WoMaster

COVER

User Manual

DS306

Industrial 6-port Managed Ethernet Switch

May,03.2018 V.1

www.womaster.eu

WoMaster

DS306 Industrial 6-port Managed Ethernet switch

User Manual

Copyright Notice

About This Manual

This user manual is intended to guide a professional installer to install and to configure the DS306 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

COVER......1

TABLE OF CONTENTS 3

1. INTRODUCTION......5

1.1 OVERVIEW 5

1.2 MAJOR FEATURES......5

2. HARDWARE INSTALLATION......6

2.1 HARDWARE DIMENSION 6

2.2 WIRING THE POWER INPUTS 7

2.3 WIRING THE ALARM RELAY OUTPUT (DO) 7

2.4 CONNECTING THE GROUDING SCREW......8

2.5 DIN RAIL MOUNTING 8

2.6 WIRING THE FIBER CONNECTOR (ST/SC) 9

3. WEB MANAGEMENT CONFIGURATION......10

3.1 SYSTEM......12

3.1.1 INFORMATION 12

3.1.2 USER ACCOUNT......13

3.1.3 IP SETTING 14

3.1.4 DATE AND TIME 15

3.1.5 DHCP SERVER......16

3.2 ETHERNET PORT 18

3.2.1 PORT STATUS......18

3.2.2 PORT SETTING......19

3.2.3 VLAN SETTING......20

3.2.4 RATE CONTROL 22

3.3 REDUNDANCY 23

3.3.1 RSTP SETTINGS......23

3.3.2 ERPS SETTINGS......26

3.3.2.1 ERPS SETTINGS 27

3.3.2.2 ERPS STATUS 29

3.4 QUALITY OF SERVICE (QOS) 31

3.4.1 QoS SETTING......31

3.4.2 CoS MAPPING 32

3.4.3 DSCP MAPPING......33

3.5 WARNING 34

3.5.1 EMAIL ALERT *34*

3.5.2 PING WATCHDOG *35*

3.5.3 SYSLOG SETTING *36*

3.5.4 RELAY OUTPUT *36*

3.5.5 EVENT TYPE *37*

3.5.6 SNMP *37*

3.5.6.1 SNMP SETTING 37

3.5.6.2 SNMP V3 40

3.6 DIAGNOSTICS 42

3.6.1 EVENT LOGS *42*

3.6.2 ARP TABLE *43*

3.6.3 PORT STATISTICS *43*

3.6.4 PORT MIRROR *44*

3.6.5 LLDP *45*

3.6.6 PING *46*

3.7 BACKUP AND RESTORE 46

3.8 FIRMWARE UPGRADE 47

3.9 RESET TO DEFAULTS 48

3.10 SAVE 49

3.11 LOGOUT 49

3.12 REBOOT 49

4. SPECIFICATIONS 50

1. INTRODUCTION

1.1 OVERVIEW

DS306 is WoMaster Industrial Layer 2 Managed Ethernet Switch that equipped with 4 Gigabit Ethernet port and 2 ST/SC fiber connectors. This managed switch also can be smartly configured by WoMaster advanced management utility, WebGUI, CLI, Telnet and SNMP V1/V2c/V3/trap. For the best traffic control, the switch management side features have been utilized: Flow Control, VLAN, Class of Service, QoS, Rate Control and Port Mirror.

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), ITU-T G.8032 v1/v2 Ethernet Ring Protection Switching (ERPS)**.** Provide sub-50ms protection and recovery switching for Ethernet traffic and can interoperate with 3rd party industrial switch and still remain fast recovery time. IEC 61000-6-2 / 61000-6-4 Heavy Industrial EMC certified design, rugged enclosure and -40~70°C wide operating temperature range, - all these features guarantee stable performance of DS306 for surveillance data transmission under vibration and shock in rolling stocks, traffic control systems and other harsh environments.

Excellent security features also provided, such as DHCP client, DHCP server, Management IP, SSH, SSL 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 DS306 Switch:

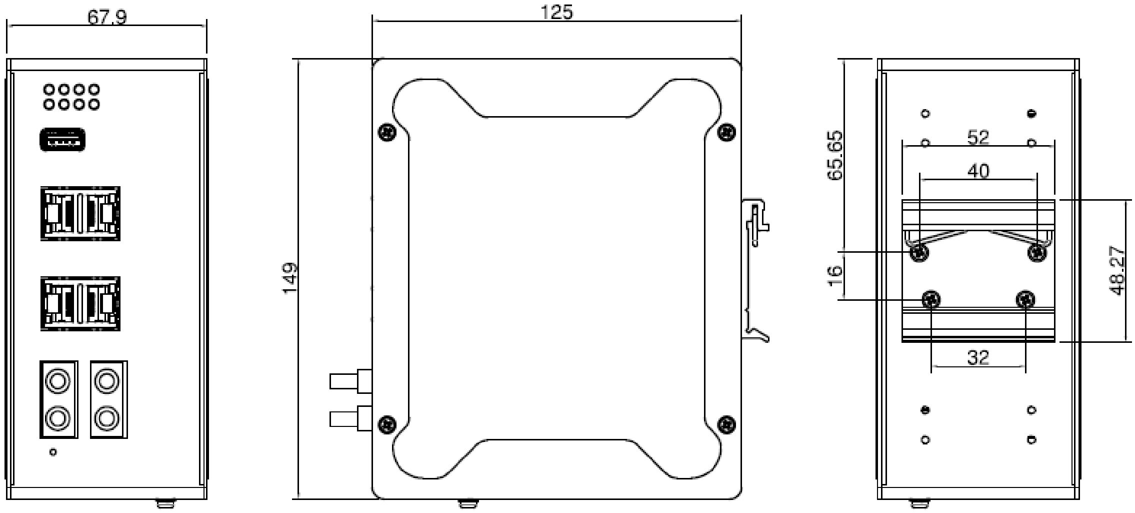
- 4 x 100/1000MBase-T ports and 2 x 100BaseFX ports, ST or SC connector
- All ports provide sub-50ms protection and recovery switching for Ethernet traffic.
- Rapid Spanning Tree Protocol (RSTP), ITU-T G.8032 v1/v2 Ethernet Ring Protection Switching (ERPS)
- Advanced management features: Flow Control/VLAN/QoS/Class of Service/Rate Control/Port Mirror/DHCP server, Client,
- Advanced Security system by Management IP, SSH and SSL
- 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, WebGUI, Telnet, SNMP for network Management
- Event relay output for enhanced alarm control
- Robust design protects from mechanical deformation
- Support redundant power input with reverse polarity protection
- Wide range operating temperature -40~70˚C
- IP30 ingress protection

2. HARDWARE INSTALLATION

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

2.1 HARDWARE DIMENSION

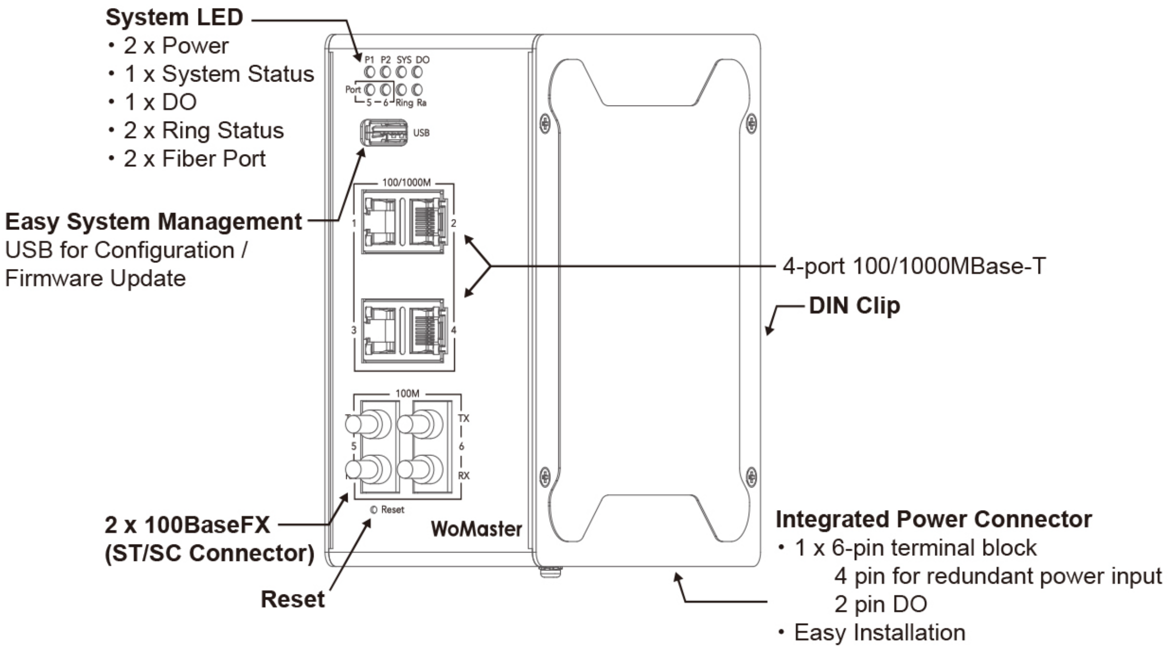
Dimensions of DS306: 67.9 x 149 x 125 mm (W x H x D) / without DIN Rail Clip



Front Panel Layout

The front panel from DS306 switches include 4 ports Gigabit Ethernet, 2 ST/SC fiber connectors, System LED, USB for configuration/firmware management, Reset button, 1 x 6-pin terminal block connector (4 pin for redundant power inputs and 2 pin for alarm relay output) and 1 chassis grounding screw.. On the rear side of switch there is DIN rail clip attached.

DS306



System LED
- 2 x Power
- 1 x System Status
- 1 x DO
- 2 x Ring Status
- 2 x Fiber Port

Easy System Management
USB for Configuration /
Firmware Update

4-port 100/1000MBase-T

DIN Clip

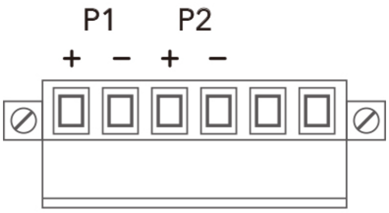
2 x 100BaseFX
(ST/SC Connector)

Reset

Integrated Power Connector
- 1 x 6-pin terminal block
  4 pin for redundant power input
  2 pin DO
- Easy Installation

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.



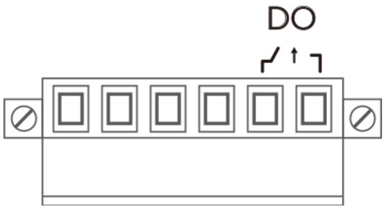
Wiring the Power Input

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 12VDC to DC 48V DC (recommended to use DC 24V 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)

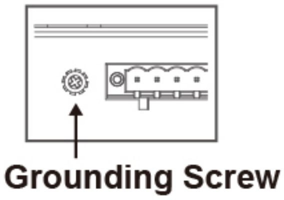
The relay output contacts are located on the front panel of the switch. The relay output consists of the 2-pin terminal block connector that used to detect user-configured events. The two wires attached to the fault contacts form a close circuit when a user-configured event is triggered. If a user-configured 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.

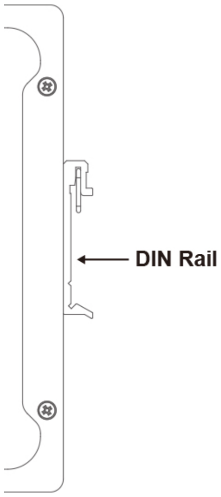
2.4 CONNECTING THE GROUDING SCREW

Grounding screw is located at the bottom 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.



2.5 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:

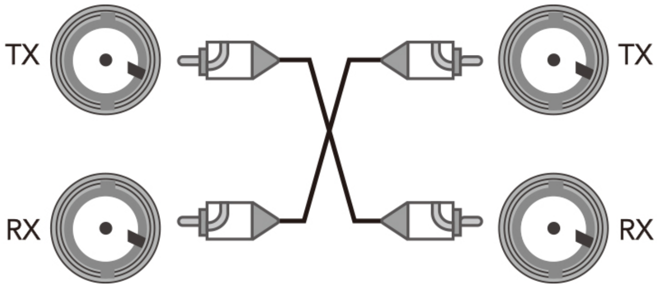
1. Insert the top side of DIN Rail track into the slot of DIN Rail clip.
2. Lightly clip the bottom of DIN-Rail to the track and make sure it attached well.
3. To remove the switch from the track, reverse the steps.

2.6 WIRING THE FIBER CONNECTOR (ST/SC)

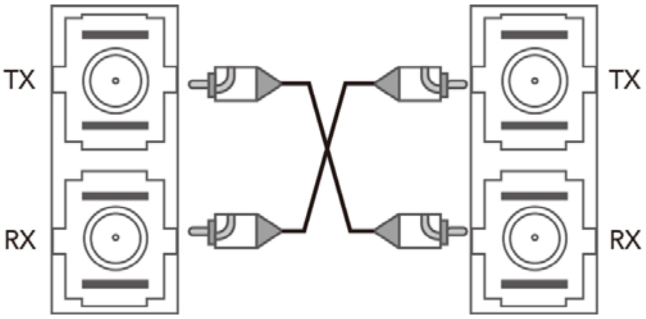
DS306 switches are equipped with fiber ports. To connect the fiber port, remember to link the Tx (transmit) port to the Rx (receive) port of the receiving device, and the Rx (receive) port to the Tx (transmit) port of transmitting device. The concept in cable installation for the SC/ST port and its cable is quite simple. For example, if you are connecting devices A and B; contrary to electrical signals, optical signals do not require a circuit in order to transmit data. Therefore, one of the optical lines is used to transmit data from device A to device B, and the other optical line is used transmit data from device B to device A. Connect the Tx port of device A to the Rx port of device B, and the Rx port of device A to the Tx port of device B.

WARNING: Be careful when connecting the fiber port, wrong connection will cause the fiber port not working properly.

Duplex ST type Fiber port



Duplex SC type Fiber port



WARNING: ***Attention: Visible laser radiation! Be careful! Do not stare into beam!***

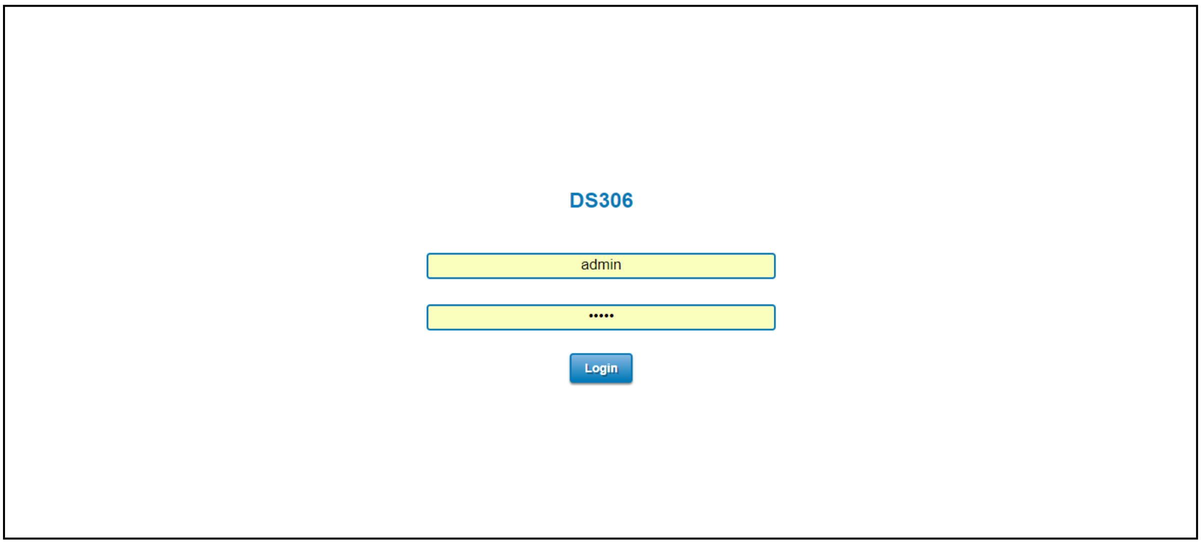
3. WEB MANAGEMENT CONFIGURATION

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. This manual describes the procedures for Web Interface and how to configure and monitor the managed switch only.

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 192.168.1.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**.



