Table of Contents

Araknis 220/320/420 Series Managed Switch

Installation and Software Guide

Thank you for choosing an Araknis® x20 Series Network Switch. With updated modern aesthetics, and a managed interface, the Araknis 220/320/420 series switch is a sleek and highly capable addition to any network.

Series overview

Model	Port Facing	Total RJ45	1G, PoE+ (30W)	2.5G, PoE+ (30W)	1G, No PoE	SFP Ports	PoE Budget
AN-420-SW-R-44-POE	Rear	44	28	16		4x 10G	740
AN-420-SW-F-	Front	48	32	16		4x 10G	740

48-POE							
AN-420-SW-R-24-POE	Rear	24	16	8		4x 10G	410
AN-420-SW-F-24-POE	Front	24	16	8		4x 10G	410
AN-420-SW-R-16-POE	Rear	16	12	4		2x 10G	250
AN-420-SW-F-16-POE	Front	16	12	4		2x 10G	250
AN-320-SW-R-24-POE	Rear	24	24			2x 1G	375
AN-320-SW-F-24-POE	Front	24	24			2x 1G	375
AN-320-SW-R-16-POE	Rear	16	16			2x 1G	250
AN-320-SW-F-16-POE	Front	16	16			2x 1G	250
AN-320-SW-R-8-POE	Rear	8	8			2x 1G	130
AN-320-SW-F-8-POE	Front	8	8			2x 1G	130
AN-320-SW-F-48	Front	48			48	4x 1G	x
AN-320-SW-R-24	Rear	24			24	2x 1G	x
AN-320-SW-F-24	Front	24			24	2x 1G	x
AN-320-SW-R-16	Rear	16			16	2x 1G	x
AN-320-SW-F-16	Front	16			16	2x 1G	x
AN-320-SW-R-8	Rear	8			8	2x 1G	x
AN-320-SW-F-8	Front	8			8	2x 1G	x
AN-220-SW-R-44-POE	Rear	44	44			4x 1G	380
AN-220-SW-F-48-POE	Front	48	48			4x 1G	380
AN-220-SW-R-24-POE	Rear	24	24			2x 1G	190
AN-220-SW-F-24-POE	Front	24	24			2x 1G	190
AN-220-SW-R-16-POE	Rear	16	16			2x 1G	130
AN-220-SW-F-16-POE	Front	16	16			2x 1G	130
AN-220-SW-R-8-POE	Rear	8	8			2x 1G	65
AN-220-SW-F-8-	Front	8	8			2x 1G	6

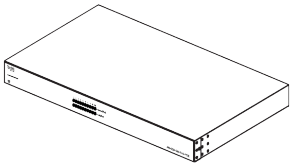
POE							

Note: All PoE models support both PoE (802.11af) and PoE+ (802.11at) standards.

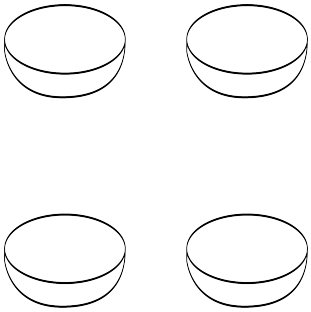
Note: For 420 models, lower port numbers are 1G and upper ports are 2.5G. The ports are marked.

Unboxing

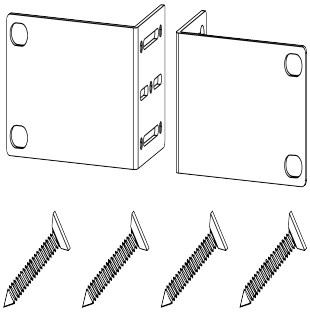
The package contains:



Switch



Rubber feet for flat surfaces (4)

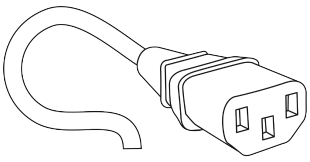


Rack-mount kit: ears (2), screws (8)

Quick Start Guide

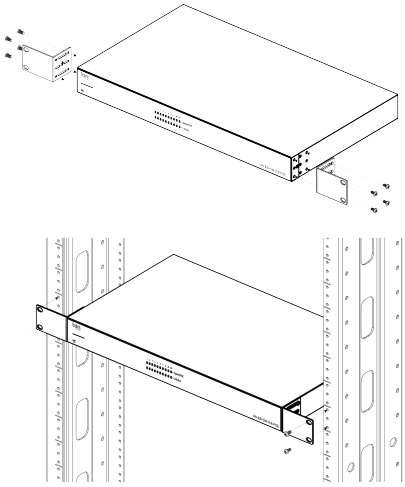
QR card

Installation

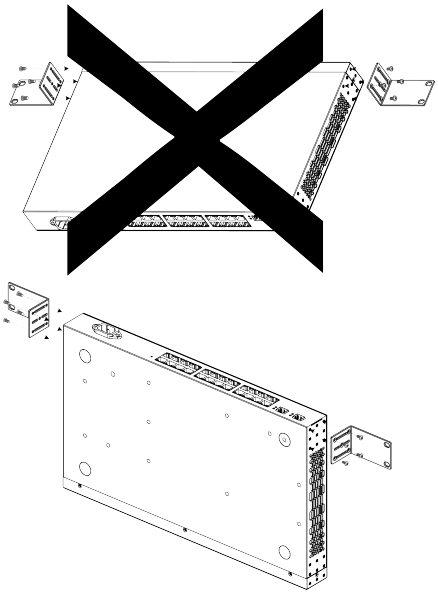


AC power cord

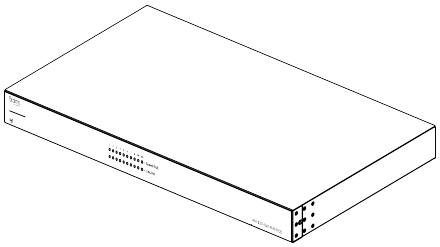
Rack mount



Wall mount



Shelf mount



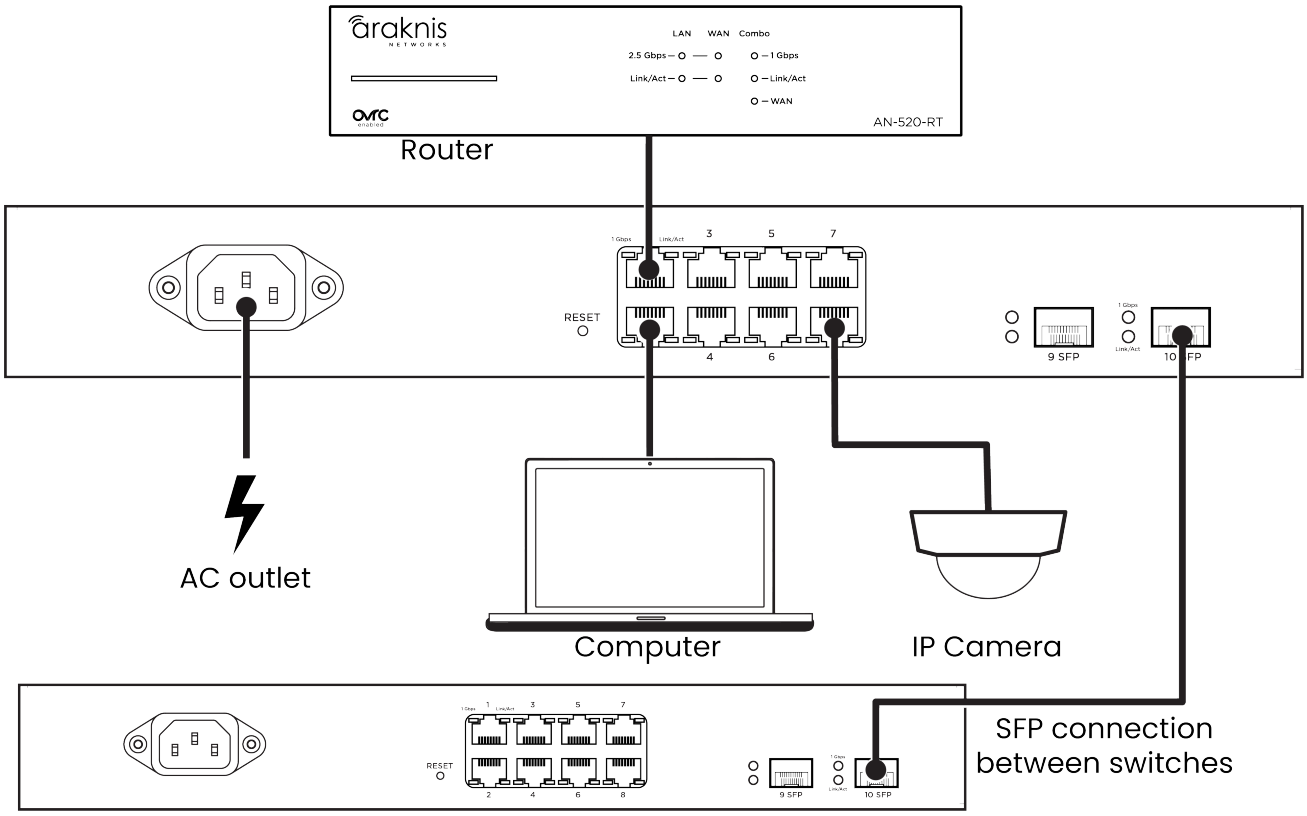
Caution: To avoid possible interference or damage, do not stack equipment on top of the switch.

If wall mounting, the Ethernet ports must face the floor or ceiling. Wall mounting is not recommended for the AN-320-SW-F/R-POE and AN-320-SW-F-48.

Rack mounting guidelines

- The maximum ambient temperature of the space the switch is installed in should not exceed 122 °F/50 °C.
- Allow to air flow through the rack.
- Verify all the leveling feet or casters are adjusted correctly and they come in contact with the supporting surface. Always load heavier equipment at the bottom of the rack.
- Make sure the rack is grounded and the equipment is surge protected.
- Do not overload the power equipment, or the switch. Check out our **WattBox Best Practices** for more information.

Connections

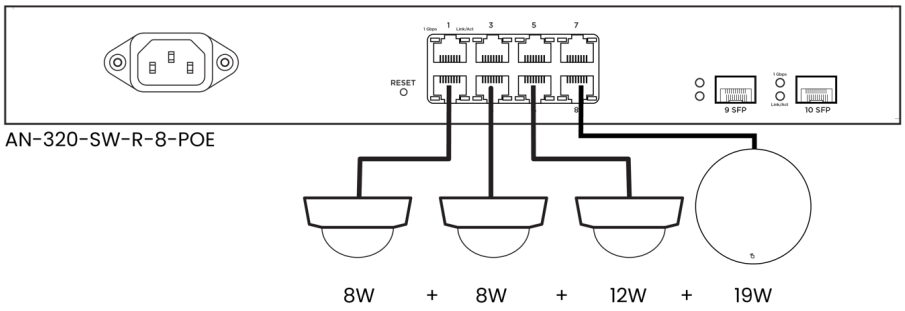


Note: Connect SFP ports using Araknis SFP adapters for RJ45 or multi-mode fiber cables. SFP adapters sold separately.

Pro Tip: Manually set the SFP port speed to 1G when connecting to a device that only supports 1G to avoid potential negotiation issues.

PoE budgeting

The PoE budget (Power over Ethernet) limits the amount of power available to all ports, with a maximum of 30W on an individual port. Add the total number of possible watts that the connected devices can consume to make sure everything can receive power reliably. Below is an example that uses an AN-320-SW-R-8-POE.



Total PoE budget available = 130W

Total PoE device consumption = 42W

PoE budget left available = 88W

LED states and reset procedures

LED	LED state	Description
Power	On	Switch is powered on
	Off	Switch is powered of

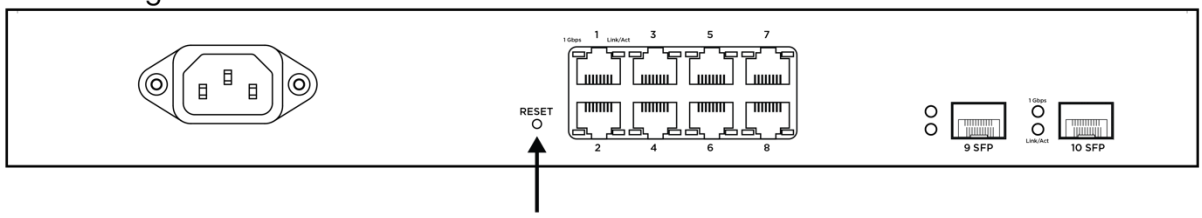
1Gbps	On	Port is connected at 1000Mbps
	Off	Port is connected at 10/100Mbps
Link/Act	On	Port detects a connection
	Blinking	Packets are flowing through the port
	Off	Port does not detect a connection

Reset procedures

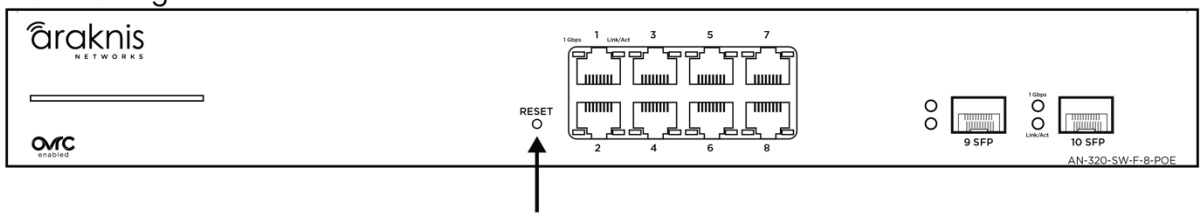
To **restart** the switch, press and hold the Reset button for 5 seconds, then release.

To **factory default** the switch, press and hold the Reset button for 10-15 seconds until the LEDs flash once.

Rear-facing



Front-facing

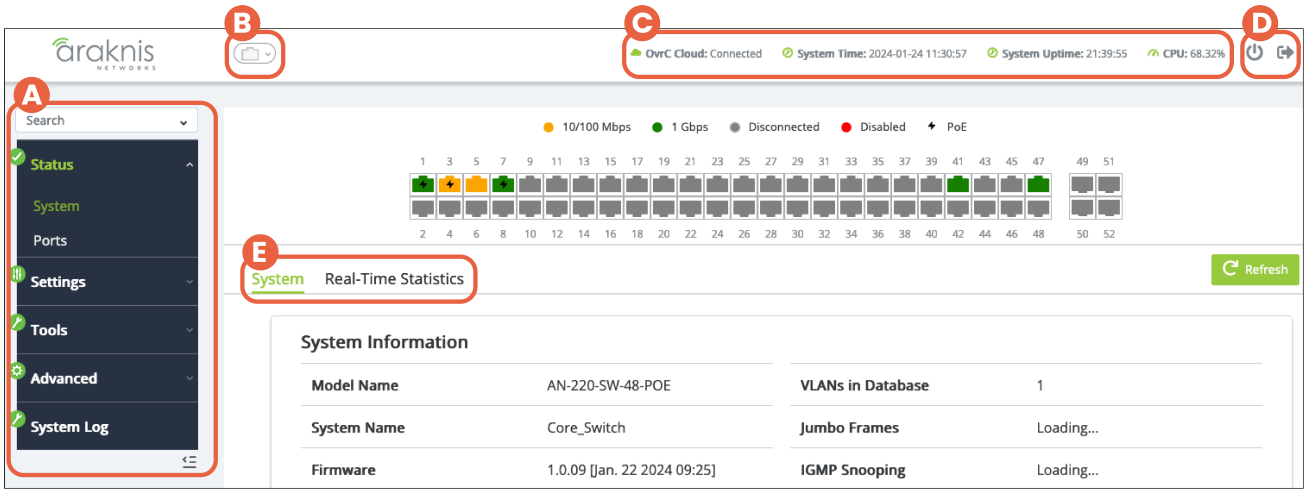


Interface overview

Araknis 220 and 320 switches use the main navigation menu and page tabs to organize the system information and configurable settings.

Definitions

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

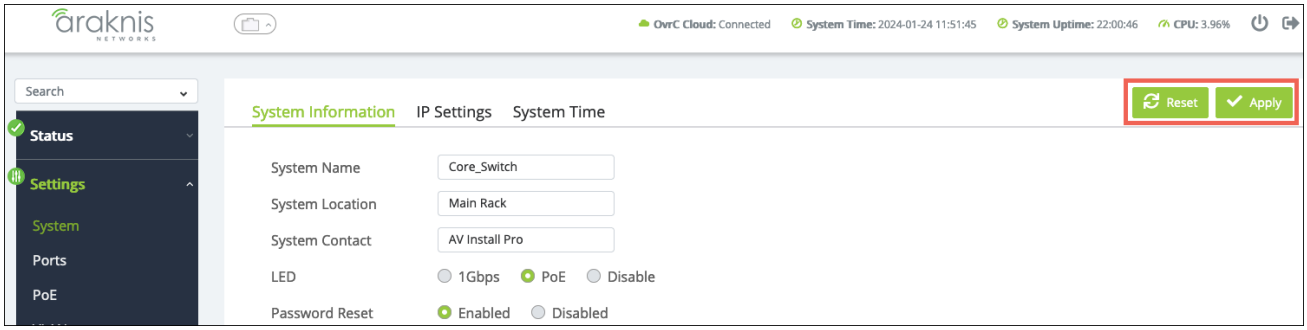


1. **Main Navigation Menu** — Click on the headers to access the submenus to configure and maintain the switch. There's a button at the lower right to collapse the menu.

> **Pro Tip:** Use the Search bar to find settings and jump to their pages.

2. **Port Status** — Click to toggle the port status display at the top of the page.
3. **Top Bar** — Displays the overall status of the switch, including the system uptime, the current time, OvrC cloud connection, memory, and system usage.
4. **Restart and Logout** — Use these buttons to restart or log out of the switch.
5. **Navigation Tabs** — Click on a tab to access more settings under the submenu.

Applying and resetting changes



The **Apply** changes button is in the upper right corner of the page. Use the **Reset** button if you'd like to revert the changes to their last saved state.

System

This page provides an overview of the switch's configuration. Click the **Refresh** button for the latest information.

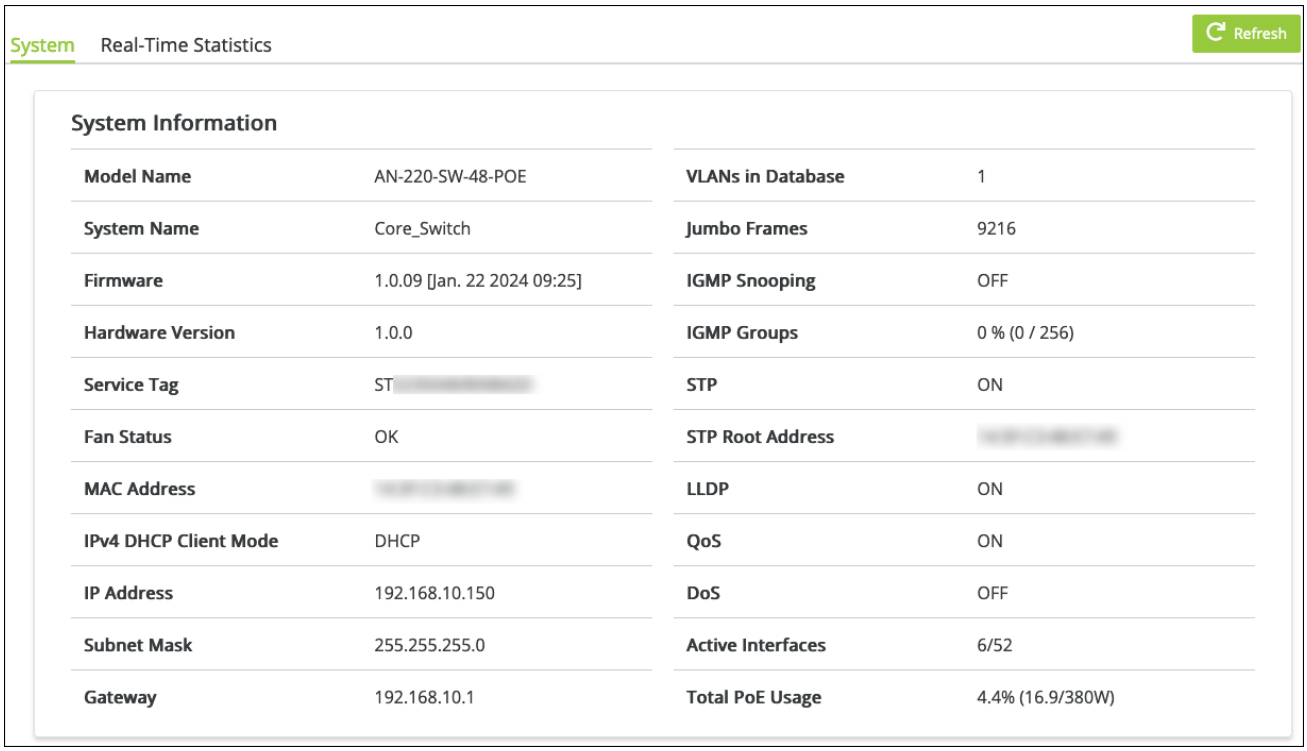


Table field descriptions:

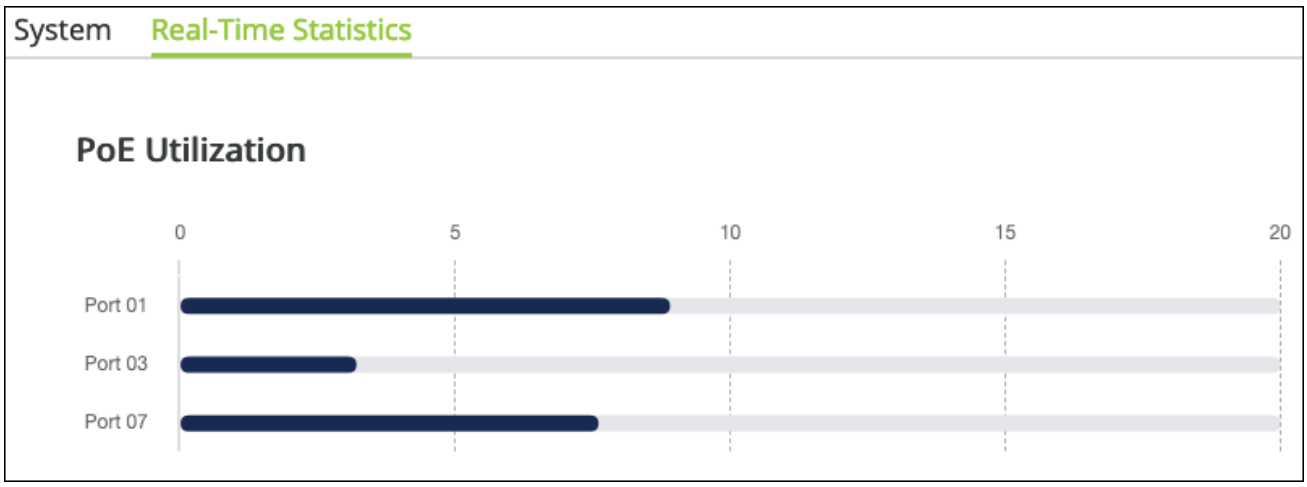
- **Model Name** — Use this field to verify the switch's model number. Notated as AN (Araknis) – SW (switch) – R/F (rear or front-facing ports) - X (the number of RJ-45 ports the switch has) - POE (Power-over-Ethernet).
- **System Name** — This is the name the switch appears under when identified on the network. This field can be changed under **Settings** > **System**.
- **Firmware**— Displays the firmware version installed on the switch. Use OvrC to verify if the switch is up to date and update it if it isn't.
- **Hardware Version** — Displays the hardware version.
- **Service Tag** — A unique identifying number that is used to add the switch to OvrC, manually.
- **Fan Status** — Displays the operating status of the fans.
- **MAC Address** — A unique identifier that appears in network scans. This address is required if the switch is being manually added to OvrC.
- **IPv4 DHCP Client Mode** — Shows if the switch is configured for a DHCP or static IP address. Configurable under **Settings** > **System** > **IP Settings**.
- **IP Address** — Displays the IP address of the switch.
- **Subnet Mask** — Shows the subnet mask assigned to the switch.
- **Gateway** — Displays the IP address of the router.
- **VLANs in Database** — The number of VLANs configured on the switch under Settings > VLANs.
- **Jumbo Frames** — The currently configured payload limit for jumbo frames. Configurable under **Ports** > **Jumbo Frames**.
- **IGMP Snooping** — Shows if IGMP Snooping is enabled on the switch. Configurable under **Settings** > **Multicast**.

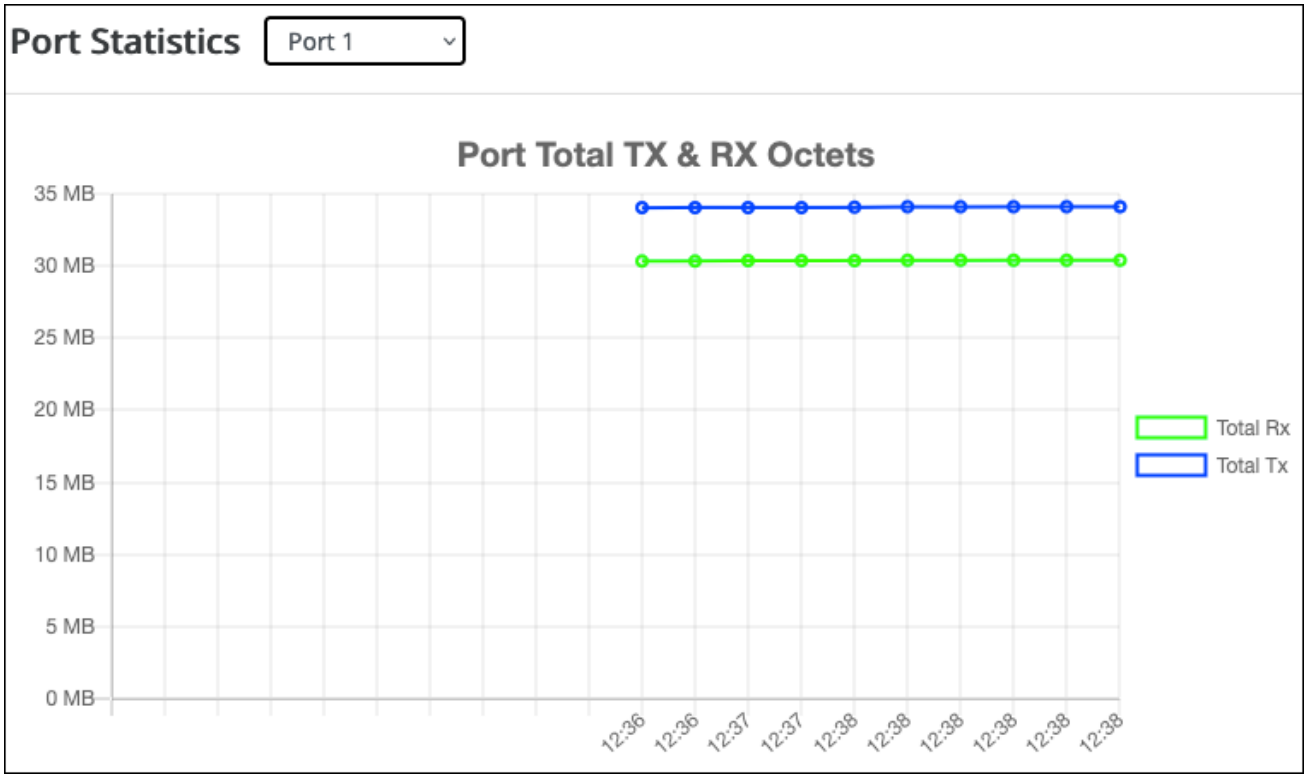
- **IGMP Groups** — Displays the amount of Multicast Groups registered on the switch. See Settings > **Multicast** > **IGMP Snooping** > **Group List** for more info.
- **STP** — Displays if Spanning Tree Protocol is enabled on the switch. Configurable under **Settings** > **STP**.
- **STP Root Address** — Displays the address of the interface acting as the STP Root Address on the network.
- **LLDP** — Displays if LLDP (link layer discovery protocol) is enabled on the switch. Configurable under **Advanced** > **Neighbors** > **LLDP**.
- **QoS** — Displays whether QoS (Quality of Service) is enabled on the switch. Configurable under **Advanced** > **QoS**.
- **DoS** — Displays if DoS (Denial of Service) prevention is enabled on the switch. Configurable under **Advanced** > **DoS**.
- **Active Interfaces** — Displays the number of switch ports currently in use and the total possible interfaces for the switch.
- **Total PoE Usage** — The amount of Power-over-Ethernet currently in use on the switch and the percentage of the total budget in use.

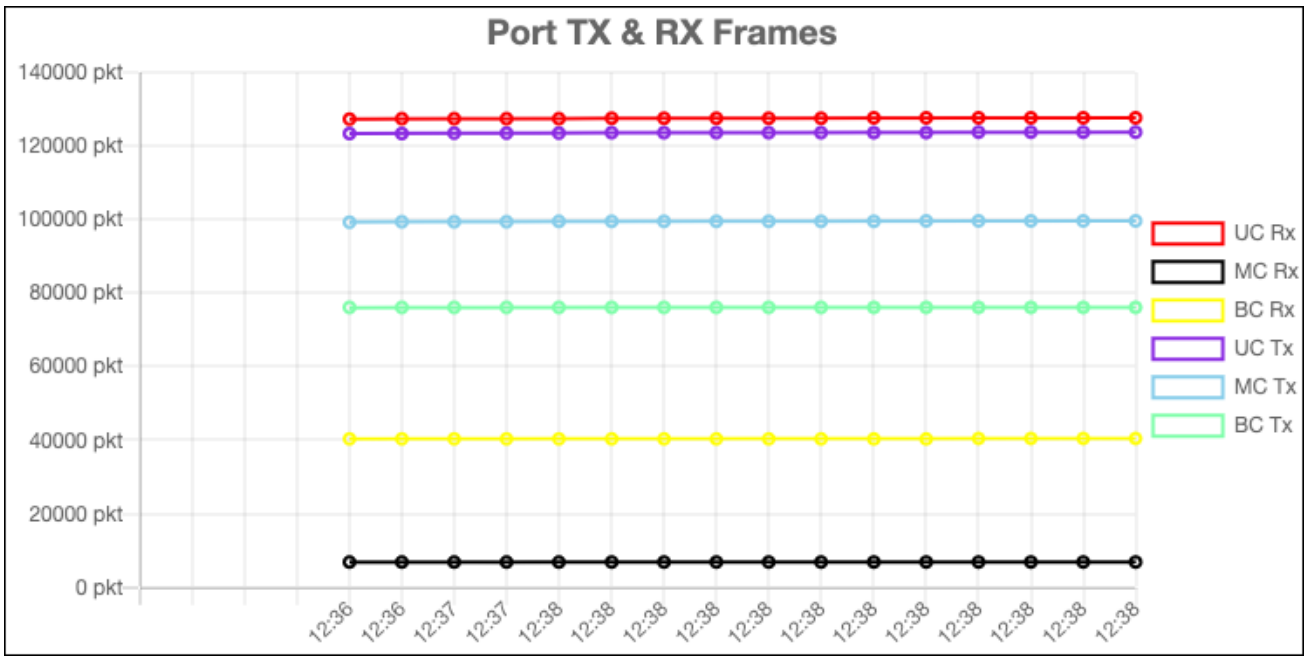
Pro Tip: Do not use more than 80% of the total budget. When calculating the budget, use the total possible amount of power the connected devices may draw.

Real-Time Statistics

Use this tab to view real-time statistics about PoE utilization and statistics per port.


System
Real-Time Statistics
PoE Utilization
0
5
10
15
20
Port 01
Port 03
Port 07


Port Statistics
Port 1
Port Total TX & RX Octets
35 MB
30 MB
25 MB
20 MB
15 MB
10 MB
5 MB
0 MB
12:36
12:36
12:37
12:37
12:38
12:38
12:38
12:38
12:38
12:38
Total Rx
Total Tx



Ports

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

Port Status

Port	Name	Link Status	Link Speed	Aggregation Group	Bytes Sent	Errors Sent	Bytes Received	Errors Received
1	Port 1	Link Up	Auto (1Gbps Full)		34.14 MB	0 pkts	30.46 MB	0 pkts
2	Port 2	Link Down	Auto		0.00 B	0 pkts	0.00 B	0 pkts
3	Port 3	Link Up	Auto (100Mbps Full)		33.72 MB	0 pkts	1.60 MB	0 pkts
4	Port 4	Link Down	Auto		0.00 B	0 pkts	0.00 B	0 pkts

Table field descriptions:

- **Port** — The number assigned to the port of the switch. The SFP ports are always the last.
- **Name** — The assignable name for the port. Edit the name at **Settings** > **Ports** > **General**.
- **Link Status** — Displays if the link is up or down.

- **Link Speed** — Shows the speed setting for the port. Configurable under **Settings** > **Ports**.

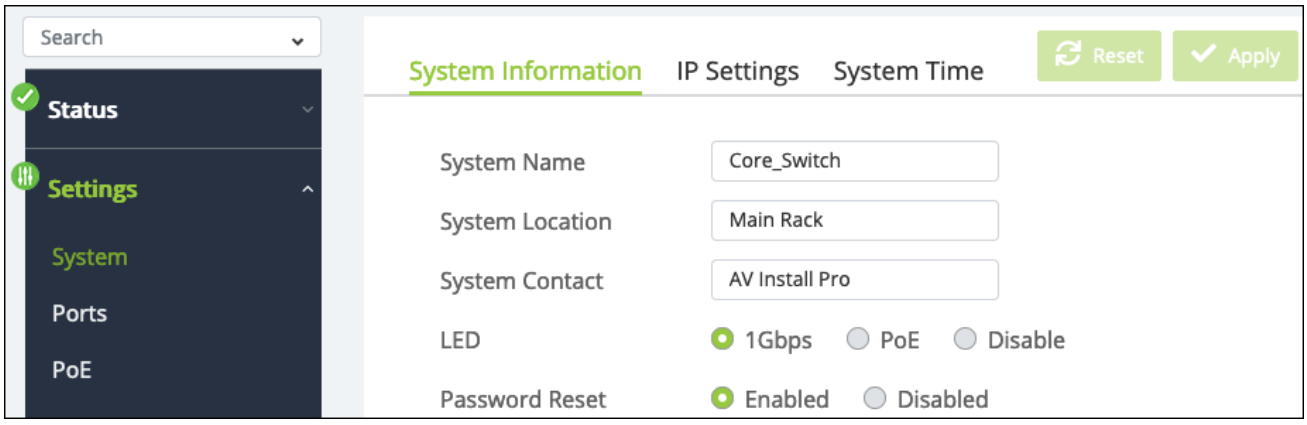
> **Pro Tip:** Manually set the SFP port speed to 1G when connecting to a device that only supports 1G to avoid potential negotiation issues.

- **Aggregation Group** — Displays the link aggregation group the port is a member of, if configured under **Settings** > **Link Aggregation**.
- **Bytes Sent** — The number of bytes, in seconds, being transmitted on the port.
- **Errors Sent** — The number of error packets transmitted from the port.
- **Bytes Received** — The number of bytes, in seconds, being received on the port.
- **Errors Received** — The number of error packets the port has received.

System

System Information

Use this page to update the general configuration of the switch.



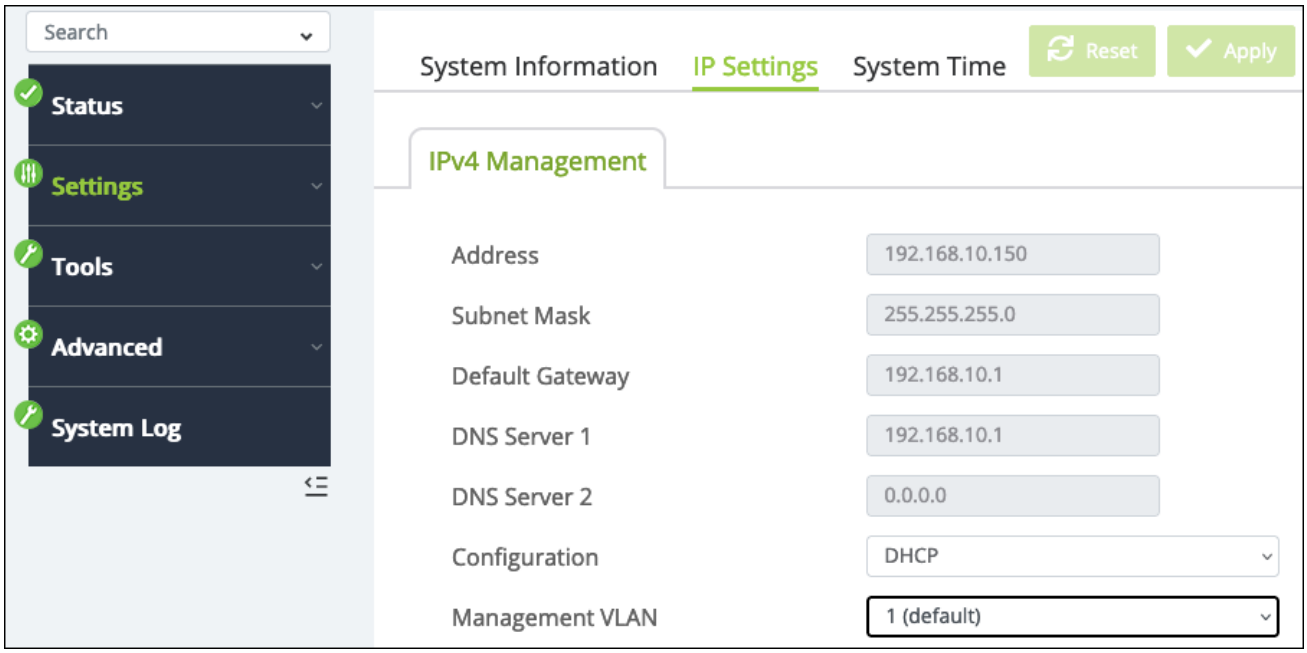
Configurable settings include:

- **System Name** — This is the name of the switch that appears under during network scans by other applications. This name should be unique to the switch.
- **Device Location** — Enter where the switch is located.
- **System Contact** — Enter the name of your company to provide the user of the switch a point of contact, should they need it.
- **LED** — Select the behavior of the port Speed/PoE LEDs. Whether they illuminate for a 1Gbps connection, if they're delivering PoE, or disable them.
- **Password Reset** — Select whether the password reset feature of the "Reset procedures" on page 8 is enabled.

IP Settings

Use this page to configure the switch's IPv4 address and Management VLAN.

Pro Tip: Leave the switch as DCHP and make a MAC or IP reservation in the router to avoid potential loss of connectivity from network changes.

