Table of Contents

AN-620-SW

Araknis 620 Switch Layer 3 Managed Switch User Manual

Definitions

- **Interface** — A port on the switch. Also called a switchport.
- **Clients** — A device on the network. Sometimes written as a client device.

Quick links:

- Araknis 620 Switch Quick Start Guide
- Configuring an Araknis 620 Switch for MoIP (link incoming)

Interface access

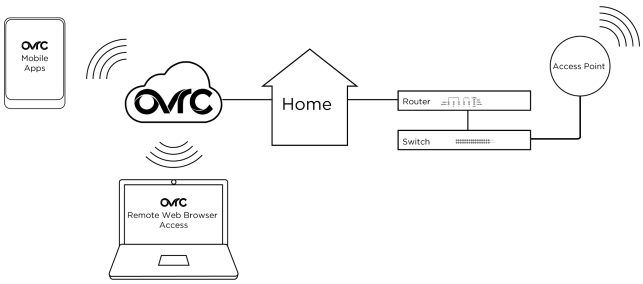
Araknis switches can be configured through OvrC or the local interface. The local interface is accessible using OvrC's webconnect feature, typing the switch's DHCP address into your browser's address bar, or using the switch's default IP address.

Configuring the switch in OvrC

OvrC provides remote device management, real-time notifications, and intuitive customer management, using your computer or mobile device. Setup is plug-and-play, with no port forwarding or DDNS address required.

To add this device to your OvrC account:

1. Connect the switch to the internet.
2. Log into OvrC (**www.ovrc.com**).
3. Scan the site using an OvrC Pro device, or add the switch manually by entering the MAC address and Service Tag.



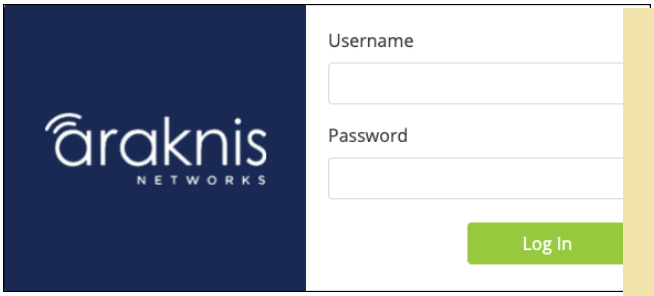
Logging into the web interface

1. Log into the switch using the default credentials:

Username	araknis
Password	araknis

2. You must update the password after initial login.

 # Indented table using this topic from the user guide. I modified the code for this specific topic



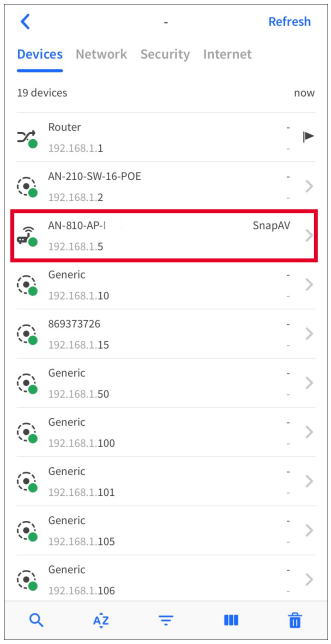
Tip: Strong passwords are long and unrelated to the client's public details. For example, thepepperonipizzas is stronger and easier to remember than P@ssword or thesmiths.

Other access methods: DHCP IP address

The switch is configured to DHCP by default so that the DHCP server can assign an IP address when the switch is connected to the network (the DHCP server is usually the router). This address can be used for accessing the web interface.

Use one of these methods to find the IP address of the switch:

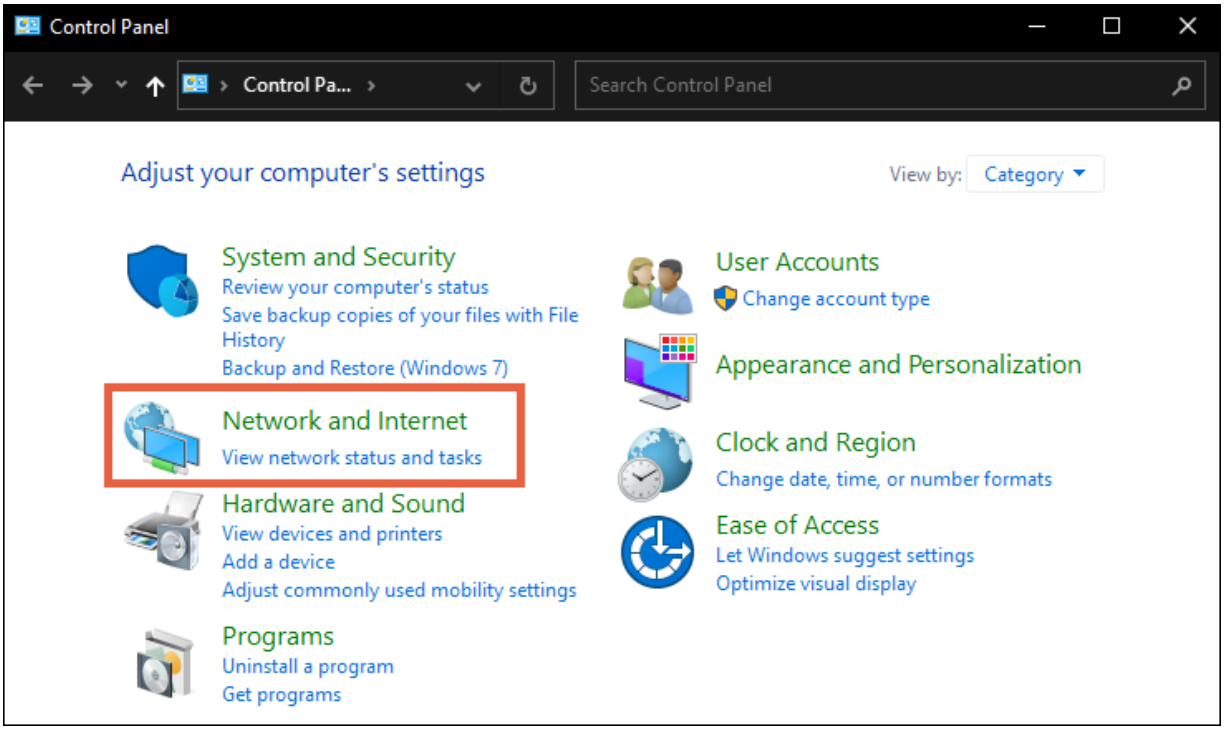
- Check the device list in OvrC.
- Check the client table on your router.
- Use a network scanner (e.g. Fing) to scan the network. The Araknis switch manufacturer field displays SnapAV.
- See the highlighted field in the Fing screenshot to the right for an example of an Araknis device being identified.



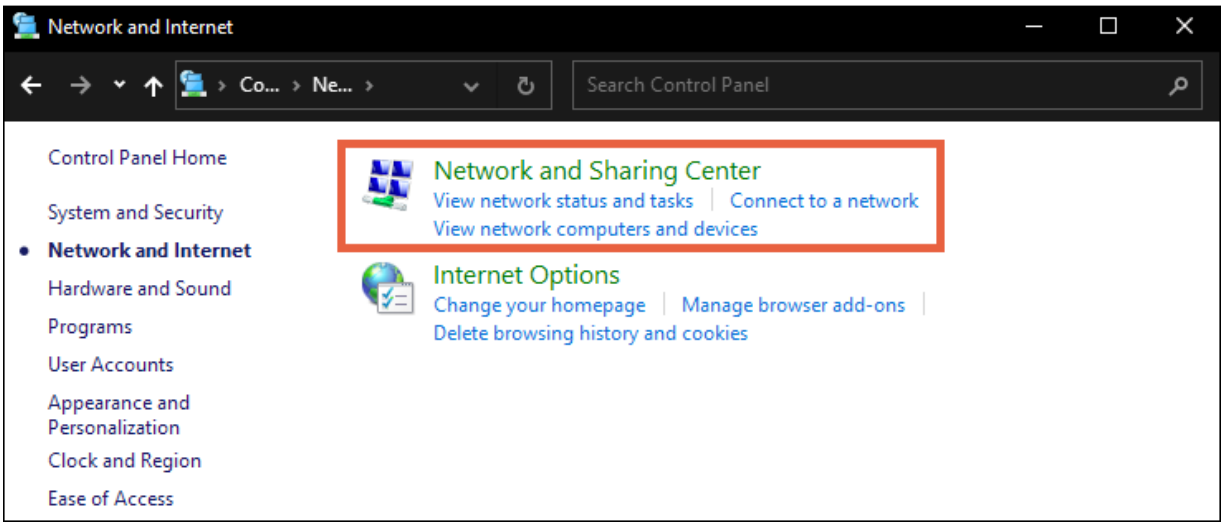
Accessing the switch using the default IP address

If the switch is not given a DHCP address, or needs to be accessed while not connected to a network, you can configure your computer's network connection to access the switch using the default IP address, **192.168.20.254**.

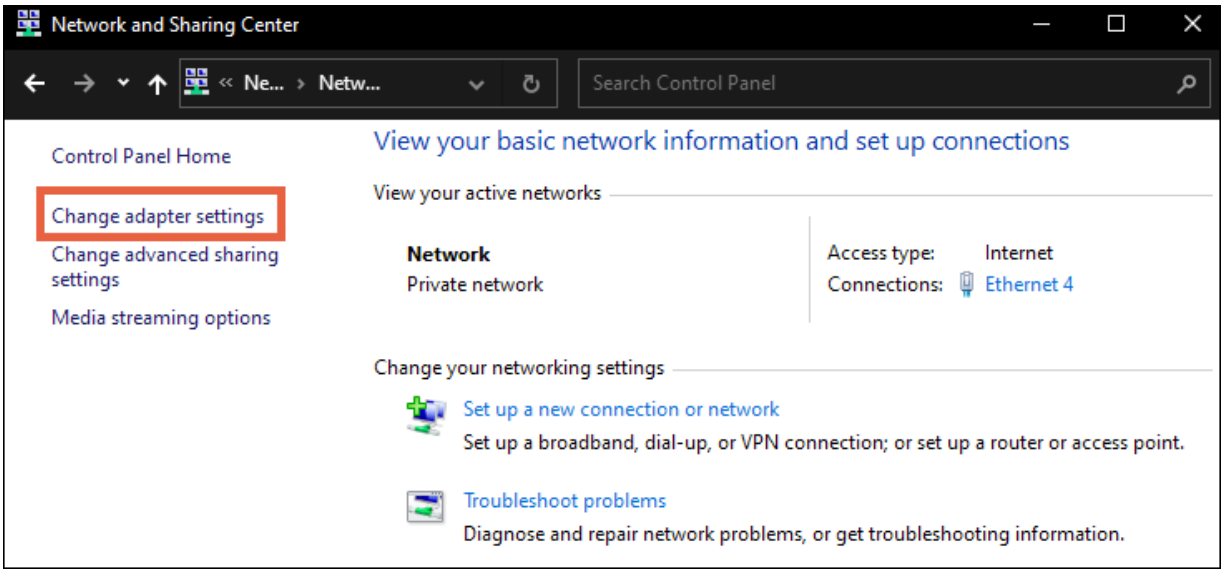
1. Connect your PC to the switch using an Ethernet cable.
2. Open the Control Panel and click **Network and Internet**.



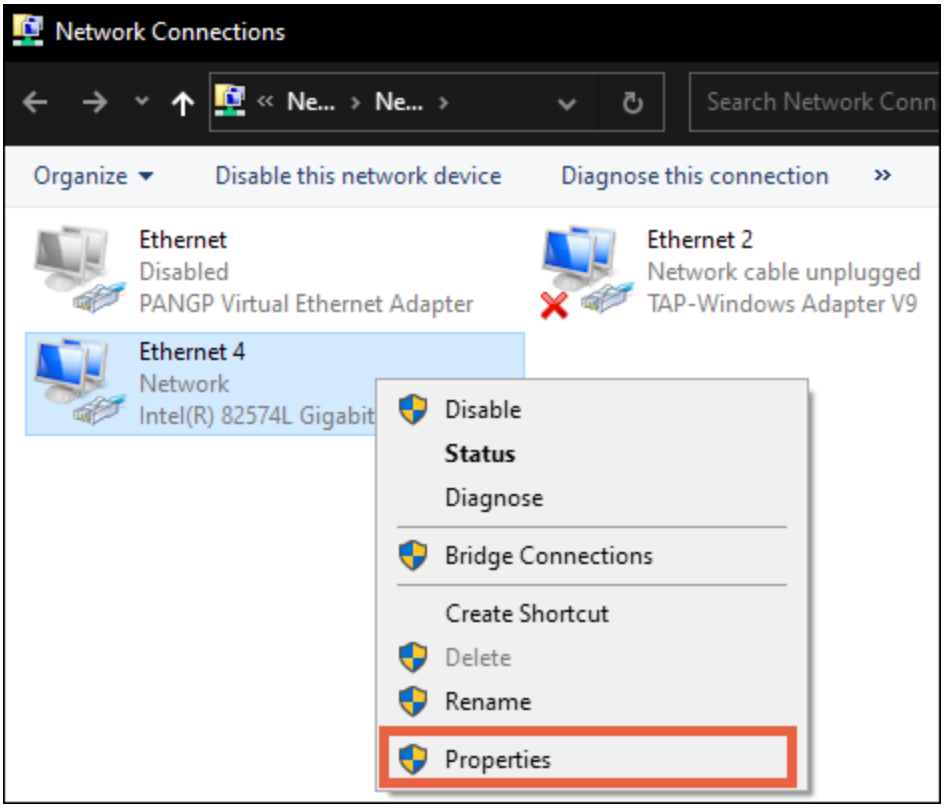
3. Click **Network and Sharing Center**.



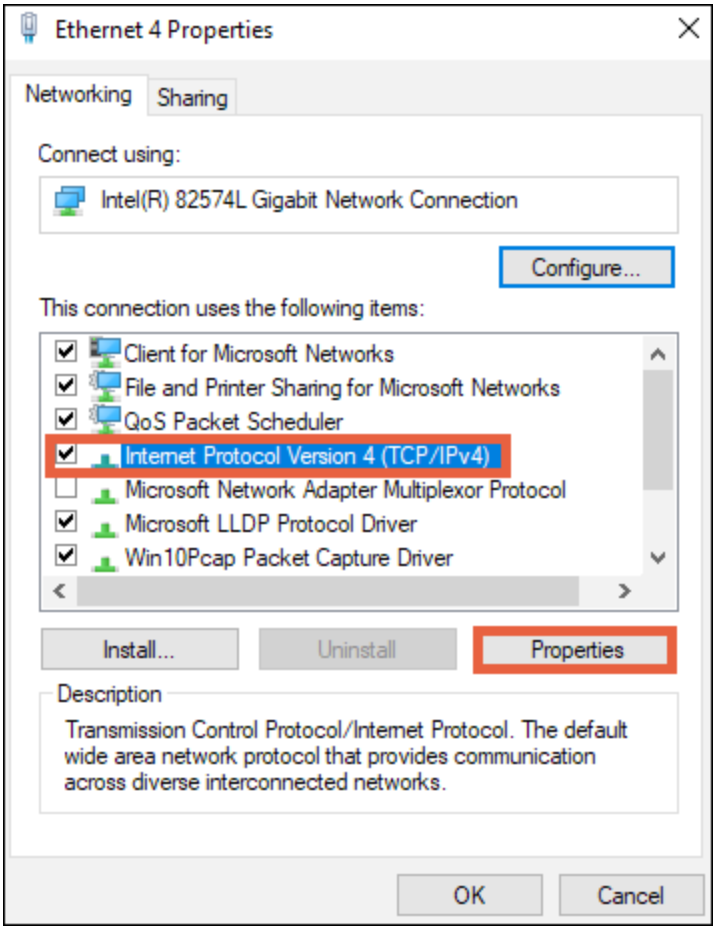
4. Click **Change adapter settings**.



5. Right-click the icon for the wired network connection, then left-click **Properties**.

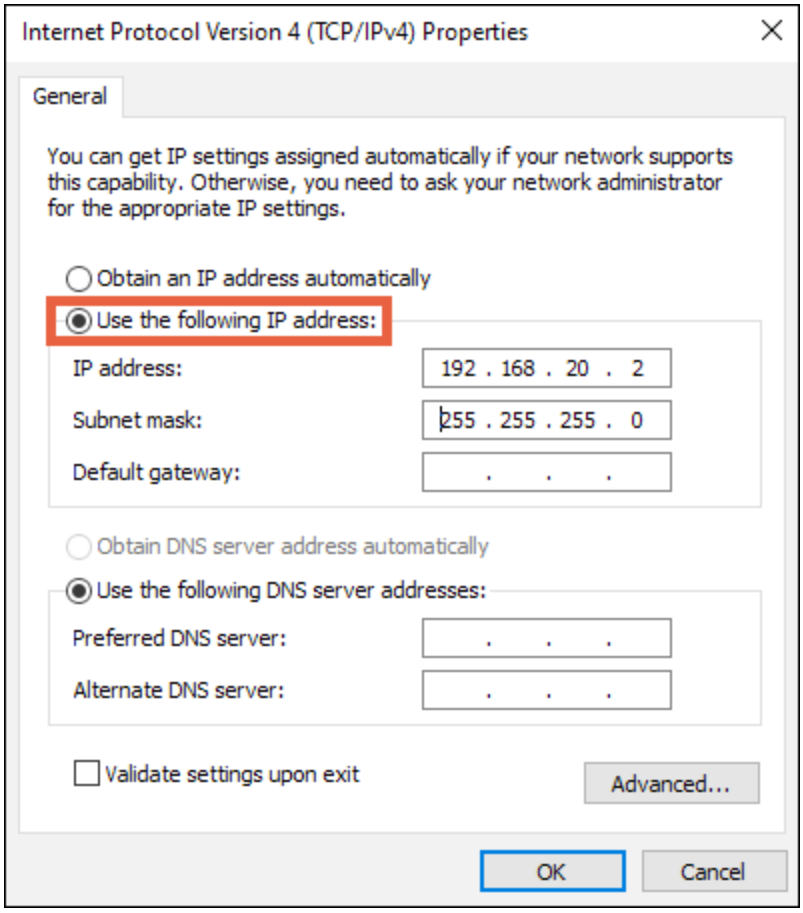


6. Select **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties**



7. In the General tab, click **Use the following IP address:** and enter the IP address and subnet mask, then click **OK**.

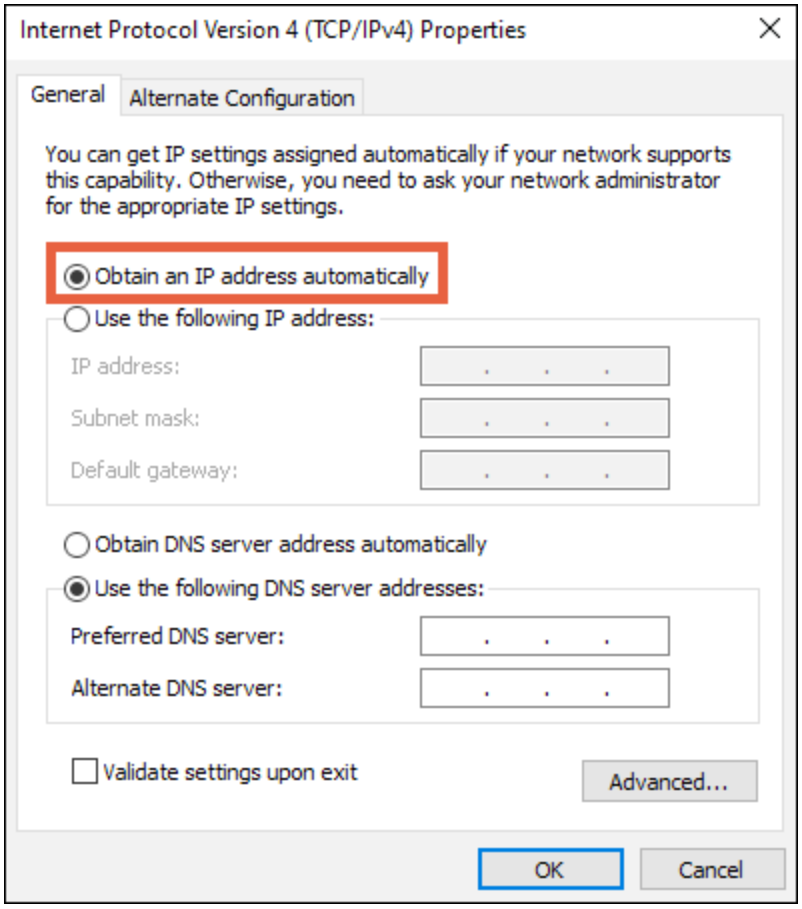
IP Address	192.168.20.2
Subnet Mask	255.255.255.0



8. Open a browser and navigate to https://192.168.20.253/. Log in using the default credentials:

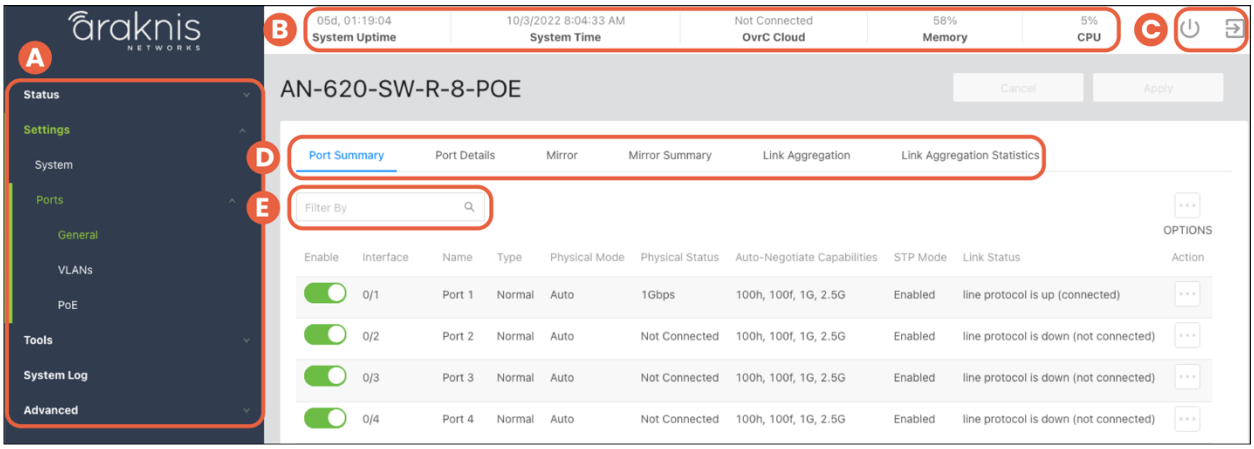
Username	araknis
Password	araknis

9. After configuring the switch, set your computer's IPv4 Properties back to Obtain an IP address automatically, then click **OK**.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

Interface overview

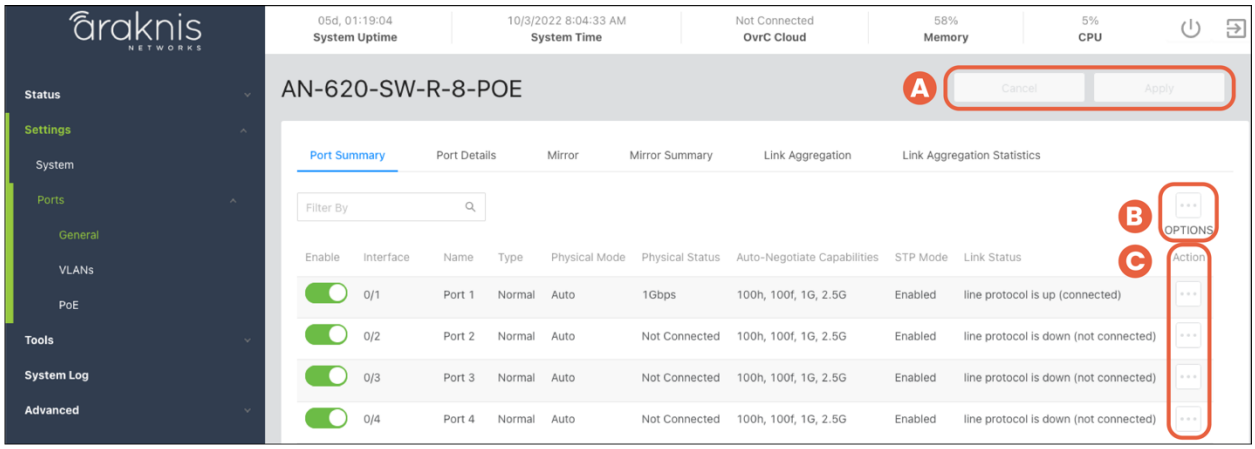
Araknis 620 switches use the main navigation menu and page tabs to organize the system information and configurable settings.



1. **Main Navigation Menu** — Click on the headers to access the submenus to configure and maintain the switch.
2. **Top Bar** — Displays the overall status of the switch, including the system uptime, the current time, OvrC cloud connection, memory, and system usage.
3. **Restart and Logout** — Use these buttons to restart or log out of the switch.
4. **Navigation Tabs** — Click on a tab to access more settings under the submenu.
5. **Filter By** — Type a value to filter the data on the page. You do not need to press enter or return.

Note: Click the info icon to learn more about individual settings.

Applying and saving changes

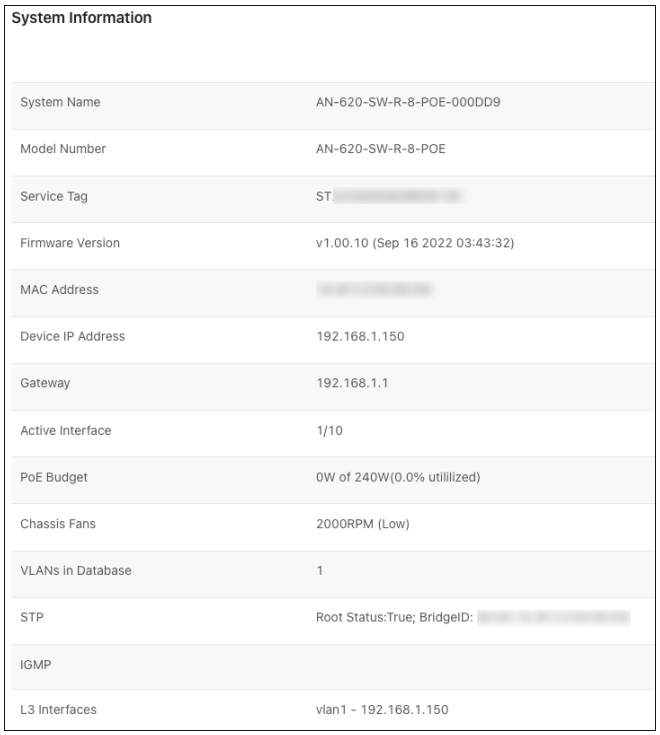


1. **Apply and Cancel** — Use these buttons to apply or cancel changes.
2. **Options** — Use this button to select multiple ports, refresh the page, or reset the settings to their default state.
3. **Action** — Use this button to make changes to individual ports.

Status

System

This page provides an overview of the switch's configuration.



System Information

System Name	AN-620-SW-R-8-POE-000DD9
Model Number	AN-620-SW-R-8-POE
Service Tag	ST
Firmware Version	v1.00.10 (Sep 16 2022 03:43:32)
MAC Address	
Device IP Address	192.168.1.150
Gateway	192.168.1.1
Active Interface	1/10
PoE Budget	0W of 240W(0.0% utililized)
Chassis Fans	2000RPM (Low)
VLANs in Database	1
STP	Root Status:True; BridgeID:
IGMP	
L3 Interfaces	vlan1 - 192.168.1.150

- **System Name** — This is the name that the switch appears under when it is identified on the network. This field can be changed under **Settings** > **System**.
- **Model Number** — Use this field to verify the switch's model number. Notated as AN (Araknis) – SW (switch) – R/F (rear or front-facing ports) – X (the number of RJ-45 ports the switch has) -POE (Power-over-Ethernet).
- **Service Tag** — A unique identifying number that is used to add the switch to OvrC, manually.

