

COVER

User Manual

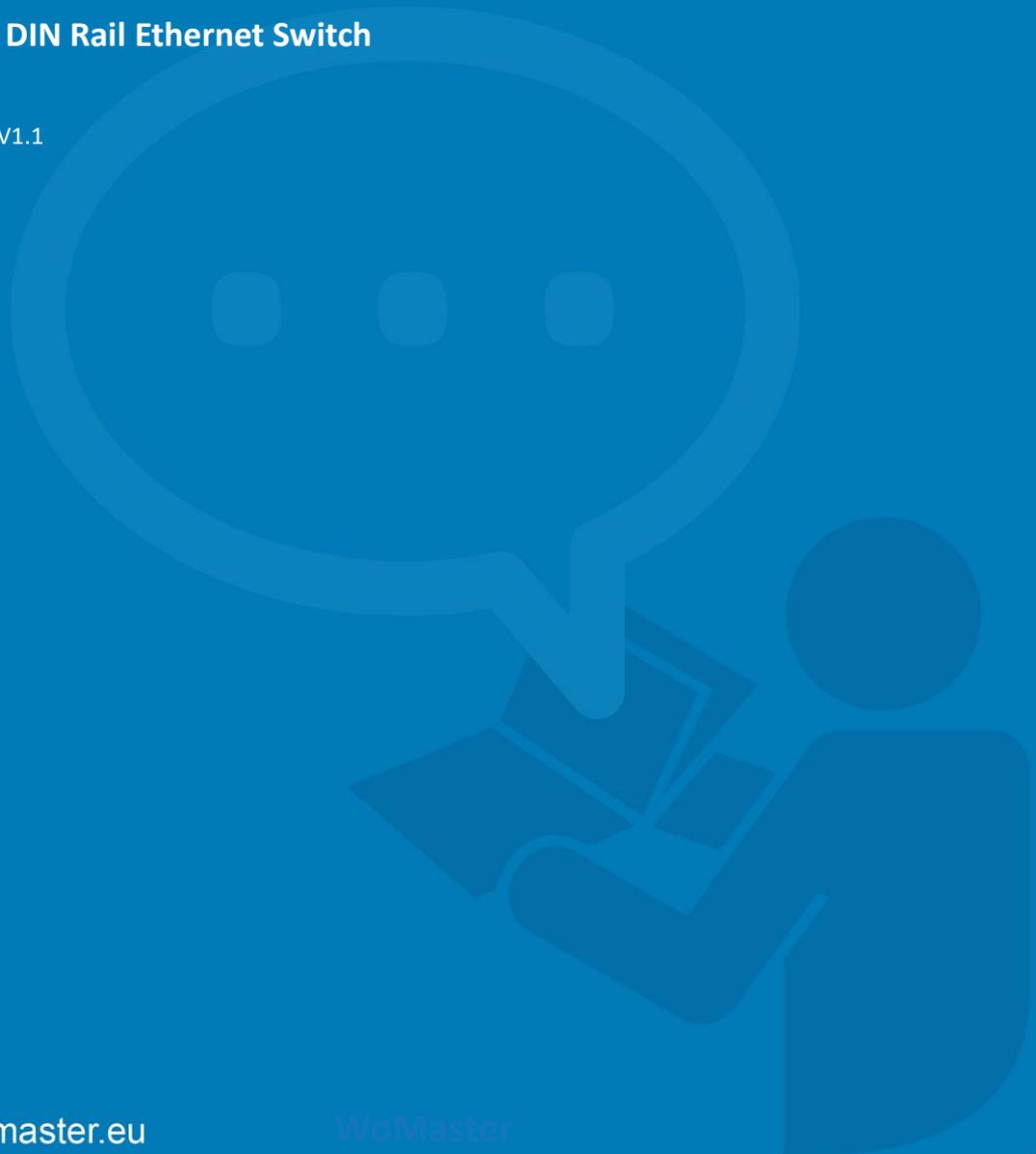
DP310

Industrial DIN Rail PoE Switch

DS310

Industrial DIN Rail Ethernet Switch

May.07.2019 V1.1



WoMaster

DP310 Industrial DIN rail PoE switch
DS310 Industrial DIN rail Ethernet switch

User Manual

Copyright Notice

© WoMaster. All rights reserved.

About This Manual

This user manual is intended to guide a professional installer to install and to configure the DP310 and DS310 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	6
1.1 OVERVIEW	6
1.2 MAJOR FEATURES	7
2. HARDWARE INSTALLATION.....	8
2.1 HARDWARE DIMENSION	8
2.2 WIRING THE POWER INPUTS	10
2.3 WIRING THE ALARM RELAY OUTPUT (DO)	11
2.4 WIRING THE DIGITAL INPUT (DI)	12
2.5 CONNECTING THE GROUING SCREW	13
2.6 DIN RAIL MOUNTING	13
3. WEB MANAGEMENT CONFIGURATION	14
3.1 SYSTEM.....	16
3.1.1 INFORMATION	16
3.1.2 USER ACCOUNT	17
3.1.2.1 LOCAL USER	17
3.1.2.2 RADIUS SERVER	18
3.1.3 IP SETTING	19
3.1.3.1 IPv4	19
3.1.3.2 IPv6	20
3.1.4 DATE AND TIME	22
3.1.4.1 NTP SETTING	22
3.1.4.2 PTP SETTING	24
3.1.5 DHCP SERVER.....	25
3.2 ETHERNET PORT.....	31
3.2.1 PORT SETTING.....	31
3.2.2 PORT STATUS.....	32
3.2.3 RATE CONTROL	33
3.2.4 PORT TRUNK	34
3.3 POWER OVER ETHERNET (DP310 ONLY).....	37
3.3.1 PoE STATUS.....	37
3.3.2 PoE CONTROL.....	38
3.3.3 PoE SCHEDULING	40

3.3.4 ALIVE CHECK	40
3.3.5 PoE EVENT	41
3.4 REDUNDANCY	42
3.4.1 RSTP SETTINGS	42
3.4.2 MSTP SETTINGS.....	46
3.4.3 ERPS SETTINGS	49
3.4.3.1 ERPS SETTINGS	50
3.4.3.2 ERPS STATUS	52
3.4.4 LOOP PROTECTION.....	55
3.5 VLAN	56
3.5.1 VLAN SETTING	57
3.5.2 VLAN PORT SETTING	59
3.5.3 VLAN STATUS	60
3.5.4 PVLAN SETTING	60
3.5.5 PVLAN PORT SETTING	61
3.5.6 PVLAN STATUS	62
3.5.7 GVRP SETTING.....	63
3.6 QUALITY OF SERVICE (QoS)	64
3.6.1 QoS SETTING	64
3.6.2 CoS MAPPING	65
3.6.3 DSCP MAPPING	66
3.7 MULTICAST	67
3.7.1 IGMP QUERY	68
3.7.2 IGMP SNOOPING.....	69
3.7.3 GMRP SETTING	70
3.8 SNMP.....	71
3.8.1 SNMP V1/V2c SETTING	71
3.8.2 SNMP V3	72
3.8.3 SNMP TRAP.....	73
3.9 SECURITY	74
3.9.1 PORT SECURITY	74
3.9.2 IP SECURITY.....	75
3.9.3 IEEE 802.1x.....	76
3.10 INDUSTRIAL.....	80
3.10.1 Modbus TCP/IP	80
3.11 WARNING	91
3.11.1 RELAY OUTPUT.....	91
3.11.2 EVENT TYPE.....	92
3.11.3 SYSLOG SETTING	93
3.11.4 EMAIL ALERT	94

3.12 DIAGNOSTICS.....	95
3.12.1 LLDP SETTING	95
3.12.2 MAC TABLE	96
3.12.3 PORT STATISTICS.....	98
3.12.4 PORT MIRROR	99
3.12.5 EVENT LOGS	100
3.12.6 PING.....	100
3.13 BACKUP AND RESTORE	101
3.14 FIRMWARE UPGRADE	102
3.15 RESET TO DEFAULTS.....	103
3.16 SAVE	104
3.17 LOGOUT	104
3.18 REBOOT	104
3.19 FRONT PANEL.....	105
4. SPECIFICATIONS	錯誤! 尚未定義書籤。

1. INTRODUCTION

1.1 OVERVIEW

DP310/DS310 is Womaster Managed Switch that provides 8-port Fast Ethernet, where DP310'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 DP310/DS310 provides 2 RJ45/SFP Gigabit Ethernet combo ports that can prioritize stream, such as video and also optimize VoIP. Gigabit Ethernet combo ports provides high speed uplink connection to higher level backbone switches with Ring Network Redundancy technology ensures the reliability of high-quality video transfer. 100/1000Mbps 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 DP310/DS310 for surveillance data transmission under vibration and shock in rolling stocks, traffic control systems and other harsh environments.

This managed 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.

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 DP310/DS310 Switch:

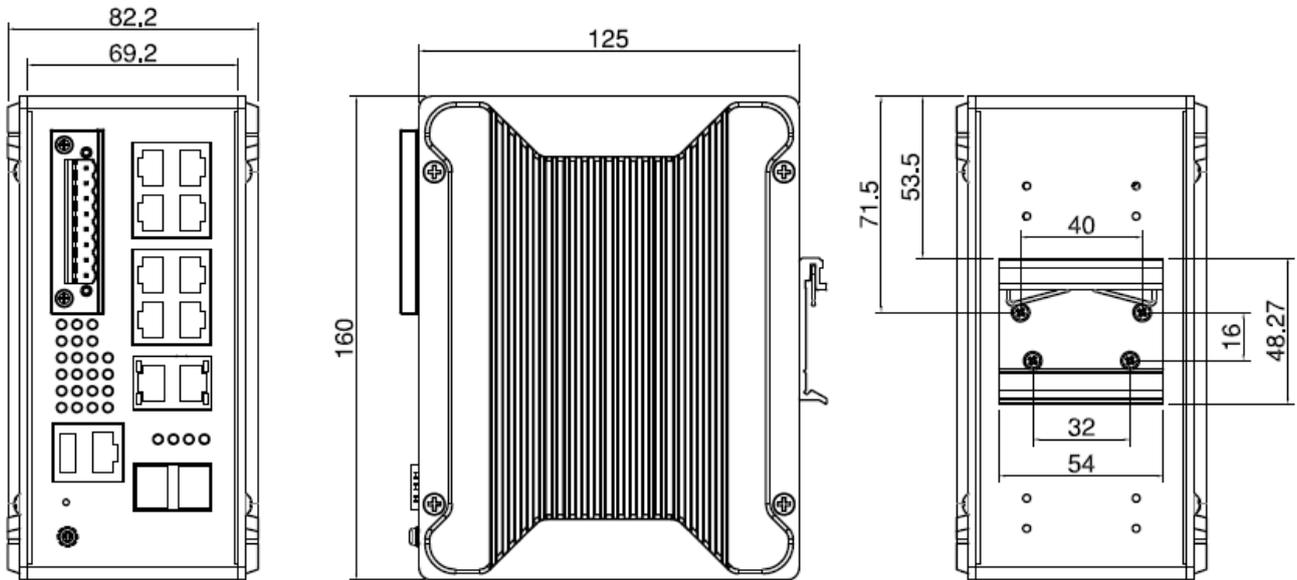
- 8 x 10/100 Base-TX PoE ports and 2 x 10/100/1000 RJ-45/ SFP combo ports
- IEEE 802.3af 15.4W / IEEE 802.3at 30W High Power PoE (DP310)
- 240W ultra high PoE budget and excellent power efficiency even in 75°C operating temperature (DP310)
- SFP ports support 100/1000 Mbps with Digital Diagnostic Monitoring (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
- IP30 ingress protection

