Panasonic

WEB Reference

Layer2 Ethernet Switch

Model Number: ZLP91089/ZLP91249
ZLP91240

The target model for this reference is as follows.

Model name	Model number	Firmware version
GA-MU8TPoE+	ZLP91089	1.0.0-2.03.17 or higher
XG-MU24TPoE+	ZLP91249	1.0.0-3.03.17 or higher
XG-MU24T	ZLP91240	1.0.0-3.03.17 or higher

Table of Contents

1 Login to device

Once your switch device has been set with IP address, you can login to the device web dashboard as management interface via browser:

Figure 1-1 Device's Web dashboard

1.1 Function Menu Bar

At the left-hand side of web management page, there's a function menu bar where 5 categories of functions are grouped under "Monitor", "Configure", "Analyze", 'User Management", and "Security", respectively.

Figure 1-2 Function Menu Bar

1.2 User Menu

In the upper right corner of the web administration page is the user menu, which is divided into four categories: "Reset," "Reboot," "Continuous PoE Power," and "Logout," respectively.

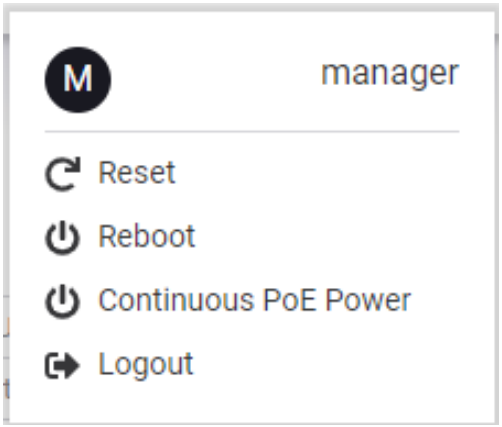

Figure 1-3 User Menu

1.3 Monitor your device

This section allows users to monitor their devices in a more efficient way where each specific function item can be used to let user get quick understanding of device status including POE utilization, usage statistics, and connected device info, etc.

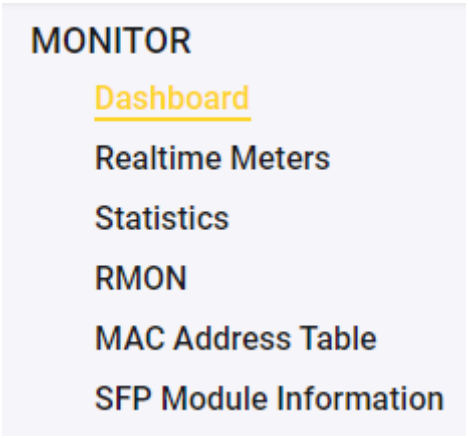

Figure 1-4 Function Items in Monitor Menu bar

1.4 Dashboard

Dashboard provides an overview for your device status:

1.4.1 Summary

Summary view lists most crucial system information for your managed device such as Model Name, Firmware Version, Serial No., MAC Address, System Uptime, IP Address, Subnet Mask, Gateway, and PoE usage statistics, etc.

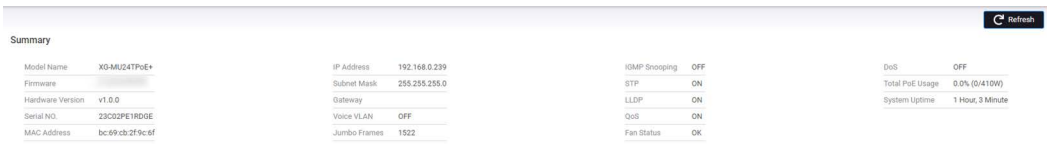

Figure 1-5 Summary

1.4.2 Total PoE utilization by port

The utilization chart lists per-port PoE utilization to let users get quick grasp on power consumption of each connected device on the switch device.

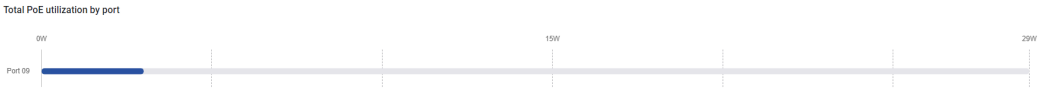

Figure 1-6 Total PoE utilization by port

1.4.3 VLAN

VLAN list provides all configured VLAN IDs with respective assigned port members in tagged/untagged columns.

VLAN

VLAN ID	Name	Tagged	Untagged
1	default	-	1-28,t1-t8
20		9	-

Figure 1-7 VLAN

1.5 Realtime Meters

This page facilitates real-time monitoring on managed devices.

1.5.1 CPU Loading

The CPU loading chart provides the real-time reading on CPU loading for monitoring.

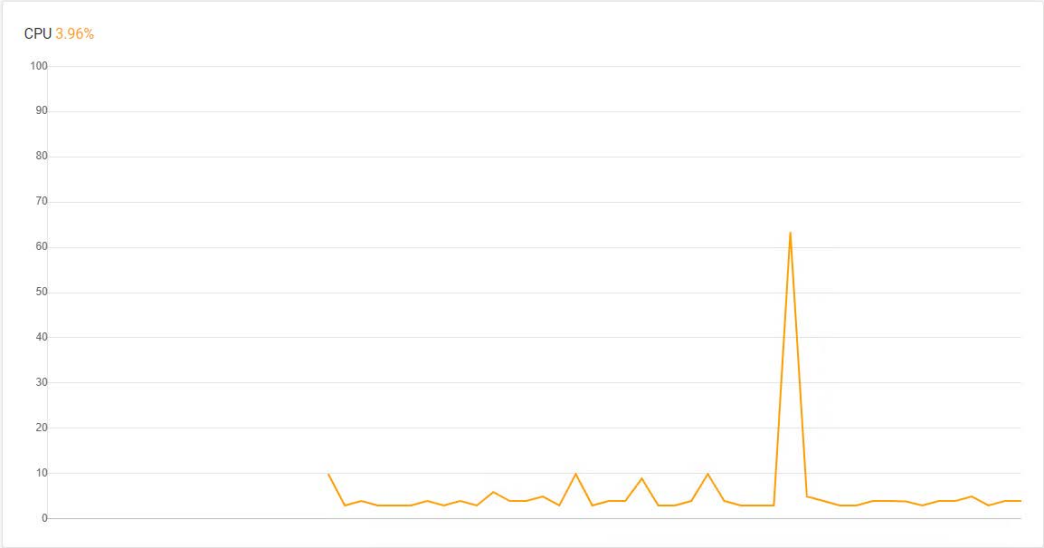

Figure 1-8 CPU Loading

1.5.2 Memory Usage

The memory usage chart provides the real-time reading on memory usage for monitoring.

Figure 1-9 Memory Usage

1.6 Statistics

The Port Statistics page displays a summary for all types of port traffic statistics.

1.6.1 L2 Statistics

1.6.1.1 Spanning Tree

Items	Descriptions
Port	Displays the port for which statistics are displayed.
RX BPDU	Displays the number of all BPDU received on the port.
TX BPDU	Displays the number of BPDU transmitted on the port.
Invalid BPDU	Displays the number of Invalid BPDU on the port.

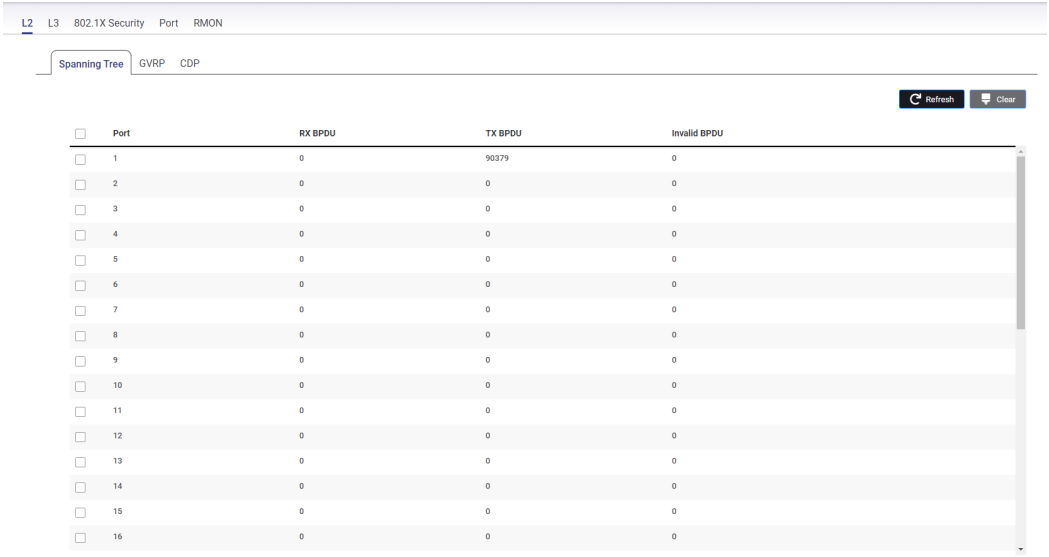

Figure 1-10 Spanning Tree

1.6.1.2 GVRP

Defined in the IEEE 802.1Q standard, Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) is an application for the control of VLANs.

Items	Descriptions
Port	Displays the port for which statistics are displayed.
RxJoinEmpty	Displays the number of GVRP Join Empty event packets received on the port.
RxLeaveIn	Displays the number of GVRP Leave In event packets received on the port.
RxLeaveAll	Displays the number of GVRP Leave All event packets received on the port.
RxLeaveEmpty	Displays the number of GVRP Leave Empty event packets received on the port.
RxEmpty	Displays the number of GVRP Empty event packets received on the port.
RxTotal	Displays the number of total GVRP packets received on the port.
Drop	Displays the number of drop traffics on the port.
TxJoinEmpty	Displays the number of GVRP Join Empty event packets transmitted on the port.
TxJoinIn	Displays the number of GVRP Join In event packets transmitted on the port.
TxLeaveIn	Displays the number of GVRP Leave In event packets transmitted on the port.
TxLeaveAll	Displays the number of GVRP Leave All event packets transmitted on the port.
TxLeaveEmpty	Displays the number of GVRP Leave Empty event packets transmitted on the port
TxEmpty	Displays the number of GVRP Empty event packets transmitted on the port
TxTotal	Displays the number of Total GVRP packets transmitted on the port

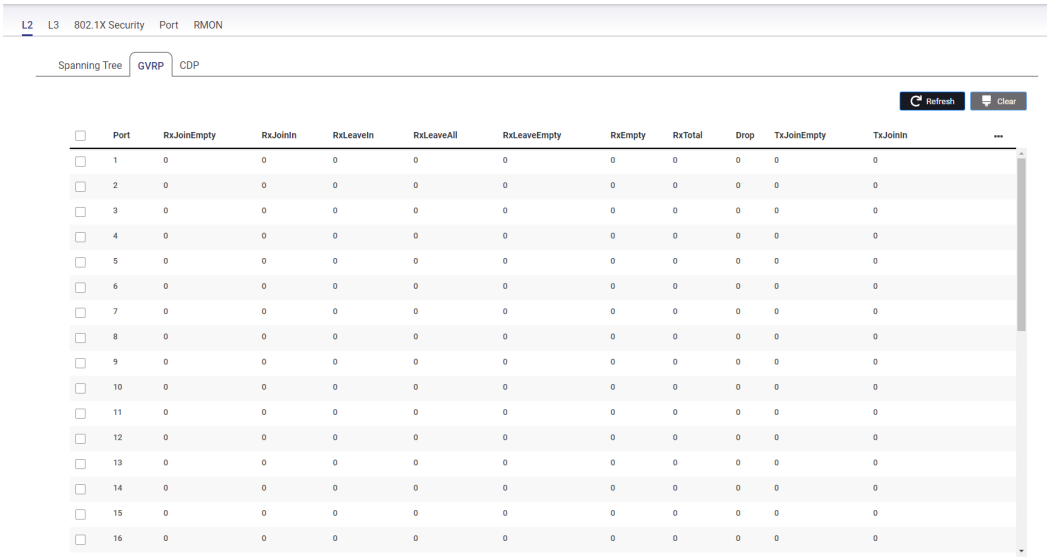

Figure 1-11 GVRP

1.7 L3 Statistics

1.7.1 DHCP Snooping

DHCP Snooping is a layer 2 security mechanism incorporated into the switch, preventing rogue DHCP servers from offering unauthorized IP addresses to DHCP clients.
Upon DHCP snooping enabled on a VLAN, the switch will examine DHCP messages sent from untrusted hosts with the VLAN and extracts their IP addresses/lease information to build and maintain the DHCP snooping database. After verification by this database, verified hosts can be granted access to the network.

Items	Descriptions
VLAN	Displays the VLAN for which statistics are displayed.
RXDicovers	Displays the number of DHCP Discover packets received on the port.
RXRequests	Displays the number of DHCP Request packets received on the port.
RXReleases	Displays the number of DHCP Release packets received on the port.
RXDeclines	Displays the number of DHCP Decline packets received on the port.

Items	Descriptions
RXInforms	Displays the number of DHCP Inform packets received on the port.
TXOffers	Displays the number of DHCP Offer packets transmitted on port.
TXAcks	Displays the number of DHCP ACK packets transmitted on the port.
TXNaks	Displays the number of DHCP Nak packets transmitted on the port.
MACDiscard	Displays the number of MAC Discard on the port.
ServerDiscard	Displays the number of Server Discard on the port.
OptionDiscard	Displays the number of Option Discard on the port.
TotalDiscard	Displays the total number of Discard on the port.

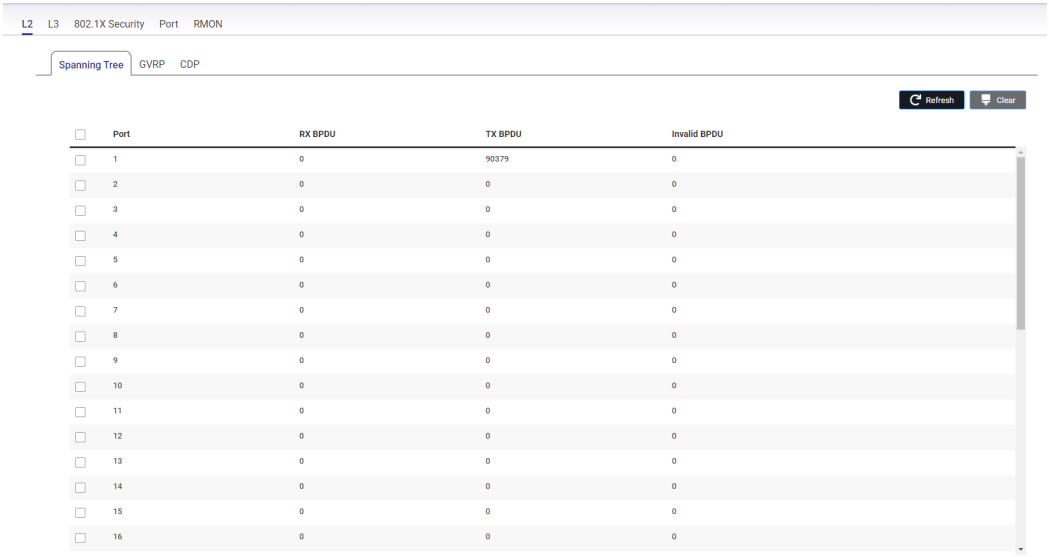

Figure 1-12 DHCP Snooping

1.7.2 802.1X Security

Items	Descriptions
Port	Displays the port for which statistics are displayed.
TxReqId	Displays the number of 802.1x-Request/Identity messages transmitted on the port.
TxReq	Displays the number of transmitted 802.1x-Request frames other than Request/Identity on the port.

Items	Descriptions
TxTotal	Displays the total number of EAPOL messages transmitted on the port.
RxStart	Displays the number of EAPOL-Start messages received on the port.
RxLogoff	Displays the number of 802.1x-Logoff messages received on the port.
RxRespId	Displays the number of 802.1x-Response/Identity frames received on the port.
RxResp	Displays the number of 802.1x-Response messages received other than Response/Identity.
RxInvalid	Displays the number of invalid EAPOL messages received on the port.
RxlenErr	Displays the number of EAPOL messages with incorrect length received on the port.
RxTotal	Displays the number of EAPOL messages received on the port.
RxVersion	Displays the version number of the EAPOL message received on the port.
LastRxSrcMac	Displays the source MAC address in the last EAPOL message received on the port.

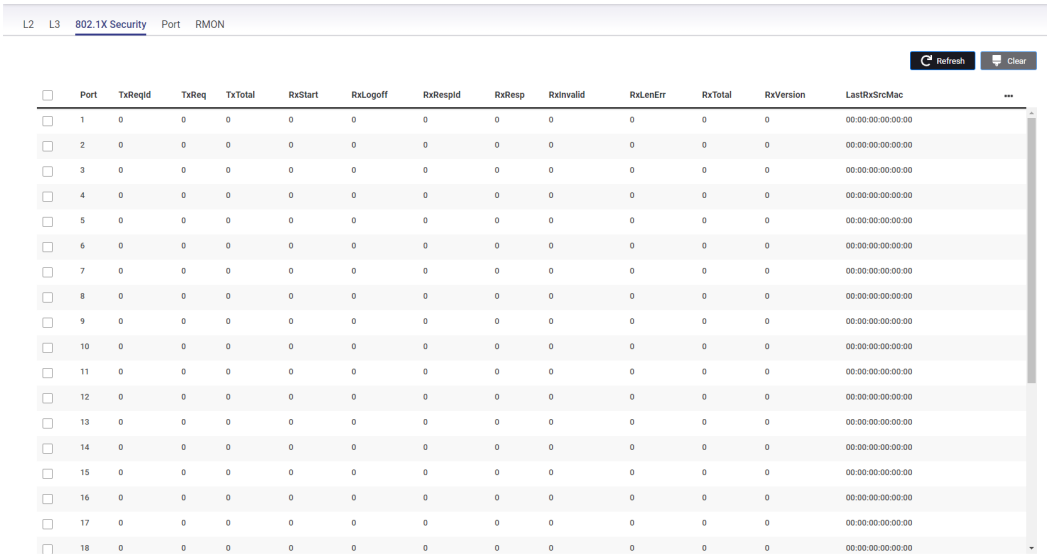

Figure 1-13 802.1X Security

1.7.3 Port

Items	Descriptions
Port	Displays the port for which statistics are displayed.
RXOctets	Displays the number of octets for all packets received on the port.
RXUcast	Displays the number of unicast packets received on the port.
RXNUcast	Displays the number of non-unicast packets received on the port.
RXDiscard	Displays the number of received packets discarded on the port.
TXOctets	Displays the number of octets for all packets transmitted on the port.
TXUcast	Displays the number of unicast packets transmitted on port.
TXNUcast	Displays the number of non-unicast packets transmitted on the port.
TXDiscard	Displays the number of transmitted packets discarded on the port.
RXMcast	Displays the number of multicast packets received on the port.
RXBcast	Displays the number of broadcast packets received on the port.
TXMcast	Displays the number of multicast packets transmitted on the port.
TXBcast	Displays the number of broadcast packets transmitted on the port.

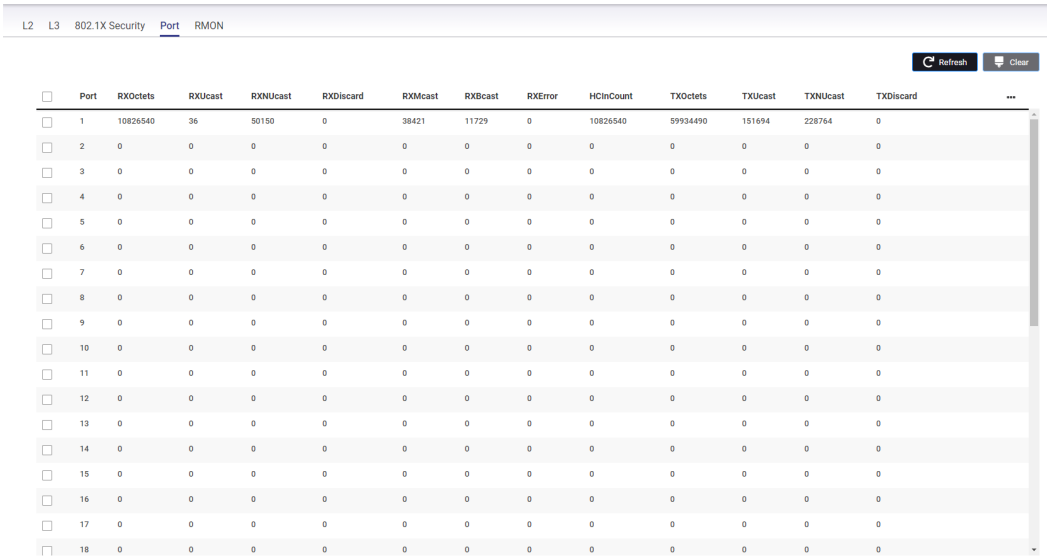

Figure 1-14 Port

1.7.4 RMON

Items	Descriptions
ID	Displays entry index.
Data Source	Displays the corresponding switch port.
Drop Events	Displays the number of dropped events that have occurred on the port.
Octets	Displays the number of octets received on the port.
Pkts	Displays the number of packets received on the port.
Broadcast Pkts	Displays the number of good broadcast packets received on the port. This number does not include Multicast packets.
Multicast Pkts	Displays the number of good Multicast packets received on the port.
CRC Align Errors	Displays the number of CRC and Align errors that have occurred on the port
Fragments	Displays the number of fragments received on the port.

Figure 1-15 RMON

1.8 RMON

Remote Network Monitoring (RMON) is used to support monitoring and protocol analysis of LANs by enabling various network monitors and console systems to exchange network monitoring data.

1.8.1 Stat List

Stat List allows users to add entry of data source for RMON monitoring.

Figure 1-16 Stat List

Items	Descriptions
Index	Enter the index of entry.
Data Source	Select the corresponding switch port.
Owner	Click the Apply button to accept the changes or the Cancel button to discard them.

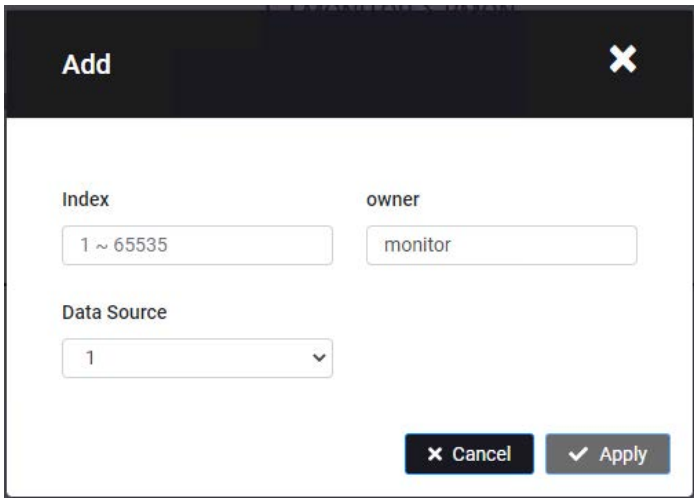

Figure 1-17 Stat List(Additional Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

1.8.2 Event List

The Event List defines RMON events on the switch.

Items	Descriptions
Index	Enter the entry number for event.
Event Type	Select the event type. Log: The event is a log entry. SNMP Trap: The event is a trap. Log & Trap: The event is both a log entry and a trap.
Community	Enter the community to which the event belongs.
Description	Displays the number of good broadcast packets received on the interface.
Last Time Sent	Displays the time that event occurred.
Owner	Enter the switch that defined the event.

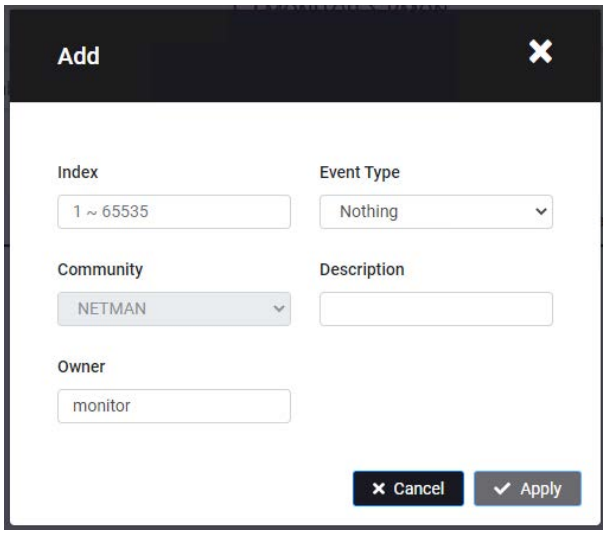

Figure 1-18 Event List(Additional Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

1.8.3 Event Log Table

From here, you can view specific event logs for the switch. Choose an event log you wish to view from the drop-down list.

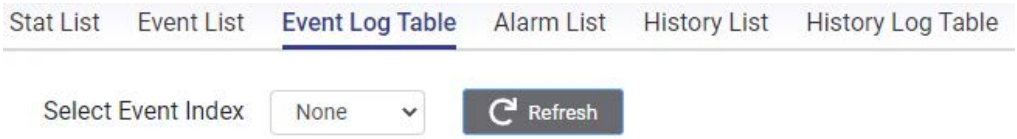

Figure 1-19 Event Log Table

1.8.4 Alarm List

You can configure network alarms to occur when a network problem is detected. Choose your preferences for the alarm from the drop-down boxes.

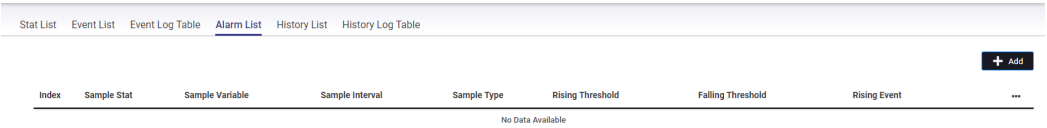

Figure 1-20 Alarm List

Items	Descriptions
Index	Enter the entry number for the Alarm List.
Sample Port	Select the port from which the alarm samples were taken.
Sample Variable	Select the variable of samples for the specified alarm sample.
Sample Interval	Enter the alarm interval time.
Sample Type	Select the sampling method for the selected variable and compare the value against the thresholds. Absolute: Compares the values with the thresholds at the end of the sampling interval. Delta: Subtracts the last sampled value from the current value.
Rising Threshold	Enter the rising number that triggers the rising threshold alarm.
Falling Threshold	Enter the falling number that triggers the falling threshold alarm.
Rising Event	Enter the event number by the falling alarms are reported.

Items	Descriptions
Falling Event	Enter the event number by the falling alarms are reported.
Owner	Enter the switch that defined the alarm.

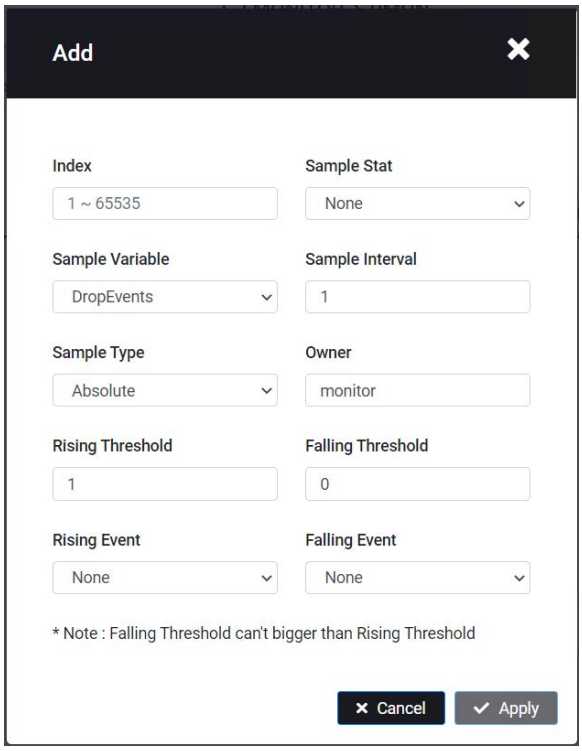

Figure 1-21 Alarm List(Additional Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

1.8.5 History List

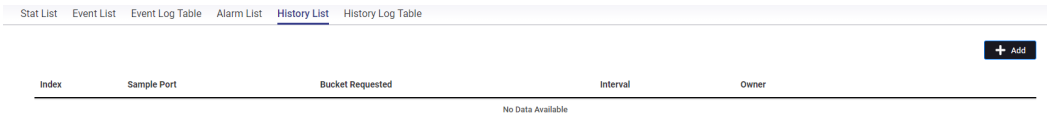

Figure 1-22 History List

Items	Descriptions
Index	Enter the entry number for the History List.

Items	Descriptions
Sample Port	Select the port from which the history samples were taken.
Bucket Requested	Enter the number of samples to be saved. The range is from 1 to 50.
Interval	Enter the time that samples are taken from the ports. The field range is from 1 to 3600.
Owner	Enter the RMON user that requested the RMON information. The range is from 0 to 32 characters.

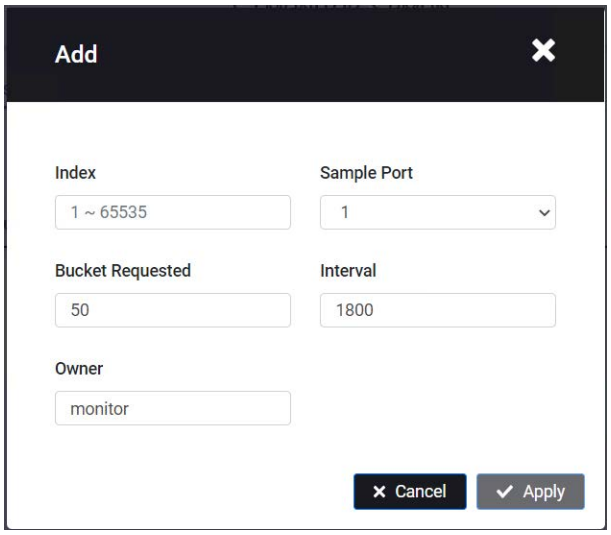

Figure 1-23 History List(Additional Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

1.8.6 History Log Table

From here, you can view the History Index for history logs on the switch. Select a history index to view from the drop-down box.

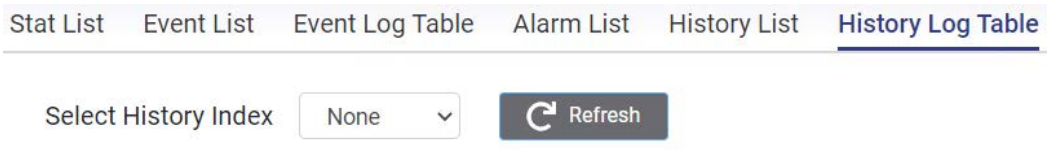

Figure 1-24 History Log Table

1.9 MAC Address Table

The MAC address table contains address information that the Switch uses to forward traffic between the inbound and outbound ports. All MAC addresses in the address table are associated with one or more ports. When the Switch receives traffic on a port, it searches the Ethernet switching table for the MAC address of the destination. If the MAC address is not found, the traffic is flooded out all of the other ports associated with the VLAN. All of the MAC address that the Switch learns by monitoring traffic are stored in the dynamic address. A static address allows you to manually enter a MAC address to configure a specific port and VLAN.

1.9.1 Static MAC Address

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address. When you specify a static MAC address, you set the MAC address to a VLAN and a port; thus it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch. Static MAC addresses along with the Switch's port security allow only devices in the MAC address table on a port to access the Switch.

Figure 1-25 Static MAC Address

Click the **Add** button to add new entry:

Items	Descriptions
Index	Displays the index for the static MAC address table.
Port	Select the port where the MAC address entered in the previous field will be automatically forwarded.
VID	Enter the VLAN ID on which the IGMP Snooping querier is administratively enabled and for which the VLAN exists in the VLAN database
MAC Address	Enter a unicast MAC address for which the switch has forwarding or filtering information.

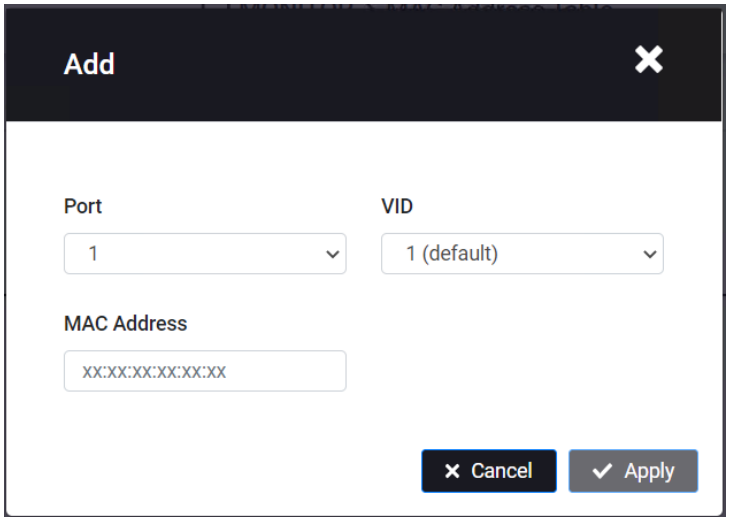

Figure 1-26 Static MAC Address(Additional Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

1.9.2 Dynamic MAC Address

The Switch will automatically learn the device's MAC address and store it to the dynamic MAC address table. If there is no packet received from the device within the aging time, the Switch adopts an aging mechanism for updating the tables from which MAC address entries will be removed from related network devices. The dynamic MAC address table shows the MAC addresses and their associated VLANs learned on the selected port.