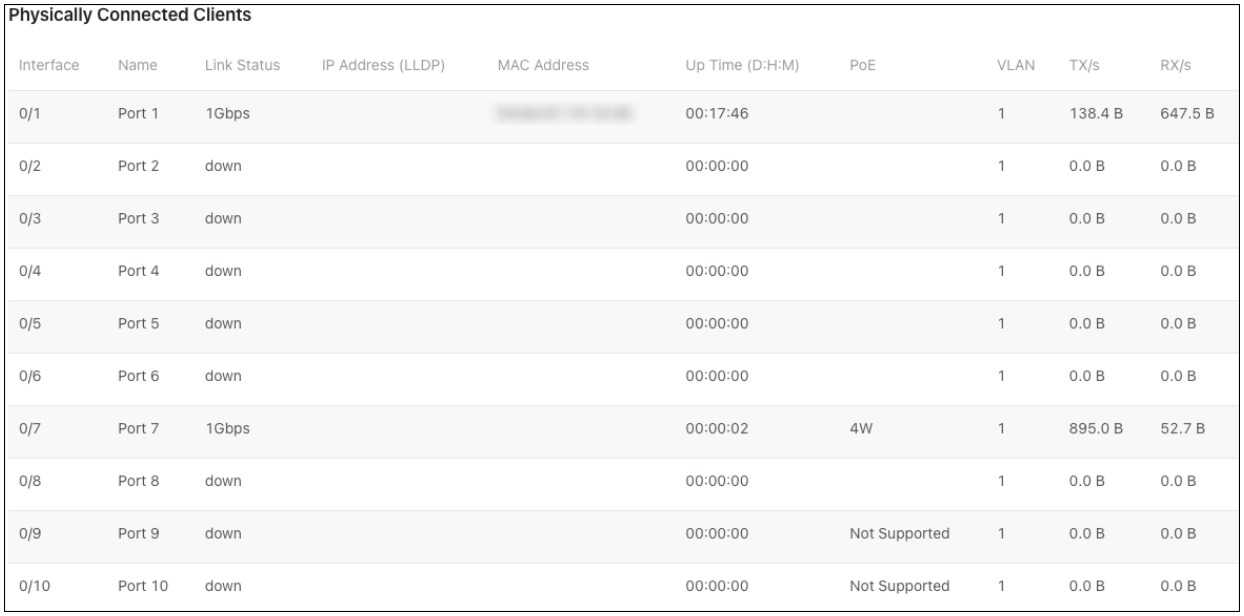
- **Firmware Version** — Displays the firmware version installed on the switch. Use OvrC to verify if the switch is up to date and update the switch if it isn't.
- **MAC Address** — A unique identifier that appears in network scans. This address is required if the switch is being manually added to OvrC.
- **Device IP Address** — Displays the IP address of the switch.
- **Gateway** — Displays the IP address of the router.
- **Active Interface** — The number of ports that detect a connection compared to the total number of ports on the switch.
- **PoE Budget** — The amount of Power-over-Ethernet being currently used on the switch.

Pro Tip: Do not use more than 80% of the total budget. When calculating the budget, use the total possible amount of power the connected devices may draw.

- **Chassis Fans** — Shows the rotations per minute (RPM) of the fan and gauge how high the use of the fans is, in parenthesis. Low, Medium, High, Max, or OTP (Over Temperature Protection). The switch stays in OTP until the system temperature falls within the normal range.
- **VLANs in Database** — Displays the number of VLANs that are configured on the switch.
- **STP** — Provides details about the Spanning Tree Protocol (STP) configuration on the switch. See **Switching** > **Spanning Tree Protocol** for more information.
- **IGMP** — Provides details about the Internet Group Management Protocol (IGMP) configuration on the switch. See **Switching** > **IGMP Snooping** for more information.
- **L3 Interfaces** — Displays the DHCP servers the switch is interacting with.

Ports

This page provides information about specific switchport configurations. Refresh the page to update the page.



Physically Connected Clients

Interface	Name	Link Status	IP Address (LLDP)	MAC Address	Up Time (D:H:M)	PoE	VLAN	TX/s	RX/s
0/1	Port 1	1Gbps		[redacted]	00:17:46		1	138.4 B	647.5 B
0/2	Port 2	down			00:00:00		1	0.0 B	0.0 B
0/3	Port 3	down			00:00:00		1	0.0 B	0.0 B
0/4	Port 4	down			00:00:00		1	0.0 B	0.0 B
0/5	Port 5	down			00:00:00		1	0.0 B	0.0 B
0/6	Port 6	down			00:00:00		1	0.0 B	0.0 B
0/7	Port 7	1Gbps			00:00:02	4W	1	895.0 B	52.7 B
0/8	Port 8	down			00:00:00		1	0.0 B	0.0 B
0/9	Port 9	down			00:00:00	Not Supported	1	0.0 B	0.0 B
0/10	Port 10	down			00:00:00	Not Supported	1	0.0 B	0.0 B

- **Interface** — The number assigned to the port of the switch. The SFP ports are always the last two ports.
- **Name** — The assignable name for the port. Edit the name at **Settings** > **Ports** > **General**.
- **Link Status** — Displays the connection speed between the switch and the connected device. If there is no connection status is “down.”
- **IP Address (LLDP)** — Displays the IP address of the connected device (learned by LLDP).
- **MAC Address** — The MAC address of the device connected to the port.
- **Up Time (D:H:M)** — The amount of time the switch has detected a connection to the device in Days:Hours:Minutes.
- **PoE** — The amount of PoE power the switch is delivering to the connected device.
- **VLAN** — The VLAN ID assigned to the port.
- **TX/s** — The number of bytes, in seconds, being transmitted on the port.
- **RX/s** — The number of bytes, in seconds, being received on the port.

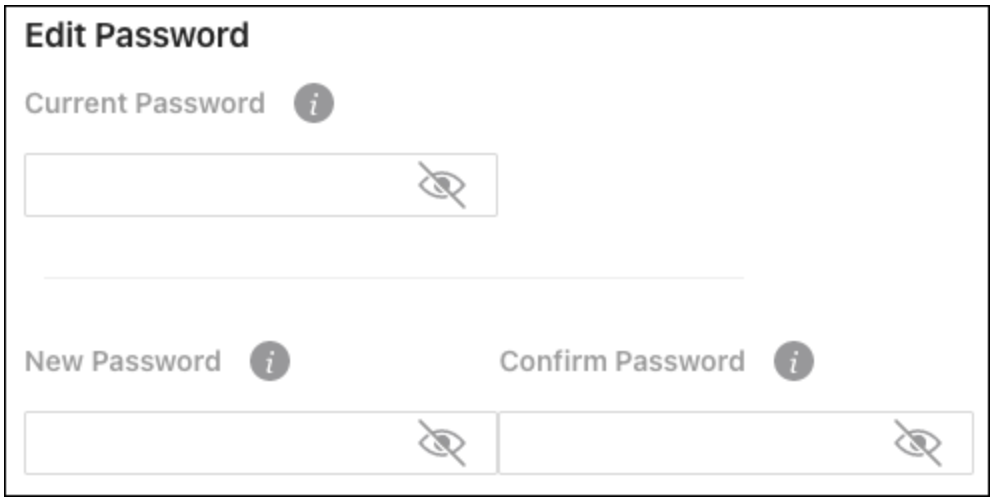
Settings

System

Use this page to update the general configuration of the switch. Below are the configurable settings and best practices.

Click the **Apply** button at the top of the page to save changes.

Edit Password

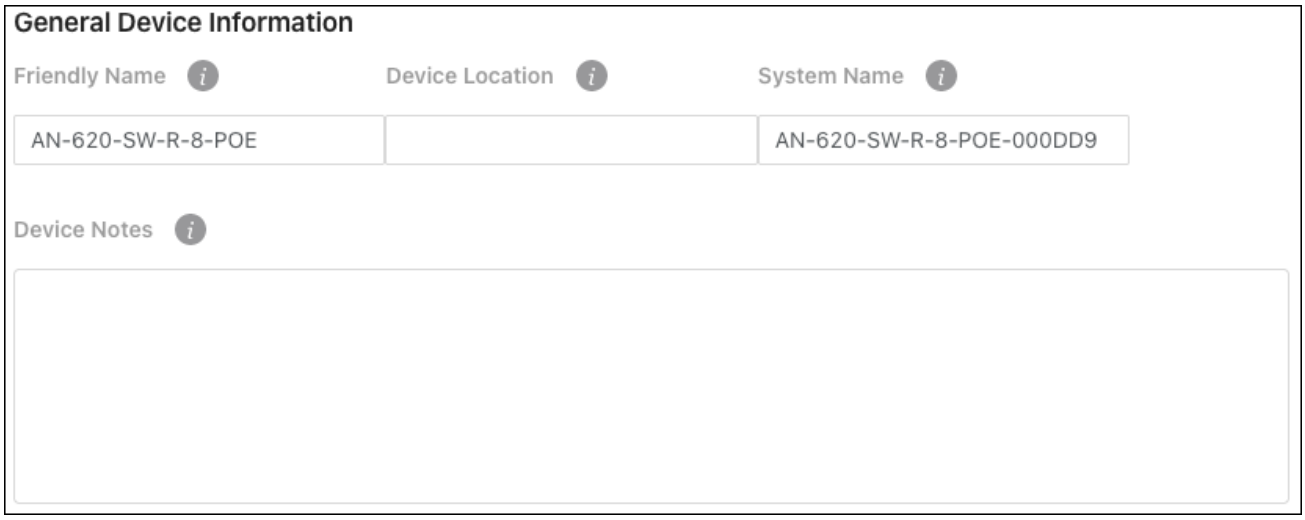


Pro Tip: Strong passwords are long and unrelated to the client's public details. For example, thepepperonipizzas is stronger and easier to remember than P@ssword or thesmiths.

Edit Username

There is only one configurable user for switch access. The username should be unique and standardized across all devices.

General Device Information



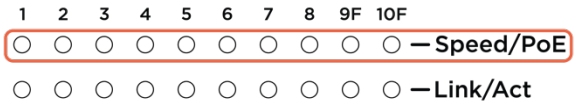
- **Friendly Name** — Give a name that makes the switch easily identifiable. Such as “Core Switch - Rack.”
- **Device Location** — Enter where the switch is located.
- **System Name** — This is the name that the switch appears under during network scans by other applications. This name should be unique to the switch.

- **Device Notes** — Enter additional configuration notes that wouldn't be displayed on the **Status** > **System** page. Such as what a VLAN is being used for on this switch.

Pro Tip: If you're using OvrC, these notes should be entered there as well.

LEDs

This setting determines the behavior of the **Speed/PoE** LED on the front of the switch.



Options include:

- **Max Speed** — Illuminates if the connection to the device is at the maximum possible speed.
- **PoE** — Illuminates if the switch is providing power to the connected device.
- **Disabled** — Turns the LED off.

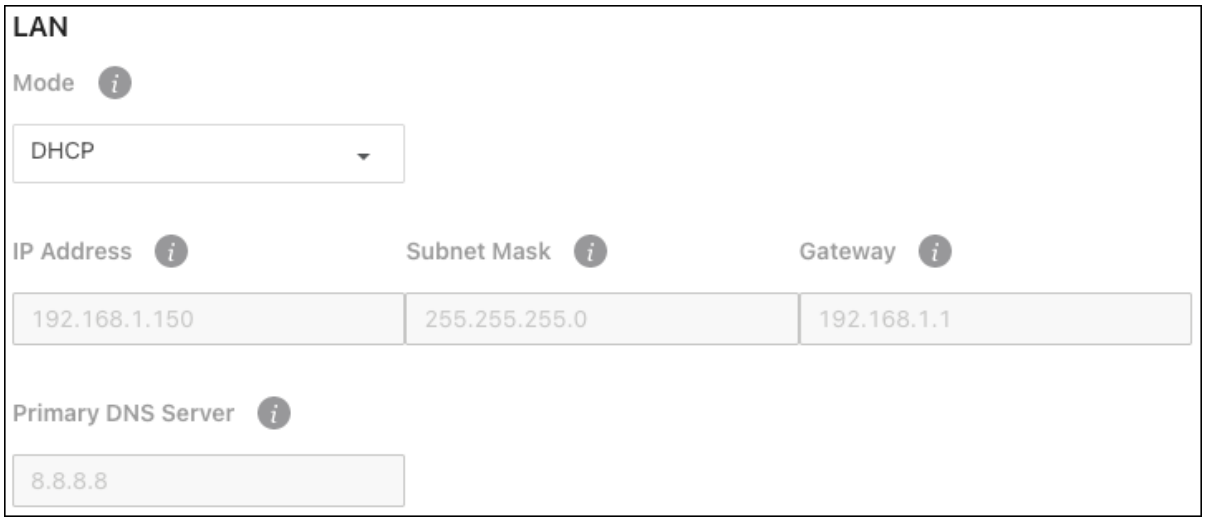
Pro Tip: The LED Behavior should be standardized across all switch installations. Be sure to leave notes about the LED Behavior If it's not standardized.

Adjust Time Zone

Configure the Time Zone that the switch is physically installed under.

LAN

Pro Tip: Leave the switch as DHCP and make a MAC or IP reservation in the router.

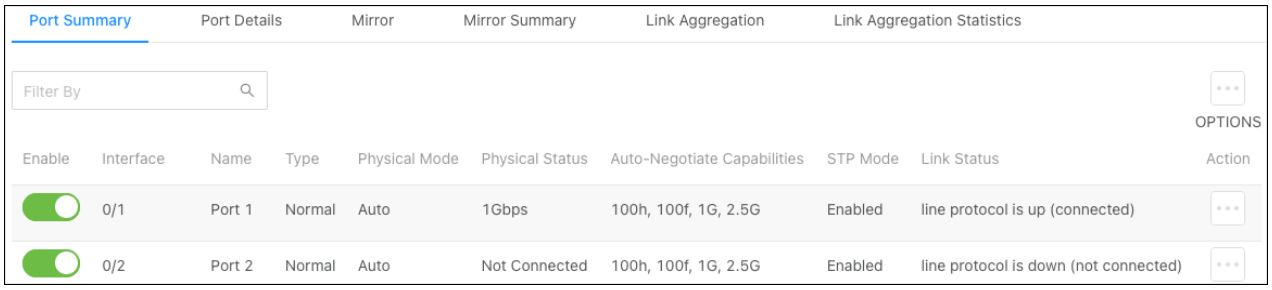


Ports

General

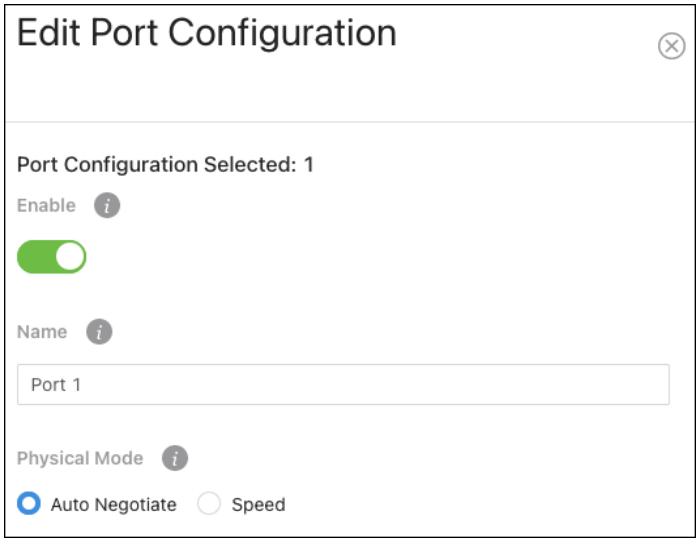
Port Summary

Use this page to quickly edit port settings.



Click the **Enable** toggle to enable or disable a port.

Use the **Options** (⋯) button to select multiple ports for configuration or the **Action** button to edit an individual port. Configurable settings appear in the Edit Port Configuration window.



Click the **Apply** button at the top of the page to save changes.

Configurable settings include:

- **Enable** — Toggle to allow traffic to pass through the port. Disable the port to prevent someone from plugging additional devices into the switch or to troubleshoot potential issues with a connected device.
- **Name** — Enter an easily identifiable name for the device connected to the port.
- **Physical Mode** — Configure the port speed and duplex mode.
    - **Auto Negotiate** — Advertises the duplex mode and speed for an auto-negotiation process with the device connected to the port. Click the "x" on the speed and duplex modes you do not want the switch to advertise.
    - **Speed** — Select speed to force the port to 100 Mbps half or full duplex.
- **STP Mode** — Toggle to enable or disable STP on the port.
- **Link Trap** — Toggle to enable or disable the port from broadcasting if it has a connection or not.
- **MTU (Maximum Transmission Unit)** — Enter the value for the largest possible packet size, in bytes, that a port can transmit.
- **Flow Control** — Use this feature to manage the data transfer rate between the switch and connected device(s). Flow control can be configured to only send or receive flow control packets. It can also be set to both.

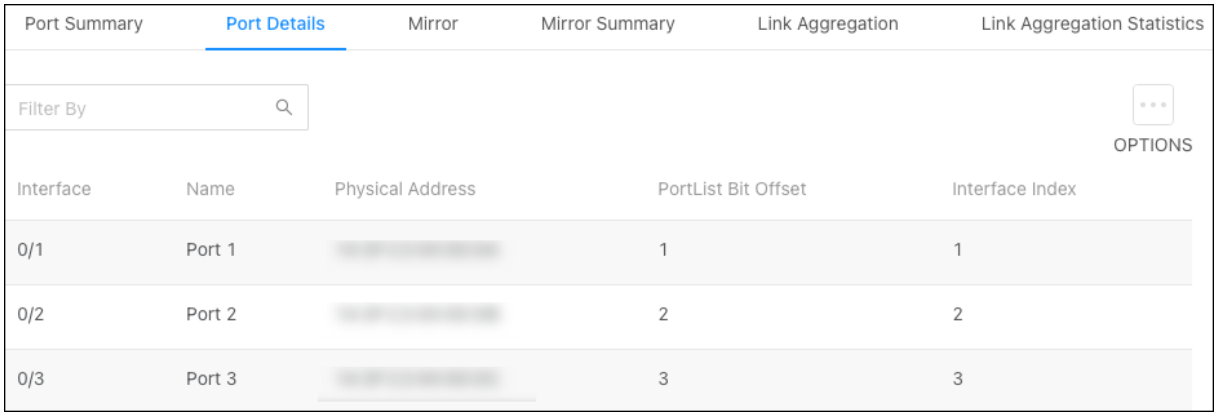
  Pro Tip: Leave flow control to the default **None** unless you have a specific application for the feature.

- **Broadcast Storm Recovery Level** — Enable to limit the amount of broadcast frames accepted and forwarded by the port by percentage, BPS (bits per second), or PPS (packets per second).

- **Multicast Storm Recovery Level** — Enable to limit the amount of multicast frames accepted and forwarded by the port by percentage, BPS (bits per second), or PPS (packets per second).
- **Unicast Storm Recovery Level** — Enable to limit the amount of unicast frames accepted and forwarded by the switch by percentage, BPS (bits per second), or PPS (packets per second).

Port Details

Use this page to quickly view port information such as Physical Address, Port List Bit Offset, and the Interface Index. Use the **Options** (⋯) button to refresh the page.



The physical address is the MAC address for the individual port.

Mirror

Use port mirroring to mimic the traffic flowing through one port to another. Port mirroring is typically used to capture a recording of network traffic for troubleshooting purposes.

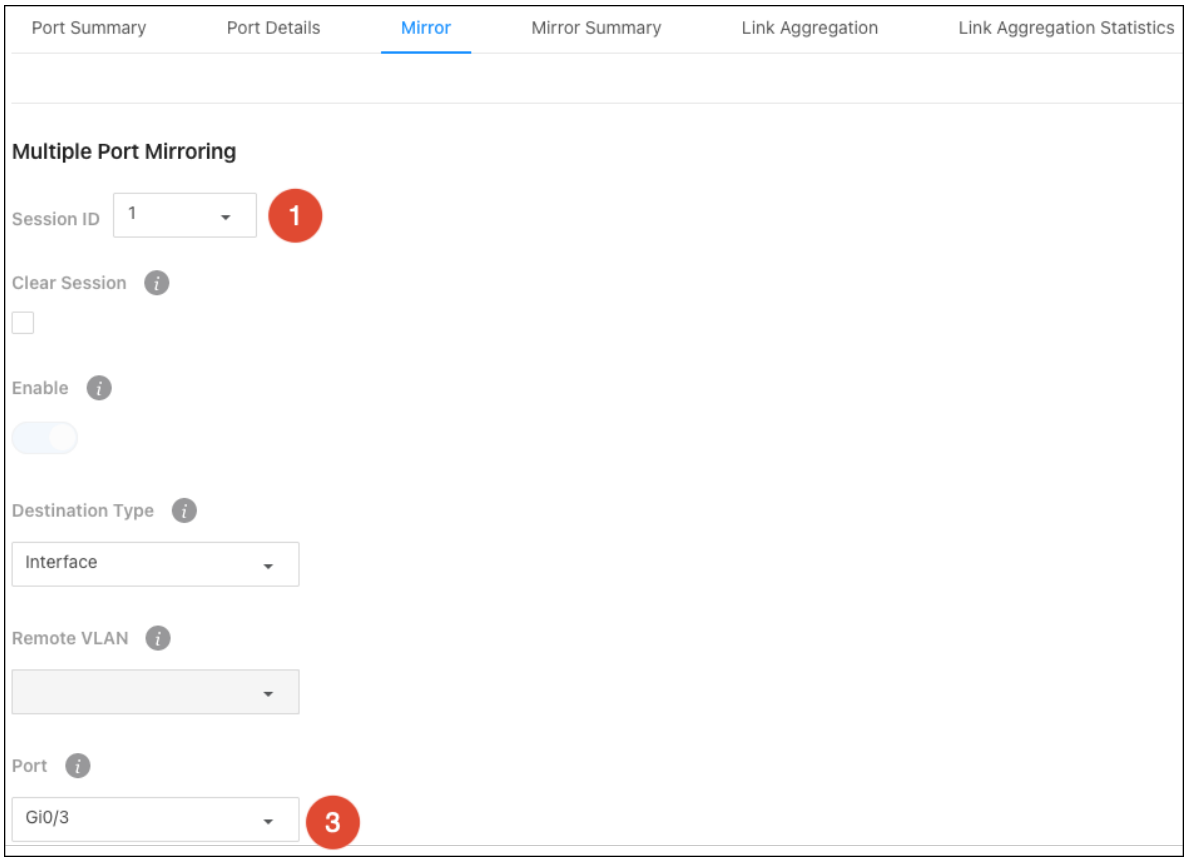
To configure port mirroring:

1. Select a **Session ID**. You cannot have multiple sessions with the same ID. If you have no current port mirroring sessions, use Session ID 1.

You do not have to click Enable. This toggle is automatically enabled after you save the session settings.

2. Select a **Destination Type**. This is typically **Interface**.

3. Enter the **Port** number to receive transmit/receive data from the **Source Ports**. For example, if port 3 has a PC running Wireshark for packet capture, enter 3 in the Port field.

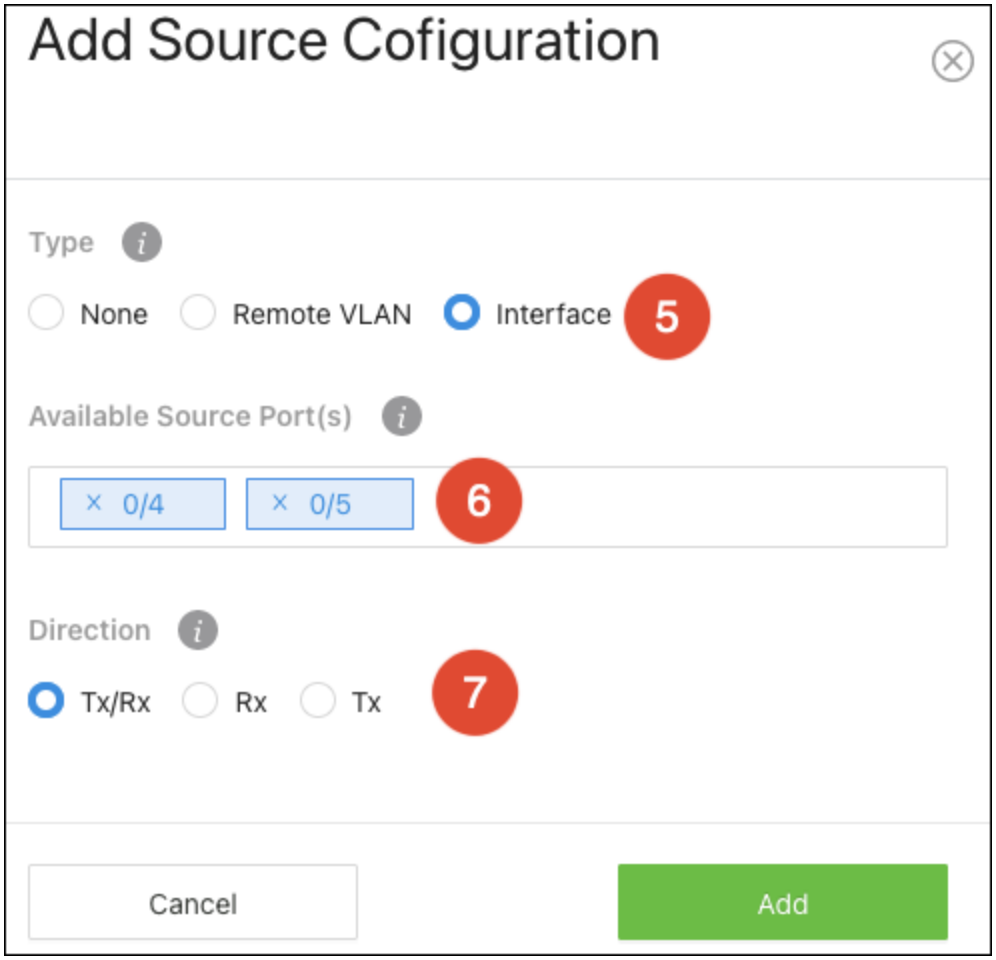


4. Click the **Options** (⋯) button and select **Add** to select the port(s) you want to mirror.

5. In the new window, select **Interface** as the Type.

6. Use the **Available Source Port(s)** dropdown to select the port(s) to mirror.

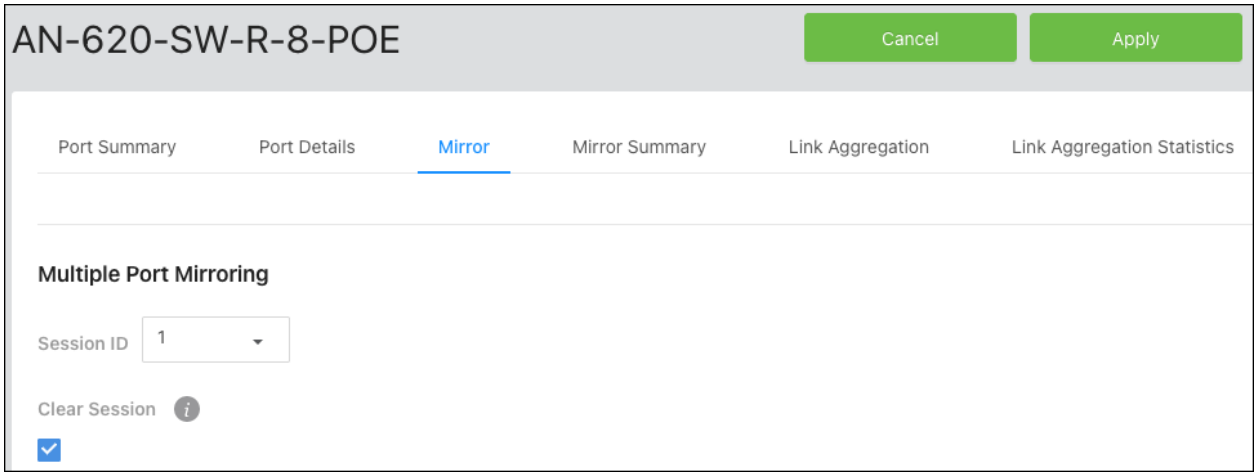
7. For **Direction**, select whether you want to mirror the packets being received (Rx), transmitted (Tx), or both (Tx/Rx), then click **Add**.



