

Aruba Instant On 1830 Switch Series Management and Configuration Guide



Published: 2022
Edition: 0.5

Notices

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

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

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

Acknowledgments

IEEE 802.3af[™], IEEE 802.3at[™] are trademarks of the Institute of Electrical and Electronics Engineers. All other trademarks and registered trademarks are owned by their respective owners.

Chapter 1: About This Document	6
Applicable Products.....	6
Latest Version Available Online.....	6
Related Documents.....	6
Supported Features	6
Chapter 2: Getting Started	9
Connecting the Switch to the Network.....	9
Operating System and Browser Support.....	9
Selecting Local Web Management Mode	10
Getting Started With the Web Interface.....	11
Logging On.....	11
GUI Interface Layout and Features.....	11
Common Page Elements	12
Saving Changes.....	13
Switch Panel View.....	13
Port State Indicator	14
Port Information	14
System LEDs	15
Chapter 3: Dashboard	17
Graphical Display	17
System Information	17
System Time	18
Device Information	19
System Resource Usage	19
Device Locator	20
Getting Started Wizard.....	20
Active Users	21
Chapter 4: Setup Network	22
Get Connected.....	22
IPv4 Setup Options	22
HTTP/S Management Settings	23
Management VLAN Settings.....	24
SNMP Settings.....	25
System Time	26
Time Configuration.....	26
Daylight Saving Configuration.....	27

User Management	29
Logged In Sessions	29
User Accounts	30
Adding a User Account	30
Changing User Account Information	32
Removing a User Account	32
Account Security Settings	32
Password Strength Rules	33
Password Keyword Exclusion	34
Schedule Configuration	35
Schedules	36
Adding a Schedule	37
Removing a Schedule	39
Chapter 5: Switching Features	40
Port Configuration	40
Graphical Display	40
Global Configuration	40
Interface Configuration	41
Modifying Interface Settings	43
Interface Statistics	44
Port Mirroring	45
Mirroring Sessions	45
Configuring a Port Mirroring Session	46
Loop Protection	48
Global Configuration	49
Interface Configuration	49
Loop Protection Configuration	50
IGMP Snooping	51
Global Configuration	51
IGMP Snooping VLAN Configuration	52
IGMP Snooping Multicast Router Interface Configuration	56
Configuring Multicast Router Settings on Interfaces	56
Multicast Forwarding Database	57
Interface Auto Recovery	58
Global Configuration	58
Suspended Interfaces	59
Trunk Configuration	60
Graphical Display	61
Global Configuration	61
Trunk Configuration	62
Modifying Trunk Settings	63
EEE Configuration	65
Global Configuration	65
Global Status	66

Interface Status	66
Chapter 6: Spanning Tree	68
Global Configuration	68
Global Settings	69
Spanning Tree Statistics	71
CST Configuration	71
CST Port Configuration	72
Additional Actions on CST Ports	73
Chapter 7: Virtual LAN	77
VLAN Configuration	77
Graphical Display	77
VLAN Configuration	78
VLAN Membership	80
VLAN Membership - By Interface Tab	80
VLAN Membership - By VLAN Tab	81
VLAN Interface Configuration	82
Chapter 8: Neighbor Discovery	84
LLDP	84
LLDP Global Configuration	85
LLDP Global Information	85
Interface Configuration	86
Remote Device Information	89
Local Device Information	90
LLDP Statistics	92
LLDP-MED	93
LLDP-MED Global Configuration	93
LLDP Global Information	94
Interface Configuration	94
Remote Device Information	96
Displaying Remote Device Details	97
Chapter 9: Power over Ethernet	99
PoE Configuration	100
Graphical Display	100
Activity	100
Priority	100
Class	100
Status	101
Consumption History	102
Port Configuration	102
Edit Port PoE Configuration	104
PoE Port Details	105
Chapter 10: Quality of Service (QoS)	108

Class of Service	108
802.1p Priority Mapping	108
Configuring 802.1p CoS Mapping	109
Interface CoS Configuration	109
Configuring the CoS on an Interface.....	110
Chapter 11: Security	111
Overview	111
Denial of Service Protection	111
Global Settings.....	112
SYN Attack Status Tab	113
Interface Settings Tab	113
HTTPS Certificate	115
HTTPS Certificate Settings	115
Generate a Self-Signed Certificate	116
Using a Certificate Signed by a Certificate Authority	118
View a Certificate	119
Chapter 12: Diagnostics	121
Unexpected Restart Information	121
Global Log Settings.....	121
Remote Log Server	122
Buffered Log.....	124
Log File	125
Ping	126
Ping Settings	126
Ping Results	128
Support File	128
Cable Test	130
Interface Configuration	131
MAC Table	132
MAC Address Table	132
Chapter 13: Maintenance	134
Backup and Update Files	135
Secure Copy Protocol (SCP) Usage	135
Configuration File Operations	137
Reset	138
Reboot Device.....	138
Reset to Factory Defaults.....	139
Chapter 14: Support	141
Websites	141
Accessing Aruba Support	141
Accessing Updates	141
Warranty Information	142

Regulatory Information	142
Additional Regulatory Information	142
Documentation Feedback	143

The Aruba Instant On 1830 Switch Series are designed to meet the needs of small business network environments — simple to set up and manage and are secure and reliable. Aruba Instant On deployments can be managed through a mobile application supported on iOS and Android, through a cloud portal that is accessible through a web browser, or using a local web GUI. This manual details using the web GUI to manage the switch.

Applicable Products

This guide applies to these products:

- Aruba Instant On 1830 8G Switch
- Aruba Instant On 1830 8G 4p Class4 PoE 65W Switch
- Aruba Instant On 1830 24G 2SFP Switch
- Aruba Instant On 1830 24G 12p Class4 PoE 2SFP 195W Switch
- Aruba Instant On 1830 48G 4SFP Switch
- Aruba Instant On 1830 48G 24p Class4 PoE 4SFP 370W Switch

Latest Version Available Online

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

<https://community.arubainstanton.com>

Related Documents

- *Aruba Instant On 1830 Installation and Getting Started Guide*
- *START HERE: Installation, Safety, and Regulatory Information for the Aruba Instant On 1830 Switches*
- *Aruba Instant On User Guide*

Supported Features

Aruba Instant On 1830 Switch Series switches include support for the following:

- IEEE 802.3 10BASE-T
- IEEE 802.3u 100BASE-TX
- IEEE 802.3ab 1000BASE-T
- Cable Test
- HTTP and HTTPS sessions (5 sessions total)
- 16,384 MAC entries
- IEEE 802.2af: Power over Ethernet
- IEEE 802.3at
- IEEE 802.3x: Flow control
- IEEE 802.1Q: VLANs - up to 256. VLANs 4094 and 4093 reserved for internal usage (available VLAN ID 1-4092)
- IEEE 802.1p
- IEEE 802.1D: Spanning Tree Protocol
- IEEE 802.1W: Rapid Spanning Tree Protocol
- IEEE 802.1AB: Link Layer Discovery Protocol (LLDP and LLDP-MED)
- Trunk (LAG) support
 - o LAGs
 - 8 port units: up to 4 LAGS - up to 4 active port members in each
 - 24 port units: up to 8 LAGS - up to 8 active port members in each
 - 48 port units: up to 16 LAGS - up to 8 active port members in each
 - o IEEE 802.3ad: Link aggregation (LACP). The number of LACP candidate ports is twice the number of supported active port members in the LAG.
 - o Static Trunks
- Jumbo packet support
- Auto-MDI/MDIX
- Storm Control (global)
- Ingress Rate Limiting (per port)
- Port Mirroring
- IGMP Snooping v1/v2
- Global time scheduler (3 schedules)
 - o PoE
 - o Port shutdown
- Static IP address assignment
- DHCP client
- DHCP fallback
- User Accounts (up to 5, Read/write, Read only)
- Password management (aging, lockout, strength check, key word exclusion)
- SNMPv1
- DoS Protection
- SNTP (RFC 2030)
- Loop Protection
- IEEE 802.3az: Energy Efficient Ethernet
- 802.1p priority to queue mapping (DSCP has set values)

- Number of egress queues (traffic priority) – 4
- Ping (IPv4)
- Dual image support
- Firmware Update over HTTP, HTTPS, TFTP, SCP
- Config File backup / restore
- Syslog Log (local & remote)
 - o 1 remote syslog server
 - o Up to 1000 entries on Buffered log
 - o Up to 200 in Log file (Flash)

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

Connecting the Switch to the Network

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



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

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

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

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

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

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

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

Operating System and Browser Support

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

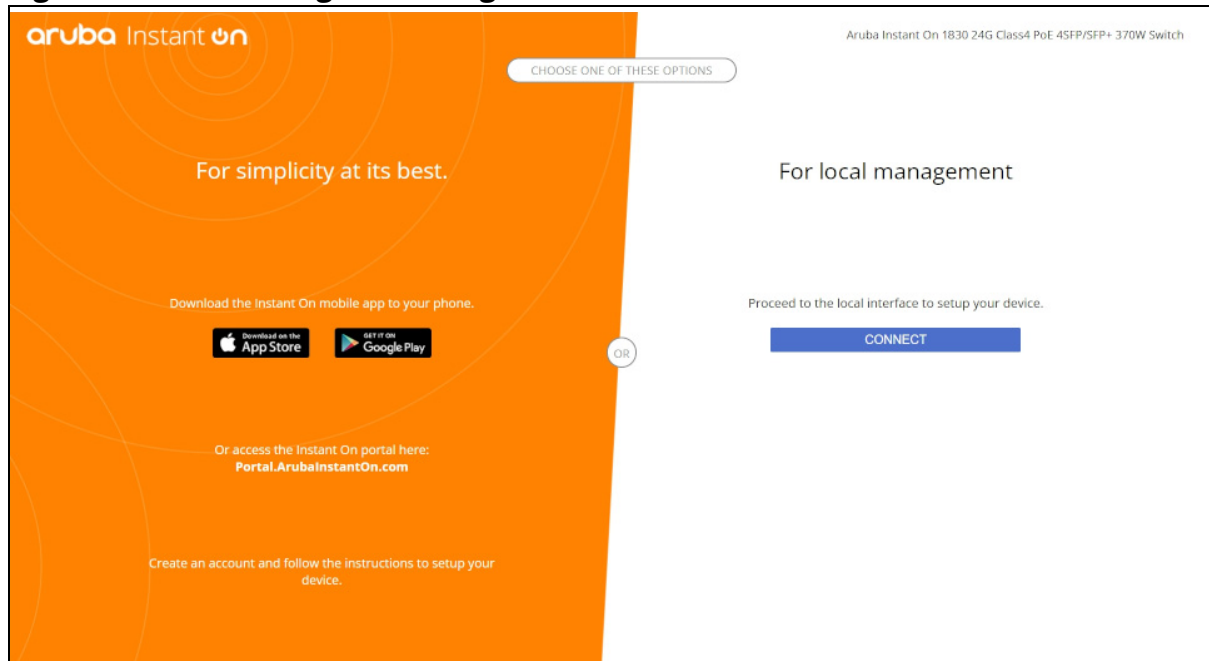
Table 1. Operating System and Browser Support

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

Selecting Local Web Management Mode

Upon first connecting directly to the switch, you are presented with a welcome page indicating the choice to manage the switch locally using the web interface (detailed in this guide). In addition the welcome page outlines instructions to create and configure a portal account. Simply follow the instructions provided in the links to create, activate and connect your switch to the cloud portal.

Figure 1. Selecting the Management Mode



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

Select CONNECT to manage the switch locally using the web interface and continue on in this guide. If you would rather use the Aruba Instant On Cloud Portal to manage the switch, see the *Aruba Instant On 1830 Switch Series Installation and Getting Started Guide* and the *Aruba Instant On User Guide*.

Getting Started With the Web Interface

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

Logging On

Follow these steps to log on through the web interface:

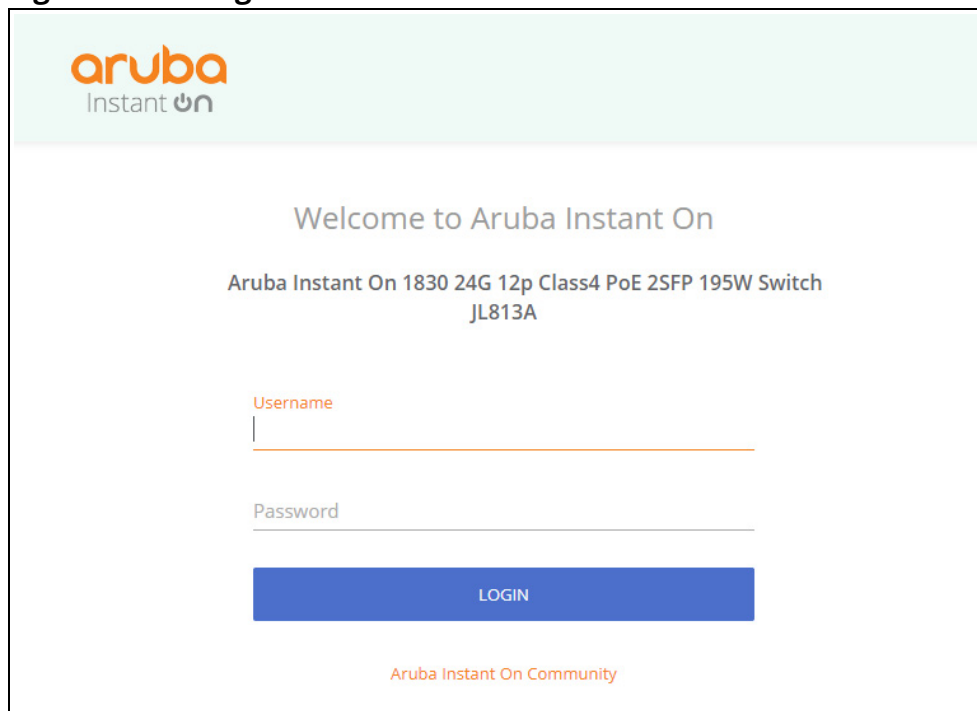
1. Open a web browser and enter the IP address of the switch in the web browser address field.
2. On the Login screen, enter the username and password (if one has been set), and then click **Log In**.

By default, the username is **admin** and there is no password. After the initial log on, the administrator is prompted to configure a password.



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

Figure 2. Login Screen



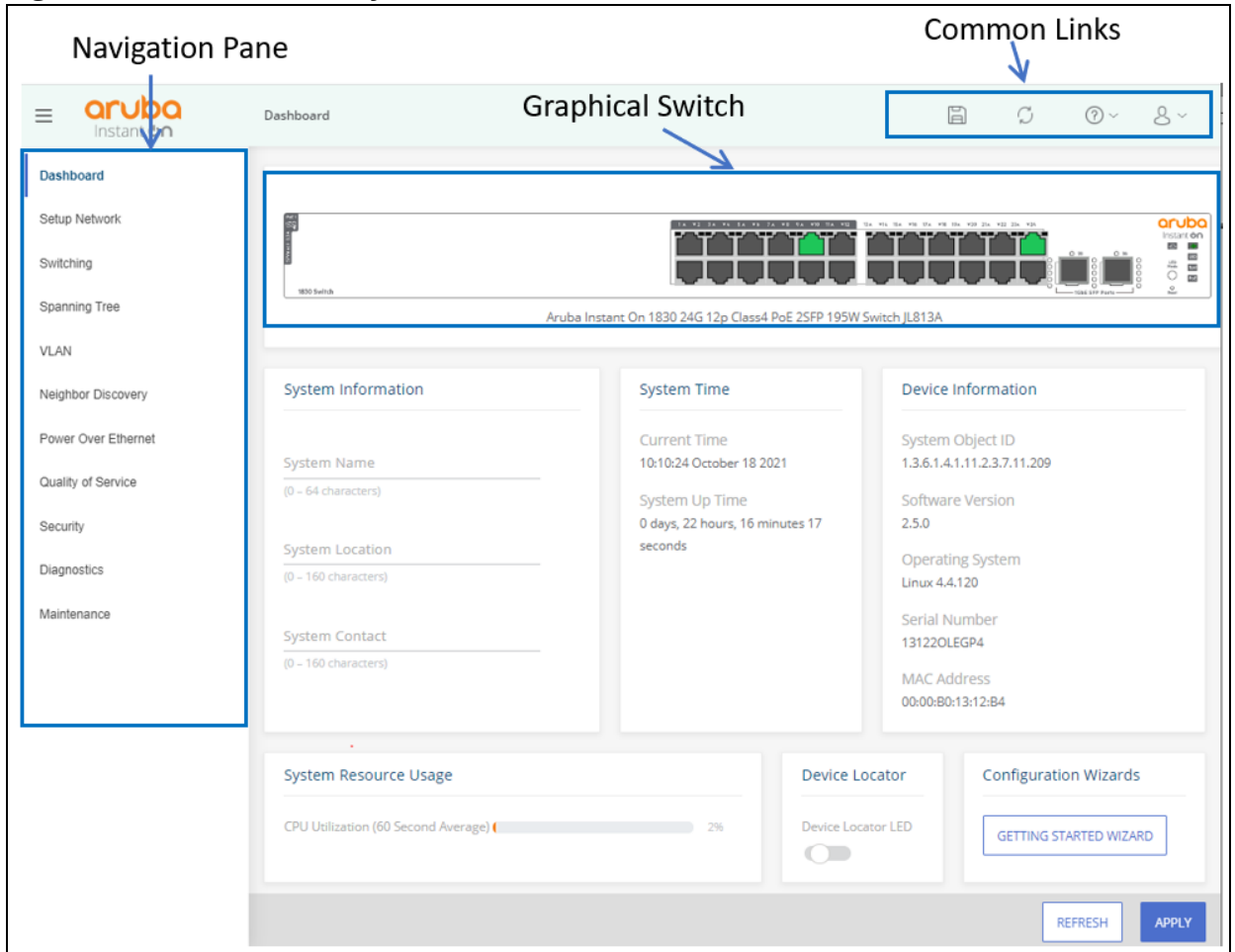
GUI Interface Layout and Features

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

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

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

Figure 3. Interface Layout and Features

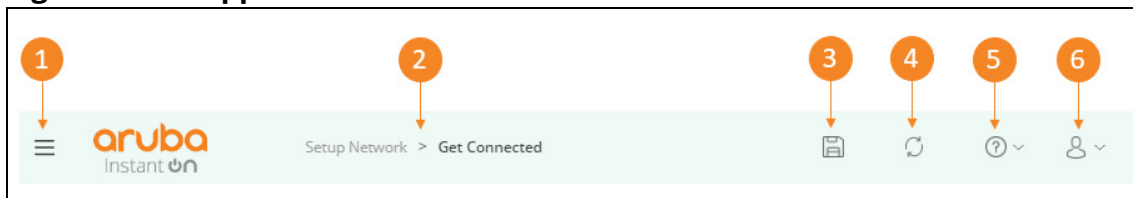


Click on any topic in the navigation pane to display related configuration options.

Common Page Elements






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

Figure 4. Upper Panel




Use the buttons to do the following:



Table 2. Upper Panel Components

Label	Description
1	Click Show Navigation  to toggle the navigation pane that shows all the screens that are available for the switch.
2	This shows the current screen.
3	Click Save Configuration  to save the current configuration. This icon appears only when there are unsaved changes.
4	Click Refresh  to refresh the screen.
5	Click Help  on any page to display a help panel that explains the fields and configuration options on the page.
6	Click Profile  to view your profile information, or to log out.





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

The bottom of the screen includes the following buttons:

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

Saving Changes

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

Switch Panel View

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

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

Figure 5. Switch Panel View

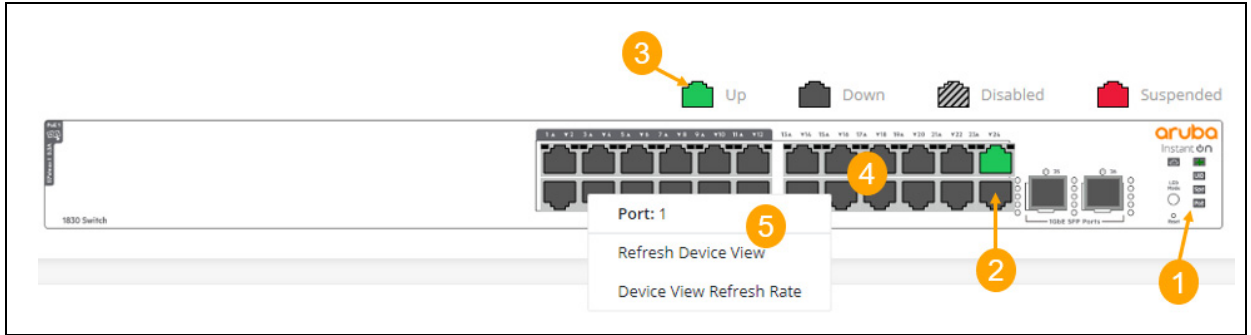


Table 3. Switch Panel Components

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

Port State Indicator

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

Table 4. Port State Indicators

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

Port Information

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

- Port name. If the port is a trunk member, the trunk ID of the trunk is appended to the port name (for example: Port: 30 (TRK 7))
- Description. The description of the port, or the trunk if the port is a trunk member.
- The link status. Up, Down, Disabled, or Suspended. If the port is a trunk member, the status should be that of the trunk.

- Speed. The current speed of the port This field is only displayed for ports or trunks that are up. If the port is a trunk member, the speed is that of the trunk.

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

System LEDs

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





Figure 6. System LED Indicators



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

Table 5. System LED Indicators

Indicator	Color	Image	Description
Power	Green/ Orange		<ul style="list-style-type: none"> • On (green)—The switch is receiving power. This is an indication of normal operating condition. • Off—The switch is powered off or is NOT receiving power. • Slow flash (orange) <ul style="list-style-type: none"> • Self-test and initialization is in progress (boot-up). • A fault or self-test failure has occurred on the switch, one of the switch ports, the PSU, or the fan. The Status LED for the component with the fault will blink simultaneously.
UID (Locator)	Blue		<ul style="list-style-type: none"> • Blinking slowly—The locator function has been enabled to help physically locate the standalone unit. • Off—Locator function was not activated by user, or if activated – function was manually disabled by user, or the Locator function timer has expired.
Speed Mode	Green		<ul style="list-style-type: none"> • On—Speed Mode has been selected and port LEDs are used to indicate port speed information. • Off—Speed Mode is not selected.
PoE Mode	Green/ Orange		<ul style="list-style-type: none"> • On solid green - PoE Mode has been selected and port LEDs are used to indicate PoE information. • On solid orange - PoE Mode is selected, and a port has an internal PoE hardware failure. The specific port LED with fault also flashes in this case. • Slow flash orange - PoE Mode has NOT been selected, but a port has an internal PoE hardware failure. • NOTE: In this case, the specific Port LED will NOT flash. • LED is off - PoE mode is not selected, and there are no PoE hardware failures on ports.

Indicator	Color	Image	Description
Cloud LED	green/ orange		<p>Indicates the Cloud status of the switch:</p> <ul style="list-style-type: none"> • Slow flash green—the switch is in the process of establishing a connection, to the cloud portal. • On green—the switch has successfully completed the "onboarding process/procedure" and is fully operational, in cloud managed mode (connected to cloud portal). • On orange—The switch has detected an error/fault, and cannot connect to the cloud portal NOTE - the Global Status LED does not flash. • Alternating between green/orange—the switch is connected to the cloud portal, and ready for setup, through the App/Portal This is a temporary state, which occurs while the switch is connected to the cloud portal, but not fully on-boarded yet.
LED Mode		 	<p>This button determines the Port LED indication. Press this button to change to a different mode. The supported modes are:</p> <ul style="list-style-type: none"> • Link/activity - this is the default mode of device operation. There is no indication for this mode (speed and PoE Mode LEDs are off). The LED Mode will switch back to the link/activity state 10 minutes after selecting a non-default mode (speed or PoE) • Speed • PoE (for units that support PoE) <p>The speed and PoE LED modes have specific global LED indicating the selected mode.</p>
Reset button			<p>Reset the system. Press and release to reset the switch. Press and hold for 5 seconds or longer, to reset the switch to factory defaults.</p>

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

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

The page also supports the following configuration wizard:

- Getting started Wizard

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

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

Graphical Display

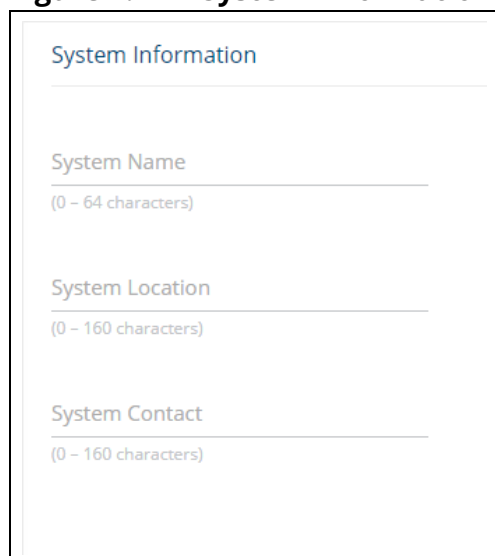
The top of the Dashboard page shows a graphical representation of the switch front panel. This panel view has a display of the ports, each with its current status.

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

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

System Information

Figure 7. System Information Tile



The image shows a screenshot of a 'System Information' tile. The tile has a title 'System Information' at the top. Below the title, there are three input fields, each with a label and a character limit:

- System Name**: (0 - 64 characters)
- System Location**: (0 - 160 characters)
- System Contact**: (0 - 160 characters)

Table 6. System Information Fields

Field	Description
System Name	Enter the preferred name to identify this switch. A maximum of 63 alpha-numeric, case-sensitive characters is allowed. The system name must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. The user-configurable switch name will appear in the login screen banner.
System Location	Enter the location of this switch. A maximum of 160 alpha-numeric, case-sensitive characters is allowed, including special characters (!, ", #, \$, %, &, ', (,), *, +, ,, -, ., /, :, ;, <, =, >, ?, @, [,], \, ^, _ ` {, }, ~, and space). This field is blank by default.
System Contact	Enter the name of the contact person for this switch. A maximum of 160 alpha-numeric, case-sensitive characters is allowed, including special characters (!, ", #, \$, %, &, ', (,), *, +, ,, -, ., /, :, ;, <, =, >, ?, @, [,], \, ^, _ ` {, }, ~, and space). This field is blank by default.

System Time

Figure 8. System Time Tile

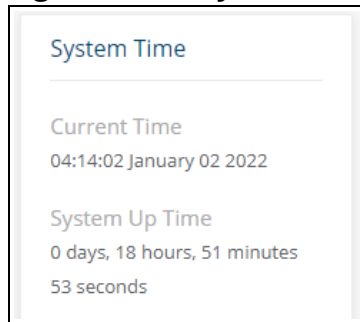


Figure 9. System Time Fields

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

Device Information

Figure 10. Device information Tile



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

Table 7. Device Information Fields

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

System Resource Usage

Figure 11. System Resource Usage Tile

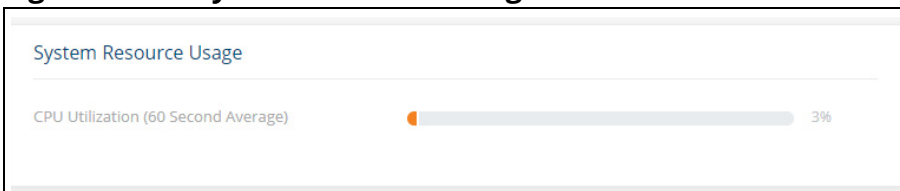


Table 8. System Resource Usage Fields

Field	Description
CPU Utilization	The percentage of CPU utilization for the entire system averaged over the past 60 seconds.

