WoMaster

COVER

User Manual

# DP412

**Industrial 8G + 4GF Layer 2 PoE Cyber Security Switch**

# DS412

**Industrial 8G + 4GF Layer 2 Cyber Security Switch**

Sept.21.2018 V.1

www.womaster.eu

# WoMaster

**DP412** Industrial 8G + 4GF Layer 2 PoE Cyber Security Switch
**DS412** Industrial 8G + 4GF Layer 2 Cyber Security Switch

# User Manual



## About This Manual

This user manual is intended to guide a professional installer to install and to configure the DP412 and DS412 switch. It includes procedures to assist you in avoiding unforeseen problems.

**NOTE:**

Only qualified and trained personnel should be involved with installation, inspection, and repairs of this switch.

### Disclaimer

WoMaster reserves the right to make changes to this Manual or to the product hardware at any time without notice. Information provided here is intended to be accurate and reliable. However, it might not cover all details and variations in the equipment and does not claim to provide for every possible contingency met in the process of installation, operation, or maintenance. Should further information be required or should particular problem arise which are not covered sufficiently for the user's purposes, the matter should be referred to WoMaster. Users must be aware that updates and amendments will be made from time to time to add new information and/or correct possible unintentional technical or typographical mistakes. It is the user's responsibility to determine whether there have been any such updates or amendments of the Manual. WoMaster assumes no responsibility for its use by the third parties.

### WoMaster Online Technical Services

At WoMaster, you can use the online service forms to request the support. The submitted forms are stored in server for WoMaster team member to assign tasks and monitor the status of your service. Please feel free to write to help@womaster.eu if you encounter any problems.

# TABLE OF CONTENTS

# 1. INTRODUCTION

## 1.1 OVERVIEW

DP412/DS412 is WoMaster 12G Layer 2 Managed Switch that provides 8-port Giga Ethernet, where DP412's ports are supported by IEEE 802.3af/at compliant for highly critical PoE applications so it can deliver up to 15.4W and 30W power per port to enable the high-power requiring devices. LLDP power negotiation function and 2-Event classification of IEEE 802.3at PoE plus support the PoE ports. The switch's power budget is 240W per unit at 75°C for the system and can deliver maximum 30W per port. For the best traffic control, the switch management side features have been utilized: LACP, VLAN, QinQ, QoS, IGMP snooping, and etc.

In order to uplink connection, the DP412/DS412 provides 4 SFP ports that can prioritize stream, such as video and also optimize VoIP. 1000Mbps SFP type fiber transceiver and DDM (Digital Diagnostic Monitoring) type SFP transceivers also equipped the switch for diagnosing transmission problem through maintenance and debugging of the signal quality.

WoMaster managed switch is designed to provide faster, secure, and more stable network. One advantage that makes it a powerful switch is that it supports network redundancy protocols/technologies such as Rapid Spanning Tree Protocol (RSTP)/Multiple Spanning Tree Protocol (MSTP), ITU-T G.8032 v1/v2 Ethernet Ring Protection Switching (ERPS). IEC 61000-6-2 / 61000-6-4 Heavy Industrial EMC certified design, rugged enclosure and -40~75°C wide operating temperature range, - all these features guarantee stable performance of DP412/D412 for surveillance data transmission under vibration and shock in rolling stocks, traffic control systems and other harsh environments.

This switch also can be smartly configured by WoMaster advanced management utility, Web Browser, SNMP, Telnet and RS-232 local console with its command like interface.

Advanced Cyber Security and redundancy features, guarantee the fastest network recovery, zero packet loss data transmission, and high level of network protection against the hackers' attacks. Excellent security features also provided, such as DHCP client, DHCP server with IP and MAC binding, 802.1X Port Based Network Access Control, SSH for Telnet security, IP Access table, port security and many other security features. All of these features in order to ensure the secure data communication.

## 1.2 MAJOR FEATURES

Below are the major features of DP412/DS412 Switch:

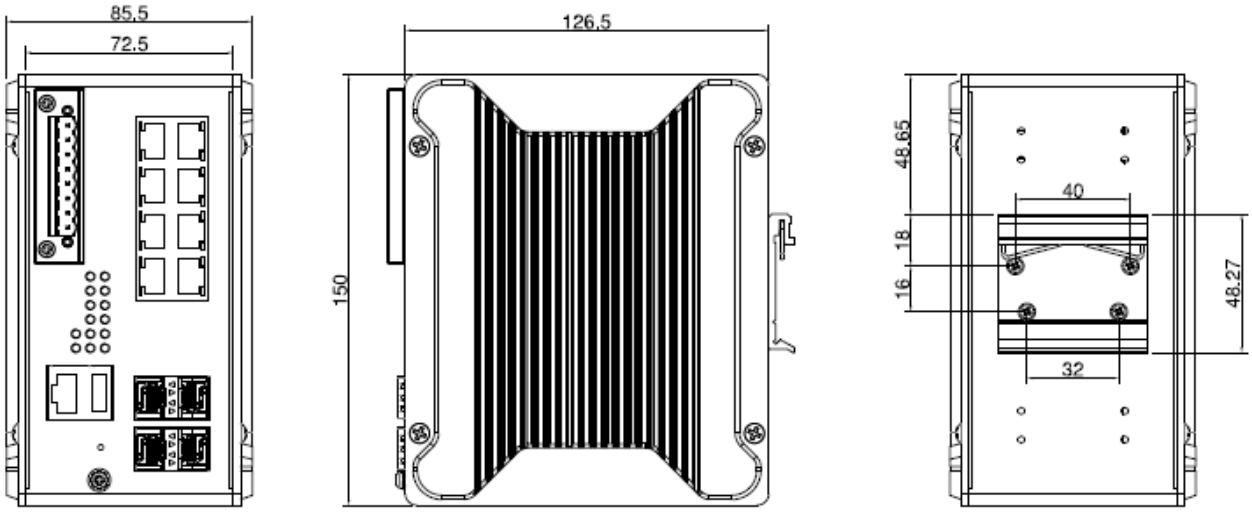
- 12-port Full Gigabit Ethernet with 8-port RJ-45 and 4-port SFP
- IEEE 802.3at 30W High Power PoE (DP412)
- 240W ultra high PoE budget and excellent power efficiency even in 75°C operating temperature (DP412)
- SFP ports support 100/1000 Mbps with Digital Diagnostic Monitoring (DDM) to monitor long distance fiber quality
- All ports provide sub-50ms protection and recovery switching for Ethernet traffic.
- Rapid Spanning Tree Protocol (RSTP)/Multiple Spanning Tree Protocol (MSTP), ITU-T G.8032 v1/v2 Ethernet Ring Protection Switching (ERPS)
- Advanced management features: LACP/VLAN/Q-in-Q/Private VLAN/ GVRP/QoS/IGMP Snooping/Rate Control/ Online Multi-Port Mirror/ Advanced DHCP server, Client,
- Advanced Security system by Port Security, Access IP list, SSH and HTTPS Login
- Event Notifications through E-mail, SNMP trap and SysLog
- IEEE 802.1AB LLDP and optional NMS software for auto-topology and group management
- CLI interface, Web, SNMP/RMON for network Management
- Multiple event relay output for enhanced alarm control
- Hi-Pot Isolation Protection for ports and power
- Steel Metal with Aluminum for heat dissipation
- Wide range operating temperature -40~75˚C
- IP31 ingress protection

# 2. HARDWARE INSTALLATION

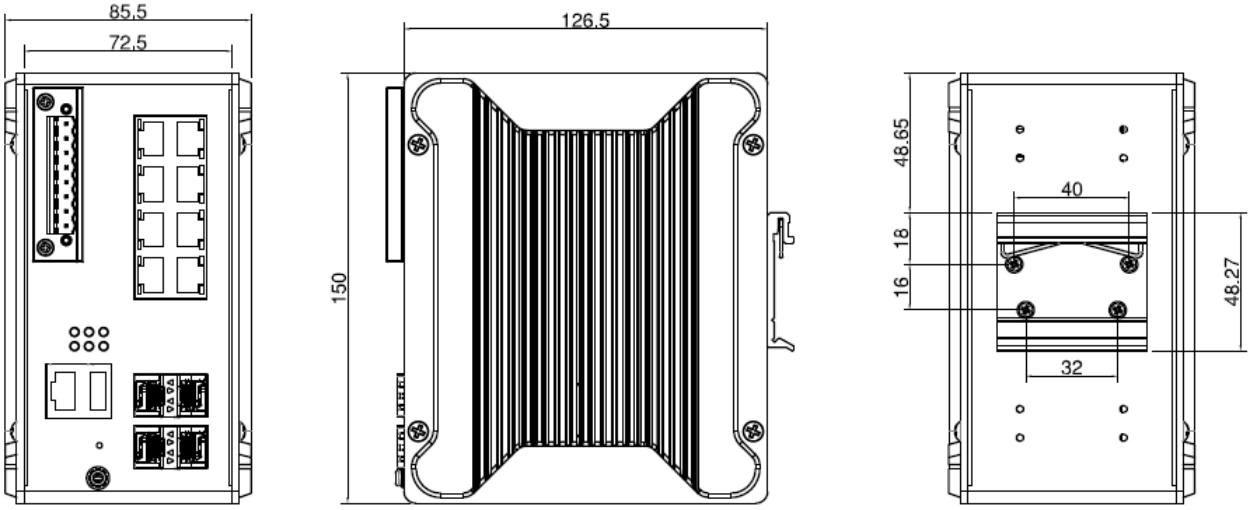
This chapter introduces hardware, and contains information on installation and configuration procedures.

## 2.1 HARDWARE DIMENSION

Dimensions of DP412: 85.5 x 150 x 126.5 (W x H x D) / without DIN Rail Clip



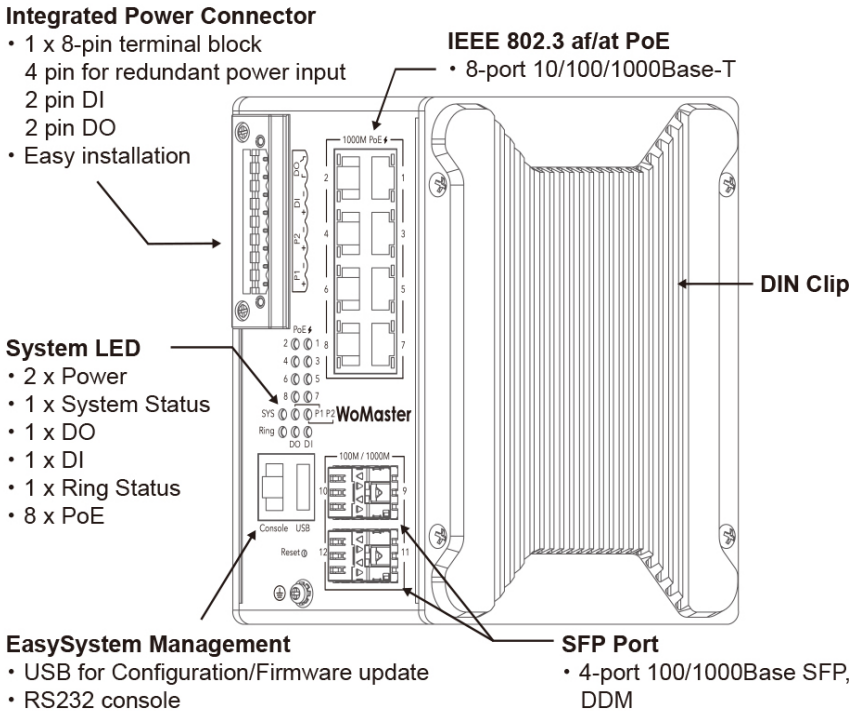

Dimensions of DS412: 85.5 x 150 x 126.5 (W x H x D) / without DIN Rail Clip



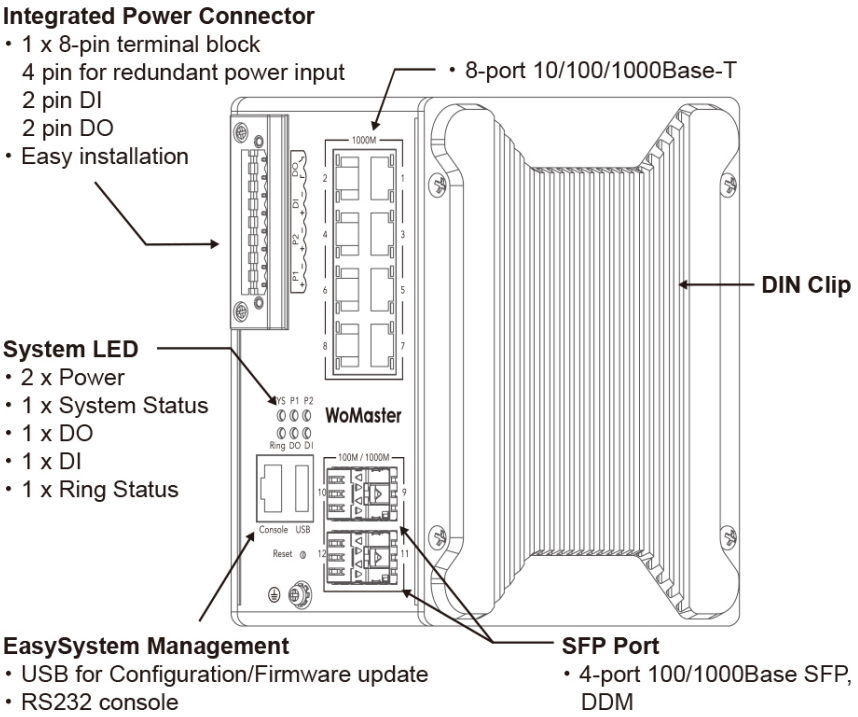
## Front Panel Layout

The front panel from DP412 and DS412 switches includes 8 ports Giga Ethernet, 4 SFP ports, System LED, USB for configuration/firmware management, RJ-45 diagnostic console, 1 x 8-pin terminal block connector (4 pin for power inputs, 2 pin for digital input and 2 pin for alarm relay output) and 1 chassis grounding screw. The difference is for DP412 it is provided with PoE LED. On the rear side of switch there is DIN rail clip attached.

**DP412**



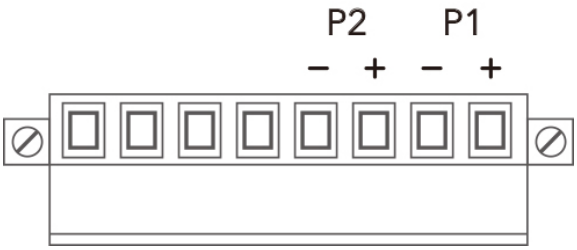

**DS412**



## 2.2 WIRING THE POWER INPUTS

Power Input port in the switch provides 2 sets of power input connections (P1 and P2) on the terminal block. x

On the picture below is the power connector.



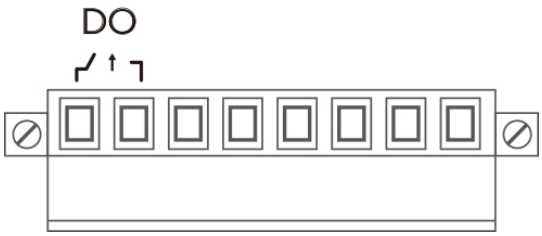

**Wiring the Power Input**

1. Insert the positive and negative wires into the V+ and V- contact on the terminal block connector.
2. Tighten the wire-clamp screws to prevent the power wires from being loosened.
3. Connect the power wires to suitable AC/DC Switching type power supply. The input DC voltage should be in the range of 46VDC to DC 57V DC (recommended to use DC 48V power supply).

> **WARNING:** Turn off AC power input source before connecting the Power to the terminal block connectors, for safety purpose. Don not turn-on the source of AC/DC power before all of the connections were well established.

## 2.3 WIRING THE ALARM RELAY OUTPUT (DO)

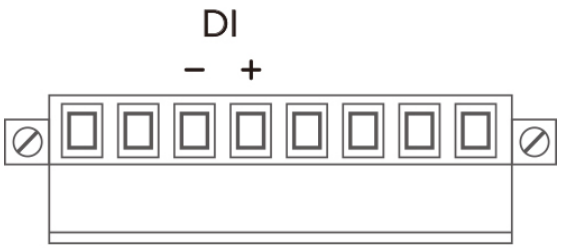
The relay output contacts are located on the front panel of the switch. The relay output consists of the 2-pin terminal block connector that used to detect user-configured events. The two wires attached to the fault contacts form a close circuit when a user-configured event is triggered. If a user-configured event does not occur, the fault circuit remains opened. The fault conditions such as power failure, Ethernet port link break or other pre-defined events which can be configured in the switch. Screw the DO wire tightly after digital output wire is connected.




**NOTE:** The relay contact only supports 0.5 A current, DC 24V. Do not apply voltage and current higher than the specifications.

## 2.4 WIRING THE DIGITAL INPUT (DI)

The Digital Input accepts one external DC type signal input that consists of two contacts on the terminal block connector on the switch's top panel. And can be configured to send alert message through Ethernet when the signal is changed. The signal may trigger and generated by external power switch, such as door open trigger switch for control cabinet. The switch's Digital Input accepts DC signal and can receive Digital High Level input DC 11V~30V and Digital Low Level input DC 0V~10V.




Here are the steps to wire the Digital Input:

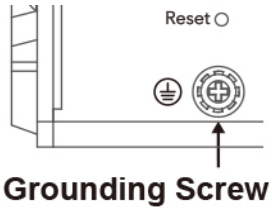
**STEP 1**: Insert the negative and positive wires into the -/+ terminals, respectively.

**STEP 2**: To keep the wires from pulling loose, tighten the wire-clamp screws on the front of the terminal block connector.

**STEP 3**: Insert the terminal block connector prongs into the terminal block receptor, which is located on the switch's top panel.

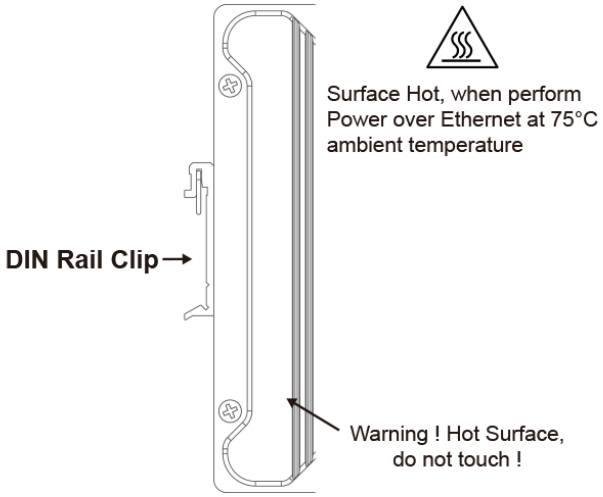
## 2.5 CONNECTING THE GROUDING SCREW

Grounding screw is located on the front side of the switch. Grounding Screw helps limit the effects of noise due to electromagnetic interference (EMI) such as lighting or surge protection. Run the ground connection from the ground screw to the grounding surface prior to connecting devices. And tighten and wire to chassis grounding for better durability.




## 2.6 DIN RAIL MOUNTING

The EN50022 DIN-Rail plate should already attached at the back panel of the switch screwed tightly. If you need to reattach the DIN-Rail attachment plate to the switch, make sure the plate is situated towards the top, as shown by the following figures.




To mount the switch on DIN Rail track, do the following instruction:

1. Insert the top side of DIN Rail track into the slot of DIN Rail clip.
2. Lightly clip the bottom of DIN-Rail to the track and make sure it attached well.
3. To remove the switch from the track, reverse the steps.

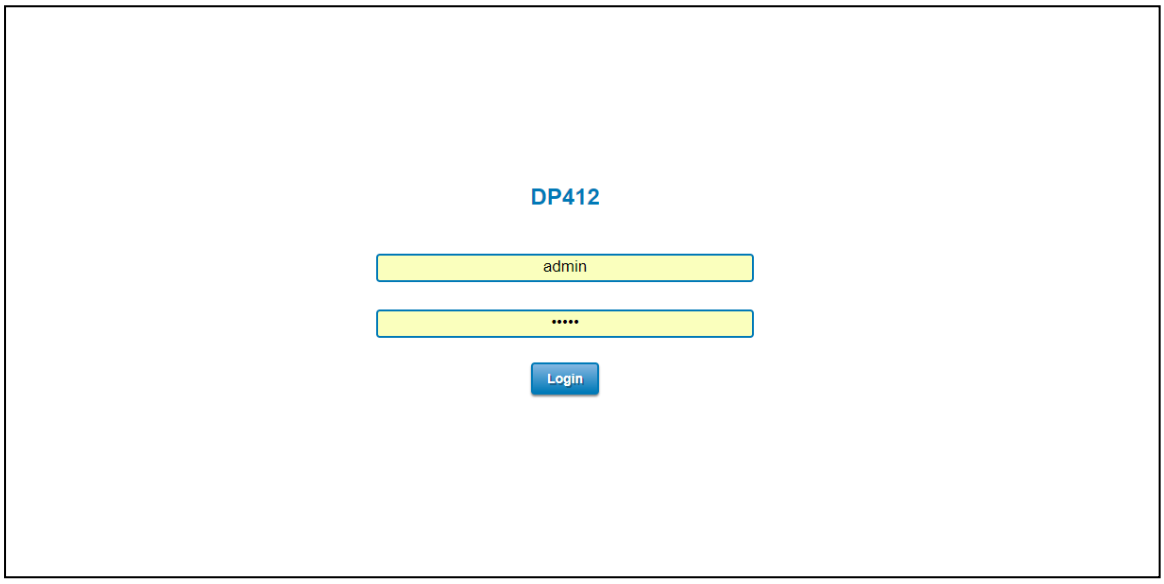
# 3. WEB MANAGEMENT CONFIGURATION

To access the management interface, WoMaster has several ways access mode through a network; they are web management, console management and telnet management. Web interface management is the most common way and the easiest way to manage a network, through web interface management, a switch interface offering status information and a subset of switch commands through a standard web browser. If the network is down, another alternative to access the management interface can be used. The alternative way is by using console and telnet management which is offer configuration way through CLI Interface. WoMaster also provide excellent alternative by configure the switch via RS232 console cable if user doesn't attach user admin PC to the network, or if user loses network connection to Managed Switch. This manual describes the procedures for Web Interface and how to configure and monitor the managed switch only. For the CLI management interface please refers to the *CLI Command User Manual*.

## ***PREPARATION FOR WEB INTERFACE MANAGEMENT***

WoMaster provides Web interface management that allows user through standard web-browser such as Microsoft Internet Explorer, or Mozilla, or Google Chrome, to access and configure the switch management on the network.

1. Plug the DC power to the switch and connect switch to computer.
2. Make sure that the switch default IP address is **192.168.10.1**.
3. Check that PC has an IP address on the same subnet as the switch. For example, the PC and the switch are on the same subnet if they both have addresses that start 192.168.10.x (Ex: **192.168.10.2)**. The subnet mask is 255.255.255.0.
4. Open command prompt and ping **192.168.10.1** to verify that the switch is reachable.
5. Launch the web browser (Internet Explorer or Mozilla Firefox or Google Chrome) on the PC.
6. Type **http://192.168.10.1** (or the IP address of the switch). And then press **Enter** and the login page will appear.
7. Type user name and the password. Default user name: **admin** and password: **admin**. Then click **Login**.



In this Web management for Featured Configuration, user will see all of WoMaster Switch's various configuration menus at the left side from the interface. Through this web management interface user can configure, monitoring, and set the administration functions. The whole information used web management interface to introduce the featured functions. User can use all of the standard web-browser to configure and access the switch on the network.

Following topics are covered in this chapter:

## 3.1 SYSTEM

When the user login to the switch, user will see the system section appear. This section provides all the basic setting and information or common setting from the switch that can be configured by the administrator.
Following topics is included:

3.1.1 Information

3.1.2 User Account

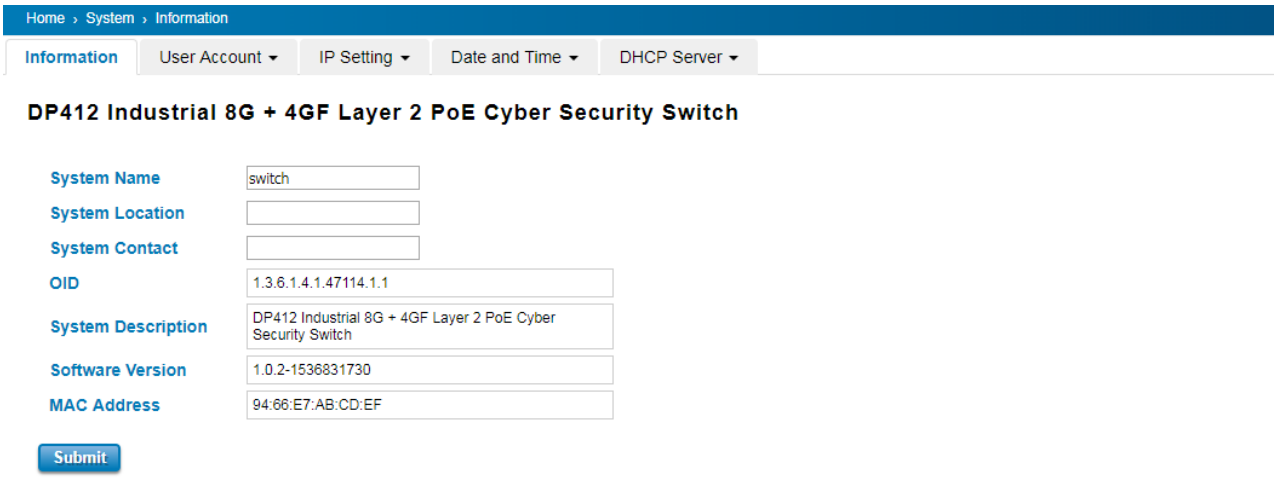
3.1.3 IP Setting

3.1.4 Date and Time

3.1.5 DHCP Server

### 3.1.1 INFORMATION

Information section, this section shows the basic information from the switch to make it easier to identify different switches that are connected to User network. The figure below shows the interface of the Information section.




The description of the Information's interface is as below:

| TERMS | DESCRIPTION |
|---|---|
| **System Name** | **Default: switch**<br>Set up a name to the switch device. |
| **System Location** | **Default: Blank**<br>User can specify the switch's physical location. |
| **System Contact** | **Default: Blank**<br>User can specify the contact person here. User can type the name, mail address or other information of the administrator. |
| **OID** | Indicates the Object ID of the switch. |
| **System Description** | Display the name of the product. |
| **Software Version** | Display the firmware latest version that installed in the device. |
| **MAC Address** | Display the hardware's MAC address that assigned by the manufacturer. |

> **NOTE:** For any kind of changes in configuration settings always remember to click on **Save** to save the settings. Otherwise, all of settings User has made will be lost when the switch is powered off or restarted.

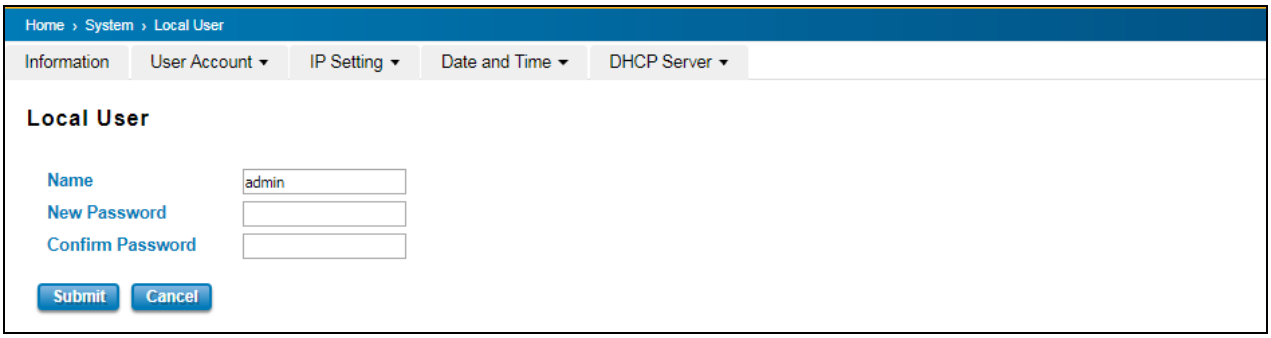
After finish the configuration, click on **Submit** to apply User settings.

## 3.1.2 USER ACCOUNT

WoMaster' switch supports the management accounts; with the Name default setting is **admin** and the authority allow user to configure all of configuration parameters. Below is the **User Account** section that consists of two interfaces, Local User and Radius Interface.

> **NOTE:** For security consideration, please change the password after first log in.

### 3.1.2.1 LOCAL USER




The Local User interface describes how to configure the system user name and password for the web management login. To change the Name and Password, user just needs to input a new Name and New Password then confirm the new password in this Local User section. After finished, click **Submit** to apply the changes. Don't forget to **Save** the settings. Try to re-login with the new User Name and Password.

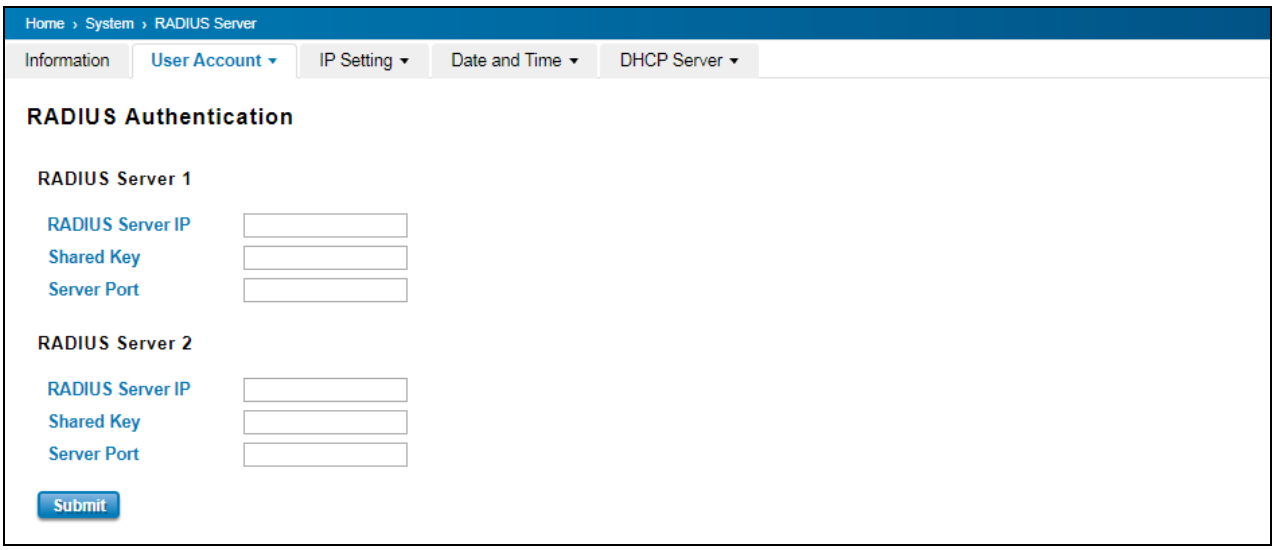
The description of the Local User interface is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Name** | **Default: admin**<br>Key in new user name here. |
| **New Password** | **Default: admin**<br>Key in new password here. |
| **Confirm Password** | Re-type the new password again to confirm it. |

After finished setting up the User Name and Password, click on **Submit** to apply the configuration.

### 3.1.2.2 RADIUS SERVER

The Remote Authentication Dial In User Service (RADIUS) mechanism is a centralized "AAA" (Authentication, Authorization and Accounting) system for connecting to network services. The fundamental purpose of RADIUS is to provide an efficient and secure mechanism for user account management. RADIUS server system allows you to access the switch through secure networks against unauthorized access.




How to set up a RADIUS server:

a. Enter the IP address of the RADIUS server in **Server IP Address**

b. Enter the **Shared Secret** of the RADIUS server

c. Enter the **Server port** if necessary, by default RADIUS server listens to port 1812

d. Click **Submit**

The description of the RADIUS Authentication interface is as below:

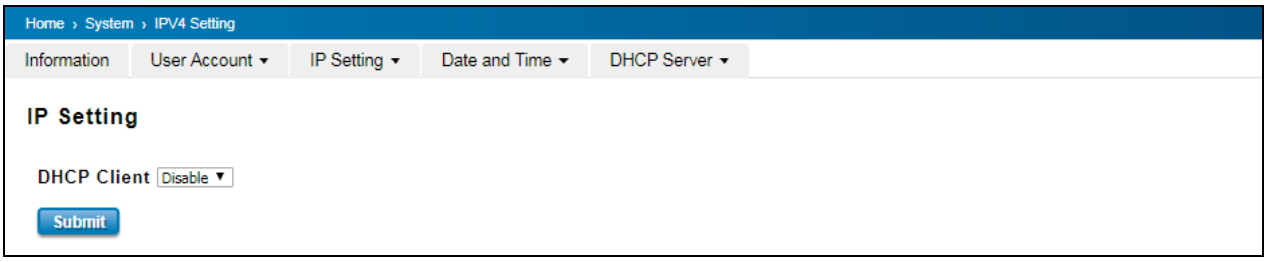
| TERMS | DESCRIPTION |
|---|---|
| **RADIUS Server IP** | Radius Server IP Address |
| **Shared Key** | Shared key are used to verify that RADIUS messages, with the exception of the Access-Request message, are sent by a RADIUS-enabled device that is configured with the same shared key. Shared key also verify that the RADIUS message has not been modified in transit (message integrity). |
| **Server Port** | Set communication port of an external RADIUS server as the authentication database. The general value is 1812 |

### 3.1.3 IP SETTING

IP Setting section allows users to configure both IPv4 and IPv6 values for management access over the network. WoMaster switch supports both IPv4 and IPv6, and can be managed through either of these address types.

#### 3.1.3.1 IPv4

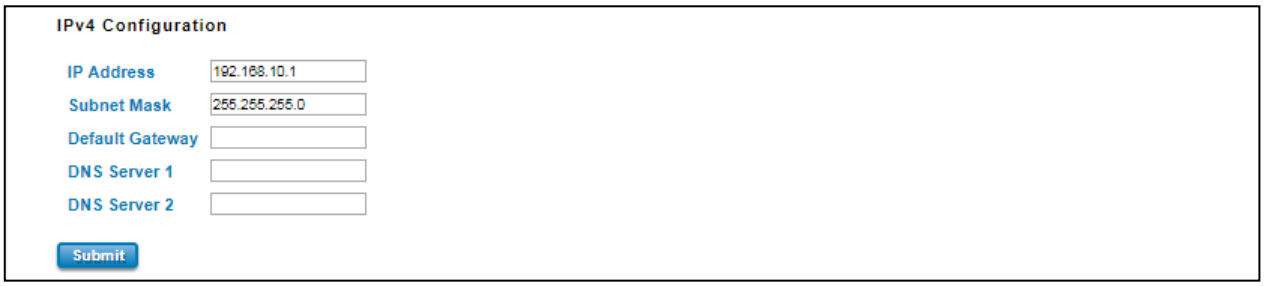
**DHCP Client**




When DHCP Client function is enabled, an IP address will be assigned to the switch from the network's DHCP server. In this mode, the default IP address will be replaced by the one assigned by DHCP server. If DHCP Client is disabled, the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup. The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **DHCP Client** | Select to **Enable** or **Disable** to activate or deactivate the DHCP Client function. |

**IPv4 Configuration**




The IPv4 Configuration includes the switch's IP address and subnet mask, as well as the IP address of the default gateway. In addition, input cells are provided for the IP addresses of a 1st and 2nd DNS server. Configure the managed switch's IP settings. The figure below shows the user interface of IPv4 Configuration.

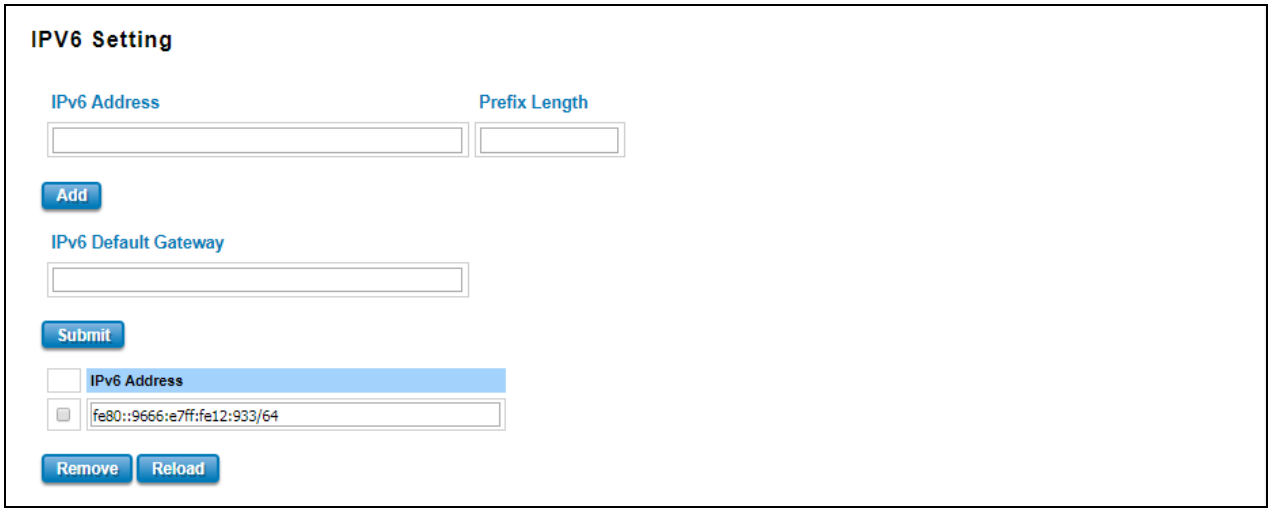
The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **IP Address** | **Default: 192.168.10.1**<br>Set up the IP address reserved by User network for User switch. If DHCP Client function is enabled, no need to assign an IP address to switch as it will be overwritten by DHCP server and shown here. |
| **Subnet Mask** | **Default: 255.255.255.0**<br>Assign the subnet mask for the IP address here. If DHCP Client function is |

| | |
|---|---|
| | enabled, no needs to assign the subnet mask. |
| **Default Gateway** | Assign the gateway for the switch here. |
| **DNS Server 1, DNS Server 2** | Specifies the IP address of the DNS server 1 and 2 that used in user network. |

### 3.1.3.2 IPv6

**IPv6 Setting**




An Ipv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets).The groups are separated by colons (the length of Ipv6 address is 128bits. An example of an Ipv6 address is: fe80::212:77ff:feff:1acb/64.