8. Click **Apply** at the top of the page. After the page refreshes Enable will be toggled on.

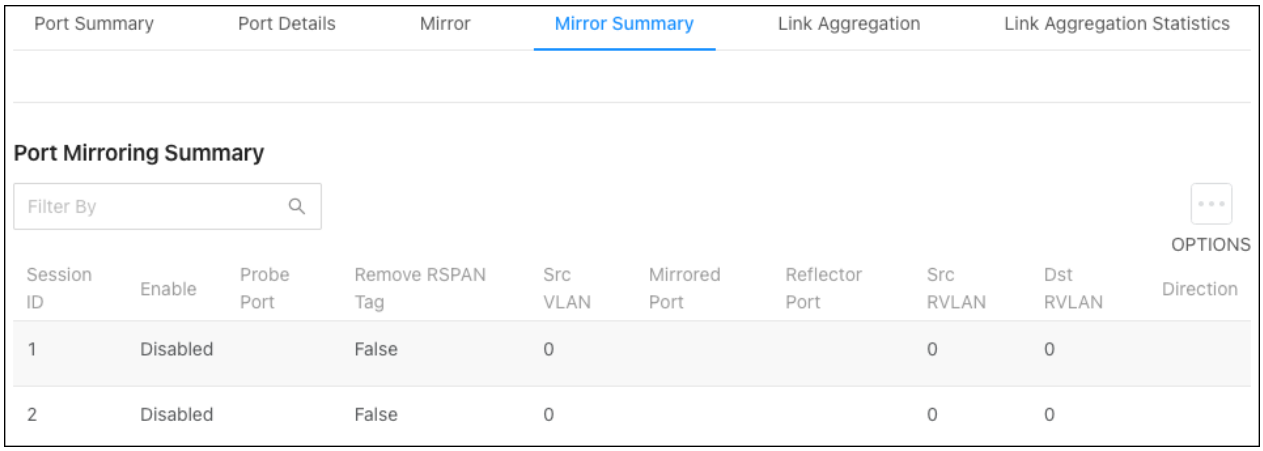
To disable a port mirroring session:

Select the **Session ID** you wish to end and click the **Clear Session** checkbox. Then click **Apply** at the top of the page.



Mirror Summary

Use this page to view configured port mirroring sessions. Use the **Options** (⋯) button to refresh the page.



Link Aggregation

Use Link Aggregation Groups (LAG) to combine the throughput of multiple ports.

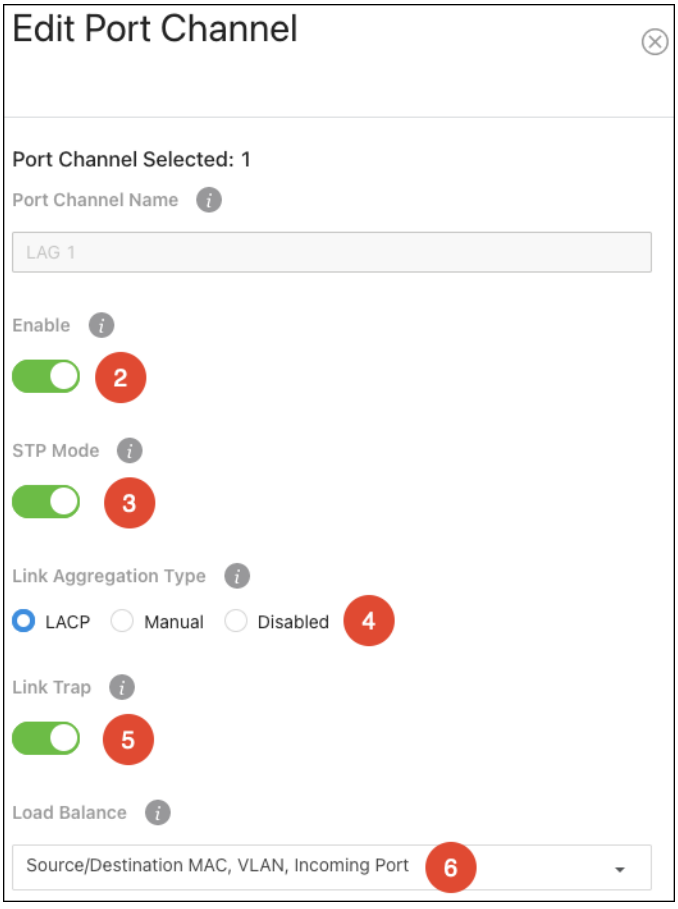
To configure a LAG:

1. Click the **Options** (⋯) button to select multiple LAGs or use the **Action** button to configure a single LAG.
2. Verify **Enabled** is toggled on.

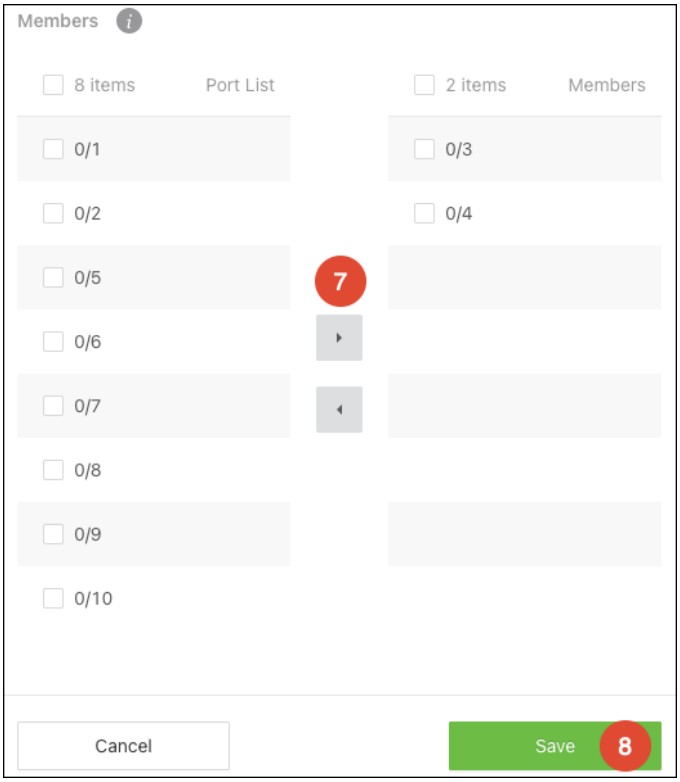
3. Enable or disable STP based on the networking needs.
4. Select a Link Aggregation Type. LACP is recommended.

- **LACP** (Link Aggregation Control Protocol) broadcasts that the connection type is a LAG to the switch you're connecting to for automatic configuration.
- **Manual** requires manual LAG configuration on the switch you're connecting to.

5. Enable or disable **Link Trap** based on the network's needs.
6. Leave **Load Balance** at the default (Source/Destination MAC, VLAN, Incoming Port), unless you have specific requirements.
   The selections are the information the switch uses to determine how to load balance the throughput of the LAG.
7. Adjust the members of the port channel (ports 3 and 4 used in the example). Use the checkboxes to select a port and the directional arrows to add/remove ports.

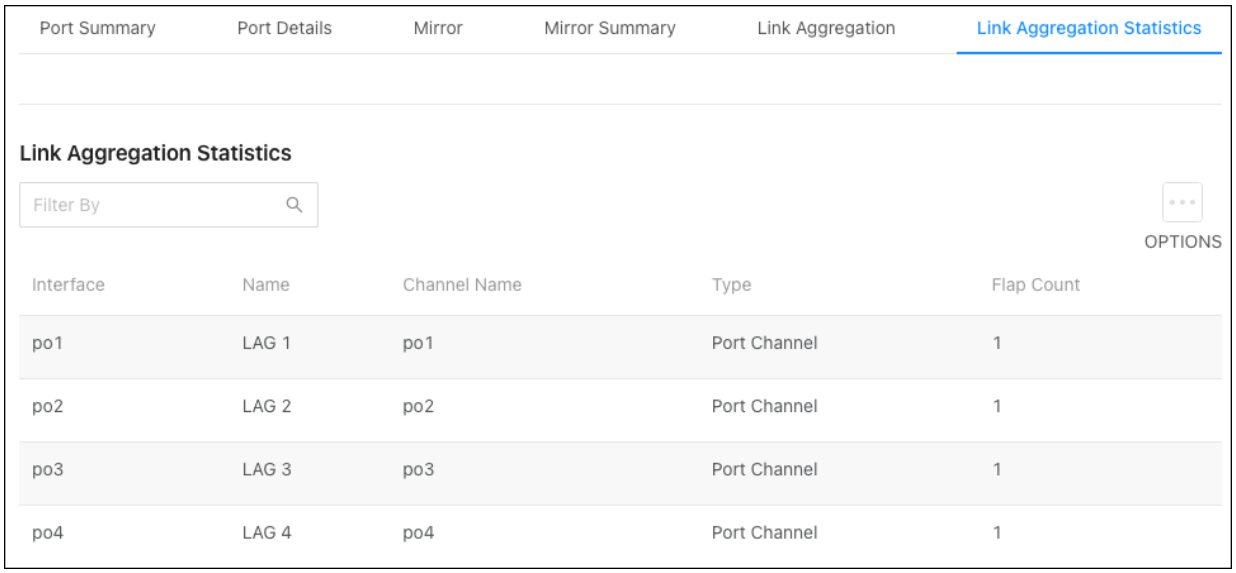


8. Click **Save** to close the window, then **Apply**.



General > Link Aggregation Statistics

Use this page to view information about configured LAGs. Use the **Options** (⋯) button to refresh the page.



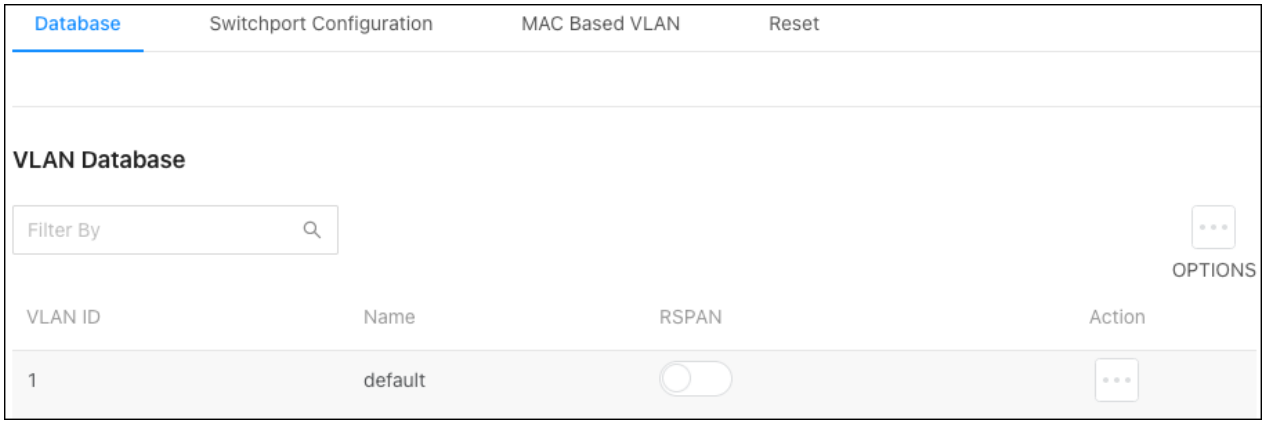
VLANs

Database

Use this page to add and view VLANs that have been configured on the switch, and to enable or disable **Remote Switched Port Analyzer** (RSPAN).

VLANs must still be applied to ports on the **VLANs** >**Switchport Configuration** page.

RSPAN allows you to mirror traffic from multiple source ports (or from all ports that are members of a VLAN) from different network devices and send the mirrored traffic to a destination port (a probe port connected to a network analyzer) on a remote device. The mirrored traffic is tagged with the RSPAN VLAN ID and transmitted over trunk ports in the RSPAN VLAN.



You can use the RSPAN toggle to enable or disable the feature or use the **Options** (⋯) button to select multiple VLANs to enable RSPAN on.

Use the **Actions** button to select an individual VLAN and give it a meaningful **Name**.

Use the **Options** (⋯) button to add a new VLAND ID to the switch.

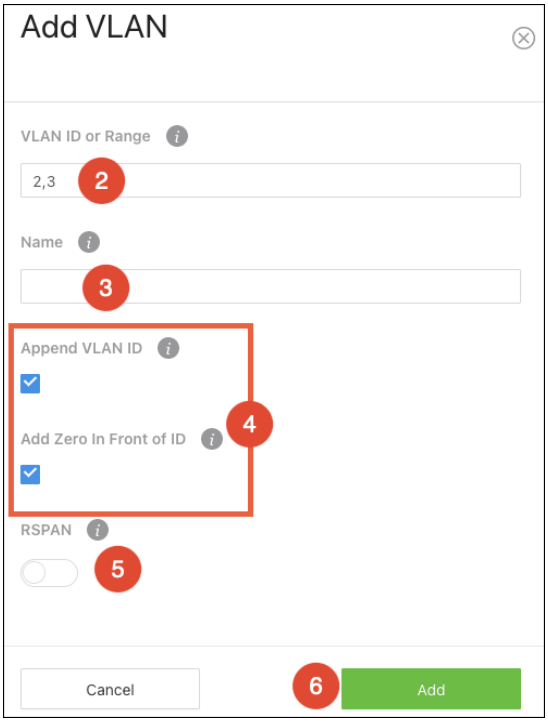
Configure the VLAN in the router before configuring the VLAN in the switch.

To add a VLAN(s) to the switch:

1. Click the **Options** (⋯) button, then click **Add**.
2. Enter the **VLAN ID**, within the range of 2-4093. Use "-" between numbers to indicate a range. Use "," to enter multiple VLAN IDs not adjacent to each other.
3. You can a meaningful **Name** for the VLAN or leave the field blank.
4. **Append** and/or **Add Zeros** in front of the VLAN ID. This allows the switch to quickly create identifiers if you're adding multiple VLANs at once.

- **Append VLAN ID** — Checking this appends the VLAN ID after the name. For example, VLAN -> VLAN2.
- **Add Zero in Front of ID** — Checking this adds zeroes in front of the VLAN ID, up to a total of 4 digits. For example, VLAN2 -> VLAN0002, VLAN123 -> VLAN0123. This only works when Append VLAN ID is selected.

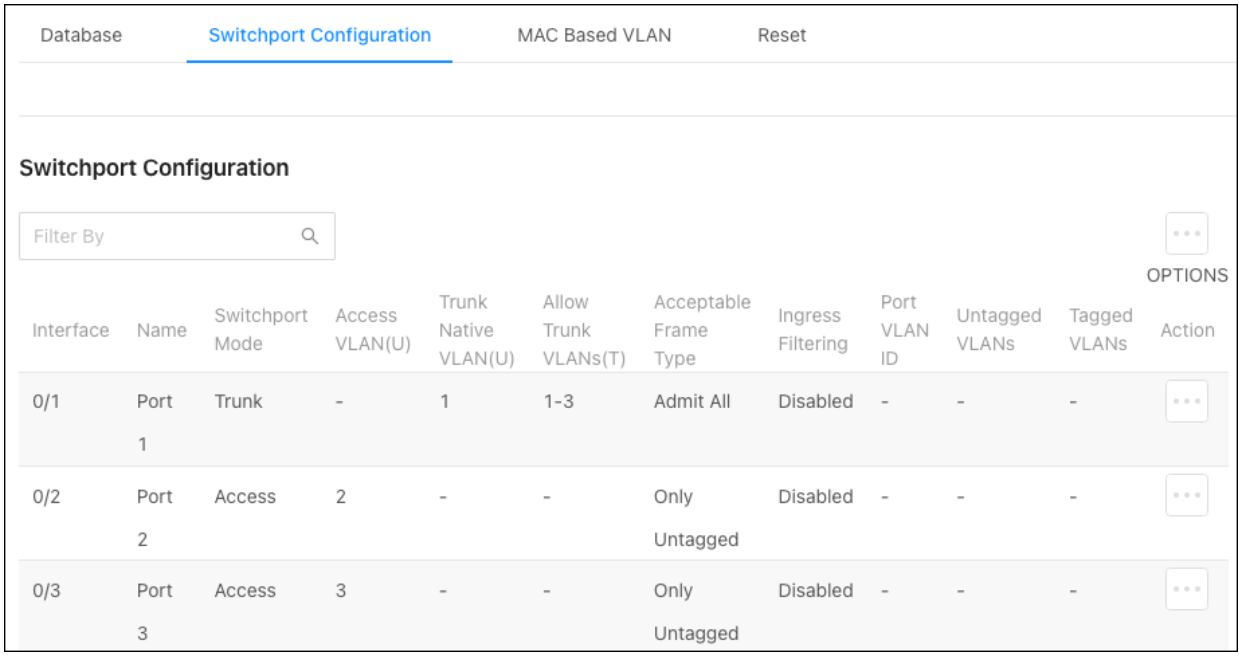
5. Enable **RSPAN**, if desired.
6. Click **Add**, then **Apply** at the top of the page.



Switchport Configuration

Use this page to quickly view and configure VLANs on specific ports. Use the **Options** ( ) button to modify multiple ports at once, or the **Action** button to edit a specific port.

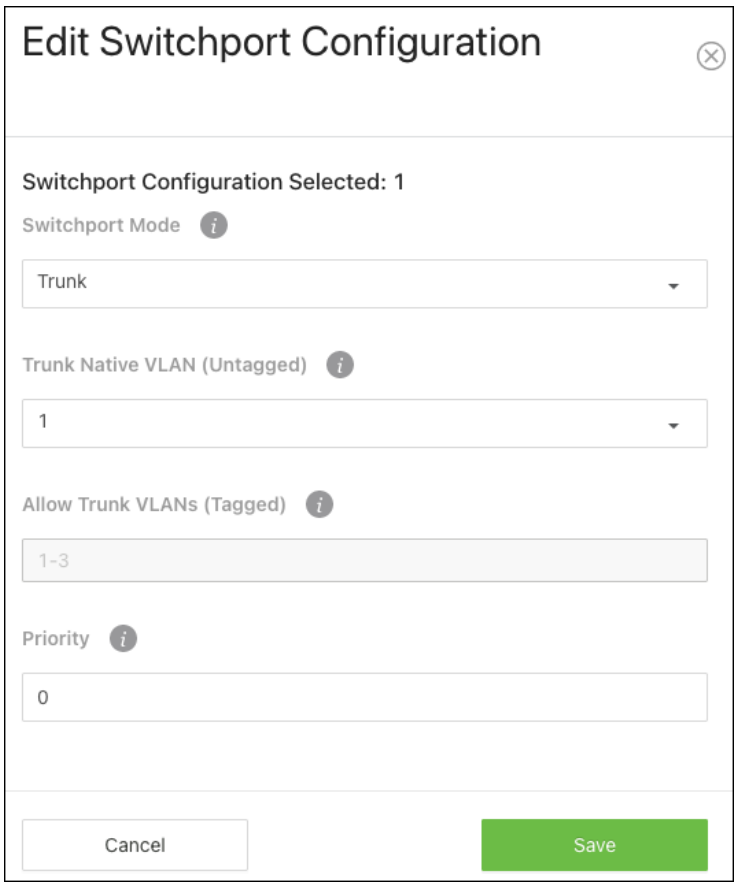
VLAN IDs must be configured on the **VLANs** > **Database** page.



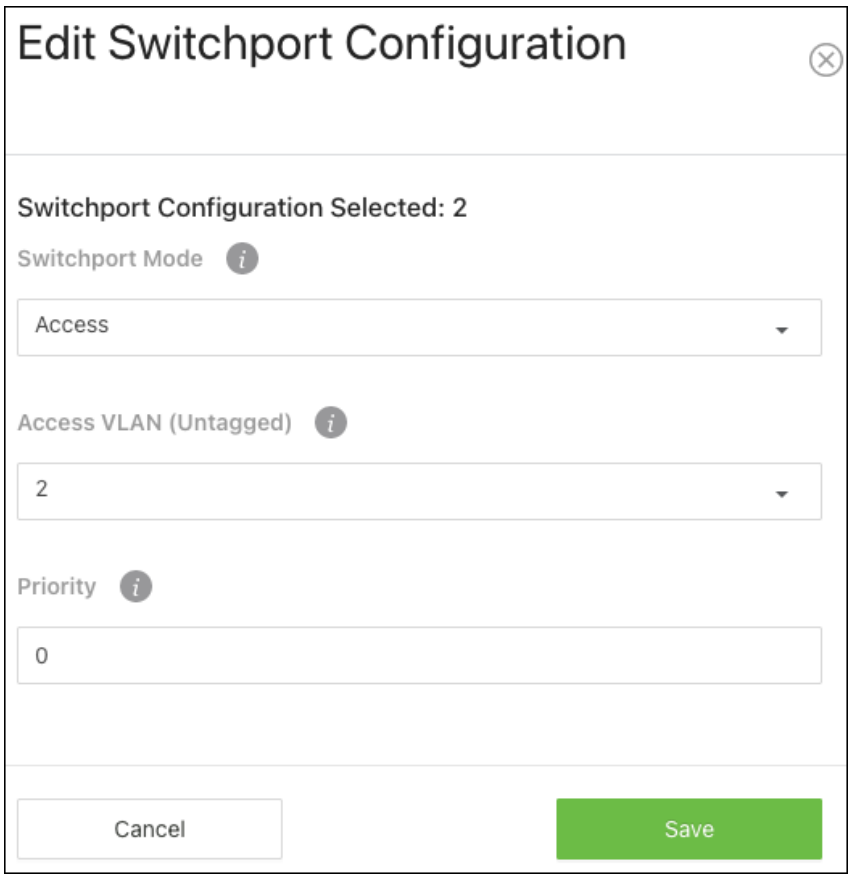
Simple configuration

To quickly configure a port(s) for VLANs, set the **Switchport Mode** to **Trunk** or **Access**.

Selecting Trunk automatically allows all the VLAN IDs configured in the switch to pass through the port. Connections to other switches are typically trunk ports.



Selecting Access requires you to select a single VLAN ID as the **Access VLAN (Untagged).** This means that only packets tagged with the selected VLAN ID can pass through this switchport.



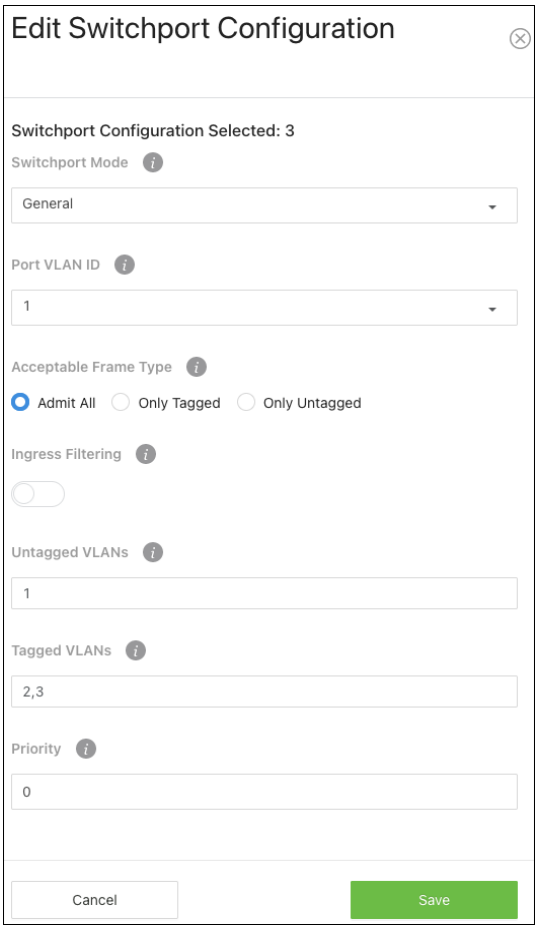
Complex configuration

If the port must pass multiple VLANs but not all, select **General** as the switchport mode.

Configurable settings include:

- **Port VLAN ID (PVID)** — Select the VLAN ID assigned to untagged, or priority tagged frames received on this port.
- **Acceptable Frame Type** — Tell the port how to handle traffic with tagged frames. All tagged VLAN frames are forwarded in accordance with the IEEE 802.1Q VLAN standard. Options include:
    - **Admit All** — The port accepts priority tagged and untagged frames and assigns them the value of the PVID assigned to the interface.
    - **Only Tagged** — The port discards any untagged or priority tagged frames it receives.
    - **Only Untagged** — The port discards any tagged frames it receives.
- **Ingress Filtering** — Enable to discard tagged frames that aren't members of the VLAN ID assigned to the port. Leave this feature disabled to accept all tagged frames.
- **Untagged VLANs** — Enter a VLAN ID in the range 1 to 4093. Use '-' to specify a range and ',' to separate VLAN IDs or VLAN ranges in the list.
- **Tagged VLANs** — Enter a VLAN ID in the range 1 to 4093. Use '-' to specify a range and ',' to separate VLAN IDs or VLAN ranges in the list.

- **Priority** — The default 802.1p priority assigned to untagged packets arriving at the interface. 802.1p is a Quality of Service (QoS) value used to differentiate traffic.

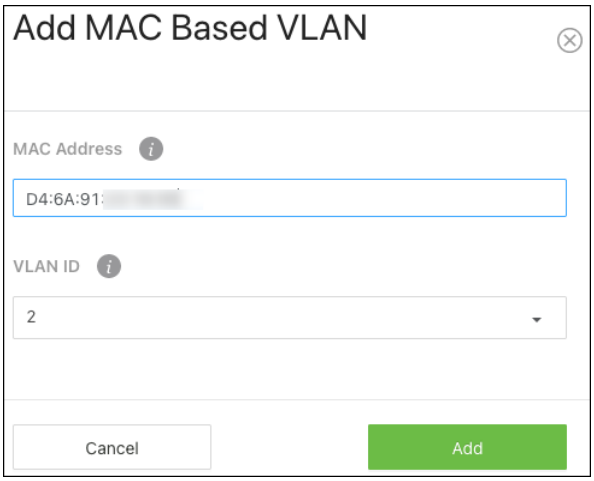


MAC Based VLAN

Use this page to bind traffic from a MAC address to a VLAN ID.

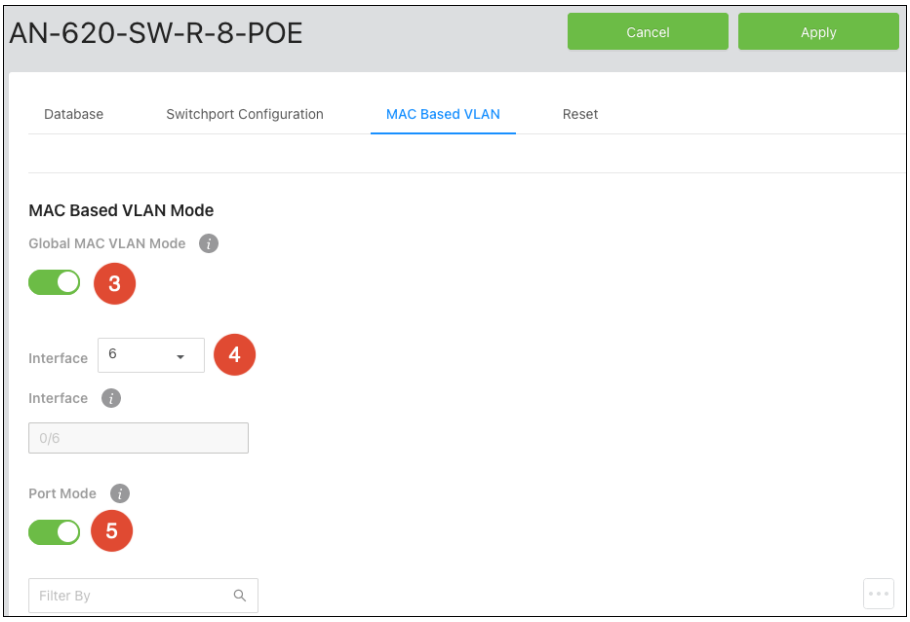
To configure a MAC based VLAN:

1. Click the **Options** (⋯) button, then **Add**.
2. Enter the **MAC address** you wish to bind to a VLAN ID, then select the **VLAN ID** to bind it to. Click **Add**.