2. HARDWARE INSTALLATION

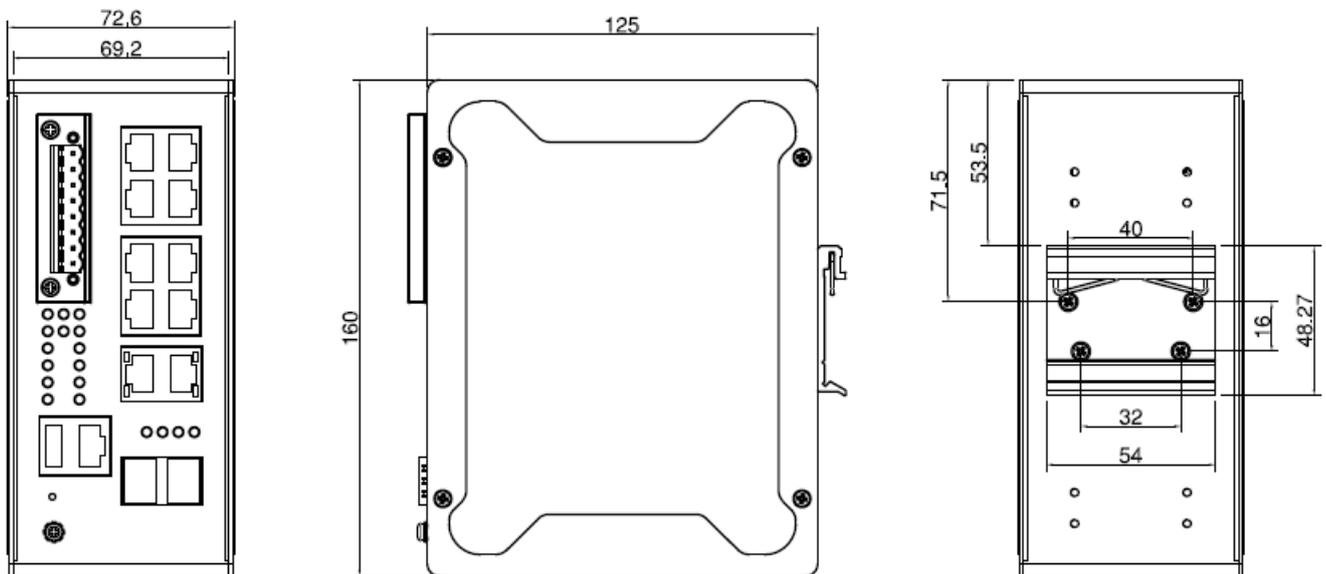
This chapter introduces hardware, and contains information on installation and configuration procedures.

2.1 HARDWARE DIMENSION

Dimensions of DP310: 82.2 x 160 x 125 (W x H x D) / without DIN Rail Clip



Dimensions of DS310: 82.2 x 160 x 125 (W x H x D) / without DIN Rail Clip



Front Panel Layout

The front panel from DP310 and DS310 switches include 8 ports Fast Ethernet, Dual Gigabit Uplink (RJ45/SFP combo 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 DP310 it is provided with PoE LED. On the rear side of switch there is DIN rail clip attached.

DP310

Integrated Power Connector

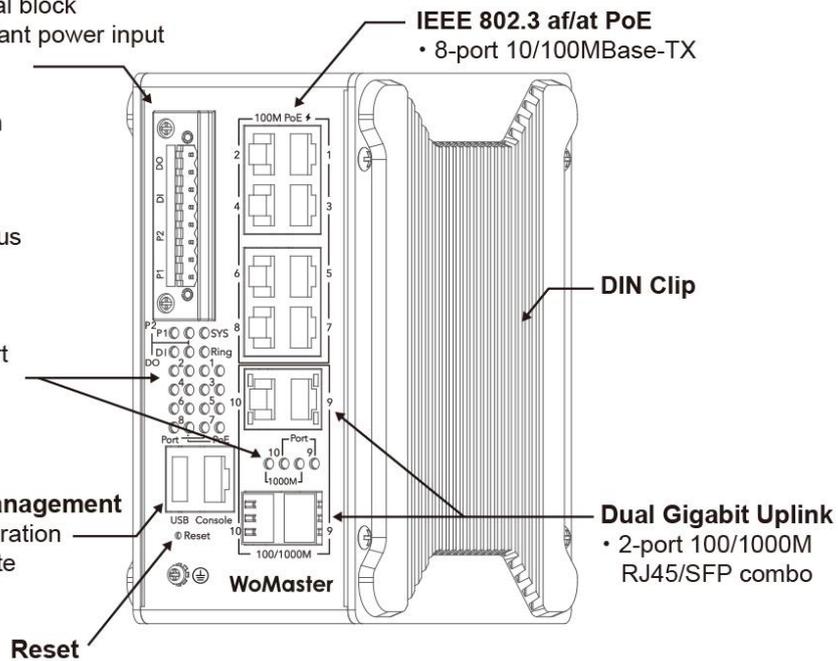
- 1 x 8-pin terminal block
- 4 pin for redundant power input
- 2 pin DI
- 2 pin DO
- Easy Installation

System LED

- 2 x Power
- 1 x System Status
- 1 x DO
- 1 x DI
- 1 x Ring Status
- 8 x Ethernet Port
- 8 x PoE
- 2 x SFP Port
- 2 x SFP 1000M

Easy System Management

- USB for Configuration /Firmware update
- RS232 console



DS310

Integrated Power Connector

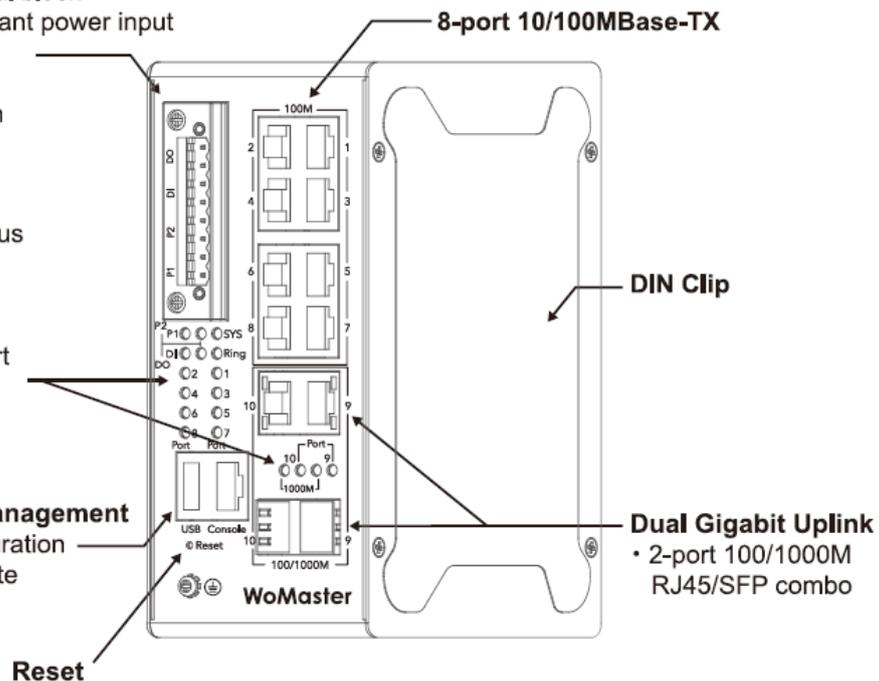
- 1 x 8-pin terminal block
- 4 pin for redundant power input
- 2 pin DI
- 2 pin DO
- Easy Installation

System LED

- 2 x Power
- 1 x System Status
- 1 x DO
- 1 x DI
- 1 x Ring Status
- 8 x Ethernet Port
- 2 x SFP Port
- 2 x SFP 1000M

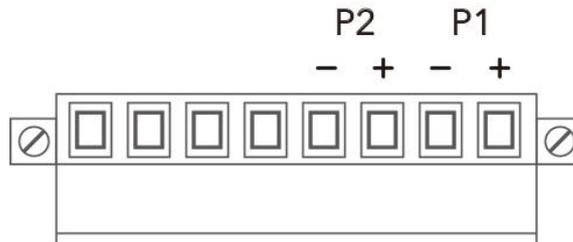
Easy System Management

- USB for Configuration /Firmware update
- RS232 console



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.



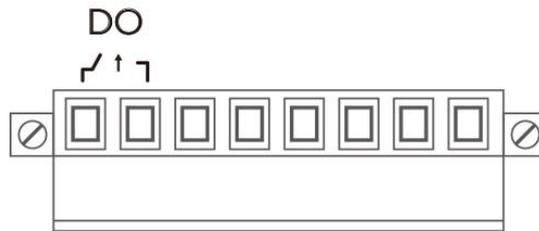
Wiring the Power Input

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)

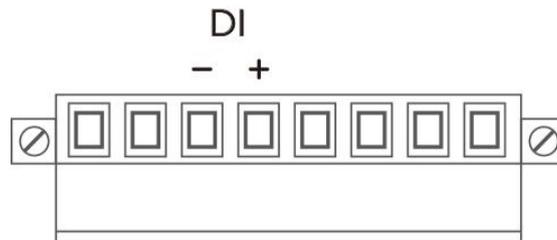
The relay output contacts are located on the front panel of the switch. The relay output consists of the 2-pin terminal block connector that used to detect user-configured events. The two wires attached to the fault contacts form a close circuit when a user-configured event is triggered. If a user-configured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

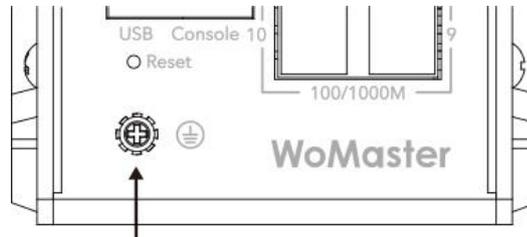
STEP 1: Insert the negative and positive wires into the -/+ terminals, respectively.

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 GROUING SCREW

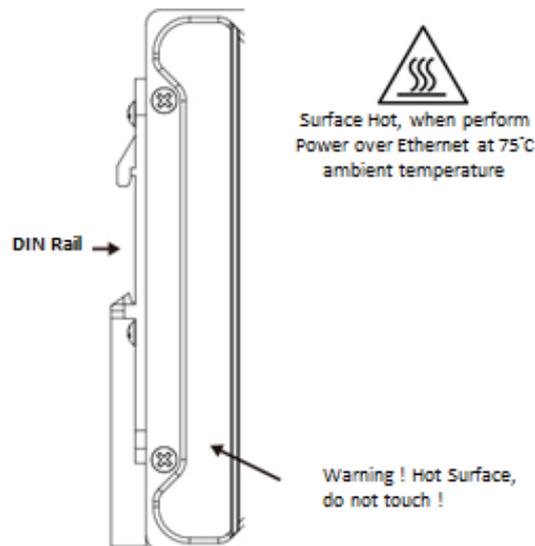
Grounding screw is located on the front side of the switch. Grounding Screw helps limit the effects of noise due to electromagnetic interference (EMI) such as lightning or surge protection. Run the ground connection from the ground screw to the grounding surface prior to connecting devices. And tighten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



Grounding Screw

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.

