EtherWAN

Hardened Managed 24-port 10/100/1000BASE-T (8-port combo SFP) and 4-port 10G SFP+ Layer 3 Switch

User's Guide - GUI

FastFind Links

Disclaimer of Liability

The information contained in this document is subject to change without notice. EtherWAN is not liable for any errors or omissions contained herein or for resulting damage in connection with the information provided in this manual.

All other trademarks are property of their respective owners.

Warranty

For details on the EtherWAN warranty replacement policy, please visit our web site at:

www.etherwan.com

Products Supported by this Manual:

EG99000

Preface

Audience

This guide is designed for the person who installs, configures, deploys, and maintains the Ethernet network. This document assumes the reader has moderate hardware, computer, and Internet skills.

Document Revision Level

This section provides a history of the revision changes to this document.

Revision	Document Version	Date	Description
A	Version 1	12/11/2018	

Changes in this Revision

This is first version of this document.

Document Conventions

This guide uses the following conventions to draw your attention to certain information.

Safety and Warnings

This guide uses the following symbols to draw your attention to certain information.

Symbol	Meaning	Description
	Note	Notes emphasize or supplement important points of the main text.
	Tip	Tips provide helpful information, guidelines, or suggestions for performing tasks more effectively.
	Warning	Warnings indicate that failure to take a specified action could result in damage to the device, or could result in serious bodily injury.

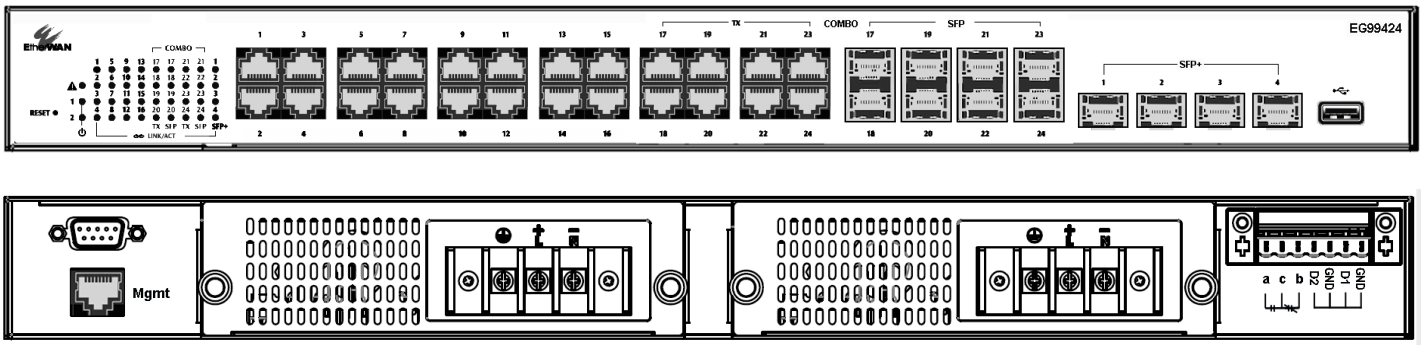
Contents

1 Introduction

EtherWAN's EG99000 is a gigabit Layer 3 switch designed for high bandwidth uplink or interconnection. With full wire speed switching capability, the EG99000 provides IP routing and switching across VLANs and subnetworks with no compromise in performance. The EG99000 supports comprehensive internetwork IP routings including static route, RIP v1 & v2, and OSPF v2 for IPv4. All these routing protocols can operate simultaneously with redistributions to each other and route control tools, including IP prefix-list and route-map.

In addition to supporting Layer 3 features, the EG99000 supports full sets of EtherWAN Layer 2 features such as port security, IGMP snooping, port-based VLAN, GARP protocols, link aggregation, access control lists and STP/RSTP/MSTP. Besides in-band management via web browser, Telnet, SSH and SNMP, the EG99000 supports out-band management via an RJ-45 port and an RS-232 console interface.

The EG99000 Series provides high reliability and nonstop operation in harsh environments where temperatures range from -40° to 75°C (-40° to 167°F), as well as in areas with high electromagnetic interference (EMI). The EG99000 is also equipped with sophisticated network and system failure recovery features including VRRP, and dual redundant power supplies to minimize the chance of network or system downtime. This makes it an ideal choice for both industrial and mission critical applications where sustained connectivity is crucial.The switch is shipped ready for use.



Unpacking and Installation

Unpacking

Unpack the items and confirm that no items are missing or damaged. Your package should include:

- One EG99000 switch
- One CD containing this user's guide
- One quick start guide

If any item is damaged or missing, notify your authorized EtherWAN representative. Keep the carton, including the original packing material, in case you need to store the product or return it.

Installing the Switch

Installation is bracket-mount. Use the enclosed screws and brackets to mount the switch in an open or enclosed rack.

- Select a power source within 6 feet (1.8 meters).
- Choose a dry area with ambient temperature between -40 and 75ºC (-40 and 167ºF).
- Be sure there is adequate airflow.

Connecting to the Data Ports

The EG99000 has the following ports:

- 24 x 10/100/1000 Mbps copper ports
- 8 x Gigabit combo ports (RJ-45 & SPF)
- 4 x 1/10G SPF+ slots
- 1 x RJ-45 Management port
- 1 x USB port

1 Gbps Combo/SFP Ports

Ports 17 – 24 are combo ports, and have two physical interfaces for each port. These ports can be used as either 10/100/1000BASE-TX on the left section or 1000BASE-FX on the right section. These ports operate in "either/or" fashion, i.e., connecting to fiber port 17 will render copper port 17 inoperable.

SPF+ Slots

SPF transceivers can be installed directly into right-side ports 17 – 24 and SPF+ ports 1 – 4. Ensure that the same type of transceiver is used at both ends of the link and that the correct type of fiber cable is used.

Connecting Power

Terminal Block

If your EG99000 comes with AC power cables, connect the cables into the power modules at the back of the switch. If your switch comes with a DC or AC terminal block (no cable), then connect the switch to a suitable power supply using 12 to 24 AWG wire. Redundant power supply is supported. However, only one power input is required to operate the switch. Input voltage is 48 VDC or 100 – 240 VAC, depending on model.

Relay Output Alarm

The switch provides one dry contact for signaling of a user-defined power or port failure. The alarm relay default is “open” and forms a closed circuit when the event occurs. The relay output can be connected to an alarm signaling device, and supports both normal open and normal closed. Relay output current is 30VDC / 1A.

Connecting to the Management Interface

Serial - Connect to the switch console by connecting the DB-9 cable to the console port of the switch and to the serial port of the computer running a terminal emulation application (such as HyperTerminal or Putty).

Configuration settings of the terminal-emulation program: Baud rate: 115,200bps, Data bits: 8, Parity: none, Stop bit: 1, Flow control: none.

TCP/IP - Connect to the switch via the RJ-45 Management port located on the rear panel below the serial port, or via one of the Ethernet ports on the front panel. Use a terminal emulation program and connect to IP address **192.168.2.10**. You can also connect to the switch through any of the RJ-45 ports on the front panel, IP address is **192.168.1.10** (VLAN1.1).

The default login name is “**root**,” **no password**.

Alternate (Backup) Firmware

Under certain circumstances, such as when there is a loss of power during an upgrade, the firmware build on the switch can become unstable. There are two firmware images stored on the switch: Active and Alternate. If the Active firmware image becomes unstable, the switch will automatically boot from the Alternate image on the next boot.

2 Web Management Interface

About the Web-based graphical user interface (GUI)

The web interface allows for remote monitoring, configuration, and control of the switch through any standard web browser. All switch features that can be configured through the Command Line Interface can also be configured through the GUI.

Note: Supported browsers are Chrome, Internet Explorer version 11, and Microsoft Edge

Default IP Address

The switch's default IP address is 192.168.1.10. The management computer must be set up so that it is on the same network as the switch. For example, the IP address of the management computer can be set to 192.168.1.100 with a subnet mask of 255.255.255.0. DHCP is disabled by default.

Login Process and Default Credentials

Once a compatible IP address has been assigned to the management computer, the user is ready to log in to the switch. To log in, type the URL http://192.168.1.10/ into the address field of the browser and hit return. (See figure below)

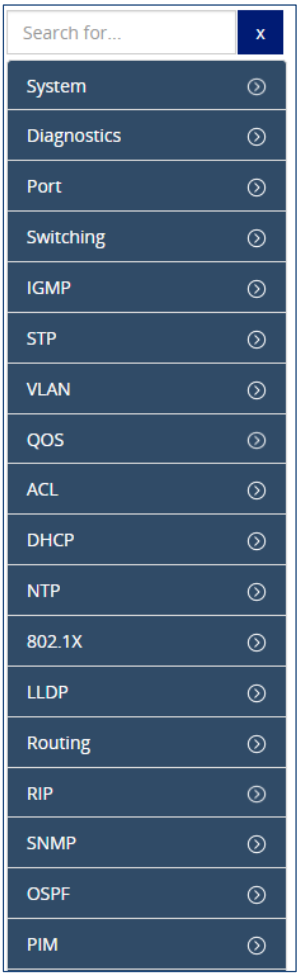
- The Default Login is **root** (case sensitive)
- There is no password by default
- Enter the login name and click the Login button

Login Screen

Navigating the GUI

At the top of every page of the web interface is a panel containing a graphic that shows status of power & ports on the switch, and an alarm indicator.

On the left of the page is the navigation panel. Each section can be expanded and collapsed to view or hide the page headings within. At the top of the navigation panel is a search box, which can be used to quickly find a specific page in the GUI. Note that search box works best with specific terms like “MSTP.” Generic search terms like “Setting” will yield many results, and it may be difficult to quickly identify the specific setting page needed.



Icons

The GUI uses a few simple icons to for viewing and editing switch configuration data.

 Refresh the panel

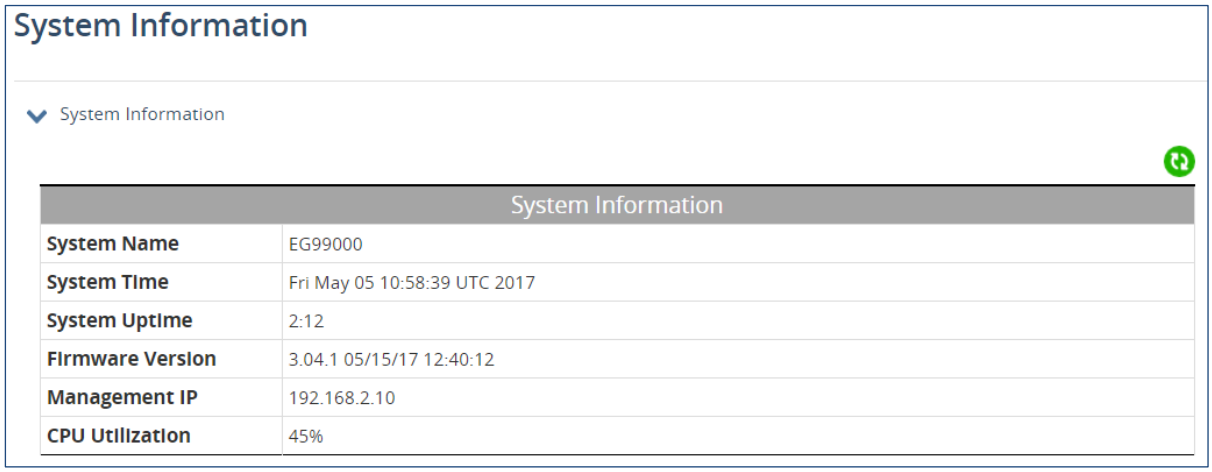
 Edit data in panel

 Add a new entry to the panel (Example: Add a new static route)

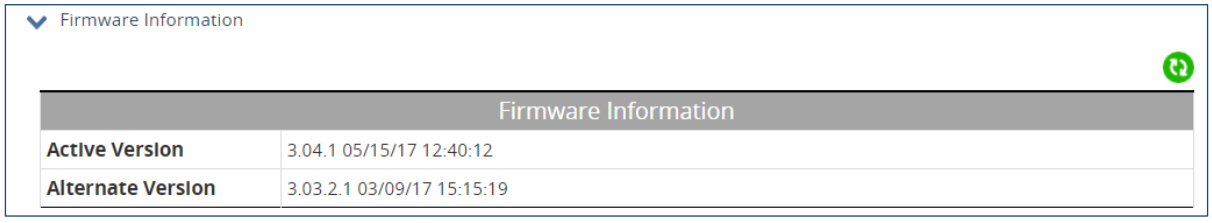
3 System Menu

System Information

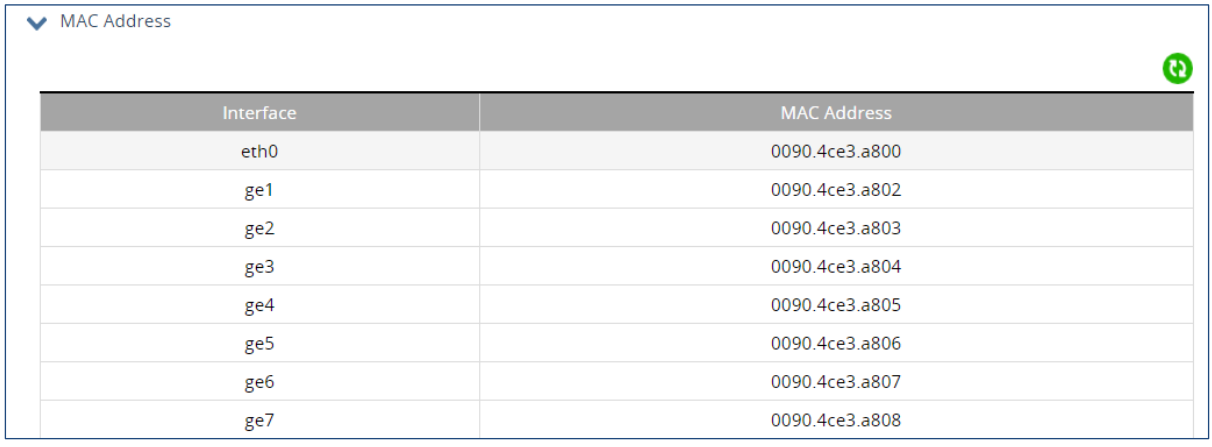
When you log into the switch GUI, you will be taken to the system information page. This is a read-only page with three panels. The first panel shows basic system info:



The second panel shows the active and alternate firmware versions.

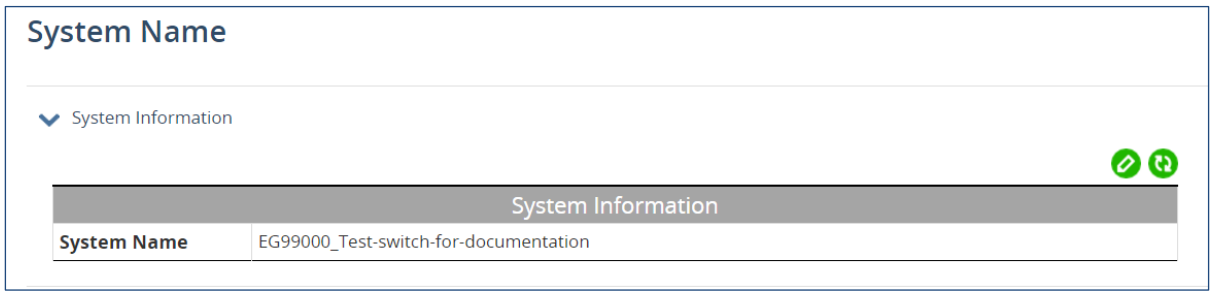


The third panel shows the MAC address of each port on the switch.



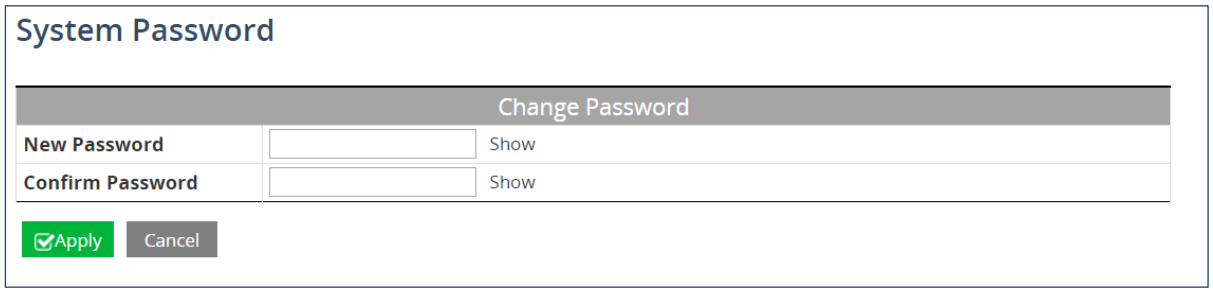
System Name

To change the system name, click the edit icon and enter a name in the field shown. The name may not contain spaces. Maximum length is 64 characters.



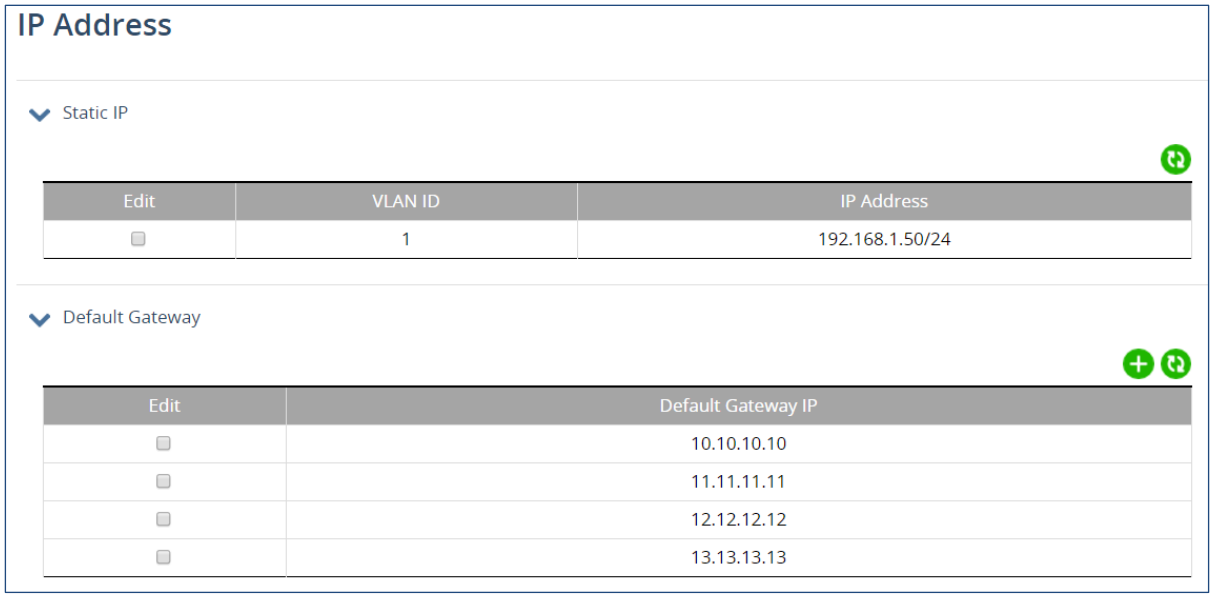
System Password

By default, there is no password assigned to the switch. To set a password, enter it into both fields and click “Apply.”



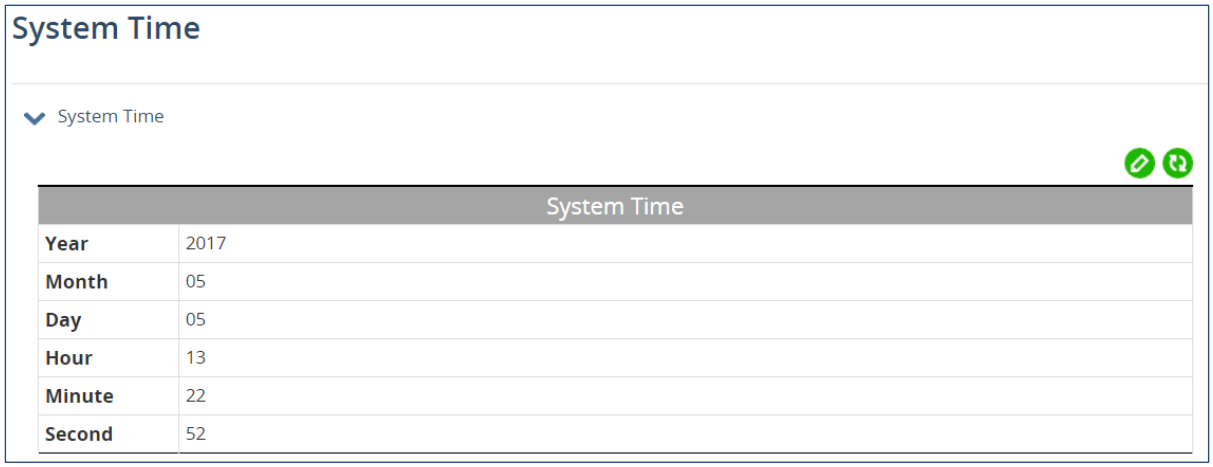
IP Address

The two panels on this page allow for the changing of the IP address of VLAN 1, and for the creation of default gateways.



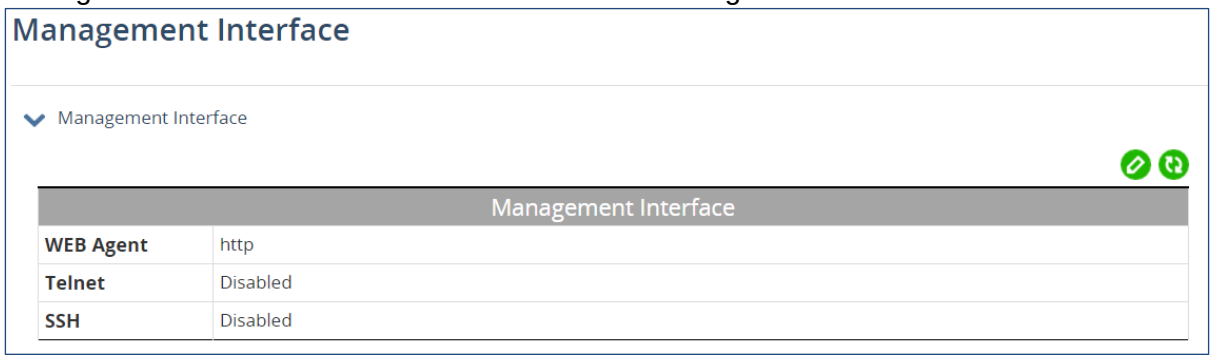
System Time

This page is for manual setting of the system time. Click the edit icon, and enter the time and date data in the corresponding fields. Click “Apply” when finished. To configure a network time server, refer to chapter on NTP.



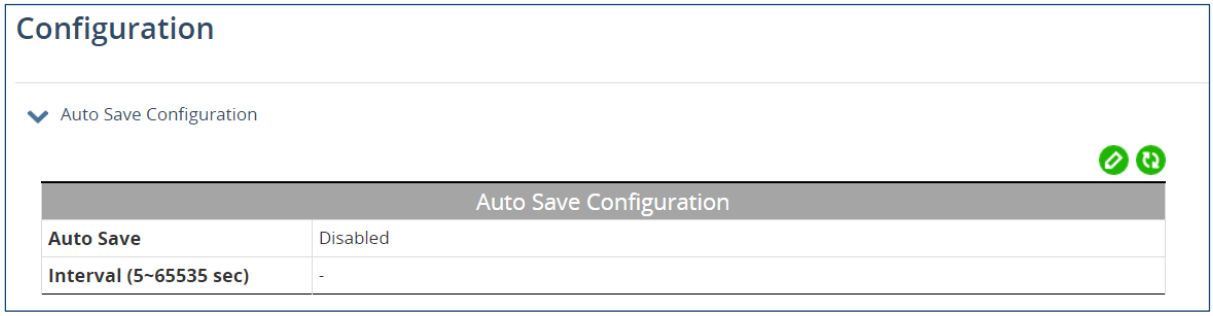
Management Interface

Enable / disable access to switch management through http, Telnet, and SSH on this page. Note that if you disable http you will lose access to the GUI, and need to use another management method to access the switch to save changes.



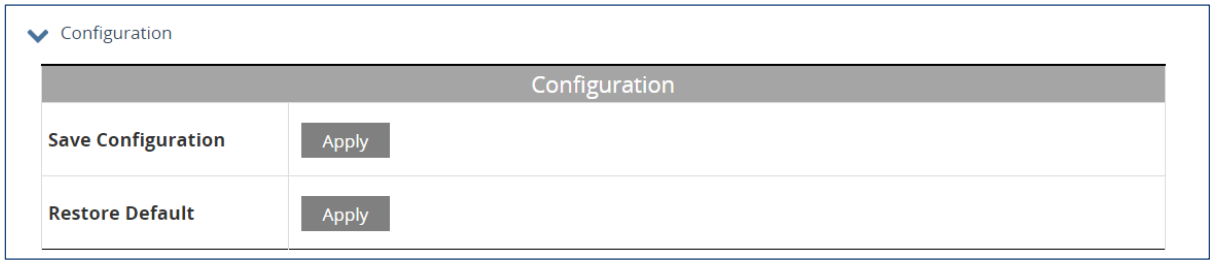
Configuration

This page is comprised of three panels. The first is for setting auto-save interval of the switch configuration. Auto-save is disabled by default.

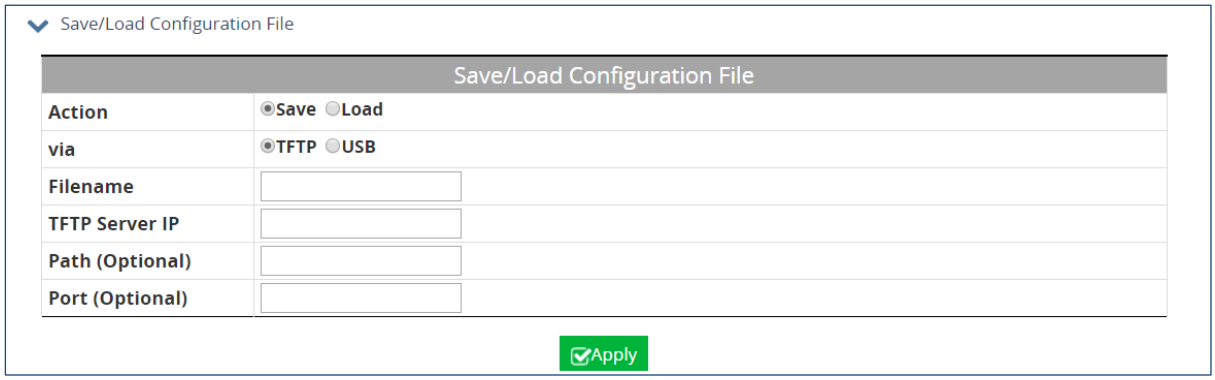


Saving Switch Configuration

The second panel is for saving the current switch configuration, and resetting the switch configuration to factory default. A confirmation message will display if the second option is chosen.

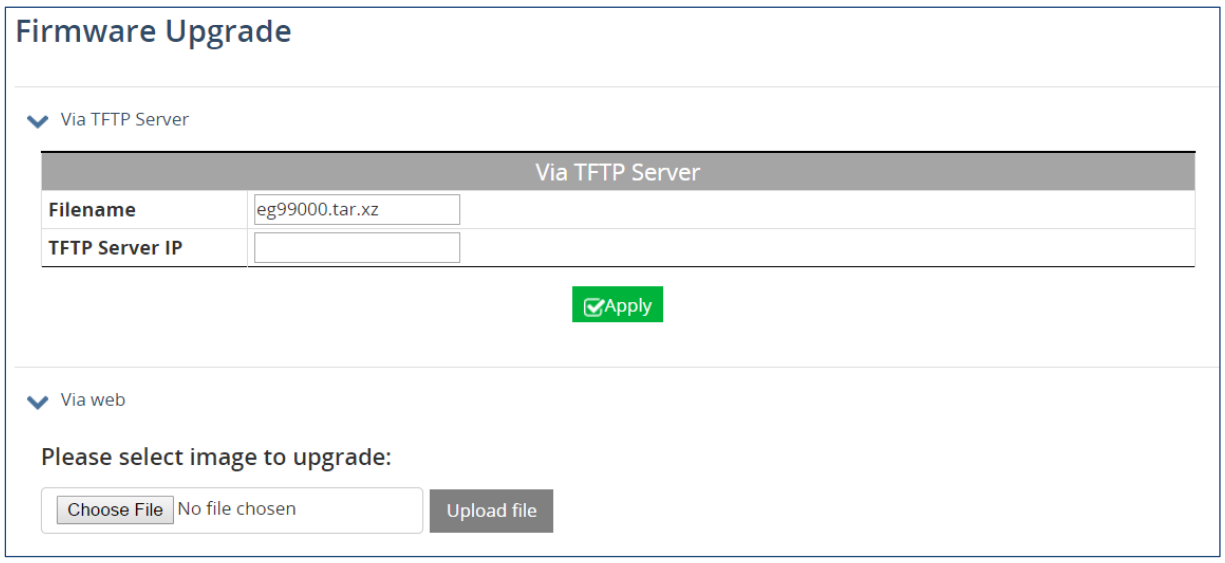


Load a switch configuration from, or save a configuration to, a TFTP server or USB flash drive using the third panel. Path and port fields are optional.



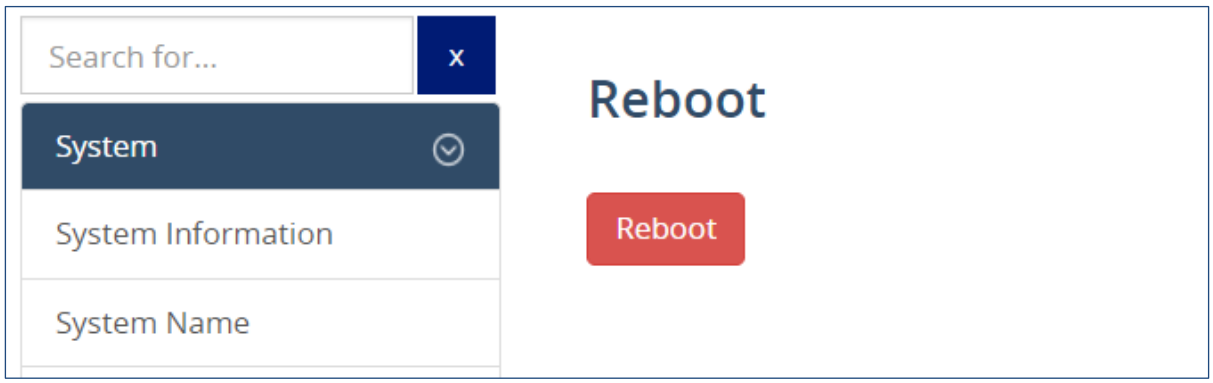
Firmware Upgrade

Firmware can be upgraded from either a TFTP server or from any drive that is accessible to the web browser. The firmware file for the switch should be in a .TGZ or .IMG format.



Reboot

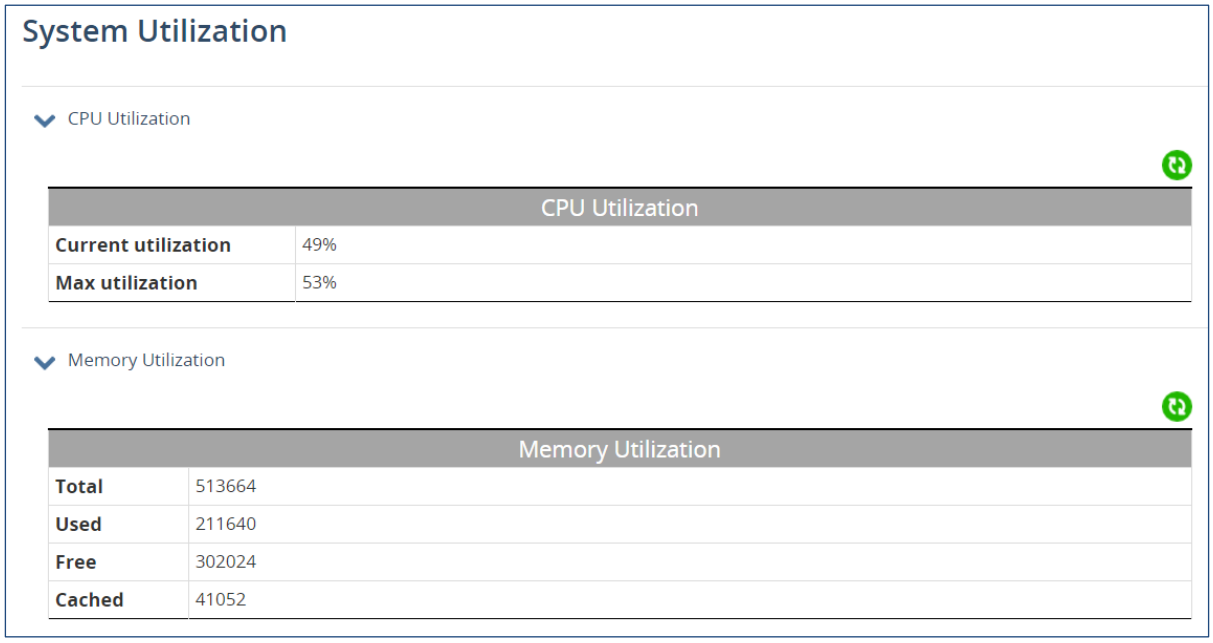
Reboot the switch.



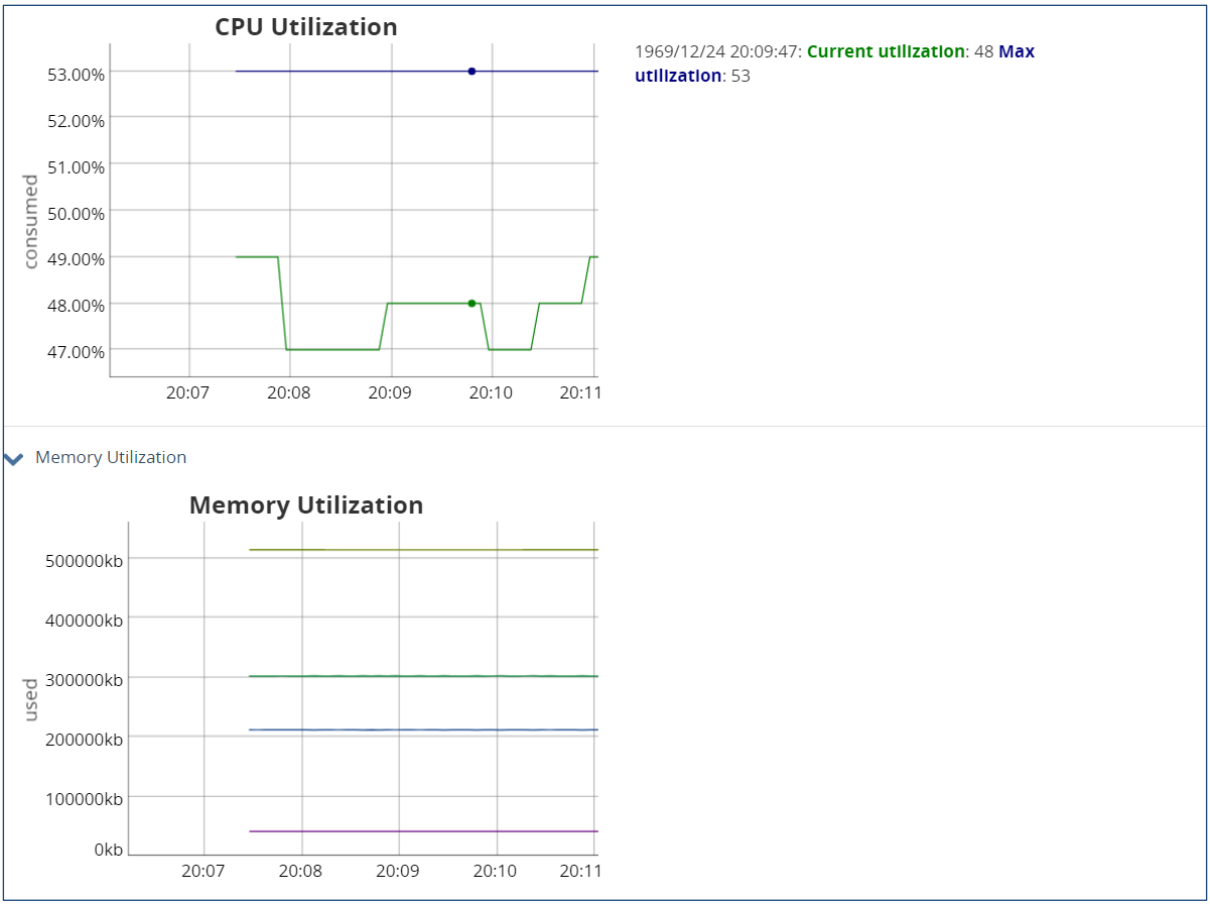
4 Diagnostics Commands

System Utilization

The System Utilization page is a read-only page for viewing the current CPU and memory utilization levels. The first panel shows utilizations as a percentage, and the second panel shows the total memory, amount used, amount free, and amount cached.

