WoMaster

COVER

User Manual

DRS610

Industrial 10-port Full Gigabit Secure Router Switch

Mar..2020 V1.0

www.womaster.eu

WoMaster

DRS610 Industrial 10-port Full Gigabit Secure Router Switch, 8GT+2GSFP

User Manual

Copyright Notice

About This Manual

This user manual is intended to guide a professional installer to install and to configure the DRS610 Secure Router Switch. It includes procedures to assist you in avoiding unforeseen problems.

NOTE:

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

Disclaimer

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

WoMaster Online Technical Services

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

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

DRS610 is WoMaster new Secure Din-Rail Route Switch product. DRS610 series is designed for industrial environments requiring high level of security design, LAN to WAN routing and high-speed Ethernet/Fiber communications, such as industrial automation, road traffic control, etc. The DRS610 Din-Rail layer 3 Router Switch supports dual WAN ports, NAT, Firewall, OpenVPN, IPSec, Routing, and L2 managed switch features such as VRRP routing and ERPS v2 network redundancy. The industrial design features wide operating temperature from -40~70ºC and high EMC protection. The platform supports cellular LTE and 5G extension by request.

DRS610 provides 10-port full-gigabit Ethernet port, it includes 2-port Gigabit RJ45 WAN port, 6-port Gigabit RJ45 and 2 100M/1000M SFP ports. The 2 WAN ports are configured to WAN 1 and WAN 2 with its own MAC address, that can be independently configure and work. The rest of 6 Gigabit RJ45 and 2 100M/1000M SFP are pre-configured as LAN ports, they supports L2 switching, management and LAN to WAN routing features. The 100M/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.

This Secure Router Switch is designed to provide faster, secure, and more stable network. One advantage that makes it a powerful switch is that it supports high speed 1.2GHz ARM processor, Dual WAN ports with fast Routing and WAN Redundancy Protection, 8 Gigabit LAN port with wire-speed L2+ switching and fast routing to WAN capacity. With one switch and WoMaster embedded software, you can have both secure Router VPN/Firewall/NAT and L3/L2 managed Routing/Switching/Redundancy/Security functionalities within one device. All of these features in order to ensure the fast and secure data communication.

1.2 MAJOR FEATURES

Below are the major features of DRS610 Secure Router Switch:

- Highly integrated Secure NAT/Firewall/VPN Router and L3/L2 Managed Switch features
- 10-port Full Gigabit Ethernet ports, including 2-port Gigabit RJ-45 WAN and 6-port Gigabit RJ-45 plus 2-port 100M/1000M Fiber SFP LAN ports
- Powerful 1.2GHz ARM Cotex-A9 processor and Non-blocking switch fabric design
- Dual WAN ports available for Network address Translation (LAN) Routing, >100Mbps LAN to WAN NAT Routing Performance
- Firewall for traffic classification, port forwarding, DMZ and deep packet inspection for Modbus TCP/UDP*
- Support OpenVPN, IPsec, DMVPN* for secure remote access
- Support VRRP for router redundancy
- Built-in DHCP Server that automatically provides and assigns IP addresses, default gateways to clients
- SFP ports support 100/1000 Mbps with Digital Diagnostic Monitoring (DDM) to monitor fiber quality
- All ports provide sub-50ms protection and recovery switching for Ethernet traffic.
- Rapid Spanning Tree Protocol (RSTP)/Multiple Spanning Tree Protocol (MSTP) and express RSTP(eRSTP)
- ITU-T G.8032 v1/v2 Ethernet Ring Protection Switching (ERPSv2)
- Dynamic Routing with Redundancy Protection: RIPv1&v2, OSPFv1&v2 for intra-domain routing within an autonomous system.
- VRRP guarantees sustainable routing in a single point of failure.
- Advanced management features: LACP/VLAN/Q-in-Q/Private VLAN/ GVRP/QoS/IGMP Snooping/Rate Control/ Online Multi-Port Mirror/ Advanced DHCP server, Client,
- Advanced Security system by Port Security, Access IP list, SSH and HTTPS Login
- Event Notifications through E-mail, SNMP trap and SysLog
- IEEE 802.1AB LLDP and optional NMS software for auto-topology and group management
- CLI interface, Web, SNMP/RMON for network Management
- Multiple event relay output for enhanced alarm control
- Hi-Pot Isolation Protection for ports and power
- Steel Metal with Aluminum for heat dissipation
- Wide range operating temperature -40~75˚C
- IP31 ingress protection

2. HARDWARE INSTALLATION

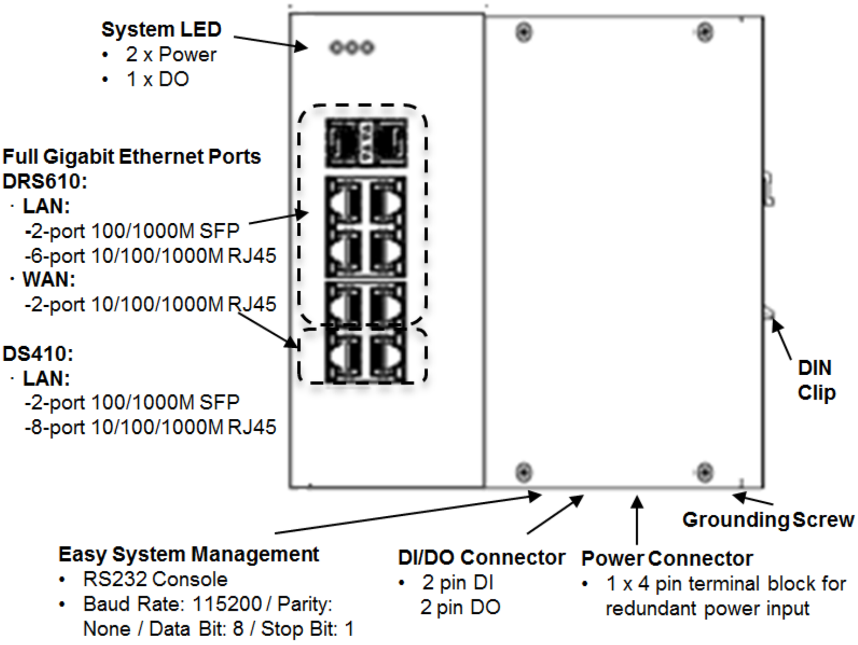
This chapter introduces hardware, and contains information on installation and configuration procedures.

2.1 APPEARANCE, PORT MAP & DIMENSION

Front Panel Layout

The front panel from DRS610 includes 8 ports Giga Ethernet, 2 SFP ports, System LED, diagnostic console, 2 x 4-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 port LED is equipped with the RJ45 and SFP connector. On the rear side of switch there is DIN rail clip attached.

DRS610



System LED
• 2 x Power
• 1 x DO
Full Gigabit Ethernet Ports
DRS610:
· LAN:
-2-port 100/1000M SFP
-6-port 10/100/1000M RJ45
· WAN:
-2-port 10/100/1000M RJ45
DS410:
· LAN:
-2-port 100/1000M SFP
-8-port 10/100/1000M RJ45
DIN Clip
Grounding Screw
Easy System Management
• RS232 Console
• Baud Rate: 115200 / Parity: None / Data Bit: 8 / Stop Bit: 1
DI/DO Connector
• 2 pin DI
2 pin DO
Power Connector
• 1 x 4 pin terminal block for redundant power input

LED Indication

LED	Status	Description
PWR (P1/P2)	Green On	DC-IN Power is On
	Off	No Power in DC-IN
Alarm (DO)	Red On	Any failures in port link, ping, power, DO and DI State by SW control
	Off	No failure occurs

LED	Status	Description
RJ45 Port	Green On	Links established
	Green Blinking	Packets transmitting/receiving
	Green Off	Link is inactive
	Amber On	Link Speed 1000M
	Amber Off	Link Speed 100M
SFP Port	Green On	Links established
	Green Blinking	Packets transmitting/receiving
	Green Off	Link is inactive
	Amber On	Link Speed 1000M
	Amber Off	Link Speed 100M

Port MAP, Default IP / WAN Interface

Interface			**DRS610**	
Interface	**Media**	**Web GUI ID**	Default IP	MAC Address
1 (WAN1)	Copper RJ45	WAN1	192.168.1.1	2nd MAC in label
2 (WAN2)	Copper RJ45	WAN2	192.168.2.1	3rd MAC in label
3~8	Copper RJ45	1~6	192.168.10.1 (VLAN 1)	1st MAC in label
9~10	Fiber SFP	7~8		

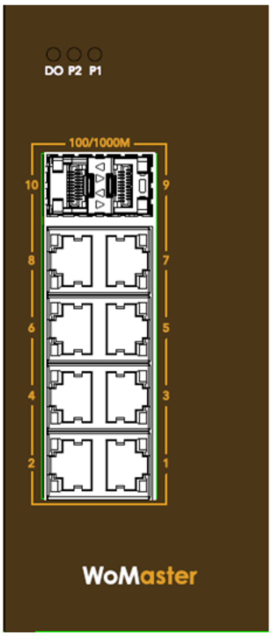
Note 1: The name of LAN port in Web GUI is started from 1~8. The physical WAN port is 1, 2 which represent for WAN 1/WAN2.

Note 2: There are 3 MAC address for DRS610's WAN1/WAN2/LAN interfaces. The print label indicates the 1st MAC of LAN interface. Add one number to the second MAC and two numbers to the third MAC address.

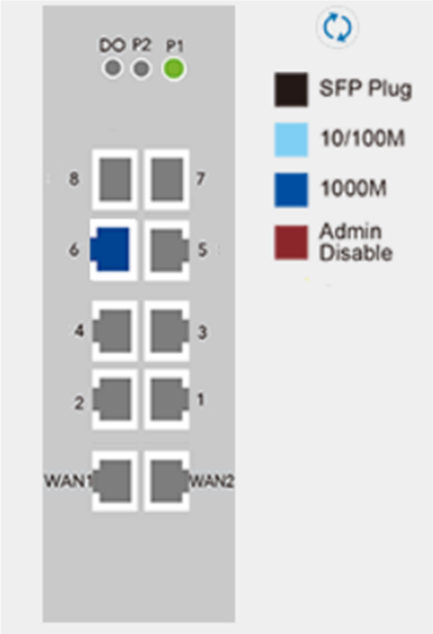
Note 3: The WAN IP is allowed to ping, but, not allowed to access web GUI in default configuration. You should enter the GUI by LAN interface and change the security policy for remote WAN access.

Note 4: Above setting is based on DRS610 V1.0 firmware. Other media type WAN port can be customized, contact our Sales for further discuss.

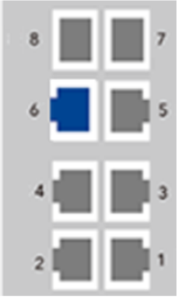
Interface



Web GUI Panel



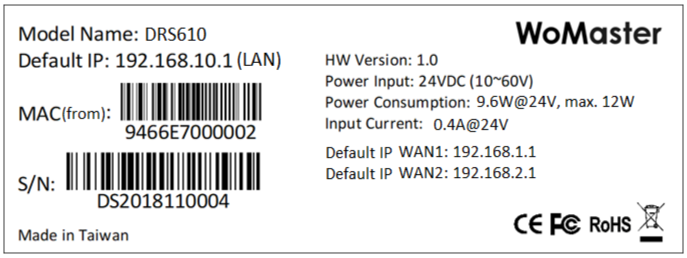
LAN Port ID



RJ45: 1~6
SFP Plug: 7/8

Product Label

Normally, you can find the product label on the top or rear side of the housing. It shows the Model Name, Default IP address, MAC address, Series number and related parameters. There are 3 MAC address for WAN1/WAN2/LAN interfaces, the MAC(from) in print label indicates the 1st MAC for LAN interface.



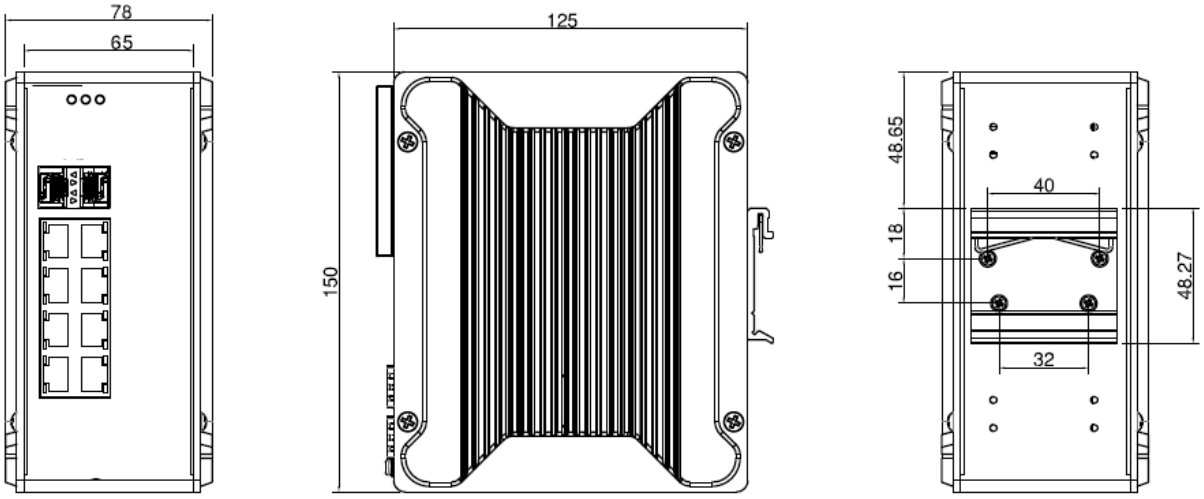
Model Name: DRS610
Default IP: 192.168.10.1 (LAN)
MAC(from): 9466E7000002
S/N: DS2018110004
Made in Taiwan

WoMaster
HW Version: 1.0
Power Input: 24VDC (10~60V)
Power Consumption: 9.6W@24V, max. 12W
Input Current: 0.4A@24V
Default IP WAN1: 192.168.1.1
Default IP WAN2: 192.168.2.1
CE FC RoHS

Add one number to the second MAC for WAN1, and two numbers to the third MAC address for WAN2. The last digit of MAC address is step by hex16, range from 0~9, A~F, for example the next MAC of 9466E7000002 is 9466E7000003…etc.

Dimension

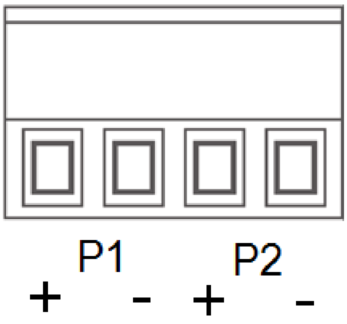
Dimensions of DRS610: 78 x 150 x 125 (W x H x D) / without DIN Rail Clip



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.



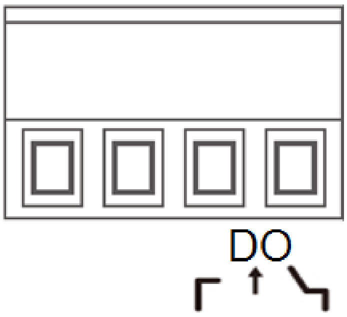
Wiring the Power Input

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 typical input DC voltage is 24V and should be in the range of 10VDC to 60VDC (recommended to use DC 24V power supply).

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

2.3 WIRING THE ALARM RELAY OUTPUT (DO)

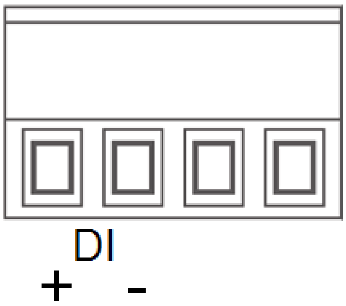
The relay output contacts are located on the front panel of the switch. The relay output consists of the 2-pin terminal block connector that used to detect user-configured events. The two wires attached to the fault contacts form a close circuit when a user-configured event is triggered. If a user-configured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



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

2.4 WIRING THE DIGITAL INPUT (DI)

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



Here are the steps to wire the Digital Input:

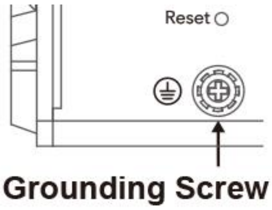
STEP 1: Insert the negative and positive wires into the -/+ terminals, respectively.

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

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

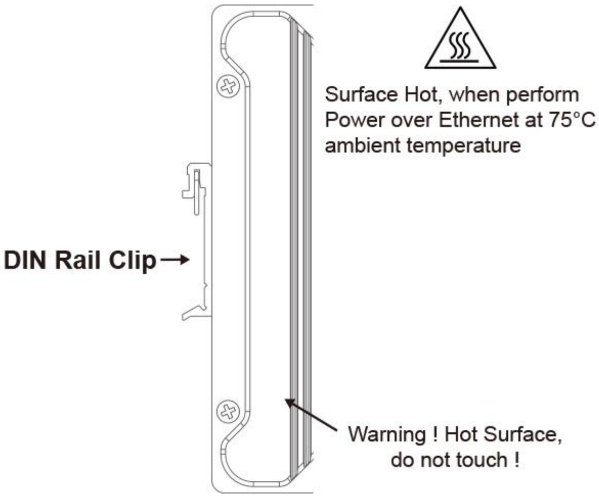
2.5 CONNECTING THE GROUDING SCREW

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



2.6 DIN RAIL MOUNTING

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


Surface Hot, when perform Power over Ethernet at 75°C ambient temperature
DIN Rail Clip
Warning ! Hot Surface, do not touch !

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.

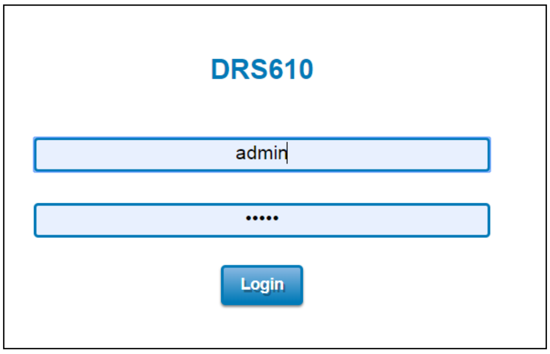
3. WEB MANAGEMENT CONFIGURATION

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.

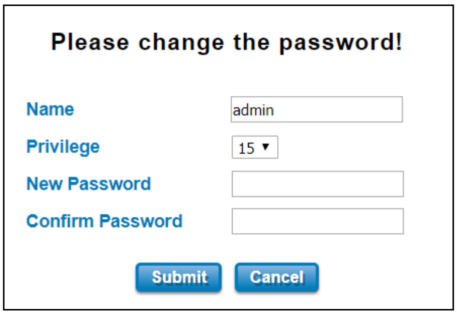
1. Plug the DC power to the switch and connect switch **(LAN port of the Router Switch)** to computer.
2. Make sure that the switch default IP address is **192.168.10.1**.
3. Check that PC has an IP address on the same subnet as the switch. For example, the PC and the switch are on the same subnet if they both have addresses that start 192.168.10.x (Ex: **192.168.10.2)**. The subnet mask is 255.255.255.0.
4. Open command prompt and ping **192.168.10.1** to verify that the switch is reachable.
5. Launch the web browser (Internet Explorer or Mozilla Firefox or Google Chrome) on the PC.
6. Type http://192.168.10.1 (or the IP address of the switch). And then press **Enter** and the login page will appear.
7. For security concern, the system will ask you enter New User **Name, Privilege, New Password and Confirm Password** at first Login, please follow the indication to enter new username, Privilege and password. You must add New User Name with **Privilege 15 (Administrator privilege)** at first login.
8. Type New user name and the password in first login. Then click **Login**.



DRS610

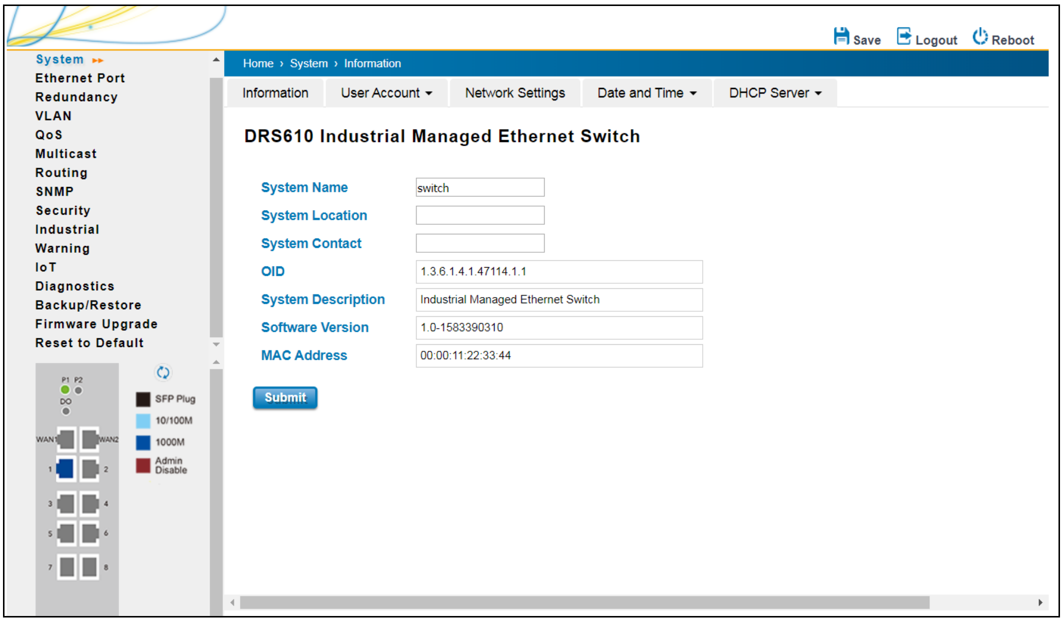
admin

•••••



Please change the password!

Name	admin
Privilege	15 ▾
New Password	
Confirm Password	



DRS610 Industrial Managed Ethernet Switch

System Name	switch
System Location	
System Contact	
OID	1.3.6.1.4.1.47114.1.1
System Description	Industrial Managed Ethernet Switch
Software Version	1.0-1583390310
MAC Address	00:00:11:22:33:44

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 IoT

3.4 Redundancy

3.5 VLAN

3.6 QoS

3.7 Multicast

3.8 Routing

3.9 SNMP

3.10 Security

3.11 Warning

3.12 Diagnostics

3.13 Backup / Restore

3.14 Firmware Upgrade

3.15 Reset to Defaults

3.16 Industrial

3.17 Save

3.18 Logout

3.19 Reboot

3.20 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

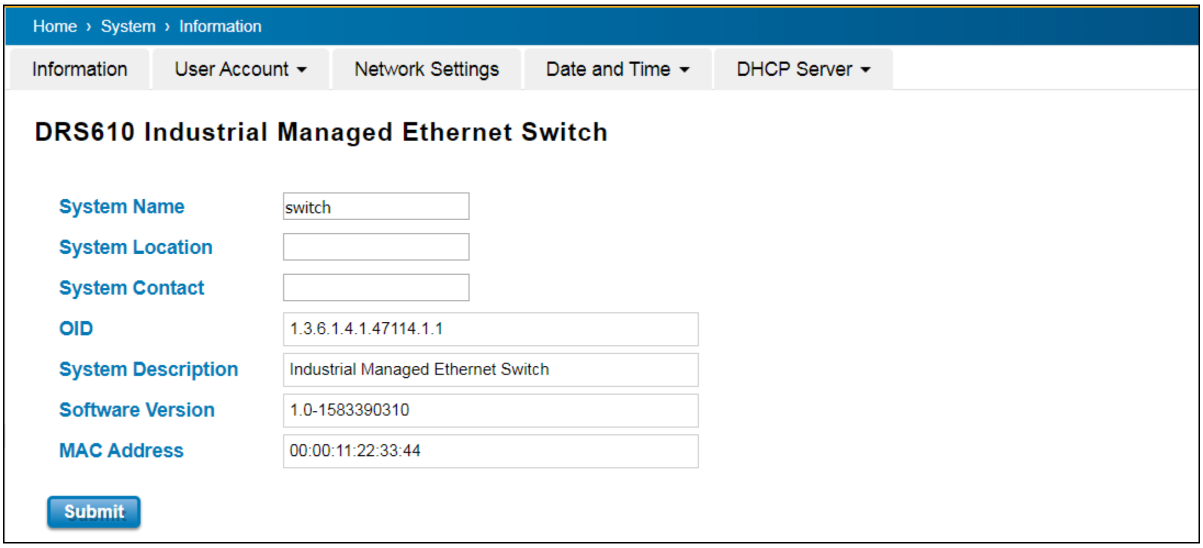
3.1.3 Network Setting

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.



DRS610 Industrial Managed Ethernet Switch

System Name	switch
System Location	
System Contact	
OID	1.3.6.1.4.1.47114.1.1
System Description	Industrial Managed Ethernet Switch
Software Version	1.0-1583390310
MAC Address	00:00:11:22:33:44

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.

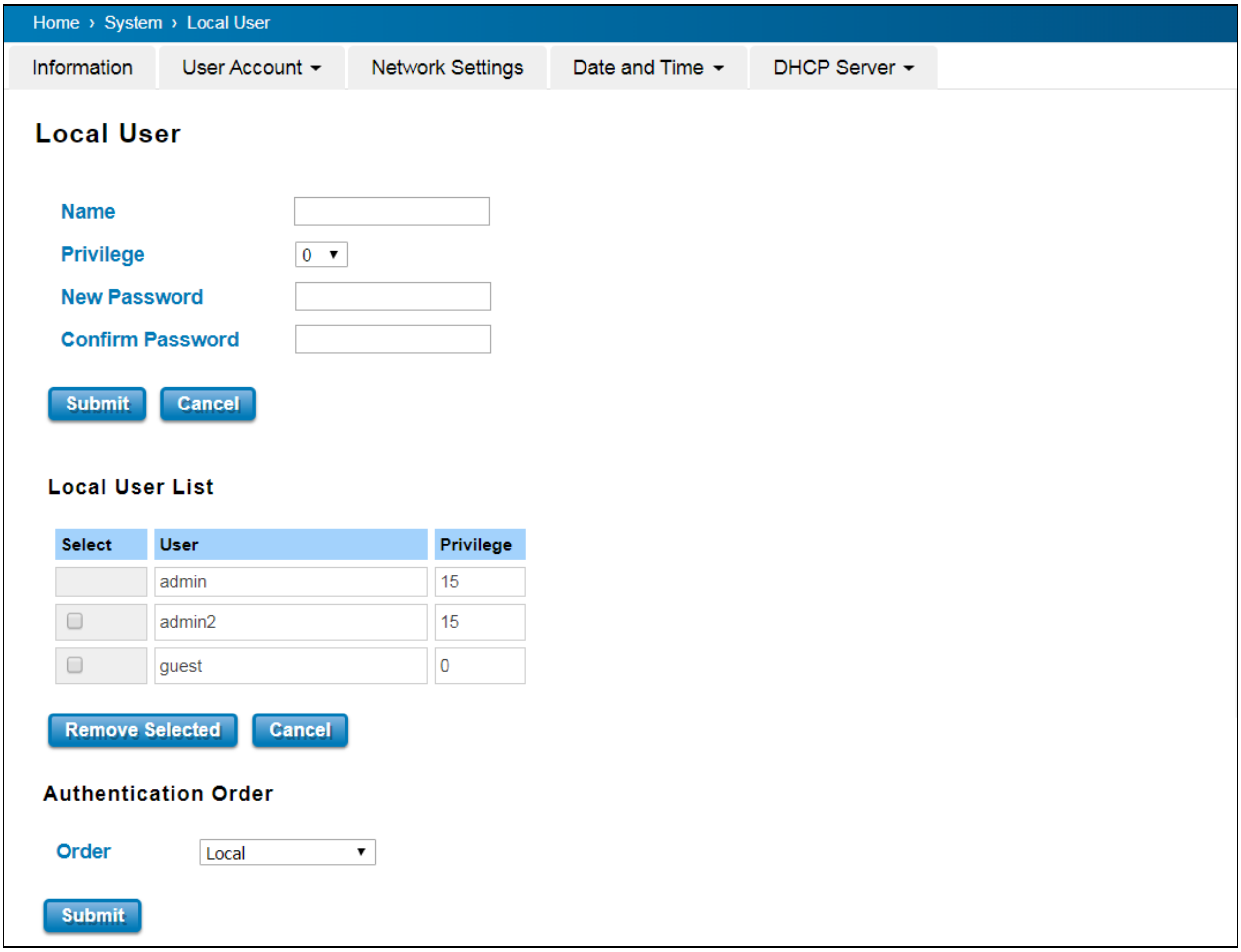
After finish the configuration, click on **Submit** to apply User settings.

3.1.2 USER ACCOUNT

WoMaster' 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 concern, the system will ask you enter New User **Name, Privilege, New Password and Confirm Password** at first Login.
> NOTE: You must have a**t least one User Name with Privilege 15 (Administrator privilege) in local user List,** otherwise you can't change the switch setting any more.

3.1.2.1 LOCAL USER



Local User

Name
Privilege 0 ▾
New Password
Confirm Password

Submit Cancel

Local User List

Select	User	Privilege
	admin	15
□	admin2	15
□	guest	0

Remove Selected Cancel

Authentication Order

Order Local ▾

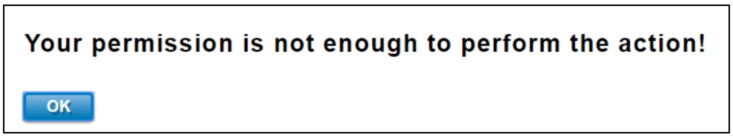
Submit

The Local User interface describes how to configure the system user name, privilege and password for the web management login. To change the Name, Privilege and Password, user just needs to input a new Name, select the

Privilege and New Password then confirm the new password in this Local User section. After finished, click **Submit** to apply the changes. You can see the new user setting is added in the table of **Local User List**. Don't forget to **Save** the settings. Try to re-login with the new User Name and Password.

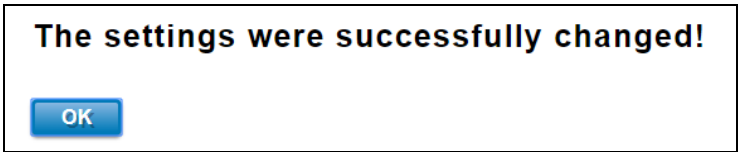
Privilege: The privilege 15 represent for administrator privilege, user can read and configure the new settings. The privilege 0 represent for Read-Only privilege. You must have a**t least one User Name with Privilege 15 (Administrator privilege) in local user list,** otherwise you can't change the switch setting any more.

Once you try change the new setting with "0" privilege, the system will prompt error message as below:



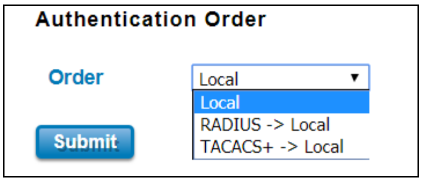
Your permission is not enough to perform the action!

Remove the user: you can Select the checkbox of the user, click "Remove Selected" to apply the change. You will see the below prompt message.



The settings were successfully changed!

Authentication Order: Select the order of the authentication types. Click "Submit" to apply the change.



Authentication Order

Order: Local

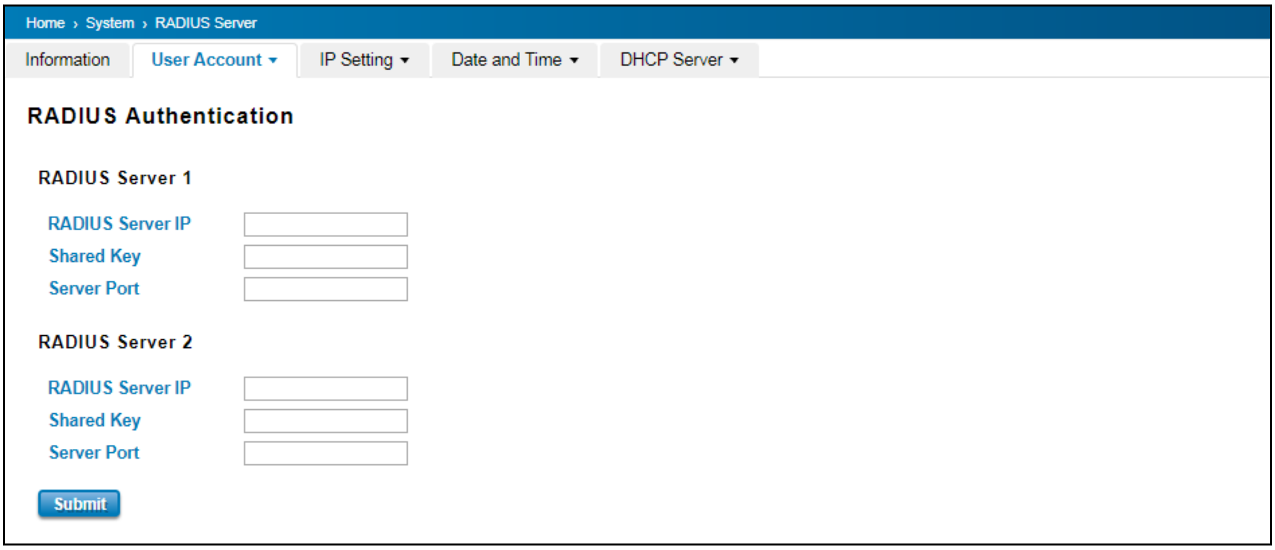
The description of the Local User interface is as below:

TERMS	DESCRIPTION
Name	**Default: admin** Key in new user name here.
Privilege	**15:** Administrator, Read and Write the new configuration **0:** Guest, Read-Only
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.



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:

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

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

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

d. Click **Submit**

The description of the RADIUS Authentication interface is as below:

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

3.1.2.3 TACACS+

The Terminal Access Controller Access Control System (TACACS+) security protocol is a recent protocol developed by Cisco. It provides detailed accounting information and flexible administrative control over the authentication and authorization processes. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide authentication, authorization, and accounting services independently. Below TACAS+ server setting allows you to configure TACAS+ Server settings.

How to set up a TACACS+ server:

a. Select the **Authentication Type.**

b. Enter the **Authentication Timeout** in seconds.

c. Enter the IP address of the TACACS+ server in **Server IP Address.**

d. Enter the **Shared Secret** of the TACACS+ server.

e. Enter the **Server port** if necessary, by default TACACS+ server listens to port 49.

f. Click **Submit**

The description of the TACAS+ interface is as below:

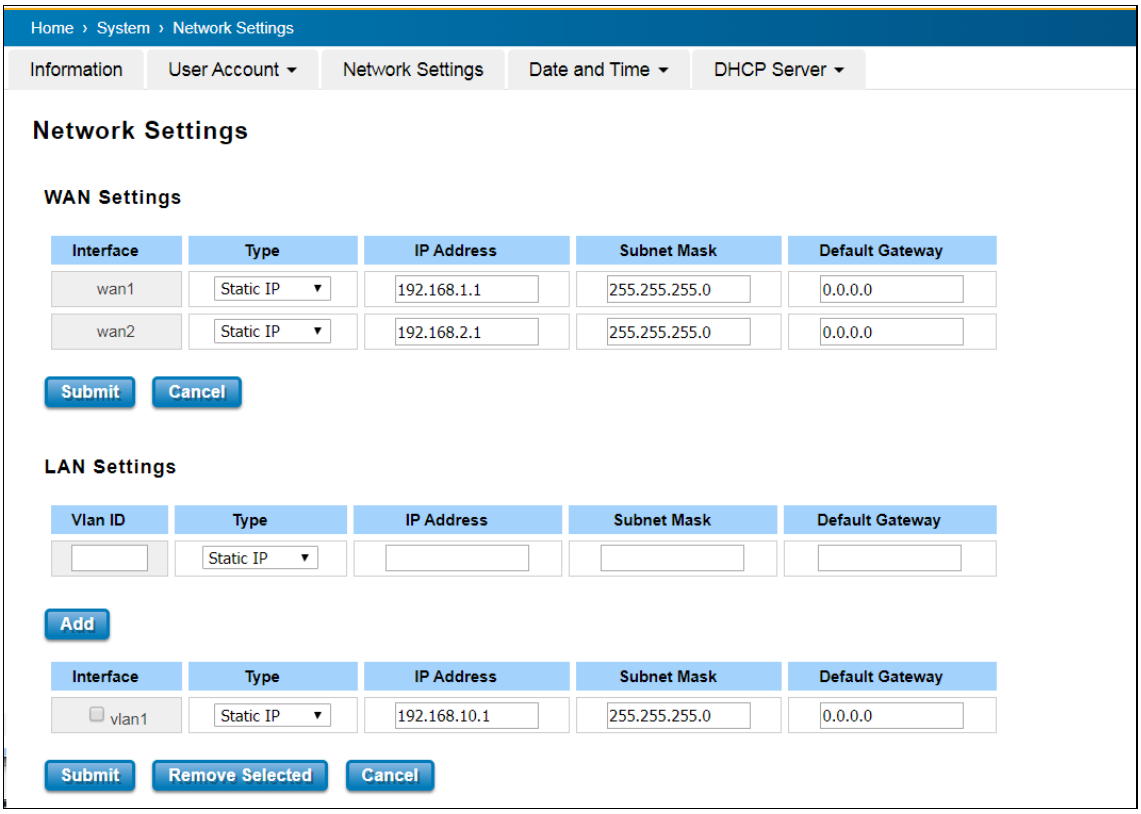
TERMS	DESCRIPTION
TACAS+ Server IP	TACACS+ Server IP Address. The system allows 2 TACAS+ servers
Share Key	Specifies the shared key for TACACS+ communications between the device and the TACACS+ server. The shared key must match the encryption used on the TACACS+ server.
Server Port	Set communication port of an external TACACS+ server as the authentication database. The general value is 49
Authentication Type	**Type: PAP,** ASCII, CHAP Select the authentication type to authenticate to the server.
Server Timeout	**Default: 5** The maximum number of seconds allowed establishing a TCP connection between the device and the TACACS+ server.

3.1.3 NETWORK SETTINGS

Network Setting section allows users to configure the WAN, LAN, DNS and ARP settings. WoMaster DRS610 Router Switch supports LAN to WAN routing. In this page, you can configure DHCP Client or Static IP and input the IP address, subnet mask and default gateway for the specific interface.

3.1.3.1 Network Settings(DRS610)

WAN Settings (DRS610)



Network Settings

WAN Settings

Interface	Type	IP Address	Subnet Mask	Default Gateway
wan1	Static IP	192.168.1.1	255.255.255.0	0.0.0.0
wan2	Static IP	192.168.2.1	255.255.255.0	0.0.0.0

LAN Settings

Vlan ID	Type	IP Address	Subnet Mask	Default Gateway
	Static IP			

Interface	Type	IP Address	Subnet Mask	Default Gateway
□ vlan1	Static IP	192.168.10.1	255.255.255.0	0.0.0.0

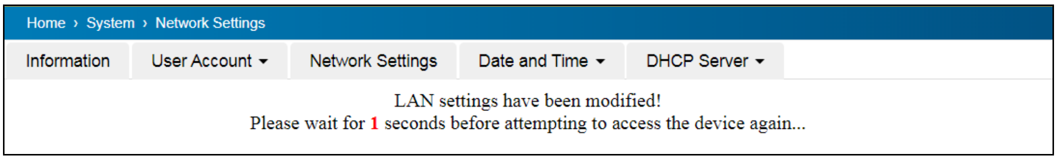
Refer to the section 2.1, Hardware Appearance and Dimension. You can find the physical port 1 is the interface of WAN 1, physical port 2 is WAN 2. The rest of physical ports are belonged to LAN interface in default.

Interface /Media		DRS610	
		Default IP	MAC Address
1 (WAN 1)	Copper RJ45	192.168.1.1	2nd MAC in label
2 (WAN 2)	Copper RJ45	192.168.2.1	3rd MAC in label
3~8	Copper RJ45	192.168.10.1	1st MAC in label

LAN Settings (DRS610)

The system also allows virtual IP interface for LAN ports to support inter-vlan routing. You can add VLAN interface and assign its network setting here. Type new VLAN ID, assign network settings and then click “**Add**”, you can find new VLAN interface is added. Refer to the Ch. 3.5 VLAN and 3.8.1.1 Inter-VLAN Routing to know more about how to add VLAN, binding port to VLAN and VLAN interfaces setup.

You can change the IP settings for the created VLAN interface, Click “**Submit**” to activate the new settings. And you’ll see the prompt while the system is going to active new setting.

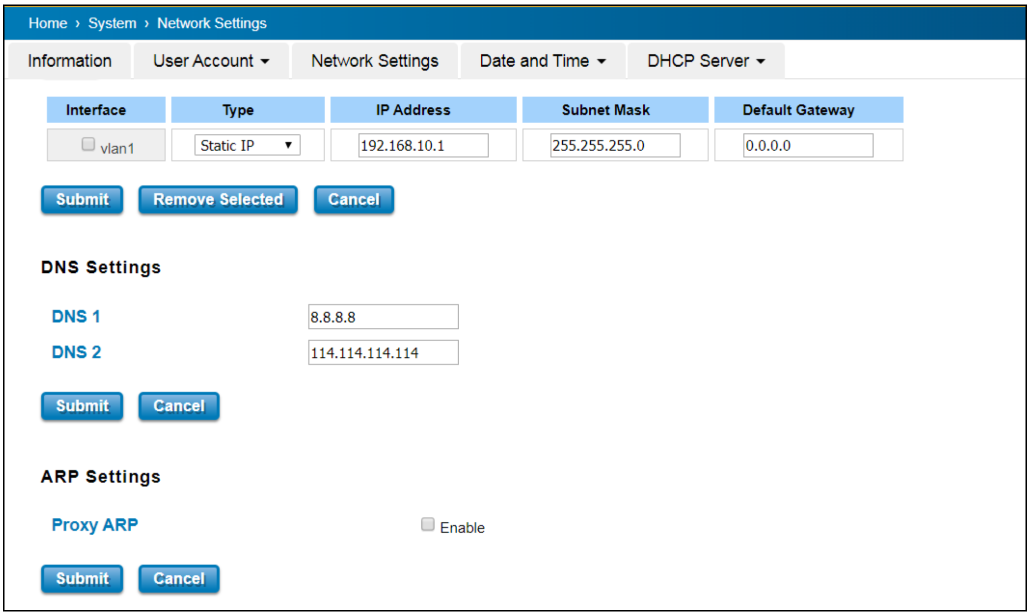


LAN settings have been modified!
Please wait for 1 seconds before attempting to access the device again...

The description of the columns is as below:

TERMS	DESCRIPTION
Interface	**WAN1: WAN port 1** **WAN2: WAN port 2** **LAN: VLAN inteface for LAN ports. Default VLAN ID/IP Interface is 1.**
VLAN ID	**Default: VLAN 1 and default IP address is configured in default.** Type new VLAN ID, assign network settings and then click "**Add**", you can find new VLAN interface is added. While adding new VLAN interface, the VLAN ID should be created in VLAN setup page first.
IP Address	**Default Mode: Static IP** **Default IP: 192.168.1.1/WAN1, 192.168.2.1/WAN2, 192.168.10.1/LAN** 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	Assign the gateway for the switch here.

DNS / ARP Setting



Interface	Type	IP Address	Subnet Mask	Default Gateway
□ vlan1	Static IP	192.168.10.1	255.255.255.0	0.0.0.0

DNS Settings

DNS 1 8.8.8.8

DNS 2 114.114.114.114

ARP Settings

Proxy ARP □ Enable

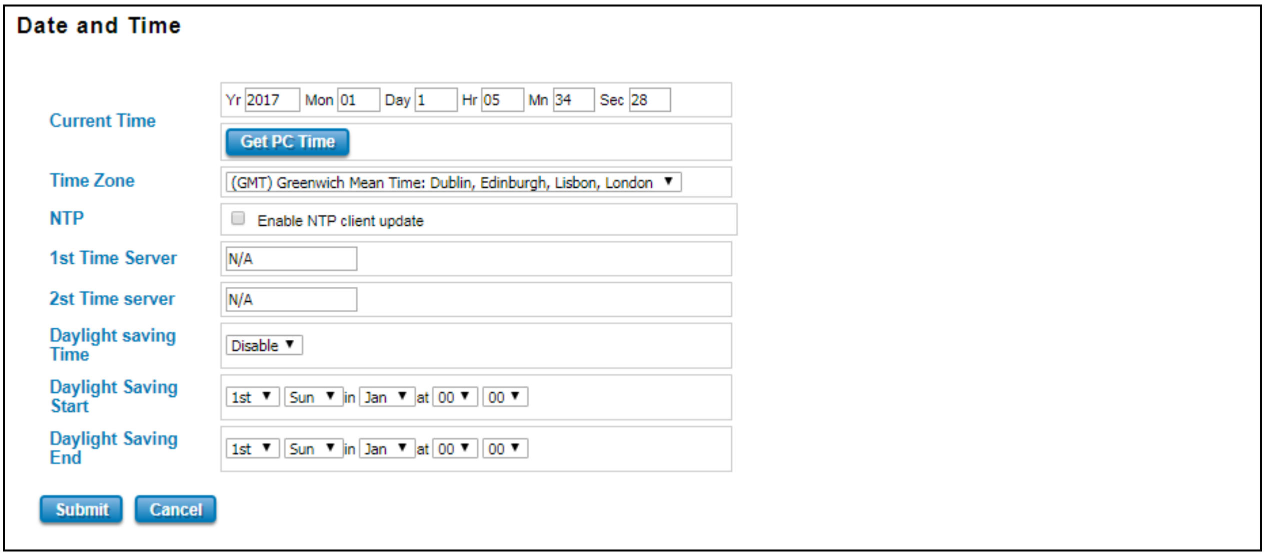
You can add two DNS Server IP Address settings for your system, and "Enable" Proxy ARP while you need.

3.1.4 DATE AND TIME

3.1.4.1 DATE AND TIME SETTING

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

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



Date and Time

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

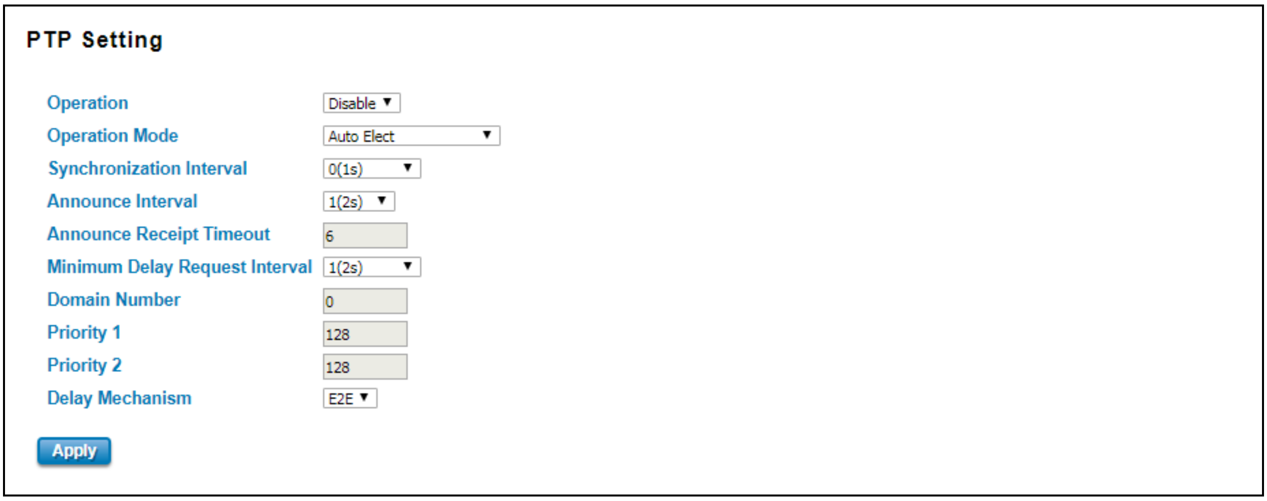
2. The switch must be configured so that it does not pass IEEE 1588 message traffic using the normal communication mechanisms of the switch.

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	Disable ▼
Operation Mode	Auto Elect ▼
Synchronization Interval	0(1s) ▼
Announce Interval	1(2s) ▼
Announce Receipt Timeout	6
Minimum Delay Request Interval	1(2s) ▼
Domain Number	0
Priority 1	128
Priority 2	128
Delay Mechanism	E2E ▼

The description of the columns is as below:

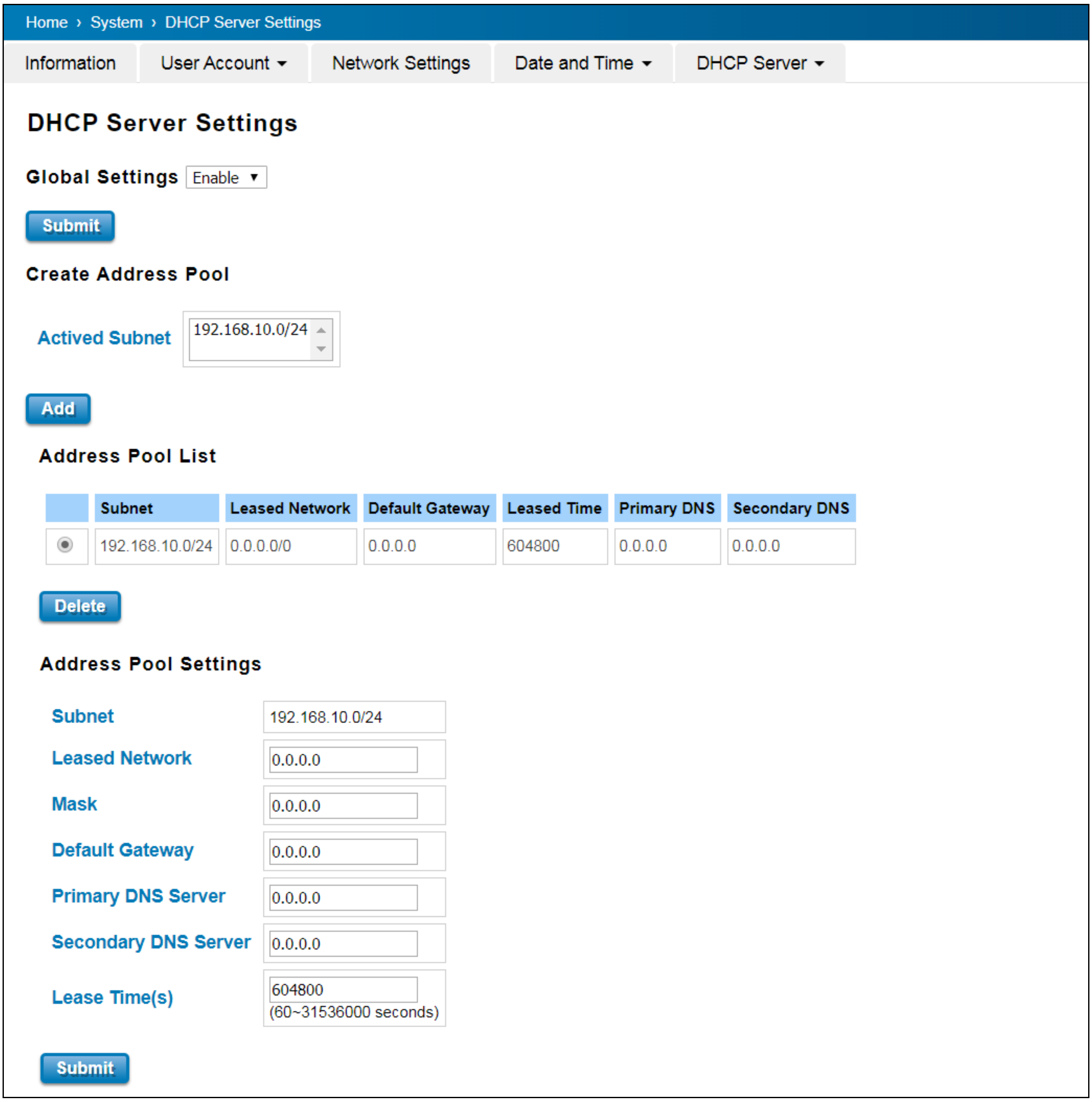
TERMS	DESCRIPTION
Operation	**Default: Disable** Enable/Disable the PTP function. This is the main option that needs to be enabled so that the PTP function will work
Operation Mode	**Default: Auto Elect** Choose Mode (Auto Elect, Preferred Master Clock or Slave)
Synchronization Interval	**Default: 0 (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 Settings

Global Settings: Enable ▾

Create Address Pool

Actived Subnet: 192.168.10.0/24

Address Pool List

	Subnet	Leased Network	Default Gateway	Leased Time	Primary DNS	Secondary DNS
●	192.168.10.0/24	0.0.0.0/0	0.0.0.0	604800	0.0.0.0	0.0.0.0

Address Pool Settings

Subnet	192.168.10.0/24
Leased Network	0.0.0.0
Mask	0.0.0.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Lease Time(s)	604800 (60~31536000 seconds)

The description of the columns is as below:

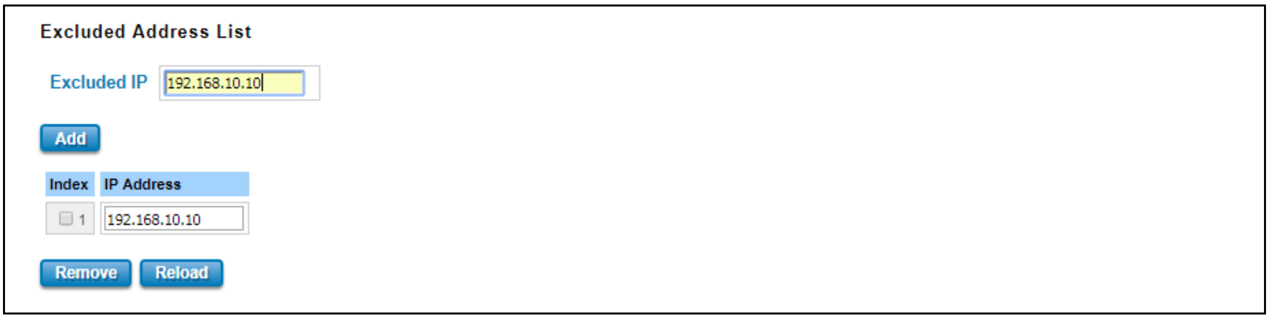
TERMS	DESCRIPTION
Global Setting	Select to **Enable** or **Disable** to activate and deactivate DHCP Server function.
Address Pool Add	Add address pool to local DHCP Server
Address Pool List	Choose the address pool setting that has been entered

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.



Excluded Address List

Excluded IP: 192.168.10.10

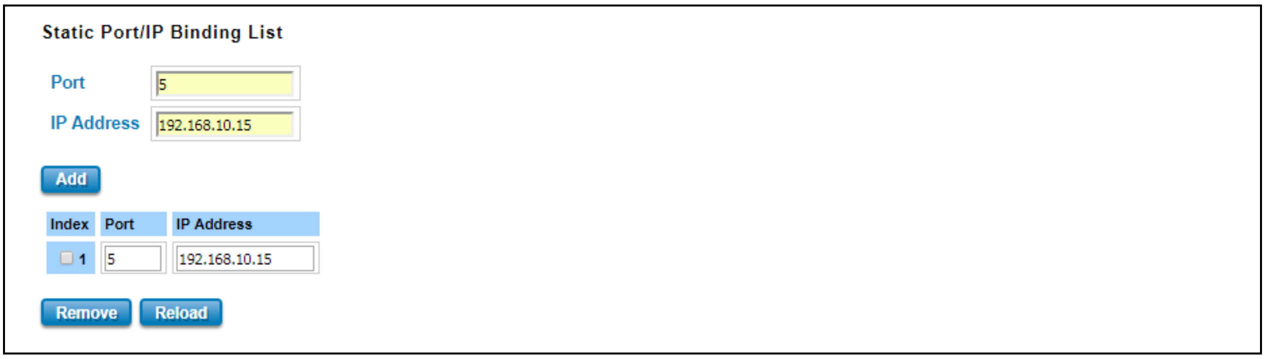
Index	IP Address
□ 1	192.168.10.10

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.**



Static Port/IP Binding List

Port: 5

IP Address: 192.168.10.15

Index	Port	IP Address
□ 1	5	192.168.10.15

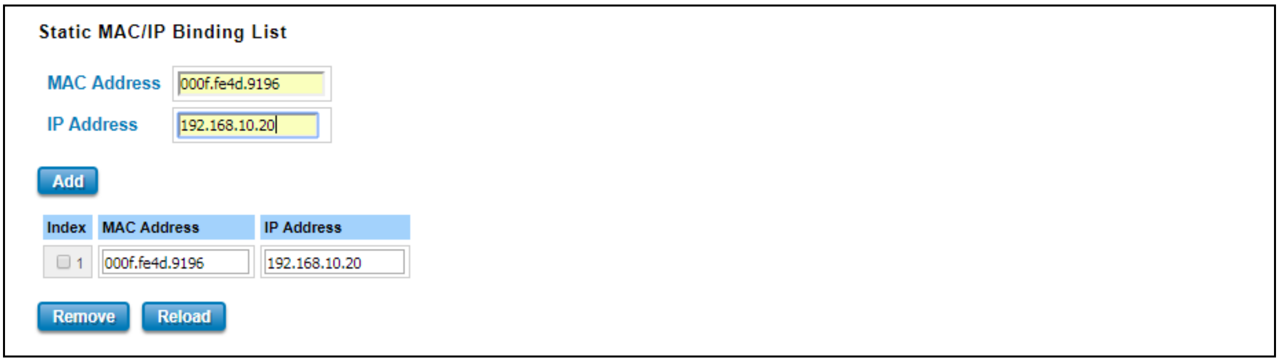
Type the specific Port and IP address, and then click **Add** to add a new Port & IP address binding rule for a specific client. The description of the columns is as below:

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: 000f.fe4d.9196

IP Address: 192.168.10.20

Index	MAC Address	IP Address
□ 1	000f.fe4d.9196	192.168.10.20

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

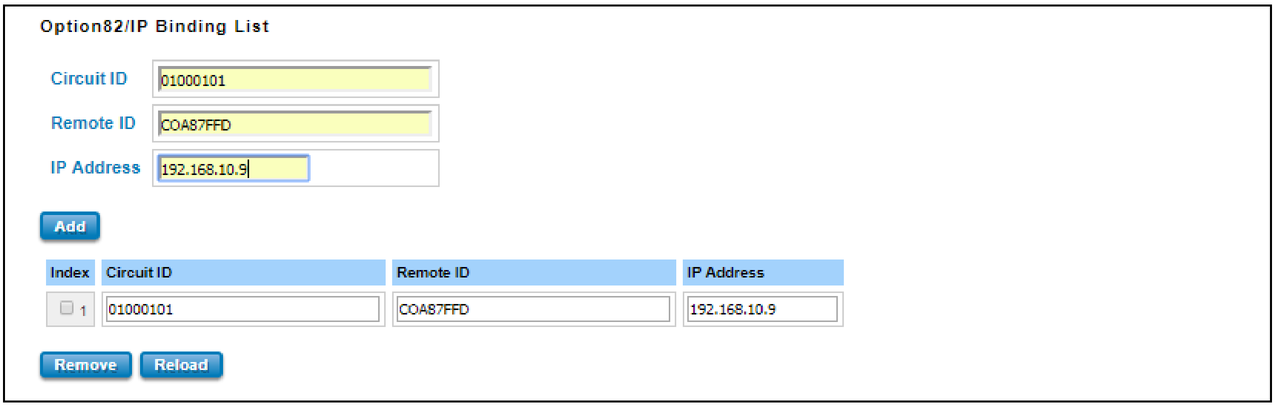
The description of the columns is as below:

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: 01000101

Remote ID: COA87FFD

IP Address: 192.168.10.9

Index	Circuit ID	Remote ID	IP Address
□ 1	01000101	COA87FFD	192.168.10.9

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**.

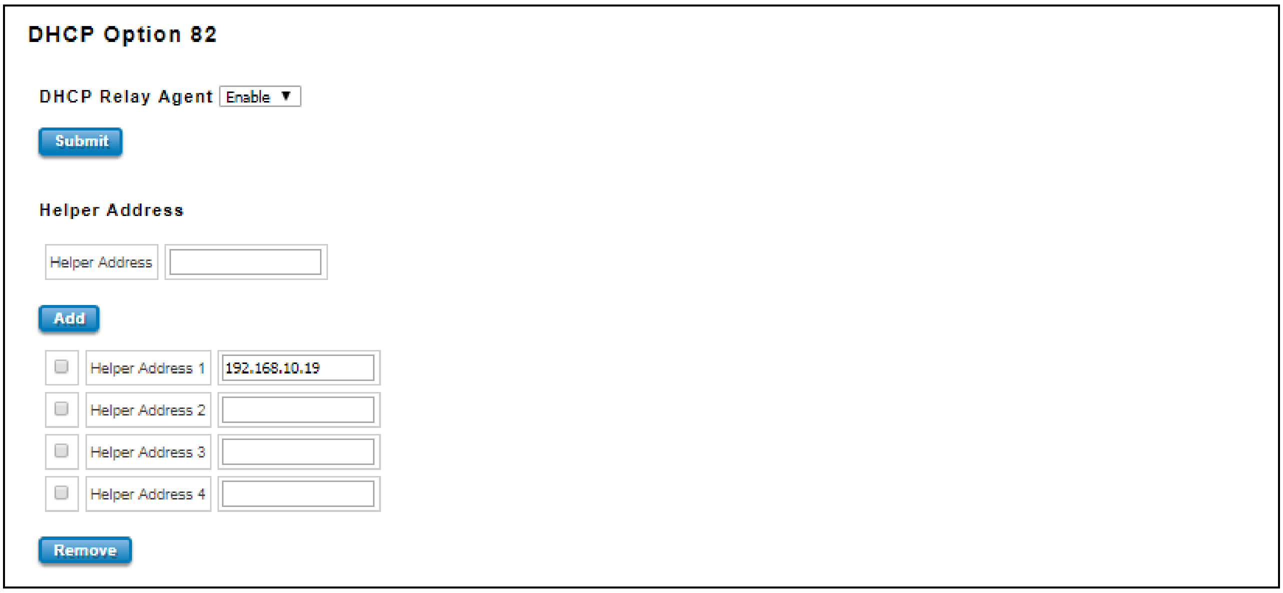
DHCP Option 82

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: Enable

Helper Address

Helper Address:

□	Helper Address 1	192.168.10.19
□	Helper Address 2	
□	Helper Address 3	
□	Helper Address 4	

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.

