Chapter 3

Managing Switch

3.1 First Time Setup

3.1.1 Overview

The Industrial Ethernet Managed Switch is a configurable device that facilitates the interconnection of Ethernet devices on an Ethernet network. This includes computers, operator interfaces, I/O, controllers, RTUs, PLCs, other switches/hubs or any device that supports the standard IEEE 802.3 protocol.

This switch has all the capabilities of a store and forward Ethernet switch plus advanced management features such as SNMP, RSTP and port mirroring. This manual details how to configure the various management parameters in this easy to use switch.

3.1.2 Introduction

To take full advantage of all the features and resources available from the switch, it must be configured for your network.

The switch implements Rapid Spanning Tree Protocol (RSTP) and Simple Network Management Protocol (SNMP) to provide most of the services offered by the switch. Rapid Spanning Tree Protocol allows managed switches to communicate with each other to ensure that there exists only one active route between each pair of network nodes and provides automatic failover to the next available redundant route. A brief explanation of how RSTP works is given in the Spanning Tree section.

The switch is capable of communicating with other SNMP capable devices on the network to exchange management information. This statistical/derived information from the network is saved in the Management Information Base (MIB) of the switch. The MIB is divided into several different information storage groups. These groups will be elaborated in detail in the Management and SNMP information section of this document. The switch implements Internet Group Management Protocol (IGMP) to optimize the flow of multicast traffic on your network.

The switch supports both port-based and tag-based Virtual LANs for flexible integration with VLAN-aware networks with support for VLAN-unaware devices.

Note! *Please go to **Tools** > **Save Configuration** to save your configuration changes if you want to keep your configuration after system reboot.*

3.1.3 Administrative Interface Access

There are several administrative interfaces to the switch:

1. A graphical web interface accessible via the switch's built-in web server, supporting HTTP.

Note! *This is the recommended method for managing the switch.*

2. An SNMP interface can be used to read/write many settings.

3.1.4 Using the Graphical (Web) Interface

The graphical interface is provided via a web server in the switch and can be accessed via a web browser such as Opera, Mozilla, or Internet Explorer.

Note! *JavaScript must be supported and enabled in your browser for the graphical interface to work correctly.*

HTTP is supported to access the web server. By default, both protocols are enabled. Either or both may be disabled to secure the switch. (See the Remote Access Security topic in this section.)

To access the graphical interface, enter a URL like HTTP://192.168.1.1 in your browser's address bar.

The web server in the switch uses a signed security certificate. When you access the server via http, you may see a warning dialog indicating that the certificate was signed by an unknown authority. This is expected and to avoid this message in the future you can choose to install the certificate on your computer.

Note! *This manual describes and depicts the web user interface in detail. The terminal interface is not specifically shown but is basically the same.*

3.1.5 Configuring the Switch for Network Access

To control and monitor the switch via the network, it must be configured with basic network settings, including an IP address and subnet mask. Refer to the quick start guide in Section 1 for how to access your switch initially.

To configure the switch for network access, select [Add Menu Address Here] to reach the System Settings menu. The settings in this menu control the switch's general network configuration.

- DHCP Enabled/Disabled: The switch can automatically obtain an IP address from a server using the Dynamic Host Configuration Protocol (DHCP). This can speed up initial set up, as the network administrator does not have to find an open IP address.
- IP Address and subnet mask configuration: The IP address for the switch can be changed to a user-defined address along with a customized subnet mask to separate subnets.

Note! *Advanced users can set the IP address to 0.0.0.0 to disable the use of an IP address for additional security. However, any features requiring an IP address (i.e., web interface, etc.) will no longer be available.*

- Default Gateway Selection: A Gateway Address is chosen to be the address of a router that connects two different networks. This can be an IP address or a Fully Qualified Domain Name (FQDN) such as “domainname.org”.
- NTP Server: The IP address or domain name of an NTP (Network Time Protocol) server from which the switch may retrieve the current time at startup. Please note that using a domain name requires that at least one domain name server be configured.

3.1.6 Configuring the Ethernet Ports

The switch comes with default port settings that should allow you to connect to the Ethernet Ports with out any necessary configuration. Should there be a need to change the name of the ports, negotiation settings or flow control settings, you can do this in the Port Configuration menu. Access this menu by selecting Setup from the Main menu, and then selecting Main Settings.

- Port Name: Each port in the managed switch can be identified with a custom name. Specify a name for each port here.
- Admin: Ports can be enabled or disabled in the managed switch. For ports that are disabled, they are virtually non-existent (not visible in terms of switch operation or spanning tree algorithm). Choose to enable or disable a port by selecting Enabled or Disabled, respectively.
- Negotiation: All copper ports and gigabit fiber ports in the managed switch are capable of auto-negotiation such that the fastest bandwidth is selected. Choose to enable auto-negotiation or use fixed settings. 100Mbps Fiber ports are Fixed speed only.
- Speed/Duplex/Flow Control: The managed switch accepts three local area network Ethernet Standards. The first standard, 10BASE-T, runs 10Mbps with twisted pair Ethernet cable between network interfaces. The second local area network standard is 100BASE-T, which runs at 100Mbps over the same twisted pair Ethernet cable. Lastly, there is 100BASE-F, which enables fast Ethernet (100Mbps) over fiber.

These options are available:

- 10h–10 Mbps, Half Duplex
- 10f –10 Mbps, Full Duplex
- 100h–100 Mbps, Half Duplex
- 100f –100 Mbps, Full Duplex

On managed switches with gigabit combination ports, those ports with have two rows, a standard row of check boxes and a row labeled “SFP” with radio buttons. The SFP setting independently sets the speed at which a transceiver will operate if one is plugged in. Otherwise, the switch will use the fixed Ethernet port and the corresponding settings for it.

3.2 Web Browser Configuration

The switch has an HTML based user interface embedded in the flash memory. The interface offers an easy to use means to manage basic and advanced switch functions. The interface allows for local or remote switch configuration anywhere on the network.

The interface is designed for use with [Internet Explorer (6.0), Chrome, Firefox].

3.2.1 Preparing for Web Configuration

The interface requires the installation and connection of the switch to the existing network. A PC also connected to the network is required to connect to the switch and access the interface through a web browser. The required networking information is provided as follows:

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.1.254
- User name: admin
- Password: admin

3.3 Log In

To access the login window, connect the device to the network, see “Connecting the Switch to Ethernet Ports” on page 22. Once the switch is installed and connected, power on the switch see the following procedures to log into your switch.

When the switch is first installed, the default network configuration is set to DHCP enabled. You will need to make sure your network environment supports the switch setup before connecting it to the network.

1. Launch your web browser on a computer.
2. In the browser’s address bar type in the switch’s default IP address (192.168.1.1). The login screen displays.
3. Enter the default user name and password (admin/admin) to log into the management interface. You can change the default password after you have successfully logged in.
4. Click **Login** to enter the management interface.

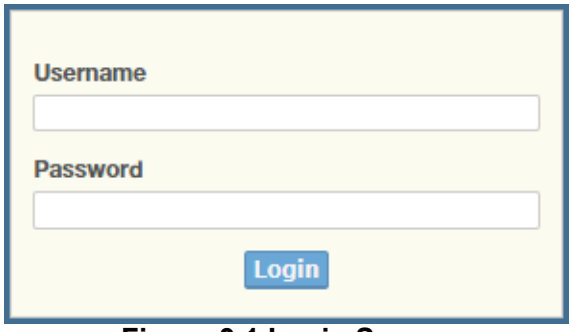


Figure 3.1 Login Screen

3.4 Recommended Practices

One of the easiest things to do to help increase the security posture of the network infrastructure is to implement a policy and standard for secure management. This practice is an easy way to maintain a healthy and secure network.

After you have performed the basic configurations on your switches, the following is a recommendation which is considered best practice policy.

3.4.1 Changing Default Password

In keeping with good management and security practices, it is recommended that you change the default password as soon as the device is functioning and setup correctly. The following details the necessary steps to change the default password.

To change the password:

1. Navigate to **Tools** > **User Account**.
2. From the User drop-down menu, select the Admin (default) account.
3. In the **User Name** field, enter admin for this account. It is not necessary to change the user name, however, a change in the default settings increases the security settings.
4. In the **Password** field, type in the new password. Re-type the same password in the **Retype Password** field.

5. Click **Apply** to change the current account settings.

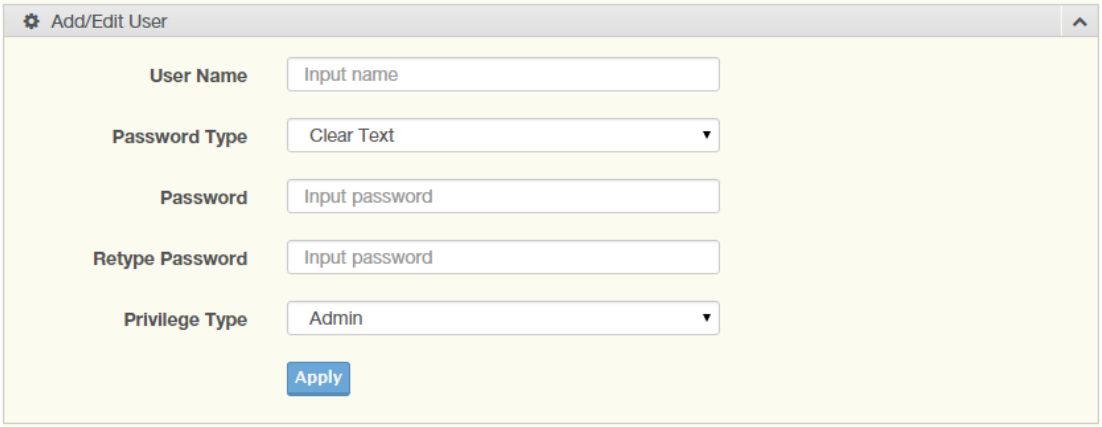


Figure 3.2 Changing a Default Password

After saving all the desired settings, perform a system save (**Tools** > **Save Configuration**). The changes are saved.

3.5 Monitoring

3.5.1 Device Information

The Device Information menu lists information, such as: System Name, System Location, MAC Address, Firmware version, and more, pertaining to the system. The information is for review only. To modify the device information, see the respective item within the user interface.

To access this page, click **Monitoring** > **Device Information**.

Device Information

Information Name	Information Value
System Name	Switch
System Location	Default
System Contact	Default
MAC Address	00:D0:C9:F5:0F:71
IP Address	192.168.1.157
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
Loader Version	1.01.S05012
Loader Date	Jul 06 2021 - 13:45:38
Firmware Version	3.00.02
Firmware Date	Jul 06 2021 - 14:05:32
System OID	1.3.6.1.4.1.10297.202.3001
System Up Time	23 days, 22 hours, 50 mins, 7 secs

Figure 3.3 Monitoring > Device Information

The following table describes the items in the previous figure.

Item	Description
System Name	Click **Switch** to enter the system name: up to 128 alphanumeric characters (default is Switch).

Item	Description
System Location	Click **Default** to enter the location: up to 256 alphanumeric characters (default is Default).
System Contact	Click **Default** to enter the contact person: up to 128 alphanumeric characters (default is Default).
MAC Address	Displays the MAC address of the switch.
IP Address	Displays the assigned IP address of the switch.
Subnet Mask	Displays the assigned subnet mask of the switch.
Gateway	Displays the assigned gateway of the switch.
Loader Version	Displays the current loader version of the switch.
Loader Date	Displays the current loader build date of the switch.
Firmware Version	Displays the current firmware version of the switch.
Firmware Date	Displays the current firmware build date of the switch.
System Object ID	Displays the base object ID of the switch.
System Up Time	Displays the time since the last switch reboot.

3.5.2 Logging Message

The Logging Message Filter page allows you to enable the display of logging message filter.

To access this page, click **Monitoring** > **Logging Message**.

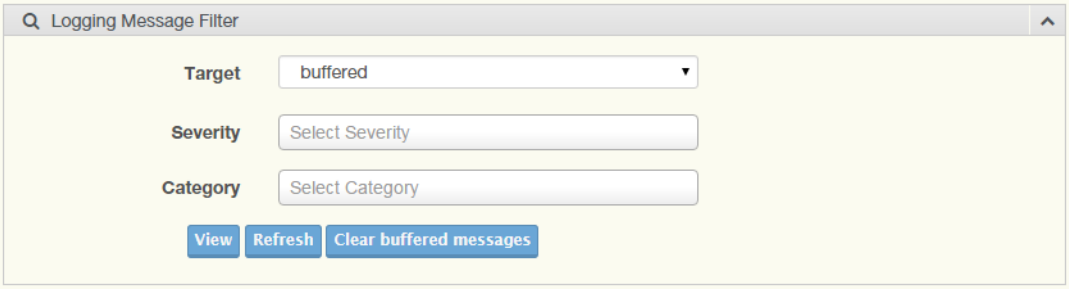


Figure 3.4 Monitoring > Logging Message

The following table describes the items in the previous figure.

Item	Description
Target	Click the drop-down menu to select a target to store the log messages. ■ Buffered: Store log messages in RAM. All log messages are cleared after system reboot. ■ File: Store log messages in a file.
Severity	The setting allows you to designate a severity level for the Logging Message Filter function. Click the drop-down menu to select the severity level target setting. The level options are: ■ emerg: Indicates system is unusable. It is the highest level of severity. ■ alert: Indicates action must be taken immediately. ■ crit: Indicates critical conditions. ■ error: Indicates error conditions. ■ warning: Indicates warning conditions. ■ notice: Indicates normal but significant conditions. ■ info: Indicates informational messages. ■ debug: Indicates debug-level messages.

Item	Description
Category	Click the drop-down menu to select the category level target setting.
View	Click **View** to display all Logging Information and Logging Message information.
Refresh	Click **Refresh** to update the screen.
Clear buffered messages	Click **Clear buffered messages** to clear the logging buffer history list.

The ensuing table for **Logging Information** table settings are informational only: Target, Severity and Category.

Logging Information

Information Name	Information Value
Target	buffered
Severity	emerg, alert, crit, error, warning, notice
Category	ACL, CABLE_DIAG, IGMP_SNOOPING, MLD_SNOOPING, L2, LLDP, Mirror, Platform, PM, Port, QoS, Rate, SNMP, STP, LBD, GVRP, Security, System, Trunk, VLAN, XRing

Figure 3.5 Monitoring > Logging Message

The ensuing table for **Logging Message** table settings are informational only: No., Time Stamp, Category, Severity and Message.

Logging Message

No.	Time Stamp	Category	Severity	Message
1	Jan 25 2000 13:20:43	System	notice	New http connection for user admin, source 192.168.1.15 ACCEPTED
2	Jan 25 2000 08:34:58	System	notice	New http connection for user admin, source 192.168.1.15 ACCEPTED
3	Jan 25 2000 07:41:13	System	notice	New http connection for user admin, source 192.168.1.15 ACCEPTED
4	Jan 25 2000 06:49:10	System	notice	New http connection for user admin, source 192.168.1.15 ACCEPTED
5	Jan 25 2000 06:47:02	Port	notice	GigabitEthernet8 link up
6	Jan 25 2000 06:44:28	System	notice	New http connection for user admin, source 192.168.1.15 ACCEPTED
7	Jan 25 2000 06:43:58	Port	notice	GigabitEthernet5 link up
8	Jan 25 2000 06:43:53	Port	notice	GigabitEthernet5 link down
9	Jan 25 2000 06:24:51	Port	notice	GigabitEthernet5 link up
10	Jan 22 2000 01:17:45	Port	notice	GigabitEthernet5 link down

Showing 1 to 10 of 20 Messages Previous 1 2 Next

Figure 3.6 Monitoring > Logging Message

3.5.3 Port Monitoring

Port Network Monitor is a bandwidth and network monitoring tool for the purpose of capturing network traffic and measuring of network throughput. The monitoring functionality includes listing of port statistics as well as port utilization.

3.5.3.1 Port Statistics

To access this page, click **Monitoring** > **Port Monitoring** > **Port Statistics**.

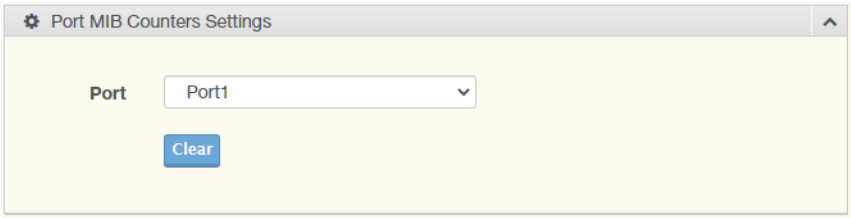


Figure 3.7 Monitoring > Port Monitoring > Port Statistics

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select a port and its captured statistical setting values.
Clear	Click **Clear** to clear the counter selections.

The ensuing table for **IF MIB Counters** settings are informational only: ifInOctets, ifInUcastPkts, ifInNUcastPkts, ifInDiscards, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts, ifOutDiscards, ifInMulticastPkts, ifInBroadcastPkts, ifOutMulticastPkts and ifOutBroadcastPkts.

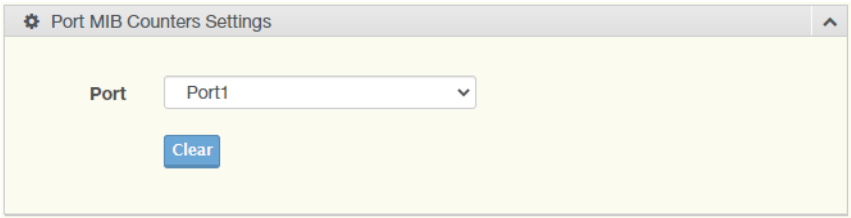


Figure 3.8 Monitoring > Port Monitoring > Port Statistics > IF MIB Counters

The ensuing table for **Ether-Like MIB Counters** settings are informational only: dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsSingleCollisionFrames, dot3StatsMultipleCollisionFrames, dot3StatsDeferredTransmissions, dot3StatsLateCollisions, dot3StatsExcessiveCollisions, dot3StatsFrameTooLongs, dot3StatsSymbolErrors, dot3ControlInUnknownOpcodes, dot3InPauseFrames and dot3OutPauseFrames.

Port1 Ether-Like MIB Counters

Ether-Like MIB Counter Name	MIB Counter Value
dot3StatsAlignmentErrors	0
dot3StatsFCSErrors	0
dot3StatsSingleCollisionFrames	0
dot3StatsMultipleCollisionFrames	0
dot3StatsDeferredTransmissions	0
dot3StatsLateCollisions	0
dot3StatsExcessiveCollisions	0
dot3StatsFrameTooLongs	0
dot3StatsSymbolErrors	0
dot3ControlInUnknownOpcodes	0
dot3InPauseFrames	0
dot3OutPauseFrames	0

Figure 3.9 Monitoring > Port Monitoring > Port Statistics > IF MIB Counters

3.5.3.2 Port Utilization

To access this page, click **Monitoring** > **Port Monitoring** > **Port Utilization**.

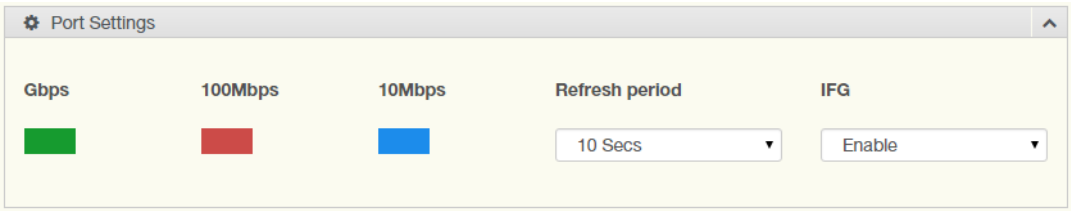


Figure 3.10 Monitoring > Port Monitoring > Port Utilization

The following table describes the items in the previous figure.

Item	Description
Refresh period	Click the drop-down menu to select and designate a period (second intervals) to refresh the information (TX and RX) listings.
IFG	Click the drop-down menu to enable or disable the Interframe Gap (IFG) statistic.

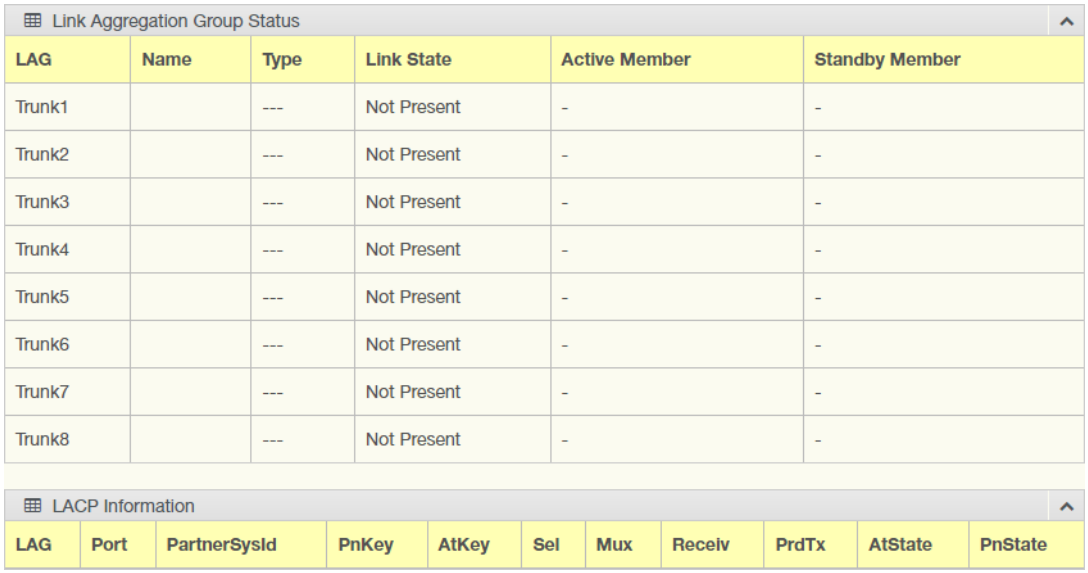
3.5.4 Link Aggregation

The Link Aggregation function provides LAG information for each trunk. It displays membership status, link state and membership type for each port.

To access this page, click **Monitoring** > **Link Aggregation**.

The ensuing table for **Link Aggregation Group Status** settings are informational only: LAG, Name, Type, Link State, Active Member and Standby Member.

The ensuing table for **LACP Information** settings are informational only: LAG, Port, PartnerSysId, PnKey, AtKey, Sel, Mux, Receiv, PrdTx, AtState and PnState.



Link Aggregation Group Status

LAG	Name	Type	Link State	Active Member	Standby Member
Trunk1		---	Not Present	-	-
Trunk2		---	Not Present	-	-
Trunk3		---	Not Present	-	-
Trunk4		---	Not Present	-	-
Trunk5		---	Not Present	-	-
Trunk6		---	Not Present	-	-
Trunk7		---	Not Present	-	-
Trunk8		---	Not Present	-	-

LACP Information

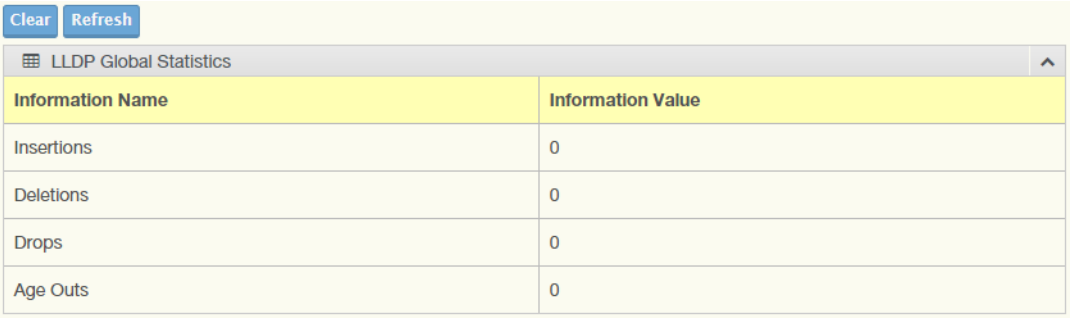
LAG	Port	PartnerSysId	PnKey	AtKey	Sel	Mux	Receiv	PrdTx	AtState	PnState

Figure 3.11 Monitoring > Link Aggregation

3.5.5 LLDP Statistics

The LLDP Statistics page displays the LLDP statistics.

To access this page, click **Monitoring** > **LLDP Statistics**.



Clear Refresh

LLDP Global Statistics

Information Name	Information Value
Insertions	0
Deletions	0
Drops	0
Age Outs	0

Figure 3.12 Monitoring > LLDP Statistics

The following table describes the items in the previous figure.

Item	Description
Clear	Click **Clear** to reset LLDP Statistics of all the interfaces.
Refresh	Click **Refresh** to update the data on the screen with the present state of the data in the switch.

The ensuing table for **LLDP Global Statistics** settings are informational only: Insertions, Deletions, Drops and Age Outs.

The ensuing table for **LLDP Port Statistics** settings are informational only: Port, TX Frames (Total), RX Frames (Total, Discarded and Errors), RX TLVs (Discarded and Unrecognized) and RX Ageouts (Total).

LLDP Port Statistics

Port	TX Frames	RX Frames			RX TLVs		RX Ageouts
	Total	Total	Discarded	Errors	Discarded	Unrecognized	Total
Port1	0	0	0	0	0	0	0
Port2	0	0	0	0	0	0	0
Port3	0	0	0	0	0	0	0
Port4	0	0	0	0	0	0	0
Port5	155602	894	3	0	0	0	1
Port6	0	0	0	0	0	0	0
Port7	0	0	0	0	0	0	0
Port8	232	2	0	0	0	0	0

Figure 3.13 Monitoring > LLDP Statistics

3.5.6 IGMP Statistics

The IGMP Statistics function displays statistical package information for IP multicasting.

To access this page, click **Monitoring** > **IGMP Statistics**.

Clear Refresh

IGMP Statistics

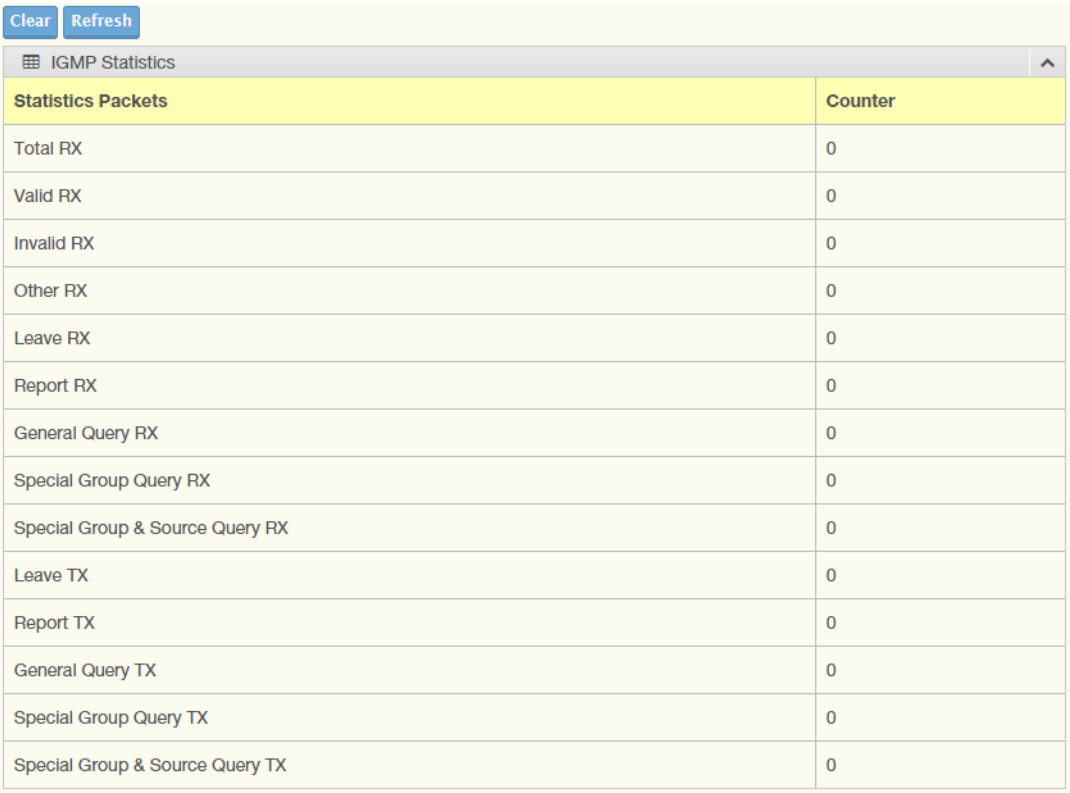
Statistics Packets	Counter
Total RX	0
Valid RX	0
Invalid RX	0
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Special Group Query RX	0
Special Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Special Group Query TX	0
Special Group & Source Query TX	0

Figure 3.14 Monitoring > IGMP Statistics

The following table describes the items in the previous figure.

Item	Description
Clear	Click **Clear** to refresh IGMP Statistics of all the interfaces.
Refresh	Click **Refresh** to update the data on the screen with the present state of the data in the switch.

The ensuing table for **IGMP Statistics** settings are informational only: Total RX, Valid RX, Invalid RX, Other RX, Leave RX, Report RX, General Query RX, Special Group Query RX, Special Group & Source Query RX, Leave TX, Report TX, General Query TX, Special Group Query TX and Special Group & Source Query TX.



Statistics Packets	Counter
Total RX	0
Valid RX	0
Invalid RX	0
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Special Group Query RX	0
Special Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Special Group Query TX	0
Special Group & Source Query TX	0

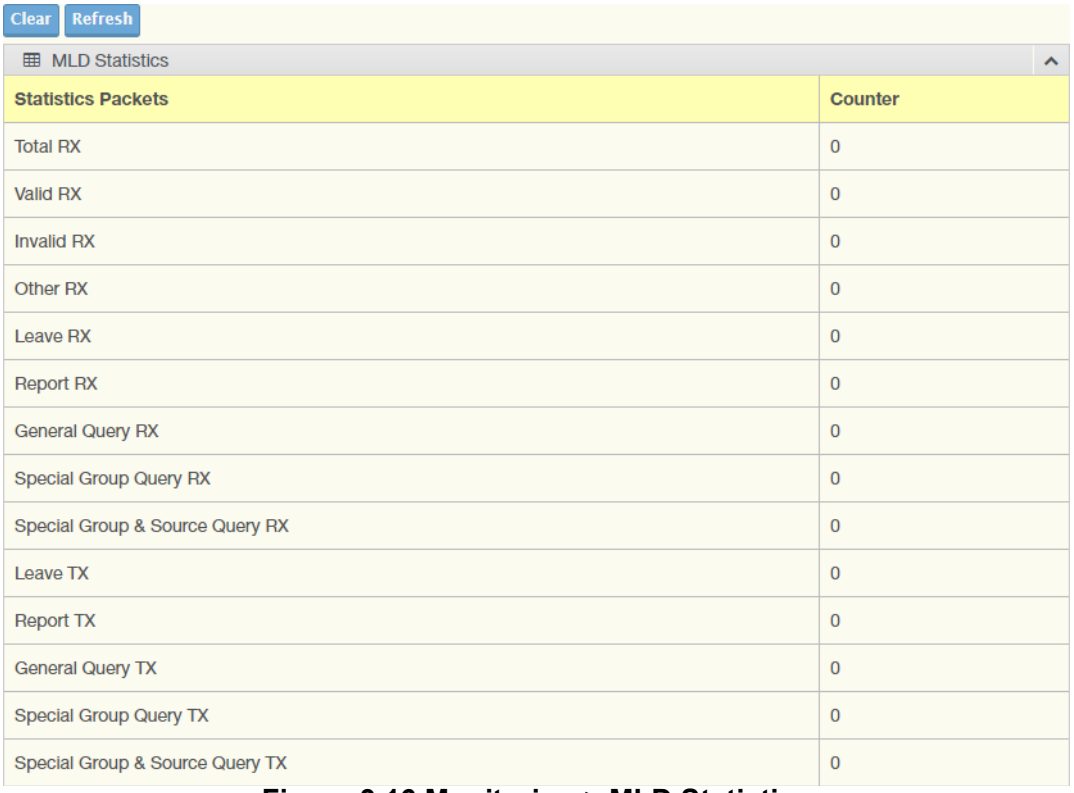
Figure 3.15 Monitoring > IGMP Statistics

3.5.7 MLD Statistics

The MLD Statistics function displays information about Multicast Listener Discovery (MLD) statistics. By default, the device collects statistics of received and transmitted MLD control messages regarding currently active multicast group subscribers.

The ensuing table for **MLD Statistics** settings are informational only: Total RX, Valid RX, Invalid RX, Other RX, Leave RX, Report RX, General Query RX, Special Group Query RX, Special Group & Source Query RX, Leave TX, Report TX, General Query TX, Special Group Query TX, and Special Group & Source Query TX.

To access this page, click **Monitoring** > **MLD Statistics**.



Statistics Packets	Counter
Total RX	0
Valid RX	0
Invalid RX	0
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Special Group Query RX	0
Special Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Special Group Query TX	0
Special Group & Source Query TX	0

Figure 3.16 Monitoring > MLD Statistics

The following table describes the items in the previous figure.

Item	Description
Clear	Click **Clear** to refresh IGMP Statistics of all the interfaces.
Refresh	Click **Refresh** to update the data on the screen with the present state of the data in the switch.

3.6 System

3.6.1 IP Settings

The IP Settings menu allows you to select a static or DHCP network configuration. The Static displays the configurable settings for the static option.

To access this page, click **System** > **IP Settings**.

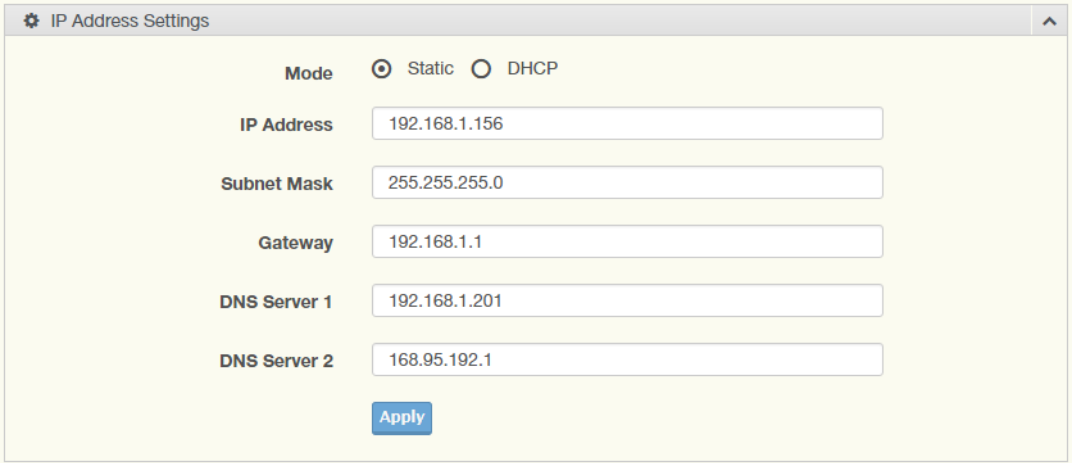


Figure 3.17 System > IP Settings

The following table describes the items in the previous figure.

Item	Description
Mode	Click the radio button to select the IP Address Setting mode: Static, DHCP, or BOOTP. **Note:** PN models do not support the Mode feature.
IP Address	Enter a value to specify the IP address of the interface. The default is 192.168.1.1.
Subnet Mask	Enter a value to specify the IP subnet mask for the interface. The default is 255.255.255.0.
Gateway	Enter a value to specify the default gateway for the interface. The default is 192.168.1.254.
DNS Server 1	Enter a value to specify the DNS server 1 for the interface. The default is 168.95.1.1.
DNS Server 2	Enter a value to specify the DNS server 2 for the interface. The default is 168.95.192.1.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **IP Address Information** settings are informational only: DHCP State, BOOTP State, Static IP Address, Static Subnet Mask, Static Gateway, Static DNS Server 1 and Static DNS Server 2.