The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Ipv6 Address** | Add the IPv6 address. The network portion of the address can be configured by specifying the Prefix and using a EUI-64 interface ID in the low order 64 bits. The host portion of the address is automatically generated using the modified EUI-64 form of the interface identifier (Switch's MAC address). |
| **Prefix Length** | The size of subnet or netwok, and it equivalent to the subnetmask, but written in different. Then click **Add** to apply new address to the system. |
| **Ipv6 Default Gateway** | The prefix value must be formatted according to the RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. |
| **Ipv6 Address** | **The default IP address of the Switch: fe80::212:77ff:feff:1acb/64**<br>Select existed Ipv6 address and click **Remove** to delete IP address. Click **Reload** to refresh and reload list. |

## Neighbor Cache

The IPv6 neighbor table includes the neighboring node's IPv6 address, Interface, MAC Address, and the current state of the entry.


The description of the columns is as below:

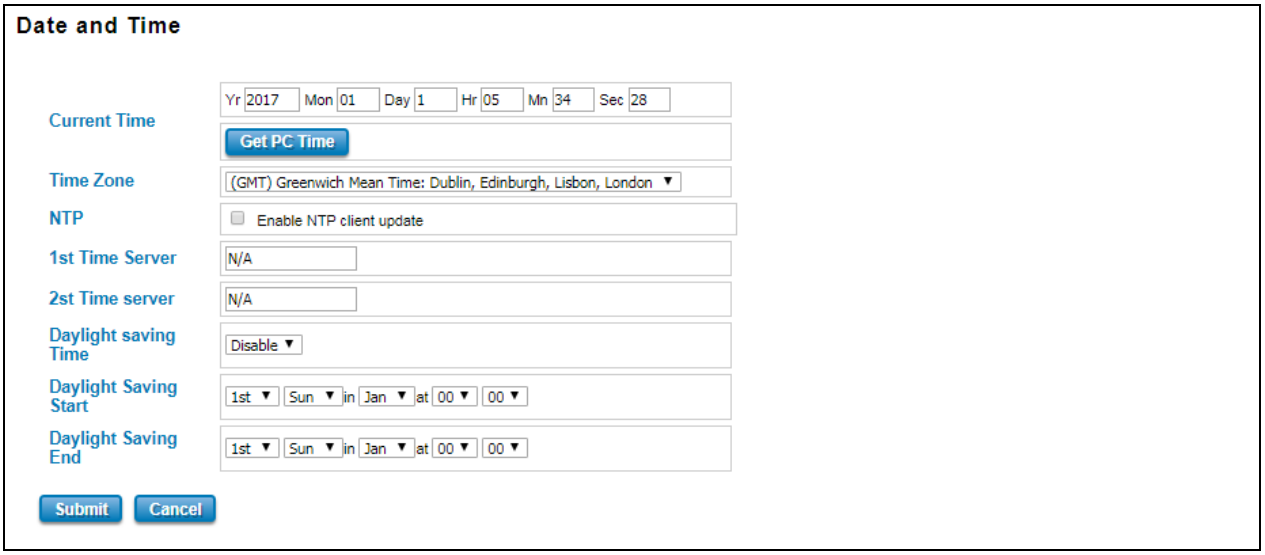
| TERMS | DESCRIPTION |
|---|---|
| **Neighbor Cache** | The system will update Neighbor Cache automatically, and user also can click **Reload** to refresh the table. |

## 3.1.4 DATE AND TIME

### 3.1.4.1 DATE AND TIME SETTING

The WoMaster' switch has a time calibration function based on information from an NTP server or user specified time and date, allowing functions such as automatic warning emails to include a time and date stamp.

> **NOTE:** The WoMaster' switch does not have a real-time clock. The user must update the Current Time to set the initial time for the WoMaster' switch after each reboot, especially when there is no NTP server on the LAN or Internet connection.




The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Current Time** | User can configure time by input it manually. User also can click the **Get Time from PC** to get PC's time setting. |
| **Time Zone** | Choose the Time Zone section to adjust the time zone based on the user area. |
| **NTP** | **Enable NTP Client update** by checking this box. The system will send request packet to acquire current time from the NTP server that assigned.<br>***Make sure that the switch also has the internet connection.** |
| **1st Time Server & 2nd Time Server** | Choose from NTP Server List, to adjust User system time. |
| **Daylight Saving Time** | Enable the Daylight Saving Function and the setting of function start and end time or disable it. |
| **Daylight Saving Start** & **Daylight Saving End** | Allows user to sets the Start and End time individually. |

After finished configuring, click on **Submit** to activate the configuration.

## ***IEEE 1588 PTP***

### IEEE 1588

IEEE 1588 was published in 2002, expands the performance capabilities of Ethernet networks to control systems that operate over a communication network. In recent years an increasing number of electrical power systems have been using a more distributed architecture with network technologies that have less stringent timing specifications. IEEE 1588 generates a master-slave relationship between the clocks, and enforces the specific timing requirements in such power systems. All devices ultimately get their time from a clock known as the grandmaster clock. In its basic form, the protocol is intended to be administration free."

### How Does an Ethernet Switch Affect 1588 Synchronization?

An Ethernet switch potentially introduces multi-microsecond fluctuations in the latency between the 1588 grandmaster clock and a 1588 slave clock. When these fluctuations are incorrect, it will cause synchronization errors. The magnitude of these fluctuations depends on the design of the Ethernet switch and the details of the communication traffic. Experiments with prototype implementations of IEEE 1588 indicate that with suitable care the effect of these fluctuations can be successfully managed. For example, use of appropriate statistics in the 1588 devices to recognize significant fluctuations and use suitable averaging techniques in the algorithms controlling the correction of the local 1588 clock will be good design means to achieve the highest time accuracy.

### Can Ethernet switches be designed to avoid the effects of these fluctuations?

A switch can be designed to support IEEE 1588 while avoiding the effects of queuing. In this case two modifications to the usual design of an Ethernet switch are necessary:

1. The **Boundary Clock and Transparent Clock** functionalities defined by IEEE 1588 must be implemented in the switch.

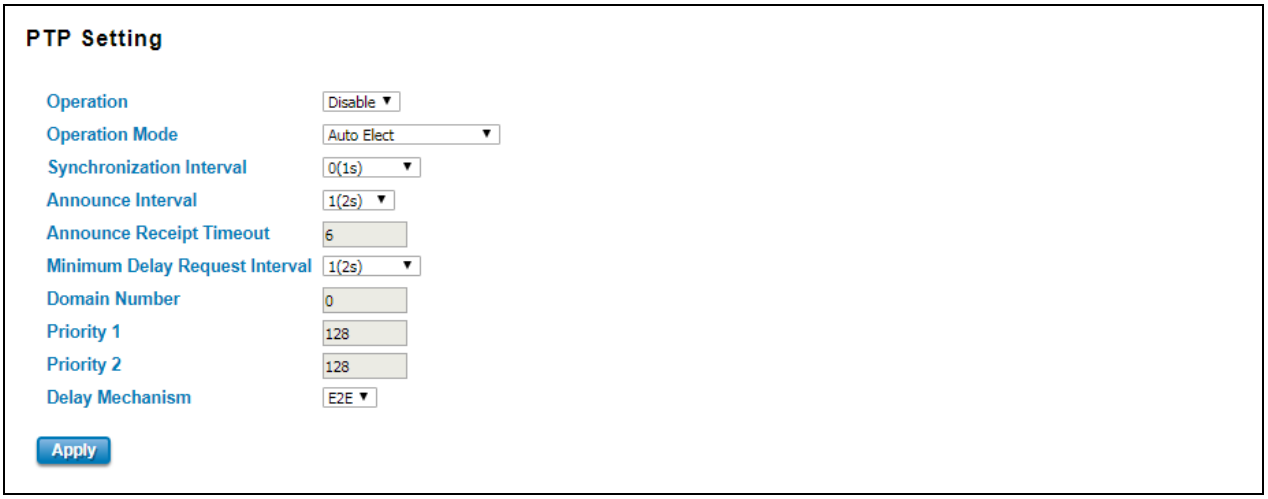
2. The switch must be configured so that it does not pass IEEE 1588 message traffic using the normal communication mechanisms of the switch.

Such an Ethernet switch will synchronize clocks directly connected to one of its ports to the highest possible accuracy.

The main function of IEEE 1588 is to synchronize the clocks of different end devices over a network at speeds faster than one Micro-second. After time synchronized, the system time will display the correct time of the PTP server.

### 3.1.4.2 PTP SETTING

The PTP can be set in this PTP Setting webpage in which the user can configure PTP. The top part of this figure allows the users to enable or disable the PTP function. To enable PTP on the managed switch, please choose Enable. Note that the PTP functions will not active if the Operation is disabled. Please see description of PTP Setting in table description. Note that after setting the desired PTP Setting, please click Apply button to allow the configuration take effect.




The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Operation** | **Default: Disable**<br>Enable/Disable the PTP function. This is the main option that needs to be enabled so that the PTP function will work |
| **Operation Mode** | **Default: Auto Elect**<br>Choose Mode (Auto Elect, Preferred Master Clock or Slave) |
| **Synchronization Interval** | **Default: 0 (1s)**<br>Set the interval of the sync packet transmitted time. Small interval causes too frequent sync, which will cause more load to the device and network. |
| **Announce Interval** | **Default: 1 (2s)**<br>Sets the announce message interval |
| **Announce Receipt Timeout** | **Default: 6**<br>The multiple of announce message receipt timeout by the announce message interval. |
| **Minimum Delay Request Interval** | **Default: 1 (2s)**<br>Minimal delay request message interval |
| **Domain Number** | Subdomain name (IEEE 1588-2002) or the domain Number (IEEE 1588-2008) fields in PTP messages |
| **Priority 1** | **Default: 128**<br>Set the clock priority 1 (PTP version 2). The lower values take precedence to be |

| | |
|---|---|
| | selected as the master clock in the best master clock algorithm, 0 = highest priority, 255 = lowest priority. |
| **Priority 2** | **Default: 128**<br>Set the clock priority 2 (PTP version 2). The lower values take precedence to be selected as the master clock in the best master clock algorithm (BMCA), 0 = highest priority, 255 = lowest priority. |
| **Delay Mechanism** | **Default: E2E**<br>Configures the delay mechanism in boundary clock mode.<br>**E2E** - The delay request or response mechanism used in the boundary clock mode.<br>**P2P** - The peer-to-peer mechanism used in the boundary clock mode |

## 3.1.5 DHCP SERVER

### DHCP Server Setting

WoMaster' switch has DHCP Server Function that will provide a new IP address to DHCP Client. After enable DHCP Server function, set up the Network IP address for the DHCP server IP address, Subnet Mask, Default Gateway address and Lease Time for client. Below is the DHCP Server Setting interface

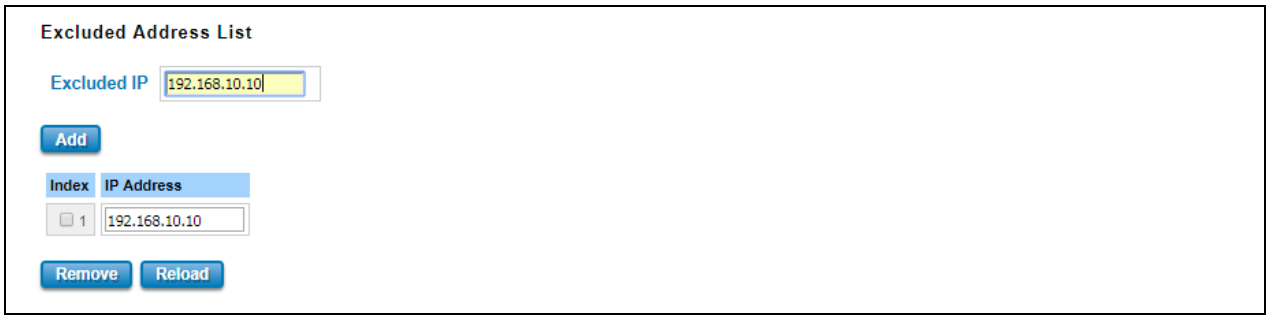

The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Global Setting** | Select to **Enable** or **Disable** to activate and deactivate DHCP Server function. |
| **Pool Name** | Add address pool name to local DHCP Server |
| **Network** | Enter the starting IP addresses for the DHCP server's IP assignment. |
| **Mask** | Assign the subnet mask for the IP address here. |
| **Default Gateway** | Enter the ending IP addresses for the DHCP server's IP assignment. |
| **Lease Time** | The maximum length of time for the IP address lease. Enter the Lease time in minutes. (Lease Time range: 60-31536000 seconds) |

The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set user computers to be DHCP clients by setting their TCP/IP settings to “Obtain an IP Address Automatically.” When user turns the computers on, they will automatically load the proper TCP/IP settings provided by the switch. If User manually assigns IP addresses to User computers or devices, make sure the IP addresses are outside of this range or User may have an IP conflict. After finished configuring, click on **Submit** to activate the configuration.

## Excluded Address List

The figure below shows the **Excluded Address List,** the IP address that is listed in the **Excluded Address List** table will not be assigned to the network devices.

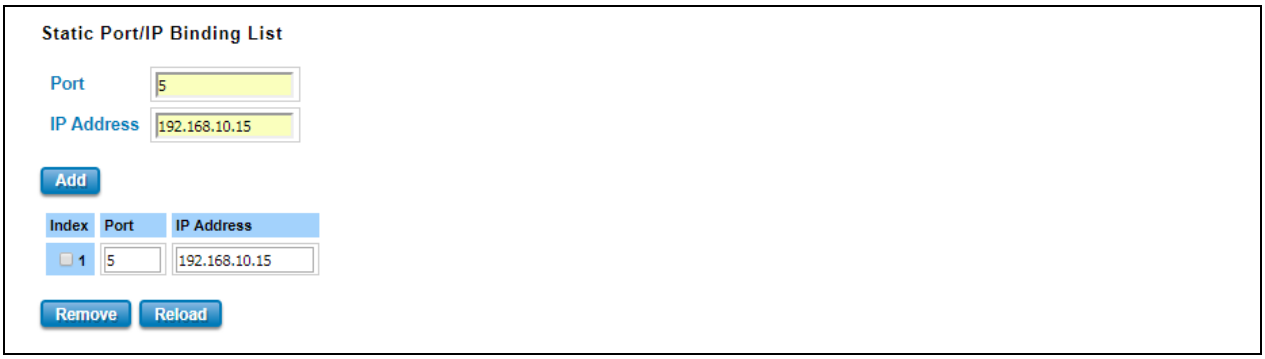



The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Excluded Address List** | Type a specific address into the **Excluded IP** field for the DHCP server reserved IP address. Then click **Add,** to remove an IP address from the list click **Remove**. To refresh the list, click **Reload**. |

## Static Port/IP Binding List

The figure below is the web interface for **Static Port/IP Binding List.**



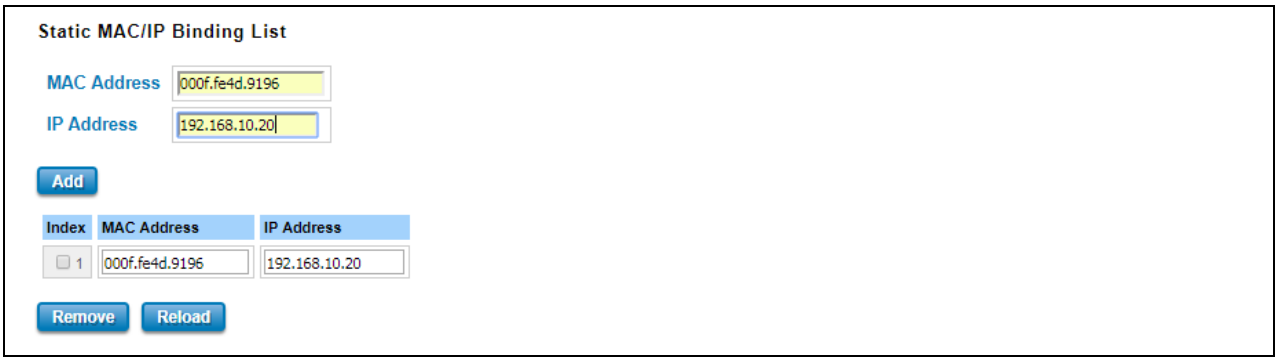

Type the specific Port and IP address, and then click **Add** to add a new Port & IP address binding rule for a specific client. The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Port** | The port that wishes binding. |
| **IP Address** | The IP address that will assign to the device with the Binding MAC address. |

To remove from the binding list, select the index and click **Remove**. To refresh the list, click **Reload**.

## Static MAC/IP Binding List

The figure below is the web interface for **Static MAC/IP Binding List.**




Type the specific MAC and IP address, and then click **Add** to add a new MAC & IP address binding rule for a specific client.

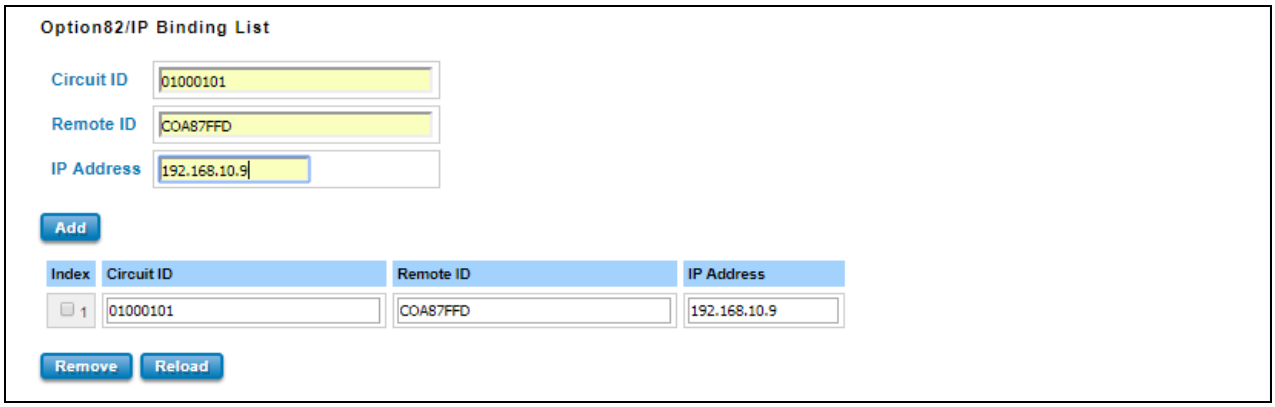
The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **MAC Address** | The MAC address of the device that wishes binding. |
| **IP Address** | The IP address that will assign to the device with the Binding MAC address. |

To remove from the binding list, select the index and click **Remove**. To refresh the list, click **Reload**.

## Option 82/IP Binding List

The figure below is the web interface for **Option 82/IP Binding List.**




Type the specific Circuit ID, Remote ID and IP address, and then click **Add** to add a new binding rule for a specific client.

The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Circuit ID** | The Circuit ID of the device that wishes binding. |
| **Remote ID** | The Remote ID of the device that wishes binding. |
| **IP Address** | The IP address that will assign to the device with the Binding MAC address. |

To remove from the binding list, select the index and click **Remove**. To refresh the list, click **Reload**.

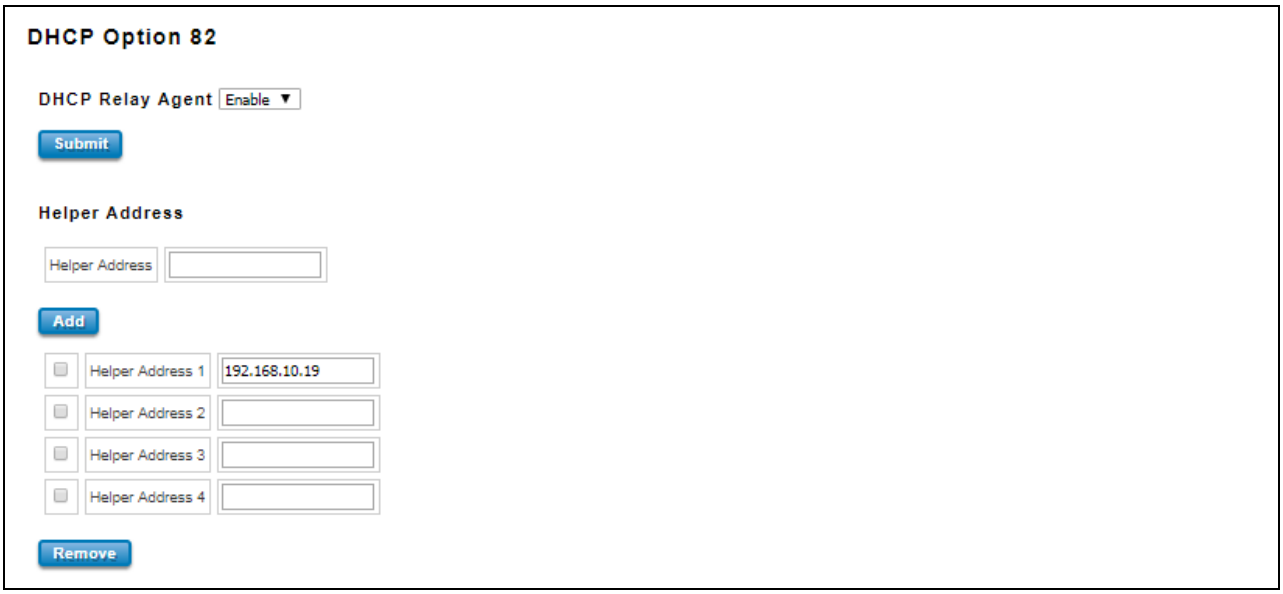
## DHCP Option 82

The DHCP Relay Agent (or DHCP Option 82) makes it possible for DHCP broadcast messages to be sent over routers. The DHCP Relay Agent enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or those that are not located on the local subnet.

**DHCP Option 82** is used by the relay agent to insert additional information into the client's DHCP request. The Relay Agent Information option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers can recognize the Relay Agent Information option and use the information to implement IP addresses to Clients.

When DHCP Option 82 is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

The Option 82 information contains 2 sub-options, Circuit ID and Remote ID, which define the relationship between the end device IP and the DHCP Option 82 server. The **Circuit ID** is a 4-byte number generated by the Ethernet switch—a combination of physical port number and VLAN ID.




The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **DHCP Option 82** | Select to **Enable** or **Disable** to activate or deactivate DHCP relay agent function, and then select the modification type of option 82. |
| **Helper Address** | There are 4 fields for the DHCP server's IP address. Fill the field with preferred IP address of DHCP Server. |

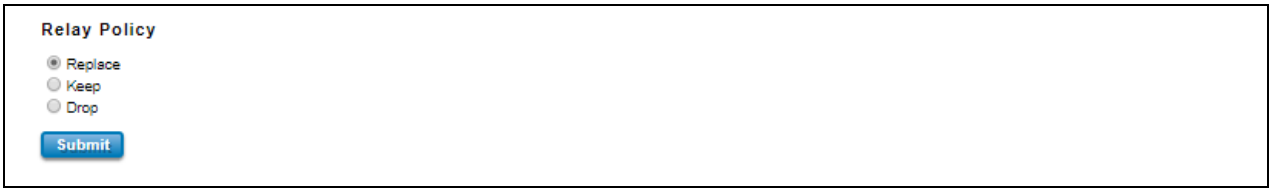
And click **Submit** to activate the DHCP relay agent function. All the DHCP packets from client will be modified by the policy and forwarded to DHCP server through the gateway port. When **Option 82** is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address).

## Relay Policy

**Replace -** Replaces the existing option 82 field and adds new option 82 field. (This is the default setting).

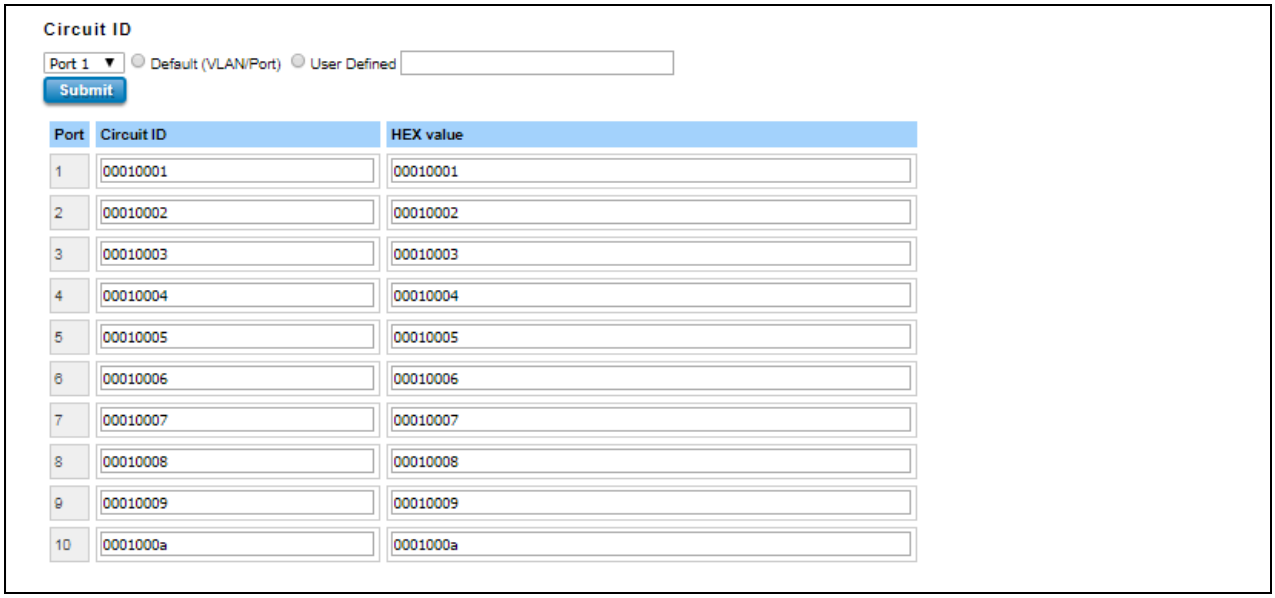
**Keep** - Keeps the original option 82 field and forwards to server.

**Drop** - Drops the option 82 field and do not add any option 82 field.

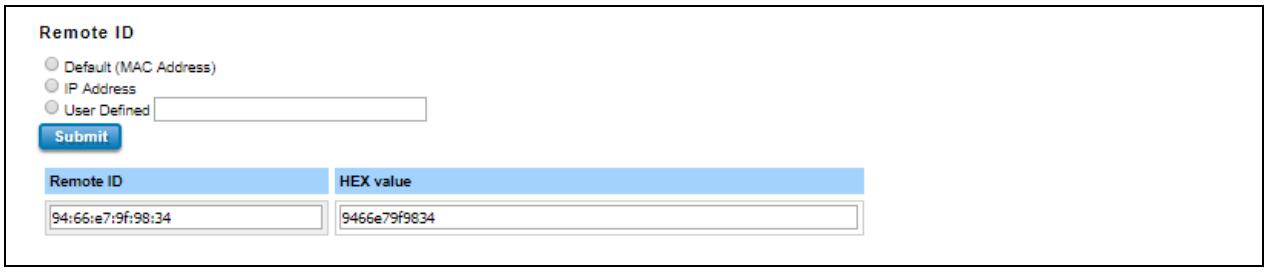



## Circuit ID & Remote ID

The DHCP Option 82 information also contains 2 sub-options, **Circuit ID** and **Remote ID**, which define the relationship between the end device IP and the DHCP Option 82 server. The Circuit ID is a 4-byte number generated by the Ethernet switch. To activate this section, please make sure that DHCP Relay Agent is enabled.




The format of the **Circuit ID** is shown above: 00–01–00–01, this is where the first byte is “00”, the second and the third byte “01-00” is formed by the port VLAN ID, and the last byte “01” is formed by the port number. For example: 00–01–00–01 is the **Circuit ID** of port number 1 with port VLAN ID 1.

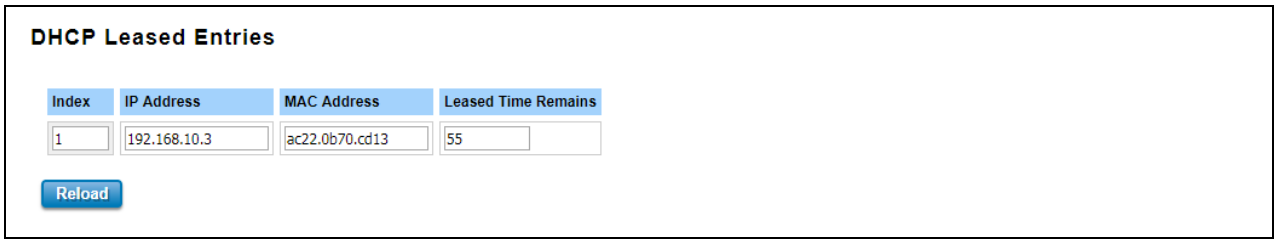



The **Remote ID** identifies the relay agent itself and can be one of the following:

1. The IP address of the relay agent.
2. The MAC address of the relay agent.
3. A combination of IP address and MAC address of the relay agent.
4. A user-defined string.

**DHCP Leased Entries**

The figure below shows the **DHCP Leased Entries.** It will show the MAC and IP address that was assigned by switch.




Click the **Reload** button to refresh the list.

The description of the columns is as below:

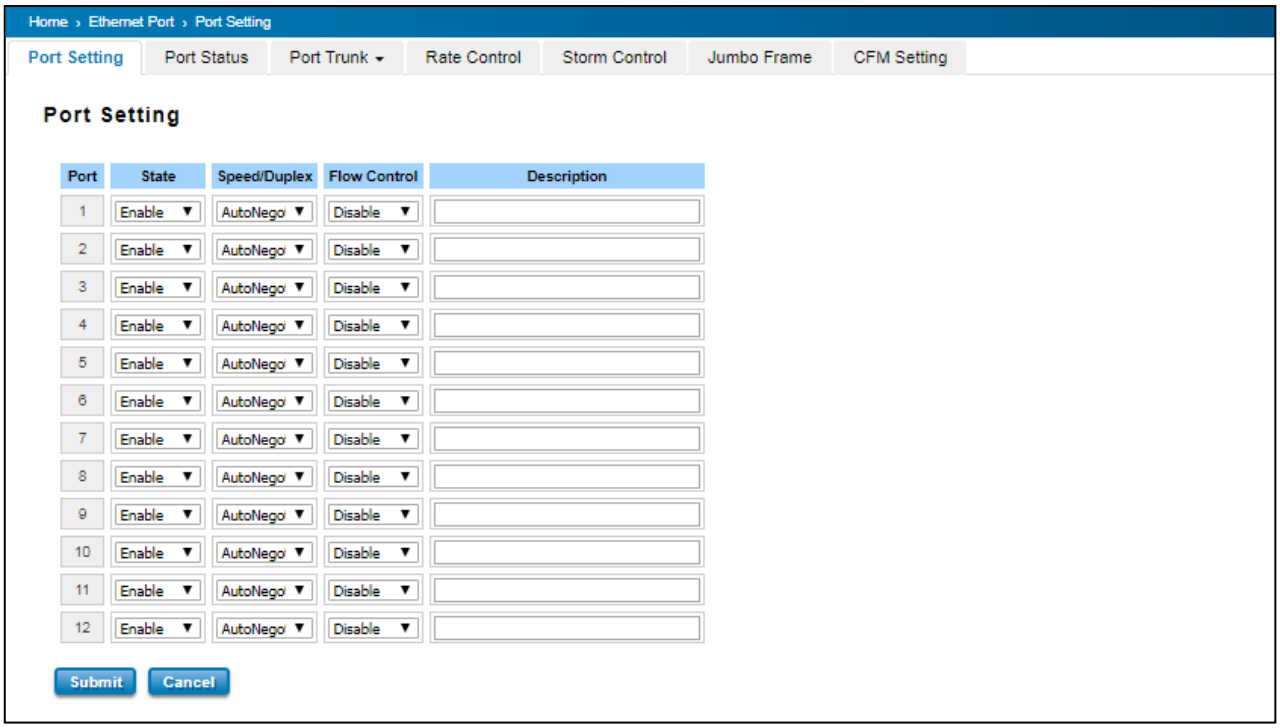
| TERMS | DESCRIPTION |
|---|---|
| **IP Address** | IP address that was assigned by switch. |
| **MAC Address** | MAC address that was assigned by switch. |
| **Leased Time Remains** | Remains time for the IP address leased |

## 3.2 ETHERNET PORT

Ethernet Port section is used to access the port configuration and rate limit control. It also allows User to view port status and port trunk information.

### 3.2.1 PORT SETTING

Port Settings section allows users to enable or disable each port function; state the speed/duplex of each port; and enable or disable the flow control of the port.



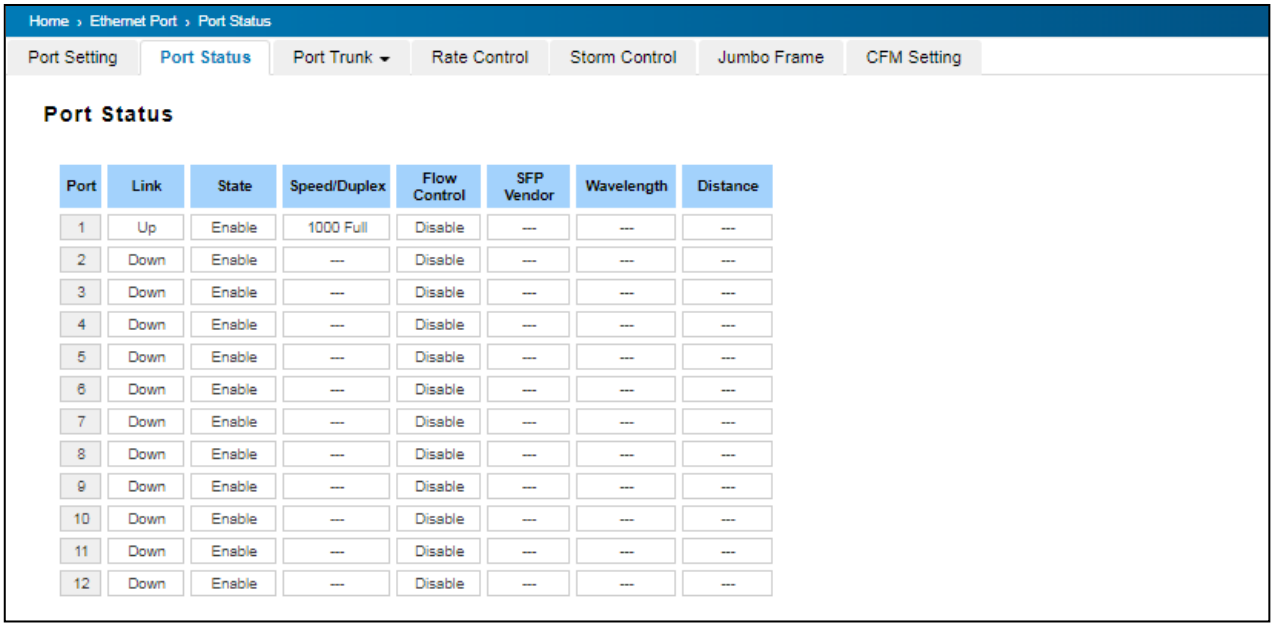

The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| Port | Shows port number |
| State | **Default: Enable**<br>Enable or disable a port |
| Speed/Duplex | **Default: AutoNegotiation**<br>Users can set the bandwidth of each port as Auto-negotiation, 100 full,100 half,10 full,10 half mode for **Giga Ethernet Port 1~8 (ge1~ge8)**. For **Gigabit Ethernet Port 9~12: (ge9~ge12)**, it can be set up to 100M Full Duplex(100 Full) only. |
| Flow Control | **Default: Disable**<br>**Enable** means that User need to activate the flow control function in order to let the flow control of that corresponding port on the switch to work. **Disable** means that User doesn't need to activate the flow control function, as the flow control of that corresponding port on the switch will work anyway. |
| **Description** | The description of interface. |

After finished configuring the settings, click on **Submit** to save the configuration.

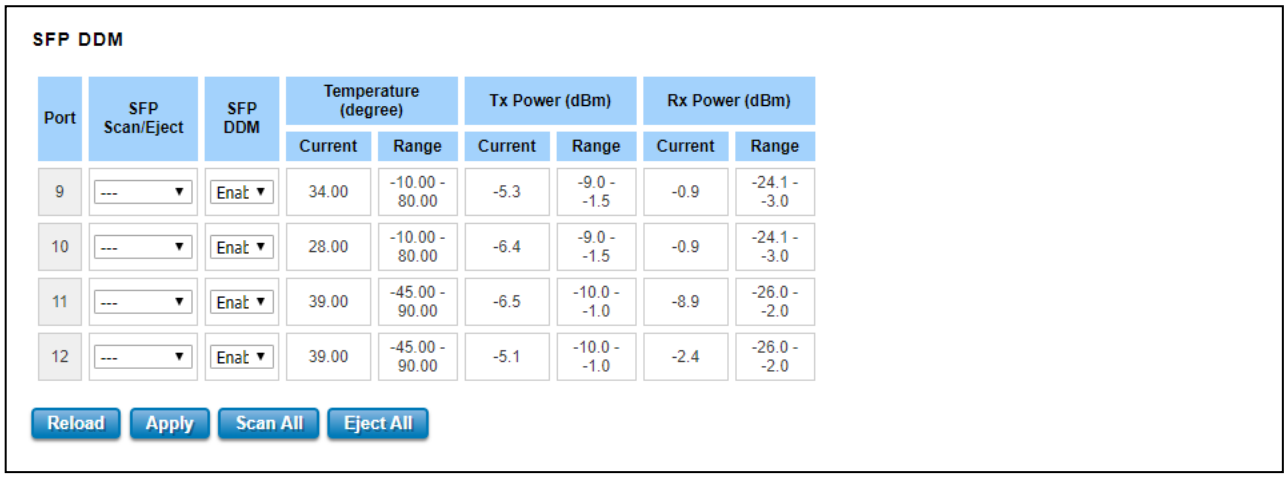
## 3.2.2 PORT STATUS

Port Status provides current port status.