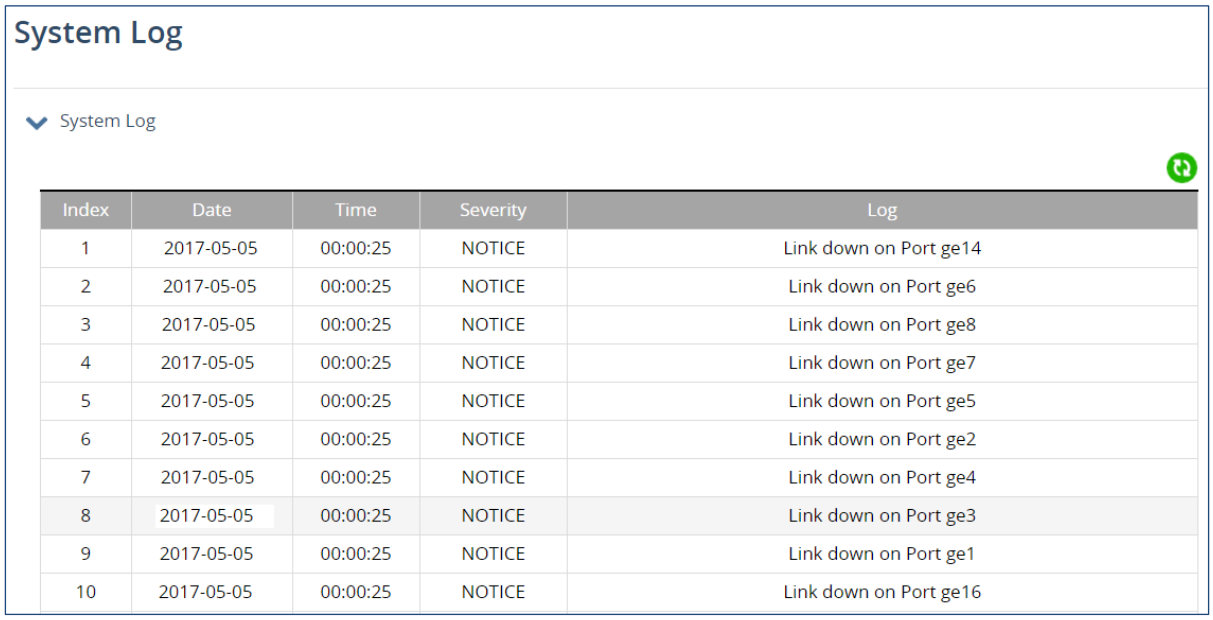


Below these are real-time graphs of CPU and memory usage. Mouse over any point on these graphs to see detailed information.


CPU Utilization
53.00%
52.00%
51.00%
50.00%
49.00%
48.00%
47.00%
consumed
20:07
20:08
20:09
20:10
20:11
1969/12/24 20:09:47: Current utilization: 48 Max utilization: 53
Memory Utilization
Memory Utilization
500000kb
400000kb
300000kb
200000kb
100000kb
0kb
used
20:07
20:08
20:09
20:10
20:11

System Log

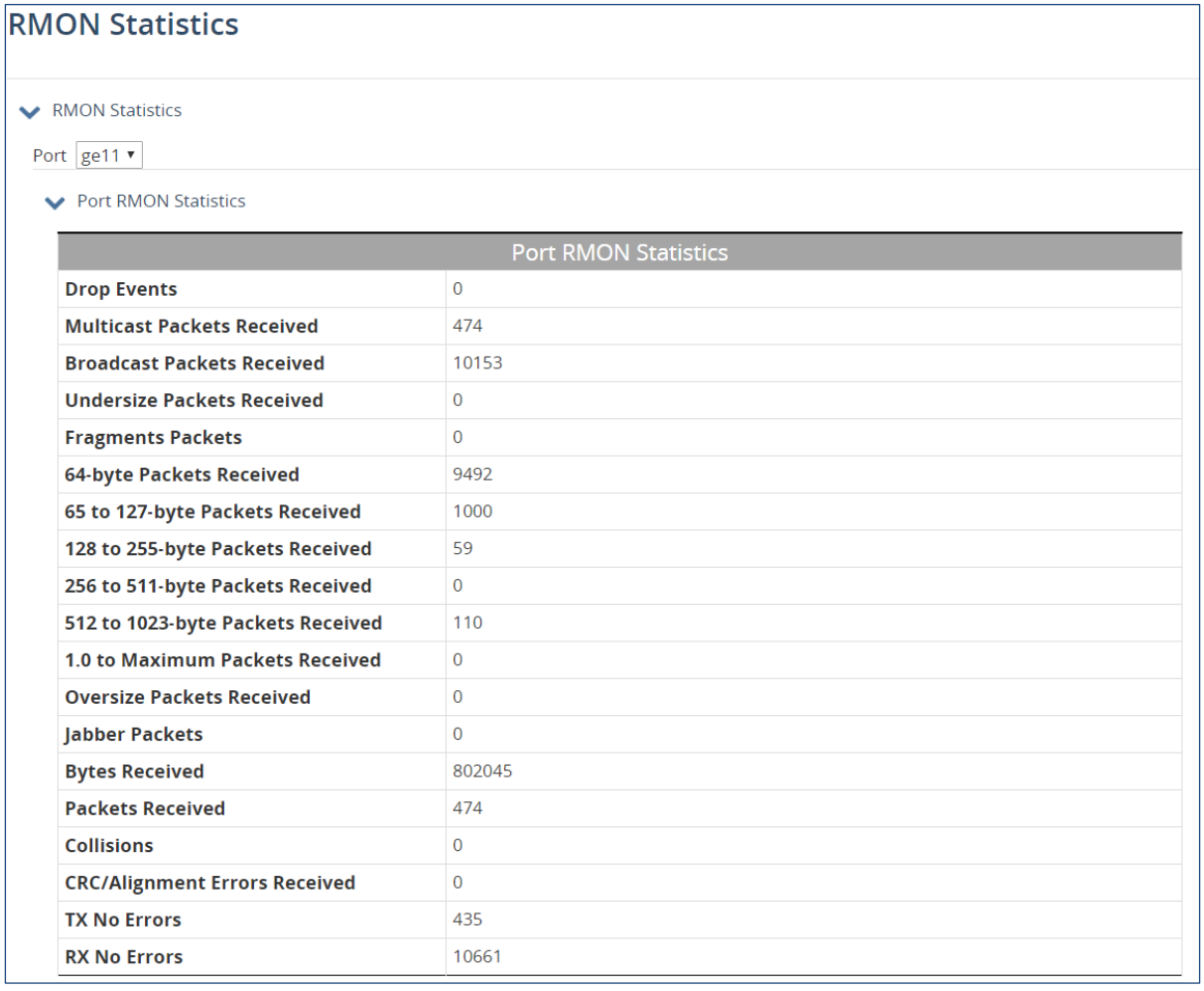
The System Log shows the data and time of system events, such as port links going up or down.



Index	Date	Time	Severity	Log
1	2017-05-05	00:00:25	NOTICE	Link down on Port ge14
2	2017-05-05	00:00:25	NOTICE	Link down on Port ge6
3	2017-05-05	00:00:25	NOTICE	Link down on Port ge8
4	2017-05-05	00:00:25	NOTICE	Link down on Port ge7
5	2017-05-05	00:00:25	NOTICE	Link down on Port ge5
6	2017-05-05	00:00:25	NOTICE	Link down on Port ge2
7	2017-05-05	00:00:25	NOTICE	Link down on Port ge4
8	2017-05-05	00:00:25	NOTICE	Link down on Port ge3
9	2017-05-05	00:00:25	NOTICE	Link down on Port ge1
10	2017-05-05	00:00:25	NOTICE	Link down on Port ge16

RMON Statistics

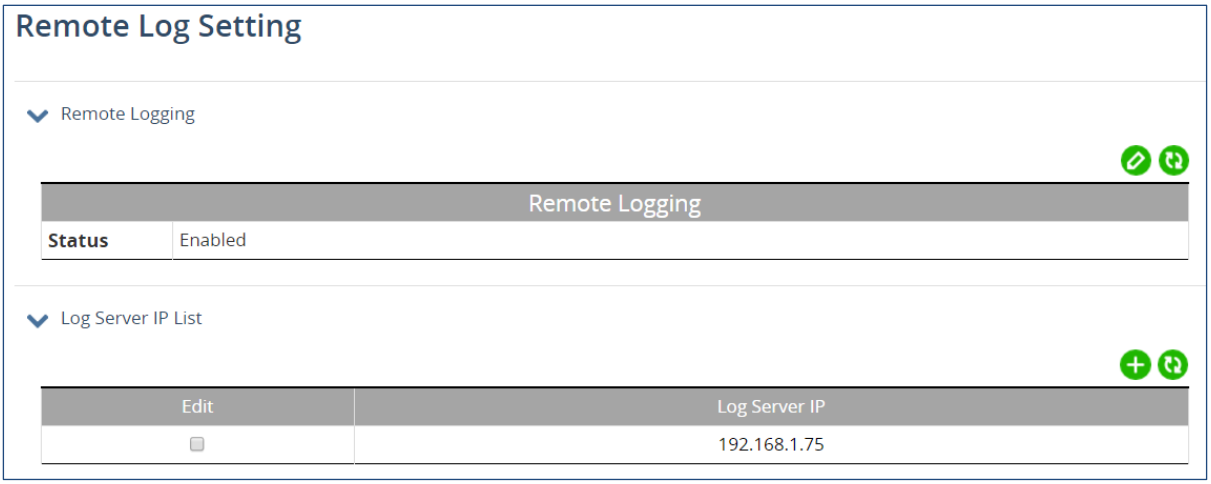
RMON Statistics gives a detailed listing of the types and quantity of packets that a particular port has seen since the last reboot of the switch.



Port RMON Statistics	
Drop Events	0
Multicast Packets Received	474
Broadcast Packets Received	10153
Undersize Packets Received	0
Fragments Packets	0
64-byte Packets Received	9492
65 to 127-byte Packets Received	1000
128 to 255-byte Packets Received	59
256 to 511-byte Packets Received	0
512 to 1023-byte Packets Received	110
1.0 to Maximum Packets Received	0
Oversize Packets Received	0
Jabber Packets	0
Bytes Received	802045
Packets Received	474
Collisions	0
CRC/Alignment Errors Received	0
TX No Errors	435
RX No Errors	10661

Remote Logging

Remote Logging to a Syslog server allows administrators to log important system and debugging information. The Remote Logging configuration page allows reporting to a Syslog server to be enabled or disabled as well as management of a list of Syslog servers to report to. Enable or disable remote logging in the top panel, and use the bottom panel to add, edit, or delete log server IP addresses.



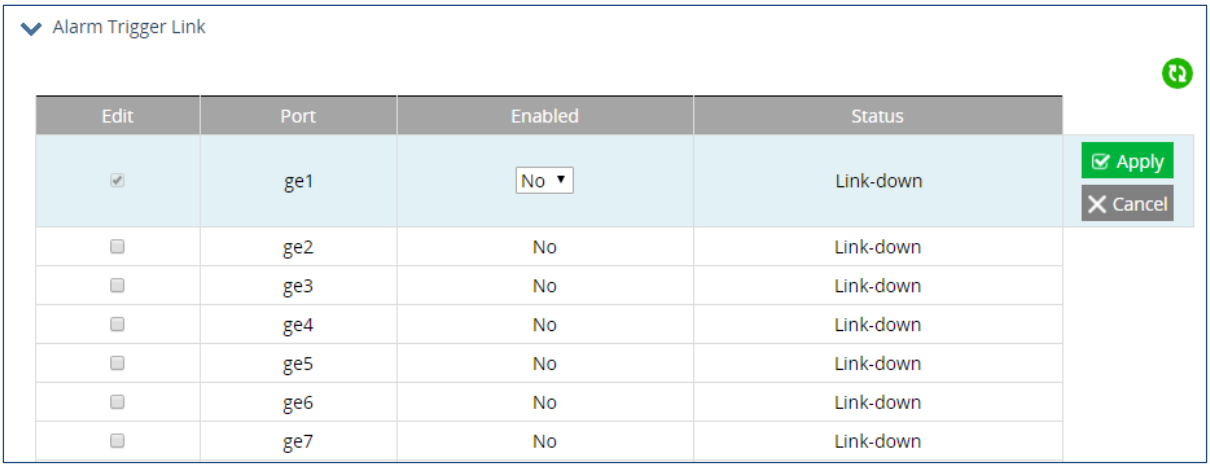
Alarm Setting

Alarms can be set for a variety of general switch conditions including link down, redundant power failure, and overheating. When equipped with a DDI compatible SFP module, major and minor alarms can also be set for SFP temperature, voltage, power, and TX bias. By default, alarms are sent to the system log, and displayed on the top panel of the web interface. Alarms can also be sent as SNMP traps to an SNMP server. External alarm devices can be configured using the relay output alarm.

NOTE: To configure specific threshold values for DDI SFP alarms, you must use the command line interface (CLI).

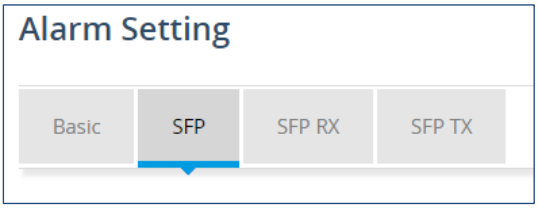
The Alarm Setting page is divided into four sections, accessible by tabs at the top of the page.

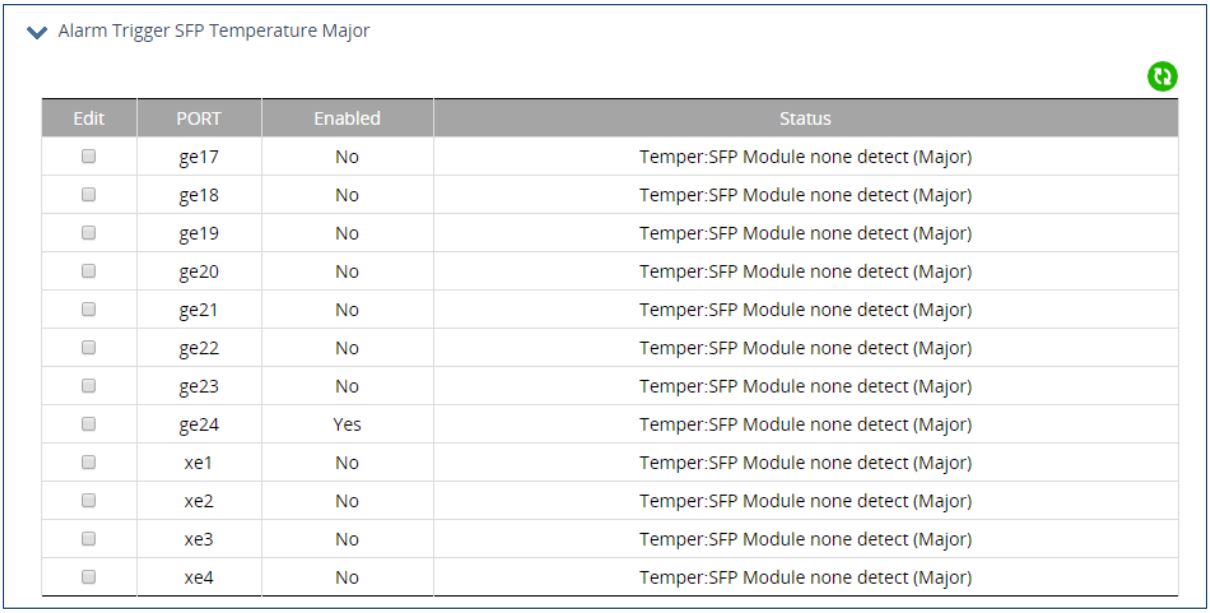
In the first section, **Basic** alarms can be set for failure on any port, either power input (if dual power inputs are used), and system temperature.

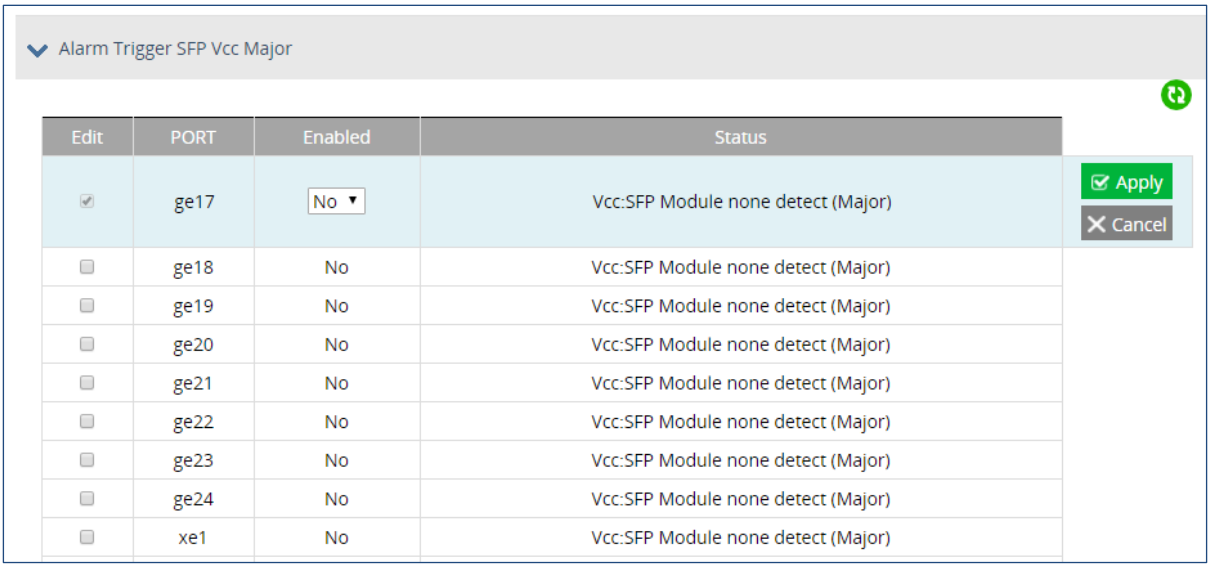


To set a link-down alarm check the box next to a port, and click "Apply"

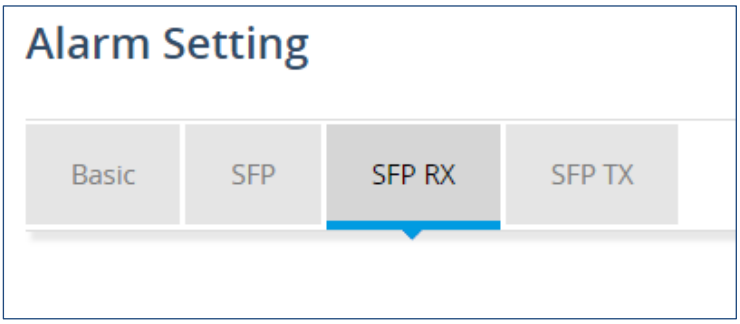
Panels on the second tab panels allow for setting of major and minor alarms for SFP temperature and voltage.

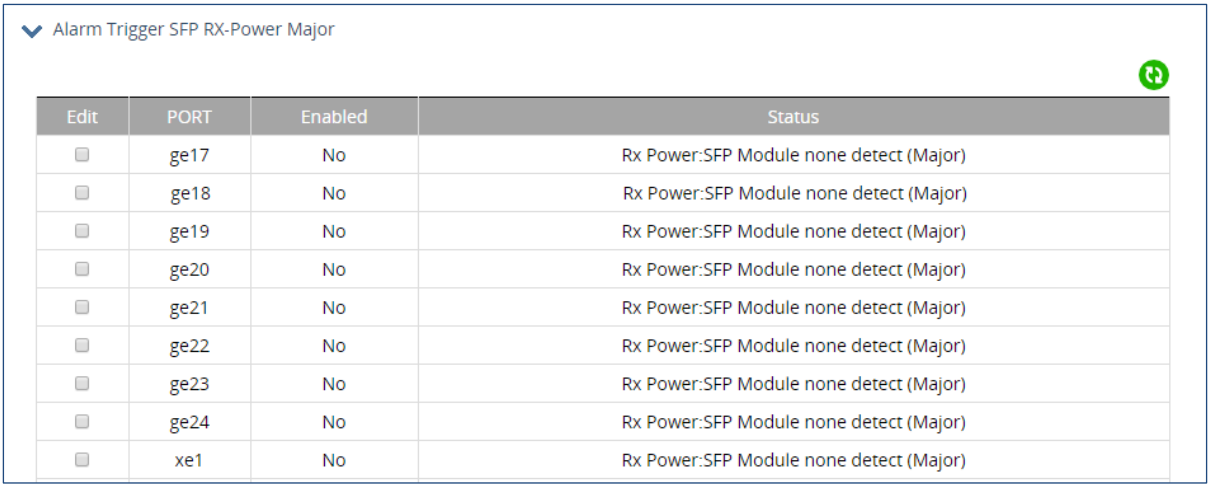




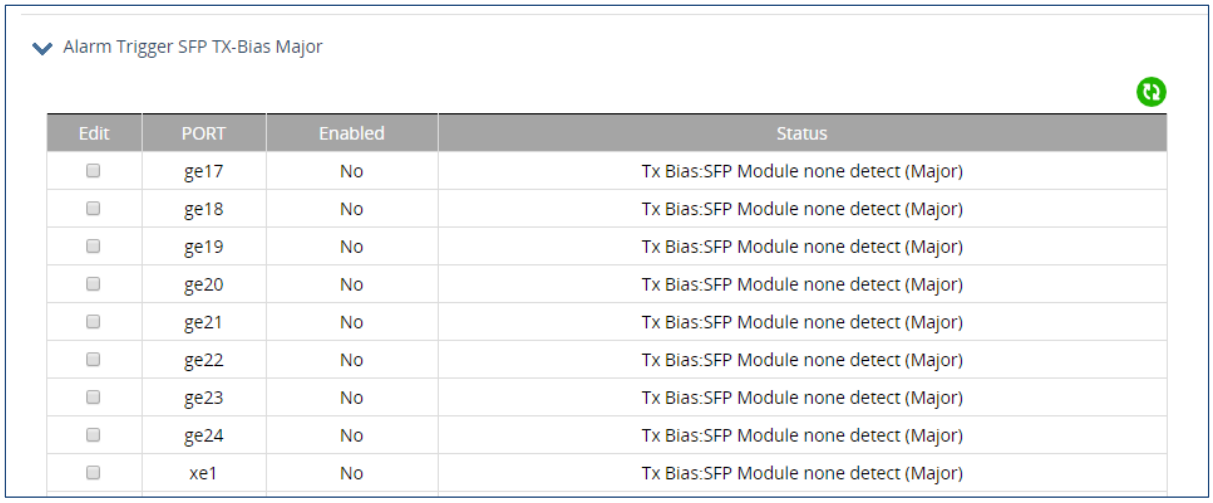


On the third tab are panels to set major and minor alarms for RX power. This is the optical power ratio received in decibels (dB).





The fourth tab contains panels for setting major and minor alarms for TX Bias and TX Power. TX Bias is the transmit bias power signal, in milliamperes (mA). TX Power is the transmit power signal, in decibels (dB).

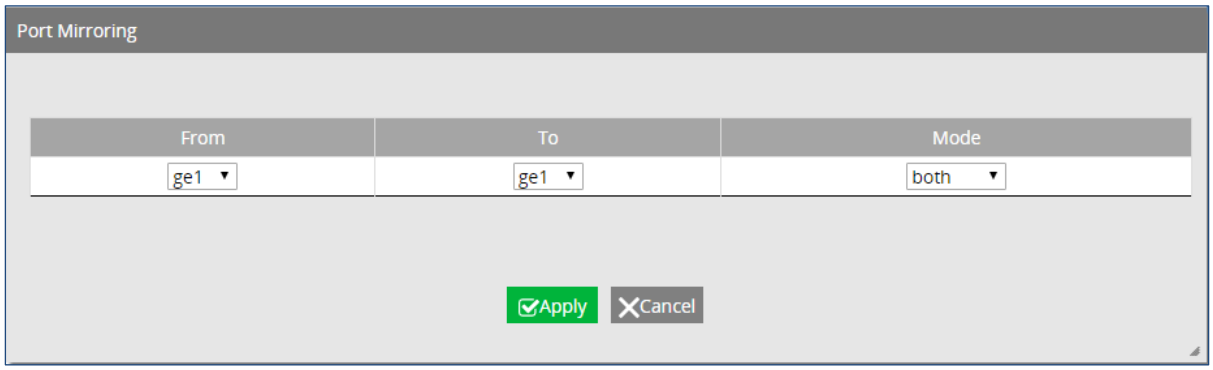


Edit	PORT	Enabled	Status
	ge17	No	Tx Bias:SFP Module none detect (Major)
	ge18	No	Tx Bias:SFP Module none detect (Major)
	ge19	No	Tx Bias:SFP Module none detect (Major)
	ge20	No	Tx Bias:SFP Module none detect (Major)
	ge21	No	Tx Bias:SFP Module none detect (Major)
	ge22	No	Tx Bias:SFP Module none detect (Major)
	ge23	No	Tx Bias:SFP Module none detect (Major)
	ge24	No	Tx Bias:SFP Module none detect (Major)
	xe1	No	Tx Bias:SFP Module none detect (Major)

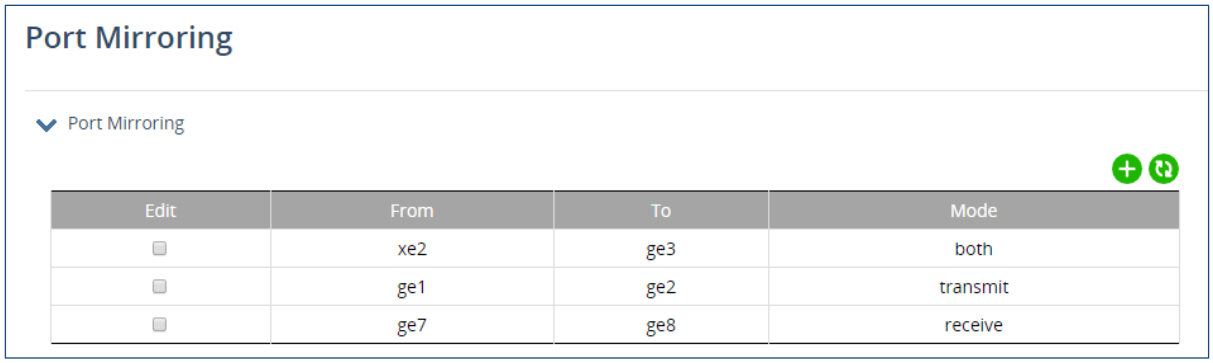
Port Mirroring

To configure port mirroring, click the add icon, and enter the **From** and **To** ports. Select the desired mode: transmit (mirror transmits traffic), receive (mirror receives traffic), or both (traffic is mirrored in both directions).

Port mirroring can only be configured on interfaces of the same type, e.g., only a switchport interface can mirror a switchport interface. Issuing a switchport command on a port where mirroring is enabled will remove port mirroring on that interface.



Existing mirrors can be viewed and deleted from the initial page.


Port Mirroring
Port Mirroring
Edit
From
To
Mode
xe2
ge3
both
ge1
ge2
transmit
ge7
ge8
receive

5 Port Commands

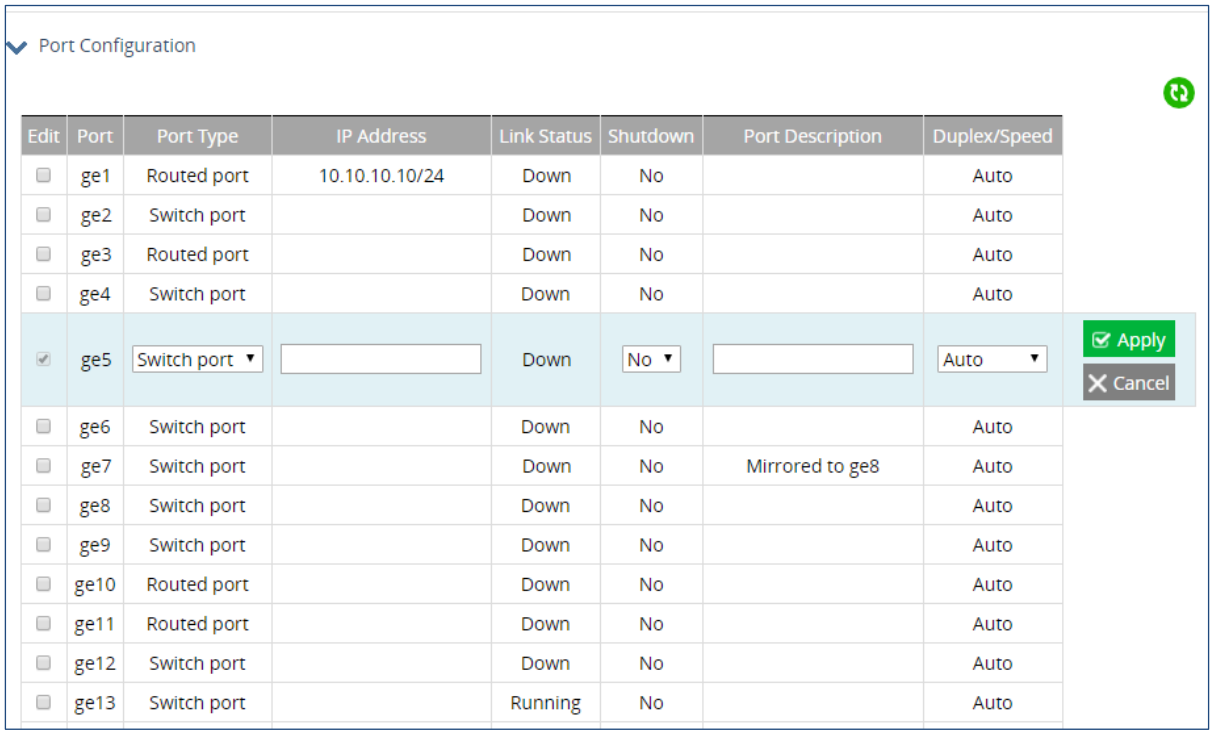
Port Configuration

Port configuration contains features as flow control, port speed, and duplex settings. These settings can be very useful when the switch is connected to a latency-critical device such as a VOIP phone, IP camera, or video multiplexor. The ability to alter port settings can make the difference between a poorly responding device and one that functions without loss of data or clarity.

.The **Configuration** page shows (see figure below):

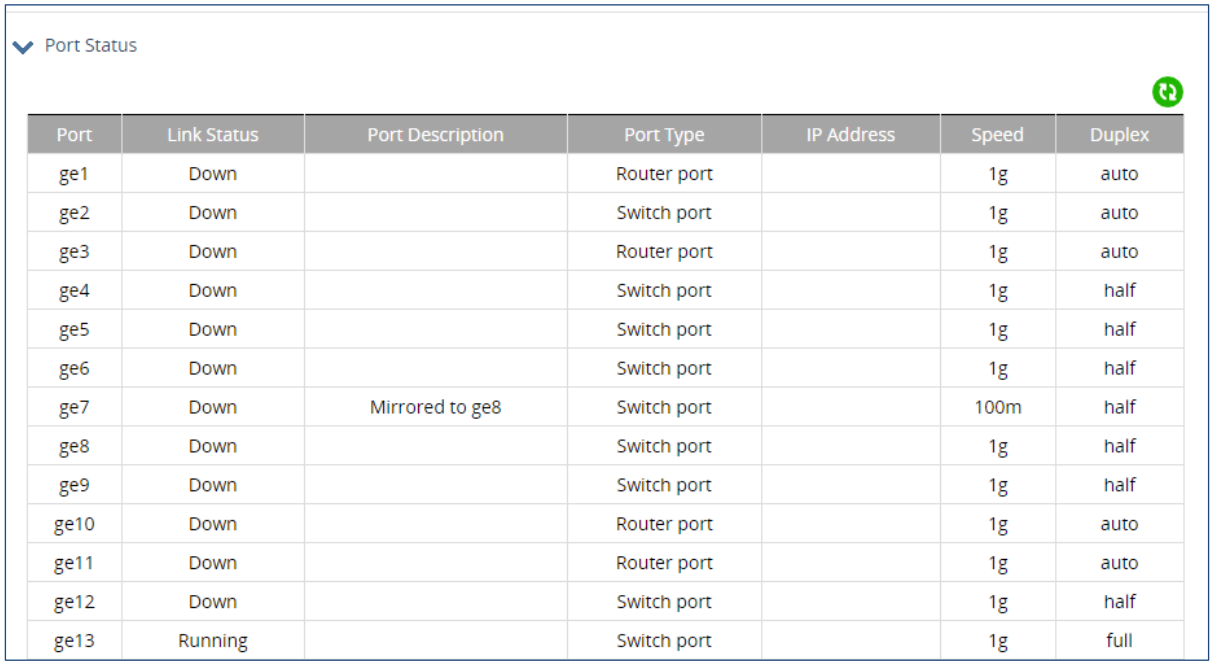
- **Port Type**– Routed port or Switch port
- **IP address** – For routed ports only, aaa.bbb.ccc.ddd/mm format
- **Link Status** – Operational State of the Port's Link (Read-Only)
- **Shutdown** – Shutdown state
- **Port Description** – User-supplied description, 80 characters maximum
- **Duplex / Speed** – Options are Auto, 100M/FD, 100M/HD, 10M/FD, and 10M/HD.

Click the check box to modify the settings for a port, and click "Apply" when finished.



Port Status

This is a read-only page that lists the settings described in the previous section.

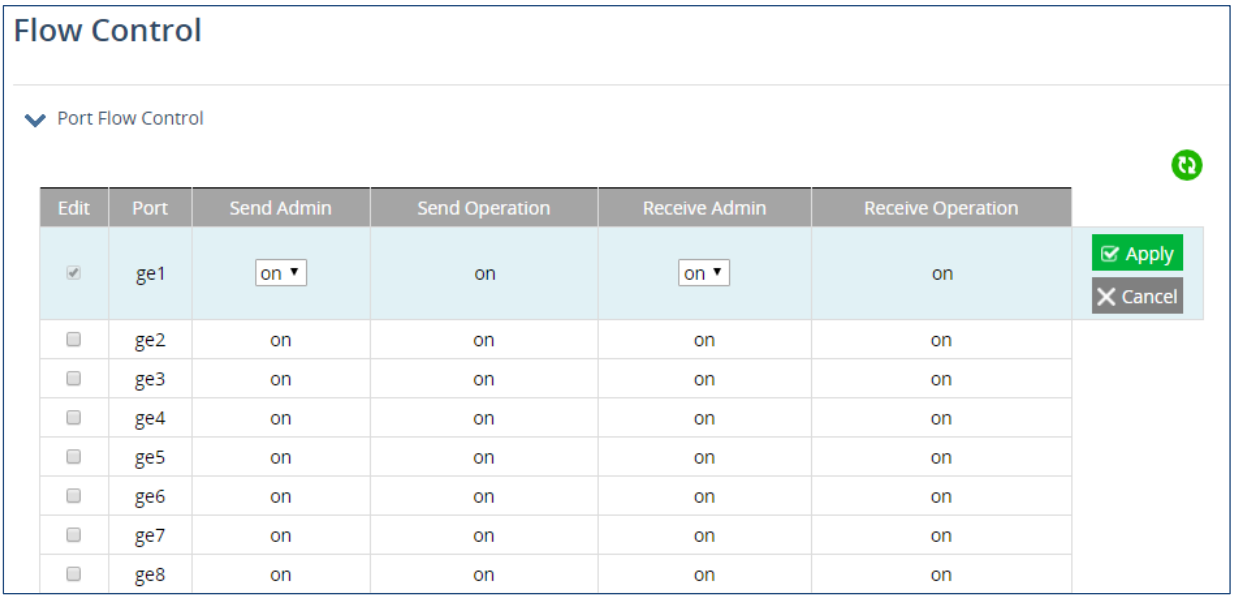


Port	Link Status	Port Description	Port Type	IP Address	Speed	Duplex
ge1	Down		Router port		1g	auto
ge2	Down		Switch port		1g	auto
ge3	Down		Router port		1g	auto
ge4	Down		Switch port		1g	half
ge5	Down		Switch port		1g	half
ge6	Down		Switch port		1g	half
ge7	Down	Mirrored to ge8	Switch port		100m	half
ge8	Down		Switch port		1g	half
ge9	Down		Switch port		1g	half
ge10	Down		Router port		1g	auto
ge11	Down		Router port		1g	auto
ge12	Down		Switch port		1g	half
ge13	Running		Switch port		1g	full

Flow Control

Flow control allows switches of different speeds to communicate. When enabled, the lower speed switch can request that the higher speed switch refrains from sending packets. Transmissions are temporarily halted to prevent overflows. Flow control in enabled by default on all ports.

