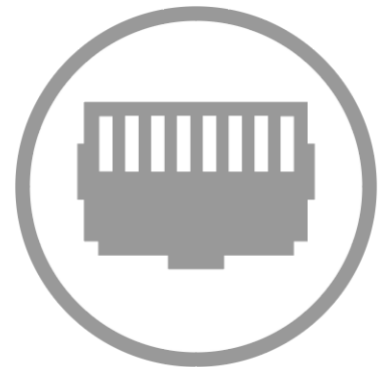




MS Series

LAYER 3 SWITCHES WITH OVRC
MS-1212, MS-2424, MS-2400, MS-2416, MS-4424

User Guide



Contents

Introduction	6
Switches	6
Switch specifications*	6
Technical Support.....	6
Installing.....	7
Getting to know your switch	8
Front panel	8
Back panel	9
Accessing the switch	10
Navigating the switch.....	10
Tabs	10
Tab layouts	11
Tiles and sub-tabs	12
Table content	12
Viewing, adding, and editing.....	13
Editing multiple items	14
Configure.....	15
Overview	16
Connections	17
Interfaces	18
Tiles	18
Add or edit an interface	18
Completing the dialog.....	19
Tiles	19
Ports	20
Port Summary	21
Port Details.....	23
VLAN.....	24
Database	24
Completing the dialog.....	25
Explanations	25
Switchport Configuration	26
Edit Switchport Configuration.....	26
Completing the dialog.....	27

Explanations: Switchport Configuration dialog	27
VLAN Subpage: Reset.....	28
PoE.....	29
Port Configuration.....	30
Port Configuration settings	30
Edit Port Configuration settings.....	31
Completing the dialog	31
General	32
Edit PoE General Settings.....	32
Statistics (read only).....	33
Details (read only)	34
Backup.....	36
Logs	36
Reset to factory default settings.....	37
Reset using the interface	37
Reset using the physical RESET button	38
Advanced.....	38
Configuring IGMP Snooping	39
Enabling VLAN IGMP snooping status.....	40
Configuring multicast router VLANs	42
Configuring IGMP Snooping Querier.....	44
VLAN Configuration.....	45
VLAN Status.....	46
Configuring Unregistered Multicast Behavior	46
Exception Details.....	47
Interface Configuration	48
Configuring Spanning Tree Protocol	49
CST Configuration.....	50
CST Port Configuration.....	52
MST Configuration	55
MST Port Configuration	56
Spanning Tree Statistics	58
Loop Protection.....	58
How to Configure Loop Protection	58
Loop Protection Configuration Table.....	60
Firmware	61
SNMP	61
How to Configure an SNMP Community or Group	62
How to Configure Trap Receivers for SNMP v1 and 2	63
How to Configure Trap Receivers for SNMP v3	64
SNMP Access Control Groups	65
How to Add a New SNMP v3 User	67

SNMP View Entry	68
SNMP Source Interface Configuration	68
SNMP Server Configuration	70
Time Ranges	71
Time Range Configuration	71
Entry Configuration	72
Logs.....	73
Event Log.....	73
Persistent Log.....	73
Logging Hosts	75
Log Configuration	76
Syslog Source Interface Configuration	77
SNTP	78
SNTP Global Configuration.....	79
SNTP Global Status	80
SNTP Server Configuration.....	80
Server Status	81
Source Interface Configuration	82
System Statistics.....	83
Switch Statistics.....	83
Port Summary Statistics	84
Port Detailed Statistics	85
Class of Service	85
How to Map IP DSCP	85
How to Apply Interface Shaping Rates	87
How to Configure CoS Interface Queues	87
Access Control List Rules.....	88
How to add an ACL Type and Identifier	89
How to Associate an ACL with an Interface	90
How to add ACLs to VLANs.....	93
ACL Statistics	94
ACL Rule Configurations.....	96
DiffServ	99
Global Configuration	99
Class Summary	100
Class Configuration	101
Policy Summary.....	104
Policy Configuration	104
Service Summary.....	106
Auto VoIP Configuration	106
Auto VoIP Global Configuration.....	107
How to Add OUIs.....	107
How to Configure OUI-Based Auto VoIP Priority	109
How to Configure Protocol-Based Auto VoIP Priority	109
802.1p (Priority Mapping)	112

Warranty & Legal information 113

FCC statement

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Changes or modifications not expressly approved by Control4 could void the user's authority to operate the equipment. Shielded CAT5e or better cables are required in order to comply with the FCC Rules part 15 limits for a Class B digital device.

Introduction

To accommodate residential networking needs, Pakedge offers five residential cloud-managed switch models: MS-1212, MS-2400, MS-2416, MS-2424, MS-4424. This all-new switch series offers low- to high-capacity switches that can be used on anything from a large to small home network.

With key Layer 2 and Layer 3 managed switch functionality, these devices are best suited for high-end multimedia and control applications.

Switches

Name	SKU
Pakedge L3 Managed Switch, 12 1G PoE+ 190W, 2 10G SFP+	MS-1212
Pakedge L3 Managed Switch, 24 1G, 2 10G SFP+	MS-2400
Pakedge L3 Managed Switch, 24 1G 16 PoE+ 245W, 2 10G SFP+	MS-2416
Pakedge L3 Managed 24 Port Switch 24 Ports PoE+ 2 10G SFP+	MS-2424
Pakedge L3 Managed Switch, 44 1G 24 PoE+ 370W, 4 10G SFP+	MS-4424

Switch specifications*

Managed switch SKU	Total # of ports	Ports with no PoE support	Ports with PoE+	Power budget	SFP+ ports
MS-1212	12	-	12 ports	190W	(2) 10G ports
MS-2400	24	24 ports	-	-	(2) 10G ports
MS-2416	24	-	16	245W	(2) 10G ports
MS-2424	24	-	24	370W	(2) 10G ports
MS-4424	44	-	24	370W	(4) 10G ports

*For a full list of specifications, see the data sheet at pkdgc.co/ms-ds.

Technical Support

Pakedge is committed to providing you with exceptional support on all of our products. If you want to speak with one of our representatives, contact us at:

Email: support@pakedge.com

Phone: **650-385-8703**

Visit our website for up-to-date support information at www.pakedge.com.

Be prepared to provide your product's model and serial number. Your model and serial numbers are printed on a label located on the electronic housing.

Installing

For installation procedures, refer to the *Quick Start Guide* that came with the switch or go to pkdge.co/ms-qsg. You can also visit the Dealer Portal for current manuals and quick start guides.

For rack installation, make sure that the amount of air flow required for safe operation of the equipment is not compromised.

Caution: If you install the switch in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room temperature. Make sure you install the equipment somewhere within the recommended temperature range. For free-standing installation, make sure that the switch has at least 3.75 cm (1.5 in.) of clearance on each side to allow for adequate air flow and cooling.

Getting to know your switch

This manual outlines the steps for configuring the web user interface settings for the Pakedge MS Series and can be used for the following products: MS-1212, MS-2400, MS-2416, MS-2424, and MS-4424.

Package contents:

- Switch
- AC adapter
- Ethernet cable
- Rack mount set
- Quick Start Guide



Front panel

LED Type	LED Color	LED Definition
Power LED	Blue	<ul style="list-style-type: none"> • Solid Blue: Device is on • Flicker Blue: Device is booting • Off: Device is off
PoE/Ethernet port LED	Blue/Amber	<ul style="list-style-type: none"> • Solid Blue: No Data is Transmitting • Flicker Blue: Data is Transmitting • Off: Link Down • Solid Amber: PoE is Powering, No Data is Transmitting • Flicker Amber: PoE is Powering and Data is Transmitting
SFP Port LED	Blue	<ul style="list-style-type: none"> • Solid Blue: No Data is Transmitting • Flicker Blue: Data is Transmitting • Off: Link Down

Back panel



Reset button press	Result
>5 seconds <10 seconds	On button release between 5 and 10 seconds: Set login username/password to default
>=10 seconds	On button release after 10 seconds: Revert to firmware default configurations

Accessing the switch

To access the switch's interface:

1. Connect the managed switch to a power source. The PWR LED lights up and the fans start.
2. Connect the switch to the network or directly to the router. Connect your computer to the same network.
3. Navigate to the network router in order to find the DHCP table. Look for the host name matching the model and MAC address of the switch and note the corresponding IP address obtained by the switch.
4. Navigate to the IP address listed in the router DHCP table for the switch.
5. Enter the Username and Password. The default username is **admin** and the password is **password**.

Important: You must change this default username and password.

Navigating the switch

When you log in to the switch, you will see seven tabs: Overview, Connections, Configure, Interfaces, Backup, Logs, and Advanced.



Click a tab to configure and start monitoring your switch. See below for a summary of features on each tab.

Tabs

Tab	Summary	Sub-categories
Overview	Quick view of switch status and critical settings.	n/a

Connections	Displays a list of connected clients.	n/a
Configure	Specifies device's network information (username, device name/location) and network protocol (DHCP or Static).	n/a
Interfaces	Access and manage settings for the switch's physical and virtual interface settings.	Port, VLAN, PoE
Backup	Save a configuration (backup) and then restore a configuration file.	
Logs	Displays a sortable record of system events affected by the switch.	n/a
Advanced	Less often used or more complex configuration settings. Perform maintenance, view statistics, and configure settings for various services and protocols (IGMP Snooping, STP, LLDP, etc.).	<ul style="list-style-type: none"> • Firmware • IGMP Snooping • IGMP Snooping Querier • Multicast Forwarding Database • Spanning Tree

Tab layouts

When you click on a tab, most will display a table.

This table lets you monitor, edit, and add specific switch settings.

PoE Add/Edit

⌂
Port Configuration
General
Statistics
Details
...

View

Enable	Interface	Name	Priority	Power Mode	Power Limit Type	Power Limit
<input checked="" type="checkbox"/>	0/1		Low	at30W	User	30000
<input checked="" type="checkbox"/>	0/2		Low	at30W	User	30000

Tiles and sub-tabs

If a tab has several sub-categories, it is divided into Tiles and Sub-tabs.

The screenshot shows the 'Interfaces' tab selected. It contains three tiles: 'Port' (Settings specific to physical switch port interfaces), 'VLAN' (Configurations for Layer 2 VLANs), and 'PoE' (Power over Ethernet settings and information). The 'PoE' tile is expanded to show a sub-tab menu with 'Port Configuration', 'General', 'Statistics', and 'Details'. Below this is a table with columns: Enable, Interface, Name, Priority, Power Mode, and Power Limit Type. Two rows are visible, both with 'On' status, '0/1' and '0/2' interfaces, 'Low' priority, 'at30W' power mode, and 'User' power limit type.

On these tabs, select a tile and sub-tab to view its tables.

Table content

From the open table, monitor, edit, or add specific switch settings.

This screenshot shows the 'PoE' configuration page. The 'Port Configuration' sub-tab is selected. There is an 'Add/Edit' button and a menu icon (three dots) in the top right. The table below has columns: Enable, Interface, Name, Priority, Power Mode, Power Limit Type, and Power Limit. Two rows are visible, both with 'On' status, '0/1' and '0/2' interfaces, 'Low' priority, 'at30W' power mode, 'User' power limit type, and '30000' power limit.

The rest of the guide outlines steps for configuring the settings on each tab.

Viewing, adding, and editing

If a table allows for editing, a **More** (⋮) icon displays above the table.

Enable	Interface	Name	Type	Physical Mode	Physical Status	Auto Negotiate Capabilities
<input checked="" type="checkbox"/>	0/1		Normal	Auto	Unknown	10h10f100h100f1000f
<input checked="" type="checkbox"/>	0/2		Normal	Auto	Unknown	10h10f100h100f1000f
<input checked="" type="checkbox"/>	0/3		Normal	Auto	Unknown	10h10f100h100f1000f

To change a switch setting, access a tab, click its **More** (⋮) icon, then click **Add**, **Edit**, or **Delete**.

Pagedge MS-1212

Overview
Connections
Configure
Interfaces
Backup
Logs
Advanced

Edit Password

Current Password

Complete the dialog, then click **Apply** (at the top of the page) to finalize your changes.

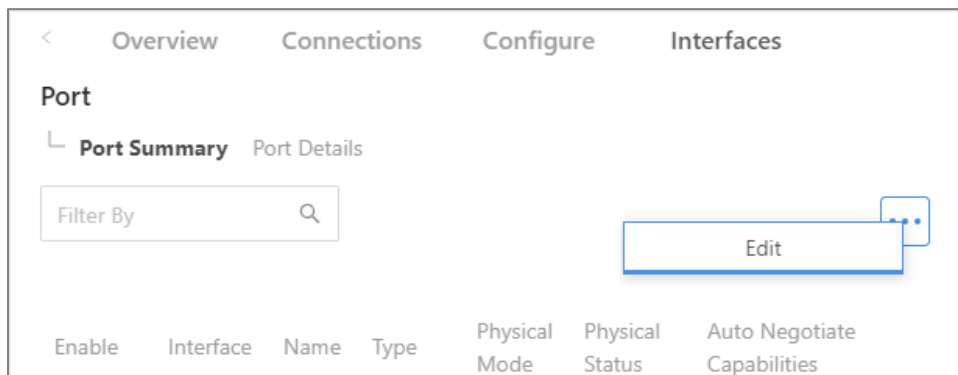
Important! Changes will **not** be saved until you click **Save** in the dialog and **Apply** at the top of the page.

Editing multiple items

On many tabs, you can edit several items at once.

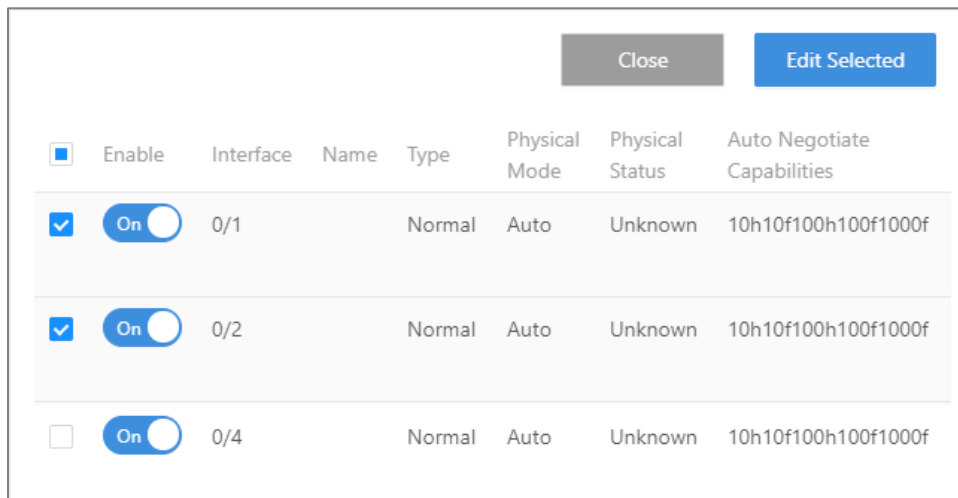
To edit multiple items:

1. Log in to the switch. Navigate to the desired tab (or sub-tab).
2. From the tab, select the **More** (⋮) icon (upper right) and click **Edit**.



An “edit” check box appears next to each item

3. Select the “edit” checkbox next to each item you want to edit, then click **Edit Selected**.



Caution: Editing multiple items requires caution. Be sure the correct items are selected before making changes.

4. Complete the dialog and click **Save**, then click **Apply** at the top of the page.
5. Designated changes are applied to the selected items.

Configure

The first time you log in, you are brought to the *Configure* tab.

Here you must change your username and password (required) and specify the device's network information and network protocol.

- *Edit Password, Edit Username*
 - The first time you log in, you must change these from the defaults (“admin” and “password”) to new credentials.
- *General Device Information*
 - **Friendly Device Name:** Give the switch a descriptive name to identify it on its web interface screen.
 - **Device Location:** Describe the physical location of the switch here.
 - **Device Notes:** List any other useful information about the switch.
 - **Time Zone:** Select the time zone used for the switch’s event logs.
- *LAN*

Mode: Select **DHCP** or **Static**.

- *DHCP:* If you selected **DHCP**, the following fields are read only.
- *Static:* If you selected **Static**, complete the following fields:
 - **IP Address:** Enter the IP address for the switch’s local network. (For a DHCP network, this field is read-only.)
 - **Subnet Mask:** Enter the switch’s subnet mask. (For a DHCP network, this field is read-only.)
 - **DHCP Start/End:** Assign the first and last IP addresses you would like to use in the DHCP range. Each interface can have up to four DHCP.

- **Primary DNS Server:** Assign the primary DNS server.

Overview

The *Overview* tab gives you a quick view of the switch's status and critical settings.

The screenshot displays the 'Overview' tab for a Pakedge MS-1212 switch. At the top, there are navigation tabs: Overview, Connections, Configure, Interfaces, Backup, Logs, and Advanced. The main header shows the device name 'Pakedge MS-1212' and a location field. Below this, the 'Current Status' is 'Up (for 1 Days 3 Hours 52 Minutes)'. There are two buttons: 'Update Firmware' and 'Restart Device'. A table lists various services and their data:

Service	Service Name	Service Data
ActiveInterface	ActiveInterface	2/14
PoeBudget	PoeBudget	0W of 190W(0% utilized)
CpuUsage	CpuUsage	27%
MemoryUsage	MemoryUsage	42%
Uptime	Uptime	1 Days 3 Hours 52 Minutes
Firmware	Firmware	0.01.0.100035
SerialNumber	SerialNumber	TW [redacted]
v lans	v lans	1
STP	STP	Root Status:False; BridgeID: [redacted]

On this page, you will find information on the current firmware version, number of active ports on the switch, system-level PoE utilization, CPU and memory usage, uptime, serial number, and more.

If there is new firmware available for the switch, you will see a message alerting you with an option to download it.

- **Notifications:** System notifications display at the very top of the tab. This example shows a firmware update is available.
- **Device Name:** The device name (assigned in the *Configure* tab) appears here.
- **IP address and MAC address:** The device's assigned IP address and system MAC address is shown here.
- **Location:** Displays the configured "Location" of the device.
- **Current Status:** Shows the switch's up/down status.
- **Update Firmware:** Click to open the *Update Firmware* screen (also accessible under the *Advanced* tab). The screen also displays the firmware's release notes.
- **Restart device:** Click to restart (power cycle) the switch. It happens immediately, with no confirmation dialog.
- **Services:** Displays the status of current services and settings and indicates with an icon whether the service or setting is optimally configured.

Connections

The *Connections* tab displays a list of connected clients.

Overview Connections Configure Interfaces Backup Logs Advanced

Packedge MS-1212

Packedge MS-1212

Update Firmware Restart Device

Physically Connected Clients

Interface	Name	Link Status	IP Address	MAC Address	Up Time	PoE	VLAN	TX/s	RX/s
0/1		down				0W	1	0.0 b	0.0 b
0/2		down				0W	1	0.0 b	0.0 b
0/3		down				0W	1	0.0 b	0.0 b
0/4		down				0W	1	0.0 b	0.0 b
0/5		down				0W	1	0.0 b	0.0 b
0/6		down				0W	1	0.0 b	0.0 b
0/7		1G	192.168.1.127		01:03:49	0W	1	12.2 Kb	360.0 b

Click any column heading to sort the list by that field. Available fields are:

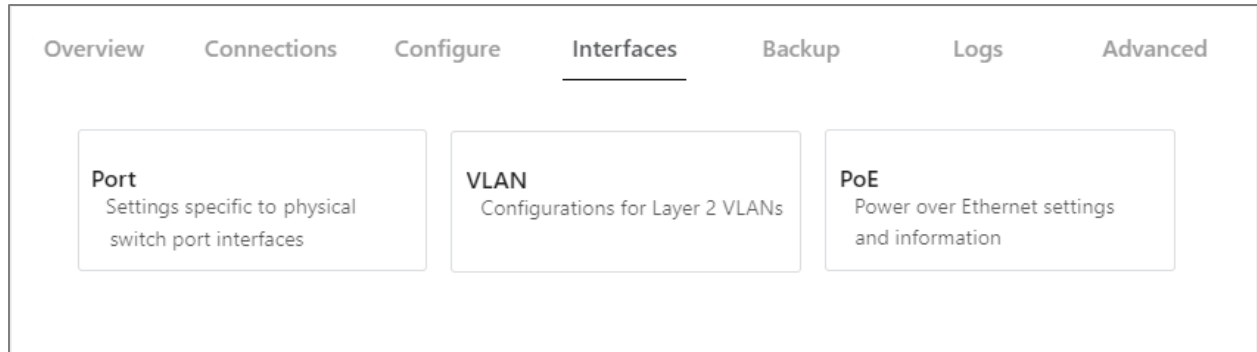
- **Interface:** Physical interface on the switch
- **Name:** Device name assigned by the user
- **Link Status:** Link speed/status of the interface
- **IP Address:** IP address of connected device (learned by LLDP)
- **MAC Address:** MAC address of connected device (learned by LLDP)
- **Up Time:** Up time for each interface
- **PoE:** PoE usage per interface
- **VLAN:** VLAN configured on the port
- **TX:** Traffic transported from the port
- **RX:** Traffic received by the port

Interfaces

The *Interfaces* tab provides management features for the switch's physical and virtual interfaces and PoE settings (port, VLAN, and PoE settings).

Tiles

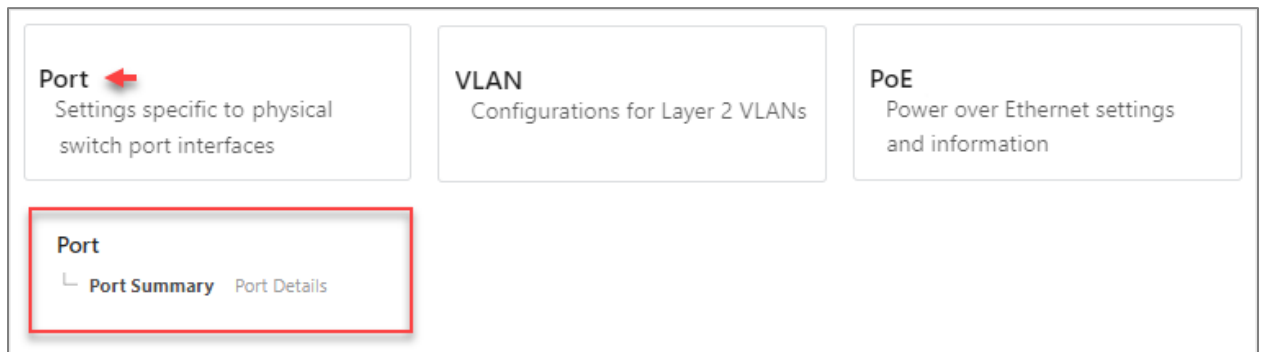
The *Interfaces* tab opens to three tiles: *Ports*, *VLANs*, and *PoE*.