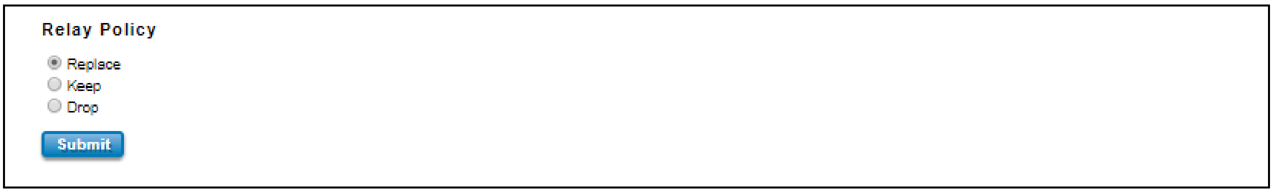
And click **Submit** to activate the DHCP relay agent function. All the DHCP packets from client will be modified by the policy and forwarded to DHCP server through the gateway port. When **Option 82** is enabled on the switch, a subscriber device is identified by the switch port through which it connects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

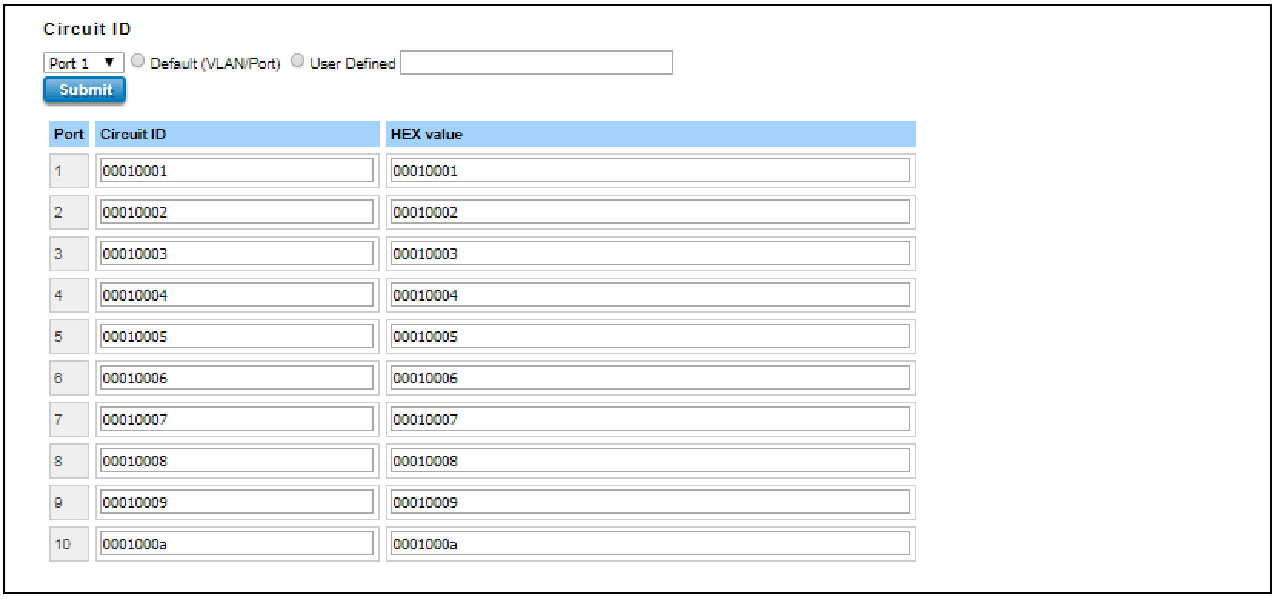


Relay Policy

● 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.

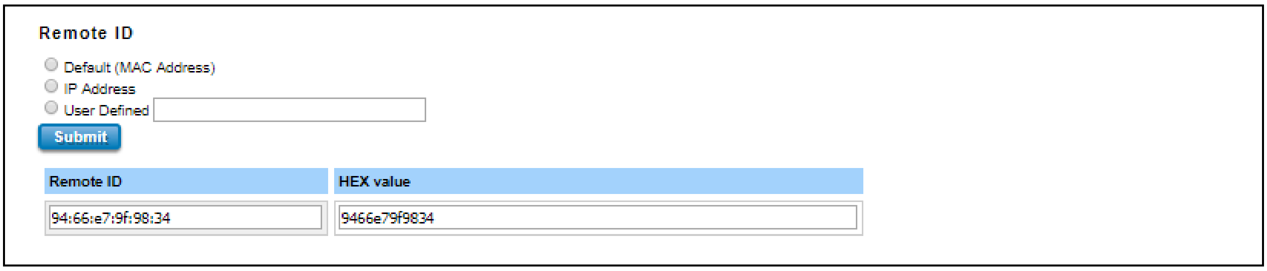


Circuit ID

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.

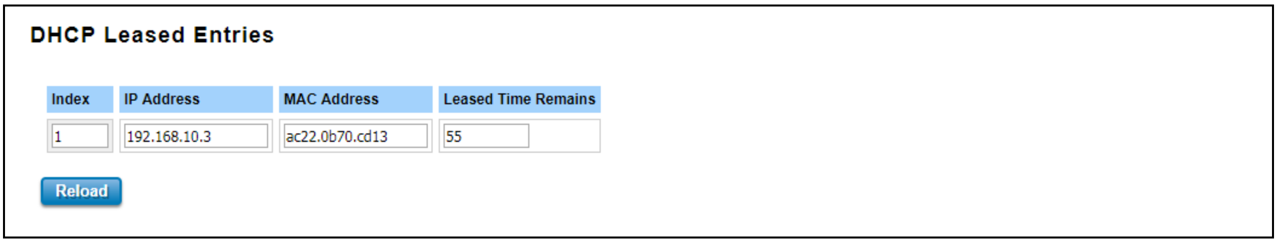
2. The MAC address of the relay agent.

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:

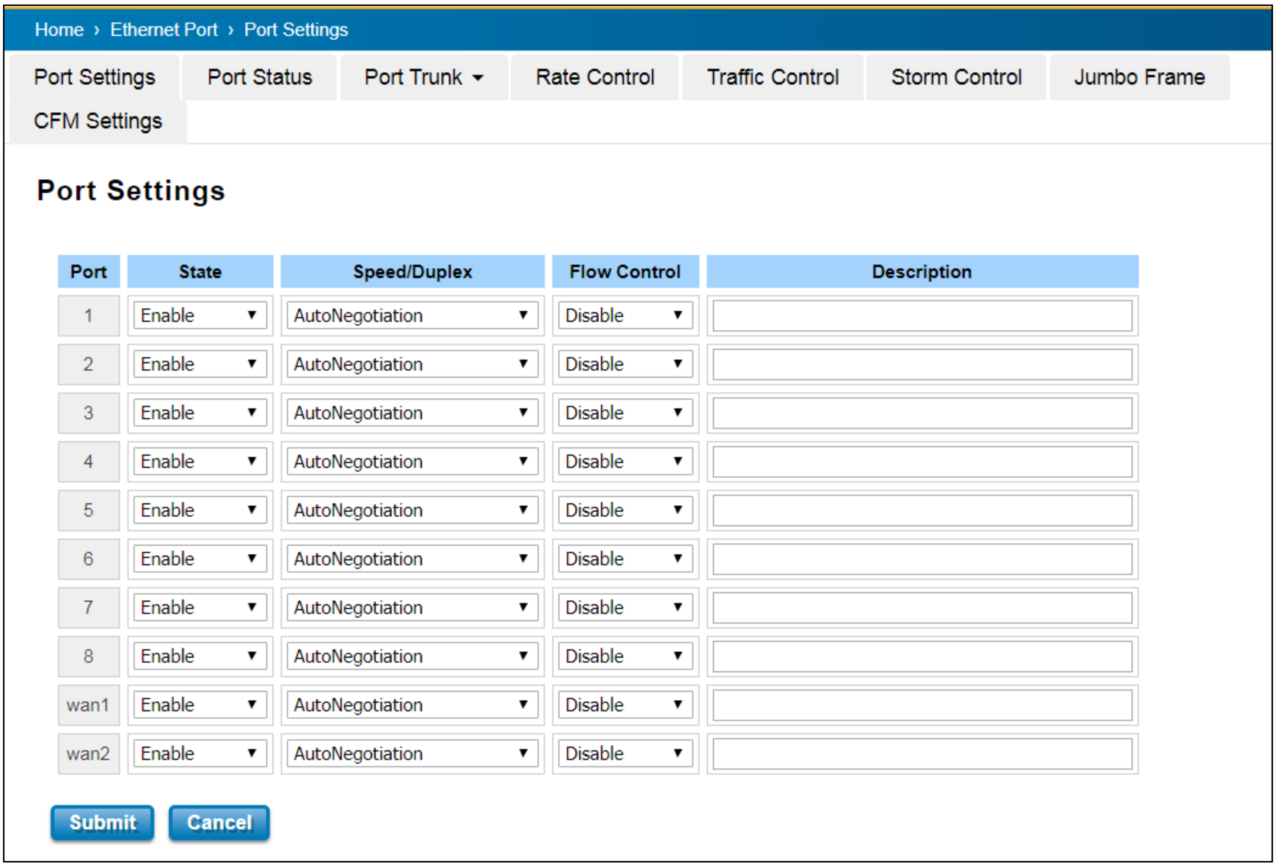
TERMS	DESCRIPTION
IP Address	IP address that was assigned by switch.
MAC Address	MAC address that was assigned by switch.
Leased Time Remains	Remains time for the IP address leased

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. In DRS610, since the first two ports are WAN ports, LAN port ID is not comfort to physical interface ID, check Ch2.1 Hardware Appearance and Dimension first.

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.



Port Settings

Port	State	Speed/Duplex	Flow Control	Description
1	Enable ▾	AutoNegotiation ▾	Disable ▾	
2	Enable ▾	AutoNegotiation ▾	Disable ▾	
3	Enable ▾	AutoNegotiation ▾	Disable ▾	
4	Enable ▾	AutoNegotiation ▾	Disable ▾	
5	Enable ▾	AutoNegotiation ▾	Disable ▾	
6	Enable ▾	AutoNegotiation ▾	Disable ▾	
7	Enable ▾	AutoNegotiation ▾	Disable ▾	
8	Enable ▾	AutoNegotiation ▾	Disable ▾	
wan1	Enable ▾	AutoNegotiation ▾	Disable ▾	
wan2	Enable ▾	AutoNegotiation ▾	Disable ▾	

The description of the columns is as below:

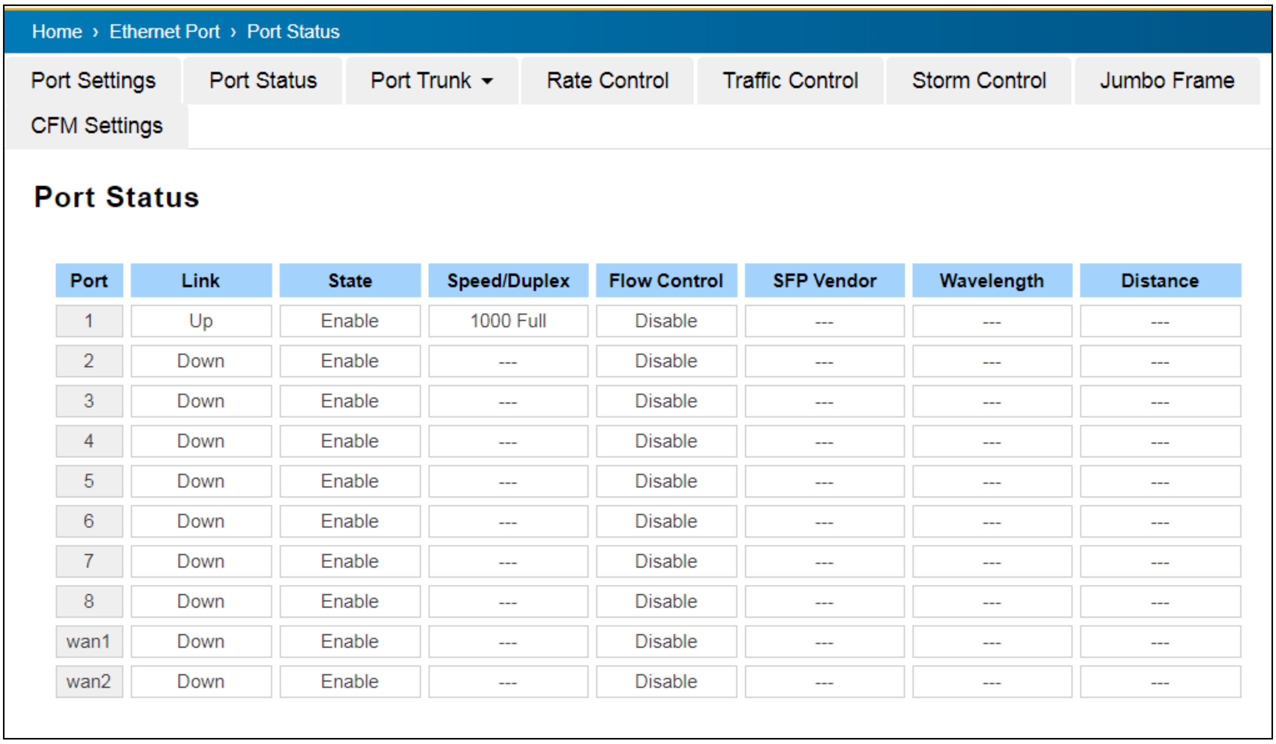
TERMS	DESCRIPTION
Port	Shows port number. Wan1 is physical port 1. Wan 2 is physical port 2. Port 1 to 8 means the LAN ports. 7/8 is fiber SFP socket.
State	**Default: Enable** Enable or disable a port
Speed/Duplex	**Default: AutoNegotiation** Users can set the bandwidth of each port as Auto-negotiation, 100 full,100 half,10 full,10 half mode for **Giga Ethernet Port 1~8 (ge1~ge8)**. For **Gigabit Ethernet Port 9~12: (ge9~ge12)**, it can be set up to 100M Full Duplex(100 Full) only.

Flow Control	**Default: Disable** **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.

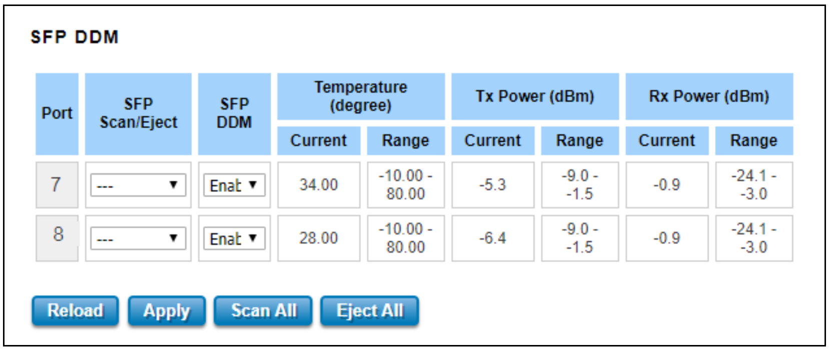


Port Status

Port	Link	State	Speed/Duplex	Flow Control	SFP Vendor	Wavelength	Distance
1	Up	Enable	1000 Full	Disable	---	---	---
2	Down	Enable	---	Disable	---	---	---
3	Down	Enable	---	Disable	---	---	---
4	Down	Enable	---	Disable	---	---	---
5	Down	Enable	---	Disable	---	---	---
6	Down	Enable	---	Disable	---	---	---
7	Down	Enable	---	Disable	---	---	---
8	Down	Enable	---	Disable	---	---	---
wan1	Down	Enable	---	Disable	---	---	---
wan2	Down	Enable	---	Disable	---	---	---

SFP DDM

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



SFP DDM

Port	SFP Scan/Eject	SFP DDM	Temperature (degree)		Tx Power (dBm)		Rx Power (dBm)	
			Current	Range	Current	Range	Current	Range
7	--- ▼	Enat ▼	34.00	-10.00 - 80.00	-5.3	-9.0 - -1.5	-0.9	-24.1 - -3.0
8	--- ▼	Enat ▼	28.00	-10.00 - 80.00	-6.4	-9.0 - -1.5	-0.9	-24.1 - -3.0

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

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

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

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

3.2.3 PORT TRUNK

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

Port Trunk Concept

Port trunking protocol that provides the following benefits:

- Flexibility in setting up User network connections, since the bandwidth of a link can be doubled, tripled, or quadrupled.
- Redundancy—if one link is broken, the remaining trunked ports share the traffic within this trunk group.
- Load sharing—MAC client traffic can be distributed across multiple links.

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

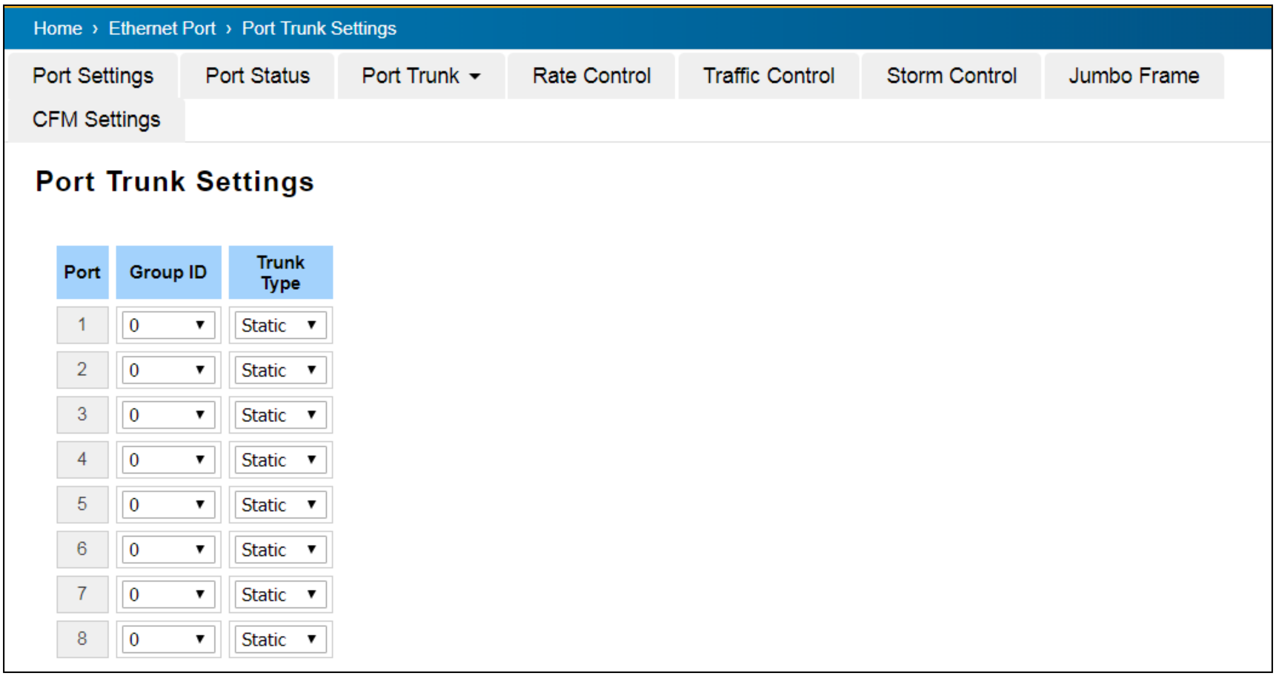
If all ports on both switch units are configured as 100BaseTX and they are operating in full duplex mode, this means that users can double, triple, or quadruple the bandwidth of the connection by port trunk between two switches.

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

- Communication redundancy will be reset.
- 802.1Q VLAN will be reset.
- Multicast Filtering will be reset.
- Port Lock will be reset and disabled.
- Set Device IP will be reset.
- Mirror will be reset.

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

Port Trunk Setting



Port Trunk Settings

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

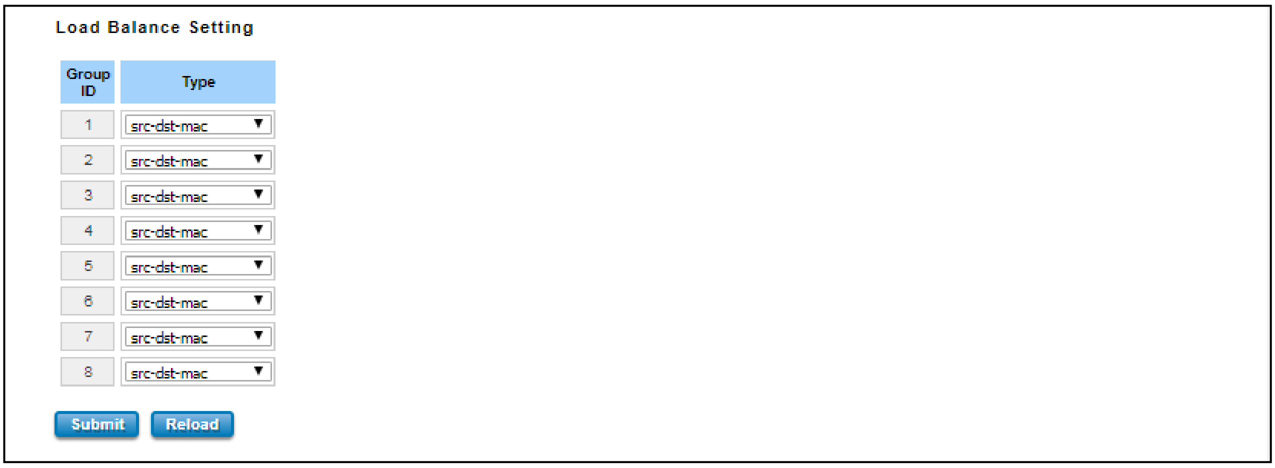
The switch can support up to 8 trunk groups with 2 trunk members. Since the member ports should use same speed/duplex, max trunk members would be 8 for 100Mbps, and 2 members for Gigabit.

The description of the columns is as below:

TERMS	DESCRIPTION
Group ID	**Default: 0** 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.

Load Balance Setting



Load Balance Setting

Group ID	Type
1	src-dst-mac
2	src-dst-mac
3	src-dst-mac
4	src-dst-mac
5	src-dst-mac
6	src-dst-mac
7	src-dst-mac
8	src-dst-mac

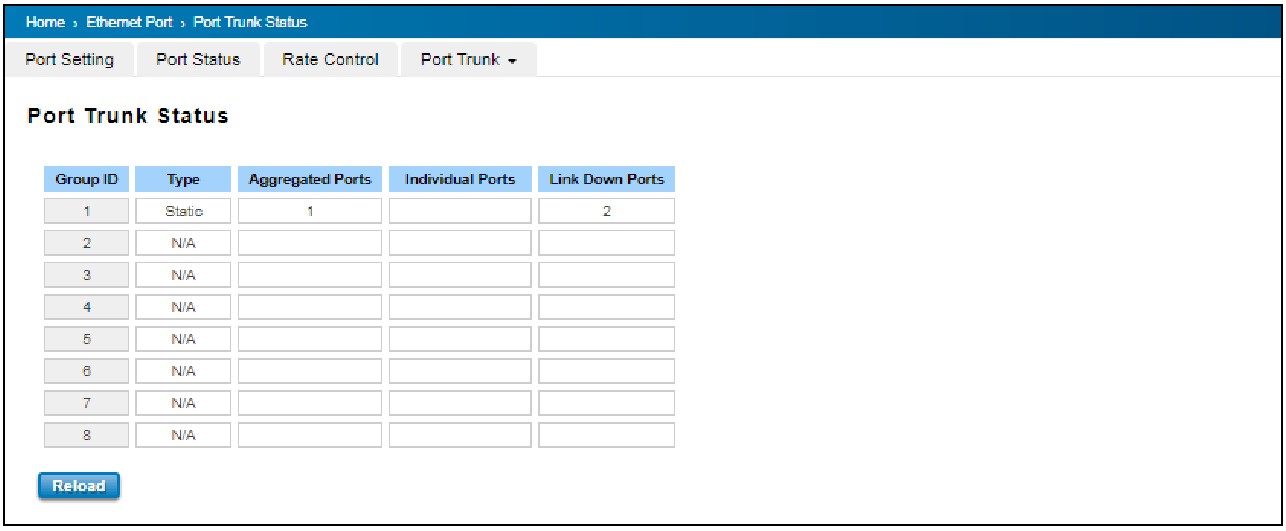
Load Balance Type: Each Trunk Group can support several Load Balance types that can be seen from the table below:

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

Click **Submit** to apply your settings.

Port Trunk Status

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



Port Trunk Status

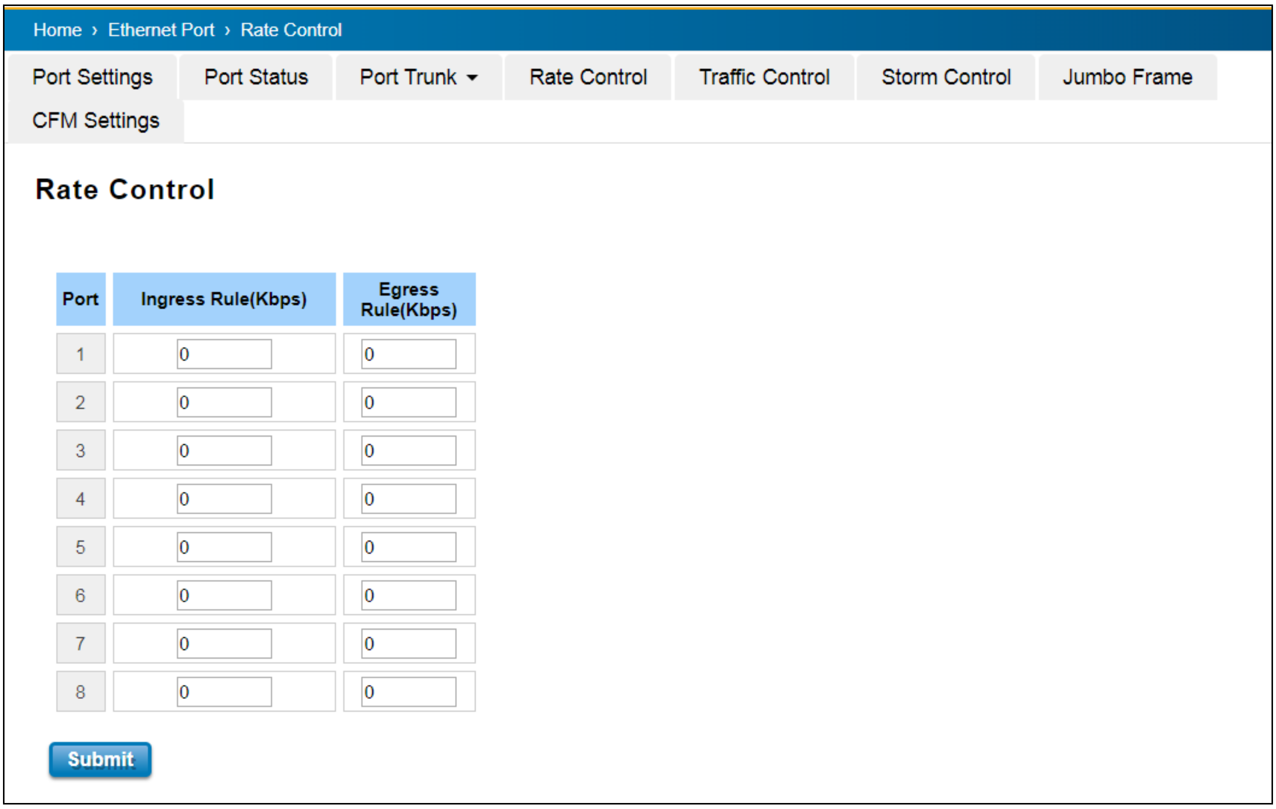
Group ID	Type	Aggregated Ports	Individual Ports	Link Down Ports
1	Static	1		2
2	N/A			
3	N/A			
4	N/A			
5	N/A			
6	N/A			
7	N/A			
8	N/A			

The description of the columns is as below:

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

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

3.2.4 RATE CONTROL



Port	Ingress Rule(Kbps)	Egress Rule(Kbps)
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0

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

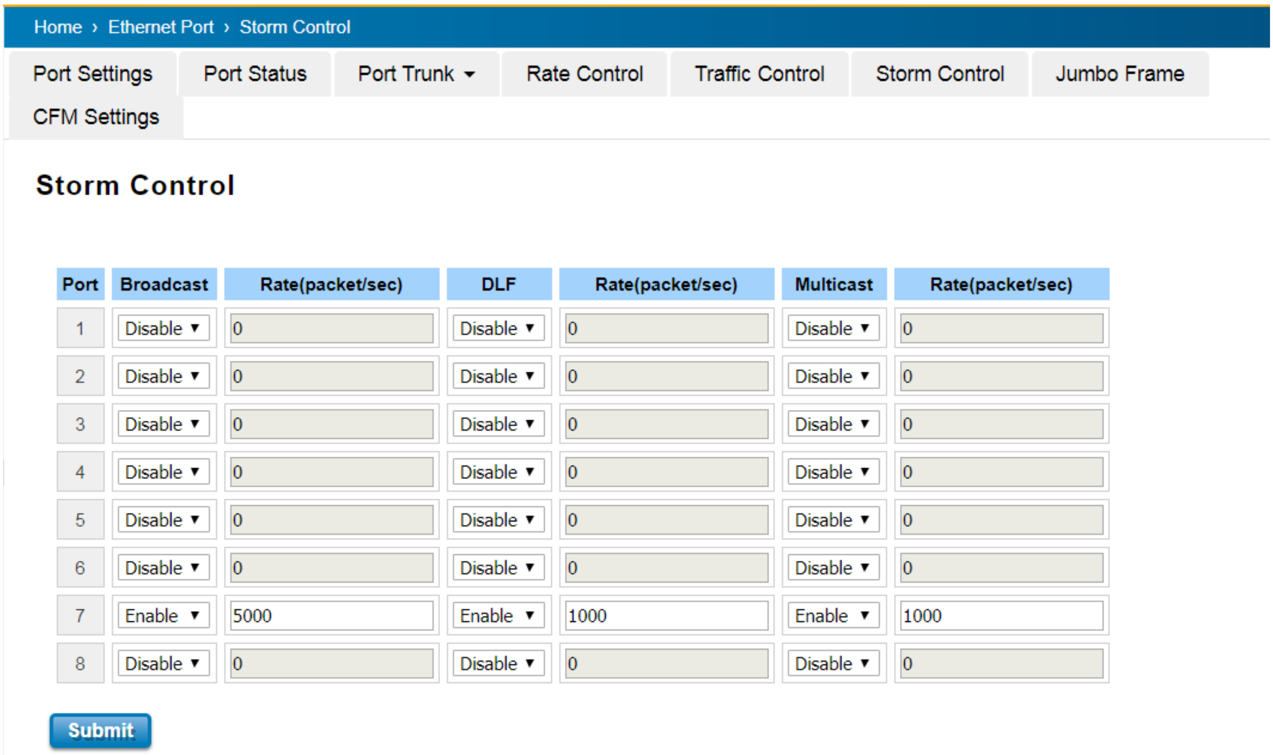
The description of the columns is as below:

TERMS	DESCRIPTION
Packet Type	Select the packet type that wanted to filter.
Ingress	The packet types of the Ingress Rule listed here include **Broadcast Only** / **Broadcast and multicast** / **Broadcast, Multicast and Unknown Unicast** or **All**.
Egress	The packet types of the Egress Rule (outgoing) only support **all** packet types.
Rate (Ingress & Egress)	**Default value Ingress: 8 Mbps** **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.

3.2.5 STORM CONTROL

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



Storm Control

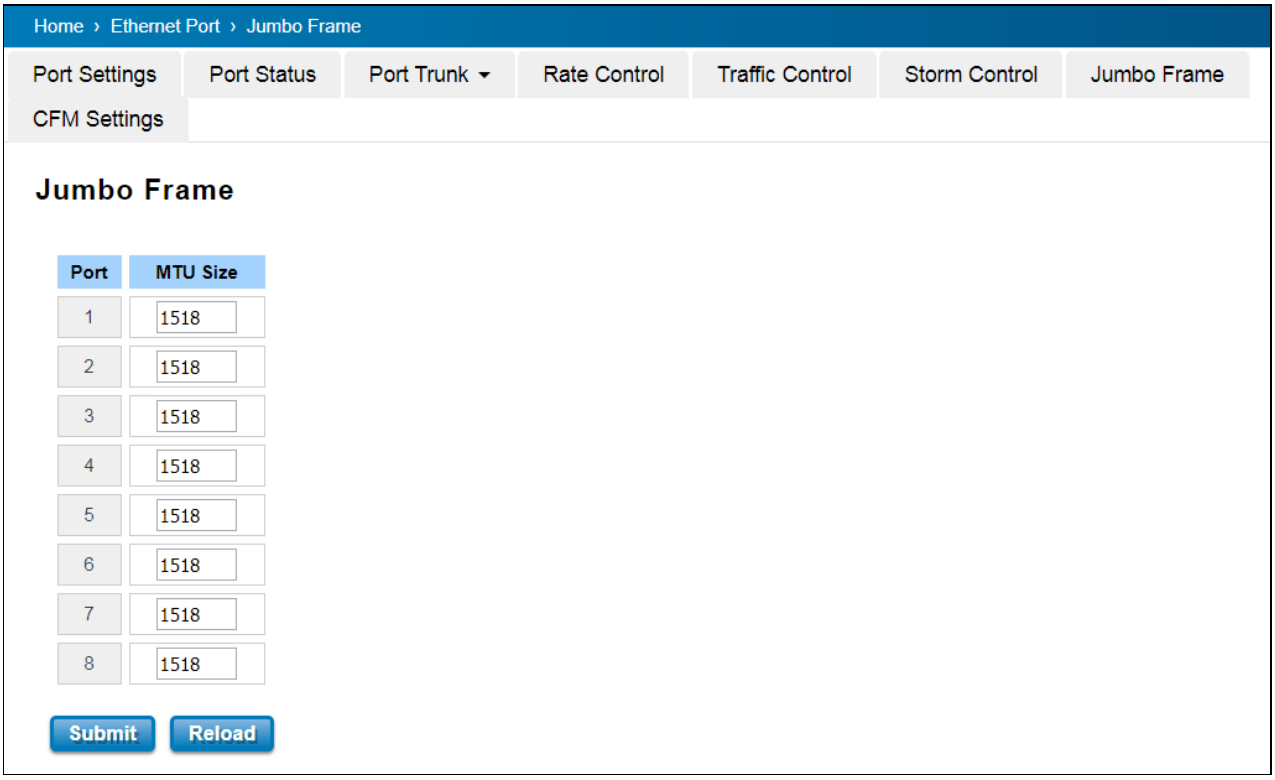
Port	Broadcast	Rate(packet/sec)	DLF	Rate(packet/sec)	Multicast	Rate(packet/sec)
1	Disable ▾	0	Disable ▾	0	Disable ▾	0
2	Disable ▾	0	Disable ▾	0	Disable ▾	0
3	Disable ▾	0	Disable ▾	0	Disable ▾	0
4	Disable ▾	0	Disable ▾	0	Disable ▾	0
5	Disable ▾	0	Disable ▾	0	Disable ▾	0
6	Disable ▾	0	Disable ▾	0	Disable ▾	0
7	Enable ▾	5000	Enable ▾	1000	Enable ▾	1000
8	Disable ▾	0	Disable ▾	0	Disable ▾	0

Click Submit to apply the configuration.

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

3.2.6 JUMBO FRAME

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



Jumbo Frame

Port	MTU Size
1	1518
2	1518
3	1518
4	1518
5	1518
6	1518
7	1518
8	1518

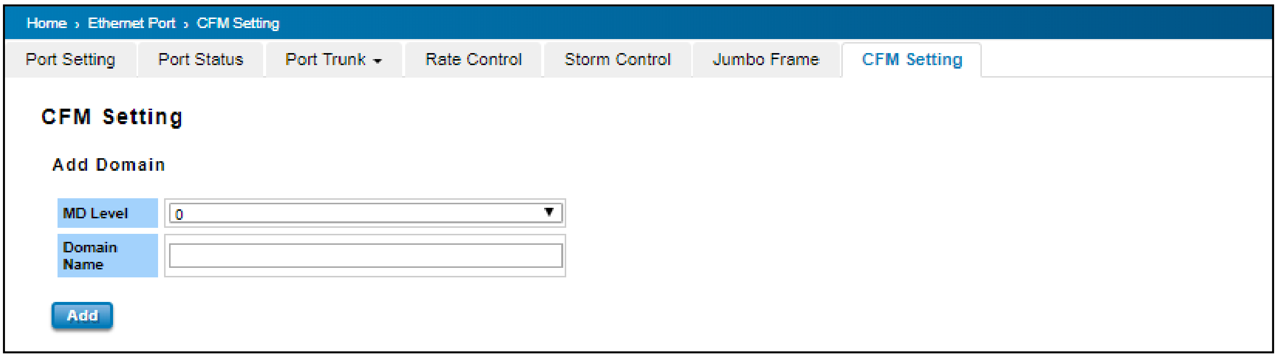
3.2.7 CFM SETTING

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

Continuity Check Protocol (CCP): "Heartbeating" messages for CFM. The Continuity Check Message (CCM) provides a means to detect connectivity failures in an MA. CCMs are multicast messages. CCMs are confined to a domain (MD). These messages are unidirectional and do not solicit a response. Each MEP transmits a periodic multicast Continuity Check Message inward towards the other MEPs. DP612/DS612 support Hardware CCM transition. The transition/receiving interval can up to 3.3ms to support detection Gigabit Ethernet cooper interface in 10ms.

Below is the CFM CCP configuration page. In this page user may configure the Maintenance Domain, Maintenance Association and the Maintenance association End Point setting.

Add Domain



CFM Setting

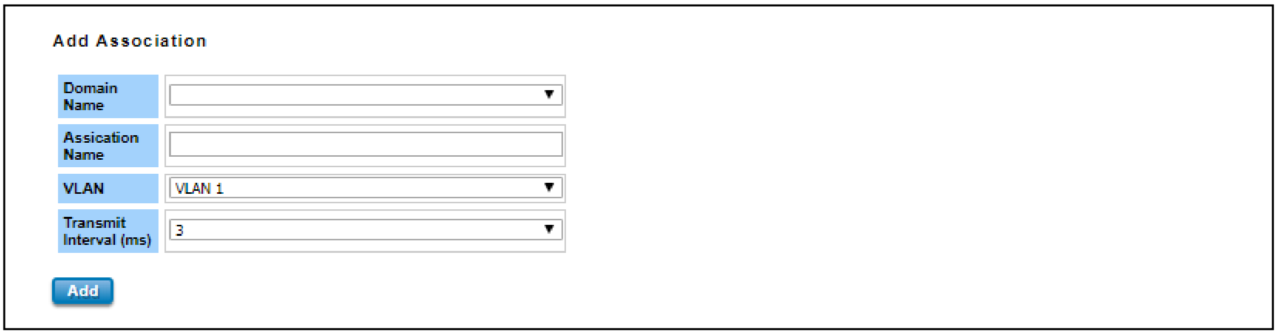
Add Domain

MD Level	0 ▼
Domain Name	

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

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

Add Association



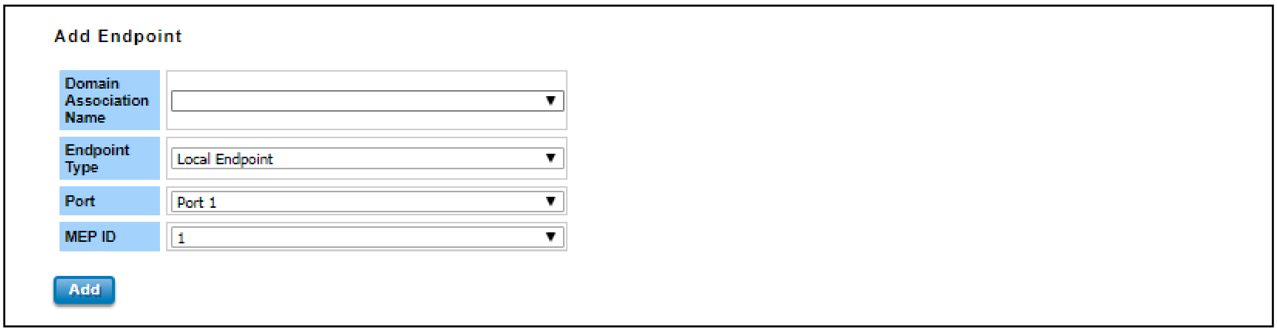
Add Association

Domain Name	▼
Assication Name	
VLAN	VLAN 1 ▼
Transmit Interval (ms)	3 ▼

Choose the Domain Name from the list that has been added up then add a new Association Name for the Maintenance Association. After that choose the VLAN, Please create VLAN first, and each port set to be “tagged” Add the Domain association name, end point type, port number and and the MEP ID then click **Add.**

TERMS	DESCRIPTION
Domain Name	Choose the Domain Name that has been added
Association Name	Enter the Association Name. Association name, maximum of 45 characters
VLAN	Choose VLAN that has been assigned
Domain Name	Enter a new Domain Name. Domain name, maximum of 43 characters

Add Endpoint


Add Endpoint

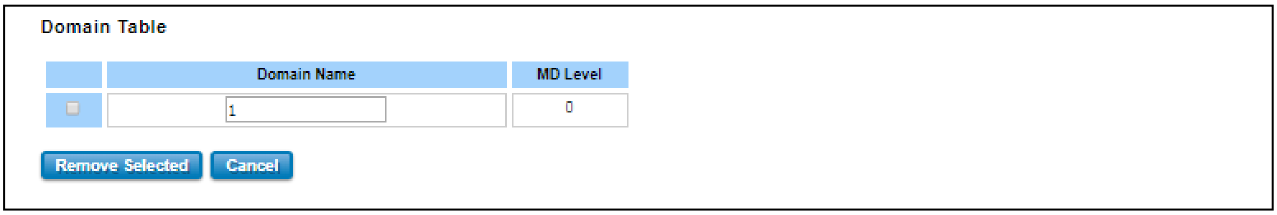
Domain Association Name	
Endpoint Type	Local Endpoint
Port	Port 1
MEP ID	1

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

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

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

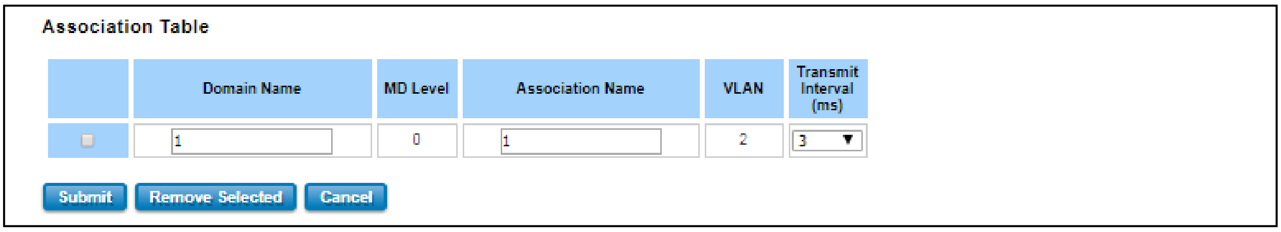
Domain Table


Domain Table

	Domain Name	MD Level
□	1	0

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

Association Table



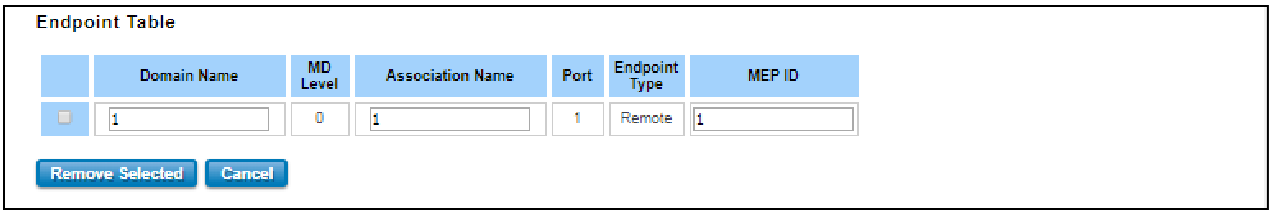
Association Table

	Domain Name	MD Level	Association Name	VLAN	Transmit Interval (ms)
□	1	0	1	2	3 ▼

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

Endpoint Table

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



Endpoint Table

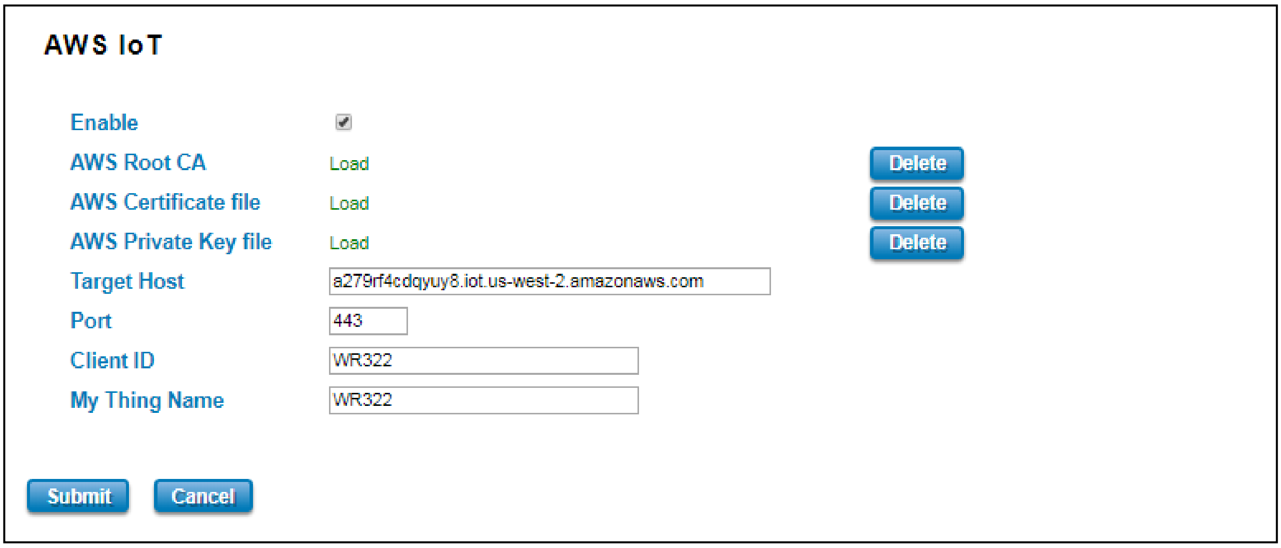
	Domain Name	MD Level	Association Name	Port	Endpoint Type	MEP ID
□	1	0	1	1	Remote	1

3.3 IoT

Over the past decade or so, the word “cloud” has taken on a new meaning to many people. Rather than a visible mass of condensed water vapor floating in the sky, the cloud has taken to the IoT industry in the form of data. WoMaster Industrial Router is supported with private clouds, ThingsMaster and public clouds, AWS and Microsoft Azure. Clouds offer great promise in improving the agility and flexibility of IT to respond to the requirements of the business cost effectively. The security challenges raised by the loss of control and visibility in the journey to the cloud can be addressed in terms of securing infrastructure, information, identities, and devices.

3.3.1 AWS IoT

Amazon Web Services IoT enables secure, bi-directional communication between Internet-connected things (such as sensors, actuators, embedded devices, or smart appliances) and the AWS cloud over MQTT and HTTP. For more information please visit: http://aws.amazon.com/iot/.



AWS IoT

Enable	☑	
AWS Root CA	Load	Delete
AWS Certificate file	Load	Delete
AWS Private Key file	Load	Delete
Target Host	a279rf4cdqyuy8.iot.us-west-2.amazonaws.com	
Port	443	
Client ID	WR322	
My Thing Name	WR322	

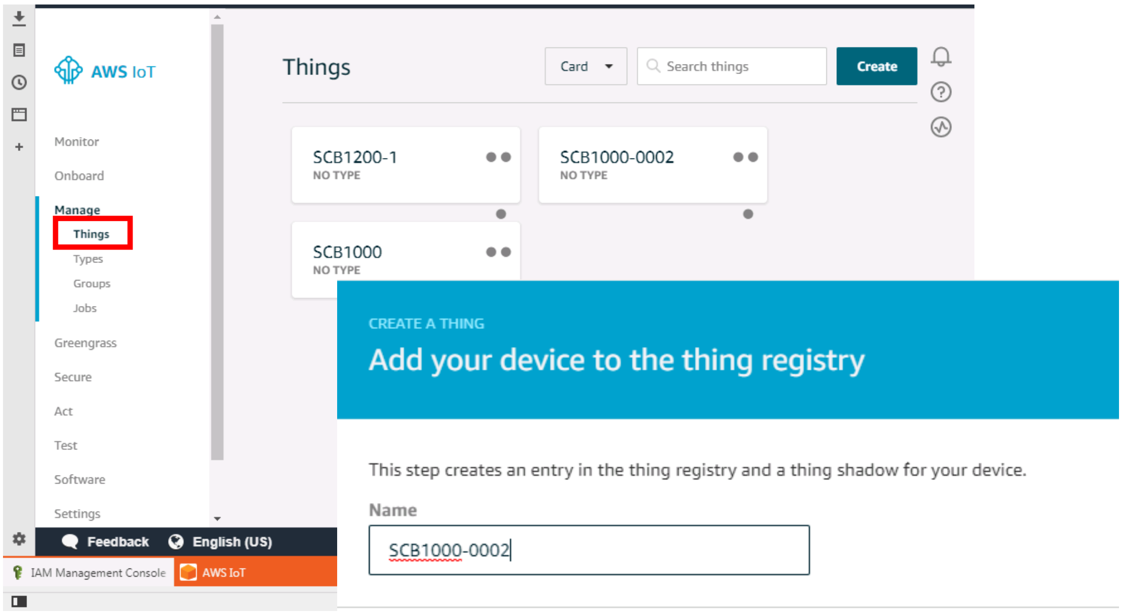
The description of the columns is as below:

TERMS	DESCRIPTION
Enable	Enable the AWS IoT function
AWS Root CA	Root CA is necessary. User can download it from the AWS.
AWS Certificate file	Certificate is necessary. User can download it from the AWS.
AWS Private Key file	Private key is necessary. User can download it from the AWS.
Target Host	Enter the target host
Port	**Default: 433** Because AWS uses the HTTPS traffic, user need to add an inbound rule on port 443
Client ID	Enter the device client ID
My Thing Name	Enter the registered device name (Need to be the same)

Click **Submit** to apply the configuration.

HOW TO CONNECT THE DEVICE TO AWS

- Create and login to AWS account.
- Select AWS IoT Services – click Thing.
- Add your device shadow.



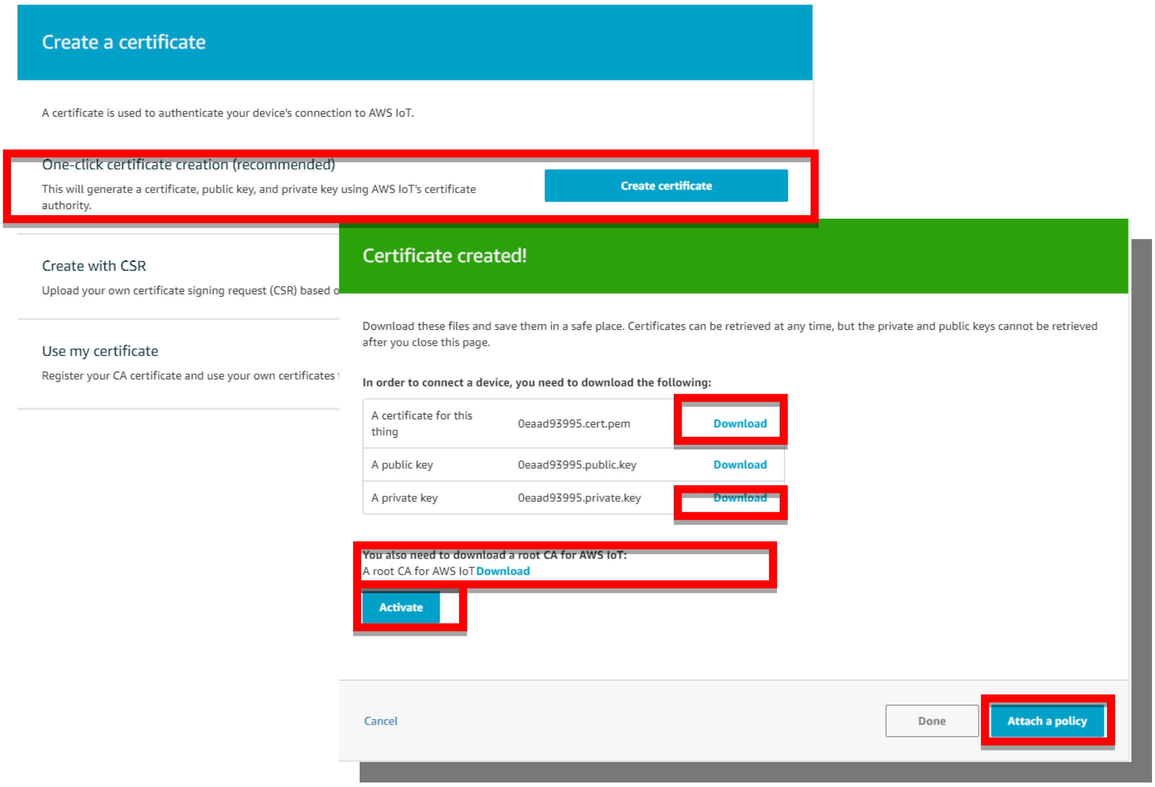
CREATE A THING

Add your device to the thing registry

This step creates an entry in the thing registry and a thing shadow for your device.

Name: SCB1000-0002

- Create and download the key or certificate.



Create a certificate

A certificate is used to authenticate your device's connection to AWS IoT.

One-click certificate creation (recommended)

This will generate a certificate, public key, and private key using AWS IoT's certificate authority.

Create with CSR

Upload your own certificate signing request (CSR) based o

Use my certificate

Register your CA certificate and use your own certificates

Certificate created!

Download these files and save them in a safe place. Certificates can be retrieved at any time, but the private and public keys cannot be retrieved after you close this page.

In order to connect a device, you need to download the following:

A certificate for this thing	0eaad93995.cert.pem	Download
A public key	0eaad93995.public.key	Download
A private key	0eaad93995.private.key	Download

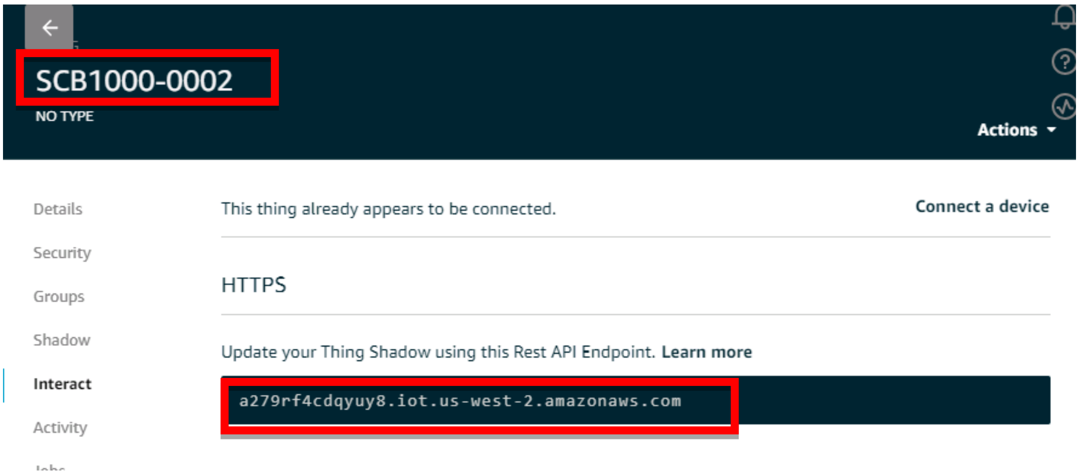
You also need to download a root CA for AWS IoT:
A root CA for AWS IoT Download

Certificate, private key, root CA is necessary. Public key is used by AWS server to authenticate with private key. The public key and private cannot be downloaded back after the user closes the page. Policy can be added later.

- Get the Target host to connect with the device.

  Go to Manage -> Things -> click the device name -> Click Interact.

  Copy the HTTPS link to update user's Thing Shadow using this Rest API Endpoint.



SCB1000-0002

NO TYPE

This thing already appears to be connected.

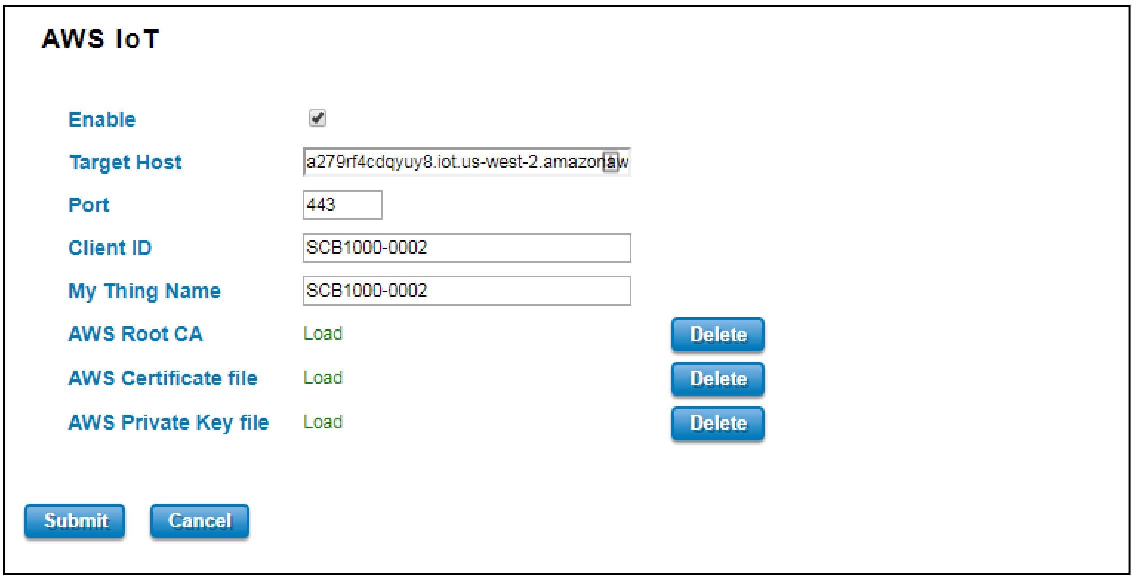
HTTPS

Update your Thing Shadow using this Rest API Endpoint. Learn more

```
a279rf4cdqyuy8.iot.us-west-2.amazonaws.com
```

- Connect the device to AWS.

  Copy the link and paste on the Target Host field at the AWS IoT page.



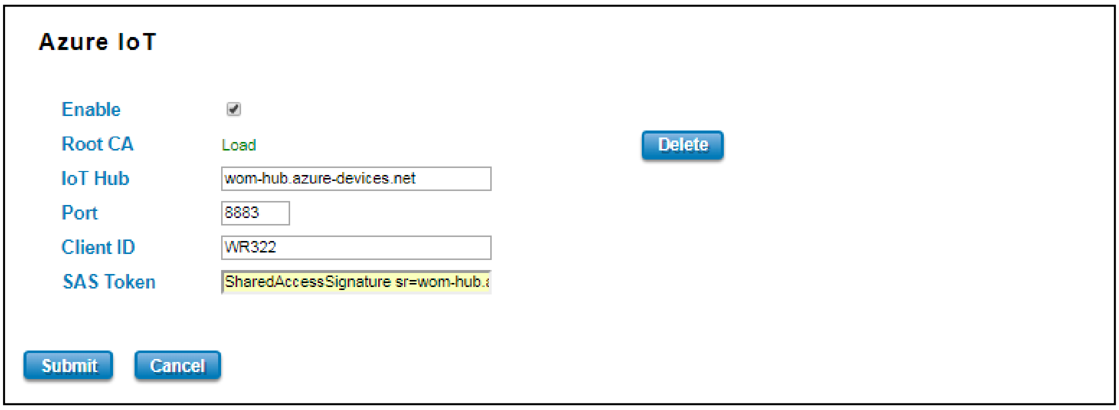
AWS IoT

Enable	☑	
Target Host	a279rf4cdqyuy8.iot.us-west-2.amazonaw	
Port	443	
Client ID	SCB1000-0002	
My Thing Name	SCB1000-0002	
AWS Root CA	Load	Delete
AWS Certificate file	Load	Delete
AWS Private Key file	Load	Delete

3.3.2 AZURE IoT

Azure IoT Hub is a fully managed service that enables reliable and secure bi-directional communications between millions of Internet of Things (IoT) devices and a solution back end. One of the biggest challenges that IoT projects face is how to reliably and securely connect devices to the solution back end. To address this challenge, IoT Hub:

- Offers reliable device-to-cloud and cloud-to-device hyper-scale messaging.
- Enables secure communications using per-device security credentials and access control.
- Includes the most popular communication protocols.



Azure IoT

Enable	☑
Root CA	Load
IoT Hub	wom-hub.azure-devices.net
Port	8883
Client ID	WR322
SAS Token	SharedAccessSignature sr=wom-hub.a

The description of the columns is as below:

TERMS	DESCRIPTION
Enable	Enable Azure IoT function
Root CA	Download and enter the root CA.
IoT Hub	Enter the IoT hub server, this information can be found at the azure platform
Port	**Default: 8883** Display the port number. Because Azure IoT uses the MQTT protocol, so user needs to enter 8883 port number that belongs to MQTT protocol.
Client ID	Enter the client ID
SAS Token	Enter the SAS Token that needs to be generated by software. (Azure Device Explorer)

Click **Submit** to apply the configuration.

HOW TO CONNECT THE DEVICE TO MICROSOFT AZURE

CREATE IOT HUB

To register the device in Azure Portal, user has to follow the guide "Get started with Azure IoT Hub for Java": https://azure.microsoft.com/en-us/documentation/articles/iot-hub-java-java-getstarted/.