IP Address Information

Information Name	Information Value
Mode	Static
Current IP Address	192.168.1.157
Current Subnet Mask	255.255.255.0
Current Gateway	192.168.1.1
Current DNS Server 1	192.168.1.1
Static IP Address	192.168.1.157
Static Subnet Mask	255.255.255.0
Static Gateway	192.168.1.1
Static DNS Server 1	192.168.1.1
Static DNS Server 2	0.0.0.0

Figure 3.18 System > IP Settings > IP Address

3.6.2 IPv6 Settings

To access this page, click **System** > **IPv6 Settings**.

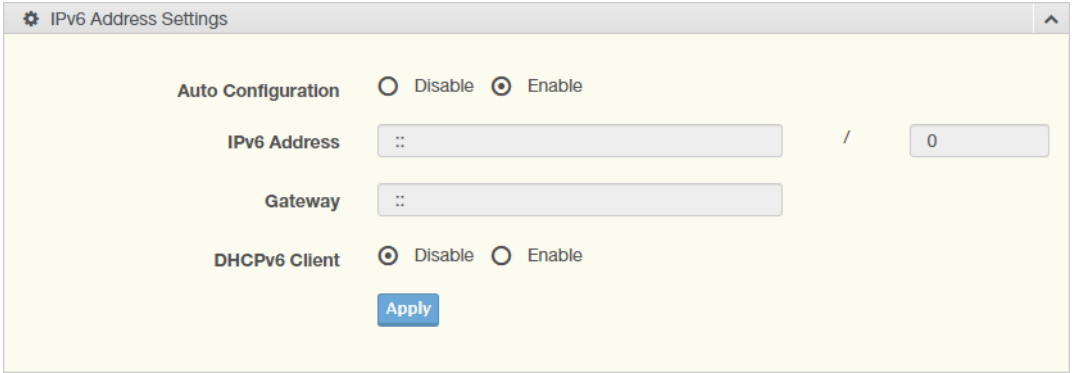
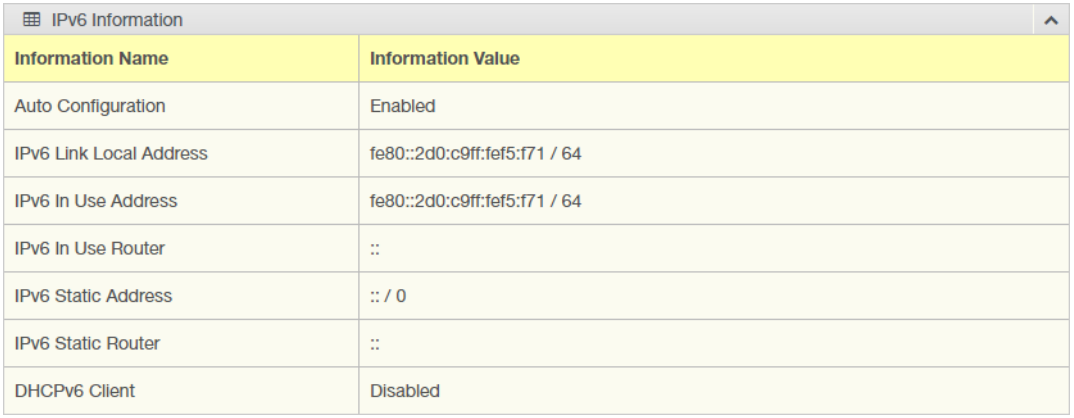


Figure 3.19 System > IPv6 Settings

The following table describes the items in the previous figure.

Item	Description
Auto Configuration	Select the radio button to enable or disable the IPv6.
IPv6 Address	Enter a value to specify the IP address of the interface. The default is fe80::2d0:c9ff:fef5:f71 / 64.
Gateway	Enter a value to specify the default gateway for the interface.
DHCPv6 Client	Click to enable or disable the DHCPv6 client. Enter the DHCPv6 address for the system.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **IPv6 Information** settings are informational only: Information Name, Auto Configuration, IPv6 Link Local Address, IPv6 In Use Address, IPv6 In Use Router, IPv6 Static Address, IPv6 Static Router, DHCPv6 Client.


IPv6 Information

Information Name	Information Value
Auto Configuration	Enabled
IPv6 Link Local Address	fe80::2d0:c9ff:fef5:f71 / 64
IPv6 In Use Address	fe80::2d0:c9ff:fef5:f71 / 64
IPv6 In Use Router	::
IPv6 Static Address	:: / 0
IPv6 Static Router	::
DHCPv6 Client	Disabled

Figure 3.20 System > IPv6 Settings

3.6.3 DHCP Client Option 82

The DHCP Client Option 82 configurable Circuit ID and Remote ID feature (not supported on PN models) enhances validation security by allowing you to select naming choices sub options. You can select a switch-configured hostname or specify an ASCII test string for the remote ID. You can also configure an ASCII text string to override the circuit ID.

Note! *PN models do not support the DHCP Client Option 82 feature.*

To access this page, click **System** > **DHCP Client Option 82**.

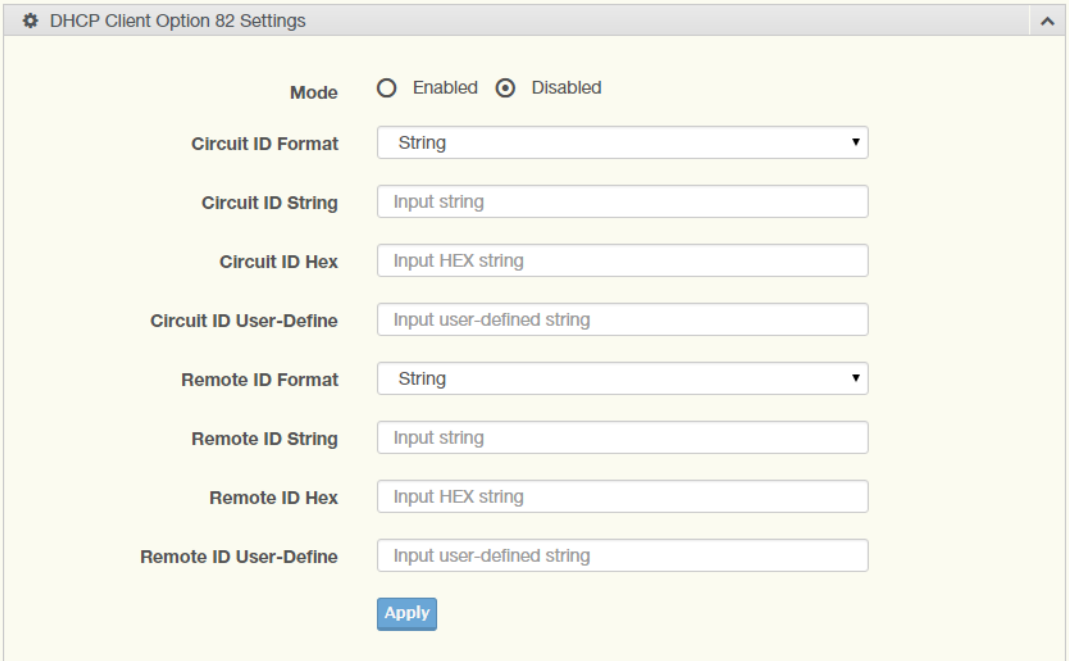


Figure 3.21 System > DHCP Client Option 82

The following table describes the items in the previous figure.

Item	Description
Mode	Click the radio button to enable or disable the DHCP Client Option 82 mode.
Circuit ID Format	Click the drop-down menu to set the ID format: String, Hex, User Definition.
Circuit ID String	Enter the string ID of the corresponding class.
Circuit ID Hex	Enter the hex string of the corresponding class.
Circuit ID User-Define	Enter the user definition of the corresponding class.
Remote ID Format	Click the drop-down menu to set the Remote ID format: String, Hex, User Definition.
Remote ID String	Enter the remote string ID of the corresponding class.
Remote ID Hex	Enter the remote hex string of the corresponding class.
Remote ID User-Define	Enter the remote user definition of the corresponding class.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **DCHP Client Option 82 Information** settings are informational only: Information Name, Status, Circuit ID Format, Circuit ID String, Circuit ID Hex,

Circuit ID User-Define, Remote ID Format, Remote ID String, Remote ID Hex, Remote ID User-Define.

DHCP Client Option 82 Information

Information Name	Information Value
Status	Disabled
Circuit ID Format	String
Circuit ID String	
Circuit ID Hex	
Circuit ID User-Define	
Remote ID Format	String
Remote ID String	
Remote ID Hex	
Remote ID User-Define	

Figure 3.22 System > DHCP Client Option 82

3.6.4 DHCP Auto Provision

The DHCP Auto Provision feature (not supported on PN models) allows you to load configurations using a server with DHCP options. Through the remote connection, the switch obtains information from a configuration file available through the TFTP server.

Note! *PN models do not support the DHCP Auto Provision feature.*

To access this page, click **System** > **DHCP Auto Provision**.

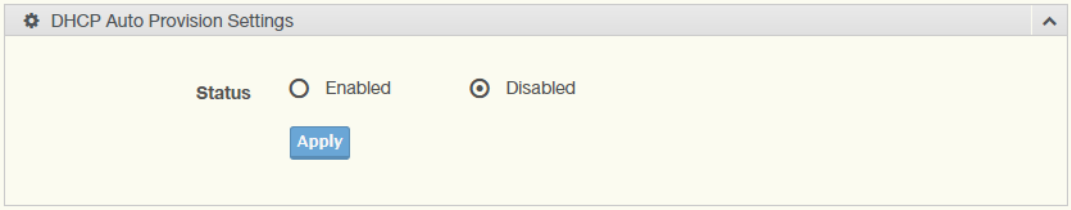


Figure 3.23 System > DHCP Auto Provision

The following table describes the items in the previous figure.

Item	Description
Status	Select the radio button to enable or disable the DHCP Auto Provisioning Setting.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **DHCP Auto Provision Information** settings are informational only: Status.

DHCP Auto Provision Information

Information Name	Information Value
Status	Disabled

Figure 3.24 System > DHCP Auto Provision

3.6.5 Management VLAN

By default the VLAN is the management VLAN providing communication with the switch management interface.

To access this page, click **System** > **Management VLAN**.

Figure 3.25 System > Management VLAN

The following table describes the items in the previous figure.

Item	Description
Management VLAN	Click the drop-down menu to select a defined VLAN.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Management VLAN State** are informational only: Management VLAN.

Figure 3.26 System > Management VLAN

3.6.6 System Time

To access this page, click **System** > **System Time**.

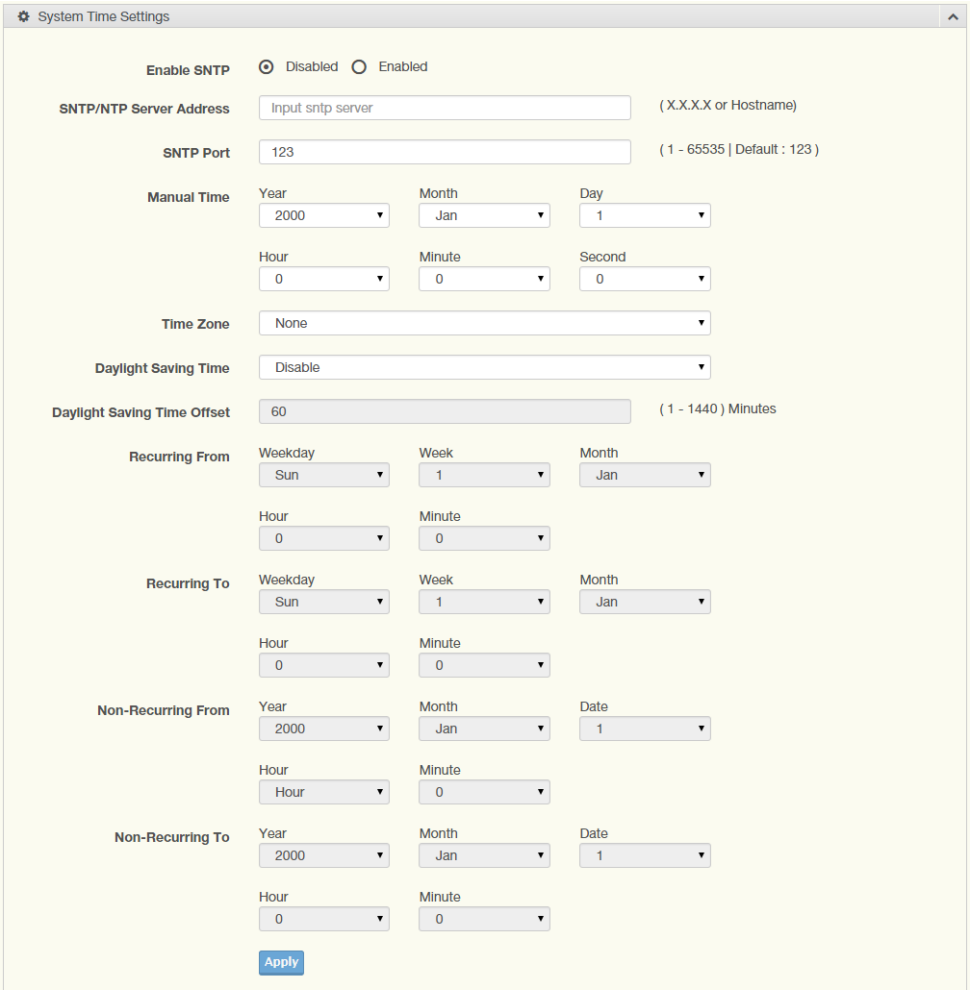


Figure 3.27 System > System Time

The following table describes the items in the previous figure.

Item	Description
Enable SNTP	Click the radio button to enable or disable the SNTP.
SNTP/NTP Server Address	Enter the address of the SNTP server. This is a text string of up to 64 characters containing the encoded unicast IP address or hostname of a SNTP server. Unicast SNTP requests will be sent to this address. If this address is a DNS hostname, then that hostname should be resolved into an IP address each time a SNTP request is sent to it.
SNTP Port	Enter the port on the server to which SNTP requests are to be sent. Allowed range is 1 to 65535 (default: 123).
Manual Time	Click the drop-down menus to set local date and time of the system.
Time Zone	Click the drop-down menu to select a system time zone.
Daylight Saving Time	Click the drop-down menu to enable or disable the daylight saving time settings.
Daylight Saving Time Offset	Enter the offsetting variable in seconds to adjust for daylight saving time.
Recurring From	Click the drop-down menu to designate the start date and time for daylight saving time.
Recurring To	Click the drop-down menu to designate the end date and time for daylight saving time.

Item	Description
Non-Recurring From	Click the drop-down menu to designate a start date and time for a non-recurring daylight saving time event.
Non-Recurring To	Click the drop-down menu to designate the end date and time for a non-recurring daylight saving time event.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **System Time Information** settings are informational only: Current Date/Time, SNTP, SNTP Server Address, SNTP Server Port, Time zone, Daylight Saving Time, Daylight Saving Time Offset, From and To.

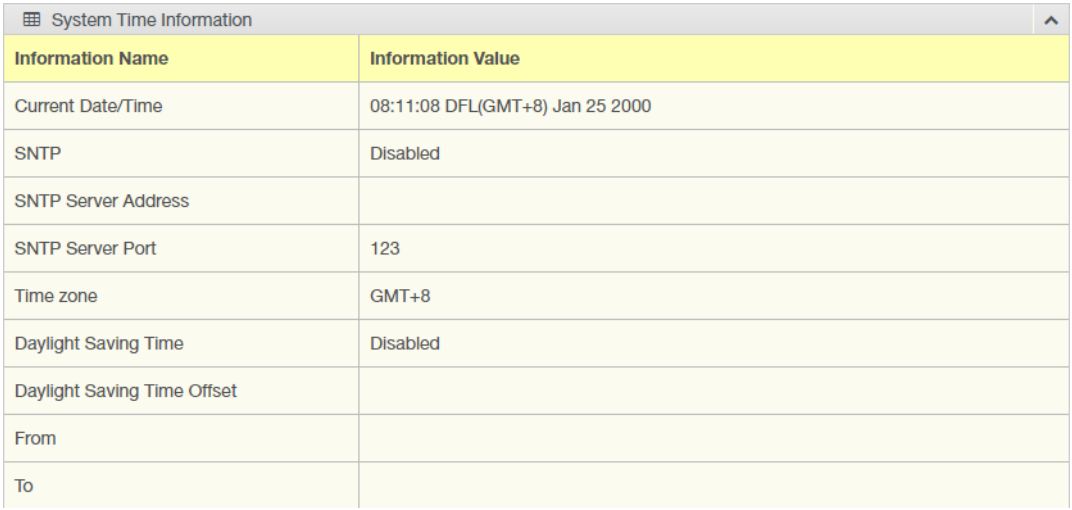


Figure 3.28 System > System Time

3.6.7 Network Port

To access this page, click **System** > **Network Port**.

Figure 3.29 System > Network Port

The following table describes the items in the previous figure.

Item	Description
HTTP	By default, the HTTP port setting is set to port 80. To assign the web interface to a different port, enter the port number in the field.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Port Status** settings are informational only: Protocol Name, Port Value.

Figure 3.30 System > Network Port

3.7 L2 Switching

3.7.1 Port Configuration

Port Configuration describes how to use the user interface to configure LAN ports on the switch.

To access this page, click **L2 Switching** > **Port Configuration**.

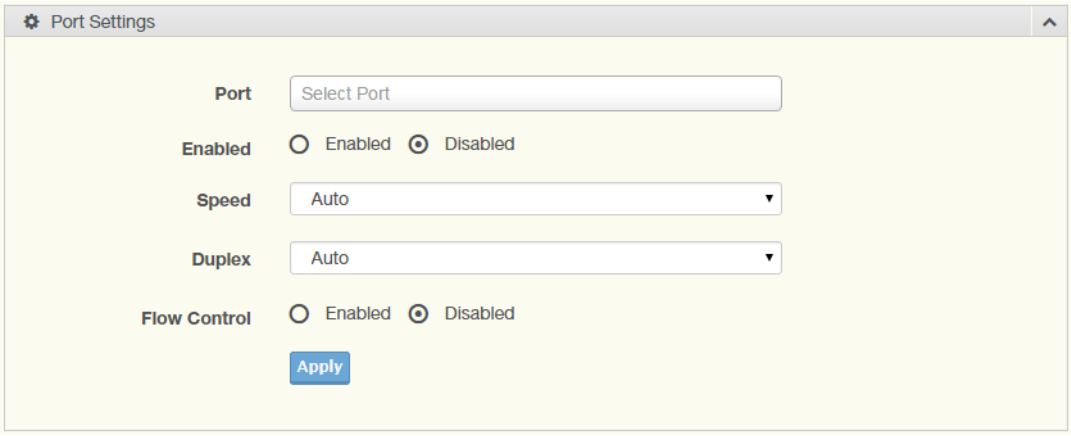


Figure 3.31 L2 Switching > Port Configuration

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select the port for the L2 Switch setting.
Enabled	Click the radio-button to enable or disable the Port Setting function.
Speed	Click the drop-down menu to select the port speed: Auto, Auto-10M, Auto-100M, Auto-1000M, Auto-10/100M, 10M, 100M or 1000M. **Note:** PN models only support the Speed and Duplex in a single feature setting.
Duplex	Click the drop-down menu to select the duplex setting: Auto, Full. or Half. **Note:** PN models only support the Speed and Duplex in a single feature setting.
Flow Control	Click the radio button to enable or disable the flow control function.
Apply	Click **Apply** to save the values and update the screen.

The **Port Name Settings** displays. To access this page, click **L2 Switching** > **Port Configuration**.

Figure 3.32 L2 Switching > Port Configuration

Item	Description
Display Method	Click the drop-down menu to select the port name display method: Description (default), Original.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Port Status** settings are informational only: Port, **Edit** (click to enter description), Enable State, Link Status, Speed, Duplex, FlowCtrl Config and FlowCtrl Status.

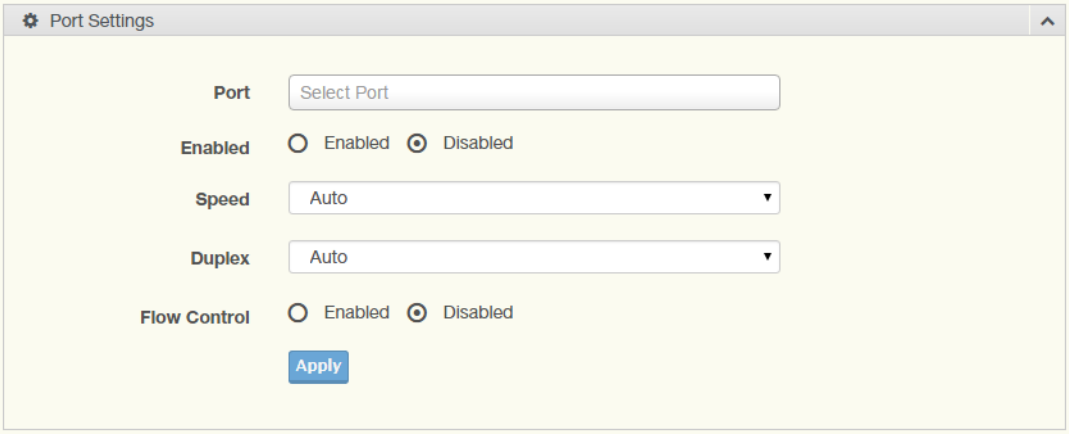


Figure 3.33 L2 Switching > Port Configuration > Port Name Settings

3.7.2 Port Mirror

Port mirroring function allows the sending of a copy of network packets seen on one switch port to a network monitoring connection on another switch port. Port mirroring can be used to analyze and debug data or diagnose errors on a network or to mirror either inbound or outbound traffic (or both).

There are no preset values in the Port Mirror. The displayed values do not represent the actual setting values.

To access this page, click **L2 Switching** > **Port Mirror**.

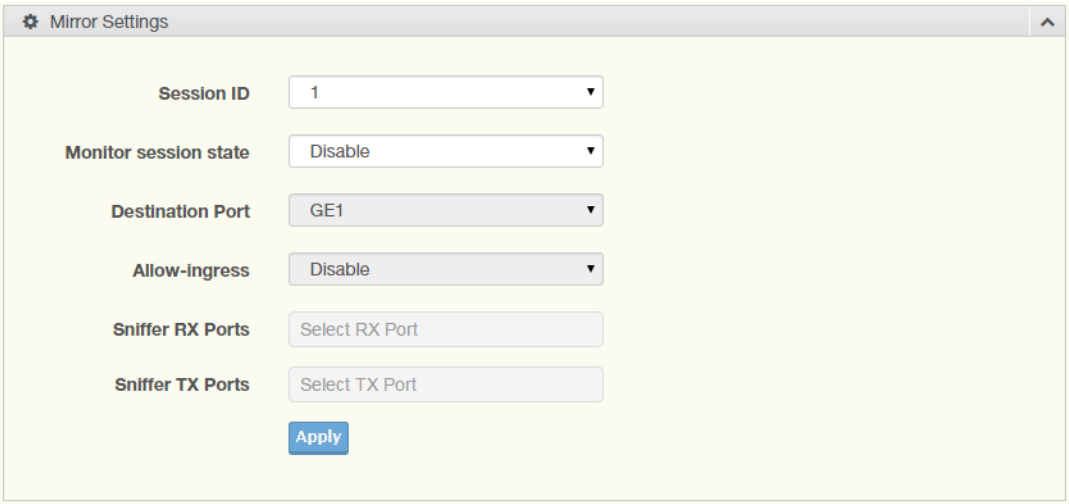


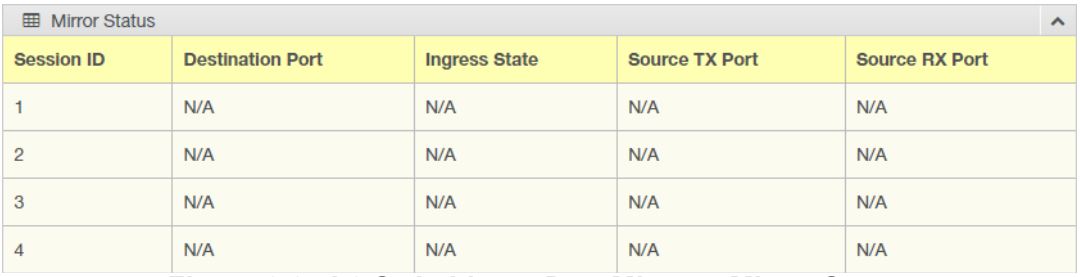
Figure 3.34 L2 Switching > Port Mirror

The following table describes the items in the previous figure.

Item	Description
Session ID	Click the drop-down menu to select a port mirroring session from the list. The number of sessions allowed is platform specific.
Monitor session state	Click the drop-down menu to enable or disable the session mode for a selected session ID.
Destination Port	Click the drop-down menu to select the destination port and receive all the traffic from configured mirrored port(s).
Allow-ingress	Click the drop-down menu to enable or disable the Allow-ingress function.

Item	Description
Sniffer RX Ports	Enter the variable to define the RX port.
Sniffer TX Ports	Enter the variable to define the TX port.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Mirror Status** settings are informational only: Session ID, Destination Port, Ingress State, Source TX Port and Source RX Port.


Mirror Status

Session ID	Destination Port	Ingress State	Source TX Port	Source RX Port
1	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A

Figure 3.35 L2 Switching > Port Mirror > Mirror Status

3.7.3 Link Aggregation

Link Aggregation is a method for combining multiple network connections in parallel in order to increase throughput beyond the capability of a single connection, and to provide redundancy in case one of the links should fail.

3.7.3.1 Load Balance

The Load Balancing page allows you to select between a MAC Address or IP/MAC Address algorithm for the even distribution of IP traffic across two or more links.

To access this page, click **L2 Switching** > **Link Aggregation** > **Load Balance**.

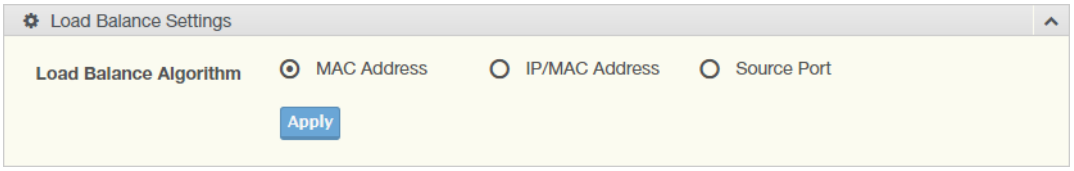
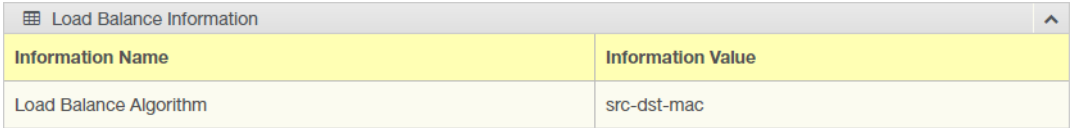


Figure 3.36 L2 Switching > Link Aggregation > Load Balance

The following table describes the items in the previous figure.

Item	Description
Load Balance Algorithm	Select the radio button to select the Load Balance Setting: MAC Address, IP/MAC Address, Source Port.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Load Balance Information** settings are informational only: Load Balance Algorithm.


Load Balance Information

Information Name	Information Value
Load Balance Algorithm	src-dst-mac

Figure 3.37 L2 Switching > Link Aggregation > Load Balance

3.7.3.2 LAG Management

Link aggregation is also known as trunking. It is a feature available on the Ethernet gateway and is used with Layer 2 Bridging. Link aggregation allows for the logical merging of multiple ports into a single link.

To access this page, click **L2 Switching** > **Link Aggregation** > **LAG Management**.

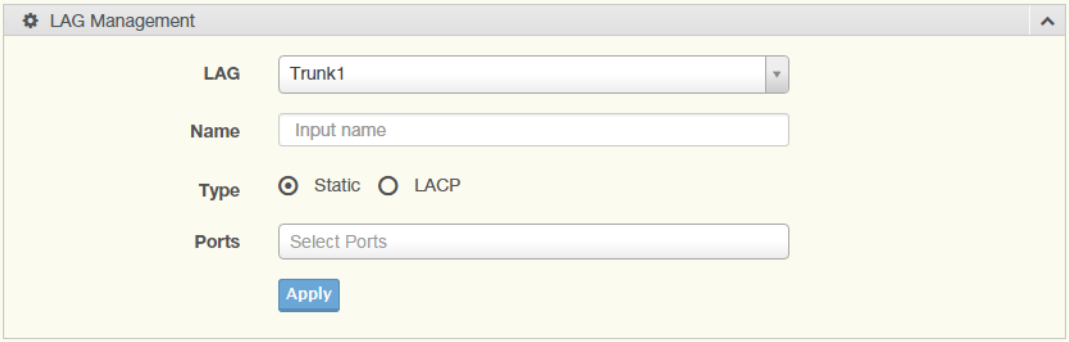


Figure 3.38 L2 Switching > Link Aggregation > LAG Management

The following table describes the items in the previous figure.

Item	Description
LAG	Click the drop-down menu to select the designated trunk group: Trunk 1~8.
Name	Enter an entry to specify the LAG name.
Type	Click the radio button to specify the type mode: Static or LACP.
Ports	Click the drop-down menu to select designated ports: Port1-10.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **LAG Management Information** settings are informational only: LAG, Name, Type, Link State, Active Member, Standby Member, **Edit** (click to modify the settings) and **Clear** (click to load default settings).

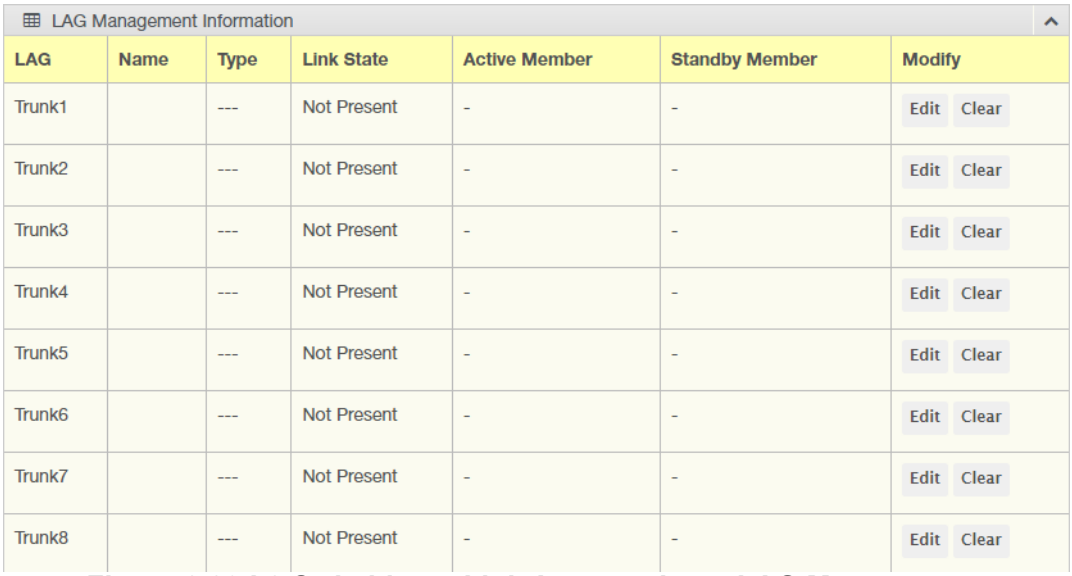


Figure 3.39 L2 Switching > Link Aggregation > LAG Management

3.7.3.3 LAG Port Settings

The LAG Port Settings page allows you to enable or disable, set LAG status, speed and flow control functions.

In this example we will configure a LAG between the following switches:

To access this page, click **L2 Switching** > **Link Aggregation** > **LAG Port Settings**.

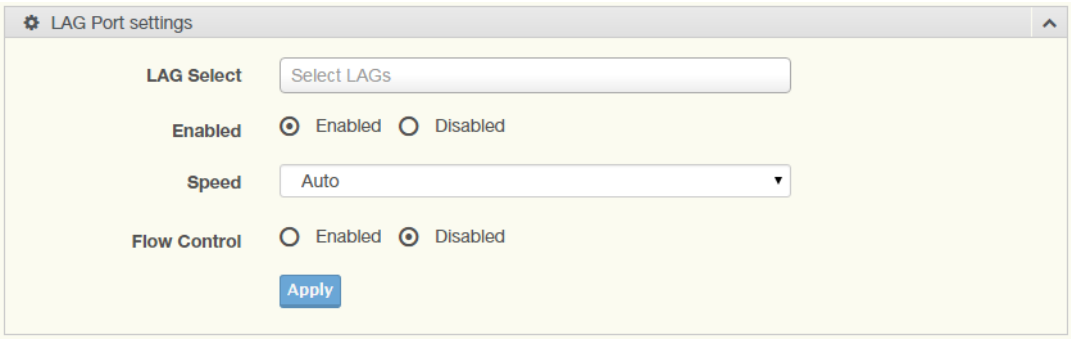


Figure 3.40 L2 Switching > Link Aggregation > LAG Port Settings

The following table describes the items in the previous figure.

Item	Description
LAG Select	Click the drop-down menu to select a predefined LAG trunk definition: LAG 1-8.
Enabled	Click the radio button to enable or disable the LAG Port.
Speed	Click the drop-down menu to select the port speed: Auto, Auto-10M, Auto-100M, Auto-10/100M, 10M or 100M.
Flow Control	Click the radio button to enable or disable the Flow Control for the LAG Port.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **LAG Port Status** settings are informational only: LAG, Description, Port Type, Enable State, Link Status, Speed, Duplex, FlowCtrl Config and FlowCtrl Status.

LAG Port Status

LAG	Description	Port Type	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
Trunk1			Enabled		Auto	Auto	Disabled	Disabled
Trunk2			Enabled		Auto	Auto	Disabled	Disabled
Trunk3			Enabled		Auto	Auto	Disabled	Disabled
Trunk4			Enabled		Auto	Auto	Disabled	Disabled
Trunk5			Enabled		Auto	Auto	Disabled	Disabled
Trunk6			Enabled		Auto	Auto	Disabled	Disabled
Trunk7			Enabled		Auto	Auto	Disabled	Disabled
Trunk8			Enabled		Auto	Auto	Disabled	Disabled

Figure 3.41 L2 Switching > Link Aggregation > LAG Port Status

3.7.3.4 LACP Priority Settings

The LACP Priority Settings page allows you to configure the system priority for LACP.

To access this page, click **L2 Switching** > **Link Aggregation** > **LACP Priority Settings**.

Figure 3.42 L2 Switching > Link Aggregation > LACP Priority Settings

The following table describes the items in the previous figure.

Item	Description
System Priority	Enter the value (1-65535) to designate the LACP system priority.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **LACP Information** settings are informational only: System Priority.

Figure 3.43 L2 Switching > Link Aggregation > LACP Priority Information

3.7.3.5 LACP Port Settings

Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. By configuring the LACP function, the switch can negotiate an automatic bundling of links by sending LACP packets to the peer device (also implementing LACP).

To access this page, click **L2 Switching** > **Link Aggregation** > **LACP Port Settings**.