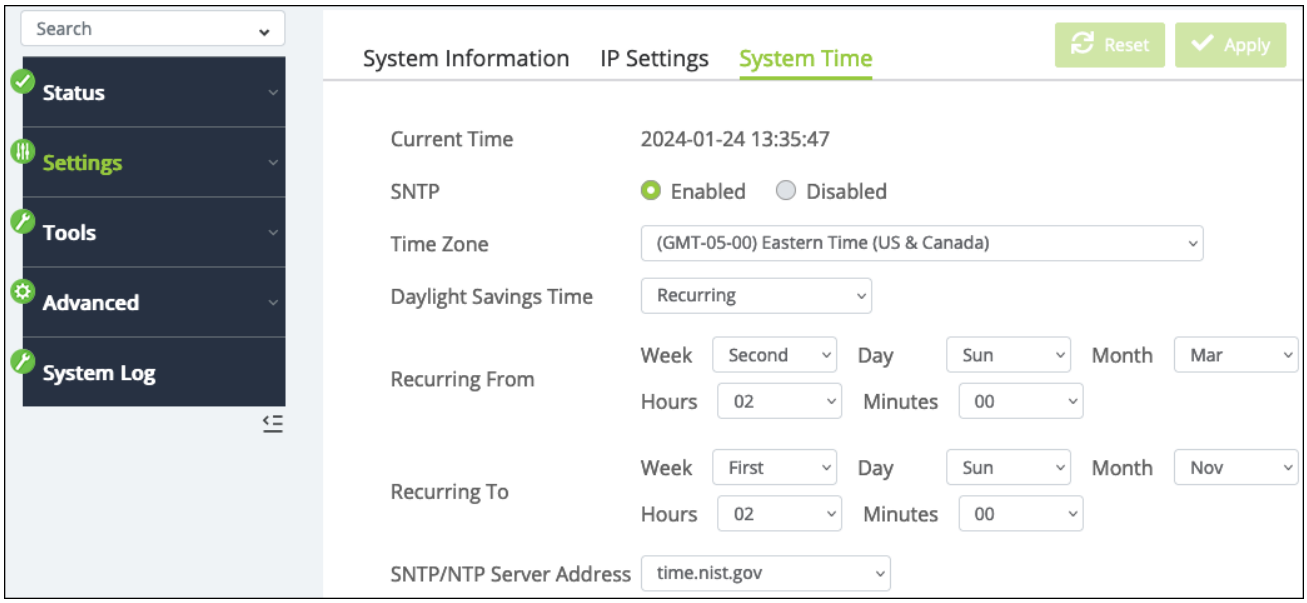


Configurable settings include:

- **Address** — The IPv4 address assigned to the switch.
- **Subnet Mask** — The subnet mask assigned to the switch.
- **Default Gateway** — The default gateway of the network the switch is on.
- **DNS Server 1 and 2** — The DNS servers assigned to the switch.
- **Configuration** — Select DHCP or Static. You must select Static to edit the fields above.
- **Management VLAN** — Allows you to select which VLAN you must be connected to for access to the switch's local user interface.

System Time

Use this page to configure the switch's system time manually or how the time is automatically configured.



Configurable settings include:

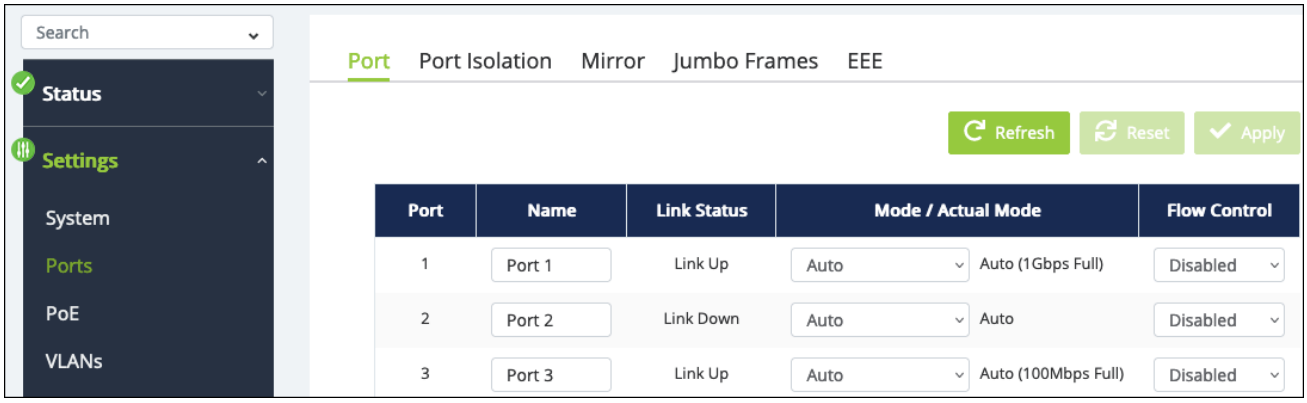
- **Current Time** — The switch's current system time.
- **SNTP (Simple Network Time Protocol)** — Enable to allow the switch to automatically grab the date and time for the location it's installed in.

- **Time Zone** — Select the time zone the switch is installed under.
- **Daylight Savings Time** — Select **Recurring** if the switch is installed in a location that recognizes Daylight Savings Time.
- **Recurring From** — Set the start time for Daylight Savings Time.
- **Recurring To** — Set the end time of Daylight Savings Time.
- **SNTP/NTP Server Address** — Select the server the switch contacts to keep its system time up to date.

Ports

Port

Use this page to assign port names, speed, and alter their Flow Control settings.



Configurable settings include:

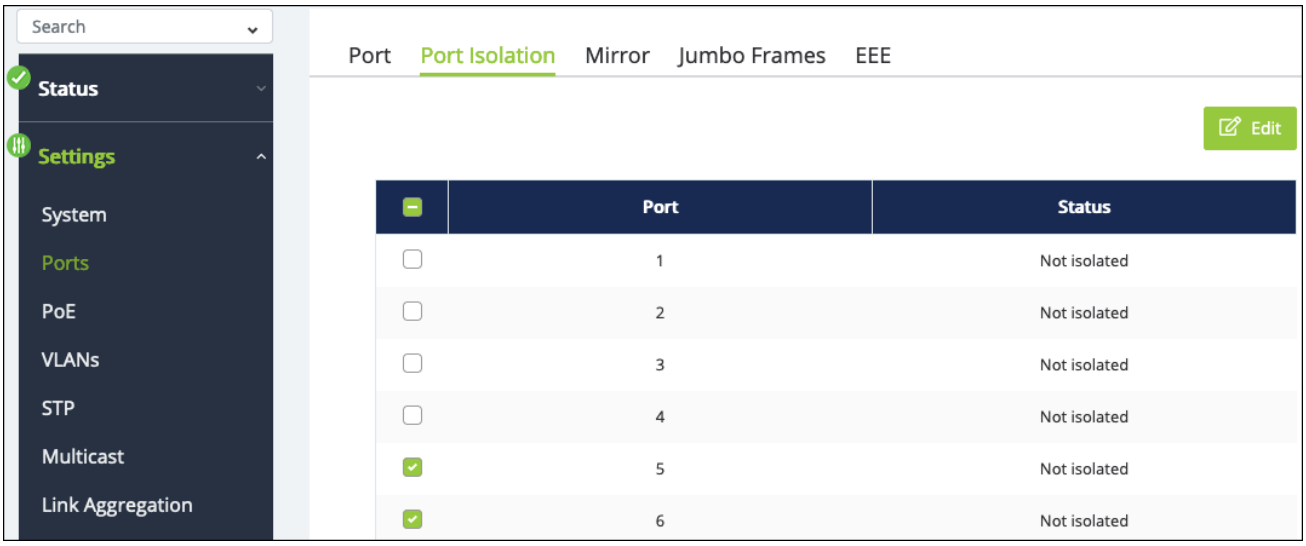
- **Port** — The port number.
- **Port Name** — Enter a meaningful name for the port, like the name of the device connected to it. These names populate in OvrC.
- **Link Status** — Whether the port detects a connection or not.
- **Mode/Actual Mode** — Use the drop-down to select the maximum transfer speed of the port. The true connection speed is displayed in parentheses.

- **Flow Control** — Enable or disable Flow control on the port. Flow control attempts to regulate the transfer rate between network devices so they do not receive more data than they can process.

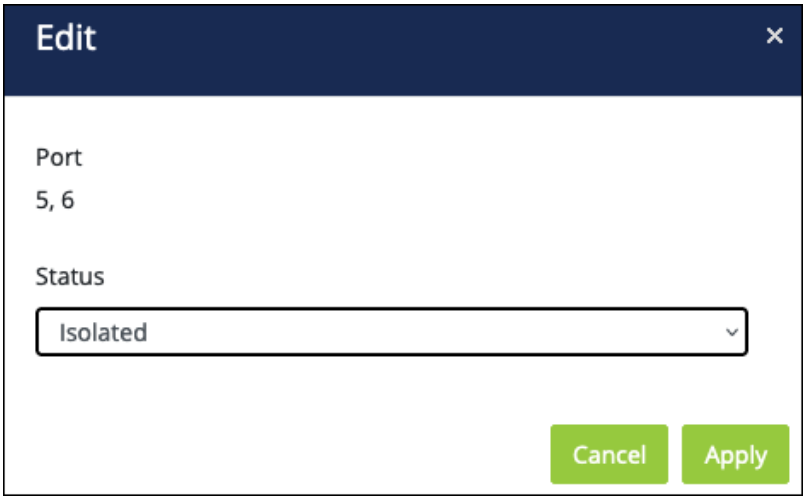
Port Isolation

Port isolation allows you to restrict ports from communicating with downstream ports. They can still communicate with upstream ports.

1. To isolate a port(s), select them, then click **Edit**.



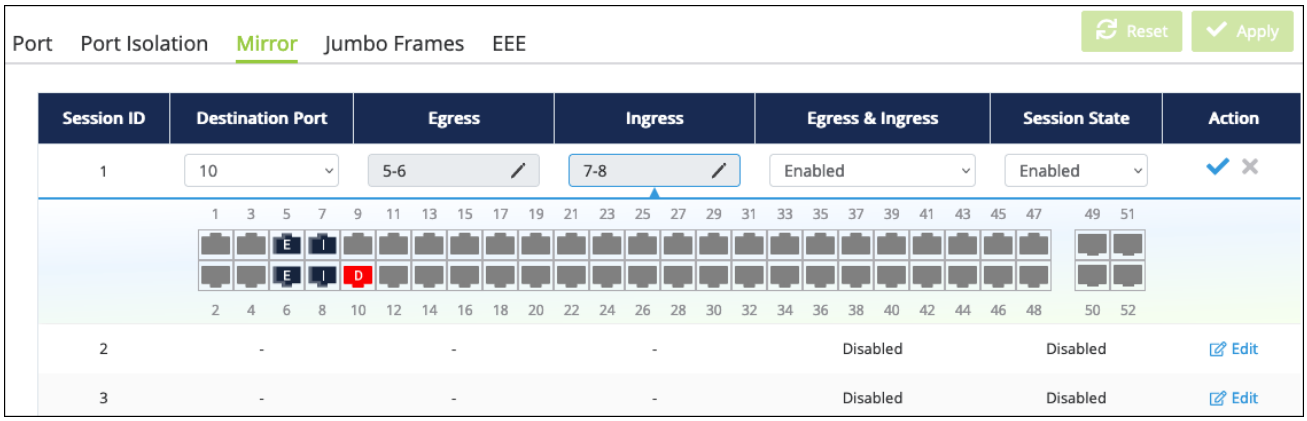
2. Set the **Status** to **Isolate**, then click **Apply**.



Mirror

Port mirroring allows you to monitor traffic from selected ports by mirroring their traffic to a Destination Port, which typically has a computer running port analyzer software to capture the traffic. You can create three total mirroring sessions on the switch.

Caution: Disable unnecessary sessions to avoid issues and reduce processing overhead on the switch.



To create a port mirroring session:

1. Click the **Edit** button in the far right of an empty session row.
2. Set the **Destination Port** to the port number of the connected computer running the analyzer software
3. For **Egress**, select the ports you want to monitor the traffic being sent out on.
4. For **Ingress**, select the ports you want to monitor traffic arriving on.
5. Set the **Egress & Ingress** drop-down to **Enable**.
6. Set the **Session State** to **Enable**.
7. Click the **checkmark icon** under **Action**, then click **Apply** at the top right of the page.

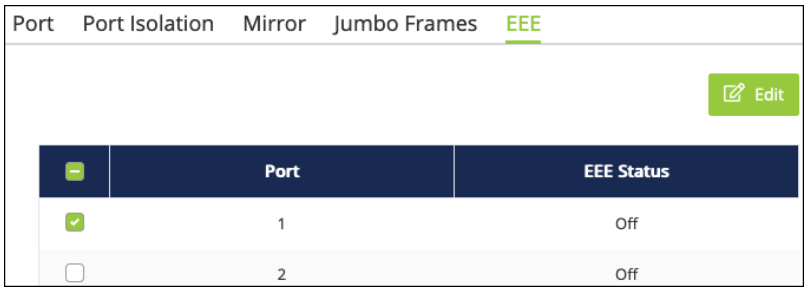
Caution: Disable unnecessary sessions to avoid possible issues and reduce processing overhead on the switch.

Jumbo Frames

Use this page to edit the maximum payload limit the switch can receive.

EEE

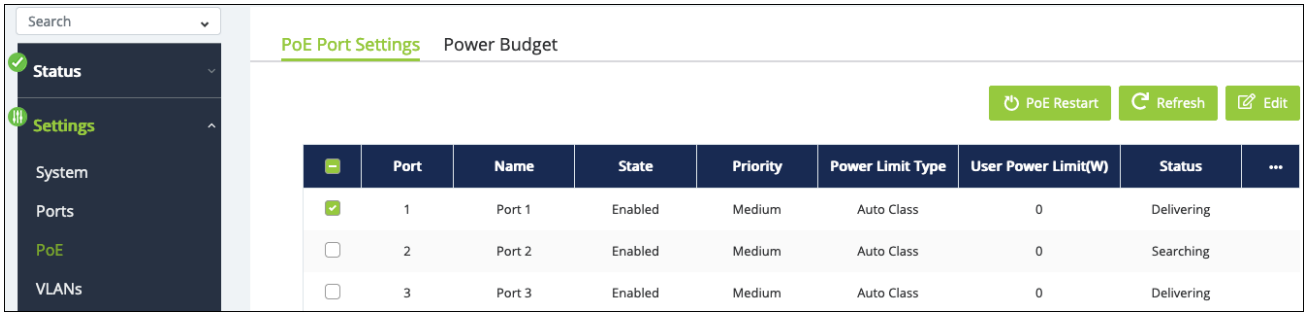
Use this page to enable **EEE (Energy Efficient Ethernet)** on a per-port basis.

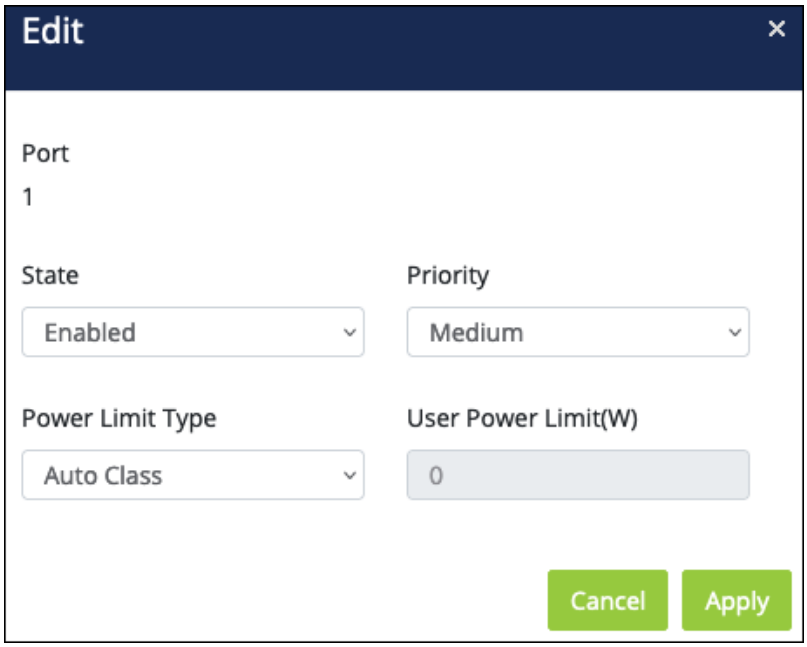


PoE

PoE Port Settings

Use this page to select a specific port(s) and **Restart** their PoE power or **Edit** their PoE settings. Use the ••• button to edit the table fields.



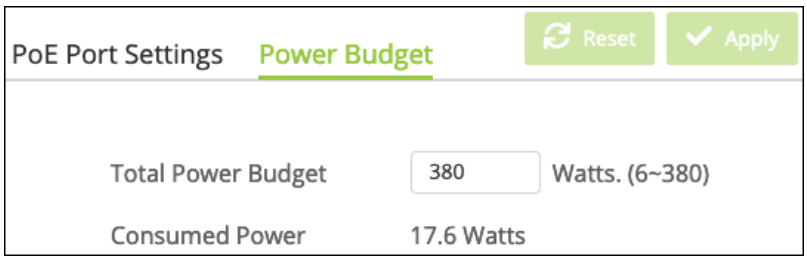


Configurable settings include:

- **State** — Enabled or disabled.
- **Priority** — The priority level for PoE power to be delivered to the port. Devices like access points are typically set to High.
- **Power Limit Type** — Auto Class or User defined.
- **User Power Limit(W)** — Only available if the Power Limit Type is User defined. Enter a value between 1-30.

Power Budget

Use this page to alter the **Total Power Budget** of the switch.

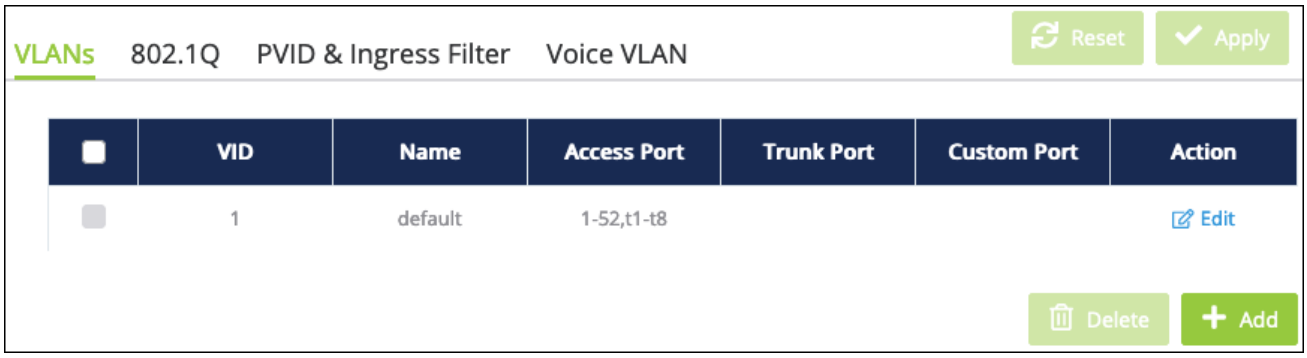


VLANs

VLANs, or **Virtual Local Area Networks**, segment a LAN into logical sub-networks with isolated broadcast domains over the same physical topology.

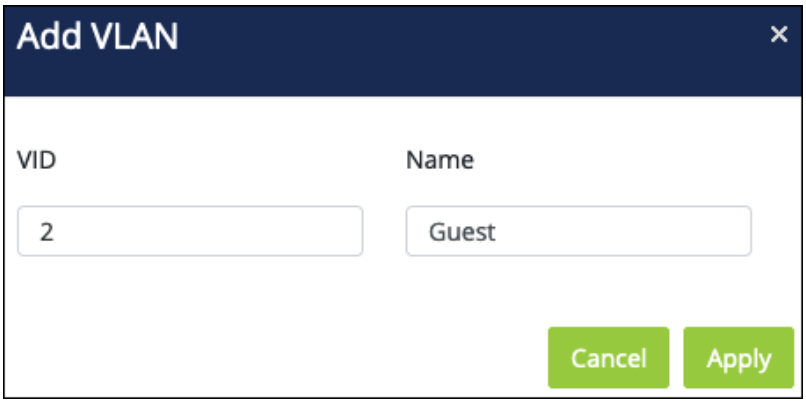
VLANs behave like isolated networks, even though data is moving through the same physical network. VLANs logically group client devices that need to communicate, and restrict data from clients that shouldn't be receiving it.

Use this page to edit or add VLANs.

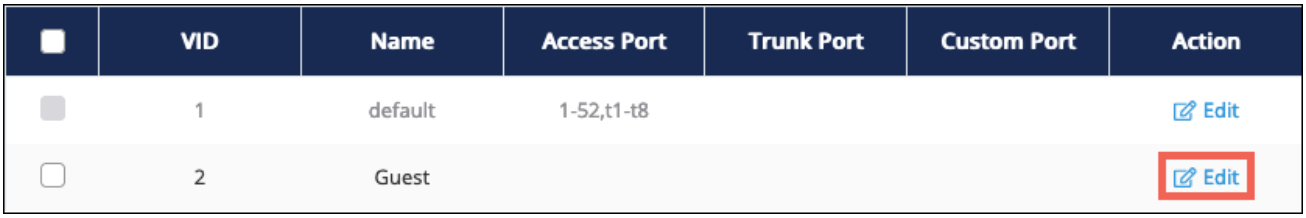


To add a VLAN:

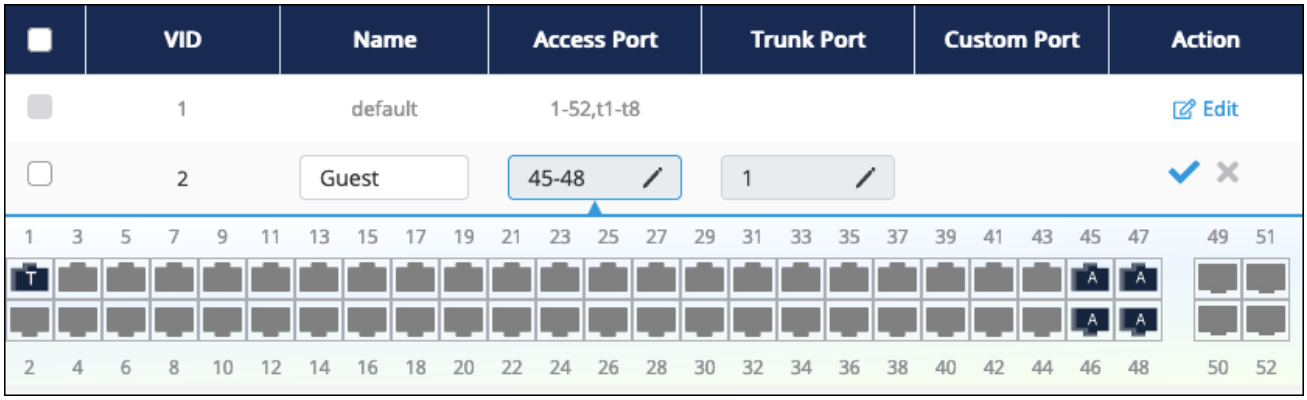
1. Click the **Add** button.
2. Enter a **VID** and a meaningful **Name**. Then click **Apply**.



3. Click the **Edit** button in the far right of the VLAN's row.



4. For **Access Ports**, select ports that should only be in contact with clients on the selected VLAN.
5. For **Trunk Ports**, select ports that can communicate across VLANs. This is typically the switch's uplink port.
6. Click the **checkmark icon**, then click **Apply** at the top of the page.



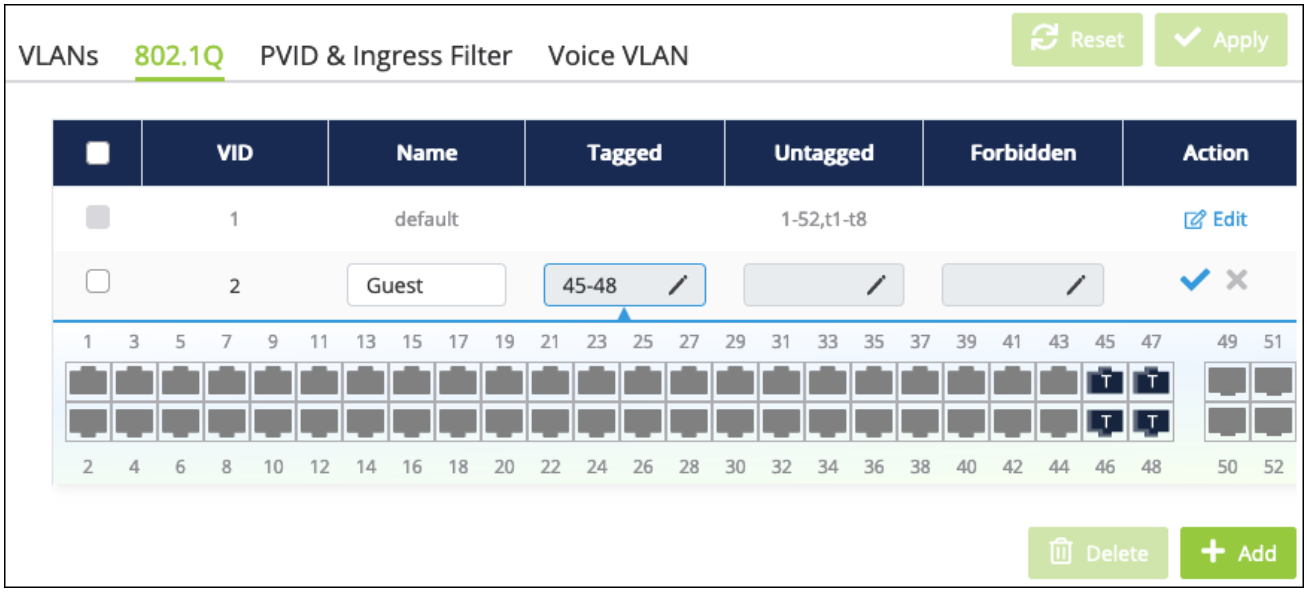
Note: Custom ports are only configurable from the **PVID & Ingress Filter** page.

802.1Q

802.1Q (also known as Dot1q) is used to tag the traffic as belonging to a VLAN. By clicking Edit in a VLANs row, you can select which ports to **Tag** with that VLANs traffic and which port should be **Untagged**.

You can also **Add** a VLAN from this page.

Note: Configured Trunk ports are Tagged and Access ports are Untagged. If you try to make a change to an existing VLAN you're asked to create a new VLAN instead.

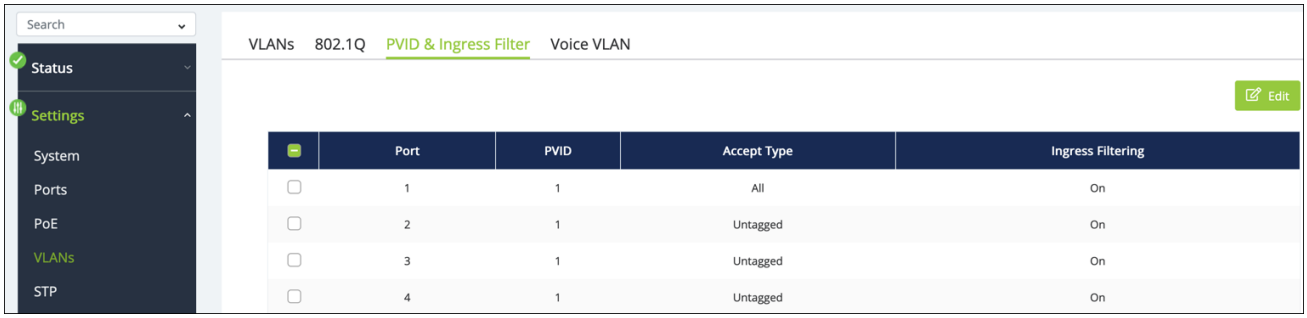


Click the **checkmark icon**, then **Apply** to save your changes.

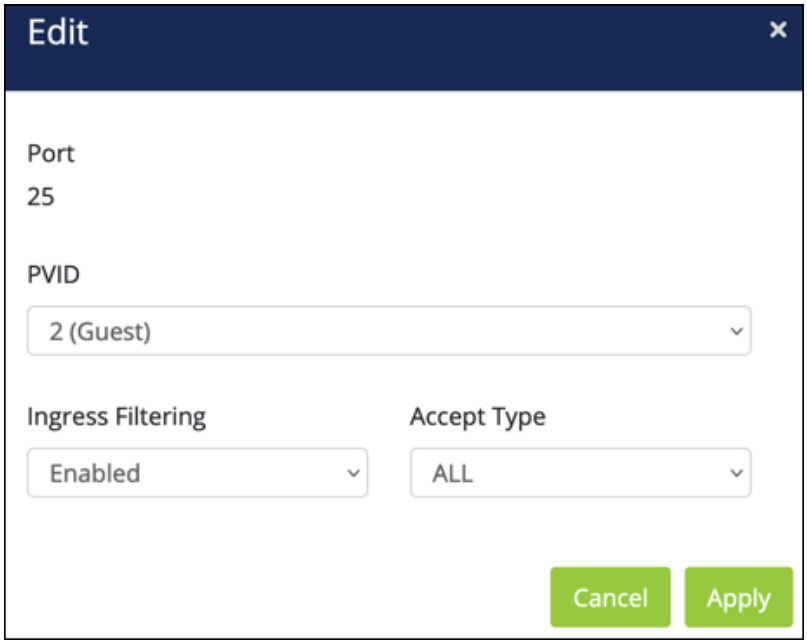
PVID & Ingress Filter

Ingress filtering discards frames from ports that are not a member of the VLAN they are trying to access. Use this page to assign ingress filtering rules to a port's **PVID,** a switchport property used to identify what VLAN it's a member of.

Note: Ingress filtering is enabled on access ports by default to filter out tagged frames from other VLANs.



To edit a port's ingress filtering rules, select the port(s), then click the **Edit** button. You can enable or disable ingress filtering and tell it what type of traffic to accept. Tagged, untagged, or all.



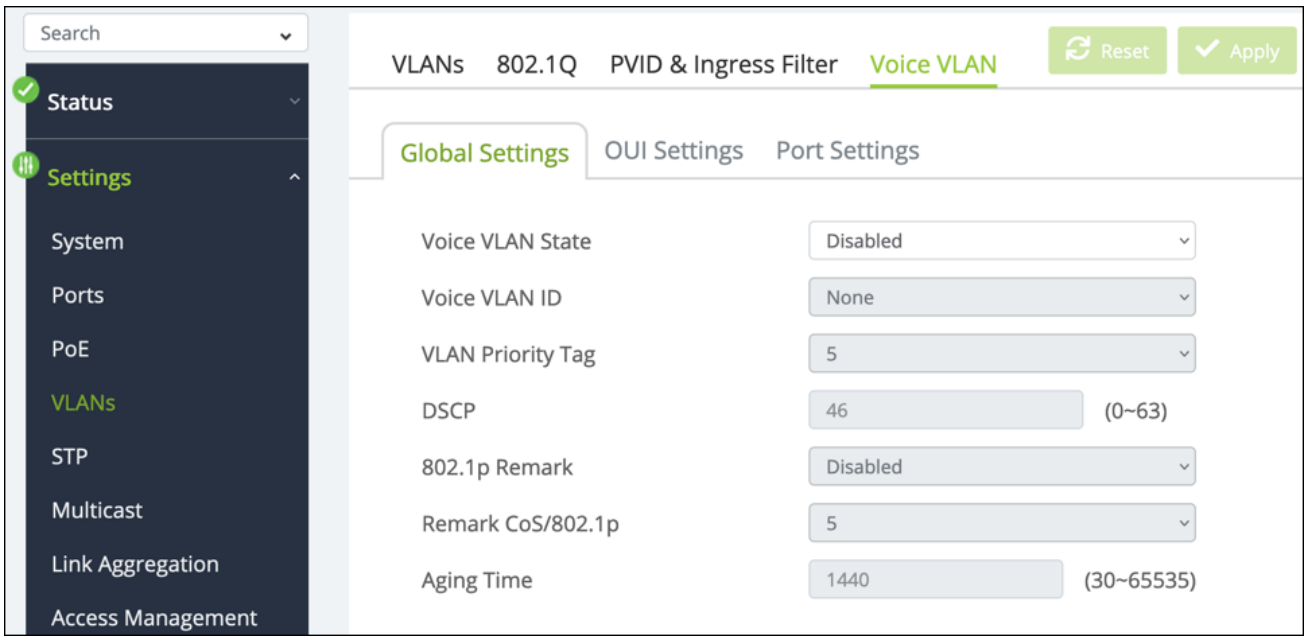
Voice VLAN

Voice over Internet Protocol (VoIP) allows telephone calls over a data network, like the internet. With the network acting as the backbone for many multimedia applications, it's important to properly configure the switch to prioritize VoIP traffic to ensure the

application runs smoothly.

Global Settings

Use this page to assign a VLAN to segregate the voice traffic from non-voice traffic. The default VLAN cannot be used.



Configurable settings include:

- **Voice VLAN State** — Select Disable, Auto, or OUI. The **Auto** feature detects voice traffic in the switch and provides them with a better class of service. **OUI** allows you to manually configure the packet priority.
- **Voice VLAN ID** — Select the VLAN being used for VoIP. It cannot be the default VLAN.
- **VLAN Priority Tag** — Can only be edited with an Auto selection. Select the priority tag to assign to voice traffic.
  Default: 5
- **DSCP** — Can only be edited with an Auto selection. Select the DSCP value for voice traffic.
  Default: 46

- **802.1p Remark** — Can only be edited with an OUI selection. Enable or disable 802.1p remarks in packets to prioritize voice packets.
  Default: Disabled
- **Remark CoS/802.1p** — Can only be edited with an OUI selection. Select what priority level to give voice packets if 802.1p Remark is enabled. Higher values receive a higher priority.
  Default: 5
- **Aging Time** — Can only be edited with an OUI selection. The number of minutes the switch monitors a port for VoIP traffic. If the switch does not receive voice traffic on that port for the allotted time the switch removes the port from the Voice VLAN.
  Default: 1440

OUI Settings

Use this page to add **Organizationally Unique Identifiers (OUIs)** that a connected device may have in their OUI database. Device manufacturers can include OUIs in a network adapter to help identify it. OUI's are a unique 24-bit number assigned by the IEEE registration authority. The switch comes with some preconfigured OUIs.

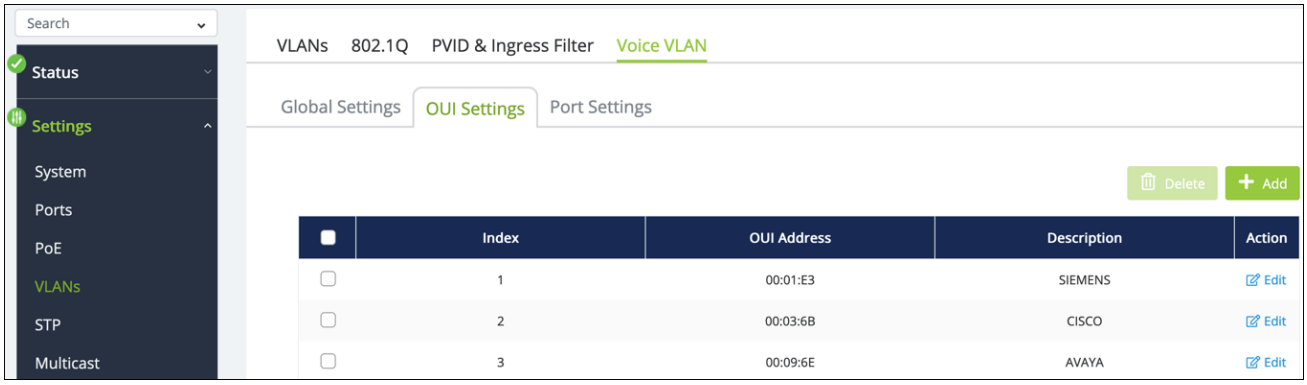


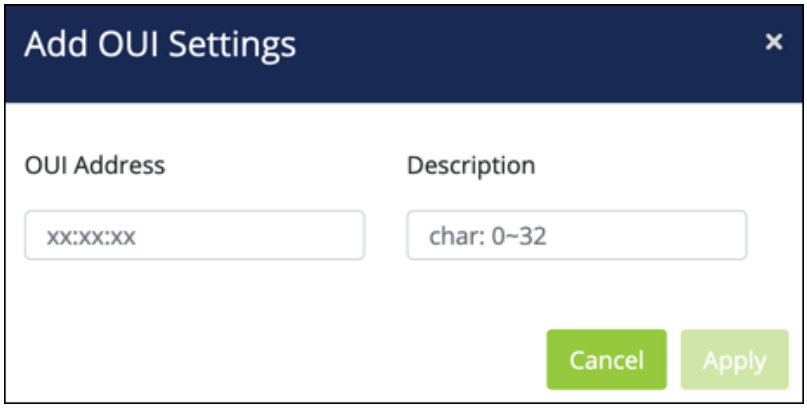
Table field descriptions:

- **Index** — An identifier number for the OUI.
- **OUI Address** — The first portion of a MAC address used to identify the

manufacturer.

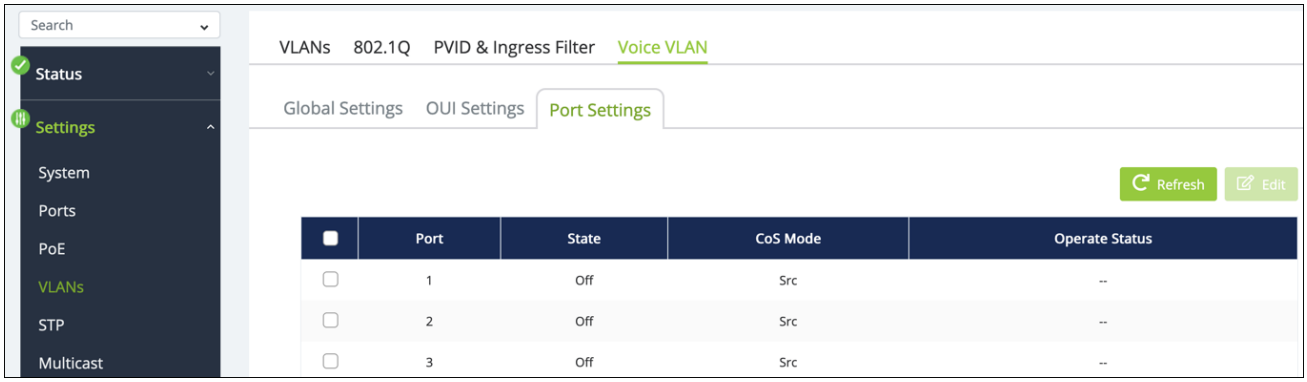
- **Description** — The manufacturer or phone system name.

Click the **Add** button to enter a new OUI for the list.



Port Settings

Use this page to manage Voice VLAN settings for individual ports.

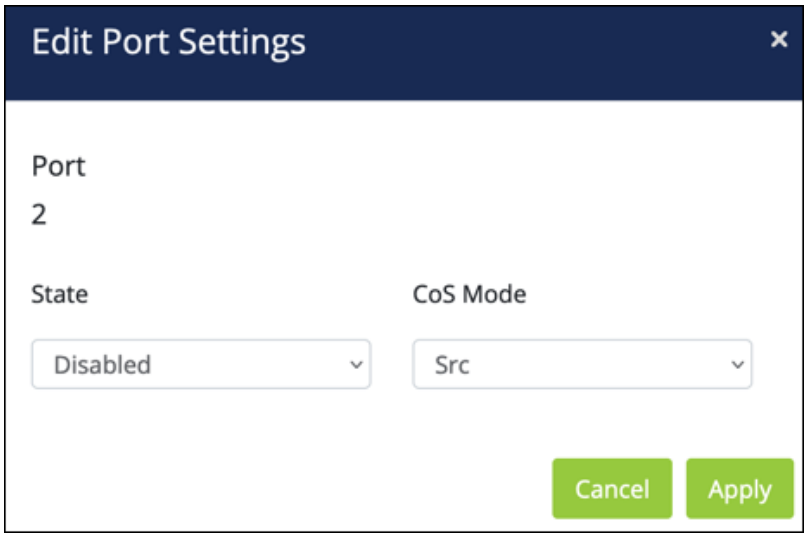


Configurable settings include:

- **Port** — The switchport identifier.
- **State** — Whether the port is examining voice traffic or not.
- **CoS Mode** — The Class of Service (CoS) mode in use on the port.
    - **Src** — (Default) Only packets from the source MAC address are given QoS prioritization on the Voice VLAN.
    - **All** — All of the packets on the VLAN are given QoS prioritization.