3. Enable **Global MAC VLAN Mode**.
4. Select the **Interface** (switchport) to apply the MAC Based VLAN to.

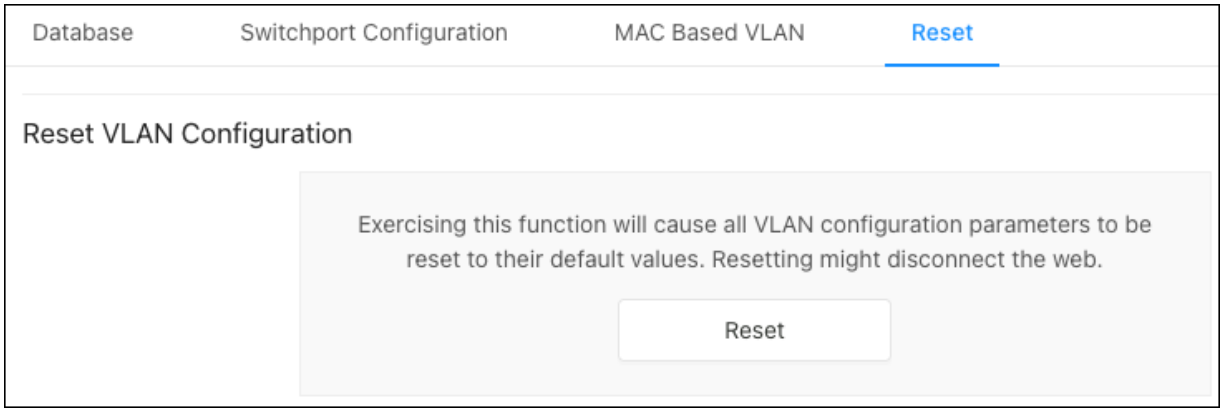
5. Enable **Port Mode**, then click **Apply** at the top of the page.



6. The MAC Based VLAN appears at the bottom of the page.

Reset

Click the **Reset** button to reset all the VLAN settings on the switch.

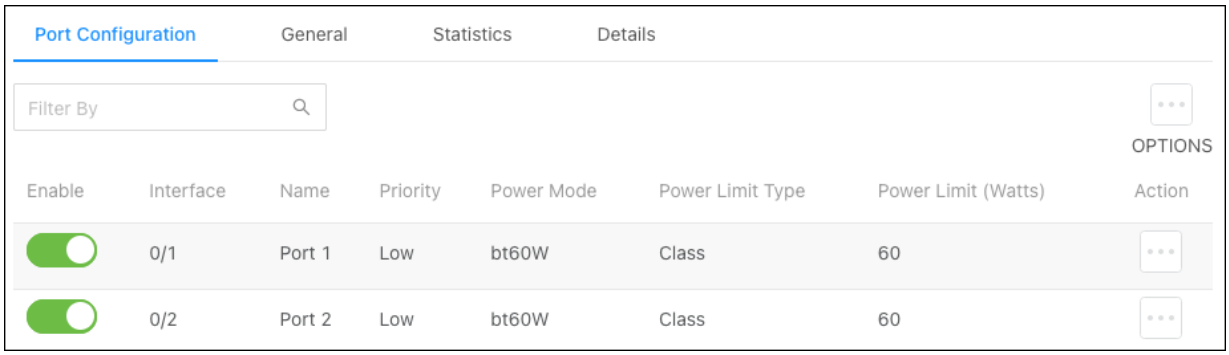


PoE

Port Configuration

Use this page to quickly enable/disable PoE on ports and view the PoE configuration on each port.

Use the **Options** (⋯) button to select multiple ports for configuration or the **Action** button to edit an individual port.



Configurable settings include:

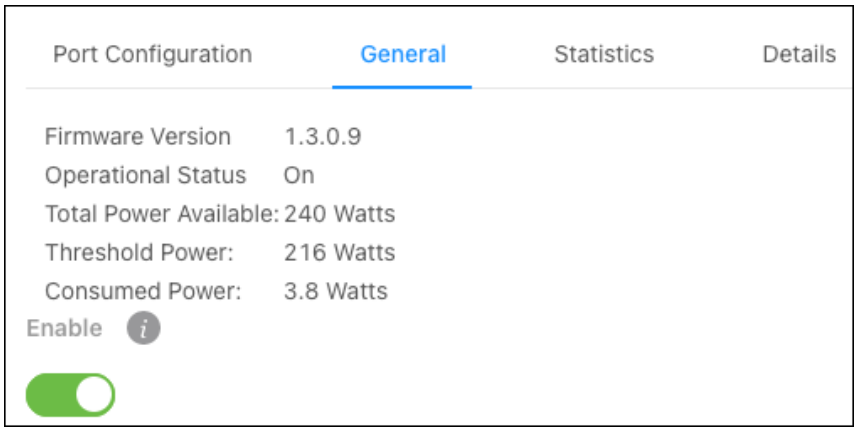
- **Enable** — Toggle to enable/disable PoE on the port.
- **Priority** — Set a priority level for PoE power allocation. Higher priority levels should be reserved for devices that are critical for the system to operate, such as access points.
- **Power Mode** — Set the PoE power standard for the port. Selecting a PoE class supports the PoE+ power standard, which provides up to 60W of power. Legacy supports 3W – 15W of power. Supported power modes include:
  - bt60W (default)
  - at30W
  - af15W
  - Legacy
- **Power Limit Type** — Select the type of power limiting for the port. Options include:

- **Class (default)** — Follows the negotiated PoE class limitations.
- **User** — Follows the Power Limit (Watts) setting.
- **None** - No power limit.

- **Power Limit (Watts)** — Enter the maximum amount of watts that the port can support.
- **Detection Type** — Select a detection protocol for the port to use. Options include:
  - 4Pt-Dot3af (default)
  - 4Pt-Dot3af+Legacy
  - Legacy
  - None

General

Use this page to configure global PoE settings for the switch. The top of the page displays PoE totals.



Configurable features include:

- **Enable** — Enable or disable PoE for the entire switch.
- **System Usage Threshold** — Enter the total percentage of the switch's usable PoE budget. For example, setting the threshold to 90% means that only 90% of the switch's total PoE budget can be used. This prevents the switch from being

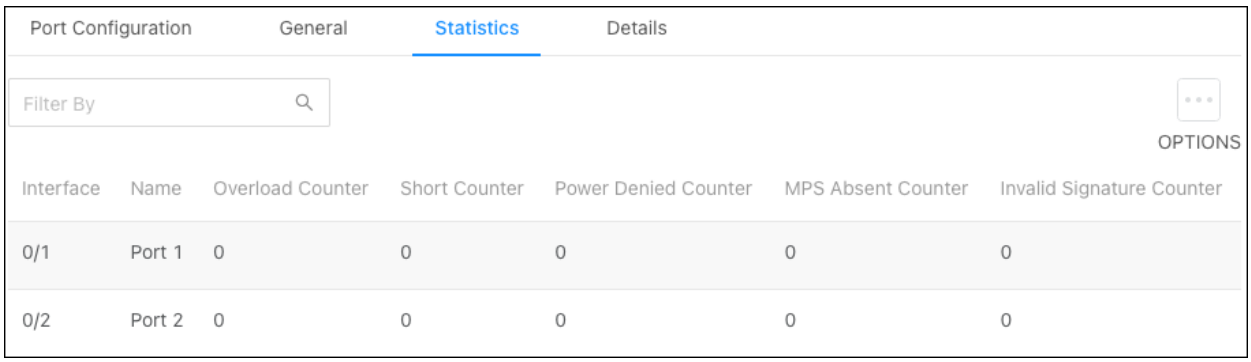
overloaded.

- **Power Management Mode** — Select the method that the switch determines PoE. By default, the switch decides PoE power dynamically, but you can set it to static. Doing so requires manual wattage entry on the Port Configuration page.
- **Port Auto Reset Mode** — Enable or disable the ability for the switch to automatically reset a port.
- **Traps** — Enable to allow the switch to send alerts about PoE statuses, such as PoE being enabled or disabled on a port.
- **Fast PoE Mode** — Enable Fast PoE for the switch to provide PoE power before the boot process completes.
- **Perpetual PoE Mode** — Enable to allow the switch to continue providing PoE power if the switch is restarting.

Statistics

Use this page to view PoE error counts when troubleshooting potential PoE issues.

An error on the switch confirms there is a PoE issue, but it does not mean the issue is caused by the switch. Troubleshoot the connected device and Ethernet cable.



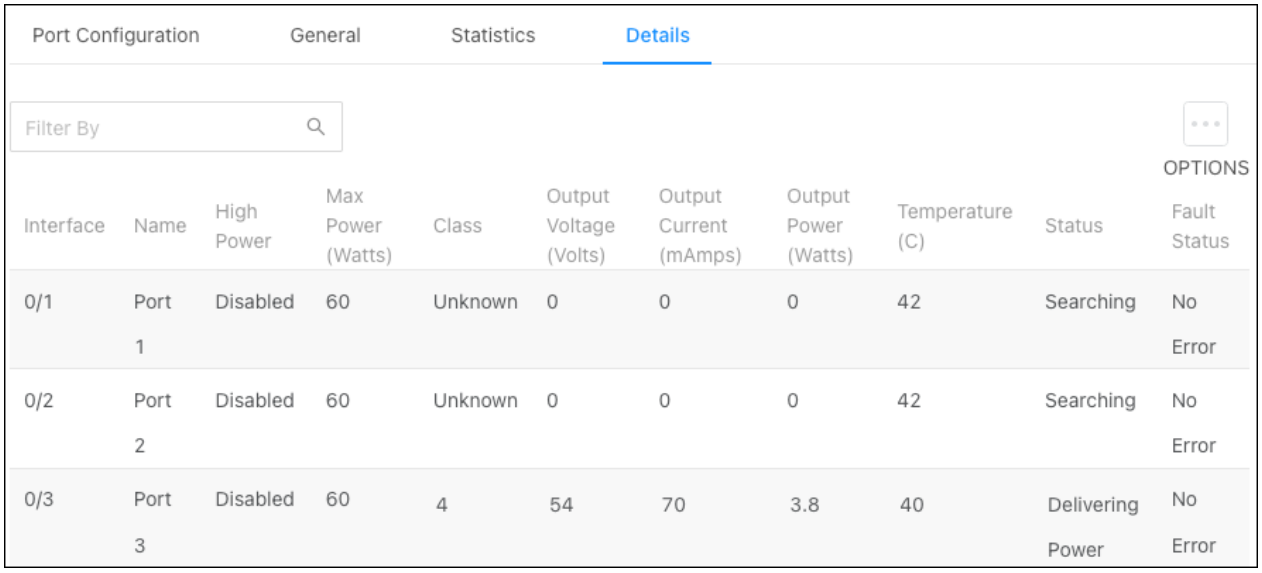
Interface	Name	Overload Counter	Short Counter	Power Denied Counter	MPS Absent Counter	Invalid Signature Counter
0/1	Port 1	0	0	0	0	0
0/2	Port 2	0	0	0	0	0

Counter explanations:

- **Overload Counter** — The number of times there has been a power overload.
- **Short Counter** — The number of times there has been a short-circuit condition.
- **Power Denied Counter** — The number of times the connected device has been denied power.
- **MPS Absent Counter** — The number of times power has stopped because the powered device couldn't be detected.
- **Invalid Signature Counter** — The number of times an invalid signature was received.
  Signature detection is used to detect the presence of a powered device, where a resistance value on the connected device is expected to be found within a particular range.

Details

Use the details page to gather information about the PoE status of each port. Click **Options** (⋯), then **Refresh** to update the page.



Tools

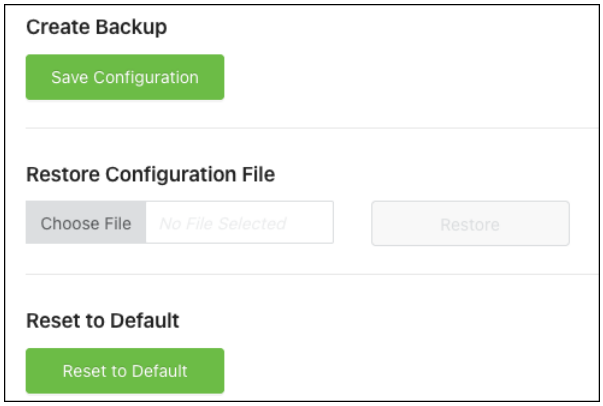
Firmware Management

Use this page to manually update the firmware on the switch. The image selected when loading the page is the active image. If the firmware fails to boot, the switch switches to the other image as a failsafe.

Pro Tip: Use OvrC to confirm if the switch is up to date. If not, click the Update button for OvrC to update the switch to the latest firmware. OvrC automatically switches between the active and backup images when performing upgrades.

Configuration Management

Use this page to save a backup of the switch's configuration or to reset the switch to the default settings.

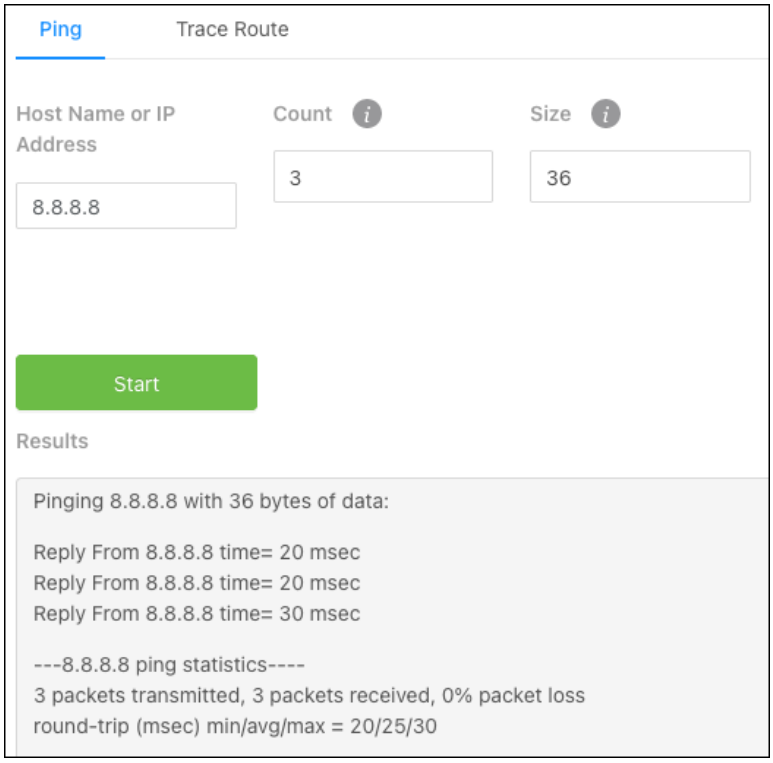


Diagnostic Utilities

Ping

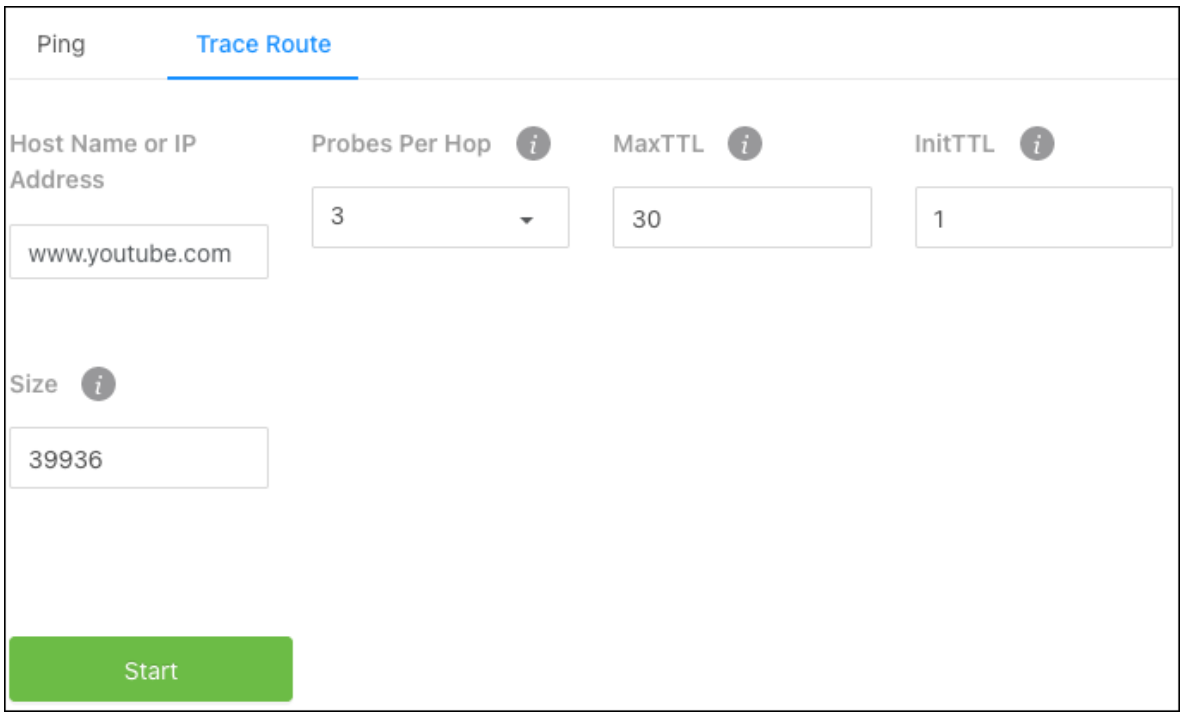
Use a ping test to measure the amount of time it takes to reach an address on the local network or the internet. You can enter the IP address or the hostname, such as www.wikipedia.com.

Pro Tip: Before selecting a DNS server, use a ping test to measure the fastest response time.



Traceroute

Use a traceroute to diagnose network interruptions between the switch and an address on the local network or the internet. You can enter an IP address or a hostname, such as www.youtube.com.


Ping
Trace Route
Host Name or IP Address
www.youtube.com
Probes Per Hop
3
MaxTTL
30
InitTTL
1
Size
39936
Start

Advanced

System

Management Access

Use the System Connectivity page to configure connection settings for the switch.

Configurable settings include:

- **Telnet** — Enable to allow telnet connections on port 23.
- **HTTPS** — Enable to require an HTTPS connection for the switch's local interface. When enabled, you must type **https://** before the IP address in your browser's address bar.
- **SSH** — Enable to allow SSH connections. You can specify the **port** to use and The **Session Timeout,** in seconds.

SNTP

Global Configuration

Use this page to configure the **Simple Network Time Protocol (SNTP)** to make the switch's clock time accurate to the millisecond.

The SNTP server the switch synchronizes to is configured on the **Server Configuration** tab.

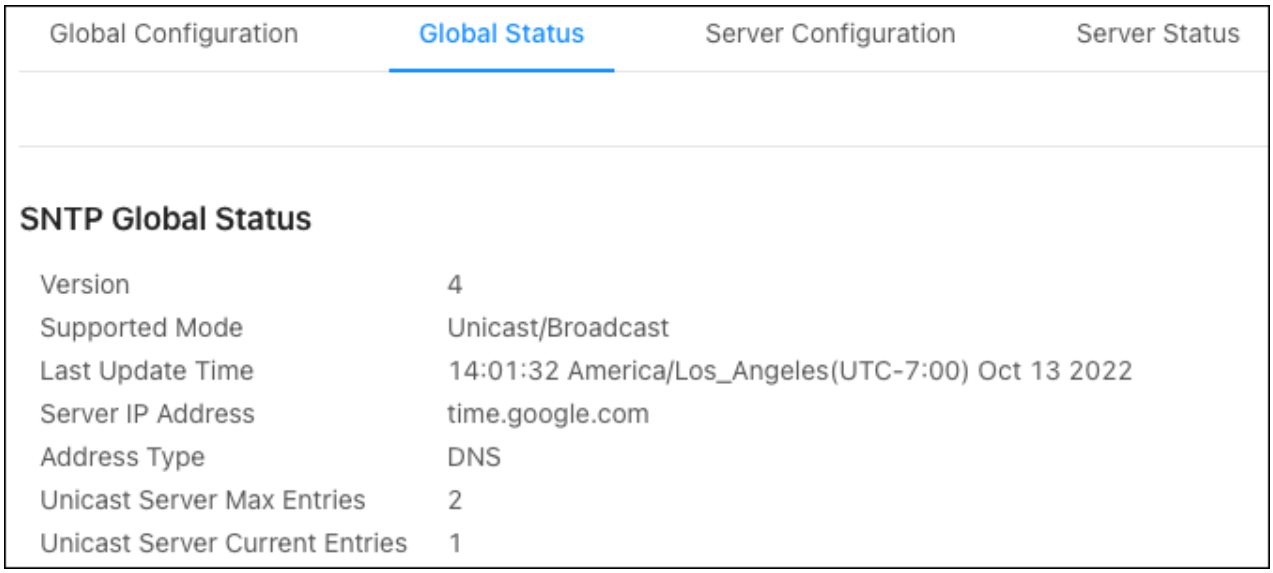
Configurable settings include:

- **Client Mode** — Use the dropdown to determine how SNTP operates. Options include:

    - **Unicast** — Makes STNP operate in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply to determine the time, and potential round-trip delays to calculate an offset from the local time.
    - **Broadcast** — SNTP operates like it's multicast but uses a local broadcast address instead of a multicast address. The broadcast address has a single subnet scope, while a multicast address has an internet-wide scope.
    - **Disable** — Disables the SNTP protocol on the switch.
- **Port** — Enter a local UDP port to listen for responses and/or broadcasts.
- **Unicast Poll Interval (Seconds)** — Enter the number of seconds between unicast poll requests, expressed as a power of two when configured in unicast mode.
- **Unicast Poll Timeout (Seconds)** — Enter the number of seconds between broadcast poll requests, expressed as a power of two when configured in unicast mode. Broadcasts received prior to the expiry of the interval are discarded.
- **Broadcast Poll Timeout (Seconds)** — Enter the maximum amount of time to wait for a poll to complete, between 1 - 30 seconds
- **Broadcast Delay Time (microseconds)** — Enter the maximum amount of time the SNTP client needs to wait for a response from the server, bewteen 1000 -15000 microseconds.
- **Broadcast SNTP Server** — Displays the SNTP server of broadcast.
- **Unicast Poll Retry** — Enter the number of times to retry a request to an SNTP server after the first time-out before attempting to use the next configured server when configured in unicast mode.
- **Number of Servers Configured** — Displays the number of SNTP servers configured on the Server Configuration tab.

Global Status

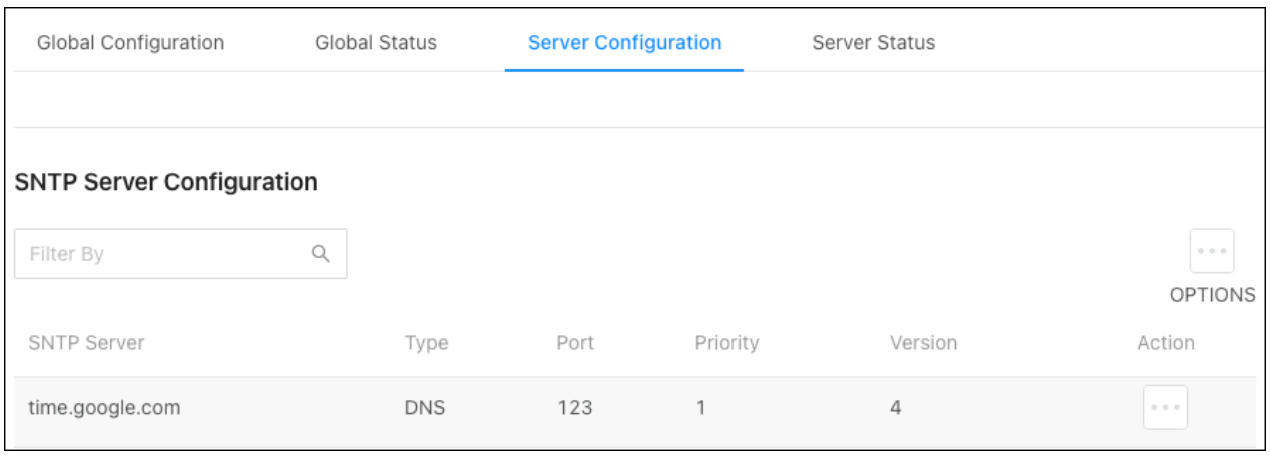
Use this page to view the SNTP server configuration of the switch.



Server Configuration

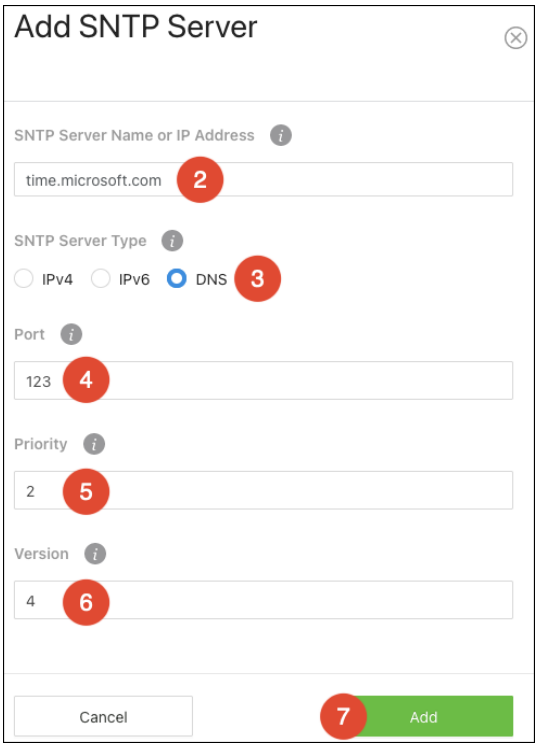
Use this page to add SNTP servers and configure the priority of which server should be used first, and which should be used in case the servers with a higher priority cannot be contacted.

Use the **Options** (⋯) button to refresh the page, add, or select multiple servers to configure. Use the **Action** button to edit or delete an existing SNTP server.



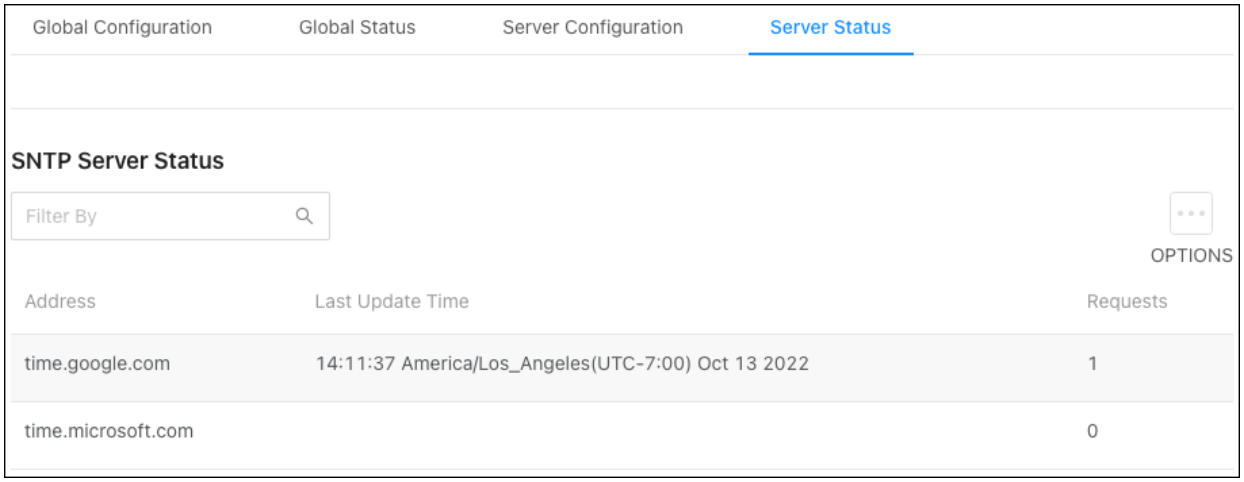
To add an SNTP server:

1. Click **Options** (⋯), then **Add**.
2. Enter an SNTP Server Name or IP Address.
3. Select an **SNTP Server Type**, meaning whether it's an IPv4, IPv6, or DNS address.
4. Enter a UDP Port the SNTP server to communicate on.
5. Enter the **Priority** level that the SNTP server should be used. If it's a fallback address in case the default SNTP server fails, enter 2.
6. Enter the protocol **Version** number. The default is 4.
7. Click **Add**, then **Apply** at the top of the page.



Server Status

Use this page to see the last updated time the switch has received from the configured SNTP server(s) and how many requests the switch has made to the server(s).