DS306

admin

•••••

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

3.2 Ethernet Port

3.3 Redundancy

3.4 QoS

3.5 Warning

3.6 Diagnostics

3.7 Backup / Restore

3.8 Firmware Upgrade

3.9 Reset to Defaults

3.10 Save

3.11 Logout

3.12 Reboot

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

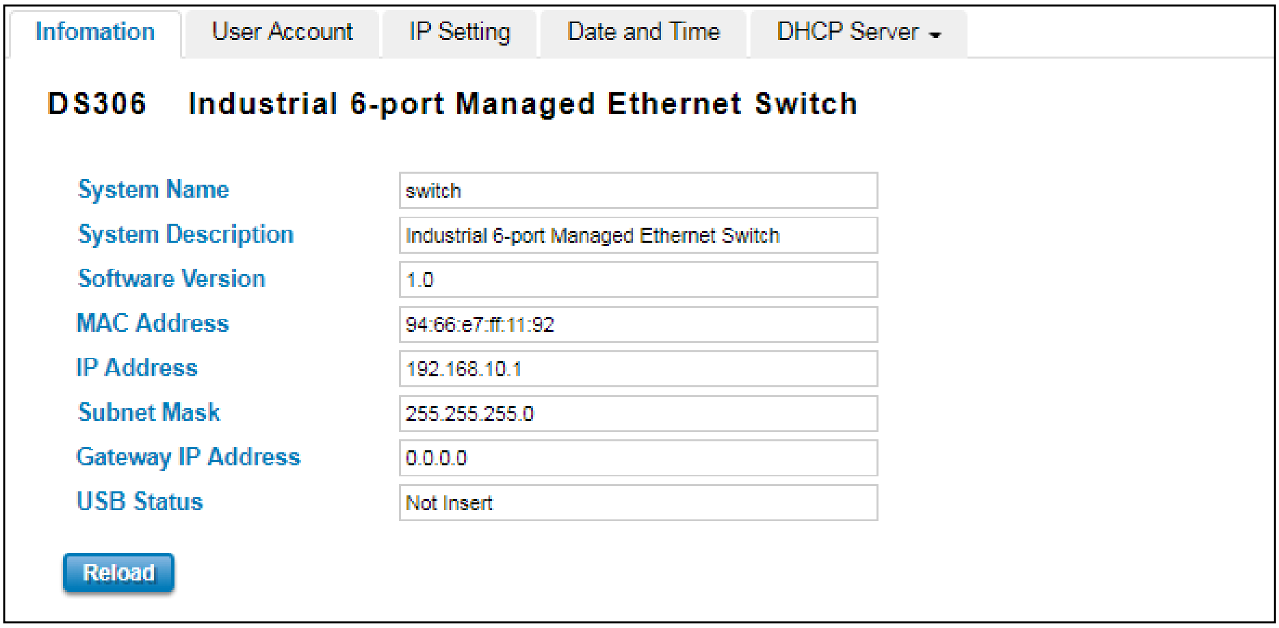
3.1.3 IP Setting

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.



DS306 Industrial 6-port Managed Ethernet Switch

System Name	switch
System Description	Industrial 6-port Managed Ethernet Switch
Software Version	1.0
MAC Address	94:66:e7:ff:11:92
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
USB Status	Not Insert

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

TERMS	DESCRIPTION
System Name	**Default: Switch** Set up a name to the switch device.
System Description	Display the switch description.
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.
IP Address	Display the assigned IP Address.
Subnet Mask	Display the assigned subnet mask.
Gateway IP Address	Display the assigned Gateway IP Address

USB Status	Show the USB status if inserted or not inserted.

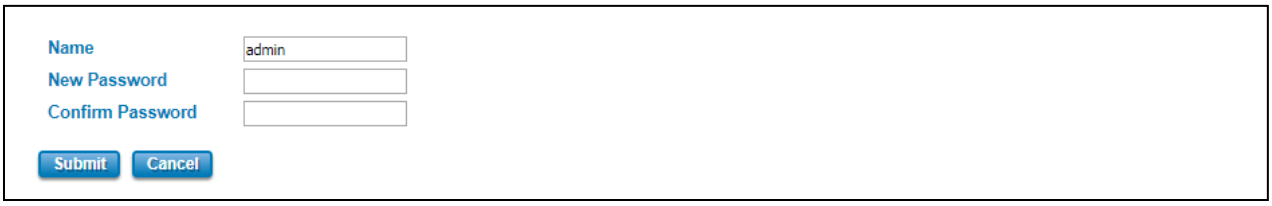
NOTE: For any kind of changes in configuration settings always remember to click on **Save** to save the settings. Otherwise, all of settings User has made will be lost when the switch is powered off or restarted.

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

3.1.2 USER ACCOUNT

WoMaster's 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 supported with Local User.

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



Name: admin
New Password:
Confirm Password:

This User Account 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 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:

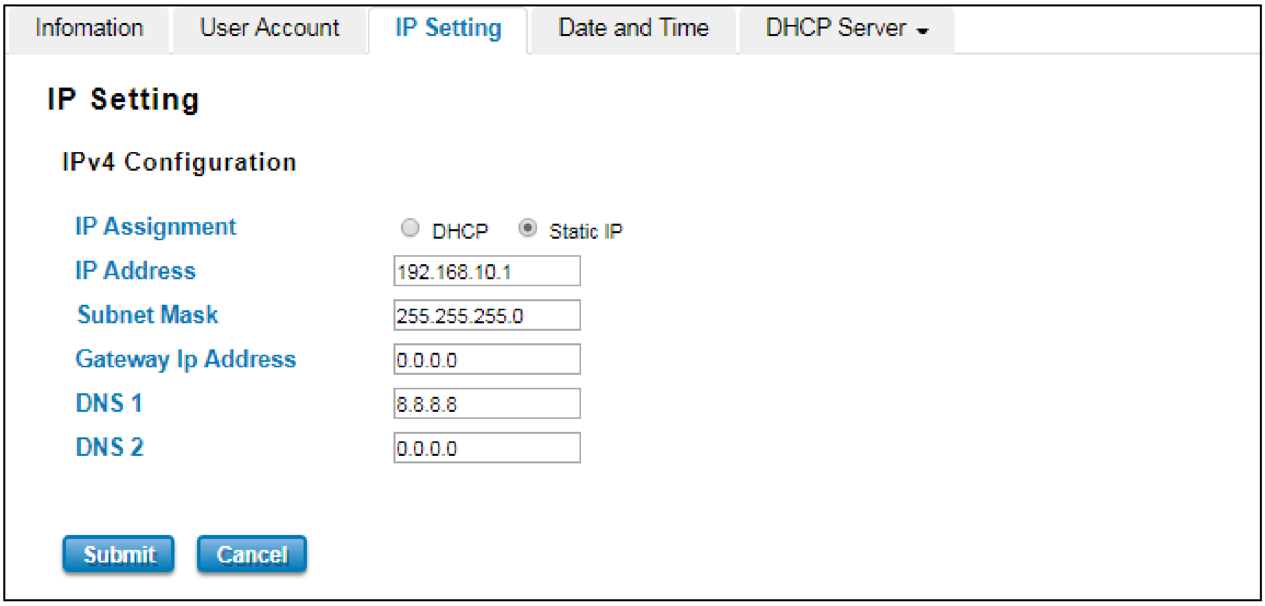
TERMS	DESCRIPTION
Name	**Default: admin** Key in new user name here.
New Password	**Default: blank** Key in new password here.
Confirm Password	Re-type the new password again to confirm it.

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

3.1.3 IP SETTING

IP Setting section allows users to configure IPv4 values for management access over the network.

IPv4 Configuration



IP Setting

IPv4 Configuration

IP Assignment	○ DHCP ● Static IP
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway Ip Address	0.0.0.0
DNS 1	8.8.8.8
DNS 2	0.0.0.0

The IPv4 Configuration includes the switch's IP address, 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.

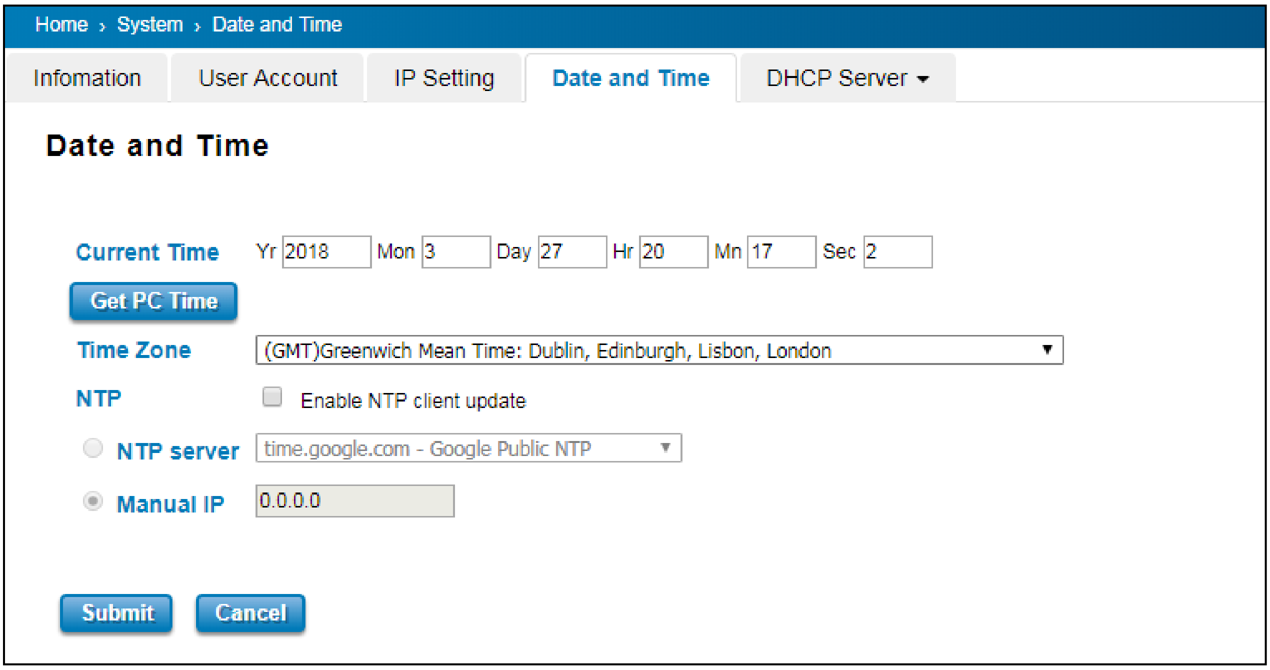
The description of the columns is as below:

TERMS	DESCRIPTION
IP Assignment	Set up the IP Address by choose the DHCP (DHCP Client) mode or Static IP mode. **DHCP** – by choose this mode, the switch will received the IP that assigned by the DHCP server. (the interface would blocked the IP Address, Subnet Mask and Gateway IP Address column) **Static** – by choose this mode, user may assign the IP Address by input he IP Address, Subnet Mask and Gateway IP Address column
IP Address	**Default: 192.168.10.1** Set up the IP address reserved by User network for User switch. If DHCP mode is activated, no needs to assign the IP Address.
Subnet Mask	**Default: 255.255.255.0** Assign the subnet mask for the IP address here. If DHCP mode is activated, no needs to assign the subnet mask.
Gateway IP Address	**Default: 0.0.0.0** Assign the gateway for the switch here. If DHCP mode is activated, no needs to assign the gateway IP Address.
DNS 1, DNS 2	Specifies the IP address of the DNS server 1 and 2 that used in user network.

3.1.4 DATE AND TIME

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 has 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. Press **Save** will write the system time to RTC.



Date and Time

Current Time Yr 2018 Mon 3 Day 27 Hr 20 Mn 17 Sec 2

Time Zone (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

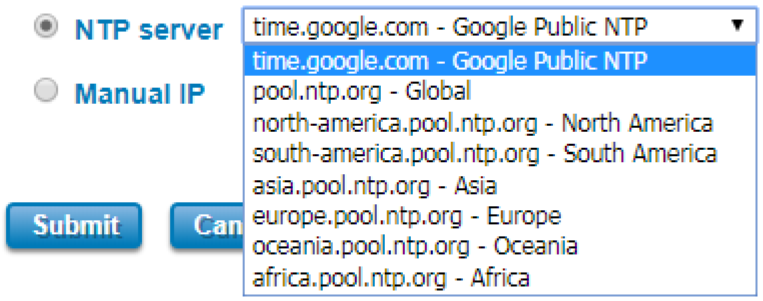
NTP □ Enable NTP client update

○ NTP server time.google.com - Google Public NTP

● Manual IP 0.0.0.0

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. ***Make sure that the switch also has the internet connection.**
NTP Server	Choose from NTP Server List, to adjust User system time.

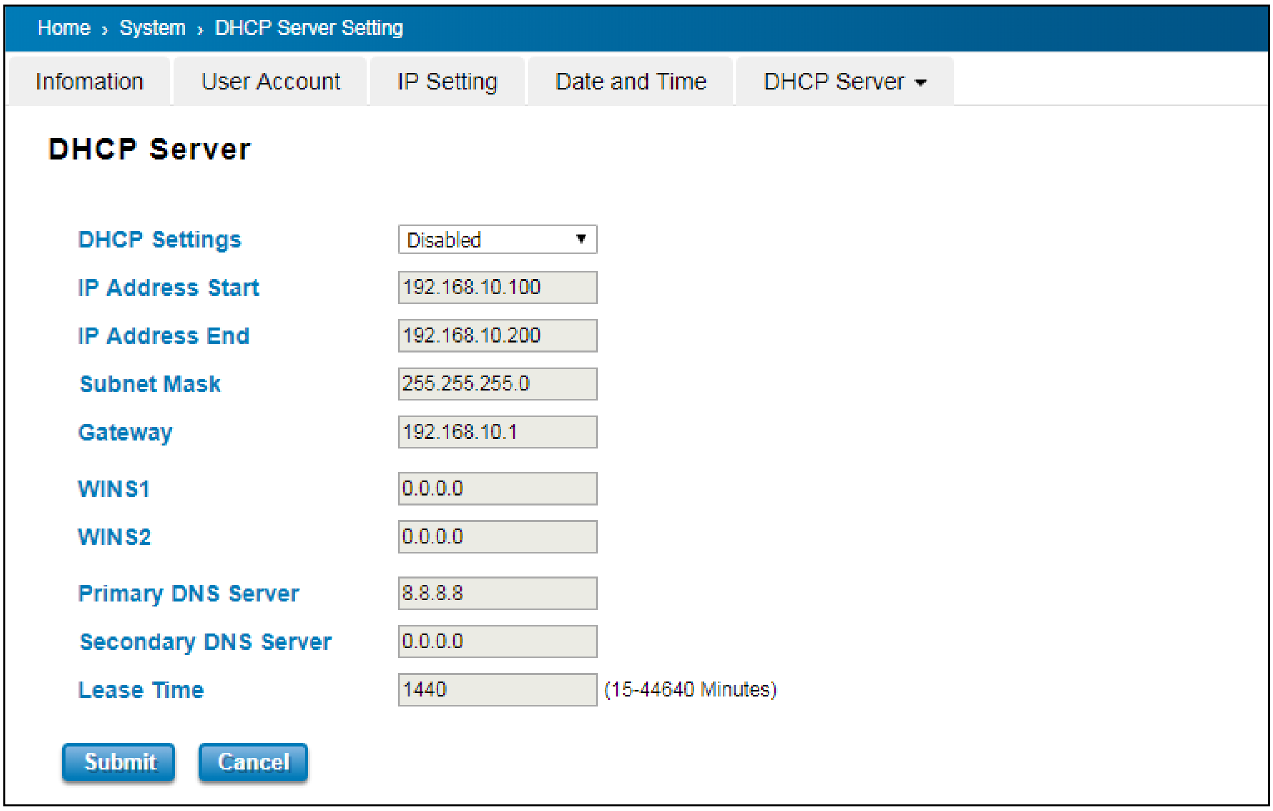
	 ● NTP server time.google.com - Google Public NTP ▼ ○ Manual IP time.google.com - Google Public NTP pool.ntp.org - Global north-america.pool.ntp.org - North America south-america.pool.ntp.org - South America asia.pool.ntp.org - Asia europe.pool.ntp.org - Europe oceania.pool.ntp.org - Oceania africa.pool.ntp.org - Africa Submit Can
Manual IP	User can assign the proper NTP server by input manually to synchronize the time.

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

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 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.



Home › System › DHCP Server Setting

Infomation | User Account | IP Setting | Date and Time | DHCP Server ▾

DHCP Server

DHCP Settings: Disabled ▼

IP Address Start: 192.168.10.100

IP Address End: 192.168.10.200

Subnet Mask: 255.255.255.0

Gateway: 192.168.10.1

WINS1: 0.0.0.0

WINS2: 0.0.0.0

Primary DNS Server: 8.8.8.8

Secondary DNS Server: 0.0.0.0

Lease Time: 1440 (15-44640 Minutes)

Submit Cancel

The description of the columns is as below:

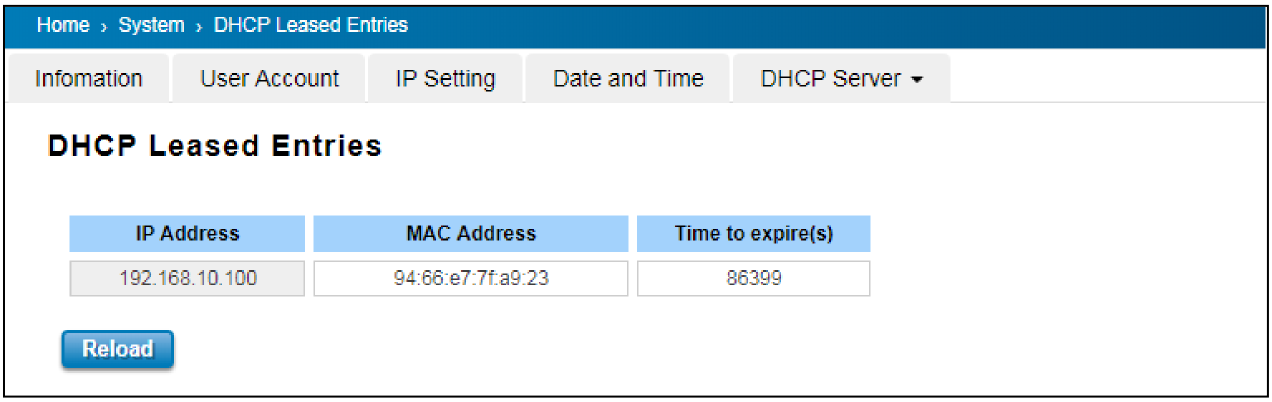
TERMS	DESCRIPTION
DHCP Setting	Select to **Enable** or **Disable** to activate and deactivate DHCP Server function.
IP Address Start	Enter the starting IP addresses for the DHCP server’s IP assignment.