Device Locator

Figure 12. Device Locator Tile

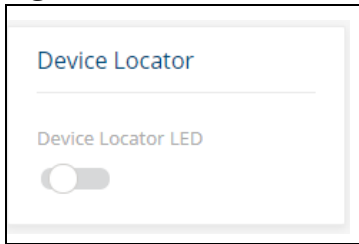


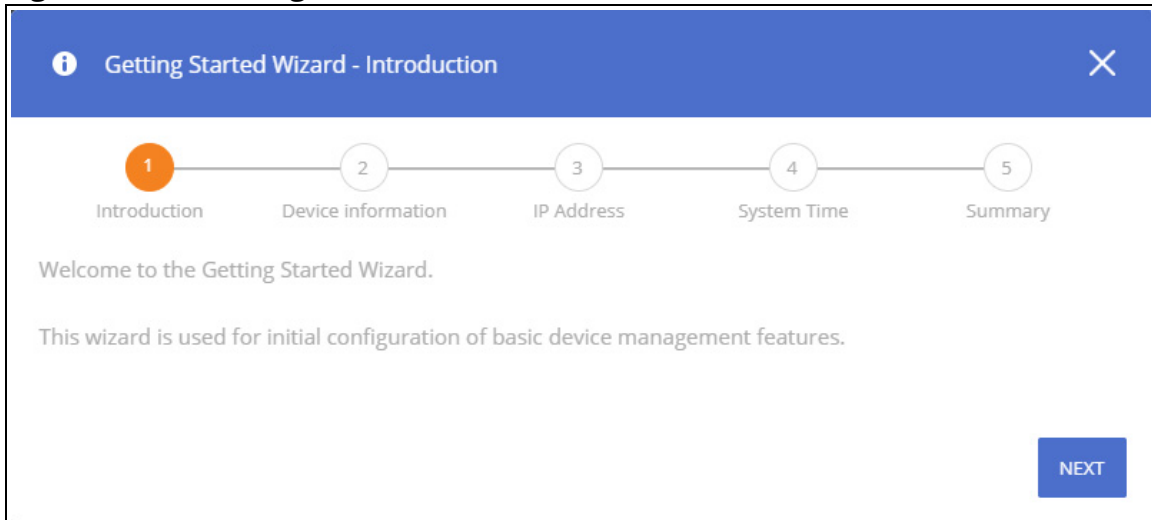
Table 9. Device Locator Field

Field	Description
Device Locator LED	Enable this feature to start flashing the physical device locator LED for 30 minutes.

Getting Started Wizard

Click the **GETTING STARTED WIZARD** button to open the Getting Started Wizard that walks you through the stages of initial configuration of the basic management features of the Aruba Instant On 1830 Switch Series.

Figure 13. Getting Started Wizard



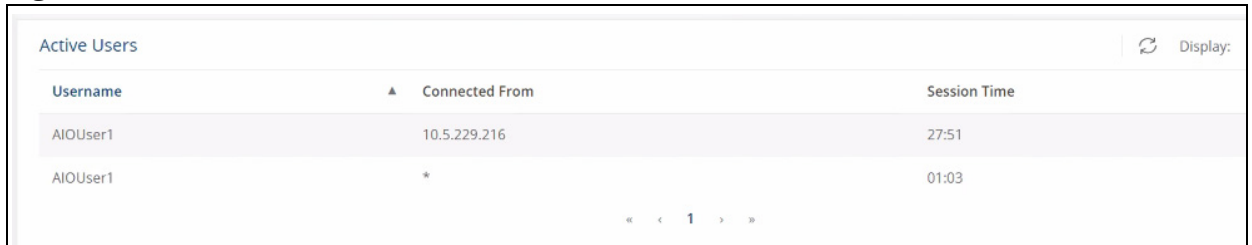
These are the steps that the wizard takes you through.

- Step 1 - Introduction screen. Click the NEXT button to proceed with the configuration wizard.
- Step 2 - Device Information, enter a System Name, System Location and System Contact information to help identify the device.
Click **NEXT** to go to the next screen in the configuration wizard.
- Step 3 - IP Address. Set up the IP interface. For more information on the fields in this screen, see [IPv4 Setup Fields](#).
Click **NEXT** to go to the next screen in the configuration wizard.
- Step 4 - System Time. Set up the device clock. For more information on the fields in this screen, see [Time Configuration Fields](#).
Click **NEXT** to go to the next screen in the configuration wizard.
- Step 5 - Summary. This screen details the changes that were configured. Click APPLY to apply the changes to the next session.
Click **CLOSE** to close the wizard.

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

Active Users

Figure 14. Active Users Tile



Username	Connected From	Session Time
AIOUser1	10.5.229.216	27:51
AIOUser1	*	01:03



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

Table 10. Active Users Fields

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

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

Get Connected

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

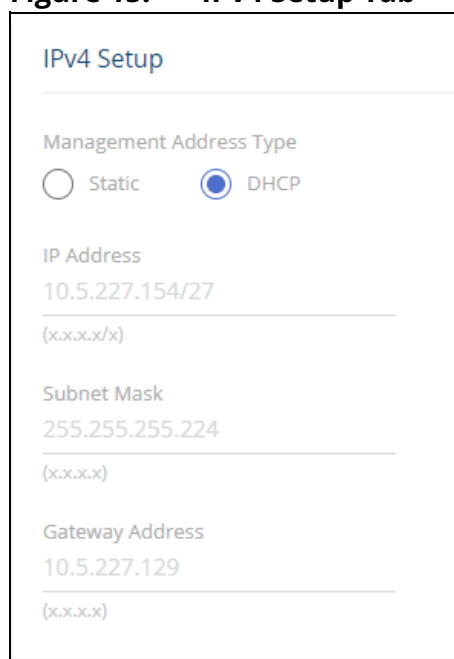
To display the Get Connected page, click **Setup Network > Get Connected**.

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

IPv4 Setup Options

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

Figure 15. IPv4 Setup Tab



IPv4 Setup

Management Address Type

Static DHCP

IP Address

10.5.227.154/27

(x.x.x.x/x)

Subnet Mask

255.255.255.224

(x.x.x.x)

Gateway Address

10.5.227.129

(x.x.x.x)



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

Table 11. IPv4 Setup Fields

Field	Description
Management Address Type	Select the type of network connection: <ul style="list-style-type: none">• Static—Select this option to configure the IP address, subnet mask, and gateway fields for data entry.• DHCP—Select this option to configure the switch to obtain IP information from a DHCP server on the network. If the DHCP server responds, then the assigned IP address is used. If DHCP is enabled but the DHCP server does not respond, the default static IP address 192.168.1.1 is used. DHCP operation is enabled by default. When a DHCP server assigns an IP address to the switch, it specifies the time for which the assignment is valid. Only a user-configured static IP address is saved to flash. CAUTION: Changing the protocol type or IP address discontinues the current connection; you can log on again using the new IP address information.
IP Address	The IPv4 address for the switch. If the Protocol Type is set to DHCP, this field displays the IP address assigned by the DHCP server. If the Protocol Type is set to Static, the IP address can be manually configured in this field. The default IP address is 192.168.1.1. Note: A broadcast, multicast, or network IP address cannot not be entered in this field.
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.

HTTP/S Management Settings

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

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

Figure 16. HTTP/S Management Settings Tabs

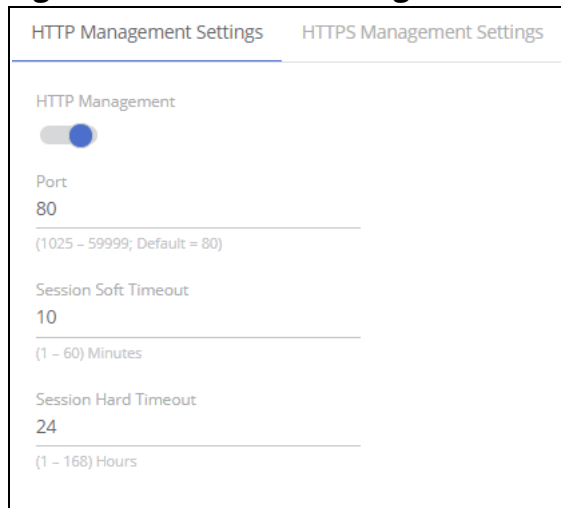
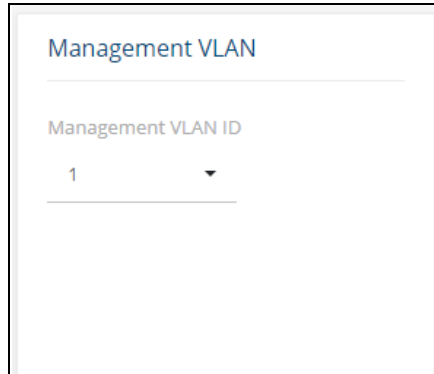


Table 12. HTTP/S Management Settings Fields

Field	Description
HTTP/S Management	Enables or disables the HTTP or HTTPS administrative mode. When enabled, the switch can be accessed through a web browser using the HTTP/S protocol. By default HTTP/s management is enabled.
Port	The TCP port number on which the HTTP/S server listens for requests. Existing HTTP/S login sessions are closed whenever this value is changed. All new HTTP sessions must use the new port number. Note: Before changing this value, check your system to make sure the desired port number is not currently being used by any other service. For HTTP the default is 80, for HTTPS the default is 443. The valid range for this port number is 1025-59999.
Session Soft Timeout	Session inactivity timeout value, in minutes. A logged-in user that does not exhibit any HTTP/S activity for this amount of time is automatically logged out of the HTTP/S session. By default, the timeout is 10 minutes. The valid range is 1-60.
Session Hard Timeout	Session hard timeout value, in hours. A user connected to the switch through an HTTP/S session is automatically logged out after this amount of time regardless of the amount of HTTP/S activity that occurs. By default, the timeout is 24 hours. The valid range is 1-168.

Management VLAN Settings

Figure 17. Management VLAN Tile



The figure shows a configuration tile for Management VLAN. It has a title "Management VLAN" and a label "Management VLAN ID" above a dropdown menu. The dropdown menu currently displays the value "1".

Table 13. Management VLAN Fields

Field	Description
Management VLAN ID	<p>The Management IP address configured on this tile is applied to the Management VLAN.</p> <p>By default, the management VLAN ID is 1. The management VLAN can be any value between 1 and 4092. All ports are members of VLAN 1 by default; the administrator may want to create a different VLAN to assign as the management VLAN. In this case, the IP address is applied to the other VLAN configured by the user.</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>

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

SNMP Settings

Figure 18. SNMP Settings Tile

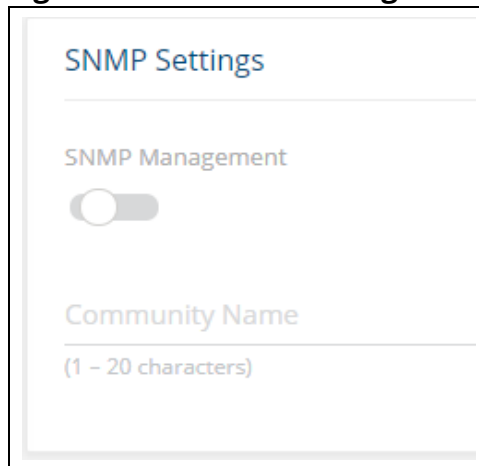


Table 14. SNMP Settings Fields

Field	Description
SNMP Management	Activate to set SNMP management, V1 protocol.
Community Name	When SNMP management is active, you can enter a name for the community.

System Time

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

Time Configuration

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

Figure 19. Time Configuration Tile

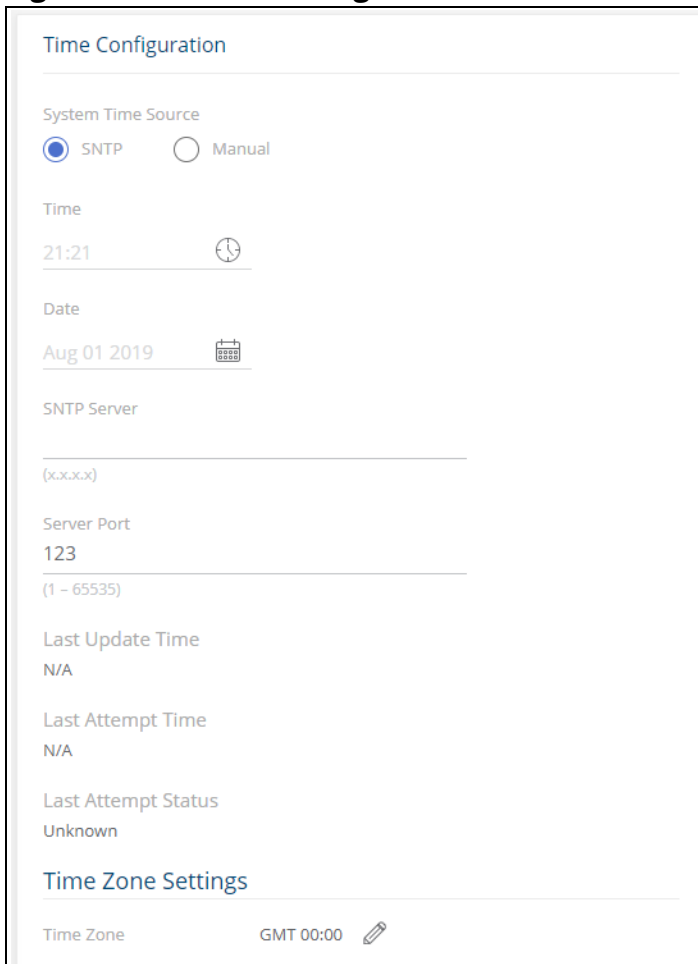



Table 15. Time Configuration Fields

Field	Description
System Time Source	Select SNTP (Simple Network Time Protocol) to configure the switch to acquire its time settings from an SNTP server. When selected, only the SNTP Configuration fields are available for configuration. Select Manual to disable SNTP and configure the time manually. You can manually set the date and time in the fields mentioned below.
Time	The current time. This value is determined by an SNTP server. When SNTP is disabled, the system time increments from the active image creation time stamp. You can also configure the time manually.
Date	The current date. This value is determined by an SNTP server. When SNTP is disabled, the system time increments the active image creation time stamp.
SNTP 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.
Last Attempt 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"> • Unknown — None of the following values apply or no message has been received. • Up—The SNTP operation was successful and the system time was updated. • Request Timed Out—A SNTP request timed out without receiving a response from the SNTP server. • Down—Connection not established with SNTP server. • In Process—currently establishing connection with SNTP server.
Time Zone Settings	
Time Zone	The currently set time zone. To edit, click the Edit button  The default is (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London.
Acronym	The acronym for the time zone, if one is configured on the system (for example, PST, EDT).

Daylight Saving Configuration

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

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

Figure 20. Daylight Saving Configuration Tile

Daylight Saving Configuration

Daylight Saving Time

Recurring ▼

Non Recurring Range

Start Date

Jul 28 2019

Starting Time of Day

End Date

Ending Time of Day

Recurring Range

Start Week

Last ▼

Start Day

Sunday ▼

Start Month

Table 16. Daylight Saving 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. • EU—The system clock uses the standard recurring daylight saving time settings used in countries in the European Union. • USA—The system clock uses the standard recurring daylight saving time settings used in the United States. • Recurring—The settings will be in effect for the upcoming period and subsequent years. • Non-Recurring—The settings will be in effect only for a specified period during the year (that is, they will not carry forward to subsequent years). <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>

Field	Description
Non Recurring 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 Date—Use the calendar to set the day, month, and year when the change to DST occurs. • Starting Time of Day—Set the hour and minutes when the change to DST occurs. Or, enter the hours and minutes in 24-hour format (HH:MM). • End Date—Use the calendar to set the day, month, and year when the change from DST occurs. • Ending Time of Day—Set the hour and minutes when the change from DST occurs. Or, enter the hours and minutes in 24-hour format (HH:MM).
Recurring Range	<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. Changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

User Management

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

Click **Setup Network > User Management** to add switch management users, change user settings, or remove users.

Logged In Sessions

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

Figure 21. Logged In Sessions Tile

Username	Connected From	Session Time	Session Type
guest	10.4.82.2	39:07	HTTP

Table 17. Logged In Sessions Fields

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

User Accounts

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

Figure 22. User Accounts Tile

User Accounts								
<input type="checkbox"/>	Username	▲ Access Level	Lockout Status	Password Expiration				
<input type="checkbox"/>	admin	Read/Write	False	N/A				

Table 18. User Accounts Fields

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

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

Adding a User Account

To add a new user account, from the User Accounts tile, click the **Add Entry** button and configure the settings.

Figure 23. Add New User Dialog Box

The dialog box is titled "Add New User" and contains the following fields and options:

- Username:** A text input field with a character limit of 1 to 20 characters.
- Password Configuration Method:** Two radio buttons: "Regular" (selected) and "Encrypted".
- Password:** A text input field with a character limit of 8 to 64 characters.
- Confirm:** A text input field with a character limit of 8 to 64 characters.
- Access Level:** Two radio buttons: "Read Only" (selected) and "Read/Write".

Buttons at the bottom right: CANCEL and APPLY.

Configure the settings for the new user.

Table 19. New User Configuration Fields

Field	Description
Username	Enter the name you want to give to the new account. (You can only enter data in this field when you are creating a new account.) Usernames are up to 20 alphanumeric characters in length and are not case sensitive. Valid characters include all the alphanumeric characters and the dash ('-') and underscore ('_') characters. Username <i>default</i> is not valid.
Password Configuration Method	Specify Regular for unencrypted passwords, or Encrypted to enter a password that is already encrypted. This option is usually used when the password is copied from an existing configuration file.
Password	Enter the password for the account. It will not display as it is typed, only asterisks (*) or dots (.) will show, based on the browser used. By default, passwords must be greater than eight characters and can be up to 64 characters in length, and are case sensitive.
Confirm	Enter the password again, to confirm that you entered it correctly. This field will not display, but will show asterisks (*) or dots (.), based on the browser you use.
Access Level	Indicates the access or privilege level for this user. The options are: <ul style="list-style-type: none">• Read Only - The user can view the configuration but cannot modify any fields.• Read/Write - The user can view and modify the configuration.

Click **APPLY**.

Changing User Account Information


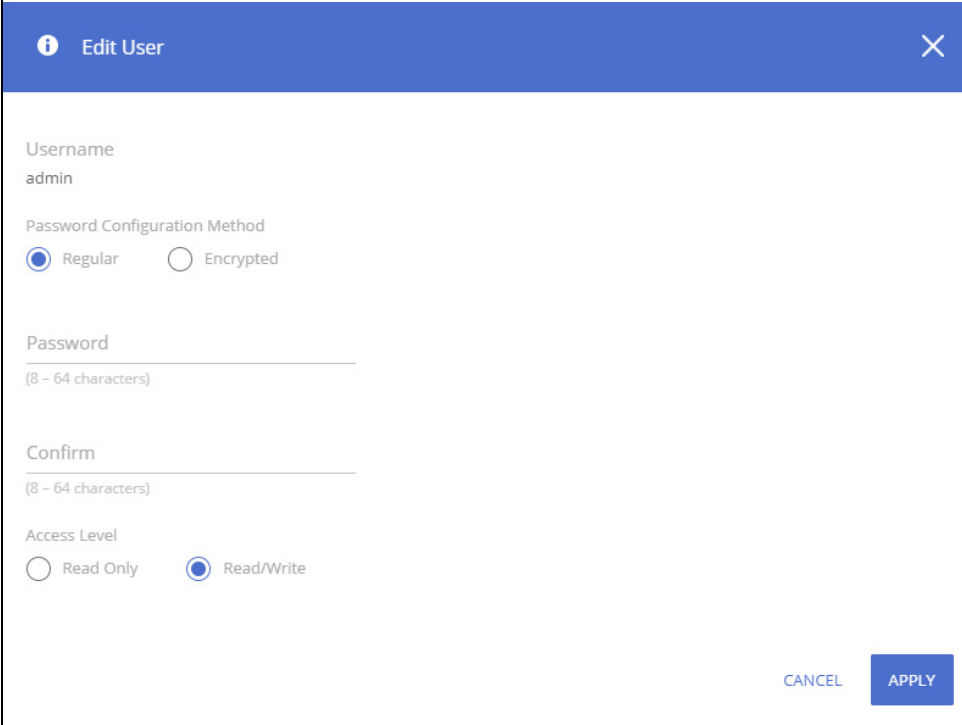
You cannot change the name of an existing user, but you can change the password, privilege, and password settings. To change user information, select the username with the information to change and click the **Edit** button . Update the fields as needed, and click **APPLY**.

Figure 24. Edit Existing User Dialog Box



Edit User

Username
admin

Password Configuration Method
 Regular Encrypted


Password
(8 - 64 characters)

Confirm
(8 - 64 characters)

Access Level
 Read Only Read/Write

CANCEL APPLY

Removing a User Account

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

Account Security Settings

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

Figure 25. Account Security Settings Tile

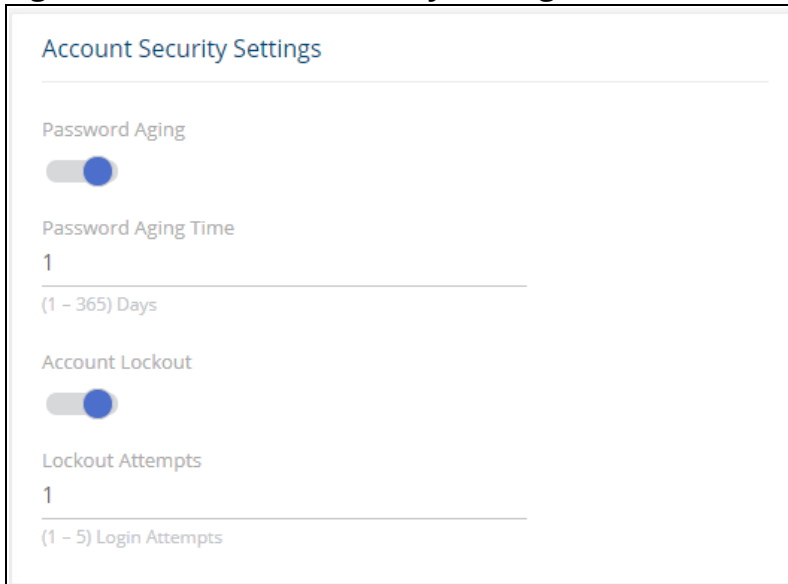


Table 20. Account Security Settings Fields

Field	Description
Password Aging	Activate this to enable setting a maximum age for a user password. Users will need to change their password before the maximum age.
Password Aging Time	Set the amount of days that the password can be used before it is changed to a new password.
Account Lockout	Activate this to enable setting a maximum number of password attempts before the account is locked.
Lockout Attempts	After a user fails to log in this number of times, the user is locked out until the password is reset by the administrator.

Password Strength Rules

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

Figure 26. Password Strength Rules Tile

Password Strength Rules

Password Strength Enforcement

Minimum Length

8

(0 - 64 characters)

Character Repetition Enforcement

Maximum Number of Repeated Characters

1

(1 - 16)

Minimum Character Classes

0

(0 - 4)

Table 21. Password Strength Rules Fields

Field	Description
Password Strength Enforcement	Enable or disable the password strength check feature. Enabling this feature forces the user to configure passwords that comply with the strong password configuration specified in the following fields.
Minimum Length	Passwords must have at least this many characters (0 to 64).
Character Repetition Enforcement	Enable or disable the character repetition enforcement feature. Enabling this feature limits the number of repeated characters allowed in the password.
Maximum Number of Repeated Characters	Specify the maximum number of repeated characters a password is allowed to include. An example of four repeated characters is <i>aaaa</i> .
Minimum Character Classes	Specify the minimum number of character classes a password must contain. There are four character classes: <ul style="list-style-type: none">• Uppercase• Lowercase• Numbers• Special Characters

Password Keyword Exclusion

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

Figure 27. Password Exclusion Tile

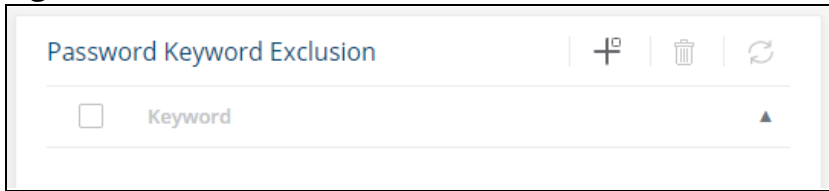


Table 22. Password Exclusion Field

Field	Description
Keyword	<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 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**.

Schedule Configuration

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

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

- PoE - to set the time ranges when PoE power is provided.
- Port Admin status - to set the time ranges when the port is operationally enabled.

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

Schedules

Figure 28. Schedules Tile

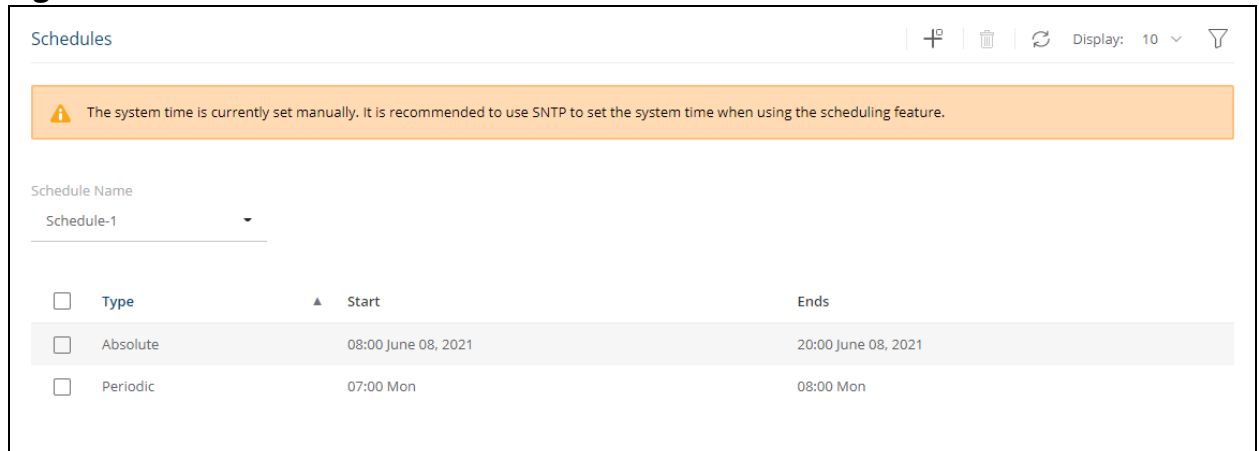



Table 23. Schedule Fields

Field	Description
Schedule Name	Select the schedule to view from the drop-down list to display information on time periods configured for the schedule, if any.
Type	The type of time period entry, which is one of the following: <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.Periodic—A recurring entry that takes place at fixed intervals. This type of entry occurs at the same time on one or more days of the week.
Start	For an absolute entry, this field indicates the time, day, month, and year that the entry begins. If this field is blank, the absolute entry became active when it was configured. For a periodic entry, this field indicates the time and day(s) of the week that the entry begins.
Ends	For an absolute entry, indicates the time, day, month, and year that the entry ends. If this field is blank, the absolute entry does not have a defined end. For a periodic entry, this field indicates the time and day(s) of the week that the entry ends.

