WoMaster

User Manual

COVER

WR312G-LTE/WR322GR-2xLTE 3D

Industrial Secure Cellular Router (Serial Server)

Mar.2024 V3.1

HW3.0

www.womaster.eu

WoMaster

WR312G-LTE/WR3222GR-LTEx2 3D

Industrial Secured and Rugged LTE Serial Router (Dual Core) Series

User Manual

About This Manual

This user manual is intended to guide a professional installer to install and to configure the WoMaster Industrial Secured and Rugged LTE Serial Router. 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 router.

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

New industrial secure LTE router WR322GR Series enhances routing performance with dual-core 880MHz CPU and support concurrent dual Cellular networks. The RS232/422/485 DB9 ports with Modbus RTU features can connect sensor and meter data to cloud wirelessly.

The WR322GR router supports dual LTE with DSDA (Dual SIM Dual Active) and LTE to Ethernet WAN redundancy to guarantee not-stop WAN connectivity. To safeguard cybersecurity, security features such as Firewall, OpenVPN, GRE tunnel are supported. The embedded MQTTS, CoAP and RESTful API enable instant public cloud integration such as AWS or Azure. The ThingsMaster OTA can also be set up for an instant and secured access to receive data or manage devices remotely.

WR322GR Series is an innovative Industrial Secure Dual LTE router. WR312G Series is designed for IIOT applications by single radio LTE or Wi-Fi interface, while WR322GR by dual LTE or LTE + Wi-Fi interfaces. Each LTE supports 2T2R MIMO to deliver high bandwidth up to 150Mbps uplink and 50Mbps downlink, while IEEE 802.11ac + 802.11n Wi-Fi 2T2R MIMO delivers high bandwidth up to 1166M(866M+300M)bps. The router support Dual SIM Dual Active and Dual Standby. Dual SIM Dual Active means the two LTE interfaces can be activated and connect to the internet at the same time, and backup with each other. The router will send the uplink stream through different LTE interface automatically. Besides, each LTE interface can have one or dual SIM cards, it also means you can insert up to 4 SIM cards to different carriers.

1.2 MAJOR FEATURES

Below are the major features of WR302GR/312GR/322GR Series:

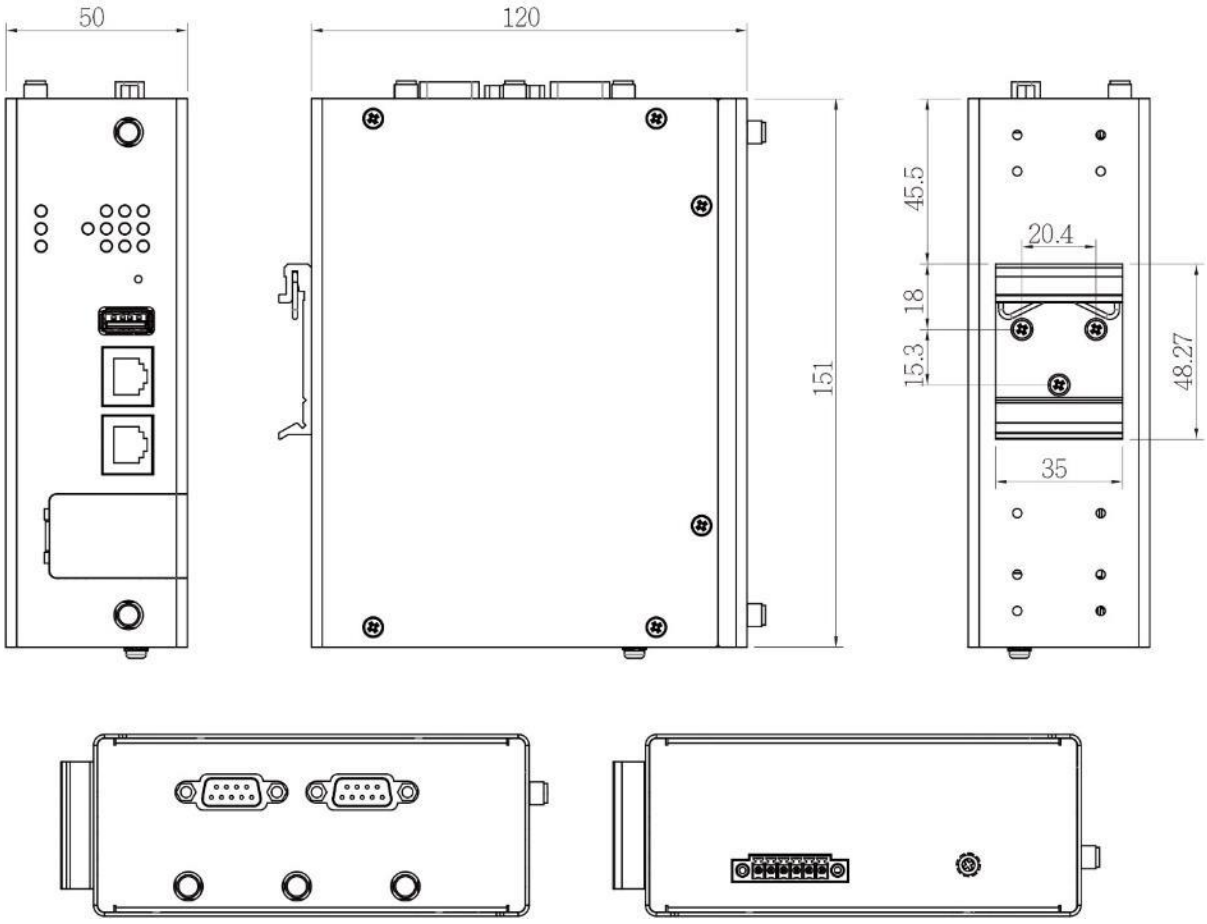
- Dual Core High Speed Processor
- 2 x 100/1000MBase-T RJ45, Auto Negotiation for routing or bridging
- LTE Cat.4 2T2R MIMO delivers high bandwidth up to 150Mbps uplink and 50Mbps downlink
- Supports Dual SIM for Dual Active and Dual Standby, dual LTE redundancy with non-stop carrier switch time
- Supports GSMA eUICC Compliant SIM, chip SIM socket is reserved and can be produced upon customize request
- Supports one or two RS232/422/485 DB-9 interfaces, mainly design for Serial over LTE connectivity
- Support GPS for location services in WR322GR models
- Optional Wi-Fi model supports Dual Bands Dual WLAN Radios, IEEE 802.11ac Wi-Fi 2T2R MIMO and IEEE 802.11n Wi-Fi 2T2R MIMO delivers high bandwidth up to 1166(866+300)Mbps (WLAN series)
- Supports Watchdog, Ping watchdog, Periodic/schedule Reboot, Serial communication, IPv4, SNMP v1/v2c/v3/Trap, Private MIB, DHCP server/client, DDNS, System Log, SD card configuration, ARP response over 802.2 LLC SNAP
- Cellular Configuration: Radio on/off, 4G LTE/3G HSPA Configuration, SIM Security, Connection Status, Dual SIM Standby setting, Cellular diagnostic, SMS Reboot
- Wireless redundancy: Cellular to Eth-WAN Redundant
- Advanced Security system by OpenVPN, IPsec, Firewall, DMZ, Port Forwarding, HTTPs Login
- Event Notifications through E-mail, SNMP trap, SysLog and Digital/Relay Output
- Traffic Management features: NAT Routing and Traffic shaping.
- Web, SNMP for network Management, CLI interface for diagnostic. Network diagnostic by iperf/netconf
- Steel Metal Housing and aluminum heat sinks inside for heat dissipation
- Wide range operating temperature -40~70˚C
- Typical 24V (9-48V) power input
- IP30 ingress protection

2. HARDWARE INSTALLATION

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

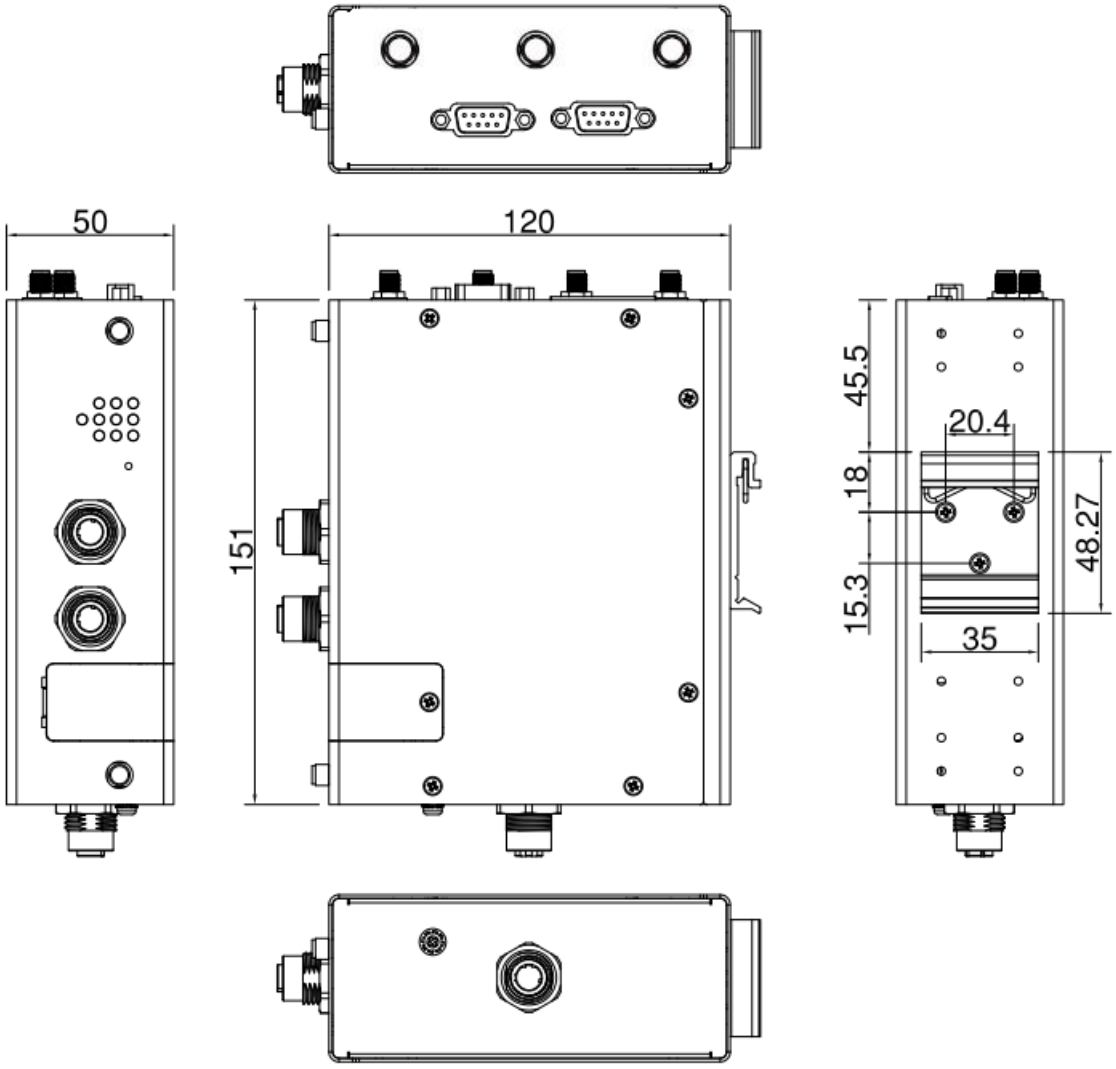
2.1 HARDWARE DIMENSION

Dimensions of WR3x2G: 50 x 151 x 120 (W x H x D) / without DIN Rail Clip



Note: 1 Serial or 2 Serial ports is upon the model.

Dimensions of WR3x2G-M12: 50 x 151 x 120 (W x H x D) / without DIN Rail Clip

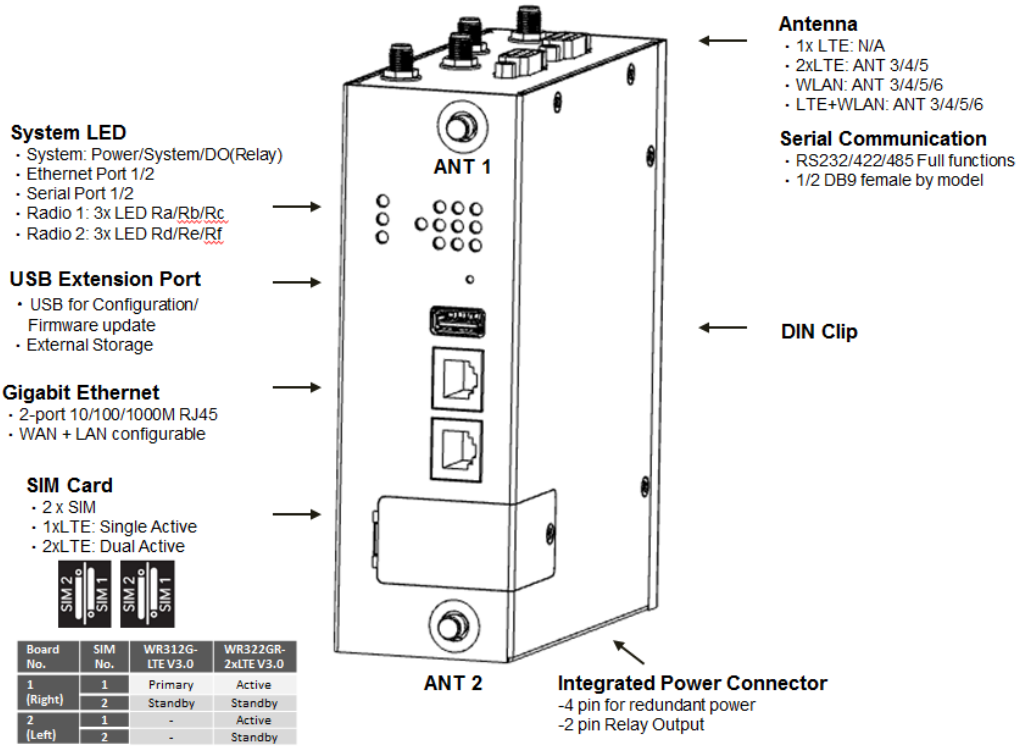


Note 1: 1 Serial or 2 Serial ports is upon the model.

Note 2: M12 model is manufactured by MoQ, check with our sales for detail.

Front Panel Layout

The front panel from WR3x2GR routers include 2 ports Giga Ethernet (100/1000 Base-T, RJ45), System + Ethernet + Radio LEDs, USB for configuration/firmware management (Not available for C Series), Reset button, 1 or 2 RS232/422/485 DB-9 serial ports on top, 1 x 6-pin terminal block connector (4 pin for power inputs and 2 pin for Relay Output) and 1 chassis grounding screw on bottom side. There are up to 5 SMA antenna sockets for WR322GR-2xLTE model, up to 6 SMA antennas for LTE + Wi-Fi model. On the rear side of the device, there is DIN rail clip attached.



Antenna Map:

	WR312G-LTE	WR322GR-2xLTE	WR322GR-WLAN+LTE
Ant 1	**LTE-Main**	**LTE-Main**	**LTE-Main**
Ant 2	**LTE- Diversity**	**LTE- Diversity**	**LTE- Diversity**
Ant 3	**-**	**LTE-Main**	**Wi-Fi 5 Main**
Ant 4	**-**	**GPS/GNSS**	**Wi-Fi 4 Main**
Ant 5	**-**	**LTE- Diversity**	**Wi-Fi 5 Div.**
Ant 6	**-**		**Wi-Fi 4 Div.**

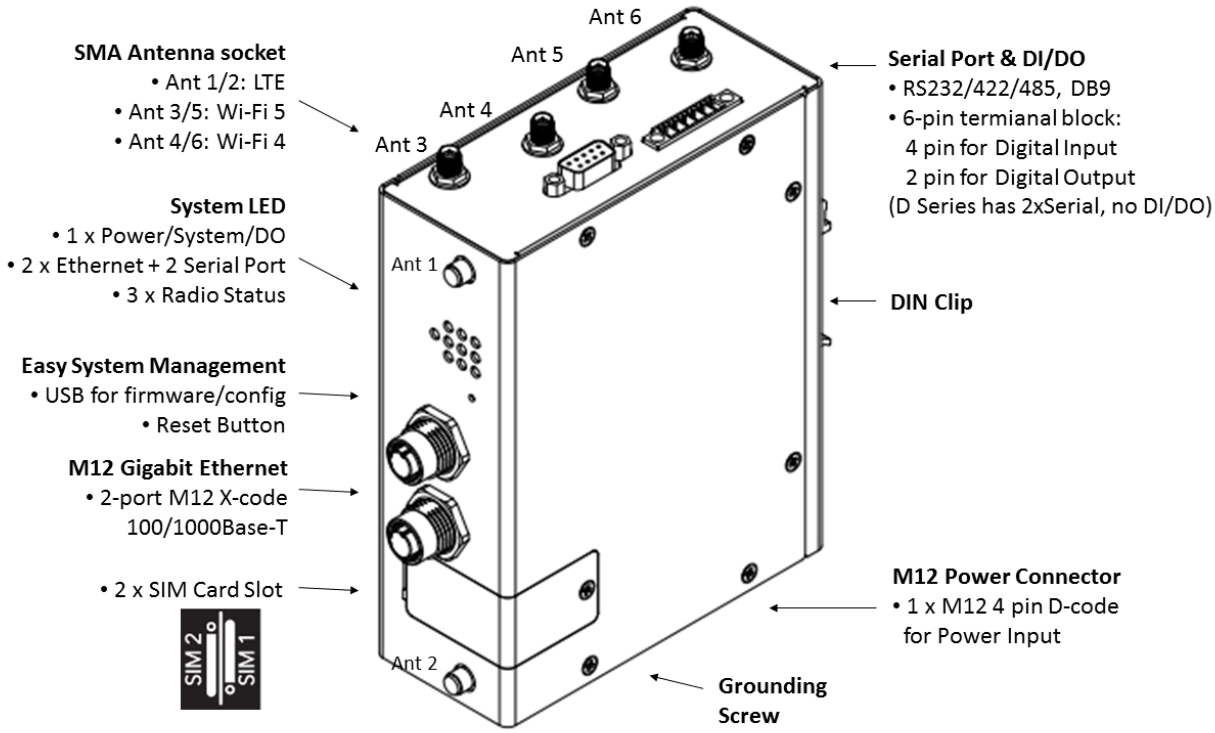
Wi-Fi 5: IEEE 802.11ac

Wi-Fi 4: IEEE 802.11n

Note1: All models use the same antenna socket location. WR302 does not have an antenna socket.

Note 2: Due to the different number of antennas used by LTE/WLAN models, the unused antenna positions will be covered by caps.

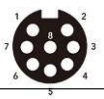
WR3x2G-M12



2x M12 8-pin X-code/A-code Ethernet:

Standard Connector: X-code

(A-code M12 by request)

100/1000Base-T M12 Type	Pin	A-Code Female	X-Code Female
X-Code 	1	D3-	D1+
	2	D4+	D1-
	3	D4-	D2+
	4	D1-	D2-
A-Code 	5	D2+	D4+
	6	D1+	D4-
	7	D3+	D3-
	8	D2-	D3+

1x M12 Power:

Pin	DESC
1	V1 +
2	V2 +
3	V2 -
4	V1 -

Antenna Map:

	WR312A-M12-LTE	WR312A-M12-2xLTE	WR322A-M12-WLAN+LTE
Ant 1	**LTE-Main**	**LTE-Main**	**LTE-Main**
Ant 2	**LTE- Diversity**	**LTE- Diversity**	**LTE- Diversity**
Ant 3	**-**	**LTE-Main**	**Wi-Fi 5 Main**
Ant 4	**-**	**GPS/GNSS**	**Wi-Fi 4 Main**
Ant 5	**-**	**LTE- Diversity**	**Wi-Fi 5 Div.**
Ant 6	**-**		**Wi-Fi 4 Div.**

Wi-Fi 5: IEEE 802.11ac, Wi-Fi 4: IEEE 802.11n

Note1: All models use the same antenna socket location. WR302 does not have an antenna socket.

Note 2: Due to the different number of antennas used by LTE/WLAN models, the unused antenna positions will be covered by caps.

2.2 INSTALLATION

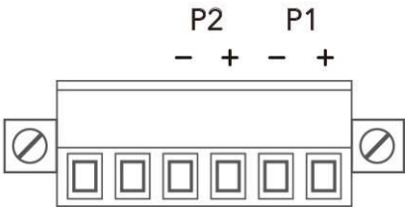
After unpack the box, follow the steps below in order to properly connect the device. For better Wi-Fi performance, put the device in a clearly visible spot, as obstacles such as walls and doors hinder the signal.

1. First, assemble router by attaching the necessary antennas and inserting the SIM card.
2. To power up router, please use the power adapter included in the box.

> **WARNING:** Using a different power adapter can damage and void the warranty for this product

2.3 WIRING THE POWER INPUTS

Power Input port in the router provides 2 sets of power input connections (P1 and P2) on the terminal block. On the picture below is the power connector.



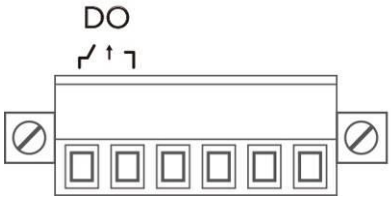
Wiring the Power Input

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 DC Switching type power supply. The typical input DC voltage is 24V, range of 12VDC to 60VDC.

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

2.4 WIRING THE ALARM RELAY OUTPUT (DO)

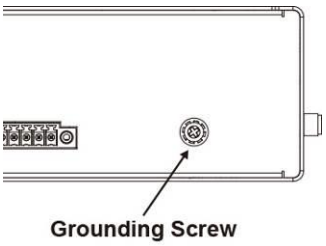
The relay output contacts are located on the front panel of the router. The relay output consists of the 2-pin terminal block connector that used to detect user-configured events. The two wires attached to the fault contacts form a close circuit when a user-configured event is triggered. If a user-configured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



NOTE: The relay contact only supports 1 A current, DC 24V. Do not apply voltage and current higher than the specifications.

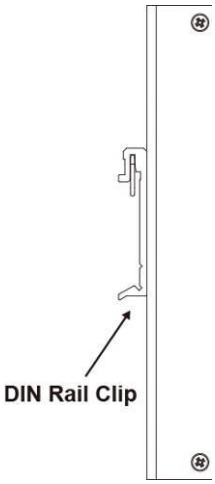
2.5 CONNECTING THE GROUNDING SCREW

Grounding screw is located on the bottom side of the router. 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 be already attached to the back panel of the device screwed tightly. If user needs to reattach the DIN-Rail attachment plate to the device, make sure the plate is situated towards the top, as shown by the following figures.



To mount the router 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 device from the track, reverse the steps.

2.7 ANTENNA

WR312G & WR322GR are supported with up to 5/6 antenna sockets upon the model, where 4G LTE, GPS, and Wi-Fi antennas are supported. All of the antennas are connected to the router by screwing all the antennas to the SMA connector on the front panel of the router.

WiFi Antenna

Frequency	2400 ~ 2500 MHz 5150 ~ 5850 MHz
V.S.W.R	<= 2.0 @ 2400 ~ 2500 MHz <= 2.0 @ 5150 ~ 5850 MHz The data is tested with 1M cable
Peak Gain	2.4G: 3.55dBi, 5GHz: 5.28dBi 2400~2500MHz: 2.4~3.55dBi 5150~5850MHz: 3.41~5.28dBi
Efficiency	70 % @ 2400 ~ 2500 MHz 85 % @ 5150 ~ 5850 MHz
Directional	Omni-directional
Impedance	50 Ohm
Dimension	200xΦ13 mm
Connector Type	SMA Male Reverse
Operational Temperature	- 40 °C ~ +65 °C

LTE Antenna

Frequency	690 ~ 960 MHz / 1710 ~ 2700 MHz
V.S.W.R	<= 3.0
Radiation	Omni
Peak Gain	3.15dBi 690MHz: 1.36dBi, 960MHz: 1.37dBi, 1710MHz: 3.12dBi, 1800MHz: 1.29dBi 1900MHz: 2.63dBi, 2100MHz: 1.47dBi, 2170MHz: 1.14dBi, 2500MHz: 3.15dBi 2600MHz: 2.46dBi, 2700MHz: 1.89dBi
Directional	Omni-directional
Impedance	50 Ohm
Connector	SMA Male
Dimension	200xΦ13 mm
Operational Temperature	- 20 °C ~ +65 °C

NOTE: Please refer to device stick for antenna combination of different models

Antenna Placement

	WR312G-LTE	WR322GR-2xLTE	WR322GR-WLAN+LTE
Ant 1	**LTE-Main**	**LTE-Main**	**LTE-Main**
Ant 2	**LTE- Diversity**	**LTE- Diversity**	**LTE- Diversity**
Ant 3	**-**	**LTE-Main**	**Wi-Fi 5 Main**
Ant 4	**-**	**GPS/GNSS**	**Wi-Fi 4 Main**
Ant 5	**-**	**LTE- Diversity**	**Wi-Fi 5 Div.**
Ant 6	**-**		**Wi-Fi 4 Div.**

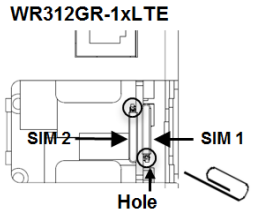
2.8 SIM CARD INSTALLATION AND DUAL SIM DUAL ACTIVE

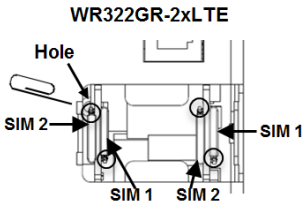
SIM Card Slot

The SIM Card Slot is used to insert the cellular card. The WR3x2 Series can support Dual SIM redundant.

To install/uninstall SIM card:

1. Use screwdriver to loosen screws and remove SIM cover.
2. Insert a paper clip or a SIM-eject tool into the hole beside the SIM socket. Push in towards the device, but don't force it. The SIM 1 is the primary SIM in the default configuration.





3. (When install) Draw out SIM tray and install SIM card on top side of tray
   (When uninstall) Draw out SIM tray and uninstall SIM card

> **WARNING:** Be careful when install the SIM Card, wrong installation procedure will cause damage. Please follow the mechanical print out to install the SIM Card.

4. Insert tray back to SIM socket and reattach SIM cover.
5. To Configure SIM Card Setting, check the Chapter 3.5 Cellular settings in user manual.

Dual SIM Dual Active

The WR322GR-2xLTE supports dual 4G LTE Active mode to guarantee non-stop connectivity. Open the protection cap and insert the SIM card to the SIM trap holder of the radio. The indication of single/dual radio is as below:

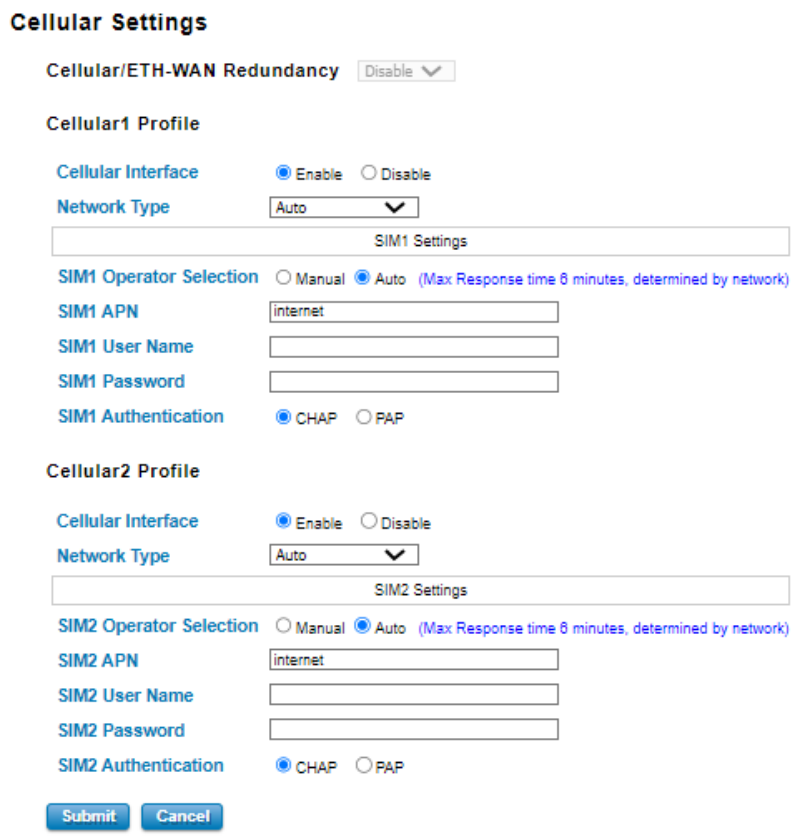
Board No.	SIM No.	WR312GR-LTE V3.0	WR322GR-2xLTE V3.0
1 (Right)	1	Primary	Active
	2	Standby	Standby
2 (Left)	1	-	Active
	2	-	Standby

In single Radio model, each radio support dual SIM, the SIM 1 is primary, SIM 2 is standby SIM.

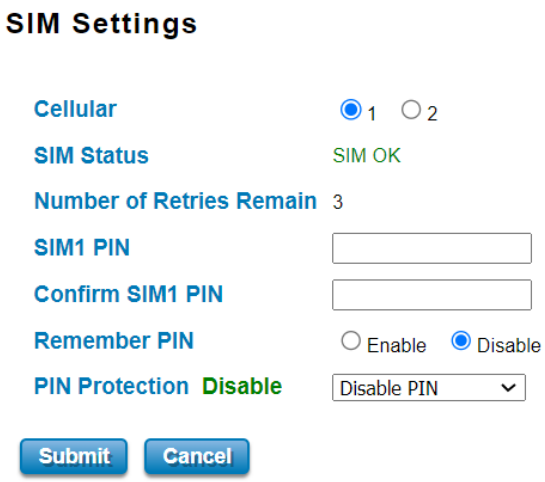
In dual Radio model (Ex: WR322GR-2xLTE), there are two radios and the radio on board 1 (the board with the Ethernet ports) is Cellular 1, its SIM 1 is the Active/Primary SIM of Cellular 1. The radio on another board is Cellular 2, its SIM 1 is the Active/Primary SIM of Cellular 2. The two Radio interfaces also accept 2 SIM cards, then the SIM2 of each radio will be standby SIM, it is only activated while the SIM 1 failure.

In dual Radio model, you can configure the Cellular profile for each radio in Cellular Setting, SIM setting and security PIN of each Cellular and monitor the status of each Cellular.

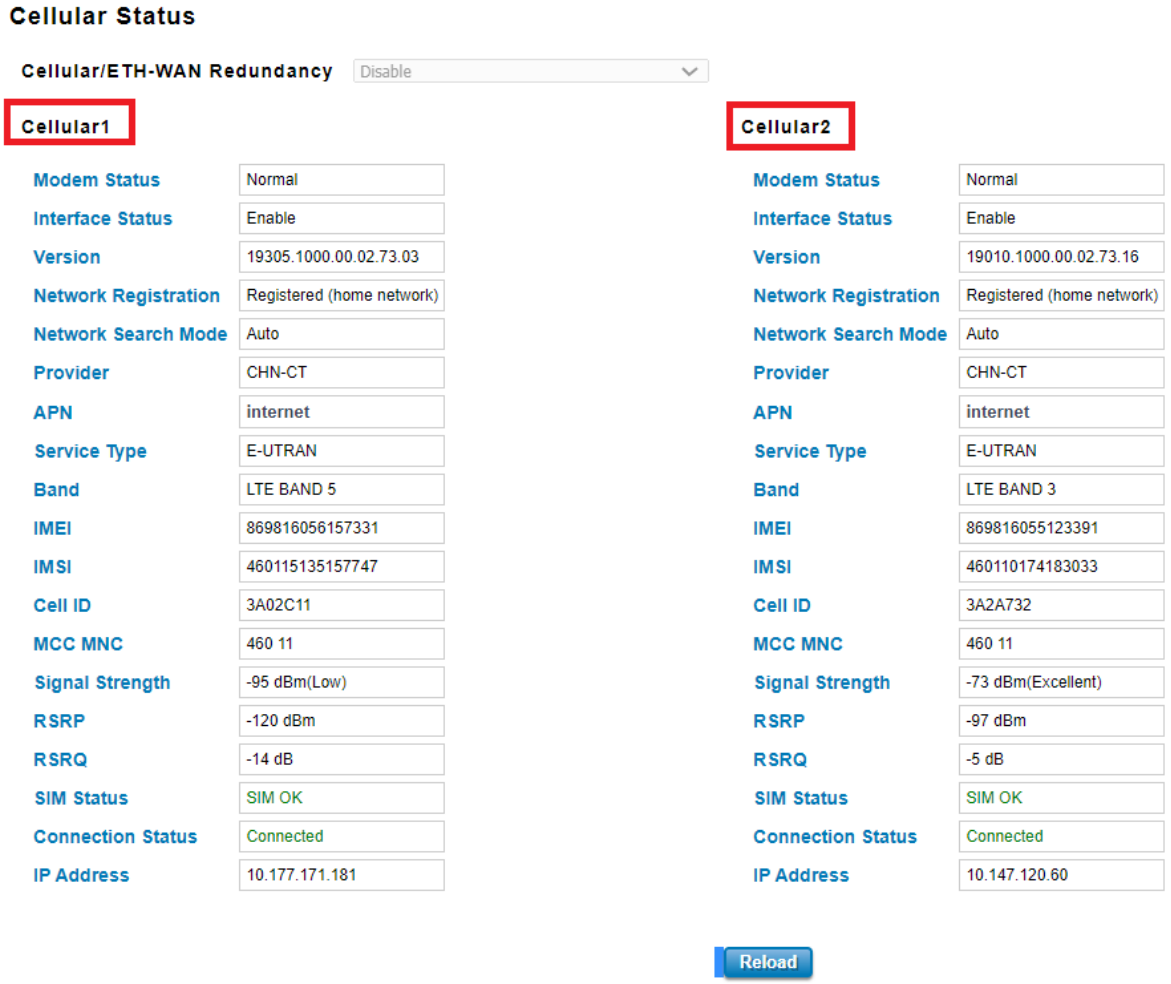
Cellular Setting: Enable or Disable the Cellular Interface and configure its settings. The 2 Cellular interfaces can be Enabled or just enable one of them in Dual Radio model. You can find the detail description in Chapter 3.5.2 CELLULAR SETTING.



SIM Setting: Select the Cellular 1 or 2 you'd like to configure. You can find the detail description in Chapter 3.5.3 SIM SETTING.

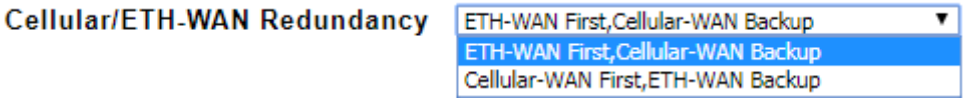


Cellular Status: Check the Cellular 1 and Cellular 2 status in the same page. You can find the detail description in Chapter 3.5.1 CELLULAR STATUS.

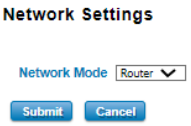
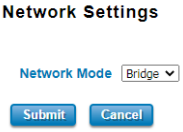


Cellular/ETH-WAN Redundancy:

After you configured Network Mode as Router mode, you can also configure Ethernet-WAN and CELLULAR Redundancy setting. Select the Cellular/ETH-WAN Redundancy mode you prefer.



Below table shows the sequence of the Cellular/ETH-WAN Redundancy in dual radio mode.

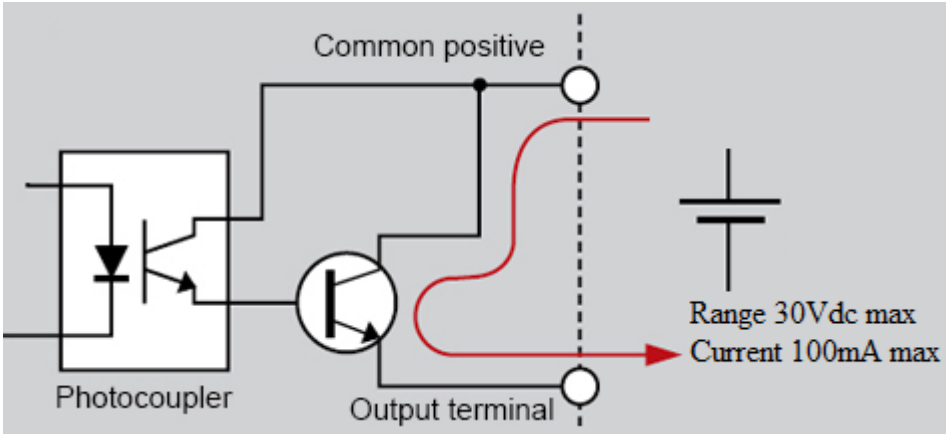
Network Mode	Setting	Ethernet-WAN 1	Ethernet-WAN 2	Cellular 1	Cellular 2
Router Mode 	ETH-WAN First, Cellular-WAN Backup	**1**	2	3	4
	Cellular-WAN First, Eth-WAN Backup	3	4	**1**	2
Bridge Mode 	-	3 (LAN)		**1**	2

If you just have one Cellular or one Eth-WAN port, ignore the 2nd WAN/Cellular interface in above table.

2.9 WIRING THE DIGTIAL OUTPUT

Note: The feature is just applied to the model with Digital Output. The feature is customized feature, contact our sales for detail.

The digital output of the 2-pin terminal block connector are 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.



Wiring the Digital Output

6. Insert the positive and negative wires into the DO+ and DO- contact on the terminal block connector.
7. Tighten the wire-clamp screws to prevent the wires from being loosened.

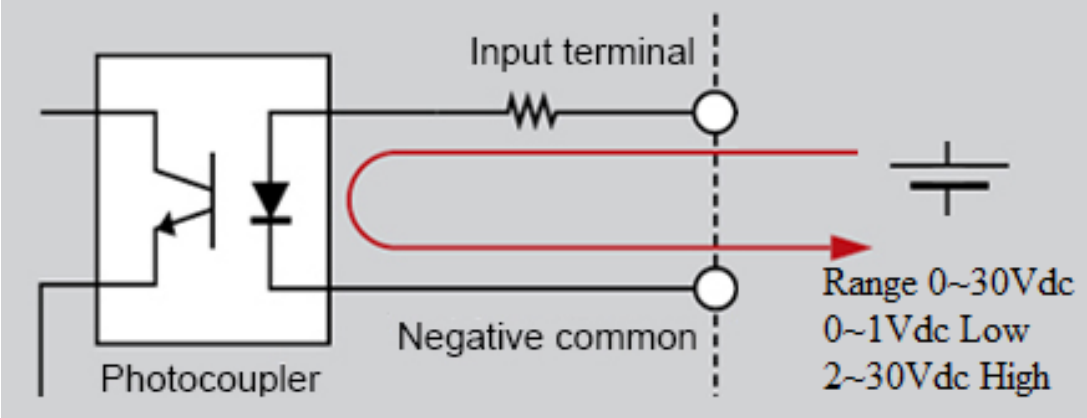
> **WARNING:** Please confirm the wire installation according to the above steps, otherwise it would not work properly. It only supports 0.1 A current, DC 30V. Do not apply voltage and current higher than the specifications.

Note: All WR312/322 supports Relay Output. However, not every model of WR312/322 series supports Digital Input and Digital Output.

2.10 WIRING THE DIGTIAL INPUT(DI)

Note: The feature is just applied to the model with Digital Input. The feature is customized feature, contact our sales for detail.

To wire the DI on the Terminal block, use screwdriver to loosen screws, insert the positive and negative wires into the DI 1/2/3 and COM contact and then tighten screws after the DI wire is connected.



