EDIMAX
NETWORKING PEOPLE TOGETHER

IGS-5208

User Manual

01-2019 / v1.0

Edimax Technology Co., Ltd.
No. 278, Xinhu 1st Rd., Neihu Dist., Taipei City, Taiwan
Email: support@edimax.com.tw

Edimax Technology Europe B.V.
Fijenhof 2, 5652 AE Eindhoven, The Netherlands
Email: support@edimax.nl

Edimax Computer Company
3444 De La Cruz Blvd., Santa Clara, CA 95054, USA
Live Tech Support: 1(800) 652-6776
Email: support@edimax.com

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Table of Contents

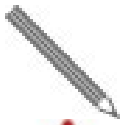
Intended Readers

This manual provides information regarding to all the aspects and functions needed to install, configure, use, and maintain the product you've purchased.

This manual is intended for technicians who are familiar with in-depth concepts of networking management and terminologies.

Icons for Note, Caution, and Warning

To install, configure, use, and maintain this product properly, please pay attention when you see these icons in this manual:



A **Note** icon indicates important information which will guide you to use this product properly.

A **Caution** icon indicates either a potential for hardware damage or data loss, including information that will guide you to avoid these situations.

A **Warning** icon indicates potentials for property damage and personal injury.

If you have any questions, please contact our technical support via email: service@edimax.com.tw.

I. Product Overview

This section will give you an overview of this product, including its feature functions and hardware/software specifications.

- **Product Brief Description**
- **Product Specification**
- **Hardware Description**
- **Hardware Installation**

I-1 Product Brief Description

Introduction

This switch is a DIN Rail type industrial Gigabit managed Switch is designed with eight 10/100/1000M RJ45 ports and two Gigabit SFP slots for highly critical applications such as real time IP video surveillance, WiMAX systems and Wireless APs.

Ethernet Ring Protection Switching (ERPSv2)

Ring network topology ensures the reliability of the connections among all the switches in the network. This switch supports ERPSv2 with easy to set up user interface, which allows it to recover from network disconnection in less than 20ms with 250 switches connected in a ring network topology while transmitting/receiving data at full network speed. Also, this switch supports multiple ERPS instances, allowing different VLANs have their own ERPS instances.

USB Port for Save/Restore Configuration & System Log/Firmware Storage

This switch comes with a USB port for connecting a USB storage device to the industrial switch. Configuration files, switch system log and firmware can be stored in the USB storage device for the switch to access. When a USB storage device is connected to the switch, it will load the configuration file in the storage device and apply all the settings, saving on-site installation time and effort.

Redundant Power Inputs & Embedded Protecting Circuit

This switch provides two power inputs that can be connected simultaneously to live DC power source. If one of the power input fails, the other live source acts as a backup to automatically support the switch's power needs without compromising network service qualities. Also, it supports automatic protection switching and load balance, while its embedded protecting circuit can protect your system from over input/output voltages and rectifier malfunctions.

Outstanding Management and Enhanced Security

This switch provides various network control and security features to ensure the reliable and secure network connection. To optimize the industrial network environment the switch supports advanced network features, such as Tag VLAN, IGMP Snooping, Quality of Service (QoS), Link Aggregation Control Protocol (LACP), Rate Control, etc. The switch can be smartly configured through Web Browser, SNMP Telnet and RS-232 local console with its command like interface. The failure notifications are sent through e-mail, SNMP trap, Local/Remote system log, multiple event alarm relay.

I-2 Product Specification

Interface	
10/100/1000 Base RJ45 Ports	8
1000Base-X SFP Slot	2
Console Port for CLI Management	1
USB Port	1x USB 2.0 storage for firmware update, configuration backup, restore, boot up and system log

System Performance		
Packet Buffer		12Mbits
MAC Address Table Size		16K
Switching Capacity		20Gbps
Forwarding Rate		14.88Mpps
L2 Features		
Auto-negotiation		•
Auto MDI/MDIX		•
Flow Control (duplex)	802.3x (Full)	•
	Back-Pressure (Half)	•
Spanning Tree	IEEE 802.1D (STP)	•
	IEEE 802.1w (RSTP)	•
	IEEE 802.1s (MSTP)	•
VLAN	VLAN Group	4K
	Tagged Based	•
	Port-based	•
	Voice VLAN	•
Link Aggregation	IEEE 802.3ad with LACP	•
IGMP Snooping	IGMP Snooping v1/v2/v3	Supports 1023 IGMP groups
	IGMP Static Multicast Addresses	•
	Querier, Immediate Leave	•
Storm Control		•
G.8032 - Ethernet Ring Protection Switching (ERPS)		•
Jumbo Frame Support		9.6KB
QoS Features		
CoS		•
DSCP		•
WRR/SPQ Queuing		•
Security		
Management System User Name/Password Protection		•
IEEE 802.1x Port-based Access Control		•
RADIUS (Authentication, Authorization, Accounting)		•
HTTP & SSL (Secure Web)		•
SSH v2.0 (Secured Telnet Session)		•
Management		
Command Line Interface (CLI)		•
Web Based Management		•
Telnet		•
Firmware Upgrade via HTTP		•

Configuration Download/Upload	•
SNMP (v1/v2c/v3)	•
RMON (1,2,3,&9 groups)	•
DHCP (Client/Relay/Option82)	•
System Event/Error Log	•
NTP/LLDP	•
Port Mirroring	•
Industrial Profiles	Ethernet/IP, Modbus TCP
Mechanical	
Input Power	DC12~48V, Dual Redundant
Power Connection	1 removable 4-contact terminal block
Max. Power Consumption	17W
Dimension (H*W*D)	72.2 x 145 x 113 mm
Weight	0.85KG
LED	**Per unit:** PWR1, PWR2, Fault, Ring Master, Ring State **Ports:** Link/Active with highest speed (Green), low speed (Amber)
Button	1 mulltiple function reset button
Operating Temperature	-40 to 75°C
Storage Temperature	-40 ~ 85°C
Operating Humidity	5~95% (non-condensing)
MTBF	>100,000 Hours
Industrial Standard	
Alarm Contact	1 relay output with current carrying capacity of 1A @ 24 VDC
Reverse Polarity Protection	•
Overload Current Protection	•
Casing	IP30 protection, aluminum alloy case
EMI	FCC Part 15 Subpart B Class A, CE EN 55022 Class A
EMS	IEC61000-4-2 (ESD Level 4), IEC61000-4-3 (RS Level 3) IEC61000-4-4 (EFT Level 4), IEC61000-4-5 (Surge Level 4) IEC61000-4-6 (CS Level 3), IEC61000-4-8 (Magnetic Field Level 4)
Shock	IEC60068-2-27
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
Green	RoHS Compliant
Installation	DIN-Rail mounting or optional wall mounting
Standard	
IEEE 802.3 – 10BaseT	•
IEEE 802.3u – 100BaseTX	•
IEEE 802.3ab – 1000BaseT	•
IEEE 802.3z 1000BaseSX/LX	•
IEEE 802.3x – Flow Control	•
IEEE 802.1Q – VLAN	•
IEEE 802.1p – Class of Service	•
IEEE 802.1D – Spanning Tree	•
IEEE 802.1w – Rapid Spanning Tree	•

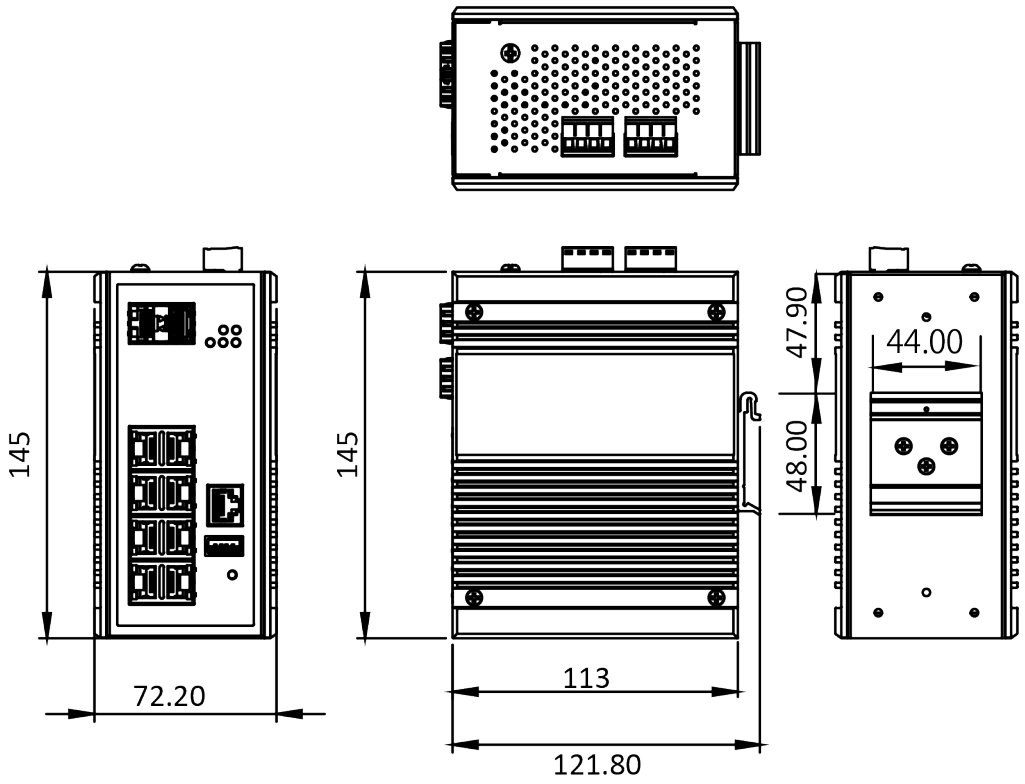
IEEE 802.1s – Multiple Spanning Tree	•
IEEE 802.3ad – Link Aggregation Control Protocol (LACP)	•
IEEE 802.1AB – LLDP (Link Layer Discovery Protocol)	•
IEEE 802.1X – Access Control	•
ITU-T G.8032/Y.1344 - Ethernet Ring Protection Switching (ERPS)	•

I-3. Hardware Description

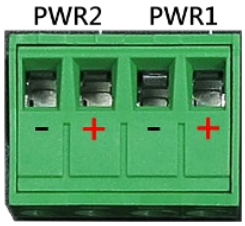
This section mainly describes the hardware of this switch and gives a physical and functional overview on the certain switch.

Dimension

The dimension of this Switch is 145 mm (H) x 72.20 mm (W) x 113 mm (D). The figure down below is the drawing of detail mechanical design:

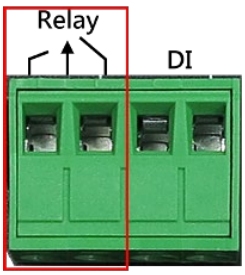


Wiring Power Inputs



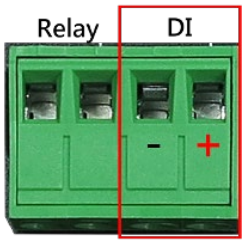
1. Insert the positive and negative wires into the PWR1 (+,-) and PWR2 (+,-) on the 4-contact terminal block connector.
2. 2. Tighten the screws to prevent the wires from loosening.

Wiring Fault Alarm



1. Insert the wires into the left two contacts of the 4-contact terminal block (Fault Alarm Relay).
2. Tighten the screws to prevent the wires from loosening.
3. The relay will detect the power and link failure.
4. Users can connect the relay to an alarm and buzzer so that when the relay forms an open circuit, the users will be notified.

Wiring Digital Inputs



1. Insert the positive and negative wires into the right two contacts (+,-) of the 4-contact terminal block (DI).
2. Tighten the screws to prevent the wires from loosening.
3. The system will detect the voltage go through the DI.
   - +13 to +30V for state "1"
   - -30 to +3V for state "0"
   - Max. input current: 8mA

Double-Secure Power Input Fault Alarm

The power inputs are designed as a "common negative", which implies that the negative input is connected, but "double-secure" is supported to prevent the un-notified failure of power from one of the negative inputs. If one of the negative power input fails, the system will detect it and the system will trigger the event if the users set the fault alarm or event log for powers.

LED Status

LED	Color	Status	Description
PWR1	Green	On	Power is supplied on the power input 1.
		Off	Power is not supplied on the power input 1.
PWR2	Green	On	Power is supplied on the power input 2.
		Off	Power is not supplied on the power input 2.
Fault	Green	On	The system boots up and in normal operation.
		Off	The system is powered off or during booting.
	Red	On	The configured event of failure is triggered.
RM	Green	On	This device has the Ring Master.
		Off	The Ring Master is not on the device.
Ring	Green	On	The Ring protocol is enabled and works normally.
		Flickering	The Ring protocol is enabled, but works abnormally.
		Off	The Ring protocol is disabled.
SFP Slot P9 to P10 (1000M)	Green	On	The 1000Mbps link of the fiber port is active.
		Flickering	Data is transmitted on the fiber port at 1000Mbps.
		Off	The 1000Mbps link of the fiber port is inactive.
LAN Port P1 to P8 (1000M)	Green	On	The 1000Mbps link of the port is active.
		Flickering	Data is transmitted on the port at 1000Mbps.
		Off	The 1000Mbps link of the port is inactive.
LAN Port P1 to P8 (10/100M)	Green	On	The 10/100Mbps link of the port is active.
		Flickering	Data is transmitted on the port at 10/100Mbps.
		Off	The 10/100Mbps link of the port is inactive.

Reset Button

A multifunctional reset button is provided. Use a pointed object such as toothpick or paper clip (straightened) to press the reset button.

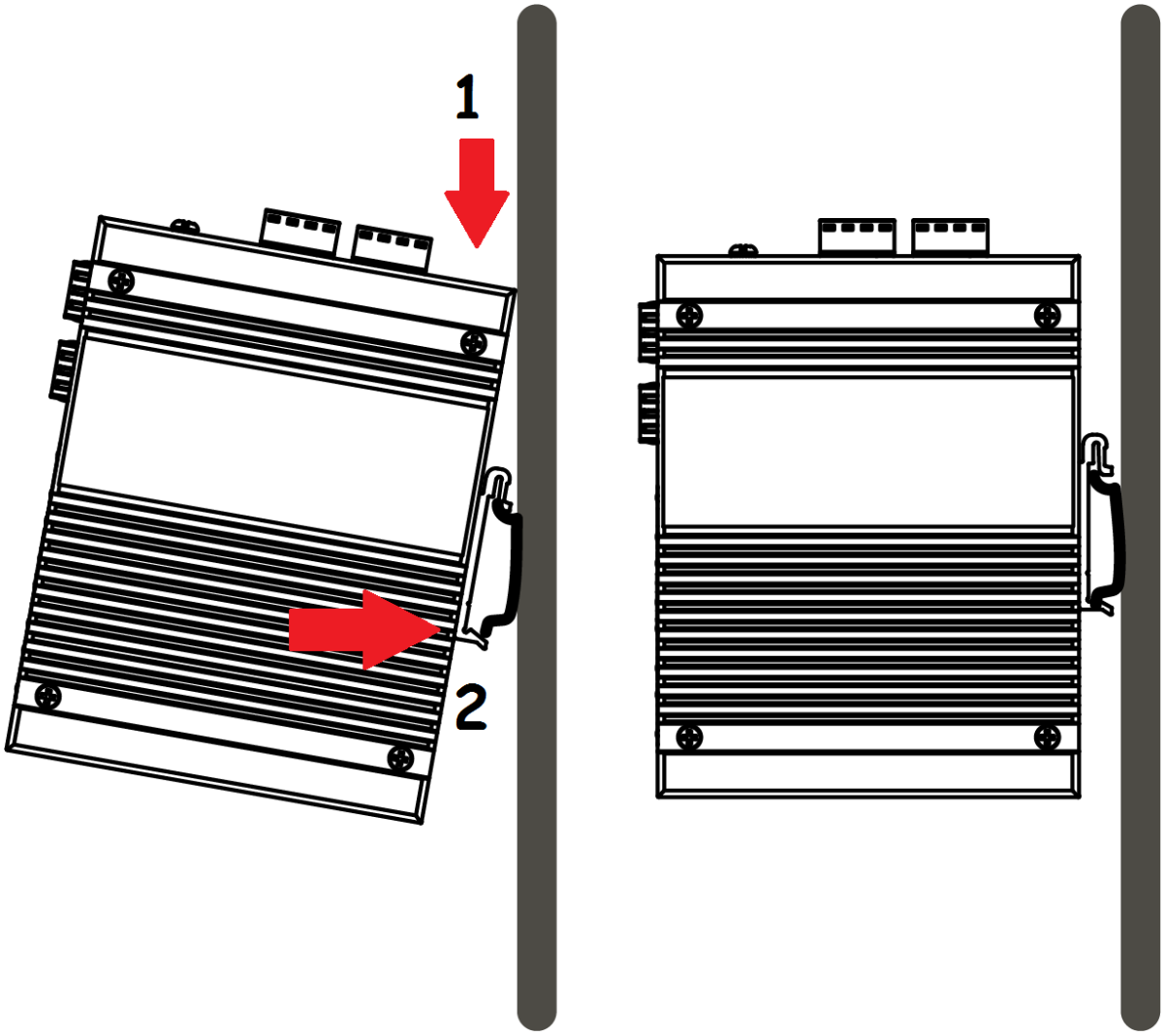
Press Time (Sec)	Action
1	Save the running configuration to the USB device named "running-config".
4	Reboot the system.
More than 7	Reset the system to factory default and reboot it.

I-4. DIN-Rail Mounting

The DIN-Rail clip is already attached on the rear side of the switch supports EN 50022 standard DIN Rail, in the following diagram includes the dimension of EN 50022 DIN Rail.

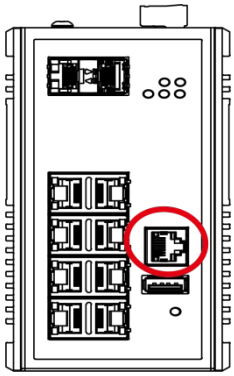
Follow the steps below to mount the switch on the DIN-Rail track.

1. Insert the upper end of the DIN-Rail clip into the back of the DIN-Rail track from its upper side
2. Lightly push the bottom of the DIN-Rail clip into the track.
3. Check if the DIN-Rail clip is tightly attached to the track.
4. To remove the switch from the track, reverse the steps above.



I-5. Console Connection

The Console port is for local management by using a terminal emulator or a computer with terminal emulation software.



- DB9 connector connect to computer COM port
- Baud rate: 115200bps
- 8 data bits, 1 stop bit
- None Priority
- None flow control

I-6. Connecting Cable

The port 1~4 is the copper ports, it requests UTP/STP cable.
The port 5 ~ 6 are the SFP slots, purchase the suitable fiber transceiver from your supplier and connect the fiber cable for the link.

Ethernet cable Request

The wiring cable types for data transmission are as below.

10 Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable, EIA/TIA-568 100-ohm (Max. 100m)

100 Base-TX: 2-pair UTP/STP Cat. 5 cable, EIA/TIA-568 100-ohm (Max. 100m)

1000 Base-T: 4-pair UTP/STP Cat. 5 cable, EIA/TIA-568 100-ohm (Max. 100m)

The wiring cable types for data transmission and power delivery in any speed are Cat. 5 or above.

SFP Installation

While install the SFP transceiver, make sure the SFP type of the 2 ends is the same and the transmission distance, wavelength, fiber cable can meet your request. It is suggested to purchase the SFP transceiver with the switch provider to avoid any incompatible issue.

The way to connect the SFP transceiver is to Plug in SFP fiber transceiver fist. The SFP transceiver has 2 plug for fiber cable, one is TX (transmit), the other is RX (receive). Cross-connect the transmit channel at each end to the receive channel at the opposite end.

The switch is equipped with one dry relay output for port link fails or power fails. This session introduces how to enable the event alarm DIP switch to alert field technician once the failure event is occurred. The new configuration is activated immediately without system reset when DIP SWITCH is changed.

On the bottom side of the switch, there is one 9-Pin DIP SWITCH for alarm control. By inserting the port and power wiring to set up the alarm, the DIP SWITCH of the intended Alarm is switched to “ON”. The relay output will form a short circuit if the alarm occurred.

II. Preparing for Management

This section will guide your how to manage this product via serial console, management web page, and Telnet/SSH interface.

The switch provides *in-band* managements.

In-Band Management: In-band management allows you to manage your switch with a web browser (such as Microsoft IE, Mozilla Firefox, or Google Chrome) as long as your PC and the switch are connected to the same network.

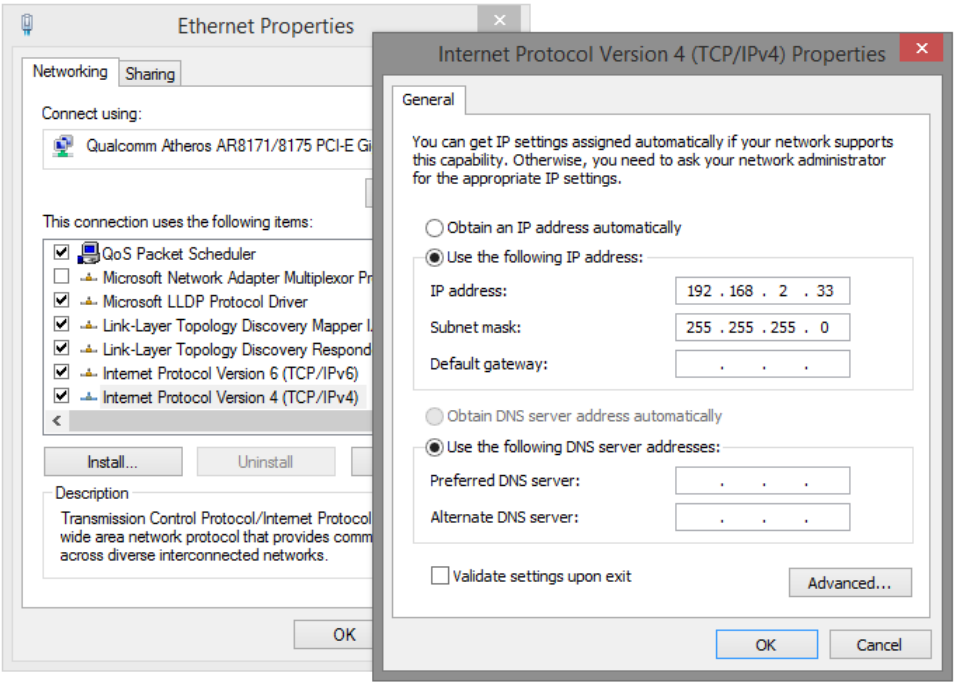
- **Preparation for Web Interface**

II-1. Preparation for Web Interface

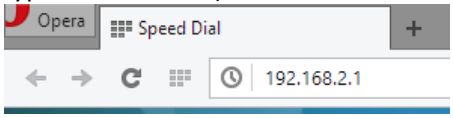
The management web page allows you to use a web browser (such as Microsoft IE, Google Chrome, or Mozilla Firefox) to configure and monitor the switch from anywhere on the network.

Before using the web interface to manage your switch, please verify that your switch and your PC are on the same network. Please follow the steps down below to configure your PC properly:

1. Verify that the network interface card (NIC) of your PC is operational and properly installed, and that your operating system supports TCP/IP protocol.
2. Connect your PC with the switch via an RJ45 cable.
3. The default IP address of the switch is **192.168.2.1**. The switch and your PC should locate within the same IP Subnet. Change your PC's IP address to 192.168.2.X, where X can be any number from 2 to 254. Please make sure that the IP address you've assigned to your PC cannot be the same with the switch.



4. Launch the web browser (IE, Firefox, or Chrome) on your PC.
5. Type **192.168.2.1** (or the IP address of the switch) in the web browser's URL field, and press Enter.



6. The web browser will prompt you to sign in. The default username/password is admin/admin. For more information, please refer to Appendix A: IP Configuration for Your PC.

III. Web Management

As mentioned in *II-1. Preparation for Web Interface*, This switch provides a web-based management interface. You can make all settings and monitor system status with this management web page.

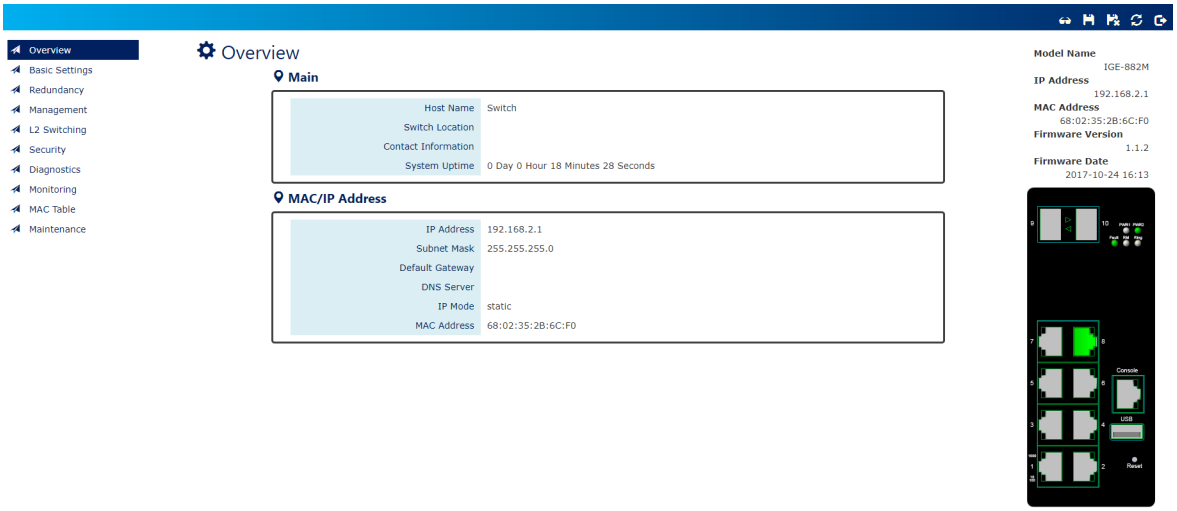
III-1. Web Management - Overview

When you log in, the configuration web page will display current system status.

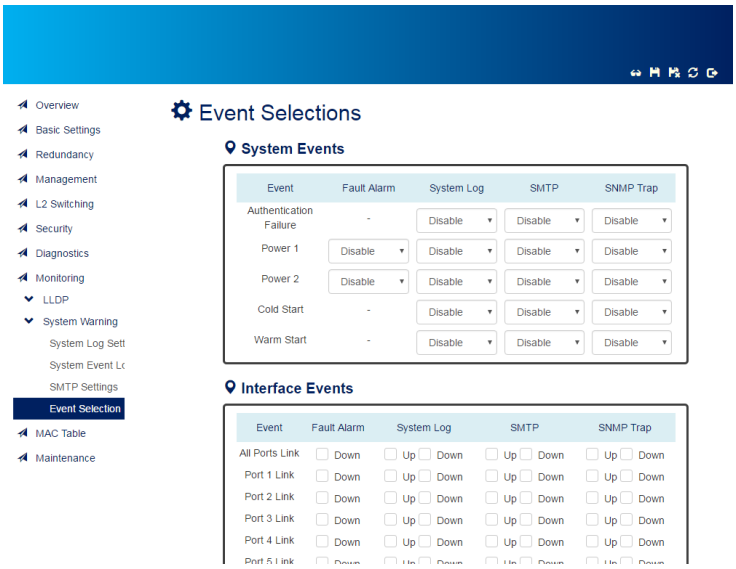
1. Hide/Show Model Information

   When a low-resolution environment is used to configure the system via the web console, the "Model Information" field can be hidden to have a better view.

   Show Model Information:



   Hide Model Information:



2. **Save Configuration**

After configuring, click the icon to save the configurations to the "**startup-config**" file. The configurations are retained in the system until a factory reset default is done.

3. **Restore Factory Default**

Removes the configurations saved in the system. After restoring factory default, all the settings will be set to default values.

4. **Reboot System**

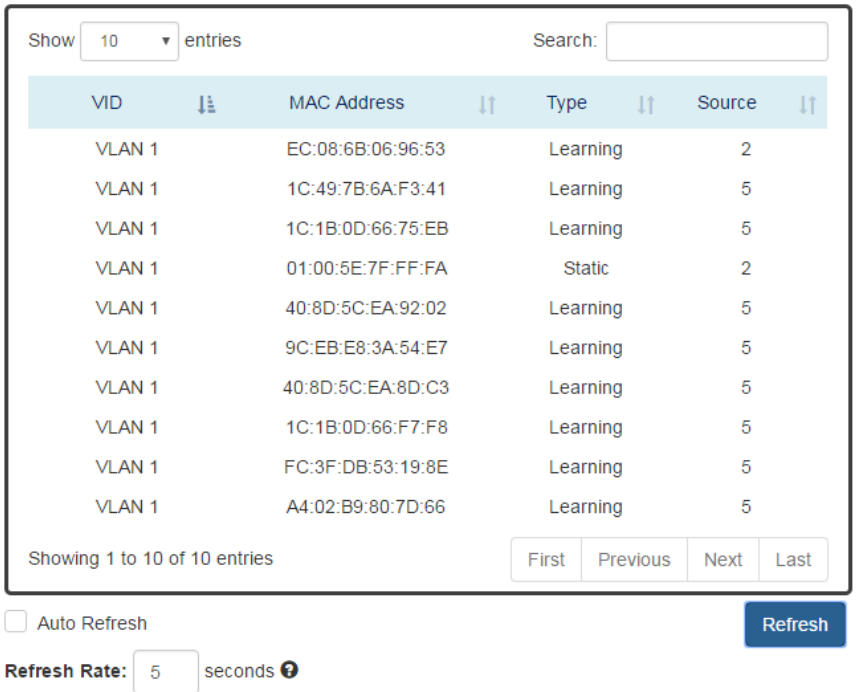
Reboots the device and restarts the system.

5. **System Logout**

This option enables you to sign out from the system. Users have to login again if they want to configure the settings.
The system will **auto-logout** after the "timeout" timer expires. The "timeout" timer is configured in the CLI mode by using the "exec-timeout" command.
The maximum value of the timer in the web console is **30 mins**.

A User-Friendly Data Table

A user-friendly data table is provided on the"**IPv6 Neighbor Table**", "**IGMP Snooping Table**", "**VLAN Table**", "**LLDP Neighbor Table**", and "**MAC Address Table**". The following section details how to use the data table functions to help the users to observe the information easily.
The following example is "**MAC Address Table**".



- Show 10 entries

Users will be able to select a value to display the numberof entries in one page. The following values can be selected - "**10**", "**25**", "**50**", and "**100**" selections. By default, "**10**" is selected.

- Search:

The search option enables you to search a key word in the data. It will search all the columns and identify the data rows that match the search criteria.

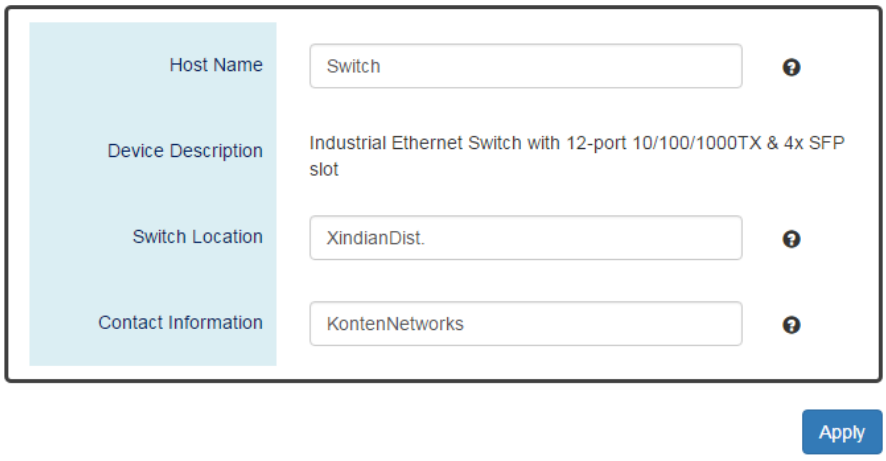
- Showing 1 to 10 of 31 entries

It displays the total number of entries and the current entry number.

- and
  This option orders the field from **smaller to larger** or from **larger to smaller**.
- First | Previous | Next | Last
  Changes to “First”, “Previous”, “Next”, or “Last” page.
  In addition to the above functions, “**Refresh**” and “**Auto Refresh**” function are available for all status page including “**IPv6 Neighbor Table**”, “**RSTP Port Status**”, “**Port Status**”, “**IGMP Snooping Table**”, “**VLAN Table**”, “**Trunking Status**”, “**LLDP Neighbor Table**”, and “**MAC Address Table**”.
- Auto Refresh
  Selecting this checkbox enablesthe “Auto Refresh” function and deselecting the checkbox disables the“Auto Refresh” function.
- **Refresh Rate:** 5 seconds
  The Refresh Rate option is a **global** configurable variable. When the Auto Refresh option is enabled, the status will refresh automatically based on the Refresh Rate interval.
  The range of theRefresh Rate is **from 5 to 300** second(s).
  The default Refresh Rate is **5** seconds.
- Refresh (Refresh Button)
  You can click the **“Refresh”** button to manually refresh the status.

III-2. Web Management - System

System Information



For more information, move the mouse over the icon in the system.

- **Host Name**
  It is useful to identify the difference between the switches, for example: CoreSwitch01.
  The **max. length** for the Host Name is **32 characters**.
  Note: #, \, ', ", ? are **invalid** characters.

- **Device Description**
  The Device Description is fixed and defined by the system.
  It contains the copper port number, fiber port number, and PoE information (if supported).

- **Switch Location**
  It is useful to find the location of the switches, for example: Area01.
  The **max. length** for the Switch Location is **32 characters**.
  Note: #, \, ', ", ? are **invalid** characters.