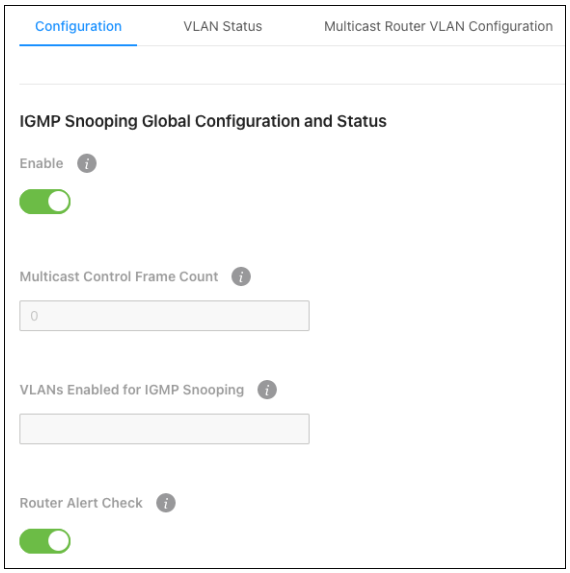


Switching

IGMP Snooping

Configuration

Use this page to enable IGMP Snooping on the switch and view related counts.



Configurable settings:

- **Enable** — Enables/disables IGMP snooping on the switch.
- **Router Alert Check** — Enable for the switch to inspect packets when they are being forwarded, even though the packet is not directly addressed to this switch.

Read-only fields:

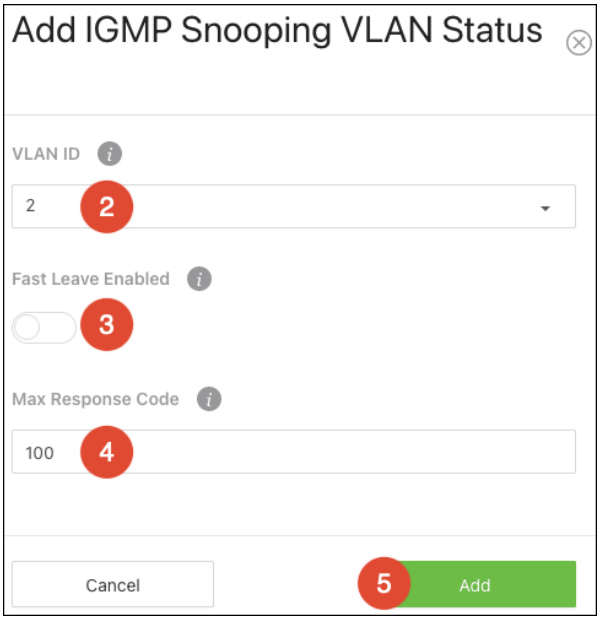
- **Multicast Control Frame Count** — The number of multicast frames the switch has processed.
- **VLANS Enabled for IGMP Snooping** — The number of VLANs configured on the switch for IGMP snooping.

VLAN Status

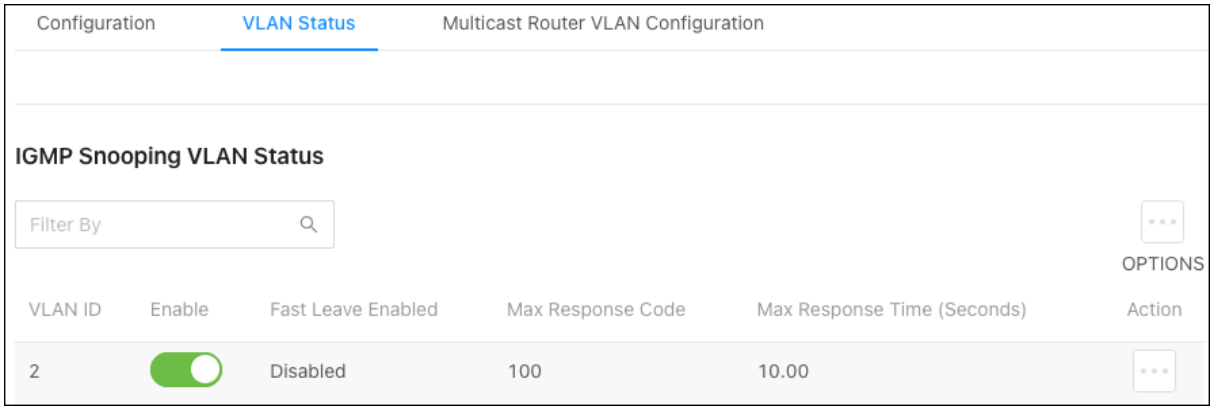
Use this page to add VLANs to the IGMP configuration of the switch.

To configure a VLAN for IGMP snooping:

1. Click **Options** (⋯), then **Add.**
2. Select a **VLAN ID.**
3. Enable **Fast Leave** if the multicast streams are each more than half the available bandwidth of the switch port.
4. The **Max Response Code** field displays the maximum time allowed before the switch sends a responding report. The default value is 100.
5. Click **Add**, then **Apply** at the top of the page.

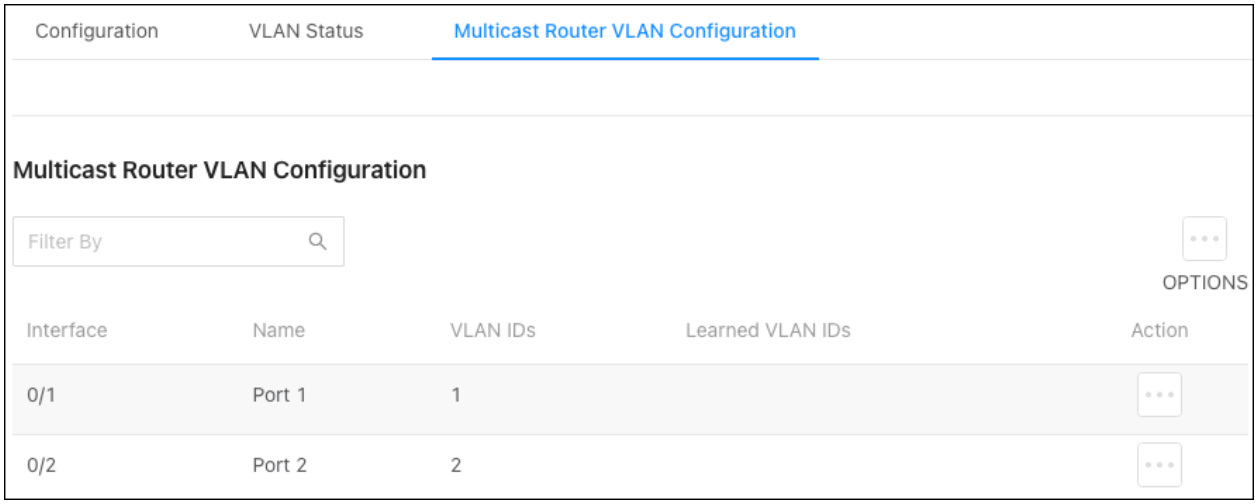


VLANs configured for IGMP Snooping appear at the bottom of the page.



Multicast Router VLAN Configuration

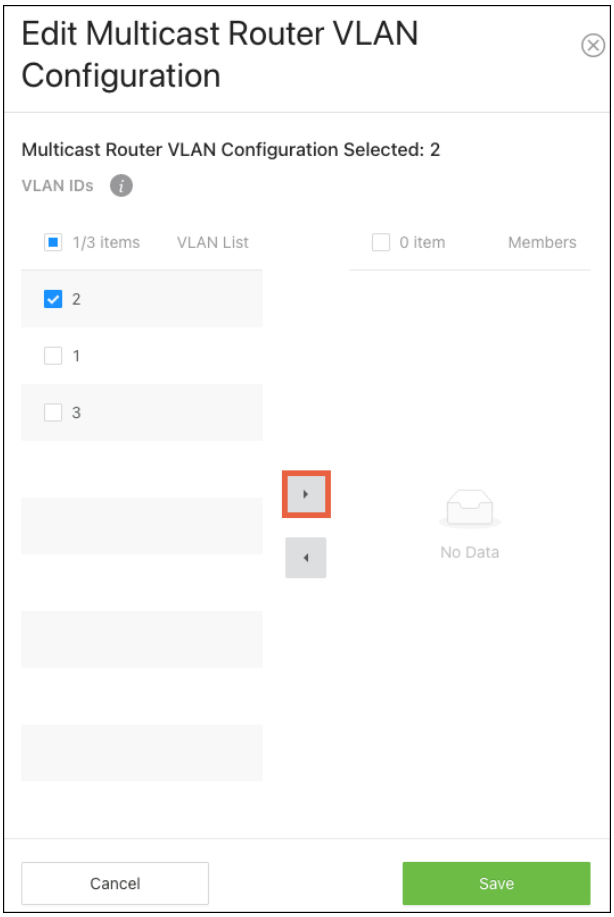
Use this page to configure VLANs for multicast routing. When enabled, multicast routers learn which multicast groups are active by periodically checking with each member of the multicast group. Read Understanding Multicast & IGMP for more information about multicast groups.



To configure multicast routing:

1. Use the **Options** (⋯) button to configure multiple ports or the **Actions** button to edit a single port.
2. Select the **VLAN ID(s)** you want the port to act as the multicast router for, then click the **right arrow** to add them.

3. Click **Save**, then **Apply** at the top of the page.



IGMP Snooping Querier

VLAN Configuration

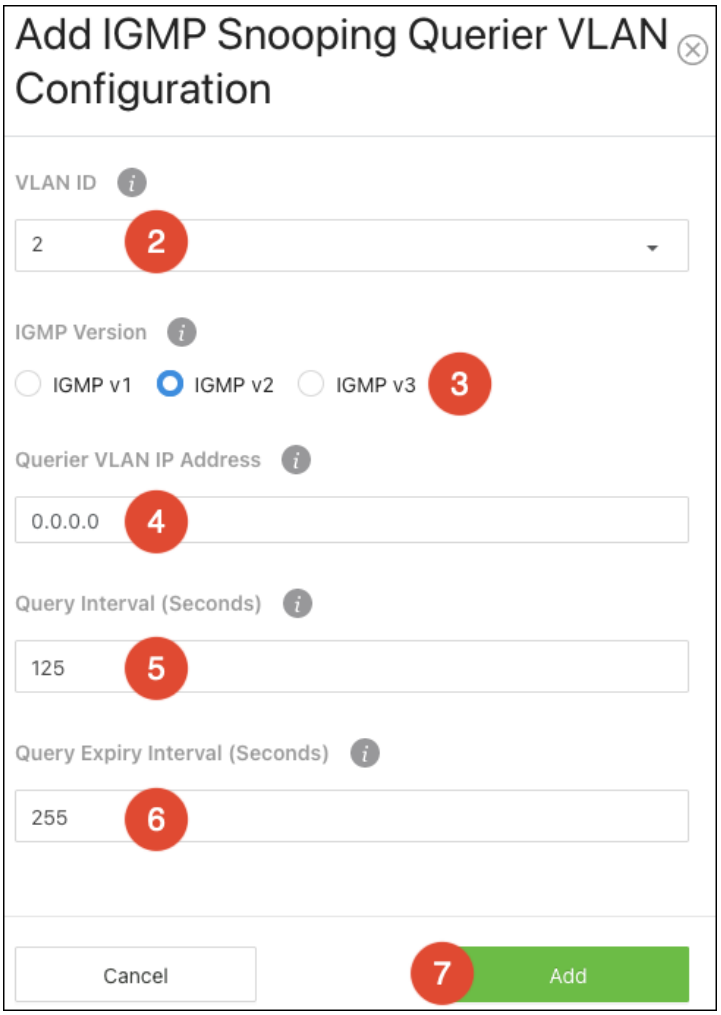
Use this page to add VLANs that the switch should act as the IGMP querier for. To learn more about IGMP queriers, read Understanding Multicast & IGMP.

Caution: Only enable **IGMP Snooping Querier** on the switch where your IGMP topology starts, called the **core IGMP switch**. This IGMP querying switch asks each device on the network which multicast traffic they want.

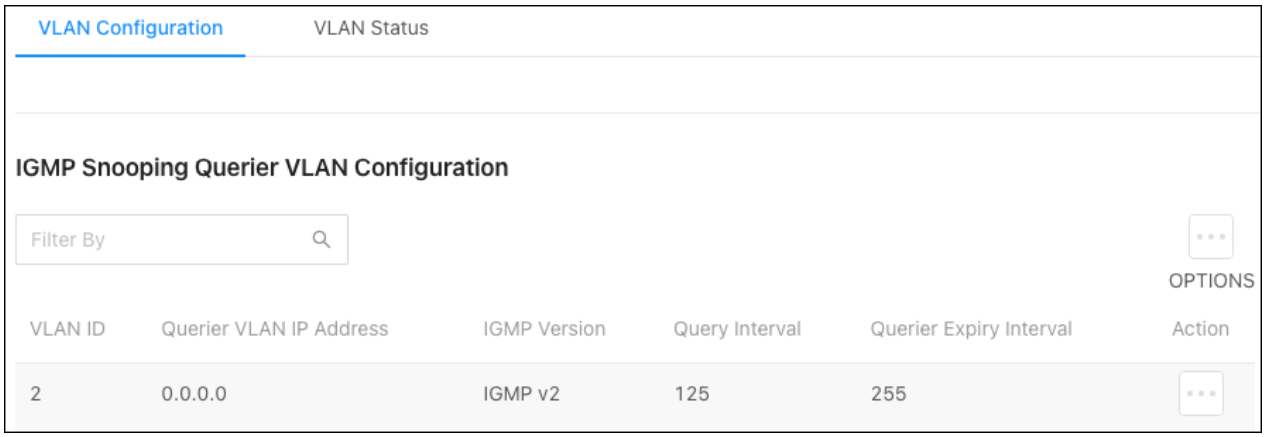
To add a VLAN to the switch's IGMP snooping querier configuration:

1. Click the **Options** button (), then **Add**.
2. Select a **VLAN ID**.
3. Select the **IGMP Version** to use when making inquiries.
4. The **Querier VLAN IP Address** is typically left at the default address (0.0.0.0), but it can be changed.
5. For the **Query Interval**, enter the amount of time (in seconds) that the IGMP snooping querier should wait between sending periodic IGMP queries. The default value is 125.
6. The **Query Expiry Interval** is the amount of time (in seconds) that the device remains in non-querier mode after it has discovered that there is a multicast querier in the network. The default value is 255.

7. Click **Add**, then **Apply** at the top of the page.

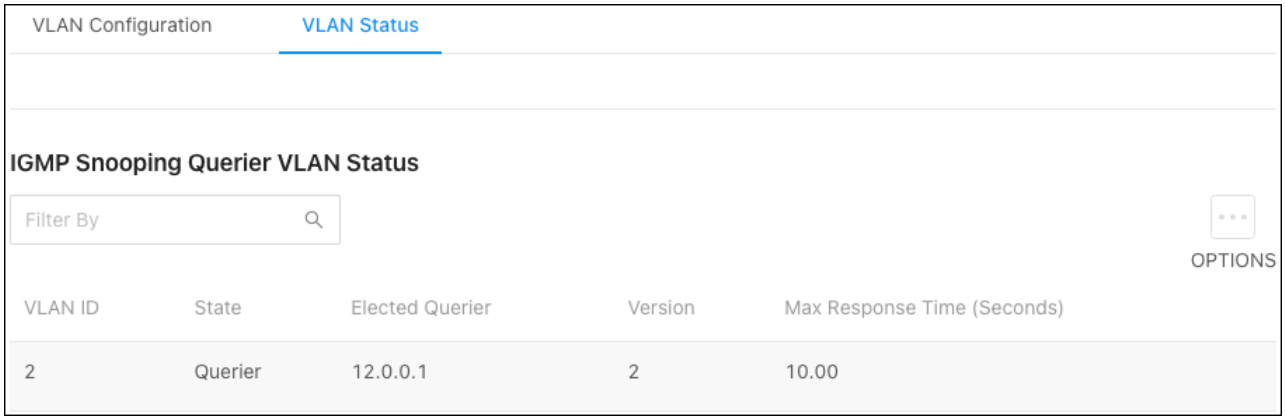


Configured VLANs are listed at the bottom of the page.



VLAN Status

Use this page to view information about the IGMP snooping querier status for all VLANs that have the snooping querier enabled.

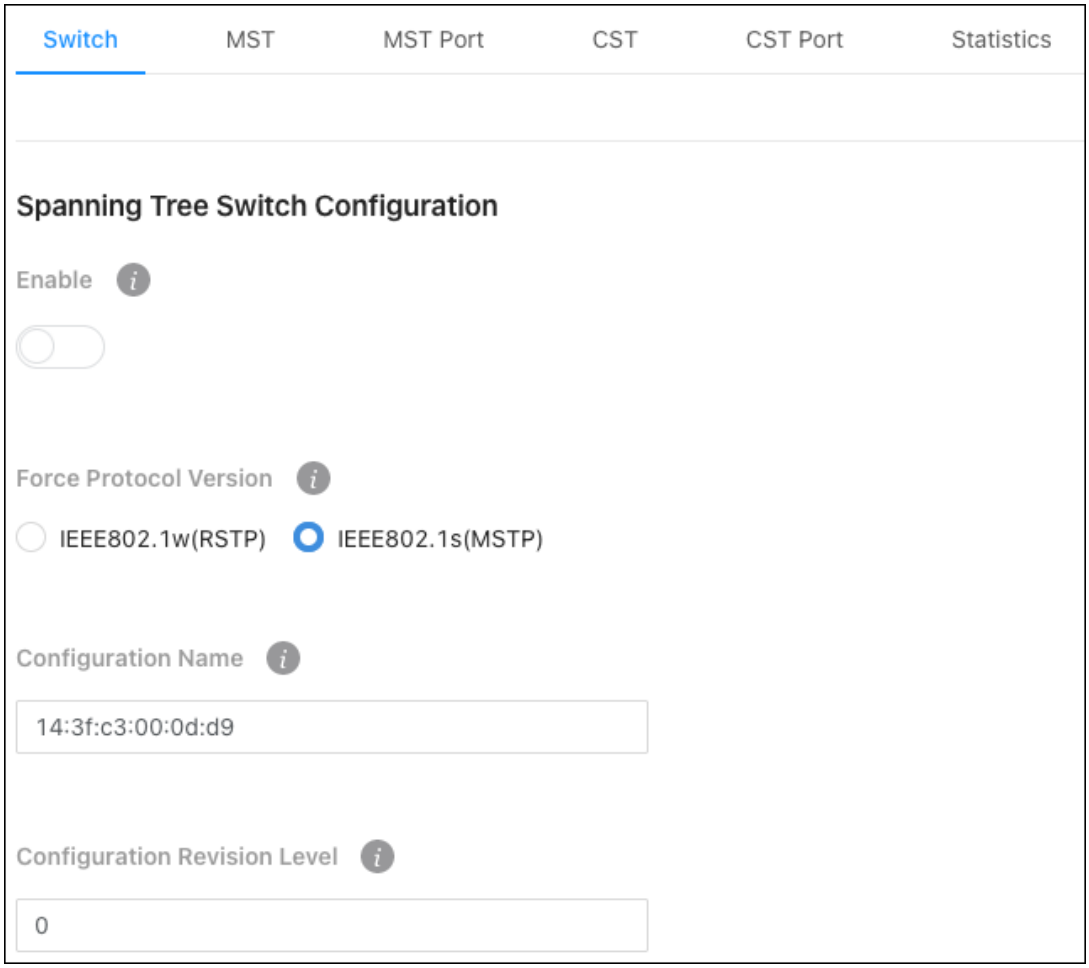


Spanning Tree Protocol

Switch

Use this page to configure global **Spanning Tree Protocol (STP)** settings for the switch.

STP is a Layer 2 protocol that decides the best path for LAN traffic when multiple options exist, preventing network loops while guaranteeing redundancy in case of link failure. For more information about STP, read Understanding Spanning Tree Protocol (STP) & Best Practices.



Configurable settings include:

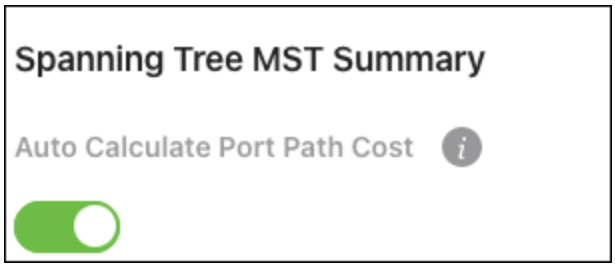
- **Enable** — Enables STP on the switch.
- **Force Protocol Version** — Choose the STP version for the switch to use.
    - **IEEE 802.1w (RTSP)**— Rapid Spanning Tree Protocol (RSTP) behaves like classic STP but can also configure and recognize full-duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to the Forwarding state and the suppression of Topology Change Notifications.
    - **IEEE 802.1s** (MSTP) — Multiple Spanning Tree Protocol (MSTP) includes all the advantages of RSTP and supports multiple spanning tree instances to efficiently channel VLAN traffic over different interfaces. MSTP is compatible with both RSTP and STP.
- **Configuration Name** — Typically left alone, you can enter the name of the MSTP region. Each switch that participates in the same MSTP region must share the same Configuration Name, Configuration Revision Level, and MST-to-VLAN mappings
- **Configuration Revision Level** — This number must be the same on all switches participating in the MSTP region.

MST

Use the MST Configuration page to view and configure the Multiple Spanning Tree Instances (MSTIs) on the device.

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

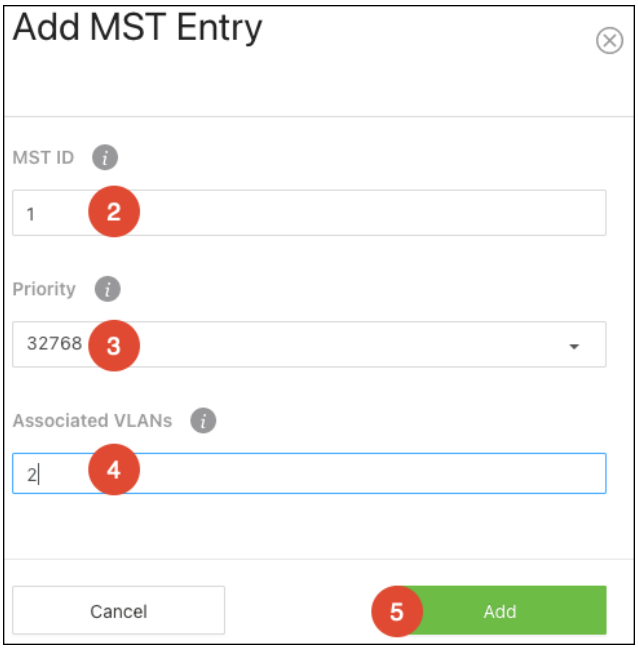
You can enable **Auto Calculate Port Path Cost** so the path cost from the port to the root bridge is automatically determined by the speed of the interface. If disabled, it must be configured manually.



To add an MST instance:

1. Click the **Options** button (⋯), then **Add**.
2. Enter a number for the **MST ID**.
3. Enter a **Priority** value. This value affects the likelihood that the bridge is selected as the root bridge. A lower value increases the probability that the bridge is selected as the root bridge. For more information, read Understanding Spanning Tree Protocol (STP) & Best Practices for more information.
4. Enter the VLAN ID(s) to map to the MST instance in the **Associated VLANs** field.

5. Click **Add**, then **Apply** at the top of the page.



MST instances appear in the table at the bottom of the page.

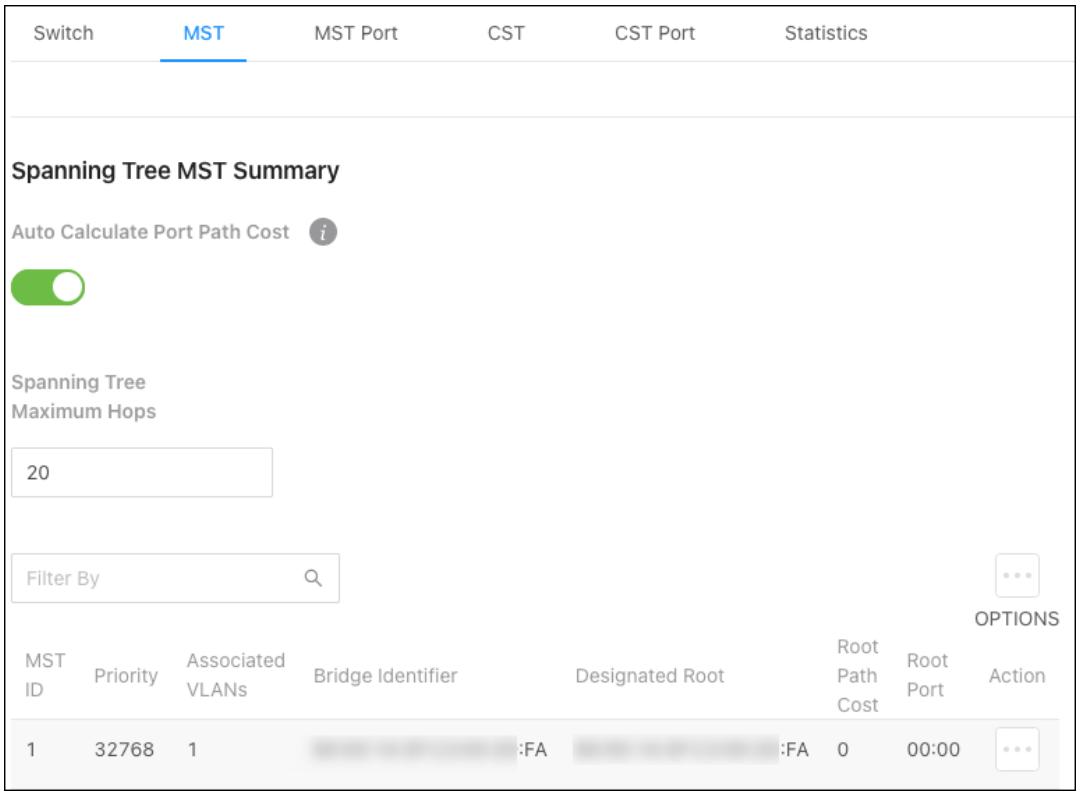


Table field descriptions:

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

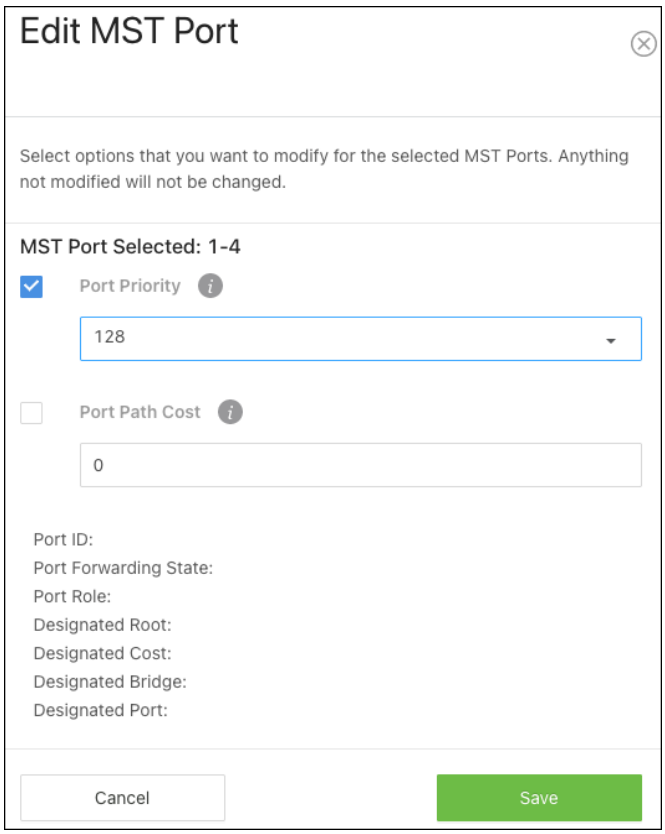
MST Port

Use this page to view and configure the Multiple Spanning Tree (MST) settings for each interface on the device.

You must configure an MST instance on the MST tab before configuring an interface.

To configure MST for an interface:

1. Select an **MST ID** from the dropdown.
2. Click the **Options** button (⋯), **Edit**, then select the Interface(s) and click **Edit Selected**. If you only want to edit a single port, click the Action button next to it, then click Edit.
3. Click to select the settings you want to modify, Port Priority or Port Path Cost, then click **Save**.



The MST Port Summary table displays information about the currently selected MST ID.