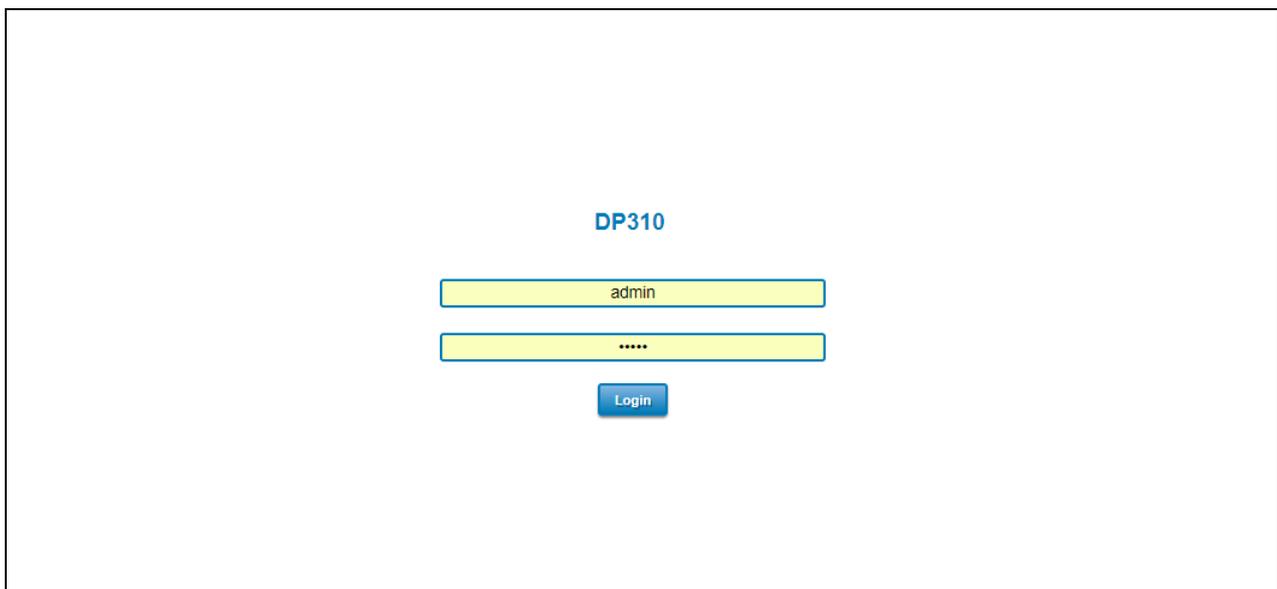
3. WEB MANAGEMENT CONFIGURATION

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 192.168.1.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**.



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 Power over Ethernet (PoE Models only)
- 3.4 Redundancy
- 3.5 VLAN
- 3.6 QoS
- 3.7 Multicast
- 3.8 SNMP
- 3.9 Security
- 3.10 Warning
- 3.11 Diagnostics
- 3.12 Backup / Restore
- 3.13 Firmware Upgrade
- 3.14 Reset to Defaults
- 3.15 Save
- 3.16 Logout
- 3.17 Reboot
- 3.18 Front Panel

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 screenshot shows the 'Information' configuration page for a DP310 Industrial Managed Switch. The page has a breadcrumb trail 'Home > System > Information' and a navigation menu with tabs for 'Information', 'User Account', 'IP Setting', 'Date and Time', and 'DHCP Server'. The main content area is titled 'DP310 Industrial Managed Switch' and contains several configuration fields: 'System Name' (value: switch), 'System Location', 'System Contact', 'OID' (value: 1.3.6.1.4.1.47114.1.1.1), 'System Description' (value: DP310 Industrial Managed Ethernet Switch), 'Software Version' (value: 1.0-1504148492), and 'MAC Address' (value: 94:66:E7:12:09:33). A 'Submit' button is located at the bottom left of the form.

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 Location	Default: Blank User can specify the switch's physical location.
System Contact	Default: Blank 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.

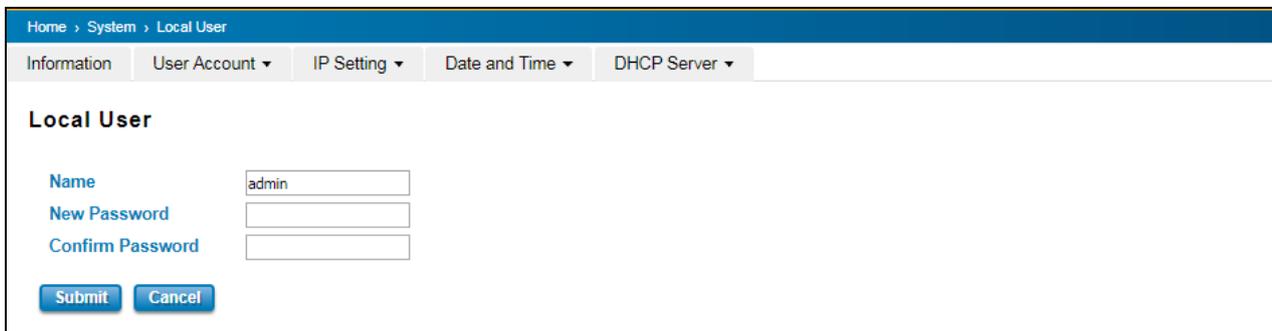
After finish the configuration, click on **Submit** to apply User settings.

3.1.2 USER ACCOUNT

Womaster'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 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 Key in new user name here.
New Password	Default: admin 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.

Home > System > RADIUS Server

Information | **User Account** | IP Setting | Date and Time | DHCP Server

RADIUS Authentication

RADIUS Server 1

RADIUS Server IP

Shared Key

Server Port

RADIUS Server 2

RADIUS Server IP

Shared Key

Server Port

How to set up a RADIUS server:

- Enter the IP address of the RADIUS server in **Server IP Address**
- Enter the **Shared Secret** of the RADIUS server
- Enter the **Server port** if necessary, by default RADIUS server listens to port 1812
- 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

The screenshot shows the 'IP Setting' configuration page. At the top, there is a breadcrumb trail: 'Home > System > IPv4 Setting'. Below this, there are navigation tabs: 'Information', 'User Account', 'IP Setting', 'Date and Time', and 'DHCP Server'. The 'IP Setting' tab is active. Underneath, the 'DHCP Client' is set to 'Disable' with a dropdown arrow. A blue 'Submit' button is located at the bottom left of the configuration area.

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 screenshot shows the 'IPv4 Configuration' page. It contains five input fields: 'IP Address' with the value '192.168.22.4', 'Subnet Mask' with '255.255.255.0', 'Default Gateway' with '192.168.22.254', 'DNS Server 1', and 'DNS Server 2'. A blue 'Submit' button is located at the bottom left.

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 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 Assign the subnet mask for the IP address here. If DHCP Client function is

	enabled, no needs to assign the subnet mask.
Default Gateway	Default: 192.168.10.254. 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

IPv6 Setting

IPv6 Address Prefix Length

IPv6 Default Gateway

IPv6 Address

fe80::9666:e7ff:fe12:933/64

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 network, 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 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.

Neighbor Cache

IPv6 Address	Interface	Link Layer (MAC) Address	State
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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 NTP 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.

Date and Time

Current Time Yr 2017 Mon 01 Day 1 Hr 05 Mn 34 Sec 28

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

NTP Enable NTP client update

1st Time Server N/A

2st Time server N/A

Daylight saving Time Disable ▼

Daylight Saving Start 1st ▼ Sun ▼ in Jan ▼ at 00 ▼ 00 ▼

Daylight Saving End 1st ▼ Sun ▼ in Jan ▼ at 00 ▼ 00 ▼

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.
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.

PTP Setting

Operation

Operation Mode

Synchronization Interval

Announce Interval

Announce Receipt Timeout

Minimum Delay Request Interval

Domain Number

Priority 1

Priority 2

Delay Mechanism

The description of the columns is as below:

TERMS	DESCRIPTION
Operation	Default: Disable 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 Choose Mode (Auto Elect, Preferred Master Clock or Slave)
Synchronization Interval	Default: 0 (1s) 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) Sets the announce message interval
Announce Receipt Timeout	Default: 6 The multiple of announce message receipt timeout by the announce message interval.
Minimum Delay Request Interval	Default: 1 (2s) 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 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 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 Configures the delay mechanism in boundary clock mode. E2E - The delay request or response mechanism used in the boundary clock mode. 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

DHCP Server Setting

Global Setting

Address Pool Setting

Network

Mask

Default Gateway

Lease Time(s)
(60~31536000 seconds)

The description of the columns is as below:

TERMS	DESCRIPTION
Global Setting	Select to Enable or Disable to activate and deactivate DHCP Server function.
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 screenshot shows the 'Excluded Address List' configuration page. At the top, there is a text input field labeled 'Excluded IP' with the value '192.168.10.10'. Below this is a blue 'Add' button. Underneath is a table with two columns: 'Index' and 'IP Address'. The table contains one row with the index '1' and the IP address '192.168.10.10'. At the bottom of the table are two buttons: 'Remove' and 'Reload'.

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**.

The screenshot shows the 'Static Port/IP Binding List' configuration page. It features two text input fields: 'Port' with the value '5' and 'IP Address' with the value '192.168.10.15'. Below these is a blue 'Add' button. Underneath is a table with three columns: 'Index', 'Port', and 'IP Address'. The table contains one row with the index '1', the port '5', and the IP address '192.168.10.15'. At the bottom of the table are two buttons: 'Remove' and 'Reload'.

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**.

Static MAC/IP Binding List

MAC Address

IP Address

Add

Index	MAC Address	IP Address
<input type="checkbox"/> 1	<input type="text" value="000f.fe4d.9196"/>	<input type="text" value="192.168.10.20"/>

Remove **Reload**

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**.

Option82/IP Binding List

Circuit ID

Remote ID

IP Address

Add

Index	Circuit ID	Remote ID	IP Address
<input type="checkbox"/> 1	<input type="text" value="01000101"/>	<input type="text" value="COA87FFD"/>	<input type="text" value="192.168.10.9"/>

Remove **Reload**

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.

DHCP Option 82

DHCP Relay Agent

Helper Address

Helper Address

<input type="checkbox"/>	Helper Address 1	<input type="text" value="192.168.10.19"/>
<input type="checkbox"/>	Helper Address 2	<input type="text"/>
<input type="checkbox"/>	Helper Address 3	<input type="text"/>
<input type="checkbox"/>	Helper Address 4	<input type="text"/>

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.

Relay Policy

Replace
 Keep
 Drop

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.

Circuit ID

Port 1 Default (VLAN/Port) User Defined

Port	Circuit ID	HEX value
1	00010001	00010001
2	00010002	00010002
3	00010003	00010003
4	00010004	00010004
5	00010005	00010005
6	00010006	00010006
7	00010007	00010007
8	00010008	00010008
9	00010009	00010009
10	0001000a	0001000a

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.

Remote ID

Default (MAC Address)
 IP Address
 User Defined

Remote ID	HEX value
94:66:e7:9f:98:34	9466e79f9834

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.

DHCP Leased Entries

Index	IP Address	MAC Address	Leased Time Remains
1	192.168.10.3	ac22.0b70.cd13	55

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.

Following items are included in this group:

3.2.1 Port Setting

3.2.2 Port Status

3.2.3 Rate Control

3.2.4 Port Trunk

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 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 1~8 (fe1~fe8) . For Gigabit Ethernet Port 9~10: (ge9~ge10) , it can be set up to 1000M Full Duplex(1000 Full) and 1000M Half Duplex(1000 Half).
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.
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.

Port	Link	State	Speed/Duplex	Flow Control	SFP Vendor	Wavelength	Distance
1	Up	Enable	100 Full	Disable	---	---	---
2	Down	Enable	---	Disable	---	---	---
3	Up	Enable	100 Full	Disable	---	---	---
4	Down	Enable	---	Disable	---	---	---
5	Down	Enable	---	Disable	---	---	---
6	Down	Enable	---	Disable	---	---	---
7	Down	Enable	---	Disable	---	---	---
8	Down	Enable	---	Disable	---	---	---
9	Down	Enable	---	Disable	---	---	---
10	Down	Enable	---	Disable	---	---	---

SFP DDM

Womaster Industrial Switch supports the SFP module with digital diagnostics monitoring (DDM) function. User can check the physical or operational status 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.