Click the Refresh button to get the updated list:

Figure 1-27 Dynamic MAC Address

Items	Descriptions
Index	Displays the index for the dynamic MAC address table.
Port	Select the port to which the entry refers.

Items	Descriptions
VID	Displays the VLAN ID corresponding to the MAC address.
MAC Address	Displays the MAC addresses that the Switch learned from a specific port

1.9.3 MAC Aging Time

Specify the MAC Aging Time for the MAC address entry on the switch.

Figure 1-28 MAC Aging Time

1.9.4 MAC Filters

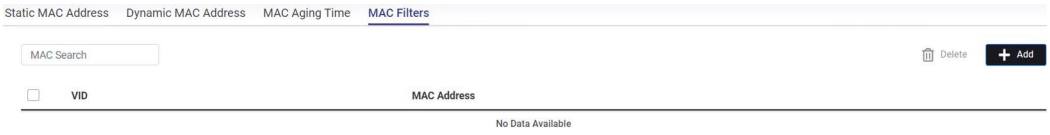

Figure 1-29 MAC Filter

1.10 SFP Module Information

TBD for this part (SFP Module Information upon update)

1.10.1 Module

Select the port from the drop-down to retrieve module information:

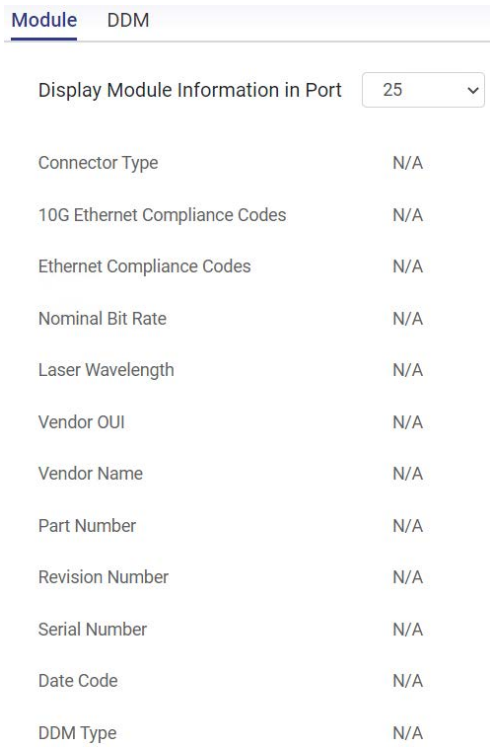

Figure 1-30 Module

1.10.2 DDM

Select the port from the drop-down to retrieve DDM information:

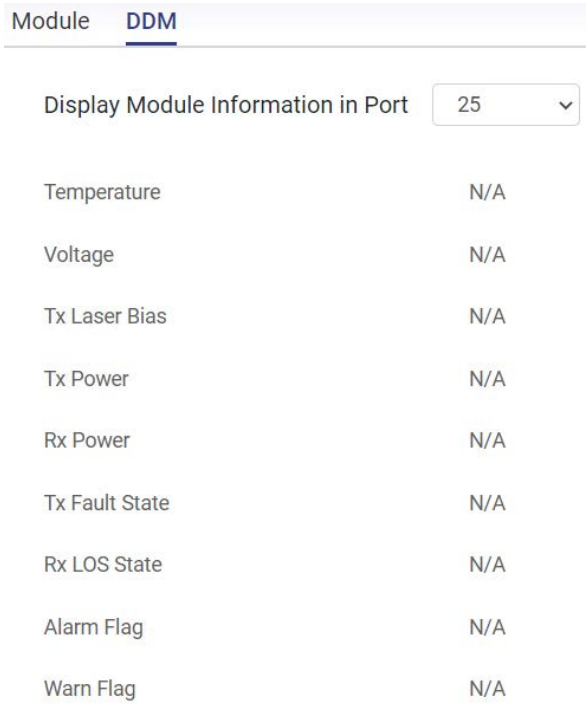

Figure 1-31 DDM

2 System Settings

This page shows the summary of general system information for the switch including the system information, IP settings, ARP settings, system time, and Neighbor Discovery Table.

2.1 System Information

Figure 2-1 System Information

Items	Descriptions
System Name	Configures/Displays the system name of the device.
System Location	Configures/Displays the installed location of the device.
System Contact	Configures/Displays the contact info of the installed device.

2.2 IP Settings

The IP Settings tab contains fields for assigning IP addresses and Management VLAN. IP addresses are either defined as static or are retrieved using the Dynamic Host Configuration Protocol (DHCP). DHCP assigns dynamic IP addresses to devices on a network. DHCP ensures that network devices can have a different IP address every time the device connects to the network.

2.2.1 IPv4 Management

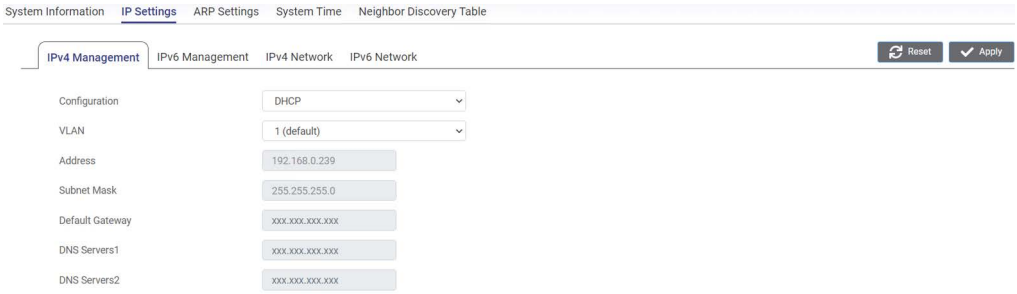

Figure 2-2 IPv4 Management

Items	Descriptions
VLAN	Configure/Displays the management VLAN for the device.
Address	Displays the IP address of the device.
Subnet Mask	Displays the subnet mask of the device.
Configuration	Configures/Displays IP settings by DHCP or Static.

Click the **Apply** button to apply the changes or the **Reset** button to discard them.

2.2.2 IPv6 Management

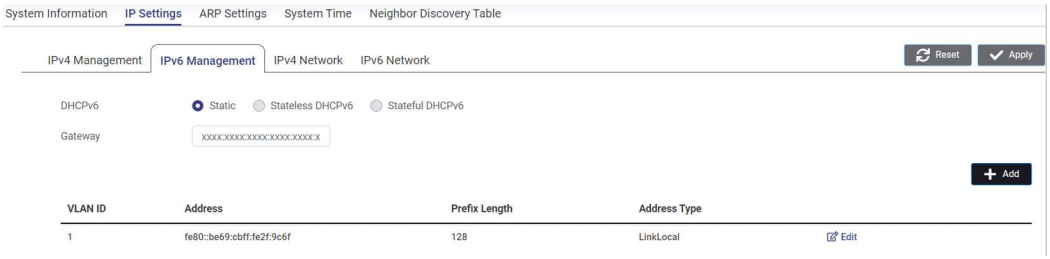

Figure 2-3 IPv6 Management

Items	Descriptions
VLAN	Configure/Displays the management VLAN for the device.
Address	Displays the IPv6 address of the device.
Prefix Length	Displays the prefix length of the device's IPv6 address.
Address Type	Displays address type of this IPv6 address.

Click the **Apply** button to apply the changes or the **Reset** button to discard them.

2.2.3 IPv4 Network

Figure 2-4 IPv4 Network

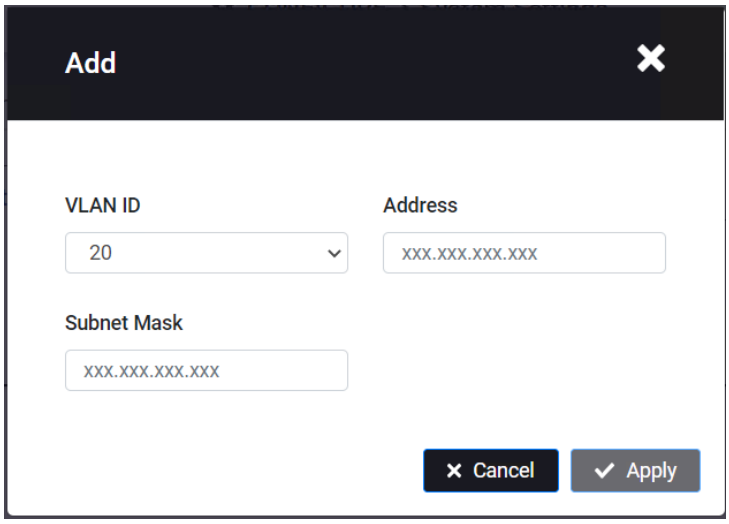

Figure 2-5 IPv4 Network(Additional Screen)

Items	Descriptions
VLAN ID	Select the VLAN ID for the IPv4 network.
Address	Enter the IP address of the added network.
Subnet Mask	Enter the subnet mask of the added network.

Click the **Apply** button to apply the changes or the **Reset** button to discard them.

2.3 IPv6 Network

Figure 2-6 IPv6 Network

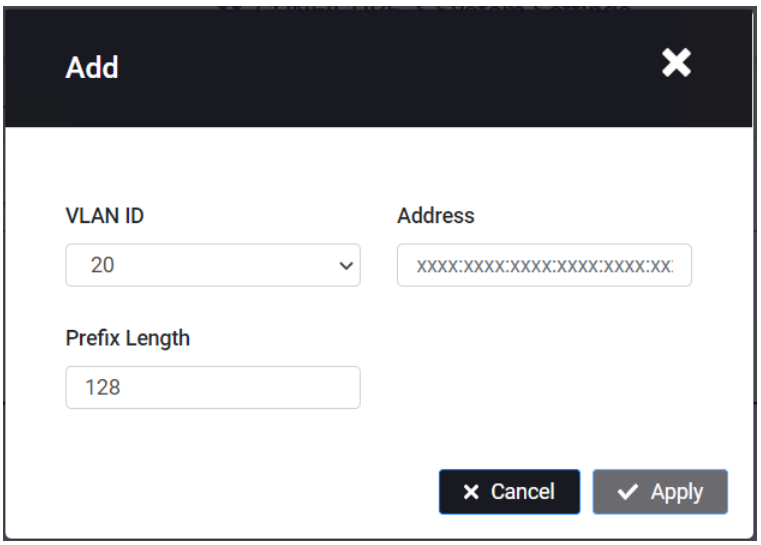

Figure 2-7 IPv6 Network(Additional Screen)

Items	Descriptions
VLAN ID	Select the VLAN ID for the IPv6 network.
Address	Enter the IP address of the added network.
Prefix Length	Enter the prefix length of the added network.

2.4 ARP Settings

ARP (Address Resolution Protocol) is used to discover link layer address (like MAC address) associated with a given Internet layer address, typically an IPv4 address.

2.4.1 Global Settings

Figure 2-8 Global Settings

Items	Descriptions
Max Retries	Configures/Displays the max times for the ARP Retry.
Timeout	Configures/Displays the value of the ARP Timeout.

Click the **Apply** button to apply the changes or the **Reset** button to discard them.

2.4.2 ARP Table

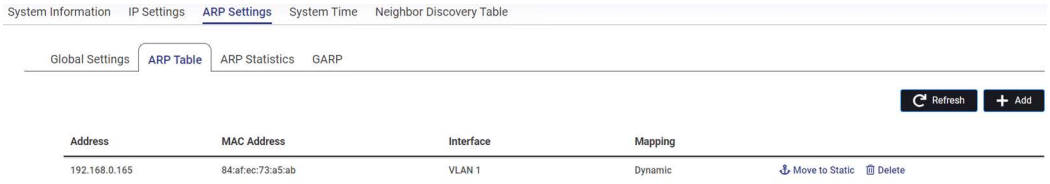

Figure 2-9 ARP Table

Items	Descriptions
Address	Displays the IP address for the found device.
MAC	Displays the MAC address of the associated IP address.
Interface	Displays the interface for the found IP address.
Mapping	Displays the mapping method for the found IP address.

Click the **Add** button to add an entry or the **Refresh** button to update the table.

2.4.3 ARP Statistics

The list will show ARP statistics of the system for total and respective specific types.

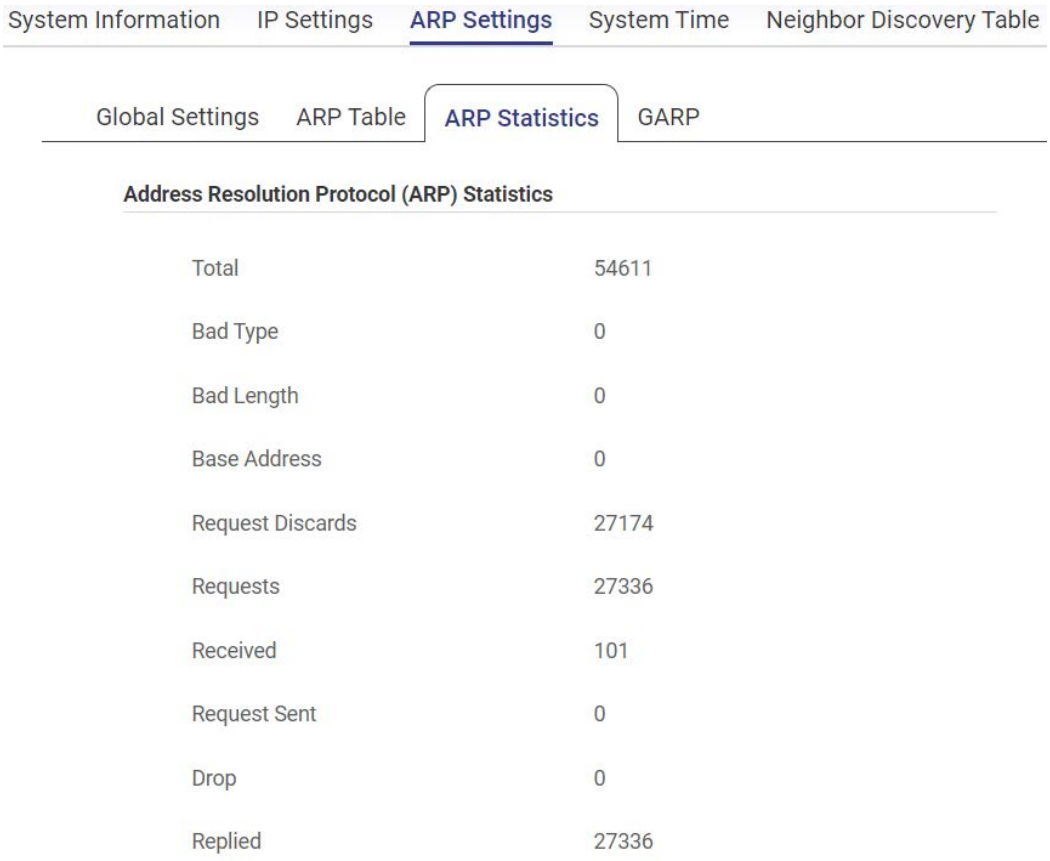

Figure 2-10 ARP Statistics

2.4.4 GARP

Figure 2-11 GARP

2.5 System Time

Use the System Time screen to view and adjust date and time settings. The switch supports Simple Network Time Protocol (SNTP). SNTP ensures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. This switch operates only as an SNTP client and cannot provide time services to other systems.

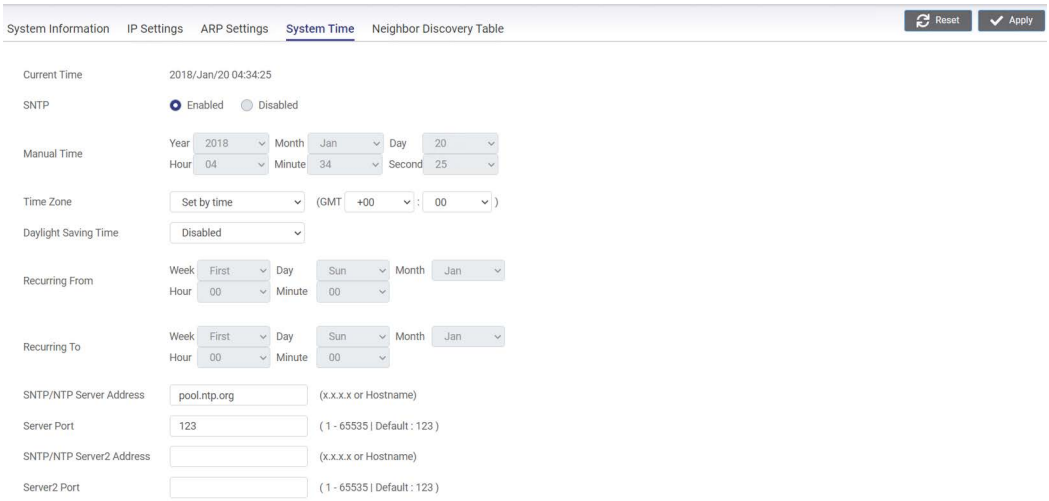

Figure 2-12 System Time

Items	Descriptions
Current time	Displays the current system time.
Enable SNTP	Select whether to enable or disable system time synchronization with an SNTP server.
Time Zone	Configure the time zone setting either by setting GMT difference or by country.
Daylight Savings Time	Select from Disabled, Recurring or Non-recurring.
Daylight Savings Time Offset	Enter the time of Daylight Savings Time Offset.
Recurring From	Select the Day, Week, Month, and Hour from the list.
Recurring To	Select the Day, Week, Month, and Hour from the list.
SNTP/NTP Server Address	Enter the IP address or hostname of the SNTP/NTP server.
Server Port	Enter the server port of the SNTP/NTP server.

2.5.1 To configure date/time through SNTP:

1.Next to the Enable SNTP, select Enable.
2.In the Time Zone Offset list, select by country or by the GMT time zone where the switch is located.
3.Next select Disabled, Recurring, or Non-Recurring for Daylight Savings Time. Daylight saving is a period from late Spring to early Fall when many countries set their clocks forward or backward by one hour to give more daytime light in the evening.
4.In the SNTP/NTP Server Address field, enter the IP address or the host name of the SNTP/NTP server.
5.Finally, enter the port number on the SNTP server to which SNTP requests are sent. The valid range is from 1−65535. The default is: 123.
6.Click Apply to update the system settings.

2.5.2 To configure date/time manually:

1.Next to the Enable SNTP, select Disable.
2.In the Manual Time field, use the drop-down boxes to manually select the date and time you wish to set.
3.In the Time Zone Offset list, select by country or by the Coordinated Universal Time (UTC/GMT) time zone in which the switch is located.
4.Next select Disabled, Recurring or Non-recurring for Daylight Savings Time. Daylight saving is a period from late Spring to early Fall when many countries set their clocks forward or backward by one hour to give more daytime light in the evening.
5.Click Apply to update the system settings.

2.6 Neighbor Discovery Table

This list shows IPv6 neighbors where the switch uses NDP (Neighbor Discovery Protocol) to determine the Layer 2 MAC addresses for neighboring hosts.

Figure 2-13 Neighbor Discovery Table

Click the **Add** button to add an entry or the **Refresh** button to update the table.

3 SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol designed specifically for managing and monitoring network devices. Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from and configuring network devices such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network. SNMP is used to exchange management information between a network management system (NMS) and a network device. A manager station can manage and monitor the switch through their network via SNMPv1, v2c and v3. An SNMP managed network consists of two components: agents and a manager.

An agent translates the local management information from the managed switch into a form that is compatible with SNMP. SNMP allows a manager and agents to communicate with each other for the purpose of accessing Management Information Bases (MIBs). SNMP uses an extensible design, where the available information is defined by MIBs. MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing Object Identifiers (OID). Each OID identifies a variable that can be read or set via SNMP.

The manager is the console through which network administrators perform network management functions.

Several versions of SNMP are supported. They are v1, v2c, and v3. SNMPv1, which is defined in RFC 1157. "A Simple Network Management Protocol (SNMP)" is a standard that defines how communication occurs between SNMP-capable devices and specifies the SNMP message types. Version 1 is the simplest and most basic of versions. There may be times when it's required to support older hardware. SNMPv2c is defined in RFC 1901 "Introduction to Community-Based SNMPv2," RFC 1905 "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", and RFC 1906 "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)." SNMPv2c updates protocol operations by introducing a GetBulk request and authentication based on community names. Version 2c adds several enhancements to the protocol such as support for "Informs." Because of this, v2c has become

the most widely used version. Unfortunately, a major weakness of v1 and v2c is security. To combat this, SNMP v3 adds security features that overcome the weaknesses in v1 and v2c. If possible, it is recommended that you use v3, especially if you plan to transmit sensitive information across unsecured links. However, the extra security feature makes configuration a little more complex.

In SNMPv3, User-based Security Model (USM) authentication is implemented along with encryption, allowing you to configure a secure SNMP environment. The SNMPv3 protocol uses different terminology than SNMPv1 and SNMPv2c as well. In the SNMPv1 and SNMPv2c protocols, the terms agent and manager are used. In the SNMPv3 protocol, agents, and managers are renamed to entities. With the SNMPv3 protocol, you create users and determine the protocol used for message authentication as well as if data transmitted between two SNMP entities is encrypted.

The SNMPv3 protocol supports two authentication protocols: HMAC-MD5-96 (MD5) and HMAC-SHA-96 (SHA). Both MD5 and SHA use an algorithm to generate a message digest. Each authentication protocol authenticates a user by checking the message digest. In addition, both protocols use keys to perform authentication. The keys for both protocols are generated locally using the Engine ID and the user password to provide even more security.

In SNMPv1 and SNMPv2c, user authentication is accomplished using types of passwords called community strings, which are transmitted in clear text and not supported by authentication. Users can assign views to community strings that specify which MIB objects can be accessed by a remote SNMP manager.

The default community strings for the switch used for SNMPv1 and SNMPv2c management access for the switch are public, which allows authorized management stations to retrieve MIB objects, and private, which allows authorized management stations to retrieve and modify MIB objects.

3.1 Global Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (application layer) protocol designed specifically for managing and monitoring network devices. The SNMP agents maintain a list of variables

that are used to manage the device. The variables are defined in the Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent.

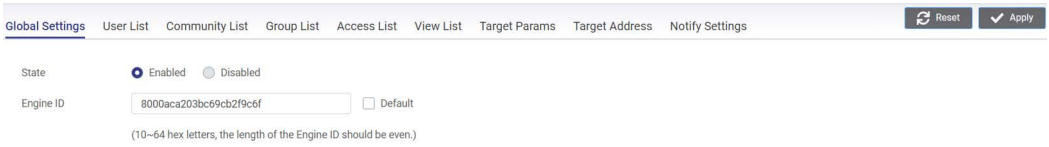

Figure 3-1 Global Settings

- **Status**: Choose "Enabled" or "Disabled" for this option.
- **Engine ID**: SNMP engine ID is used to uniquely identify an SNMPv3 entity in a management domain. The length of the Engine ID should be even, allowing 10~64 hex letters; by default, an SNMP engine ID consists of an enterprise number and individual device information.

Click the **Apply** button to apply the changes or the **Reset** button to discard them.

3.2 User List

Figure 3-2 User List

Items	Descriptions
User Name	Shows SNMP user names.
Privilege Mode	Shows corresponding privilege mode for the user.
Authentication Protocol	Shows corresponding authentication protocol used by the user.
Encryption Protocol	Shows corresponding encryption protocol used by the user.

Click the **Add** button to add an user.

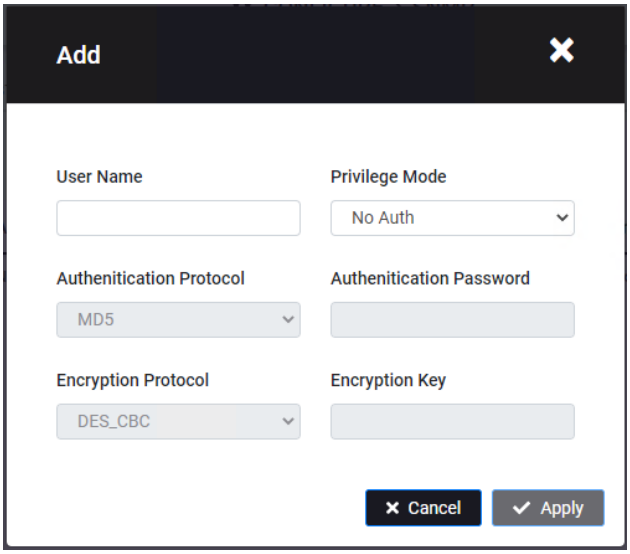

Figure 3-3 User List(Additional Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

3.3 Community List

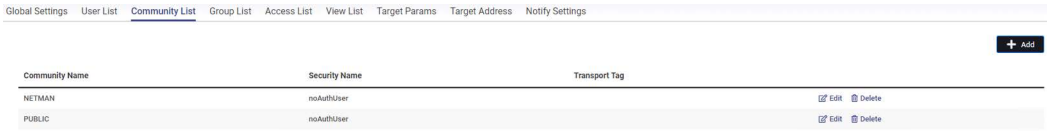

Figure 3-4 Community List

Items	Descriptions
Community Name	Shows SNMP community name.
Security Name	Shows corresponding security method/name for the community.
Transport Tag	Shows corresponding transport tag for the community.

Click the **Add** button to add an entry in the list:

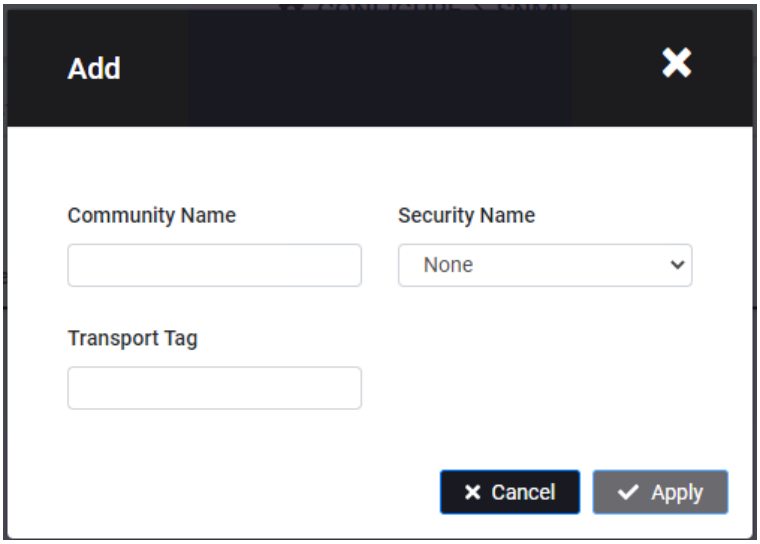

Figure 3-5 Community List(Additional Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

3.4 Group List

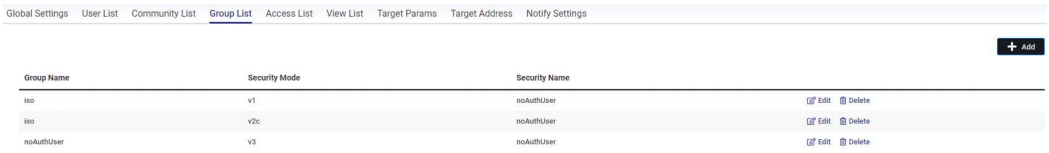

Figure 3-6 Group List

Items	Descriptions
Group Name	Shows SNMP group name.
Security Mode	Shows corresponding security mode for the group.
Security Name	Shows corresponding security method/name for the group.

Click the **Add** button to add an entry in the list:

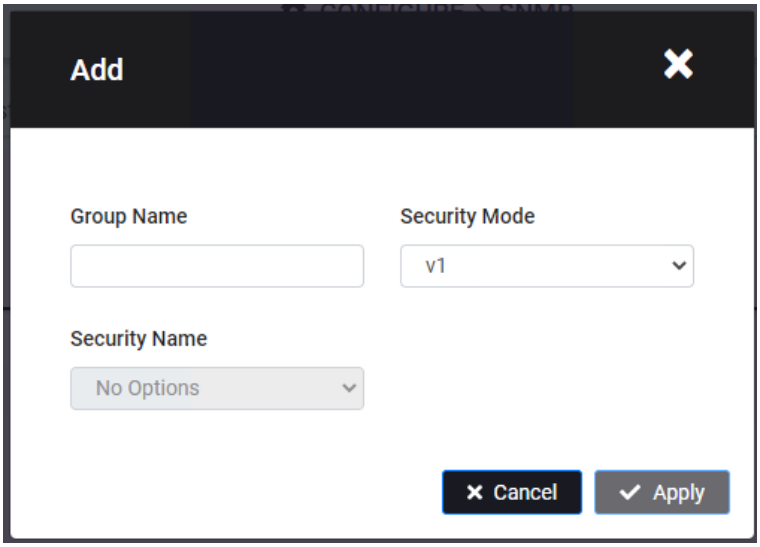

Figure 3-7 Group List(Additional Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

3.5 Access List

Figure 3-8 Access List

Items	Descriptions
Group Name	Shows SNMP group name.
Security Mode	Shows corresponding security mode for the group.
Privilege Mode	Shows corresponding privilege mode for the group.
Read View	Shows permission mode for read view.
Write View	Shows permission mode for write view.
Notify View	Shows permission mode for notify view.

3.6 View List

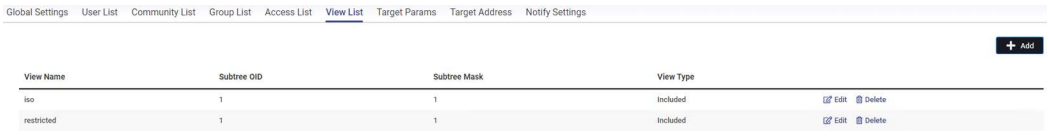

Figure 3-9 View List

Items	Descriptions
View Name	Shows SNMP view name.
Subtree OID	Shows corresponding subtree OID.
Subtree Mask	Shows corresponding subtree mask.
View Type	Shows corresponding view type to be included/ excluded.

Click the **Add** button to add an entry in the list:

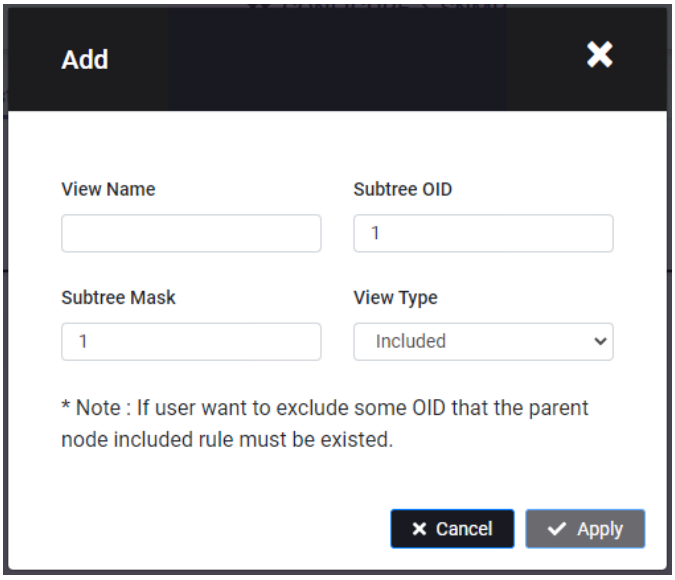

Figure 3-10 View Type(Additional Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

3.7 Target Parameters

Figure 3-11 Target Parameters

Items	Descriptions
Target Parameter Name	Shows target parameter name.
Message Processing Model	Shows corresponding message processing model. (v1, v2c, or v3)
Security Mode	Shows corresponding security mode (v1, v2c, or v3).
Security Name	Shows corresponding security name.
Privilege Mode	Shows corresponding privilege mode.

Click the **Add** button to add an entry in the list:

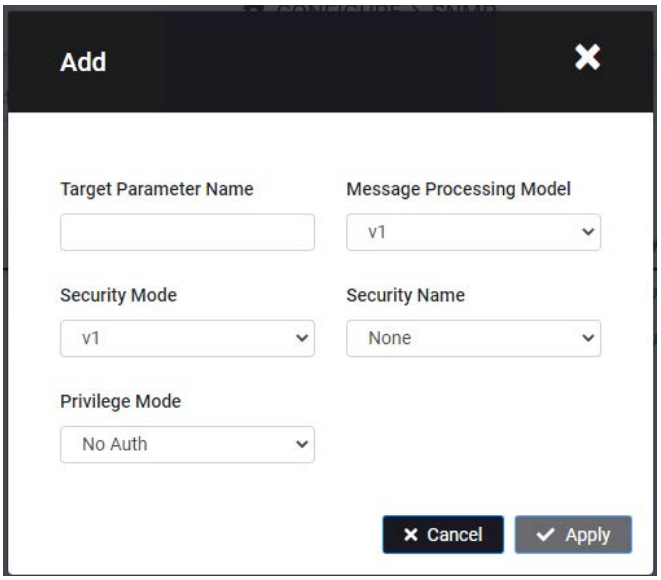

Figure 3-12 Target Parameters(Additional Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

3.8 Target Address

Figure 3-13 Target Address

Items	Descriptions
Target Address Name	Shows target address name.
IP Address	Shows corresponding IP address.
UDP Port	Shows corresponding UDP port.
Timeout	Shows corresponding timeout value.
Retry	Shows corresponding retry times.
Tag Identifier	Shows corresponding tag identifier.
Target Parameter	Shows corresponding target parameter.