IP Address End	Enter the ending IP addresses for the DHCP server's IP assignment.
Subnet Mask	Assign the subnet mask for the IP address here.
Gateway	Assign the gateway for the router here for DHCP Server.
WINS1	Enter WINS Server 1 IP address
WINS2	Enter WINS Server 2 IP address
Primary DNS Server	Specifies the IP address of the Primary DNS server that used in DHCP network.
Secondary DNS Server	Specifies the IP address of the Secondary DNS server that used in DHCP network.
Lease Time	The maximum length of time for the IP address lease. Enter the Lease time in minutes. (Lease Time range: 15-44640 minutes)

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.

DHCP Leased Entries

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



DHCP Leased Entries

IP Address	MAC Address	Time to expire(s)
192.168.10.100	94:66:e7:7f:a9:23	86399

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.
Time to expire(s)	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.

Following items are included in this group:

3.2.1 Port Status

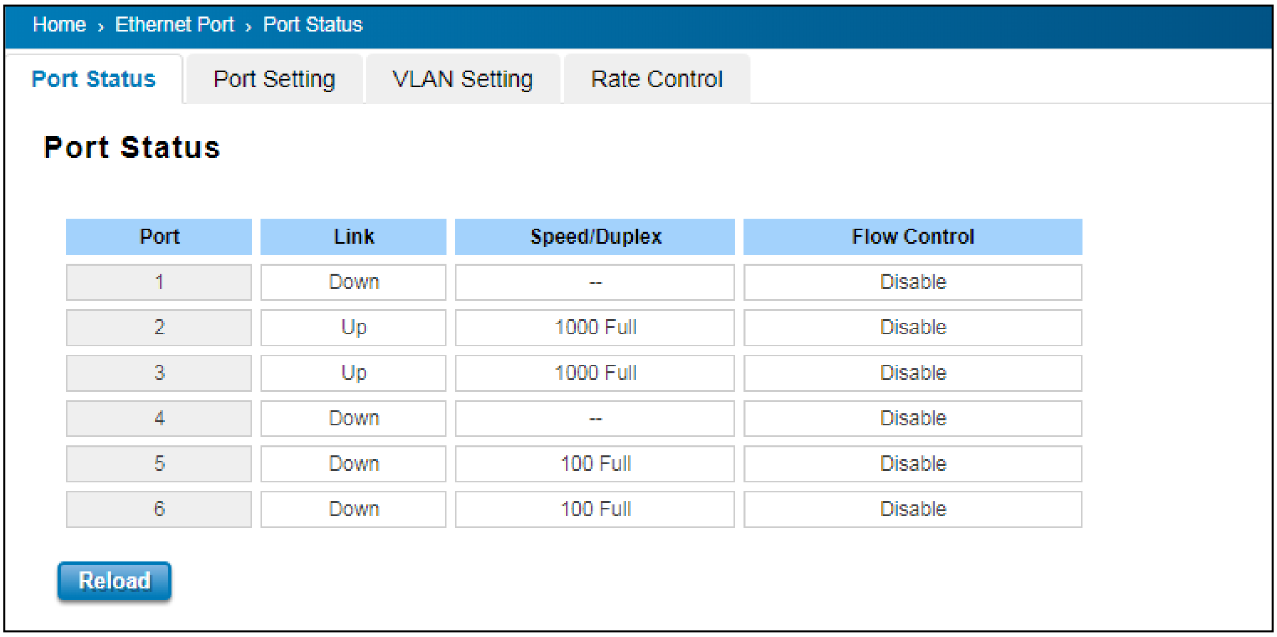
3.2.2 Port Setting

3.2.3 Rate Control

3.2.4 Port Trunk

3.2.1 PORT STATUS

Port Status provides current port status, such as the Port number, Link status if the port is up or down, show the speed/duplex for each port and the flow control.



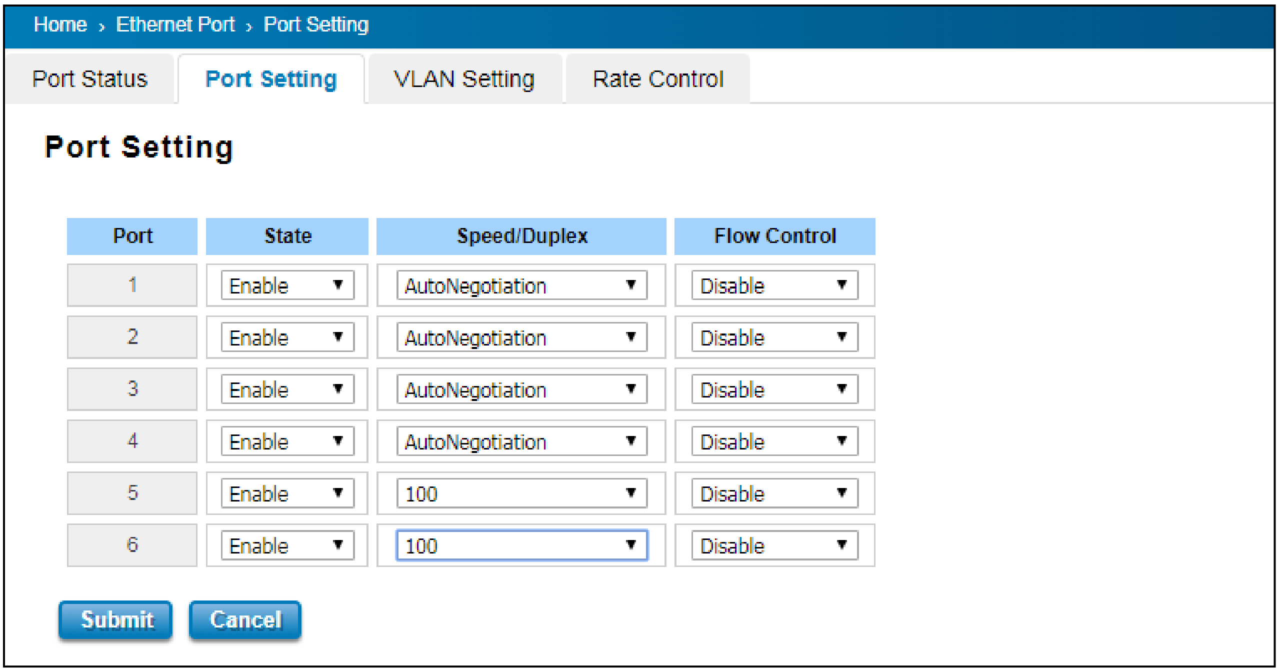
Port Status

Port	Link	Speed/Duplex	Flow Control
1	Down	--	Disable
2	Up	1000 Full	Disable
3	Up	1000 Full	Disable
4	Down	--	Disable
5	Down	100 Full	Disable
6	Down	100 Full	Disable

Click **Reload** to refresh the table.

3.2.2 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.



Port Setting

Port	State	Speed/Duplex	Flow Control
1	Enable	AutoNegotiation	Disable
2	Enable	AutoNegotiation	Disable
3	Enable	AutoNegotiation	Disable
4	Enable	AutoNegotiation	Disable
5	Enable	100	Disable
6	Enable	100	Disable

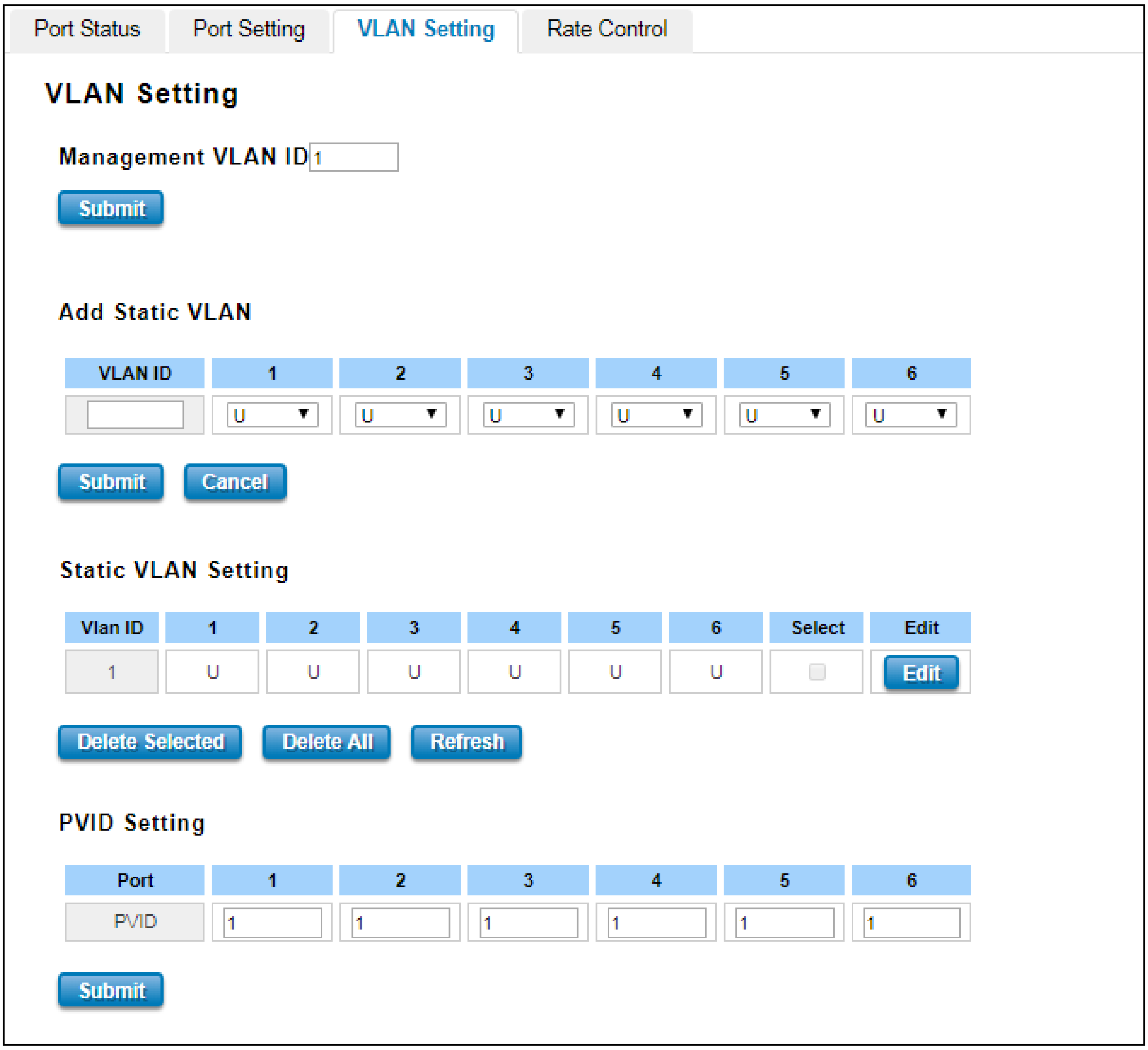
The description of the columns is as below:

TERMS	DESCRIPTION
Port	Shows port number
State	**Default: Enable** Enable or disable a port
Speed/Duplex	**Default: AutoNegotiation** Users can set the bandwidth of each port as Auto-negotiation, 100 full,100 half,10 full,10 half mode for **Fast Ethernet Port 1~4**. For **Fiber Port 5~6:** it can be set to 100.
Flow Control	**Default: Disable** **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.

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

3.2.3 VLAN SETTING

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. 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.



VLAN Setting

Management VLAN ID 1

Add Static VLAN

VLAN ID	1	2	3	4	5	6
	U ▼	U ▼	U ▼	U ▼	U ▼	U ▼

Static VLAN Setting

Vlan ID	1	2	3	4	5	6	Select	Edit
1	U	U	U	U	U	U	□	Edit

PVID Setting

Port	1	2	3	4	5	6
PVID	1	1	1	1	1	1

The description of the columns is as below:

TERMS	DESCRIPTION
Management VLAN ID	**Default : 1**. 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.
Add Static VLAN	By select the VLAN and click the Edit button, user can assign a VLAN ID or VLAN Name and User can specify the egress (outgoing) port

	rule to be **Untagged or Tagged**
Static VLAN Setting	At this section user can edit the VLAN that has been added, include the name and egress rule.
PVID Setting.	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.

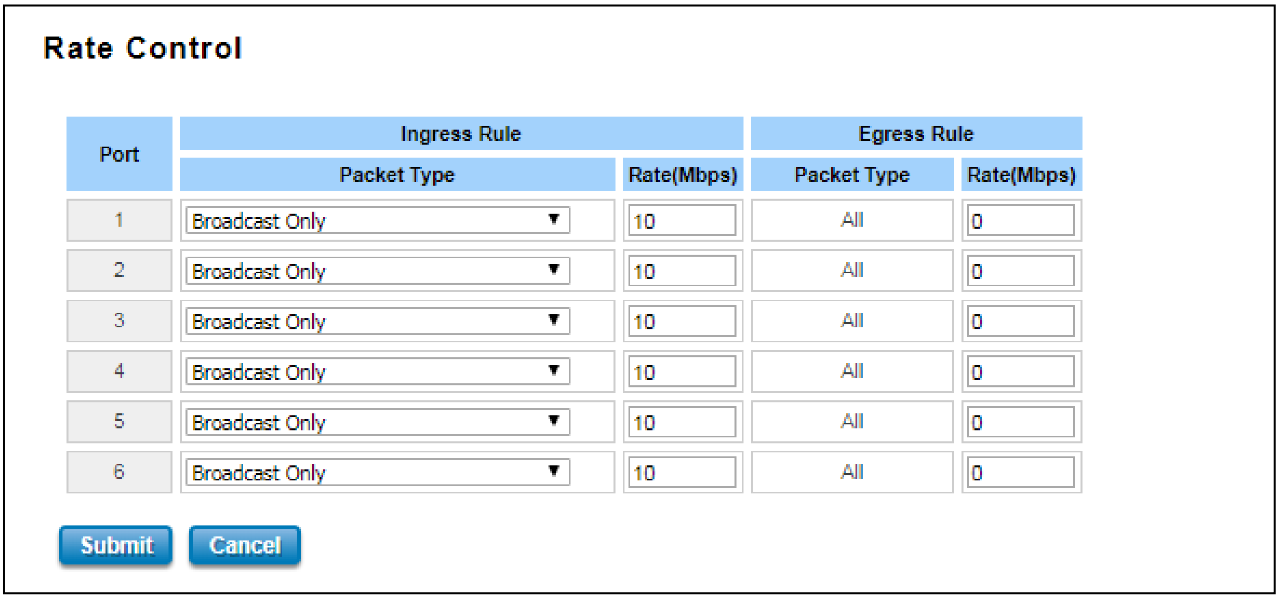
The steps to create a new VLAN: Type in Add Static VLAN section, and click **Submit** to create a new VLAN. Then User can see the new VLAN in the Static VLAN Setting table. After created the VLAN, the status of the VLAN will remain in Unused until User adds ports to the VLAN.

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.

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.



Rate Control

Port	Ingress Rule		Egress Rule	
	Packet Type	Rate(Mbps)	Packet Type	Rate(Mbps)
1	Broadcast Only ▼	10	All	0
2	Broadcast Only ▼	10	All	0
3	Broadcast Only ▼	10	All	0
4	Broadcast Only ▼	10	All	0
5	Broadcast Only ▼	10	All	0
6	Broadcast Only ▼	10	All	0

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: 10 Mbps** **Default value Egress: 0 Mbps (**0 stands for disabling the rate control for the port.**)** Valid values are from 1Mbps-100Mbps for fast Ethernet ports and gigabit Ethernet ports. The step of the rate is 1 Mbps.

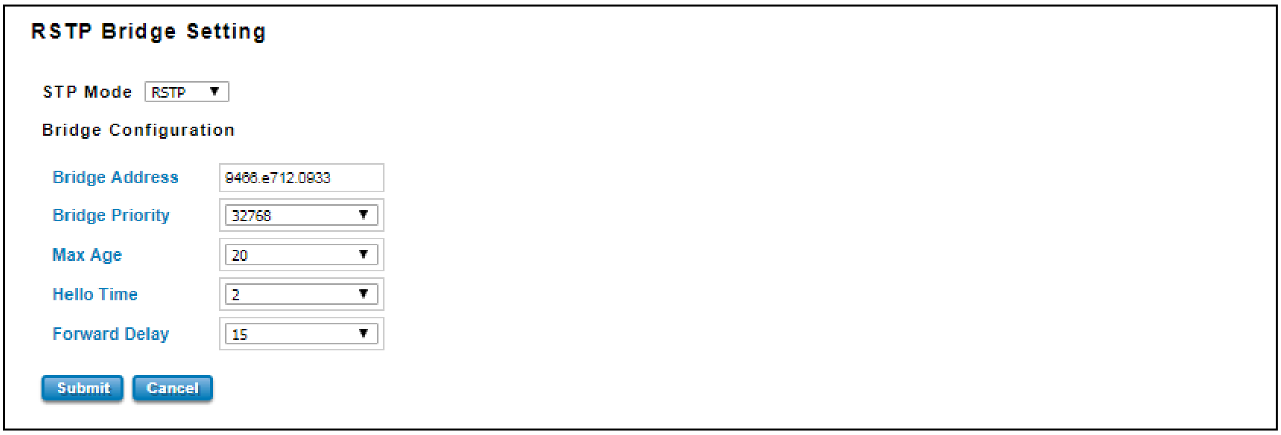
Click on **Submit** to apply the configuration.

3.3 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) 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.