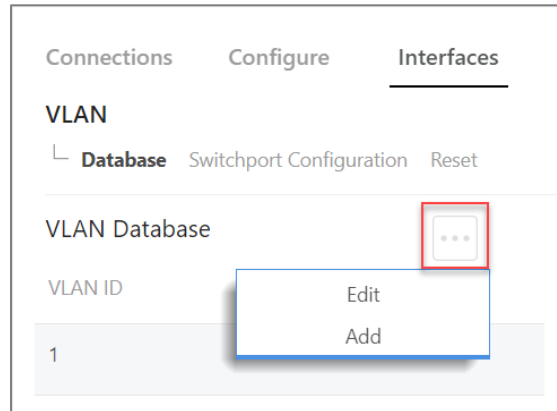
Add or edit an interface

To add or edit an interface:

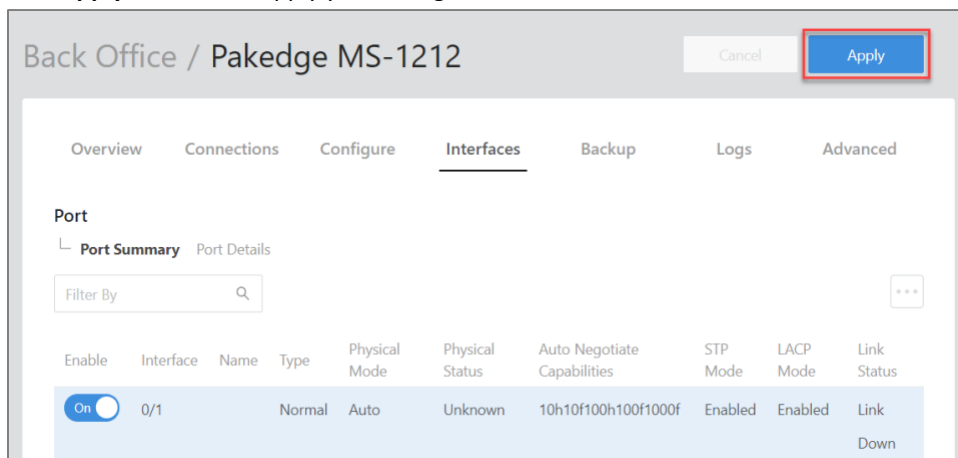
1. Log in to the switch and click the **Interfaces** tab, then click a tile (Port, VLAN, PoE).



2. From the tile, select a sub-tab (*Port>Port Summary*), then click the **More** (⋮) icon.
 - a. To edit, click the **More** (⋮) icon and click **Edit**.
 - b. To add, click the **More** (⋮) icon and click **Add**.



3. Make any adjustments, then click **Continue**.
4. Click **Apply** to save and apply your changes.



Important! Your changes will not be saved until you click **Apply**.

Completing the dialog

Depending on the selected interface, you will see different editing options. See below for a summary of each tile.

Tiles

- **Port:** Manage the port summary and port details.
- **VLAN:** Manage the VLAN database, switchport configurations, or reset the VLAN.
- **PoE:** Manage PoE settings: Port Configuration, General, Statistics, and Details.

Ports

To access Ports, go to **Interfaces > Ports**.

On the **Interface** tab's first tile, **Ports**, view or manage physical switch port settings.

Port

Port Summary Port Details

Filter By

Enable	Interface	Name	Type	Physical Mode	Physical Status	Auto Negotiate Capabilities	STP Mode	LACP Mode	Link Status
<input checked="" type="checkbox"/>	0/1		Normal	Auto	Unknown	10h10f100h100f1000f	Enabled	Enabled	Link Down
<input checked="" type="checkbox"/>	0/2		Normal	Auto	Unknown	10h10f100h100f1000f	Enabled	Enabled	Link Down
<input checked="" type="checkbox"/>	0/3		Normal	Auto	Unknown	10h10f100h100f1000f	Enabled	Enabled	Link Down
<input checked="" type="checkbox"/>	0/4		Normal	Auto	Unknown	10h10f100h100f1000f	Enabled	Enabled	Link Down

Choose from two sub-tabs:

- **Port Summary:** View or configure key port settings, including the port name, port status, enable/disable various modes, and configure autonegotiation.
- **Port Details:** View port information such as physical addresses, port list bit offset, and interface index.

Overview Connections Configure Interfaces

Port

Port Summary **Port Details**

Interface	Name	Physical Address	PortList Bit Offset	Interface Index
0/1			1	1
0/2			2	2
0/3			3	3

Click a sub-tab to access its settings.

Port Summary

To access Port Summary, go to **Interfaces > Ports > Port Summary**.

The first sub-tab is **Port Summary**.

From the **Port Summary** sub-tab, view or configure key port settings. Monitor port status, enable/disable various modes, and configure auto-negotiation and other settings.

Port

Port Summary
Port Details

Filter By

Enable	Interface	Name	Type	Physical Mode	Physical Status	Auto Negotiate Capabilities	STP Mode	LACP Mode	Link Status
<input checked="" type="checkbox"/>	0/1		Normal	Auto	Unknown	10h10f100h100f1000f	Enabled	Enabled	Link Down
<input checked="" type="checkbox"/>	0/2		Normal	Auto	Unknown	10h10f100h100f1000f	Enabled	Enabled	Link Down
<input checked="" type="checkbox"/>	0/3		Normal	Auto	Unknown	10h10f100h100f1000f	Enabled	Enabled	Link Down
<input checked="" type="checkbox"/>	0/4		Normal	Auto	Unknown	10h10f100h100f1000f	Enabled	Enabled	Link Down

Edit

To edit available *Port Summary* settings:

1. Log in to the switch, then click **Interfaces > Port > Port Summary**.
2. Click **More** () , then click **Edit**.
3. Check the box next to items you want to edit, then click **Edit Selected**.

Caution! When editing multiple ports, make sure the correct ports are selected before making changes.
4. Complete the dialog (see below).
5. In the dialog, click **Save**, then click **Apply** at the top of the page to save your changes.

Completing the dialog

For help completing the dialog, see the table below.

Fields below can be viewed, edited, or both.

Field	Function
Enable	Turns port on/off.
Interface	Identifies the port or link aggregation.
Name	Edit the name of an interface.
Type	Displays interface type.
Admin Mode (Enabled/Disabled)	When editing, use this field to enable or disable the interface's Administrative Mode . Note: If a port or LAG is administratively disabled, it cannot forward traffic.
Physical Mode (Auto Negotiate/ Speed)	Port speed and duplex mode. If the mode is Auto , the duplex mode and speed are set from the auto-negotiation process.
Auto Negotiate Capabilities	Indicates the list of configured capabilities for a port when Auto Negotiate is on.
Speed	If Auto Negotiate is turned off, Speed indicates default speed (in Mbps) allocated to the selected ports.
Physical Status	Indicates the port speed and duplex mode for physical interfaces. The physical status for LAGs is not reported.
STP Mode (Enable/Disable)	The Spanning Tree Protocol (STP) Administrative Mode associated with the port or LAG.
LACP Mode (Enable/Disable)	Shows the Administrative Mode of the Link Aggregation Control Protocol (LACP).
Link Status, Link Trap	Indicates whether the link is up or down. The link is the physical connection between the port or LAG and the interface on another device.
MTU	When editing, specify the MTU (Maximum Transmit Unit) of the interface.
Broadcast Storm Recovery Level	When editing, specify the broadcast storm control threshold for the port. Broadcast storm control limits the number of broadcast frames accepted and forwarded by the port. <ul style="list-style-type: none"> • Enable/Disable, then select a percentage or PPS. • Select None/Shutdown/Trap.
Multicast Storm Recovery Level	When editing, specify the multicast storm control threshold for the port. This setting limits the number of multicast frames accepted and forwarded by the port. <ul style="list-style-type: none"> • Enable/Disable, then select a percentage or PPS. • Select None/Shutdown/Trap.

Unicast Storm Recovery Level	<p>When editing, specify the unicast storm control threshold for the port. Unicast storm control limits the number of unicast frames accepted and forwarded by the switch.</p> <ul style="list-style-type: none"> • Enable/Disable, then select a percentage or PPS. • Select None/Shutdown/Trap.
------------------------------	---

Edit port names

You can edit the display name for each port on this page. Port names help distinguish one port from another (for example, Touch Screen, Camera, Controller).

To edit port names:

1. Log in to the switch.
2. Click **Interfaces > Port > Port Details**.
3. Click the **More** (⋮) icon and click **Edit**.
4. Select the check box next to items you want to edit, then click **Edit Selected**.

Caution! When editing multiple ports, make sure the correct ports are selected before making changes.
5. Enter the port's new name.
6. Click **Save**, then click **Apply** to save your changes.

Port Details

To access Port Details, go to **Interfaces > Ports > Port Details**.

Under Port Details, edit each port's name or view port information such as Physical Address, Port List Bit Offset, and Interface Index.

Interface	Name	Physical Address	PortList Bit Offset	Interface Index
0/1			1	1
0/2			2	2
0/3			3	3

VLAN

To access the VLAN tile, go to **Interfaces > VLAN**.

On the **Interface** tab's second tile, VLAN, you can configure Layer 2 VLANs.



Choose from three sub-tabs:

- **Database:** View active VLANs and create new VLANs.
- **Switchport Configuration:** View/edit each switchport Interface, Name, Switchport Mode, Native VLAN, and Tagged VLANs.
- **Reset:** Return VLAN configuration parameters to their default values.

Database

To access VLAN database information, go to **Interfaces > VLAN > Database**.

The first VLAN sub-tab is **Database**.

From the *VLAN Database* sub-tab, view, edit, or create active VLANs.

The screenshot shows the 'VLAN Database' sub-tab. It features a 'Filter Table By' input field and a table with columns 'VLAN ID' and 'Name'. A context menu is open over the table, showing 'Edit' and 'Add' options. The table contains the following data:

VLAN ID	Name
1	VLAN0002
2	VLAN0003
3	VLAN0003
4	VLAN0004

Create VLAN

To add a VLAN in the VLAN database:

1. Go to **Interfaces > VLAN > VLAN Database**.
2. On the upper right, click the **More** (⋮) icon.
3. Click **Add**.
4. Complete the dialog, then click **Apply** to activate the new VLAN.

Edit VLAN Data Base

To edit a VLAN in the VLAN database:

1. Go to **Interfaces > VLAN > VLAN Database**.
2. On the upper right, click the **More** (⋮) icon.
3. Click **Edit**.
4. Complete the dialog, then click **Apply** to save your work.

Completing the dialog

See below for help completing the *Add VLAN* dialog.

The screenshot shows a dialog box titled "Add VLAN". It has a close button in the top right corner. Below the title bar, there are two input fields. The first is labeled "VLAN ID or Range" and contains the number "2". The second is labeled "Name" and contains the text "VLAN 2". At the bottom of the dialog, there are two buttons: "Cancel" on the left and "Add" on the right.

Explanations

Field	Function
VLAN ID or Range	Add a new VLAN to the list of VLAN interfaces on the router.
Name	Enter a name to label the VLAN for identification.

Switchport Configuration

To access the VLAN switchport configuration, go to **Interfaces > VLAN > Switchport Configuration**.


The second VLAN sub-tab is *Switchport Configuration*.

Interface	Name	Switchport Mode	Access VLAN	Native VLAN	Allow VLANs
0/1		Access	1	1	1-4093
0/2		Access	1	1	1-4093
0/3		Access	1	1	1-4093
0/4		Access	1	1	1-4093

From the *Switchport Configuration* sub-tab, assign switchport settings per port. Select **Switchport Mode Access** or **Trunk**.

Edit Switchport Configuration

To edit Switchport Configuration:

1. Select **Interfaces > VLAN > Switchport Configuration**.
2. Click the **More** () icon, then click **Edit**.
3. Select the check box next to items you want to edit, then click **Edit Selected**.
Caution! Before making changes, make sure the correct ports are selected.
4. Complete the dialog.
5. Click **Save**, then click **Apply** to save your changes.

Completing the dialog

See below for help completing the *Edit Switchport Configuration* dialog.

Edit Switchport Configuration ✕

Switchport Configuration Selected: 2,3

Switchport Mode

Access ▾

Access VLAN

1

Priority

0

Cancel

Save

Explanations: Switchport Configuration dialog

Title	Function	Default option
Interface	Interface associated with the rest of the data in the row. <i>Note: When editing, this field identifies all interfaces that are being configured.</i>	
Name	Name associated with the Interface on the row.	
Switchport Mode	The switchport mode of the interface, which is one of the following: <ul style="list-style-type: none"> • Access: Access mode is suitable for ports connected to end stations or end users. Access ports participate only in one VLAN. They accept and transmit untagged packets. • Trunk: Trunk mode is intended for ports that are connected to other switches. Trunk ports can participate in multiple VLANs and accept both tagged and untagged packets. 	Access
Native VLAN	The VLAN ID assigned to untagged or priority tagged frames received on this port in either Access or Trunk modes. This value is also known as the Port VLAN ID (PVID). In a tagged frame, the VLAN is identified by the VLAN ID in the tag.	1

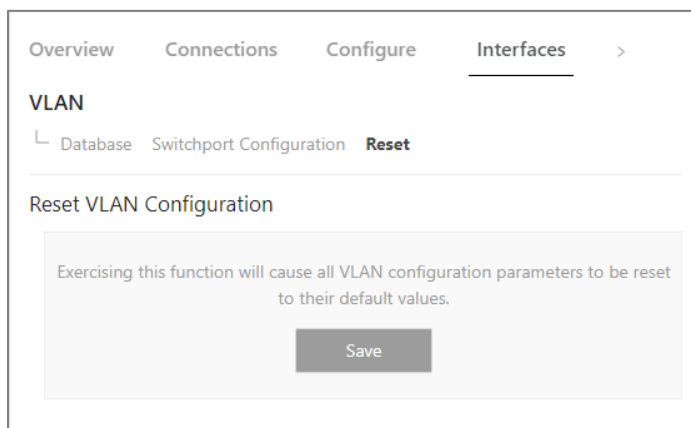
Tagged VLANs	The VLAN ID(s) allowed to communicate on this port using 802.1q tagging as well as Untagged. The Native VLAN (PVID) should always be included in this setting along with Tagged VLANs that are to be allowed on the port.	1
Priority	Default 802.1p priority assigned to untagged packets arriving at the interface.	0

VLAN Subpage: Reset

To access the VLAN reset feature, go to **Interfaces > VLAN > Reset**.

From the *Reset* sub-tab, click the **Reset** button to return the VLAN configuration parameters to their default values.

1. Go to **Interfaces > VLAN > Reset** to reset VLAN configurations.



2. Click **Save** to reset all VLAN configuration parameters to their default values.

PoE

To access the PoE tile, go to **Interfaces > PoE**.

On the *Interface* tab's third tile, **PoE**, view and manage PoE (Power over Ethernet) settings.

The screenshot shows the PoE configuration page with the following structure:

- Navigation tabs: Overview, Connections, Configure, **Interfaces**, Backup
- Section: PoE
- Sub-tabs: **Port Configuration**, General, Statistics, Details
- Filter By: [Search box] [More options]
- Table with columns: Enable, Interface, Name, Priority, Power Mode, Power Limit Type, Power Limit

Enable	Interface	Name	Priority	Power Mode	Power Limit Type	Power Limit
<input checked="" type="checkbox"/>	0/1		Low	at30W	User	30000
<input checked="" type="checkbox"/>	0/2		Low	at30W	User	30000
<input checked="" type="checkbox"/>	0/3		Low	at30W	User	30000

Choose from four sub-tabs: *Port Configuration*, *General Settings*, *Statistics*, and *Details*.

- **Port Configuration:** View/configure key port settings.
 - *Enable the port. Select a port Name, Priority, Power Mode, Power Limit.*
- **General:** View/configure additional port settings.
 - *Set the port's System Threshold, enable/disable Power Management Mode and Traps.*
- **Statistics:** View only. *Monitor counters for key port statistics.*
 - *Counters: Overload Counter, Short Counter, Power Denied Counter, MPS Absent Counter, Invalid Signature Counter.*
- **Details:** View only. *View other port statistics.*
 - *View settings for each interface: Max Power, Class, Output Voltage/Current/ Power, Temperature, Status, and Fault Status.*

Port Configuration

To access PoE port configurations, go to **Interfaces > PoE > Port Configuration**.

The first PoE sub-tab is *Port Configuration*.

From the *Port Configuration* sub-tab, view/edit current port settings.

The screenshot shows the PoE configuration page with the following data:

Enable	Interface	Name	Priority	Power Mode	Power Limit Type	Power Limit
<input checked="" type="checkbox"/>	0/1		Low	at30W	User	30000
<input checked="" type="checkbox"/>	0/2		Low	at30W	User	30000
<input checked="" type="checkbox"/>	0/3		Low	at30W	User	30000
<input checked="" type="checkbox"/>	0/4		Low	at30W	User	30000

See below for an explanation of each setting.

Port Configuration settings

Setting	Function
Enable	Indicates whether PoE is enabled/disabled on the interface.
Interface	Interface associated with the data in the row.
Name	Name associated with the Interface on the row.
Priority	Priority of the port when allocating available power.
Power Mode	When enabled, the port supports the PoE+ power standard, which allows for providing up to 30W of power.
Power Limit Type	Type of power limiting used for the port.
Power Limit (mWatts)	Specifies power limit for the port. <i>Displays only when Power Limit Type is set to User.</i>

Edit Port Configuration settings

To edit a Port Configuration setting:

1. Select **Interfaces > Port > PoE > Port Configuration**.
2. At the top of the page, click the **More** (⋮) icon and click **Edit**.
3. Select the check box next to items you want to edit, then click **Edit Selected**.
Caution: Before making changes, make sure the correct ports are selected.
4. Complete the dialog.
5. In the dialog, click **Save**, then click **Apply** to save your changes.

Completing the dialog

See below for help completing the *Edit Port Configuration* dialog.

Explanations: Edit Port Configuration dialog

Title	Function	Input values/ validation	Default
Enable	Indicates whether PoE is administratively enabled or disabled on the interface.	<ul style="list-style-type: none"> • Enable • Disable 	Enable
Priority	Priority of the port when allocating available power.	<ul style="list-style-type: none"> • Critical • High • Medium • Low 	Low
Power Mode	When enabled, the port supports the PoE+ power standard, which allows for providing up to 30W of power.	<ul style="list-style-type: none"> • Disable • Legacy • af15W • at30W 	at30W
Power Limit Type	Type of power limiting used for the port.	<ul style="list-style-type: none"> • None • Class • User 	User

Power Limit (mWatts)	Power limit for the port, which can be specified. This field displays only when <i>Power Limit Type</i> is set to <i>User</i> .	3000 to 30000	30000
Detection Type	Protocol(s) that can be used to detect the presence of a PD when connected to a PoE port. This setting should only need to be modified for compatibility with old endpoint devices.	<ul style="list-style-type: none"> • Legacy • 4Pt-Dot3af • 4Pt-Dot3af+Legacy • 2Pt-Dot3af • 2Pt-Dot3af+Legacy • None 	4Pt-Dot3af
Timer Schedule	The time range from the list of time ranges configured on the system.	None	None

General

To access general PoE settings, go to **Interfaces > PoE > General**.

From the *PoE General* sub-tab, view or configure additional port settings.

PoE

↳ Port Configuration **General** Statistics Details

Firmware Version 2.0.2.8

Operational Status off

Total Power Available: 190000 mWatts

Threshold Power: 171000 mWatts

Consumed Power: 0

System Usage Threshold

90%

Power Management Mode

Dynamic ▼

Port Auto Reset Mode

Traps

●

On the *General* sub-tab, edit the port's *System Threshold* or enable/disable *Power Management Mode* and *Traps*.

Edit PoE General Settings

To adjust a setting on the *General* sub-tab:

1. Go to **Interfaces > PoE > General**.
2. Complete the fields.
3. To save your changes, click **Apply**.

Explanations: PoE General setting

Title	Function
Operational Status	The current status of the switch PoE functionality.
Total Power Available	The total power in mW that can be provided by the switch.
Threshold Power	This value is determined by the configurable System Usage Threshold percent.
Consumed Power	The amount of power in mW currently being consumed by connected PoE devices.
System Usage Threshold (%) <i>Click to type.</i>	A percentage of the total power available. This percentage determines the <i>Threshold Power</i> . The Threshold Power is the maximum amount of the PoE power budget that will be allocated from the switch.
Power Management Mode <i>Select Static or Dynamic.</i>	The method by which the PoE controller determines supplied power.
Port Auto Reset Mode <i>Select/unselect.</i>	Select/Unselect Auto Reset Mode.
Traps <i>Slide to enable/disable.</i>	Enable/Disable traps.

Statistics (read only)

To access PoE statistics, go to **Interfaces > PoE > Statistics**.

From the third *PoE* sub-tab, **Statistics**, monitor counters for key PoE port activities.

Overview	Connections	Configure	<u>Interfaces</u>	Backup	Logs	Advanced
PoE						
└ Port Configuration General Statistics Details						
Interface	Name	Overload Counter	Short Counter	Power Denied Counter	MPS Absent Counter	Invalid Signature Counter
0/1		0	0	0	0	0
0/2		0	0	0	0	0
0/3		0	0	0	0	0
0/4		0	0	0	0	0

- **Counters available for monitoring:**
Overload Counter, Short Counter, Power Denied Counter, MPS Absent Counter, Invalid Signature Counter.

No editing features are available on this page.

Explanations

Title	Function
Refresh	Click to refresh PoE port statistics.
Interface	Interface associated with the rest of the data in the row.
Name	The name associated with the Interface on the row.
Overload Counter	Number of times there has been a power overload.
Short Counter	Number of times there has been a short-circuit condition.
Power Denied Counter	Number of times the powered device has been denied power.
MPS Absent Counter	Number of times power has stopped because the powered device was not detected.
Invalid Signature Counter	Number of times an invalid signature was received. Signature detection is a stage in detecting the presence of a powered device, where a resistance value on the powered device is expected to be found within a particular range.

Details (read only)

*To access PoE details, go to **Interfaces > PoE > Details**.*

From the fourth *PoE* sub-tab, **Details**, monitor additional PoE information for each interface.

Overview	Connections	Configure	Interfaces	Backup	Logs	Advanced				
PoE										
└ Port Configuration General Statistics Details										
Interface	Name	High Power	Max Power (mWatts)	Class	Output Voltage (Volts)	Output Current (mAmps)	Output Power (mWatts)	Temperature (C)	Status	Fault Status
0/1		Enabled	30000	Not Defined	0	0	0	31	Searching	No Error
0/2		Enabled	30000	Not Defined	0	0	0	31	Searching	No Error
0/3		Enabled	30000	Not Defined	0	0	0	31	Searching	No Error
0/4		Enabled	30000	Not Defined	0	0	0	31	Searching	No Error

View each interface's *Max Power*, *Class*, *Output Voltage/Current/ Power*, *Temperature*, *Status*, and *i*.

No editing features are available on this page.

Explanations

Title	Input type	Function
Interface	View Only	Interface associated with the rest of the data in the row.
Name	View Only	User-assigned name for the interface on the row.
High Power	View Only	Indicates whether High Power mode is enabled or disabled.
Max Power (mWatts)	View Only	Displays the configured power limit.
Class	View Only	If <i>Power Limit Type</i> is set to <i>Class</i> , this field displays the class of the connected device, as learned in LLDP messages.
Output Voltage (Volts)	View Only	Voltage being applied to the connected device.
Output Current (mAmps)	View Only	Current (in mA) being drawn by the powered device.
Output Power (mWatts)	View Only	Power (in mW) being drawn by the connected device.
Temperature (°C)	View Only	Temperature (in °C) measured at the PoE port.
Status	View Only	Current powering status of the interface.
Fault Status	View Only	Fault information (if any).

Backup

The *Backup* tab allows you to save a configuration (backup) and restore the configuration file.

- **Save Configuration:** Click to save a file that contains all of this switch's settings.
- **Choose File:** Click to select a saved configuration backup file to use for restoring settings.
- **Restore:** Click to restore switch settings using the selected configuration backup file.

Logs

The *Logs* tab displays a record of system events affected by the switch. The events are categorized by severity, timestamp, component, and details.