Click the **Add** button to add an entry in the list:

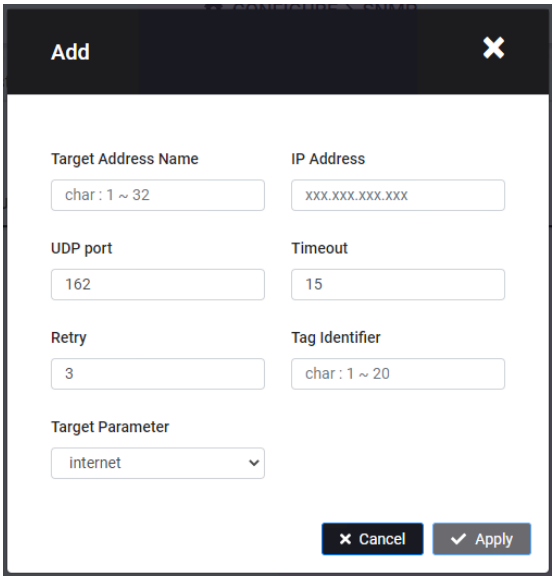

Figure 3-14 Target Address(Additional Screen)

3.9 Notify Settings

Figure 3-15 Notify Settings

Items	Descriptions
Notify Name	Shows corresponding Notify name.
Tag Identifier	Shows corresponding Tag Identifier; a tag is used to define a set of target addresses to receive the notification.
Notify Type	Shows corresponding Notify type (Traps or Infroms)

Click the **Add** button to add an entry in the list:

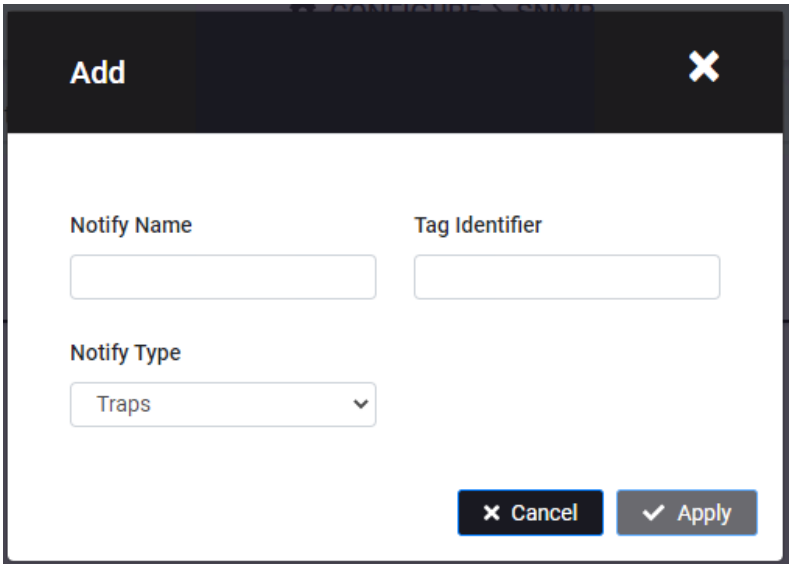

Figure 3-16 Notify Settings(Additional Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

4 Port Settings

Use this screen to view and configure switch port settings.

4.1 Port

The port settings page allows you change the configuration of the ports on the switch in order to find the best balance of speed and flow control according to your preferences. Configuring Gigabit ports require additional factors to be considered when arranging your preferences for the switch compared to 10/100 ports.

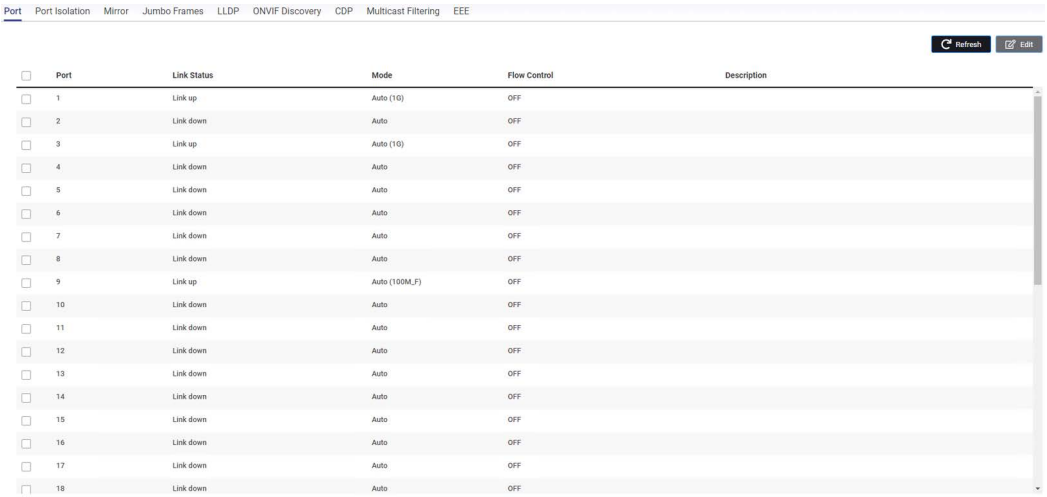

Figure 4-1 Port

Items	Descriptions
Port	Displays the port number.
Link Status	Indicates whether the link is up or down.

Items	Descriptions
Mode	Select the speed and the duplex mode of the Ethernet connection on this port. Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The switch uses IEEE 802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE 802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.

4.2 Port Isolation

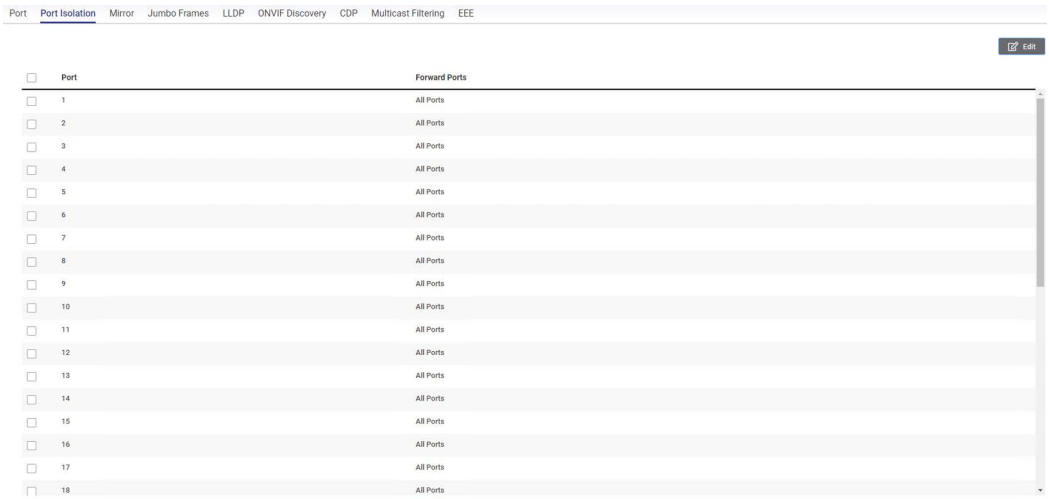

Figure 4-2 Port Isolation

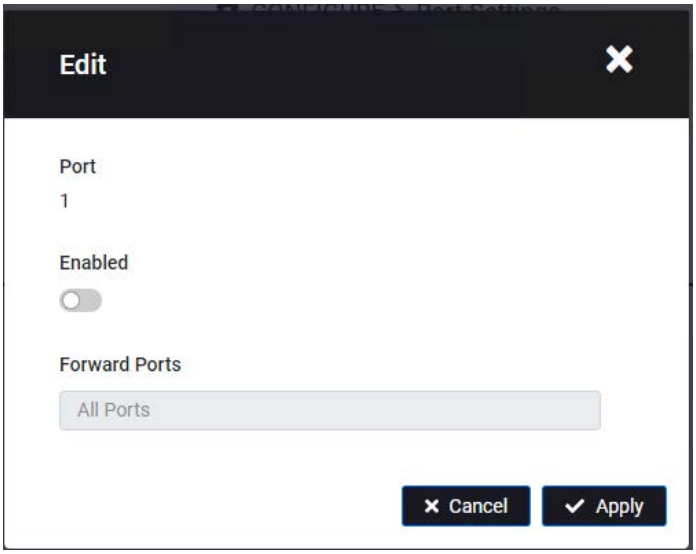

Figure 4-3 Port Isolation(Edit Screen)

Port Isolation feature provides L2 isolation between ports within the same broadcast domain. When enabled, Isolated ports can forward traffic to Not Isolated ports, but not to other Isolated ports. Not Isolated ports can send traffic to any port whether Isolated or Not Isolated. The default setting is Not Isolated.

Click **Apply** to update the system settings.

4.3 Mirror

Figure 4-4 Mirror

Mirror settings mirror network traffic by forwarding copies of incoming and outgoing packets from specific ports to a monitoring port. The packet that is copied to the monitoring port will be the same format as the original packet.

Port mirroring is useful for network monitoring and can be used as a diagnostic tool. Use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, detecting intrusions, monitoring, and predicting traffic patterns, and other correlating events. Port mirroring is needed for traffic analysis on a switch because a switch normally sends packets only to the port to which the destination device is connected. The analyzer captures and evaluates the data without affecting the client on the original port. Port mirroring can consume significant CPU resources while active, so be cautious of such usage when configuring the switch.

Items	Descriptions
Session ID	A number identifying the mirror session. This switch only supports up to 4 mirror sessions.
Destination Port	Select the port for traffic purposes from source ports mirrored to this port.
Egress/Ingress (Source TX/ RX Port)	Sets the source port from which traffic will be mirrored. TX Port: Only frames transmitted from this port are mirrored to the destination port. RX Port: Only frames received on this port are mirrored to the destination port. Both: Frames received and transmitted on this port are mirrored to the specified destination port. None: Disables mirroring for this port.
Egress & Ingress State	Select whether to enable or disable ingress traffic forwarding.
Session State	Select whether to enable or disable port mirroring.

4.4 Jumble Frame

Figure 4-5 Jumble Frame

Ethernet has used the 1500-byte frame size since its inception. Jumbo frames are network-layer PDUs that have a size much larger than the typical 1500-byte Ethernet Maximum Transmission Unit (MTU) size. Jumbo frames extend Ethernet to 9000 bytes, making them large enough to carry an 8 KB application datagram plus packet header overhead. If you intend to leave the local area network at high speeds, the dynamics of TCP will require you to use large frame sizes.

The switch supports a jumbo frame size of up to 9216 bytes. Jumbo frames need to be configured to work on the ingress and egress port of each device along the end-to-end transmission path. Furthermore, all devices in the network must also be consistent on the maximum jumbo frame size, so it is important to do a thorough investigation of all your devices in the communication paths to validate their settings.

Items	Description
Jumbo Frame	Enter the size of jumbo frame. The range is from 1522 to 9216 bytes.

Click **Apply** to update the system settings.

4.5 LLDP

Link Layer Discovery Protocol (LLDP) is the IEEE 802.1AB standard for switches to advertise their identity, major capabilities, and neighbors on the 802 LAN. LLDP allows users to view the discovered information to identify system topology and detect faulty configurations on the LAN. LLDP is essentially a neighbor discovery protocol that uses Ethernet connectivity to advertise information to devices on the same LAN and store information about the network. The information transmitted in LLDP advertisements flow in one direction only: from one device to its neighbors. This information allows the device to quickly identify a variety of other devices, resulting in a LAN that interoperates smoothly and efficiently.

LLDP transmits information as packets called LLDP Data Units (LLDPDUs). A single LLDPDU is transmitted within a single 802.3 Ethernet frame. A basic LLDPDU consists of a set of Type-Length-Value elements (TLV), each of which contains information about the device. A single LLDPDU contains multiple TLVs. TLVs are short information elements that communicate complex data. Each TLV advertises a single type of information.

4.5.1 Global Settings

Select whether to enable or disable the LLDP feature on the switch. Next, enter the Transmission Interval, Holdtime Multiplier, Reinitialization Delay parameter, and the Transmit Delay parameter. When finished, click Apply to update the system settings.

Figure 4-6 LLDP (Global Settings)

Items	Description
State	Select Enabled or Disabled to activate LLDP for the switch.
Transmission Interval	Enter the interval at which LLDP advertisement updates are sent. The default value is 30. The range is from 5 to 32768.

Items	Description
Holdtime Multiplier	Enter the amount of time that LLDP packets are held before packets are discarded and measured in multiples of the Advertised Interval. The default is 4. The range is from 2 to 10.
Reinitialization Delay	Enter the amount of time of delay before reinitializing LLDP. The default is 2. The range is from 1 to 10.
Transmit Delay	Enter the amount of time that passes between successive LLDP frame transmissions. The default is 2 seconds. The range is from 1 to 8191 seconds.

4.5.2 Local Device

LLDP devices must support chassis and port ID advertisement, as well as the system name, system ID, system description, and system capability advertisements. Here, you can view detailed LLDP information for the switch.

Figure 4-7 LLDP (Local Device)

Items	Description
Chassis ID Subtype	Displays the chassis ID type.
Chassis ID	Displays the chassis ID of the device transmitting the LLDP frame.
System Name	Displays the administratively assigned device name.
System Description	Describes the device.
Capabilities Supported	Describes the device functions.
Capabilities Enabled	Describes the device functions.

Items	Description
Port ID Subtype	Displays the port ID type.

4.5.3 Remote Device

LLDP devices must support chassis and port ID advertisement, as well as the system name, system ID, system description, and system capability advertisements. From here you can view detailed LLDP Information for the remote device.

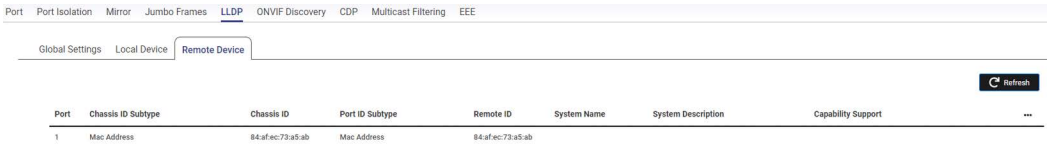

Figure 4-8 LLDP (Remote Device)

Items	Description
Port	Displays the port.
Chassis ID Subtype	Displays the chassis ID type.
Chassis ID	Displays the chassis ID of the device that is transmitting the LLDP frame.
Port ID Subtype	Displays the port ID type.
Remote ID	Displays the remote ID.
System Name	Displays the administratively assigned device name.
Time to Live	Displays the time to live.
Auto-Negotiation Supported	Displays state for the auto-negotiation supported.
Auto-Negotiation Enabled	Displays state for the auto-negotiation enabled.
Auto-Negotiation Advertised Capabilities	Displays the type of auto-negotiation advertised capabilities.
Operational MAU Type	Displays the type of MAU.
802.3 Maximum Frame Size	Displays the maximum size of 802.3 maximum frame.
802.3 Link Aggregation Capabilities	Displays the 802.3 Link Aggregation capabilities.
802.3 Link Aggregation Status	Displays the status of 802.3 Link Aggregation.
802.3 Link Aggregation Port ID	Displays the port ID of 802.3 Link Aggregation.

4.6 ONVIF Discovery

4.6.1 Global Settings

Figure 4-9 ONVIF Discovery(Global Settings)

4.6.2 Remote Device

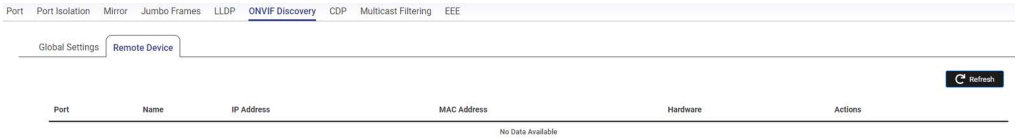

Figure 4-10 ONVIF Discovery(Remote Device)

4.7 CDP

4.7.1 Global Settings

Figure 4-11 CDP(Global Settings)

4.7.2 Port

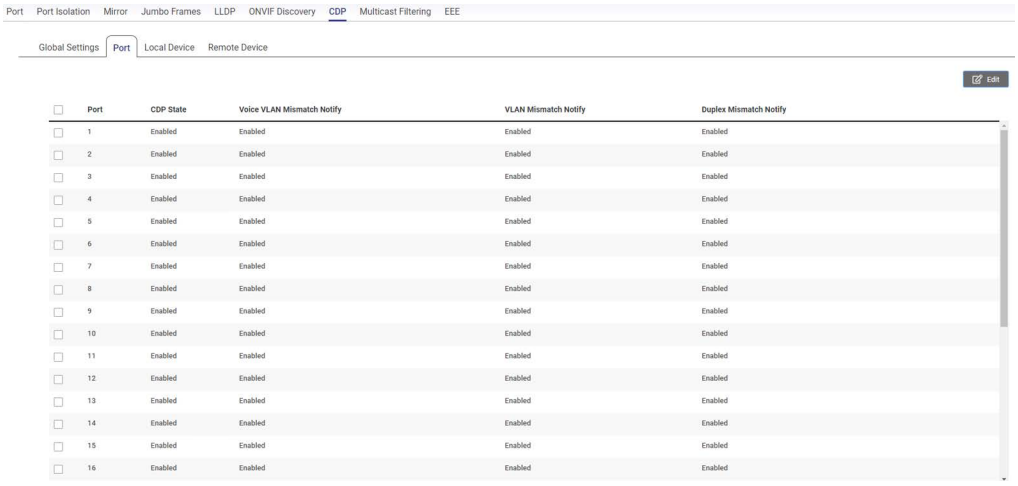

Figure 4-12 CDP(Port)

4.7.3 Local Device

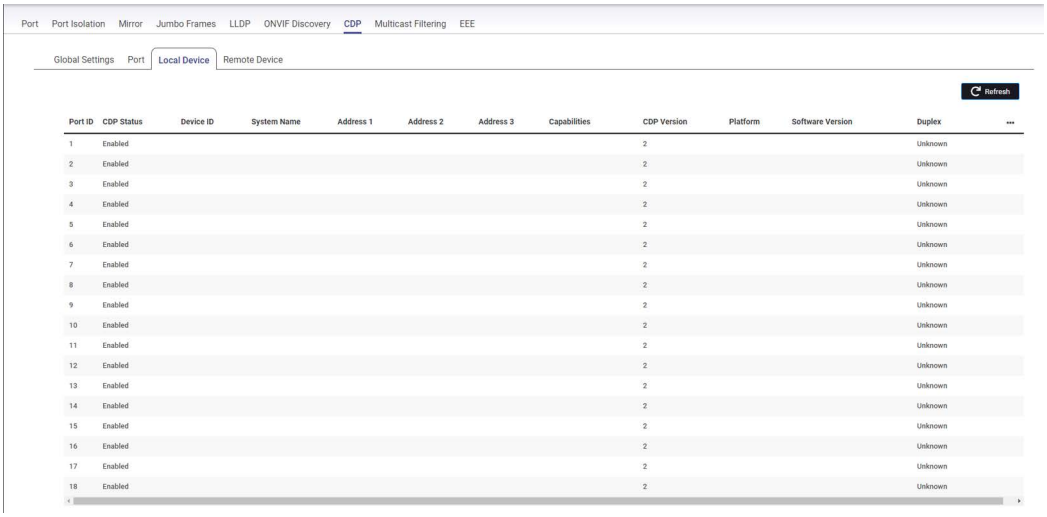

Figure 4-13 CDP(Local Device)

4.7.4 Remote Device

Figure 4-14 CDP(Remote Device)

4.8 Multicast Filtering

Figure 4-15 Multicast Filtering

Select Enabled or Disabled for Multicast Filtering.
Click **Apply** to save settings.

4.9 EEE

Energy Efficient Ethernet (EEE), an Institute of Electrical and Electronics Engineers (IEEE) 802.3az standard, reduces the power consumption of physical layer devices during periods of low link utilization. EEE saves energy by allowing PHY non-essential circuits to shut down when there is no traffic.

Network administrators have long focused on the energy efficiency of their infrastructure, and the EnGenius Layer 2 switch complies with the IEEE's Energy-Efficient Ethernet (EEE) standard. The EEE compliant switch offers users the ability to utilize power that Ethernet links use only during data transmission. Lower Power Idle (LPI) is the method for achieving the power saving during Ethernet ideal time.

Use the EEE configuration page to configure Energy Efficient Ethernet.

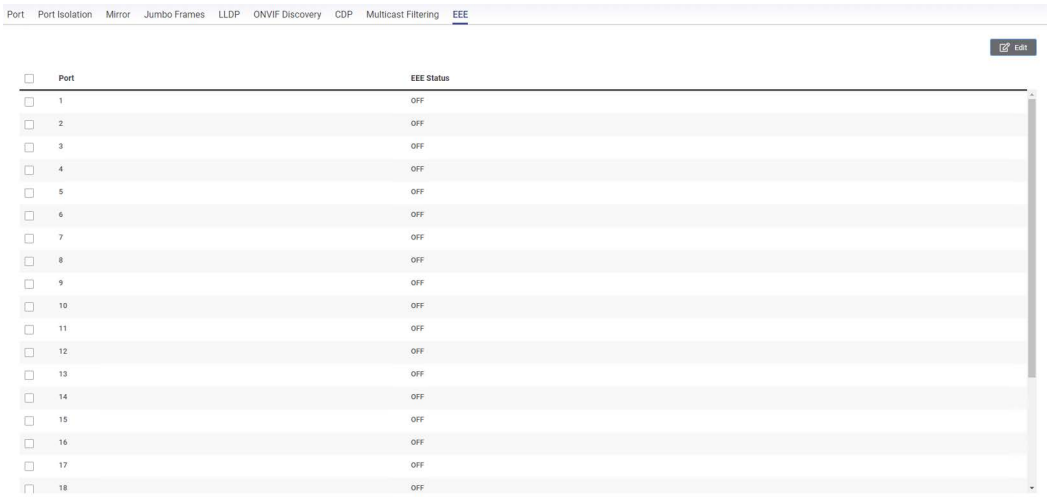

Figure 4-16 EEE

Item	Description
Port	Display the port for which the EEE setting is displayed.
EEE Status	Enable or disable EEE for the specified port.

5 Power Supply

5.1 PoE

The PoE Management screen contains system PoE information for monitoring the current power usage and assigns the total amount of power the switch can provide to all its PoE ports.

5.2 Power Budget

Figure 5-1 Power Budget

Temperature Tolerance Mode: Select Enabled or Disabled the Temperature Tolerance Mode, which limits the power supply capacity to allow operation even in a 60 degrees Celsius environment.
Click Apply to save the settings.

Total Power Budget: Enter the amount of power the switch can provide to all ports.
Consumed Power: Displays the total amount of power (in watts) currently being delivered to all PoE ports.

Click the **Apply** button to apply the changes or the **Reset** button to discard them.

5.3 PoE Port Settings

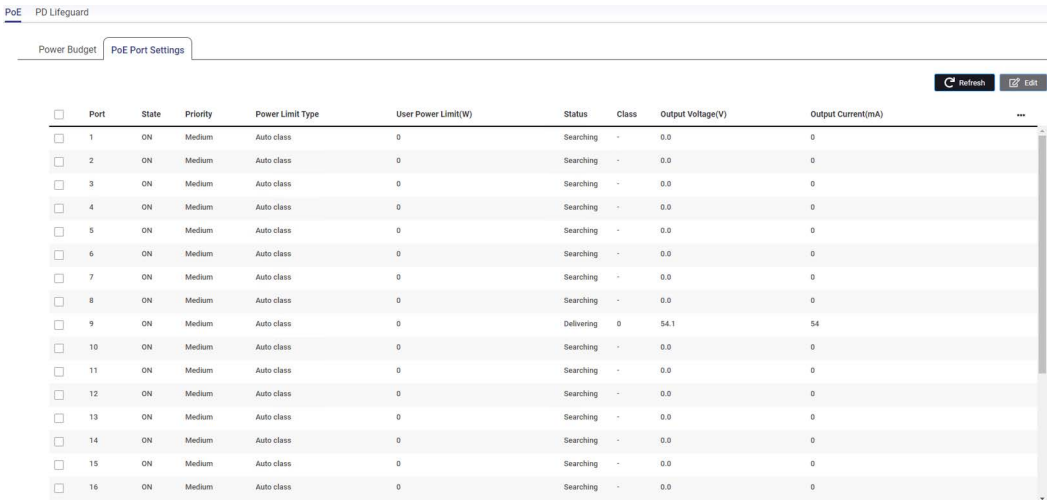

Figure 5-2 PoE Port Settings

Items	Descriptions
Port	Displays the specific port for which PoE parameters are defined. PoE parameters are assigned to the powered device that is connected to the selected port.
State	Displays the active participating members of the trunk group. Enable: Enables the Device Discovery protocol and provides power to the device using the PoE module. The Device Discovery protocol lets the device discover powered devices attached to device interfaces and learn their classification. Disable: Disables the Device Discovery protocol and halts the power supply delivering power to the device using the PoE module.
Priority	Select the port priority if the power supply is low. The field default is low. For example, if the power supply is running at 99% usage, and port 1 is prioritized as high, but port 6 is prioritized as low, port 1 is prioritized to receive power and port 6 may be denied power. Low: Sets the PoE priority level as low. Medium: Sets the PoE priority level as medium. High: Sets the PoE priority level as high. Critical: Sets the PoE priority level as critical.

Items	Descriptions
Power Limit Type	Shows the classification of the powered device. The class defines the maximum power that can be provided to the powered device.
User Power Limit (W)	Select this option to set the power limit on the value configured in the User Power Limit field. Set the maximum amount of power that can be delivered by a port. Note: The User Power Limit can only be implemented when the Class value is set to User-Defined.
Status	Shows the port's PoE status. The possible field values are: Delivering Power: The device is enabled to deliver power via the port. Disabled: The device is disabled from delivering power via the port. Test Fail: The powered device test has failed. For example, a port could not be enabled and cannot be used to deliver power to the powered device. Testing: The powered device is being tested. For example, a powered device is tested to confirm it is receiving power from the power supply. Searching: The device is currently searching for a powered device. Searching is the default PoE operational status. Fault: The device has detected a fault on the powered device when the port is forced on. For example, the power supply voltage is out of range, a short occurs, there is a communication error with PoE devices, or an unknown error occurs.
Class	The possible field values are: Class 0: The maximum power level at the Power Sourcing Equipment is 15.4 Watts. Class 1: The maximum power level at the Power Sourcing Equipment is 4.0 Watts. Class 2: The maximum power level at the Power Sourcing Equipment is 7.0 Watts. Class 3: The maximum power level at the Power Sourcing Equipment is 15.4 Watts. Class 4: The maximum power level at the Power Sourcing Equipment is 30 Watts.
Output Voltage (V)	Shows the output voltage in Volts.
Output Current (mA)	Shows the output current in mA.
Output Power (W)	Shows the output power in W.

Select the port and click **Edit** button to revise settings; users may also click the **Reset** button to discard them.

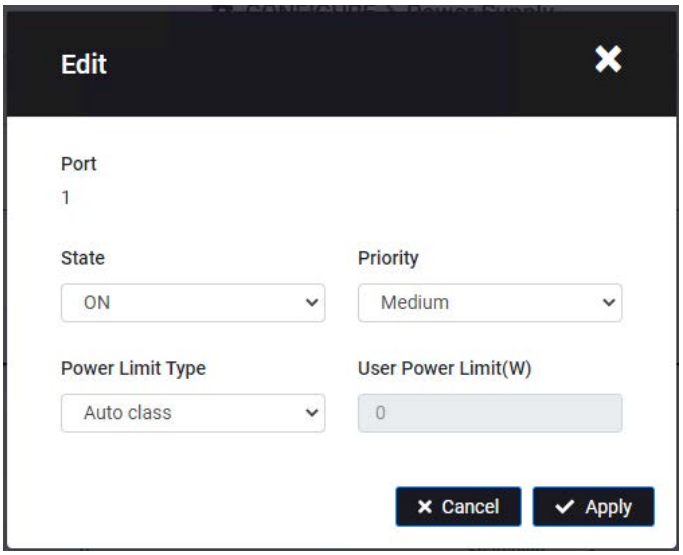

Figure 5-3 PoE Port Settings(Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

5.4 PD Lifeguard

5.4.1 Global Settings

Figure 5-4 Global Settings

5.4.2 Advanced Configuration

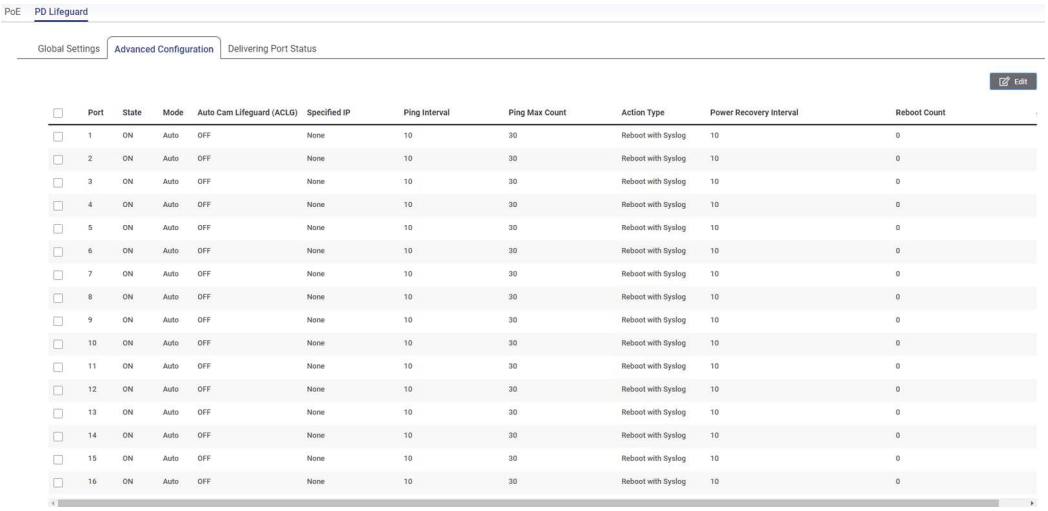

Figure 5-5 Advanced Configuration

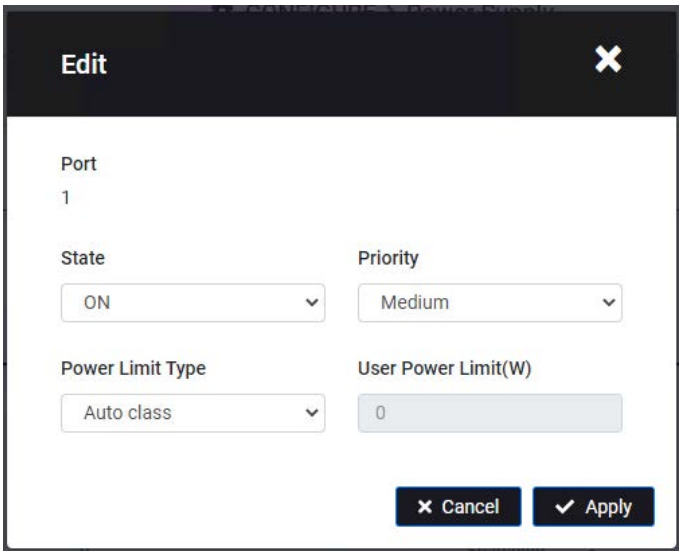

Figure 5-6 Advanced Configuration(Edit Screen)

5.4.3 Delivering Port Status

Figure 5-7 Delivering Port Status

Items	Descriptions
Port	Displays the port number.
State	Indicates whether enabled or disabled.
Mode	Displays the corresponding mode: Force Ping – Use Pinging method . Auto – LLDP & Ping (default)
Polling method	Displays the corresponding polling method.
MAC Address	Displays the corresponding MAC address.
Management IP	Displays the management IP.
Action Taken	Displays the corresponding action taken.

Click the **Refresh** button to get the latest status.

6 VLAN Settings

A virtual LAN (VLAN) is a group of ports that form a logical Ethernet segment on a Layer 2 switch which provides better administration, security, and management of multicast traffic. A VLAN is a network topology configured according to a logical scheme rather than a physical layout. When you use a VLAN, users can be grouped by logical function instead of physical location. All ports that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. VLANs let you logically segment your network into different broadcast domains so that you can group ports with related functions into their own separate, logical LAN segments on the same switch. This allows broadcast packets to be forwarded only between ports within the VLAN which can avoid broadcast packets being sent to all the ports on a single switch. A VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. VLANs also improve security by limiting traffic to specific broadcast domains.