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



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

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

Adding a Schedule


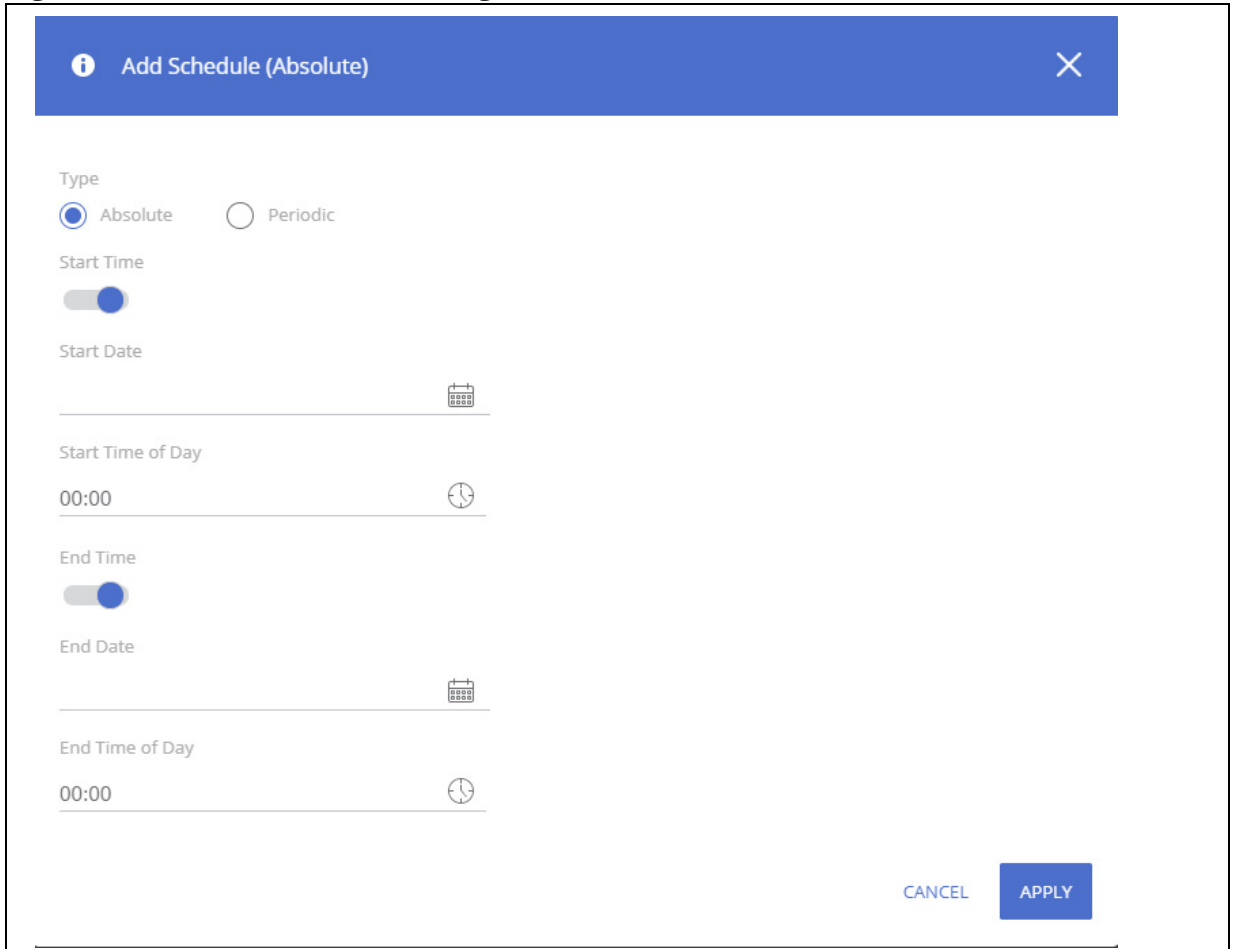
To add a schedule, from the Schedules tile, click the **Add Entry** button  and configure the settings.


Figure 29. Add Schedule Dialog Box - Absolute Schedule




Add Schedule (Absolute)


Type
 Absolute Periodic


Start Time

Start Date


Start Time of Day
00:00 

End Time

End Date


End Time of Day
00:00 

CANCEL APPLY


Figure 30. Add Schedule Dialog Box - Periodic Schedule

Table 24. New Schedule Configuration Fields

Field	Description
Type	The type of schedule. Can be one of the following: <ul style="list-style-type: none"> • Absolute. There can one absolute schedule in each schedule. The absolute schedule does not repeat. • Periodic. Each schedule can have multiple periodic schedules. A periodic schedule occurs at the same time every day or on one or more days of the week.
Absolute Schedule Fields	
Start Time	Enable the Start Time setting to apply the schedule Start Date. If the Start Time is disabled, the schedule Start Date will be active at the time of configuration.
Start Date	Select the start date from the calendar.
Start Time of Day	Set the time of day to start the schedule.
End Time	Activate this field to enable setting the End point of the schedule. If End Time is not activated, the schedule continues indefinitely.
End Date	Select the end date from the calendar.
End Time of Day	Set the time of day to end the schedule.

Field	Description
Periodic Schedule Fields	
Start Day	Select the day of the week to start the schedule, from the drop-down list.
Start Time of Day	Set the time of day to start the schedule.
End Day	Select the day of the week to end the schedule, from the drop-down list.
End Time of Day	Set the time of day to end the schedule.

Removing a Schedule

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

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

Port Configuration

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

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

Graphical Display

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

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

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

Global Configuration

These are the global configuration options that you can set:

Figure 31. Global Configuration

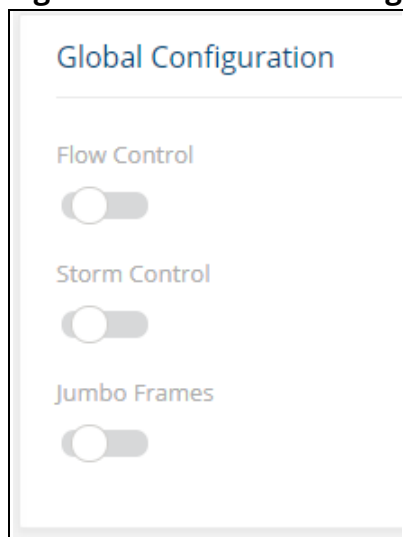


Table 25. Global Configuration Fields

Field	Description
Flow Control	When a port becomes congested, it may begin dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss. When 802.3x flow control is enabled, a lower-speed switch can communicate with a higher-speed switch by requesting that the higher-speed switch refrain from sending packets. Transmissions are temporarily halted to prevent buffer overflows.
Storm Control	The switch supports Global storm control settings. By default, global storm control is disabled. The Storm Control feature protects against conditions where incoming packets flood the LAN, causing network performance degradation. The software includes Storm Control protection for unicast traffic with an unknown destination, and for broadcast and multicast traffic. When enabled, the following storm control settings are applied to all switch interfaces: <ul style="list-style-type: none">Storm Control rate limit - 5% of interface speed. The limit is applied separately to each type of storm control - unicast (including unknown unicast), multicast or broadcast.Packets that exceed the threshold limits are dropped.
Jumbo Frames	Sets both MTU and MRU values <ul style="list-style-type: none">If disabled - frame size is limited to 1518 bytesIf enabled - frame size is limited to 10240 bytes. Changing this setting requires saving the configuration and rebooting the switch. The new setting is applied only after reboot.



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



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

Interface Configuration

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

Figure 32. Interface Configuration Tile

Interface Configuration											
Interface	Description	Type	Admin Mode	Schedule	Physical Mode	Physical Status	Auto Negotiation Capabilities	STP Mode	LACP Mode	Link Status	
<input type="checkbox"/> 1		Normal	Enabled	None	Auto	Unknown	10h 10f 100h 100f 1000f	Enabled	N/A	Link Down	
<input type="checkbox"/> 2		Normal	Enabled	None	Auto	Unknown	10h 10f 100h 100f 1000f	Enabled	N/A	Link Down	
<input type="checkbox"/> 3		Normal	Enabled	None	Auto	Unknown	10h 10f 100h 100f 1000f	Enabled	N/A	Link Down	
<input type="checkbox"/> 4		Normal	Enabled	None	Auto	Unknown	10h 10f 100h 100f 1000f	Enabled	N/A	Link Down	

Table 26. Interface Configuration Fields

Field	Description
Interface	The port or trunk ID.
Description	The current description, if any, associated with the interface to help identify it.
Type	The interface type, which can be one of the following: <ul style="list-style-type: none"> Normal—The port is a normal port, which means it is not a Link Aggregation Group (LAG) member (also known as Trunk), or configured for port mirroring. All ports are normal ports by default. Trunk Member—The port is a member of a trunk. Mirrored—The port is configured to mirror its traffic (ingress, egress, or both) to another port (the probe port). Probe—The port is configured to receive mirrored traffic from one or more source ports.
Admin Mode	The administrative mode of the interface. If a port or trunk is administratively disabled, it cannot forward traffic. The possible values are: <ul style="list-style-type: none"> Enabled: Administratively enabled. Disabled: Administratively disabled.
Schedule	The schedule for activation of certain switch features, as defined in Schedule Configuration .
Physical Mode	The port speed and duplex mode. If the mode is Auto, all the port capabilities are advertised, and the duplex mode and speed are set from the auto-negotiation process.
Physical Status	Indicates the port speed and duplex mode for physical interfaces. The physical status for a trunk is not reported. When a port is down, the physical status is unknown.
Auto Negotiation Capabilities	Indicates the list of configured capabilities for a port when Auto Negotiate is enabled. The Capability status for a trunk is not reported.
STP Mode	The Spanning Tree Protocol (STP) Administrative Mode associated with the port or LAG. STP is a layer 2 protocol that provides a tree topology for switches on a bridged LAN. STP allows a network to have redundant paths without the risk of network loops by providing a single path between end stations on a network. The possible values for STP mode are: <ul style="list-style-type: none"> Enabled - Spanning tree is enabled for this port. Disabled - Spanning tree is disabled for this port.
LACP Mode	Indicates the Link Aggregation Control Protocol administration state. This field can have the following values: <ul style="list-style-type: none"> Enabled: The port is a Trunk member. Trunk is an LACP Trunk. Disabled: The port is a Trunk member. Trunk is a Static Trunk (not LACP). N/A: The port is not a member of a Trunk, or port type is Trunk (TRK).

Field	Description
Link Status	Indicates the link status of the port. The possible values are: <ul style="list-style-type: none"> Link up. Link down. Suspended: Automatically disabled by the system due to schedule configurations, or error conditions. For example, an interface may be disabled by the switch due to an error condition. See the error logs for more information.

Modifying Interface Settings



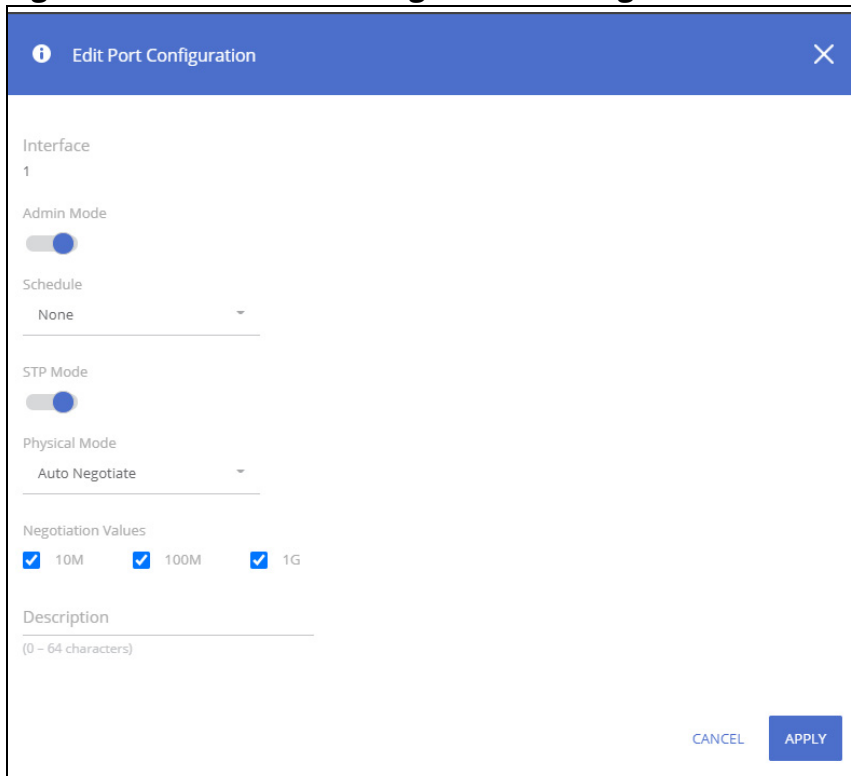
To change the port configuration of one or more interfaces, check the box to the left of one or more interfaces and click **Edit** . To edit all the interfaces at the same time, click **Edit All** .

Figure 33. Edit Port Configuration Dialog Box



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

Table 27. Edit Port Configuration Fields

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

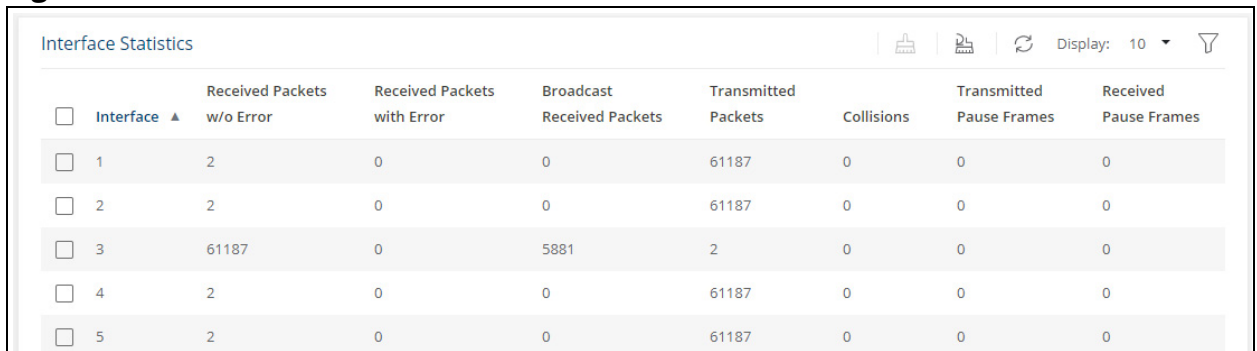
Field	Description
Schedule	Select one of the previously defined schedules. See Schedule Configuration for more information on schedules.
STP Mode	Enable or disable STP on the interface.
Physical Mode	Set the port speed and duplex to either auto-negotiation or one of the available options.
Negotiation Values	Determines the link speed settings advertised by the switch during the auto-negotiation.
Description	Describe the interface to help identify it.

Interface Statistics

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

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


Figure 34. Interface Statistics Tile



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

Table 28. Interface Statistics Fields

Field	Description
Interface	The port or trunk ID.
Received Packets w/o Error	The count of packets received on the port without any packet errors.
Received Packets with Error	The count of packets received on the port with errors.
Broadcast Received Packets	The count of broadcast packets received on the port.
Transmitted Packets	The number of packets transmitted out of the port.
Collisions	The number of packet collisions.
Transmitted Pause Frames	The number of Ethernet pause frames transmitted. This information is collected for ports but not for trunks.
Received Pause Frames	The number of Ethernet pause frames received. This information is collected for ports but not for trunks.

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

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

Port Mirroring

Port Mirroring is used to monitor the network traffic that one or more ports send and receive. The Port Mirroring feature creates a copy of the traffic that the source interface handles and sends it to a probe port (also known as destination port).

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

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



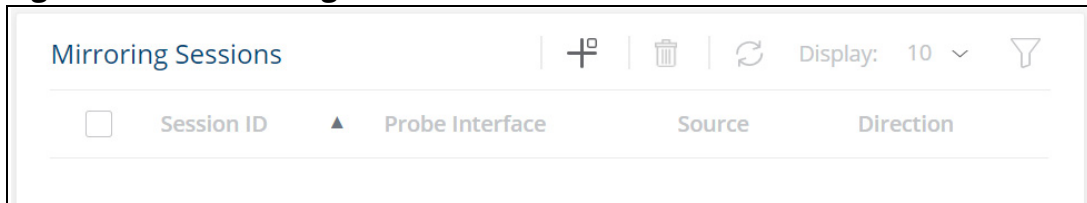
When configuring port mirroring, avoid oversubscribing the destination port to prevent the loss of mirrored data.

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

Mirroring Sessions

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

Figure 35. Mirroring Sessions Tile



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


Table 29. Mirroring Sessions Fields

Field	Description
Session ID	The port mirroring session ID. Up to four port mirroring sessions are allowed.
Probe Interface	The switch port to which packets will be mirrored. Typically, a network protocol analyzer is connected to this port. If the port is configured as an interface or probe port, it receives traffic from all configured source ports.
Source	The ports or VLAN configured to mirror traffic to the destination. NOTE: You can configure multiple source ports or one source VLAN per session. VLANs can be defined as sources only in Session ID 1.

Field	Description
Direction	The direction of traffic on the source port (or source ports) that is sent to the specified destination. A source VLAN mirrors RX traffic only. Possible values for source ports are: <ul style="list-style-type: none"> Tx/Rx – Both ingress and egress traffic. Rx – Ingress traffic only. Tx – Egress traffic only.

Configuring a Port Mirroring Session

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

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


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

Figure 36. Add Mirroring Dialog Box

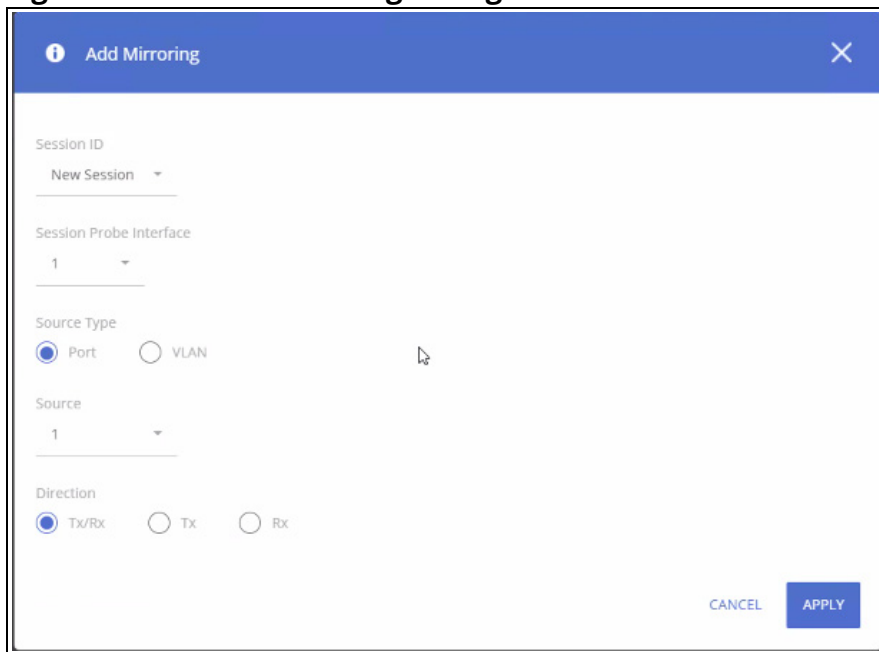


Figure 37.

Table 30: Add Mirroring Dialog Box Fields

Field	Description
Session ID	The identifier for the session being configured. For a new session, the ID is New Session.

Field	Description
Session Probe Interface	The physical port to use as the source probe port to which traffic will be mirrored.
Source Type	The type of interface to use as the source: <ul style="list-style-type: none"> Port – Traffic is mirrored to and/or from a physical port on the switch. VLAN – Traffic to a configured VLAN is mirrored. In other words, all the packets received on all the physical ports that are members of the VLAN are mirrored. VLAN can be specified as source only if the session ID is 1.
Source	Specify the source interfaces for mirrored traffic. interface type depends on the value set in the Source Type field.
Direction	The direction of traffic on the source port (or source ports) that is sent to the specified destination. A source VLAN mirrors only received packets. Possible values for source ports are: <ul style="list-style-type: none"> Tx/Rx – Both ingress and egress traffic. Tx – Egress traffic only. Rx – Ingress traffic only.

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



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



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

Loop Protection

Loops on a network consume resources and can degrade network performance. Detecting loops manually can be very cumbersome and time consuming. The Aruba Instant On 1830 Switch Series software provides an automatic loop protection feature.

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

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

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

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

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

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

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

Global Configuration

Figure 38. Global Configuration

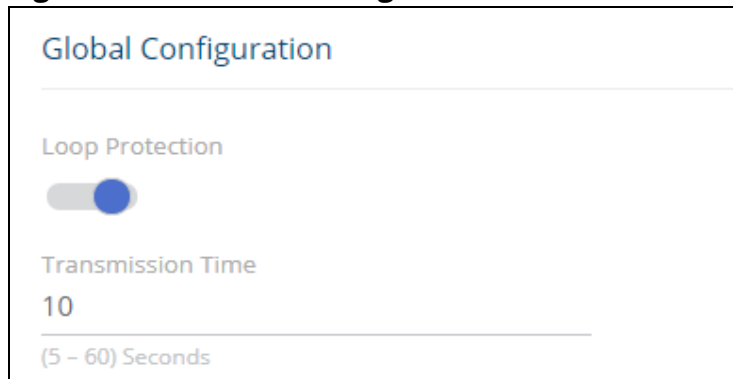


Table 31. Global Configuration Fields

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

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

Interface Configuration

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

Figure 39. Interface Configuration Tile

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

Table 32. Loop Protection Interface Configuration Fields

Field	Description
Interface	The port or trunk ID.
Loop Protection	Indicates whether the feature is administratively enabled or disabled on the port. Loop Protection is disabled by default.
Loop Detection Status	The current loop protection status of the port. <ul style="list-style-type: none"> Enabled - no loop present Disabled - Loop detection is disabled, or the port is down Loop detected - Loop has been detected and port disabled Inactive - Loop detection operational state is disable for the port

Loop Protection Configuration


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

Figure 40. Edit Loop Detection Dialog Box

Edit Loop Detection

Interface
1

Loop Protection

CANCEL APPLY

Table 33. Edit Loop Protection Fields

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

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

IGMP Snooping

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

When enabled, the switch supports IGMPv1 and IGMPv2.

Global Configuration

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

Figure 41. Global Configuration Tile

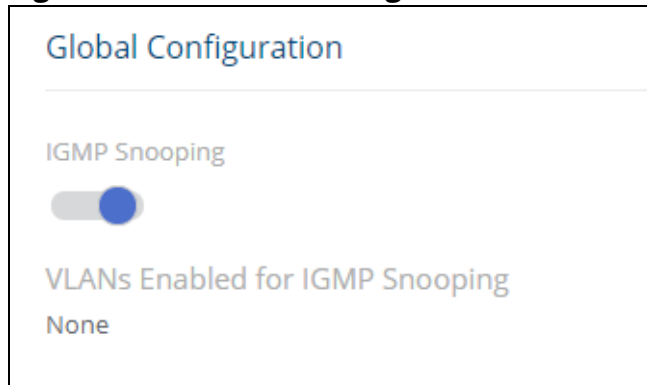


Table 34. Global Configuration Fields

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

Field	Description
VLANs Enabled for IGMP Snooping	Identifies the VLAN ID of each VLAN on which IGMP snooping is administratively enabled. If IGMP snooping is not enabled on any VLANs, this field shows None .

If you change the Admin Mode, click **APPLY** to save the changes for the current switch configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

IGMP Snooping VLAN Configuration

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

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

Figure 42. IGMP Snooping VLAN Configuration Tile

<input type="checkbox"/>	VLAN ID ▲	IGMP Snooping Admin Mode	Fast Leave	Query Interval (Seconds)	Max Response Time (Seconds)	Group Membership Interval (Seconds)	Multicast Router Expiration Time (Seconds)
<input type="checkbox"/>	1	Disabled	Disabled	125	10	260	250

Table 35. IGMP Snooping VLAN Configuration Fields

Field	Description
VLAN ID	The VLAN interface associated with the rest of the data in the row. When configuring IGMP snooping settings, this field identifies the VLAN interface(s) that are being configured.
IGMP Snooping Admin Mode	The administrative mode of IGMP snooping on the VLAN interface. IGMP snooping must be enabled globally and on a VLAN interface to be able to snoop IGMP packets and determine which segments should receive multicast packets directed to the group address.
Fast Leave	The administrative mode of Fast Leave on the VLAN interface. If Fast Leave is enabled, the VLAN interface can be immediately removed from the Layer 2 forwarding table entry upon receiving an IGMP leave message for a multicast group without first sending out MAC-based general queries.
Query Interval (Seconds)	The expected Frequency, in seconds, at which IGMP query messages are forwarded on this VLAN interface.
Max Response Time (Seconds)	The maximum number of seconds a host can wait before sending a group report once it receives a membership query. The specified value should be less than the Group Membership Interval.

Field	Description
Group Membership Interval (Seconds)	The number of seconds the VLAN interface should wait for a report for a particular group on the VLAN interface before the IGMP snooping feature deletes the VLAN interface from the group. This field is read-only. The value shown is calculated based on the following formula: Query interval*2 + max response time
Multicast Router Expiration Time (Seconds)	The number of seconds the VLAN interface should wait to receive a query before it is removed from the list of VLAN interfaces with multicast routers attached. This field is read-only.


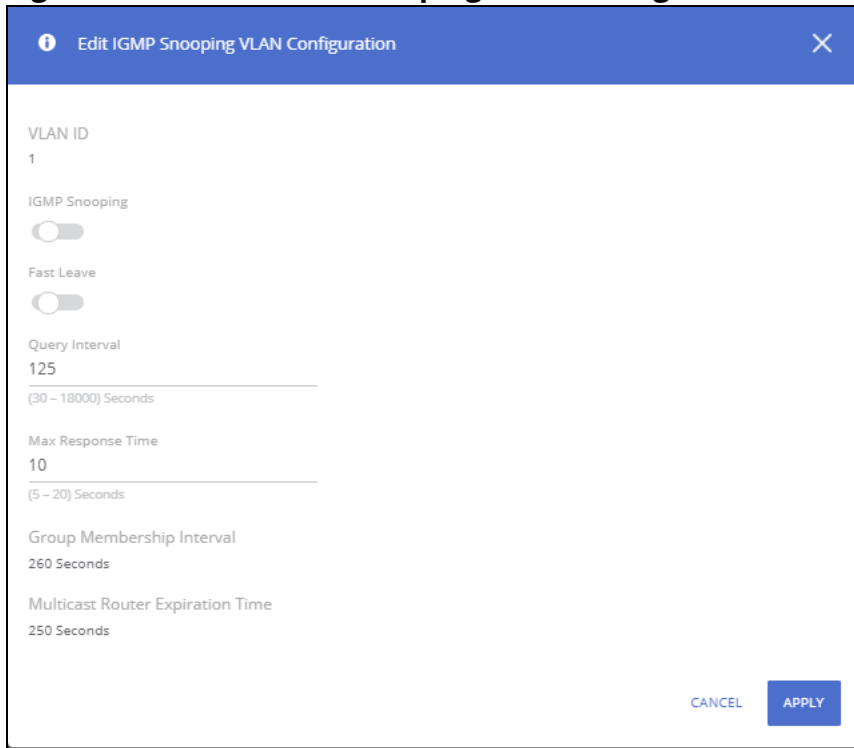
To change the snooping VLAN configuration, check the box to the left of one or more interfaces and click **Edit**  .