- **Operate Status** — Displays the current operating status of the voice VLAN on the port.

Select a port(s), then click the **Edit** button to change these settings.



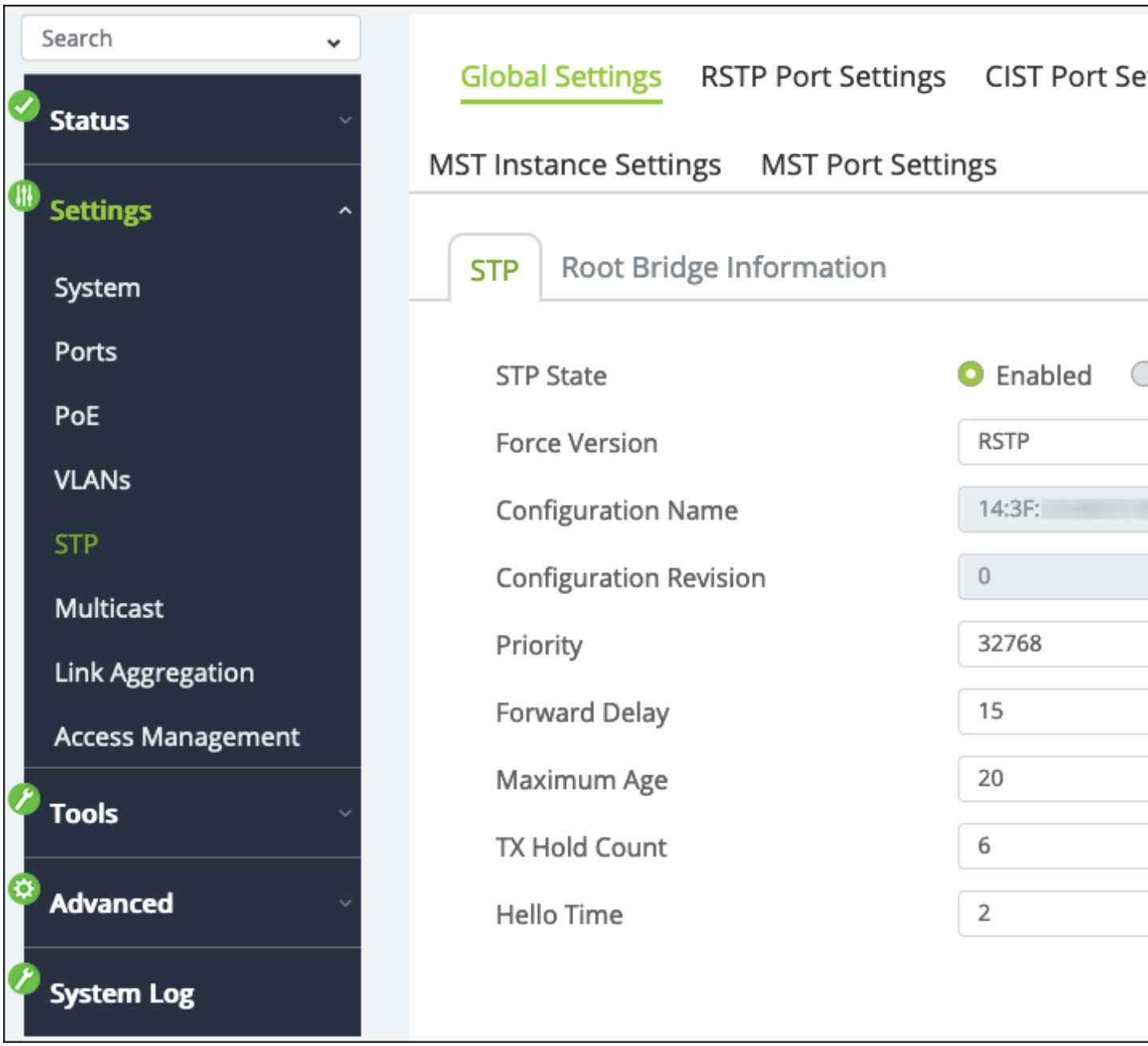
STP

Global Settings

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**.

STP

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



Configurable settings include:

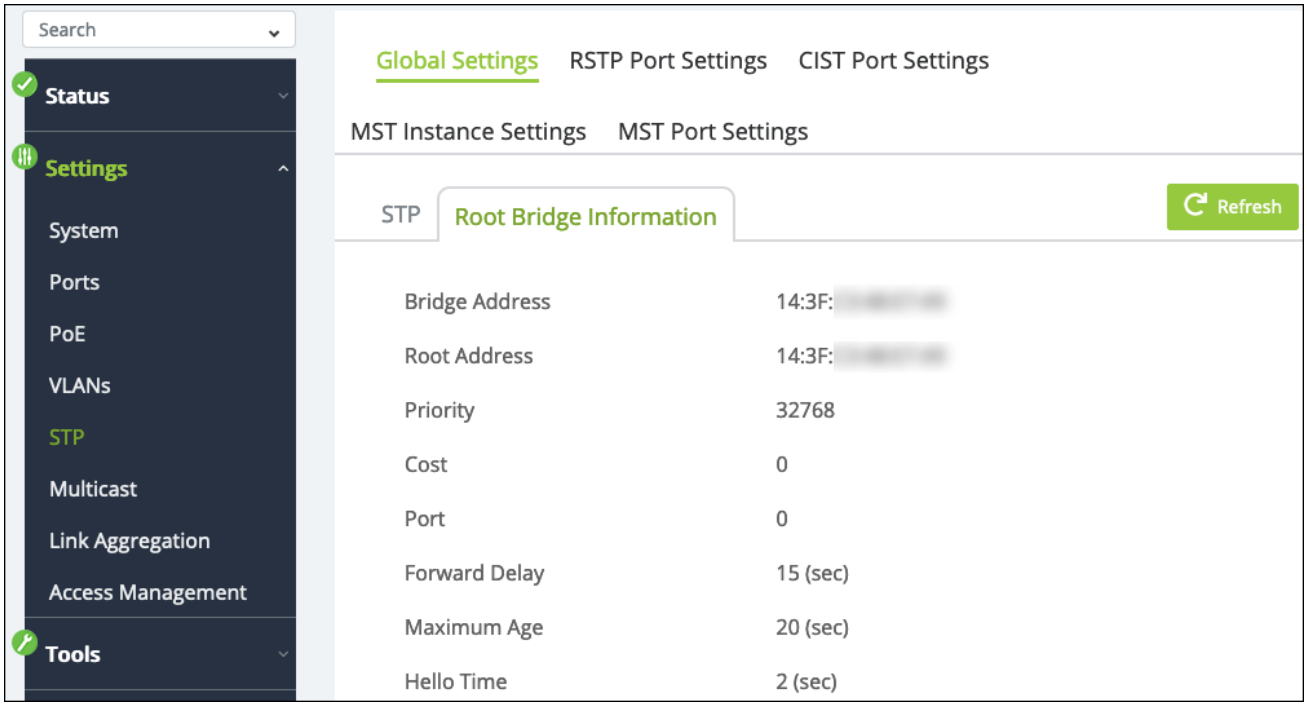
- **STP State** — Enables or disables STP on the switch.
- Force Protocol Version — Choose the STP version for the switch to use.

    - **RSTP** — (Default) 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.
    - **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** — Only configurable if MSTP is selected and is typically left alone, you can enter the name of the MSTP region. Each switch participating in the same MSTP region must share the same Configuration Name, Configuration Revision Level, and MST-to-VLAN mappings.
- **Configuration Revision** — This number must be the same on all switches participating in the MSTP region.
- **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**.
  Default: 32768
- **Forward Delay** — The amount of time a bridge remains in a listening and learning state before forwarding packets.
  Default: 15
- **Maximum Age** — The amount of time a bridge waits before implementing a topological change.
  Default: 20
- **TX Hold Count** — The maximum number of BPDUs (Bridge Protocol Data Units) that a bridge is allowed to send within a hello time window.
  Default: 6

- **Hello Time** — The number of seconds between BPDUs (Bridge Protocol Data Units) sent by the root bridge.
  Default: 2

Root Bridge Information

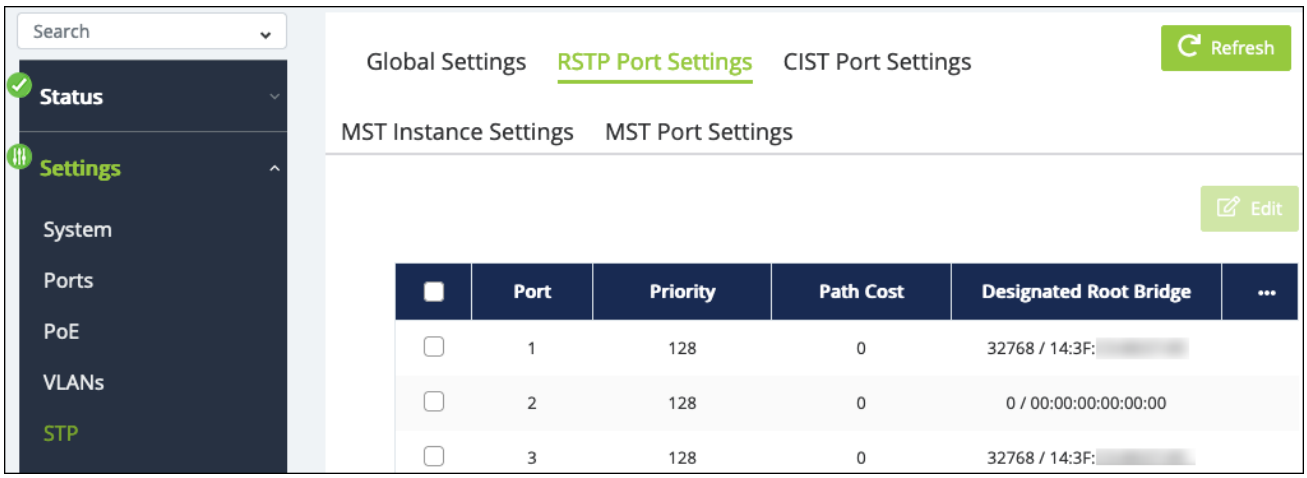
This page displays information about the device acting as the Root Bridge of the local network's STP configuration.

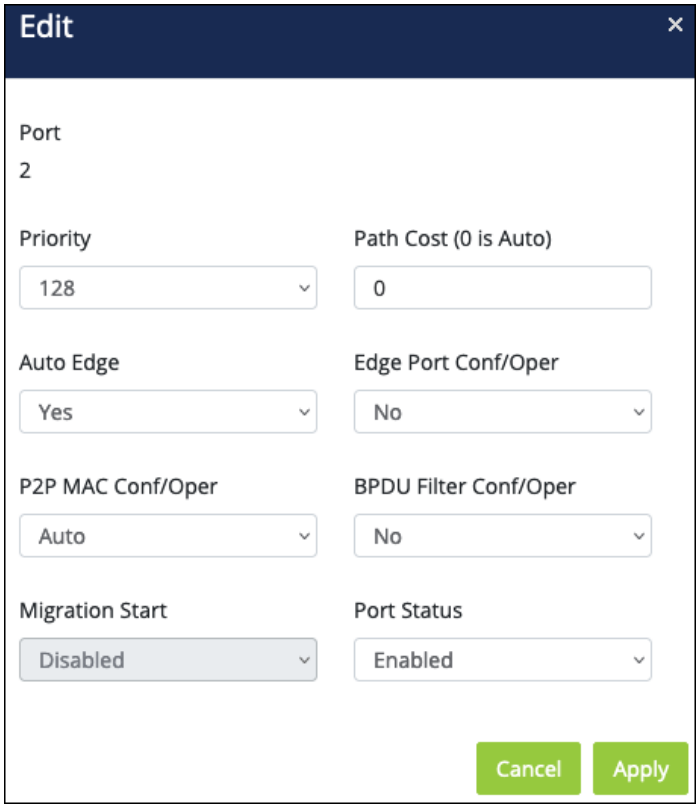


RSTP Port Settings

Use this page to modify **RTSP (Rapid Spanning Tree Protocol)** settings on a per-port basis. The table provides STP information specific to each port. Use the ••• button to edit the table fields.

Select a port(s), then click the **Edit** button to make changes.





Configurable settings include:

- **Port** — The port number being configured.
- **Priority** — The path cost from the port to the root bridge.

  Default: 128
- **Path Cost** — The path cost from the interface to the RTSP regional root.

  Default: 0 (Auto)

- **Auto Edge** — Enable to allow the interface to become an edge port if it does not receive any BPDUs within a given amount of time.

  Default: Yes

> **Pro Tip:** If **Edge Port Conf/Oper** is set to **Yes**, set **Auto Edge** to **No** to avoid conflicts.

- **Edge Port Conf/Oper (Configured/Operating)** — Select Yes to allow the interface to become an edge port if it does not receive any BPDUs within a given amount of time.

  Default: No

> **Pro Tip:** If **Edge Port Conf/Oper** is set to **Yes**, set **Auto Edge** to **No** to avoid conflicts.

- **P2P MAC Conf/Oper** — Auto (the default) allows P2P ports to function in full duplex mode. Select **Yes** to force P2P ports into full duplex or **No** for no P2P functionality.

  Default: Auto

- **BPDU Filter Conf/Oper** — When enabled, BPDU traffic is filtered on the edge ports. Edge ports do not need to participate in the spanning tree, so BPDU filtering allows BPDU packets received on edge ports to be dropped.

  Default: No

- **Migration Start** — Enable to force the port to use the newest configuration.

  Default: Disabled

- **Port Status** — Enable or disable STP on the port.

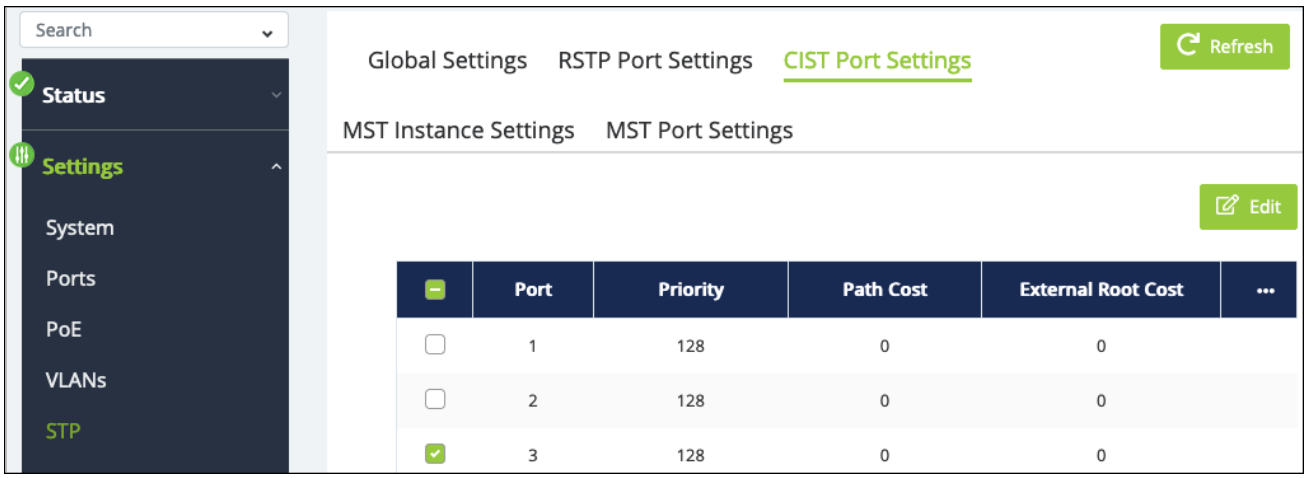
  Default: Enabled

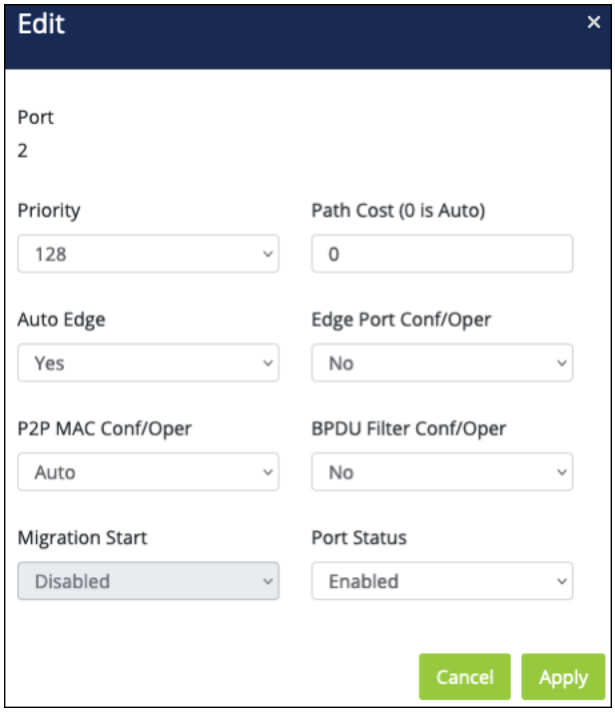
CIST Port Settings

Use this page to modify **CIST (Common and Internal Spanning Tree)** settings on a per-port basis. The table provides STP information specific to each port. Use the ••• button to edit the table fields.

Note: The **Force Version** on the STP > Global page must be **MSTP** to configure CIST.

Select a port(s), then click the **Edit** button to make changes.





Configurable settings include:

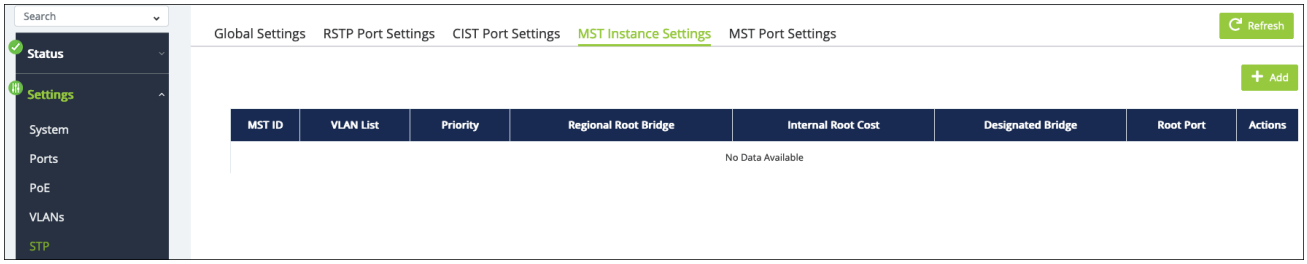
- **Port** — The port number being configured.
- **Priority** — The path cost from the port to the root bridge.
- **Path Cost** — The path cost from the interface to the RSTP regional root.
- **Auto Edge** — Enable to allow the interface to become an edge port if it does not receive any BPDUs within a given amount of time.
- **Edge Port Conf/Oper (Configured/Operating)** — Select Yes to allow the interface to become an edge port if it does not receive any BPDUs within a given amount of time.
- **P2P MAC Conf/Oper** — Auto (the default) allows P2P ports to function in full duplex mode. Select **Yes** to force P2P ports into full duplex or **No** for no P2P functionality.
- **BPDU Filter Conf/Oper** — When enabled, BPDU traffic is filtered on the edge ports. Edge ports do not need to participate in the spanning tree, so BPDU filtering allows BPDU packets received on edge ports to be dropped.

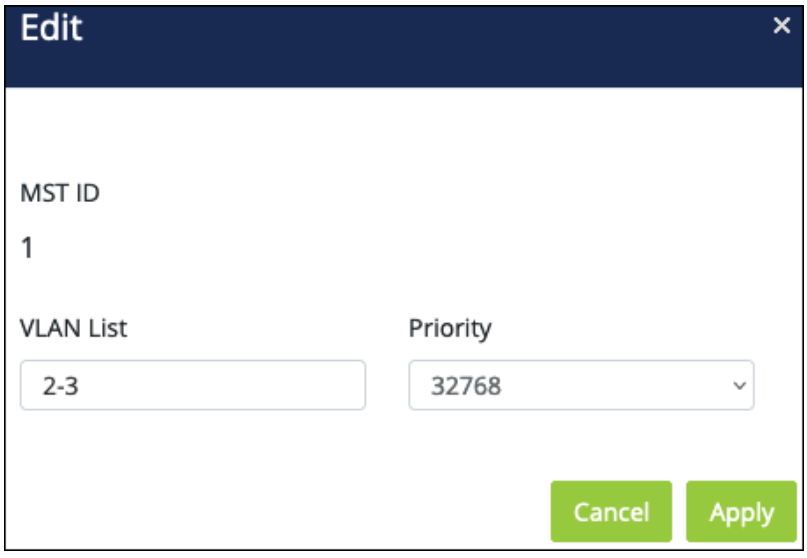
- **Migration Start** — Enable to force the port to use the newest configuration.
- **Port Status** — Enable or disable STP on the port.

MST Instance Settings

Multiple Spanning Tree Protocol (MSTP) maps multiple VLANs to one spanning tree topology. Since there are rarely as many unique topologies as VLANs in a network, using MST saves switch CPU power by reducing the number of spanning tree instances required to handle all VLANs on the device. Each MST instance acts as its own RSTP node within the network's CIST.

Click the **Add** button to create an MST instance.





Configurable settings include:

- **MST ID** — Select an identifier for the MST instance.
- **VLAN List** — Enter the VLAN ID or VLAN ID range to map to the MSTI (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.
  Default: 32768

MST Port Settings

Use this page to view and configure the Multiple Spanning Tree (MST) settings on a per-port basis.

Use the **MST ID** drop-down at the top of the table to select which MST ID information to view and edit.

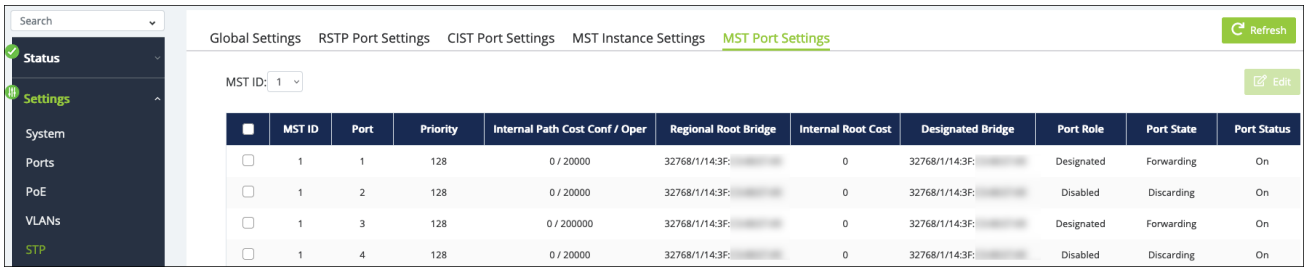
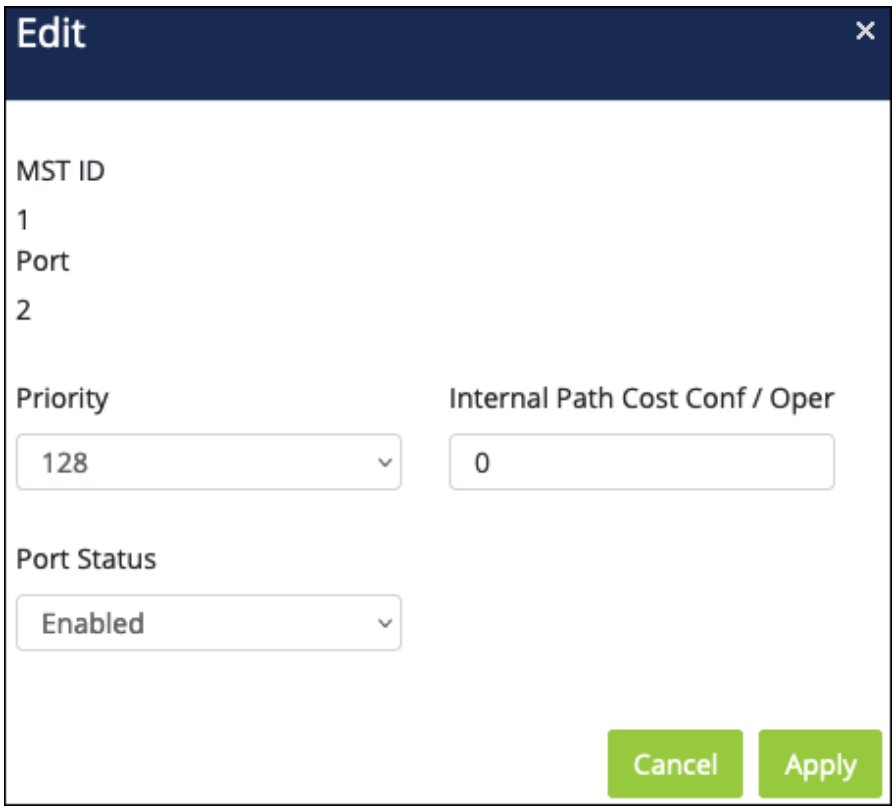


Table field descriptions:

- **MST ID** — The identifier for the MST instance.
- **Port** — The port number of the switch.
- **Priority** — The priority for the port within the MSTI. This value is used to determine which interface 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.

- **Internal Path Cost** — (Configured/Operating) The MST port table displays the current operational internal path cost. Configure the path cost by selecting the port, then clicking Edit.
- **Regional Root Bridge** — The regional root bridge of the selected MST ID. Different MST IDs can have a different regional root bridge.
- **Internal Root Cost** — Displays the cost to reach the regional root bridge inside the MSTP region. When a BPDU is received on an internal port, this cost is adjusted based on the receiving boundary port cost. This information is not shared or counted outside the region.
- **Designated Root Bridge** — 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.
- **Port Role** — Roles include:
    - **Root** – The port links the switch to the root bridge device.
    - **Designated** — Ports in use within the MSTP region.
    - **Disabled** — Port is not in use.
- **Port State** — States include:
    - **Root** — The port links the switch to the root bridge device.
    - **Disabled** — Port is not in use.
- **Port Status** — Whether the port is on or not.

Select a port(s), then click the **Edit** button to make changes.



Configurable settings include:

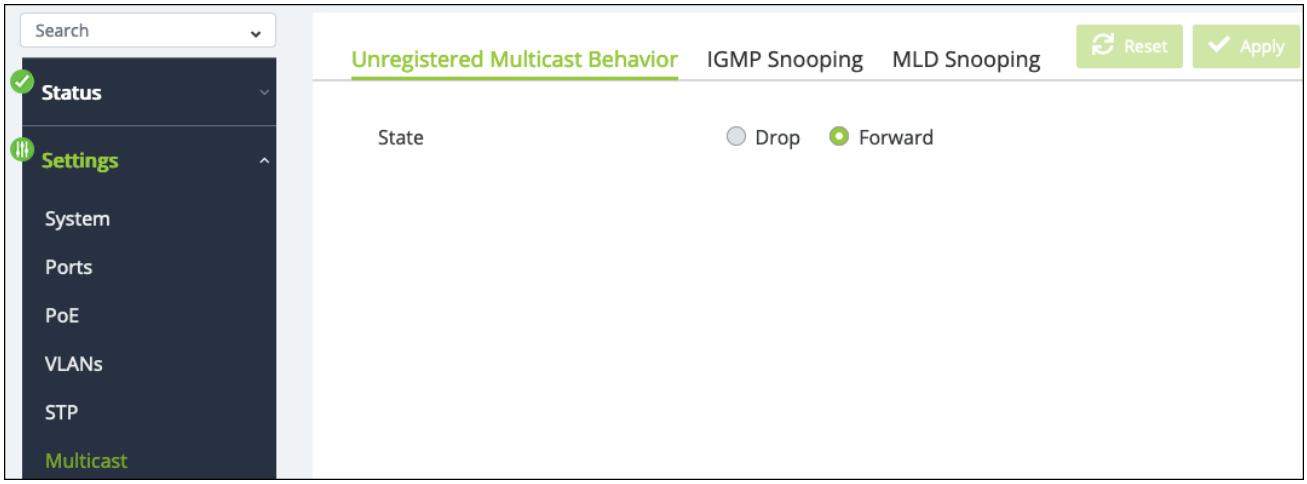
- **Priority** — The priority for the port within the MSTI. This value is used to determine which interface becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
  Default: 128
- **Internal Path Cost** — (Configured/Operating) Set the configured internal path cost in this window. The MST port table displays the current operational internal path cost.
  Default: 0
- **Port Status** — Enable or disable STP on the port.
  Default: Enabled

Multicast

Multicast is a one-to-many network relationship. It allows one device to send data to multiple destinations at the same time. Common multicast applications include MoIP, SDDP, and AirPlay. For more information, read **Understanding Multicast & IGMP**.

Unregistered Multicast Behavior

Use this page to configure how the switch should handle unregistered multicast traffic.



Available states are:

- **Forward** — (Default) Unregistered multicast packets are forwarded to all active interfaces on the switch but not to the CPU, to reduce overhead.
- **Drop** — The switch does not forward unregistered multicast packets to the interfaces.

IGMP Snooping

The **Internet Group Management Protocol (IGMP)** is a mechanism used on IPv4 networks to establish multicast group memberships.

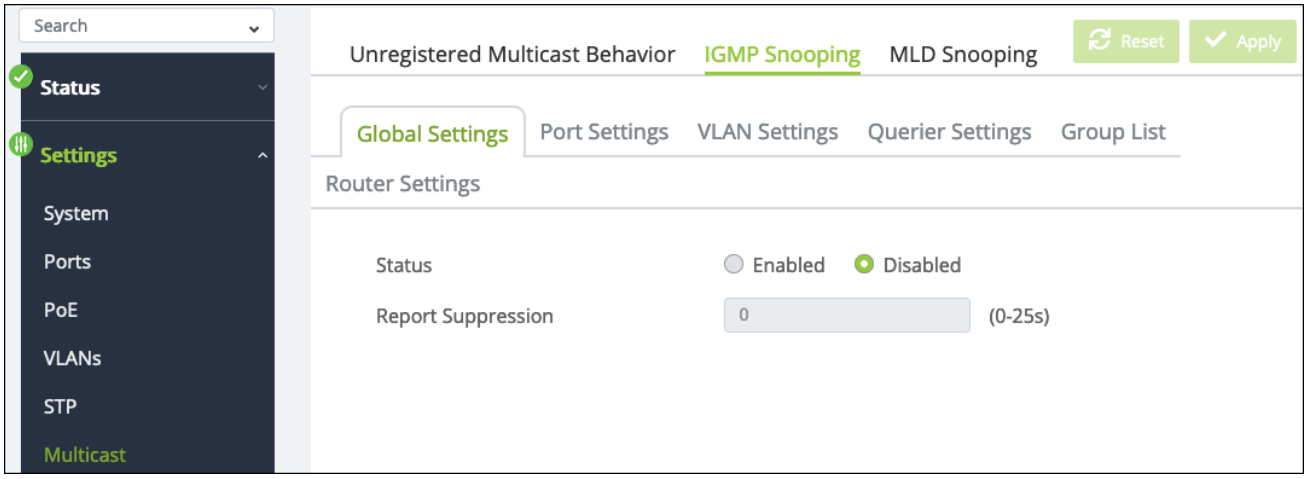
Note: IGMP does not manage all multicast traffic. read **Understanding Multicast & IGMP** for more information.

Global Settings

Use this page to enable IGMP snooping and change the **Report Suppression** time (in seconds).

Report suppression time is the amount of time the switch delays duplicate IGMP report messages to reduce the amount of IGMP snooping messages sent over the network. Default is 0, which means disabled.

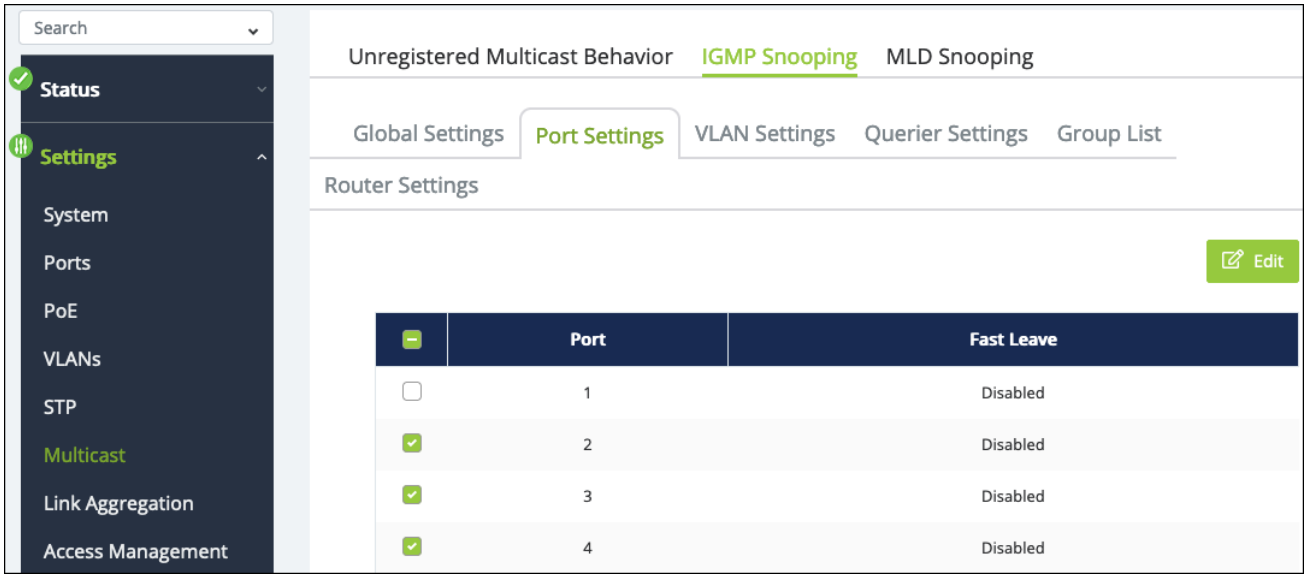
Note: Report suppression is not a feature of IGMPv3.

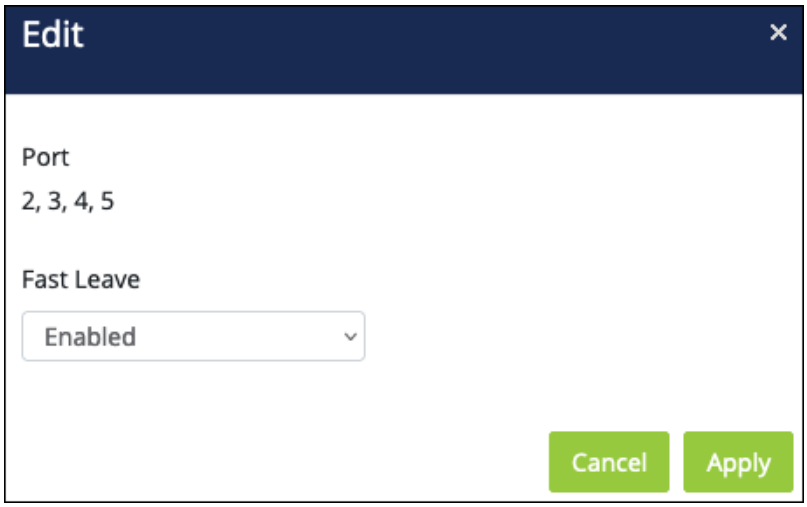


Port Settings

Use this page to enable or disable **Fast Leave** on a port(s). Fast Leave tells a port receiving an IGMP leave message to remove the associated multicast group from the port, without waiting for the normal message interval to end. This feature is typically enabled when the multicast streams are each more than half the available bandwidth of the switch port.

Select a port(s), then click the **Edit** button to change the Fast Leave status.

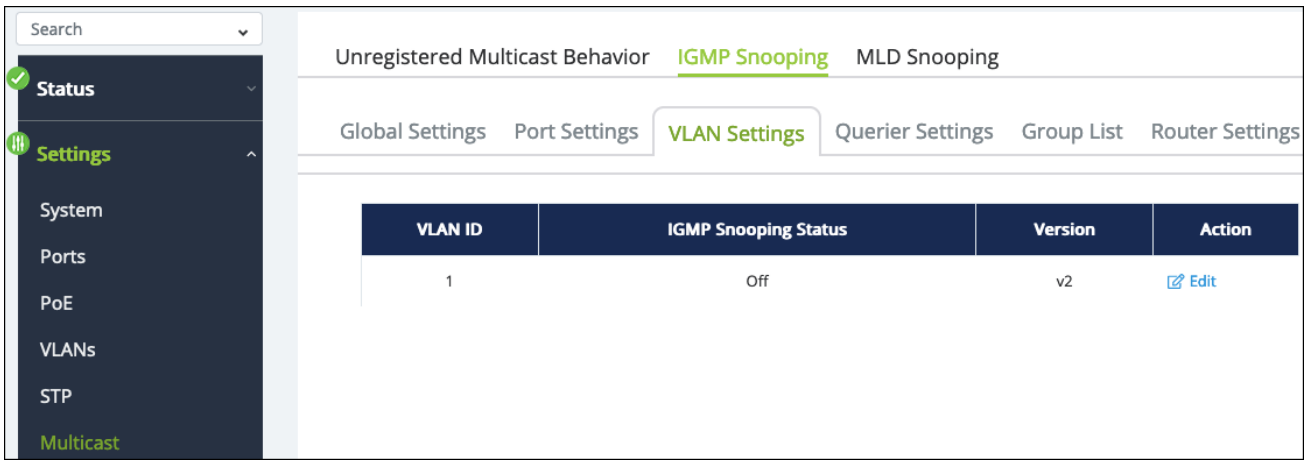




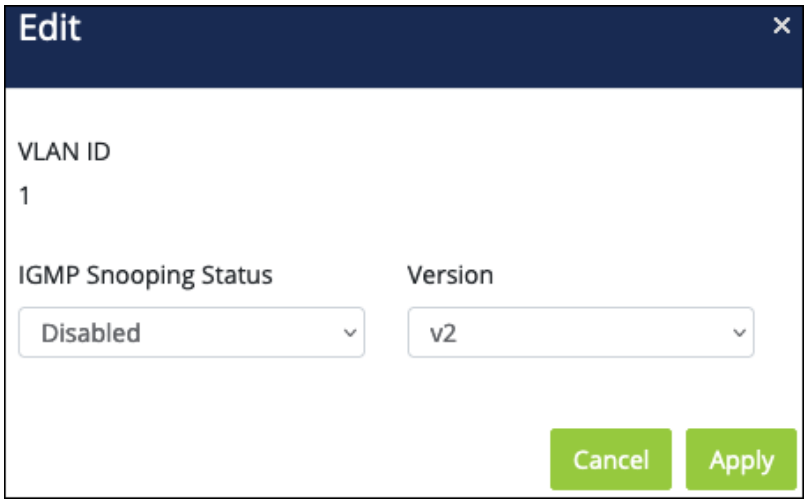
VLAN Settings

Use this page to enable IGMP snooping and select the IGMP version on a per-VLAN basis.

Click the **Edit** button, under the **Action** column, to change the IGMP Snooping Status of a VLAN.



Note: Consult the application documentation when choosing an IGMP version.



Querier Settings

Use this page to modify the IGMP Querier configuration on each VLAN. An **IGMP Snooping Querier** asks all the devices on the network what multicast traffic they want. IGMP-enabled devices send IGMP Join messages back to the IGMP Snooping Querier. The Querier sends this information to each switch to update their **IGMP Multicast Group Tables**, which are used to organize the multicast addresses that switch ports are asking for.

Use the ••• button to edit the table fields. Click the **Edit** button, under the **Action** column, to change the IGMP Snooping Status of a VLAN.