The guide explains how to create an IoT Hub and a device entity. It is important to annotate the connection string generated after creating the device entity. User will need this parameter later for the device configuration (WoM IoT Configuration).

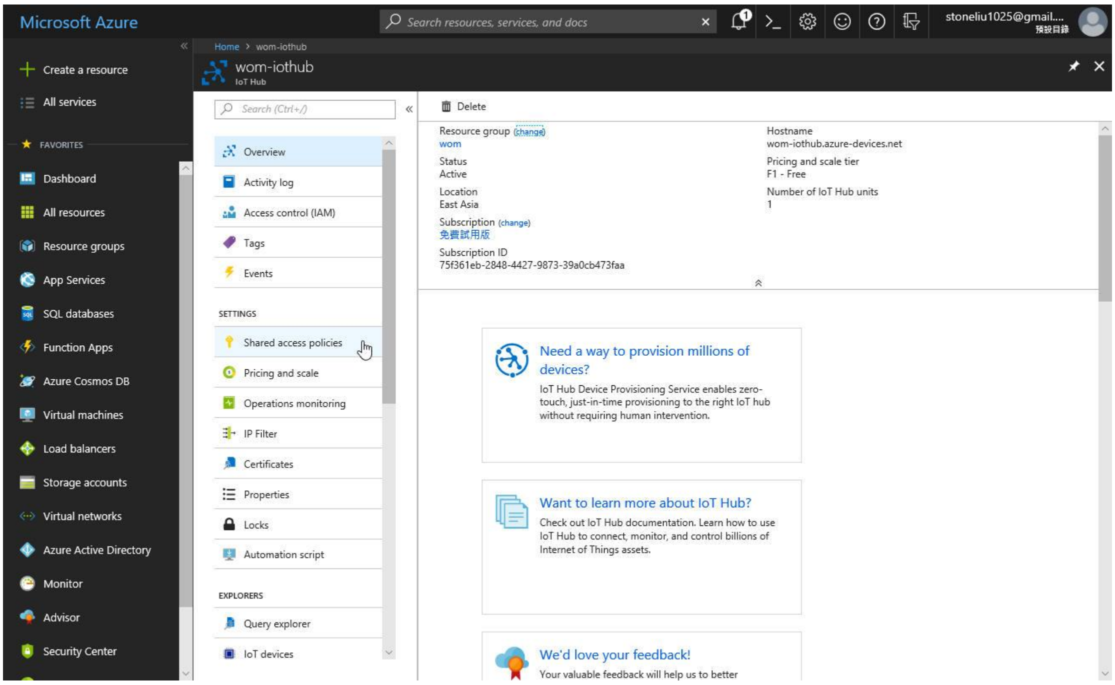
CONFIGURE THE DEVICE AS A MQTT CLIENT

In the Microsoft Azure Portal, go to IoT Hub menu and select:

Devices > myCreatedDevice > Shared access policies > iothubowner > Connection string - primary key.

User has to annotate the value of this field.

1. Get the connection string. Click the IoT Hub -> Shared access policies.



Resource group (change)
wom

Status
Active

Location
East Asia

Subscription (change)
免費試用版

Subscription ID
75f361eb-2848-4427-9873-39a0cb473faa

Hostname
wom-iothub.azure-devices.net

Pricing and scale tier
F1 - Free

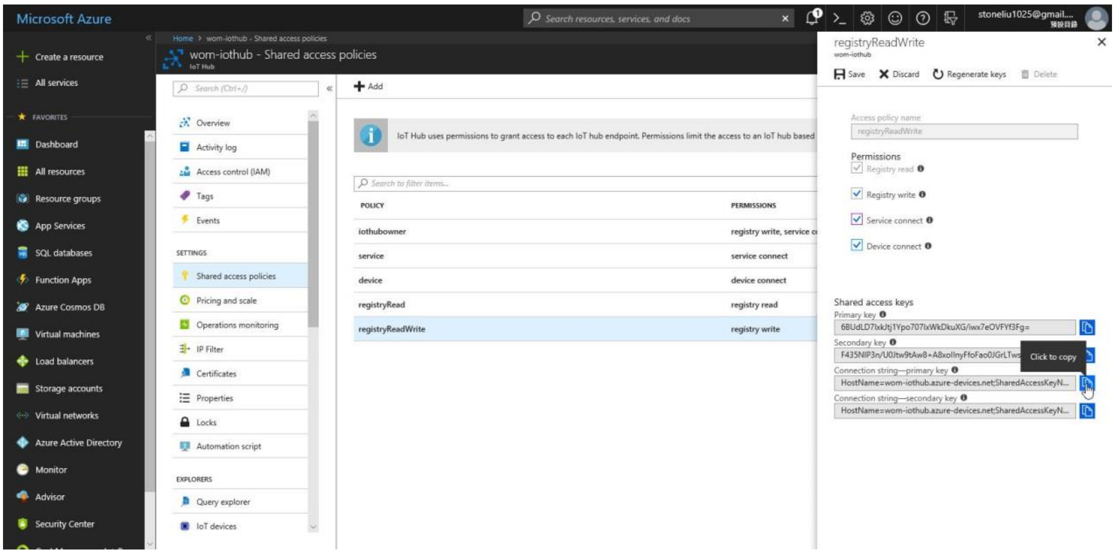
Number of IoT Hub units
1

Need a way to provision millions of devices?
IoT Hub Device Provisioning Service enables zero-touch, just-in-time provisioning to the right IoT hub without requiring human intervention.

Want to learn more about IoT Hub?
Check out IoT Hub documentation. Learn how to use IoT Hub to connect, monitor, and control billions of Internet of Things assets.

We'd love your feedback!
Your valuable feedback will help us to better

2. Click registryReadWrite -> copy the Connection string---Primary Key.



IoT Hub uses permissions to grant access to each IoT hub endpoint. Permissions limit the access to an IoT hub based

POLICY	PERMISSIONS
iothubowner	registry write, service c
service	service connect
device	device connect
registryRead	registry read
registryReadWrite	registry write

Access policy name
registryReadWrite

Permissions
☑ Registry read
☑ Registry write
☑ Service connect
☑ Device connect

Shared access keys

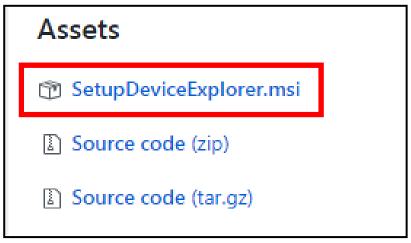
Primary key
6BUdLD7lxkJtj1Ypo707lxWkDkuXG/iwx7eOVFYf3Fg=

Secondary key
F435NIP3n/U0Jtw9tAw8+A8xollnyFfoFao0JGrLTws

Connection string—primary key
HostName=wom-iothub.azure-devices.net;SharedAccessKeyN...

Connection string—secondary key
HostName=wom-iothub.azure-devices.net;SharedAccessKeyN...

3. Download and install the Azure Device Explorer to generate the SAS Token. Go to this link to download the software: https://github.com/Azure/azure-iot-sdk-csharp/releases/download/2018-3-13/SetupDeviceExplorer.msi



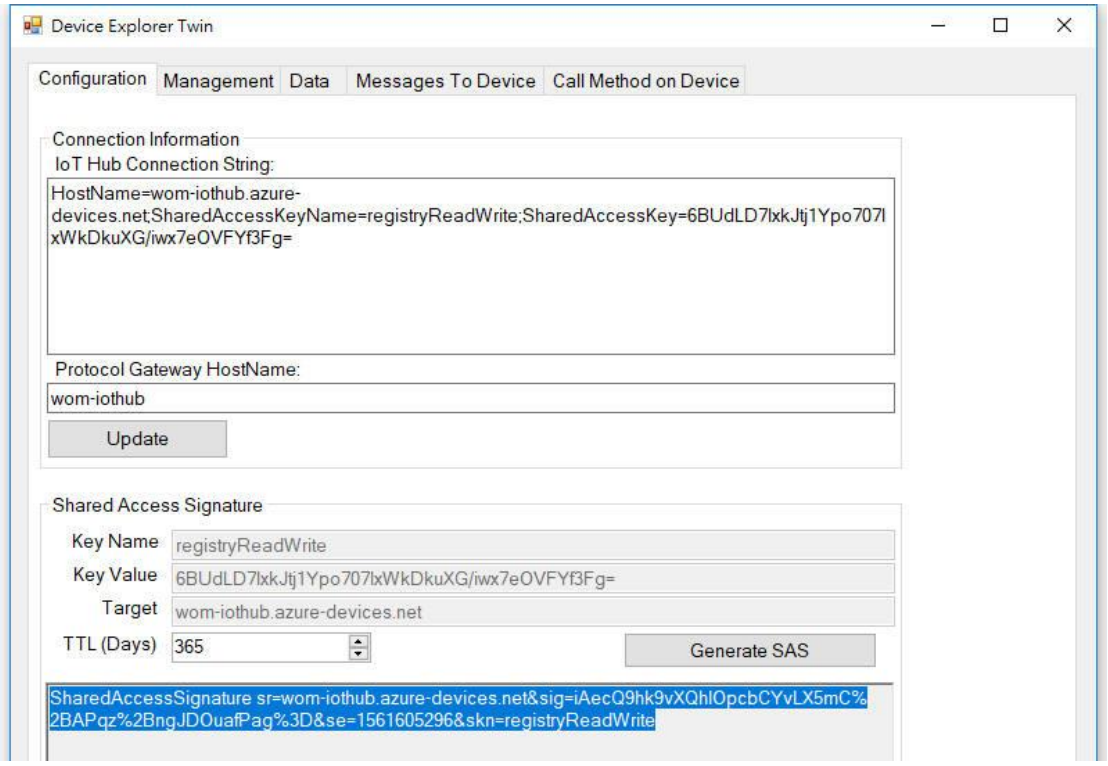
Assets

SetupDeviceExplorer.msi

Source code (zip)

Source code (tar.gz)

4. Paste the Connection String --- Primary Key to the IoT Hub Connection String box. Then type the Protocol Gateway HostName and click Update. In the end, generate the SAS Token.



Connection Information

IoT Hub Connection String:

```
HostName=wom-iothub.azure-
devices.net;SharedAccessKeyName=registryReadWrite;SharedAccessKey=6BUdLD7lxkJtj1Ypo707l
xWkDkuXG/iwx7eOVFYf3Fg=
```

Protocol Gateway HostName: wom-iothub

Shared Access Signature

Key Name: registryReadWrite

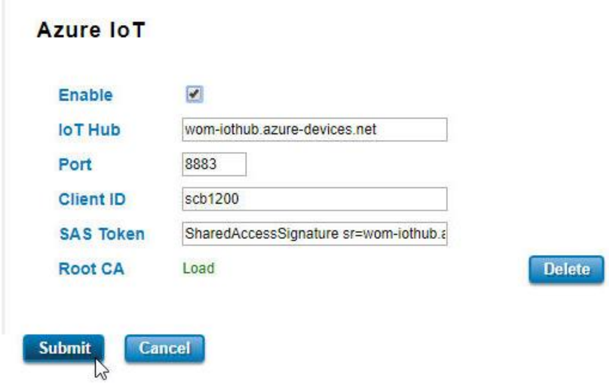
Key Value: 6BUdLD7lxkJtj1Ypo707lxWkDkuXG/iwx7eOVFYf3Fg=

Target: wom-iothub.azure-devices.net

TTL (Days): 365

```
SharedAccessSignature sr=wom-iothub.azure-devices.net&sig=iAecQ9hk9vXQhlOpcbCYvLX5mC%
2BAPqz%2BngJDOuafPag%3D&se=1561605296&skn=registryReadWrite
```

5. Configure the MQTT Client from the Web GUI. Enter the value based on the IoT Hub setting. And the device is connected to the cloud.



Azure IoT

Enable ☑

IoT Hub: wom-iothub.azure-devices.net

Port: 8883

Client ID: scb1200

SAS Token: SharedAccessSignature sr=wom-iothub.a

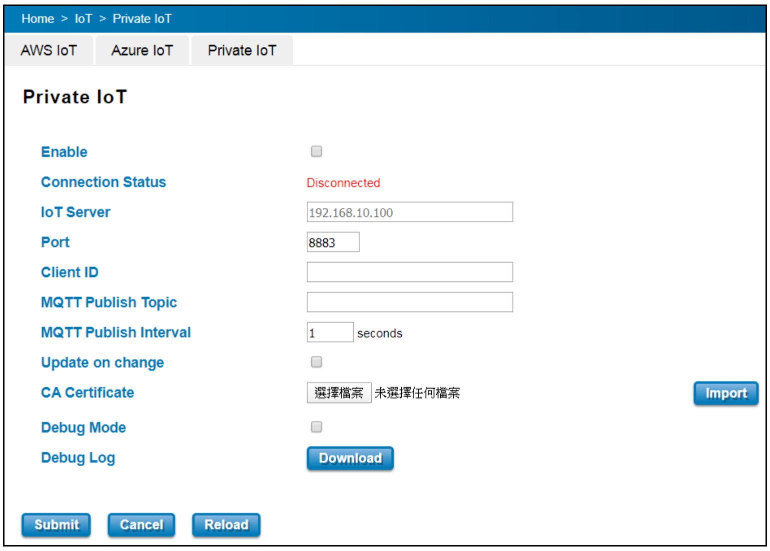
Root CA: Load

Please find the Root CA through this link: https://github.com/Azure/azure-iot-sdk-c/blob/master/certs/certs.c

3.3.3 PRIVATE IoT

WoMaster provides its private cloud service, ThingsMaster that could support the Industrial Plants Network. Under the cloud architecture, software, hardware, applications, and storage can all be provided as services. The cloud network service has the advantages of easy expansion, rapid adjustment, and minimal management, and can dynamically meet increasing demands. Users can access the data which stored on the cloud anywhere, anytime, and seamlessly share to any authorized users.

If you already have your own Private Cloud Management System with supporting MQTT communication protocol, you can connect our Router to your system, you can configure the setting in this page. Since different cloud management software provider may have different connectivity design, once you find interoperability problem on connecting, contact with our sales/technical window for further discuss and diagnostic.



Private IoT

Enable □

Connection Status: Disconnected

IoT Server: 192.168.10.100

Port: 8883

Client ID:

MQTT Publish Topic:

MQTT Publish Interval: 1 seconds

Update on change □

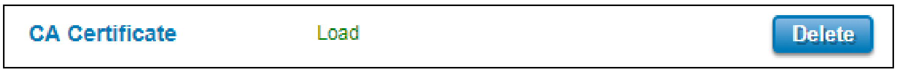
CA Certificate: 選擇檔案 未選擇任何檔案

Debug Mode □

Debug Log

The description of the columns is as below:

TERMS	DESCRIPTION
Enable	Enable the Private IoT function

Connection Status	Here shows the Connection Status, Disconnected in default and Connected while successfully connected to our private cloud Server.
IoT Server	Enter the specific IP of IoT Server.
Port	The specific TCP/IP port number, default is 8883 for MQTT
Client ID	Enter the client ID that has been registered.
MQTT Publish Topic	Specify the MQTT Topic
MQTT Publish Interval	The interval time of MQTT publish, default is 1 sec.
Update on Change	The system only updates info while the status is changed.
CA Certificate	The function from this certificate file is to create an encrypted MQTT communication. User can apply the file from the administrator, or get this file when download the ThingsMaster server file. After uploaded, the UI shows **“Load”**  CA Certificate Load
Debug Mode	After you confirmed all the setting, but, you still have problem on connecting to private IoT server. Enable the Debug mode here then you can download the debug log.
Debug Log	Click “Download” to download the debug log and send to our technical person for further diagnostic.

Click **Submit** to apply the configuration.

HOW TO ESTABLISH AND CONNECT TO THE THINGSMASTER CLOUD SERVER

Note: The UI of the ThingMaster, ThingMaster OTA RMS and VMWare software and download link is often updated, following steps and figures may be updated.

1. Download and install VMware Workstation Player.

Please Download the software in VMWave web site or Search VMWare Workstation Player by Search engine, ex: Google. Download and install the VMWare Workstation, then you can have two operating system in one computer and quick start install the WoMaster ThingMaster trail version.

2. Download the server file from the link that sent by the Sales. Contact the WoMaster Sales/Tech window and apply the link of ThingMaster Trail version.

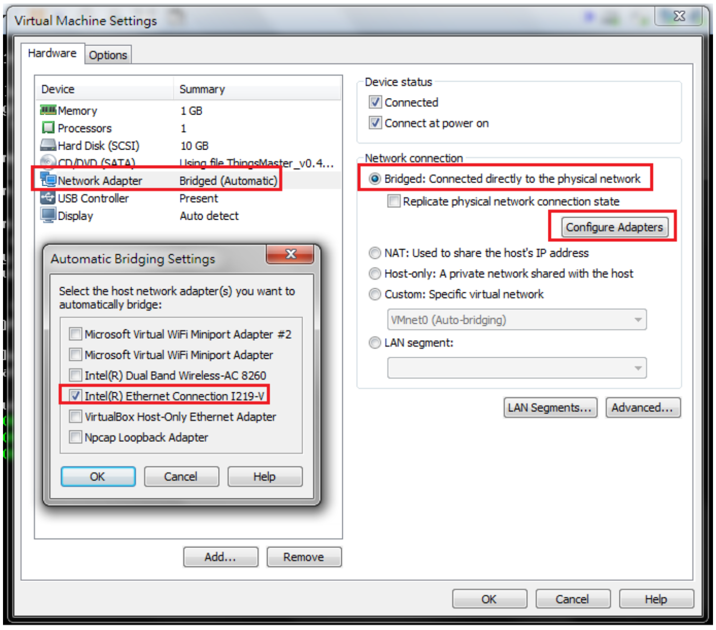
3. Open a Virtual Machine from disk and import.

Note: Ignore the warning message, check “Do not show this message again” then click Retry.

4. Configure network adapter of ThingsMaster VM to make sure that the laptop or the computer can ping the Virtual Machine.

- Go to Player -> Managed -> Virtual Machine Settings
- Choose the Network Adapter
- Set the Network Connection to Bridged
- Click Configure Adapters
- Select the Network Card that user used, user may choose either Wireless or Ethernet connection.

Note: User should only enable the NIC which under the same network with the device.



Virtual Machine Settings

Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SCSI)	10 GB
CD/DVD (SATA)	Using file ThingsMaster_v0.4...
Network Adapter	Bridged (Automatic)
USB Controller	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

● Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

○ Custom: Specific virtual network

VMnet0 (Auto-bridging)

○ LAN segment:

Automatic Bridging Settings

Select the host network adapter(s) you want to automatically bridge:

□ Microsoft Virtual WiFi Miniport Adapter #2

□ Microsoft Virtual WiFi Miniport Adapter

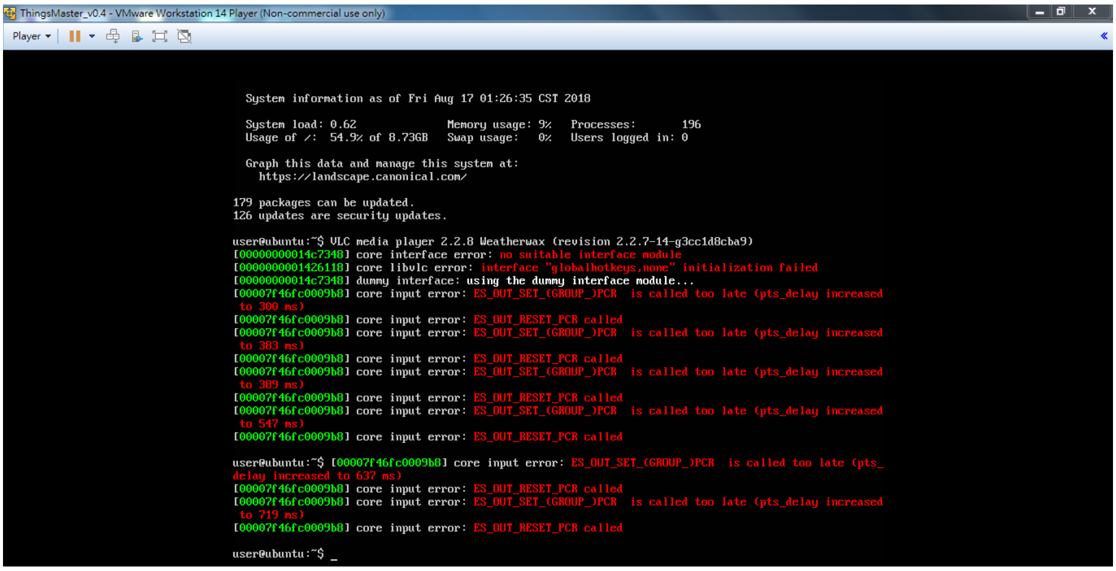
□ Intel(R) Dual Band Wireless-AC 8260

☑ Intel(R) Ethernet Connection I219-V

□ VirtualBox Host-Only Ethernet Adapter

□ Npcap Loopback Adapter

5. Start the Virtual Machine, wait till the starting process is done then the ThingsMaster is established.

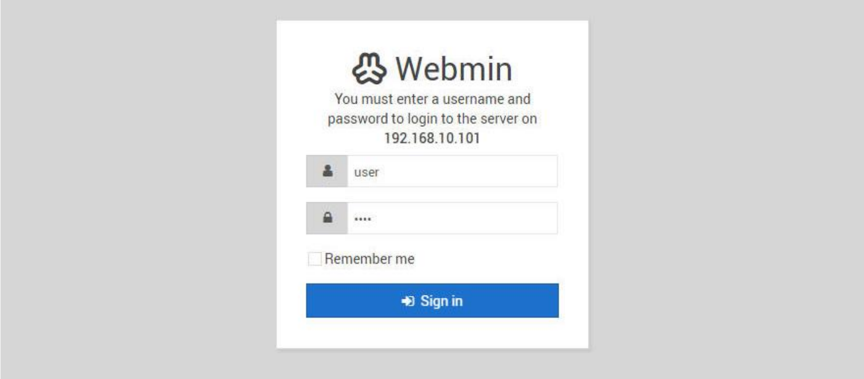

ThingsMaster_v0.4 - VMware Workstation 14 Player (Non-commercial use only)
Player ▾

```
   System information as of Fri Aug 17 01:26:35 CST 2018

   System load: 0.62               Memory usage: 9%   Processes:       196
   Usage of /:  54.9% of 8.73GB    Swap usage:   0%   Users logged in: 0

   Graph this data and manage this system at:
     https://landscape.canonical.com/

 179 packages can be updated.
 126 updates are security updates.

 user@ubuntu:~$ VLC media player 2.2.8 Weatherwax (revision 2.2.7-14-g3cc1d8cba9)
 [00000000014c7348] core interface error: no suitable interface module
 [0000000001426118] core libvlc error: interface "globalhotkeys,none" initialization failed
 [00000000014c7348] dummy interface: using the dummy interface module...
 [00007f46fc0009b8] core input error: ES_OUT_SET_(GROUP_)PCR  is called too late (pts_delay increased
  to 300 ms)
 [00007f46fc0009b8] core input error: ES_OUT_RESET_PCR called
 [00007f46fc0009b8] core input error: ES_OUT_SET_(GROUP_)PCR  is called too late (pts_delay increased
  to 383 ms)
 [00007f46fc0009b8] core input error: ES_OUT_RESET_PCR called
 [00007f46fc0009b8] core input error: ES_OUT_SET_(GROUP_)PCR  is called too late (pts_delay increased
  to 389 ms)
 [00007f46fc0009b8] core input error: ES_OUT_RESET_PCR called
 [00007f46fc0009b8] core input error: ES_OUT_SET_(GROUP_)PCR  is called too late (pts_delay increased
  to 547 ms)
 [00007f46fc0009b8] core input error: ES_OUT_RESET_PCR called

 user@ubuntu:~$ [00007f46fc0009b8] core input error: ES_OUT_SET_(GROUP_)PCR  is called too late (pts_
 delay increased to 637 ms)
 [00007f46fc0009b8] core input error: ES_OUT_RESET_PCR called
 [00007f46fc0009b8] core input error: ES_OUT_SET_(GROUP_)PCR  is called too late (pts_delay increased
  to 719 ms)
 [00007f46fc0009b8] core input error: ES_OUT_RESET_PCR called

 user@ubuntu:~$ _
```

6. Open a web browser to Login to Webmin by SSL in order to change some VM configurations.

Default: https://192.168.10.101:10000

User Name/Password: user/user



You must enter a username and password to login to the server on 192.168.10.101

user

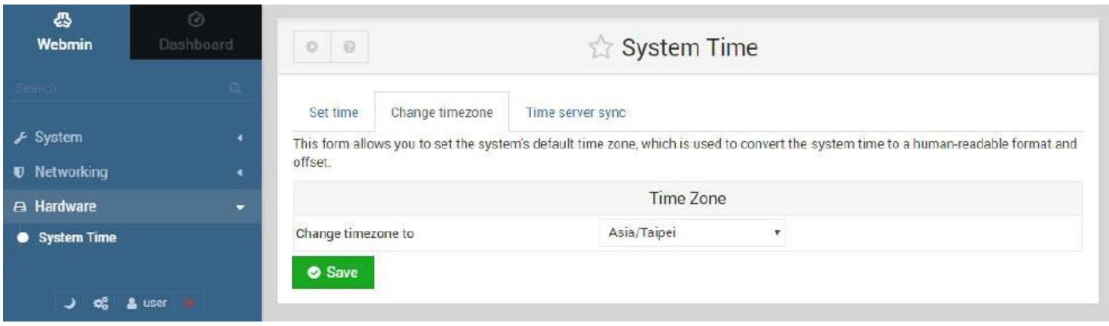
····

□ Remember me

7. Configure the IP address and Gateway (optional). Select ‘eth0’ to change IP address and add default gateway if needed.

8. Configure Date & Time of the ThingsMaster Virtual Machine.

Please adjust the time and change time zone of the VM first. User can configure it from the Webmin interface. Go to Hardware -> System Time -> Set Time -> Change Time Zone



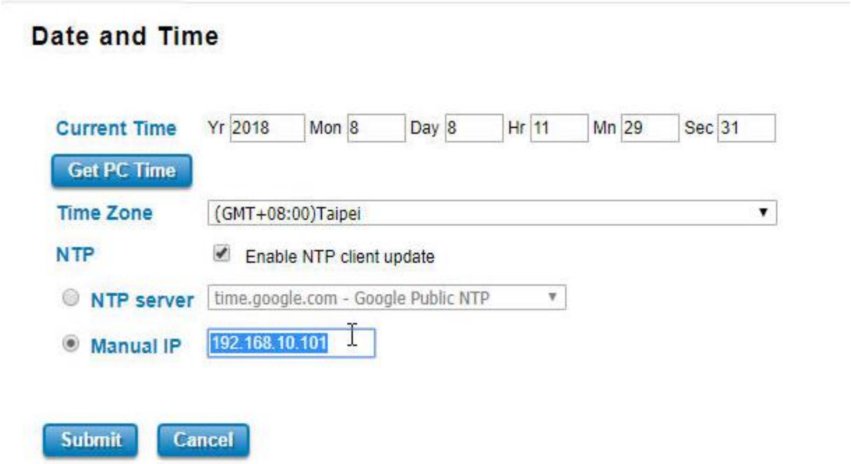
This form allows you to set the system's default time zone, which is used to convert the system time to a human-readable format and offset.

Change timezone to: Asia/Taipei

9. Adjust the time setting by using NTP

ThingsMaster server has already enabled NTP service; user can synchronize the system time of the device by using NTP.

- Enable the NTP Client from the Web GUI -> choose the Manual IP -> enter the server IP Address (192.168.10.101)



Date and Time

Current Time: Yr 2018 Mon 8 Day 8 Hr 11 Mn 29 Sec 31

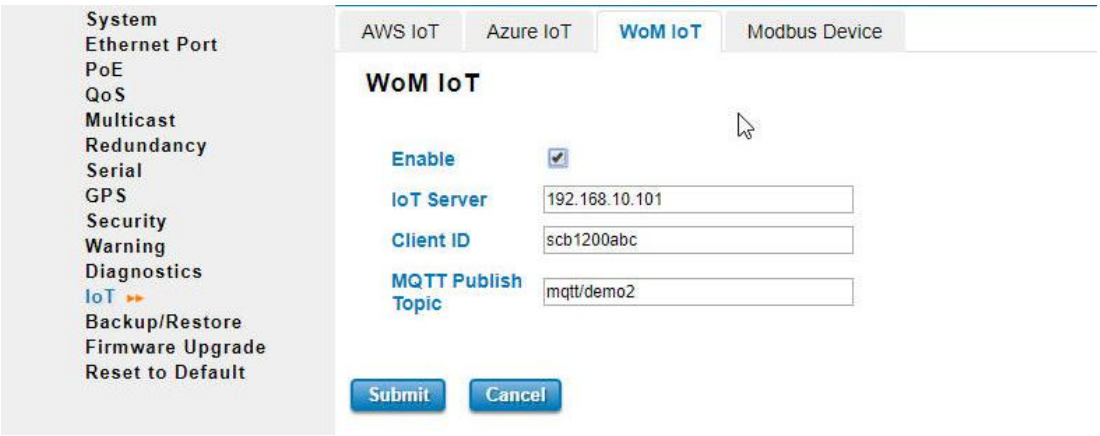
Time Zone: (GMT+08:00)Taipei

NTP: ☑ Enable NTP client update

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

● Manual IP: 192.168.10.101

10. Enable WoM IoT service and get connected to the ThingsMaster.



WoM IoT

Enable: ☑

IoT Server: 192.168.10.101

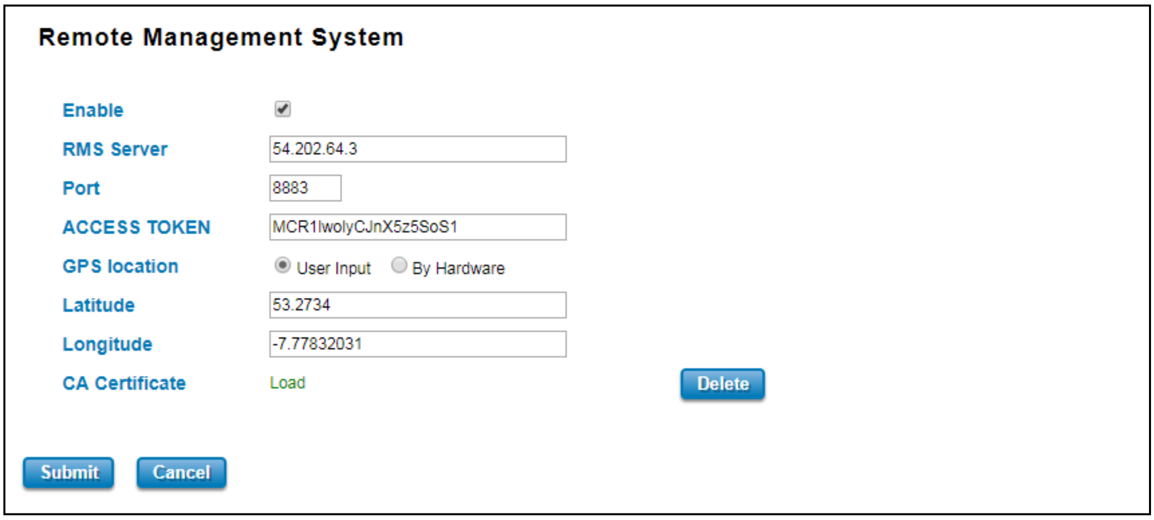
Client ID: scb1200abc

MQTT Publish Topic: mqtt/demo2

3.3.4 RMS

WoMaster supports Over-the-Air Remote Monitoring System (RMS), **ThingMaster OTA**. This page allows the user to configure the RMS settings for the device, so that the device will be monitored through the ThingsMaster OTA RMS. The software is strong and easily to monitor your network over-the-air, you can apply the software with up to thousand nodes monitoring from our sales.

Not every version firmware supports this feature, while you have need to run over-the-air monitoring and doesn't find the configuration file, please contact our sales/technical window for further discuss.



Remote Management System

Enable ☑

RMS Server 54.202.64.3

Port 8883

ACCESS TOKEN MCR1lwolyCJnX5z5SoS1

GPS location ● User Input ○ By Hardware

Latitude 53.2734

Longitude -7.77832031

CA Certificate Load

The description of the columns is as below:

TERMS	DESCRIPTION
Enable	Check the box to enable the RMS function.
RMS Server	Enter the RMS Server IP Address
Port	**Default: 8883**
ACCESS TOKEN	Generate the token from ThingsMaster RMS; this access token is used to access the device.
GPS Location	**User Input**: User input the device location information. **By Hardware**: if the device is supported with the GPS feature, then it will directly generate the location.
Latitude	Enter the Latitude coordinate of the device
Longitude	Enter the Longitude coordinate of the device
CA Certificate	The function from this certificate file is to create an encrypted MQTT communication. User will get this file when download the ThingsMaster server file. **Note. This field only supports in ThingsMaster v1.1**

Click Submit to apply the configuration. After succeed with the registration then the device will appear on the ThingsMaster OTA RMS dashboard.

HOW TO ESTABLISH AND CONNECT TO THE THINGSMASTER OTA RMS SERVER

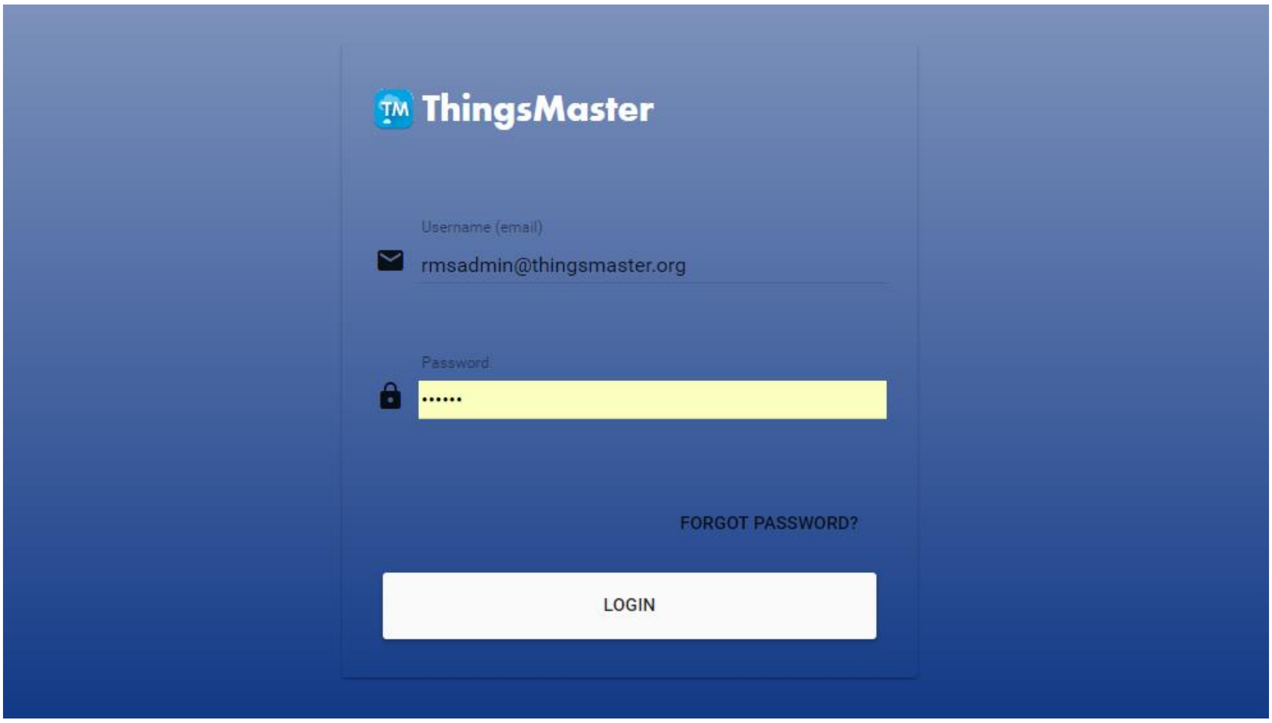
Note: The UI of the ThingMaster, ThingMaster OTA RMS and VMWare software and download link is often updated, following steps and figures may be updated.

1. Contact our Sales to get the access to the ThingsMaster RMS Account.

2. Login to ThingsMaster OTA RMS, using RMS Account.

Login: <User RMS Account>

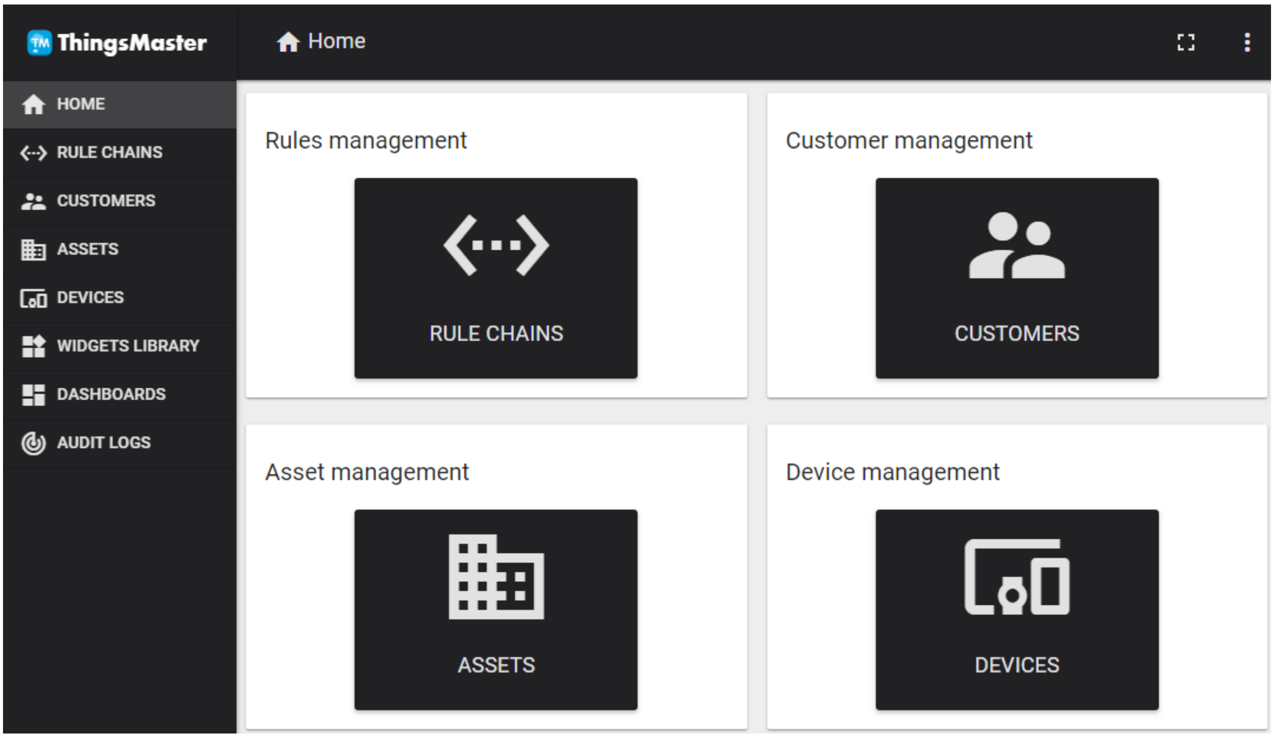
Password: <User RMS Password>



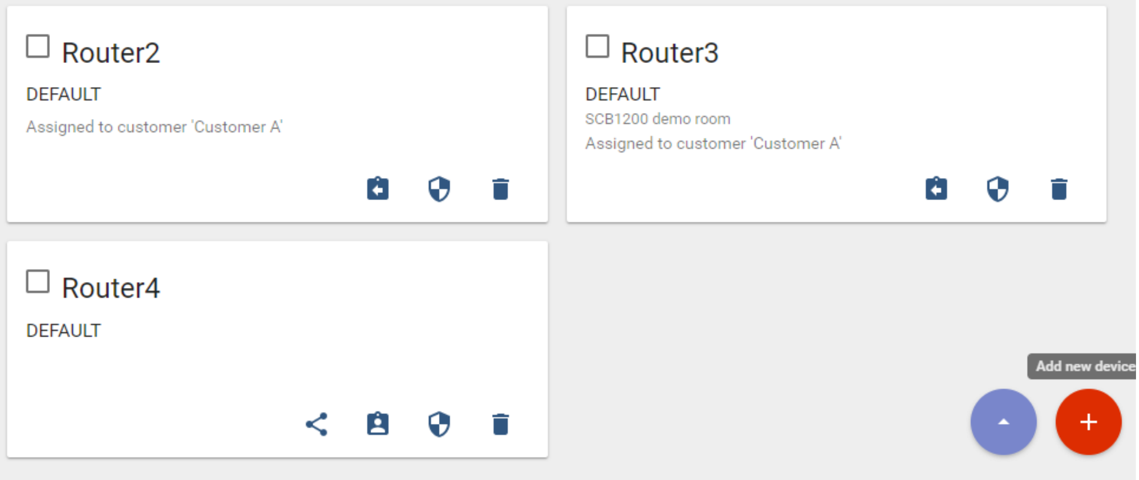
Username (email): rmsadmin@thingsmaster.org

Password: ••••••

3. Go to Home -> Device Management to register the device.



4. Add new device information, by clicking the “+” at the corner of the page.



□ Router2

DEFAULT

Assigned to customer 'Customer A'

□ Router3

DEFAULT

SCB1200 demo room

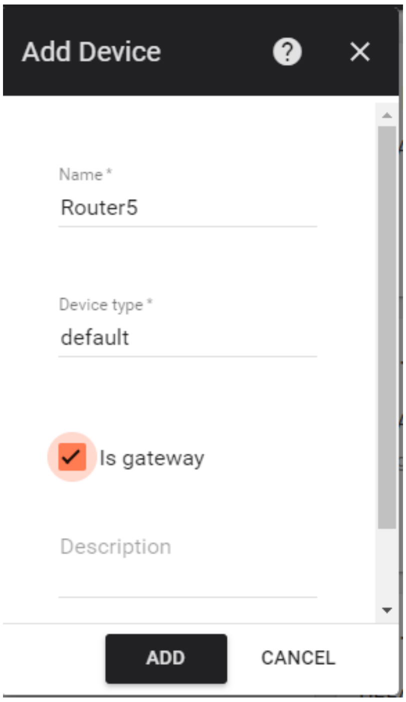
Assigned to customer 'Customer A'

□ Router4

DEFAULT

After click “+” menu then a page will pop up. Enter the device information.

- Name: Please start the name with Router + Number.
- Device type: default
- Is gateway: check the box
- Click **Add**



Add Device

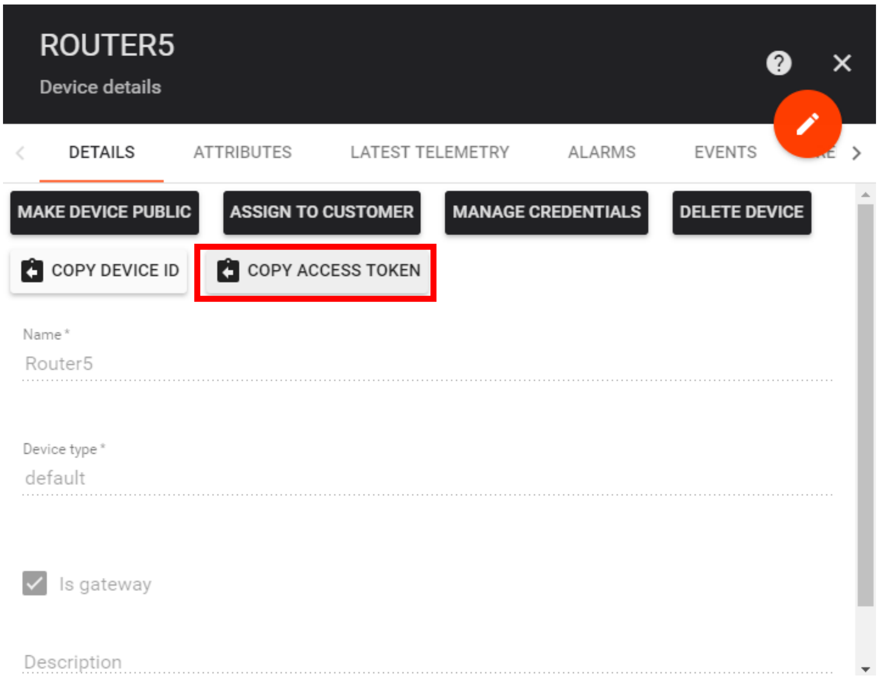
Name *
Router5

Device type *
default

☑ Is gateway

Description

5. After the device is registered, then click on the device folder go to Details -> Click on Copy Access Token. This access token is code to link the device with the RMS Server.



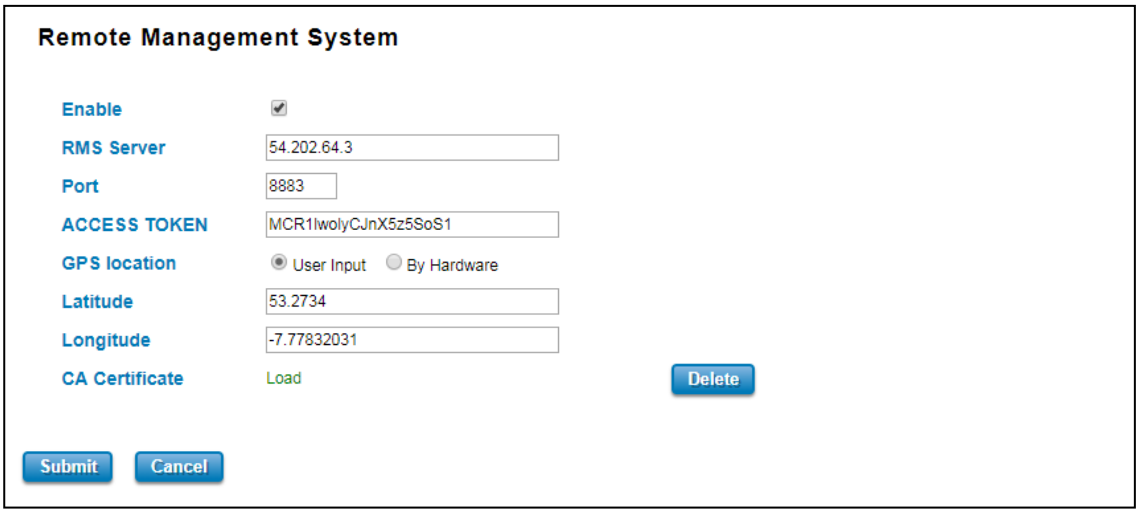
Name *
Router5

Device type *
default

☑ Is gateway

Description

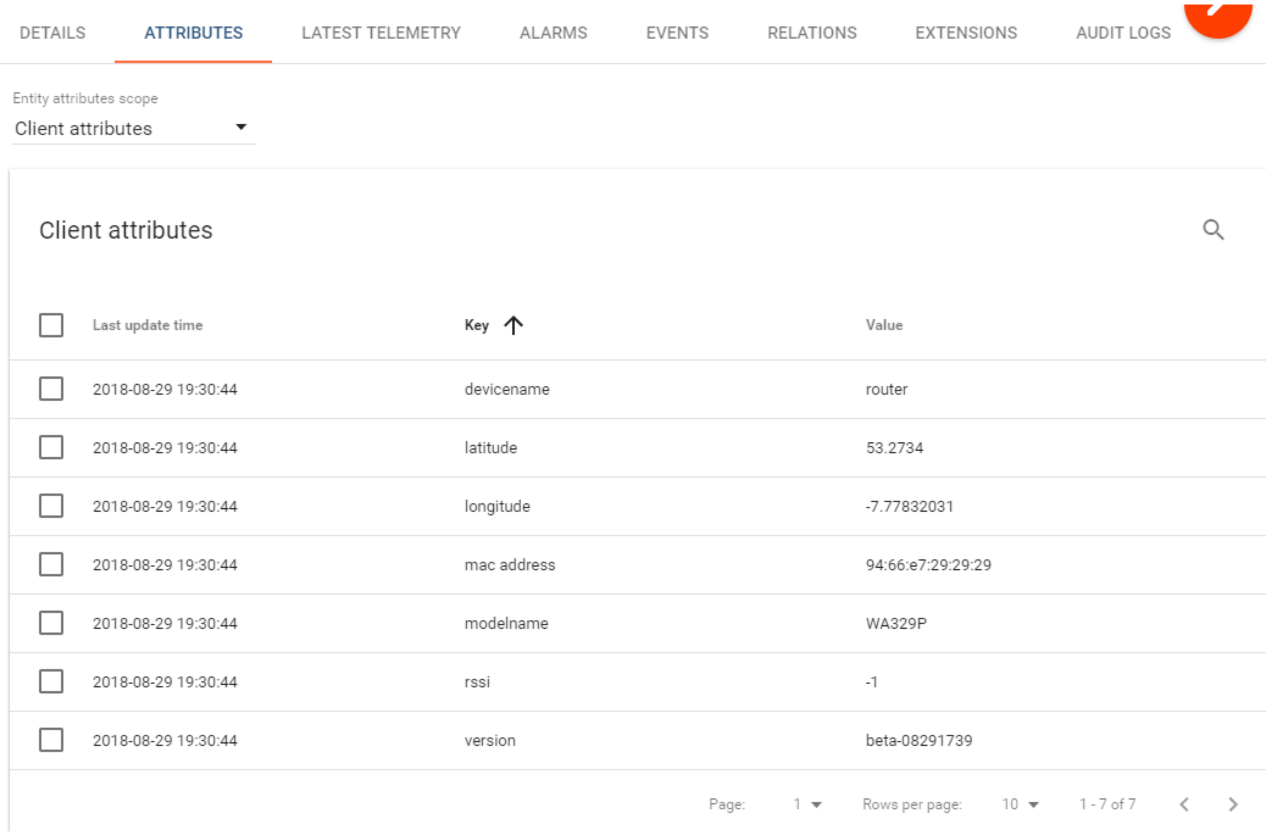
6. Go to the Web GUI -> IoT -> RMS. Paste the Access Token code to the Web GUI. And complete the configuration.



Remote Management System

Enable	☑	
RMS Server	54.202.64.3	
Port	8883	
ACCESS TOKEN	MCR1lwolyCJnX5z5SoS1	
GPS location	● User Input ○ By Hardware	
Latitude	53.2734	
Longitude	-7.77832031	
CA Certificate	Load	Delete

7. After the configuration is done then go back to ThingsMaster RMS Server. And then click on the newly added Router -> Attributes-> Client Attributes to see if the data has been uploaded.



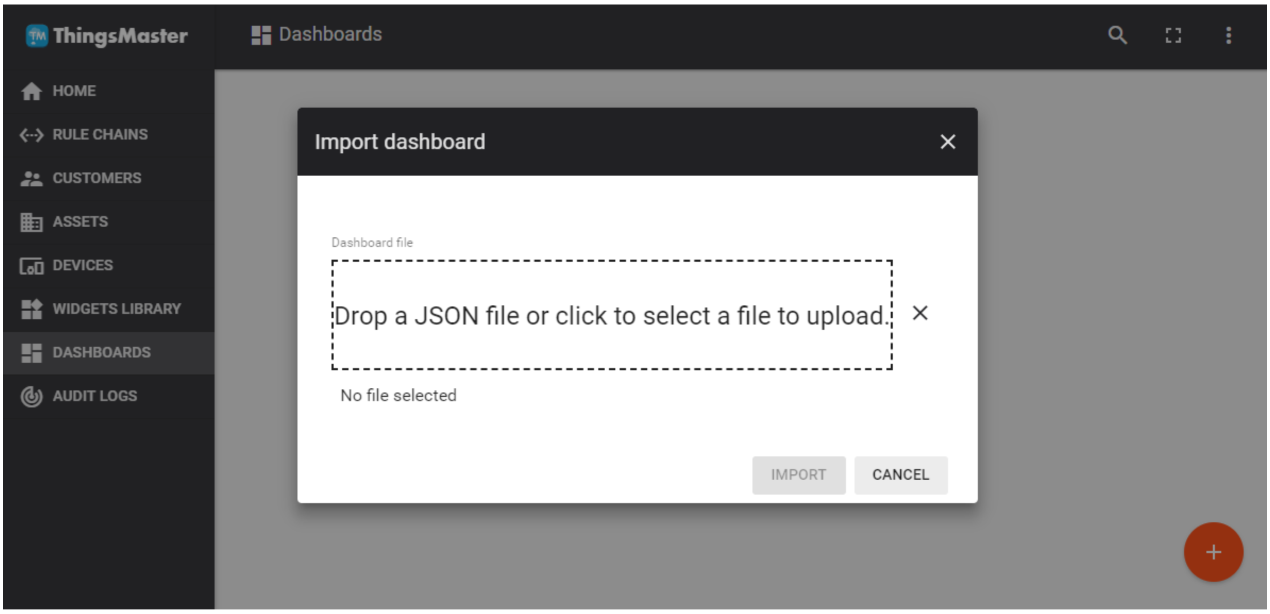
Entity attributes scope: Client attributes

Client attributes

□	Last update time	Key ↑	Value
□	2018-08-29 19:30:44	devicename	router
□	2018-08-29 19:30:44	latitude	53.2734
□	2018-08-29 19:30:44	longitude	-7.77832031
□	2018-08-29 19:30:44	mac address	94:66:e7:29:29:29
□	2018-08-29 19:30:44	modelname	WA329P
□	2018-08-29 19:30:44	rssi	-1
□	2018-08-29 19:30:44	version	beta-08291739

Page: 1 Rows per page: 10 1 - 7 of 7

8. If all of the data has been uploaded, user can create a dashboard to visualize the data. Go to Dashboards menu. In this page, user can upload the JSON file that sent by the WoMaster Sales in the email. Click the "+" to import JSON File or Create a new Dashboard.



Import dashboard

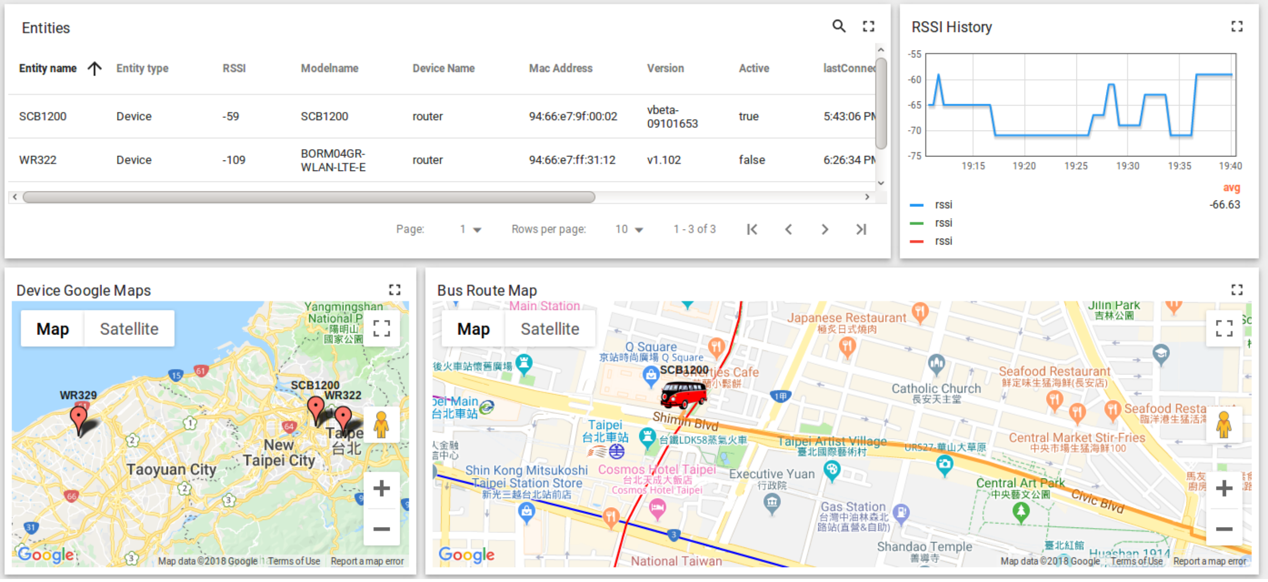
Dashboard file

Drop a JSON file or click to select a file to upload.

No file selected

IMPORT CANCEL

9. After the JSON file is uploaded, the dashboard will show as below:



Entities

Entity name ↑	Entity type	RSSI	Modelname	Device Name	Mac Address	Version	Active	lastConnec
SCB1200	Device	-59	SCB1200	router	94:66:e7:9f:00:02	vbeta-09101653	true	5:43:06 PM
WR322	Device	-109	BORM04GR-WLAN-LTE-E	router	94:66:e7:ff:31:12	v1.102	false	6:26:34 PM

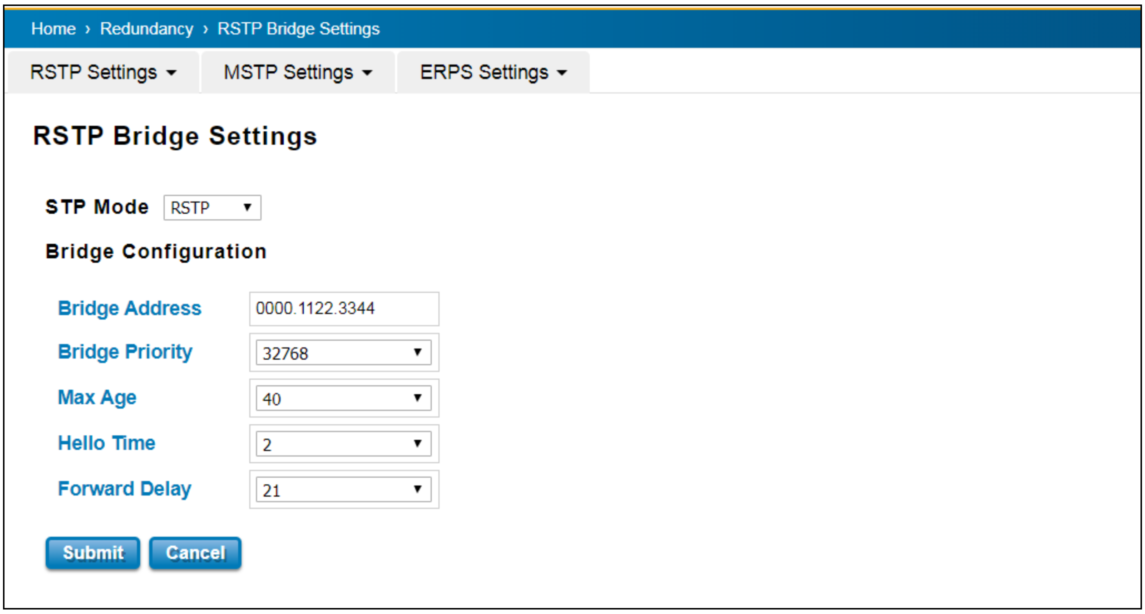
Page: 1 Rows per page: 10 1 - 3 of 3

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 **Enhanced RSTP, 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.



RSTP Bridge Settings

STP Mode: RSTP

Bridge Configuration

Bridge Address	0000.1122.3344
Bridge Priority	32768
Max Age	40
Hello Time	2
Forward Delay	21

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.

<u>Bridge Configuration</u>

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

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

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

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

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

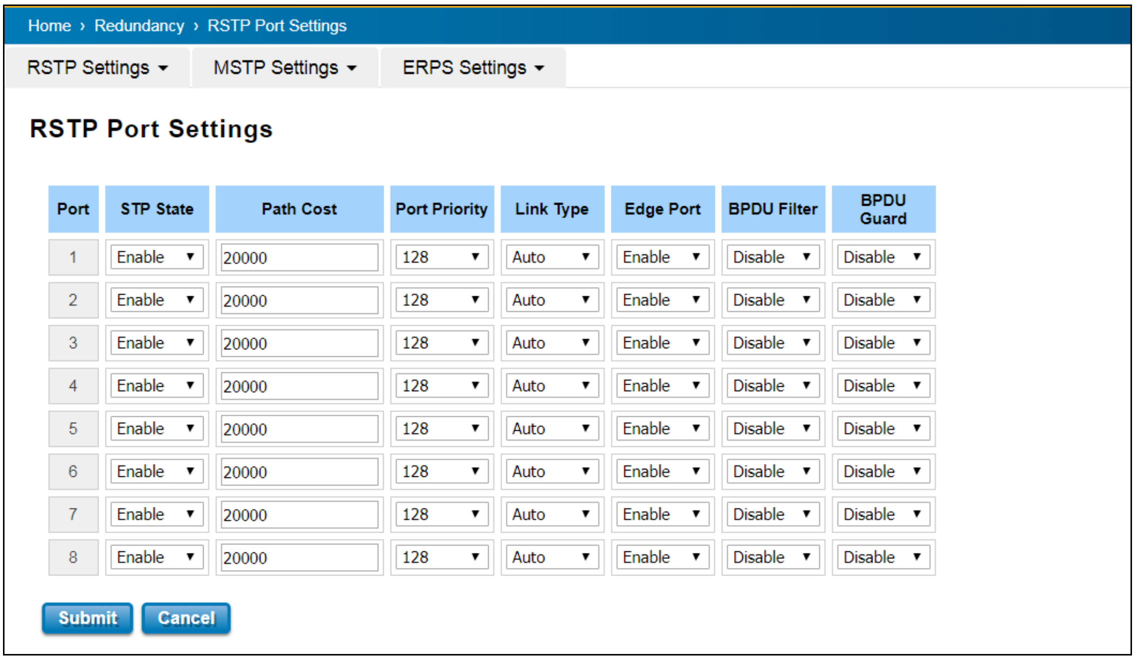
Forward Delay Time (4-30): Enter a value between 4 and 30 seconds. This value is the time that a port waits before changing from Spanning Tree Protocol learning and listening states to forwarding state.