Figure 43. Edit IGMP Snooping VLAN Configuration Dialog Box



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

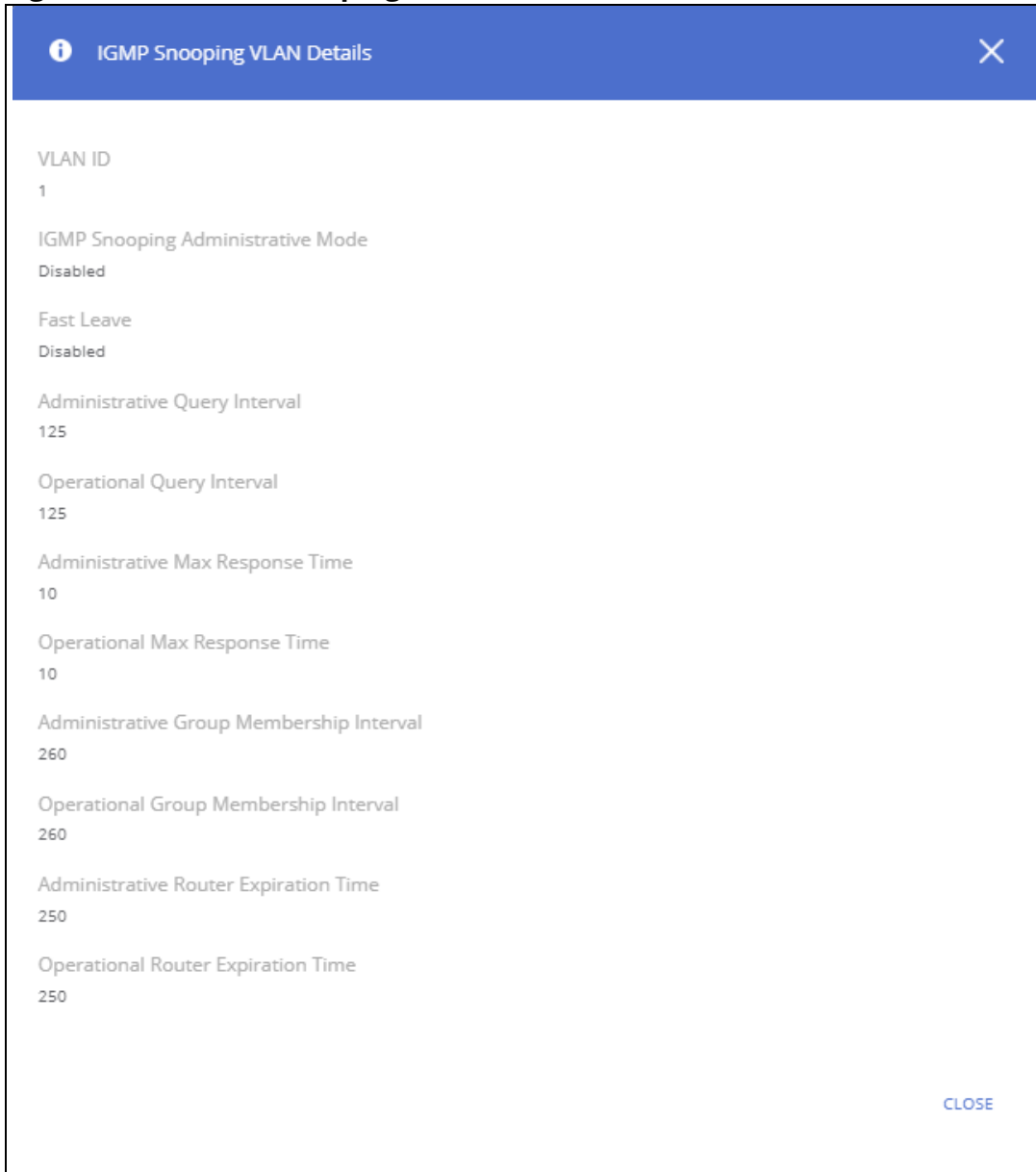
Table 36. Edit IGMP Snooping VLAN Configuration Fields

Field	Description
VLAN ID	The VLAN interface(s) that are being configured.
IGMP Snooping	The administrative mode of IGMP snooping on the VLAN interface. To be operational, IGMP snooping needs to be enabled globally and on the VLAN.

Field	Description
Fast Leave	The administrative mode of Fast Leave on the VLAN interface. If Fast Leave is enabled, the VLAN interface can be immediately removed from the Layer 2 forwarding table entry upon receiving an IGMP leave message for a multicast group without first sending out group-based general queries.
Query Interval	The expected Frequency, in seconds, at which IGMP query messages are sent on this VLAN interface.
Max Response Time	The maximum number of seconds a host can wait before sending a group report once it receives a membership query. The specified value should be less than the Group Membership Interval.
Group Membership Interval	The interval that must pass before the router decides that no members of a group or source exist on the network. This value is not configurable. The default is 260 seconds.
Multicast Router Expiration Time	The number of seconds after which a multicast router entry is timed out. This value is not configurable. The default value is 250 seconds.

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

Figure 44. IGMP Snooping VLAN Details



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

Table 37. IGMP Snooping VLAN Details Fields

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

Field	Description
Operational Max Response Time	Indicates the operational value of the Max Response Time parameter.
Operational Group Membership Interval	The operational value of the Group Membership Interval parameter.
Operational Router Expiration Time	The operational value of the Router expiration Time parameter.

IGMP Snooping Multicast Router Interface Configuration

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

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

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

Figure 45. IGMP Snooping Multicast Router Configuration Tile

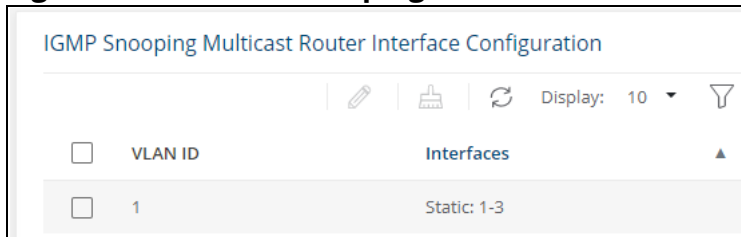



Table 38. IGMP Snooping Multicast Router Configuration Fields

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

Configuring Multicast Router Settings on Interfaces

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


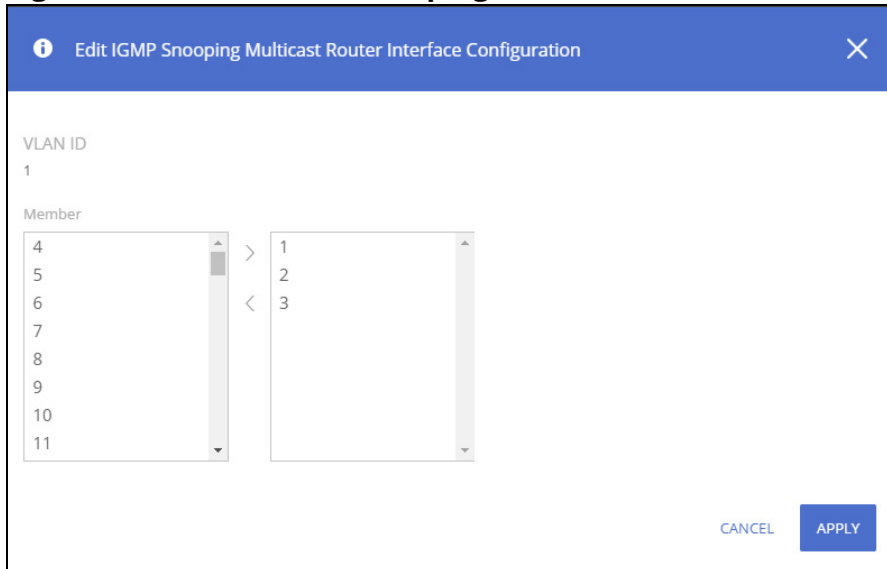
To change the multicast router membership for one or more interfaces, select each entry (that is, VLAN) you wish to modify and click **Edit**  .

Figure 46. Edit IGMP Snooping Multicast Router Interface Configuration Dialog Box



Select one or more interfaces that you want to configure as IGMP snooping multicast router interfaces and click the right arrow. To remove an interface from the list on the right, select it and press the left arrow.

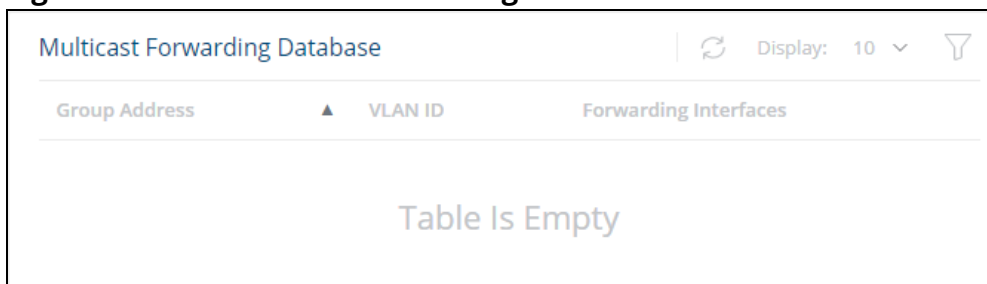
Click **APPLY** to save the changes for the current switch configuration. The changes take effect immediately and are applied to each of the selected interfaces. The changes are not retained across a switch reset unless you click **Save Configuration**.


Multicast Forwarding Database

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

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

Figure 47. Multicast Forwarding Database Tile



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


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

Table 39. Multicast Forwarding Database Fields

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

Interface Auto Recovery

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

Features supported by Auto Recovery are listed below. Each feature is listed with the error conditions that cause a port to be placed into the suspended state:

- **BPDU Guard:** If a port that has the BPDU Guard feature enabled receives a BPDU, the port state is set to Suspended.
- **Loop Protection:** If a loop is detected on an interface with loop protection enabled, the port state is set to Suspended.

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

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

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

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

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

Global Configuration

These are the global configuration options that you can set:

Figure 48. Global Configuration

The screenshot shows a configuration page titled "Global Configuration". It contains three settings:

- BPDGuard**: A toggle switch that is currently turned off.
- Loop Protection**: A toggle switch that is currently turned off.
- Auto Recovery Time**: A text input field containing the value "300". Below the input field, the range "(30 - 86400) Seconds" is displayed.

Table 40. Interface Auto Recovery Global Configuration Fields

Field	Description
BPDGuard	When BPDGuard 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 BPDGuard Auto Recovery mode is disabled, a port that has received a BPDU and has been placed in the suspended state will remain in that state until an administrator manually enables it. BPDGuard Auto Recovery is disabled by default.
Loop Protection	If a loop is detected on an interface with loop protection enabled, the port state is set to Suspended. Loop Protection is disabled by default.
Auto Recovery Time	This configures the Auto Recovery time interval, in seconds. The Auto Recovery time interval is common for all the components. The default value of the timer is 300 seconds and the range is from 30 to 86400 seconds.

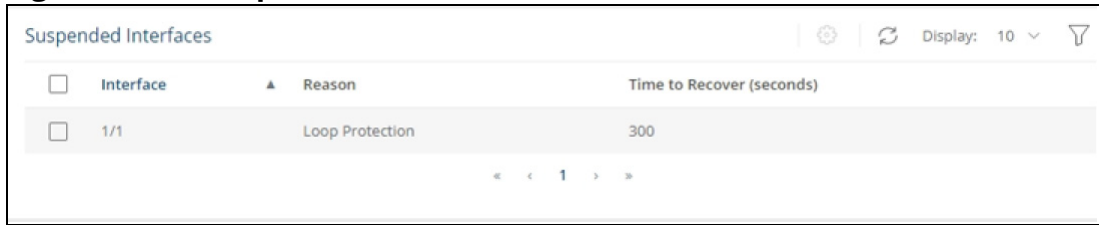
If you modify these settings, click **APPLY** to save the changes for the current switch configuration. The changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

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

Suspended Interfaces

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


Figure 49. Suspended Interfaces



Interface	Reason	Time to Recover (seconds)
1/1	Loop Protection	300

Table 41. Suspended Interfaces Fields

Field	Description
Interface	The interface that is suspended. If no interfaces are in the suspended state, the table is blank.
Reason	If the switch detects an error condition for an interface, the switch puts the interface in the suspended state, meaning that it has been intentionally disabled because it has encountered errors. The reasons that the interface can go into a suspended state include the following: <ul style="list-style-type: none">• BPDU Guard• Loop Protection
Time to Recover (seconds)	When Auto Recovery is enabled and the interface is placed in the suspended state, then a recovery timer starts for that interface. Once this timer expires, the switch checks if the interface is in the suspended state. If yes, then the switch enables the interface.

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



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

Trunk Configuration

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

A trunk interface can be either static or dynamic:

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

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

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

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

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

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

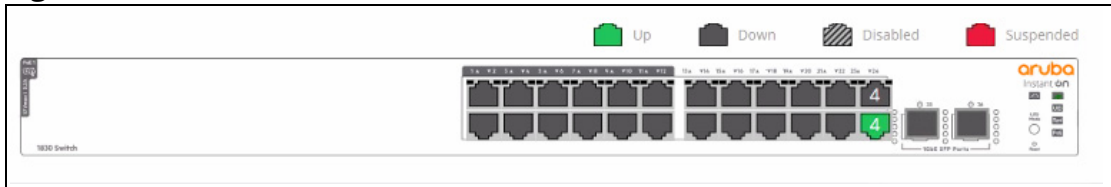


Trunks are sometimes referred to as link aggregation groups (LAGs) or port-channels.

Graphical Display

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

Figure 50. Switch Panel View



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

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

Global Configuration

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

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

- Source and Destination MAC, IP and TCP/UDP Port fields
- Source and Destination MAC fields

- Source and Destination MAC and IP fields (this is the default)

Figure 51. Trunk Configuration Global Configuration Section

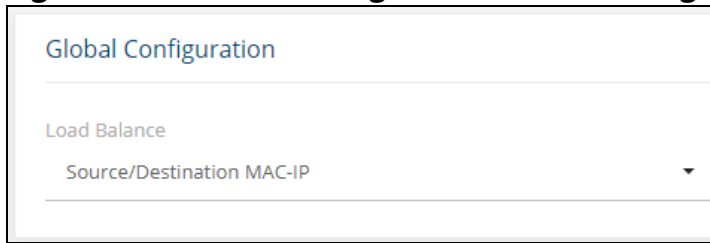


Table 42. Trunk Configuration Global Configuration Fields

Field	Description
Load Balance	These are the Load balance options: <ul style="list-style-type: none"> • Source/Destination MAC-IP-TCP/UDP Port • Source/Destination MAC • Source/Destination MAC-IP

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

Trunk Configuration

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

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

Figure 52. Trunk Configuration

Trunk	Description	Type	Admin Mode	Link Status	Members	Active Ports
<input type="radio"/> TRK 1		Static	Enabled	Down		
<input type="radio"/> TRK 2		Static	Enabled	Down		
<input type="radio"/> TRK 3		Static	Enabled	Down		
<input type="radio"/> TRK 4		Static	Enabled	Down		
<input type="radio"/> TRK 5		Static	Enabled	Down		
<input type="radio"/> TRK 6		Static	Enabled	Down		
<input type="radio"/> TRK 7		Static	Enabled	Down		

The following information is displayed for each trunk.

Table 43. Trunk Configuration Fields

Field	Description
Trunk	The trunk ID.
Description	The trunk description, if any, associated with the interface to help identify it.
Type	Trunks can be either dynamic or static, but not both: <ul style="list-style-type: none">• LACP—Link Aggregation Control Protocol (LACP, IEEE standard 802.3ad). An LACP-enabled port automatically detects the presence of other aggregation-capable network devices in the system and exchanges Link Aggregation Control Protocol Data Units (LACPDU) with links in the trunk. The PDUs contain information about each link and enable the trunk to maintain them.• Static—Static trunks are assigned to a bundle by the administrator. Members do not exchange LACPDU. A static trunk does not require a partner system to be able to aggregate its member ports. This is the default port type.
Admin Mode	Whether the trunk is administratively enabled or disabled. This setting is enabled by default.
Link Status	Indicates the operational status of the trunk interface, which can be Up, Up (SFP) for ports with an installed SFP transceiver, or Down.
Members	The ports that are members of the trunk. By default, no ports belong to any trunk.
Active Ports	The ports that are actively participating members of a trunk. A member port that is operationally or administratively disabled or does not have a link is not an active port.

Modifying Trunk Settings


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

Figure 53. Edit Trunk Configuration Dialog Box

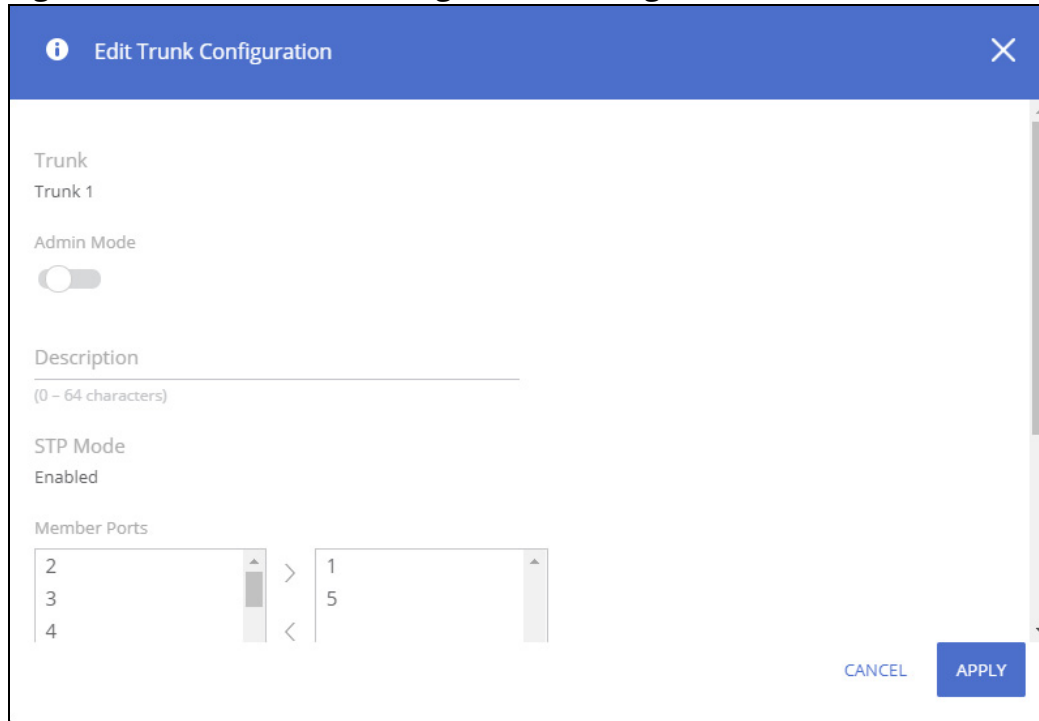


Table 44. Edit Trunk Configuration Fields

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

Note the following considerations when configuring trunks and trunk members:

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

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

EEE Configuration

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

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

Global Configuration

Figure 54. Global Configuration

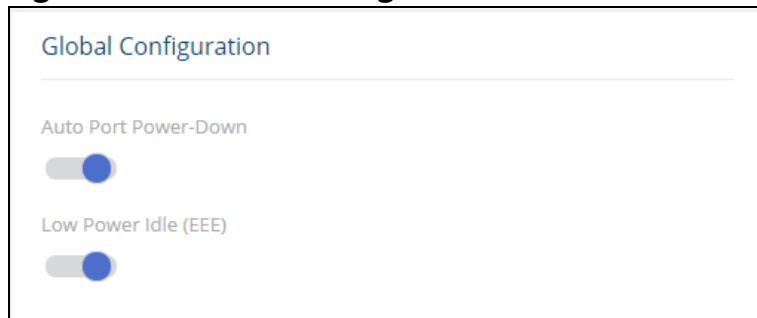


Table 45. Global Configuration Fields

Field	Description
Auto Port Power-Down	When this feature is enabled and the port link is down, the PHY automatically goes down for a short period of time. The port wakes up when it senses activity on the link. This feature enables saving power consumption when no link partner is present. This feature is enabled by default.
Low Power Idle (EEE)	EEE (Energy Efficient Ethernet) saves power by reducing power consumption on network ports that are not forwarding traffic. When Low Power Idle (EEE) is enabled, the ports will enter a low-power mode to reduce power consumption during periods there is no traffic on a network port. The EEE feature works on ports in auto-negotiation mode, where the port is negotiated to either 100 Mbps full duplex or 1 Gbps (1000 Mbps) full duplex. EEE feature is enabled by default NOTE: EEE is active only if port auto-negotiation mode is enabled.

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

Global Status

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

Figure 55. Global Status

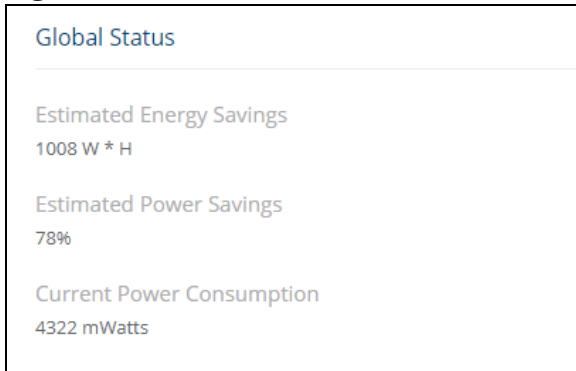


Table 46. Global Status Fields

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

Interface Status

This page displays EEE status information for each interface.

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

Figure 56. Interface Status Tile

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

Table 47. EEE Status Fields

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

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

Aruba Instant On 1830 Switch 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 inter-operate with switches running the STP protocol by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

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

Global Configuration

These are the global configurations for Spanning Tree Switch:

Figure 57. Spanning Tree Global Configuration Page



The screenshot displays the 'Global Configuration' page for Spanning Tree. The page includes the following settings:

- Spanning Tree Admin Mode:** A toggle switch that is currently turned on (blue).
- Protocol Version:** Two radio buttons are present: 'STP' (unselected) and 'RSTP' (selected).
- Bridge Priority:** A dropdown menu showing the value '32768'.
- Bridge Max Age:** A text input field containing '20', with a range of '(6 - 40) Seconds' indicated below it.
- Bridge Forward Delay:** A text input field containing '15', with a range of '(4 - 30) Seconds' indicated below it.
- BPDUs Filter:** A toggle switch that is currently turned off (grey).

Table 48. Spanning Tree Global Configuration Fields

Field	Description
Spanning Tree Admin Mode	The administrative mode of STP on the switch. When enabled, the switch participates in the root bridge election process and exchanges Bridge Protocol Data Units (BPDUs) with other switches in the spanning tree to determine the root path costs and maintain topology information. By default, Admin Mode is enabled.
Protocol Version	The STP version the switch uses, which is one of the following: <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. This is the default protocol.
Bridge Priority	The value that helps determine which bridge in the spanning tree is elected as the root bridge during STP convergence. A lower value increases the probability that the bridge becomes the root bridge. The default priority is 32768. The valid range is 0-61440, in steps of 4096.
Bridge Max Age	The amount of time a bridge waits before implementing a topological change. The default is 20. The valid range is 6-40.
Bridge Forward Delay	The amount of time a bridge remains in a listening and learning state before forwarding packets. The default is 15. The valid range is 4-30.
BPDU Filter	When enabled, this feature filters the BPDU traffic on ports when spanning tree is disabled.

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

Global Settings

These are the Global Settings that you can view:

Figure 58. Spanning Tree Global Settings Page

Global Settings		
Root Bridge Identifier 32768:00:00:00:01:02	Root Path Cost 80000	Topology Change Count 196
Bridge Hello Time 2 Seconds	Root Port 23	Root Guarded Interfaces N/A
Spanning Tree Tx Hold Count 3	Max Age 20 Seconds	TCN Guarded Interfaces N/A
Bridge Identifier 32768:00:00:B0:13:12:B4	Forward Delay 15 Seconds	BPDU Filtered Interfaces N/A
Time Since Topology Change 13:03	Hold Time 1 Seconds	

Table 49. Spanning Tree Global Settings Fields

Field	Description
Root Bridge Identifier	The bridge identifier of the root bridge for the spanning tree. The identifier is made up of the bridge priority and the base MAC address. When electing the root bridge for the spanning tree, if the bridge priorities for multiple bridges are equal, the bridge with the lowest MAC address is elected as the root bridge.
Bridge Hello Time	The amount of time the root bridge waits between sending hello BPDUs.
Spanning Tree Tx Hold Count	The maximum number of BPDUs that a bridge is allowed to send within a hello time window.
Bridge Identifier	A unique value that is automatically generated based on the bridge priority value and the base MAC address of the bridge. When electing the root bridge for the spanning tree, if the bridge priorities for multiple bridges are equal, the bridge with the lowest MAC address is elected as the root bridge.
Time Since Topology Change	The amount of time that has passed since the topology of the spanning tree has changed since the switch was last reset.
Root Path Cost	The path cost to the designated root for the CST. Traffic from a connected switch to the root bridge takes the least-cost path to the bridge.
Root Port	The port on the bridge with the least-cost path to the designated root for the CST.
Max Age	The amount of time a bridge waits before implementing a topological change.
Forward Delay	The forward delay value for the root port bridge.
Hold Time	The minimum amount of time between transmissions of Configuration BPDUs.
Topology Change Count	The number of topology changes that occurred since last time the device reloaded.
Root Guarded Interfaces	A list of interfaces currently having the Root Guard parameter set.
TCN Guarded Interfaces	A list of interfaces currently having the TCN Guard parameter set.

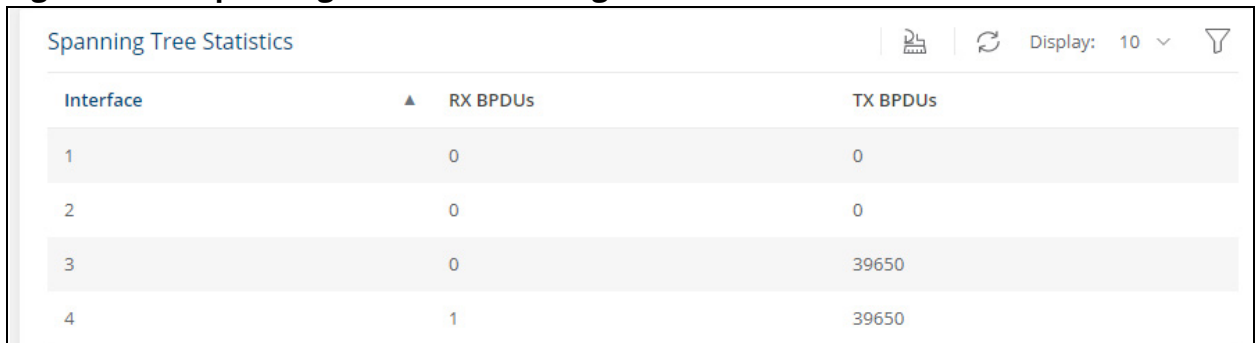
Field	Description
BPDU Filtered Interfaces	A list of interfaces currently having the BPDU Filter parameter set.

Spanning Tree Statistics

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

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

Figure 59. Spanning Tree Statistics Page



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

Table 50. Spanning Tree Statistics Fields

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

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

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

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

CST Configuration

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

mation about the interface's role in the CST topology, select the interface to view or configure and click **Edit**.

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

CST Port Configuration

Figure 60. CST Port Configuration Tile

<input type="checkbox"/>	Interface	▲ Port Role	Port Forwarding State	Port Priority	Port Path Cost
<input type="checkbox"/>	1	Disabled	Disabled	128	2000000
<input type="checkbox"/>	2	Disabled	Disabled	128	20000
<input type="checkbox"/>	3	Designated	Forwarding	128	20000
<input type="checkbox"/>	4	Designated	Forwarding	128	20000

Table 51. CST Port Configuration Fields

Field	Description
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring CST settings for an interface, this field identifies the interface being configured.
Port Role	The role of the port within the CST, which is one of the following: <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. • Disabled – The port is physically down, or 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 physically down, or administratively disabled and is not part of the spanning tree.
Port Priority	The priority for the port within the CST. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost from the assigned port to this port.