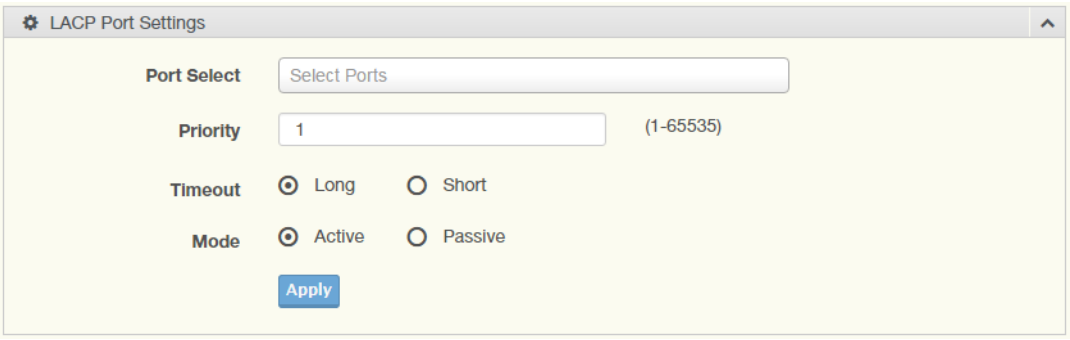


Figure 3.44 L2 Switching > Link Aggregation > LACP Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Select a port for the LACP Port Settings. The listed available settings are: Port1-10. However, the available settings are dependent on the connected LACP device and may not be listed as displayed in the current figure.
Priority	Enter a variable (1 to 65535) to assign a priority to the defined port selection.
Timeout	Click the radio button to select a long or short timeout period.
Mode	Click the radio button to select the setting mode: Active or Passive. ■ Active: Enables LACP unconditionally. ■ Passive: Enables LACP only when an LACP device is detected (default state).
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **LACP Port Information** settings are informational only: Port Name, Priority, Timeout and Mode.

LACP Port Information

Port Name	Priority	Timeout	Mode
Port1	1	Long	Passive
Port2	1	Long	Passive
Port3	1	Long	Passive
Port4	1	Long	Passive
Port5	1	Long	Passive
Port6	1	Long	Passive
Port7	1	Long	Passive
Port8	1	Long	Passive

Figure 3.45 L2 Switching > Link Aggregation > LACP Port Information

3.7.4 802.1Q VLAN

The 802.1Q VLAN feature allows for a single VLAN to support multiple VLANs. With the 802.1Q feature you can preserve VLAN IDs and segregate different VLAN traffic.

The 802.1Q VLAN tag feature encapsulates the 802.1Q VLAN tagging within another 802.1Q VLAN tag. The outer tag is assigned following the AP group, while the inner VLAN ID is assigned dynamically by the AAA server.

3.7.4.1 VLAN Management

The management of VLANs is available through the VLAN Settings page. Through this page you can add or delete VLAN listings and add a prefix name to an added entry.

To access this page, click **L2 Switching** > **802.1Q VLAN** > **VLAN Management**.

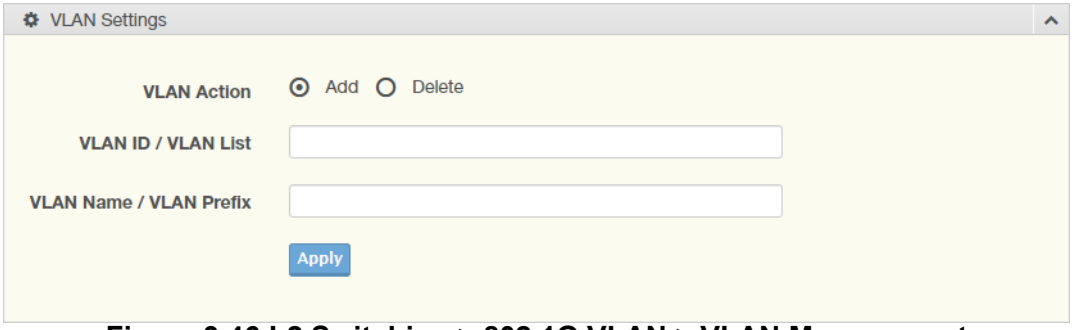


Figure 3.46 L2 Switching > 802.1Q VLAN > VLAN Management

The following table describes the items in the previous figure.

Item	Description
VLAN Action	Click the radio button to add or delete the VLAN entry shown in the previous field.
VLAN ID / VLAN List	Enter the name of the VLAN ID or list entry to setup.
VLAN Name / VLAN Prefix	Enter the prefix to be used by the VLAN list entry in the previous field.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **VLAN Table** settings are informational only: VLAN ID, VLAN Name, VLAN Type and **Edit** (click to enter VLAN name).

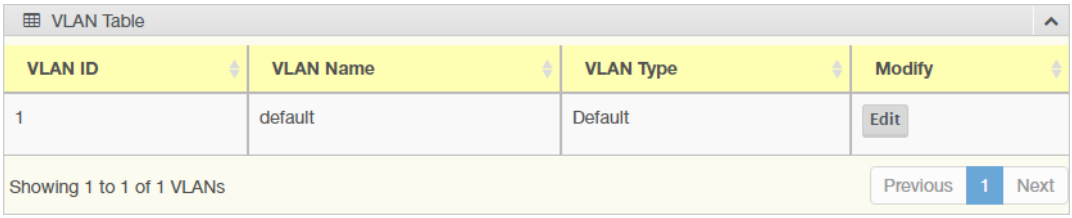


Figure 3.47 L2 Switching > 802.1Q VLAN > VLAN Table

3.7.4.2 PVID Settings

The PVID Settings page allows you to designate a PVID for a selected port, define the accepted type and enable/disable the ingress filtering.

To access this page, click **L2 Switching** > **802.1Q VLAN** > **PVID Settings**.

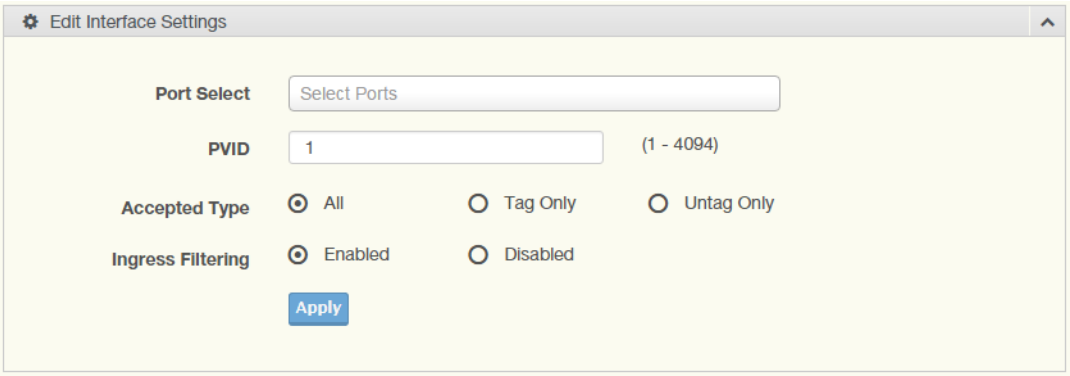


Figure 3.48 L2 Switching > 802.1Q VLAN > PVID Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Click the drop-down menu to select a port and edit its settings: Port1-10, or Trunk1 - Trunk8.
PVID	Enter the VLAN ID you want assigned to untagged or priority tagged frames received on this port. The value ranges 1 to 4094. The default is 1.
Accepted Type	Click the radio button to specify which frames to forward. Tag Only discards any untagged or priority tagged frames. Untag Only discards any tagged frames. All accepts all untagged and tagged frames. Whichever you select, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN standard. The default is All.
Ingress Filtering	Click the radio button to specify how you want the port to handle tagged frames. If you enable Ingress Filtering, a tagged frame will be discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. If you select Disabled, all tagged frames will be accepted. The default is Disabled.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Port VLAN Status** settings are informational only: Port, Interface VLAN Mode, PVID, Accept Frame Type and Ingress Filtering.

3.7.4.3 Port to VLAN

The Port to VLAN page allows you to add a port to a VLAN and select the related parameters.

To access this page, click **L2 Switching** > **802.1Q VLAN** > **Port to VLAN**.

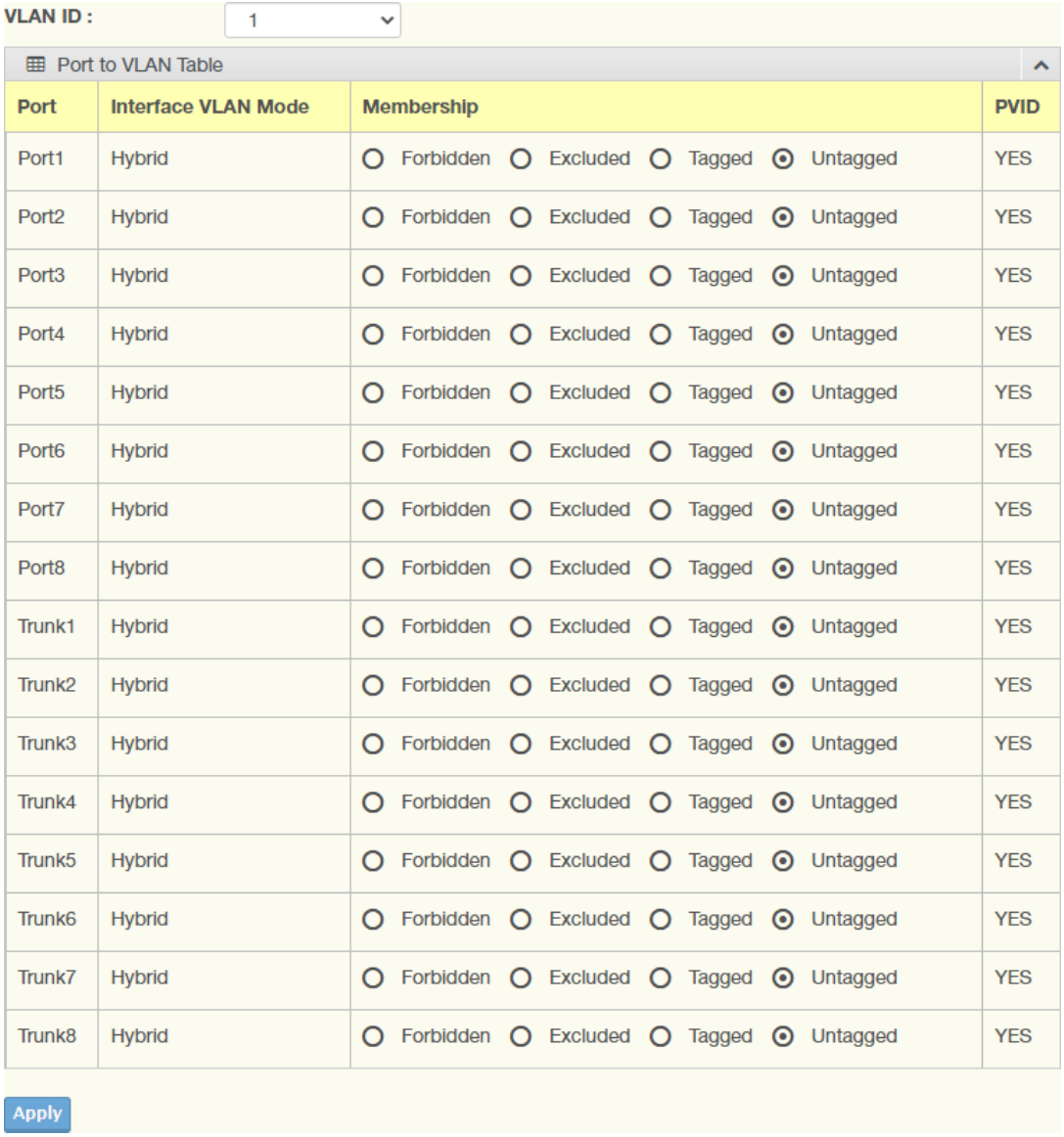


Figure 3.49 L2 Switching > 802.1Q VLAN > Port to VLAN

The following table describes the items in the previous figure.

Item	Description
Port	Displays the assigned port to the entry.
Interface VLAN Mode	Displays the assigned mode to the listed VLAN port. ■ Hybrid: Port hybrid model. ■ Access: Port hybrid model. ■ Trunk: Port hybrid model. ■ Tunnel: Port hybrid model.
Membership	Displays the assigned membership status of the port entry, options include: Forbidden, Excluded Tagged or Untagged.
Apply	Click **Apply** to save the values and update the screen.

3.7.4.4 Port-VLAN Mapping

To access this page, click **L2 Switching** > **802.1Q VLAN** > **Port-VLAN Mapping**.

The ensuing table for **Port-VLAN Mapping Table** settings are informational only: Port, Mode, Administrative VLANs and Operational VLANs.

3.7.5 GARP

The Generic Attribute Registration Protocol (GARP) is a local area network (LAN) protocol. The protocol defines procedures for the registration and de-registration of attributes (network identifiers or addresses) by end stations and switches with each other.

3.7.5.1 GARP Settings

To access this page, click **L2 Switching** > **GARP** > **GARP Settings**.

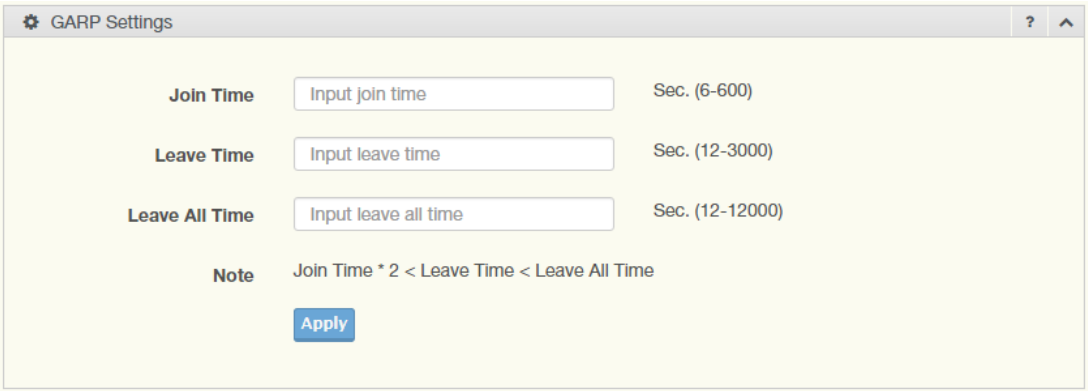


Figure 3.50 L2 Switching > GARP > GARP Settings

The following table describes the items in the previous figure.

Item	Description
Join Time	Enter a value to specify the time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group in centiseconds. Enter a number between 6 and 600. An instance of this timer exists for each GARP participant for each port.
Leave Time	Enter a value to specify the time to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry, in centiseconds. This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service. Enter a number between 12 and 3000. An instance of this timer exists for each GARP participant for each port.
Leave All Time	Enter a value to specify the Leave All Time controls how frequently Leave All PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. The timer is specified in centiseconds. Enter a number between 12 and 12000. An instance of this timer exists for each GARP participant for each port.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **GARP Information** settings are informational only: Join Time, Leave Time and Leave All Time.

3.7.5.2 GVRP Settings

The GVRP Settings page allows you to enable or disable the GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) protocol which facilitates control of virtual local area networks (VLANs) within a larger network.

To access this page, click **L2 Switching** > **GARP** > **GVRP Settings**.

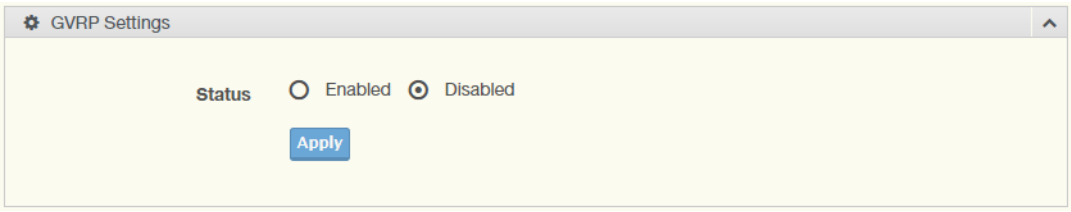


Figure 3.51 L2 Switching > GARP > GVRP Settings

The following table describes the items in the previous figure.

Item	Description
Status	Click to enable or disable the GARP VLAN Registration Protocol administrative mode for the switch. The factory default is Disable.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **GVRP Information** settings are informational only: GVRP.

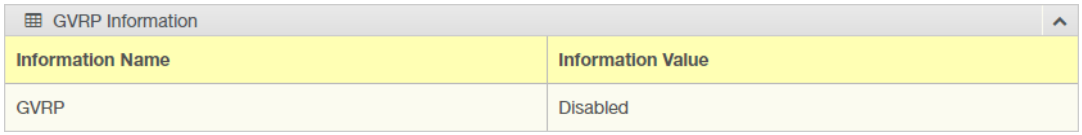


Figure 3.52 L2 Switching > GARP > GVRP Settings

3.7.6 802.3az EEE

The 802.3az Energy Efficient Ethernet (EEE) innovative green feature reduces energy consumption through intelligent functionality:

- Traffic detection — Energy Efficient Ethernet (EEE) compliance
- Inactive link detection

Inactive link detection function automatically reduces power usage when inactive links or devices are detected.

To access this page, click **L2 Switching** > **802.3az EEE**.

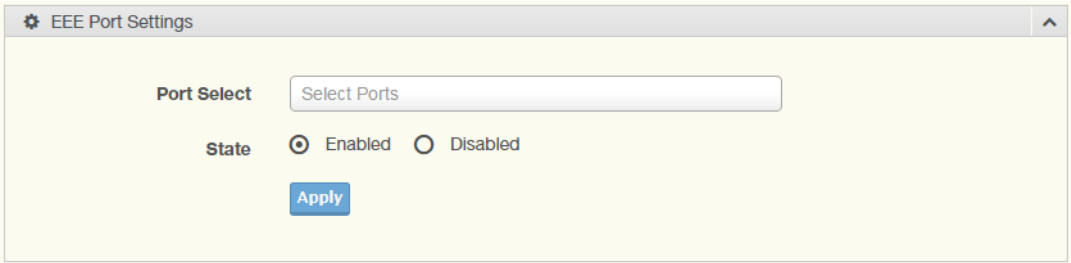


Figure 3.53 L2 Switching > 802.3az EEE

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the port to setup the EEE function.
State	Click **Enabled** or **Disabled** to set the state mode of the port select setting.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **EEE Enable Status** settings are informational only: Port and EEE State.

EEE Port Status

Port	EEE State
Port1	Disabled
Port2	Disabled
Port3	Disabled
Port4	Disabled
Port5	Disabled
Port6	Disabled
Port7	Disabled
Port8	Disabled

Figure 3.54 L2 Switching > 802.3az EEE

3.7.7 Multicast

Multicast forwarding allows a single packet to be forwarded to multiple destinations. The service is based on L2 switch receiving a single packet addressed to a specific Multicast address. Multicast forwarding creates copies of the packet, and transmits the packets to the relevant ports.

3.7.7.1 Multicast Filtering

The Multicast Filtering page allows for the definition of action settings when an unknown multicast request is received. The options include: Drop, Flood, or Router Port.

To access this page, click **L2 Switching** > **Multicast** > **Multicast Filtering**.

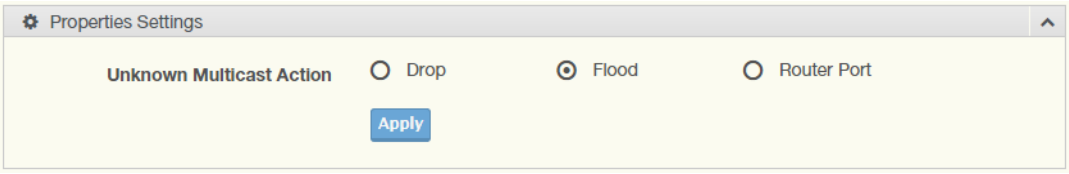


Figure 3.55 L2 Switching > Multicast > Multicast Filtering

The following table describes the items in the previous figure.

Item	Description
Unknown Multicast Action	Select the configuration protocol: Drop, Flood, or Router Port, to apply for any unknown multicast event.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Properties Information** settings are informational only: Unknown Multicast Action.

Properties Information

Information Name	Information Value
Unknown Multicast Action	Flood

Figure 3.56 L2 Switching > Multicast > Multicast Filtering

3.7.7.2 IGMP Snooping

IGMP Snooping is defined as the process of listening to Internet Group Management Protocol (IGMP) network traffic. IGMP Snooping allows a network switch to listen in

on the IGMP conversation between hosts and routers and maintain a map of which links need which IP multicast streams. Multicasts can be filtered from the links which do not need them in turn controlling which ports receive specific multicast traffic.

IGMP Settings

To access this page, click **L2 Switching** > **Multicast** > **IGMP Snooping** > **IGMP Settings**.

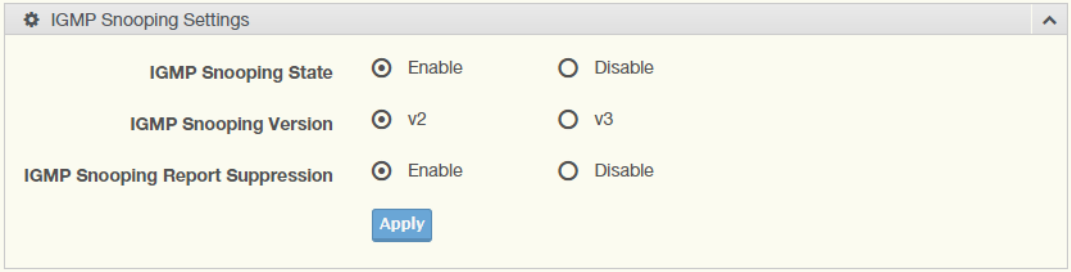


Figure 3.57 L2 Switching > Multicast > IGMP Snooping > IGMP Settings

The following table describes the items in the previous figure.

Item	Description
IGMP Snooping State	Select **Enable** or **Disable** to designate the IGMP Snooping State.
IGMP Snooping Version	Select designate the IGMP Snooping Version: V2 or V3.
IGMP Snooping Report Suppression	Select **Enable** or **Disable** to setup the report suppression for IGMP Snooping.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **IGMP Snooping Information** settings are informational only: IGMP Snooping State, IGMP Snooping Version and IGMP Snooping V2 Report Suppression.

Figure 3.58 L2 Switching > Multicast > IGMP Snooping > IGMP Settings

The ensuing table for **IGMP Snooping Table** settings are informational only: Entry No., VLAN ID, IGMP Snooping Operation State, Router Ports Auto Learn, Query Robustness, Query Interval (sec.), Query Max Response Interval (sec.), Last Member Query count, Last Member Query Interval (sec), Immediate Leave and **Edit** (click to modify the settings).

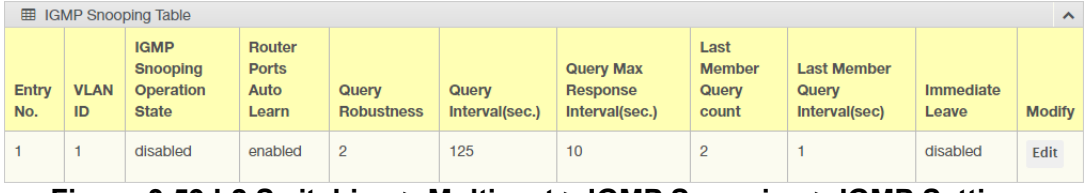


Figure 3.59 L2 Switching > Multicast > IGMP Snooping > IGMP Settings

IGMP Querier

IGMP Querier allows snooping to function by creating the tables for snooping. General queries must be unconditionally forwarded by all switches involved in IGMP snooping.

To access this page, click **L2 Switching** > **Multicast** > **IGMP Snooping** > **IGMP Querier**.

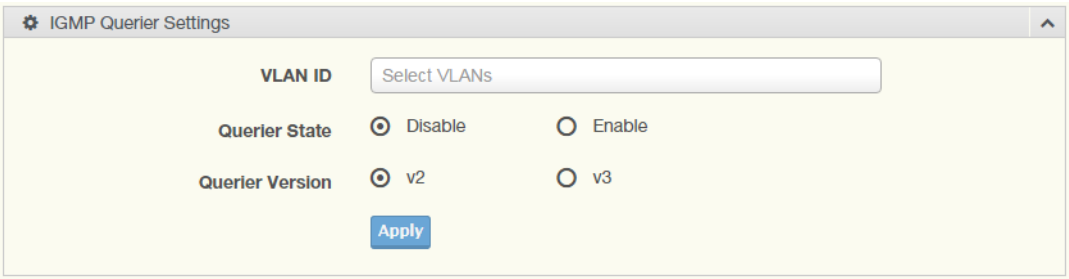


Figure 3.60 L2 Switching > Multicast > IGMP Snooping > IGMP Querier

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Select the VLAN ID to define the local IGMP querier.
Querier State	Select **Disable** or **Enable** to configure the VLAN ID (IGMP Querier).
Querier Version	Select the querier version (V2 or V3) designated to the selected VLAN ID.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **IGMP Querier Status** settings are informational only: VLAN ID, Querier State, Querier Status, Querier Version and Querier IP.

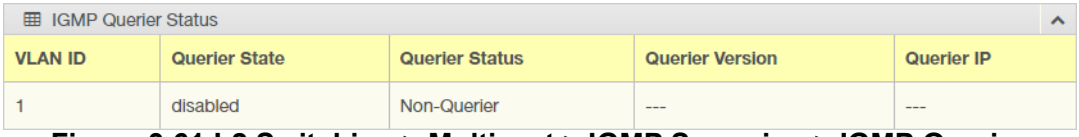


Figure 3.61 L2 Switching > Multicast > IGMP Snooping > IGMP Querier

3.7.7.3 IGMP Static Groups

To access this page, click **L2 Switching** > **Multicast** > **IGMP Snooping** > **IGMP Static** Groups.

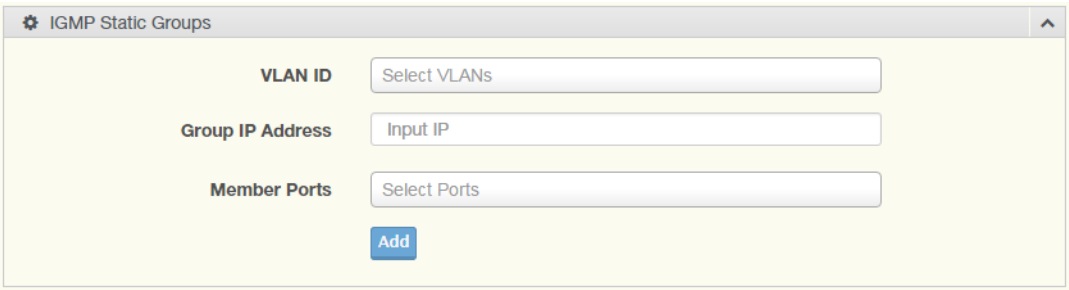


Figure 3.62 L2 Switching > Multicast > IGMP Snooping > IGMP Static Groups

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Select the VLAN ID to define IGMP static group.
Group IP Address	Enter the IP address assigned to the VLAN ID.
Member Ports	Enter the port numbers to associate with the static group.
Add	Click **Add** to add an IGMP group.

The ensuing table for **IGMP Static Groups Status** settings are informational only: VLAN ID, Group IP Address, Member Ports and Modify.

Figure 3.63 L2 Switching > Multicast > IGMP Snooping > IGMP Static Groups

Multicast Groups

To access this page, click **L2 Switching** > **Multicast** > **IGMP Snooping** > **Multicast Groups**.

The ensuing table for **Multicast Groups** settings are informational only: VLAN ID, Group IP Address, Member Ports, Type and Life (Sec).

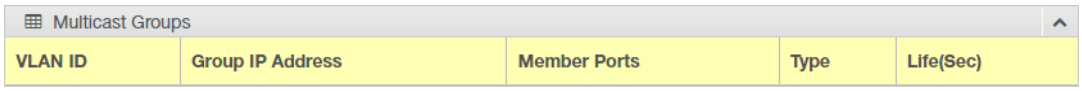


Figure 3.64 L2 Switching > Multicast > IGMP Snooping > Multicast Groups

Router Ports

To access this page, click **L2 Switching** > **Multicast** > **IGMP Snooping** > **Router Ports**.

The ensuing table for **Router Ports** settings are informational only: VLAN ID, Port and Expiry Time (Sec).

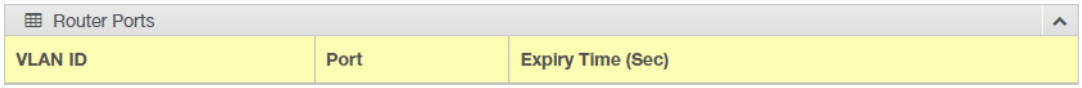


Figure 3.65 L2 Switching > Multicast > IGMP Snooping > Router Ports

3.7.7.4 MLD Snooping

The MLD Snooping page allows you to select the snooping status (enable or disable), the version (v1 or v2) and the enabling/disabling of the report suppression for the MLD querier, which sends out periodic general MLD queries and are forwarded through all ports in the VLAN.

MLD Settings

To access this page, click **L2 Switching** > **Multicast** > **MLD Snooping** > **MLD Settings**.

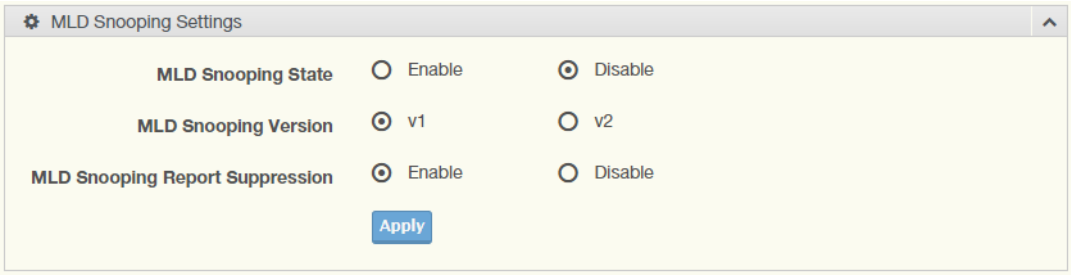


Figure 3.66 L2 Switching > Multicast > MLD Snooping > MLD Settings

The following table describes the items in the previous figure.

Item	Description
MLD Snooping State	Select **Enable** or **Disable** to setup the MLD Snooping State.
MLD Snooping Version	Select the querier version (V1 or V2) designated to the MLD Snooping Version.
MLD Snooping Report Suppression	Select **Enable** or **Disable** to designate the status of the report suppression.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **MLD Snooping Information** settings are informational only: MLD Snooping State, MLD Snooping Version and MLD Snooping V2 Report Suppression.

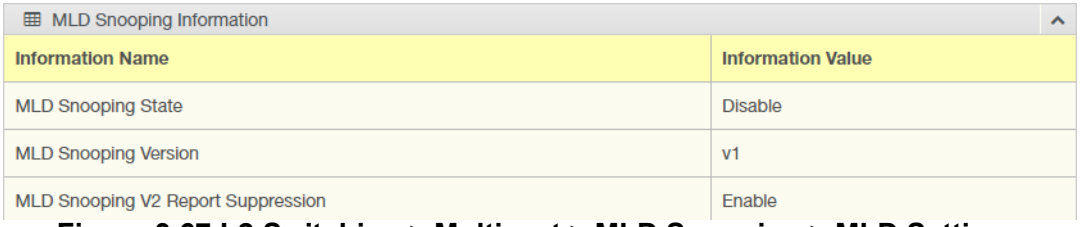


Figure 3.67 L2 Switching > Multicast > MLD Snooping > MLD Settings

The ensuing table for **MLD Snooping Table** settings are informational only: Entry No., VLAN ID, MLD Snooping Operation State, Router Ports Auto Learn, Query Robustness, Query Interval (sec.), Query Max Response Interval (sec.), Last Member Query count, Last Member Query Interval (sec), Immediate Leave and **Edit** (click to modify the settings).

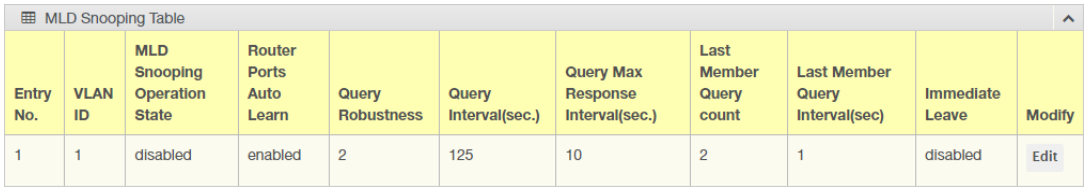


Figure 3.68 L2 Switching > Multicast > MLD Snooping > MLD Settings

MLD Querier

The MLD Querier page allows you to select and enable/disable the MLD querier and define the version (IGMPv1 or IGMPv2) when enabled.

To access this page, click **L2 Switching** > **Multicast** > **MLD Snooping** > **MLD Querier**.

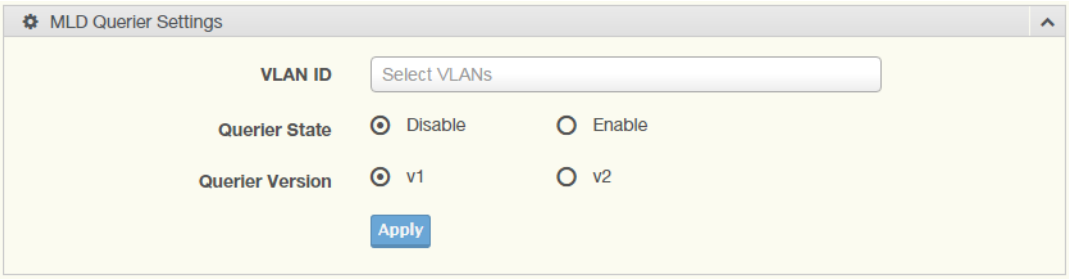


Figure 3.69 L2 Switching > Multicast > MLD Snooping > MLD Querier

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Enter the VLAN ID to configure.
Querier State	Select **Enable** or **Disable** status on the selected VLAN. ■ Enable: Enable IGMP Querier Election. ■ Disable: Disable IGMP Querier Election.
Querier Version	Select the querier version (IGMPV1 or IGMPV2) designated to the MLD Querier function.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **MLD Querier Status** settings are informational only: VLAN ID, Querier State, Querier Status, Querier Version and Querier IP.

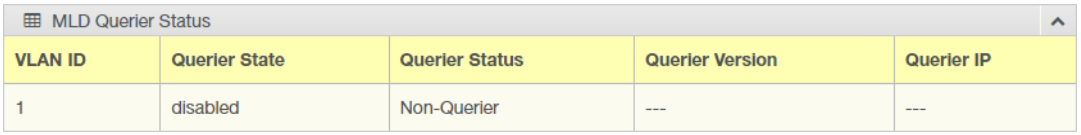


Figure 3.70 L2 Switching > Multicast > MLD Snooping > MLD Querier

MLD Static Group

The MLD Static Group page allows you to configure specified ports as static member ports.

To access this page, click **L2 Switching** > **Multicast** > **MLD Snooping** > **MLD Static Group**.

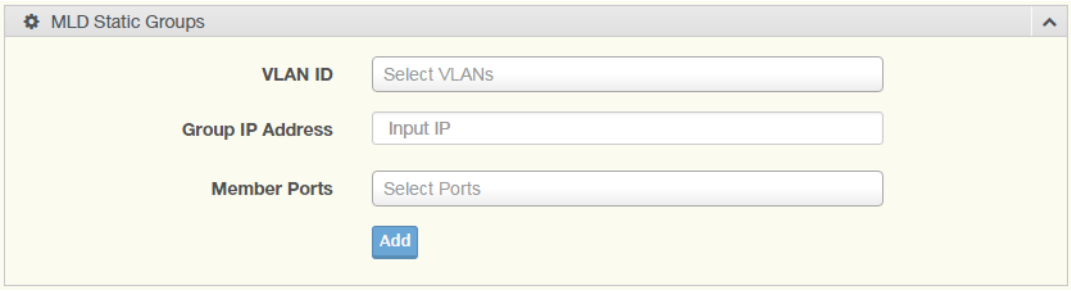


Figure 3.71 L2 Switching > Multicast > MLD Snooping > MLD Static Group

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Enter the VLAN ID to define the local MLD Static Group.
Group IP Address	Enter the IP address associated with the static group. Format: prefix/ prefix_length.
Member Ports	Enter the ports designated with the static group.
Add	Click **Add** to add a MLD static group.