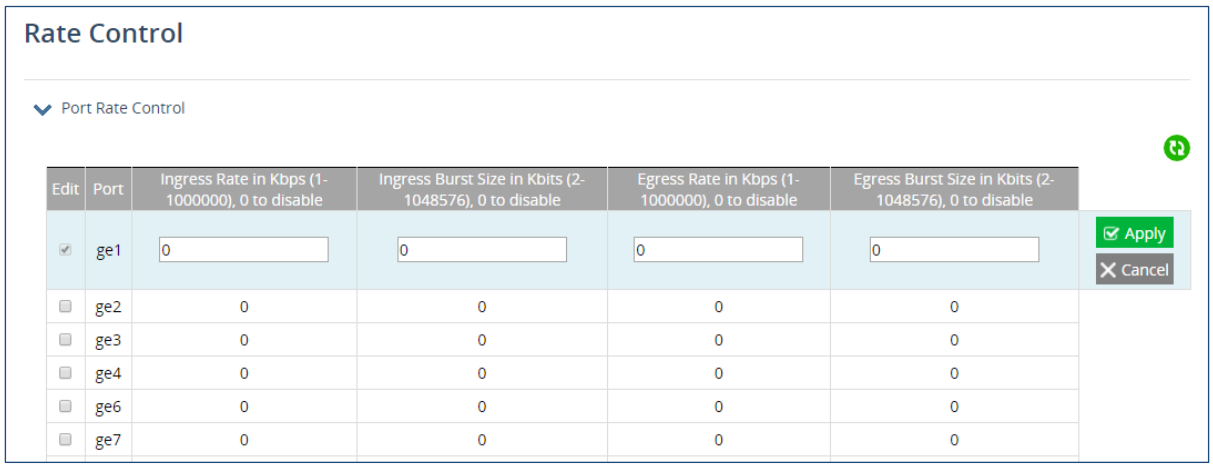
When enabling or editing flow control on a port, click the check box next to the port, then set the **Send Admin** and **Receive Admin** fields to **on** or **off**, enabling or disabling the port's ability to send and receive flow control administrative requests. Then click "Apply."



Rate Control

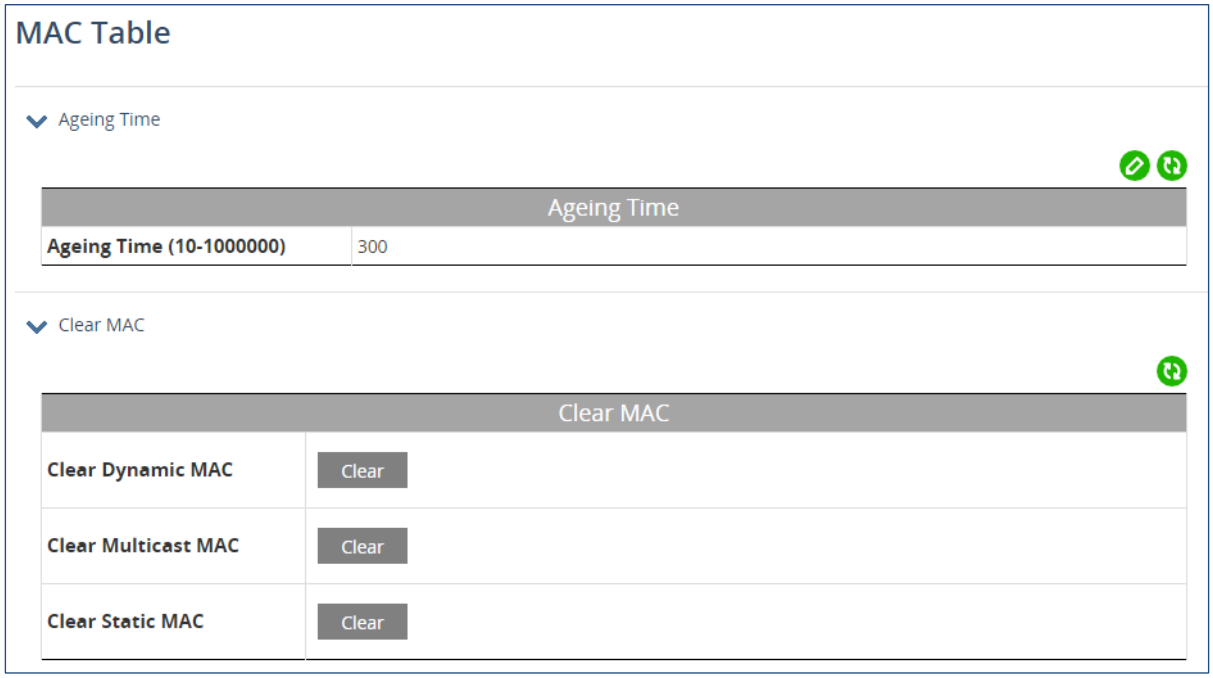
Rate control forces a port to drop packets when an ingress / egress rate limit has been exceeded. Click on the check box next to a port, and enter the limits for **Ingress Rate in Kbps**, **Ingress Burst Size in Kbits**, **Egress Rate in Kbps**, and **Egress Burst Size in Kbits**. Then click “Apply.”

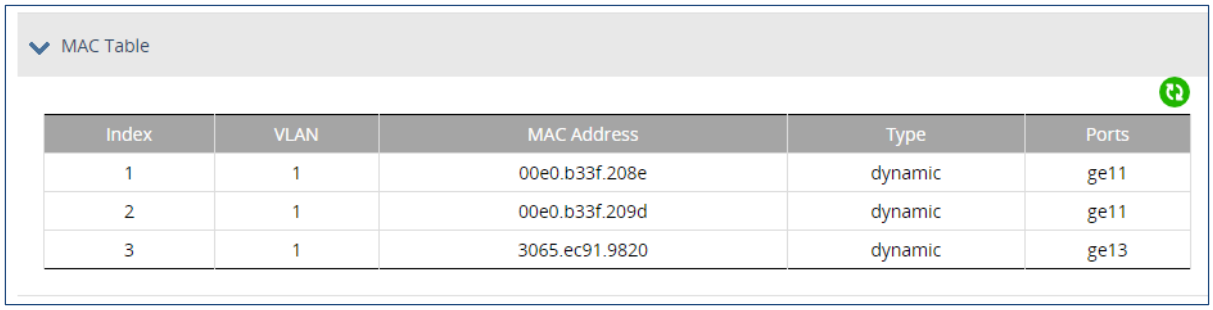
To disable Rate Control on a port, set all values to zero.



MAC Table

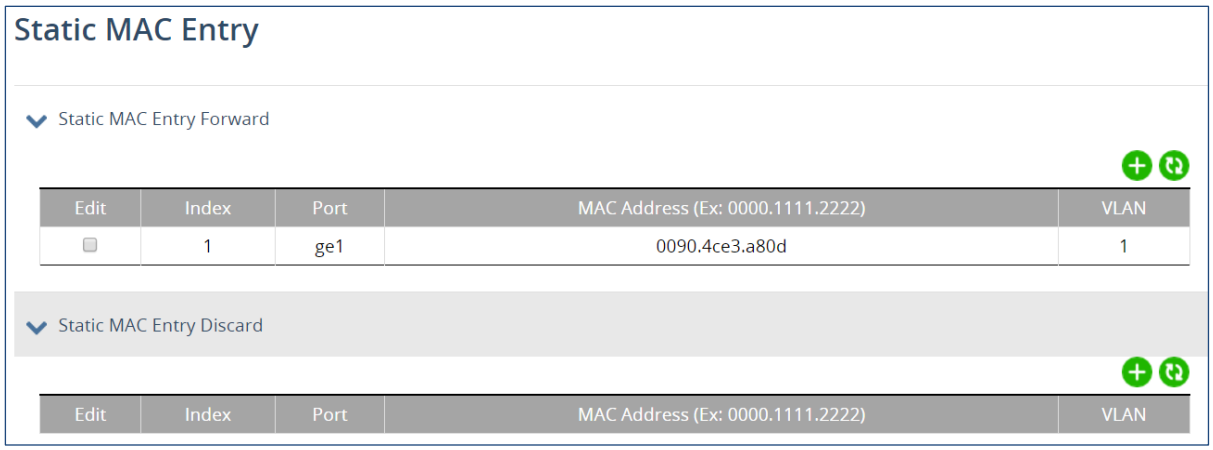
The MAC Table page contains a panel for setting the Ageing Time, one for clearing Dynamic, Mulitcast, and Static MAC addresses, and a read-only panel for viewing the current MAC Table. Change the Ageing time (the time that a networked device's MAC address will live in the switch's memory before being removed) by clicking the edit icon, and entering the desired Ageing Time in seconds. Then click "Apply."





Static MAC Entry

Static MAC Entry Forward allows you to specify a MAC address on a particular port and VLAN rather than adjusting the ageing time for the entire switch. Alternatively, you can prevent a MAC address from ever being registered with a switch by using **Static MAC Entry Discard**.

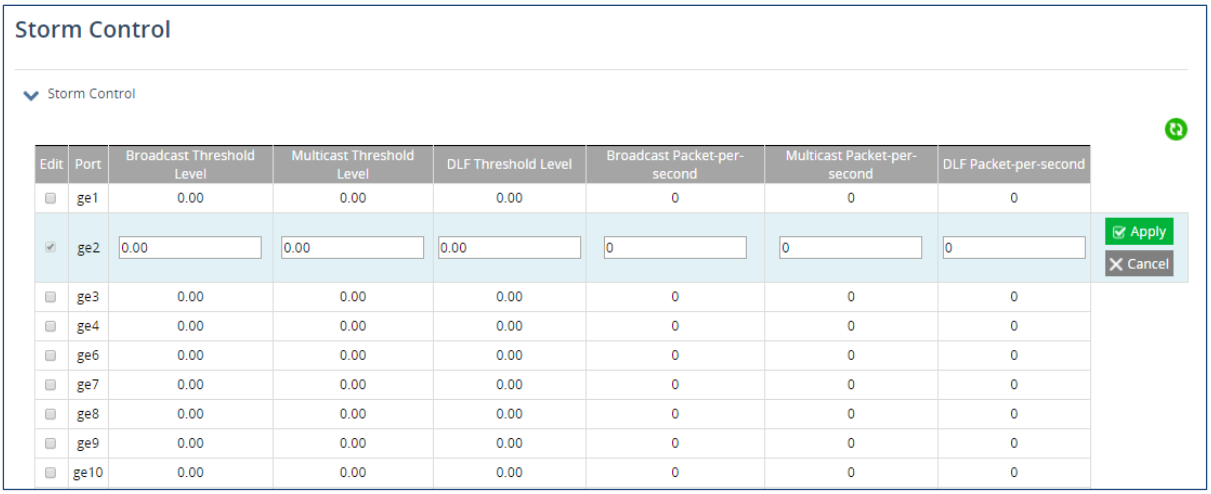


Storm Control

Set the rising threshold level for broadcast, multicast, or destination lookup failure traffic. The storm control action occurs when traffic utilization reaches the set level. Storm control blocks the forwarding of unnecessary flooded traffic.

To enable Storm Control on a port, select it by clicking the check box on the left. Then enter values for:

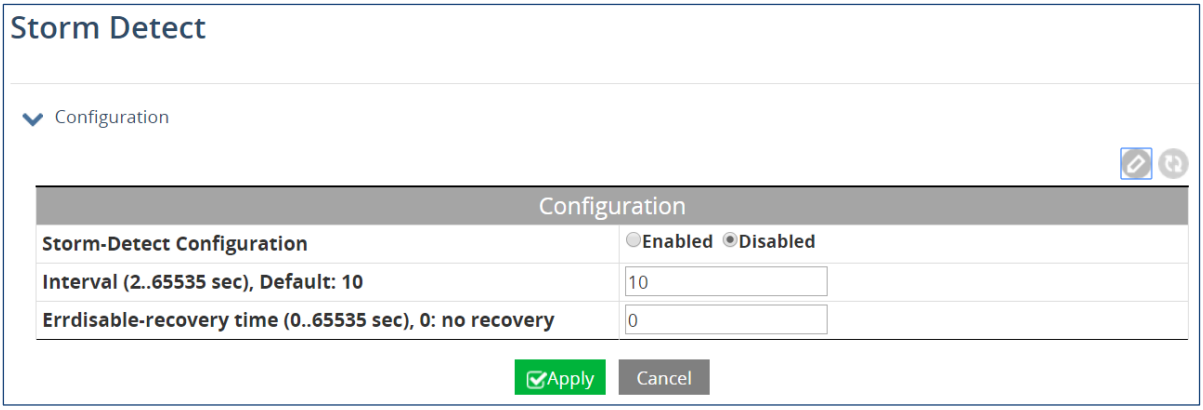
Broadcast Threshold Level: Broadcast rate limiting, based on percentage of the maximum speed (in packets per second) of the interface
Multicast Threshold Level: Multicast rate limiting, based on percentage of the maximum speed (in packets per second) of the interface
DLF Threshold Level: Destination lookup failure, based on percentage of the maximum speed (pps) of the interface
Broadcast Packet-per-second: Broadcast rate limiting, based on total number of packets
Multicast Packet-per-second: Multicast rate limiting, based on total number of packets
DLF Packet-per-second: Destination lookup failure, based on total number of packets



Storm Detect

Storm Detect can disable a port that is receiving excessive Broadcast and/or Multicast packets. The switch can be configured to take action based on percentage of bandwidth utilization or number of packets per second.

To enable Storm Detect globally, click the edit icon and then **Enable**. Then set the Storm Detect **interval** to a value between 2 and 65535 seconds. Set the **errdisable-recovery time** to value between 0 and 65535 seconds.

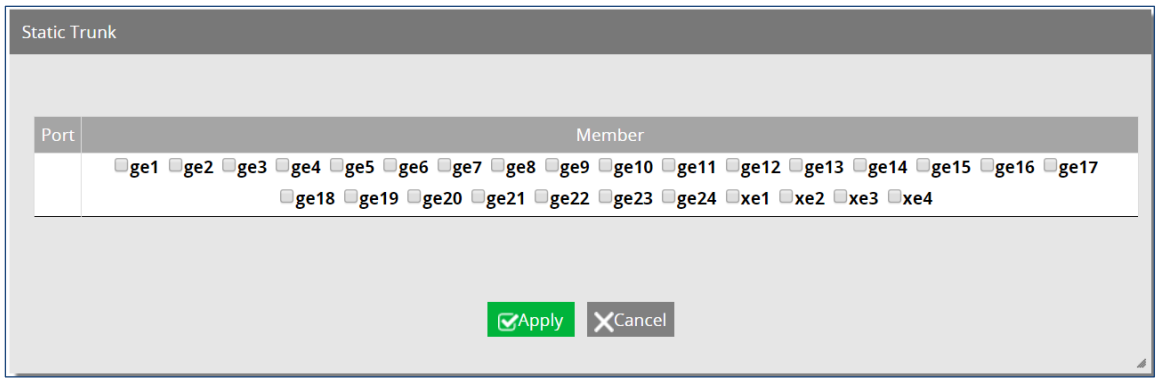


Configure the Storm Detect parameters for each port by clicking on the check box and entering values for:

By Utilization: Percentage of port's maximum speed
By Broadcast / Multicast+Broadcast: Type of packet to be monitored
Packets Per Second: Threshold for Storm Detect activation

Trunking

The switch supports Static Channel Trunking for up to 12 trunks. To add a trunk, click the add icon in either the **Static Trunk** or **LACP Trunk** section, and then select the ports to be added. Then click “Apply.”

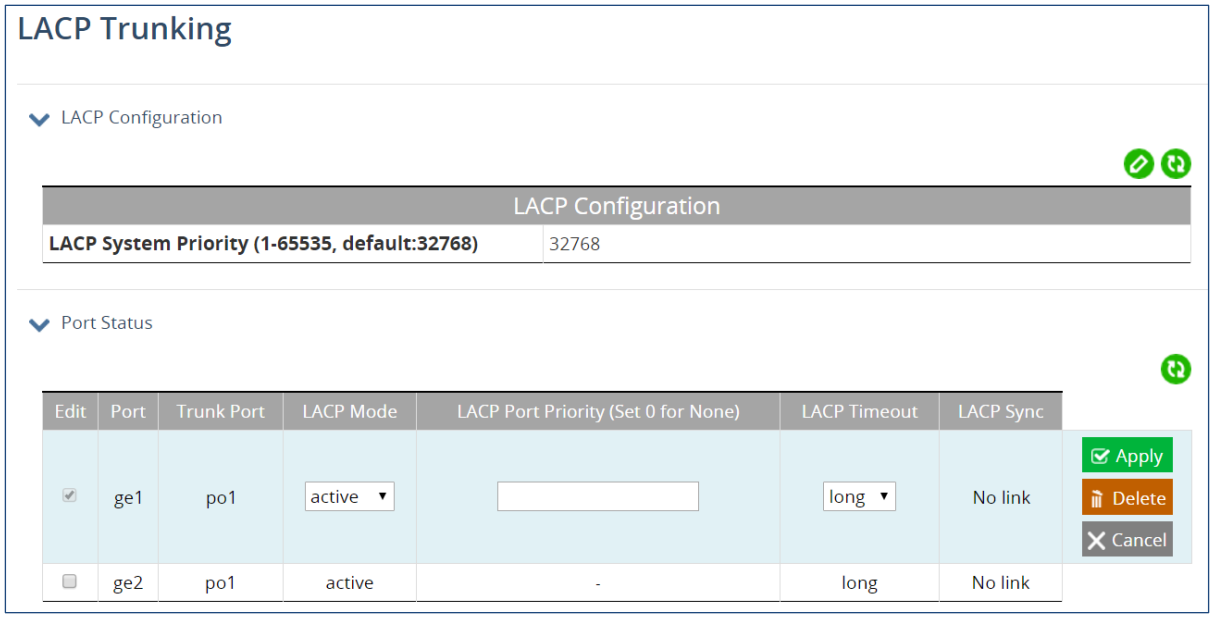


LACP Trunking

The Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP). This means that both sides of the LACP channel must be configured for LACP which implies both devices must support it.

The LACP system priority is used with the MAC address of the switch to create a system ID and to negotiate with other switches. A higher number means a lower priority.

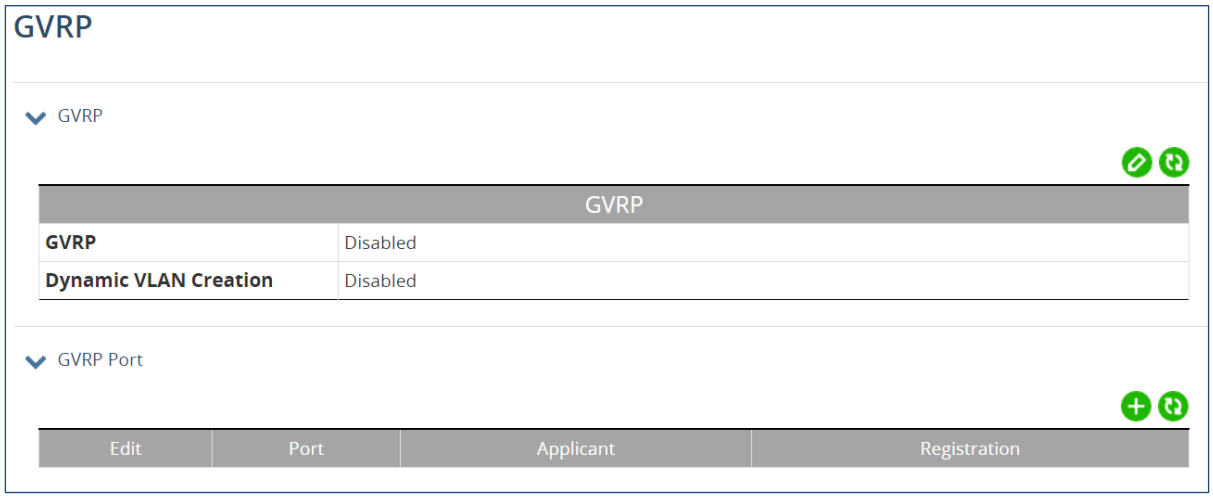
LACP port priority is set on each LACP port. The port priority is used with the port number to create the port identifier. The port priority determines which ports will be put in standby mode when aggregation for all ports is impossible.

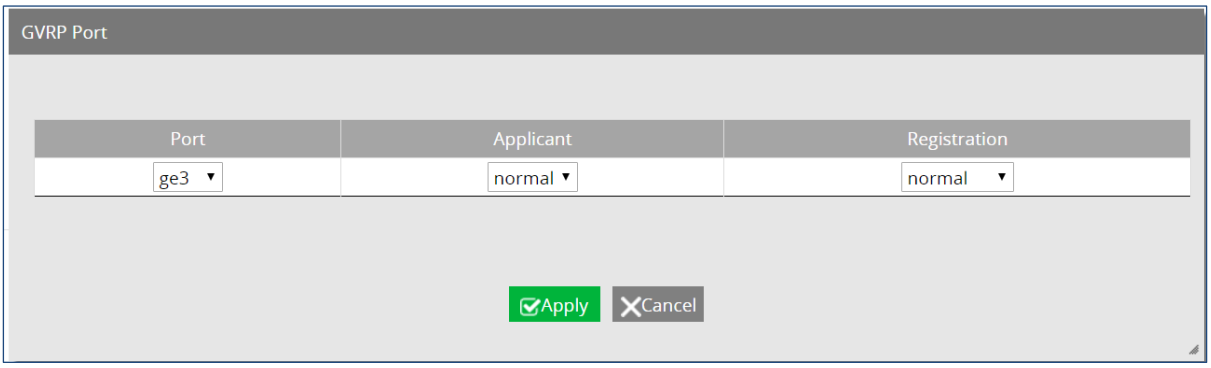


GVRP

GVRP is used to dynamically create VLANs on a switch. Any IEEE 802.1Q compliant switch must implement this protocol.

To enable GVRP, click the edit icon and then the radio button next to **GVRP** and/or **Dynamic VLAN Creation**. Then add a GVRP port by clicking the add icon, and selecting the desired port, **normal** or **active** status for the Applicant, and **normal**, **fixed**, or **forbidden** for Registration.



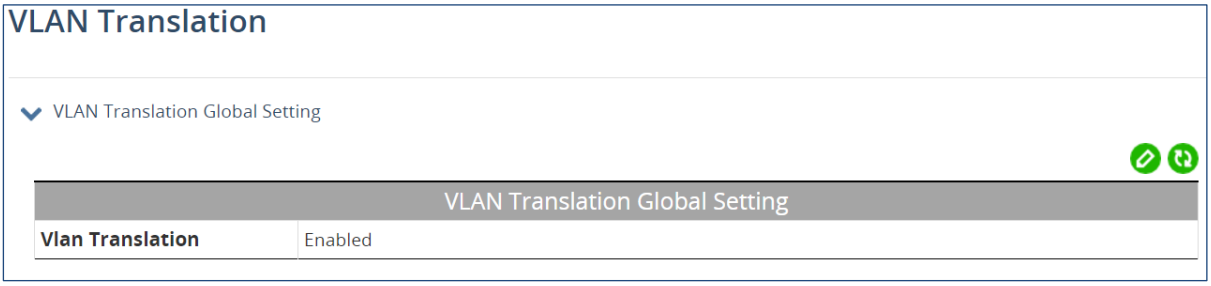


Add GVRP Port

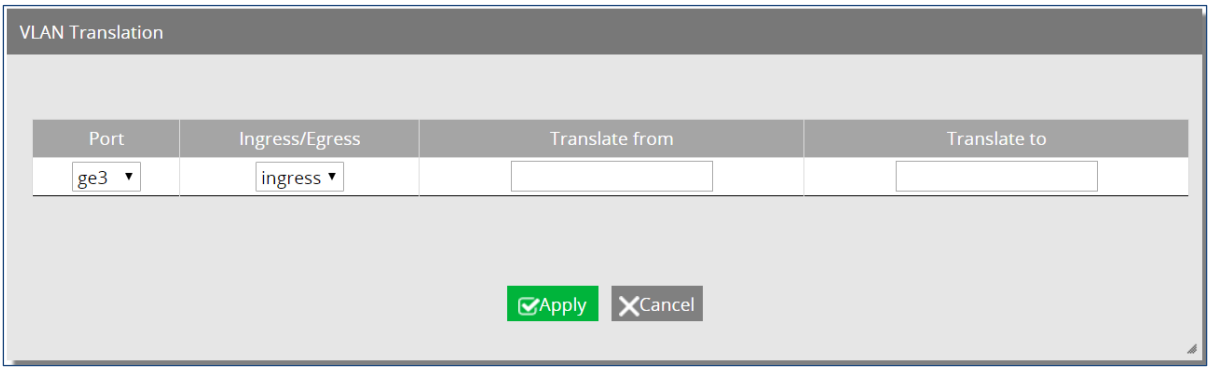
VLAN Translation

In VLAN translation, a VLAN tag is removed from an Ethernet frame and rewritten to a different VLAN. This effectively “translates” the frame from one VLAN ID to another. This can be very useful when merging two networks in which the same VLAN is used by both.

To enable VLAN translation, click the edit icon and then click the radio button next to **enable**.



To add a new translation entry, click the add icon. Select the port, and whether the translation is to take effect on packet **ingress** or **egress**. Then enter the corresponding VLAN IDs in the **Translate from** and **Translate to** fields. Then click “Apply.”



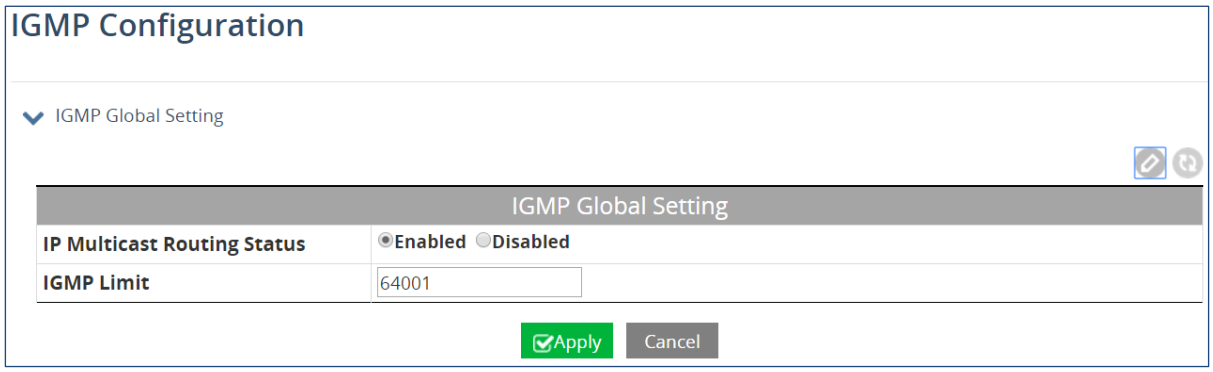
7 IGMP

IGMP Configuration

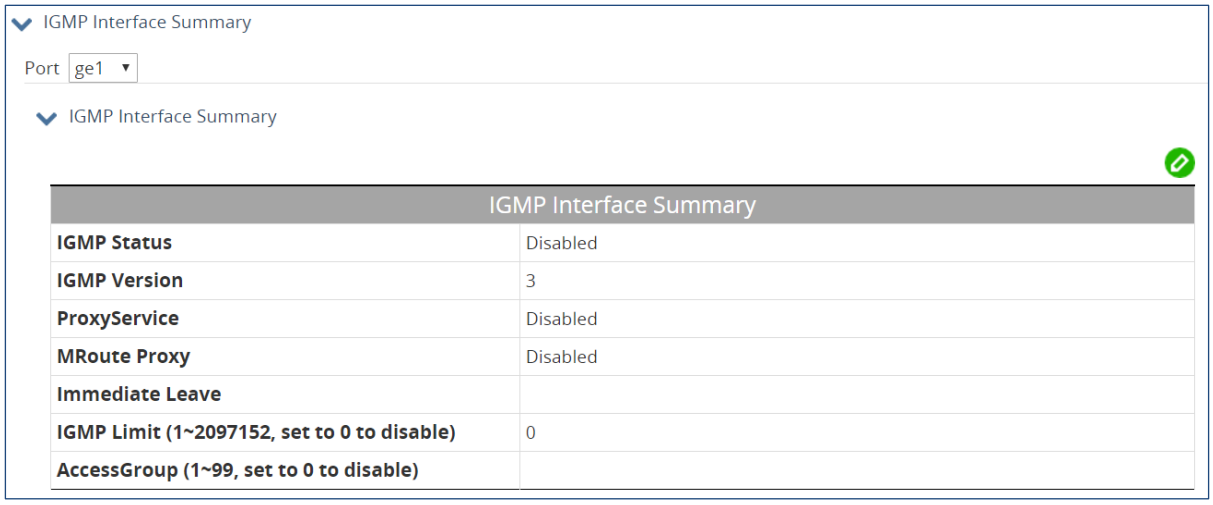
IGMP (Internet Group Management Protocol) was designed to manage IP multicast applications. There are three versions of IGMP, and all versions are backwards compatible:

IGMP version 1 sends queries to 224.0.0.1, while membership reports are sent to the group's multicast address.
IGMP version 2 accelerates the leaving of a group, and makes other adjustments to timeouts. Leave-group messages are sent to 224.0.0.2. It also introduces a group-specific query, which is sent to the multicast address of the group.
IGMP version 3 introduces source-specific multicasts. Membership reports are sent to 224.0.0.22

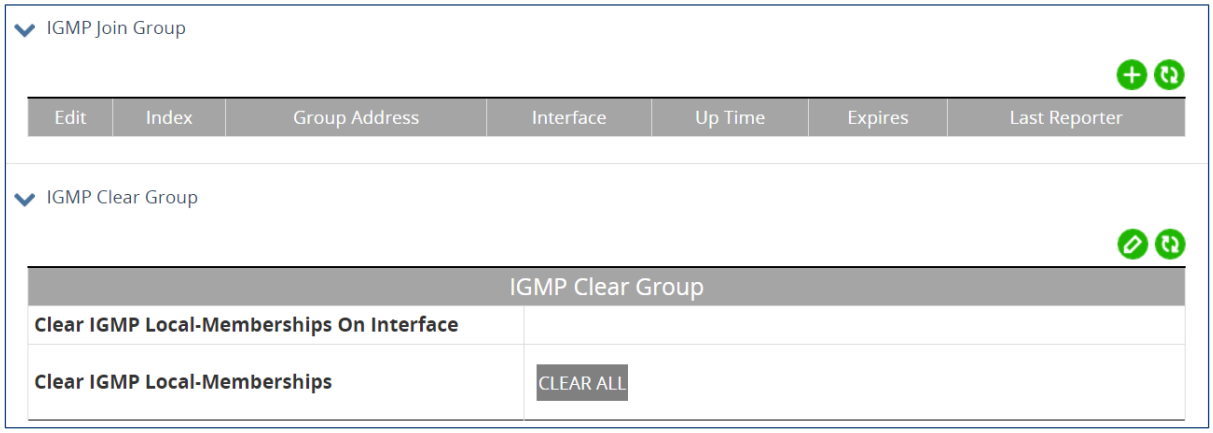
To enable IGMP globally on the switch, click the edit icon in the top panel, and select the radio button next to **enabled**. Enter a number for the **IGMP Limit**, which is the maximum number of group membership states (range is 1-2097152).



To enable IGMP on an interface, select the interface from the drop-down menu in the second panel, then click the edit icon. Select the radio button next to **enabled**, and then select the IGMP version to be run. Enable **ProxyService** and/or **MRoute Proxy** if needed. Then set the **Immediate Leave**, **IGMP Limit**, and **Accessgroup** parameters.



In the bottom panel, you can add IGMP Join Groups, and clear selected or all IGMP Local Memberships.



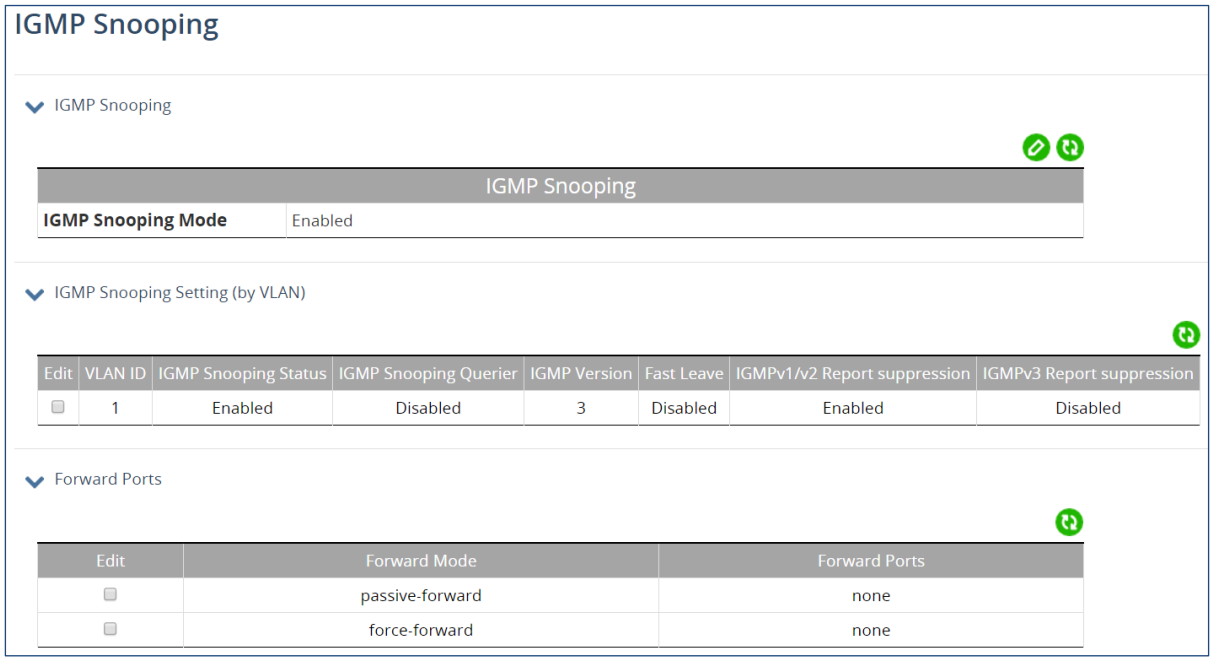
IGMP Snooping

A switch running IGMP snooping will dynamically determine which hosts connected to a particular VLAN in the switch should receive specific multicasts. The switch “snoops” (listens in on) IGMP messages and other multicast transmissions. The switch then determines which ports are associated with each multicast transmission.

Enable IGMP snooping by clicking the edit icon in the first panel, and selecting **enabled**. Then click “Apply.”

To configure IGMP settings for a specific VLAN, click the check box next to the VLAD ID. Then set the parameters for **IGMP Snooping Status**, **IGMP Snooping Querier**, **IGMP Version** (1 -3), **Fast Leave**, **IGMPv1/v2 Report suppression**, and **IGMPv3 Report suppression.**

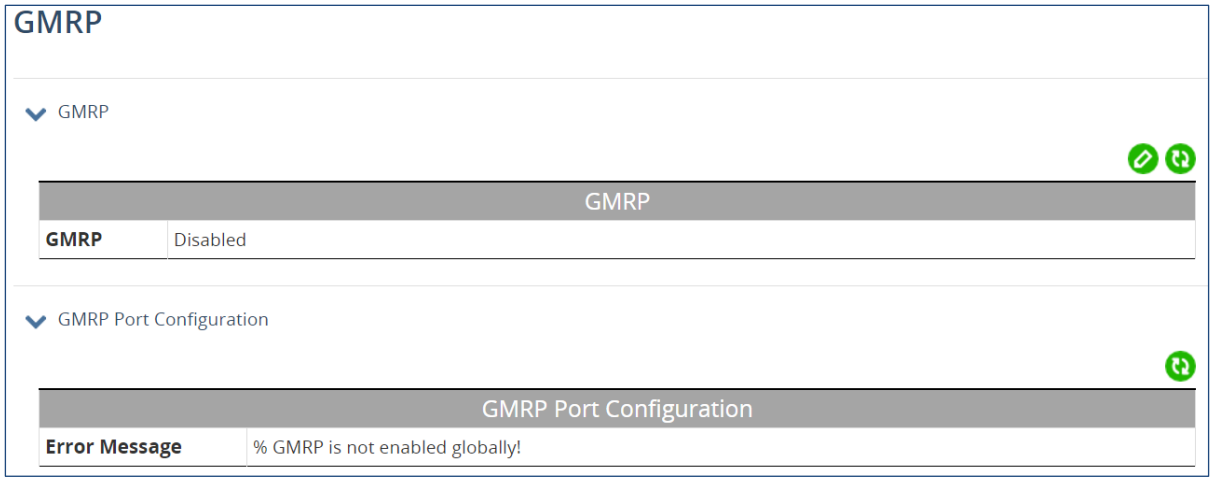
In the bottom panel, select which ports will take a **passive-forward** role, and which ones will be **force-forward**.