Additional Actions on CST Ports

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




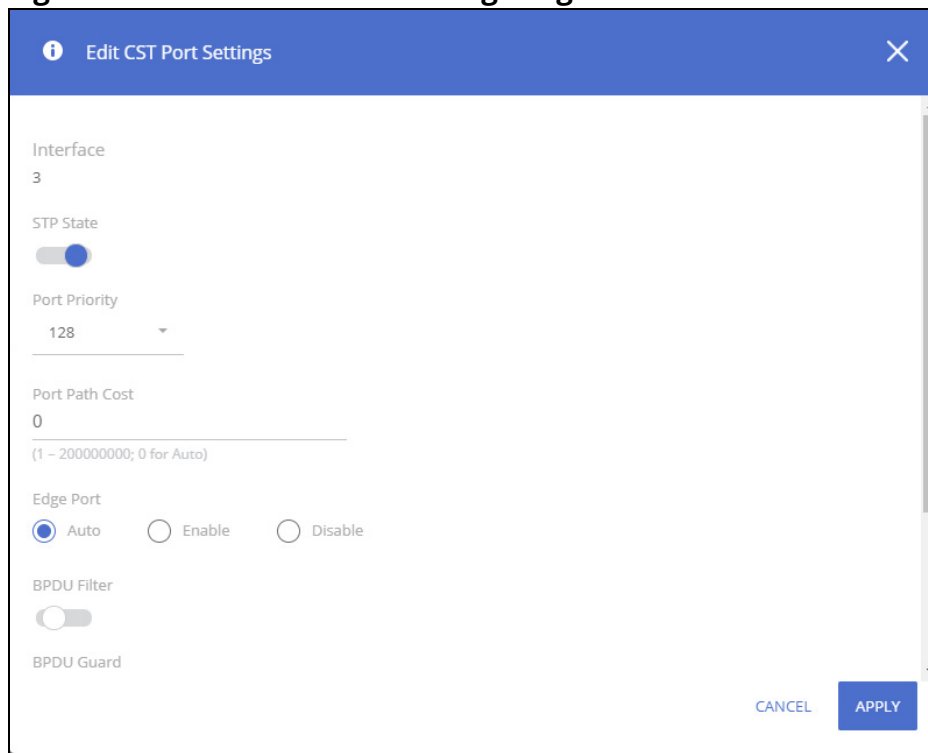
- View **Details**  . This option is available if you have a single port selected. For more information, see [CST Port Details Fields](#).
- **Edit** CST Settings  . This option is available if you select one or more ports. The same settings are applied to all selected interfaces. For more information,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

Figure 61. Edit CST Port Settings Page



The screenshot shows a configuration window titled "Edit CST Port Settings". The settings are as follows:

- Interface: 3
- STP State: Enabled
- Port Priority: 128
- Port Path Cost: 0 (range: 1 - 200000000; 0 for Auto)
- Edge Port: Auto, Enable, Disable
- BPDUs Filter: Disabled
- BPDUs Guard: Disabled

Buttons for "CANCEL" and "APPLY" are located at the bottom right of the window.

Table 52. Edit CST Port Fields

Field	Description
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring CST settings for an interface, this field identifies the interface being configured.
STP State	The port STP state. If set to enabled, the port will be part of the spanning tree topology. If set to disable, the port will not participate in spanning tree topology. The default state is enabled.

Field	Description
Port Priority	The priority for the port within the CST. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost associated with this port. If set to 0 cost will be determined based on port speed (auto).
Edge Port	Indicates whether the interface is configured as an edge port the following settings are supported: <ul style="list-style-type: none"> • Auto - Enables edge port on switch, but only following a few seconds delay after port is up (this is the default) • Enable - edge port is enabled on interface • Disable - edge port is disabled on interface.
BPDU Filter	When enabled, this feature filters the BPDU traffic on the port, if STP is administratively disabled on interface. This feature requires BPDU filtering to be enabled globally.
BPDU Guard	When enabled, BPDU Guard can disable edge ports that receive BPDU packets. This prevents a new switch from entering the existing STP topology. Thus devices that were originally not a part of STP are not allowed to influence the STP topology.
Root Guard	When enabled, Root Guard allows the interface to discard any superior information it receives to protect the root of the switch from changing. The port gets put into discarding state and does not forward any frames.
TCN Guard	When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.


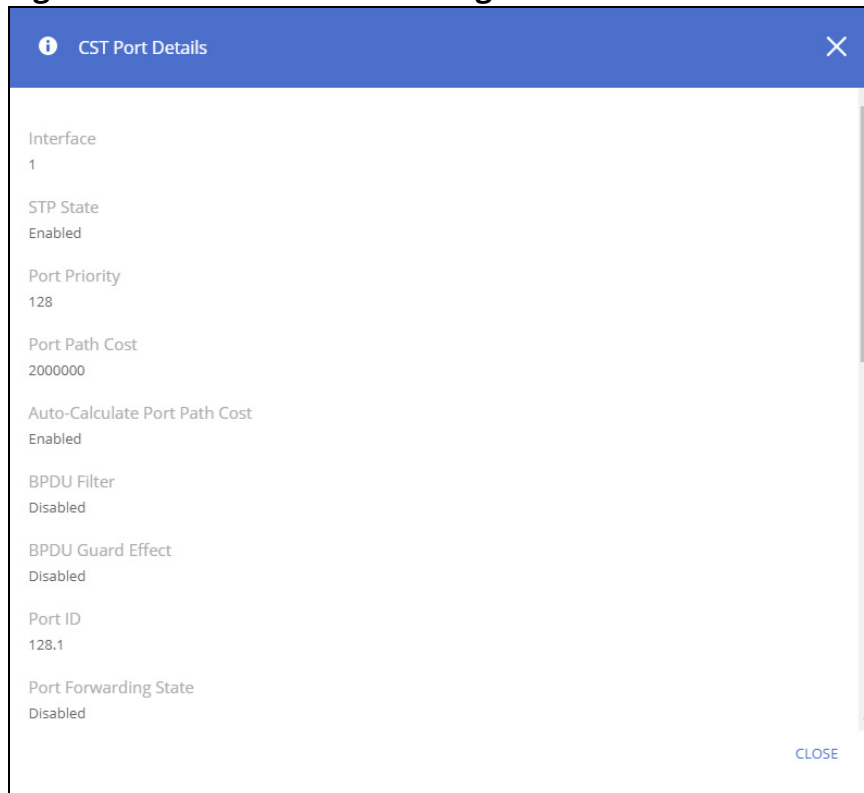
To view additional information about an interface's role in the CST topology, select the interface to view, and then click **Details** 

Figure 62. CST Port Details Page



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

Table 53. CST Port Details Fields

Field	Description
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row. When configuring CST settings for an interface, this field identifies the interface being configured.
STP State	The port STP state. If set to enabled, the port will be part of the spanning tree topology. If set to disable, the port will not participate in spanning tree topology. The default state is enabled.
Port Priority	The priority for the port within the CST. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Port Path Cost	The path cost associated with this port. If set to 0 cost will be determined based on port speed (auto).
Auto-calculate Port Path Cost	Shows whether the path cost from the port to the root bridge is automatically determined by the speed of the interface (Enabled) or configured manually (Disabled).
BPDU Filter	When enabled, this feature filters the BPDU traffic on the port, if STP is administratively disabled on interface. This feature requires BPDU filtering to be enabled globally.
BPDU Guard Effect	When enabled, BPDU Guard can disable edge ports that receive BPDU packets. This prevents a new switch from entering the existing STP topology. Thus devices that were originally not a part of STP are not allowed to influence the STP topology.

Field	Description
Port ID	A unique value that is automatically generated based on the port priority value and the interface index.
Port Forwarding State	<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. • Disabled – The port is administratively disabled and is not part of the spanning tree.
Designated Root	The bridge ID of the root bridge for the CST.
Designated Cost	The path cost offered to the LAN by the designated port.
Designated Bridge	The bridge ID of the bridge with the designated port.
Designated Port	The port ID of the designated port.
Admin Edge Port	The edge port setting on port - Auto, Enabled or Disabled.
Edge Port	Indicates if edge port is Active or Inactive on the interface.
Point-to-point MAC	Indicates whether the link type for the interface is a point-to-point link.
Root Guard	When enabled, Root Guard allows the interface to discard any superior information it receives to protect the root of the switch from changing. The port gets put into discarding state and does not forward any frames.
TCN Guard	When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.

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

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

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

Aruba Instant On 1830 Switch Series switches support up to 64 VLANs.

VLAN Configuration

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

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

Graphical Display

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

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

Figure 63. VLAN Switch Panel View



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

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

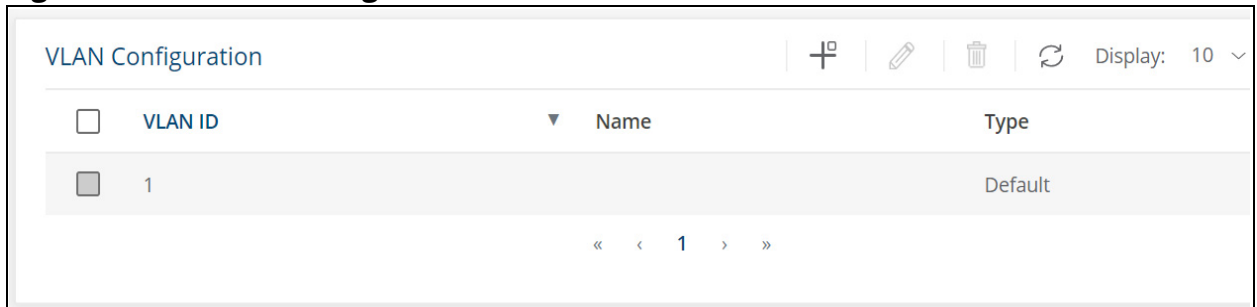
If there is no indication, this means that the port is not a member of a VLAN. For more information, see [Switch Panel View](#).

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

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

VLAN Configuration

Figure 64. VLAN Configuration Tile



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

VLAN 1 is also the default management VLAN, which identifies the VLAN that management users must be a member of. The administrator can configure a different VLAN as the management VLAN. See **Management VLAN Settings** for additional information about the management VLAN.

The following information is displayed for each VLAN:

Table 54. VLAN Configuration Fields

Field	Description
VLAN ID	The numerical VLAN identifier (VID) assigned to the VLAN, from 1 to 4092. Note: VLAN 0 (VID = 0x000 in a frame) is reserved and is used to indicate that the frame does not belong to any VLAN. In this case, the 802.1Q tag specifies only a priority and the value is referred to as a <i>priority tag</i> .
Name	A user-configurable name that identifies the VLAN.
Type	The type of VLAN, which can be one of the following: <ul style="list-style-type: none"> Default—The default VLAN. This VLAN is always present, and the VLAN ID is 1. RADIUS—A VLAN created by a RADIUS VLAN assignment. Static—A user-configured VLAN.


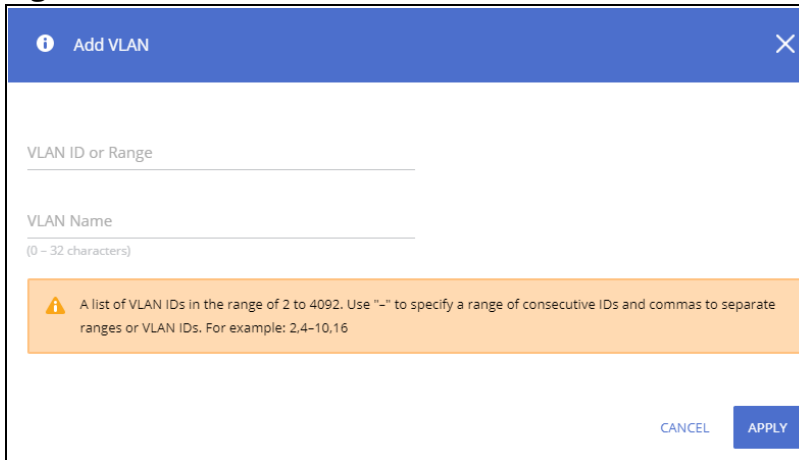
To add a VLAN, click **Add**  .

Figure 65. Add VLAN



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



VLAN 4093 and 4094 are reserved for internal system use.

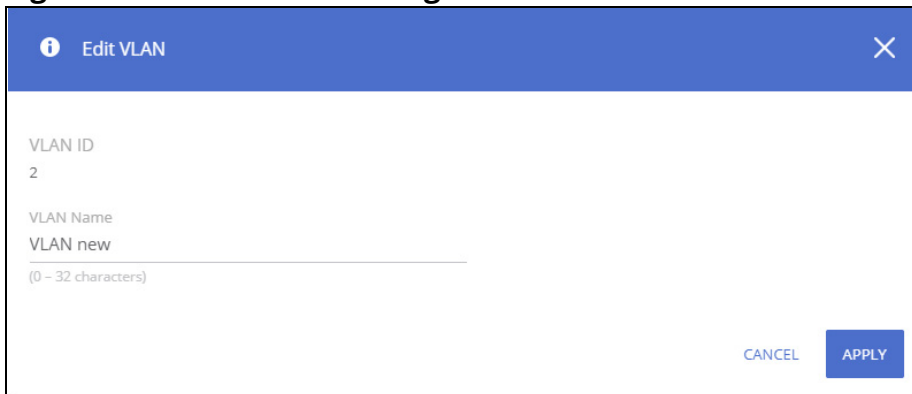
To create a range of VLANs, specify the beginning and ending VLAN IDs, separated by a dash. Optionally you can define a name for the VLAN in the **VLAN Name** field.

To create multiple non-sequential VLANs, separate each VLAN ID with a comma. You can create up to 64 VLANs.

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

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

Figure 66. Edit VLAN Dialog Box



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

VLAN Membership

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

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

This tile has two tabs:

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

VLAN Membership - By Interface Tab

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

Figure 67. VLAN Membership - By Interface Tab

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

Table 55. VLAN Membership - By Interface Fields

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

To configure VLAN Membership - By Interface, select one or more ports and click **Edit** . Or, click **Edit All** to configure all ports at the same time.

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

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

VLAN Membership - By VLAN Tab

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

Figure 68. VLAN Membership - By VLAN Tab

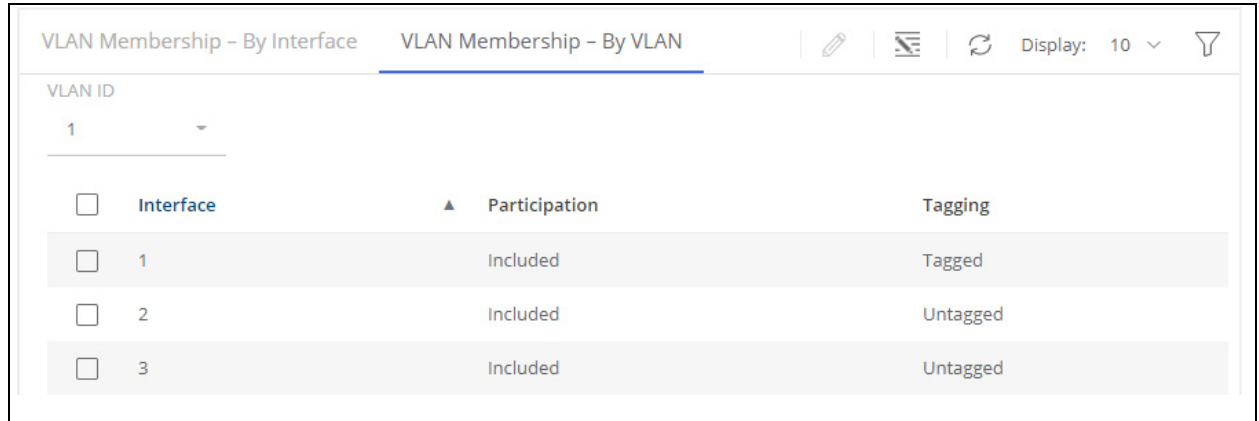


Table 56. VLAN Membership - By VLAN Tab Fields

Field	Description
VLAN ID	Select the VLAN ID for which you want to view interface memberships.
Interface	The port or trunk ID.
Participation	The participation mode of the interface in the selected VLAN, which is one of the following: <ul style="list-style-type: none"> Included – The port is a member of the selected VLAN. This mode is also equivalent to registration fixed in the IEEE 802.1Q standard. Excluded – The port is not a member of the selected VLAN. This mode is also equivalent to registration forbidden in the IEEE 802.1Q standard.
Tagging	The tagging behavior for each port in this VLAN, which is one of the following: <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 VLAN Membership - By VLAN, select the VLAN to configure, from the VLAN ID dropdown, then select one or interfaces and click **Edit** . Or, click **Edit All** to configure all the interfaces at the same time.

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

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

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

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

VLAN Interface Configuration

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

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



Figure 69. VLAN Interface Configuration Tile

<input type="checkbox"/>	Interface ▲	Port VLAN ID	Acceptable Frame Type	Ingress Filtering	Untagged VLAN	Tagged VLANs
<input type="checkbox"/>	1	1	Tagged and Untagged	Enabled	1	1
<input type="checkbox"/>	2	1	Tagged and Untagged	Enabled	1	1
<input type="checkbox"/>	3	1	Tagged and Untagged	Enabled	1	1
<input type="checkbox"/>	4	1	Tagged and Untagged	Enabled	1	1
<input type="checkbox"/>	5	1	Tagged and Untagged	Enabled	1	1

Table 57. VLAN Interface Configuration Fields

Field	Description
Interface	Identifies the physical interface or LAG associated with the rest of the data in the row.
Port VLAN ID	The VLAN ID assigned to untagged or priority tagged frames received on this port. This value is also known as the Port VLAN ID (PVID). In a tagged frame, the VLAN is identified by the VLAN ID in the tag.

Field	Description
Acceptable Frame Type	<p>Indicates how the interface handles untagged and priority tagged frames:</p> <ul style="list-style-type: none"> • Tagged and Untagged– Untagged and priority tagged frames received on the interface are accepted and assigned the value of the Port VLAN ID for this interface. • Tagged Only– The interface discards any untagged or priority tagged frames it receives. • Untagged Only– The interface discards any tagged frames it receives. <p>For all options, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN standard.</p>
Ingress Filtering	<p>Shows how the port handles tagged frames.</p> <ul style="list-style-type: none"> • Enabled: A tagged frame is discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. This is the default setting • Disabled: All tagged frames are accepted.
Untagged VLAN	VLANs that are configured on the port to transmit egress packets as untagged.
Tagged VLANs	VLANs that are configured on the port to transmit egress packets as tagged.

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

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

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

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

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

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

LLDP

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

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

LLDP Global Configuration

Figure 70. LLDP Global Configuration Tile

LLDP Global Configuration

Transmit Interval
30
(5 – 32768) Seconds

Transmit Hold Multiplier
4
(2 – 10) Seconds

Re-Initialization Delay
2
(1 – 10) Seconds

Modification Interval
5
(5 – 3600) Seconds

You can configure the following global settings:

Table 58. LLDP Global Configuration Fields

Field	Description
Transmit Interval	Specify the time between transmission of LLDPDUs. The range is from 5 to 32768 seconds and the default is 30 seconds.
Transmit Hold Multiplier	Specify the multiplier value on the transmit interval, which is used to compute the time-to-live (TTL) value associated with LLDPDUs. The range is from 2 to 10 seconds, and the default is 4 seconds.
Re-Initialization Delay	Specify the number of seconds to wait before attempting to re-initialize LLDP on a port after the LLDP operating mode on the port changes. The range is from 1 to 10 seconds and the default is 2 seconds.
Modification Interval	Specify the minimum number of seconds to wait between transmissions of remote data change notifications. The range is from 5 to 3600 seconds and the default is 5 seconds.

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

LLDP Global Information

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

Figure 71. LLDP Global Information

LLDP Global Information

Chassis ID
00:00:B0:17:12:00

Chassis ID Subtype
MAC Address

Capabilities Supported
Bridge

Capabilities Enabled
Bridge

Table 59. LLDP Global Information Fields

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

Interface Configuration

The following information is displayed for each LLDP interface.

Figure 72. Interface Configuration

Interface Configuration

 Display: 10 v

<input type="checkbox"/>	Interface ▲	Link Status	Transmit	Receive	Notify	Transmit Management Information
<input type="checkbox"/>	1	Link Down	Enabled	Enabled	Enabled	Yes
<input type="checkbox"/>	2	Link Up	Enabled	Enabled	Enabled	Yes
<input type="checkbox"/>	3	Link Up	Enabled	Enabled	Enabled	Yes
<input type="checkbox"/>	4	Link Up	Enabled	Enabled	Enabled	Yes
<input type="checkbox"/>	5	Link Up	Enabled	Enabled	Enabled	Yes

Table 60. Interface Configuration Fields

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


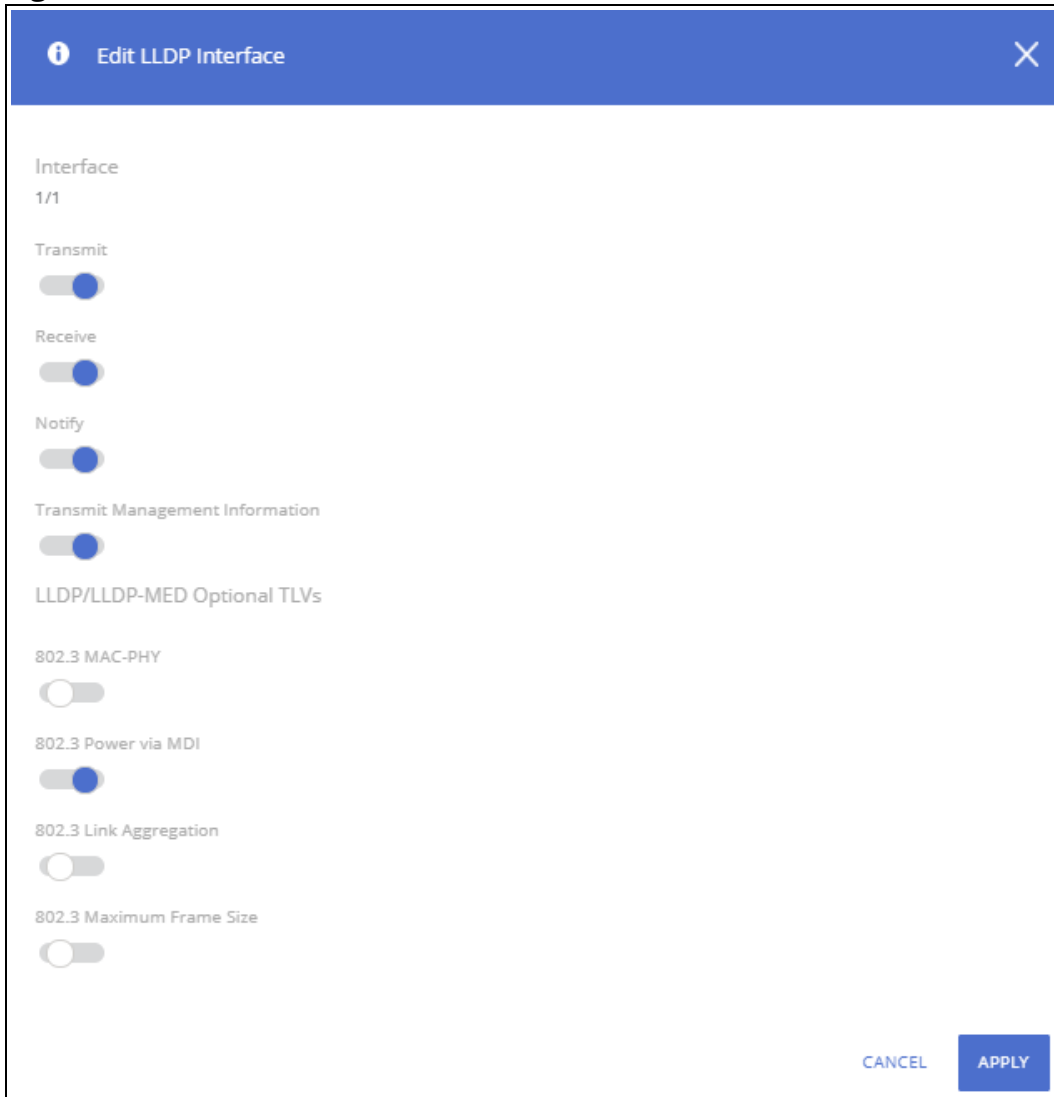
To modify interface settings, select one or more interfaces and click **Edit** to display the Edit LLDP Interface page. Or, click **Edit All**  to configure all interfaces at the same time.

Figure 73. Edit LLDP Interface



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

Table 61. Additional LLDP Interface Fields

Field	Description
802.3 MAC-PHY	Duplex and bit rate capability and the current duplex and bit rate settings of the sending device.
802.3 Power via MDI	This field appears for PoE devices. This TLV supports the following extensions. <ul style="list-style-type: none"> Type 2 (12 octets) Type 3 (29 octets) This option is enabled by default.

Field	Description
802.3 Link Aggregation	Set to enable the link (associated with the port on which the LLDP PDU is transmitted) to be aggregated.
802.3 Maximum Frame Size	Maximum frame size capability of the MAC/PHY implementation.

Device Information Tile

This tile has two tabs:

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

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

Remote Device Information

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

Figure 74. Remote Device Information Tab

Interface	Remote ID	Chassis ID	Port ID	Port Description	System Name	Capabilities Supported	Capabilities Enabled	System ID
1/1	3	00:00:00:02:17:03	1/2	1/2		Bridge	Bridge	

Table 62. Remote Device Information Fields

Field	Description
Interface	The device interface that received the LLDP data from the remote system.
Remote ID	The identifier assigned to the remote system that sent the LLDPDU.
Chassis ID	The hardware platform ID for the remote system.
Port ID	The physical address of the port on the remote device that sent the LLDP data.
Port Description	The port description configured on the remote device. If the port description is not configured, the field may show the interface number of the remote port, or it may be blank.
System Name	The system description configured on the remote device. If the system description is not configured, the field is blank.

Field	Description
Capabilities Supported	The capabilities on the remote device. The possible capabilities include other, repeater, bridge, WLAN AP, router, telephone, DOCSIS cable device, and station.
Capabilities Enabled	The capabilities on the remote device that are enabled.
System ID	The reported management IP or MAC addresses of the remote device.

Local Device Information

Use the Local Device Information tab to view LLDP information for switch interfaces.

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

Figure 75. Local Device Information Tab

Interface	Port ID	Port ID Subtype	Port Description
1	1	Interface Name	1
2	2	Interface Name	2
3	3	Interface Name	3
4	4	Interface Name	4
5	5	Interface Name	5

Table 63. Local Interface Information Fields

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


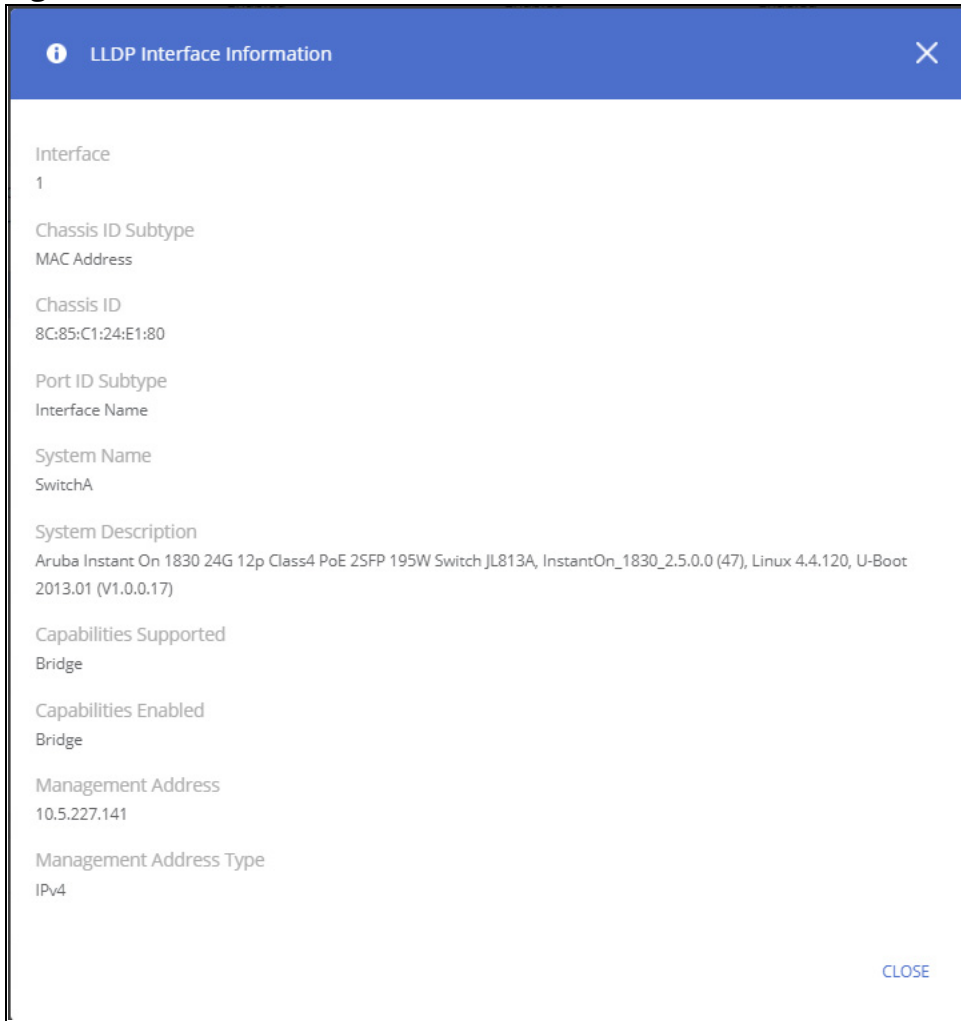
To view additional information about an interface, select the interface row and click **Details**  .