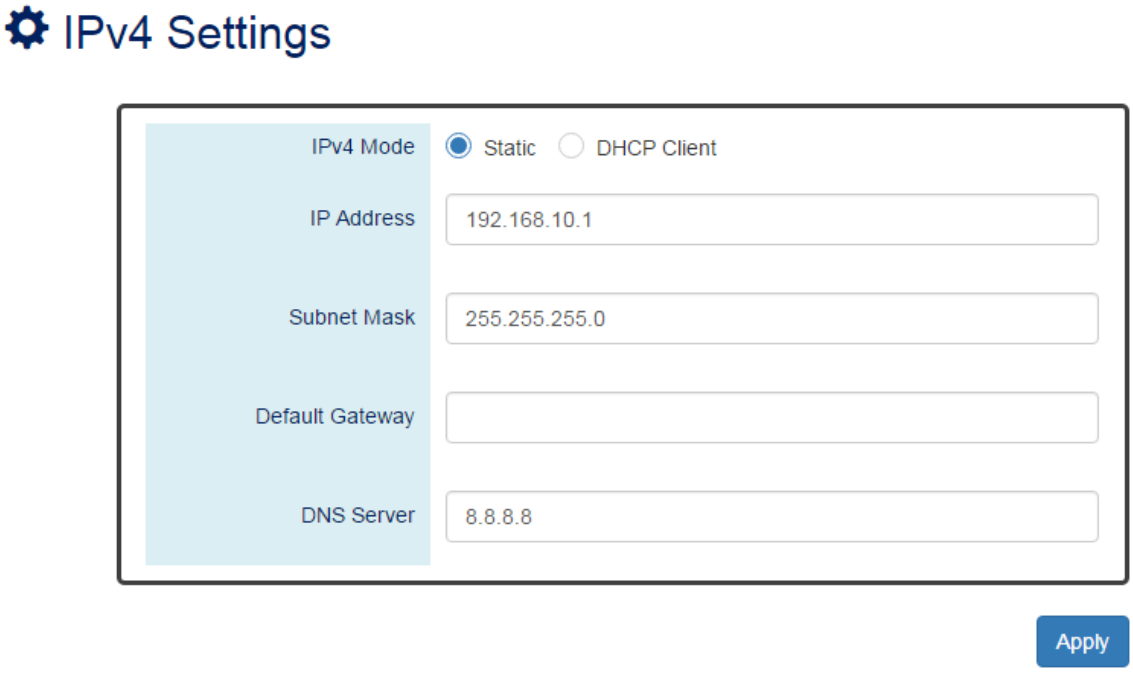
- **Contact Information**
  Records the information of the person responsible for this device and also the contact details.
  Note: #, \, ', ", ? are **invalid** characters.

- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

III-3. Web Management – IPv4 Settings

Internet Protocol Version 4 (**IPv4**) is the fourth version of the Internet Protocol. It is used on the packet-switched networks and with connectionless communication. IPv4 has four bytes (32 bits) address and the address space is limited to 4,294,967,296 (2^{32}) unique addresses. On the local area network (LAN), the "Private Network" is used. It starts from **192.168.0.0** and the address space contains 65,025 (2^{16}) IP addresses. The frames can only be sent to the host in the same subnet. For example, the default IP Address of the switch is "192.168.10.1".When the users want to connect to the web console of the switch, an IP address from "192.168.10.2" to "192.168.10.254" must be assigned to the host.

CONFIGURE IPV4 INFORMATION



- **IPv4 Mode**
  There are 2 ways to configure IPv4 address - one is to configure a **static** IP address manually and another one is to get an IP address by **DHCP**.
  If the IPv4 mode is "**DHCP Client**", IPv4 information fields will be set to "**Disabled**".

- **IP Address**
  Assigns an unique static IP Address in the subnet to access the system.
  The default IP Address is **"192.168.2.1"**.

- **Subnet Mask**
  Defines the type of network, to which this device is connected to.
- **Default Gateway**
  The IP address of the router used to connect a LAN to a WAN.
- **DNS Server**
  Specifies the IP address of the DNS Server so that the users can connect to another device based on the **URL** instead of the IP address.
- 

(Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

III-4. Web Management – IPv6 Settings

Internet Protocol Version 6 (**IPv6**) is a solution to deal with the address space limitation of IPv4 and it is the most recent version of Internet Protocol. It is intended to replace IPv4. IPv6 is a **Layer 3** (Internet Layer) protocol, which is used on the packet-switched networks and with connectionless communication. There are 16 bytes (128 bits) for an IPv6 address and the address space is up to 2^{128} unique addresses. The IPv6 address is usually represented in hexadecimal digits, 8 groups of 4 digits, and each group is separated by a "**:**" (**colon**). For example, the DNS server address in IPv6 is "2001:4860:4860:0000:0000:0000:0000:8888".

CONFIGURE IPV6 INFORMATION

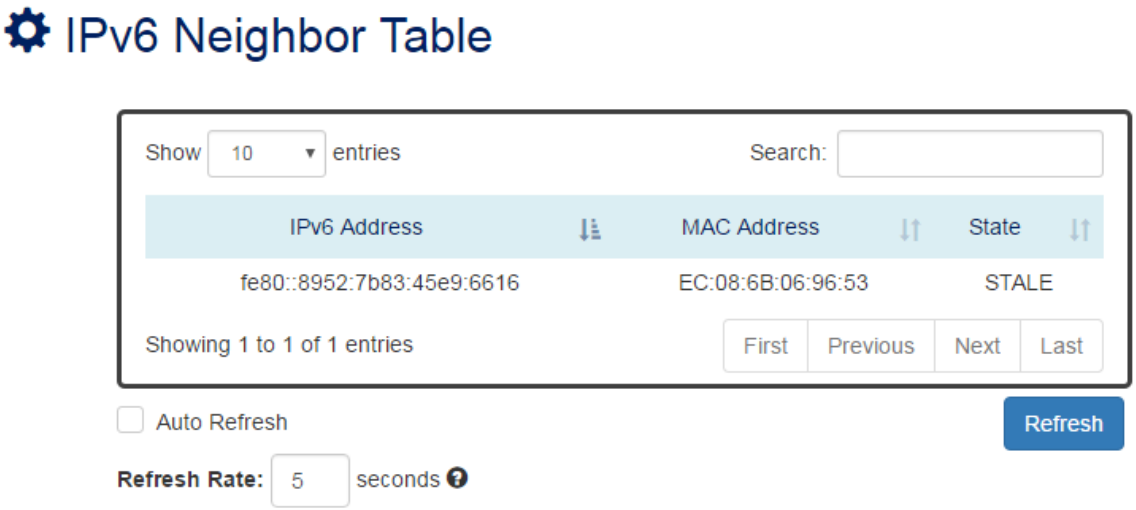
- **IPv6 Mode**
  "Enable" or "Disable" IPv6. When the IPv6 Mode is enabled, other devices can connect to this unit. The default IPv6 Mode is "**Enable**".

- **Default Address**
  This is the Default IPv6 Address for this device. It is a **Link-Local** address and is automatically generated from the **MAC Address** of the device.

- **IPv6 Addresses**
  Enables the users to define other IPv6 addresses for this device.
  The IPv6 address contains 2 section - **IPv6 address** and **prefix**. The default Prefix is **64-bit**.
  ➕: Click the **plus icon** to add a IPv6 Address row.
  ✖: Click the **remove icon** to delete the IPv6 Address row.

- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

IPV6 NEIGHBOR TABLE



- **IPv6 Address**
  This filed displays the IPv6 address of the neighbor.
- **MAC Address**
  This filed displays the MAC address of the neighbor.
- **State**
  The connection state can be “DELAY”, “REACHABLE”, “STALE”, “FAILED”, or “PROBE”.

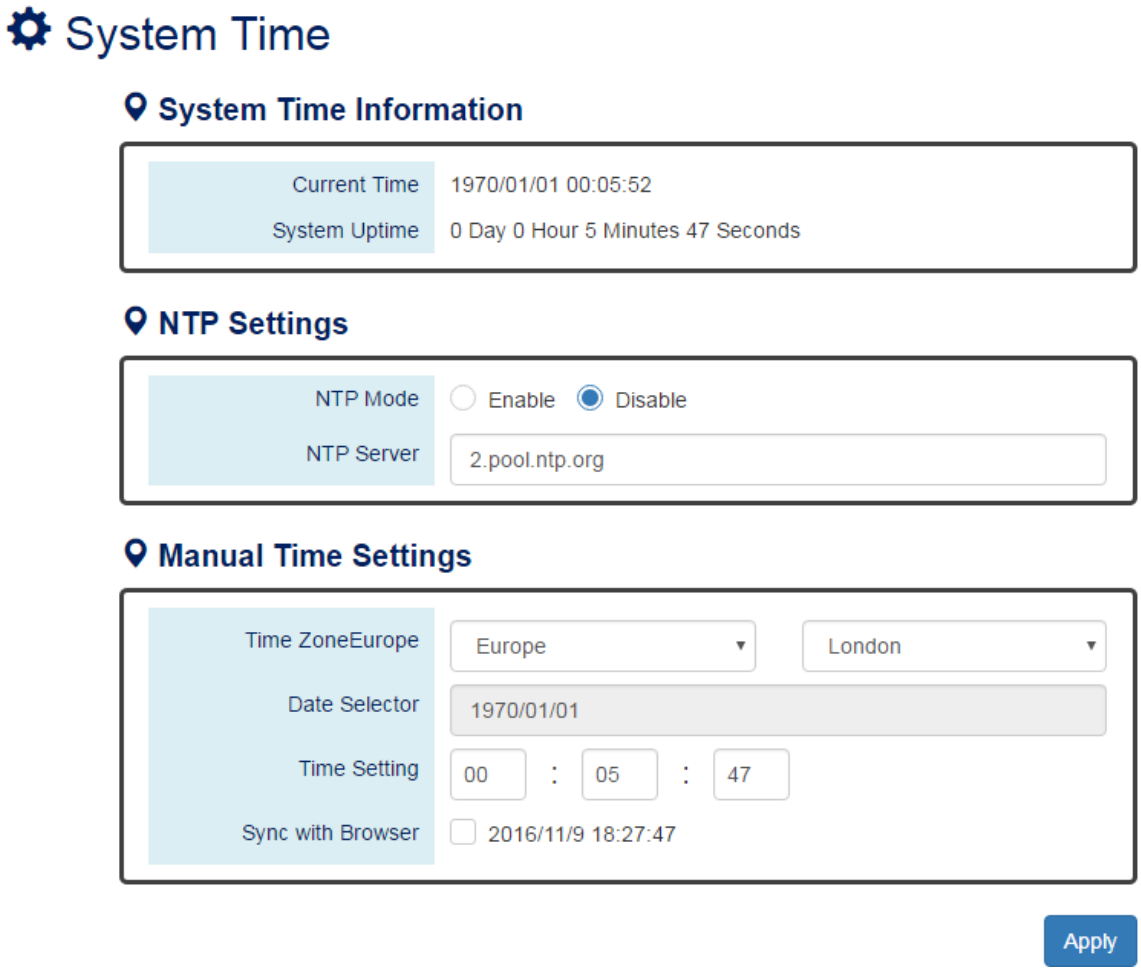
III-5. Web Management – System Time

The **System Time** represents the date and time. The system uptime defines the passing time after the system boots up. There is no battery on the switch and hence the system time cannot be saved in the system. Users can configure the time zone and system time manually by synchronizing the time with the browser or by enabling the "**NTP**" service to get the time from a **NTP Server**.

NTP

Network Time Protocol (**NTP**) is a clock synchronization protocol, which is used to synchronize the system time with the NTP server. NTP is one of the oldest Internet Protocols in use from 1985 until now. It works based on a client-server model, but it can also be used in peer-to-peer relationships. The NTP application on the switch is follows the client-server model and the switch plays a role in the NTP Client.

CONFIGURE SYSTEM TIME INFORMATION



- System Time Information
  - Current Time: The current date time of the system.
  - System Uptime: The system boot up duration.
- NTP Settings
  - NTP Mode
    "Enable" or "Disable" NTP Service. If NTP Mode is enabled, the system will sync time with NTP Server on an hourly basis.
  - NTP Server
    This field displays the URL or the IP address of the host that provides the NTP Service.

- **Manual Time Settings**
  - Time Zone
    Select the Time Zone to define the local time offset from GMT.
  - Date Selector
    Select the system date manually. The format is "**year/month/day**".
  - Time Setting
    Define the system time manually. The format is "**hour:minute:second**".
  - Sync with Browser
    Select the checkbox to synchronize the system time with the **browser time**.
- 

(Apply Button)

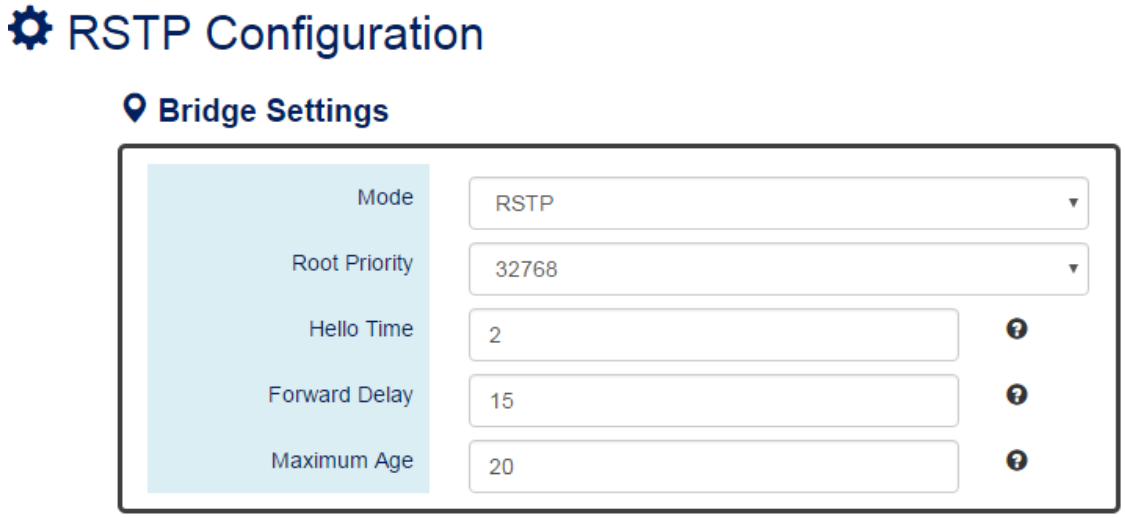
After configuring above fields, click "**Apply**" button to make the changes effective.

III-6. Web Management – RSTP Configuration

The **Spanning-Tree Protocol** is a standard protocol that is defined in **IEEE 802.1D**. It is used to build a **logical loop-free** topology for layer-2 Networks. The basic function of the protocol is to prevent loops and broadcast flooding around the switches. STP allows spare links in the network design to provide **backup paths** when the active link fails and requires a **convergence time** of **30-50 seconds** to recover the topology when the topology is changed. This prompted the use of **Rapid Spanning-Tree Protocol** as it provides a faster convergence when the topology is changed.

RSTP was introduced by IEEE as **802.1w**. It can respond within **3 x "Hello Time"** when a topology is changed. The "Hello Time" is a configurable value and it is very important for RSTP. The default RSTP value is **2 seconds** and typically, the convergence time for RSTP is **under 6 seconds**. This is much better than STP and makes RSTP to be the mainstream.

CONFIGURE RSTP BASICINFORMATION



For more information, move the mouse over the icon in the system.

- **System Time Information**
  RSTP: Enable STP and run "RSTP" for redundancy.
  Disable: Disable STP. Users have to enable another protocol to prevent from loop.

- **Root Priority**
  It is used to define the "**Root Bridge**". The bridge with the **lowest Root Priority** is the "Root Bridge". If all the bridges are set to the same Root Priority value, the system will select the Root Bridge based on the **MAC Addresses**.
  The range of Root Priority is **from 0 to 61440**(**multiple of 4096)**.
  The default Root Priority is **32768**.

- **Hello Time**
  It is very important and used to determine the interval to send BPDU (management frame) to check the RSTP topology and status.
  The range of Hello Time is **from 1 to 10** second(s).
  The default Hello Time is **2** seconds.

- **Forward Delay**
  A delay/timer is used to determine when to change the **Path State** from Learning/Listening to Forwarding.
  The range of Forward Delay is **from 4 to 30** seconds.
  The default Forward Delay is **15** seconds.

- **Maximum Age**
  A timer that is used to wait for the Hello BPDU from the Root Bridge. If this device receives the BPDU before the timer expires, the timer will be reset. Else, the device will send the topology changed BPDU to notify other devices.
  The range of Maximum Age is **from 6 to 40** seconds.
  The default Maximum Age is **20** seconds

The relationship between "Hello Time", "Forward Delay", and "Maximum Age" is:

2 x (Forward Delay - 1 sec) >= Max Age >= 2 x (Hello Time + 1 sec)

Configure RSTP Port Information

Port Settings

No.	Path Cost	Port Priority	Admin P2P	Edge	Admin STP
Port1	0	128	Shared	Auto	Enable
Port2	0	128	Shared	Auto	Enable
Port3	0	128	Shared	Auto	Enable
Port4	0	128	Shared	Auto	Enable
Port5	0	128	Shared	Auto	Enable
Port6	0	128	Shared	Auto	Enable
Port7	0	128	Shared	Auto	Enable
Port8	0	128	Shared	Auto	Enable
Port9	0	128	Shared	Auto	Enable
Port10	0	128	Shared	Auto	Enable
Port11	0	128	Shared	Auto	Enable
Port12	0	128	Shared	Auto	Enable

Apply

For more information, move the mouse over the icon in the system.

- **No.**
  Port1 to PortN, where N is based on the total port number.

- **Path Cost**
  The costfrom the current node to another device.
  The range of Path Cost is **from 0 to 200000000**.
  The default Path Cost is **0**. This implies that the Path Cost is decided by the system.

- **Port Priority**
  Used to decide the port to be blocked in the Ring topology.
  The range of Root Priority is **from 0 to 240** and are in **multiple of 16**.
  The default Root Priority is **128**.

- **Admin P2P**
  The Admin P2P is the link-type for each port.
  P2P: It is a full-duplex link.
  Shared: It is a half-duplex link.

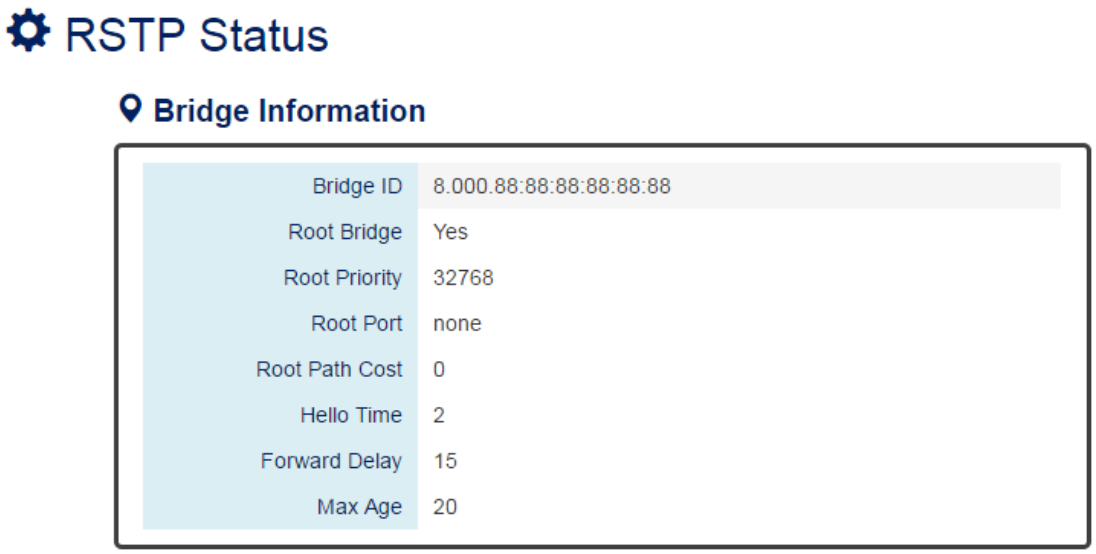
- **Edge**
  A port that can connect to a **non-STP device** is called an Edge port. Users can manually fix a port to non-Edge or Edge.
  Auto: The system **automatically** identifies an Edge or Non-Edge.
  Edge: The port is forced to be an Edge port. An edge port will directly be transitioned to the "**Forwarding**" state and is not required to wait for the "Forward Delay". If a port is directly connected to a non-STP device, users can manually set it to "Edge" and enable it to transmit faster.
  Non-Edge: The port is forced to be a Non-Edge port. This implies that the port will go through Learning/Listening to Forwarding state even though it is connected to an end device or not.

- **Admin STP**
  "Enable" or "Disable" the Spanning-tree protocol that is running on the specific port.

- 

(Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

RSTP STATUS



- **Bridge ID**
  This field shows the **unique** identity of this node when it is part of a network. It contains **8 bytes** - the first 2 bytes are for **Bridge Priority** (configurable) and the remaining 6 bytes are for the **MAC Address** (unique).

- **Root Bridge**
  It is elected from the switches in the STP topology via several **STP messages (BPDU)**. The Root Bridge is the node with the **lowest Root Priority**. If all of the nodes are with the same Root Priority, the Root Bridge will be selected based on their **MAC Addresses**.

- **Root Priority**
  It is used to define the "**Root Bridge**". The bridge with the **lowest Root Priority** is the "Root Bridge". If all bridges are set to the same Root Priority value, the system will select the Root Bridge based on the **MAC Addresses**.

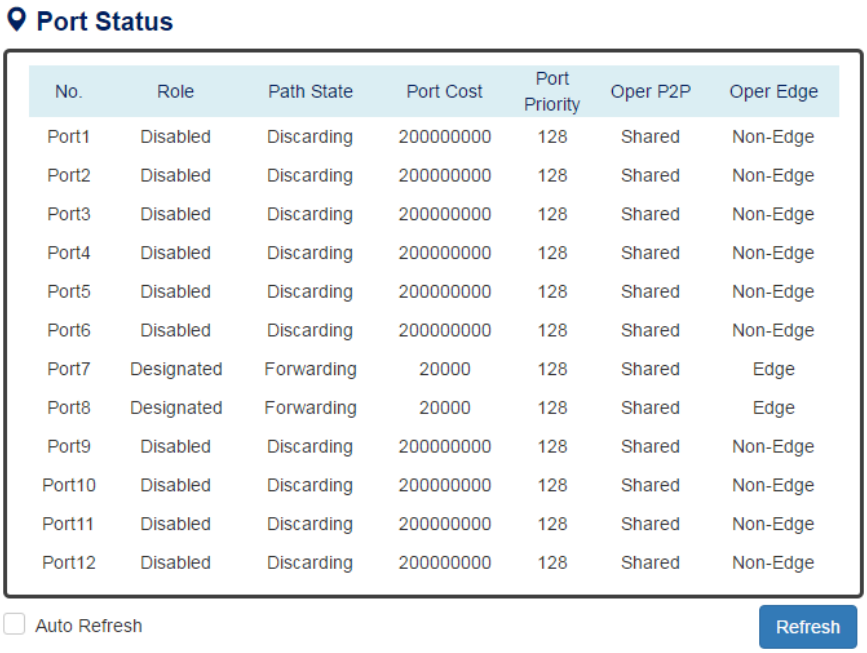
- **Root Port**
  It is the port that is **connected to the Root Bridge** and with the **lowest cost**. If the Root Port shows "**none**", it implies this node is the Root Bridge.

- **Root Path Cost**
  It is the cost from the current node to the Root Bridge.

- **Hello Time**
  It is used to determine the interval to send BPDU (management frame) to check the RSTP topology and status.

- **Forward Delay**
  It is used to determine when to change the **Path State** from Learning/Listening to Forwarding.

- **Max Age**
  It is used during waiting for Hello BPDU from the Root Bridge.



- **No.**
  Port1 to PortN, N is based on the total port number.
- **Role**
  This field shows the role of the STP port.
  Root: This is the root port, which is connected to the Root Bridge with the lowest cost.
  Designated: This is the designated port, which can send the best BPDU on the segment to other connected nodes.
  Alternate: This is the alternate port, which is blocked. This port can still receive useful BPDU **from another bridge**. When it receives a useful BPDU, it will help to forward it on the segment.
  Backup: This is the backup port, which is blocked. It corresponds with "Alternate Port" to the blocking state. This port also receives useful BPDU, but the BPDU is **from the same bridge**. When it receives a useful BPDU, it will help to forward it on the segment.
  Disabled: The port is not linked up.
- **Path State**
  This field shows the path state of this STP port.
  Discarding: The port state can be "Disabled", "Blocking", or "Listening". The incoming frames are dropped and learning MAC addresses are stopped.
  Learning: The port is learning MAC addresses, but the incoming frames are dropped.
  Forwarding: The port in the forwarding state forwards the incoming frames based on the learned MAC address table.
- **Port Cost**
  This is the cost from the port to the Root Bridge. Spanning-tree Protocol assumes the path cost is determined by the **access speeds of the links**. The **default RSTP path cost** is shown in the following table:

Speed	RSTP Path Cost	Speed	RSTP Path Cost
4 Mbps	5,000,000	1000 Mbps (1Gbps)	20,000
10 Mbps	2,000,000	2000 Mbps (2 Gbps)	10,000
16 Mbps	1,250,000	10000 Mbps (10 Gbps)	2,000
100 Mbps	200,000		

- **Port Priority**
  The Port Priority is used to determine the Root Port on a non-root bridge. The port with the lowest Port Priority value gets the higher priority.
- **Oper. P2P**
  This field shows the link-type of the STP port. P2P means "**point-to-point**" and Shared means "**point-to-multiple**".
- **Oper. Edge**
  This field shows the edge state of this STP port.

III-7. Web Management – ERPS

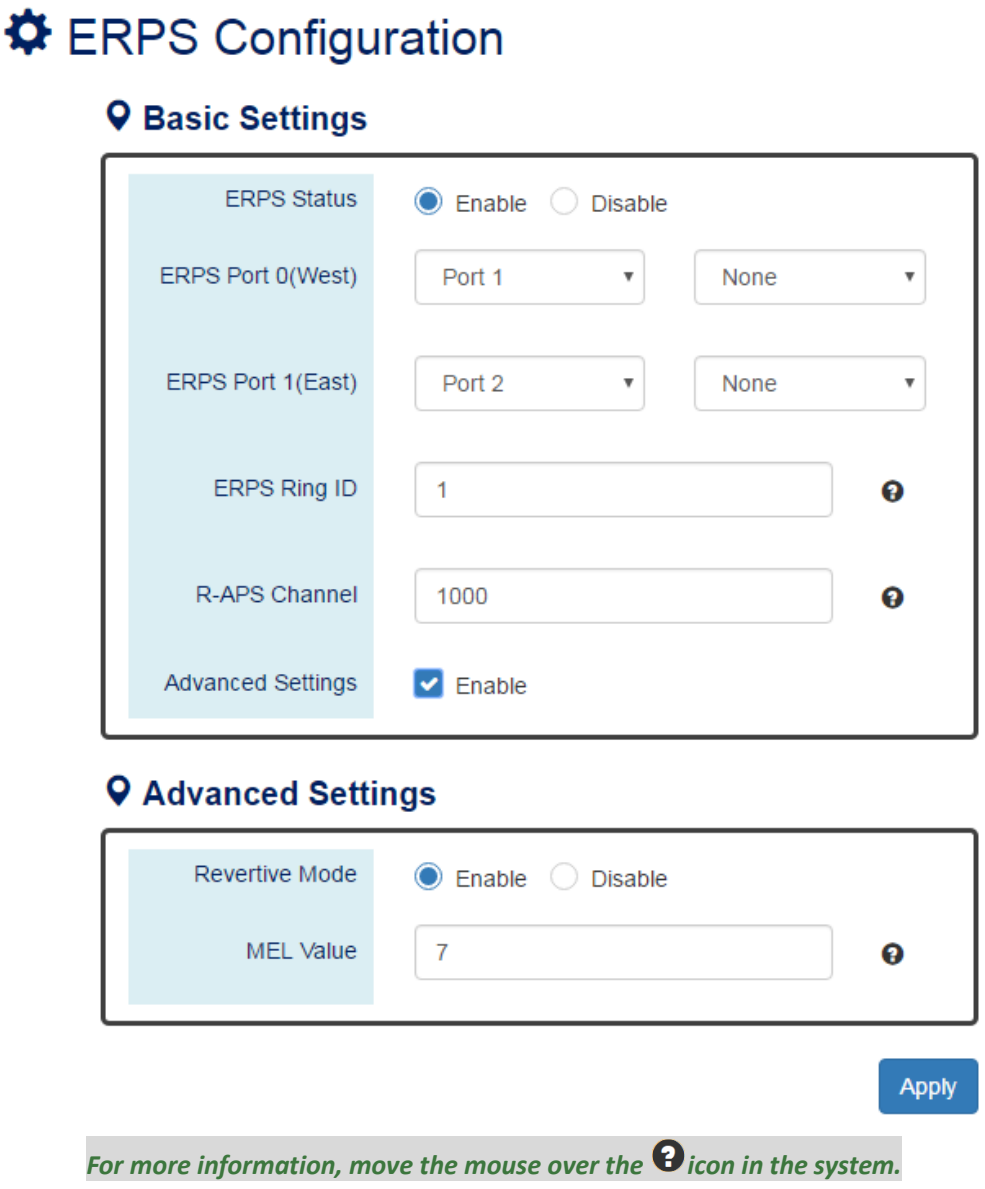
Ethernet Ring Protection Switching (ERPS) applies the protection switching mechanism for Ethernet traffic in a ring topology. This mechanism is defined in ITU-T G8032. You can avoid the possible loops in a network by implementing the ERPS function. This is done by blocking the flow of traffic to the Ring Protection Link (RPL) there by protecting the entire Ethernet ring.

When an ERPS is implemented in a ring topology, only one switch is allocated as the owner. This switch is in charge of blocking the traffic in the RPL to avoid loops. The switch adjacent to the RPL owner is called the RPL neighbor node and it is responsible for blocking the end of the RPL during normal condition. The participating switches that are adjacent to the RPL owner or neighbor in a ring are called the members or RPL next-neighbor nodes. The primary function of these switches is to forward the received traffic.

To make sure that a ring is up and loop-free, Ring Automatic Protection Switching message is sent regularly as control messages by nodes on the ring. The RPL owner identifies a signal failure (SF) in a ring when the RPL owner misses the poll packets or reads from the fault detection packets. When the fault is identified, the RPL owner unblocks the ring protection link (RPL) and permits the protected VLAN traffic through.

ERPS, similar to STP, provides a loop-free network by using polling packets to detect faults. If a fault occurs, ERPS restores itself by sending traffic over a protected reverse path rather than making a calculation to identify the forwarding path. The fault detection mechanism in the ERPS enables the ERPS to join in less than 50 milliseconds and recovers quickly to forward traffic.

CONFIGURE ERPSINFORMATION



For more information, move the mouse over the icon in the system.

- Basic Settings
  - ERPS Status
    "Enable" or "Disable" ERPS protocol running on the switch. By default, the ERPS protocol is **enabled**.
  - ERPS Port 0
    The ERPS Port 0 is also called "**West** Port". Select one of the switch ports to be the Port 0 of ERPS and decide the role of the port.
  - ERPS Port 1
    The ERPS Port 1 is also called "**East** Port". Select one of the switch ports to be the Port 1 of ERPS and decide the role of the port.

    Note: Only One of the switch ports can be configured as ERPS Port 0 or ERPS Port 1.

Role	Description
Owner	There is only one "Owner" in the ERPS ring topology. The Owner is responsible for blocking the traffic in RPL and protects one side of the RPL.
Neighbor	There is only one"Neighbor" in the ERPS ring topology. The Neighbor is the port connected with the Owner port and protects another side of the RPL.

None The “None” implies that theport is other than an Owner or aNeighbor.

- ERPS Ring ID
  The ID is the identifier of the ring. The members in the same ring must be set to the same ERPS Ring ID.

  The range of the ERPS Ring ID is **from 1 to 239**.

  The defaultERPS Ring ID is **1**.

- R-APS Channel
  The R-APS Channel is used to forward ERPS information and is mapped to the VLAN IDs. These VLAN IDs cannot be set as traffic VLANID. The members in the same ring must be set to the same R-APS Channel.

  The range of the R-APS Channel is **from 1 to 4094**.

  The defaultR-APS Channel is **1000**.

- **Advanced Settings**
  The Advanced Settings field is only displayed when the “Advanced Settings” checkbox is selected in the Basic Settings.

  - Revertive Mode
    “Enable” or “Disable”the ERPS Revertive Mode. If the Revertive Mode is enabled, the blocked link will revert to the RPL link after the failed link is recovered.

    By default, the ERPS Revertive Mode is **enabled**.

  - MEL Value
    The MEL implies the MEG Level. The MEL is afield in the R-APS PDU. Alarge MEL value involves more devices. For example, level 7 contains levels 0 to 6.

    The range of the MEL Value is **from 0 to 7**.

    The default MEL Value is **7**.