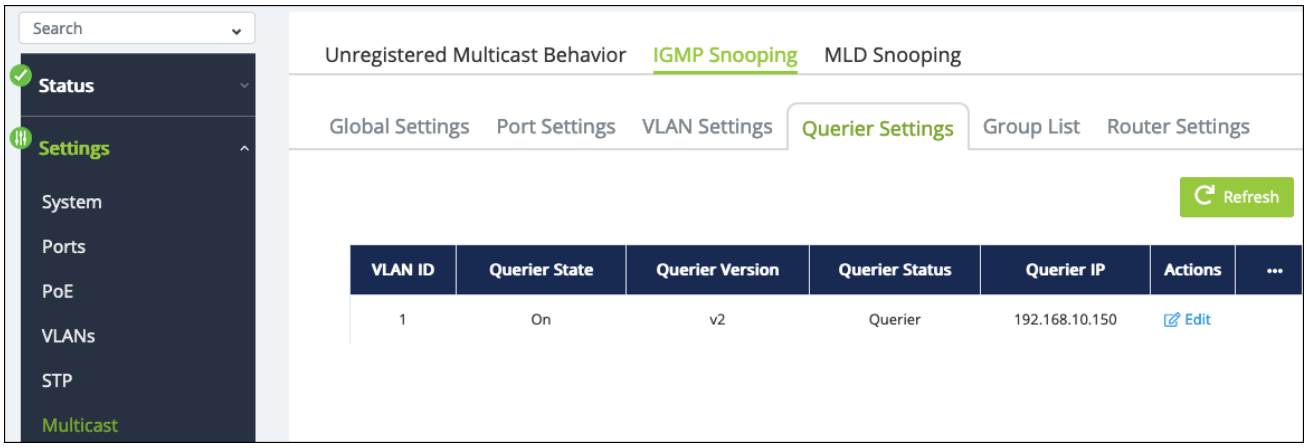
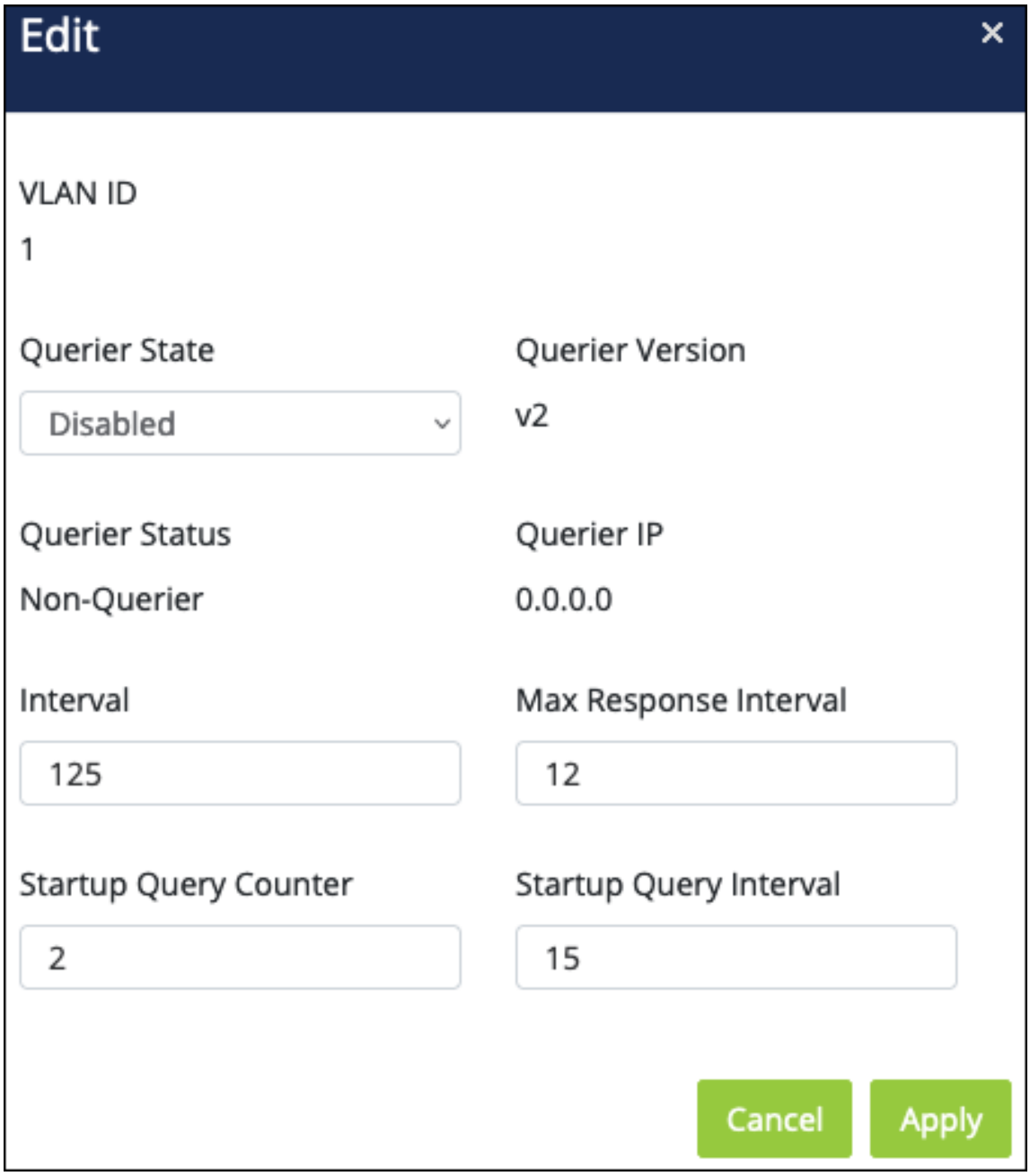


Table field descriptions:

- **VLAN ID** — The VLAN identifier used to configure IGMP snooping.
- **Querier State** — Displays if IGMP querier is enabled for this switch on the VLAN.
- **Querier Version** — The IGMP version configured for the VLAN under the VLAN Settings tab.
  Default: 2
- **Querier IP** — The IP address of the device acting as the IGMP querier on the VLAN.



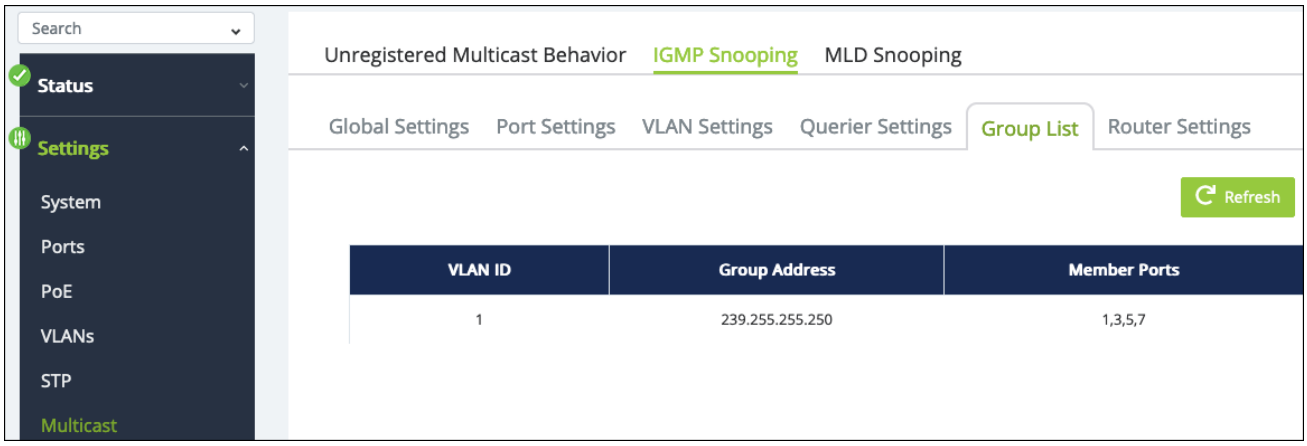
Configurable settings include:

- **Querier State** — Enable or disable this switch as an IGMP querier for the VLAN.
- **Interval** — The amount of time (in seconds) that the switch sends querier messages to discover which multicast groups the hosts on the network have joined.
  Default: 125

- **Startup Query Counter** — The number of IGMP queries the switch sends at startup.
  Default: 2
- **Max Response Interval** — The maximum amount of time (in seconds) that hosts are allowed to wait before responding to the General Query.
  Default: 12
- **Startup Query Interval** — The amount of time (in seconds) that the switch sends IGMP queries at startup.
  Default: 15

Group List

This page displays the multicast groups (**Group Address**) reporting to the switch and the ports (**Member Ports**) that are sending and receiving packets in that group.



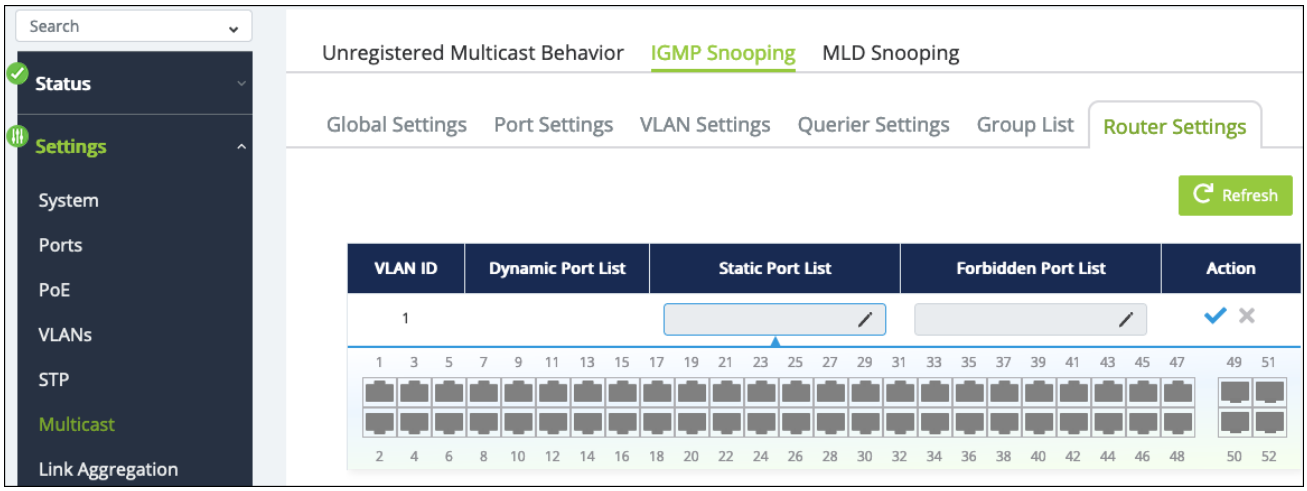
Router Settings

Use this page to configure **Multicast router ports (Mrouter ports)** for specific VLANs. Mrouter ports forward multicast messages to other members of the multicast group.

Multicast router (Mrouter) port types:

- **Dynamic** — The port learned that it should be a router port through IGMP messaging on the network.
- **Static** — The port is manually configured to be a multicast router port.
- **Forbidden** — These ports are not configurable for multicast routing.

Click the **Edit** button, under the Actions column to add ports to the Static and Forbidden port lists. Click the **checkmark** button to save those changes.



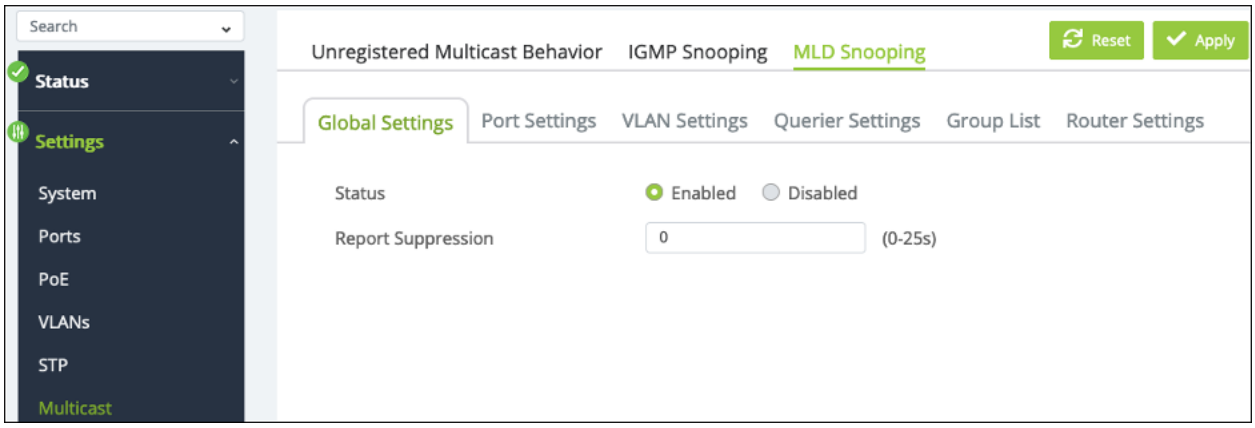
MLD Snooping

MLD (Multicast Listener Discovery) snooping is used by IPv6 multicast routers to detect multicast listeners.

Global Settings

Use this page to enable MLD snooping and change the **Report Suppression** time (in seconds).

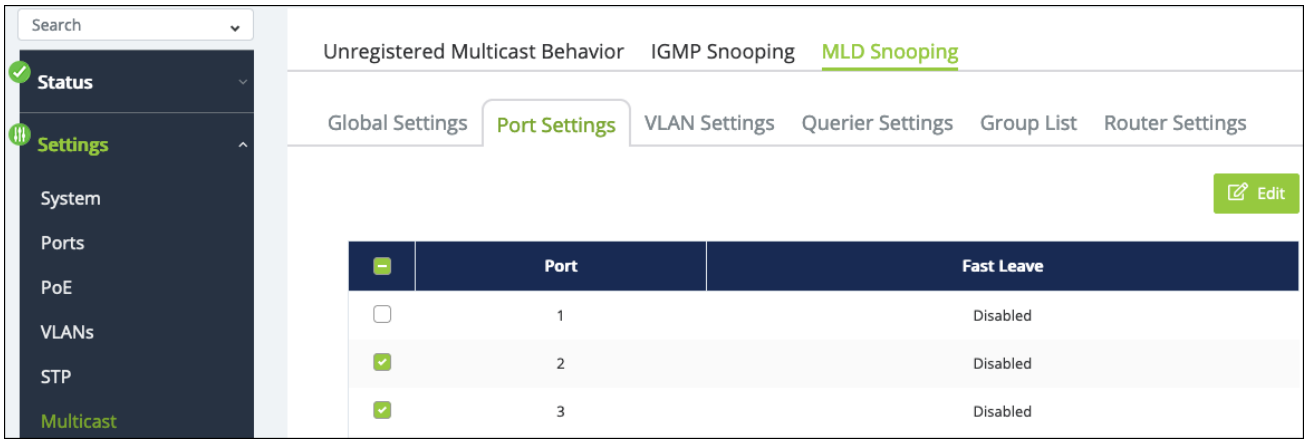
Report suppression time is the amount of time the switch delays duplicate IGMP report messages to reduce the amount of MLD snooping messages sent over the network. Default is 0.

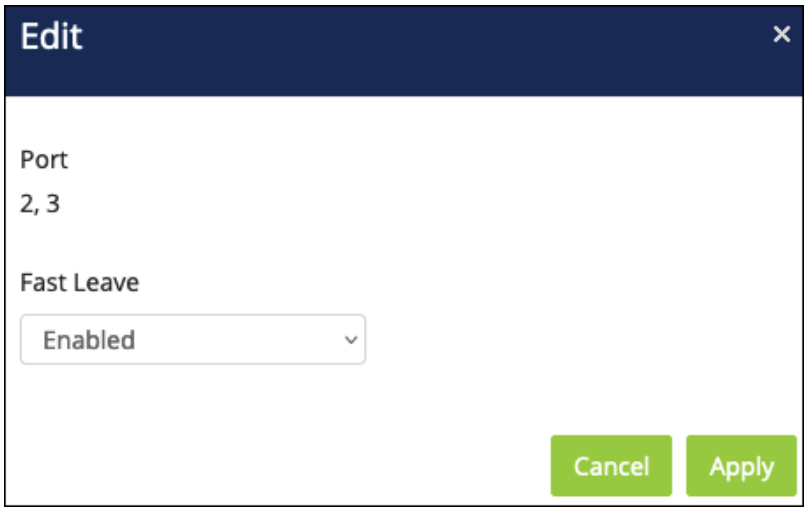


Port Settings

Use this page to enable or disable **Fast Leave** on a port(s). Fast Leave tells a port receiving an MLD leave message to remove the associated multicast group from the port, without waiting for the normal message interval to end. This feature is typically enabled when the multicast streams are each more than half the available bandwidth of the switch port.

Select a port(s), then click the **Edit** button to change the Fast Leave status.

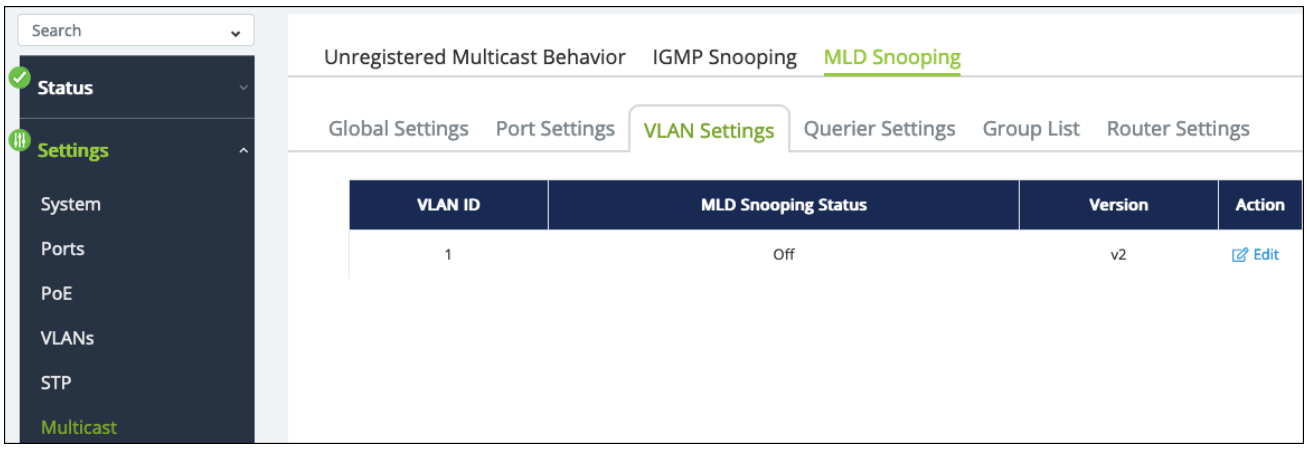




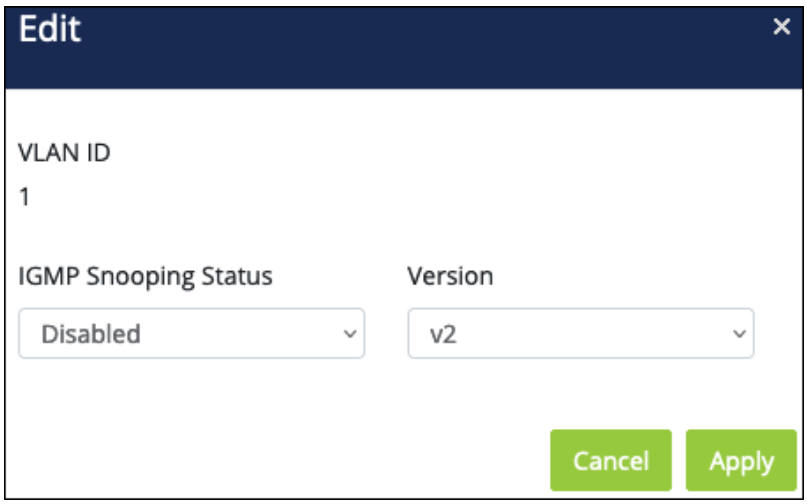
VLAN Settings

Use this page to enable MLD snooping and select the IGMP version on a per-VLAN basis.

Click the **Edit** button, under the **Action** column, to change the MLD Snooping Status of a VLAN.



Note: Consult the application documentation when choosing an MLD version.



Querier Settings

Use this page to modify the MLD Querier configuration on each VLAN. An MLD **Snooping Querier** asks all the devices on the network what multicast traffic they want. MLD-enabled devices send MLD Join messages back to the MLD Snooping Querier. The Querier sends this information to each switch to update their **MLD Multicast Group Tables**, which are used to organize the multicast addresses that switch ports are asking for.

Use the ••• button to edit the table fields. Click the **Edit** button, under the **Action** column, to change the IGMP Snooping Status of a VLAN.

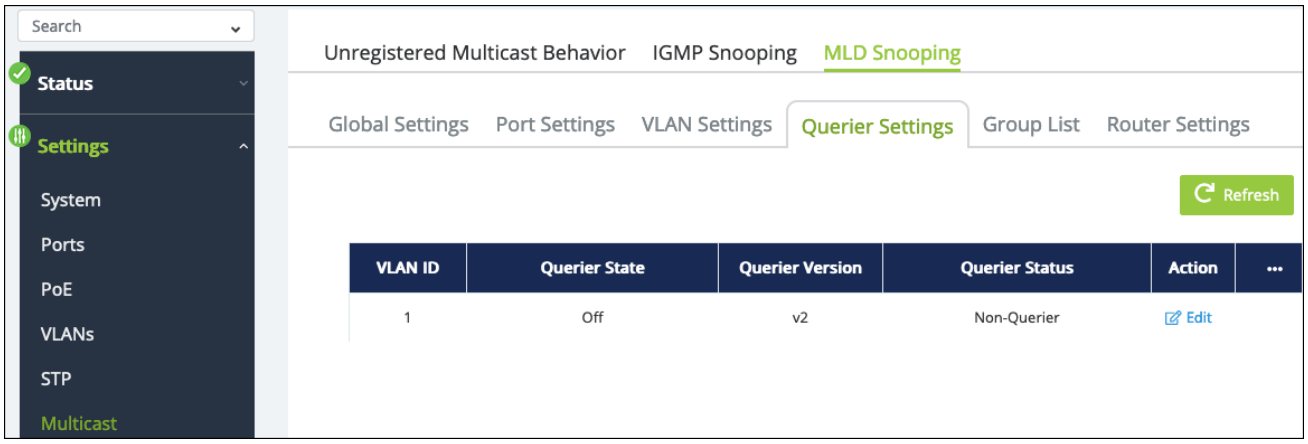
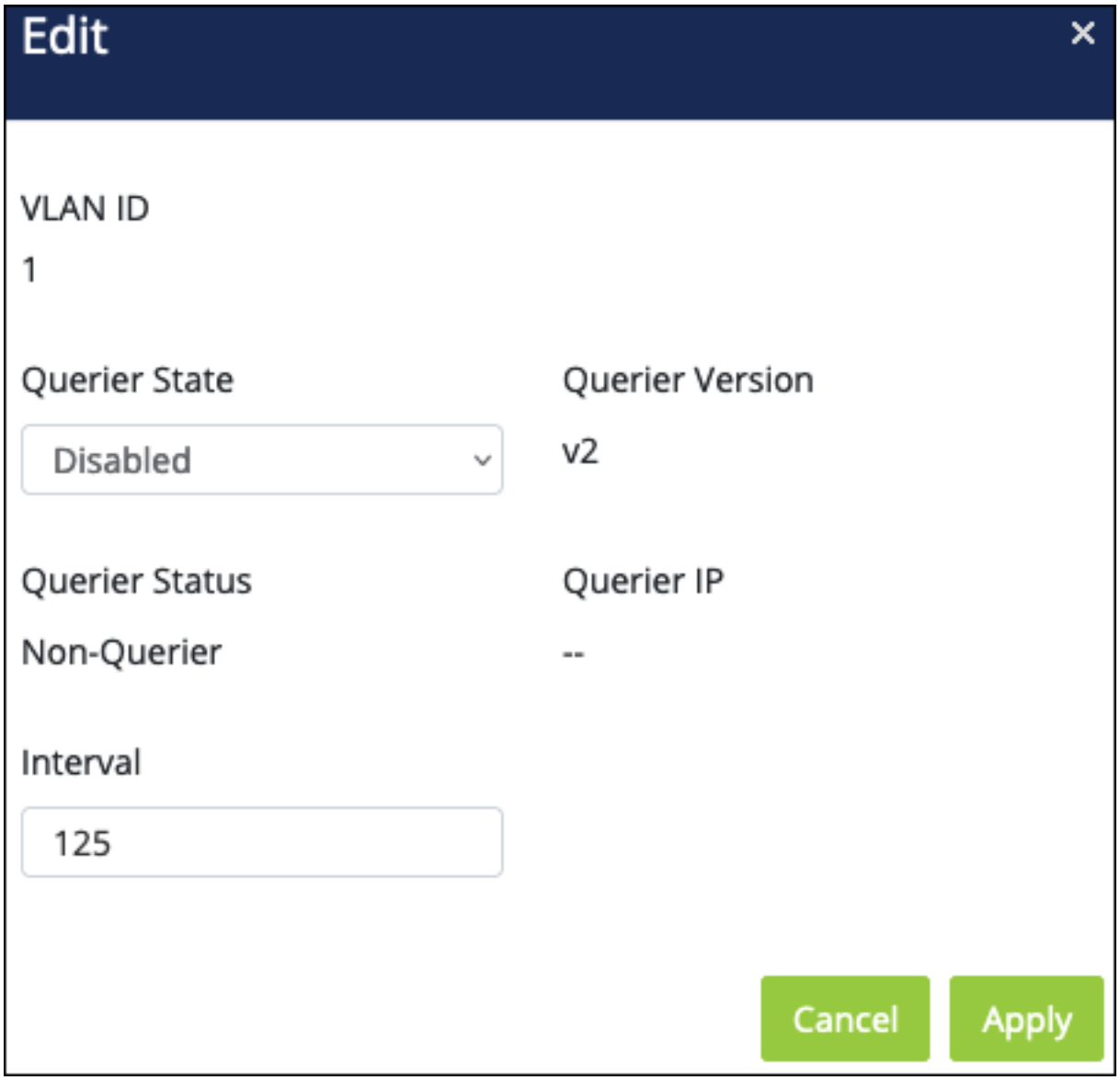


Table field descriptions:

- **VLAN ID** — The VLAN identifier used to configure MLD snooping.
- **Querier State** — Displays if MLD querier is enabled for this switch on the VLAN.
- **Querier Version** — The MLD version configured for the VLAN under the VLAN Settings tab.
  Default: 2
- **Querier Status** — Whether or not the switch is acting as the MLD querier on the VLAN.

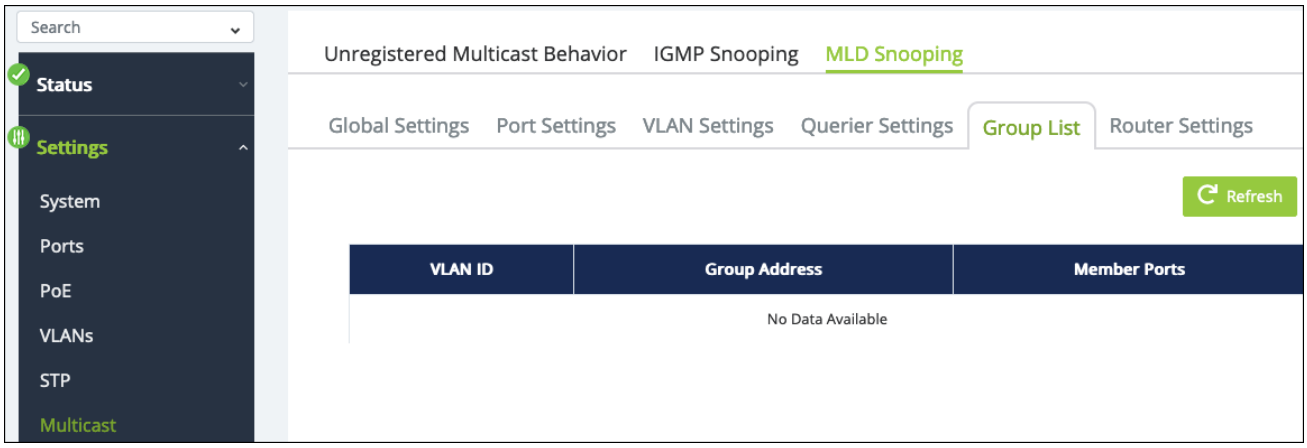


Configurable settings include:

- **Querier State** — Enable or disable this switch as an MLD querier for the VLAN.
- **Interval** — The amount of time (in seconds) that the switch sends querier messages to discover which multicast groups the hosts on the network have joined.
  Default: 125

Group List

This page displays the MLD multicast groups (**Group Address**) reporting to the switch and the ports (**Member Ports**) that are sending and receiving packets in that group.



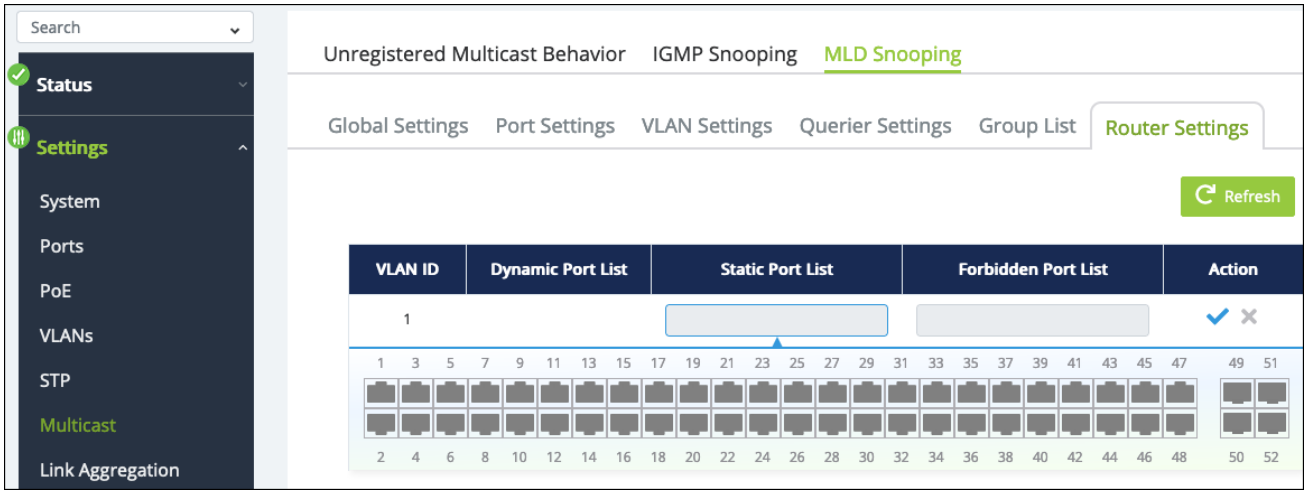
Router Settings

Use this page to configure **Multicast router ports (Mrouter ports)** for specific VLANs. Mrouter ports forward multicast messages to other members of the multicast group.

Multicast router (Mrouter) port types:

- **Dynamic** — The port learned that it should be a router port through MLD messaging on the network.
- **Static** — The port is manually configured to be a multicast router port.
- **Forbidden** — These ports are not configurable for multicast routing.

Click the **Edit** button, under the Actions column to add ports to the Static and Forbidden port lists. Click the **checkmark** button to save those changes.



Link Aggregation

Link Aggregation (Port Trunking) uses multiple ports in parallel to increase the link speed between two switches, increasing redundancy for higher availability.

LAG

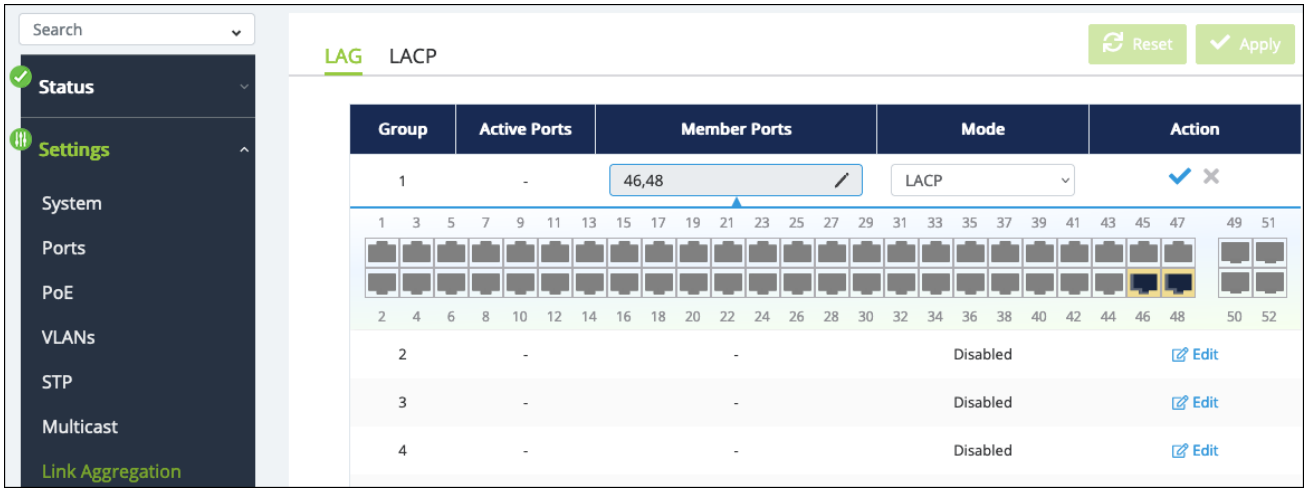
Use this page to create a **Link Aggregation Group (LAG)**.

This switch supports two modes for link aggregation:

- **Link Aggregation Control Protocol (LACP)**, which can create LAGs on the switch you're connecting to if it also supports LACP.
- **Static**, which requires LAG to be created on both switches.

Click the **Edit** button, under the Action column, to create or edit a LAG. Click the **checkmark button** to save changes.

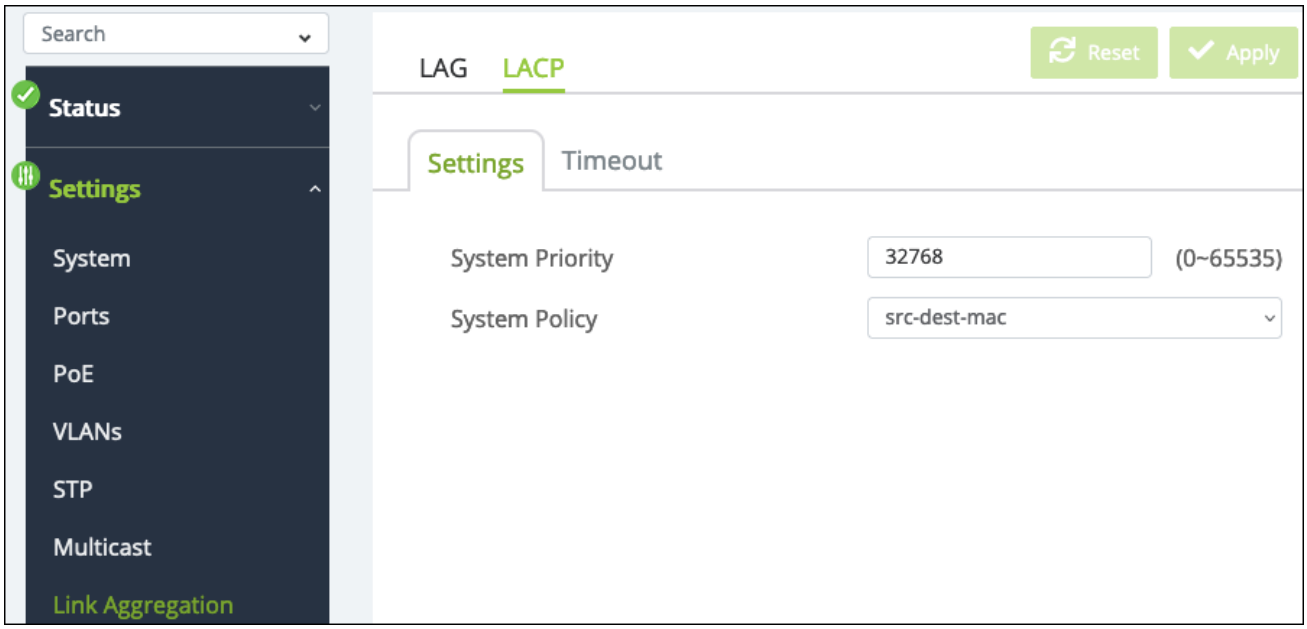
Note: Ports cannot be a member of multiple LAGs.



LACP

Use this page to configure the Link Aggregation Control Protocol for the switch.

Settings



Configurable settings include:

- **System Priority** — The priority value the switch takes in determining which switch informs others of a LAG creation. The lower the number the higher the priority level. If multiple switches share the same priority number, the switch with a small MAC

address takes priority.

Defaut: 32768

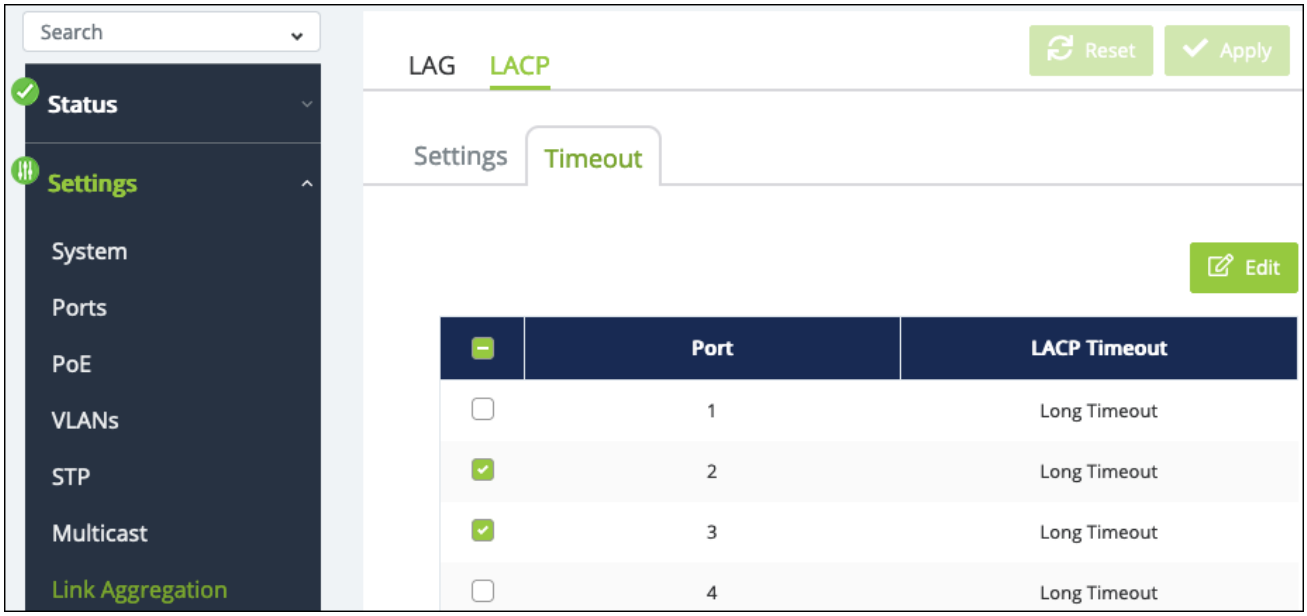
- **System Policy** — Select a load balancing policy. Options are:
  - **src-mac** — Calculated by source MAC addresses.
  - **dest-mac** — Calculated by destination MAC addresses.
  - **src-dest-mac** — Calculated by the Exclusive-Or result of destination MAC addresses.
  - **src-ip** — Calculated by source IP addresses.
  - **dest-ip** — Calculated by destination IP addresses.
  - **src-dest-ip** — Calculated by the Exclusive-Or result of destination IP addresses.
  - **dest-l4-port** — Calculated by the destination TCP port and IP address.
  - **src-l4-port** — Calculated by the source TCP port and IP address.