Severity	Log Time	Component	Detail
info	Jan 16 15:44:58	USER_MGR	[INFO] HTTPS Session 25 started for user support connected from 10.11.110.146
info	Jan 16 15:44:43	TRAPMGR	[NOTE] HTTPS session : Login to the switch is not successful, User ID: support
info	Jan 16 15:44:43	USER_MGR	[INFO] HTTPS session : User support couldn't login to the switch due to unsuccessful authentication
info	Jan 16 15:38:36	USER_MGR	[INFO] HTTPS Session 24 ended for user support connected from 10.11.110.146
info	Jan 16	USER_MGR	[INFO] HTTPS Session 24 started for user support connected from 10.11.110.146

To change the number of log items displayed:

1. In the **Logs** tab, click the **Options** (⋮) button, then click the number of rows to display at one time.

To clear or refresh the log:

1. In the **Logs** tab, click the **Options** (⋮) button, then click **Clear Logs** or **Refresh Logs**. The log file is cleared or refreshed.

To download the log:

1. In the **Logs** tab, click the **Options** (⋮) button, then click **Download Logs**.
2. Accept the default **logs.txt** filename or type a new name, then navigate to the destination folder and click **Save**. The log file is saved.

Tip: When troubleshooting, save log files often, using filenames in a date/timestamp format, for example, **2020-06-09-1013a.txt**.

Overview	Connections	Configure	Interfaces	Backup	Logs	Advanced
Filter By <input type="text"/>						⋮
Severity	Log Time	Component	Detail			
Minor	Oct 11 20:43:47	BONJOUR	[INFO] Bonjour received Hostname CHANGED event			
Minor	Oct 11 20:43:47	BONJOUR	[INFO] Bonjour received Hostname CHANGED event			
Major	Oct 11 20:43:46	DHCP_CLI	[INFO] set_variable_tag : Tag already set with size(22)			
Debug	Oct 11 20:39:43	CLI_WEB	[NOTE] Telnet send did not complete. Reason Socket operation on non-socket.			
Critical	Oct 11 20:39:42	USER_MGR	[INFO] HTTP Session 14 started for user admin connected from 10.21.1.24			

Reset to factory default settings

While setting up or troubleshooting, you may need to reboot the switch or restore it to its factory default settings.

Caution: Do *not* power off the switch during a factory reset.

Reset using the interface

To only restart the switch, maintaining all settings:

1. In the **Overview** or **Connections** tab, click **Restart Device**. The switch restarts.

To reset to factory default settings, deleting all user settings:

Caution: Performing this reset will delete all of your settings on the switch.

1. In the **Overview** or **Connections** tab, click **Reset to Default**.
2. Click **Factory Default**, then click **Yes**. The switch restarts with default configurations.

Reset using the physical RESET button

Your switch has a recessed RESET button accessible through a pinhole next to the Ethernet port underneath the switch.

To only reboot the switch, maintaining all settings:

1. While power is connected, insert a narrow, pointed object (such as a straightened paper clip) into the hole.
2. Press and release the button.

To reset to factory default settings, deleting all user settings:

Caution: Performing this reset will delete all of your settings on the switch.

1. While power is connected, insert a narrow, pointed object (such as a straightened paper clip) into the hole.
2. Press and hold the button for at least **ten** seconds, then release it.

Advanced

From the **Advanced** tab, perform advanced tasks.

Perform maintenance, view statistics, and configure settings for various services and protocols.

Below is a summary of each feature available on the **Advanced** tab.

Advanced feature	Summary
IGMP Snooping	Manage, configure, and monitor <i>IGMP Snooping</i> settings per VLAN interface.
IGMP Snooping Querier	Manage, configure, and monitor <i>IGMP Snooping Querier</i> settings. Set the query interval, configure VLAN query settings, and view VLAN status.
Unregistered Multicast Behavior	Configure the behavior of Unregistered multicast traffic when <i>IGMP Snooping</i> is enabled. Allows for exception rules to be created allowing some multicast groups to continue to flood while the rest are set to <i>Drop</i> .
Spanning Tree Protocol	Manage, configure, and monitor STP activity for <i>MST</i> , <i>MST Ports</i> , and <i>CST Ports</i> .
IP IGMP	Allows ports to be configured as a dedicated network for IGMP Snooping. Ports become a routable interface with a dedicated IP address and IGMP Snooping is isolated to the individual port and the network below that port.
IP Multicast	Configure IP Multicast Routing using Protocol-Independent Multicast – Sparse Mode (PIM-SM) to make the switch act as a multicast router for the network.
IP Multicast Information	Monitor IP Multicast Routing Information for Elected Bootstrap Router, Rendezvous Point Mapping, and Multicast Route Table.
Firmware	Update the switch firmware for functionality improvements and feature enhancements.

Configuring IGMP Snooping

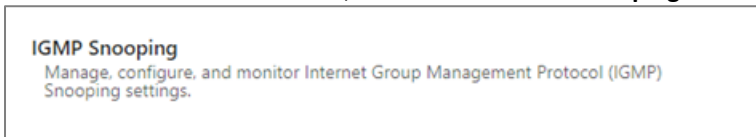
Internet Group Management Protocol (IGMP) Snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch. Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255.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

A traditional Ethernet network may be separated into different network segments to prevent placing too many devices onto the same shared media. Bridges and switches connect these segments. When a packet with a broadcast or multicast destination address is received, the switch will forward a copy into each of the remaining network segments in accordance with the IEEE MAC Bridge standard. Eventually, the packet is made accessible to all nodes connected to the network.

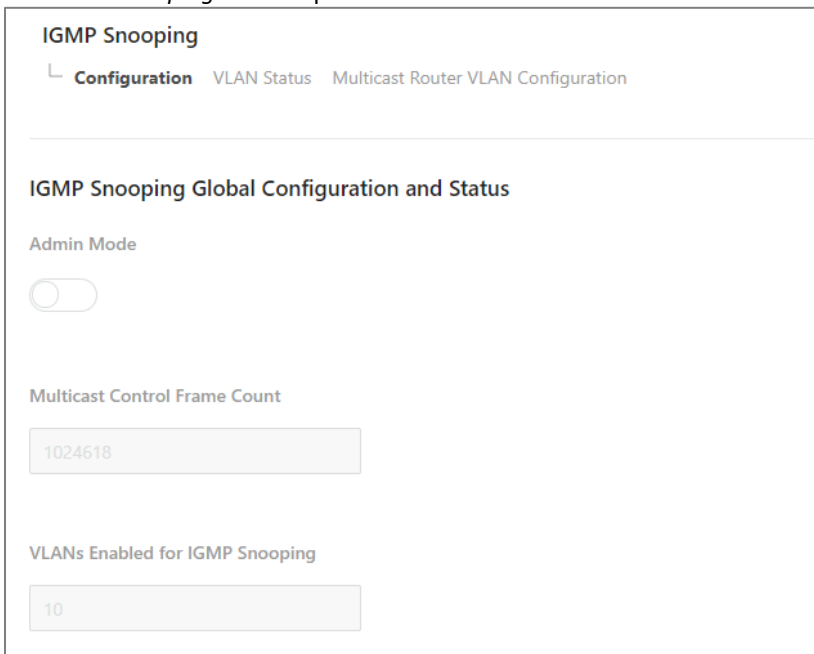
This approach works well for broadcast packets that are intended to be seen or processed by all connected nodes. In the case of multicast packets, however, this approach could lead to less efficient use of network bandwidth, particularly when the packet is intended for only a small number of nodes. Packets will be flooded into network segments where no node has any interest in receiving the packet. While nodes will rarely incur any processing overhead to filter packets addressed to un-requested group addresses, they are unable to transmit new packets onto the shared media for the period of time that the multicast packet is flooded. The problem of wasting bandwidth is even worse when the LAN segment is not shared, for example in Full Duplex links. Allowing switches to snoop IGMP packets is a creative effort to solve this problem. The switch uses the information in the IGMP packets as they are being forwarded throughout the network to determine which segments should receive packets directed to the group address.

To access the *IGMP Snooping* configuration menu:

1. Click the switch's **Advanced** tab, then click the **IGMP Snooping** tile.



The *IGMP Snooping* screen opens.



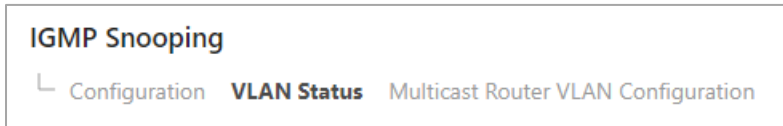
Field	Description
Admin Mode	Toggle the Admin Mode button to Enable or Disable IGMP Snooping globally. The default is <i>disabled</i> . This must be enabled before configuring IGMP Snooping per VLAN interface.
Multicast Control Frame Count	Shows the number of multicast control frames that have been processed by the CPU. This field is read only.
VLANs enabled for IGMP Snooping	Lists the VLANs currently enabled for IGMP snooping. This field is read only.

Enabling VLAN IGMP snooping status

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

To enable and view VLAN IGMP snooping status:

1. In the *IGMP Snooping* screen, click the **VLAN Status** tab.



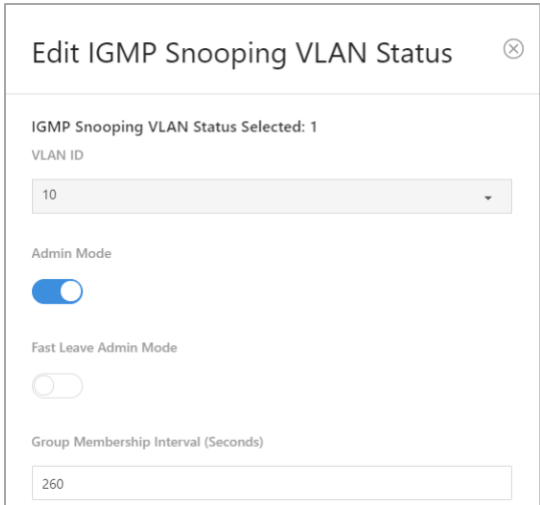
The *IGMP Snooping VLAN Status* screen opens.

IGMP Snooping VLAN Status								...
VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval (Seconds)	Max Response Time (Seconds)	Multicast Router Expiration Time (Seconds)	Report Suppression Mode	Action	
10	<input checked="" type="checkbox"/>	Disabled	260	10	0	Disabled	...	

Field	Description
VLAN ID	The VLAN associated with the rest of the data in the row. Only VLANs that have been configured on the system and are not already enabled for IGMP snooping appear in the list. When modifying IGMP snooping settings, this field identifies the VLAN that is being configured.
Admin Mode	The administrative mode of IGMP snooping on the VLAN. IGMP snooping must be enabled globally and on a VLAN for the VLAN to be able to snoop IGMP packets to determine which network segments should receive multicast packets directed to the group address.
Fast Leave Admin Mode	The administrative mode of Fast Leave on the VLAN. If <i>Fast Leave</i> is enabled, the VLAN can be immediately removed from the Layer 2 forwarding table entry upon receiving an IGMP leave message for a multicast group without first sending out MAC-based general queries.
Group Membership Interval (Seconds)	The number of seconds the VLAN should wait for a report for a particular group on the VLAN before the IGMP snooping feature deletes the VLAN from the group.
Max Response Time (Seconds)	The number of seconds the VLAN should wait after sending a query if does not receive a report for a particular group. The specified value should be less than the Group Membership Interval.

Multicast Router Expiration Time (Seconds)	The number of seconds the VLAN should wait to receive a query before it is removed from the list of VLANs with multicast routers attached.
Report Suppression Mode	<p>The IGMPv1 and IGMPv2 report suppression mode. The device uses IGMP report suppression to limit the membership report traffic sent to multicast-capable routers. When this mode is enabled, the device does not send duplicate reports to the multicast router. Note that this mode is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports. The options are as follows:</p> <ul style="list-style-type: none"> • Enabled: Only the first IGMP report from all hosts for a group IGMP report is forwarded to the multicast routers. • Disabled: The device forwards all IGMP reports from all hosts in a multicast group to the multicast routers.

- To change the IGMP snooping settings for an IGMP-snooping-enabled VLAN, click the three-dot menu (...) next to the entry with the settings to change, then click **Edit**. The *Edit IGMP Snooping VLAN Status* screen opens.

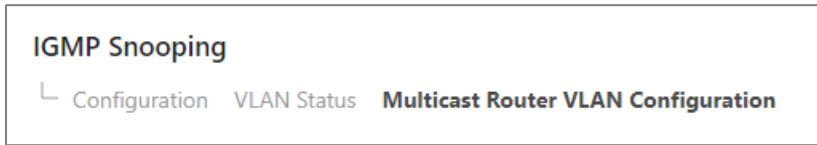


- Change the settings, then click **Save**.

Configuring multicast router VLANs

To configure multicast router VLANs:

1. In the *IGMP Snooping* screen, click the **Multicast Router VLAN Configuration** tab.



The *Multicast Router VLAN Configuration* screen opens.

Interface	Name	VLAN IDs	OPTIONS
0/1	MolP Controller		
0/2	MolP TX-215B3E		
0/3	Nvidia Shield		
0/4	Roku 4		
0/5	WA-2200-O		
0/6	RK-1		
0/7	MS-1212 - 1.110		

2. Click to select the interface to change, then click **Edit Selected**.

Filter By	Interface	Name	VLAN IDs
	<input checked="" type="checkbox"/>	0/1	MoIP Controller

The *Edit Multicast Router VLAN Configuration* screen opens.

Edit Multicast Router VLAN Configuration

Multicast Router VLAN Configuration Selected: 1

2 items 0 item

- 1
- 10

No Data

Cancel Save

Configuring IGMP Snooping Querier

To access the *IGMP Snooping Querier* configuration menu:

1. Click the switch's **Advanced** tab, then click the **IGMP Snooping** tile.



The *IGMP Snooping Querier Configuration* screen opens.

Field	Description
Admin Mode	When enabled, the IGMP snooping querier sends out periodic IGMP queries that trigger IGMP report messages from the switches that want to receive IP multicast traffic. IGMP snooping listens to these IGMP reports to establish appropriate forwarding.
IP Address	The snooping querier address to be used as source address in periodic IGMP queries. This address is used when no IP address is configured on the VLAN on which the query is being sent. The default entry to allow the switch to use its own IP address is 0.0.0.0.
IGMP Version	The IGMP protocol version used in periodic IGMP queries.
Query Interval (Seconds)	The amount of time the IGMP snooping querier on the device should wait between sending periodic IGMP queries.
Querier Expiry Interval (Seconds)	The amount of time the device remains in non-querier mode after it has discovered that there is a multicast querier in the network.

VLAN Configuration

Use this page to enable the IGMP snooping querier feature on one or more VLANs and to configure per-VLAN IGMP snooping querier settings. Only VLANs that have the IGMP snooping querier feature enabled appear in the table.

1. In the *IGMP Snooping Querier* screen, click the **VLAN Configuration** tab.



The *IGMP Snooping Querier VLAN Configuration* screen opens.



Field	Description
VLAN ID	The VLAN on which the IGMP snooping querier is enabled. When enabling the IGMP snooping querier on a VLAN, use this menu to select the desired VLAN. Only VLANs that have been configured on the system and are not already enabled for the IGMP snooping querier appear in the menu. When modifying IGMP snooping querier settings, this field identifies the VLAN that is being configured.
Querier Election Participation	The participation mode for the IGMP snooping querier election process: <ul style="list-style-type: none"> • Enabled: The IGMP snooping querier on this VLAN participates in the querier election process when it discovers the presence of another querier in the VLAN. If the snooping querier finds that the other querier source IP address is lower than its own address, it stops sending periodic queries. If the snooping querier wins the election (because it has the lowest IP address), then it continues sending periodic queries. • Disabled: When the IGMP snooping querier on this VLAN sees other queriers of the same version in the VLAN, the snooping querier moves to the non-querier state and stops sending periodic queries.
Querier VLAN IP Address	The IGMP snooping querier address the VLAN uses as the source IP address in periodic IGMP queries sent on the VLAN. If this value is not configured, the VLAN uses the global IGMP snooping querier IP address.

- To add the IGMP snooping querier settings for an IGMP-snooping enabled VLAN, click the three-dot menu (⋮) next to the entry with the settings to change, then click **Add**. The *Add IGMP Snooping Querier VLAN Configuration* screen opens.

Add IGMP Snooping Querier VLAN ⊗
Configuration

VLAN ID
10

Querier Election Participation

Querier VLAN IP Address
0.0.0.0

Cancel Add

VLAN Status

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

- In the *IGMP Snooping Querier* screen, click the **VLAN Status** tab.

IGMP Snooping Querier

Configuration VLAN Configuration **VLAN Status**

The *IGMP Snooping Querier VLAN Status* screen opens.

IGMP Snooping Querier VLAN Status

Filter By

OPTIONS

VLAN ID	State	Version	Last IP Address	Last Version	Max Response Time (Seconds)
---------	-------	---------	-----------------	--------------	-----------------------------

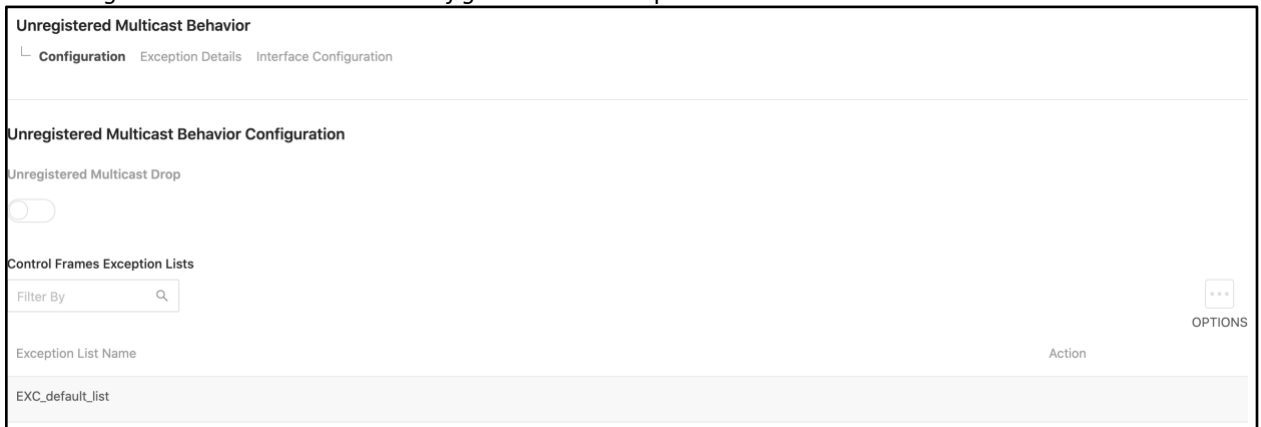
Configuring Unregistered Multicast Behavior

To access the *Unregistered Multicast Behavior* configuration menu:

- Click the switch’s **Advanced** tab, then click the **Unregistered Multicast Behavior** tile.

Unregistered Multicast Behavior
Configure the behavior of Unregistered multicast traffic when IGMP Snooping is enabled.

The *Unregistered Multicast Behavior Configuration* screen opens.

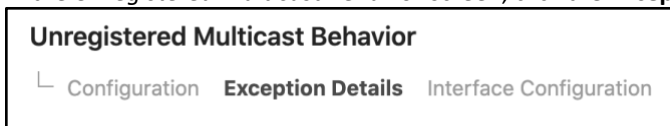


Field	Description
Unregistered Multicast Drop	When enabled along with IGMP Snooping being enabled on a VLAN, multicast packets destined for any multicast group address which has not been learned by a port on the switch will be dropped. When disabled, any unregistered multicast will be flooded on the switch. Traffic destined for the multicast addresses within 224.0.0.x will continue to flood with <i>Drop</i> set to Enabled as these groups are required for IGMP messaging.
Exception List Name	Displays the default ACL exception list available to the switch. In the future, additional lists may be added.

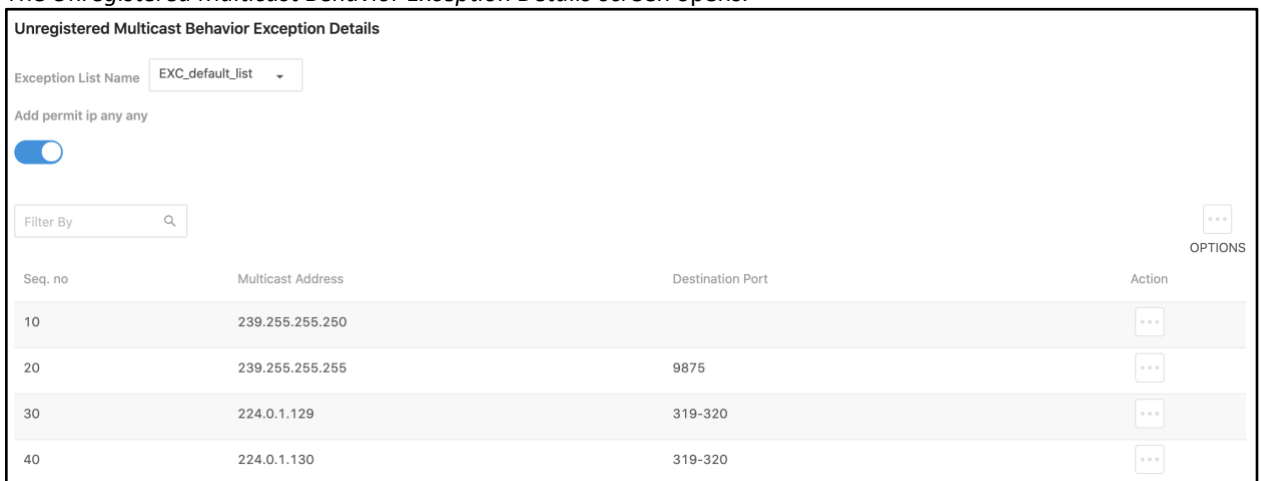
Exception Details

Use this page to configure which Multicast addresses and destination ports should be allowed to continue flooding while *Unregistered Multicast Behavior* is set to **Drop**.

1. In the *Unregistered Multicast Behavior* screen, click the **Exception Details** tab.



The *Unregistered Multicast Behavior Exception Details* screen opens.

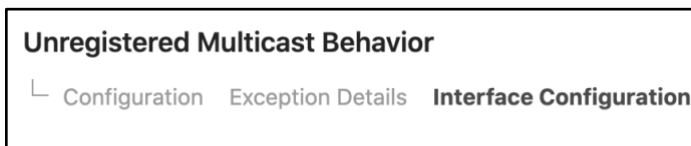


Field	Description
Exception List Name	Allows for multiple exception lists to be edited on this page. Currently only one exception list is supported.
Add "permit ip any any"	This will add an ACL rule to permit IP traffic from and to any. This is defaulted to be included, because it is needed in order to continue accessing the switch and passing traffic while <i>Unregistered Multicast</i> is set to Drop . This should be required in only rare cases where other ACLs have been configured which satisfy this rule. DISABLING THIS SETTING MAY CAUSE ALL DATA THROUGH THE SWITCH TO STOP AND ACCESS TO BE BLOCKED. CONSOLE ACCESS WOULD BE REQUIRED TO REGAIN ACCESS WITHOUT A FACTORY RESET TO DEFAULTS.
Seq. no	The ACL rule number for each exception entry
Multicast Address	The Multicast Address to be allowed to flood
Destination Port	The optional destination port of traffic destined for the Multicast Address. This can be left blank to specify any port, a single port, or a range of ports using "-".