6.1 802.1Q

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. The IEEE 802.1Q specification establishes a standard method for tagging Ethernet frames with VLAN membership information. The key for IEEE 802.1Q to perform its functions is in its tags. 802.1Q-compliant switch ports can be configured to transmit tagged or untagged frames. A tag field containing VLAN information can be inserted into an Ethernet frame. When using 802.1Q VLAN configuration, you configure ports to be a part of a VLAN group. When a port receives data tagged for a VLAN group, the data is discarded unless the port is a member of the VLAN group.

Figure 6-1 802.1Q

Item	Description
Enabled	Enables 802.1Q VLANs. This feature is enabled by default.
VID	Displays the VLAN ID for which the network policy is defined. The range of the VLAN ID is from 1 to 4094.
Name	Enter the VLAN name. You can use up to 32 alphanumeric characters.
Tagged Port	Frames transmitted from this port are tagged with the VLAN ID.
Untagged Port	Frames transmitted from this port are untagged.

NOTE:
The switch's default setting is to assign all ports to a single 802.1Q VLAN(VID 1).
Please keep this in mind when configuring the VLAN settings for the switch.

Figure 6-2 802.1Q(Add VLAN Screen)

6.2 VLAN Table

This table shows VLAN ID with its port members.

Figure 6-3 VLAN Table

Item	Description
VID	Displays the VLAN ID on the switch (range from 1 to 4094).
Name	Displays the VLAN name.
Status	Displays the VLAN status.
Protocol	Displays the protocol associated with this VID.
Port Status	Displays the member ports' status (either Tagged or Untagged).

6.3 PVID & Ingress Filter

When an untagged packet enters a switch port, the PVID (Port VLAN ID) will be attached to the untagged packet and forward frames to a VLAN specified VID part of the PVID. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address. If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the switch will drop the packet. Within the switch, different PVIDs mean different VLANs, so VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given switch. If no VLANs are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1.

Figure 6-4 PVID & Ingress Filter

Item	Description
Port	Displays the VLAN ID to which the PVID tag is assigned. Configure the PVID to assign untagged or tagged frames received on the selected port.
PVID	Enter the PVID value. The range is from 1 to 4094.
Accept Type	Select Tagged Only and Untagged Only from the list. Tagged Only: The port discards any untagged frames it receives. The port only accepts tagged frames. Untagged Only: Only untagged frames received on the port are accepted. All: The port accepts both tagged and untagged frames.
Ingress Filtering	Specify how you wish the port to handle tagged frames. Select Enabled or Disabled from the list. Enabled: Tagged frames are discarded if VID does not match the PVID of the port. Disabled: All frames are forwarded in accordance with the IEEE 802.1Q VLAN.

NOTE
To enable PVID functionality, the following requirements must be met:

- All ports must have a defined PVID.
- If no other value is specified, the default VLAN PVID is used.
- If you wish to change the port's default PVID, you must first create a VLAN that includes the port as a member.

Click **Edit** to update the system settings.

Figure 6-5 PVID & Ingress Filter(Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

6.4 GVRP

GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is based on the Generic Attribute Registration Protocol (GARP) and 802.1 Q, facilitating control of VLANs within a larger network. When GVRP is activated, it transmits and receives GARP Packet Data Units (GPDUs), allowing users to configure a VLAN on one switch and then propagating its information across the network, instead of the previously required creation of the VLAN on each switch in the network.

6.4.1 Global Settings

Select "Enabled" to let adjacent VLAN-aware devices exchange VLAN information with each other with the use of the Generic VLAN Registration Protocol (GVRP).

Figure 6-6 Global Settings

Click **Apply** button to update the system settings.

6.4.2 Port Settings

Once GVRP setting is enabled, each switch port can be edited further for related settings.

Figure 6-7 Port Settings

Figure 6-8 Port Settings(Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

6.5 VLAN Trunking

6.5.1 Global Settings

Figure 6-9 Voice Trunking(Global Settings)

6.5.2 Port Settings

Figure 6-10 VLAN Trunking(Port Settings)

Figure 6-11 VLAN Trunking(Port Settings_Edit Screen)

6.6 Voice VLAN

Enhance your Voice over IP (VoIP) service by configuring ports to carry IP voice traffic from IP phones on a specific VLAN. Voice VLAN provides QoS to VoIP, ensuring that the quality of the call does not deteriorate if the IP traffic is received erratically or unevenly.

6.6.1 Global Settings

Figure 6-12 Voice VLAN(Global Settings)

Items	Descriptions
Voice VLAN State	Select Disabled, Auto, or OUI for Voice VLAN on the switch.
Voice VLAN ID	Sets the Voice VLAN ID for the network. Only one Voice VLAN is supported on the switch.

Items	Descriptions
802.1p Remark	Enable this function to have outgoing voice traffic to be marked with the selected CoS value.
Remark CoS/802.1p	Defines a service priority for traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active on a port. (Range: 0 to 7; Default: 6)
Aging Time	The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of the voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop. The range for aging time is from 1 to 65535 minutes. The default is 1440 minutes.

Click **Apply** to update the system settings.

6.6.2 OUI Settings

The switches determine whether a received packet is a voice packet by checking its source MAC address. VoIP traffic has a pre-configured Organizationally Unique Identifiers (OUI) prefix in the source MAC address. You can manually add specific manufacturer's MAC addresses and description to the OUI table. All traffic received on the Voice VLAN ports from the specific IP phone with a listed OUI is forwarded on the voice VLAN.

Figure 6-13 Voice VLAN(OUI Settings)

Items	Descriptions
Index	Displays the VoIP sequence ID.

Items	Descriptions
OUI Address	Globally unique ID assigned to a vendor by the IEEE to identify VoIP equipment.
Description	Displays the ID of the VoIP equipment vendor.

To configure the OUI settings, click the **Edit** button to re-configure the specific entry. Click the **Delete** button to remove the specific entry and click the Add button to create a new OUI entry. Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Figure 6-14 Voice VLAN(OUI Settings_Add Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

6.6.3 Port Settings

Enhance your VoIP service further by configuring ports to carry IP voice traffic from IP phones on a specific VLAN. Voice VLAN provides QoS to VoIP, ensuring that the quality of voice does not deteriorate if the IP traffic is received unevenly. When VoIP device is connected to a specific port, this is used to configure switch port's Voice VLAN and assign CoS mode.

Figure 6-15 Voice VLAN(Port Settings)

Figure 6-16 Voice VLAN(Port Settings_Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

6.7 Private VLAN

Figure 6-17 Private VLAN

Figure 6-18 Private VLAN(Add Screen)

7 Spanning tree

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches. This allows the switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network and provide backup links which automatically take over when a primary link goes down.

Spanning Tree Protocol (STP) provides a tree topology for the switch. There are different types of Spanning tree versions supported, including Spanning Tree Protocol (STP) IEEE 802.1D, Multiple Spanning Tree Protocol (MSTP) IEEE 802.1w, and Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s. Please note that only one spanning tree can be active on the switch at a time.

7.1 Global Settings

Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on switches. Spanning Tree Protocol (STP) allows you to ensure that you do not create loops when you have redundant paths in the network. STP provides a single active path between two devices on a network in order to prevent loops from being formed when the switch is interconnected via multiple paths.

STP uses a distributed algorithm to select a bridging device that serves as the root for the spanning tree network. It does this by selecting a root port on each bridging device to incur the lowest path cost when forwarding a packet from that device to the root device. It then selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. Next, all ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, disabling all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops. STP provides a single active path

between two devices on a network in order to prevent loops from being formed when the switch is interconnected via multiple paths.

Once a stable network topology has been established, all bridges listen for Hello Bridge Protocol Data Units (BPDUs) transmitted from the Root Bridge of the Spanning Tree. If a bridge does not receive a Hello BPDU after a predefined interval (known as the Maximum Age), the bridge will assume that the link to the Root Bridge is down and unavailable. This bridge then initiates negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause the switch to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency. Once the STP is enabled and configured, primary links are established, and duplicated links are blocked automatically. The reactivation of the blocked links is also automatic.

7.1.1 STP

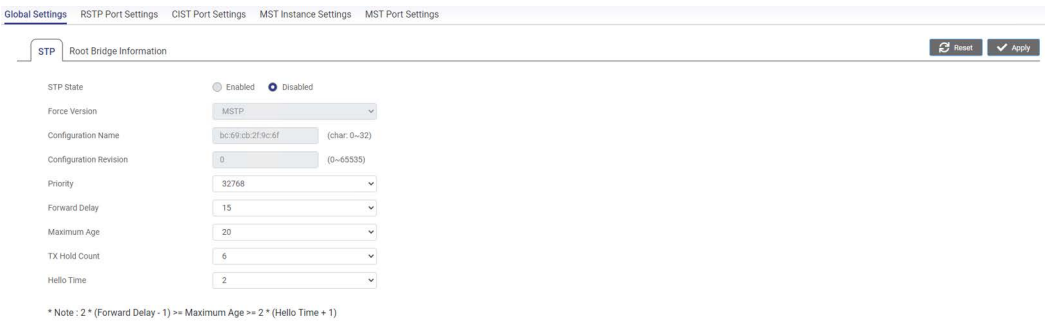

Figure 7-1 Global Settings(STP)

Items	Descriptions
STP	Select whether to enable or disable the spanning tree operation on the switch.
Force Version	Select the Force Protocol Version parameter for the switch. RSTP (Rapid Spanning Tree Protocol): IEEE 802.1w MSTP (Multiple Spanning Tree Protocol): IEEE 802.1s
Configuration Name	Specify the configuration name.
Configuration Revision	Specify the configuration revision.

Items	Descriptions
Priority	Assigns the priority for the bridge. When switches are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge.
Forward Delay	Configures the Switch Forward Delay Time. This is the time (in seconds) the root switch will wait before changing states (called listening to learning).
Maximum Age	Configures the bridge Switch Maximum Age Time. This is the amount of time a bridge waits before sending a configuration message. The default is 20 seconds.
Tx Hold Count	Configures Tx Hold Count to limit the maximum transmission rate of the switch where the number of BPDUs that can be transmitted during every hello time period ranges between a minimum of one and a maximum not exceeding Tx-Hold-Count values.
Hello Time	Configures the Switch Hello Time. This is the amount of time a bridge remains in a listening and learning state before forwarding packets.

Multiple Spanning Tree Protocol (MSTP) defined in IEEE 802.1s, enables multiple VLANs to be mapped to reduce the number of spanning-tree instances needed to support many VLANs. If there is only one VLAN in the network, a single STP works fine.

If the network contains more than one VLAN, however, the logical network configured by a single STP would work, but it becomes more efficient to use the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN groups. MSTP provides multiple forwarding paths for data traffic and enables load balancing.

STP and RSTP prevent loops from forming by ensuring that only one path exists between the end nodes in your network. RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. With STP, convergence can take up to a minute to complete in a larger network. This can result in the loss of communication between various parts of the network during the convergence process so STP can subsequently lose data packets during transmission.

RSTP on the other hand is much faster than STP. It can complete a convergence in seconds, so it greatly diminishes the possible impact the

process can have on your network compared to STP. RSTP reduces the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails and retain the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

Select whether to enable or disable the Spanning Tree function for the switch. Next, select whether you wish to enable STP, RSTP, or MSTP. Again, please note that only one Spanning tree function can be active at a time.

Click Apply to save settings.

7.1.2 Root Bridge Information

The Root Bridge serves as an administrative point for all Spanning Tree calculations to determine which redundant links to block in order to prevent network loops. From here, you can view all the information regarding the Root Bridge within the STP.

All other decisions in a spanning tree network, such as ports being blocked and ports being put in a forwarding mode, are made regarding a root bridge. The root bridge is the “root” of the constructed “tree” within a spanning tree network. Thus, the root bridge is the bridge with the lowest bridge ID in the spanning tree network. The bridge ID includes two parts: the bridge priority (2 bytes) and the bridge MAC address (6 bytes). The 802.1d default bridge priority is 32768. STP devices exchange Bridge Protocol Data Units (BPDUs) periodically. All bridges “listen” for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (called the Maximum Age), the bridge assumes that the link to the root bridge is down. The bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

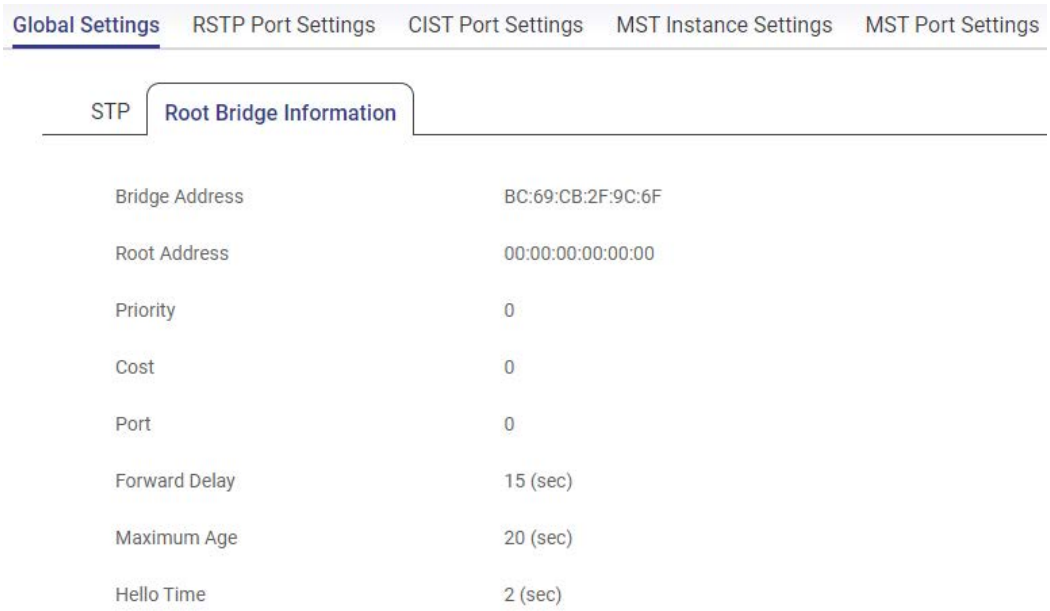

Figure 7-2 Global Settings(Root Bridge Information)

Items	Descriptions
Bridge Address	Displays the bridge MAC address.
Root Address	Displays the root bridge MAC address. Root in root bridge refers to the base of the spanning tree, which the switch could be configured for.
Priority	Displays the priority for the bridge. When switches are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge.
Cost	Display the root bridge cost.
Port	Display the root bridge port.
Forward Delay	Displays the Switch Forward Delay Time. This is the time (in seconds) the root switch will wait before changing states (called listening to learning).
Maximum Age	Displays the bridge Switch Maximum Age Time. This is the amount of time a bridge waits before sending a configuration message. The default is 20 seconds.
Hello Time	Displays the Switch Hello Time. This is the amount of time a bridge remains in a listening and learning state before forwarding packets. The default is 15 seconds.

7.2 RSTP Port Settings

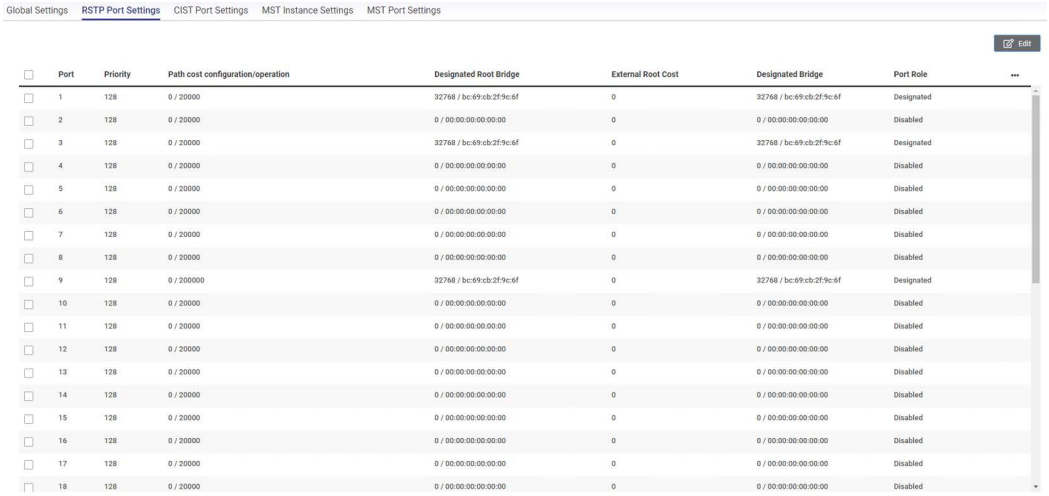

Figure 7-3 RSTP Port Settings

Items	Descriptions
Port	Port or trunked port identifier.
Priority	Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. When more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is from 0 to 240, in steps of 16; and the default is 128.
Path Cost	The Internal Path Cost setting allows you to specify the relative cost of sending spanning tree traffic through the interface to adjacent bridges within a spanning tree region.
Designated Root Bridge	Displays the root bridge; it is comprised using the bridge priority and the base MAC address of the bridge.
External Root Cost	Displays external root cost.
Designated Bridge	This is the bridge identifier of the bridge of the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Edge Port Conf/Oper	Displays the edge port state.

Items	Descriptions
P2P MAC Conf/Oper	Displays the P2P MAC Conf/Oper.
Port Role	Each bridge port that is enabled, assigned a port role within each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled.
Port State	The forwarding state of this port. The state parameters are Discarding, Learning, Forwarding, or Disabled.
Port Status	Displays either Enabled or Disabled for the port.

Choose the ports and click **Edit** to update the bridge settings.

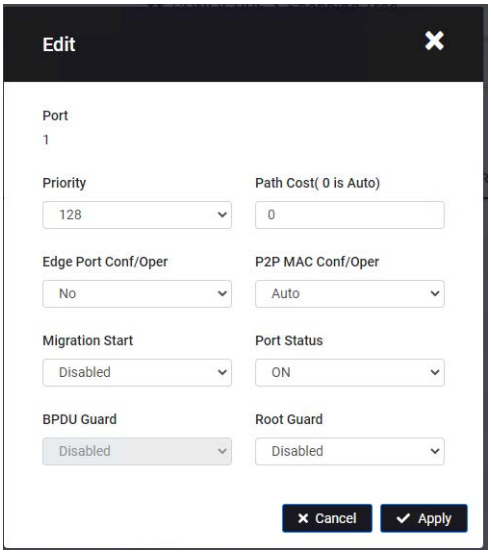

Figure 7-4 RSTP Port Settings(Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

7.3 CIST Port Settings

The Common Instance Spanning Tree (CIST) protocol is formed by the spanning tree algorithm running among bridges that support the IEEE 802.1w, IEEE 802.1s, and IEEE 802.1D standards. A Common and Internal Spanning Tree (CIST) represents the connectivity of the entire network and it is equivalent to a spanning tree in an STP/RSTP.

The CIST inside a Multiple Spanning Tree instance (MST) region is the same as the CST outside a region. All regions are bound together using a

CIST, which is responsible for creating loop-free topology across regions, whereas the MSTI controls topology inside regions. CST instances allow different regions to communicate between themselves. CST is also used for traffic within the region for any VLANs not covered by a MSTI. In an MSTP-enabled network, there is only one CIST that runs between MST regions and single spanning tree devices. A network may contain multiple MST regions and other network segments running RSTP. Multiple regions and other STP bridges are interconnected using a single CST.

Use the CIST Ports Settings page to configure and view STA attributes for interfaces when the spanning tree mode is set to STP or RSTP. You may use a different priority or path cost for ports of the same media type to indicate a preferred path or edge port to indicate if the attached device can support fast forwarding or link type to indicate a point-to-point connection or shared-media connection.

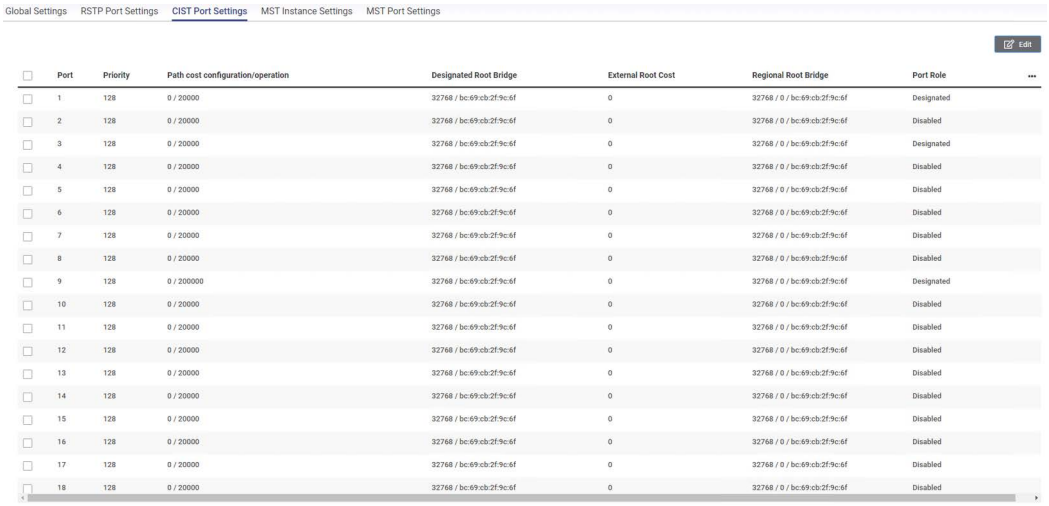

Figure 7-5 CIST Port Settings

Items	Descriptions
Port	Port or trunked port identifier.

Items	Descriptions
Priority	Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. When more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is from 0 to 240, in steps of 16; and the default is 128.
Internal Path Cost Conf/ Oper	The Internal Path Cost setting allows you to specify the relative cost of sending spanning tree traffic through the interface to adjacent bridges within a spanning tree region.
External Path Cost Conf/ Oper	The External Path Cost setting is used to calculate the cost of sending spanning tree traffic through the interface to reach an adjacent spanning tree region. The spanning tree algorithm tries to minimize the total path cost between each point of the tree and the root bridge.
Designated Root Bridge	Displays the root bridge for the CST. It is comprised using the bridge priority and the base MAC address of the bridge.
Internal Root Cost	This is the cost to the CIST regional root in a region.
External Root Cost	External root cost is the cost to the CIST root.
Regional Root Bridge	This is the bridge identifier of the CST regional root. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Port Cost	Enter the cost of the port.
Edge Port Conf/Oper	Displays the edge port state.
Designated Bridge	This is the bridge identifier of the bridge of the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Port Role	Each MST bridge port that is enabled is assigned a port role within each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled.
Port State	The forwarding state of this port. The state parameters are Discarding, Learning, Forwarding, or Disabled.

Choose the ports and click **Edit** to update the bridge settings.

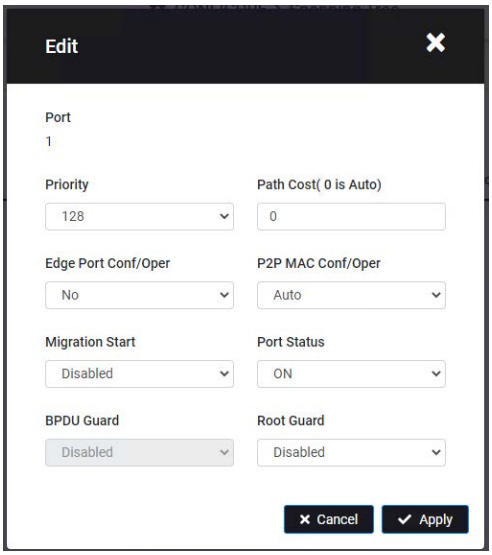

Figure 7-6 CIST Port Settings(Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

7.4 MST Instance Settings

This page displays the current MSTI configuration information for the switch. From here you can update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for ports you wish to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Note that lower priority values mean higher priorities for forwarding packets.

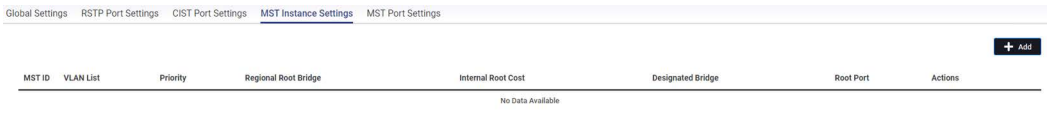

Figure 7-7 MST Instance Settings

Items	Descriptions
MST ID	Displays the ID of the MST group that is created. A maximum of 15 groups can be set for the switch.
Port	Displays port or trunked port ID.

Items	Descriptions
Priority	Select the bridge priority value for the MST. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if you set the priority to any value from 0 through 4095, the priority is set to 0. The default priority is 32768. The valid range is from 0 to 61440.
Internal Path Cost Conf	The Internal Path Cost setting allows you to specify the relative cost of sending spanning tree traffic through the interface to adjacent bridges within a spanning tree region.
Internal Path Cost Oper	Displays the operation cost of the path from this bridge to the root bridge.
Regional Root Bridge	This is the bridge identifier of the CST regional root. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Root Cost	Displays the path cost to the designated root for the selected MST instance.
Designated Bridge	Displays the bridge identifier of the bridge for the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Port Cost	This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within an STP instance. Selecting this parameter with a value in the range of 1 to 200000000 will set the quickest route when a loop occurs. A lower internal cost represents a quicker transmission. Selecting 0 (zero) for this parameter will set the quickest optimal route automatically for an interface.
Port Role	Each MST bridge port that is enabled is assigned a port role for each spanning tree. The port role is one of the following values: Root, Designated, Alternate, Backup, Master, or Disabled.

Items	Descriptions
Port State	Indicates the current STP state of a port. If enabled, the port state determines what forwarding action is taken regarding traffic. The possible port states are: Disabled: STP is disabled on the port. The port forwards traffic while learning MAC addresses. Blocking: The port is blocked and cannot be used to forward traffic or learn MAC addresses. Listening: The port is in listening mode. The port cannot forward traffic or learn MAC addresses in this state. Learning: The port is in learning mode. The port cannot forward traffic. However, it can learn new MAC addresses. Forwarding: The port is in forwarding mode. The port can forward traffic and learn new MAC addresses in this state.

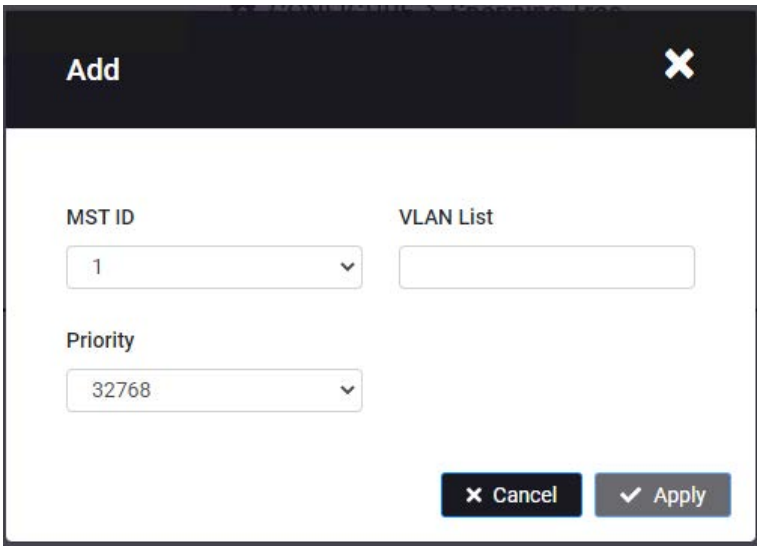

Figure 7-8 MST Instance Settings(Add Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

7.5 MST Port Settings

Figure 7-9 MST Port Settings

Items	Descriptions
MST ID	Displays the ID of the MST group that is created. A maximum of 15 groups can be set for the switch.
Port	Displays port or trunked port ID.
Priority	Select the bridge priority value for the MST. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if you set the priority to any value from 0 through 4095, the priority is set to 0. The default priority is 32768. The valid range is from 0 to 61440.
Internal Path Cost Conf	The Internal Path Cost setting allows you to specify the relative cost of sending spanning tree traffic through the interface to adjacent bridges within a spanning tree region.
Internal Path Cost Oper	Displays the operation cost of the path from this bridge to the root bridge.
Regional Root Bridge	This is the bridge identifier of the CST regional root. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Root Cost	Displays the path cost to the designated root for the selected MST instance.

Select the port and click the Edit button to update the settings:

8 Link Aggregation

A Link Aggregation Group (LAG) optimizes port usage by linking a group of ports together to form a single, logical, higher-bandwidth link. Aggregating ports multiplies the bandwidth and increases port flexibility for the switch. Link Aggregation is most used to link a bandwidth intensive network device (or devices), such as a server, to the backbone of a network.

The participating ports are called members of a port trunk group. Since all ports of the trunk group must be configured to operate in the same manner, the configuration of one port of the trunk group is applied to all ports of the trunk group. Thus, you will only need to configure one of any of the ports in a trunk group. A specific data communication packet will always be transmitted over the same port in a trunk group. This ensures the delivery of individual frames of a data communication packet will be received in the correct order. The traffic load of the LAG will be balanced among the ports according to aggregate arithmetic. If the connections of one or several ports are broken, the traffic of these ports will be transmitted on the normal ports to guarantee reliable connection.

When you aggregate ports, the ports and LAG must fulfill the following conditions:

- All ports within a LAG must be the same media/format type.
- A VLAN is not configured on the port.
- The port is not assigned to another LAG.
- The Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in the LAG have the same ingress filtering and tagged modes.
- All ports in the LAG have the same back pressure and flow control modes.
- All ports in the LAG have the same priority.
- All ports in the LAG have the same transceiver type.
- Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.

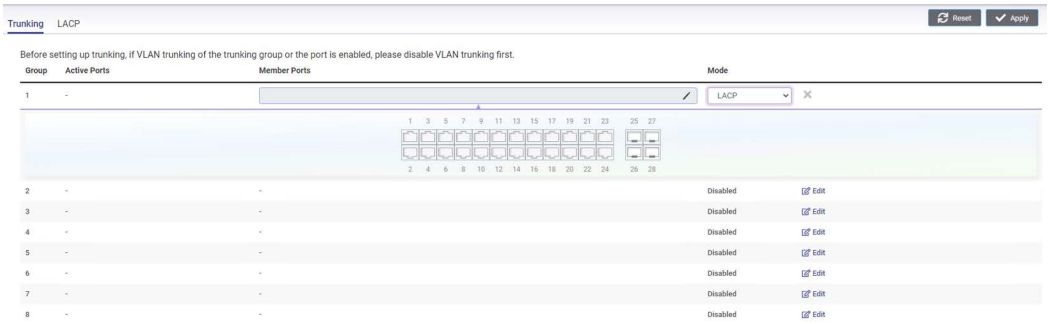

Figure 8-1 Link Aggregation

LACP is a dynamic protocol which helps to automate the configuration and maintenance of LAGs. The main purpose of LACP is to automatically configure individual links to an aggregate bundle, while adding new links and helping to recover from link failures if the need arises. LACP can monitor to verify if all the links are connected to the authorized group. LACP is a standard in computer networking; hence, LACP should be enabled on the switch's trunk ports initially for both the participating switches/devices that support the standard, to use it.

8.1 Trunking

Port trunking allows you to assign physical links to one logical link that functions as a single, higher-speed link, providing dramatically increased bandwidth. Use port trunking to bundle multiple connections and use the combined bandwidth as if it were a single larger “pipe.”

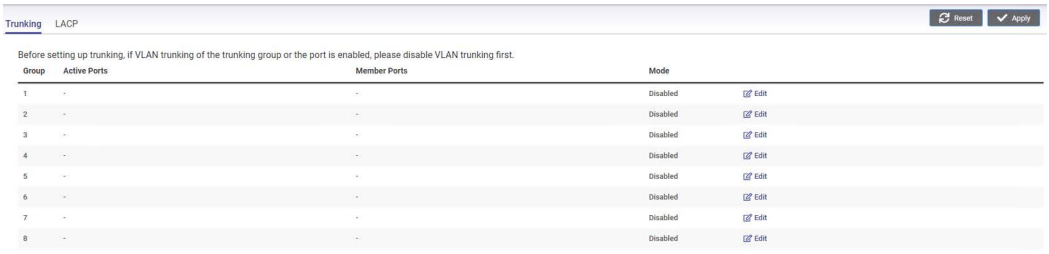

Figure 8-2 Link Aggregation(Trunking)

Important:
You must enable Trunk Mode before you can add a port to a trunk group.