The ensuing table for **MLD Static Groups Status** settings are informational only: VLAN ID, Group IP Address, Member Ports and Modify.

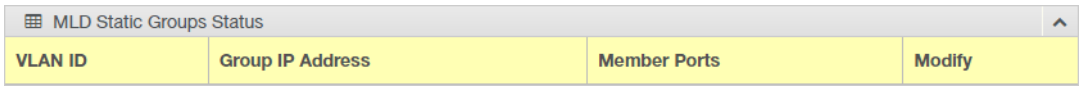


Figure 3.72 L2 Switching > Multicast > MLD Snooping > MLD Static Group

Multicast Groups

To access this page, click **L2 Switching** > **Multicast** > **MLD Snooping** > **Multicast Groups**.

The ensuing table for **Multicast Groups** settings are informational only: ID, Group IP Address, Member Ports, Type and Life (Sec).

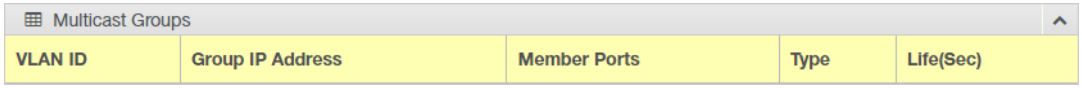


Figure 3.73 L2 Switching > Multicast > MLD Snooping > Multicast Groups

Router Ports

To access this page, click **L2 Switching** > **Multicast** > **MLD Snooping** > **Router Ports**.

The ensuing table for **Router Ports** settings are informational only: VLAN ID, Port and Expiry Time (Sec).

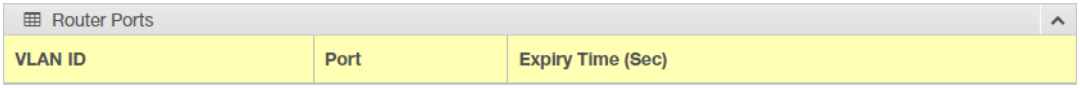


Figure 3.74 L2 Switching > Multicast > MLD Snooping > Router Ports

3.7.8 Jumbo Frame

Jumbo frames are frames larger than the standard Ethernet frame size of 1518 bytes. The Jumbo Frame function allows the configuration of Ethernet frame size.

To access this page, click **L2 Switching** > **Jumbo Frame**.

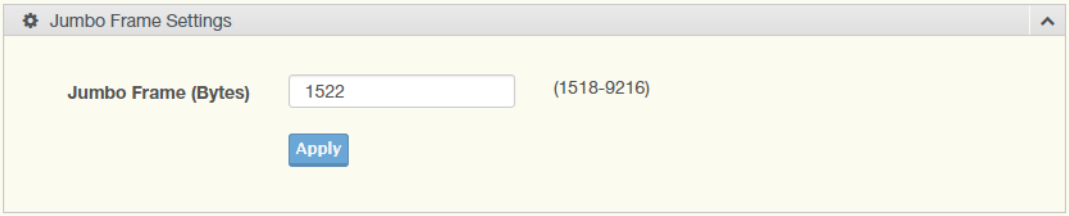


Figure 3.75 L2 Switching > Jumbo Frame

The following table describes the items in the previous figure.

Item	Description
Jumbo Frame (Bytes)	Enter the variable in bytes (1518 to 9216) to define the jumbo frame size.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Jumbo Frame Config** settings are informational only: Jumbo Frame (Bytes).

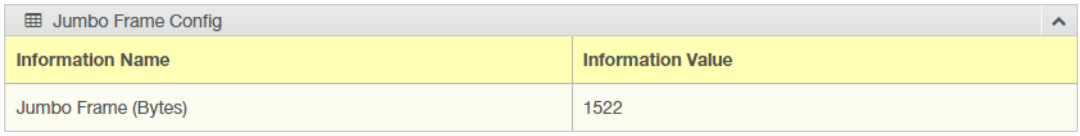


Figure 3.76 L2 Switching > Jumbo Frame

3.7.9 Spanning Tree

The Spanning Tree Protocol (STP) is a network protocol to ensure loop-free topology for any bridged Ethernet local area network.

3.7.9.1 STP Global Settings

The STP Global Settings page allows you to set the STP status, select the configuration for a BPDU packet, choose the path overhead, force version and set the configuration revision range.

To access this page, click **L2 Switching** > **Spanning Tree** > **STP Global Settings**.

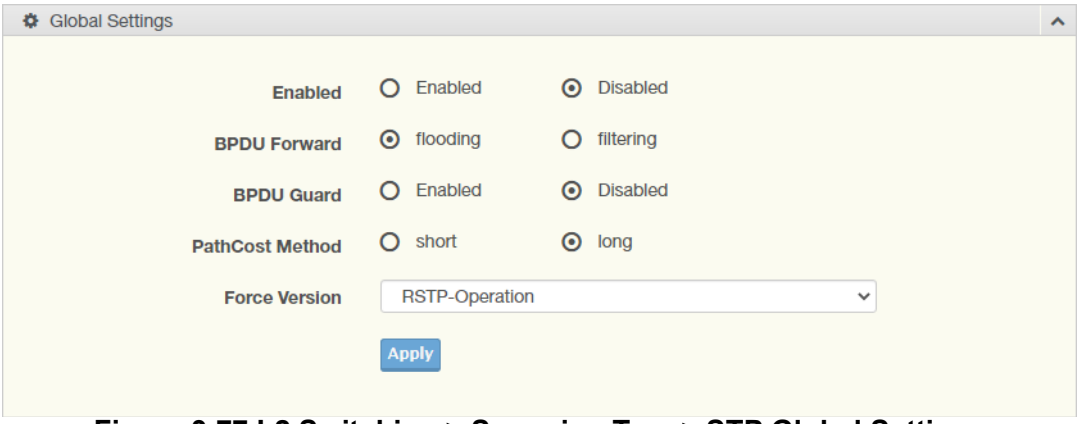


Figure 3.77 L2 Switching > Spanning Tree > STP Global Settings

The following table describes the items in the previous figure.

Item	Description
Enabled	Click the radio-button to enable or disable the STP status.
BPDU Forward	Select **flooding** or **filtering** to designate the type of BPDU packet.
BPDU Guard	Click to enable of disable (default) the function. The feature protects the spanning tree by monitoring the port for BPDUs. If an unautho-rized entry is detected, the port is shut down.
PathCost Method	Select short or long to define the method of used for path cost calcula-tions.
Force Version	Click the drop-down menu to select the operating mode for STP. ■ STP-Compatible: 802.1D STP operation. ■ RSTP-Operation: 802.1w operation.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **STP Information** settings are informational only: STP, BPDU Forward, PathCost Method and Force Version.

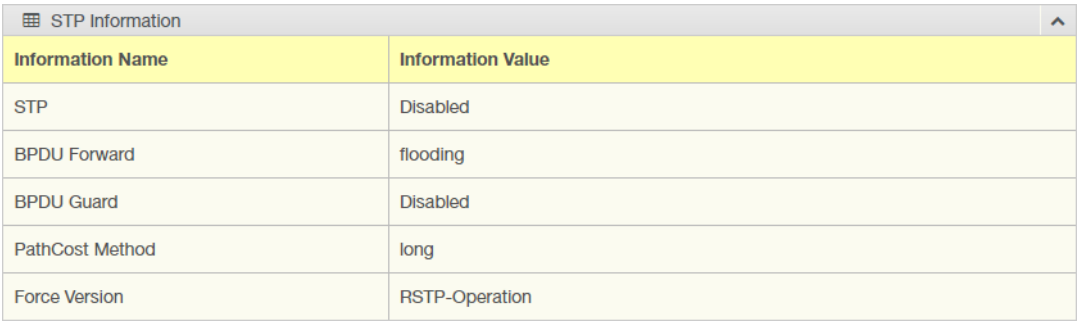


Figure 3.78 L2 Switching > Spanning Tree > STP Global Settings

3.7.9.2 STP Port Settings

The STP Port Settings page allows you to configure the ports for the setting, port's contribution, configure edge port, and set the status of the BPDU filter.

To access this page, click **L2 Switching** > **Spanning Tree** > **STP Port Settings**.

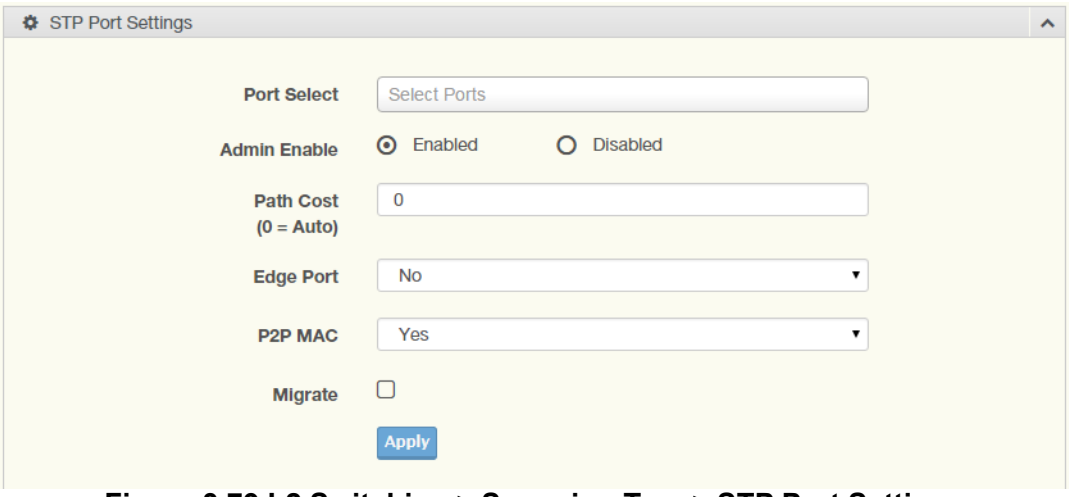
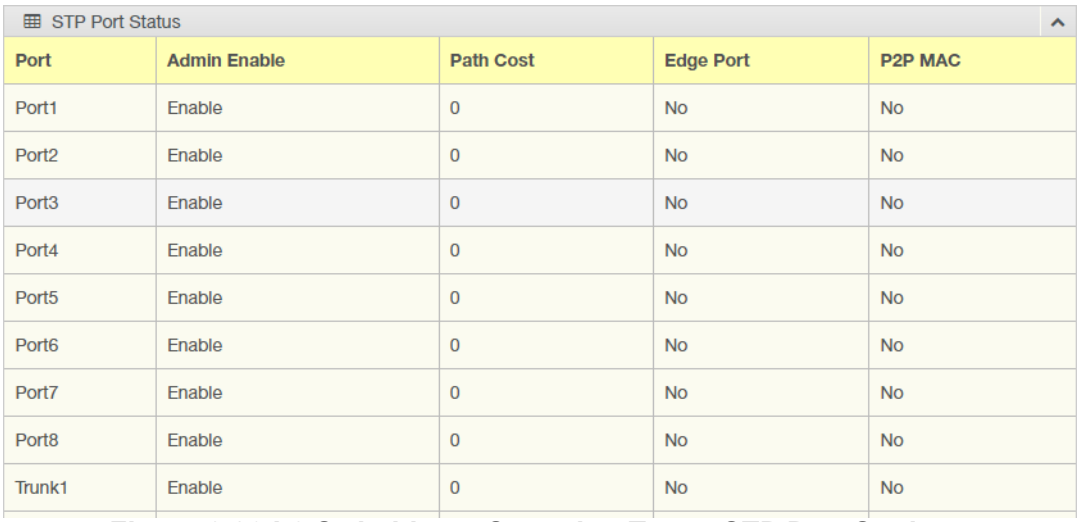


Figure 3.79 L2 Switching > Spanning Tree > STP Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Select the port list to specify the ports that apply to this setting.
Admin Enable	Select **Enabled** or **Disabled** to setup the admin profile for the STP port.
Path Cost (0 = Auto)	Set the port's cost contribution. For a root port, the root path cost for the bridge. (0 means Auto).
Edge Port	Click the drop-down menu to set the edge port configuration. ■ No: Force to false state (as link to a bridge). ■ Yes: Force to true state (as link to a host).
P2P MAC	Click the drop-down menu to set the Point-to-Point port configuration. ■ No: Force to false state. ■ Yes: Force to true state.
Migrate	Click the check box to enable the migrate function. Forces the port to use the new MST/RST BPDUs, requiring the switch to test on the LAN segment. for the presence of legacy devices, which are not able to understand the new BPDU formats.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **STP Port Status** settings are informational only: Port, Admin Enable, Path Cost, Edge Port and P2P MAC.


STP Port Status

Port	Admin Enable	Path Cost	Edge Port	P2P MAC
Port1	Enable	0	No	No
Port2	Enable	0	No	No
Port3	Enable	0	No	No
Port4	Enable	0	No	No
Port5	Enable	0	No	No
Port6	Enable	0	No	No
Port7	Enable	0	No	No
Port8	Enable	0	No	No
Trunk1	Enable	0	No	No

Figure 3.80 L2 Switching > Spanning Tree > STP Port Settings

3.7.9.3 STP Bridge Settings

The STP Bridge Settings page allows you to configure the priority, forward delay, maximum age, Tx hold count, and the hello time for the bridge.

To access this page, click **L2 Switching** > **Spanning Tree** > **STP Bridge Settings**.

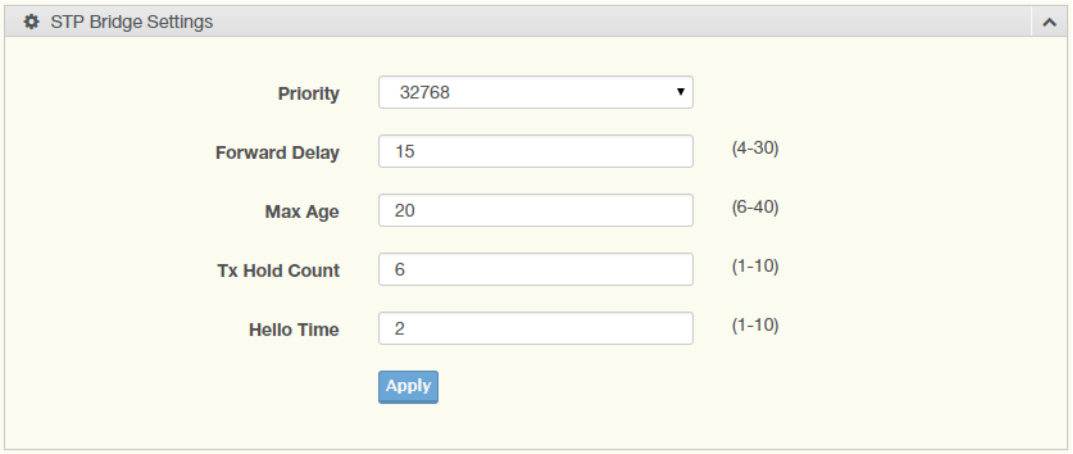


Figure 3.81 L2 Switching > Spanning Tree > STP Bridge Settings

The following table describes the items in the previous figure.

Item	Description
Priority	Click the drop-down menu to select the STP bridge priority.
Forward Delay	Enter the variable (4 to 30) to set the forward delay for STP bridge settings.
Max Age	Enter the variable (6 to 40) to set the Max age for STP bridge settings.
Tx Hold Count	Enter the variable (1 to 10) to designate the TX hold count for STP bridge settings.
Hello Time	Enter the variable (1 to 10) to designate the Hello Time for STP bridge settings.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **STP Bridge Information** settings are informational only: Priority, Forward Delay, Max Age, Tx Hold Count and Hello Time.

STP Bridge Information

Information Name	Information Value
Priority	32768
Forward Delay	15
Max Age	20
Tx Hold Count	6
Hello Time	2

Figure 3.82 L2 Switching > Spanning Tree > STP Bridge Settings

The ensuing table for **STP Bridge Status** settings are informational only: Bridge Identifier, Designated Root Bridge, Root Path Cost, Designated Bridge, Root Port and Last Topology Change.

STP Bridge Status

Information Name	Information Value
Bridge Identifier	32768/ 0/00:D0:C9:F5:0F:71
Designated Root Bridge	0/ 0/00:00:00:00:00:00
Root Path Cost	0
Designated Bridge	0/ 0/00:00:00:00:00:00
Root Port	0 / 0
Last Topology Change	0

Figure 3.83 L2 Switching > Spanning Tree > STP Bridge Settings

3.7.9.4 STP Port Advanced Settings

The STP Port Advanced Settings page allows you to select the port list to apply this setting.

To access this page, click **L2 Switching** > **Spanning Tree** > **STP Port Advanced Settings**.

Figure 3.84 L2 Switching > Spanning Tree > STP Port Advanced Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Select the port to designate the STP settings.
Priority	Click the drop-down menu to designate a priority.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **STP Port Status** settings are informational only: Port, Identifier (Priority / Port Id), Path Cost Conf/Oper, Designated Root Bridge, Root Path Cost, Designated Bridge, Edge Port Conf/Oper, P2P MAC Conf/Oper, Port Role and Port State.

STP Port Status

Port	Identifier (Priority / Port Id)	Path Cost Conf/Oper	Designated Root Bridge	Root Path Cost	Designated Bridge	Edge Port Conf/Oper	P2P MAC Conf/Oper	Port Role	Port State
Port1	128 / 1	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled
Port2	128 / 2	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled
Port3	128 / 3	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled
Port4	128 / 4	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled
Port5	128 / 5	0 / 20000	0 / 00:00:00:00:00:00	0	0 /	No / No	No / No	Disabled	Forwarding

Figure 3.85 L2 Switching > Spanning Tree > STP Port Advanced Settings

3.7.9.5 STP Statistics

To access this page, click **L2 Switching** > **Spanning Tree** > **STP Statistics**.

The ensuing table for **STP Statistics** settings are informational only: Port, Configuration BPDUs Received, TCN BPDUs Received, Configuration BPDUs Transmitted and TCN BPDUs Transmitted.

STP Statistics

Port	Configuration BPDUs Received	TCN BPDUs Received	Configuration BPDUs Transmitted	TCN BPDUs Transmitted
Port1	0	0	0	0
Port2	0	0	0	0
Port3	0	0	0	0
Port4	0	0	0	0
Port5	0	0	0	0
Port6	0	0	0	0
Port7	0	0	0	0

Figure 3.86 L2 Switching > Spanning Tree > STP Statistics

3.7.10 X-Ring Elite

The X-Ring Elite function provides an improvement over Spanning Tree and Rapid Spanning Tree and a rapid auto recovery in the event that the network suffers a corrupt or broken link and prevents network loops.

3.7.10.1 X-Ring Elite Settings

The X-Ring Elite Settings allows you to enable or disable the state of the X-Ring settings.

To access this page, click **L2 Switching** > **X-Ring Elite** > **X-Ring Elite Settings**.

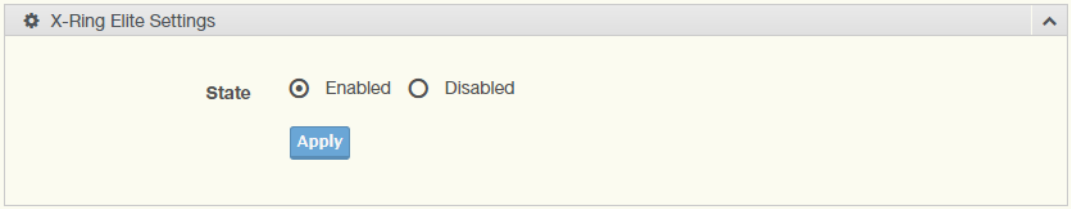


Figure 3.87 L2 Switching > X-Ring Elite > X-Ring Elite Settings

The following table describes the items in the previous figure.

Item	Description
State	Select **Enabled** or **Disabled** to setup the X-Ring Elite mode.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Information** settings are informational only: X-Ring Elite State.

Information

Information Name	Information Value
X-Ring Elite State	Enabled

Figure 3.88 L2 Switching > X-Ring Elite > X-Ring Elite Settings

3.7.10.2 X-Ring Elite Groups

The X-Ring Elite Groups page allows you to select the function and role for each device and the connected ports.

To access this page, click **L2 Switching** > **X-Ring Elite** > **X-Ring Elite Groups**.

Figure 3.89 L2 Switching > X-Ring Elite > X-Ring Elite Groups

The following table describes the items in the previous figure.

Item	Description
Ring ID	Enter a number to specifies a ranging from 1 to 255 to identify a given X-Ring Elite group.
Role	Click the drop-down menu to select the ring role.
Port 1	Click the drop-down menu to define the port designation.
Port 2	Click the drop-down menu to define the port designation.
Add	Click **Add** to save the values and update the screen.

The ensuing table for **Information** settings are informational only: Ring ID, Role, Port 1, Port 2 and **Delete** (click to delete the desired Ring ID).

Figure 3.90 L2 Switching > X-Ring Elite > X-Ring Elite Groups

3.7.11 Loopback Detection

The Loopback Detection function is used to detect looped links. By sending detection frames and then checking to see if the frames returned to any port on the device, the function is used to detect loops.

3.7.11.1 Global Settings

The Global Settings page allows you to configure the state (enabled or disabled) of the function, select the interval at which frames are transmitted and the delay before recovery.

To access this page, click **L2 Switching** > **Loopback Detection** > **Global Settings**.

Figure 3.91 L2 Switching > Loopback Detection > Global Settings

The following table describes the items in the previous figure.

Item	Description
State	Select **Enabled** or **Disabled** to setup the loopback mode.

Item	Description
Interval	Enter the variable in seconds (1 to 32767) to set the interval at which frames are transmitted.
Recover Time	Enter the variable in seconds (60 to 1000000) to define the delay before recovery.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Loopback Detection Global Information** settings are informational only: State, Interval and Recover Time.

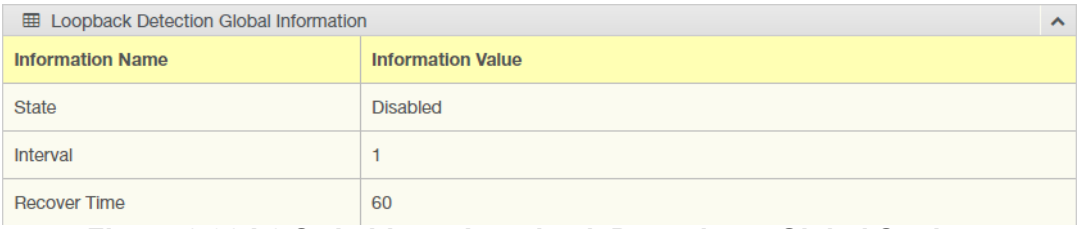


Figure 3.92 L2 Switching > Loopback Detection > Global Settings

3.7.11.2 Port Settings

The Port Settings page allows you to select ports that are detected by the loopback detection function and configure their status (enabled or disabled).

To access this page, click **L2 Switching** > **Loopback Detection** > **Port Settings**.

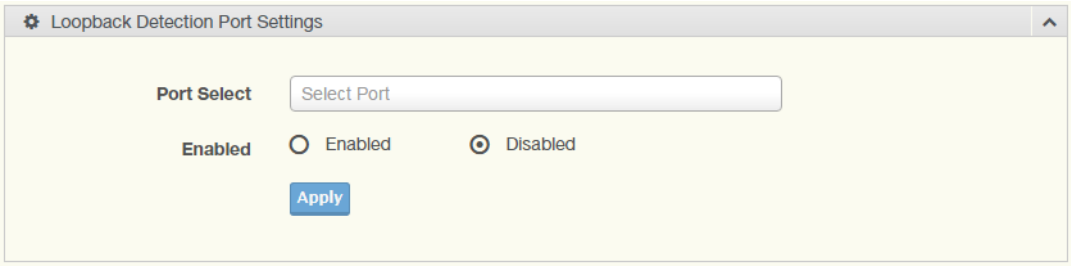


Figure 3.93 L2 Switching > Loopback Detection > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the port to define the local loopback detection setting.
Enabled	Select **Enabled** or **Disabled** to setup the Loopback Detection function.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Loopback Detection Port Information** settings are informational only: Port, Enable State and Loop Status.

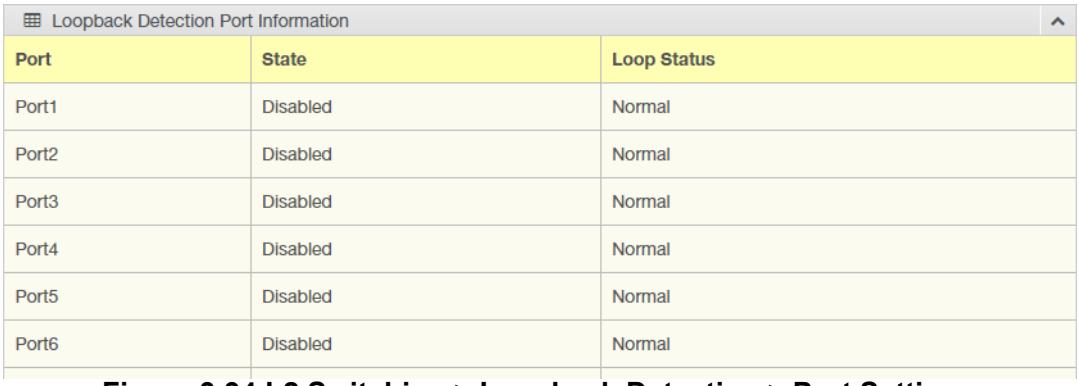


Figure 3.94 L2 Switching > Loopback Detection > Port Settings

3.8 MAC Address Table

The MAC Address Table provides access to the Static MAC Settings, MAC Aging Time, and Dynamic Forwarding.

3.8.1 Static MAC

The Static MAC page allows you to configure the address for forwarding of packets, the VLAN ID of the listed MAC address and the designated Port.

To access this page, click **MAC Address Table** > **Static MAC**.

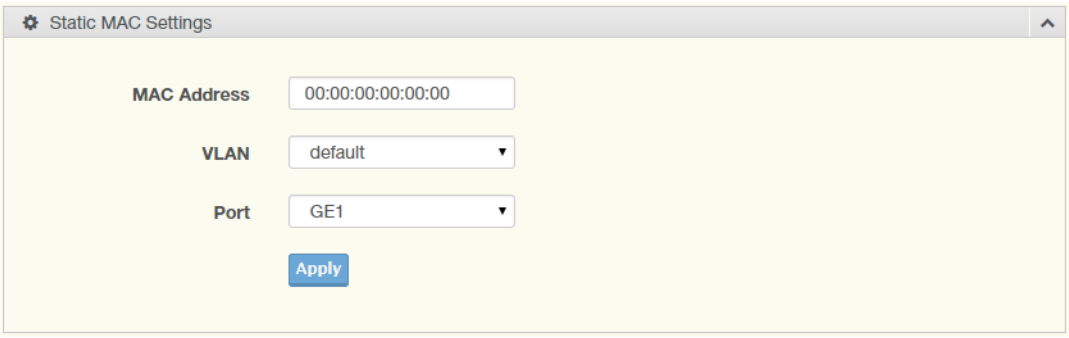


Figure 3.95 MAC Address Table > Static MAC

The following table describes the items in the previous figure.

Item	Description
MAC Address	Enter the MAC address to which packets are statically forwarded.
VLAN	Click the drop-down menu to select the VLAN ID number of the VLAN for which the MAC address is residing.
Port	Click the drop-down menu to select the port number.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Static MAC Status** settings are informational only: No., MAC Address, VLAN, Port and **Delete** (click to delete the desired MAC address).

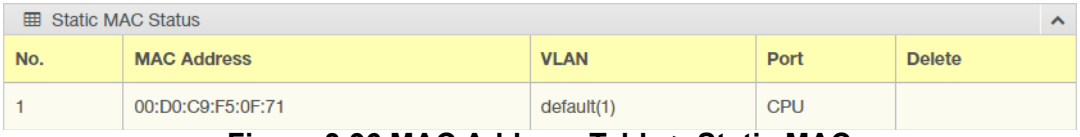


Figure 3.96 MAC Address Table > Static MAC

3.8.2 MAC Aging Time

The MAC Aging Time page allows you to set the MAC address of the aging time to study.

To access this page, click **MAC Address Table** > **MAC Aging Time**.

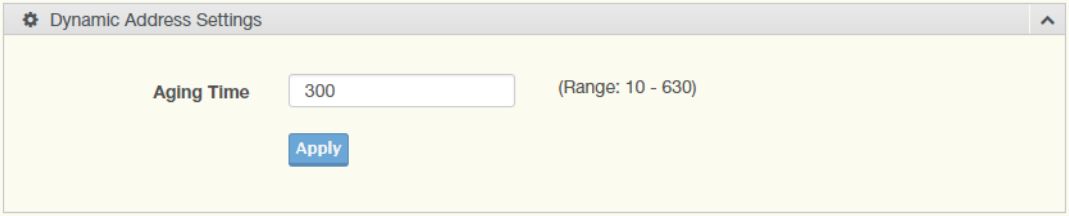


Figure 3.97 MAC Address Table > MAC Aging Time

The following table describes the items in the previous figure.

Item	Description
Aging Time	Enter the variable (10 to 630) to define the time required for aging.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Dynamic Address Status** settings are informational only: Aging time.

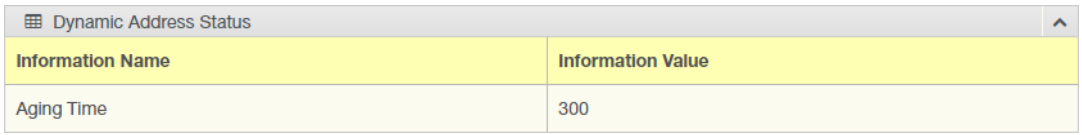


Figure 3.98 MAC Address Table > MAC Aging Time

3.8.3 Dynamic Forwarding Table

The Dynamic Forwarding function allows you to configure an address tables, which contain the following:

- The port each hardware address is associated with
- The VLAN to show or clear dynamic MAC entries
- The MAC address selection

To access this page, click **MAC Address Table** > **Dynamic Forwarding Table**.

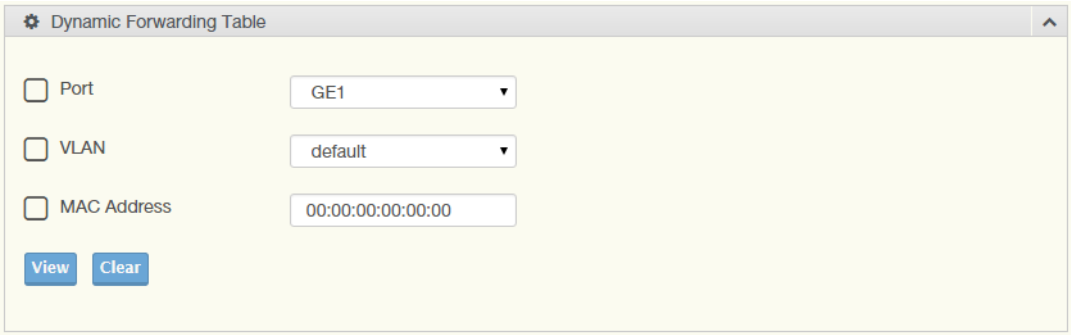


Figure 3.99 MAC Address Table > Dynamic Forwarding Table

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select the port number to show or clear dynamic MAC entries. If a port, VLAN or MAC address is not selected the whole dynamic MAC table is displayed or cleared.
VLAN	Click the drop-down menu to select the VLAN to show or clear dynamic MAC entries.
MAC Address	Enter the MAC address to show or clear dynamic MAC entries. If a port, VLAN or MAC address is not selected the whole dynamic MAC table is displayed or cleared.
View	Click **View** to display the MAC address information.
Clear	Click **Clear** to clear the MAC Address Information table.

The ensuing table for **MAC Address Information** settings are informational only: MAC Address, VLAN, Type, Port and **Add to Static MAC** (click to add the MAC address to static MAC address list).

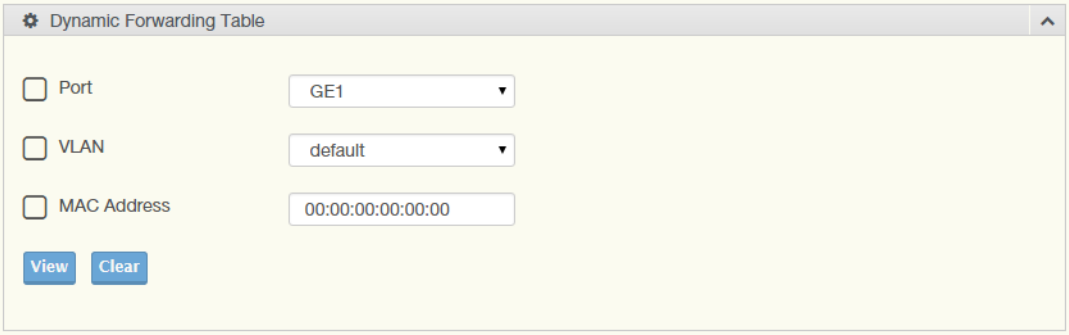


Figure 3.100 MAC Address Table > Dynamic Forwarding Table

3.9 Security

The Security function allows for the configuration of Storm Control, Port Security, Protected Ports, DoS Prevention, Applications, and 802.1x.

3.9.1 Storm Control

The Storm Control page allows you to setup the units and Preamble/IFG to manage the occurrence of packet flooding on the LAN and consequent traffic to prevent the degrading of network performance.

3.9.1.1 Global Settings

To access this page, click **Security** > **Storm Control** > **Global Settings**.

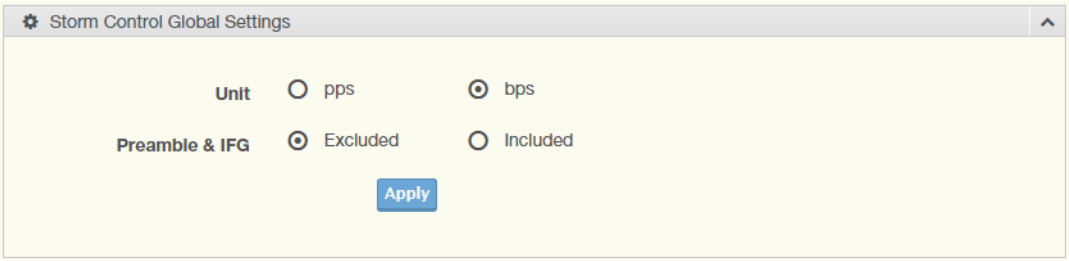


Figure 3.101 Security > Storm Control > Global Settings

The following table describes the items in the previous figure.

Item	Description
Unit	Select **pps** or **bps** control units for the Storm Control function.
Preamble & IFG	Select **Excluded** or **Included** to setup the Storm Control Global settings. ■ Excluded: exclude preamble & IFG (20 bytes) when count ingress storm control rate. ■ Included: include preamble & IFG (20 bytes) when count ingress storm control rate.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Storm Control Global Information** settings are informational only: Unit and Preamble & IFG.

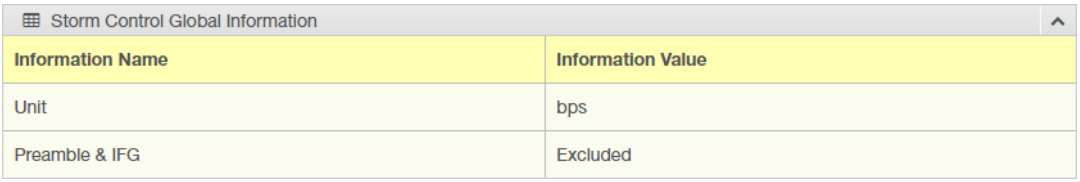


Figure 3.102 Security > Storm Control > Global Settings

3.9.1.2 Port Settings

The Port Settings page allows you to configure the port and the type of storm control association along with the value of the storm rate for the selected port.

To access this page, click **Security** > **Storm Control** > **Port Settings**.