Interface Configuration

Use this page to configure which Exception Lists are applied to each port. Currently only one Exception List can be created. In the future, multiple lists may be added.

1. In the *Unregistered Multicast Behavior* screen, click the **Interface Configuration** tab.



The *Exception List Interface Configuration* screen opens.

Exception List Interface Configuration			
Interface	Name	Exception List	Action
0/1	Port 1	EXC_default_list	
0/2	Port 2	EXC_default_list	
0/3	Port 3	EXC_default_list	

Configuring Spanning Tree Protocol

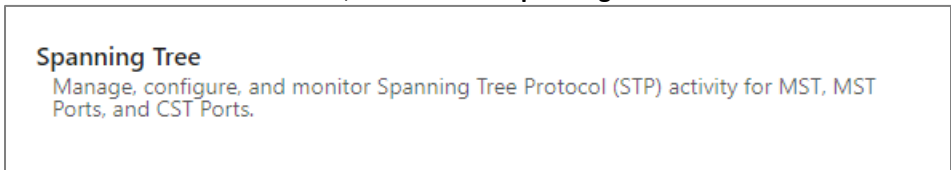
The Spanning Tree Protocol (STP) provides a tree topology for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops. Spanning tree versions supported include Common STP, Multiple STP, and Rapid STP. Classic STP provides a single path between end stations, avoiding and eliminating loops.

Multiple Spanning Tree Protocol (MSTP) supports multiple instances of Spanning Tree to efficiently channel VLAN traffic over different interfaces. Each instance of the Spanning Tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree (RSTP), with slight modifications in the working but not the end effect (chief among the effects is the rapid transitioning of the port to “Forwarding”). The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full-duplex connectivity and ports which are connected to end stations, resulting in rapid transitioning of the port to “Forwarding” state and the suppression of Topology Change Notification. These features are represented by the parameters “point to point” and “edgeport.” MSTP is compatible to both RSTP and STP. It behaves appropriately to STP and RSTP bridges.

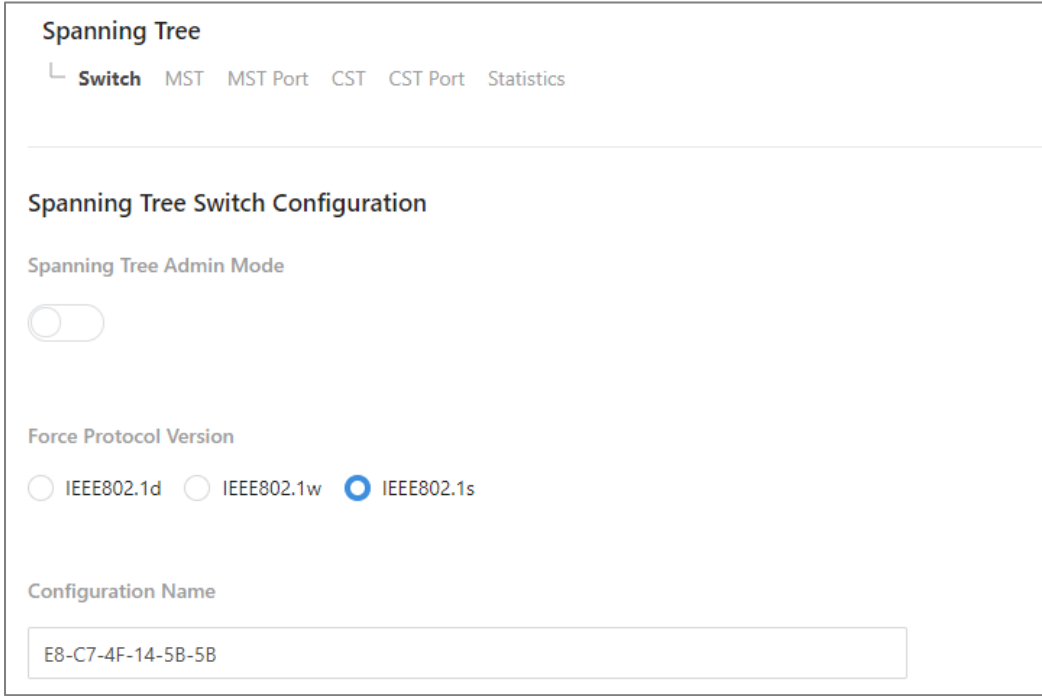
A MSTP bridge can be configured to behave entirely as a RSTP bridge or a STP bridge.

To access the *Spanning Tree Switch Configuration* menu:

1. Click the switch’s **Advanced** tab, then click the **Spanning Tree** tile.



The *Spanning Tree Switch Configuration* screen opens.



Field	Description
Spanning Tree Admin Mode	The administrative mode of STP on the device. When enabled, the device participates in the root bridge election process and exchanges Bridge Protocol Data Units (BPDUs) with other switches in the spanning tree to determine the root path costs and maintain topology information.
Force Protocol Version	The STP version the device uses, which is one of the following: <ul style="list-style-type: none"> • IEEE 802.1d: Classic STP provides a single path between end stations, avoiding and eliminating loops. • IEEE 802.1w: Rapid Spanning Tree Protocol (RSTP) behaves like classic STP but also has the ability to configure and recognize full-duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to the Forwarding state and the suppression of Topology Change Notifications. • IEEE 802.1s: Multiple Spanning Tree Protocol (MSTP) includes all the advantages of RSTP and also supports multiple spanning tree instances to efficiently channel VLAN traffic over different interfaces. MSTP is compatible with both RSTP and STP.
Configuration Name	The name of the MSTP region. Each switch that participates in the same MSTP region must share the same Configuration Name, Configuration Revision Level, and MST-to-VLAN mappings.
Configuration Revision Level	The revision number of the MSTP region. This number must be the same on all switches that participate in the MSTP region.
Configuration Digest Key	The 16-byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID-to-MST ID mapping).
Configuration Format Selector	The version of the configuration format being used in the exchange of BPDUs.

CST Configuration

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

1. In the *Spanning Tree* screen, click the **CST** tab.



The *Spanning Tree CST* screen opens.

Spanning Tree	
<ul style="list-style-type: none"> Switch MST MST Port CST CST Port Statistics 	
Spanning Tree CST Configuration	
Bridge Priority	<input type="text" value="32768"/>
Bridge Max Age	<input type="text" value="20"/>
Bridge Forward Delay	<input type="text" value="15"/>

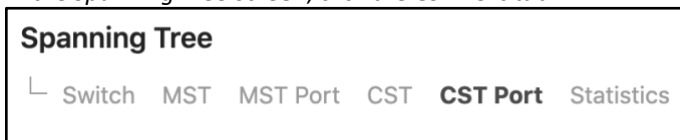
Field	Description
Bridge Priority	The value that helps determine which bridge in the spanning tree is elected as the root bridge during STP convergence. A lower value increases the probability that the bridge becomes the root bridge.
Bridge Max Age	The amount of time a bridge waits before implementing a topological change.
Bridge Hello Time	The amount of time the root bridge waits between sending hello BPDUs.
Bridge Forward Delay	The amount of time a bridge remains in a listening and learning state before forwarding packets.
Spanning Tree Maximum Hops	The maximum number of hops a Bridge Protocol Data Unit (BPDU) is allowed to traverse within the spanning tree region before it is discarded.
BPDU Guard	When enabled, can disable edge ports that receive BPDU packets. This prevents a new device from entering the existing STP topology, so devices that were originally not a part of STP are not allowed to influence the STP topology.
BPDU Filter	When enabled, filters the BPDU traffic on the edge ports. When spanning tree is disabled on a port, BPDU filtering allows BPDU packets received on that port to be dropped.
Spanning Tree Tx Hold Count	The maximum number of BPDUs that a bridge is allowed to send within a hello time window.
Bridge Identifier	A unique value that is automatically generated based on the bridge priority value and the base MAC address of the bridge. When electing the root bridge for the spanning tree, if the bridge priorities for multiple bridges are equal, the bridge with the lowest MAC address is elected as the root bridge.
Time Since Topology Change	The amount of time that has passed since the topology of the spanning tree has changed since the device was last reset.
Topology Change Count	The number of times the topology of the spanning tree has changed.
Topology Change	Indicates whether a topology change is in progress on any port assigned to the CST. If a change is in progress, the value is True. Otherwise, it is False.
Designated Root	The bridge identifier of the root bridge for the CST. The identifier is made up of the bridge priority and the base MAC address.

Root Path Cost	The path cost to the designated root for the CST. Traffic from a connected device to the root bridge takes the least-cost path to the bridge. If the value is 0, the cost is automatically calculated based on port speed.
Root Port	The port on the bridge with the least-cost path to the designated root for the CST.
Max Age	The amount of time a bridge waits before implementing a topological change.
Forward Delay	The forward delay value for the root port bridge.
Hold Time	The minimum amount of time between transmissions of Configuration BPDUs.
CST Regional Root	The bridge identifier of the CST regional root. The identifier is made up of priority value and the base MAC address of the regional root bridge.
CST Path Cost	The path cost to the CST tree regional root.

CST Port Configuration

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

1. In the *Spanning Tree* screen, click the **CST Port** tab.



The *Spanning Tree CST Port* screen opens.

The screenshot shows the 'Spanning Tree CST Port Summary' screen. It includes a search filter and a table with the following data:

Interface	Name	Port Role	Port Forwarding State	Port Priority	Port Path Cost	Description	Action
0/1	Port 1	Disabled	Manual Forwarding	128	0		...
0/2	Port 2	Disabled	Manual Forwarding	128	0		...
0/3	Port 3	Disabled	Manual Forwarding	128	0		...

2. Select one interface to edit and view detailed information, or select multiple interfaces to edit.

Edit CST Port Entry ⊗

CST Port Entry Selected: 1

Port Priority

Admin Edge Port

Port Path Cost

External Port Path Cost

Field	Description
Port Priority	The priority for the port within the CST. This value is used to determine which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Admin Edge Port	Select this option to administratively configure the interface as an edge port. An <i>edge port</i> is an interface that is directly connected to a host and is not at risk of causing a loop.
Port Path Cost	The path cost from the port to the root bridge.
External Port Path Cost	The cost of the path from the port to the CIST root. This value becomes important when the network includes multiple regions.
Port Mode	The administrative mode of spanning tree on the port.
Auto Edge	When enabled, Auto Edge allows the interface to become an edge port if it does not receive any BPDUs within a given amount of time.
Root Guard	When enabled, Root Guard allows the interface to discard any superior information it receives to protect the root of the device from changing. The port gets put into discarding state and does not forward any frames.
Loop Guard	When enabled, Loop Guard prevents an interface from erroneously transitioning from a blocking state to forwarding when the interface stops receiving BPDUs. The port is marked as being in <i>loop-inconsistent state</i> . In this state, the interface does not forward frames.
TCN Guard	When enabled, TCN Guard restricts the interface from propagating any topology change information received through that interface.

Auto-calculate Port PathCost:	Enabled
Hello Timer:	2
Auto-calculate External Port Path Cost:	Enabled
BPDU Guard Effect:	Disabled
Port ID:	80:01
Port Up Time Since Counters Last Cleared:	8d:21:16:9
Port Forwarding State:	Manual Forwarding
Port Role:	Disabled
Designated Root:	██████████
Designated Cost:	0
Designated Bridge:	██████████
Designated Port:	00:00
Topology Change Acknowledge:	False
Edge Port:	Disabled
Point-to-point MAC:	True
CST Regional Root:	██████████
CST Path Cost:	0
Loop Inconsistent State:	False
Transitions Into LoopInconsistentState:	0
Transitions Out Of LoopInconsistentState:	0

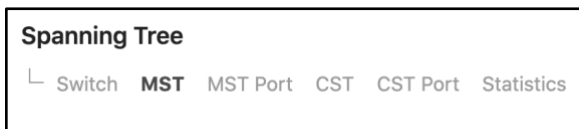
Field	Description
Auto-calculate Port Path Cost	Shows whether the path cost from the port to the root bridge is automatically determined by the speed of the interface (Enabled) or configured manually (Disabled).
Hello Timer	The amount of time the port waits between sending hello BPDUs.
Auto-calculate External Port Path Cost	Shows whether the path cost from the port to the CIST root is automatically determined by the speed of the interface (Enabled) or configured manually (Disabled).
BPDU Guard Effect	Shows the status of BPDU Guard Effect on the interface. When enabled, BPDU Guard Effect can disable edge ports that receive BPDU packets. This prevents a new device from entering the existing STP topology, so devices that were originally not a part of STP are not allowed to influence the STP topology.
Port ID	A unique value that is automatically generated based on the port priority value and the interface index.
Port Up Time Since Counters Last Cleared	The amount of time that the port has been up since the counters were cleared.
Port Role	The role of the port within the CST, which is one of the following: <ul style="list-style-type: none"> • Root: A port on the non-root bridge that has the least-cost path to the root bridge. • Designated: A port that has the least-cost path to the root bridge on its segment. • Alternate: A blocked port that has an alternate path to the root bridge. • Backup: A blocked port that has a redundant path to the same network segment as another port on the bridge. • Master: The port on a bridge within an MST instance that links the MST instance to other STP regions. • Disabled: The port is administratively disabled and is not part of the spanning tree.
Designated Root	The bridge ID of the root bridge for the CST.

Designated Cost	The path cost offered to the LAN by the designated port.
Designated Bridge	The bridge ID of the bridge with the designated port.
Designated Port	The port ID of the designated port.
Topology Change Acknowledge	Indicates whether the next BPDU to be transmitted for this port will have the topology change acknowledgment flag set.
Edge Port	Indicates whether the interface is configured as an edge port (Enabled).
Point-to-point MAC	Indicates whether the link type for the interface is a point-to-point link.
CST Regional Root	The bridge ID of the bridge that has been elected as the root bridge of the CST region.
CST Path Cost	The path cost from the interface to the CST regional root.
Loop Inconsistent State	Identifies whether the interface is currently in a loop-inconsistent state. An interface transitions to a loop-inconsistent state if Loop Guard is enabled and the port stops receiving BPDUs. In this state, the interface does not transmit frames.
Transitions Into LoopInconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out Of LoopInconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

MST Configuration

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

1. In the *Spanning Tree* screen, click the **MST** tab.



The *Spanning Tree MST* screen opens.

The screenshot shows the 'Spanning Tree MST Summary' screen. It features a search bar labeled 'Filter By' with a magnifying glass icon. Below the search bar is a table with the following columns: MST ID, Priority, Associated VLANs, Bridge Identifier, Time Since Topology Change, Designated Root, Root Path Cost, Root Port, and Action. An 'OPTIONS' menu icon is visible in the top right corner of the table area.

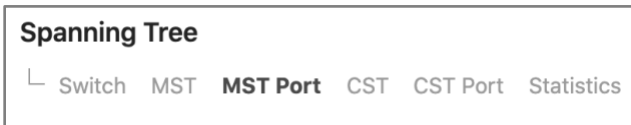
Field	Description
MST ID	The number that identifies the MST instance.

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

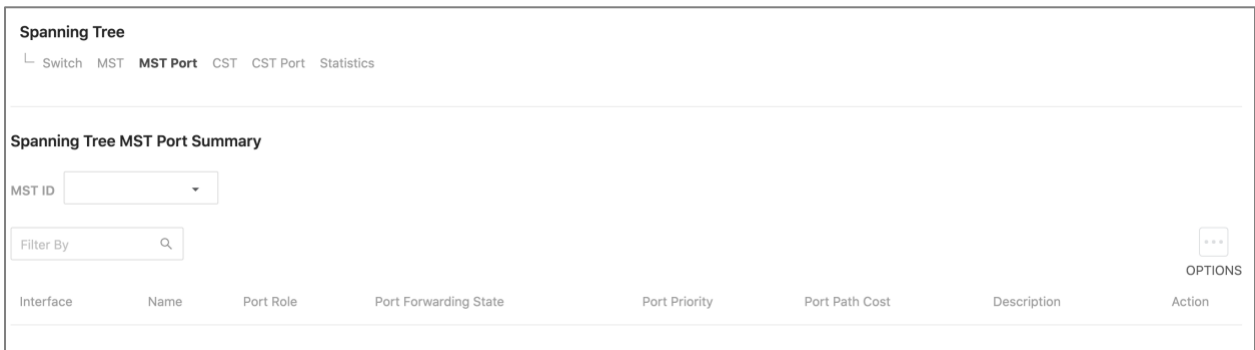
MST Port Configuration

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

1. In the *Spanning Tree* screen, click the **MST Port** tab.



The *Spanning Tree MST Port* screen opens.



An MST instance must first be created under the *MST* tab before an MST ID can be selected. Once selected, all ports are shown, can be configured, and more detail can be viewed by selecting **Edit** for the desired interface.

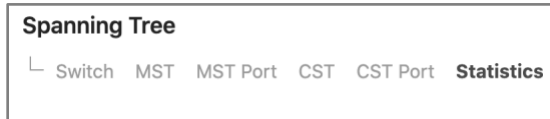
Field	Description
-------	-------------

Auto-calculate Port Path Cost	Shows whether the path cost from the port to the root bridge is automatically determined by the speed of the interface (Enabled) or configured manually (Disabled).
Hello Timer	The amount of time the port waits between sending hello BPDUs.
Auto-calculate External Port Path Cost	Shows whether the path cost from the port to the CIST root is automatically determined by the speed of the interface (Enabled) or configured manually (Disabled).
BPDU Guard Effect	Shows the status of BPDU Guard Effect on the interface. When enabled, BPDU Guard Effect can disable edge ports that receive BPDU packets. This prevents a new device from entering the existing STP topology, so devices that were originally not a part of STP are not allowed to influence the STP topology.
Port ID	A unique value that is automatically generated based on the port priority value and the interface index.
Port Up Time Since Counters Last Cleared	The amount of time that the port has been up since the counters were cleared.
Port Role	The role of the port within the CST, which is one of the following: <ul style="list-style-type: none"> • Root: A port on the non-root bridge that has the least-cost path to the root bridge. • Designated: A port that has the least-cost path to the root bridge on its segment. • Alternate: A blocked port that has an alternate path to the root bridge. • Backup: A blocked port that has a redundant path to the same network segment as another port on the bridge. • Master: The port on a bridge within an MST instance that links the MST instance to other STP regions. • Disabled: The port is administratively disabled and is not part of the spanning tree.
Designated Root	The bridge ID of the root bridge for the CST.
Designated Cost	The path cost offered to the LAN by the designated port.
Designated Bridge	The bridge ID of the bridge with the designated port.
Designated Port	The port ID of the designated port.
Topology Change Acknowledge	Indicates whether the next BPDU to be transmitted for this port will have the topology change acknowledgment flag set.
Edge Port	Indicates whether the interface is configured as an edge port (Enabled).
Point-to-point MAC	Indicates whether the link type for the interface is a point-to-point link.
CST Regional Root	The bridge ID of the bridge that has been elected as the root bridge of the CST region.
CST Path Cost	The path cost from the interface to the CST regional root.
Loop Inconsistent State	Identifies whether the interface is currently in a loop-inconsistent state. An interface transitions to a loop-inconsistent state if Loop Guard is enabled and the port stops receiving BPDUs. In this state, the interface does not transmit frames.
Transitions Into LoopInconsistent State	The number of times this interface has transitioned into loop-inconsistent state.
Transitions Out Of LoopInconsistent State	The number of times this interface has transitioned out of loop-inconsistent state.

Spanning Tree Statistics

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

1. In the *Spanning Tree* screen, click the **Statistics** tab.



The *Spanning Tree Statistics* screen opens.

Spanning Tree Statistics									
Interface	Name	STP BPDUs Rx	STP BPDUs Tx	RSTP BPDUs Rx	RSTP BPDUs Tx	MSTP BPDUs Rx	MSTP BPDUs Tx	SSTP BPDUs Rx	SSTP BPDUs Tx
0/1	Port 1	0	0	0	0	0	0	0	0
0/2	Port 2	0	0	0	0	0	0	0	0
0/3	Port 3	0	0	0	0	0	0	0	0
0/4	Port 4	0	0	0	0	0	0	0	0

Field	Description
Interface	The port or link aggregation group (LAG) associated with the rest of the data in the row.
Name	The user-configured name of the port or link aggregation group (LAG).
STP BPDUs Rx	The number of classic STP (IEEE 802.1d) BPDUs received by the interface.
STP BPDUs Tx	The number of classic STP BPDUs sent by the interface.
RSTP BPDUs Rx	The number of RSTP (IEEE 802.1w) BPDUs received by the interface.
RSTP BPDUs Tx	The number of RSTP BPDUs sent by the interface.
MSTP BPDUs Rx	The number of MSTP (IEEE 802.1s) BPDUs received by the interface.
MSTP BPDUs Tx	The number of MSTP BPDUs sent by the interface.

Loop Protection

Advanced > Loop Protection

Loop Protection detects loops in downstream switches that do not have spanning tree configured. When a loop protected interface detects a loop, it can disable itself.

Note: Do not use Loop Protection on uplink ports between switches with spanning tree enabled. Loop Protection is designed for unmanaged switches that drop spanning tree BPDUs.

How to Configure Loop Protection

Loop Protection sends loop protection protocol data units (PDUs) to the multicast address 01:80:C2:00:00:08. When an interface receives a PDU, it compares the source MAC address with the switch's. If the MAC address matches a loop is detected and a configured action is taken. **Shutdown Port**, **Shutdown Port and Log**, or **Log Only**.

To configure Loop Protection:

1. **Enable** Loop Protection globally for the switch.



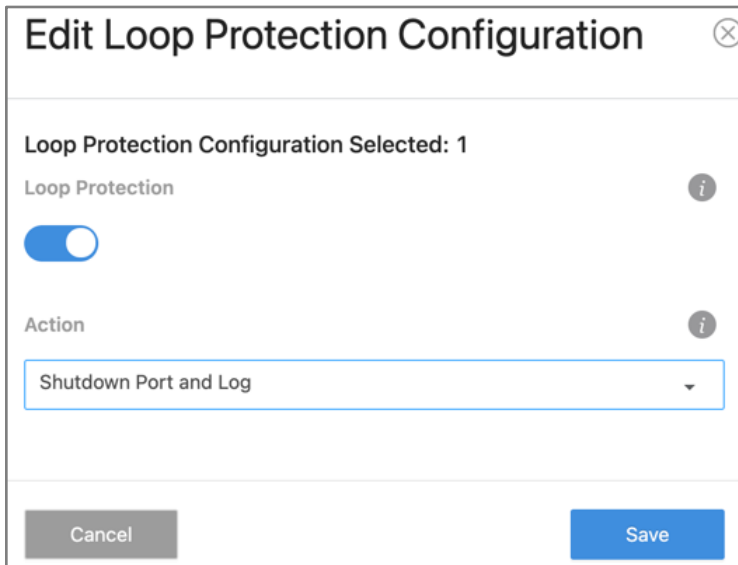
2. Enter values in the fields below the **Enable** toggle. Use the table below for guidance.

Field	Description
Transmission Time (Seconds)	The time interval (in seconds) that the switch sends PDU packets on Loop Protected interfaces.
Maximum PDU Received	The amount of PDU packets an interface receives before taking the configured action.
Shutdown Time (Seconds)	The amount of seconds the interface shuts down when a loop is detected.

3. Click the Action button in the interface row you want to configure.

Interface	Name	Loop Protection	Action	Status	Loop	Loop Count	Time of Last Loop	Action
0/1	UL - Lab Rack MS- 2416	<input type="checkbox"/>	Shutdown Port	Link Up		0	Aug 10 03:43:19 2021 America/Denver(UTC-6:00)	...