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

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

RSTP Port Settings

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



RSTP Port Settings

Port	STP State	Path Cost	Port Priority	Link Type	Edge Port	BPDU Filter	BPDU Guard
1	Enable	20000	128	Auto	Enable	Disable	Disable
2	Enable	20000	128	Auto	Enable	Disable	Disable
3	Enable	20000	128	Auto	Enable	Disable	Disable
4	Enable	20000	128	Auto	Enable	Disable	Disable
5	Enable	20000	128	Auto	Enable	Disable	Disable
6	Enable	20000	128	Auto	Enable	Disable	Disable
7	Enable	20000	128	Auto	Enable	Disable	Disable
8	Enable	20000	128	Auto	Enable	Disable	Disable

The description of the columns is as below:

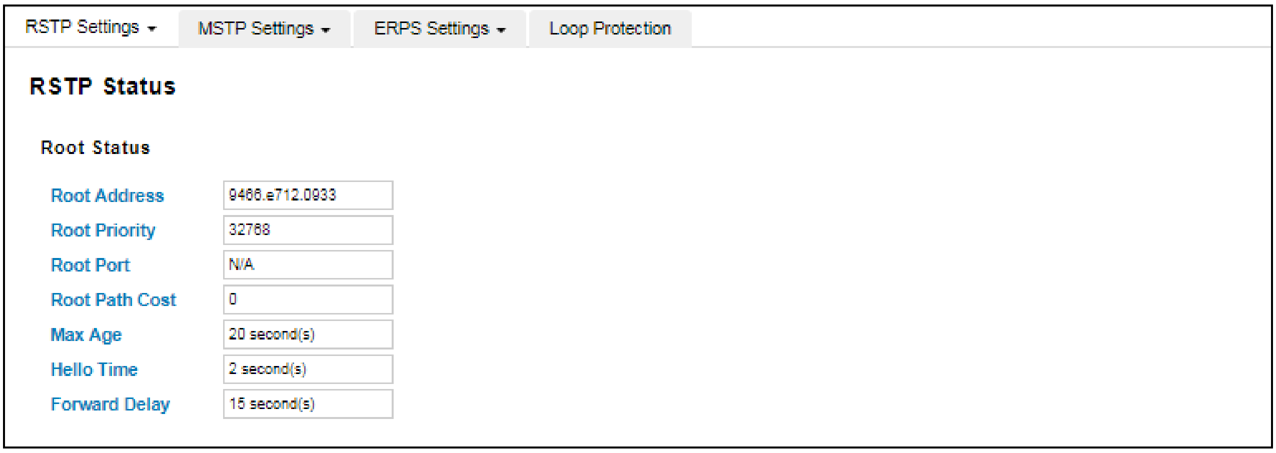
TERMS	DESCRIPTION
STP State	**Default: Enable** To enable or disable STP function.
Path Cost	Enter a number between 1 and 200,000,000. This value represents the "**cost**" of the path to the other bridge from the transmitting bridge at the specified port.
Priority	Enter a value between 0 and 240, using 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.

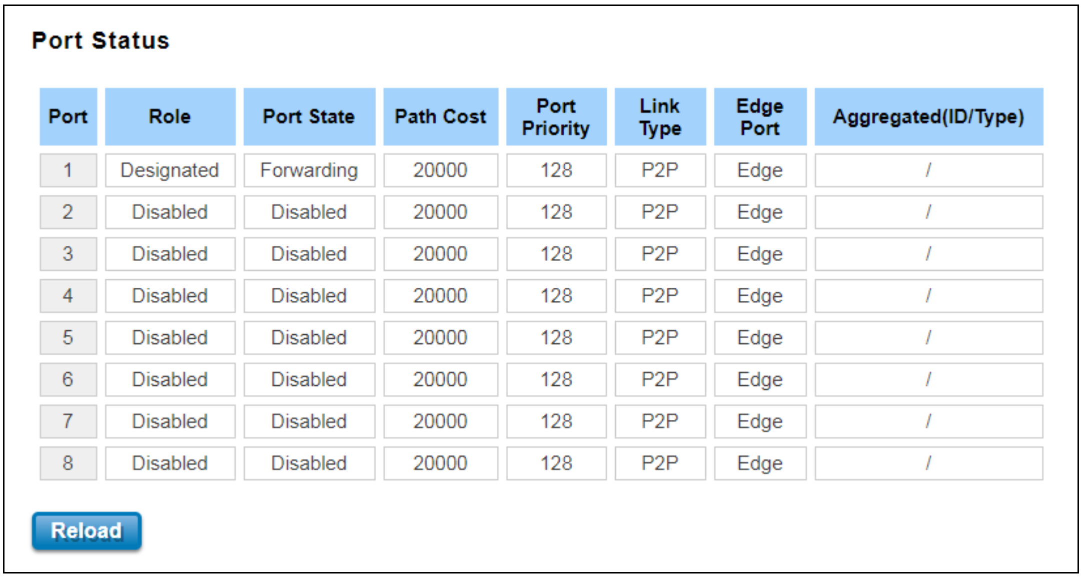


RSTP Status

Root Status

Root Address	9466.e712.0933
Root Priority	32768
Root Port	N/A
Root Path Cost	0
Max Age	20 second(s)
Hello Time	2 second(s)
Forward Delay	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 BPDU sent from the root switch.



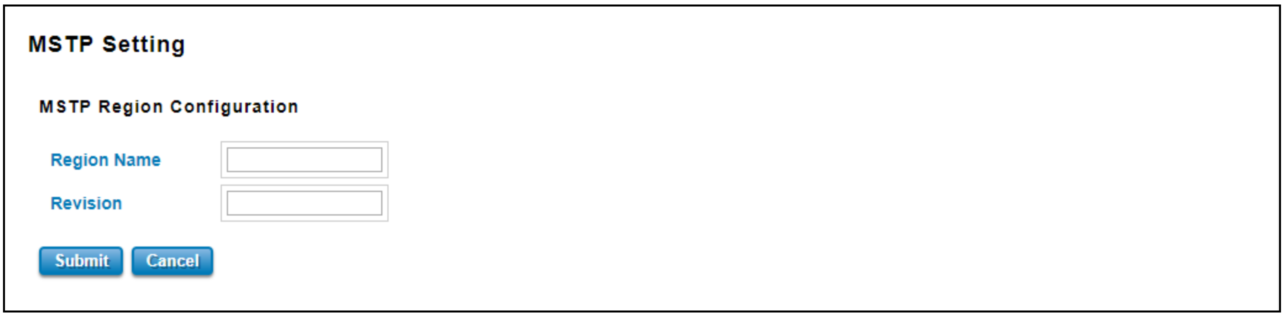
Port Status

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

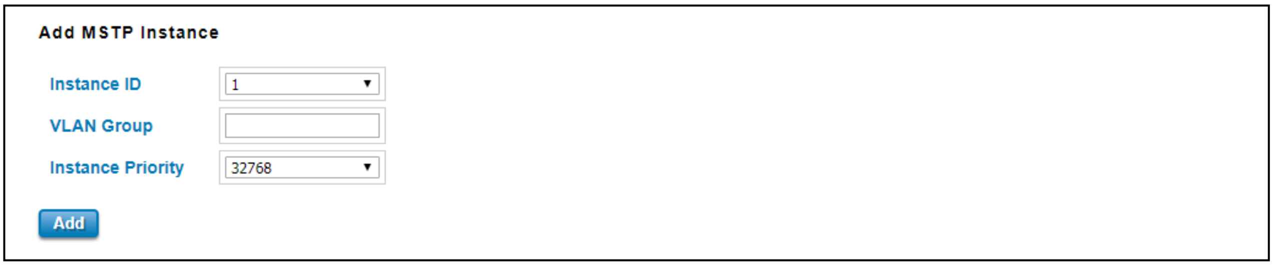
Revision

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: 1

VLAN Group

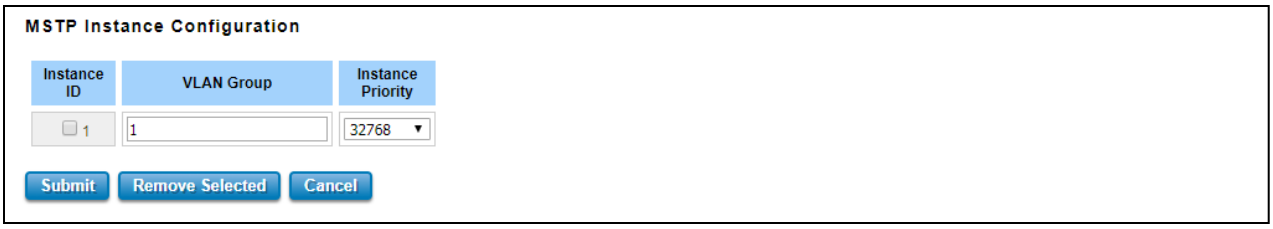
Instance Priority: 32768

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.

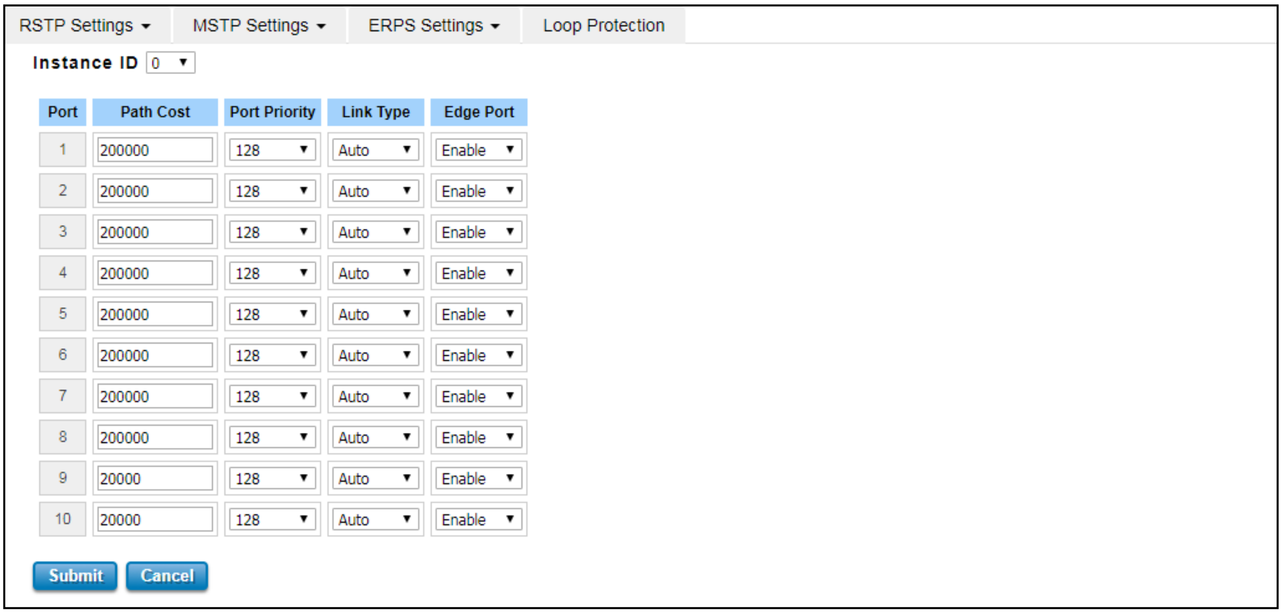


MSTP Instance Configuration

Instance ID	VLAN Group	Instance Priority
□ 1	1	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.



Instance ID 0 ▾

Port	Path Cost	Port Priority	Link Type	Edge Port
1	200000	128	Auto	Enable
2	200000	128	Auto	Enable
3	200000	128	Auto	Enable
4	200000	128	Auto	Enable
5	200000	128	Auto	Enable
6	200000	128	Auto	Enable
7	200000	128	Auto	Enable
8	200000	128	Auto	Enable
9	20000	128	Auto	Enable
10	20000	128	Auto	Enable

The description of the columns is as below:

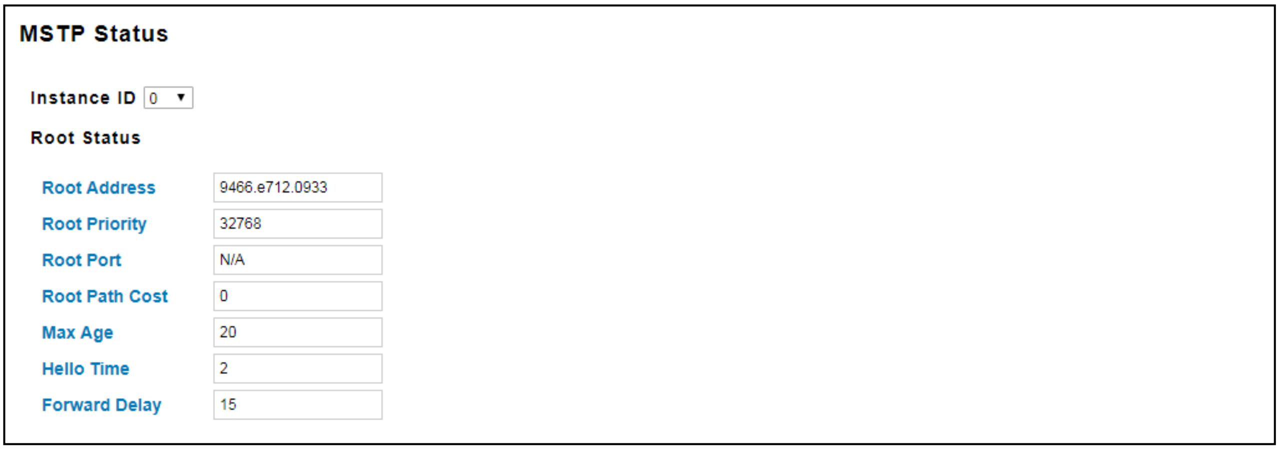
TERMS	DESCRIPTION
Path Cost	Enter a number between 1 and 200,000,000. This value represents the cost of the path to the other bridge from the transmitting bridge at the specified port. Path cost value is derived from the media speed of an interface. If a loop occurs, the MSTP uses cost when selecting 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.



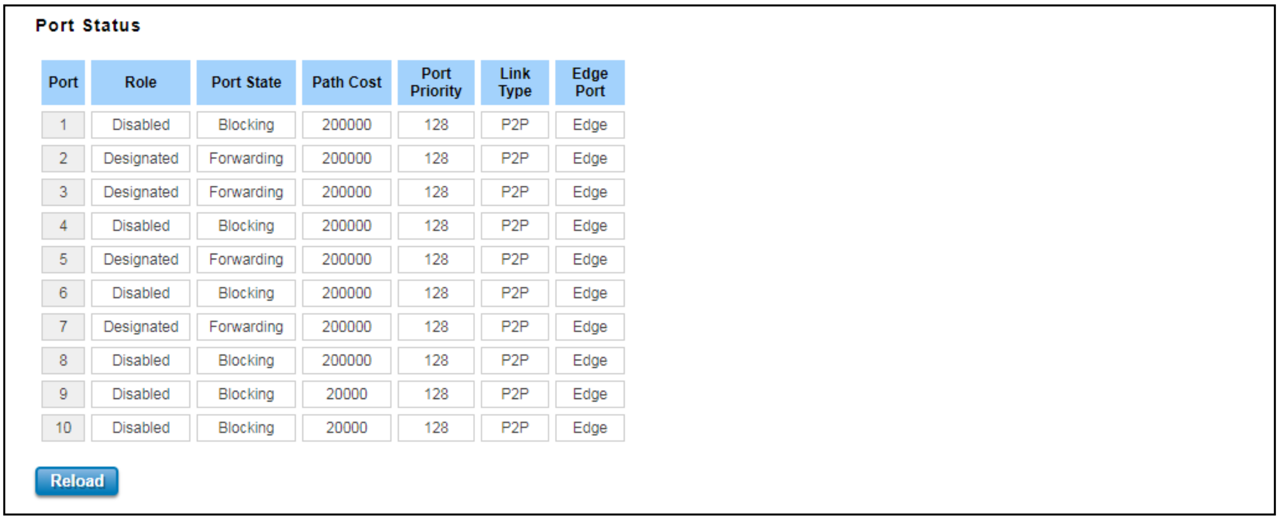
MSTP Status

Instance ID 0 ▼

Root Status

Root Address	9466.e712.0933
Root Priority	32768
Root Port	N/A
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15

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 Enhanced Rapid Spanning Tree Protocol (eRSTP)

With the support of new software, the switch can support enhanced RSTP (eRSTP), which can increase the number of large **Ring** network topologies. This setting is limited to the ring network architecture and needs to be modified with the Max Age value. The Max Age represents the step level from the Root Switch to the most remote level. For example, when the Max Age setting is modified, it represents Root (0) to the most remote switch (Max). The maximum recommended number is "Max Age-1", for example: When setup the Max age = 40, (40 is the maximum value defined in RSTP protocol), the maximum recommended number is 39 units.

Why maximum 80 units?

The maximum device of eRSTP is **Two** times of **"MAX Age"**. In eRSTP Ring network mode, while the MAX Age is configured to 40, the maximum unit eRSTP Ring can support is 2 times of 40, which means the level of connected switches in Root Switch's left side and right side is 40, so that you have connect up to 80 units. **The eRSTP supports maximum 80 units in a Ring network only, it is NOT Allowed to connect more than 80 switches, the 81th switch can be controlled in a eRSTP Ring network**. To achieve maximum 80 units, the **Max Age** in RSTP setting should be configured to **40**, this is MUST configuration in RSTP setup page.

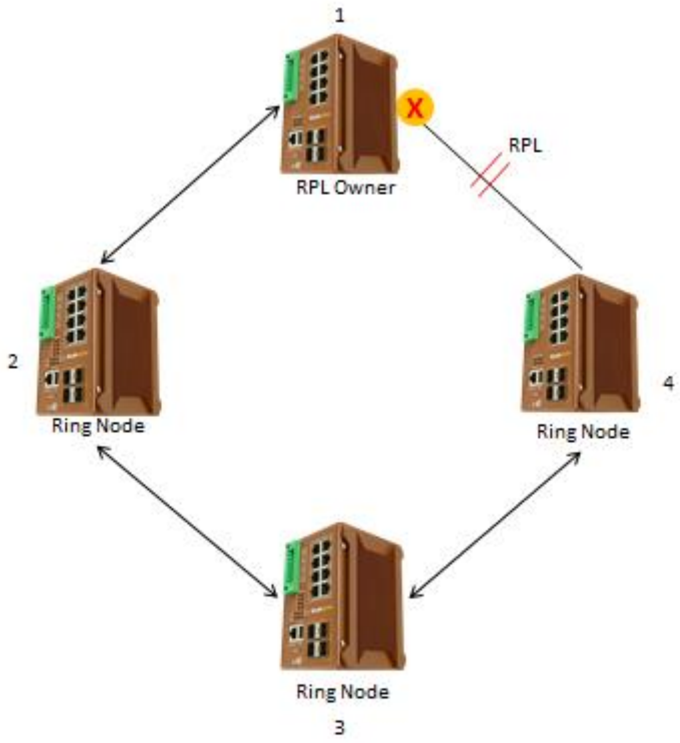
How to Enable?

The enhanced RSTP (eRSTP) is supported by default and the settings are the same as RSTP, however, it is recommended that the eRSTP is used in the ring network **with all our brand products**, to achieve the best use effect and avoid the unexpected compatibility problems between different manufacturers. It is not recommended to be used in the complex/non-Ring Network topology.

For the use of eRSTP suggestions, you can consult with our technical window.

3.4.4 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.

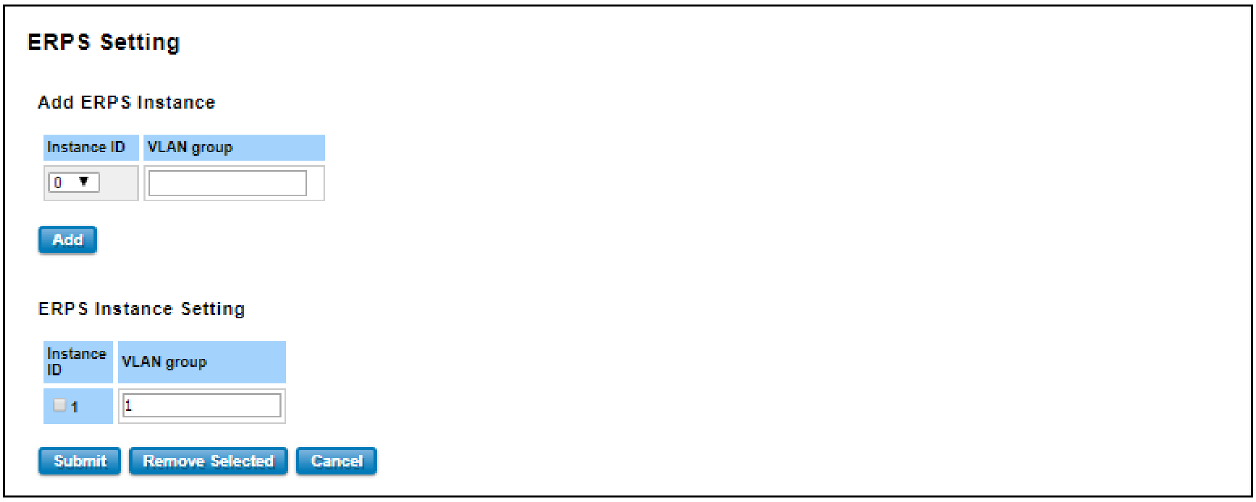


The figure above shows that each Ethernet Ring Node is connected to other Ethernet Ring Nodes that participating in the same Ethernet Ring using two independent links. In the Ethernet ring, loops can be avoided by guaranteeing that traffic may flow on all but one of the ring links at any time. This particular 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.

3.4.4.1 ERPS SETTINGS

ERPS Setting



ERPS Setting

Add ERPS Instance

Instance ID	VLAN group
0 ▼	

ERPS Instance Setting

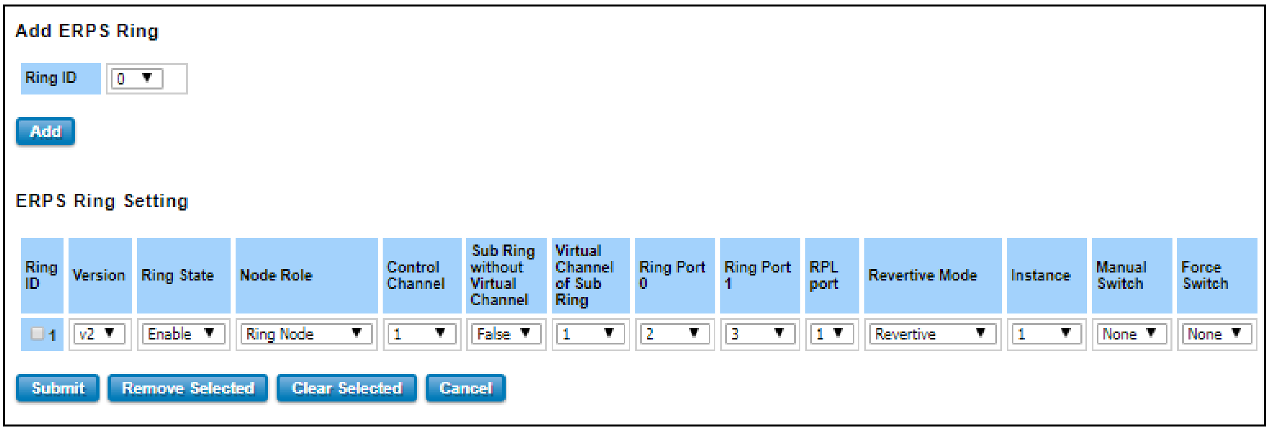
Instance ID	VLAN group
□ 1	1

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	0 ▼

ERPS Ring Setting

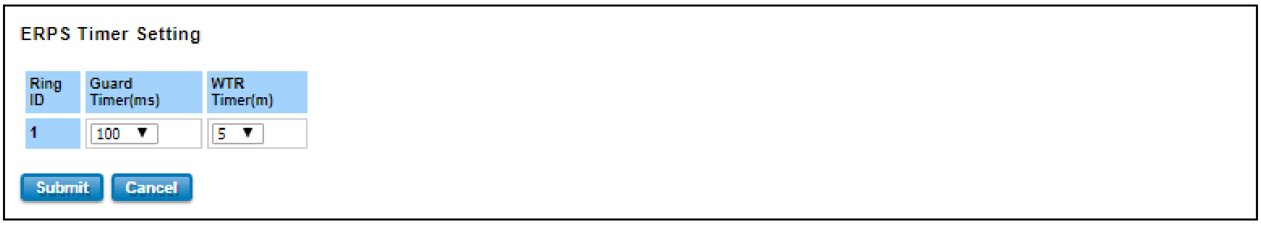
Ring ID	Version	Ring State	Node Role	Control Channel	Sub Ring without Virtual Channel	Virtual Channel of Sub Ring	Ring Port 0	Ring Port 1	RPL port	Revertive Mode	Instance	Manual Switch	Force Switch
□ 1	v2 ▼	Enable ▼	Ring Node ▼	1 ▼	False ▼	1 ▼	2 ▼	3 ▼	1 ▼	Revertive ▼	1 ▼	None ▼	None ▼

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 Ring Port 0 or Ring Port 1 as the RPL block.
Revertive Mode	**Default: Revertive** **Revertive mode**, after the conditions causing a protection switch has cleared; the traffic channel is restored to the working transport entity that is blocked on the RPL. In **Non-Revertive mode**, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.
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



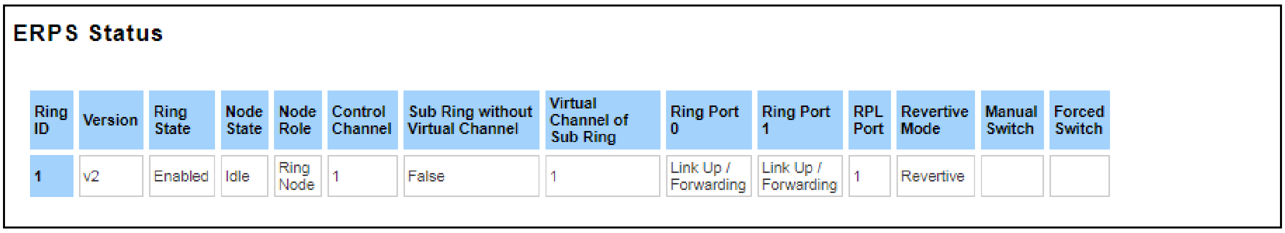
ERPS Timer Setting

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 1 and 12 minutes with a default value of 5 minutes.

3.4.4.2 ERPS STATUS

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



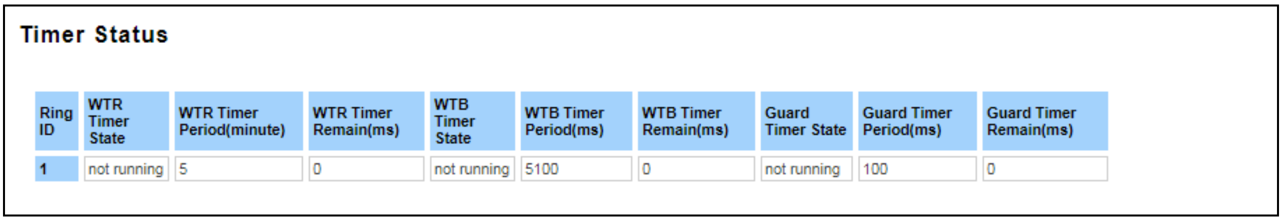
ERPS Status

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

TERMS	DESCRIPTION
Ring ID	Display the Ring ID
Version	ERPS Protocol Version - v1 or v2.
Ring State	**Default: Disable** Enabled - Ring Status is enable Disabled - Ring Status is disable
Node State	Status from the **Ring is Idle, Protection, Manual Switch, Force Switch** or **Pending.**
Node Role	It can be either **RPL owner** or **RPL Neighbor** or **Ring Node.**
Control Channel	Control Channel is referred to the VLANs number (1-4094)
Sub Ring without Virtual Channel	**Default: False** **True** – if have a virtual channel **False** – if doesn't have any virtual channel
Virtual Channel of Sub Ring	**Default: 1** Sub-rings can have a virtual channel on the interconnected node. Choose the number based on the VLANs Range (1-4094)
Ring Port 0	The status from the port Link up/link down and Forwarding/Blocking
Ring Port 1	The status from the port Link up/link down and Forwarding/Blocking

RPL Port	The port status as the RPL block.
Revertive Mode	**Default: Revertive** **Revertive mode**, after the conditions causing a protection switch has cleared; the traffic channel is restored to the working transport entity that is, blocked on the RPL. In **Non-Revertive mode**, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.
Manual Switch	Status from the Ring Port 0 and 1 or None
Force Switch	Status from the Ring Port 0 and 1 or None

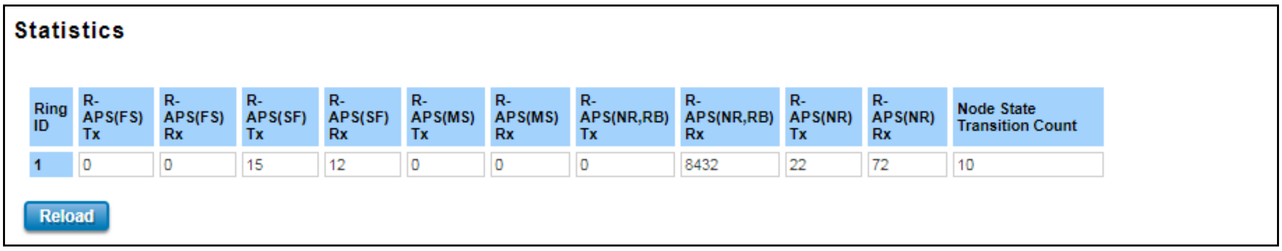
Timer Status



Timer Status

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

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



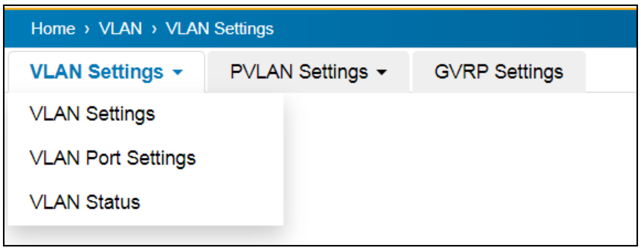
Statistics

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

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

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

3.5 VLAN



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

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

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

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

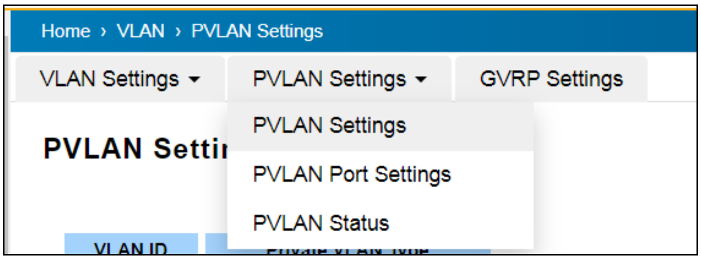
Benefits of VLANs

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

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

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

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



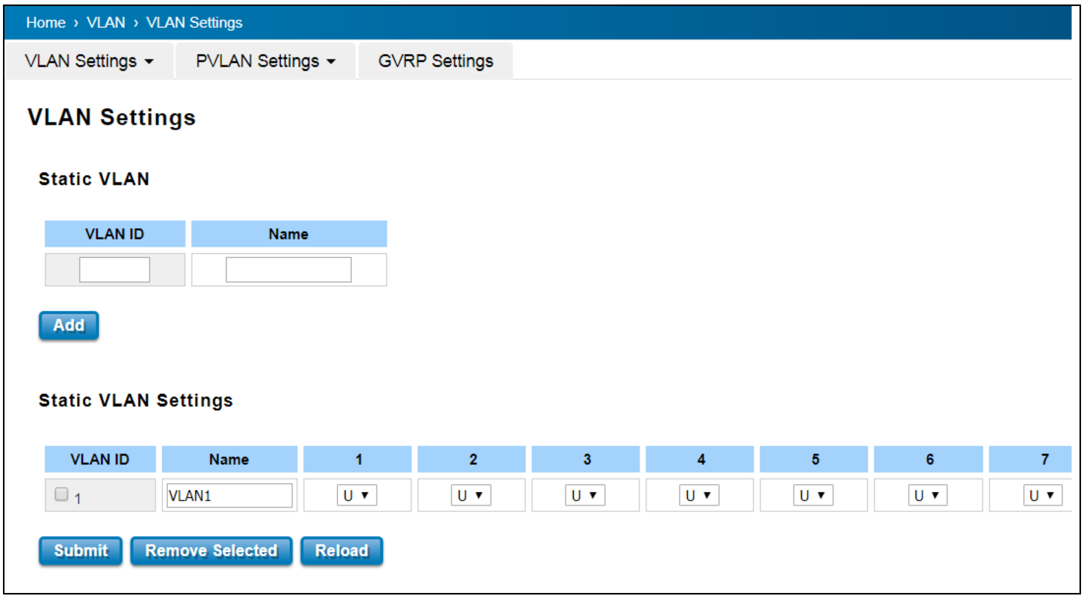
This switch also has **private VLAN** functions; it helps to resolve the primary VLAN ID shortage, client ports' isolation and network security issues. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains, allowing User to isolate the ports on the switch from each other. A subdomain consists of a primary VLAN and one or more secondary VLANs. All VLANs in a private VLAN domain share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another. The secondary VLANs may either be isolated VLANs or community VLANs. A host on an isolated VLAN can only communicate with the associated promiscuous port in its primary VLAN.

Hosts on community VLANs can communicate among themselves and with their associated promiscuous port but not with ports in other community VLANs. The Private VLAN provides **primary** and **secondary VLAN** within a single switch.

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

3.5.1 VLAN SETTING

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



VLAN Settings

Static VLAN

VLAN ID	Name

Static VLAN Settings

VLAN ID	Name	1	2	3	4	5	6	7
□ 1	VLAN1	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾

The description of the columns is as below:

TERMS	DESCRIPTION
Management VLAN ID (DS410)	**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. The VLAN ID is also the virtual interface for L3 Routing, you can assign IP Address/Netmask in Network Settings page.
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).

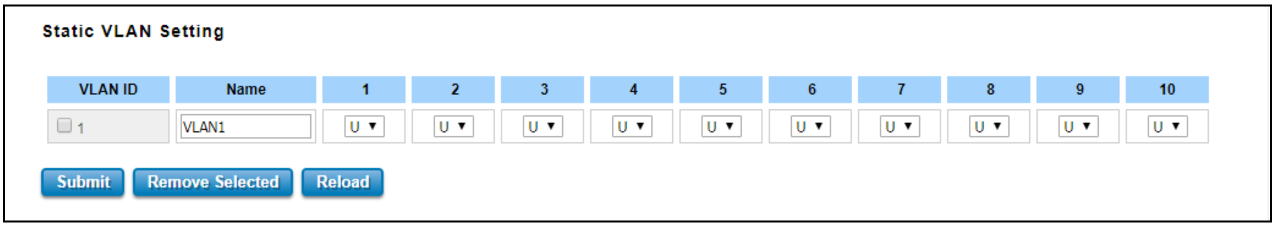
The steps to create a new VLAN: Type in VLAN ID and NAME, and press **Add** to create a new VLAN. Then User can see the new VLAN in the Static VLAN Configuration table. After created the VLAN, the status of the VLAN will remain in Unused until User adds ports to the VLAN.

NOTE:

Before User changed the management VLAN ID or Remove any VLAN by Web and Telnet, remember that the port attached by the administrator should be still the member port of the VLAN/IP Subnet; otherwise the administrator can't access the switch via the network.

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
□ 1	VLAN1	U	U	U	U	U	U	U	U	U	U

The description of the columns is as below:

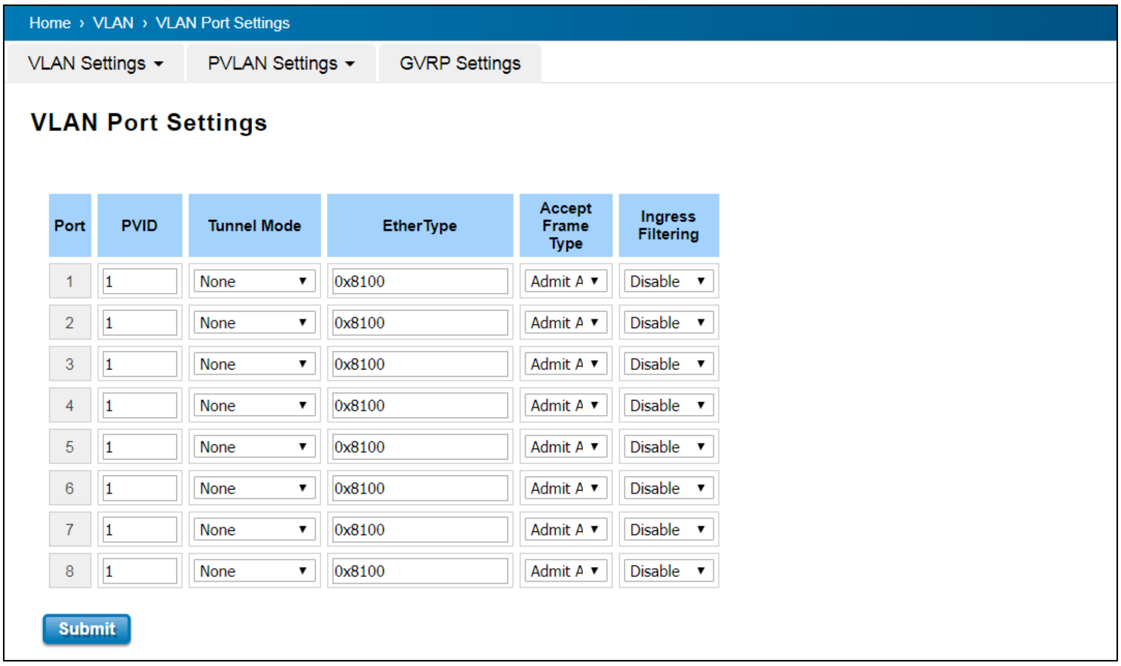
TERMS	DESCRIPTION
--	Not available
U/Untag	Indicates that egress/outgoing frames are not VLAN tagged.
T/Tag	Indicates that egress/outgoing frames are to be VLAN tagged.

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.



VLAN Port Settings

Port	PVID	Tunnel Mode	EtherType	Accept Frame Type	Ingress Filtering
1	1	None	0x8100	Admit A	Disable
2	1	None	0x8100	Admit A	Disable
3	1	None	0x8100	Admit A	Disable
4	1	None	0x8100	Admit A	Disable
5	1	None	0x8100	Admit A	Disable
6	1	None	0x8100	Admit A	Disable
7	1	None	0x8100	Admit A	Disable
8	1	None	0x8100	Admit A	Disable

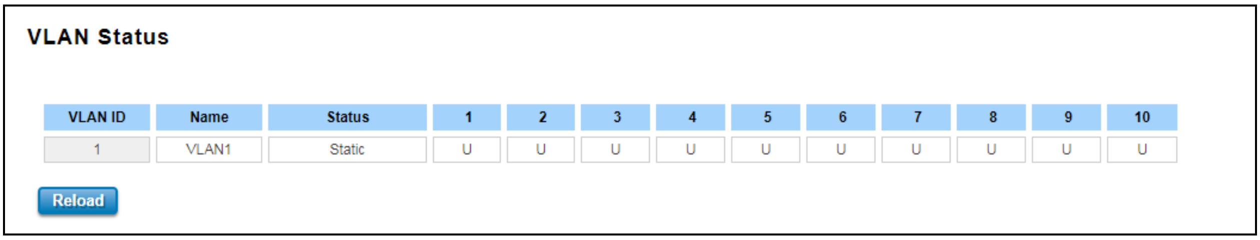
The description of the columns is as below:

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	**Default: None** **None** : This is Port that no using Q in Q **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. **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. **802.1Q Tunnel Uplink-Add-PVID**: Assign second VLAN tag for specify VLANs.
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.



VLAN Status

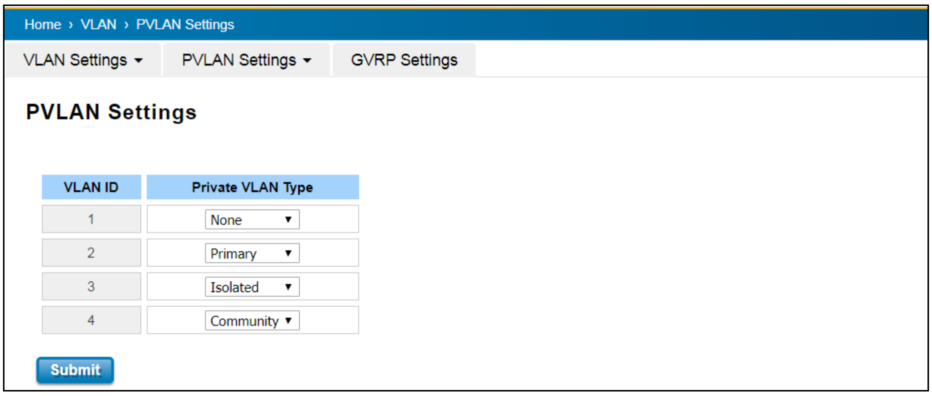
VLAN ID	Name	Status	1	2	3	4	5	6	7	8	9	10
1	VLAN1	Static	U	U	U	U	U	U	U	U	U	U

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



PVLAN Settings

VLAN ID	Private VLAN Type
1	None
2	Primary
3	Isolated
4	Community

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:

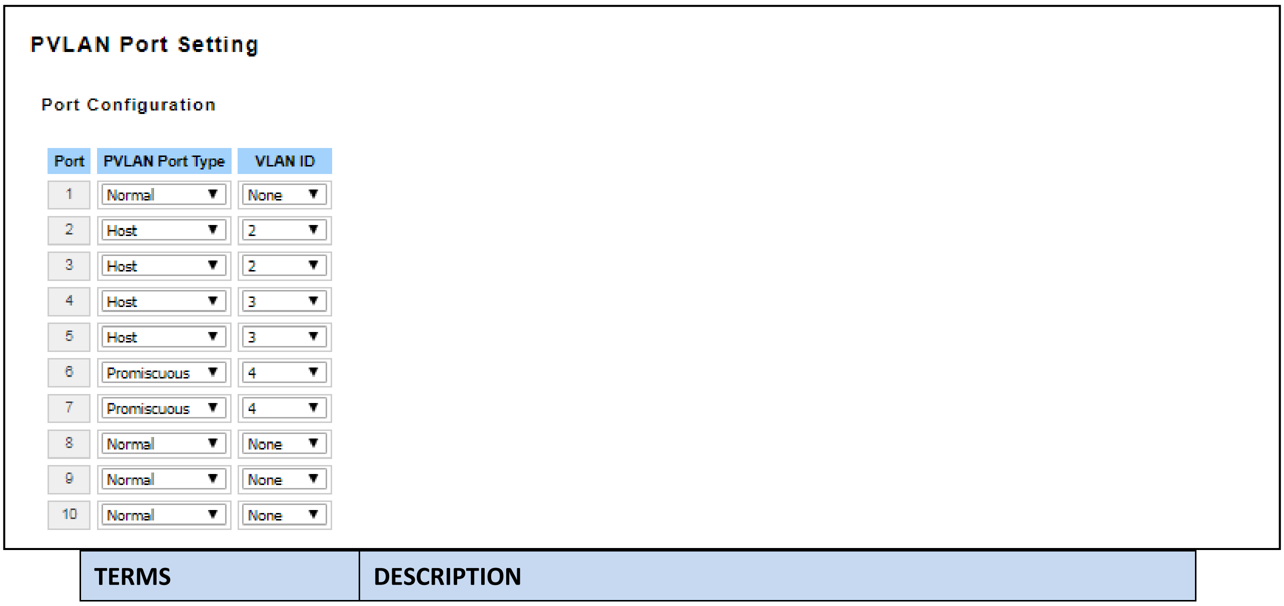
TERMS	DESCRIPTION
None	The VLAN is not included in Private VLAN.
Primary	The VLAN is the Primary VLAN. The member ports can communicate with secondary ports.
Isolated	The VLAN is the Isolated VLAN. The member ports of the VLAN are isolated.
Community	The VLAN is the Community VLAN. The member ports of 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:



PVLAN Port Setting

Port Configuration

Port	PVLAN Port Type	VLAN ID
1	Normal	None
2	Host	2
3	Host	2
4	Host	3
5	Host	3
6	Promiscuous	4
7	Promiscuous	4
8	Normal	None
9	Normal	None
10	Normal	None

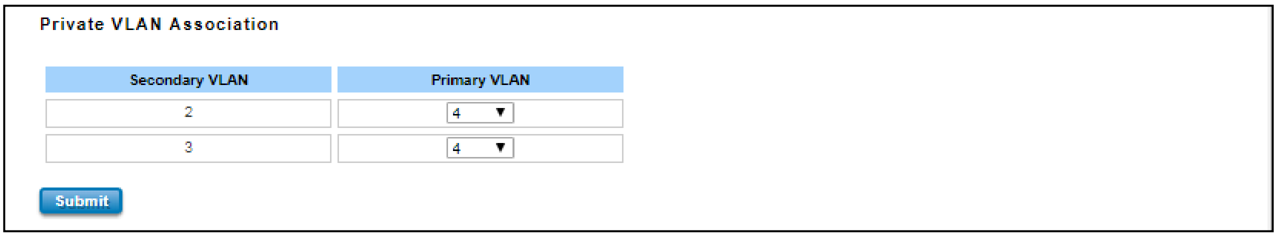
TERMS	DESCRIPTION

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

Private VLAN Association (PVLAN)

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

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

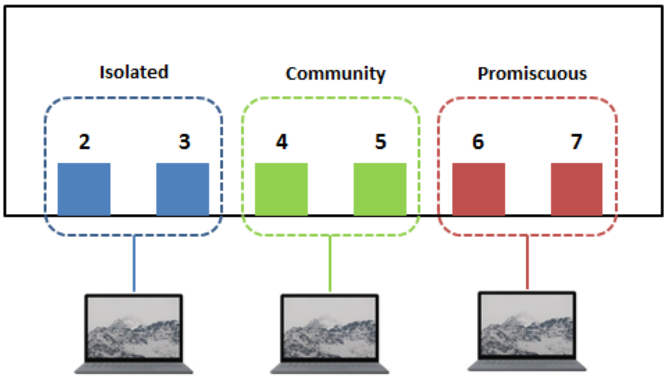


Private VLAN Association

Secondary VLAN	Primary VLAN
2	4 ▼
3	4 ▼

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

For example:



1. Create VLAN and Assign the Private VLAN Type:

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

2. Associate the Secondary VLAN to Primary VLAN:

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

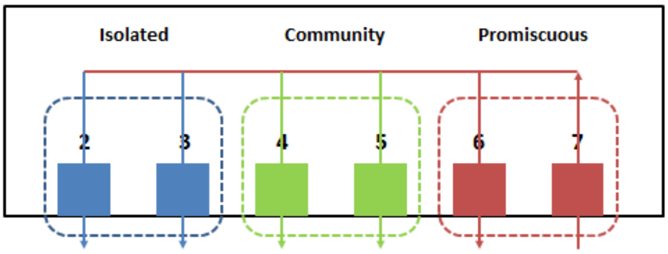
3. Configure the Private VLAN Port:

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

- VLAN 3 – **Community** -> Map the Host port to VLAN 3. (Port 4 and 5)

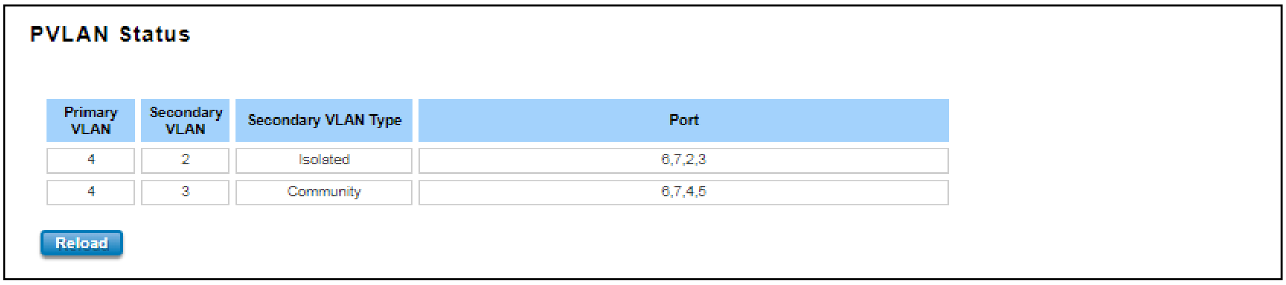
5. Result (See 3.5.6 PVLAN Status):

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



3.5.6 PVLAN STATUS

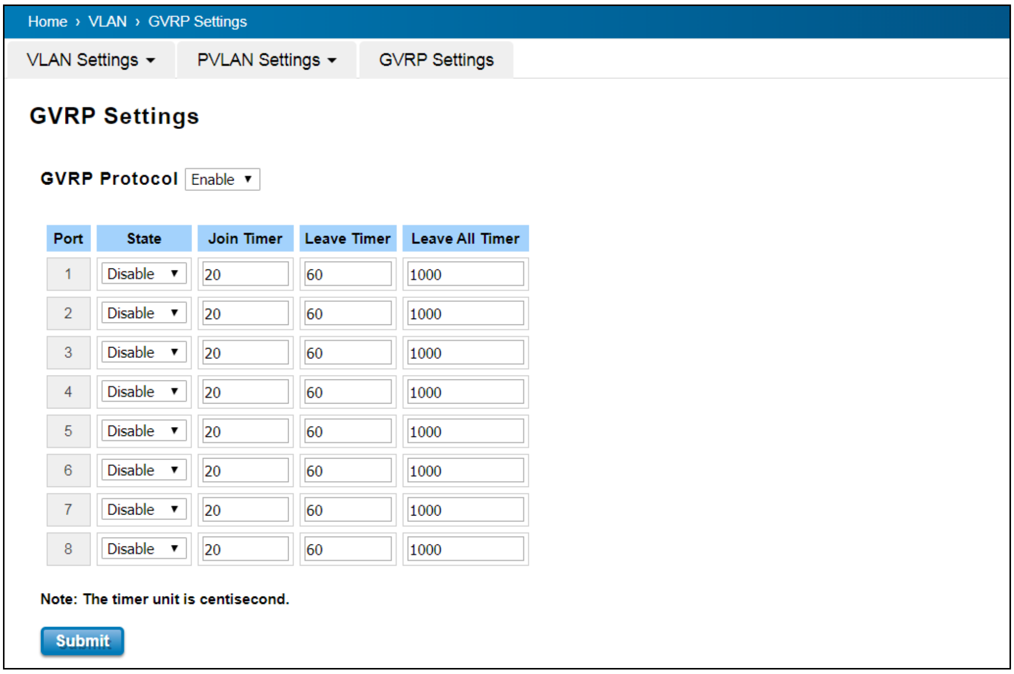
This page allows User to see the Private VLAN status information.



PVLAN Status

Primary VLAN	Secondary VLAN	Secondary VLAN Type	Port
4	2	Isolated	6,7,2,3
4	3	Community	6,7,4,5

3.5.7 GVRP SETTING



GVRP Settings

GVRP Protocol: Enable ▾

Port	State	Join Timer	Leave Timer	Leave All Timer
1	Disable ▾	20	60	1000
2	Disable ▾	20	60	1000
3	Disable ▾	20	60	1000
4	Disable ▾	20	60	1000
5	Disable ▾	20	60	1000
6	Disable ▾	20	60	1000
7	Disable ▾	20	60	1000
8	Disable ▾	20	60	1000

Note: The timer unit is centisecond.

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:

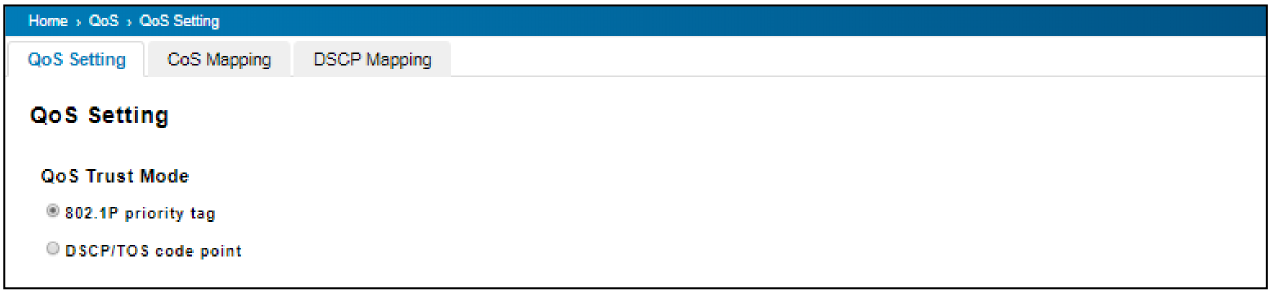
TERMS	DESCRIPTION
GVRP Protocol	**Default: Disable** Allow user to enable / disable GVRP function globally.
State	**Default: Disable** After enable GVRP globally, here still can enable/disable GVRP by port.
Join Timer	**Default: 20** Controls the interval of sending the GVRP Join BPDU. An instance of 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 from the switch to provide different priority to different applications, users or data flows, or to guarantee a certain level of performance to a data flow. QoS guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications. QoS can also help to reduce traffic problems and control the traffic by deliver the high priority first. This section allows User to configure Quality of Service settings for each port by configure the priorities in order to provide a smooth data traffic.

3.6.1 QoS SETTING

The figure below shows QoS Setting.



QoS Setting

QoS Trust Mode

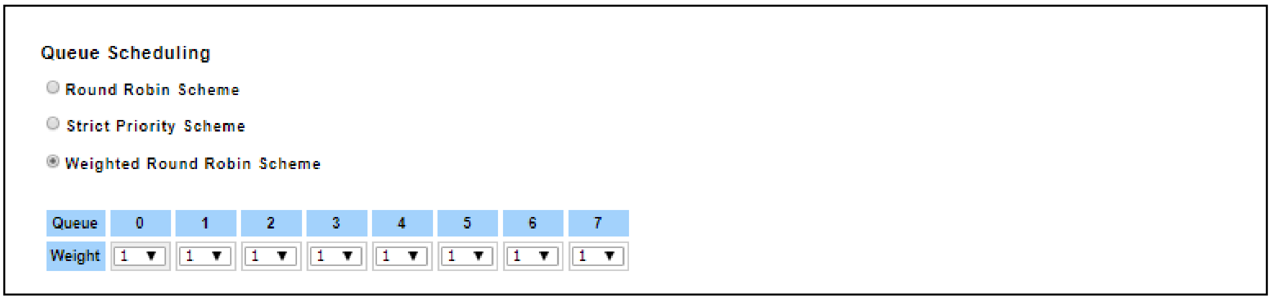
● 802.1P priority tag

○ DSCP/TOS code point

QoS Trust Mode

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

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



Queue Scheduling

○ Round Robin Scheme

○ Strict Priority Scheme

● Weighted Round Robin Scheme

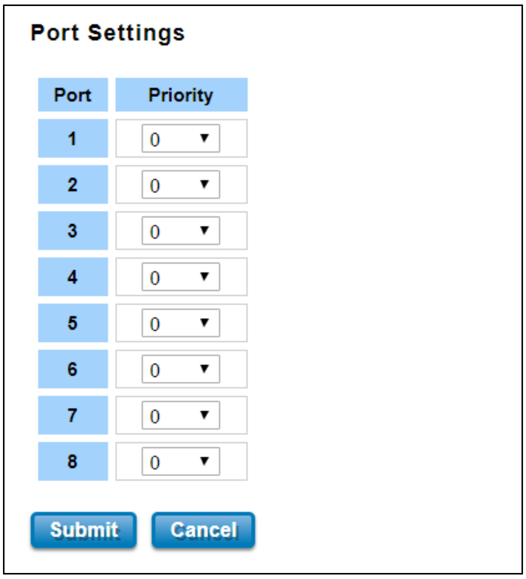
Queue	0	1	2	3	4	5	6	7
Weight	1 ▼	1 ▼	1 ▼	1 ▼	1 ▼	1 ▼	1 ▼	1 ▼

Queue Scheduling

User may select the Queue Scheduling rule:

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

Port Setting



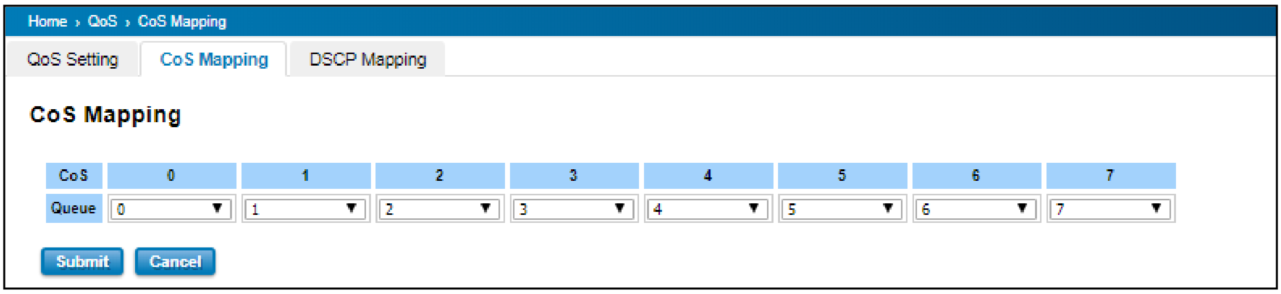
Port Settings

Port	Priority
1	0 ▼
2	0 ▼
3	0 ▼
4	0 ▼
5	0 ▼
6	0 ▼
7	0 ▼
8	0 ▼

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

3.6.2 CoS MAPPING

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



CoS Mapping

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

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

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

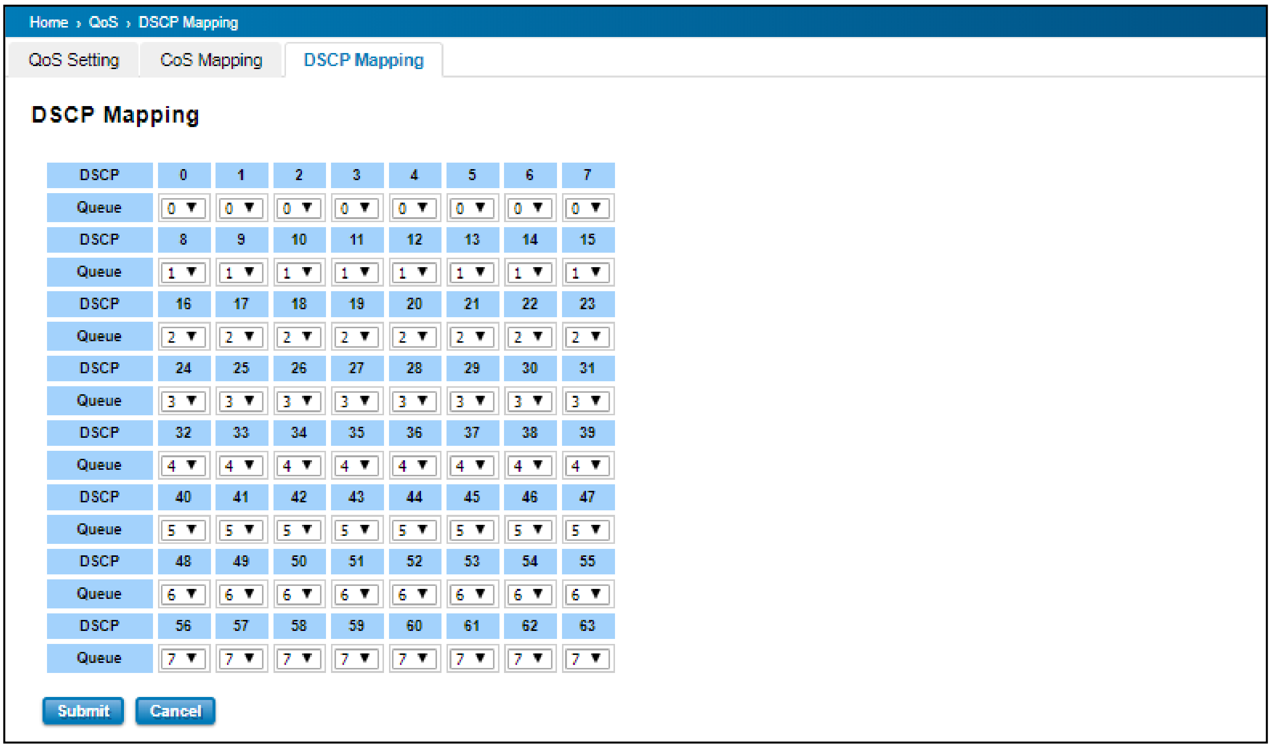
For the step in configuration

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

2. Click the **Submit** button.

3.6.3 DSCP MAPPING

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



DSCP Mapping

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

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

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

3.7 MULTICAST

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

Following sections are included in this group:

3.7.1 IGMP Query

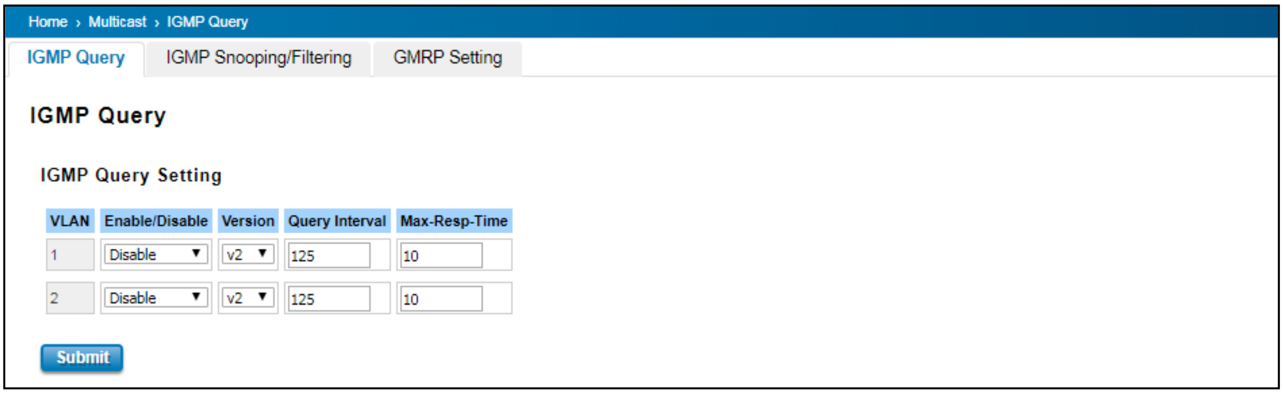
3.7.2 IGMP Snooping

3.7.3 GMRP Setting

3.7.1 IGMP QUERY

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

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



IGMP Query

IGMP Query Setting

VLAN	Enable/Disable	Version	Query Interval	Max-Resp-Time
1	Disable	v2	125	10
2	Disable	v2	125	10

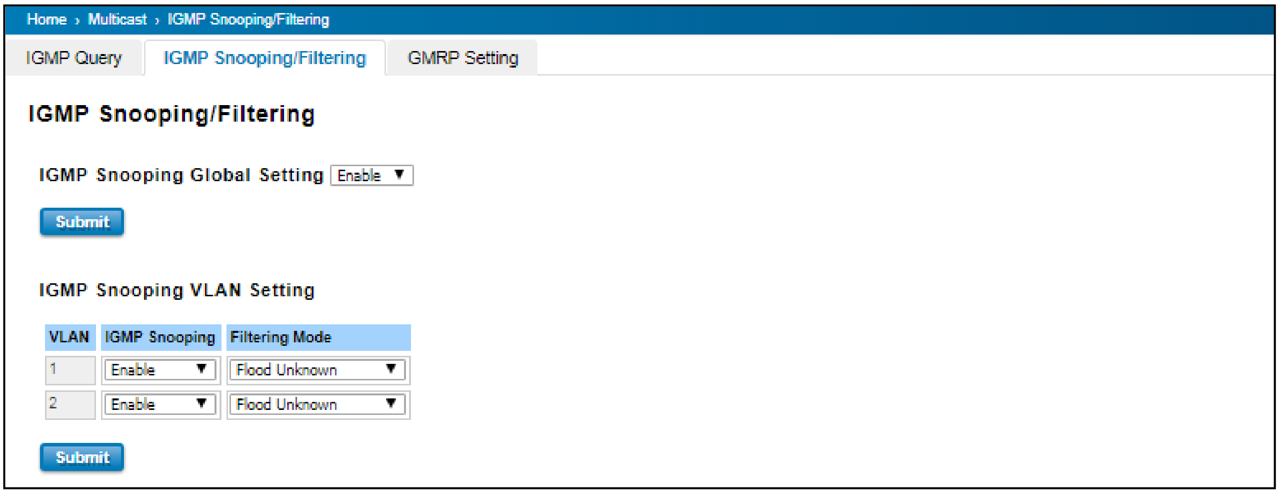
For networks with more than one IGMP querier, a switch with the lowest IP address becomes the IGMP querier.