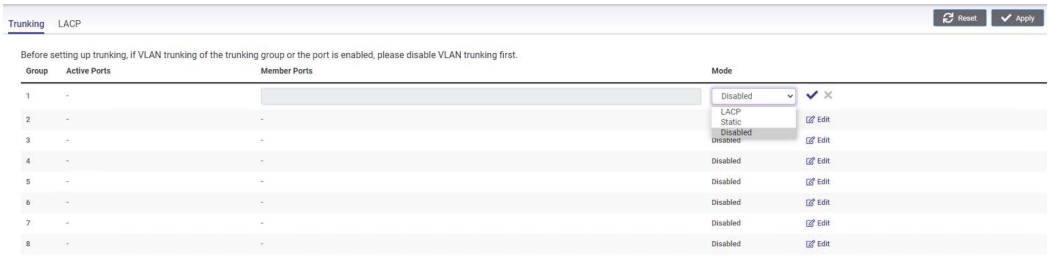

Figure 8-3 Link Aggregation(Trunking_Setting Screen)

Items	Descriptions
Group	Displays the number of the given trunk group. You can utilize up to 8 link aggregation groups with each group consisting up to 8 ports on the switch.
Active Ports	Displays the active participating members of the trunk group.
Member Port	Select the ports you wish to add to the trunk group. Up to eight ports per group can be assigned. Static: The Link Aggregation is configured manually for specified trunk group. LACP: The Link Aggregation is configured dynamically for specified trunk group.
Mode	LACP allows for the automatic detection of links in a port trunking group when connected to a LACP-compliant switch. You will need to ensure that both the switch and the device it's connected to are in the same mode for them to function; otherwise, they will not work. Static configuration is used when connecting to a switch that does not support LACP.

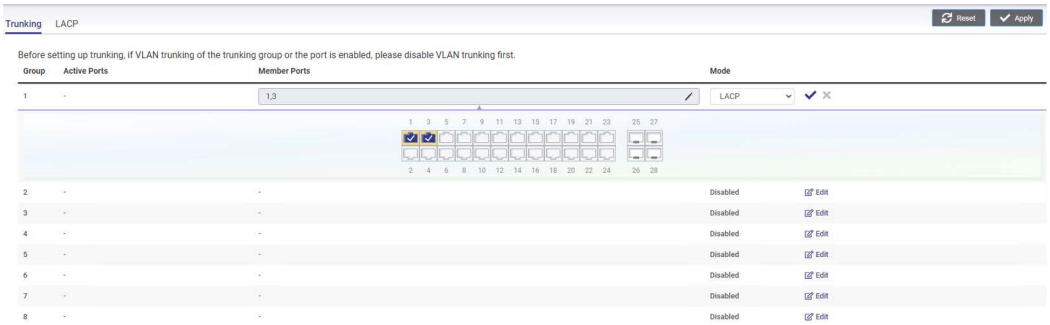

Figure 8-4 LACP Mode for Trunking Configuration

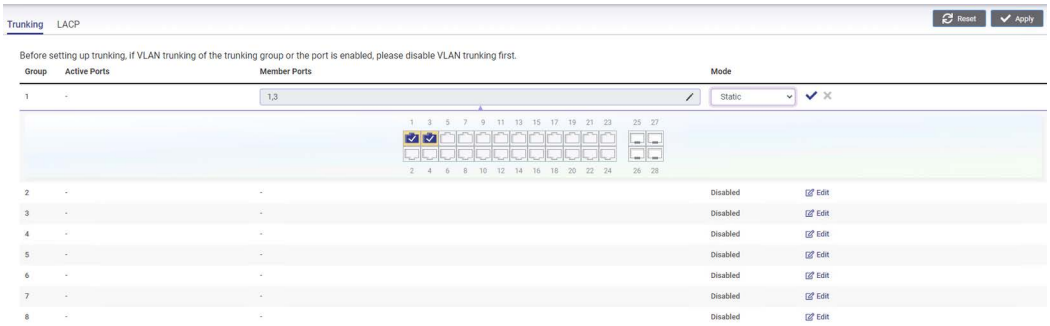

Figure 8-5 Static Mode for Trunking Configuration

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

8.2 LACP

8.2.1 Settings

Assign a system priority to run with Link Aggregation Control Protocol (LACP), which will become a backup link if another link goes down. The lowest system priority can make decisions about which ports it is actively running in case a link goes down. If two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port. If a LAG already exists with the maximum number of allowed port members, and LACP is subsequently enabled on another port using a higher priority than an existing member, the newly configured port will replace the existing port member that has a lower priority. A smaller number indicates a higher priority level. The range is from 0-65535 and default is 32768.

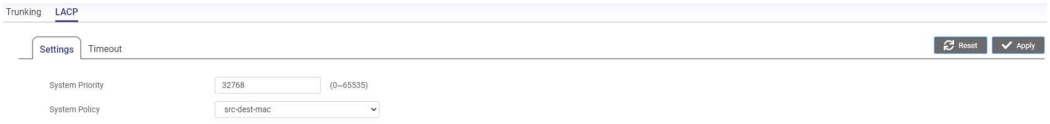

Figure 8-6 LACP(Settings)

Click **Apply** to save settings.

Items	Descriptions
System Priority	Enter the LACP priority value to the system. The default is 32768 and the range is from 1 to 65535.
System Policy	Select the system policy from the drop-down list.

8.2.2 Timeout

Link Aggregation Control Protocol (LACP) allows the exchange of information regarding the link aggregation between two members of the aggregation. The LACP Time Out value is measured in a periodic interval. Check first whether the port in the trunk group is up. When the interval expires, it will be removed from the trunk. Set a Short Timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. The default value for LACP time out is Long Timeout.

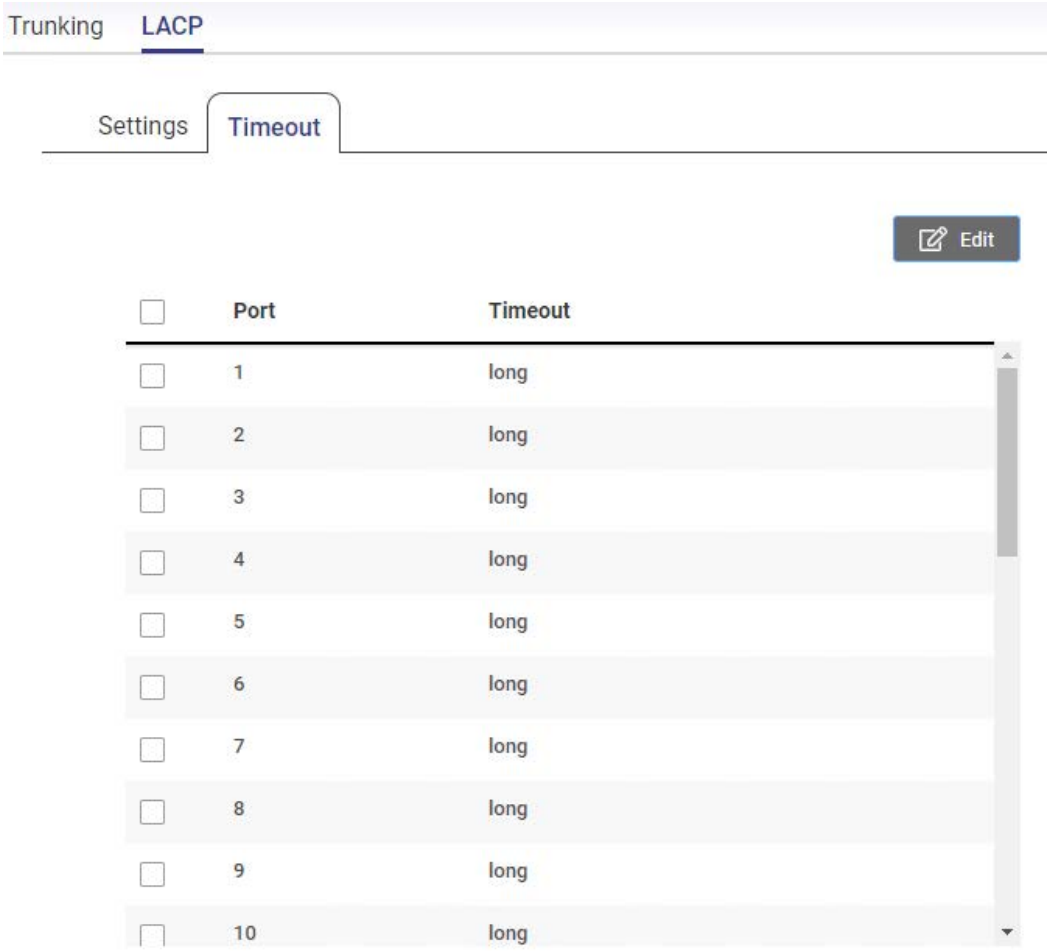

Figure 8-7 LACP(Timeout)

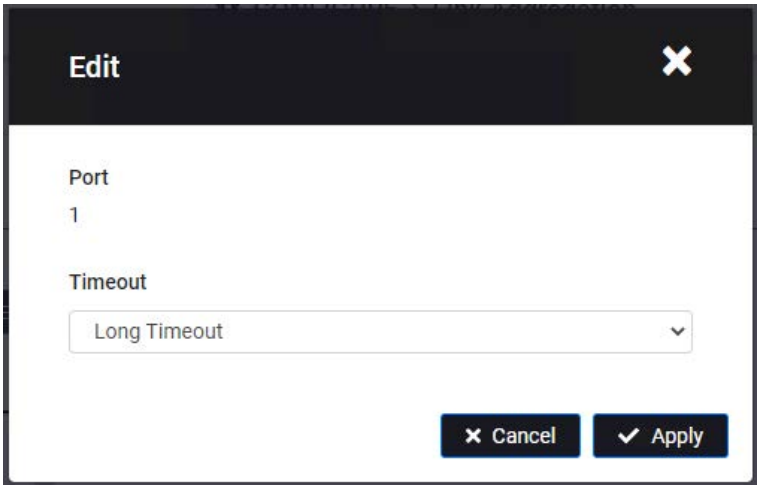

Figure 8-8 LACP(Timeout_Edit Screen)

Items	Descriptions
Timeout	Select the administrative LACP timeout. **Long Timeout**: The LACP PDU will be sent for every 30 seconds. The LACP timeout value is 90 seconds. **Short Timeout**: The LACP PDU will be sent every second. The timeout value is 3 seconds.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

9 L3 Protocols

9.1 IGMP Snooping

Internet Group Management Protocol (IGMP) Snooping allows a switch to forward multicast traffic intelligently. Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any host that wishes to receive the multicast register with their local multicast switch.

A multicast group is a group of end nodes that want to receive multicast packets from a multicast application. After joining a multicast group, a host node must continue to periodically issue reports to remain a member. Any multicast packets belonging to that multicast group are then forwarded by the switch from the port.

A switch supporting IGMP Snooping can passively snoop on IGMP Query, Report, and Leave packets transferred between IP Multicast switches and IP Multicast hosts to determine the IP Multicast group membership. IGMP Snooping checks IGMP packets passing through the network and configures multicasting accordingly. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. It enables the switch to forward packets of multicast groups to those ports that have validated host nodes. The switch can also limit flooding of traffic to IGMP designated ports. This improves network performance by restricting the multicast packets only to switch ports where host nodes are located. IGMP Snooping significantly reduces overall Multicast traffic passing through your switch. Without IGMP Snooping, Multicast traffic is treated in the same manner as a broadcast transmission, which forwards packets to all ports on the network.

Items	Descriptions
IGMPv1	Defined in RFC 1112. An explicit join message is sent to the switch, but a timeout is used to determine when hosts leave a group.
IGMPv2	Defined in RFC 2236. Adds an explicit leave message to the join message so that the switch can more easily determine when a group has no interested listeners on a LAN.
IGMPv3	Defined in RFC 3376. Support for a single source of content for a multicast group. When IGMPv3 snooping and multicast filtering function are enabled simultaneously, it may cause issues with the use of RIP/OSPF. Please avoid placing MU series switching hubs with multicast filtering functionality in conjunction with IGMP snooping between L3 Switching hubs.

9.1.1 Global Settings

Click to enable or disable the IGMP Snooping feature for the switch. Next, select whether you wish to enable or disable the Report Suppression feature for the switch.

Figure 9-1 IGMP Snooping(Global Settings)

Items	Descriptions
Status	Select to enable or disable IGMP Snooping on the switch. The switch snoops all IGMP packets it receives to determine which segments should receive packets directed to the group address when enabled. The default setting is: Disabled.
Report Suppression	Select whether Report Suppression is Enabled or Disabled for IGMP Snooping. The Report Suppression feature limits the amount of membership reports the member sends to multicast capable routers.

Click **Apply** to update the system settings.

9.1.2 Port Settings

Review or configure Fast leave option per switch port.

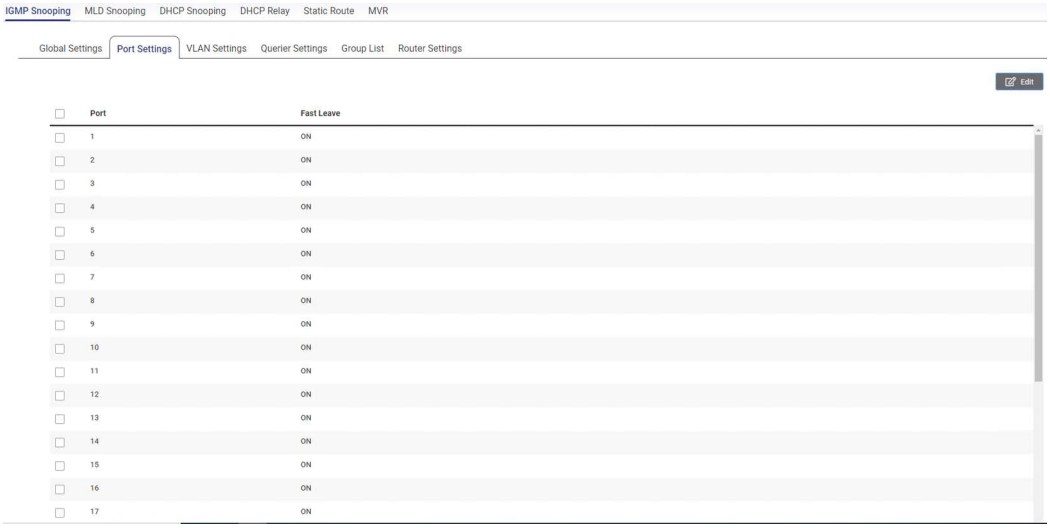

Figure 9-2 IGMP Snooping(Port Settings)

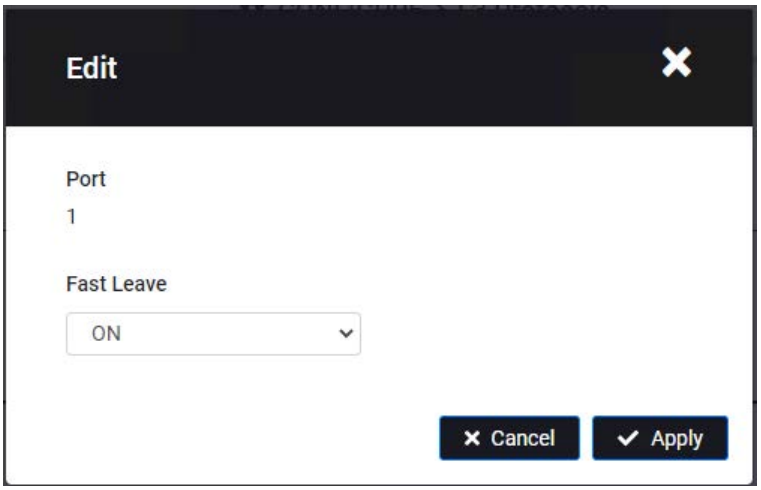

Figure 9-3 IGMP Snooping(Port Settings_Edit)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

If Fast Leave is not used, a multicast querier will send a GS-query message when an IGMPv2 group leave message is received. The querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period. If Fast Leave is enabled, the switch assumes that only one host is connected to the port. Therefore, Fast Leave should only be enabled on a port if it is connected to only one IGMP-enabled device.

Fast Leave is supported with IGMPv2 and IGMPv3 Snooping when IGMP Snooping is enabled. Fast Leave does not apply to a port if the switch has learned that a multicast querier is attached to it.
Fast Leave can improve bandwidth usage for a network which frequently experiences many IGMP host add and leave requests.

9.1.3 VLAN Settings

Use the IGMP Snooping VLAN Settings to configure IGMP Snooping settings for VLANs on the system. The switch performs IGMP Snooping on VLANs that send IGMP packets. You can specify the VLANs that IGMP Snooping should be performed on. Choose from the drop-down box whether to enable or disable IGMP Snooping. Next, choose the version of IGMP Snooping.

Figure 9-4 IGMP Snooping(VLAN Settings)

Items	Descriptions
VLAN ID	Displays the VLAN ID.
IGMP Snooping Status	Enables or disables the IGMP Snooping feature for the specified VLAN ID.
Version	Select the IGMP version you wish to use. If an IGMP packet received by the interface has a version higher than the specified version, this packet will be dropped.

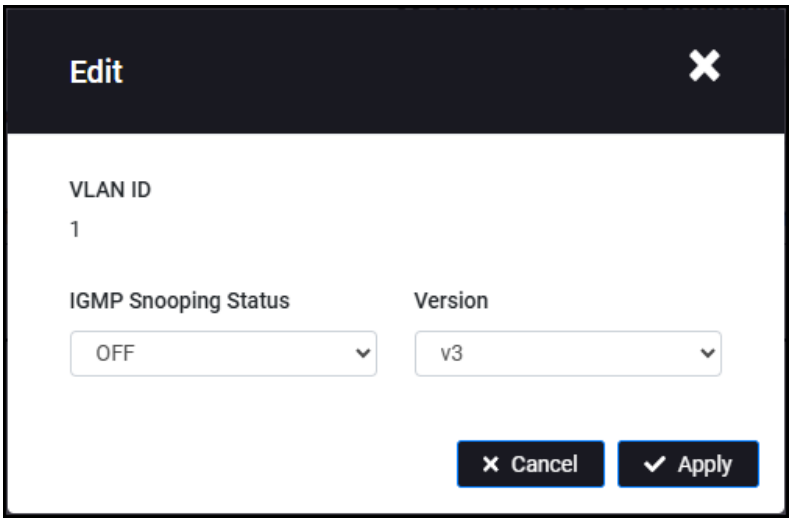

Figure 9-5 IGMP Snooping(VLAN Settings_Edit)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

9.1.4 Querier Settings

IGMP Snooping requires that one central switch to periodically query all end devices on the network to announce their multicast memberships and this central device is the IGMP querier. The snooping switch sends out periodic queries with a time interval equal to the configured querier query interval. The IGMP query keeps the switch updated with the current multicast group membership information. If the switch does not receive the updated membership information, then it will stop forwarding multicasts to specified VLANs.

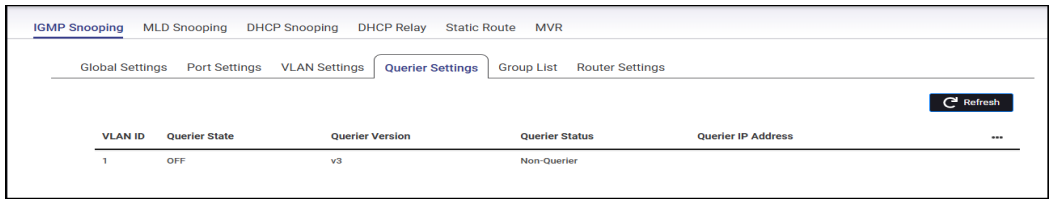

Figure 9-6 IGMP Snooping(Querier Settings)

Items	Descriptions
VLAN ID	Displays the VLAN ID.
Querier State	Select whether to enable or disable the IGMP querier state for the specified VLAN ID. A querier can periodically ask their hosts if they wish to receive multicast traffic. The querier feature will check whether hosts wish to receive multicast traffic when enabled. An elected querier will assume the role of querying the LAN for group members and then propagate the service requests onto any upstream multicast switch to ensure that it will continue to receive the multicast service. This feature is only supported for IGMPv1 and v2 snooping.
Querier Version	Display the version of IGMP packet that will be sent by this port. If an IGMP packet received by the port has a version higher than the specified version, this packet will be dropped.
Querier Status	Display the querier status.
Interval	Enter the amount of time in seconds between general query transmissions. The default is 125 seconds.
Max Response Interval	Enter the maximum response time used in the queries that are sent by the snooping querier. The default is 10 seconds.
Startup Query Counter	Enter the number of the startup query counter.

Items	Descriptions
Startup Query Interval	Specify the Startup Query Interval.

9.1.5 Group List

The Group List displays VLAN ID, group IP address, and members port in the IGMP Snooping list.

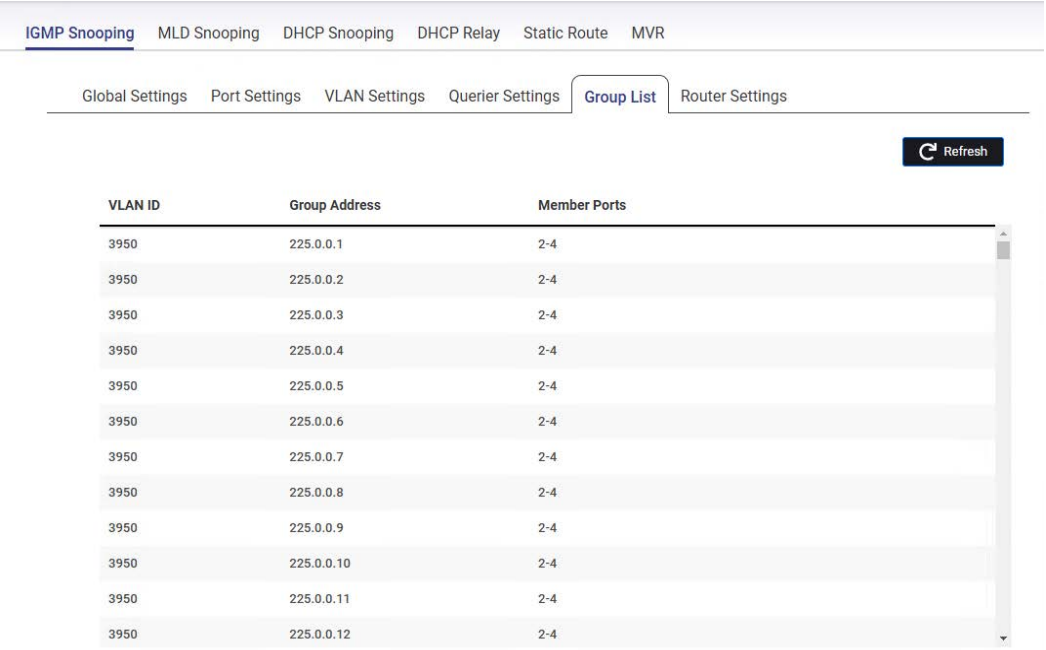

Figure 9-7 IGMP Snooping(Group List)

9.1.6 Router Settings

The Router Settings shows the learned multicast router attached port if the port is active and a member of the VLAN. Select the VLAN ID you would like to configure and enter the Static and Forbidden ports for the specified VLAN IDs. All IGMP packets snooped by the switch will be forwarded to the multicast router reachable from the port.

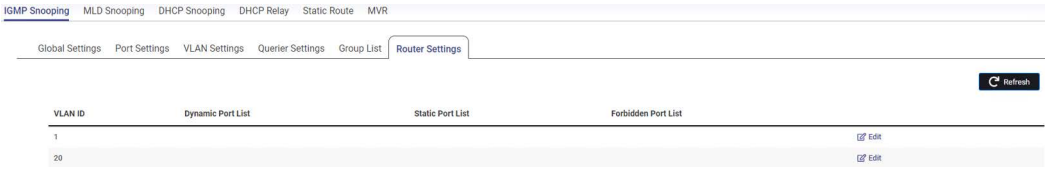

Figure 9-8 IGMP Snooping(Router Settings)

Items	Descriptions
VLAN ID	Displays the VLAN ID.
Dynamic Port List	Displays router ports that have been dynamically configured.
Static Port list	Designates a range of ports as being connected to multicast-enabled routers. Ensures that all the packets will reach the multicast-enabled router.
Forbidden Port List	Designates a range of ports as being disconnected to multicast-enabled routers. Ensures that the forbidden router port will not propagate routing packets out.

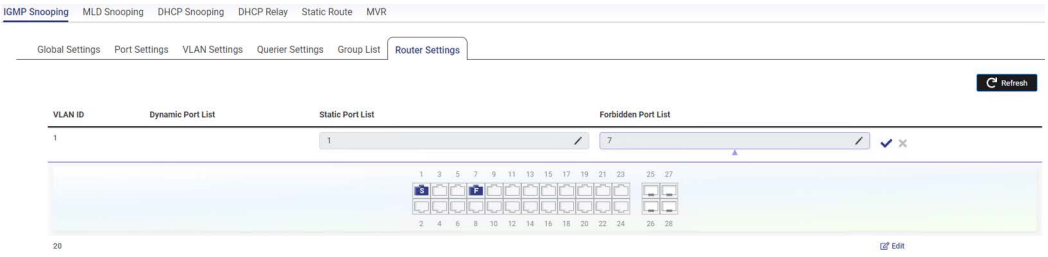

Figure 9-9 IGMP Snooping(Router Settings_Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

9.2 DHCP Snooping

This feature provides an extra layer of security by filtering untrusted DHCP messages where users can specify authorized DHCP servers for the networks and connect to the switch's trusted ports to serve underlying clients on this switch.

9.2.1 Global Settings

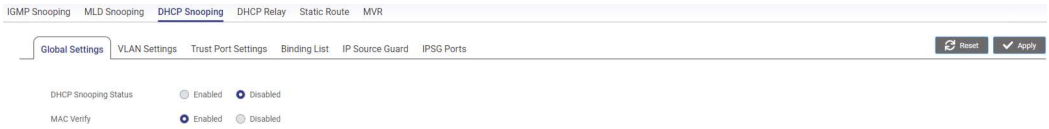

Figure 9-10 DHCP Snooping(Global Settings)

Items	Descriptions
DHCP Snooping Status	Select to enable or disable the DHCP Snooping feature.
MAC Verify	Select to enable or disable the MAC address verification feature.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

9.2.2 VLAN Settings

This page lists the VLANs configured on the switch with DHCP Snooping default disabled.

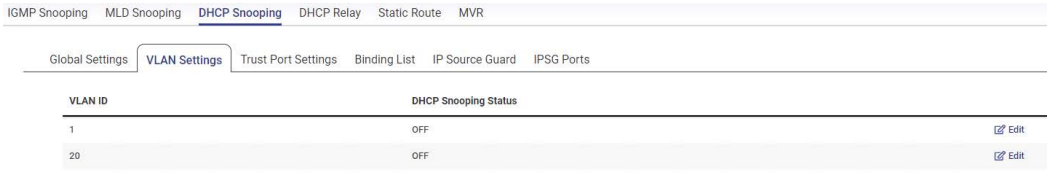

Figure 9-11 DHCP Snooping(VLAN Settings)

Users can click **Edit** button to enable DHCP snooping on a specific VLAN.

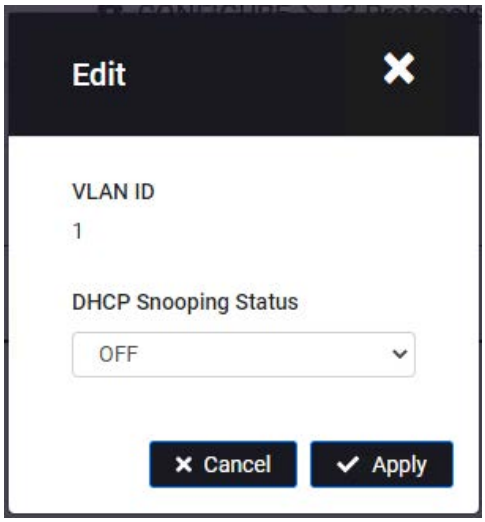

Figure 9-12 DHCP Snooping(VLAN Settings_Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

9.2.3 Trust Port Settings

Switch ports can be configured as either trusted or untrusted ports, respectively.

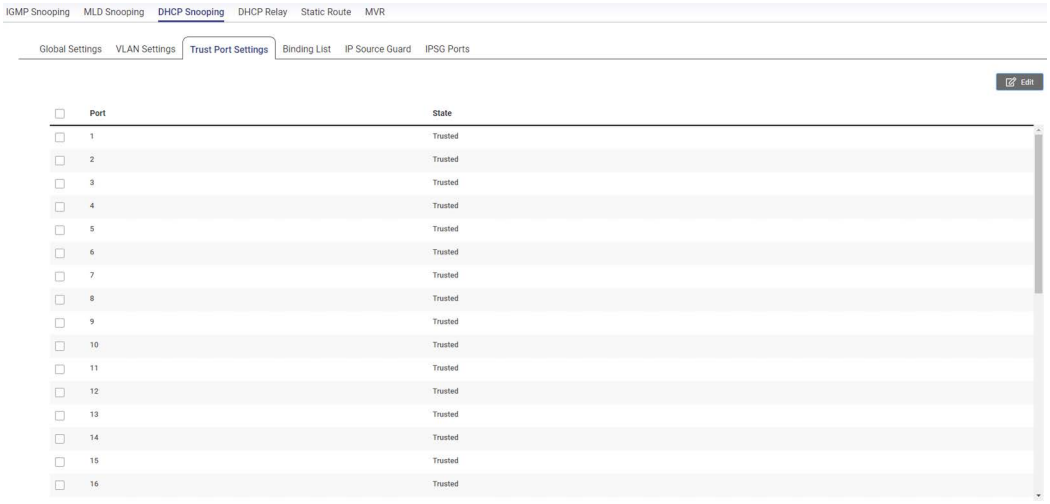

Figure 9-13 DHCP Snooping(Trust Port Settings)

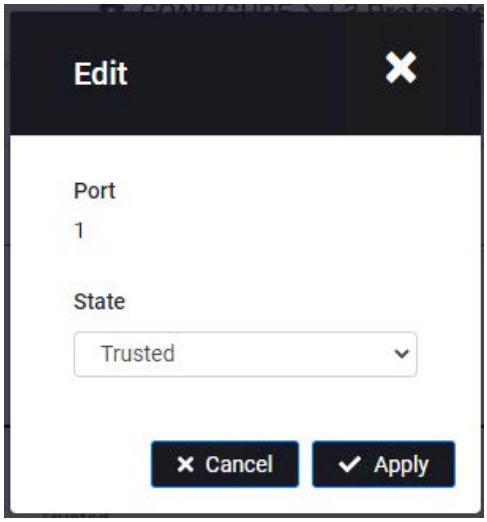

Figure 9-14 DHCP Snooping(Trust Port Settings_Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

9.2.4 Binding List

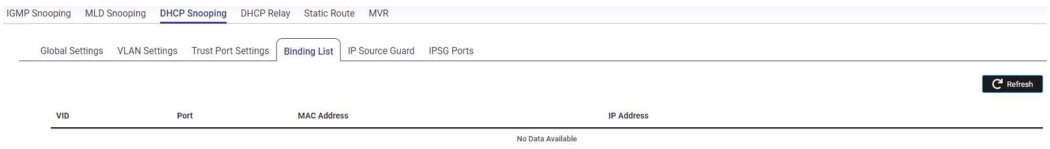

Figure 9-15 DHCP Snooping(Binding List)

9.2.5 IP Source Guard

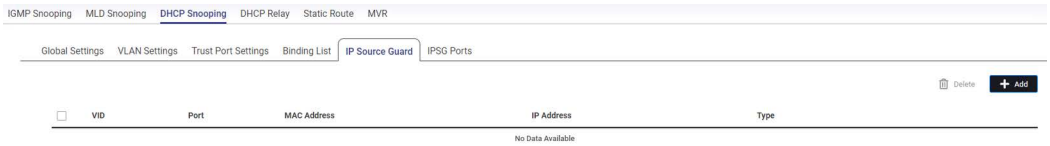

Figure 9-16 DHCP Snooping(IP Source Guard)

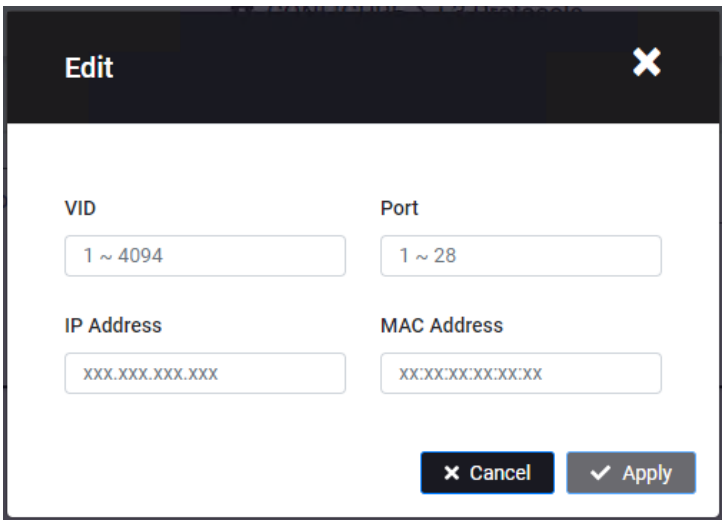

Figure 9-17 DHCP Snooping(IP Source Guard_Edit Screen)

9.2.6 IPSG Ports

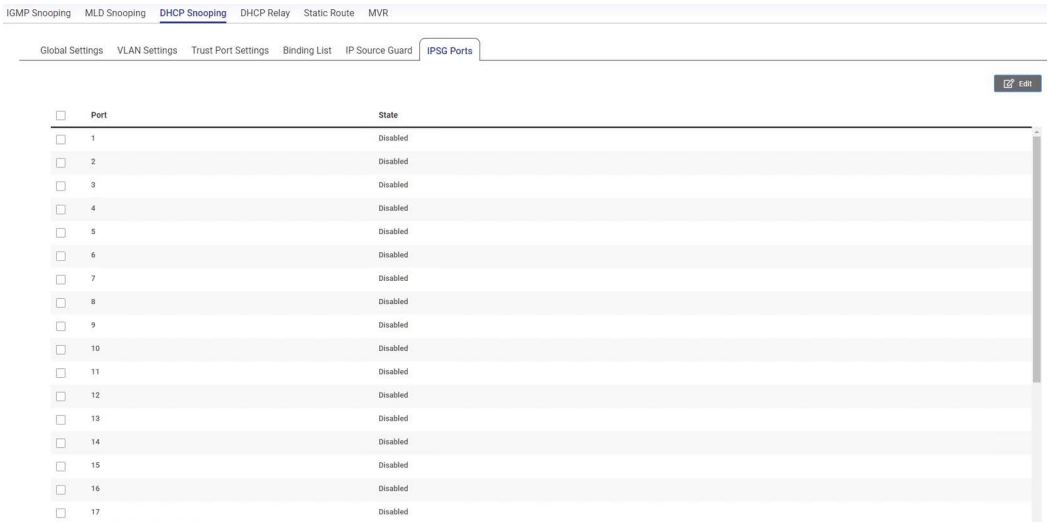

Figure 9-18 DHCP Snooping(IPSG Ports)

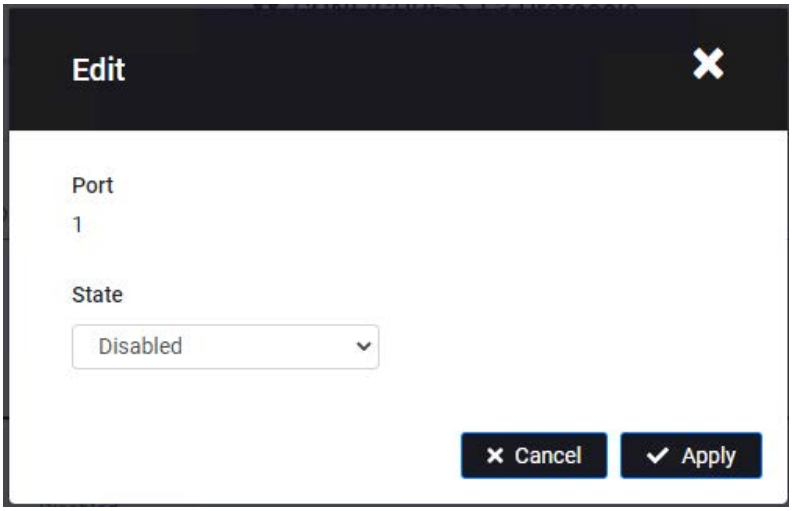

Figure 9-19 DHCP Snooping(IPSG Ports_Edit Screen)

9.3 DHCP Relay

9.3.1 Global Settings

Choose "**Enabled**" and click the **Apply** button to activate this feature.