- Apply (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

III-8. Web Management – SNMP

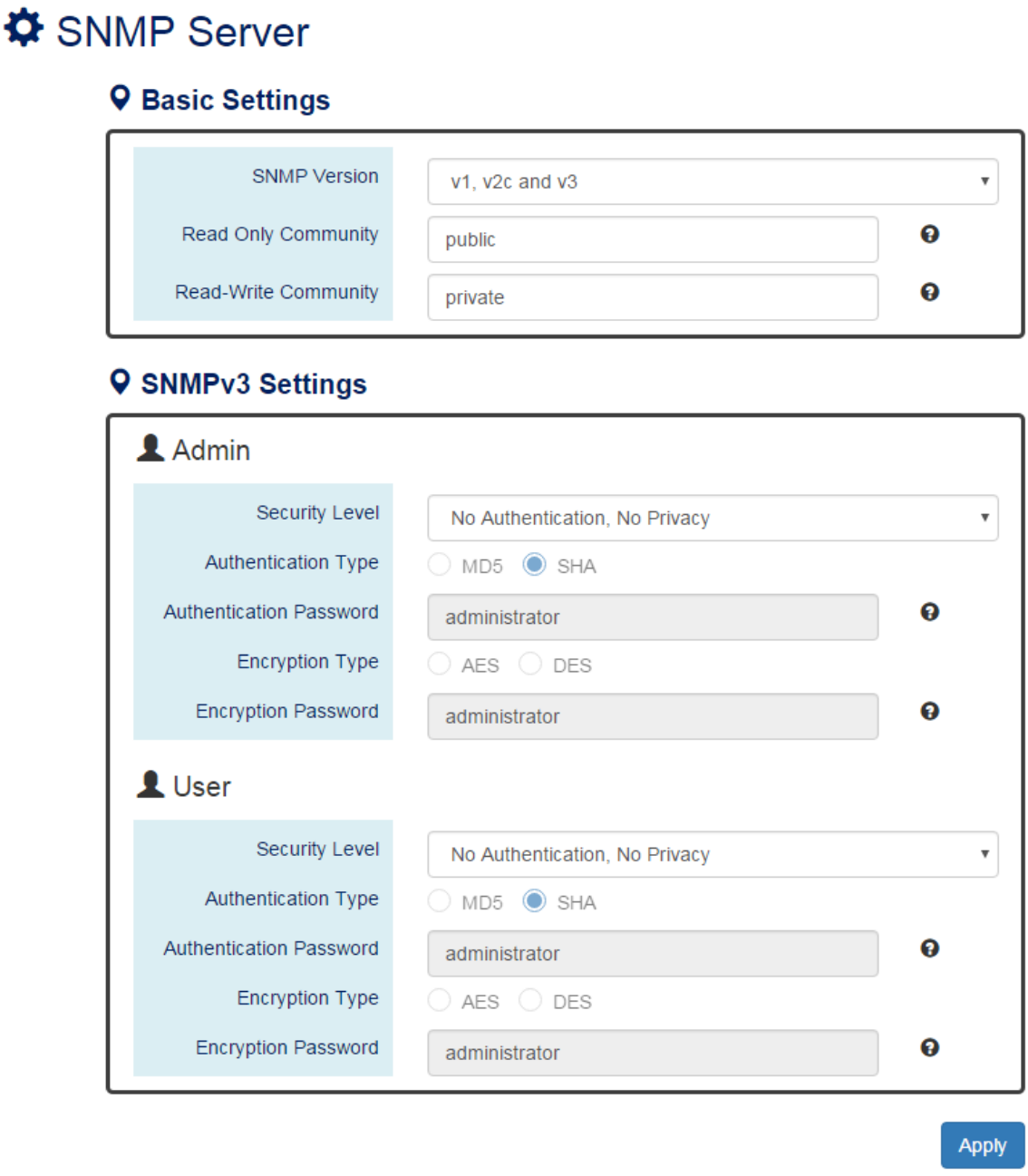
Simple Network Management Protocol (SNMP) is a standard for collecting and structuring information on the managed devices of the IP network. It can also modify some of the information to change the behavior of the devices. SNMP is usually used in monitoring the network. The users can remotely query the information provided by the devices running SNMP.

The switches support SNMP v1, v2c, and v3. SNMP v1 and v2c authenticates with a community string for "**read-only**" or "**read-write**" permission. The SNMP v3 authentication requires to select an authentication level (**MD5** or **SHA**) and also supports data encryption to make the data safer.

For the SNMP version and authentication method relationship, refer to the table below:

Version	Web Setting	Authentication	Encryption	Method
v1 & v2c	Read Only Community	Community String	No	String match for authentication
	Read-Write Community	Community String	No	String match for authentication
v3	Security Level – No Authentication, No Privacy	No	No	Access by an account (admin or user)
	Security Level – Authentication, No Privacy	MD5 / SHA	No	Access by an account (admin or user) and password with more than 8 characters, which is based on MD5 or SHA
	Security Level – Authentication, Privacy	MD5 / SHA	Yes AES / DES	Access by an account (admin or user) and password more than 8 characters, which is based on MD5 or SHA. The data encryption is based on AES or DES and the key requires 8 to 32 characters.

CONFIGURE SNMP SERVER INFORMATION



For more information, move the mouse over the ? icon in the system.

- **Basic Settings**
  - SNMP Version
    The system enables the SNMP "**v1, v2c and v3**" authentication by default. The users can enable the SNMP server on only "**v1 and v2c**" or "**v3**". "**None**" refers to disabling the SNMP server.
  - Read Only Community
    The community used to access the SNMP server with the "**read-only**" privilege.

    The **max.length** for the Read Only Community is **32 characters**.

    Note: #, \, ', ", ? are **invalid** characters.
  - Read-Write Community
    The community used to access the SNMP server with the "**read-write**" privilege.

    The **max.length** for the Read-Write Community is **32 characters**.

    Note: #, \, ', ", ? are **invalid** characters.

- **SNMPv3 Settings**
  This section is displayed only when the **SNMP Version** is set to “v3” or “v1, v2c and v3”. Two accounts are provided – Admin and User to access the SNMP agent. The users can set different levels for the 2 accounts.
  - Security Level
    No Authentication, No Privacy: Access by an account “admin” or “user”.

    Authentication, No Privacy: Access by an account “admin” or “user” with password.

    Authentication, Privacy: Access by an account “admin” or “user” with password and the data will be encrypted.
  - Authentication Type
    Two algorithms are provided - **MD5** and **SHA** for authentication password.
  - Authentication Password
    A string/key is used to authenticate the SNMP Server and obtain the access permission. It will be hashed by MD5 or SHA before authentication.

    The min. length for the Read-Write Community is **8 characters.**

    The max.length for the Read-Write Community is **32 characters**.

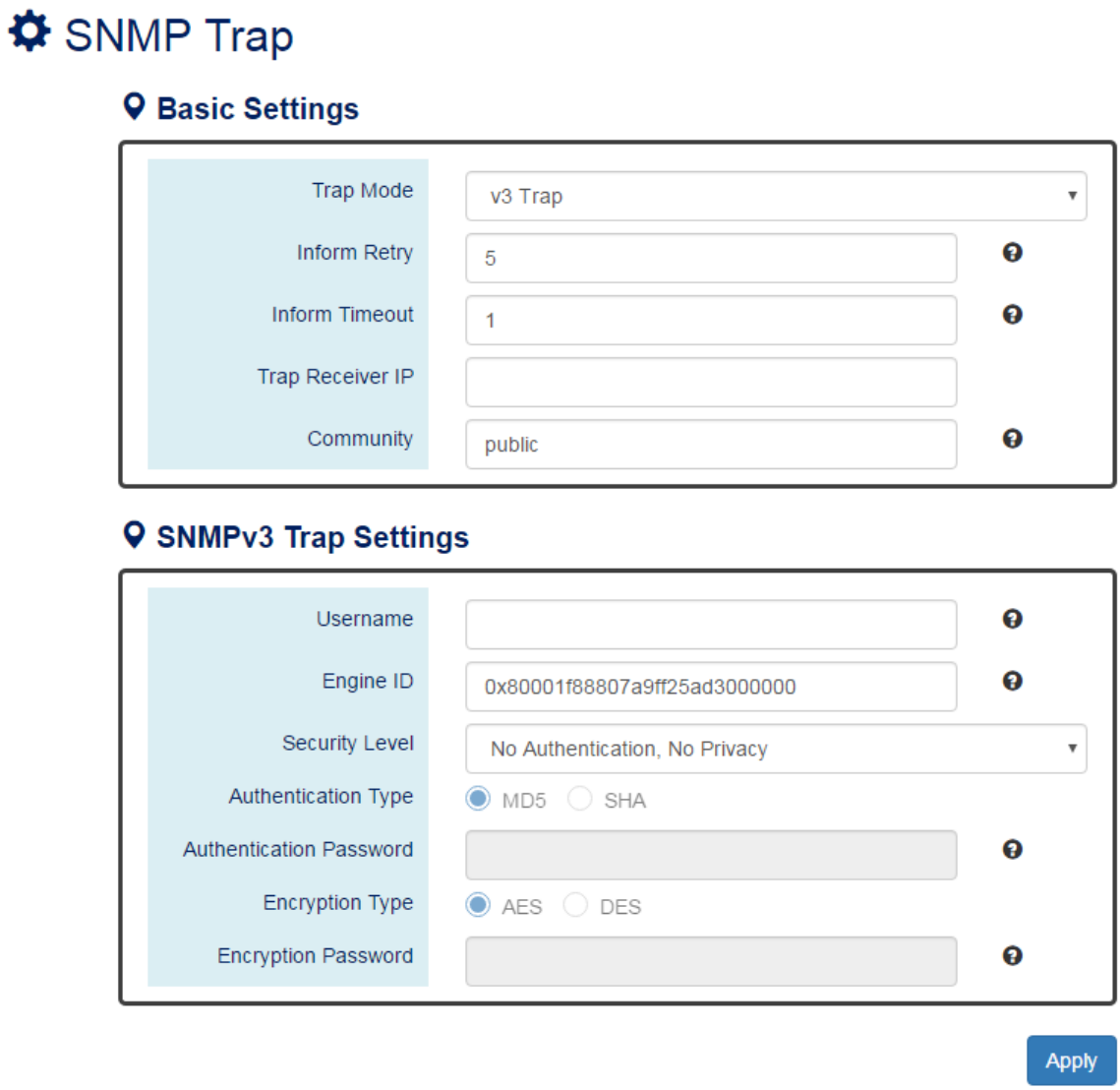
    Note: #, \, ', ", ? are **invalid** characters.
  - Encryption Type
    Two algorithms are provided - **AES** and **DES** for data encryption.
  - Encryption Password
    A string/key is used to encrypt the data that is sent to the SNMP server.

    The min. length for theRead-Write Communityis **8 characters.**

    The max.length for the Read-Write Community is **32 characters**.

    Note: #, \, ', ", ? are **invalid** characters.
- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

CONFIGURE SNMP TRAP INFORMATION



For more information, move the mouse over the ? icon in the system.

- **Basic Settings**
  - Trap Mode
    The system enables the SNMP "**v1, v2c and v3**" authentication by default. Users can enable the SNMP server only on "**v1 and v2c**" or "**v3**". "**None**" indicates disabling the SNMP server.
  - Inform Retry
    The SNMP trap will send "Retry" times when the trap set to "v2 Inform" or "v3 Inform" mode.

    The range of the Inform Retry is **from 1 to 100**.

    The default Inform Retry is **5**.
  - Inform Timeout
    The interval is used to send trap when the trap set to "v2 Inform" or "v3 Inform" mode.

    The range of the Inform Retry is **from 1 to 300** second(s).

    The default Inform Retry is **1** second.
  - Trap Receiver IP
    The IP address is the IP address of the trap server to receive the trap information.

- Community
  The string in the SNMP trap is the identity of the device.

  The max.length for the Community is **32 characters**.

  Note: #, \, ', ", ? are **invalid** characters.

- **SNMPv3 Trap/Inform Settings**
  This section is displayed only when **Trap Mode** are set to “v3 Trap” or “v3 Inform”.
  - Username
    Specify the username for authentication with the SNMP trap server.
  - Engine ID
    The Engine ID is the identifier for the given SNMP application.
  - Security Level
    No Authentication, No Privacy: Access using the username assigned to the users.

    Authentication, No Privacy: Access using the username assigned to the users with password.

    Authentication, Privacy: Access using the username assigned to the users with password and the data will be encrypted.
  - Authentication Type
    Two algorithms are provided - **MD5** and **SHA** for authentication password.
  - Authentication Password
    A string/key is used to authenticate the SNMP trap server and obtain the permission. It will be hashed by MD5 or SHA before authentication.

    The min. length for the Read-Write Community is **8 characters.**

    The max.length for the Read-Write Community is **32 characters**.

    Note: #, \, ', ", ? are **invalid** characters.
  - Encryption Type
    Two algorithms are provided - **AES** and **DES** for data encryption.
  - Encryption Password
    A string/key is used to encrypt the data sent to the SNMP trap server.

    The min. length for the Read-Write Community is **8 characters.**

    The max.length for the Read-Write Community is **32 characters**.

    Note: #, \, ', ", ? are **invalid** characters.

- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

III-9. Web Management – DHCP

DHCP Server/Client

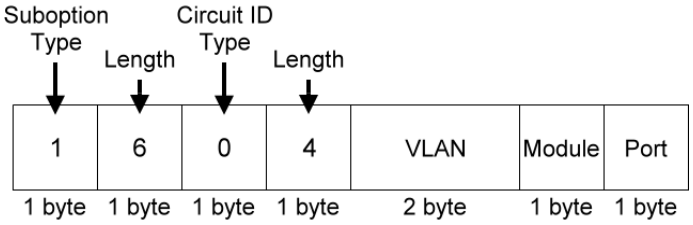
DHCP, **Dynamic Host Configuration Protocol**, is a standardized protocol used in the IP networks. The DHCP Server holds an **IP address pool** and when a DHCP Client request for an IP address, the DHCP Server picks an IP address from the pool and assigns it to the client. DHCP Server also manages other IP information such as **Default Gateway** and **DNS Server**. DHCP is very useful to configure the IP information for a number of devices. Only the administrator can enable the DHCP Client for each device and setup the DHCP Server. The clients will then obtain a unique IP address and other IP settings to connect to the network.

DHCP Server Binding

Apart from dynamically allocating an IP address to a DHCP Client, the DHCP Server also provides a function to manually assign a **static IP address** to the device with a specific MAC Address. This is called as DHCP Server Binding.

DHCP Relay/Option82

In a large network, there might be several subnets existed and the DHCP Client is not able to serve by DHCP Servers directly. In this case, we need a relay agent to help to transmit the request frames to the DHCP Servers. When a relay agent receives the broadcast request frame from a DHCP Client, the relay agent will transmit the frame to the DHCP Servers, which are in the same subnet by unicast.
Option 82 is an information option to identify the clients by **Circuit ID** and **Remote ID**. The **Circuit ID** is an identity containing the **interface** name and/or **VLAN** information, and the **Remote ID** is to identify the **remote host** (the relay agent). The DHCP Server can distribute an IP address to the DHCP Client according to Option 82 information and make the IP addresses more controllable.
The frame format for the **Circuit ID** is as below:

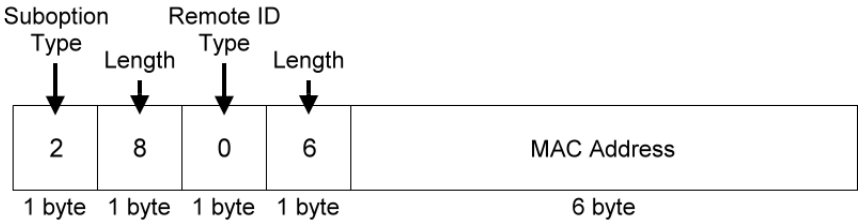


- **VLAN**
  The VLAN field is for the **management VLAN ID**, which is natively set to **1**.

- **Module**
  The stack number for the device sending the DHCP request is on. For industrial switches, this byte is always filled as **0**.

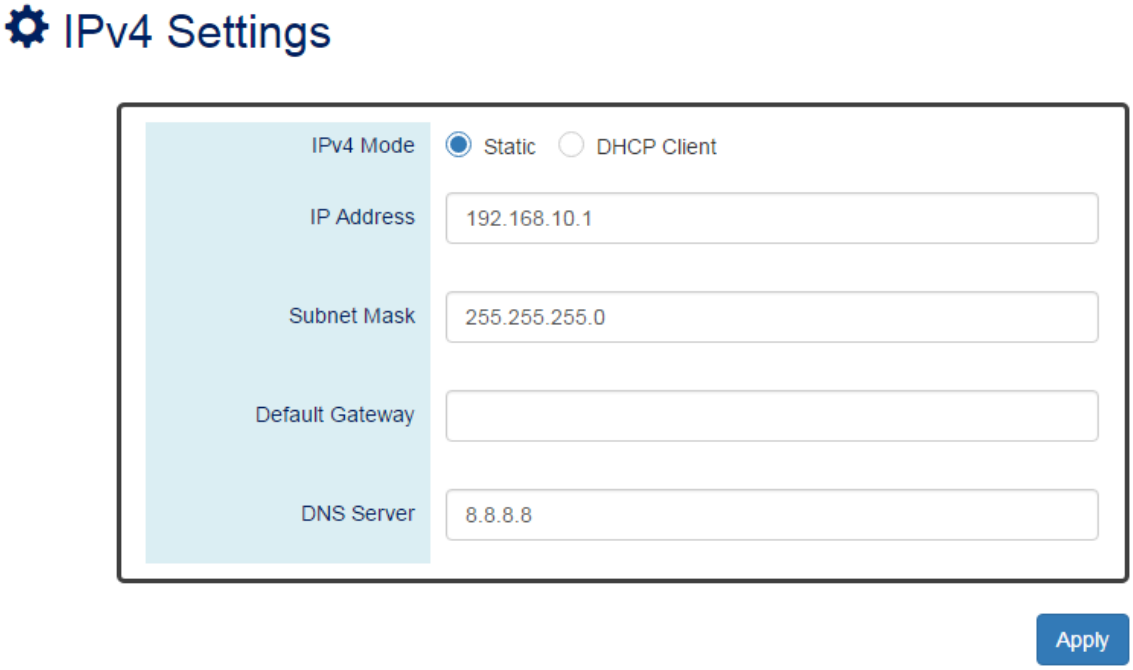
- **Port**
  The port number identifies the incoming DHCP request frame/DHCP Client.

The frame format for the **Remote ID** is as below:



- **MAC Address**
  By default, the MAC address is set to the MAC address of DHCP relay agent.

CONFIGURE DHCP CLIENT

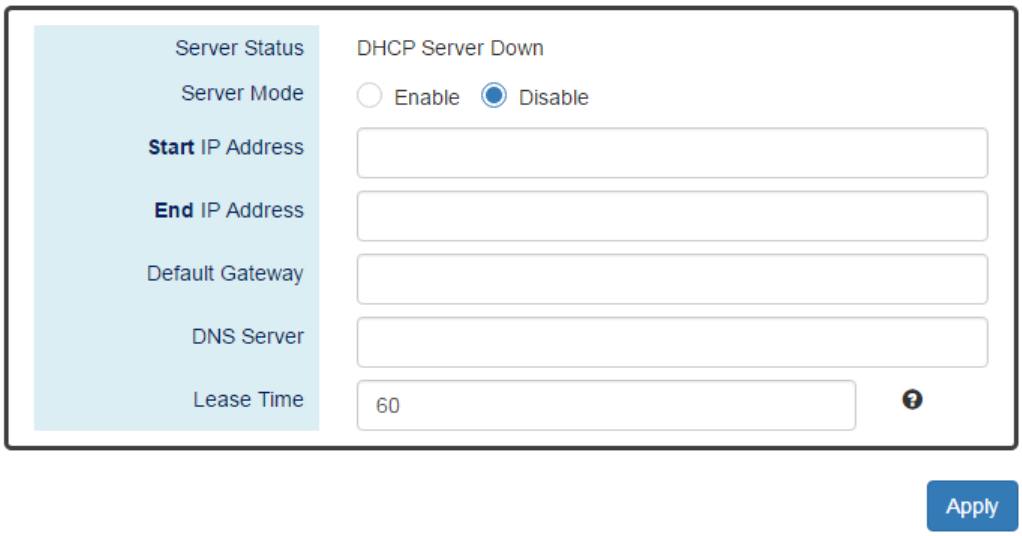


- **IPv4 Mode**
  Set the **IPv4 Mode** to "**DHCP Client**" to enable the DHCP Client. The system sends a **discovery frame** to the network and tires to obtain an IP address from the DHCP Server.

  After enabling the DHCP Client, users need to connect to the **Console Port** to get the IP address by using "***show ip address***" on the CLI.

- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

CONFIGURE DHCP SERVER INFORMATION



For more information, hover the mouse over the ? icon in the system.

- **Server Status**
  Shows the status of the DHCP server: **Down** or **Up.**

- **Server Mode**
  "Enable" or "Disable" the DHCP Server function.

- **Start IP Address**
  Set the range of the IP pool. The "Start IP Address" is the starting.

  "Start IP Address" must be in the **same subnet** as that of the switch itself.

- **End IP Address**
  Set the range of IP pool. The "End IP Address" is the end.

  "End IP Address" must be in the **same subnet** as that of the switch itself.

- **Default Gateway**
  Set the Default Gateway for the DHCP Clients to make them connect to the WAN.

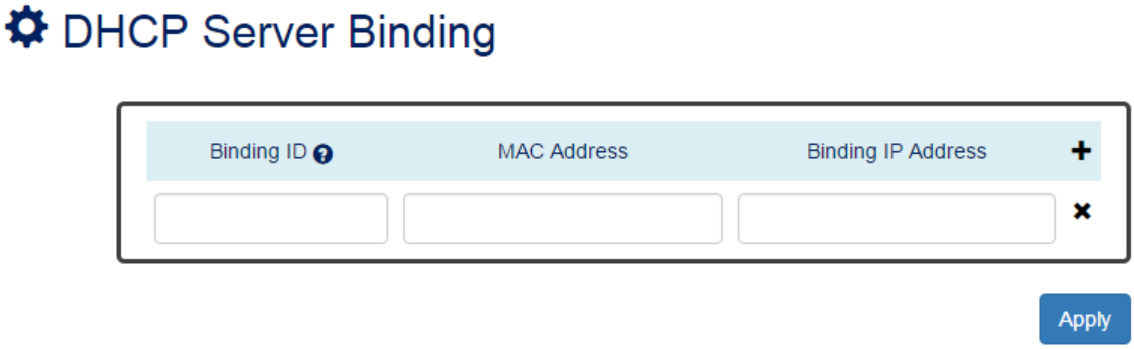
  "Default Gateway" must be in the **same subnet** as that of the switch itself.

- **DNS Server**
  Set the DNS Server for the DHCP Clients to make them connect to another device based on the **URL** instead of IP address.

- **Lease Time**
  DHCP Server leases an IP address to a device for **a period of time**. When the lease time expires, the DHCP server may assign a different IP address in the pool to the device.

- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

Configure DHCP Server Binding Information



For more information, hover the mouse over the icon in the system.

- **Binding ID**
  An ID used to identify the binding.

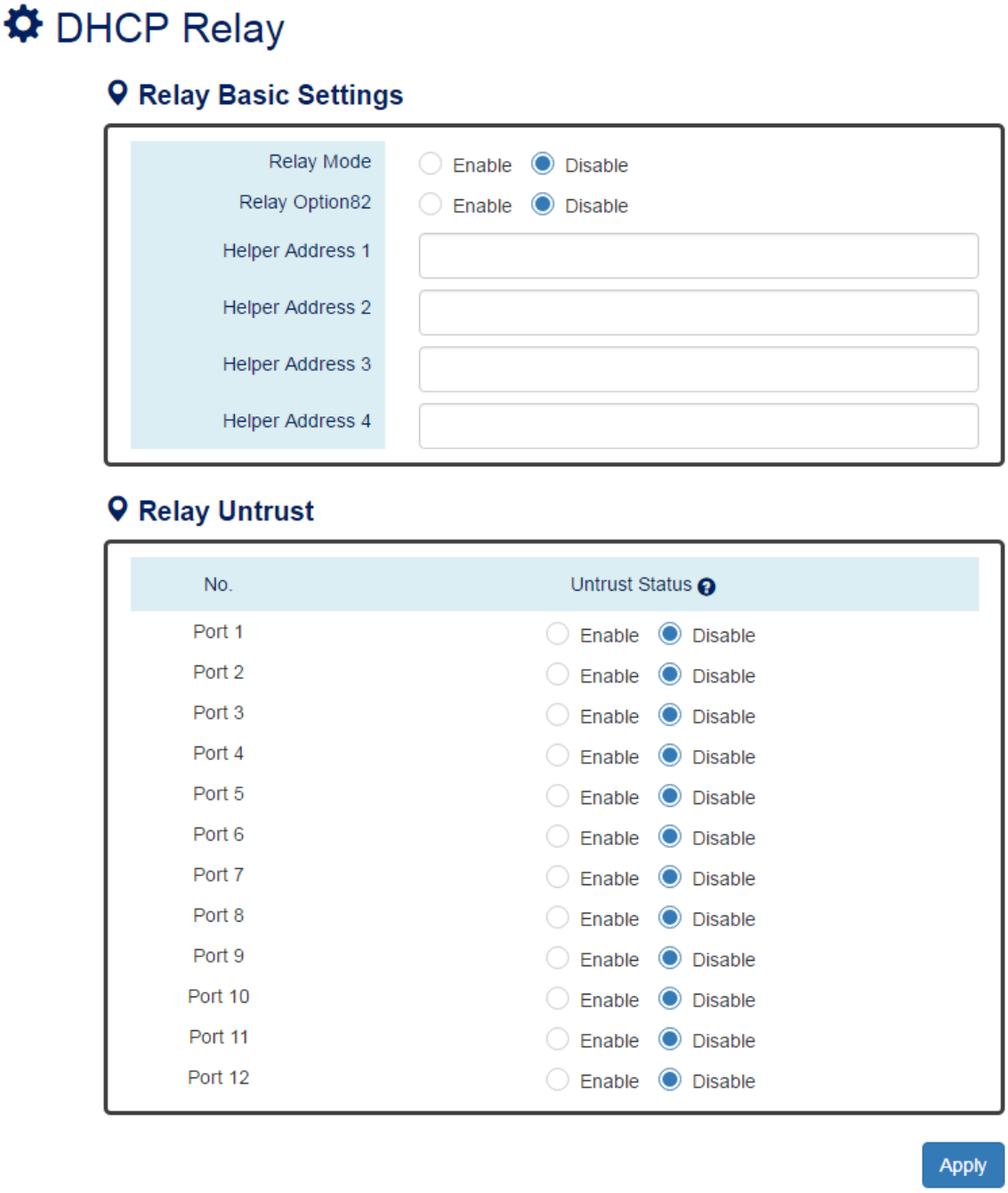
  The range of the Binding ID is **from 1 to 32**.

- **MAC Address**
  The device with the specified MAC Address will be assigned to the static Binding IP Address.

- **Binding IP Address**
  A static IP Address will be assigned to the specified MAC Address.

- ➕: Click the **plus icon** to add a DHCP Binding row.
- ✖: Click the **remove icon** to delete the DHCP Binding row.
- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

CONFIGURE DHCP RELAY INFORMATION



For more information, move the mouse over the icon in the system.

- Relay Basic Settings
  - Relay Mode
    "Enable" or "Disable" the DHCP Relay function.
  - Relay Option82
    "Enable" or "Disable" the DHCP Relay with Option82 tag.
  - Helper Address 1 - 4
    The **IP Addresses** of the **DHCP Servers** provide IP addresses to the DHCP Clients. A backup of Four Helper Addresses are available during breakdown.

- **Relay Untrust**
  - No.
    Port1 to PortN, where N is based on the total port number.
  - Untrust Status
    “Enable” or “Disable” to untrust the specific port. If the untrusted status is enabled on a port, the system will **drop** the DHCP management frames on the port.
- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

III-10. Web Management – ModBUS/TCP

Modbus is a popular communication protocol used for the **industrial serial devices**. It is usually working as "**master-slave**" architecture and working with **programmable logic controllers** which are also called **PLC**s. The Modbus/TCP implies to provide Modbus Messaging service on the TCP/IP, so that the devices which are running Modbus can communicate with each other with Modbus messages. The Modbus messages are encapsulated with an Ethernet TCP/IP wrapper on the basis of the standard. During the transmission, the switches can only acquire the encapsulated information when the Modbus/TCP is enabled. If users would like to understand the real content of Modbus message, users have to install other utilities such as "ModScan". Our switches implements the Modbus/TCP registers including system information, firmware information, port information, and packet information. The details refer to the "Modbus Data Mapping Information" section.

DATA FORMAT AND FUNCTION CODE

The primary four types of Modbus/TCP data format are as following:

Data Access Type		Function Code	Function Name
Bit Access	Physical Discrete Inputs	2	Read Discrete Inputs
	Internal Bits or Physical Coils	1	Read Coils
Word Access (16-bit Access)	Physical Input Registers	4	Read Input Registers
	Physical Output Registers	3	Read Holding Registers

MODBUS DATA MAPPING INFORMATION

In the following tables, we assume the total port number is **8**.

The following table is for **Function Code 3** (**Holding Registers**) / **Function Code 6**.

Address Offset	Data Type	Interpretation	Description
System Information			
0x0000 to 0x0008	1 word	HEX	**Port 1 to Port 8 Status** 0x0000: Disable 0x0001: Enable **Port 1 to Port 8 Status Configuration** 0x0000: Disable 0x0001: Enable

The following table is for **Function Code 4** (**Input Registers**). The data map addresses in the following table starts from **Modbus address 30001**. For example, the address offset 0x0000H equals Modbus address 30001, and the address offset 0x0030H equals Modbus address 30049. All the information read from our switches is in the **HEX mode** and users can refer to the ASCII table for the translation (e.g. 0x4B='K', 0x74='t').

Address Offset	Data Type	Interpretation	Description
System Information			
0x0030	20 words	ASCII	**Product Name = "MT-0804G"** Word 0 Hi byte = 'M' Word 0 Lo byte = 'T' Word 1 Hi byte = '-' Word 1 Lo byte = '0' Word 2 Hi byte = '8' Word 2 Lo byte = '0' Word 3 Hi byte = '4' Word 3 Lo byte = 'G'
0x0050	1 word		Product Serial Number
0x0051	2 words	HEX	**Firmware Version** For example: Word 0 = 0x0103 Word 1 = 0x0200 Firmware version is 1.3.2

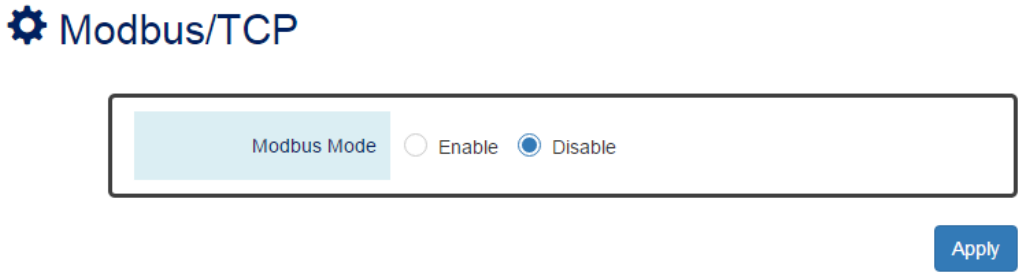
Address Offset	Data Type	Interpretation	Description
System Information			
0x0053	2 words	HEX	**Firmware Release Date** For example: Word 0 = 0x1719 Word 1 = 0x1506 Firmware was released on 2015-06-17 at 19 o'clock
0x0055	3 words	HEX	**Ethernet MAC Address** Ex: MAC = 01:02:03:0A:0B:0C Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x02 Word 1 Hi byte = 0x03 Word 1 Lo byte = 0x0A Word 2 Hi byte = 0x0B Word 2 Lo byte = 0x0C
0x0058	1 word	HEX	**Power 1** 0x0000: Off 0x0001: On

Address Offset	Data Type	Interpretation	Description
0x0059	1 word	HEX	**Power 2** 0x0000: Off 0x0001: On
0x005A	1 word	HEX	**Fault LED Status** 0x0000: Boot error 0x0001: Normal 0x0002: Fault
0x0082	1 word	HEX	**DO1** 0x0000: Off 0x0001: On

Address Offset	Data Type	Interpretation	Description
Port Information			
0x1000 to 0x1008	1 word	HEX	**Port 1 to Port 8 Status** 0x0000: Link down 0x0001: Link up 0x0002: Disable 0xFFFF: No port
0x1100 to 0x1108	1 word	HEX	**Port 1 to Port 8 Speed** 0x0000: 10M-Half 0x0001: 10M-Full 0x0002: 100M-Half 0x0003: 100M-Full 0xFFFF: No port
0x1200 to 0x1208	1 word	HEX	**Port 1 to Port 8 Flow Ctrl** 0x0000: Off 0x0001: On 0xFFFF: No port
0x1300 to 0x1313 (Port 1) 0x1314 to 0x1327 (Port 2) … 0x138C to 0x139F (Port 8)	20 words	ASCII	**Port 1 to Port 8 Description** Port Description = “100Tx,RJ45.” Word 0 Hi byte = ‘1’ Word 0 Lo byte = ‘0’ Word 1 Hi byte = ‘0’ Word 1 Lo byte = ‘T’ … Word 4 Hi byte = ‘4’ Word 4 Lo byte = ‘5’ Word 5 Hi byte = ‘.’ Word 5 Lo byte = ‘\0’
Packet Information			
Address Offset	**Data Type**	**Interpretation**	**Description**
0x2000 to 0x200F	2 words	HEX	Port 1 to Port 8 Tx Packets Ex: port 1 Tx Packet Amount = 13248635 Received Modbus response: 0x13248635 Word 0 = 1324 Word 1 = 8635

Address Offset	Data Type	Interpretation	Description
0x2080 to 0x208F	2 words	HEX	Port 1 to Port 8 Tx Bytes Ex: port 1 Tx Btyes Amount = 13248635 Received Modbus response: 0x13248635 Word 0 = 1324 Word 1 = 8635
0x2100 to 0x21(YY*2-1)	2 words	HEX	Port 1 to YY Rx Packets Ex: port 1 Rx Packet Amount = 13248635 Received Modbus response: 0x13248635 Word 0 = 1324 Word 1 = 8635
0x2180 to 0x218F	2 words	HEX	Port 1 to Port 8 Rx Bytes Ex: port 1 Rx Btyes Amount = 13248635 Received Modbus response: 0x13248635 Word 0 = 1324 Word 1 = 8635

CONFIGURE MODBUS/TCP INFORMATION



- **Modbus Mode**
  “Enable” or “Disable”the Modbus/TCP function.
- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

III-11. Web Management – UPnP

UPnP is **Universal Plug and Play**, a set of networking protocol that permits the network devices to seamlessly discover each other in the networks. It is promoted by the UPnP Forum, but since 2016, all UPnP efforts are managed by the Open Connectivity Foundation.
UPnP extends "**plug and play**" to connect to a network device without configuration. When an UPnP device such as printer, Wi-Fi AP, or mobile device connects to a network, it will automatically establish the working configurations with another device.