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 interval period of querier to send the query.
Query Maximum Response Time (s)	The response time for querier detects to confirm there are no more directly connected group members on a LAN.

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

3.7.2 IGMP SNOOPING

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



IGMP Snooping/Filtering

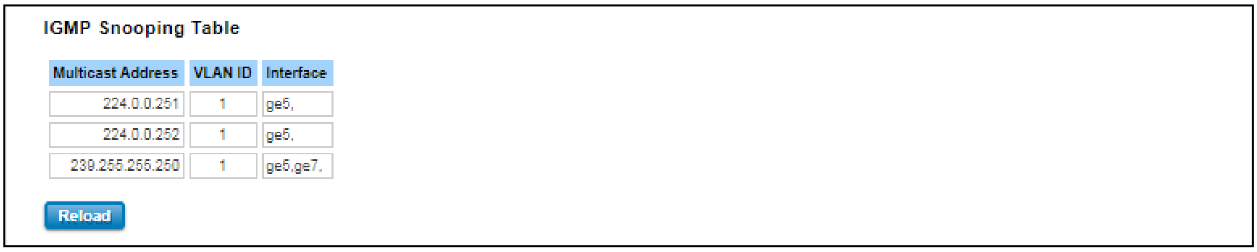
IGMP Snooping Global Setting: Enable

IGMP Snooping VLAN Setting

VLAN	IGMP Snooping	Filtering Mode
1	Enable	Flood Unknown
2	Enable	Flood Unknown

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

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

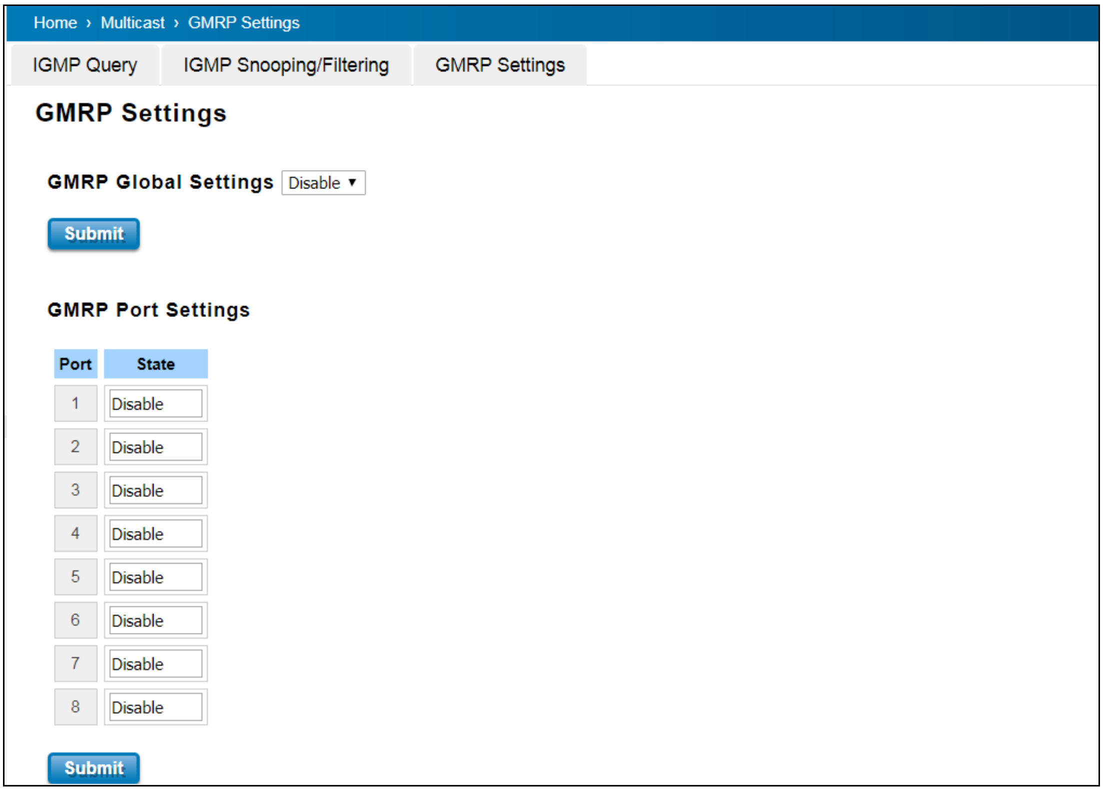


IGMP Snooping Table

Multicast Address	VLAN ID	Interface
224.0.0.251	1	ge5,
224.0.0.252	1	ge5,
239.255.255.250	1	ge5,ge7,

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.



GMRP Settings

GMRP Global Settings: Disable ▾

GMRP Port Settings

Port	State
1	Disable
2	Disable
3	Disable
4	Disable
5	Disable
6	Disable
7	Disable
8	Disable

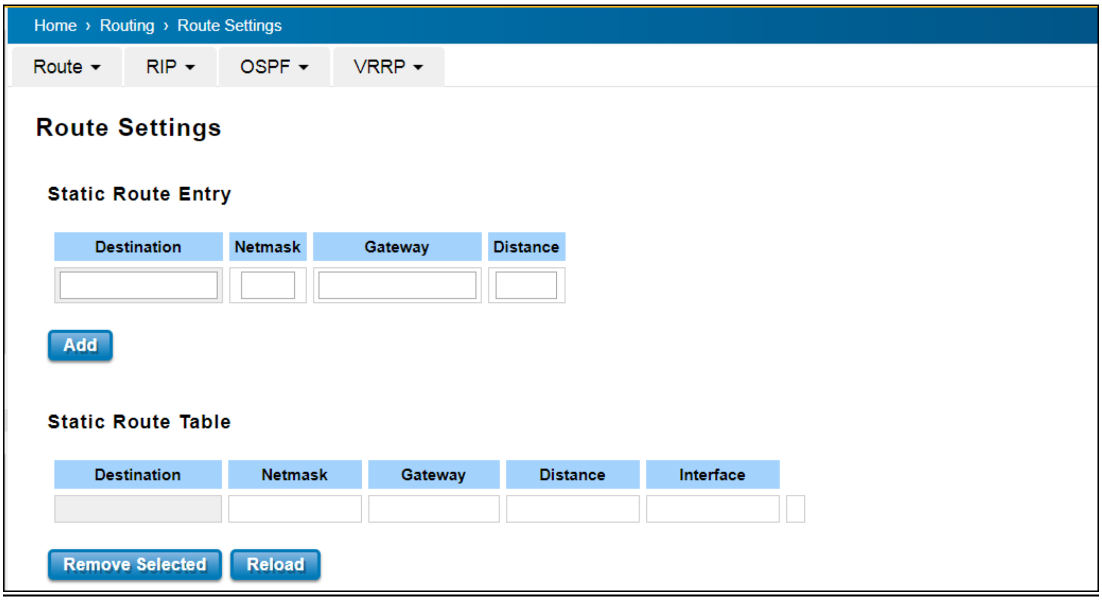
3.8 ROUTING

Routing Feature is the most important feature of the Layer 3 Switch. Layer 3 routing feature is requested since the hosts located in different broadcast domain can't communicate each other, once there is a need to communicate among the different VLANs. WoMaster Switch combines Layer 2 switching and Layer 3 routing within the single platform. In the Routing Configuration pages allows users create the Routing Interfaces, enable routing capability, enable unicast/multicast routing protocols, configure router redundancy policy and check the related routing information.

3.8.1 ROUTE

This configuration page allowed user to configure the route entry and display the route table.

<u>Static Route Entry Setting</u>



Static Route Entry

Static route entries go to and go from a stub network to another stub network. The static route is usually configured to connect the neighbor router/switch; the both routers/switches then can communicate through the route. While configuring Static Route, all the fields in Route entry like the destination network and its netmask, the valid route interface to the destination and distance are needed to be specified.

TERMS	DESCRIPTION
Destination	The destination address of static route entry.
Netmask	The destination address netmask of static route entry.
Gateway	The gateway IP address of static route entry.
Distance	The distance of static route entry.

Click the **Add** button to add a static route entry.

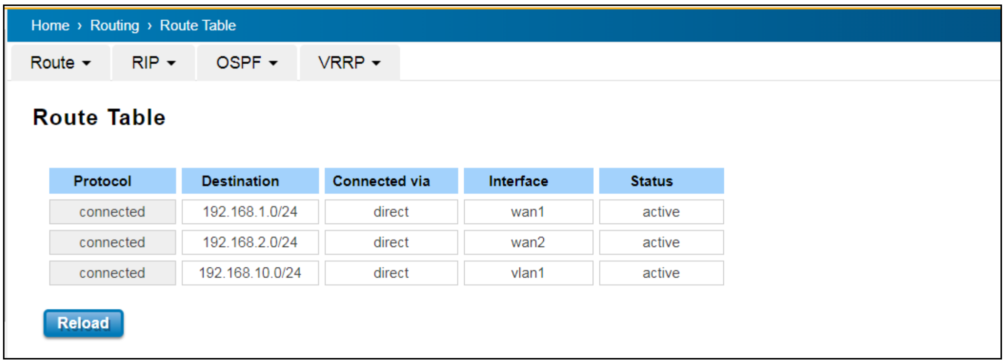
Static Route Table

This table displays the routing table information after user adds the static route entry form.

TERMS	DESCRIPTION
Destination	The destination address of static route entry.
Netmask	The destination address netmask of static route entry.
Gateway	The gateway IP address of static route entry.
Distance	The distance of static route entry.
Metric	The metric of static route entry.
Interface	The IP interface of static route entry.

Click the **Remove Selected** button to remove selected route entry. Click the **Reload** button to reload Route Entry Table information.

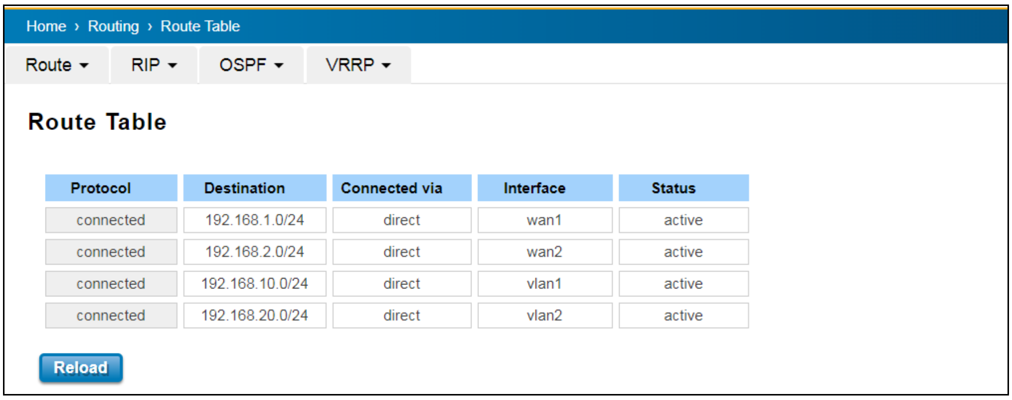
Route Table



Route Table

Protocol	Destination	Connected via	Interface	Status
connected	192.168.1.0/24	direct	wan1	active
connected	192.168.2.0/24	direct	wan2	active
connected	192.168.10.0/24	direct	vlan1	active

DRS610 has 3 interfaces in default, WAN1, WAN2 and the VLAN 1 for LAN ports. In Route table, you can see “direct” in “Connected via” field, the direct means direct interface or local interface.



Route Table

Protocol	Destination	Connected via	Interface	Status
connected	192.168.1.0/24	direct	wan1	active
connected	192.168.2.0/24	direct	wan2	active
connected	192.168.10.0/24	direct	vlan1	active
connected	192.168.20.0/24	direct	vlan2	active

Once user adds new VLAN and assign IP address to it, the new “Direct” interface of that VLAN is added, for example the VLAN 2 in above screen. The new VLAN can be added in VLAN setting (Ch. 3.5, Home->VLAN), the IP address of new VLAN can be configured in Network setting (Ch. 3.1.3, Home ->System ->Network Settings). The status of the new VLAN is “active” in default and the two VLAN interfaces in LAN can be routed.

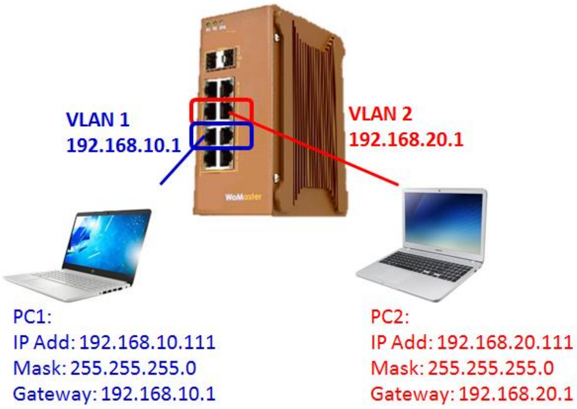
Once the routing interfaces changed, the system maintains information and updates the routing table. It is important to find out the possible and best route in the field especially when troubleshooting the network problem.

The description of the Route Table is as below:

TERMS	DESCRIPTION
Protocol	The field shows the entry is a local interface or learnt from the routing protocol. The **connected** represents for the local interface. The **OSPF** shows the entry is learnt from the routing protocol, OSPF.
Destination	The destination address of static route entry.
Connected via	The IP interface wherever the network learnt from. The interface is usually the next hop’s IP address. **Direct:** The local interface. DRS610 has WAN1, WAN2 and LAN in default.
Interface	Show the VLAN Interface wherever the network connected to or learnt from.
Status	Shows the entry status is active or not. The status of the interface must be in “active” status while running routing process.

3.8.1.1 VLAN Routing Example

Following is the example to create Inter-VLAN Routing between the VLAN 1 and VLAN 2.

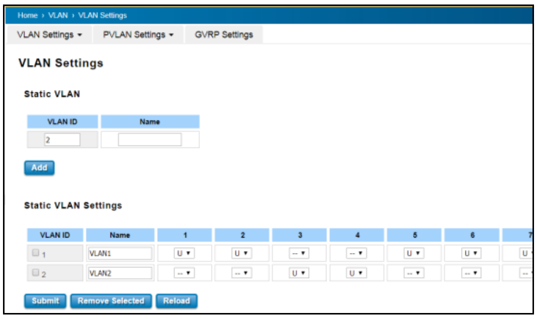


1. Add New VLAN 2 and assign member port 3 and port 4 to the VLAN:

   Type VLAN ID 2 in Static VLAN, click “Add”

   Select the member ports (port 3⁄4) and egress mode “U(Untag)” for connected PC.

   Assign PVID to member ports (port 3⁄4) to 2 in VLAN Port Settings.



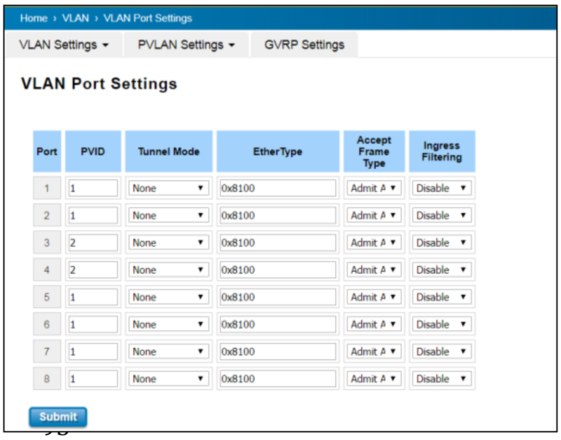
VLAN Settings

Static VLAN

VLAN ID	Name
2	

Static VLAN Settings

VLAN ID	Name	1	2	3	4	5	6	7
□ 1	VLAN1	U ▾	U ▾	-- ▾	-- ▾	U ▾	U ▾	U
□ 2	VLAN2	-- ▾	-- ▾	U ▾	U ▾	-- ▾	-- ▾	--

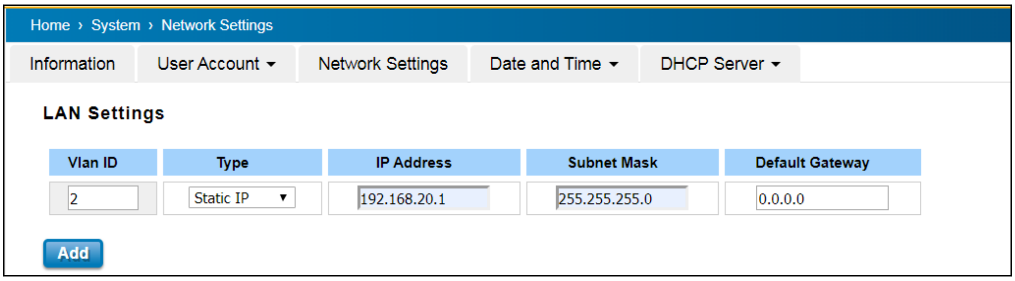


VLAN Port Settings

Port	PVID	Tunnel Mode	EtherType	Accept Frame Type	Ingress Filtering
1	1	None ▾	0x8100	Admit A ▾	Disable ▾
2	1	None ▾	0x8100	Admit A ▾	Disable ▾
3	2	None ▾	0x8100	Admit A ▾	Disable ▾
4	2	None ▾	0x8100	Admit A ▾	Disable ▾
5	1	None ▾	0x8100	Admit A ▾	Disable ▾
6	1	None ▾	0x8100	Admit A ▾	Disable ▾
7	1	None ▾	0x8100	Admit A ▾	Disable ▾
8	1	None ▾	0x8100	Admit A ▾	Disable ▾

2. New VLAN interface setting in System -> Network Setting - LAN Setting.

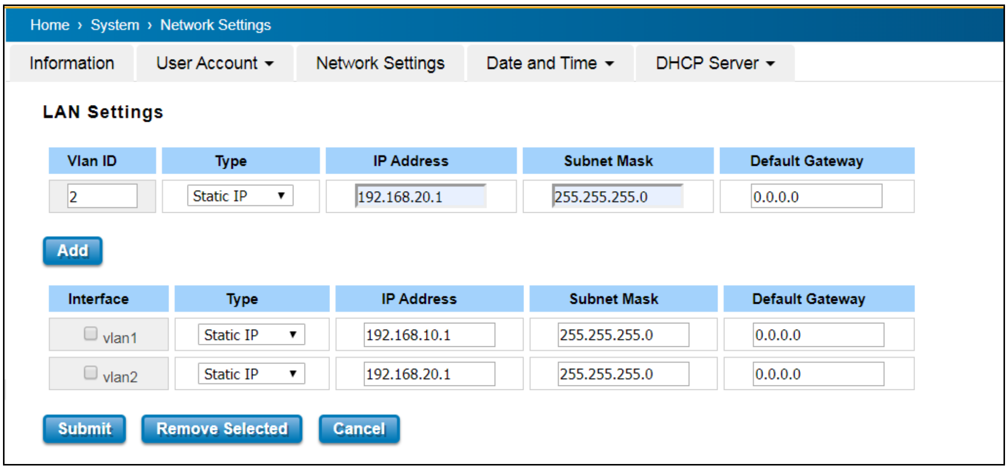
   Assign IP Address 192.168.20.1 to New VLAN interface, VLAN ID is 2. The click **“Add”**.



LAN Settings

Vlan ID	Type	IP Address	Subnet Mask	Default Gateway
2	Static IP	192.168.20.1	255.255.255.0	0.0.0.0

   After Added, you can find new VLAN 2 interface is created.

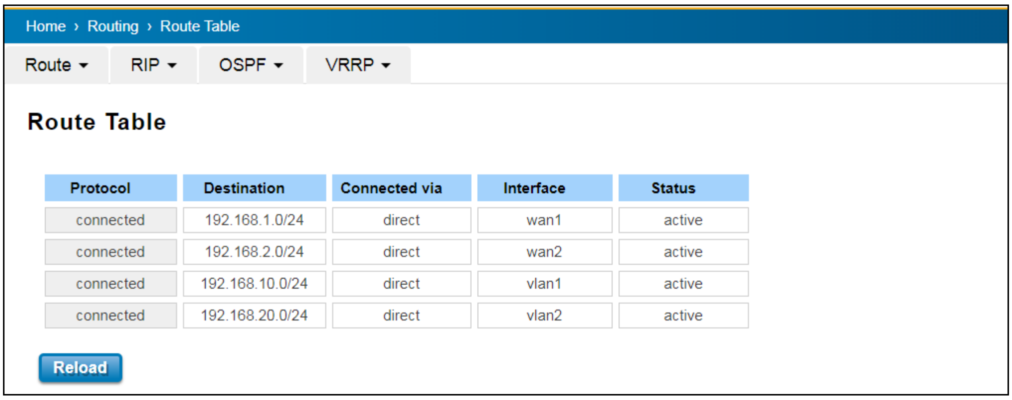


LAN Settings

Vlan ID	Type	IP Address	Subnet Mask	Default Gateway
2	Static IP	192.168.20.1	255.255.255.0	0.0.0.0

Interface	Type	IP Address	Subnet Mask	Default Gateway
□ vlan1	Static IP	192.168.10.1	255.255.255.0	0.0.0.0
□ vlan2	Static IP	192.168.20.1	255.255.255.0	0.0.0.0

3. Check Route Table in Routing -> Route Table. The VLAN 2 interface is created and status is **“active”**.



Route Table

Protocol	Destination	Connected via	Interface	Status
connected	192.168.1.0/24	direct	wan1	active
connected	192.168.2.0/24	direct	wan2	active
connected	192.168.10.0/24	direct	vlan1	active
connected	192.168.20.0/24	direct	vlan2	active

4. Ping Test to check the Inter-VLAN Routing between the two VLAN interfaces.

   Connect PC1 to VLAN 1. Configure PC1 IP Address “192.168.10.x”, mask 255.255.255.0(24 bit) and the default gateway is “192.168.10.1”.

   Connect PC2 to VLAN 2. Configure PC2 IP Address “192.168.20.x”, mask 255.255.255.0(24 bit) and the default gateway is “192.168.20.1”.

   PC 1 and PC 2 Ping their default gateway to check the setting and link is correctly first.

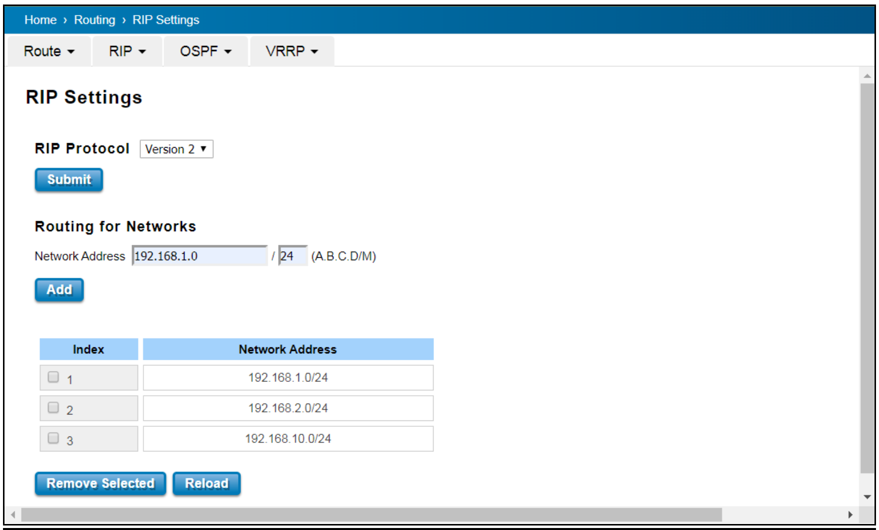
   PC 1/PC 2 Ping with each other to check the VLAN Routing is workable.

5. The above example can be applied to LAN to WAN routing. Make sure the connected PC’s IP address, mask and default gateway are correctly configured and the PC connects to correct interface.

3.8.2 RIP

The Industrial L3 managed switch also implements a dynamic routing protocol to allow automatically learning and updating of routing table. In this subsection, one of the dynamic routing protocols can be setup by the users. Routing Information Protocol (RIP) is a distance vector-based routing protocol that can make decision on which interface the L3 managed switch should forward Internet Protocol (IP) packet and can share information about how to route traffic among network devices that use the same routing protocol. RIP sends routing-update messages periodically every 30 seconds and when there is a change in network topology. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. RIP can also be used to automatically build up a routing table.

RIP Setting



RIP Settings

RIP Protocol: Version 2 ▾

Routing for Networks

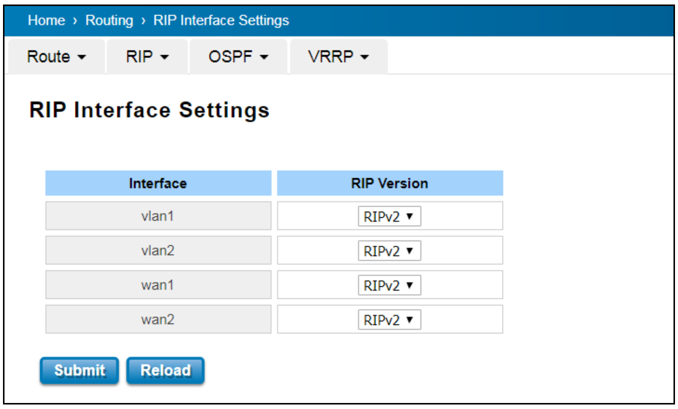
Network Address 192.168.1.0 / 24 (A.B.C.D/M)

Index	Network Address
□ 1	192.168.1.0/24
□ 2	192.168.2.0/24
□ 3	192.168.10.0/24

TERMS	DESCRIPTION
RIP Protocol	Choose the RIP protocol **Version 1** or **Version 2** or **Disable** RIP protocol in here. Click the **Submit** button to apply RIP protocol setting.
Routing for Networks	All the networks no matter directly connected or learnt from other router/switch should be added to the switch. The format is IP Network/bit mask. For example, 192.168.10.0/24. (24 = 255.255.255.0) Type the IP network of WAN interface can active WAN port. For example, 192.168.1.0/24, the IP of WAN1, that can active WAN 1 interface for RIP. After type the network address, click the **Add** to add a routing network.

Click the **Add** button to add a routing network. Click the **Remove Selected** button to remove selected network address. Click the **Reload** button to reload RIP information.

RIP Interface Setting



RIP Interface Settings

Interface	RIP Version
vlan1	RIPv2 ▾
vlan2	RIPv2 ▾
wan1	RIPv2 ▾
wan2	RIPv2 ▾

TERMS	DESCRIPTION
Interface	The created interface ID, include WAN1, WAN2 and VLAN IDs.
RIP Version	RIP version of IP interface. (RIPv1, RIPv2 and Both)

Click the **Submit** button to apply RIP interface settings. Click the **Reload** button to reload RIP interface configuration.

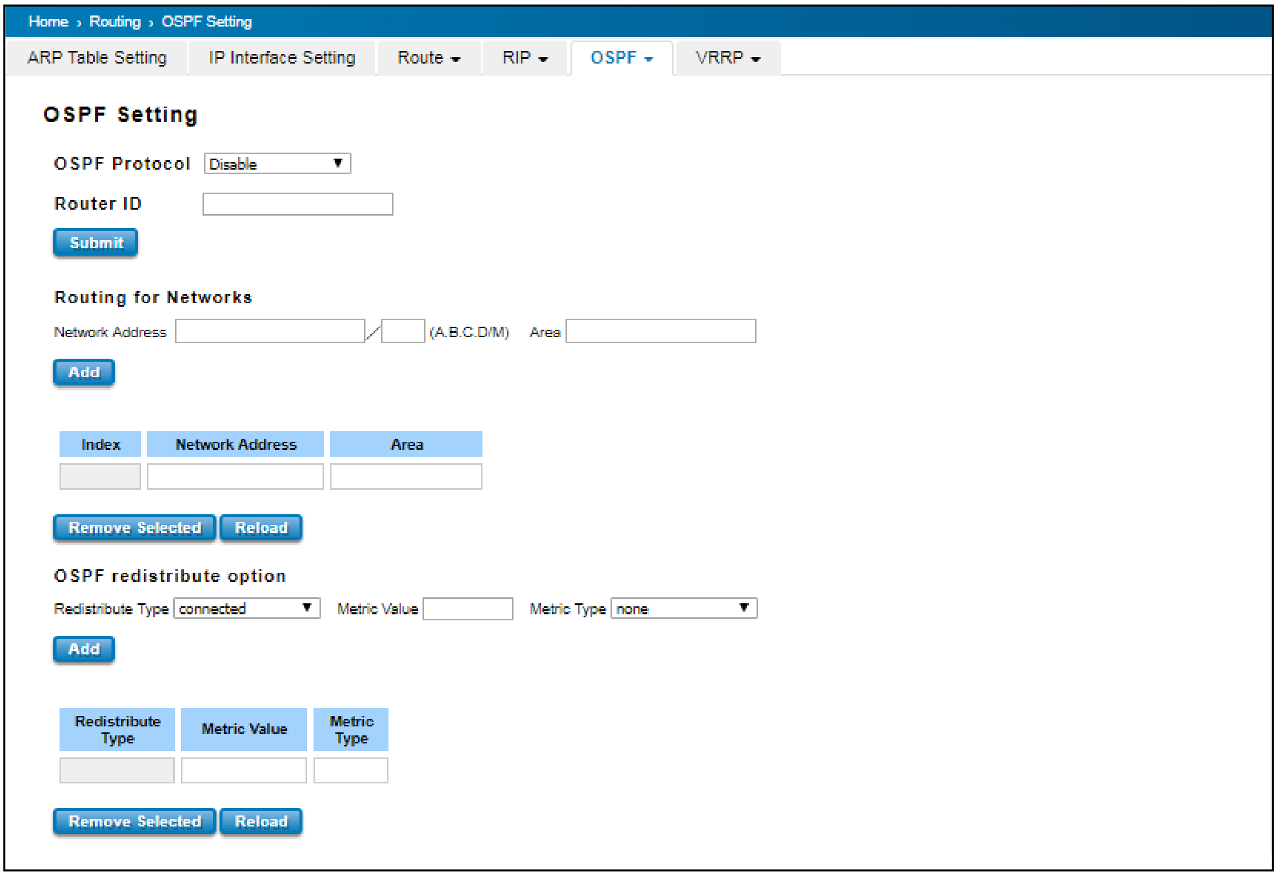
3.8.3 OSPF

Open Shortest Path First is a link-state protocol that equips the IP, mask, the type of network, the routers connected to that network. The State is its relationship to its neighboring routers. The Metric is the distance between the 2 links; it is usually the bandwidth of the link in link-state protocol. The Link State Database is the collection of all these link states. The destination network address, the shortest metric to the network and the IP address of the next hop are specified in the link state database. It propagates link-state advertisements (LSAs) to its neighbor switches. When compared with RIP (Routing Information Protocol) which is a distance vector based routing protocol, OSPF can provide scalable network support and faster convergence time for network routing state. OSPF is widely used in large networks such as ISP (Internet Service Provider) backbone and enterprise networks.

The OSPF is a complex protocol which defines the role of the router/switch when it is installed in different Areas. The Area is a group of routers, the OSPF uses flooding to exchange link-state updates between routers. The routers within the same area update its routing table. Any change in routing information is flooded to all routers in the same area

WoMaster Layer3 Managed Switch design comforts to the OSPF Version 2 specification. Typically, the switch acts as the Internal Router, a router within the area; the Designated Router, the Master router in the same broadcast domain within the area; the Area Board Router which is the boundary router between different area. While configuring the OSPF network, the area ID should be configured with the same IP address or the same area ID.

OSPF Setting



OSPF Setting

OSPF Protocol: Disable ▼

Router ID:

Submit

Routing for Networks

Network Address: / (A.B.C.D/M) Area:

Add

Index	Network Address	Area

Remove Selected | Reload

OSPF redistribute option

Redistribute Type: connected ▼ Metric Value: Metric Type: none ▼

Add

Redistribute Type	Metric Value	Metric Type

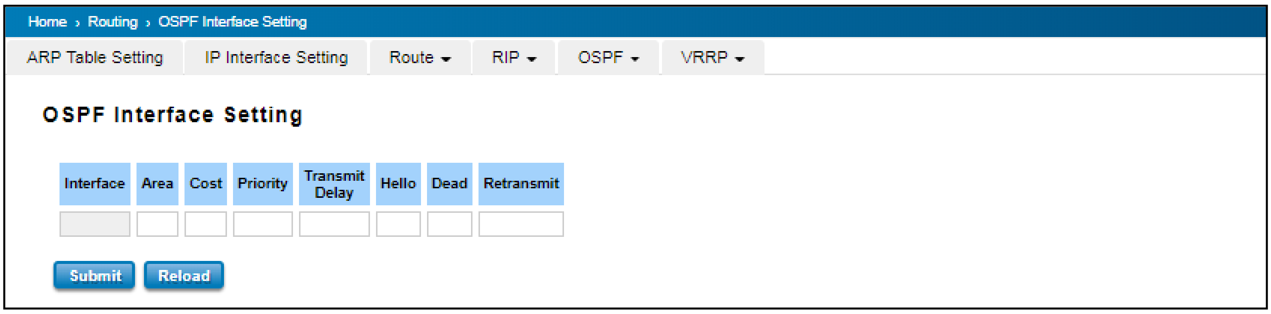
Remove Selected | Reload

TERMS	DESCRIPTION
OSPF Protocol	**Enable** or **Disable** the OSFP routing protocol.
Router ID	The router ID can be any IP address, however, the IP address of the existed local interface is suggested. With such IP address, you can find the router/switch easier. Router ID is used while connected multiple OSPF routers/switches to the same broadcast domain, the lowest Router ID will be selected as the Designated Router in the network.
Routing for Network	Type the **Network Address** and the **Area** ID in the field.

Click **Add** to apply the setting then the new entry will appear in the network table below. Click the **Remove** Selected button to remove the selected network. Click the **Reload** button to reload the table.

> NOTE: All the Area ID of the router/switch within the same area should use the same IP address or ID. All the network address should be added.

OSPF Interface Setting



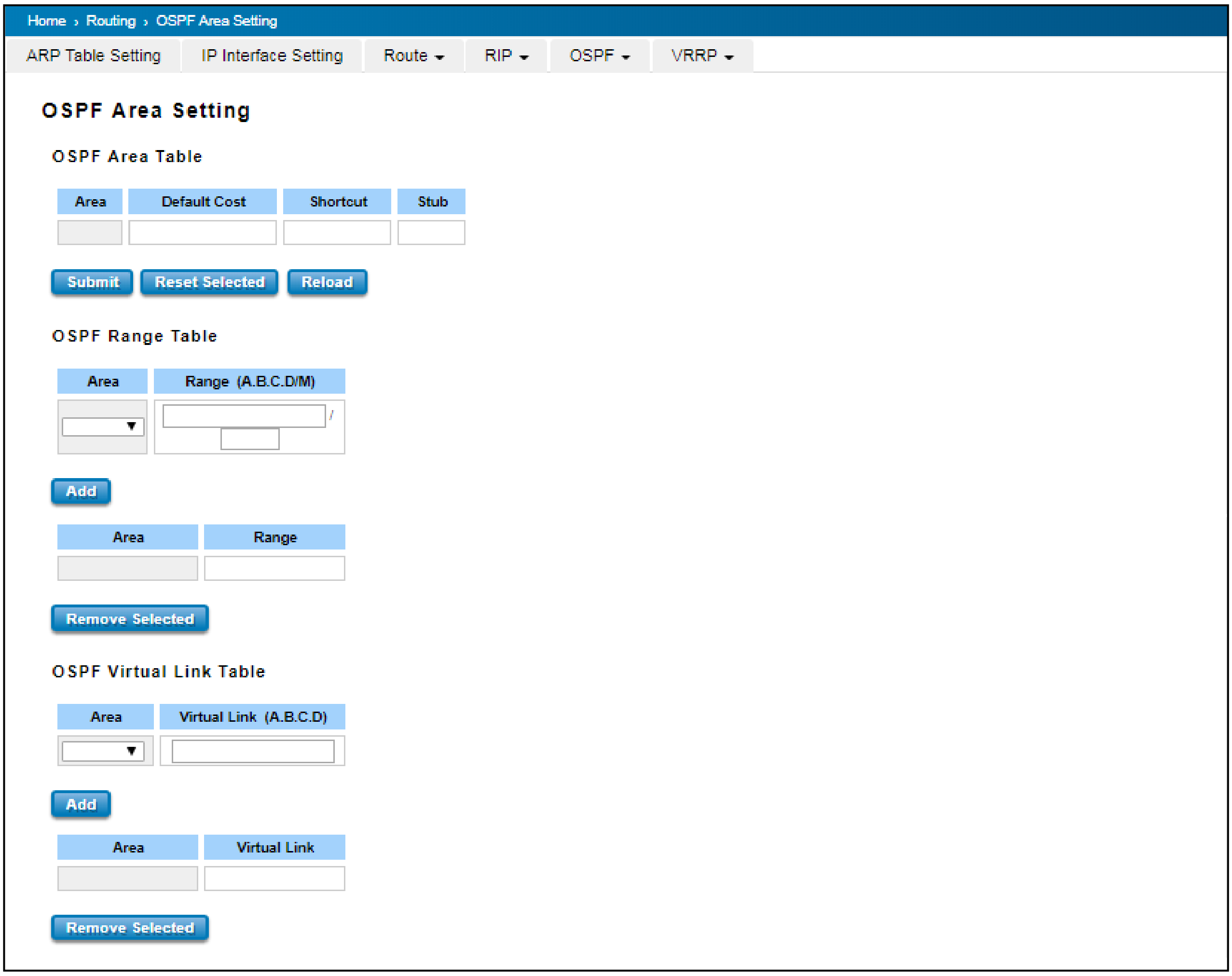
TERMS	DESCRIPTION
Interface	The VLAN Interface name.
Area	The area ID of the Interface you added. The Area ID must be the same for all routers/switches on a network.
Cost	The distance of this link/Interface, the default is identified depends on what the bandwidth is by the system. The value can be changed to decide the best router.
Priority	The priority of this link/Interface. Set priority to help find the OSPF designated router for a network. The default is 1. The range is 0 to 255.
Transmit Delay	The transmit delay timer of this link/Interface. Transmit Delay is the estimated number of seconds to wait before sending a link state update packet. The default value is 1 second.
Hello	The Hello timer of this link/Interface. The value must be the same for all routers/switches on a network. The default value is 10 seconds. The min. value is 1.
Dead	The Dead Interval Timer of this link/Interface. The Dead timer is the time to

	identify whether the interface is down or not before the neighbors declare the OSPF router to be down. The default value is 4 times (40 seconds) than the Hello interval (default is 10).
Retransmit	The count of Retransmit of this link/Interface. The Retransmit time specifies the number of seconds between link state advertisement transmissions. The default value is 5 seconds.

Once finish configuring the settings, click on **Apply** to apply configuration.

OSPF Area Setting

This page allows user to configure the OSPF Area information. An OSPF domain is divided into different areas. Areas are logical grouping of hosts and networks, including their routers having interfaces connected to any of the included networks. Each area maintains its own link state database. In OSPF, all areas must be connected to a backbone area. The backbone area is responsible for distributing routing information between non-backbone areas. The WoMaster Switch is usually installed as internal router of a single Area environment. While there are multiple areas in the network, this page allows modify the Area information and Virtual Link.

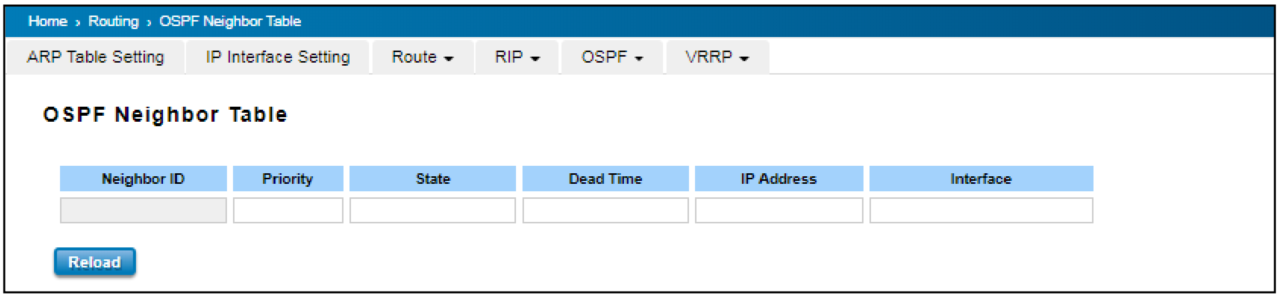


TERMS	DESCRIPTION
Area	This field indicates the area ID. Select the ID you want to modify here.
Default Cost	The default cost of the area ID.
Shortcut	No Defined, Disable, Enable. This indicates whether the area is the OSPF ABR shortcut mode.
Stub	Represents whether the specified Area is a stub area or not. The possible values are No Defined, No Summary and Summary. Summary is used to advertise summary routes.

Click the **Apply** button to apply OSPF area settings. Click the **Remove Selected** button to remove selected area. Click the **Reload** button to reload OSPF area configurations.

OSPF Neighbor Table

This page allows user to see the OSPF Neighbor information. The Neighbor interface and its state will be listed here.



OSPF Neighbor Table

Neighbor ID	Priority	State	Dead Time	IP Address	Interface

TERMS	DESCRIPTION
Neighbor ID	Display the Router ID of the Neighbor routers/switches.
Priority	Show the priority of the link.
State	While the **State** is changed to **Full**, which means the exchange progress is done.
Dead Time	The activated time of the link.
IP Address	Shows the learnt IP interface of the next hops.
Interface	Shows the connected local interface.

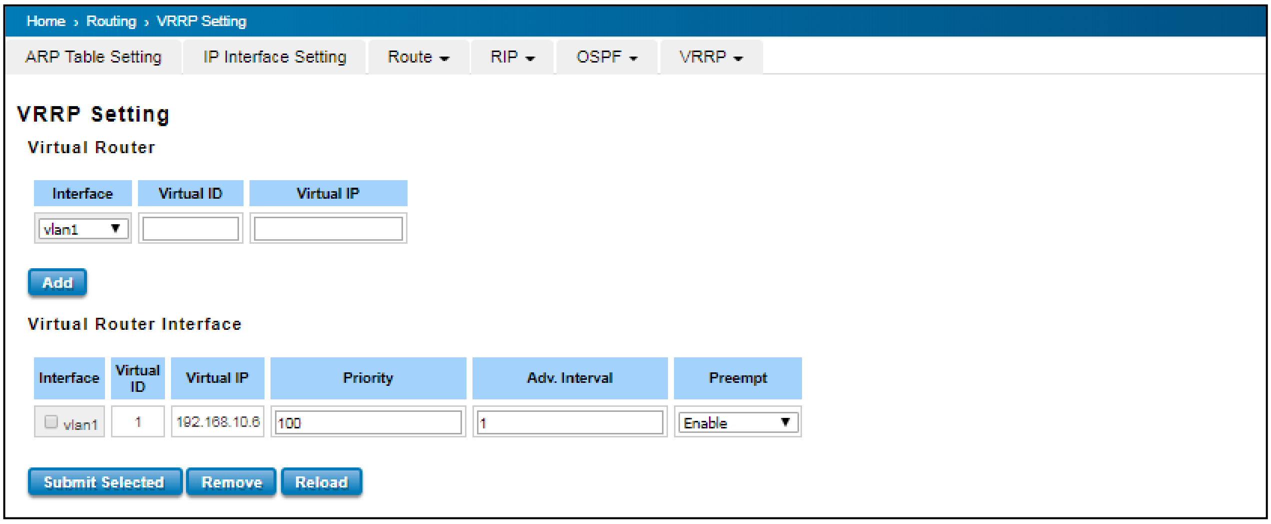
Click **Reload** to update the information from the table.

3.8.4 VRRP

A VRRP (Virtual Router Redundancy Protocol) is a computer networking protocol aimed to eliminate the single point of failure by automatically assigning available IP routers to participating hosts. Using a virtual router ID (VRID) address and virtual router IP (VRIP) address to represent itself, a virtual router consists of two or more physical routers, including one master router and one or more backup routers. All routers in the virtual router group share the same VRID and VRIP. The master router provides primary routing and the backup routers monitor the status of the master router and become active if the master router fails.

VRRP Setting

The fields allow you to create the Virtual Router Interface. All the layer 3 switches within the same VRRP domain should be located within the same IP network and equips with the same Virtual ID and Virtual IP address.



VRRP Setting

Virtual Router

Interface	Virtual ID	Virtual IP
vlan1 ▼		

Virtual Router Interface

Interface	Virtual ID	Virtual IP	Priority	Adv. Interval	Preempt
□ vlan1	1	192.168.10.6	100	1	Enable ▼

Virtual Router

TERMS	DESCRIPTION
Interface	Select the interface for the VRRP domain. The VRRP is applied to VLAN Interface of LAN port in DRS610.
Virtual ID	This is a virtual ID range from 1~255. The switches within the same VRRP domain should have the same Virtual ID.
Virtual IP	This is the virtual IP of the VRRP domain. This is the Gateway IP of the clients.

Click **Add** once finish the configuration. Then a new entry is created in the Virtual Router Interface Configuration page. After the VRRP interface is created, user can see the new entry and adjust the settings to decide the policy of the VRRP domain.

Virtual Router Interface

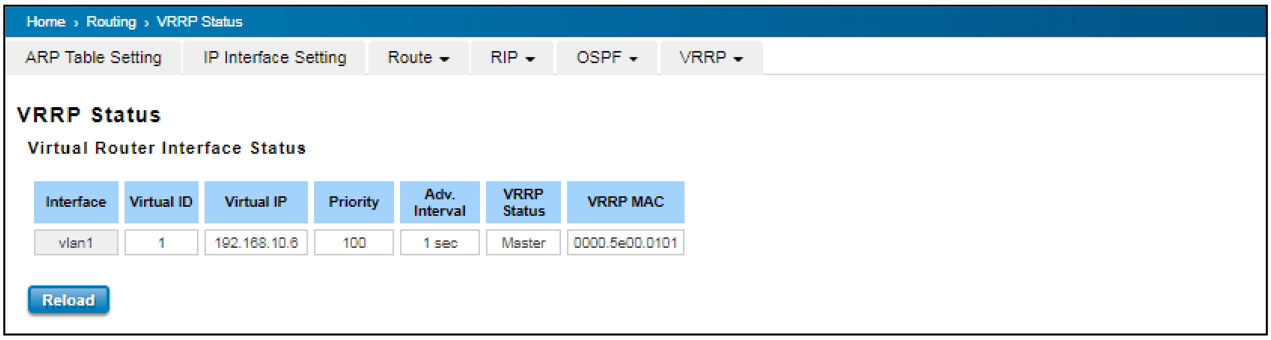
TERMS	DESCRIPTION
Interface	Select the interface for the VRRP domain.
Virtual ID	This is a virtual ID range from 1~255. The switches within the same VRRP domain should have the same Virtual ID.
Virtual IP	This is the virtual IP of the VRRP domain. This is the Gateway IP of the clients.
Priority	The priority of the entry of this switch. In VRRP domain, the VRRP switches must have the same Virtual ID and Virtual IP settings and choose who should be the VRRP Master switch. The switch equips with the highest priority will be selected as the VRRP master. The priority setting field can be manually changed, the range is from 1~254, 255 for virtual IP owner and 100 for backup by default.

Adv. Interval	This field indicates how often the VRRP switches exchange the VRRP settings. Default: 1 sec. The interval time must be the same of all the routes in the same VRRP ID.
Preempt	While the VRRP Master link is failure, the VRRP Backup will take over its job immediately. However, while the VRRP master link is recovered, who should be the Master? The Preempt decide whether the VRRP master should be recovered or not. While the Preempt is **Enable** and the interface is VRRP Master, the interface will be recovered. While the Preempt is **Disable** and the interface is VRRP Master, there is no change while the link is recovered. The VRRP backup acts as the Master before restart the switches.

Click the **Submit Selected** button to apply the configuration. Click the **Remove Selected** button to remove selected setting. Click the **Reload** button to reload table.

VRRP Status

The VRRP represent for the Virtual Router Redundancy Protocol. To further ensure the high reliability of an environment, the Layer 3 switch supports the VRRP protocol allowing the hosts to continuously direct traffic to the default gateway without the default gateway configuration change.



VRRP Status

Virtual Router Interface Status

Interface	Virtual ID	Virtual IP	Priority	Adv. Interval	VRRP Status	VRRP MAC
vlan1	1	192.168.10.6	100	1 sec	Master	0000.5e00.0101

TERMS	DESCRIPTION
Interface	Select the interface for the VRRP domain.
Virtual ID	This is a virtual ID range from 1~255. The switches within the same VRRP domain should have the same Virtual ID.
Virtual IP	This is the virtual IP of the VRRP domain. This is the Gateway IP of the clients.
Priority	The priority of the entry of this switch. In VRRP domain, the VRRP switches must have the same Virtual ID and Virtual IP settings and choose who should be the VRRP Master switch. The switch equips with the highest priority will be selected as the VRRP master. The priority setting field can be manually changed, the range is from 1~254, 255 for virtual IP owner and 100 for backup by default.

Adv. Interval	This field indicates how often the VRRP switches exchange the VRRP settings.
VRRP Status	While the VRRP Master link is failure, the VRRP Backup will take over its job immediately
VRRP MAC	This field indicates the VRRP MAC in this configuration entry.

3.9 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.

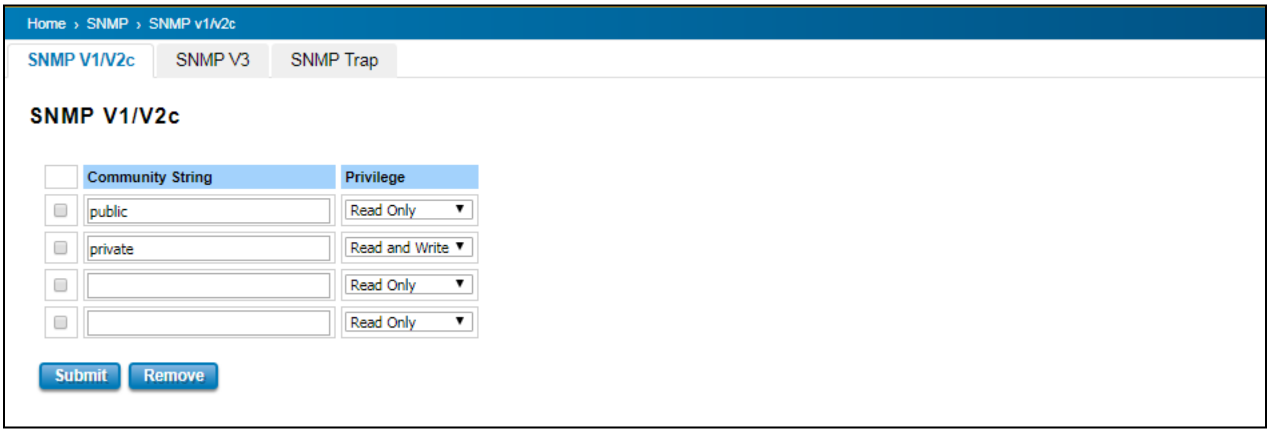
3.9.1 SNMP V1/V2c SETTING

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**.

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

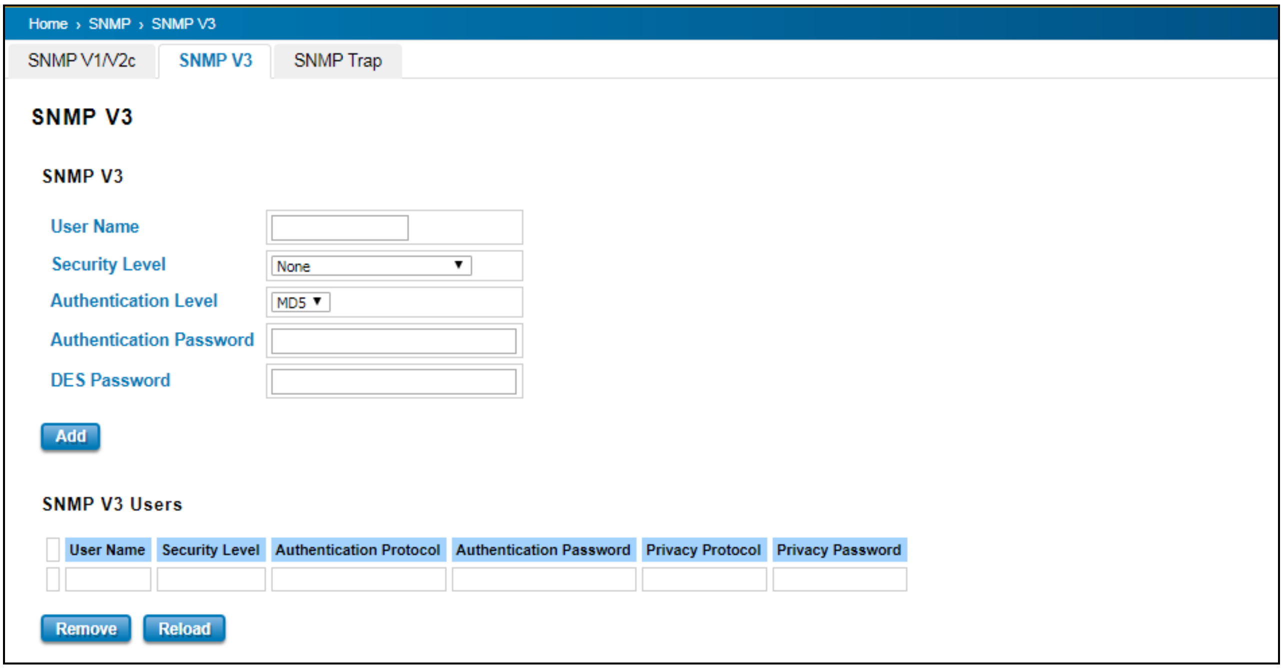


SNMP V1/V2c

	Community String	Privilege
□	public	Read Only
□	private	Read and Write
□		Read Only
□		Read Only

3.9.2 SNMP V3

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



SNMP V3

SNMP V3

User Name	
Security Level	None
Authentication Level	MD5
Authentication Password	
DES Password	

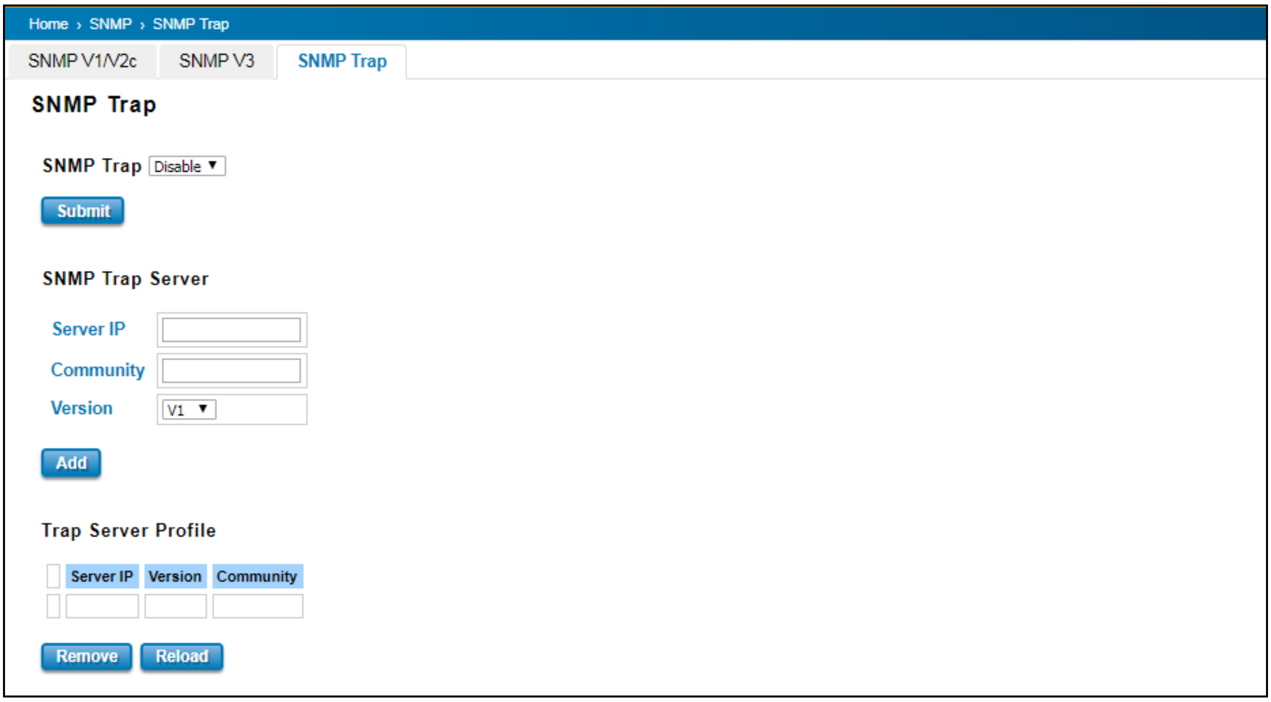
SNMP V3 Users

□	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
□						

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.

3.9.3 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.



SNMP Trap

SNMP Trap: Disable

SNMP Trap Server

Server IP:

Community:

Version: V1

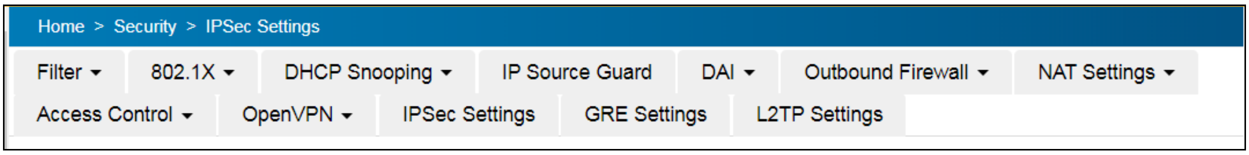
Trap Server Profile

□	Server IP	Version	Community
□			

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.