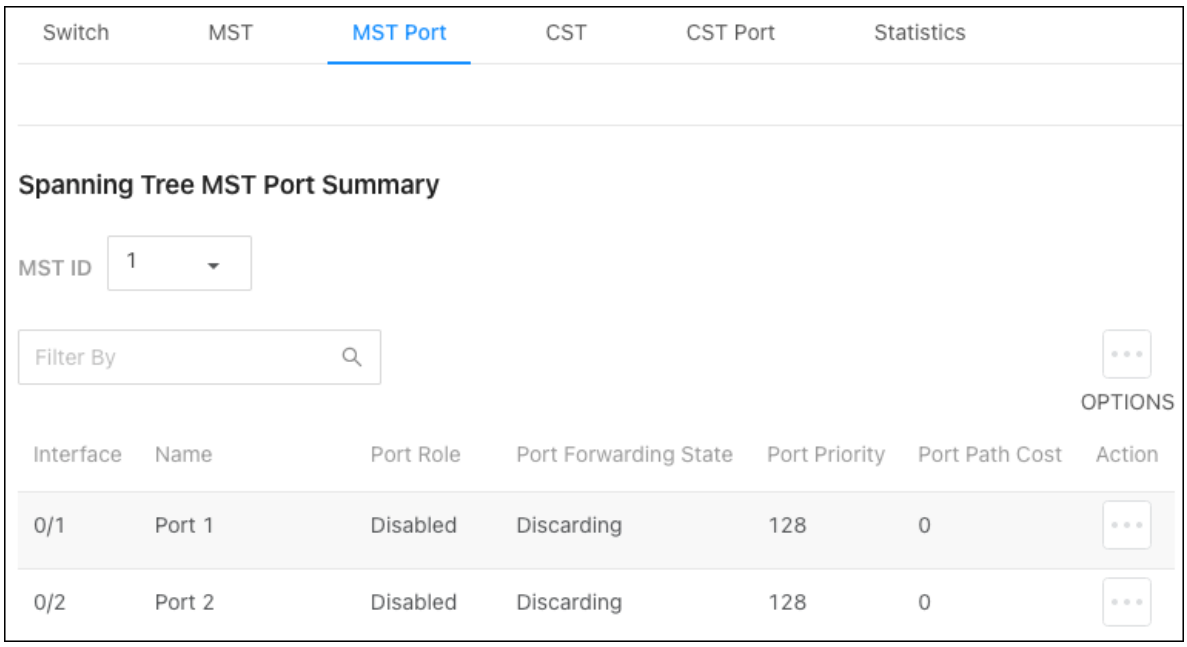


Table field descriptions:

- **Interface** — The port number.
- **Name** — The name given to the port. Configurable on **Settings** > **Ports** > **General** > **Port Summary** page.
- **Port Role** — The role of the port within the MST is one of the following:
  - **Root** — A port on the non-root bridge that has the least-cost path to the root bridge.
  - **Designated** — A port that has the least-cost path to the root bridge on its segment.
  - **Alternate** — A blocked port that has an alternate path to the root bridge.
  - **Backup** — A blocked port that has a redundant path to the same network segment as another port on the bridge.
  - **Master** — The port on a bridge within an MST instance that links the MST instance to other STP regions.

    - **Disabled** — The port is administratively disabled and is not part of the spanning tree.
- **Port Forwarding State** — How traffic is flowing through the port. States include:
    - **Blocking** — Blocks the flow of traffic. When a device is first connected to a port, it enters the blocking state.
    - **Learning** — The port is relaying information from a high-priority BPDU to the other ports on the switch.
    - **Disabled** — Disables the port.
    - **Err-disabled** — Allows STP to block the flow of traffic when it detects a loop, or forward traffic to a port if the connection changes.
- **Port Priority** - The bridge priority for the spanning-tree instance. This value affects the likelihood that the bridge is selected as the root bridge. A lower value increases the probability that the bridge is selected as the root bridge.
- **Port Path Cost** — The path cost from the interface to the MST regional root.

CST

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

Configurable settings include:

- **Bridge Priority** — This value affects the likelihood that the bridge is selected as the root bridge. A lower value increases the probability that the bridge is selected as the root bridge. For more information, read Understanding Spanning Tree Protocol (STP) & Best Practices for more information.
- **Bridge Max Age** — The amount of time a bridge waits before implementing a topological change.
- **Bridge Forward Delay** — The amount of time a bridge remains in a listening and learning state before forwarding packets.

- **Spanning Tree Maximum Hops** — The maximum number of hops a Bridge Protocol Data Unit (BPDU) is allowed to traverse within the spanning tree region before it is discarded.
- **BPDU Guard** — When enabled, this feature can disable edge ports that receive BPDU packets. This prevents a new device from entering the existing STP topology, so devices that were originally not a part of STP are not allowed to influence the STP topology.
  Pro Tip: Do not enable this feature unless there's a specific use case for it.
- **Spanning Tree TX Hold Count** — The maximum number of BPDUs that a bridge is allowed to send within a hello time window.
- **Auto Calculate Port Path Cost** — The path cost from the port to the root bridge is automatically determined by the speed of the interface. If disabled, it must be configured manually.

The bottom of the page provides general CST information.

Bridge Hello Time:	2
Bridge Identifier:	00:00:14:3F:C3:00:0D:D9
Time Since Topology Change:	0d:00:00:00
Topology Change Count:	0
Designated Root:	0:0:0:0:0:0:0:0
Root Path Cost:	0
Root Port:	00:00
Max Age:	20
Forward Delay:	15
Hold Time:	6
CST Regional Root:	00:00:14:3F:C3:00:0D:D9

CST Port

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

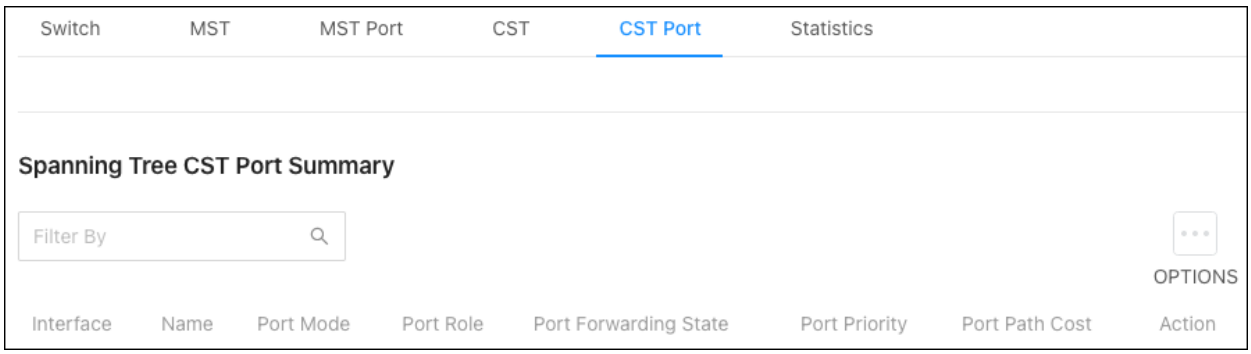


Table field descriptions:

- **Interface** — The port number.
- **Name** — The name given to the port. Configurable on **Settings** > **Ports** > **General** > **Port Summary** page.
- **Port Mode** — The role of the port within the CST, which is one of the following:
  - **Root** — A port on the non-root bridge that has the least-cost path to the root bridge.
  - **Designated** — A port that has the least-cost path to the root bridge on its segment.
  - **Alternate** — A blocked port that has an alternate path to the root bridge.
  - **Backup** — A blocked port that has a redundant path to the same network segment as another port on the bridge.
  - **Master** — The port on a bridge within an MST instance that links the MST instance to other STP regions.
  - **Disabled** — The port is administratively disabled and is not part of the spanning.
- **Port Forwarding State** — How traffic is flowing through the port. States include:

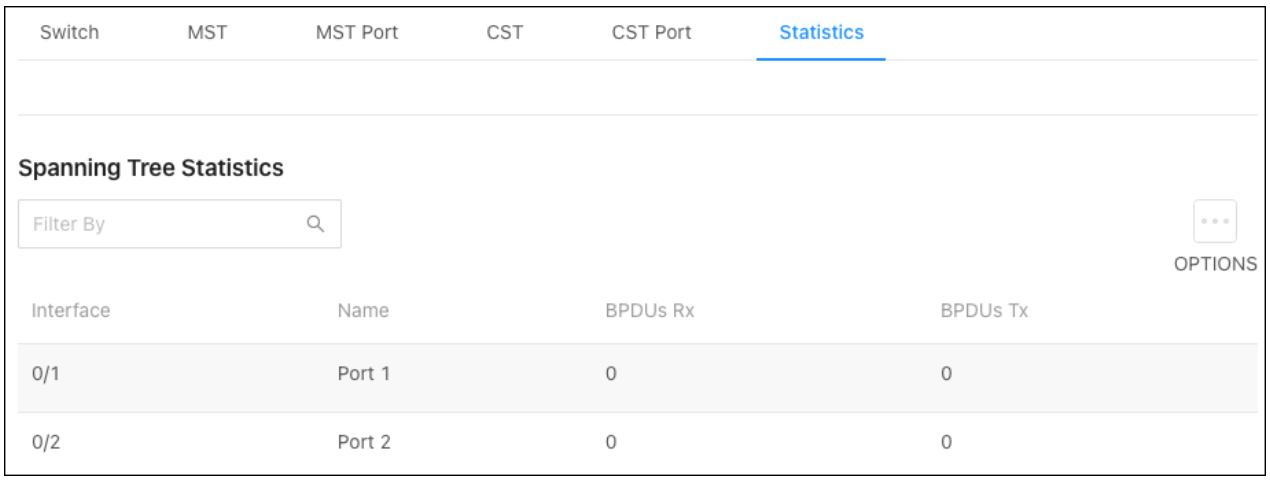
- **Blocking** — Blocks the flow of traffic. When a device is first connected to a port, it enters the blocking state.
- **Learning** — The port is relaying information from a high-priority BPDU to the other ports on the switch.
- **Disabled** — Disables the port.
- **Err-disabled** — Allows STP to block the flow of traffic when it detects a loop, or forward traffic to a port if the connection changes.

- **Port Priority** — The port's location in the network topology and how well it's situated to pass traffic.
- **Port Path Cost** — The path cost from the interface to the CST regional root.
- **Action** — Whether the port is permitting or denying traffic.

Click the **Action** button to edit a port's priority.

Statistics

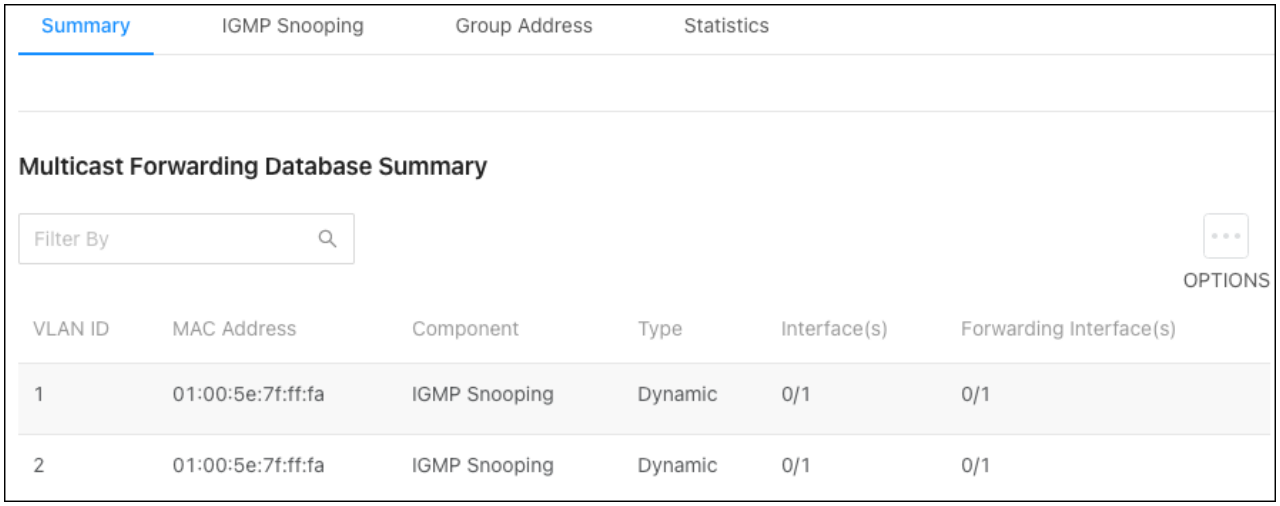
Use this page to view how many BPDUS have been transmitted and received on individual ports. Click the **Options** (⋯) button, then **Refresh** to get the latest statistics.



Multicast Forwarding Database

Summary

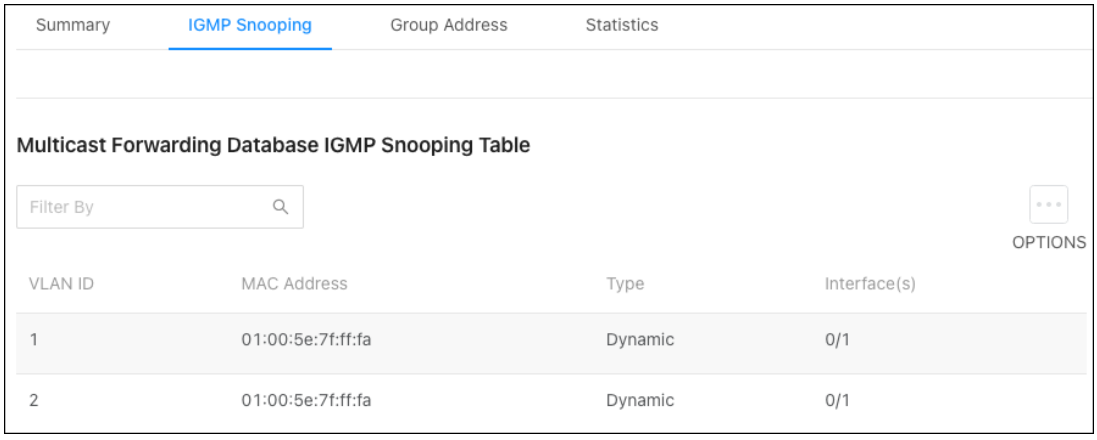
Use this page for a summary of the multicast data collected by the switch. Click **Options** (⋯), then **Refresh** to get the latest information.



IGMP Snooping

Use this table to gather information about the IGMP snooping traffic collected by the switch.

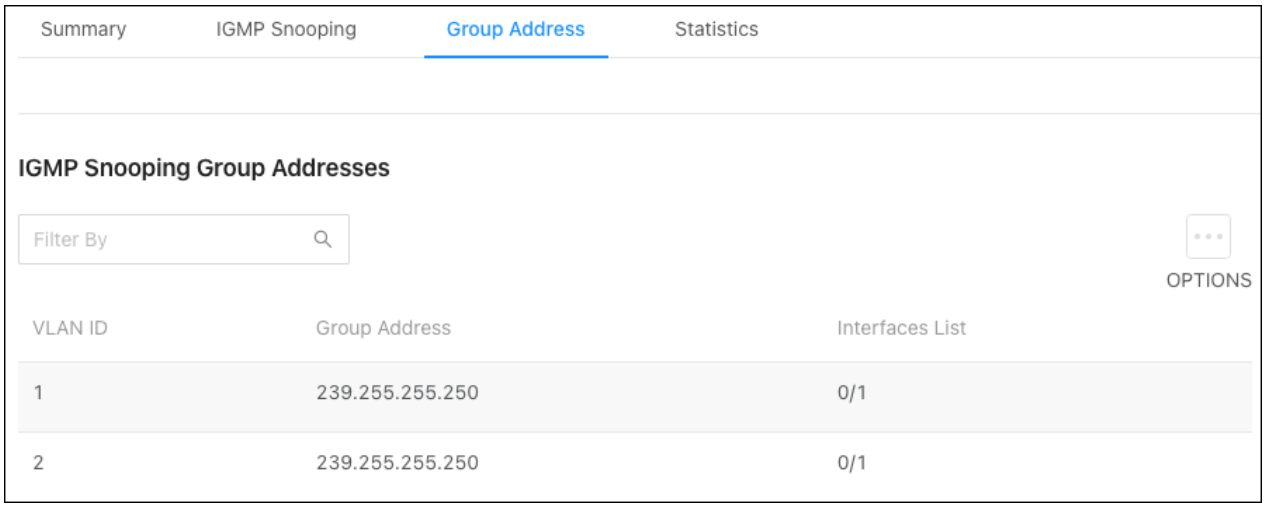
Click **Options** (⋯), then **Refresh** to get the latest information or click **Clear** to reset the table.



Note: Not all multicast traffic is handled by IGMP snooping. Read Understanding Spanning Tree Protocol (STP) & Best Practices for more information.

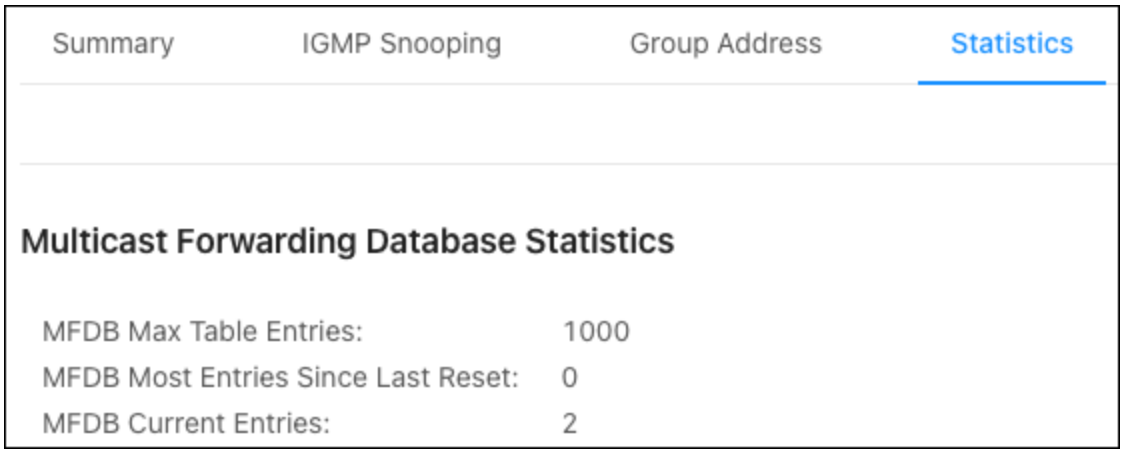
Group Address

Use this table to see the multicast group addresses the switch has recorded. Click **Options** (⋯), then **Refresh** to get the latest information.



Statistics

Use this page to view multicast statistics the switch has gathered.

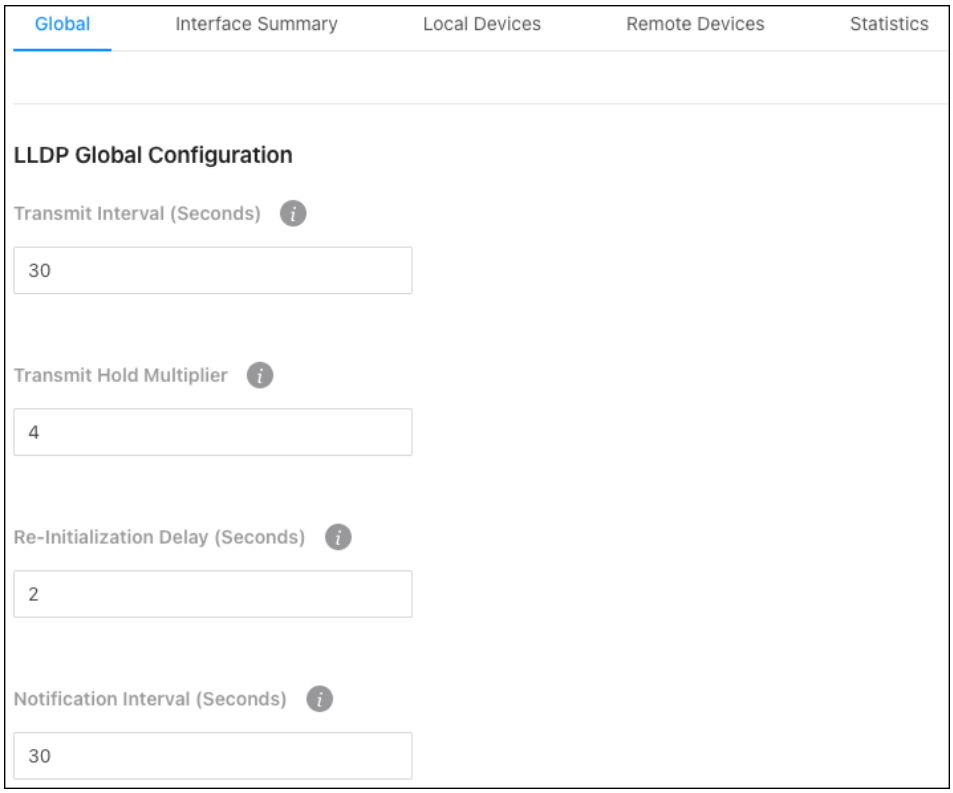


Neighbors

LLDP

Global

Use this page to configure global **Link Layer Discovery Protocol (LLDP)** settings for the switch. LLDP is a generic protocol used to advertise the device's capabilities to other devices on the network.



Configurable settings include:

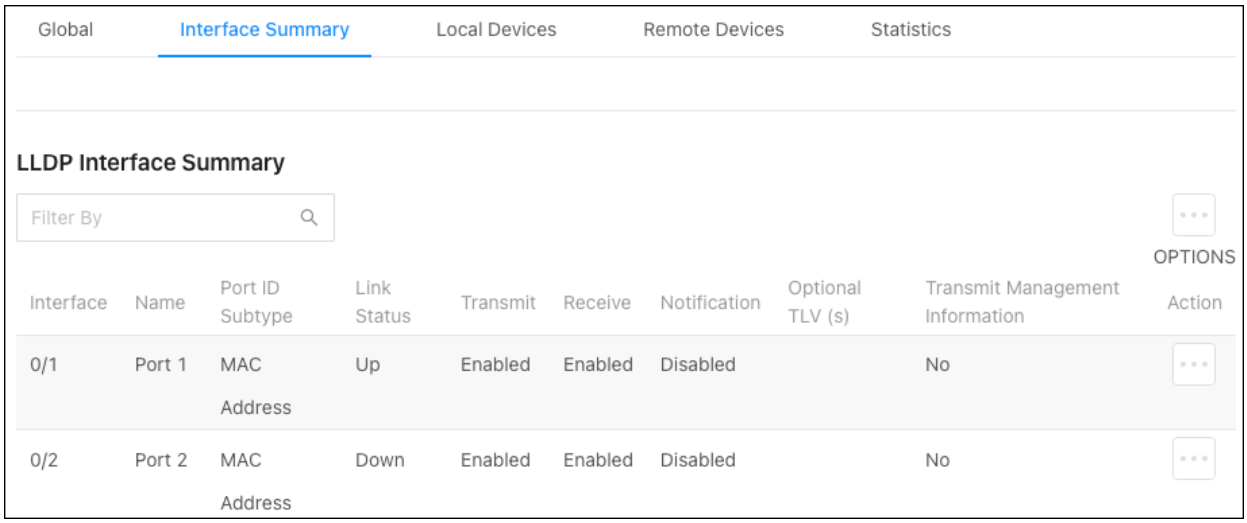
- **Transmit Interval (Seconds)** — The number of seconds between LLDP transmissions.
- **Transmit Hold Multiplier** — Multiply the value entered with the Transmit interval to determine the Time to Live (TTL) value that the switch advertises.

The TTL value is the number of network hops that a packet can take before it's discarded by the router.

- **Re-Initialization Delay (Seconds)** — The number of seconds to wait before attempting to reinitialize LLDP on a port after the port's LLDP operating mode changes.
- **Notification Interval (Seconds)** — The minimum number of seconds to wait between transmissions of SNMP trap notifications on the switch.

Interface Summary

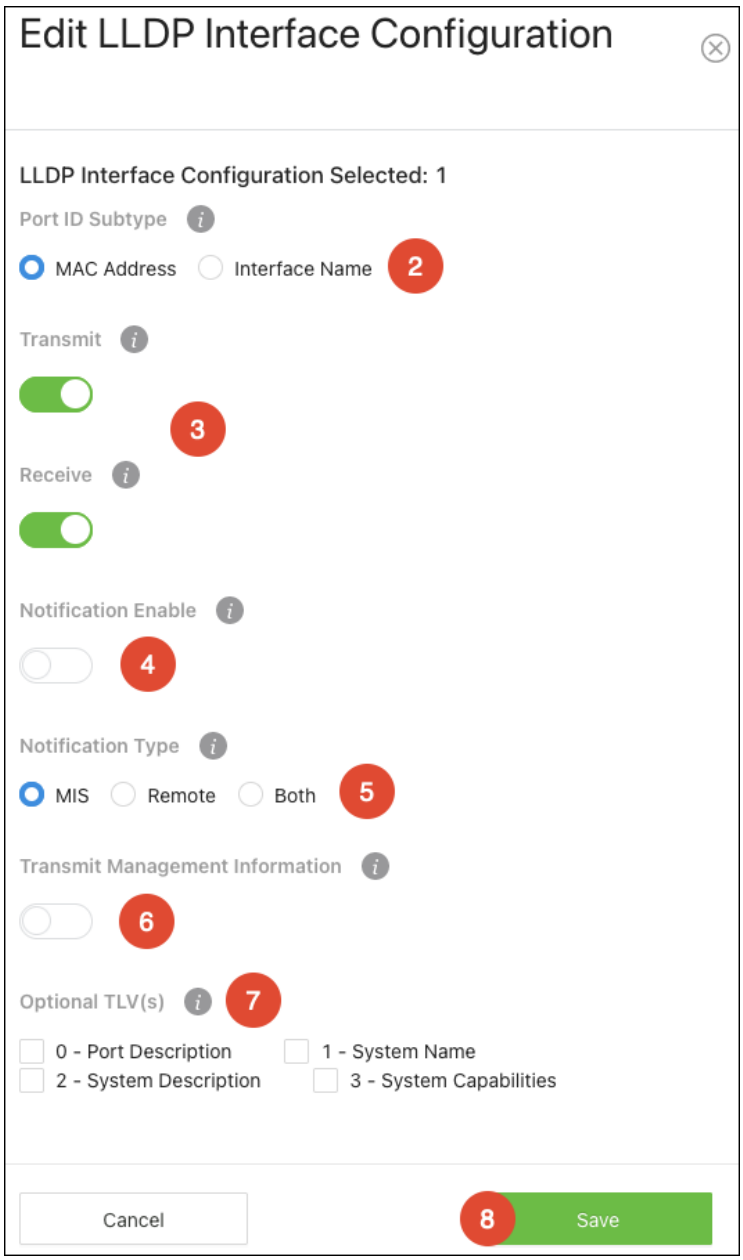
Use this page to configure LLDP settings on individual ports.



To configure LLDP on a port(s):

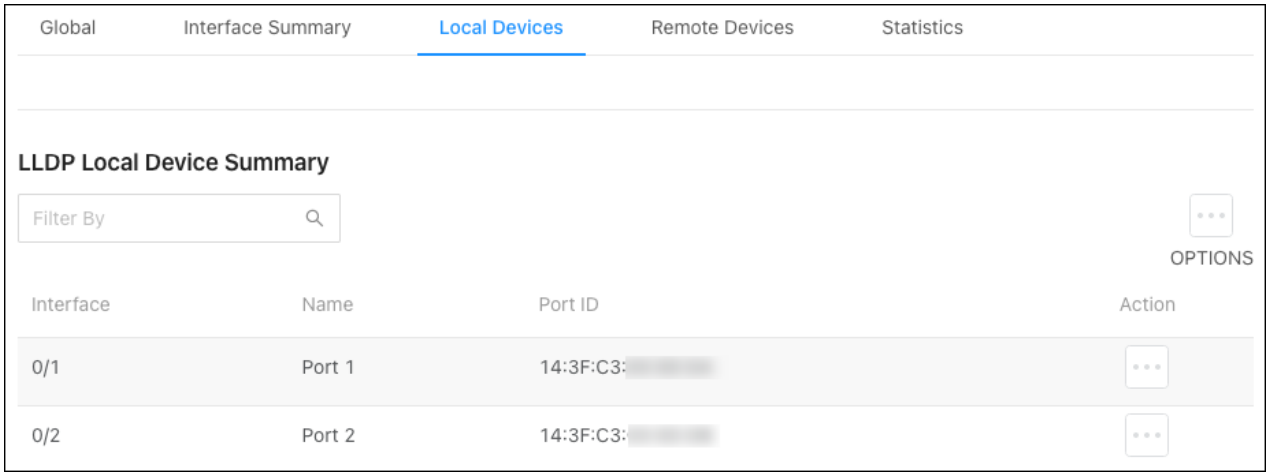
1. Click the **Options** (⋯) button to edit multiple ports, or the **Action** button to edit an individual port.
2. For **Port ID Subtype**, select if you'd like LLDP to advertise the port's **MAC address** or the **Interface Name**.
3. Enable or disable if the port can Transmit or Receive LLDP advertisements.
4. Toggle **Notification Enable** on to let the port send LDDP notifications.
5. Select a **Notification Type**. When Notification Enable is on, MIS is the only option.