Wiring the Digital Input

1. Insert the positive and negative wires into the DI 1/2/3 and COM contact on the terminal block connector.
2. Tighten the wire-clamp screws to prevent the wires from being loosened.
3. Input signal voltages range from 0 volts to 1 volts for a "**low**" logic state and 2 volts to 30 volts for a "**high**" logic state.

WARNING: Please confirm the wire installation according to the above steps, otherwise it would not work properly.

Note: All WR312/322 supports Relay Output. However, not every model of WR312/322 series supports Digital Input and Digital Output.

2.11 HARDWARE WATCHDOG

The device provides a hardware watchdog mechanism for critical event, such as system reboot is to cut the power of the whole device to get a clean restart of all components. Some of the features are also available as watchdog. Refer to:

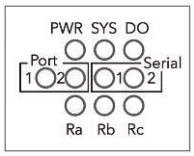
3.10.2 Ping Watchdog,

3.10.7 Periodic Reboot all use the Cutting Power Reset.

3.5.7 for SMS remote control reboot.

2.12 LED Indication

System & Interface LED:



LED	Status	Description
PWR	Green On	DC-IN Power is On
	Off	No Power in DC-IN
System LED	Green On	Ready
	Green Blinking	Firmware updating
	Off	Not Ready
DO (Relay)	Red On	Any failures SW control
	Off	No failure occurs
Giga Ethernet Port 1 / 2	Green On	Links established
	Green Blinking	Packets transmitting/receiving
	Off	Link is inactive
Serial 1	Green Blinking	Packets transmitting/receiving
Serial 2 (D Series only)	Green Blinking	Packets transmitting/receiving
	Not Active	Serial 2 is Not available

Radio LED:

WR312G-LTE/WR312GR-WLAN/WLAN+LTE (Ra/Rb/Rc)

LED		LTE Model	WLAN Model
Radio 1	Ra	SIM detected: Green On SIM not detected: Off	Wi-Fi 5 (5802.11ac) AP Mode: Green On, Client Mode: Green Blinking
	Rb	2/3G connection: Green On Not 2/3G connection: Off	Wi-Fi 4 (802.11n) AP Mode: Green On, Client Mode: Green Blinking
	Rc	4G connection: Green On Not 4G connection: Off	-

WR322GR-2xLTE/

WR322GR-WLAN+LTE(Rd/Re/Rf)

LED		2x LTE Status
Radio 1 / 2	Ra / Rd	SIM detected: Green On SIM not detected: Off
	Rb / Re	2/3G connection: Green On Not 2/3G connection: Off
	Rc / Rf	4G connection: Green On Not 4G connection: Off

Note: WR3x2-M12 series LED is the same as WR312G/322GR Series.

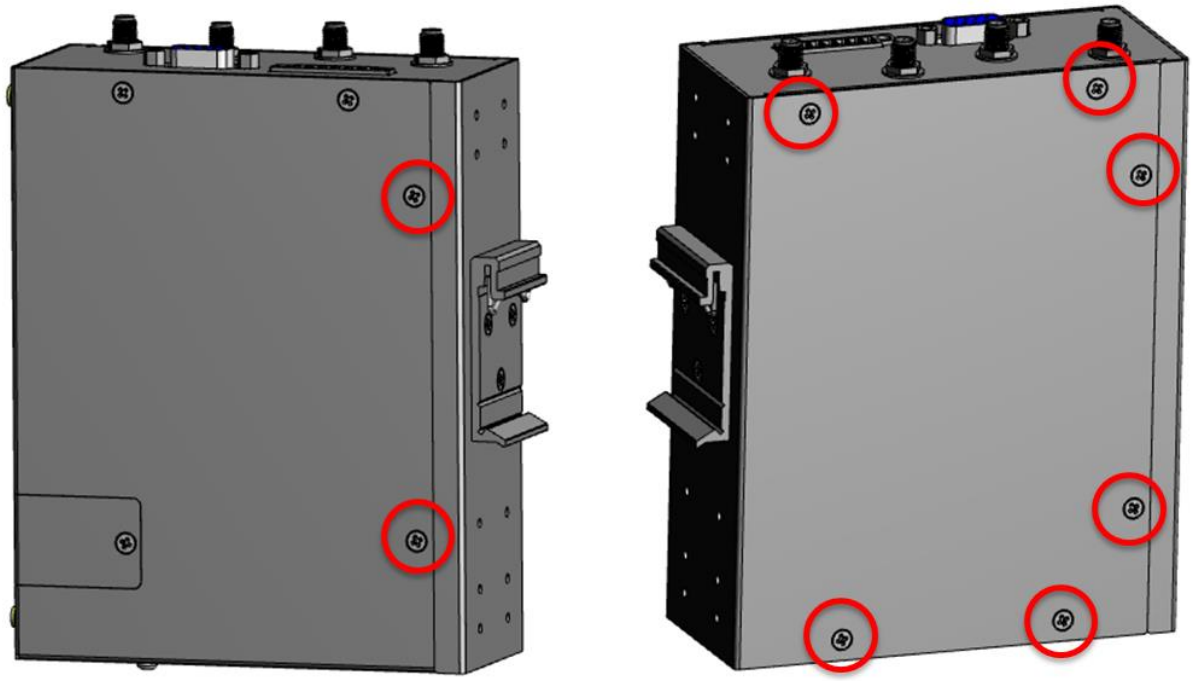
2.13 Micro SD Card (Reserved)

Note: The feature is just applied to the model with Micro SD. The feature is customized feature, contact our sales for detail.

The SD Card Slot is reserved inside the housing, it is used for field diagnostic data logging/option for storage per demand. To insert SD card after purchased, you need to open the housing, insert it correctly and carefully. For safety and warranty concern, we prefer to insert SD card during production. Please contact our sales while you need to use SD feature, we can do this according to the order.

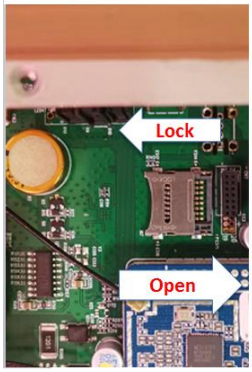
Following is the steps to insert SD card.

1. Shut down the power.
2. Please wear anti-static gloves when disassembling the housing.
3. Unlock the screws to open the side panel. There are several heat sinks pasted on the side panel, please keep them clean and put them back when re-assembling.

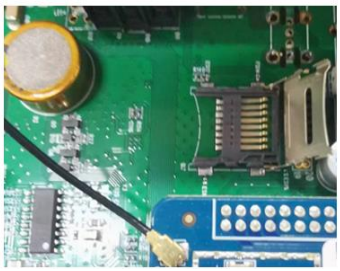


4. Prepare the SD card. Please always use industrial grade SD card, it has better lifecycle and wider range of the operating temperature.
5. Follow the below steps put the SD card into the socket.

1. Find the socket and check the Open/Lock direction.

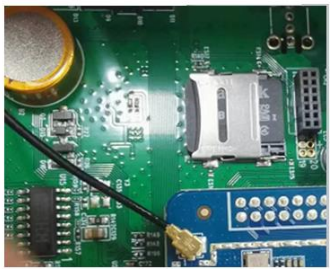


2. Open the SD socket.



3. Put the SD into the socket.

4. Lock the SD socket.



6. After inserted the SD card.
7. Lock the side panel and put the heat sink back correctly.

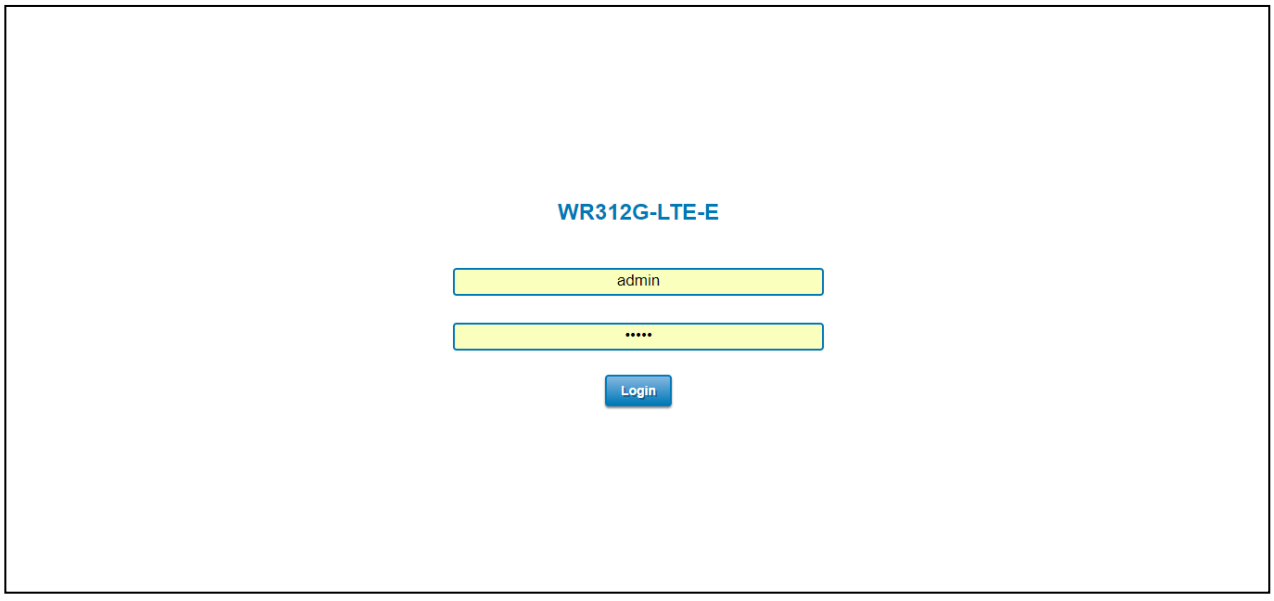
3. WEB MANAGEMENT CONFIGURATION

To access the management interface, WoMaster router has two ways access mode through a network; they are web 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 router interface offering status information and a subset of device 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 telnet management which is offer configuration way through CLI Interface. This manual describes the procedures for Web Interface and how to configure and monitor the managed router only.

PREPARATION FOR WEB INTERFACE MANAGEMENT

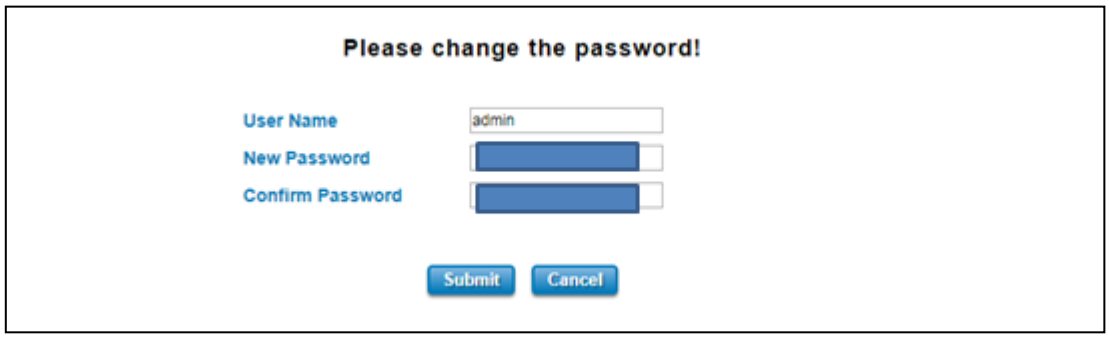
WoMaster provides Web interface management that allows user through standard web-browser such as Microsoft Internet Explorer, or Mozilla, or Google Chrome, to access and configure the router management on the network.

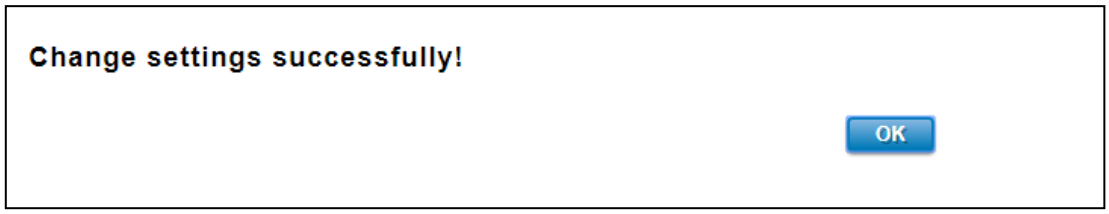
1. Plug the DC power to the router and connect router to computer.
2. Make sure that the router default IP address is **192.168.10.1**.
3. Check that PC has an IP address on the same subnet as the router. For example, the PC and the router are on the same subnet if they both have addresses that start 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 router 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 router). And then press **Enter** and the login page will appear.
7. Type user name and the password. In earlier firmware, the default user name: **admin** and password: **admin**. Then click **Login**. In latest firmware, the system will ask you **enter the new password in your first login.** Please follow the prompt to enter new password.



8. In first Login, then user will be asked to change the default password with a new password.

Enter new password and Submit to apply the change.

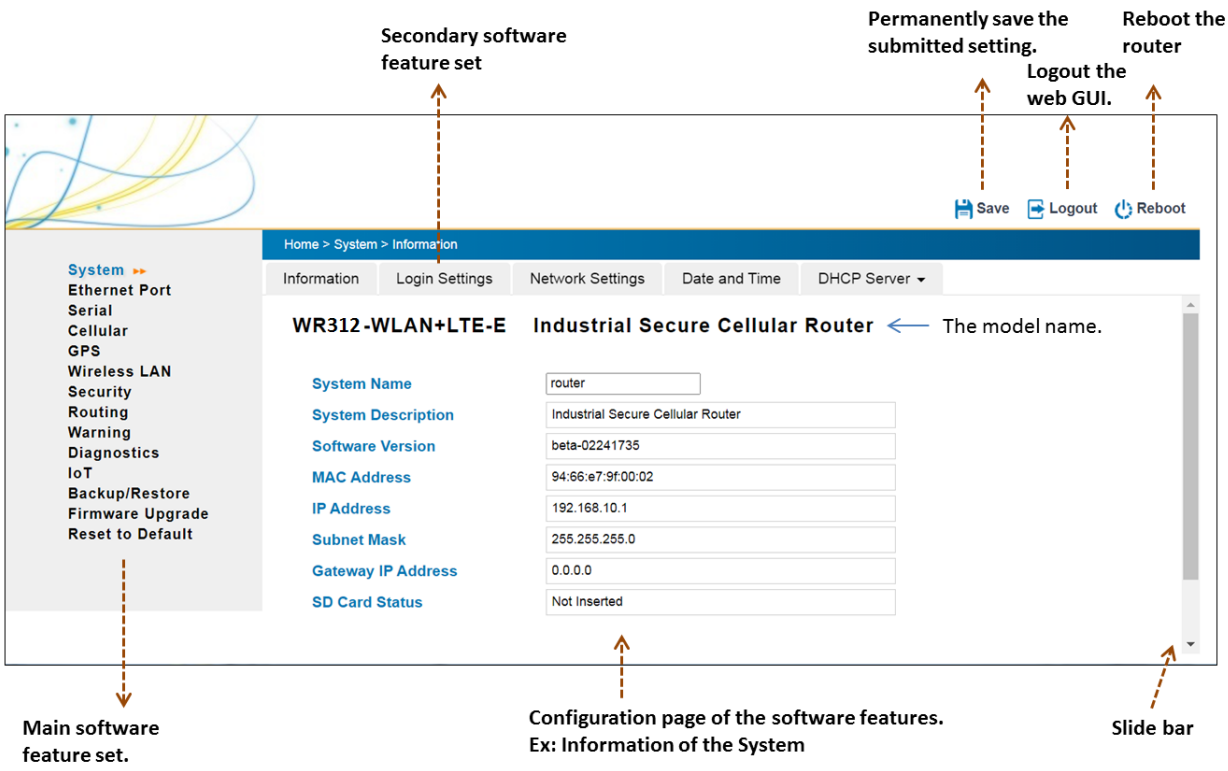




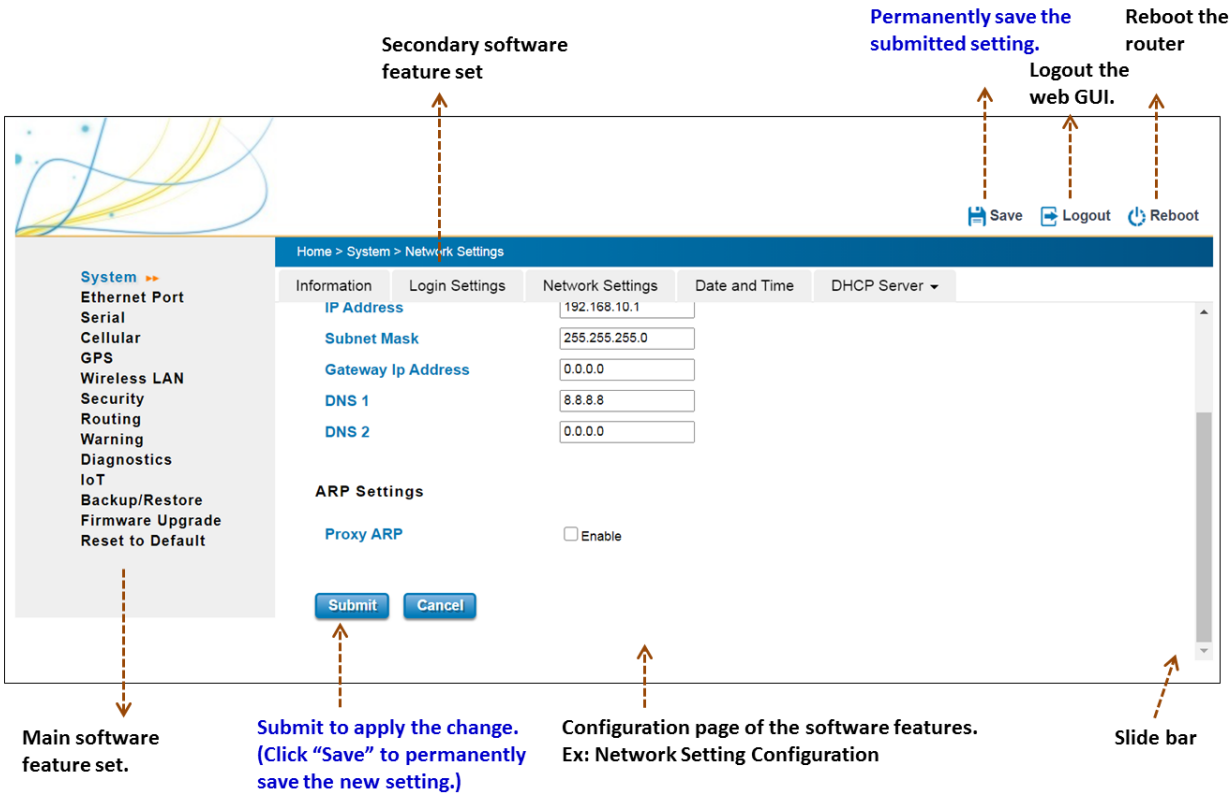
Then re-login with the new password.

Note: User must finish changing the password in web GUI before login with CLI.

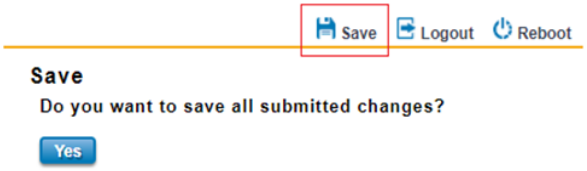
Web GUI Console Example 1: System Information



Web GUI Console Example 2: Network Setting Configuration. Click "Submit" to apply the change. **Click "Save" to save the new setting permanently, the setting will be remained after reboot.**



After click **“Save”, click “Yes” to save the submitted changes.** Please wait around 5-10 seconds, the system will then save the new settings to flash permanently. Do not power off or reboot the system during the 5-10 seconds.



In this Web management for Featured Configuration, user will see all of WoMaster Cellular Router'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 router on the network.

Following topics are covered in this chapter:

3.1 SYSTEM

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

3.1.1 Information

3.1.2 Login Setting

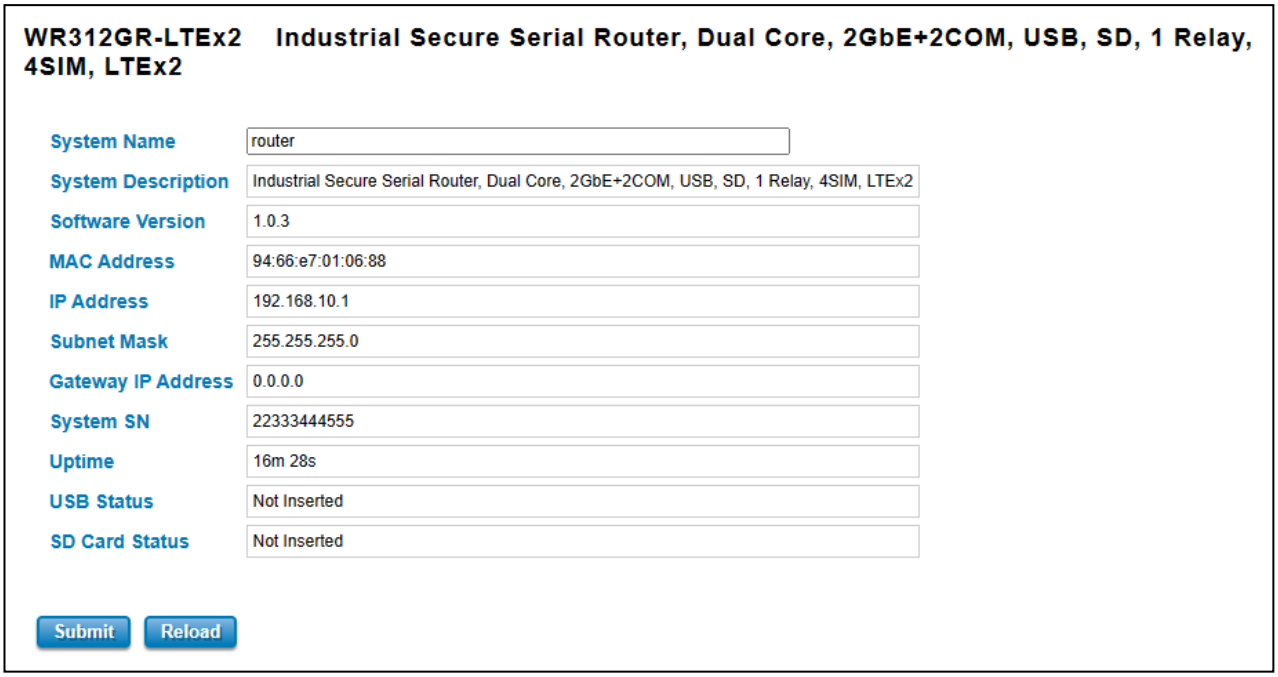
3.1.3 Network Settings

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 router to make it easier to identify different router that is connected to User network and also it shows the Cellular Status and LAN Settings information. The figure below shows the interface of the Information section.



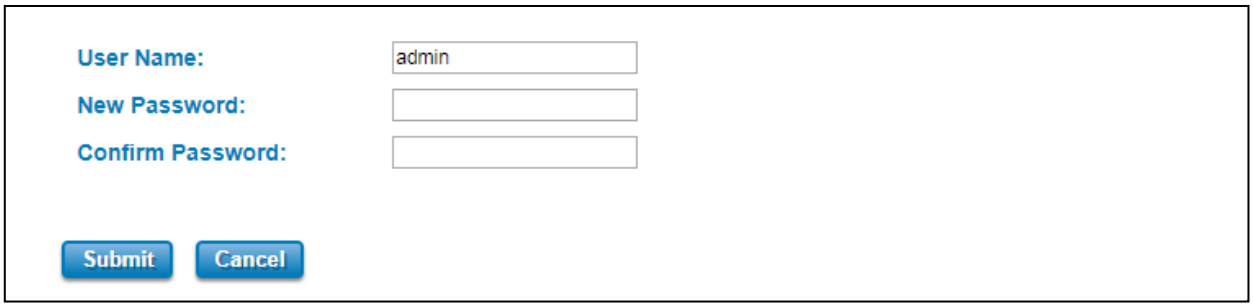
The description of the Information's interface is as below:

TERMS	DESCRIPTION
System Name	**Default: router** Set up a name to the device.
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.
IP Address	Display the IP Address of the device
Subnet Mask	Display the subnet mask of the device
Gateway IP Address	Display the Gateway IP Address of the device

System SN	Display the System SN of the device
UPtime	Display the uptime of the device
USB Status	Display the USB port status when the USB is plugged or unplugged.
SD Card Status	Display the SD Card port status when the SD Card is inserted or not inserted.

3.1.2 LOGIN SETTING

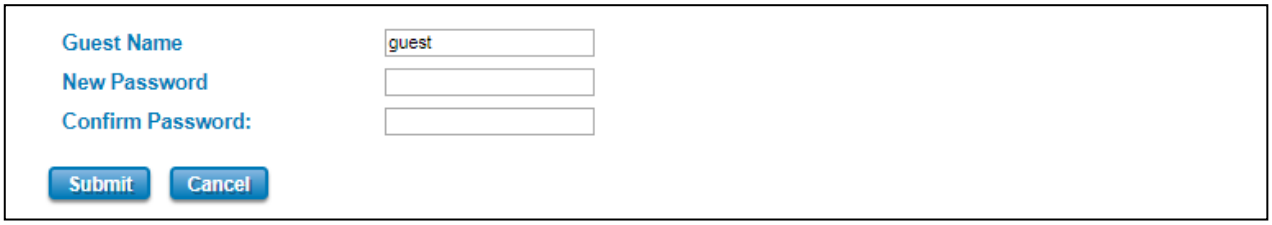
WoMaster' router supports Login Setting that has several authentication methods. It is supported with TACACS+, Radius, and Multi-User Authentication. This Login Setting consists of two level, admin and guest. Where the admin level, it has the privilege to read and write and for the guest level the privilege is read only. Below is the **Login Setting** section for **admin level**.



With the Name default setting is **admin** and the authority allow user to configure all of configuration parameters.

The Login Setting interface describes how to configure the system username and password for the web management login. To change the Name and Password, user just needs to input a new Name and New Password then confirm the new password in this section. Try to re-login with the new User Name and Password.

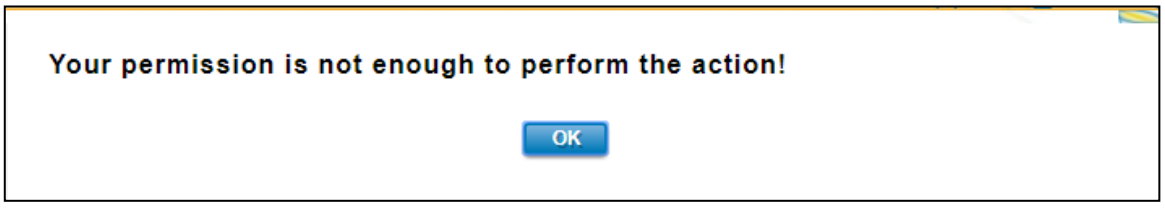
Below is the interface for **guest level**.



With the Name default setting is **guest** and the authority allow user to read only all of configuration parameters.

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

When user try to change the configuration, message will appear if user is not permitted to configure the configuration. Below is the interface.



The description of the Login Setting interface is as below:

TERMS	DESCRIPTION
User Name/ Guest Name	**Default: admin/guest** Key in new username here.
New Password	Key in new password here.
Confirm Password	Re-type the new password again to confirm it.

After finishing configure the Username and Password, click on **Submit** to apply the configuration. Don't forget to **Save** the configuration.

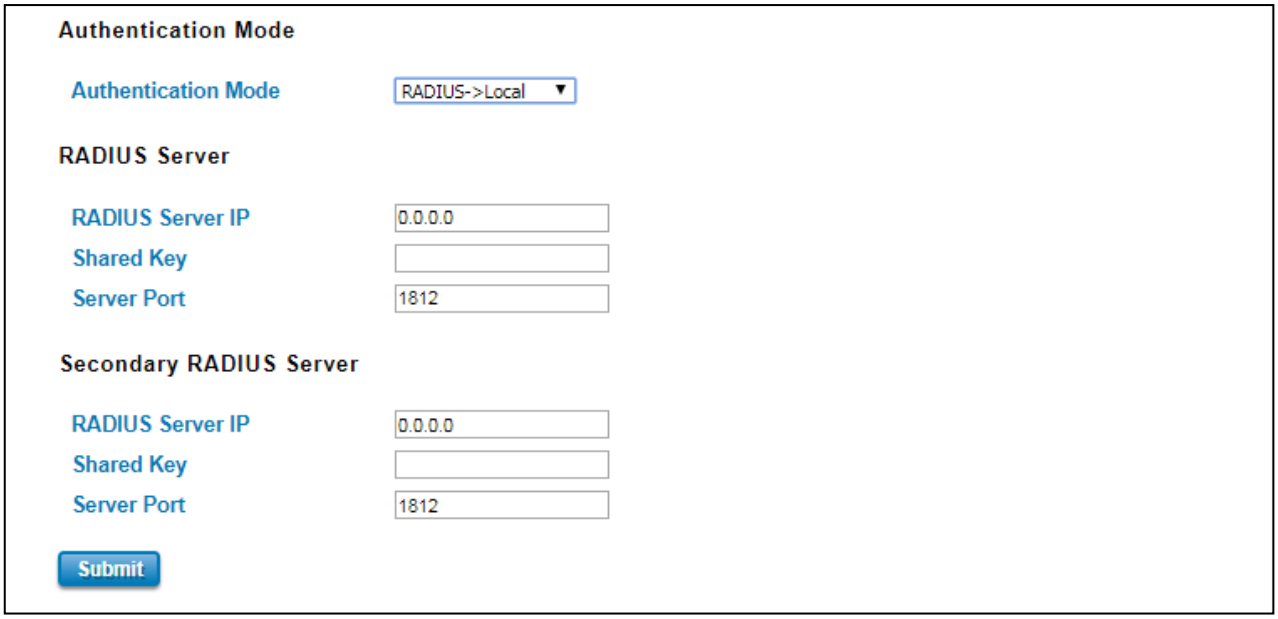
User Authentication Mode

The user authentication can be performed locally and remotely using Radius or TACACS+ authentication server. It has 5 authentication modes which are Local, RADIUS, RADIUS->Local, TACPLUS, and TACPLUS->Local. The default authentication method is Local method, where it works for multi user authentication that has been explained above.

RADIUS

The Remote Authentication Dial-In User Service (RADIUS) protocol was developed by Livingston Enterprises as an access server authentication and accounting protocol. The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, PAP or CHAP, UNIX login, and other authentication mechanisms.

Below is the RADIUS and RADIUS to Local authentication mode interface where the device takes a role as a RADIUS client that needs to authenticate with the RADIUS server database. For the RADIUS to Local mode, the authentication will try remote authentication first, falling back to local authentication mode if remote mode fails.



Support RADIUS/802.1X server and RADIUS/802.1X to Local mode

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

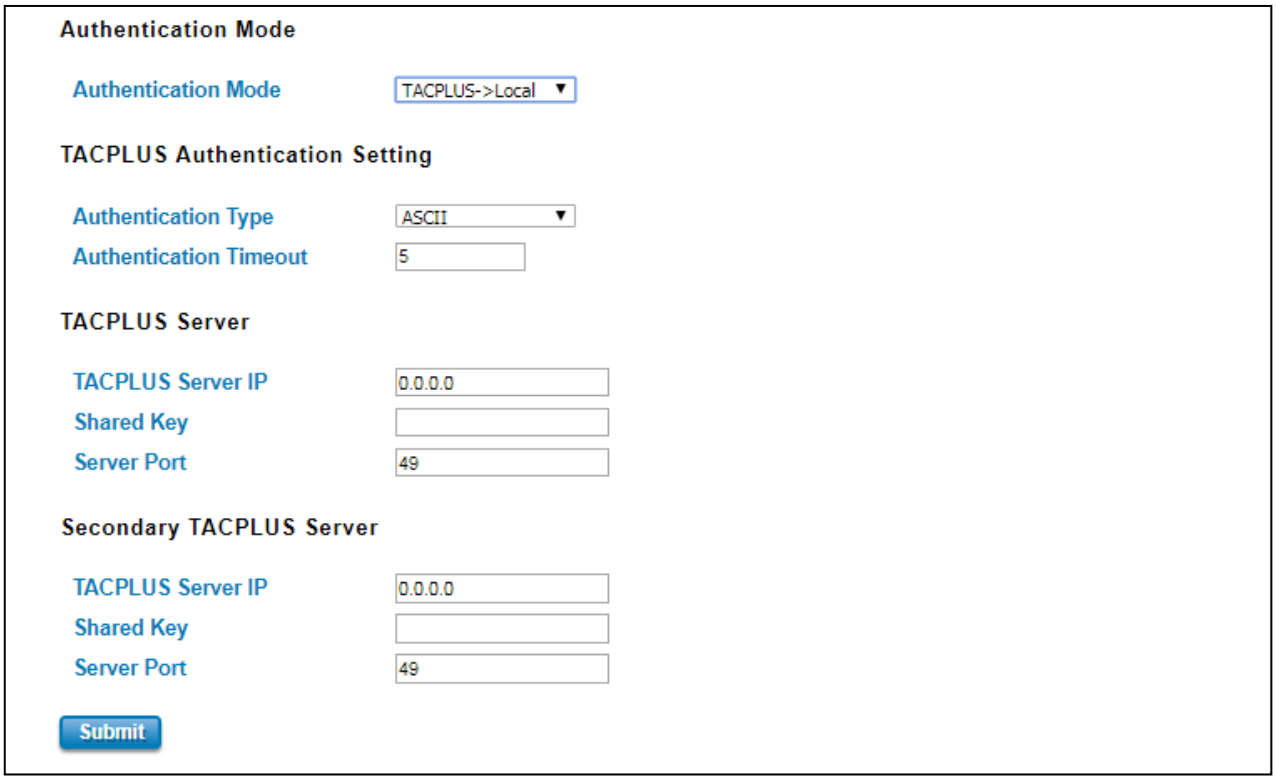
d. Click **Submit**

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

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 is the interface for TACPLUS and TACPLUS to Local authentication mode. For the TACPLUS to Local mode, the authentication will try remote authentication first, falling back to local authentication mode if remote mode fails or cannot be reached.



How to set up a TACACS+ server:

e. Select the **Authentication Type.**

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

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

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

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

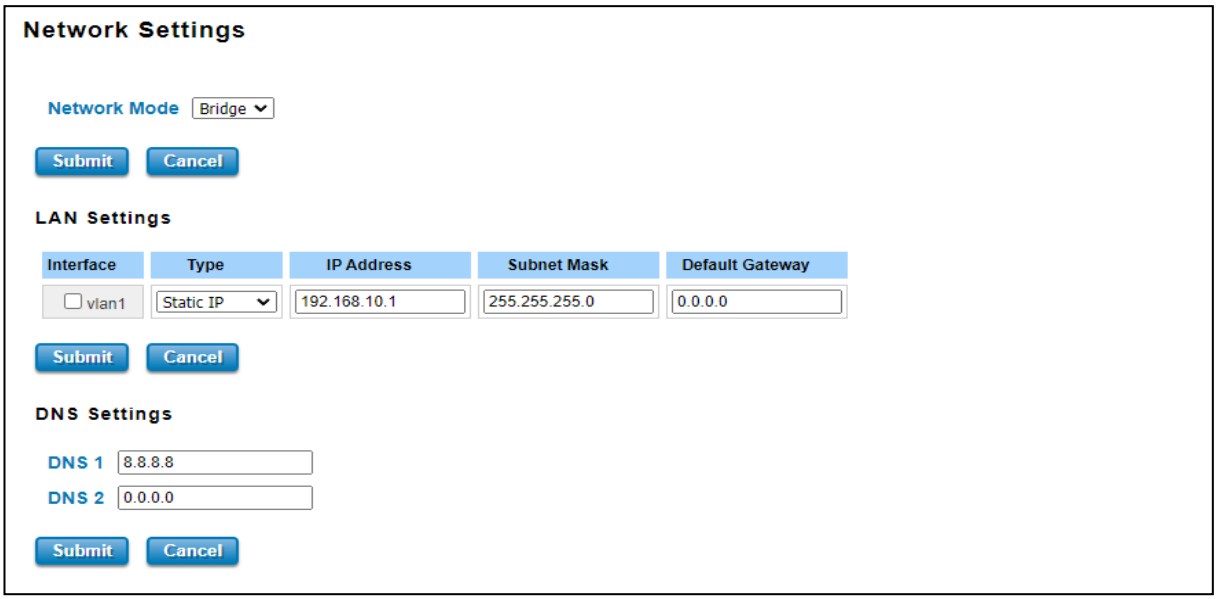
j. Click **Submit**

The description of the TACACS+ Authentication interface is as below:

TERMS	DESCRIPTION
Authentication Type	**Default: ASCII** Select the authentication type to authenticate to the server.
Authentication Timeout	**Default: 5** The maximum number of seconds allowed establishing a TCP connection between the device and the TACACS+ server. If the server cannot be reached within the limit time, and it will directly change to Local. This configuration is applied to TACPLUS->Local mode only.
TACPLUS Server IP	TACACS+ Server IP Address
Shared 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

3.1.3 NETWORK SETTING

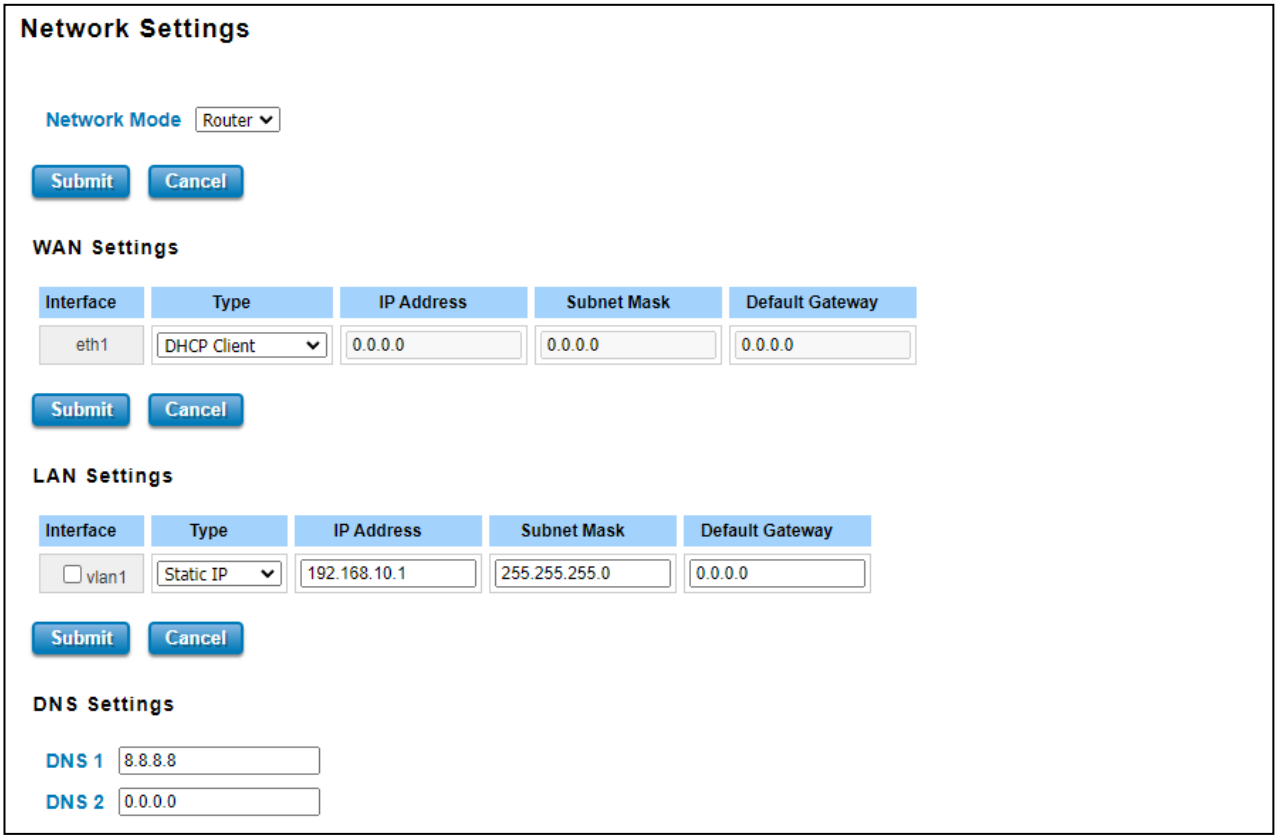
The Network Setting section allows users to configure both IPv4 values for management access over the network. WoMaster' router supports IPv4, and can be managed through either of these address types. Below is the Network Setting interface for **Bridge Mode**.