Figure 9-20 DHCP Relay(Global Settings)

9.3.2 DHCP Relay Server

Specify the DHCP server's IP address to be relayed.

Figure 9-21 DHCP Relay(DHCP Relay Server)

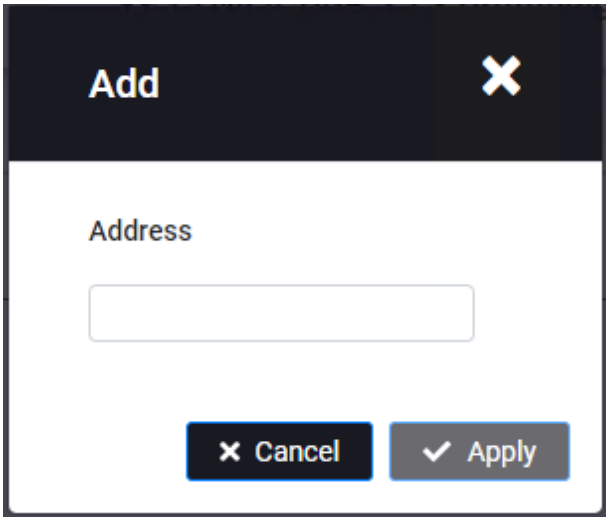

Figure 9-22 DHCP Relay(DHCP Relay Server_Add Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

9.4 Static Route

Static route is a routing type in which network administrators can configure the routes into the routing table and it's used by the network device to send packets to a destination network via a specific IPv4 or IPv6 route/gateway.

9.4.1 IPv4 Route

Figure 9-23 Static Route(IPv4 Route)

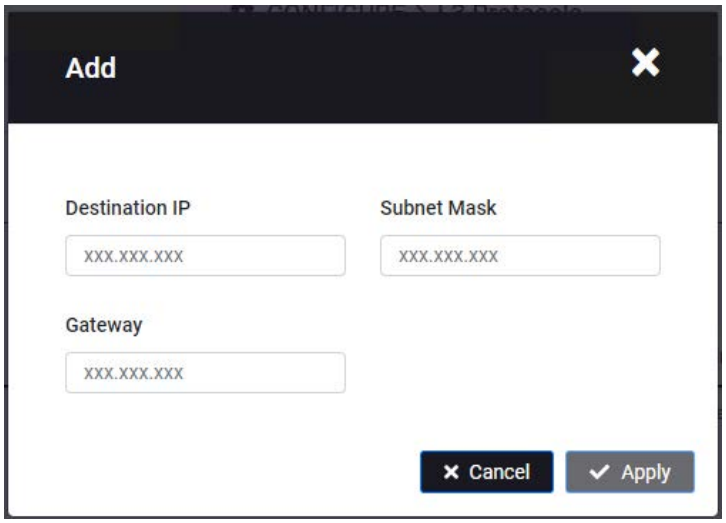

Figure 9-24 Static Route(IPv4 Route_Add Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

9.4.2 IPv6 Route

Figure 9-25 Static Route(IPv6 Route)

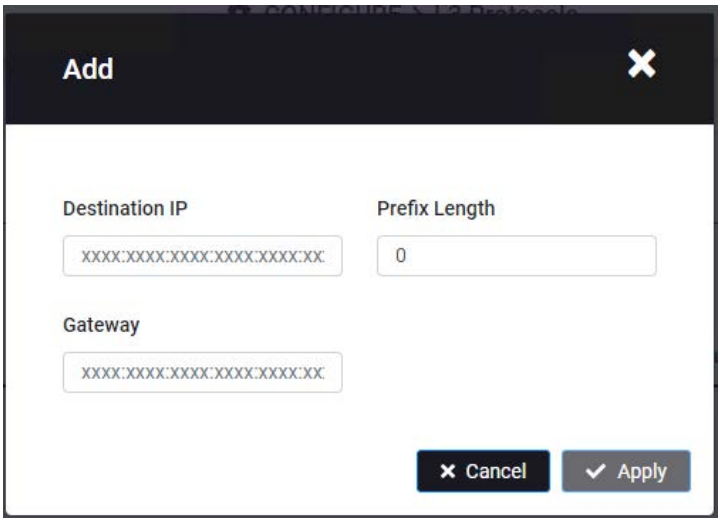

Figure 9-26 Static Route(IPv6 Route_Add Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

10 LBD

To lower loop-incurred impact to system performance, LBD mechanism can be enabled to let switch periodically broadcast loopback detection packets so a switch can detect a loop when it receives its own LBD packe

10.1 Global Settings

Select "**Enabled**" and click **Apply** button to activate the settings.

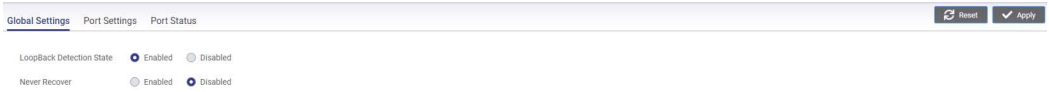

Figure 10-1 LBD(Global Settings)

10.2 Port Settings

Figure 10-2 LBD(Port Settings)

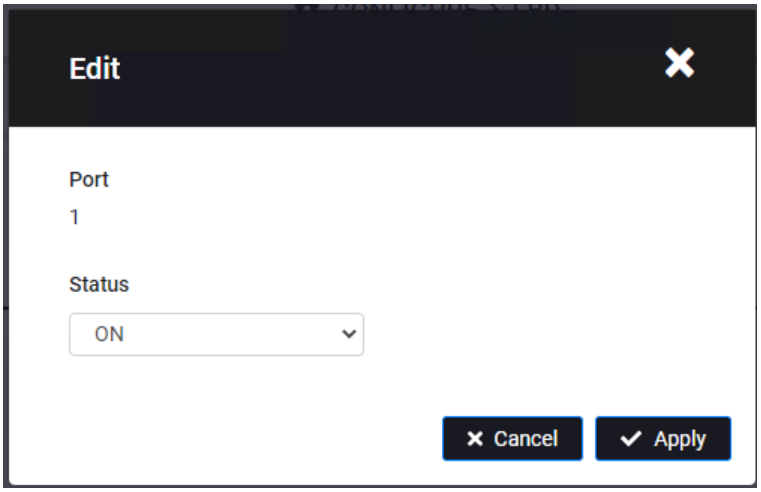

Figure 10-3 LBD(Port Settings_Edit Screen)

10.3 Port Status

Figure 10-4 LBD(Port Status)

Click Refresh to update the per-port status.

11 QoS

11.1 Global Settings

There are two options for applying QoS information onto packets: the IEEE 802.1p Class of Service (CoS) priority field within the VLAN tag of tagged Ethernet frames, and Differentiated Services (DiffServ) Code Point (DSCP). Each port on the switch can be configured to trust one of the packet fields (IEEE 802.1p , DSCP or DSCP+IEEE 802.1p). Packets that enter the switch's port may carry no QoS information as well. If so, the switch places such information into the packets before transmitting them to the next node. Thus, QoS information is preserved between nodes within the network and the nodes know which label to give each packet. A trusted field must exist in the packet for the mapping table to be of any use. When a port is configured as untrusted, it does not trust any incoming packet priority designations and uses the port default priority value instead to process the packet.

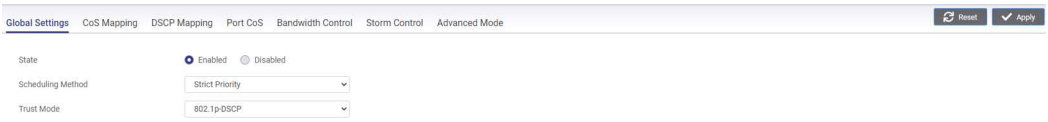

Figure 11-1 Global Settings

Items	Descriptions
State	Select whether QoS is enabled or disabled on the switch.
Scheduling Method	Selects the Strict Priority or WRR to specify the traffic scheduling method. Strict Priority: Specifies traffic scheduling based strictly on the queue priority. WRR: Uses the Weighted Round-Robin (WRR) algorithm to handle packets in priority classes of service. It assigns WRR weights to queues.

Items	Descriptions
Trust Mode	Select which packet fields to use for classifying packets entering the switch. DSCP: Classify traffic based on the DSCP (Differentiated Services Code Point) tag value. 802.1p: Classify traffic based on the IEEE 802.1p. The eight priority tags that are specified in IEEE 802.1p are from 1 to 8.

Click **Apply** to update the system settings.

11.2 CoS Mapping

Use the Class of Service (CoS) Mapping feature to specify which internal traffic class to map to the corresponding CoS value. CoS allows you to specify which data packets have greater precedence when traffic is buffered due to congestion.

Figure 11-2 CoS Mapping

Items	Descriptions
CoS	Displays the CoS priority tag values, where 0 is the lowest and 7 is the highest.
Queue	Check the CoS priority tag box and select the Queue values for each CoS value in the provided fields. Eight traffic priority queues are supported, and the field values are from 1 to 8, where one is the lowest priority and eight is the highest priority.

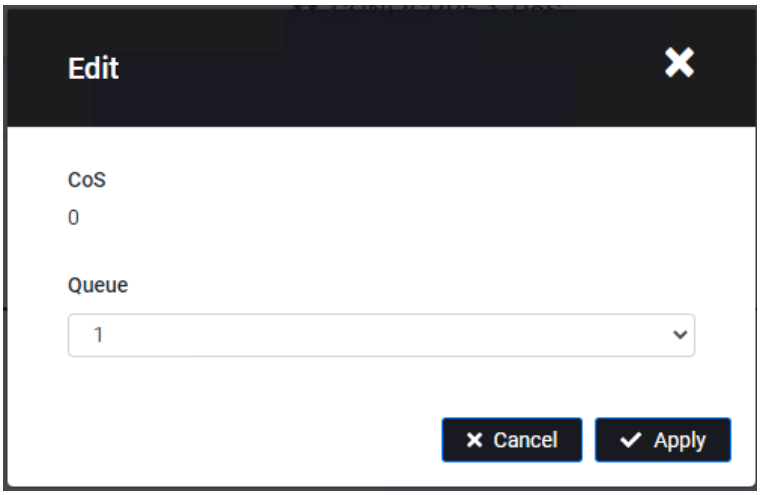

Figure 11-3 CoS Mapping(Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

11.3 DSCP Mapping

Use Differentiated Services Code Point (DSCP) Mapping feature to specify which internal traffic class to map to the corresponding DSCP values. DSCP Mapping increases the number of definable priority levels by reallocating bits of an IP packet for prioritization purposes.

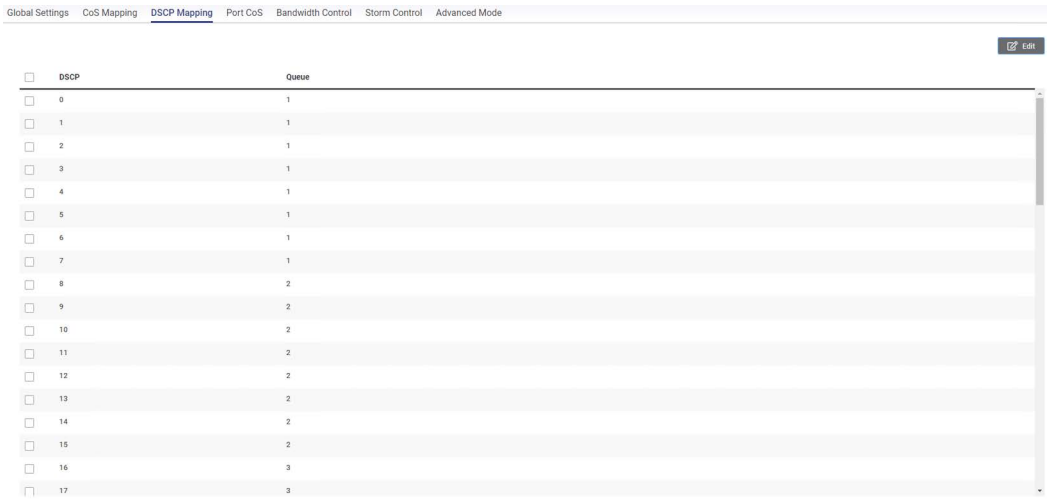

Figure 11-4 DSCP Mapping

Items	Descriptions
DSCP	Displays the packet's DSCP values, where 0 is the lowest and 10 is the highest.
Queue	Check the CoS priority tag box and select the Queue values for each DSCP in the provided fields. Eight traffic priority queues are supported, and the field values are from 1 to 8, where one is the lowest priority and eight is the highest priority.

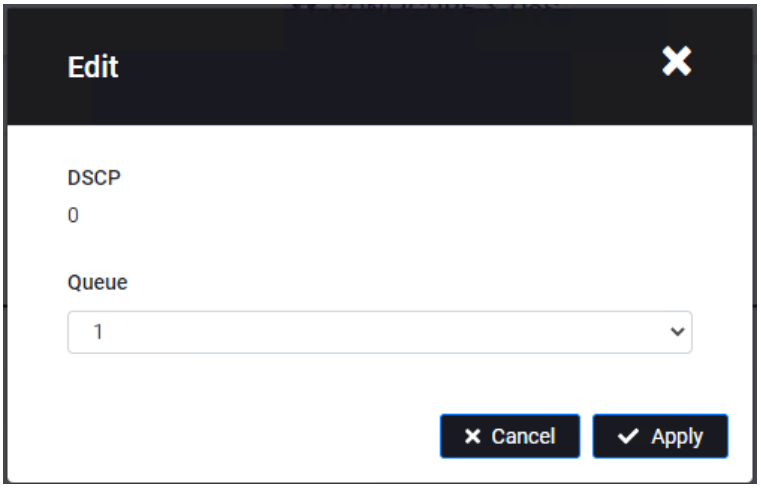

Figure 11-5 DSCP Mapping(Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

11.4 Port Cos

From here, you can configure the QoS port settings for the switch. Select a port you wish to set and choose a CoS value from the drop-down box. Next, select to enable or disable the Trust setting to let any CoS packet be marked at ingress.

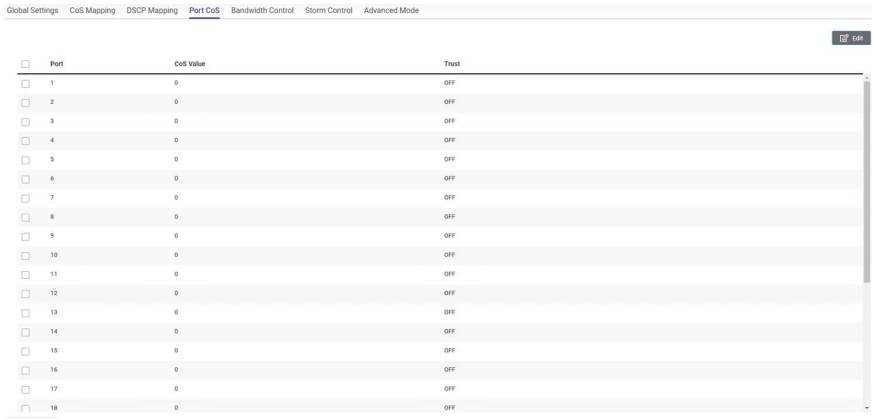

Figure 11-6 Port Cos

Items	Descriptions
Port	Displays the ports for which the CoS parameters are defined.
CoS Value	Select the CoS priority tag values, where 0 is the lowest and 7 is the highest.
Trust	Select Enabled to trust any CoS packet marking at ingress. Select Disabled to not trust any CoS packet marking at ingress.Qos will not work unless Trust is set to Enable.

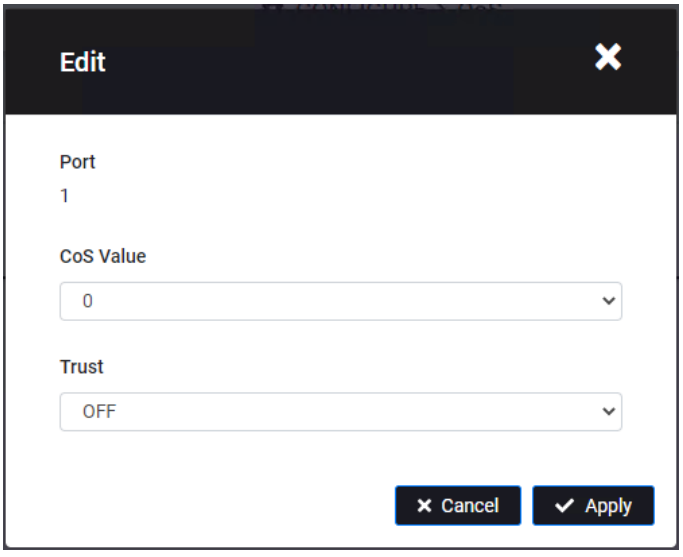

Figure 11-7 Port Cos(Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

11.5 Bandwidth Control

The Bandwidth Control feature allows users to define the bandwidth settings for a specified port's Ingress Rate Limit and Egress Rate.

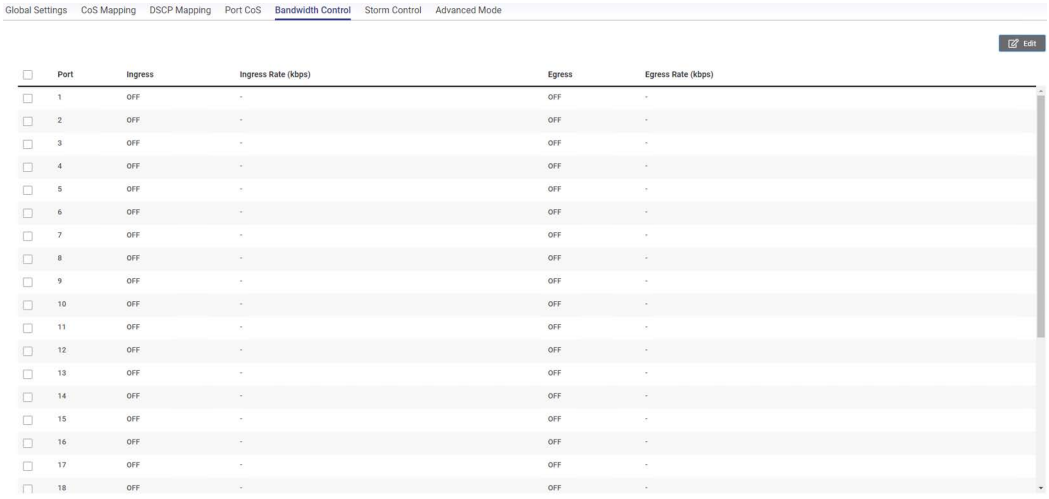

Figure 11-8 Bandwidth Control

Items	Descriptions
Port	Displays the ports for which the bandwidth settings are displayed.
Ingress	Select enable or disable ingress on the interface.
Ingress Rate	Enter the ingress rate in kilobits per second. The gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second.
Egress	Select from the drop-down box to Enable or Disable egress on the interface.
Egress Rate	Enter the egress rate in kilobits per second. The gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second.

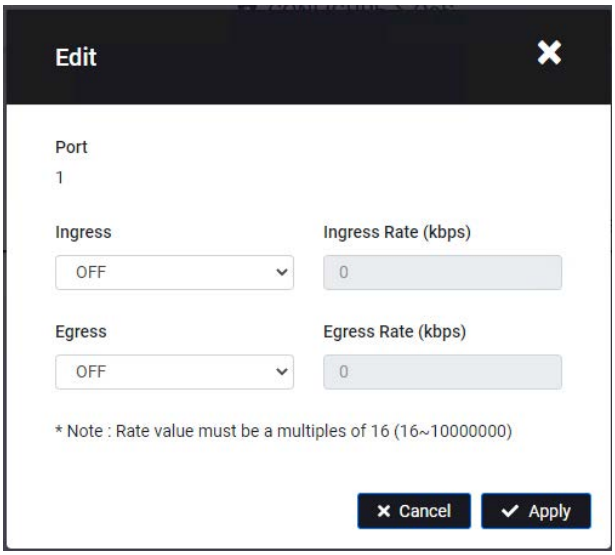

Figure 11-9 Bandwidth Control(Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

11.6 Storm Control

Storm Control limits the amount of Broadcast, Unknown Multicast, and Unknown Unicast frames accepted and forwarded by the switch. Storm Control can be enabled per port by defining the packet type and the rate that the packets are transmitted at. The switch measures the incoming Broadcast, Unknown Multicast, and Unknown Unicast frames rates separately on each port, and discards the frames when the rate exceeds a user-defined rate.

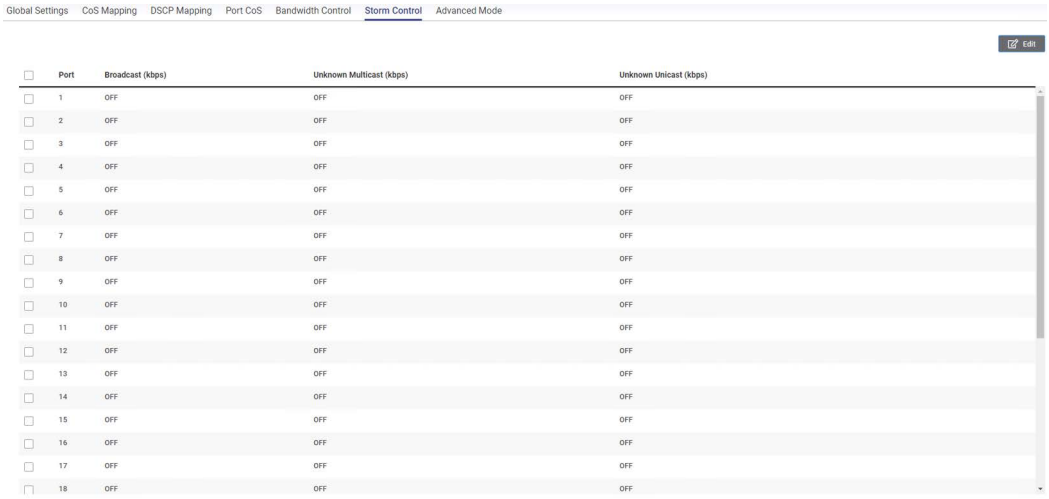

Figure 11-10 Storm Control

Items	Descriptions
Port	Displays the ports for which the Storm Control information is displayed.
Broadcast	Enter the broadcast rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.
Unknown Multicast	Enter the Unknown Multicast rate in kilobits per second. The gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.
Unknown Unicast	Enter the Unknown Unicast rate in kilobits per second. The gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.

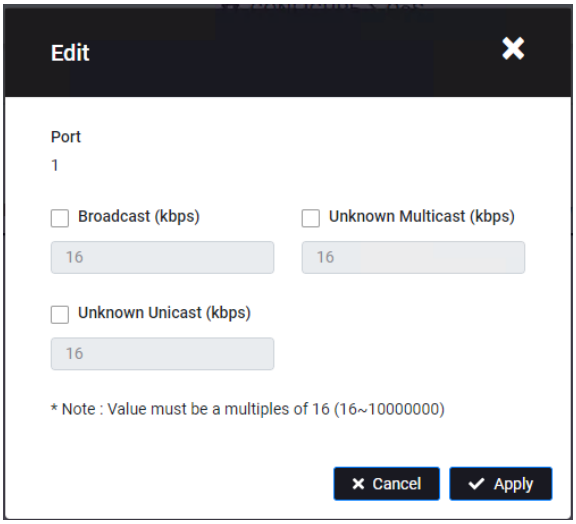

Figure 11-11 Storm Control(Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

11.7 Advanced Mode

Advanced mode allows users to further customize matching criteria to apply QoS onto incoming traffics; the switch then places such information into the packets before transmitting them to the next node.

11.7.1 Class Mapping

Use this page to view and add class mapping for QoS.

Figure 11-12 Advanced Mode(Class Mapping)

Items	Descriptions
CLS Name	Enter the policy name of class for QoS mapping.
Status	Indicates the status for the class mapping policy.
Source MAC Address	Enter the source MAC address.
Source IP Address	Enter the source IP address.

Items	Descriptions
Source IP Address Mask	Enter the mask of the source IP address.
Source Port	Enter the source port.
Destination MAC Address	Enter the destination MAC address.
Destination IP Address	Enter the destination IP address.
Destination IP Address Mask	Enter the mask of the destination IP address.
Destination Port	Enter the destination port.
Ethertype Value (Hex)	Enter the Ethertype value.
VLAN ID	Select the VLAN ID from drop-down list.
VLAN Priority	Select the VLAN priority from drop-down list.
Protocol	Select protocol from list or ID.
DSCP	In Type of Service, enter the DSCP. The range is from 0 to 63.

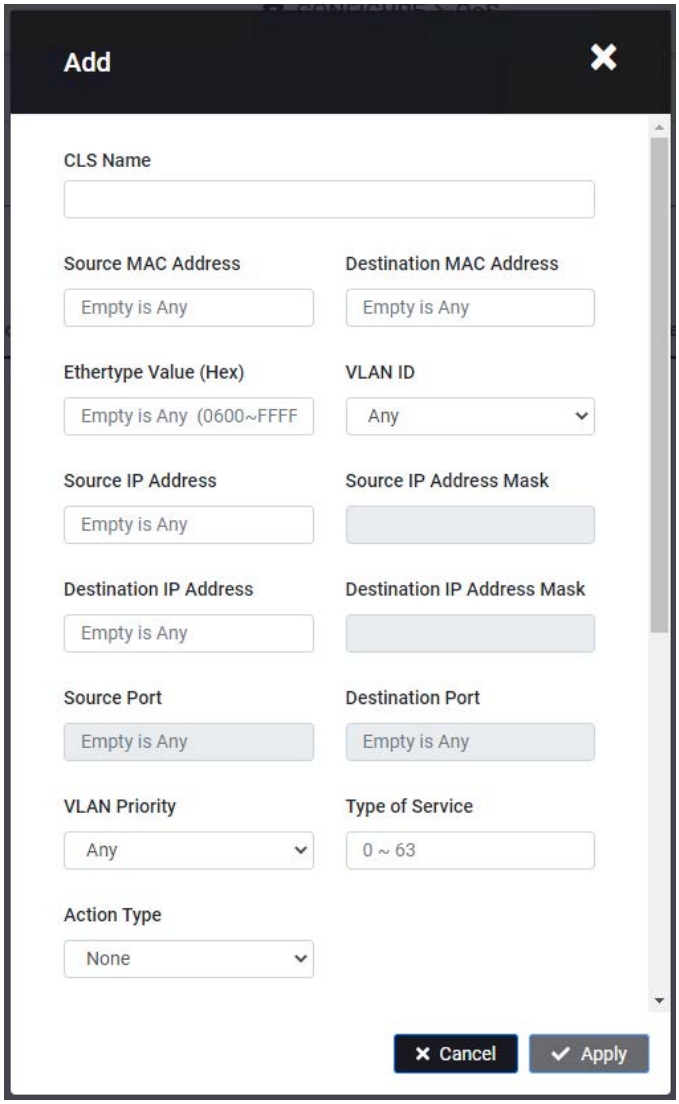

Figure 11-13 Advanced Mode(Class Mapping_Edit Screen)

In Action Type, select either "802.1p set to" or "DSCP set to" along with value specified in the corresponding field to apply QoS class mapping. Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

11.7.2 Policy Mapping

Use this page to view and assign class mapping policy onto switch ports for QoS.

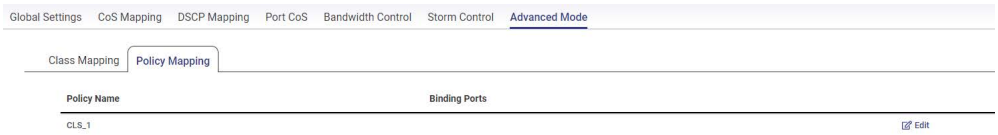

Figure 11-14 Advanced Mode(Policy Mapping)

Items	Descriptions
Policy Name	Displays the class mapping policy defined in Class Mapping.
Binding Ports	Enter the switch port number to bind the mapping policy for QoS.

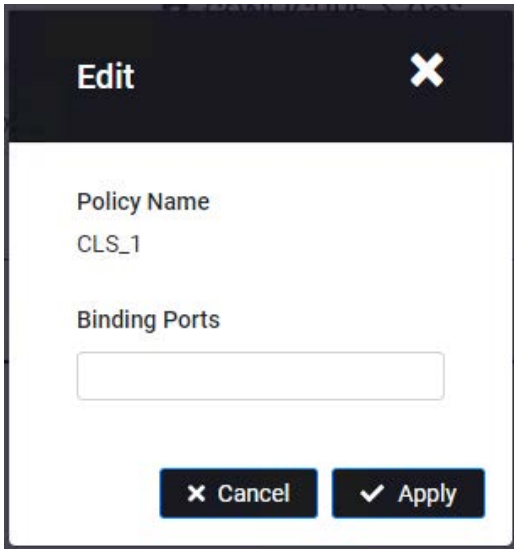

Figure 11-15 Advanced Mode(Policy Mapping_Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

12 Access Control

An Access Control List (ACL) allows you to define classification rules or establish criteria to provide security to your network by blocking unauthorized users and allowing authorized users to access specific areas or resources. ACLs can provide basic security for access to the network by controlling whether packets are forwarded or blocked at the switch ports. Access Control Lists (ACLs) are filters that allow you to classify data packets according to content in the packet header, such as the source address, destination address, source port number, destination port number, and more. Packet classifiers identify flows for more efficient processing. Each filter defines the conditions that must match for inclusion in the filter. ACLs (Access Control Lists) provide packet filtering for IP frames (based on the protocol, TCP/UDP port number or frame type) or layer 2 frames (based on any destination MAC address for unicast, broadcast, or multicast, or based on VLAN ID or VLAN tag priority). ACLs can be used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols. Policies can be used to differentiate service for client ports, server ports, network ports, or guest ports. They can also be used to strictly control network traffic by only allowing incoming frames that match the source MAC and source IP address on a specific port. ACLs are composed of Access Control Entries (ACEs), which are rules that determine traffic classifications. Each ACE is a considered a single rule, and up to 256 rules may be defined on each ACL, with up to 3000 rules globally. ACLs are used to provide traffic flow control, restrict contents of routing updates, and determine which types of traffic are forwarded or blocked. This criterion can be specified based on the MAC address or IP address.