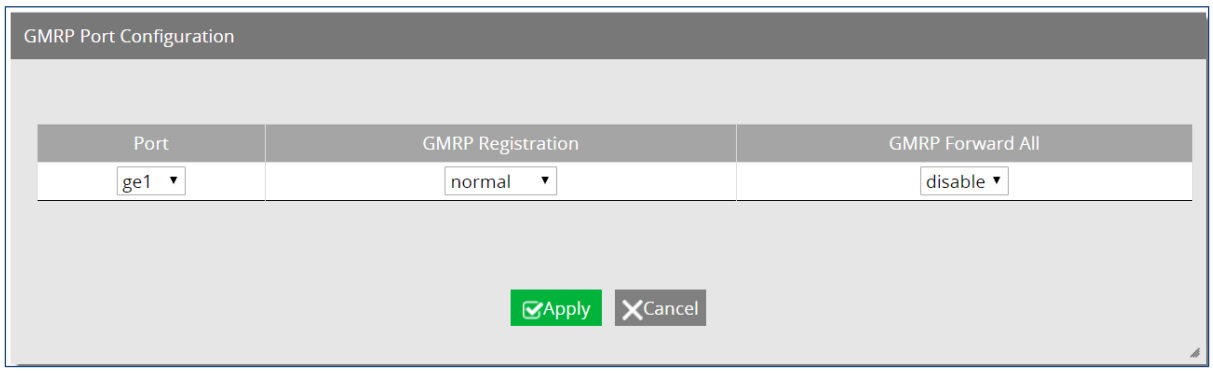


GMRP

The settings in the GMRP feature controls how the switch automates the process of multicast packet forwarding, both within a single switch as wells as between switches in a bridged network. With the GMRP feature enabled, when the switch receives any GMRP multicast group registration requests from either a multicast client or a neighbor switch, the switch will register these multicast groups on these ports and will only transmit the multicast packets that belong to these groups to these ports. The switch will also automatically propagate these multicast group registrations onto the neighbor switches to allow the neighbor switches to forward the multicast packets that belong to these groups to the local switch.

To enable GMRP, click the edit icon and select enabled. Once GMRP is enabled, you can configure GMRP on a port. Click the add icon in the lower panel, and use the drop-down menu to select a port. Set the GMRP Registration: **normal**, **fixed**, **forbidden**, or **restricted**. Set GMRP Forward All field to **enable** or **disable**. Then click “Apply.”


GMRP
GMRP
GMRP
GMRP
Disabled
GMRP Port Configuration
GMRP Port Configuration
Error Message
% GMRP is not enabled globally!


GMRP Port Configuration
Port
GMRP Registration
GMRP Forward All
ge1
normal
disable
Apply
Cancel

8 STP

The Spanning Tree algorithm works by designating a single switch (The Root Bridge) in the network, as the root or the parent to all the switches. All the switches in the network will use the same algorithm to form unique paths all the way back to the Root Bridge. Some switches establish a blocking point (a port on a switch) somewhere along the path to prevent a loop. There are 3 versions of the Spanning Tree protocol, STP, RSTP, MSTP, and they are all backwards compatible with each other.

Spanning Tree Protocol (STP)

This is the original Spanning Tree protocol, and it has been superseded by both the RSTP and MSTP protocol. It is based on a network with a maximum diameter of no more than 17 switches. It uses timers to synchronize any changes in the network topology, and this could take minutes. It is not recommended that you use this version of the Spanning Tree protocol.

Rapid Spanning Tree protocol (RSTP)

The RSTP protocol is the new enhanced version of the original STP protocol. It uses an enhanced negotiation mechanism to directly synchronize any topology changes between switches; it no longer uses timers as in the original STP protocol, which results in a faster re-convergence time. The maximum allowed network diameter for the RSTP protocol is 40 switches.

Multiple Spanning Tree Protocol (MSTP)

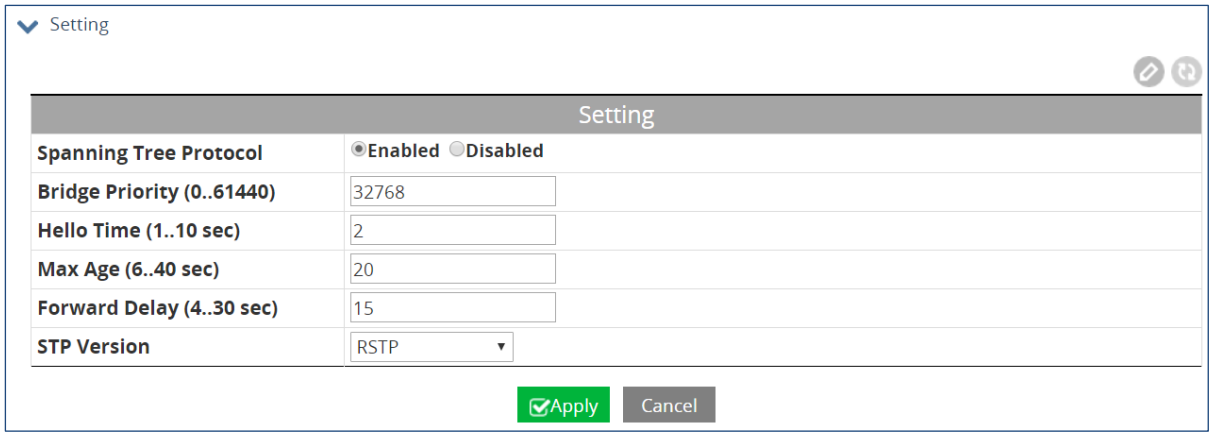
The MSTP protocol extends the RSTP protocol by simultaneously running multiple instances of the Spanning Tree Protocol and mapping different VLANs to each instance, thus providing load balance across multiple switches. The MSTP protocol accomplishes this by creating new extended sections within the RSTP protocol, called Regions. Each region runs its own instance of the Spanning Tree Protocol. Within each Region, the MSTP protocol can accommodate a network diameter of up to 40 switches. There can be a maximum of 40 Regions in a single MSTP network.

Global Configuration

Spanning Tree Protocol is enabled by default. To enable/disable STP, click the edit icon in the lower panel of the page, and click the corresponding radio button. The set values for the following fields:

- **Bridge Priority** – Bridge Priority is used to set the Root and backup Root Bridge. Default is 32768. Range is 0 to 61440.
- **Hello Time** – The rate at which BPDUs (Bridge Protocol Data Units) are sent. Default is 2 seconds. Range is 1 to 10 seconds.

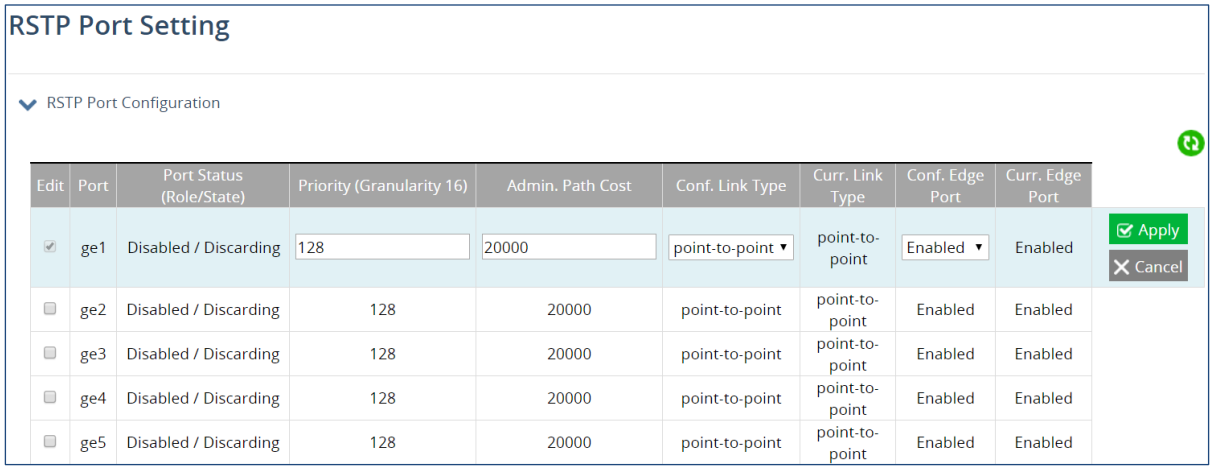
- **Max Age** – Hop count limit for BPDU packets. Range is 6 to 40. Default is 20.
- **Forward Delay –** Range is 4 to 30 seconds. Default is 15 seconds.
- **STP Version –** Select from MSTP, RSTP, or STP compatible



RSTP Port Setting

Configure individual port RSTP settings on this page. Click the checkbox next to the desired ports, and set the following parameters:

- **Port Priority** – Port Priority range is between 0 and 240 in multiples of 16.
- **Admin Path Cost** – range is between 1 and 200,000,000.
- **Conf. Link Type** – This is the spanning tree link type. Choose **auto (**link type is set based on the interface's duplex setting**)**, **point-to-point**, or **shared**.
- **Conf. Edge Port –** Select **enable** to make the interface an edge port.



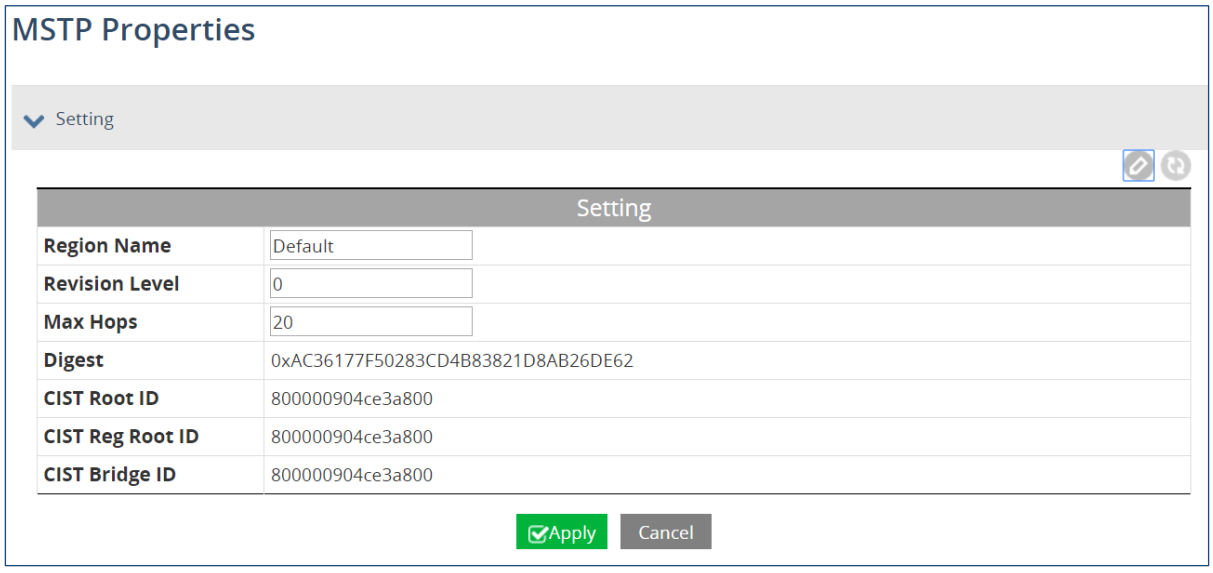
MSTP Properties

In order to form a MSTP Region, the switches that will be connected together to form the MSTP Region must have the same values for these parameters:

- Region name
- Revision level
- Configuration Digest

The first two parameters can be configured directly on the MSTP Properties screen. **Configuration Digest** will be automatically calculated by the switch based on the **VLAN** to **MSTI (Multiple Spanning Tree Instance)** mapping. The **VLAN** to **MSTI** instance mapping must be the same for all the switches within the same **MSTP Region.**

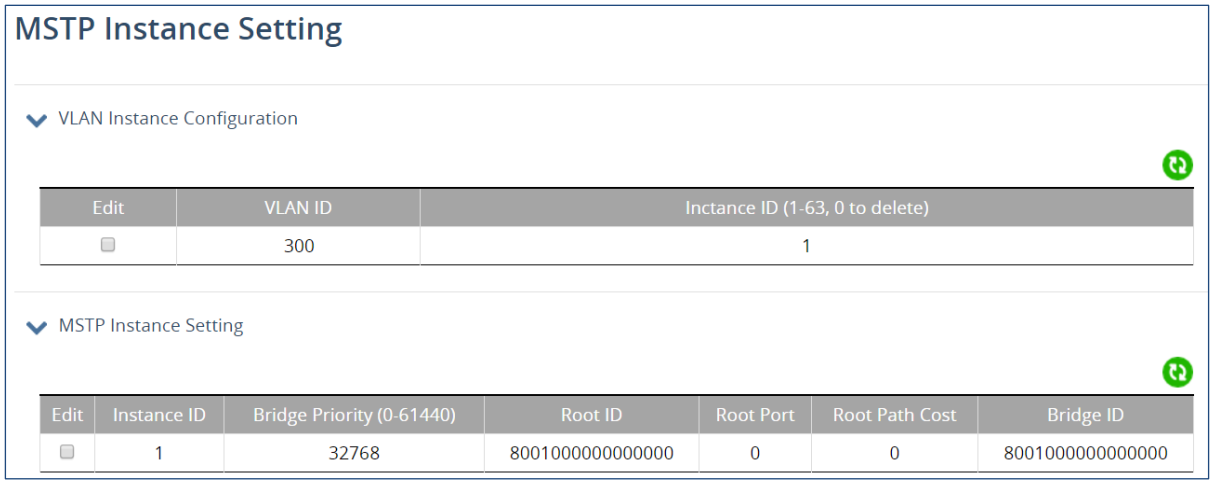
Click the edit icon, and enter the **Region Name**, **Revision Level**, and **Max Hops**. Then click "Apply."



MSTP Instance Setting

Select the **VLAN** that you want to map to an MSTP instance by clicking the corresponding check box next to the VLAN ID. Then enter the instance ID and click "Apply."

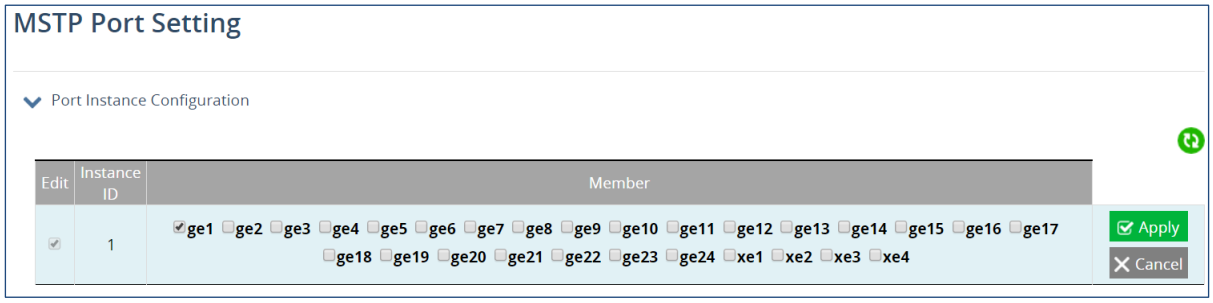
Configure the MSTP instance by clicking the check box next to the Instance ID, and entering the Bridge Priority (range is 0 to 61440).



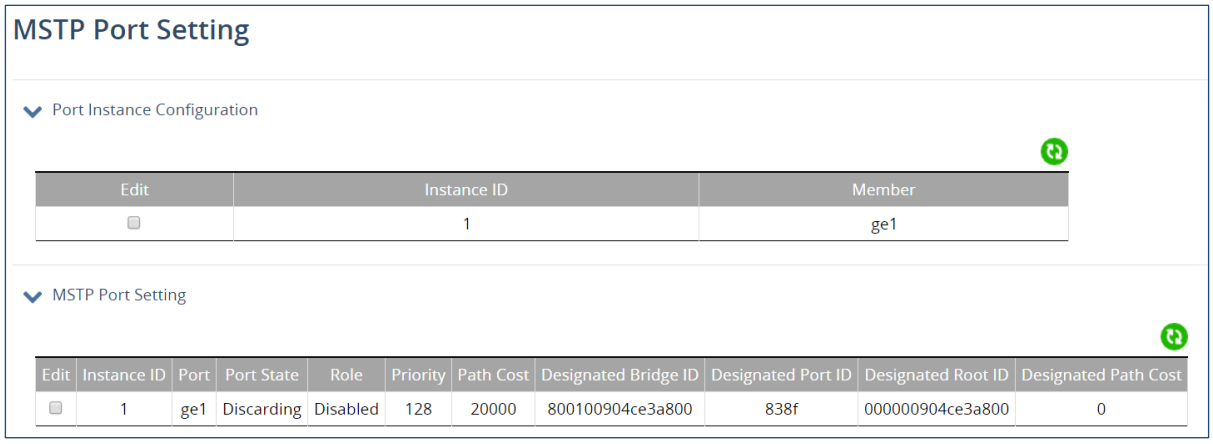
MSTP Port Setting

You can adjust the location of the blocking port in a MSTP network by modifying the **Port Priority** and the **Path Cost** of the ports on the switch. Modifying the **Port Priority** adjusts the blocking port between two switches. Modify the **Port Cost** adjusts the location of the blocking port in a MSTP loop.

First assign ports to an MSTP instance by clicking the check box next to the instance ID, and then the check boxes next to the ports you want to add.



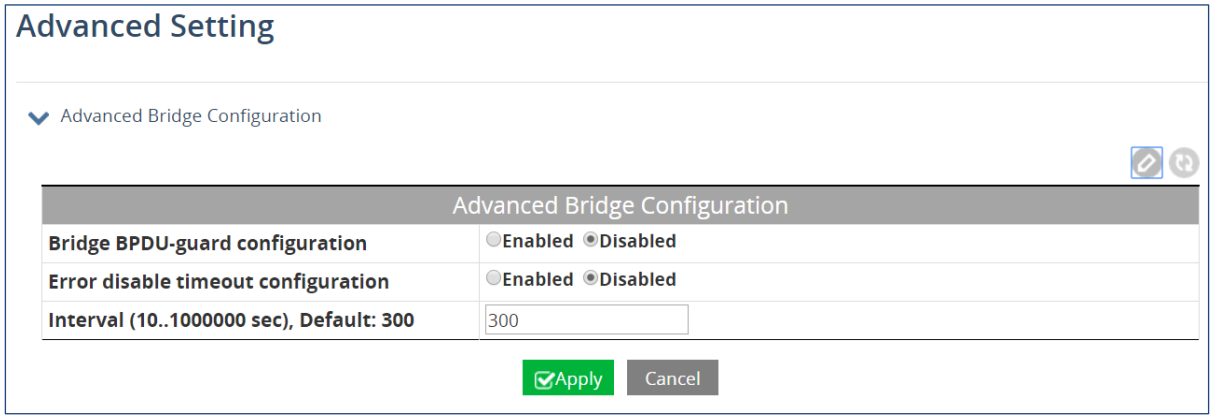
To modify the **Port Priority** and the **Path Cost**, click the check box next to the corresponding MSTP instance in the bottom panel, and enter values in those fields. Then click “Apply.”



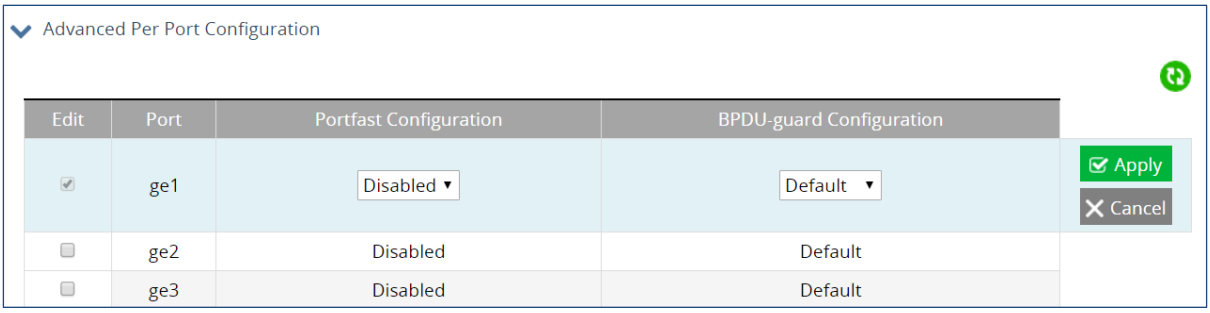
Advanced Setting

The top panel of the Advanced Setting page contains three settings which determine how the switch handles BPDU packets.

- **Bridge bpdu-guard configuration -** When the BPDU Guard feature is set for a bridge, all portfast-enabled ports of the bridge that have **bpdu-guard** set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed.
- **Error disable timeout configuration –** Enabling this allows a Disabled port to re-enable itself automatically after the specified Interval.
- **Interval –** Default is 300 seconds. This is the length of time a port will remain disabled after shutting down due to the **bpdu-guard**.



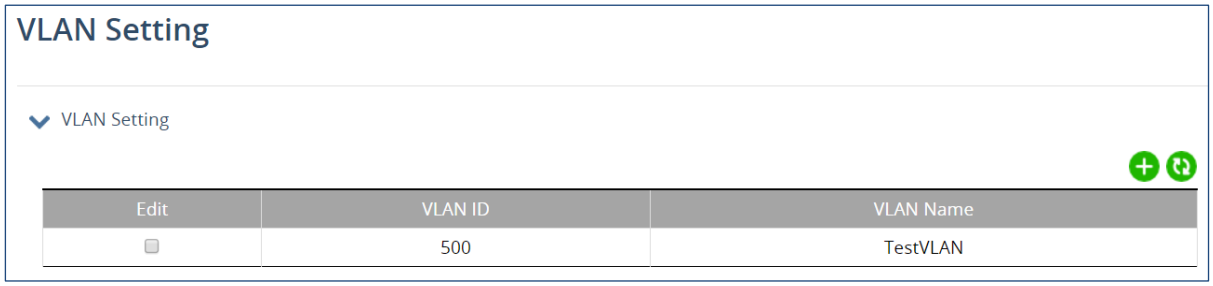
In the Advanced Power Port configuration panel, you can enable **Portfast**, which sets a port as an edge-port to enable rapid transitions, and enable disable **BPDU-Guard Configuration**. When set to default, the port will use the Advanced Bridge Configuration settings. Enable or Disable to override the Bridge BPDU-Guard settings.


Advanced Per Port Configuration
Edit
Port
Portfast Configuration
BPDU-guard Configuration
ge1
Disabled
Default
Apply
Cancel
ge2
Disabled
Default
ge3
Disabled
Default

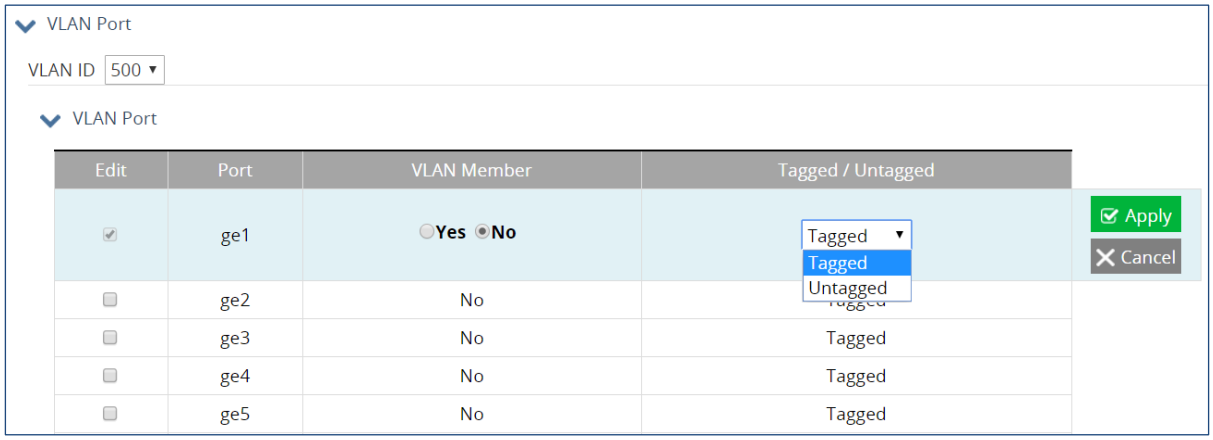
9 VLAN

VLAN Setting

VLANS are created and modified in the VLAN Setting panel. Click the add icon, and then enter the VLAN ID and the VLAN name. The VLAN name should not be more than 32 characters, and cannot include spaces. If you do not specify a VLAN name, the system will create one. Click “Apply” when finished.

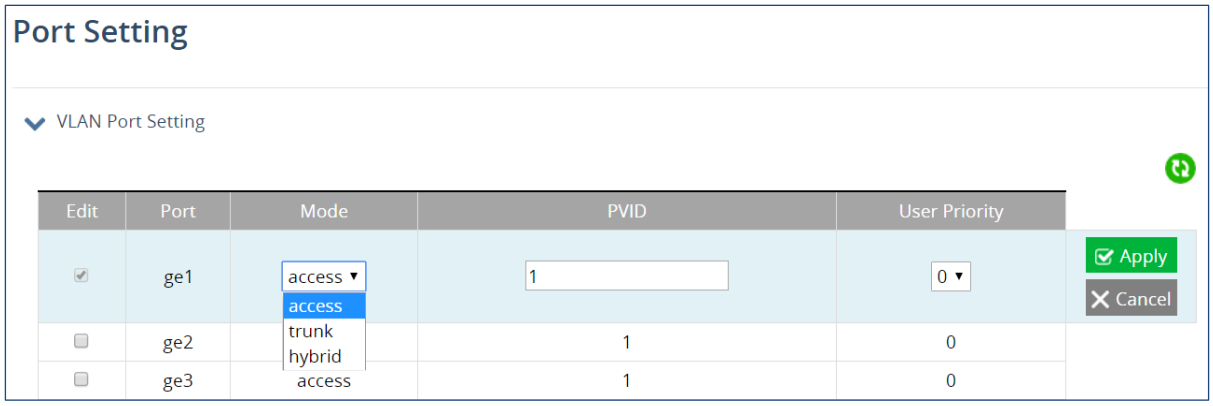


After a VLAN has been created, use the VLAN Port panel to attach specific ports to the VLAN, and to set as Tagged or Untagged. Click “Apply” when finished.



Port Setting

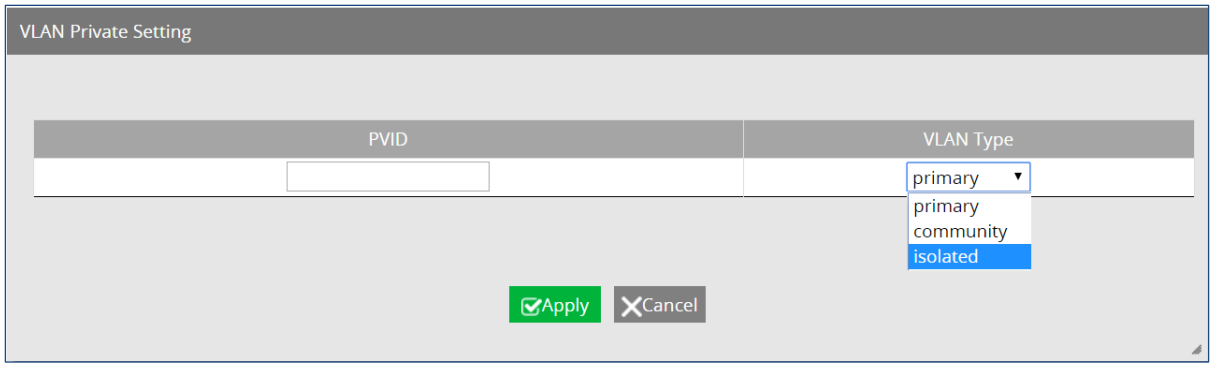
Configure the port type (**access**, **trunk**, or **hybrid**), **PVID**, and **User Priority** for each switch port.



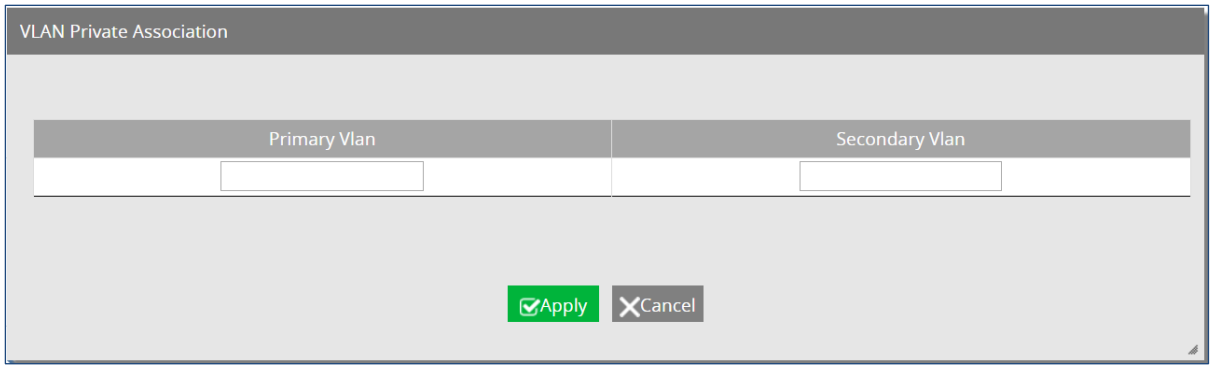
Private VLAN

In private VLANs, a primary VLAN is broken into secondary VLANs, classified as either **community** or **isolated**. Hosts in an isolated secondary VLAN can't communicate with anything except the **promiscuous** port, which is usually a gateway. In private VLANs, a primary VLAN is broken into secondary VLANs, classified as either **community** or **isolated**. Hosts in an isolated secondary VLAN can't communicate with anything except the **promiscuous** port, which is usually a gateway or uplink. Hosts within the same community can communicate with other members of that community VLAN.

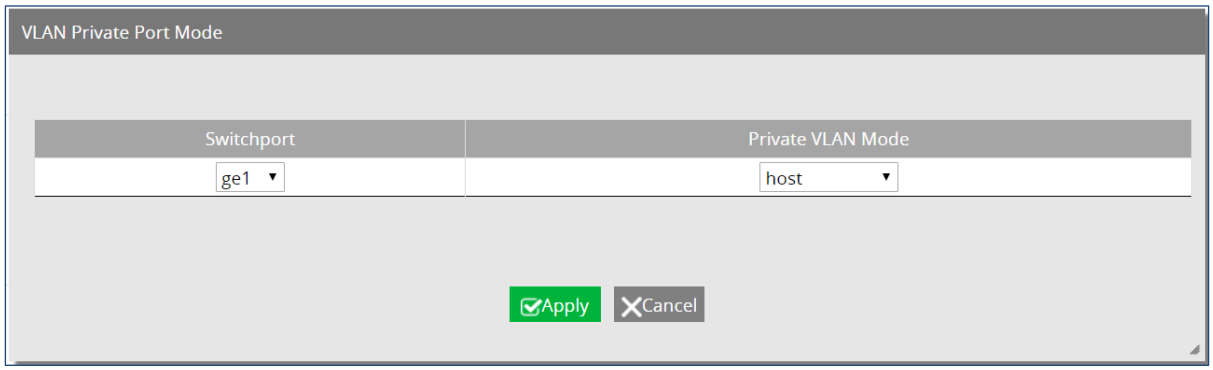
The first panel of the Private VLAN screen is Private VLAN Setting, where VLANs are added and set as primary, community, or isolated. Note that the VLANS added here must have been already created on the VLAN Setting screen. To add a private VLAN, click the add icon, and enter the VLAN ID. Then select the **VLAN Type**, and click “Apply.”



Private VLAN associations are set up in the second panel. Click the add icon, and enter the VLAN ID of the primary and secondary VLANs. Then click “Apply.”



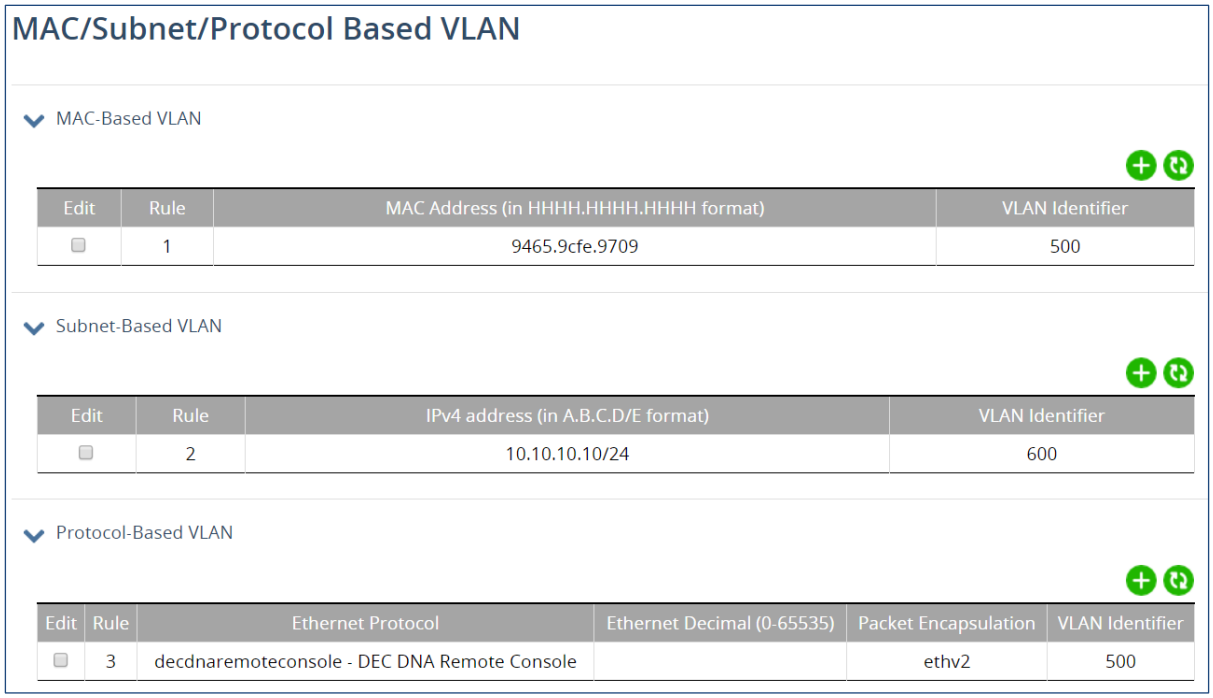
In the third panel, configure port status in a private VLAN. Click the add icon, then the select the port using the drop-down menu. Set the port as either **host** or **promiscuous**. Then click "Apply." Note that ports still must be made a member of the secondary VLAN on the VLAN Setting screen.

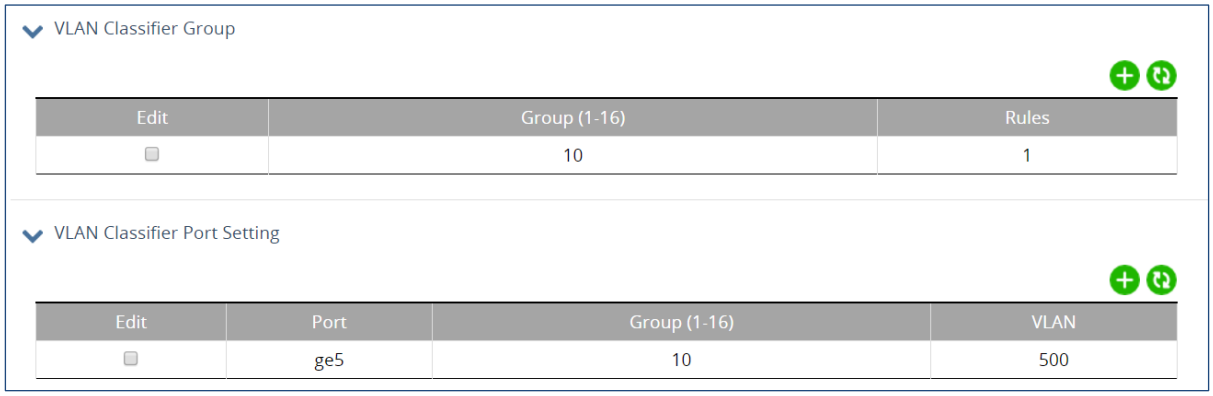


MAC/Subnet/Protocol Based VLAN

In port-based VLANs, a port is mapped directly to a VLAN. Instead of a port, you can also map MAC addresses, IPv4 addresses, or an Ethernet protocol to a specific VLAN. Each mapping must have its own rule number. When aping to a protocol, you must also specify the type of packet encapsulation: **ethv2**, **snapllc**, or **nosnapllc**.