Port	SFP Scan/Eject	SFP DDM	Temperature (degree)		Tx Power (dBm)		Rx Power (dBm)	
			Current	Range	Current	Range	Current	Range
9	---	Enable	---	---	---	---	---	---
10	---	Enable	---	---	---	---	---	---

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

TERMS	DESCRIPTION
SFP Vendor	Vendor name of the SFP transceiver user plugged.
Wavelength	The wave length of the SFP transceiver user plugged.
Distance	The distance of the SFP transceiver user plugged.
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 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	8	All	0
2	Broadcast Only	8	All	0
3	Broadcast Only	8	All	0
4	Broadcast Only	8	All	0
5	Broadcast Only	8	All	0
6	Broadcast Only	8	All	0
7	Broadcast Only	8	All	0
8	Broadcast Only	8	All	0
9	Broadcast Only	8	All	0
10	Broadcast Only	8	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: 8 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.

3.2.4 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 trunking between two switches.

When User activates port trunking, 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 trunking has been activated, User can configure these items again for each trunking 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.

Port	Group ID	Trunk Type
1	0	
2	0	
3	0	
4	0	
5	0	
6	0	
7	0	
8	0	
9	0	
10	0	

[Submit](#) [Reload](#)

The description of the columns is as below:

TERMS	DESCRIPTION
Group ID	Default: 0 Group ID is the ID for the port trunk group. Ports with same group ID are in the same group.
Type	Default: Blank 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.

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.

Group ID	Type	Aggregated Ports	Individual Ports	Link Down Ports
1	Static	1		2
2	N/A			
3	N/A			
4	N/A			
5	N/A			
6	N/A			
7	N/A			
8	N/A			

Reload

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**.

3.3 POWER OVER ETHERNET (DP310 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. DP310 which is an industrial DIN Rail PoE Switch compliant with IEEE 802.3af and IEEE 802.3at. DP310 adapts 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 5 was enabled and is supplying power to a Class 2 Powered Device (PD) indicated under the Classification column. The PD device is rated at 47.5V and 45mA. The total power consumption for this PD is 1.9W with Budget 5W. To check the status of the PoE port, please click on the Reload button.

The screenshot displays the PoE Status page with several tabs: PoE Status (selected), PoE Control, PoE Schedule, Alive Check, and PoE Event. The main content area shows system power metrics:

DC1 Power	48 V, Budget 7 W
DC2 Power	48 V, Budget 7 W
Primary Power	DC1, DC2
Secondary Power	---
Total Power Budget	7 W
Total Output Power	1.9 W
Utilization	27 %
Event	Normal

Below these metrics is a table with 8 columns: Port, Mode, Status, Class, Budget(w), Consumption(W), Voltage(V), and Current(mA). The data for each port is as follows:

Port	Mode	Status	Class	Budget(w)	Consumption(W)	Voltage(V)	Current(mA)
1	Disable	Off	---	---	0.0	0.0	0
2	Disable	Off	---	---	0.0	0.0	0
3	Disable	Off	---	---	0.0	0.0	0
4	Disable	Off	---	---	0.0	0.0	0
5	Enable	Powering	Class2	5.0	1.9	47.5	45
6	Disable	Off	---	---	0.0	0.0	0

The description of the columns is as below:

TERMS	DESCRIPTION
Mode	Enable/Disable/Schedule Indicates the PoE port status
Status	Default: Off PoE status is included Off, Powering, and Searching. Off – PoE is inactive. Powering – PoE is enabled and powering the PD. 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 CONTROL

The PoE control includes 3 parts, **System Setting**, **Port setting** and **PD status detection**. The following section will introduce the function.

System Setting

The screenshot shows the 'PoE System Control' interface. At the top, there are navigation tabs: 'PoE Status', 'PoE Control' (selected), 'PoE Schedule', 'Alive Check', and 'PoE Event'. Below the tabs, the 'PoE System Control' section is visible. Under 'System Setting', there is a 'PoE System' dropdown menu currently set to 'Disable'. Below this, there are two sections for 'Power 1 Settings' and 'Power 2 Settings'. Each section has input fields for 'Budget(W)' (set to 0) and 'Voltage(V)' (set to 48). At the bottom left, there are 'Submit' and 'Cancel' buttons.

The figure above is **System Setting** interface. In this section, user can enable or disable the PoE function.

The description of the columns is as below:

TERMS	DESCRIPTION
PoE System	Enable or disable system's PoE function.
Budget (W)	The power supply maximum output budget. Both power budget of DC 1 and DC2 will be aggregated.
Voltage (V)	Default: 48V The voltage of applied to the power input. Here, we suggest using the same specification of power supply. If the power supply with different output voltage, it may cause system draw more current from one power model which with higher voltage.

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

PoE Port Control

Port	Mode	Powering Mode	Budget(W)	Priority
1	Disable	802.3af	32.0	Critical
2	Disable	802.3af	32.0	Critical
3	Disable	802.3af	32.0	Critical
4	Disable	802.3af	32.0	Critical
5	Disable	802.3af	32.0	Critical
6	Disable	802.3af	32.0	Critical
7	Disable	802.3af	32.0	Critical
8	Disable	802.3af	32.0	Critical

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. *Forced mode will ignore the classification behaviors and apply power onto the RJ-45, uses the forced mode must be carefully.
Budget (W)	Allows user assign the budget control in this field.
Priority	Supports 3 levels, Critical, High and Low.

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.

PoE Schedule

PoE Schedule on

Time	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00	<input type="checkbox"/>						
01:00	<input type="checkbox"/>						
02:00	<input type="checkbox"/>						
03:00	<input type="checkbox"/>						
04:00	<input type="checkbox"/>						
05:00	<input type="checkbox"/>						
06:00	<input type="checkbox"/>						
07:00	<input type="checkbox"/>						
08:00	<input type="checkbox"/>						

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

PD Alive Check

Enable PD Alive Check

PD	IP Address	Cycle Time(s)	Delete
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

DP310 supports 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.

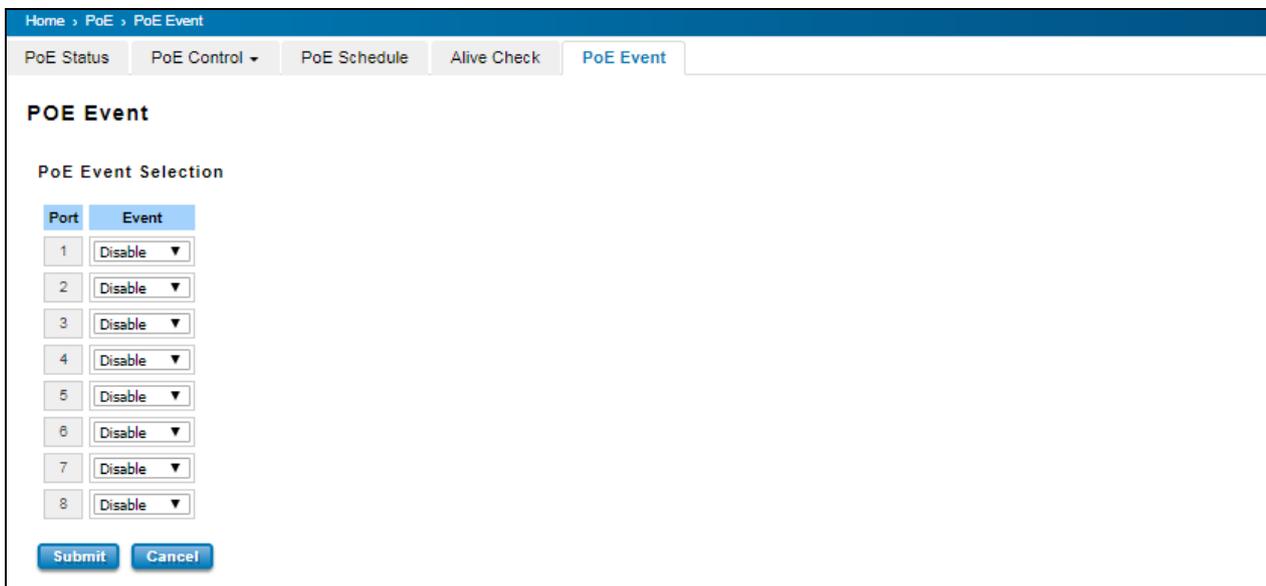
The description of the columns is as below:

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

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.



The screenshot shows a web interface for configuring PoE Event settings. At the top, there is a breadcrumb trail: Home > PoE > PoE Event. Below this, there are several tabs: PoE Status, PoE Control (with a dropdown arrow), PoE Schedule, Alive Check, and PoE Event (which is currently selected). The main content area is titled "POE Event" and contains a section for "PoE Event Selection". This section features a table with two columns: "Port" and "Event". The "Port" column lists ports 1 through 8. The "Event" column shows a dropdown menu for each port, all currently set to "Disable". At the bottom of the configuration area, there are two buttons: "Submit" and "Cancel".

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 screenshot shows a web interface for configuring RSTP settings. At the top, there are four tabs: "RSTP Settings" (selected), "MSTP Settings", "ERPS Settings", and "Loop Protection". Below the tabs is the "RSTP Bridge Setting" section. It features a "STP Mode" dropdown menu currently set to "RSTP". Underneath is the "Bridge Configuration" section, which contains five input fields: "Bridge Address" (text input with value "9486.e712.0933"), "Bridge Priority" (dropdown menu with value "32768"), "Max Age" (dropdown menu with value "20"), "Hello Time" (dropdown menu with value "2"), and "Forward Delay" (dropdown menu with value "15"). At the bottom of the configuration area are two buttons: "Submit" and "Cancel".

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 $n \times 4096$ 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.

$2 \times (\text{Forward Delay Time} - 1 \text{ sec}) \geq \text{Max Age Time} \geq 2 \times (\text{Hello Time value} + 1 \text{ sec})$

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 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. P2P - means P2P is enabled; the 2 ends work in full duplex mode. 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.

RSTP Settings ▾
MSTP Settings ▾
ERPS Settings ▾
Loop Protection

RSTP Status

Root Status

Root Address	<input type="text" value="9466.e712.0933"/>
Root Priority	<input type="text" value="32768"/>
Root Port	<input type="text" value="N/A"/>
Root Path Cost	<input type="text" value="0"/>
Max Age	<input type="text" value="20 second(s)"/>
Hello Time	<input type="text" value="2 second(s)"/>
Forward Delay	<input type="text" value="15 second(s)"/>

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 BPDUs sent from the root switch.

Port Status

Port	Role	Port State	Path Cost	Port Priority	Link Type	Edge Port	Aggregated(ID/Type)
1	Disabled	Disabled	200000	128	P2P	Edge	/
2	Disabled	Blocking	200000	128	P2P	Edge	/
3	Disabled	Blocking	200000	128	P2P	Edge	/
4	Disabled	Disabled	200000	128	P2P	Edge	/
5	Disabled	Disabled	200000	128	P2P	Edge	/
6	Disabled	Disabled	200000	128	P2P	Edge	/
7	Disabled	Disabled	200000	128	P2P	Edge	/
8	Disabled	Disabled	200000	128	P2P	Edge	/
9	Disabled	Disabled	20000	128	P2P	Edge	/
10	Disabled	Disabled	20000	128	P2P	Edge	/

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

MSTP Setting

MSTP Region Configuration

Region Name

Revision

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 The revision for the Region. Range: 0-65535

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

Add MSTP Instance

Add MSTP Instance

Instance ID

VLAN Group

Instance Priority

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 Instance Configuration

Instance ID	VLAN Group	Instance Priority
<input type="checkbox"/> 1	<input type="text" value="1"/>	<input type="text" value="32768"/>

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.