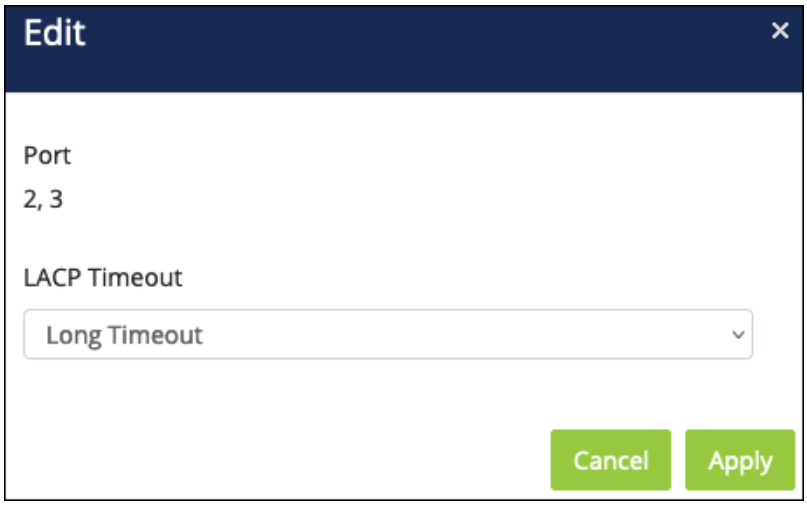
Default: src-dst-mac

Timeout

Use this page to set the LACP Timeout for each port. Select a port(s), then click the **Edit** button to change the timeout settings.

The default **Long Timeout** sends LACP control packets every 30 seconds. **Short Timeout** sends LACP control packets every second.





Access Management

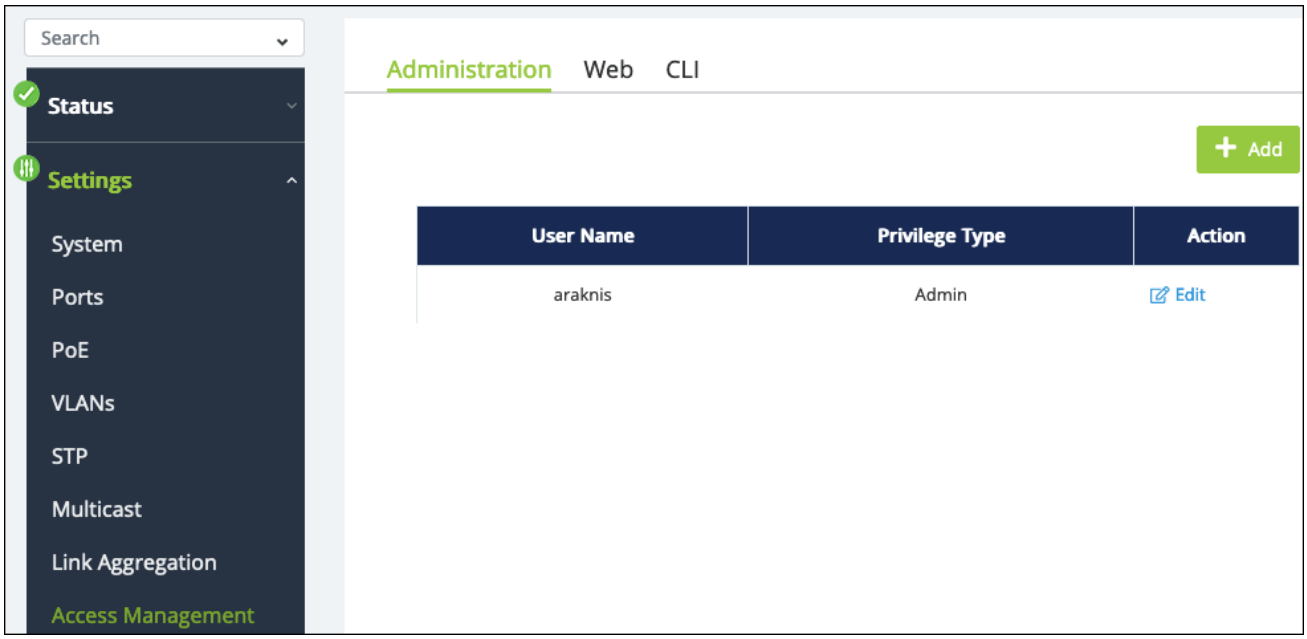
This switch allows you to configure access management settings on the Administration, Web, and CLI (Command Line Interface) levels.

Administration

Use this page to **Add**, **Edit**, and **Delete** users. The available user privileges are:

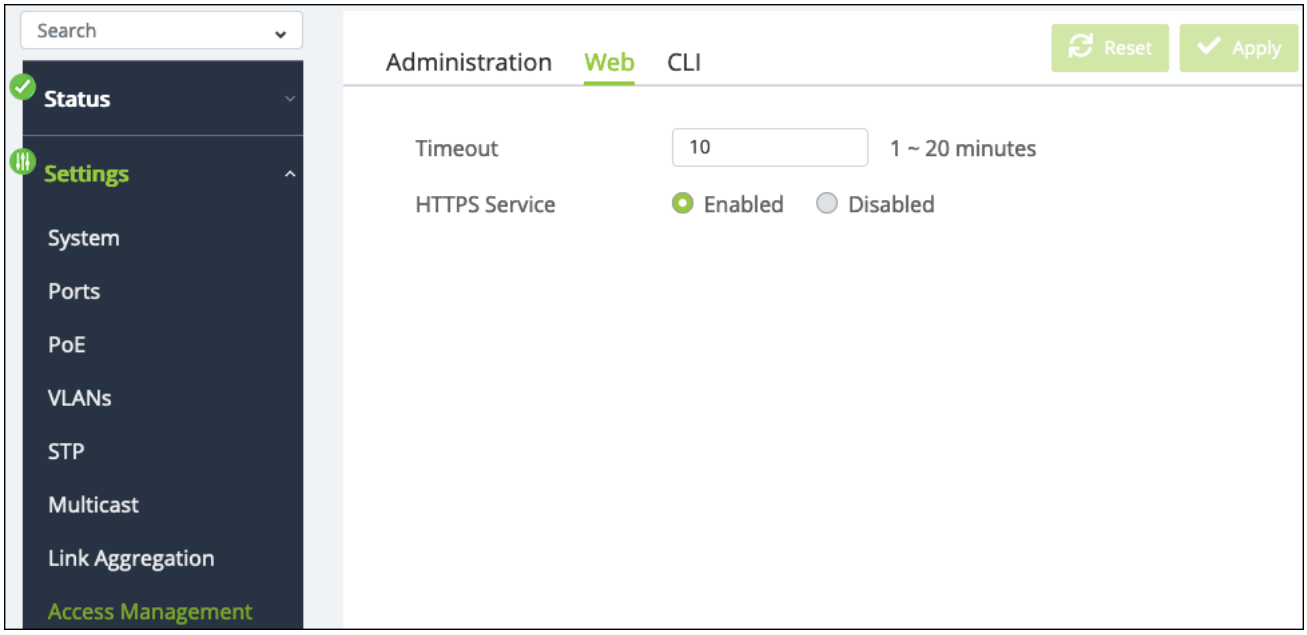
- **Admin** — Has full access to the switch.
- **User** — Allows access to the switch, but removes the ability to make changes.

Note: The original admin username cannot be changed from “araknis” and it cannot be deleted.



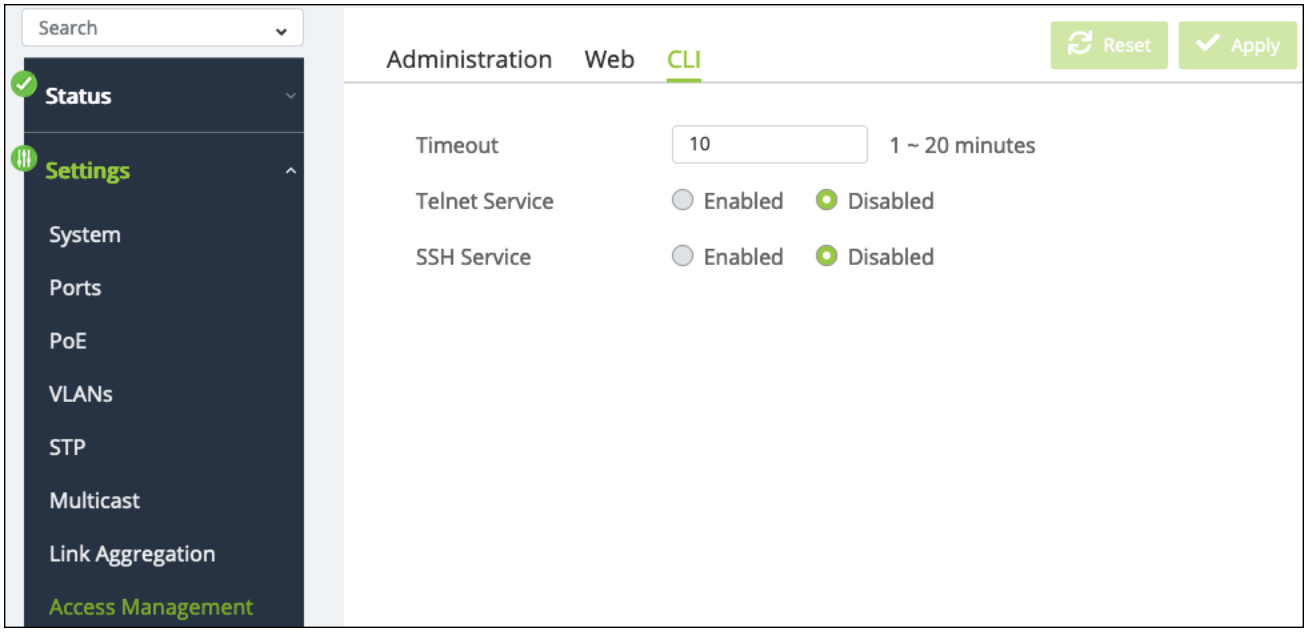
Web

Use this page to enable or disable the **HTTPS service** and **Timeout**.



CLI

Use this page to enable or disable the **Telnet** and **SSH** Service and alter the **Timeout** settings.

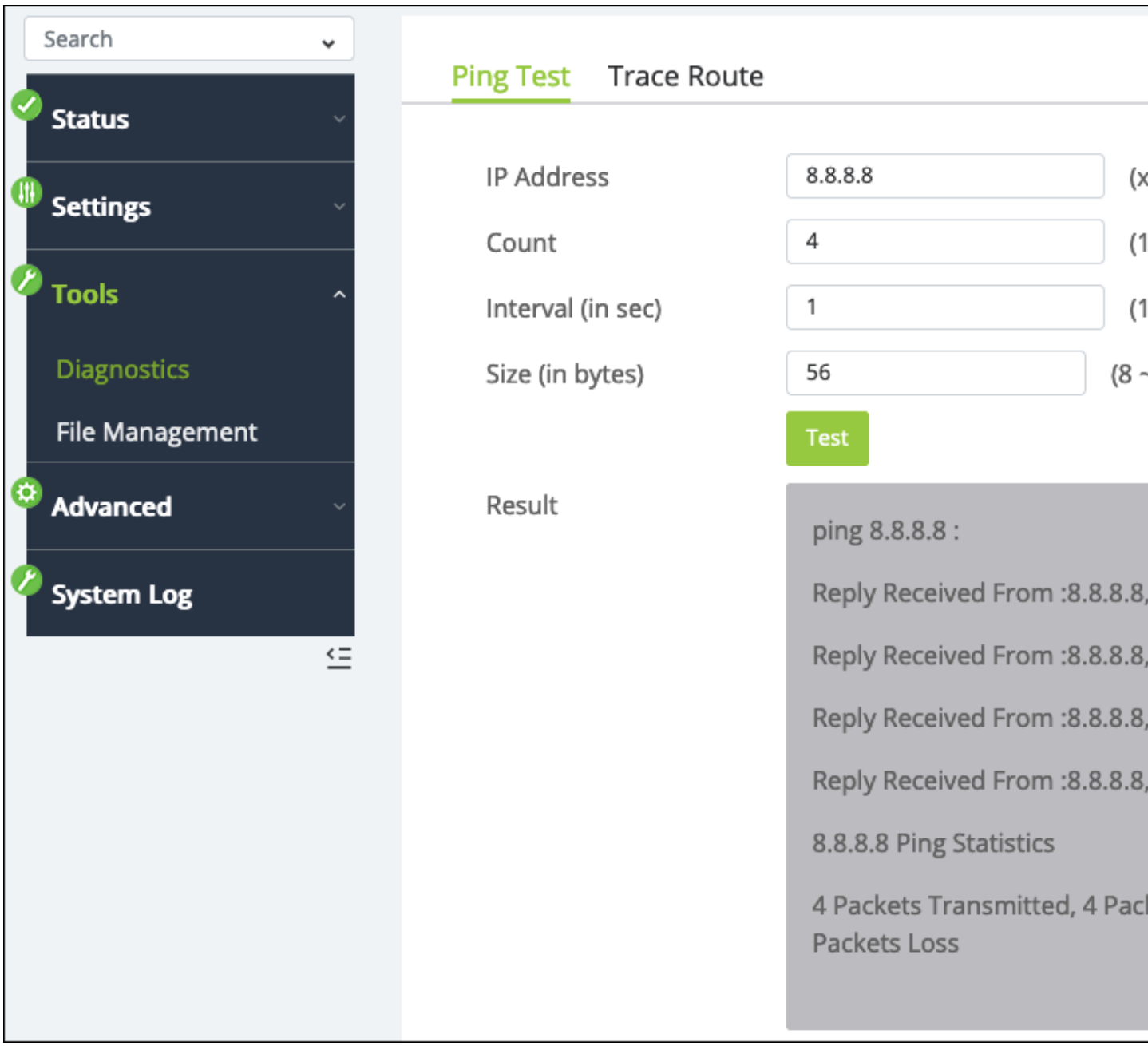


Diagnostics

Ping Test

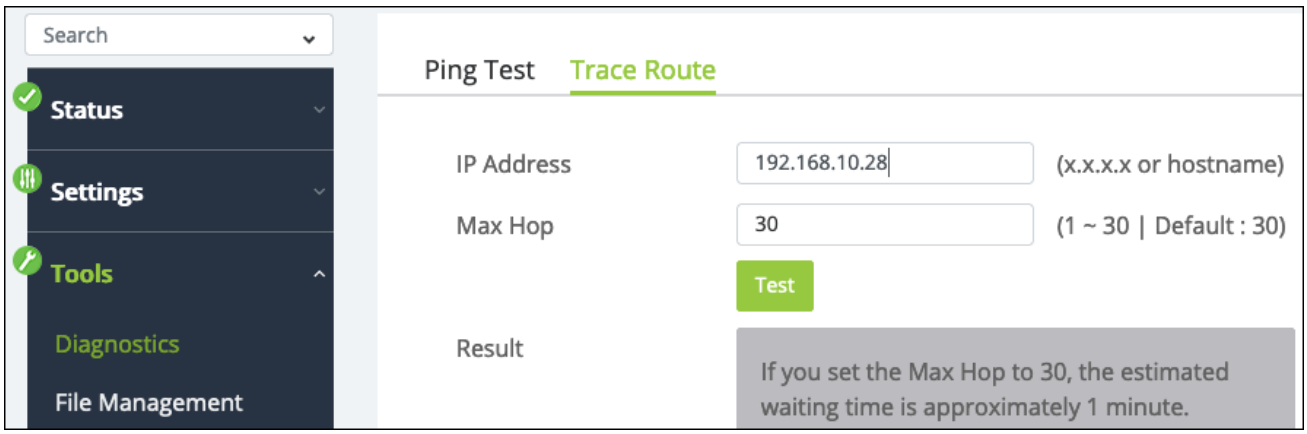
Use a ping test to measure the amount of time it takes to reach an address on the local network or the internet. You can enter the IP address or the hostname, such as www.wikipedia.com.

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



Trace Route

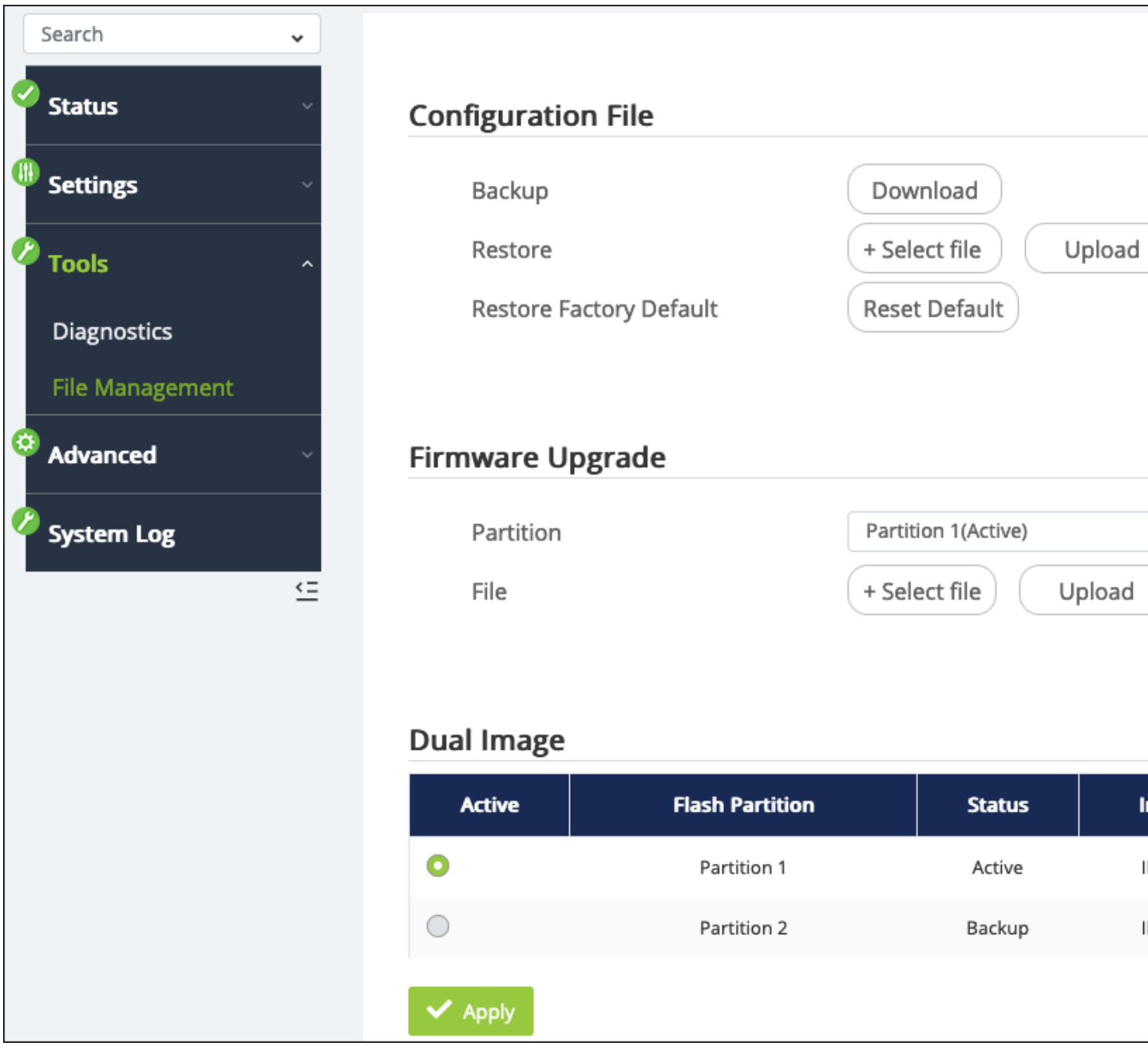
Use a traceroute to diagnose network interruptions between the switch and an address on the local network or the internet. You can enter an IP address or a hostname, such as www.youtube.com.



File Management

Use this to download or upload a configuration file, restore factory defaults, and perform firmware upgrades.

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.



Note: You can use either partition to update the switch. OvrC always updates the inactive partition.

Neighbors

MAC Address Table

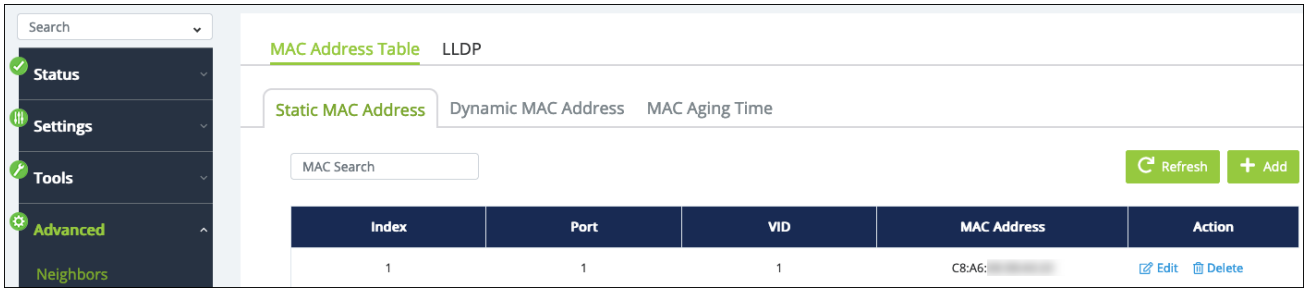
Use these tables to see which MAC addresses are connected to the switch and add static MAC address entries.

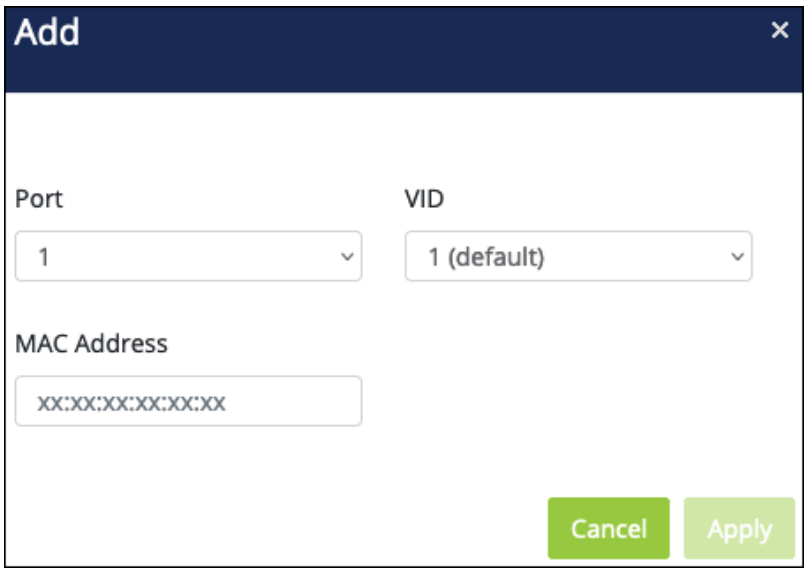
Static MAC Address

Static MAC address entries speed up the recovery time for critical devices after a restart. They can also be used to recognize a virtual machine on a port.

Click the **Add** button to create a static MAC address. Use the **Edit** and **Delete** buttons in the **Action** column to modify the table.

Pro Tip: Use the Dynamic MAC Address table to make discovered MAC addresses static to avoid typing mistakes.

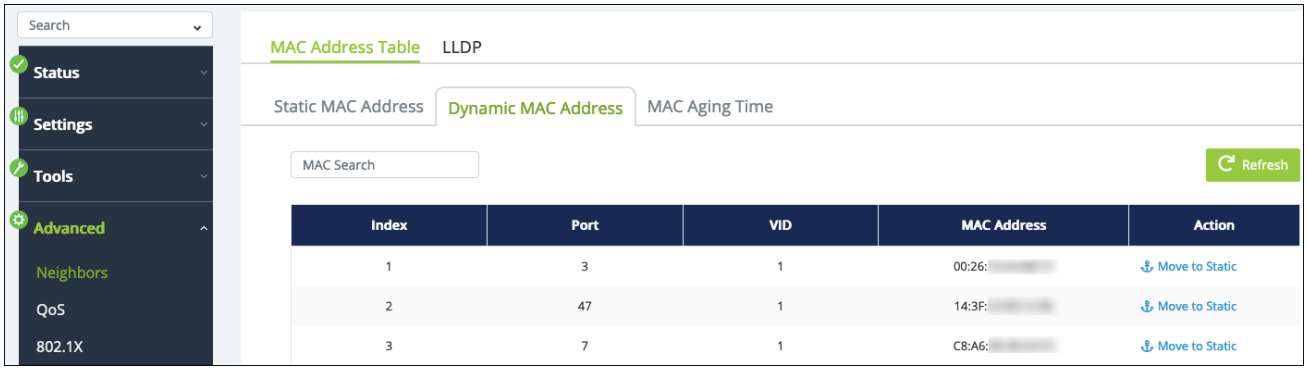




Dynamic MAC Address

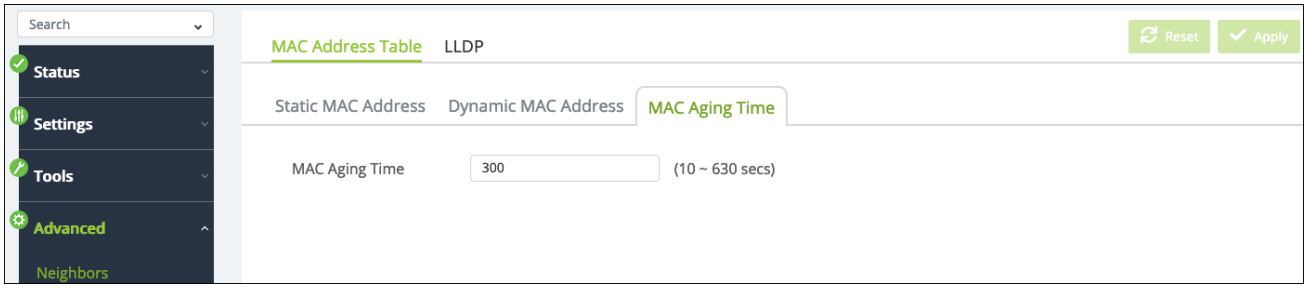
The switch discovers dynamic MAC addresses. This table shows which port the MAC address is connected to and the VLAN ID (VID) it was discovered on.

Use the **Move to Static** button under the **Actions** column to statically assign the address.



MAC Aging Time

Use this page to adjust the MAC Aging Time. This is the amount of time the switch waits to remove a MAC address from the Dynamic MAC address table after it stops sending packets to the switch. The default is 300 seconds.

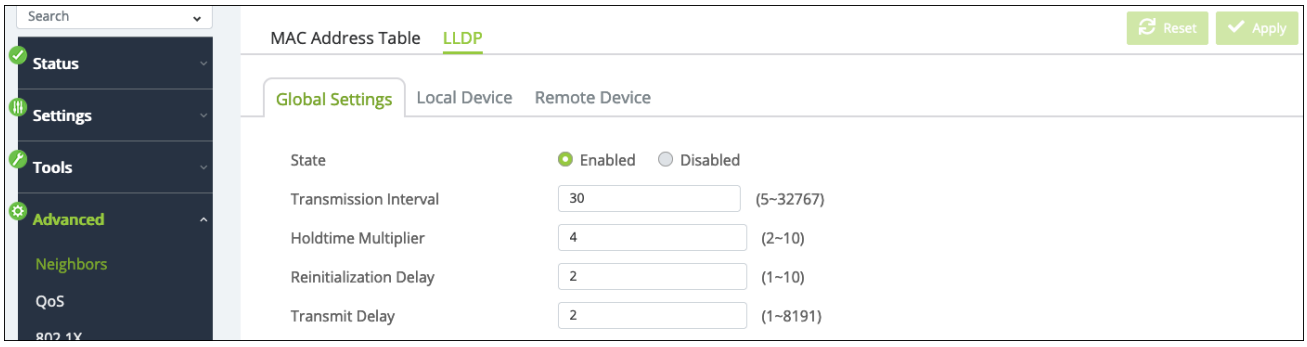


LLDP

Link Layer Discovery Protocol (LLDP) is a generic protocol used to advertise the device's capabilities to other devices on the network.

Global Settings

Use this page to enable and configure LLDP.



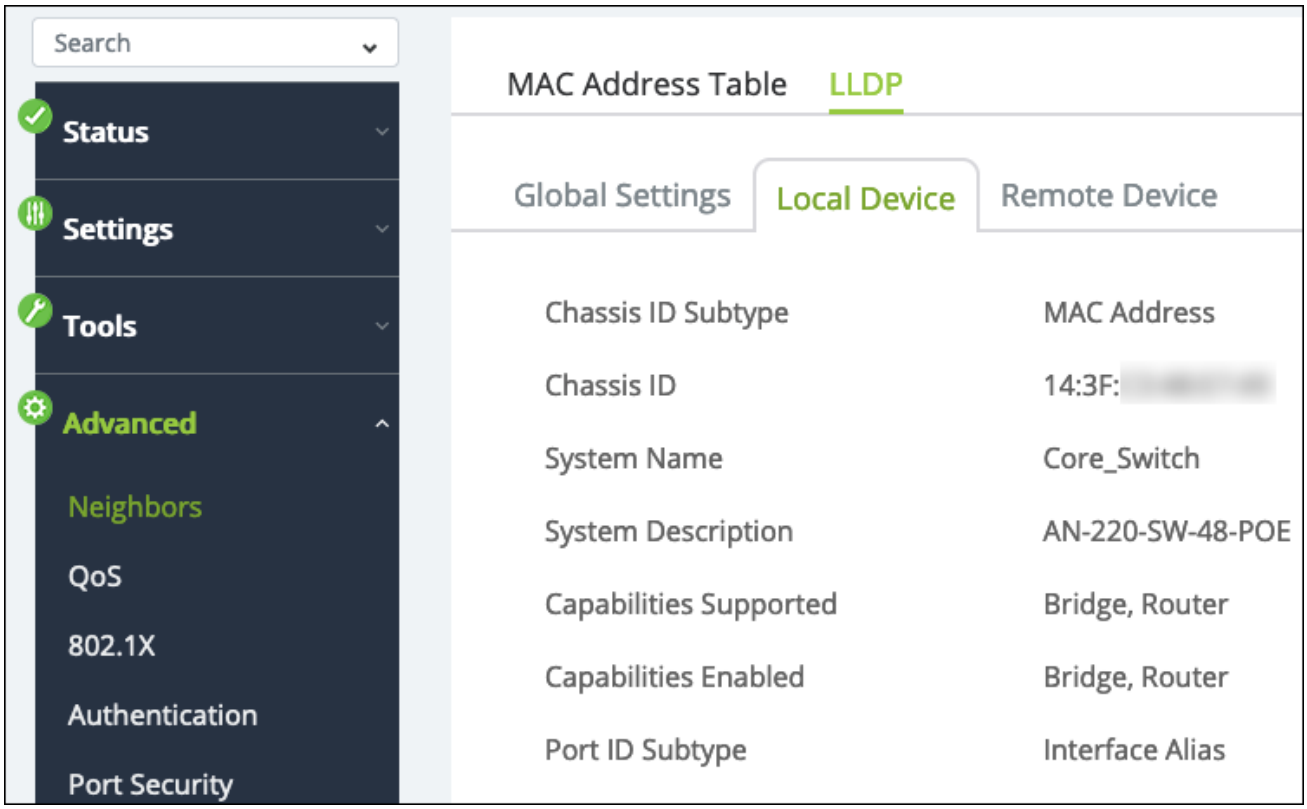
Configurable settings include:

- **Transmission Interval (Seconds)** — The number of seconds between LLDP transmissions.
  Default: 30
- **Holdtime 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.
  Default: 4

- **Reinitialization Delay** — The number of seconds to wait before attempting to reinitialize LLDP on a port after the port's LLDP operating mode changes.
  Default: 2
- **Transmit Delay** — The amount of time of time to wait before sending updated LLDP information after a configuration change.
  Default: 2

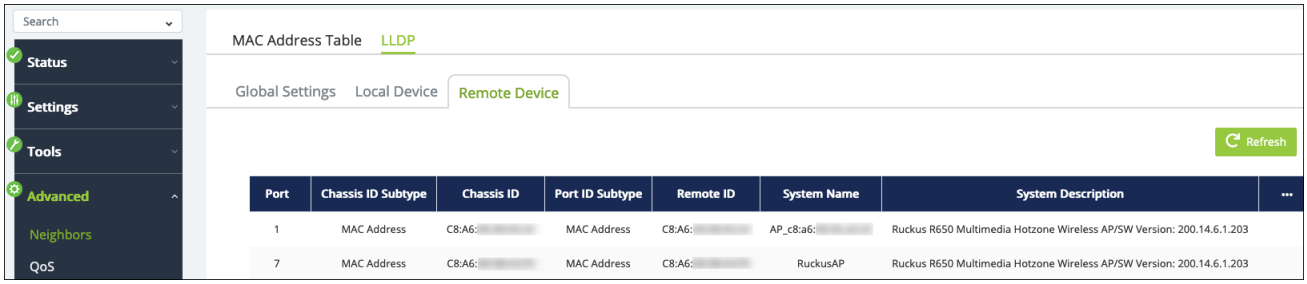
Local Device

This page displays the LLDP information of the switch.



Remote Device

This page displays a table with LLDP information the switch has collected from local network hosts. Use the ••• button to edit the table fields.

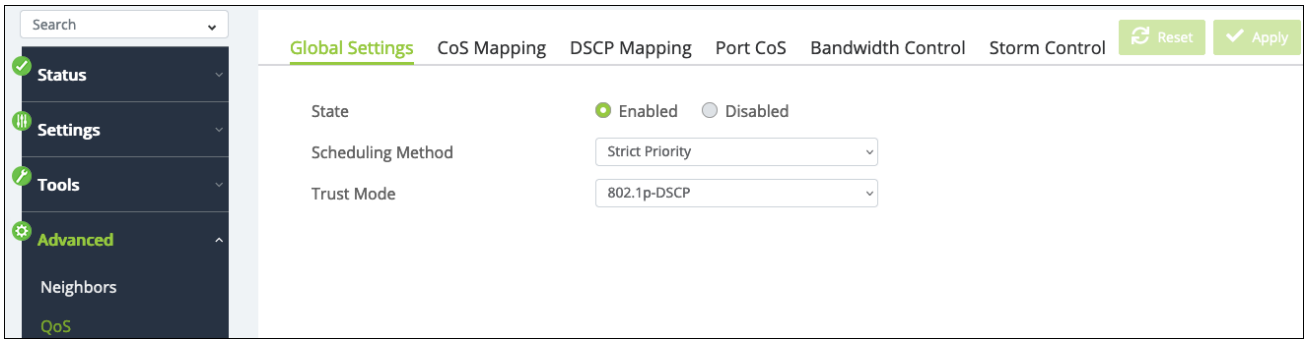


QoS

Quality of Service (QoS) organizes and prioritizes packet flow and bandwidth use on the LAN based on traffic type, source, or destination to help guarantee network performance for critical services.

Global Settings

Use this page to enable and configure QoS.



Configurable settings include:

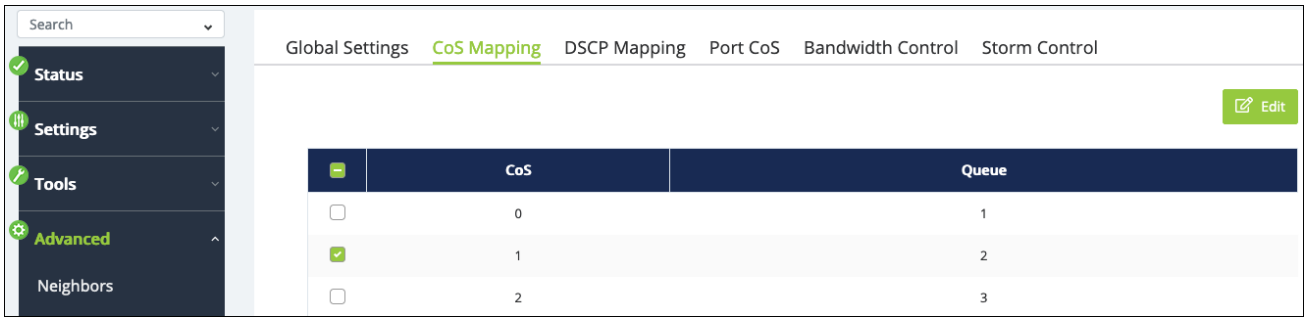
- **State** — Enabled or disabled.
- **Scheduling Method** — options include:
  - **Strict Priority** — (Default)Traffic is scheduled specifically based on queue priority.
  - **WRR** — Use the Weighted Round Robin algorithm to prioritize traffic queues.
- **Trust Mode** — options include:

- **802.1p - DSCP** — (Default)Traffic is prioritized based on both 802.1p and DSCP priority tags.
- **DSCP** — Traffic is prioritized based on its DSCP priority tag.
- **802.1p** — Traffic is prioritized based on its 802.1p priority tag.

CoS Mapping

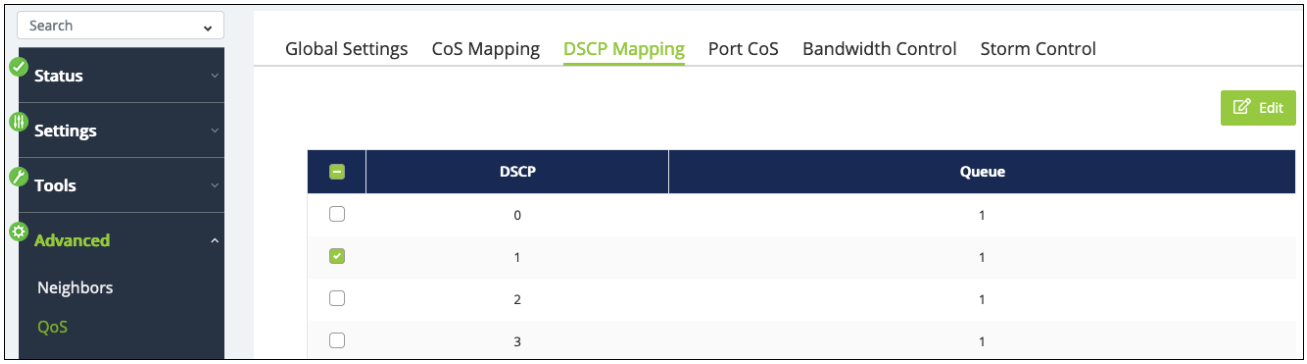
Class of Service (CoS) allows you to directly configure certain aspects of switch queueing, allowing you to configure Quality of Service (QoS) behavior when the complexities of DiffServ aren't required. The priority of a packet arriving at an interface can be steered to the appropriate outbound CoS queue through a mapping table. The CoS queue characteristics, such as minimum guaranteed bandwidth and transmission rate shaping, are configurable at the queue or port level.

Use this page to assign traffic of different CoS priority levels to the desired queue. Select a COS value(s), then click the Edit button to make changes.



DSCP Mapping

Use this page to assign DSCP values to a Queue. Select a **DSCP** value(s), then click the **Edit** button to make changes.