3.3.1 RSTP SETTINGS

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



RSTP Bridge Setting

STP Mode: RSTP

Bridge Configuration

Bridge Address	9466.e712.0933
Bridge Priority	32768
Max Age	20
Hello Time	2
Forward Delay	15

The STP mode includes the **STP**, **RSTP** 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.

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.

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.

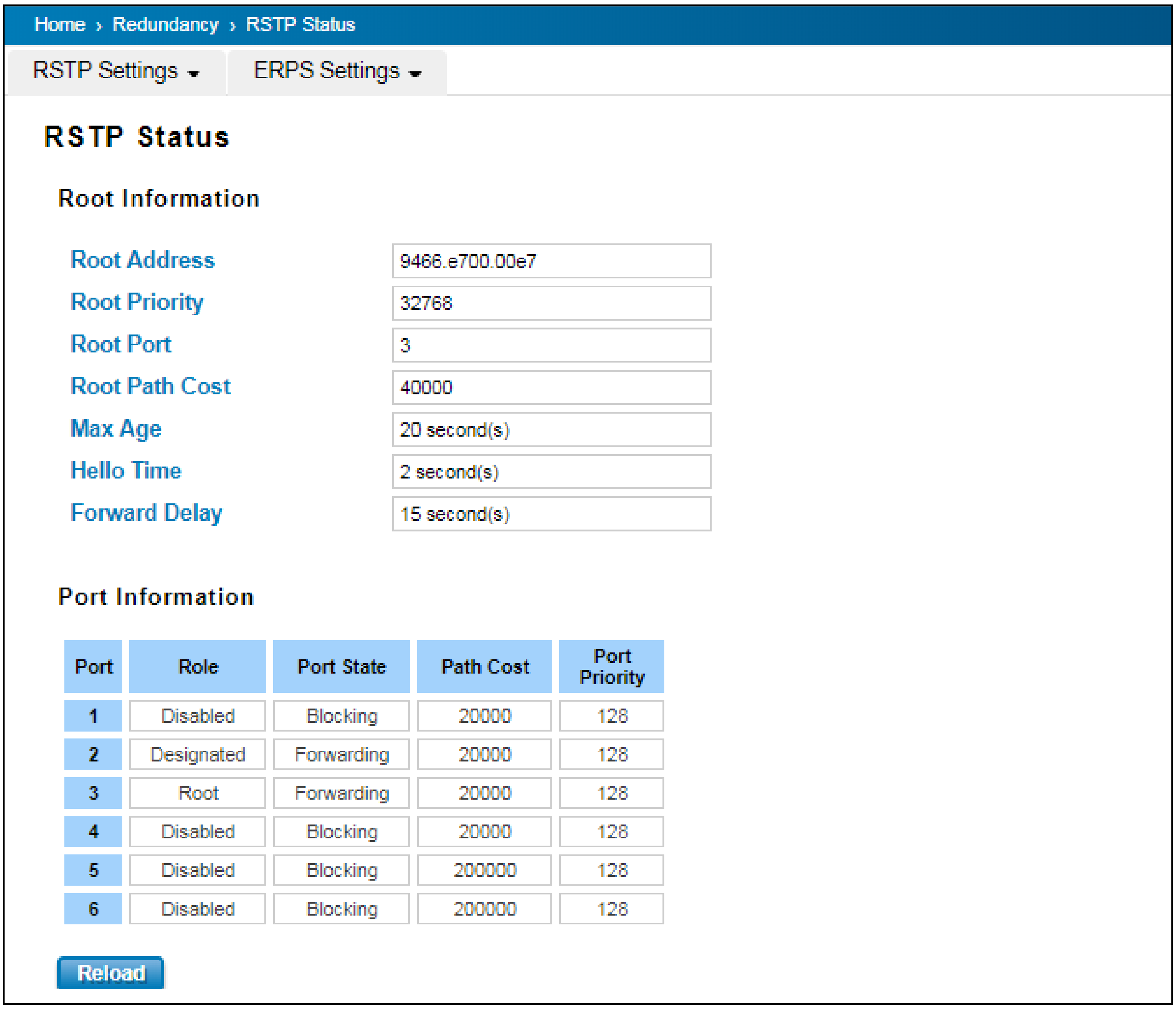
Once user has completed user configuration, click on **Submit** to apply user settings.

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 Status

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



RSTP Status

Root Information

Root Address	9466.e700.00e7
Root Priority	32768
Root Port	3
Root Path Cost	40000
Max Age	20 second(s)
Hello Time	2 second(s)
Forward Delay	15 second(s)

Port Information

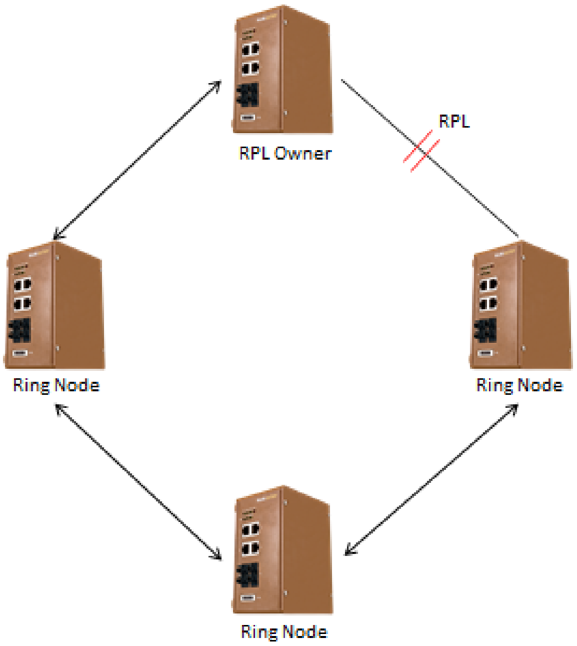
Port	Role	Port State	Path Cost	Port Priority
1	Disabled	Blocking	20000	128
2	Designated	Forwarding	20000	128
3	Root	Forwarding	20000	128
4	Disabled	Blocking	20000	128
5	Disabled	Blocking	200000	128
6	Disabled	Blocking	200000	128

Root Information: 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.

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

3.3.2 ERPS SETTINGS

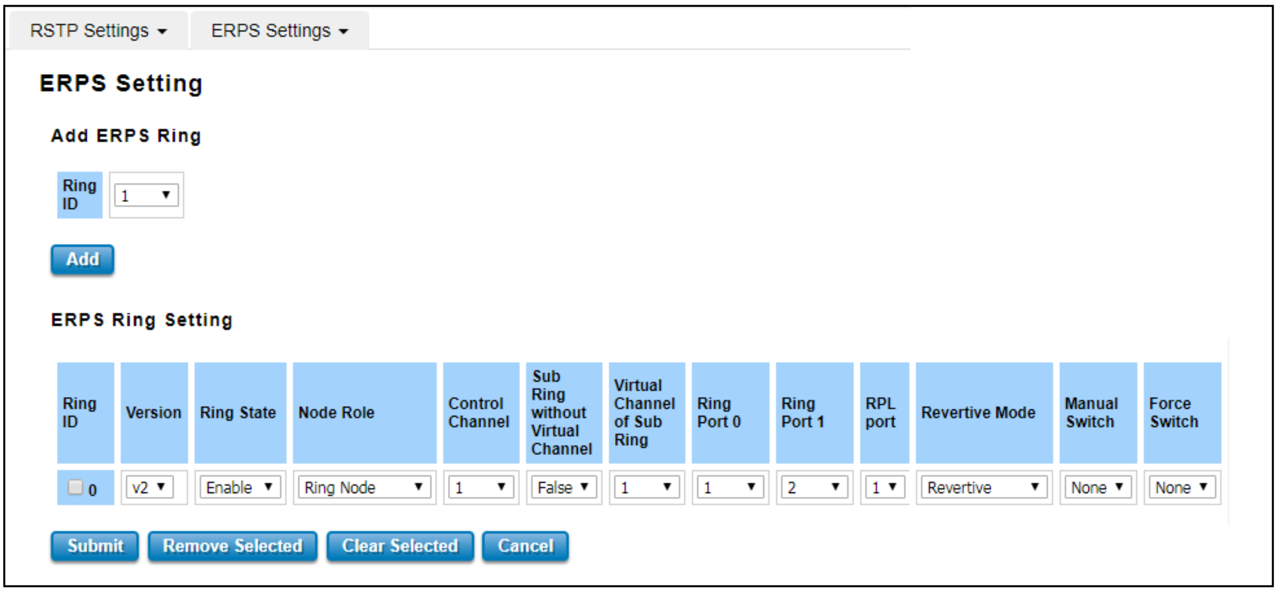
Ethernet Ring Protection Switching (ERPS) is a protocol for Ethernet layer network rings. The protocol specifies the protection mechanism for sub-50ms delay time. The ring topology provides multipoint connectivity economically by reducing the number of links. ERPS provides highly reliable and stable 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.

3.3.2.1 ERPS SETTINGS



ERPS Setting

Add ERPS Ring

Ring ID: 1 ▾

ERPS Ring Setting

Ring ID	Version	Ring State	Node Role	Control Channel	Sub Ring without Virtual Channel	Virtual Channel of Sub Ring	Ring Port 0	Ring Port 1	RPL port	Revertive Mode	Manual Switch	Force Switch
□ 0	v2 ▾	Enable ▾	Ring Node ▾	1 ▾	False ▾	1 ▾	1 ▾	2 ▾	1 ▾	Revertive ▾	None ▾	None ▾

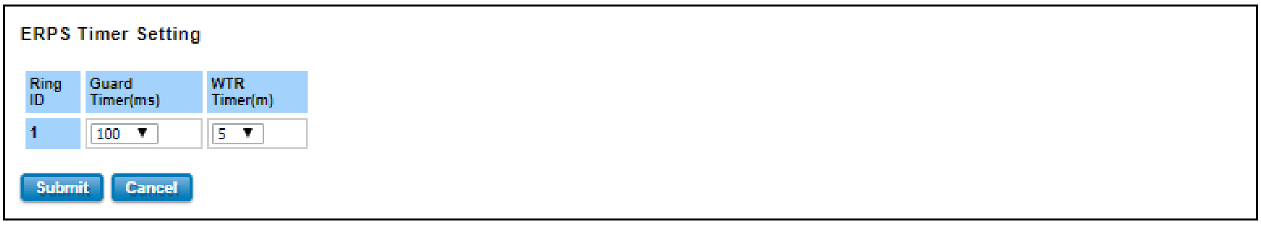
Add ERPS Ring is a section to add the Ring ID of the created Protection group; it must be an integer value between 0 and 31. The maximum numbers of ERPS Protection Groups that can be created are 32. Click the ID of a Protection group to enter the configuration page. After click Add button, one line will 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** Enable - Ring Status is enable Disable - Ring Status is disable
Node Role	It can be either RPL owner or RPL Neighbor or Ring Node.
Control Channel	**Default: 1** 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** **True** – if doesn’t have a virtual channel **False** – if have any virtual channel
Virtual Channel of Sub Ring	**Default: 1** 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.
RPL Port	This allows you to select the Ring Port 0 or Ring Port 1 as the RPL block.
Revertive Mode	**Default: Revertive** **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	**Default: None** In the absence of a failure or FS, Manual 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.
Force Switch	**Default: None** 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



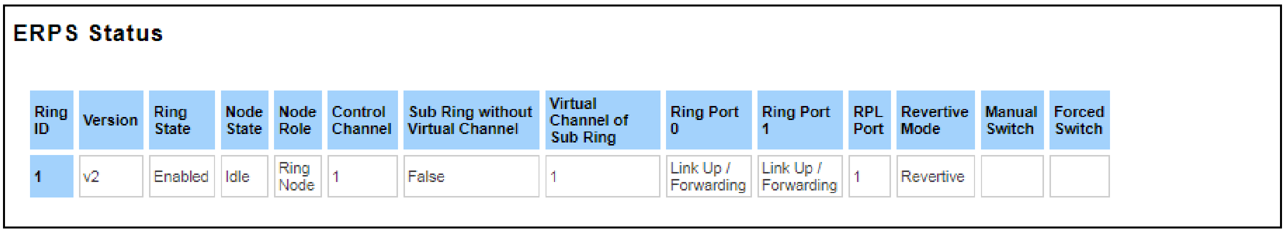
ERPS Timer Setting

Ring ID	Guard Timer(ms)	WTR Timer(m)
1	100 ▼	5 ▼

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.

3.3.2.2 ERPS STATUS

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

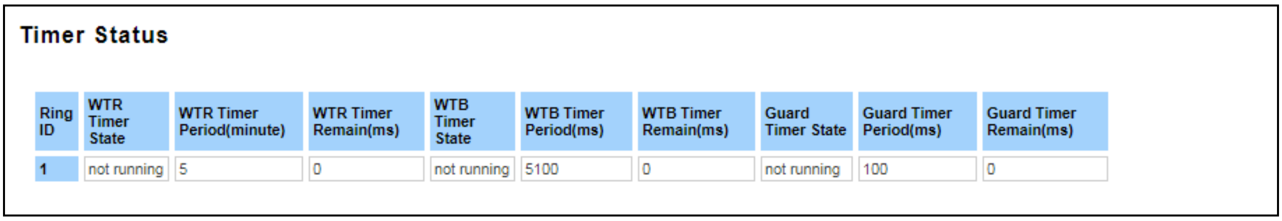


ERPS Status

Ring ID	Version	Ring State	Node State	Node Role	Control Channel	Sub Ring without Virtual Channel	Virtual Channel of Sub Ring	Ring Port 0	Ring Port 1	RPL Port	Revertive Mode	Manual Switch	Forced Switch
1	v2	Enabled	Idle	Ring Node	1	False	1	Link Up / Forwarding	Link Up / Forwarding	1	Revertive		

TERMS	DESCRIPTION
Ring ID	Display the Ring ID
Version	ERPS Protocol Version - v1 or v2.
Ring State	**Default: Disable** Enabled - Ring Status is enable 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** **True** – if have a virtual channel **False** – if doesn't have any virtual channel
Virtual Channel of Sub Ring	**Default: 1** 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
RPL Port	The port status as the RPL block.
Revertive Mode	**Default: Revertive** **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

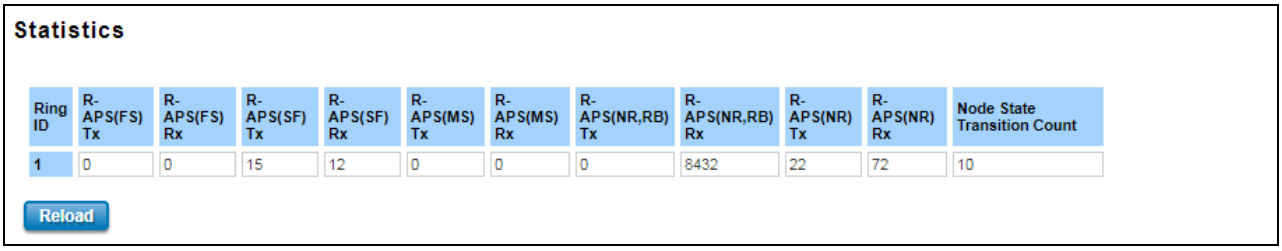
Timer Status



Timer Status

Ring ID	WTR Timer State	WTR Timer Period(minute)	WTR Timer Remain(ms)	WTB Timer State	WTB Timer Period(ms)	WTB Timer Remain(ms)	Guard Timer State	Guard Timer Period(ms)	Guard Timer Remain(ms)
1	not running	5	0	not running	5100	0	not running	100	0

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.



Statistics

Ring ID	R-APS(FS) Tx	R-APS(FS) Rx	R-APS(SF) Tx	R-APS(SF) Rx	R-APS(MS) Tx	R-APS(MS) Rx	R-APS(NR,RB) Tx	R-APS(NR,RB) Rx	R-APS(NR) Tx	R-APS(NR) Rx	Node State Transition Count
1	0	0	15	12	0	0	0	8432	22	72	10

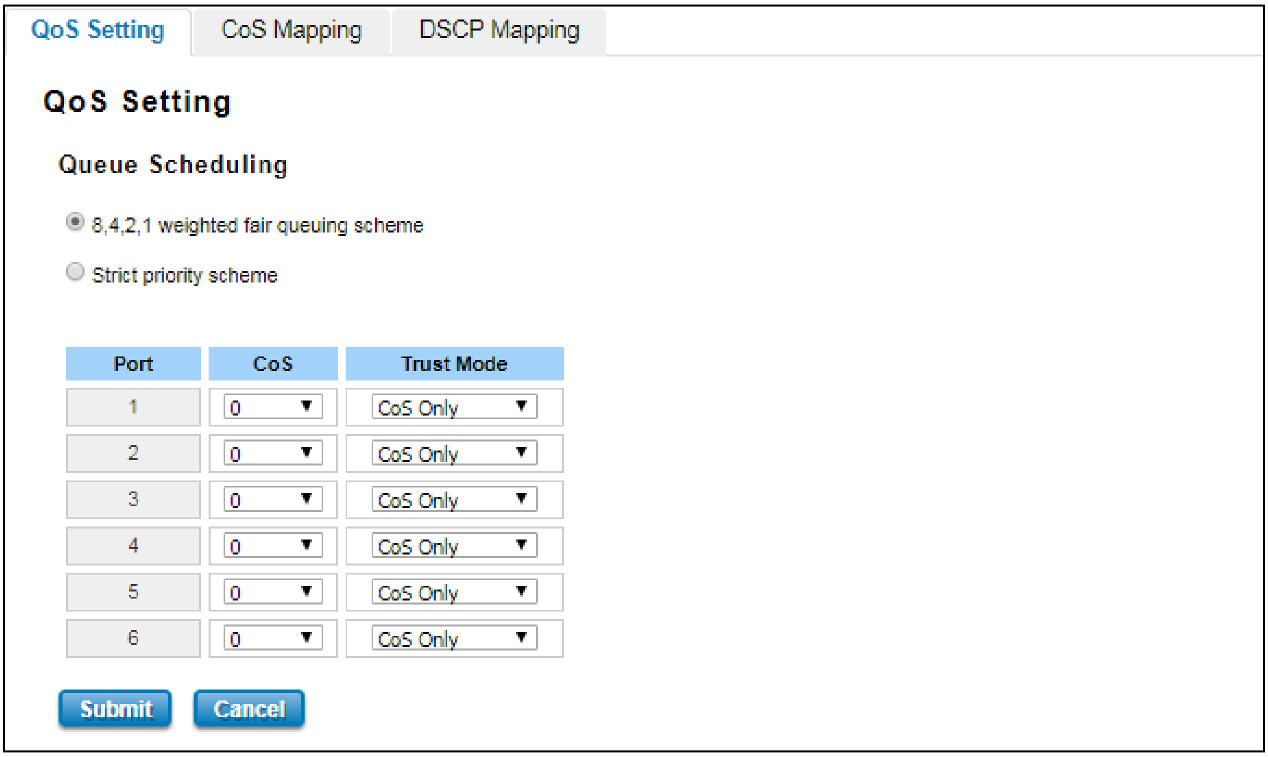
TERMS	DESCRIPTION
Ring ID	Display the Ring ID.
R-APS(FS) Tx	The number of R-APS messages with Forced Switch (FS) being sent.
R-APS(FS) Rx	The number of R-APS messages with Forced Switch (FS) being received.
R-APS(SF) Tx	The number of R-APS messages with Signal Fail (SF) being sent.
R-APS(SF) Rx	The number 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.