The description of the columns is as below:

TERMS	DESCRIPTION
LAN Access Type	User can select to DHCP or Static IP to activate the function. **DHCP:** Select DHCP to activate DHCP Client Function, no need to assign IP Address and received IP Address from DHCP Server. **Static IP:** Select Static IP to configure the IP configuration manually
IP Address	**Default: 192.168.10.1** Set up the IP address reserved by User network for User device. If DHCP Client function is enabled, no need to assign an IP address to device as it will be overwritten by DHCP server and shown here.
Subnet Mask	**Default: 255.255.255.0** Assign the subnet mask for the IP address here. If DHCP Client function is enabled, no needs to assign the subnet mask.
Default Gateway	**Default: 0.0.0.0.** Assign the gateway for the device here.
DNS 1	Specifies the IP address of the DNS server 1 that used in user network.
DNS 2	Specifies the IP address of the DNS server 2 that used in user network.

And below is the Network Setting interface for the **Router Mode** where it supports with the WAN port on port 1. User can configure the WAN Settings.



The IPv4 Configuration includes the router's IP address and subnet mask, as well as the IP address of the default gateway. In addition, input cells are provided for the IP addresses of a 1st and 2nd DNS server.

It is also supported DNS Proxy which uses the Domain Name Relay Daemon (DNRD). It takes DNS queries from hosts, and forwards them to the "real" DNS server. It takes DNS replies from the DNS server, and forwards them to the client. It is meant to be used for home networks that can connect to the internet using one of several ISP's. DNRD is pretty simple. Configure the managed router's IP settings. The figure above shows the user interface of IPv4 Configuration. The description of the columns is as below:

TERMS	DESCRIPTION
WAN Access Type	User can select to DHCP Client or Static IP to activate the function. **DHCP Client:** Select DCHP Client to activate DHCP Client Function, no need to assign IP Address and received IP Address from DHCP Server. **Static IP:** Select Static IP to configure the IP configuration manually
IP Address	**Default: 192.168.1.1** Set up the IP address reserved by User network for User device. If DHCP Client function is enabled, no need to assign an IP address to device as it will be overwritten by DHCP server and shown here.
Subnet Mask	**Default: 255.255.255.0** Assign the subnet mask for the IP address here. If DHCP Client function is enabled, no needs to assign the subnet mask.

Default Gateway	**Default: 0.0.0.0.** Assign the gateway for the device here.
DNS 1	Specifies the IP address of the DNS server 1 that used in user network.
DNS 2	Specifies the IP address of the DNS server 2 that used in user network.

Proxy ARP

Proxy ARP is a technique in which one host, usually a router answers ARP requests intended for another node located on another network. The router or "faking" its identity or pretends to be the target of the ARP requests by sending ARP responses that associate its own MAC address with the real (destination) node's IP address. The router acts as a proxy and takes responsibility for routing packets to the real destination. Proxy ARP can help machines on a subnet reach remote subnets without the need to configure routing or a default gateway.

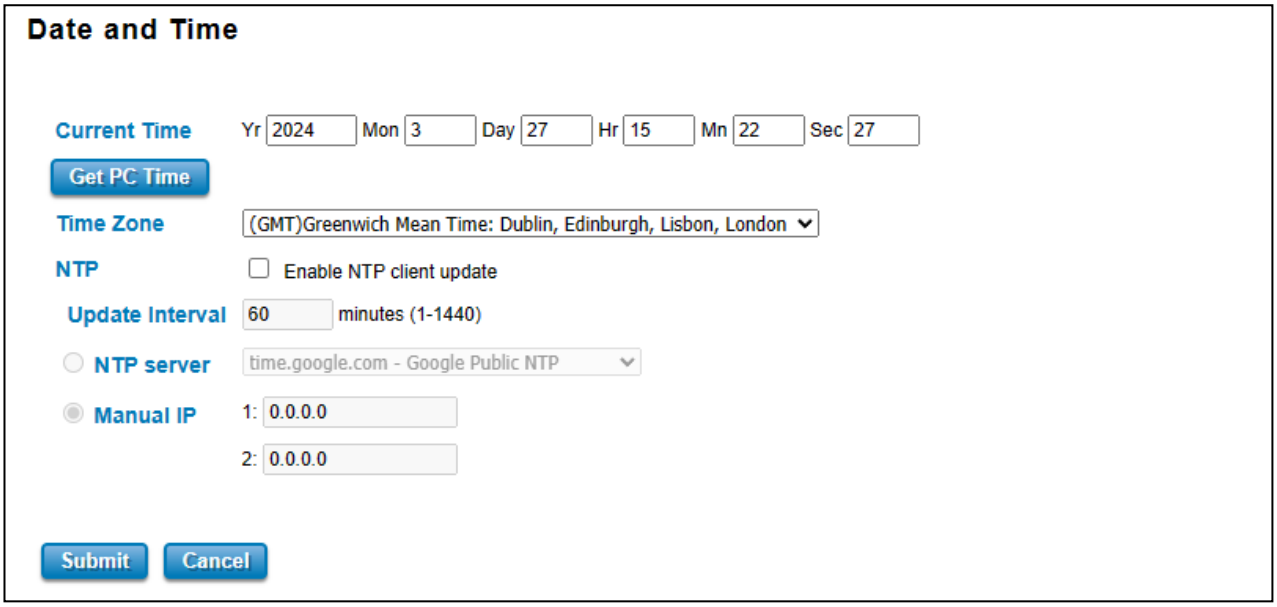
When Proxy ARP is enabled, if the router receives an ARP request for which it has a route to the target (destination) IP address, the router responds by sending a Proxy ARP reply packet containing its own MAC address. The host that sent the ARP request then sends its packets to the router, which forwards them to the intended host.

Below is the interface.

Check the box to enable the function of Proxy ARP.

3.1.4 DATE AND TIME

The WoMaster router 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.



The description of the columns is as below:

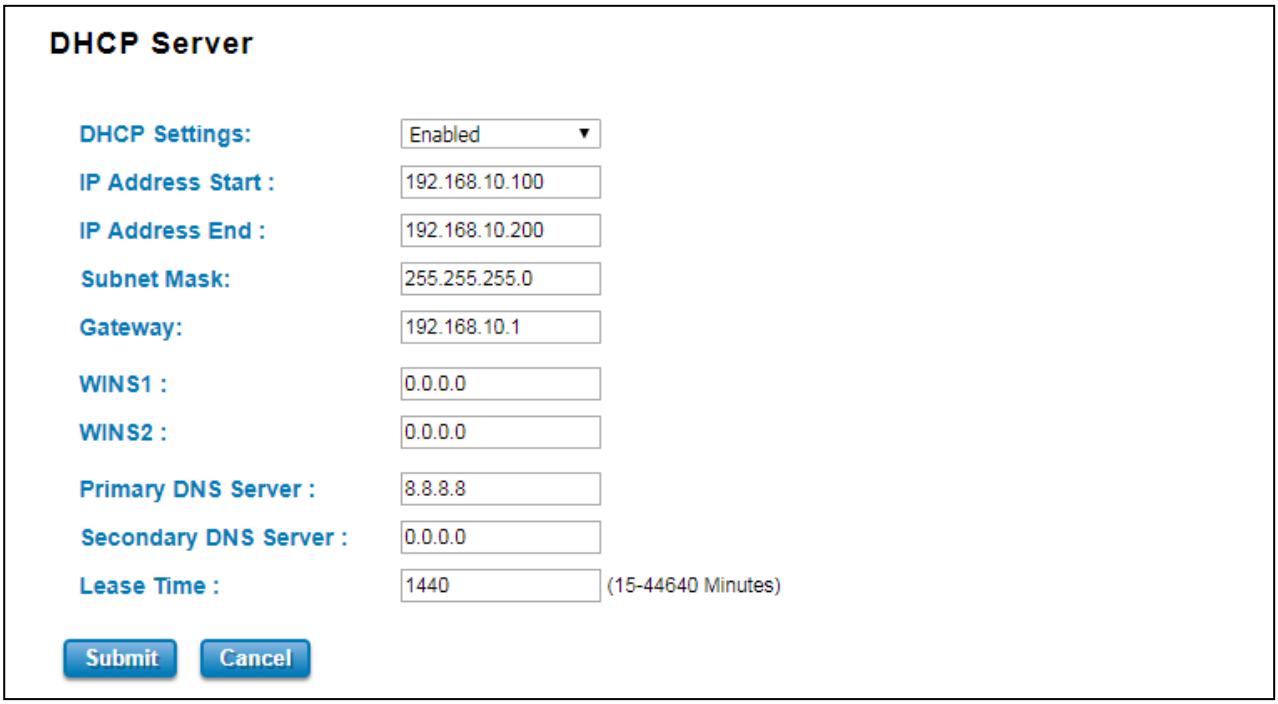
TERMS	DESCRIPTION
Current Time	User can configure time by input it manually. User also can click the **Get PC Time or Get Time from Cellular** to get the time setting. Get PC Time: get the time the PC Get Time from Cellular: get the time from the cellular network.
Time Zone	Choose the Time Zone section to adjust the time zone based on the user area.
NTP	**Enable NTP Client update** by checking this box. Input **Update interval** time. Select the time server from the **NTP Server** dropdown list or select **Manual IP** to manually input the IP address of available time server. ***Make sure that the device also has the internet connection.**

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

3.1.5 DHCP SERVER

DHCP Server Setting

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



The description of the columns is as below:

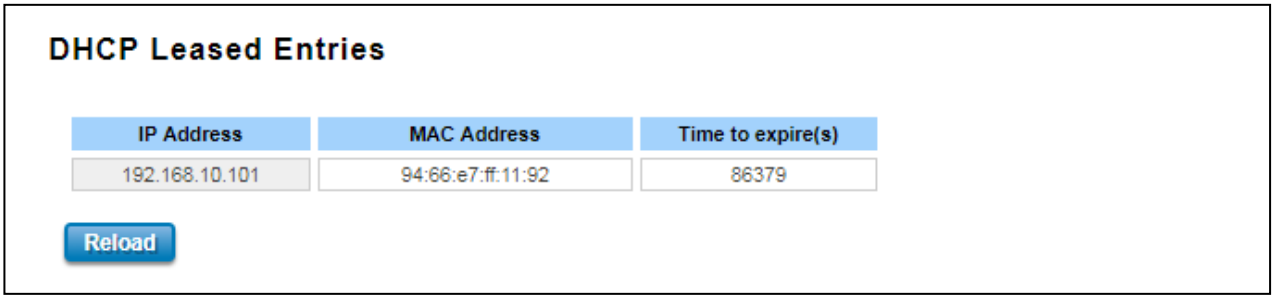
TERMS	DESCRIPTION
DHCP Setting	Select to **Enable** or **Disable** to activate and deactivate DHCP Server function.
IP Address Start	Assign the IP Address Start range.
IP Address End	Assign the IP Address End range.

Subnet Mask	**Default: 255.255.255.0** Assign the subnet mask for the IP address here for DHCP Server.
Gateway	Assign the gateway for the router here for DHCP Server.
WIN S1	Enter WINS Server 1 IP address
WIN S2	Enter WINS Server 2 IP address
Primary DNS Server	Enter Primary DNS Server that used in user network.
Secondary DNS Server	Enter Secondary DNS Server that used in user network.
Lease Time	**Default: 1440** The maximum length of time for the IP address lease. Enter the Lease time in minutes. (Lease Time range: 15-44640 minutes)

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

DHCP Leased Entries

The figure below shows the **DHCP Leased Entries.** It will show the MAC and IP address that was assigned by router. 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 router.
MAC Address	The MAC Address of the network interface that was used to acquire the lease.
Time to expire(s)	Remains time for the IP address from DHCP Server leased.

3.2 ETHERNET PORT

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

Following items are included in this group:

3.2.1 Port Status

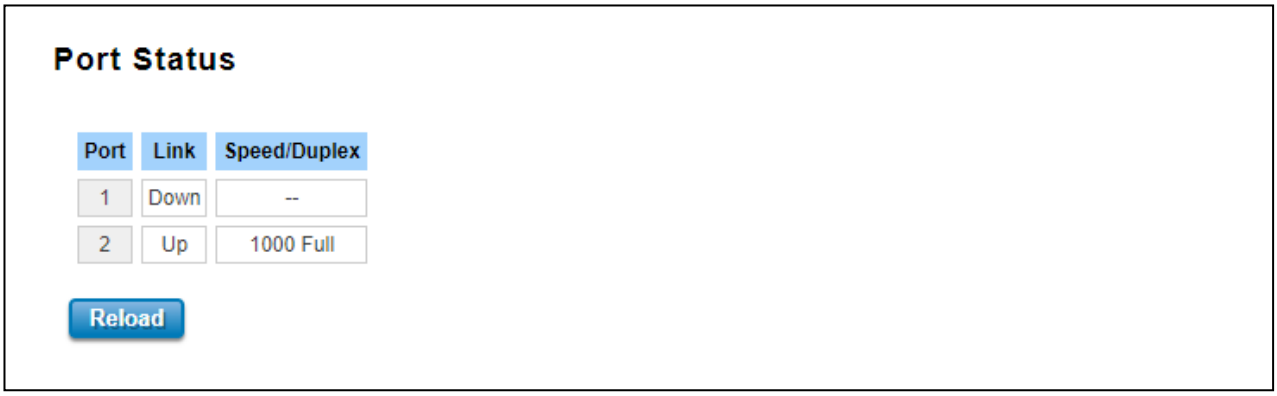
3.2.2 Port Setting

3.2.3 VLAN Setting

3.2.4 Traffic Control

3.2.1 Port STATUS

Port Status section allows users to see the current status from the Ethernet such as port state and speed/duplex



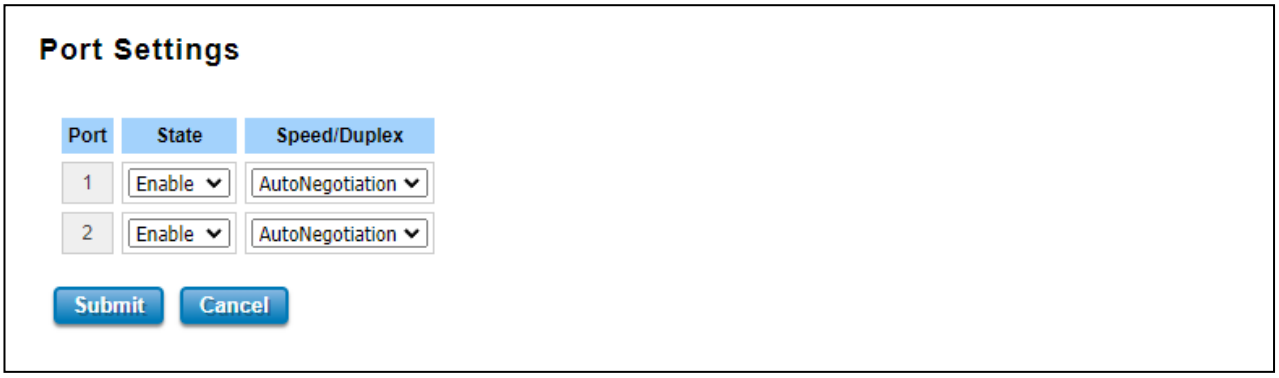
The description of the columns is as below:

TERMS	DESCRIPTION
Link	Display the Ethernet status, whether it is Link Up or Link Down.
Speed/Duplex	**Default: N/A** Show the Speed/Duplex for each port, such as 10 full,10 half,100 full,100 half mode for **Giga Ethernet Port 1~2 (ge1~ge2)**

Click on **Reload** to update the information.

3.2.2 Port SETTING

Use this page to configure the port setting such as the state and the speed / duplex for the Ethernet port.



The description of the Ethernet Setting page is as below:

TERMS	DESCRIPTION
Ethernet 1	**Default: Enable** **Default: Auto / Auto-Negotiation** Configure the Speed/Duplex of the port Ethernet 1. Users can set the bandwidth of each port as Auto-negotiation, 100 full, 100 half, 10 full, 10 half mode.
Ethernet 2	**Default: Enable** **Default: Auto / Auto-Negotiation** Configure the Speed/Duplex of the port Ethernet 2. Users can set the bandwidth of each port as Auto-negotiation, 100 full, 100 half, 10 full, 10 half mode.

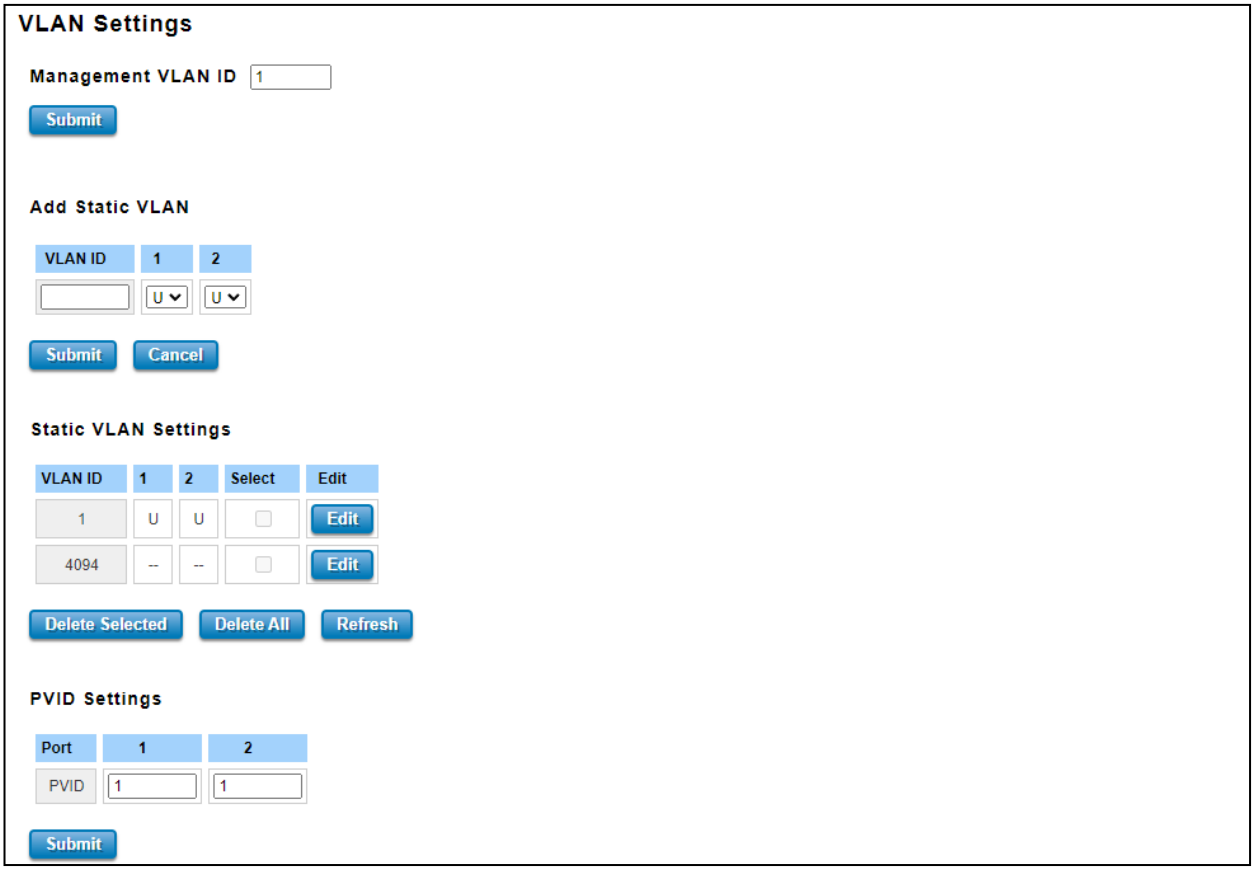
Click **Submit** to apply the configuration that just made.

3.2.3 VLAN SETTINGS

The router's LAN port (Port 1-8) supports VLAN feature.

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, User can segment User network without being restricted by physical connections—a limitation of traditional network design. To configure 802.1Q VLAN and port-based VLANs on the WoMaster switch, use the VLAN Settings page to configure the ports. User can assign Management VLAN, create the static VLAN, and assigns the Egress rule for the member ports of the VLAN.

The description of the columns is as below:



The description of the Ethernet Setting page is as below:

TERMS	DESCRIPTION
Management VLAN ID	**Default : 1**. The switch supports management VLAN. The management VLAN ID is the VLAN ID of the CPU interface so that only member ports of the management VLAN can ping and access the switch.
Add Static VLAN	By select the VLAN and click the Edit button, user can assign a VLAN ID or VLAN Name and User can specify the egress (outgoing) port rule to be **Untagged or Tagged**
Static VLAN Setting	At this section user can edit the VLAN that has been added, include the name and egress rule.
PVID Setting.	The abbreviation of the **Port VLAN ID**. PVID allows the switches to identify which port belongs to which VLAN. To keep things simple, it is recommended that PVID is equivalent to VLAN IDs. The values of PVIDs are from 0 to 4095. But, 0 and 4095 are reserved. User can't input these 2 PVIDs. 1 is the default value. 2 to 4094 are valid and available in this column.

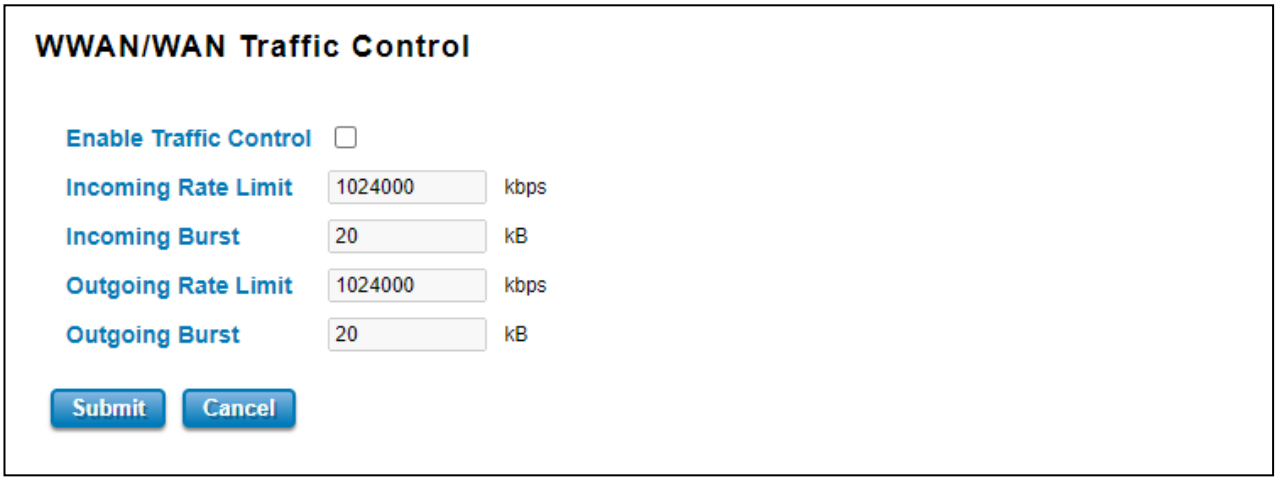
The steps to create a new VLAN: Type in Add Static VLAN section, and click **Submit** to create a new VLAN. Then User can see the new VLAN in the Static VLAN Setting table. After created the VLAN, the status of the VLAN will remain in Unused until User adds ports to the VLAN.

NOTE:

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

3.2.4 TRAFFIC CONTROL

Traffic control is a form of flow control used to enforce a strict bandwidth limit at a port. User can configure separate Incoming Outgoing rate limits and burst



The description of the columns is as below:

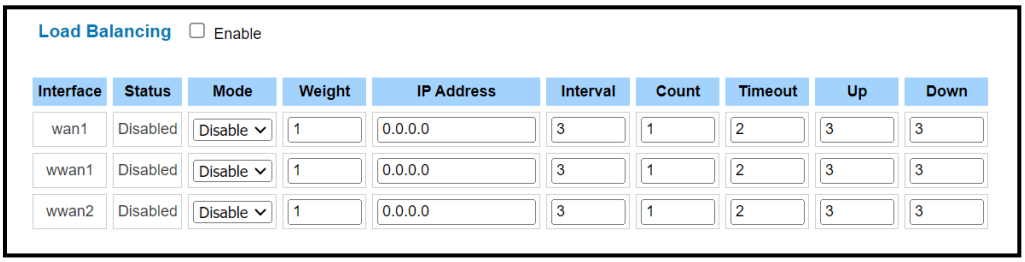
TERMS	DESCRIPTION
Enable Traffic Control	Check the box to activate the function
Incoming Rate Limit	**Default: 1024000 kbit/s** Set the maximum incoming rate.
Incoming Burst	**Default: 20 kBytes** Set the maximum incoming burst.
Outgoing Rate Limit	**Default: 1024000 kbit/s** Set the maximum outgoing rate.
Outgoing Burst	**Default: 20 kBytes** Set the maximum outgoing burst.

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

3.2.5 Load Balancing

Load balancing is a technique used to distribute network traffic across multiple servers or network links to optimize performance and reliability. It involves redirecting incoming requests to different servers or services based on various factors such as server availability, network conditions, or request type.

Load balancing helps to distribute the workload evenly across the available resources, preventing overloading any single server or link. This ensures that systems can handle increased traffic efficiently and provide a better user experience.

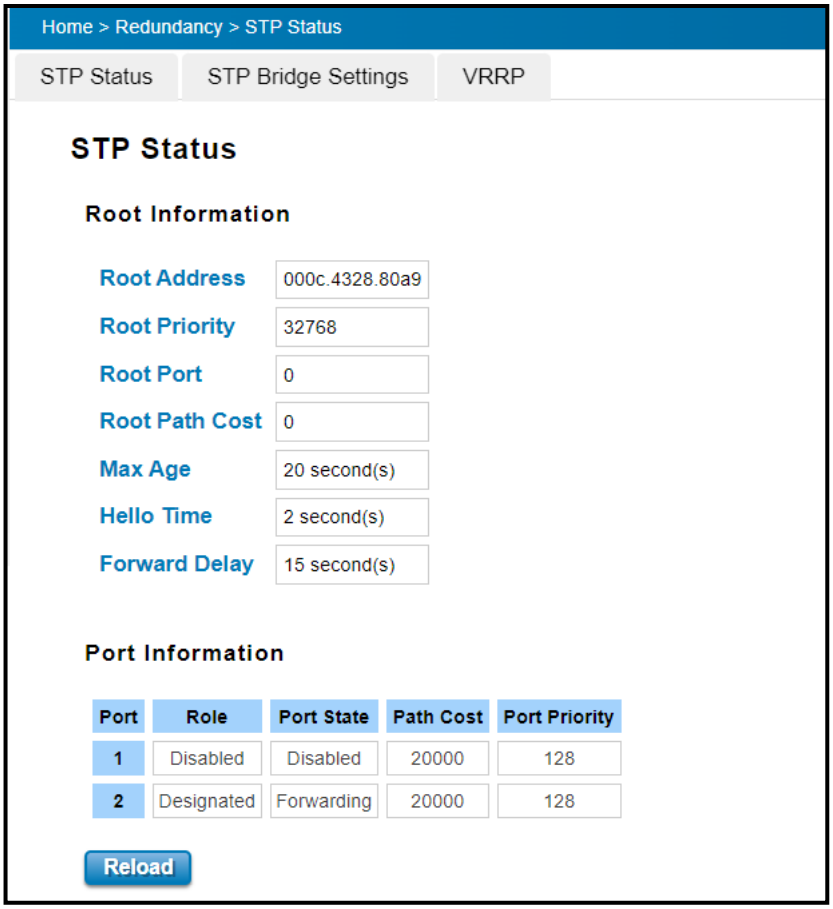


3.3 REDUNDANCY

Redundancy role of 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 connection is inadvertently disconnected or damaged. This switch is supported with VRRP (Virtual Routing Redundancy Protocol). 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. This is a particularly important feature for industrial applications, since it could take several minutes to locate the disconnected or severed connection.

3.3.1 STP STATUS

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

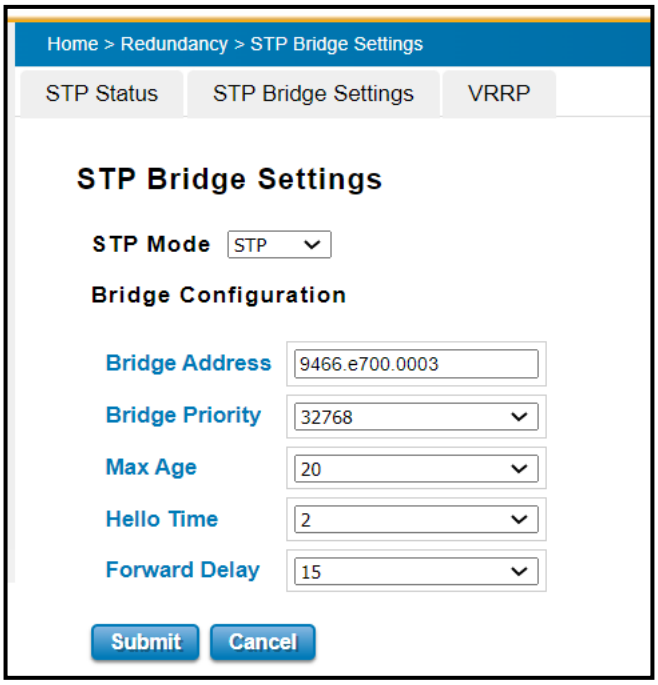


Root Information: User can see root Address, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root switch.

Port Information: User can see port number, port Role, Port State, Path Cost and Port Priority.

3.3.2 STP BRIGDE SETTING

The STP mode includes the **STP** and **Disable**. User can select the STP mode for user system first. The default mode is RSTP enabled. After user selects the STP mode; user should continue to configure the global Bridge parameters for STP.



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.

Bridge Configuration

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

Bridge 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.

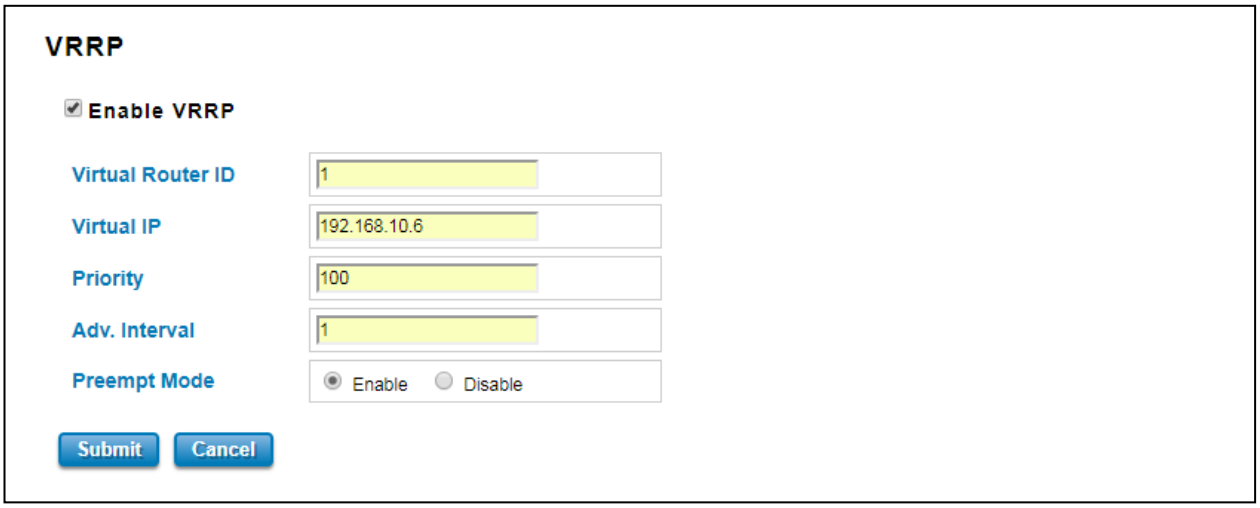
NOTE: User must follow the rule to configure Hello Time, Forwarding Delay, and Max Age parameters.

2× (Forward Delay Time – 1 sec) ≥ Max Age Time ≥ 2 × (Hello Time value + 1 sec)

3.3.3 VRRP

VRRP Setting

The field allows user 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.



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

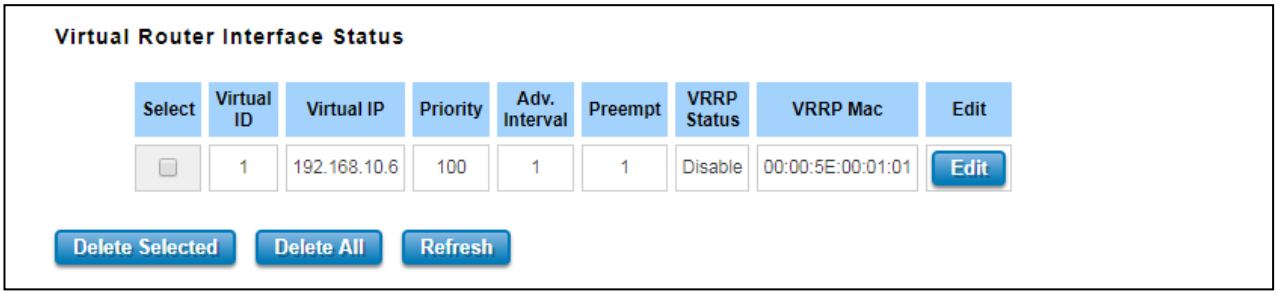
TERMS	DESCRIPTION
Enable VRRP	Check the box to enable the function.
Virtual Router ID	This is a virtual ID range from 1~255. The switches within the same VRRP domain should have the same Virtual ID.
Virtual IP	This is the virtual IP of the VRRP domain. This is the Gateway IP of the clients.
Priority	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.
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 restarting 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 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.



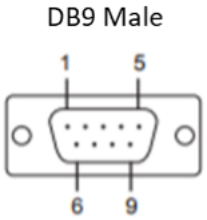
TERMS	DESCRIPTION
Interface	Show the interface for the VRRP domain.
VirtualID	This is a virtual ID range from 1~255. The switches within the same VRRP domain should have the same Virtual ID.
Virtual IP	This is the virtual IP of the VRRP domain. This is the Gateway IP of the clients.
Priority	The priority 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.

Click **Refresh** to refresh the list. Click **Select** to the specific list then user can do several actions such as **Edit** and **Delete Selected**. Click **Delete All** to delete all of the list.

3.4 SERIAL

This router also equipped with two serial ports which are RS232/422/485 ports that able to connect to local serial devices (Refer to the Appendix). And these serial ports support TCP Server, TCP Client, and UDP Listening. From the web management interface, it has two configuration pages for Serial 1 and Serial 2.

Below is the pin assignment



Pin	RS232	RS485-4w/422	RS485-2w
1	DCD	TX-	Data-
2	TXD	RX+	-
3	RXD	TX+	Data+
4	DSR	-	-
5	GND	GND	-
6	DTR	RX-	-
7	CTS	-	-
8	RTS	-	-
9	RI	-	-

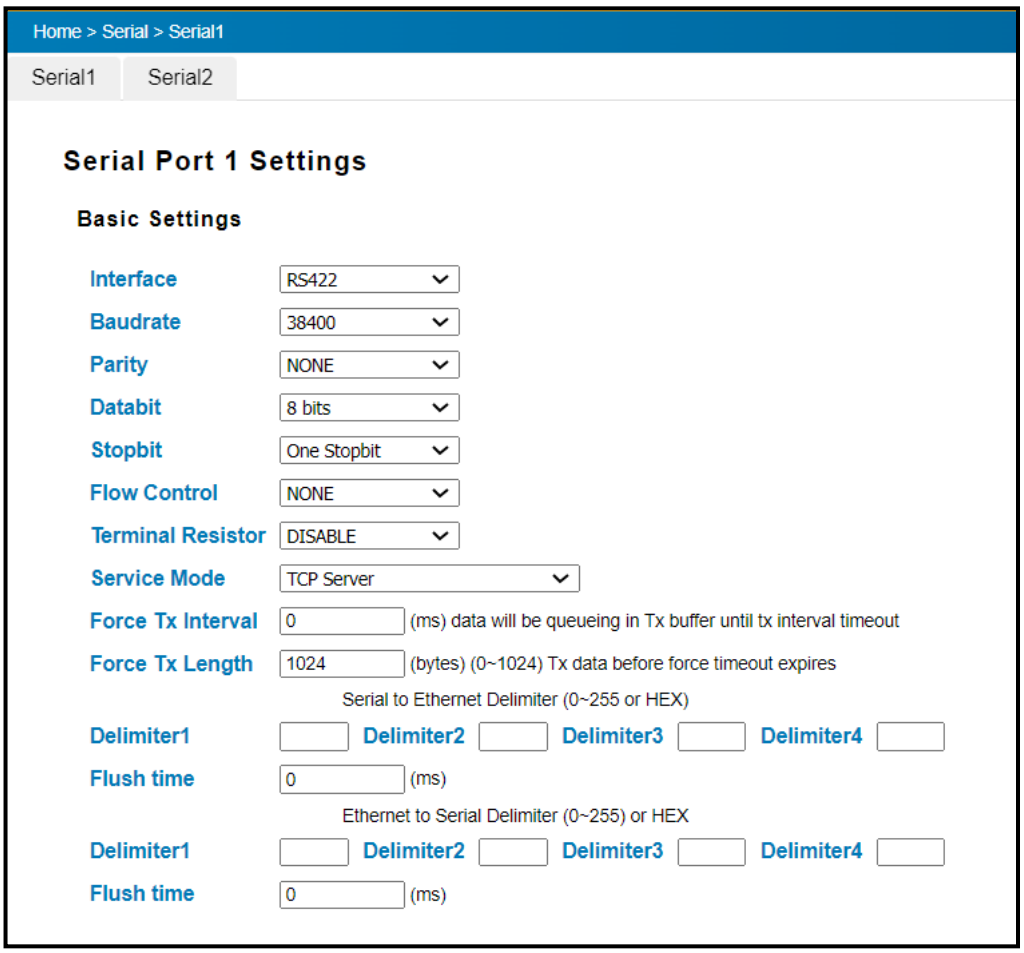
RS-232 is the most common serial interface and used to ship as a standard component on most Windows-compatible desktop computers. Now it is more common to use RS-232 over USB using a converter. RS-232 only allows for one transmitter and one receiver on each line. RS-232 also uses a Full-Duplex transmission method.

RS422 is an improved version of RS232, it uses twisted pair cable to reduce the noise, and it uses signaling balancing to transmit data, so what is signal balanced – It uses a voltage-difference between the two lines as an indication of the signal value, with this method the data is able to transmit for longer distance with faster data rates, with RS422 the data can transmit up to 10 Mbps at 50 feet or 100 Kbps at 4000 feet. RS422 is capable of multi-drop capability, it limits up to 10 slaves in the data line.

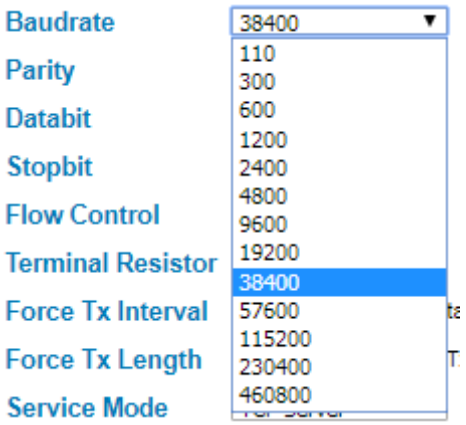
RS-485 is a superset of RS-422 and expands on the capabilities. RS-485 was made to address the multi-drop limitation of RS-422, allowing up to 32 devices to communicate through the same data line. Both RS-485 and RS-422 have multi-drop capability, but RS-485 allows up to 32 devices and RS-422 has a limit of 10.