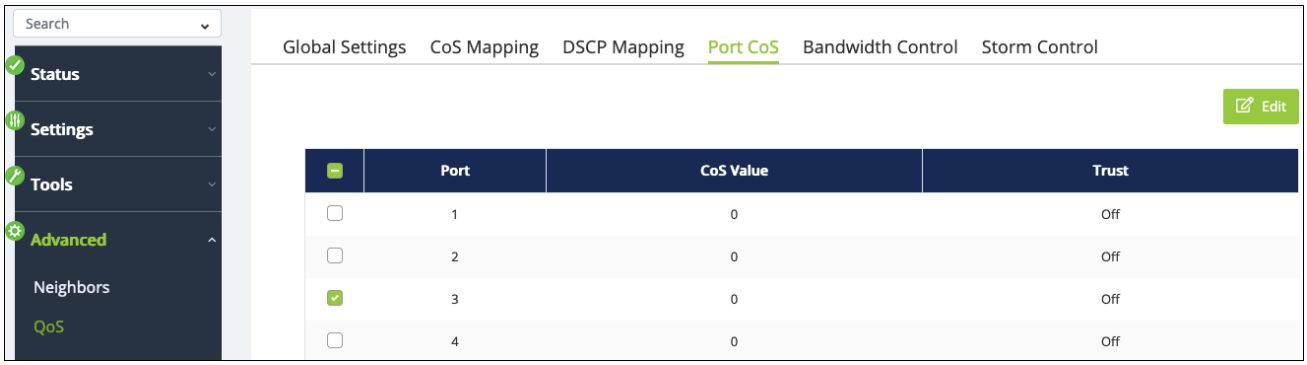


Port CoS

Use this page to assign a **CoS Value** to ports and turn **Trust** On or Off. Configure the **Trust Mode** on the **QoS** > **Global Settings** page.

On tells the switch to trust the QoS tag from the connected device. **Off** does not trust the QoS tag of the connected device and re-tags the traffic.

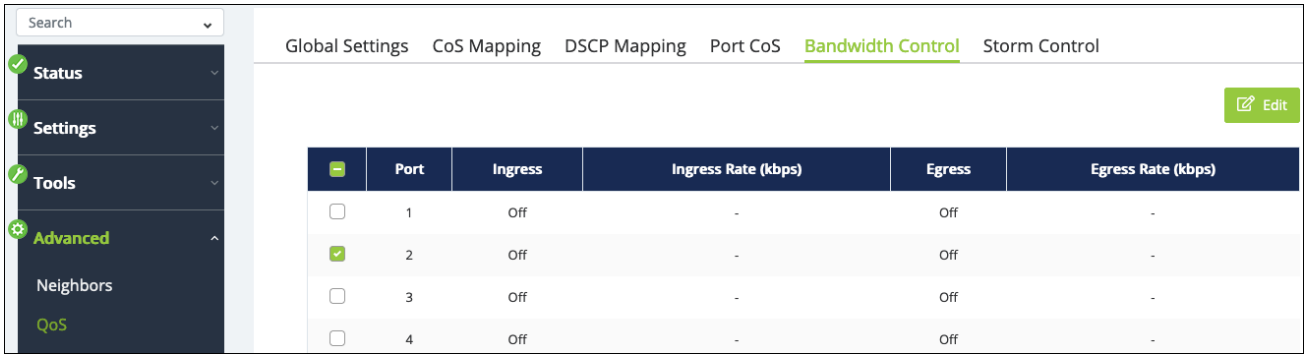
Select a **Port(**s), then click the **Edit** button to make changes.

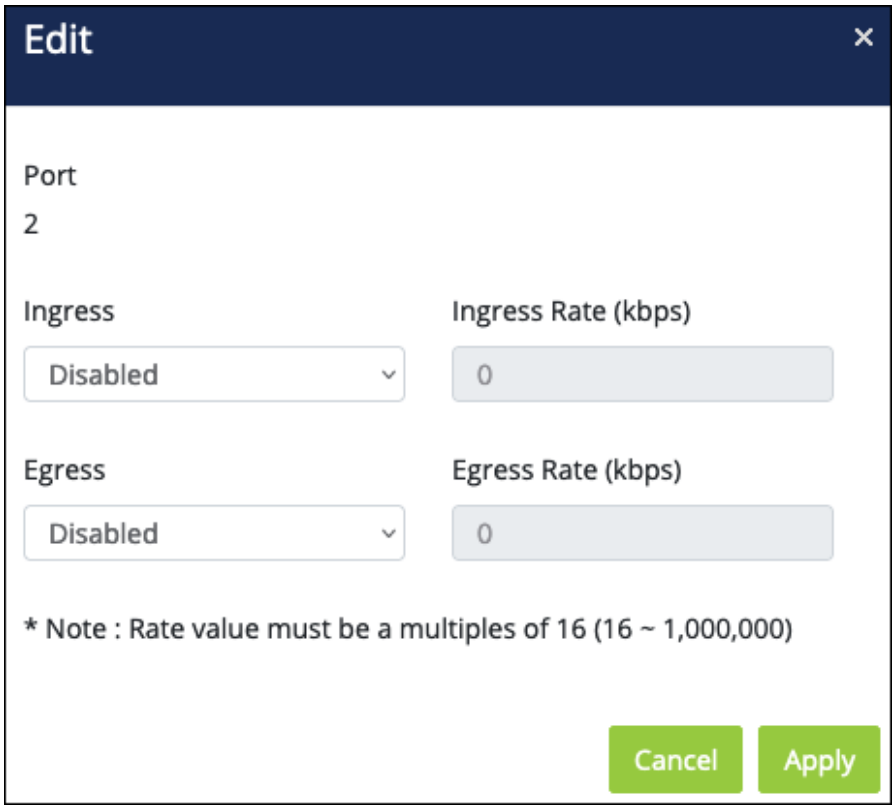


Bandwidth Control

Configure **Bandwidth Control** to limit the amount of traffic allowed to pass into or out of the ports.

Select a **Port(**s), then click the **Edit** button to make changes.





Configurable settings include:

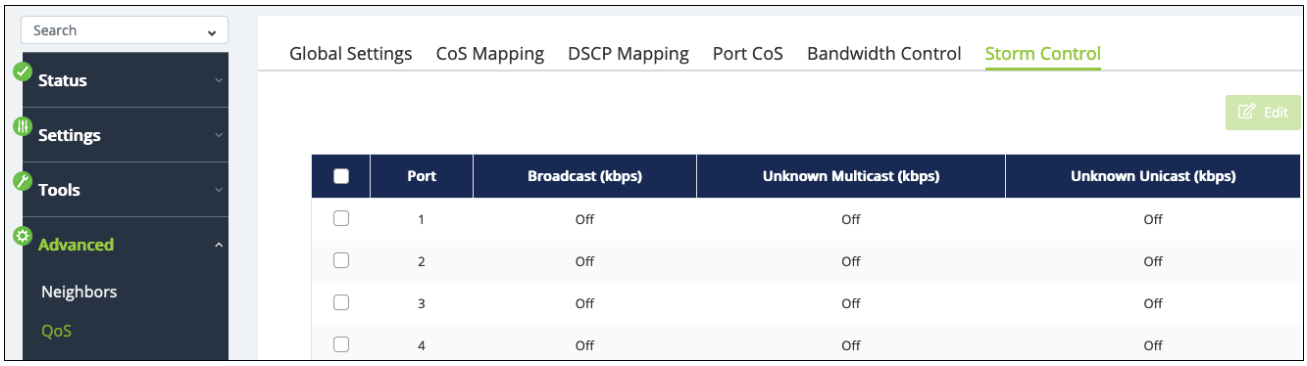
- **Ingress and Ingress Rate (kbps)** — Enable to limit the data rate of incoming traffic.
- **Egress and Egress Rate (kbps)** — Enable to limit the data rate of outgoing traffic.

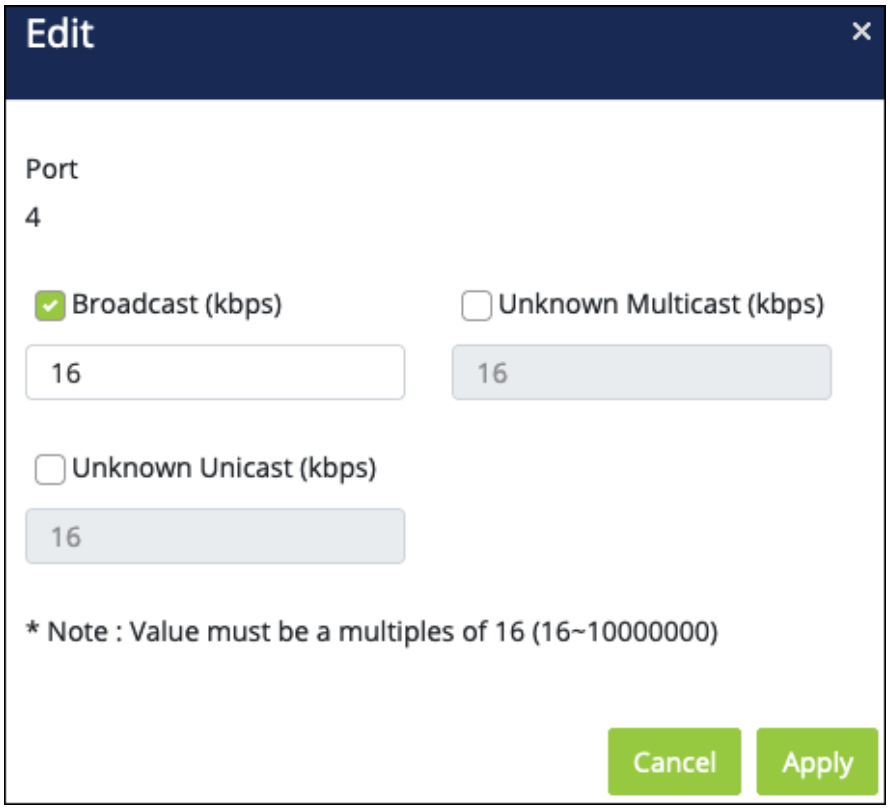
Note: Rate values must be a multiple of 16 between 16 and 1,000,000.

Storm Control

Use this page to configure **Storm Control** to limit the amount of broadcast, unknown multicast, and unknown unicast packets coming into ports on the switch. Excessive frames are discarded when the specified limit is passed.

Select a **Port(**s), then click the **Edit** button to make changes.





Configurable settings include:

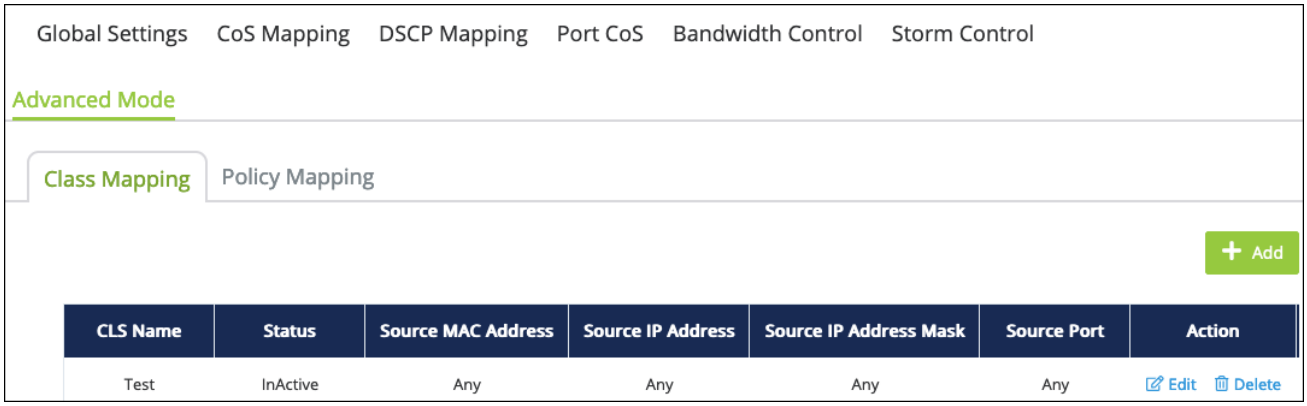
- **Broadcast (kbps)** — Check the box to enable Broadcast storm control, then enter the maximum broadcast traffic rate.
- **Unknown Multicast (kbps)** — Check the box to enable Multicast storm control, then enter the maximum multicast traffic rate.
- **Unknown Unicast (kbps)** — Check the box to enable Unicast storm control, then enter the maximum unicast traffic rate.
- **Note:** Rate values must be a multiple of 16 between 16 and 1,000,000.

Advanced Mode (420 only)

Use these tabs to add more criteria to match and apply QoS to incoming traffic.

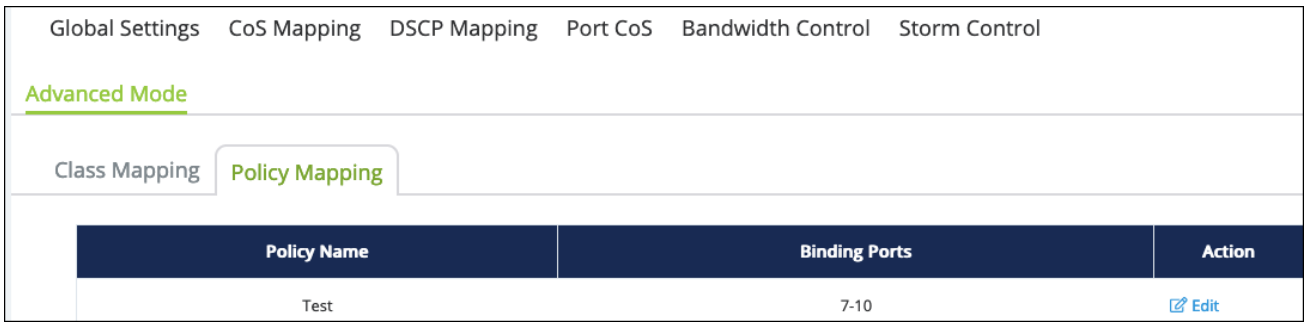
Class Mapping

Use this tab to Add, Edit, or Delete, Class Mapping for QoS.



Policy Mapping

Use this page to assign Class Mapping policies to switchports. Use commas to separate multiple ports or a dash to enter a port range.

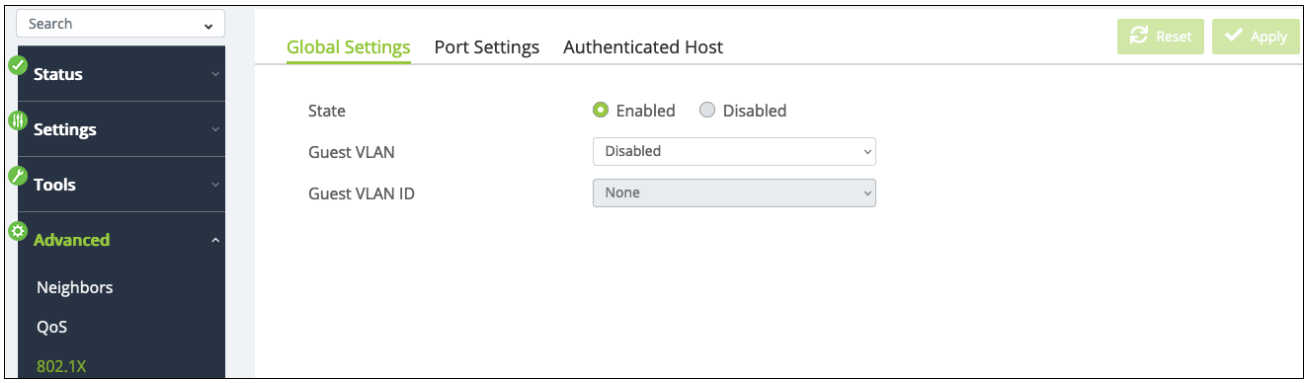


802.1X

802.1x allows port-based client authentication with the use of a RADIUS server.

Global Settings

Use this page to enable and configure 802.1x.



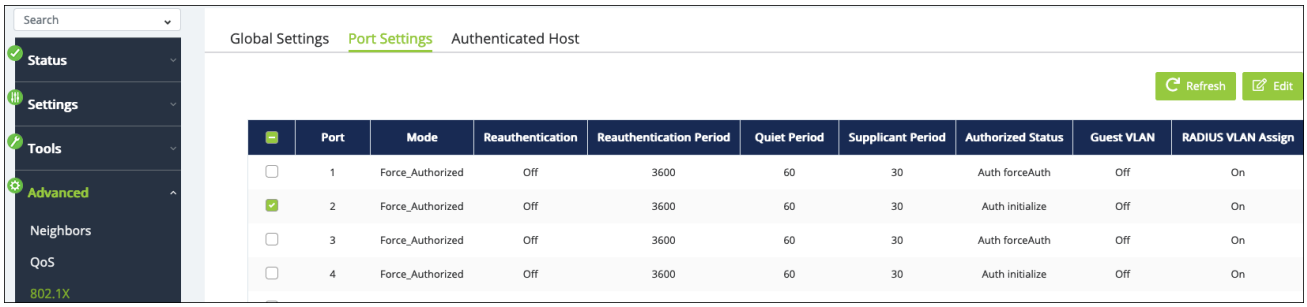
Configurable settings include:

- **State** — Enabled or disabled.
- **Guest VLAN** — Enable or disable guest VLAN use for 802.1x. When enabled, all unauthorized clients will be connected to the VLAN.
- **Guest VLAN ID** — Select a VLAN ID to use for the Guest VLAN, if enabled.

Port Settings

Use this page to view and edit the 802.1x configuration for each port.

Select a **Port(**s), then click the **Edit** button to make changes.



Configurable settings include:

- **Mode** — Options include:
  - **Auto** — The port only allows packets used for authentication and network discovery until the client is authenticated, then allows uninterrupted traffic.
  - **Force unAuthorized** — The port remains unauthorized and ignores all attempts to authenticate a client.
  - **Force Authorized** — (Default) The port behaves as if an authenticated client is connected.
- **Reauthentication** — When enabled, a client that fails to authenticate cannot try again until the next period based on the reauthentication period.
- **Reauthentication Period** — The amount of time, in seconds, the switch reauthenticates users to verify that only authorized users can stay online. Default: 3600
- **Quiet Period** — The amount of time, in seconds, that the switch refuses authentication requests from a client that previously failed authentication. Default: 60
- **Authorized Status** — Displays the current authorized status of the port.

- **Supplicant Period** — The amount of time, in seconds, the switch waits to receive a response from a client before sending another request.
  Default: 30
- **Guest VLAN** — Enable or disable the guest VLAN on the port.
  Default: Off
- **RADIUS VLAN Assign** — Also known as Dynamic VLAN Assignment or VLAN Steering. This is the RADIUS server authenticating the user also assigns the user a VLAN.
  Default: On

Authenticated Host

This page displays hosts that have connected and authenticated using 802.1x.

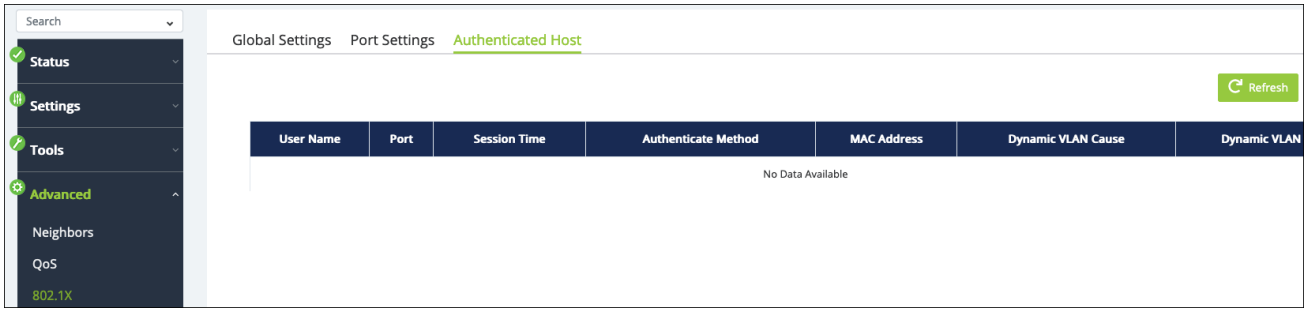
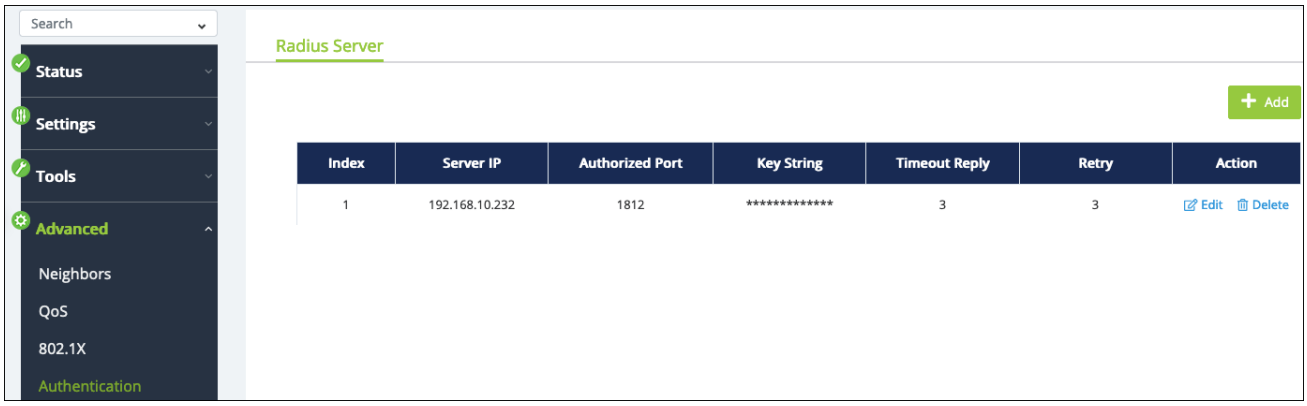


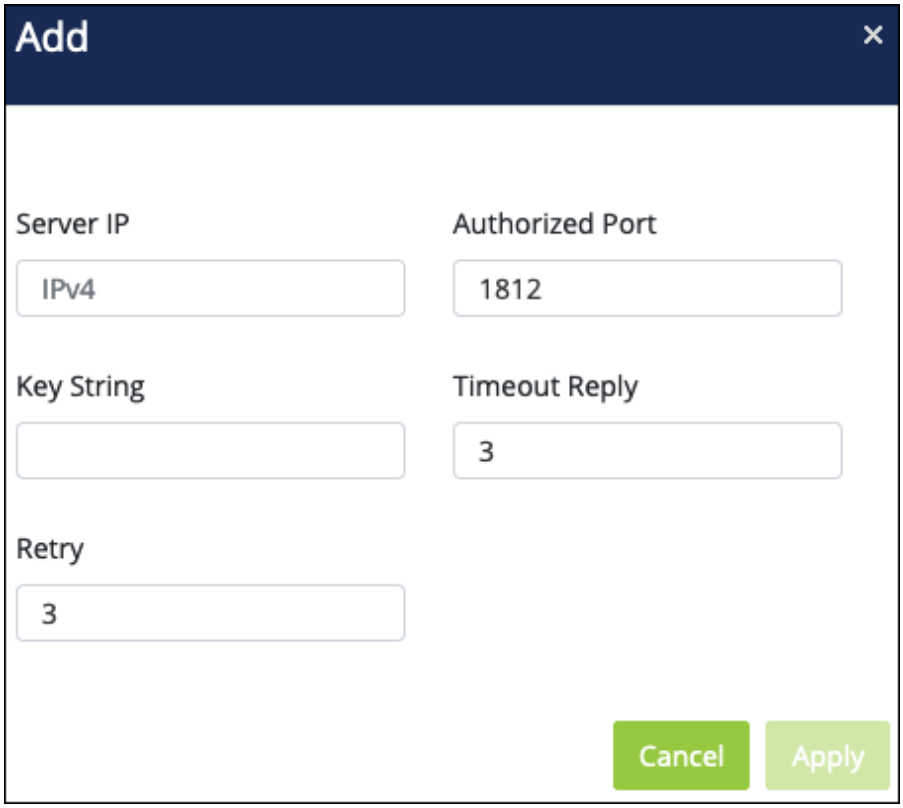
Table field descriptions:

- **User Name** — The name of the user configured on the RADIUS server.
- **Port** — The switchport the user is authenticated on.
- **Session Time** — The amount of time since the user was authenticated for the current session.
- **Authenticate Mode** — The method used to authenticate the user.
- **MAC Address** — The MAC address of the connected client port.
- **Dynamic VLAN Cause** — Displays the method being used for host authentication.
- **Dynamic VLAN** — Displays the VLAN the host has been assigned.

Authentication

Use this page to **Add**, **Edit**, or **Delete** a RADIUS server. The **Remote Authentication Dial-In User Service (RADIUS)** protocol provides central management for users connecting for network services.





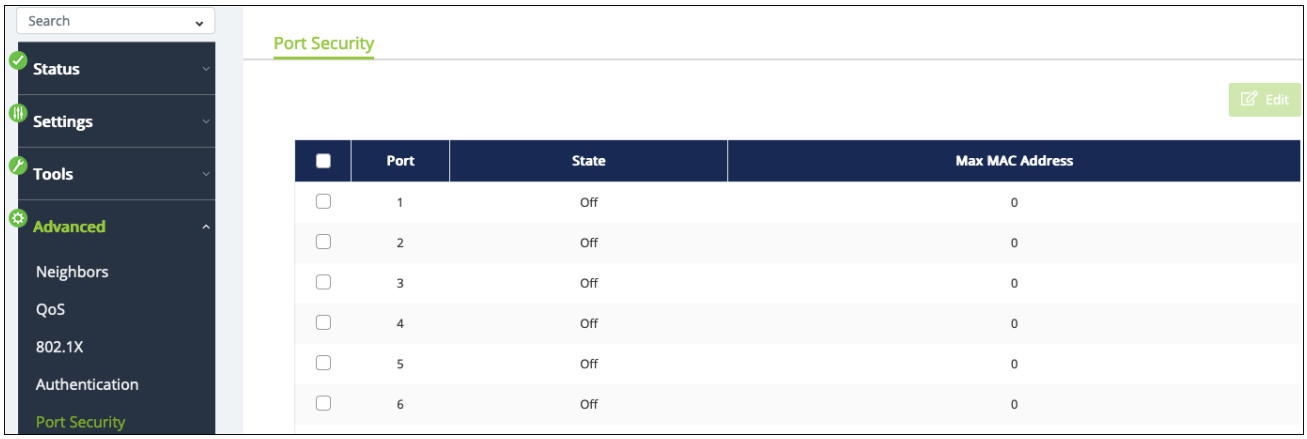
Configurable settings include:

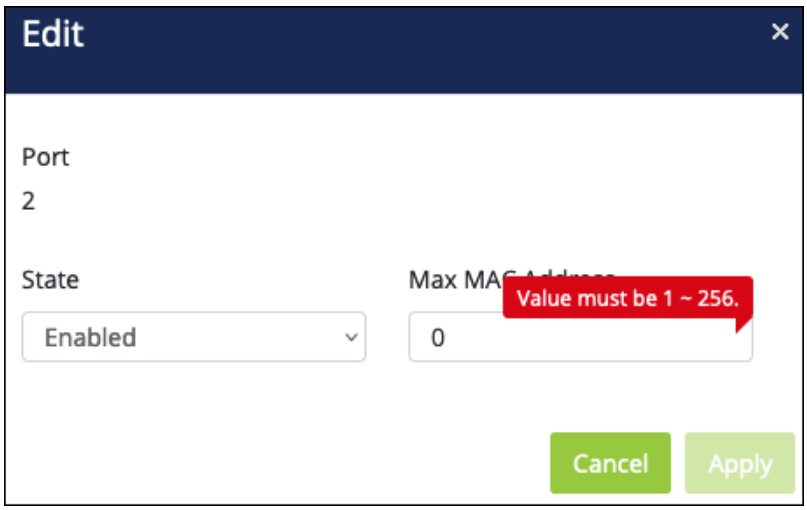
- **Server IP** — The IPv4 address of the RADIUS server.
- **Authorized Port** — The port to communicate with the RADIUS server.
- **Key String** — Enter the authentication key required to connect with the RADIUS server.
- **Timeout Reply** — The number of seconds the switch waits for a reply before it attempts to connect again.
  Default: 3
- **Retry** — The number of attempts the switch makes to connect to the RADIUS server before it stops.
  Default: 3

Port Security

Use this page to limit the number of connected devices on a given port by limiting the total number of MAC addresses a port can identify.

Select a **Port**(s), then click the **Edit** button to set limitations.





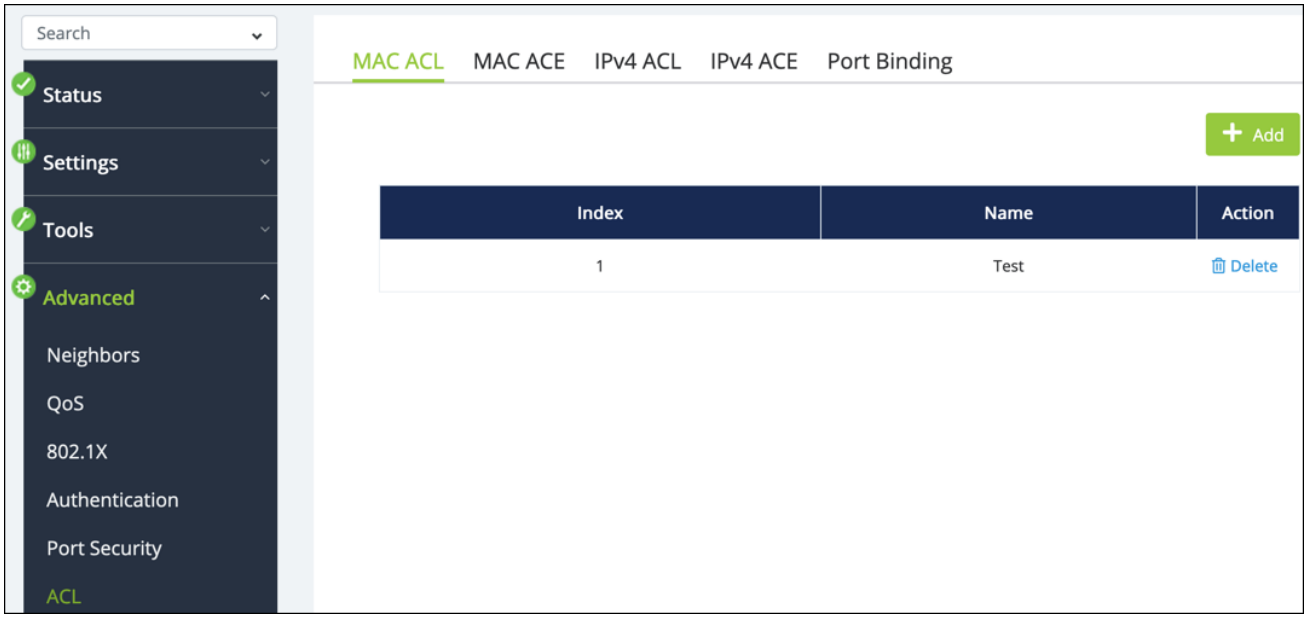
Note: The Max MAC address value must be between 1-256.

ACL

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.

MAC ACL

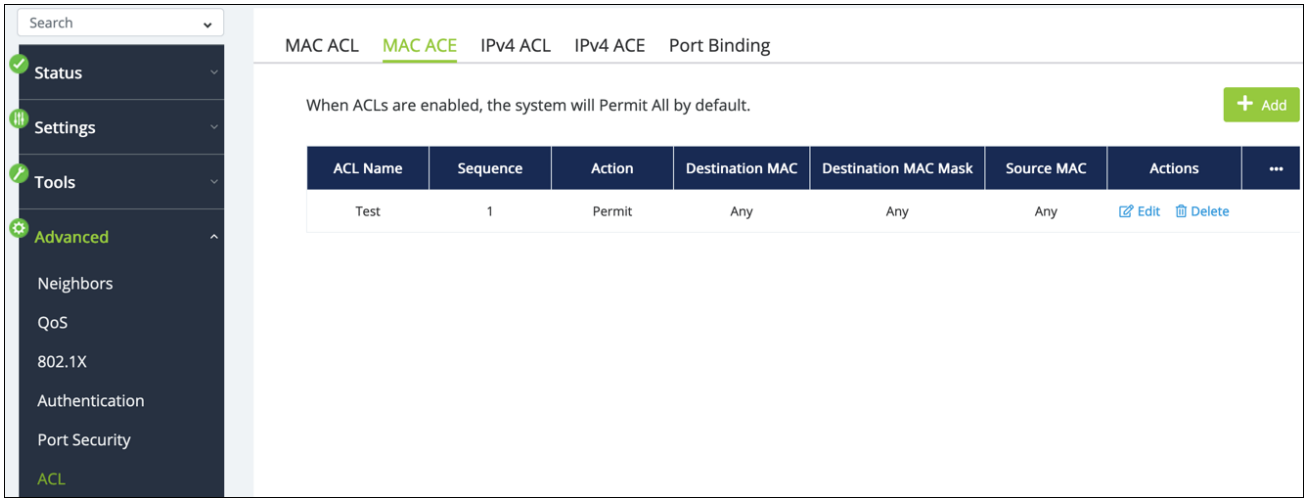
Use this page to add ACLs to the switch configuration. Click the **Add** button to create a new ACL.

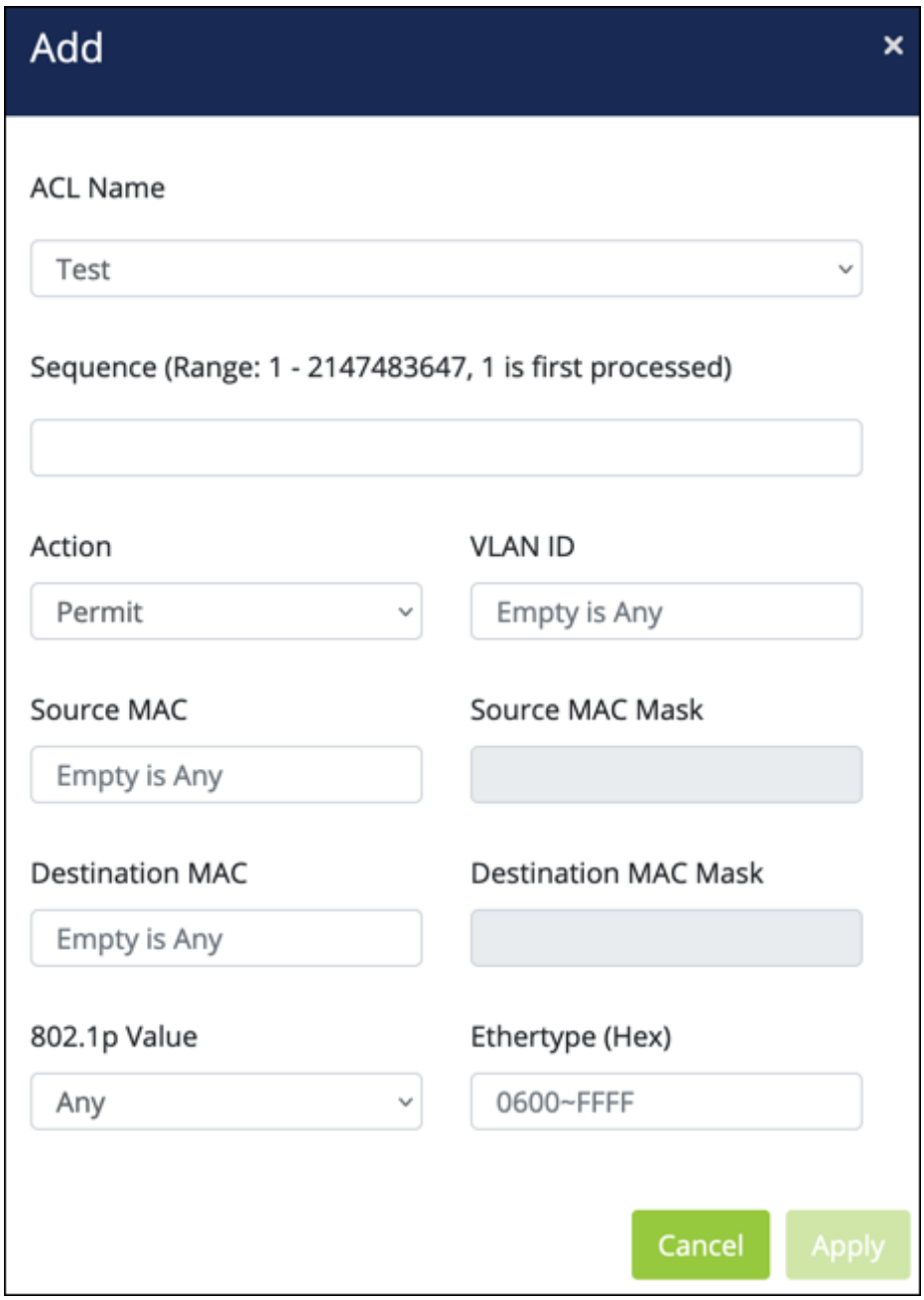


MAC ACE

Use this page to define **Access Control Entries (ACEs)** associated with each MAC ACL list. Use the ••• button to edit the table fields.

Click the **Add** button to create a new ACE. Click the **Edit** or **Delete** button under the Action column to change the ACE configuration.





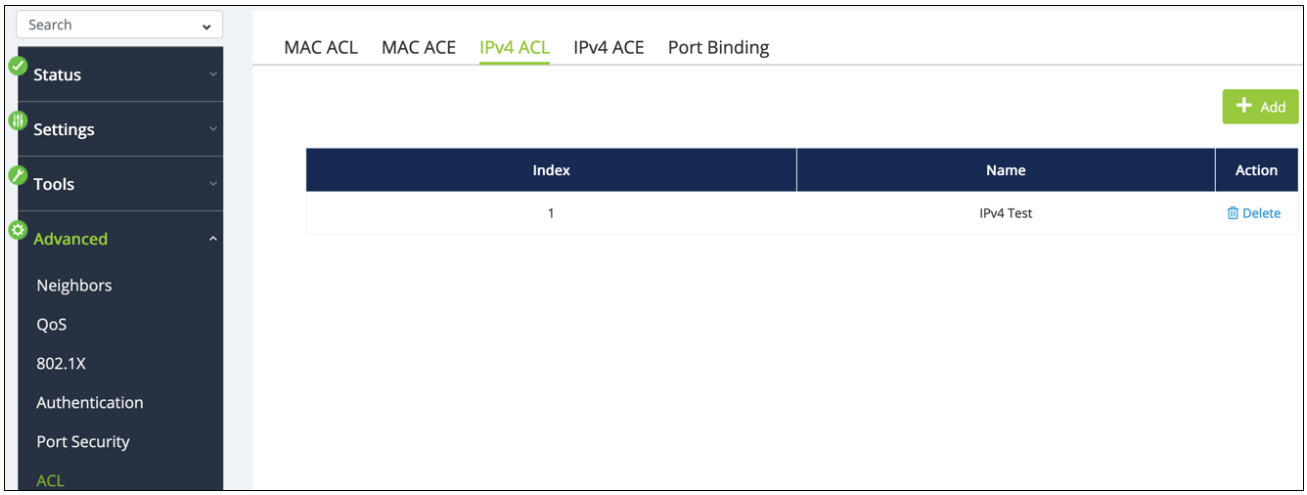
Configurable settings include:

- **ACL Name** — Select an ACL to associate with the ACE.
- **Sequence Range** — Enter a value for the ACE to be processed sequentially with the other ACEs. The smallest value is processed first.
- **Action** — Select whether to permit or deny traffic that meets the set criteria.

- **VLAN ID** — Enter the VLAN ID to monitor.
- **Source MAC** — If desired, enter a Source MAC address to monitor. If the field is left blank all MAC addresses on the VLAN are monitored.
- **Source MAC Mask** — Only available if a Source MAC address is defined. Enter a Source MAC mask to monitor for. Use this field to filter multiple addresses within a range.
- **Destination MAC** — If desired, enter a Destination MAC address to monitor. If the field is left blank all MAC addresses on the VLAN are monitored.
- **Destination MAC Mask** — Only available if a Destination MAC address is defined. Enter a Destination MAC mask to monitor for. Use this field to filter multiple addresses within a range.
- **802.1p Value** — Enter an 802.1p to value to monitor.
- **Ethertype (Hex)** — Typically left blank. A value restricts traffic using certain protocols.