3.4 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.

3.4.1 QoS SETTING

The figure below shows QoS Setting.



QoS Setting

Queue Scheduling

● 8,4,2,1 weighted fair queuing scheme

○ Strict priority scheme

Port	CoS	Trust Mode
1	0	CoS Only
2	0	CoS Only
3	0	CoS Only
4	0	CoS Only
5	0	CoS Only
6	0	CoS Only

Queue Scheduling

User may select the Queue Scheduling rule:

By using the **8,4,2,1 weight fair queuing scheme**: The switch will follow 8:4:2:1 rate to process priority queue from High to lowest queue. The rate here means 8 with the highest priority in the queue, 4 with middle priority, 2 for low priority, and 1 with the lowest priority.

Use **a strict priority scheme:** The priority here is always the higher queue will be processed first, except the higher queue is empty.

The description of the columns is as below:

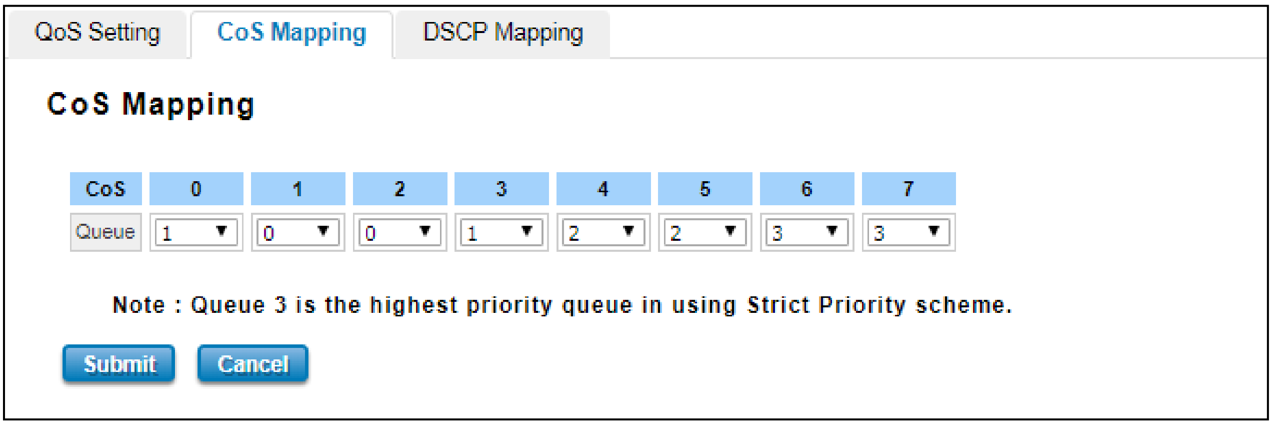
TERMS	DESCRIPTION
CoS	Indicate default port priority value for untagged or priority-tagged frames.
Trust Mode	**Default: COS Only** Indicate Queue Mapping types for User to select.

COS Only	Port priority will only follow COS-Queue Mapping User has assigned.
DSCP Only	Port priority will only follow DSCP-Queue Mapping User has assigned.
COS First	Port priority will follow COS-Queue Mapping first, and then DSCP-Queue Mapping rule.
DSCP First	Port priority will follow DSCP-Queue Mapping first, and then COS-Queue Mapping rule.

When the switch receives the frames, it will attach the value to the CoS field of the incoming VLAN-tagged packets. User can enable 0,1,2,3,4,5,6 or 7 to the port._After configuration, press **Submit** to enable the settings.

3.4.2 CoS MAPPING

This section allows user to assign CoS priorities to different queues. WoMaster switch only supports 4 physical queues, Lowest, Low, Middle and High represent by numbers from 0 to 3. Below is the interface.



CoS Mapping

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

Note : Queue 3 is the highest priority queue in using Strict Priority scheme.

User can find CoS values 1 and 2 are mapped to physical Queue 0, the lowest queue. CoS values 0 and 3 are mapped to physical Queue 1, the low/normal physical queue. CoS values 4 and 5 are mapped to physical Queue 2, the middle physical queue. CoS values 6 and 7 are mapped to physical Queue 3, the high physical queue.

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

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

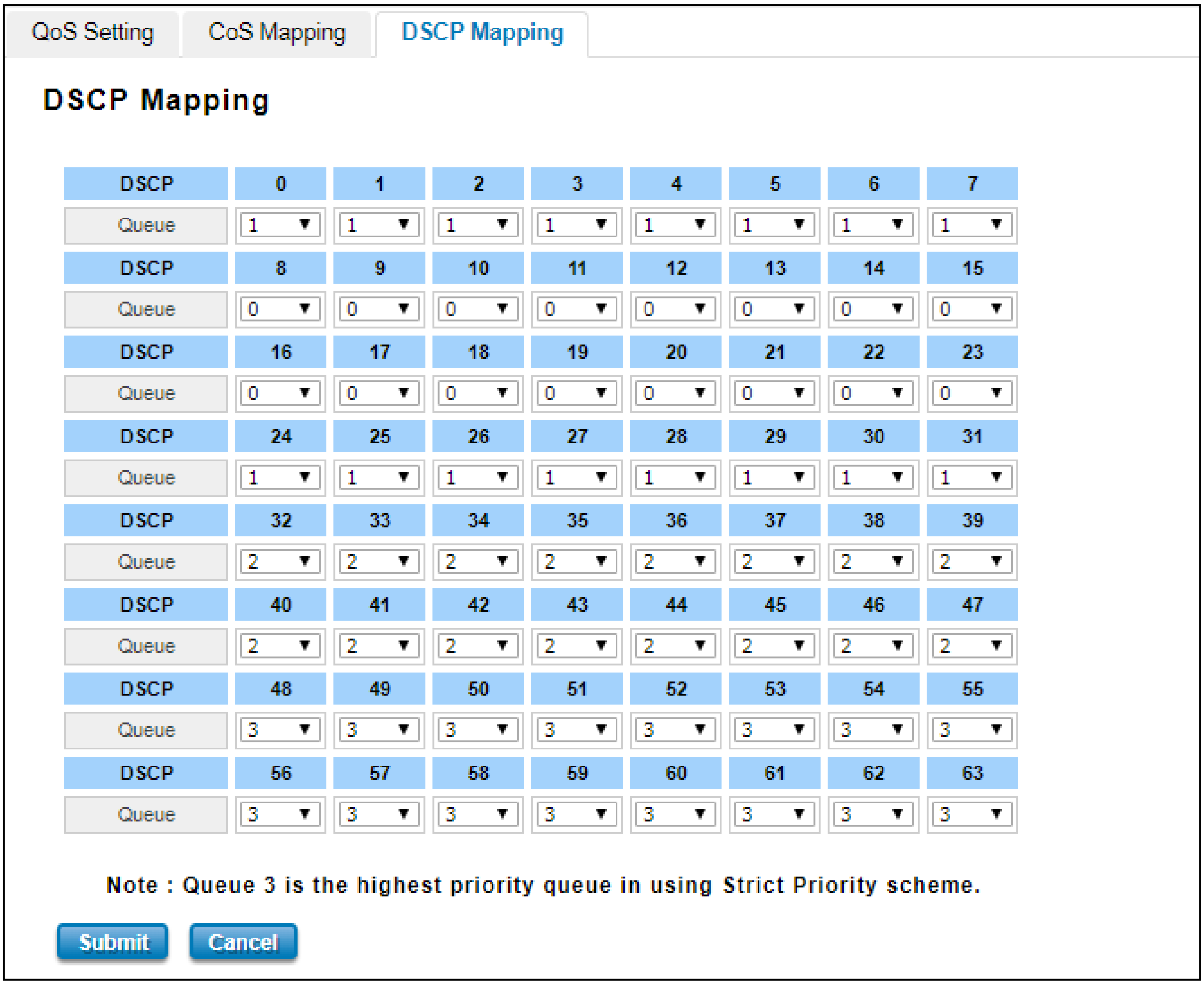
For the step in configuration

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

2. Click the Submit button.

3.4.3 DSCP MAPPING

This page is to assign DSCP priorities to different Queues. The WoMaster switch only supports 4 physical queues, Lowest, Low, Middle and High that represent by number 0 ~ 3. 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.



DSCP Mapping

DSCP	0	1	2	3	4	5	6	7
Queue	1	1	1	1	1	1	1	1
DSCP	8	9	10	11	12	13	14	15
Queue	0	0	0	0	0	0	0	0
DSCP	16	17	18	19	20	21	22	23
Queue	0	0	0	0	0	0	0	0
DSCP	24	25	26	27	28	29	30	31
Queue	1	1	1	1	1	1	1	1
DSCP	32	33	34	35	36	37	38	39
Queue	2	2	2	2	2	2	2	2
DSCP	40	41	42	43	44	45	46	47
Queue	2	2	2	2	2	2	2	2
DSCP	48	49	50	51	52	53	54	55
Queue	3	3	3	3	3	3	3	3
DSCP	56	57	58	59	60	61	62	63
Queue	3	3	3	3	3	3	3	3

Note : Queue 3 is the highest priority queue in using Strict Priority scheme.

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

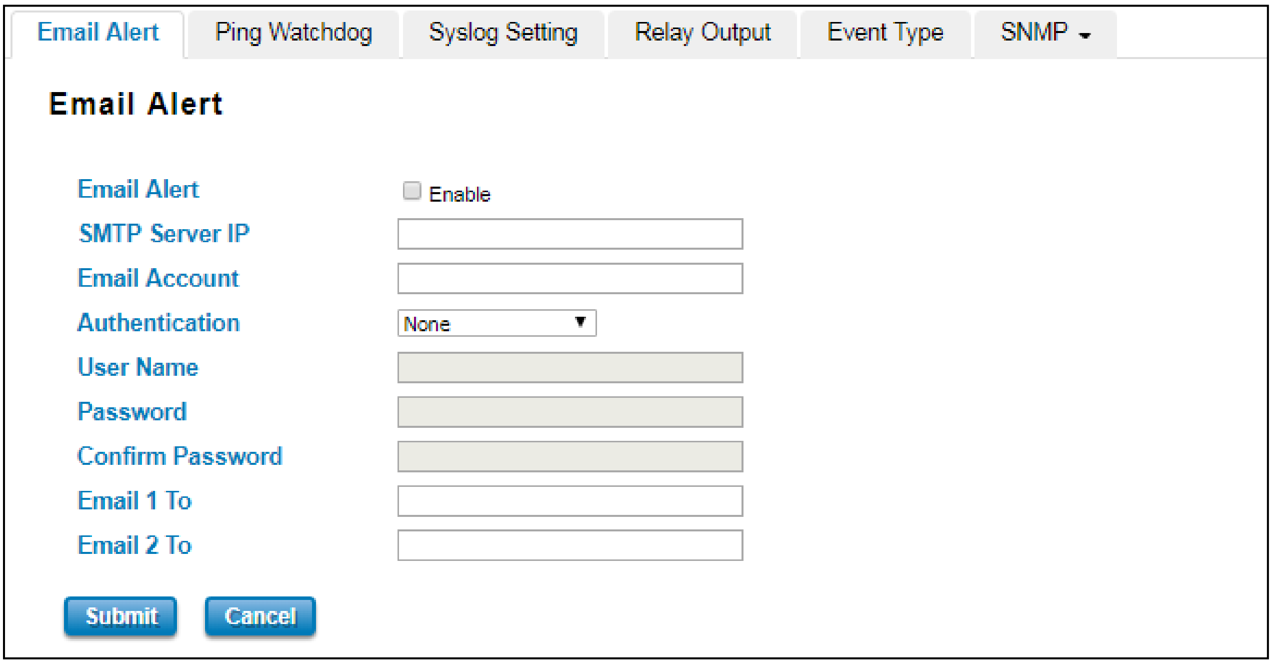
DSCP Value and Priority Queues Setting	Description	Factory Default
0 to 7	Maps different TOS values to one of 4 different egress queues.	1
8 to 15		0
16 to 23		0
24 to 31		1
32 to 39		2
40 to 47		2
48 to 55		3
56 to 63		3

3.5 WARNING

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

3.5.1 EMAIL ALERT

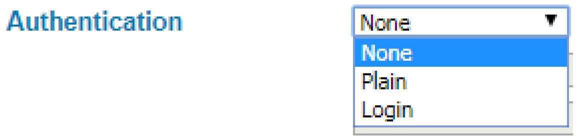
WoMaster switch provides the option of automatically sending an e-mail if an alarm event occurs (for example to the network administrator). The e-mail contains the identification of the sending device, a description of the cause of the alarm in plain language, and a time stamp. This allows centralized 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.



Email Alert

Email Alert	☐ Enable
SMTP Server IP	
Email Account	
Authentication	None
User Name	
Password	
Confirm Password	
Email 1 To	
Email 2 To	

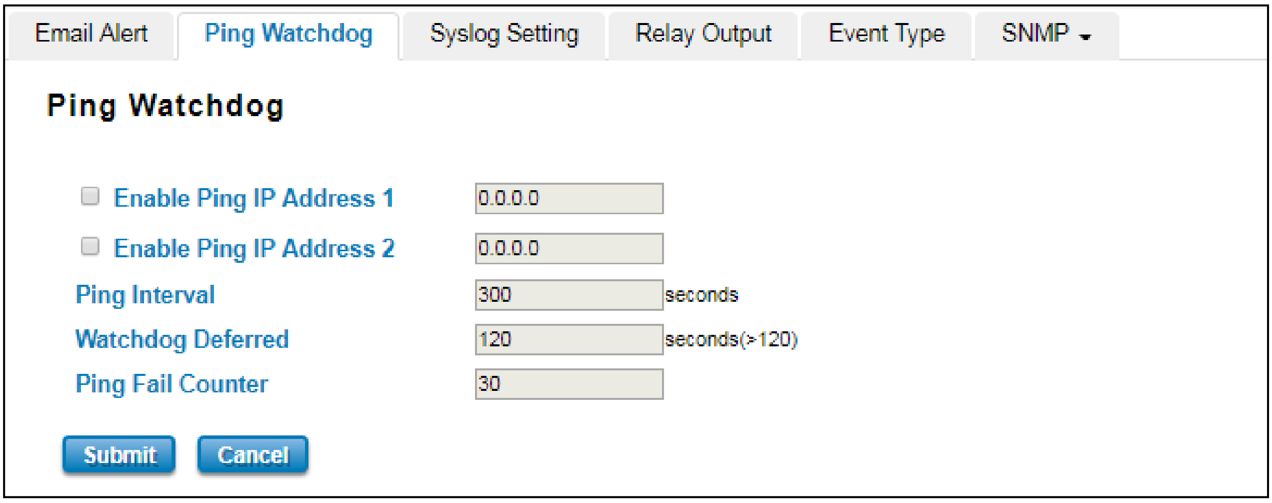
The description of the columns is as below:

TERMS	DESCRIPTION
Email Alert	Check the box to enable the function
SMTP Server IP	Enter the IP address of the email Server
Email Account	Click on check box to enable password
Authentication	 Choose the Authentication mode (None, Plain, Login)
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 2 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)

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

3.5.2 PING WATCHDOG



Ping Watchdog

☐ Enable Ping IP Address 1 0.0.0.0

☐ Enable Ping IP Address 2 0.0.0.0

Ping Interval 300 seconds

Watchdog Deferred 120 seconds(>120)

Ping Fail Counter 30

Ping Watchdog is a feature that helps WoMaster' router to allow user continuously ping a specific remote host for connection status using a user-defined IP address (or an Internet gateway). In this section, WoMaster provide two target IP Addresses, in order if the other one cannot be reach there is another back up IP address. There are two conditions in this Ping Watchdog section, the first one is when the device continuously ping the target IP and in the end it can reach one of the target IPs the device would not reboot. But if both targets IPs cannot be reached, the device will start counting the Ping Fail Counter time till it can be reached. If it is unable to ping the target IP address, this device will automatically reboot. After User finishes configuring the settings, click on **Submit** to apply User configuration.