Multiple rules can be grouped into a single **VLAN Classifier Group**, which can be created in the third panel. In the fourth panel, a VLAN Classifier Group can be assigned to a port.

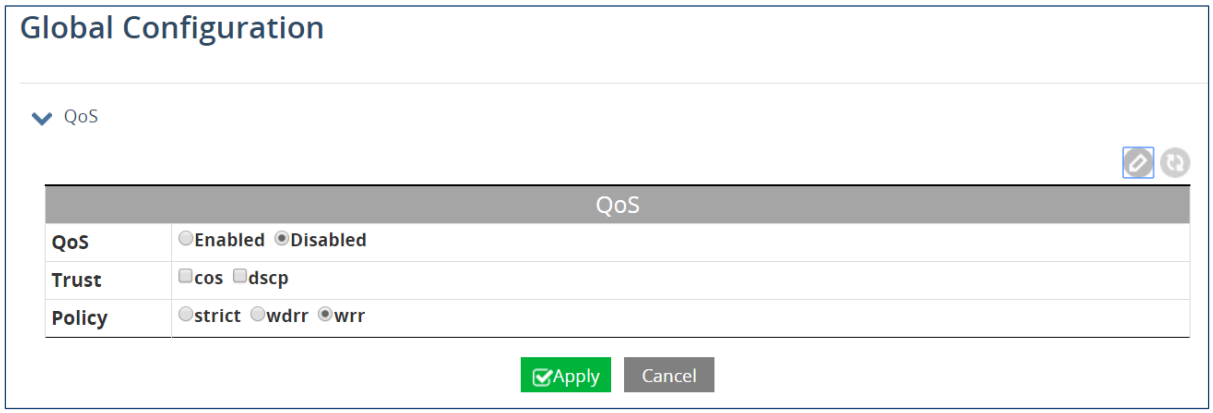

MAC/Subnet/Protocol Based VLAN
MAC-Based VLAN
Edit
Rule
MAC Address (in HHHH.HHHH.HHHH format)
VLAN Identifier
1
9465.9cfe.9709
500
Subnet-Based VLAN
Edit
Rule
IPv4 address (in A.B.C.D/E format)
VLAN Identifier
2
10.10.10.10/24
600
Protocol-Based VLAN
Edit
Rule
Ethernet Protocol
Ethernet Decimal (0-65535)
Packet Encapsulation
VLAN Identifier
3
decdnaremoteconsole - DEC DNA Remote Console
ethv2
500


VLAN Classifier Group
Edit
Group (1-16)
Rules
10
1
VLAN Classifier Port Setting
Edit
Port
Group (1-16)
VLAN
ge5
10
500

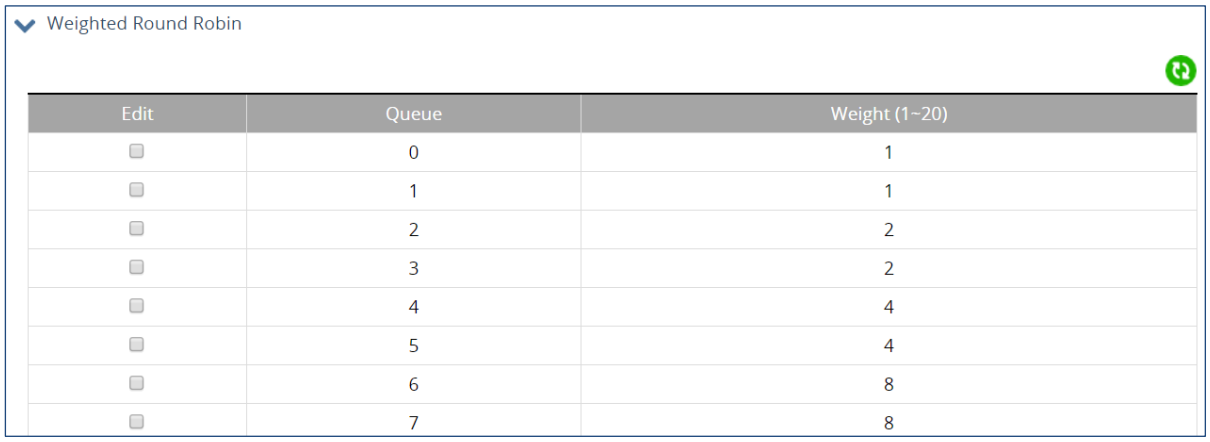
10 QOS

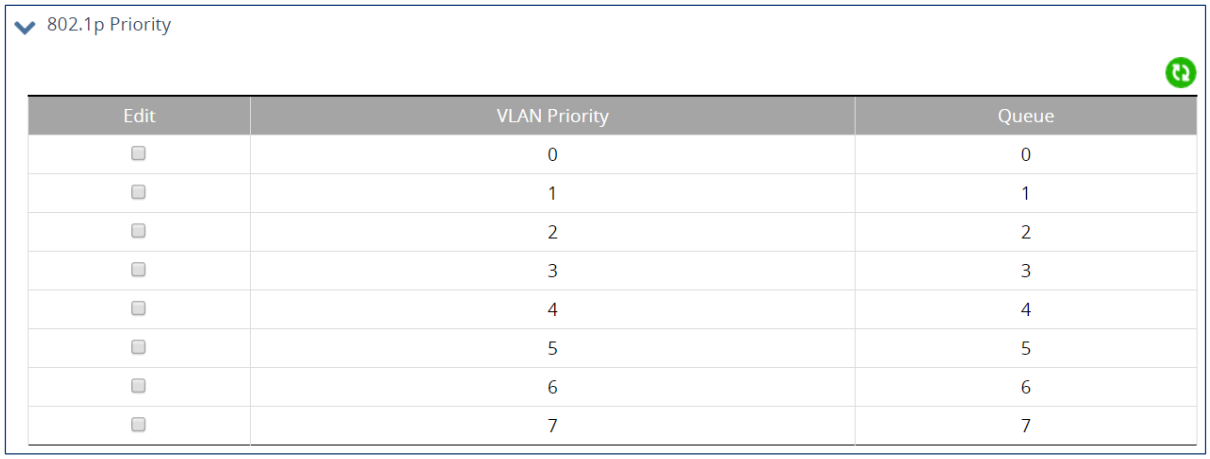
Global Configuration

To enable QoS, click the edit icon on the first panel and select the radio button next to **enabled**. Then select either **cos** (Class of Service) or **dscp** (Diffserv Code Point). Choose a queuing policy: **strict** (strict priority), **wdrr** (weighted deficit round robin), or **wrr** (weighted round robin).



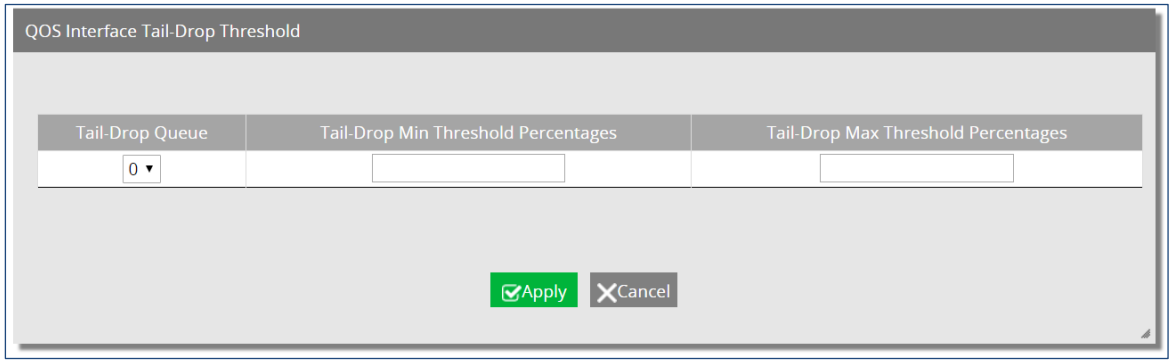
Enter the weight and the 802.1p priority for each queue in the second and third panels.

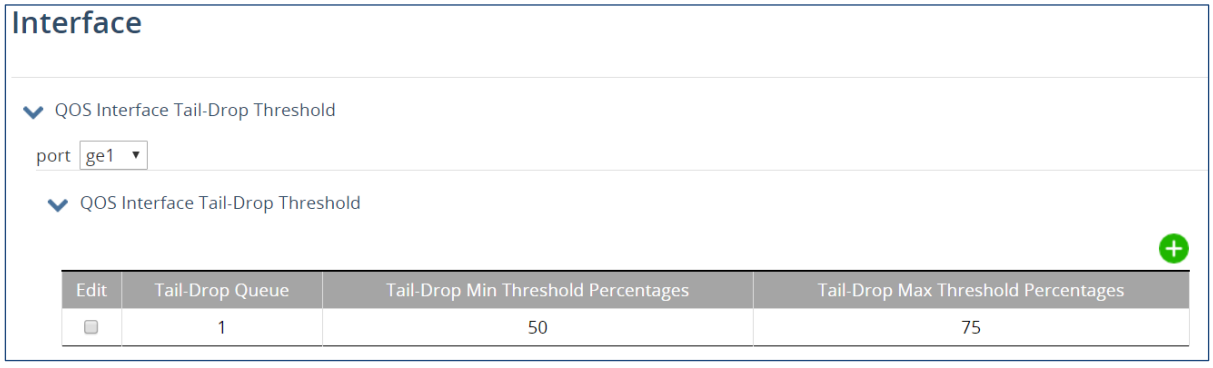




Interface

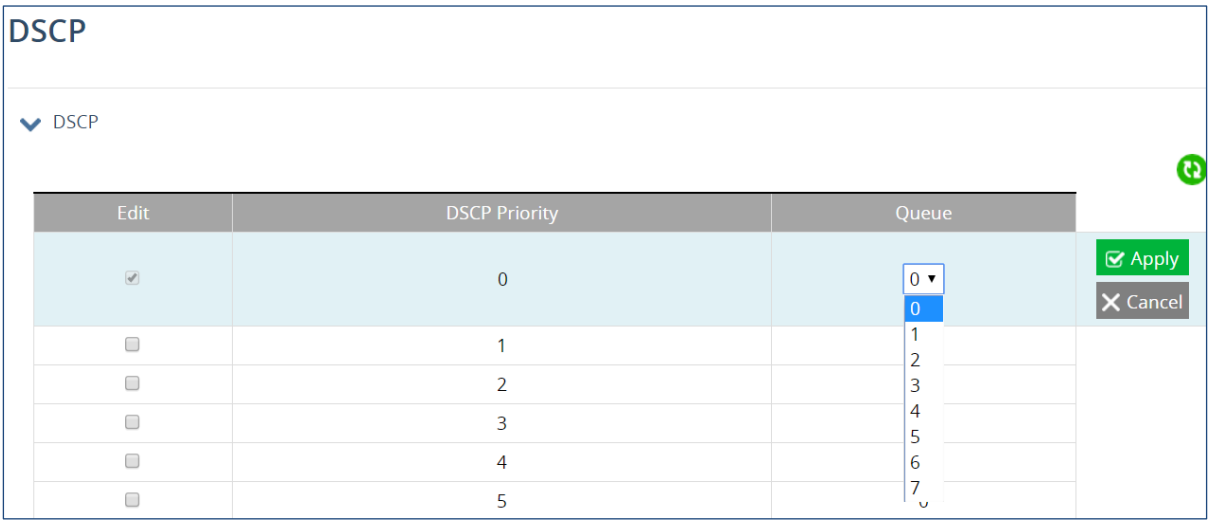
Tail drop is a queue management algorithm that determines when the switch needs to drop packets. When the queue is filled to its maximum capacity, the newly arriving packets are dropped until the queue has enough room to accept incoming traffic. Note that the minimum threshold cannot exceed the maximum threshold.





DSCP

The DSCP screen lets you choose DSCP priorities, which are by default assigned to the lowest-priority queue, 0. For each DSCP priority, you can change the value of the queue to between 0 and 7.



11 ACL

ACL Information

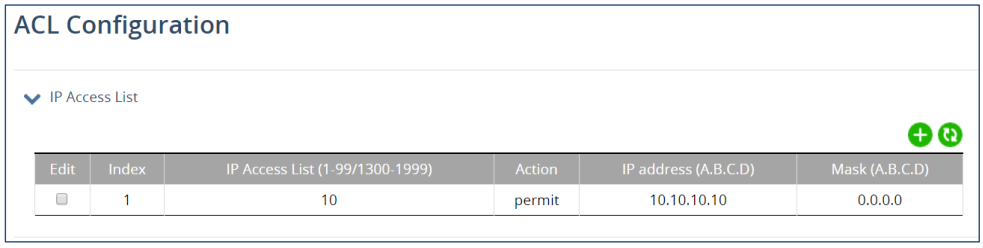
The ACL Information screen is a read-only page for viewing which ACL Policy Maps are applied to which ports. Just select the port to be viewed with the drop-down menu.

ACL Configuration

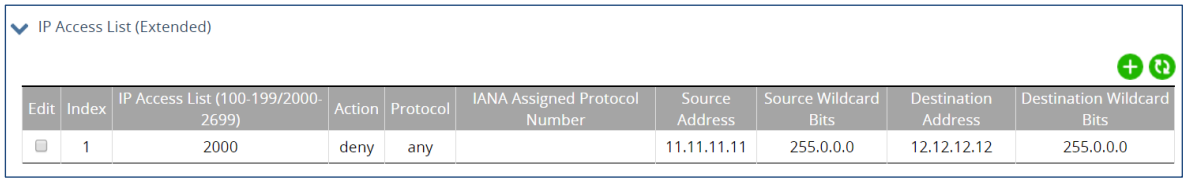
In order to enable ACL on the switch, QoS must first be enabled.

1. Create and configure an ACL Access List first.
2. Next, you will need to create and configure an ACL Class Map,
3. Associate the previously created ACL Access Lists to this ACL Class Map.
4. Next, create and configure an ACL Policy Map
5. Associate all the appropriate and necessary ACL Classes into this ACL Policy Map.
6. Then apply this ACL Policy Map (and all the Access Lists that it contains) to a specific port.

Create a standard IP Access List in the first panel by clicking the add icon and entering the required parameters.

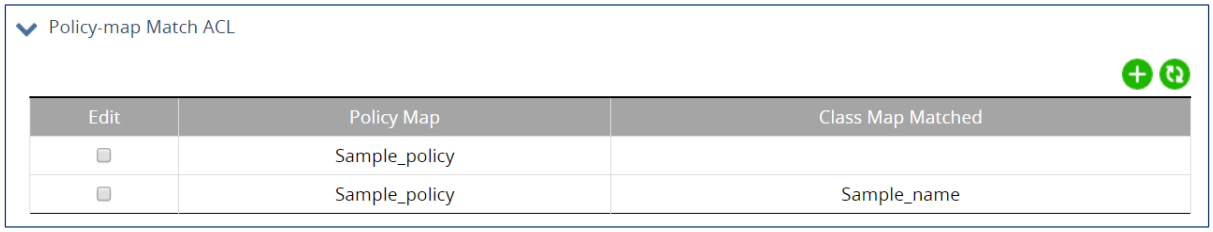


In the second panel, Extended IP ACLs are created in the same way.

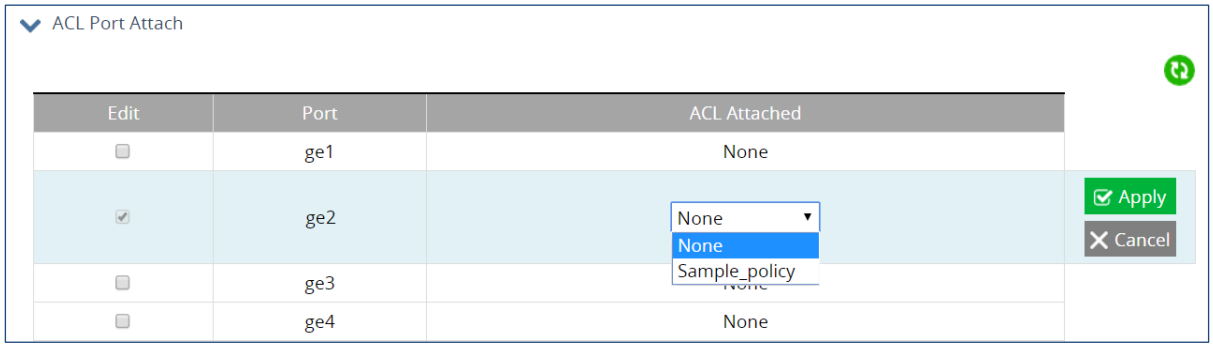


In third panel, Class Maps are created and assigned an Access List.

In the fourth panel, ACL Policy Maps are creates and assigned one or more Class Maps.



In the fifth and final panel, existing ACL policies can be applied to ports.

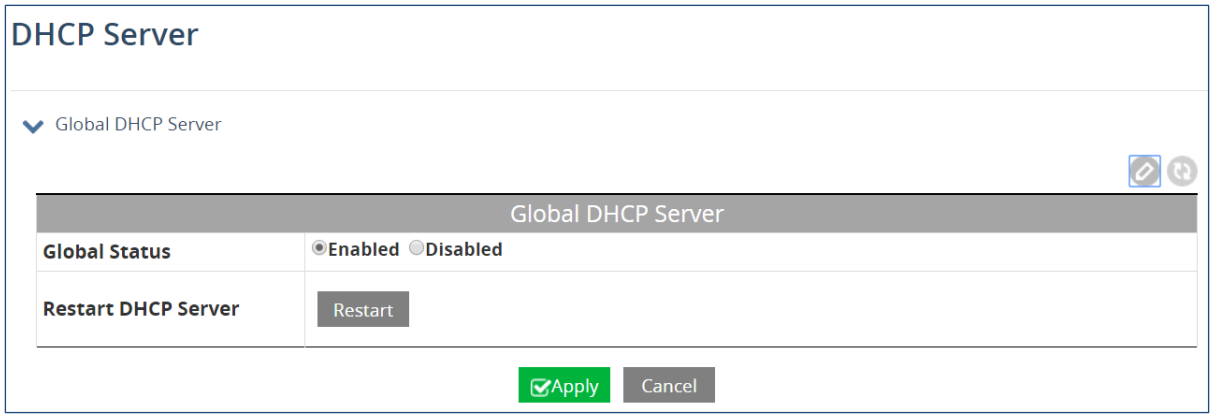


12 DHCP

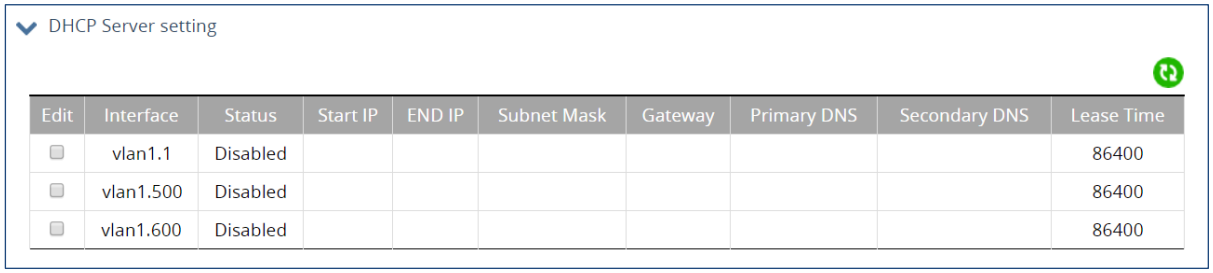
DHCP Server

The EtherWAN switch can function as a DHCP server for a single VLAN (it can be any VLAN) on the switch. When functioning as a DHCP server, the EtherWAN switch can be configured with a range of IP addresses, default gateway and DNS servers, which will allow the switch to use the dynamic configuration function of the DHCP protocol to provide any TCP/IP device that is a DHCP client, to dynamically obtain an IP address, default router, and DNS servers. The EtherWAN DHCP server can also be configured with a lease period that the DHCP clients are allowed the use of their assigned IP address. In this simple implementation, both the DHCP Client and the DHCP Server must be on the same network (same VLAN).

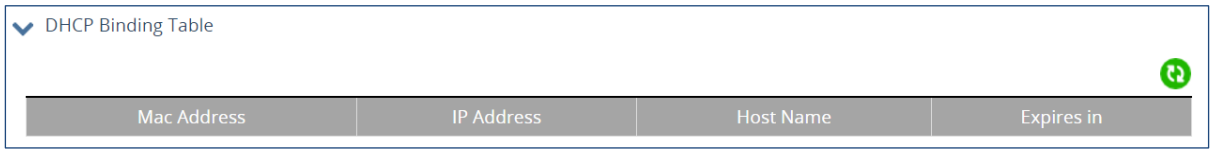
To enable DHCP, click the edit icon on the first panel, and click the radio button next to **enabled**. Then click “Apply.”



In the second panel, select the VLAN for which you want to configure DHCP, and enter the start IP, end IP, Subnet mask, Gateway, Primary & Secondary DNS, and Lease Time.



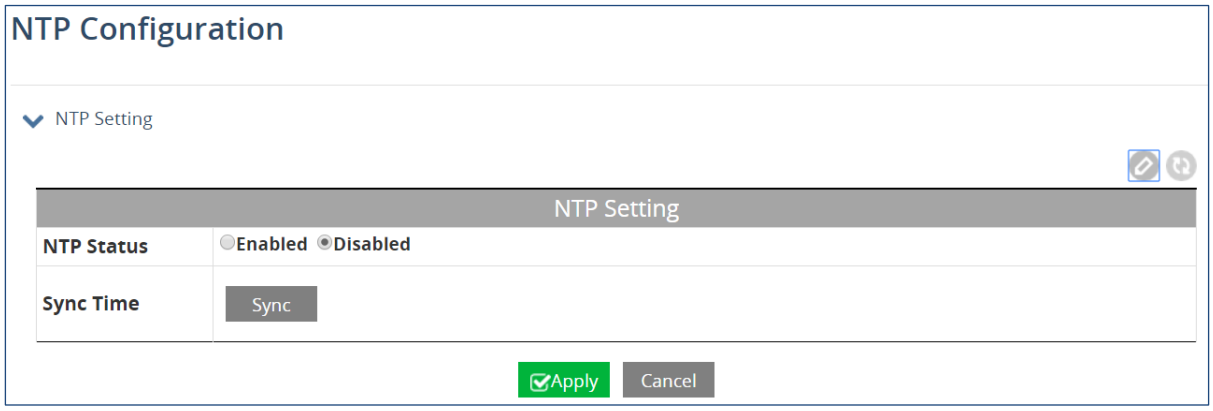
The DHCP Binding table at the bottom is a read-only table that displays which IP addresses has been allocated to which DHCP clients.


DHCP Binding Table
Mac Address
IP Address
Host Name
Expires in

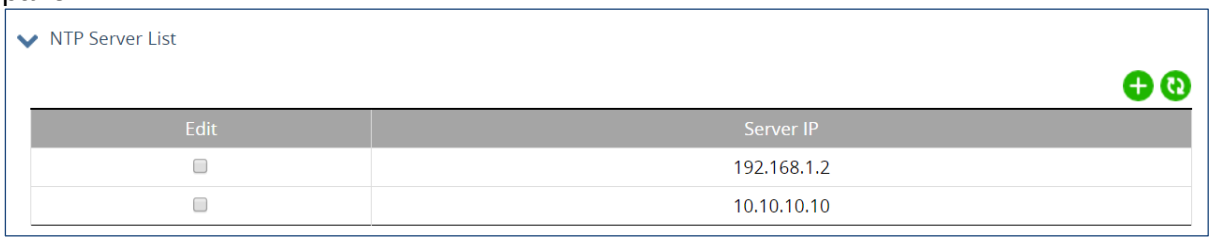
13 NTP

NTP Configuration

To enable Network Time Protocol (NTP), click the edit icon on the first panel, and click the radio button next to **enabled**. Then click “Apply.” Use the “Sync” button to force the switch to synchronize the system time with the server.

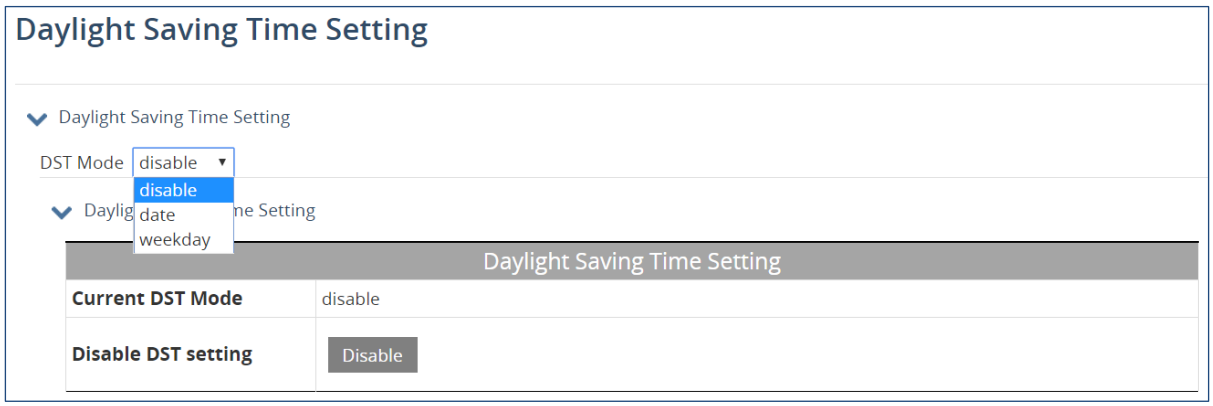


Add NTP servers in the second panel by clicking the add icon, entering the IP address of the NTP server, and then clicking “Apply.” You can see a list of all current NTP servers in this panel.

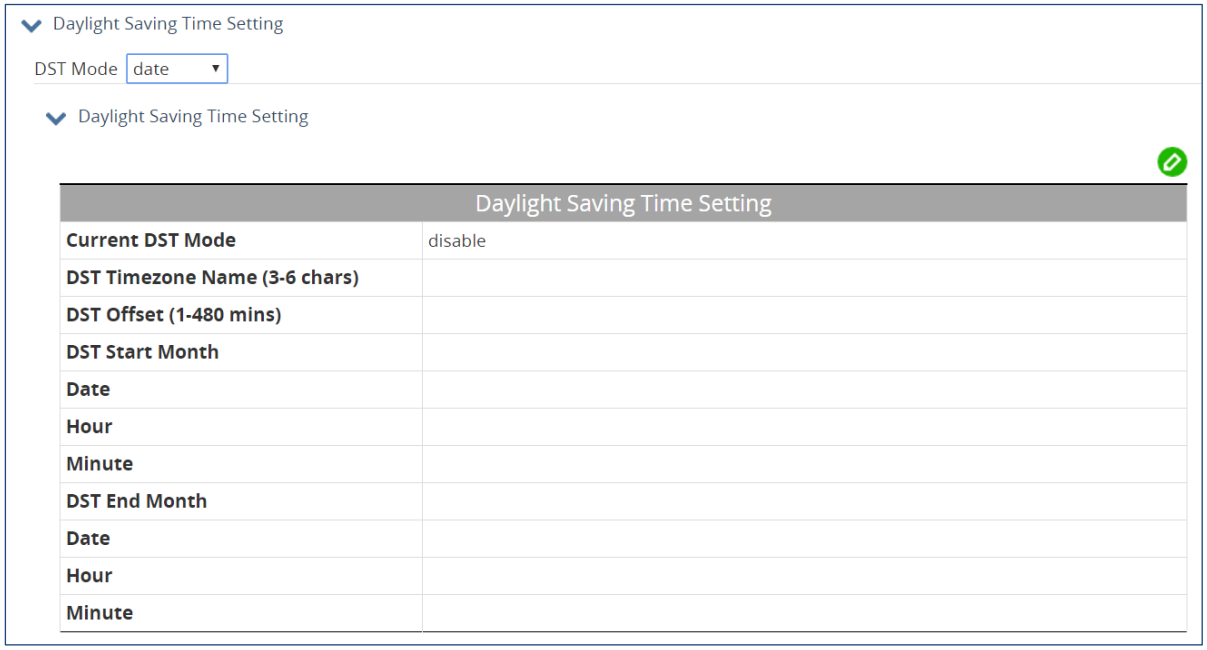


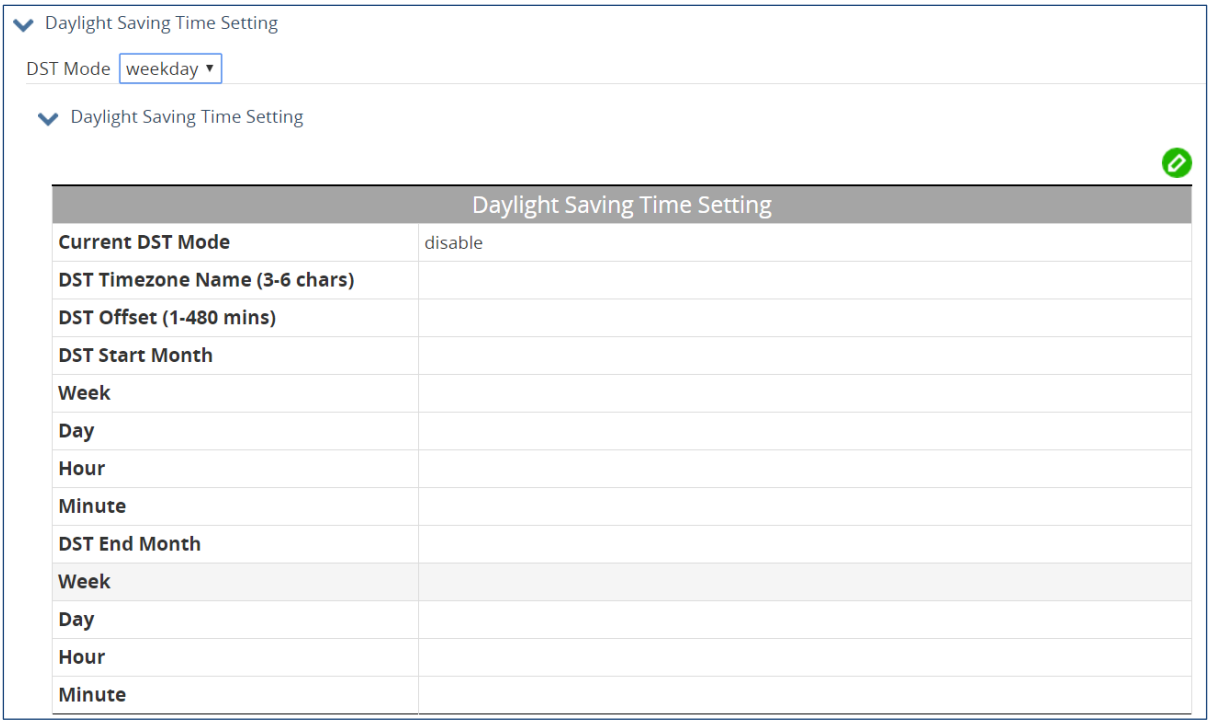
Daylight Saving Time Setting

There are two ways to set daylight saving on the switch: Weekday Mode and Date Mode. To enable daylight saving time, select the desired mode.



The only difference between the two modes is the method by which the starting and ending dates are entered.





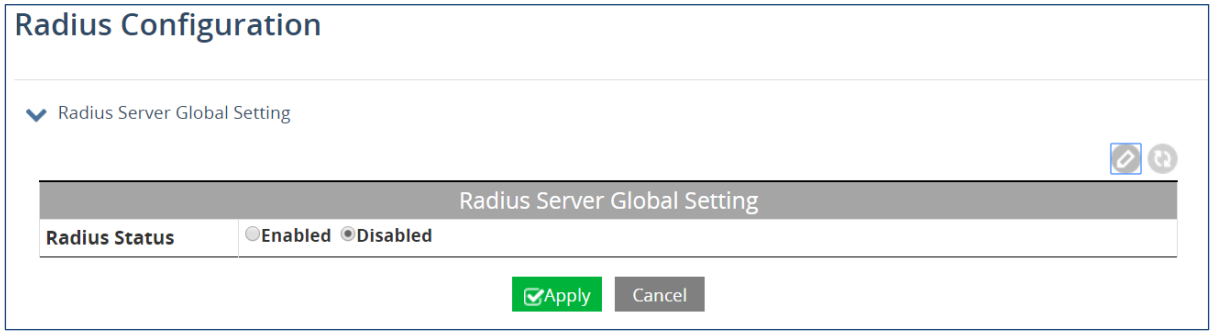
Daylight Saving Time Setting	
Current DST Mode	disable
DST Timezone Name (3-6 chars)	
DST Offset (1-480 mins)	
DST Start Month	
Week	
Day	
Hour	
Minute	
DST End Month	
Week	
Day	
Hour	
Minute	

14 8021.X

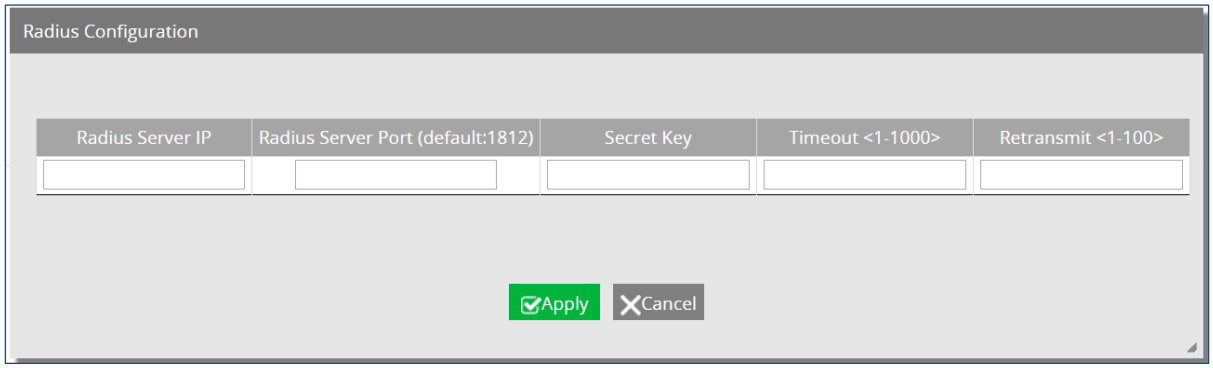
Radius Configuration

By default, the 802.1X function is globally disabled on the EtherWAN switch. If you want to use the 802.1X port based security on a port, you must enable it globally on the switch first, and then enable it on a per port basis.

To enable Radius globally, click the edit icon on the first panel, and click the radio button next to **enabled**. Then click “Apply.”



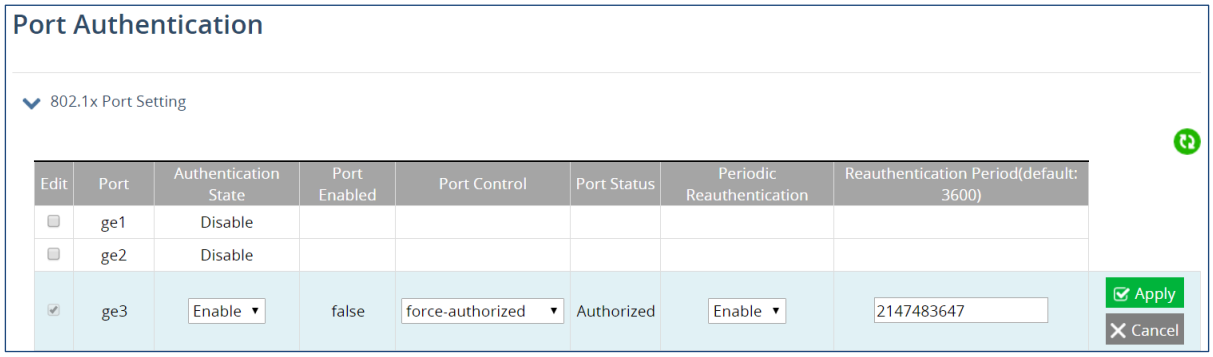
To add a Radius server, click the add icon in the second panel. Enter the **Radius Server IP address**, **Radius Server Port**, **Secret Key**, **Timeout**, and **Retransmit** values.



Port Authentication

Click the check box next to the port for which you want to configure Radius, and set the Authentication state to **enable**. Set the Port control feature to **auto** (enables 802.1X authentication, port starts in unauthorized state), **force-authorized** (disables 802.1X authentication, port transitions to the authorized state without authentication), or **force-unauthorized** (port stays in unauthorized state, and ignores authentication attempts).