- A new window appears. Enable **Loop Protection** on the interface, then select an **Action** to take. **Shutdown Port, Shutdown Port and Log**, or **Log Only**. Then, click **Save**.



- The window closes and you return to the Loop Protection Configuration table. Click **Apply** at the top of the page.

Loop Protection Configuration Table

The Loop Protection Configuration table gives an overview of what interfaces have Loop Protection enabled, how they're configured, and the **Time of Last Loop**.

Filter By <input type="text"/>								...
Interface	Name	Loop Protection	Action	Status	Loop	Loop Count	Time of Last Loop	OPTIONS
0/1	UL - Lab Rack MS- 2416	<input checked="" type="checkbox"/>	Shutdown Port	Link Up		0	Aug 10 03:43:19 2021 America/Denver(UTC-6:00)	...
0/2	Home PC	<input type="checkbox"/>	Shutdown Port	Link Up		0	Aug 10 03:43:19 2021 America/Denver(UTC-6:00)	...
0/3	Office WB- 250-IPW-2	<input type="checkbox"/>	Shutdown Port	Link Up		0	Aug 10 03:43:19 2021 America/Denver(UTC-6:00)	...
0/4	Nvidia Jetson Nano	<input type="checkbox"/>	Shutdown Port	Link Down		0	Aug 10 03:43:19 2021 America/Denver(UTC-6:00)	...

The following table describes each field in the table. The **Options** (⋮) button can be used to **Refresh** the table, which clears the configuration of each interface.

Field	Description
Interface	The switchport or LAG number.
Name	The name configured for the switchport or LAG.
Loop Protection	Shows if Loop Protection is enabled or not. Click to enable.
Action	The action taken if a loop is detected.
Status	The interface's status. Link Up indicates the interface is operating normally. Link Down indicates the interface is shut down because a loop is detected.
Loop	Indicates if a loop is detected. If blank, there is no loop.
Loop Count	The number of times a loop has been detected on the interface.
Time of Last Loop	The date and time of the last loop detected on the interface.
Action	Click this button to edit the interface's Loop Protection status and action taken.

Firmware

Click this tile to access cloud and local firmware upgrades.

If your firmware is up to date, this screen shows your current firmware version and provides a link for that firmware's *Release Notes*.

If a firmware update is available, this screen also shows the update version and the update's *Release Notes*. Click **Upgrade** to update the firmware from the cloud.

SNMP

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

SNMP Versions 1 and 2

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

SNMP Version 3

SNMP v3 adds access control and trap mechanisms. The **User Security Model (USM)** for SNMP v3 includes:

- **Authentication:** Provides data integrity and data origin authentication.
- **Privacy:** Protects against exposure of message content by encrypting the information with Cipher-Block Chaining (CBC). Authentication and privacy is enabled on an SNMP message.
- **Timeliness:** Protects against message delay and redundancy by comparing incoming messages with their time information.
- **Key Management:** Defines key generation, updates, and use.

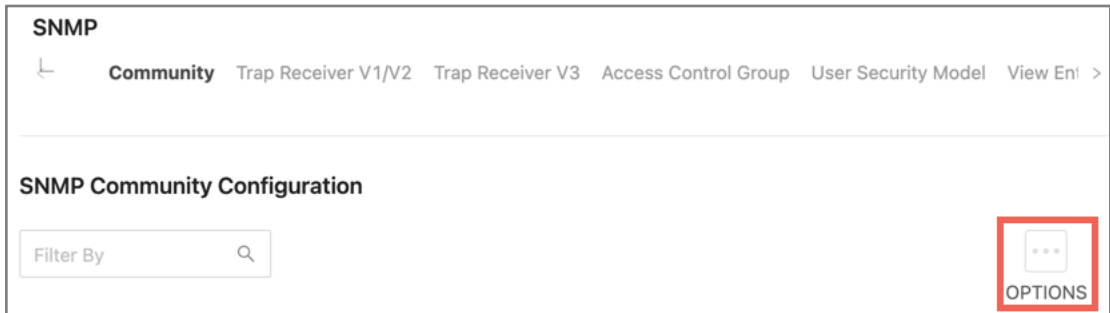
How to Configure an SNMP Community or Group

Advanced > SNMP > Community

Manage access rights by defining communities. Changing community names also changes access rights. SNMP Communities are only definable for SNMP v1 and 2. SNMP v3 uses groups and assigns users to them.

To Configure an SNMP Community or Group:

1. Click the **Options** (⋮) button, then **Add**.



2. A new window appears. Select the **mode** you want to configure. **Community** or **Group**.



3. Use the below table to configure the chosen mode.

Mode	Field	Description
Community	Community Name	Community name used in SNMPv1 and 2 packets.
	IP Address	Specifies the IP address that can connect with this community.
	Community Access	Select the access control policy of this community.
	Community View	Specifies the community view for this community. No access is granted if the field is empty.
Group	Community Name	Community name used in SNMPv1 and 2 packets.
	IP Address	Specifies the IP address that can connect with this community.

	Group Name	Specifies the community view for this community. No access is granted if the field is empty.
--	------------	--

- Click the **Apply** button at the top of the page.

Use the **Action** (...) button to edit or delete individual communities. Use the **Options** (...) button to **Delete** multiple communities by clicking **Edit** or click **Refresh** to clear all configured communities.

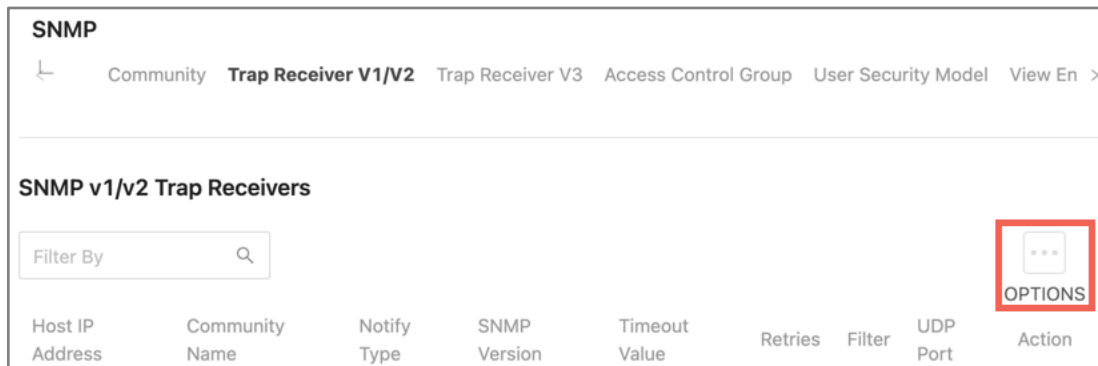
How to Configure Trap Receivers for SNMP v1 and 2

Advanced > SNMP > Trap Receiver V1/V2

Use this page to configure the SNMP v1 or 2 management host that's receiving notifications about traps generated by the switch. The SNMP management host is also known as the **trap receiver**.

To configure a trap receiver:

- Click the **Options** (...) button, then **Add**.



- Use the below table to help you configure the fields in the new window. Click **Add**, when done.

Field	Description
Host IP Address	The IP address of the trap receiver that is going to receive the traps generated by the switch.
Community Name	The name of the SNMP community that includes the trap receiver and the SNMP agent on the switch.
Notify Type	The type of SNMP notification sent to the trap receiver. The options are: <ul style="list-style-type: none"> 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.
SNMP Version	Select the version of SNMP being used.
Filter	The name of the filter for the trap receiver. The filter is configured using the CLI and defines which MIB objects to include or exclude from the view. Note: This field is optional.
UDP Port	The UDP port notifications are sent to on the trap receiver. If no value is specified the default UDP port value is used.

Retries	Only available if Inform is selected. The number of times an inform message is sent if it is not acknowledged by the trap receiver.
Timeout Value	Only available if Inform is selected. The number of seconds to wait for acknowledgement from the trap receiver before resending an inform message.

3. Click the **Apply** button at the top of the page.

Use the **Action** (⋮) button to edit or delete individual trap receivers. Use the **Options** (⋮) button to **Delete** multiple trap receivers by clicking **Edit** or click **Refresh** to clear all trap receivers.

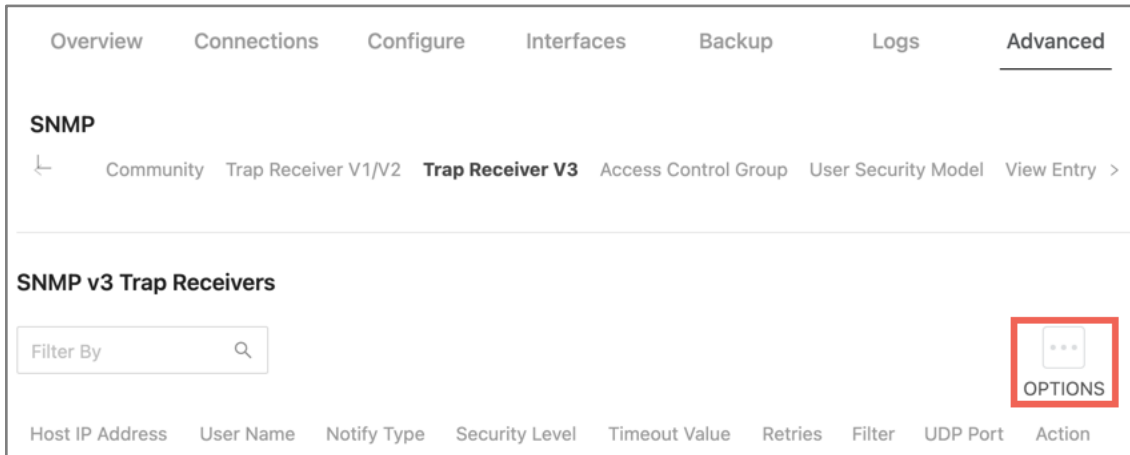
How to Configure Trap Receivers for SNMP v3

Advanced > SNMP > Trap Receivers V3

Use this page to configure the SNMP v1 or 2 management host that's receiving notifications about traps generated by the switch. The SNMP management host is also known as the **trap receiver**.

To configure a trap receiver:

1. Click the **Options** (⋮) button, then **Add**.



2. Use the below table to help you configure the fields in the new window. Click **Add**, when done.

Field	Description
Host IP Address	The IP address of the trap receiver that is going to receive the traps generated by the switch.
User Name	The SNMP username authorized to receive the SNMP notification.
Notify Type	The type of SNMP notification sent to the trap receiver. The options are: <ul style="list-style-type: none"> • 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.
Security Level	The security level of the SNMP user. Available options are: <ul style="list-style-type: none"> • No Auth No Priv: No security. • Auth No Priv: Authentication with no data encryption. With this security level, users send SNMP messages using an MD5 key for authentication, without a DES key for encryption. • Auth Priv: Authentication and data encryption. With this security level, users send an MD5 key for authentication and a DES key for encryption.
Filter	The name of the filter for the trap receiver. The filter is configured using the CLI and defines which MIB objects to include or exclude from the view. <i>Note: This field is optional.</i>
UDP Port	The UDP port notifications are sent to on the trap receiver. If no value is specified the default UDP port value is used.
Retries	Only available if Inform is selected. The number of times an inform message is sent if it is not acknowledged by the trap receiver.
Timeout Value	Only available if Inform is selected. The number of seconds to wait for acknowledgement from the trap receiver before resending an inform message.

3. Click the **Apply** button at the top of the page.

Use the **Action** (⋮) button to edit or delete individual trap receivers. Use the **Options** (⋮) button to **Delete** multiple trap receivers by clicking **Edit** or click **Refresh** to clear all trap receivers.

SNMP Access Control Groups

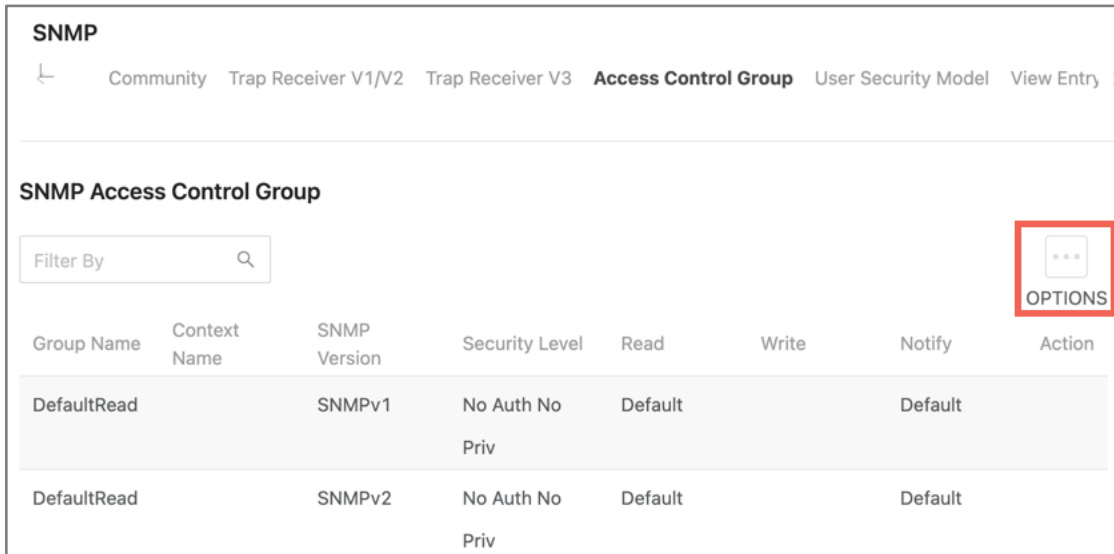
Advanced > SNMP > Access Control Group

Use this page to configure **SNMP Access Control Groups** and view a summary of the configured access control groups. These SNMP groups allow network managers to assign different authorization levels and access rights to specific switch features and attributes.

The SNMP community can reference an SNMP group to provide security and context for agents receiving requests and initiating traps, as well as management system tasks. An SNMP agent cannot respond to a request from a management system outside the group or groups its configured for. The switch is preconfigured with several default SNMP groups.

To add a new SNMP access control group:

1. Click the **Options** (⋮) button, then **Add**.



2. Use the below table to help you configure the fields in the new window. Click **Add**, when done.

Field	Description
Group Name	Enter a name to identify the SNMP access control group.
SNMP Version	The SNMP version associated with the group.
Security Level	Only available for SNMP v3 . Available options are: <ul style="list-style-type: none"> • No Auth No Priv: No security. • Auth No Priv: Authentication with no data encryption. With this security level, users send SNMP messages using an MD5 key for authentication, without a DES key for encryption. • Auth Priv: Authentication and data encryption. With this security level, users send an MD5 key for authentication and a DES key for encryption.
Context Name	The SNMP context associated with the SNMP group. A user or a management application uses the context name to get the performance information from the MIB objects associated with the context name. The Context Engine ID identifies the SNMP entity that should process the request (the physical router), and the Context Name tells the agent in which context it should search for the objects requested by the user or management application.
Group Access Rights Read	The level of read access rights for the group. The dropdown includes the available SNMP views, which restricts management access to viewing the contents of the agent.
Group Access Rights Write	The level of write access rights for the group. The dropdown includes the available SNMP views, which permits management read/write access to the contents of the agent but not to the community.
Group Access Rights Notify	The level of notify access rights for the group. The dropdown includes the available SNMP views, which permits sending SNMP traps or informs.

3. Click the **Apply** button at the top of the page.

Use the **Action** (...) button to edit or delete access control groups. Use the **Options** (...) button to **Delete** access control groups by clicking **Edit** or click **Refresh** to clear all configured access control groups. Default groups remain.

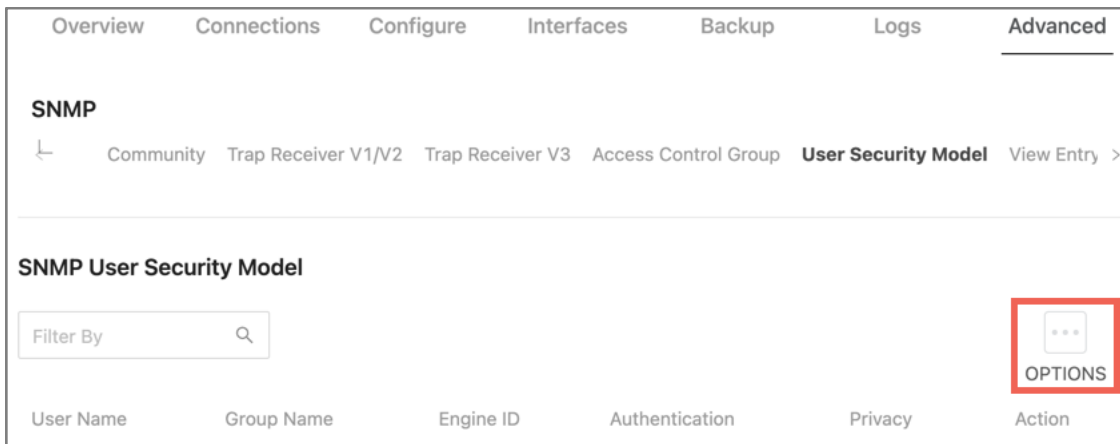
How to Add a New SNMP v3 User

Advanced > SNMP > User Security Model

Use this page to configure SNMP v3 users.

To configure a new SNMP v3 user:

1. Click the **Options** (...) button, then **Add**.



2. Use the below table to help you configure the fields in the new window. Click **Add**, when done.

Field	Description
Engine ID Type	Each SNMP v3 agent has an engine ID as a unique identifier for the device. Select the Engine ID type being used. Local or Remote .
User Name	A unique identifier for the user. Leading or embedded blanks cannot be used.
Group Name	The SNMP group name to associate the user with.
Authentication Method	Select an authentication protocol to use. Options include: <ul style="list-style-type: none"> • None: No authentication is used. • MD5: This protocol requires a password of 1-32 hexadecimal characters. • SHA: This protocol requires a password of 1-32 hexadecimal characters. • MD5-Key: This protocol requires a pre-generated MD5 authentication key of 32 hexadecimal characters. • SHA-Key: This protocol requires a pre-generated SHA authentication key of 40 hexadecimal characters.

4. Click the **Apply** button at the top of the page.

Use the **Action** (...) button to edit or delete users. Use the **Options** (...) button to **Delete** users by clicking **Edit** or click **Refresh** to clear all users.

SNMP View Entry

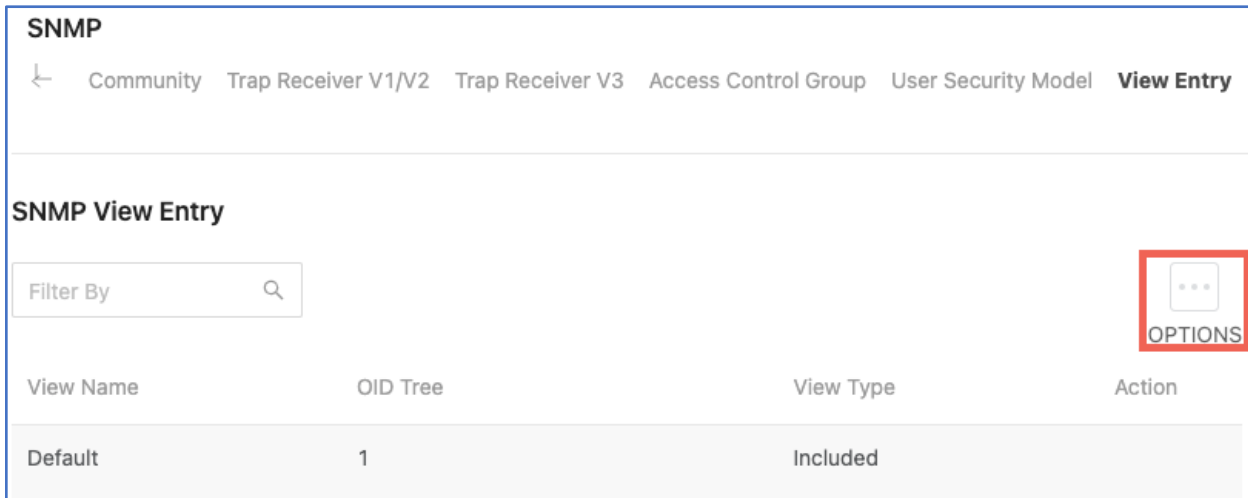
Advanced > SNMP > View Entry

An **SNMP View** is a mapping between SNMP scalar and tabular objects and the access rights configured for the view. Use this page to configure access to one or more **MIB OID** (MIB Object Identifier) nodes for an **SNMP View Name**.

Note: An **SNMP View Entry** must be configured for an **SNMP v3 agent** to work.

To configure a new SNMP view entry:

1. Click the **Options** (...) button, then **Add**.



2. Use the below table to help you configure the fields in the new window. Click **Add**, when done.

Field	Description
View Name	Enter a unique name to identify the SNMP view.
View Type	Select an View Type to use. Options include: <ul style="list-style-type: none"> • Included: Grants access to the OID subtree. • Excluded: Denies access to the OID subtree.
OID Tree	The ASN.1 subtree to grant or deny access to.

3. Click the **Apply** button at the top of the page.

Use the **Action** (...) button to SNMP view entries. Use the **Options** (...) button to **Delete** view entries by clicking **Edit** or click **Refresh** to clear all view entries.

SNMP Source Interface Configuration

Advanced > SNMP > Source Interface Configuration

Use this page to specify the physical or logical interface to use as the SNMP client source interface. When an IP address is configured on the source interface, the IP address is used in the IP header of SNMP management packets for all SNTP communications between the between the local SNMP client and the remote SNTP server. This allows security devices, like firewalls, to identify incoming source packets from a specific device.

To configure an SNMP trap source interface:

1. Select a source interface **type**. There are two options to choose from:
 - **None**: The primary IP address of the originating (outbound) interface is used as the source address.
 - **Interface**: The primary IP address of the physical switchport is used as the source address.

The screenshot shows the configuration page for SNMP. At the top, there is a breadcrumb trail: Access Control Group > User Security Model > View Entry > **Source Interface Configuration** > Server Configuration. Below this, the main heading is "SNMP Trap Source Interface Configuration". Under the heading, there are two sections: "Type" and "Interface". The "Type" section has two radio button options: "None" (unselected) and "Interface" (selected). The "Interface" section has a dropdown menu currently set to "Network". Both sections have an information icon (i) to their right.

1. The **Interface** dropdown can only be set to **Network**. This option includes the physical port, VLAN routing interface, and the network source IP.
2. Click **Apply** at the top of the page.

SNMP Server Configuration

Advanced > SNMP > Server Configuration

Use this page to specify the UDP port number the SNMP server uses to listen for requests. Changing this value may cause existing SNMP transactions to cease communicating with the device until the client applications are reconfigured to use the new port number.

SNMP

← rap Receiver V3 Access Control Group User Security Model View Entry Source Interface Configuration **Server Configuration**

SNMP Server Configuration

SNMP Server Port ⓘ

Click **Apply** to save changes.

Time Ranges

Use these pages to configure time ranges for **Access Command Lists (ACLs)**. Time ranges can be set for one or more rules within an ACL using a periodic or absolute time, except for the deny all rule each ACL has.

Time ranges must have a name before they can be referenced by an ACL rule.

Time Range Configuration

Advanced > Time Ranges > Configuration

Click the **Options** (⋮) button to create or edit a named Time Range. Use the **Action** (⋮) button to delete a Time Range.

Click **Enable** to make the Time Ranges active. Read the below table for descriptions of the **Time Range Summary** fields.