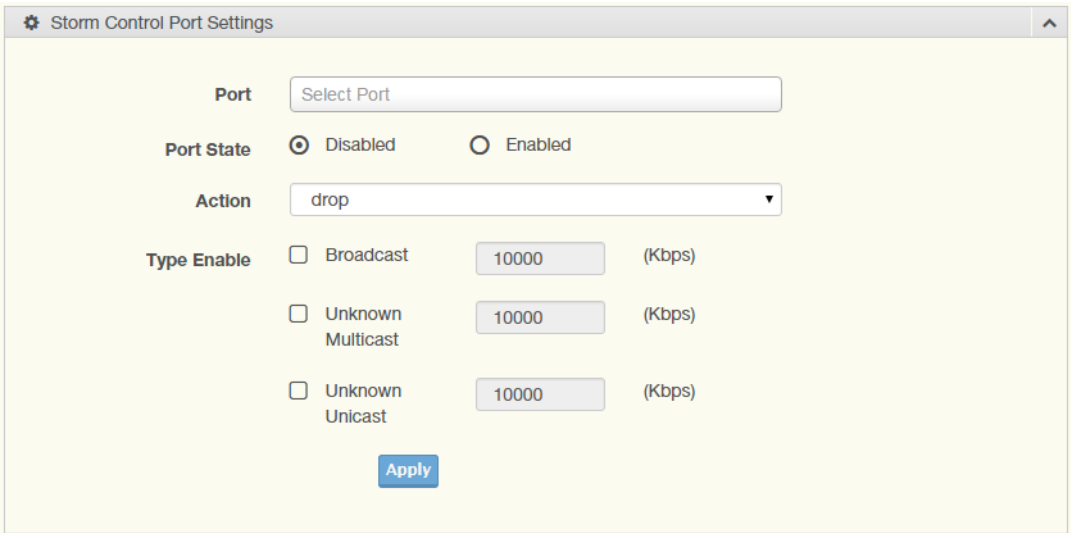
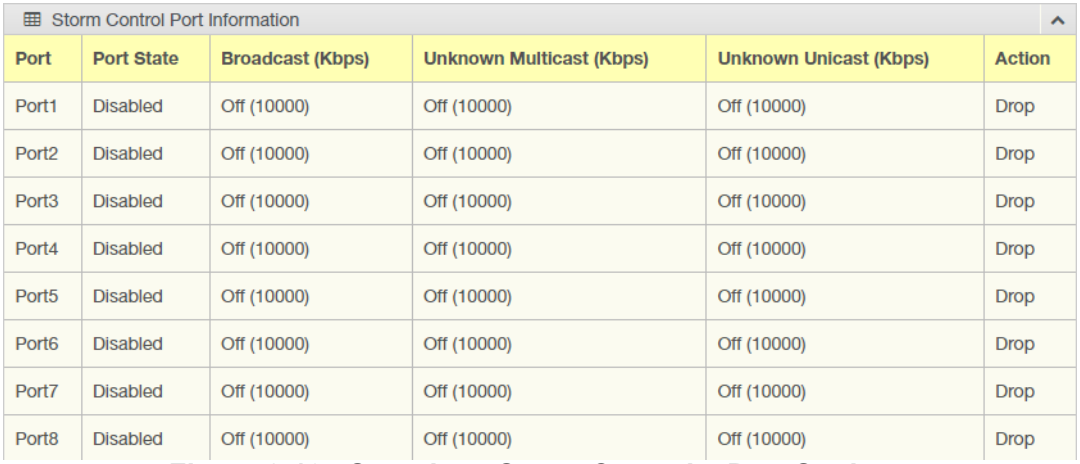


Figure 3.103 Security > Storm Control > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number to designate the local port for the Storm Control function.
Port State	Select **Disabled** or **Enabled** to define the port state
Action	Click the drop-down menu to select the type of action to designate for the selected port during a Storm Control incident. The options are Drop and Shutdown.
Type Enable	Click the radio button to enable Broadcast, Unknown Multicast, or Unknown Unicast. ■ Broadcast: Select the variable in Kbps to define the broadcast bandwidth. ■ Unknown Multicast: Select the variable in Kbps to define the multicast setting. ■ Broadcast: Select the variable in Kbps to define the unknown unicast setting.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Storm Control Port Information** settings are informational only: Port, Port State, Broadcast (Kbps), Unknown Multicast (Kbps), Unknown Unicast (Kbps) and Action.



Storm Control Port Information

Port	Port State	Broadcast (Kbps)	Unknown Multicast (Kbps)	Unknown Unicast (Kbps)	Action
Port1	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
Port2	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
Port3	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
Port4	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
Port5	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
Port6	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
Port7	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
Port8	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop

Figure 3.104 Security > Storm Control > Port Settings

3.9.2 Port Security

The Port Security page allows you to configure port isolation behavior.

To access this page, click **Security** > **Port Security**.

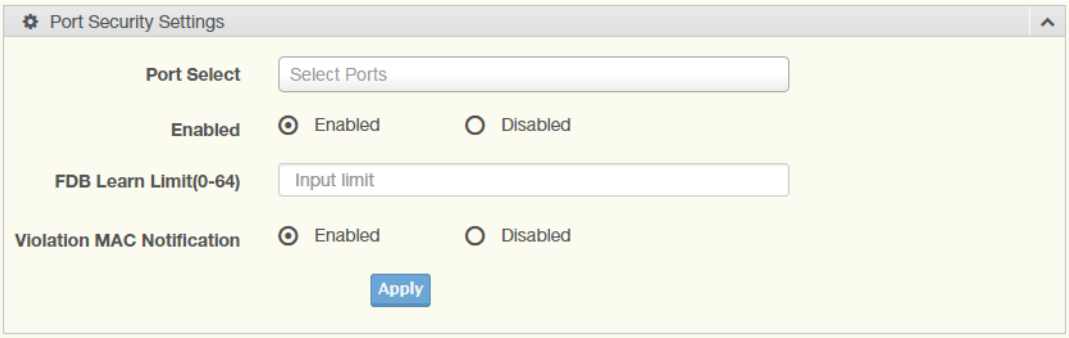


Figure 3.105 Security > Port Security

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter a single or multiple port numbers to configure.
Enabled	Select **Enabled** or **Disabled** to define the selected Port.
FDB Learn Limit (0-64)	Enter the variable (0 to 64) to set the learn limit for the FDB setting.
Violation MAC Notification	Select **Enabled** or **Disabled** to define the selected Port.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Port Security Information** settings are informational only: Port, Enabled, FDB Learn Limit and Violation MAC Notification.

Port Security Information

Port	Enabled	FDB Learn Limit	Violation MAC Notification
Port1	Disabled	0	Disabled
Port2	Disabled	0	Disabled
Port3	Disabled	0	Disabled
Port4	Disabled	0	Disabled
Port5	Disabled	0	Disabled
Port6	Disabled	0	Disabled
Port7	Disabled	0	Disabled
Port8	Disabled	0	Disabled

Figure 3.106 Security > Port Security

3.9.3 Protected Ports

The Protected Port page allows you to configure a single or multiple ports as a protected or unprotected type.

To access this page, click **Security** > **Protected Ports**.

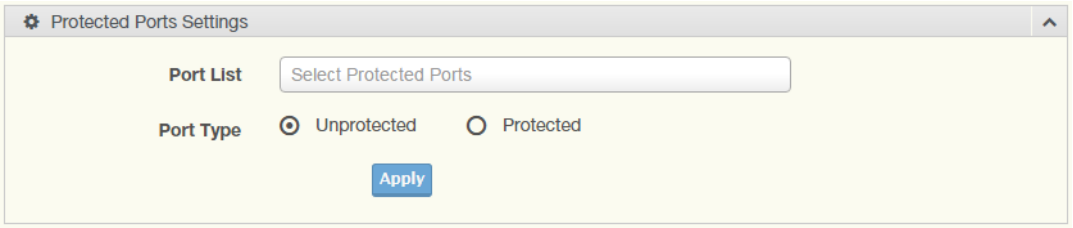


Figure 3.107 Security > Protected Ports

The following table describes the items in the previous figure.

Item	Description
Port List	Enter the port number to designate for the Protected Port setting.
Port Type	Select **Unprotected** or **Protected** to define the port type.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Protected Ports Status** settings are informational only: Protected Ports and Unprotected Ports.

Protected Ports Status

Protected Type	Port List
Protected Ports	
Unprotected Ports	all

Figure 3.108 Security > Protected Ports

3.9.4 DoS Prevention

The DoS Prevention page allows you to setup (enabled or disabled) the denial of service.

3.9.4.1 DoS Global Settings

The DoS Global Settings page allows you to configure (enabled or disabled) the setting for each function.

To access this page, click **Security** > **DoS Prevention** > **DoS Global Settings**.

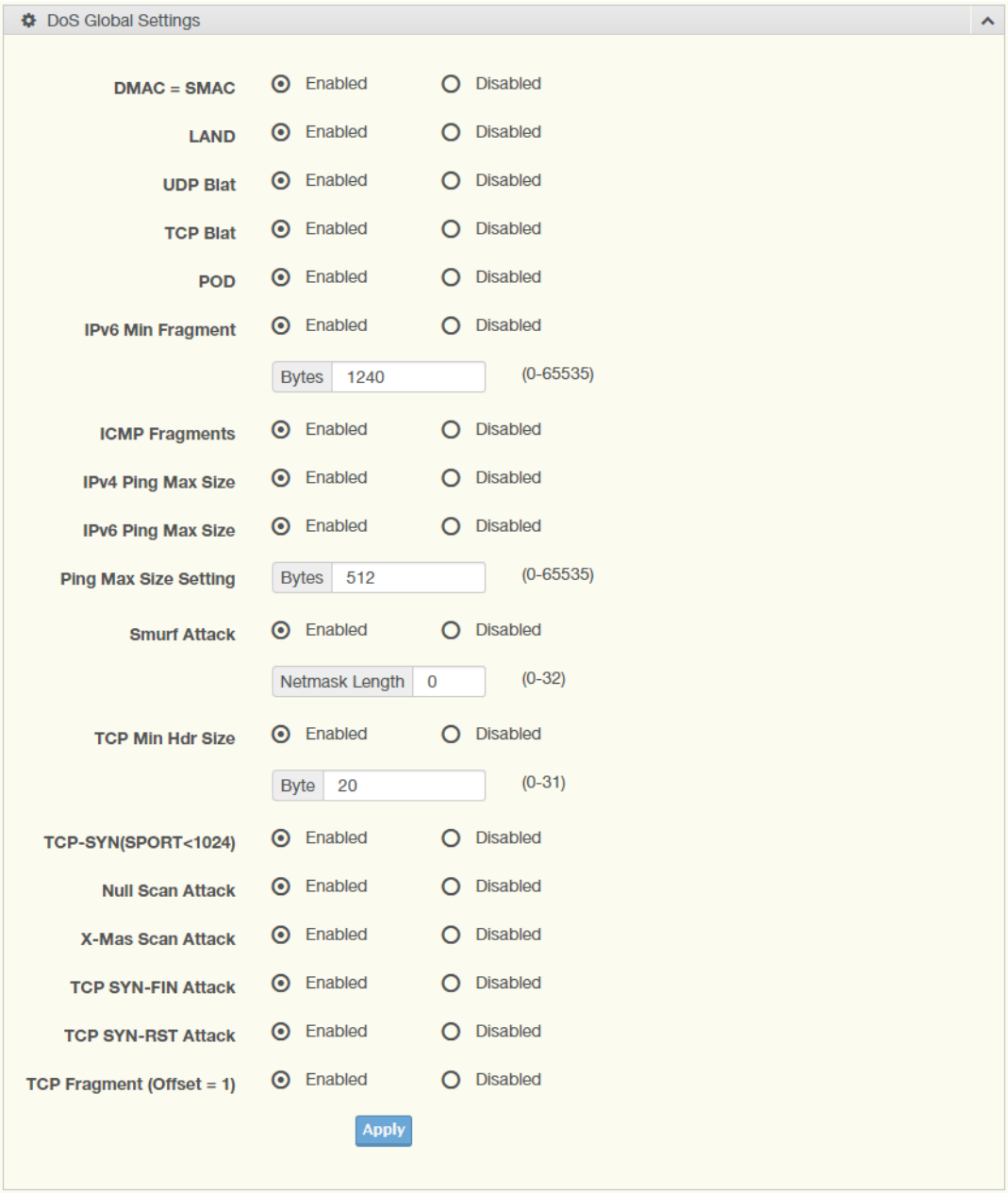


Figure 3.109 Security > DoS Prevention > DoS Global Settings

The following table describes the items in the previous figure.

Item	Description
DMAC = SMAC	Click **Enabled** or **Disabled** to define DMAC-SMAC for the DoS Global settings.
LAND	Click **Enabled** or **Disabled** to define LAND for the DoS Global settings.
UDP Blat	Click **Enabled** or **Disabled** to define UDP Blat for the DoS Global settings.
TCP Blat	Click **Enabled** or **Disabled** to define TCP Blat for the DoS Global settings.
POD	Click **Enabled** or **Disabled** to define POD for the DoS Global settings.
IPv6 Min Fragment	Click **Enabled** or **Disabled** to define minimum fragment size for the IPv6 protocol. Enter the variable in bytes (0 to 65535) to set the minimum fragment size when the function is enabled.

Item	Description
ICMP Fragments	Click **Enabled** or **Disabled** to define the ICMP Fragments function.
IPv4 Ping Max Size	Click **Enabled** or **Disabled** to set the maximum ping size for the IPv4 protocol.
IPv6 Ping Max Size	Click **Enabled** or **Disabled** to set a maximum ping size for the IPv6 protocol.
Ping Max Size Setting	Enter the variable in bytes (0 to 65535) to set the maximum ping size.
Smurf Attack	Click **Enabled** or **Disabled** to set the Smurf Attack function.
TCP Min Hdr Size	Click **Enabled** or **Disabled** to set the minimum header size. Enter the variable in bytes (0 to 31) to set the minimum header size.
TCP-SYN (SPORT < 1024)	Click **Enabled** or **Disabled** to set the TCP synchronization function (sport < 1021).
Null Scan Attack	Click **Enabled** or **Disabled** to set the Null Scan Attack function.
X-Mas Scan Attack	Click **Enabled** or **Disabled** to set the X-Mas Scan function.
TCP SYN-FIN Attack	Click **Enabled** or **Disabled** to set the TCP synchronization termination attack function.
TCP SYN-RST Attack	Click **Enabled** or **Disabled** to set the TCP synchronization reset attack function.
TCP Fragment (Offset = 1)	Click **Enabled** or **Disabled** to set the TCP fragment function (offset =1).
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **DoS Global Information** settings are informational only: DMAC = SMAC, Land Attack, UDP Blat, TCP Blat, POD (Ping of Death), IPv6 Min Fragment Size, ICMP Fragment Packets, IPv4 Ping Max Packet Size, IPv6 Ping Max Packet Size, Smurf Attack, TCP Min Header Length, TCP Syn (SPORT < 1024), Null

Scan Attack, X-Mas Scan Attack, TCP SYN-FIN Attack, TCP SYN-RST Attack and TCP Fragment (Offset = 1).

DoS Global Information

Information Name	Information Value
DMAC = SMAC	Enabled
Land Attack	Enabled
UDP Blat	Enabled
TCP Blat	Enabled
POD (Ping of Death)	Enabled
IPv6 Min Fragment Size	Enabled (1240 Bytes)
ICMP Fragment Packets	Enabled
IPv4 Ping Max Packet Size	Enabled (512 Bytes)
IPv6 Ping Max Packet Size	Enabled (512 Bytes)
Smurf Attack	Enabled (Netmask Length: 0)
TCP Min Header Length	Enabled (20 Bytes)
TCP Syn (SPORT < 1024)	Enabled
Null Scan Attack	Enabled
X-Mas Scan Attack	Enabled
TCP SYN-FIN Attack	Enabled
TCP SYN-RST Attack	Enabled
TCP Fragment (Offset = 1)	Enabled

Figure 3.110 Security > DoS Prevention > DoS Global Settings

3.9.4.2 DoS Port Settings

The DoS Port Settings page allow you to configure DoS security (enabled or disabled) for the selected port.

To access this page, click **Security** > **DoS Prevention** > **DoS Port Settings**.

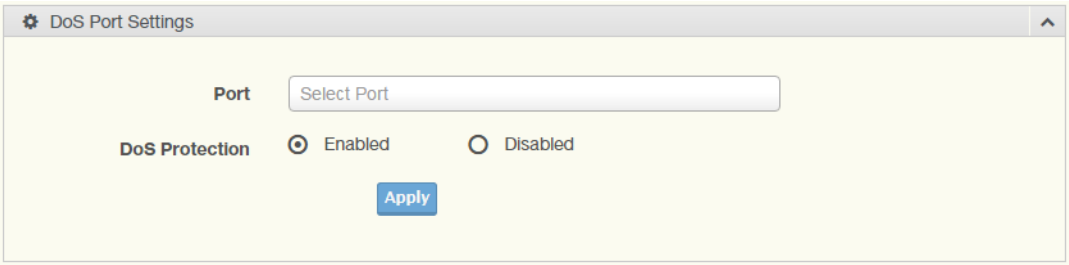


Figure 3.111 Security > DoS Prevention > DoS Port Settings

The following table describes the items in the previous figure.

Item	Description
Port	Select the port to configure for the DoS prevention function.
DoS Protection	Click **Enabled** or **Disabled** to set the DoS Port security function state.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **DoS Port Status** settings are informational only: Port and DoS Protection.

DoS Port Status

Port	DoS Protection
Port1	Disabled
Port2	Disabled
Port3	Disabled
Port4	Disabled
Port5	Disabled
Port6	Disabled
Port7	Disabled
Port8	Disabled
Trunk1	Disabled
Trunk2	Disabled
Trunk3	Disabled
Trunk4	Disabled
Trunk5	Disabled
Trunk6	Disabled
Trunk7	Disabled
Trunk8	Disabled

Figure 3.112 Security > DoS Prevention > DoS Port Settings

3.9.5 Applications

The Applications function allows you to configure various types of AAA lists.

3.9.5.1 HTTP

The HTTP page allows you to combine all kinds of AAA lists to the HTTP line. Attempts to access the switch's Web UI from HTTP are first authenticated.

To access this page, click **Security** > **Applications** > **HTTP**.

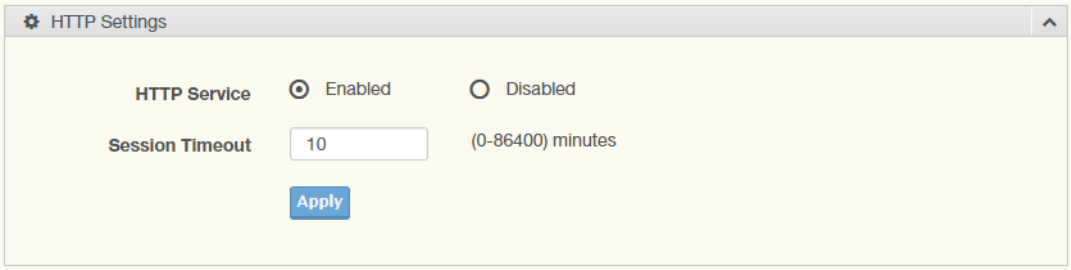


Figure 3.113 Security > Applications > HTTP

The following table describes the items in the previous figure.

Item	Description
HTTP Service	Click **Enabled** or **Disabled** to set up Ethernet encapsulation (remote access) through HTTP function.
Session Timeout	Enter the variable in minutes (0 to 86400) to define the timeout period for the HTTP session.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **HTTP Information** settings are informational only: HTTP Service and Session Timeout.

Figure 3.114 Security > Applications > HTTP

3.9.6 802.1x

The 802.1x function provides port-based authentication to prevent unauthorized devices (clients) from gaining access to the network.

3.9.6.1 802.1x Global Settings

The 802.1x Global Settings page allows you to set the state (enabled or disabled) for the selected IP server address, port, accounting port and associated password, including a re-authentication period.

To access this page, click **Security** > **802.1x** > **802.1x Global Settings**.

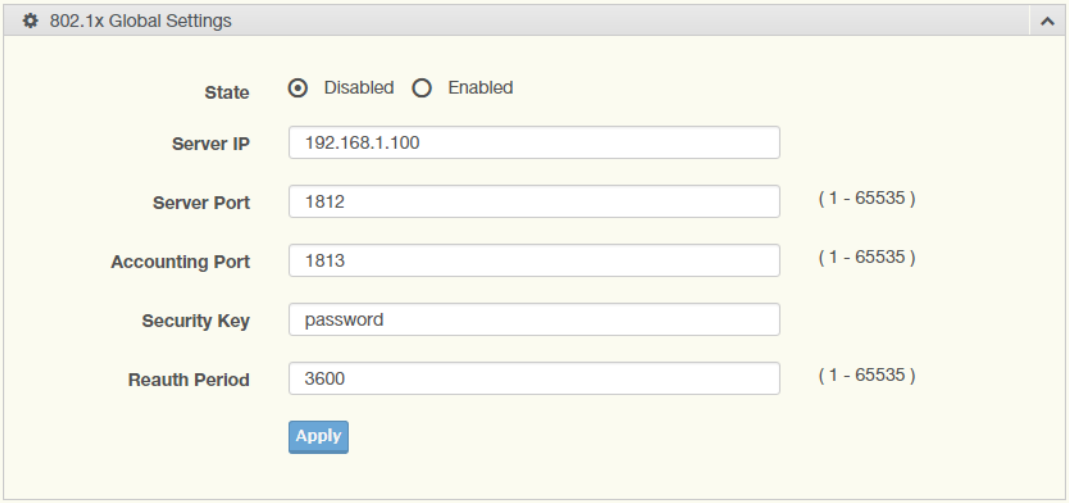


Figure 3.115 Security > 802.1x > 802.1x Global Settings

The following table describes the items in the previous figure.

Item	Description
State	Click **Enabled** or **Disabled** to set up 802.1x Setting function.
Server IP	Enter the IP address of the local server providing authentication function.
Server Port	Enter the port number (1 to 65535) assigned to the listed Server IP.
Accounting Port	Enter the port number (1 to 65535) assigned to the listed server IP configured to provide authorization and authentication for network access.
Security Key	Enter the variable to define the network security key used in authentication.
Reauth Period	Enter the variable in seconds to define the period of time between authentication attempts.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **802.1x Information** settings are informational only: 802.1x State, Server IP, Server Port, Accounting Port, Security Key and Reauth Period.

802.1x Information

Information Name	Information Value
802.1xState	Disabled
Server IP	192.168.1.100
Server Port	1812
Accounting Port	1813
Security Key	password
Reauth Period	3600

Figure 3.116 Security > 802.1x > 802.1x Global Settings

3.9.6.2 802.1x Port Configuration

The 802.1x Port Configuration page allows you to identify the authorization state for a port by using a MAC or Port authentication base.

To access this page, click **Security** > **802.1x** > **802.1x Port Configuration**.

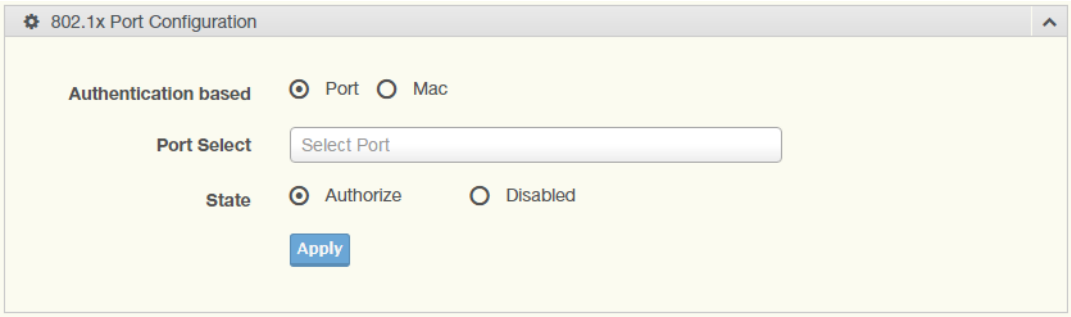


Figure 3.117 Security > 802.1x > 802.1x Port Configuration

The following table describes the items in the previous figure.

Item	Description
Authentication based	Click **Port** or **Mac** to designate the type of configuration for the 802.1x Port setting.
Port Select	Enter the port number associated with the configuration setting.
State	Click **Authorize** or **Disabled** to define the listed port's state mode.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **802.1x Port Authorization** settings are informational only: Port and Port State.

802.1x Port Authorization

Port	802.1x Port Authorization
Port1	Disabled
Port2	Disabled
Port3	Disabled
Port4	Disabled
Port5	Disabled
Port6	Disabled
Port7	Disabled

Figure 3.118 Security > 802.1x > 802.1x Port Configuration

3.10 QoS

The QoS function allows you to configure settings for the switch QoS interface and how the switch connects to a remote server to get services.

3.10.1 General

Traditionally, networks operate on a best-effort delivery basis, all traffic has equal priority and an equal chance of being delivered in a timely manner. When there is congestion, all traffic has an equal chance of being dropped.

The QoS feature can be configured for congestion-management and congestion-avoidance to specifically manage the priority of the traffic delivery. Implementing QoS in the network makes performance predictable and bandwidth utilization much more effective.

The QoS implementation is based on the prioritization values in Layer 2 frames.

3.10.1.1 QoS Properties

The QoS Properties allows you to set the QoS mode.

To access this page, click **QoS** > **General** > **QoS Properties**.

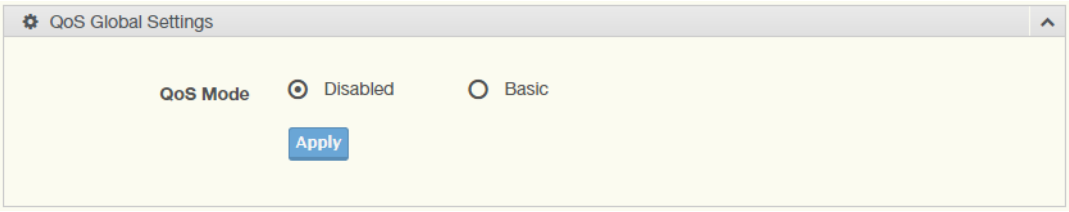


Figure 3.119 QoS > General > QoS Properties

The following table describes the items in the previous figure.

Item	Description
QoS Mode	Select **Disabled** or **Basic** to setup the QoS function.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **QoS Global Information** settings are informational only: QoS Mode.

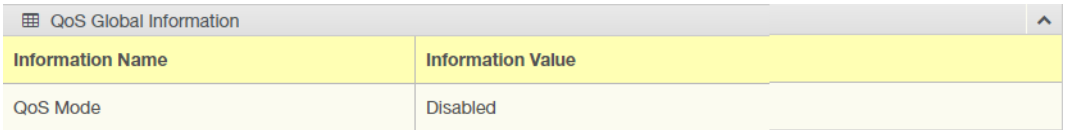


Figure 3.120 QoS > General > QoS Properties

3.10.1.2 QoS Settings

Once the QoS function is enabled, you can configure the available settings.

To access this page, click **QoS** > **General** > **QoS Settings**.

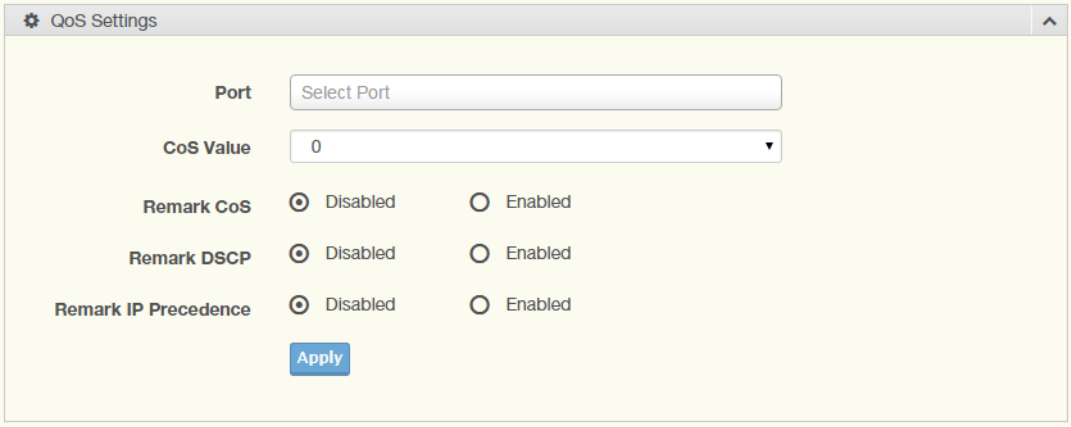


Figure 3.121 QoS > General > QoS Settings

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number to associate with the QoS setting.
CoS Value	Click the drop-down menu to designate the Class of Service (CoS) value (0 to 7) for the Port entry.
Remark CoS	Click **Disabled** or **Enabled** to setup the Remark CoS function. When enabled the LAN (preassigned priority values) is marked at Layer 2 boundary to CoS values.
Remark DSCP	Click **Disabled** or **Enabled** to setup the DSCP remark option for the QoS function.
Remark IP Precedence	Click **Disabled** or **Enabled** to setup the Remark IP Precedence for the QoS function.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **QoS Status** settings are informational only: Port, CoS value, Remark CoS, Remark DSCP and Remark IP Precedence.

QoS Status

Port	CoS Value	Remark CoS	Remark DSCP	Remark IP Precedence
Port1	0	Disabled	Disabled	Disabled
Port2	0	Disabled	Disabled	Disabled
Port3	0	Disabled	Disabled	Disabled
Port4	0	Disabled	Disabled	Disabled
Port5	0	Disabled	Disabled	Disabled
Port6	0	Disabled	Disabled	Disabled
Port7	0	Disabled	Disabled	Disabled
Port8	0	Disabled	Disabled	Disabled
Trunk1	0	Disabled	Disabled	Disabled
Trunk2	0	Disabled	Disabled	Disabled

Figure 3.122 QoS > General > QoS Settings

3.10.1.3 Queue Scheduling

The switch support eight CoS queues for each egress port. For each of the eight queues, two types of scheduling can be configured: Strict Priority and Weighted Round Robin (WRR).

Strict Priority scheduling is based on the priority of queues. Packets in a high-priority queue are always sent first and packets in a low-priority queue are only sent after all the high priority queues are empty.

Weighted RoundRobin (WRR) scheduling is based on the user priority specification to indicate the importance (weight) of the queue relative to the other CoS queues. WRR scheduling prevents low-priority queues from being completely ignored during periods of high priority traffic. The WRR scheduler sends some packets from each queue in turn.

To access this page, click **QoS** > **General** > **QoS Scheduling**.

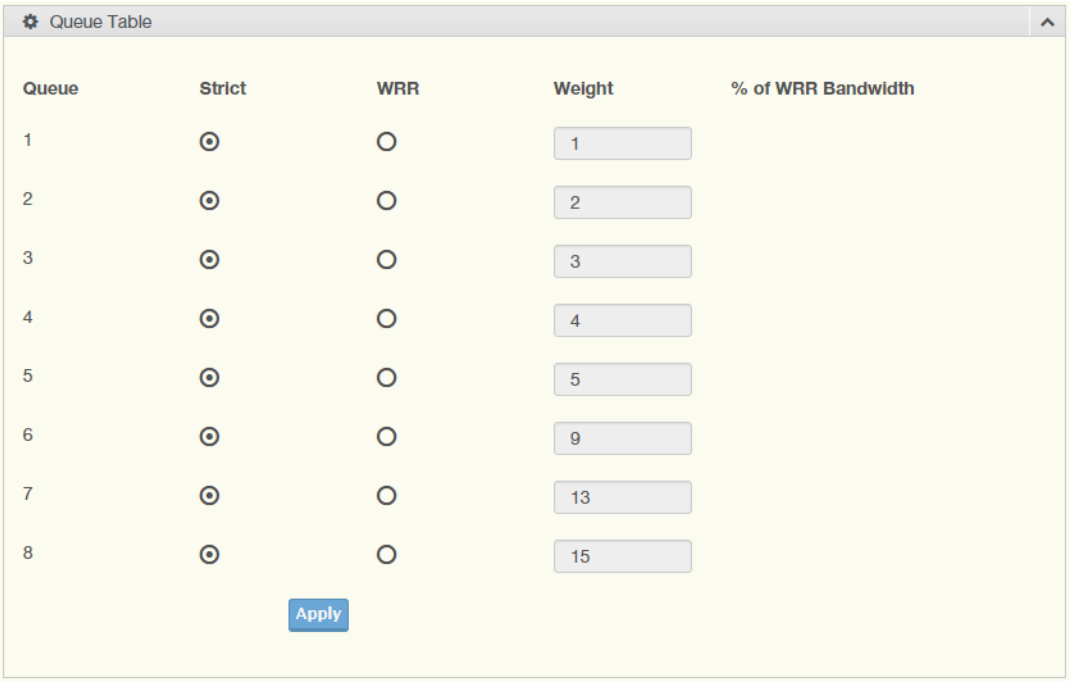


Figure 3.123 QoS > General > QoS Scheduling

The following table describes the items in the previous figure.

Item	Description
Queue	Queue entry for egress port.
Strict	Select Strict to assign the scheduling designation to the selected queue.
WRR	Select WRR to assign the scheduling designation to the selected queue.
Weight	Enter a queue priority (weight) relative to the defined entries (WRR only).
% of WRR Bandwidth	Displays the allotted bandwidth for the queue entry in percentage values.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Queue Information** settings are informational only: Strict Priority Queue Number.

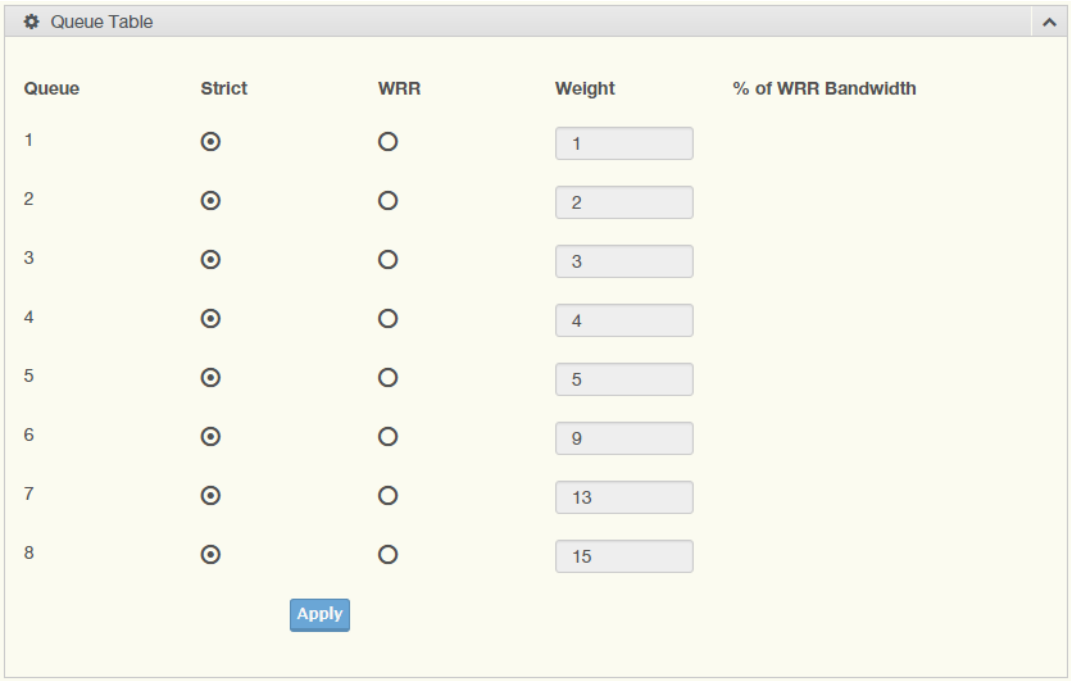


Figure 3.124 QoS > General > QoS Scheduling

3.10.1.4 CoS Mapping

The CoS Mapping allows you to apply CoS mapping.