CONFIGURE UPNP INFORMATION

For more information, move the mouse over the icon in the system.

- **UPnP Mode**
  "Enable" or "Disable"the UPnP function.

- **Advertisement Interval**
  A time period used to send the UPnP advertisement frame.

  The range of the Advertisement Interval is **from 300 to 86400** seconds.

  The default Advertisement Interval is **1800**seconds.

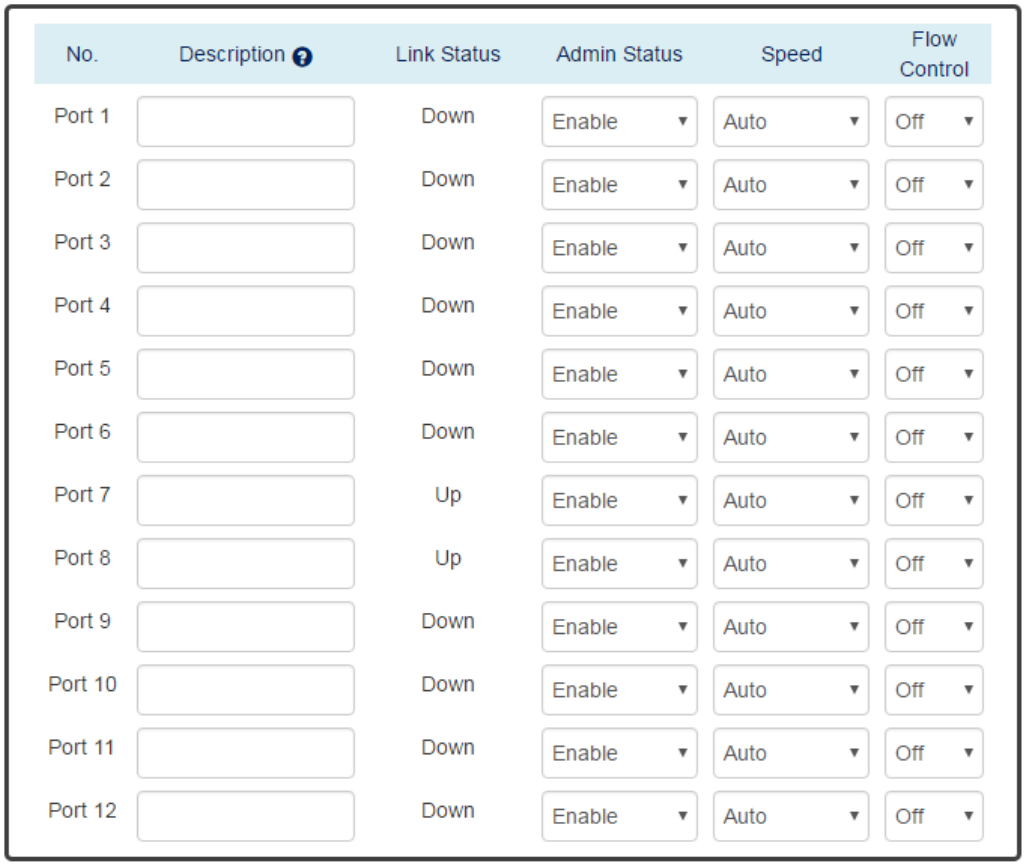
- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

III-12. Web Management – Port Management

Port Management contains a “Description” field that is used to describe the port, “Enable” or “Disable” option to turn on or turn off a specific port, configure the speed-duplex for the port, and Flow Control on the port. In the Port Status page, the users can obtain information such as Link Status, Speed, Duplex, Flow Control, Tx and Rx in Bytes, and PoE status. These are very helpful for the administrator to manage the interfaces on the switch.

CONFIGURE PORT INFORMATION

Port Settings



No.	Description	Link Status	Admin Status	Speed	Flow Control
Port 1		Down	Enable	Auto	Off
Port 2		Down	Enable	Auto	Off
Port 3		Down	Enable	Auto	Off
Port 4		Down	Enable	Auto	Off
Port 5		Down	Enable	Auto	Off
Port 6		Down	Enable	Auto	Off
Port 7		Up	Enable	Auto	Off
Port 8		Up	Enable	Auto	Off
Port 9		Down	Enable	Auto	Off
Port 10		Down	Enable	Auto	Off
Port 11		Down	Enable	Auto	Off
Port 12		Down	Enable	Auto	Off

Apply

For more information, move the mouse over the icon in the system.

- **No.**
  Port1 to PortN, where N is based on the total port number.
- **Description**
  The description for the port is helpful for the administrator to identify the difference between the ports.

  The **max.length** for the Description is **32 characters**.

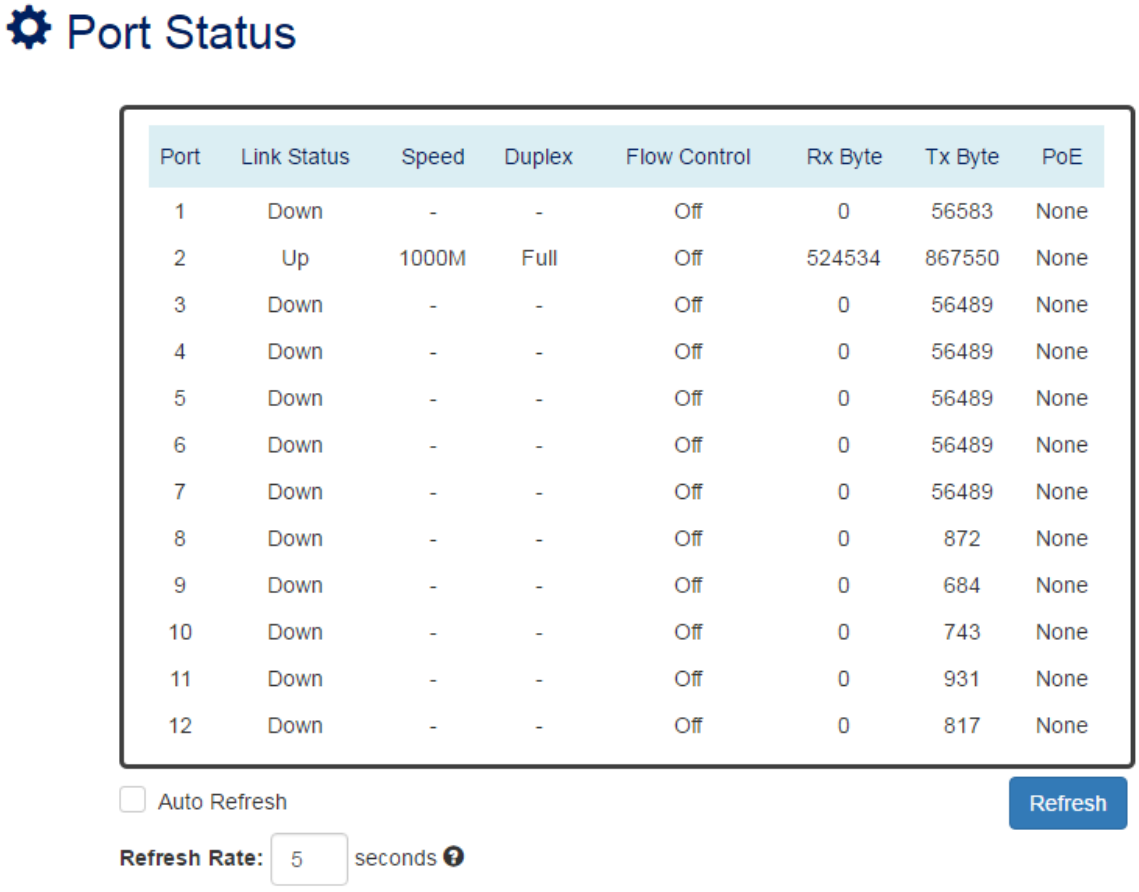
  Note: #, \, ', ", ? are **invalid** characters.
- **Link Status**
  Link Status shows “Up”, “Down”, or “Disable” to reflect the link status of the port.
- **Admin Status**
  “Enable” or “Disable” the Admin Status of the port to restrict the transmission on the port.

  Note: Administrator can **turn off the un-used port** to **secure** the network with unexpected device.

- **Speed**
  The users are able to manually fix the speed and duplex or automatically run auto-negotiation to determine the speed and duplex.
  - Auto: The port follows IEEE 802.3u protocol to auto-negotiate with connected device.
  - 100M-Full: The port transmits frames with **100Mbits** per second speed and **full duplex**.
  - 100M-Half:The port transmits frames with **100Mbits** per second speed and **half duplex**.
  - 10M-Full:The port transmits frames with **10Mbits** per second speed and **full duplex**.
  - 10M-Half:The port transmits frames with **10Mbits** per second speed and **half duplex**.
- **Flow Control**
  “Enable” or “Disable”the Flow Control when the speed is set to “Auto”. Enabling the Flow Control helps to prevent the traffic from losing when the network is in congestion.
- 

(Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

PORT STATUS



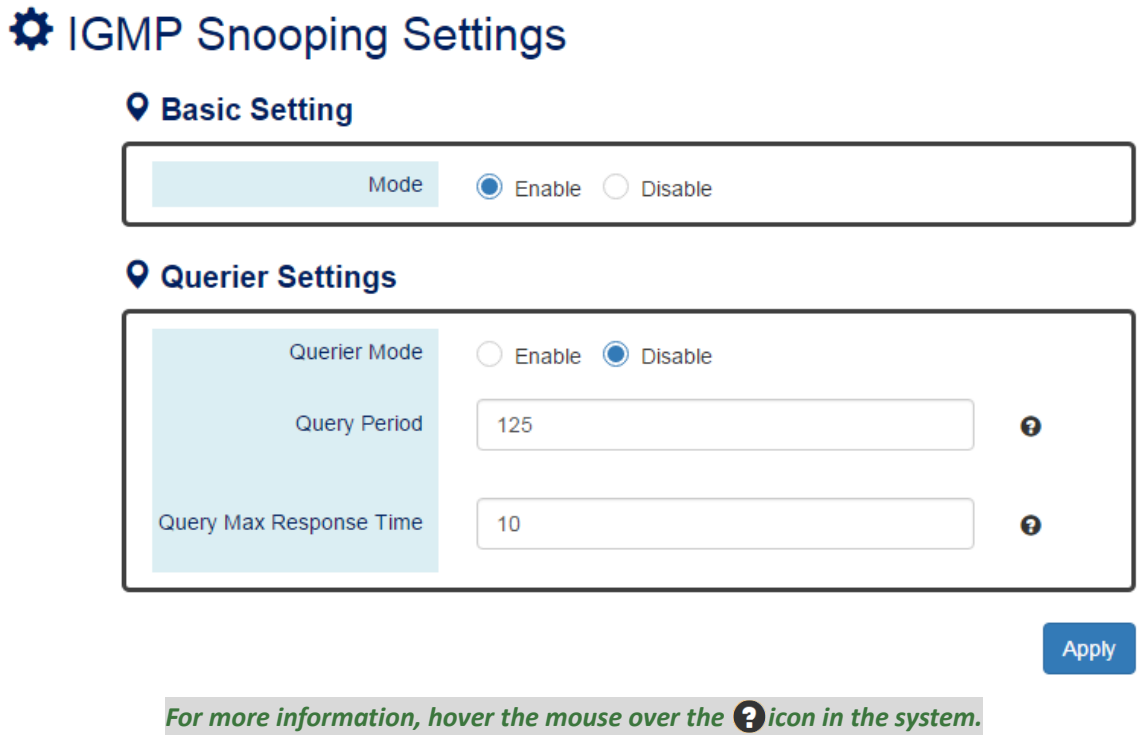
- **Port**
  Port 1 to N, where N is based on the total port number.
- **Link Status**
  Link Status displays the link state (“Up” or “Down”) of the port. If the port is disabled, it displays “Disabled”.
- **Speed**
  Speed displays the access speed in bit per second of the port. If the port is linked down, it displays“-“.
- **Duplex**
  Duplex displays the link-type (Full or Half) of the port. If the port is linked down, it displays“-“.
- **Flow Control**
  It is the state (On or Off) of the Flow Control.
- **Rx Byte**
  This is the total **received** frames formatted in byte.
- **Tx Byte**
  This is the total **transmitted** frames formatted in byte.
- **PoE** (PoE Model Only)
  PoE displaysthe PoE state (Delivery, No PD, Disabled, None) of the port. If the port does not support PoE function, it displays“None”.

  Note: This information is displayed on the system that supports the PoE function.

III-13. Web Management – IGMP Snooping

Internet Group Management Protocol (IGMP) is used in communicating among hosts and establishing a multicast group membership on the IPv4 networks (Layer 3). IGMP provides the ability to prune **multicast traffic** to those who need this kind of traffic and reduce the amount of traffic on the network. However, switches work on the MAC Layer (Layer 2) and are unable to obtain IGMP information. **IGMP Snooping** allows the switch to listen to the IGMP communication between hosts and routers, and maintains a table of multicast IPs and group members. **IGMP Snooping** can prevent the hosts on the LAN from receiving traffic from a non-joined multicast group and save bandwidth of the network.

CONFIGURE IGMP SNOOPING INFORMATION



For more information, hover the mouse over the icon in the system.

- **Basic Setting**
  - Mode
    "Enable" or "Disable" the IGMP Snooping function.

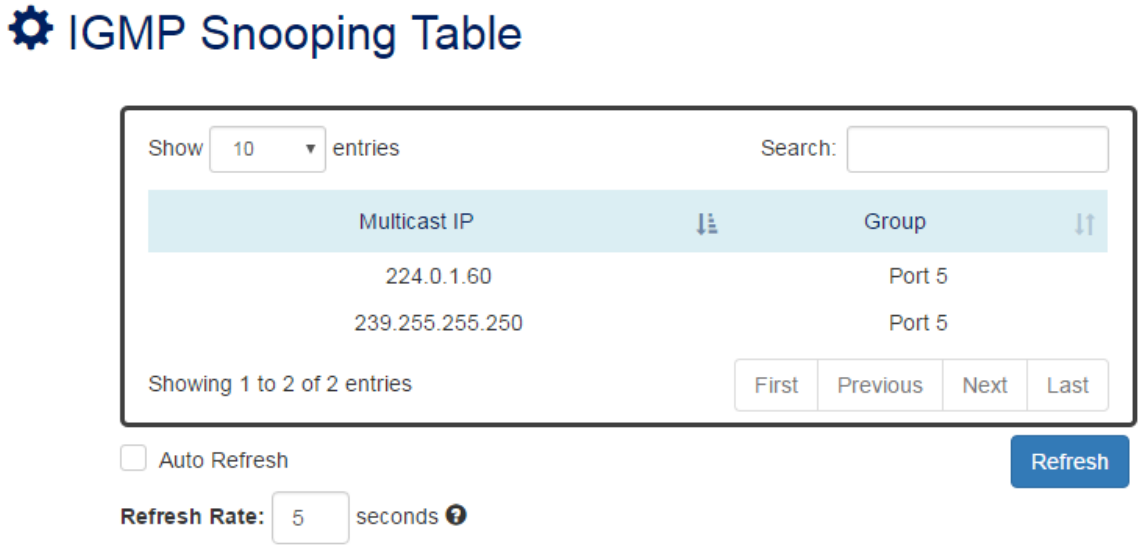
- **Querier Settings**
  - Querier Mode
    "Enable" or "Disable" the IGMP Snooping Querier function. If it is enabled, the system sends IGMP snooping **version 1 and 2** queries.
  - Querier Period
    This period is the interval to send the IGMP snooping queries.

    The range of theQuerier Period is **from 1 to 3600** seconds.

    The default Querier Period Interval is **125** seconds.
  - Query Max Response Time
    This is a timer to wait for the member response of the IGMP groups. It is used in **removing** the information of the IGMP groups if no member responds to the query.

- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

IGMP Snooping Table



- **Multicast IP**
  The Multicast IP is the IP address of the multicast group.

- **Group**
  The group shows the port number, which joined the group.

III-14. Web Management – 802.1Q VLAN

802.1Q VLAN

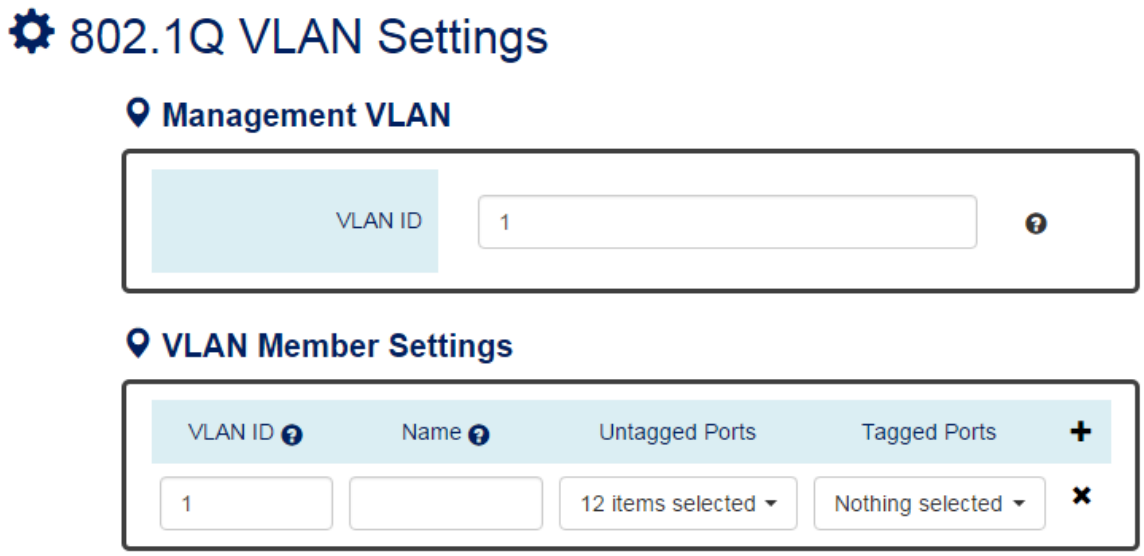
Virtual Local Area Network (VLAN) is a structure that can ease Network planning. The devices in a VLAN can be located anywhere without the restriction of physical connections, but work like they are on the same physical segment.

IEEE 802.1Q defines **VLAN tagging** conception for the Ethernet frames. VLAN tagging supports frames in the different VLAN groups transmitting on a link (called **VLAN trunk**). The maximum number of VLANs on the Ethernet network is 4096. TheVLAN 0 and VLAN 4095are for specific use and hence the usable VLAN number is **4094**.

VLAN Q-IN-Q

VLAN Q-in-Q, also called **Stacked VLAN**, is an extension for 802.1Q VLAN. It supports a maximum of 4096*4096 VLAN groups. VLAN Q-in-Q can apply a port to a provider, customer, or tunnel for different applications. The header of the stacked VLAN frame contains two 802.1Q Headers with different Ethertype (TPID). The TPID “0x88A8” is the outer tag by default and the TPID “0x8100” is the inner tag for 802.1Q VLAN. Customized ethertype called **Specific Provider Ethertype** are supported if one or more ports are set to “**Specific Provider**”.

CONFIGURE 802.1Q VLAN INFORMATION



For more information, move the mouse over the icon in the system.

Management VLAN

- VLAN ID
  The VLAN ID is for the native VLAN. Only the ports in the same VLAN as Management VLAN can **access the switch** configuration console via **Ethernet**.

  The range of theVLAN ID is **from 1 to 4094**.

  The default Management VLAN ID is **1**.

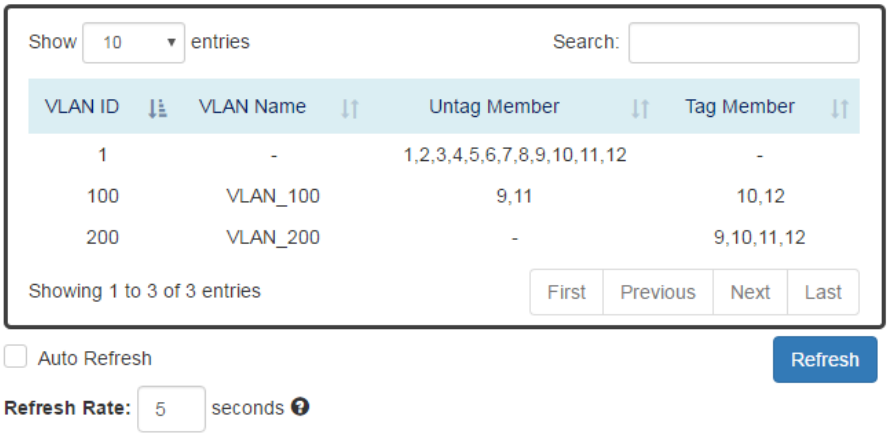
- **VLAN Member Settings**
  - VLAN ID
    Assigns a unique VLAN ID to this VLAN group.

    The range of the VLAN ID is **from 1 to 4094**.
  - Name
    Assigns a name to this VLAN group to identify the different VLANs.

    The **max.length** for the Name is **32 characters**.

    Note: #, \, ', ", ? are **invalid** characters.
  - Untagged Ports
    Sets the untagged ports for this VLAN group. The system **removes the VLAN tag** before transmitting from the port that is set to "**untagged**". Usually, this port is connected to the end device that belongs to this VLAN.
  - Tagged Ports
    Sets the tagged ports for this VLAN group. The system **keeps the VLAN tag** when transmitting from the port that is set to "**tagged**". Usually this port is connected to another switch and uses the VLAN tag to transfer the VLAN information.
  - ➕: Click the **plus icon** to add a VLAN Member row.
  - ✖: Click the **remove icon** to delete the VLAN Member row.

802.1Q VLAN TABLE



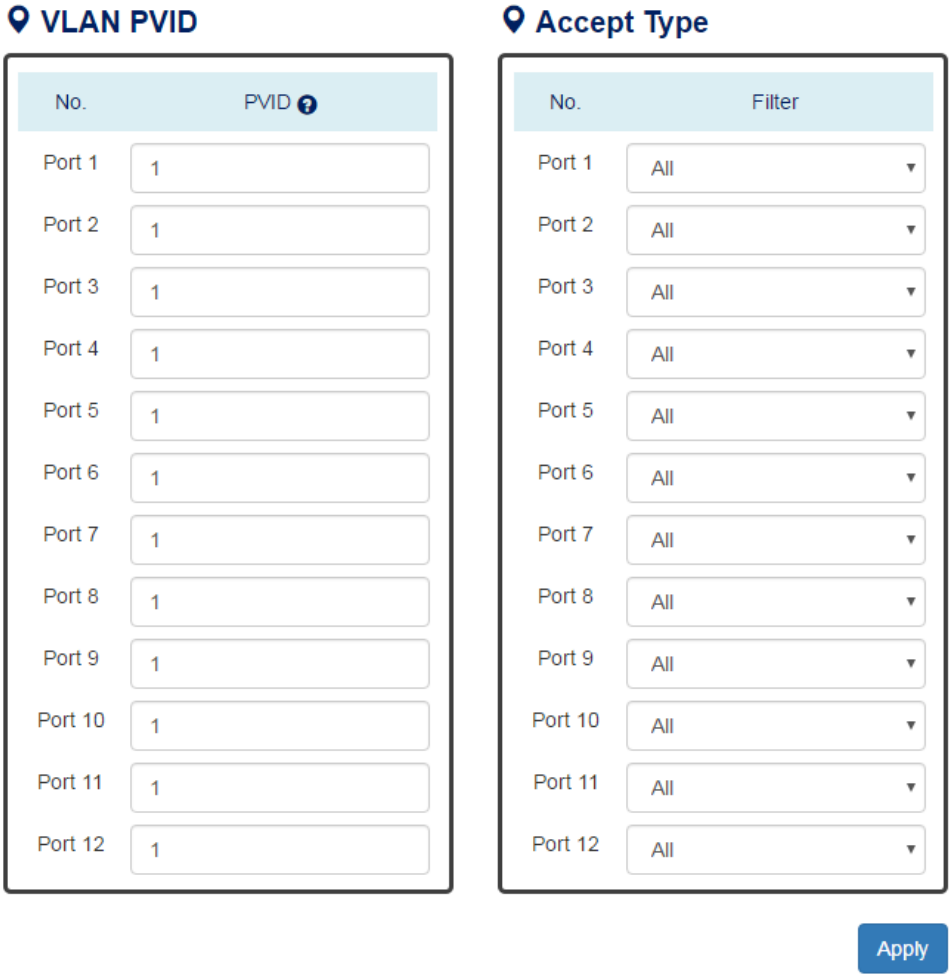
- **VLAN ID**
  This is the assigned unique **VLAN ID** for this VLAN group.

- **VLAN Name**
  This is the assigned **VLAN Name** for this VLAN group.

- **Untag Member**
  These ports are assigned as VLAN untagged ports.

- **Tag Member**
  These ports are assigned as VLAN tagged ports.

Configure 802.1Q VLAN PVID & Accept Type



For more information, move the mouse over the ? icon in the system.

- VLAN PVID
  - No.
    Port1 to PortN, where N is based on the total port number.
  - PVID
    Assign a VLAN ID to the frames without a VLAN tag that come into the specific port.

- Accept Type
  - No.
    Port1 to PortN, where N is based on the total port number.
  - Filter
    Three types of filters are provided: All, Tagged Only, Untagged Only.

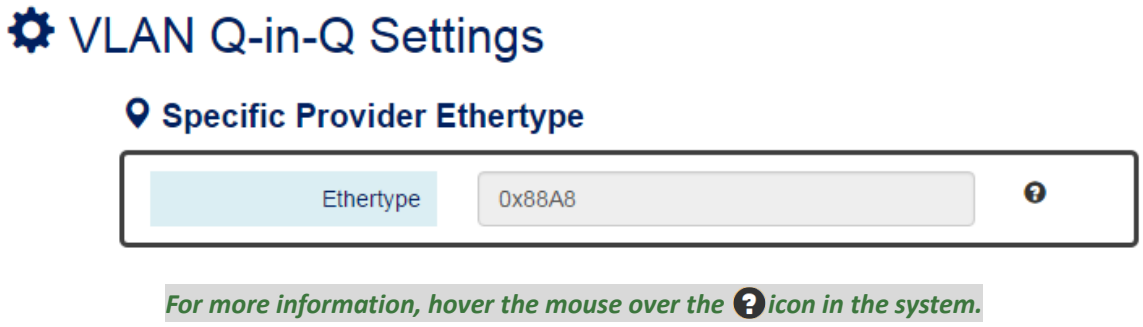
    All: Accept both tagged and untagged frames that come into the port.

    Tagged Only: Accept only tagged frames that come into the port.

    Untagged Only: Accept only untagged frames that come into the port.

- Apply (Apply Button)
  After configuring the above fields, click "**Apply**" button to make it effective.

CONFIGURE VLAN Q-IN-Q

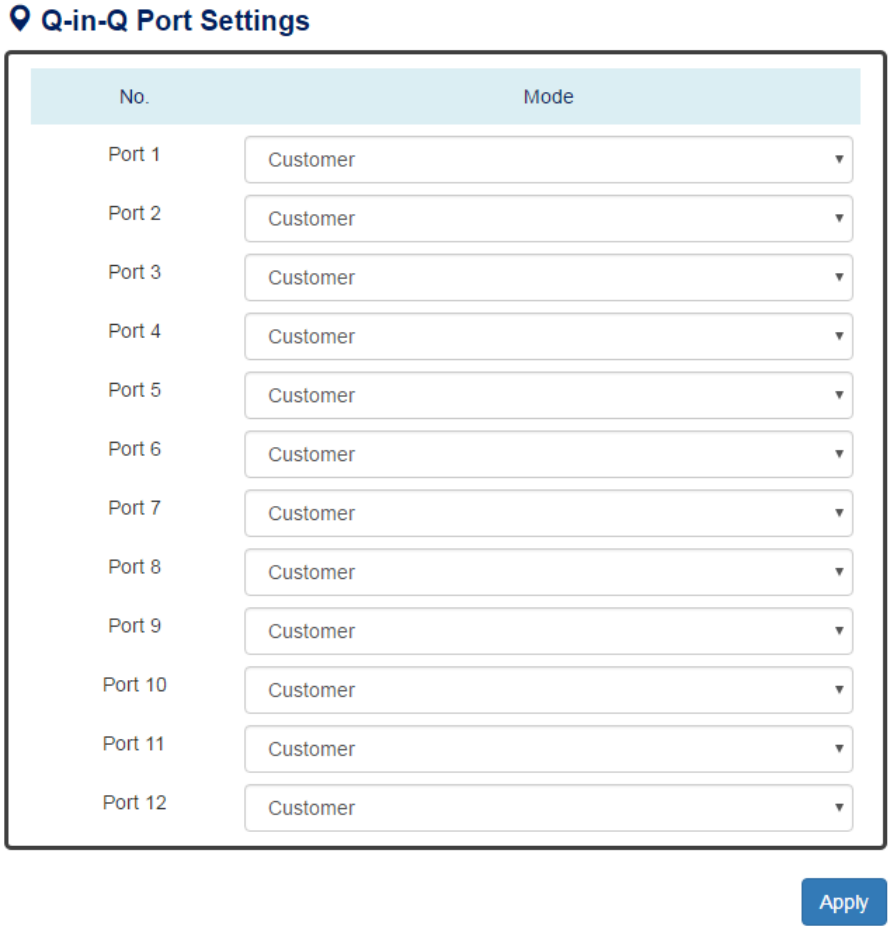


For more information, hover the mouse over the icon in the system.

- **Specific Provider Ethertype**
  This is a global configuration and an Ethertype is assigned for all ports, which are configured as "**Specific Provider**". This field is locked (disabled) until at least one port is configured to the "**Specific Provider**" in the "**Q-in-Q Port Settings**" section.

  The range of theProvider Ethertype is **from 0x0000 to 0xFFFF**,but **0x8100** is **invalid**.

  The defaultProvider Ethertype is **0x88A8**.



- **Q-in-Q Port Settings**
  - No.
    Port1 to PortN, where N is based on the total port number.
  - Mode
    Set the port to one of the Q-in-Q mode.
    The Egress is dependent on the connected device and hence the egress action is skipped.

Mode	Ingress

Q-in-Q Tunnel	**Untagged** Frames: Add TPID:0x88A8 tag and forward. **Tagged** Frames: 1. TPID:0x8100: Add TPID:0x88A8 tag and forward. 2. TPID:0x88A8: Forward the frames.

Mode	Ingress
Customer	A port set to “Customer” runs typically 802.1Q VLAN. **Untagged** Frames: Add TPID:0x8100 tag and forward. **Tagged** Frames: 1. TPID:0x8100: a. Same VLAN ID: Forward the frames. b. Different VLAN ID: Discard the frames. 2. TPID:0x88A8: Discard the frames.
Provider	**Untagged** Frames: Add TPID:0x88A8 tag and forward. **Tagged** Frames: 1. TPID:0x8100: Discard the frames. 2. TPID:0x88A8: a. Same VLAN ID: Forward the frames. b. Different VLAN ID: Discard the frames.
Specific Provider	Users define the Ethertype for the Provider service. **Untagged** Frames: Add the user-defined TPID tag and forward. **Tagged** Frames: 1. TPID:0x8100: Discard the frames. 2. TPID:0x88A8: Discard the frames. 3. TPID:[user-defined]: a. Same VLAN ID: Forward the frames. b. Different VLAN ID: Discard the frames.

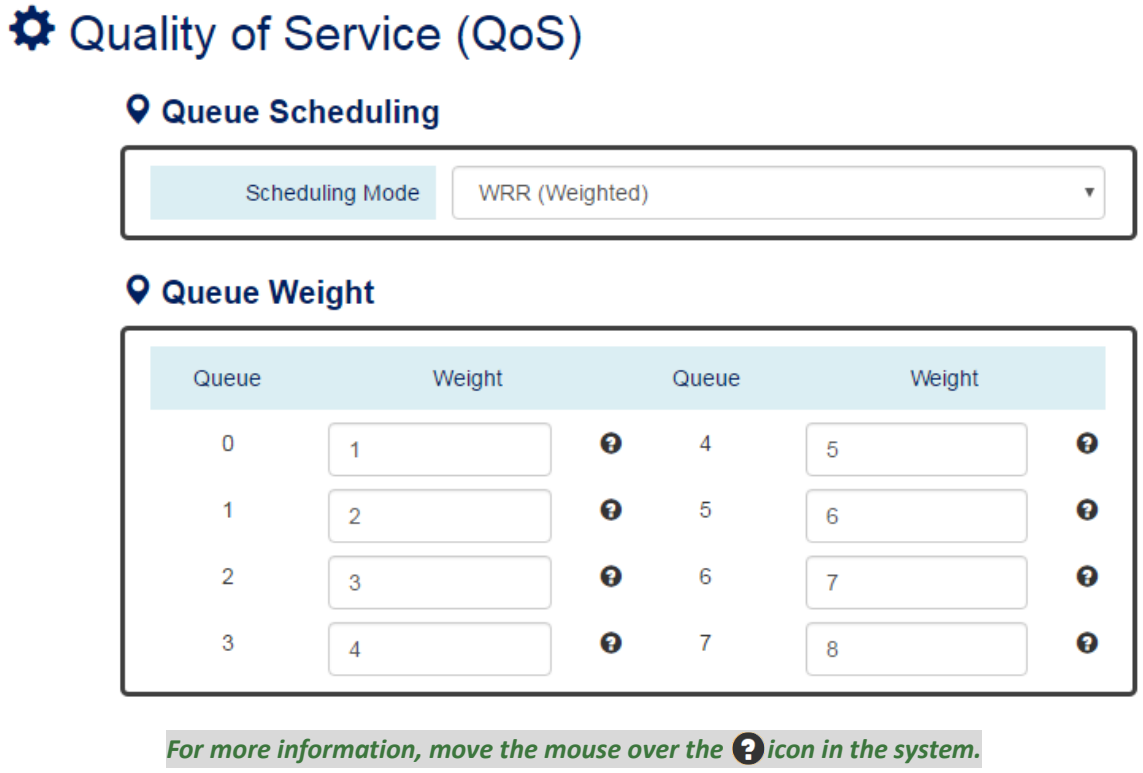
- Apply (Apply Button)

  After configuring above fields, click "**Apply**" button to make the changes effective.