Time Ranges

↳ **Configuration** Entry Configuration

Time Range Summary

Enable

Filter By ⋮

Time Range Name	Time Range Status	Periodic Entry Count	Absolute Entry	Action
Test_Range	Inactive	1	Does not exist	⋮

Field	Description
Time Range Name	The name entered to identify the Time Range.
Time Range Status	Shows if the Time Range is currently active.
Periodic Entry Count	The number of periodic time range entries currently configured with the Time Range.
Absolute Entry	The number of absolute time range entries currently configured with the Time Range.

Entry Configuration

Advanced > Time Ranges > Entry Configuration

Use this page to add periodic and absolute time range entries.

To add a Time Range Entry:

1. Select a Time Range Name from the dropdown, then click the **Options** (⋮) button.

2. The Add Time Range window appears. Select the **Entry Type** to create. **Periodic** or **Absolute**.

3. Use the below table to configure the entry. Fields differ based on the type of entry chosen. Click **Add**, when done.

Entry Type	Field	Description
Periodic	Start Days	Select the day the time range entry begins. If more than one day is selected, they must match the End Days field.
	Starting Time of Day	Enter the time of day the entry begins. Uses a 24-hour format.
	End Days	The day, or days, the entry ends. If multiple days are selected, they must match the Start Days field.
	Ending Time of Day	The time of day the entry ends. Uses a 24-hour format.
Absolute	Starts	The calendar day the entry begins.
	Ends	The calendar day the entry ends.

To delete a Time Range Entry, click the **Action** (⋮) button next to the entry.


Logs

The logs display a record of system events affected by the switch and can be configured to only display the most pertinent system information.

Event Log

Advanced > Logs > Event Log

Use the *Event Log* page to view system events recorded since the last restart of the switch. Refresh the page to see new events. The **Options** (⋮) button gives you the ability to display a specified number of rows, and to **Refresh** the logs.

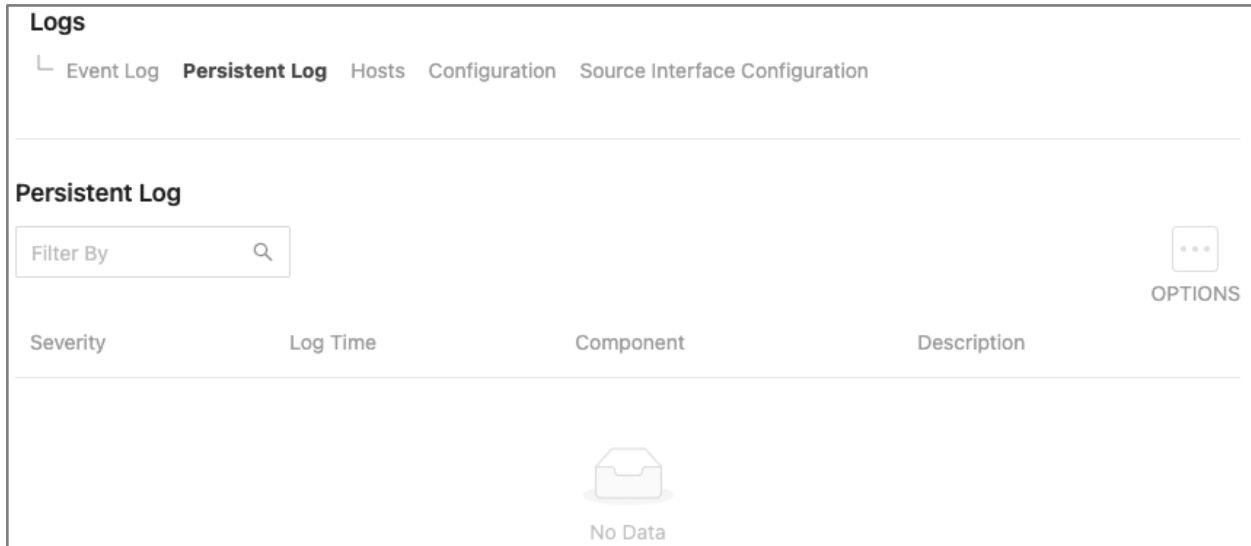
Logs					
Event Log Persistent Log Hosts Configuration Source Interface Configuration					
Event Log					
Filter By <input type="text"/>					 OPTIONS
Type	Filename	Line	Task ID	Code	Event Time
EVENT	bootos.c	207	043B76B4	AAAAAAAA	0d:00:01:09
EVENT	bootos.c	207	04EB36B4	AAAAAAAA	0d:00:01:09
EVENT	bootos.c	207	0488D6B4	AAAAAAAA	0d:00:01:08
EVENT	bootos.c	207	0541B6B4	AAAAAAAA	0d:00:01:09
EVENT	bootos.c	207	052B26B4	AAAAAAAA	0d:00:01:04

Field	Description
Type	The incident category of the log entry. Event, Error, etc.
Filename	The source code file name of the event's origin.
Line	The line number of the event within the source code.
Task ID	The system identifier of the task that was running when the event occurred.
Code	An event-specific code assigned to the event.
Event Time	A time stamp (days:hours:minutes:seconds) that indicates when the event occurred in reference to the system's uptime.

Persistent Log

Advanced > Logs > Persistent Log

The *Persistent Log* page shows current events, and events recorded before the last system restart. Refresh the page to see new events. The **Options** (⋮) button gives you the ability to display a specified number of rows, and to **Refresh** the logs.



Field	Description
Severity	The severity level of the log entry. The severity levels displayed can be configured in Log Configuration .
Log Time	A time stamp (days:hours:minutes:seconds) that indicates when the event occurred.
Component	The component that issued the log entry.
Description	A text description of the log entry.

Logging Hosts


Advanced > Logs > Hosts


Use the *Logging Hosts* page to configure remote hosts to send and capture logs to. Click the **Options** (⋮) button to **Edit**, **Add** a new host, or **Refresh** the list.


Logs

↳ Event Log Persistent Log **Hosts** Configuration Source Interface Configuration

Logging Hosts

Filter By 

 **OPTIONS**

Host	Status	Port	Severity Filter	Transport Mode	Authentication Mode	CertificateIndex	Action
 No Data							

Field	Description
Host	The IP address or DNS-resolvable host name of the remote host that is receiving log messages.
Status	Indicates if the host is configured to actively log or not.
Port	The UDP port on the logging host that the syslog messages are being sent.
Severity Filter	Severity level threshold for log messages, configured on the Log Configuration page. All log messages with a severity level at and above the configured threshold are sent to the logging host.
Transport Mode	UDP or TLS. If TLS is not configured the default transport mode is UDP.
Authentication Mode	Using TLS, the security user can configure anonymous authentication mode, where no client authentication is done by the syslog server. Using x509/name authentication mode, two-way authentication is done by the syslog client and the syslog server.
Certificate Index	Index used to identify corresponding certificate files.
Action	Edit or remove a logging host.

Log Configuration

Advanced > Logs > Configuration

Use these fields to configure the behavior and data for the switch to log.

Buffered Log Configuration

- **Admin Mode:** Enabled by default, this feature logs data to the buffered (RAM) file.
- **Behavior:** Specifies what happens when the buffered log is full.
 - **Wrap:** Deletes the oldest messages.
 - **Stop on Full:** Stops writing new messages.

Fields	Description	Input Values	Default
Admin Mode	Enable to log data to the buffered (RAM) file.	Enable or Disable	Enabled
Severity Filter	Specifies what happens when the buffered log is full. <ul style="list-style-type: none"> • Wrap: Deletes the oldest messages. • Stop on Full: Stops writing new messages. 	Wrap Stop on Full	Wrap

Command Logger Configuration

Enable or **Disable** logging of command-line interface (CLI) commands issued to the switch.

Console Log Configuration

Fields	Description	Input Values	Default
Enable Toggle	Enable or disable logging to any attached serial device to the switch.	Enable or Disable	Disable
Severity Filter	The Severity Filter sets the severity of the messages to log. All messages at or above the selected severity level are logged to the console. Severity levels include: <ul style="list-style-type: none"> • Emergency: The switch cannot be used. • Alert: Immediate action necessary. • Critical: The switch is experiencing urgent system failures. • Error: The switch is experiencing non-urgent failures. • Warning: The switch is experiencing conditions that lead to an error if no action is taken. • Notice: The switch is experiencing significant conditions. • Info: Provides non-critical information. • Debug: Provides debug-level information. 	Emergency Alert Critical Error Warning Notice Info Debug	Alert

Persistent Log Configuration

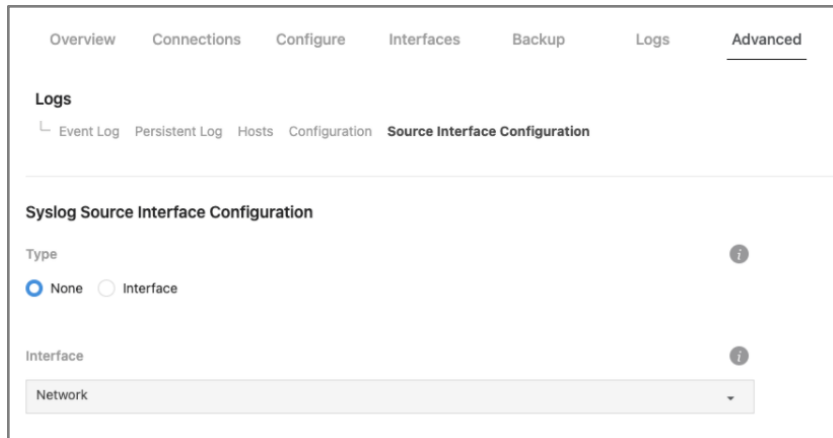
Fields	Description	Input Values	Default
Enable Toggle	Enable or disable logging to the persistent log. These messages are not deleted when the switch restarts.	Enable or Disable	Disable
Severity Filter	<p>The Severity Filter sets the severity of the messages to log. All messages at or above the selected severity level are logged to the switch.</p> <p>Severity levels include:</p> <ul style="list-style-type: none"> • Emergency: The switch cannot be used. • Alert: Immediate action necessary. • Critical: The switch is experiencing urgent system failures. • Error: The switch is experiencing non-urgent failures. • Warning: The switch is experiencing conditions that lead to an error if no action is taken. • Notice: The switch is experiencing significant conditions. • Info: Provides non-critical information. • Debug: Provides debug-level information. 	Emergency Alert Critical Error Warning Notice Info Debug	Alert

Syslog Configuration

Fields	Description	Input Values	Default
Enable Toggle	<p>Enable or disable logging to the configured syslog hosts.</p> <p>When disabled, the switch does not relay logs to syslog hosts and no messages are sent to any collector/relay.</p> <p>When enabled messages are sent to the collectors/relays using the values configured for each collector/relay.</p>	Enable or Disable	Disable
Protocol Version	The RFC version of the syslog protocol.	RFC 3164 or RFC 5424	RFC 3164
Local UDP Port	The UDP port the switch sends syslog messages from.	1-65535	514

*Syslog Source Interface Configuration***Advanced > Logs > Source Interface Configuration**

Use the *Syslog Source Interface Configuration* page to configure the port that the Syslog host is connected to.



- **Type:** Select *Interface* to configure a Syslog Source Interface. Default is *None*.
- **Interface:** Use the dropdown to select the type of interface being used.
 - **Interface:** Select the physical port the source interface is connected to.
 - **VLAN:** Select the VLAN the source interface is connected to.

SNTP

Simple Network Time Protocol (SNTP) assures the switch's clock time is accurate to the millisecond, by synchronizing to an SNTP server. The MS switch can only operate as an SNTP client and cannot provide time services to other systems.

Time sources are established by **Stratums**, which define the accuracy of the reference clock. The higher the stratum (zero being the highest) the more accurate the clock. The switch receives time from stratum 1 and above because the switch itself is a stratum 2 device.

Examples of stratums:

- **Stratum 0:** An actual time clock, such as a GPS system, is used as the time source.
- **Stratum 1:** A server directly linked to a stratum 0 source is used. Stratum 1 time servers provide primary network time standards.
- **Stratum 2:** A time source connected to a stratum 1 server over a network. Such as a stratum 2 server receiving time over the network, via NTP, from a stratum 1 server.

SNTP time definitions are determined by the following time levels:

- **T1:** The time that the original request was sent by the client.
- **T2:** The time that the original request was received by the server.
- **T3:** The time that the server sent a reply.
- **T4:** The time that the client received the server's reply.

The switch can poll **unicast** and **broadcast** server types for the server time.

Unicast information is used for polling a server with a known IP address. SNTP servers configured on the switch are the only servers polled for synchronization information. This is the most secure method for synchronization. When selected, SNTP information is only accepted from SNTP servers defined on the **SNTP Server Configuration** page.

Broadcast information is used for polling a server with an unknown IP address. When a broadcast message is sent from an SNTP server, the SNTP client listens. If broadcast polling is enabled, any synchronization information is accepted. Even if the information was not requested, making broadcast an unsecure polling method.

The switch retrieves synchronization information by either actively requesting information or at every poll interval.

If unicast and broadcast polling are enabled, the information is retrieved in the following order:

1. Information from SNTP servers defined on the **SNTP Server Configuration page** is prioritized. If no servers are defined then the switch accepts time information from any responding SNTP server.
2. If more than one unicast server responds, synchronization information is prioritized for the server with the lowest stratum.
3. If the servers have the same stratum, synchronization information is accepted from the SNTP server that responds first.

Message Digest 5 (MD5) Authentication safeguards device synchronization paths to SNTP servers. The MD5 algorithm produces a 128-bit hash and is a variation of MD4 that increases security. MD5 verifies the integrity of the communication and authenticates its origin.

SNTP Global Configuration

Advanced > SNTP > Global Configuration

Use this page to view and adjust SNTP parameters. The below table describes the available fields and their options.

Field	Description
Client Mode	Use the dropdown to specify the SNTP Client Mode. Options include: <ul style="list-style-type: none"> • Disable: SNTP is not operational. • Unicast: STNP operates in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply to determine the time, and potential round-trip delays to calculate an offset from the local time. • Broadcast: SNTP operates like it's multicast but uses a local broadcast address instead of a multicast address. The broadcast address has a single subnet scope, while a multicast address has an internet wide scope.
Port	Specifies the local UDP port to listen for responses and or broadcasts.
Unicast Poll Interval (Seconds)	Specifies the number of seconds between unicast poll requests, expressed as a power of two when configured in unicast mode. Allowed range is 6 to 10.
Broadcast Poll Interval (Seconds)	Specifies the number of seconds between broadcast poll requests, expressed as a power of two when configured in unicast mode. Allowed range is 6 to 10. Broadcasts received prior to the expiry of the interval are discarded.
Unicast Poll Timeout (Seconds)	The number of seconds to wait for an SNTP response when configured in unicast mode. Allowed range is 1 to 30.
Unicast Poll Retry	The number of times to retry a poll request to an SNTP server after the first time out, before attempting to use the next configured server. Allowed range is 0 to 10. Used when configured in unicast mode.
Number of Servers Configured	Shows the number of unicast server entries currently configured in the switch.

SNTP Global Status

Advanced > SNTP > Global Status

This page displays information about the switch's SNTP client. The below table describes the fields on the page.

Field	Description
Version	The SNTP version the client supports.
Supported Mode	The SNTP modes the client supports. Multiple modes may be supported.
Last Update Time	The local date and time (UTC) the SNTP client last updated the system clock.
Last Attempt Time	The local date and time (UTC) of the last SNTP request, or receipt of an unsolicited message.
Last Attempt Status	The status of the last SNTP request or unsolicited message for both unicast and broadcast modes. Possible statuses include: <ul style="list-style-type: none"> • Other: No message has been received. • Success: The SNTP operation was successful, and the system time has been updated. • Request Timed Out: The SNTP request timed out without receiving a response from the server. • Bad Date Encoded: The time provided by the SNTP server is invalid. • Version Not Supported: The SNTP version supported by the server is not compatible with the switch's version. • Server Unsynchronized: The SNTP server is not synchronized with its peers. This is indicated via the <i>leap indicator</i> field on the SNTP message. • Server Kiss Of Death: The SNTP server has indicated that no further queries are to be sent to this server. This is indicated by a stratum field of 0 in a message received from a server.
Server IP Address	The IP address of the server of the last valid packet received. An empty string is shown if no valid packet is received.
Address Type	The address type of the SNTP server address of the last valid packet received.
Server Stratum	The stratum of the server of the last valid packet received.
Reference Clock ID	The reference clock identifier of the last valid packet received.
Server Mode	The mode of the server of the last valid packet received.
Unicast Server Max Entries	The maximum number of unicast server entries configurable for the switch.
Unicast Server Current Entries	The current number of valid unicast server entries configured on the switch.
Broadcast Count	The number of unsolicited broadcast SNTP messages received and processed by the SNTP client since the last time the switch was restarted.

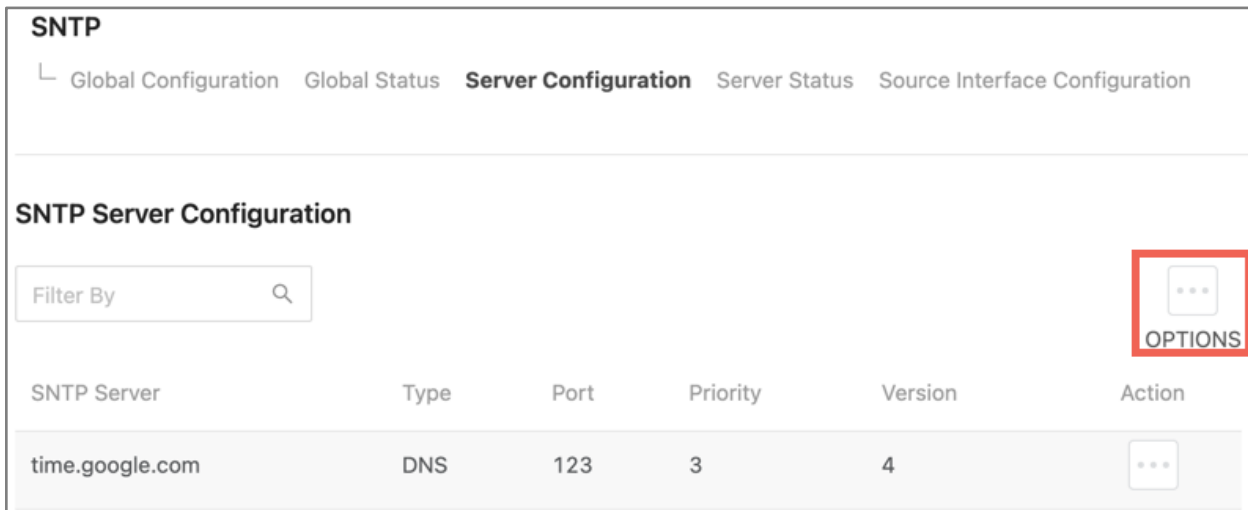
SNTP Server Configuration

Advanced > SNTP > Server Configuration

Use this page to add and modify information for SNTP Servers.

To add an SNTP Server:

1. Click the **Options** (⋮) button, then click **Add**.



2. A new window appears. Use the table below to fill in the fields, then click **Save** to close the window.

Field	Description
SNTP Server Name or IP Address	The address or SNTP server name of the SNTP server being used to synchronize the system time. It can be the IPv4 address, IPv6 address, or Hostname.
SNTP Server Type	IPv4, IPv6, or DNS.
Port	The port number being used to communicate with the SNTP server.
Priority	Enter a priority between 1 and 3. 1 being the highest priority. The switch attempts to use the highest priority server, and if unavailable, uses the next highest server.
Version	The protocol version number.

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

Use the **Action** (⋮) button to edit or delete a SNTP server configuration.

Server Status

Advanced > SNTP > Server Status

This page display information about the status of the SNTP servers configured on the switch. Use the **Options** (⋮) button to refresh the page for the most current information.

The below table describes the information in each column.

Field	Description
Address	Lists all the existing SNTP server addresses.
Last Update Time	The local date and time (UTC) that this SNTP server was used to update the system clock.
Last Attempt Time	The local date and time (UTC) that this server was last queried.

Last Attempt Status	<p>The status of the last SNTP request or unsolicited message for both unicast and broadcast modes. Possible statuses include:</p> <ul style="list-style-type: none"> • Other: No message has been received. • Success: The SNTP operation was successful, and the system time has been updated. • Request Timed Out: The SNTP request timed out without receiving a response from the server. • Bad Date Encoded: The time provided by the SNTP server is invalid. • Version Not Supported: The SNTP version supported by the server is not compatible with the switch's version. • Server Unsynchronized: The SNTP server is not synchronized with its peers. This is indicated via the <i>leap indicator</i> field on the SNTP message. <p>Server Kiss Of Death: The SNTP server has indicated that no further queries are to be sent to this server. This is indicated by a stratum field of 0 in a message received from a server.</p>
Requests	The number of SNTP request made to this server since the last time the switch was restarted.
Failed Requests	The number of failed SNTP requests made to this server since the last time the switch was restarted.

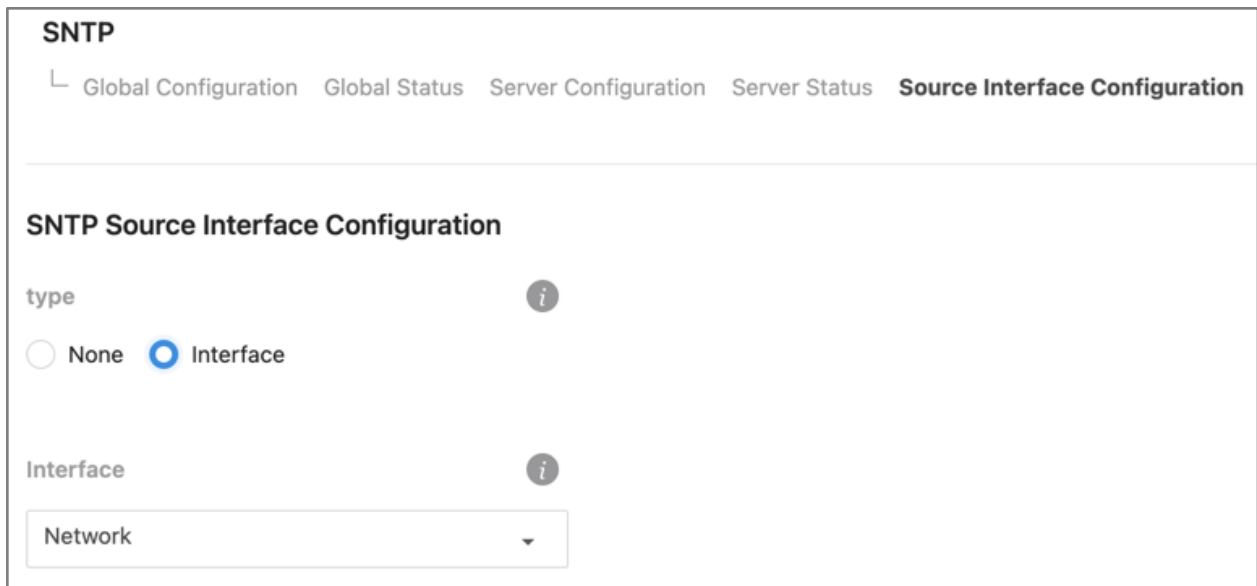
Source Interface Configuration

Advanced > SNTP > Source Interface Configuration

Use this page to specify the physical or logical interface to use as the SNTP client source interface. When an IP address is configured on the source interface, the IP address is used in the IP header of SNTP management packets for all SNTP communications between the between the local SNTP client and the remote SNTP server. This allows security devices, like firewalls, to identify incoming source packets from a specific device.