IPv4 ACL

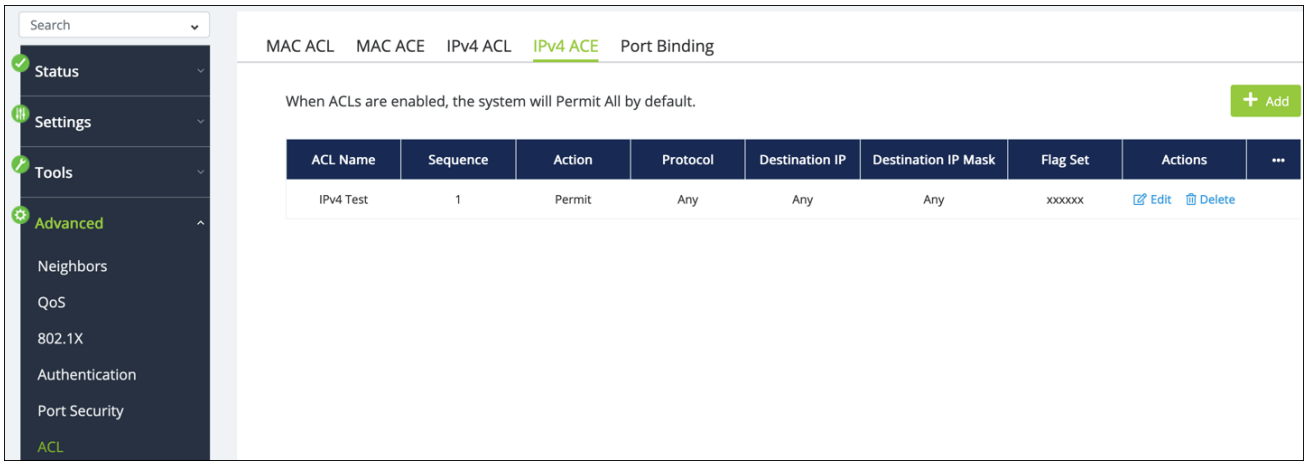
Use this page to create rules for incoming and outgoing traffic for specific IPv4 addresses. Click the **Add** button to add a new rule.

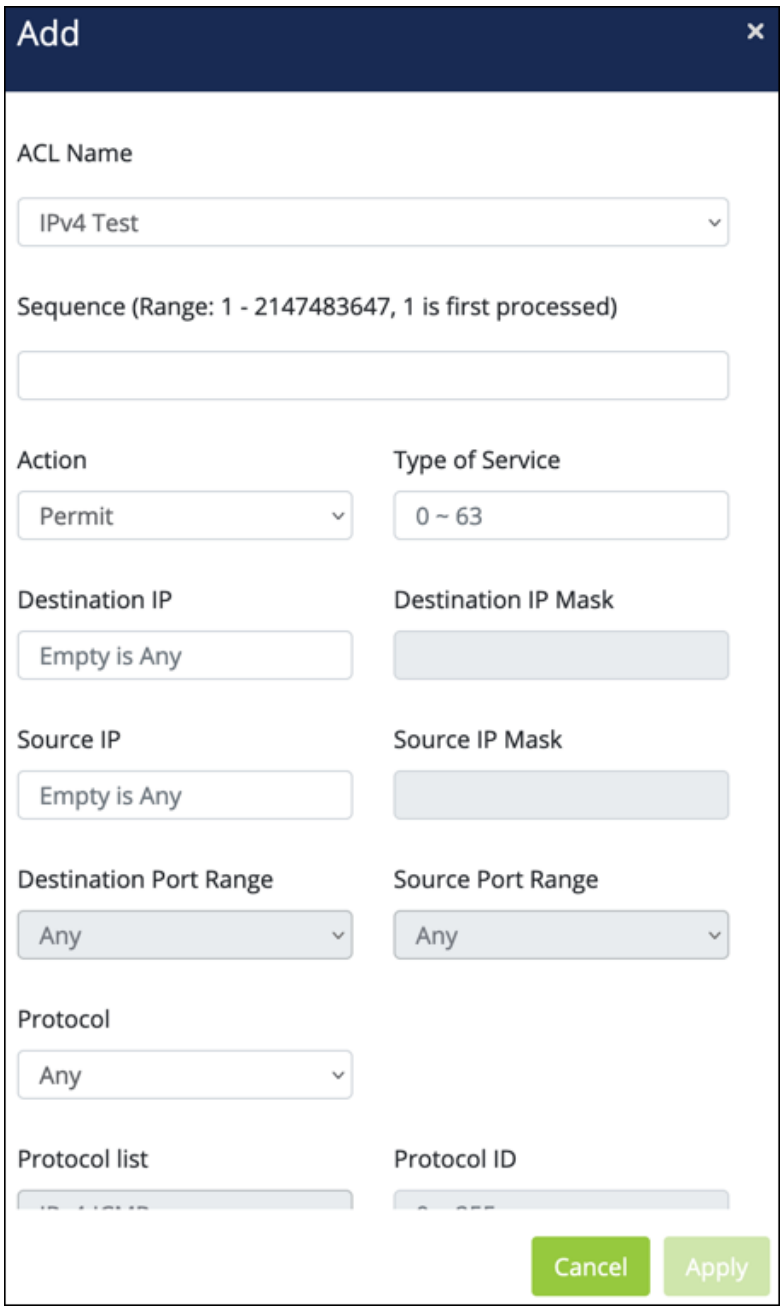


IPV4 ACE

Use this page to define **Access Control Entries (ACEs)** associated with each IPv4 ACL list. Use the ••• button to edit the table fields.

Click the **Add** button to create a new ACE. Click the **Edit** or **Delete** button under the Action column to change the ACE configuration.





Configurable settings include:

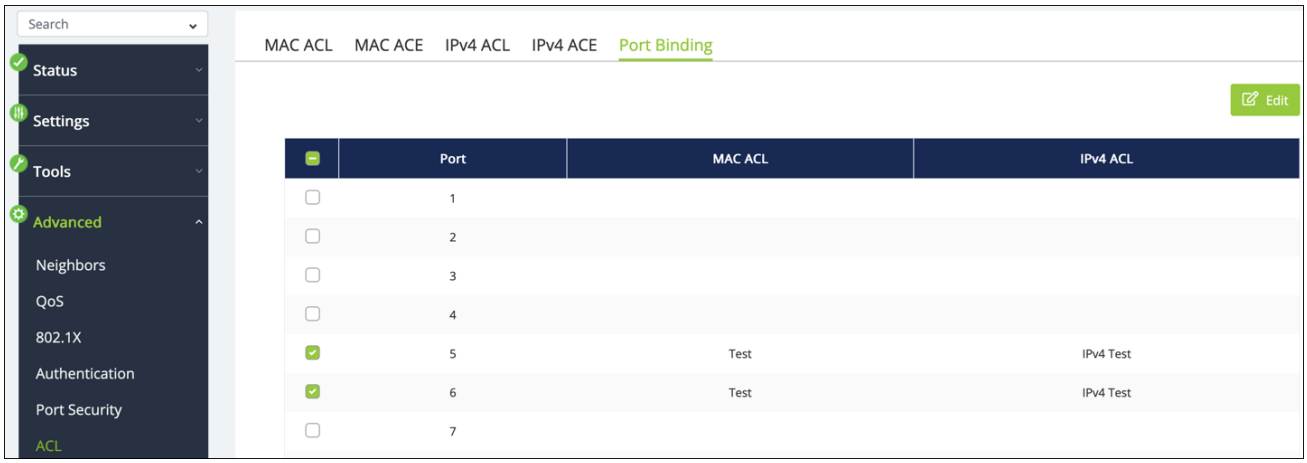
- **ACL Name** — Select an ACL to associate with the ACE.
- **Sequence Range** — Enter a value for the ACE to be processed sequentially with the other ACEs. The smallest value is processed first.
- **Action** — Select whether to permit or deny traffic that meets the set criteria.

- **Type of Service** — Enter a DSCP index to monitor.
- **Destination IP** — If desired, enter a Destination IPv4 address to monitor. If the field is left blank all IPv4 addresses on the VLAN are monitored.
- **Destination IP Mask** — Only available if a Destination IPv4 address is defined. Enter a Destination IPv4 mask to monitor for. Use this field to filter multiple addresses within a range.
- **Source IP** — If desired, enter a Source IPv4 address to monitor. If the field is left blank all IPv4 addresses on the VLAN are monitored.
- **Source IP Mask** — Only available if a Source IPv4 address is defined. Enter a Source IPv4 mask to monitor for. Use this field to filter multiple addresses within a range.
- **Destination Port Range** — Only available if the selected Protocol is port-based. Use the drop-down to select **Single** to enter a Destination Port to monitor.
- **Source Port Range** — Only available if the selected Protocol is port-based. Use the drop-down to select **Single** to enter a Source Port to monitor.
- **Protocol** — Select **Any**, from the **Protocol List**, or **Protocol** ID. These selections alter the selections below.
- **Protocol list** — The **Protocol** must be set to **Protocol List** to select the protocol type to monitor.
- **Protocol ID** — The **Protocol** must be set to **Protocol ID** to enter a protocol ID type to monitor.
- **ICMP** — Only available if the selected Protocol is ICMP-based. Select **Any**, from the **ICMP List**, or the **ICMP ID**.
- **ICMP list** — The **Protocol** must be set to **ICMP List** to select the ICMP type to monitor.
- **ICMP ID** — The **Protocol** must be set to **ICMP List** to enter the ICMP ID to monitor.
- **ICMP Code** — Enter the code value to monitor.

- **TCP Flags** — Only available if the selected Protocol is TCP-based. Use the drop-downs to set the below TCP Flag types to monitor.
    - Urg
    - Ack
    - Psh
    - Rst
    - Syn
    - Fin

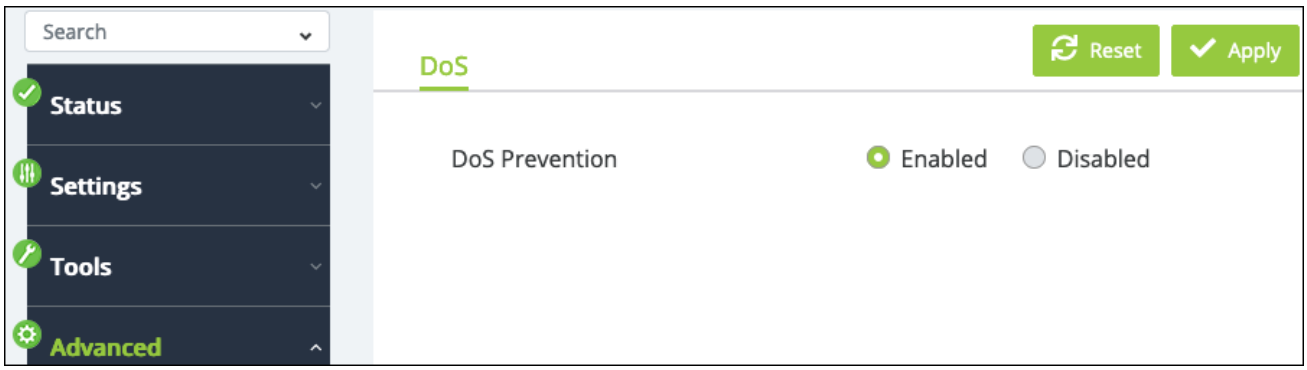
Port Binding

Use this page to assign MAC and IPv4 ACLs to specific ports. Select a **Port**(s), then click the **Edit** button to assign ACLs.



DoS

Use this page to enable **Denial of Service (DOS)** Prevention.



SNMP

Simple Network Management Protocol (SNMP) is a Layer 7 protocol for managing and monitoring network equipment from a central SNMP manager.

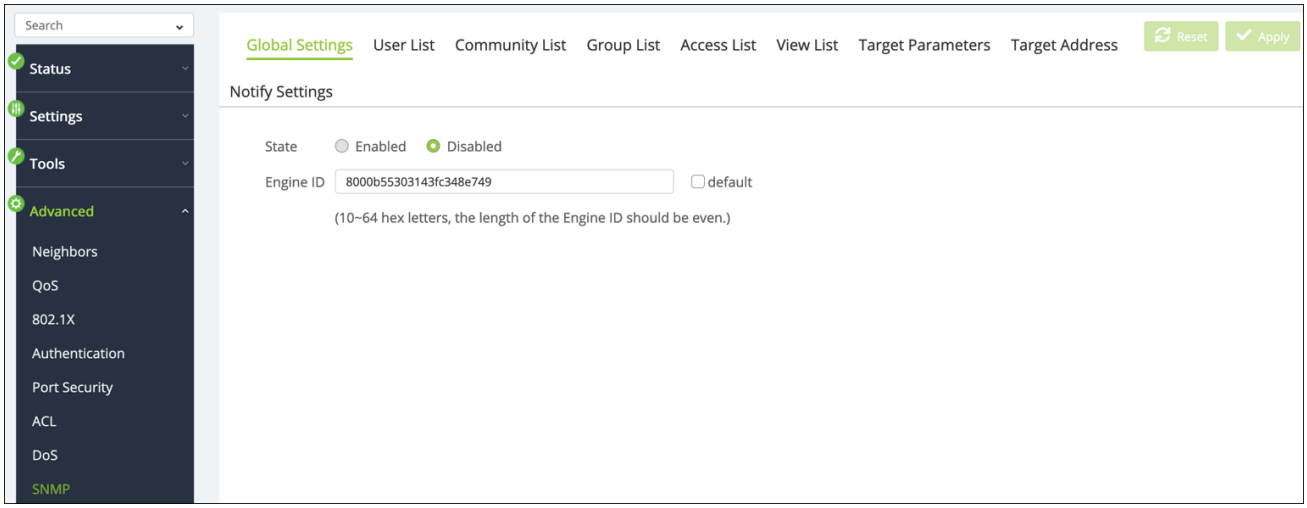
Managed devices that support SNMP run their own agent software; the SNMP agent maintains a defined set of variables that are used to manage the switch. These objects are defined in a **Management Information Base (MIB)**.

The Araknis switch includes an SNMP agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the switch and the traffic passing through its ports. SNMP client software can access the switch SNMP agent through SNMP community strings. These community strings are used for authentication.

SNMPv3 provides additional security features that cover message integrity, authentication, encryption, and control user access to specific objects in the MIB.

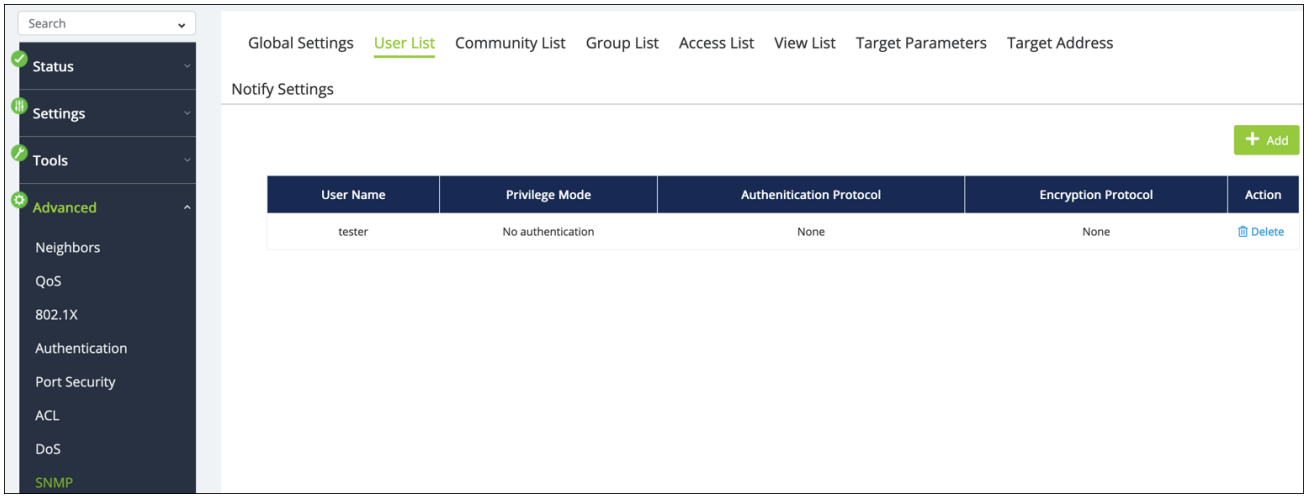
Global Settings

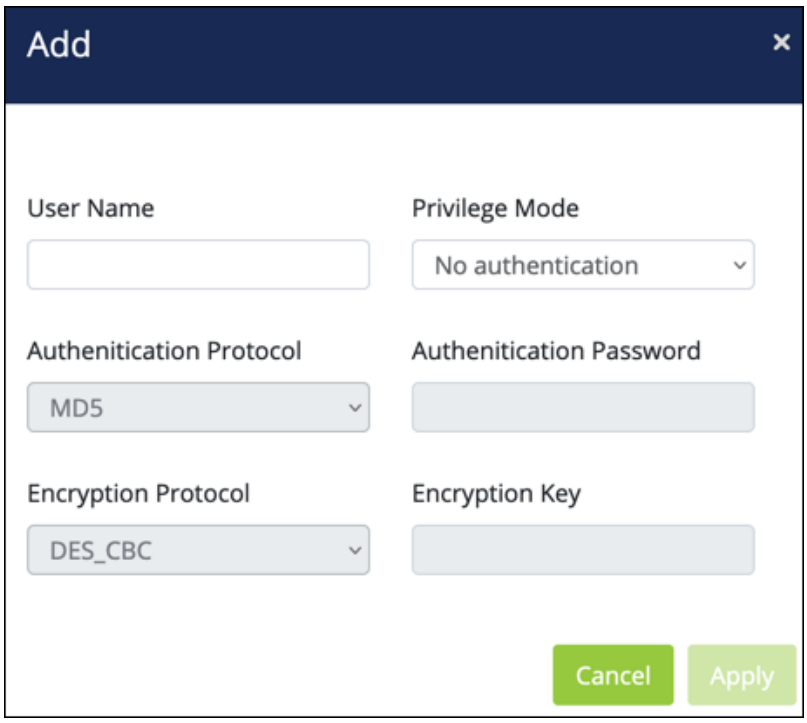
Use this page to enable or disable SNMP and to enter an **Engine ID** or select the **default** option. Some equipment may ask for the Engine ID when prompted to use the switch as an SNMP server.



User List

Use this page to configure SNMP users. Click the **Add** button to create a new user.



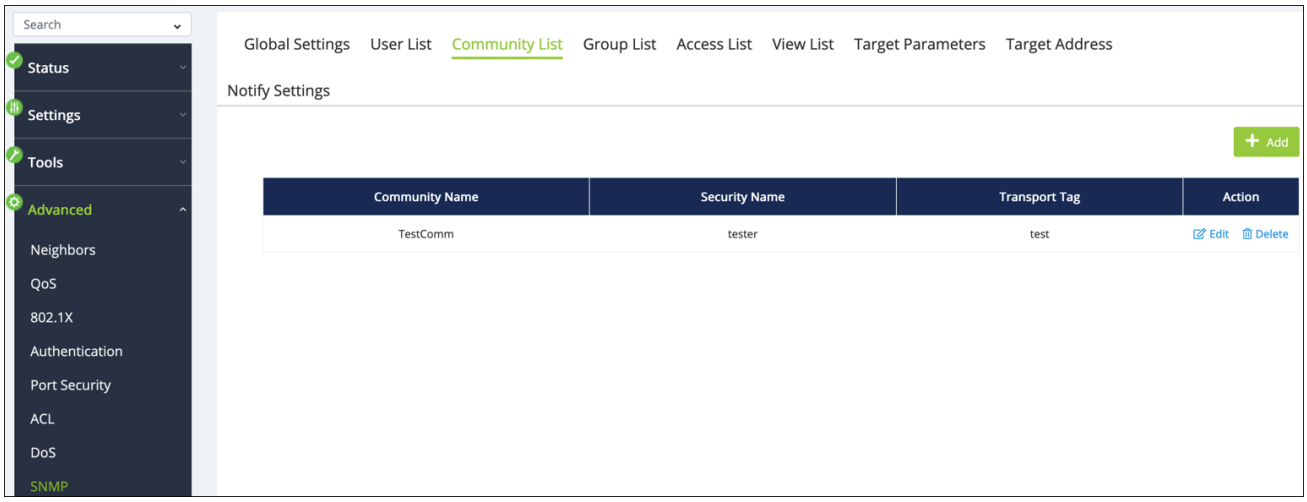


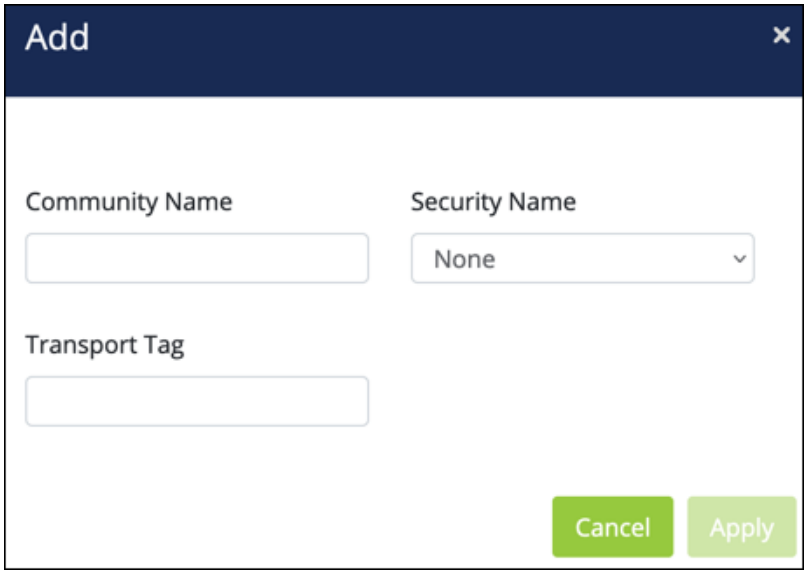
Configurable settings include:

- **User Name** — Enter a user name for the user.
- **Privilege Mode** — Use the drop-down to select one of the following:
  - **No authentication** — No authentication is used.
  - **Authentication** — SNMP messages are authenticated.
  - **Privilege** — SNMP messages are encrypted.
- **Authentication Protocol** — Select MD5 or SHA. The Privilege Mode must be set to Authentication to make a selection.
- **Authentication Password** — Enter a password for user authentication.
- **Encryption Protocol** — Select whether to use DES or AES encryption. The **Privilege Mode** must be set to **Privilege** to make a selection.
- Encryption Key — Enter a key to use that is at least 8 characters long.

Community List

Use this page to create SNMP Communities. Click the **Add** button to create a new community. Use the **Edit** and **Delete** buttons under the Action column to change the configuration.





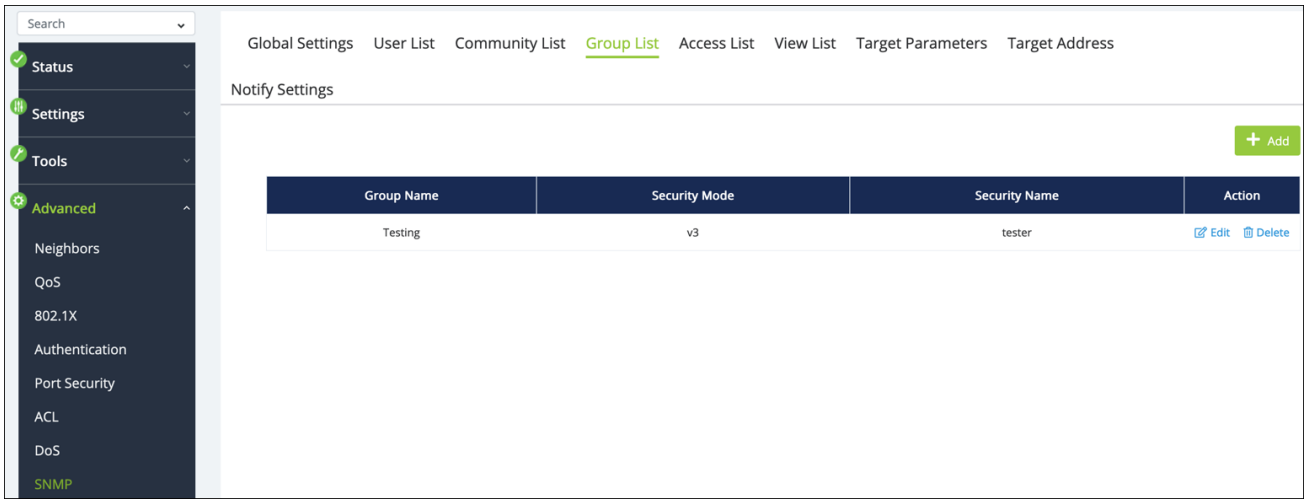
Configurable settings include:

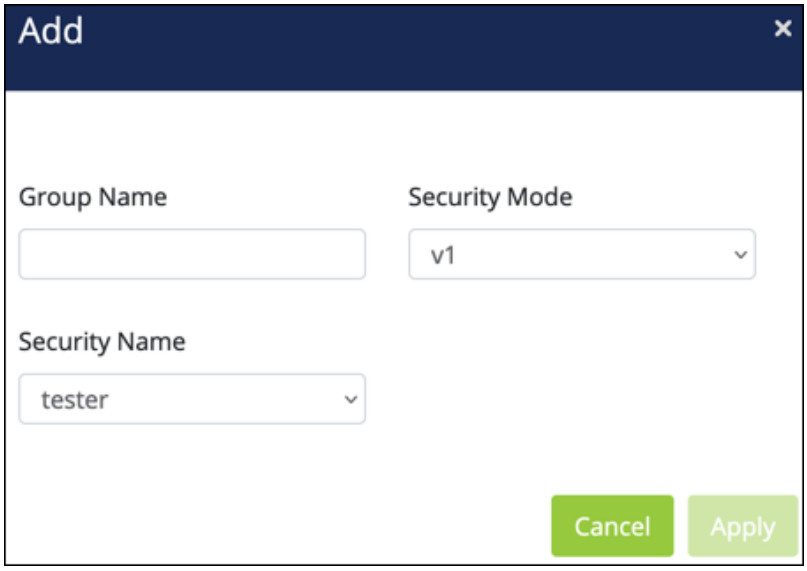
- **Community Name** — Enter a name for the community.
- **Security Name** — Select an SNMP user name to add to the Community, or none.

- **Transport Tag** — Enter a tag value to compare with the other transport endpoints to identify requests from this community.

Group List

Use this page to create SNMP Groups. Click the **Add** button to create a new community. Use the **Edit** and **Delete** buttons under the Action column to change the configuration.





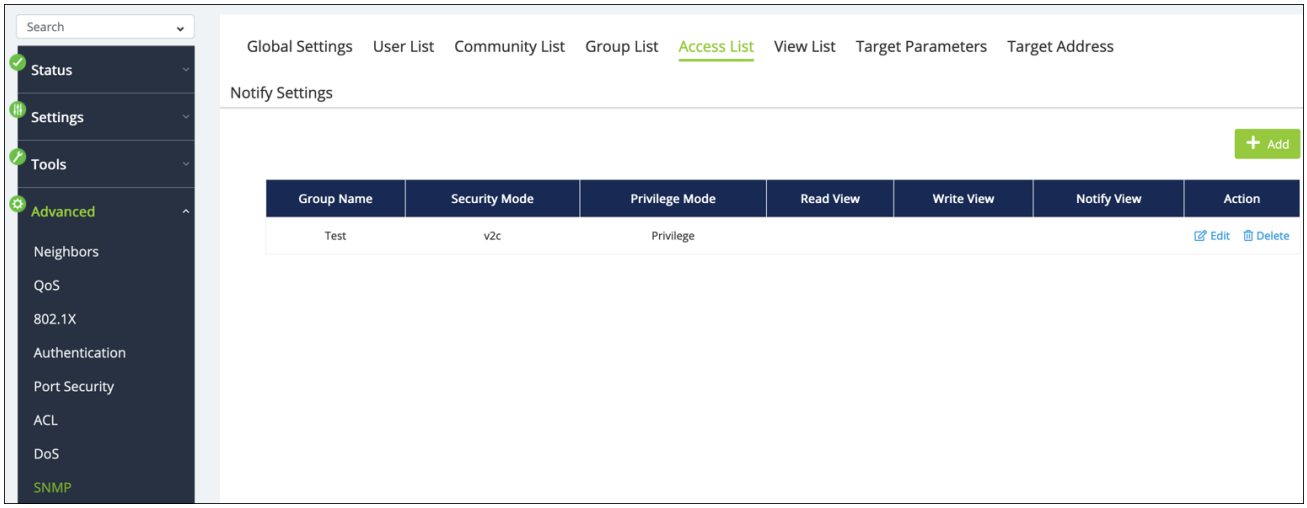
Configurable settings include:

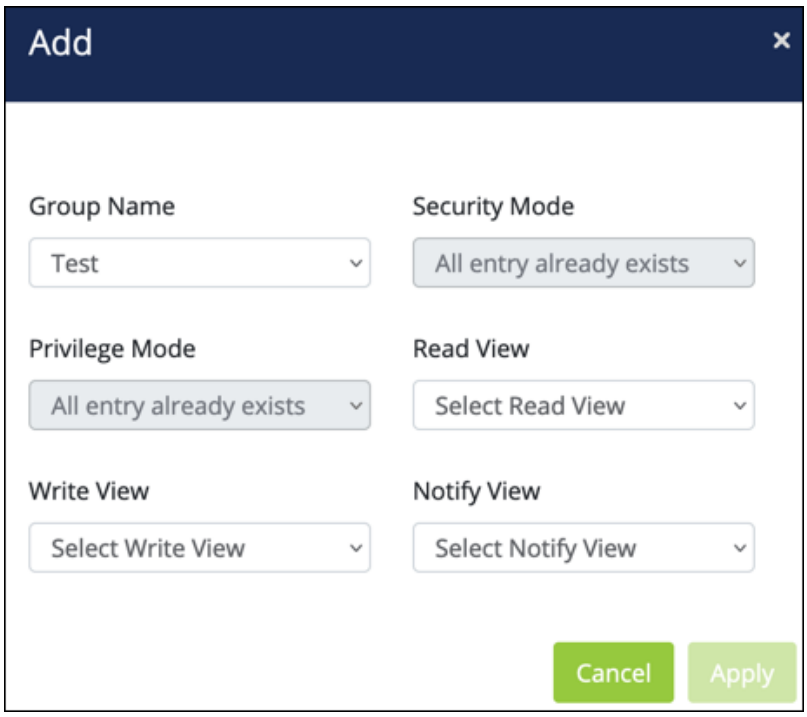
- **Group Name** — Enter a name for the group.
- **Security Mode** — Select SNMP version 1, 2c, or 3.
- **Security Name** — Select an SNMP user.

Access List

Use this page to create an Access List and apply it to an SNMP Group. Access Lists control which addresses can manage and monitor the switch.

Click the **Add** button to create a new community. Use the **Edit** and **Delete** buttons under the Action column to change the configuration.





Configurable settings include:

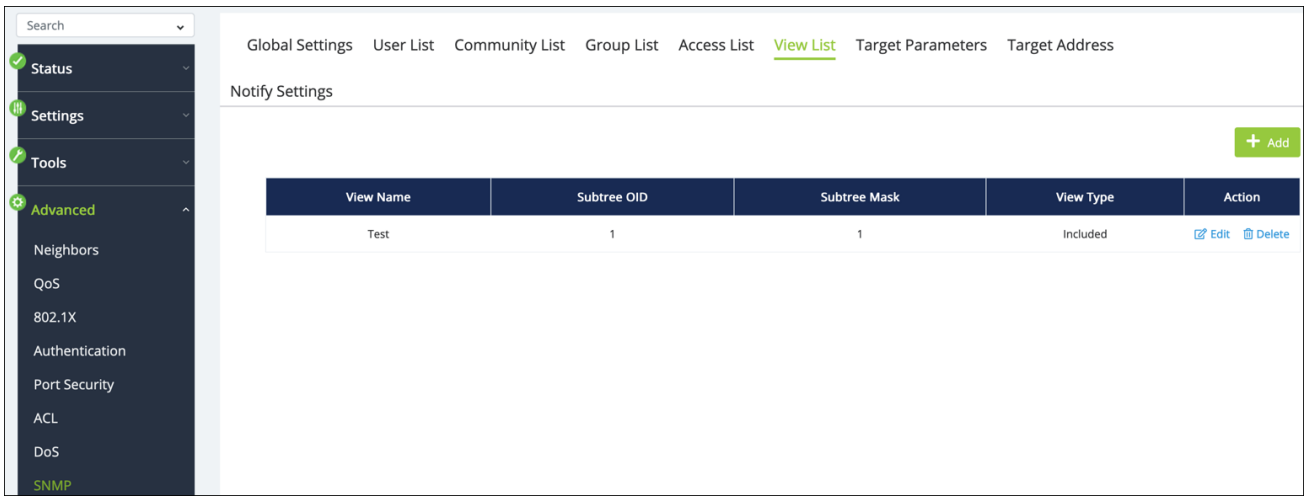
- **Group Name** — Select a previously configured SNMP Group.
- **Security Mode** — Follows the SNMP Group security mode.
- **Privilege Mode** — Follows the SNMP User Privilege mode.

Note: Read, Write, and Notify View cannot be changed.

View List

Use this page to create **SNMP Views**, which are used as a mapping between SNMP scalar and tabular objects and the access rights configured for the View.

Click the **Add** button to create a new View. Use the **Edit** and **Delete** buttons under the Action column to change the configuration.



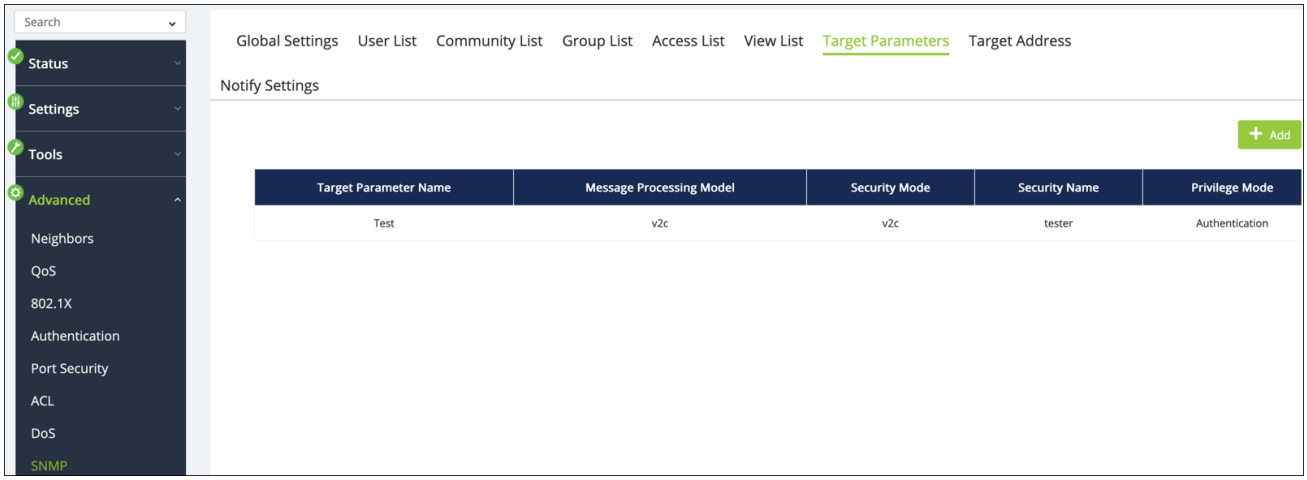
Configurable settings include:

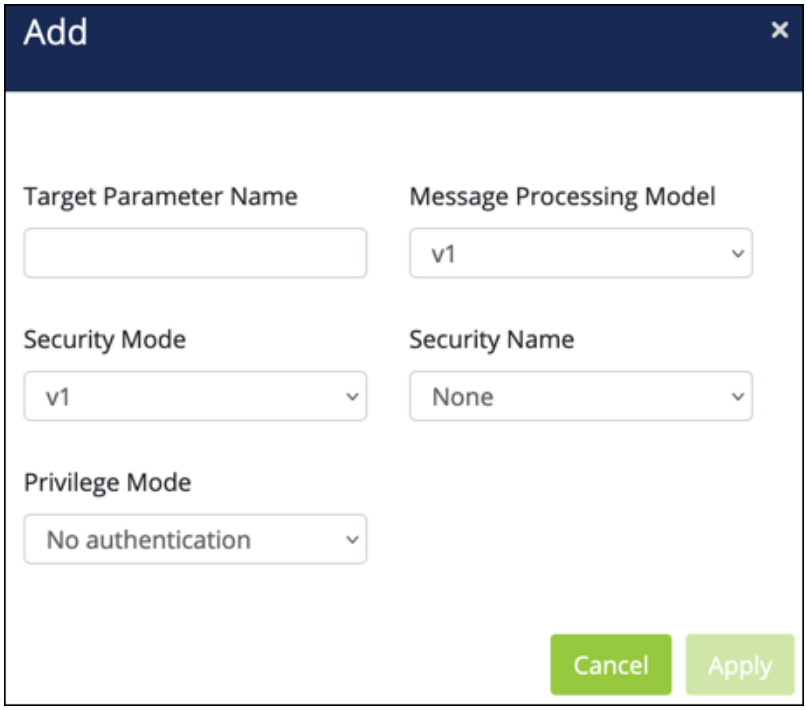
- **View Name** — Enter a name for the View.
- **Subtree OID** — Enter the Subtree Object Identifier (OID) value (must begin with a "."). This value identifies an MIB tree that will be granted or denied access by the SNMP manager.
- **Subtree Mask** — Enter 0 (zero) for does not concern, or 1 for is concerned.
- **View Type** — Select Included or Excluded.

Target Parameters

Use this page to create Target Parameters for use in generating messages. These parameters are referenced in the Target Address Table.

Click the **Add** button to create a new Target Parameter. Use the **Edit** and **Delete** buttons under the Action column to change the configuration.