### SFP DDM

WoMaster Industrial Switch supports the SFP module with digital diagnostics monitoring (DDM) function. This technology allows the user to monitor real-time parameters of the fiber optic transceivers, like optical input/output power, temperature, and transceiver supply voltage of an SFP module via SFP DDM section. This section shows and configures the operational status, such as Scan/Eject the SFP, Enable/Disable SFP DDM, Temperature degree, Tx Power statistics, Rx Power Statistics in real time.




From the figure above, the real-time diagnostic parameters can be monitored to alert the system when the transceiver's specified operating limits are exceeded and compliance cannot be ensured. Basically the SFP DDM has its own specification, as we can see from the table it is showed the temperature, Tx Power and Rx Power range. If all of the current values are higher or lower than the available range or does not meet the SFP vendor specification, there would be a problem for the fiber connection.

The description of the Port Status and SFP DDM columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **SFP Scan/Eject** | Scan the SFP module or Eject the SFP module. |
| **SFP DDM** | Enable/Disable the DDM function. |
| **Temperature** | The specific temperature range and current temperature detected of DDM SFP transceiver. |
| **Tx Power (dBm)** | The range and current transmit power of DDM SFP transceiver. |
| **Rx Power (dBm)** | The range and current received power of DDM SFP transceiver. |

Click **Reload** to reload the all port information, click **Scan All** to scan the SFP transceiver module and display the statistics. **Eject All** to eject the SFP transceiver that User has selected or plugged. User can eject one port or eject all by click the **Eject All** button. Click **Apply** to apply the configuration that just made.

### 3.2.3 PORT TRUNK

**Port Trunk**, also called "Link Aggregation", is a method of combining multiple network connections in parallel to increase throughput beyond what a single connection could sustain. The aggregated ports can be viewed as one physical port so that the bandwidth is higher than merely one single Ethernet port. The member ports of the same trunk group can balance the loading and backup for each other. WoMaster' industrial managed switches support 2 types of Port Trunk. One is LACP (dynamic) and the other is Static. Link Aggregation Control Protocol (LACP), which is a protocol running on layer 2, provides a standardized means in accordance with IEEE 802.3ad to bundle several physical ports together to form a single logical channel. LACP mode is more flexible, and it can change modes, either trunk or single port. Dynamic Port Trunk also provides a redundancy function, in case one of the links fails. If one of the trunk members has failed, it will still work well in LACP mode, but it will link down if using static mode. All the ports within the logical channel or so-called logical aggregator work at the same connection speed and LACP operation requires full-duplex mode. Static mode is still necessary, because some devices only support static trunk.

#### Port Trunk Concept

Port trunking protocol that provides the following benefits:

• Flexibility in setting up User network connections, since the bandwidth of a link can be doubled, tripled, or quadrupled.

• Redundancy—if one link is broken, the remaining trunked ports share the traffic within this trunk group.

• Load sharing—MAC client traffic can be distributed across multiple links.

To avoid broadcast storms or loops in User network while configuring a trunk, first disable or disconnect all ports that User want to add to the trunk or remove from the trunk. After User finish configuring the trunk, enable or re-connect the ports.

If all ports on both switch units are configured as 100BaseTX and they are operating in full duplex mode, this means that users can double, triple, or quadruple the bandwidth of the connection by port trunk between two switches.

When User activates port trunk, certain settings on each port will be reset to factory default values or disabled:

• Communication redundancy will be reset.

• 802.1Q VLAN will be reset.

• Multicast Filtering will be reset.

• Port Lock will be reset and disabled.

• Set Device IP will be reset.

• Mirror will be reset.

After port trunk has been activated, User can configure these items again for each trunk port.

## Port Trunk Setting

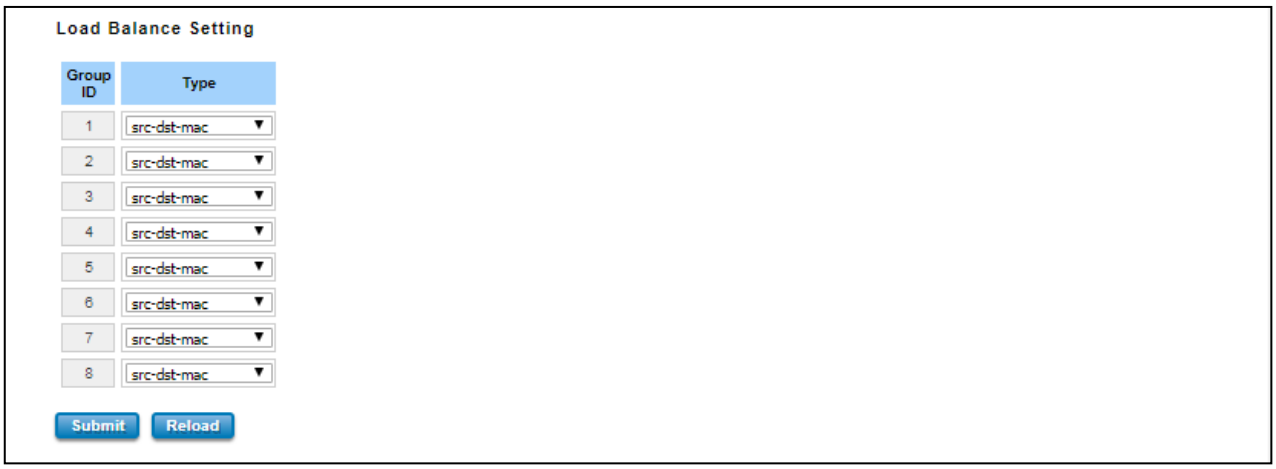

The switch can support up to 8 trunk groups with 2 trunk members. Since the member ports should use same speed/duplex, max trunk members would be 8 for 100Mbps, and 2 members for Gigabit.

The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Group ID** | **Default: 0**<br>Group ID is the ID for the port trunk group. Ports with same group ID are in the same group. |
| **Type** | **Default: Blank**<br>**Static** and **LACP.** Each Trunk Group can only support Static or LACP. Choose the type User need here. |

Click on **Submit** to apply the configuration, and **Reload** to refresh the table.

## Load Balance Setting



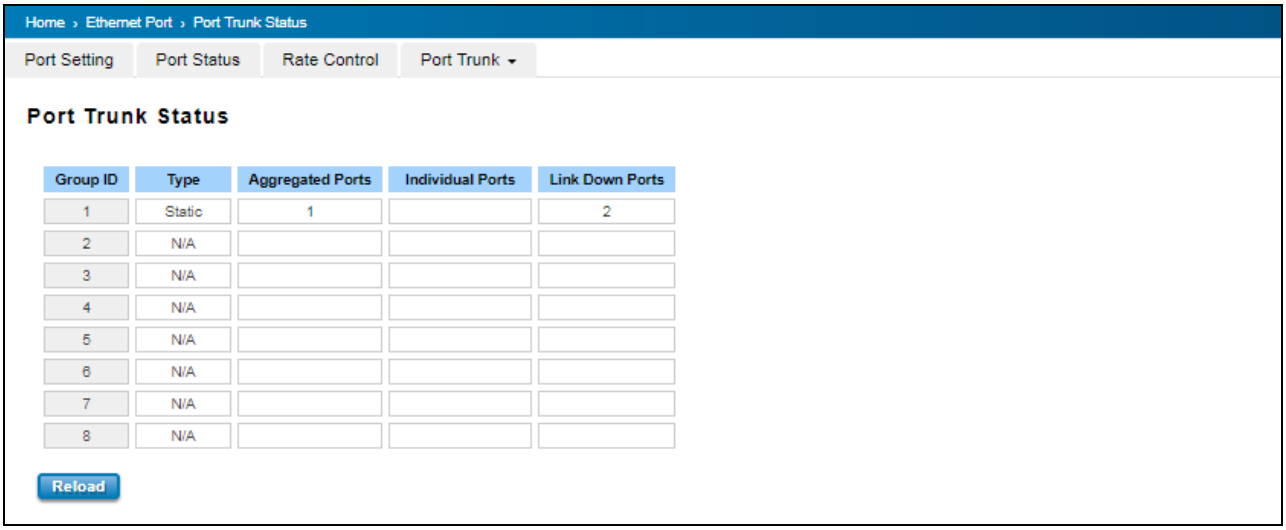

**Load Balance Type:** Each Trunk Group can support several Load Balance types that can be seen from the table below:

| Type | Description |
|---|---|
| src-mac | load distribution is based on the source MAC address |
| dst-mac | load distribution is based on the destination-MAC address |
| src-dst-mac | load distribution is based on the source and destination MAC address |
| src-ip | load distribution is based on the source IP address |
| dst-ip | load distribution is based on the destination IP address |
| src-dst-ip | load distribution is based on the source and destination IP address |

Click **Submit** to apply your settings.

## Port Trunk Status

This page shows the status of port aggregation. Once the aggregation ports are negotiated well, User will see following status. The figure below is the Port Trunk Status interface.



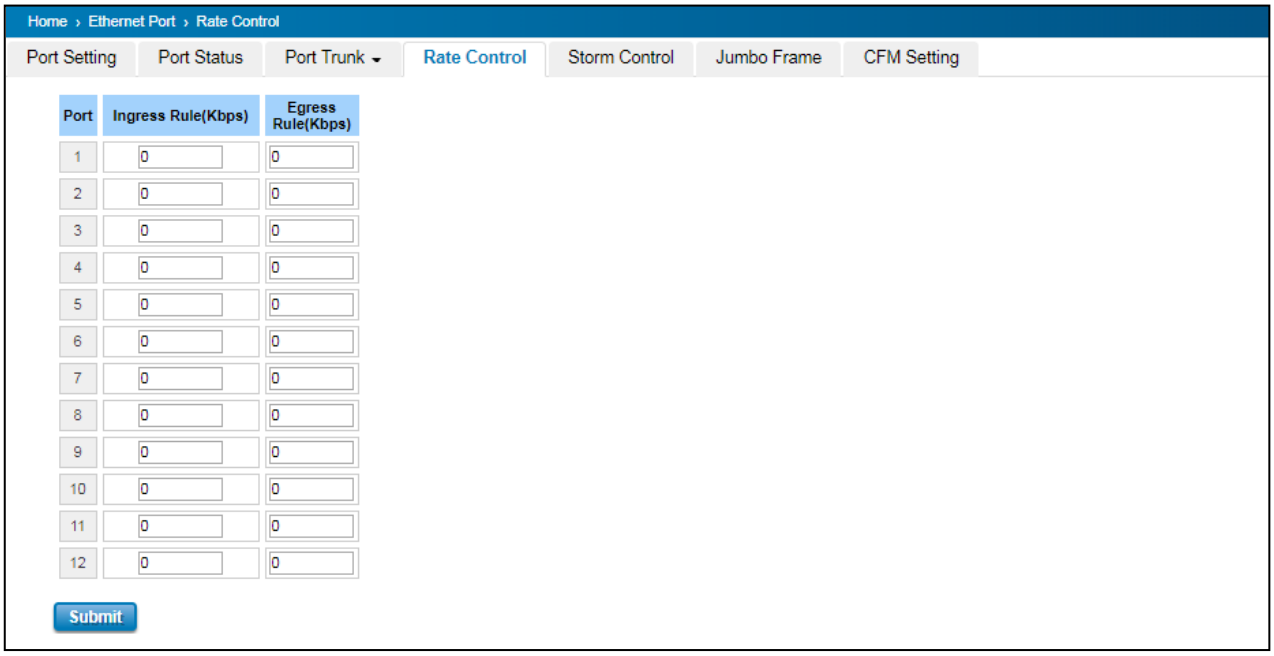
The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Group ID** | Display Trunk 1 to Trunk 5 setup in Aggregation Setting. |
| **Type** | Static or LACP setup in Aggregation Setting. |
| **Aggregated Ports** | When LACP links well, User can see the member ports in aggregated column. |
| **Individual Ports** | When LACP is enabled, member ports of LACP group which are not connected to correct LACP member ports will be displayed in the Individual column. |
| **Link Down** | When LACP is enabled, member ports of LACP group which are not linked up will be displayed in the Link Down column. |

To refresh the list, click **Reload**.

## 3.2.4 RATE CONTROL

Rate control is a form of flow control used to enforce a strict bandwidth limit at a port. User can program separate transmit (Egress Rule) and receive (Ingress Rule) rate limits at each port, and even apply the limit to certain packet types.




The description of the columns is as below:

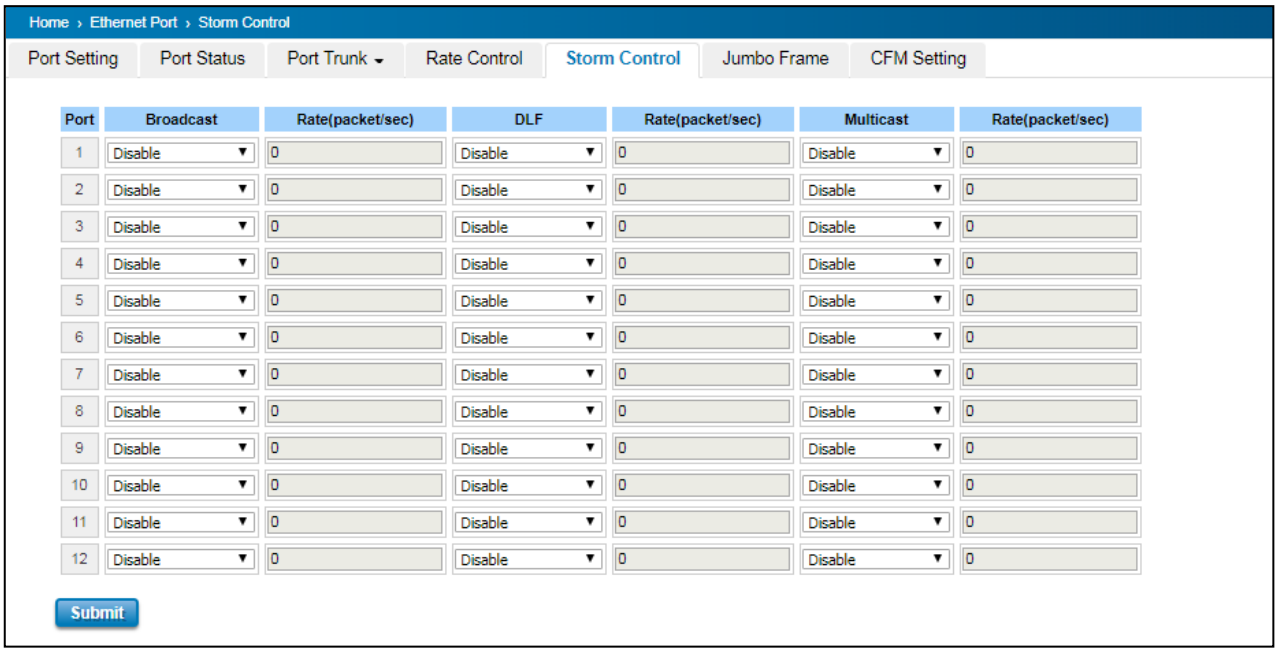
| TERMS | DESCRIPTION |
|---|---|
| **Packet Type** | Select the packet type that wanted to filter. |
| **Ingress** | The packet types of the Ingress Rule listed here include **Broadcast Only** / **Broadcast and multicast** / **Broadcast, Multicast and Unknown Unicast** or **All**. |
| **Egress** | The packet types of the Egress Rule (outgoing) only support **all** |

| | |
|---|---|
| | packet types. |
| **Rate (Ingress & Egress)** | **Default value Ingress: 8 Mbps**<br>**Default value Egress: 0 Mbps (**0 stands for disabling the rate control for the port.**)**<br>Valid values are from 1Mbps-100Mbps for fast Ethernet ports and gigabit Ethernet ports. The step of the rate is 1 Mbps. |

Click on **Submit** to apply the configuration.

## 3.2.5 STORM CONTROL

A LAN storm appears when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the implementation, mistakes in network configuration, or users issuing a denial-of-service attack can cause a storm. Storm control prevents traffic on a LAN from being disrupted by a broadcast, DLF, or multicast storm on a port. In this page, user can configure the storm control for each port.

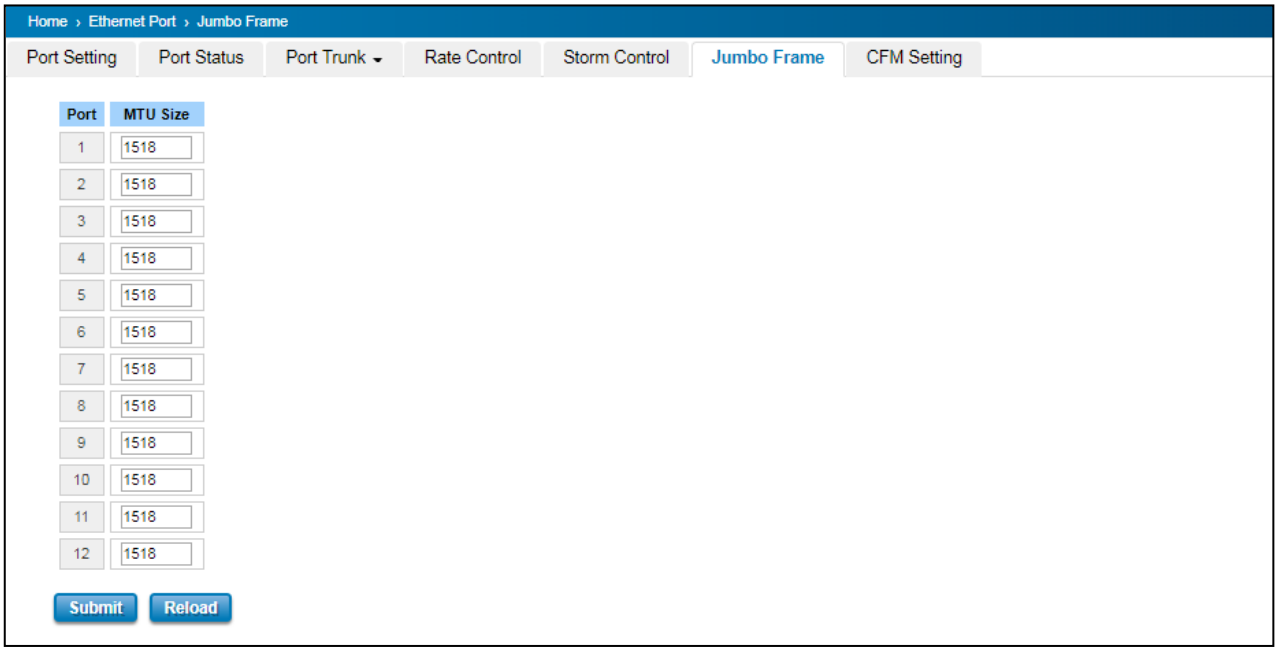



Click Submit to apply the configuration.

| TERMS | DESCRIPTION |
|---|---|
| **Broadcast** | Default: Disable<br>Set enable to control Broadcast Packets |
| **DLF** | Default: Disable<br>Set enable to control Destination Lookup Failure packets |
| **Multicast** | Default: Disable<br>Set enable to control Multicast Packets |
| **Rate(Packet/Sec)** | Rate limit value 0~262142 packet/sec |

## 3.2.6 JUMBO FRAME

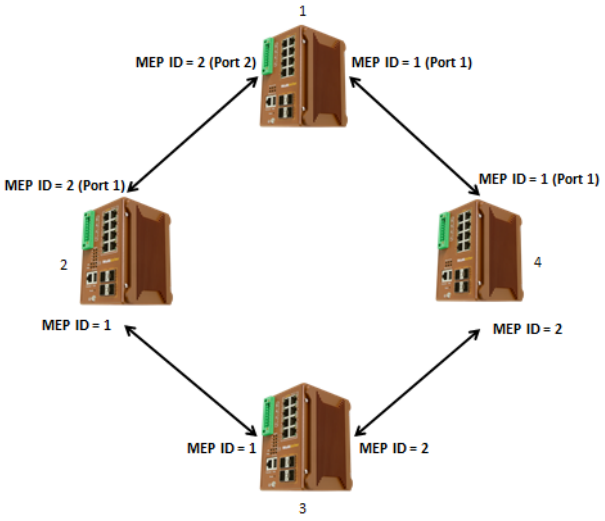
The switch allows user to configure the size of the Maximum Transmission Unit. The default value is 1,518bytes. The maximum Jumbo Frame size is 9,216 bytes.




## 3.2.7 CFM SETTING

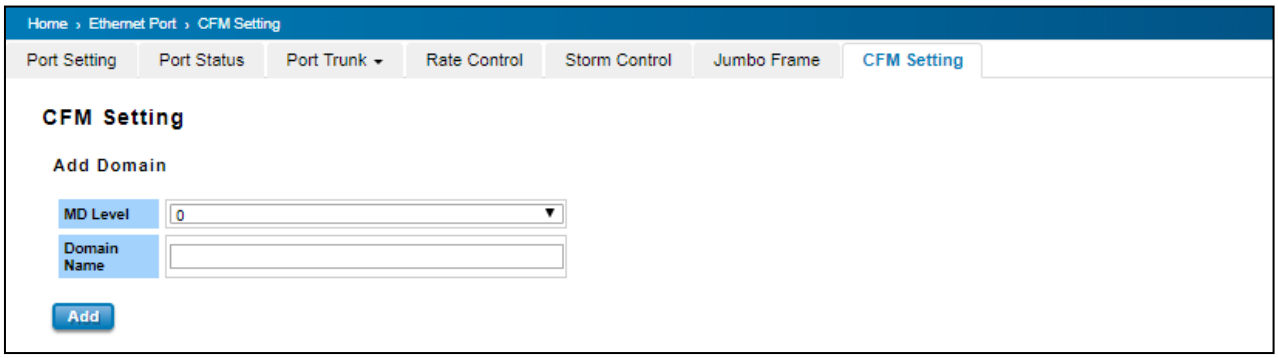
Ethernet Connectivity Fault Management (CFM, IEEE 802.1ag) is an end-to-end Ethernet OAM that can cross multiple domains to monitor the health of the entire service instance. A service instance can be a native Ethernet VLAN. CFM is a connectivity checking mechanism that uses its own Ethernet frames (its Ethertype is 0x8902 and it has its own MAC address) to validate the health of the service instance.

Continuity Check Protocol (CCP): "Heartbeating" messages for CFM. The Continuity Check Message (CCM) provides a means to detect connectivity failures in an MA. CCMs are multicast messages. CCMs are confined to a domain (MD). These messages are unidirectional and do not solicit a response. Each MEP transmits a periodic multicast Continuity Check Message inward towards the other MEPs. DP412/DS412 support Hardware CCM transition. The transition/receiving interval can up to 3.3ms to support detection Gigabit Ethernet cooper interface in 10ms.



The MEP ID in a link connection should be the same. For the example above the ERPS Ring, the port 1 from device one, the MEP ID is 1 and the port 1 from device 4, the MEP ID is also 1. In one device the MEP ID cannot be the same, it can be used only for a port. Below is the CFM CCP configuration page. In this page user may configure the Maintenance Domain, Maintenance Association and the Maintenance association End Point setting.

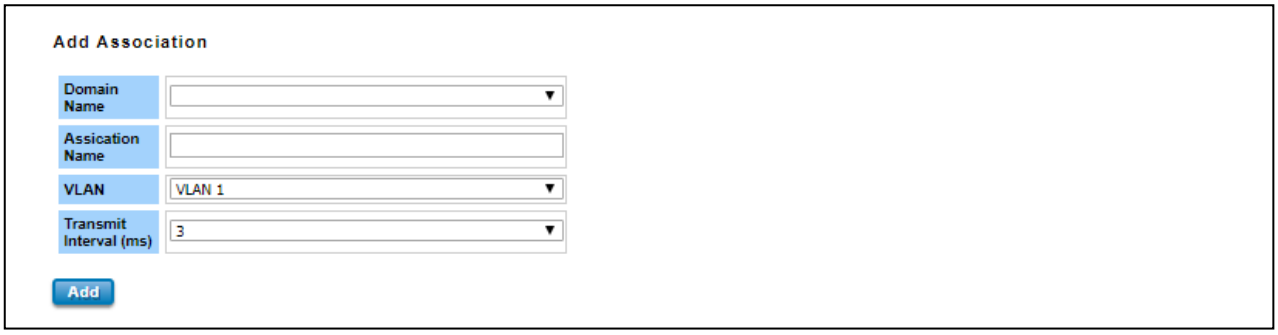
**Add Domain**




Add the Domain name and the MD level then click **Add.**

| TERMS | DESCRIPTION |
|---|---|
| **MD Level** | Select the MD Level from 0~7<br>The eight levels range from 0 to 7. A hierarchical relationship exists between domains based on levels. The larger the domain, the higher the level value.<br>Recommended values of levels are as follows:<br>Customer Domain: Largest (e.g., 7)<br>Provider Domain: In between (e.g., 3)<br>Operator Domain: Smallest (e.g., 1) |
| **Domain Name** | Enter a new Domain Name. Domain name, maximum of 43 characters |

**Add Association**



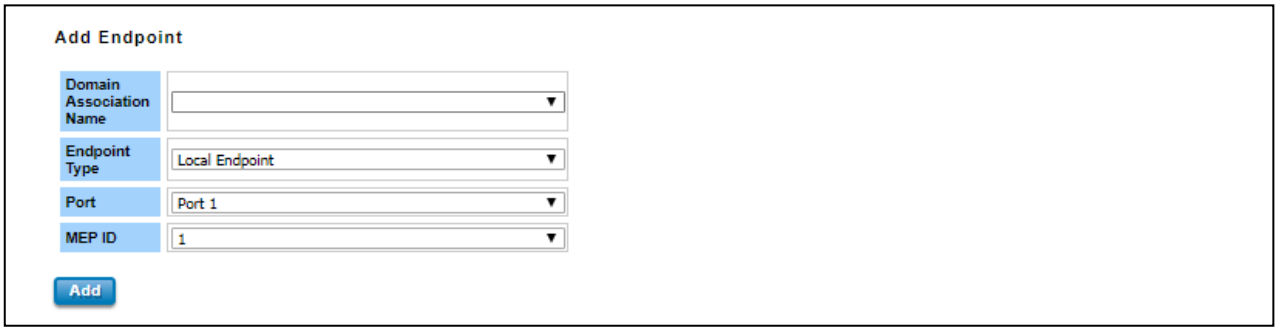

Choose the Domain Name from the list that has been added up then add a new Association Name for the Maintenance Association. After that choose the VLAN, Please create VLAN first, and each port set to be “tagged”

Add the Domain association name, end point type, port number and the MEP ID then click **Add.**

| TERMS | DESCRIPTION |
|---|---|
| **Domain Name** | Choose the Domain Name that has been added |
| **Association Name** | Enter the Association Name. Association name, maximum of 45 characters |
| **VLAN** | Choose VLAN that has been assigned |

| | |
|---|---|
| **Domain Name** | Enter a new Domain Name. Domain name, maximum of 43 characters |

**Add Endpoint**

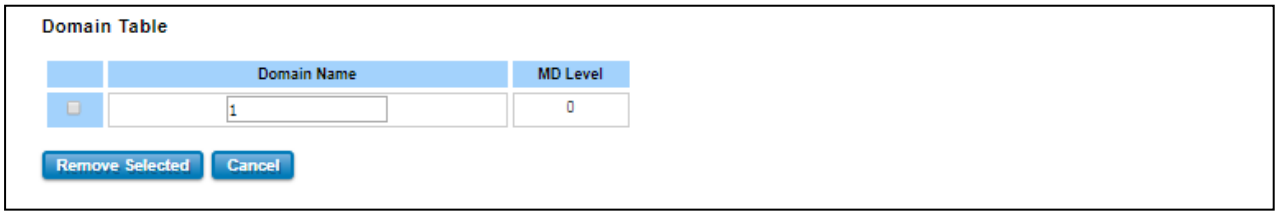



Points at the edge of the domain, define the boundary for the domain. A MEP sends and receives CFM frames through the relay function, drops all CFM frames of its level or lower that come from the wire side.

All of the configuration above will directly appear at the three tables below, Domain Table, Association Table and the Endpoint Table.

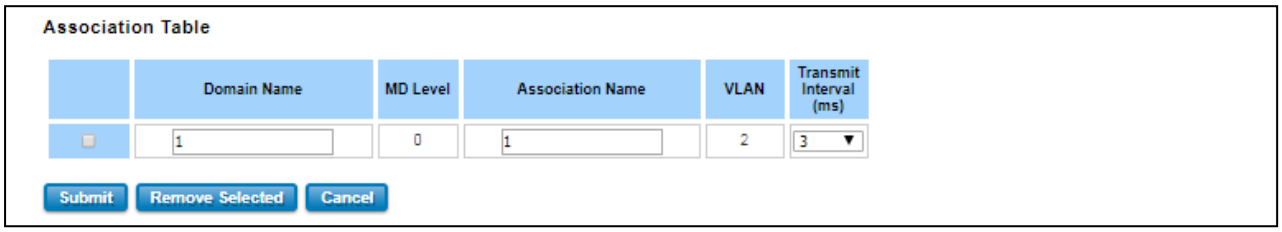
| TERMS | DESCRIPTION |
|---|---|
| **Domain Association Name** | Choose the Domain Association Name that has been added |
| **Endpoint Type** | **Default: Local Endpoint**<br>Choose between Local Endpoint and Remote Endpoint<br>Local Endpoint: Set the port as the Continuity Check Message (CCM) sender.<br>Remote Endpoint: Set the port as the Continuity Check Message (CCM) receiver. |
| **Port** | **Default: Port 1**<br>Choose port that need to be assigned |
| **MEP ID** | **Default: 1**<br>Choose the MEP ID. One MEP refer to one MEP ID |

**Domain Table**




This section shows the Domain entry. User may delete the list, by select the list and click **Remove Selected**

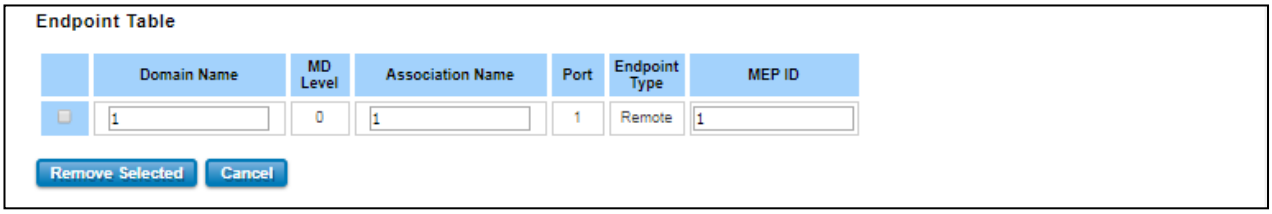
**Association Table**




This section shows the Association entry. In this table, user can configure the Configure Continuity Check Message transmit interval (default 3 ms), and after that click Submit to apply the setting. User may delete the list, by select the list and click **Remove Selected**

**Endpoint Table**

This section shows the Endpoint entry. User may delete the list, by select the list and click **Remove Selected**



## 3.3 POWER OVER ETHERNET (PoE MODELS ONLY)

Power over Ethernet has become increasingly popular due in large part to the reliability provided by PoE Ethernet switches that supply the necessary power to Powered Devices (PD) when AC power is not readily available or cost-prohibitive to provide locally. WoMaster' industrial DIN Rail PoE Switch compliant with IEEE 802.3af and IEEE 802.3at. All of WoMaster' switches adapt 8-Port PoE injectors in port 1 to port 8, each port with the ability to deliver 30W to compatible IEEE 802.3at standard and provides 240W power budget for hall system.

Power over Ethernet can be used with:

• Surveillance cameras

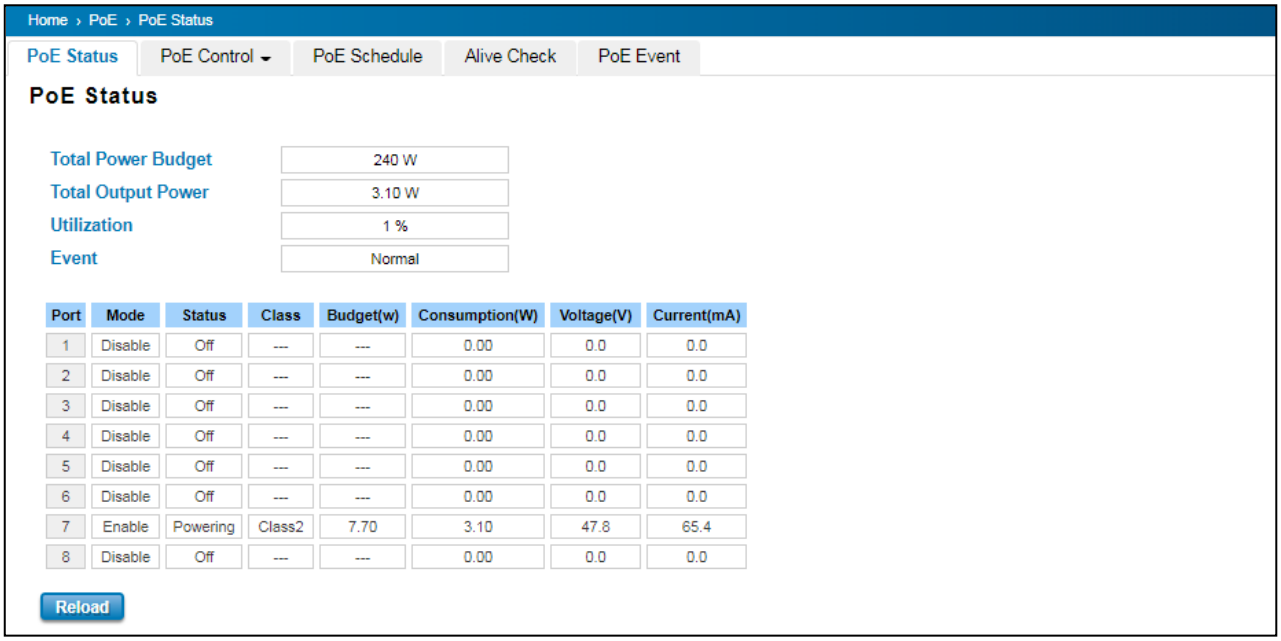
• Security I/O sensors

• Industrial wireless access points

• Emergency IP phones

### 3.3.1 PoE STATUS

The PoE Status page shows the system PoE status and the operating status of each PoE Port. The information includes PoE mode, Operation status, and PD class, Power Consumption, Voltage and Current. For example, in the figure below, Port 7 was enabled and is supplying power to a Class 2 Powered Device (PD) indicated under the Classification column. The PD device is rated at 47.8V and 65.4mA. The total power consumption for this PD is 3.10W with Budget 7.70W. To check the status of the PoE port, please click on the Reload button.



The description of the columns is as below:

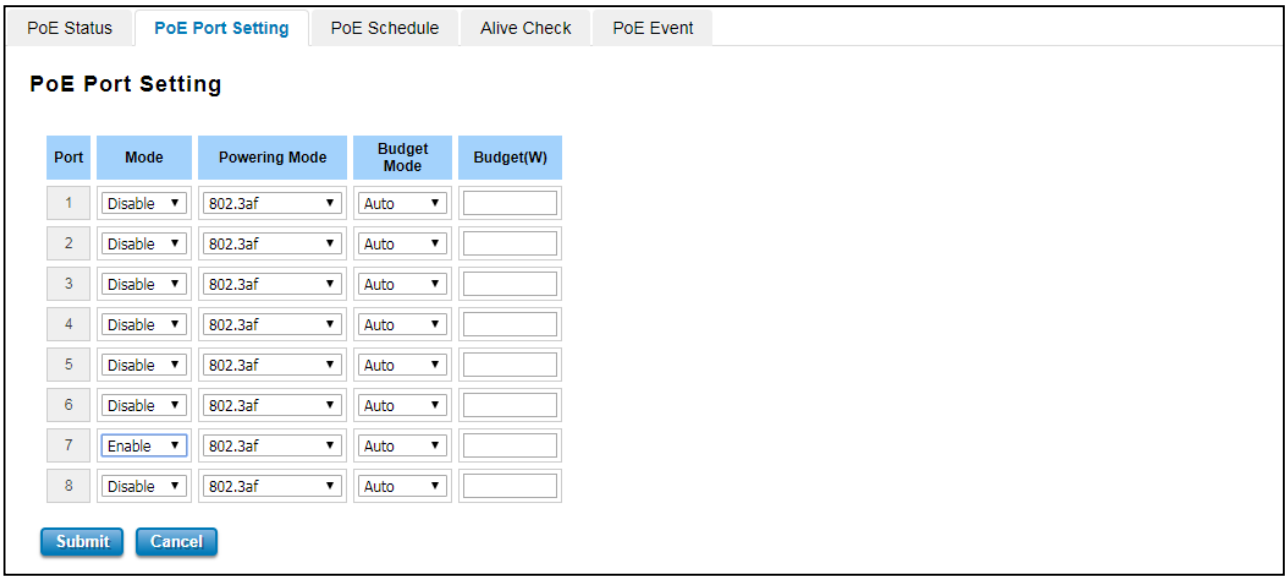
| TERMS | DESCRIPTION |
|---|---|
| **Mode** | Enable/Disable/Schedule Indicates the PoE port status |
| **Status** | **Default: Off**<br>PoE status is included Off, Powering, and Searching.<br>Off – PoE is inactive.<br>Powering – PoE is enabled and powering the PD.<br>Searching – Searching the PD which need the power. |
| **Class** | Indicates the PD included in which PoE class. |
| **Consumption (W)** | Indicates the actual Power consumed value for PoE port |
| **Voltage (V)** | Indicates the actual Voltage consumed value for PoE port |
| **Current (mA)** | Indicates the actual Current consumed value for PoE port |

## 3.3.2 PoE PORT SETTING

The PoE Port Setting allows user to enable the PoE for each port, powering mode, budget mode, and the budget (W).