RSTP Settings ▾
MSTP Settings ▾
ERPS Settings ▾
Loop Protection

Instance ID 0 ▾

Port	Path Cost	Port Priority	Link Type	Edge Port
1	<input type="text" value="200000"/>	<input type="text" value="128"/>	<input type="text" value="Auto"/>	<input type="text" value="Enable"/>
2	<input type="text" value="200000"/>	<input type="text" value="128"/>	<input type="text" value="Auto"/>	<input type="text" value="Enable"/>
3	<input type="text" value="200000"/>	<input type="text" value="128"/>	<input type="text" value="Auto"/>	<input type="text" value="Enable"/>
4	<input type="text" value="200000"/>	<input type="text" value="128"/>	<input type="text" value="Auto"/>	<input type="text" value="Enable"/>
5	<input type="text" value="200000"/>	<input type="text" value="128"/>	<input type="text" value="Auto"/>	<input type="text" value="Enable"/>
6	<input type="text" value="200000"/>	<input type="text" value="128"/>	<input type="text" value="Auto"/>	<input type="text" value="Enable"/>
7	<input type="text" value="200000"/>	<input type="text" value="128"/>	<input type="text" value="Auto"/>	<input type="text" value="Enable"/>
8	<input type="text" value="200000"/>	<input type="text" value="128"/>	<input type="text" value="Auto"/>	<input type="text" value="Enable"/>
9	<input type="text" value="20000"/>	<input type="text" value="128"/>	<input type="text" value="Auto"/>	<input type="text" value="Enable"/>
10	<input type="text" value="20000"/>	<input type="text" value="128"/>	<input type="text" value="Auto"/>	<input type="text" value="Enable"/>

Submit
Cancel

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. Auto - means to auto select P2P or Share mode. P2P - means P2P is enabled; the 2 ends work in full duplex mode. 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.

MSTP Status

Instance ID

Root Status

Root Address

Root Priority

Root Port

Root Path Cost

Max Age

Hello Time

Forward Delay

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.

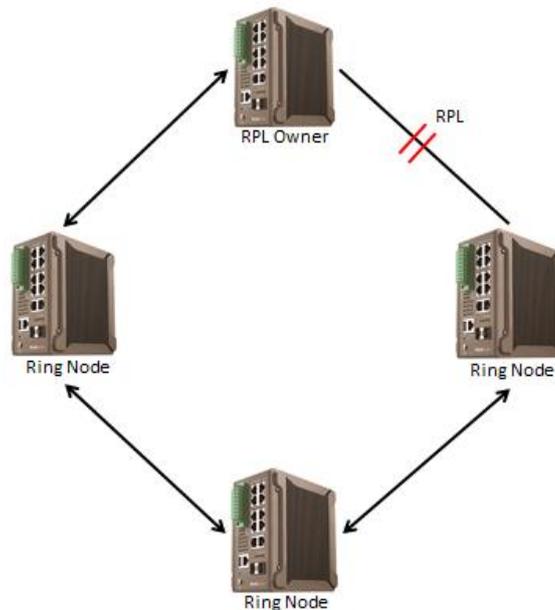
Port Status

Port	Role	Port State	Path Cost	Port Priority	Link Type	Edge Port
1	Disabled	Blocking	200000	128	P2P	Edge
2	Designated	Forwarding	200000	128	P2P	Edge
3	Designated	Forwarding	200000	128	P2P	Edge
4	Disabled	Blocking	200000	128	P2P	Edge
5	Designated	Forwarding	200000	128	P2P	Edge
6	Disabled	Blocking	200000	128	P2P	Edge
7	Designated	Forwarding	200000	128	P2P	Edge
8	Disabled	Blocking	200000	128	P2P	Edge
9	Disabled	Blocking	20000	128	P2P	Edge
10	Disabled	Blocking	20000	128	P2P	Edge

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

ERPS Setting

Add ERPS Instance

Instance ID: VLAN group:

ERPS Instance Setting

Instance ID: VLAN group:

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

Ring ID:

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	Instance	Manual Switch	Force Switch
1	v2	Enable	Ring Node	1	False	1	2	3	1	Revertive	1	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 east port or west port 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.
Instance	Select the Instance ID, the available number is 1-15.
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 5 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.

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 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

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

[Reload](#)

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.

3.4.4 LOOP PROTECTION

Since firmware of WoMaster switch supports loop elimination function that is based on per port or system configure. It prevents any communicate looping caused by RSTP and Ring when ring topology changes. The following figure shows the Loop Protection page.

Port	Loop Protection	Status
1	Disable	--
2	Disable	--
3	Disable	--
4	Disable	--
5	Disable	--
6	Disable	--
7	Disable	--
8	Disable	--
9	Disable	--
10	Disable	--

The description of the columns is as below:

TERMS	DESCRIPTION
Loop Protection	Enable/ Disable Loop Protection function by per port.
Status	Shows the port status. If there is looping occurred, it will show Loop Detected and Disabled information and the link indicator will not turn-off, and also the port is disabled by system. Once the looping is fixed, the blocked port will keep at blocked state, and must be enabled by manual or perform system reset to recovery it.

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 lower Secondary VLANs.
Secondary VLAN	The client ports are usually defined within secondary VLAN. The secondary VLAN includes Isolated VLAN and Community VLAN. The client ports can be isolated VLANs or can be grouped in the same Community VLAN. The ports within the same community VLAN can communicate with each other.

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. 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 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.

Static VLAN Setting

VLAN ID	Name	1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/> 1	VLAN1	U ▼	U ▼	U ▼	U ▼	U ▼	U ▼	U ▼	U ▼	U ▼	U ▼

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.

Home > VLAN > VLAN Port Setting

VLAN Setting | **VLAN Port Setting** | VLAN Status | PVLAN Setting | PVLAN Port Setting | PVLAN Status | GVRP Setting

VLAN Port Setting

Port	PVID	Tunnel Mode	Accept Frame Type	Ingress Filtering
1	1	None	Admit All	Disable
2	1	None	Admit All	Disable
3	1	None	Admit All	Disable
4	1	None	Admit All	Disable
5	1	None	Admit All	Disable
6	1	None	Admit All	Disable
7	1	None	Admit All	Disable
8	1	None	Admit All	Disable
9	1	None	Admit All	Disable
10	1	None	Admit All	Disable

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	<p>Default: None</p> <p>None : This is Port that no using Q in Q</p> <p>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.</p> <p>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.</p> <p>802.1Q Tunnel Uplink-Add-PVID: Assign second VLAN tag for specify VLANs.</p>
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	<p>Normal: The Normal port is None PVLAN ports; it remains its original VLAN setting.</p> <p>Host: The Host type ports can be mapped to the Secondary VLAN.</p> <p>Promiscuous: The promiscuous port can be associated to the Primary VLAN.</p>
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.

Private VLAN Association

Secondary VLAN	Primary VLAN
3	2 ▼
4	2 ▼
5	2 ▼

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

For example:

- 1. VLAN Create:** VLAN 2-5 are created in VLAN Configuration section.
- 2. Private VLAN Type:** VLAN 2-5 has its Private VLAN Type configured in Private VLAN Configuration page. VLAN 2 is belonged to Primary VLAN. VLAN 3-5 are belonged to secondary VLAN (Isolated or Community).
- 3. Private VLAN Association:** Associate VLAN 3-5 as the Secondary VLAN to VLAN 2 as the Primary VLAN in Private VLAN Association first.

4. Private VLAN Port Configuration

VLAN 2 – Primary -> The member port of VLAN 2 is promiscuous port.

VLAN 3 – Isolated -> The Host port can be mapped to VLAN 3.

VLAN 4 – Community ->The Host port can be mapped to VLAN 3.

VLAN 5 – Community ->The Host port can be mapped to VLAN 3.

5. Result:

VLAN 2 -> VLAN 3, 4, 5; member ports can communicate with ports in secondary VLAN.

VLAN 3 -> VLAN 2, member ports are isolated, but it can communicate with member port of VLAN 2..

VLAN 4 -> VLAN 2, member ports within the community can communicate with each other and communicate with member port of VLAN 2.

VLAN 5 -> VLAN 2, member ports within the community can communicate with each other and communicate with member port of VLAN 2.

3.5.6 PVLAN STATUS

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

PVLAN Status

Primary VLAN	Secondary VLAN	Secondary VLAN Type	Port
2	3	Isolated	1,2

[Reload](#)

3.5.7 GVRP SETTING

Home > VLAN > GVRP Setting

VLAN Setting | VLAN Port Setting | VLAN Status | PVLAN Setting | PVLAN Port Setting | PVLAN Status | **GVRP Setting**

GVRP Setting

GVRP Protocol

Port	State	Join Timer	Leave Timer	Leave All Timer
1	<input type="text" value="Disable"/>	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>
2	<input type="text" value="Disable"/>	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>
3	<input type="text" value="Disable"/>	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>
4	<input type="text" value="Disable"/>	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>
5	<input type="text" value="Disable"/>	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>
6	<input type="text" value="Disable"/>	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>
7	<input type="text" value="Disable"/>	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>
8	<input type="text" value="Disable"/>	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>
9	<input type="text" value="Disable"/>	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>
10	<input type="text" value="Disable"/>	<input type="text" value="20"/>	<input type="text" value="60"/>	<input type="text" value="1000"/>

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 Allow user to enable / disable GVRP function globally.
State	Default: Disable After enable GVRP globally, here still can enable/disable GVRP by port.
Join Timer	Default: 20 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 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 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 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 ensure high-priority traffic is delivered first. This section allows User to configure Traffic Prioritization settings for each port with regard to setting priorities.

3.6.1 QoS SETTING

The figure below shows QoS Setting.

Home > QoS > QoS Setting

QoS Setting | CoS Mapping | DSCP Mapping

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
7	0	CoS Only
8	0	CoS Only

Queue Scheduling

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 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.

3.6.2 CoS MAPPING

This section allows user to change CoS values to Physical Queue mapping table. WoMaster switch only supports 4 physical queues, Lowest, Low, Middle and High represent by numbers from 0 to 3. In WoMaster switch, users can freely assign the mapping table or follow the suggestion of the 802.1p standard. Below is the interface.

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.

Submit **Cancel**

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

3.6.3 DSCP MAPPING

This page is to change DSCP values to Physical Queue mapping table. Since the switch fabric only supports 4 physical queues, Lowest, Low, Middle and High. 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.

The screenshot shows the 'DSCP Mapping' configuration page. It features a grid with 8 rows of DSCP ranges and their corresponding queue assignments. The 'Queue' column contains dropdown menus with the following values: 1, 0, 0, 1, 2, 2, 3, 3.

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

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. 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 (Internet Group Management Protocol) is an Internet Protocol that provides a way for internet device to report its multicast group membership to adjacent routers. In effect, IGMP Snooping manages multicast traffic by making use of switches, routers, and hosts that support IGMP. IGMP has three fundamental types of messages, as shown below:

MESSAGE	DESCRIPTION
Query	A message sent from the querier (an IGMP router or a switch) which asks for a response from each host that belongs to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit as a member of a specific multicast group.

User can enable **IGMP Snooping** and **IGMP Query** functions in this section. User will see the information of the IGMP Snooping function in this section, including different multicast groups' VID and member ports, and IP multicast addresses that range from 224.0.0.0 to 239.255.255.255.

In this section, Force filtering can determine whether the switch flooding is unknown multicast or not.