To access this page, click **QoS** > **General** > **CoS Mapping**.

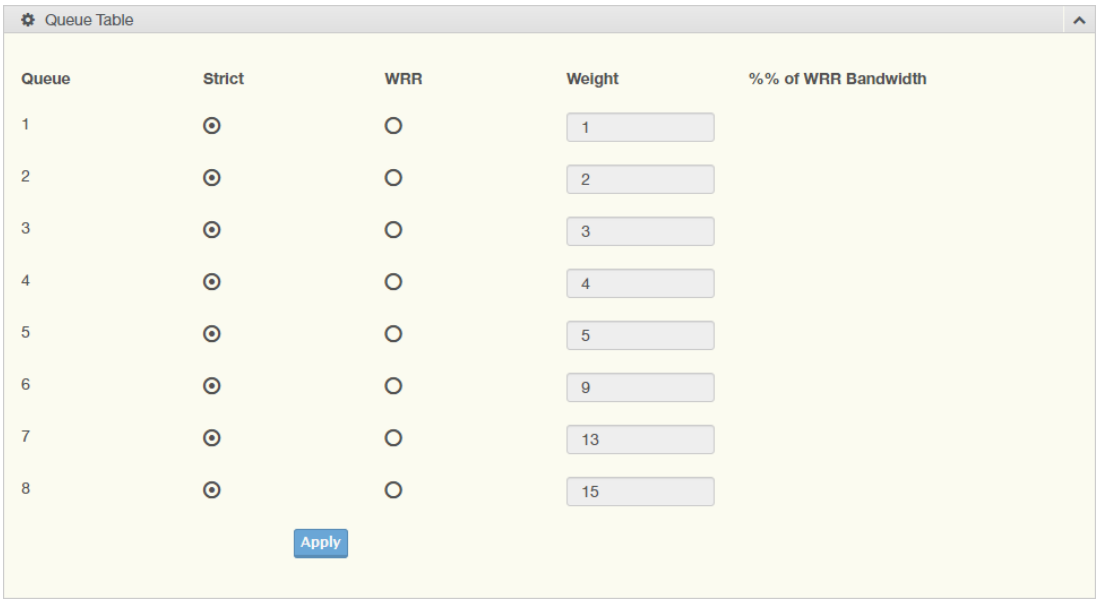


Figure 3.125 QoS > General > CoS Mapping

The following table describes the items in the previous figure.

Item	Description
CoS to Queue Mapping	
Class of Service	Displays the CoS for the queue entry.
Queue	Click the drop-down menu to select the queue priority for selected CoS
Queue to CoS Mapping	

Item	Description
Queue	Displays the queue entry for CoS mapping.
Class of Service	Click the drop-down menu to select the CoS type
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Queue Mapping Information** settings are informational only: Queue and Mapping to CoS.

CoS Mapping Information

CoS	Mapping to Queue
0	2
1	1
2	3
3	4
4	5
5	6
6	7
7	8

Figure 3.126 QoS > General > CoS Mapping

The ensuing table for **Queue Mapping Information** settings are informational only:Queue and Mapping to CoS.

Queue Mapping Information

Queue	Mapping to CoS
1	1
2	0
3	2
4	3
5	4
6	5
7	6
8	7

Figure 3.127 QoS > General > CoS Mapping

3.10.1.5 DSCP Mapping

The DSCP to Queue mapping function maps queue values in incoming packets to a DSCP value that QoS uses internally to represent the priority of the traffic. The following table shows the DSCP to Queue map.

If these values are not appropriate for your network, you need to modify them.

To access this page, click **QoS** > **General** > **DSCP Mapping**.

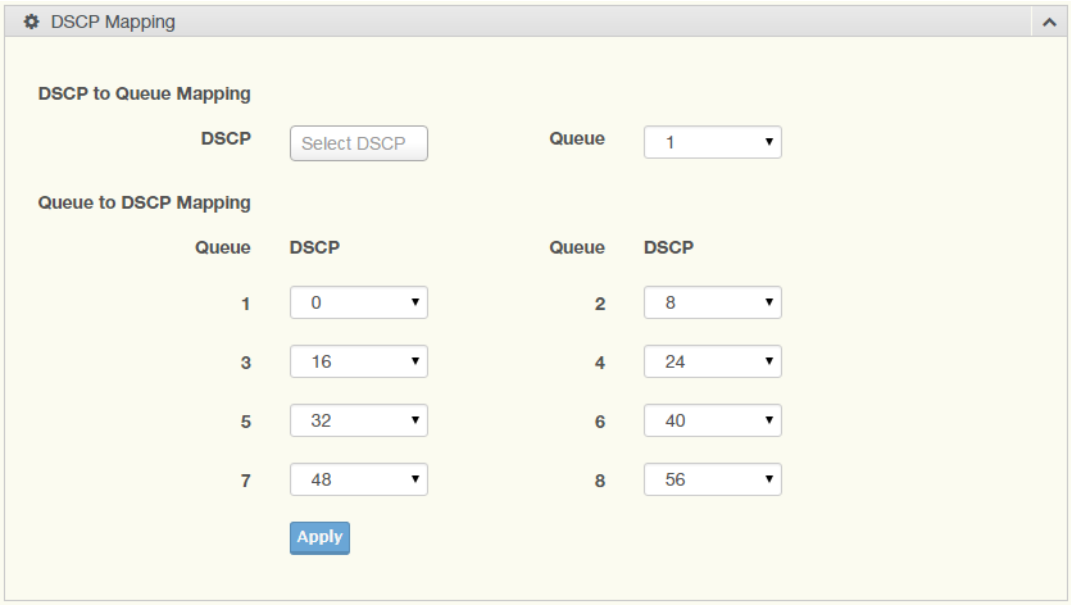


Figure 3.128 QoS > General > DSCP Mapping

The following table describes the items in the previous figure.

Item	Description
DSCP to Queue Mapping	
DSCP	Enter the DSCP entry to define the precedence values.
Queue	Click the drop-down menu to select the queue designation for the DSCP value.
Queue to DSCP Mapping	
Queue	Displays the queue value for the DSCP map.
DSCP	Enter the DSCP entry to define the precedence values.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **DSCP Mapping Information** settings are informational only: DSCP and Mapping to Queue.

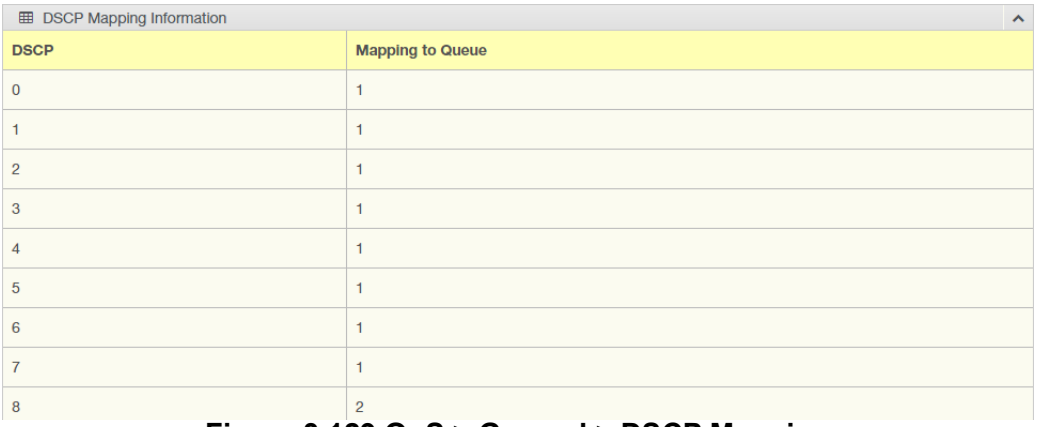


Figure 3.129 QoS > General > DSCP Mapping

3.10.1.6 IP Precedence Mapping

The IP Precedence Mapping allows you to set IP Precedence mapping.

To access this page, click **QoS** > **General** > **IP Precedence Mapping**.

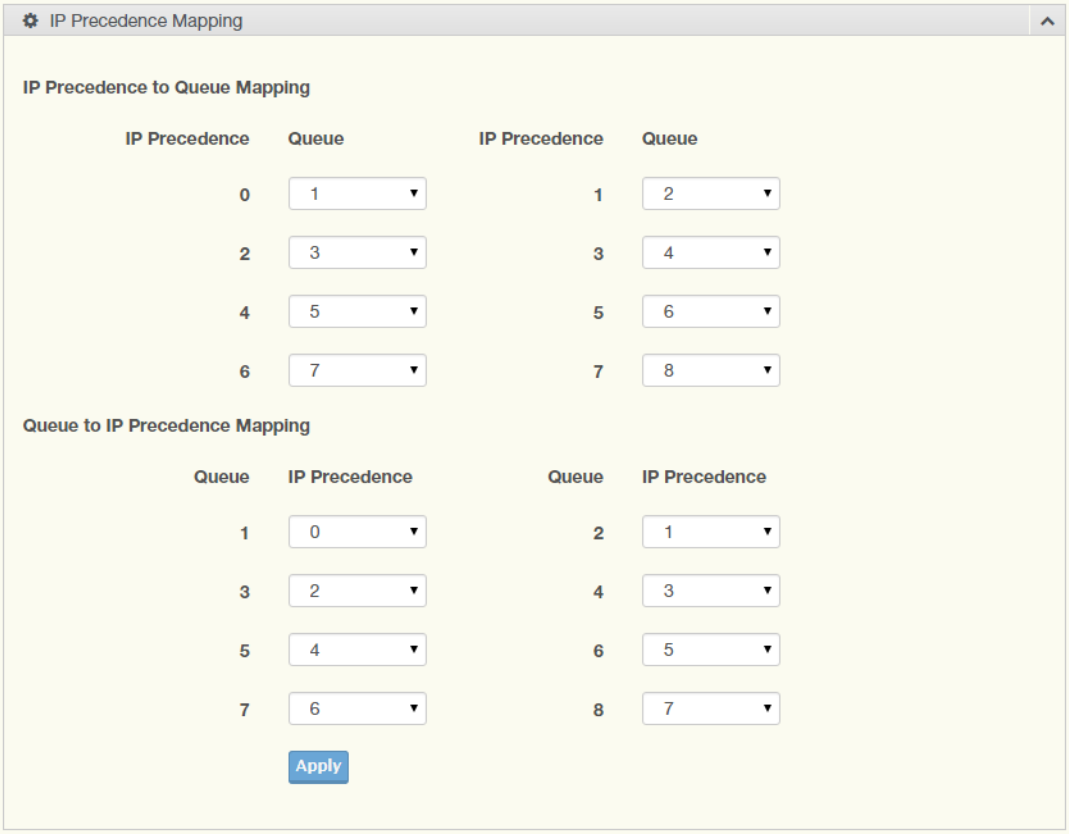


Figure 3.130 QoS > General > IP Precedence Mapping

The following table describes the items in the previous figure.

Item	Description
IP Precedence to Queue Mapping	
IP Precedence	Displays the IP precedence value for the queue map.
Queue	Click the drop-down menu to map a queue value to the selected IP precedence.
Queue to IP Precedence Mapping	
Queue	Displays the queue entry for mapping IP precedence values.
IP Precedence	Click the drop-down menu to map an IP precedence value to the selected queue.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **IP Precedence Mapping Information** settings are informational only: IP Precedence and Mapping to Queue.

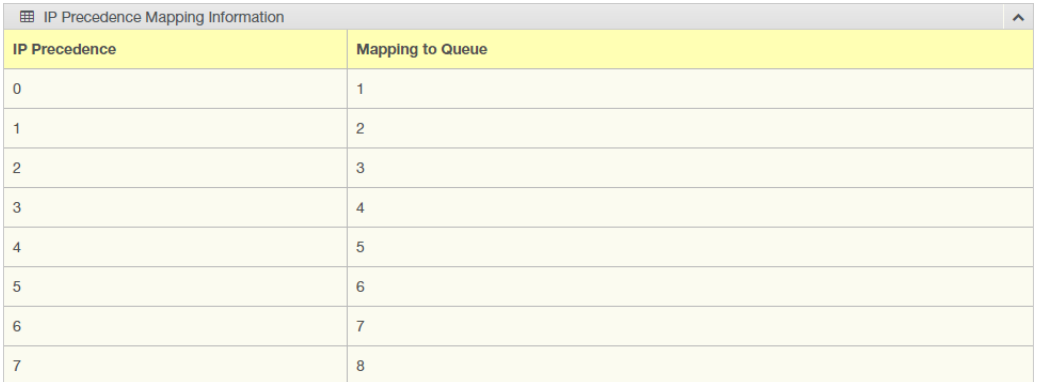


Figure 3.131 QoS > General > IP Precedence Mapping

The ensuing table for **Queue Mapping Information** settings are informational only: Queue and Mapping to IP Precedence.

Queue Mapping Information

Queue	Mapping to IP Precedence
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7

Figure 3.132 QoS > General > IP Precedence Mapping

3.10.2 QoS Basic Mode

Quality of Service (QoS) allows to give preferential treatment to certain types of traffic at the expense of others. Without QoS, the switch offers best-effort service to each packet, regardless of the packet contents or size sending the packets without any assurance of reliability, delay bounds, or throughput.

3.10.2.1 Global Settings

The Global Settings page allows you to configure the trust mode to a port selection.

To access this page, click **QoS** > **QoS Basic Mode** > **Global Settings**.

The function is only available when the device is set to **QoS Basic mode**.

Figure 3.133 QoS > QoS Basic Mode > Global Settings

The following table describes the items in the previous figure.

Item	Description
Trust Mode	Click the drop-down menu to select the trust state of the QoS basic mode, settings: CoS/802.1p (default), none, DSCP, CoS/802.1p-DSCP, IP Precedence.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **QoS Information** settings are informational only: Trust Mode.

QoS Global Information

Information Name	Information Value
QoS Mode	Disabled

Figure 3.134 QoS > QoS Basic Mode > Global Settings

3.10.2.2 Port Settings

The Port Settings page allows you to define a trust state (enabled or disabled) to a listed port.

To access this page, click **QoS** > **QoS Basic Mode** > **Port Settings**.

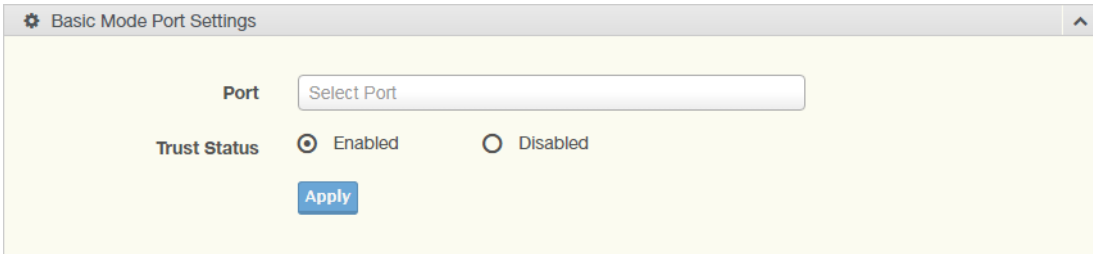


Figure 3.135 QoS > QoS Basic Mode > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number for the QoS basic mode setting.
Trust State	Select **Enabled** or **Disabled** to set the port's trust state status.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **QoS Port Status** settings are informational only: Port and Trust State.

Basic Mode Port Information

Port	Trust Status
Port1	Enabled
Port2	Enabled
Port3	Enabled
Port4	Enabled
Port5	Enabled
Port6	Enabled
Port7	Enabled
Port8	Enabled
Trunk1	Enabled

Figure 3.136 QoS > QoS Basic Mode > Port Settings

3.10.3 Rate Limit

Rate Limits features control on a per port basis. Bandwidth control is supported for the following: Ingress Bandwidth Control, Egress Bandwidth Control and Egress Queue.

3.10.3.1 Ingress Bandwidth Control

The Ingress Bandwidth Control page allows you to configure the bandwidth control for a listed port.

The device must be in QoS Basic mode to configure the feature.

To access this page, click **QoS** > **Rate Limit** > **Ingress Bandwidth Control**.

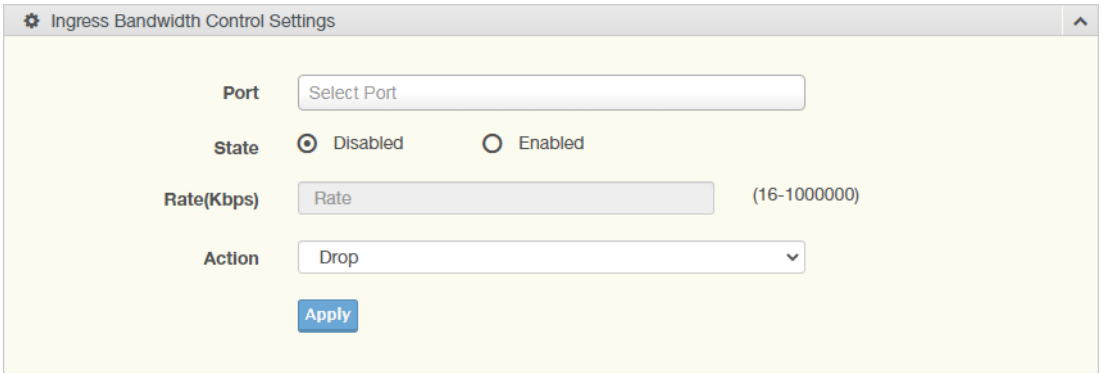


Figure 3.137 QoS > Rate Limit > Ingress Bandwidth Control

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number for the rate limit setup.
State	Select **Disabled** or **Enabled** to set the port's state status.
Rate (Kbps)	Enter the value in Kbps (16 to 1000000) to set as the bandwidth rate for the selected port.
Action	Click the drop-down menu to select the action to associate with the control policy: Drop (default) or shutdown.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Ingress Bandwidth Control Status** settings are informational only: Port and Ingress Rate Limit (Kbps).

Ingress Bandwidth Control Status

Port	Ingress RateLimit (Kbps)	Action
Port1	Off	Drop
Port2	Off	Drop
Port3	Off	Drop
Port4	Off	Drop
Port5	Off	Drop
Port6	Off	Drop
Port7	Off	Drop
Port8	Off	Drop

Figure 3.138 QoS > Rate Limit > Ingress Bandwidth Control

3.10.3.2 Egress Bandwidth Control

The Egress Bandwidth Control page allows you to set the egress bandwidth control for a listed port.

To access this page, click **QoS** > **Rate Limit** > **Egress Bandwidth Control**.

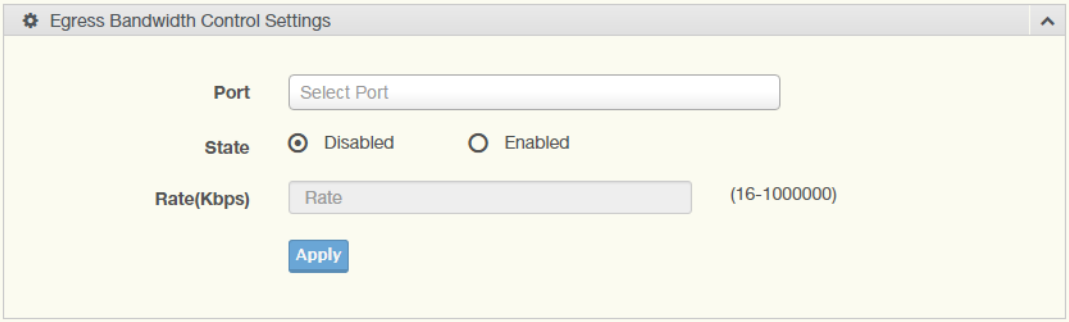


Figure 3.139 QoS > Rate Limit > Egress Bandwidth Control

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number to set the Egress Bandwidth Control.
State	Select **Disabled** or **Enabled** to set the Egress Bandwidth Control state.
Rate (Kbps)	Enter the value in Kbps (16 to 1000000) to set the Egress Bandwidth rate.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Egress Bandwidth Control Status** settings are informational only: Port and Egress Rate Limit (Kbps).

Egress Bandwidth Control Status

Port	Egress RateLimit (Kbps)
Port1	Off
Port2	Off
Port3	Off
Port4	Off
Port5	Off
Port6	Off
Port7	Off
Port8	Off

Figure 3.140 QoS > Rate Limit > Egress Bandwidth Control

3.10.3.3 Egress Queue

The Egress Queue page allows you to set the egress bandwidth parameters.

To access this page, click **QoS** > **Rate Limit** > **Egress Queue**.

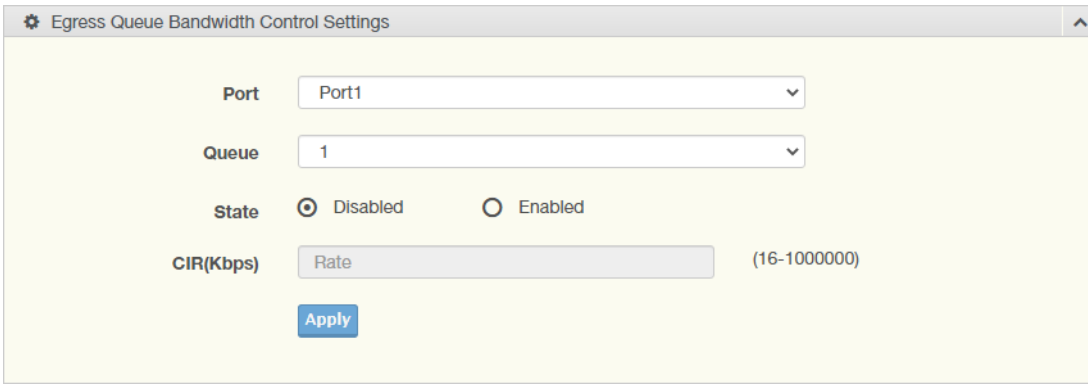


Figure 3.141 QoS > Rate Limit > Egress Queue

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select the port to define the Egress queue.
Queue	Click the drop-down menu to set the queue order for the Egress setting.
State	Click **Disabled** or **Enabled** to set the Egress queue state.
CIR (Kbps)	Enter the value in Kbps (16 to 1000000) to set the CIR rate for the Egress queue.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **FE1 Egress Per Queue Status** settings are informational only: Queue Id and Egress Rate Limit (Kbps).

Port1 Egress Per Queue Status

Queue Id	Egress RateLimit (Kbps)
1	Off
2	Off
3	Off
4	Off
5	Off
6	Off
7	Off
8	Off

Figure 3.142 QoS > Rate Limit > Egress Queue

3.11 Management

3.11.1 LLDP

LLDP is a one-way protocol without request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function.

3.11.1.1 LLDP System Settings

The LLDP System Settings allows you to configure the status (enabled or disabled) for the protocol, set the interval for frame transmission, set the hold time multiplier and the re-initialization delay.

To access this page, click **Management** > **LLDP** > **LLDP System Settings**.

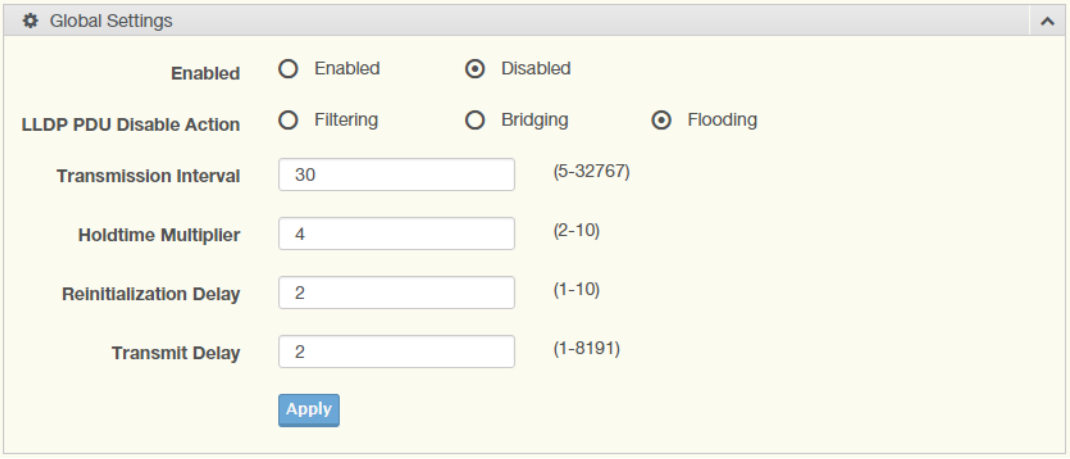


Figure 3.143 Management > LLDP > LLDP System Settings

The following table describes the items in the previous figure.

Item	Description
Enabled	Click **Enabled** or **Disabled** to set the Global Settings state.
LLDP PDU Disable Action	Click to select the LLDP PDU handling action when LLDP is globally disabled. Options include: Filtered, Bridged, or Flooded.
Transmission Interval	Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5 to 32768 seconds.
Holdtime Multiplier	Select the multiplier on the transmit interval to assign to TTL.
Reinitialization Delay	Select the delay length before re-initialization.
Transmit Delay	Select the delay after an LLDP frame is sent.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **LLDP Global Config** settings are informational only: LLDP Enabled, LLDP PDU Disable Action, Transmission Interval, Holdtime Multiplier, Reinitialization Delay and Transmit Delay.

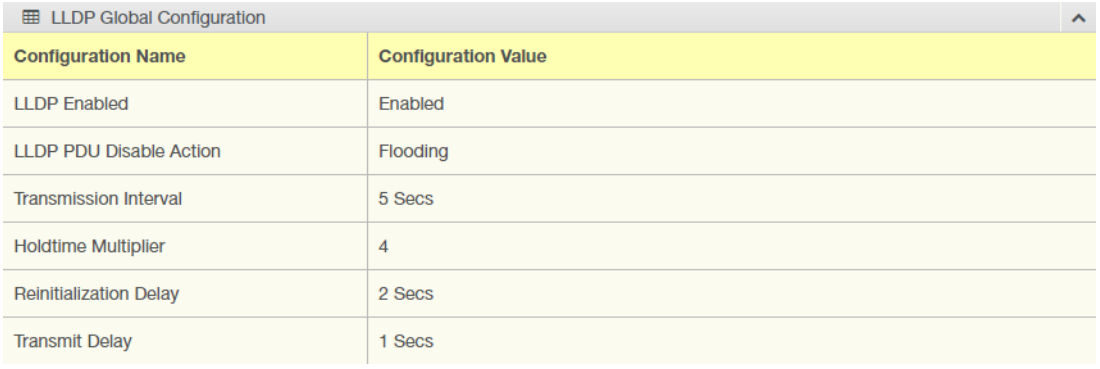


Figure 3.144 Management > LLDP > LLDP System Settings

3.11.1.2 LLDP Port Settings

The LLDP Port Settings page allows you to configure the state (enabled or disabled) of the selected port.

To access this page, click **Management** > **LLDP** > **LLDP Port Settings**.

Figure 3.145 Management > LLDP > LLDP Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the port number associated with the LLDP setting.
State	Click the drop-down menu to select the LLDP port state.
Apply	Click **Apply** to save the values and update the screen.

Optional TLVs Selection

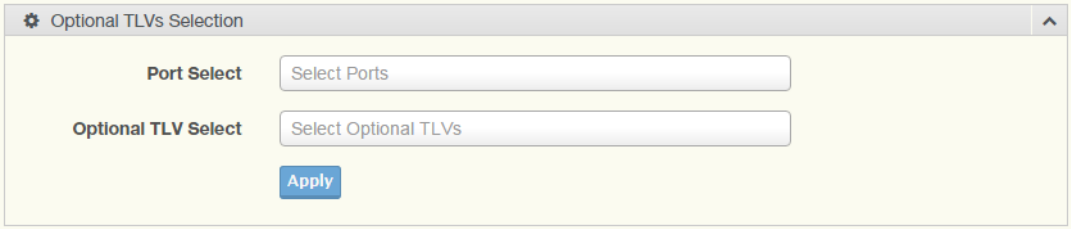


Figure 3.146 Management > LLDP > LLDP Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the port number associated with the TLV (optional) selection.
Optional TLV Select	Click the drop-down menu to select the LLDP optional TLVs to be carried (multiple selections are allowed). ■ System Name: To include system name TLV in LLDP frames. ■ Port Description: To include port description TLV in LLDP frames. ■ System Description: To include system description TLV in LLDP frames. ■ System Capability: To include system capability TLV in LLDP frames. ■ 802.3 MAC-PHY: ■ 802.3 Link Aggregation: ■ 802.3 Maximum Frame Size: ■ Management Address: ■ 802.1 PVID:
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **LLDP Port Status** settings are informational only: Port, State and Selected Optional TLVs.

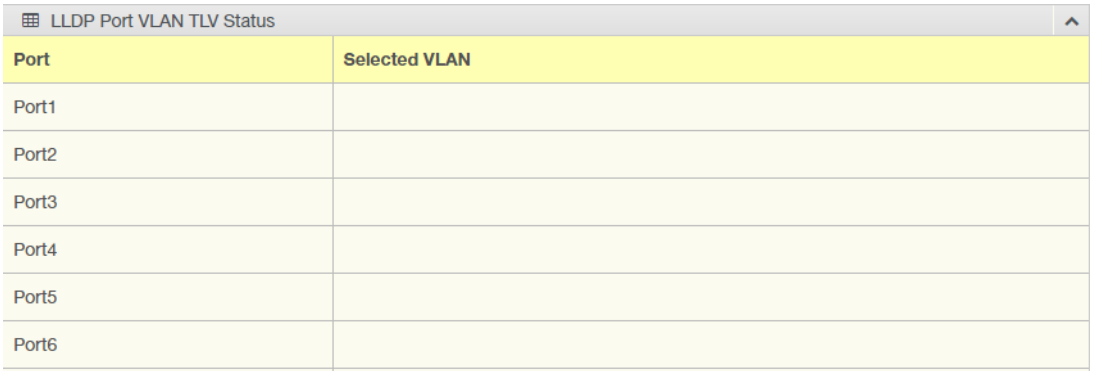


Figure 3.147 Management > LLDP > LLDP Port Settings

VLAN Name TLV VLAN Selection

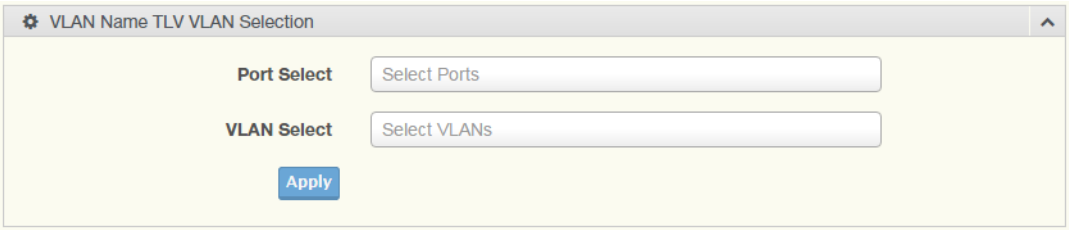


Figure 3.148 Management > LLDP > LLDP Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the port number to associated with the TLV selection.
VLAN Select	Select the VLAN Name ID to be carried out (multiple selection is allowed).
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **LLDP Port VLAN TLV Status** settings are informational only: Port and Selected VLAN.

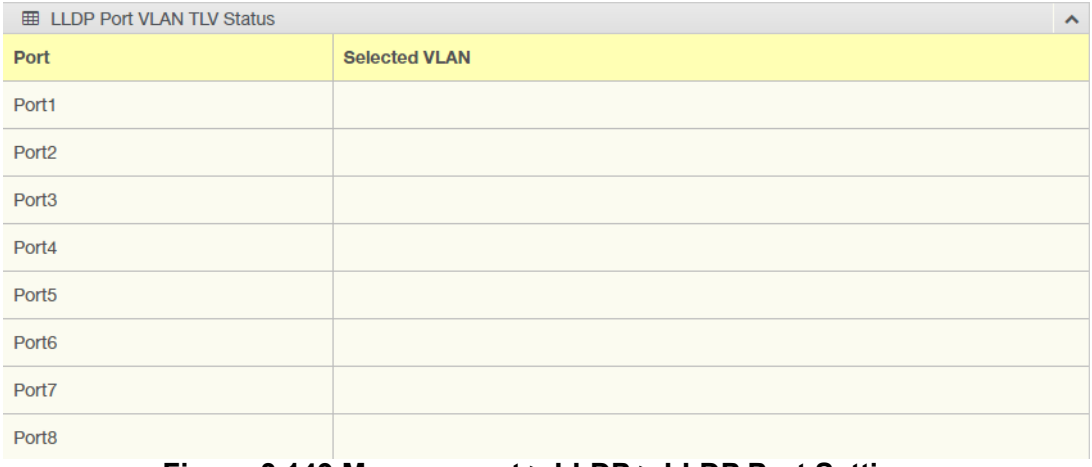


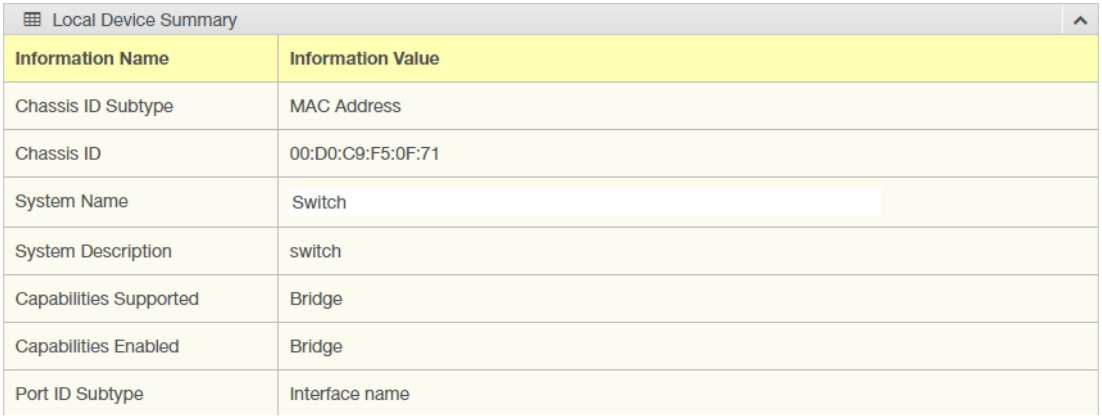
Figure 3.149 Management > LLDP > LLDP Port Settings

3.11.1.3 LLDP Local Device Info

The LLDP Local Device Info page allows you to view information regarding network devices, providing that the switch has already obtained LLDP information on the devices.

To access this page, click **Management** > **LLDP** > **LLDP Local Device Info**.

The ensuing table for **Local Device Summary** settings are informational only: Chassis ID Subtype, Chassis ID, System Name, System Description, Capabilities Supported, Capabilities Enabled and Port ID Subtype.

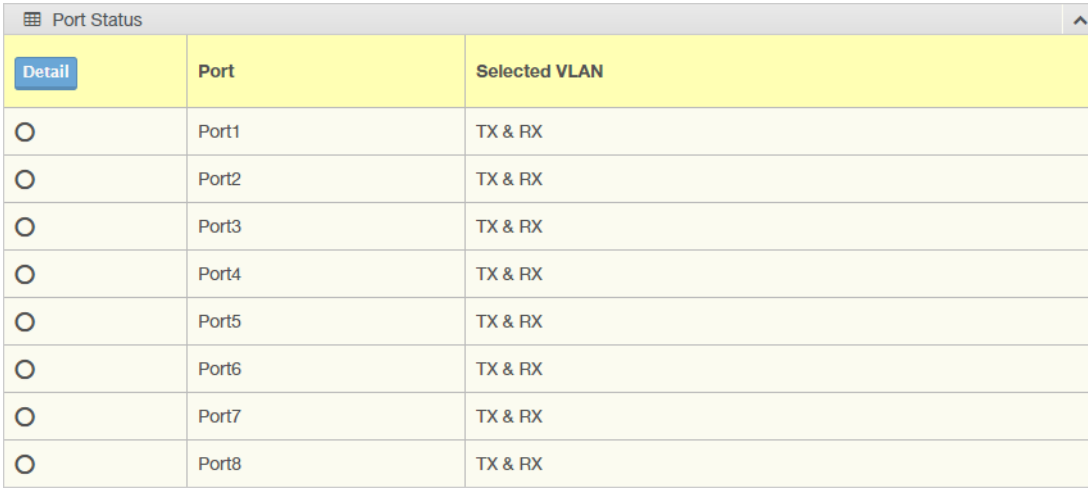


Local Device Summary

Information Name	Information Value
Chassis ID Subtype	MAC Address
Chassis ID	00:D0:C9:F5:0F:71
System Name	Switch
System Description	switch
Capabilities Supported	Bridge
Capabilities Enabled	Bridge
Port ID Subtype	Interface name

Figure 3.150 Management > LLDP > LLDP Local Device Info

The ensuing table for **Port Status** settings are informational only: Port, Selected VLAN and **Detail** (click the radio box and click **Detail** to displays the details).