Enable **Periodic Reauthentication** if needed. If Periodic Reauthentication is enabled, enter a value for the interval (in seconds) between reauthorization attempts. Click “Apply” when finished.

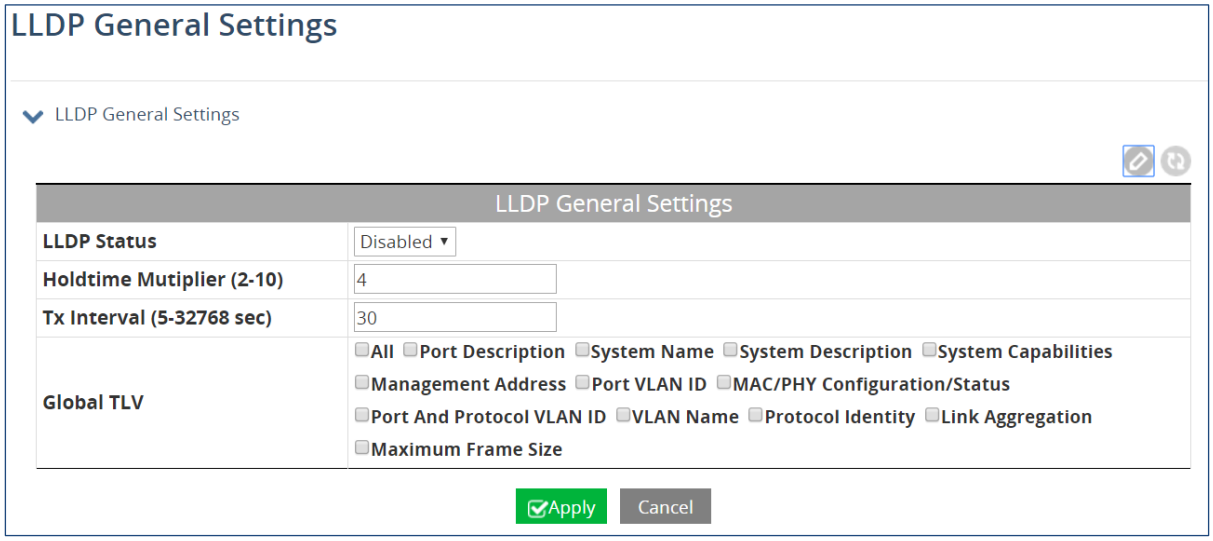


15 LLDP

The Link Layer Discovery Protocol (LLDP) allows network devices to advertise their identity, capabilities, and neighbors on a local network.

LLDP General Settings

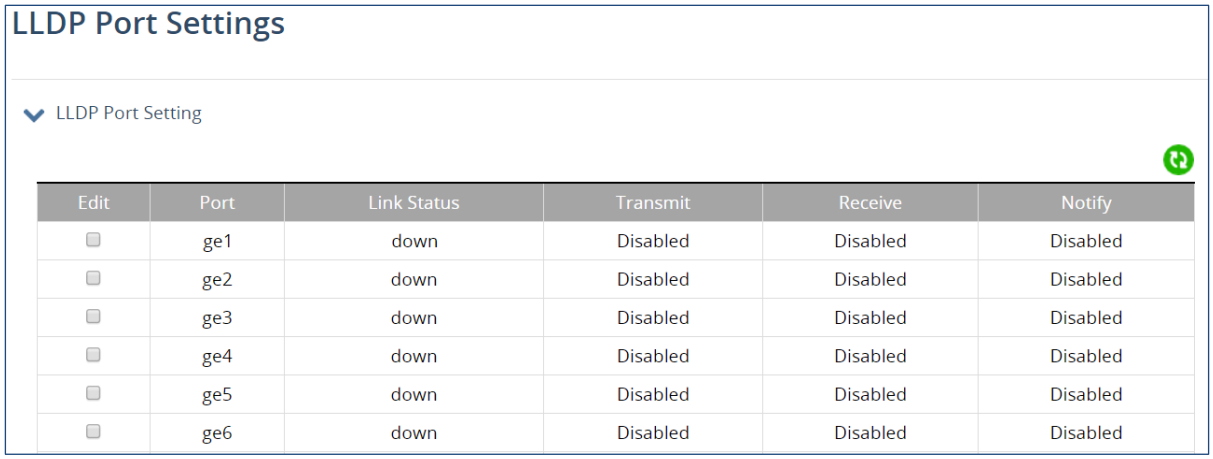
To enable LLDP, click the edit icon on the first panel, and select **enabled** from the drop-down menu. Enter a value for the **Holdtime Multiplier**, which is used to compute the actual time-to-live (TTL) value used in an LLDP frame. Then enter the **TX Interval**, which adjusts the time that LLDP information is transmitted by the switch. Finally, select items that will be advertised in the **Global TLV** (Time – Length – Value) by clicking in the corresponding check boxes. Click “Apply” when finished.



LLDP Port Settings

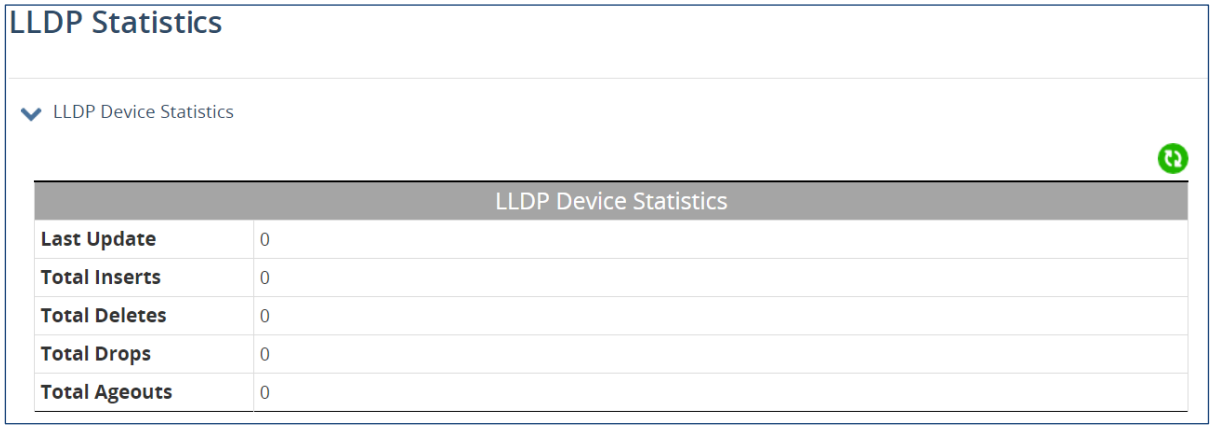
LLDP Ports Settings allows the individual ports on the switch to be configured for LLDP independently of one another. Each port can be configured to transmit LLDP information, receive LLDP information, and notify (via SNMP or Syslog) if there are changes in the LLDP information received from neighboring devices.

Click the check box next to the port for which LLDP is to be configured. Select enabled or disabled for the **Transmit**, **Receive**, and **Notify** fields.

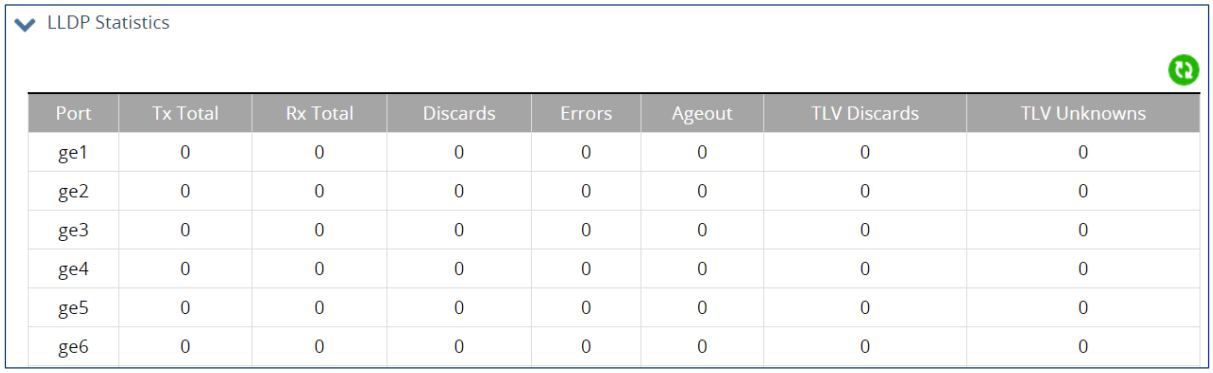


LLDP Statistics

The top panel of the LLDP Statistics screen is LLDP Device Statistics, a read-only panel that shows total values for **Last Update**, **Total Inserts**, **Total Deletes**, **Total Drops**, and **Total Ageouts**.

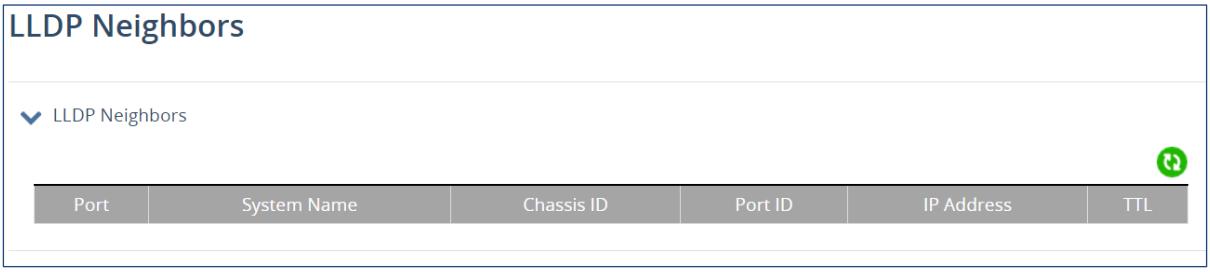


The second panel shows LLDP statistics per port, including **Tx Total**, **Rx Total**, **Discards**, **Errors**, **Ageout**, **TLV Discards**, and **TLV Unknowns**.



LLDP Neighbors

LLDP Neighbors is a read-only page (see Figure 108) that will display all the LLDP capable devices detected by the switch. The following information about connected LLDP-enabled devices is displayed in a tabular format. The columns displayed are: **Port**, **Chassis ID**, **Port ID**, **IP Address**, and **TTL** (Time to Live).



16 Routing

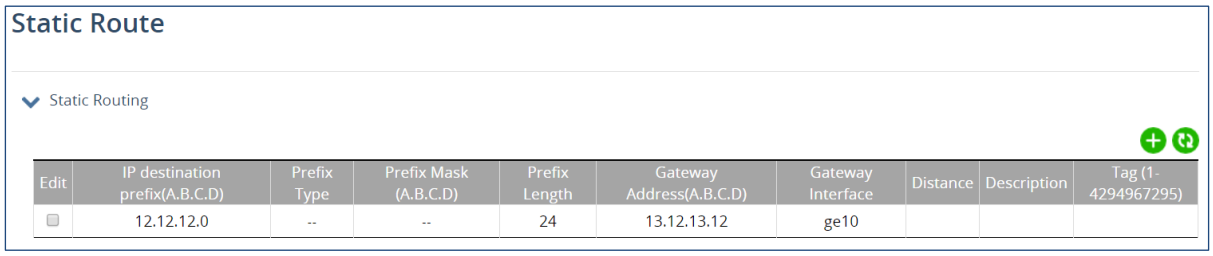
Static Route

Static routes are created by specifying the next hop to which the switch forwards data for a specific subnet. Configured static routes will be added to the routing table database and stored in the switch.

To add a new static route, click the add icon, and then enter values for the following fields:

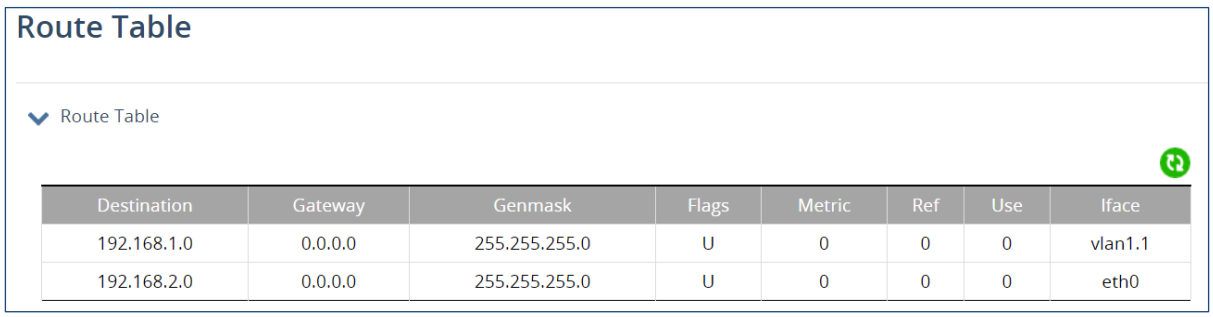
IP destination prefix (A.B.C.D) — Subnet IP destination prefix
Prefix Type — *Mask* or *Length,* corresponding field type below appears based on selection.
Prefix Mask— A.B.C.D format, if Prefix Type is Mask
Prefix Length — 0 - 32
Gateway Address — A.B.C.D format
Gateway Interface — Gateway nexthop interface name
Distance — 1 – 255, Administrative Distance
Description — Description of the static route
Tag — Range is 1-4294967295, Tag used as a "match" value to control redistribution via route maps

Click "Apply" when finished. Existing routes can be edited by clicking the checkbox next to the IP destination prefix on the left.



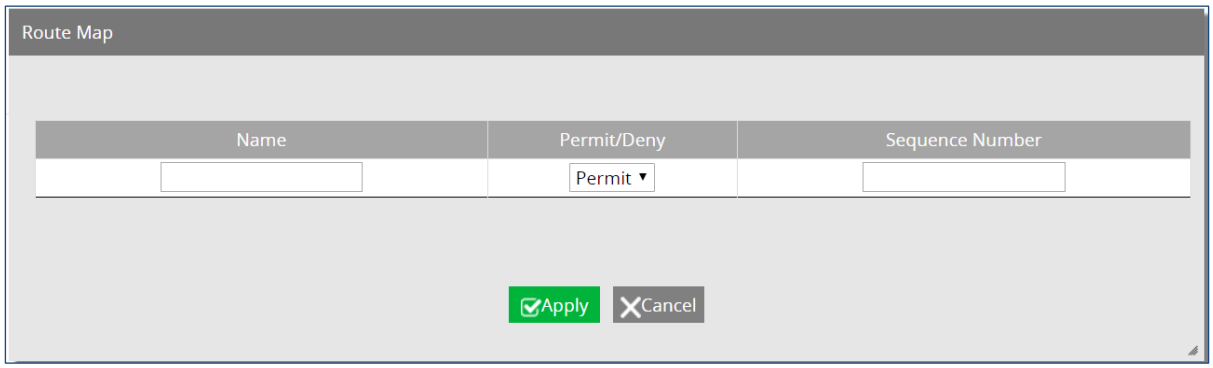
Route Table

The routing table is a read-only screen that shows existing routes.

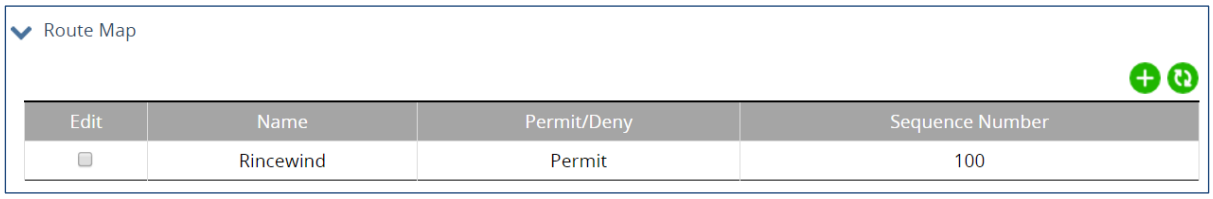


Route Map

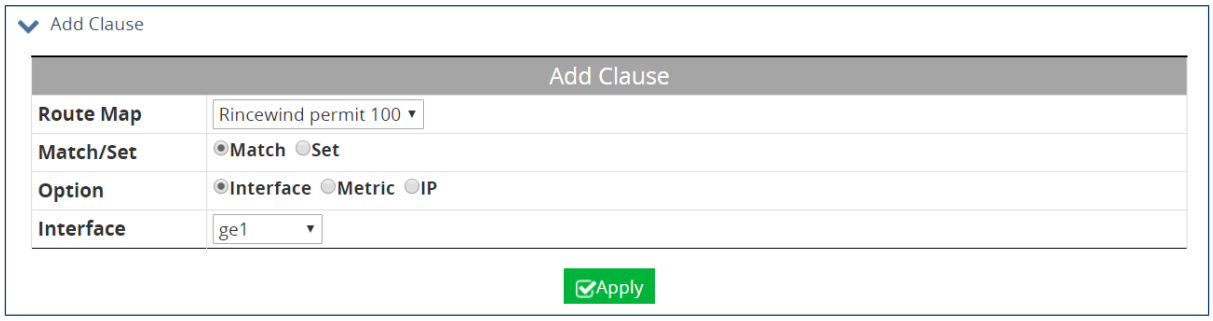
Route Maps can be used for both redistribution and policy routing. To create a route map, click the add icon. Enter the **name** of the route map, the type (**Permit** or **Deny**), and the sequence number (Sequence to insert to or delete from an existing route-map entry. Then click “Apply.”



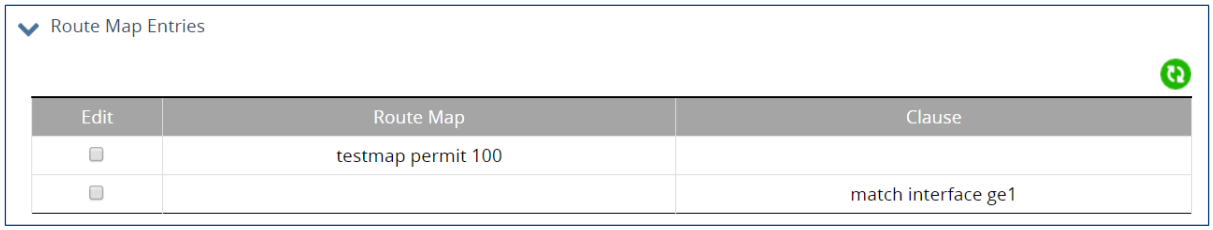
Existing route maps can be deleted by clicking the corresponding check box and clicking “Delete.”



Add match Clauses in the second panel. These are the conditions that must be met in order for a route map to redistribute from one routing protocol to another.



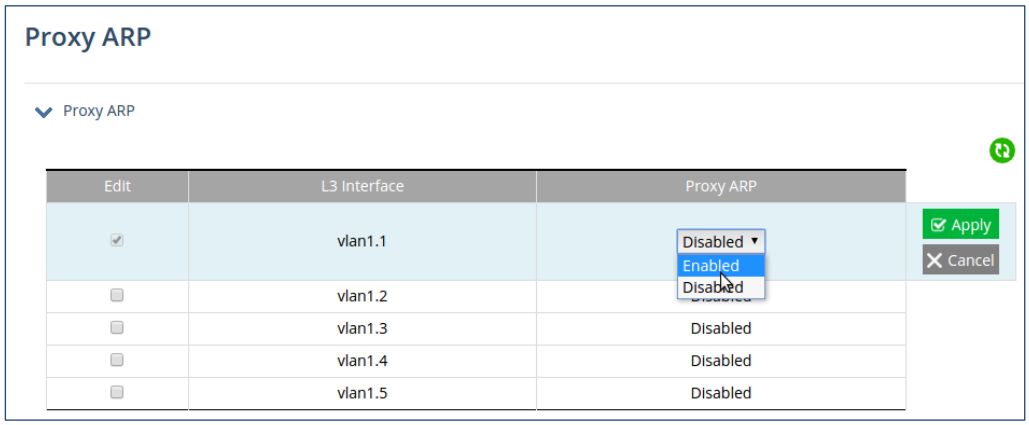
The Route Map Entries panel is a read-only panel that shows configured Route Maps.



Proxy ARP

Proxy ARP allows the switch to answer ARP queries for a network address that is not on that network. The ARP Proxy is aware of the location of the traffic's destination, and offers its own MAC address as the (seemingly) final destination. The "captured" traffic is then typically routed by the Proxy to the intended destination via another interface or via a tunnel.

To enable Proxy ARP, select an interface or VLAN by clicking the check box at the left. Select enable, and then click “Apply.”



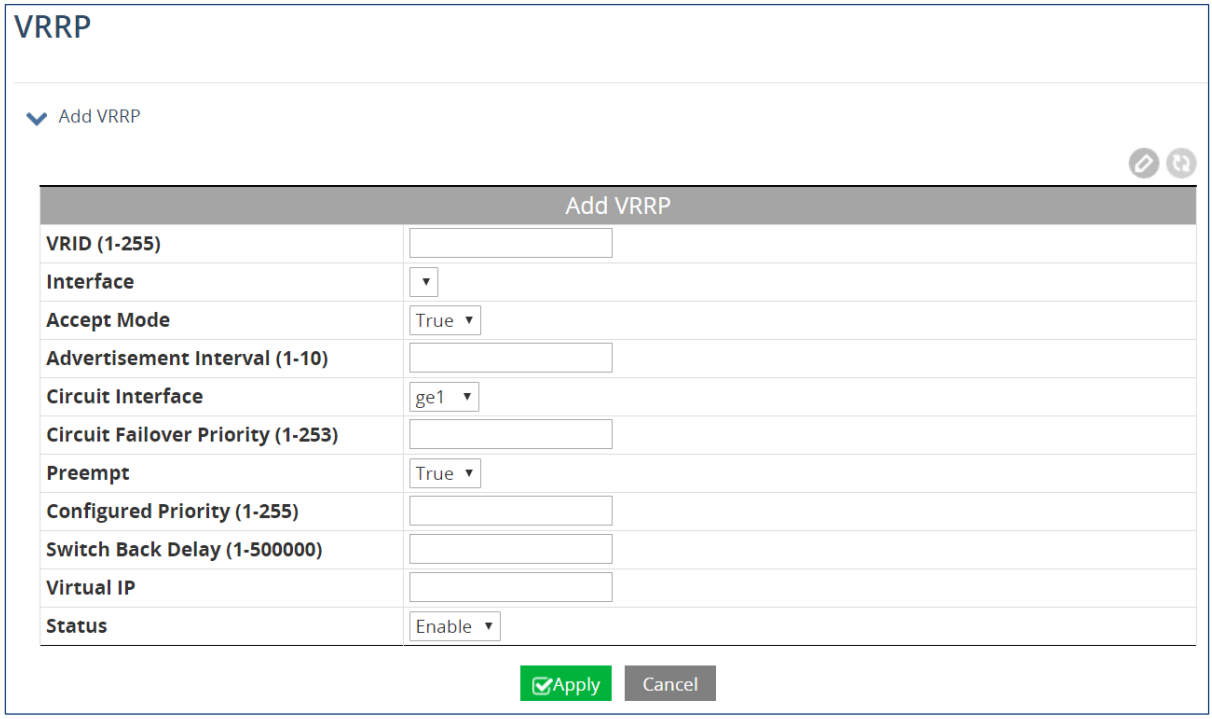
VRRP

VRRP (Virtual Router Redundancy Protocol) is a distance-vector routing protocol that uses hop count as a routing metric. VRRP eliminates the risk of a single point of failure inherent in a static default routing environment. It specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. One of the major advantages of VRRP is that it makes default path available without requiring configuration of dynamic routing on every end-host.

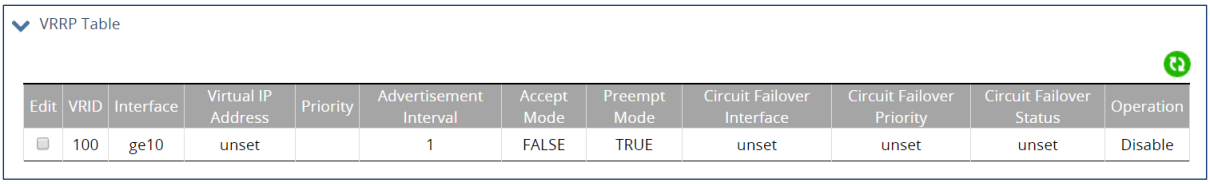
To configure VRRP:

- Click the edit icon.

- Enter a Virtual Router Identifier (VRID), from 1 – 255.
- Select the physical interface or VLAN that will be used for virtual routing.
- Set **Accept Mode** to true or false. Accept Mode allows the switch to respond to pings (ICMP EchoRequests) sent to the VRRP virtual IP address.
- Set the **Advertisement Interval** (the rate at which the Master router sends advertisement packets to all members of the VRRP group) in seconds. Range is from 1 – 10. These packets indicate that the master router is still operational.
- Select the circuit interface to be used for circuit failover.
- Set the **Circuit Failover Priority**. This is the value by which the virtual router decrements its priority value during a circuit failover event. Configure this value to be greater than the difference of priorities between the master and backup routers.
- Set the **Preempt Mode** to True or False. If true, this specifies that the router with the highest priority will function as a backup to the Master router when master is unavailable.
- Set the priority. If you are configuring the master router, set this value to 255. For other VRRP routers, use a value from 1 - 254. If the master router fails, the router with the highest priority will become the new master.
- Set the **Switch Back Delay** for the timer for the master VRRP router.
- Enter the virtual IP address for the VRRP session.
- Set the status to enable.
- Click the “Apply” button.



Details of existing instances of VRRP can be viewed in the VRRP table at the bottom of the screen.


VRRP Table
Edit
VRID
Interface
Virtual IP Address
Priority
Advertisement Interval
Accept Mode
Preempt Mode
Circuit Failover Interface
Circuit Failover Priority
Circuit Failover Status
Operation
100
ge10
unset
1
FALSE
TRUE
unset
unset
unset
Disable

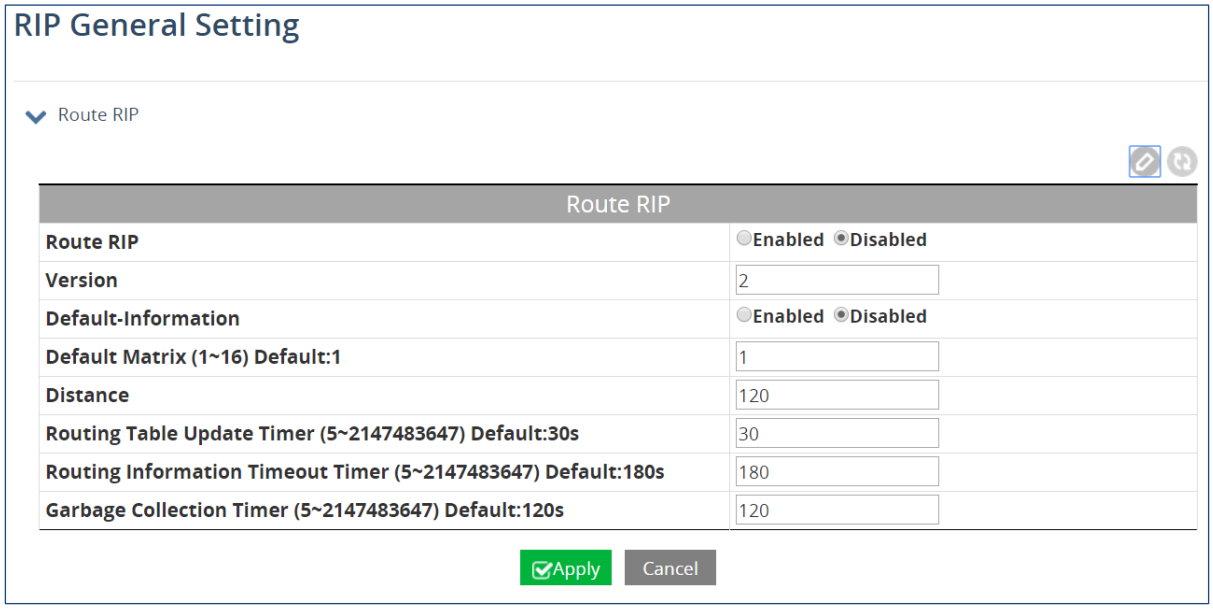
17 RIP

RIP General Setting

The Routing Information Protocol (RIP) is a distance-vector routing protocol that uses hop count as a routing metric. RIP prevents routing loops by setting a limit on the number of hops allowed in a path from source to destination.

To enable and configure RIP on the managed switch:

- Click the edit icon.
- Set the Router RIP field to **Enable**.
- Choose RIP version 1 or 2.
- Enable/disable **Default Information** to distribute default routes.
- Set the **Default Matrix** value in the range of 1 to 16.
- Set the Distance from 1 to 255 (Default value is 120)
- Set the timings for the **Routing Table Update Timer**, the **Routing Information Timeout Timer**, and the **Garbage Collection Timer** (Default values are 30, 180, and 120 seconds respectively).
- Click “Apply”.

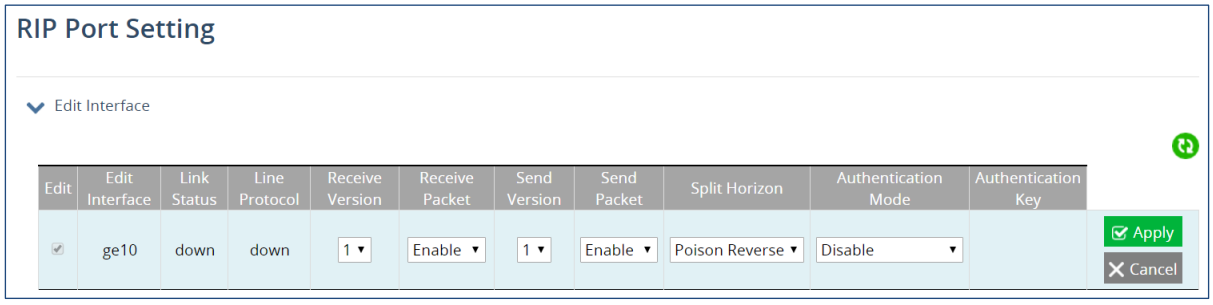


RIP Port Setting

In order for a port to be displayed on this screen, the interface must first be added on the RIP Network by Interface panel. To configure RIP port settings:

1. Select the interface by clicking the corresponding check box.
2. Set the RIP receive version (1, 2, or both)
3. Set Receive packets to enable or disable.

4. Set the Send Version to 1 or 2.
5. Set Send Packet to Enable or Disable.
6. For the Split Horizon Field, select enable, disable, or poison reverse.
7. Set the Authentication Mode to **disable**, **MD5**, or **simple password**.
8. If the Authentication Mode is MD5 or Simple Password, set the Authentication Key (1 – 16 characters).
9. Click “Apply.”



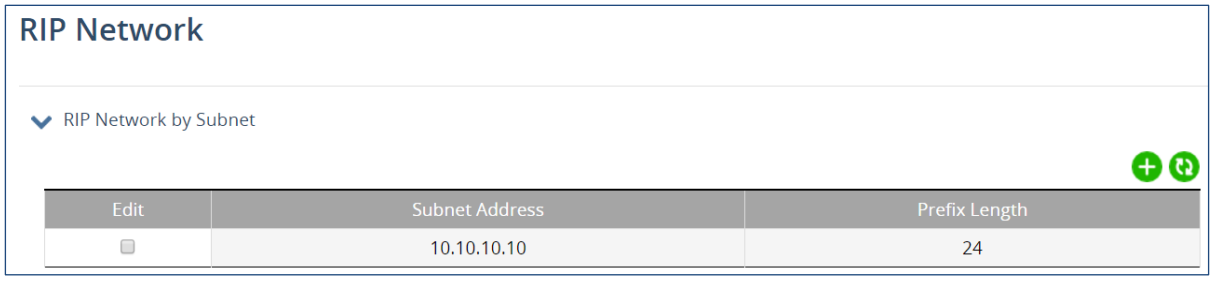
RIP Route

The RIP route table is a read-only page that shows existing RIP routes. The Routing Table fields are:

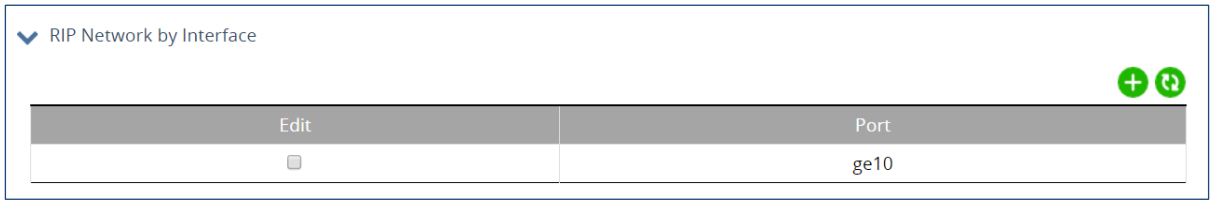
- **Route Code** – (R)ip, (K)ernel, (C)onnected, (S)tatic
- **Network** – IP address of destination network
- **Next Hop** – Next closest router or Layer 3 switch towards destination
- **Metric** – Number of hops
- **From** – IP address of source router
- **I/F** – Interface
- **Time** – Duration of time since last update

RIP Network

On the RIP Network screen, you can add or delete subnet addresses and interfaces to be advertised by RIP. To add a subnet, click the add icon in the top panel, and enter the subnet address and prefix length. Then click “Apply.”

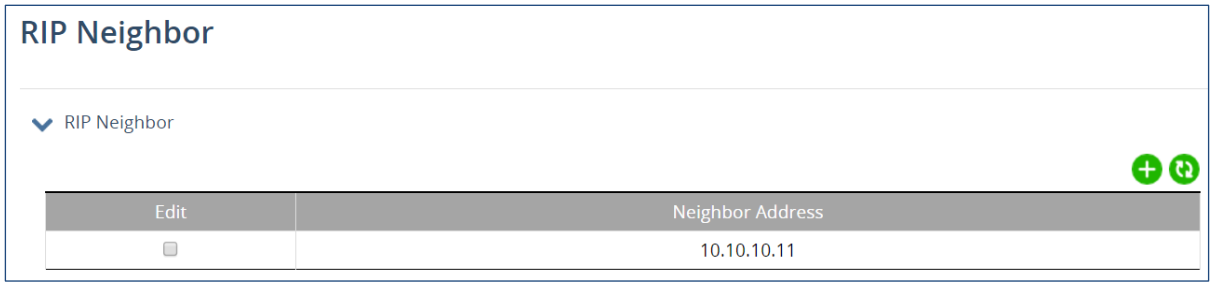


To add an interface, click the add icon, select the interface from the drop-down list, and then click “Apply.”



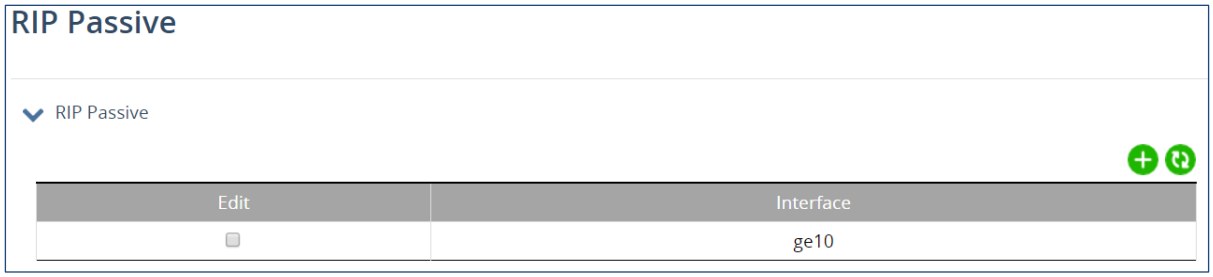
RIP Neighbor

The RIP Neighbor screen is used to add/delete RIP neighbor IP addresses. To add a neighbor, click the add icon and then add the IP address of the neighboring router or Layer 3 switch, and click “Apply.” Select existing neighbors from the list and click “Delete” to remove them.