Following commands are included in this group:

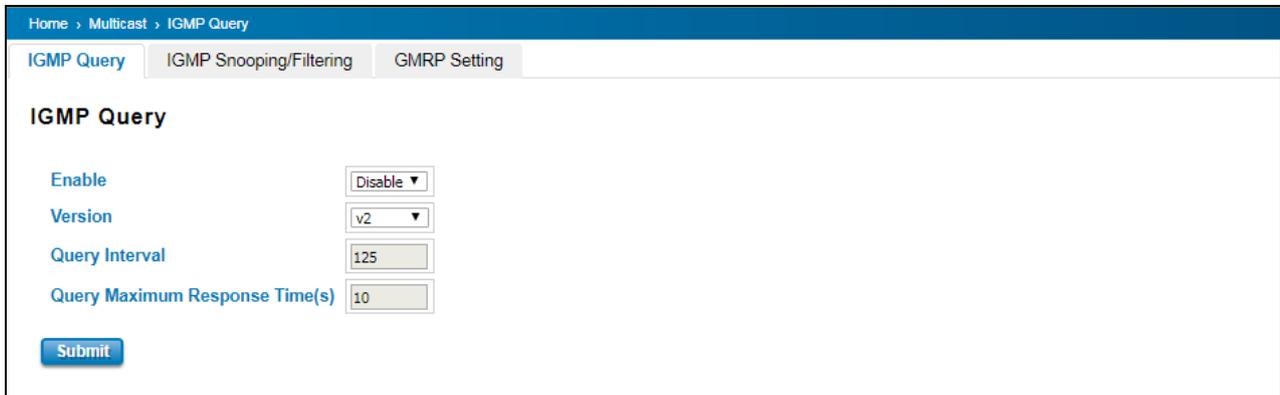
3.7.1 IGMP Query

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 Enable the IGMP Query function
Version	Default: V2 V1 means IGMP V1 General Query V2 means IGMP V2 General Query.
Query Interval(s)	The period of query sent by querier.
Query Maximum Response Time	The span 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, assign IGMP Snooping for specific VLAN, and view IGMP Snooping table from dynamic learnt or static manual key-in. WoMaster Switch support IGMP snooping V1/V2/V3 automatically and IGMP query V1/V2. 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 here. After enabling IGMP Snooping, User can then enable IGMP Snooping for specific VLAN. User can enable IGMP Snooping for some VLANs so that some of the VLANs will support IGMP Snooping and others won't.
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. - Flood Unknown: The switch would filter the unknown packets that transmit through the network

IGMP Snooping Table: In the table, User can see multicast group IP address, VLAN ID it belongs to, and member ports of the multicast group. WoMaster Managed Switch series supports 256 multicast groups. Click on **Reload** to refresh the table.

Static Router Port(s)

Port	1	2	3	4	5	6	7	8	9	10
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

IGMP Snooping Table

Multicast Address	VLAN ID	Interface
224.0.0.251	1	fe1,
224.0.0.252	1	fe1,
239.255.255.250	1	fe1,

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.

Home > Multicast > GMRP Setting

IGMP Query IGMP Snooping/Filtering **GMRP Setting**

GMRP Setting

GMRP Global Setting

GMRP Port Setting

Port	State
1	<input type="text" value="Disable"/>
2	<input type="text" value="Disable"/>
3	<input type="text" value="Disable"/>
4	<input type="text" value="Disable"/>
5	<input type="text" value="Disable"/>
6	<input type="text" value="Disable"/>
7	<input type="text" value="Disable"/>
8	<input type="text" value="Disable"/>
9	<input type="text" value="Disable"/>
10	<input type="text" value="Disable"/>

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. Default community string is Public.
Read and Write	User has the ability to read and set the values of MIB tables. 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**. 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.

Home > SNMP > SNMP v1/V2c

SNMP V1/V2c | SNMP V3 | SNMP Trap

SNMP V1/V2c

Community String	Privilege
<input type="checkbox"/> public	Read Only
<input type="checkbox"/> private	Read and Write
<input type="checkbox"/>	Read Only
<input type="checkbox"/>	Read Only

3.8.2 SNMP V3

SNMP v3 can provide more security functions when the user performs remote management through SNMP protocol. It delivers SNMP information to the administrator with user authentication; all of data between the switch and the administrator are encrypted to ensure secure communication.

TERMS	DESCRIPTION
User Name	Set up the user name.
Security Level	Default: None Here the user can select the following levels of security: None, User Authentication, and Authentication with privacy.
Authentication Level	Default: MD5 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 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 Port Security

3.9.2 IP Security

3.9.3 IEEE 802.1x

3.9.1 PORT SECURITY

Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. Port Security feature allows User to stop the MAC address learning for specific port. After stopping MAC learning, only the MAC address listed in Port Security 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.

The description of the columns is as below:

TERMS	DESCRIPTION
Port Security State	Default: Disable Change Port Security State of the port to Enable first.
Add Port Security Entry	Select the port, and type VLAN ID and MAC address. Format of the MAC address is xxxx.xxxx.xxxx. Ex: 0012.7701.0101. Max volume of one port is 10. So the system can accept 100 Port Security MAC addresses in total.
Show Port Security List	This table shows User those enabled port security entries. User can click on Remove to delete the entry.

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

3.9.2 IP SECURITY

In IP Security section, User can set up specific IP addresses to grant authorization for management access to the device via a web browser or Telnet.

Home > Security > IP Security

Port Security | IP Security | 802.1X ▼

IP Security

IP Security Disable ▼

Submit

Add Secure IP

Security IP

Add

IP Security List

Index	Security IP
<input type="text"/>	<input type="text"/>

Remove

The description of the columns is as below:

TERMS	DESCRIPTION
IP Security	Select Enable and Submit to enable IP security function.
Add Security IP	User can assign specific IP addresses, and then press Add . Only these IP addresses can access and manage the switch via a web browser or Telnet. Max security IP is 10.
IP Security List	This table shows User added security IP addresses. User can press Remove to delete,

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

3.9.3 IEEE 802.1x

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.

802.1X Setting

System Auth Control ▾

Authentication Method ▾

RADIUS Server

RADIUS Server IP

Shared Key

Server Port

Accounting Port

Secondary RADIUS Server

RADIUS Server IP

Shared Key

Server Port

Accounting Port

Local RADIUS User

User Name	Password	VID
<input type="text"/>	<input type="text"/>	<input type="text"/>

Local RADIUS User List

User	Name	Password	VID
	<input type="text"/>	<input type="text"/>	<input type="text"/>

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 a 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.

Home > Security > 802.1X Port Setting

Port Security | IP Security | 802.1X ▾

802.1X Port Setting

802.1X Port Configuration

Port	Port Control	MAB	Re-authentication	Max Request	Guest VLAN	Host Mode	Admin Control Direction
<input type="checkbox"/> 1	Force Authorized ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 2	Force Authorized ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 3	Force Authorized ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 4	Force Authorized ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 5	Force Authorized ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 6	Force Authorized ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 7	Force Authorized ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 8	Force Authorized ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 9	Force Authorized ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 10	Force Authorized ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾

802.1X Timeout Configuration

Port	Re-Auth Period(s)	Quiet Period(s)	Tx period(s)	Supplicant Timeout(s)	Server Timeout(s)
1	3600	60	30	30	30
2	3600	60	30	30	30
3	3600	60	30	30	30
4	3600	60	30	30	30
5	3600	60	30	30	30
6	3600	60	30	30	30
7	3600	60	30	30	30
8	3600	60	30	30	30
9	3600	60	30	30	30
10	3600	60	30	30	30

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 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.
Control Direction	Determined devices can send 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.

Home > Security > 802.1X Port Status

Port Security | IP Security | 802.1X ▾

802.1X Port Status

Port	Port Control	MAB	Authorized Status	Authorized Supplicant	Oper Control Direction
1	Force Authorized	Disable	Authorized	NONE	Both
2	Force Authorized	Disable	Authorized	NONE	Both
3	Force Authorized	Disable	Authorized	NONE	Both
4	Force Authorized	Disable	Authorized	NONE	Both
5	Force Authorized	Disable	Authorized	NONE	Both
6	Force Authorized	Disable	Authorized	NONE	Both
7	Force Authorized	Disable	Authorized	NONE	Both
8	Force Authorized	Disable	Authorized	NONE	Both
9	Force Authorized	Disable	Authorized	NONE	Both
10	Force Authorized	Disable	Authorized	NONE	Both

[Reload](#)

3.10 Industrial

WoMaster Switch supports industrial protocol for user to communicate the devices in factory.

Following topics are included in this section:

3.10.1 Modbus TCP/IP

3.10.1 Modbus TCP/IP

Modbus TCP/IP (also Modbus-TCP) is simply the Modbus RTU protocol with a TCP interface that runs on Ethernet.

The Modbus messaging structure is the application protocol that defines the rules for organizing and interpreting the data independent of the data transmission medium. WoMaster Switch operate as slave device. The following picture is the setting page which you can switch on the status to enable Modbus TCP function. Also, you can apply the value for listening port, max Modbus TCP Master/Client, idle timeout(ms) in this page. The default value of listening port is 502.

Home > Industrial > Modbus TCP

Modbus TCP

Modbus TCP

Status: Disable

Listening Port: 502

Max Modbus TCP Master/Client: 10

Idle Timeout (ms): 3000

Submit

Modbus TCP/IP Mapping Table

We take DS310 for example. Only differs from product name and description.

Word Address	Data Type	Description
System Information		
0x0000	16 words	Product Name = "DS310" Word 0 Hi byte = 'D' Word 0 Lo byte = 'S' Word 1 Hi byte = '3' Word 1 Lo byte = '1' Word 2 Hi byte = '0' Word 2 Lo byte = '\0' (other words = 0)
0x0010	128 words	Product Description = " Industrial Managed Ethernet Switch"

		<p>Word 0 Hi byte = 'l' Word 0 Lo byte = 'n' Word 1 Hi byte = 'd' Word 1 Lo byte = 'u' Word 2 Hi byte = 's' Word 2 Lo byte = 't' Word 3 Hi byte = 'r' Word 3 Lo byte = 'i' Word 4 Lo byte = 'a' Word 4 Hi byte = 'l' Word 14 Lo byte = 'S' Word 14 Hi byte = 'w' Word 15 Lo byte = 'i' Word 15 Hi byte = 't' Word 16 Lo byte = 'c' Word 16 Hi byte = 'h' Word 17 Lo byte = '\0' (other words = 0)</p>
0x0090	128 words	SNMP system name (string)
0x0110	128 words	SNMP system location (string)
0x0190	128 words	SNMP system contact (string)
0x0210	32 words	SNMP system OID (string)
0x0230	2 words	System uptime (unsigned long)
0x0232 to 0x02FF	206 words	Reserved address space
0x0300	2 words	<p>Boot loader version Word 0 Hi byte = first number of version Word 0 Lo byte = second number of version Word 1 Hi byte = third number of version Word 1 Lo byte = fourth number of version Version = v1.0.3.0 Word 0 Hi byte = 0x1 Word 0 Lo byte = 0x0 Word 1 Hi byte = 0x3 Word 1 Lo byte = 0x0</p>
0x0302	2 words	<p>Firmware Version Word 0 Hi byte = first number of version Word 0 Lo byte = second number of version</p>

		<p>Word 1 Hi byte = third number of version</p> <p>Word 1 Lo byte = fourth number of version</p> <p>Ex: Version = v1.2</p> <p>Word 0 Hi byte = 0x1</p> <p>Word 0 Lo byte = 0x2</p> <p>Word 1 Hi byte = 0x0</p> <p>Word 1 Lo byte = 0x0</p> <p>Version = v1.2.3</p> <p>Word 0 Hi byte = 0x1</p> <p>Word 0 Lo byte = 0x2</p> <p>Word 1 Hi byte = 0x3</p> <p>Word 1 Lo byte = 0x0</p> <p>Version = v1.2.3.4</p> <p>Word 0 Hi byte = 0x1</p> <p>Word 0 Lo byte = 0x2</p> <p>Word 1 Hi byte = 0x3</p> <p>Word 1 Lo byte = 0x4</p>
0x0304	2 words	<p>Firmware Release Date</p> <p>Firmware was released on 2018-08-11 at 09 o'clock</p> <p>Word 0 = 0x0B09</p> <p>Word 1 = 0x1208</p>
0x0306	3 words	<p>Ethernet MAC Address</p> <p>Ex: MAC = 01-02-03-04-05-06</p> <p>Word 0 Hi byte = 0x01</p> <p>Word 0 Lo byte = 0x02</p> <p>Word 1 Hi byte = 0x03</p> <p>Word 1 Lo byte = 0x04</p> <p>Word 2 Hi byte = 0x05</p> <p>Word 2 Lo byte = 0x06</p>
0x0309 to 0x3FF	247 words	Reserved address space
0x0400	2 words	<p>IP address</p> <p>Ex: IP = 192.168.10.1</p> <p>Word 0 Hi byte = 0xC0</p> <p>Word 0 Lo byte = 0xA8</p> <p>Word 1 Hi byte = 0x0A</p> <p>Word 1 Lo byte = 0x01</p>
0x0402	2 words	Subnet Mask
0x0404	2 words	Default Gateway
0x0406	2 words	DNS Server