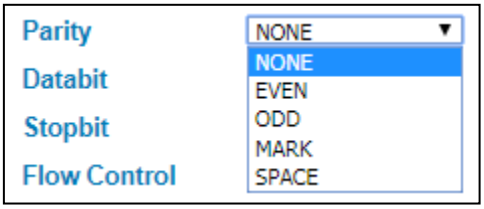
Serial 1 & 2

This configuration page is an interface to configure the serial setting.



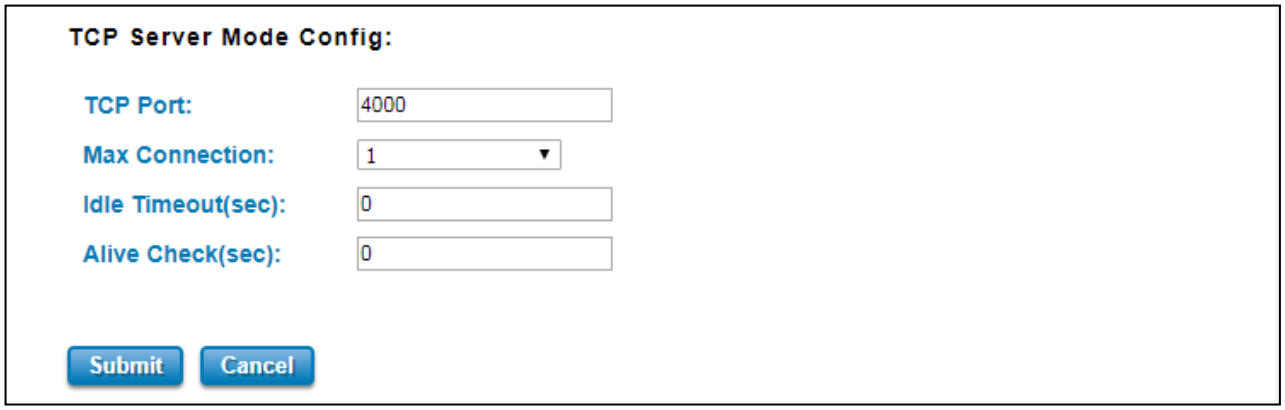
The description of the columns is as below:

TERMS	DESCRIPTION
Interface	**Default : RS422** Choose and change the interface type from the drop down list. The serial port supports the RS232, RS422, RS485-2w, and RS485-4w.
Baudrate	**Default: 38400** Serial baud rate, a speed measurement of communication. It indicates the number of bit transfers per second. 
Parity	**Default: NONE**

	Set parity bit of serial data.  For even and odd parity, the serial port will set the parity bit (the last bit after the data bits) to a value to ensure that the transmission has an even or odd number of logic high bits. Mark and space parity does not actually check the data bits, but simply sets the parity bit high for marked parity or low for spaced parity.
Databit	**Default: 8 bits** Indicates the number of bits in a transmitted data package.
Stopbit	**Default: One Stopbit** The stop bit follows the data and parity bits in serial communication. It indicates the end of transmission.
Flow Control	**Default: NONE** Flow control manages data flow between devices in a network to ensure it is processed efficiently. Too much data arriving before a device is prepared to manage it causes lost or retransmitted data.
Terminal Resistor	**Default: Disable** Enable to prevent serial signal reflection.
Service Mode	Choose TCP Server, TCP Client, and UDP listening.
Force TX Interval	**Default: 0 (ms)** Force TX interval time is to specify the timeout when no data has been transmitted and queue data before the time interval is expired.
Force TX Length	**Default: 1024 (bytes)** To specify the length of the data before Force timeout expires.
Serial to Ethernet	**Delimiter**: User can define max. 4 delimiters (0~255, Hex) for each way. The data will be held until Flush Time is expired. 0 means disable. The factory default is 0. **Flush Time**: The received data will be queued in the buffer until all the delimiters are matched. When the Flush Time is expired the data will be sent.
Ethernet to Serial	**Delimiter**: User can define max. 4 delimiters (0~255, Hex) for each way. The data will be held until Flush Time is expired. 0 means disable. The factory default is 0. **Flush Time**: The received data will be queued in the buffer until all the delimiters are matched. When the Flush Time is expired the data will be

	sent.

The other section from this Serial page is TCP Server Mode Config. This page allows user to configure the basic settings of TCP Server Mode.



The description of the columns is as below:

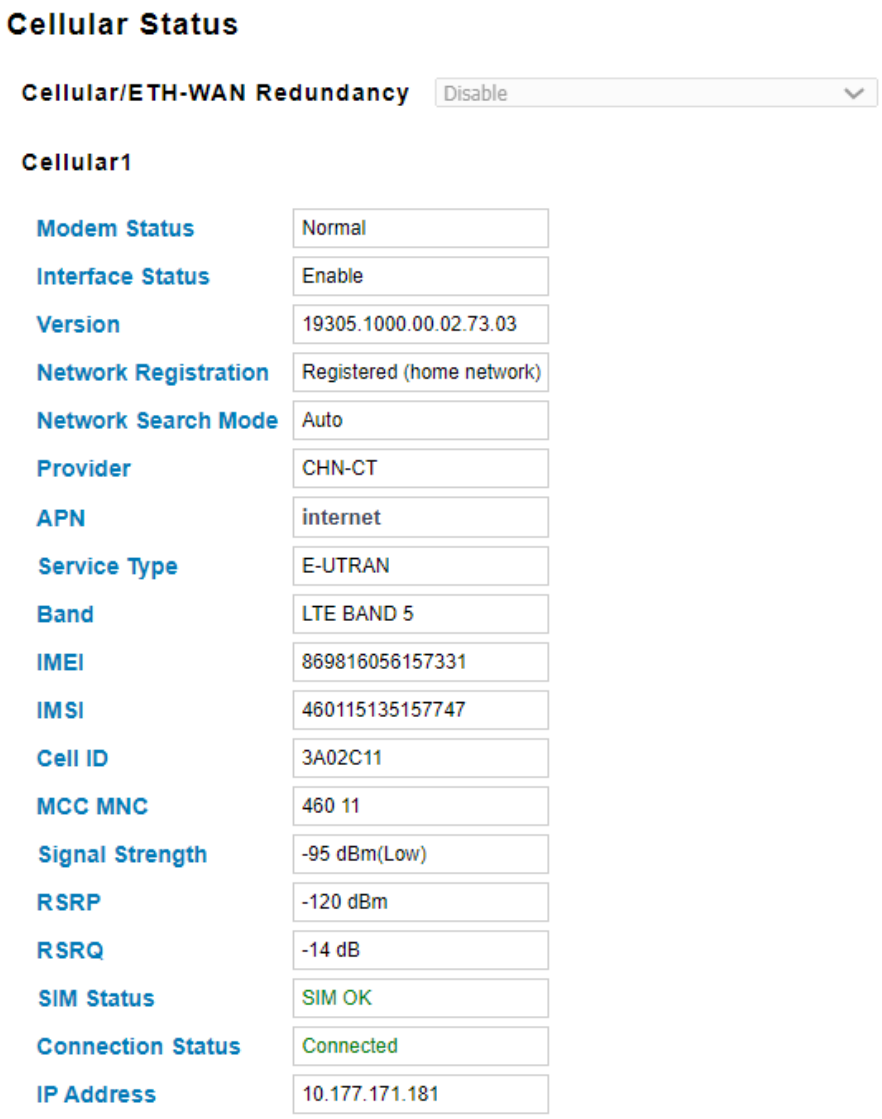
TERMS	DESCRIPTION
TCP Port	**Default: Serial 1 – 4000, Serial 2 - 4002** Assign the available TCP port number. The port number of TCP Server and TCP Client should be the same.
Max Connection	Configures the maximum connection number from 1 to 5.
Idle Timeout (sec)	When serial port stops data transmission for a defined period of time (Idle Timeout), the connection will be closed and the port will be freed and re-try for connection with other hosts. Zero is disabled this setting (default). If Multilink is configured, only the first host connection is effective for this setting.
Alive Check (sec)	The device will send a TCP alive check package in each defined time interval (Alive Check) to remote host to test the TCP connection. If the TCP connection is not alive, the connection will be closed and the port will be freed for other hosts. If user sets it as zero, it means disable this setting.

3.5 CELLULAR

This Cellular page provides the Cellular Status; configure Cellular Setting, and configure SIM Setting. WoMaster Industrial Router is supported with redundant SIM and Dual SIM Card; user can choose SIM1 or SIM2 for the main SIM Card.

3.5.1 CELLULAR STATUS

The figure below shows Cellular Status.

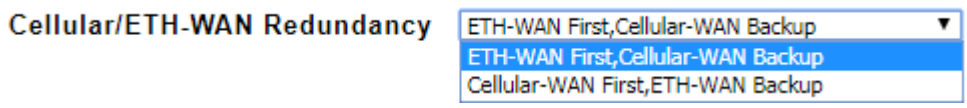


Cellular2

Modem Status	Normal
Interface Status	Enable
Version	19010.1000.00.02.73.16
Network Registration	Registered (home network)
Network Search Mode	Auto
Provider	CHN-CT
APN	internet
Service Type	E-UTRAN
Band	LTE BAND 3
IMEI	869816055123391
IMSI	460110174183033
Cell ID	3A2A732
MCC MNC	460 11
Signal Strength	-73 dBm(Excellent)
RSRP	-97 dBm
RSRQ	-5 dB
SIM Status	SIM OK
Connection Status	Connected
IP Address	10.147.120.60

Reload

The description of the columns is as below:

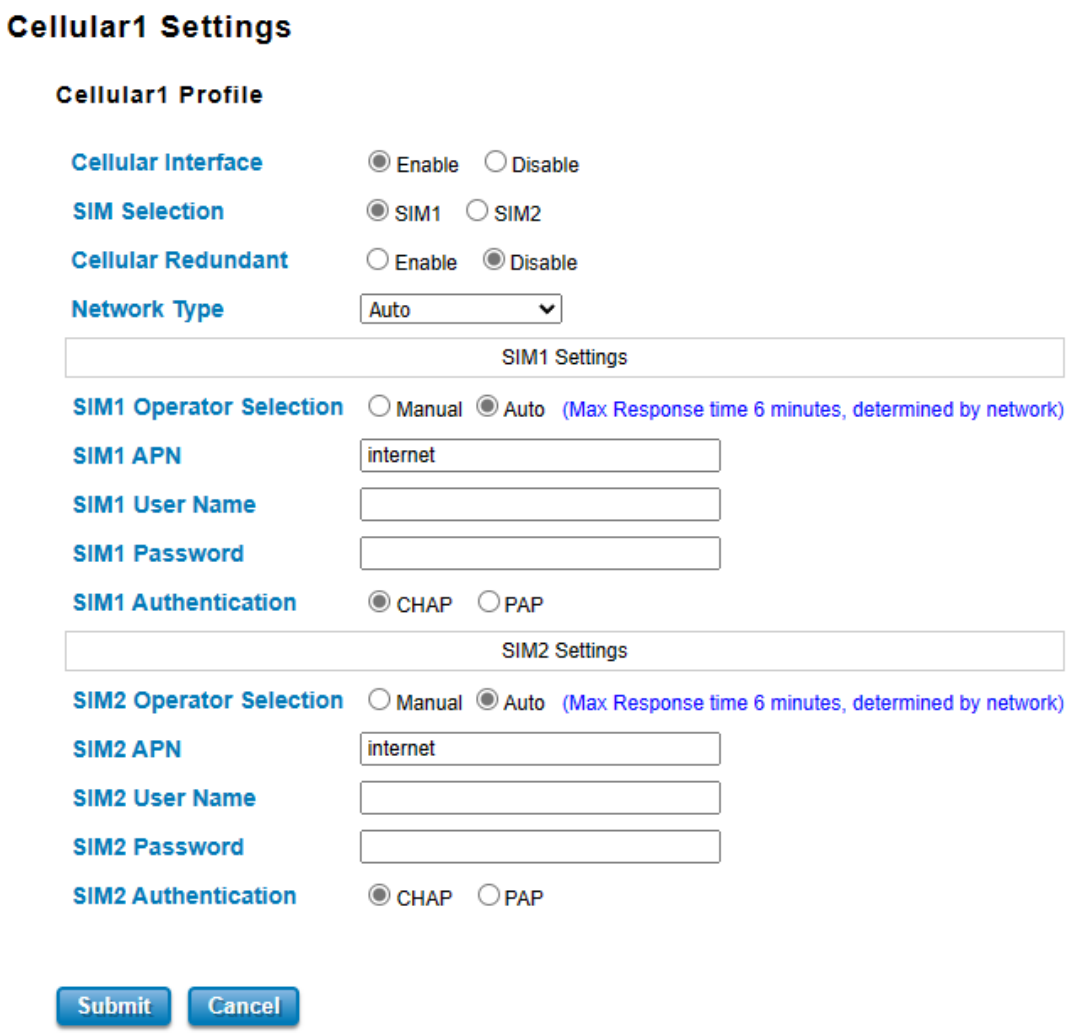
TERMS	DESCRIPTION
Cellular/ETH.WAN Redundancy	**Default: Disabled** User can choose the redundancy mode:  **ETH-WAN First, Cellular-WAN Backup**: by choosing this mode, the redundancy mode would be like prioritize the ETH-WAN connection; if the ETH-WAN connection has a problem then the Cellular-WAN would be the backup connection. **Cellular-WAN First, ETH-WAN Backup**: by choosing this mode, the redundancy mode would be like prioritize the Cellular-WAN connection; if the Cellular-WAN connection has a problem then the ETH-WAN would be the backup connection.
Modem Status	Display the modem status
Interface Status	Display the Cellular interface status Enabled or Disabled
Version	Display the firmware version of the cellular module.

Network Registration	Display the status of the network registration
Network Search Mode	Display the network search mode (Auto, 2G Only, 3G Only and LTE Only)
Current SIM Index	Display the current in used SIM card (1 or 2)
Provider	Display the ISP (MCC+MNC) that user used.
APN	Every ISP has a specific APN (Access Point Name) assigned to its cellular network. The system can read this name from the SIM card.
Service Type	The connected ISP will update the service type here. The possible types are GSM – 2G, UMTS – 3G, GSM W/EGPRS, UTRAN W/HSDPA (download), UTRAN W/HSUPA(upload), UTRAN W/HSDPA and HSUPA(download & upload), E-UTRAN - LTE , No Service(default value)
Band	Display the connected band
IMEI	Display the International Mobile Equipment Identity (IMEI)
IMSI	Display the International Mobile Subscriber Identity (IMSI)
Cell ID	Display the Cell Identity (CID)
Signal Strength	The signal strength to the remote connected base station. If the signal strength shows low, please change the device location or mounting the antenna in better location. Below are the signal strength definitions in our system: Low: -113 dBm or less~-95 dBm Medium: -93 dBm ~ -85 dBm Good: -83dBm ~-75 dBm Excellent:-73 dBm ~-51 dBm Not known or not detectable: No base station detected
RSRP	Display the RSRP(Reference Signal Received Power) value. The higher value indicates better signal power.
RSRQ	Display the RSRQ (Reference Signal Received Quality) value. The higher value indicates better signal quality.
SIM Status	Show the installed SIM Status. **SIM OK:** The SIM card is okay to use. **SIM not inserted:** The SIM card is not inserted. **SIM PIN Locked:** The SIM card is locked due to PIN error. It may be caused by error typing PIN password many times. **SIM PUK Locked:** The SIM Card PUK is locked due to PIN error after user three times input the wrong password. Contact the ISP to resolve the issue.
Connection Status	**Connection Status:** **Connected:** The cellular interface is connected. **Not Connected:** The cellular interface is not connected.
IP Address	The IP Address assigned by the ISP. While the cellular is connected, the IP address will display here.

3.5.2 CELLULAR SETTING

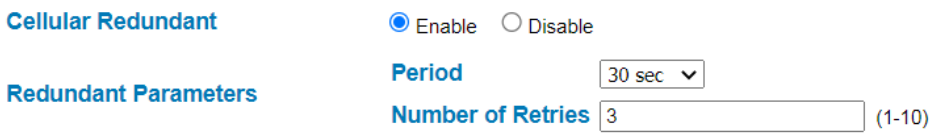
This section displays the Cellular Setting configuration page and also in this configuration page user may activate the redundant SIM function. In this section, user may Enable/Disable the Cellular Interface, SIM Selection, Cellular Redundant, Network Type; SIM 1/2 settings include the Operation code (MCC+MNC), APN, User Name, Password and the Authentication mode. The system will check the status of the cellular module every few seconds, if it can't be configured, please wait a few second or refresh the web interface. After you changed the setting, the router will reconnect to the base station and you will need to wait couple seconds for the new connection.

The figure below is the interface of the router:



The description of the columns is as below:

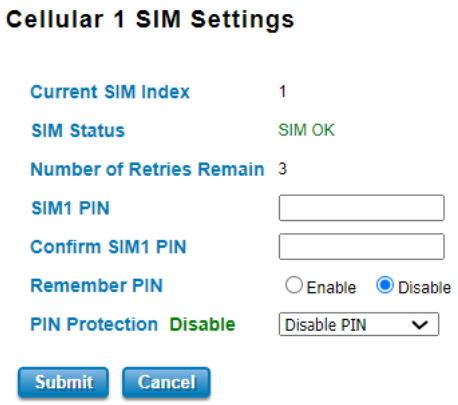
TERMS	DESCRIPTION
Cellular Interface	To enable or disable the cellular interface. Click check to disable the function.
SIM Selection	**Default: SIM1** User can select the SIM card 1 or 2 that want to be activated or used. Not every model supports dual SIM, if the hardware doesn't support dual SIM, the SIM2 setting is not available.
Cellular Redundant	**Default: Disable**

	By enable this function, the SIM redundant function will be activated. The main function of this feature is to have the backup SIM if the main SIM card is unable to use or have a problem connection.  **Redundant Parameters** configuration appears after the user enables the function. If the SIM card cannot be read after the redundant parameters are expired then it will directly change to read the other SIM card. **Period:** Set the period time to read the SIM card. The default value is 30 Seconds. **Number of Entries:** Set the number of entries to give the remaining trial to read the SIM card. The default value is 3.
Network Type	Set the Network Type, the option would be: **Auto: Search the network automatically** **2G Only: only receive the 2G signal.** **3G Only: only receive the 3G signal.** **LTE Only: only receive LTE/4G signal.** **NR5G: only receive the 5GNR signal, or known as 5GNR SA mode.** **LTE+NR5G: available to receive the 5GNR signal, or known as 5GNR NSA mode.** The network type in different models is different. The GUI only shows the available type.
SIM1/2 APN	Set the APN of the carrier provider.
SIM1/2 Operation Code(MCC+MNC)	Set the **MCC Mobile Country Code) + MNC (Mobile Network Code)** of the carrier provider. You can get the number while you apply the service from your carrier provider. For example, the 46692 represents MCC=466 + MNC=92. The 466 represent for Taiwan, 92 represent for Chunghwa Telecom LDM, the network provider in Taiwan. **Note:** We have APN/MCC+MNC code of the known providers written into our system, but, it may not cover all countries/operators. If you can't connect to internet, please double check the APN and MCC+MNC code and enter the correct number manually.
SIM1/2 User Name	Set the User Name
SIM1/2 Password	Set the password.
SIM1/2 Authentication	Choose CHAP or PAP mode for the authentication mode. **CHAP**: Challenge Handshake Authentication Protocol, With CHAP, the authenticator (i.e. the server) sends a randomly generated ``challenge'' string to the client, along with its hostname. **PAP**: Password Authentication Protocol, PAP works basically the same way as the normal login procedure. The authenticates itself by sending a user name and a password to the server

3.5.3 SIM SETTING

This section displays the SIM configuration such as SIM Status and SIM pin configuration. And in this section, user can enable or disable the SIM protection function. Apply the PIN number to the SIM cards; and make sure user enters the correct PIN number when activating the connection, after that the connection will start working. And also user can change the new PIN settings.

The figure below belongs to the single SIM model:



TERMS	DESCRIPTION
Current SIM Index	Display the current in used SIM Card slot (1 / 2)
SIM Status	Show the installed SIM Status. **SIM OK:** The SIM card is okay to use. **SIM not inserted:** The SIM card is not inserted. **SIM PIN Locked:** The SIM card is locked due to PIN error. It may be caused by error typing PIN password many times. **WARNING:** SIM PUK Locked status will appear when the SIM Card PUK is locked due to PIN error after user three times input the wrong password. Contact the ISP to resolve the issue.
Number of Retries Remain	Display the remaining chance to enter the PIN numbers.
SIM1PIN	Enter new SIM1/2 PIN numbers
Confirm SIM1PIN	Confirm the new SIM1/2 PIN numbers
Remember PIN	Click enable to save the PIN numbers
PIN Protection	Activate the PIN protection feature. Choose the mode from the drop list. **Disable PIN**: Disable the PIN Protection feature **Enable PIN**: Activate the PIN Protection feature **Change PIN**: Change the PIN number, make sure user type the new PIN Number first at the SIM1 PIN textbox.

Click **Submit** to apply the configuration.

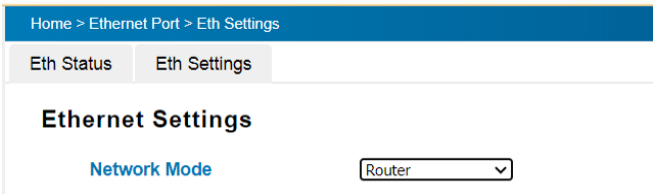
3.5.4 Cellular Diag

The Celluar Diag is used to get further information for the device of cellular records.

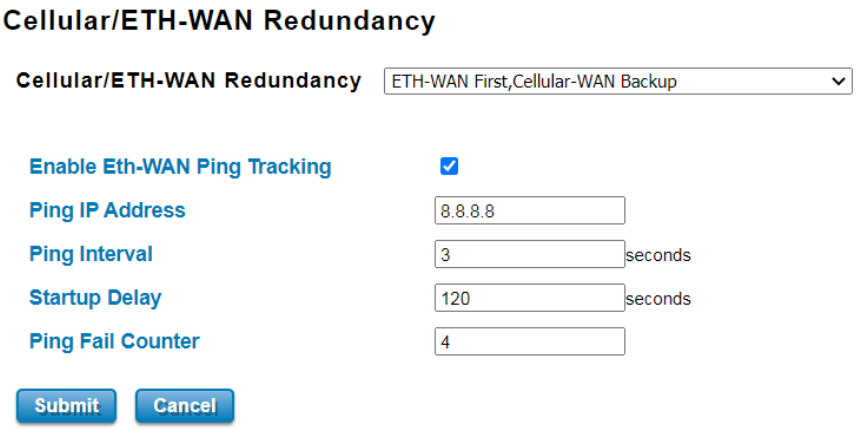
TERMS	DESCRIPTION
Generate Diagnosis File	Klick the button “Generate” and wait for 10S to generate the log file.
Download Diagnosis File	Klick the button “Download” for the log file.

3.5.5 CELLULAR/WAN REDUNDANCY

The feature allows user setup the WAN to Cellular redundancy while Ethernet-WAN port link down or unexpected failure, the cellular is activated automatically. Before enabled the feature, you should enabled the Ethernet Setting in Router mode, which means the two Ethernet ports are separated to different network interface, the port 1 acts as WAN port and port 2 acts as LAN port.



The Cellular/Eth-WAN Redundancy setup page:



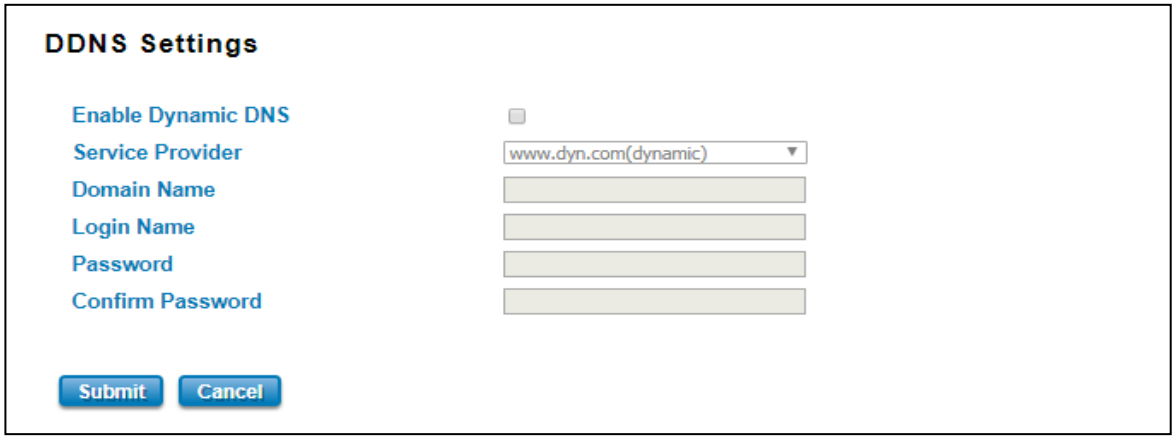
The description of the columns is as below:

TERMS	DESCRIPTION
Cellular/Eth-WAN Mode	Choose which is the main WAN interface and which is backup? **ETH-WAN First, Cellular-WAN Backup (Default)** or **Cellulr-WAN First, Eth-WAN Backup**:

Enable Eth-WAN Ping Tracking	You can enable the Ping tracking to check the active status of the WAN interface. After enabled and configured following settings, the router will continuously check the status of the target IP address, once the router can't pin the target IP, the backup interface will be activated immediately.
Ping Interval	Ping interval time, default: 3 second
Startup Delay	The router starts Ping tracking after the Startup Delay time. Default: 120 Note: Considering the WAN interface may not get IP immediately after system startup, please remain startup delay time longer.
Ping Fail Counter	The counter indicates how many times ping fail means WAN interface failure. Default: 4

3.5.6 DDNS SETTING

The DDNS (Dynamic Domain Name Service) is a method of keeping a domain name mapping to a dynamic public IP address. A dynamic public IP address is assigned for every connection request. After the user sets up the DDNS service, the DDNS service provider will automatically update the connection information if the public IP address has been changed. In this section, the user may configure the DDNS Setting.

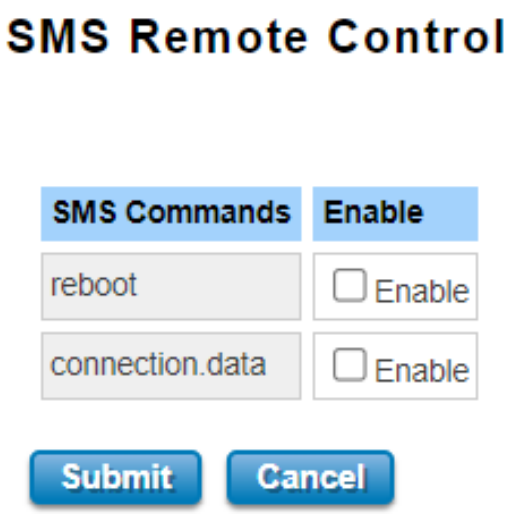


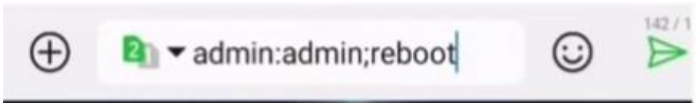
TERMS	DESCRIPTION
Enable Dynamic DNS	Check the box to enable the function
Service Provider	Select the Domain service provider from the list.
Domain Name	Enter the domain name
Login Name	Enter Login Name that used when applying the domain name
Password	Enter Password that used when applying the domain name
Confirm Password	Enter the Password once again to confirm.

After finishing configure any of the above setting, click on **"Submit"** to apply the configuration. Click "**Save -> Save to Flash**" to permanently save the configuration.

3.5.7 SMS REMOTE CONTROL

User can send the SMS message to remote reboot the router and get the connection data information. “Enable” the SMS Commands through the Web GUI, and then you can send the command from your cellphone.



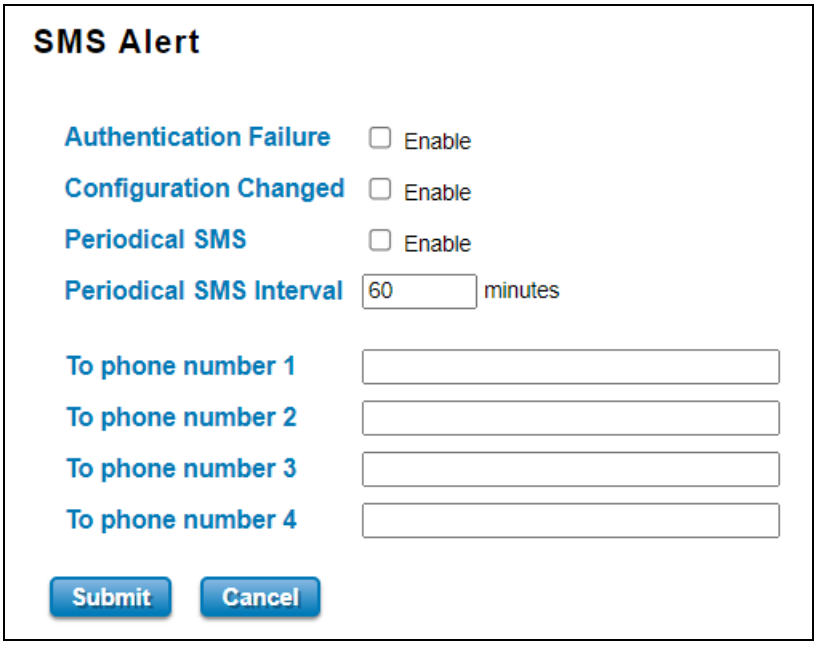
TERMS	DESCRIPTION
Reboot	Enable -> User can remote reboot the router by sending the SMS commands. The SMS message format is “**User_Name:Password;reboot**”. Example: select the router’s phone number, type message” **admin:admin;reboot**”.  The cellphone will received the reply: “OK”. And then the router will be rebooted later. 
Connection.data	Enable -> User can get the connection status/information of the target router. The information includes IMEI, signal strength, IP address and ICCID. The SMS message format is “**User_Name:Password;connection.data**”. Example: select the router’s phone number, type message” **admin:admin;connection.data**”. The cellphone will received the reply: “OK”. And then the router will send the cellular connection data to the phone.

Note: The router support SMS message to reboot router currently, if you have other need, please contact our Sales/Service div., we can discuss this by project need.

3.5.8 SMS Alert

SMS alerts, also known as SMS notifications or text alerts, are messages that are automatically sent to subscribers who have indicated that they want to receive text messages.



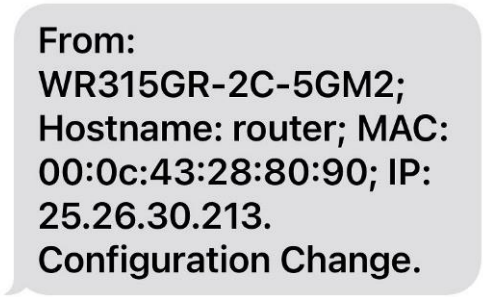
The description of the columns is as below:

TERMS	DESCRIPTION
Authentication Failure	Enable -> The router will send Authentication Failure SMS message to the target phone number while someone try login with the incorrect username/password.
Configuration Changed	Enable -> The router will send Configuration Changed message to the target phone number while someone try login with the incorrect

	username/password.
Periodical SMS	Select the Periodical SMS Alert to Enable
Periodical SMS Interval	Set the Periodical SMS Interval time.
To phone number 1	Set the phone number
To phone number 2	Set the phone number
To phone number 3	Set the phone number
To phone number 4	Set the phone number

Below figure is an example of the received “Configuration Change” SMS Alert.

Below figure is an example of the received “Configuration Change” SMS Alert.

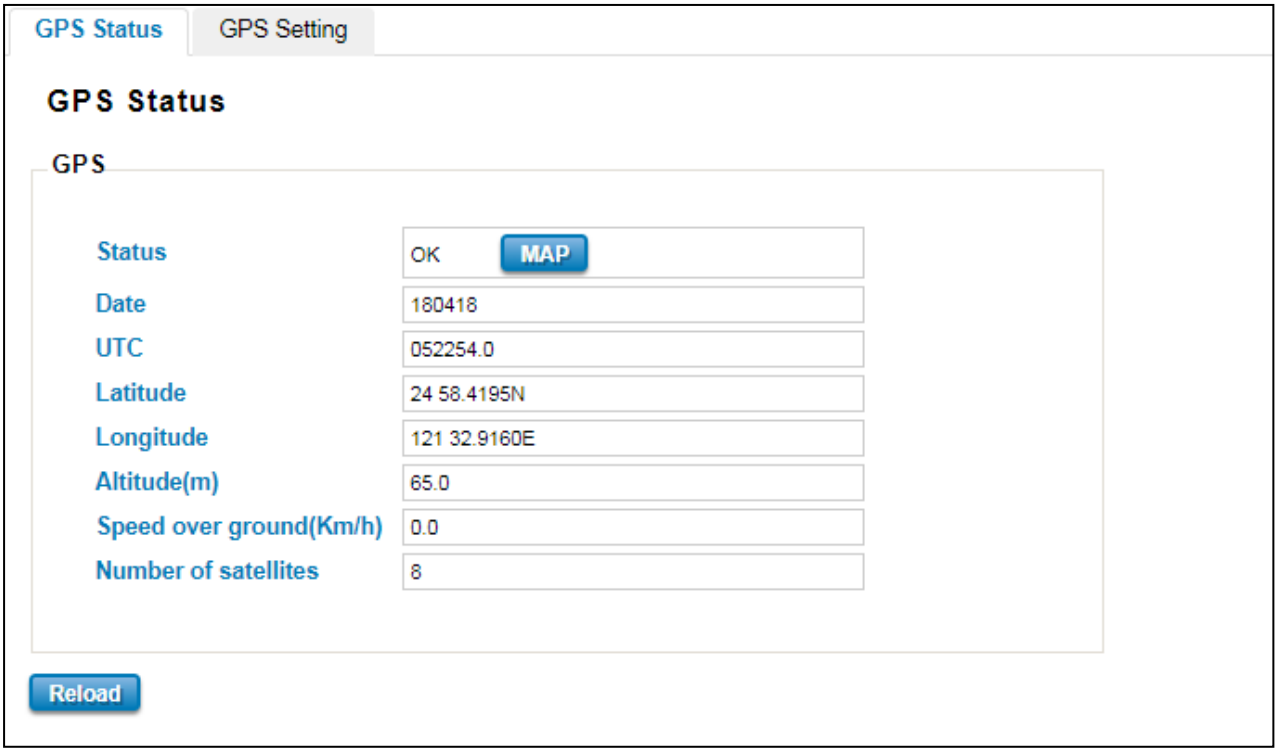


3.6 GPS

This GPS section has the function to show the current position of the device. The purpose of this feature is to display the location of each device if there is device installation in large number. It could help the technician to track the device location. WoMaster GPS feature is supported with the Global Navigation Satellite Systems use satellite technology to provide insight on the geographic location of connected devices. GNSS is an inclusive term for the category of global systems including GPS, GLONASS, BeiDou, and Galileo. Modern positioning and timing modules have evolved to take advantage of multiple GNSS constellations at once. Combining multiple satellite systems improves availability of signals, gives operators more access, and increases accuracy. Recent driving tests combining GPS and GLONASS showed a noticeable improvement in both precision and performance when compared with single system results. Whether user is navigating a position in a crowded city, a vast desert, or a dense forest, utilizing multiple GNSS systems can help the device stays connected and centered.

3.6.1 GPS STATUS

The first configuration page is GPS Status, where user can see all of the GPS information such as the GPS Status, Date, UTC, Latitude, Longitude, Altitude (m), Speed over ground(Km/h) and the Number of satellites.

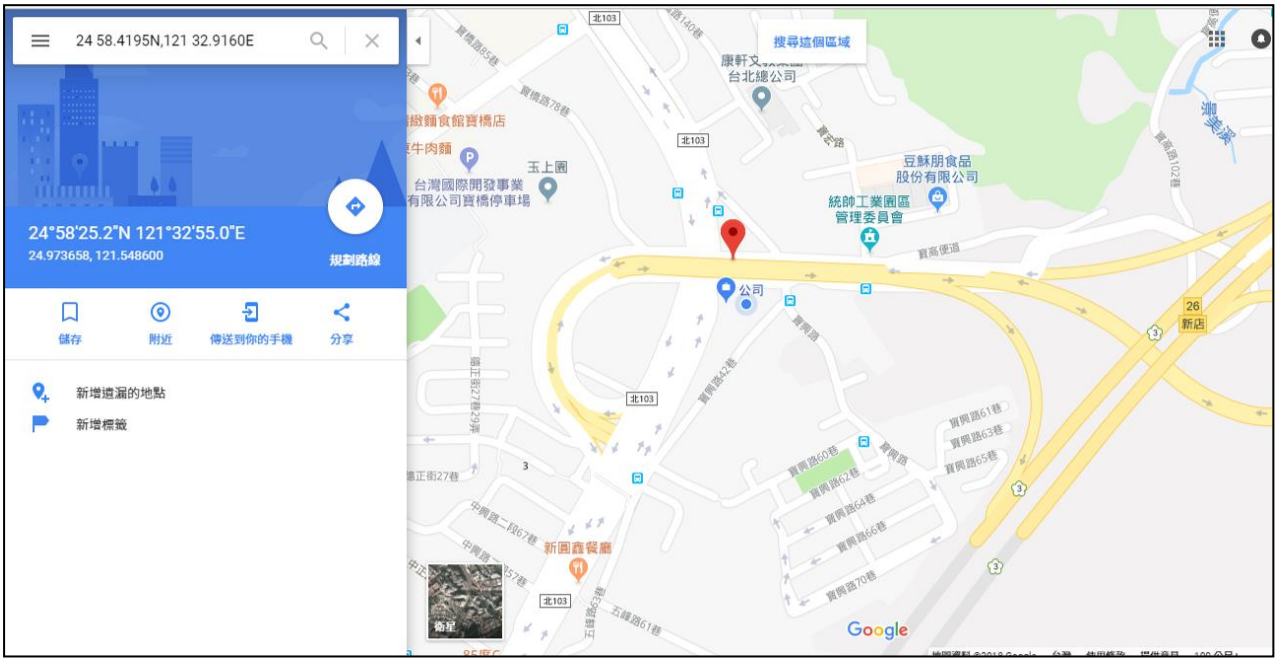


The description of the columns is as below:

TERMS	DESCRIPTION
Status	Display the GPS interface status OK or Disabled
Date	Display the current date.
UTC	Display the Coordinated Universal Time (UTC)
Latitude	Display the latitude of the coordinate

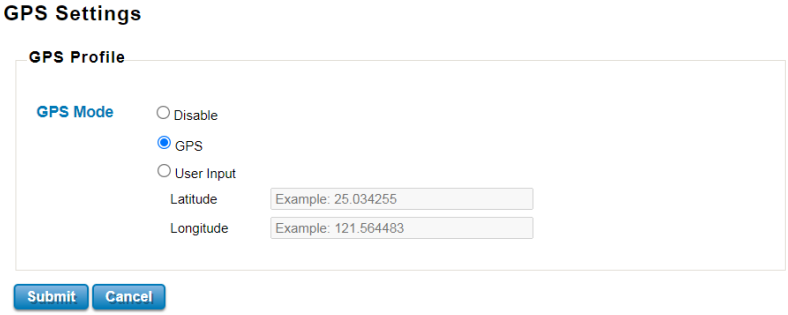
Longitude	Display the longitude of the coordinate
Altitude(m)	Display the altitude of the coordinate show the height or distance of an object from sea level.
Speed over ground(Km/h)	Display the speed over ground.
Number of satellites	Display the number of satellites that help to fix the position (Minimum 4 satellites).