The following section will introduce the function.

### System Setting




The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Mode** | Enable/Disable/Schedule port's PoE function. |
| **Powering Mode** | 802.3af, 802.3at (LLDP), 802.3at (2-event) and forced mode.<br>***Forced mode will ignore the classification behaviors and apply power onto the RJ-45, uses the forced mode must be carefully.** |
| **Budget Mode** | Choose budget mode as auto or manual. If auto the budget would be delivered automatically based on the end device requirement. If user choose manual, user can input the number at the budget text box. |
| **Budget (W)** | Input the budget. |

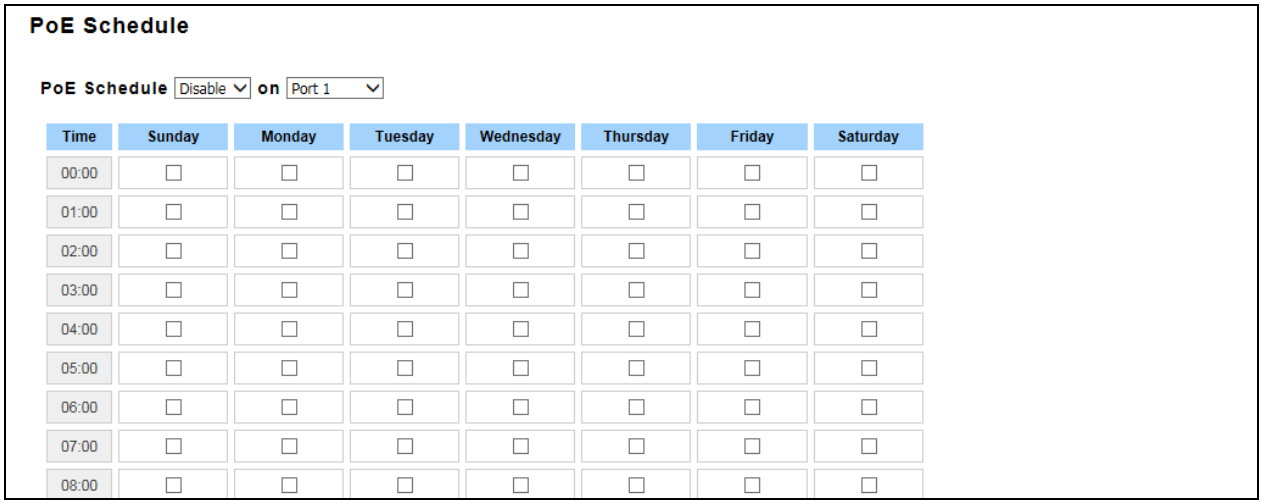
If the system PoE consumption is over the system budget control, the PoE system will turn off low priority port PoE function, until the consumption is becomes smaller than the system budget. After finished configuring the settings, click on **Submit** to save the configuration.

To enable the IEEE 802.3at High Power PoE function, the power input voltage should be DC 50 ~57V to obtain better performance. Applies DC 48V to PoE Switch and perform 30W high power output may cause the PoE disable automatically. To avoid this issue, we suggest adjust the power supply output to 50V DC or higher. In usually, the Switching power supply adopted adjust resistor for voltage fine tune.

> **WARNING:** During the PoE operating, the surface will accumulate heat and caused surface temperature becomes higher than ambient temperature. Do remember don't touch device surface during PoE operating.

### 3.3.3 PoE SCHEDULING

For energy saving or power recycle powered devices, the PoE managed switch's **PoE scheduling** interface allows users to appoint any date and time to enable or disable PoE functions for each PoE port. User need to configure **PoE Scheduling** and select a target port manually to enable this function. The figure below is PoE Schedule interface.




The PoE schedule supports hourly and weekly base PoE schedule configuration. **Enable** and select the target port and marking the time frame, then click **Submit** to activate the PoE scheduling function on selected port.

## 3.3.4 ALIVE CHECK

### PD Alive Check


WoMaster' Switches support a useful function that help user to maintain the PD's status and help use to saving the maintenance time and money. Once user defined this function, the PoE Switch will request PD system and turn-off PoE power if PD system does not echo the request. After the duration time (cycle time), the PoE switch will start request PD again.

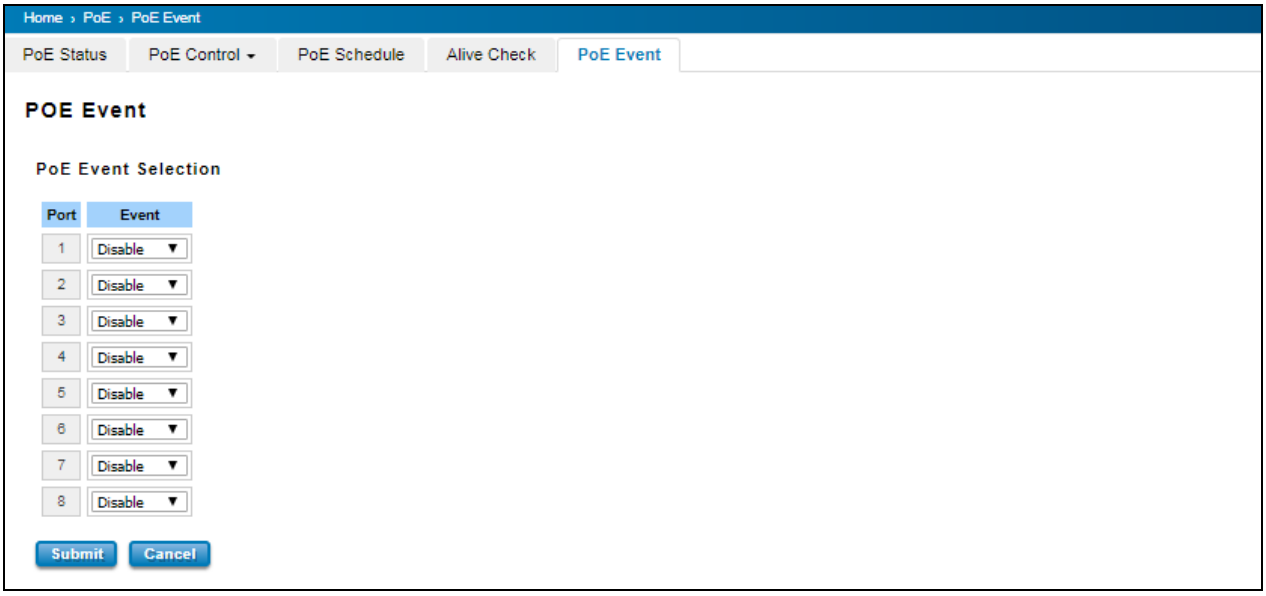
The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **IP address** | PD's IP-address that installed on the port. |
| **Cycle time** | User measured the PD system boots duration time.<br>*Most of PD system – IP camera will take at least 40~50 seconds.<br>Here, we suggest that user sets the cycle time to 90 seconds. |
| **Delete** | Delete PD's IP-address that has been selected. |

After finished configuring the settings, click on **Submit** to save the configuration.

### 3.3.5 PoE EVENT

In this section, user is allowed to configure the PoE Event, the value is Enable and Disable. When the status is enabled PoE itself will detect the PD, then it will deliver the power when the PD is detected.

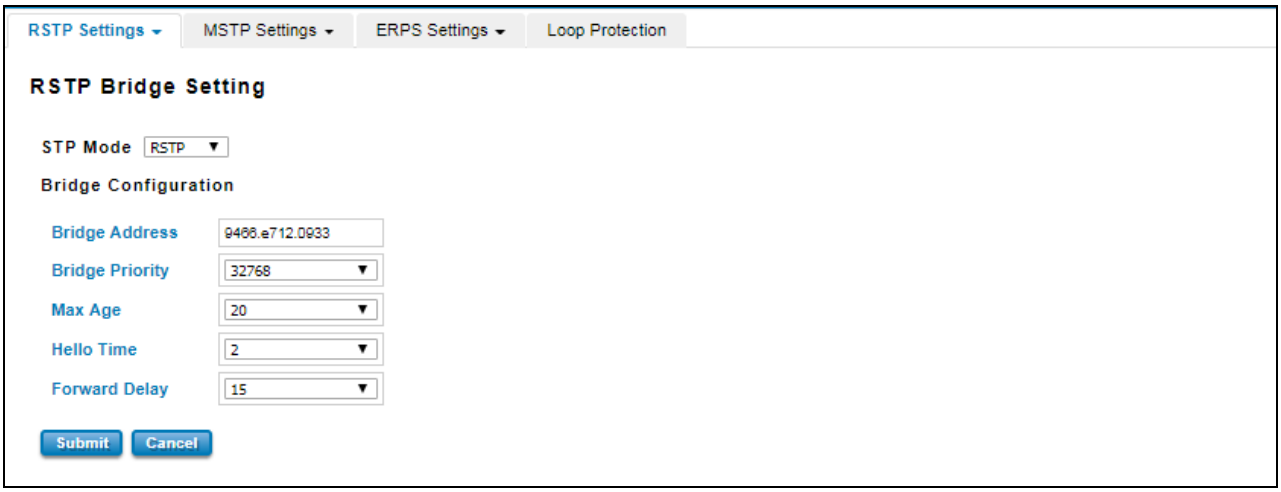


## 3.4 REDUNDANCY

Redundancy role on the network is to help protect critical links against failure, protects against network loops, and keeps network downtime at a minimum. Sustainable, uninterrupted data communication network is critical for industrial applications. Network Redundancy allows user to set up redundant loops in the network to provide a backup data transmission route in the event that a cable is inadvertently disconnected or damaged. This switch supports Rapid Spanning Tree Protocol (RSTP)/Multiple Spanning Tree Protocol (MSTP) and ITU-T G.8032 v1/v2 Ethernet Ring Protection Switching (ERPS). ERPS (Ethernet Ring Protection Switching) or ITU-T G.8032 is a loop resolution protocol, just like STP. Convergence time is much quicker in ERPS. Unlike in STP, most of the ERPS parameters are management configured – which link to block in the start etc. Normally ERPS is implemented with-in the same administrator domain, there by having control on the nodes participating in the Ring. This technology provides sub-50ms protection and recovery switching for Ethernet traffic. This is a particularly important feature for industrial applications, since it could take several minutes to locate the disconnected or severed cable.

### 3.4.1 RSTP SETTINGS

This page allows select the RSTP mode and configuring the global RSTP Bridge Configuration.




The STP mode includes the **STP**, **RSTP**, **MSTP** and **Disable**. User can select the STP mode for user system first. The default mode is RSTP enabled. After user selects the STP or RSTP mode; user should continue to configure the global Bridge parameters for STP and RSTP. If user selects the MSTP mode, user need go to MSTP Configuration page.

#### *Spanning Tree Protocol (STP)*

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

#### *Rapid Spanning Tree Protocol (RSTP)*

If the destination from a switch is more than one path, it will lead to looping condition that can generate broadcast storms in a network. The spanning tree was created to combat the negative effects of message loops in switched

networks. A spanning tree algorithm is used to automatically sense whether a switch has more than one way to communicate with a node. It will then select the best path, and block the other path. Spanning Tree Protocol (STP) introduced a standard method to accomplish this. Rapid Spanning Tree Protocol (RSTP) was adopted and represents the evolution of STP, providing much faster spanning tree convergence after a topology change.

### *MSTP (Multiple Spanning Tree Protocol)*

MSTP is a direct extension of RSTP that can provide an independent spanning tree for different VLANs. It simplifies network management by limiting the size of each region, and prevents VLAN members from being segmented from the group. MSTP can provide multiple forwarding paths and enable load balancing. By understand the architecture, allow you effectively maintain and operate the correct spanning tree. One VLAN can be mapped to an instance. The maximum Instance of the switch is 16, with the range is from 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. An MST Region may contain multiple MSTP Instances.

MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree that is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

To configure the MSTP setting, the STP Mode of the RSTP Settings page should be changed to MSTP mode first. After enabled MSTP mode, user can go to the MSTP Settings page.

**Bridge Configuration**

**Bridge Address:** This shows the switch's MAC address.

**Priority (0-61440)**: RSTP uses bridge ID to determine the root bridge, the bridge with the highest bridge ID becomes the root bridge. The bridge ID is composed of bridge priority and bridge MAC address. So that the bridge with the highest priority becomes the highest bridge ID. If all the bridge ID has the same priority, the bridge with the lowest MAC address will then become the root bridge.

> **NOTE:**
>
> 1. The bridge priority value must be in multiples of 4096. A device with a lower number has a higher bridge priority.
> 2. The Web GUI allows user selects the priority number directly. This is the convenient of the GUI design. When user configures the value through the CLI or SNMP, user may need to type the value directly. Please follow the n x 4096 rules for the Bridge Priority.

**Max Age (6-40)**: Enter a value from 6 to 40 seconds here. This value represents the time that a bridge will wait without receiving Spanning Tree Protocol configuration messages before attempting to reconfigure.

**Hello Time (1-10)**: Enter a value from 1 to 10 seconds here. This is a periodic timer that drives the switch to send out BPDU (Bridge Protocol Data Unit) packet to check current STP status. The root bridge of the spanning tree topology periodically sends out a **hello** message to other devices on the network to check if the topology is normal. The **hello time** is the amount of time the root has waited during sending hello messages.

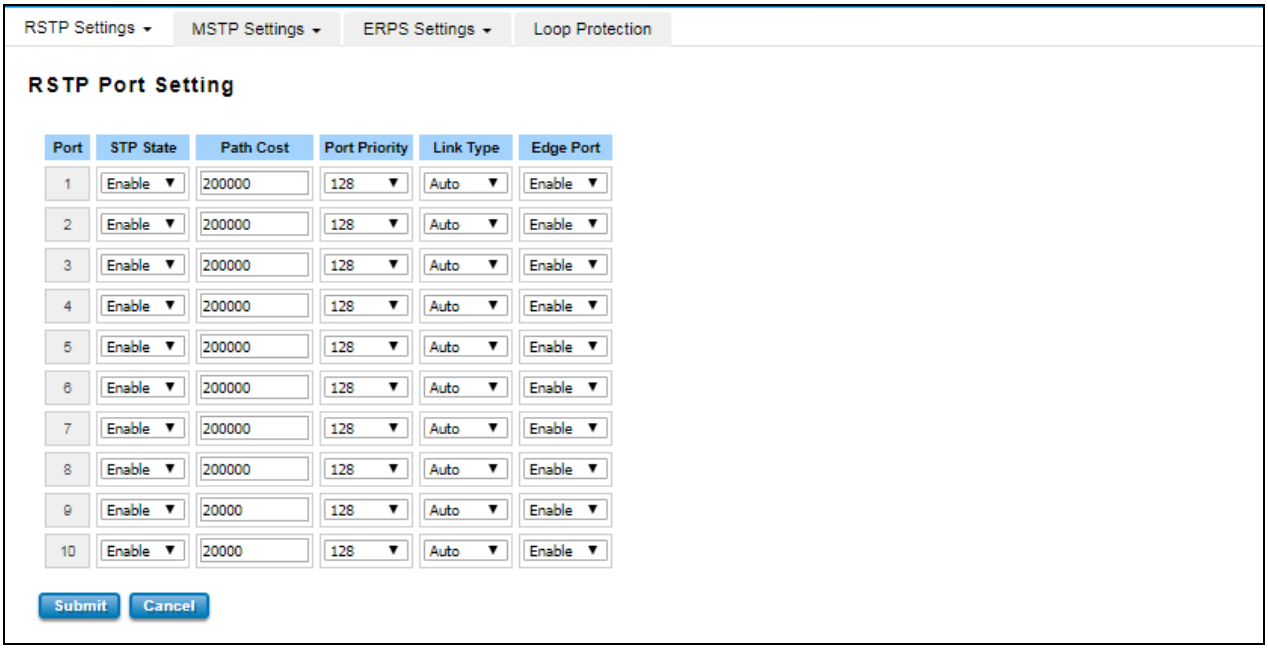
**Forward Delay Time (4-30)**: Enter a value between 4 and 30 seconds. This value is the time that a port waits before changing from Spanning Tree Protocol learning and listening states to forwarding state.

Once user has completed user configuration, click on **Submit** to apply user settings.

> **NOTE:** User must follow the rule to configure Hello Time, Forwarding Delay, and Max Age parameters.
>
> **2× (Forward Delay Time – 1 sec) ≥ Max Age Time ≥ 2 × (Hello Time value + 1 sec)**

## RSTP Port Settings

Select the port user wants to configure and user will be able to view current setting and status of the port.




The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **STP State** | **Default: Enable**<br>To enable or disable STP function. |
| **Path Cost** | Enter a number between 1 and 200,000,000. This value represents the "**cost**" of the path to the other bridge from the transmitting bridge at the specified port. |
| **Priority** | Enter a value between 0 and 240, using multiples of 16. This is the value that decides which port should be blocked by priority in a LAN. |
| **Link Type** | There are 3 types for user selects **Auto, P2P** and **Share.** Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This function allows link status of the link to be manipulated administratively. **Auto** - means to auto select P2P or Share mode.<br>**P2P -** means P2P is enabled; the 2 ends work in full duplex mode.<br>**Share -** means P2P is disabled; the 2 ends may connect through a share media and work in half duplex mode. |

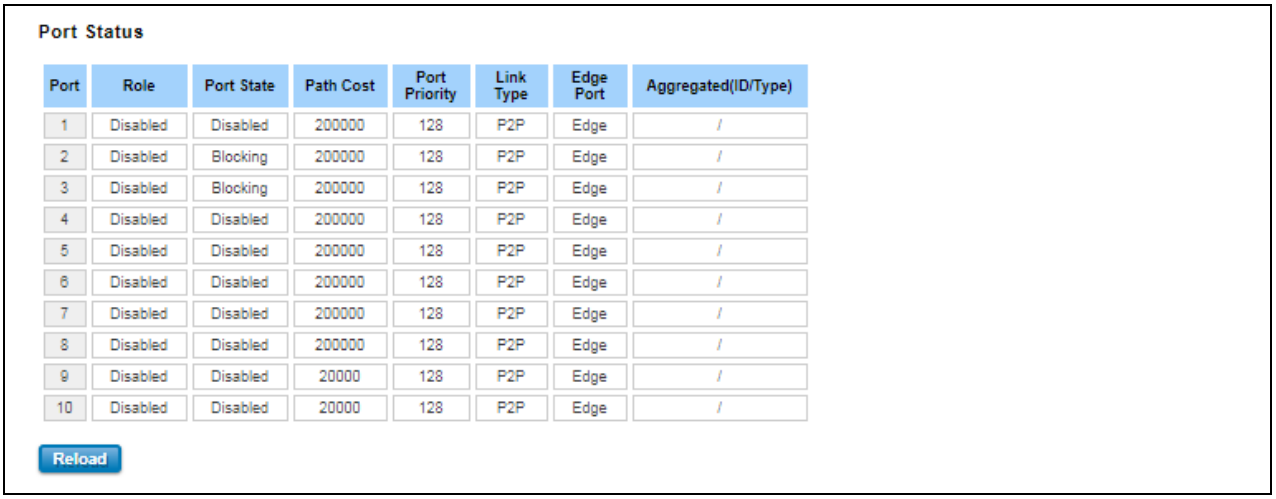
| | |
|---|---|
| **Edge Port** | A port directly connected to the end stations cannot create a bridging loop in the network. To configure this port as an edge port, set the port to the **Enable** state. When the non-bridge device connects an admin edge port, this port will be in blocking state and turn to forwarding state in 4 seconds. |

Once user finished user configuration, click on **Submit** to save user settings.

## RSTP Status

This page allows user to see the information of the root switch and port status.

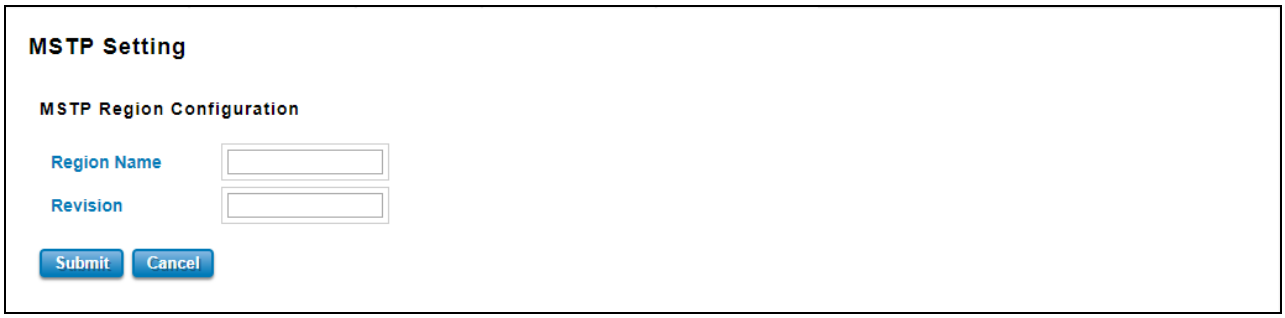

**Root Status:** User can see root Bridge ID, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root switch.




**Port Status:** User can see port Role, Port State, Path Cost, Port Priority, Oper P2P mode, Oper edge port mode and Aggregated (ID/Type).

## 3.4.2 MSTP SETTINGS

**MSTP Region Configuration**




This page allows configure the Region Name and its Revision, mapping the VLAN to Instance and check current MST Instance configuration. The network can be divided virtually to different Regions. The switches within the Region should have the same Region and Revision level.

| TERMS | DESCRIPTION |
|---|---|
| **Region Name** | The name for the Region. Maximum length: 32 characters. |
| **Revision** | **Default: 0**<br>The revision for the Region. Range: 0-65535 |

Once user finished user configuration, click on **Submit** to apply user settings.

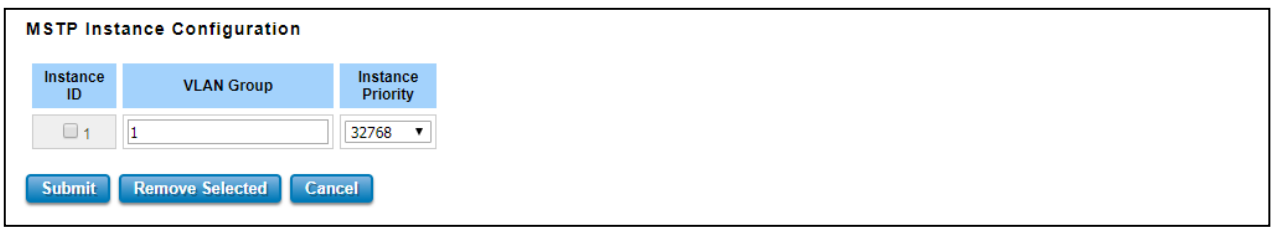
**Add MSTP Instance**


This page allows mapping the VLAN to Instance and assign priority to the instance. Before mapping VLAN to Instance, user should create VLAN and assign the member ports first. Please refer to the VLAN setting page. **After** finish the configuration, click on **Add** to apply user settings.

| TERMS | DESCRIPTION |
|---|---|
| **Instance ID** | Select the Instance ID, the available number is 1-15. |
| **VLAN Group** | Type the VLAN ID that user wants mapping to the instance. |
| **Instance Priority** | Assign the priority to the instance. (0-61440) |

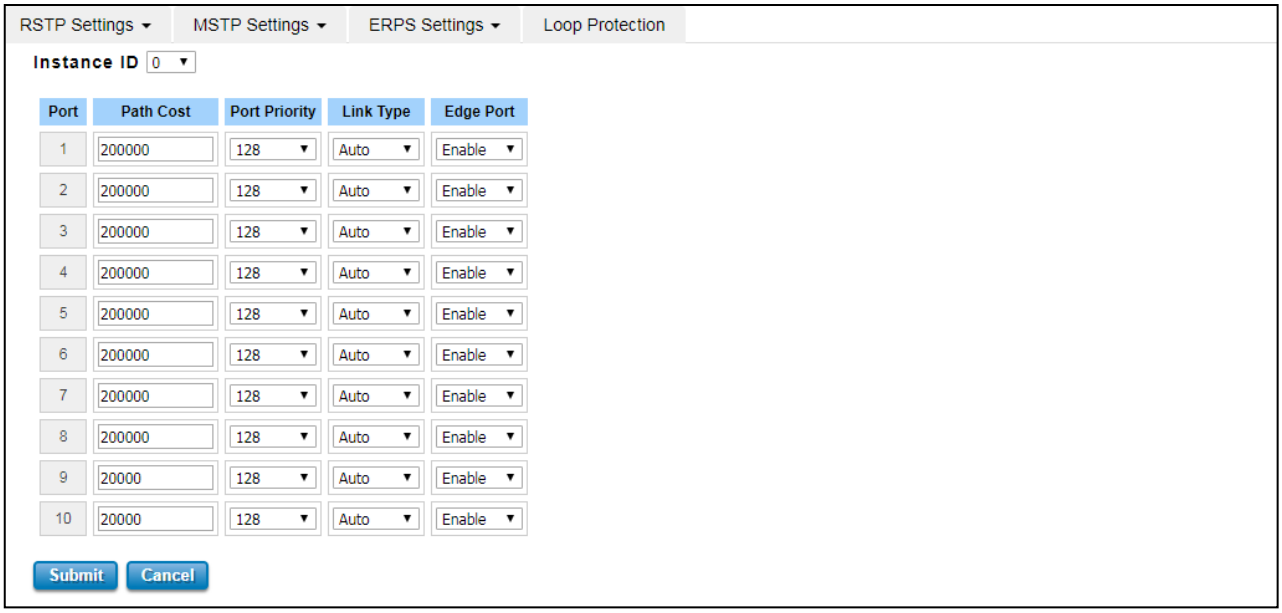
**MST Instance Configuration**

This page allows user to see the current MST Instance Configuration user added. Click on **Submit** to apply the setting. User can **Remove** the instance in this page.



## MSTP Port Setting

This page allows configure the Port settings. Choose the Instance ID user wants to configure. The MSTP enabled and linked up ports within the instance will be listed in this table. Note that the ports not belonged to the Instance, or the ports not MSTP activated will not display. The meaning of the Path Cost, Priority, Link Type and Edge Port is the same as the definition of RSTP.




The description of the columns is as below:

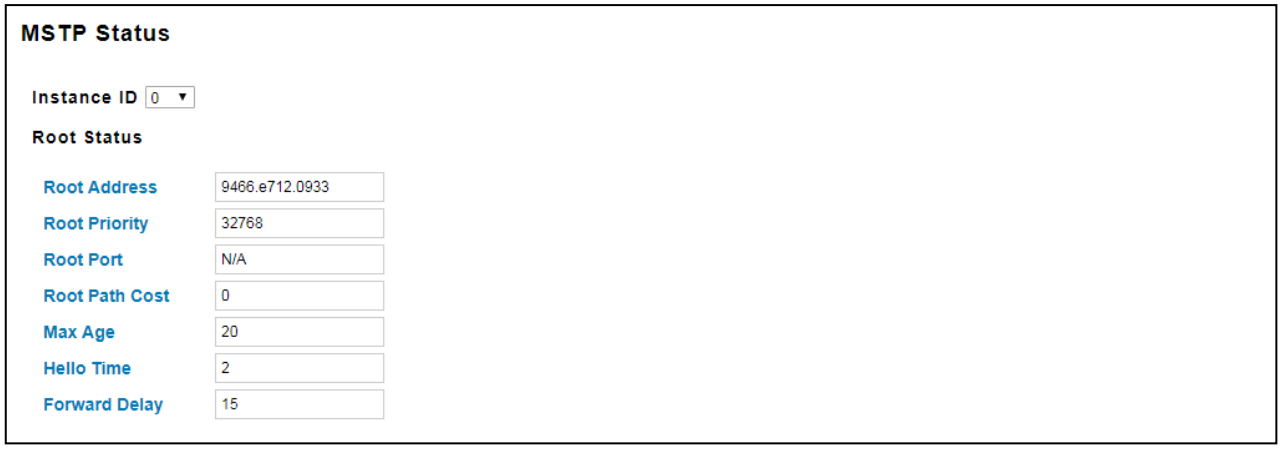
| TERMS | DESCRIPTION |
|---|---|
| **Path Cost** | Enter a number between 1 and 200,000,000. This value represents the cost of the path to the other bridge from the transmitting bridge at the specified port. Path cost value is derived from the media speed of an interface. If a loop occurs, the MSTP uses cost when selecting an interface to put in the forwarding state. Lower cost values can be assigned to interfaces that selected first and higher cost values that selected last. If all interfaces have the same cost value, the MSTP puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces. |
| **Port Priority** | Enter a value between 0 and 240. This is the value that decides which port should be blocked by priority in a LAN. |
| **Link Type** | There are 3 types for user selects **Auto, P2P** and **Share.** Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This function allows link status of the link to be manipulated administratively.<br>**Auto** - means to auto select P2P or Share mode.<br>**P2P -** means P2P is enabled; the 2 ends work in full duplex mode.<br>**Share -** means P2P is disabled; the 2 ends may connect through a share media and work in half duplex mode. |

| | |
|---|---|
| **Edge Port** | A port directly connected to the end stations cannot create a bridging loop in the network. To configure this port as an edge port, set the port to the **Enable** state. When the non-bridge device connects an admin edge port, this port will be in blocking state and turn to forwarding state in 4 seconds. |

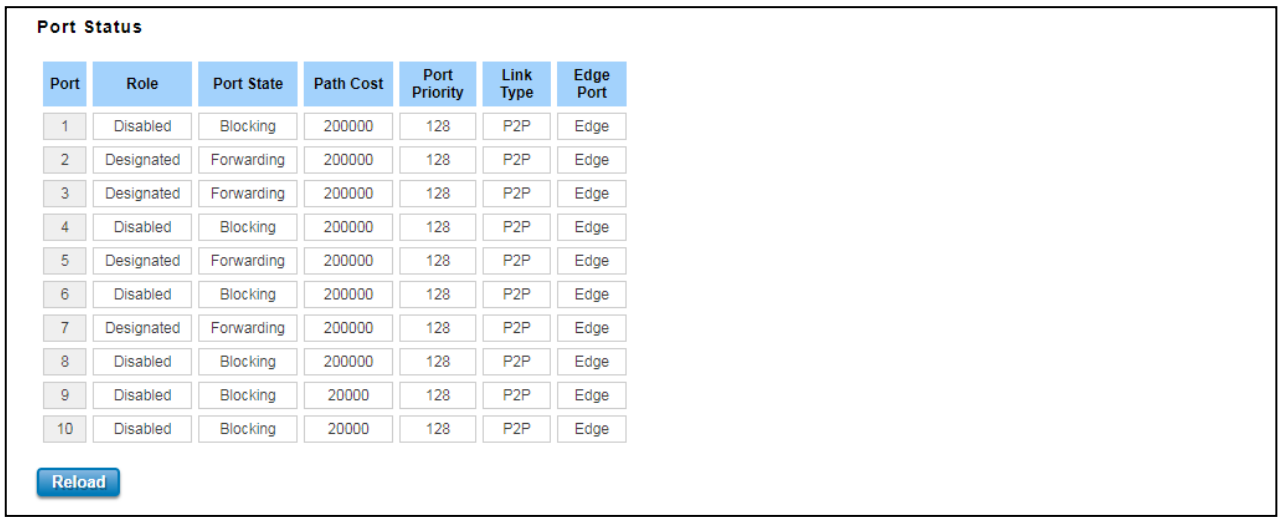
Once user finished user configuration, click on **Submit** to save user settings.

## MSTP Status

This page allows user to see the current MSTP status. Choose the **Instance ID** first. If the instance is not added, the information remains blank. The **Root Information** shows the setting of the Root switch.



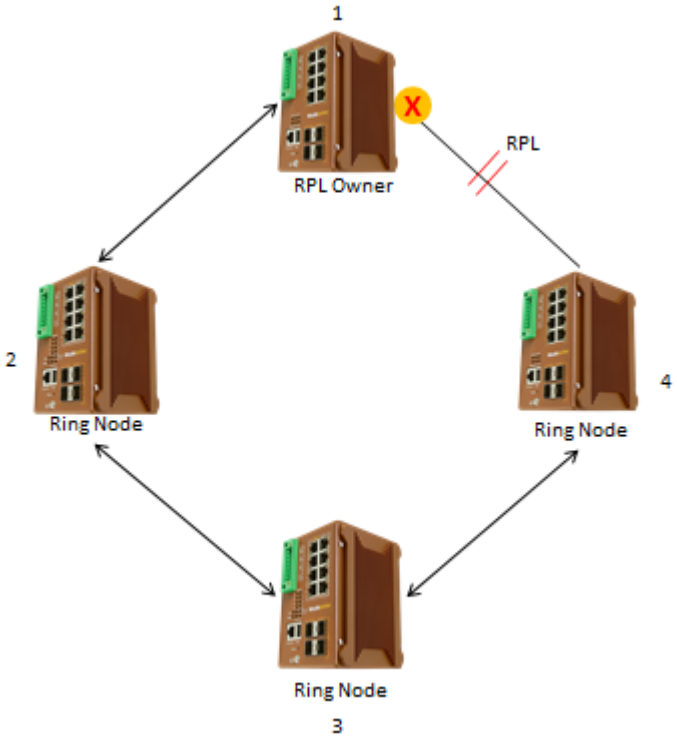

**Root Status:** User can see Root Address, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root switch based on the Instance ID.




**Port Status:** User can see port Role, Port State, Path Cost, Port Priority, Link Type and the Edge Port within the instance. Click **Reload** to refresh the information display.

### 3.4.3 ERPS SETTINGS

Ethernet Ring Protection Switching (ERPS) is a protocol for Ethernet layer network rings. The protocol specifies the protection mechanism for sub-50ms delay time. The ring topology provides multipoint connectivity economically by reducing the number of links. ERPS provides highly reliable and stable protection in the ring topology, and it never forms loops, which can affect network operation and service availability.

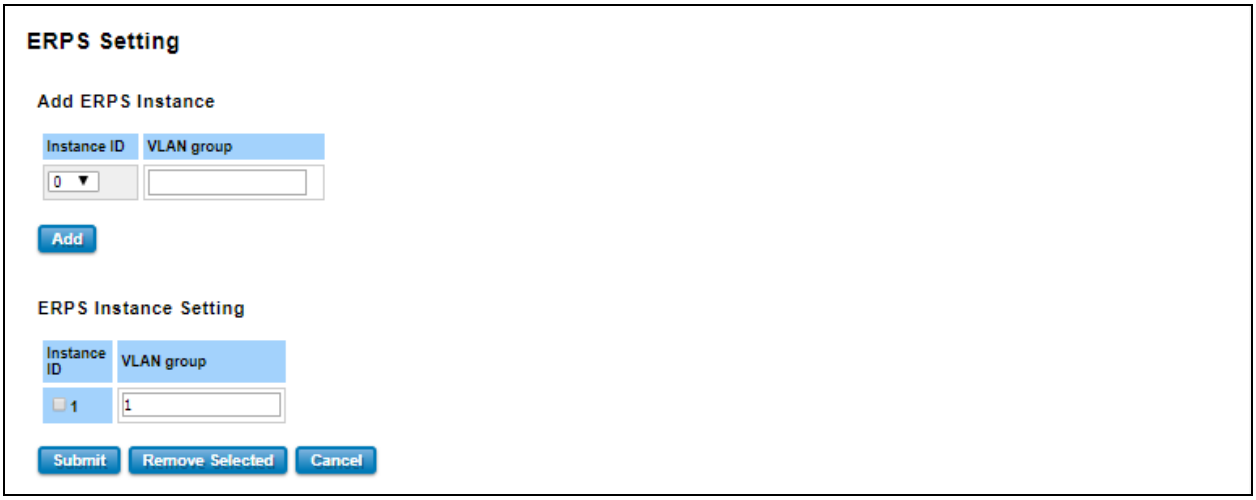



The figure above shows that each Ethernet Ring Node is connected to other Ethernet Ring Nodes that participating in the same Ethernet Ring using two independent links. In the Ethernet ring, loops can be avoided by guaranteeing that traffic may flow on all but one of the ring links at any time. This particular link is called Ring Protection Link (RPL). A control message called Ring Automatic Protection Switch (R-APS) coordinates the activities of switching on/off the RPL. Under normal conditions, this link is blocked by the Owner Node. Thus, loops can be avoided by this mechanism. In case an Ethernet ring failure occurs, one designated Ethernet Ring Node called the RPL Owner Node will be responsible for unblocking its end of the RPL to allow RPL to be used as a backup link. The RPL is the backup link when one link failure occurs.

WoMaster managed switches provide a number of Ethernet ring protocol. The ERPS/Ring section is subdivided into two menus, which are: ERPS Setting and ERPS Status.

### 3.4.3.1 ERPS SETTINGS

## ERPS Setting

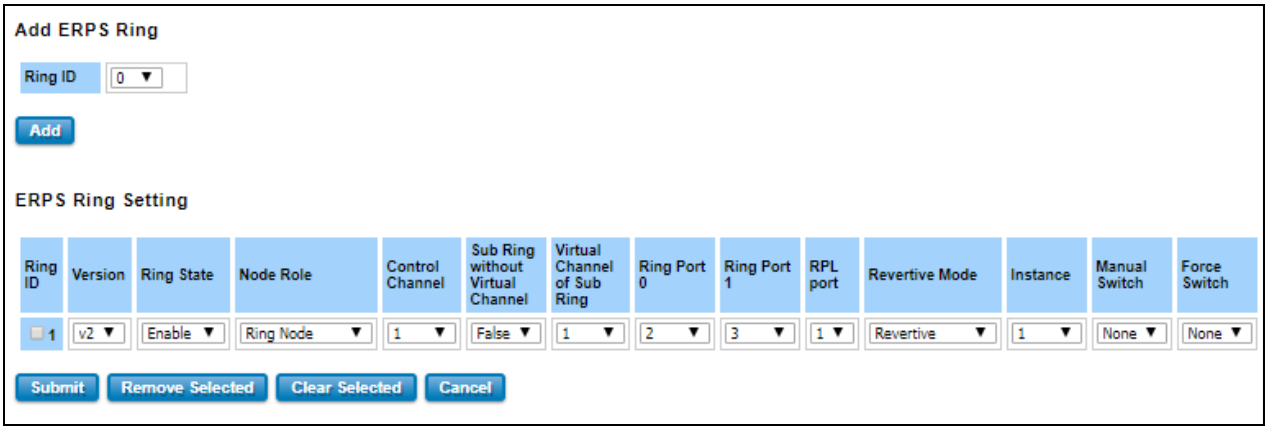



**Add ERPS Instance** is a section for mapping the VLAN to Instance. Before mapping VLAN to Instance, user should create VLAN and assign the member ports first. Please refer to the VLAN setting page.