0x0408 to 0x04FF	248 words	Reserved address space (IPv6 or others)
0x0500	1 word	Power1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0501	1 word	Power2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0502	1 word	Power3 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0503	1 word	Power4 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0504 to 0x050F	12 words	Reserved address space
0x0510	1 word	DI1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0511	1 word	DI2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0512 to 0x051F	14 words	Reserved address space
0x0520	1 word	DO1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0521	1 word	DO2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0522 to 0x052F	14 words	Reserved address space
0x0530	1 word	SYS LED (Green light) 0x0000:Off 0x0001:On

		0x0002: blinking 0x0003: blinking fast 0xFFFF: unavailable
0x0531	1 word	SYS LED(Yellow light) 0x0000:Off 0x0001:On 0x0002: blinking 0x0003: blinking fast 0xFFFF: unavailable
0x0532	1 word	R.S. LED (Green light) 0x0000:Off 0x0001:On 0x0002: blinking 0x0003: blinking fast 0xFFFF: unavailable
0x0533	1 word	R.S. LED (Yellow light) 0x0000:Off 0x0001:On 0x0002: blinking 0x0003: blinking fast 0xFFFF: unavailable
Port Information (32 Ports)		
0x1000 to 0x101F	1 word	Operating Status 0x0000: Link down 0x0001: Link up 0x0002: Disable 0xFFFF: No port
0x1020 to 0x103F	1 word	Speed/Duplex 0x0000: Not Connected 0x0001: 10M-Half 0x0002: 10M-Full 0x0003: 100M-Half 0x0004: 100M-Full 0x0005: 1000M-Half 0x0006: 1000M-Full 0xFFFF: No port
0x1040 to 0x105F	1 word	Flow Control 0x0000: off 0x0001: on

		0xFFFF: No port
0x1060 to 0x107F	1 word	MDI/MDIX 0x0000: MDI 0x0001: MDIX 0xFFFF: No port
0x1080 to 0x109F	1 word	Medium mode 0x0000: copper 0x0001: fiber 0x0002: none 0xFFFF: No port
0x10A0 to 0x10BF	1 word	STP Status 0x0000: disabled 0x0001: blocking 0x0002: listening 0x0003: learning 0x0004: forwarding 0xFFFF: No port
0x10C0 to 0x12BF	16 words	Port Description
Packet information (32 Ports)		
0x2000 to 0x203F	2 words	Tx Packets Ex: port 1 Tx Packet Amount = 44332211 Received MODBUS response: 0x44332211 Word 0 = 4433 Word 1 = 2211
0x2040 to 0x207F	2 words	Rx Packets Ex: port 1 Rx Packet Amount = 44332211 Received MODBUS response: 0x44332211 Word 0 = 4433 Word 1 = 2211
0x2080 to 0x20BF	2 words	Tx Error Packets Ex: port 1 Tx Packet Amount = 44332211 Received MODBUS response: 0x44332211 Word 0 = 4433 Word 1 = 2211
0x20C0 to 0x20FF	2 words	Rx Error Packets Ex: port 1 Rx Packet Amount = 44332211 Received MODBUS response: 0x44332211 Word 0 = 4433 Word 1 = 2211

0x2100 to 0x2BFF	2816 words	Reserved address space
0x2C00	1 words	Clear ROMN by bitmap of port 1 to 16 Write to clear Read to return 0x0000 To clear port 1 Word = 0x0001 To clear port 1 and 2 Word = 0x0003
0x2C01	1 words	Clear ROMN by bitmap of port 17 to 32 Write to clear Read to return 0x0000 To clear port 17 Word = 0x0001 To clear port 17 and 18 Word = 0x0003
Network Redundancy Information *		
0x3000	1 word	Ring 0's Status 0x0000: none 0x0001: Disable 0x0002: Enable 0xFFFF: unavailable
0x3001	1 word	Ring 0's Version 0x0000: none 0x0001: v1 0x0002: v2 0xFFFF: unavailable
0x3002	1 word	Ring 0's Node State 0x0000: Disabled 0x0001: Initial 0x0002: Idle 0x0003: Protection 0x0004: Manual Switch 0x0005: Forced Switch 0x0006: Pending 0xFFFF: unavailable
0x3003	1 word	Ring 0's Ring Type 0x0000: none 0x0001: Major Ring

		0x0002: Sub Ring 0xFFFF: unavailable
0x3004	1 word	Ring 0's Node Role 0x0000: none 0x0001: Ring node 0x0002: RPL Owner 0x0003: RPL Neighbor 0xFFFF: unavailable
0x3005	1 word	Ring 0's Control Channel
0x3006	1 words	Ring 0's Sub Ring without Virtual Channel 0x0000: none 0x0001: True 0x0002: False 0xFFFF: unavailable
0x3007	1 word	Ring 0's Virtual Channel of Sub Ring
0x3008	1 word	Ring 0's Ring Port 0 0x0000: none 0x0001: port 1 0x0002: port 2 ... 0x001C: port 28 0xFFFF: unavailable
0x3009	1 word	Ring 0's Ring Port 1 0x0000: none 0x0001: port 1 0x0002: port 2 ... 0x001C: port 28 0xFFFF: unavailable
0x300A	1 word	Ring 0's Ring Port 0 state 0x0000: disabled 0x0001: blocking 0x0002: listening 0x0003: learning 0x0004: forwarding
0x300B	1 word	Ring 0's Ring Port 1 state 0x0000: disabled 0x0001: blocking

		<p>0x0002: listening</p> <p>0x0003: learning</p> <p>0x0004: forwarding</p>
0x300C	1 word	<p>Ring 0's Ring Port 0 RMEP ID</p> <p>0x0000: none</p> <p>0x0001: RMEP ID = 1</p> <p>0x0002: RMEP ID = 2</p> <p>...</p> <p>0x1FFF: RMEP ID = 8191</p> <p>0xFFFF: unavailable</p>
0x300D	1 word	<p>Ring 0's Ring Port 1 RMEP ID</p> <p>0x0000: none</p> <p>0x0001: RMEP ID = 1</p> <p>0x0002: RMEP ID = 2</p> <p>...</p> <p>0x1FFF: RMEP ID = 8191</p> <p>0xFFFF: unavailable</p>
0x300E	1 word	<p>Ring 0's RPL port</p> <p>0x0000: RPL port = Ring port 0</p> <p>0x0001: RPL port = Ring port 1</p> <p>0xFFFF: unavailable</p>
0x300F	1 word	<p>Ring 0's Revertive Mode</p> <p>0x0000: Revertive</p> <p>0x0001: non-Revertive</p> <p>0xFFFF: unavailable</p>
0x3010	1 word	Ring 0's Instance
0x3011	1 word	<p>Ring 0's Manual Switch</p> <p>0x0000: Manual Switch port = Ring port 0</p> <p>0x0001: Manual Switch port = Ring port 1</p> <p>0x0001: Manual Switch port = none</p> <p>0xFFFF: unavailable</p>
0x3012	1 word	<p>Ring 0's Force Switch</p> <p>0x0000: Force Switch port = Ring port 0</p> <p>0x0001: Force Switch port = Ring port 1</p> <p>0x0001: Force Switch port = none</p> <p>0xFFFF: unavailable</p>
0x3013 to 0x301F	13 words	Reserved address space
0x3020 to		ERPS Ring 1's Information

0x303F		
0x3040 to 0x305F		ERPS Ring 2's Information
0x3060 to 0x307F		ERPS Ring 3's Information
0x3080 to 0x309F		ERPS Ring 4's Information
0x30A0 to 0x30BF		ERPS Ring 5's Information
0x30C0 to 0x30DF		ERPS Ring 6's Information
0x30E0 to 0x30FF		ERPS Ring 7's Information
0x3100 to 0x311F		ERPS Ring 8's Information
0x3120 to 0x313F		ERPS Ring 9's Information
0x3140 to 0x315F		ERPS Ring 10's Information
0x3160 to 0x317F		ERPS Ring 11's Information
0x3180 to 0x319F		ERPS Ring 12's Information
0x31A0 to 0x31BF		ERPS Ring 13's Information
0x31C0 to 0x31DF		ERPS Ring 14's Information
0x31E0 to 0x31FF		ERPS Ring 15's Information
0x3200 to 0x321F		ERPS Ring 16's Information
0x3220 to 0x323F		ERPS Ring 17's Information
0x3240 to 0x325F		ERPS Ring 18's Information
0x3260 to 0x327F		ERPS Ring 19's Information
0x3280 to		ERPS Ring 20's Information

0x329F		
0x32A0 to 0x32BF		ERPS Ring 21's Information
0x32C0 to 0x32DF		ERPS Ring 22's Information
0x32E0 to 0x32FF		ERPS Ring 23's Information
0x3300 to 0x331F		ERPS Ring 24's Information
0x3320 to 0x333F		ERPS Ring 25's Information
0x3340 to 0x335F		ERPS Ring 26's Information
0x3360 to 0x337F		ERPS Ring 27's Information
0x3380 to 0x339F		ERPS Ring 28's Information
0x33A0 to 0x33BF		ERPS Ring 29's Information
0x33C0 to 0x33DF		ERPS Ring 30's Information
0x33E0 to 0x33FF		ERPS Ring 31's Information

* Network Redundancy Information: by request

3.11 WARNING

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

3.11.1 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 DC1 Power DC2 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 Restart Period: duration of output open. Hold Period: duration of Ping hold time.	Ping target device and trigger relay to emulate power reset for remote device, if remote system crash. 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 (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.

3.11.2 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 screenshot shows the 'System Event' configuration page. At the top, there is a breadcrumb trail: 'Home > Warning > System Event'. Below this, there are four tabs: 'Relay Output', 'Event Type' (which is selected), 'Syslog Setting', and 'Email Alert'. The main content area is titled 'System Event' and contains a list of events with checkboxes, all of which are checked:

- Device Cold Start
- Device Warm Start
- Authentication Failure
- Time Synchronization Failure
- Power 1 Failure
- Power 2 Failure
- Relay Output 1
- DI 1 Change
- Ring Event
- Loop Protection
- SFP Event

At the bottom of the configuration area, there are two buttons: 'Submit' and 'Cancel'.

The screenshot shows the 'Ethernte Port Event' configuration page. At the top, there is a breadcrumb trail: 'Home > Warning > Port Event'. Below this, there are four tabs: 'Relay Output', 'Event Type' (which is selected), 'Syslog Setting', and 'Email Alert'. The main content area is titled 'Ethernte Port Event' and contains a table for configuring link states for 10 ports:

Port	Link State
1	Disable
2	Disable
3	Disable
4	Disable
5	Both
6	Disable
7	Disable
8	Disable
9	Disable
10	Disable

At the bottom of the configuration area, there are two buttons: 'Submit' and 'Cancel'.

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.
Ring Event	Ring Status has changed or backup path is activated.
Loop Protection	Loop event is indicated.
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.

3.11.3 SYSLOG SETTING

System Log is useful to provide system administrator locally or remotely monitor switch events history. 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 occurred events selected in the Event Selection page to System Log table of the switch. User can monitor the system logs in [Diagnostics] / [Syslog Setting] page.

Remote Mode: The remote mode is also known as Server mode in WoMaster managed switch. In this mode, User should assign the IP address of the System Log server. The switch will send the occurred events selected in Event Selection page 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. When enabling Local or Both modes, User can monitor the system logs in [Diagnostics] / [Event Log] page

3.11.4 EMAIL ALERT

WoMaster switch supports E-mail Warning feature. The switch will send the occurred events to remote E-mail server. The receiver can then receive notification by E-mail. The E-mail warning is conformed to SMTP standard.