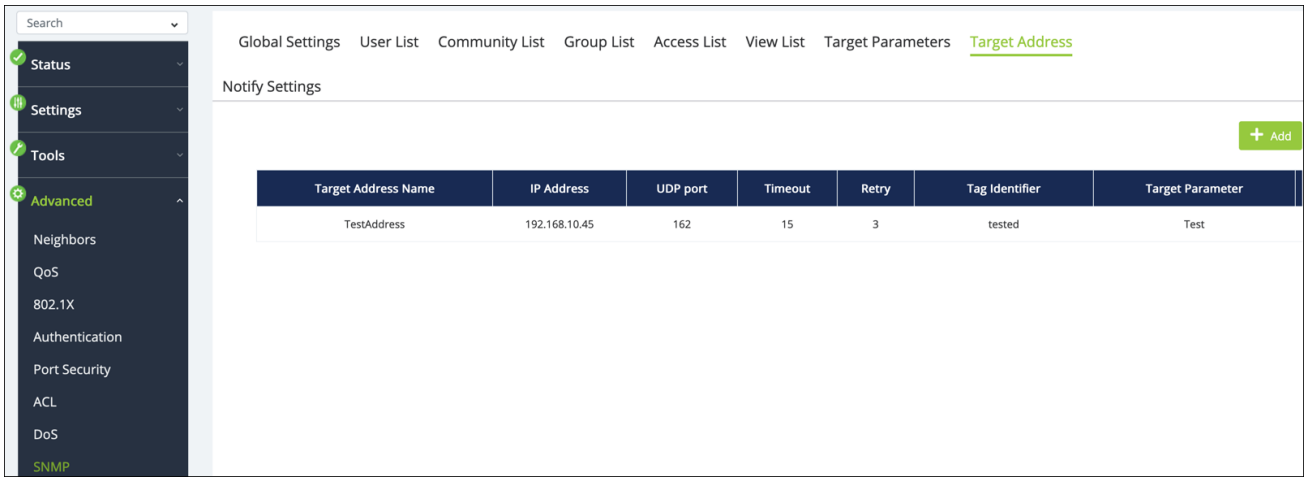


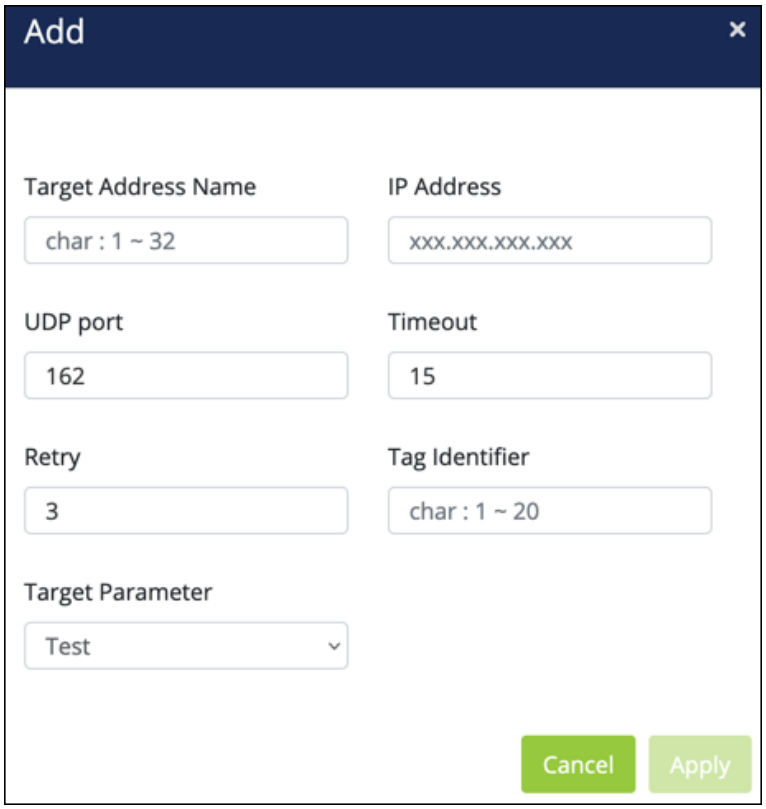
Configurable settings include:

- **Target Parameter Name** — Enter a name for the parameter.
- **Message Processing Model** — Select the SNMP version. 1, 2c, or 3.
- **Security Mode** —Select SNMP v1, 2c, or 3.
- **Security Name** — Select an SNMP user.
- **Privilege Mode** — Select no authentication, authentication, or privilege.

Target Address

Use this page to create Target Addresses to receive notifications. Click the **Add** button to create a new Target Address. Use the **Edit** and **Delete** buttons under the Action column to change the configuration.



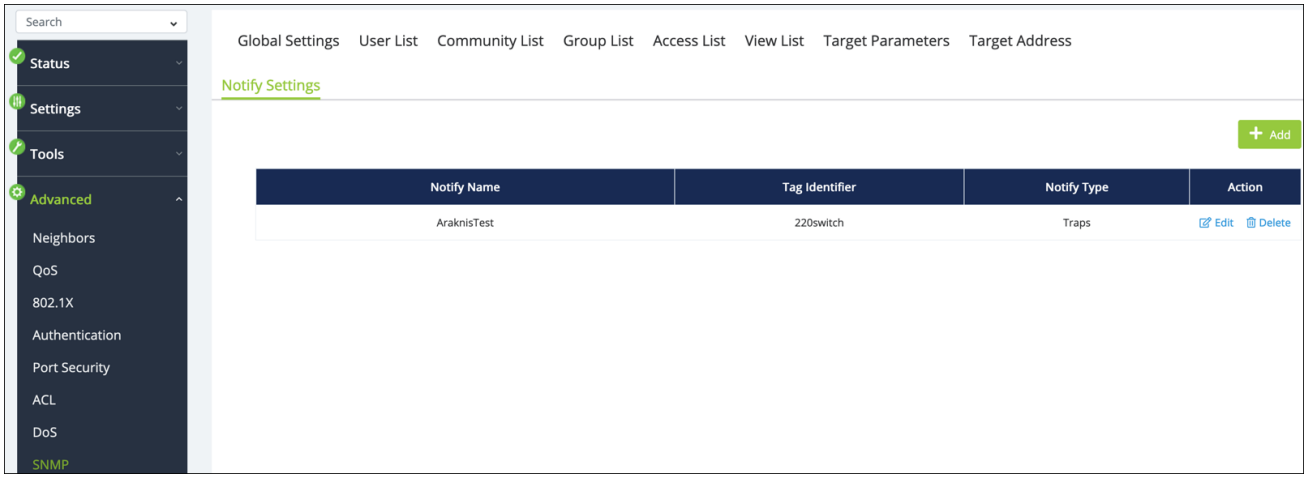


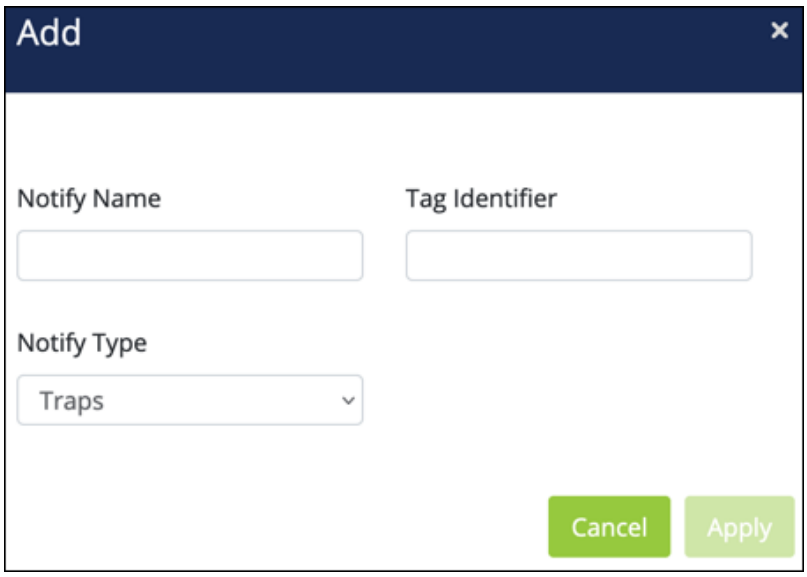
Configurable settings include:

- **Target Address Name** — Enter a name for the target.
- **IP Address** — Enter an IP address for the target.
- **UDP Port** — The UDP port to communicate on.
- **Timeout** — The amount of time (in seconds) the switch will wait for a reply from the target before reattempting.
- **Retry** — The number of times the switch will attempt to contact the target address.
- **Target Identifier** — Enter a name to act as the target address's identifier.
- **Target Parameter** — Select a Target parameter.

Notify Settings

Use this page to configure the notifications sent to the Target IP Address(es). Click the **Add** button to create a new notification. Use the **Edit** and **Delete** buttons under the Action column to change the configuration.





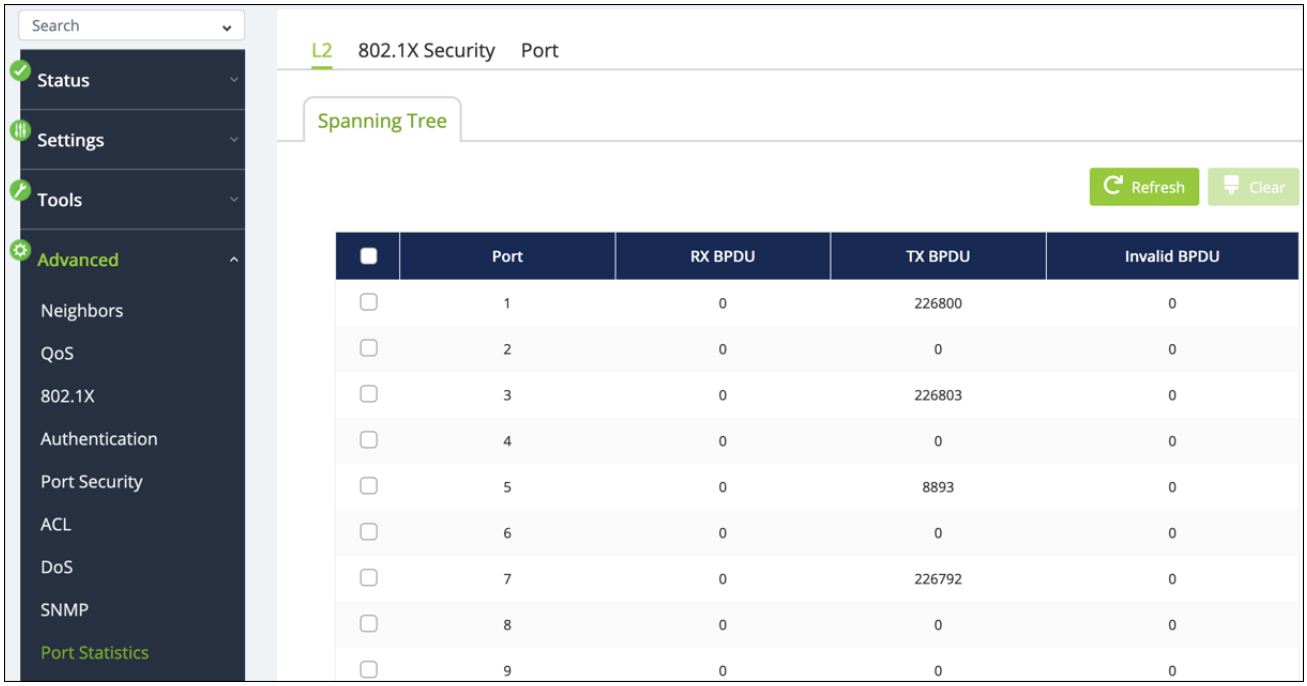
Configurable settings include:

- **Notify Name** — Enter a name for the notifications.
- **Tag Identifier** — Enter a name to act as the notification's identifier.
- **Notify Type** — Select Trap or Inform:
  - **Trap** — An SNMP message that notifies the host when an event occurs on the switch. This message is not acknowledged by the trap receiver.
  - **Inform** — Only available for SNMP v2. An SNMP message that notifies the host when an event occurs on the switch. This message is acknowledged by the trap receiver.

Port Statistics

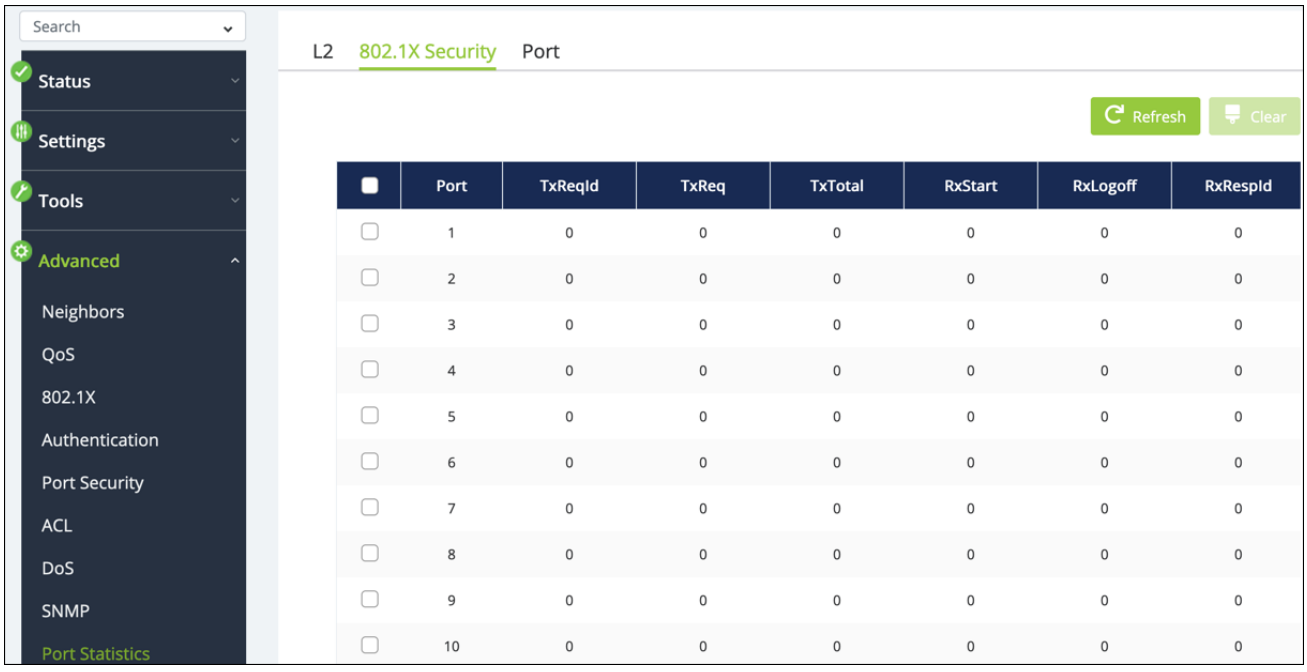
L2

Use this page to view Spanning Tree statistics for each port. You can select a **Port**(s) and click the **Clear** button to restart the data gathered.



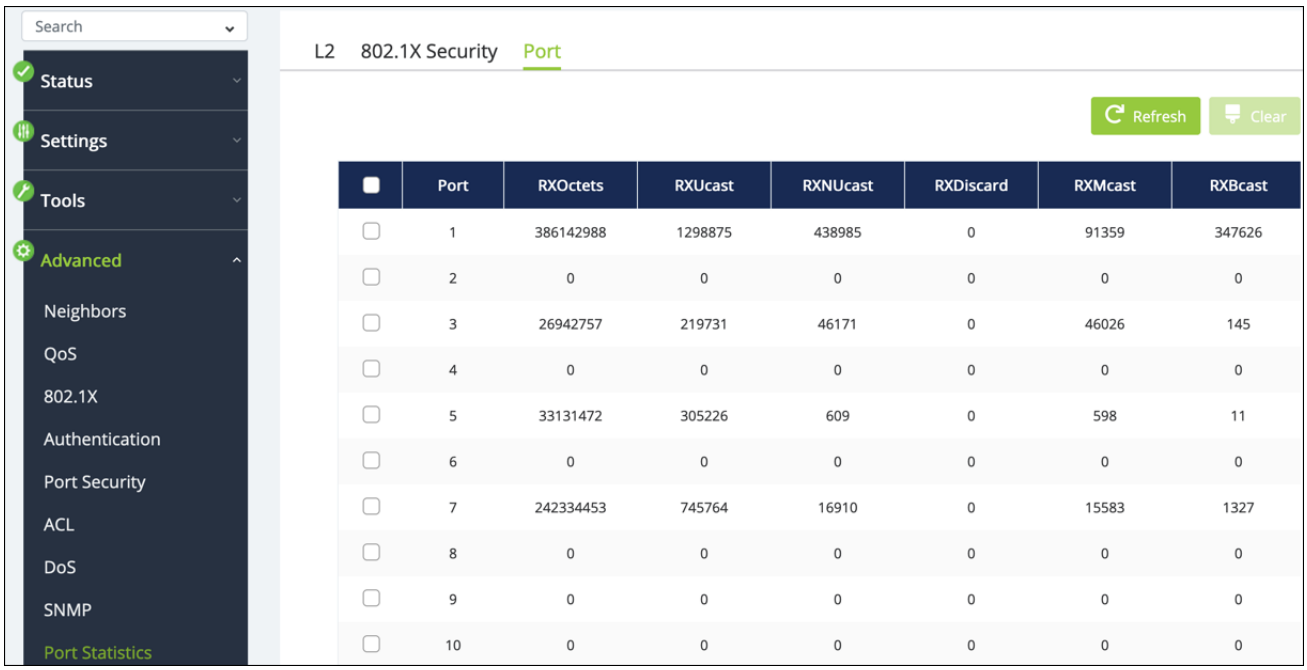
802.1X Security

Use this page to view 802.1x statistics for each port. You can select a **Port**(s) and click the **Clear** button to restart the data gathered.



Port

Use this page to view general statistics for each port. You can select a **Port**(s) and click the **Clear** button to restart the data gathered.

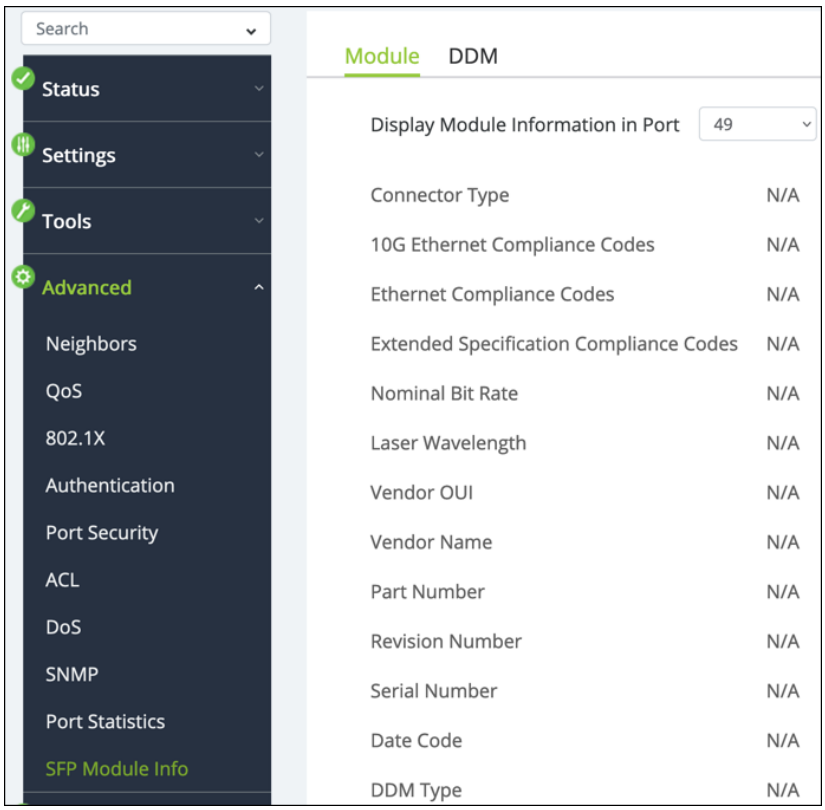


Port	RXOctets	RXUcast	RXNUcast	RXDiscard	RXMcast	RXBcast
1	386142988	1298875	438985	0	91359	347626
2	0	0	0	0	0	0
3	26942757	219731	46171	0	46026	145
4	0	0	0	0	0	0
5	33131472	305226	609	0	598	11
6	0	0	0	0	0	0
7	242334453	745764	16910	0	15583	1327
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0

SFP Module Info

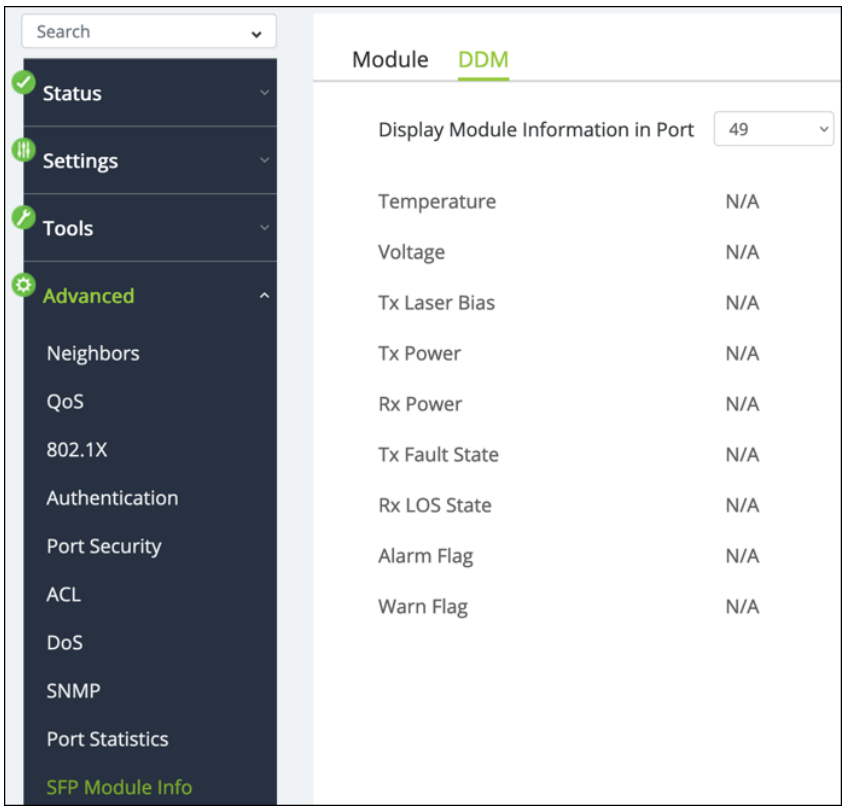
Module

Use this page to view information about the SFP module in a specific port. Use the **Display Module Information in Port drop-down** to select the SFP module you want to see data for.



DDM

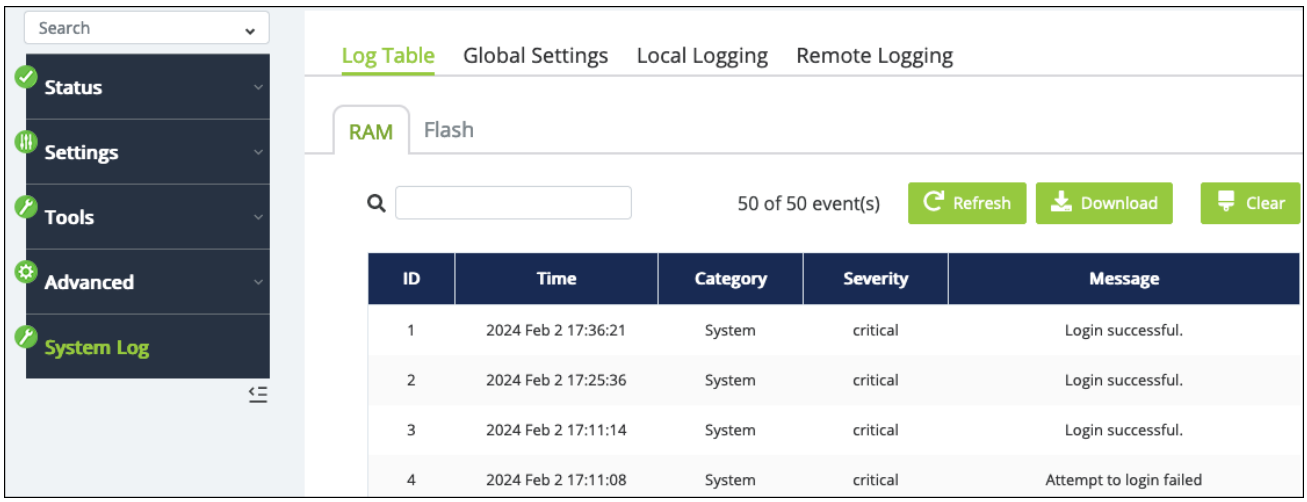
Use this page to view the SFP module's **Digital Diagnostic Monitoring (DDM)** from a specific port. Use the **Display Module Information in Port drop-down** to select the SFP module you want to see data for.



System Logs

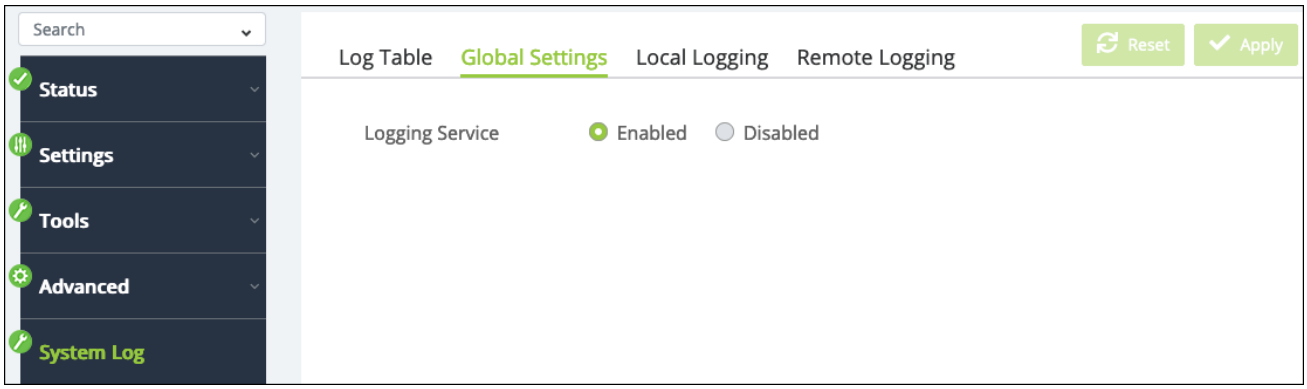
Log Table

Use this page to review, refresh, download, or clear events recorded to the switch's log. There are separate tabs for events recorded to the RAM (temporary) and Flash (permanent) memory.



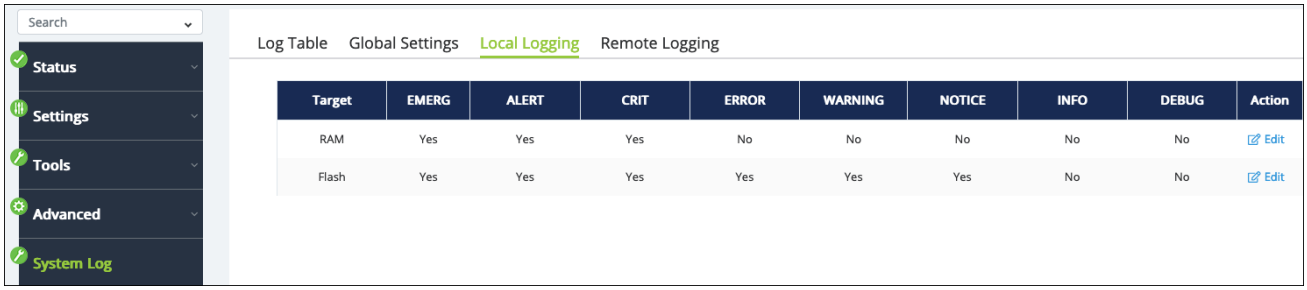
Global Settings

Use this page to enable or disable logging.

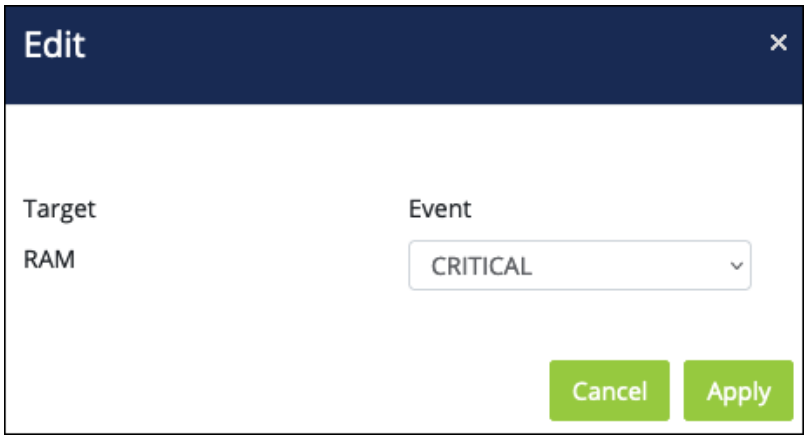


Local Logging

Use this page to select the type of events recorded to the RAM and Flash logs. Click the **Edit** button in the Action column of the Log row you wish to make changes to.

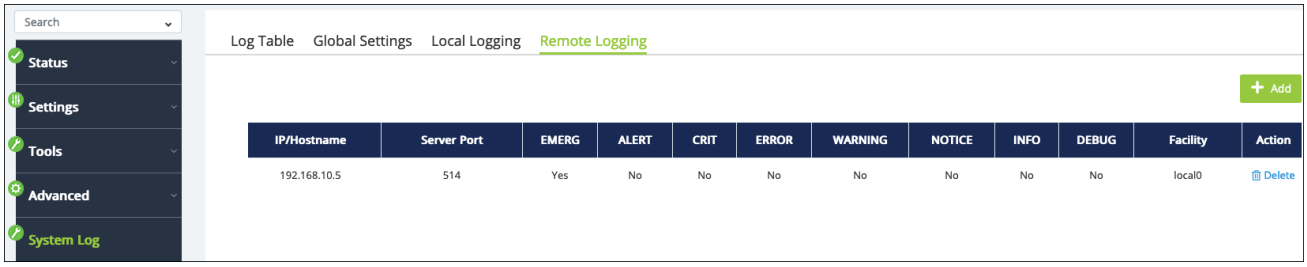


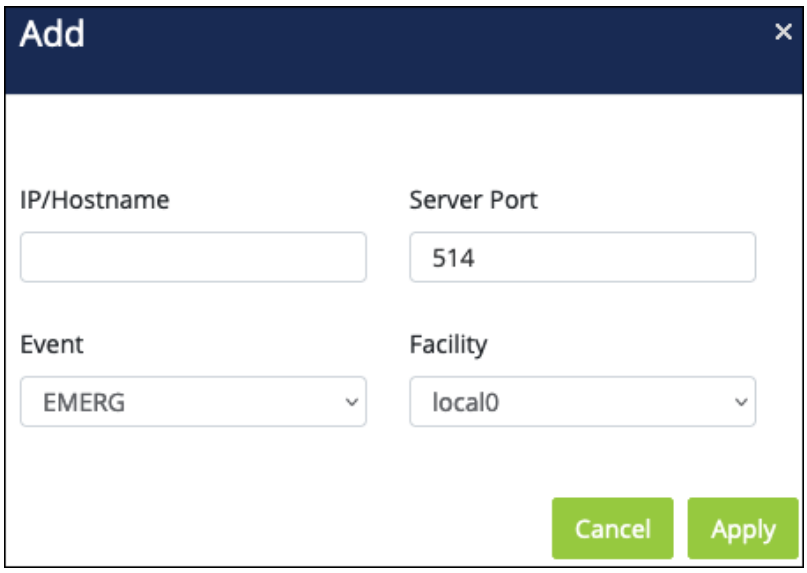
In the Edit window, select the **Event** type you'd like to change the state of (yes or no), then click **Apply**.



Remote Logging

Use this page to configure a remote server to record logs to. Click the **Add** button to configure a new server. Click the **Edit** button in the Action column of the server's row to make changes.





Configurable settings include:

- **IP/Hostname** — Enter the IP address of the remote log server.
- **Server Port** — Enter the port to communicate with the server.
- **Event** — Select the event type you want to record. The default is EMERG(ency). To add more event types to log, apply the current configuration, then edit the server entry and select another event type, then click Apply.
- **Facility** — Select the facility value for the remote logging event (local 0-7). Default: local 0

Specifications

	AN-220-SW	AN-320-SW	AN-420-SW
Hardware			
Form-Factor	1U Rackmount 12.99" x 1.73" x 9.05" (8)	1U Rackmount 12.99" x 1.73" x 9.05" (8/ 8-POE)	N/A
	1U Rackmount 17.32" x 1.73" x 10.23" (16)	1U Rackmount 17.32" x 1.73" x 10.23" (16/ 16-POE)	1U Rackmount 17.32" x 1.73" x 16.14" (F/R-16-POE)
	1U Rackmount 17.32" x 1.73" x 10.23" (24)	1U Rackmount 17.32" x 1.73" x 10.23" (24) 17.32" x 1.73" x 16.14" (24-POE)	1U Rackmount 17.32" x 1.73" x 16.14" (F/R-24-POE)
	1U Rackmount 17.32" x	N/A	1U Rackmount 17.32" x

	1.73" x 16.14" (44)		1.73" x 16.14" (R-44-POE)
	1U Rackmount 17.32" x 1.73" x 16.22" (48)	1U Rackmount 17.32" x 1.73" x 10.22" (48/ 48-POE)	1U Rackmount 17.32" x 1.73" x 16.14" (F-48-POE)
Power Consumption	8 port - Max.: 82.81W; Device: 11.20W	Max: 10W (8) Max: 157.06W; Device: 12.92W (8-POE)	N/A
	16 port - Max.: 173.90W; Device: 18.12W	Max: 12.48W (16) Max: 297.74W; Device: 22.30W (16-POE)	Device: 34.617; Device with POE: 284.617 (R-16-POE) Device: 31.927; Device with POE: 281.927 (F-16-POE)
	24 port - Max.: 235.65W; Device: 27.13W	Max: 18.29W (24) Max: 441.05W; Device: 26.65W (24-POE)	Device: 39.86W; Device with POE:449.86 (R-24-POE) Device: 37.41W; Device with POE:447.41 (F-24-POE)
	44 Port - Max.: 417.67W; Device:42.67W	N/A	Device: 69.1W; Device with POE: 809.1W (R-44-POE)
	48 port - Max: 481.40W; Device: 48.90W	Max: 38.40W (F-48)	Device: 63.47W; Device with POE: 803.47W (F-48-POE)
Line Voltage	100-240V AC, 50/60Hz	100-240V AC, 50/60Hz	100-240 VAC, 50/60Hz
Weight	5.1 lb (8)	6.94 lb (8)/ 4.45 lb (8-POE)	N/A
	7.4 lb (16)	7.56 lb(16)/ 6.23 lb (16-POE)	10.54 lb (R-16-POE)/10.42 lb (F-16-POE)
	7.7 lb (24)	12.2 lb (24)/ 6.41 lb (24-POE)	11.50 lb (R-24-POE)/11.36 lb (F-24-POE)
	12.46 lb (44)	N/A	12.76 lb (R-44-POE)
	13.4 lb (48)	8.2 lb (48)	12.60 lb (F-48-POE)
10M/100M/1G BASE-T RJ45 Ports	8 (8)	8 (8)	N/A
	16 (16)	16 (16)	12 (16)
	24 (24)	24 (24)	16 (24)
	44 (44)	N/A	28 (44)
	48 (48)	48 (48)	32 (48)
100M/1G/2.5G BASE-T RJ45 Ports	N/A	N/A	4 (16)
			8 (24)
			16 (44)
			16 (48)

SFP Ports	2 (8/16/24)	2 (8/16/24)	N/A
	4 (44/48)	4 (44/48)	4 (16/24/44/48)
PoE Budget	65W (8)	130W (8)	N/A
	130W (16)	250W (16)	250W (16)
	190W (24)	375W (24)	410W (24)
	375 (44)	N/A	740W (44)
	375W (48)	740W (48)	740W (48)
Max PoE Per Port	30W	30W	30W
Simultaneously PoE Per Port	8W	15W	15W
Performance			
CPU Speed	500MHz (8/16/24)	500MHz (8/16/24)	800MHz (16/24)
	700MHz (44/48)	700MHz (48)	1GHz (44/48)
Flash Memory	256Mb	256Mb	1Gb(NAND)/128Mb(NOR)
RAM Memory	2Gb	2Gb	4Gb
MAC Entries	16K	16K	16K(16/24); 32K (44/48)
ARP Entries	192	192	192
Switching Capacity (bi-directional)	20Gbps (8)	20Gbps (8)	N/A
	36Gbps (16)	36Gbps (16)	124Gbps (16)
	52Gbps (24)	52Gbps (24)	152Gbps (24)
	96Gbps (44)	N/A	208Gbps (44)
	104Gbps (48)	104Gbps (48)	224Gbps (48)
Forwarding Mode	Store and Forward/LIFO	Store and Forward/LIFO	Store and Forward/LIFO
Forwarding Rate (@ 88-bytes)	28 Mpps (8)	28 Mpps (8)	N/A
	51 Mpps (16)	51 Mpps (16)	176 Mpps (16)
	74 Mpps (24)	74 Mpps (24)	216 Mpps (24)
	136 Mpps (44)		295 Mpps (44)
	148 Mpps (48)	148 Mpps (48)	318 Mpps (48)
Packet Buffer	512KB (8/16/24) 12Mb (44/48)	512KB (8/16/24) 12Mb (48)	12Mb (16/24) 16Mb (44/48)
Jumbo frames	10K	10K	10K
Multicast IGMP Group Membership (L2)	256	256	256
VLANs	256	256	256
ACLS	16	16	16
LAGs	8	8	8
CLI	Yes	Yes	Yes
Features			

QoS Features	Priority Queues: 8 queues per port Rate Limiting - Ingress: 16kbps~1000Mbps Rate Limiting - Egress: 16kbps~1000Mbps Scheduling: WRR, Strict Priority, WRR+Strict Priority CoS: 802.1p, IP DSCP/TOS, Physical Port ACL (L2/L3/L4) ACL (IPv4) Storm Control (Per Port)	Priority Queues: 8 queues per port Rate Limiting - Ingress: 16kbps~1000Mbps Rate Limiting - Egress: 16kbps~1000Mbps Scheduling: WRR, Strict Priority, WRR+Strict Priority CoS: 802.1p, IP DSCP/TOS, Physical Port ACL (L2/L3/L4) ACL (IPv4) Storm Control (Per Port)	Priority Queues: 8 queues per port Rate Limiting - Ingress: 16kbps~1000Mbps Rate Limiting - Egress: 16kbps~1000Mbps Scheduling: WRR, Strict Priority, WRR+Strict Priority CoS: 802.1p, IP DSCP/TOS, Physical Port ACL (L2/L3/L4) ACL (IPv4) Storm Control (Per Port) Class Mapping Policy Mapping
PoE Features	802.3af/at Auto PD Classification Max Power Output per Port: 30W Max Simultaneous Power per Port: 8W	802.3af/at Auto PD Classification Max Power Output per Port: 30W Max Simultaneous Power per Port: 15W	802.3af/at Auto PD Classification Max Power Output per Port: 30W Max Simultaneous Power per Port: 15W
VLAN Features	802.1Q Port-based VLANs Voice VLAN	802.1Q Port-based VLANs Voice VLAN	802.1Q Port-based VLANs Voice VLAN
ACL Features	Ingress/Egress MAC based IP based	Ingress/Egress MAC based IP based	Ingress/Egress MAC based IP based
Layer 2 Features	SNMP IGMPv1/v2/v3 Snooping IGMP v2/v3 IGMP Querier Unregistered MCast Filtering 802.1X LAG Spanning Tree Protocol Flow Control EEE Jumbo Frames	SNMP IGMPv1/v2/v3 Snooping IGMP v2/v3 IGMP Querier Unregistered MCast Filtering 802.1X LAG Spanning Tree Protocol Flow Control EEE Jumbo Frames	SNMP IGMPv1/v2/v3 Snooping IGMP v2/v3 IGMP Querier Unregistered MCast Filtering 802.1X LAG Spanning Tree Protocol Flow Control EEE Jumbo Frames DHCP Snooping
Layer 3 Features	N/A	N/A	IP Routing Static Routing DHCP Relay
Management Features	OvrC FW Upgrade: TFTP, HTTP Port Mirroring: One to One, Many to One SNTP Dual FW Image Persistent Logging Remote Logging	OvrC FW Upgrade: TFTP, HTTP Port Mirroring: One to One, Many to One SNTP Dual FW Image Persistent Logging Remote Logging	OvrC FW Upgrade: TFTP, HTTP Port Mirroring: One to One, Many to One SNTP Dual FW Image Persistent Logging Remote Logging
Temperature Range	Operating: 0°C ~ + 50°C Storage: -20°C ~ + 70°C	Operating: 0°C ~ + 50°C Storage: -20°C ~ + 70°C	Operating: 0°C ~ + 50°C Storage: -40°C ~ + 70°C
Humidity Range	Operation: 10%~90%	Operation: 10%~90%	Operation: 10%~90% RH

	RH	RH	
Certifications	FCC, CE, UL	FCC, CE, UL	FCC, IC, CE, RCM, UL