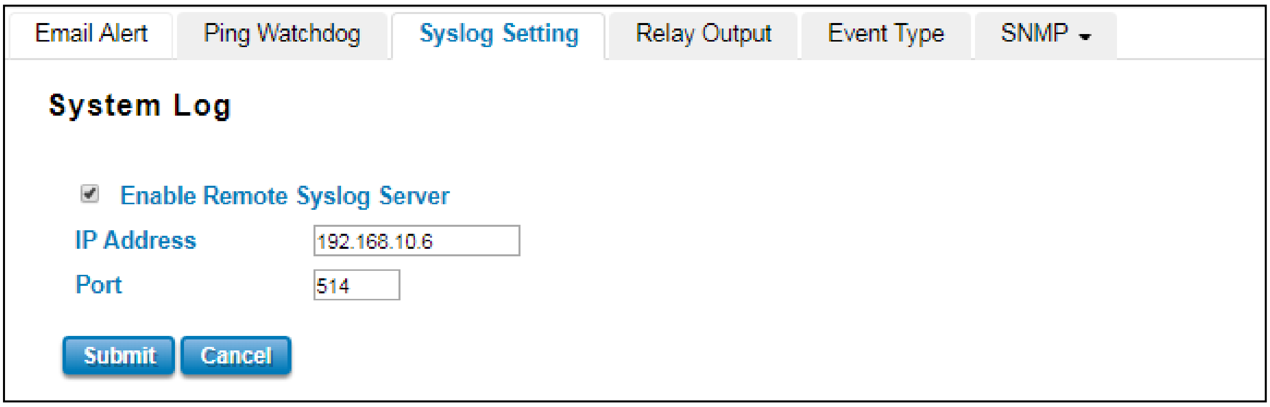
The description of the columns is as below:

TERMS	DESCRIPTION
Enable Ping IP Address 1	Clicks enable to activate the feature. Set the first IP Address to check if the device is alive or not
Enable Ping IP Address 2	Clicks enable to activate the feature. Set the second IP Address to check if the device is alive or not
Ping Interval	**Default: 300 (seconds)** Set the interval timer to Ping the remote device. Every 300 seconds the device will try to ping the target IP.
Watchdog Deferred	**Default: 120 (seconds) >120** The device needs time to boot, the startup delay use to buffer to prevent the device continue to reboot itself.
Ping Fail Counter	**Default: 30** When the remaining ping fail counter reach to 0 or reach the failure count, the device will reboot.

Click **Submit** to apply the configuration.

3.5.3 SYSLOG SETTING

Systems 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.



System Log

☑ Enable Remote Syslog Server

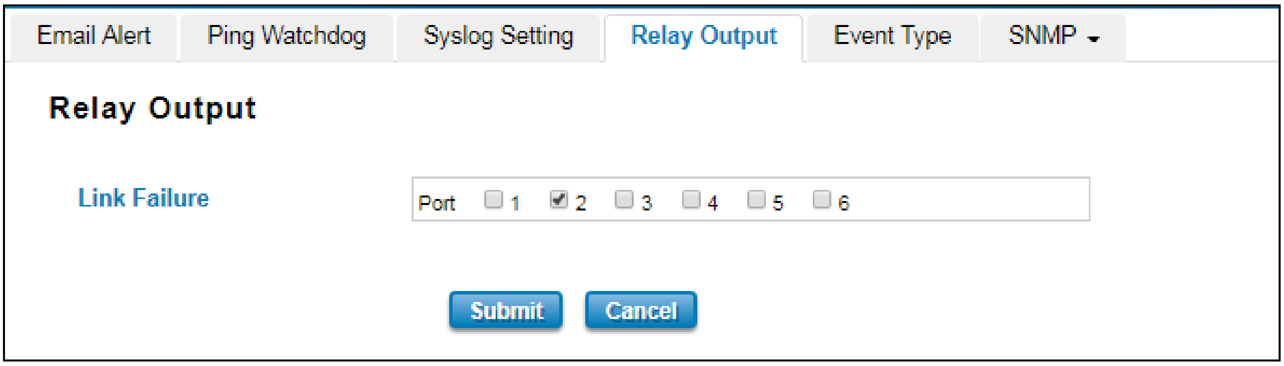
IP Address: 192.168.10.6

Port: 514

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

3.5.4 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 discrete output is on during normal conditions and turned off in the event of an alarm condition. The Relay Output configuration interface has shown as below:



Relay Output

Link Failure: Port □ 1 ☑ 2 □ 3 □ 4 □ 5 □ 6

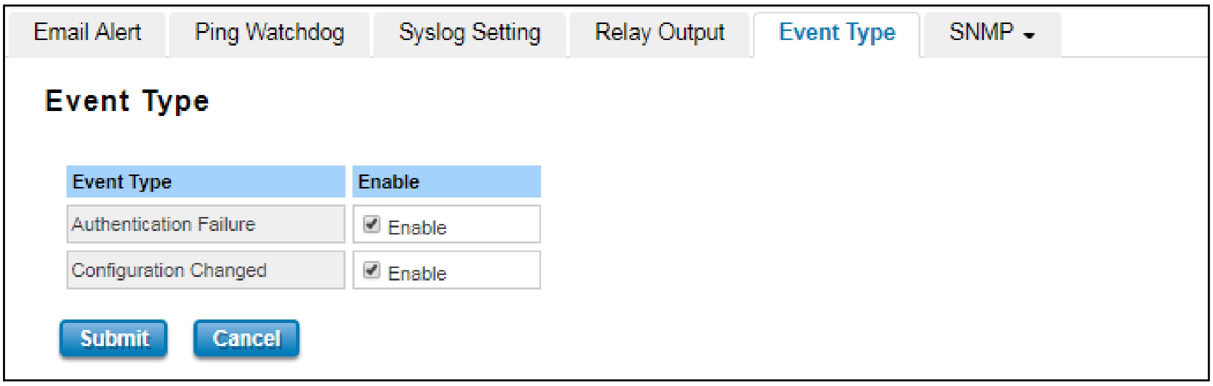
The condition or term described as following table.

TERMS	CONDITION	DESCRIPTION
Link Failure	Port number	Monitoring port link down event

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.

3.5.5 EVENT TYPE

On this page, user can specify how the switch reacts to system events. To enable or disable the options, click the relevant check boxes of the columns. There are two basic Event Types which are Authentication Failure that related when the authentication process between your local computer and the remote device has failed and Configuration Changed that related to the any changing in configuration.



Event Type

Event Type	Enable
Authentication Failure	☑ Enable
Configuration Changed	☑ Enable

TERMS	DESCRIPTION
Authentication Failure	When the authentication fails, the system will issue the event log/email alert to the system log/SMTP server respectively.
Configuration Changed	When there are any kinds of changing in the configuration, the system will issue the event log/email alert to the system log/SMTP server respectively.

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

3.5.6 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' Router support SNMP V2c and V3

3.5.6.1 SNMP SETTING

In this page user may configure the SNMP setting, click enable to activate the function. Select the Protocol version (V2c/V3), configure the server port, set up the password for the Get Community and specify the password for Set Community.

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.

SNMPv2C

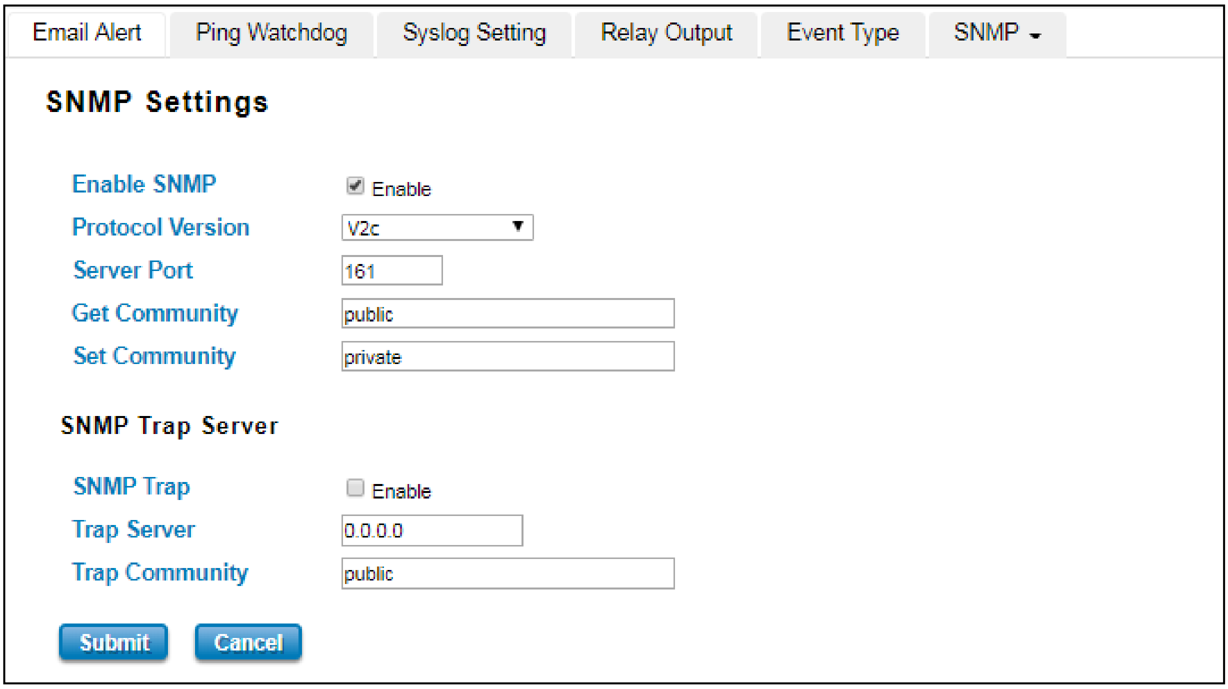
SNMPv2c is a sub-version of SNMPv2. Its key advantage over previous versions is the Inform command. Unlike Traps, which are simply received by a manager, Informs are positively acknowledged with a response message. If a manager does not reply to an Inform, the SNMP agent will resend the Inform.

SNMP V3

SNMPv3 is the newest version of SNMP. Its primary feature is enhanced security.

SNMPv3 security comes primarily in 2 forms:

- **Authentication** is used to ensure that traps are read by only the intended recipient.
- **Privacy** encrypts the payload of the SNMP message to ensure that it cannot be read by unauthorized users.



SNMP Settings

Enable SNMP ☑ Enable

Protocol Version V2c

Server Port 161

Get Community public

Set Community private

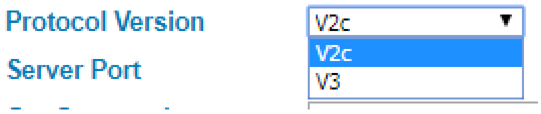
SNMP Trap Server

SNMP Trap □ Enable

Trap Server 0.0.0.0

Trap Community public

The description of the columns is as below:

TERMS	DESCRIPTION
Enable SNMP	Click the box to enable the SNMP function.
Protocol Version	**Default: V2c** Select the SNMP protocol version.  Protocol Version V2c Server Port V2c V3
Server Port	**Default: 161** Sets the port on which SNMP data has been sent. User can specify port by marking on user defined and specify port that user wants SNMP data to be sent.
Get Community	**Default: public** Create the name for a group or community of administrators who can view SNMP data.
Set Community	**Default: private** Create the name for a group or community of administrators who can write or edit SNMP data.

After finish with the configuration, clicks **Submit** to activate the function.

SNMP Trap Server

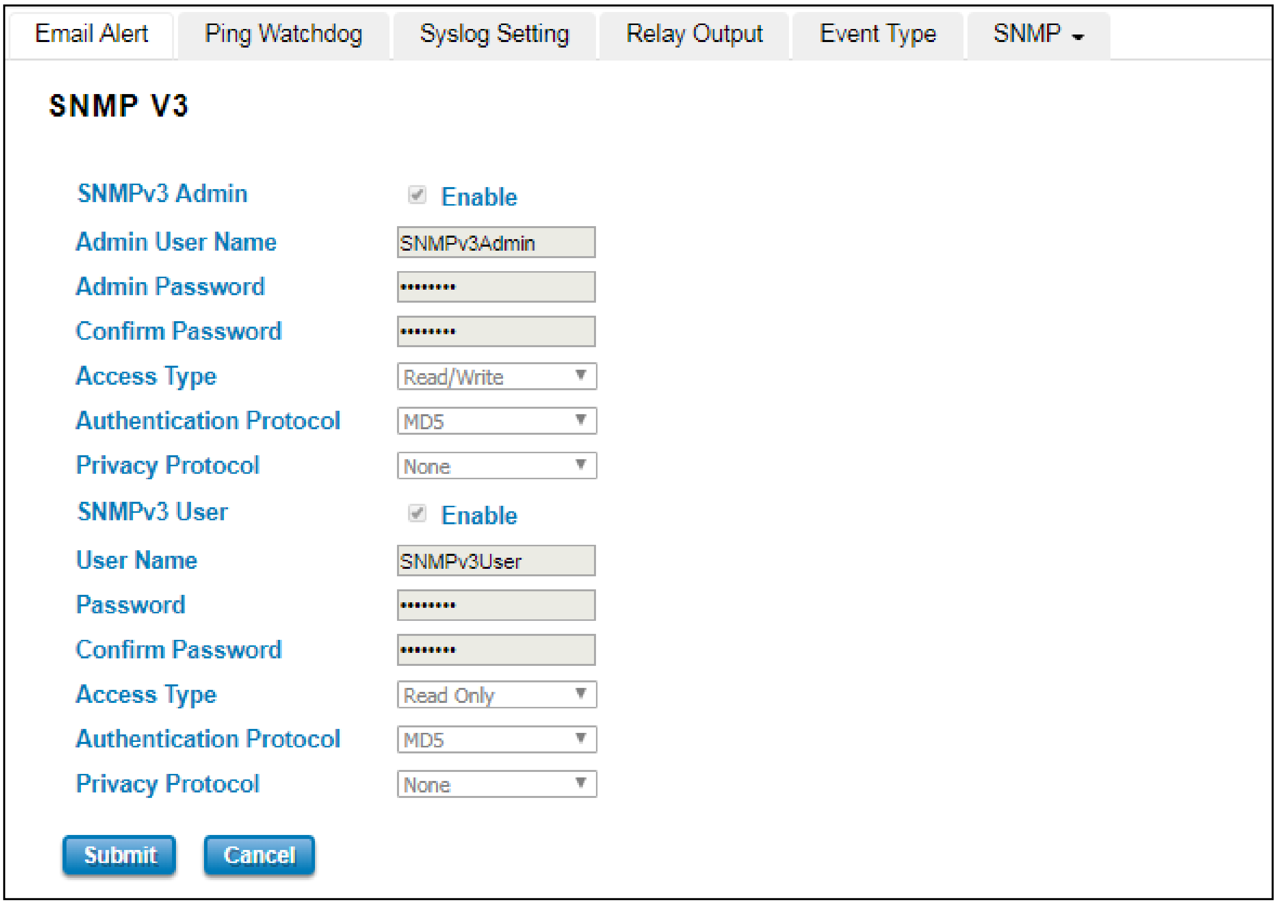
SNMP trap is the most frequently used SNMP messages. These messages are sent to the manager by an agent when an issue needs to be reported. SNMP traps are quite unique if compared to other message types, since they are the only method that can be directly initiated by an SNMP agent. The other types of messages are either initiated by the SNMP manager or sent as a result of the manager's request. This ability makes SNMP traps indispensable in most networks. It is the most convenient way for an SNMP agent to inform the manager that something wrong is going on. The description of the columns is as below:

TERMS	DESCRIPTION
SNMP Trap	Clicks enable to activate the function. All of events that associated with the device will be sent to the server in real time, and can be seen by remote clients
Trap Server	**Default: 0.0.0.0** Set the IP Address of the trap server where to report the events.
Trap Community	**Default: public** Create the name for a group or community of administrators who can allow to report the events. If the the group is match then the events can be reported.

After finish with the configuration, clicks **Submit** to activate the function.

3.5.6.2 SNMP V3

SNMP v3 can provide more security functions when the user performs remote management through SNMP protocol. This field displays the SNMPv3 configuration page for Admin and User. If the value from Access Type is set to **Read-Write,** the SNMPv3 user will be able to set and retrieve parameters on the system. And if the value is set to **Read Only,** the SNMPv3 user will only be able to retrieve parameter information. It delivers SNMP information to the administrator with user authentication; all of data between the router and the administrator are encrypted to ensure secure communication. SNMPv3 requires an authentication level of MD5 or DES to encrypt data to enhance data security. To activate the page make sure user has already choose SNMPv3 at the SNMP Setting page.



SNMP V3

SNMPv3 Admin	☑ Enable
Admin User Name	SNMPv3Admin
Admin Password	••••••••
Confirm Password	••••••••
Access Type	Read/Write
Authentication Protocol	MD5
Privacy Protocol	None
SNMPv3 User	☑ Enable
User Name	SNMPv3User
Password	••••••••
Confirm Password	••••••••
Access Type	Read Only
Authentication Protocol	MD5
Privacy Protocol	None

TERMS	DESCRIPTION
SNMPv3 Admin	Clicks enable to activate the function and the entries for SNMPv3 Admin.
Admin User Name	**Default: SNMPv3Admin** Set up the User Name for the SNMPv3 Admin
Admin Password	Set up the Password for the SNMPv3 Admin
Confirm Password	Confirm the Admin for the SNMPv3 Admin
Access Type	Access type for the SNMPv3 Admin, choose Read Only or Read and Write
Authentication Protocol	**Default: MD5** Provides authentication based on MD5 or SHA algorithms.