12.1 MAC ACL

This page displays the currently defined MAC-based ACLs profiles. To add a new ACL, click Add and enter the name of the new ACL.

Figure 12-1 MAC ACL

Items	Descriptions
Index	Profile identifier.
Name	Enter the MAC based ACL name. You can use up to 32 alphanumeric characters.

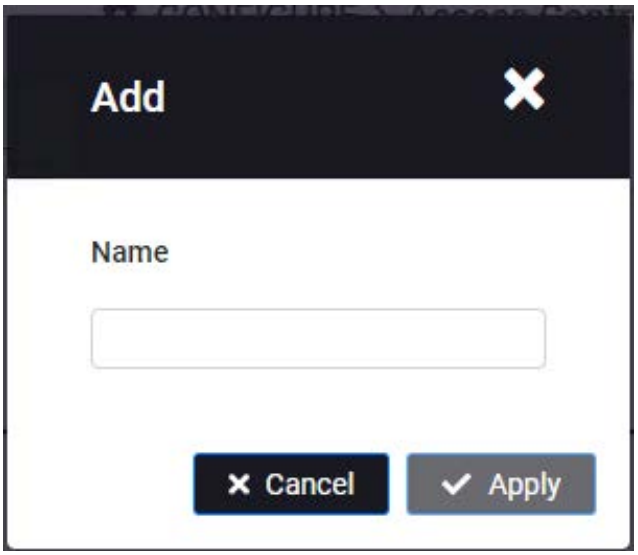

Figure 12-2 MAC ACL(Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

12.2 MAC ACE

Use this page to view and add rules to MAC-based ACLs.

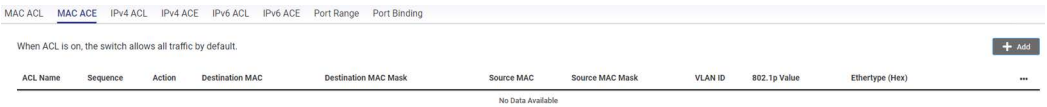

Figure 12-3 MAC ACE

Click the **Add** button to add new MAC ACE rule:

Items	Descriptions
ACL Name	Select the ACL from the list.
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from **1 to 2147483647**, 1 being processed first.
Action	Select what action to take if a packet matches the criteria. **Permit**: Forward packets that meet the ACL criteria. **Deny**: Drops packets that meet the ACL criteria.
Destination MAC Value	Enter the destination MAC address.
Destination MAC Wildcard Mask	Enter a MAC address mask for the destination MAC address. A mask of 00:00:00:00:00:00 means the bits must be matched exactly; **ff:ff:ff:ff:ff:ff** means the bits are irrelevant. Any combination of 0s and ffs can be used.
Source MAC Value	Enter the source MAC address.
Source MAC Wildcard Mask	Enter a MAC address mask for the source MAC address. A mask of 00:00:00:00:00:00 means the bits must be matched exactly; **ff:ff:ff:ff:ff:ff** means the bits are irrelevant. Any combination of 0s and ffs can be used.
VLAN ID	Enter the VLAN ID to which the MAC address is attached in MAC ACE. The range is from **1 to 4094**.
IEEE 802.1p Value	Enter the IEEE 802.1p value. The range is from **0 to 7**.
Ethertype Value	Selecting this option instructs the switch to examine the Ethernet type value in each frame's header. This option can only be used to filter Ethernet II formatted packets. A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), and 8137 (IPX).

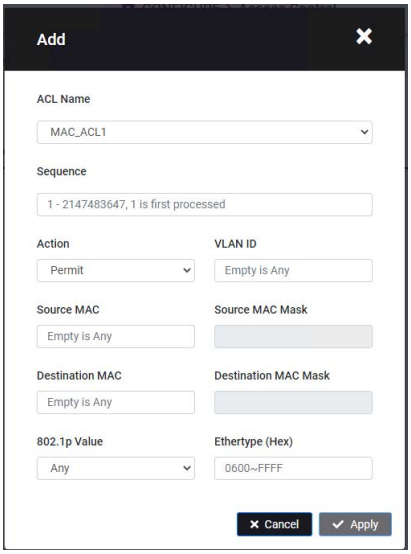

Figure 12-4 MAC ACE(Add Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

12.3 IPv4 ACL

This page displays the currently defined IPv4-based ACLs profiles. To add a new ACL, click Add and enter the name of the new ACL.

Figure 12-5 IPv4 ACL

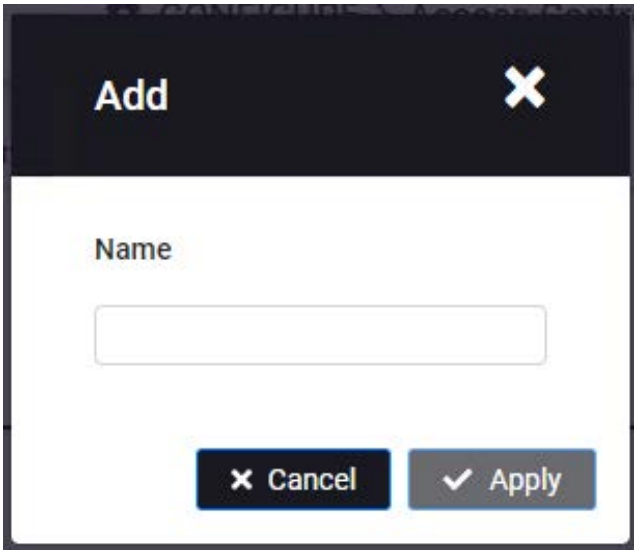

Figure 12-6 IPv4 ACL(Add Screen)

Items	Descriptions
Index	Displays the current number of ACLs.
Name	Enter the IP based ACL name. You can use up to 32 alphanumeric characters.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

12.4 IPv4 ACE

Use this page to view and add rules to IPv4-based ACLs.

Figure 12-7 IPv4 ACE

Click the **Add** button to add new IPv4 ACE rule:

Items	Descriptions
ACL Name	Select the ACL from the list for which a rule is being created.

Items	Descriptions
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from **1 to 2147483647**, 1 being processed first.
Action	Select what action to take if a packet matches the criteria. **Permit**: Forwards packets that meet the ACL criteria. **Deny**: Drops packets that meet the ACL criteria.

Items	Descriptions
Protocol	Select Any, Protocol ID, or Select from a List in the drop-down menu. Any: Check Any to use any protocol. Protocol ID: Enter the protocol in the ACE to which the packet is matched. Select from List: Selects the protocol from the list in the provided field. • ICMP: Internet Control Message Protocol (ICMP). The ICMP enables the gateway or destination host to communicate with the source host. • IPinIP: IP in IP encapsulates IP packets to create tunnels between two routers. This ensures that the IP in IP tunnel appears as a single interface, rather than several separate interfaces. • TCP: Transmission Control Protocol (TCP). Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery and guarantees that packets are transmitted and received in the order they are sent. EGP Exterior Gateway Protocol (EGP). Permits exchanging routing information between two neighboring gateway hosts in an autonomous systems network. • IGP: Interior Gateway Protocol (IGP). Enables a routing information exchange between gateways within an autonomous network. • UDP: User Datagram Protocol (UDP). UDP is a communication protocol that transmits packets but does not guarantee their delivery. • HMP: The Host Mapping Protocol (HMP) collects network information from various network hosts. HMP monitors hosts spread over the Internet as well as hosts in a single network. • RDP: Reliable Data Protocol (RDP). Provides a reliable data transport service for packet-based applications. • IPv6: Matches the packet to the IPV6 protocol. • IPv6: Rout: Routing Header for IPv6. • IPv6: Frag: Fragment Header for IPv6. • RVSP: Matches the packet to the ReSerVation Protocol(RSVP). • IPv6: ICMP: The Internet Control Message Protocol (ICMP) allows the gateway or destination host to communicate with the source host.

Items	Descriptions
Protocol	• **OSPF**: The Open Shortest Path First (OSPF) protocol is a link-state hierarchical interior gateway protocol (IGP) for network routing Layer Two (2) tunneling protocols. It is an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs). • **PIM**: Matches the packet to Protocol Independent Multicast (PIM). • **L2TP**: Matches the packet to Internet Protocol (L2IP).
Destination IP Address Value	Enter the destination IP address.
Destination IP Mask	Enter the mask of the destination IP address.
Destination Port Range	Enter the destination port range.
Source IP Address Value	Enter the source IP address.
Source IP Mask	Enter the mask of the source IP address.
Source Port Range	Enter the source port range.
Flag Set	Select whether to handle each six TCP control flags; URG (Urgent), ACK (Acknowledgment), PSH (Push), RST (Reset), SYN (Synchronize), and FIN (Fin) from drop-down menu. Don't Care: The ACE does not treat the TCP control flag. Set: The packet with the TCP control flag being set matches the criteria. Unset: The packet with the TCP control flag being unset matches the criteria.
DSCP	In Type of Service, select **Any** or **DSCP to match** from drop-down list. When **DSCP to match** is selected, enter the DSCP. The range is from 0 to 63.
ICMP	Select **Any, Protocol ID**, or **Select from List** from drop-down menu. **Protocol ID**: Enter the protocol in the ACE to which the packet is matched. The range is from 0 to 255. **Select from List**: Select the ICMP from the list in the provided field.
ICMP Code	Select Any or User Defined from drop-down menu. When User Defined is selected, enter the ICMP code value. The range is from 0 to 255.
Actions	Select Edit or Delete for this entry.

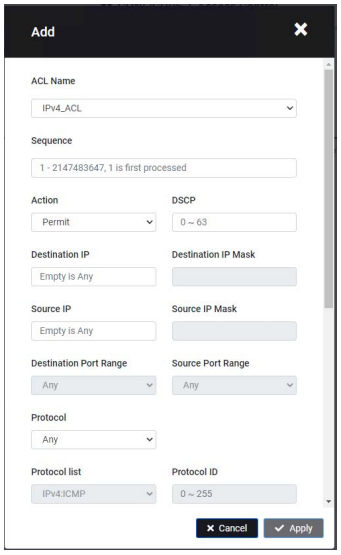

Figure 12-8 IPv4 ACE(Add Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

12.5 IPv6 ACL

This page displays the currently defined IPv6-based ACLs profiles. To add a new ACL, click Add and enter the name of the new ACL.

Figure 12-9 IPv6 ACL

Items	Descriptions
Index	Displays the current number of ACLs.
Name	Enter the IPv6 based ACL name. You can use up to 32 alphanumeric characters.

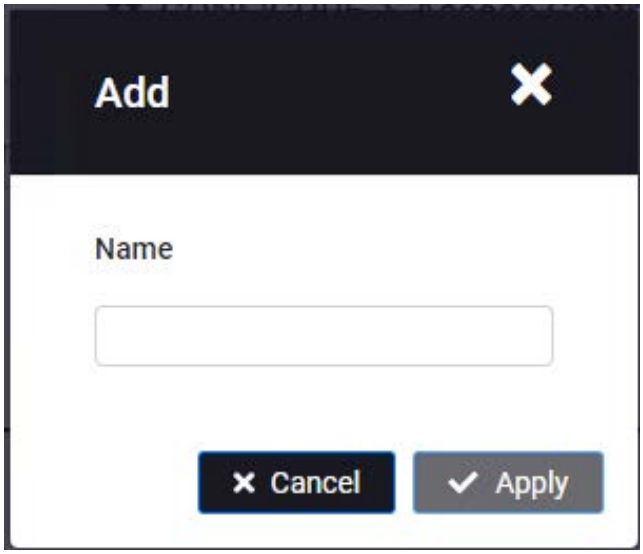

Figure 12-10 IPv6 ACL(Add Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

12.6 IPv6 ACE

Allows IPv6 Based Access Control Entry (ACE) to be defined within a configured ACL.

Figure 12-11 IPv6 ACE

Click the Add button to add new IPv6 ACE rule:

Items	Descriptions
ACL Name	Select the ACL from the list.
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1 to 2147483647, 1 being processed first.
Action	Select what action to take if a packet matches the criteria. Permit: Forward packets that meet the ACL criteria. Deny: Drops packets that meet the ACL criteria.

Items	Descriptions
Protocol	Select the Any, Protocol ID, or Select from List from drop-down menu. Protocol ID: Enter the protocol in the ACE to which the packet is matched. Select from List: Select the protocol from the list in the provided field.
Destination IP Address Value	Enter the destination IP address.
Destination IP Prefix Length	Enter the prefix length of the destination IP address. The range is from 0 to 128.
Destination Port Range	Select Any or Range from the list. Enter the destination port that is matched to packets. The range is from 0 to 65535.
Source IP Address Value	Enter the source IP address.
Source IP Prefix Length	Enter the prefix length of the new source IP address. The range is from 0 to 128.
Source Port Range	Select Any or Range from the list. Enter the source port that is matched to packets. The range is from 0 to 65535.
Flag Set	Select whether to handle each six TCP control flags; URG (Urgent), ACK (Acknowledgment), PSH (Push), RST (Reset), SYN (Synchronize), and FIN (Fin) from drop-down menu. Don't Care: The ACE does not treat the TCP control flag. Set: The packet with the TCP control flag being set matches the criteria. Unset: The packet with the TCP control flag being unset matches the criteria.
DSCP	Select Any or DSCP to match from drop-down list. When DSCP to match is selected, enter the DSCP. The range is from 0 to 63.
ICMP	Select Any, Protocol ID, or Select from List from drop-down menu. Protocol ID: Enter the protocol in the ACE to which the packet is matched. The range is from 0 to 255. Select from List: Select the ICMP from the list in the provided field.
ICMP Code	Select Any or User Defined from drop-down menu. When User Defined is selected, enter the ICMP code value. The range is from 0 to 255.
Actions	Select Edit or Delete for this entry.

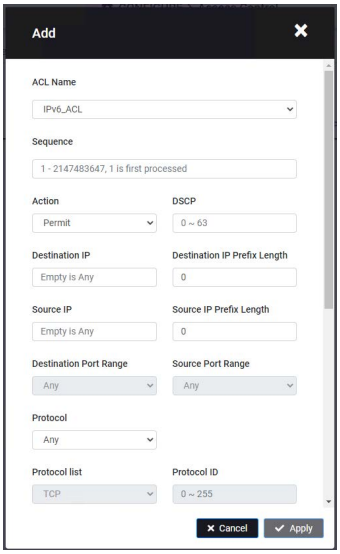

Figure 12-12 IPv6 ACE(Add Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

12.7 Port Range

Use this section to configure specified port range.

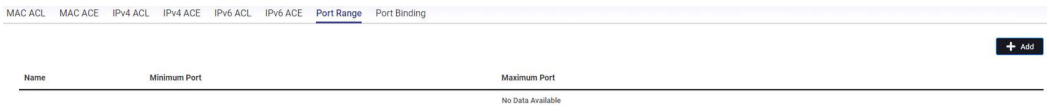

Figure 12-13 Port Range

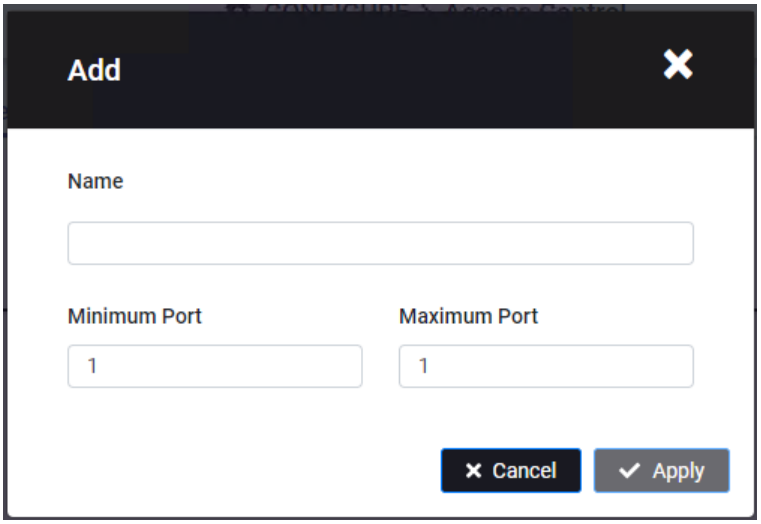

Figure 12-14 Port Range(Add Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

12.8 Port Binding

When an ACL is bound to an interface, all the rules that have been defined for the ACL are applied to that interface. Whenever an ACL is assigned on a port or LAG, flows from that ingress or egress interface that do not match the ACL are matched to the default rule of dropping unmatched packets. To bind an ACL to an interface, simply select an interface and select the ACL(s) you wish to bind.

Click **Edit** to update the system settings.

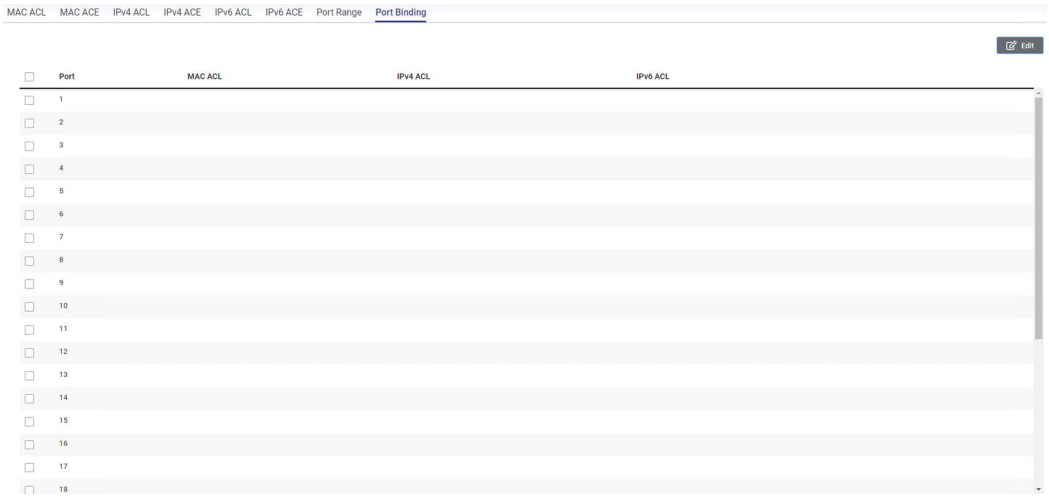

Figure 12-15 Port Binding

Items	Descriptions
Port	Select the port to which the ACLs are bound.
MAC ACL	Select the MAC ACL rule to apply to the port.
IPv4 ACL	Select the IPv4 ACL rule to apply to the port.
IPv6 ACL	Select the IPv6 ACL rule to apply to the port.

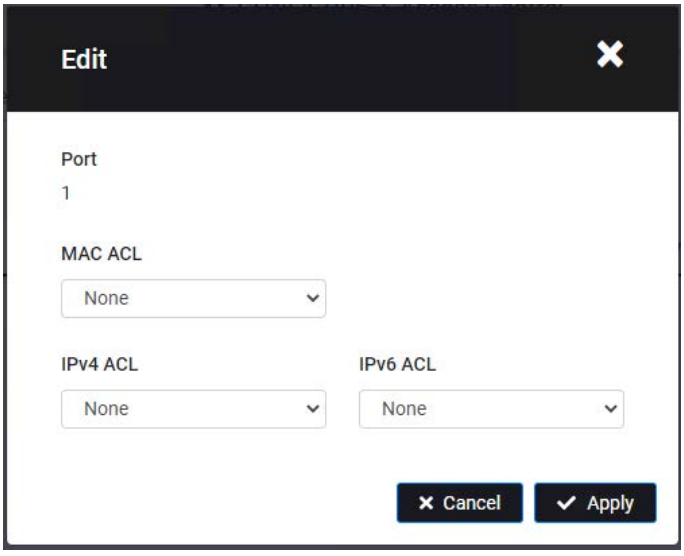

Figure 12-16 Port Binding(Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

13 Firmware

13.1 Firmware Upgrade

Follow this procedure to upgrade the Firmware.

1. Click to start upgrading.
2. Click Choose File. When a window opens, browse to the location of your new Firmware.
3. Select the new Firmware file and click OK.
4. A prompt will displays to confirm the Firmware Upgrade. Click OK and follow the on-screen instructions to complete the Firmware Upgrade.

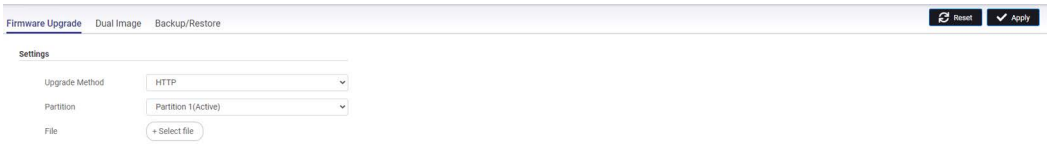

Figure 13-1 Firmware Upgrade

WARNING
Backup your configuration before upgrading to prevent loss of settings information.

Note
The upgrade process may require a few minutes to complete. It is advised to clear your browser cache after upgrading your firmware.

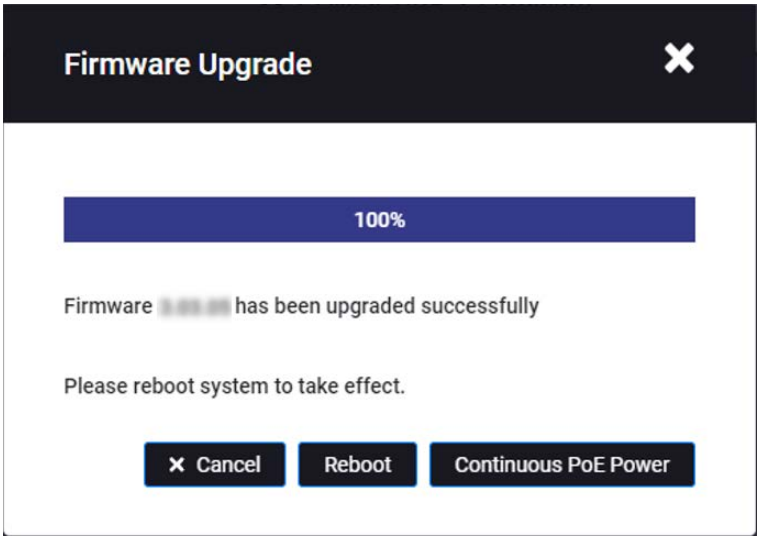

Figure 13-2 Firmware Upgrade

Continuous PoE Power appears only for XG-MU24TPoE+.

13.2 Dual Image

The switch maintains two versions of the switch image in its permanent storage. One image is the active image, and the second image is the backup image. The Dual Image screen enables the user to select which partition will be set as active after the next reset. The switch boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non-active image.

Figure 13-3 Dual Image

Items	Descriptions
Active	Selects the partition you wish to be active.
Flash Partition	Displays the number of the partition.
Status	Displays the partition which is currently active on the switch.
Image Name	Displays the name/version number of the image.
Image Size	Displays the size of the image file.

Items	Descriptions
Created Time	Displays the time the image was created.

Click **Apply** to update the system settings.

13.3 Backup/Restore

This feature is used for saving your current configuration to a file on your computer or a TFTP server, or to restore previously saved configuration settings to the switch using a configuration file from your local drive or TFTP server.

Figure 13-4 Backup/Restore

Click **Apply** to download configuration settings to your computer or a TFTP server, or to upload previously saved configuration file to the system.

14 LOG

The Syslog protocol allows devices to send event notification messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences across an IP network to syslog servers. It then collects the event messages, providing powerful support for users to monitor network operations and diagnose malfunctions. A Syslog-enabled device can generate a syslog message and send it to a Syslog server.
Syslog is defined in RFC 3164. The RFC defines the packet format, content, and system log related information of Syslog messages. Each Syslog message has a facility and severity level. The Syslog facility identifies a file in the Syslog server. Refer to the documentation of your Syslog program for details.

14.1 Global Settings

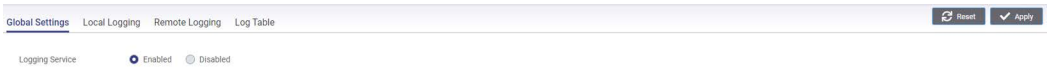

Figure 14-1 Global Settings

From here, you can select "Enabled or "Disabled" for the log settings of the switch.
Click the **Apply** button to apply the changes or the **Reset** button to discard them.

14.2 Local Logging

Figure 14-2 Local Logging

The following table describes the Syslog severity levels.

Code	Severity	Description	General Description
0	EMERG	System is unusable.	A "panic" condition usually affecting multiple apps/ servers/sites. At this level, all tech staff on call would be notified.
1	ALERT	Action must be taken immediately.	Should be corrected immediately. Therefore, notify staff who can fix the problem. An example would be the loss of a primary ISP connection.
2	CRIT	Critical conditions.	Should be corrected immediately but indicates failure in a secondary system; an example is a loss of a backup ISP connection.
3	ERROR	Error conditions.	Non-urgent failures, which should be relayed to developers or admins; each item must be resolved within a given time.

Code	Severity	Description	General Description
4	WARNING	Warning conditions.	Warning messages, not an error, but indication that an error will occur if action is not taken (e.g. file system 85% full). Each item must be resolved within a given time.
5	NOTICE	Normal but significant condition.	Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.
6	INFO	Informational messages.	Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required.
7	DEBUG	Debug messages.	Messages that contain information for debugging purpose.

Click the **Edit** button to apply the changes in RAM or Flash target, respectively.

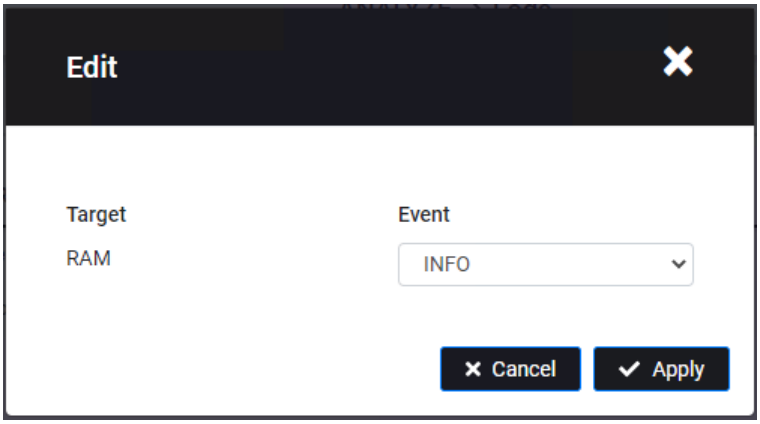

Figure 14-3 Local Logging(Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

14.3 Remote Logging

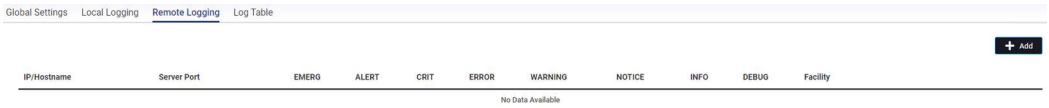

Figure 14-4 Remote Logging

The internal log of the ECS switch has a fixed capacity; at a certain level, the ECS switch will start deleting the oldest entries to make room for the newest. If you want a permanent record of all logging activities, you can set up your syslog server to receive log content from the ECS switch. Use this page to direct all logging to the syslog server. Click the Add button, define your syslog server, and select the severity level of events you wish to log.

Click the **Add** button to add the remote server for syslog logging:

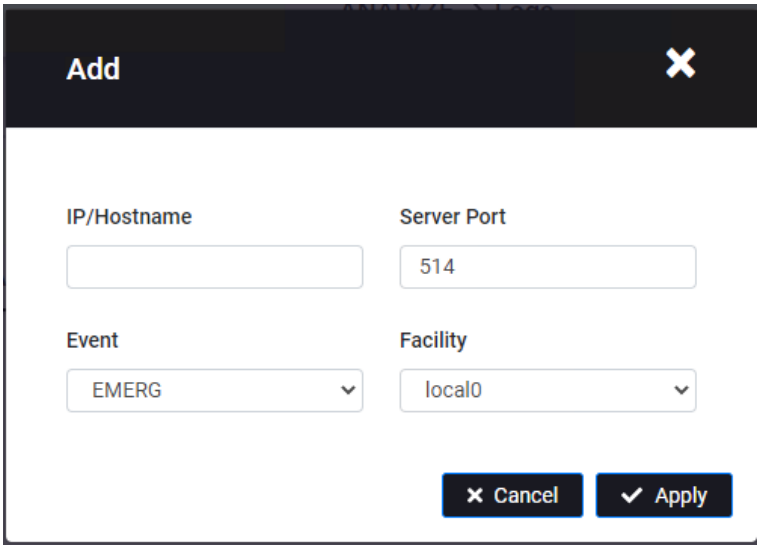

Figure 14-5 Remote Logging(Add Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

14.4 Log Table

This page displays the most recent records in the switch's internal log. Log entries are listed in reverse chronological order (with the latest logs at the top of the list). Click a column header to sort the content by that category.

14.4.1 Display logs in

- **RAM**: The information stored in the system's RAM log will be lost after the switch is rebooted or powered off.
- **Flash**: The information stored in the system's Flash will be kept effective even if the switch is rebooted or powered off.

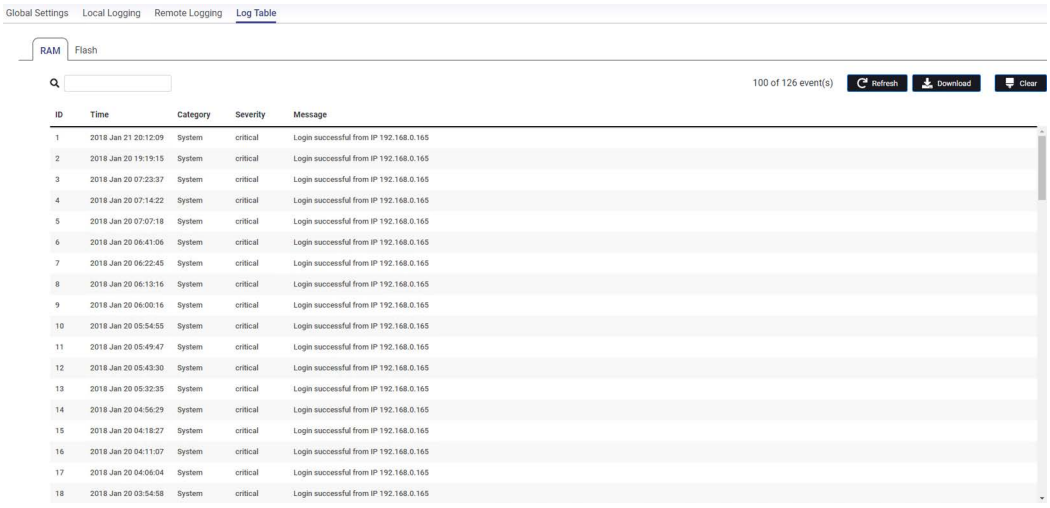

Figure 14-6 RAM

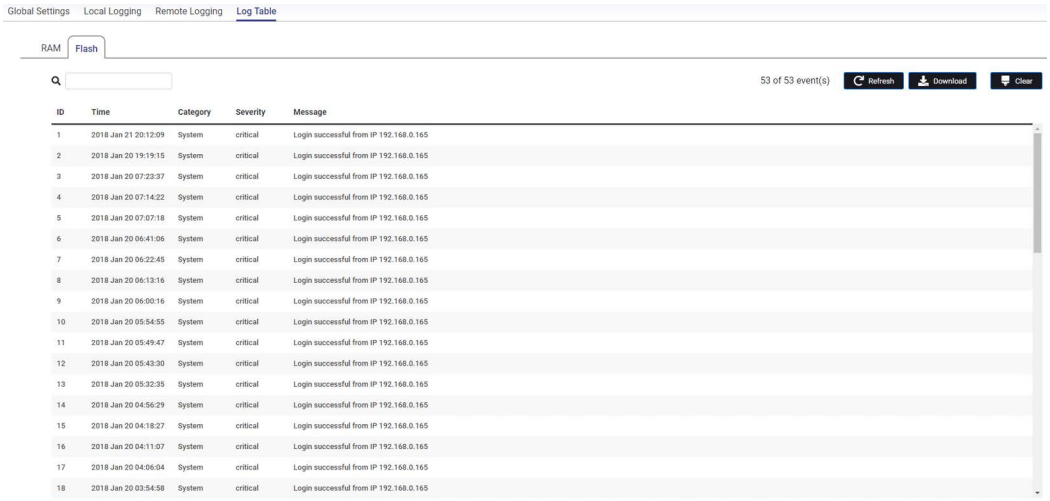

Figure 14-7 Flash

14.4.2 Download

Click the **Download** button to export the current buffered log to a .txt file.