After click the **Add** button, the Instance ID and the VLAN group information will directly display in the **ERPS Instance Setting** section.

| TERMS | DESCRIPTION |
|---|---|
| **Instance ID** | Select the Instance ID, the available number is 1-15. |
| **VLAN Group** | Type the VLAN ID that user wants mapping to the instance. |

## Add ERPS Ring



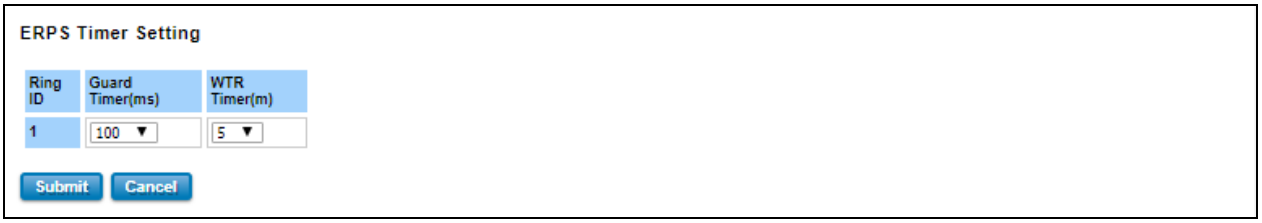

**Add ERPS Ring** is a section to add the Ring ID of the created Protection group; it must be an integer value between 0 and 31. The maximum numbers of ERPS Protection Groups that can be created are 32. Click the ID of a Protection group to enter the configuration page. After click Add button, one line will be directly created in the **ERPS Ring Setting** section. The ERPS Ring Setting section is a table that used to set up the ERPS Ring configuration.

Below is the description table.

| TERMS | DESCRIPTION |
|---|---|
| **Ring ID** | Display the Ring ID |
| **Version** | ERPS Protocol Version - v1 or v2. |
| **Ring State** | **Default: Disable**<br>Enable - Ring Status is enable<br>Disable - Ring Status is disable |
| **Node Role** | It can be either RPL owner or RPL Neighbor or Ring Node. |
| **Control Channel** | **Default: 1**<br>Control channel is implemented using a VLAN. Each ERP instance uses a tag-based VLAN for sending and receiving R-APS messages. (1-4094) |
| **Sub Ring without Virtual Channel** | **Default: False**<br>**True** – if doesn't have a virtual channel<br>**False** – if have any virtual channel |
| **Virtual Channel of Sub Ring** | **Default: 1**<br>Sub-rings can have a virtual channel on the interconnected node. Choose the number based on the VLANs Range (1-4094) |
| **Ring Port 0** | This will create a Port 0 of the switch in the Ring. Choose the port number that belongs to Ring port 0 |
| **Ring Port 1** | This will create Port 1 of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance. Choose the port number that belongs to Ring port 1. |
| **Ring Port 0 RMEP ID** | **Default: None**<br>The remote MEP id that CFM monitored of ERPS ring port detection. (Range 1 -8191). Please check the CFM Setting (MEP ID) |
| **Ring Port 1 RMEP ID** | **Default: None**<br>The remote MEP id that CFM monitored of ERPS ring port detection. (Range 1 -8191). Please Check the CFM Setting (MEP ID). |
| **RPL Port** | This allows you to select the Ring Port 0 or Ring Port 1 as the RPL block. |
| **Revertive Mode** | **Default: Revertive**<br>**Revertive mode**, after the conditions causing a protection switch has cleared; the traffic channel is restored to the working transport entity that is blocked on the RPL. In **Non-Revertive mode**, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared. |
| **Instance** | Select the Instance ID, the available number is 1-15. |
| **Manual Switch** | **Default: None**<br>In the absence of a failure or FS, Manual Switch command forces a block on the |

| | |
|---|---|
| | ring port where the command is issued.<br>Choose 0 or 1, refers to Ring Port 0 or Ring Port 1. |
| **Force Switch** | **Default: None**<br>Forced Switch command forces a block on the ring port where the command is issued. Choose 0 or 1, refers to Ring Port 0 or Ring Port 1. |

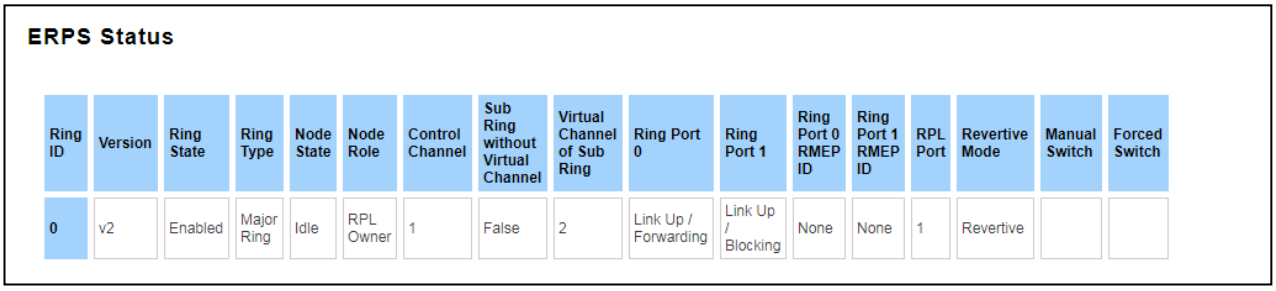
## ERPS Timer Setting




| TERMS | DESCRIPTION |
|---|---|
| **Guard Timer (ms)** | Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2000 ms, with a default value of 100 ms. |
| **WTR Timer (m)** | The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 1 and 12 minutes with a default value of 5 minutes. |

### 3.4.3.2 ERPS STATUS

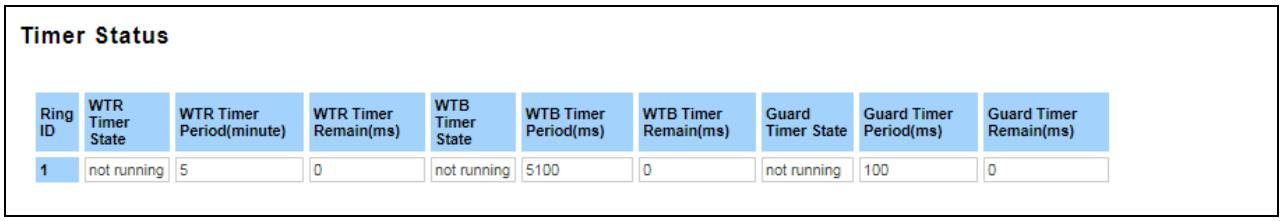
In this section, user can check the ERPS Status, Timer Status and Statistics from the Ring.



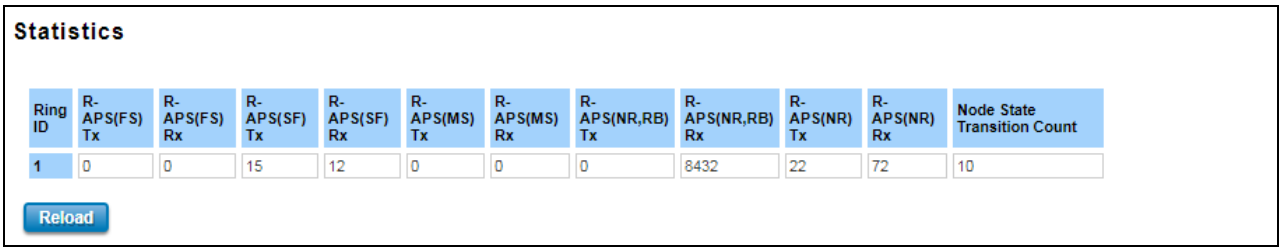

| TERMS | DESCRIPTION |
|---|---|
| **Ring ID** | Display the Ring ID |
| **Version** | ERPS Protocol Version - v1 or v2. |
| **Ring State** | **Default: Disable**<br>Enabled - Ring Status is enable<br>Disabled - Ring Status is disable |
| **Node State** | Status from the **Ring is Idle, Protection, Manual Switch, Force Switch** or **Pending.** |
| **Node Role** | It can be either **RPL owner** or **RPL Neighbor** or **Ring Node.** |
| **Control Channel** | Control Channel is referred to the VLANs number (1-4094) |

| | |
|---|---|
| **Sub Ring without Virtual Channel** | **Default: False**<br>**True** – if have a virtual channel<br>**False** – if doesn't have any virtual channel |
| **Virtual Channel of Sub Ring** | **Default: 1**<br>Sub-rings can have a virtual channel on the interconnected node. Choose the number based on the VLANs Range (1-4094) |
| **Ring Port 0** | The status from the port Link up/link down and Forwarding/Blocking |
| **Ring Port 1** | The status from the port Link up/link down and Forwarding/Blocking |
| **Ring Port 0 RMEP ID** | Show the remote MEP id that CFM monitored of ERPS ring port detection. |
| **Ring Port 1 RMEP ID** | Show the remote MEP id that CFM monitored of ERPS ring port detection. |
| **RPL Port** | The port status as the RPL block. |
| **Revertive Mode** | **Default: Revertive**<br>**Revertive mode**, after the conditions causing a protection switch has cleared; the traffic channel is restored to the working transport entity that is, blocked on the RPL. In **Non-Revertive mode**, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared. |
| **Manual Switch** | Status from the Ring Port 0 and 1 or None |
| **Force Switch** | Status from the Ring Port 0 and 1 or None |

**Timer Status**




| TERMS | DESCRIPTION |
|---|---|
| **Ring ID** | Display the Ring ID |
| **WTR Timer State** | Running or not Running status |
| **WTR Timer Period (minute)** | WTR timeout in milliseconds. |
| **WTR Timer Remain (ms)** | Remaining WTR timeout in milliseconds. |
| **WTB Timer State** | Running or not Running status |
| **WTB Timer Period (ms)** | WTB timeout in milliseconds. |
| **WTB Timer Remain (ms)** | Remaining WTB timeout in milliseconds. |
| **Guard Timer State** | Running or not Running status |
| **Guard Timer Period (ms)** | Guard Timer timeout in milliseconds. |
| **Guard Timer Remain (ms)** | Remaining Guard Timer timeout in milliseconds. |




| TERMS | DESCRIPTION |
|---|---|
| **Ring ID** | Display the Ring ID. |
| **R-APS(FS) Tx** | The number of R-APS messages with Forced Switch (FS) being sent. |
| **R-APS(FS) Rx** | The number of R-APS messages with Forced Switch (FS) being received. |
| **R-APS(SF) Tx** | The number of R-APS messages with Signal Fail (SF) being sent. |
| **R-APS(SF) Rx** | The number of R-APS messages with Signal Fail (SF) being received. |
| **R-APS(MS) Tx** | The number of R-APS messages with Manual Switch (MS) being sent. |
| **R-APS(MS) Rx** | The number of R-APS messages with Manual Switch (MS) being received. |
| **R-APS(NR, RB) Tx** | The number of R-APS messages with a No Request, RPL Blocked (NR,RB) being sent. |
| **R-APS(NR, RB) Rx** | The number of R-APS messages with a No Request, RPL Blocked (NR,RB) being received. |
| **R-APS(NR) Tx** | The number of R-APS messages with a No Request (NR) being sent. |
| **R-APS(NR) Rx** | The number of R-APS messages with a No Request (NR) being received. |
| **Node State Transition Count** | The number of state transition that detected in the Ring. |

## 3.5 VLAN

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, User can segment User network without being restricted by physical connections—a limitation of traditional network design. With VLANs User can segment User network into:

• **Departmental groups**—User could have one VLAN for the marketing department, another for the finance department, and another for the product development department.

• **Hierarchical groups**—User could have one VLAN for directors, another for managers, and another for general staff.

• **Usage groups**—User could have one VLAN for email users and another for multimedia users.

**Benefits of VLANs**

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides User with three other benefits:

• **VLANs ease the relocation of devices on networks:** With a VLAN setup, if a host originally on the Marketing VLAN, is moved to a port on another part of the network, and retains its original subnet membership, User only needs to specify that the new port is on the Marketing VLAN. User does not need to do any re-cabling.

• **VLANs provide extra security:** Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on the Marketing VLAN needs to communicate with devices on the Finance VLAN, the traffic must pass through a routing device or Layer 3 switch.

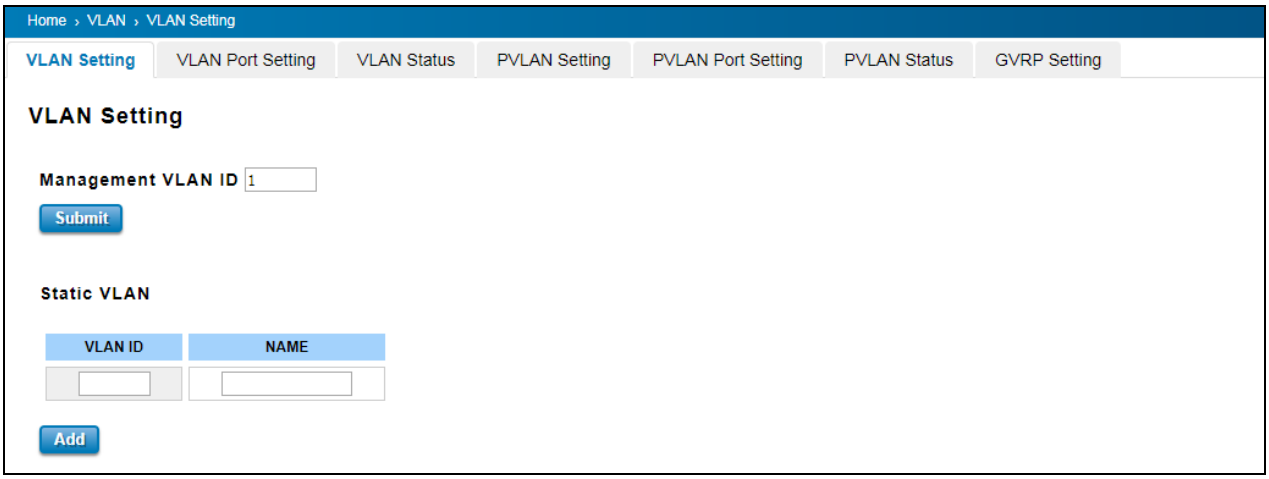
• **VLANs help control traffic:** VLANs increase the efficiency of User network because each VLAN can be set up to contain only those devices that need to communicate with each other.

This switch also has **private VLAN** functions; it helps to resolve the primary VLAN ID shortage, client ports' isolation and network security issues. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains, allowing User to isolate the ports on the switch from each other. A subdomain consists of a primary VLAN and one or more secondary VLANs. All VLANs in a private VLAN domain share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another. The secondary VLANs may either be isolated VLANs or community VLANs. A host on an isolated VLAN can only communicate with the associated promiscuous port in its primary VLAN. Hosts on community VLANs can communicate among themselves and with their associated promiscuous port but not with ports in other community VLANs. The Private VLAN provides **primary** and **secondary VLAN** within a single switch.

| TERMS | DESCRIPTION |
|---|---|
| **Primary VLAN** | The uplink port is usually the primary VLAN. A primary VLAN contains promiscuous ports that can communicate with the Secondary VLANs. |
| **Secondary VLAN** | The client ports are usually defined within secondary VLAN. The secondary VLAN includes Isolated VLAN and Community VLAN. |

### 3.5.1 VLAN SETTING

To configure 802.1Q VLAN and port-based VLANs on the WoMaster switch, use the VLAN Settings page to configure the ports. , User can assign Management VLAN, create the static VLAN, and assigns the Egress rule for the member ports of the VLAN.




The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Management VLAN ID** | **Default : 1**.<br>The switch supports management VLAN. The management VLAN ID is the VLAN ID of the CPU interface so that only member ports of the management VLAN can ping and access the switch. |
| **Static VLAN** | User can assign a VLAN ID and VLAN Name for new VLAN here. |
| **VLAN ID** | **Default: 1**<br>Used by the switch to identify different VLANs. Valid VLAN ID is between 1 and 4094. |
| **Name** | A reference for network administrator to identify different VLANs. The available character is 12 for User to input. If User don't input VLAN name, the system will automatically assign VLAN name for the VLAN. The rule is VLAN (VLAN ID). |

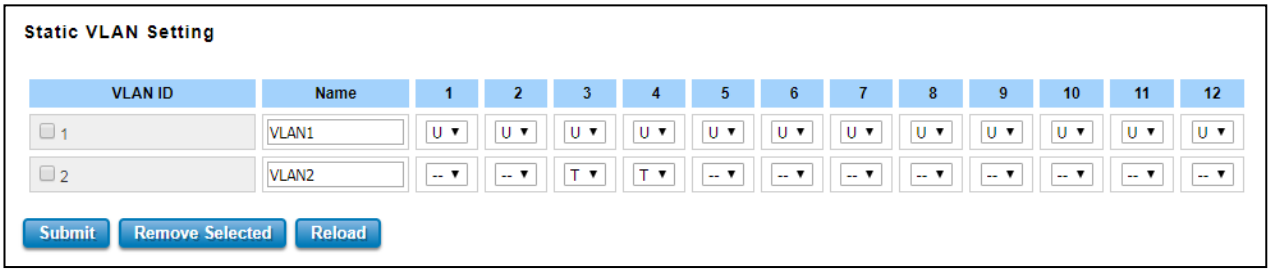
The steps to create a new VLAN: Type in VLAN ID and NAME, and press **Add** to create a new VLAN. Then User can see the new VLAN in the Static VLAN Configuration table. After created the VLAN, the status of the VLAN will remain in Unused until User adds ports to the VLAN.

**NOTE:**

1. Before User changed the management VLAN ID by Web and Telnet, remember that the port attached by the administrator should be the member port of the management VLAN; otherwise the administrator can't access the switch via the network.
2. WoMaster switch supports max 256 groups VLAN.

## Static VLAN Configuration

Static VLAN Configuration table is presented on the figure below. User can see the created VLANs and specify the egress (outgoing) port rule to be **Untagged or Tagged** here.




The description of the columns is as below:

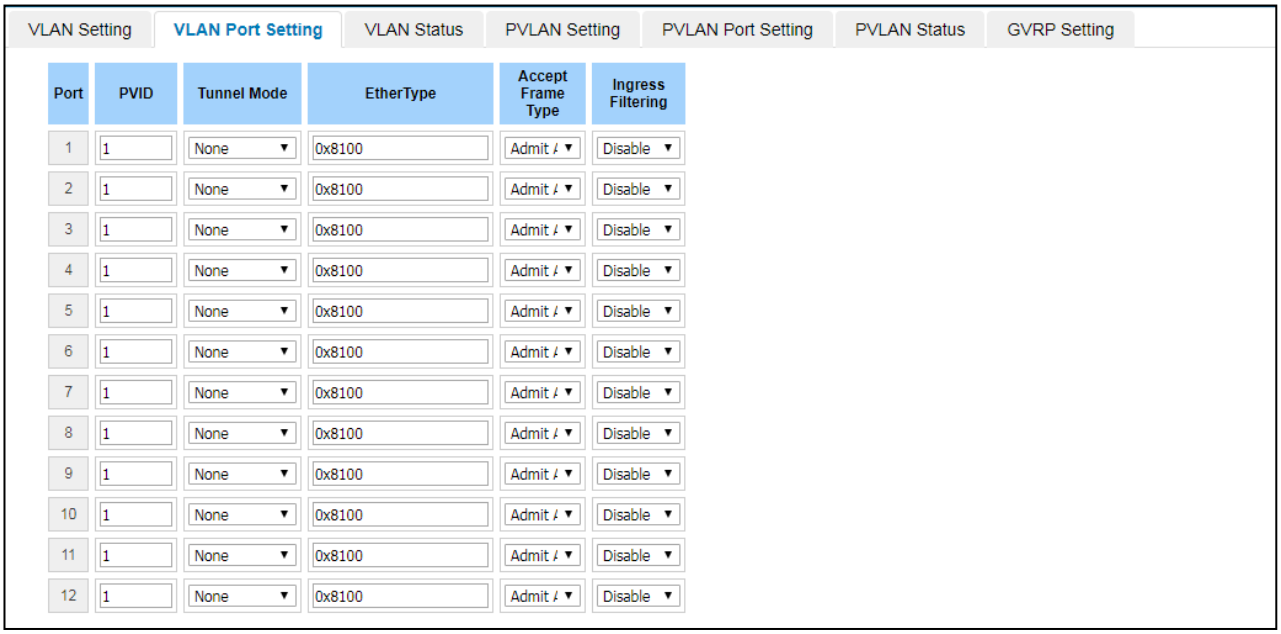
| TERMS | DESCRIPTION |
|---|---|
| -- | Not available |
| **U/Untag** | Indicates that egress/outgoing frames are not VLAN tagged. |
| **T/Tag** | Indicates that egress/outgoing frames are to be VLAN tagged. |

**Steps to configure Egress rules :**

Select the VLAN ID. Entry of the selected VLAN turns to light blue. Assign Egress rule of the ports to **U** or **T**. Press **Submit** to apply the setting. If User wants to remove one VLAN, select the VLAN entry. Then press **Remove** button.

## 3.5.2 VLAN PORT SETTING

VLAN Port Setting allows User to setup VLAN port parameters to specific port.



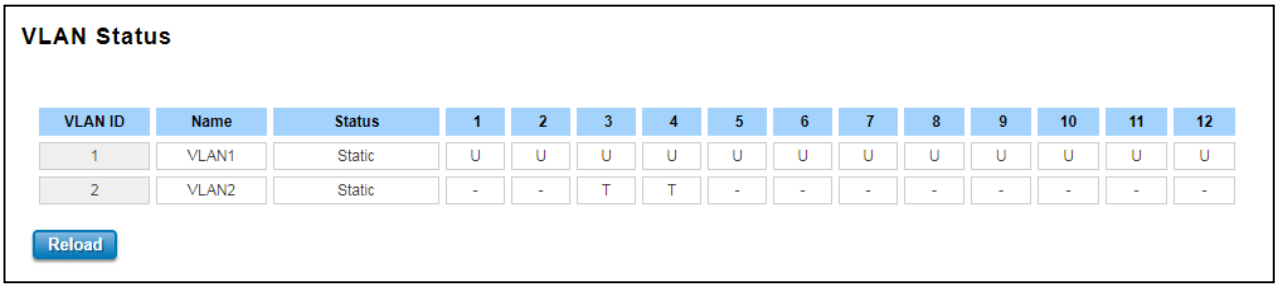

The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **PVID** | The abbreviation of the **Port VLAN ID**. PVID allows the switches to identify which port belongs to which VLAN. To keep things simple, it is recommended that PVID is equivalent to VLAN IDs. The values of PVIDs are from 0 to 4095. But, 0 and 4095 are reserved. User can't input these 2 PVIDs. 1 is the default value. 2 to 4094 are valid and available in this column. |
| **Tunnel Mode** | **Default: None**<br>**None** : This is Port that no using Q in Q<br>**802.1Q Tunnel**: As the Ingress port, is connected to the client port. Configures Q in Q tunneling for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.<br>**802.1Q Tunnel Uplink**: As the egress port, that is, the middle switch port. Configures Q in Q tunneling for an uplink port to another device within the service provider network.<br>**802.1Q Tunnel Uplink-Add-PVID**: Assign second VLAN tag for specify VLANs. |
| **Ether Type** | **Default: 0x8100**<br>It is used to indicate which protocol is encapsulated in the payload of the frame. |
| **Accept Frame Type** | This column defines the accepted frame type of the port. There are 2 modes User can select, **Admit All** and **Tag Only**. Admit All mode means that the port can accept both tagged and untagged packets. **Tag Only** mode means that the port can only accept tagged packets. |
| **Ingress Filtering** | Ingress filtering helps VLAN engine to filter out undesired traffic on a port. When Ingress Filtering is enabled, the port checks whether the incoming frames belong to the VLAN |

| | |
|---|---|
| | they claimed or not. Then the port determines if the frames can be processed or not. For example, if a tagged frame from Engineer VLAN is received, and Ingress Filtering is enabled, the switch will determine if the port is on the Engineer VLAN's Egress list. If it is, the frame can be processed. If it's not, the frame would be dropped. |

### 3.5.3 VLAN STATUS

This table shows User current status of User VLAN, including VLAN ID, Name, Status, and Egress rule of the ports.

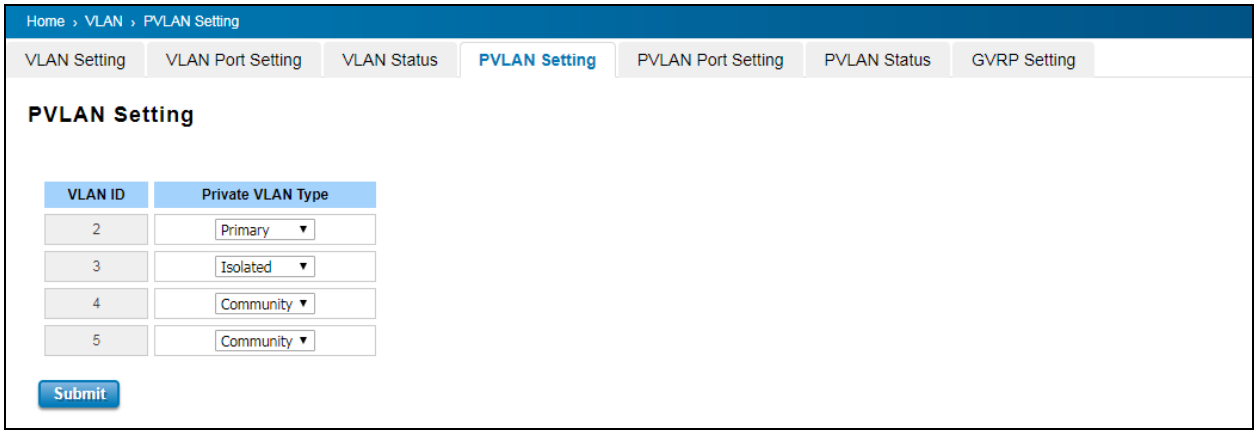



The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **VLAN ID** | ID of the VLAN. |
| **Name** | Name of the VLAN. |
| **Status** | **Static** shows this is a manually configured static VLAN. This VLAN is not workable yet. **Dynamic** means this VLAN is learnt by GVRP. |

After created the VLAN, the status of this VLAN will remain in unused status until User adds ports to the VLAN.

### 3.5.4 PVLAN SETTING




The figure above is PVLAN Setting interface. PVLAN Configuration allows User to assign Private VLAN type. After created VLAN in VLAN Configuration page, the available VLAN ID will display here. Choose the Private VLAN types for each VLAN User wants configure.

The description of the columns is as below:

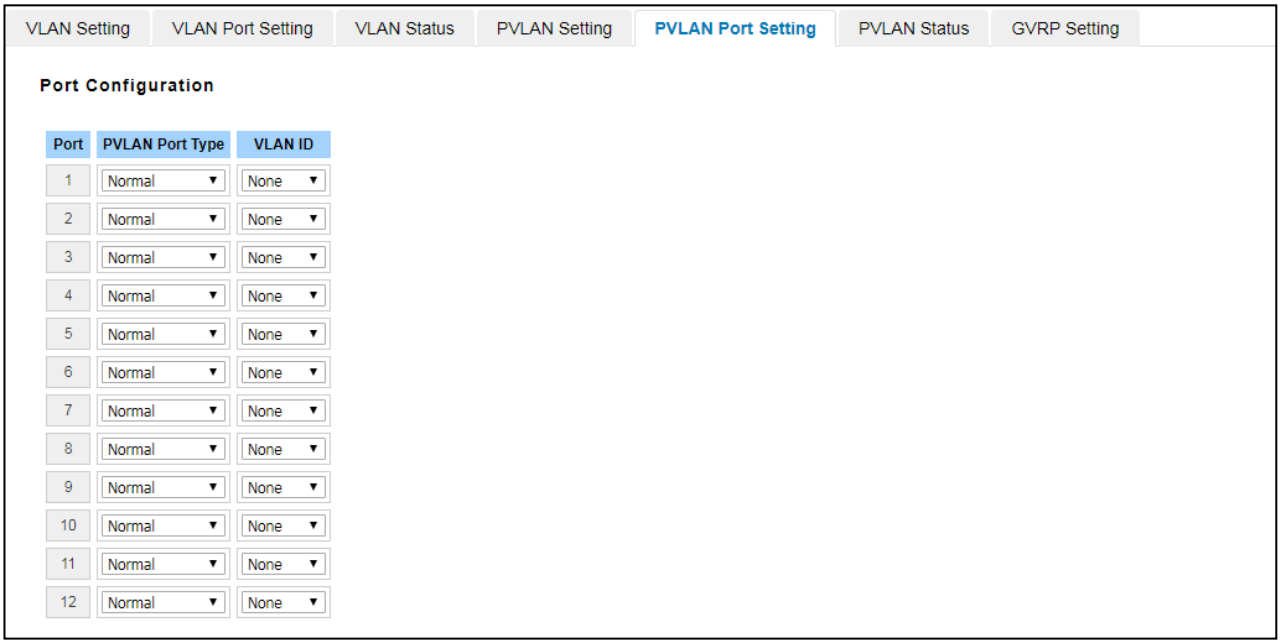
| TERMS | DESCRIPTION |
|---|---|
| **None** | The VLAN is not included in Private VLAN. |
| **Primary** | The VLAN is the Primary VLAN. The member ports can communicate with secondary ports. |

| | |
|---|---|
| **Isolated** | The VLAN is the Isolated VLAN. The member ports of the VLAN are isolated. |
| **Community** | The VLAN is the Community VLAN. The member ports of the VLAN can communicate with each other. |

## 3.5.5 PVLAN PORT SETTING

PVLAN Port Setting page allows configure Port Configuration and Private VLAN Association.

### Port Configuration



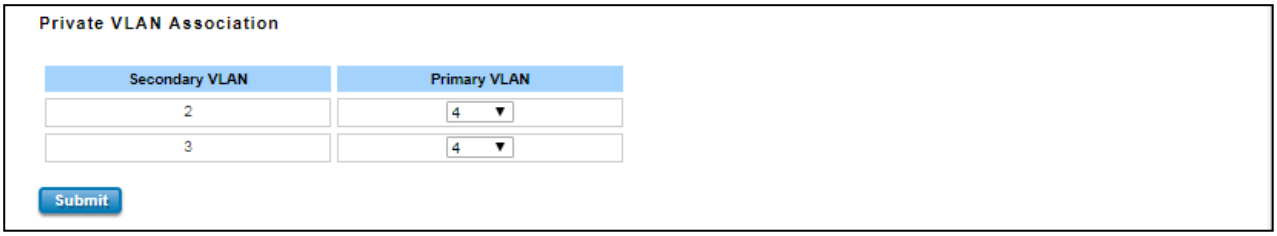

The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **PVLAN Port Type** | **Normal:** The Normal port is None PVLAN ports; it remains its original VLAN setting.<br>**Host:** The Host type ports can be mapped to the Secondary VLAN.<br>**Promiscuous:** The promiscuous port can be associated to the Primary VLAN. |
| **VLAN ID** | After assigned the port type, the web UI display the available VLAN ID the port can associate to. |

### Private VLAN Association (PVLAN)

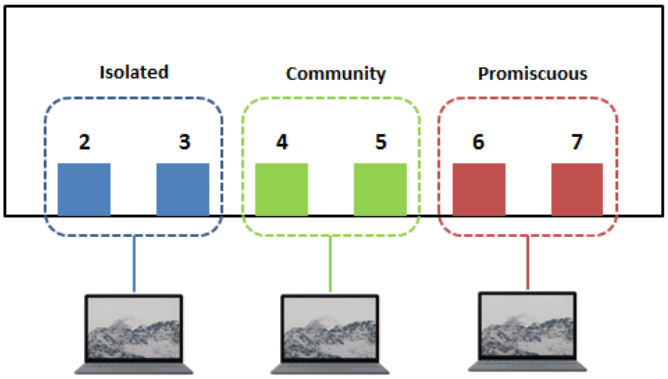
**Secondary VLAN:** Secondary VLAN is included Isolated and Community VLAN Type that assigned in Private VLAN Configuration section. User can select the Secondary VLAN ID here.

**Primary VLAN:** Primary VLAN is included the Primary VLAN Type that assigned in Private VLAN Configuration section. User can select the Primary VLAN ID here.




Before configuring PVLAN port type, the Private VLAN Association should be done first.

For example:




**1. Create VLAN and Assign the Private VLAN Type:**

The very first thing that user need to do is create the VLAN and make sure that the ports are assigned to specific VLAN. After created VLAN, assign the Private VLAN type for each VLAN, for example: VLAN 2 -> Isolated (Secondary VLAN), VLAN 3 -> Community (Secondary VLAN) and VLAN 4 -> Primary.

**2. Associate the Secondary VLAN to Primary VLAN:**

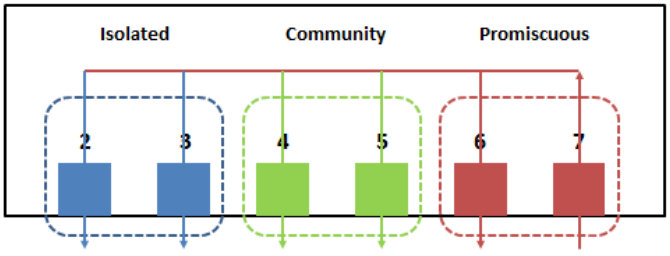
After create the VLAN and assign the Private VLAN Type, then associate the secondary VLAN, VLAN 2 and 3 to VLAN 4 as the Primary VLAN in Private VLAN Association section..

**3. Configure the Private VLAN Port:**

- VLAN 4 – **Primary** -> The member port of VLAN 4 is Promiscuous port. (Port 6 and 7)
- VLAN 2 – **Isolated** -> Map the Host port to VLAN 2. (Port 2 and 3)
- VLAN 3 – **Community** -> Map the Host port to VLAN 3. (Port 4 and 5)

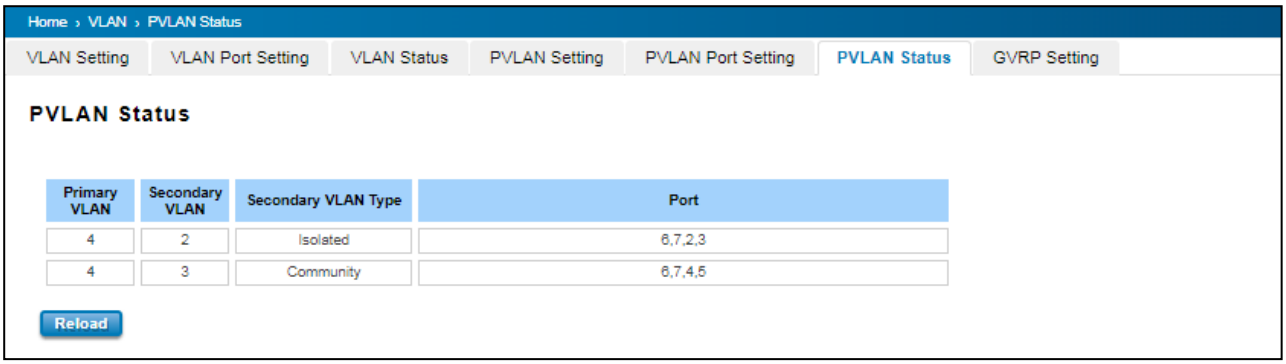
**5. Result (See 3.5.6 PVLAN Status):**

- VLAN 4 -> VLAN 2 and 3; member ports (6 & 7) can communicate with ports in secondary VLAN.
- VLAN 2 -> VLAN 4; member ports (2 & 3) are isolated and cannot communicate each other, but they can communicate with Primary VLAN ports.
- VLAN 3 -> VLAN 4; member ports (4 & 5) within the community can communicate with each other and communicate with Primary VLAN ports.

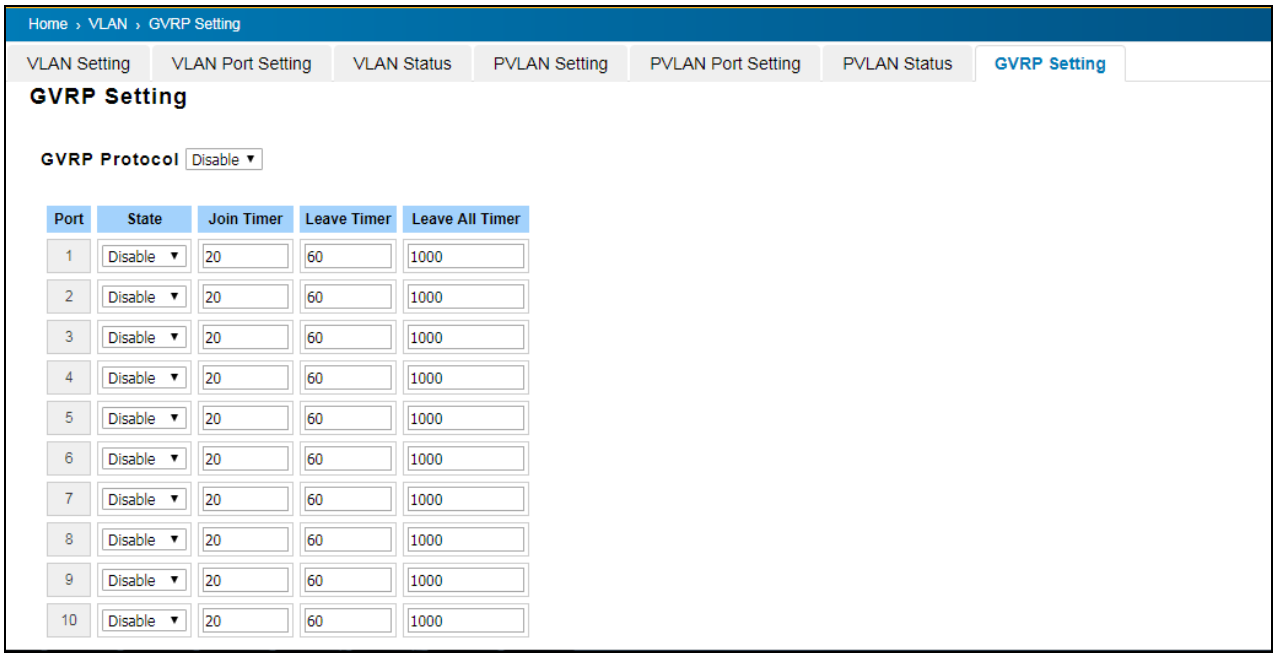


## 3.5.6 PVLAN STATUS

This page allows User to see the Private VLAN status information.