Figure 76. LLDP Interface Information



This page displays the following fields.

Table 64. LLDP Interface Information Fields

Field	Description
Interface	The interface ID.
Chassis ID Subtype	The type of information used to identify the chassis.
Chassis ID	The hardware platform identifier for the switch.
Port ID Subtype	The type of information used to identify the interface
System Name	The user-configured system name for the switch. The system name is configured on the Dashboard page.
System Description	The switch description which includes information about the product model and platform.
Capabilities Supported	The primary function(s) the switch supports.
Capabilities Enabled	The primary function(s) the switch supports that are enabled.

Field	Description
Management Address	The address, such as an IP address, associated with the management interface of the switch.
Management Address Type	The protocol type or standard associated with the management address.

LLDP Statistics

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


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

Figure 77. LLDP Statistics Tile

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

Table 65. LLDP Statistics Fields

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

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

LLDP-MED

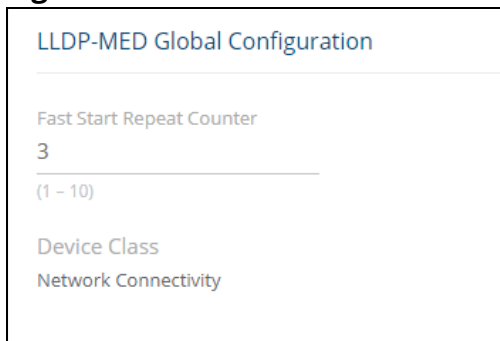
Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) is an enhancement to LLDP that enables:

- Auto-discovery of LAN policies (such as VLAN and Layer 2 Priority settings) for VoIP phones and other network elements.
- Switch location discovery for creation of location databases. For example, this information is used during emergency calls to identify the location of the MED (for VoIP and enhanced 911 services).
- Extended and automated power management of Power over Ethernet (PoE) endpoints.
- Inventory management, enabling network administrators to track their network devices and determine their characteristics (manufacturer, software and hardware versions, serial/asset number).

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

LLDP-MED Global Configuration

Figure 78. LLDP-MED Global Configuration Tile



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

The following global settings display:

Table 66. LLDP-MED Global Configuration Fields

Field	Description
Fast Start Repeat Counter	The number of LLDP-MED Protocol Data Units (LLDPDUs) that are transmitted during the fast start period when LLDP-MED is enabled. The valid range is 1-10. The default is 3.
Device Class	The device's MED classification. The Aruba Instant On 1830 Switch Series switch is classified as a Network Connectivity device.

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

LLDP Global Information

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



The same tile appears in the LLDP page.

Figure 79. LLDP Global Information

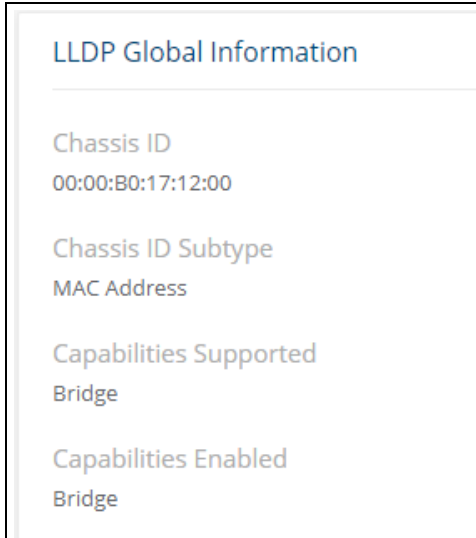


Table 67. LLDP Global Information Fields

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

Interface Configuration

Use this tile to view and configure the interfaces.

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

Figure 80. Interface Configuration Tile

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

The following information is displayed for each port:

Table 68. LLDP-MED Interface Configuration Fields

Field	Description
Interface	The ID of the physical and trunk interfaces.
Link Status	The link status of the interface, which is either Up or Down. An interface that is down does not forward traffic.
MED Mode	The administrative status of LLDP-MED on the interface. When enabled, the LLDP-MED transmit and receive functions are effectively enabled on the interface. This feature is enabled by default.
Notification Status	Indicates whether LLDP-MED topology change notifications are enabled or disabled on the interface. This feature is disabled by default.
Operational Status	Indicates whether the interface is configured to transmit TLVs. To transmit TLVs, the interface must be enabled to receive and transmit LLDPDUs and must be connected to an LLDP-MED switch. The switch waits for the LLDP-MED switch to advertise its information before the switch transmits its own LLDP-MED TLVs, at which point the operational status becomes enabled.
Transmitted TLVs	The LLDP-MED TLV(s) that the interface transmits. The Aruba Instant On 1830 Switch Series switch, can transmit TLVs of the following types: <ul style="list-style-type: none"> • Capabilities • Network Policy • Power Sourcing Entity (PSE)

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

Figure 81. Edit LLDP-MED Interface

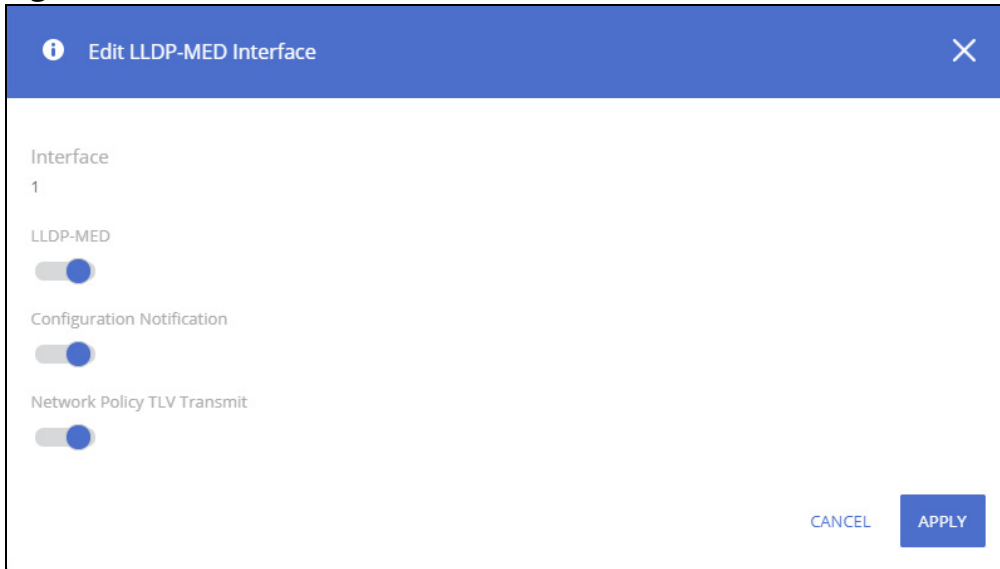


Table 69. Edit LLDP-MED Interface Fields

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

Remote Device Information

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

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

Figure 82. LLDP-MED Remote Device Information Page

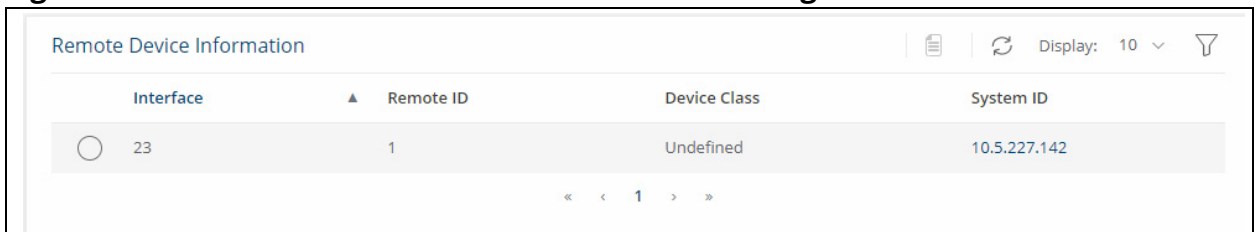



Table 70. LLDP Remote Device Summary Fields

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	The MED Classification advertised by the TLV from the remote device. The following three classifications represent the actual endpoints: <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) The fourth device is Network Connectivity Device, which is typically a device such as a LAN switch or router, IEEE 802.1 bridge, or IEEE 802.11 wireless access point.
System ID	The reported management IP addresses of the remote device.

Displaying Remote Device Details

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

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

Table 71. LLDP Remote Device Information Fields

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

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

Power Over Ethernet (PoE) functionality is supported on certain Aruba Instant On 1830 Switch Series switch models, enabling designated switch ports to provide power to connected devices. These PoE ports are referred to as power source equipment (PSE).

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

The 8-port non-PoE Gigabit Ethernet model can be powered by an upstream PoE switch for environments where no line power is available. Port 1 supports Class 3 PoE with the capability of receiving IEEE 802.3af PoE power up to a maximum of 13W.

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

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

The 1830 Class 4 PoE switches support the IEEE 802.3af/at standards providing 30W of power for Class 4 PD connections while maintaining backwards compatibility with IEEE 802.3af/at standards.

All PoE Class 4 switch ports are capable of delivering 30W per PoE port, up to the maximum power supply budget.

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



The information in this chapter relates to switches that support PoE. This page appears only if the switch supports PoE.

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

Table 72. PoE Maximum Power per Model

Switch	PoE Support	Maximum Power
Aruba Instant On 1830 8G (PD) Switch	1 port class 3 PoE	13W
Aruba Instant On 1830 8G 4p Class 4 PoE 65W Switch	4 ports class 4 PoE	65W
Aruba Instant On 1830 24G 12P Class 4 PoE 2SFP 195W Switch	12 ports class 4 PoE	195W
Aruba Instant On 1830 48G 24P Class 4 PoE 4SFP 370W Switch	24 ports class 4 PoE	370W

PoE Configuration

Use the PoE Configuration Page to view PoE status, consumption history and Port Configuration. To view this page, click **Power Over Ethernet > PoE Configuration** in the navigation pane.




Graphical Display

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

Click the radio buttons to show the related information.

Activity

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

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

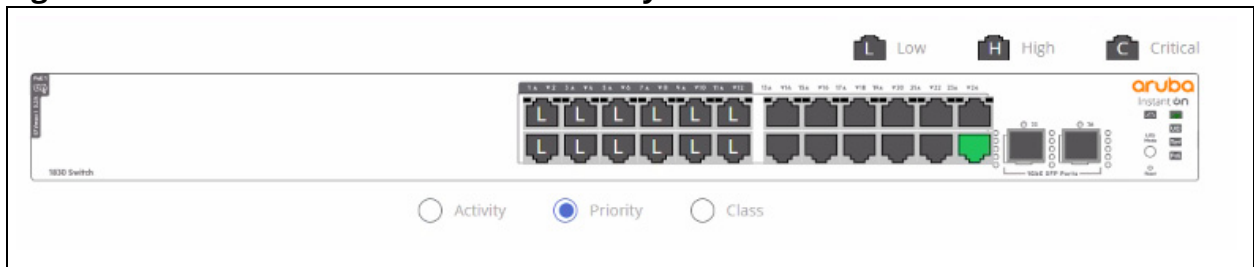
Priority

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

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

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

Figure 83. PoE Switch Panel View - Priority



Class

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

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

Click a PoE port in this screen to open the **Edit Port PoE Configuration** page.

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

Status

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

Figure 84. Status Tile

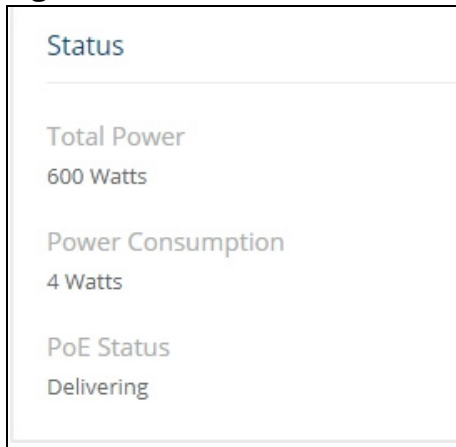


Table 73. Status Fields

Field	Description
Total Power (Watts)	The total power in watts that can be provided by the switch.
Power Consumption (Watts)	The amount of power in watts currently being consumed by connected PoE devices (PD).
PoE Status	The current status of the switch PoE functionality. Possible values are: <ul style="list-style-type: none"> • Delivering—At least one port on the switch is delivering power to a connected switch, and no port is in Fault state. • Idle—The PoE functionality is operational but no ports are delivering power, and no ports have errors. • Faulty—one or more ports is not functioning due to a hardware fault or is in the hardware fault-recovery state. • Not Functional—PoE is not functional on switch due to a hardware failure. • Error—One or more ports is in PoE fault state. this does not include hardware-related fault states.



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

Consumption History

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

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

Figure 85. Consumption History Tile

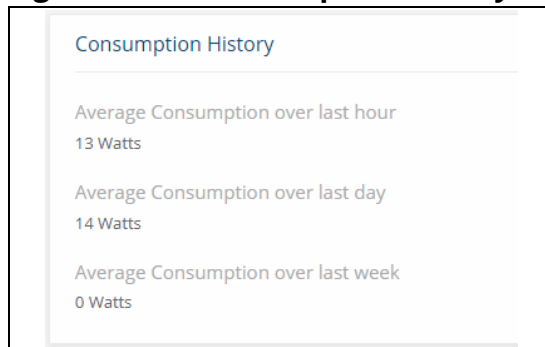


Table 74. Consumption History Fields

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

Port Configuration

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

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

Figure 86. PoE Port Configuration Tile

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

The following settings are displayed.

Table 75. PoE Port Configuration Fields

Field	Description
Interface	The port number.
Admin Mode	Indicates whether PoE is administratively enabled or disabled on the port. This feature is enabled by default.
Priority	The priority of the port when allocating available power. Power is delivered to the higher-priority ports when needed before providing it to the lower priority ports. Possible values are Critical, High and Low. Low is the lowest priority and the default for all ports.
Schedule	The scheduled time when source power is available on this port. Options are: <ul style="list-style-type: none"> None—Source power is available at all times. This is the default selection. Schedule 1—Source power is available during the configured schedule in Schedule 1. Schedule 2—Source power is available during the configured schedule in Schedule 2. Schedule 3—Source power is available during the configured schedule in Schedule 3. You can configure schedules on the Schedule Configuration page in Setup Network.
Class Limit	By default, the power is not limited <ul style="list-style-type: none"> The class limit of a port can be set to class 3 or unlimited.
Pre-Standard Detection	Indicates whether Pre-Standard Detection is allowed. The 4-point detection scheme defined in IEEE 802.3 is used by default. If this mechanism fails to detect a connected PD, and pre-standard detection is allowed, then pre-standard detection is used.
Power Management Mode	Select the method by which the PoE controller determines supplied power. Possible values are: <ul style="list-style-type: none"> Class—The power allocated to each port is reserved and is not available to any other port, even when less than the maximum allocation is being used. Usage—The power allocated to each port is not reserved. Unused power may be allocated from one port to another as needed, up to the power limit defined for each port. This is the default selection.
Status	The status of the port as a provider of Power over Ethernet. Such devices are referred to as power-sourcing equipment (PSE). Possible values are: <ul style="list-style-type: none"> Disabled—The operational status of the PSE is disabled. Delivering Power—The PSE is delivering power. Fault—The PSE has experienced a fault condition. Searching—The PSE is transitioning between states. Recovering—the port is recovering from a previous condition of internal hardware fault.
Output Power	Power consumed on port, in watts.

Field	Description
Fault Status	<p>Indicates the type of fault condition that exists on the port . Possible values are:</p> <ul style="list-style-type: none"> • None - the port is not in fault condition. • Short - a Short fault condition exists on the port. • Overload - a PoE Overload fault condition exists on the port. • Power Denied - Power on port is denied due to power over-subscription condition on the switch. • Hardware Fault - a general Hardware fault occurred on the switch which prevents power on port • Internal HW Fault - a hardware fault occurred on the interface. • Other - a fault of a type not specified above occurred on the port. <p>NOTE: This field is relevant only if the status of the port is Fault.</p>

Edit Port PoE Configuration



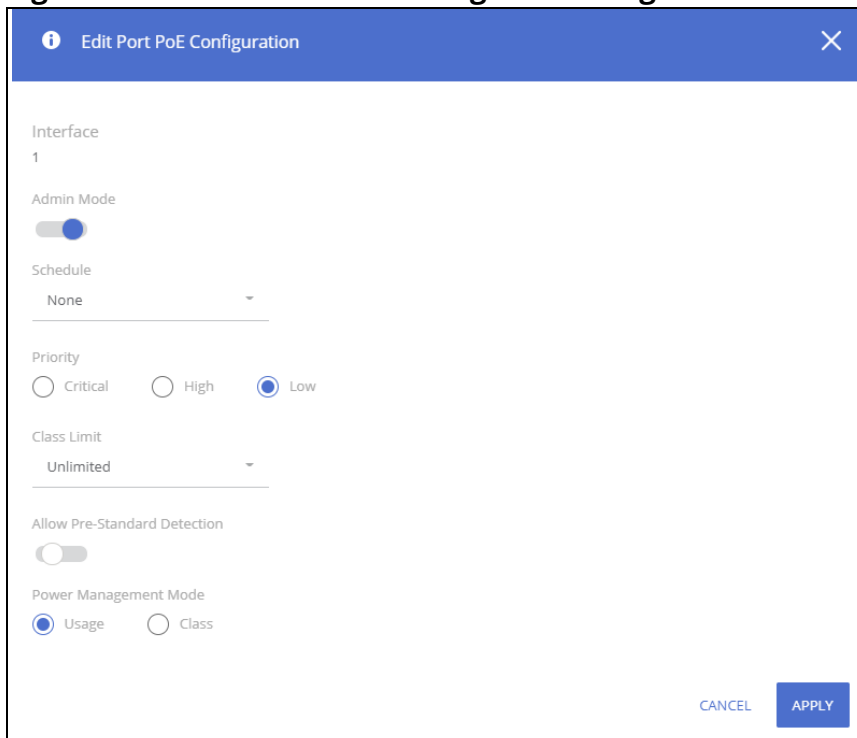
To change PoE settings for a port, select the checkbox associated with it and lick **Edit**  . Or, click **Edit All**  to configure all PoE enabled ports at the same time.

Figure 87. Edit Port PoE Configuration Page



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

PoE Port Details


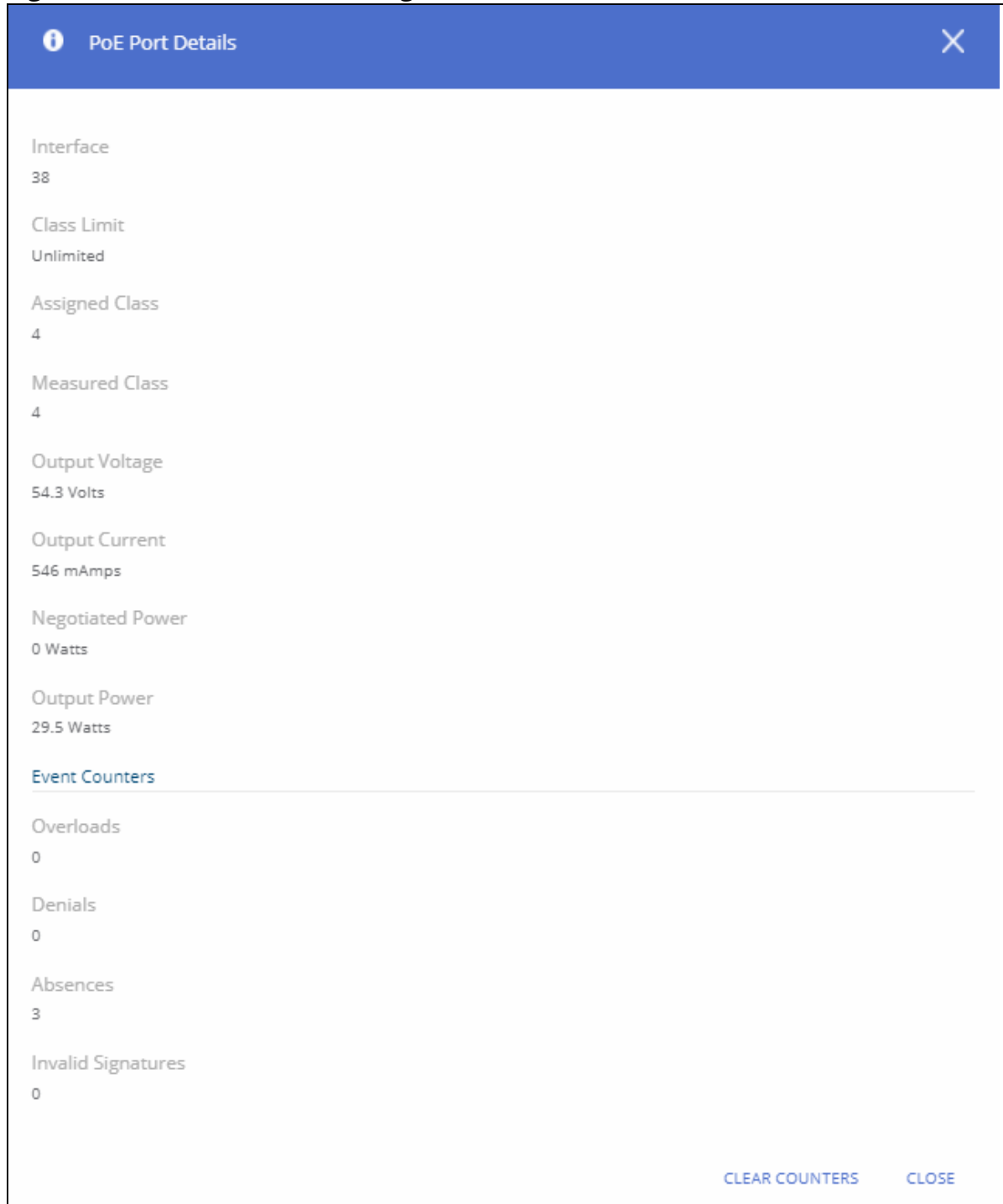
To view additional PoE configuration information for a port, select the port and click **Details**  .

Figure 88. PoE Port Details Page



The screenshot displays a modal window titled "PoE Port Details" with a close button (X) in the top right corner. The content is organized into several sections:


- Interface:** 38
- Class Limit:** Unlimited
- Assigned Class:** 4
- Measured Class:** 4
- Output Voltage:** 54.3 Volts
- Output Current:** 546 mAmps
- Negotiated Power:** 0 Watts
- Output Power:** 29.5 Watts
- Event Counters:**
 - Overloads: 0
 - Denials: 0
 - Absences: 3
 - Invalid Signatures: 0


At the bottom right of the modal, there are two buttons: "CLEAR COUNTERS" and "CLOSE".

Table 76. PoE Port Details Fields

Field	Description
Class Limit	Shows the class limit: <ul style="list-style-type: none"> • Unlimited • Class 3
Measured Class	The class of power requested by the powered device. Possible values are Unknown and Class 0 through Class 4. A higher class value indicates that the switch provides higher power.
Assigned Class	The class of power actually supplied to the powered device. This class may be lower than the measured class because of lack of available power or if the port does not support the measured class.
Output Voltage	The voltage being applied to the connected switch.
Output Current	The current in milliamps being drawn by the connected switch.
Negotiated Power	Power in watts negotiated between the port and connected switch.
Output Power	Power in watts being drawn by the connected switch.
Event Counters	
Overloads	The number of power overload events detected on the port.
Denials	The number of times that the powered device was denied power.
Absences	The number of times that power was stopped to the powered device, because the powered device was not detected.
Invalid Signatures	The number of that an invalid signature was received. Signatures are the means by which the powered device identifies itself to the PSE. Signatures are generated during powered device detection, classification, or maintenance.



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

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

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. The priority of a packet arriving at an interface can be used to steer the packet to the appropriate outbound CoS queue through a mapping table. CoS queue characteristics that affect queue mapping, such as minimum guaranteed bandwidth, transmission rate shaping, etc., are user-configurable at the queue (or port) level.

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

802.1p Priority Mapping

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

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

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

Figure 89. 802.1p Priority Mapping Tile

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

Table 77. 802.1p Priority Mapping Configuration Fields

Field	Description
802.1p Priority	The 802.1p priority value to be mapped.
Traffic Class	The internal traffic class to which the corresponding 802.1p priority value is mapped. The default value for each 802.1p priority level is displayed for reference.

Configuring 802.1p CoS Mapping

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

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

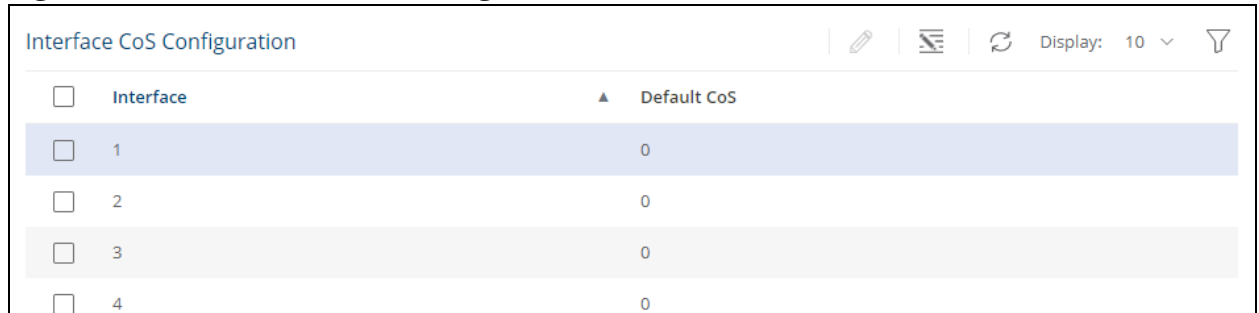
Your changes take effect immediately but are not retained across a switch reset unless you click **Save Configuration**.

Interface CoS Configuration

Use the **Interface CoS Configuration** page to configure the Default CoS to all ports or to a specific port.

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

Figure 90. Interface Cos Configuration Tile




Interface	Default CoS
<input type="checkbox"/> 1	0
<input type="checkbox"/> 2	0
<input type="checkbox"/> 3	0
<input type="checkbox"/> 4	0

Table 78. Interface CoS Configuration Fields

Field	Description
Interface	Selects the CoS configurable interface to be affected by the Interface Shaping Rate.
Default 802.1p Priority	Sets the default CoS for the interface.

Configuring the CoS on an Interface

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

To configure the CoS for one or more interfaces:



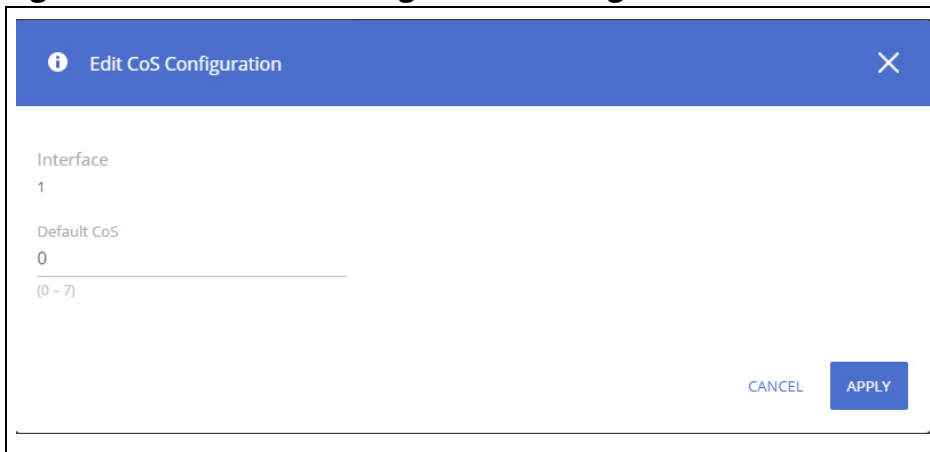

1. Select each interface to configure and click **Edit** . If you select multiple interfaces, or if you use **Edit All** , the same settings are applied to all selected interfaces. The **Edit CoS Configuration** dialog box appears.