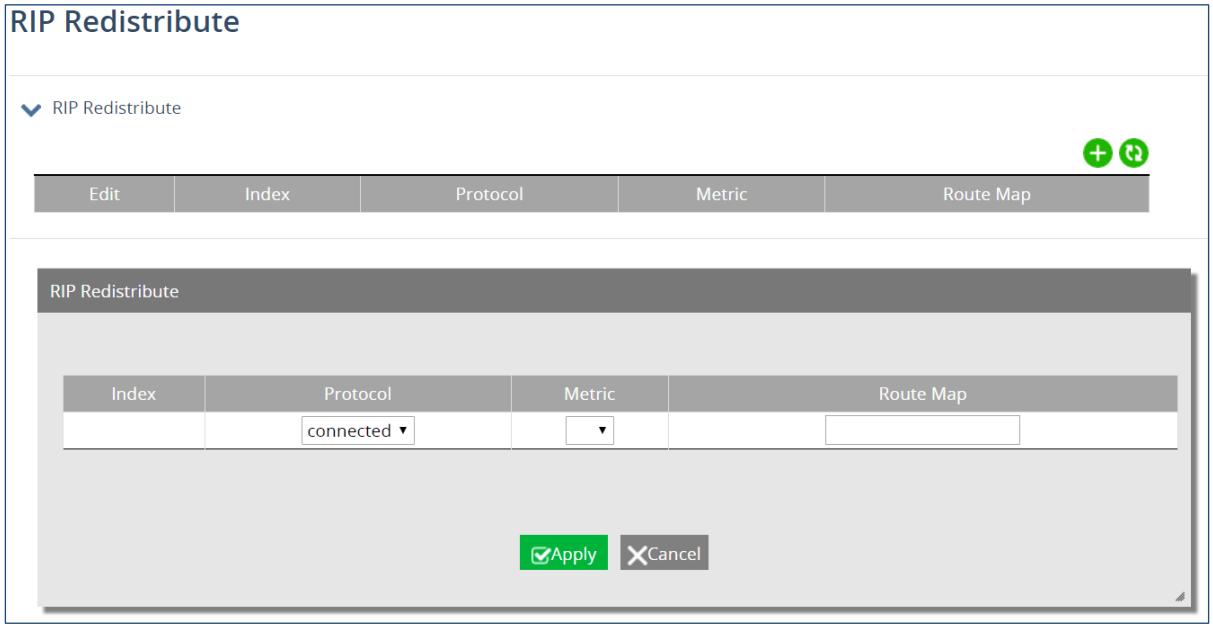
RIP Passive

On the RIP Passive screen, you can select an interface to be “passive,” that is, to prevent the RIP routing process from sending multicast/broadcast updates on that interface. Click the add icon, select the desired interface from the drop-down menu, then click “Apply” to make that interface passive. You can select and delete passive interfaces from the Passive Interface List by clicking the check box next to the interface and then clicking “Delete.” Doing so will return that interface to sending multicast/broadcast updates normally.



RIP Redistribute

Redistribution is using a routing protocol to advertise routes that have been learned by another routing protocol, static routes, or directly connected routes. To add an item to the redistribute list, select the protocol (**connected** or **static**), a route map that has been previously defined, and the desired metric, then click the “Apply” button.



18 SNMP

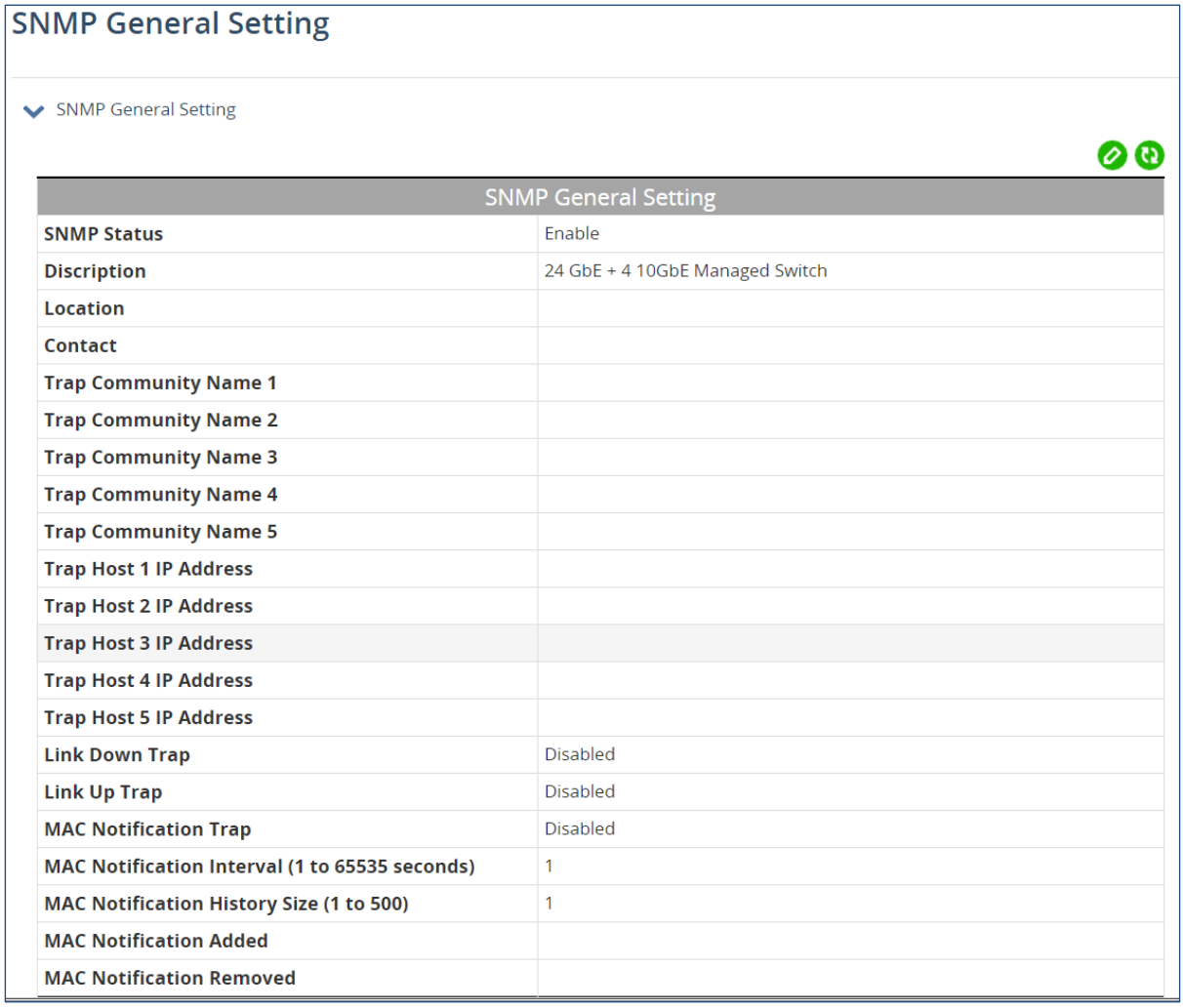
SNMP General Setting

SNMP is a TCP/IP application layer network management protocol that allows any TCP/IP device to be managed across a TCP/IP network. It is based on the client-server paradigm. The server (called a SNMP Agent) runs a process on the managed device that listens for a client's NMS (Network Management Station) polling requests to fetch or set a data item on the managed device. The SNMP Agent can also send alert messages (called Traps) to an NMS automatically, based on the occurrence of certain events on the device that the Agent resides.

To configure SNMP general settings, click the edit icon, and enter values for the following fields:

1. Set the SNMP Status to **enable**.
2. Enter a short description (up to 256 characters) into the **Description** field.
3. Enter a name into the entry field next to **Location**.
4. Enter a name (up to 256 characters) into the entry field next to **Contact**.
5. Enter a trap community name (up to 256 characters) into any of the fields next to Trap Community Name 1 – 5. Community names identify the SNMP Trap community group that the traps on this switch should be sending to. The identical Trap community names should also be set on the NMS hosts that will be receiving the traps. Each name defined corresponds with the **Trap host IP address** fields with the same number below.
6. Enter an IP address for the NMS host(s) that should be receiving traps from this switch, into the fields next to any of the 5 **Trap Host IP Address** fields.
7. Enable or disable the **Link Down Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups when any port on the switch moves from the link up state to the link down state.
8. Enable or disable the **Link Up Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups when any port on the switch moves from the link down state to the link up state.
9. Enable or disable the **MAC Notification Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups anytime there is a change in the MAC table on certain selected ports of the switch.
10. Set the interval between the MAC notification traps that you want the switch to send by entering the interval (in number of seconds from 1 to 65535) into the entry field next to **MAC Notification Interval (1 to 65535 seconds)**.
11. Set the size of the MAC notification history table by entering the total number of records (from 1 to 500) that the switch will keep for user to review at any one time into the entry field next to **MAC Notification History Size (1 to 500)**.
12. Select which ports on the switch for which traps should be sent when there is a new MAC address added to the MAC table for the port, by checking the corresponding check boxes for these ports in the **MAC Notification Added** section.
13. Select which ports on the switch for which traps should be sent when there is a MAC address being removed from the MAC table for the port, by checking the corresponding check boxes for these ports in the **MAC Notification Removed** section.

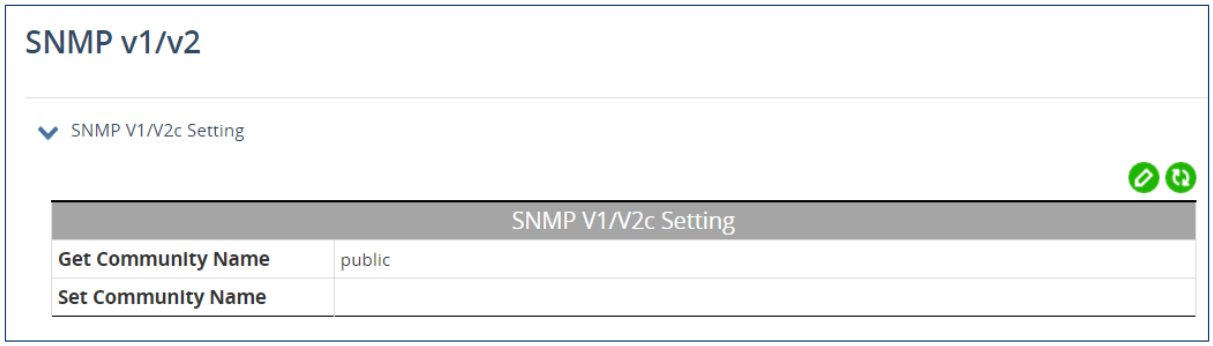
14. Click the “Apply” button when finished.
15. Save the configuration.



SNMP General Setting	
SNMP Status	Enable
Discription	24 GbE + 4 10GbE Managed Switch
Location	
Contact	
Trap Community Name 1	
Trap Community Name 2	
Trap Community Name 3	
Trap Community Name 4	
Trap Community Name 5	
Trap Host 1 IP Address	
Trap Host 2 IP Address	
Trap Host 3 IP Address	
Trap Host 4 IP Address	
Trap Host 5 IP Address	
Link Down Trap	Disabled
Link Up Trap	Disabled
MAC Notification Trap	Disabled
MAC Notification Interval (1 to 65535 seconds)	1
MAC Notification History Size (1 to 500)	1
MAC Notification Added	
MAC Notification Removed	

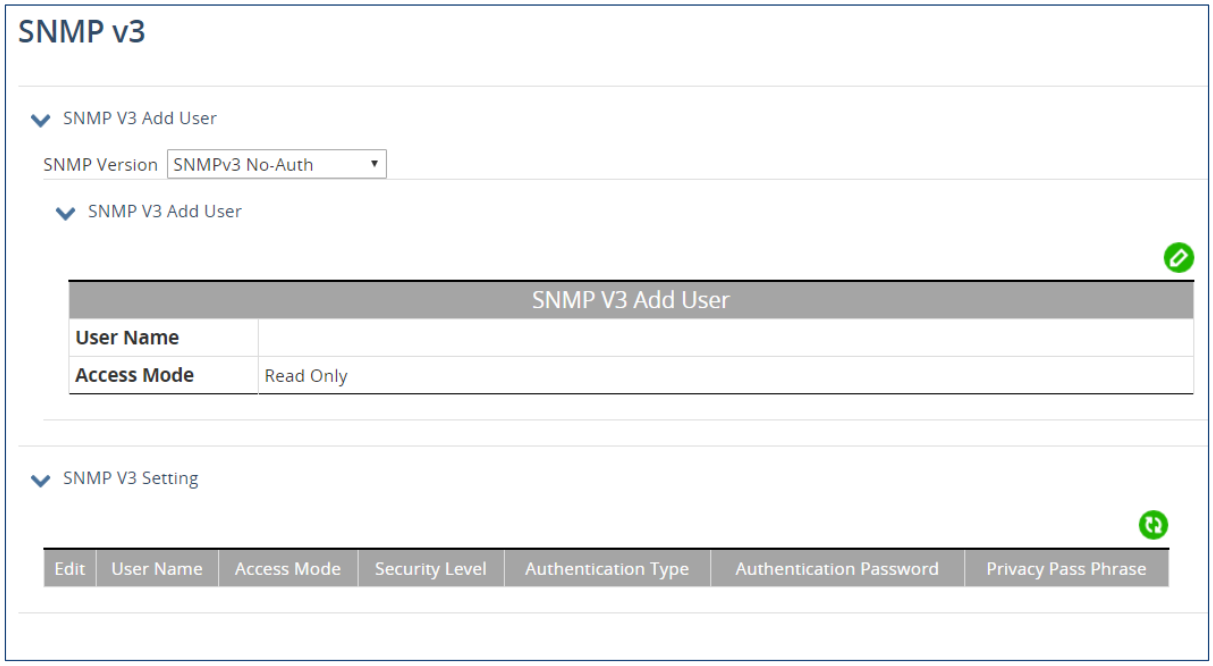
SNMP v1/v2

Click the edit icon and enter the SNMP community name into the **Get Community Name** field. This will allow the NMS to poll status information from the switch (read only). Then enter the SNMP community name, into the **Set Community Name** field. This will allow a NMS to change the status of a data item in the switch.



SNMP v3

The top panel of this screen is SNMP v3 Add User. To add a user, click the edit icon, and then enter the user name. Set the Access mode to **Read Only** or **Read/Write**. Then click “Apply.”



19 OSPF

OSPF General Setting

OSPF (Open Shortest Path First) is a link state routing protocol. It is a classless protocol with support for VLSM and CIDR, manual route summarization, incremental updates, and equal cost load balancing. OSPF uses only the interface cost as its metric. The administrative distance default value is 110. OSPF uses multicast addresses 224.0.0.5 and 224.0.0.6 for routing updates.

Devices running OSPF establish neighbor relationships, and then exchange routes. Instead of exchanging routing tables, devices exchange information about known network topologies. Each OSFP enabled device then calculates best routes and adds them to the routing table.

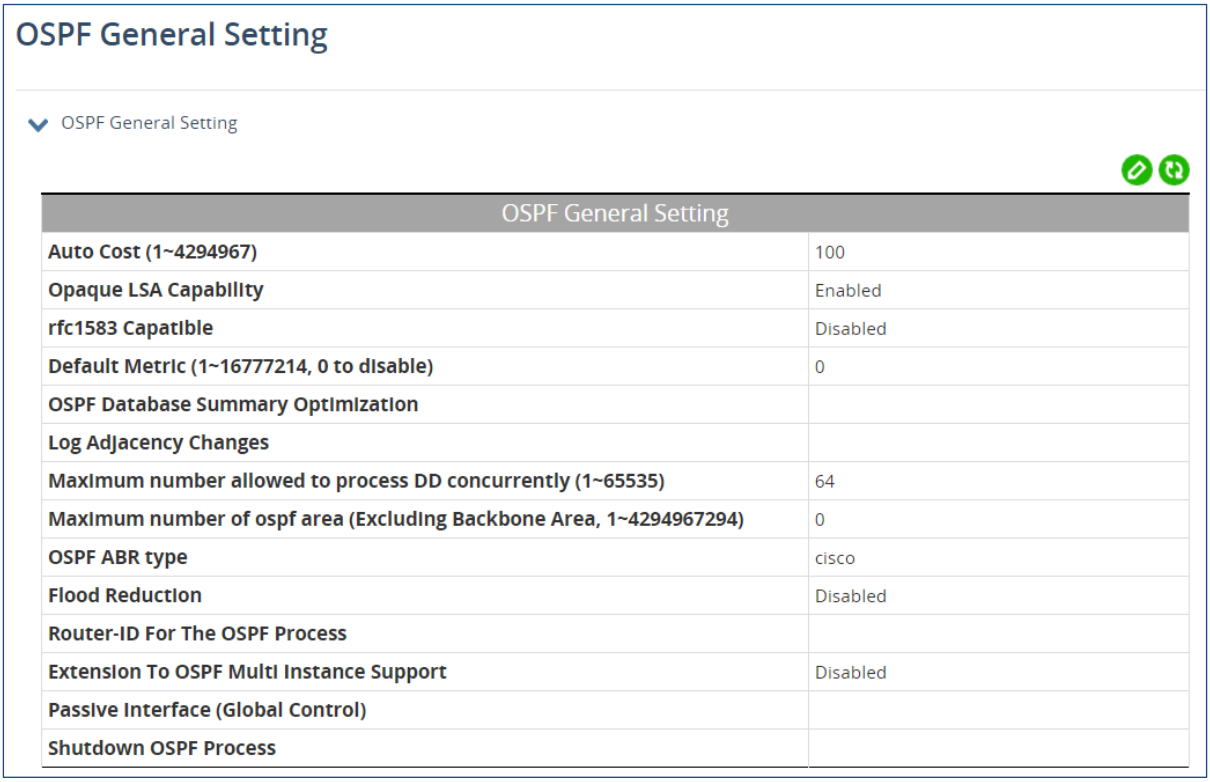
The following fields must be the same on both OSPF-enabled devices in order for them to become neighbors:

- subnet
- area id
- hello and dead interval timers
- authentication
- area stub flag
- MTU

To enable and configure OSPF, click the edit icon in the first panel, and enter values for the following fields:

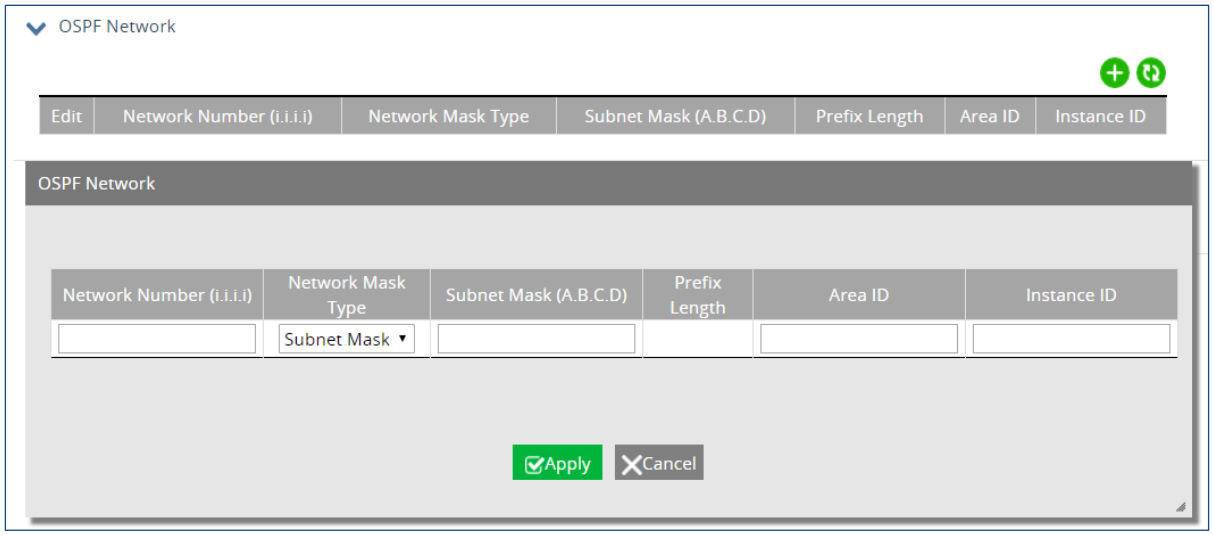
1. **Auto Cost**. **(1~4294967)** The auto-cost reference bandwidth, which controls how OSPF calculates the default metric for the interface.
2. **Opaque LSA Capability**. (enable/disable)
3. **RFC 1583 Compatibility**. (enable/disable) Setting this to enable will make the instance compatible with OSPFv2.
4. **Default Metric**. (1-16777214) A default metric facilitates redistributing routes with incompatible metrics. If the metrics do not convert, the default metric provides an alternative.
5. **OSPF Database Summary Optimization**. (enable/disable) When enabled, the database exchange process is optimized by removing the LSA from the database summary list for the neighbor, if the LSA instance in database summary list is the same as or less recent than the listed LSA in the database description packet received from the neighbor.
6. **Log Adjacency Changes**. (Log Adjacency Changes/Log Adjacency Changes-Detail)
7. **Maximum number allowed to process DD concurrently** (1~65535) Limits the number of Database Descriptors (DD) that can be processed concurrently.
8. **Maximum number of OSPF area** (Excluding Backbone Area, 1~4294967294)
9. **OSPF ABR type** (Cisco, IBM, shortcut, standard) OSPF Area Border Router (ABR) type.

10. **Flood reduction**. (enable/disable) When enabled, flood reduction reduces unnecessary refreshing and flooding of already known and unchanged information.
11. **Router-ID For The OSPF Process** (A.B.C.D)
12. **Extension to OSPF Multi Instance Support**. (enable/disable)
13. **Passive Interface (Global Control)**. (enable/disable)
14. **Shutdown OSPF Process**. (enable/disable)
15. Click “Apply” when finished.



The second panel is OSPF Network. Use this panel to enable OSPF routing with a specified area ID (and optionally an instance ID) on interfaces with IP addresses that match the specified network address.

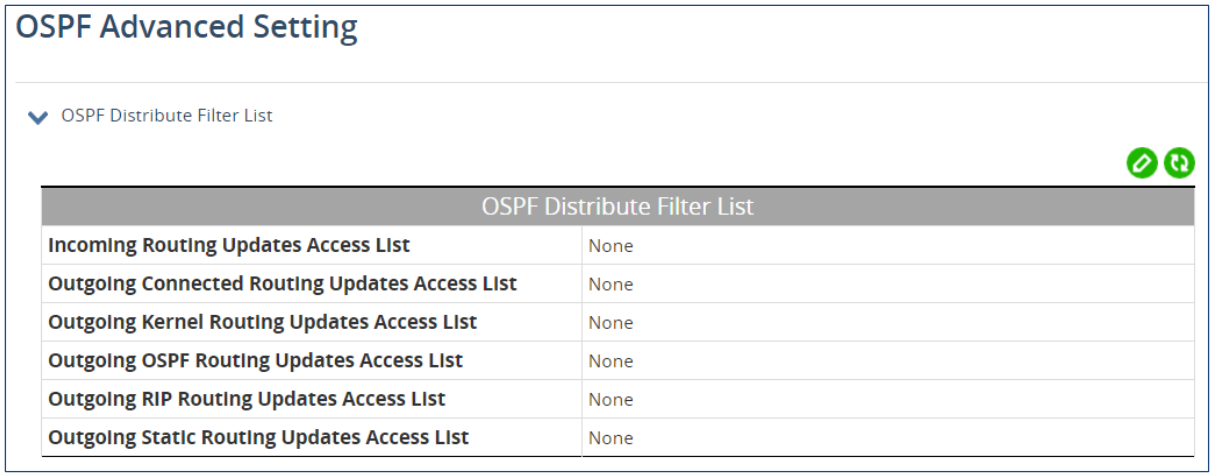
To add an OSPF network, click the add icon and enter the IPv4 network address. Select subnet mask or prefix length, and enter the value for the corresponding field that displays. Enter an **Area ID** from 0 – 4294967295, and an Instance ID from 1 – 255 (if running multiple instances of OSPF).



The final panel is for setting OSPF Timers, including Link State Advertisements (LSA), SPF Timers, and LSA Throttle Timers. Use the drop-down menu to select the timer type, and then click the edit icon in the panel displayed below.

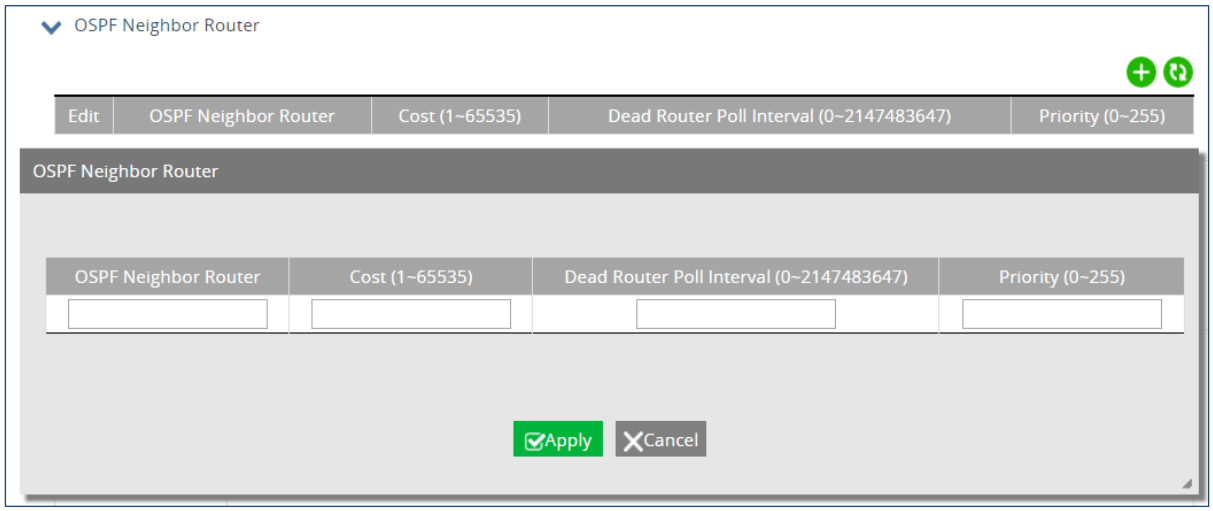
OSPF Advanced Setting

The top panel is for applying filters to networks in routing updates, redistributing other routing protocols into the OSPF routing table. Click the edit icon, and enter the name of the access to be applied next to the filter type.

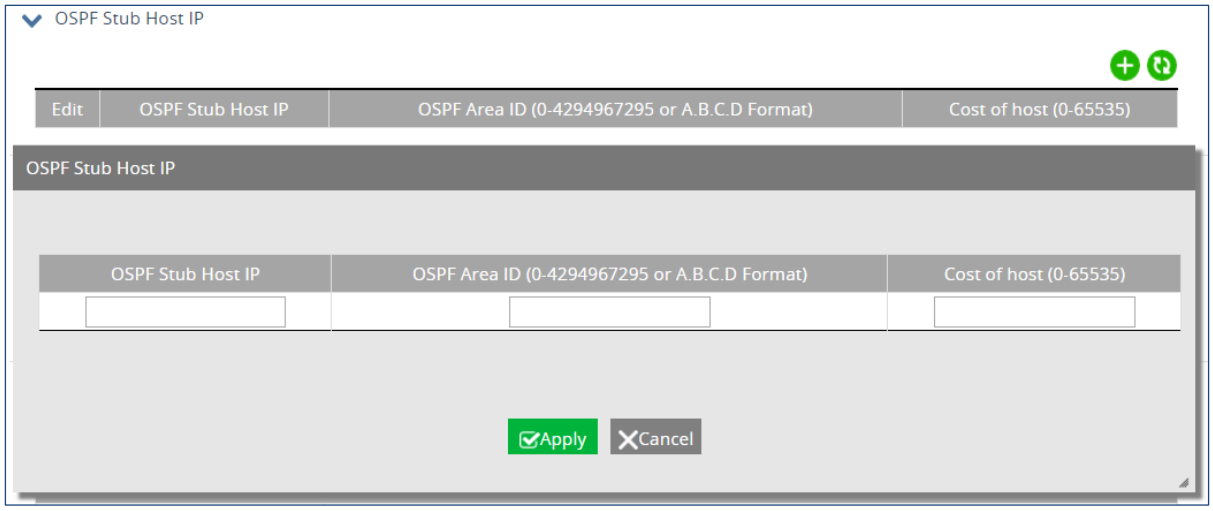


The second panel is OSPF neighbor, used to configure OSPF routers interconnecting to NBMA (Non-Broadcast Multi-Access) networks. Include one neighbor entry for each known non-broadcast network neighbor. Configure the neighbor address on the primary address of the interface.

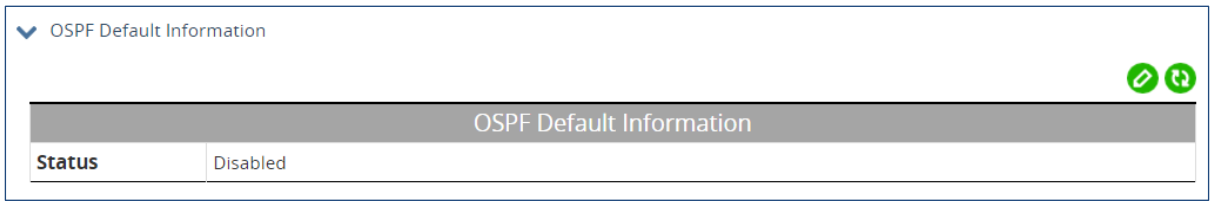
To add a neighbor router, click the add icon and enter the IP address of the neighbor in A.B.C.D format. Then enter the Cost (the Link-state metric to this neighbor), the Dead Router Poll Interval (the rate at which routers send hello packets when neighboring router is inactive, in seconds), and the priority.



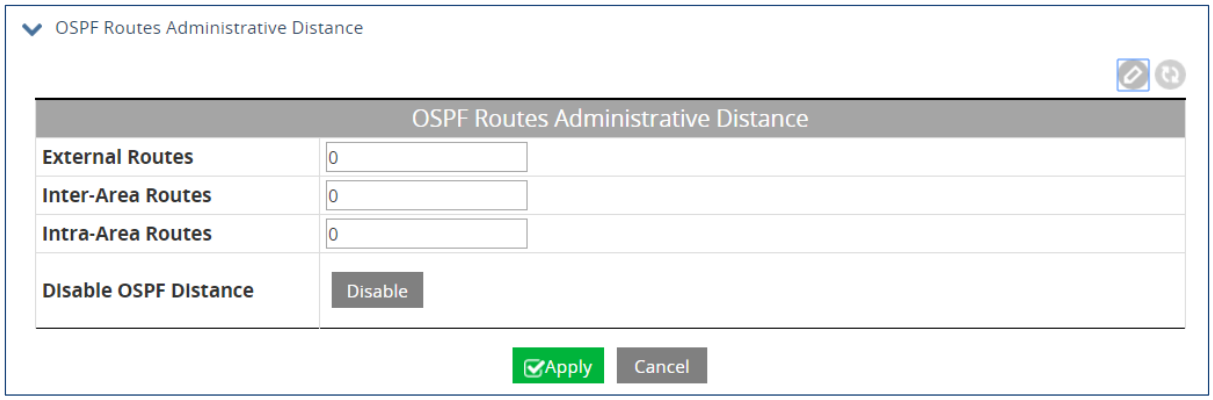
The third panel is OSPF Stub Host IP. Click the add icon, then enter the Stub Host IP address, the OSPF Area ID (0-4294967295 or A.B.C.D Format), and the Cost of host (0-65535). Click “Apply” when finished.



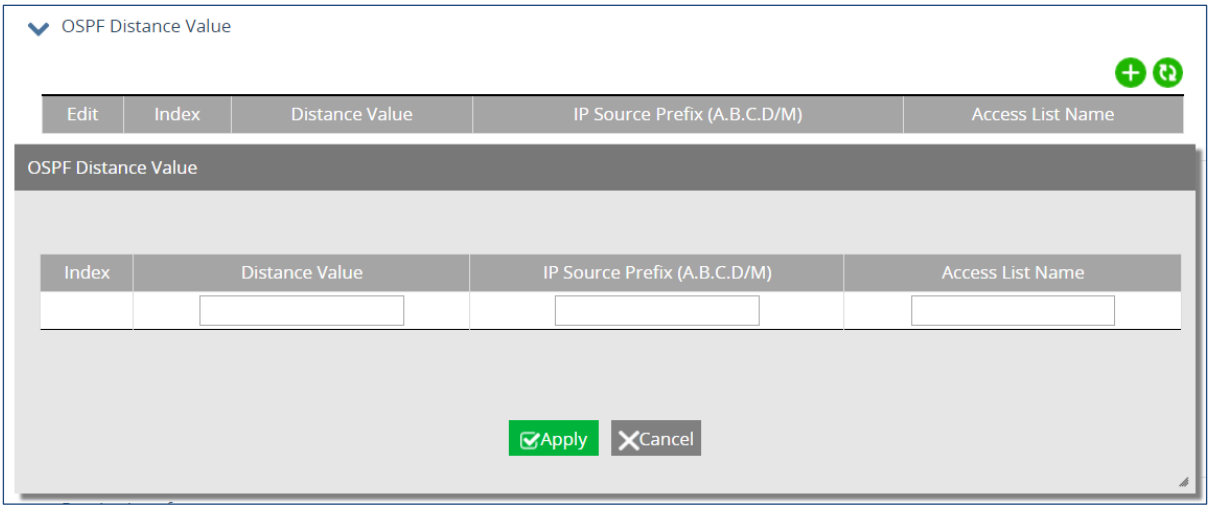
The fourth panel is OSPF Default Information. Use (enable) it to create a default external route into an OSPF routing domain.



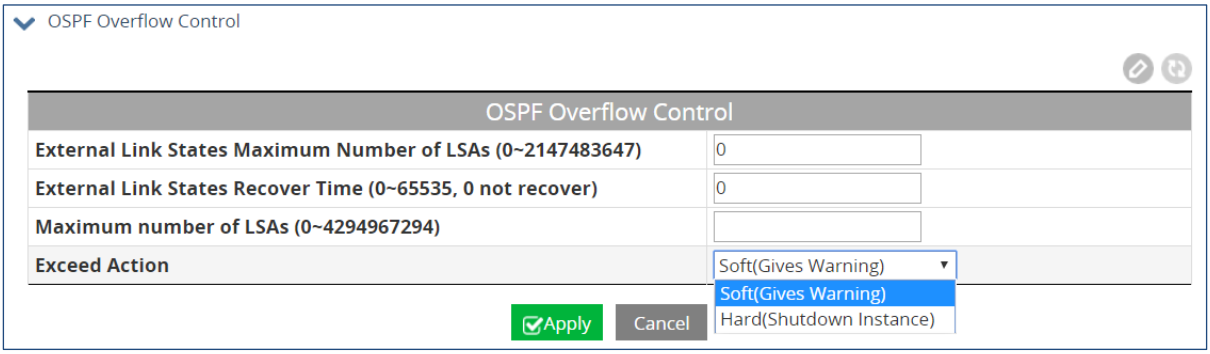
The fifth panel is used to set OSPF Routes Administrative Distance. The administrative distance rates the trustworthiness of a routing information source. A higher distance value means a lower trust rating.



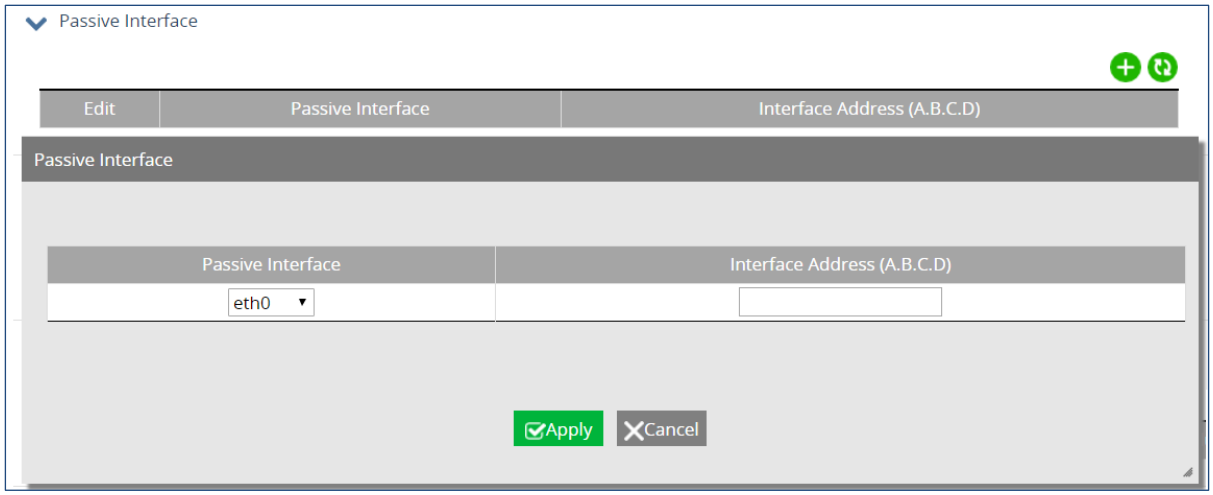
In the OSPF Distance panel, set administrative distances for access lists or next hop IP addresses. Click the add icon, and enter the distance value, the IP source prefix, and the access list name. Then click “Apply.”