To configure an SNTP source interface:

3. Select a source interface **type**. There are two options to choose from:
 - **None:** The primary IP address of the originating (outbound) interface is used as the source address.
 - **Interface:** The primary IP address of the physical switchport is used as the source address.



4. The **Interface** dropdown cannot be changed. The interface includes the physical port, VLAN routing interface, and the network source IP.
5. Click **Apply** at the top of the page.

System Statistics

Pages in the Statistics section contain information about the amount and types of traffic the switch is transmitting and receiving.

Switch Statistics

Advanced > System Statistics > Switch

The below table describes each field for the header they're under.

Use the **Options** (⋮) button to refresh the statics for a specific heading or click the **Clear Counters** button to clear all the statistics information on the page.

Heading	Field	Description
System	Interface	The interface index object value of the interface table entry associated with the switch's processor. Use this value to identify the interface when managing the switch with SNMP.
	Time Since Counters Last Cleared	The amount of time in days:hours:minutes:seconds since the statistics for the switch have been reset.
Statistics	Octets Without Error	The total number of octets (bytes) of successfully transmitted or received data by the processor. This number includes FCS octets but excludes framing bits.
	Packets Without Errors	The total number of packets successfully transmitted or received by the processor. Includes unicast, broadcast, and multicast packets.

	Packets Discarded	The number of packets chosen to be discarded to prevent them from being deliverable to a higher-layer protocol. Such as discarding packets to free up buffer space.
	Unicast Packets	The number of subnetwork-unicast packets transmitted or received from a higher-layer protocol.
	Multicast Packets	The number of packets transmitted or received being directed to a multicast address.
	Broadcast Packets	The number of packets transmitted or received being directed to a broadcast address.
Status	Current Usage	In the FDB entries column, the value is the number of learned and static entries in the MAC address table. In the VLANs column, the number shows the number of static and dynamic VLANs that exist in the VLAN database.
	Peak Usage	The highest number of entries in the MAC address table or VLAN database that an admin statically configured.
	Maximum Allowed	The maximum number of statically configured or dynamically learned entries allowed in the MAC address table or VLAN database.
	Static Entries	The current number of statically configured entries in the MAC address table or VLAN database that an admin configured.
	Dynamic Entries	The current number of dynamically learned entries in the MAC address table or VLAN database that an admin configured.
	Total Entries Deleted	The number of VLANs created and since deleted since the last time the switch was restarted. This field is not applicable to MAC address table entries.

Port Summary Statistics

Advanced > System Statistics > Port Summary

This table shows statistics about the packets transmitted and received for individual interfaces (switchports and LAGs).

Use the table below for descriptions of each table column.

Column	Description
Interface	The interface (switchport or LAG) number.
Name	The name given to the interface.
Rx Good	The total number of inbound packets received by the interface without error.
Rx Errors	The total number of inbound packets containing errors, preventing them from being deliverable on the interface.
Rx Bcast	The total number of inbound packets received by the interface directed to a broadcast address. This does not include multicast packets.
Tx Good	The total number of outbound packets received by the interface without error.
Tx Errors	The total number of outbound packets containing errors, preventing them from being transmitted.
Tx Collisions	The best estimate of the total number of collisions on the interface.

The Options (⋮) button has two options for altering the data:

- **Refresh:** Refreshes the data onscreen with the most current data for the switch.
- **Clear:** Clears all the data from the table.

Port Detailed Statistics

Advanced > System Statistics > Port Detailed

This page allows you to select an interface and view detailed statistics about it, such as the **Maximum Frame Size, MTU,** and the **Packet Lengths Received and Transmitted.**

Use the **Interface** dropdown to select a switchport or LAG. Click the **Options** (⋮) button to Refresh the page for the most current statistics.

Class of Service

Class of Service (CoS) allows you to directly configure certain aspects of switch queueing, which allows 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.

The MS switch supports up to seven configurable queues per port. The eighth queue is reserved for the internal stacking subsystem.

How to Map IP DSCP

Advanced > Class of Service > IP DSCP

Use the IP DSCP Mapping Table to map an **IP DSCP value** to a **Traffic Class.**

Class of Service		
└ IP DSCP Interface Queue		
IP DSCP		
Filter By <input type="text"/>		⋮ OPTIONS
IP DSCP	Traffic Class	Action
0	1	⋮
1	1	⋮

Click the **Action** (⋮) button to assign individual IP DSCP values to a Traffic Class.

Click the **Options** (⋮) button to assign multiple IP DSCP values to the same Traffic Class.

Click **Apply**, at the top of the page, when done.

How to Apply Interface Shaping Rates

Advanced > Class of Service > Interface

Use the table to apply an interface shaping rate to individual interfaces or to all at once.

Class of Service				
IP DSCP Interface Queue				
IP Interface Configuration				
Filter By <input type="text"/>				...
OPTIONS				
Interface	Name	Trust Mode	Shaping Rate	Action
0/1	UL - Lab Rack MS-2416	Trust IP-DSCP	0	...
0/2	Home PC	Trust IP-DSCP	0	...

1. Click the **Action** (⋮) button to edit individual interfaces. Click the **Options** (⋮) button to edit multiple.
2. A new window appears with two fields to configure. Click **Save** after entering values.

Field	Description
Trust Mode	Select the Trust Mode for ingress traffic on the interface. The options are: <ul style="list-style-type: none"> • Untrusted: The interface ignores all priority designations in incoming packets and sends them to a traffic queue based on the ingress port's default priority. • Trust dot1p: The port accepts the designated 8021.p priority encoded in the arriving packets. • Trust IP – DSCP: The port accepts the designated IP DSCP priority encoded in the arriving packets.
Shaping Rate	The maximum amount of traffic that can leave an interface. The specified value is a percentage of the maximum negotiated bandwidth.

3. Click the **Apply** button at the top of the page.

How to Configure CoS Interface Queues

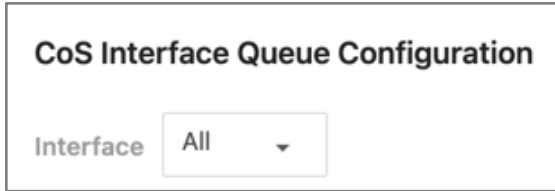
Advanced > Class of Service > Queue

Use this page to designate what a queue does by configuring switch egress queues. Configurable queue parameters include bandwidth allocations and the scheduling of packet transmissions from the set of all queues on a port.

CoS queue parameters can be configured for individual interfaces or across all interfaces.

To configure CoS interface queues:

1. Select an **Interface**. This can be an individual switchport or LAG.



2. Select an individual **Queue ID** by clicking the **Action** (⋮) button in the corresponding row, or click the **Options** (⋮) button to select multiple Queue IDs to configure.

Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type	Action
0	0	Weighted	Taildrop	⋮
1	0	Weighted	Taildrop	⋮

3. The **Edit CoS Interface Queue Configuration** window opens. Use the table below to configure the available fields, then click **Save**.

Field	Description
Queue ID	Specifies the selected Queue ID or IDs.
Minimum Bandwidth	The minimum guaranteed bandwidth allocated to the queue on the interface. Settings this value higher than the maximum bandwidth automatically increases the maximum to the same value. A value of zero means there is no guaranteed minimum. The sum of individual Minimum Bandwidth values for all queues in the selected interface cannot exceed 100.
Scheduler Type	Select one of the following: <ul style="list-style-type: none"> • Weighted: Weighted round robin associates a weight to each queue. • Strict: Services traffic with the queue's highest priority first.
Queue Management Type	Only Taildrop is available. This is only used if the connected device supports independent settings per-queue. All packets on a queue are safe until congestion occurs, at which time any additional packets are queued.

4. When the window closes, click the **Apply** button to save changes.

Use the **Restore Default** toggle or click **Options** (⋮), then **Refresh** to clear all configurations.

Access Control List Rules

Access Control Lists (ACLs) make sure that only authorized users have access to specific resources and block unwanted attempts by filtering packets based on rules. ACLs are used to control traffic flow, restrict the contents of routing updates, decide which types of traffic to block or forward, and provide network security. Pagedge MS switches support IPv4 and MAC ACLs.

To create an ACL, you must:

1. Create an **ACL rule** with an **identifier** (ACL ID) on the *Summary* page.

2. Define the ACL rule.
3. Assign the ACL ID to a switch port or VLAN interface.

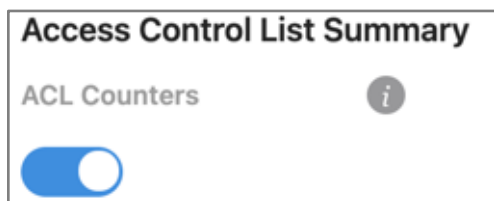
How to add an ACL Type and Identifier

Advanced > Access Control List > ACL Rule Settings > Summary

The Summary page is used to add an ACL type and identifier.

ACL Counters

Toggle **ACL Counters** on to monitor the number of matches the switch has detected for each ACL.




Adding an ACL


To add an ACL, click the **Options** (⋮) button and select **Add**. The table below describes the configurable fields.


Field	Description
ACL Identifier	A name or number that identifies an ACL. Standard and Extended IPv4 ACLs use numbers, while Named IPv4 and MAC ACLs use alphanumeric characters.
ACL Type	<p>Determines the criteria used to match packets and which attributes can be applied to matching traffic.</p> <p>IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic. IPv6 ACLs classify Layer 3 and Layer 4 IPv6 traffic. MAC ACLs classify Layer 2 traffic.</p> <p>Configurable ACL Types include:</p> <ul style="list-style-type: none"> • IPv4 Standard: Match criteria is based on the source address of the IPv4 packets. • IPv4 Extended: Match criteria can be based on the source and destination addresses, source and destination Layer 4 ports, and protocol type of the IPv4 packets. • IPv4 Named: Match criteria is identical to IPv4 Extended ACLs, but the <i>ACL Identifier</i> can be alphanumeric. • IPv6 Named: Match criteria can be based on the source and destination IPv6 addresses, source and destination Layer 4 ports, and the protocol type within IPv6 packets. • Extended MAC: Match criteria can be based on the source and destination MAC addresses, 8021.p user priority, VLAN ID, and EtherType value within Ethernet frames.



Table Summary

Access Control List Summary

ACL Counters 

Filter By 

 OPTIONS

ACL Identifier	ACL Type	Rules Used	Direction	Interfaces	VLANS	Action
EXC_default_list	IPv4 Named	9	Inbound	0/1, 0/2, 0/3, 0/4, 0/5, 0/6, 0/7, 0/8, 0/9, 0/10, 0/11, 0/12, 0/13, 0/14, lag 1, lag 2, lag 3, lag 4, lag 5, lag 6		
Dante	Extended MAC	0	Inbound			

Field	Description
ACL Identifier	A name or number that identifies an ACL. Standard and Extended IPv4 ACLs use numbers, while Named IPv4 and MAC ACLs use alphanumeric characters.
ACL Type	The criteria used to match packets and which attributes can be applied to matching traffic. IPv4 ACLs classify Layer 3 and Layer 4 IPv4 traffic. IPv6 ACLs classify Layer 3 and Layer 4 IPv6 traffic. MAC ACLs classify Layer 2 traffic.
Rules used	The number of rules configured for the ACL.
Direction	Indicates if the packet is checked against ACL rules when it is received on an interface (Inbound) or after it has been received, routed, and ready to exit an interface (Outbound).
Interfaces	The interfaces (switchports or LAGs) the ACL is applied to.
VLANS	Each VLAN the ACL is applied to.
Action Button	Edit or Delete .

How to Associate an ACL with an Interface

Advanced > Access Control List > ACL Rule Settings > Interfaces

Use the *Interfaces* page to associate an ACL with one or more interfaces. When an ACL is associated with an interface, traffic on the port is checked against the rules defined by the ACL. If the traffic does not match any of the rules it is dropped because of the deny all rule at the end of each ACL.

To Apply an ACL to an Interface:

Click the **Options** () button, then **Add**. The table below describes each field.

Add ACL Interface Configuration ✕

Interface i

x 0/1

Direction i

Inbound

Sequence Number i

0

ACL Identifier i

EXC_default_list

Cancel
Add

Field	Description
Interface	The switchports or LAGs the ACL is being applied to.
Direction	Indicates if the traffic is checked against the ACL rules as it is received on an interface (Inbound) or after it is received, routed, and ready to exit the interface (Outbound).
Sequence Number	The order that the ACL is applied to relative to other ACLs associated with the interface, in the same direction (inbound or outbound). The ACL with the lowest number is the first in the sequence.
ACL Identifier	The name or number of the ACL, configured on the <i>Summary</i> page. The ACL Identifier menu only includes the ACLs within the selected ACL type.

Table Summary

Access Control List Rules						
Summary Interfaces VLANs Statistics						
Access Control List Interface Summary						
Filter By <input type="text"/>						...
OPTIONS						
Interface	Name	Direction	Sequence Number	ACL Type	ACL Identifier	Action
0/1	UL - Lab Rack MS-2416	Inbound	10	IPv4 Extended	EXC_default_list	...
0/2	Home PC	Inbound	10	IPv4 Extended	EXC_default_list	...
0/3	Office WB-250-IPW-2	Inbound	10	IPv4 Extended	EXC_default_list	...

Field	Description
Interface	The switchports or LAGs the ACL is being applied to.
Name	The name given to the interface. Configurable on the <i>Interfaces</i> tab.
Direction	Indicates if the traffic is checked against the ACL rules as it is received on an interface (Inbound) or after it is received, routed, and ready to exit the interface (Outbound).
Sequence Number	The order that the ACL is applied to relative to other ACLs associated with the interface, in the same direction (inbound or outbound). The ACL with the lowest number is the first in the sequence.
ACL Type	Either IPv4, IPv6, or MAC.
ACL Identifier	The name or number of the ACL, configured on the <i>Summary</i> page. The ACL Identifier menu only includes the ACLs within the selected ACL type.
Action Button	Use to Delete an interface configuration.

How to add ACLs to VLANs

Advanced > Access Control List > ACL Rule Settings > VLANs

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

To Apply an ACL to VLAN:

Click the **Options** (⋮) button, then **Add**. The table below describes each field.

Add ACL VLAN Configuration ✕

VLAN ID i

Direction i

Inbound

Sequence Number i

ACL Identifier i

Cancel
Add

Field	Description
VLAN ID	The VLAN ID the ACL is applied to.
Direction	Indicates if the traffic is checked against the ACL rules as it is received on an interface (Inbound) or after it is received, routed, and ready to exit the interface (Outbound).
Sequence Number	The order that the ACL is applied to relative to other ACLs associated with the interface, in the same direction (inbound or outbound). The ACL with the lowest number is the first in the sequence.
ACL Identifier	The name or number of the ACL, configured on the <i>Summary</i> page. The ACL Identifier menu only includes the ACLs within the selected ACL type.

Table Summary

Field	Description
VLAN ID	The VLAN ID the ACL is applied to.
Direction	Indicates if the traffic is checked against the ACL rules as it is received on an interface (Inbound) or after it is received, routed, and ready to exit the interface (Outbound).
Sequence Number	The order that the ACL is applied to relative to other ACLs associated with the interface, in the same direction (inbound or outbound). The ACL with the lowest number is the first in the sequence.
ACL Type	Either IPv4, IPv6, or MAC.
ACL Identifier	The name or number of the ACL, configured on the <i>Summary</i> page. The ACL Identifier menu only includes the ACLs within the selected ACL type.
Action Button	Use to Delete an interface configuration.

ACL Statistics

Advanced > Access Control List > ACL Rule Settings > Statistics

Use this page to view how many packets an ACL has forwarded or discarded, until the number reaches the rollover value of the counter. ACL counters do not interact with DiffServ policies or policy-based routing counters.

To View and Sort the Statistics:

There are two dropdowns to sort the statistics table.

- **ACL Type:** The type of ACL.
- **ACL Identifier:** A list of ACL IDs configured on the switch for the ACL type.

Click the **Options** (⋮) button, then **Refresh** to clear the filters.

To Clear the Counters:

1. Click the **Options** (⋮) button, then **Clear**.

2. Select a **Clear Counter Mode**.

If **Rule** counter is selected, ACL Identifier and Sequence Number must be provided. If clear **ACL** counter is selected, the user can provide ACL Type to clear the hit count of all ACLs in that type, or provide an ACL Identifier to clear the hit count of that ACL.

3. Click **OK**.*Table Summary*

Access Control List Rules				
Summary Interfaces VLANs Statistics				
Access Control List Statistics				
ACL Type	IPv4 Extended ▾			
ACL Identifier	EXC_default_... ▾			
Filter By				⋮
				OPTIONS
Sequence Number	Perform Action	Match Conditions	Rule Attributes	Hit Count
10	Permit	Match all: False Protocol: UDP Destination L4 Port: 9998 Destination IP: 239.254.3.3 Destination Mask: 0.0.0.0		0
20	Permit	Match all: False Protocol: UDP Destination IP: 239.255.255.250 Destination Mask: 0.0.0.0		1412926

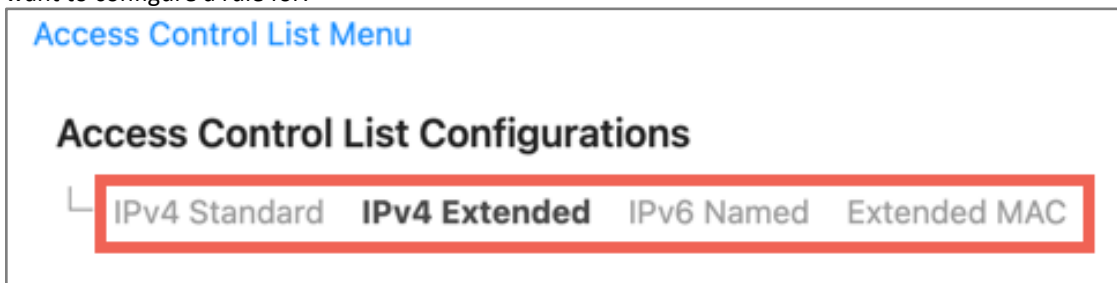
Field	Description
Sequence Number	The number that indicates the rule position within the ACL.
Perform Action	Permit or Deny.
Match Conditions	The criteria used to determine if the network traffic matches the ACL rule.
Rule Attributes	Each action the ACL rule performs.
Hit Count	The number of packets that match the ACL rule. If a rule does not have a rate limit, the hit count is the number of matched packets the port forwarded or discarded. If a rule has a rate limit, and the sent traffic exceeds the configured rate, the hit count display the matched packet count equal to the sent rate. If the sent traffic rate is less than the configured rate, the hit count displays only the matched packet count.

ACL Rule Configurations

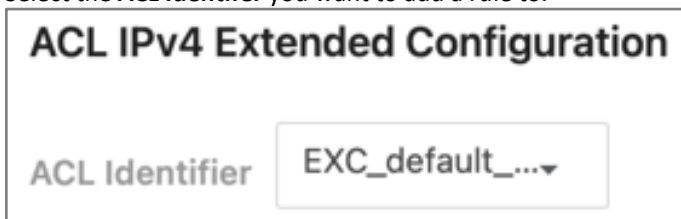
Each ACL rule must match one or more characteristics of the network traffic. When a packet matches an ACL rule condition the rule can either **Permit** or **Deny** the packet. A packet must match all the specified criteria for an ACL action (Permit or Deny) to take place. An ACL can have multiple rules, but the final rule is a deny all rule.

To Create an ACL Rule:

1. ACLs must be created at **Advanced > Access Control List > ACL Rule Settings > Summary** before rules can be configured.
2. Navigate to **Advanced > Access Control List > ACL Configurations** and click the tab of the **ACL Type** you want to configure a rule for.



3. Select the **ACL Identifier** you want to add a rule to.



4. Click the **Options** (⋮) button, **Add**, then fill in the following fields described in the below table. Click **Add**, at the bottom of the pop-up window, when done.

Field	Description
Sequence Number	<p>This number indicates the position of the rule in the ACL. If a number is not specified, the rule is automatically assigned one.</p> <p>Rules are displayed by their position in the ACL and can be renumbered.</p> <p>Packets are checked against the rules in order of low to high. If a packet matches the rule criteria it is either Permitted or Denied.</p> <p>If the packet does not match a rule, it is discarded based on the deny all rule each ACL has as the final rule.</p>
Perform Action	<p>The action that takes place when a packet matches a rule's criteria. This can be:</p> <ul style="list-style-type: none"> • Permit: The packet or frame is forwarded. • Deny: The packet or frame is dropped. <p>Note: The action selected determines the fields that follow.</p>
Remark	For personal notes. Accepts alphanumeric characters. Click the –(minus) button to delete a remark.
Every	If selected, all packets match the rule criteria and are either permitted or denied. If selected, no other match criteria can be configured.

Protocol	<i>IPv4 and IPv4 Named ACLs only.</i> The IANA-assigned protocol number to match within the packet. The following keywords can be specified: EIGRP, GRE, ICMP, IGMP, IP, IPINIP, OSPF, PIM, TCP, or UDP.
Fragments	<i>IPv4 and IPv4 Named ACLs only.</i> If selected, this rule matches on fragmented IP packets.
Source IP Address	The packet's source IP address and Source Wildcard Mask (next field) to compare to the IP address in a packet header.
Source Wildcard Mask	Determines which bits in the IP address are used and which are ignored. A wildcard mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. With a subnet mask, the mask has ones in the bit positions used for the network address and has zeros for the bit positions not used. In contrast, a wildcard mask has zeroes in a bit position that must be checked. A one in a bit position of the ACL mask indicates that the corresponding bit can be ignored. This field is required when you configure a destination IP address.
Source L4 Port Option	<i>IPv4 and IPv4 Named ACLs only.</i> Whether the packet's source L4 port value should be Equal, Not Equal, Less Than, Greater Than, or a Range.
Source L4 Port Value	<i>IPv4 and IPv4 Named ACLs only.</i> The TCP/UDP source port, or port range, to check for. Keywords can also be used, including: BGP, Domain, Echo, FTP, FTP Data, HTTP, SMTP, Telnet, POP2, and POP3. UDP port keywords include Domain, Echo, NTP, RIP, SNMP, TFTP, TIME, and WHO.
Source L4 Port Range Upper Bound	TCP port keywords include BGP, Domain, Echo, FTP, FTP Data, HTTP, SMTP, Telnet, POP2, and POP3. UDP port keywords include Domain, Echo, NTP, RIP, SNMP, TFTP, TIME, and WHO. If it is not a keyword, it would be a string that is between 0 and 65535.
Destination IP Address	The packet's destination IP address and Source Wildcard Mask (next field) to compare to the IP address in a packet header.
Destination Wildcard Mask	Determines which bits in the IP address are used and which are ignored. A wildcard mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. With a subnet mask, the mask has ones in the bit positions used for the network address and has zeros for the bit positions not used. In contrast, a wildcard mask has zeroes in a bit position that must be checked. A one in a bit position of the ACL mask indicates that the corresponding bit can be ignored. This field is required when you configure a destination IP address.
Destination L4 Port Option	<i>IPv4 and IPv4 Named ACLs only.</i> Whether the packet's destination L4 port value should be Equal, Not Equal, Less Than, Greater Than, or a Range.
Destination L4 Port Value	<i>IPv4 and IPv4 Named ACLs only.</i> The TCP/UDP destination port, or port range, to check for. Keywords can also be used, including: BGP, Domain, Echo, FTP, FTP Data, HTTP, SMTP, Telnet, POP2, and POP3. UDP port keywords include Domain, Echo, NTP, RIP, SNMP, TFTP, TIME, and WHO.
Destination L4 Port Range Upper Bound	TCP port keywords include BGP, Domain, Echo, FTP, FTP Data, HTTP, SMTP, Telnet, POP2, and POP3. UDP port keywords include Domain, Echo, NTP, RIP, SNMP, TFTP, TIME, and WHO. If it is not a keyword, it would be a string that is between 0 and 65535.
TTL Field Value	<i>IPv4 and IPv4 Named ACLs only.</i> The Time-to-Live value to check against. A number between 0 and 255.