Figure 91. Edit CoS Configuration Dialog Box



The dialog box titled "Edit CoS Configuration" features a blue header bar with an information icon on the left and a close button on the right. Below the header, the "Interface" field contains the value "1". The "Default CoS" field contains the value "0", with a range indicator "(0 - 7)" positioned below it. At the bottom right of the dialog, there are two buttons: "CANCEL" and "APPLY".

2. Specify the Default 802.1p Priority value for all interfaces identified in the Interface field(s).
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** .

Overview

The Aruba Instant On 1830 Switch Series series switch software includes a robust set of built-in security features to secure access to the switch management interface and to protect the network.

Denial of Service Protection

The Aruba Instant On 1830 Switch Series switches include Denial-of-Service (DoS) and ICMP (ping) protection features to help protect against various high-volume traffic scenarios or malicious attacks.

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



For some of the settings, the DoS feature does not generate notifications (such as error messages, SYSLOG messages, or SNMP traps) if a DoS attack occurs. The switch will simply drop DoS-related packets.

The ICMP security options help prevent the switch and the network from attacks that involve issues with the ICMP echo request packets (pings) that the switch receives.

To display the Global Settings tile, click **Security > Denial of Service Protection** in the navigation pane.

Global Settings

Figure 92. Global Settings

Global Settings

Interface Level DoS Protection

Block SYN-FIN Packets

SYN Protection Mode

Disabled Log **Log and Block**

SYN Protection Threshold

80

(20 - 200) Packets per Second

SYN Protection Period

60

(10 - 600) Seconds

Table 79. Global Setting Fields

Field	Description
Interface Level DoS Protection	Enable this option to enable Interface level DoS settings (see SYN Attack Status Tab for more information).
Block SYN-FIN Packets	Enable this option to drop, on all interfaces, TCP packets in which both SYN and FIN flags are set.
SYN Protection Mode	Enables SYN Protection on the switch. SYN Protection detects TCP SYN traffic sent to the switch IP address(es) above the defined threshold and acts accordingly. Possible values are: <ul style="list-style-type: none"> Disabled - SYN Protection is disabled on the switch. This is the default setting. Log - SYN Protection is enabled on the switch. If the TCP SYN traffic rate on a certain interface is higher than the defined threshold, the violation is report through Syslog. Log and Block - SYN Protection is enabled on the switch. If the TCP SYN traffic rate on a certain interface is higher than the defined threshold, the violation is reported through Syslog. In addition, all TCP SYN traffic on the interface is dropped for the specified duration.
SYN Protection Threshold	Defines The threshold applied to interface to activate SYN protection. Valid range is 20-200 Packets per second. Default is 80 Packets per second.
SYN Protection Period	The timeout (in seconds) after which an interface blocked by this feature gets unblocked. This setting is available only if SYN Protection mode is set to Log and Block. NOTE: If a SYN attack is still active on this interface it might become blocked again. Range is 10-600 seconds, default is 60 seconds.

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

Syn Attack Status/Interface Settings Tile

To view the SYN attack status, click the **SYN Attack Status** tab.

To view the Interface settings information, click the **Interface Settings** tab.

SYN Attack Status Tab

The SYN Attack Status tab displays the TCP SYN Protection status and last SYN attack on each interface.

Figure 93. SYN Attack Status Tab

Interface	Status	Last SYN Attack
1	Normal	
2	Normal	
3	Attacked	14-Dec-2021 07:07:16 Blocked and Logged
4	Normal	

Table 80. SYN Attack Status Fields

Field	Description
Interface	Interface identifier.
Status	Current status of the interface. Possible values are: <ul style="list-style-type: none"> Normal - TCP SYN protection is not enabled or the interface is not under a TCP SYN attack. Attacked - Interface is currently under a TCP SYN attack.
Last SYN Attack	The last time stamp in which the switch identified a SYN attack on this interface.

Interface Settings Tab

The Interface Settings tab enables configuring and provides information on the ICMP Attack Prevention and SYN Rate Protection settings for the interfaces.



The **Interface Setting** tab is enabled only if **Interface Level Dos Protection** state is enabled. Settings configured on interfaces are active only if the **Interface Level Dos Protection** setting is enabled.

Figure 94. Interface Settings

Interface	ICMP Attack Prevention	SYN Rate Protection
1	Disabled	Disabled
2	Enabled	Enabled

Table 81. Interface Settings Fields

Field	Description
Interface	Interface identifier.
ICMP Attack Prevention	Enabled or Disabled. If enabled, the interface will drop any ICMP request packet received on the interface. By default, ICMP Attack Prevention is disabled.
SYN Rate Protection	Enabled or Disabled. If enabled on an interface, this setting limits ingress TCP packets with the following flag settings to 250 packets per second: <ul style="list-style-type: none"> • SYN=1 • ACK=0 • FIN=0 Packets above the rate are dropped. By default Syn Rate Protection is disabled.

To change the setting for one or more interfaces, select it and click **Edit** . Or, click **Edit All** to configure all interfaces at the same time.

The **Edit Interface Settings** dialog box appears. Set the **ICMP Attack Prevention** and the **SYN Rate Protection** as required, and click **APPLY**.

HTTPS Certificate

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

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

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

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

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

In order to enable users to benefit from a secured connectivity, without the need to sign a certificate by a CA - the switch also supports use of unsigned certificates (also known as self-signed certificates). While not useful for proving switch identify to the browser, the self-signed certificates enable securing the management session using the public and private key.

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

HTTPS Certificate Settings

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

Figure 95. HTTPS Certificate Settings Tile

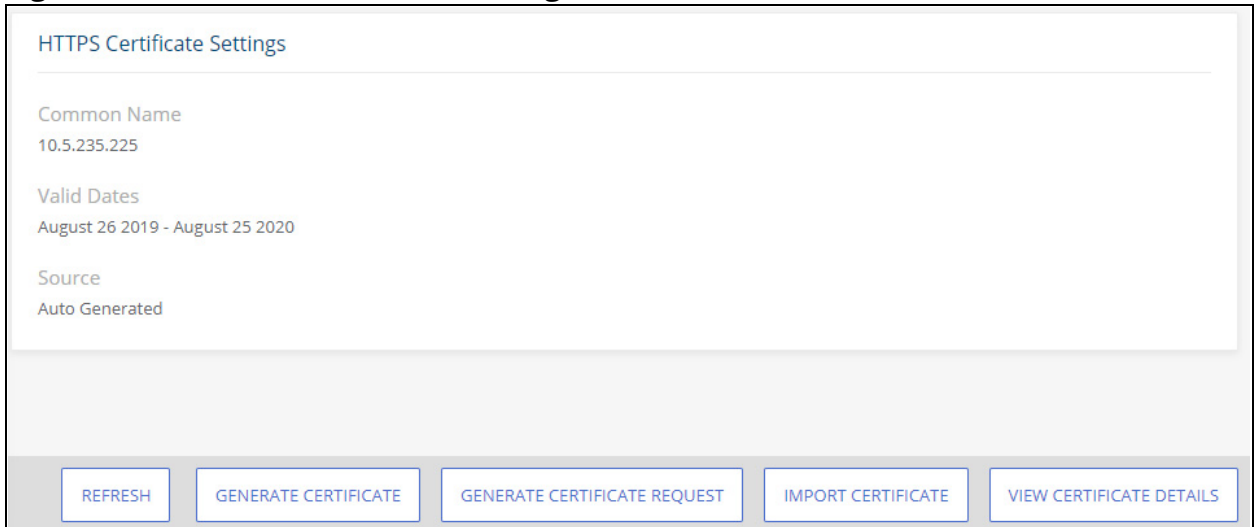


Table 82. HTTPS Certificate Settings Fields

Field	Description
Common Name	Specifies the fully qualified switch URL or IP address.
Valid Dates	The start and end dates for the certificate.
Source	Specifies whether the certificate was generated by the system (auto generated) or by the user (self defined).

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

Generate a Self-Signed Certificate

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

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

Figure 96. Generate Certificate Dialog Box

Generate Certificate

Common Name
0.0.0.0
(1 - 64 characters)

Organization Unit
(0 - 64 characters)

Organization Name
(0 - 64 characters)

Location
(0 - 64 characters)

CLEAR CANCEL APPLY

Enter the following fields:

Table 83. Generate Certificate Fields

Field	Description
Common Name	Enter the fully qualified switch URL or IP address. If unspecified, defaults to the lowest IP address of the switch at time of generation.
Organization Unit	Enter the organization unit or department name. If unspecified, field is left empty.
Organization Name	Enter the organization name. If unspecified, field is left empty.
Location	Enter the location or city name. If unspecified, field is left empty.
State	Enter the state or province name. If unspecified, field is left empty.
Country	Enter the country name abbreviation. If unspecified, field is left empty.
Duration	Enter the number of days that the certificate is valid. If unspecified, the duration is set to 365 days (1 year).
Regenerate RSA Key	Enable this feature to regenerate a pair of RSA keys. If disabled, the existing key set is used.
RSA Key Length	Select the preferred key length. By default, key length is 2048.

Using a Certificate Signed by a Certificate Authority

In order to use a certificate that is signed by a Certificate Authority (CA), you need to complete the following steps:

1. Generate a certificate request: Click **GENERATE CERTIFICATE REQUEST** and enter the fields as defined in [Generate a Self-Signed Certificate](#).



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

2. Export the certificate for signing: In the **Certificate Request** box that appears, click **COPY TO CLIPBOARD** to copy the generated certificate request to a file, and send the file to the CA for signing.
3. After the Certificate is signed by a CA, import it back to the device. The certificate needs to be imported as a PEM encoding/file type. Import the signed certificate: Click **IMPORT CERTIFICATE** and copy the certificate, and optionally RSA keys and the Public Key that you received from the CA to the dialog box fields (see ["Import Certificate Dialog Box"](#)).
 - If keys are imported together with the certificate, the public key found in the certificate must match the imported key.
 - If keys are not imported with the certificates, the public key found in the certificate must match the public key stored on the switch.
4. After copying the keys, click **APPLY**.
Importing a CA signed certificate overrides the certificate currently used on the switch.

Figure 97. Import Certificate Dialog Box

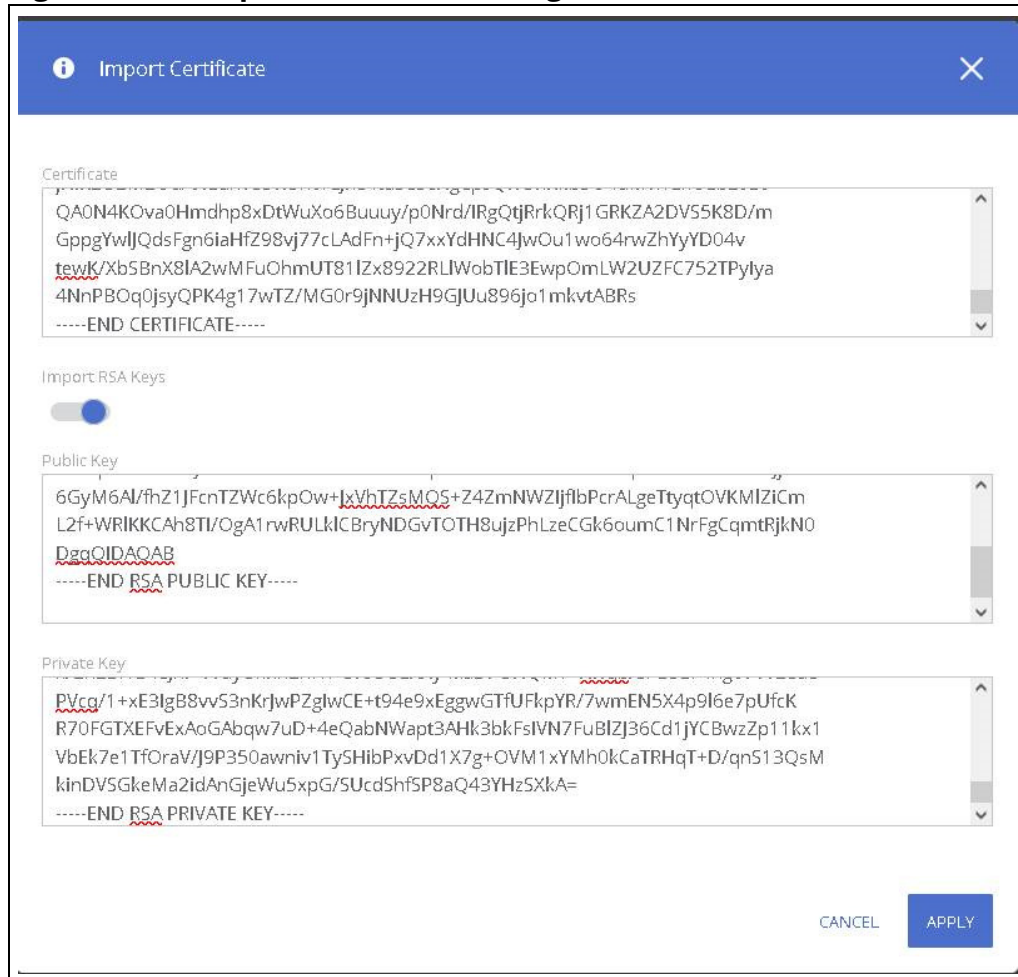


Table 84. Import Certificate Fields

Field	Description
Certificate	Paste the signed certificate into this text box.
Import RSA Keys	Enable if you need to import RSA keys.
Public Key	If Import RSA Keys is enabled, paste the public key to this text box.
Private Key	If Import RSA Keys is enabled, paste the private key to this text box.

View a Certificate

To view the current certificate details, click the **VIEW CERTIFICATE DETAILS** button.

Figure 98. Certificate Details

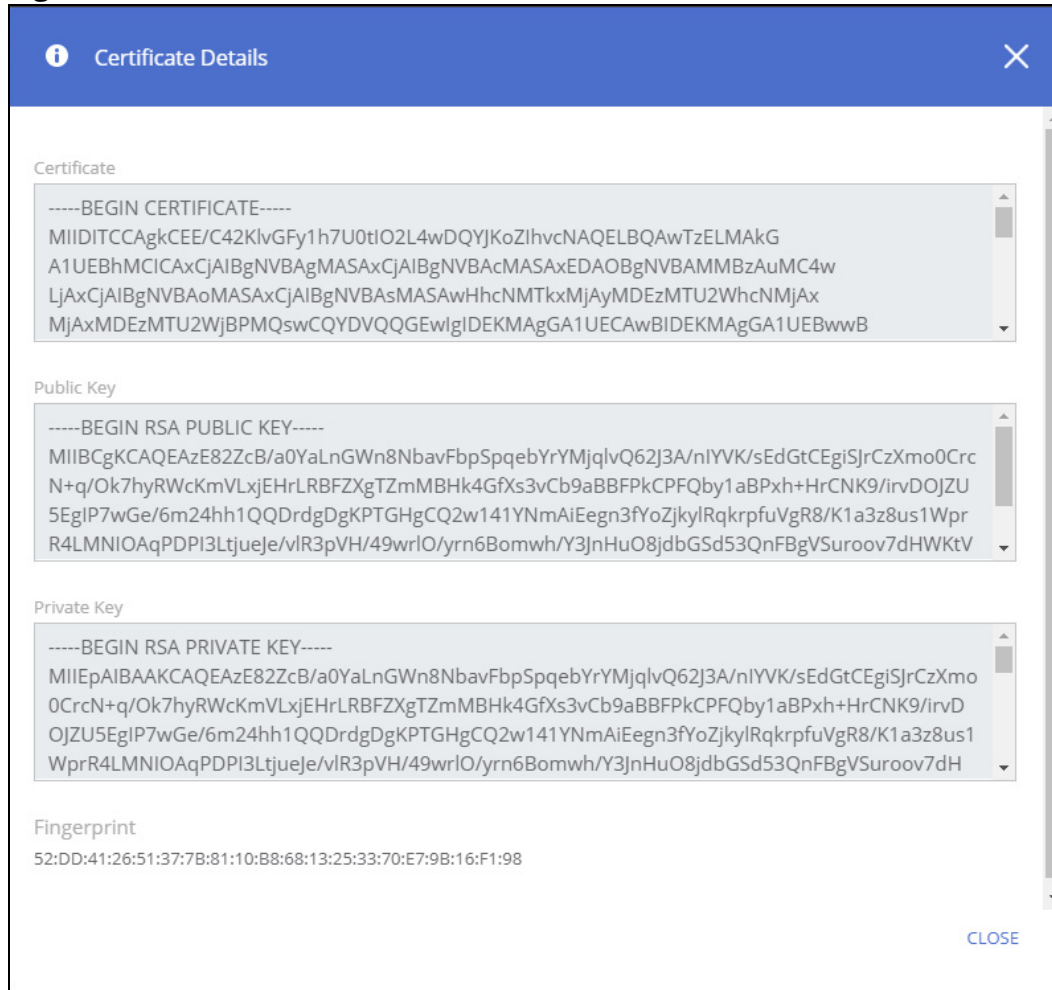


Table 85. Certificate Details Fields

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

You can use the Diagnostics pages to help troubleshoot network issues, view log and configuration information.

Logging

To configure log setting and display the Logging page, click **Diagnostics** > **Logging** in the navigation pane.

Unexpected Restart Information

The **Unexpected Restart Information** tile appears only if an unexpected restart that hasn't been cleared is registered on the switch. When an unexpected restart has occurred a notification appears on the masthead. When this notification icon is clicked, the application navigates to this page.

If there has been an unexpected restart of the switch, additional information is displayed near the top of the Logging page to alert the user of the event. The Crash Log text box displays information about the restart event, which may be helpful to technical support in diagnosing its cause. The crash log is part of the Log File entries (see [Log File](#) for more information). The file stored into non-volatile memory so that it is preserved upon reboot.

When the switch is reset to factory defaults, all crash log information is erased.

Figure 99. Unexpected Restart Information Tile



To clear the unexpected restart alert, click **Clear Unexpected Restart** this clears the unexpected restart notification from the masthead, and the **Unexpected Restart Information** tile. You can click **Save Crash Log** to save the contents of the crash log to a text file using the browser save functionality.

Global Log Settings

Use this tile to define buffered logging settings. These log messages are not preserved across device reboots.

Figure 100. Global Log Settings

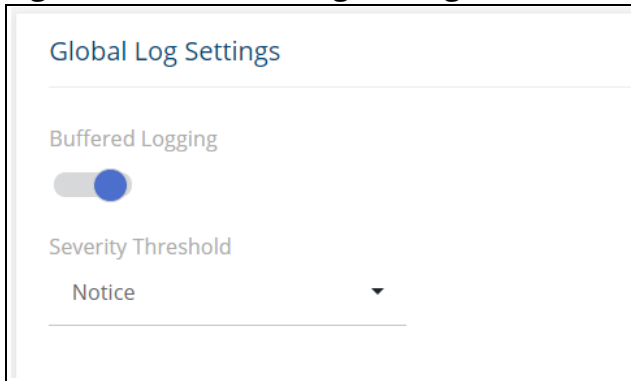


Table 86. Global Log Settings Fields

Field	Description
Buffered Logging	Enable or disable buffered logging.
Severity Threshold	Choose the appropriate severity threshold from the drop-down button. The severity can be one of the following (lowest to highest): <ul style="list-style-type: none">• Debug—The switch is providing debug-level information.• Info—The switch is providing non-critical information. This is the default level.• Notice—The switch is experiencing normal but significant conditions.• Warning—The switch is experiencing conditions that require user attention.• Error—The switch is experiencing non-urgent failures.• Critical—The switch is experiencing primary system failures.• Alert—Action must be taken immediately.• Emergency—The switch is unusable. When selecting a certain severity threshold the switch will provide that severity and all higher severity.

Remote Log Server

Use this tile to enable logging messages to a remote SYSLOG server, and to define the server address and other settings.

Figure 101. Remote Log Server

Remote Log Server

Syslog Host

Server Address
(IPv4 or IPv6)

UDP Port
514
(1 - 65535)

Severity Threshold
Warning

Table 87. Remote Log Server Fields

Field	Description
Syslog Host	Enables and disables logging to configured syslog host. When the syslog admin mode is disabled, the switch does not relay logs to syslog host. When enabled, messages are sent to configured host. This feature is disabled by default
Server Address	The IP address of the remote host that receives the log messages. The address can be one of the following: <ul style="list-style-type: none">• IPv4 address• IPv6 global address, in the format of X:X:X::X• Hostname - specify the server hostname
UDP Port	The UDP port, on the logging host, to send syslog messages. The port ID can be any value from 1 to 65535. The default is 514
Severity Threshold	Choose the appropriate severity threshold from the drop-down button. See descriptions for the available levels in Global Log Settings Fields

Buffered Log/Log File

To view the Buffered Log information, click the **Buffered Log** tab.

To view the Log File information, click the **Log File** tab.

Buffered Log

The log messages that the switch generates in response to events, faults, errors, and configuration changes are stored locally on the switch in the RAM (cache). This collection of log files is called the buffered log. When the buffered log file reaches the maximum size, the oldest message is deleted from the RAM when a new message is added. If the system restarts, all messages are cleared. The Log page displays the 200 most recent system messages, such as configuration failures and user sessions. The newest log entry, by default, is displayed at the top of the list.



If more than 1000 logs accumulate, their Log Index numbers continue to increment beyond 1000 and the oldest entries are deleted (for example, if 1400 log entries were generated since the system was last restarted or the log file was cleared, then the log file would display entries 1001 to 1400).


To view this tab, click **Diagnostics > Logging** in the navigation pane, and click the **Log File** tab in the **Buffered Log/Log File** Tile.

Figure 102. Buffered Log Tab

Index ▲	Log Time	Severity	Component	Description
1	Oct 7 2021 01:08:25	Notice	SYSLOG-N-LOGGING	Logging started.
2	Oct 7 2021 01:08:13	Info	BOOTP_DHCP_CL-I DHCPCONFIGURED	The device has been configured on interface Vlan 1 , IP 10.5.227.151, mask 255.255.255.224, DHCP server 10.5.227.131

Table 88. Buffered Log Tab Fields

Field	Description
Index	The log number.
Log Time	Time at which the log was created.
Severity	The severity level associated with the log message. The severity can be one of the following: <ul style="list-style-type: none">• Emergency—The switch is unusable.• Alert—Action must be taken immediately.• Critical—The switch is experiencing primary system failures.• Error—The switch is experiencing non-urgent failures.• Warning—The switch is experiencing conditions that require user attention.• Notice—The switch is experiencing normal but significant conditions.• Info—The switch is providing non-critical information.• Debug—The switch is providing debug-level information.
Component	The system component that issued the log entry.
Description	A text description of the event.

Click **Clear**  to delete all log messages. You may be required to confirm the delete before the logs are removed.

For information on configuring log settings, see [Global Log Settings](#).

Log File

The system sends logging messages to the local flash (Log file). When using this feature, all events with error level and higher are logged to a flash Log file and will be available for viewing even after system reboot.

When the log file reaches the maximum size, the oldest message is deleted from the flash when a new message is added.



If more than 200 logs accumulate in flash, their Log Index numbers continue to increment beyond 200 and the oldest entries are deleted (for example, if 400 log entries were generated since log file was cleared, then the log file would display entries 201 to 400).


To view this tab, click **Diagnostics > Logging** in the navigation pane, and click the **Log File** tab in the **Buffered Log/Log File** Tile.

Figure 103. Log File Tab



Table 89. Log File Tab Fields

Field	Description
Index	The log number.
Log Time	Time at which the log was created.
Severity	The severity level associated with the log message. The severity can be one of the following: <ul style="list-style-type: none"> Emergency—The switch is unusable. Alert—Action must be taken immediately. Critical—The switch is experiencing primary system failures. Error—The switch is experiencing non-urgent failures. Warning—The switch is experiencing conditions that require user attention. Notice—The switch is experiencing normal but significant conditions. Info—The switch is providing non-critical information. Debug—The switch is providing debug-level information.
Component	The system component that issued the log entry.
Description	A text description of the event.

Click **Clear**  to delete all log messages. You may be required to confirm the delete before the logs are removed.

Ping

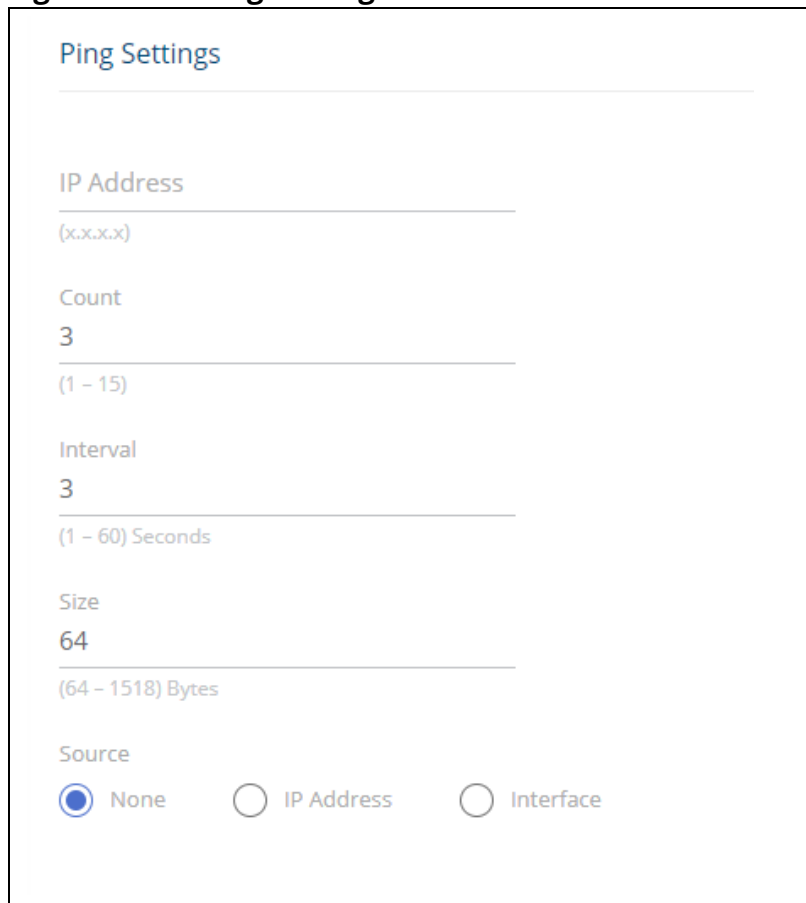
A ping request is an Internet Control Message Protocol (ICMP) echo request packet. The switch supports ICMP for sending ping requests to IPv4 addresses.

Ping Settings

Use the Ping Settings tab to send one or more ping requests from the switch to a specified IPv4 address. You can use the ping request to check whether the switch can communicate with a particular host on an IP network. The information you enter on this page is not saved as part of the switch configuration.

To display the Ping Settings tab, click **Diagnostics** > **Ping** in the navigation pane.

Figure 104. Ping Settings Tab



The screenshot shows the 'Ping Settings' configuration page. It features several input fields and a radio button group. The fields are: 'IP Address' with a placeholder '(x.x.x.x)', 'Count' with a value of '3' and a range '(1 - 15)', 'Interval' with a value of '3' and a range '(1 - 60) Seconds', and 'Size' with a value of '64' and a range '(64 - 1518) Bytes'. At the bottom, there is a 'Source' section with three radio buttons: 'None' (selected), 'IP Address', and 'Interface'.