## 3.5.7 GVRP SETTING




GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices. GVRP allows users to set-up VLANs automatically rather than manual configuration on every port of every switch in the network. The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **GVRP Protocol** | **Default: Disable**<br>Allow user to enable / disable GVRP function globally. |
| **State** | **Default: Disable**<br>After enable GVRP globally, here still can enable/disable GVRP by port. |
| **Join Timer** | **Default: 20**<br>Controls the interval of sending the GVRP Join BPDU. An instance of this timer is required on a per-Port, per-GARP Participant basis |

| | |
|---|---|
| **Leave Timer** | **Default: 60**<br>Control the time to release the GVRP reservation after received the GVRP Leave BPDU. An instance of the timer is required for each state machine that is in the LV state. |
| **Leave All Timers** | **Default: 1000**<br>Controls the period to initiate the garbage collection of registered VLAN. The timer is required on a per-Port, per-GARP Participant basis |

## 3.6 QUALITY of SERVICE (QoS)

Quality of Service (QoS) is the ability from the switch to provide different priority to different applications, users or data flows, or to guarantee a certain level of performance to a data flow. QoS guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications. QoS can also help to reduce traffic problems and control the traffic by deliver the high priority first. This section allows User to configure Quality of Service settings for each port by configure the priorities in order to provide a smooth data traffic.

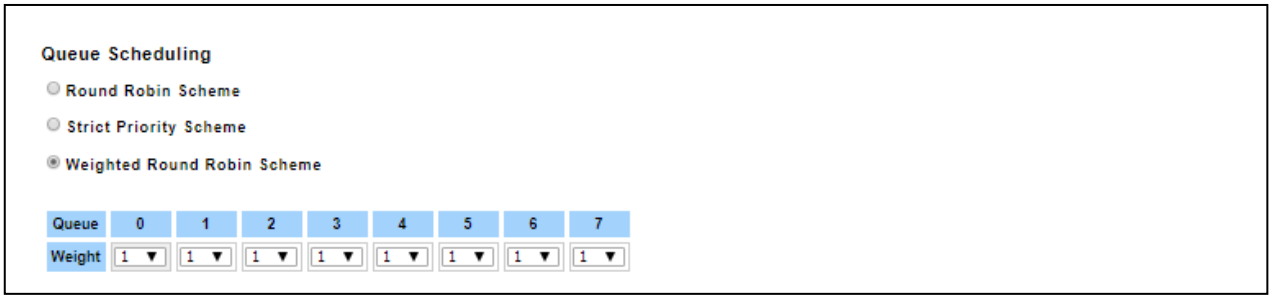
### 3.6.1 QoS SETTING

The figure below shows QoS Setting.


**QoS Trust Mode**

**802.1P Priority Tag**: If 802.1P is selected the switch relies on a packet's CoS information to determine priority. This is related to the settings in the CoS-Queue Mapping page

**DSCP/TOS Code Point**: If DSCP/TOS is selected the switch relies on a packets differentiated services code point information to determine the priority. This is related to the settings in the DSCP-Priority Mapping page.

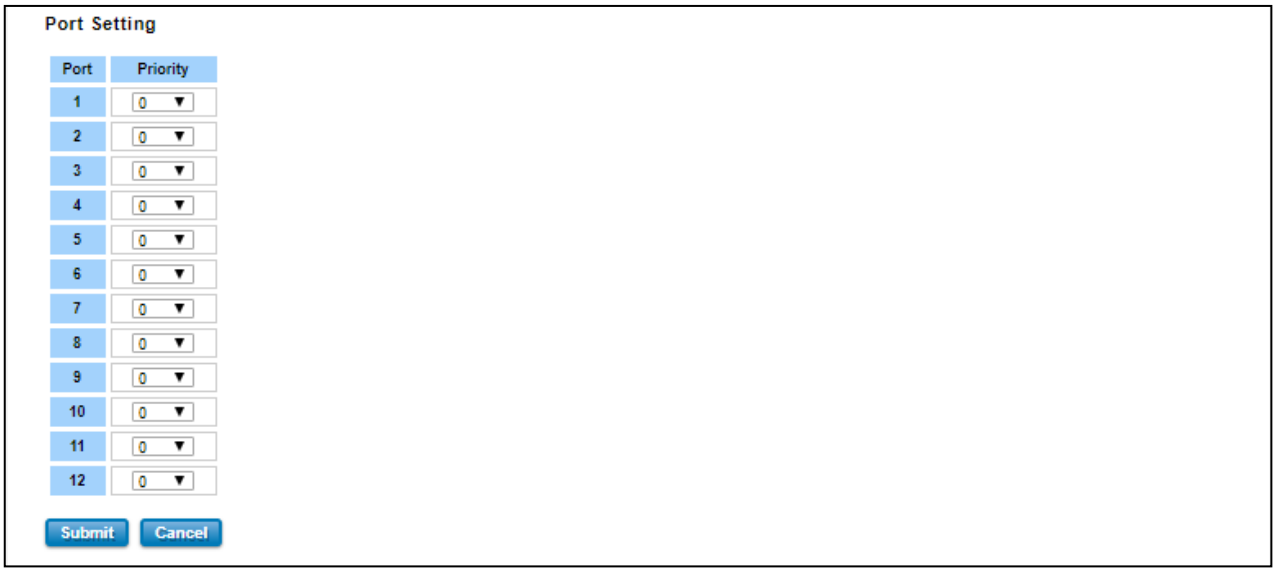



**Queue Scheduling**

User may select the Queue Scheduling rule:

- **Use Round Robin Scheme:** The Round Robin scheme means all the priority has the same privilege, the traffic is forward cyclic from highest to lowest.
- **Use strict priority scheme:** The priority here always the higher queue will be processed first, except the higher queue is empty.
- **Use Weighted Round Robin scheme.** This scheme allows users to assign new weight ratio from 1 to 10 for each class where 10 is the highest ratio.

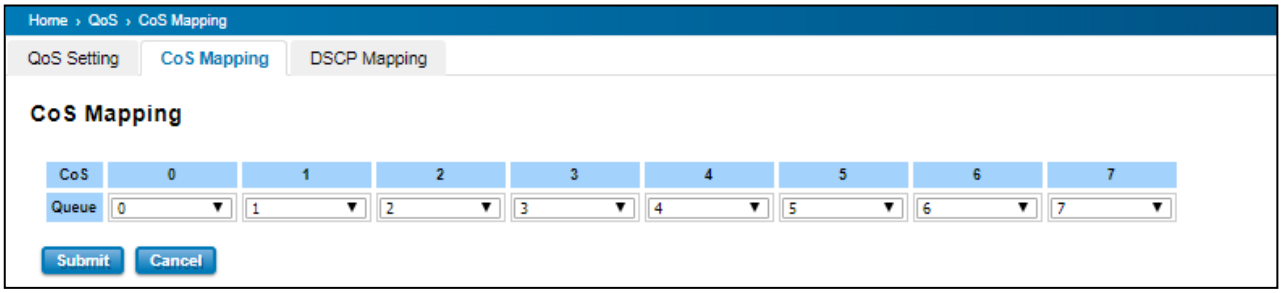
**Port Setting**




Choose the Queue value of each port, the port then has its default priority. The Queue 7 is the highest port-based queue, 0 is the lowest queue. The traffic injected to the port follows the queue level to be forwarded, but the outgoing traffic does not bring the queue level to next switch. Click the **Submit** button to apply the configuration changes.

## 3.6.2 CoS MAPPING

This section allows user to change CoS values to Physical Queue mapping table. In WoMaster switch, users can freely assign the mapping table or follow the suggestion of the 802.1p standard. Below is the interface.




The service classes (CoS) are assigned to the queues as default as follows:

- COS 0 → Queue 0
- COS 1 → Queue 1
- COS 2 → Queue 2
- COS 3 → Queue 3
- COS 4 → Queue 4
- COS 5 → Queue 5
- COS 6 → Queue 6
- COS 7 → Queue 7

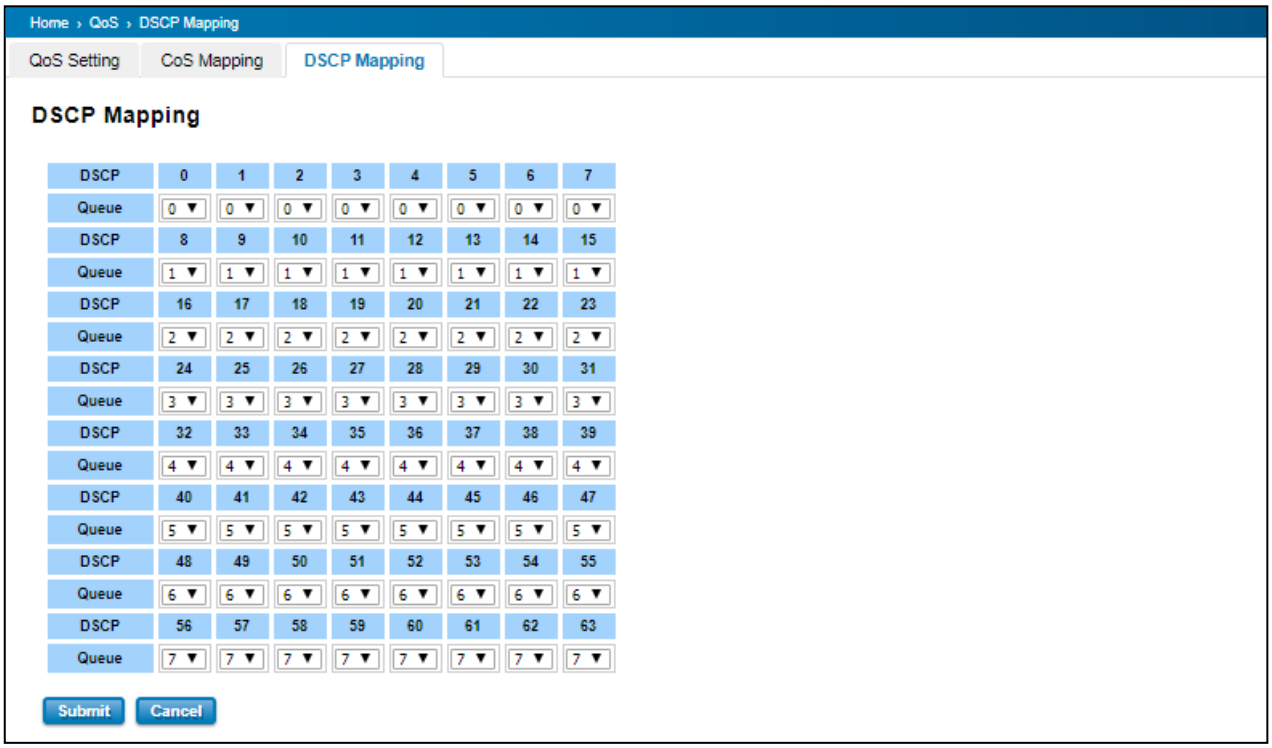
For the step in configuration

1. For each value in the **CoS** column, select the queue from the **Queue** drop-down list.

2. Click the **Submit** button.

## 3.6.3 DSCP MAPPING

This page is to change DSCP values to Physical Queue mapping table. Users should therefore assign how to map DSCP value to the level of the physical queue. Users can freely change the mapping table to follow the upper layer 3 switch or routers' DSCP setting.




After configuration, press **Submit** to enable the settings.

| DSCP Value and Priority Queues Setting | Description | Factory Default |
|---|---|---|
| 0 to 7 | Maps different TOS values to one of 8 different egress queues. | 0 |
| 8 to 15 | | 1 |
| 16 to 23 | | 2 |
| 24 to 31 | | 3 |
| 32 to 39 | | 4 |
| 40 to 47 | | 5 |
| 48 to 55 | | 6 |
| 56 to 63 | | 7 |

## 3.7 MULTICAST

Multicasts are similar to broadcasts, they are sent to all end stations on a LAN or VLAN that belong to the multicast group. Multicast filtering is the function, which end stations can receive the multicast traffic if the connected ports had been included in the specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to the registered end stations. For multicast filtering, WoMaster switch uses IGMP Snooping technology. IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic, thereby reducing the amount of traffic on the Ethernet LAN. In effect, it manages multicast traffic by making use of switches, routers, and hosts that support IGMP.

Following sections are included in this group:

3.7.1 IGMP Query

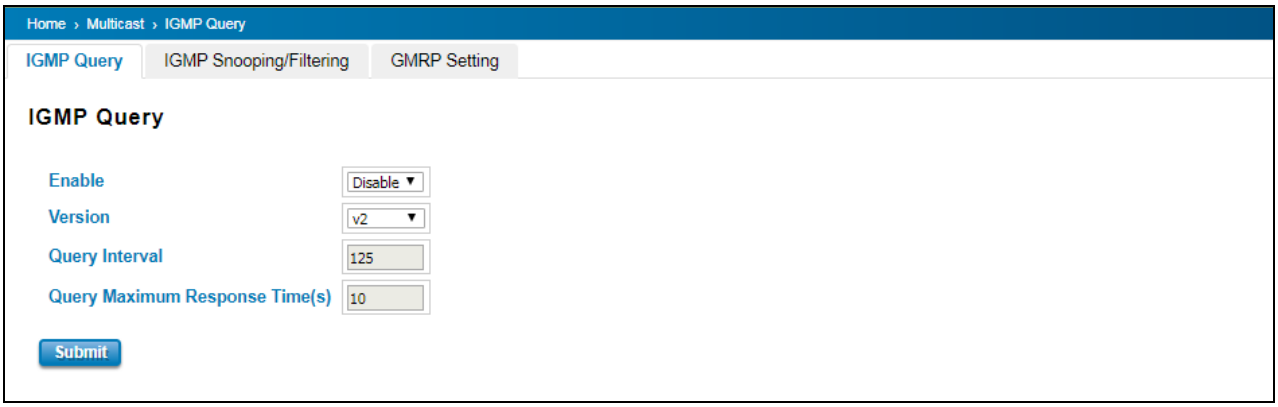
3.7.2 IGMP Snooping

3.7.3 GMRP Setting

### 3.7.1 IGMP QUERY

This page allows users to configure **IGMP Query** feature. Since the device can only be configured by member ports of the management VLAN, IGMP Query can only be enabled on the management VLAN. If User wants to run IGMP Snooping feature in several VLANs, User should notice that whether each VLAN has its own IGMP Querier first.

The IGMP querier periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it.



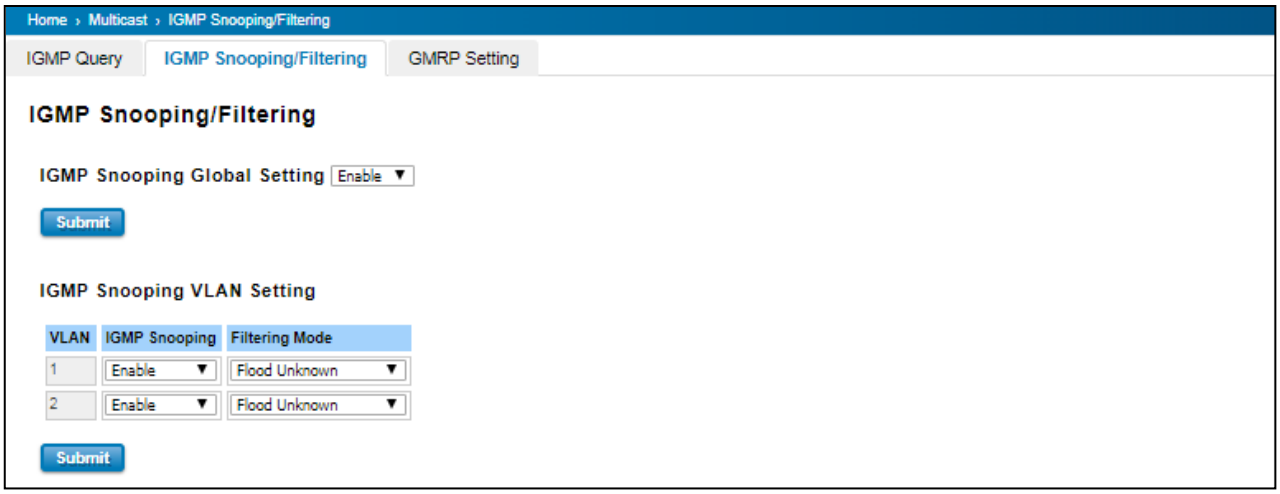

For networks with more than one IGMP querier, a switch with the lowest IP address becomes the IGMP querier.

| TERMS | DESCRIPTION |
|---|---|
| **Enable** | **Default: Disable**<br>Enable the IGMP Query function |
| **Version** | **Default: V2**<br>**V1** means IGMP V1 General Query<br>**V2** means IGMP V2 General Query. |
| **Query Interval(s)** | The interval period of querier to send the query. |
| **Query Maximum Response Time (s)** | The response time for querier detects to confirm there are no more directly connected group members on a LAN. |

Once User finished configuring the settings, click on **Submit** to apply User configuration.

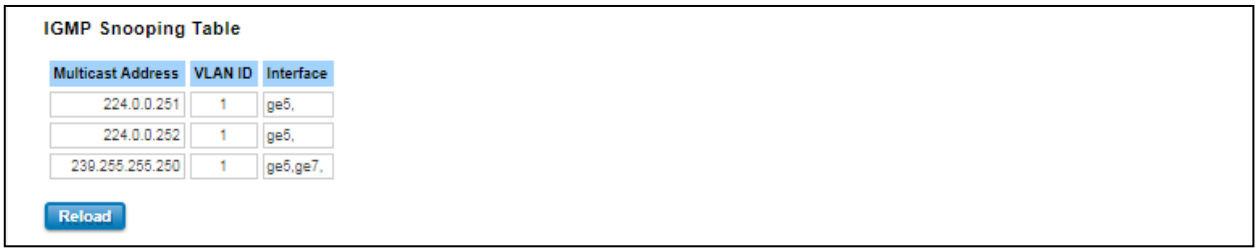
## 3.7.2 IGMP SNOOPING

This page is to enable IGMP Snooping feature. After enable the feature, user may assign IGMP Snooping function to specific VLAN, and the IGMP Snooping table will show the specific multicast group from dynamic learnt or manual input. By enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch.



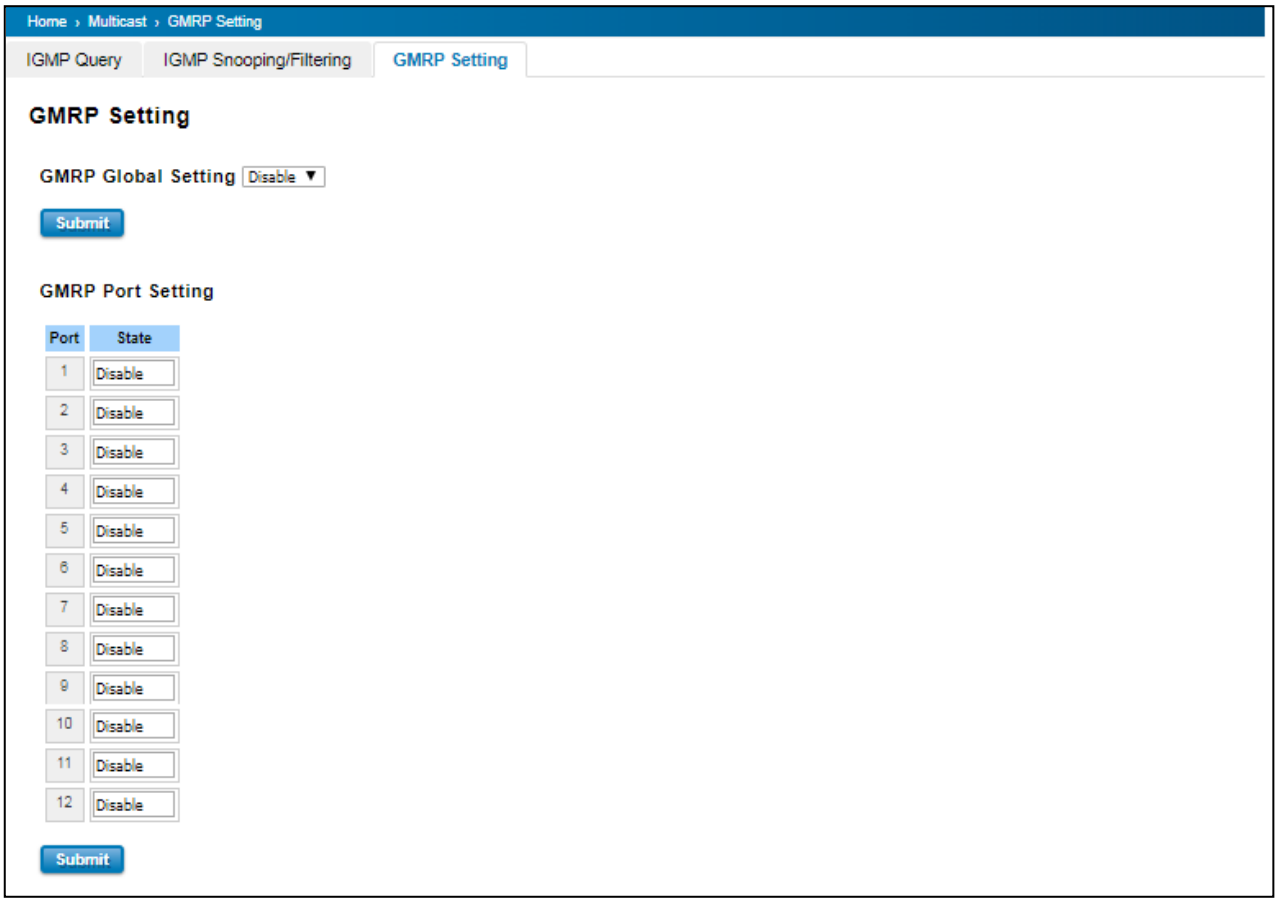

| TERMS | DESCRIPTION |
|---|---|
| **IGMP Snooping Global Setting** | User can select **Enable** or **Disable** this function here. After enabling IGMP Snooping, User can then enable IGMP Snooping for specific VLAN. |
| **IGMP Snooping** | Select the **Enable** to activate the IGMP Snooping. In the same way, User can also **Disable** IGMP Snooping for certain VLANs. |
| **Filtering Mode** | It allows the switch to filter the unknown-multicast data flow. Multicast Filtering Mode is Flood unknown, discard unknown and source only learning.<br>- Flood Unknown: The switch would filter the unknown packets that transmit through the network and the packets will be flooded to the member ports of the same VLAN.<br>- Discard Unknown: Non-member ports will not receive the unknown packets because the filter discards the unknown multicast.<br>- Source Only Learning: The switch learns the IP multicast group from the IP multicast data stream and only forwards traffic to the multicast ports. |

**IGMP Snooping Table**: User can see several information such as multicast IP address, VLAN ID from the multicast group, and the interface member ports of the multicast group (256 multicast groups)




## 3.7.3 GMRP SETTING

GARP Multicast Registration Protocol (GMRP) is a Generic Attribute Registration Protocol (GARP) application that provides a constrained multicast flooding facility similar to IGMP snooping. GMRP and GARP are industry-standard protocols defined by the IEEE 802.1P. The GMRP Setting allows bridges and end stations to dynamically register group membership information with the MAC bridges attached to the same LAN segment and for that information to be disseminated across all bridges in the Bridged LAN that supports extended filtering services.



## 3.8 SNMP

SNMP is a standard TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates. System management software uses SNMP to allow administrators to remotely monitor and manage thousands of systems on a network, often by presenting the data gathered from monitored devices in a snapshot or dashboard view. WoMaster Managed Switch support SNMP v1 and v2c and V3.

SNMP managed network consists of two main components: agents and a manager. An agent is a management software module that resides in a managed switch. An agent translates the local management information from the managed device into a SNMP compatible format. The manager is the console through the network.

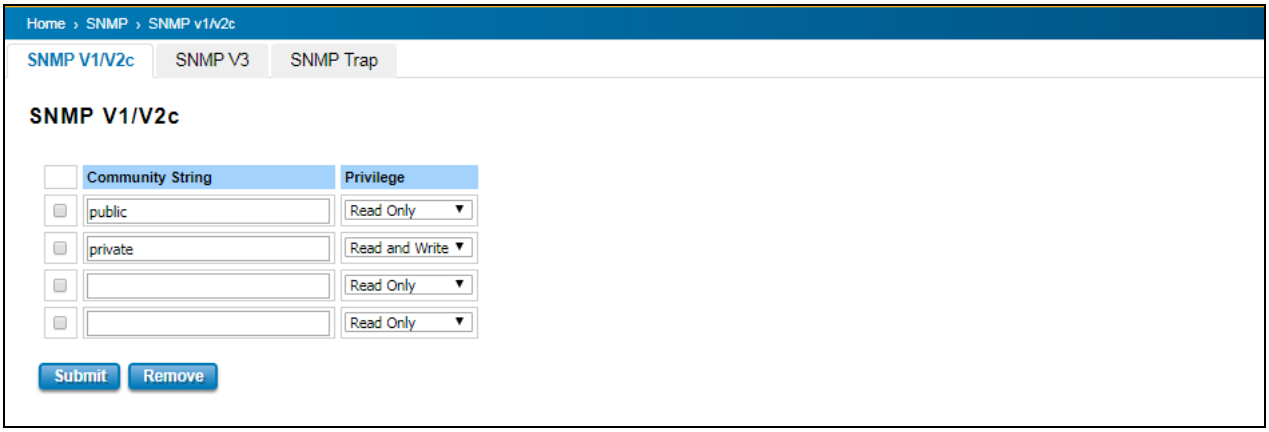
### 3.8.1 SNMP V1/V2c SETTING

In this page allows users to define the new community string set and remove the unwanted community string. The community string can be viewed as the password because SNMP V1/V2c doesn't request User to enter password before User tries to access SNMP agent. The community includes 2 privileges, Read Only and Read and Write.

| PRIVILEGE | DESCRIPTION |
|---|---|
| Read Only | User only has the ability to read the values of MIB tables.<br>Default community string is Public. |
| Read and Write | User has the ability to read and set the values of MIB tables.<br>Default community string is Private. |

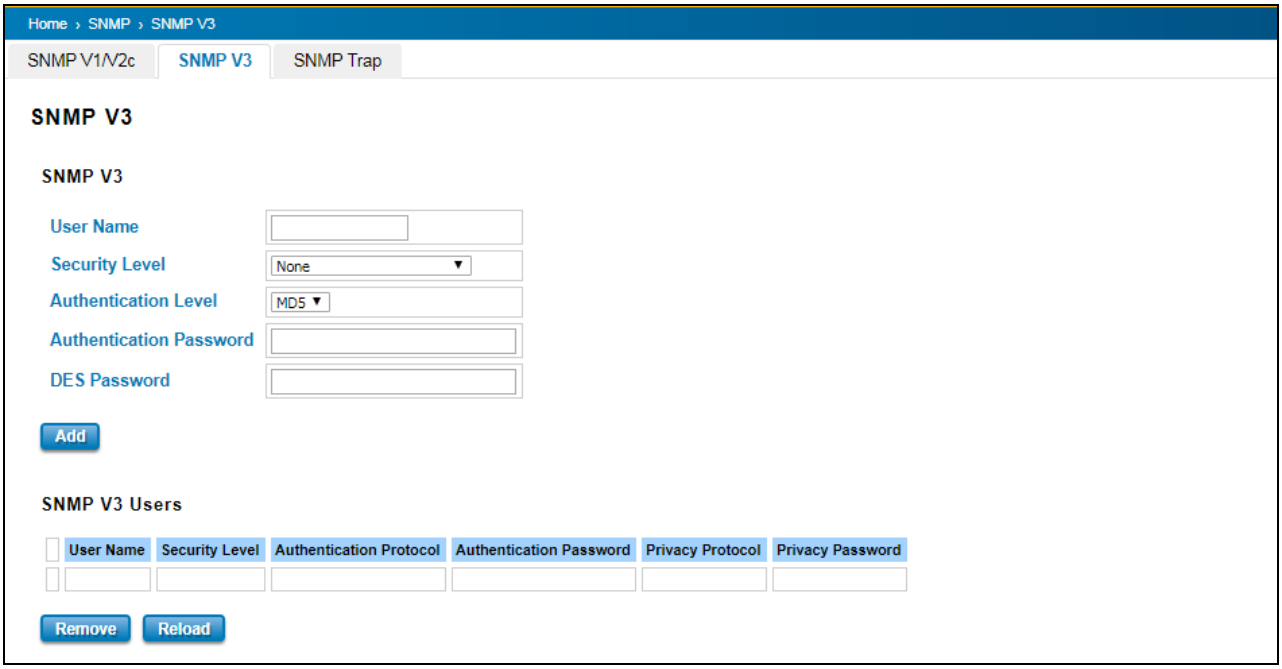
WoMaster Managed Switch allows users to assign 4 community strings. Type the community string and select the privilege. Then press **Submit**.

> NOTE: When User first installs the device in User network, we highly recommend user to change the community string. Since most SNMP management application uses Public and Private as their default community name, this might be the leakage of the network security.



## 3.8.2 SNMP V3

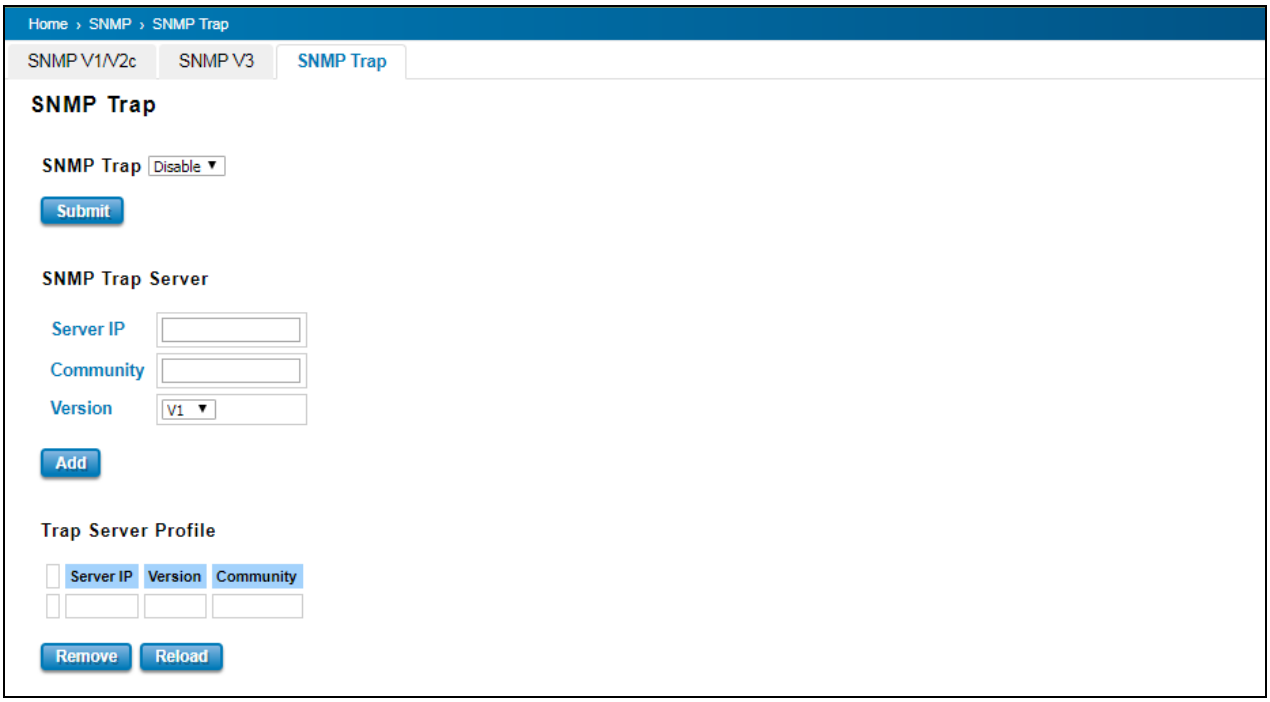
SNMPv3 provides network monitoring and control through SNMP protocol that provides secure access to devices by a combination of authenticating (MD5 & SHA) and encrypting packets over the network to ensure the secure communication. The security model that is used by SNMPv3 is an authentication strategy that is set up for a user and user group. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is used for an SNMP packet.




| TERMS | DESCRIPTION |
|---|---|
| **User Name** | Set up the user name. |
| **Security Level** | **Default: None**<br>Here the user can select the following levels of security: None, User Authentication, and Authentication with privacy. |
| **Authentication Level** | **Default: MD5**<br>MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value. SHA (Secure Hash Algorithm) hash functions refer to five Federal Information Processing Standard-approved algorithms for computing a condensed digital representation. |
| **Authentication Password** | Here the user enters the SNMP v3 user authentication password. |
| **DES Password** | Here the user enters the password for SNMP v3 user DES Encryption. |

### 3.8.3 SNMP TRAP

SNMP Trap is the notification feature defined by SNMP protocol. All the SNMP management applications can understand such trap messages generated by the switch. If no trap manager is defined, no traps will be issued. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version. Below is the SNMP Trap Interface.




| TERMS | DESCRIPTION |
|---|---|
| **SNMP Trap** | **Default: Disable**<br>Enable / Disable SNMP Trap |
| **Server IP** | Enter the IP address of the trap manager. |
| **Community** | Enter the community string for the trap station. |
| **Version** | Select the SNMP trap version type—v1 or v2c. |

After configuration, Click **Add** then User can see the change of the SNMP pre-defined standard traps.

## 3.9 SECURITY

WoMaster Switch provides several security features for User to secure access to its management functions and it can be remotely managed (monitored and configured).

Following topics are included in this section:

3.9.1 Filter

3.9.2 IEEE 802.1X

### 3.9.1 FILTER

Filter is known as Access Control List feature. There are 2 major types; one is MAC Filter that allows user to define the access rule based on the MAC address flexibility. Another one is IP Filter. It includes the IP security, IP Standard access list and advanced IP based access lists.

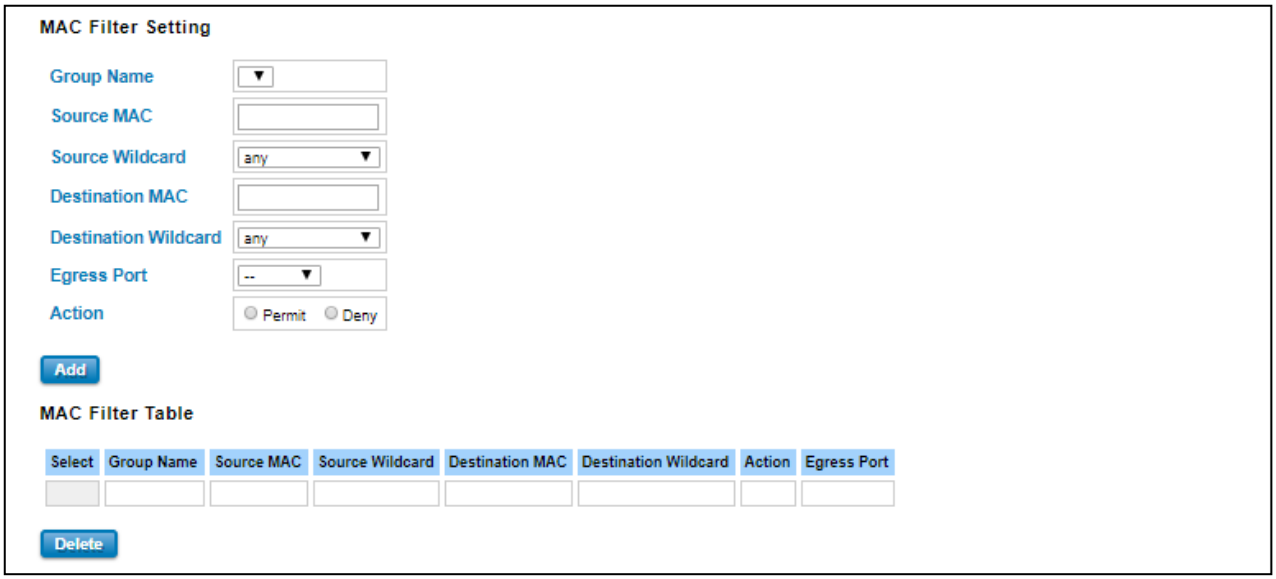
#### MAC Filter

Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. Mac Filter feature allows User to stop the MAC address learning for specific port. After stopping MAC learning, only the MAC address listed in the list can access the switch and transmit/receive traffic. This is a simple way to secure User network environment and not to be accessed by hackers.

**MAC Filter Group**


Create a group of MAC Filters by entering a name and clicking the **Add** button to create a new Filter Group. The MAC Filter Group table provides the following information. **Select** the entry and click the **Delete** button then the Filter Group is deleted. Click the **Reload** button to reload the MAC Filter Group table.