IGMP Type	<i>IPv4 and IPv4 Named ACLs only.</i> IGMP message type to check against. This option is only available is the protocol is IGMP.
ICMP Type	<i>IPv4 and IPv4 Named ACLs only.</i> ICMP message type to check against. This option is only available is the protocol is ICMP.
ICMP Code	<i>IPv4 and IPv4 Named ACLs only.</i> ICMP message code to check against. This option is only available is the protocol is ICMP.
ICMP Message	<i>IPv4 and IPv4 Named ACLs only.</i> Specify one of the following supported ICMP messages: Echo, Echo-Reply, Host-Redirect, Mobile-Redirect, NetRedirect, Net-Unreachable, Redirect, Packet-Too-Big, Port-Unreachable, Source-Quench, Router-Solicitation, Router-Advertisement, TimeExceeded, TTL-Exceeded, and Unreachable. This option is available only if the protocol is ICMP.
TCP Flags	<i>IPv4 and IPv4 Named ACLs only.</i> When a + flag is specified, a match occurs if the flag is set in the TCP header. When a - flag is specified, a match occurs if the flag is not set in the TCP header. If Established is selected, a match occurs if either RST or ACK bits are set in the TCP header. This option is available only if the protocol is TCP.
IP DSCP	The IP DSCP value in the IPv6 packet to match to the rule. The DSCP value is defined as the high-order six bits of the Service Type octet in the IPv6 header.
IP Precedence	The IP Precedence field in a packet is defined as the high-order three bits of the Service Type octet in the IP header.
IP TOS Bits	Matches based on the Type of Service (TOS) bits in the IP header. The IP TOS field in a packet is defined as all eight bits of the Service Type octet in the IP header. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a TOS Bits value of 0xA0 and a TOS Mask of 0xFF. Requires the bits in a packet's TOS field to match the two-digit hexadecimal number entered in this field.
IP TOS Wildcard Mask	The bit positions used for comparison against the IP TOS field in a packet. Specifying TOS Mask is optional. The format is the same as IP TOS Bits: two-digit hexadecimal numbers.
Assign Queue	The number that identifies the hardware egress queue that handles all the packets matching this rule.
Interface	The switchports or LAGs the ACL is being applied to.
Interface Action	Redirect: Redirects traffic, that matches the rule, to the selected interface instead of being processed on the original port. The redirect function and mirror function are mutually exclusive. Mirror: Mirrors traffic, that matches the rule, to the selected interface. Mirroring is like the redirect function, except that in flow-based mirroring a copy of the permitted traffic is delivered to the mirror interface while the packet is forwarded normally through the device.
Log	If selected, the ACL rule is logged.
Time Range Name	The name of the time range that imposes a time limitation on the ACL rule. If a time range with the specified name does not exist, and the ACL containing this ACL rule is associated with an interface, the ACL rule is applied immediately. If a time range with the specified name exists, and the ACL containing this ACL rule is associated with an interface, the ACL rule is applied when the time-range with the specified name becomes active. The ACL rule is removed when the time-range with the specified name becomes inactive. It can be between 1 to 31 characters.
Committed Rate	The allowed transmission rate for packets on the interface.

Burst Size	They number of bytes allowed during temporary traffic bursts.
------------	---

DiffServ

DiffServ (Differentiated Services) allows traffic to be classified into streams and given QoS treatment with defined per-hop behaviors. Packets are classified and processed by specified criteria that's defined by a class.

Policy attributes may be defined on a per-class instance basis and are applied when a match occurs. A policy can contain multiples classes. When the policy is active, the actions taken depend on which class matches the packet.

Global Configuration

Advanced > Diffserv > Global

Use this page to enable DiffServ and view the MIB table.

Enabling DiffServ

Diffserv

[Global](#)
[Class Summary](#)
[Class Configuration](#)
[Policy Summary](#)
[Policy Configuration](#)
[Service Summary](#)

Diffserv Global Configuration and Status

Enable i

Enable to use DiffServ. When **Disabled**, DiffServ configuration is saved and can be changed. Click **Apply**, in the top right corner of the page, to save changes.

MIB Table

MIB Table	Current Number / Maximum Number
Class Table	1/32
Class Rule Table	0/192
Policy Table	0/32
Policy Instance Table	0/896
Policy Attribute Table	0/2688
Service Table	0/58

Each row shows the **Current** and **Maximum Number** of each rule or policy entries, in a Current Number / Maximum Number format.

Class Summary

Advanced > Diffserv > Class Summary

Use this page to create or remove DiffServ classes and to view a summary of each class on the switch. The **Action** (⋮) button can be used to **Edit** or **Delete** an existing class.

Diffserv

Global **Class Summary** Class Configuration Policy Summary Policy Configuration Service Summary

Diffserv Class Summary

Filter By ⋮
OPTIONS

Name	Type	Protocol	Match Criteria	Action
TestClass	All	IPv4		⋮

To Add a DiffServ Class:

1. Click the **Options** (⋮) button to **Add** a new Class.

The 'Add Class' dialog box is shown with the following fields and options:

- Class Name:** A text input field.
- Type:** Radio buttons for 'All' (selected) and 'Any'.
- Protocol:** Radio buttons for 'IPv4' (selected) and 'IPv6'.
- Buttons:** 'Cancel' and 'Add'.

2. Enter a **Class Name**.
3. Specify a **Class Type**:
 - **All:** All the DiffServ Class criteria must be met for a packet match.
 - **Any:** If any of the DiffServ Class criteria are met there is a packet match.
4. Select the **Protocol** to use for filtering class types. Either **IPv4** or **IPv6**, then click **Add**.

Class Configuration

Advanced > Diffserv > Class Configuration

Use this page to add Match Criteria to a DiffServ class.

To add criteria to a DiffServ Class:

1. Use the **Class** dropdown to select a previously created class.

The 'Diffserv Class Configuration' page shows a dropdown menu for 'Class' with 'TestClass' selected.

2. Click the **Options** (⋮) button, then **Add**, for the **Add Match Criteria** window to appear.

Diffserv Class Configuration

Class

Type i

L3 Protocol i

Filter By Q

Match Criteria
Value
Action

⋮
 OPTIONS

3. Use the table below to help you configure the match criteria. Only enter values into the fields needed. Click **Add**, to save the match criteria.

Field	Description
Any	Toggle on for all packets to match this class. If on, no other match criteria needs to be configured.
Reference Class	Select another class to match the criteria defined within. A class can reference only one other class.
Class of Service	Select the Class of Service (CoS) value required in the packet header to the criteria.
Secondary Class of Service	Select a secondary Class of Service (CoS) value required in the packet header to the criteria.
EtherType Keyword	Select a protocol to require the EtherType value in the Ethernet frame header to the criteria.
EtherType Value	Enter a custom EtherType value to the criteria.
VLAN ID	Enter a VLAN ID, or ID range. If you configure a range, a match occurs if a packet's VLAN ID is the same as any VLAN ID within the range.
Secondary VLAN ID	Enter a secondary VLAN ID, or ID range. If you configure a range, a match occurs if a packet's VLAN ID is the same as any VLAN ID within the range.
Source MAC Address	Enter a source MAC address to add to the criteria.
Source MAC Mask	The MAC mask, which specifies the bits in the source MAC address to compare against an Ethernet frame. Use F's and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means the data is insignificant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note: This not a wildcard mask, like ACLs use.
Destination MAC Address	Enter a destination MAC address to add to the criteria.

Destination MAC Mask	<p>The MAC mask, which specifies the bits in the destination MAC address to compare against an Ethernet frame. Use F's and zeros to configure the MAC mask.</p> <p>An F means that the bit is checked, and a zero in a bit position means the data is insignificant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number).</p> <p>Note: This not a wildcard mask, like ACLs use.</p>
IP Precedence	The IP Precedence field in a packet is defined as the high-order three bits of the Service Type octet in the IP header.
IP Type of Service (ToS) Bits	Enter a two-digit hexadecimal number to match the bits in a packet's ToS field.
IP Type of Service Mask	Specify the bit positions that are used for comparison against the IP ToS field in a packet.
Protocol	Select a keyword to add to the criteria. If you use this option, you cannot enter a Protocol Value.
Protocol Value	Enter an IANA L4 protocol number to add to the criteria.
Source L4 Protocol	Select an L4 keyword from the list to add to the criteria. If you select a keyword, you cannot enter a Source L4 Port value.
Source L4 Port	Enter a source port, or port range, to add to the criteria. If you configure a range, a match occurs if a packet's source port number is the same as any destination port number within the range.
Destination L4 Protocol	Select an L4 keyword from the list to add to the criteria. If you select a keyword, you cannot enter a Destination L4 Port value.
Destination L4 Port	Enter a destination port, or port range, to add to the criteria. If you configure a range, a match occurs if a packet's destination port number is the same as any destination port number within the range.
IP DSCP Keyword	<p>Select a IP DSCP keyword code to add to the criteria. If you select a keyword, you cannot configure an IP DSCP Value.</p> <p>Note: <i>be</i> and <i>cs0</i> are identical.</p>
IP DSCP Value	Enter an IP DSCP Value to add to the criteria.

Policy Summary

Advanced > Diffserv > Policy Summary

Use this page to create or remove DiffServ policies. The table summarizes information about the policies configured on the switch.

To add a Policy:

1. Click the **Options** (⋮) button, then **Add**.

2. Enter a **Policy Name**.
3. The **Type** field has one option to enable. Select **In**, to apply the policy to inbound traffic. Deselect the field to apply the policy to outbound traffic. Click **Add** when finished.

Policy Configuration

Advanced > Diffserv > Policy Configuration

Use this page to configure policy attributes. The policy attributes identify the action or actions taken when a packet matches a class rule.

To add policy attributes:

1. Select a configured **Policy**.
2. Click the **Options** (⋮) button, then **Add**, for the **Add Policy Attribute** window to appear.

3. Use the table below to help you configure the match criteria. Only enter values into the fields needed. Click **Add**, to save the match criteria.

Field	Description
Class	The DiffServ class associated with the policy. Autofilled.
Assign Queue	Select a Queue ID Value to which the packets of this policy-class are assigned.
Drop	Select this option to drop packets that match the policy-class.
Mark Class of Service	Use this field to mark all packets in a traffic stream with the specified Class of Service (CoS) queue value. Enter a value (0 to 7) to mark in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted.
Mark IP DSCP	Enter a value (1 through 7) to mark packets in the policy's associated traffic stream.
Mark IP Precedence	Enter a value (1 through 7) to mark packets in a traffic stream that matches the policy. The Mark IP Precedence field is then selectable in other fields.
Mirror Interface	Select this option to copy the traffic stream to a specified egress port (physical or LAG) without bypassing normal packet forwarding. This action can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment. Use the dropdown to select the interface to mirror traffic to.
Police Simple Color Mode	Select this option to enable simple traffic policing. Simple policing uses a single data rate and burst size, resulting in either a conform or violate action.
Police Simple Committed Rate (Kbps)	Enter the maximum arrival rate of incoming packets for the policy, in Kbps.
Police Simple Conform Action	Select the action to take on packets below the committed rate (conforms).
Police Simple Violate Action	Select the action to take on packets above the committed rate (violates).
Police Single Rate Color Mode	Select this option to enable single-rate traffic policing. Single-rate policing uses a single data rate and two burst sizes, resulting in a conform , violate , or exceed action.
Police Single Rate Committed Rate (Kbps)	Enter the maximum arrival rate of incoming packets for the policy, in Kbps.
Police Single Rate Committed Burst Size (Kbytes)	Enter the amount of packets allowed in a burst when the arrival rate is under (conforms to) the Single Rate Committed Rate value .
Police Single Rate Conform Action	Select the action to take on packets below the committed rate (conforms).
Police Single Rate Exceed Action	Select the action to take when a burst of packets exceeds the Police Single Rate Committed Burst Rate .
Police Single Rate Violate Action	Select the action to take on packets above the committed rate (violates).
Police Two Rate Color Mode	Select this option to enable simple traffic policing. Two-rate policing uses two data rates and burst sizes, resulting in either a conform , violate or exceed action.
Police Two Rate Committed Rate (Kbps)	Enter the maximum arrival rate of incoming packets for the policy, in Kbps.

Police Two Rate Committed Burst Size (Kbytes)	Enter the amount of packets allowed in a burst when the arrival rate is under (conforms to) the Two Rate Committed Rate value .
Police Two Rate Conform Action	Select the action to take on packets below the committed rate (conforms).
Police Two Rate Exceed Action	Select the action to take when a burst of packets exceeds the Police Two Rate Committed Burst Rate .
Police Two Rate Violate Action	Select the action to take on packets above the committed rate (violates).
Redirect Interface	Allows you to select an interface (switchport or LAG) to force a classified traffic stream to.

Service Summary

Advanced > Diffserv > Service Summary

Use this page to add or remove DiffServ policies to interfaces or edit the policy mappings, by clicking the **Options** (⋮) button.

Diffserv				
Global Class Summary Class Configuration Policy Summary Policy Configuration Service Summary				
Diffserv Service Summary				
Filter By <input type="text"/>				<input type="button" value="⋮"/> OPTIONS
Interface	Direction	Status	Policy	Action
0/1	Inbound		Test	<input type="button" value="⋮"/>
0/2	Inbound		Test	<input type="button" value="⋮"/>

Auto VoIP Configuration

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 make sure the application runs smoothly.

The Auto VoIP feature detects VoIP streams in the switch and provides them a better class of service. Interfaces with Auto VoIP configuration scan incoming traffic for the following protocols:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

When the switch detects a call-control protocol it assigns that session's traffic to the highest CoS queue, generally used for time-sensitive traffic.

Auto VoIP Global Configuration

Advanced > VoIP > Global


Use this page to assign a VLAN to segregate the VoIP traffic from non-VoIP traffic. This feature does not rely on LLDP-MED support from the connected devices.

Enter the VLAN ID to assign the VoIP traffic to.

Auto VoIP

Global OUI Table OUI Based Auto VoIP Protocol Based Auto VoIP

Auto VoIP Global Switch Configuration

Auto VoIP VLAN(0 to reset) 

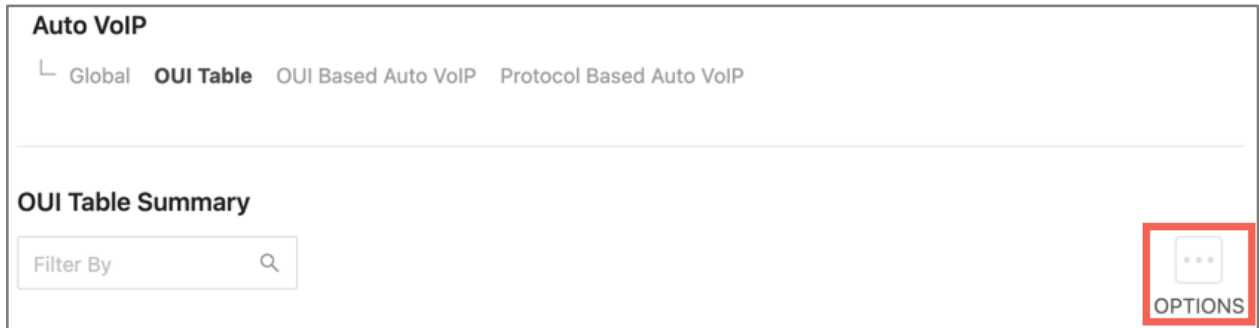
How to Add OUIs

Advanced > VoIP > OUI Table

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.

To add an OUI to the table:

1. Click the **Options** (⋮) button and select **Add**.



Auto VoIP

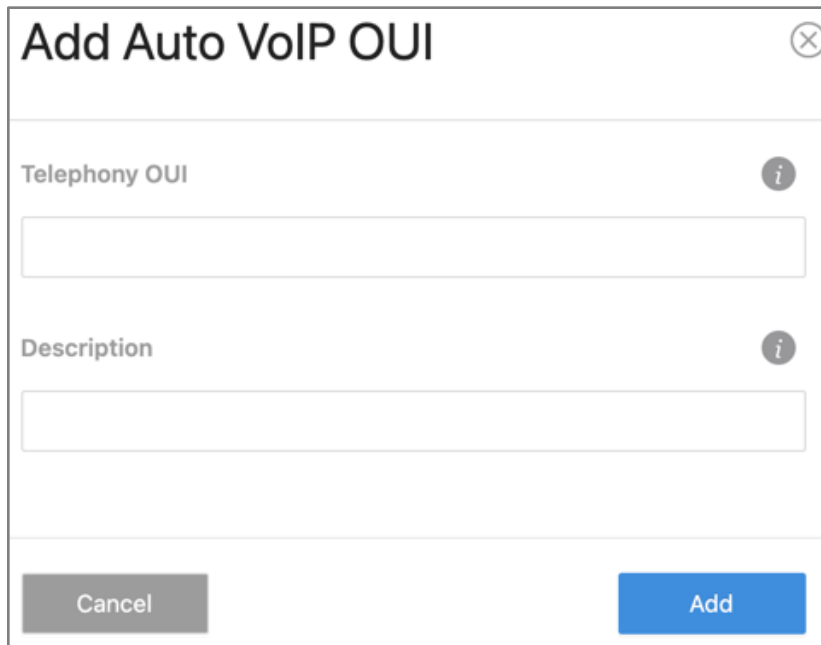
Global **OUI Table** OUI Based Auto VoIP Protocol Based Auto VoIP

OUI Table Summary

Filter By

OPTIONS

2. A new window appears. Enter the **Telephony OUI**.
3. Enter a **Description**, like a manufacturer name, to identify the OUI in the OUI table, then click **Add**.



Add Auto VoIP OUI

Telephony OUI

Description

To **delete** an added OUI, click the **Action** (⋮) button next to its entry.

How to Configure OUI-Based Auto VoIP Priority

Advanced > VoIP > OUI Based Auto VoIP

Enter the **Priority** value to assign configure the 802.1p priority for traffic that matches a configured OUI.

OUI Based Auto VoIP

Auto VoIP VLAN i

30

Priority i

7

The OUI Table allows you to enable Auto VoIP on interfaces and view their operational status.

OUI-based Auto VoIP can be enabled on an interface by:

- Clicking the toggles next to an interface.
- Clicking the **Action** (⋮) button on the far right of the interface row.
- Clicking the **Option** (⋮) button above the table and selecting multiple interfaces.

Enable	Interface	Name	Operational Status	Action
<input checked="" type="checkbox"/>	0/1	UL - Lab Rack MS-2416	Down	⋮
<input checked="" type="checkbox"/>	0/2	Home PC	Up	⋮
<input checked="" type="checkbox"/>	0/3	Office WB-250-IPW-2	Down	⋮

No matter how you select an interface, click the **Apply** button at the top of the page to confirm the selection.

How to Configure Protocol-Based Auto VoIP Priority

Advanced > VoIP > Protocol Based Auto VoIP

Use this page to configure protocol-based Auto VoIP settings and to enable or disable Auto VoIP on an interface.

Select a Prioritization Type:

- **Remark:** Remarks the VoIP traffic with the specified 802.1p priority value at the ingress interface.

The screenshot shows a configuration panel for the 'Remark' prioritization type. At the top, the title 'Prioritization Type' is followed by an information icon. Below this, there are two radio button options: 'Remark' (which is selected) and 'Traffic Class'. Underneath, the label '802.1p Priority' is followed by another information icon. A red rectangular box highlights the empty input field for the 802.1p priority value.

- **Traffic Class:** Assigns VoIP traffic to the specified 802.1p priority value when egressing the interface.

The screenshot shows a configuration panel for the 'Traffic Class' prioritization type. At the top, the title 'Prioritization Type' is followed by an information icon. Below this, there are two radio button options: 'Remark' and 'Traffic Class' (which is selected). Underneath, the label '802.1p Priority' is followed by an information icon. A light gray input field is present but empty. Below that, the label 'Traffic Class' is followed by an information icon. A red rectangular box highlights the input field containing the number '7'.

Protocol-based Auto VoIP can be enabled on an interface by:

- Clicking the toggles next to an interface.
- Clicking the **Action** (⋮) button on the far right of the interface row.
- Clicking the **Option** (⋮) button above the table and selecting multiple interfaces.

Filter By <input type="text"/>					⋮
Enable	Interface	Name	Operational Status	Options	
<input checked="" type="checkbox"/>	0/1	UL - Lab Rack MS-2416	Down	⋮	
<input checked="" type="checkbox"/>	0/2	Home PC	Up	⋮	
<input checked="" type="checkbox"/>	0/3	Office WB-250-IPW-2	Down	⋮	

No matter how you select an interface, click the **Apply** button at the top of the page to confirm the selection.

802.1p (Priority Mapping)

The priority mapping feature allows traffic prioritization at the MAC level by using the 802.1p tag attached to the layer 2 frame. Each switch port has multiple queues to give preference to distinct packets based on the class of service (CoS) criteria specified. The rate at which a packet is sent to a port depends on how the queue is configured and the amount of traffic in other queues for the port. If there must be a delay, packets are held in the queue until the scheduler authorizes the transmission.

802.1p										
└─ 802.1p										
802.1p Priority Mapping										
Filter By <input type="text"/>										⋮
										OPTIONS
Interface	Name	Priority 0	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Priority 6	Priority 7	Action
0/1	UL - Lab Rack MS-2416	1	0	0	1	2	2	3	3	⋮
0/2	Home PC	1	0	0	1	2	2	3	3	⋮
0/3	Office WB-250-IPW-2	1	0	0	1	2	2	3	3	⋮

Field	Description
Interface	The user-configured name of the port or link aggregation group (LAG).
Priority	The heading row of the table that lists the 802.1p priority level (0-7). Incoming frames with an assigned 802.1p priority value are mapped to the corresponding traffic class in the device.
802.1p Priority	The 802.1p priority value to map.
Traffic Class	Traffic class is the data displayed in the table, which is the internal traffic class corresponding to the 802.1p priority level.



11734 S Election Road

Draper, UT 84020

Warranty & Legal information

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

Copyright ©2021, Snap One, LLC. All rights reserved. Snap One and its respective logos are registered trademarks or trademarks of Snap One, LLC (formerly known as Wirepath Home Systems, LLC), in the United States and/or other countries. 4Store, 4Sight, Control4, Control4 My Home, SnapAV, Araknis Networks, BakPak, Binary, Dragonfly, Episode, Luma, Mockupancy, Nearus, NEEO, Optiview, OvrC, Pakedge, Sense, Strong, Strong Evolve, Strong VersaBox, SunBriteDS, SunBriteTV, Triad, Truvision, Visualint, WattBox, Wirepath, and Wirepath ONE are also registered trademarks or trademarks of Snap One, LLC. Other names and brands may be claimed as the property of their respective owners. Snap One makes no claim that the information contained herein covers all installation scenarios and contingencies, or product use risks. Information within this specification subject to change without notice.

210913

200-00650-C