Port Status

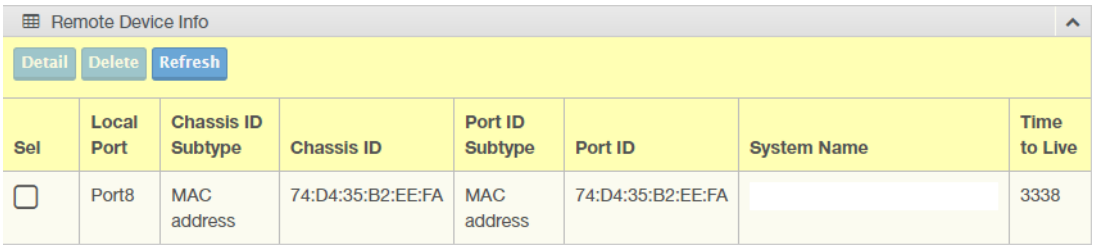
Detail	Port	Selected VLAN
○	Port1	TX & RX
○	Port2	TX & RX
○	Port3	TX & RX
○	Port4	TX & RX
○	Port5	TX & RX
○	Port6	TX & RX
○	Port7	TX & RX
○	Port8	TX & RX

Figure 3.151 Management > LLDP > LLDP Local Device Info

3.11.1.4 LLDP Remote Device Info

The LLDP Remote Device Info page allows you to view information about remote devices, LLDP information must be available on the switch.

To access this page, click **Management** > **LLDP** > **LLDP Remote Device Info**.



Remote Device Info

Detail Delete Refresh

Sel	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live
☐	Port8	MAC address	74:D4:35:B2:EE:FA	MAC address	74:D4:35:B2:EE:FA		3338

Figure 3.152 Management > LLDP > LLDP Remote Device Info

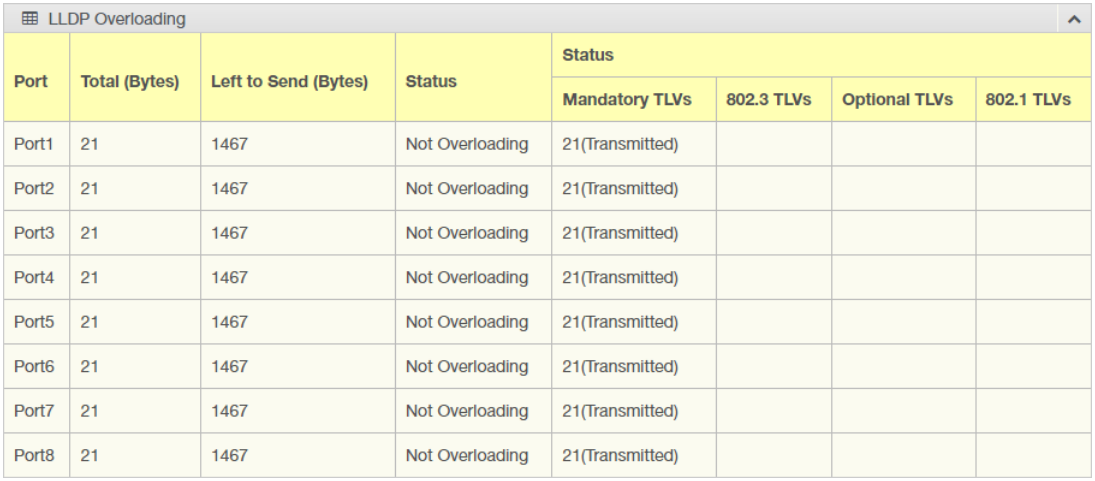
The following table describes the items in the previous figure.

Item	Description
Detail	Click to display the device details.
Delete	Click to delete the selected devices.
Refresh	Click to refresh the remote device information list.

3.11.1.5 LLDP Overloading

To access this page, click **Management** > **LLDP** > **LLDP Overloading**.

The ensuing table for **LLDP Overloading** settings are informational only: Port, Total (Bytes), Left to Send (Bytes), Status and Status (Mandatory TLVs, 802.3 TLVs, Optional TLVs and 802.1 TLVs).



LLDP Overloading

Port	Total (Bytes)	Left to Send (Bytes)	Status	Status			
				Mandatory TLVs	802.3 TLVs	Optional TLVs	802.1 TLVs
Port1	21	1467	Not Overloading	21(Transmitted)			
Port2	21	1467	Not Overloading	21(Transmitted)			
Port3	21	1467	Not Overloading	21(Transmitted)			
Port4	21	1467	Not Overloading	21(Transmitted)			
Port5	21	1467	Not Overloading	21(Transmitted)			
Port6	21	1467	Not Overloading	21(Transmitted)			
Port7	21	1467	Not Overloading	21(Transmitted)			
Port8	21	1467	Not Overloading	21(Transmitted)			

Figure 3.153 Management > LLDP > LLDP Overloading

3.11.2 SNMP

Simple Network Management Protocol (SNMP) is a protocol to facilitate the monitoring and exchange of management information between network devices. Through SNMP, the health of the network or status of a particular device can be determined.

3.11.2.1 SNMP Settings

The SNMP Settings page allows you to set the SNMP daemon state (enabled or disabled).

To access this page, click **Management** > **SNMP** > **SNMP Settings**.

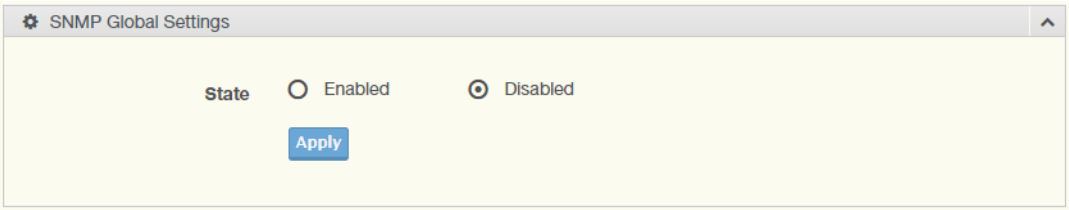


Figure 3.154 Management > SNMP > SNMP Settings

The following table describes the items in the previous figure.

Item	Description
State	Click **Enabled** or **Disabled** to define the SNMP daemon.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **SNMP Information** settings are informational only: SNMP.

Figure 3.155 Management > SNMP > SNMP Settings

3.11.2.2 SNMP Community

The SNMP Community page provides configuration options for the community.

SNMP v1 and SNMP v2c use the group name (Community Name) certification. It's role is similar to the password function. If SNMP v1 and SNMP v2c are used, you can go directly from the configuration settings to this page to configure the SNMP community.

To access this page, click **Management** > **SNMP** > **SNMP Community**.

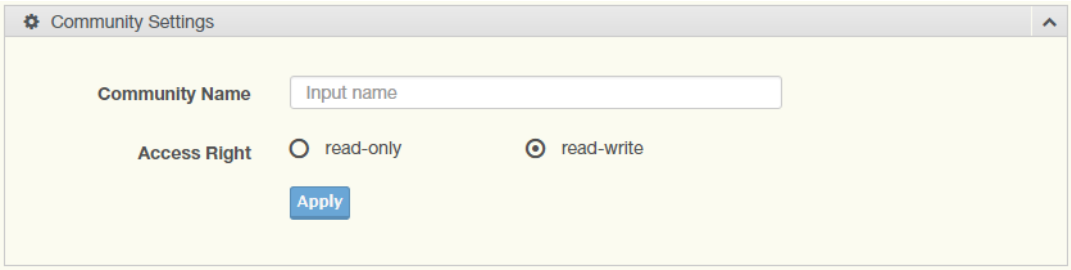


Figure 3.156 Management > SNMP > SNMP Community

The following table describes the items in the previous figure.

Item	Description
Community Name	Enter a community name (up to 20 characters).
Access Right	Click the radio box to specify the access level (read only or read write)
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Community Status** settings are informational only: No., Community Name, Access Right and **Delete** (click to delete the desired community name).

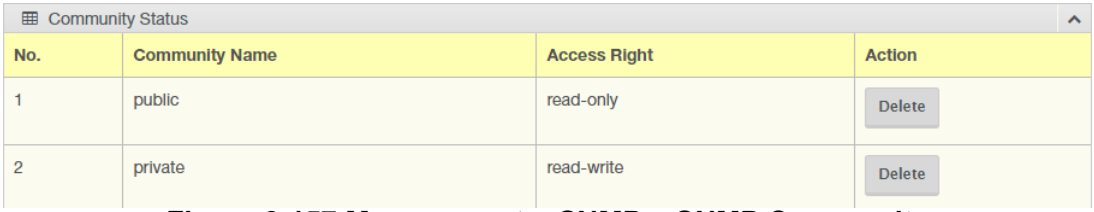


Figure 3.157 Management > SNMP > SNMP Community

3.11.2.3 SNMPv3 EngineID

The SNMPv3 EngineID feature is used to manage an SNMP module, and uniquely identifies the SNMP entity in the management domain. The device uses an internal algorithm to generate the SNMP engine ID.

To access this page, click **Management** > **SNMP** > **SNMPv3 EngineID**.

Figure 3.158 Management > SNMP > SNMPv3 EngineID

The following table describes the items in the previous figure.

Item	Description
SNMP EngineID	Displays the unique SNMP engine identifier.

3.11.2.4 SNMPv3 Settings

The SNMPv3 Settings page allows you to create SNMP groups. The users have the same level of security and access control permissions as defined by the group settings.

To access this page, click **Management** > **SNMP** > **SNMPv3 Settings**.

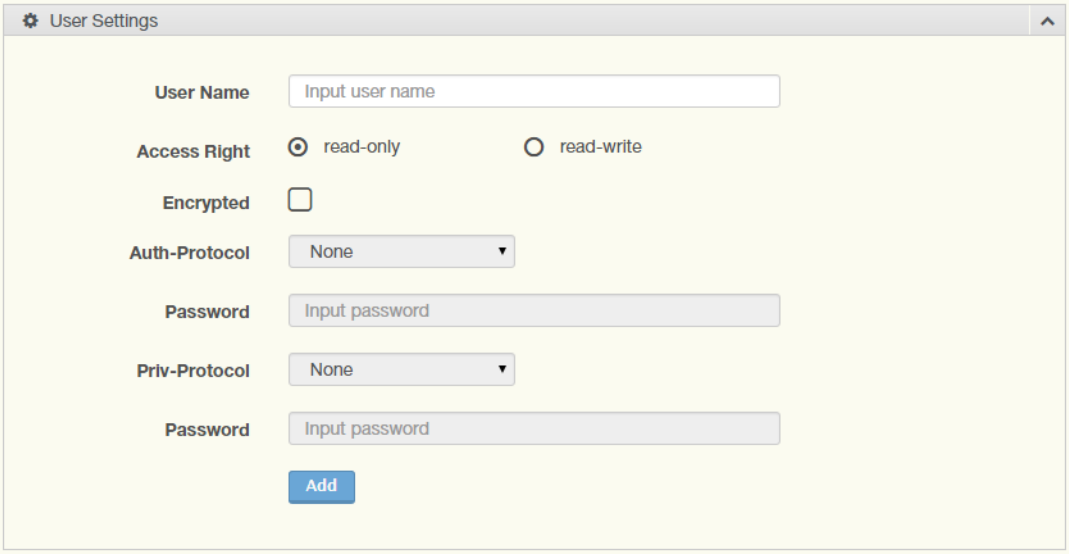


Figure 3.159 Management > SNMP > SNMPv3 Settings

The following table describes the items in the previous figure.

Item	Description
User Name	Enter a user name (up to 32 characters) to create an SNMP profile.
Access Right	Click **read-only** or **read-write** to define the access right for the profile.
Encrypted	Click the option to set the encrypted option for the user setting.
Auth-Protocol	Click the drop-down menu to select the authentication protocol: MD5 or SHA. The field requires a user password. ■ MD5: specify HMAC-MD5-96 authentication level ■ SHA: specify HMAC-SHA authentication protocol
Password	Enter the characters to define the password associated with the authentication protocol.
Priv-Protocol	Click the drop-down menu to select a privacy protocol: none, DES, or AES. The field requires a user password. ■ None: no privacy protocol ■ DES: Data Encryption Standard ■ AES: Advanced Encryption Standard

Item	Description
Password	Enter the characters to define the password associated with the authorization protocol.
Add	Click **Add** to save the values and update the screen.

The ensuing table for **User Status** settings are informational only: User Name, Access Right, Auth-Protocol, Priv-Protocol and **Delete** (click to delete the desired user name).

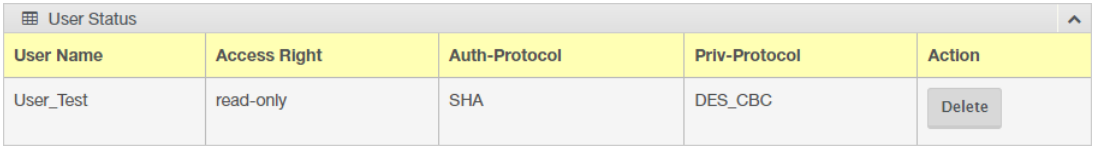


Figure 3.160 Management > SNMP > SNMPv3 Settings

3.11.2.5 SNMP Trap

The SNMP Trap page allows you to set the IP address of the node and the SNMP credentials corresponding to the version that is included in the trap message.

To access this page, click **Management** > **SNMP** > **SNMP Trap**.

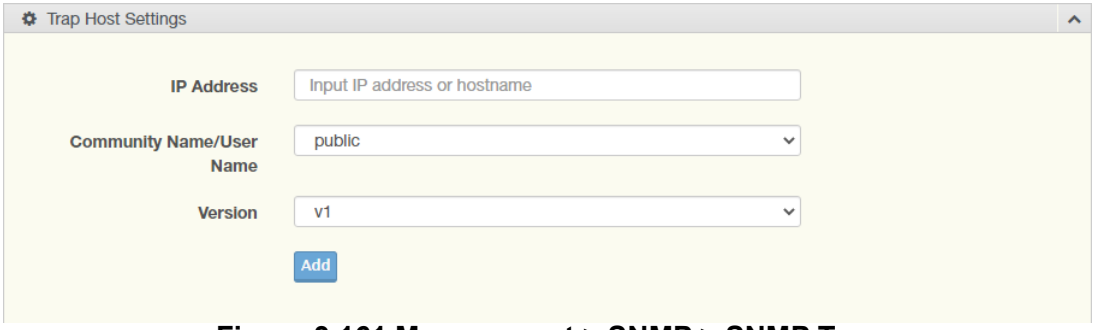


Figure 3.161 Management > SNMP > SNMP Trap

The following table describes the items in the previous figure.

Item	Description
IP Address	Enter the IP address to designate the SNMP trap host.
Community Name	Click the drop-down menu to select a defined community name.
Version	Click the drop-down menu to designate the SNMP version credentials (v1 or v2c).
Add	Click **Add** to save the values and update the screen.

The ensuing table for **Trap Host Status** settings are informational only: No., IP Address, Community Name, Version and **Delete** (click to delete the desired IP address).

Figure 3.162 Management > SNMP > SNMP Trap

3.11.3 TCP Modbus

The TCP Modbus function allows for client-server communication between a switch module (server) and a device in the networking running MODBUS client software (client).

3.11.3.1 TCP Modbus Settings

The TCP Modbus Settings page allows you to configure the modbus function.

To access this page, click **Management** > **TCP Modbus** > **TCP Modbus Settings**.

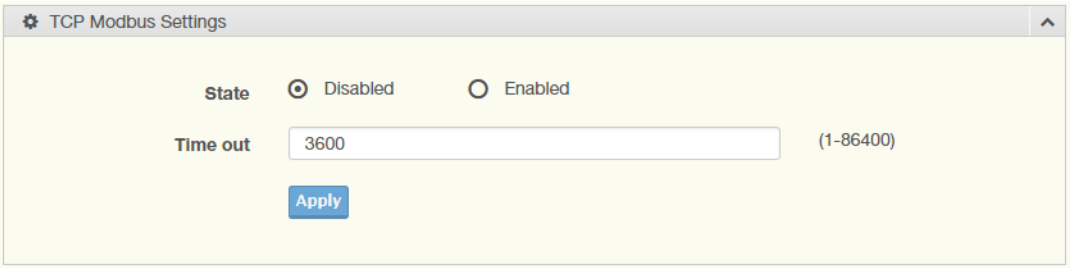


Figure 3.163 Management > TCP Modbus > TCP Modbus Settings

The following table describes the items in the previous figure.

Item	Description
State	Click **Disabled** or **Enabled** to set the TCP Modbus state.
Time out	Enter the value (1 to 86400) to define the timeout period between transport time.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **TCP Modbus Status** settings are informational only: TCP Modbus status and TCP Modbus time out.

Figure 3.164 Management > TCP Modbus > TCP Modbus Settings

3.11.4 DHCP Server

The Dynamic Host Configuration Protocol (DHCP) is a network protocol enabling a server to automatically assign an IP address to a computer from a defined range of numbers configured for a given network.

3.11.4.1 Status Settings

The Status Settings page allows you to configure the DHCP server mode (enabled or disabled).

To access this page, click **Management** > **DHCP Server** > **Status Settings**.

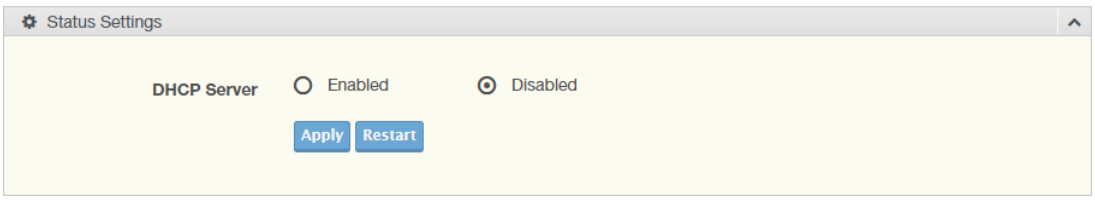


Figure 3.165 Management > DHCP Server > Status Settings

The following table describes the items in the previous figure.

Item	Description
DHCP Server	Select **Enable** or **Disable** to designate the DHCP server function type. When a new DHCP server mode is selected, the switch requires a system restart for the new mode to take effect.
Apply	Click **Apply** to save the values and update the screen.
Restart	Click **Restart** to have the switch perform a system restart function. In the event that the IP settings are changed, the DHCP server must be restarted for the IP settings to take effect.

The ensuing table for **Status Information** settings are informational only: DHCP Server Service.

Figure 3.166 Management > DHCP Server > Status Settings

3.11.4.2 Global Settings

The Global Settings page allows you to configure the global settings for the DHCP function.

To access this page, click **Management** > **DHCP Server** > **Global Settings**.

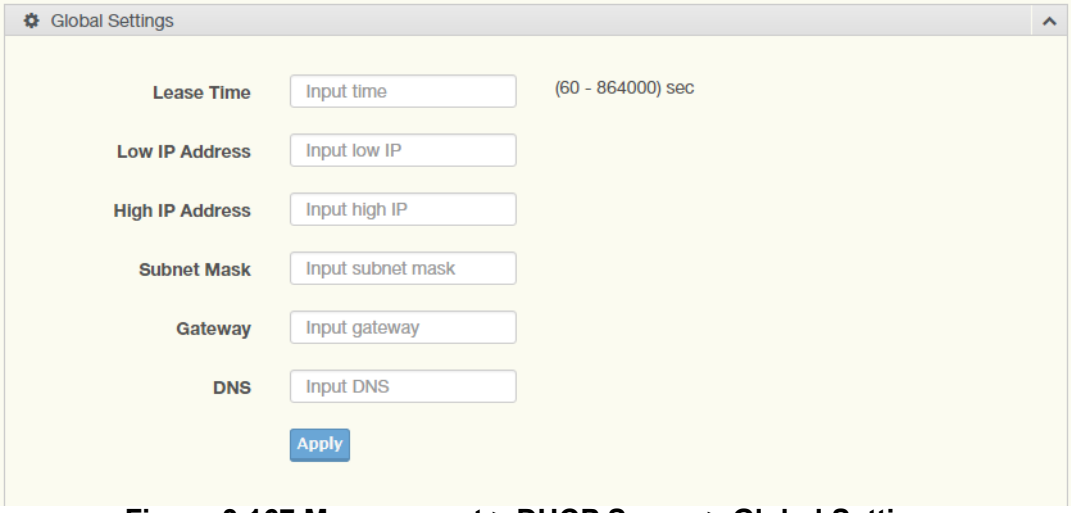


Figure 3.167 Management > DHCP Server > Global Settings

The following table describes the items in the previous figure.

Item	Description
Lease Time	Type in the value designating the lease time (60 - 864000) in seconds for each setting lease.
Low IP Address	Type in the value designating the lowest range in the IP address pool.
High IP Address	Type in the value designating the highest range in the IP address pool.
Subnet Mask	Type in the value designating the subnet mask for the IP address pool.
Gateway	Type in the value designating the gateway for the IP address pool.
DNS	Type in the value designating the DNS for the IP address pool.
Apply	Click **Apply** to save the values and update the screen.

To access this page, click **Management > DHCP Server > Global Settings**.
The following figure displays the **Global Information** settings.

Figure 3.168 Management > DHCP Server > Global Settings

3.11.4.3 Port Settings

The Port Settings page allows you to configure selected ports for the DHCP function.
To access this page, click **Management** > **DHCP Server** > **Port Settings**.

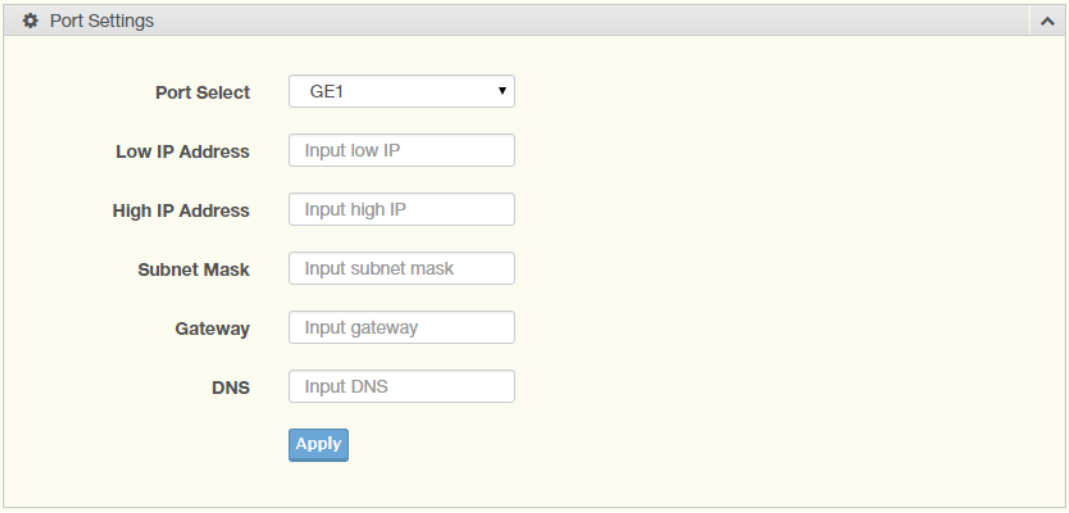


Figure 3.169 Management > DHCP Server > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Click the drop-down menu to select a pre-defined port to configure. The sub options are designated for the selected port.
Low IP Address	Type in the value designating the lowest range in the IP address pool.

The ensuing table for **Port Information** settings are informational only: Port, Low IP Address, High IP Address, Subnet Mask, Gateway, and DNS. In Modify, click **Edit** to modify the port entry or **Clear** to restore the default settings.

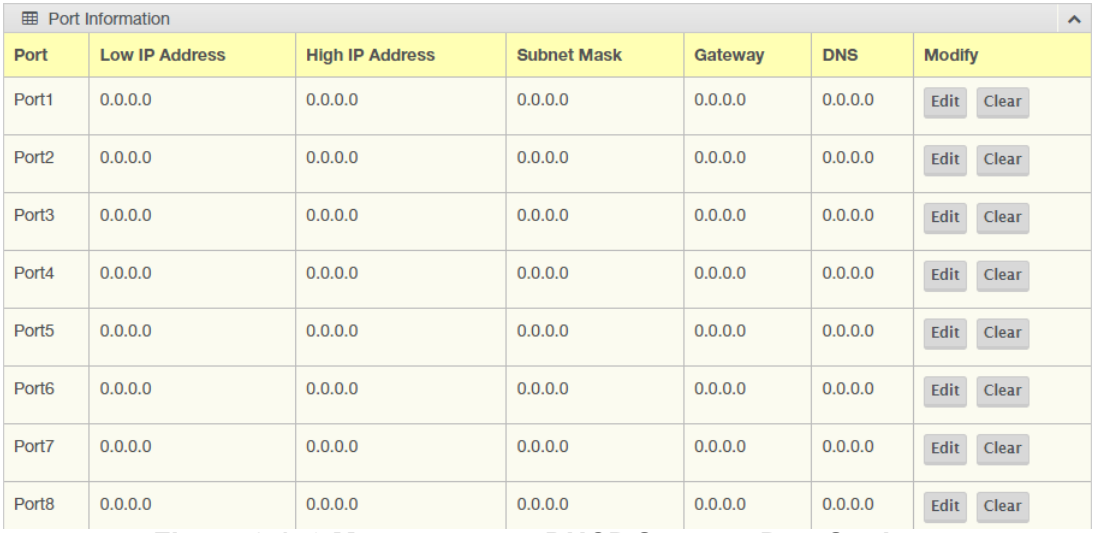


Figure 3.170 Management > DHCP Server > Port Settings

3.11.4.4 VLAN Settings

The device supports clients on both physical and virtual LANs (VLANS). Through the DHCP server function, the device can assign IP configurations for the nodes on the same network.

To access this page, click **Management** > **DHCP Server** > **VLAN Settings**.

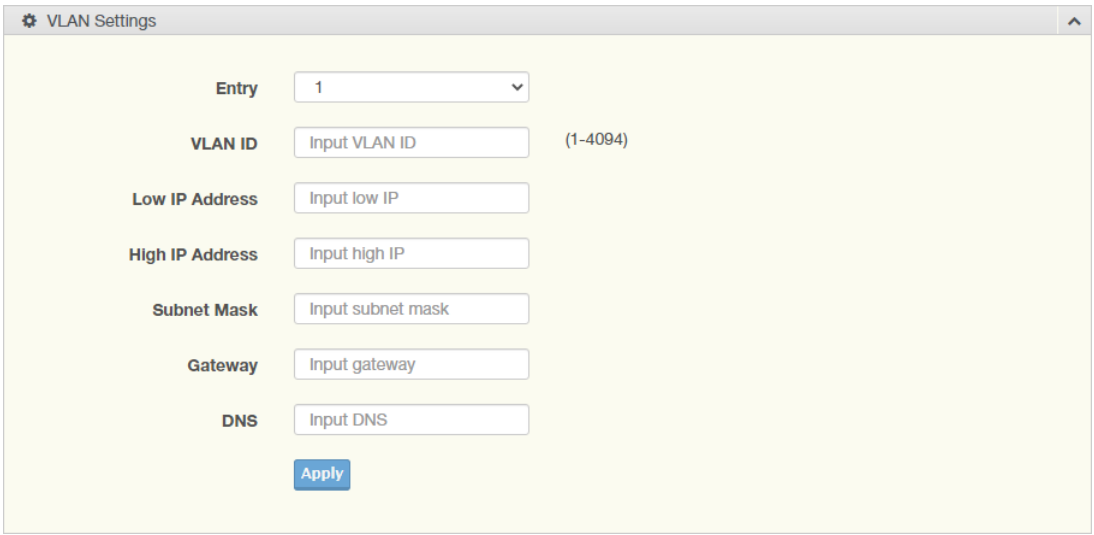


Figure 3.171 Management > DHCP Server > VLAN Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Click the drop-down menu to select a pre-defined port to configure. The sub options are designated for the selected port.
Low IP Address	Type in the value designating the lowest range in the IP address pool.

The ensuing table for **Entry Information** settings are informational only: Entry, Information Name and Information Value. In Modify, click **Edit** to change entry or **Clear** to reset all information.

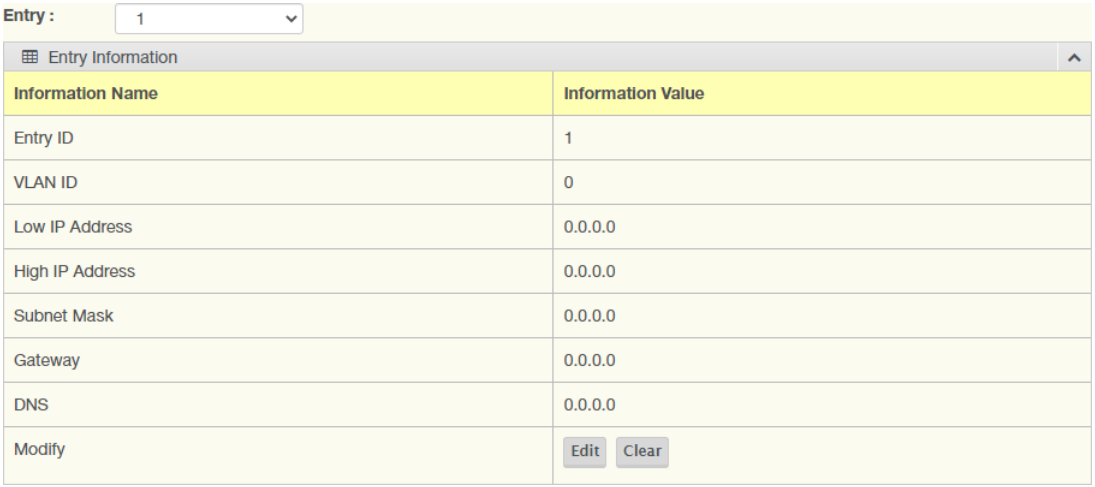


Figure 3.172 Management > DHCP Server > VLAN Settings

3.11.4.5 Option 82 Settings

The Option 82 Settings, also known as the DHCP relay agent information option, provide information about the network location of a DHCP client. In turn, the DHCP server uses the information to implement IP addresses or other parameters for the client.

To access this page, click **Management** > **DHCP Server** > **Option 82 Settings**.

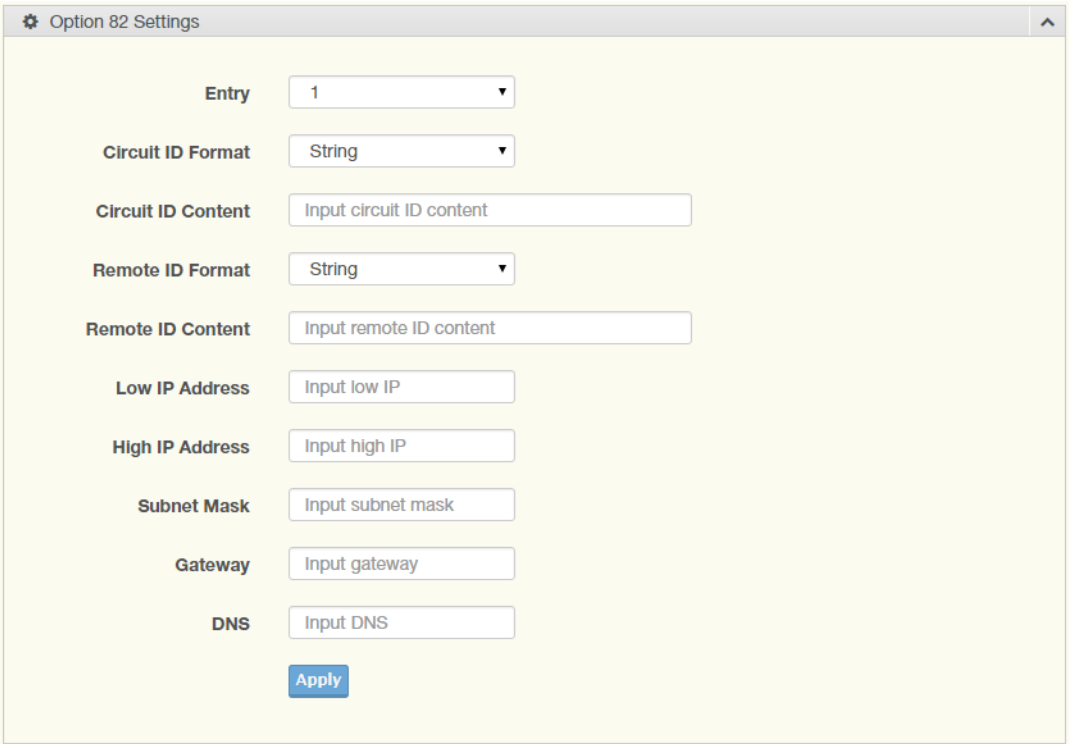


Figure 3.173 Management > DHCP Server > Option 82 Settings

The following table describes the items in the previous figure.

Item	Description
Entry	Click the drop-down menu to select an entry for the Option 82 setting.

Item	Description
Circuit ID Format	Click the drop-down menu to select the format of the circuit ID: string or hex.
Circuit ID Content	Enter the circuit ID string on the switch on which the request was received.
Remote ID Format	Click the drop-down menu to select the format of the remote ID: string or hex.
Remote ID Content	Enter the remote ID string of the host.
Low IP Address	Type in the value designating the lowest range in the IP address pool.
High IP Address	Type in the value designating the highest range in the IP address pool.
Subnet Mask	Type in the value designating the subnet mask for the IP address pool.
Gateway	Type in the value designating the gateway for the IP address pool.
DNS	Type in the value designating the DNS for the IP address pool.
Apply	Click **Apply** to save the values and update the screen.

To access this page, click **Management > DHCP Server > Option 82 Settings**.

The following figure displays the **Entry Information** settings.

Figure 3.174 Management > DHCP Server > Option 82 Settings

3.11.4.6 Client MAC Settings

To access this page, click **Management** > **DHCP Server** > **Client MAC Settings**.

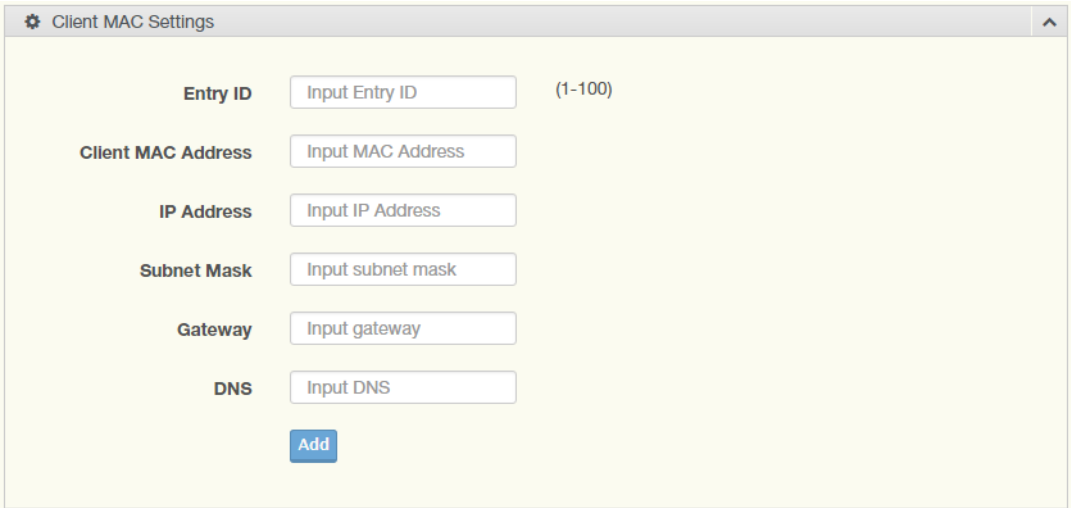


Figure 3.175 Management > DHCP Server > Client MAC Settings

The following table describes the items in the previous figure.