At the status section, a MAP button appears. Click this button to show the specific location of your device through the Google Maps. After user clicks the button, the figure below will be appeared.



3.6.2 GPS SETTING

In this GPS Setting section, user can enable/disable the GPS Interface or Type specific GPS location by User Input.



The description of the columns is as below:

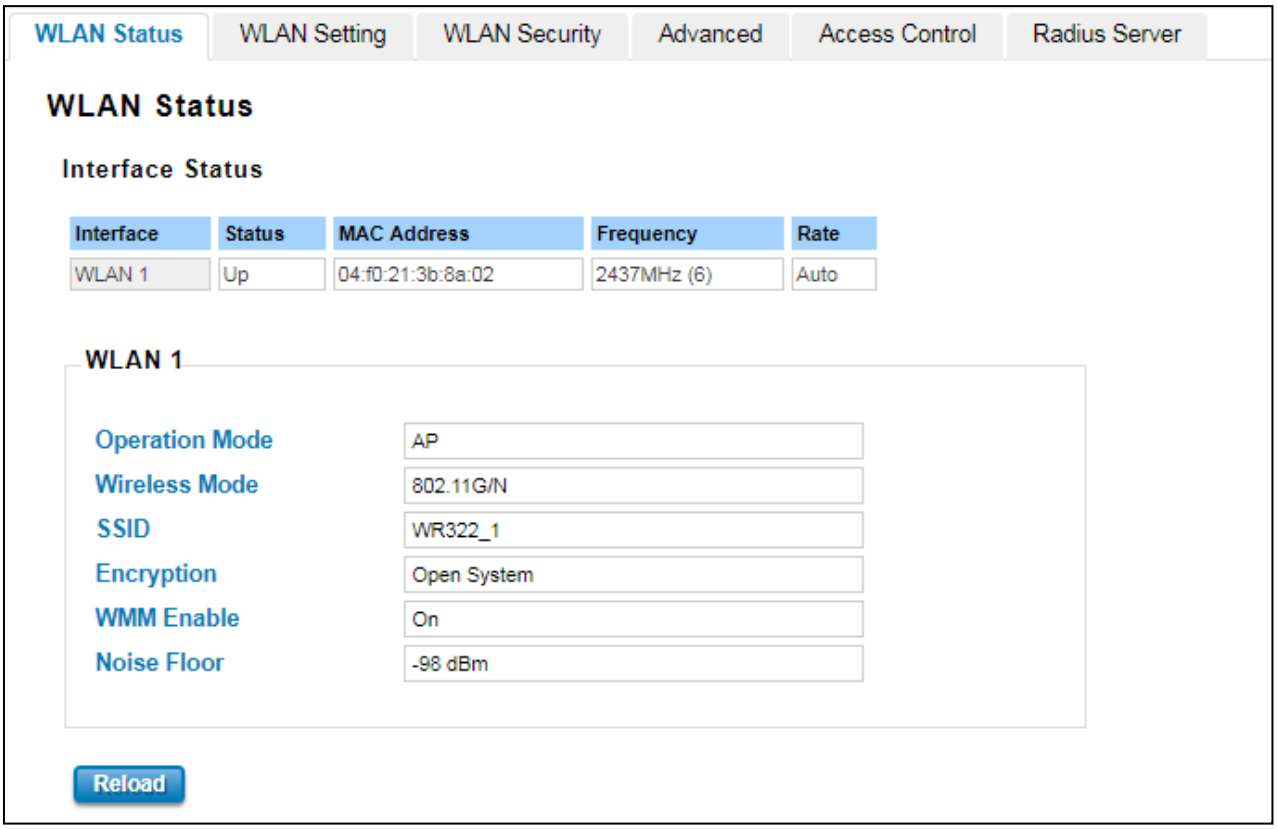
TERMS	DESCRIPTION
Disable	Display the GPS interface status OK or Disabled
GPS	Enable the GPS interface. Note that the GPS antenna must be installed.
User Input	Type the specific Latitude and Longitude address for your router.

3.7 WIRELESS LAN (MODEL with Wi-Fi 5)

This Wireless LAN configuration pages only support the device that supported with Wi-Fi feature. This configuration page allows users to configure the Wireless LAN configuration. Several settings are provided here such as the WLAN Status, WLAN Setting, WLAN Security, Advanced and the Auto Offload.

3.7.1 WLAN STATUS

The figure below shows the WLAN status.



The description of the columns is as below:

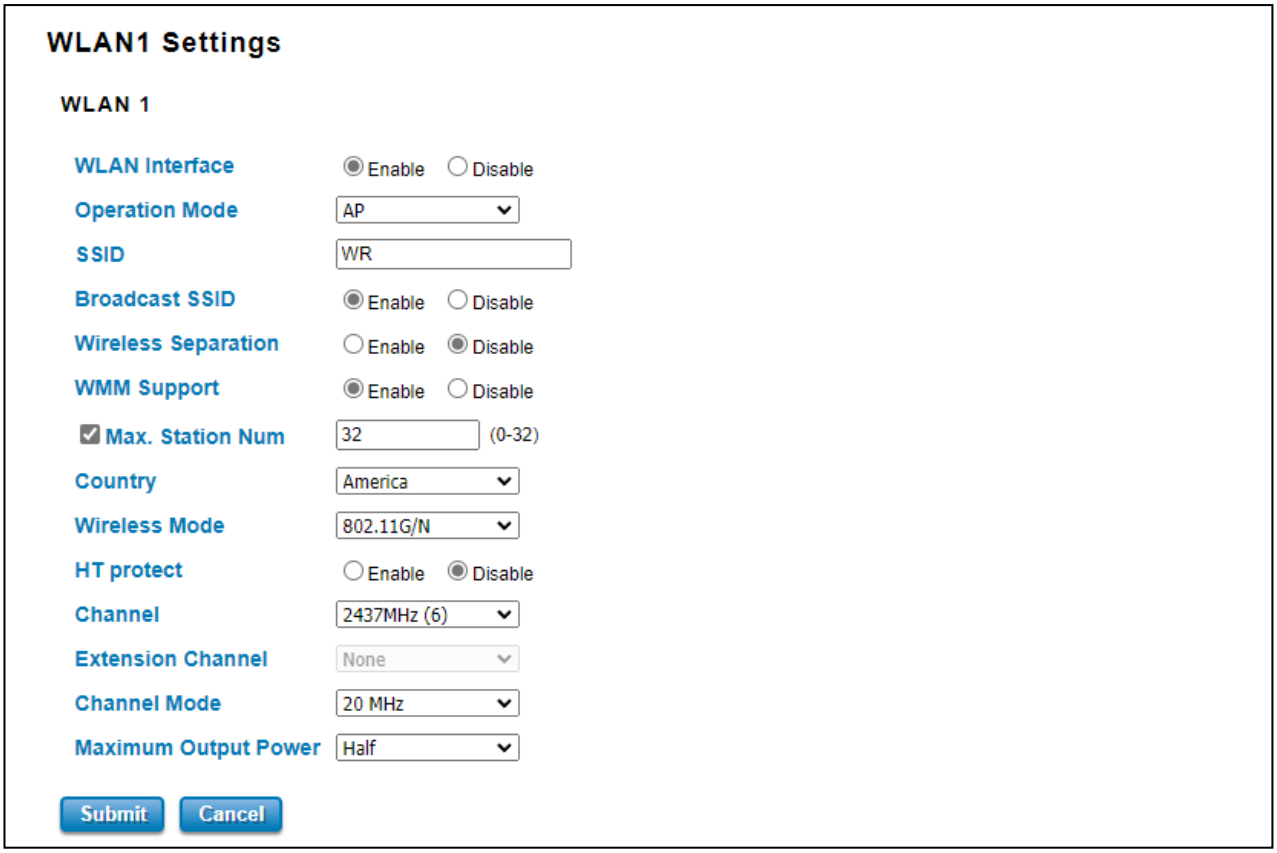
TERMS	DESCRIPTION
Operation Mode	Display the current operating modes on the device
Wireless Mode	Display the current wireless mode
SSID	Display the primary name of the SSID
Encryption	Display the encryption mode.
WMM Enable	Display the status of the WMM support.
Noise Floor	Display the background noise level.

3.7.2 WLAN SETTING

WLAN Setting page, on this page user may configure the parameters for Wireless LAN Interface includes change wireless interface modes and all of the related parameters for each operation mode. And user can enable or disable the WLAN interface.

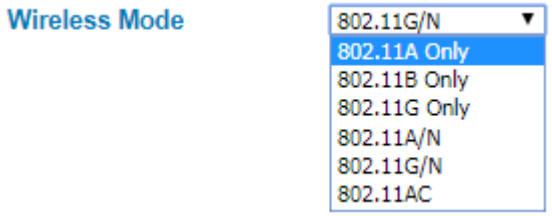
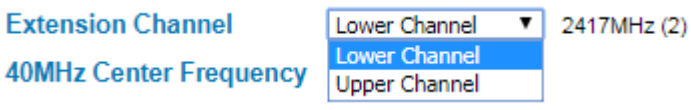
AP

The Access Point mode, it establishes a wireless connection, receive from wireless clients and provide connection for wireless client devices, the client can search and connect to several the access points. In AP mode interface, user can configure the SSID name, Enable or Disable Broadcast SSID, select the Wireless mode, set the HT Protect to Enabled or Disabled, set the Channel, Extension Channel, configures the Channel Mode, Maximum Output Power, Data Rate and Extension Channel Protection.



The description of the columns is as below:

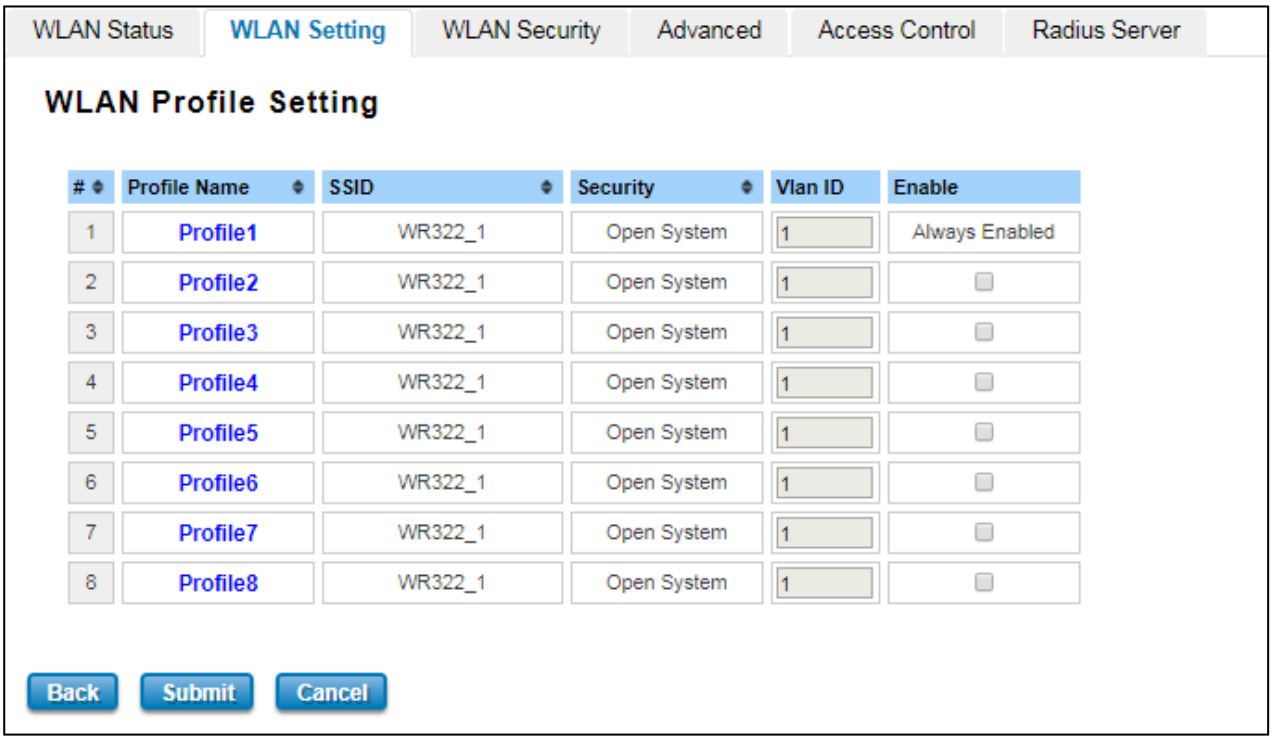
TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless functions.
Operation Mode	**Default: AP** Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	**Default: WR** Input the primary name of the access point.
Broadcast SSID	**Default: Enabled.**

	By enabling the broadcast SSID, it makes the AP can be accessed and searched by the clients, and for the security concern by disabling this broadcast SSID, the network will be hidden in order to prevent any malicious attack.
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has adifferent configuration. For each wireless mode, it has the specific frequency and it has different basic setting.. 
HT Protect	**Default: Disabled** Select Enabled to activate the High Throughput protect to ensure HT transmission with MAC mechanism.
Channel	**Default: 2437MHz (6)** Select the proper channel, each country has different band user may select the channel based on the situation. Or select auto to automatically set the channel. 
Extension Channel	**Default: Lower Channel 2417MHz (2)**  This option would be appeared when user select the Channel Mode to 20/40MHz or 40MHz. To put range for the frequency, it provides the Lower Channel (2417MHz (2)) with the 40MHz center frequency is 2427MHz (4) and Upper Channel (2457MHz (10)) with the 40MHz center frequency is 2447MHz (8).
Channel Mode	**Default: 20MHz**

	Channel Mode 20 MHz 20 MHz 20/40 MHz 40 MHz There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user select 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequency, and for the 40MHz, it provides bigger data rate and received the 40MHz frequency. But basically, if the transmission happened between the AP and the client, both AP and client can have the negotiation phase about the frequency.
Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna. Maximum Output Power Half Lowest Eighth Quarter Half Full
Data Rate	**Default: Auto** Select the specific data rate in order to control the transmission rate. **Auto** is preferred rate, the access point will automatically select the highest available rate to transmit. User may select the low rate when there is no great demand for transmission speed, for long distance transmission.
Extension Channel Protection	Extension Channel Protection None None CTS to Self RTS-CTS Select from the dropdown list option between **CTS-Self or RTS-CTS** to avoid conflict with other wireless network and to improve the ability of the device to catch all the wireless transmissions. By activating this function it may decrease wireless network performance.

Click **Submit** to apply the configuration

At the SSID section, there is a **Multi SSID** button appeared. This AP mode supports the multiple SSID or multiple access point connections. So user may separate the connection into several access points and it is supported with 8 profiles for multiple SSID. Click the button then another form will appear, see the figure below.

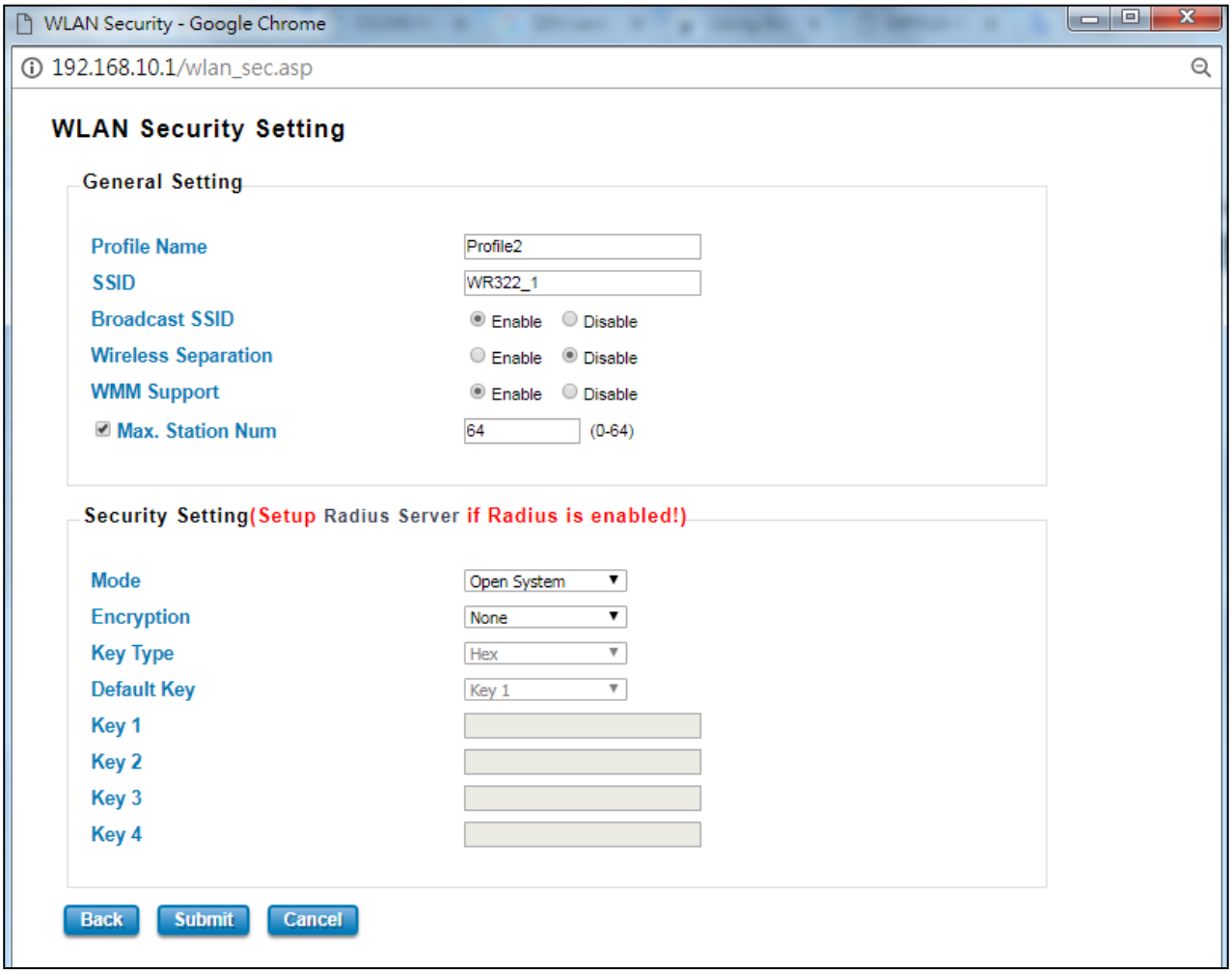


The description of the column is as below:

TERMS	DESCRIPTION
Profile Name	Display the available WLAN Profile name
SSID	Display the SSID Name.
Security	Display the current security mode for the Wirelless network
VLAN ID	Display the VLAN ID
Enable	Check the box to enable the WLAN Profile. When user enabled the Profile, user may configure the WLAN Setting by click the Profile name.

Click **Submit** to apply the configuration

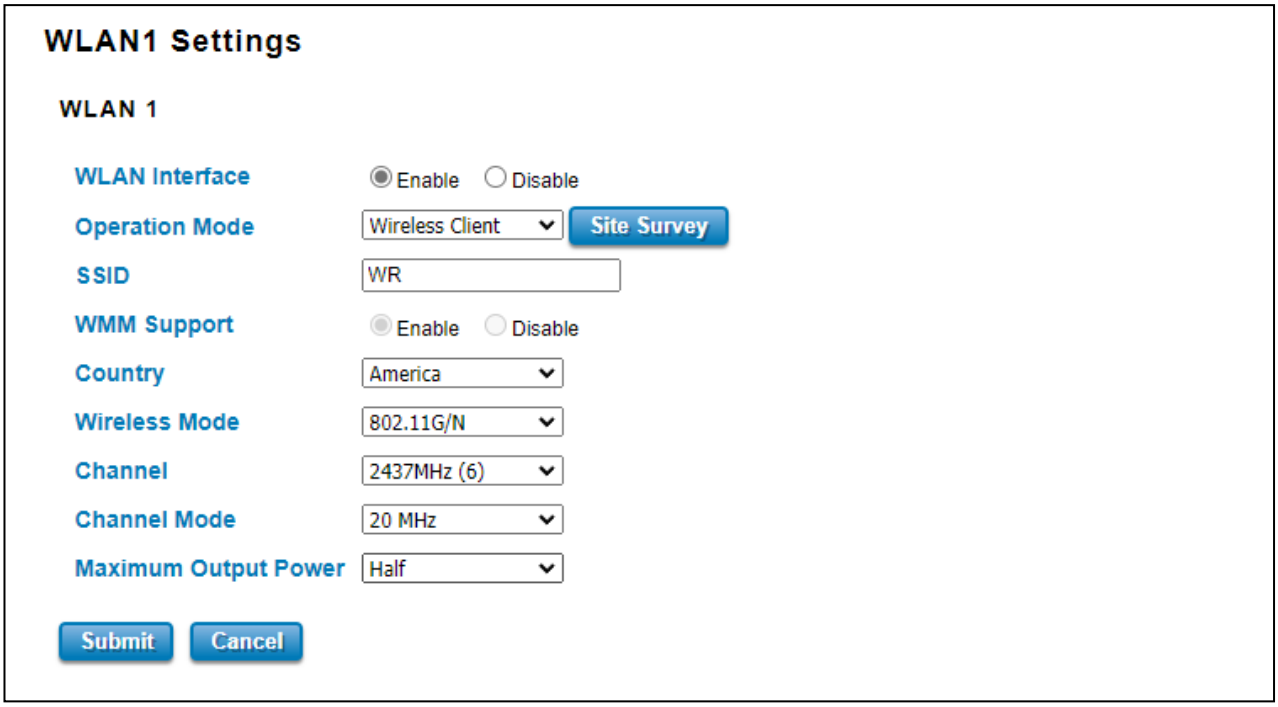
The Multi SSID section shows the configuration page where the Profile1 always enabled. In this section, user may configure each Profile by check the box to enable the Profile and then click the profile name to open the configuration page for specific Profile. The figure below is the pop-up WLAN Security configuration page for each Profile. In this configuration page, user can configure the AP profile, divide the AP connection and set the security setting by put the encryption mode and set the key or password to access the AP. Refers to the WLAN Security Section for more description (3.7.3).



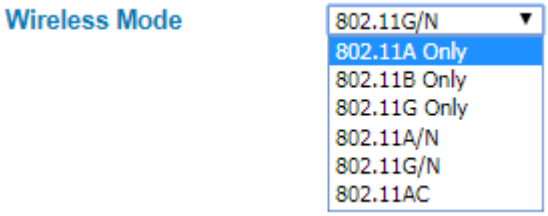
Click **Submit** to apply the configuration

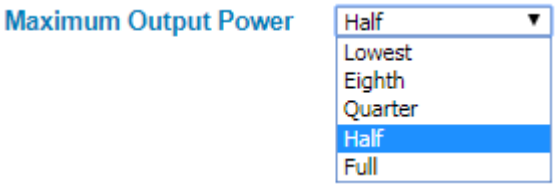
Wireless Client

Wireless Client mode, in this mode the device is able to connect to the Access Point and join the wireless network around the device that opens the connection. User can find the best connection for the AP by click the **Site Survey** and the AP list will appear.



The description of the columns is as below:

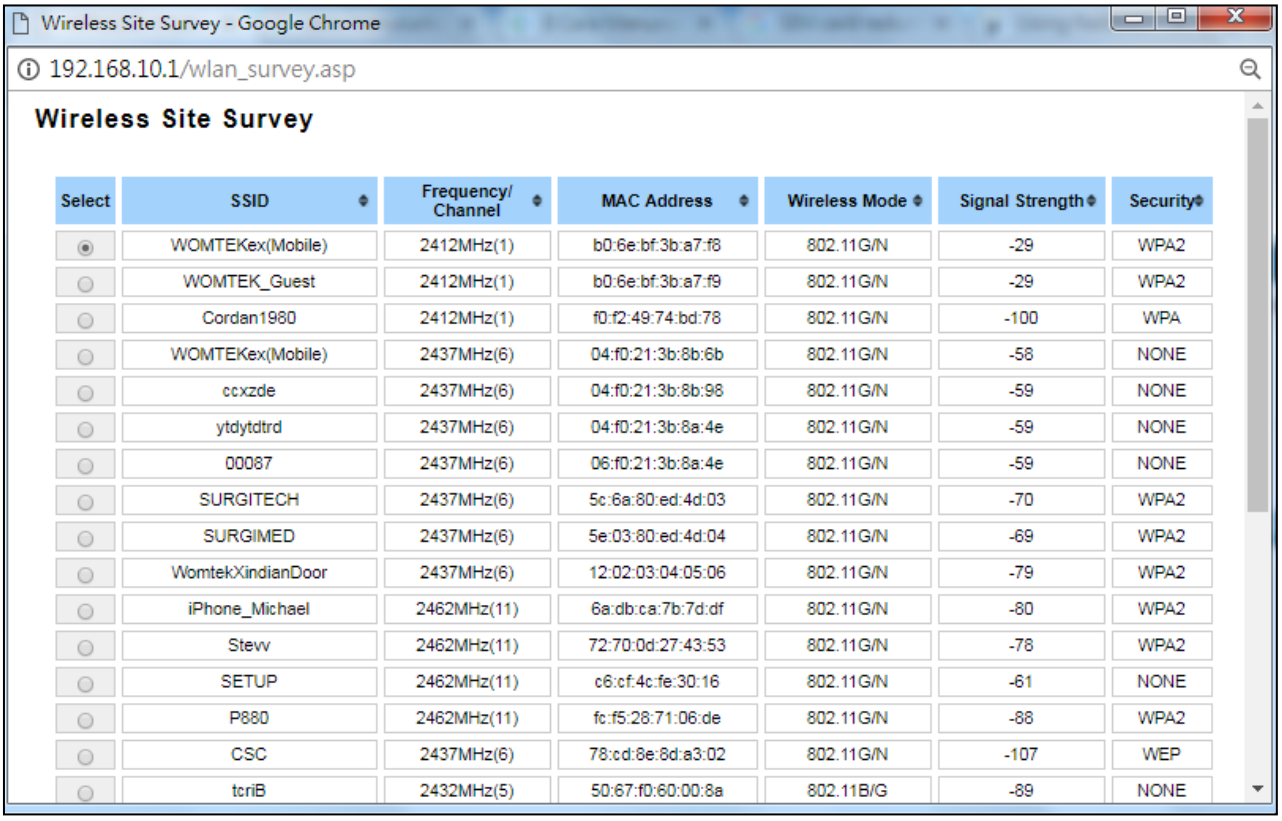
TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless functions.
Operation Mode	Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	**Default: WR** Input the primary name of the access point.
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has a different configuration. For each wireless mode, it has a specific frequency and it has different basic setting.. 
Channel	**Default: 2437MHz (6)** Select the proper channel, each country has different band user may select the channel based on the situation. Or select auto to automatically set the

	channel. 
Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna. 
Data Rate	**Default: Auto** Select the specific data rate in order to control the transmission rate. **Auto** is preferred rate; the access point will automatically select the highest available rate to transmit. User may select lower rate when there is no great demand for transmission speed, for long distance transmission.
Extension Channel Protection	 Select from the drop down list option between **CTS-Self or RTS-CTS** to avoid conflict with other wireless network and to improve the ability of the device to catch all the wireless transmissions. By activating this function, it may decrease wireless network performance.

Click **Submit** to apply the configuration

Wireless Site Survey (Wireless Client & WDS-Client)

Click the Site Survey button to open the Wireless Site Survey page. On this page user may choose the Access Point that appeared on the list. After selects the specific AP, then click **Selected** to apply the choice. Click **Scan** to refresh the list.



Select	SSID	Frequency/ Channel	MAC Address	Wireless Mode	Signal Strength	Security
◉	WOMTEKex(Mobile)	2412MHz(1)	b0:6e:bf:3b:a7:f8	802.11G/N	-29	WPA2
○	WOMTEK_Guest	2412MHz(1)	b0:6e:bf:3b:a7:f9	802.11G/N	-29	WPA2
○	Cordan1980	2412MHz(1)	f0:f2:49:74:bd:78	802.11G/N	-100	WPA
○	WOMTEKex(Mobile)	2437MHz(6)	04:f0:21:3b:8b:6b	802.11G/N	-58	NONE
○	ccxzde	2437MHz(6)	04:f0:21:3b:8b:98	802.11G/N	-59	NONE
○	ytdytdtrd	2437MHz(6)	04:f0:21:3b:8a:4e	802.11G/N	-59	NONE
○	00087	2437MHz(6)	06:f0:21:3b:8a:4e	802.11G/N	-59	NONE
○	SURGITECH	2437MHz(6)	5c:6a:80:ed:4d:03	802.11G/N	-70	WPA2
○	SURGIMED	2437MHz(6)	5e:03:80:ed:4d:04	802.11G/N	-69	WPA2
○	WomtekXindianDoor	2437MHz(6)	12:02:03:04:05:06	802.11G/N	-79	WPA2
○	iPhone_Michael	2462MHz(11)	6a:db:ca:7b:7d:df	802.11G/N	-80	WPA2
○	Stevv	2462MHz(11)	72:70:0d:27:43:53	802.11G/N	-78	WPA2
○	SETUP	2462MHz(11)	c6:cf:4c:fe:30:16	802.11G/N	-61	NONE
○	P880	2462MHz(11)	fc:f5:28:71:06:de	802.11G/N	-88	WPA2
○	CSC	2437MHz(6)	78:cd:8e:8d:a3:02	802.11G/N	-107	WEP
○	tcriB	2432MHz(5)	50:67:f0:60:00:8a	802.11B/G	-89	NONE

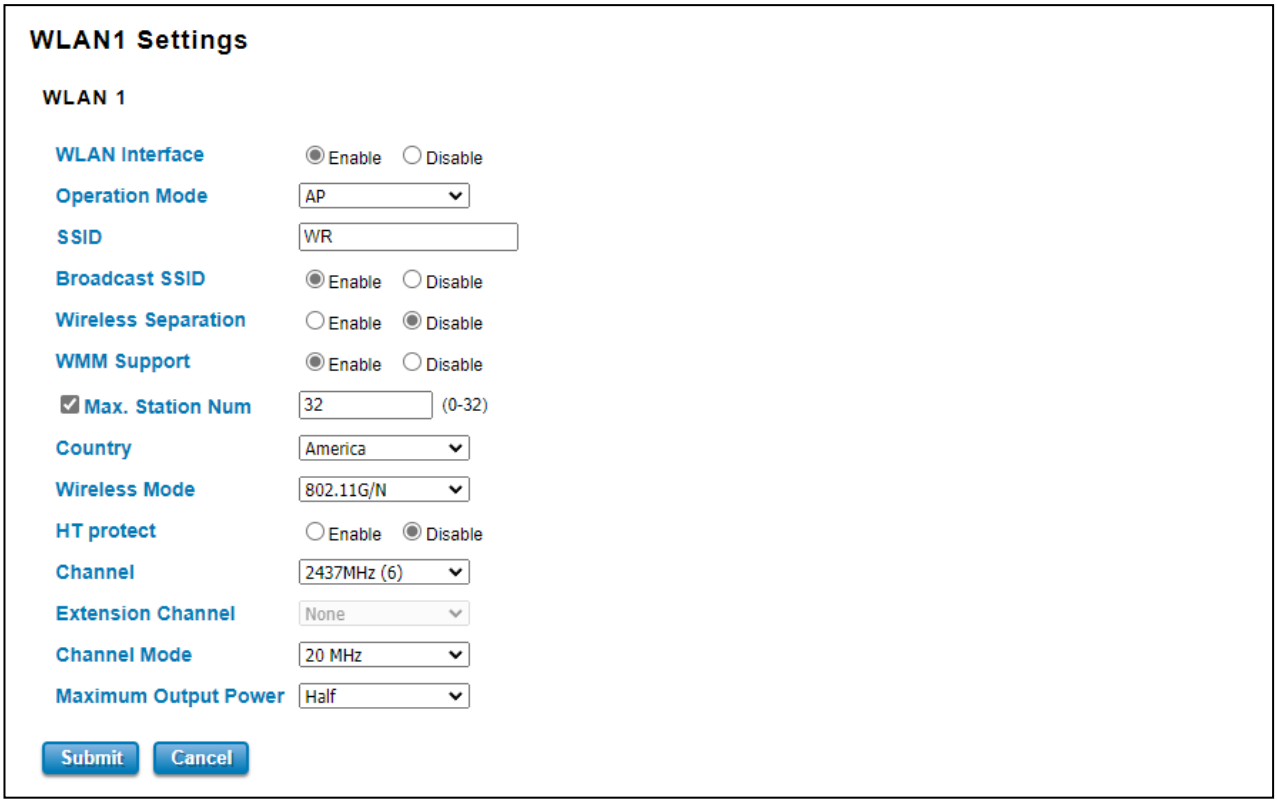
The description of the columns is as below:

TERMS	DESCRIPTION
Select	Select the SSID.
SSID	Display the detected SSID's name
Frequency/Channel	Display the current frequency of the AP.
MAC Address	Display the listed AP MAC Address.
Wireless Mode	Display the Wireless mode.
Signal Strength	Display the signal strength
Security	The security mode of the Access Point.

Click **Selected** to connect to the specific SSID.

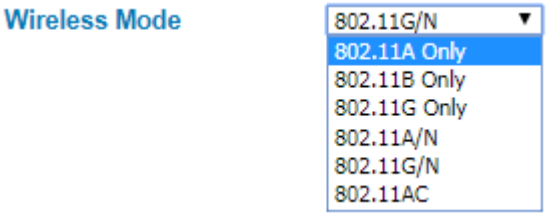
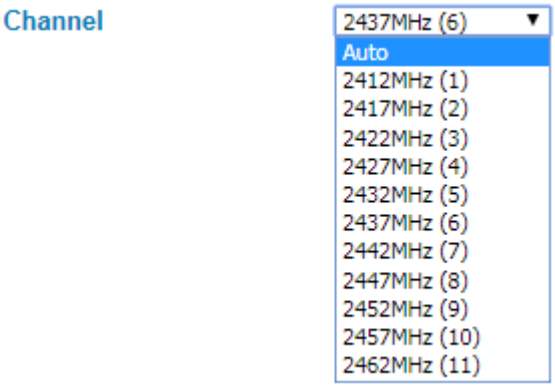
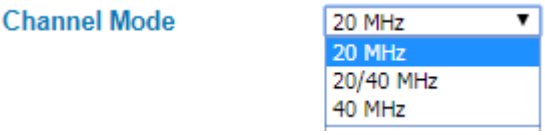
WDS-AP

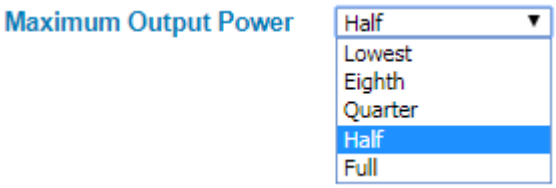
The WDS-AP mode usually implements the Point to Point (P2P) connection, so the access point should be WDS-AP and the wireless client should be WDS-Client. So in this case, the AP just can share the connection to the specific wireless client that has its MAC Address. But WDS-AP can be a repeater to provide network access to general clients.



The description of the columns is as below:

TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless functions.
Operation Mode	**Default: AP** Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	**Default: WR322_1** Input the primary name of the access point.
Broadcast SSID	**Default: Enabled.** By enabling the broadcast SSID, it makes the AP can be accessed and searched by the clients, and for the security concern by disabling this broadcast SSID, the network will be hidden in order to prevent any malicious attack.
Wireless Separation	**Default: Disabled.** By enabling the function, connected clients will be separated and can reach each other (ex: can't ping each other)
WMM Support	**Default: Enabled.**

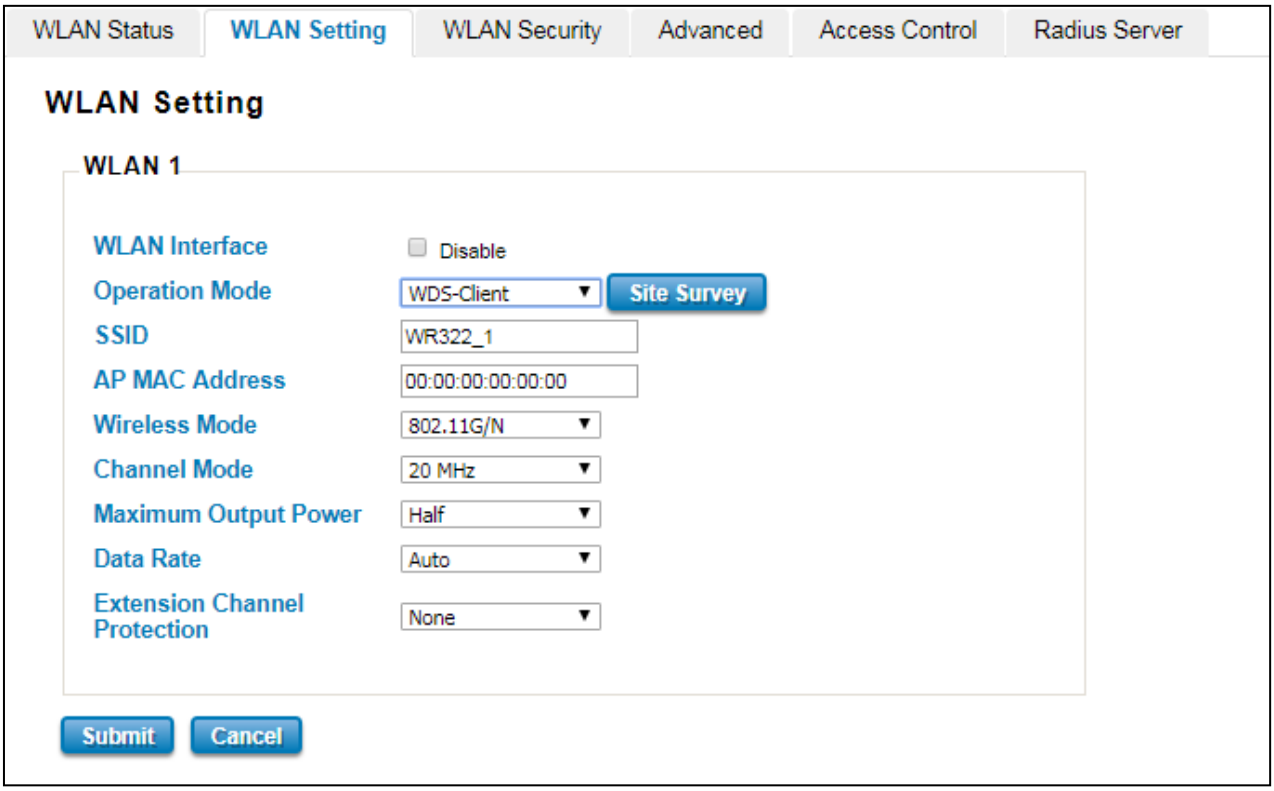
	To enable or disable WIFI multi-media QoS.
Max. Station Num	**Default: 32** Specify the maximum number of connected clients
Country	Select your country code for band regulation.
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has a different configuration. For each wireless mode, it has the specific frequency and it has different basic setting.. 
HT Protect	**Default: Disabled** Select Enabled to activate the High Throughput protect to ensure HT transmission with MAC mechanism.
Channel	**Default: 2437MHz (6)** Select the proper channel, each country has different band user may select the channel based on the situation. Or select auto to automatically set the channel. 
Channel Mode	**Default: 20MHz**  There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user select 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequency, and for the 40MHz, it provides bigger data rate and received the 40MHz frequency. But basically, if the transmission happened between the AP and the client, both AP and client can have the negotiation phase about the frequency.

Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna. 