III-15. Web Management – Quality of Service (QoS)

Quality of Service which known as **QoS** provides a stable and predictable transmitting service. It is useful to manage the bandwidth more efficiently based on the requirement of applications. Users are able to set **different priorities** for different traffics to satisfy the services which need a fixed bandwidth and have more sensitive of delay. **Quality of Service** can also optimize the restrict bandwidth resource and control the network traffic of the switches.

CONFIGURE QOS INFORMATION



For more information, move the mouse over the ? icon in the system.

- Queue Scheduling
  - Scheduling Mode
    Select the scheduling mode for the Quality of Service.

    WRR: **Weighted Round Robin**. WRR ensures that every queue takes turns to transmit the traffic by its weight.

    Strict: **Strict Priority Queue**. The traffic is transmitted based on the priority, which is from highest to lowest.

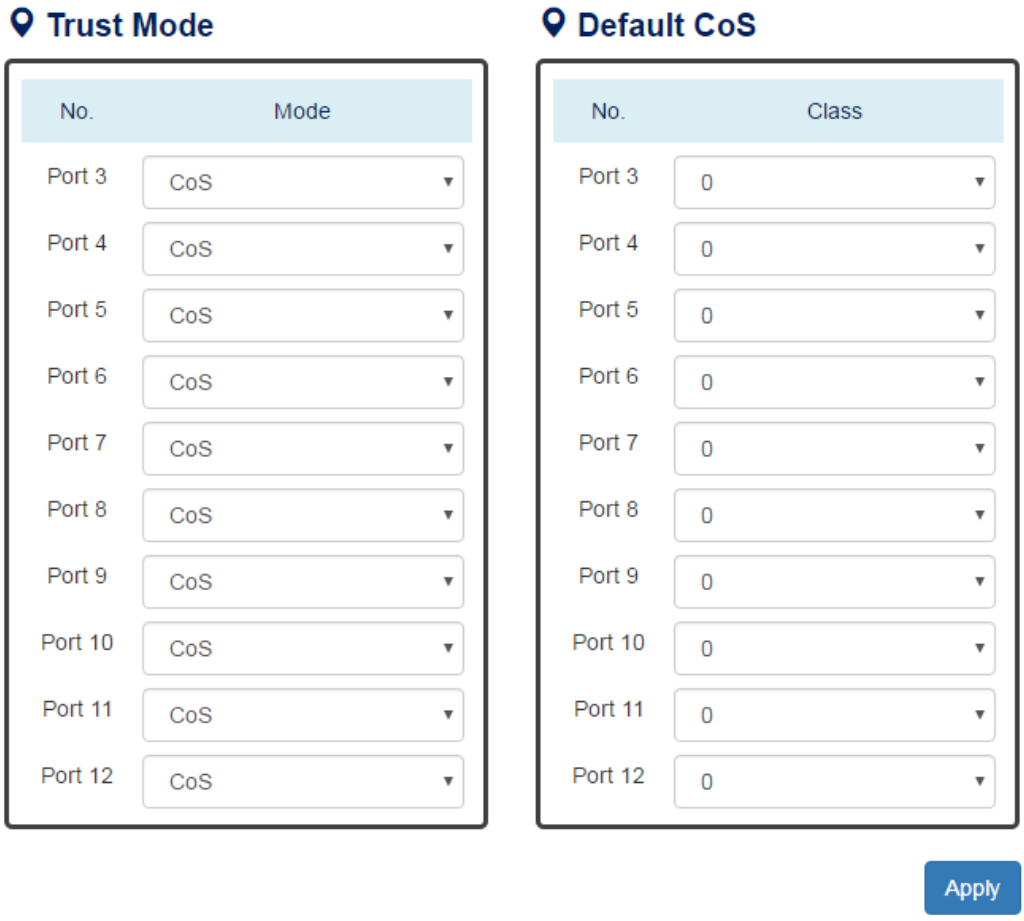
- **Queue Weight**
  - Queue
    Eight queues from queue 0 to queue 7 are supported.
  - Weight
    Enables you to configure a specific weight for the port.

    The range of the Weight is **from 1 to 100**. There is no need to sum all queues to 100.

    The default Weight for each queue is displayed in the table:

Queue	0	1	2	3	4	5	6	7
Weight	1	2	3	4	5	6	7	8

Configure QoS Trust Mode and Default CoS



- Trust Mode
  - No.
    Port1 to PortN, where N is based on the total port number.
  - Mode
    CoS: Class of Service. Use the 3-bit “PRI” field in the VLAN tag. It enables you to assign traffic to 8 different classes **from 0 to 7**.

    DSCP: Use 6-bit field “DSCP” in the Type of Service (ToS) tag. It enables you to assign traffic to 64 different types **from 0 to 63**.

- Default CoS
  - No.
    Port1 to PortN, where N is based on the total port number.

Class

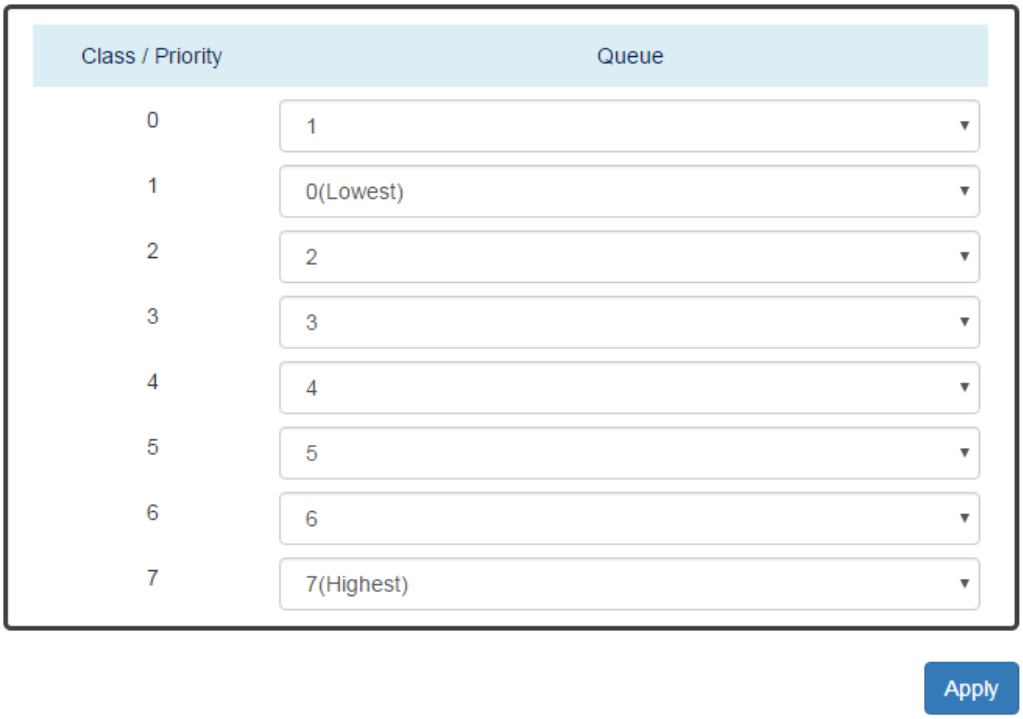
You can assign a default class to the port. The system follows the assigned CoS classes to transmit frames if there is **no VLAN tag** in the frame header.

The default Class for each port is **0**.

- Apply (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

CONFIGURE COS MAPPING



- **Class / Priority**
  There are **3 bits** for the "Class of Service" field called "**PRI**" in the VLAN tag and there are 8 classes **from 0 to 7**.

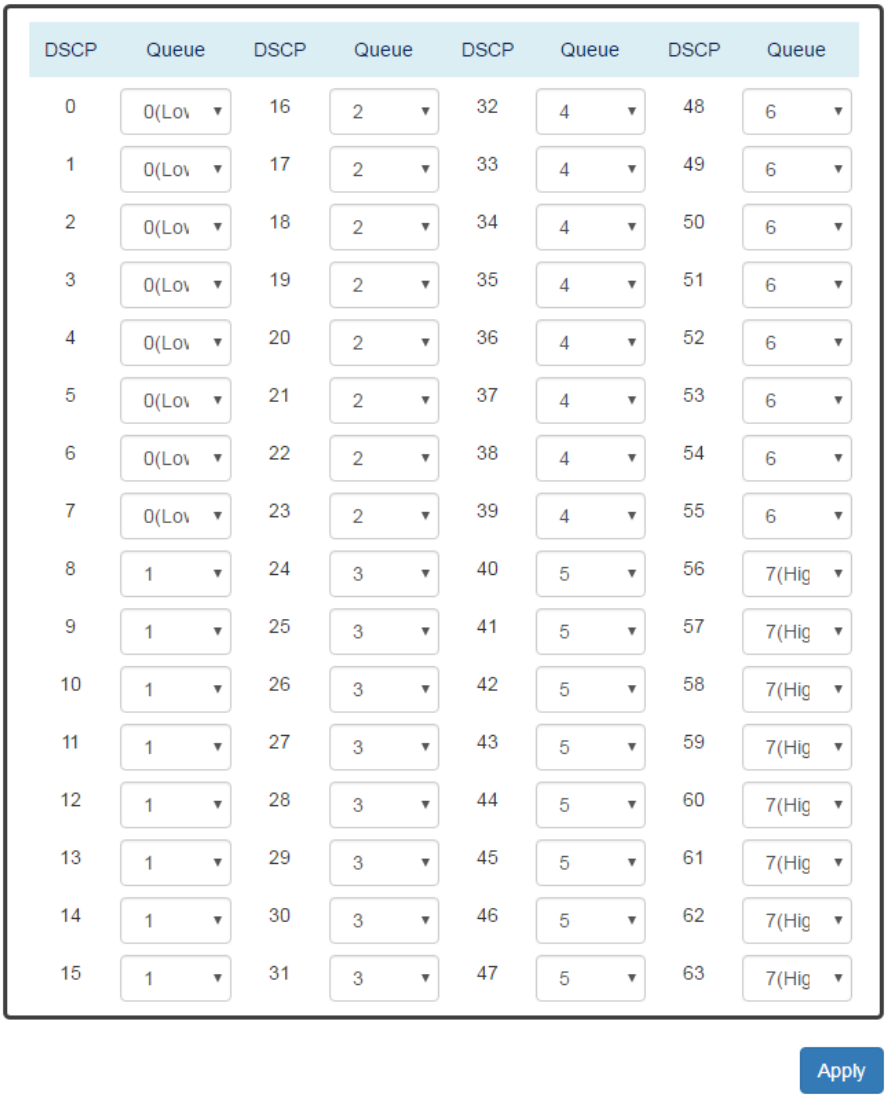
- **Queue**
  The chipset supports **8 queues from queue 0 to queue 7**. The queue 0 is the lowest priority queue and the queue 7 is the highest priority queue.

  The default Queue for each class is displayed in the table:

Class	0	1	2	3	4	5	6	7
Queue	1	0	2	3	4	5	6	7

Configure ToS Mapping

DSCP Mapping



- **DSCP**
  There are **6 bits** for the "**DSCP**" in ToS tag and hence there are 64 classes **from 0 to 63**.

- **Queue**
  The chipset supports **8 queues from queue 0 to queue 7**. The queue 0 is the least priority queue and the queue 7 is the highest priority queue.

  The default Queue for each type is displayed in the table:

Type	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
Queue	0	1	2	3	4	5	6	7

- 

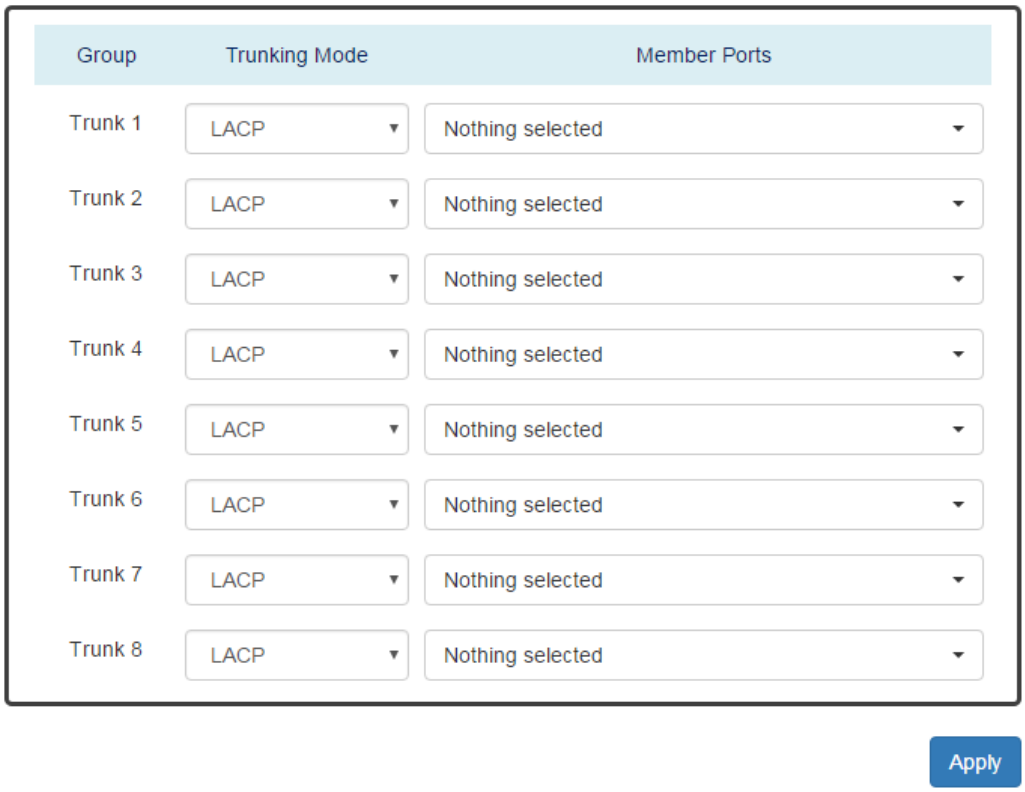
(Apply Button)

  After configuring above fields, click "**Apply**" button to make the changes effective.

III-16. Web Management – Port Trunk

Port Trunk is also known as **Link Aggregation**, and it is a protocol to group links to a trunk. A total of **8** trunk groups are provided. It is a good method to reach load balance and link backup. For example, when port 1 to port 4 are combined to trunk 1 and all ports support 100Tx and set to full-duplex, the bandwidth of the trunk will be 800Mbps. The traffic transmitting on the trunk is distributed to one of the link by the source **MAC address** to reach the load balance. When the trunk mode is set to LACP and when one of the link is broken, the traffic will transmit on another link on the group.

CONFIGURE PORT TRUNK INFORMATION



- **Group**
  Eight trunk groups from **Trunk 1** to **Trunk 8** are supported.

- **Trunking Mode**
  Two trunking modes are available: “LACP” and “Static”.

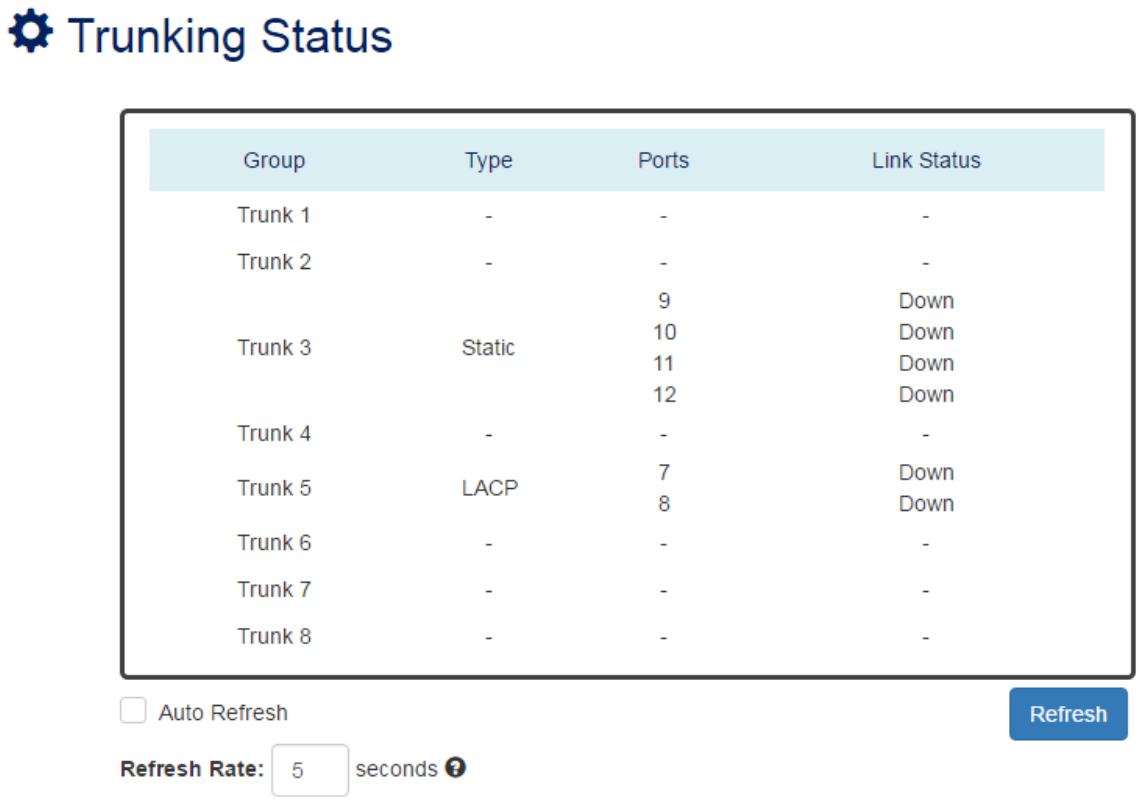
  Static: The traffic is transmitted on one of the links in the group. The link is determined by the MAC Address in the frame header. If the link is broken, the traffic cannot transmit on the other links in the group.

  LACP: It is also known as “Dynamic” trunking. If the current transmitting link is broken, the traffic can be transmitted on another link in the group.

- **Member Ports**
  The selected ports are joined in the Trunk group. A port can only be in one of the trunk group.

- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

PORT TRUNK STATUS



- **Group**
  The supported trunk groups are from **Trunk 1** to **Trunk 8**.

- **Type**
  The trunk mode set for this group maybe "**LACP**" or "**Static**". This field displays"-" if no members are in the group.

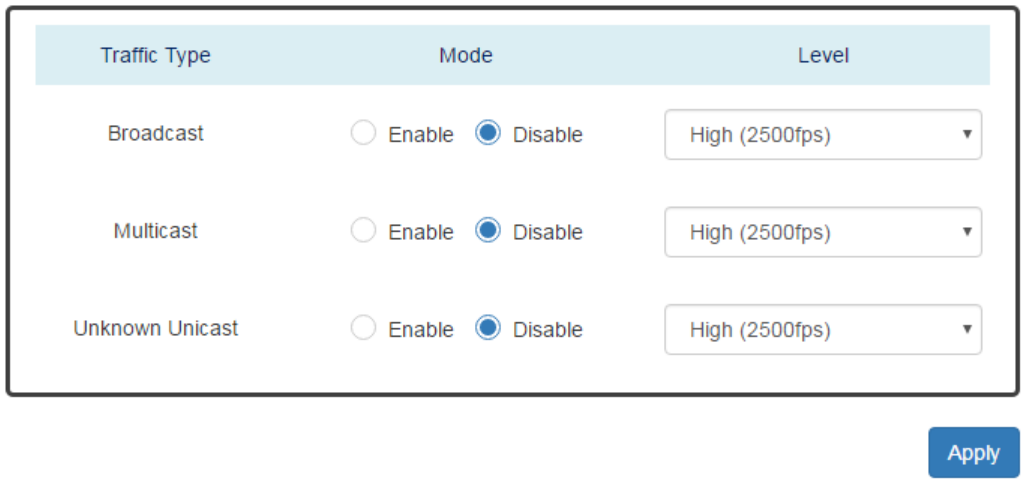
- **Ports**
  The selected member ports in the group will be displayed in this column.

- **Link Status**
  This field displays the link state (Up or Down) for the specific port.

III-17. Web Management – Storm Control

A traffic storm happens when there is excessive packets **flood** to the LAN and decreases the performance. The **Storm Control** function is used to prevent the system from breaking down by the broadcast, multicast, or unknown unicast traffic storm. When the **Storm Control** is enabled on the specific traffic type, the system will monitor the incoming traffic. If the traffic is more than the configured level, the traffic will be dropped to avoid the storm.

CONFIGURE STORM CONTROL INFORMATION



- **Traffic Type**
  Three types of traffics are supported in the Storm Control: **Broadcast**, **Multicast**, and **Unknown Unicast**.

- **Mode**
  “Enable” or “Disable” Storm Control function in the specific traffic type.

- **Level**
  Three frame levels are available: **High**, **Middle**, and **Low**. If the frames of specific traffic type are more than the set level, the system will drop the type of frames to prevent the system from breaking down.

  HIGH: MORE THAN 2500 FRAME PER SECOND.

  MID: MORE THAN 1000 FRAME PER SECOND.

  LOW: MORE THAN 500 FRAME PER SECOND.

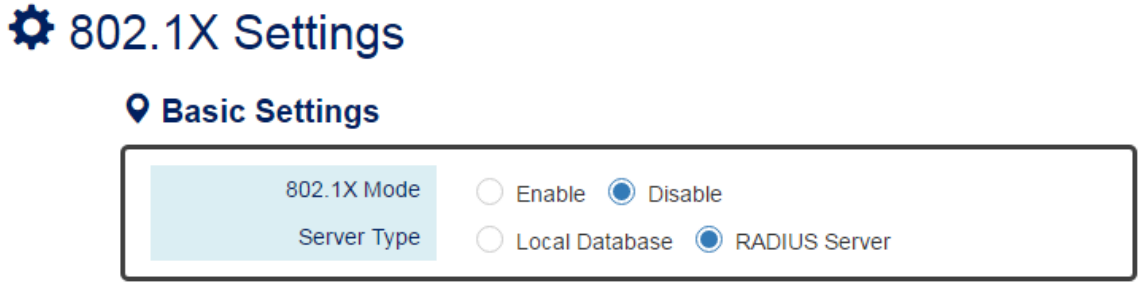
- 

(Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

III-18. Web Management – 802.1X

802.1X is an **IEEE** standard defined **Port-based Network Access Control**. It provides a more secured authentication mechanism for the devices, which would like to connect to a LAN or a WAN. The **Port-based** Network Access Control protocol is a convenient method for the users because the authentication is per-port and once the port passes the authentication, it is not required to authenticate again when changing to another device, i.e., without security. Therefore, **MAC-based** access control is provided. It is a more secure, but less convenient method for authentication. Only the device with the MAC Address that has passed the authentication can be added to the networks. These two methods are optional on each port and the users can select one of them on different ports.

CONFIGURE 802.1X BASIC INFORMATION



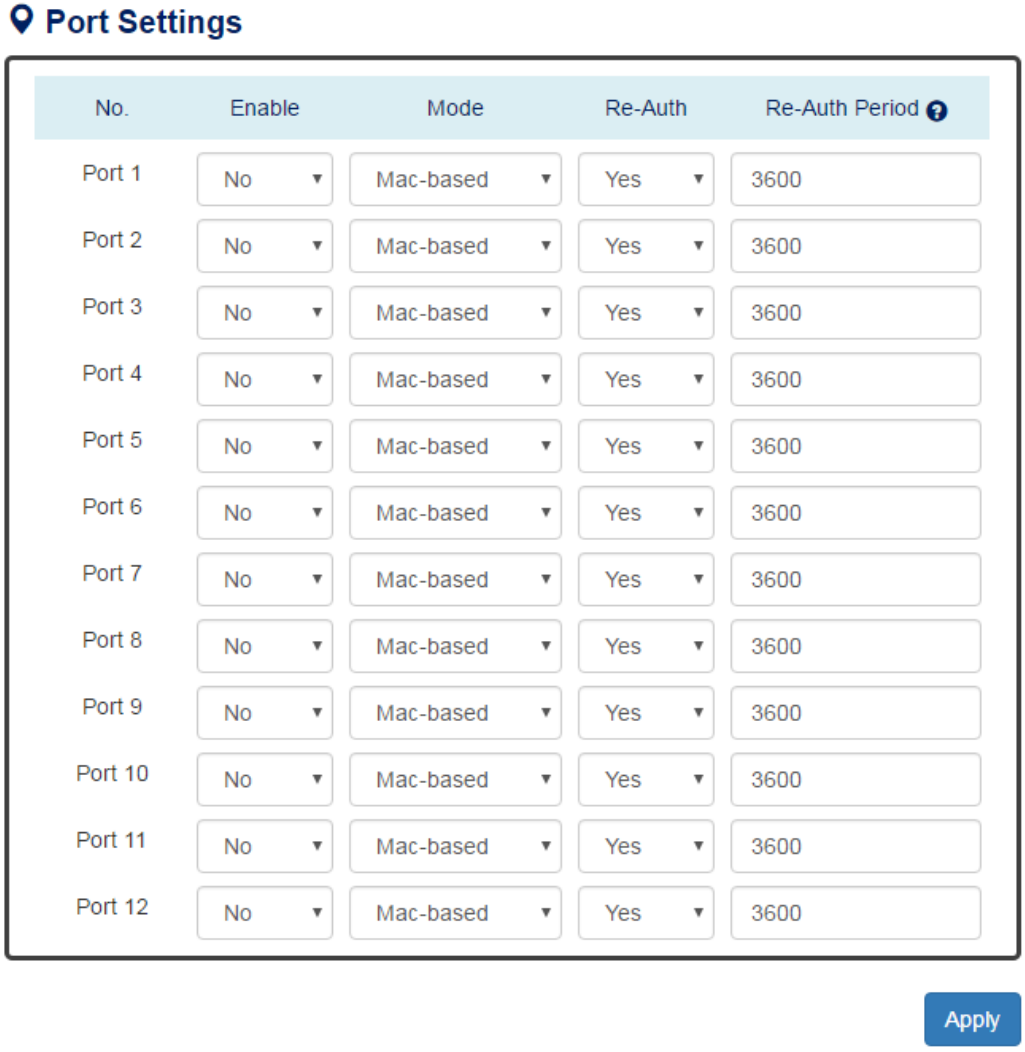
For more information, move the mouse over the icon in the system.

- **Basic Settings**
  - 802.1X Mode
    "Enable" or "Disable" 802.1X function on the switch.
  - Server Type
    Select the 802.1X server type to "Local Database" or "RADIUS Server".

    Local Database: The database is maintained in a table stored in the switch. The client has to send the username and password to authenticate with the switch's database.

    RADIUS Server: The database is maintained in other devices running RADIUS service. The authentication follows the RADIUS protocol including communication and encryption.

CONFIGURE 802.1X PORT INFORMATION



For more information, move the mouse over the icon in the system.

- **Port Settings**
  - No.
    Port1 to PortN, where N is based on the total port number.
  - Enable
    "Enable" or "Disable" 802.1X function on the port. "Yes" means 802.1X is enabled on the port and the port is locked until it passes the authentication.
  - Mode
    Select the 802.1X mode to "Mac-based" or "Port-based".

    Mac-based: Only the MAC Address, which passed the authentication, can connect to the networks.

    Port-based: If the port had passed the authentication, every device connected to the port can connect to the networks.

    Re-Auth

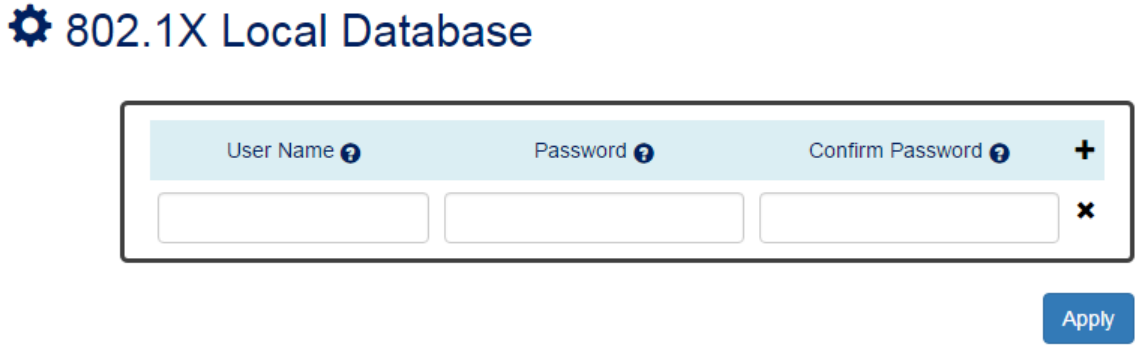
    "Enable" or "Disable" re-authentication on the port. "Yes" means re-authentication is enabled on the port and the port has to re-authenticate with the server every re-auth period.
  - Re-Auth Period

This is a time interval, which is used in re-authenticating the server.

- Apply (Apply Button)

  After configuring above fields, click "**Apply**" button to make the changes effective.

CONFIGURE LOCAL DATABASE INFORMATION



- **User Name**

  The User Name is used in authentication.

  The **max.length** for the User Name is **32 characters**.

  Note: #, \, ', ", ? are invalid characters.

- **Password**

  The Password is used in authentication.

  The **max.length** for the Password is **20 characters**.

  Note: #, \, ', ", ? are invalid characters.

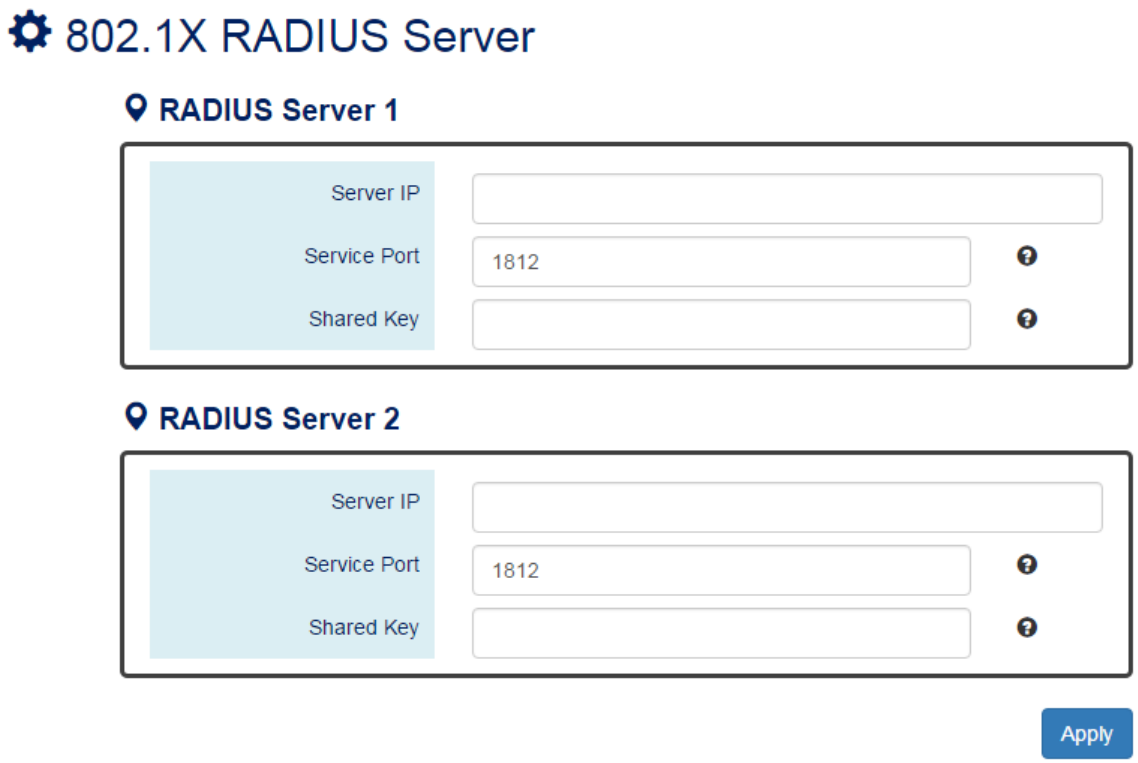
- **Confirm Password**

  The Confirm Password field must be the same as Password field.

- ➕: Click the **plus icon** to add a Username/Password row.
- ✖: Click the **remove icon** to delete the Username/Password row.
- Apply (Apply Button)

  After configuring above fields, click "**Apply**" button to make the changes effective.

Configure RADIUS Server Information



For more information, move the mouse over the icon in the system.

- **Server IP**

  The Server IP is the IP address of the server.