6. Enable **Transmit Management Information** so other remote management devices on the network can locate the switch.
7. Select **Optional TLV(s)** for the switch to advertise.
8. Click **Save**, then **Apply** at the top of the page.

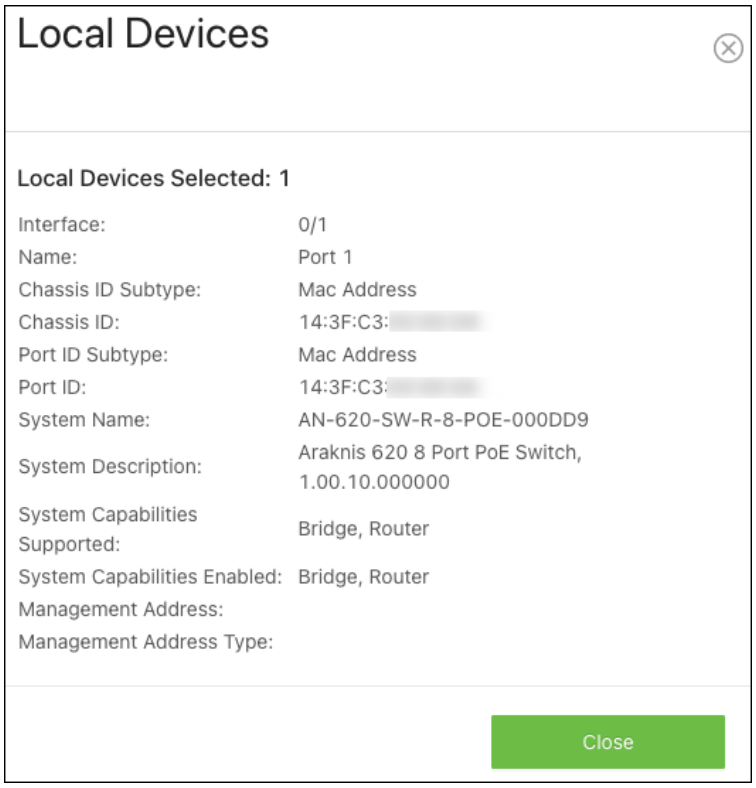


Local Devices

Use this page to gather LLDP information about the switchports.

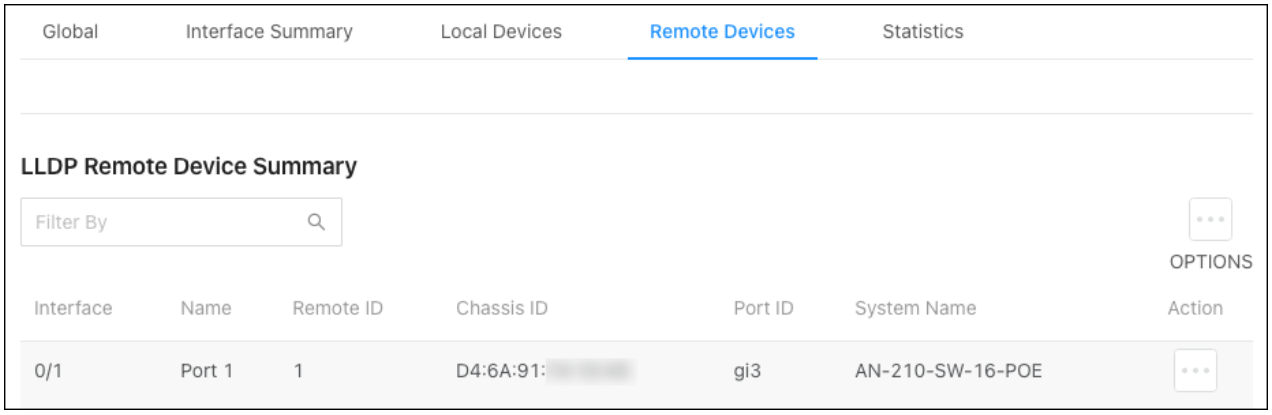


Click the **Actions** button to get more information about the port.

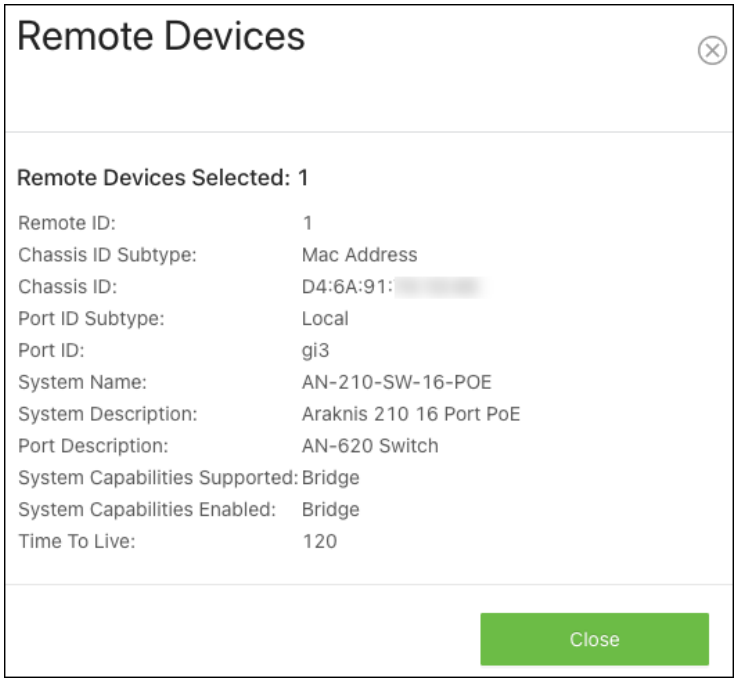


Remote Devices

Use this page to view LLDP information collected by the device connected to the switch's port.

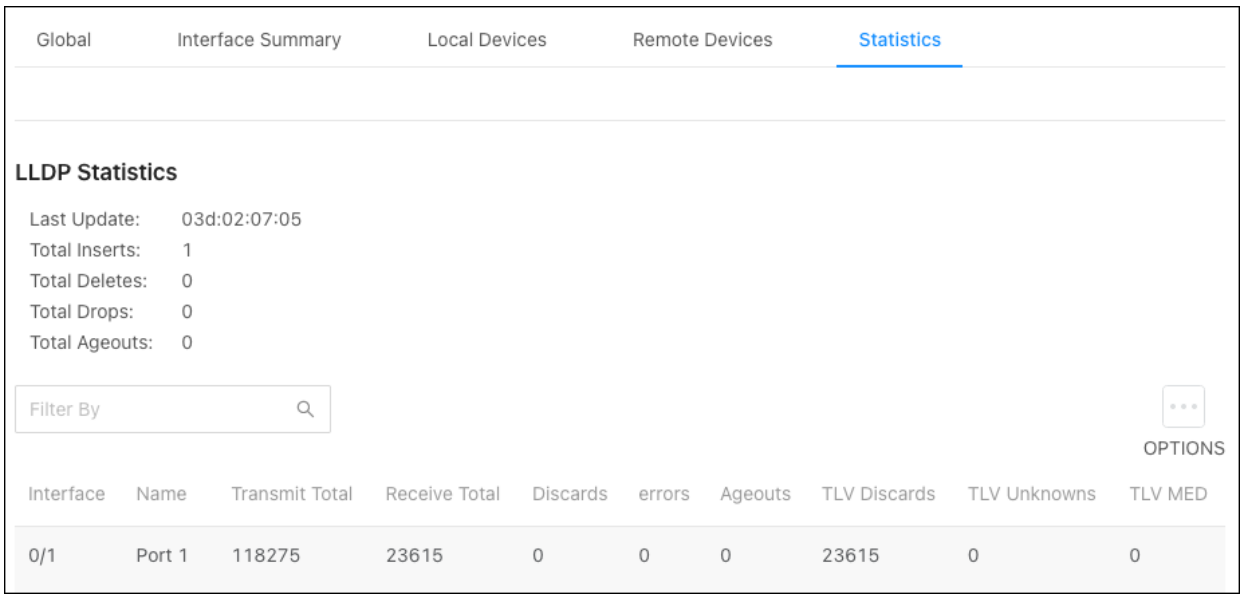


Click the **Actions** button to get more information about the connected device.



Statistics

Use this page to view LLDP counts. Click **Options** (⋯), then **Refresh** to get the most up-to-date information. Click **Clear** to reset the table.



LLDP-MED

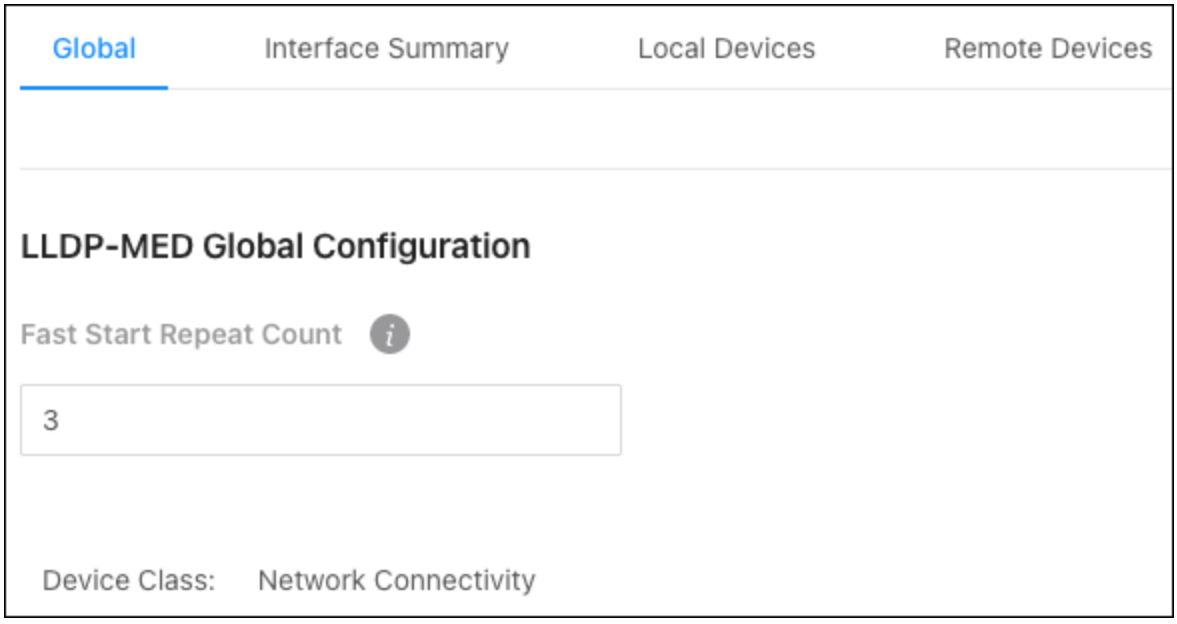
Global

LLDP-MED is an extension of LLDP. MED stands for Media Endpoint Device and is typically used for voice over IP (VoIP).

LLDP and LLDP-MED cannot operate simultaneously. If a device receives LLDP packets it cannot send LLDP-MED packets until it receives LLDP-MED packets. Likewise, for LLDP.

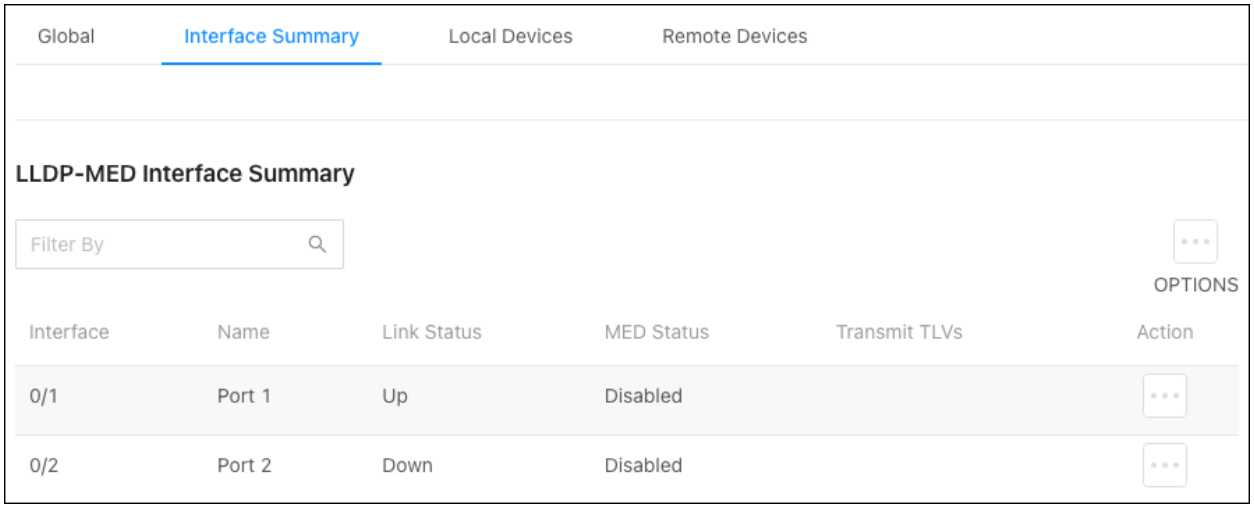
Use this page to enter a value for the **Fast Start Repeat Count**. This is the number of LLDP-MED Protocol Data Units (PDUs) that can be transmitted.

Click **Apply** to save changes.



Interface Summary

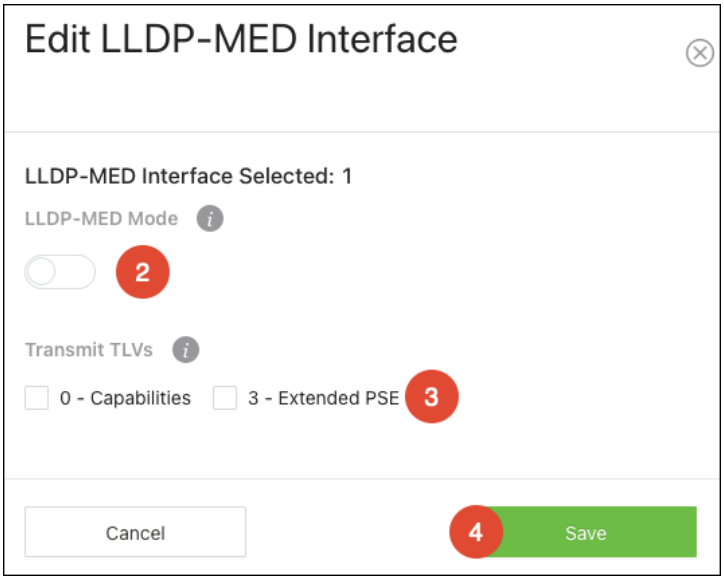
Use this page to configure LLDP-MED settings on individual ports.



To configure LLDP-MED on a port(s):

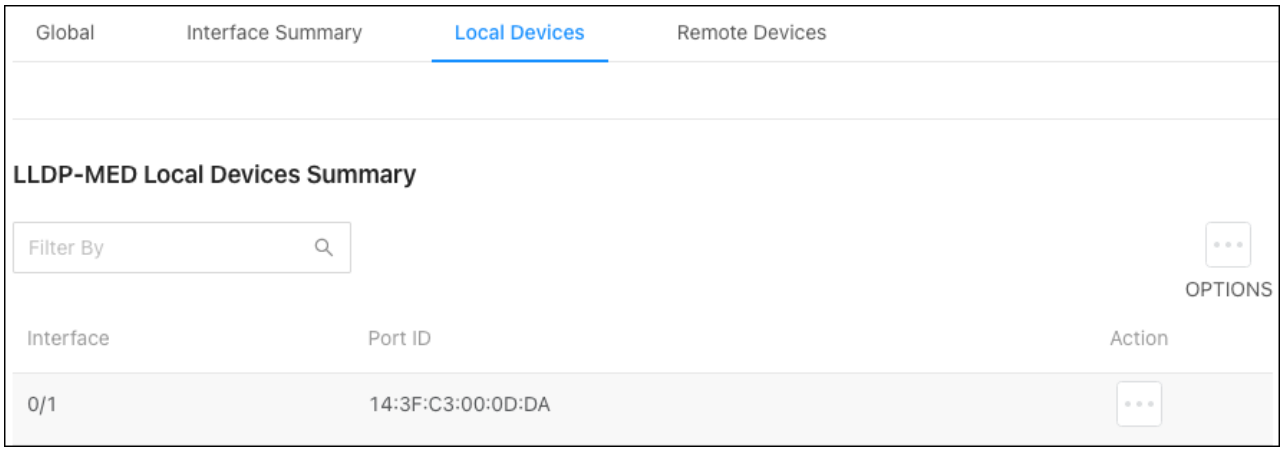
1. Click the **Options** (⋯) button to edit multiple ports, or the **Action** button to edit an individual port.
2. Enable or disable **LLDP-MED** on the port.
3. Select optional **Transmit TLVs** to advertise.

4. Click **Save**, then **Apply** at the top of the page.

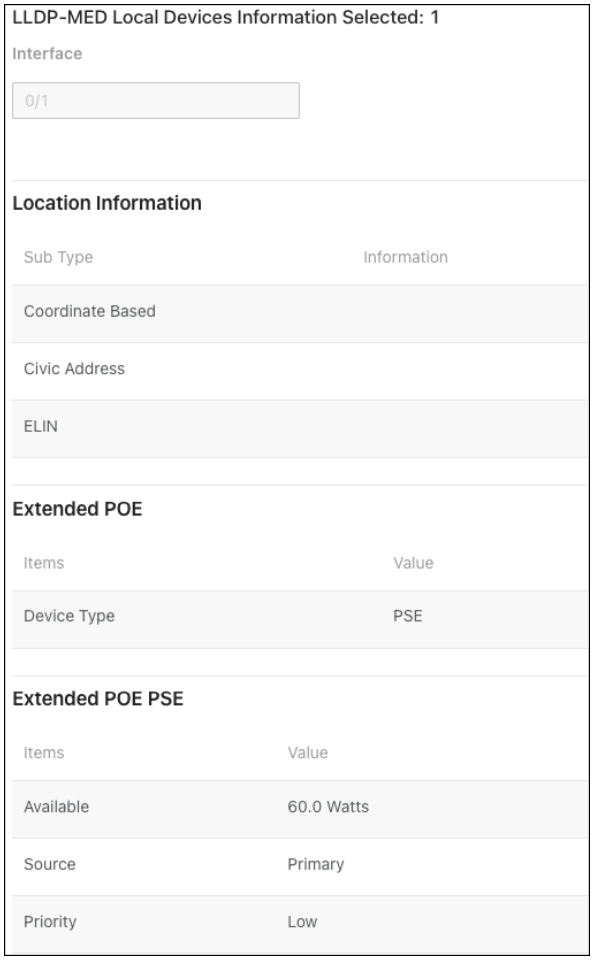


Local Devices

Use this page to gather LLDP-MED information about the switchports.

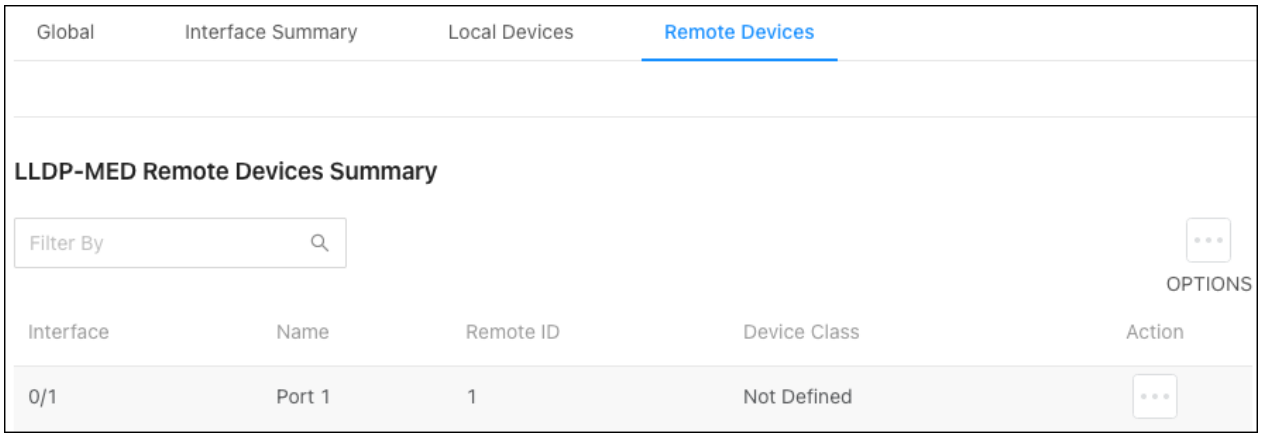


Click the **Actions** button to get more information about the port.

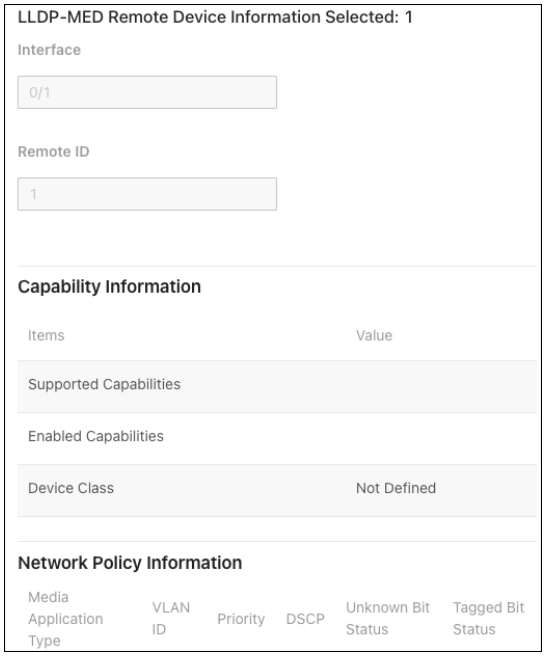


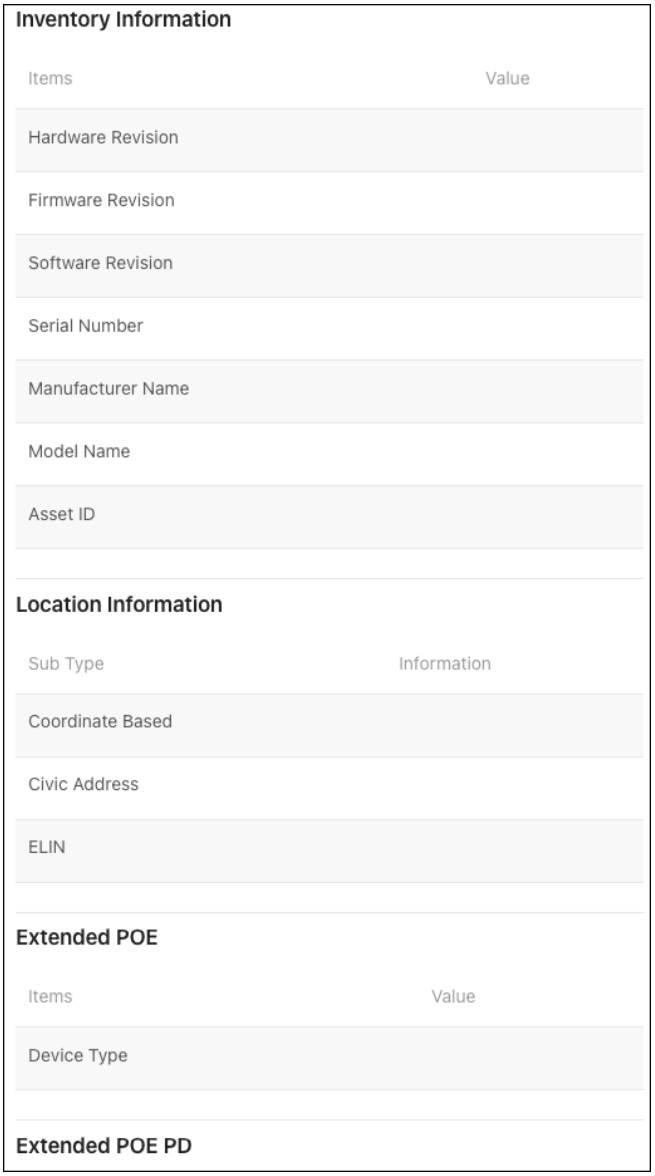
Remote Devices

Use this page to view LLDP-MED information collected by the device connected to the switch's port.



Click the **Actions** button to get more information about the port.

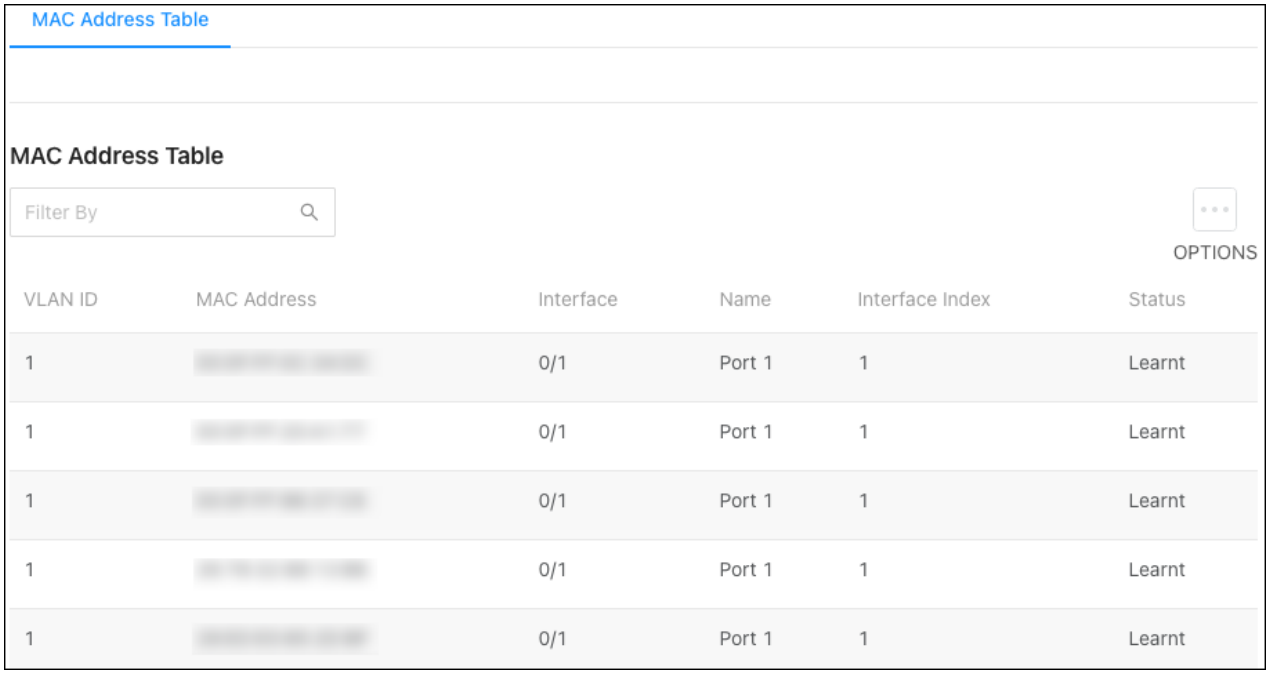




MAC Address Table

Use the page to see which MAC addresses the switch has recorded traffic from on a port(s) and which VLAN they're a member of. Use the **Options** (⋯) button to refresh the page, or to select how many rows to display.

Pro Tip: Use the Filter By field to search for MAC addresses.



ARP Table

Summary

The ARP table displays MAC and IP address of devices that have communicated with the switch.

Use the **Options** (⋯) button to refresh the page or clear the table. Use the **Action** button to delete an individual entry.