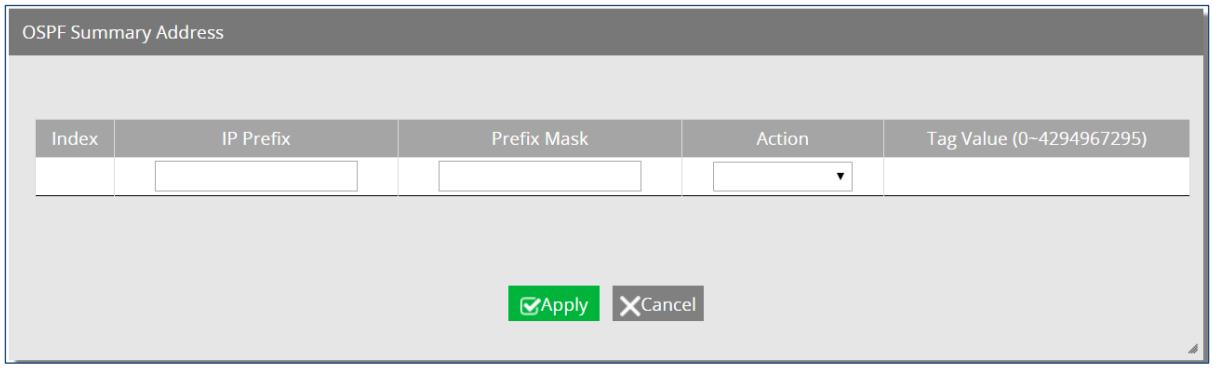
The OSPF Overflow Control Panel contains the settings for the maximum number of LSAs that can be supported by the OSPF instance.



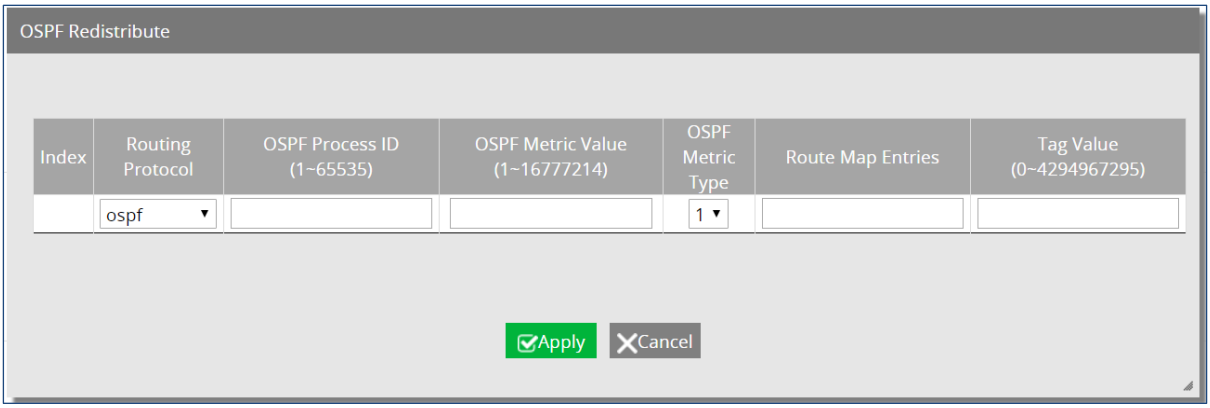
The seventh panel, OSPF Passive interface is used to suppress sending Hello packets on an interface. Click the add icon, and then enter the interface and the interface IP address. Then click “Apply.”



The OSPF Summary Address panel is used to summarize or suppress external routes with the specified address range. An address range is a pairing of a starting address and a mask that is almost the same as IP network number. Click the add icon, and enter the IP prefix, the Prefix Mask, the action (**not advertise** or **tag**), and the tag value. Then click “Apply.”



The final panel is OSPF Redistribute, for redistributing routes from a routing protocol, static route, and kernel route into an OSPF routing table. Click the add icon, and select the routing protocol (OSPF, connected, kernel, RIP, static route). Enter the OSPF Process ID, Metric Value, and Metric Type. Finally, specify the route map reference and the tag value. Click “Apply when finished.

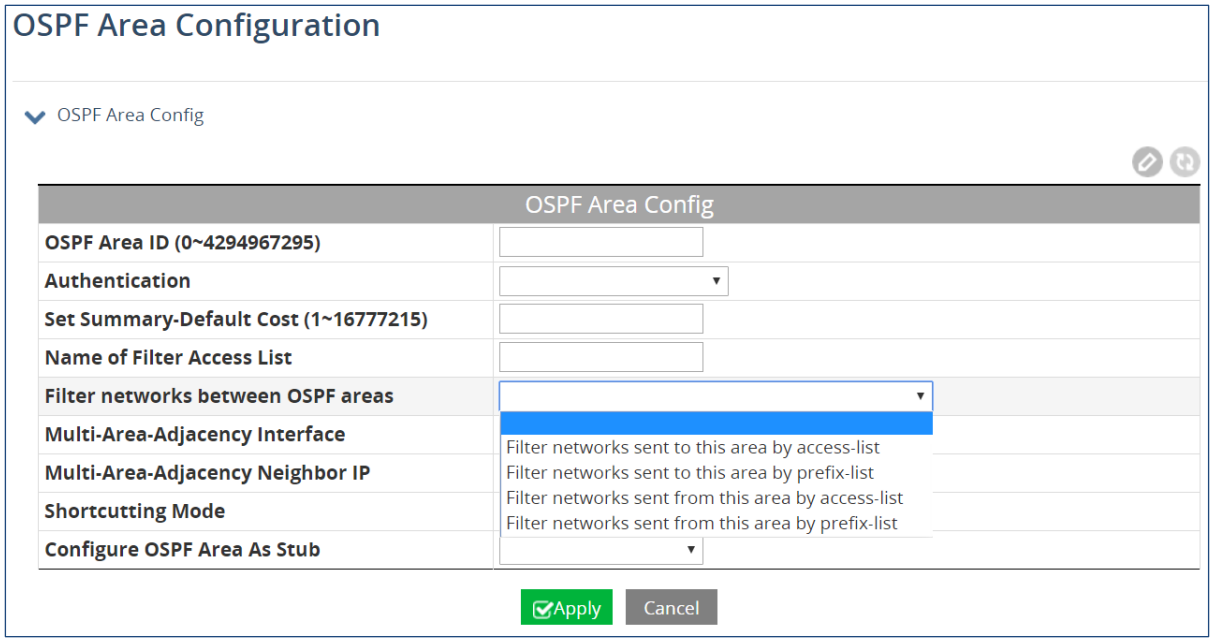


OSPF Area Configuration

The OSPF Area Configuration screen is comprised of five panels, the first of which is OSPF Area Config, used for defining areas and authentication. To add an area, click the edit icon and enter values for the following fields:

1. OSPF Area ID
2. Authentication
3. Set Summary-Default Cost
4. Name of Filter Access List
5. Filter networks between OSPF areas
6. Multi-Area-Adjacency Interface
7. Multi-Area-Adjacency Neighbor IP
8. Shortcutting Mode
9. Configure OSPF Area As Stub

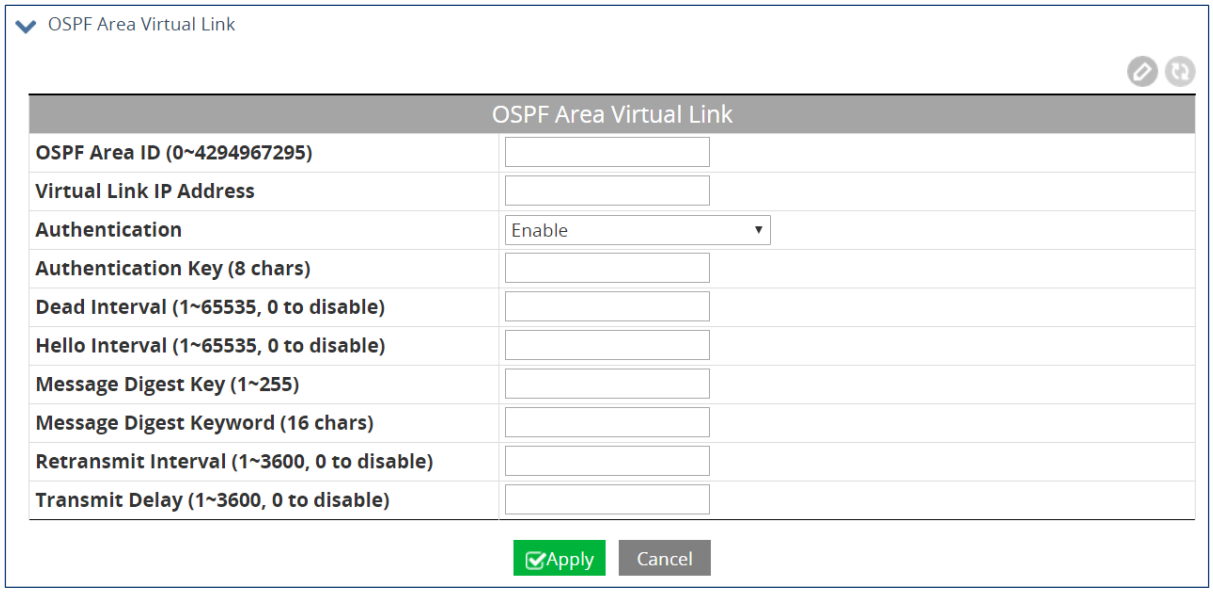
Click “Apply” when finished



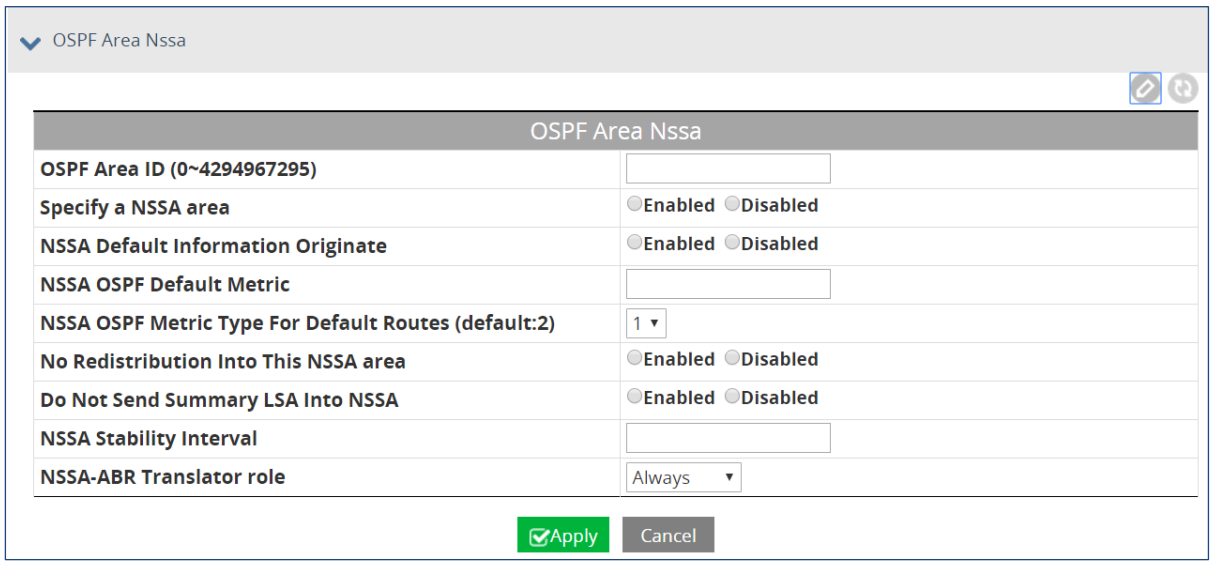
All OSPF areas must be connected to the backbone area 0. If this is not physically possible, a Virtual Link can be used. A virtual link is connects through another area that is connected to area 0. To create an OSPF Area Virtual Link, click the add icon in the second panel and enter values for the following fields:

1. OSPF Area ID
2. Virtual Link IP Address
3. Authentication
4. Authentication Key (8 chars)
5. Dead Interval
6. Hello Interval
7. Message Digest Key
8. Message Digest Keyword
9. Retransmit Interval
10. Transmit Delay

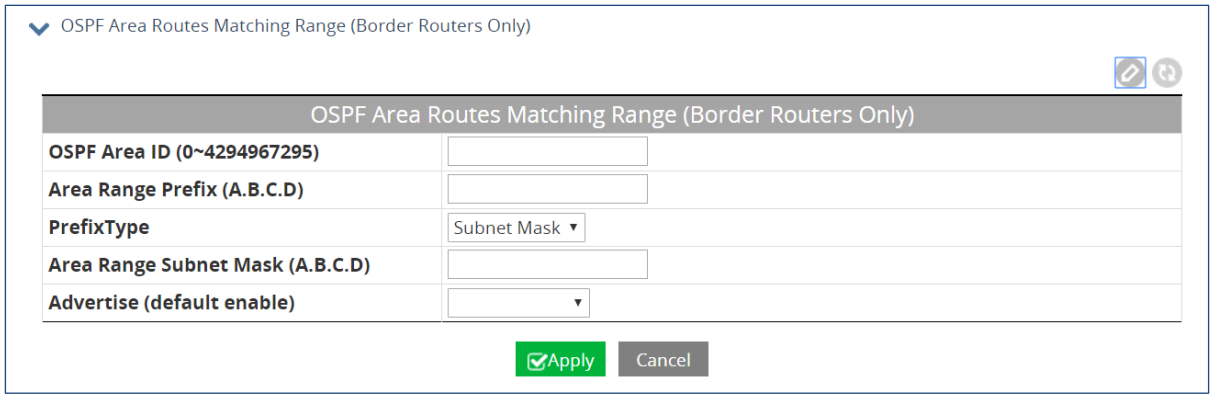
Click “Apply” when finished.



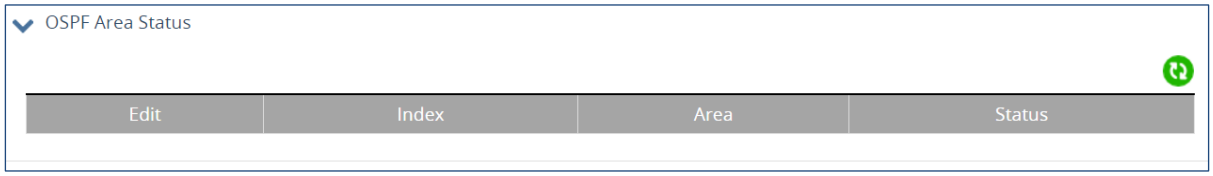
The third panel is for creating OSPF NSSA Areas. An NSSA (Not So Stubby Area) (NSSA) is an OSPF stub area that can also import external route information. External routes from other areas are not flooded into an NSSA, but route information from the NSSA is translated and flooded into other areas (like the backbone).



The OSPF Area Routes Matching Range panel allows OSPF routes to be summarized at an area boundary. A single summary route is then advertised to other areas by the Area Border Routers (ABRs). Routing information is condensed at area boundaries and outside the area.



The final panel is OSPF Area Status. It is read only, and displays the current Index, Area and Status of created OSPF areas.

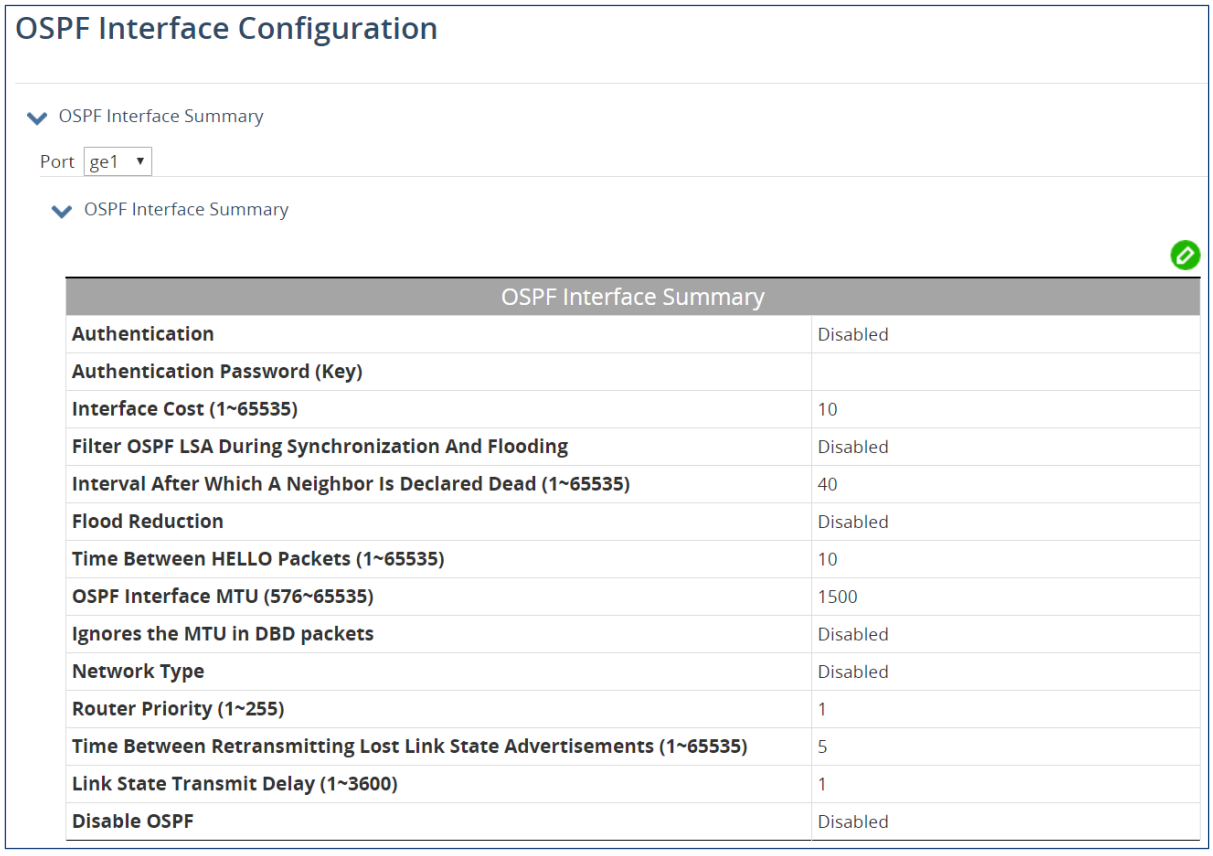


OSPF Interface Configuration

OSPF must be enabled on at least one interface in order to be activated on a network. Select the port from the drop-down menu in the upper left and then click the edit icon. Enter values for the following fields in the OSPF Interface Summary panel.

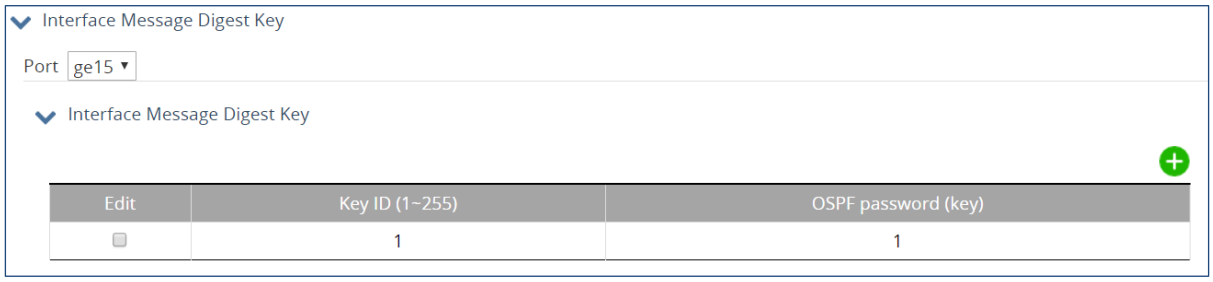
1. Authentication
2. Authentication Password (Key)
3. Interface Cost
4. Filter OSPF LSA During Synchronization And Flooding
5. Interval After Which A Neighbor Is Declared Dead
6. Flood Reduction
7. Time Between HELLO Packets
8. OSPF Interface MTU
9. Ignores the MTU in DBD packets
10. Network Type
11. Router Priority
12. Time Between Retransmitting Lost Link State Advertisements
13. Link State Transmit Delay
14. Disable OSPF

Click “Apply” when finished.



OSPF Interface Summary	
Authentication	Disabled
Authentication Password (Key)	
Interface Cost (1~65535)	10
Filter OSPF LSA During Synchronization And Flooding	Disabled
Interval After Which A Neighbor Is Declared Dead (1~65535)	40
Flood Reduction	Disabled
Time Between HELLO Packets (1~65535)	10
OSPF Interface MTU (576~65535)	1500
Ignores the MTU in DBD packets	Disabled
Network Type	Disabled
Router Priority (1~255)	1
Time Between Retransmitting Lost Link State Advertisements (1~65535)	5
Link State Transmit Delay (1~3600)	1
Disable OSPF	Disabled

The second panel on this screen is for configuring the Interface Message Digest Key, which allows for uninterrupted transitions between passwords. This is helpful for administrators who want to change the OSPF password without disrupting communication. Click the add icon, and enter the key and the OSPF password. Click “Apply” when done.

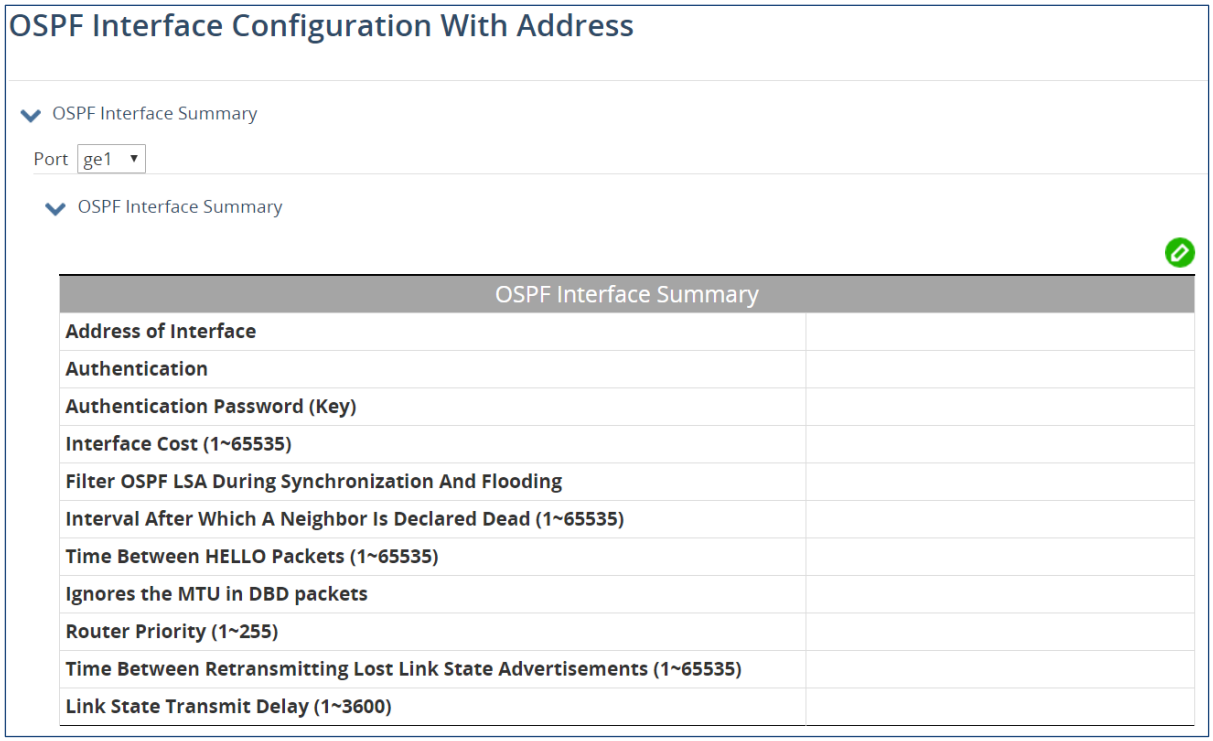


OSPF Interface Configuration With Address

The OSPF Interface Summary panel on this screen is similar to the one in the OSPF Interface Configuration screen, except that the OSPF area is restricted to an IP address. Select the port from the drop-down menu in the upper left and then click the edit icon. Enter values for the following fields:

1. Address of Interface
2. Authentication
3. Authentication Password (Key)
4. Interface Cost
5. Filter OSPF LSA During Synchronization And Flooding
6. Interval After Which A Neighbor Is Declared Dead
7. Time Between HELLO Packets
8. Ignores the MTU in DBD packets
9. Router Priority
10. Time Between Retransmitting Lost Link State Advertisements
11. Link State Transmit Delay

Click “Apply” when finished.



The Interface OSPF Statistics panel is a read-only panel that shows the index, interface address, and statistics for the selected port.

20 PIM (Protocol Independent Multicast)

Global Configuration

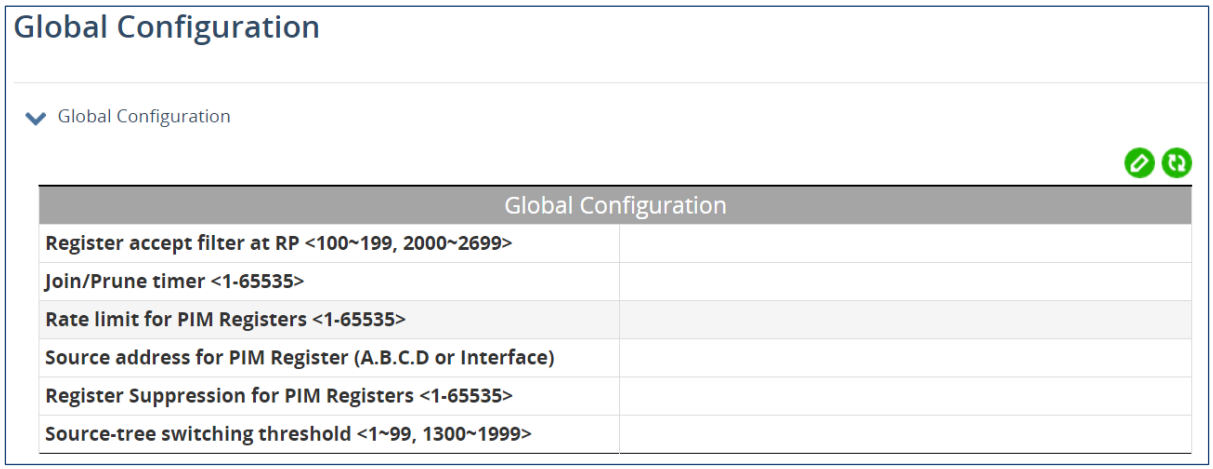
Protocol Independent Multicast (PIM) is a family of multicast routing protocols (MRP). There are two PIM modes: Sparse (PIM-SM) and Dense (PIM-DM).

PIM works with any unicast routing protocol to get route information to a Rendezvous Point (RP) and source. PIM neighbors are established through the exchange of Hello messages. A Designated Router (DR) is chosen in the subnet connected to the receivers. The DR sends periodic Join/Prune messages toward a group-specific RP for each group where there are active members.

To configure PIM globally, click the edit icon and enter values for the following fields:

1. Register accept filter at RP
2. Join/Prune timer
3. Rate limit for PIM Registers
4. Source address for PIM Register (A.B.C.D or Interface)
5. Register Suppression for PIM Registers
6. Source-tree switching threshold

Click “Apply” when finished.

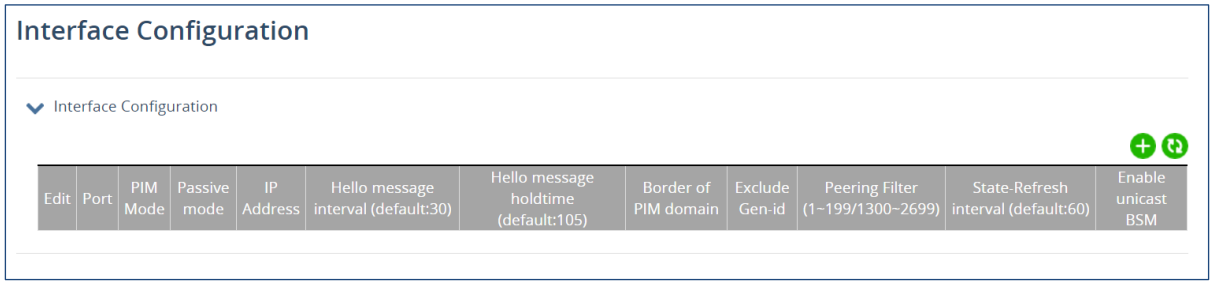


Interface Configuration

To configure PIM on an interface, click the add icon and enter values for the following fields:

1. Port
2. PIM Mode
3. Passive mode

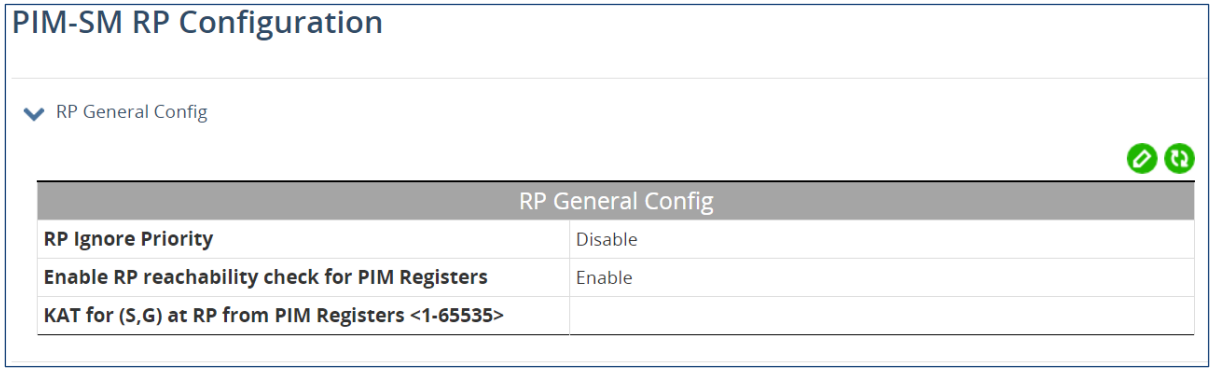
4. IP Address
5. Hello message interval (default:30)
6. Hello message holdtime (default:105)
7. Border of PIM domain
8. Exclude Gen-id
9. Peering Filter (1~199/1300~2699)
10. State-Refresh interval (default:60)
11. Enable unicast BSM



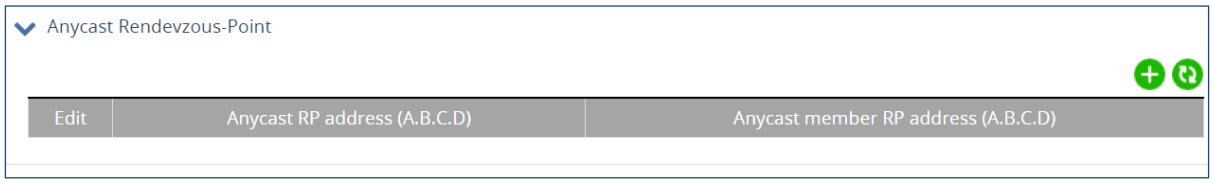
PIM-SM RP Configuration

A Rendezvous Point (RP) is where sources and receivers of multicast data meet. Sources send traffic to the RP, which is then forwarded to receivers along a shared distribution tree. When the first hop router of the receiver learns about the source, it creates a source-based distribution tree by sending a join message to the source.

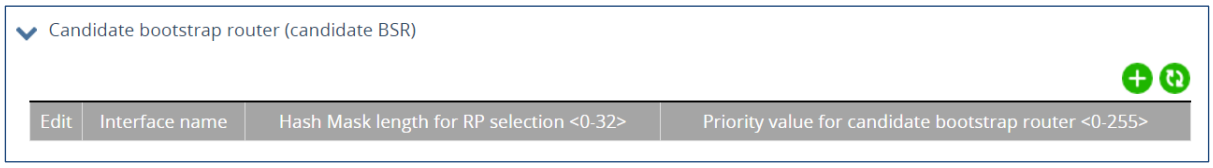
The first panel on this screen is RP General Configuration (sparse mode). To configure a PIM Sparse Mode RP, click the edit icon, and enable/disable the RP Ignore Priority and Enable RP Reachability Check for PIM registers fields. Then set the KeepAliveTimer at RP value. Click “Apply” when finished.



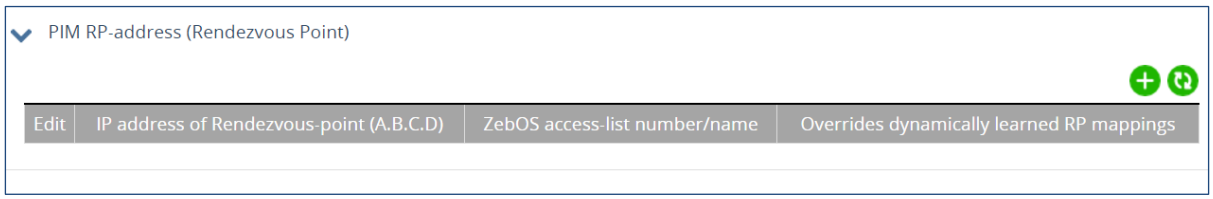
The second panel is Anycast Rendezvous-Point. Use it to set the Anycast RP address and Anycast Member RP address.



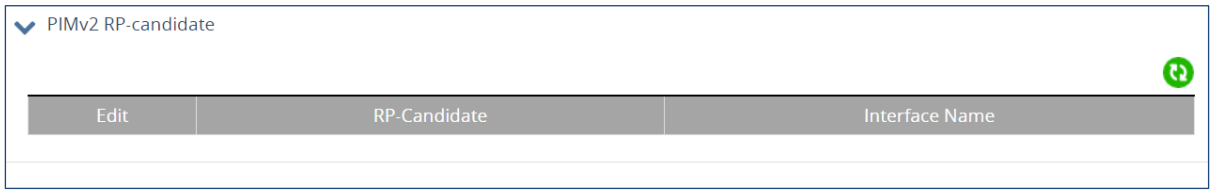
The third panel is Candidate Bootstrap Router (Candidate BSR). Routers learn RP information from the BSR. Click the add icon, and enter the Interface name, The Hash Mask length, and the Priority value for candidate BSR. Click “Apply” when finished.



The fourth panel is for configuring the RP. Enter the IP address of the RP, the access list number or name, and enable/disable the switch’s ability to override dynamically learned RP mappings.

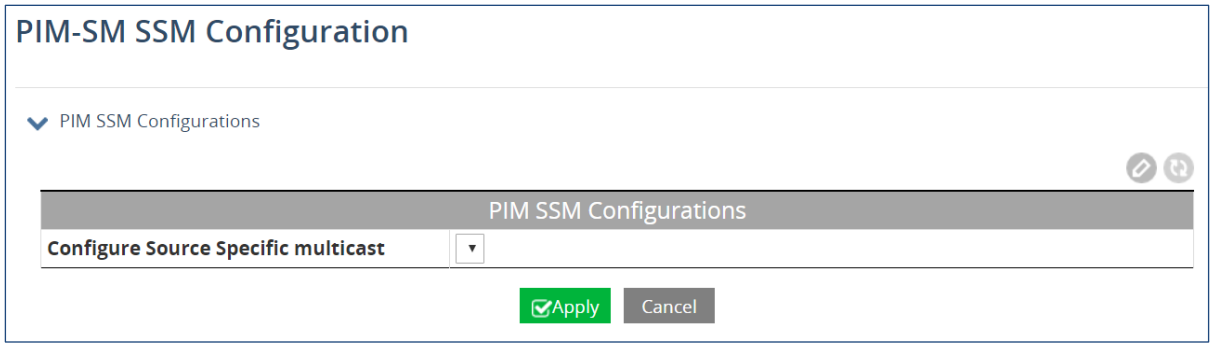


The fifth and final panel is a read only panel that shows existing RPs and interfaces.



PIM-SM SSM Configuration

PIM Source-Specific Multicast (PIM-SSM) builds trees that are rooted in a single source. Configure a source specific multicast by clicking the edit icon, and selecting a source from the drop-down list. Click “Apply” when finished.



PIM-SM Neighbor Table

This is a read-only table that shows the current information for all PIM-SM neighbors.

Contact Information

EtherWAN System, Inc.

www.etherwan.com

USA Office

2301 E. Winston Road
Anaheim, CA 9280
Tel: +1-714-779-3800
Email: info@etherwan.com

Pacific Rim Office

8F., No.2, Alley 6, Lane 235, Baoqiao Rd.
Xindian District, New Taipei City 231
Taiwan
Tel: +886 -2- 6629-8986
Email: info@etherwan.com.tw

EG99000 Layer 3 Hardened Managed Ethernet Switch
December 11, 2018