**MAC Filter Setting**

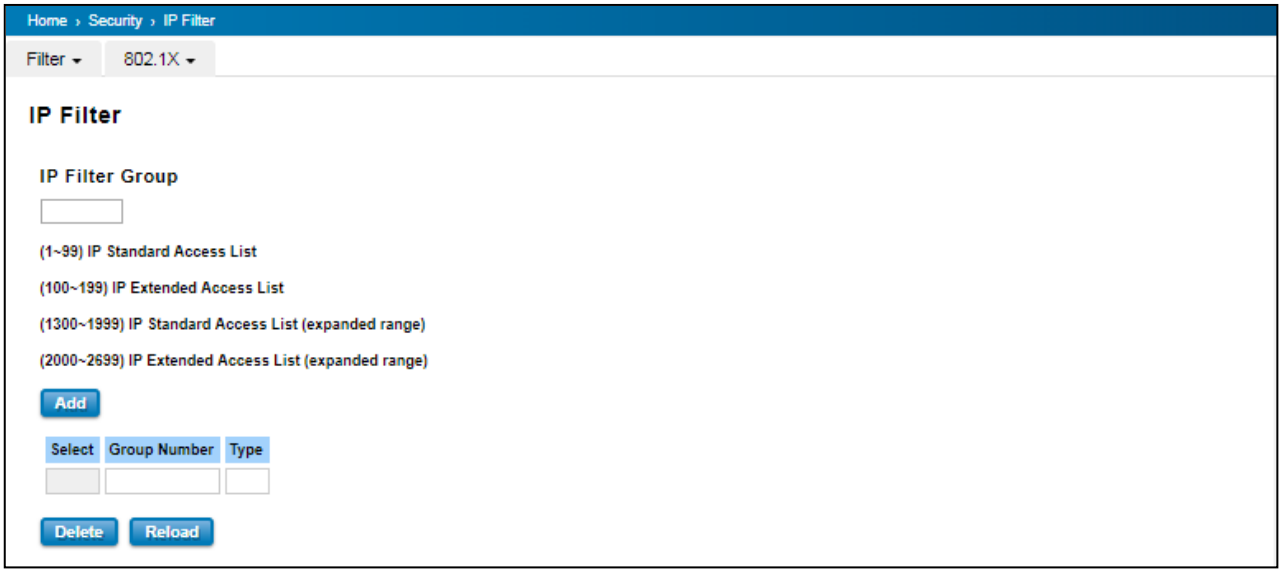



In this form user may configure the MAC Filter Setting. The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Group Name** | This is the name of the MAC Filter Group. |
| **Source MAC** | This is the source MAC Address of the packet. |
| **Source Wildcard** | This is the mask of the MAC Address. |
| **Destination MAC** | This is the destination MAC Address of the packet. |
| **Destination Wildcard** | This is the mask of the MAC Address. |
| **Egress Port** | This is the outgoing (exiting) port number. |
| **Action** | This is the filter action, which is to deny or permit the packet.<br>**Permit:** to permit traffic from specified sources.<br>**Deny:** to deny traffic from those sources. |

Once User finishes configuring the settings, click on **Submit/Add** to apply User configuration.

## IP Filter




User can create a group of IP Filters with following numbers.

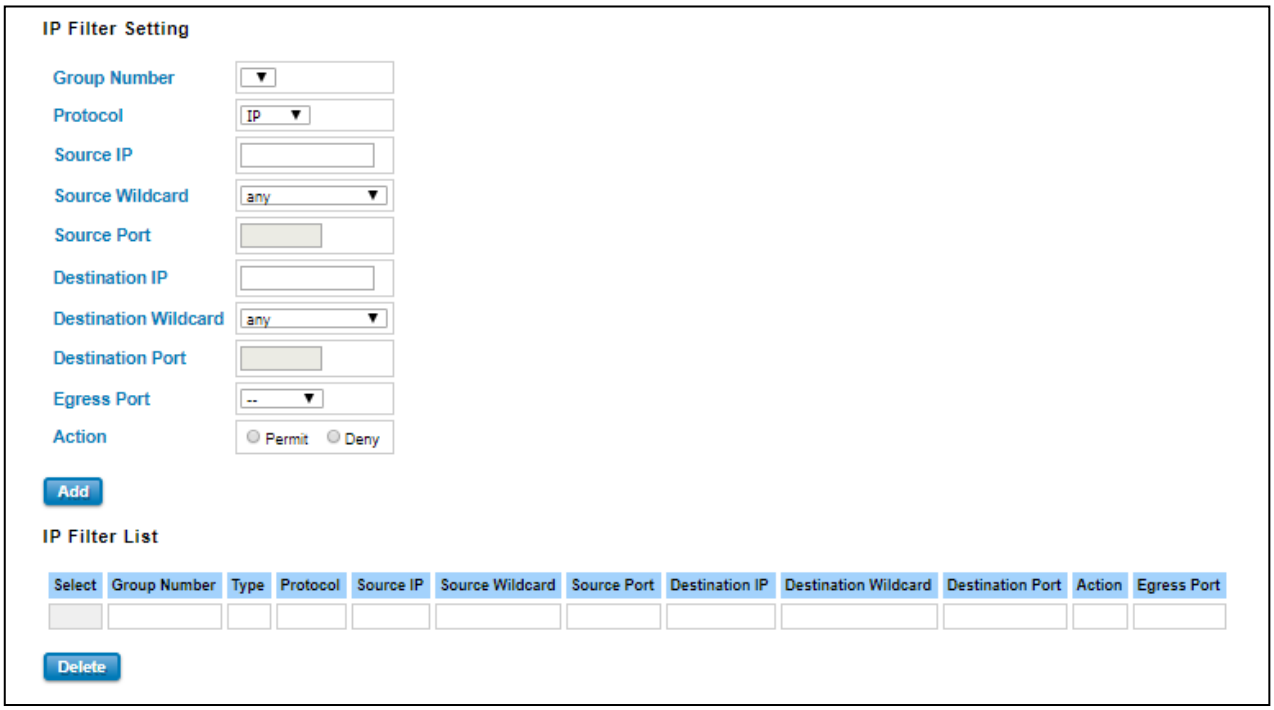
1 - 99: IP Standard Access List

100 – 199: IP Extended Access List

1300 – 1999: IP Standard Access List (expanded range)

2000 – 2699: IP Extended Access List (expanded range)

After entering the IP Filter Group number, click the **Add** to create the new Filter Group.




**IP Filter Setting**

| TERMS | DESCRIPTION |
|---|---|
| **Group Number** | Number of the Filter Group. |

| | |
|---|---|
| **Protocol** | This is the L4 protocol (IP/TCP/UDP/ICMP). |
| **Source IP** | This is the source IP address of the packet. |
| **Source Wildcard** | This is the mask of the IP address. |
| **Source Port** | This is the source port of L4 protocol (TCP/UDP) |
| **Destination IP** | This is the destination IP address of the packet. |
| **Destination Wildcard** | This is the mask of the IP address. |
| **Destination Port** | This is the destination port of L4 protocol (TCP/UDP). |
| **Egress Port** | This is the outgoing (exiting) port number. |
| **Action** | This is the filter action, which is to deny or permit the packet.<br>**Permit:** to permit traffic from specified sources.<br>**Deny:** to deny traffic from those sources. |

**IP Filter List**

| TERMS | DESCRIPTION |
|---|---|
| **Select** | Selected the entry for delete. |
| **Group Number** | Number of the Filter Group. |
| **Type** | This is the filter group type (standard or extended). |
| **Protocol** | This is the L4 protocol (IP/TCP/UDP/ICMP). |
| **Source IP** | This is the source IP address of the packet. |
| **Source Wildcard** | This is the mask of the IP address. |
| **Source Port** | This is the source port of L4 protocol (TCP/UDP) |
| **Destination IP** | This is the destination IP address of the packet. |
| **Destination Wildcard** | This is the mask of the IP address. |
| **Destination Port** | This is the destination port of L4 protocol (TCP/UDP). |
| **Action** | This is the filter action, which is to deny or permit the packet. Click the **Delete** button to remove the Filter that has been selected. |
| **Egress Port** | This is the outgoing (exiting) port number. |

## Filter Attach

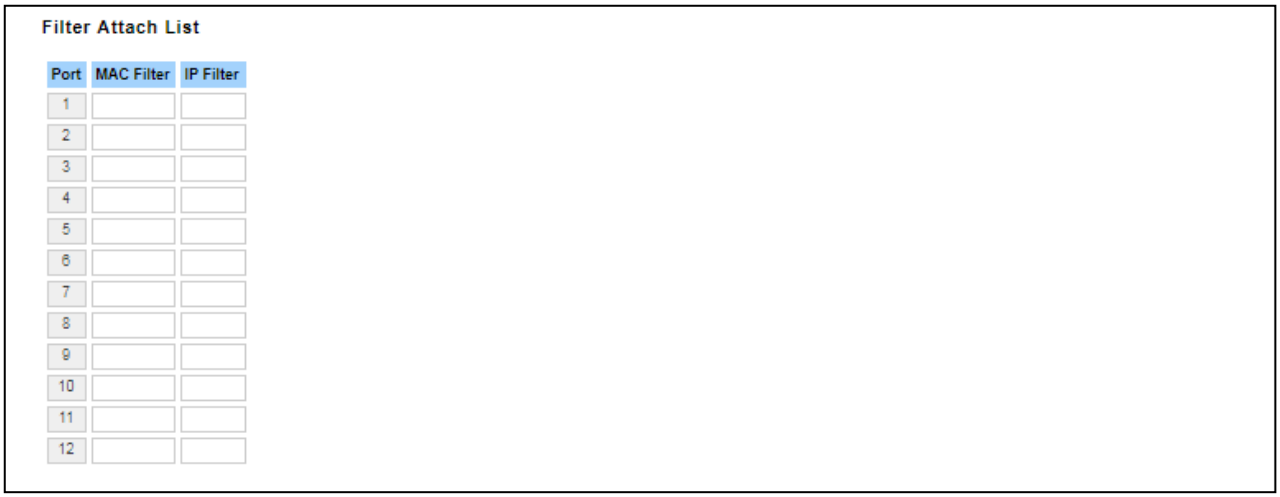
This page allows you to attach filters created on the IP Filter and MAC Filter pages to ports on the switch.


| TERMS | DESCRIPTION |
|---|---|
| **Port** | Select the port that needs to be attached the filter. |
| **MAC Filter** | Select a MAC address based filter to attach to the interface. |
| **IP Filter** | Select an IP address based filter to attach to the interface. |

Click the **Submit** button to apply the configurations.

### Filter Attach List

This table displays what filters are currently attached to each port.




| TERMS | DESCRIPTION |
|---|---|
| **Port** | The port number. |
| **MAC Filter** | The filter attached MAC address |
| **IP Filter** | The filter attached IP address |

## 3.9.2 IEEE 802.1X

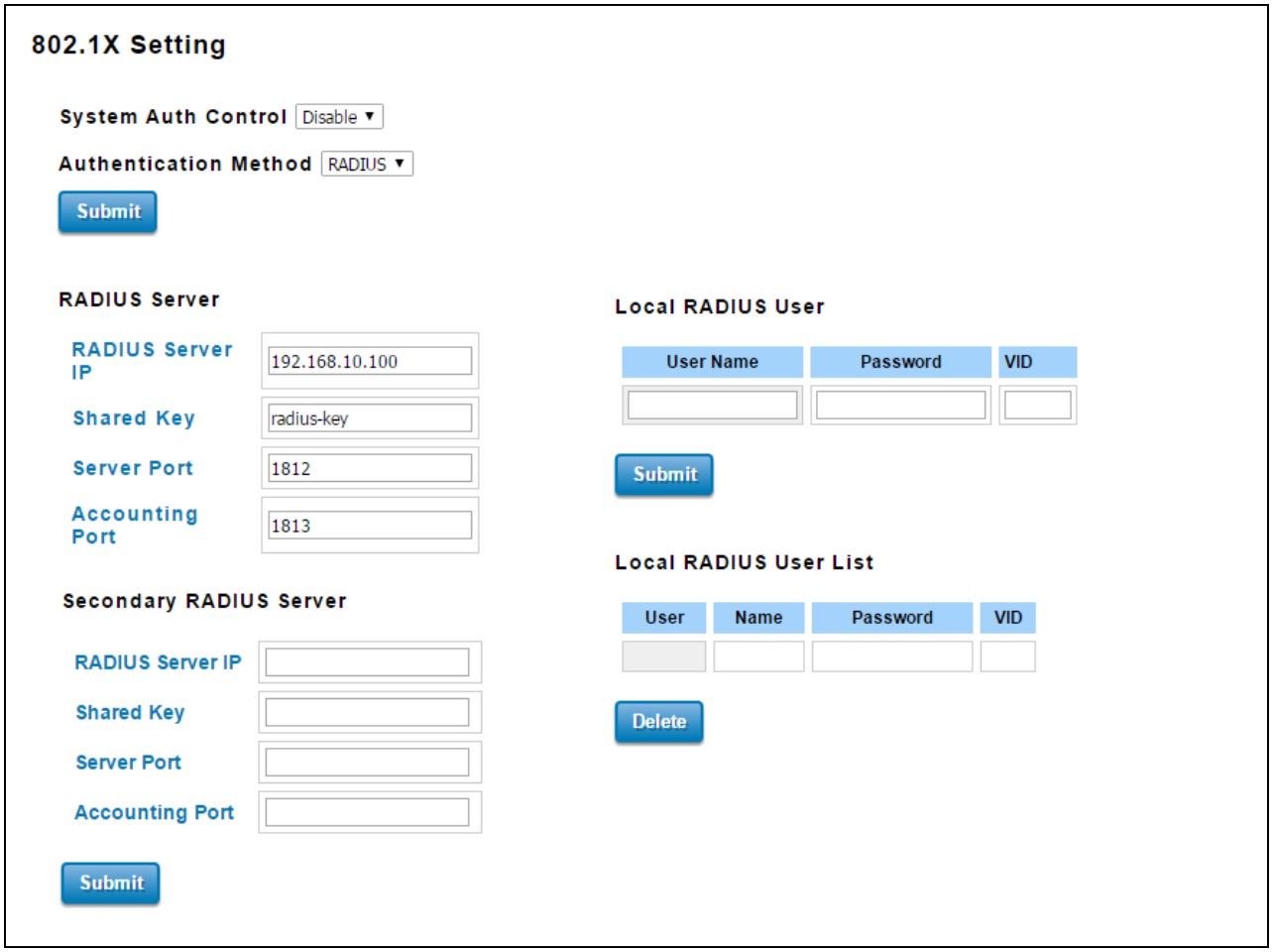
802.1X is an IEEE Standard for Port-based Network Access Control that provides an authentication mechanism to devices that wish to attach to a LAN or WLAN. Port-based network access control protocol contains 3 parts, supplicant, authenticator, and authentication server. With 802.1X authentication, a username can be linked with an IP address, MAC address, and port. This provides greater visibility into the network. 802.1X also provides more security because it only allows traffic transmitting on authenticated ports or MAC addresses.

**RADIUS**

RADIUS is used in the authentication process. Database of authorized users is maintained on a RADIUS server. There is an authenticator, our switch enabling 802.1X, to forward the authentication requests between authentication (RADIUS) server and client. Allowing or denying the requests decides if the client can connect to a LAN/WAN or not.

### 802.1X Setting

IEEE 802.1X is the protocol that performing authentication to obtain access to IEEE 802 LANs. It is port-base network access control. With the function, WoMaster switch could control which connection is available or not.



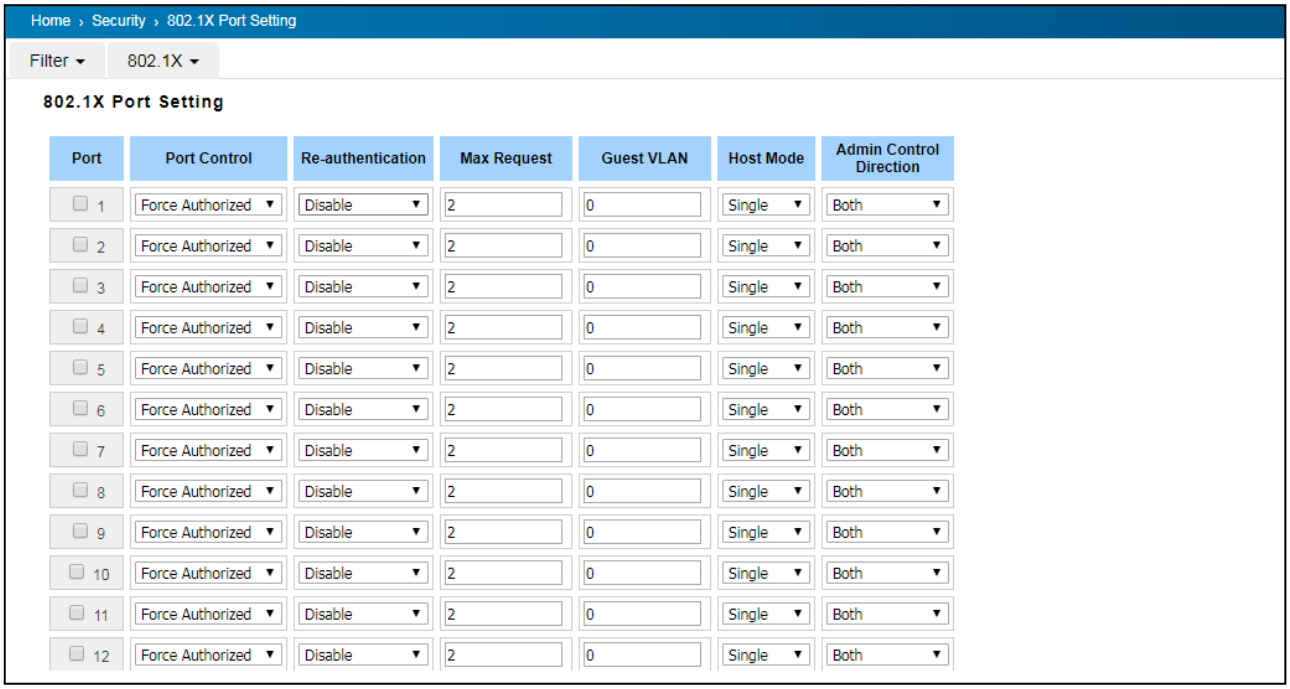

The description of the columns is as below:

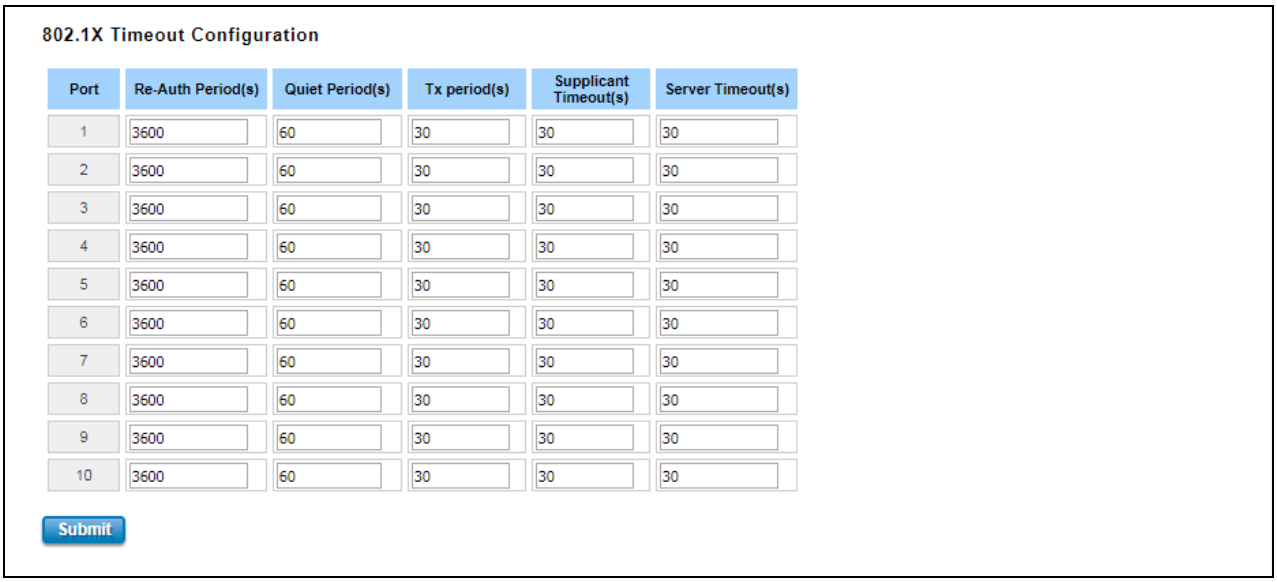
| TERMS | DESCRIPTION |
|---|---|
| **System Auth Control** | To enable or disable the 802.1X authentication. |
| **Authentication Method** | Radius is an authentication server that provide key for authentication, with this |

| | |
|---|---|
| | method, user must connect switch to server. If user selects Local for the authentication method, switch use the local user data base which can be created in this page for authentication. |
| **Radius Server IP** | The IP address of Radius server |
| **Shared Key** | It is the password for communicate between switch and Radius Server. |
| **Server Port** | UDP port of Radius server. |
| **Accounting Port** | Port for packets that contain the information of account login or logout. |
| **Secondary Radius Server IP** | Secondary Radius Server could be set in case of the primary radius server down. |
| **802.1X Local User** | Here User can add Account/Password for local authentication. |
| **802.1X Local User List** | This is a list shows the account information; User also can remove selected account. |

## 802.1X Port Setting

After the configuration of Radius Server or Local user list, user also need configure the authentication mode, authentication behavior, applied VLAN for each port and permitted communication. The following information will explain the port configuration.






The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Port control** | Force Authorized means this port is authorized; the data is free to in/out. Force unauthorized just opposite, the port is blocked. If users want to control this port with Radius Server, please select Auto for port control. |
| **Re-authentication** | **Default: 3600 seconds**<br>If enable this field, switch will ask client to re-authenticate. |
| **Max Request** | The maximum times that the switch allow client request. |
| **Guest VLAN** | 0 to 4094 is available for this field. If this field is set to 0, that means the port is blocked after authentication fail. Otherwise, the port will be set to Guest VLAN. |
| **Host Mode** | If there are more than one device connected to this port, set the Host Mode to single means only the first PC authenticate success can access this port. If this port is set to multi, all the devices can access this port once any one of them pass the authentication. |
| **Admin Control Direction** | Determined devices can end data out only or both send and receive. |
| **Re-Auth Period** | Control the Re-authentication time interval, 1~65535 are available. |
| **Quiet Period** | When authentication failed, Switch will wait for a period and try to communicate with radius server again. |
| **Tx period** | The time interval of authentication request. |
| **Supplicant Timeout** | The timeout for the client authenticating |
| **Sever Timeout** | The timeout for server response for authenticating. |

Once User finishes configuring the settings, click on **Submit** to apply User configuration.

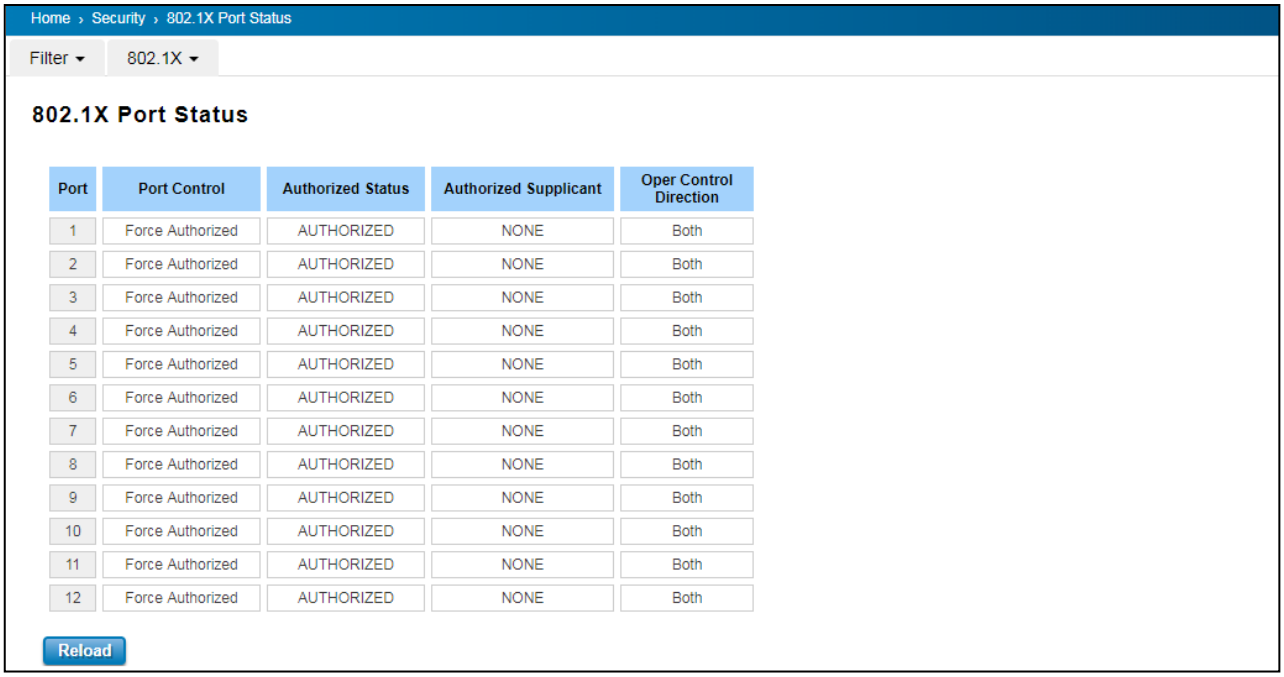
Click **Initialize Selected** to set the authorize state of selected port to initialize status.

Click **Re-authenticate Selected** to send EAP Request to supplicant to request re-authentication.

Click **Default Selected** to reset the configurable 802.1X parameters of selected port to the default values.

## 802.1X Port Status

User can observe the port status for Port control, Authorized Status, Authorized Supplicant and Open Control Direction from each port.



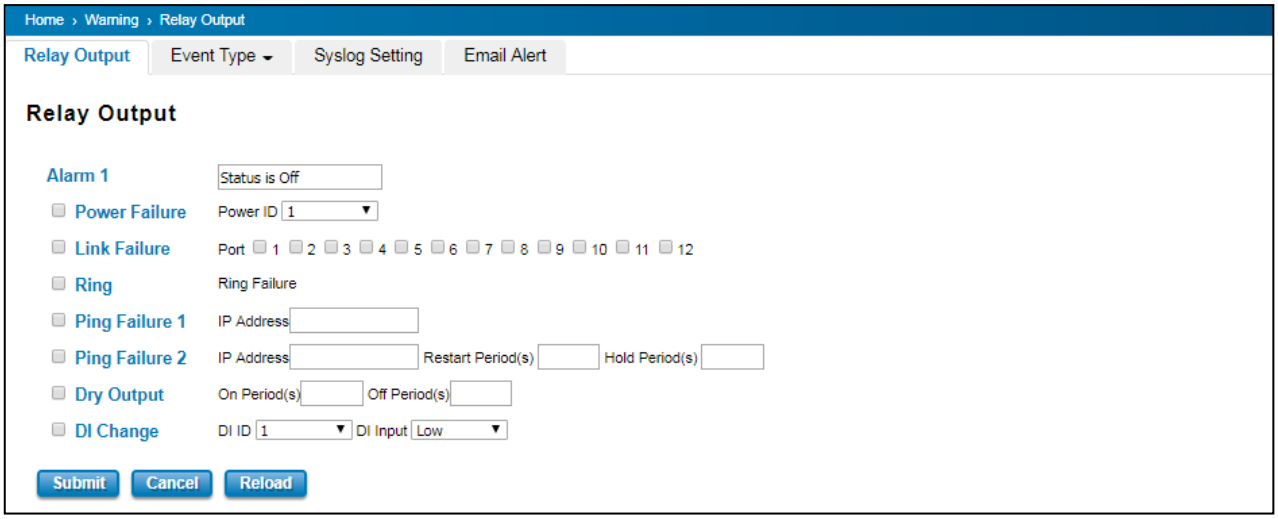
## 3.10 WARNING

The switch provides several types of Warning feature for remote monitoring of end devices status or network changes.

### 3.10.1 RELAY OUTPUT

WoMaster switch provides 1 alarm relay output, also known as Digital Output. These settings in Relay Output section control the events that will trigger the alarm output. The OK discrete output is on during normal conditions and turned off in the event of an alarm condition. The relay output supports multiple event relay binding function.

The Relay Output configuration interface has shown as below:




The condition or term described as following table.

| TERMS | CONDITION | DESCRIPTION |
|---|---|---|
| **Power Failure** | Power ID 1<br>Power ID 2<br>Any | Detect power input status. If one of condition occurred, relay triggered. |
| **Link Failure** | Port number | Monitoring port link down event |
| **Ring** | Ring failure | If ring topology changed |
| **Ping Failure 1** | **IP Address:** remote device's IP address. | If target IP does not reply ping request, then relay active. |
| **Ping Failure 2** | **IP address:** remote device's address<br>**Restart Period**: duration of output open.<br>**Hold Period:** duration of Ping hold time. | Ping target device and trigger relay to emulate power reset for remote device, if remote system crash.<br>Note: once perform Ping Restart; the relay output will form a short circuit. |
| **Dry Output** | **On period:** duration of relay output short (close). | Relay continuous perform On/Off behavior with different duration. |

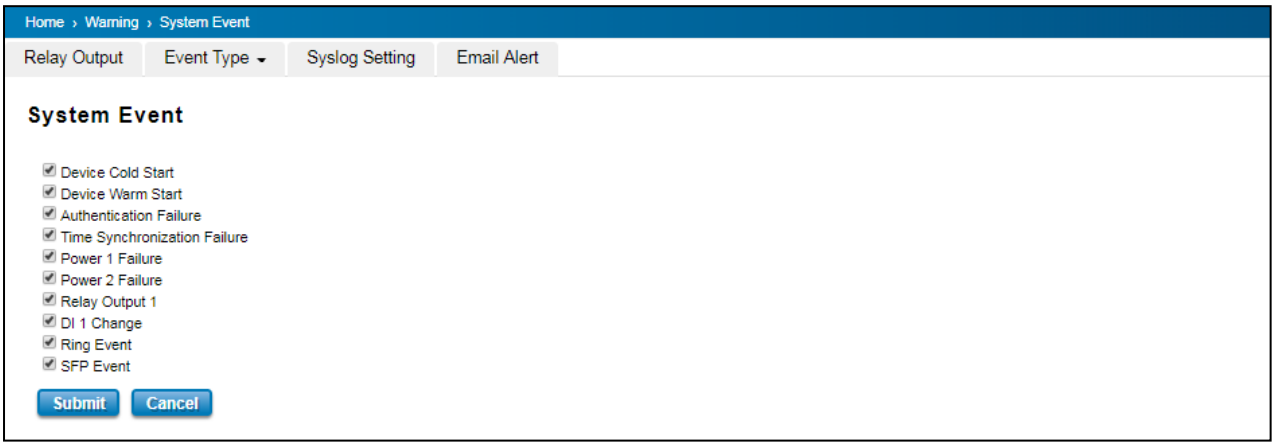
| | | |
|---|---|---|
| | **Off period**: duration of relay output open. | |
| **DI Change** | DI number<br>(the switch supports 1 DI) | Relay trigger when DI states change to Hi or Low |

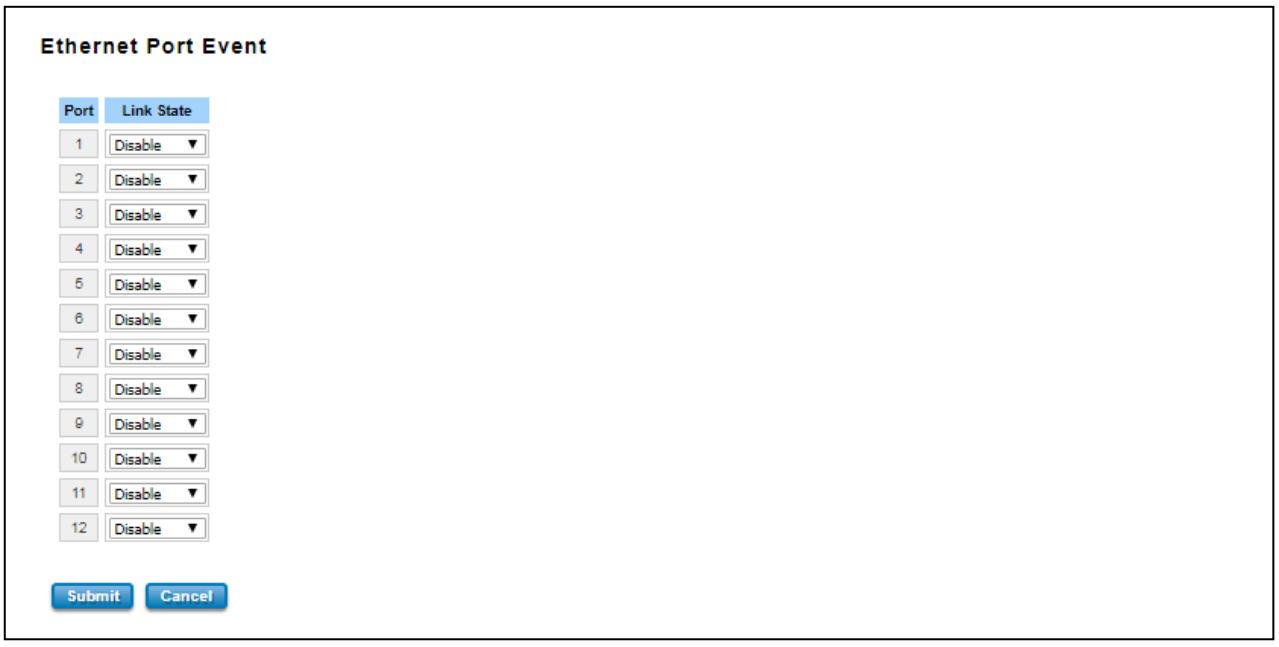
The relay supports multiple event trigger function; click and select type of event and setting the detail information, and then clicks **Submit** to activate the relay alarm function.

## 3.10.2 EVENT TYPE

Event Types can be divided into two basic groups: System Event and Port Event. System Event are related to the overall function of the switch, whereas Port Event related to the activity of specific ports

Once User finishes configuring the settings, click on Submit to apply User configuration.



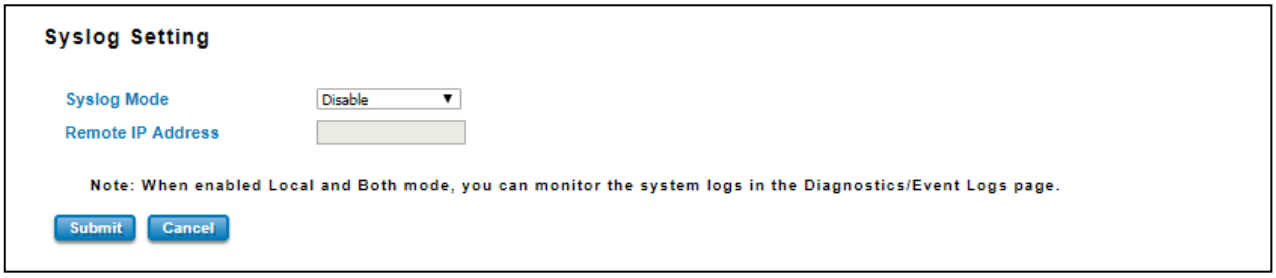



The description of the columns is as below:

| System Event Selection | Warning Event is sent when….. |
|---|---|
| Device Cold Start | Power is cut off and then reconnected. |
| Device Warm Start | Reboot the device by CLI or Web UI. |
| Authentication failure | An incorrect password, SNMP Community String is entered. |
| Time Synchronize Failure | Accessing to NTP Server is failure. |
| Power 1/ 2 Failure | The power input is failure. |
| Relay Output 1 | The Digital Output is on. |
| DI 1 Change | The Digital Input change |
| Ring Event | Ring Status has changed or backup path is activated. |
| SFP Event | The SFP transceiver's state is abnormal. |
| **Port Event** | **Warning Event is sent when…..** |
| Up | The port is connected to another device |
| Down | The port is disconnected (e.g. the cable is pulled out, or the opposing devices turns down) |
| Both | The link status changed. |

## 3.10.3 SYSLOG SETTING

System Log can provide the switch events history by locally or remotely monitor. There are 3 System Log modes provided by the switch, local mode, remote mode and both.




**Local Mode**: In this mode, the device will print the selected events in the Event Selection page to System Log table of the switch.

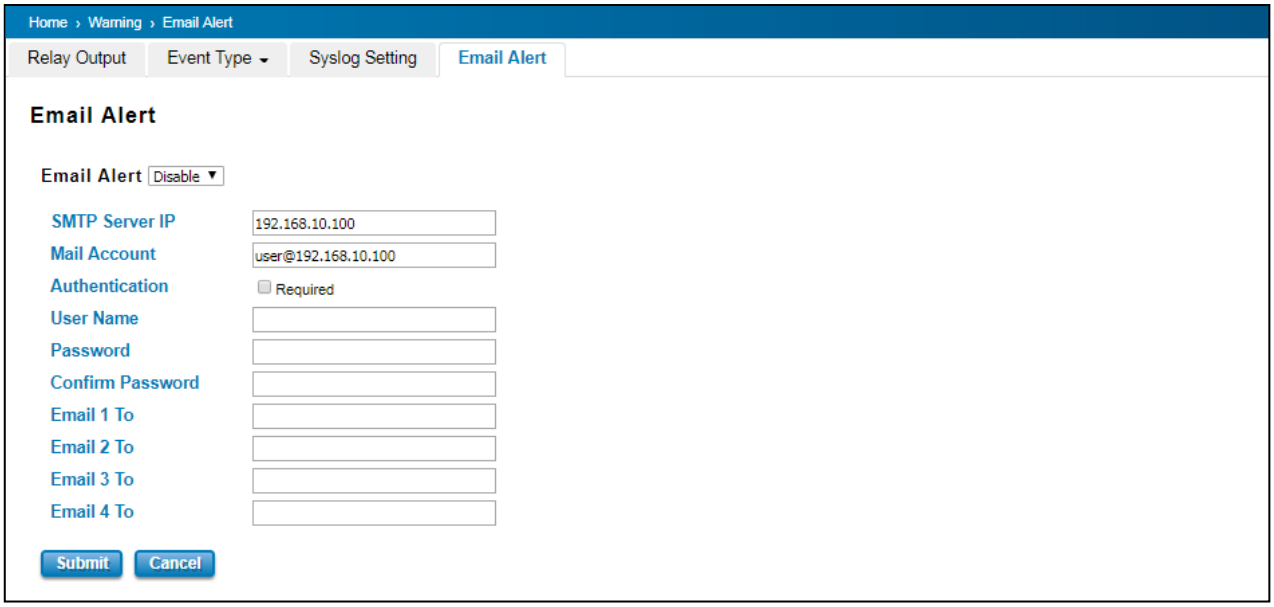
**Remote Mode**: In this mode, User should assign the IP address of the System Log server. Then the selected occurred events will be sent to System Log server User assigned.