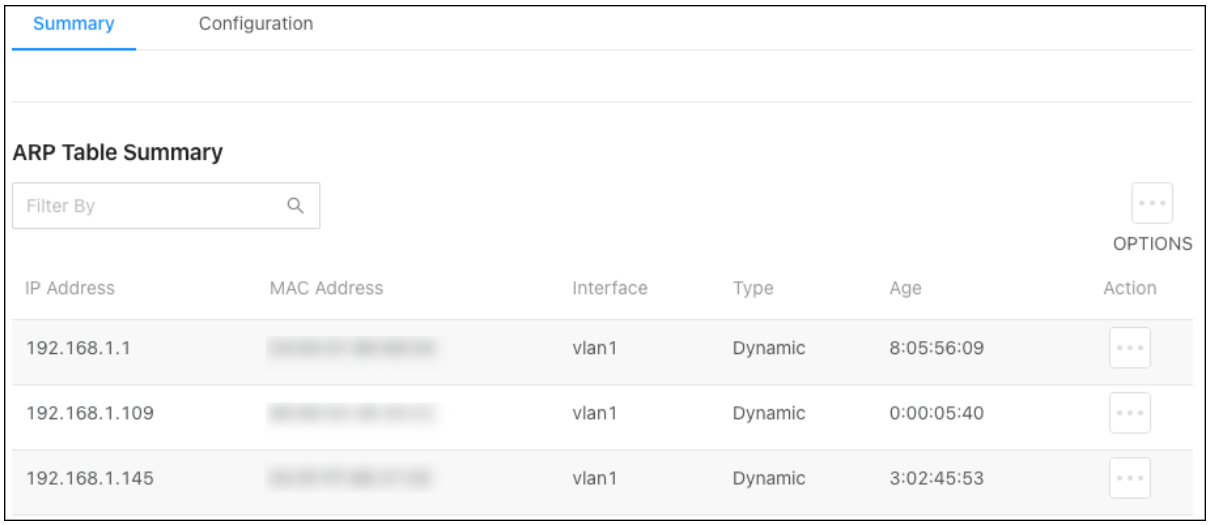
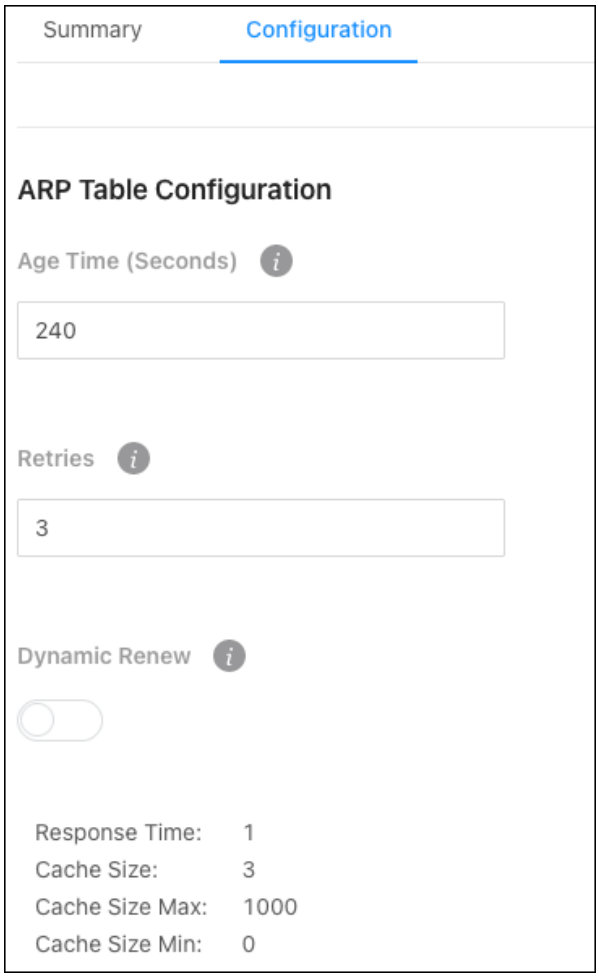


Table fields include:

- **IP Address** — The IP address of the device.
- **MAC Address** — The MAC address of the device.
- **Interface** — The VLAN ID associated with the device.
- **Type** – The type of IP address the device is broadcasting. Dynamic or static. Devices with MAC reservations appear as dynamic.
- **Age** – How long the switch has seen the connection to the device. (Days:Hours:Minutes:Seconds)

Configuration

Use this page to configure the ARP Table's settings.



Configurable settings include:

- **Age Time (Seconds)** — The amount of time that a dynamic ARP entry remains in the ARP table before aging out.
- **Retries** — The number of attempts the switch will send an ARP request if an ARP response isn't received. This number includes the initial ARP request.
- **Dynamic Renew** — Enable to allow the switch to automatically renew dynamic ARP entries when they age out.

Routing

Router

Configuration

Use this page to act configure the switch as a layer 3 device by routing packets between interfaces configured for IP routing.

Configurable options include:

- **Enable** — Enables the routing feature globally on the switch.
- **ICMP Echo Replies** — Enable to allow the device to send ICMP Echo Reply messages in response to ICMP Echo Request (ping) messages it receives.
- **ICMP Redirects** — Enable to allow the device to send ICMP Redirect messages to hosts. An ICMP Redirect message notifies a host when a better route to a particular destination is available on the network segment.
- **Forward Net Directed Broadcasts** — A network-directed broadcast is a broadcast directed to a specific subnet. Enable this feature to forward network-directed broadcasts. If disabled, network-directed broadcasts are dropped.
- **ICMP Rate Limit Interval** — Enter the maximum burst interval for ICMP error messages transmitted by the switch. The rate limit for ICMP error messages is configured as a token bucket. The ICMP Rate Limit Interval specifies how often the token bucket is initialized with tokens of the size configured in the ICMP Rate Limit Burst Size field.
- **ICMP Rate Limit Burst Size** — Enter the number of ICMP error messages that can be sent during the burst interval configured in the ICMP Rate Limit Interval field.
- **Static Route Preference** — The default distance (preference) for static routes. Lower route-distance values are preferred when determining the best route. This value is used when using the CLI to configure a static route and no preference is specified. Changing the Static Route Preference does not update the preference of

existing static routes.

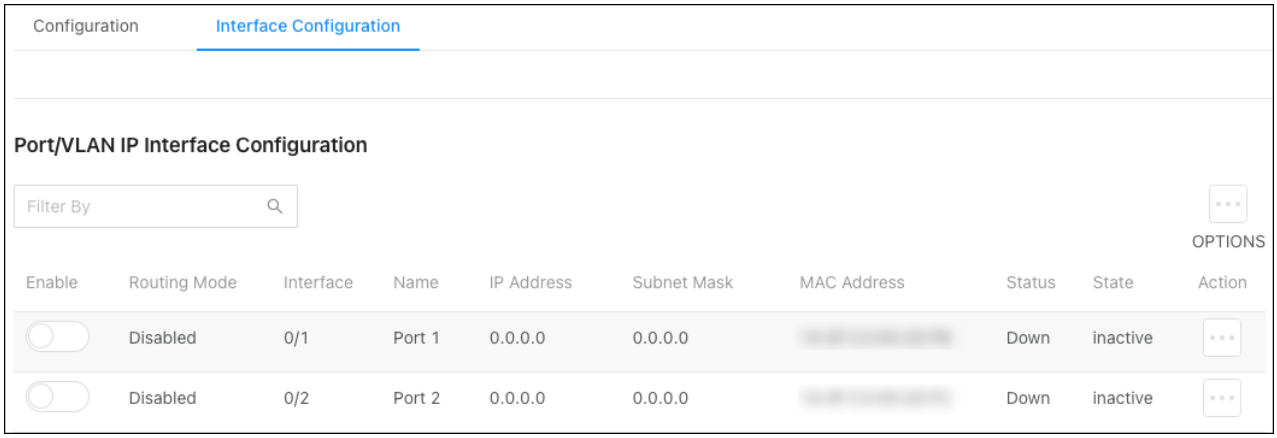
- **Global Default Gateway** — The gateway IP address that the switch uses. If the destination IP address in a packet does not match any routes in the routing table, the packet is sent to the default gateway. The gateway specified in this field is preferable to a default gateway learned from a DHCP server.

Interface Configuration

Use this page to enable and configure routing on specific interfaces. Each interface is disabled by default.

Use the **Options** (⋯) button to add a VLAN, or the **Action** button in an interface row to configure routing features.

Each row has a toggle to quickly enable or disable the interface.



Configurable options include:

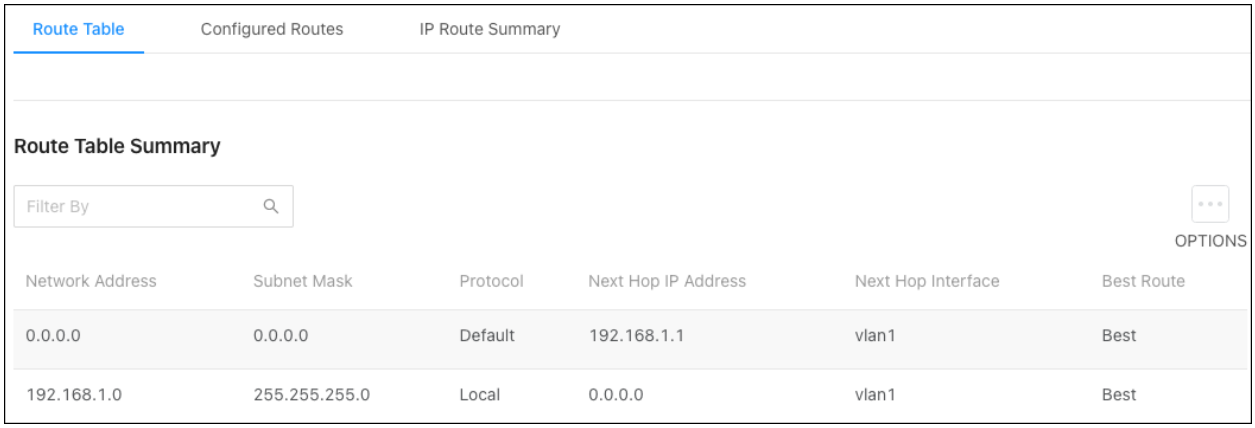
- **Type** — The type of interface being configured.
- **Interface** — The type of interface being configured. VLAN or Interface (port).
- **Routing Mode** — Enable to use the routing feature on the interface.
- **Enable** — Enables the port to forward traffic.
- **IP Address Configuration Method** — Select the method that the interfaces obtain an IP Address. Options include:

    - **None** — The interface does not receive an IP address.
    - **Manual** — Select this option to use the fields below to configure the interface's IP address and subnet mask.
    - **DHCP** —The interface automatically obtains an IP address from the DHCP server.
- **IP Address** — Only available when the interface IP Address Configuration Method is set to Manual.
- **Subnet Mask** — Only available when the interface IP Address Configuration Method is set to Manual.
- **Bandwidth** — Configure the bandwidth on the interface. This setting communicates the speed of the interface to higher-level protocols.
- **Encapsulation Type** — The link layer encapsulation type for packets transmitted from the interface. **Ethernet** is the only option.
- **Destination Unreachables** — When enabled, the interface is allowed to send ICMP Destination Unreachable message to a host if the intended destination cannot be reached. If this option is clear, the interface does not send ICMP Destination Unreachable messages.
- **ICMP Redirects** — When enabled, the interface is allowed to send ICMP Redirect messages to notify a host when a better route to a particular destination is available on the network segment. ICMP Redirects must be enabled both globally, and on the interface, to work.

IP Routing

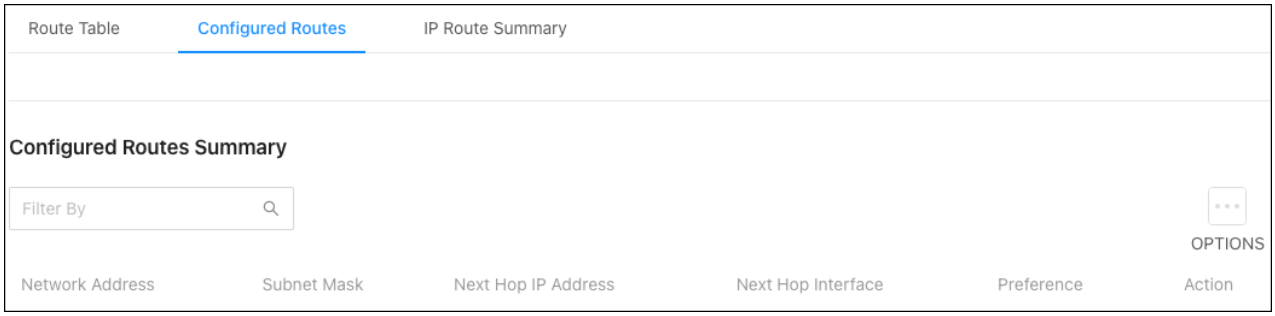
Route Table

Use this table to view routes on the switch. Use the **Options** (⋯) button to refresh the page.


Route Table
Configured Routes
IP Route Summary
Route Table Summary
Filter By
OPTIONS
Network Address
Subnet Mask
Protocol
Next Hop IP Address
Next Hop Interface
Best Route
0.0.0.0
0.0.0.0
Default
192.168.1.1
vlan1
Best
192.168.1.0
255.255.255.0
Local
0.0.0.0
vlan1
Best

Configured Routes

Use this page to view and configure routes on the switch. Click the **Options** (⋯) button to add a new route.



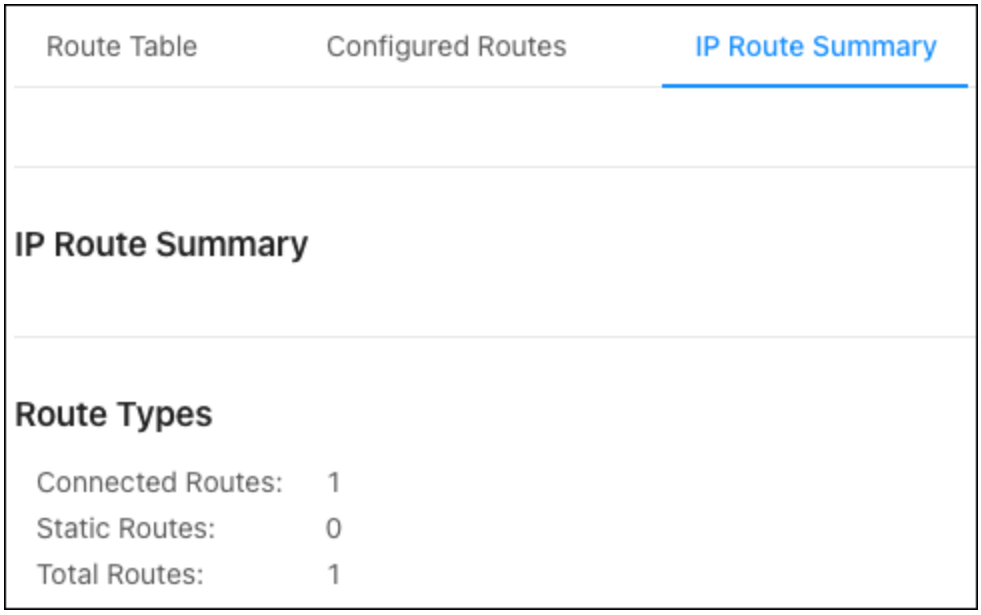
Configurable settings include:

- **Route Type** — Select one of the following routes to configure:
  - **Default** — The route the device uses to send a packet if the routing table does not contain a longer matching prefix for the packet's destination. The routing table can contain only one default route.
  - **Static** — A manually added route.
  - **Static Reject** — A route where packets that match the route are discarded instead of forwarded. The device might send an ICMP Destination Unreachable message.
- **Network Address** — Enter the IP route prefix for the destination network. This IP address must contain only the network portion of the address and not the host bits. When adding a default route, this field must be 0.0.0.0.
- **Subnet Mask** — Enter the IP subnet mask (also known as the network mask or netmask) associated with the network address. The subnet mask defines which portion of an IP address belongs to the network prefix, and which portion belongs to the host identifier. When adding a default route, this field must be 0.0.0.0.

- **Next Hop IP Address** — Enter the outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination. The next router is always an adjacent neighbor or the IP address of the local interface for a directly attached network. When adding a static reject route, this field must be 0.0.0.0 because the packets are dropped rather than forwarded.
- **Preference** — Enter a preference value for the route. A lower preference value is a more preferred route. When the routing table has more than one route to the same network, the device selects the route with the lowest route preference.

IP Route Summary

This page displays a summary of the IP routes and route table counters the switch has collected.



QoS

ACL Rules

Summary

Use this page to configure **Access Command List (ACL)** Rules. Access Control Lists (ACLS) make sure that only authorized users have access to specific resources and block unwanted attempts by filtering packets based on rules. ACLs are used to control traffic flow, restrict the contents of routing updates, decide which types of traffic to block or forward, and provide network security.

To add an ACL rule:

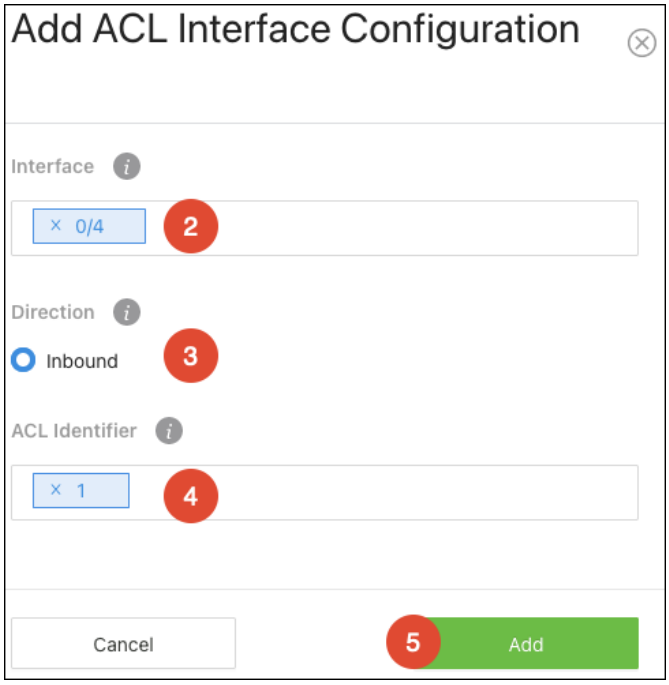
1. Click **Options** (⋯), then **Add**.
2. Select an **ACL Type**:
   - **IPv4 Standard** - Match criteria is based on the source address of IPv4 packets.
   - **IPv4 Extended** - Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of IPv4 packets. The ACL identifier can be an alphanumeric name instead of a number, known as IPv4 Named in other switches.
3. Enter a number for the **ACL ID**.
4. Click **Add**, then **Apply** at the top of the page.

Interfaces

Use this page to add an ACL rule to a port(s).

To add an ACL rule to a port:

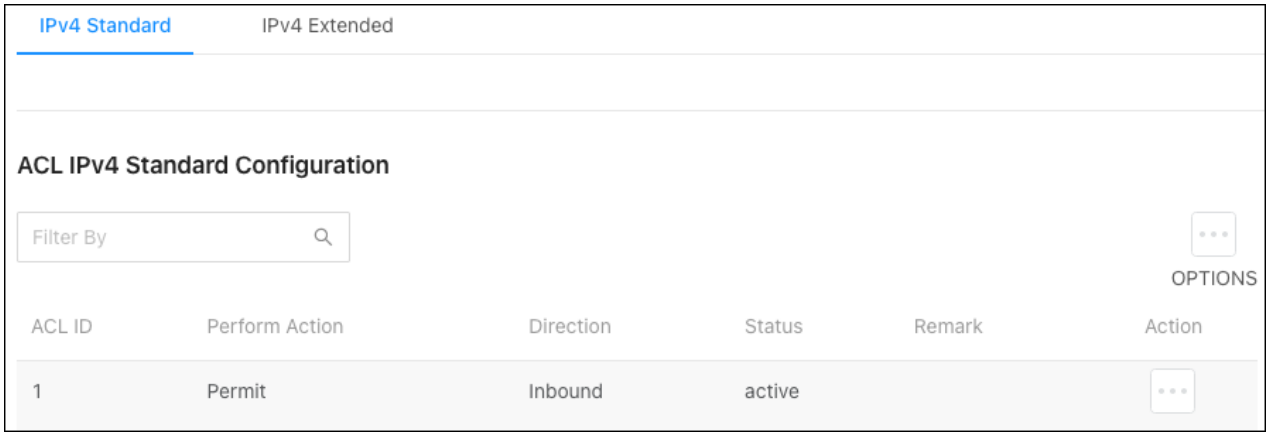
1. Click **Options** (⋯), then **Add**.
2. Select the **Interface** (port) to apply the ACL rule to.
3. Select **Inbound** as the **Direction**, if the packets should be checked against the ACL rules when the port(s) receives it. Do not select Inbound if the packets should be checked when the packets are exiting the port(s).
4. Select the **ACL Identifier** of the ACL rule to apply to the port(s).
5. Click **Add**, then **Apply** at the top of the page.



ACL Configuration

IPv4 Standard

Use this page to configure IPv4 Standard ACLs. Click the **Options** (⋯) button to edit multiple ACLs or the **Actions** button to edit a single ACL.



Configurable settings include:

- **Perform Action** — The action to take when a packet or frame matches the criteria in the rule:
  - **Permit** — The packet or frame is forwarded.
  - **Deny** — The packet or frame is dropped.
  - Redirect — Redirect to interface.
  - **Copy-to-cpu** - Configures the copying of protocol control packets to control plane CPU.
  - **Drop Copy-to-cpu** - Copies TCP protocol control packets to control plane CPU without switching packets.
- **Redirect** — The port(s) the ACL redirects to.
- **Source IP Address** — The source port IP address in the packet and source IP mask (in the second field) to compare to the IP address in a packet header or string 'ANY' (default).
- **Source IP Mask** — An IP Mask for the source or string 'ANY' (default).
- **Destination IP Address** — The destination port IP address in the packet and destination IP mask (in the second field) to compare to the IP address in a packet header or string 'ANY' (default).
- **Destination IP Mask** — An IP Mask for the destination or string 'ANY' (default).

- **Remark** — Use remarks as a keyword to make ACLs easier to understand in network scans. Accepts alpha-numeric and special characters (-, _, and space). The remark can be up to 100 characters and is case-sensitive.

IPv4 Extended

Use this page to configure IPv4 Extended ACLs. Click the **Options** (⋯) button to edit multiple ACLs or the **Actions** button to edit a single ACL.

Configurable settings include:

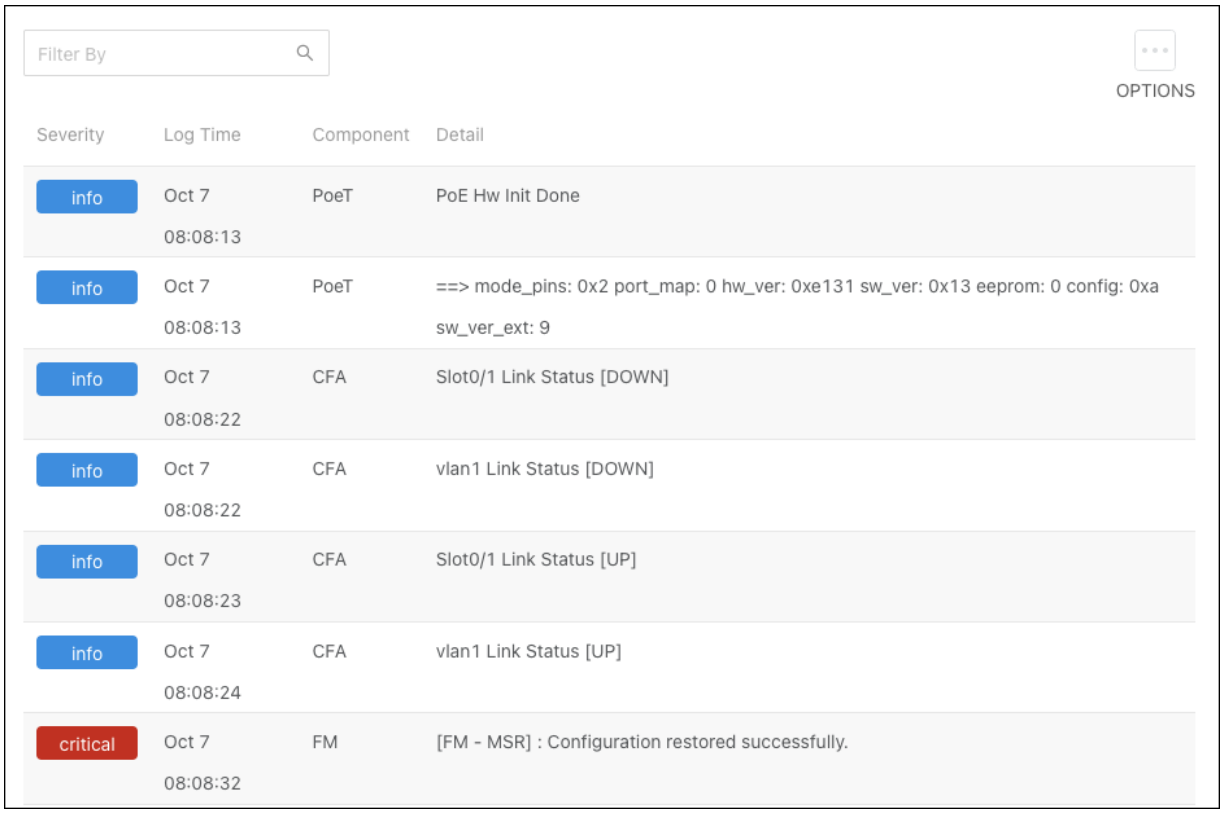
- **Perform Action** — The action to take when a packet or frame matches the criteria in the rule:
  - **Permit** — The packet or frame is forwarded.
  - **Deny** — The packet or frame is dropped.
  - **Redirect** — Redirect to interface.
  - **Copy-to-cpu** - Configures the copying of protocol control packets to control plane CPU.
  - **Drop Copy-to-cpu** - Copies TCP protocol control packets to control plane CPU without switching packets.
- **Redirect** — The port(s) the ACL redirects to.

- **Source IP Address** — The source port IP address in the packet and source IP mask (in the second field) to compare to the IP address in a packet header or string 'ANY' (default).
- **Source IP Mask** — An IP Mask for the source or string 'ANY' (default).
- **Destination IP Address** — The destination port IP address in the packet and destination IP mask (in the second field) to compare to the IP address in a packet header or string 'ANY' (default).
- **Protocol** — The IANA-assigned protocol to match within the IP packet.
- **IGMP Type** — The IP ACL rule to match on the specified IGMP type. This option is available only if the protocol is IGMP.
- **ICMP Type** — The IP ACL rule to match on the specified ICMP type. This option is available only if the protocol is ICMP.
- **ICMP Code** — The IP ACL rule to match on the specified ICMP code. This option is available only if the protocol is ICMP.
- **TCP Flags** — The IP ACL rule to match on the TCP flags. This option is available only if the protocol is TCP.
- **IP TOS** — Matches on the Type of Service (TOS) in the IP header.

System Log

Use the system log page to view and download events recorded by the switch. Click the **Options** (⋯) button to refresh the page, choose how many rows to display, or download the logs.

Pro Tip: Use the Filter by field to quickly find the event types you're looking for. Examples are critical, poe, or vlan.



Technical Support

For chat and telephone, visit **snp1.co/techsupport** • Email: **TechSupport@SnapOne.com**. Visit **snp1.co/tc** for discussions, instructional videos, news, and more.

Warranty and Legal Notices

Find details of the product's Limited Warranty and other resources such as regulatory notices and patent and safety information, at **snapone.com/legal** or request a paper copy from Customer Service at **866.424.4489**.

Copyright© 2023, Snap One, LLC. All rights reserved. Snap One and its respective logos are registered trademarks or trademarks of Snap One, LLC (formerly known as Wirepath Home Systems, LLC), in the United States and/or other countries. 4Store, 4Sight, Control4, Control4 My Home, SnapAV, Araknis Networks, BakPak, Binary, Dragonfly, Episode, Luma, Mockupancy, Nearus, NEEO, Optiview, OvrC, Pakedge, Sense, Strong, Strong Evolve, Strong VersaBox, SunBriteDS, SunBriteTV, Triad, Truvision, Visualint, WattBox, Wirepath, and Wirepath ONE are also registered trademarks or trademarks of Snap One, LLC. Other names and brands may be claimed as the property of their respective owners. Snap One makes no claim that the information contained herein covers all installation scenarios and contingencies, or product use risks. Information within this specification subject to change without notice.

230712

AN-620-SW-A