- **Service Port**

  The Service Port is the listening port on the RADIUS server.

- **Shared Key**

  The key is used in establishing the connection between the server and the authenticator before authentication.

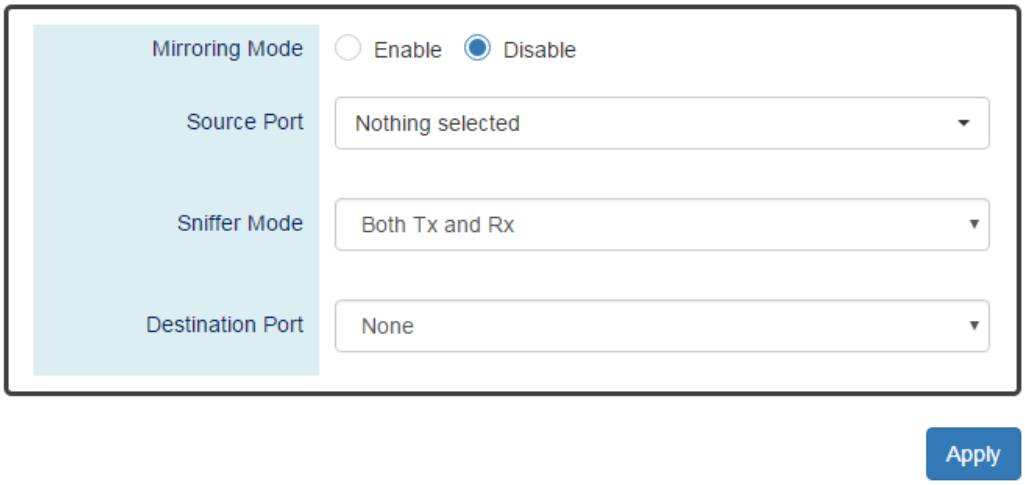
- Apply (Apply Button)

  After configuring above fields, click "**Apply**" button to make the changes effective.

III-19. Web Management – Port Mirroring

Port Mirroring is a feature that copies the incoming or outgoing packets on one or more ports to another destination port. It is very useful to monitor the network traffic and analyze the copied traffic. **Port Mirroring** helps network management to keep a close eye on the network and debug when some issues arise.

CONFIGURE PORT MIRRORING INFORMATION



- **Mirroring Mode**
  "Enable" or "Disable" the Port Mirroring function. If the user enables Port Mirroring function, the system will transmit the traffic of the specific "Sniffer Mode" from "Source Port" to "Destination Port".

- **Source Port**
  The traffic on the Source Ports will be sniffed to the Destination Port.

- **Sniffer Mode**
  Both Tx and Rx: Sniffs both transmitting and receiving traffics.

  Tx Only: Sniffs only the transmitting traffic.

  Rx Only: Sniffs only the receiving traffic.

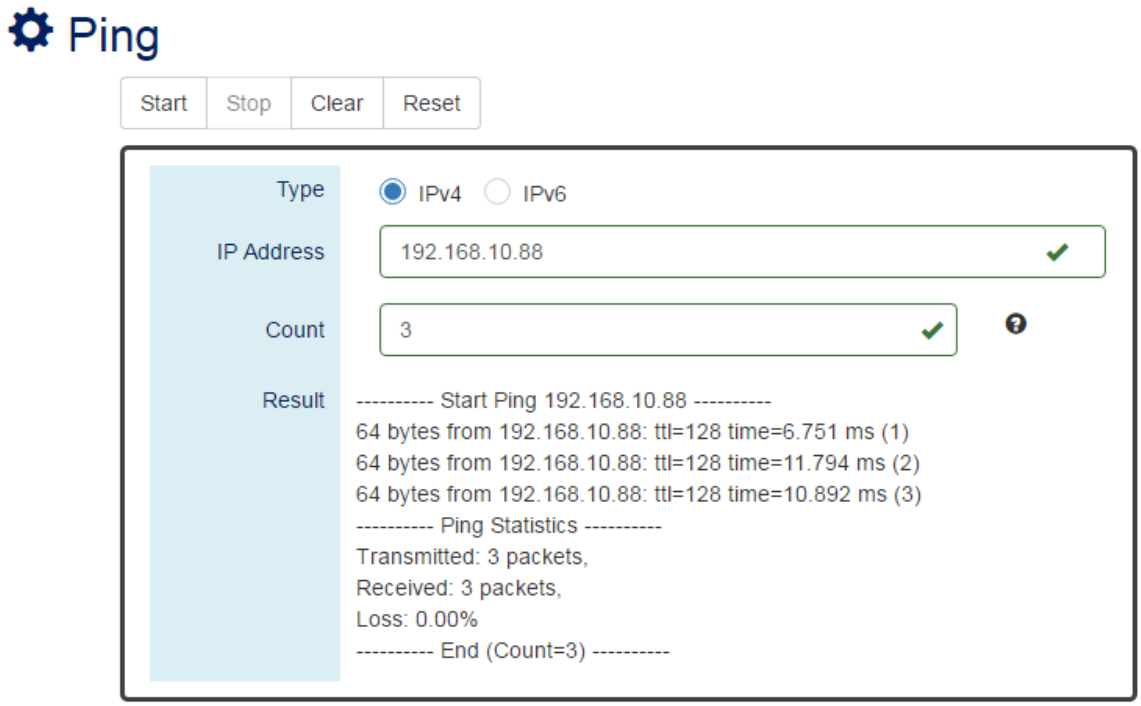
- **Destination Port**
  The traffic will sniff to the Destination Port. This port is usually connected to a host running the software to observe the packets.

- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

III-20. Web Management – Ping

Ping is a tool used to test the reachability of a device on the IP network. Ping is enabled by sending **Internet Control Message Protocol** (**ICMP**) request to the target device and waits for the response packet from the target device to check the connection.

PING ANOTHER DEVICE WITH IPV4/IPV6



For more information, move the mouse over the icon in the system.

- **Type**
  Ping a connected device with "**IPv4**" or "**IPv6**" protocol.
- **IP Address**
  The IP address of the connected device is verified based on the type.
- **Count**
  Sets the count times. The system will send "Count" number ICMP packets to the specific IP address and wait for the response.

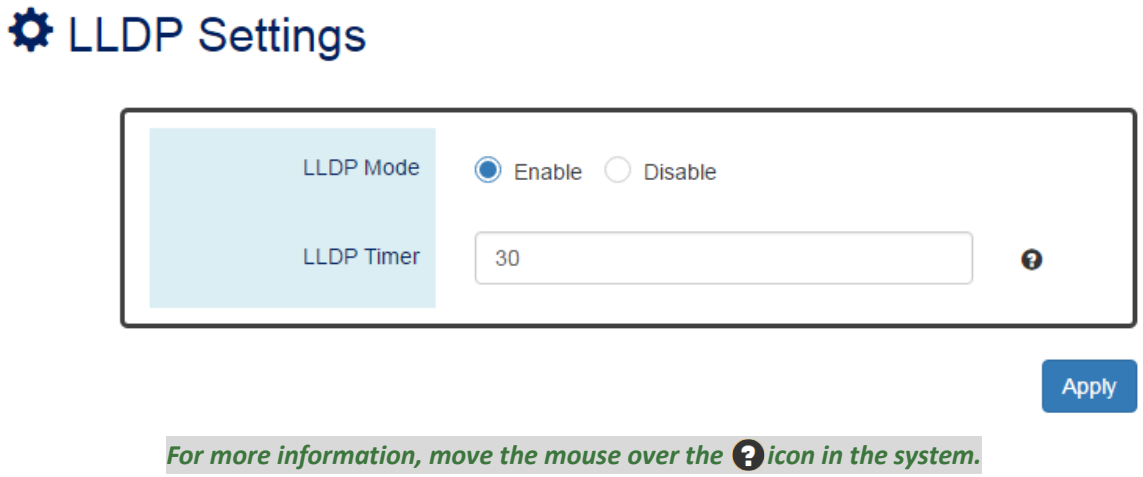
  The range of the Count is **from 3 to 50**.

  The default Count is **3**.
- **Result**
  The result of the ping shows the response from the specific IP address. If the specific IP address does notrespond, it dispalys No Response.
- **"Start" Button**
  Click the "Start" Button to start the ping to the IP address.
- **"Stop" Button**
  Click the "Stop" Button to stop the ping to the IP address before the count is completed.
- **"Clear" Button**
  Click the "Clear" Button to clear the "Result".
- **"Reset" Button**
  Click the "Reset" Button to clear the "Result" and reset the "IP Address" and "Count" number.

III-21. Web Management – LLDP

LLDP is **Link Layer Discovery Protocol** and it is a vendor-neutral layer 2 protocol that is defined by **IEEE 802.1AB**. **LLDP** is used in advertising identity of the devices, capabilities and neighbors on the LAN. The information from the neighbors enables the switch to quickly identify the devices and interoperate with each other more smoothly and efficiently. The neighbor table shows the information about the device that is next to the port. The LLDP can only get information from the device that is close to it. If the users want to know the topology of the LAN, they can collect all information from the device and analysis the neighbor table.

CONFIGURE LLDP INFORMATION



For more information, move the mouse over the icon in the system.

- **LLDP Mode**
  "Enable" or "Disable" the LLDP function.

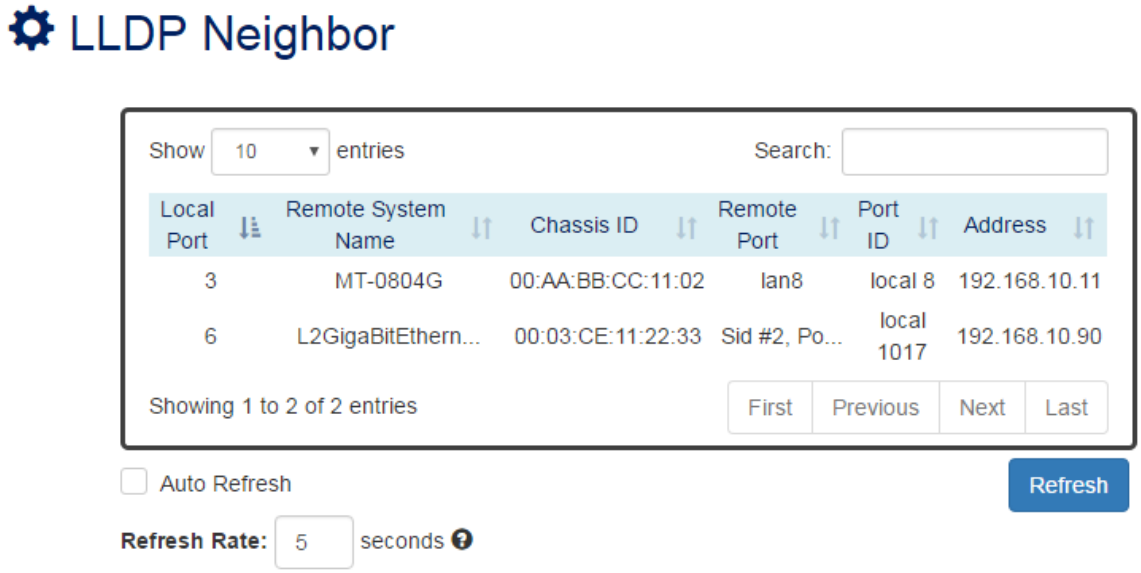
- **LLDP Timer**
  The LLDP Timer is a time interval to send LLDP messages.

  The range of the LLDP Timer is **from 5 to 32767** seconds.

  The default LLDP Timer is **30** seconds.

- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

LLDP Neighbor Table



- **Local Port**
  The port connected to the LLDP neighbor on the local switch.

- **Remote System Name**
  This is the system name of the LLDP neighbor. This value is set and provided by the remote device.

- **Chassis ID**
  The Chassis ID defines the **MAC Address** of the LLDP neighbor.

- **Remote Port**
  This field displays the **port information** received from the LLDP neighbor.

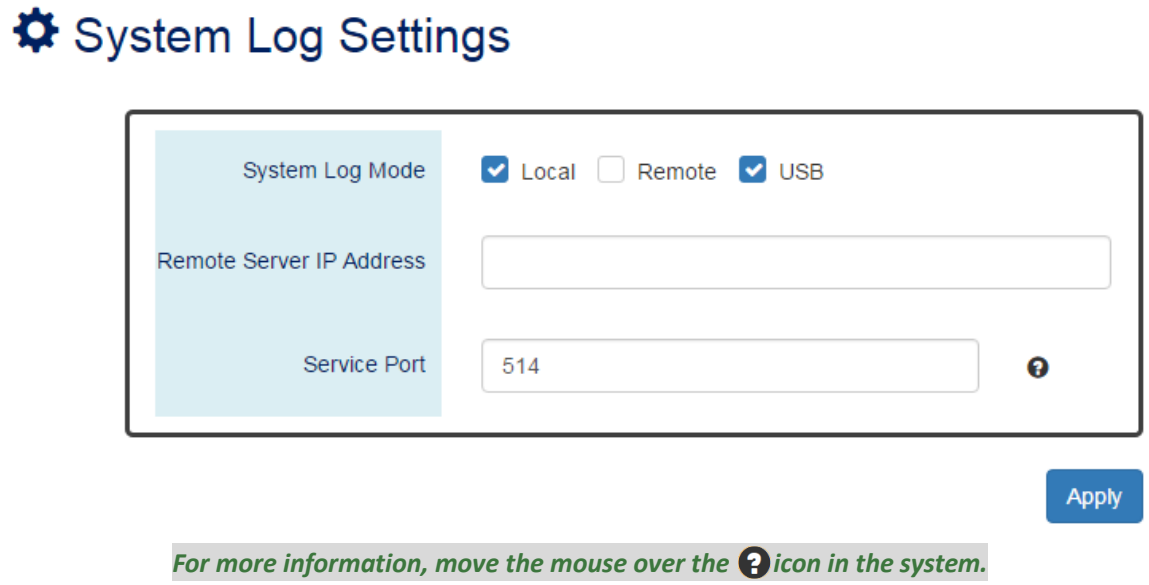
- **Port ID**
  The Port ID displays the **port identity** of the connected port on the LLDP neighbor.

- **Address**
  The Address displays the **IP address** of the LLDP neighbor.

III-22. Web Management – System Warning

System Warning contains “System Event Log”, “SMTP Settings”, and “Event Selection” for different types of services such as “Fault Alarm”, “System Log”, “SMTP”, and “SNMP Trap”. These logs are very useful for the administrator to manage and debug the system. When the system is powered off or when someone tries to login the system or the system reboots abnormally, or when some of the interfaces are linked down, the system sends log messages to notify specific users and record the events on the server or assigned platform. Users can also connect an alarm buzzer to the relay alarm pins. When the configured “Fault Alarm” events are triggered, the alarm buzzer will ring to notify the users.

CONFIGURE SYSTEM WARNING INFORMATION



For more information, move the mouse over the icon in the system.

- **System Log Mode**
  The port connected to the LLDP neighbor on the local switch.

- **Remote Server IP Address**
  The field contains the IP Address of the remote server. If the “**Remote**” mode is enabled, users have to assign this IP Address to receive the system logs.

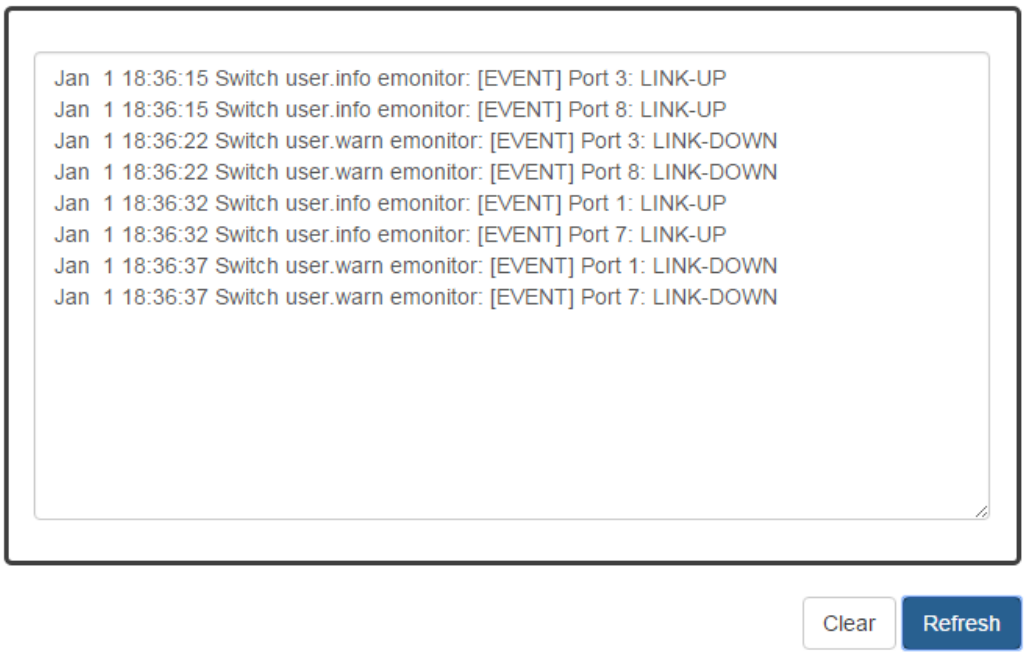
- **Service Port**
  The port is used to listen to the system log packets on the remote server.

  The range of the Service Port is **from 1 to 65535**.

  The default Service Port is **514**.

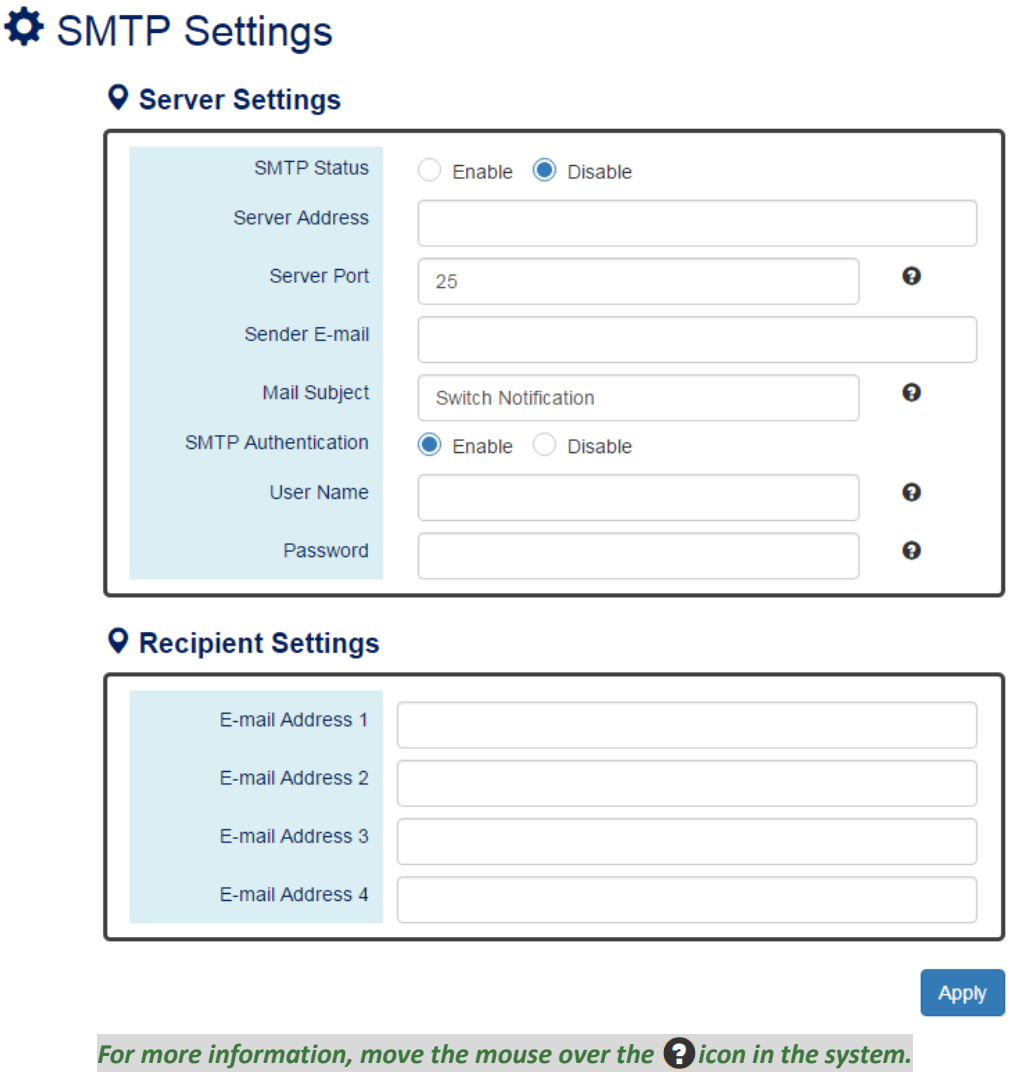
- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

System Event Log



- **Log Text Area**
  The system event information displays if the "**Local**" system log mode is enabled and the configured events are triggered.
- Clear (Clear Button)
  Click the "Clear" button to clear the system event log in the text area.
- Refresh (Refresh Button)
  Click the "Refresh" button to refresh the system event log in the text area.

CONFIGURE SMTP INFORMATION



For more information, move the mouse over the ? icon in the system.

- **Server Settings**
  - SMTP Status
    "Enable" or "Disable" the SMTP function.
  - Server Address
    This is the **IP address** or **URL** of the SMTP Server. For example, the SMTP server address provided by Google is "smtp.gmail.com".
  - Server Port
    This field is the port listening on the server for the SMTP request. For security, we suggest users configure the server port to **465** for **SSL** or **587** for **TLS**.

    The range of the Service Port is **from 1 to 65535**.

    The default Service Port is **25**. Port 25 is the default port for e-mail server.
  - Sender E-mail
    The Sender E-mail is the e-mail address used to send the notifications to Recipients.
  - Mail Subject
    The Mail Subject is a string that is displayed in the E-mail title.

    Note: #, \, ', ", ? are **invalid** characters.
  - SMTP Authentication

"Enable" or "Disable" to authenticate the SMTP server with the configured username and password.

- User Name
  The username is used in authentication with the SMTP server.

  The **max.length** for the User Name is **32 characters**.

  Note: #, \, ', ", ? are **invalid** characters.
- Password
  The password is used in authentication with the SMTP server.

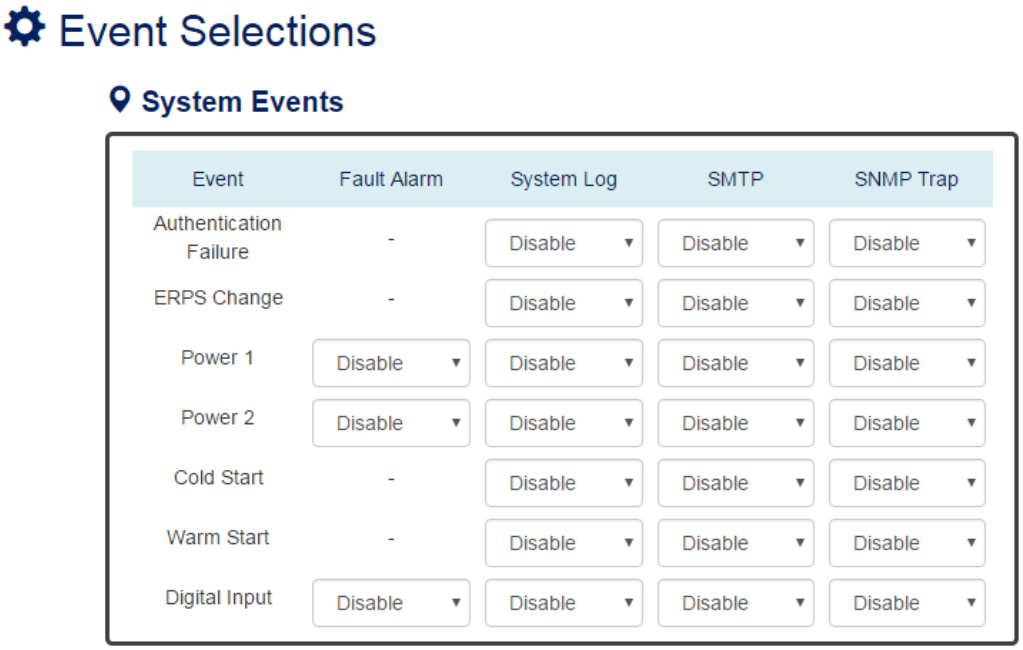
  The **max.length** for the Password is **32 characters**.

  Note: #, \, ', ", ? are **invalid** characters.

- **Recipient Settings**
  - E-mail Address 1-4
    The configured e-mail address will receive the notifications if the SMTP is enabled and the events set on "Event Selection" are triggered.
- Apply (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

CONFIGURE EVENT SELECTIONS



- **Event**

  There are 5 events on the System Events.

  Authentication Failure: Login failed on the web console or CLI. It maybe caused due to incorrect username or password.

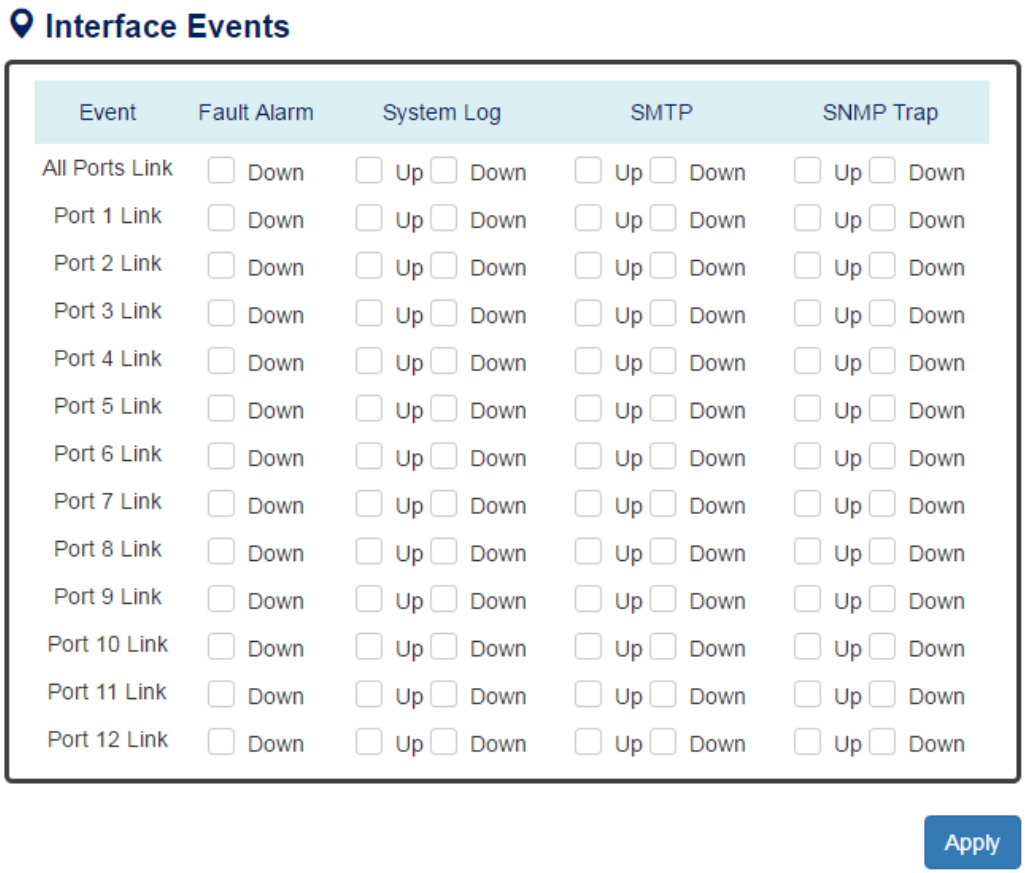
  ERPS Change: The ERPS function is working and the topology is changed.

  Power 1 or 2:The power 1 or 2 is powered off.

  Cold Start: The system reboots due to interruption of power supply.

  Warm Start: The system reboots by issuing “reboot” command on CLI or clicking the “reboot icon” on the web console.

  Digital Input: The signal from the digital input is changed from high to low or low to high.



- **Event**
  The events on the "Interface Events" display the **link status** for each port. Fault Alarm is triggered only during link down and other system log types support both link up and link down.

- **Fault Alarm**
  The **Fault LED** will turn on **red** and relay will turn ON, if the configured events are triggered. By default, the Fault LED is **green** and relay is turned OFF in the normal situation,.

- **System Log**
  When the configured events are triggered, the logs will be displayed in the "System Event Log" page, remote server, or saved to a USB file named "**message**". This is based on the settings of the "**System Log Mode**" in the "**System Log Settings**" page.

- **SMTP**
  If the SMTP is enabled and the configured events are triggered, the system will send an e-mail notification to the e-mail addresses of the assigned recipient set in the "**SNMP Settings**" page.

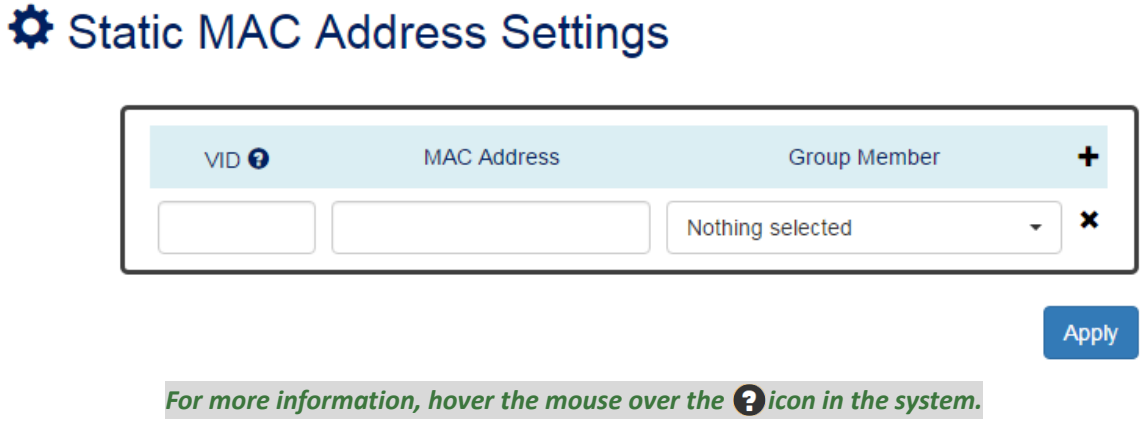
- **SNMP Trap**
  If the SNMP Trap is enabled and the configured events are triggered, the system will send event information to the assigned "**Trap Receiver IP**", which is set in the "**SNMP Trap**" page.

- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

III-23. Web Management – MAC Table

MAC address is **Media Access Control** address, which is used in layer 2 switching. A **MAC Address table** is maintained by the switch to transmit frames more efficiently. When the switch receives a frame, the system will check the MAC table and forward the frame to the corresponding port. The MAC Address table is built dynamically by the received frames and when the system receives a frame with an unknown MAC address, it **floods** the frame to all LAN ports in the same VLAN. When the destination device replies the system identifies the MAC Address and the target port.

CONFIGURE STATIC MAC ADDRESS INFORMATION



For more information, hover the mouse over the icon in the system.

- **VID**
  The VID is the VLAN group ID, which contains the configured MAC Address.

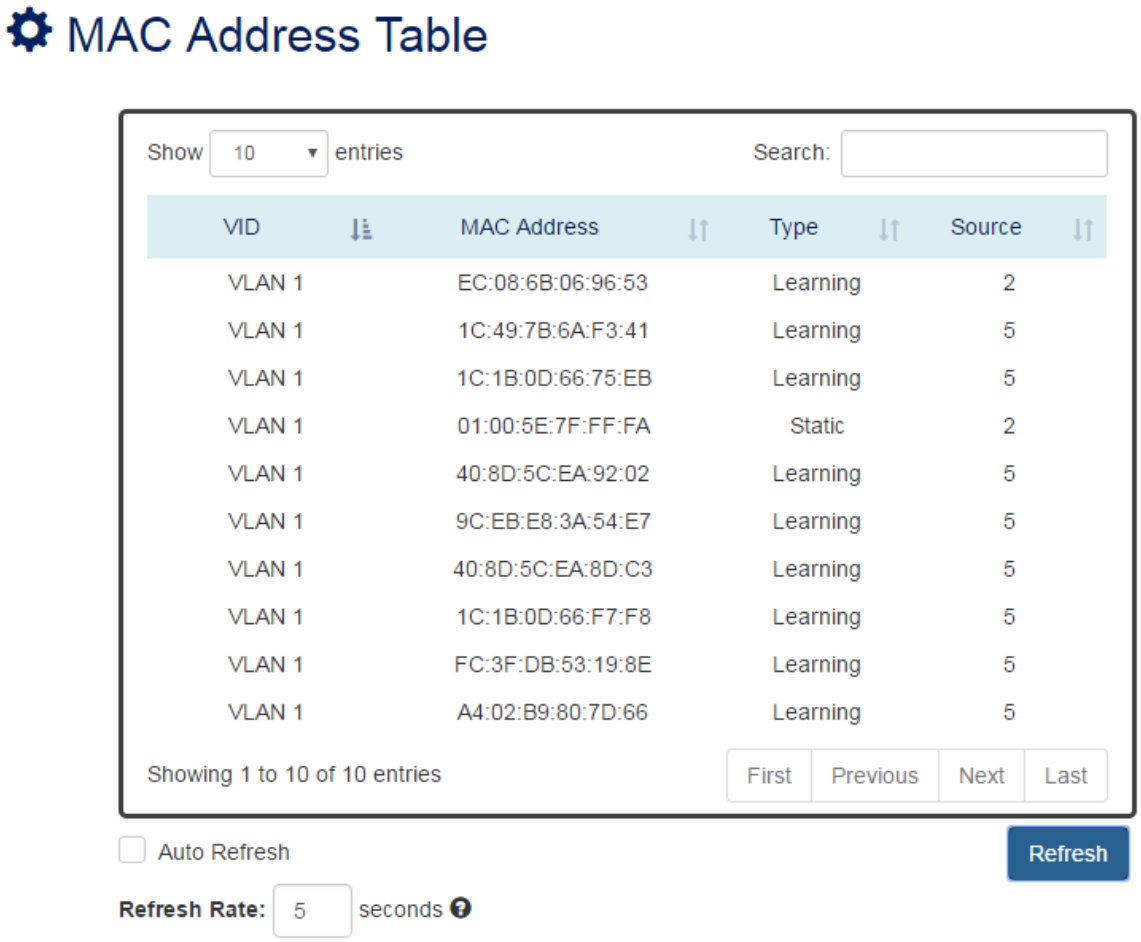
  The range of the VID is **from 1 to 4094**.