Table 90. Ping Settings Fields

Field	Description
IP Address	Specify the IP address you want to reach.
Count	Specify the number of packets to send. The range is 1 to 15 packets and the default is 3 packets.
Interval	Specify the delay between ping packets. The range is from 1 to 60 seconds, and the default is 3 seconds.
Size	Specify the size of the ping packet to be sent. Changing the size allows you to troubleshoot connectivity issues with a variety of packet sizes. The range is from 0 to 1518 bytes, and the default is 64 bytes.
Source	The source IP address or interface to use when sending a ping request which can be one of the following: <ul style="list-style-type: none"> • None – No specific source is required. • IP Address – Use the IP address specified in the Source IPv4 Address field as the source. • Interface – Use the specified switch interface as a source.
Source IP Address	The source IP address to use when sending a ping request. This field is enabled when IP Address is selected as the source option.
Source Interface	The interface to use when sending a ping request. This field is enabled when Interface is selected as the source option. The default interface to use is the network port.

Click **APPLY** to ping the specified host. Click **Stop Ping** to end a ping in progress. If you do not click **Stop Ping**, the pings continue until the number of pings specified in the Count field has been reached — even if you navigate away from the Ping IPv4 page.

The results of the ping operation can be viewed in the **Ping Results** tile.

Ping Results

This tile shows the Ping status and results.

Table 91. Ping Results Fields

Field	Description
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. • 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 switch that was pinged. • The Internet Control Message Protocol (ICMP) number of the packet, starting from 1. • The time it took to receive a reply, in microseconds. • The number of ping packets sent and received, the percent of packets that were lost, and the minimum, average, and maximum round-trip time for the responses in milliseconds.

Support File

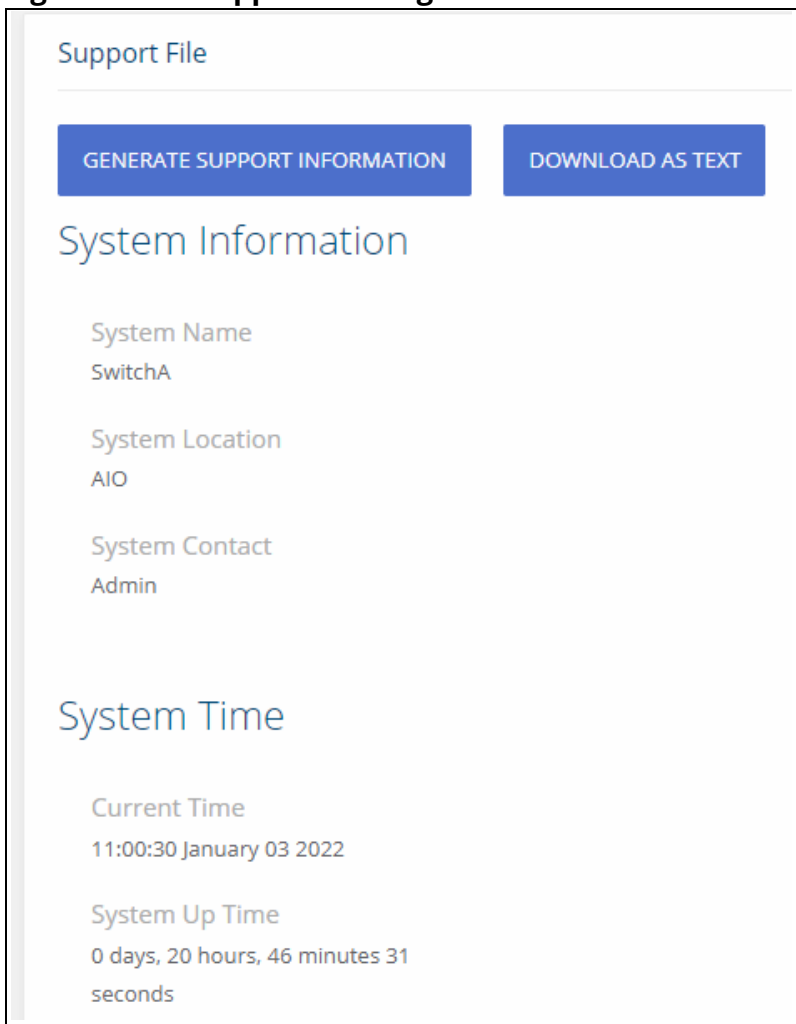
Use the support file page to display summary information for the switch on a single page.

To display the Support File page, click **Diagnostics > Support File** in the navigation pane and click the **GENERATE SUPPORT INFORMATION** button. The **Support File Page** shows a partial view of the resulting information.



Generating the support file may take several minutes. During this time switch management will not be available.

Figure 105. 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.

- System Time— Current Time and System Up Time.
- Device Information— Software and OS versions.
- System Resource Usage— CPU and memory usage data.
- Image Status and Image Description— The active and backup image status and versions.
- Buffered Log and Configuration— Messages and logging configuration details.
- Syslog Configuration— Syslog status and remote port and address information.
- Locator LED Configuration— Locator LED status.
- MAC Table— Address forwarding table and summary statistics.
- Time Configuration and Time Zone— SNTP client status and time zone configuration.
- Daylight Saving Time— The daylight saving time mode on the system.
- Date Range and Recurring Date— Configuration of the date range or recurring date.
- Network Details— Switch IP and MAC addresses.
- Web Parameters and Management Access— Web session timeout and access port and management VLAN information.
- User Accounts and Passwords— User access, logged-in users, and password manager configuration.
- Port Status and Port Summary Statistics— Port and trunk configuration details, summary, and statistics.
- Port Mirroring Configuration— Enable/disable status and source and destination port configuration
- Flow Control and Storm Control Configuration— Enable/disable status.
- Spanning Tree Switch Configuration — Global and per-port configuration, status, and statistics.
- Loop Protection Configuration and Status— Per interface configuration and statistics
- IGMP Snooping— Enable/disable information and statistics
- SNMP— SNMP v1 information.
- 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
- CoS— 802.1p CoS mapping per interface, CoS interface queue configuration.
- Auto DoS Features— Enable/disable status.
- ICMP Settings— Global ICMP configuration.
- Green Features (EEE) Configuration— Global and per-port enable/disable status and power consumption data
- PoE Configuration— On switches that support PoE, global and per-port configuration and schedule settings.

Support file information can be saved and downloaded to management system using the native browser file system. The name of the downloaded file is SupportFile.htm.

To download the support file, click the **DOWNLOAD AS TEXT** button. This button is only displayed after the support information is gathered and shown in the screen.

Cable Test

This feature detects and reports potential cabling issues, such as cable opens, or cable shorts, on Copper Links. This feature also provides distance to the fault if exists, and total length of cable.

Cable length measurement is available when link is up. Length is automatically detected. Length reports has a minimum Length of 50Meter and is provided with a 30 meter resolution (up to 50, 50 to 80, 80 to 110 etc)



Only short circuits across wires within a pair are reported. If there is a short circuit across wires not in a pair, it will not be reported.

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

Interface Configuration


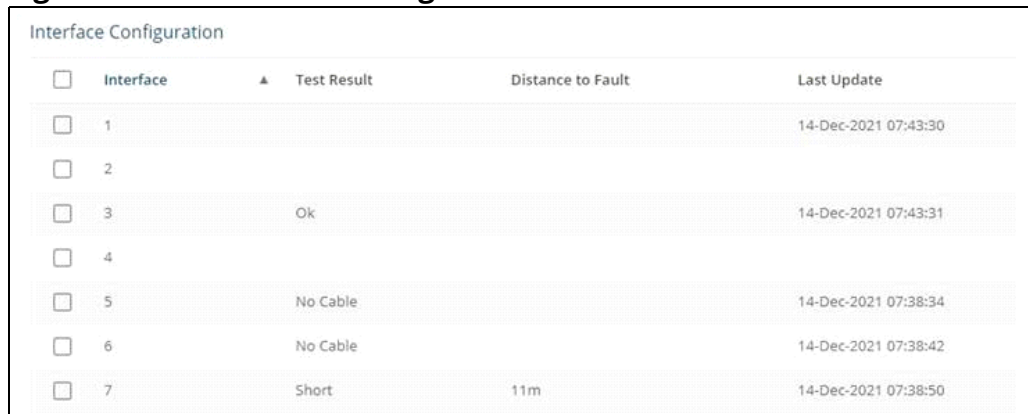
This tile shows the interface configuration of the cables. To run a test, select one or more interfaces and click the **Test**  button.

Figure 106. Interface Configuration



<input type="checkbox"/>	Interface	▲ Test Result	Distance to Fault	Last Update
<input type="checkbox"/>	1			14-Dec-2021 07:43:30
<input type="checkbox"/>	2			
<input type="checkbox"/>	3	Ok		14-Dec-2021 07:43:31
<input type="checkbox"/>	4			
<input type="checkbox"/>	5	No Cable		14-Dec-2021 07:38:34
<input type="checkbox"/>	6	No Cable		14-Dec-2021 07:38:42
<input type="checkbox"/>	7	Short	11m	14-Dec-2021 07:38:50

Table 92. Interface Configuration Fields

Field	Description
Interface	The interface ID.
Test Result	This field appears only after a test was run on the interface. These are the test result options: <ul style="list-style-type: none">• Ok• No cable is connected• Open cable• Shorted cable• Unknown
Distance to Fault	This field appears only after a test was run on the interface. In the case of a fault, this column shows the distance to the fault.

Field	Description
Last Update	This field appears only after a test was run on the interface. The last time a test was activated on this interface.
Cable Length	Length reports has a minimum Length of 50Meter and provides a 30 meter resolution (up to 50, 50 to 80, 80 to 110, and so on) NOTE: Cable length info is not available for interfaces running in speeds lower than 1 Gbps.
Port Status	Displays the current port status.



Cable status test requires activation, per-interface by user. Activation of the test will cause link down state for a few milliseconds.

MAC Table

The MAC address table keeps track of the Media Access Control (MAC) addresses associated with each port. This table enables the switch to forward unicast traffic through the appropriate port. The MAC address table is sometimes called the bridge table or the forwarding database. The address table supports up to 16K MAC address entries for the 24 and 48 port devices, and 8K for the 8 port devices.

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

MAC Address Table

Figure 107. MAC Address Table Tile

MAC Address Table					Display: 10
VLAN ID	MAC Address	Interface	Interface Index	Status	
1	00:00:00:11:11:11	47	47	Learned	
1	00:00:44:44:55:88	CPU	0	Management	
1	00:22:12:52:03:77	47	47	Learned	

Table 93. MAC Address Table Fields

Field	Description
VLAN ID	The VLAN with which the MAC address is associated.
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a six-byte MAC address, with each byte separated by colons.

Field	Description
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 <i>SNMP</i> to manage the switch.
Status	<p>Provides information about the entry and why it is in the table. Possible values are the following:</p> <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. • Other—The address was added dynamically through an unidentified protocol or method.

You can use the maintenance pages to upgrade software, save the switch configuration, and select which of two software images is the active image and which is the backup image.

Dual Image Configuration

The switch can store up to two software images. One image is the active image and the other is the backup image (not actively running on the switch). You can select which image to load during the next boot cycle and add a description for each image on the switch.

To display the Dual Image Configuration page, click **Maintenance** > **Dual Image Configuration**.

Figure 108. Dual Image Configuration Page

The screenshot shows the 'Dual Image Configuration' page with the following fields and values:

- Active Image Version:** 2.5.0
- Active Image Description:** (0 - 60 characters)
- Backup Image Version:** 2.5.0
- Backup Image Description:** (0 - 60 characters)
- Next Active Image:** Radio buttons for 'Active (2.5.0)' (selected) and 'Backup (2.5.0)'.

Table 94. Dual Image Configuration Fields

Field	Description
Active Image Version	The version ID of the Active image
Active Image Description	Description of the Active image.
Backup Image Version	The version ID of the Backup image.
Backup Image Description	Description of the Backup image.

Field	Description
Next Active Image	The firmware image that will become active the next time the switch is rebooted. To make the current backup image the active image, select Backup , then reboot the switch. When a new image is loaded to the Backup Image, the Backup Image automatically becomes the next active image.

Click **APPLY** to save your changes to the switch.

Backup and Update Files



The Backup and Update page enables you to save a backup of the switch's image, configuration files or error log (transfer a file from the switch), or update the switch firmware and configuration files (transfer a file to the switch), from a remote system.

Files can be backed up and updated using HTTP, TFTP, or SCP protocols.

Secure Copy Protocol (SCP) Usage

Secure Copy Protocol (SCP) is a protocol which allows secure file transfer between hosts on the network. SCP runs over TCP port 22, and uses SSH for data transfer and authentication thereby ensuring confidentiality of transferred data.

The switch acts as an SCP client and it can send or receive files to/from an SCP server. The switch uses username and password credentials to authenticate to the SCP server.

To display this page, click **Maintenance** > **Backup and Update Files** in the navigation pane. You need to use the **Next**  and **Back**  buttons to complete the various fields and start the transfer process. These are the steps for filling in the backup or update operation:


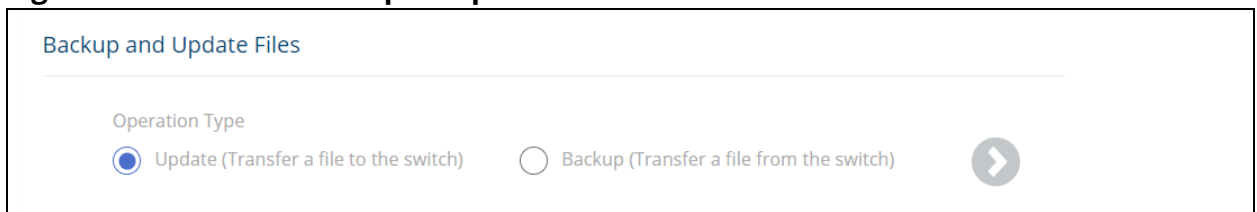

1. Select the Operation Type and then click **Next** 
 - o Select **Update** to update the switch firmware or configuration files (transfer a file to the switch).
NOTE: Firmware upgrades can only be performed on the backup image.
 - o Select **Backup** to save a backup of the current image, configuration file or error log (transfer a file from the switch).

Figure 109. Select Backup or Update



The screenshot shows the 'Backup and Update Files' page. Under the 'Operation Type' section, there are two radio buttons: 'Update (Transfer a file to the switch)' which is selected, and 'Backup (Transfer a file from the switch)'. To the right of these buttons is a 'Next' button with a right-pointing arrow icon.

2. Select the **File Type** and then click **Next** .

These are the available file types:

File Type	Description	Available for Operation Type
Active Image	Select this option to backup/copy the active image file. The active image file is the one running currently on the switch.	Backup only
Backup Image	Select this option to transfer a new image to the switch. The code file is stored as the backup image. After updating the backup image, you can use the Dual Image Configuration page to make it the active image upon the next reboot. NOTE: You cannot directly update the active image.	Update and Backup
Startup Configuration	Select this option to update or backup the stored configuration file. In case of startup configuration update, if the copy operation resulted in an error (for example wrong configuration lines), the update is stopped.	Update and Backup
Running Configuration	Select this option to back up the running configuration file.	Backup only
Backup Configuration	Select this option to update or backup the stored backup configuration file. The backup configuration file is stored on the switch for future reference. It is not active unless copied to the running configuration.	Update only
Error Log	Select this option to backup the switch log file. The log file is the file on flash. It stores syslog messages, from level error and higher.	Backup only

3. Select the Transfer Protocol, and then click **Next** .

These are the available protocols:

- o HTTP - this protocol does not require any additional fields
- o TFTP - this protocol requires the Server Address and File Name
- o SCP - this protocol requires the Server Address, Username, Password, and File Name

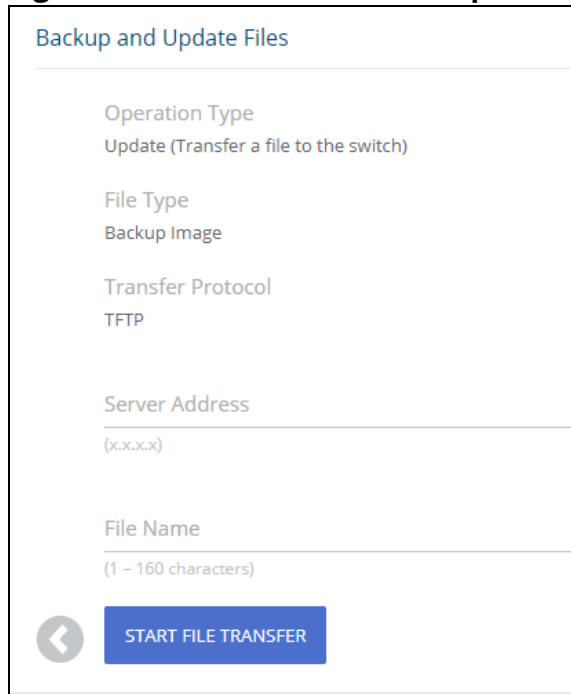
4. Enter any additional fields as required.

Field	Description
Server Address	(TFTP/SCP only) Enter the IP address of the TFTP/SCP server to use for file transfer (Update or Backup).
File Name	(TFTP/SCP only) Enter the path on the server where you want to put the file followed by the name to be applied to the file as it is saved. This can differ from the actual file name on the switch. The path can be 0 to 160 characters and the file name can be 1 to 32 characters. The file name can have ASCII printable characters, excluding the following: \\, /, :, *, ?, ", <, >,
Username	For SCP transfer, if the server requires authentication, specify the user name for remote login to the server that will receive the file.
Password	For SCP transfer, if the server requires authentication, specify the password for remote login to the server that will receive the file.

5. Click **START FILE TRANSFER** to start the transfer. For a TFTP or SFTP backup, the switch begins the

transfer to the specified location. For an HTTP update, browse to the location on your management station where the file you want to update to switch is located.
For HTTP backup - the file will be saved to the download folder specified by the browser.

Figure 110. File Transfer Example - TFTP Protocol



The screenshot shows a web interface titled "Backup and Update Files". It contains several configuration fields:

- Operation Type:** Update (Transfer a file to the switch)
- File Type:** Backup Image
- Transfer Protocol:** TFTP
- Server Address:** (x.x.x.x)
- File Name:** (1 - 160 characters)

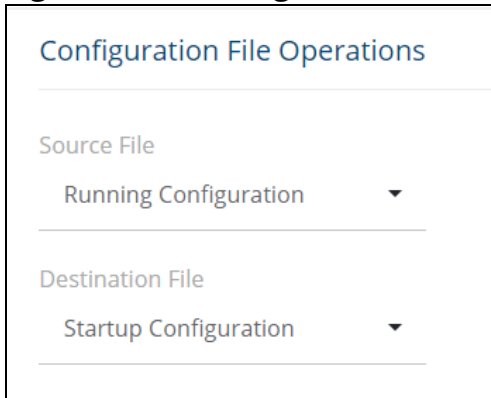
At the bottom left, there is a back arrow icon. At the bottom center, there is a blue button labeled "START FILE TRANSFER".

Configuration File Operations

Use this page to copy the information contained in one configuration file to another configuration file on the switch.

To display this page, click **Maintenance > Configuration File Operations** in the navigation pane.

Figure 111. Configuration Files Operations Page



The screenshot shows a web interface titled "Configuration File Operations". It contains two dropdown menus. The first is labeled "Source File" and has "Running Configuration" selected. The second is labeled "Destination File" and has "Startup Configuration" selected.

Table 95. Configuration Files Operations Fields

Field	Description
Source File	Select the configuration file that will overwrite the contents in the selected destination file. The source file options are as follows: <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 **START FILE TRANSFER** to initiate the file transfer operation.

Reset

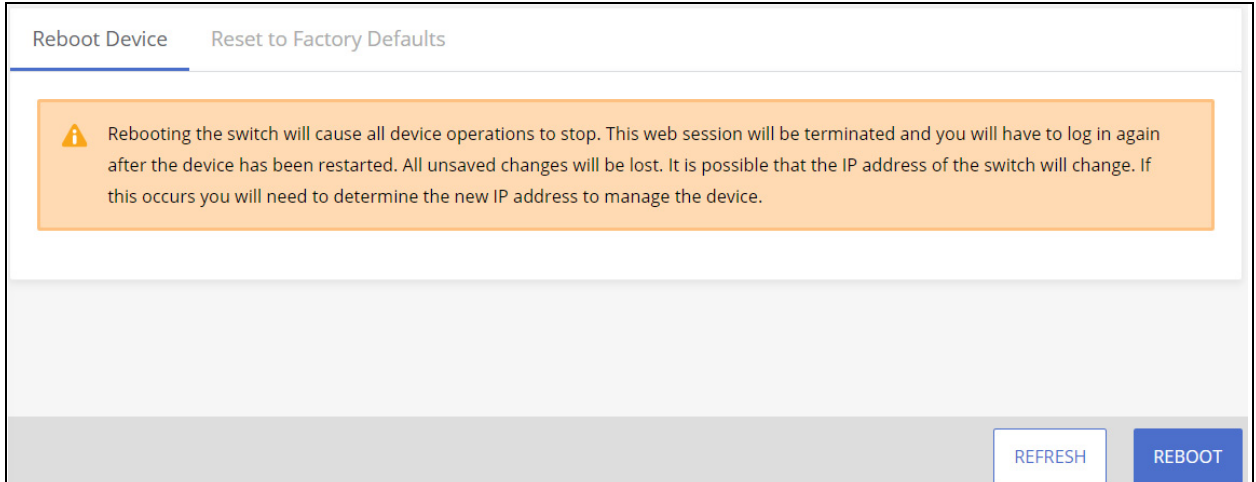
This page enables Rebooting the switch or Resetting to Factory Defaults.

Reboot Device

Use this feature to perform a software reboot of the switch. If you applied configuration changes, click the **Save Configuration** button in the upper right of any page before rebooting. If the switch is configured to use DHCP to acquire its IP address, the address may change upon restart; you will need to determine the address before logging back in to the management utility.

To display the Reboot Device page, click **Maintenance > Reset**, and make sure the **Reboot Device** tab is selected.

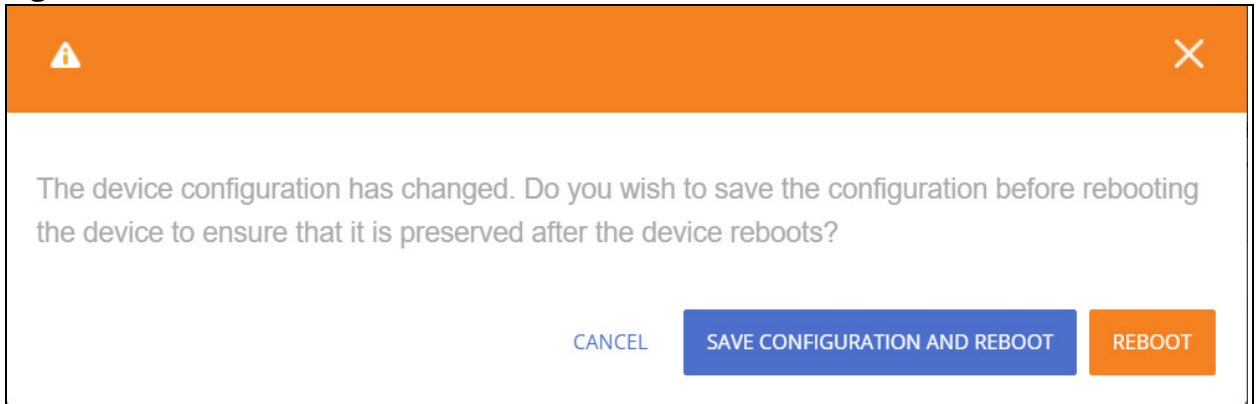
Figure 112. Reboot Device Tab



Click **REBOOT** to reboot the switch.

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

Figure 113. Save Before Reboot



Reset to Factory Defaults

You can use the Reset To Factory Defaults page to reboot the switch and restore all switch settings to their factory default values and to erase all entries in the switch log file stored in the non-volatile memory. Following Reset to Factory default the switch will reset and all configuration changes, including those that were previously saved, are reset in the running system by this action.

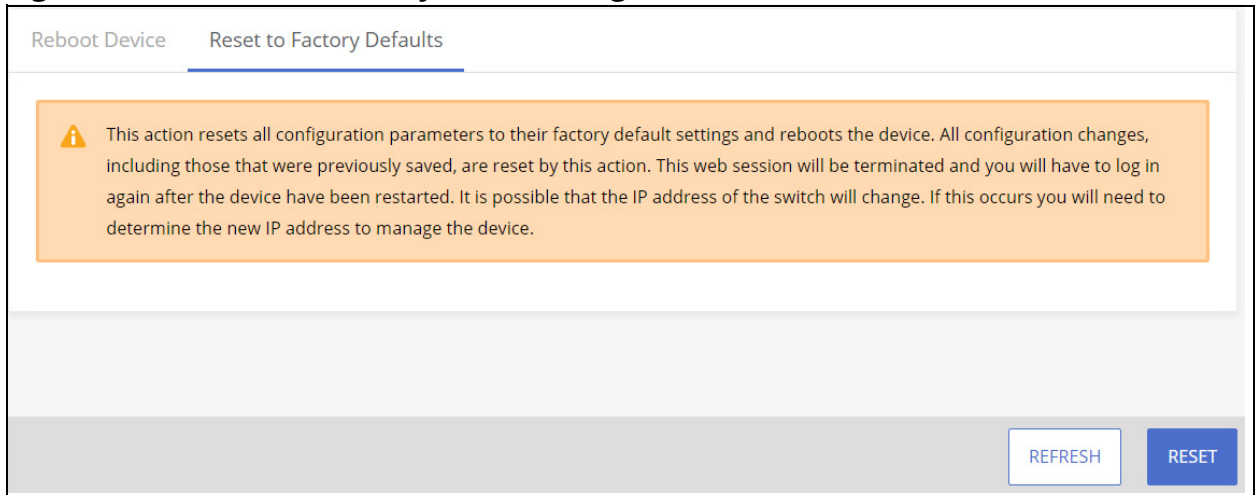
If the switch is configured to use DHCP to acquire its IP address, the address may change upon restart; you will need to determine the address before logging back in to the management utility.

To display the **Reset to Factory Defaults** page, click **Maintenance > Reset**, and make sure the **Reset to Factory Defaults** tab is selected.



It is recommended that you back up the current configuration file prior to restoring the factory defaults configuration. See **Backup and Update Files** for instructions.

Figure 114. Reset to Factory Defaults Page



Click **RESET** to reboot the switch and restore the system to the default settings.

Websites

Main Instant On site:

<https://www.arubainstanton.com/>

Support:

<https://support.arubainstanton.com/>

Instant On social forums and knowledge base:

<https://community.arubainstanton.com/>

Security Bulletins:

<https://www.arubanetworks.com/support-services/security-bulletins/>

End-user license agreement:

<https://www.arubainstanton.com/eula/>

Support contact numbers:

<https://www.arubainstanton.com/contact-support/>

Accessing Aruba Support

To access Aruba Support, go to <https://www.arubanetworks.com/support-services/>.

Be sure to collect the following information before contacting Support:

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing Updates

To download product updates:

- Aruba Support Portal <asp.arubanetworks.com/downloads>

If you are unable to find your product in the Aruba Support Portal, you may need to search My Networking,

where older networking products can be found:

My Networking www.hpe.com/networking/software

To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:

www.hpe.com/support/AccessToSupportMaterials



Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

To subscribe to eNewsletters and alerts: www.hpe.com/support/e-updates

Warranty Information

To view warranty information for your product, go to <https://www.hpe.com/support/Networking-Warranties>.

Regulatory Information

To view the regulatory information for your product, view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at the Hewlett Packard Enterprise Support Center: www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional Regulatory Information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at: www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH: www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see: www.hpe.com/info/environment

Documentation Feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.