Click **Submit** to apply the configuration

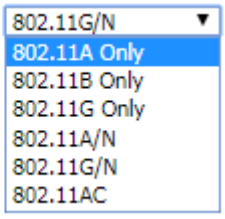
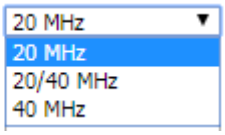
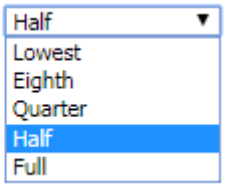
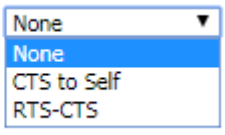
WDS-Client

In WDS-Client mode, user must specify the specific WDS-AP's SSID and MAC address. So WDS-Client just do the transmission to the WDS-AP only. In this mode, please make sure that the configuration should be the same as the WDS-AP as well.



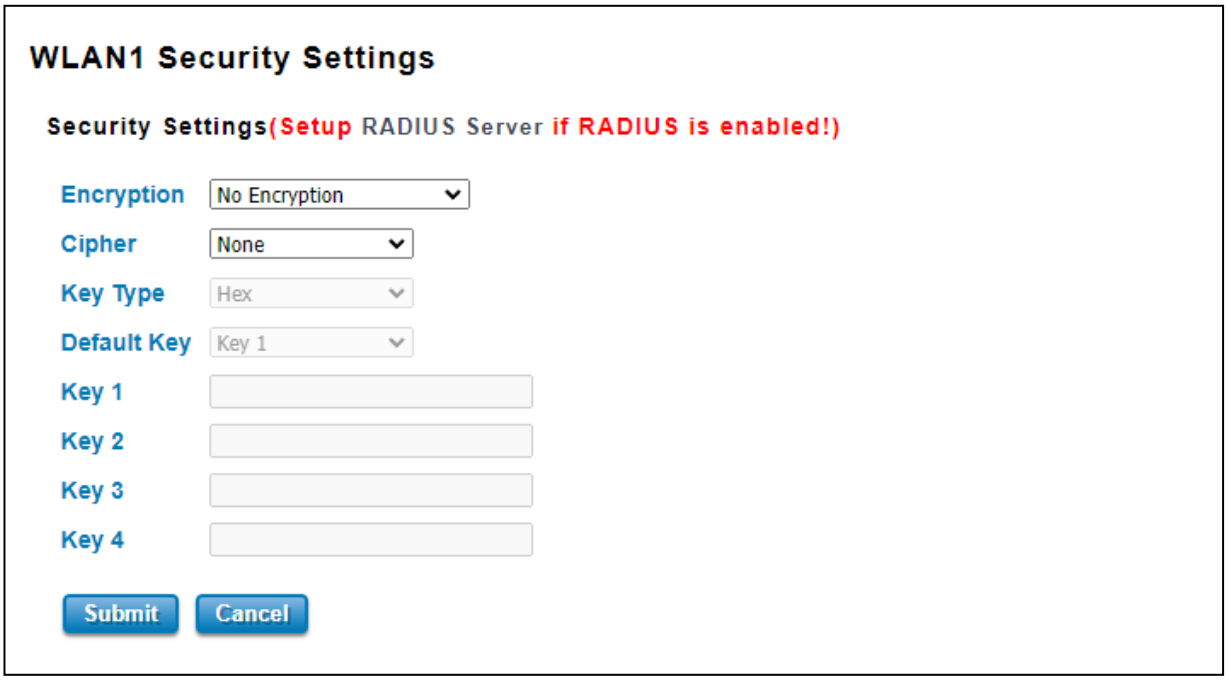
The description of the columns is as below:

TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless functions.
Operation Mode	Select the Operation Mode for the router. (AP, Wireless Client)
SSID	**Default: WR322_1** Input the primary name of the access point.
AP MAC Address	**Default: 00:00:00:00:00:00** Set the specific AP MAC Address of the WDS-AP.
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has a different configuration. For each wireless mode, it has a specific frequency and it has different basic setting.

	Wireless Mode 
Channel Mode	**Default: 20MHz** Channel Mode  There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user select 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequency, and for the 40MHz, it provides bigger data rate and received the 40MHz frequency. But basically, if the transmission happened between the AP and the client, both AP and client can have the negotiation phase about the frequency.
Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna. Maximum Output Power 
Data Rate	**Default: Auto** Select the specific data rate in order to control the transmission rate. **Auto** is preferred rate, the access point will automatically select the highest available rate to transmit. User may select the low rate when there is no great demand for transmission speed, for long distance transmission.
Extension Channel Protection	Extension Channel Protection  Select from the dropdown list option between **CTS-Self or RTS-CTS** to avoid conflict with other wireless network and to improve the ability of the device to catch all the wireless transmissions. By activate this function it may decrease wireless network performance.

3.7.3 WLAN SECURITY

On this configuration page, user can configure the WLAN Security feature.

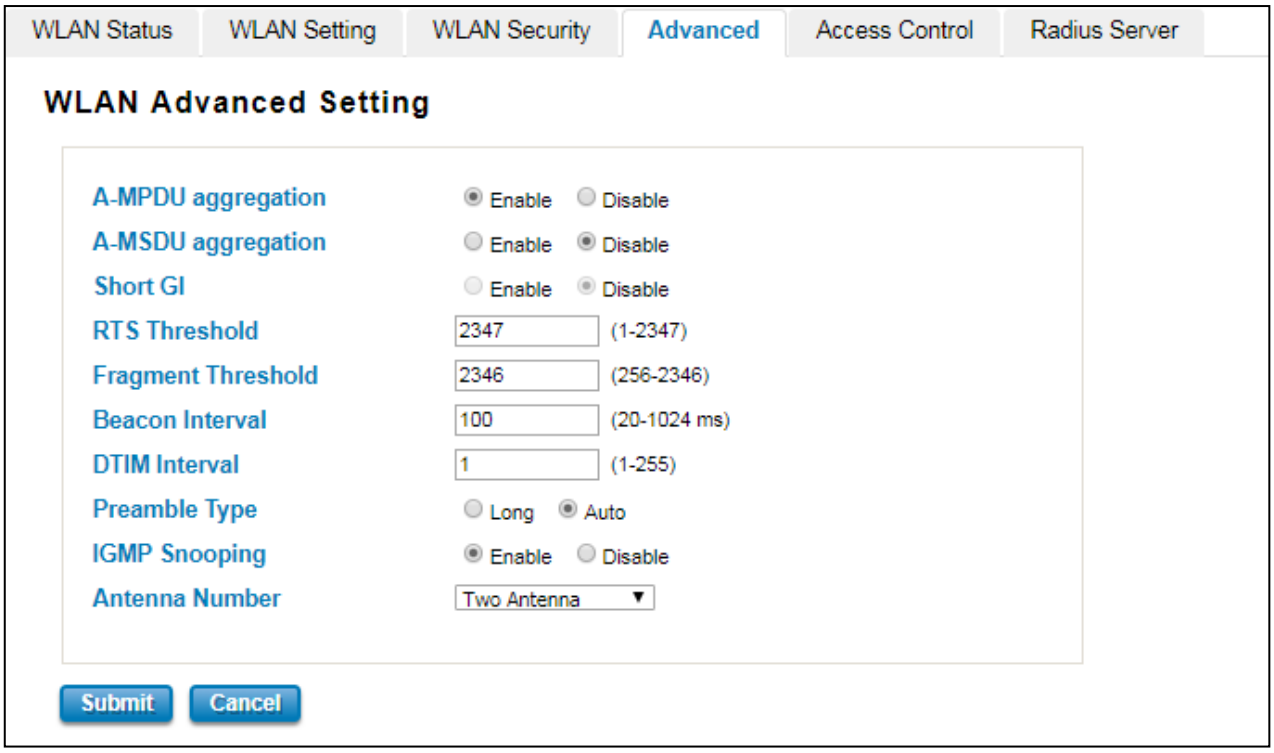


The description of the columns is as below:

TERMS	DESCRIPTION
Encryption	Configure the data encryption mode. ● **None**: Available only when the authentication type is an open system. ● **64 bits WEP**: It is made up of 10 hexadecimal numbers. ● **128 bits WEP**: It is made up of 26 hexadecimal numbers. ● **TKIP**: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK. ● **AES**: Advanced Encryption Standard, it is usually co-used with WPA2-PSK.
Key Type	**Default: Hex** WEP can be configured with a 64-bit or 128-bit Shared Key (hexadecimal or ASCII). As defined, hexadecimal number is represented by 0-9, A-F or a-f; ASCII is represented by 0-9, A-F, a-f or punctuation. Each one consists of two-digit hexadecimal.
Default Key	**Default: Key 1** Set the specific default key.
Key 1~4	Enter the specific encryption key.

3.7.4 ADVANCED

The page allows the advanced user to configure advanced wireless setting with more experience about the WLAN. If user doesn't have any qualified knowledge about WLAN, we suggest not to change the default setting except user know what is the effect when the setting is changed. The wrong configuration may impact the performance of wireless network.



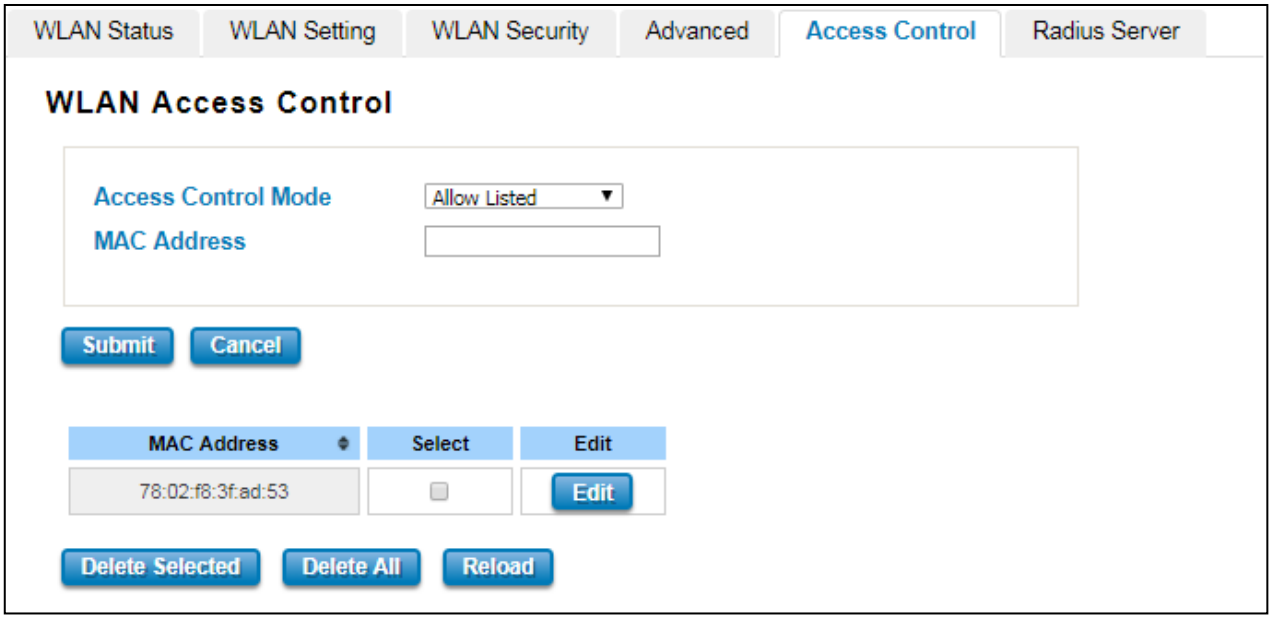
The description of the columns is as below:

TERMS	DESCRIPTION
A-MPDU/A-MSDU aggregation	For the AP mode, by enabling this function the data rate of the AP could be enhanced greatly, Do not enable this function if the wireless clients don't support A-MPDU/A-MSDU aggregation.
Short GI	Enable this function to obtain better data rate. (careful with compatibility issue)
RTS Threshold	**Default: 2347 (1-2347)** Basically, it is about the transmission process between the AP and the end station. When the AP sends Request to Send frames to station and it will do the negotiation process about sending the data frame. When the station receives an RTS frame, the station will respond with send back Clear to Send frame to confirm the right to start transmission.
Fragment Threshold	**Default: 2346 (256-2436)** Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance.

Beacon Interval	**Default: 100ms (20-1024 ms)** Specify the interval to broadcast packets.
DTIM Interval	**Default: 1 (1-255)** Delivery Traffic Indication Message interval is an additional message added after the beacon interval broadcast by access point. It is for enhancing the wireless transmission efficiency. The more intervals we added, the more power that we need. By setting a low value of DTIM, user can effectively keep the devices awake indefinitely so they never go into sleep mode when idling.
Preamble Type	**Default: Long** Preamble Type setting means that it adds some additional data header strings to help check the Wi-Fi data transmission errors. Basically, preamble type divided into two, long and short. Short is for shorter data strings that adds less data to transmit the error redundancy check which means that it is much faster. Long Preamble Type uses longer data strings which allow for better error checking capability. Auto Preamble Type the device can set the Preamble Type Automatically according to the need, which is can be long or can be short.
IGMP Snooping	**Default: Enable** By enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the AP. IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic.
Antenna Number	**Default: Two Antenna** The Antenna Number setting allows user to choose the antenna that used in the wireless connection. Basically, the default setting is set to Two antennas, because the device itself provide two antenna sockets. User can configure One Antenna or Two Antenna. Please refer to the Antenna Placement table to connect the antenna correctly.

3.7.5 ACCESS CONTROL (AP MODE)

This page allows user configure the Wireless Access Control list. User can add the rule to Allow list or Deny list for the security concern to access WLAN.

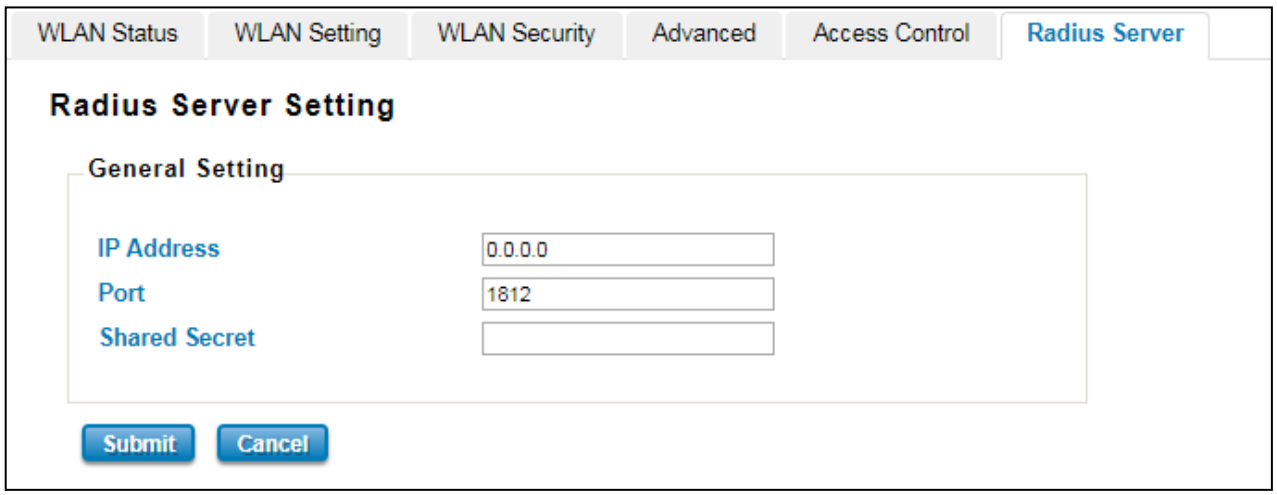


The description of the columns is as below:

TERMS	DESCRIPTION
Access Control Mode	**Default: Disable** Allow List – Allow the specific MAC Address to access the WLAN Deny List – Deny the specific MAC Address to access the WLAN
MAC Address	Display the specific MAC Address that allowed or denied to access the WLAN.
Select	Select the MAC Address list.
Edit	Click to edit the Access Control Mode for the specific MAC Address

3.7.6 RADIUS SERVER (AP MODE)

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. The RADIUS server system allows you to access the router through secure networks against unauthorized access.



How to set up a RADIUS server:

a. Enter the IP address of the RADIUS server in **Server IP Address**
b. Enter the **Shared Secret** of the RADIUS server
c. Enter the **Server port** if necessary, by default RADIUS server listens to port 1812
d. Click **Submit**

The description of the RADIUS Authentication interface is as below:

TERMS	DESCRIPTION
IP Address	Radius Server IP Address
Server Port	Set communication port on an external RADIUS server as the authentication database. The default value is 1812
Shared Key	Shared key is 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 verifies that the RADIUS message has not been modified in transit (message integrity).

3.7.7 CERTIFICATE FILE (CLIENT MODE)

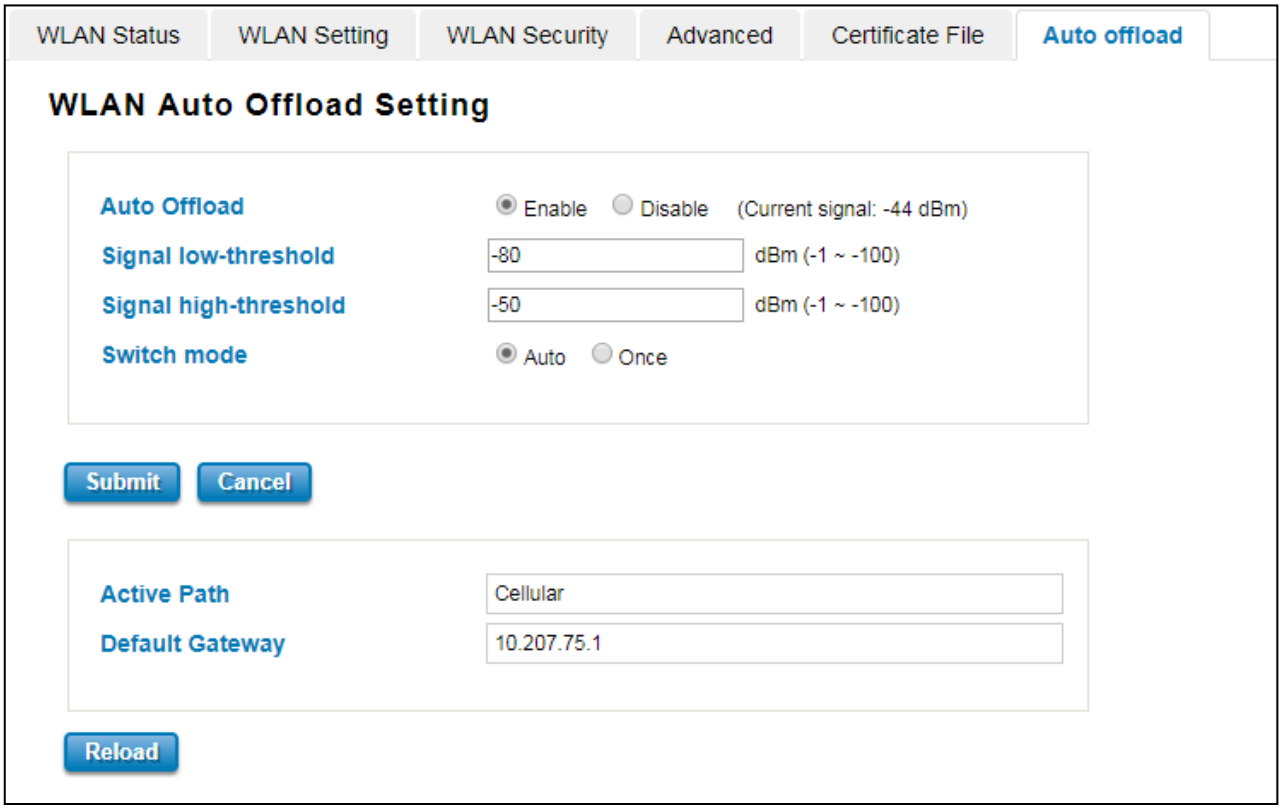
Using digital certificates for authentication method through the RADIUS that provided by the AP. User needs to upload the specific certificate file, so then the client can access the Wi-Fi connection.

The description of the columns is as below:

TERMS	DESCRIPTION
Delete User Key	Delete the selected certificate
Upload User Key	Upload a certificate file from a specified file location

3.7.8 AUTO OFFLOAD (CLIENT MODE)

The WoMaster Router Client mode is supported by the Auto Offload feature that allows the user to enable Wireless Auto Offload. User need to make sure if the device has two available connections, Wi-Fi and Cellular. The cellular cost can be reduced by using this feature because the data traffic can be shared by Cellular and Wi-Fi. If the Wi-Fi signal is poor, then the system forwards the traffic to the Cellular interface automatically.



The description of the interface is as below:

TERMS	DESCRIPTION
Auto Offload	Default: Disable Enable or Disable Auto Offload feature. This feature can be activated when the Wi-Fi is configured as the client mode and the Cellular interface is established. And it will show the current signal strength.
Signal low-threshold	**Default: -80 dBm (Range: -1 ~ -100 dBm)** When signal strength is lower than the upper range, then the connection will be directed to Cellular.
Signal high-threshold	**Default: -50 dBm (Range: -1 ~ -100 dBm)** When signal strength is higher than the upper range, then the connection will be directed to Wi-Fi.
Switch mode	**Default: Auto** When user chooses the **Auto mode**, the connection will automatically switch to the stronger signal between Wi-Fi or Cellular. If user chooses to **Once mode**, it means the connection will switch to the stronger signal once between Wi-Fi or Cellular and will stay at the connection even there were a stronger signal appear.
Active Path	Show the current active path between Wireless or Cellular.
Default Gateway	Show the default gateway IP Address.

3.8 SECURITY

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

The following topics are included in this section:

3.8.1 Access Control

3.8.2 Outbound Firewall

3.8.3 NAT Setting

3.8.4 OpenVPN

3.8.5 IPSec Setting

3.8.6 GRE Setting

3.8.7 L2TP Settings

3.8.8 DMVPN Settings

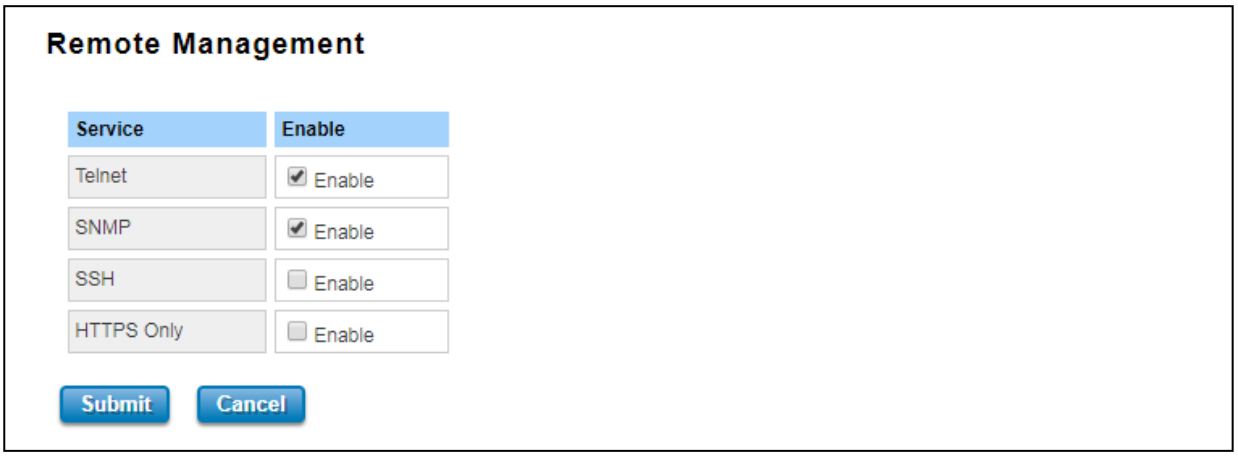
3.8.9 PPTP Settings

3.8.1 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.



The description of the columns is as below:

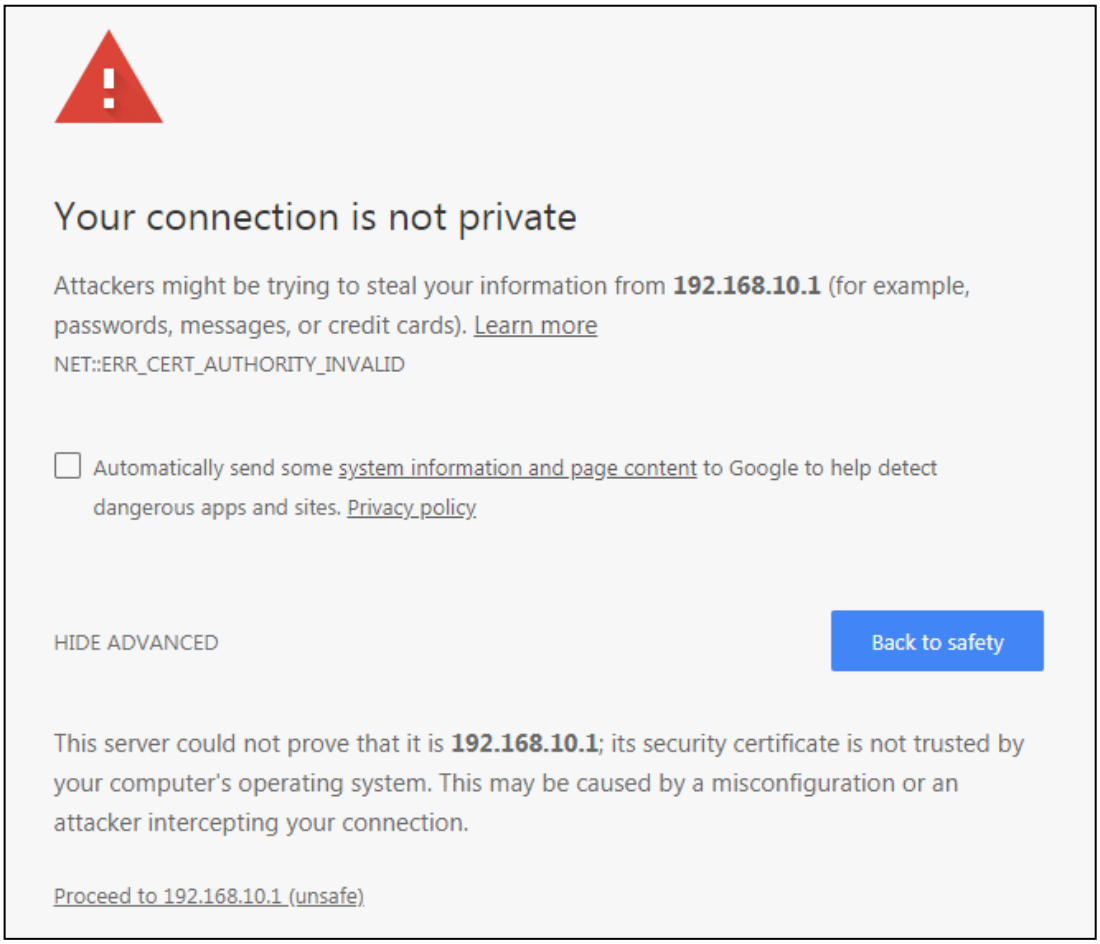
TERMS	DESCRIPTION
Telnet	Allows the user to remotely login and manage the device by Telnet. When user doesn't enable it, the connection through telnet will not allow.
SNMP	Allows the user to remotely login and manage the device by SNMP. When user doesn't enable it, the connection through SNMP will not 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

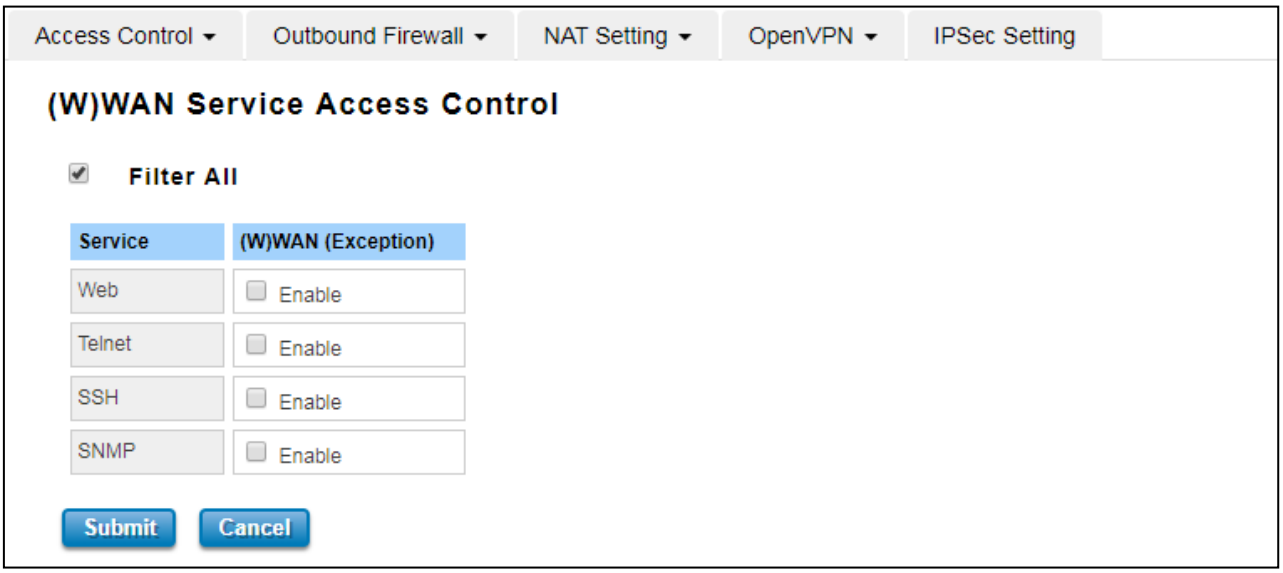
HTTP Secure is the use of the HTTP protocol over an SSL/TLS protocol. It is used primarily to protect against eavesdropping of communication between a web browser and the web site to which it is connected. This is especially important when you wish to have a secure connection over a public network such 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.



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

When user changes the device mode to **router mode (Port 1 – WAN interface)** the WAN Access feature can be activated. 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.



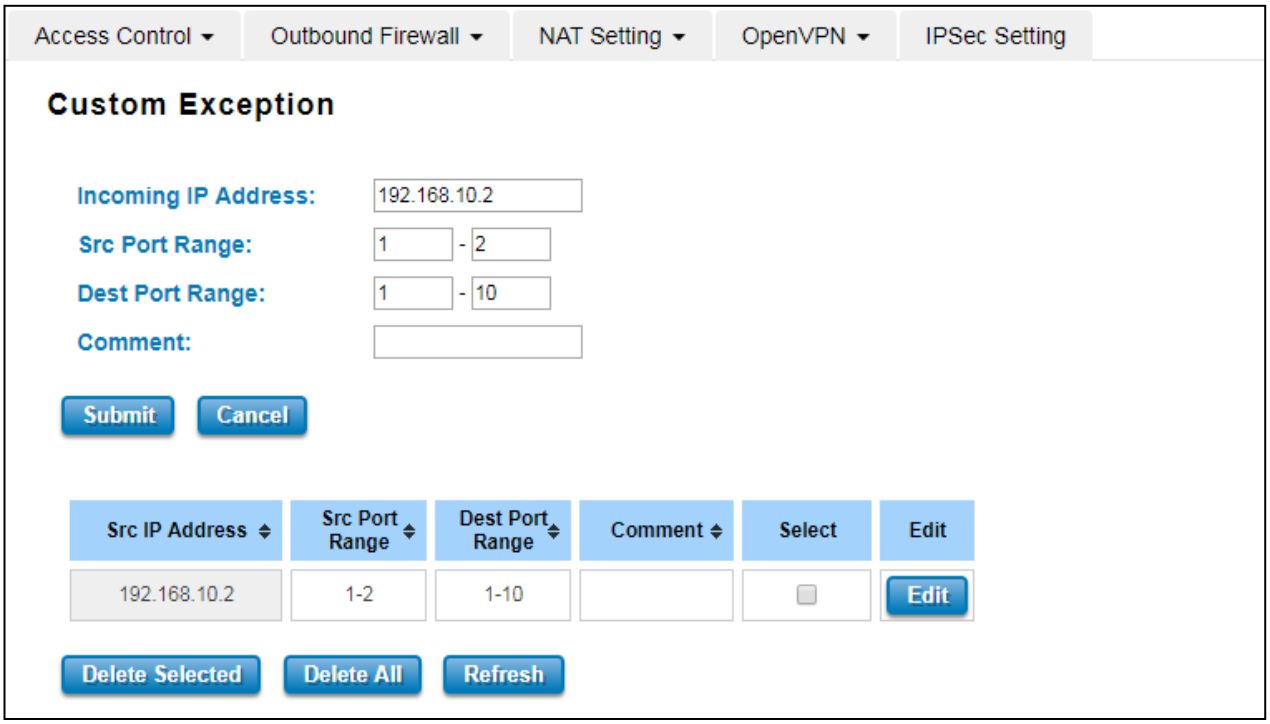
The description of the columns is as below:

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.



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.

MAC Access Control

Through this feature, only the MAC devices in the list can access the router. If the condition does not meet the requirement from the table, then the access would be denied.

Select **Enable** to activate **MAC ACL** function and then input all of the parameters to configure the port forwarding.

The description of the columns is as below:

TERMS	DESCRIPTION
Allow MAC Address	Set up specific MAC Address to access the device.
MAC Address	Display the specific MAC Address that allowed to access the device.
Select	Select the MAC Address list.
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.

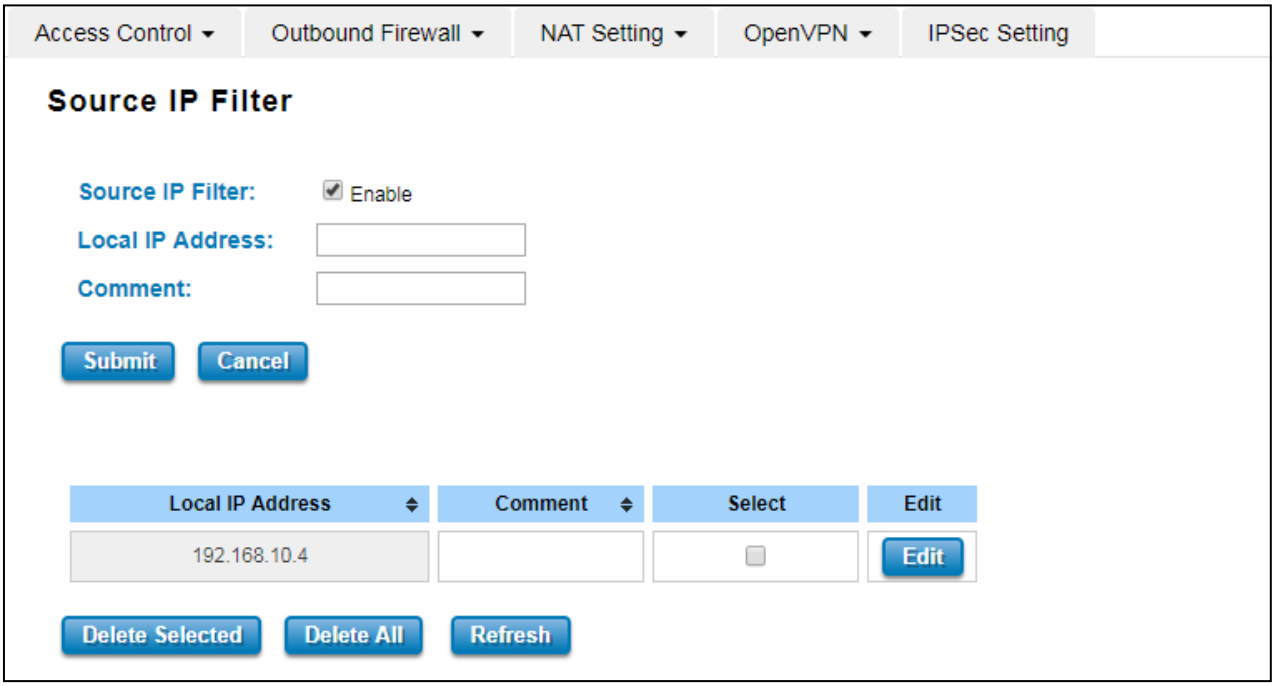
3.8.2 OUTBOUND FIREWALL

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 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.



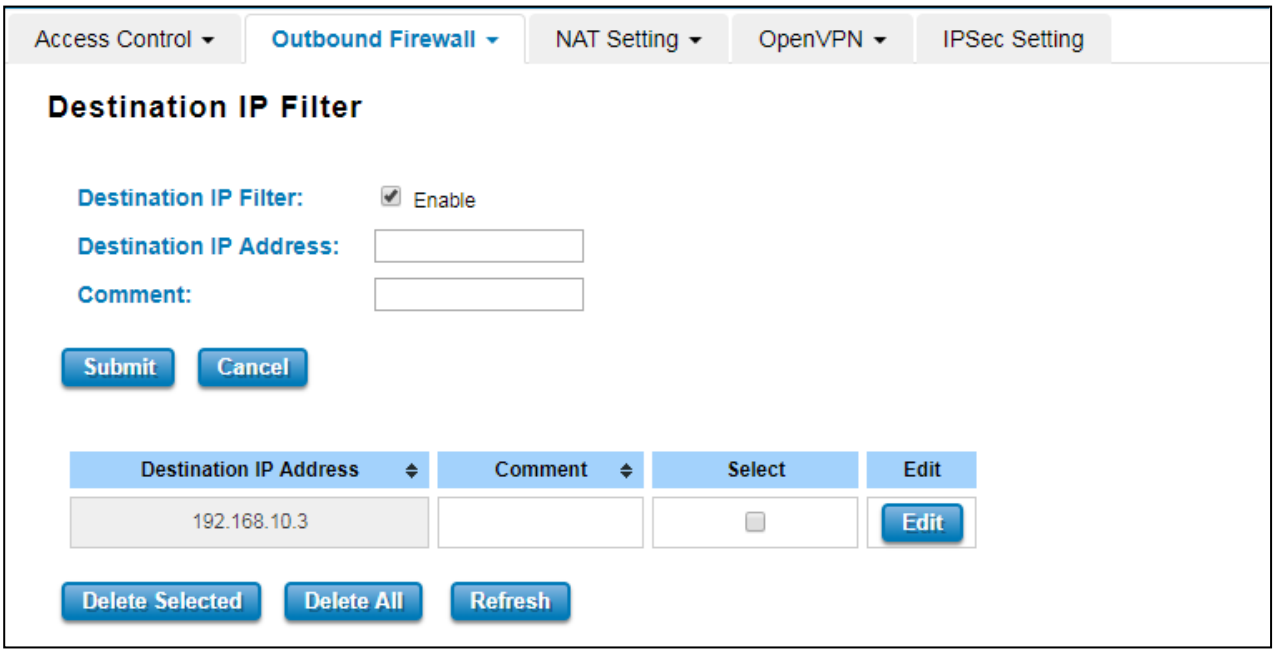
The description of the columns is as below:

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,
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.