3.10 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:

3.10.1 Filter

3.10.2 IEEE 802.1X

3.10.3 Access Control

3.10.4 Outbound Firewall

3.10.5 NAT Settings

3.10.6 OpenVPN

3.10.7 IPSec Settings

3.10.8 GRE Settings

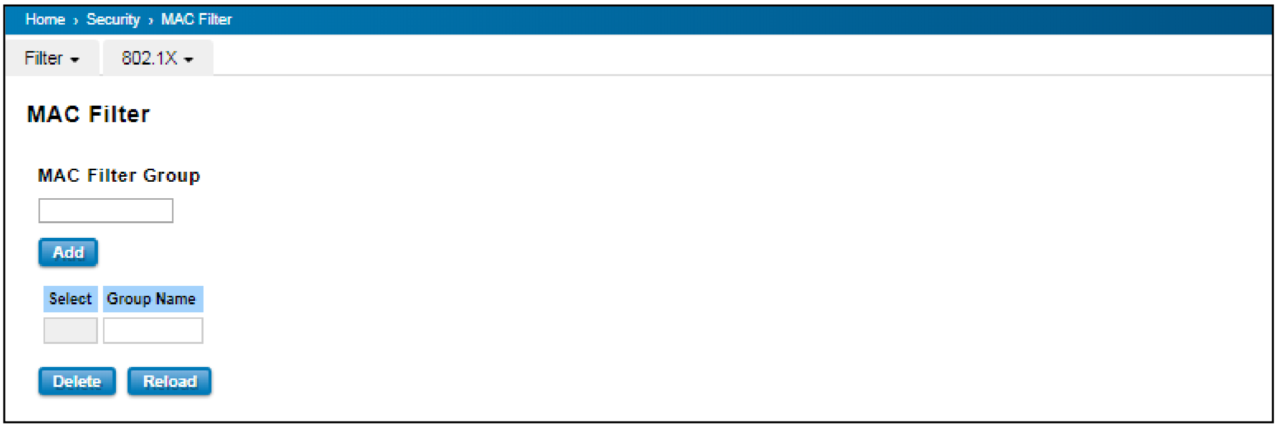
3.10.1 FILTER

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

MAC Filter

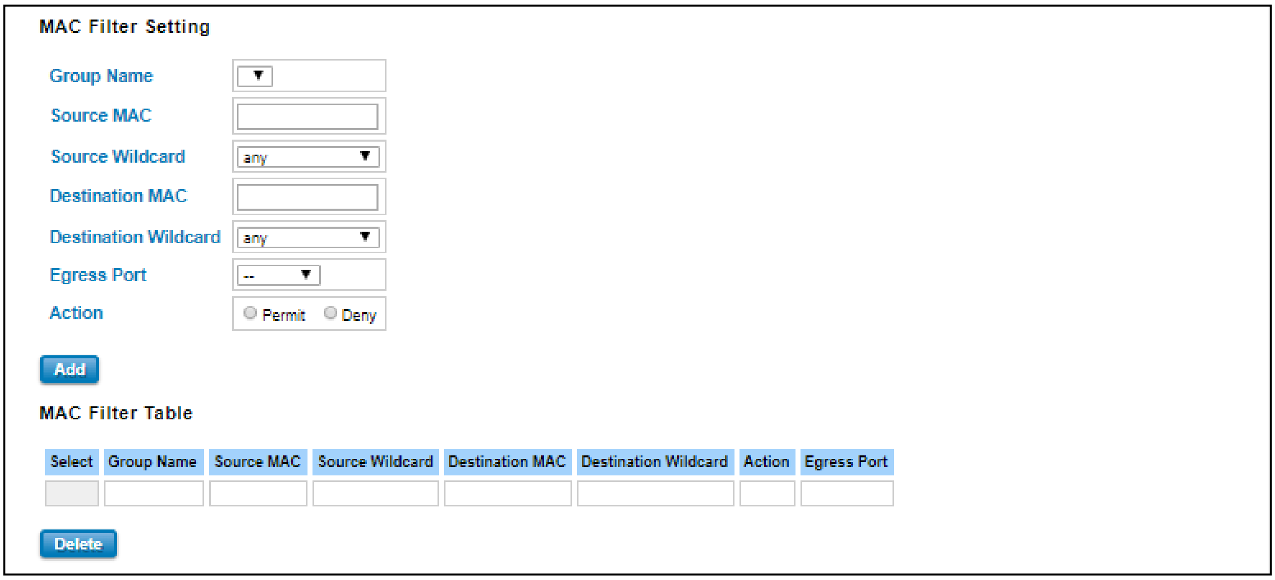
Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. Mac Filter feature allows User to stop the MAC address learning for specific port. After stopping MAC learning, only the MAC address listed in the list can access the switch and transmit/receive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

MAC Filter Group



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

MAC Filter Setting



MAC Filter Setting

Group Name	▼
Source MAC	
Source Wildcard	any ▼
Destination MAC	
Destination Wildcard	any ▼
Egress Port	-- ▼
Action	○ Permit ○ Deny

MAC Filter Table

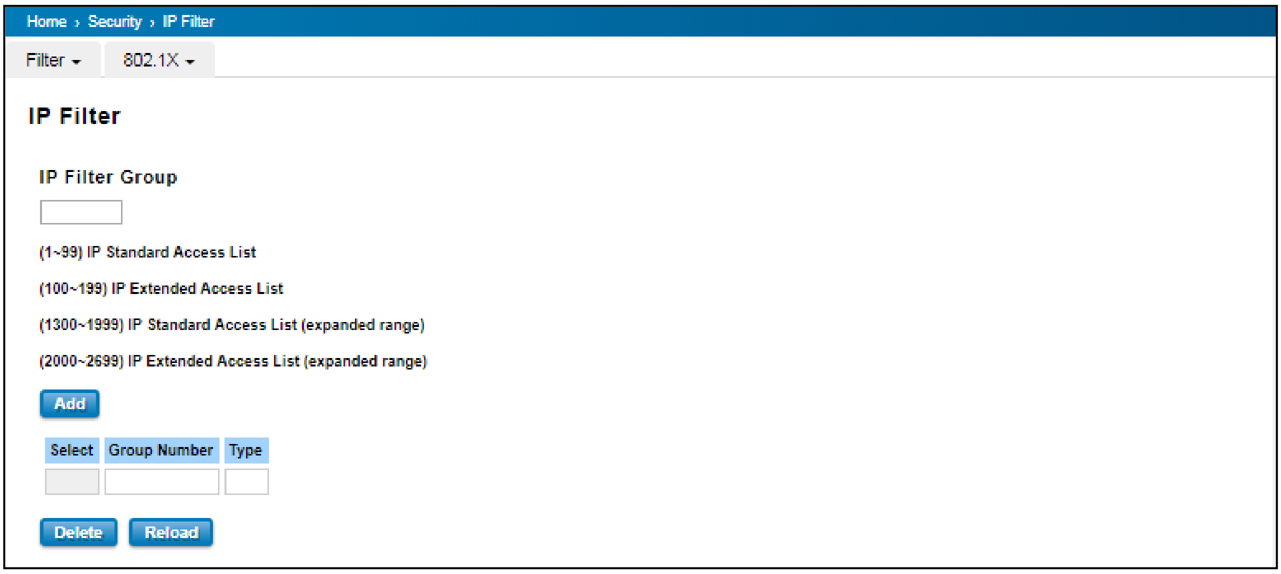
Select	Group Name	Source MAC	Source Wildcard	Destination MAC	Destination Wildcard	Action	Egress Port

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

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

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

IP Filter



IP Filter

IP Filter Group

(1~99) IP Standard Access List

(100~199) IP Extended Access List

(1300~1999) IP Standard Access List (expanded range)

(2000~2699) IP Extended Access List (expanded range)

Select	Group Number	Type

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

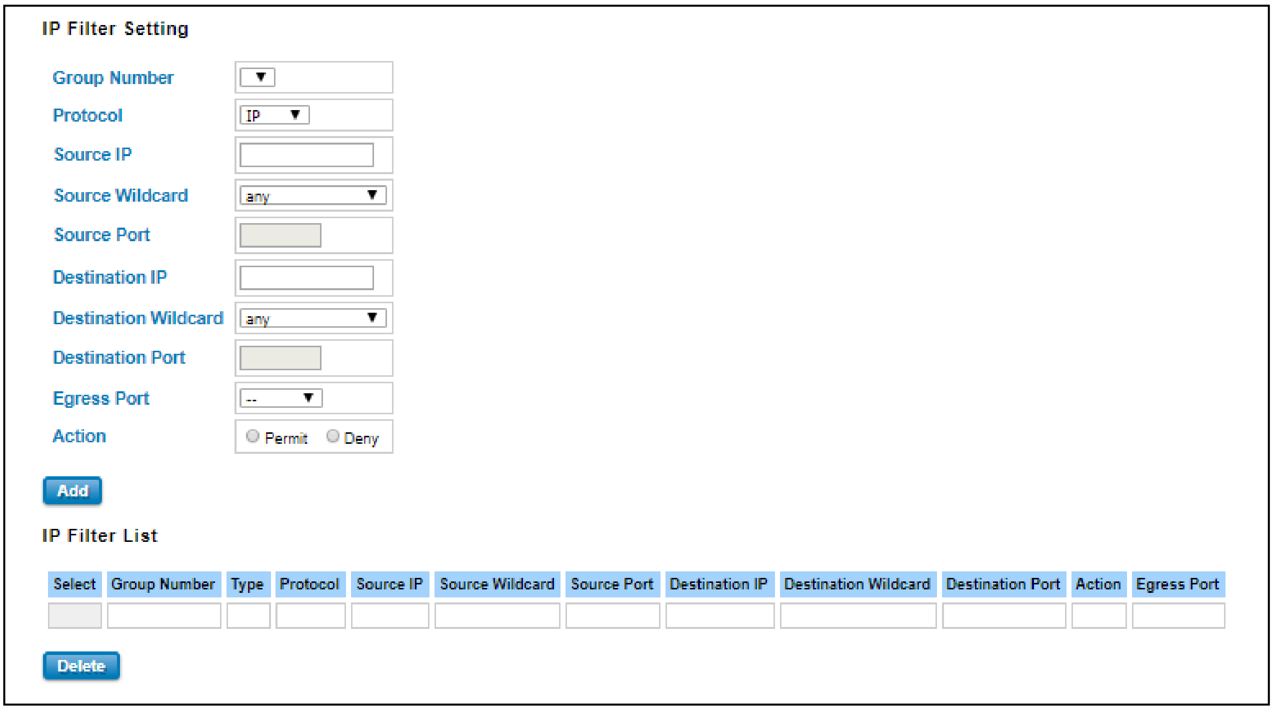
1 - 99: IP Standard Access List

100 – 199: IP Extended Access List

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

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

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



IP Filter Setting

Group Number	
Protocol	IP
Source IP	
Source Wildcard	any
Source Port	
Destination IP	
Destination Wildcard	any
Destination Port	
Egress Port	--
Action	○ Permit ○ Deny

IP Filter List

Select	Group Number	Type	Protocol	Source IP	Source Wildcard	Source Port	Destination IP	Destination Wildcard	Destination Port	Action	Egress Port

IP Filter Setting

TERMS	DESCRIPTION
Group Number	Number of the Filter Group.

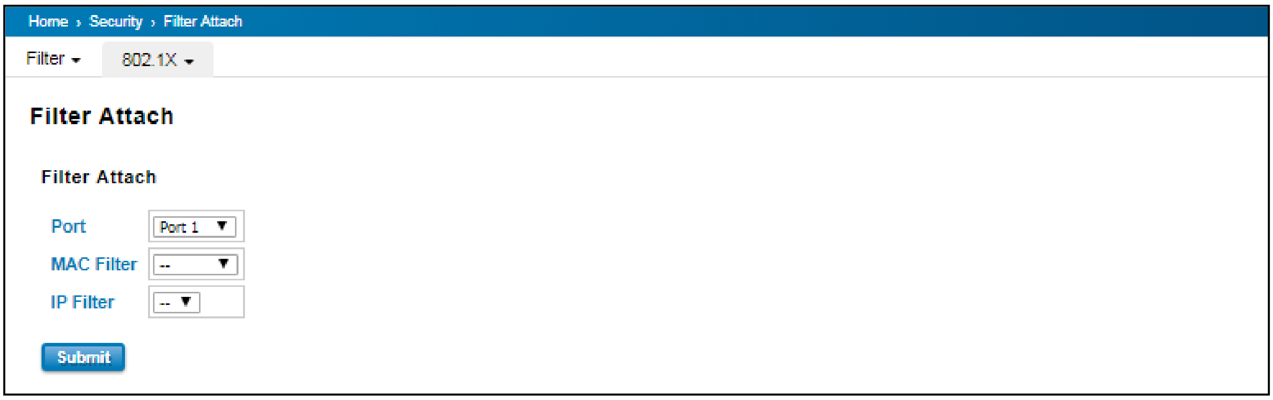
Protocol	This is the L4 protocol (IP/TCP/UDP/ICMP).
Source IP	This is the source IP address of the packet.
Source Wildcard	This is the mask of the IP address.
Source Port	This is the source port of L4 protocol (TCP/UDP)
Destination IP	This is the destination IP address of the packet.
Destination Wildcard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

IP Filter List

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

Filter Attach

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



Filter Attach

Filter Attach

Port: Port 1

MAC Filter: --

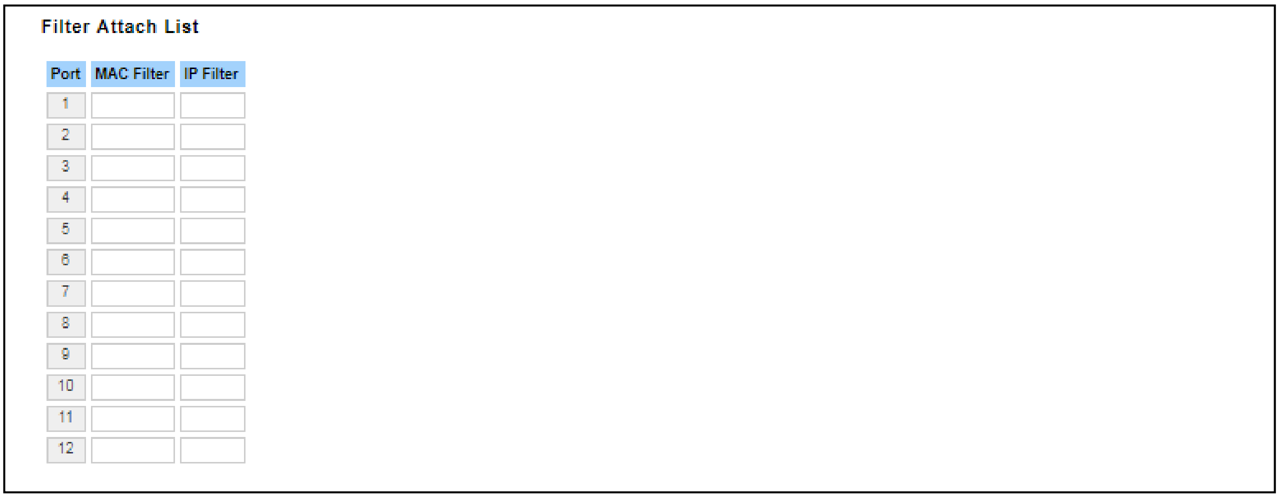
IP Filter: --

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

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

Filter Attach List

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



Filter Attach List

Port	MAC Filter	IP Filter
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

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

3.10.2 IEEE 802.1X

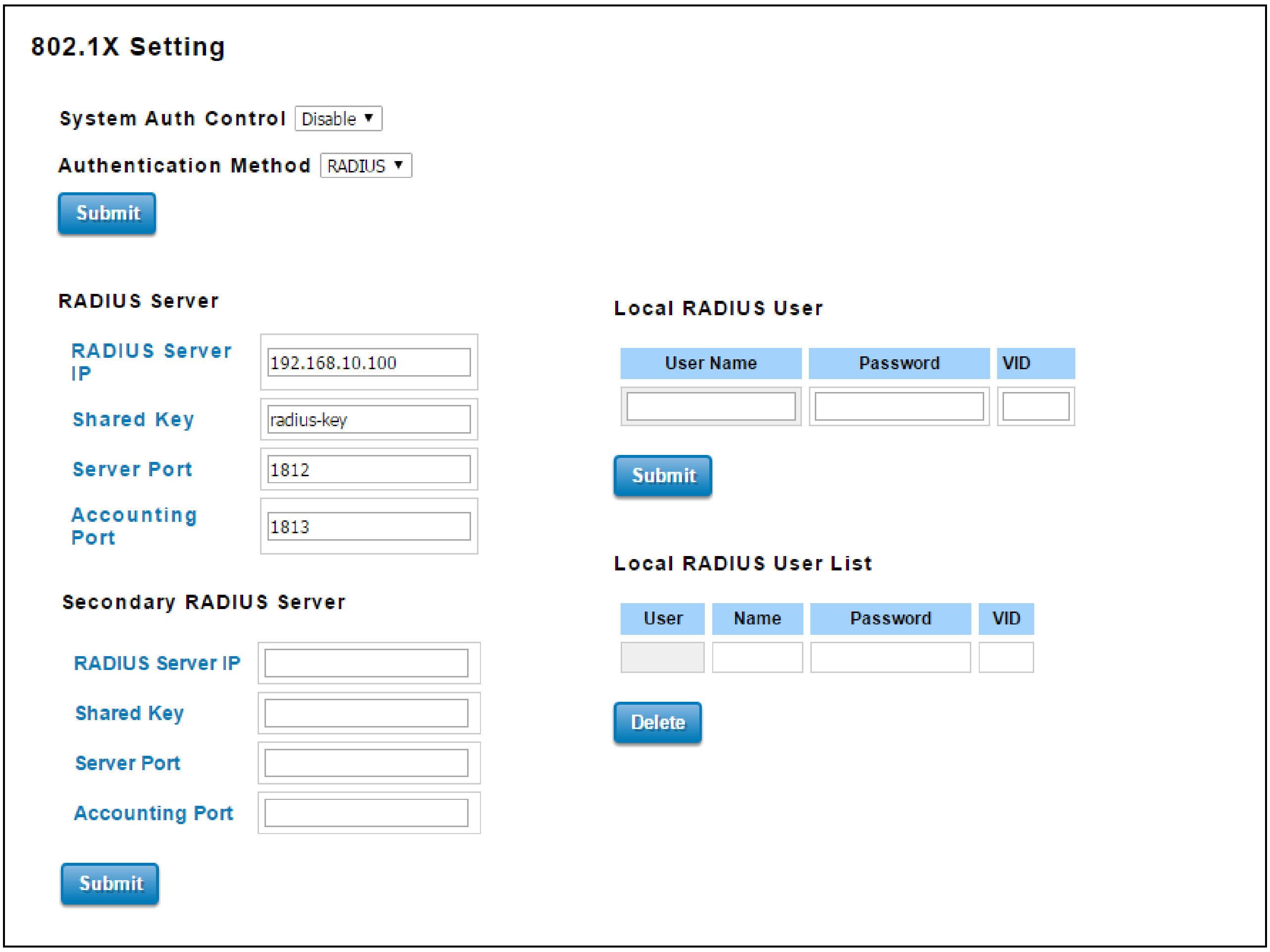
802.1X is an IEEE Standard for Port-based Network Access Control that provides an authentication mechanism to devices that wish to attach to a LAN or WLAN. Port-based network access control protocol contains 3 parts, supplicant, authenticator, and authentication server. With 802.1X authentication, a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

RADIUS

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

802.1X Setting

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


802.1X Setting

System Auth Control: Disable

Authentication Method: RADIUS

RADIUS Server

RADIUS Server IP	192.168.10.100
Shared Key	radius-key
Server Port	1812
Accounting Port	1813

Secondary RADIUS Server

RADIUS Server IP	
Shared Key	
Server Port	
Accounting Port	

Local RADIUS User

User Name	Password	VID

Local RADIUS User List

User	Name	Password	VID

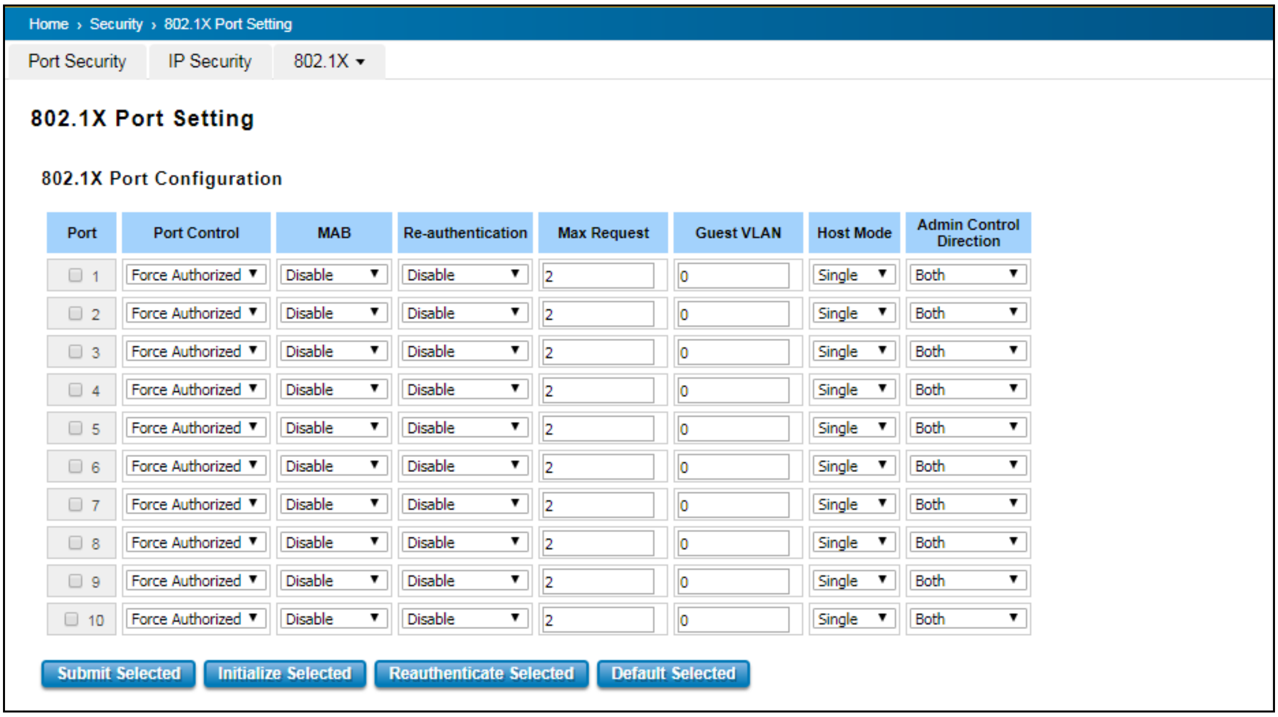
The description of the columns is as below:

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

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

802.1X Port Setting

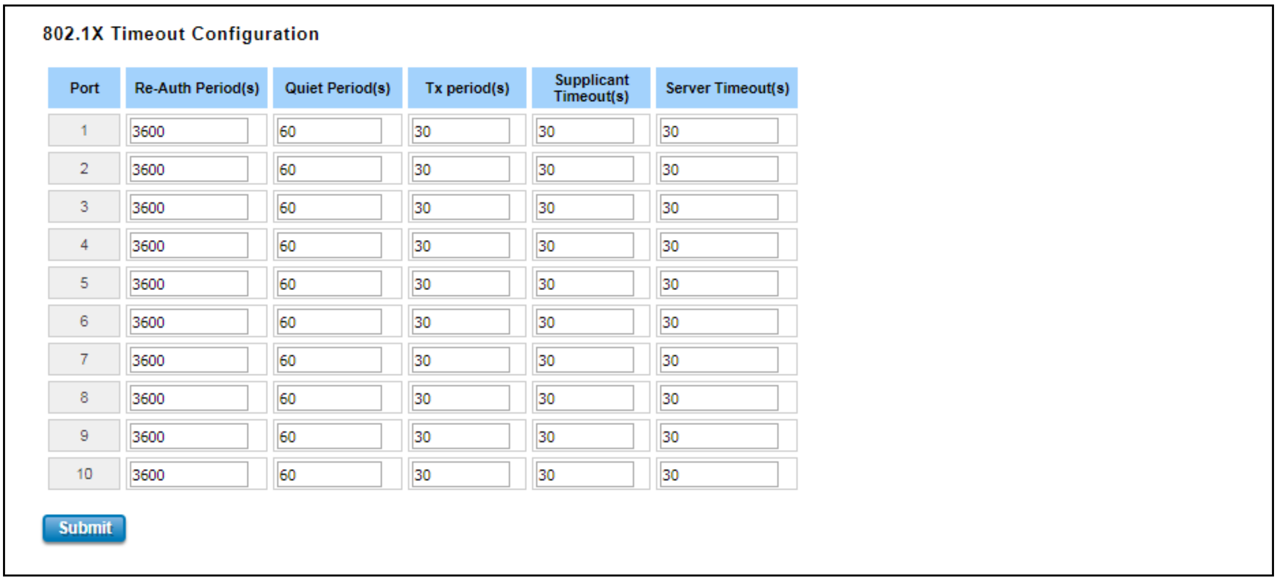
After the configuration of Radius Server or Local user list, user also need configure the authentication mode, authentication behavior, applied VLAN for each port and permitted communication. The following information will explain the port configuration.



802.1X Port Setting

802.1X Port Configuration

Port	Port Control	MAB	Re-authentication	Max Request	Guest VLAN	Host Mode	Admin Control Direction
□ 1	Force Authorized ▼	Disable ▼	Disable ▼	2	0	Single ▼	Both ▼
□ 2	Force Authorized ▼	Disable ▼	Disable ▼	2	0	Single ▼	Both ▼
□ 3	Force Authorized ▼	Disable ▼	Disable ▼	2	0	Single ▼	Both ▼
□ 4	Force Authorized ▼	Disable ▼	Disable ▼	2	0	Single ▼	Both ▼
□ 5	Force Authorized ▼	Disable ▼	Disable ▼	2	0	Single ▼	Both ▼
□ 6	Force Authorized ▼	Disable ▼	Disable ▼	2	0	Single ▼	Both ▼
□ 7	Force Authorized ▼	Disable ▼	Disable ▼	2	0	Single ▼	Both ▼
□ 8	Force Authorized ▼	Disable ▼	Disable ▼	2	0	Single ▼	Both ▼
□ 9	Force Authorized ▼	Disable ▼	Disable ▼	2	0	Single ▼	Both ▼
□ 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 end data out only or both send and receive.
Re-Auth Period	Control the Re-authentication time interval, 1~65535 are available.
Quiet Period	When authentication failed, Switch will wait for a period and try to communicate with radius server again.
Tx period	The time interval of authentication request.
Supplicant Timeout	The timeout for the client authenticating
Sever Timeout	The timeout for server response for authenticating.

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

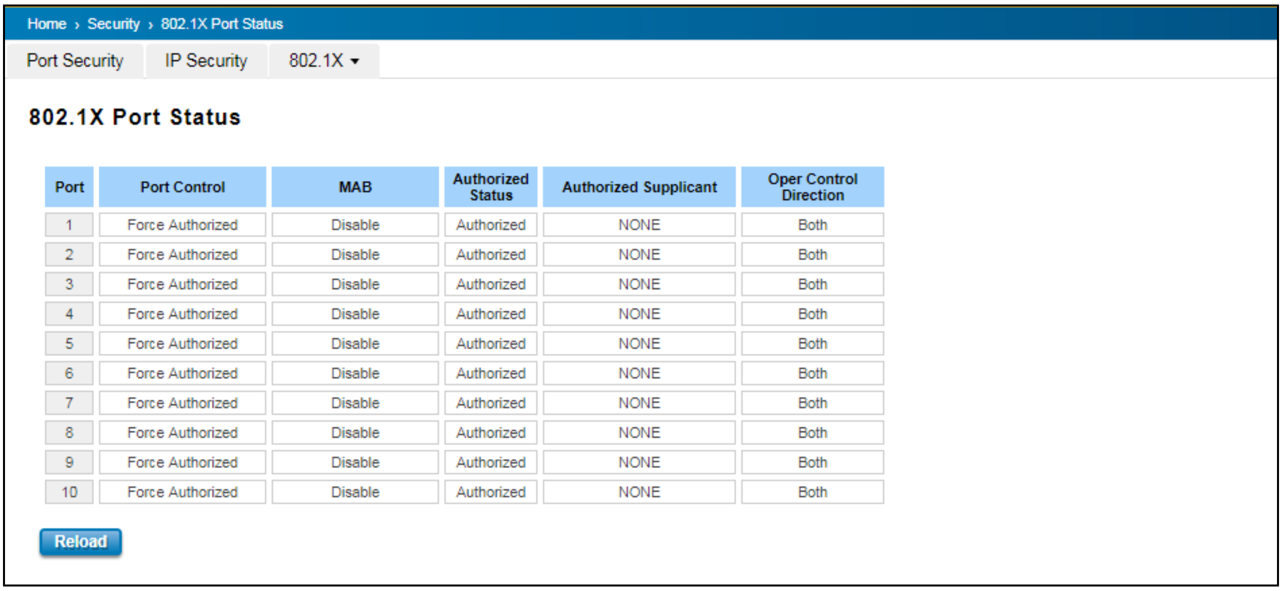
Click **Initialize Selected** to set the authorize state of selected port to initialize status.

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

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

802.1X Port Status

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



Home › Security › 802.1X Port Status

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

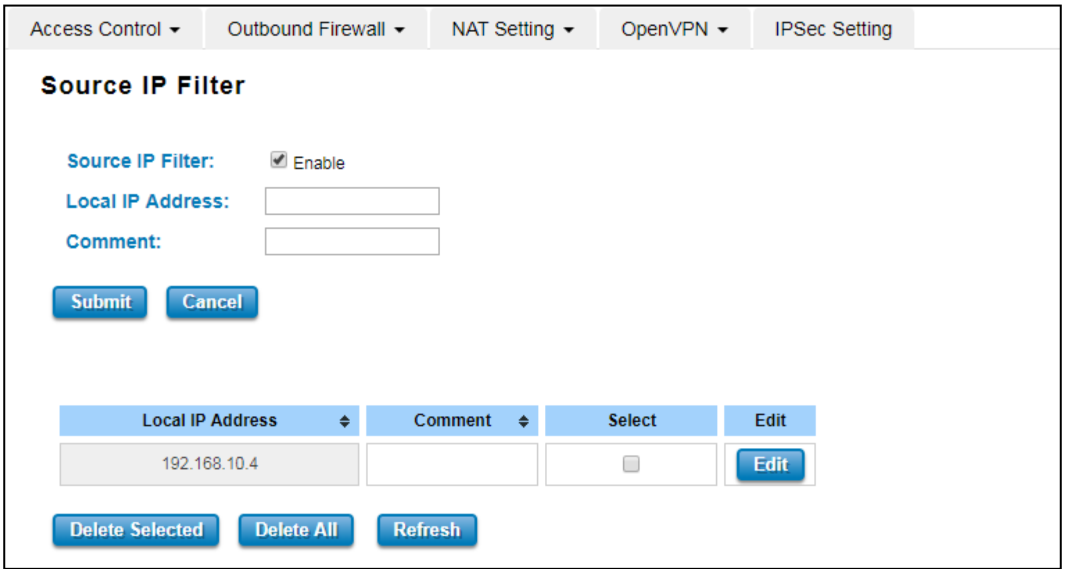
3.10.3 OUTBOUND FIREWALL

WoMaster' router has different types firewall settings, user can enable the setting, configure the rules. The following section is Outbound Firewall Settings pages where user can configure the Outbound Firewall setting.

TERMS	DESCRIPTION
Source IP Filter	Source IP addresses Filtering from LAN to Internet through the router.
Destination IP Filter	Destination IP addresses Filtering from the LAN to Internet through the router.
Source Port Filtering	Source Ports Filtering from the LAN to Internet through the router.
Destination Port Filtering	Destination Ports Filtering from the LAN to Internet through the router

Src IP Filter

By entries parameter in this table, it can restrict certain types of data packets from the local network to the internet



Source IP Filter

Source IP Filter: ☑ Enable

Local IP Address:

Comment:

Local IP Address	Comment	Select	Edit
192.168.10.4		□	Edit

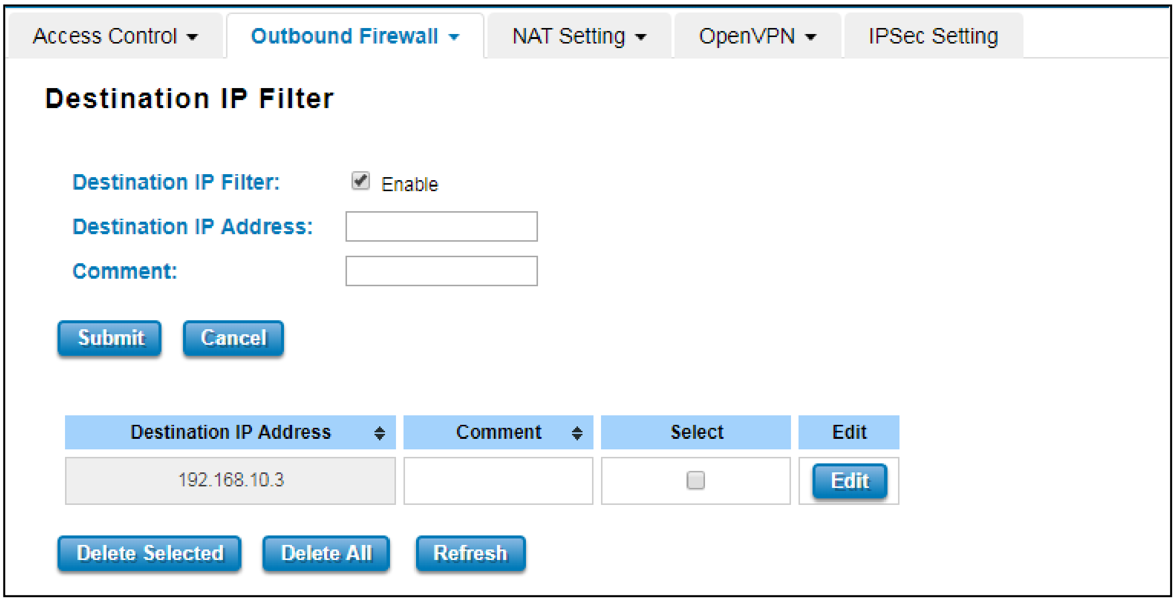
through the Router. The Source IP Filter will help to filter all of the packets that coming into the router. If the source IP is on the list, then the packets would be dropped. But if the source IP is not on the list, then the packets can be received. Select **Enable** to activate **Source IP Filtering**, type the **Local IP Address** and **Comment** to write notes for the entry. Click Submit to activate the settings. After applied, then user can see the new entry shown in the below table. The description of the columns is as below:

TERMS	DESCRIPTION
Local IP Address	Display the Source IP address.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete, or change the setting.
Edit	Click edit to modify the parameters

Click **Refresh** to refresh the table

Dest IP Filter

By entries parameters in this table are used to restrict the computers in LAN from accessing certain websites in WAN according to IP address. The concept is the same as the source IP Filter. The packet would not send to the specific IP Address that showed on the list. Only the IP Address that shows on the list that cannot receive the packets. Select **Enable** to activate **Destination IP Filtering**, type the **Destination IP Address** and **Comment** to write a note for the entry and then click Submit to apply the settings. After applied, then user can see the new entry shown in the below table.



Destination IP Filter

Destination IP Filter: ☑ Enable

Destination IP Address:

Comment:

Destination IP Address	Comment	Select	Edit
192.168.10.3		□	Edit

The description of the columns is as below:

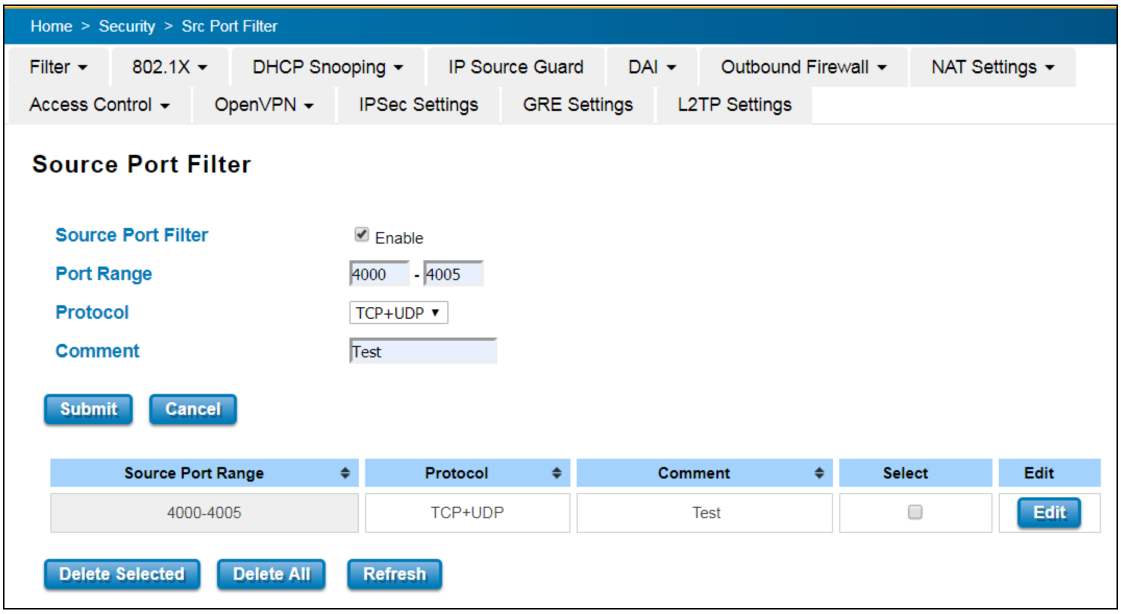
TERMS	DESCRIPTION
Destination IP Address	Display the Destination IP address.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete, or change the setting.
Edit	Click edit to modify the parameters

Click **Refresh** to refresh the table

Src Port Filter

Entries in this table are used to restrict certain ports of data packets from user's local network to the Internet through the Router. Use of such filters can be helpful in securing or restricting local network. The device just cannot receive any packets from the source port that showed on the list, the other packet that sent from any source port that not on the list would be received.

Select **Enable Source Port filtering**, type the **Port Range** of below **Protocol** type, the protocol type can be **UDP, TCP or TCP+UDP**. Type the **Comment** to write a note for the entry and then click **Submit** to activate the settings.



Source Port Filter

Source Port Filter ☑ Enable

Port Range 4000 - 4005

Protocol TCP+UDP

Comment Test

Source Port Range	Protocol	Comment	Select	Edit
4000-4005	TCP+UDP	Test	□	Edit

After applied, user can see the new entry shown in the below table.

The description of the columns is as below:

TERMS	DESCRIPTION
Source Port Range	Display the Source Port Range (Range is from 1 to 65535)
Protocol	Display the protocol that has been chosen by the user. The mode includes TCP, UDP and TCP+UDP.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete, or change the setting.
Edit	Click edit to modify the parameters

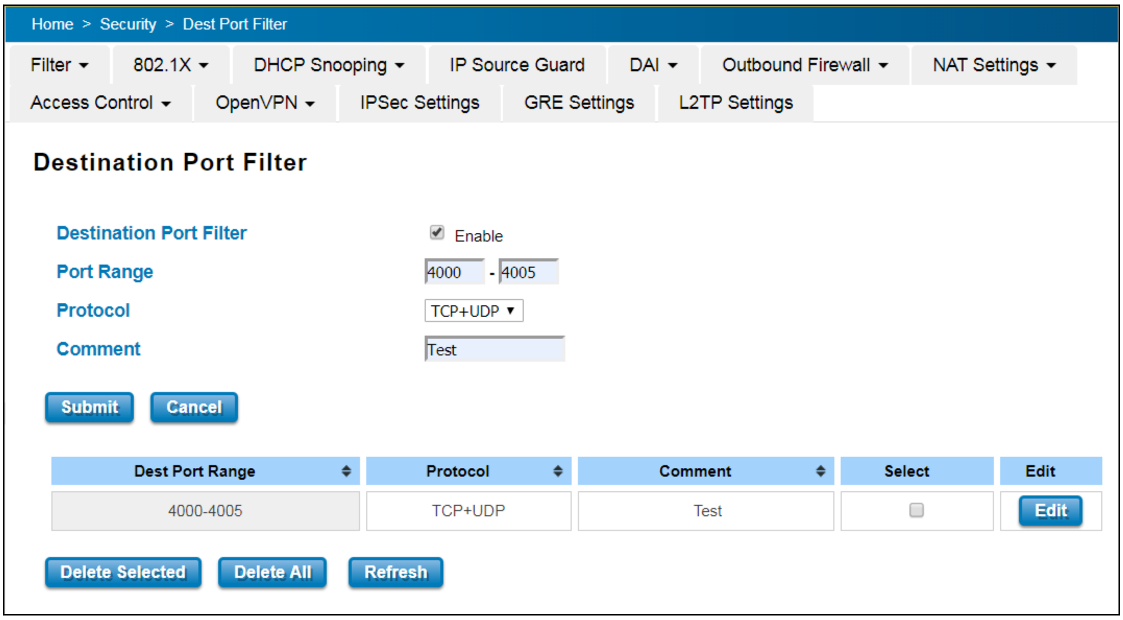
Click **Refresh** to refresh the table

Dest Port Filter

Entries in this table are used to restrict certain ports of data packets from user's local network to Internet through the router. Use of such filters can be helpful in securing or restricting local network. And the device cannot send any packets to the destination port that showed on the list.

Select **Enable Destination Port Filtering**, type the **Port Range** of below **Protocol** type, the protocol type can be **UDP, TCP or TCP+UDP**. Type the **Comment** to write note for the entry and then press **Submit** to apply the settings.

After applied, then user can see the new entry shown in the below table.



Destination Port Filter

Destination Port Filter	☑ Enable
Port Range	4000 - 4005
Protocol	TCP+UDP ▾
Comment	Test

Dest Port Range	Protocol	Comment	Select	Edit
4000-4005	TCP+UDP	Test	□	Edit

The description of the columns is as below:

TERMS	DESCRIPTION
Dest Port Range	Display the Destination Port Range (Range is from 1 to 65535)
Protocol	Display the protocol that has been chosen by the user. The mode includes TCP, UDP and TCP+UDP.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete, or change the setting.
Edit	Click edit to modify the parameters

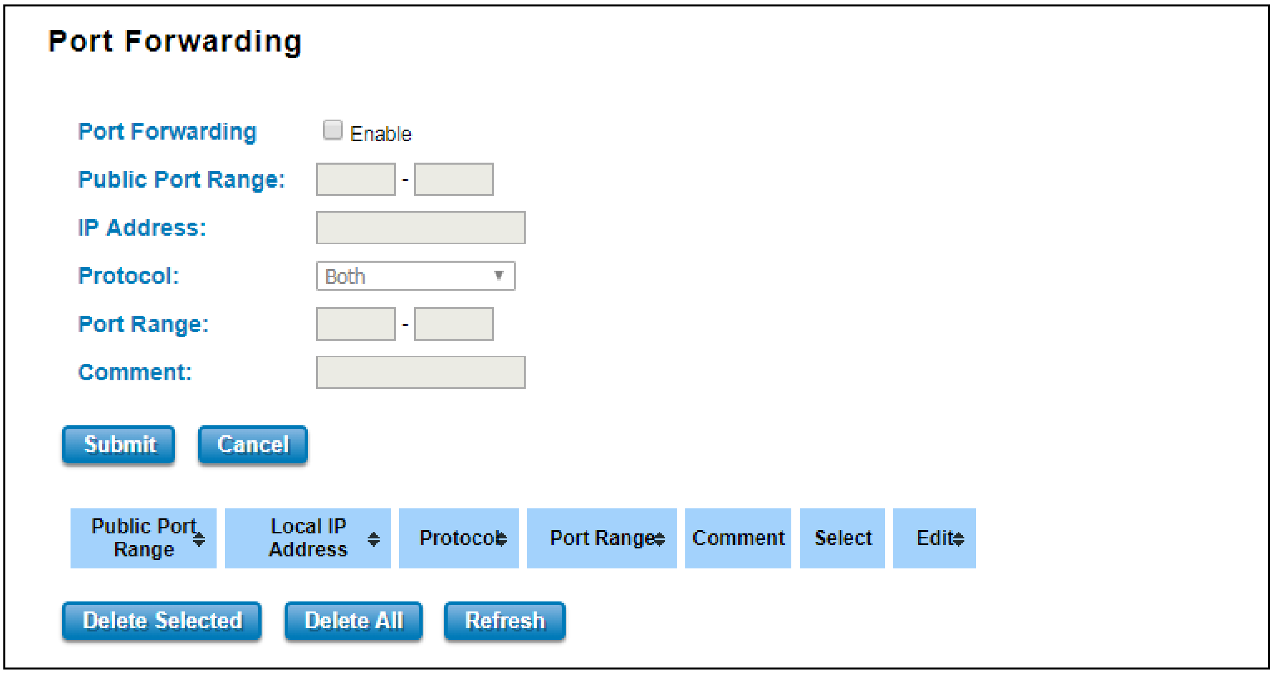
Click **Refresh** to refresh the table

3.10.4 NAT SETTING

Network Address Translation is the process where a network device, usually a firewall, assigns a public address to a device or group of devices inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economic and security purposes. The simple type of NAT provides one to one translation of IP address. It can be used to interconnect two IP networks, normally one network is for Local Area Network and the other network is for Wide Area Network/Internet. To support this function, there are two ways to do it, by using Source Network Address Translation (SNAT), Destination Network Address Translation (DNAT). Basically, Network Address Translation (NAT) occurs when one of the IP addresses in an IP packet header is changed. In a SNAT, the destination IP address is maintained and the source IP address is changed. Most commonly, a SNAT allows a host on the “inside” of the NAT, in an RFC 1918 IP address space, to initiate a connection to a host on the “outside” of the NAT. It supports the Port Forwarding, DMZ and 1 to 1 NAT configuration. A DNAT, by way of contrast, occurs when the destination address is changed and the source IP address is maintained. A DNAT allows a host on the “outside” to connect to a host on the “inside”. In both cases, the NAT has to maintain a connection table which tells the NAT where to route returning packets. An important difference between a SNAT and a DNAT is that a SNAT allows multiple hosts on the “inside” to get to any host on the “outside”. By way of contrast, a DNAT allows any host on the “outside” to get to a single host on the “inside”. It is supported in NAPT and 1 to 1 NAT features.

To configure the NAT Setting, the **Port Forwarding, DMZ, Port Mapping Policy and 1 to 1 NAT** configuration page are provided in this section.

Port Forwarding



Port Forwarding

Port Forwarding ☐ Enable

Public Port Range: -

IP Address:

Protocol: Both

Port Range: -

Comment:

Public Port Range	Local IP Address	Protocol	Port Range	Comment	Select	Edit

By configuring this table, it allows user to automatically redirect common network services to a specific machine behind the NAT firewall. Select **Enable** to activate **Port Forwarding** function and then input all of the parameters to configure the port forwarding.

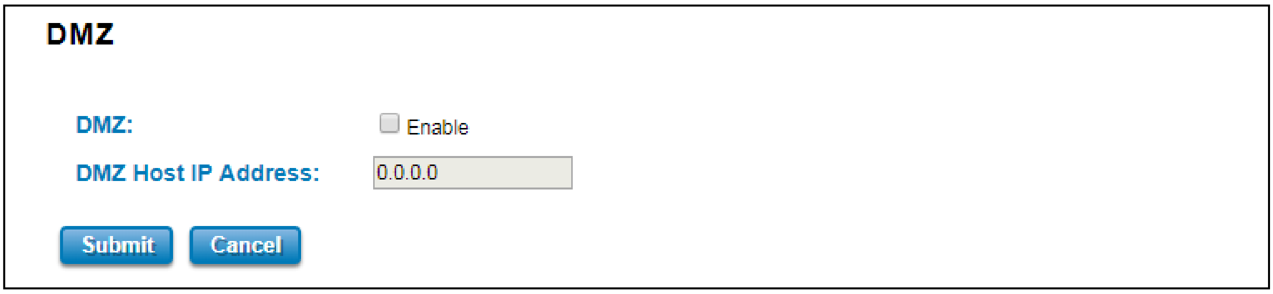
The description of the columns is as below:

TERMS	DESCRIPTION
Port Forwarding	Select Enable to activate Port Forwarding function.
Public Port Range	Configure the port range, which will be public to a WAN / Internet. User can configure one or a range of TCP/UDP port number.
IP Address	Configure the IP Address of the LAN PC. The traffic from the public port range will be redirected to this IP address.
Protocol	Configure TCP, UDP or Both (TCP + UDP) protocol type.
Port Range	Configure the port range of the LAN; the traffic from the public port will be redirected to these ports.
Comment	Add information to the entry.

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

DMZ

A **Demilitarized Zone** is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains device accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.



DMZ

DMZ: ☐ Enable

DMZ Host IP Address: 0.0.0.0

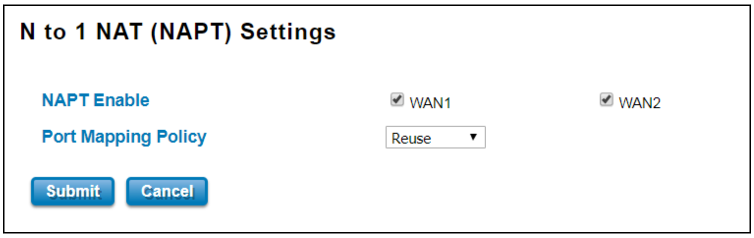
Click **Enable** to activate the function and assign the IP address of **DMZ Host IP Address**. This is the DMZ computer's IP address. Click Submit to activate the function.

The description of the columns is as below:

TERMS	DESCRIPTION
DMZ	Select Enable to activate DMZ function.
DMZ Host IP Address	Configure the port range, which will be public to a WAN / Internet. User can configure one or a range of TCP/UDP port number.

N to 1 NAT (NAPT) /Port Mapping Policy

This page allows user to Enable NAPT interface and configure the Port Mapping policy from NAT Setting.



N to 1 NAT (NAPT) Settings

NAPT Enable ☑ WAN1 ☑ WAN2

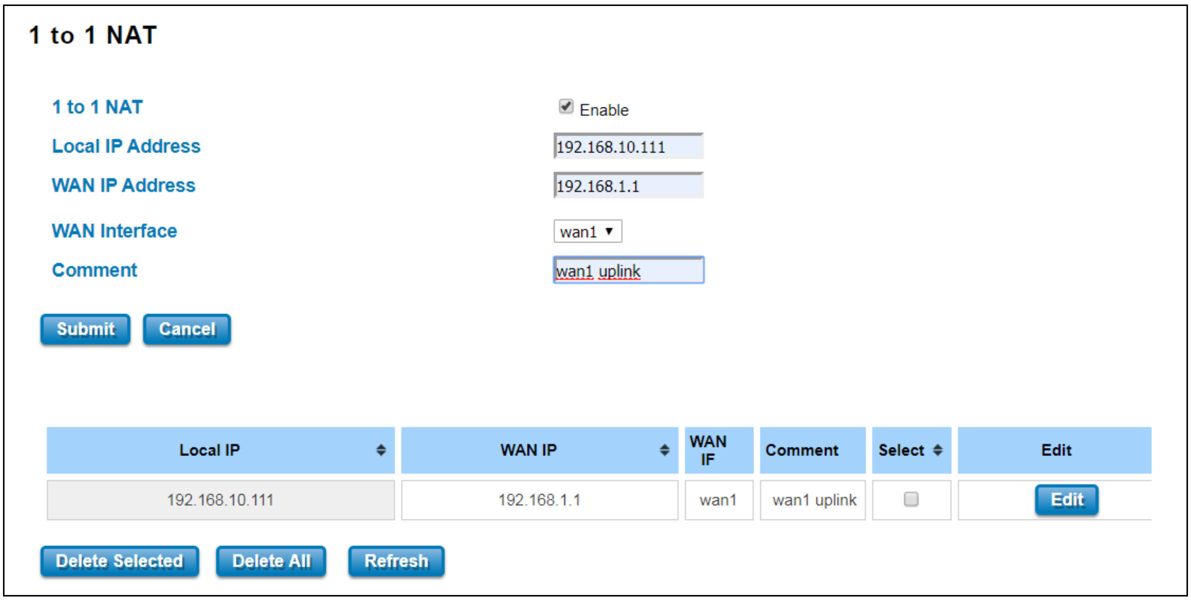
Port Mapping Policy Reuse ▼

The description of the columns is as below:

TERMS	DESCRIPTION
NAPT Enable	Select the Interface while the router supports multiple WAN ports. There are two WAN interfaces in DRS610.
Port Mapping Policy	**Default: Reuse** Reuse: Use the same port number that has been used to access the same remote device. Randomize: Change the port number every time access the remote device.

Click **Submit** to apply the configuration.

1 to 1 NAT



1 to 1 NAT

1 to 1 NAT	☑ Enable
Local IP Address	192.168.10.111
WAN IP Address	192.168.1.1
WAN Interface	wan1 ▾
Comment	wan1 uplink

Local IP	WAN IP	WAN IF	Comment	Select	Edit
192.168.10.111	192.168.1.1	wan1	wan1 uplink	□	Edit

One-to-one NAT is a way to make systems behind a firewall and configured with private IP addresses (those reserved for private use in RFC 1918) appear to have public IP addresses. With one-to-one NAT, you assign local systems RFC 1918 addresses then establish a one-to-one mapping between those addresses and public IP addresses. For outgoing connections SNAT (Source Network Address Translation) occurs and on incoming connections DNAT (Destination Network Address Translation) occurs. Below is the 1 to 1 NAT section interface.

The description of the columns is as below:

TERMS	DESCRIPTION
1 to 1 NAT	Check the box to enable the function
Local IP Address	The target local IP Address
WAN IP Address	The incoming IP Address that coming through the WAN
WAN Interface	Select the WAN interface while the router support multiple WAN interfaces
Comment	Enter a comment

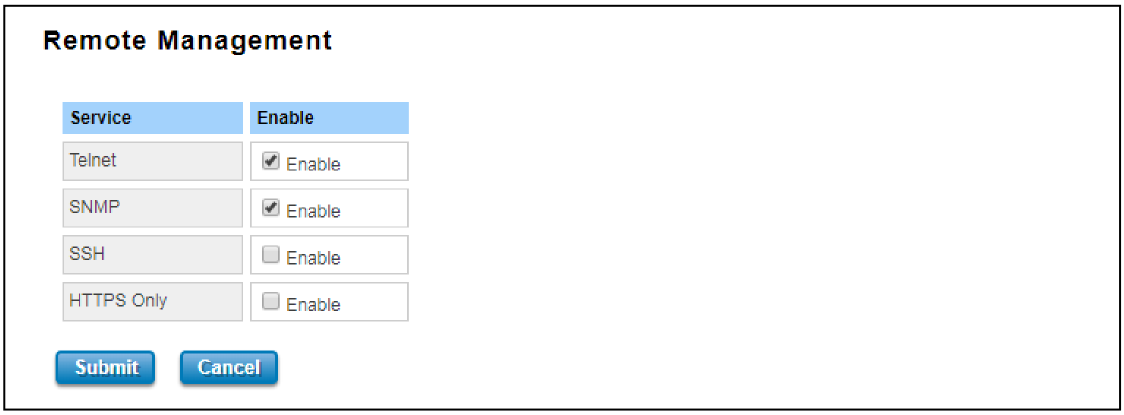
Click **Submit** to apply the configuration.

3.10.5 ACCESS CONTROL

WoMaster router provides access control mode in several ways, such as Remote Management, WAN Service Access Control and Custom Exception. By configuring this configuration, user can enhance the security access to the device.

Remote Management

Remote Management function, open the Remote Management, that would allow the user via the local access (WAN Port) Remote Management the router.



Remote Management

Service	Enable
Telnet	☑ Enable
SNMP	☑ Enable
SSH	☐ Enable
HTTPS Only	☐ Enable

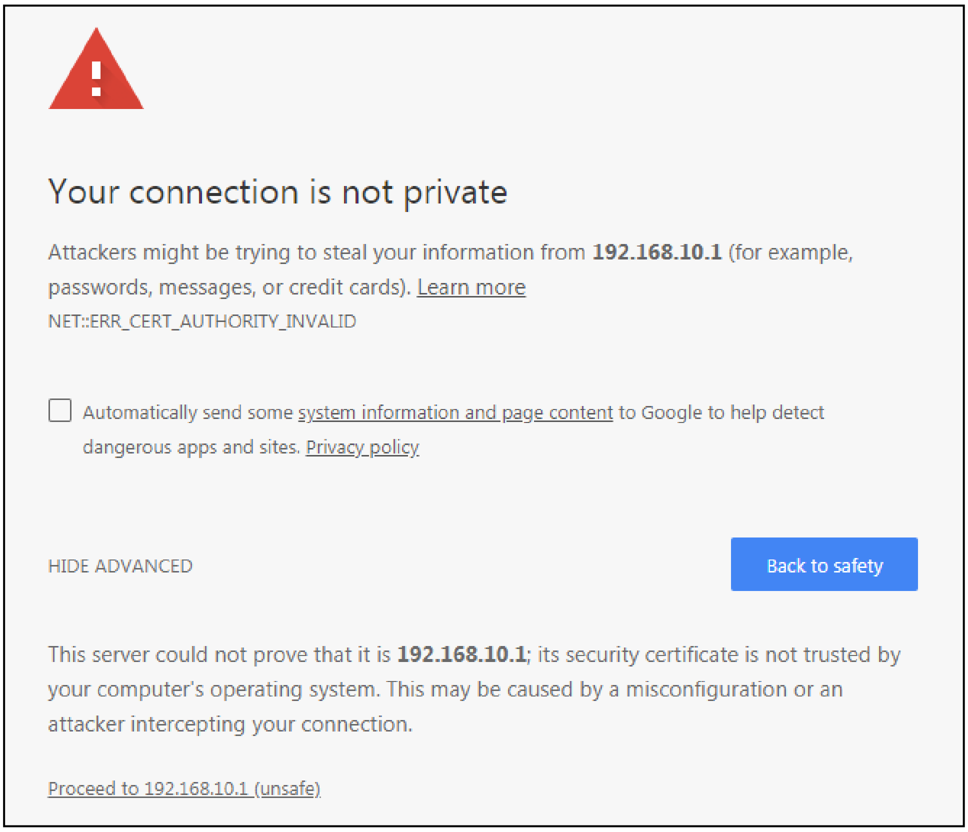
The description of the columns is as below:

TERMS	DESCRIPTION
Telnet	Allows the user to remotely login and manage the device by Telnet. When user doesn't enable it, the connection through telnet will not allow.
SNMP	Allows the user to remotely login and manage the device by SNMP. When user doesn't enable it, the connection through SNMP will not allow.
SSH	Allows the user to remotely login and manage the device by SSH/ When user doesn't enable it, the connection through SSH will not allow.
HTTPS Only	Allows the user to remotely login and manage the device by HTTPS access for secure connection, and it would disable the HTTP access.

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

HTTPS Only

HTTP Secure is the use of the HTTP protocol over an SSL/TLS protocol. It is used primarily to protect against eavesdropping of communication between a web browser and the web site to which it is connected. This is especially important when you wish to have a secure connection over a public network such as the internet. HTTPS connections are secured through the use of certificates issued by trusted certificate authorities. When a web browser makes a connection attempt to a secured web site, a digital certificate is sent to the browser so that it can verify the authenticity of the site using a built-in list of trusted certificate authorities.



Your connection is not private

Attackers might be trying to steal your information from **192.168.10.1** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

HIDE ADVANCED

Back to safety

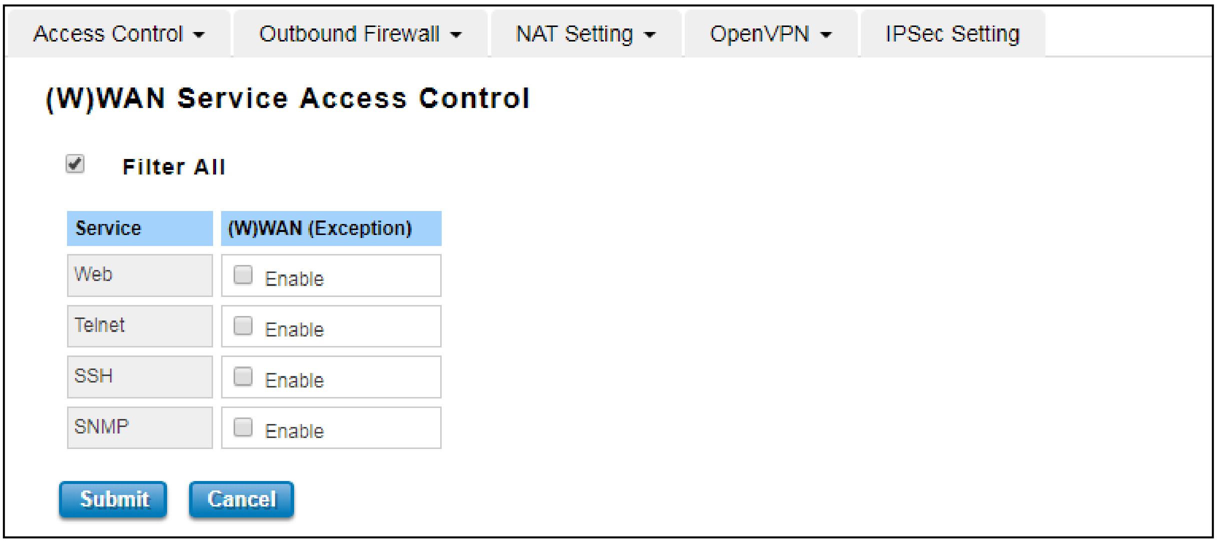
This server could not prove that it is **192.168.10.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.10.1 (unsafe)

If user uses the HTTPS Only, a warning page would appear when user access the device in order to provide a secure access. The picture above is the warning message about the digital certificate and user just need to accept this warning by click **"Proceed to 192.168.10.1 (unsafe)"**.

WAN Access

This feature is about the exception to access the device through the WAN interface for security concern. So that the access or the traffic that coming through the WAN interface can be limited as required. The user may choose the **Filter All** functions to block all access from the WAN interface or enable the exception options, then the router allows user to remotely access to the router from WAN interface.



(W)WAN Service Access Control

☑ Filter All

Service	(W)WAN (Exception)
Web	□ Enable
Telnet	□ Enable
SSH	□ Enable
SNMP	□ Enable

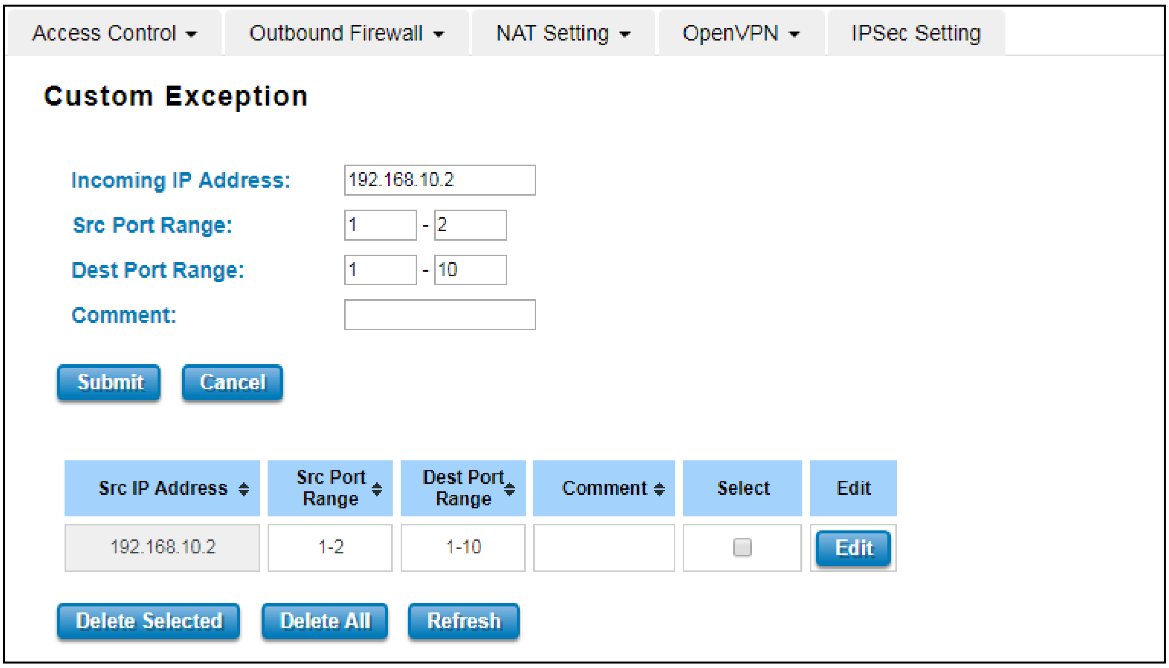
The description of the columns is as below:

TERMS	DESCRIPTION
Filter All	By select Filter All, it will block all external access from WAN interface to the device (such as SSH, SNMP, Web and Telnet) and unblock the exception options.
Web	Select this option to allow access to the router using Web (HTTP or HTTPS) from the WAN Interface
Telnet	Select this option to allow access to the router using Telnet from the WAN Interface
SSH	Select this option to allow access to the router using SSH from the WAN Interface
SNMP	Select this option to allow access to the router using SNMP from the WAN Interface

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

Custom Exception

Another choice for the access control is also provided by WoMaster, it is called custom exception feature. Through this feature, it can help to allow the incoming access through the firewall to local devices. If the condition does not meet the requirement from the table, then the access would be denied.