14.4.3 Clear

Click the **Clear** button to clear the buffered log in the system's memory.

15 Diag Tools

15.1 Cable Diagnostics

Cable Diagnostics helps you detect whether your cable has connectivity problems and provides information about where errors have occurred in the cable. The tests use Time Domain Reflectometry (TDR) technology to test the quality of a copper cable attached to a port. TDR detects a cable fault by sending a signal through the cable and reading the signal that is reflected back. All or part of the signal is reflected back either by cable defects or by the end of the cable when an issue is present. Cables are tested when the ports are in the down state, with the exception of the cable length test.

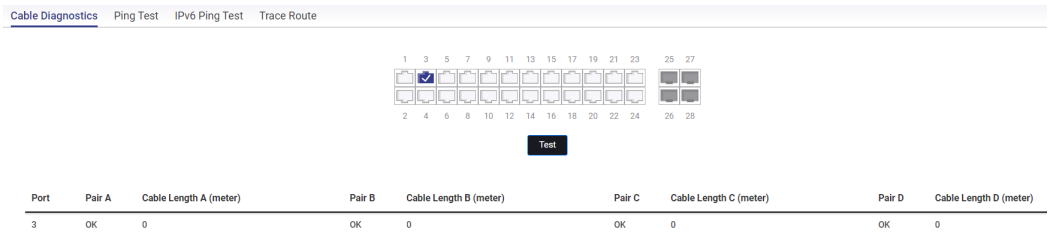

Figure 15-1 Cable Diagnostics

To verify accuracy of the test, it is recommended that you run multiple tests in case of test fault or user error.

Click **Test** to perform the cable tests for the selected port.

15.2 Ping Test

The Packet Internet Groper (Ping) Test allows you to verify connectivity to remote hosts. The ping test operates by sending Internet Control Message Protocol (ICMP) request packets to the tested host and waits for an ICMP response. In the process it measures the time from transmission to reception and records any packet loss. Send a ping request to a specified IPv4 address. Check whether the switch can communicate with a particular network host before testing.

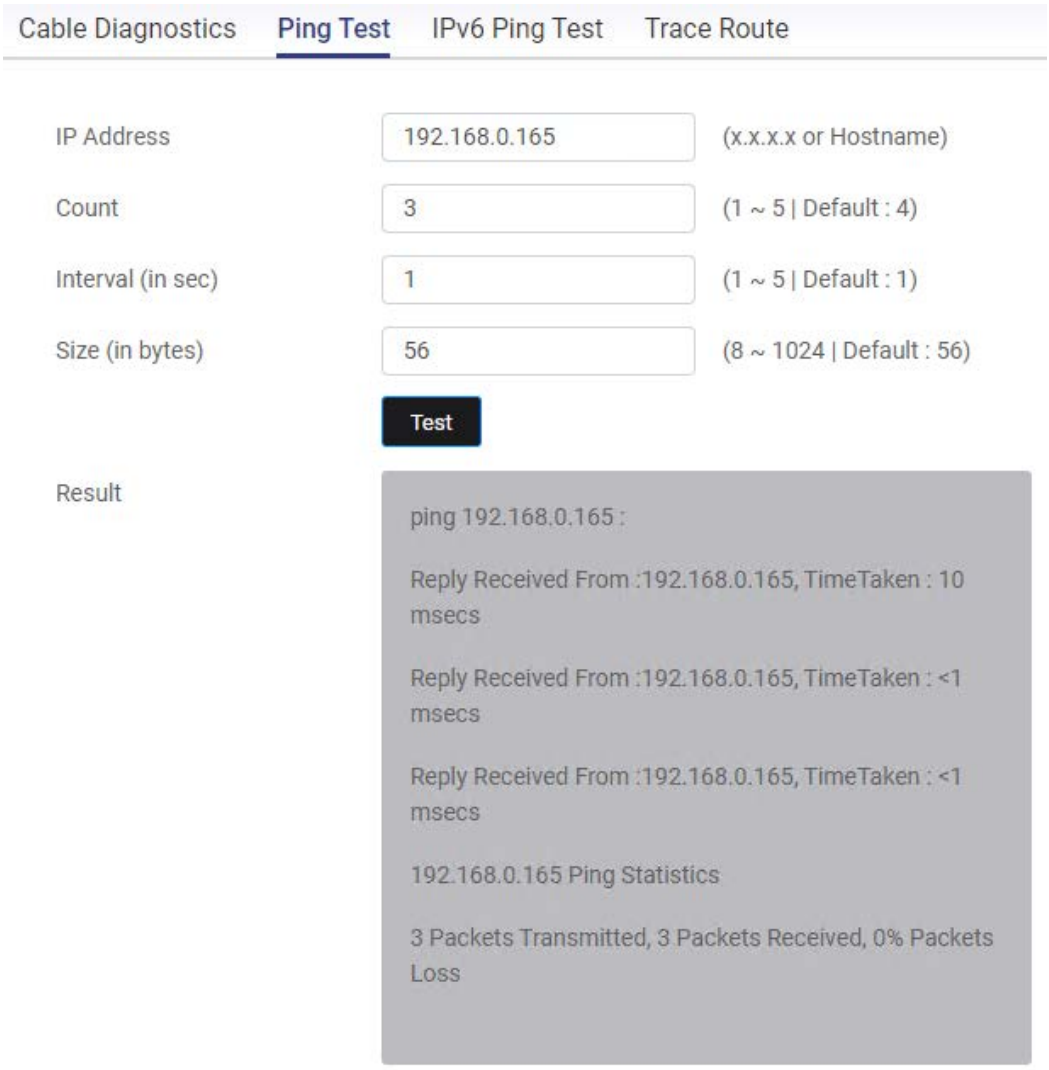

Figure 15-2 Ping Test

You can vary the test parameters by entering the data in the appropriate boxes. To verify accuracy of the test, it is recommended that you run multiple tests in case of a test fault or user error.

To verify accuracy of the test, it is recommended that you run multiple tests in case of test fault or user error.

Items	Descriptions
IP Address	Enter the IP address or the host name of the station you want the switch to ping to.
Count	Enter the number of pings to send. The range is from 1 to 5 and the default is 4.

Items	Descriptions
Interval	Enter the number of seconds between pings sent. The range is from 1 to 5 and the default is 1.
Size	Enter the size of ping packet to send. The range is from 8 to 5120 and the default is 56.
Result	Displays the ping test results.

15.3 IPv6 Ping Test

Send a ping request to a specified IPv6 address. Check whether the switch can communicate with a particular network host before testing.

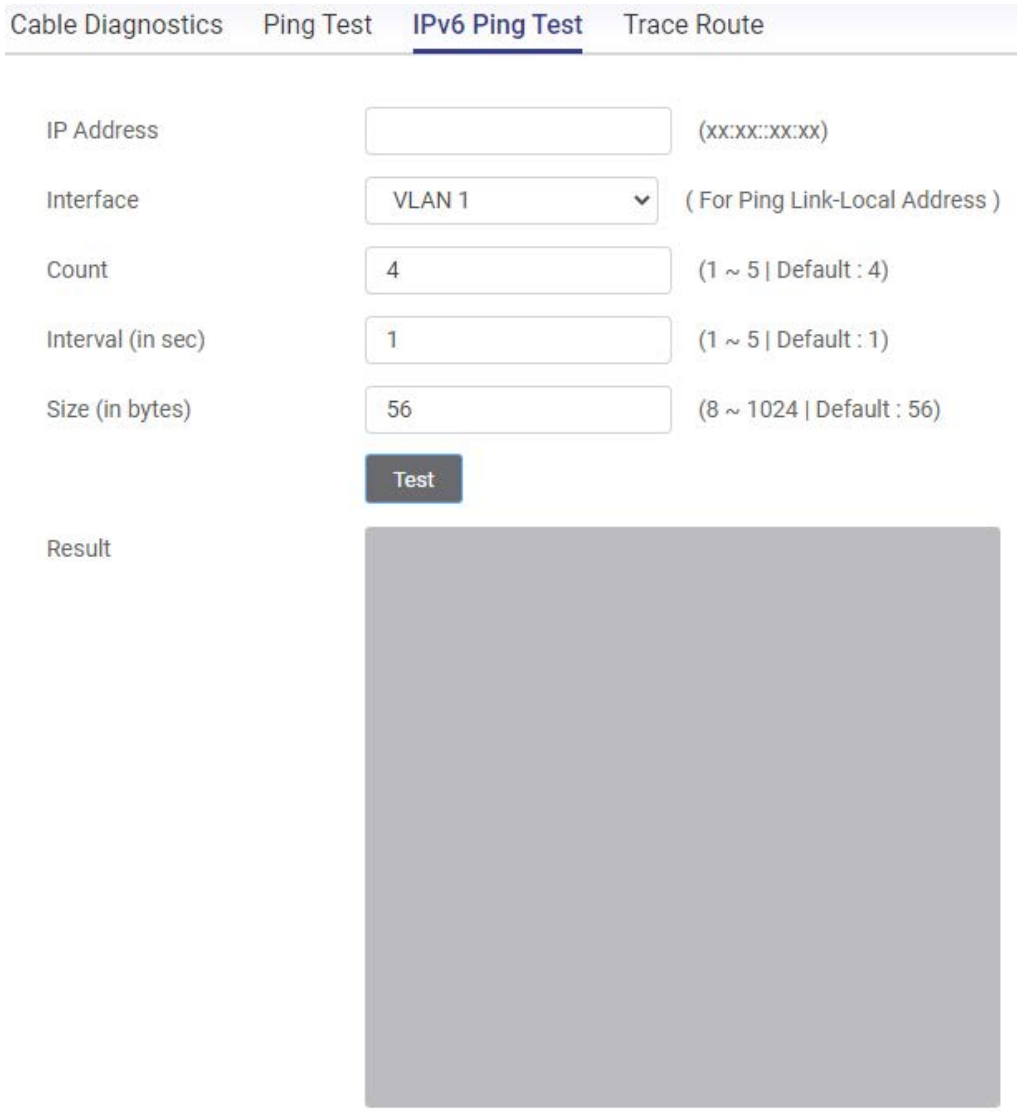

Figure 15-3 IPv6 Ping Test

You can vary the test parameters by entering the data in the appropriate boxes. To verify accuracy of the test, it is recommended that you run multiple tests in case of a test fault or user error.

Items	Descriptions
IP Address	Enter the IPv6 address or the host name of the station you want the switch to ping to.
Count	Enter the number of pings to send. The range is from 1 to 5 and the default is 4.
Interval	Enter the number of seconds between pings sent. The range is from 1 to 5 and the default is 1.
Size	Enter the size of ping packet to send. The range is from 8 to 5120 and the default is 56.
Result	Displays the ping test results.

Click **Test** to perform the ping test.

15.4 Trace Route

The trace route feature is used to discover the routes that packets take when traveling to their destination. It will list all the routers it passes through until it reaches its destination or fails to reach the destination and is discarded. In testing, it will tell you how long each hop from router to router takes via the trip time of the packets it sends and receives from each successive host in the route.

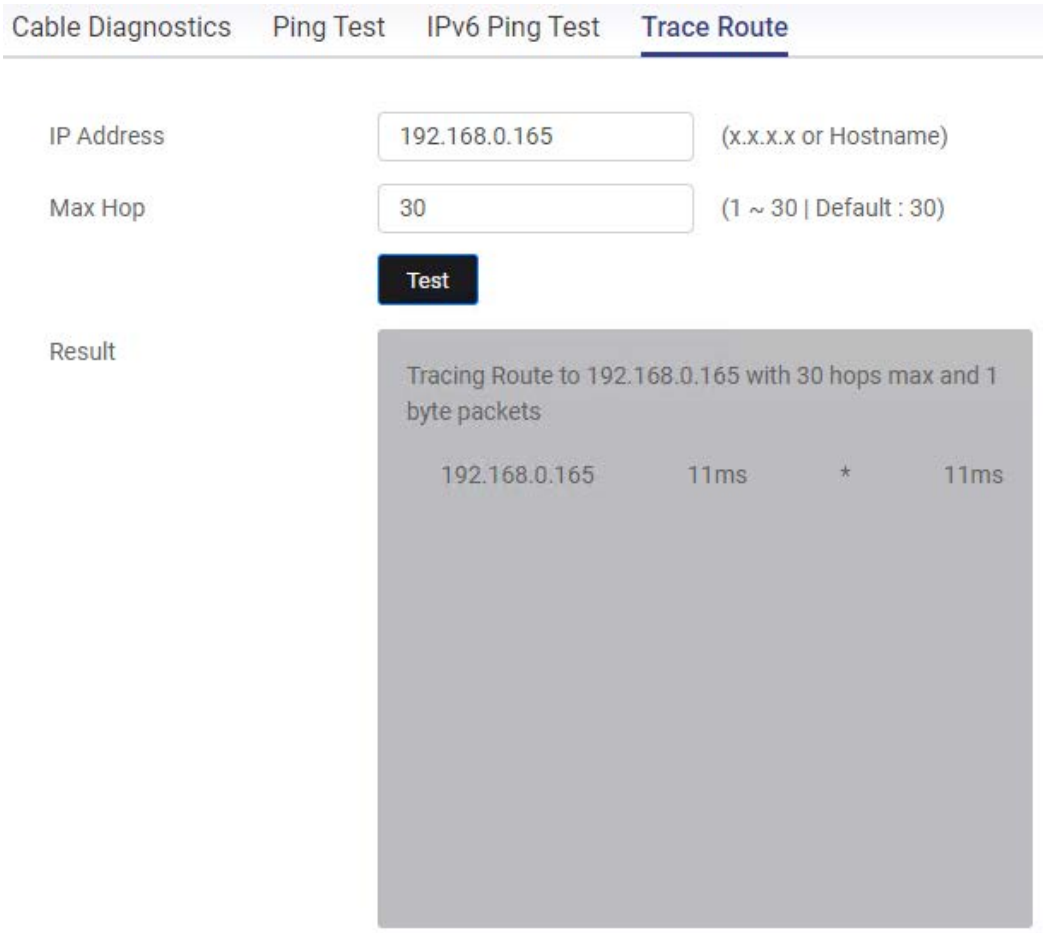

Figure 15-4 Trace Route

Items	Descriptions
IP Address	Enter the IP address or the host name of the station you wish the switch to ping to.
Max Hop	Enter the maximum number of hops. The range is from 2 to 255 and the default is 30.
Result	Displays the trace route results.

16 User Management

Use the User Management page to control management access to the switch based on manually configured usernames and passwords. A user account can only view settings without the right to configure the switch, and an admin account can configure all the functions of the switch. Click the Add button to add an account or the Edit button to edit an existing account.

Figure 16-1 User Management

Items	Descriptions
Username	Enter a username. You can use up to 18 alphanumeric characters.
Password Type	Select Clear Text or Encrypted from the list.
Password	Enter a new password for accessing the switch.
Password Retype	Repeat the new password used to access the switch.
Privilege Type	Select Admin or User from the list to regulate access rights.

Important:
Note that admin users have full access rights to the switch when determining the authority of the user account.

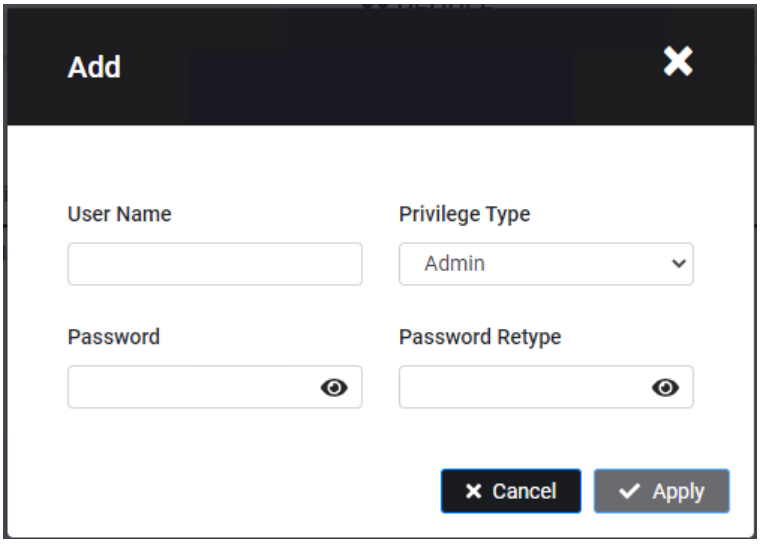

Figure 16-2 User Management(Add Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

17 802.1X

When a supplicant is connected to a switch port, the port issues an 802.1X authentication request to the attached the 802.1X supplicant. The supplicant replies with the given username and password, and an authentication request is then passed to a configured RADIUS server. The authentication server's user database supports Extended Authentication Protocol (EAP), which allows particular VLAN memberships to be defined based on each individual user. After authorization, the port connected to the authenticated supplicant then becomes a member of the specified VLAN. When the supplicant is successfully authenticated, traffic is automatically assigned to the VLAN. The EAP authentication methods supported by the switch are EAP-MD5, EAP-PEAP, and EAP-CHAPv2.

17.1 Global Settings

Figure 17-1 Global Settings

Items	Descriptions
State	Select whether authentication is Enabled or Disabled on the switch.
Guest VLAN	Select whether Guest VLAN is Enabled or Disabled on the switch. The default is Disabled.
Guest VLAN ID	Select the guest VLAN ID from the list of currently defined VLANs.

Click **Apply** to update the system settings.

17.2 Port Settings

The IEEE 802.1X port-based authentication provides a security standard for network access control with RADIUS servers and holds a network port disconnected until authentication is completed. With 802.1X port-based authentication, the supplicant provides the required credentials, such as username, password, or digital certificate to the authenticator, and the authenticator forwards the credentials to the authentication server for verification to the guest VLAN. If the authentication server determines the credentials are valid, the supplicant is allowed to access resources located on the protected side of the network.

From here, you can configure the port settings as they relate to 802.1X. First, select the mode you wish to utilize from the drop-down box. Next, choose whether to enable or disable re-authentication for the port. Enter the time span that you wish to elapse for the re-authentication Period, Quiet Period, and Supplicant Period. After this, enter the max number of times you wish for the switch to retransmit the EAP request. Finally, choose whether you wish to enable or disable the VLAN ID.

Click **Edit** to update the system settings.

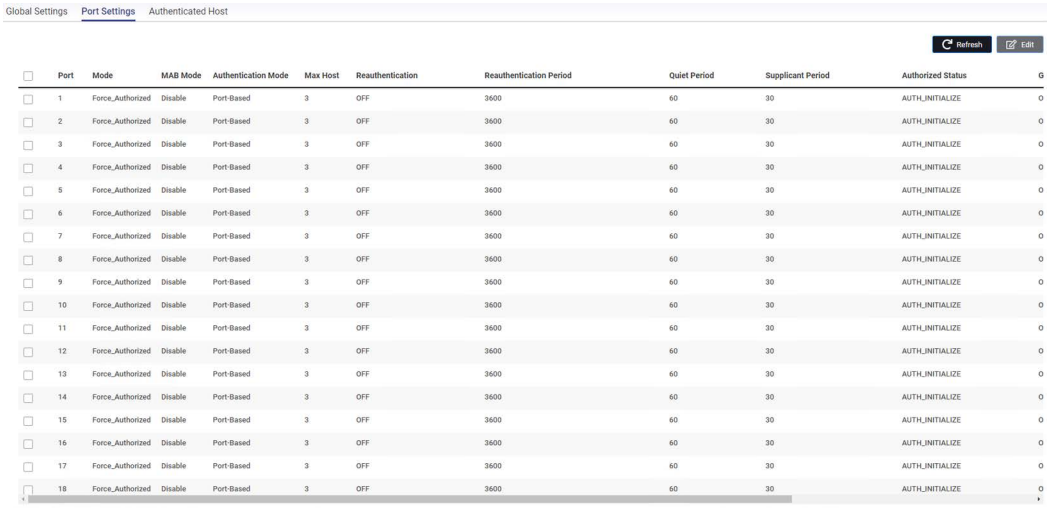

Figure 17-2 Port Settings

Items	Descriptions
Port	Displays the ports for which the 802.1X information is displayed.

Items	Descriptions
Mode	Select Auto or Force_UnAuthorized or Force_Authorized mode from the list.
Re-Authentication	Select whether port re-authentication is Enabled or Disabled.
Re-authentication period	Enter the time span in which the selected port is re-authenticated. The default is 3600 seconds.
Quiet Period	Enter the number of the device that remains in the quiet state following a failed authentication exchange. The default is 60 seconds.
Supplicant Period	Enter the amount of time that lapses before an EAP request is resent to the supplicant. The default is 30 seconds.
Max Retry	Enter the maximum number of times that the switch retransmits an EAP request to the client before it times out the authentication session. The default is 2 times.
Guest VLAN ID	Select whether guest VLAN ID is Enabled or Disabled.

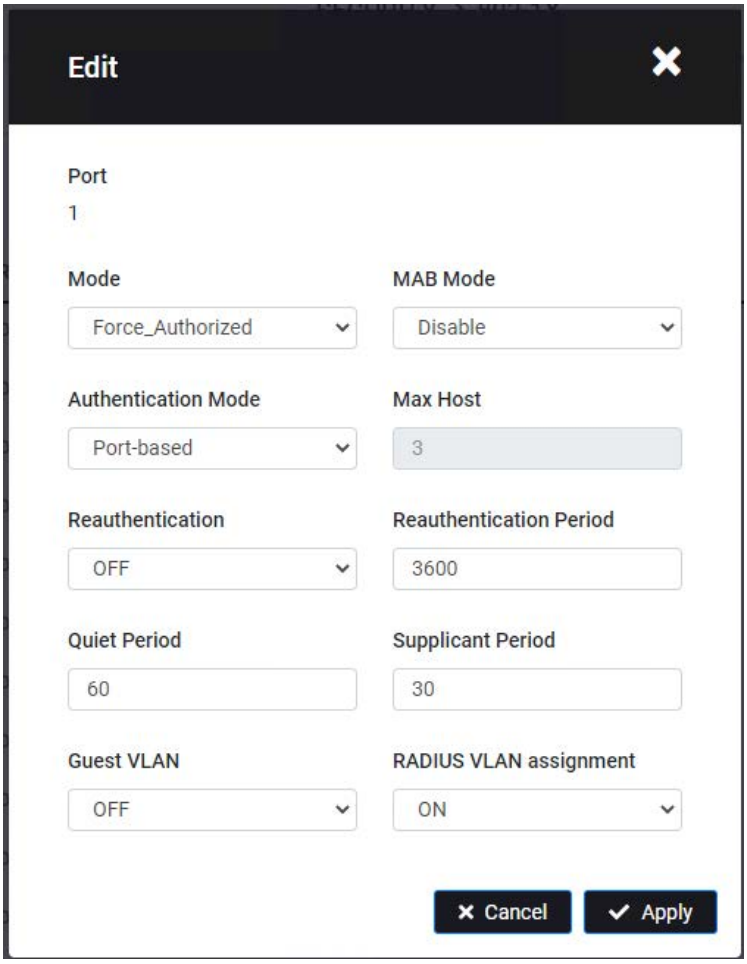

Figure 17-3 Port Settings(Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

17.3 Authenticated Host

The Authenticated Host section displays the Authenticated Username, Port, Session Time, Authenticated Method, and Mac Address.

Figure 17-4 Authenticated Host

18 Access

18.1 Web

The EnGenius Switch provides a built-in browser interface that enables you to configure and manage the switch via Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) requests selectively to help prevent security breaches on the network. You can manage your HTTP and HTTPS settings for the switch further by choosing the length of session timeouts for HTTP and HTTPS requests. Select whether to enable or disable the HTTP service and enter the HTTP Timeout session. Next, select whether to enable or disable the HTTPS service and enter the HTTPS timeout session for the switch.

Figure 18-1 Web

Items	Descriptions
Timeout	Enter the amount of time that elapses before HTTP is timed out. The default is 5 minutes. The range is from 0 to 86400 minutes.
HTTP Service	Select whether HTTP service for the switch is Enabled or Disabled. This is enabled by default.
HTTPS Service	Select whether the HTTP service is Enabled or Disabled. This is disabled by default.

Click **Apply** to update the system settings.

18.2 CLI

From here, you can configure and manage the switch's Telnet protocol settings. The Telnet protocol is a standard Internet protocol which enables terminals and applications to interface over the Internet with remote hosts by providing Command Line Interface (CLI) communication using a virtual terminal connection. This protocol provides the basic rules for making it

possible to link a client to a command interpreter. The Telnet service for the switch is enabled by default. Please note that for secure communication, it is better to use SSH over Telnet.

To configure SSH settings for the switch, first select whether you wish to enable or disable the SSH service for the switch. Note that SSH is more secure than the Telnet service when deciding which service to use. Enter the session timeout you wish to implement for SSH. Secure Shell (SSH) is a cryptographic network protocol for secure data communication network services. SSH is a way of accessing the command line interface on the network switch. The traffic is encrypted, so it is difficult to eavesdrop as it creates a secure connection within an insecure network such as the Internet. Even if an attacker were able to view the traffic, the data would be incomprehensible without the correct encryption key to decode it.

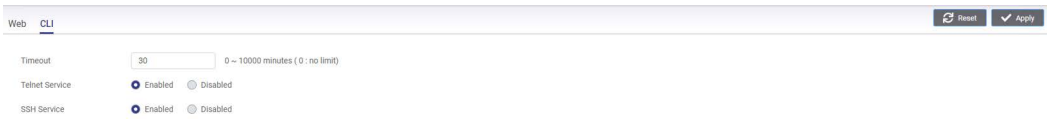

Figure 18-2 CLI

Items	Descriptions
Timeout	Enter the amount of time that elapses before the Telnet service is timed out. The default is 5 minutes. The range is from 0 to 65535 minutes.
Telnet Service	Select whether the Telnet service is Enabled or Disabled. It is enabled by default.
SSH Service	Select whether the SSH service is Enabled or Disabled. It is disabled by default.

Click **Apply** to update the system settings.

19 Port Security

Network security can be increased by limiting access on a specific port to users with specific MAC addresses. Port Security prevents unauthorized devices to the switch prior to stopping the auto-learning processing.

Click **Edit** to update the system settings.

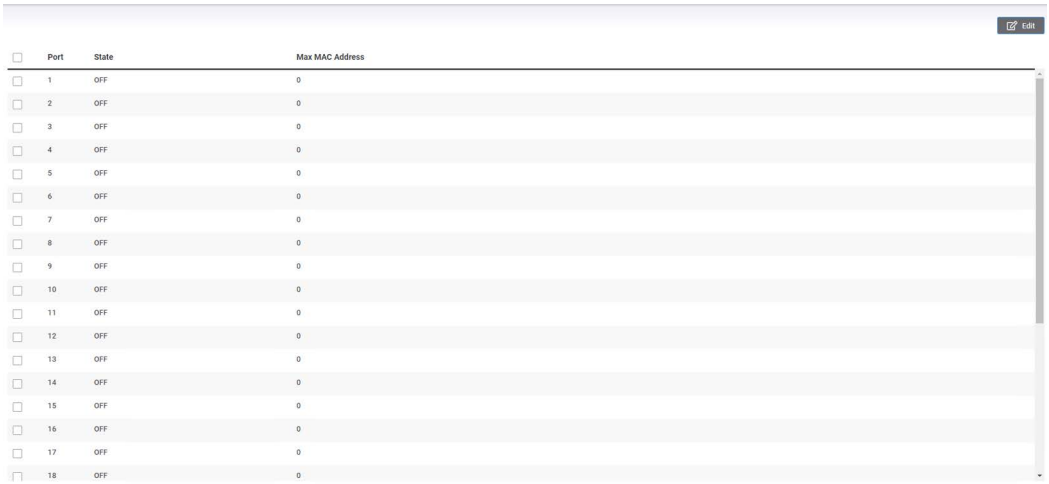

Figure 19-1 Port Security

Items	Descriptions
Port	Displays the port for which the port security is defined.
State	Select Enabled or Disabled for the port security feature for the selected port.
Max MAC Address	Enter the maximum number of MAC addresses that can be learned on the port. The range is from 1 to 256.

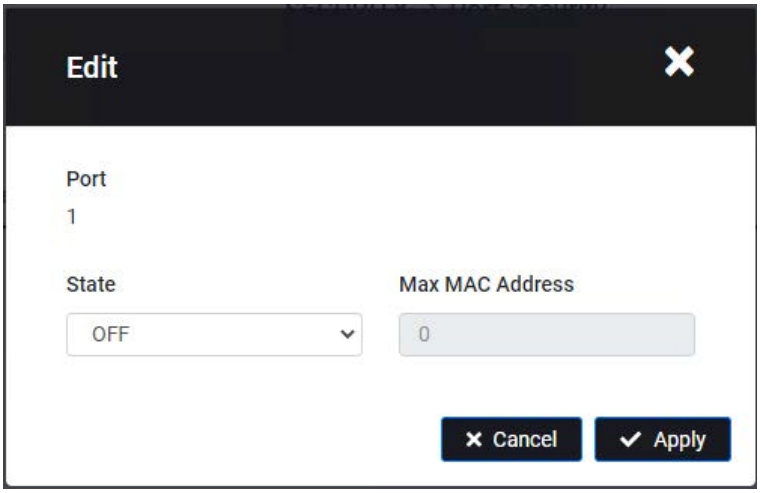

Figure 19-2 Port Security(Edit Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

20 RADIUS Server

RADIUS proxy servers are used for centralized administration.

Remote Authentication Dial in User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service for greater convenience.

RADIUS is a server protocol that runs in the application layer, using UDP as transport.

The Network switch with port-based authentication and all have a RADIUS client component that communicates with the RADIUS server.
Clients connected to a port on the switch must be authenticated by the Authentication server before accessing services offered by the switch on the LAN.

Use a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the client and server.

The RADIUS server maintains a user database, which contains authentication information.
The switch passes information to the configured RADIUS server, which can authenticate a username and password before authorizing use of the network.

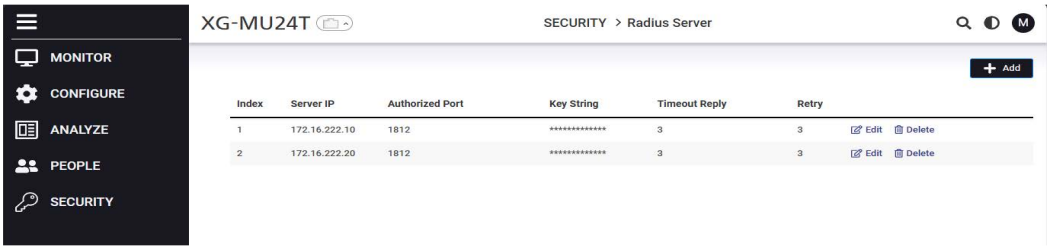

Figure 20-1 RADIUS Server

Items	Description
Index	Displays the index for registered RADIUS servers. The RADIUS server with the lower number has a higher priority. When the priority is set in the CLI, the index displayed may not match the actual priority.
Server IP	Enter the RADIUS server IP address.
Authorized Port	Enter the authorized port number. The default port is 1812.
Key String	Enter the key string used for encrypting all RADIUS communication between the device and the RADIUS server.
Timeout Reply	Enter the amount of time the device waits for an answer from the RADIUS server before switching to the next server. The default value is 3.
Retry	Enter the nSumber of transmitted requests sent to the RADIUS server before a failure occurs. The default is 3.

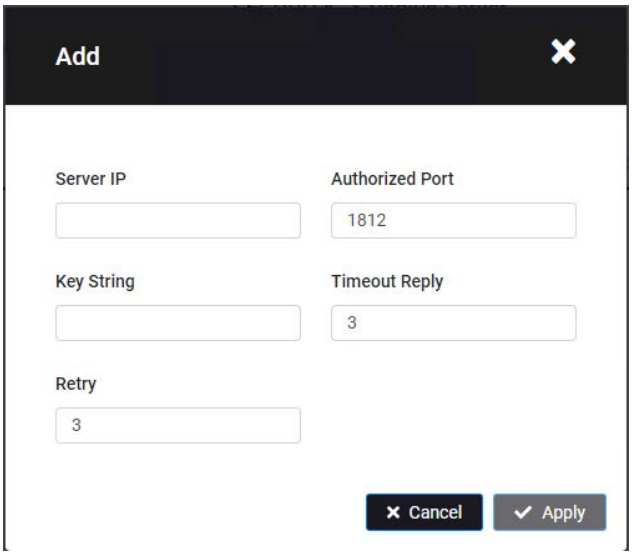

Figure 20-2 RADIUS Server(Add Screen)

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

21 DoS

DoS (Denial of Service) is used for classifying and blocking specific types of DoS attacks. From here, you can configure the switch to monitor and block different types of attacks.
On this page, the user can enable or disable the prevention of different types of DoS attacks.

Figure 21-1 DoS

Click **Apply** to update the system settings.

Panasonic Electric Works Networks Co., Ltd.

P0424-4016