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,
Edit	Click edit to modify the parameters

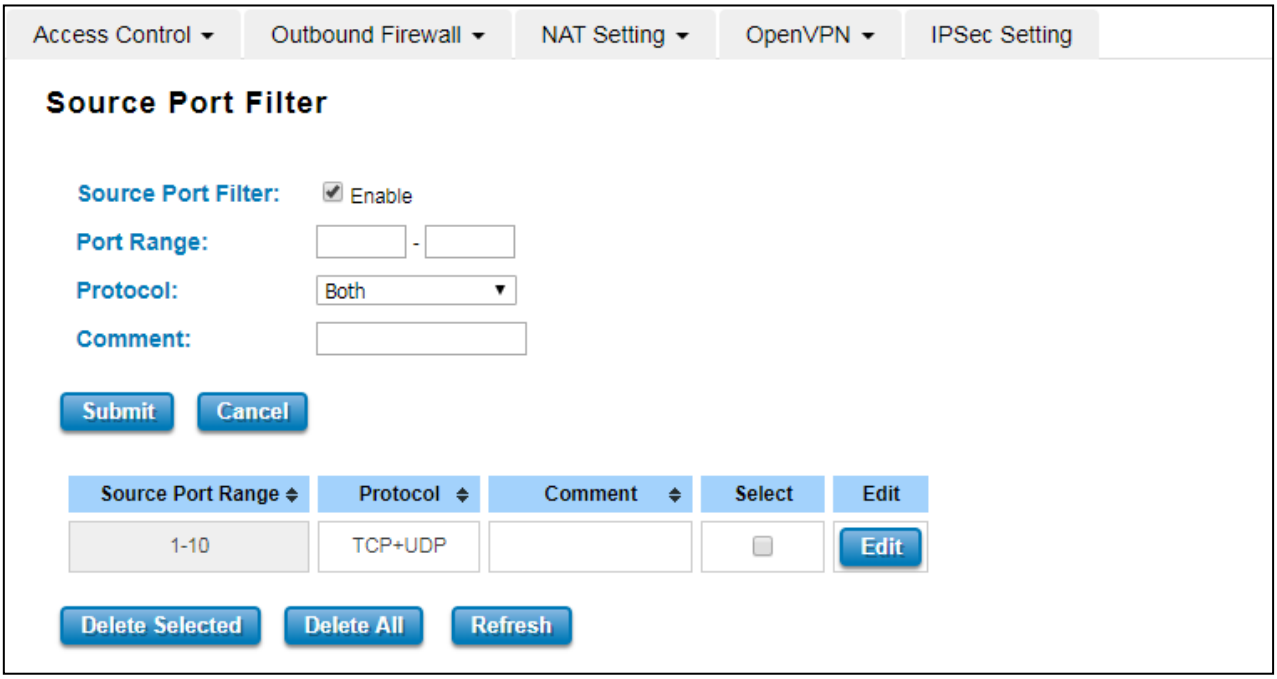
Click **Refresh** to refresh the table

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 Both**. Type the **Comment** to write a note for the entry and then click **Submit** to activate the settings.

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.
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

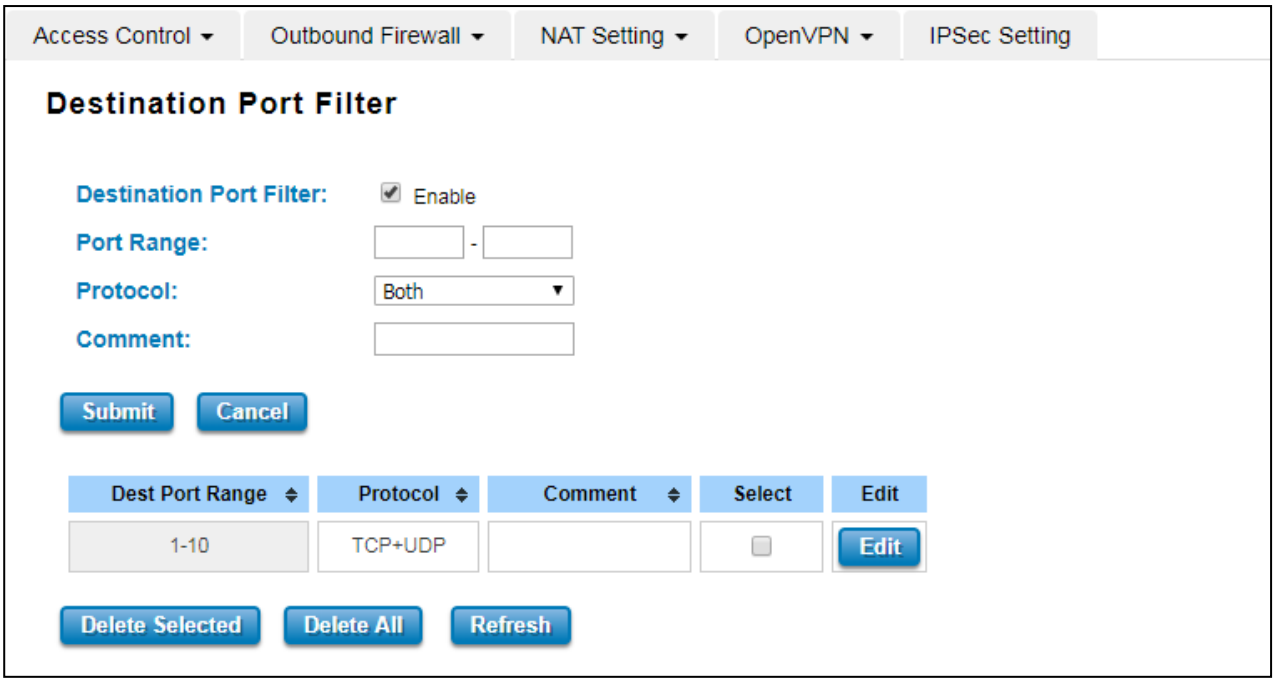
Click **Refresh** to refresh the table

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 Both**. 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.



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.
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

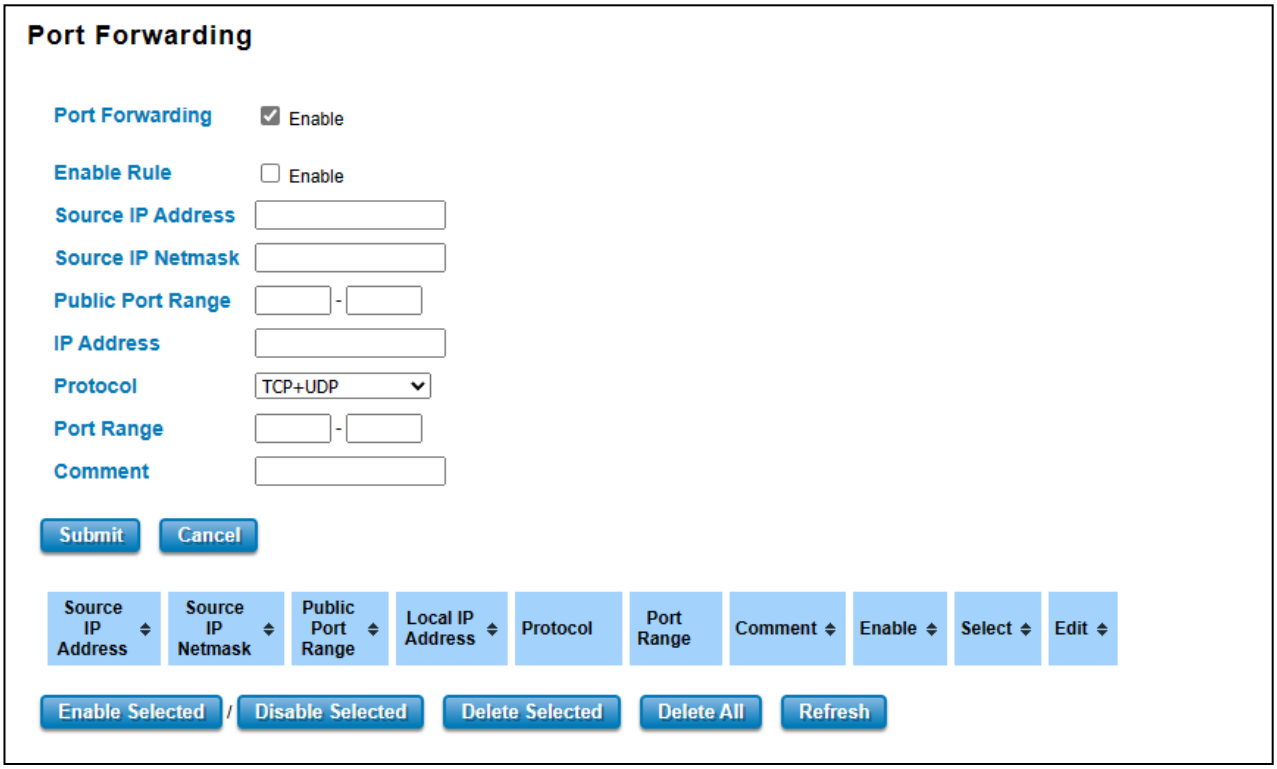
Click **Refresh** to refresh the table

3.8.3 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



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.

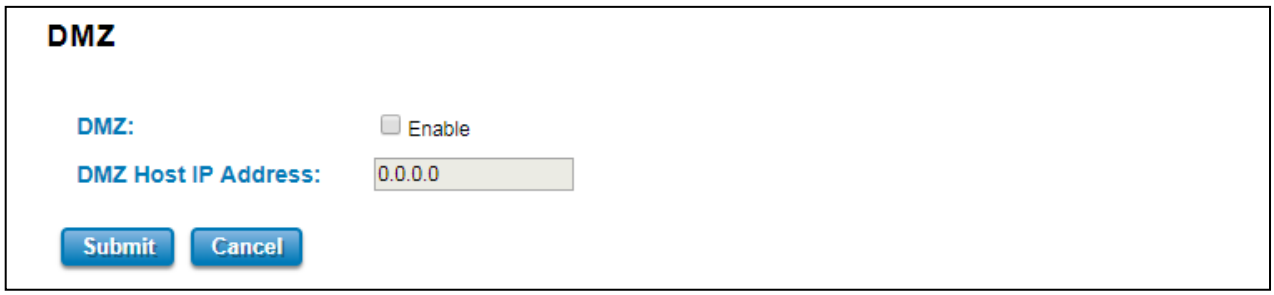
The description of the columns is as below:

TERMS	DESCRIPTION
Port Forwarding	Select Enable to activate Port Forwarding function.
Enable Rule	Select Enable to activate Port Forwarding rule
Source IP Address	Configure the source IP address of the WAN . The traffic within the public port range will be redirected from this IP address for forwarding.
Source IP Netmask	Configure the Source IP Netmask of the WAN
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.



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.

NAT Settings

This page allows user to configure the Port Mapping policy from NAT Setting.

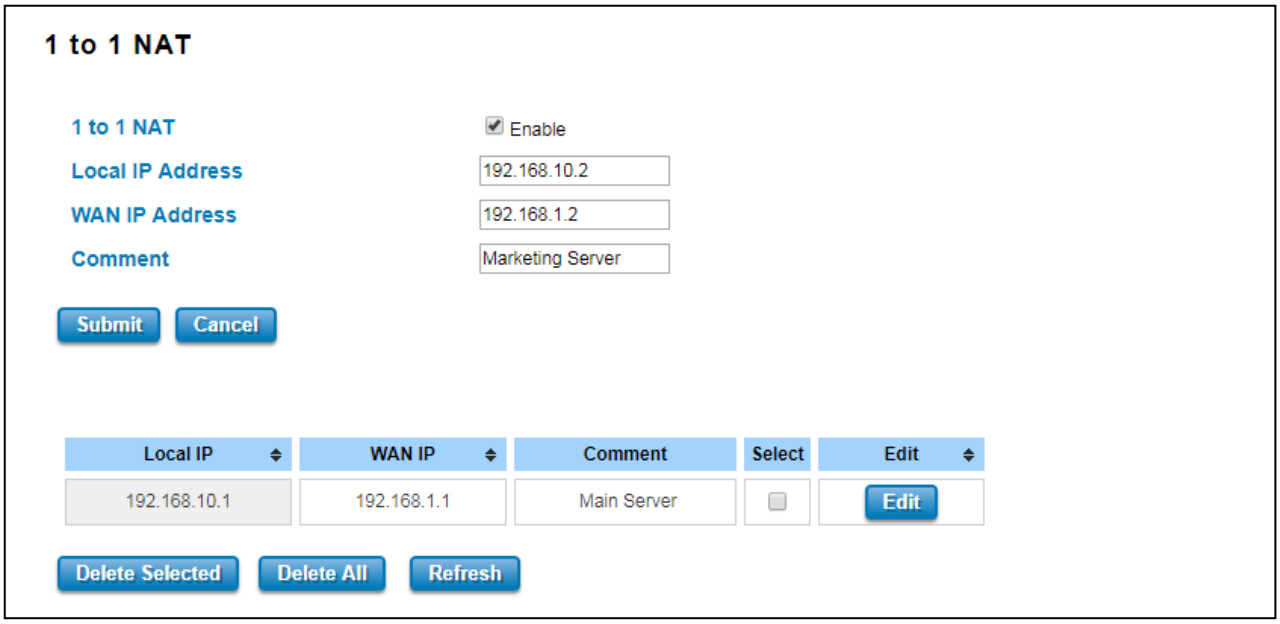
The description of the columns is as below:

TERMS	DESCRIPTION
NAPT Enable	Select the NAPT Enable
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

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
Comment	Enter a comment

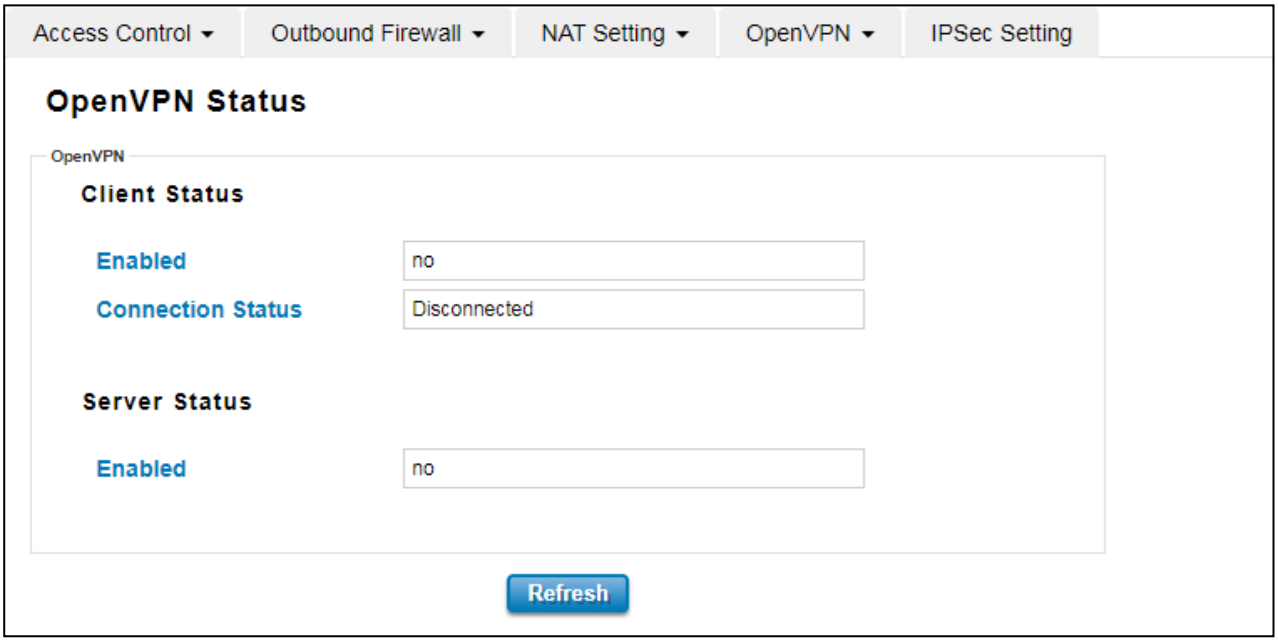
Click **Submit** to apply the configuration.

3.8.4 OPEN VPN

WoMaster router supports OpenVPN. 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.

OpenVPN Status

This section shows the VPN Client and Server current status.



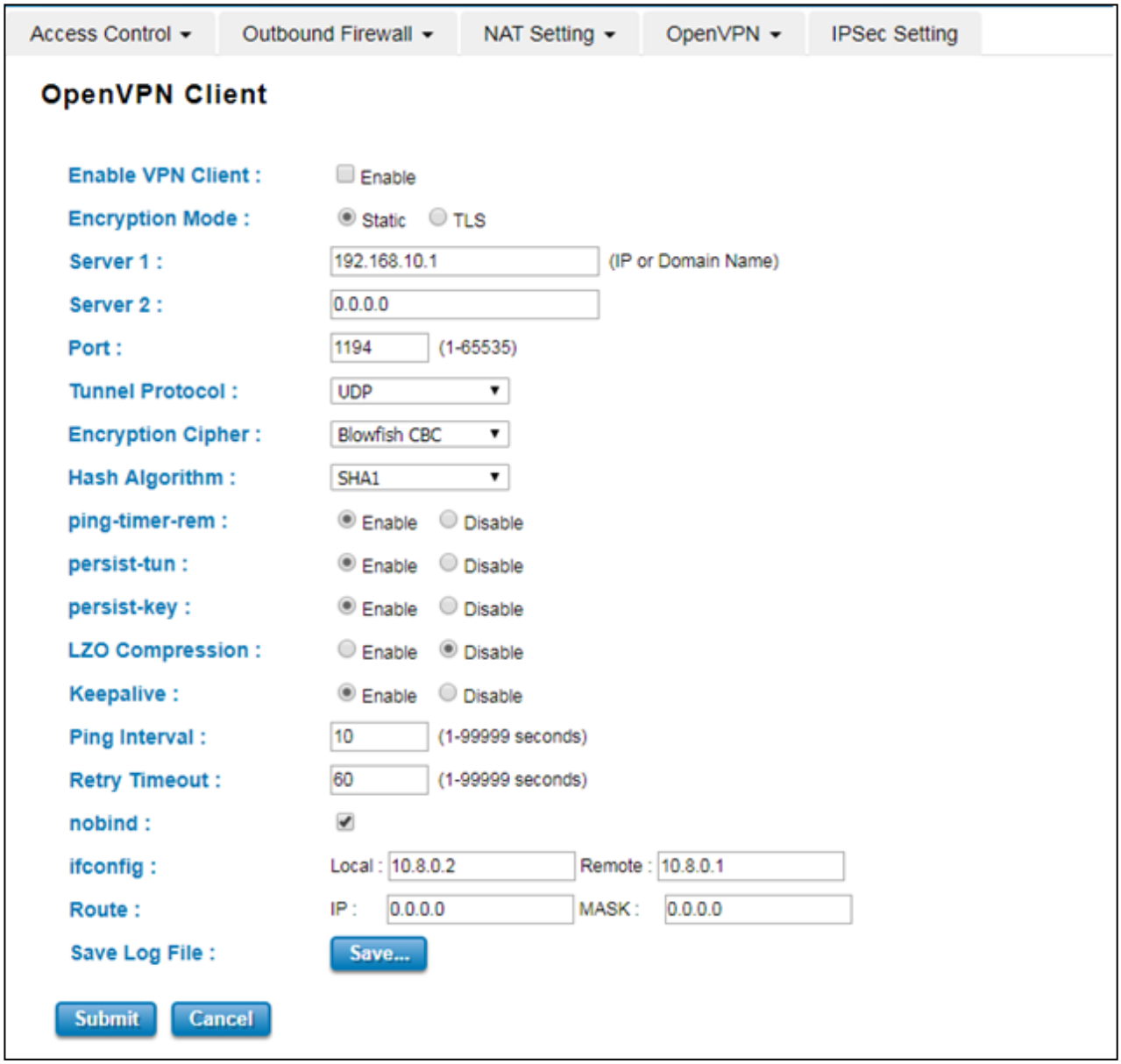
The description of the columns is as below:

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.

OpenVPN 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.



The description of the columns is as below:

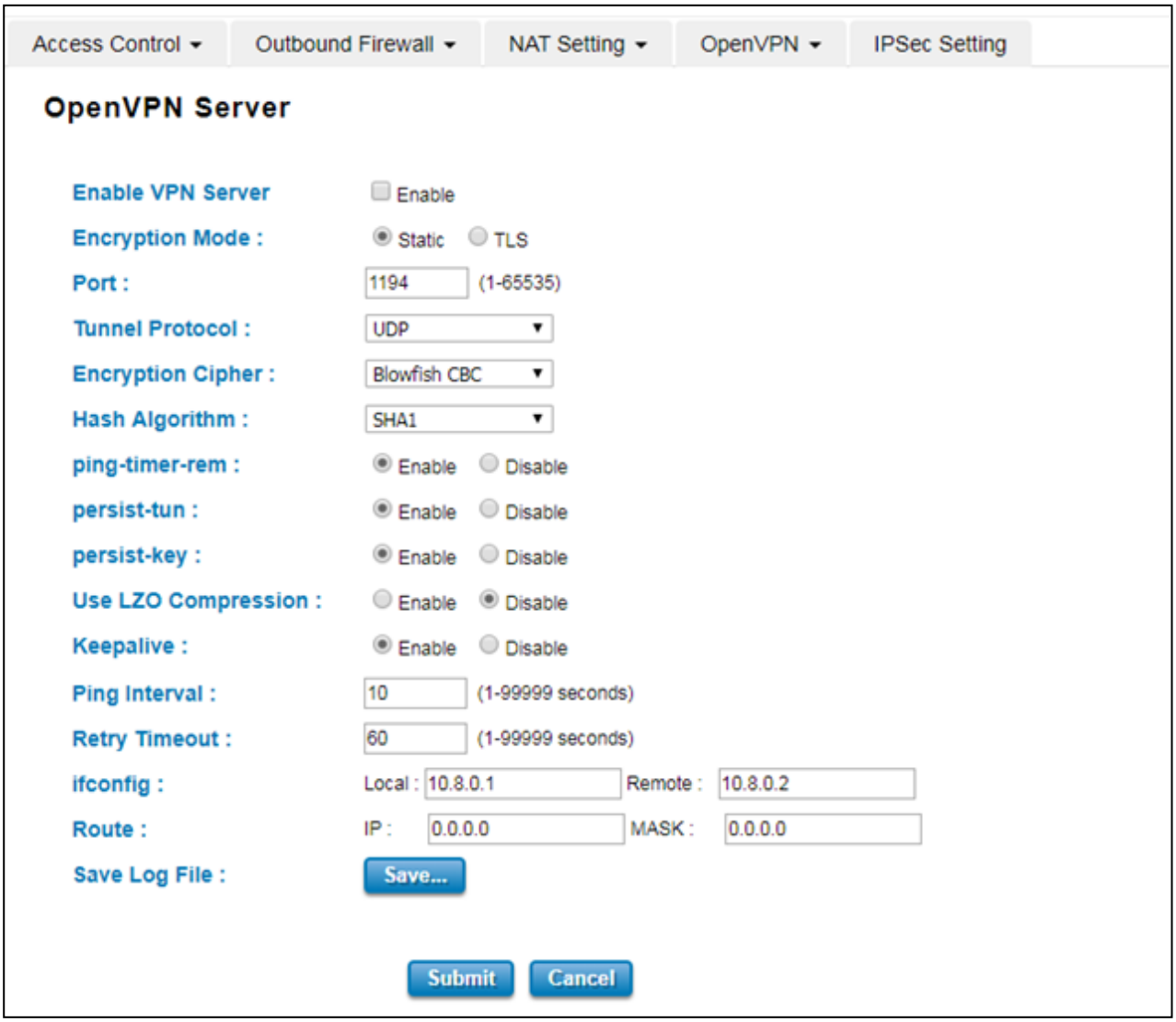
TERMS	DESCRIPTION
Enable VPN Client	Select Enable to activate the VPN Client function
Encryption Mode	Choose the Encryption Mode Static Key: Use a pre-shared static key. TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server 1	Type the IP Address of the VPN Server
Server 2	Type the 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.

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.



The description of the columns is as below:

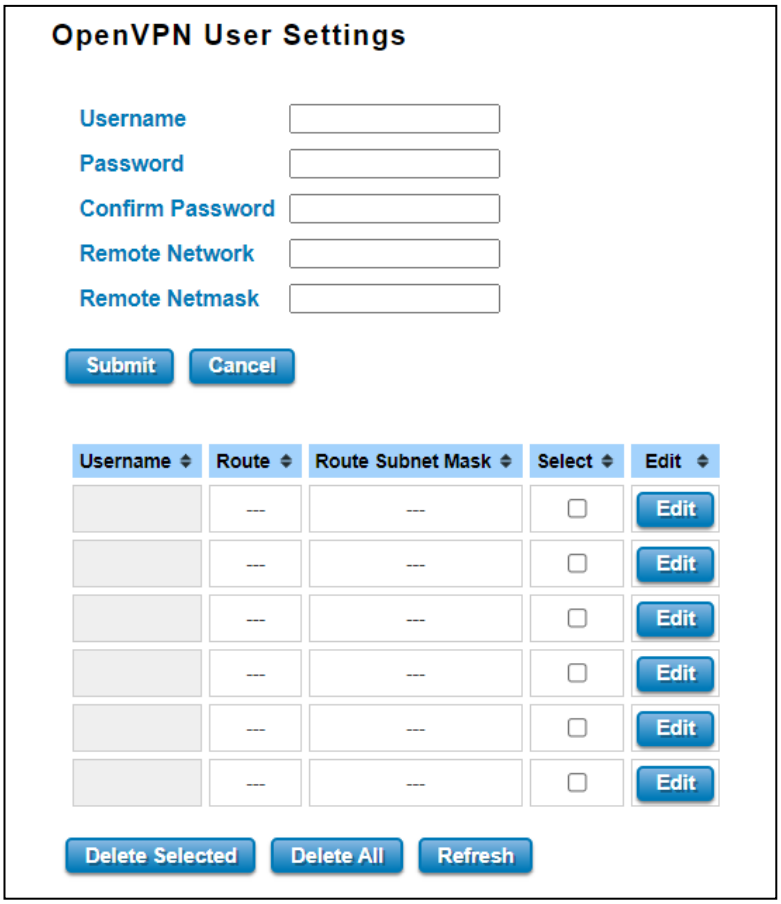
TERMS	DESCRIPTION
Enable VPN Server	Select Enable to activate the VPN Server function
Encryption Mode	Choose the Encryption Mode Static Key: Use a pre-shared static key. TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server 1	Type the IP Address of the VPN Server
Server 2	Type the 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.

OpenVPN User Settings

This page is used to set the user parameters for the OpenVPN client to connect to the OpenVPN server， The Router as a OpenVPN server supports up to 6 client connection.



The description of the columns is as below:

TERMS	DESCRIPTION
User Name	Key in user name here.
Password	Key in password here.
Confirm Password	Re-type the new password again to confirm it.
Remote Network	Key in the subnet of this user.
Remote Netmask	Key in the remote network subnet mask of the user.
Select	Select the user setting list.
Edit	Click to edit the user setting for the specific user

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.

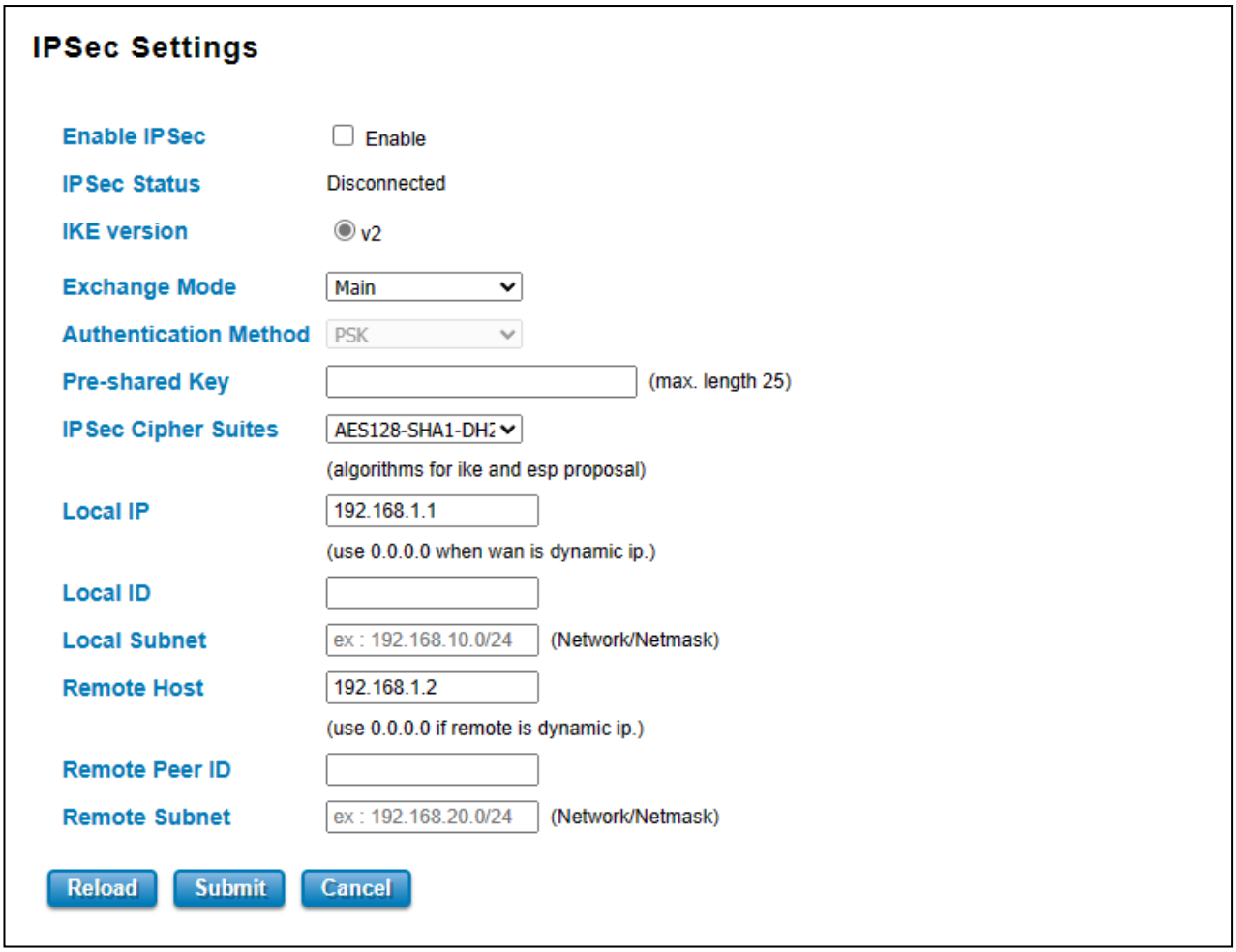
The description of the columns is as below:

TERMS	DESCRIPTION
Delete VPN Key	Delete the selected certificate
Upload VPN Key	Upload a certificate file from a specified file location

Click the "**Generate**"button to generate the corresponding key,and Click the "**Download**"button to generate the corresponding key.

3.8.5 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.

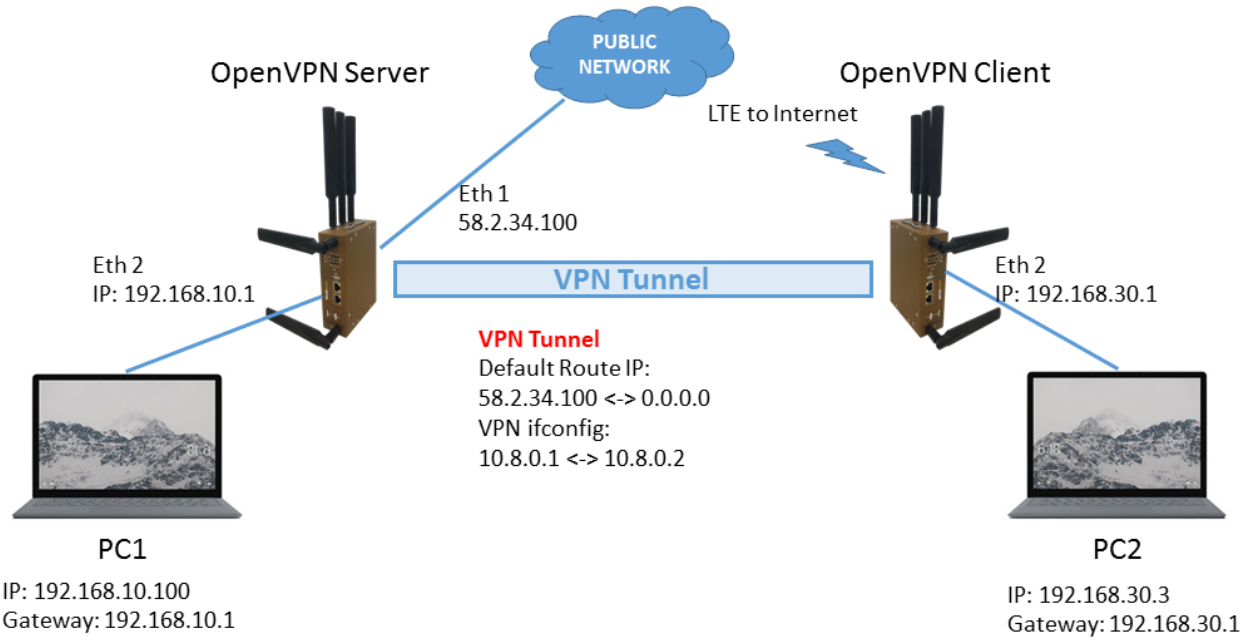


The description of the columns is as below:

TERMS	DESCRIPTION
Enable IPsec	Select Enable to activate the IPsec function
IPsec Status	Display the IPsec status, whether it is connected or disconnected
IKE version	**Default: v2**
Exchange Mode	Select Main mode and Aggressive mode
Authentication Method	Default: PSK Optional: Pre Shared Key or Certificate
Pre-shared key	**Default: 12345678** Set the preshared key
IPsec Cipher Suites	**Default: AES128-SHA1-DH2** Set algorithms for IKE and ESP proposal, choose AES128-SHA1-DH2, DES-SHA1-DH2 and 3DES-SHA1-DH2

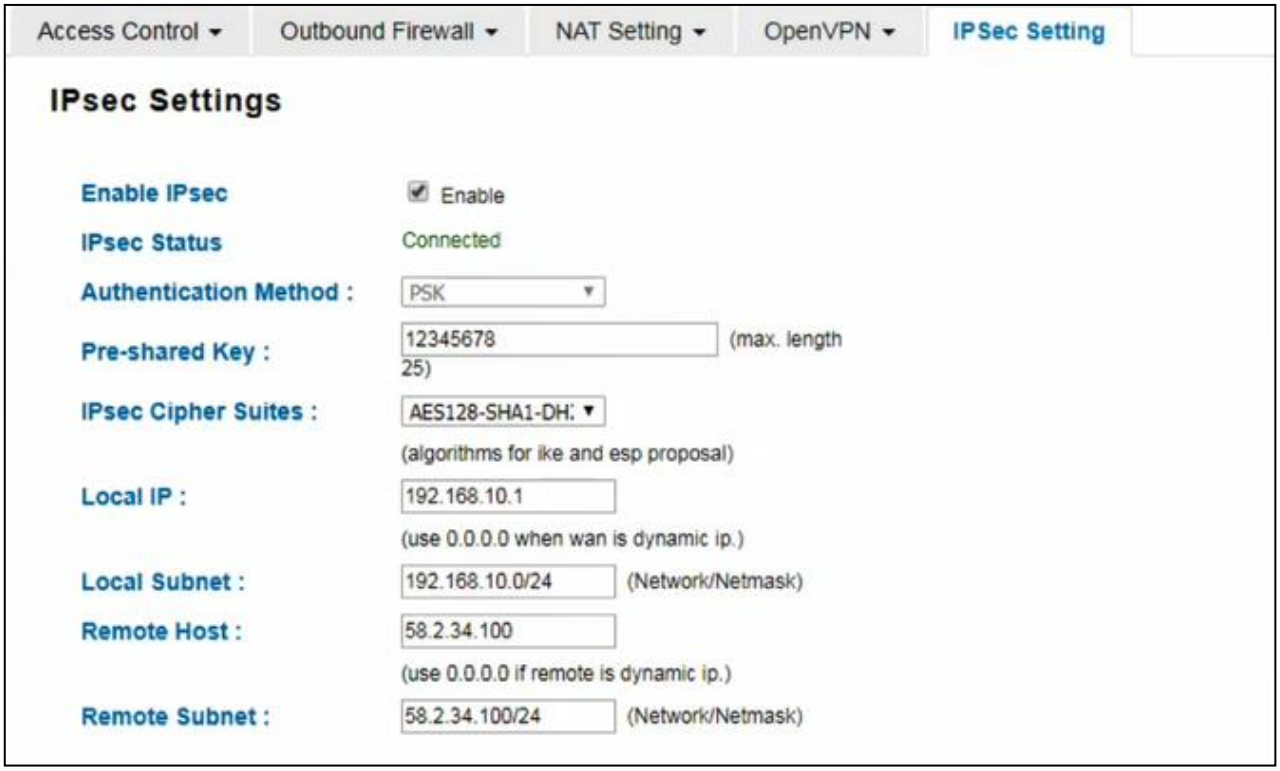
Local IP	IP Address of the local side of the tunnel. (Use 0.0.0.0 when WAN is dynamic IP.)
Local ID	Set IPsec Local device ID
Local Subnet	Set IPSec local protected subnet and subnet mask, i.e. 192.168.1.0/24
Remote Host	**Default: 0.0.0.0** Set IPsec Remote Host, use the default setting if remote is dynamic IP
Remote Peer ID	Set IPsec Remote device ID
Remote Subnet	Set IPsec Remote Protected Subnet/Subnet Netmask

Click **Submit** to apply the configuration.



The topology above is about how the branch office can get the access to the headquarter server. The two laptops are connected to the device using the Ethernet cable.

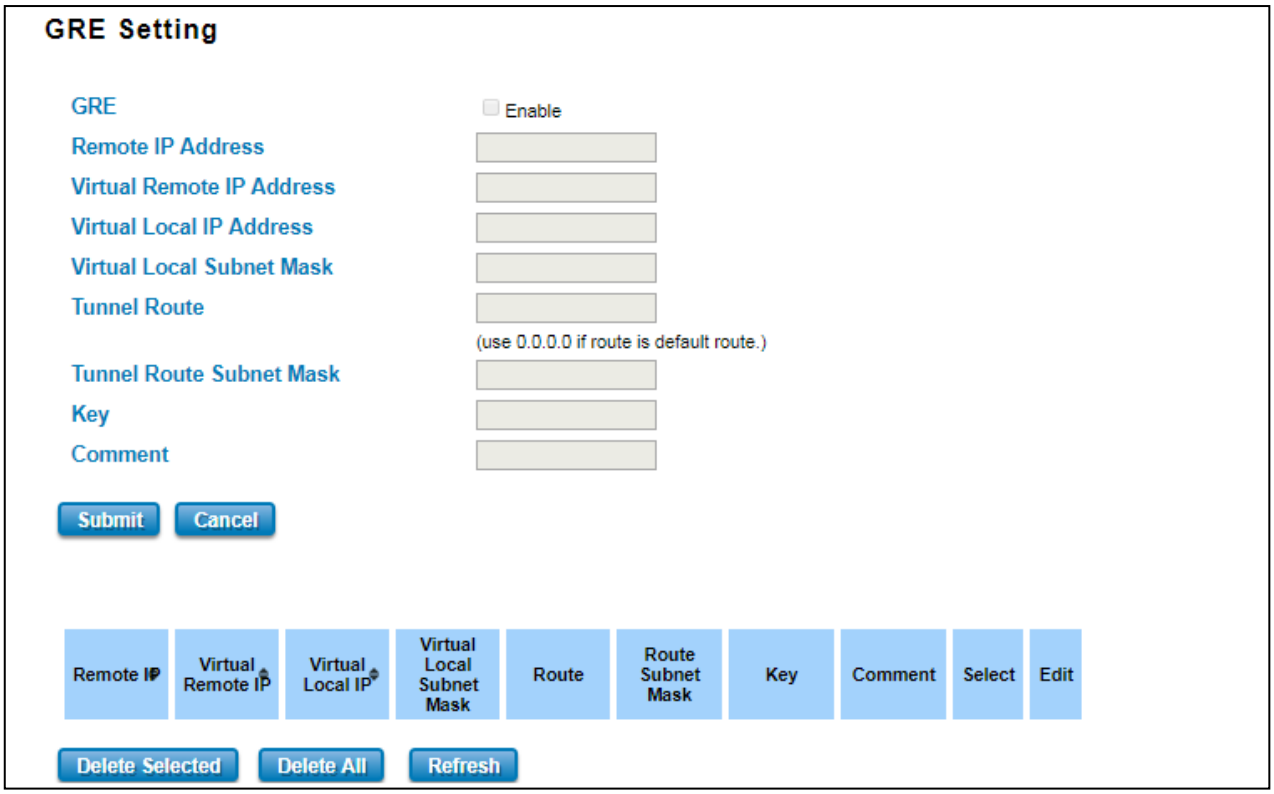
The laptop at the branch office picks a role as the VPN Client and the laptop at headquarter picks a role as the VPN Server. To get the access to the server the branch office need to connect to the VPN Server. As we can see the connection is established through the LTE connection. In this case, IPsec connection needs to be enabled. See the setting below.