Custom Exception

Incoming IP Address:	192.168.10.2
Src Port Range:	1 - 2
Dest Port Range:	1 - 10
Comment:	

Src IP Address	Src Port Range	Dest Port Range	Comment	Select	Edit
192.168.10.2	1-2	1-10		□	Edit

The description of the columns is as below:

TERMS	DESCRIPTION
Src IP Address	Set up the source IP Address that may access the device.
Src Port Range	Set up the source port range where the access came from.
Dest Port Range	Set up the destination port range where the access is going to.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete,
Edit	Click edit to modify the parameters

Once User finishes configuring the settings, click on **Submit** to apply configuration and a new line will directly appear on the table.

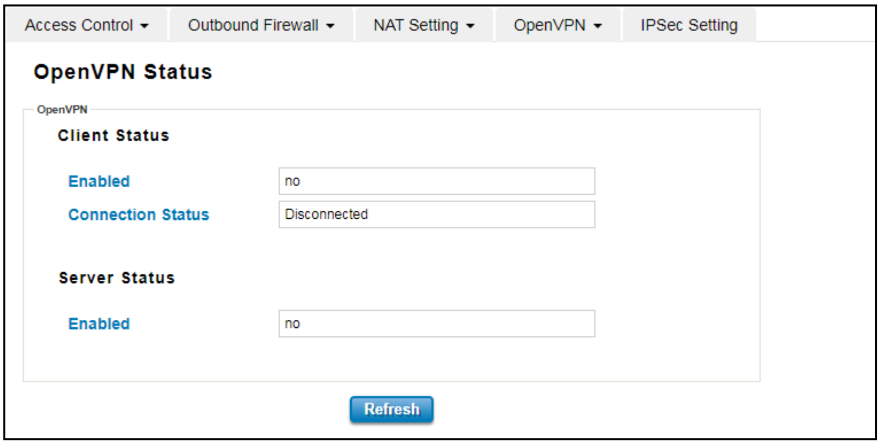
3.10.6 OPEN VPN

WoMaster router supports OpenVPN. To help user create the secure connection for the remote devices, WoMaster device supports both OpenVPN Server and OpenVPN Client. In latest firmware, WoMaster Router Switch also start to support OpenVPN Key Generation, this is import helpful tool to build Site to Site VPN easily.

It implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections. It is possible to create one-to-many tunnel for the VPN Server. OpenVPN implementation offers a cost-effective, simply configurable alternative to other VPN technologies. OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. The server and client have almost the same configuration. The difference in the client configuration is the remote endpoint IP or hostname field. Also, the client can set up the keepalive settings.

3.10.6.1 OpenVPN Status

This section shows the VPN Client and Server current status.



OpenVPN Status

OpenVPN

Client Status

Enabled: no

Connection Status: Disconnected

Server Status

Enabled: no

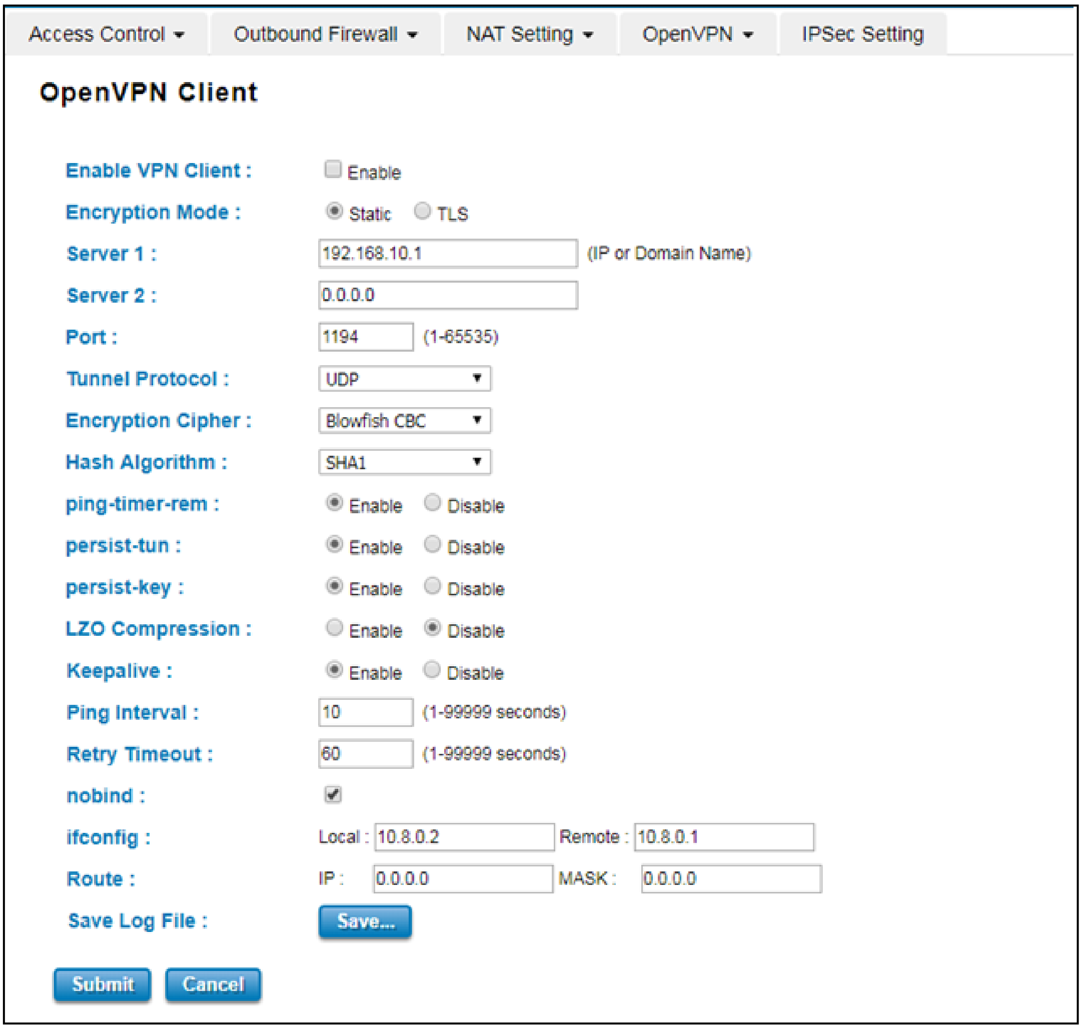
The description of the columns is as below:

TERMS	DESCRIPTION
Enabled	**Default: no** **yes:** The VPN function is enabled. **no:** The VPN function is not enabled
Connection Status	**Default: Disconnected** **Connected:** The VPN connection is established **Disconnected:** The VPN connection is not established

Click **Refresh** to update the information.

3.10.6.2 penVPN Client

This page is about the OpenVPN Client configuration page. While the device set as the VPN client, the parameters must follow the VPN Server settings. User should adjust the parameters with the administrator of the VPN server to entry the correct parameters. Two VPN servers IP are also provided in order to have the backup connection for VPN Server.



OpenVPN Client

Enable VPN Client :	□ Enable
Encryption Mode :	● Static ○ TLS
Server 1 :	192.168.10.1 (IP or Domain Name)
Server 2 :	0.0.0.0
Port :	1194 (1-65535)
Tunnel Protocol :	UDP
Encryption Cipher :	Blowfish CBC
Hash Algorithm :	SHA1
ping-timer-rem :	● Enable ○ Disable
persist-tun :	● Enable ○ Disable
persist-key :	● Enable ○ Disable
LZO Compression :	○ Enable ● Disable
Keepalive :	● Enable ○ Disable
Ping Interval :	10 (1-99999 seconds)
Retry Timeout :	60 (1-99999 seconds)
nobind :	☑
ifconfig :	Local : 10.8.0.2 Remote : 10.8.0.1
Route :	IP : 0.0.0.0 MASK : 0.0.0.0
Save Log File :	Save...

The description of the columns is as below:

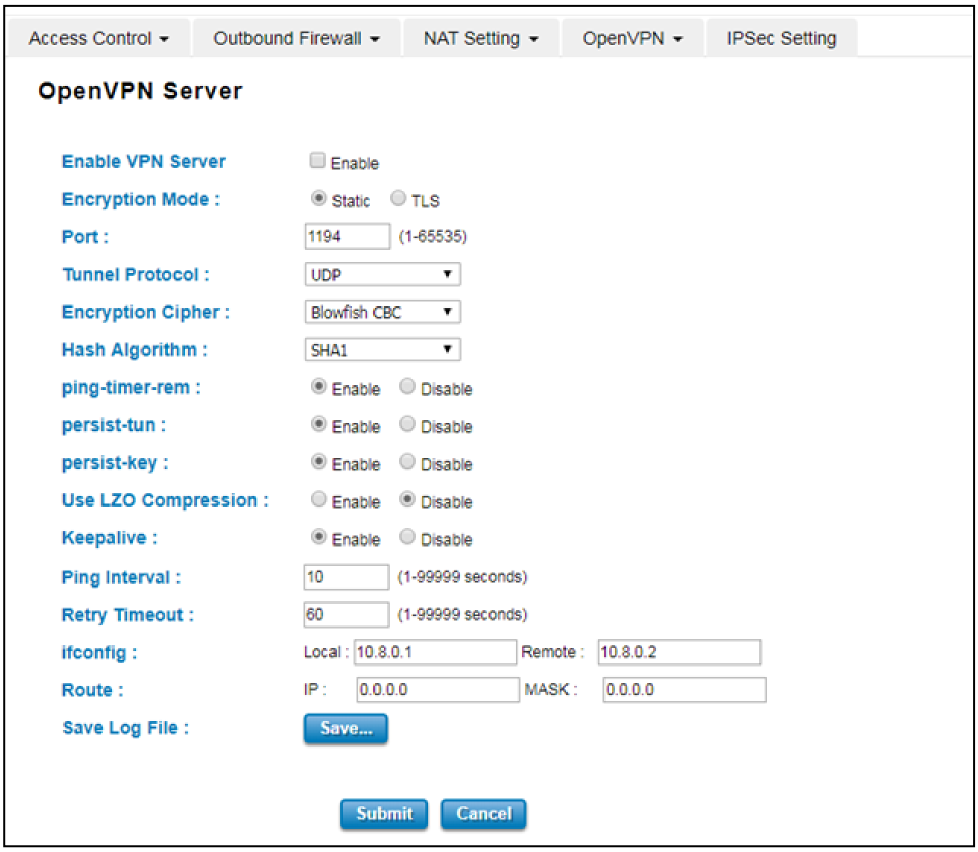
TERMS	DESCRIPTION
Enable VPN Client	Select Enable to activate the VPN Client function
Encryption Mode	Choose the Encryption Mode Static Key: Use a pre-shared static key. TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server 1	Type the IP Address of the VPN Server
Server 2	Type the second IP Address of the VPN Server if needed.
Port	**Default: 1194** Input the port number that VPN service used. Please check the VPN Server port setting. The range from 1-65535.

Tunnel Protocol	Choose use TCP or UDP to establish the VPN connection.
Encryption Cipher	Select the encryption cipher from Blowfish to AES in Pull-down menus.
Hash Algorithm	Hash algorithm provides a method of quick access to data, including SHA1，SHA256，SHA512，MD5
ping-timer-rem	**Default: Enable** Select enable or disable the ping-timer-rem, this function prevent unnecessary restart at server/client when network fail.
persist-tun	**Default: Enable** Select enable or disable the persist-tun, enable this function will keep tun(layer 3) device linkup after Keepalive timeout.
persist-key	**Default: Enable** Select enable or disable the persist-key, enable this function will keep the key first use if VPN restart after Keepalive timeout.
LZO Compression	**Default: Disable** Select use LZO Compression or not, this function compresses data to decrease the traffic but also need more CPU effort.
Keepalive	**Default: Enable** Select enable or disable Keepalive function, this function is use to detect the status of connection.
Ping Interval	**Default: 10** Input the ping interval, the range can from 1~99999 seconds.
Retry Timeout	**Default: 60** Input the retry timeout, the range can from 1~99999 seconds.
nobind	Check the box to activate nobind function. With nobind function, the source ports are random.
ifconfig	Input the tunnel IP addresses that VPN use.
Route	Input the route IP and MASK. This is the target IP domain that user can access through the VPN tunnel.
Save Log File	Click Save to keep the VPN Client Log.

Click **Submit** to apply the configuration.

3.10.6.3 OpenVPN Server

To help user create the One to One Secure connection for the remote devices, WoMaster device supports both OpenVPN Server and OpenVPN Client. This Server setting allows user to configure the Secure M2M connection for one remote Client. But WoMaster router also supports one to multiple for VPN Client.



OpenVPN Server

Enable VPN Server ☐ Enable

Encryption Mode : ● Static ○ TLS

Port : 1194 (1-65535)

Tunnel Protocol : UDP

Encryption Cipher : Blowfish CBC

Hash Algorithm : SHA1

ping-timer-rem : ● Enable ○ Disable

persist-tun : ● Enable ○ Disable

persist-key : ● Enable ○ Disable

Use LZO Compression : ○ Enable ● Disable

Keepalive : ● Enable ○ Disable

Ping Interval : 10 (1-99999 seconds)

Retry Timeout : 60 (1-99999 seconds)

ifconfig : Local : 10.8.0.1 Remote : 10.8.0.2

Route : IP : 0.0.0.0 MASK : 0.0.0.0

Save Log File :

The description of the columns is as below:

TERMS	DESCRIPTION
Enable VPN Server	Select Enable to activate the VPN Server function
Encryption Mode	Choose the Encryption Mode Static Key: Use a pre-shared static key. TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server 1	Type the IP Address of the VPN Server
Server 2	Type the second IP Address of the VPN Server if needed.
Port	**Default: 1194** Input the port number that VPN service used. Please check the VPN Server port setting. The range from 1-65535.
Tunnel Protocol	Choose use TCP or UDP to establish the VPN connection.
Encryption Cipher	Select the encryption cipher from Blowfish to AES in Pull-down menus.
Hash Algorithm	Hash algorithm provides a method of quick access to data, including SHA1, SHA256, SHA512, and MD5
ping-timer-rem	**Default: Enable**

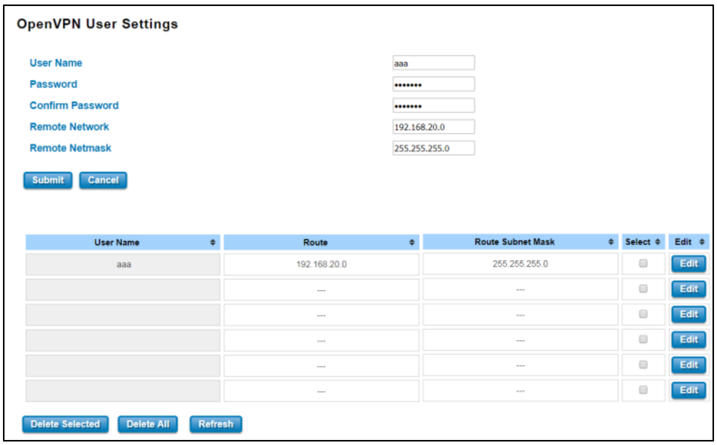
	Select enable or disable the ping-timer-rem, this function is to prevent unnecessary restart at server/client when the network fails.
persist-tun	**Default: Enable** Select enable or disable the persist-tun, enable this function will keep tun(layer 3) device linkup after Keepalive timeout.
persist-key	**Default: Enable** Select enable or disable the persist-key, enable this function will keep the key first use if VPN restart after Keepalive timeout.
LZO Compression	**Default: Disable** Select use LZO Compression or not, this function compresses data to decrease the traffic, but also need more CPU effort.
Keepalive	**Default: Enable** Select enable or disable Keepalive function, this function is used to detect the status of the connection.
Ping Interval	Input the ping interval, the range can from 1~99999 seconds.
Retry Timeout	Input the retry timeout, the range can from 1~99999 seconds.
ifconfig	Input the tunnel IP addresses that VPN use.
Route	Input the route IP and MASK. This is the target IP domain that user can access through the VPN tunnel.
Save Log File	Click Save to keep the VPN Server Log.

Click **Submit** to apply the configuration.

3.10.6.4 OpenVPN User Settings

This is extended setting of OpenVPN Server and applied in 1 Server to N Clients OpenVPN connectivity.

You can add User Name settings in this page. Add User Name, Password and Confirm Password, Remote Network and Netmask and click “Submit”. Then you can see the User Name database in below column.

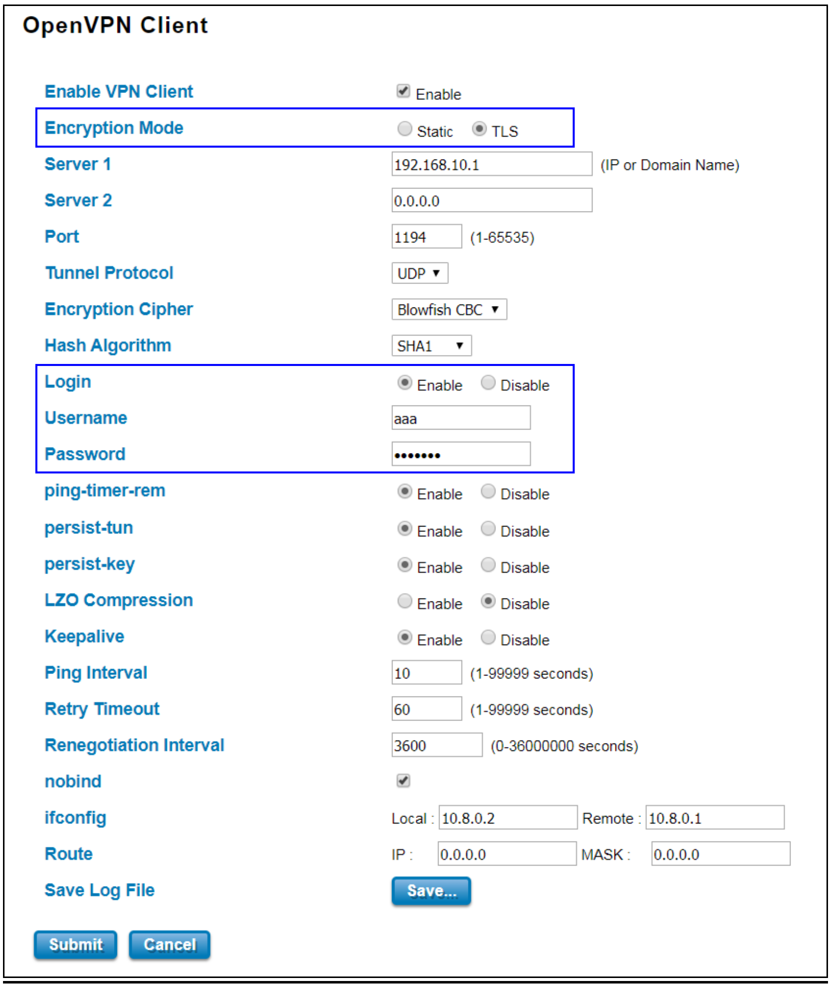


OpenVPN User Settings

User Name	aaa
Password	•••••••
Confirm Password	•••••••
Remote Network	192.168.20.0
Remote Netmask	255.255.255.0

User Name	Route	Route Subnet Mask	Select	Edit
aaa	192.168.20.0	255.255.255.0	□	Edit
	---	---	□	Edit
	---	---	□	Edit
	---	---	□	Edit
	---	---	□	Edit
	---	---	□	Edit

In OpenVPN client, you must type correct user name and password for authentication. Below is our OpenVPN client setting page, select the “**TLS**” Encryption Mode and Enable ”**Login**” checkbox, then the Username/Password columns are displayed. Type correct Username and password added in OpenVPN User Settings.

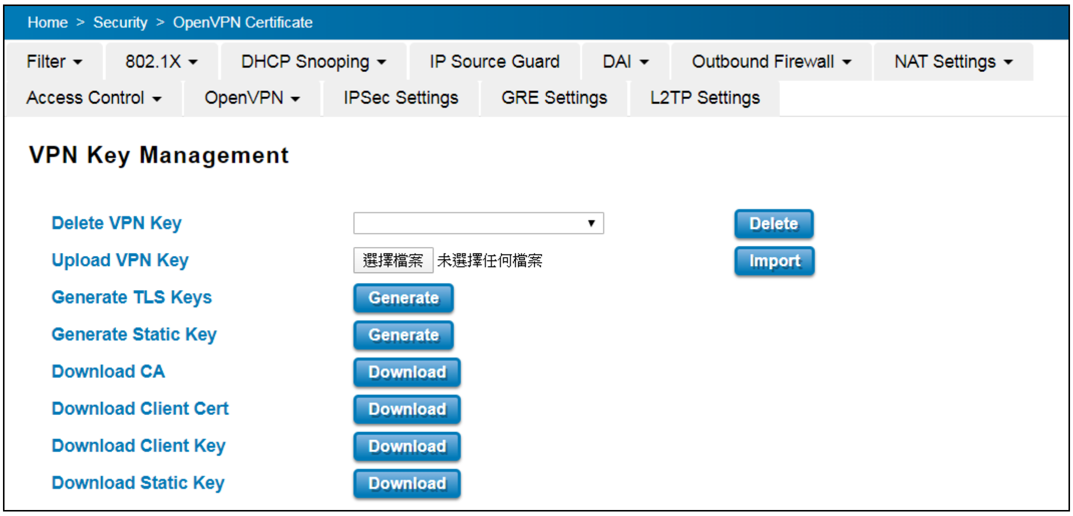


OpenVPN Client

Enable VPN Client	☑ Enable
Encryption Mode	○ Static ● TLS
Server 1	192.168.10.1 (IP or Domain Name)
Server 2	0.0.0.0
Port	1194 (1-65535)
Tunnel Protocol	UDP ▾
Encryption Cipher	Blowfish CBC ▾
Hash Algorithm	SHA1 ▾
Login	● Enable ○ Disable
Username	aaa
Password	•••••••
ping-timer-rem	● Enable ○ Disable
persist-tun	● Enable ○ Disable
persist-key	● Enable ○ Disable
LZO Compression	○ Enable ● Disable
Keepalive	● Enable ○ Disable
Ping Interval	10 (1-99999 seconds)
Retry Timeout	60 (1-99999 seconds)
Renegotiation Interval	3600 (0-36000000 seconds)
nobind	☑
ifconfig	Local : 10.8.0.2 Remote : 10.8.0.1
Route	IP : 0.0.0.0 MASK : 0.0.0.0
Save Log File	Save...

3.10.6.5 OpenVPN Certificate

Using digital certificates for authentication instead of preshared keys in VPNs is considered more secure. In WoMaster’ devices, digital certificates are one way of authenticating two peer devices to establish a VPN tunnel.



VPN Key Management

Delete VPN Key
Upload VPN Key 選擇檔案 未選擇任何檔案
Generate TLS Keys
Generate Static Key
Download CA
Download Client Cert
Download Client Key
Download Static Key

Key Generation in WoMaster Secure Router Switch

For OpenVPN connectivity, the OpenVPN Client must have the client Key/CA file generated by the OpenVPN Server. Normally, you can generate the key in your VPN server and upload to the router switch which is Open VPN client. However, while you just want to establish site to site VPN connectivity, install another Open VPN server may consume lots of cost and engineer effort.

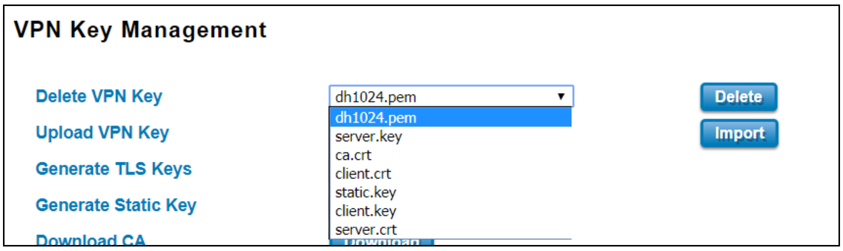
In the latest firmware, the WoMaster Secure Router Switch supports Key generation feature. Click **“Generate”** in **“Generate TLS Keys”** and **“Generate Static Key” in the Open VPN Router**, the system prompts you to wait 30 seconds to generate the key. Click “Yes” to start and wait 30 seconds. After generated, there are some VPN key/CA files generated and stored within the system. The files include both OpenVPN Server and Client key/ca files.

The two key/ca files, **dh1024.pem and server.crt** are applied to Open VPN Server only. The two files must be stored within the Open VPN server. **For security concern, the files are not allowed to download. You just need to generate the keys while configured the Router as an Open VPN Server.**

The rest of key/ca files include **CA, Client Cert and Client Key**. The three files must be stored within both the Open VPN server and client. You can download the keys to your PC and upload the files to OpenVPN client. Then the client has the same key. This is usefully tool for you to build you OpenVPN connectivity.

If you prefer to use Static Key, you can generate the **static.key** in OpenVPN Server and put the key in both OpenVPN Server and Clients.

You can see the files’ name by select the drop-down menu of “Delete VPN Key”, download/import OpenVPN client key/ca files in below columns.



VPN Key Management

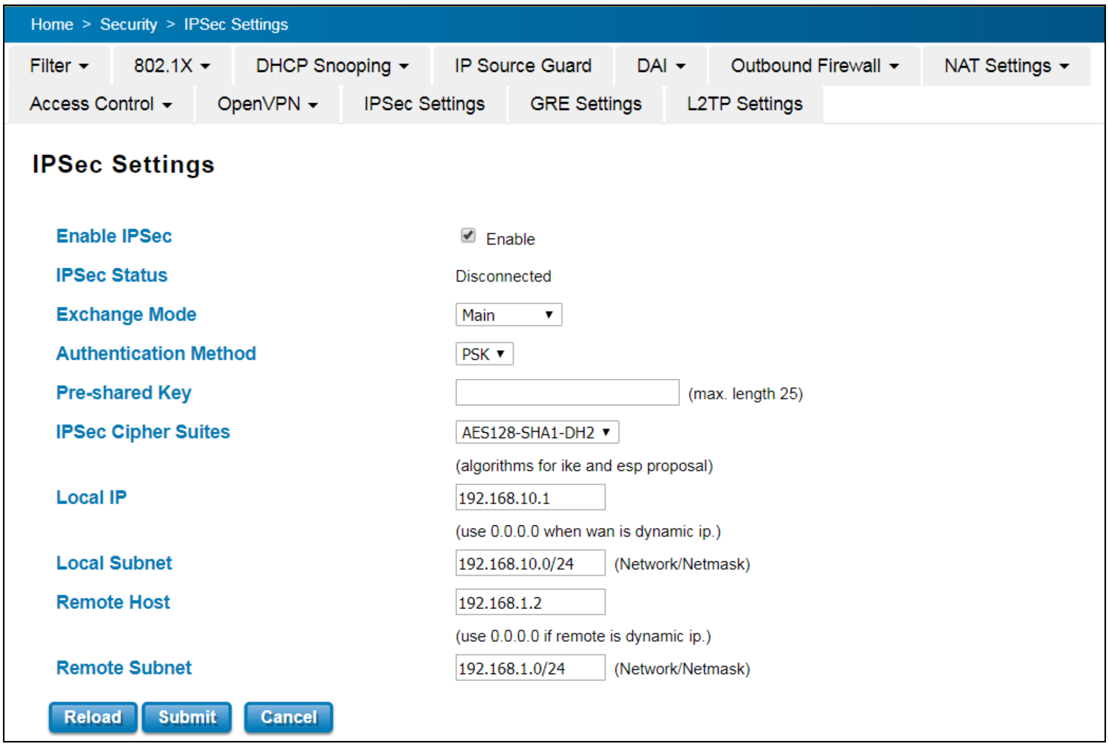
Delete VPN Key dh1024.pem
Upload VPN Key
Generate TLS Keys
Generate Static Key
Download CA

The description of the columns is as below:

TERMS	DESCRIPTION
Delete VPN Key	Display the ca/key files after generated TLS/Static Key. You can select and Delete the ca/key file here.
Upload VPN Key	Upload a certificate file from a specified file location.
Generate TLS Keys	The setting allows you to generate TLS key/ca files by the router switch. After click Generate, the system prompts you to wait 30 seconds to generate the key. Click Yes to start…then you will have multiple key/ca files.
Generate Static Key	The setting allows you to generate Static key by the router switch. After click Generate, the system prompts you to wait 30 seconds to generate the key. Click Yes to start… then you will have static.key file in the system.
Download CA	Download the generated ca.crt file here. Copy and Upload the key to the OpenVPN client Router.
Download Client Cert	Download the generated client.crt file here. Copy and Upload the key to the OpenVPN client Router.
Download Client Key	Download the generated client.key file here. Copy and Upload the key to the OpenVPN client Router.
Download Static Key	Download the generated static.key file here. Copy and Upload the key to the OpenVPN client Router while you prefer to establish OpenVPN connectivity by using Static Key.

3.10.7 IPSEC SETTING

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. By configure this configuration page, user allows IPsec tunnels to pass through the router.



IPSec Settings

Enable IPSec	☑ Enable
IPSec Status	Disconnected
Exchange Mode	Main
Authentication Method	PSK
Pre-shared Key	(max. length 25)
IPSec Cipher Suites	AES128-SHA1-DH2 (algorithms for ike and esp proposal)
Local IP	192.168.10.1 (use 0.0.0.0 when wan is dynamic ip.)
Local Subnet	192.168.10.0/24 (Network/Netmask)
Remote Host	192.168.1.2 (use 0.0.0.0 if remote is dynamic ip.)
Remote Subnet	192.168.1.0/24 (Network/Netmask)

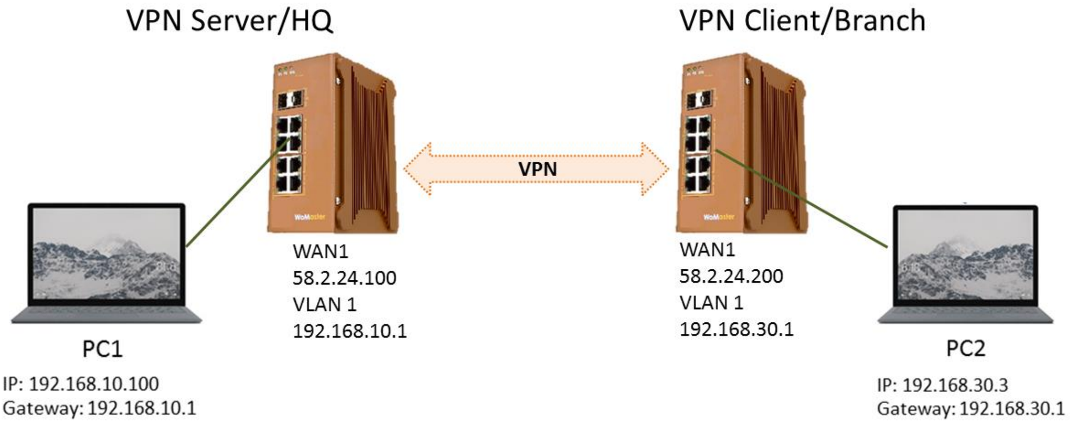
The description of the columns is as below:

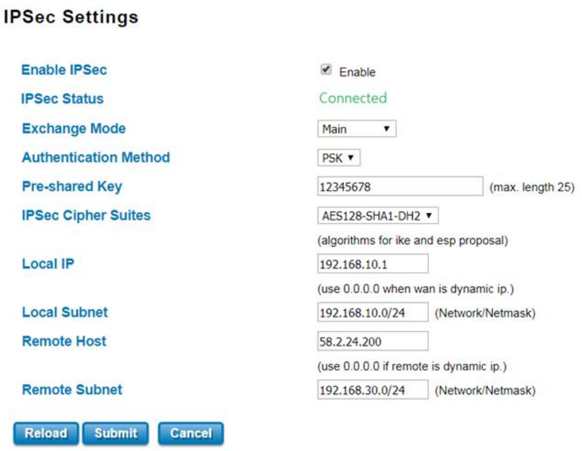
TERMS	DESCRIPTION
Enable IPsec	Select Enable to activate the IPsec function
IPsec Status	Display the IPsec status, whether it is connected or disconnected. When the VPN is connected, the IPsec status will display “Connected”. IPsec Status Connected
Exchange Mode	Main or Aggressive mode selection
Authentication Method	Default: PSK Optional: Pre Shared Key or Certificate
Pre-shared key	**Default: none** Type the Pre-shared key. The Pre-share key must be the same in both ends.
IPsec Cipher Suites	**Default: AES128-SHA1-DH2** Set algorithms for IKE and ESP proposal, choose AES128-SHA1-DH2, DES-SHA1-DH2, 3DES-SHA1-DH2 and AES256-SHA1-DH2. The cipher must be the same in both ends.
Local IP	IP Address of the local side of the tunnel. (Use 0.0.0.0 when WAN is dynamic IP.)
Local Subnet	Set IPSec local protected subnet and subnet mask, i.e. 192.168.1.0/24
Remote Host	**Default: 0.0.0.0** Set IPsec Remote Host, use the default setting if remote is dynamic IP

Remote Subnet	Set IPsec Remote Protected Subnet/Subnet Netmask

Click **Submit** to apply the configuration.

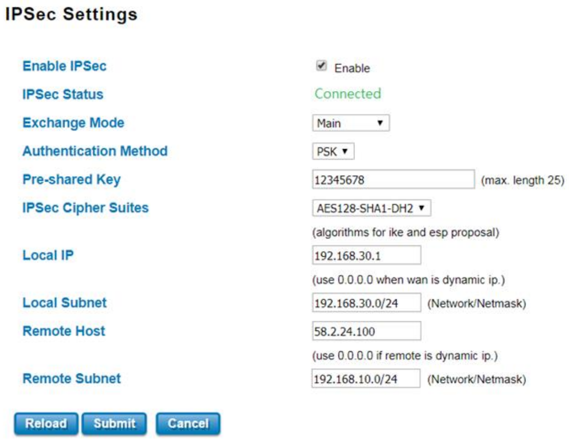
An Example of IPSec VPN:





IPSec Settings

Enable IPSec	☑ Enable
IPSec Status	Connected
Exchange Mode	Main ▾
Authentication Method	PSK ▾
Pre-shared Key	12345678 (max. length 25)
IPSec Cipher Suites	AES128-SHA1-DH2 ▾ (algorithms for ike and esp proposal)
Local IP	192.168.10.1 (use 0.0.0.0 when wan is dynamic ip.)
Local Subnet	192.168.10.0/24 (Network/Netmask)
Remote Host	58.2.24.200 (use 0.0.0.0 if remote is dynamic ip.)
Remote Subnet	192.168.30.0/24 (Network/Netmask)



IPSec Settings

Enable IPSec	☑ Enable
IPSec Status	Connected
Exchange Mode	Main ▾
Authentication Method	PSK ▾
Pre-shared Key	12345678 (max. length 25)
IPSec Cipher Suites	AES128-SHA1-DH2 ▾ (algorithms for ike and esp proposal)
Local IP	192.168.30.1 (use 0.0.0.0 when wan is dynamic ip.)
Local Subnet	192.168.30.0/24 (Network/Netmask)
Remote Host	58.2.24.100 (use 0.0.0.0 if remote is dynamic ip.)
Remote Subnet	192.168.10.0/24 (Network/Netmask)

The reference topology above is how the branch office can get the access to the headquarter. The two laptops are connected to the secure router switch through the Ethernet cable.

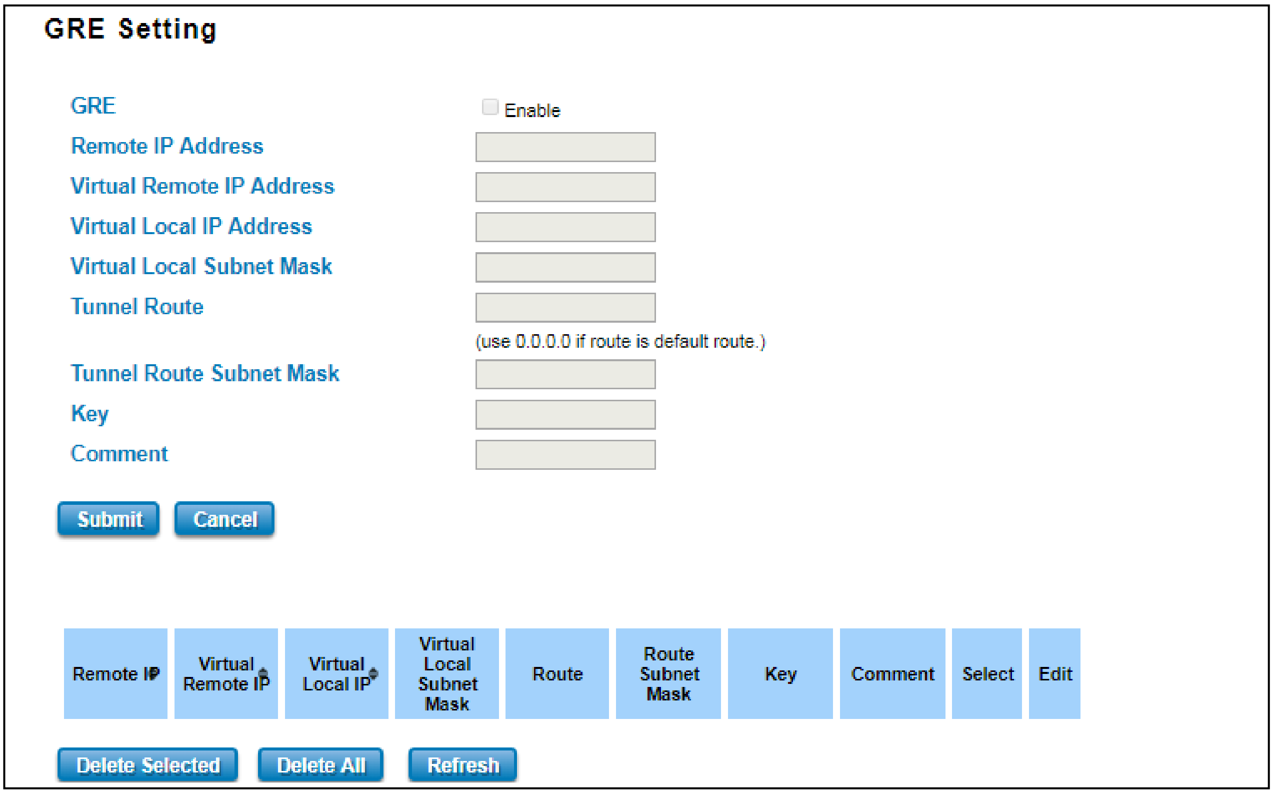
Enable the IPSec, type the same pre-share key and select the same cipher for both ends.

Configure the IP address for both ends. The Router at the branch office normally acts as the VPN Client role (not really client mode in IPSec), the Router at head quarter normally acts as the VPN Server role. The HQ normally has public IP, that's the Remote IP of the router in branch office. The local subnet in HQ is the remote subnet of the router in branch office. If you have public IP in branch, it's better to use public IP address for the WAN interface. If you just have dynamic IP address for branch office, then use 0.0.0.0 as local IP.

To check the connection status, you can use Ping tool in Router's Web GUI to check the WAN connection. You must ping remote WAN IP address successfully first. Then you can try ping from PC2 to its connected interface, WAN IP of two routers and then remote PC1. This is also the typical debugging rule to check WAN and VPN connectivity.

3.10.8 GRE SETTING

GRE (Generic Routing Encapsulation RFC2784) is a solution for tunneling RFC1812 private address-space traffic over an intermediate TCP/IP network such as the Internet. GRE tunneling does not use encryption it simply encapsulates data and sends it over the WAN port only. This page allows user to set up GRE tunnels and view information about the amount of data transmitted and received.



GRE Setting

GRE	□ Enable
Remote IP Address	
Virtual Remote IP Address	
Virtual Local IP Address	
Virtual Local Subnet Mask	
Tunnel Route	(use 0.0.0.0 if route is default route.)
Tunnel Route Subnet Mask	
Key	
Comment	

Remote IP	Virtual Remote IP	Virtual Local IP	Virtual Local Subnet Mask	Route	Route Subnet Mask	Key	Comment	Select	Edit

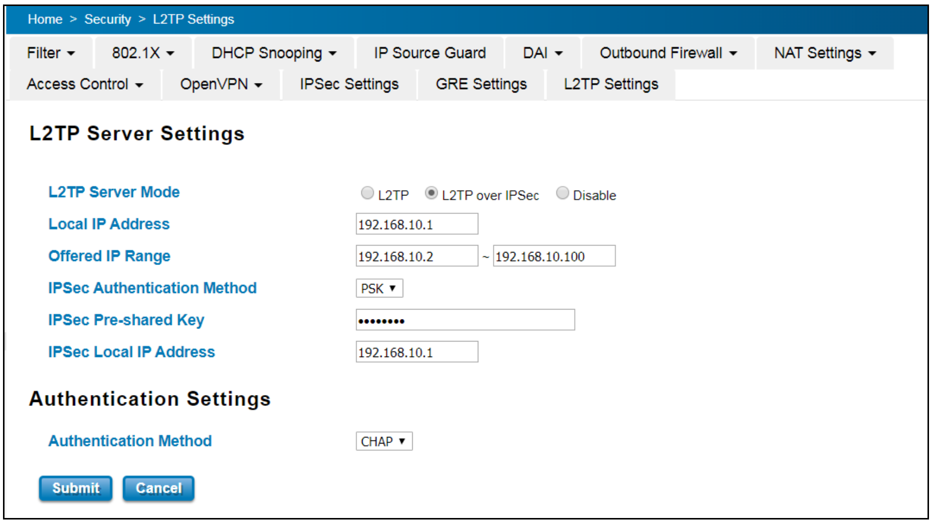
The description of the column is as below:

TERMS	DESCRIPTION
GRE	Check the box to enable the function.
Remote IP Address	Set the remote real IP Address of the GRE Tunnel
Virtual Remote IP Address	Set the remote virtual IP Address of the GRE tunnel.
Virtual Local IP Address	Set the local virtual IP Address of the GRE tunnel.
Virtual Local Subnet Mask	Set the remote virtual Netmask of the GRE tunnel.
Tunnel Route	Route, the default value is 0.0.0.0
Tunnel Route Subnet Mask	Set the subnet mask for the route
Key	Enter the key for the GRE tunnel.
Comment	Enter any comment to describe the configuration.
Select	Select the list on the table, so user can press **Edit** or **Delete Selected** to delete.

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

3.10.9 L2TP SETTING

L2TP stands for Layer 2 Tunneling Protocol. It is a VPN tunneling protocol that allows remote clients to use the public IP network to securely communicate with private corporate network servers.   The Secure Router Switch supports L2TP and additional L2TP over IPSec mode to provide L2TP with authentication and encryption. The L2TP over IPSec is popular and recommend since it provides higher security. While the Router Switch acts as L2TP Server, you can define the offered IP range, methods of Authentication type, key, handshake method and available user name/password for the connected L2TP clients. The Router Switch L2TP uses the authentication methods of PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol).



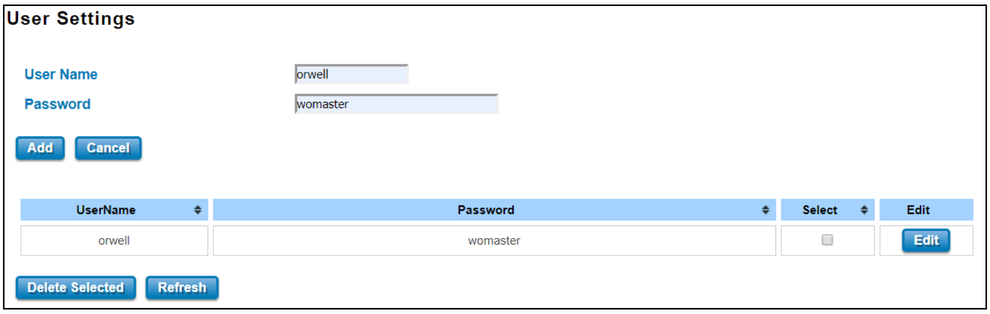
L2TP Server Settings

L2TP Server Mode	○ L2TP ● L2TP over IPSec ○ Disable
Local IP Address	192.168.10.1
Offered IP Range	192.168.10.2 ~ 192.168.10.100
IPSec Authentication Method	PSK
IPSec Pre-shared Key	••••••••
IPSec Local IP Address	192.168.10.1

Authentication Settings

Authentication Method	CHAP

The rest of the parameters are user preferential so you should set them as you need. The L2TP client can connect to the L2TP server by these UserName and Password.



User Settings

User Name	orwell
Password	womaster

UserName	Password	Select	Edit
orwell	womaster	□	Edit

The description of the column is as below:

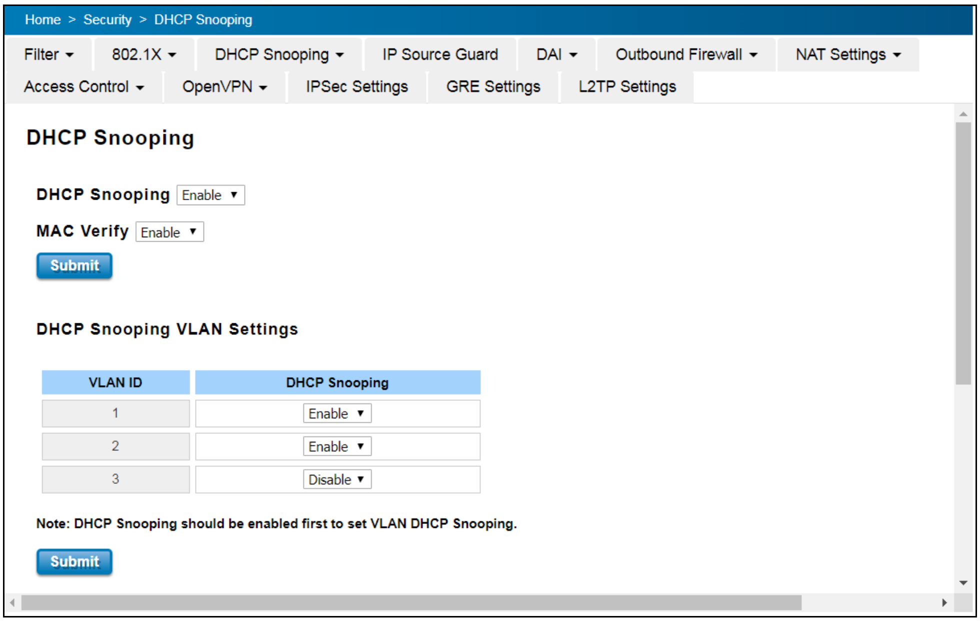
TERMS	DESCRIPTION
L2TP Server Mode	Select the L2TP or L2TP over IPSec mode. After select L2TP over IPSec mode, the Web GUI shows more settings, includes the IPSec Authentication Method, Pre-shared Key and Local IP Address setting.
Local IP Address	Set the local IP Address of the L2TP tunnel.
Offered IP Range	Set the IP range offered for the connected clients of the L2TP tunnel.
IPSec Authentication Method	Default: PSK Optional: Pre Shared Key or Certificate
IPSec Pre-shared Key	**Default: none**

	Type the Pre-shared key. The Pre-share key must be the same in both ends.
IPSec Local IP Address	IP Address of the local side of the L2TP tunnel.
Authentication Method	PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol)
User Setting	The group defines the available User Name and Password for the connected L2TP clients.
User Name	The User Name for the connected client
Password	The Password of the created User Name

3.10.10 DHCP Snooping

DHCP snooping is a security feature of DHCP and is mainly applied to switches.

The purpose of DHCP Snooping is to block illegal DHCP servers in the access network. That is, after the DHCP Snooping function is enabled, clients on the network can only obtain IP addresses from the DHCP server specified by the administrator. Due to the lack of authentication mechanism in DHCP protocol, if there is an illegal DHCP server in the network, the administrator will not be able to guarantee that the client obtains a legal address and the client may obtain the wrong IP address from the illegal DHCP server.



DHCP Snooping

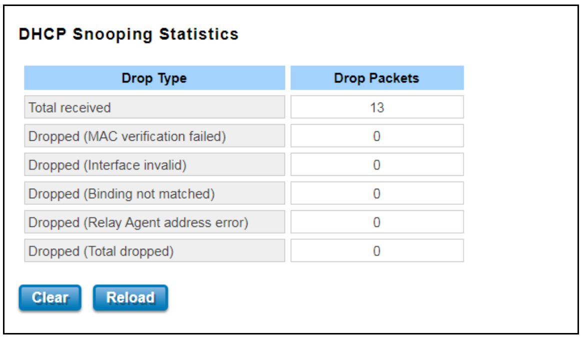
DHCP Snooping: Enable

MAC Verify: Enable

DHCP Snooping VLAN Settings

VLAN ID	DHCP Snooping
1	Enable
2	Enable
3	Disable

Note: DHCP Snooping should be enabled first to set VLAN DHCP Snooping.



DHCP Snooping Statistics

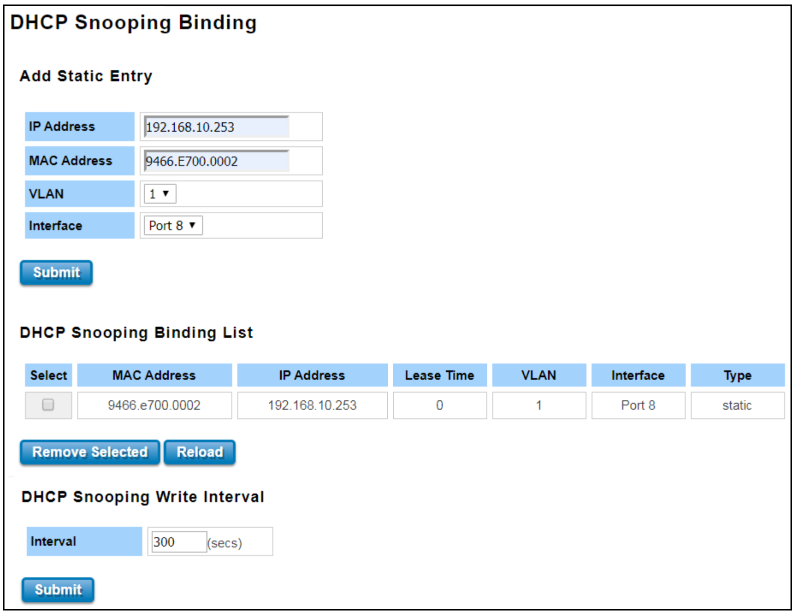
Drop Type	Drop Packets
Total received	13
Dropped (MAC verification failed)	0
Dropped (Interface invalid)	0
Dropped (Binding not matched)	0
Dropped (Relay Agent address error)	0
Dropped (Total dropped)	0

The description of the column is as below:

TERMS	DESCRIPTION
DHCP Snooping	Enable the DHCP Snooping function.
MAC Verify	Enable MAC Verify to start checking.
DHCP Snooping VLAN Setting	Enable DHCP Snooping for specific VLAN interface. DHCP Snooping should be enabled first then it’s available to Enable the DHCP Snooping for specific VLAN.
DHCP Snooping Statistics	The column shows the Drop Type and Drop Packets. It can help you check the status of your environment.

DHCP Snooping Binding

The Static Entry in DHCP Snooping Binding table allows to add tracking the specific IP Address and MAC Address for specific VLAN ID and LAN port. The DHCP Snooping Binding List table includes the client MAC address, IP address, DHCP lease time, binding type, VLAN number, and interface information on untrusted switch ports. The Trust/Untrust port setting can be configured in IP Source Guard page.



DHCP Snooping Binding

Add Static Entry

IP Address	192.168.10.253
MAC Address	9466.E700.0002
VLAN	1 ▾
Interface	Port 8 ▾

DHCP Snooping Binding List

Select	MAC Address	IP Address	Lease Time	VLAN	Interface	Type
□	9466.e700.0002	192.168.10.253	0	1	Port 8	static

DHCP Snooping Write Interval

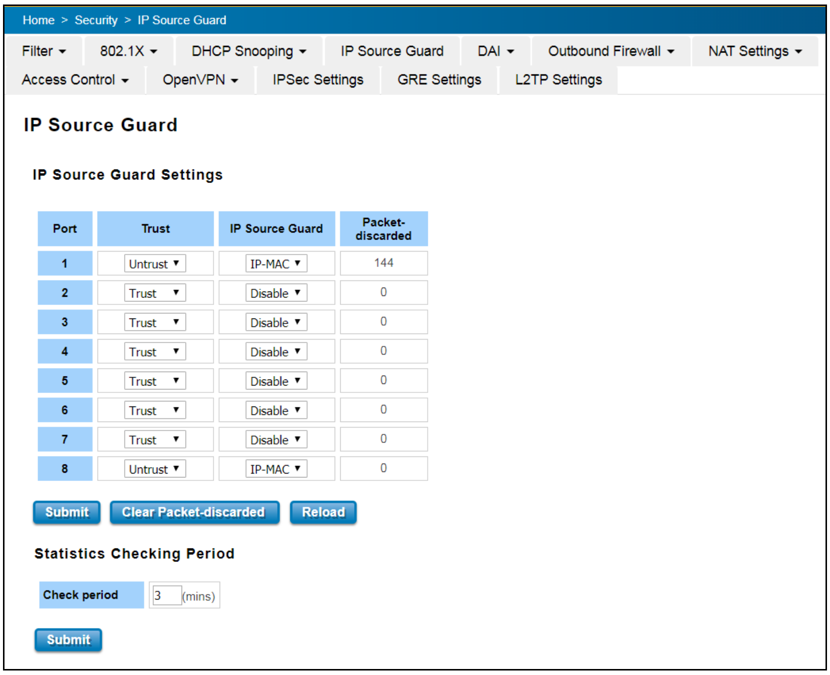
Interval	300 (secs)

The description of the column is as below:

TERMS	DESCRIPTION
IP Address	Type the IP address to bind the MAC Address of selected server.
MAC Address	Type the MAC address of the selected IP Address. The format should be like '0060.b312.3456'.
VLAN	Select the VLAN you'd like to apply.
Interface	Select the Port (LAN port) you'd like to apply.
DHCP Snooping Write Interval	Default: 300 secs

3.10.11 IP Source Guard

IP source guard can prevent the illegal use of IP by others, which is also a headache for many network managers. IP Source Guard is a security feature that restricts IP/IP-MAC traffic on untrusted L2 LAN ports by filtering traffic based on the DHCP snooping binding database.



IP Source Guard

IP Source Guard Settings

Port	Trust	IP Source Guard	Packet-discarded
1	Untrust	IP-MAC	144
2	Trust	Disable	0
3	Trust	Disable	0
4	Trust	Disable	0
5	Trust	Disable	0
6	Trust	Disable	0
7	Trust	Disable	0
8	Untrust	IP-MAC	0

Statistics Checking Period

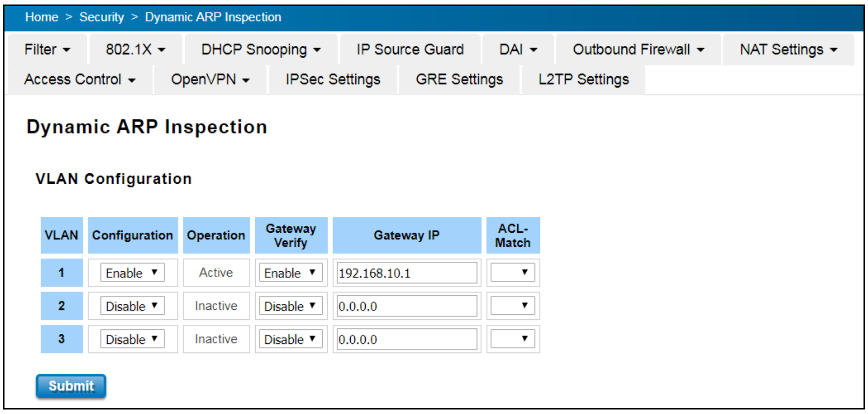
Check period: 3 (mins)

The description of the column is as below:

TERMS	DESCRIPTION
Trust	Select Trust/Untrust for each LAN port.
IP Source Guard	Select the Filter Type of IP or IP-MAC traffic.
Packet-discarded	The entry shows the discarded packet count of the port. You can manually click “Reload” to update the count. Or the system will update it based on the time of Statistic Checking Period.
Statistics Checking Period	It’s the time to update the count of discarded traffic.

3.10.12 DAI (Dynamic ARP Inspection)

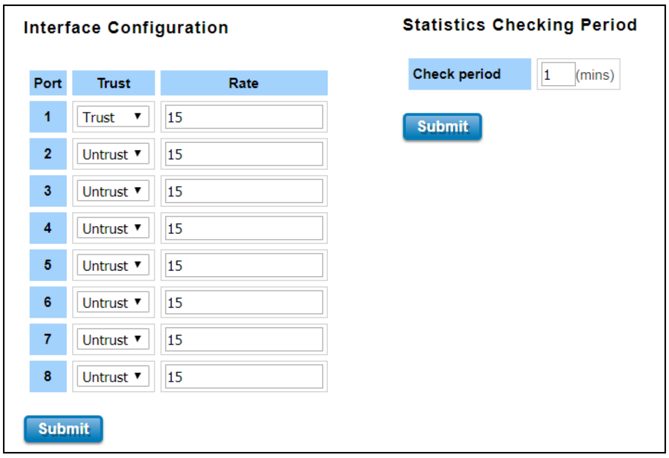
DAI (Dynamic ARP Inspection) provides IP address and MAC address binding on the switch and dynamically establishes a binding relationship. DAI is based on the DHCP Snooping binding table. For individual machines that do not use DHCP, you can use statically added ARP access-list. The DAI configuration is for VLANs. For interfaces in the same VLAN, DAI can be enabled or disabled. DAI can control the number of ARP request packets on a certain port. With this configuration, the problem of ARP attacks can be solved, and network security and stability can be better improved.



Dynamic ARP Inspection

VLAN Configuration

VLAN	Configuration	Operation	Gateway Verify	Gateway IP	ACL-Match
1	Enable	Active	Enable	192.168.10.1	
2	Disable	Inactive	Disable	0.0.0.0	
3	Disable	Inactive	Disable	0.0.0.0	



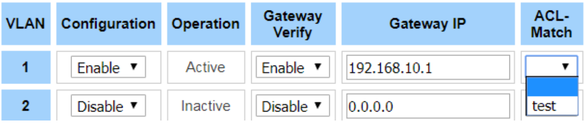
Interface Configuration

Port	Trust	Rate
1	Trust	15
2	Untrust	15
3	Untrust	15
4	Untrust	15
5	Untrust	15
6	Untrust	15
7	Untrust	15
8	Untrust	15

Statistics Checking Period

Check period 1 (mins)

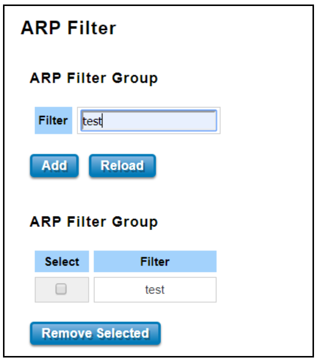
The description of the column is as below:

TERMS	DESCRIPTION
VLAN	Display the VLAN ID.
Configuration	Enable or Disable the DAI of the VLAN
Operation	Display the DAI operation state of the VLAN
Gateway Verify	Enable/Disable verify the Gateway
Gateway IP	Assign the target IP of Gateway Verify
ACL-Match	Select the target ARP filter rule. Need to set the rule in ARP Filter.  VLAN | Configuration | Operation | Gateway Verify | Gateway IP | ACL-Match 1 | Enable | Active | Enable | 192.168.10.1 | 2 | Disable | Inactive | Disable | 0.0.0.0 | test
Interface Configuration Port	The LAN Port ID

Trust	Select Trust/Untrust for each LAN port.
Rate	Configure the DAI rate limit of incoming ARP packets
Statistic Checking Period	It’s the time to update the count of DAI Statistics.

ARP Filter

Add the ARP Filter Name and then apply the ARP Filter Rule for it. Then you can see the Name/Rules in ARP Filter List table.



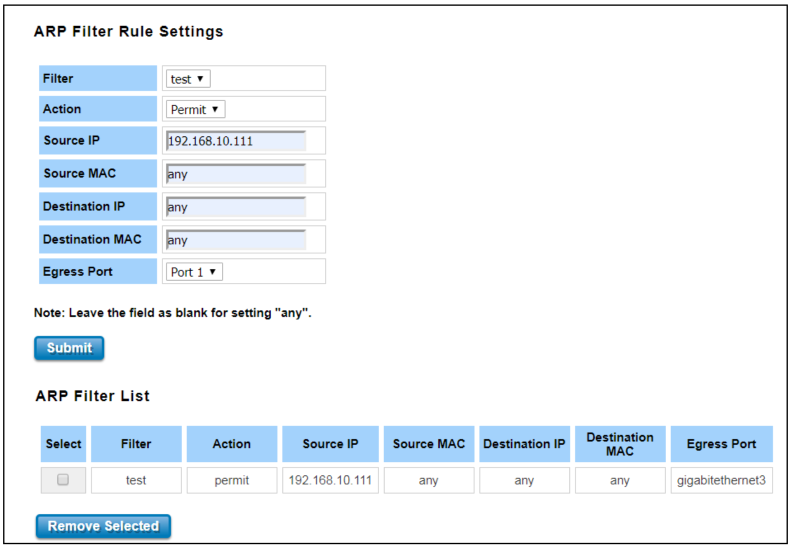
ARP Filter

ARP Filter Group

Filter: test

ARP Filter Group

Select	Filter
□	test



ARP Filter Rule Settings

Filter	test ▾
Action	Permit ▾
Source IP	192.168.10.111
Source MAC	any
Destination IP	any
Destination MAC	any
Egress Port	Port 1 ▾

Note: Leave the field as blank for setting "any".