**Both:** Above 2 modes can be enabled at the same time.

Once User finishes configuring the settings, click on **Submit** to apply User configuration.

## 3.10.4 EMAIL ALERT

WoMaster switch provides the option of automatically sending an e-mail if an alarm event occurs (for example to the network administrator). The e-mail contains the identification of the sending device, a description of the cause of the alarm in plain language, and a time stamp. This allows centralized network monitoring to be set up for networks with few nodes based on an e-mail system. On this page, you can configure SMTP servers and the four corresponding e-mail addresses.




The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Email Alert** | Enable or Disable the Email Alert function. |
| **SMTP Server IP** | Enter the IP address of the email Server |
| **Mail Account** | Enter the email Server address |
| **Authentication** | Click on check box to enable password |
| **User Name** | Enter email Account name (Max.40 characters) |
| **Password** | Enter the password of the email account |
| **Confirm Password** | Re-type the password of the email account |
| **User can set up to 4 email addresses to receive email alarm from the switch** | |
| **Email 1 To** | The first email address to receive email alert from the switch (Max. 40 characters) |
| **Email 2 To** | The second email address to receive email alert from the switch (Max. 40 characters) |
| **Email 3 To** | The third email address to receive email alert from the switch (Max. 40 characters) |
| **Email 4 To** | The fourth email address to receive email alert from the switch (Max. 40 characters) |

Once User finishes configuring the settings, click on **Submit** to apply User configuration.

# 3.11 DIAGNOSTICS

WoMaster Switch provides several types of features for User to monitor the status of the switch or diagnostic for User to check the problem when encountering problems related to the switch.

Following commands are included in this group:

3.11.1 LLDP Setting

3.11.2 MAC Table

3.11.3 Port Statistics

3.11.4 Port Mirror

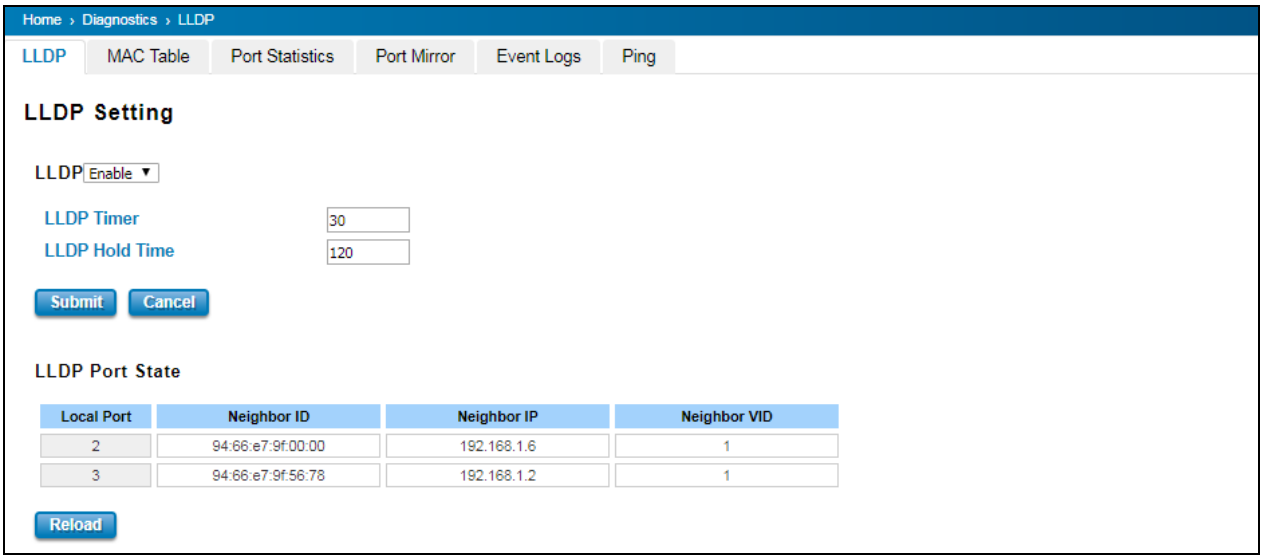
3.11.5 Event Log

3.11.6 Ping

## 3.11.1 LLDP SETTING

LLDP is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device, such as a WoMaster managed switch, to periodically send its system and configuration information to its neighbors. Because of this, all LLDP devices are kept informed of each other's status and configuration, and with SNMP. From the switch's web interface, User can enable or disable LLDP, and User can view each switch's neighbor-list, which is reported by its network neighbors. Most importantly, enabling the LLDP function allows to automatically display the neighbor ID and IP leant from the connected devices.

The configuration and settings explain as following.




| TERMS | DESCRIPTION |
|---|---|
| **LLDP** | Select to enable/disable LLDP function. |
| **LLDP Timer** | **Default: 30 seconds**<br>The interval time of each LLDP and counts in second; the valid number is from 5 to 254. |
| **LLDP Hold time** | **Default: 120 seconds** |

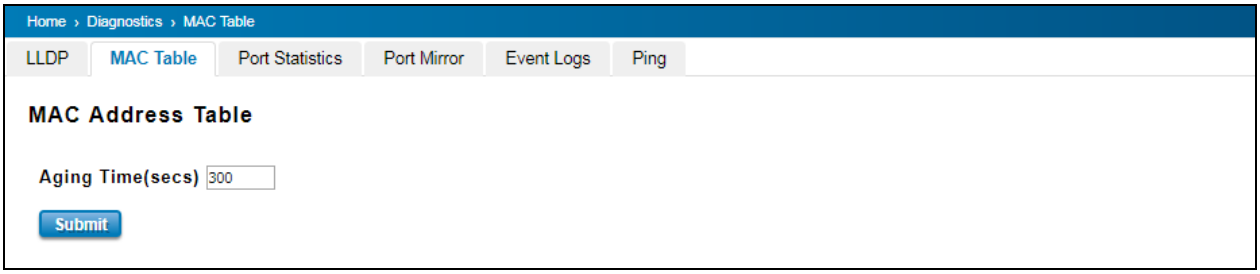
| | |
|---|---|
| | The TTL (Time To Live) timer. The LLDP state will be expired once the LLDP is not received by the hold time. |
| **Local port** | The current port number that linked with neighbor network device. |
| **Neighbor ID** | The MAC address of neighbor device on the same network segment. |
| **Neighbor IP** | The IP address of neighbor device on the same network segment. |
| **Neighbor VID** | The VLAN ID of neighbor device on the same network segment. |

## 3.11.2 MAC TABLE

In this page, users can change the Aging time, add Static Unicast MAC Address, monitor the MAC address or sort them by different packet types and ports. Click on **Submit** to change the value.

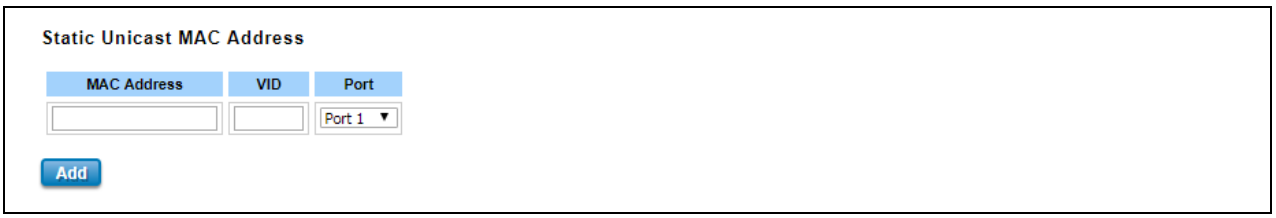
### Aging Time (Sec)

Each switch Fabric has limit size to write the learnt MAC address. To save more entries for new MAC address, the switch Fabric will age out non-used MAC address entry per Aging Time timeout. The default Aging Time is 300 seconds. The Aging Time can be modified in this page.



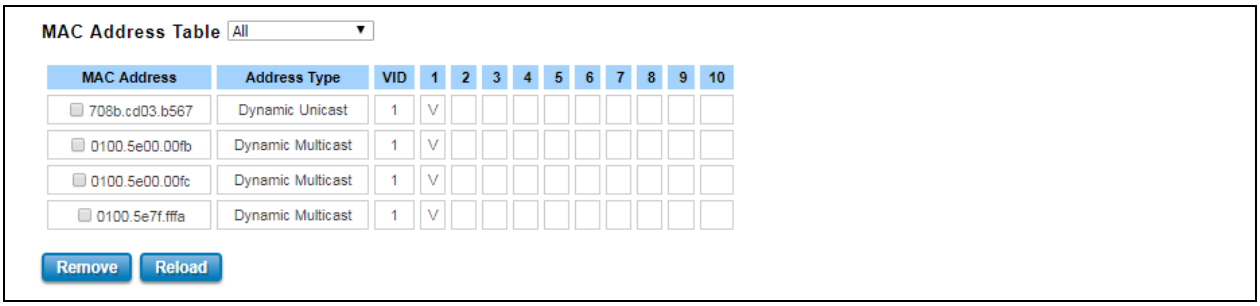

### Static Unicast MAC Address

In some applications, users may need to type in the static Unicast MAC address to its MAC address table. In this page, User can type MAC Address (format: xxxx.xxxx.xxxx), select its VID and Port ID, and then click on **Add** to add it to MAC Address table.



## MAC Address Table

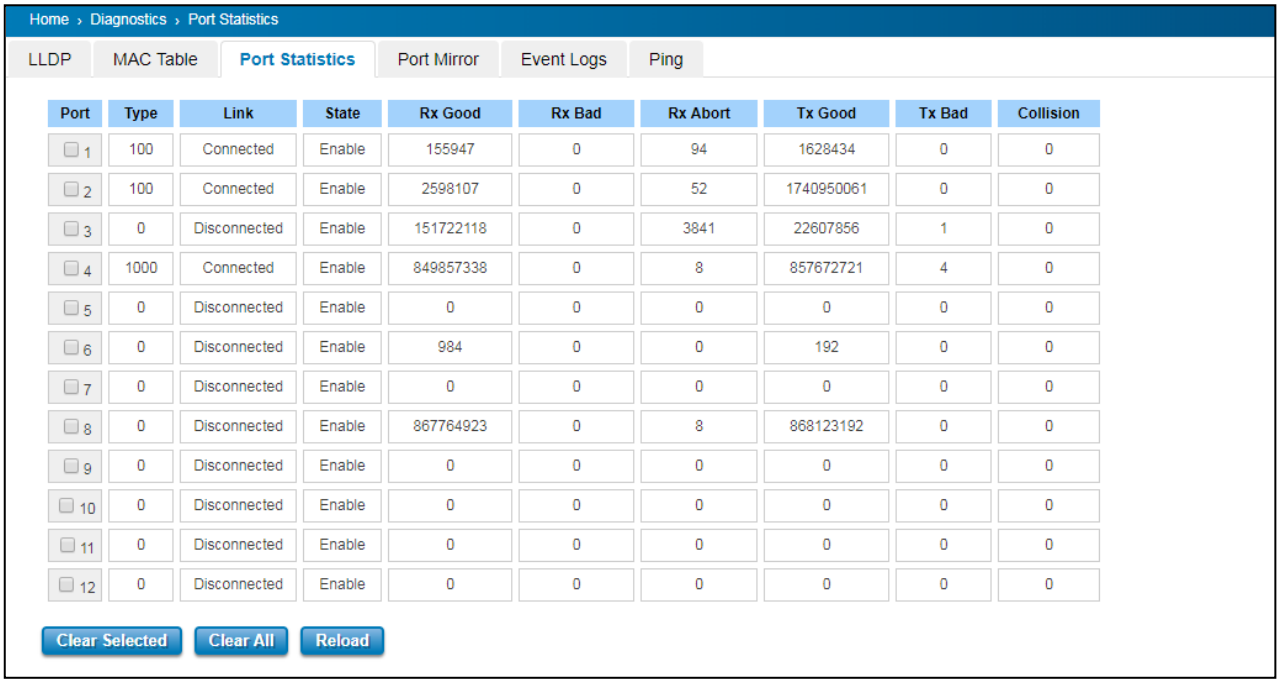
At this table, all the MAC Addresses learnt by the switch will be shown here. Use the MAC address table to ensure the port security. The MAC Address Table can be displayed based on the MAC Address Type and based on the Port.




Click on **Remove** to remove the selected static Unicast/Multicast MAC address. Click on **Reload** to refresh the table. New learnt Unicast/Multicast MAC address will be updated to MAC address table.

## 3.11.3 PORT STATISTICS

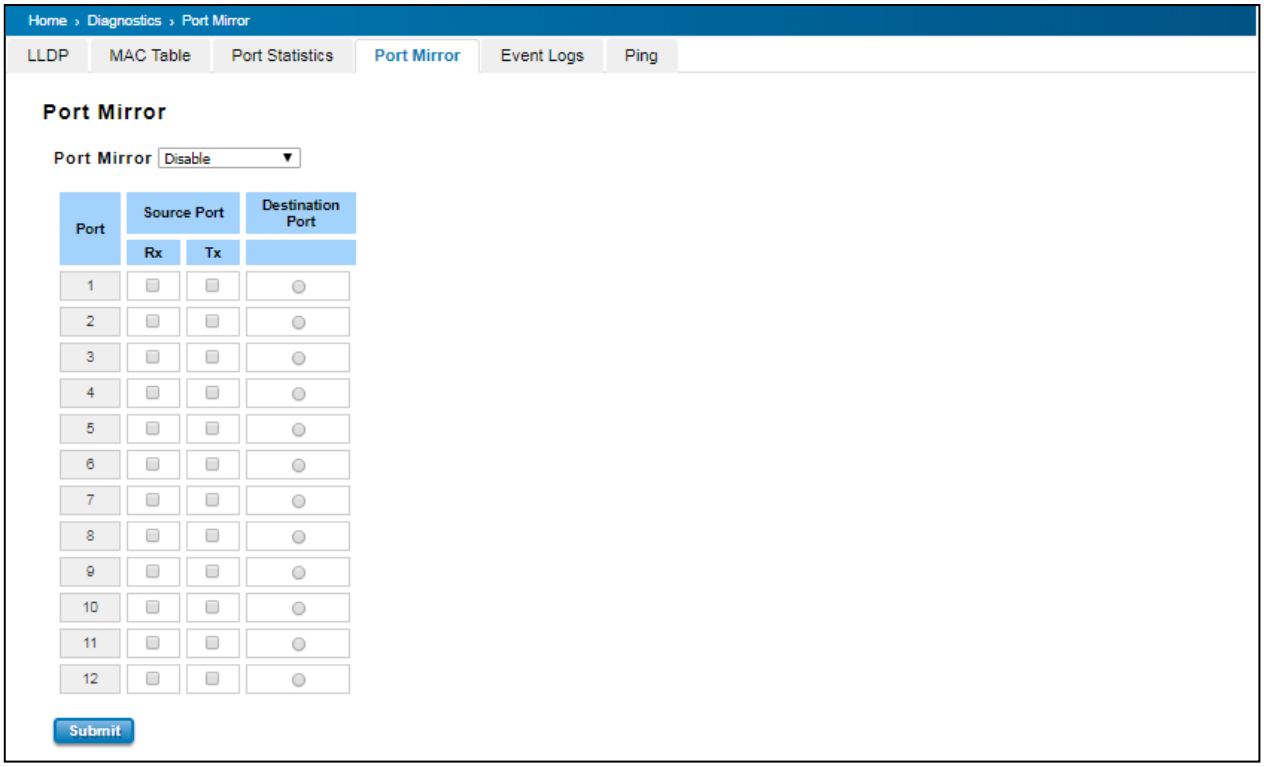
This page displays the number of error packets that is received and sent from the port. This level of detail is not available from the Dashboard graphs. The number of error packets can mean a duplex mismatch, incompatibilities with the port and its attached device, or faulty cables or attached devices. Any of these problems can cause slow network performance, data loss, or lack of connectivity. The statistics that can be viewed include Link Type, Link State, Rx Good, Rx Bad, Rx Abort, Tx Good, Tx Bad and Collision.




Click on **Clear Selected** to reinitialize the counts of the selected ports, and **Clear All** to reinitialize the counts of all ports. Click on **Reload** to refresh the counts.

## 3.11.4 PORT MIRROR

Port mirroring is a tool that allows User to monitor data that being transmitted through a specific port. User can use this feature for diagnostics, debugging, and any kind of analysis. This is done by setting up another port (the mirror port) to receive the same data being transmitted from, or both to and from, the port under observation. Using a mirror port allows the network administrator to sniff the observed port to keep tabs on network activity. Any traffic will be duplicated at the Destination Port. All of the traffics at the Destination port can be analyzed using a monitoring tool.



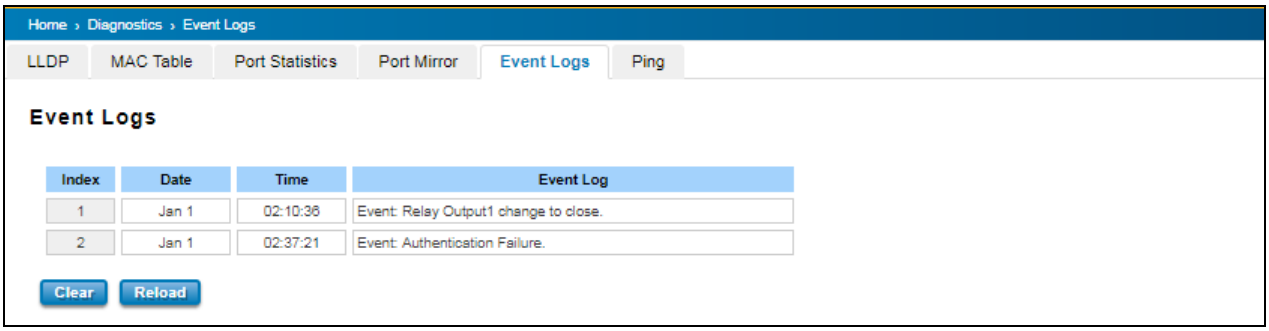

The configuration and settings explain as following.

| TERMS | DESCRIPTION |
|---|---|
| **Port Mirror** | Select Enable/Disable to enable/disable Port Mirror. |
| **Source Port** | These are the ports that User wants to monitor. The traffic of all source ports will be duplicated to destination ports. User can choose a single port, or multiple ports. Click on checkbox of the Port ID, RX, Tx or Both to select the source ports. |
| **Destination Port** | User can analyze the traffic of all the monitored ports at this port without affecting the flow of traffic on the port being monitored. Only one RX/TX of the destination port can be selected. |

Once User finishes configuring the settings, click on **Submit** to apply the settings.

## 3.11.5 EVENT LOGS

This event logs page will show and record the system events log.



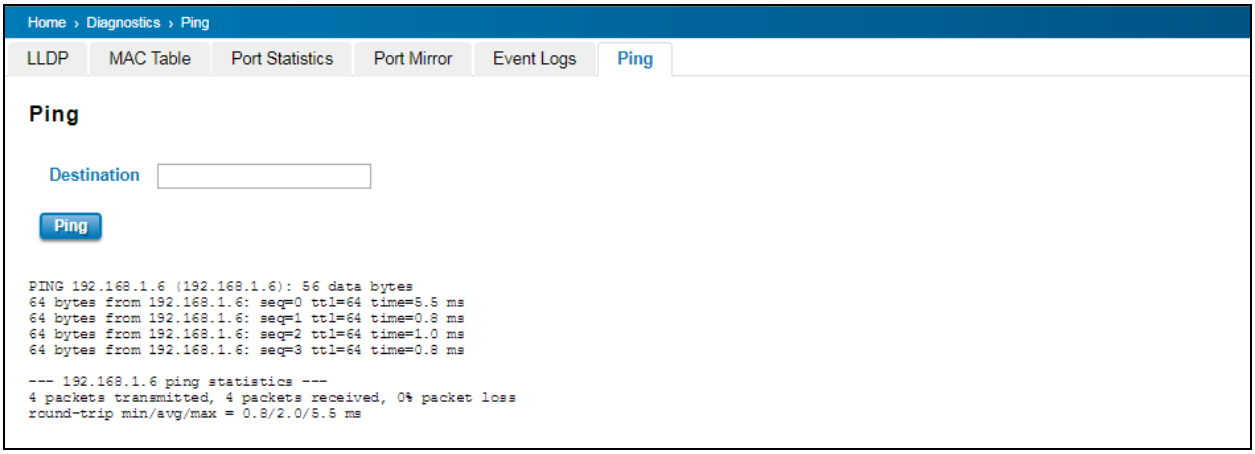

Click on **Clear** to clear the entries. Click on **Reload** to refresh the table.

The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **Index** | Event index assigned to identify the event sequence. |
| **Date** | The date is updated based on how the current date is set in the Basic Setting page. |
| **Time** | The time is updated based on how the current time is set in the Basic Setting page. |
| **Event Log** | The occurred events. |

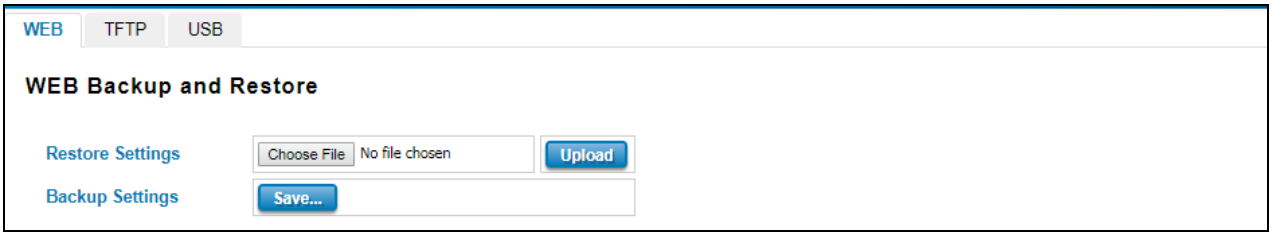
## 3.11.6 PING

WoMaster' provides **Ping** utility in the management interface, the function is to give users a simple but powerful tool for troubleshooting network problems and check that the remote device is still alive or not. Type **Destination** IP address of the target device and click on **Ping** to start the ping.



## 3.12 BACKUP AND RESTORE

User can use WoMaster' Backup and Restore configuration to save and load configuration through the switch. There are 3 modes for users to backup/restore the configuration file.




**Web** mode: In this mode, the switch acts as the file server. Users can browse the target folder and then type the file name to back-up the configuration. Browse the target folder and select existed configuration file to restore the configuration back to the switch. This mode is only provided by Web UI while CLI is not supported.


**TFTP Server** mode: In this mode, the switch acts as TFTP client. Before do so, make sure that TFTP server is ready. Then please type the IP address of TFTP Server and Backup configuration file name. This mode can be used in both CLI and Web UI.

The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **TFTP Server IP** | User needs to key in the IP address of TFTP Server here. |
| **File Name** | Type the correct file name of the configuration file. |
| **Configuration File (*.conf*)** | The configuration file of the switch is a pure text file. User can open it by word/txt read file. User can also modify the file, add/remove the configuration settings, and then restore back to the switch. |
| **Action** | User can choose to Load or Save configuration |


**USB** mode: this mode has two functions, Load Setting from File and Save Setting to USB. Load Setting from File, make sure that the USB has been plugged on and it has the *.conf* file which is the backup files. After plugged on the USB, the USB port will directly read the USB and then the backup file would be shown up by clicking the arrow down. Then click **restore**. At the Save Setting to USB part, all of the configuration settings would be saved to the USB, with *.conf*

as the file type by clicking the **Save to USB**.

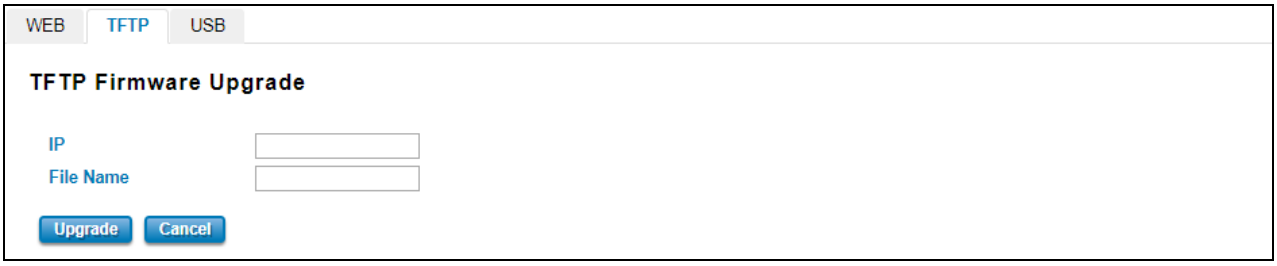
## 3.13 FIRMWARE UPGRADE

WoMaster provides the latest firmware online at www.womaster.eu. The new firmware may include new features, bug fixes or other software changes. WoMaster also provide the release notes for the update as well. For technical viewpoint, WoMaster suggests user uses the latest firmware before installing the switch to the customer site.

> **NOTE:** Note that the system will be automatically rebooted after User finished upgrading the new firmware. Please remind the attached network users before User performs this function.

There are 3 modes for users to backup/restore the configuration file, Local File mode, USB and TFTP Server mode.


**Web** mode: The switch acts as the file server. Users can browse the target folder and then type the file name to back-up the configuration. Users also can browse the target folder and select the existed upgrade file. This mode is only provided by Web UI while CLI is not supported.




**TFTP Server** mode: In this mode, the switch acts as the TFTP client. Before do so, make sure that TFTP server is ready. Then please type the IP address of TFTP Server and Backup configuration file name. This mode can be used in both CLI and Web UI.

The description of the columns is as below:

| TERMS | DESCRIPTION |
|---|---|
| **IP** | User need to key in the IP address of TFTP Server here. |
| **File Name** | Type the correct file name of the configuration file. |

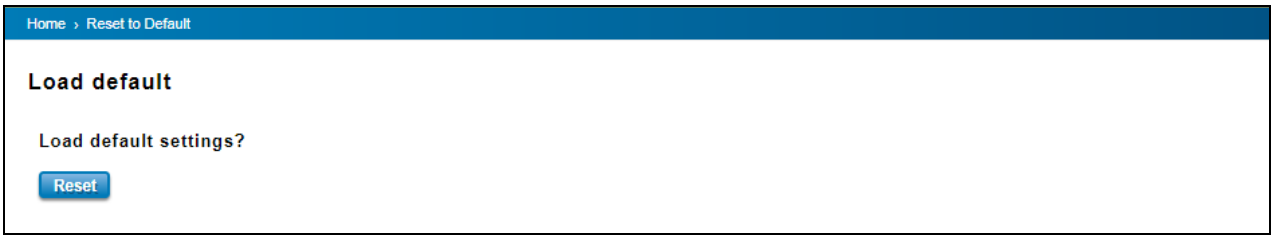
The UI also shows User the current firmware version and built date of current firmware upgrade. Please check the version number after the switch is rebooted. Input the TFTP Server IP Address and the specific File Name. Then click on **Upgrade** to start the process. After finishing transmitting the firmware, the system will copy the firmware file and replace the firmware in the flash.


**USB** mode: plugged in the USB device with the firmware file, then it will directly show the new firmware file on the list by click the arrow down. Then click **Upgrade**.

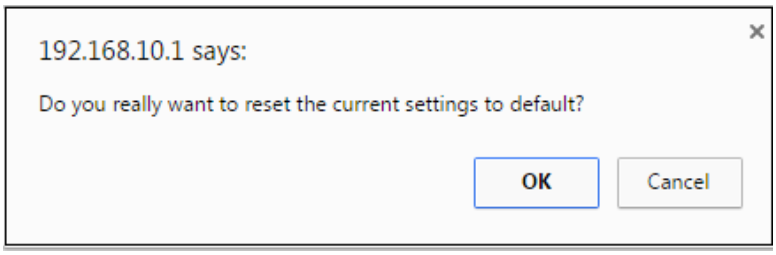
## 3.14 RESET TO DEFAULTS

This function provides users with a quick way of restoring the WoMaster switch's configuration to factory defaults. The function is available in the serial, Telnet, and web consoles.

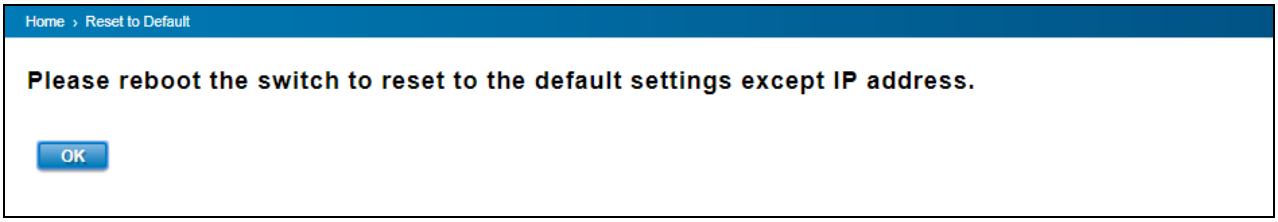
### Factory Default main screen




Pop-up message screen to show User that have done the command. Click on **OK** to close the screen.

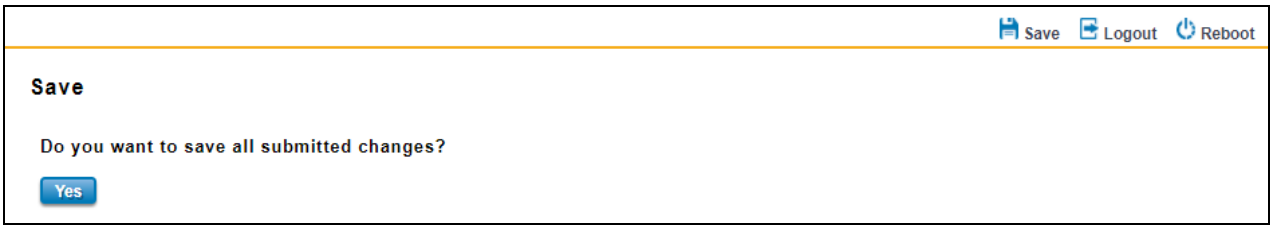



Then please go to **Reboot** page to reboot the switch. Click **OK.** The system will auto reboot the device.



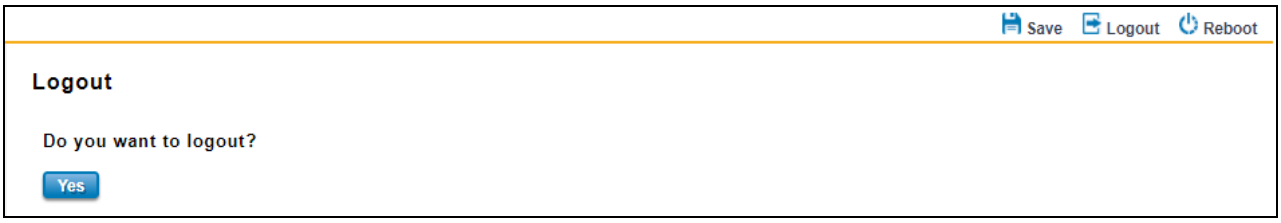
## 3.15 SAVE

**Save** option allows user to save any configuration. Powering off the switch without clicking on **Save** will cause loss of new settings. After selecting **Save**, click on **Yes** to save new configuration.




## 3.16 LOGOUT

There are 2 logout methods. If user doesn't input any command within 30 seconds, the web connection will be logged out. The Logout command allows user to manually logout the web connection. Click on **Yes** to logout.

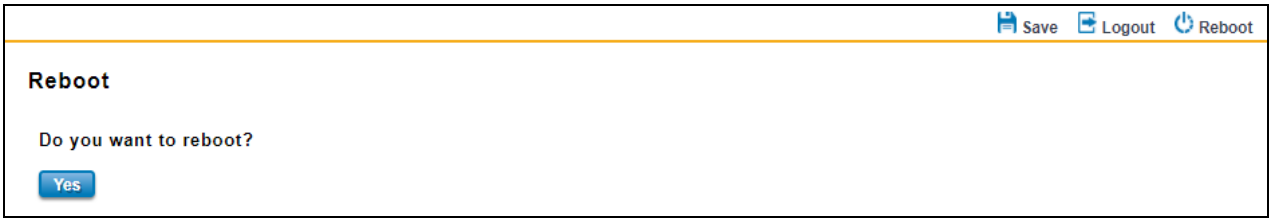



## 3.17 REBOOT

System Reboot allows user to reboot the device. Some of the feature changes require user to reboot the system. Click on **Reboot** to reboot device.

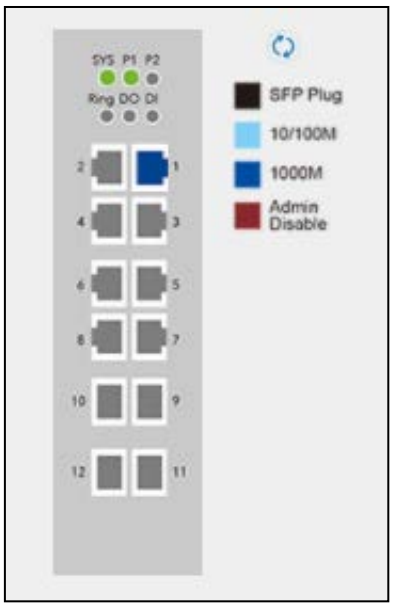
> **NOTE:** Remember to click on Save button to save configuration settings. Otherwise, the settings user made will be gone when the switch is powered off.

Reboot main screen, to do confirmation request. Click **Yes**, then the switch will reboot immediately.



## 3.18 FRONT PANEL

Front Panel commands allow user to see LED status of the switch. User can see LED and link status of the Power, DO, R.M. and Ports. Front panel interface, can be seen on the web consoles. Shown as below.




The description of the Front Panel is as below:

| Feature | LED On | LED off |
|---|---|---|
| **P1/P2** | Green on: Power is on | No power |
| **SYS** | Green on: System ready | System not ready |
| **Ring** | Green on: Ring is active<br>Amber on: Ring status is abnormal | Ring is inactive |
| **DO** | Red on: alarm relay active and contacts is short. | Red off: relay output contact is open. |
| **DI** | Green on: Digital Input is active. | Green off: Digital Input contact is not available. |
| **10/100M** | Light Blue on: Port is linked | Port link is down |
| **1000M** | Dark Blue on: The port is linked at 1000Mbps speed. | Not available |
| **Admin Disable** | Maroon on: Port disable | Not available |
| **PoE (Poe Models Only)** | Yellow on: powering | Power output over current or cable short |

# 4. SPECIFICATIONS

| Technology | DP412 / DS412 |
|---|---|
| **Standard** | IEEE 802.3af/at Power over Ethernet<br>IEEE 802.3 10Base-T Ethernet<br>IEEE 802.3u 100Base-TX Fast Ethernet<br>IEEE 802.3ab 1000Base-T Gigabit Ethernet copper<br>IEEE 802.3u 100Base-FX Fast Ethernet Fiber<br>IEEE 802.3z Gigabit Ethernet Fiber<br>IEEE 802.3x Flow Control and back-pressure<br>IEEE 802.1AB Link Layer Discovery Protocol (LLDP)<br>IEEE 802.1p Class of Service (CoS)<br>IEEE 802.1Q VLAN and GVRP<br>ITU-T G.8032 Ethernet ring protection switching(ERPS)<br>IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP)<br>IEEE 802.1Q-2005 Multiple Spanning Tree Protocol (MSTP)<br>IEEE 801.1AX/802.3ad Link Aggregation Control Protocol (LACP)<br>IEEE 802.1X Port based Network Access Protocol<br>IEEE 1588 Precision Time Protocol v1/v2<br>RFC791, RFC792, and RFC894 |
| **Performance** | |
| **Switch Technology** | Store and Forward Technology with non-blocking Switch Fabric: 24Gbps and forwarding rate: 17.8Mpps |
| **Number of MAC Address** | 16K |
| **Packet Buffer Memory** | 1.5MBytes |
| **Jumbo Frame** | 9216 Bytes |
| **Transfer performance** | 10Base-TX: 14,880pps, 100Base-TX: 148,800pps, 1000Base-TX/FX: 1,488,100pps |
| **VLAN** | 256 VLANs |
| **VLAN ID** | 1~4094 |
| **Class of Service** | 8 Priority Queues per Port |
| **Watchdog** | Hardware-based 10 seconds timer |
| **PoE (DP412)** | |
| **Power forwarding mode** | Alternative A |
| **PoE Power Budget** | PoE: Max.240W@75°C<br>Per Port: Max. 30W |
| **PoE Mode** | IEEE 802.3af/at |

| | |
|---|---|
| **Management** | System/Port Power Budget Control, PoE Scheduling, PD Alive Check, PoE Status |
| **Software** | |
| **Management Interface** | CGI WebGUI, Command Line Interface (CLI), Telnet, SNMP |
| **Time Management** | NTP, IEEE 1588 Precision Time Protocol v1/v2 |
| **Network Management** | IPv4/IPv6, SNMP v1/v2c/v3/Trap, MIBs, RMON, LLDP, DHCP server/client/Option 82, TFTP, System Log, SMTP |
| **Traffic Management** | Flow Control, Port Trunk/801.1AX/802.3ad LACP, VLAN, Private VLAN, IEEE 802.1v*, GVRP, GMRP, QinQ, QoS, RFC 2474 DiffServ, Rate Control, Storm Control, Port Mirror, IGMP Snooping v1/v2/v3, IGMP Snooping Fast-Leave/Immediate-Leave, IGMP Query, IGMP Query Solicitation/Request*, MLDv1/v2 Snooping* |
| **Security** | IEEE 802.1X/RADIUS, Private VLAN, ACL(MAC/IP filter), TLS v1.2, HTTPs/SSH |
| **Redundancy** | Rapid Spanning Tree Protocol (RSTP)/Multiple Spanning Tree Protocol (MSTP) ITU-T G.8032 v1/v2 Ethernet Ring Protection Switching (ERPS) |