- **MAC Address**
  This field is the static MAC Address of the configured member ports in the VLAN group.

- **Group Member**
  The Group Member is the port(s) in the VLAN group, to which the configured MAC Address belongs.

- ➕: Click the **plus icon** to add a static MAC Address row.
- ✖: Click the **remove icon** to delete the static MAC Address row.
- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

MAC Address Table



- **VID**
  The VID is the VLAN group ID, which contains the configured MAC Address.

- **MAC Address**
  The MAC Address column displays the learnt or configured MAC Addresses.

- **Type**
  The Type column displays the type (Learning or Static) of the MAC Address.

  Learning: The MAC address is learnt from the transmitting frames.

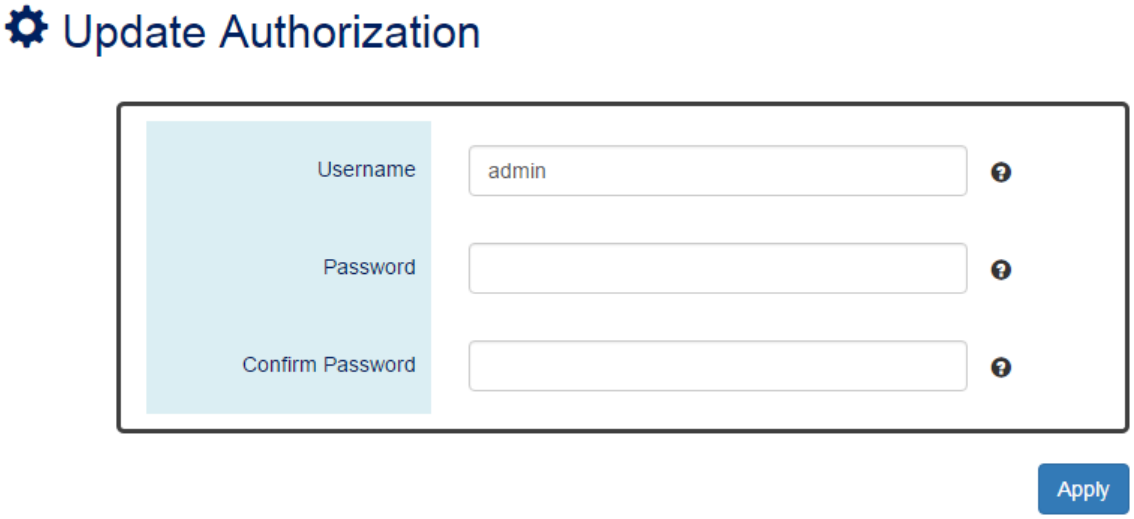
  Static: The MAC Address is configured by the users or the system.

- **Source**
  The Source column displays the port(s) to which the MAC Address belong.

III-24. Web Management – Authorization

The "**Username**" and "**Password**" are very important information both in the "**Command Line Interface**" or "**Web Console**". Users have to login into the system before doing any configuration. We strongly suggest the users to change at least the password **for security** when they are going to use this device.

CONFIGURE LOGIN INFORMATION



For more information, move the mouse over the ? icon in the system.

- **Username**
  The account used to login to the system.

  The maximum length of the Username is **20** characters

  Only **alphabet** (A-Z, a-z) and **numbers** (0-9) are allowed.

  The default Username is **admin**.

- **Password**
  The password used to login to the system.

  The maximum length of the Password is **20** characters.

  Only **alphabet** (A-Z, a-z) and **numbers** (0-9) are allowed.

  The default Password is **admin**.

- **Confirm Password**
  It is used to confirm the value specified by the users in the "Password" field. The value of the field must be the same as "Password".

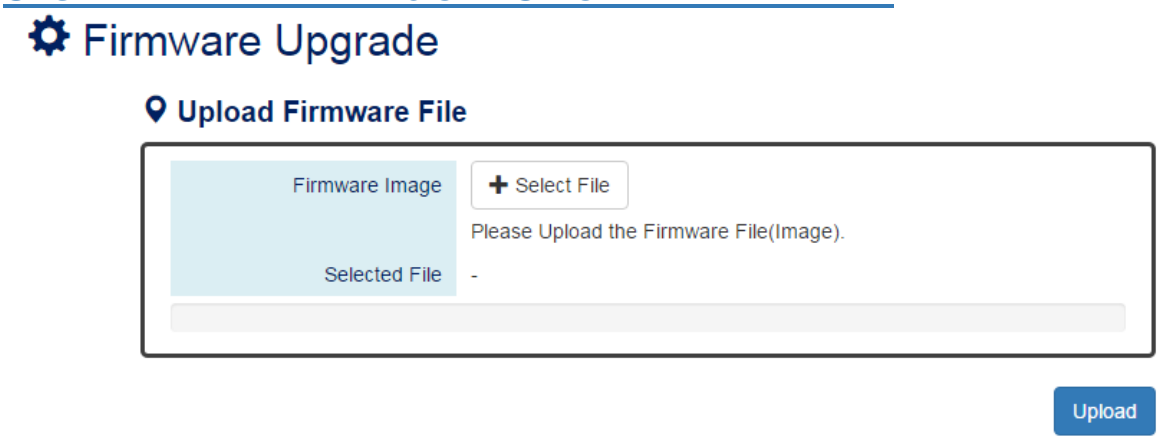
- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

III-25. Web Management – Firmware Upgrade

For a better performance and wider industrial applications, we constantly develop new features and revise the issues from the users. We suggest the users to upgrade the system to the newest firmware version to have a better user experience.

We provide 2 ways to upgrade the firmware from the Web Console, - one is saving the firmware file in the USB stick and another one is save the firmware file on the PC. If the firmware file is on the PC, the users will have to only **select the file** and click **Apply** button, for the system to upgrade it automatically.

UPGRADE FIRMWARE VERSION - UPLOAD FIRMWARE FILE



- **Firmware Image**
  Click the "**Select File**" button to select the firmware image provided by the sales or support.

  The **Firmware Version** displayed on the system can be customized by the **file name**. For example, if you want the version to be called as 1.2.3, you only need to modify the file name to XXX-**v1.2.3** (XXX is the original file name).

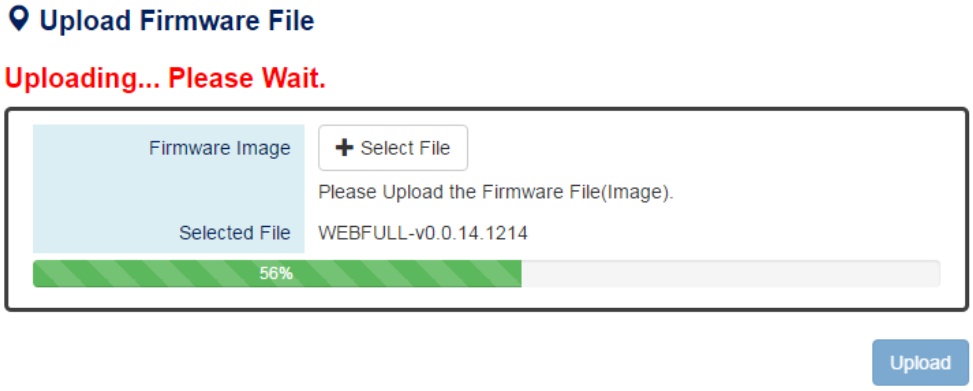
- **Selected File**
  After selecting a firmware image to be uploaded, the **selected file name** will be displayed in this field.

- Upload (Upload Button)
  After selecting the firmware image, click "Upload" button to upload it.

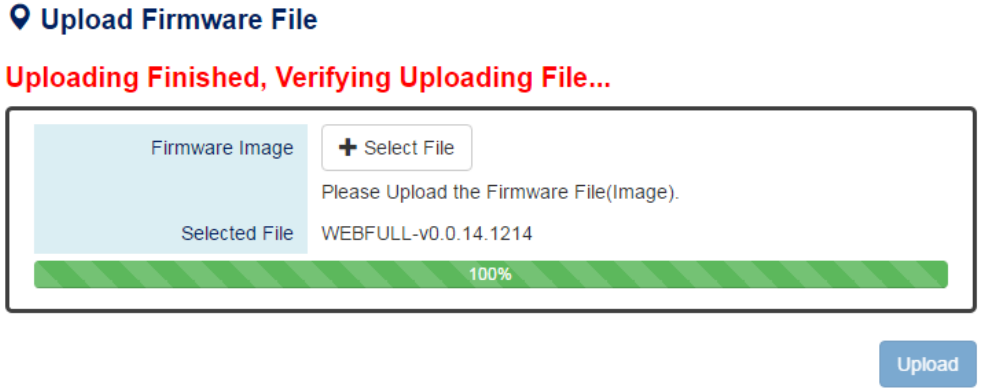
UPGRADE FIRMWARE PROCESS - UPLOADING FIRMWARE FILE

The following steps are performed when the system starts to upgrade after the "Apply" button is clicked:

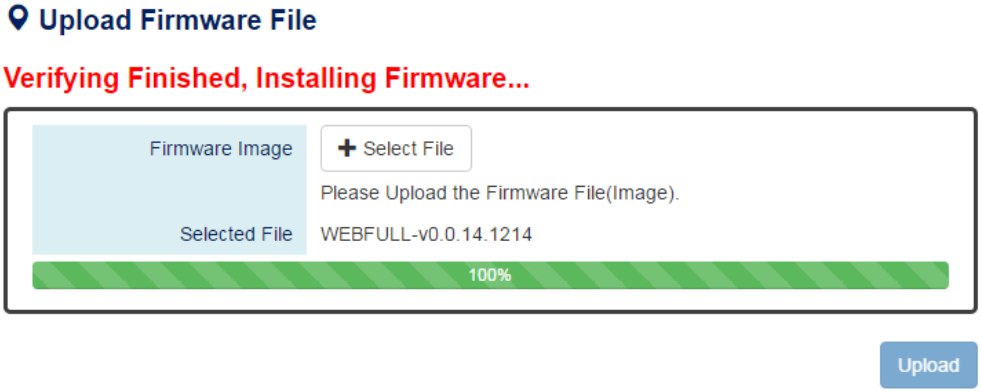
1. **Uploading** the firmware image
   The progress bar displays the uploading percentage.



2. **Verifying** the uploaded file
   When the file is **100%** uploaded, the system starts to **verify** the uploaded file to make sure it is **valid**. By default, the firmware image is encrypted to prevent the attack on man-in-the-middle. Optionally, higher encryption methodology is also provided.

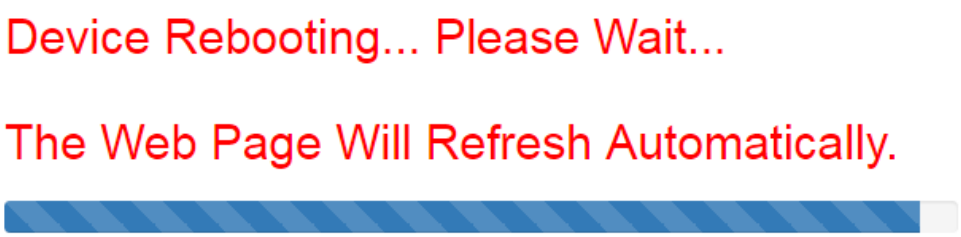


3. **Installing** the uploaded firmware image
   The new firmware will install after the system validates it.

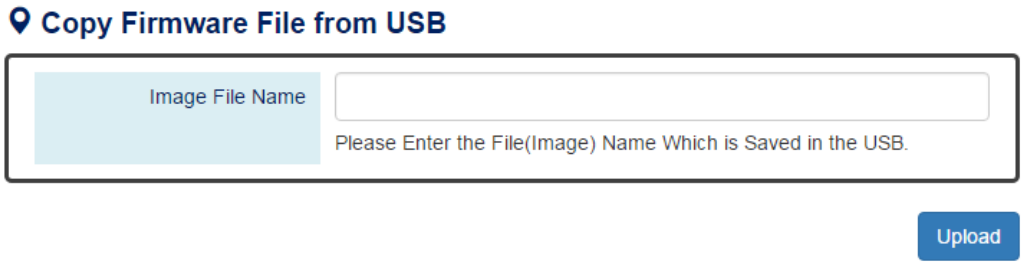


4. **Rebooting** the system
   The system will reboot automatically if the firmware is upgraded without any issue.

   The progress bar displays the rebooting progress.



Upgrade Firmware Version - Copy Firmware File from USB

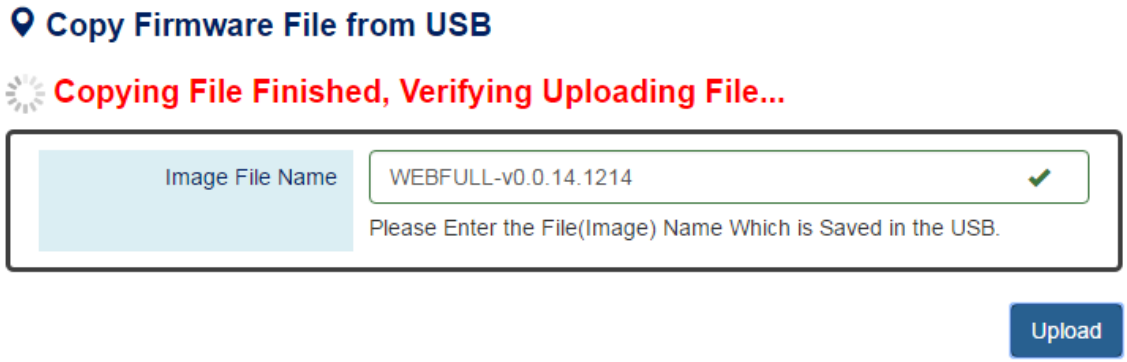


- **Image File Name**
  Enter the name of the firmware image in the USB. The system will try to identify the file with specified file name to upload it to the system.
- Upload (Upload Button)
  After entering the firmware image name, click "Upload" button to copy it from the USB to the system.

Upgrade Firmware Process - Copy Firmware File from USB

1. **Copying** the firmware image from USB to switch
   The system will also check if the USB is inserted and file exists.

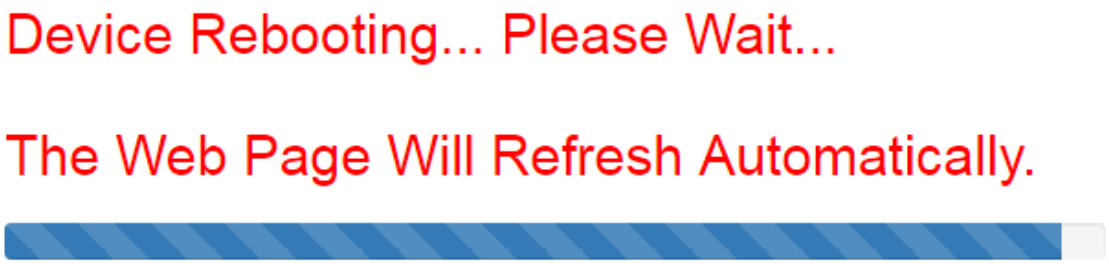
2. **Verifying** the uploaded file
   After copying the firmware file to switch, the system starts to **verify** the uploaded file to make sure it is **valid**. By default, the firmware image is encrypted to prevent the attack on man-in-the-middle. Optionally, higher encryption methodology is also provided.



3. **Installing** the uploaded firmware image
   The new firmware will install after the system makes sure it is valid.

4. **Rebooting** the system
   The system will reboot automatically if the firmware is upgraded without any issue.

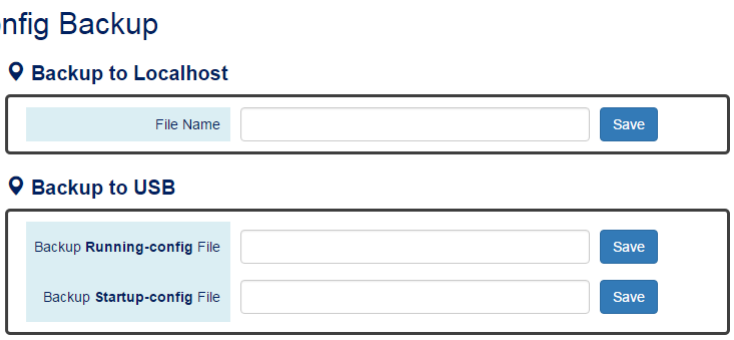
   The progress bar displays the rebooting progress.



III-26. Web Management – Config Backup

In the normal application, there are several switches in the Network and they might be configured to the same features. To facilitate this, the users can configure one of the switches and save the configuration file to local host (for example: users' PC) or USB sticks and then restore the configurations on another switch via "**Config Restore**" function. Configuration file in the USB can also have a way to fast replace the device when it is damage.

BACKUP CONFIGURATION FILE



- **Backup to Localhost**
  - File Name
    Specify the File Name for the **Startup-config** file, which will be saved to the localhost.

- **Backup to USB**
  Ensure there is a **USB stick** inserted into the USB port.
  - Backup **Running-config** File
    Specify the File Name for the saved **Running-config** file, which will be saved to the USB.
  - Backup **Startup-config** File
    Specify the File Name for the saved **Startup-config** file, which will be saved to the USB.

- Save (Save Button)
  Click the "Save" button to save the configuration file to the **Localhost** or **USB**.

NOTE:If the **File Name** filed is empty, the system assigns the default name: ***config-[datetime].cfg***

III-27. Web Management – Config Restore

We suggest users to save/backup the configurations after a series of settings. If another device needs the same configurations, users can use the **Config Restore** function to restore it.

RESTORE CONFIGURATION FILE

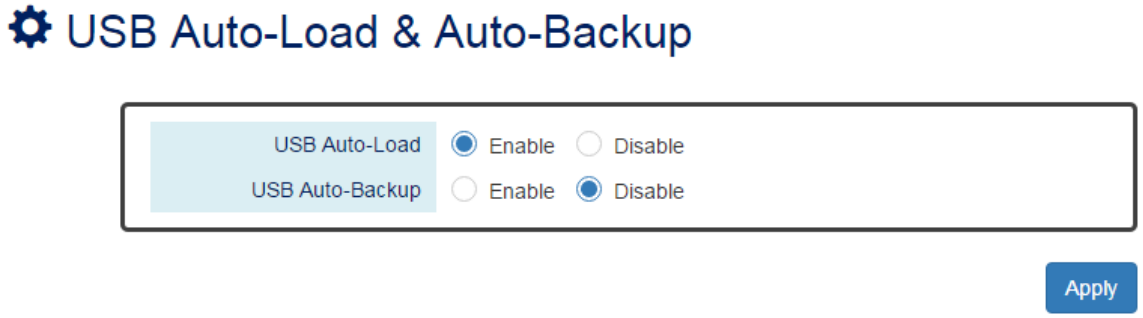
- **Restore from Localhost**
  - File Name
    Select the configuration file, which is saved in the Localhost.

- **Restore from USB**
  Please ensure there is a **USB stick** inserted into the USB port.
  - File Name in USB
    The File Name of the saved configuration file, which is saved to the USB. If the configuration file is saved in the directory, please specify the **full path**.

- Restore (Restore Button)
  Click the "Restore" button to restore the configurations from the **Localhost** or **USB**.

III-28. Web Management – USB Auto-Load &Auto-Backup

CONFIGURE USB AUTO-LOAD AND AUTO-BACKUP



- **USB Auto-Load**
  "Enable" or "Disable" the USB Auto-Load function. If "USB Auto-Load" is **enabled**, the system will search the configuration file named "**startup-config**" in the USB and load it when rebooting.

- **USB Auto-Backup**
  "Enable" or "Disable" USB Auto-Backup function. If "USB-Auto-Backup" is **enabled**, the system will save the configurations to a file named "**running-config**" in the USB when users modify the configurations.

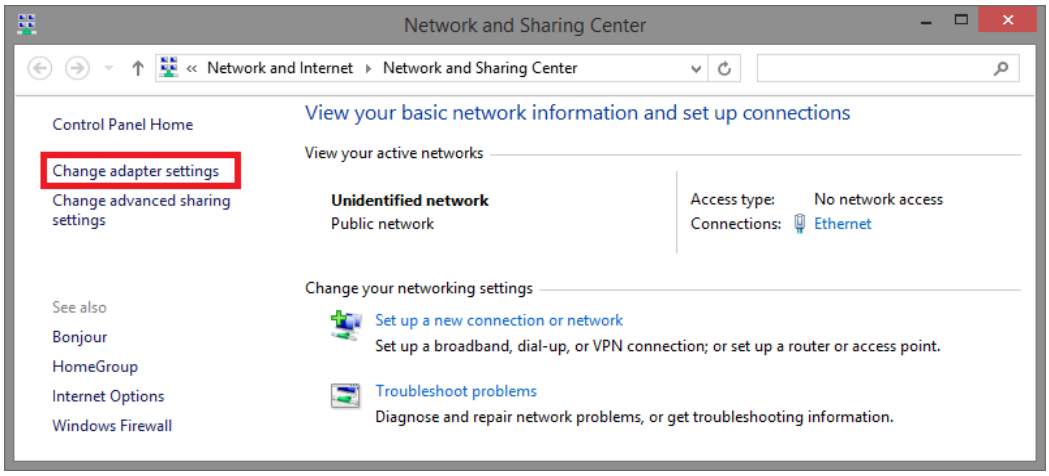
- Apply (Apply Button)
  After configuring above fields, click "**Apply**" button to make the changes effective.

Appendix A: IP Configuration for Your PC

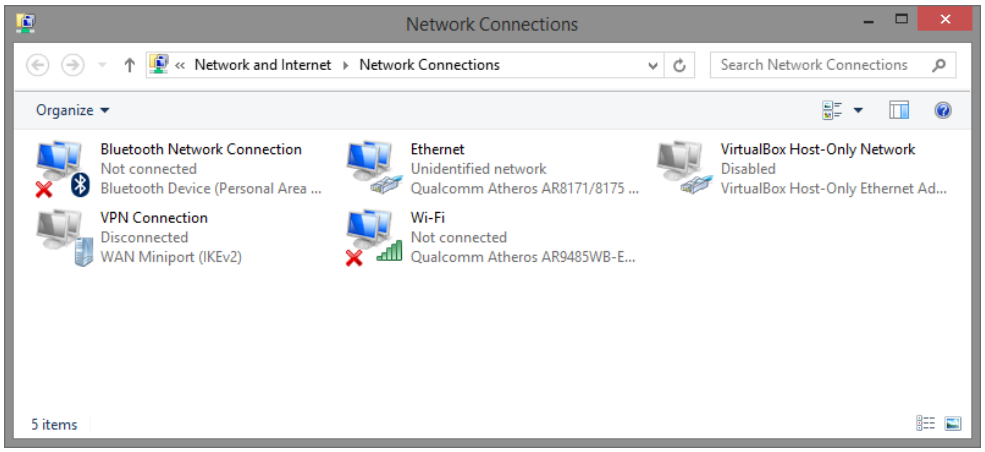
This appendix describes how to set the IP address of your PC so you can connect to product configuration webpage. The configuration webpage allows you to set system variables or monitor system status.

The following section will guide you to set the IP address properly in a Microsoft Windows 8 environment. Setting IP address in other Microsoft operating system (such as Windows 7) is quite the same and can be related.

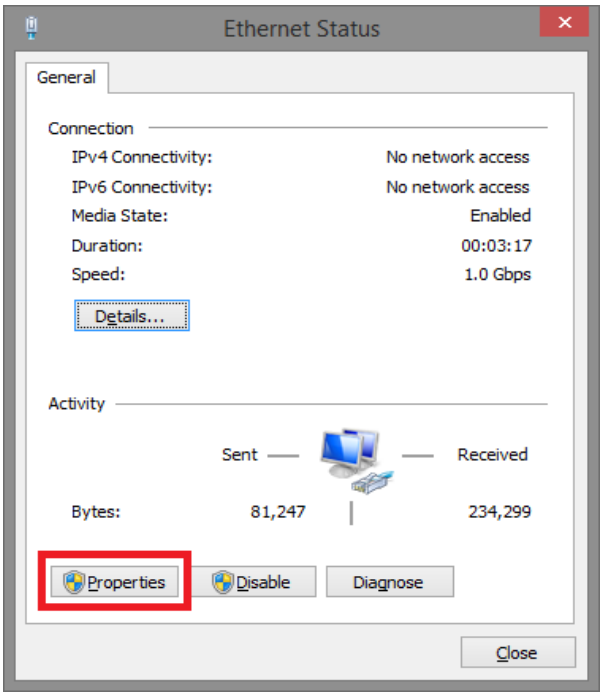
1. Open **Network and Sharing Center** in **Control Panel**, and click on **Change adapter settings** as shown in the figure down below.



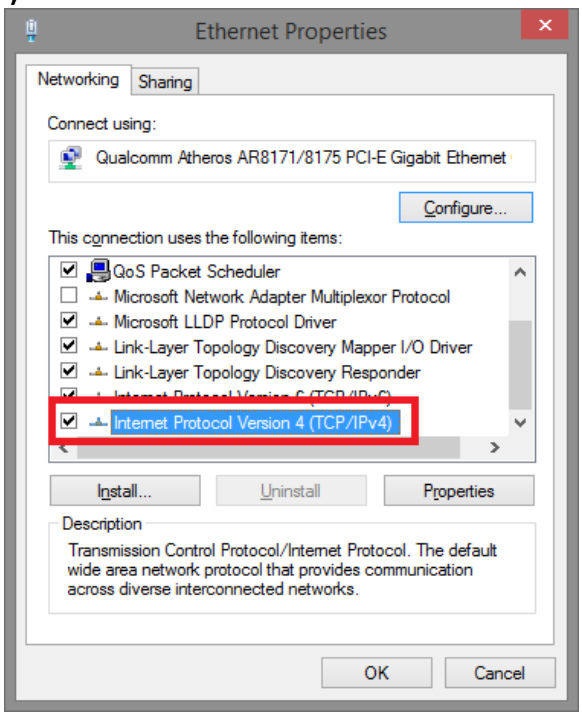
2. A **Network Connections** window will pop up, **showing** all the network connections available on your PC. Please double-click on the network connection you are using to connect the device.



3. An **Ethernet Status** window will pop up. Please click on the **Properties** button as shown in the figure down below.



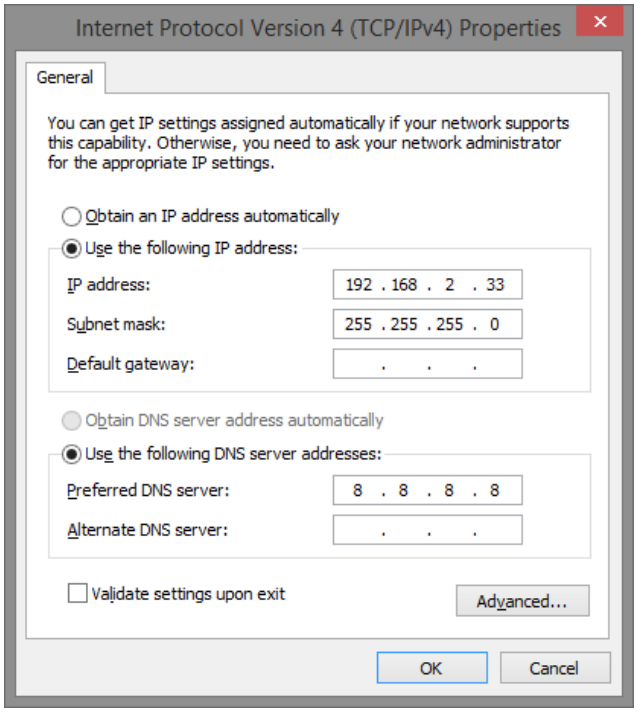
4. An **Ethernet Properties** window will pop up. Please double click on the **Internet Protocol Version 4 (TCP/IPv4)**.



5. An **Internet Protocol Version 4 (TCP/IPv4) Properties** window will pop up. Please set your PC's IP address and subnet mask as shown in the figure down below.

   By default, your product's IP address should be **192.168.2.1**.You can set any IP address as long as it's not the same with your product's IP address and is in the same network segment with your product's IP address.

   Press **OK** to apply the TCP/IPv4 settings you just made. Now you can connect to your product using a web browser (i.e. Internet Explorer, Chrome, or Firefox).


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 2 . 33
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
8 . 8 . 8 . 8
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

Appendix B: CLI Command Reference

The following are the commands that the users can use in the CLI mode. Please check if the mode is correct before issuing the command.

