address

(x.x.x.x)

File Name

(1 to 192 characters)

Username

(1 to 32 characters)

Password

(0 to 64 characters)

Digital Signature Verification

☒

Status

Begin Transfer

Close

To update a file using TFTP or SFTP, configure the following information and click **Begin Transfer**.

Table 118. TFTP and SFTP Update File Fields

Field	Description
File Type	See the options in Table 117 on page 219 .
Server Address	Enter the IP address or host name of the TFTP server.
File Name	Enter the path on the server where file is located followed by the filename. The path can be 0 to 160 characters and the file name can be 1 to 32 characters. The path and file name are separated by a slash (/). The file name can have ASCII printable characters, excluding the following: \\, /, :, *, ?, ", <, >,
Username	For SFTP transfer, if the server requires authentication, specify the user name for remote login to the server that will receive the file.
Password	For SFTP transfer, if the server requires authentication, specify the password for remote login to the server that will receive the file.
Digital Signature Verification	For the active and backup code file types, you can select this option to have the switch verify the file download with a digital signature.
Status	Status information on the update process.



CAUTION:

Do not disturb the browser window while the transfer is in progress.

Configuration Files

Use this page to copy the information contained in one configuration file to another configuration file on the device. When you click **Apply**, the copy action takes place immediately, and the source file overwrites the destination file.

To display this page, click **Maintenance > Configuration Files** in the navigation pane.

Figure 167. Copy Configuration Files Page

Copy Configuration Files

Help

Source File

Running Configuration

Destination File

Startup Configuration

Apply

Table 119. Copy Configuration Files 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: <ul style="list-style-type: none">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: <ul style="list-style-type: none">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 **Apply** to initiate the copy action.

A Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
www.hpe.com/support/hpesc

Information to collect

- 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

- 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 download product updates, go to either of the following:
 - Hewlett Packard Enterprise Support Center Get connected with updates page:
www.hpe.com/support/e-updates
 - Software Depot website:
www.hpe.com/support/softwaredepot
- To view and update your entitlements, and to link your contracts, Care Packs, 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



NOTE:IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Websites

Website	Link
Hewlett Packard Enterprise Information Library	www.hpe.com/info/enterprise/docs
Hewlett Packard Enterprise Support Center	www.hpe.com/support/hpesc
Contact Hewlett Packard Enterprise Worldwide	www.hpe.com/assistance
Subscription Service/Support Alerts	www.hpe.com/support/e-updates
Software Depot	www.hpe.com/support/softwaredepot
Customer Self Repair	www.hpe.com/support/selfrepair
Insight Remote Support	www.hpe.com/info/insightremotesupport/docs
Serviceguard Solutions for HP-UX	www.hpe.com/info/hpux-serviceguard-docs
Single Point of Connectivity Knowledge (SPOCK) Storage Compatibility Matrix	www.hpe.com/storage/spock
Storage white papers and analyst reports	www.hpe.com/storage/whitepapers

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

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.

B Warranty information

For important safety, environmental, and regulatory information, see Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at

www.hpe.com/support/Safety-Compliance-EnterpriseProducts.

Warranty information

HPE ProLiant and x86 Servers and Options (<http://www.hpe.com/support/ProLiantServers-Warranties>)

HPE Enterprise Servers (<http://www.hpe.com/support/EnterpriseServers-Warranties>)

HPE Storage Products (<http://www.hpe.com/support/Storage-Warranties>)

HPE Networking Products (<http://www.hpe.com/support/Networking-Warranties>)