Item	Description
Entry ID	Type in the value designating the entry ID.
Client MAC Address	Enter the MAC address for DHCP server.
IP Address	Enter a value to specify the IP address of the interface.
Subnet Mask	Enter a value to specify the IP subnet mask for the interface.
Gateway	Enter a value to specify the gateway for the interface.
DNS	Enter a value to specify the DNS server for the interface.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Client MAC Information** settings are informational only: Entry ID, Client MAC Address, IP Address, Subnet Mask and Modify (Click **Detail** to display the detail information of desired entry id or **Delete** to delete the desired entry id).

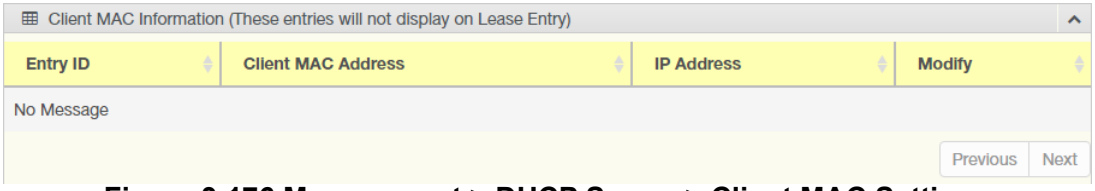


Figure 3.176 Management > DHCP Server > Client MAC Settings

3.11.4.7 Lease Entry

To access this page, click **Management** > **DHCP Server** > **Lease Entry**.

The following figure displays the **Lease entry Table s**ettings.

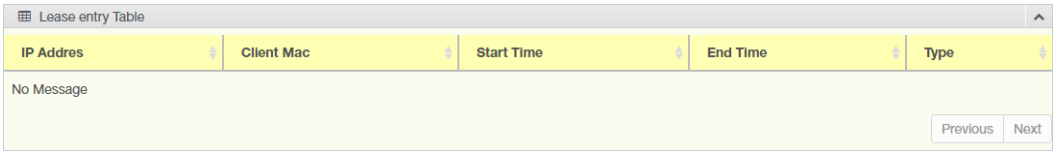


Figure 3.177 Management > DHCP Server > Lease Entry

3.12 Diagnostics

Through the Diagnostics function configuration of settings for the switch diagnostics is available.

3.12.1 Cable Diagnostics

The Cable Diagnostics page allows you to select the port for applying a copper test.

To access this page, click **Diagnostics** > **Cable Diagnostics**.

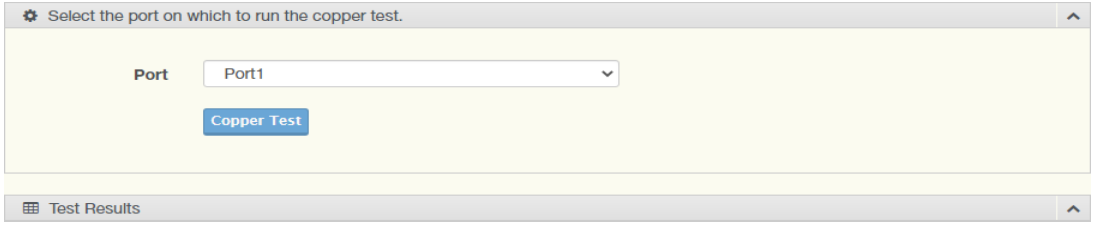


Figure 3.178 Diagnostics > Cable Diagnostics

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select a pre-defined port for diagnostic testing. Giga ports are displayed with a channel A to D designation.
Copper Test	Click **Copper Test** to display the test result for the selected port.

The ensuing table for **Test Result** settings are informational only: Port, Channel A, Cable Length A, Channel B, Cable Length B, Channel C, Cable Length C, Channel D and Cable Length D.

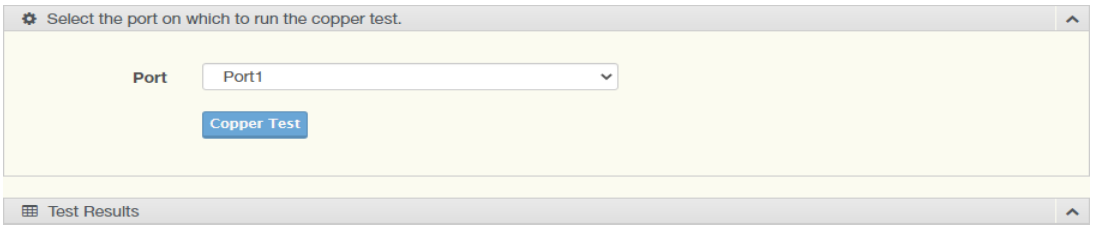


Figure 3.179 Diagnostics > Cable Diagnostics

3.12.2 Ping Test

The Ping Test page allows you to configure the test log page.

To access this page, click **Diagnostics** > **Ping Test**.

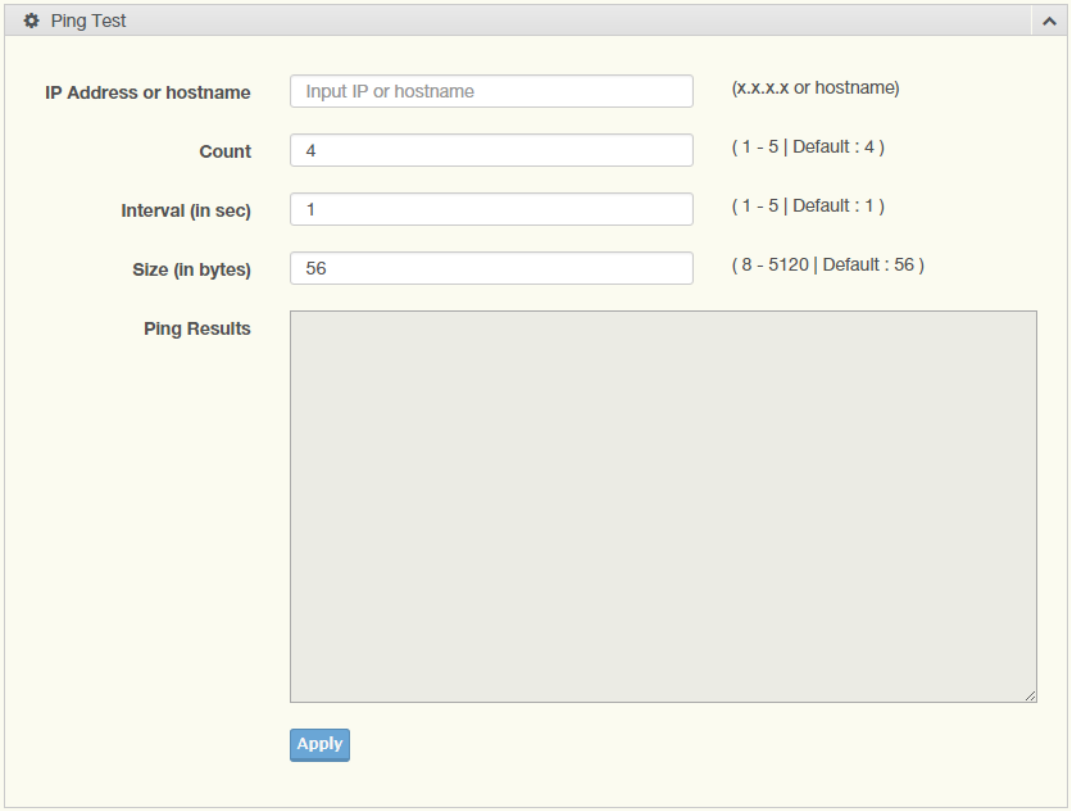


Figure 3.180 Diagnostics > Ping Test

The following table describes the items in the previous figure.

Item	Description
IP Address	Enter the IP address or host name of the station to ping. The initial value is blank. The IP Address or host name you enter is not retained across a power cycle. Host names are composed of series of labels concatenated with periods. Each label must be between 1 and 63 characters long, maximum of 64 characters.
Count	Enter the number of echo requests to send. The default value is 4. The value ranges from 1 to 5. The count entered is not retained across a power cycle.
Interval (in sec)	Enter the interval between ping packets in seconds. The default value is 1. The value ranges from 1 to 5. The interval entered is not retained across a power cycle.
Size (in bytes)	Enter the size of ping packet. The default value is 56. The value ranges from 8 to 5120. The size entered is not retained across a power cycle.
Ping Results	Display the ping reply format.
Apply	Click **Apply** to display ping result for the IP address.

3.12.3 IPv6 Ping Test

The IPv6 Ping Test page allows you to configure the Ping Test for IPv6.

To access this page, click **Diagnostics** > **IPv6 Ping Test**.

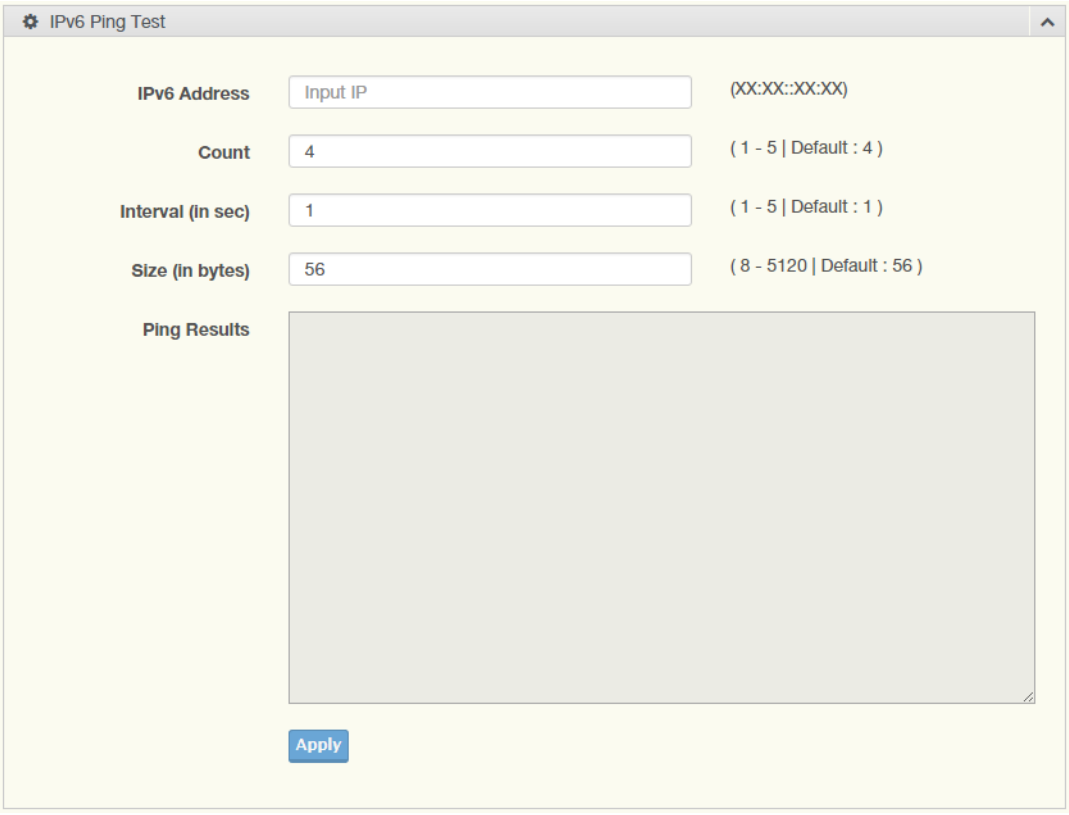


Figure 3.181 Diagnostics > IPv6 Ping Test

The following table describes the items in the previous figure.

Item	Description
IPv6 Address	Enter the IP address or host name of the station you want the switch to ping. The initial value is blank. The IP Address or host name you enter is not retained across a power cycle. Host names are composed of series of labels concatenated with dots. Each label must be between 1 and 63 characters long, and the entire hostname has a maximum of 64 characters.
Count	Enter the number of echo requests you want to send. The default value is 4. The value ranges from 1 to 5. The count you enter is not retained across a power cycle.
Interval (in sec)	Enter the interval between ping packets in seconds. The default value is 1. The value ranges from 1 to 5. The interval you enter is not retained across a power cycle.
Size (in bytes)	Enter the size of ping packet. The default value is 56. The value ranges from 8 to 5120. The size you enter is not retained across a power cycle.
Ping Results	Display the reply format of ping. PING 2222::777 (2222::777): 56 data bytes --- 2222::777 ping statistics --- 4 packets transmitted, 0 packets received, 100% packet loss Or PING 2222::717 (2222::717): 56 data bytes 64 bytes from 2222::717: icmp6_seq=0 ttl=128 time=10.0 ms 64 bytes from 2222::717: icmp6_seq=1 ttl=128 time=0.0 ms 64 bytes from 2222::717: icmp6_seq=2 ttl=128 time=0.0 ms 64 bytes from 2222::717: icmp6_seq=3 ttl=128 time=0.0 ms --- 2222::717 ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.0/2.5/10.0 ms
Apply	Click **Apply** to display ping result for the IP address.

3.12.4 System Log

3.12.4.1 Logging Service

The Logging Service page allows you to setup the logging services feature for the system log.

To access this page, click **Diagnostics** > **System Log** > **Logging Service**.

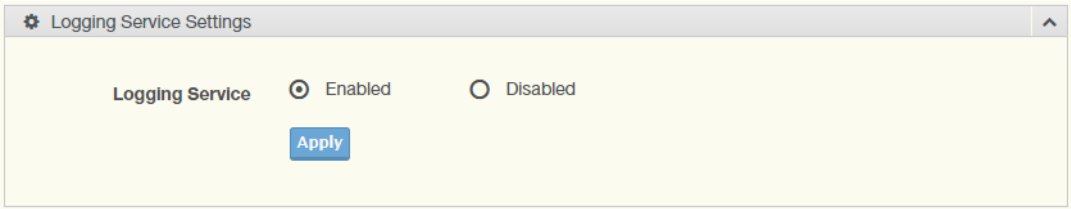


Figure 3.182 Diagnostics > System Log > Logging Service

The following table describes the items in the previous figure.

Item	Description
Logging Service	Click Enabled or Disabled to set the Logging Service status.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Logging Information** settings are informational only: Logging Service.

Figure 3.183 Diagnostics > System Log > Logging Service

3.12.4.2 Local Logging

The Local Logging page allows you to designate a local target when the severity criteria is reached.

To access this page, click **Diagnostics** > **System Log** > **Local Logging**.

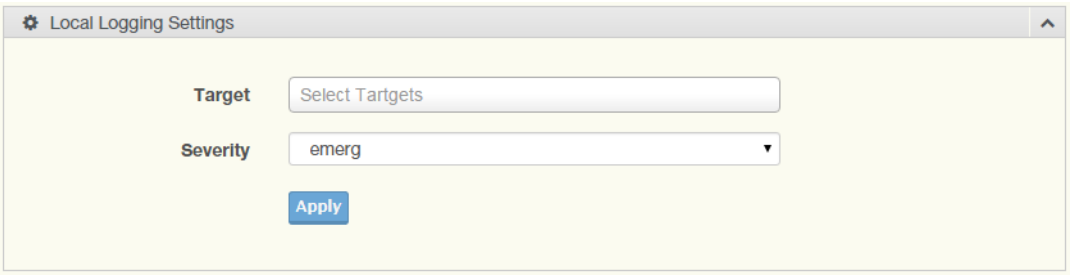


Figure 3.184 Diagnostics > System Log > Local Logging

The following table describes the items in the previous figure.

Item	Description
Target	Enter the local logging target.
Severity	Click the drop-down menu to select the severity level for local log messages. The level options are: ■ emerg: Indicates system is unusable. It is the highest level of severity ■ alert: Indicates action must be taken immediately ■ crit: Indicates critical conditions ■ error: Indicates error conditions ■ warning: Indicates warning conditions ■ notice: Indicates normal but significant conditions ■ info: Indicates informational messages ■ debug: Indicates debug-level messages
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Local Logging Settings Status** settings are informational only: Status, Target, Severity and **Delete** (click to delete the desired target).

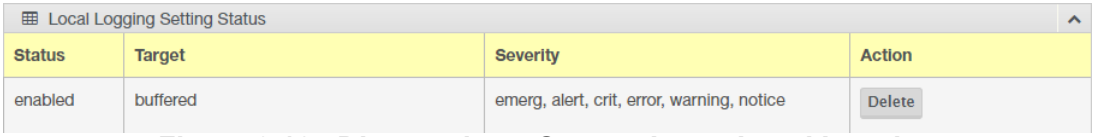


Figure 3.185 Diagnostics > System Log > Local Logging

3.12.4.3 System Log Server

The System Log Server page allows you to configure the log server.

To access this page, click **Diagnostics** > **System Log** > **System Log Server**.

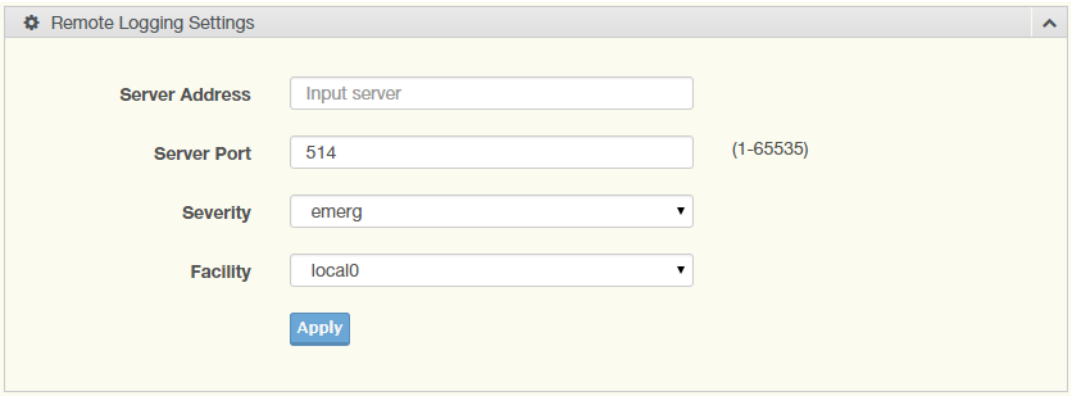


Figure 3.186 Diagnostics > System Log > System Log Server

The following table describes the items in the previous figure.

Item	Description
Server Address	Enter the IP address of the log server.
Server Port	Enter the Udp port number of the log server.
Severity	Click the drop-down menu to select the severity level for local log messages. The default is emerg. The level options are: ■ emerg: Indicates system is unusable. It is the highest level of severity ■ alert: Indicates action must be taken immediately ■ crit: Indicates critical conditions ■ error: Indicates error conditions ■ warning: Indicates warning conditions ■ notice: Indicates normal but significant conditions ■ info: Indicates informational messages ■ debug: Indicates debug-level messages
Facility	Click the drop-down menu to select facility to which the message refers.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Remote Logging Setting Status** settings are informational only: Status, Server Info, Severity, Facility and **Delete** (click to delete the desired server address).

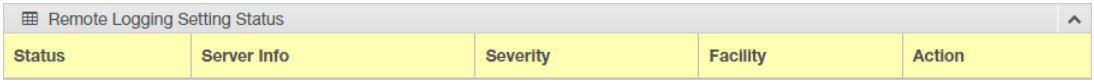


Figure 3.187 Diagnostics > System Log > System Log Server

3.13 Tools

3.13.1 IXM

The IXM tool is an industrial Ethernet switch solution to help the users deploy industrial Ethernet switch hardware by allowing users with multiple, managed Ethernet switches in the field to eliminate the need to individually connect to each device to configure it.

To access this page, click **Tools** > **IXM**.

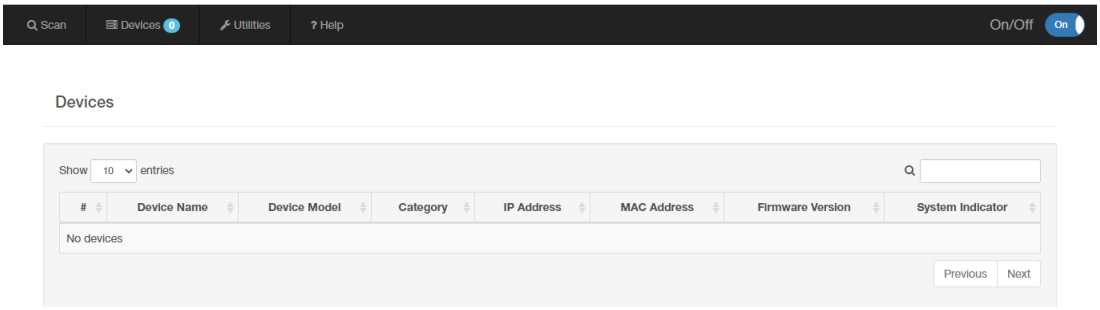


Figure 3.188 Tools > IXM

The following table describes the items in the previous figure.

Item	Description
Search Field	Enter criteria to search the IXM information.
#	Displays the reference to the device number.
Device Name	Displays the device name.
Device Model	Displays the device model type.
Category	Displays the device's category type.
IP Address	Displays the device's IP address.
MAC Address	Displays the device's IP MAC address.
Firmware Version	Displays the device's firmware version.
System Indicator	Click to view the selected device configuration information.
Previous	Click **Previous** to back to previous page.
Next	Click **Next** to go to next page.

3.13.2 Backup Manager

The Backup Manager page allows you to configure a remote TFTP sever or host file system in order to backup the firmware image or configuration file.

To access this page, click **Tools** > **Backup Manager**.

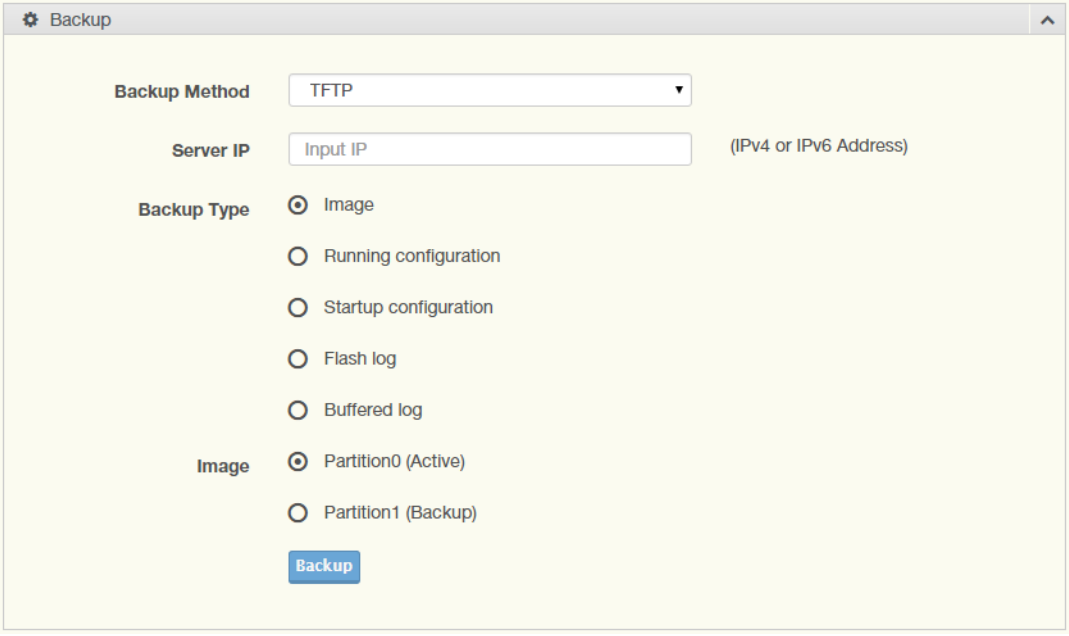


Figure 3.189 Tools > Backup Manager

The following table describes the items in the previous figure.

Item	Description
Backup Method	Click the drop-down menu to select the backup method: TFTP or HTTP.
Server IP	Enter the IP address of the backup server.
Backup Type	Click a type to define the backup method: image: running configuration, startup configuration, flash log, or buffered log.
Image	Click the format for the image type: 7710E_2C_1_00_13.bix (Active) or vmlinux.bix (backup).
Backup	Click **Backup** to backup the settings.

3.13.3 Upgrade Manager

The Upgrade Manager page allows you to configure a remote TFTP sever or host file system in order to upload firmware upgrade images or configuration files.

To access this page, click **Tools** > **Upgrade Manager**.

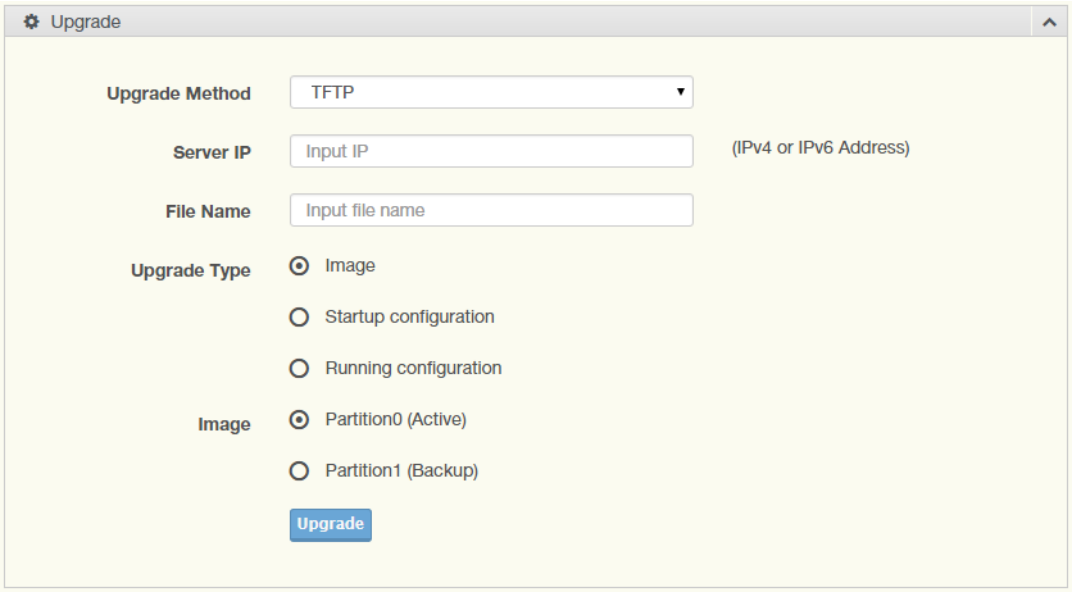


Figure 3.190 Tools > Upgrade Manager

The following table describes the items in the previous figure.

Item	Description
Upgrade Method	Click the drop-down menu to select the upgrade method: TFTP or HTTP.
Server IP	Enter the IP address of the upgrade server.
File Name	Enter the file name of the new firmware version.
Upgrade Type	Click a type to define the upgrade method: image, startup configuration, or running configuration.
Image	Click the format for the image type: 7710E_2C_1_00_13.bix (Active) or vmlinux.bix (backup).
Upgrade	Click **Upgrade** to upgrade to the current version.

3.13.4 Dual Image

The Dual Image page allows you to setup an active and backup partitions for firmware image redundancy.

To access this page, click **Tools** > **Dual Image**.

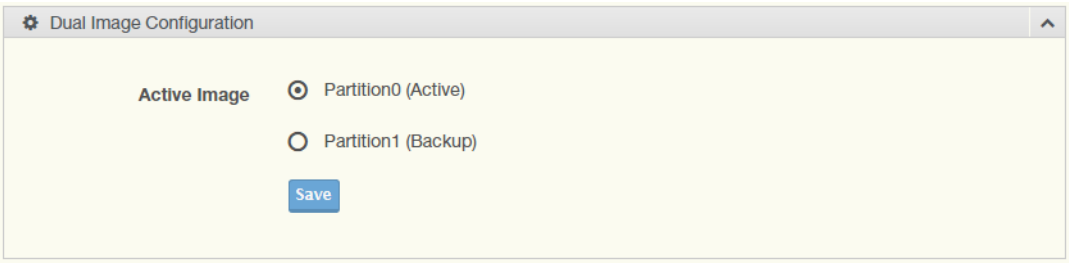


Figure 3.191 Tools > Dual Image

The following table describes the items in the previous figure.

Item	Description
Active Image	Click the format for the image type: Partition0 (Active) or Partition1 (backup).
Save	Click **Save** to save and keep the new settings.

The ensuing table for **Image Information 0/1** settings are informational only: Flash Partition, Image Name, Image Size and Created Time.

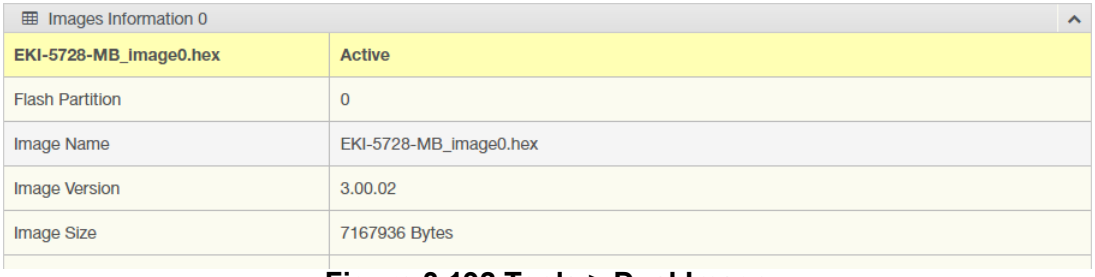


Figure 3.192 Tools > Dual Image

3.13.5 Save Configuration

To access this page, click **Tools** > **Save Configuration**.

Click **Save Configuration to FLASH** to have configuration changes you have made to be saved across a system reboot. All changes submitted since the previous save or system reboot will be retained by the switch.

3.13.6 User Account

The User Account page allows you to setup a user and the related parameters.

To access this page, click **Tools** > **User Account**.

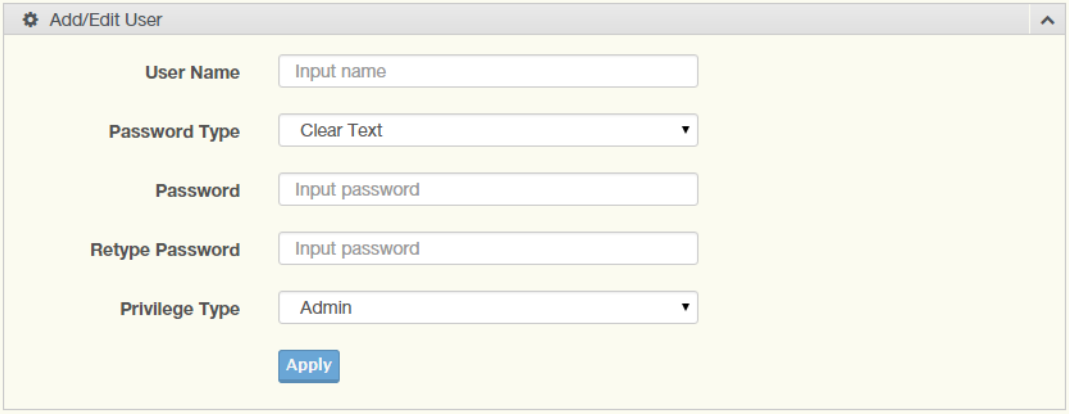


Figure 3.193 Tools > User Account

The following table describes the items in the previous figure.

Item	Description
User Name	Enter the name of the new user entry.
Password Type	Click the drop-down menu to define the type of password: **Clear Text** or **No Password**.
Password	Enter the character set for the define password type.
Retype Password	Retype the password entry to confirm the profile password.
Privilege Type	Click the drop-down menu to designate privilege authority for the user entry: **Admin** or **User**.
Apply	Click **Apply** to create a new user account.

The ensuing table for **Local Users** settings are informational only: User Name, Password Type, Privilege Type and **Delete** (click to delete the desired user account).

3.13.7 Wrong Password

The Wrong Password feature allows you to set the policy to manage wrong password entry attempts.

To access this page, click **Tools** > **Wrong Password**.

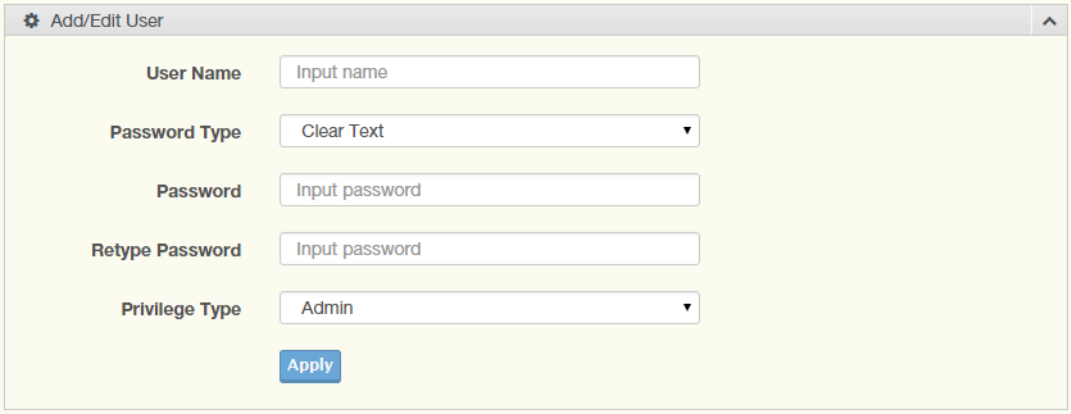


Figure 3.194 Tools > Wrong Password

The following table describes the items in the previous figure.

Item	Description
State	Click to enable (default) or disable the feature.
Retry Time	Enter the threshold for the number of retry attempts (3 - 15).
Block Time	Enter the period of time in minutes (5 - 30) an account is locked out after the retry attempt threshold is surpassed.
Apply	Click **Apply** to create a new user account.

The ensuing table for **Wrong Password Information** is informational only: Information Name and Information Values.

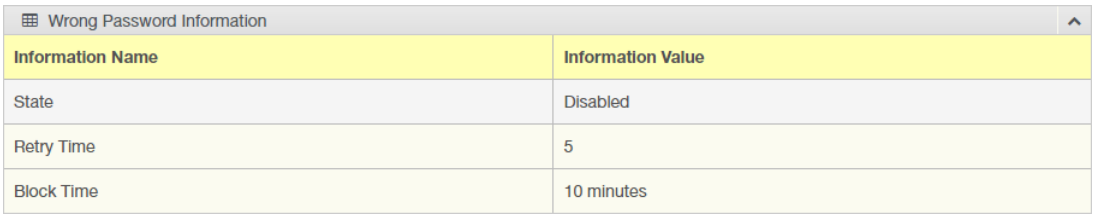


Figure 3.195 Tools > Wrong Password

3.13.8 Reset System

To access this page, click **Tools** > **Reset System**.

Click **Restore** to have all configuration parameters reset to their factory default values. All changes that have been made will be lost, even if you have issued a save.

Reset settings take effect after a system reboot.

3.13.9 Reboot Device

To access this page, click **Tools** > **Reboot Device**.

Click **Reboot** to reboot the switch. Any configuration changes you have made since the last time you issued a save will be lost.