Privacy Protocol	Specify the encryption method for SNMP communication. None and DES are available. **None**: No encryption is applied. **DES**: Data Encryption Standard, it applies a 58-bit key to each 64-bit block of data.
SNMPv3 User	Clicks enable to activate the function and the entries for SNMPv3 User
User Name	**Default: SNMPv3User** Set up the User Name for the SNMPv3 User
Password	Set up the Password for the SNMPv3 User
Confirm Password	Confirm the Admin for the SNMPv3 User
Access Type	Access type for the SNMPv3 User, choose Read Only or Read and Write
Authentication Protocol	**Default: MD5** Provides authentication based on MD5 or SHA algorithms.
Privacy Protocol	Specify the encryption method for SNMP communication. None and DES are available. **None**: No encryption is applied. **DES**: Data Encryption Standard, it applies a 58-bit key to each 64-bit block of data.

3.6 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:

3.6.1 LLDP Setting

3.6.2 MAC Table

3.6.3 Port Statistics

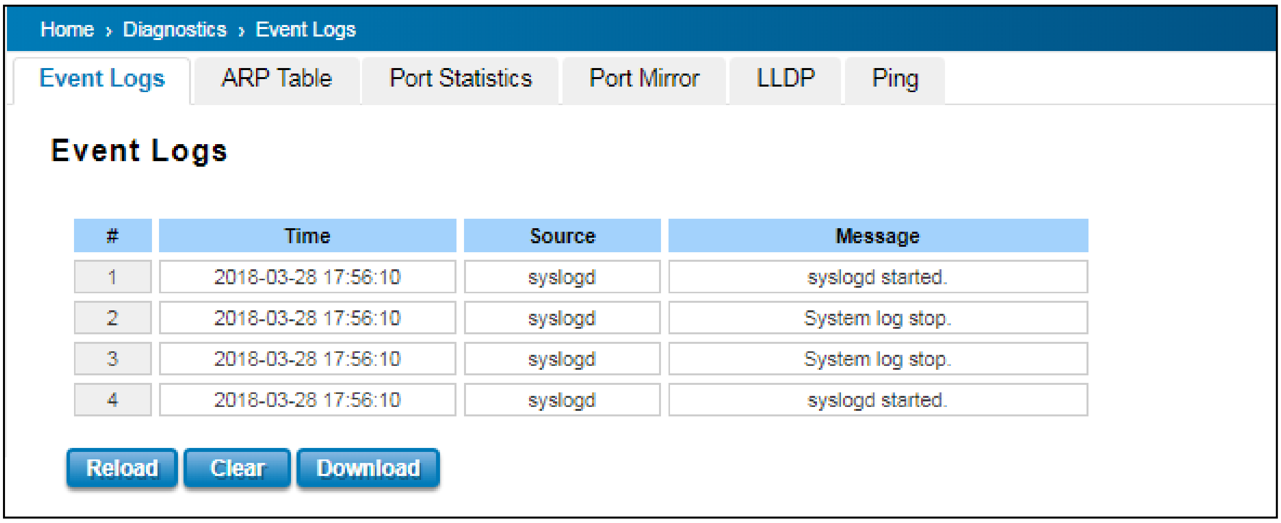
3.6.4 Port Mirror

3.6.5 Event Log

3.6.6 Ping

3.6.1 EVENT LOGS

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



Event Logs

#	Time	Source	Message
1	2018-03-28 17:56:10	syslogd	syslogd started.
2	2018-03-28 17:56:10	syslogd	System log stop.
3	2018-03-28 17:56:10	syslogd	System log stop.
4	2018-03-28 17:56:10	syslogd	syslogd started.

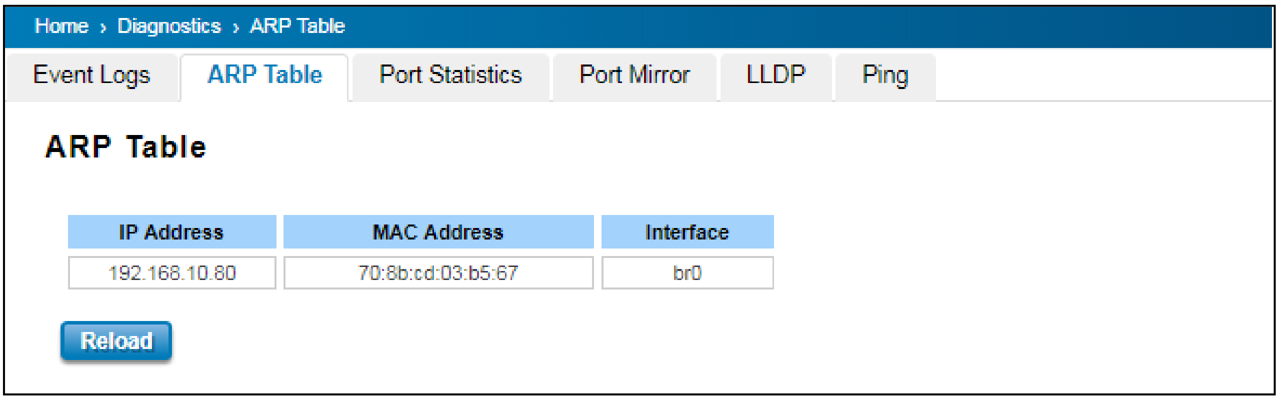
Click on **Clear** to clear the entries. Click on **Reload** to refresh the table. Click on **Download** to download the event logs

The description of the columns is as below:

TERMS	DESCRIPTION
#	Event index assigned to identify the event sequence.
Time	The date is updated based on how the current date is set in the Basic Setting page.
Source	The time is updated based on how the current time is set in the Basic Setting page.
Message	The occurred events.

3.6.2 ARP TABLE

Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a physical machine address that is recognized in the local network. In this section user may get the information about the ARP information on the switch.



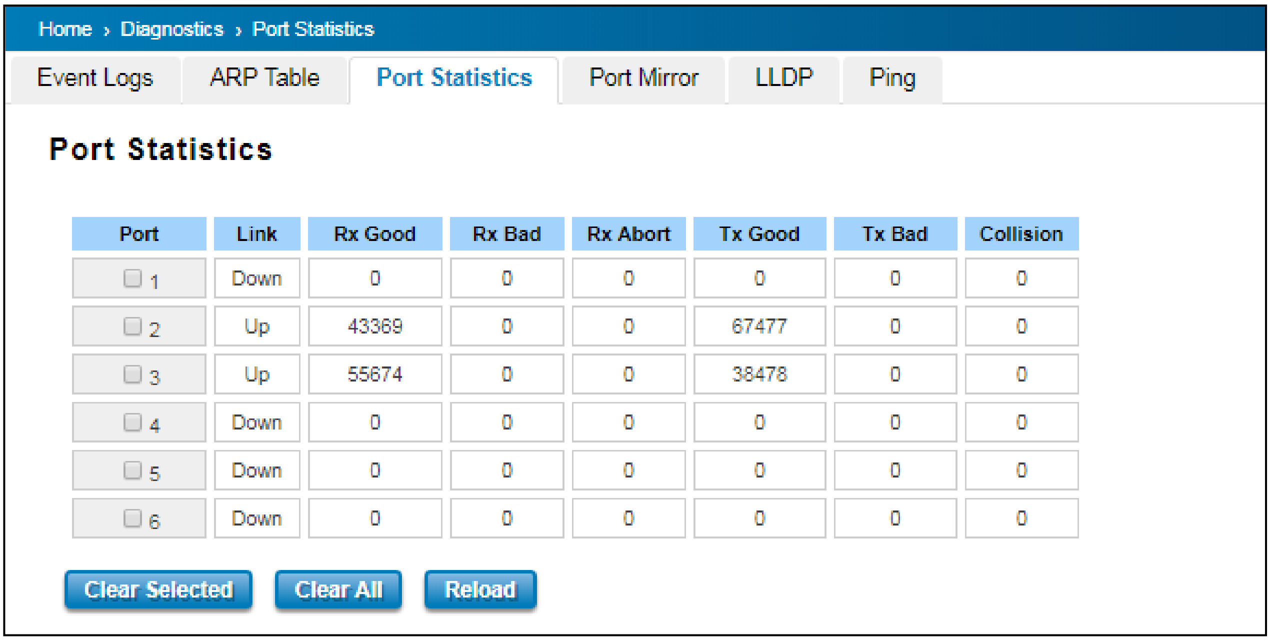
ARP Table

IP Address	MAC Address	Interface
192.168.10.80	70:8b:cd:03:b5:67	br0

In this page, users can see the IP Address, MAC Address, and the interface. Click on **Reload** to refresh the table to get specific information based.

3.6.3 PORT STATISTICS

This page displays the number of packets that is received and sent from the port. 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 Port, Link, Rx Good, Rx Bad, Rx Abort, Tx Good, Tx Bad and Collision.



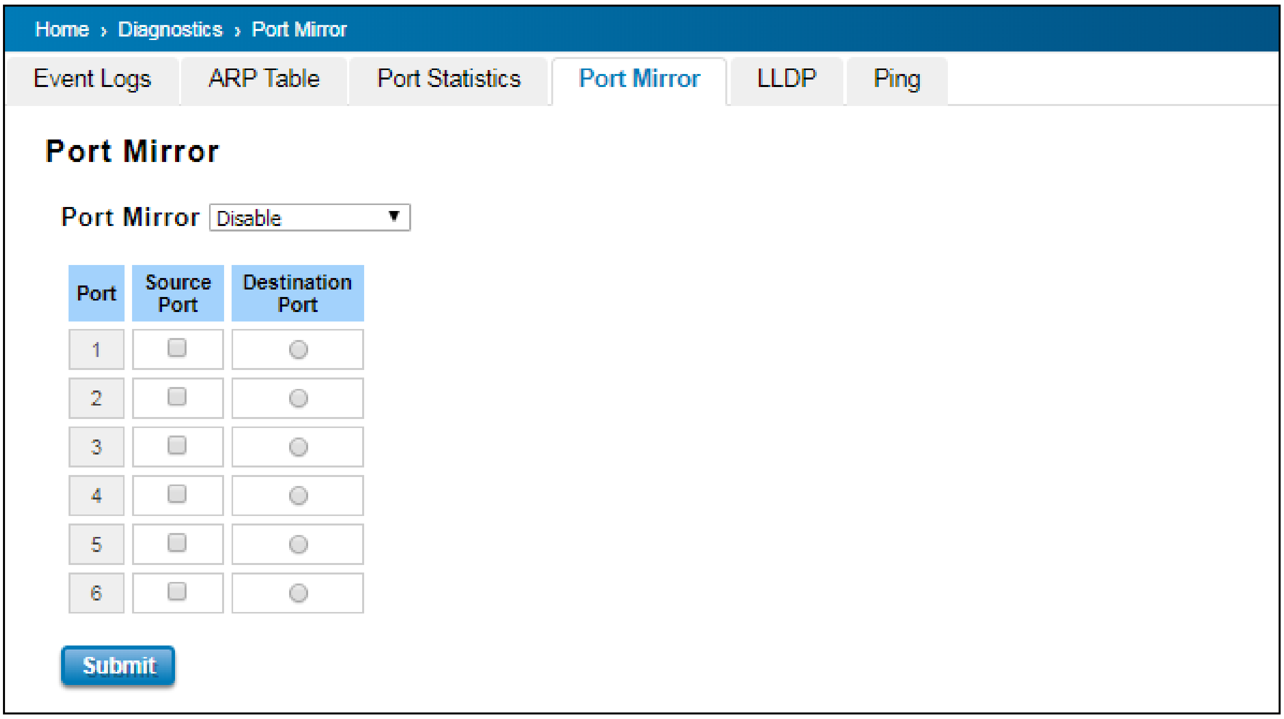
Port Statistics

Port	Link	Rx Good	Rx Bad	Rx Abort	Tx Good	Tx Bad	Collision
□ 1	Down	0	0	0	0	0	0
□ 2	Up	43369	0	0	67477	0	0
□ 3	Up	55674	0	0	38478	0	0
□ 4	Down	0	0	0	0	0	0
□ 5	Down	0	0	0	0	0	0
□ 6	Down	0	0	0	0	0	0

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

3.6.4 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.



Port Mirror

Port Mirror: Disable

Port	Source Port	Destination Port
1	□	○
2	□	○
3	□	○
4	□	○
5	□	○
6	□	○

The configuration and settings explain as following.

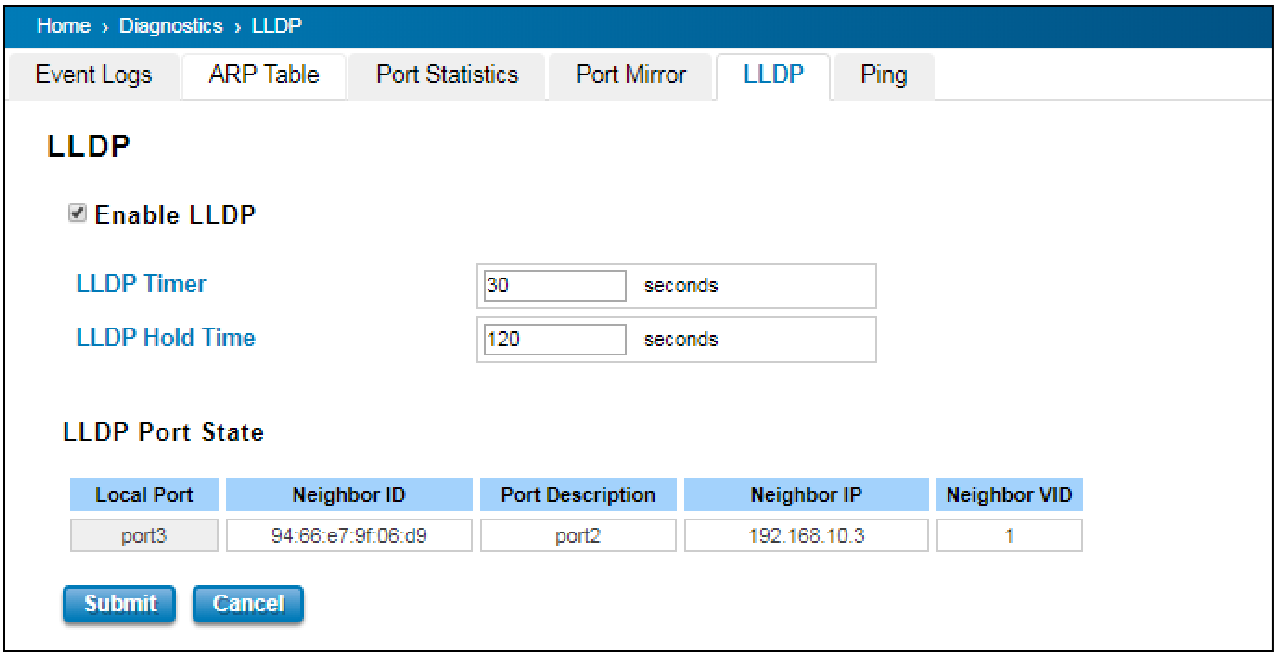
TERMS	DESCRIPTION
Port Mirror	Select Enable/Disable to enable/disable Port Mirror.
Source Port	These are the ports that User wants to monitor. The traffic of all source ports will be duplicated to destination ports. User can choose a single port, or multiple ports. Click on checkbox of the Port ID, RX, 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.

3.6.5 LLDP

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.



LLDP

☑ Enable LLDP

LLDP Timer 30 seconds

LLDP Hold Time 120 seconds

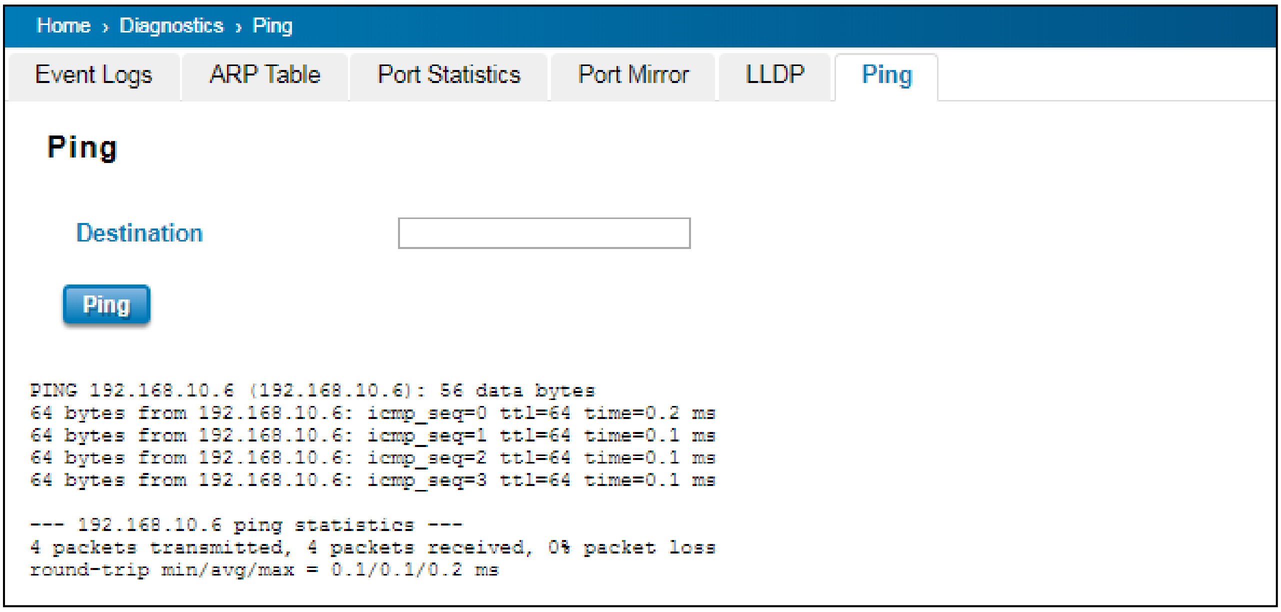
LLDP Port State

Local Port	Neighbor ID	Port Description	Neighbor IP	Neighbor VID
port3	94:66:e7:9f:06:d9	port2	192.168.10.3	1

TERMS	DESCRIPTION
Enable LLDP	Check the box to enable/disable LLDP function.
LLDP Timer	**Default: 30 seconds** 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; the valid number is from 10 to 255.
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.
Port Description	The port number from 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.