SYSTEM GROUP

Command	Explanation	Mode
erase startup-config	Reset to factory default and reboot	Configure
exec-timeout [MINUTE] [SECOND]	Set idle timeout [MINUTE] [SECOND]	Configure
hostname [HOSTNAME]	Set Switch Host Name	Configure
reboot	Reboot the switch	Configure
system contact [CONTACT]	Set system contact	Configure
system location [LOCATION]	Set device location	Configure
username [USER_ID] [PASSWORD]	Configure username and password	Configure
show exec-timeout	Display idle timeout	Configure
show hostname	Display Switch Host Name	Configure
show environment power [1|2]	Display power 1/2 status	Configure
show event status relay	Display relay status	Configure
show system contact	Display system contact	Configure
show system description	Display system description	Configure
show system location	Display system location	Configure
show system mac	Display system MAC address	Configure
show system uptime	Display system uptime	Configure
show system version firmware	Display system version	Configure
show username	Display admin ID	Configure
no exec-timeout	Default idle timeout	Configure
no hostname	Default Switch Host Name	Configure
no system contact	Clear system contact	Configure
no system location	Clear device location	Configure
no username	Default username and password	Configure

IPv4 Group

Command	Explanation	Mode
ip address [IP_ADDR] [MASK]	Set IPv4 address and netmask	Configure
ip default-gateway [DEFAULT_GATEWAY_ADDR]	Set default gateway address	Configure
ip name-server [NAME_SERVER_IP]	Set Domain Name-Server	Configure
ip ping [IPV4_ADDR] [<size PKG_SIZ> | <repeat PKG_CNT>]	Issue an IPv4 ping command	Configure
show ip address	Display Host address of IPv4	Configure
show ip default-gateway	Display default gateway address	Configure
show ip mode	Display IP mode (Static or Dynamic)	Configure
show ip name-server	Display Domain Name-Server	Configure
no ip address	Delete IPv4 address	Configure
no ip default-gateway	Clear the default gateway address	Configure
no ip name-server	Clear the domain name-server	Configure

IPv6 Group

Command	Explanation	Mode
ipv6 address add [IPV6_ADDR</PREFIX_LEN>]	Add an address and netmask of IPv6	Configure
ipv6 enable	Enable IPv6 protocol	Configure
ipv6 neighbor flush	Issue a neighbor flush command of IPv6	Configure
ipv6 ping [IPV6_ADDR] [<size PKG_SIZ> | <repeat PKG_CNT>]	Issue an IPv6 ping command	Configure
show ipv6	Display IPv6 protocol state	Configure
show ipv6 address	Display IPv6 addresses	Configure
show ipv6 default address	Display default IPv6 address	Configure
show ipv6 neighbor	Display neighbor cache of IPv6	Configure
no ipv6	Disable IPv6 protocol	Configure
no ipv6 address add [IPV6_ADDR/PREFIX_LEN]	Delete IPv6 address	Configure

TIME GROUP

Command	Explanation	Mode
clock time [hh:mm:ss] [day] [month] [year]	Configure time	Configure
clock timezone [AREA] [CITY]	Configure time zone	Configure
ntp client sync [minute | hour | day | month | year] [NUMBER]	Configure NTP client sync	Configure
ntp client timeserver [SERVER_IP/URL]	Configure NTP client time server	Configure
ntp time update	Configure NTP time update	Configure
show clock time	Show time	Configure
show clock timezone	Show timezone	Configure
show ntp client sync	Show sync time	Configure
show ntp client timeserver	Show NTP server configuration	Configure
no clock timezone	Remove timezone	Configure
no ntp client sync	Remove NTP sync time	Configure
no ntp client timeserver	Remove NTP time server configuration	Configure

STP GROUP

Command	Explanation	Mode
spanning-tree forward-time [4-30]	Set STP forward time	Configure
spanning-tree hello-time [1-10]	Set STP hello time	Configure
spanning-tree max-age [6-40]	Set max age	Configure
spanning-tree mode [rstp]	Set STP mode as [RSTP]	Configure
spanning-tree priority [0-61440]	Set STP priority	Configure
spanning-tree cost [0-200000000]	Configure STP cost	Interface
spanning-tree edge [admin-edge|admin-non-edge]	Configure STP edge	Interface
spanning-tree link-type [point-to-multiple|point-to-point]	Configure STP link type on port	Interface
spanning-tree port-priority [0-240]	Configure STP port priority	Interface
spanning-tree stp disable	Disable Spanning Tree Protocol (STP) on port	Interface
show spanning-tree forward-time	Show STP forward time	Configure
show spanning-tree hello-time	Show STP hello time	Configure
show spanning-tree max-age	Show STP max age	Configure
show spanning-tree mode	Show Spanning Tree mode (RSTP or disable)	Configure
show spanning-tree priority	Show STP priority	Configure
show spanning-tree rstp-status	Show Spanning Tree rstp status	Configure
show spanning-tree cost	Show STP cost	Interface
show spanning-tree edge	Show STP auto edge	Interface
show spanning-tree link-type	Show STP link type	Interface
show spanning-tree port-priority	Show STP port priority	Interface
show spanning-tree stp	Show STP activated status on port	Interface
no spanning-tree forward-time	Remove STP forwardtime configuration	Configure
no spanning-tree hello-time	Remove STP hello time configuration	Configure

no spanning-tree max-age	Remove STP max age configuration	Configure
no spanning-tree mode	Disable STP configuration	Configure
no spanning-tree priority	Remove STP priority configuration	Configure
no spanning-tree cost	Remove STP cost configuration	Interface
no spanning-tree edge	Remove auto edge configuration	Interface
no spanning-tree link-type	Remove link type configuration	Interface
no spanning-tree port-priority	Remove STP port priority configuration	Interface
no spanning-tree stp	Enable STP on port	Interface

SNMP GROUP

Command	Explanation	Mode
snmp server community ro [COMMUNITY]	Set v1, v2c snmp server read-only community	Configure
snmp server community rw [COMMUNITY]	Set v1, v2c snmp server read-write community	Configure
snmp server enable	Enable snmp server	Configure
snmp server enable v1-v2c-only	Enable snmp v1 and v2c	Configure
snmp server enablev3-only	Enable snmp v3 command only	Configure
snmp server v3 auth admin [md5| sha] [PASSWORD]	Set SNMPv3 admin authentication type	Configure
snmp server v3 auth user [md5| sha] [PASSWORD]	Set SNMPv3 user authentication type	Configure
snmp server v3 encryption admin [des| aes] [PASSWORD]	Set SNMPv3 admin encryption type	Configure
snmp server v3 encryption user [des| aes] [PASSWORD]	Set SNMPv3 user encryption type	Configure
snmp server v3 level admin [auth| noauth| priv]	Set SNMPv3 admin security level	Configure
snmp server v3 level user [auth| noauth| priv]	Set SNMPv3 user security level	Configure
snmp trap community [COMMUNITY]	Set v1, v2c snmp trap community	Configure
snmp trap host [TRAP_HOST_IP]	Set snmp trap host IP address	Configure
snmp trap inform retry [1-100]	Set snmp inform retry times	Configure
snmp trap inform timeout [1-300]	Set snmp inform timeout	Configure
snmp trap v3 auth [sha| md5] [PASSWORD]	Set SNMPv3 authentication type: md5 or sha	Configure
snmp trap v3 encryption [des| aes] [PASSWORD]	Set SNMPv3 encryption type: des or aes	Configure
snmp trap v3 engine-ID [ENGINE_ID]	Set snmp trap engine ID	Configure
snmp trap v3 level [auth| noauth| priv]	Set SNMPv3 trap security level	Configure
snmp trap v3 user [USER_ID]	Set SNMPv3 trap user	Configure
snmp trap version [1| 2c trap| 2c inform| 3 trap| 3 inform]	Set snmp trap version and type	Configure
show snmp server	Display snmp server status	Configure
show snmp server community ro	Display snmp server read only community	Configure
show snmp server community rw	Display snmp server writable community	Configure
show snmp server v3 auth admin	Display SNMPv3 admin authentication type and passphrase	Configure
show snmp server v3 auth user	Display SNMPv3 user authentication type and passphrase	Configure
show snmp server v3 encryption admin	Display SNMPv3 admin encryption type and passphrase	Configure
show snmp server v3 encryption user	Display SNMPv3 user encryption type and passphrase	Configure
show snmp server v3 level admin	Display SNMPv3 admin security level	Configure

show snmp server v3 level user	Display SNMPv3 user security level	Configure
show snmp trap community	Display snmp trap community	Configure
show snmp trap host	Display snmp trap host	Configure
show snmp trap inform retry	Display snmp inform retry times	Configure
show snmp trap inform timeout	Display snmp inform timeout	Configure
show snmp trap v3 auth	Display SNMPv3 authentication type and passphrase	Configure
show snmp trap v3 encryption	Display SNMPv3 encryption type and passphrase	Configure
show snmp trap v3 engine-ID	Display snmp trap engine ID	Configure
show snmp trap v3 level	Display SNMPv3 trap security level	Configure
show snmp trap v3 user	Display SNMPv3 trap user	Configure
show snmp trap version	Display snmp trap version and type	Configure
no snmp server	Disable snmp server	Configure
no snmp server community ro	Default ro-community name	Configure
no snmp server community rw	Default rw-community name	Configure
no snmp server v3 auth admin	Default SNMPv3 admin authentication type	Configure
no snmp server v3 auth user	Default SNMPv3 user authentication type	Configure
no snmp server v3 encryption admin	Default SNMPv3 admin encryption type	Configure
no snmp server v3 encryption user	Default SNMPv3 user encryption type	Configure
no snmp server v3 level admin	Default SNMPv3 admin security level	Configure
no snmp server v3 level user	Default SNMPv3 user security level	Configure
no snmp trap community	Default snmp trap community	Configure
no snmp trap host	Default snmp trap host	Configure
no snmp trap inform retry	Default snmp inform retry times	Configure
no snmp trap inform timeout	Default snmp inform timeout	Configure
no snmp trap v3 auth	Default SNMPv3 authentication type and passphrase	Configure
no snmp trap v3 encryption	Default SNMPv3 encryption type and passphrase	Configure
no snmp trap v3 engine-ID	Default snmp trap engine ID	Configure
no snmp trap v3 level	Default SNMPv3 trap security level	Configure
no snmp trap v3 user	Default SNMPv3 trap user	Configure
no snmp trap version	Default snmp trap version	Configure

DHCP GROUP

Command	Explanation	Mode
boot host dhcp	Directs the system to get an IP address	Configure
dhcp relay information option	Set DHCP-relay option	Configure
dhcp relay server [server_number: 1-4] [server_IP]	Set DHCP-relay server [1-4] IP	Configure
dhcp relay untrust	Set DHCP-relay untrusted port	Interface
dhcp server binding [bind_ID: 1 - 32] [MAC] [IP_TO_BIND]	Set binding IP and MAC of DHCP	Configure

dhcp server default-gateway [IP_ADDR]	Set default-gateway IP for DHCP client	Configure
dhcp server included-address [START_OF_IP] [END_OF_IP]	Set IP range for its client	Configure
dhcp server lease [60-2592000]	Set DHCP server lease time	Configure
dhcp server name-server [IP_ADDR]	Set name-server address for DHCP client	Configure
dhcp service relay enable	Enable DHCP relay	Configure
dhcp service server enable	Enable DHCP server	Configure
show boot host dhcp	Display DHCP client state	Configure
show dhcp relay information option	Display DHCP relay option	Configure
show dhcp relay server [server_number: 1-4]	Display DHCP relay address	Configure
show dhcp relay untrust	Display DHCP untrusted port status	Interface
show dhcp server binding	Display all DHCP bounding entries	Configure
show dhcp server default-gateway	Display DHCP default-gateway IP	Configure
show dhcp server included-address	Display DHCP included IP range	Configure
show dhcp server lease	Display DHCP server lease time	Configure
show dhcp server name-server	Display DHCP name-server	Configure
show dhcp server status	Display DHCP server status	Configure
show dhcp service relay	Display DHCP relay agent status	Configure
show dhcp service server	Display DHCP server status	Configure
no boot host dhcp	Disable DHCP client	Configure
no dhcp relay information option	Disable DHCP relay option	Configure
no dhcp relay server [server_number: 1-4]	Remove DHCP relay server [1-4] IP	Configure
no dhcp relay untrust	Default port as trusted	Interface
no dhcp server binding [bind_ID: 1-32]	Remove DHCP bounding IP and MAC	Configure
no dhcp server default-gateway	Remove DHCP default-gateway IP	Configure
no dhcp server included-address	Remove DHCP included IP range	Configure
no dhcp server lease	Remove DHCP lease time	Configure
no dhcp server name-server	Remove DHCP name-server	Configure
no dhcp service relay	Disable DHCP relay	Configure
no dhcp service server	Disable DHCP server	Configure

UPnP Group

Command	Explanation	Mode
upnp advertisement interval [300-86400]	Set UPnP advertisement interval	Configure
upnp enable	Enable Universal Plug and Play (UPnP)	Configure
show upnp	Display Universal Plug and Play (UPnP) state	Configure
show upnp advertisement interval	Display UPnP advertisement interval	Configure
no upnp	Disable Universal Plug and Play (UPnP)	Configure
no upnp advertisement interval	Default UPnP advertisement interval	Configure

PORT GROUP

Command	Explanation	Mode
flowcontrol [on | off]	Configure port's flow-control to response a pause frame	Interface
name [PORT_NAME]	Set interface name	Interface
shutdown	Disable port	Interface
speed_duplex [10 | 100] [full | half]	Configure port's speed and duplex	Interface
show interface all link summary	To display interface link status globally	Configure
show administrate	To display port's admin state	Interface
show flowcontrol	Display port's flow-control state	Interface
show link duplex	To display port's duplex	Interface
show link rx	To display port's Rx_Bytes	Interface
show link speed	To display port's speed	Interface
show link state	To display port's link state	Interface
show link summary	To display port's link summary	Interface
show link tx	To display port's Tx_Bytes	Interface
show name	To display port's name	Interface
show speed_duplex	To display port's speed and duplex	Interface
show transceiver	Transceiver information	Interface
no flowcontrol	Default flow-control as Auto mode	Interface
no name	Remove port's name	Interface
no shutdown	Enable port	Interface
no speed_duplex	Default port speed-duplex as Auto mode	Interface

POE GROUP

Command	Explanation	Mode
power inline never	Disable PoE on port	Interface
keepalive enable	Enable PoE keepalive	Interface
keepalive hold-time	Configure PoE keepalive power cycle hold-time	Interface
keepalive ip	Configure IP for PoE keepalive	Interface
keepalive time	Configure PoE keepalive cycle time	Interface
schedule enable	Enable one port PoE schedule	Interface
schedule [Sunday-Saturday] open-time [time]	Configure PoE schedule open time on one day	Interface
show power inline status	Display All PoE ports status	Configure
show keepalive table	Display All PoE keepalive info	Configure
show power inline status	Display PoE status	Interface
show keepalive	Show PoE keepalive status	Interface
show keepalive hold-time	Show PoE keepalive hold-time	Interface
show keepalive ip	Show IP for PoE keepalive	Interface
show keepalive time	Show PoE keepalive cycle time	Interface
show schedule	Disable Universal Plug and Play (UPnP)	Interface
show schedule [Sunday-Saturday] open-time	Show open time of POE schedule on one day	Interface
show schedule table	Show one port PoE schedule table	Interface
no power inline never	Enable PoE on port	Interface
no keepalive	Disable PoE keepalive	Interface
no keepalive hold-time	Default PoE keepalive power cycle hold-time	Interface
no keepalive ip	Remove IP for PoE keepalive	Interface
no keepalive time	Remove PoE keepalive cycle time	Interface
no schedule	Remove one port PoE schedule	
no schedule [Sunday-Saturday] open-time	Remove PoE schedule on one day	

IGMP SNOOPING GROUP

Command	Explanation	Mode
igmp snooping enable	To enable IGMP snooping	Configure
igmp snooping last-member count [2-10]	To set IGMP last-member-count	Configure
igmp snooping last-member interval [1-25]	To set IGMP last-member-interval	Configure
igmp snooping querier enable	To enable IGMP snooping querier	Configure
igmp snooping query interval [1-3600]	To set IGMP query interval	Configure
igmp snooping query max-respond-time [1-12]	To set IGMP max-query-respond time	Configure
show igmp snooping all	To display IGMP settings (summary)	Configure
show igmp snooping mdb	To display IGMP multicast database	Configure
no igmp snooping	To disable IGMP snooping	Configure
no igmp snooping last-member count	To default IGMP Last-Member-Count	Configure
no igmp snooping last-member interval	To default IGMP Last-Member-Interval	Configure
no igmp snooping querier	To disable IGMP querier	Configure
no igmp snooping query interval	To default IGMP query interval	Configure
no igmp snooping query max-respond-time	To default IGMP max-respond-time	Configure

VLAN GROUP

Command	Explanation	Mode
management-vlan [VLAN_ID: 1-4094]	Configure management vlan ID	Configure
provider ethertype [VALUE_IN_HEX (i.e., 0x88A8)]	Setup EtherType in S-TAG for provider port	Configure
member [untag PORT_LIST] [tag PORT_LIST]	Set VLAN member	VLAN
name [VLAN_NAME]	Set VLAN Name	VLAN
switchport accept [tagged | untagged]	Set VLAN acceptance of frame	Interface
switchport mode [d(dot1q-tunnel)| c(customer)| p(provider)| s(specific-provider)]	Configure port type as dot1q-tunnel, Customer, or Service Provider	Interface
switchport pvid [PVID: 1-4094]	Set port VLAN-Id	Interface
show management-vlan	Display management vlan ID	Configure
show provider ethertype	Display Service Provider EtherType	Configure
show vlan global	Display VLAN Global information	Configure
show member	Display port VLAN member	VLAN
show name	Displaty VLAN name	VLAN
show switchport accept	Display acceptance of VLAN frame	Interface
show switchport mode	Display VLAN interface port type	Interface
show switchport pvid	Display port VLAN-Id	Interface
no management-vlan	Set management vlan to default	Configure
no provider ethertype	Default EtherType as 0x88A8 in S-TAG for provider port	Configure
no member	Default VLAN member	VLAN
no name	Default VLAN name	VLAN
no switchport accept	Default acceptance of VLAN frame	Interface
no switchport mode	Default port type as Customer	Interface
no switchport pvid	Default port VLAN-Id	Interface

QoS Group

Command	Explanation	Mode
qos fair-queue weight [W0] [W1] [W2] [W3] [W4] [W5] [W6] [W7]	Set WRR Queue Weight	Configure
qos map cos [priority:0-7] to tx-queue [0-7]	Set Cos queue mapping of priority [0-7]	Configure
qos map dscp [0-63] to tx-queue [0-7]	Set DSCP mapping queue	Configure
qos queue-schedule [strict | wrr]	Set QoS scheduling type	Configure
qos default cos [0-7]	Set Default Class of Service (COS) value	Interface
qos trust [cos | dscp]	Set trust of cos or dscp	Interface
show qos fair-queue weight	Display WRR Queue Weight	Configure
show qos map cos	Display global QoS queue mapping status	Configure
show qos map cos [0-7]	Display QoS queue mapping status of Priority [0-7]	Configure
show qos map dscp	Display global DSCP queue mapping status	Configure
show qos map dscp [0-63]	Display DSCP queue mapping status of class [0-63]	Configure
show qos queue-schedule	Display queue scheduling type	Configure
show qos default cos	Display CoS default value	Interface
show qos trust	Display QoS trust	Interface
no qos fair-queue weight	Default WRR Queue Weight	Configure
no qos map cos [0-7]	Reset Cos queue mapping of priority [0-7]	Configure
no qos map dscp [0-63]	Reset DSCP mapping queue to default	Configure
no qos queue-schedule	Default scheduling type as WRR	Configure
no qos default cos	Reset default CoS to initial value	Interface
no qos trust	Default trust as CoS	Interface

PORT TRUNK GROUP

Command	Explanation	Mode
trunk group [1-8] [static | lacp] INTERFACES_LIST	Configure port aggregation group	Configure
show trunk group	Show all trunk groups	Configure
show trunk group [1-8]	Show trunk group [1-8]	Configure
no trunk group [1-8]	Remove trunk group [1-8]	Configure

STORM CONTROL GROUP

Command	Explanation	Mode
storm-control broadcast enable	Enable the broadcast storm control	Configure
storm-control broadcast level [low | mid | high]	Set the broadcast storm control level	Configure
storm-control multicast enable	Enable the multicast storm control	Configure
storm-control multicast level [low | mid | high]	Set the multicast storm control level	Configure
storm-control unknown-unicast enable	Enable the unknown-unicast storm control	Configure
storm-control unknown-unicast level [low | mid | high]	Set the unknown-unicast storm control level	Configure
show storm-control broadcast	Display the broadcast storm control status	Configure
show storm-control broadcast level	Display the broadcast storm control level	Configure
show storm-control multicast	Display the multicast storm control status	Configure
show storm-control multicast level	Display the multicaststorm control level	Configure
show storm-control unknown-unicast	Display the unknown-unicast storm control status	Configure
show storm-control unknown-unicast level	Display the unknown-unicast storm control level	Configure
no storm-control broadcast	Disable the broadcast storm control	Configure
no storm-control broadcast level	Default the broadcast storm control to level high	Configure
no storm-control multicast	Disable the multicast storm control	Configure
no storm-control multicast level	Default the multicast storm control to level high	Configure
no storm-control unknown-unicast	Disable the unknown-unicast storm control	Configure
no storm-control unknown-unicast level	Default the unknown-unicast storm control to level high	Configure

802.1X Group

Command	Explanation	Mode
dot1x authentication server [1|2] ip [IP]	Set 802.1X authentication server 1 or 2 address	Configure
dot1x authentication server [1|2] port [PORT]	Set 802.1X authentication server 1 or 2 port	Configure
dot1x authentication server [1|2] share-key [KEY]	Set 802.1X authentication server 1 or 2 share-key	Configure
dot1x authentication server type [local|radius]	Set 802.1X authentication server type	Configure
dot1x enable	Enable 802.1X protocol	Configure
dot1x local-db [USER] [PASSWORD]	Set 802.1X local user database	Configure
dot1x authenticator enable	Set 802.1X authenticator	Interface
dot1x mode [mac-based | port-based]	Set 802.1X mode as 1. MAC-based, 2.Port-based	Interface
dot1x reauthentication enable	Set 802.1X reauthentication	Interface
dot1x reauthentication period [60-65535]	Set 802.1X reauthentication period	Interface
show dot1x	Display 802.1X protocol state	Configure
show dot1x authentication server [1|2] ip	Display 802.1X authentication server 1 or 2 address	Configure
show dot1x authentication server [1|2] port	Display 802.1X authentication server 1 or 2 port	Configure
show dot1x authentication server [1|2] share-key	Display 802.1X authentication server 1 or 2 key	Configure
show dot1x authentication server type	Display 802.1X authentication server type	Configure
show dot1x brief	Display 802.1X information	Configure
show dot1x local-db	Display 802.1X users and password in database	Configure
show dot1x server brief	Display 802.1X RADIUS server	Configure
show dot1x authenticator	Display 802.1X authenticator state	Interface
show dot1x mode	Display 802.1X mode config	Interface
show dot1x reauthentication	Display 802.1X reauthentication state	Interface
show dot1x reauthentication period	Display 802.1X reauthentication period(in sec.)	Interface
no dot1x	Disable 802.1X protocol	Configure
no dot1x authentication server [1|2] ip	Default 802.1X authentication server 1 or 2 address	Configure
no dot1x authentication server [1|2] port	Default 802.1X authentication server 1 or 2 port	Configure
no dot1x authentication server [1|2] share-key	Default 802.1X authentication server 1 or 2 share-key	Configure
no dot1x authentication server type	Default 802.1X authentication server type	Configure
no dot1x local-db [USER]	Remove an entry in 802.1X local database	Configure
no dot1x authenticator	Disable 802.1X authenticator	Interface
no dot1x mode	Default 802.1X mode as MAC-based	Interface
no dot1x reauthentication	Disable 802.1X reauthentication	Interface
no dot1x reauthentication period	Default 802.1X reauthentication period	Interface

Port Mirror Group

Command	Explanation	Mode
mirror destination [DEST_PORT]	Set mirror interface of destination	Configure

mirror enable	Enable port mirror	Configure
mirror source [rx | tx | both] [PORT_LIST]	Set mirror interface of source	Configure
show mirror	Show port mirror enable/disable state	Configure
show mirror destination	Show port mirror destination configuration	Configure
show mirror source	Show port mirror source configuration	Configure
no mirror	Disable port mirror	Configure
no mirror destination	Delete port mirror Destination configuration	Configure
no mirror source	Delete port mirror Source configuration	Configure

LLDP GROUP

Command	Explanation	Mode
lldp enable	Enable LLDP protocol	Configure
lldp timer [5-32767]	Set LLDP timer	Configure
show lldp neighbor	Display LLDP neighbor	Configure
show lldp neighbor detail	Display LLDP neighbors in detail	Configure
show lldp state	Display LLDP status	Configure
show lldp timer	Display LLDP timer	Configure
no lldp	Disable LLDP protocol	Configure
no lldp timer	Default LLDP timer	Configure

SYSLOG GROUP

Command	Explanation	Mode
syslog local enable	Enable logging to local	Configure
syslog log clear	Clear syslog log	Configure
syslog remote enable	Enable logging to remote	Configure
syslog remote port [PORT]	Set syslog remote server port	Configure
syslog remote server [ADDRESS]	Set syslog remote server address	Configure
syslog usb enable	Enable log to USB device	Configure
show syslog local	Display local logging state	Configure
show syslog log	Display syslog messages	Configure
show syslog remote	Display remote logging state	Configure
show syslog remote port	Display remote server port	Configure
show syslog remote server	Display remote server IP	Configure
show syslog usb	Display USB logging state	Configure
no syslog local	Disable logging to local	Configure
no syslog remote	Disable logging to remote	Configure
no syslog remote port	Default syslog remote server port	Configure
no syslog remote server	Clear syslog remote server address	Configure
no syslog usb	Disable logging to USB	Configure

SMTP GROUP

Command	Explanation	Mode
smtp authentication enable	Enable SMTP authentication	Configure
smtp authentication password [PASSWORD]	Set SMTP password	Configure
smtp authentication username [USER_NAME]	Set SMTP username	Configure
smtp enable	Enable SMTP	Configure
smtp receive [1-4] [RECEIVER_ADDRESS]	Set SMTP receiver [1-4] address	Configure
smtp sender [SMTP_SENDER_ADDRESS]	Set SMTP sender	Configure
smtp server address [SMTP_SERVER_ADDRESS]	Set SMTP server address	Configure
smtp server port [SMTP_SERVER_PORT]	Set SMTP server port	Configure
smtp subject [SUBJECT]	Set SMTP subject	Configure
show smtp authentication state	Display SMTP authentication status	Configure
show smtp authentication username	Display SMTP user name	Configure
show smtp receive [1-4]	Display SMTP receiver [1-4]	Configure
show smtp sender	Display SMTP sender	Configure
show smtp server address	Display SMTP server address	Configure
show smtp server port	Display SMTP server port	Configure
show smtp state	Display SMTP service	Configure
show smtp subject	Display SMTP subject	Configure
no smtp authentication	Disable SMTP authentication	Configure
no smtp authentication password	Clear SMTP password	Configure
no smtp authentication username	Clear SMTP user name	Configure
no smtp	Disable SMTP	Configure
no smtp receive [1-4]	Clear SMTP receiver [1-4]	Configure
no smtp sender	Clear SMTP sender	Configure
no smtp server address	Clear SMTP server	Configure
no smtp server port	Clear SMTP server port	Configure
no smtp subject	Clear SMTP subject	Configure

EVENT GROUP

Command	Explanation	Mode
event alarm interface [lan1-lanN] down	Register an event of Interface DOWN	Configure
event alarm [power1|power2]	Register an event of power 1 or 2 failure	Configure
event smtp auth-failure	Register an event of authentication failure	Configure
event smtp cold-start	Register an event of cold-start	Configure
event smtp interface [lan1-lanN] down	Register an event of Interface DOWN	Configure
event smtp interface [lan1-lanN] up	Register an event of Interface UP	Configure
event smtp [power1|power2]	Register an event of power 1 or 2 failure	Configure
event smtp warm-start	Register an event of warm-start	Configure
event snmptrap auth-failure	Register an event of authentication failure	Configure
event snmptrap cold-start	Register an event of cold-start	Configure
event snmptrap interface [lan1-lanN] down	Register an event of Interface DOWN	Configure
event snmptrap interface [lan1-lanN] up	Register an event of Interface UP	Configure
event snmptrap [power1|power2]	Register an event of power 1 or 2 failure	Configure
event snmptrap warm-start	Register an event of warm-start	Configure
event syslog auth-failure	Register an event of authentication failure	Configure
event syslog cold-start	Register an event of cold-start	Configure
event syslog interface [lan1-lanN] down	Register an event of Interface DOWN	Configure
event syslog interface [lan1-lanN] up	Register an event of Interface UP	Configure
event syslog [power1|power2]	Register an event of power 1 or 2 failure	Configure
event syslog warm-start	Register an event of warm-start	Configure
show event alarm interface [lan1-lanN] down	Display interface DOWN event registration	Configure
show event alarm [power1|power2]	Display power 1 or 2 event registration	Configure
show event smtp auth-failure	Display authentication failure event registration	Configure
show event smtp cold-start	Display cold-start event registration	Configure
show event smtp interface [lan1-lanN] down	Display interface DOWN event registration	Configure
show event smtp interface [lan1-lanN] up	Display interface UP event registration	Configure
show event smtp [power1|power2]	Display power 1 or 2 event registration	Configure
show event smtp warm-start	Display warm-start event registration	Configure
show event snmptrap auth-failure	Display authentication failure event registration	Configure
show event snmptrap cold-start	Display cold-start event registration	Configure
show event snmptrap interface [lan1-lanN] down	Display interface DOWN event registration	Configure
show event snmptrap interface [lan1-lanN] up	Display interface UP event registration	Configure
show event snmptrap [power1|power2]	Display power 1 or 2 event registration	Configure
show event snmptrap warm-start	Display warm-start event registration	Configure
show event syslog auth-failure	Display authentication failure event registration	Configure
show event syslog cold-start	Display cold-start event registration	Configure
show event syslog interface [lan1-lanN] down	Display interface DOWN event registration	Configure
show event syslog interface [lan1-lanN] up	Display interface UP event registration	Configure
show event syslog [power1|power2]	Display power 1 or 2 event registration	Configure

show event syslog warm-start	Display warm-start event registration	Configure
no event alarm interface [lan1-lanN] down	Unregister an event of Interface DOWN	Configure
no event alarm [power1|power2]	Unregister an event of power 1 or 2 failure	Configure
no event smtp auth-failure	Unregister an event of authentication failure	Configure
no event smtp cold-start	Unregister an event of cold-start	Configure
no event smtp interface [lan1-lanN] down	Unregister an event of Interface DOWN	Configure
no event smtp interface [lan1-lanN] up	Unregister an event of Interface UP	Configure
no event smtp [power1|power2]	Unregister an event of power 1 or 2 failure	Configure
no event smtp warm-start	Unregister an event of warm-start	Configure
no event snmptrap auth-failure	Unregister an event of authentication failure	Configure
no event snmptrap cold-start	Unregister an event of cold-start	Configure
no event snmptrap interface [lan1-lanN] down	Unregister an event of Interface DOWN	Configure
no event snmptrap interface [lan1-lanN] up	Unregister an event of Interface UP	Configure
no event snmptrap [power1|power2]	Unregister an event of power 1 or 2 failure	Configure
no event snmptrap warm-start	Unregister an event of warm-start	Configure
no event syslog auth-failure	Unregister an event of authentication failure	Configure
no event syslog cold-start	Unregister an event of cold-start	Configure
no event syslog interface [lan1-lanN] down	Unregister an event of Interface DOWN	Configure
no event syslog interface [lan1-lanN] up	Unregister an event of Interface UP	Configure
no event syslog [power1|power2]	Unregister an event of power 1 or 2 failure	Configure
no event syslog warm-start	Unregister an event of warm-start	Configure

MAC Address Table Group

Command	Explanation	Mode
clear mac address-table dynamic	Flush dynamic MAC addresses in MAC table	Configure
mac address add [VID: 1-4094] [MAC_ADDR] [PORT]	Set a MAC address to MAC table	Configure
show mac address	Display MAC table	Configure
no mac address [VID: 1-4094] [MAC_ADDR]	Remove a MAC address from FDB	Configure

USB Group

Command	Explanation	Mode
usb auto-backup	Auto save to USB if running config is changed	Configure
usb auto-load	Auto load config from USB to switch	Configure
show usb auto-backup	Display USB auto backup activated status	Configure
show usb auto-load	Display USB auto load activated status	Configure
no usb auto-backup	Disable auto save	Configure
no usb auto-load	Disable auto load	Configure

FILE GROUP

Command	Explanation	Mode
copy running-config startup-config	Save running-config to startup-config	Configure
copy running-config usb [file]	Save running-config to USB	Configure
copy startup-config running-config	Restore from startup-config	Configure
copy usb firmware [file]	Upgrade firmware from USB	Configure
copy startup-config usb [file]	Save startup-config to USB	Configure
copy usb startup-config [file]	Restore startup-config from USB	Configure
upload file name [FILE_NAME]	Set uploading file name	Configure
upload server ip [SERVER_IP]	Set uploading server IP	Configure
upload tftp	Upload and update firmware via TFTP (slower)	Configure
upload wget	Upload and update firmware via HTTP (faster)	Configure
show upload file name	Display uploading file name	Configure
show upload server ip	Display uploading server IP	Configure
no upload file name	Default uploading file name	Configure
no upload server ip	Clear uploading server IP	Configure

COPYRIGHT

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

FCC Caution
This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communications Commission (FCC) Radiation Exposure Statement
This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 2.5cm (1 inch) during normal operation.

Federal Communications Commission (FCC) RF Exposure Requirements
This EUT is compliance with SAR for general population/uncontrolled exposure limits in ANSI/IEEE C95.1-1999 and had been tested in accordance with the measurement methods and procedures specified in OET Bulletin 65 Supplement C. The equipment version marketed in US is restricted to usage of the channels 1-11 only. This equipment is restricted to ***indoor*** use when operated in the 5.15 to 5.25 GHz frequency range.

R&TTE Compliance Statement
This equipment complies with all the requirements of DIRECTIVE 2014/30/EU OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety
This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use
The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use
None

EU Declaration of Conformity

English: This equipment is in compliance with the essential requirements and other relevant provisions of Directive 2014/30/EU.

Français: Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 2014/30/EU.

Čeština: Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 2014/30/EU.

Polski: Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 2014/30/EU.

Română: Acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2014/30/EU.

Русский: Это оборудование соответствует основным требованиям и положениям Директивы 2014/30/EU.

Magyar: Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek (2014/30/EU).

Türkçe: Bu cihaz 2014/30/EU. direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur.

Українська: Обладнання відповідає вимогам і умовам директиви 2014/30/EU.

Slovenčina: Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 2014/30/EU.

Deutsch: Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 2014/30/EU.

Español: El presente equipo cumple los requisitos esenciales de la Directiva 2014/30/EU.

Italiano: Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 2014/30/EU.

Nederlands: Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 2014/30/EU.

Português: Este equipamento cumpre os requesitos essênciais da Directiva 2014/30/EU.

Norsk: Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 2014/30/EU.

Svenska: Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 2014/30/EU.

Dansk: Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante forordninger i direktiv 2014/30/EU.

suomen kieli: Tämä laite täyttää direktiivien 2014/30/EU. oleelliset vaatimukset ja muut asiaankuuluvat määräykset.

FOR USE IN AT BE CY CZ DK EE FI FR DE GR HU
IE IT LV LT LU MT NL PL PT SK SI ES SE
GB IS LI NO CH BG RO RU TR UA

WEEE Directive & Product Disposal

At the end of its serviceable life, this product should not be treated as household or general waste. It should be handed over to the applicable collection point for the recycling of electrical and electronic equipment, or returned to the supplier for disposal.

Declaration of Conformity

We, Edimax Technology Co., Ltd., declare under our sole responsibility, that the equipment described below complies with the requirements of the European R&TTE directives.

Equipment: Industrial Ethernet Switch

Model No.: IGS-5208

The following European standards for essential requirements have been followed:

Directives 2014/30/EU

EMC : EN 55032:2012 / AC: 2013
CISPR 32: 2012
EN 61000-3-2:2014
EN 61000-3-3:2013
EN 55024:2010 + A1: 2015

Edimax Technology Europe B.V.
Fijenhof 2,
5652 AE Eindhoven,
The Netherlands

a company of :
Edimax Technology Co., Ltd.
No. 278, Xinhu 1st Rd.,
Neihu Dist., Taipei City,
Taiwan

Signature:

Printed Name: David Huang

Title: Director
Edimax Technology Europe B.V.

Date of Signature: Jan., 2019

Signature:

Printed Name: Albert Chang

Title: Director
Edimax Technology Co., Ltd.

CE

Notice According to GNU General Public License Version 2

This product includes software that is subject to the GNU General Public License version 2. The program is free software and distributed without any warranty of the author. We offer, valid for at least three years, to give you, for a charge no more than the costs of physically performing source distribution, a complete machine-readable copy of the corresponding source code.

Das Produkt beinhaltet Software, die den Bedingungen der GNU/GPL-Version 2 unterliegt. Das Programm ist eine sog. „Free Software“, der Autor stellt das Programm ohne irgendeine Gewährleistungen zur Verfügung. Wir bieten Ihnen für einen Zeitraum von drei Jahren an, eine vollständige maschinenlesbare Kopie des Quelltextes der Programme zur Verfügung zu stellen – zu nicht höheren Kosten als denen, die durch den physikalischen Kopiervorgang anfallen.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author’s protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors’ reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone’s free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The ‘“Program”‘, below, refers to any such program or work, and a ‘“work based on the Program”‘ means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term ‘“modification”‘.) Each licensee is addressed as ‘“you”‘.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy

simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and ‘“any later version’“, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM ‘“AS IS’“ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.