This page allows User to enable E-mail Alert, assign the SMTP Server IP, Sender E-mail, and Receiver E-mail. If SMTP server requests User to authorize first, User can also setup the username and password in this page.

Email Alert

Email Alert Disable ▾

SMTP Server IP

Mail Account

Authentication Required

User Name

Password

Confirm Password

Email 1 To

Email 2 To

Email 3 To

Email 4 To

The description of the columns is as below:

TERMS	DESCRIPTION
SMTP Server IP Address	Enter the IP address of the email Server
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.

3.12 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:

3.12.1 LLDP Setting

3.12.2 MAC Table

3.12.3 Port Statistics

3.12.4 Port Mirror

3.12.5 Event Log

3.12.6 Ping

3.12.1 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 learnt from the connected devices.

The configuration and settings explain as following.

Local Port	Neighbor ID	Neighbor IP	Neighbor VID
2	94:66:e7:9f:00:00	192.168.1.6	1
3	94:66:e7:9f:56:78	192.168.1.2	1

TERMS	DESCRIPTION
LLDP	Select 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.
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.

3.12.2 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)

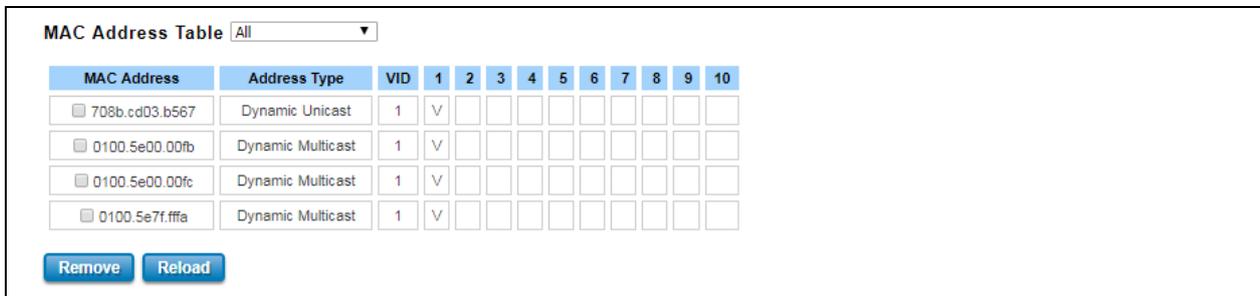
Each switch Fabric has limit size to write the learnt MAC address. To save more entries for new MAC address, the switch Fabric will age out non-used MAC address entry per Aging Time timeout. The default Aging Time is 300 seconds. The Aging Time can be modified in this page.

Static Unicast MAC Address & Static Multicast 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

User can see all the MAC Addresses learnt by the switch. The table allows users to sort the address by the packet types and port. 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.



MAC Address Table All

MAC Address	Address Type	VID	1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/> 708b.cd03.b567	Dynamic Unicast	1	V									
<input type="checkbox"/> 0100.5e00.00fb	Dynamic Multicast	1	V									
<input type="checkbox"/> 0100.5e00.00fc	Dynamic Multicast	1	V									
<input type="checkbox"/> 0100.5e7f.ffa	Dynamic Multicast	1	V									

The address type description is below:

Static Unicast MAC address can be added and deleted.

Dynamic Unicast MAC is MAC address learnt by the switch.

Static Multicast can be added by CLI and can be deleted by Web and CLI.

Dynamic Multicast will appear after User enabled IGMP and the switch learnt IGMP report.

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.

3.12.3 PORT STATISTICS

In this page, User can view operation statistics for each port. The statistics that can be viewed include Link Type, Link State, Rx Good, Rx Bad, Rx Abort, Tx Good, Tx Bad and Collision. Rx means the received packet while Tx means the transmitted packets.

Home > Diagnostics > Port Statistics

LLDP | MAC Table | **Port Statistics** | Port Mirror | Event Logs | Ping

Port Statistics

Port	Type	Link	State	Rx Good	Rx Bad	Rx Abort	Tx Good	Tx Bad	Collision
<input type="checkbox"/> 1	100	Connected	Enable	63390868	0	336	507575716	0	0
<input type="checkbox"/> 2	0	Disconnected	Enable	1907	0	0	4272845	0	0
<input type="checkbox"/> 3	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 4	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 5	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 6	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 7	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 8	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 9	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 10	0	Disconnected	Enable	0	0	0	0	0	0

If the table shows many Bad, Abort or Collision counts increased, that may mean network cable is not connected well, the network performance of the port is poor, etc. Please check network cable, Network Interface Card of the connected device, the network application, or reallocate the network traffic, etc.

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.

3.12.4 PORT MIRROR

Port mirroring is a tool that allows user to monitor data being transmitted through a specific port. 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 that goes into or out of the Source Port(s) will be duplicated at the Destination Port. This traffic can then be analyzed at the Destination port using a monitoring device or application. A network administrator will typically utilize this tool for diagnostics, debugging, or fending off attacks.

The configuration and settings explain as following.

TERMS	DESCRIPTION
Port Mirror	Select Enable/Disable to enable/disable Port Mirror.
Source Port	This is also known as Monitor Port. These are the ports User wants to monitor. The traffic of all source/monitor ports will be copied to destination/analysis ports. User can choose a single port, or any combination of ports, but User can only monitor them in Rx or TX only. Click on checkbox of the Port ID, RX, Tx or Both to select the source ports.
Destination Port	This is also known as Analysis Port. User can analyze the traffic of all the monitored ports at this port without affecting the flow of traffic on the port(s) being monitored. Only one RX/TX of the destination port can be selected. A network administrator would typically connect a LAN analyzer or Netxray device to this port.

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

3.12.5 EVENT LOGS

When System Log Local mode is selected, the switch will record occurred events in local log table. This page shows this log table. The entry includes the index, occurred data and time and content of the events.

Home > Diagnostics > Event Logs

LLDP | MAC Table | Port Statistics | Port Mirror | **Event Logs** | Ping

Event Logs

Index	Date	Time	Event Log
1	Jan 1	02:10:36	Event: Relay Output1 change to close.
2	Jan 1	02:37:21	Event: Authentication Failure.

Clear **Reload**

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	Events that have occurred.

3.12.6 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.

Home > Diagnostics > Ping

LLDP | MAC Table | Port Statistics | Port Mirror | Event Logs | **Ping**

Ping

Destination

Ping

```
PING 192.168.1.6 (192.168.1.6): 56 data bytes
64 bytes from 192.168.1.6: seq=0 ttl=64 time=5.5 ms
64 bytes from 192.168.1.6: seq=1 ttl=64 time=0.8 ms
64 bytes from 192.168.1.6: seq=2 ttl=64 time=1.0 ms
64 bytes from 192.168.1.6: seq=3 ttl=64 time=0.8 ms

--- 192.168.1.6 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.8/2.0/5.5 ms
```

3.13 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 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

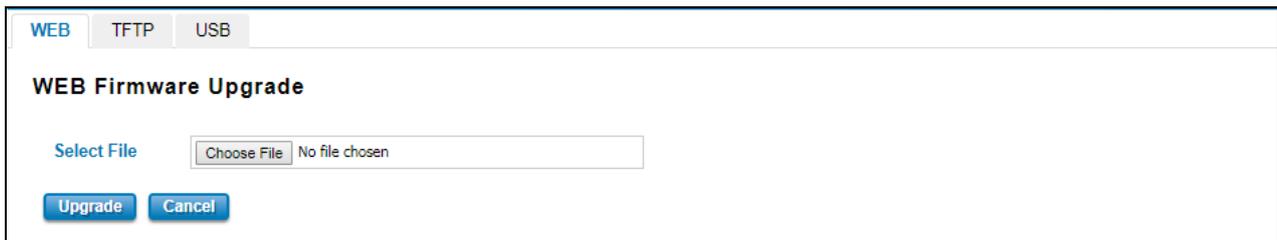
USB mode: this mode has two functions, Load Setting from File and Save Setting to USB. Load Setting from File, make sure that the USB has been plugged on and it has the .conf file which is the backup files. After plugged on the USB, the USB port will directly read the USB and then the backup file would 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**.

3.14 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**.

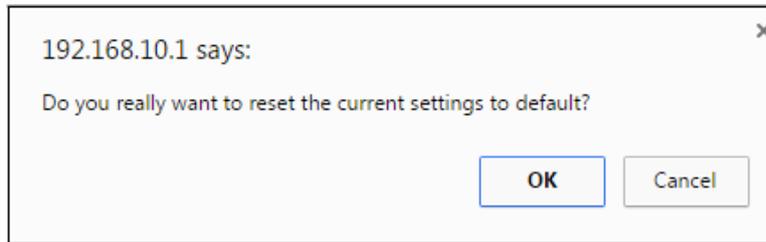
3.15 RESET TO DEFAULTS

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.

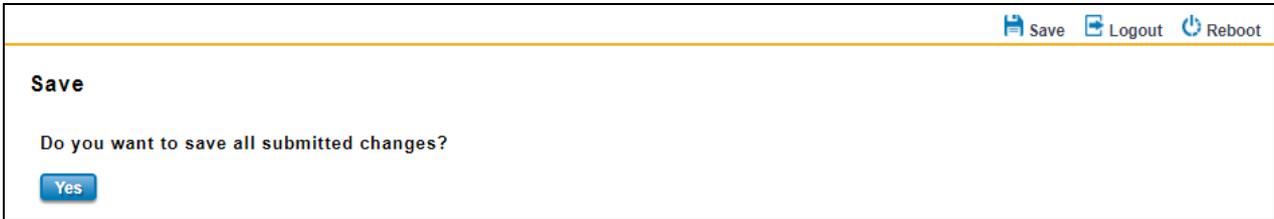


Then please go to **Reboot** page to reboot the switch. Click **OK**. The system will auto reboot the device.



3.16 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.



The screenshot shows a web interface with a top navigation bar containing 'Save', 'Logout', and 'Reboot' icons. Below the bar, the main content area is titled 'Save'. It contains the text 'Do you want to save all submitted changes?' and a single blue 'Yes' button.

3.17 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.



The screenshot shows a web interface with a top navigation bar containing 'Save', 'Logout', and 'Reboot' icons. Below the bar, the main content area is titled 'Logout'. It contains the text 'Do you want to logout?' and a single blue 'Yes' button.

3.18 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.

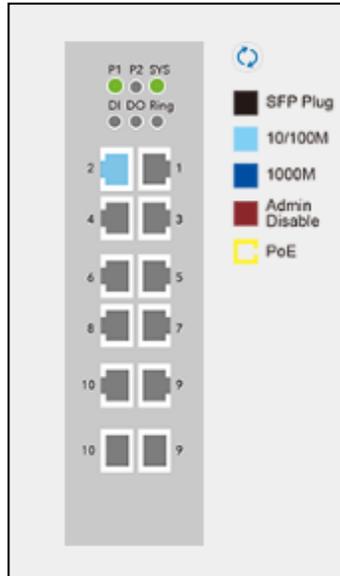
Reboot main screen, to do confirmation request. Click **Yes**, then the switch will reboot immediately.



The screenshot shows a web interface with a top navigation bar containing 'Save', 'Logout', and 'Reboot' icons. Below the bar, the main content area is titled 'Reboot'. It contains the text 'Do you want to reboot?' and a single blue 'Yes' button.

3.19 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 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. REVISION HISTORY

Version	Description	Date	Editor
V1.0	1 st released User Manual	2017/12/06	Yohan
V1.1	<ul style="list-style-type: none">- Remove spec. which can refer to datasheet- Add Modbus TCP function for FW V1.6- Update DP/DS310 dimension and DS310 front panel layout	2019/5/7	Kylie