3.6.6 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.

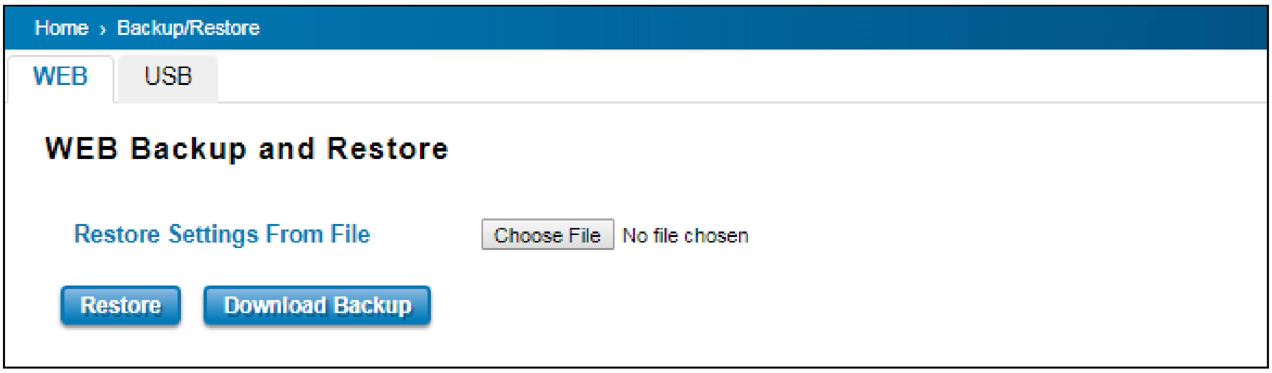


```
PING 192.168.10.6 (192.168.10.6): 56 data bytes
64 bytes from 192.168.10.6: icmp_seq=0 ttl=64 time=0.2 ms
64 bytes from 192.168.10.6: icmp_seq=1 ttl=64 time=0.1 ms
64 bytes from 192.168.10.6: icmp_seq=2 ttl=64 time=0.1 ms
64 bytes from 192.168.10.6: icmp_seq=3 ttl=64 time=0.1 ms

--- 192.168.10.6 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.2 ms
```

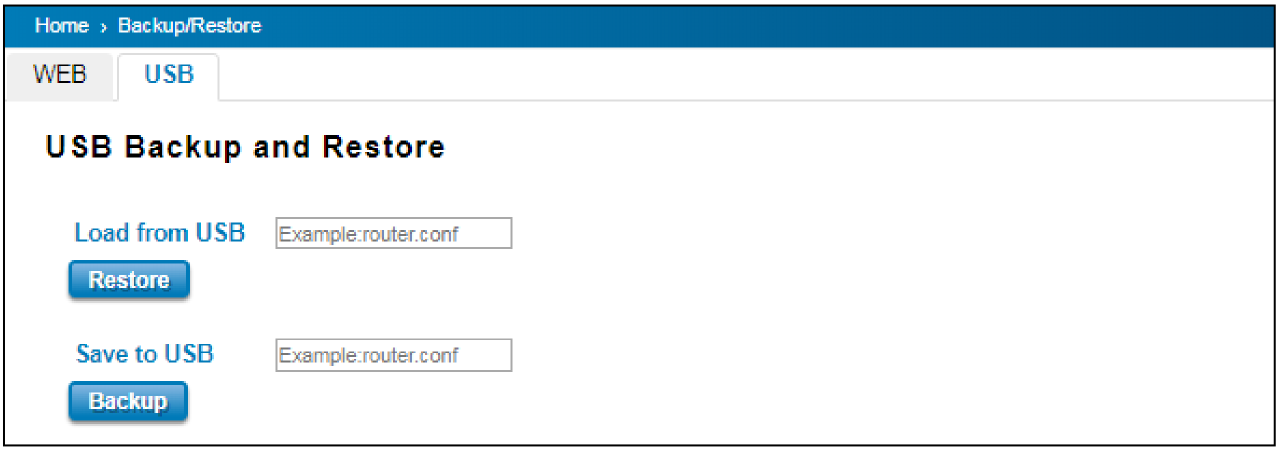
3.7 BACKUP AND RESTORE

User can use WoMaster's 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 directly click Download Backup to get the backup file. To restore the configuration, user may 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.

USB mode: this mode has two functions, **Load from USB** and **Save to USB**. Load from USB, 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. To read the backup file, please type the specific filename. 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**.

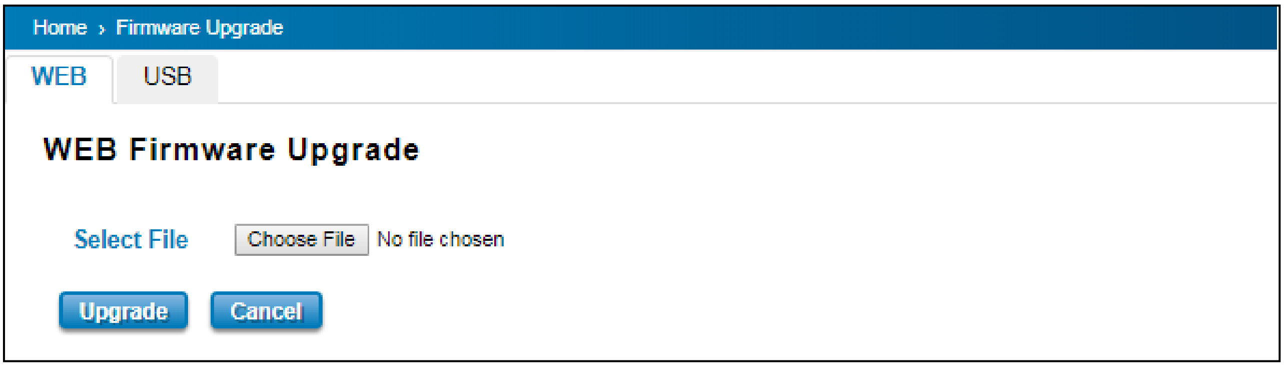


3.8 FIRMWARE UPGRADE

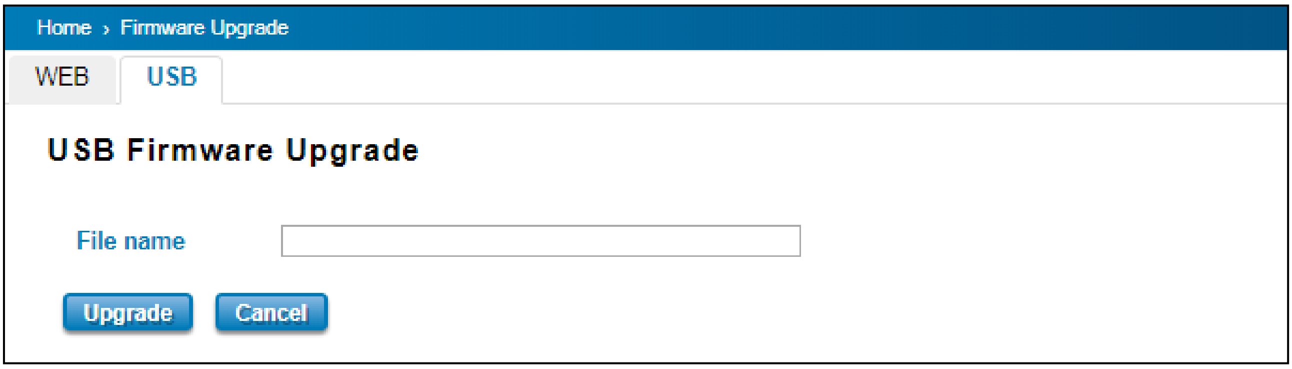
WoMaster provides the latest firmware online at www.womaster.eu. The new firmware may include new features, bug fixes or other software changes. WoMaster also provide the release notes for the update as well. For technical viewpoint, WoMaster suggests user uses the latest firmware before installing the 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 select the existed upgrade file. This mode is only provided by Web UI while CLI is not supported.



USB Firmware Upgrade

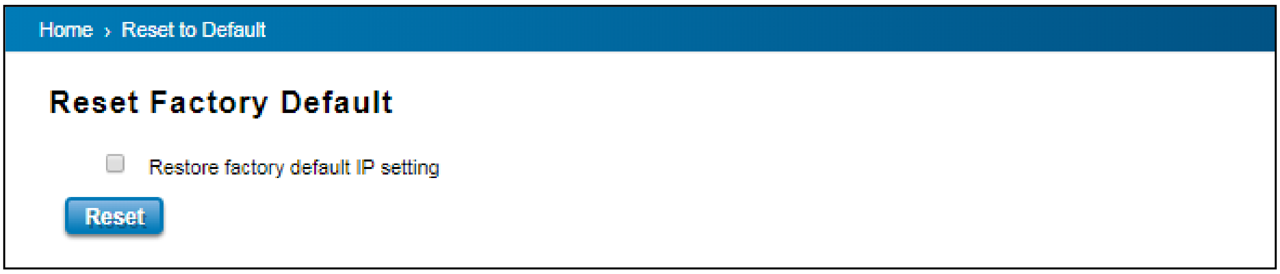
File name

USB mode: plugged in the USB device with the firmware file, then it will directly show the new firmware file on the box. Then click **Upgrade**. The restart session would start directly after the new firmware has been uploaded.

3.9 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

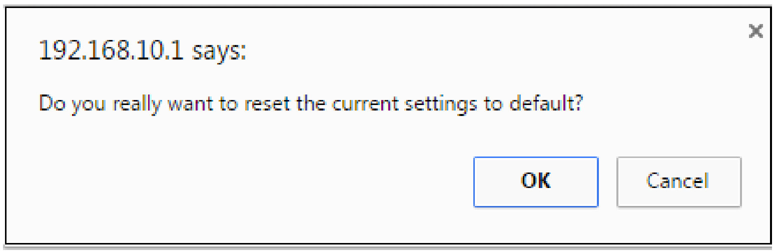


Reset Factory Default

□ Restore factory default IP setting

The factory default function has two different reset function, the first one is if user just directly click the Reset button without check the Restore factory default IP Setting, it means the reset function just reset the configuration without reset the IP Address (use the IP Address that assigned by user). But if user checks the Restore factory default IP setting, it means reset all of the configurations include the IP Address set back to the **Default IP, 192.168.10.1.**

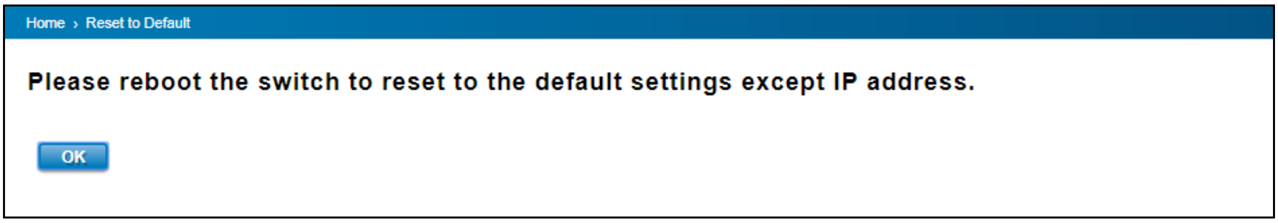
Pop-up message screen to show User that have done the command. Click on **OK** to close the screen.



192.168.10.1 says:

Do you really want to reset the current settings to default?

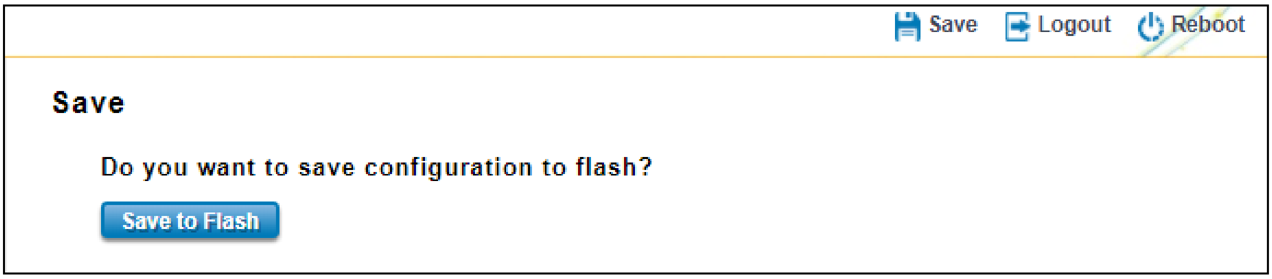
Then please go to **Reboot** page to reboot the switch. Click **OK.** The system will auto reboot the device.



Please reboot the switch to reset to the default settings except IP address.

3.10 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.

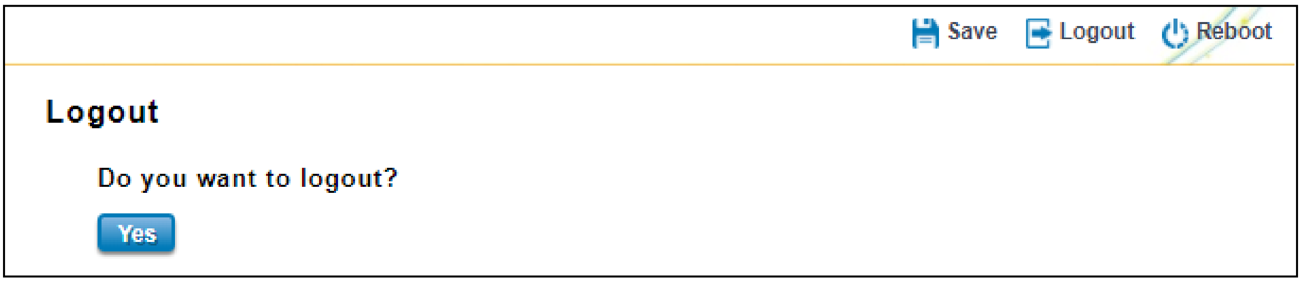


Save

Do you want to save configuration to flash?

3.11 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.



Logout

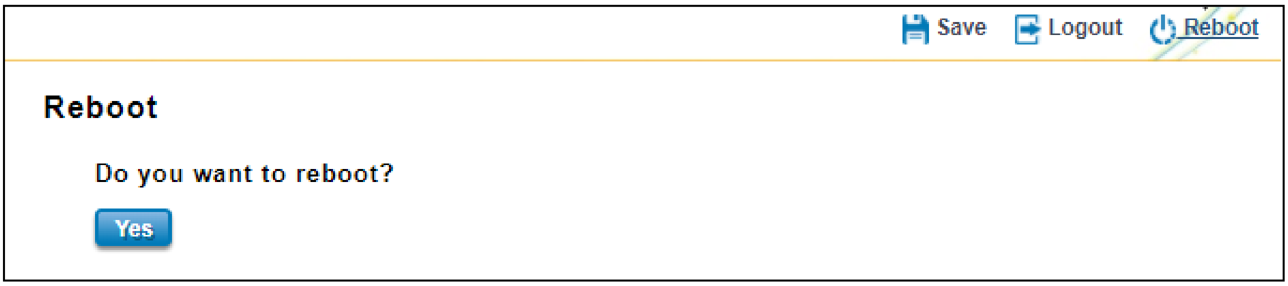
Do you want to logout?

3.12 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.



Reboot

Do you want to reboot?

4. SPECIFICATIONS

INTERFACE	DS306
Ethernet Port	4 x 100/1000MBase-T RJ45, Auto Negotiation 2 x 100BaseFX, ST or SC Connector
System LED	2 x Power: Green On 1 x SYS: Ready: (Green On), Firmware Updating: (Green Blinking) 1 x DO: Red On 2 x Fiber: Link (Green On), Activity (Green Blinking) 1 x Ring: Off: Ring disabled, Green On: Ring normal (Not RPL Owner), Green Blinking: Ring normal (RPL Owner) 1 x Ra: Green On: Ring abnormal, Green Blinking: Ring port fail
Ethernet Port LED	Link (Green On), Activity (Green Blinking)
Reset	System Reset(2~6 Seconds) / Default Settings Reset(over 7 Seconds)
USB	1 x USB for Configuration/Firmware Update
Power Input, Digital Input, Digital Output	6-Pin Removable Terminal Block Connector 4 Pin for Redundant Power 2 Pin for DO (Relay Alarm) DO: Dry Relay Output with 0.5A/24V DC

Optical Fiber					
	Distance	Wavelength	TX Range	RX Range	Link budget
Single-Mode	30KM	1310 (1280~1340)	-8~-15dBm	-3~-34dBm	19dB
Multi-Mode	2KM	1310 (1260~1360)	-10~-20dBm	-3~-32dBm	12dB

Power Requirement	
Input Voltage	24VDC (18~60VDC)
Reverse Polarity Protect	Yes
Input Current	0.3A@24V
Power Consumption	Max 7.2W@24VDC full loading, suggest to reserve 15% tolerance