ARP Filter List

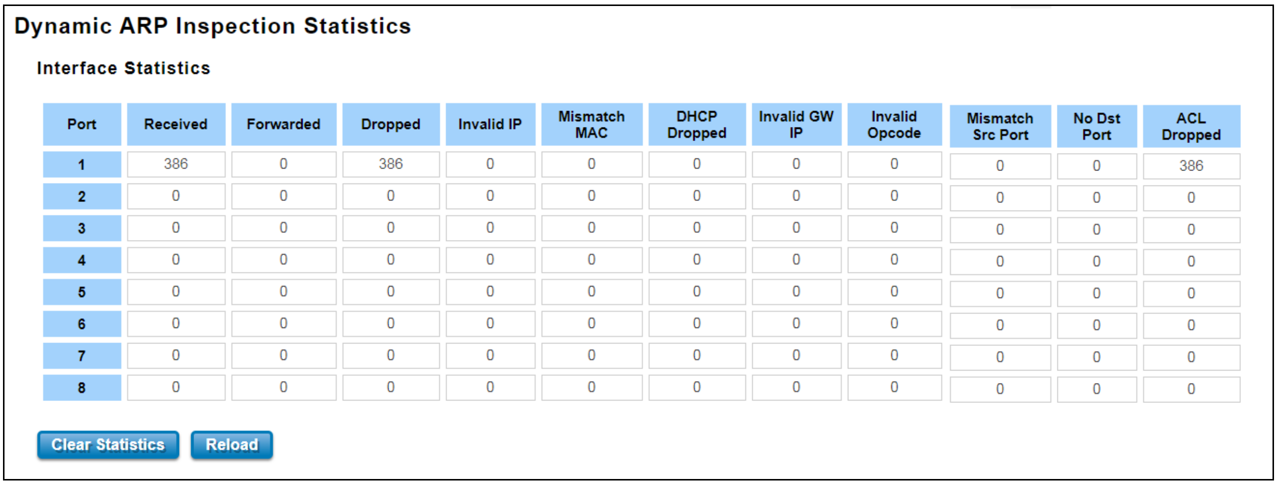
Select	Filter	Action	Source IP	Source MAC	Destination IP	Destination MAC	Egress Port
□	test	permit	192.168.10.111	any	any	any	gigabitethernet3

The description of the column is as below:

TERMS	DESCRIPTION
ARP Filter Group/Filter	Type “Name” of ARP Filter and click “Add”. The entry can be added in ARP Filter Group.
ARP Filter Rule Setting/Filter	Select the ARP Filter Entry then assign the parameters in below columns.
Action	Permit or Deny
Source IP	Configure specific IP Address for the rule. Blank/Any: All the coming source IP address.
Source MAC	Configure specific MAC Address for the rule. Blank/Any: All the coming source IP address.
Destination IP	Configure specific IP Address for the rule. Blank/Any: All the coming source IP address.
Destination MAC	Configure specific MAC Address for the rule. Blank/Any: All the coming source IP address.
Egress Port	Select the target Egress Port for the ARP Filter Entry.

Dynamic ARP Inspection Statistics

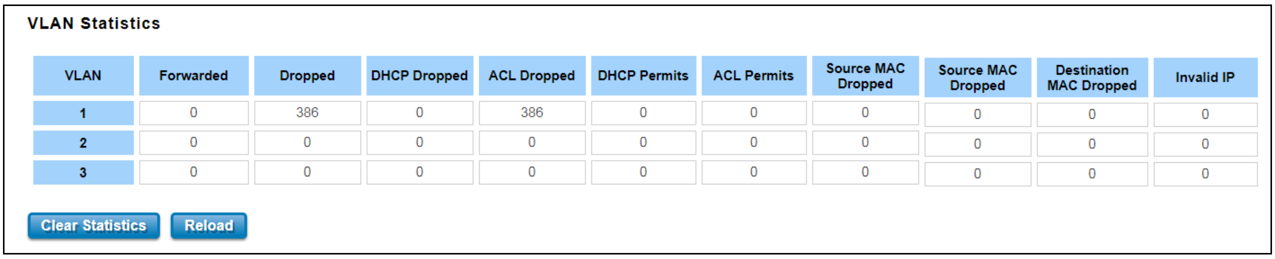
Below figures display the statistics of the Interface and VLAN for your reference. With the info, it can help you identify the overall status of the connected port and VLAN, this is used for network security diagnostic.



Dynamic ARP Inspection Statistics

Interface Statistics

Port	Received	Forwarded	Dropped	Invalid IP	Mismatch MAC	DHCP Dropped	Invalid GW IP	Invalid Opcode	Mismatch Src Port	No Dst Port	ACL Dropped
1	386	0	386	0	0	0	0	0	0	0	386
2	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0



VLAN Statistics

VLAN	Forwarded	Dropped	DHCP Dropped	ACL Dropped	DHCP Permits	ACL Permits	Source MAC Dropped	Source MAC Dropped	Destination MAC Dropped	Invalid IP
1	0	386	0	386	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0

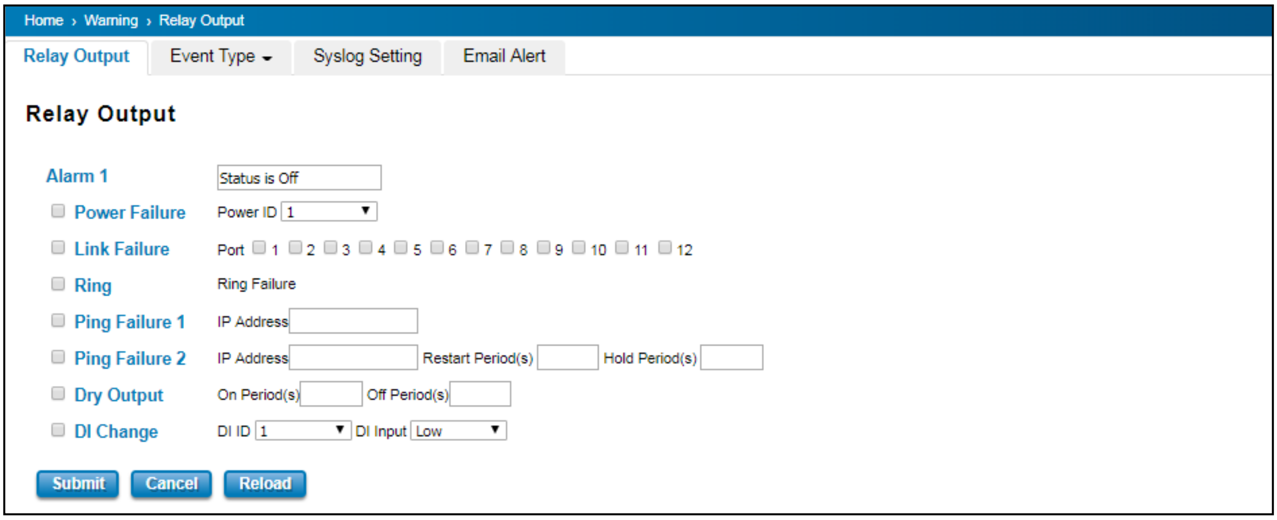
3.11 WARNING

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:



Relay Output

Alarm 1 Status is Off

□ Power Failure Power ID 1

□ Link Failure Port □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11 □ 12

□ Ring Ring Failure

□ Ping Failure 1 IP Address

□ Ping Failure 2 IP Address Restart Period(s) Hold Period(s)

□ Dry Output On Period(s) Off Period(s)

□ DI Change DI ID 1 DI Input Low

The condition or term described as following table.

TERMS	CONDITION	DESCRIPTION
Power Failure	Power ID 1 Power ID 2 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.

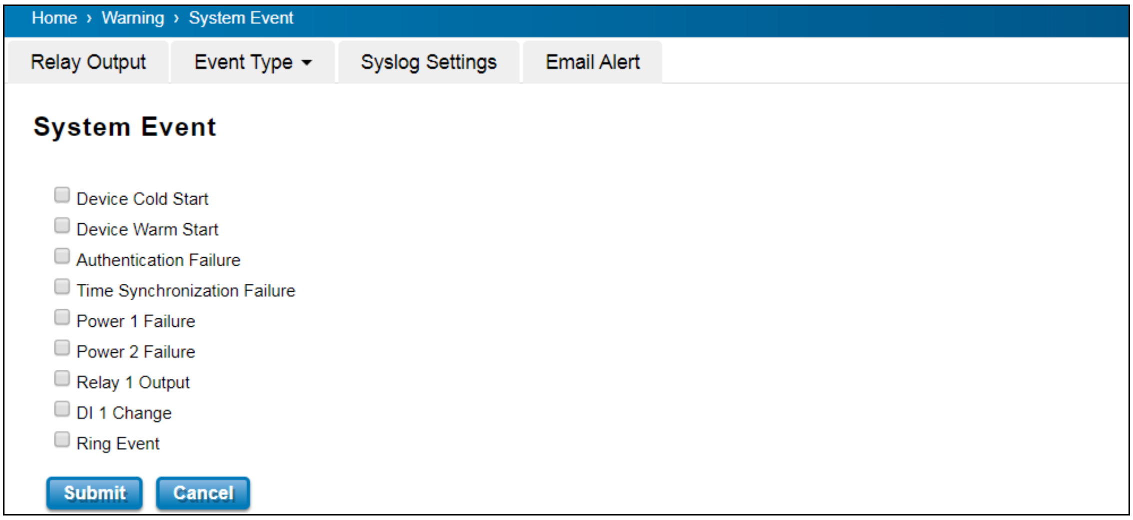
	Off period: duration of relay output open.	
DI Change	DI number (the switch supports 1 DI)	Relay trigger when DI states change to Hi or Low

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

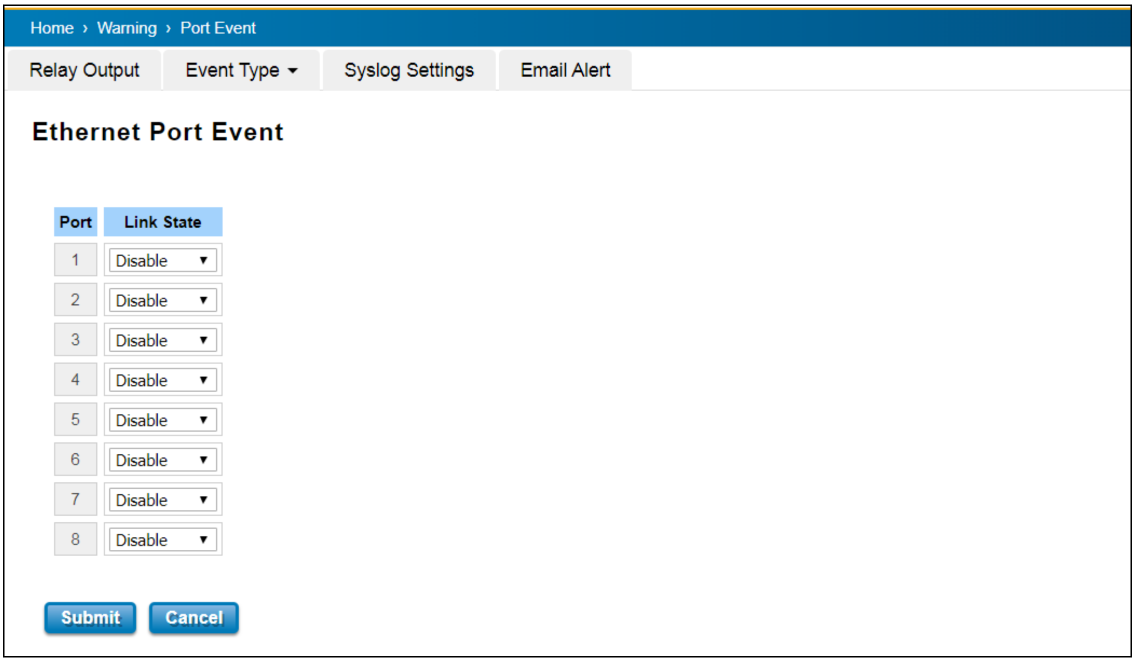
Event Types can be divided into two basic groups: System Event and Port Event. System Event are related to the overall function of the switch, whereas Port Event related to the activity of specific ports

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



System Event

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



Ethernet Port Event

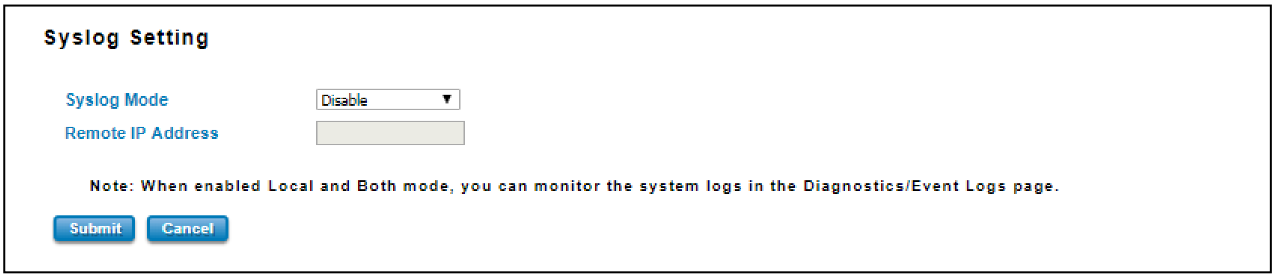
Port	Link State
1	Disable
2	Disable
3	Disable
4	Disable
5	Disable
6	Disable
7	Disable
8	Disable

The description of the columns is as below:

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

3.11.3 SYSLOG SETTING

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



Syslog Setting

Syslog Mode: Disable ▼

Remote IP Address:

Note: When enabled Local and Both mode, you can monitor the system logs in the Diagnostics/Event Logs page.

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

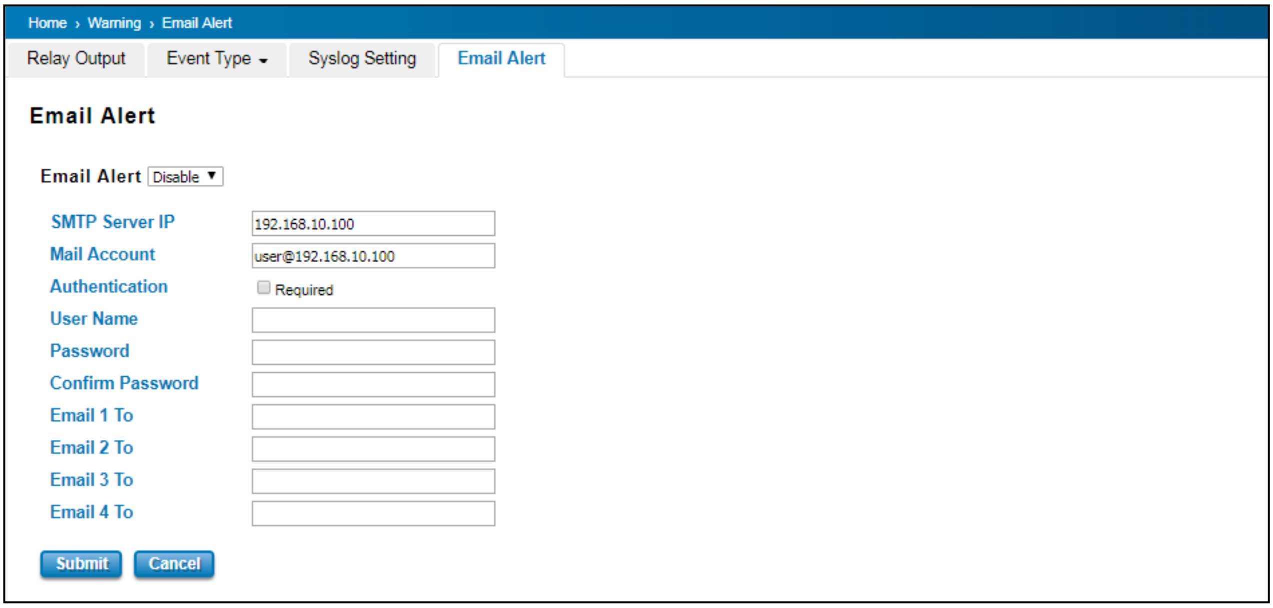
Remote Mode: In this mode, User should assign the IP address of the System Log server. Then the selected occurred events will be sent to System Log server User assigned.

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

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

3.11.4 EMAIL ALERT

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



Email Alert

Email Alert Disable

SMTP Server IP 192.168.10.100

Mail Account user@192.168.10.100

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

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

3.12 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

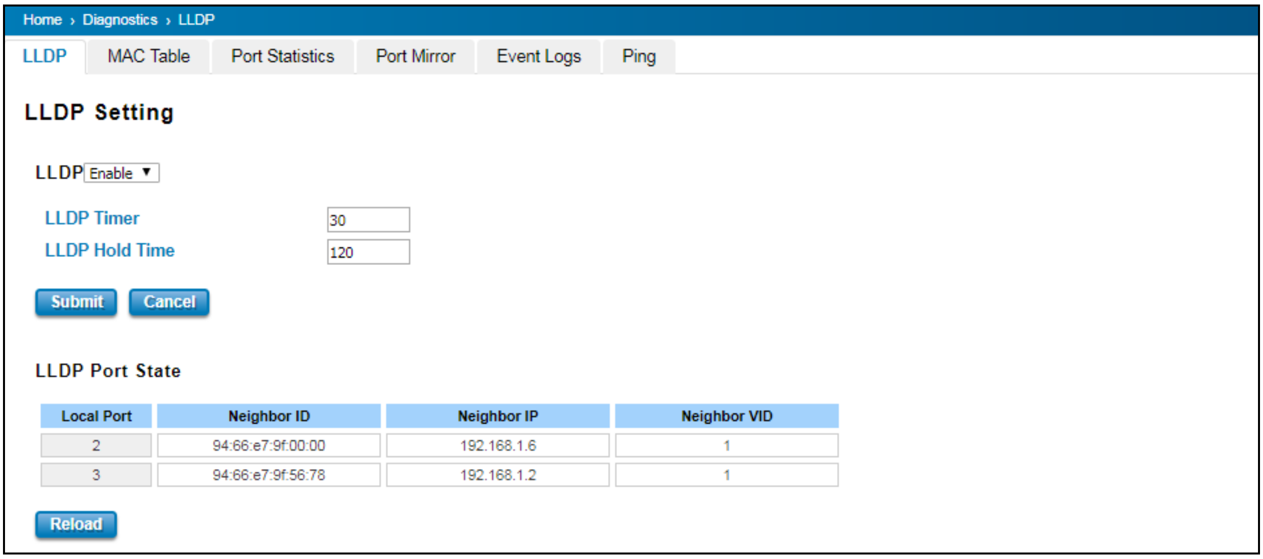
3.12.6 Ping

3.12.7 ARP Table Settings

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 leant from the connected devices.

The configuration and settings explain as following.



LLDP Setting

LLDP Enable

LLDP Timer 30

LLDP Hold Time 120

LLDP Port State

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.

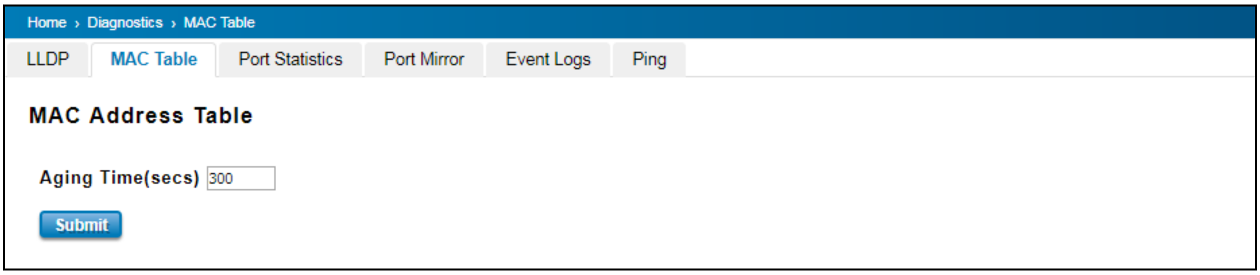
LLDP Hold time	**Default: 120 seconds** The TTL (Time To Live) timer. The LLDP state will be expired once the LLDP is not received by the hold time.
Local port	The current port number that linked with neighbor network device.
Neighbor ID	The MAC address of neighbor device on the same network segment.
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.

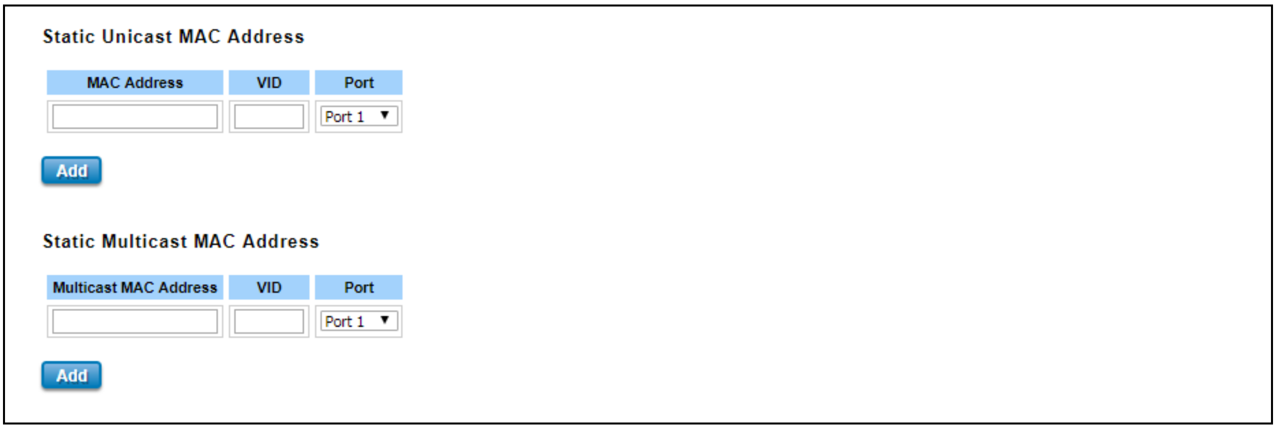


MAC Address Table

Aging Time(secs) 300

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.



Static Unicast MAC Address

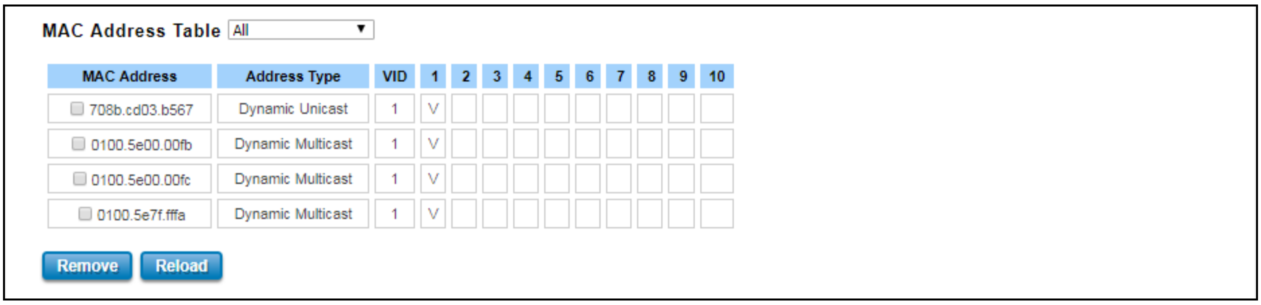
MAC Address	VID	Port
		Port 1 ▼

Static Multicast MAC Address

Multicast MAC Address	VID	Port
		Port 1 ▼

MAC Address Table

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



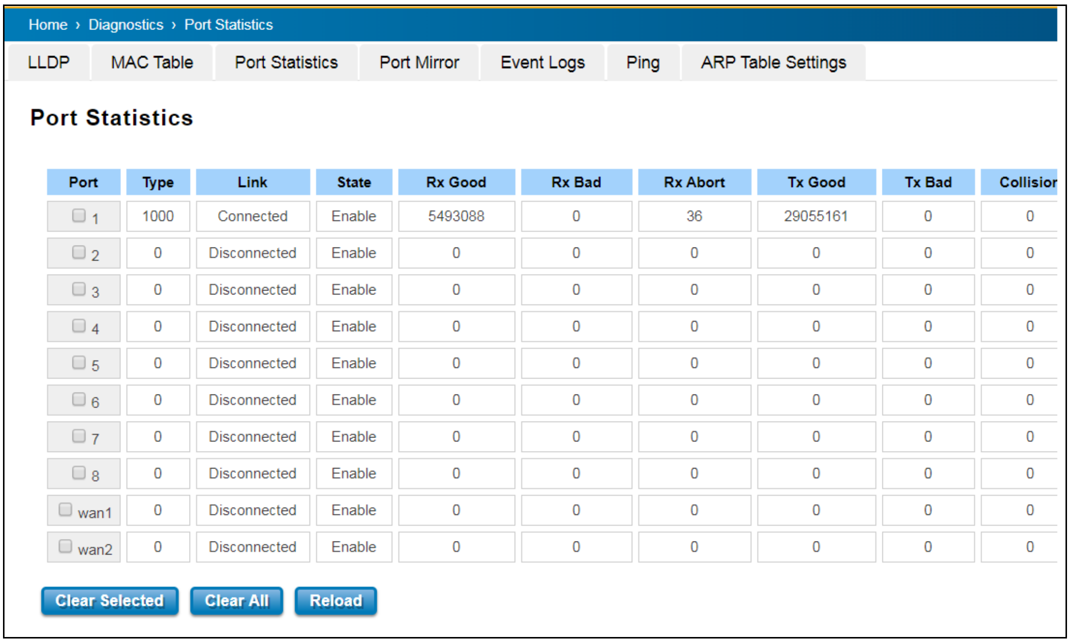
MAC Address Table All ▼

MAC Address	Address Type	VID	1	2	3	4	5	6	7	8	9	10
□ 708b.cd03.b567	Dynamic Unicast	1	V									
□ 0100.5e00.00fb	Dynamic Multicast	1	V									
□ 0100.5e00.00fc	Dynamic Multicast	1	V									
□ 0100.5e7f.fffa	Dynamic Multicast	1	V									

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

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



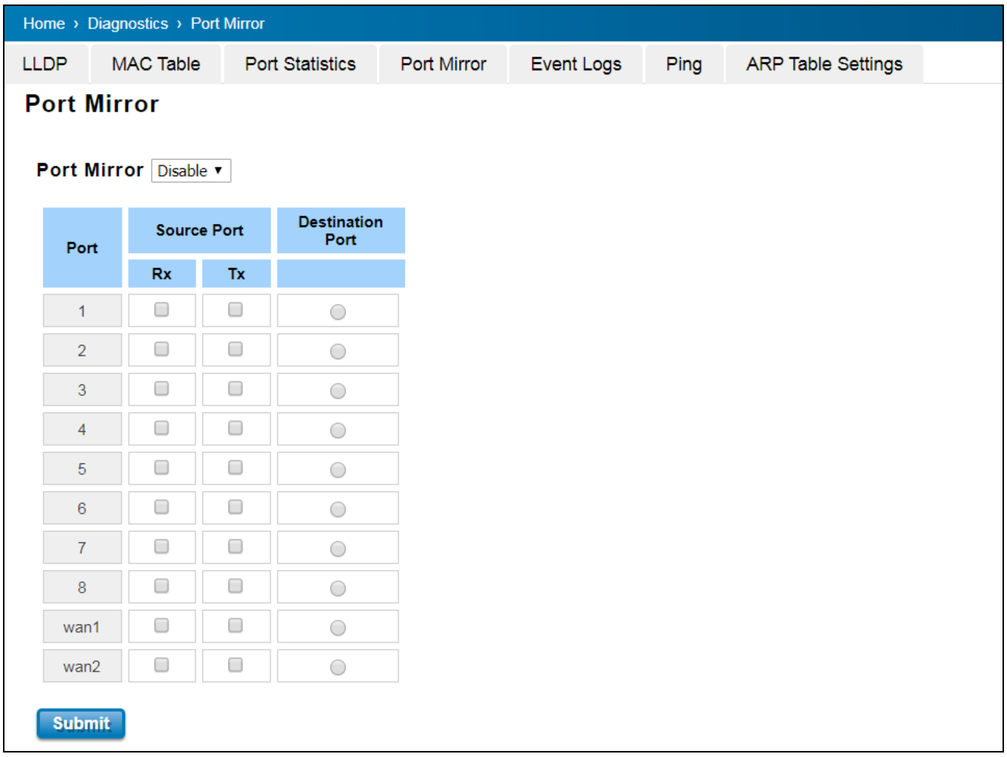
Port Statistics

Port	Type	Link	State	Rx Good	Rx Bad	Rx Abort	Tx Good	Tx Bad	Collisior
□ 1	1000	Connected	Enable	5493088	0	36	29055161	0	0
□ 2	0	Disconnected	Enable	0	0	0	0	0	0
□ 3	0	Disconnected	Enable	0	0	0	0	0	0
□ 4	0	Disconnected	Enable	0	0	0	0	0	0
□ 5	0	Disconnected	Enable	0	0	0	0	0	0
□ 6	0	Disconnected	Enable	0	0	0	0	0	0
□ 7	0	Disconnected	Enable	0	0	0	0	0	0
□ 8	0	Disconnected	Enable	0	0	0	0	0	0
□ wan1	0	Disconnected	Enable	0	0	0	0	0	0
□ wan2	0	Disconnected	Enable	0	0	0	0	0	0

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

3.12.4 PORT MIRROR

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



Port Mirror

Port Mirror: Disable

Port	Source Port		Destination Port
	Rx	Tx	
1	□	□	○
2	□	□	○
3	□	□	○
4	□	□	○
5	□	□	○
6	□	□	○
7	□	□	○
8	□	□	○
wan1	□	□	○
wan2	□	□	○

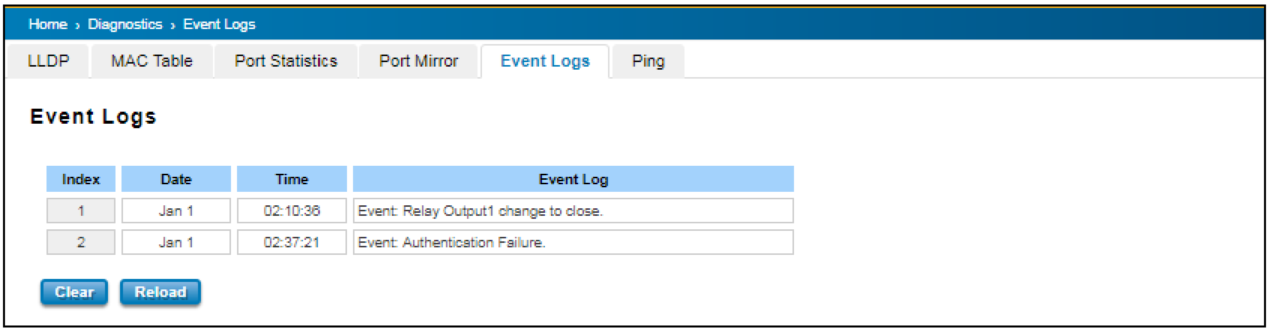
The configuration and settings explain as following.

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

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

3.12.5 EVENT LOGS

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



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.

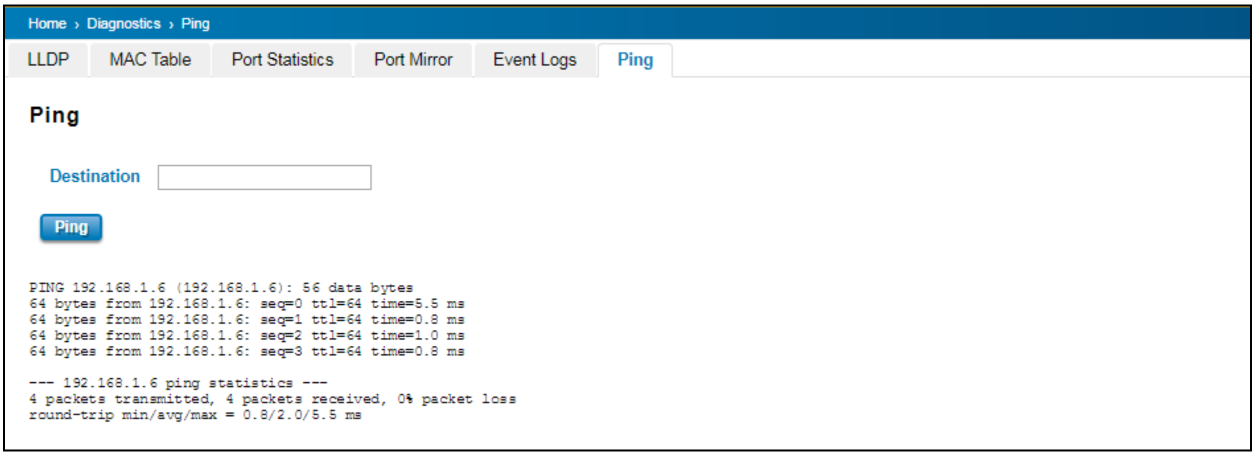
Click on **Clear** to clear the entries. Click on **Reload** to refresh the table.

The description of the columns is as below:

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

3.12.6 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.

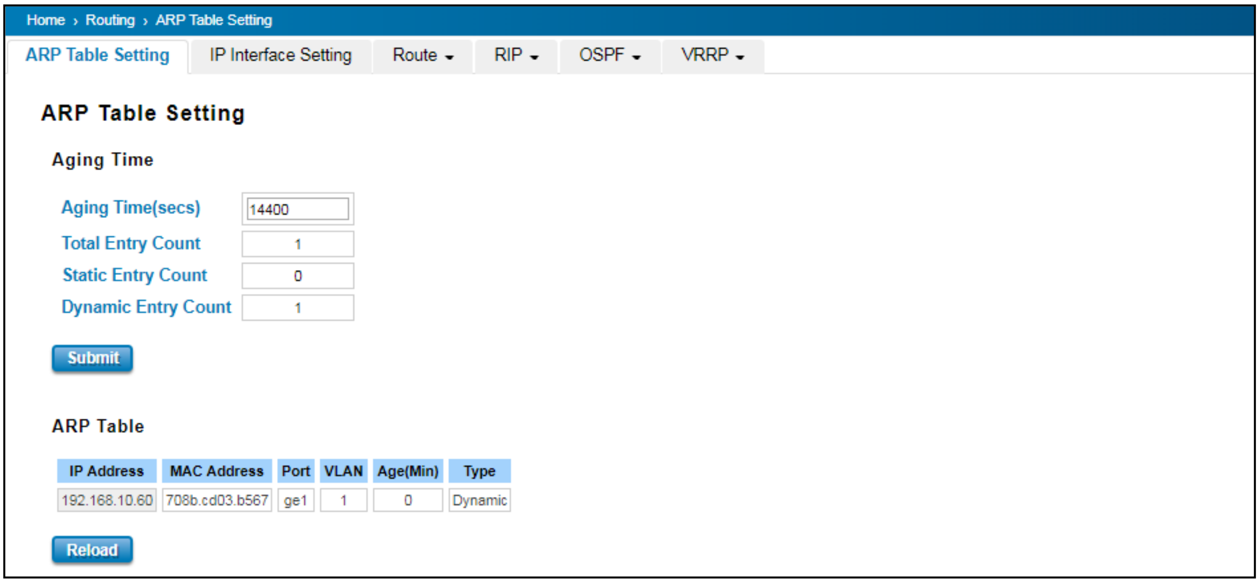


```
PING 192.168.1.6 (192.168.1.6): 56 data bytes
64 bytes from 192.168.1.6: seq=0 ttl=64 time=5.5 ms
64 bytes from 192.168.1.6: seq=1 ttl=64 time=0.8 ms
64 bytes from 192.168.1.6: seq=2 ttl=64 time=1.0 ms
64 bytes from 192.168.1.6: seq=3 ttl=64 time=0.8 ms

--- 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
```

3.12.7 ARP Table Settings

Address Resolution Protocol is a network layer protocol that query by broadcast and reply by unicast packet format. It assists IP protocol to get the MAC address of an IP destination due to the unique MAC address in the network. It is so important to find out the destination MAC address so then the traffic can be correctly and smoothly directed to the destination.

An ARP table is include the table with MAC Address/IP Address, and keep the information from the ARP reply, saving ARP operation for frequent communication and the entries are timeout with an aging mechanism. Below is the configuration page that allows user to configure the Age Time of the ARP entry and see the count of static and dynamic entry.



ARP Table Setting

Aging Time

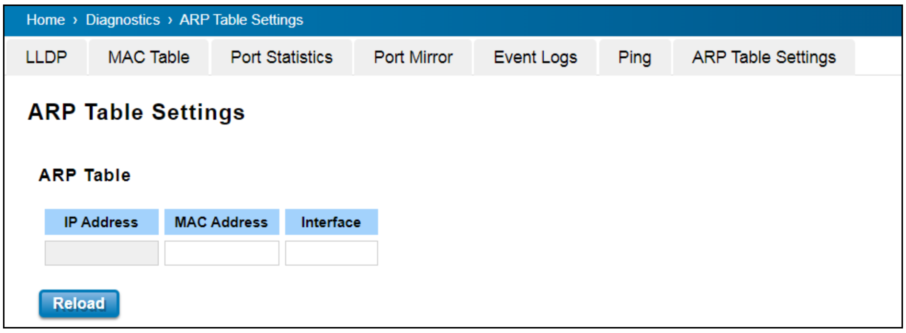
Aging Time(secs)	14400
Total Entry Count	1
Static Entry Count	0
Dynamic Entry Count	1

ARP Table

IP Address	MAC Address	Port	VLAN	Age(Min)	Type
192.168.10.60	708b.cd03.b567	ge1	1	0	Dynamic

TERMS	DESCRIPTION
Aging Time (secs)	**Default: 14400 seconds** Set the Age time for the ARP entry. Once there is no packet (IP+MAC) hit the entry within the time, the entry will be aged out. Short ARP age time leads the entry aged out easier and re-learn often, the re-learn progress lead the communication stop.
Total Entry Count	Count of total entries from the ARP Table.
Static Entry Count	Count the static entries that user configured.
Dynamic Entry Count	Count the ARP table dynamically learnt.

Click **Submit** to apply the configuration.



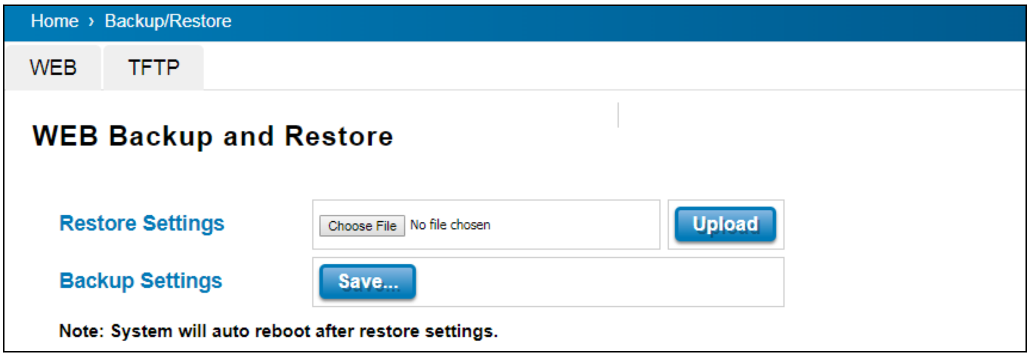
ARP Table Settings

ARP Table

IP Address	MAC Address	Interface

3.13 BACKUP AND RESTORE

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



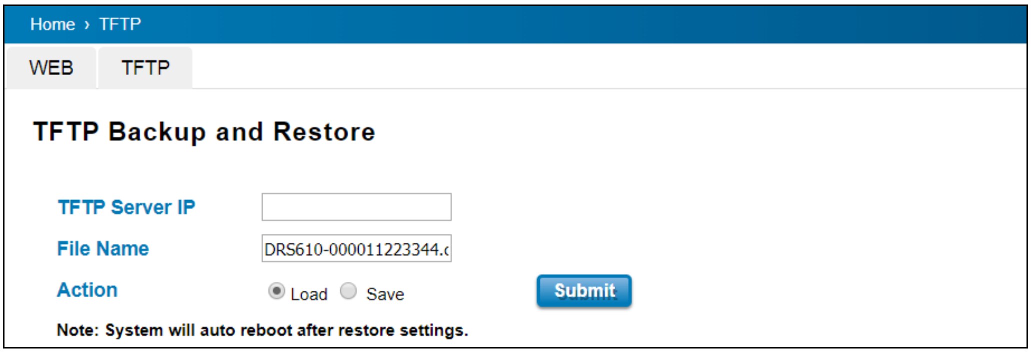
WEB Backup and Restore

Restore Settings: No file chosen

Backup Settings

Note: System will auto reboot after restore settings.

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 Backup and Restore

TFTP Server IP:

File Name: DRS610-000011223344.c

Action: ● Load ○ Save

Note: System will auto reboot after restore settings.

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:

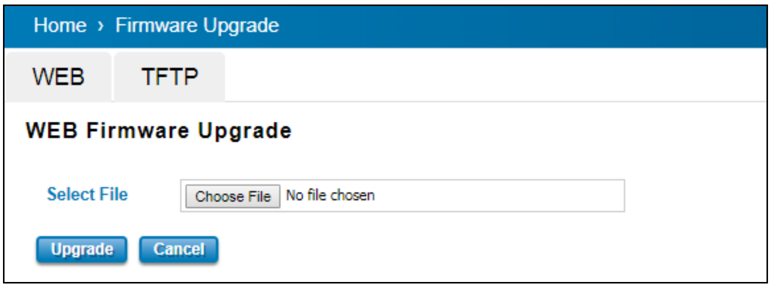
TERMS	DESCRIPTION
TFTP Server IP	User needs to key in the IP address of TFTP Server here.
File Name	Type the correct file name of the configuration file.
Configuration File (*.conf*)	The configuration file of the switch is a pure text file. User can open it by word/txt read file. User can also modify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

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.



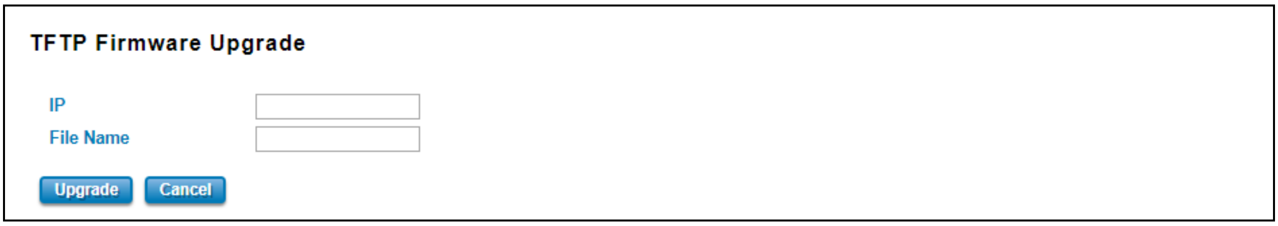
Home › Firmware Upgrade

WEB | TFTP

WEB Firmware Upgrade

Select File: Choose File No file chosen

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 Firmware Upgrade

IP:

File Name:

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:

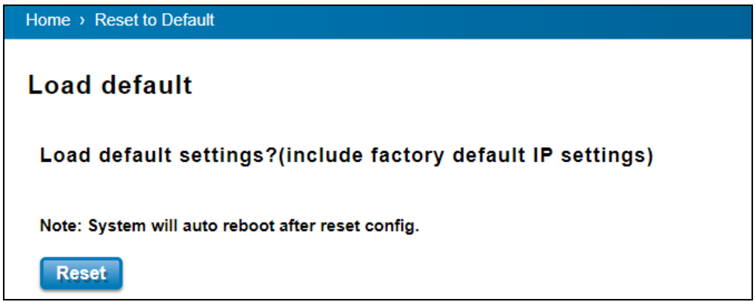
TERMS	DESCRIPTION
IP	User need to key in the IP address of TFTP Server here.
File Name	Type the correct file name of the configuration file.

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.

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.

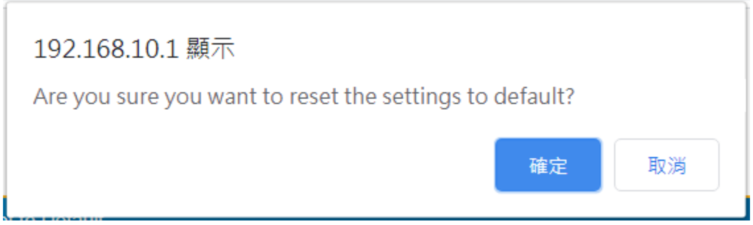
Factory Default main screen



Load default

Load default settings?(include factory default IP settings)

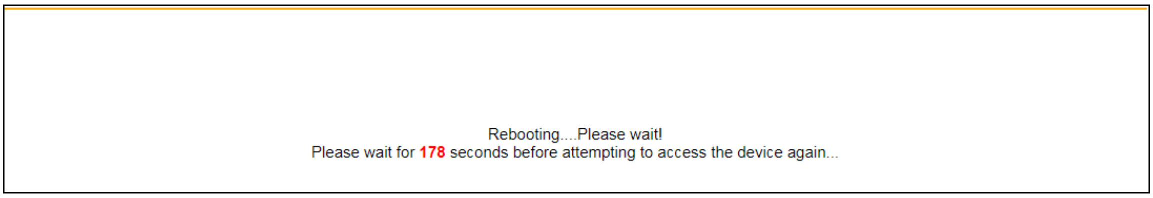
Note: System will auto reboot after reset config.



192.168.10.1 顯示

Are you sure you want to reset the settings to default?

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



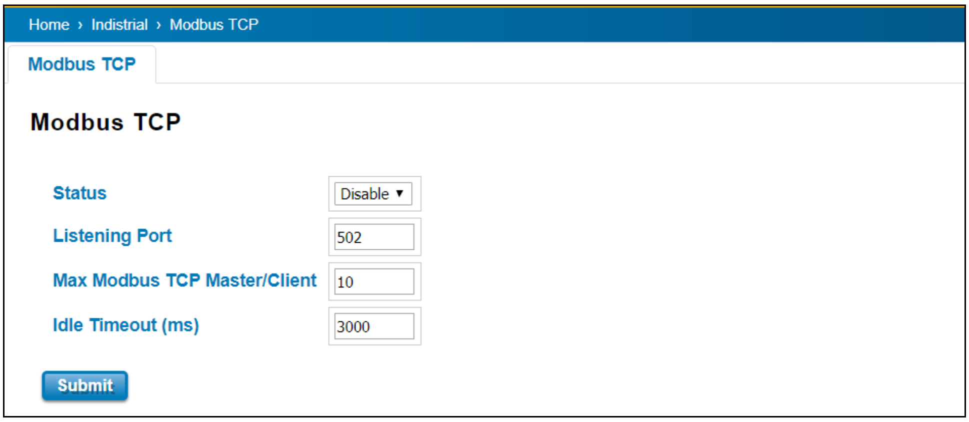
Rebooting....Please wait!
Please wait for 178 seconds before attempting to access the device again...

Hardware Reset

Once you forget the login user name or password. There is only one way to reset the switch to default. Press the “Reset” button more than 7 seconds on the bottom side of the switch. Less than 7 seconds is only available to reboot the switch.

3.16 INDUSTRIAL

WoMaster Switch's latest firmware provides Industrial Modbus features for User to monitor the status of the switch by Modbus TCP protocol. For example user can add the switch to their HMI dashboard and monitor the status by Modbus Read register.



Modbus TCP

Status: Disable
Listening Port: 502
Max Modbus TCP Master/Client: 10
Idle Timeout (ms): 3000

The description of the columns is as below:

TERMS	DESCRIPTION
Status	Select Enable/Disable to enable/disable Modbus TCP.
Listening Port	Set the TCP port for listening Modbus TCP message. The range of the number is 1 to 65535. The default is **502**.
Max Modbus TCP Master/Client	Set the maximum Modbus TCP Master/Client connection. The default is **10**.
Idle Timeout(ms)	Set the Idle Timeout for the Modbus TCP connection. The default=**3000ms**

Note: The value of Modbus TCP table in below is for reference example, different model may have different product name, description, system name…etc. Some of the new settings may be updated without earlier notice.

Run Modbus TCP poll tool to see the latest values or contact our technical window for up to date info.

The following table shows the Modbus TCP table Example:

Word Address	Data Type	Description
System Information		
0x0000	32 words	Product Name = "DRS610" (*Depends on product name) Word 0 Hi byte = 'D' Word 0 Lo byte = 'R' Word 1 Hi byte = 'S' Word 1 Lo byte = '6' Word 2 Hi byte = '1' Word 2 Lo byte = '0' …. (other words = 0)

0x0020	256 words	Product Description = " Industrial Managed Ethernet Switch" (*Depends on product description) Word 0 Hi byte = ‘I’ 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)
0x0120	128 words	SNMP system name (string)
0x01A0	128 words	SNMP system location (string)
0x0220	128 words	SNMP system contact (string)
0x02A0	32 words	SNMP system OID (string)
0x02C0	2 words	System uptime (unsigned long)
0x02C2 to 0x02FF	62 words	Reserved address space
0x0300	2 words	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
0x0302	2 words	Firmware 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 Ex: Version = v1.2 Word 0 Hi byte = 0x1 Word 0 Lo byte = 0x2 Word 1 Hi byte = 0x0 Word 1 Lo byte = 0x0 Version = v1.2.3 Word 0 Hi byte = 0x1 Word 0 Lo byte = 0x2 Word 1 Hi byte = 0x3 Word 1 Lo byte = 0x0 Version = v1.2.3.4 Word 0 Hi byte = 0x1 Word 0 Lo byte = 0x2 Word 1 Hi byte = 0x3 Word 1 Lo byte = 0x4
0x0304	2 words	Firmware Release Date Firmware was released on 2018-08-11 at 09 o'clock Word 0 = 0x0B09 Word 1 = 0x1208
0x0306	3 words	Ethernet MAC Address Ex: MAC = 01-02-03-04-05-06 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x02 Word 1 Hi byte = 0x03 Word 1 Lo byte = 0x04 Word 2 Hi byte = 0x05 Word 2 Lo byte = 0x06
0x0309 to 0x3FF	247 words	Reserved address space
0x0400	2 words	IP address Ex: IP = 192.168.10.1 Word 0 Hi byte = 0xC0 Word 0 Lo byte = 0xA8 Word 1 Hi byte = 0x0A Word 1 Lo byte = 0x01
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	1 word	DO1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0513	1 word	DO2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0514 to 0x051F	12 words	Reserved address space
0x0520	1 word	SYS LED (Green light) 0x0000:Off

		0x0001:On 0x0002: blinking 0x0003: blinking fast 0xFFFF: unavailable
0x0521	1 word	SYS LED(Yellow light) 0x0000:Off 0x0001:On 0x0002: blinking 0x0003: blinking fast 0xFFFF: unavailable
0x0522	1 word	R.S. LED (Green light) 0x0000:Off 0x0001:On 0x0002: blinking 0x0003: blinking fast 0xFFFF: unavailable
0x0523	1 word	R.S. LED (Yellow light) 0x0000:Off 0x0001:On 0x0002: blinking 0x0003: blinking fast 0xFFFF: unavailable
0x0524 to 0x0BFF	1756 words	Reserved address space
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: 10M-Half 0x0001: 10M-Full 0x0002: 100M-Half 0x0003: 100M-Full 0x0004: 1000M-Half 0x0005: 1000M-Full 0xFFFF: No port
0x1040 to	1 word	Flow Control

0x105F		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 0x14BF	32 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

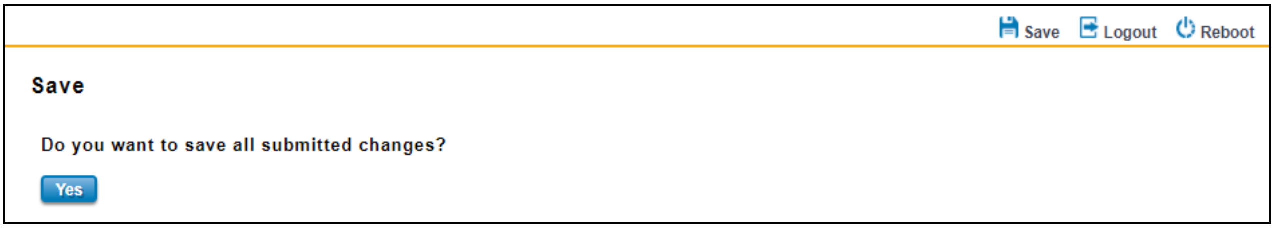
0x300B	1 word	Ring 0’s Ring Port 1 state 0x0000: disabled 0x0001: blocking 0x0002: listening 0x0003: learning 0x0004: forwarding
0x300C	1 word	Ring 0’s Ring Port 0 RMEP ID 0x0000: none 0x0001: RMEP ID = 1 0x0002: RMEP ID = 2 … 0x1FFF: RMEP ID = 8191 0xFFFF: unavailable
0x300D	1 word	Ring 0’s Ring Port 1 RMEP ID 0x0000: none 0x0001: RMEP ID = 1 0x0002: RMEP ID = 2 … 0x1FFF: RMEP ID = 8191 0xFFFF: unavailable
0x300E	1 word	Ring 0’s RPL port 0x0000: RPL port = Ring port 0 0x0001: RPL port = Ring port 1 0xFFFF: unavailable
0x300F	1 word	Ring 0’s Revertive Mode 0x0000: Revertive 0x0001: non-Revertive 0xFFFF: unavailable
0x3010	1 word	Ring 0’s Instance
0x3011	1 word	Ring 0’s Manual Switch 0x0000: Manual Switch port = Ring port 0 0x0001: Manual Switch port = Ring port 1 0x0001: Manual Switch port = none 0xFFFF: unavailable
0x3012	1 word	Ring 0’s Force Switch 0x0000: Force Switch port = Ring port 0 0x0001: Force Switch port = Ring port 1 0x0001: Force Switch port = none

		0xFFFF: unavailable
0x3013 to 0x301F	13 words	Reserved address space
0x3020 to 0x303F		ERPS Ring 1’s Information
0x3040 to 0x305F		ERPS Ring 2’s Information
0x3060 to 0x307F		ERPS Ring 3’s Information
0x3080 to 0x309F		ERPS 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		ERPS Ring 18’s Information

0x325F		
0x3260 to 0x327F		ERPS Ring 19’s Information
0x3280 to 0x329F		ERPS Ring 20’s Information
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

3.17 SAVE

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

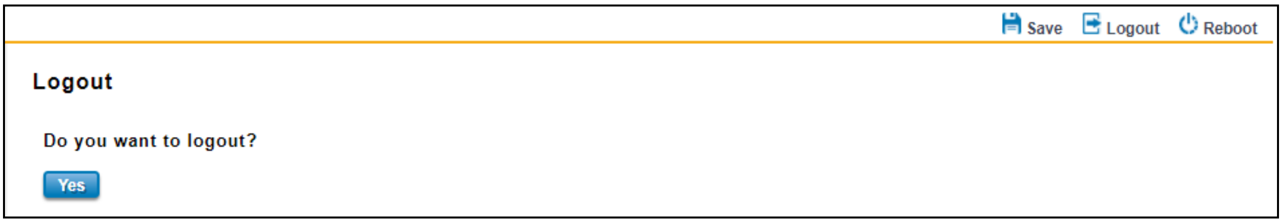


Save

Do you want to save all submitted changes?

3.18 LOGOUT

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



Logout

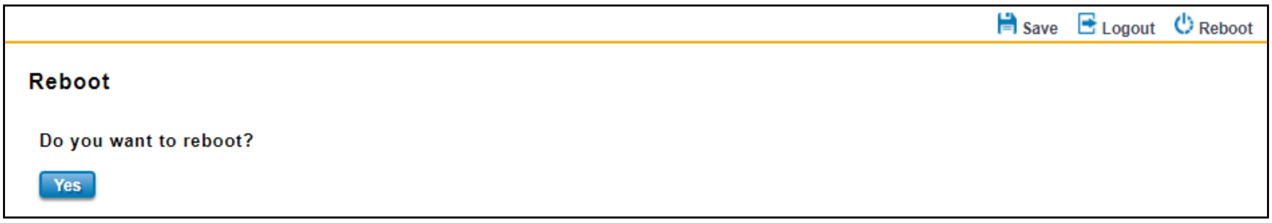
Do you want to logout?

3.19 REBOOT

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

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

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



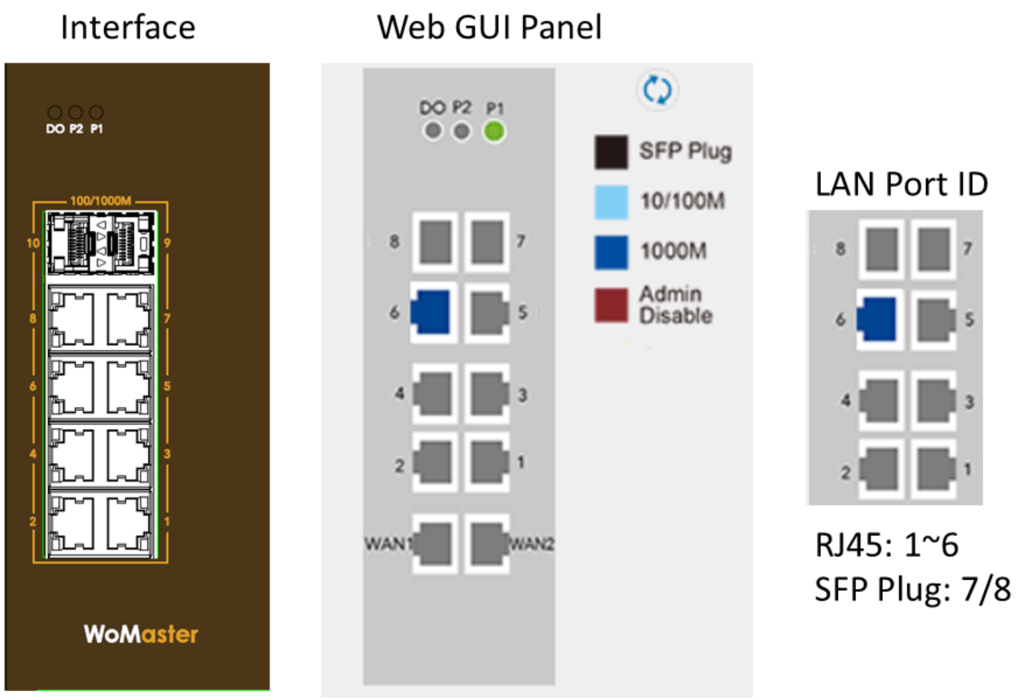
Reboot

Do you want to reboot?

3.20 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 and Ports. Front panel interface, can be seen on the web consoles. Shown as below.

Click ⟳ button to refresh and update the latest status.



The description of the Front Panel is as below:

Feature	LED On	LED off
P1/P2	Green on: Power is on	No power
DO/ALM	Red on: alarm relay active and contacts is short.	Red off: relay output contact is open.
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

4. SPECIFICATIONS

INTERFACE	DRS610	DS610
Ethernet Port	WAN Ports: 2 x 10/100/1000BaseTX RJ45, Auto Negotiation LAN Ports: 6 x 10/100/1000BaseTX RJ45, Auto Negotiation 2 x 100/1000 SFP , DDM	8 x 10/100/1000BaseTX RJ45, Auto Negotiation 2 x 100/1000 SFP, DDM
System LED	2 x Power: Green On 1 x DO: Red On	2 x Power: Green On 1 x DO: Red On
Ethernet Port LED	Link (Green On), Active (Green Blinking), Speed 1000M(Amber On), Speed 100M(Off)	Link (Green On), Active (Green Blinking), Speed 1000M(Amber On), Speed 100M(Off)
SFP Port LED	Link (Green On), Active (Green Blinking), Speed 1000M(Amber On), Speed 100M(Off)	Link (Green On), Active (Green Blinking), Speed 1000M(Amber On), Speed 100M(Off)
Reset	System Reboot(2-6 Seconds)/Default Settings Reset(over 7 seconds)	System Reboot(2-6 Seconds)/Default Settings Reset(over 7 seconds)
Console	1 x RS232 for System Configuration. Baud Rate: 115200.n.8.1	1 x RS232 for System Configuration. Baud Rate: 115200.n.8.1
Power Input, Digital Input, Digital Output	2x 4-Pin Removable Terminal Block Connector 4 Pins for Redundant Power 4 Pins for DI, DO (Relay Alarm) Digital Output: Dry Relay Output with 0.5A /24V DC Digital Input with Photo-Coupler Isolation Digital High: DC 11V~30V Digital Low: DC 0V~10V	2x 4-Pin Removable Terminal Block Connector 4 Pins for Redundant Power 4 Pins for DI, DO (Relay Alarm) Digital Output: Dry Relay Output with 0.5A /24V DC Digital Input with Photo-Coupler Isolation Digital High: DC 11V~30V Digital Low: DC 0V~10V
Power Requirement		
Input Voltage	24VDC (10~60VDC)	24VDC (10~60VDC)
Reverse Polarity Protect	Yes	Yes
Input Current	Typical 0.4A@24V	Typical 0.4A@24V
Power Consumption	Typical 9.6W@24VDC full traffic load. Max 12W@60VDC full traffic load, suggest to reserve 15% tolerance	Typical 9.6W@24VDC full traffic load. Max 12W@60VDC full traffic load, suggest to reserve 15% tolerance

Revision History

Version	Description	Date	Editor
V1.0	1st released DRS610/DS410 User Manual	Mar. 2020	Orwell