When the connection is enabled, then the IPsec status will directly change to connected status, which means that the connection is established. So that the laptop at the branch office can access the server at headquarter.

3.8.6 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.



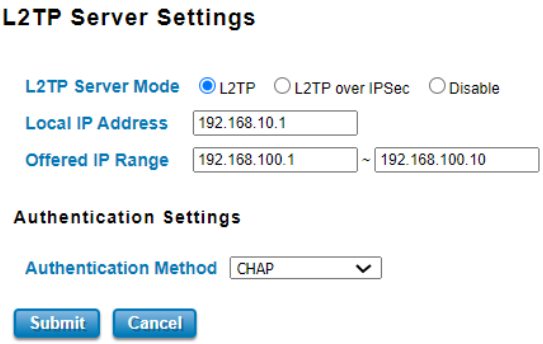
The description of the column is as below:

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.

3.8.7 L2TP SETTING

L2TP is a popular choice for remote roaming users for VPN applications since an L2TP client is built in to the Microsoft Windows operating system. In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy. Below is the L2TP Server Setting interface.

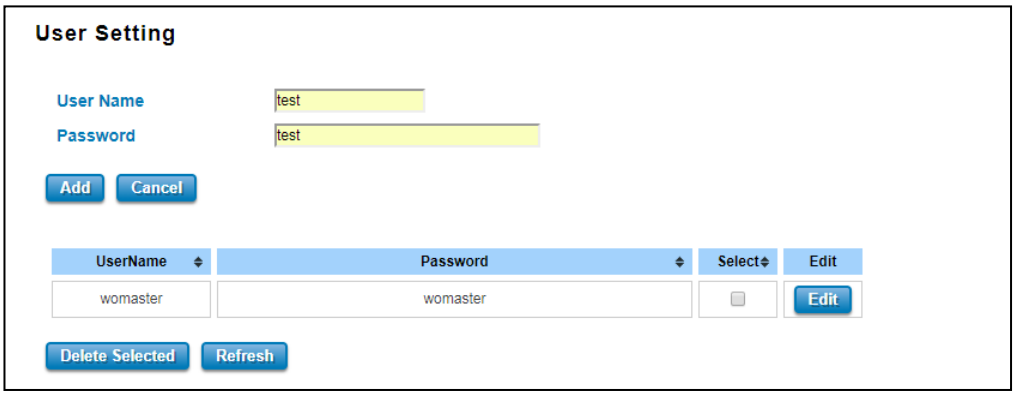


The description of the column is as below:

TERMS	DESCRIPTION
L2TP Server	Check the box to enable the function.
Local IP Address	The IP Address of the L2TP Server.
Offered IP Range	Offered IP Address range for the L2TP Clients (Maximum 10 clients)
Authentication Method	This section belongs to User Setting section. User can choose authentication using the password authentication protocol (PAP) and challenge handshake authentication protocol (CHAP).

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

Below is the User Setting for the L2TP Authentication connection.



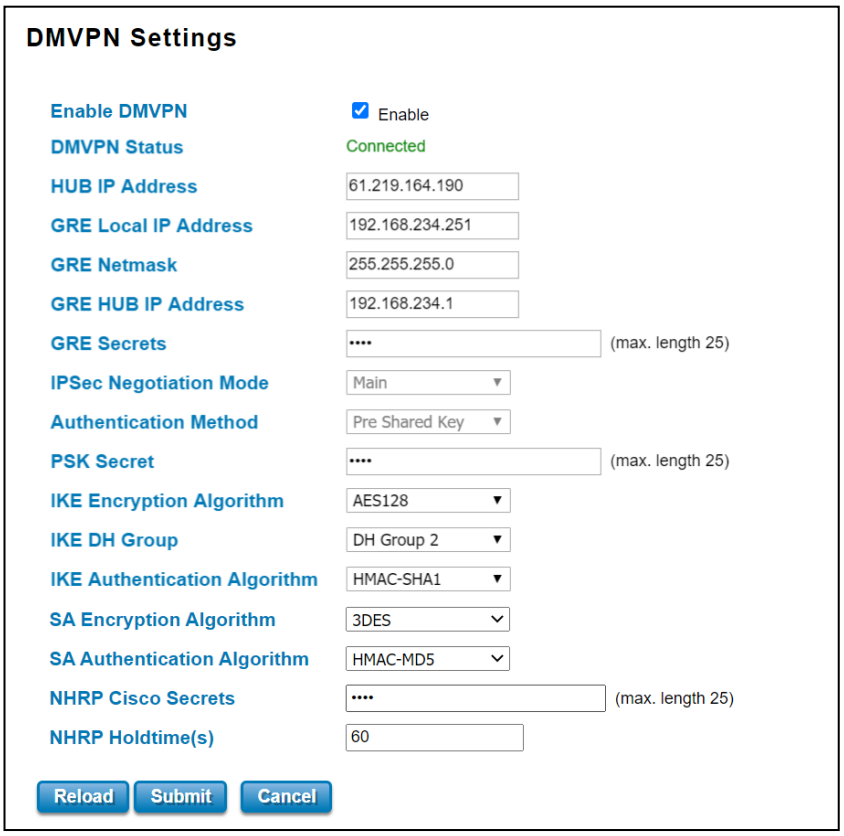
The description of the column is as below:

TERMS	DESCRIPTION
User Name	Username for L2TP connection
Password	Password for L2TP connection
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.

3.8.8 DMVPN SETTING

The Dynamic Multipoint VPN (DMVPN) feature allows users to better scale large and small IPSec VPNs by combining generic routing encapsulation (GRE) tunnels, IPSec encryption, and Next Hop Resolution Protocol (NHRP) to provide users with easy configuration through crypto profiles, which override the requirement for defining static crypto maps, and dynamic discovery of tunnel endpoints.



The description of the column is as below:

TERMS	DESCRIPTION
Enable DMVPN	Select Enable to activate the DMVPN function
DMVPN Status	Display the DMVPN status, whether it is connected or disconnected
HUB IP Address	IP address of the Hub.It is a public IP generally.
GRE Local IP Address	Set the local virtual IP Address of the GRE tunnel.
GRE Netmask	Set the netmask for the GRE tunnel IP address
GRE HUB IP Address	Set the GRE tunnel IP address for HUB
GRE Secrets	Set the key for the GRE tunnel.
IPSec Negotiation Mode	Set the IKE mode for IPSec.Only support main mode currently.
Authentication Method	Set the authentication method for IPSec.Only support PSK currently.
PSK secret	Set the PSK key for IPSec. Max. Length is 25.
IKE Encryption Algorithm	Set the IKE Encryption Algorithm.

	Optional:DES,3DES,AES128 or AES256.
IKE DH Group	Optional:DH group1, DH group 2 or DH group 5.
IKE Authentication Algorithm	Optional:HMAC-MD5 or HMAC-SHA1
SA Encryption Algorithm	Optional:DES,3DES,AES128 or AES256.
SA Authentication Algorithm	Optional:HMAC-MD5 or HMAC-SHA1
NHRP Cisco Secrets	Set the NHRP authentication key.Max. Length is 25.
NHRP Holdtime(s)	**Default: 60** Set Tunnel Link timeout.

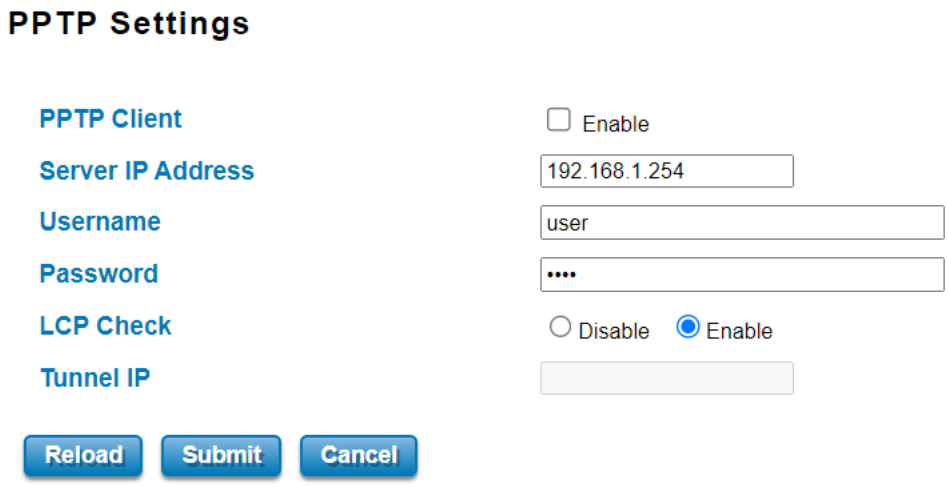
Click **Submit** to apply the configuration.

3.8.9 PPTP SETTING

PPTP (Point-to-Point Tunneling Protocol) is a network protocol used to establish a secure tunnel between two remote endpoints over a public network. It was designed to provide a secure connection over an untrusted network, such as the public internet.

PPTP creates a virtual private network (VPN) by encrypting and decrypting user traffic and then tunneling it through the public network. It uses a variety of encryption protocols to ensure the confidentiality and integrity of the transmitted data.

PPTP is primarily used to allow remote users to access a corporate network securely over the internet. It allows users to connect to internal networks and access resources as if they were directly connected to the private network.



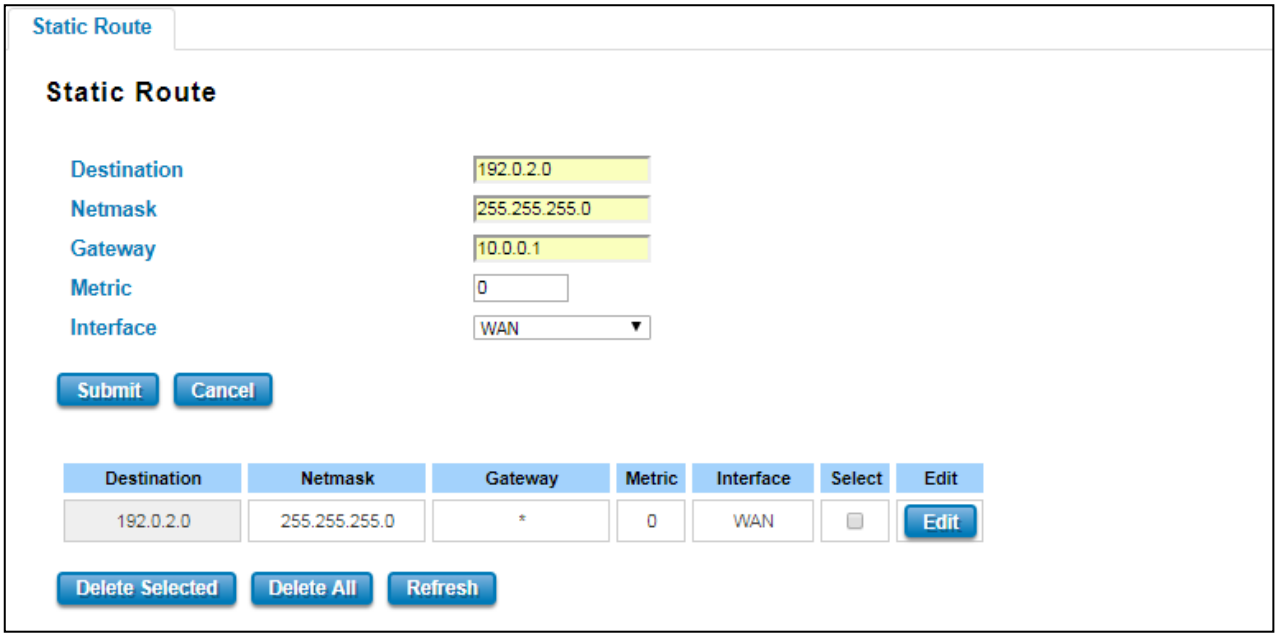
3.9 ROUTING

Layer 3 routing feature is requested since the hosts located in different broadcast domain can't communicate each other. The WoMaster Industrial Router is supported with two routing methods: static routing and dynamic routing. Dynamic routing makes use of RIPv2. The user can choose one routing method or combine the two methods to establish the routing table. In this Routing pages allows users create the Static Route and RIPv2 to do the routing.

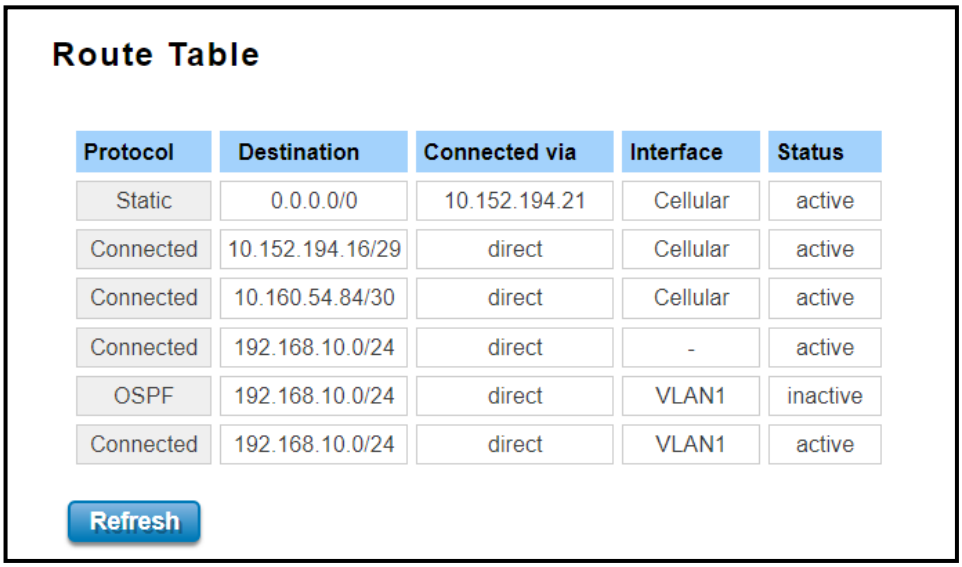
3.9.1 STATIC ROUTE

A static route is a route that is created manually by a network administrator. Static routes are typically used in smaller networks. In static routing, the Router's routing table entries are populated manually by a network administrator. The opposite of a static route is a dynamic route. In dynamic routing, the routing table entries are populated with the help of routing protocols.

The major advantages of static routing are reduced routing protocol router overhead and reduced routing protocol network traffic. The major disadvantages of static routing are network changes require manual reconfiguration in routers and network outages cannot be automatically routed around. Also it is difficult to configure static routing in a complex network. Below is the Static Route section interface.



Below figure show the Route Table.



The description of the column is as below:

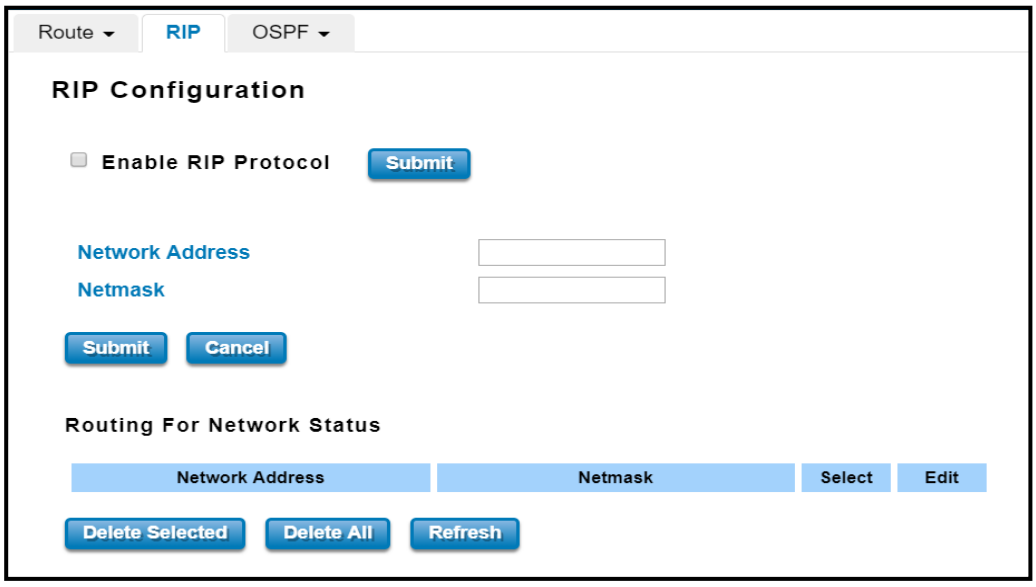
TERMS	DESCRIPTION
Destination	The Destination network IP address. For example,192.168.10.0
Netmask	Destination network's subnet mask.
Gateway	Gateway. Factory default is blank (0.0.0.0).
Metric	Assigns a cost to each available route so that the most cost-effective path can be.
Interface	The outgoing network interface. LAN, WAN, and Cellular are available to setup here.
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.

3.9.2 RIP

WoMaster Industrial Router is supported with RIPv2. The Routing Information Protocol (RIP) is a distance-vector, interior gateway (IGP) routing protocol used by routers to exchange routing information. RIP uses the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. RIP version 2 (RIPv2) was developed due to the deficiencies of the original RIP.

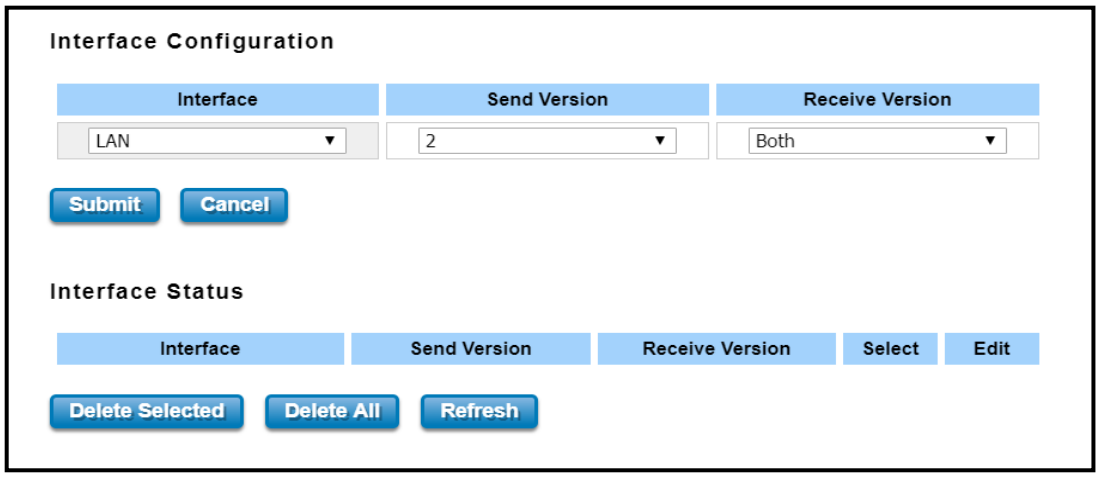
RIP Configuration



TERMS	DESCRIPTION
Enable RIP Protocol	**Submit** button to apply RIP protocol setting.
Routing for Networks	All the networks no matter directly connected or learned from other router/switch should be added to the switch. After typing the network address and netmask, click the **Submit** to add a routing network.

Click the **Submit** button to add a routing network. Click the **Delete Selected** button to remove selected network address. Click the **Refresh** button to refresh RIP information.

Interface Configuration



TERMS	DESCRIPTION
Interface	The IP interface.
RIP Version	RIP version of IP interface. (RIPv1, RIPv2 and Both)

Click the **Submit** button to apply RIP interface settings. **Delete Selected** button to remove selected interface. Click the **Refresh** button to reload RIP interface configuration.

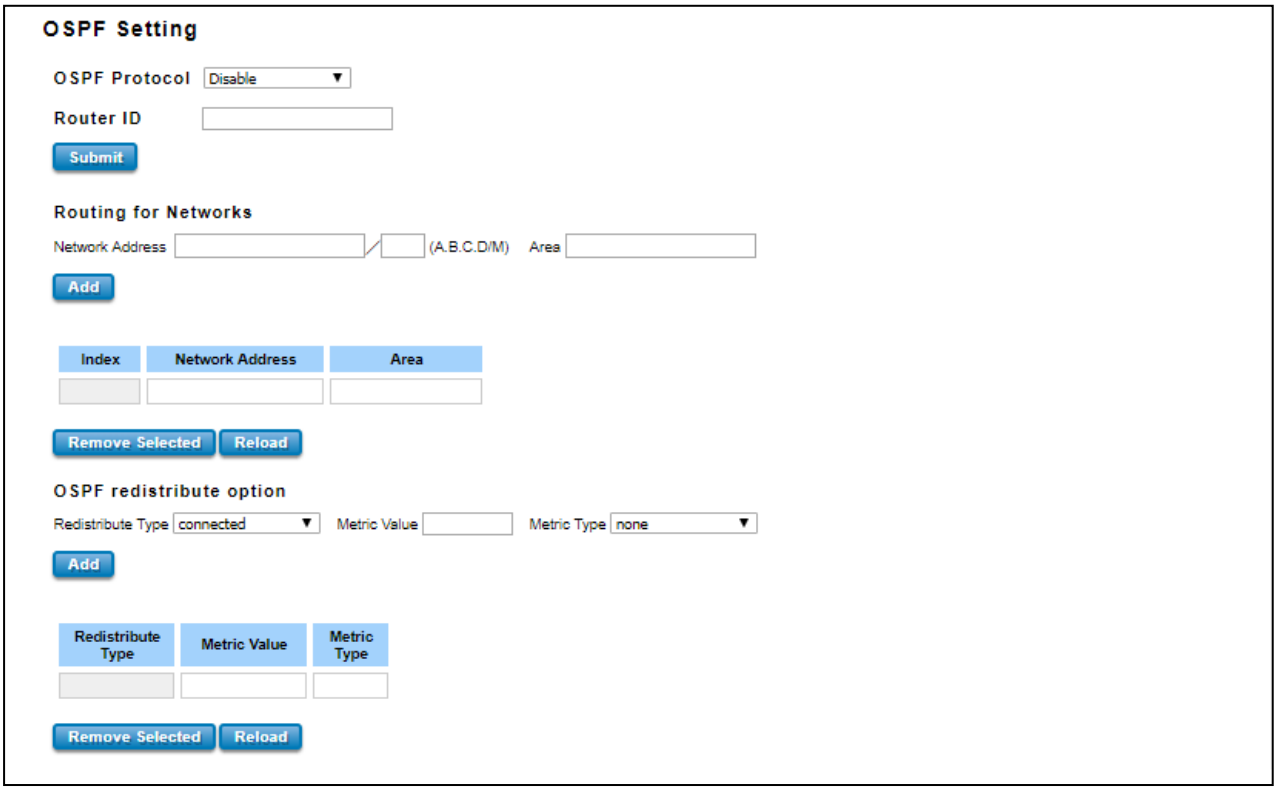
3.9.3 OSPF

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



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

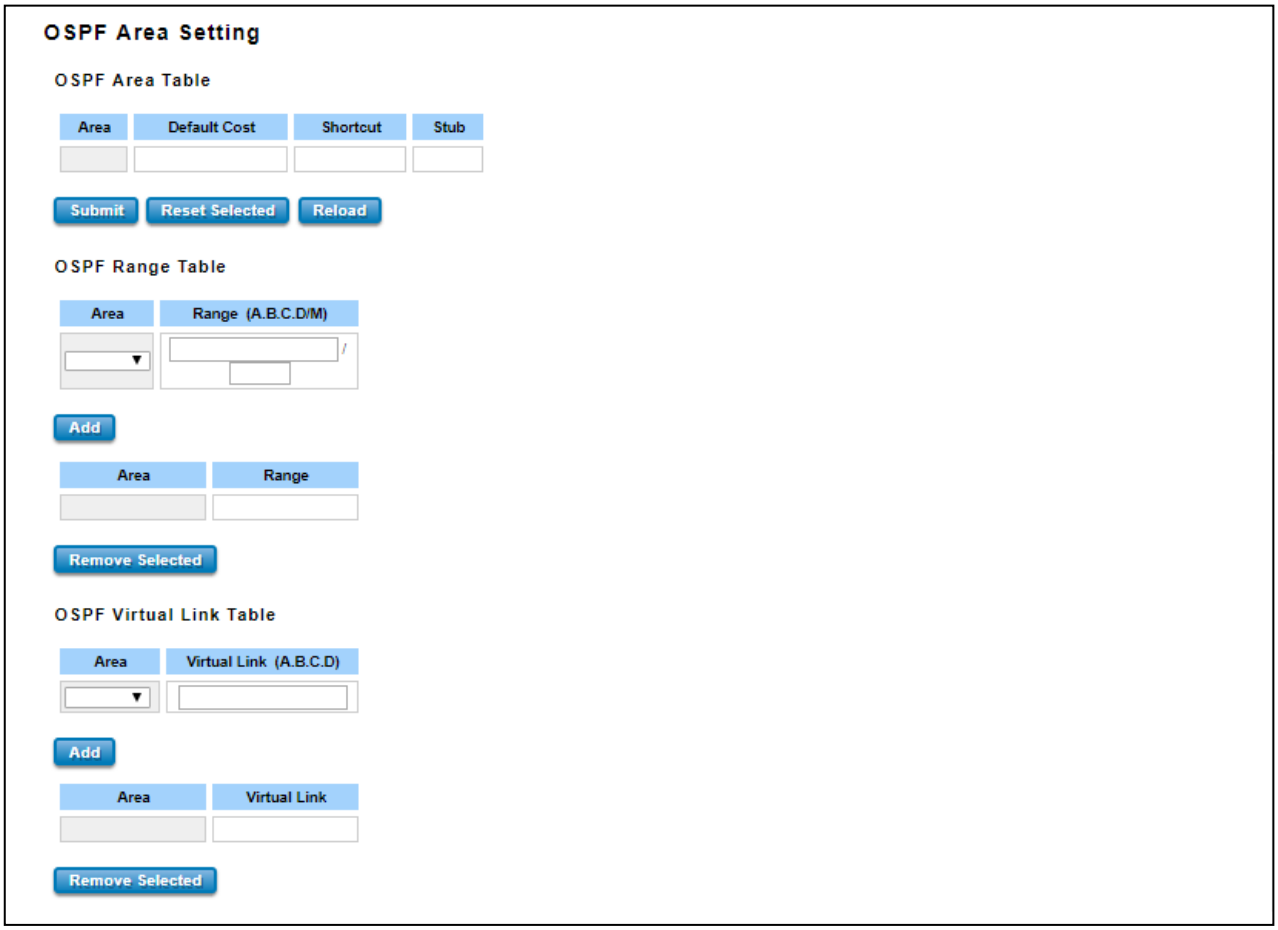
TERMS	DESCRIPTION
Interface	The VLAN Interface name.
Area	The area ID of the Interface you added. The Area ID must be the same for all routers/switches on a network.
Cost	The distance of this link/Interface, the default is identified depends on what the bandwidth is by the system. The value can be changed 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.

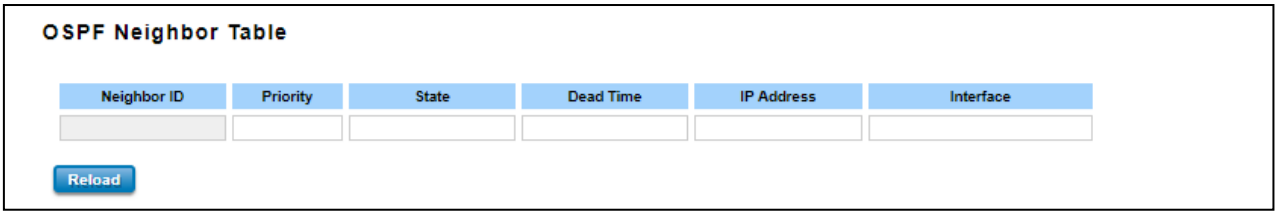
TERMS	DESCRIPTION
Area	This field indicates the area ID. Select the ID you want to modify here.
Default Cost	The default cost of the area ID.
Shortcut	No Defined, Disable, Enable. This indicates whether the area is the OSPF ABR shortcut mode.
Stub	Represents whether the specified Area is a stub area 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.



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.

OSPF Database

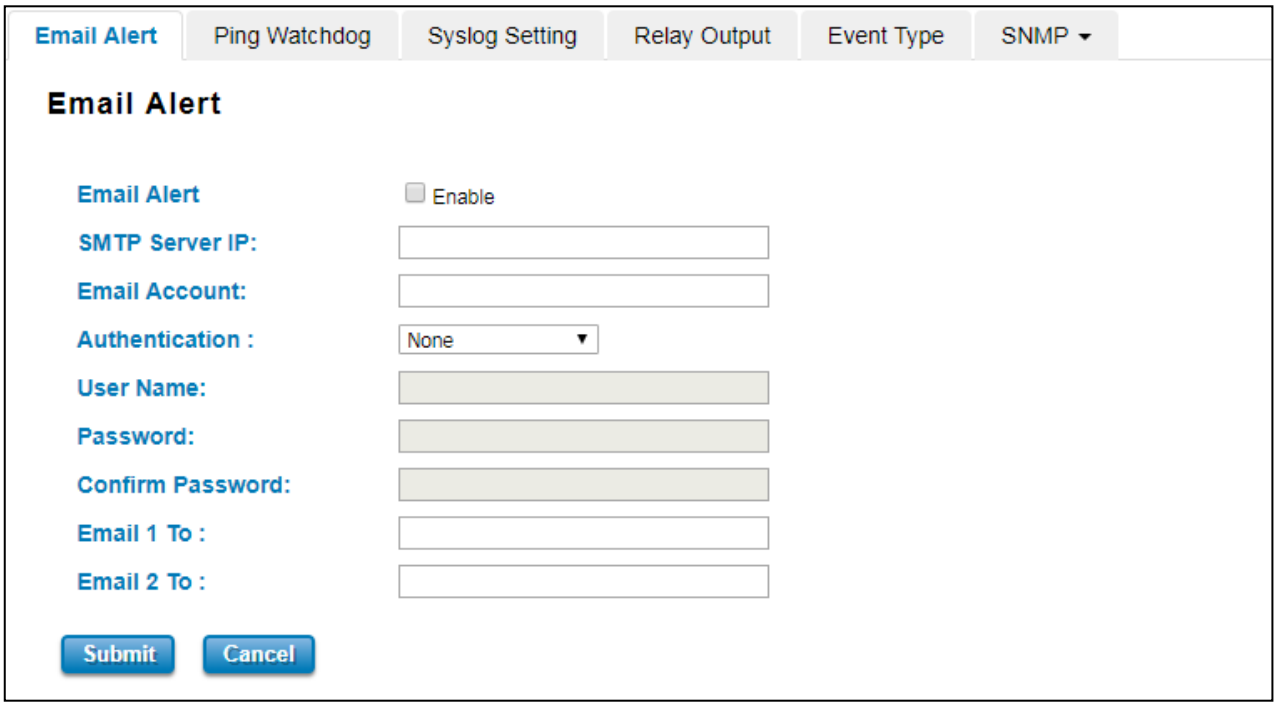
Click **Reload** to update the information.

3.10 WARNING

WoMaster' router provides several types of Warning feature for remote monitoring of end devices status or network changes.

3.10.1 EMAIL ALERT

WoMaster router supports E-mail Warning feature. With this function being enabled, the user is allowed to configure the detail settings for sending the e-mail alert to the SMTP server when the events occur. This page allows User to enable E-mail Alert, assign the SMTP Server IP, Sender E-mail, and Receiver E-mail. If the SMTP server requests User to authorize first, User can also setup the username and password on this page.

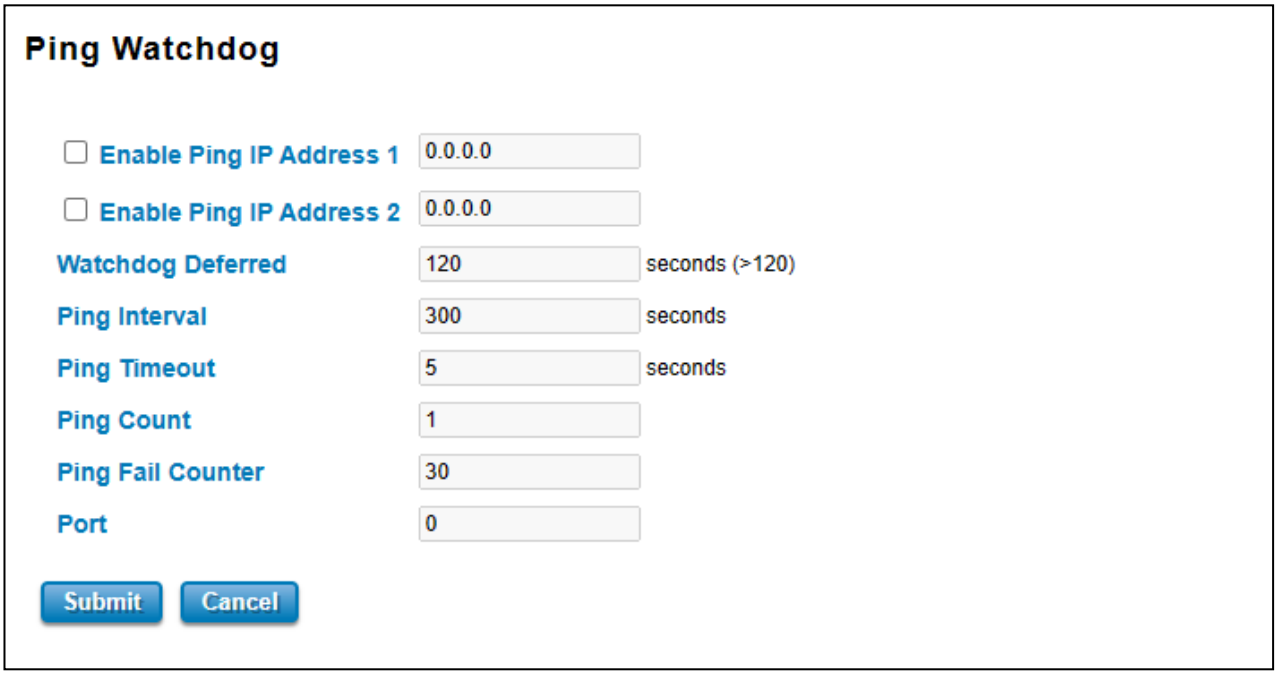


The description of the columns is as below:

TERMS	DESCRIPTION
Email Alert	Check the to enable the function
SMTP Server IP Address	Enter the IP address of the Email Server
Email Account	Enter the Email Server Account
Authentication	Choose the Authentication mode (None, Plain, Login)
User Name	Enter email Account name (Max.40 characters)
Password	Enter the password of the email account
Confirm Password	Re-type the password of the email account
User can set up to 2 email addresses to receive email alarm from the router	
Email 1 To	The first email address to receive an email alert from the router (Max. 40 characters)
Email 2 To	The second email address to receive an email alert from the router (Max. 40 characters)

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

3.10.2 PING WATCHDOG



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

The description of the columns is as below:

TERMS	DESCRIPTION
Enable Ping IP Address 1	Clicks enable to activate the feature. Set the first IP Address to check if the device is alive or not
Enable Ping IP Address 2	Clicks enable to activate the feature. Set the second IP Address to check if the device is alive or not
Watchdog Deferred	**Default: 120 (seconds) >120** The device needs time to boot, the startup delay use to buffer to prevent the device continue to reboot itself.
Ping Interval	**Default: 300 (seconds)** Set the interval timer to Ping the remote device. Every 300 seconds the device will try to ping the target IP.
Ping Timeout	**Default: 5 (seconds)** Set the timeout timer to Ping the remote device. Every 5 seconds the ping will timeout.

Ping Count	**Default: 1** The device num. of pings
Ping Fail Counter	**Default: 30** When the remaining Ping Fail Counter reach to 0 or reach the failure count, the device will reboot.
Port	Clicks enable to activate the feature. Set the port number to check if the device is alive or not

Click **Submit** to apply the configuration.

3.10.3 SYSLOG SETTING

System Log is useful to provide system administrator locally or remotely monitor router events history.

Once User finishes configuring the settings, click on **Submit** to apply User configuration. User can monitor the system logs in [Diagnostics] / [Event Log] page

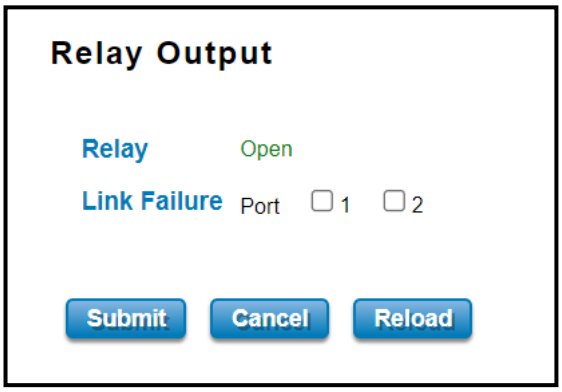
The condition or term described as following table.

TERMS	DESCRIPTION
Enable Remote Syslog Server	Select Enable to enable system log
TLS	Select Enable to enable TLS
IP Address	Specify the IP address of the server.
Port	**Default: 514** Specify the port number of the server

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

3.10.4 RELAY OUTPUT

WoMaster' router 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 Relay Output configuration interface has shown as below:



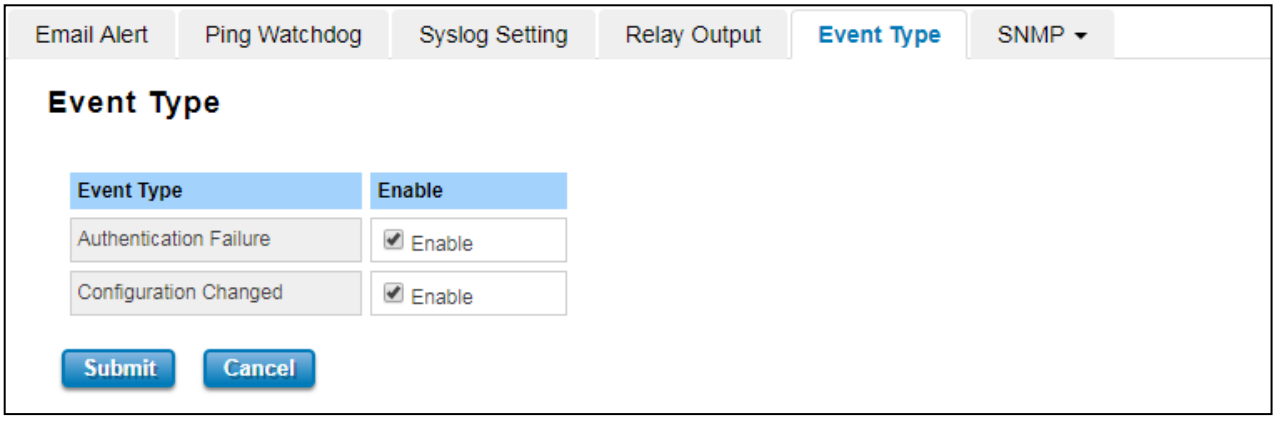
The condition or term described as following table.

TERMS	CONDITION	DESCRIPTION
Relay	ON or OFF	The status change to ON if any kind of failure is detected. OFF if the status is normal.
Link Failure	LAN Port number 1 - 2	Monitoring port link down event

After finishing the configuration, clicks **Submit** to activate the relay alarm function.

3.10.5 EVENT TYPE

In this page user allowed to select the Event Type **Event Warning Type:** The event warming type selection. It has two event types, Authentication Failure and Configuration Changed.

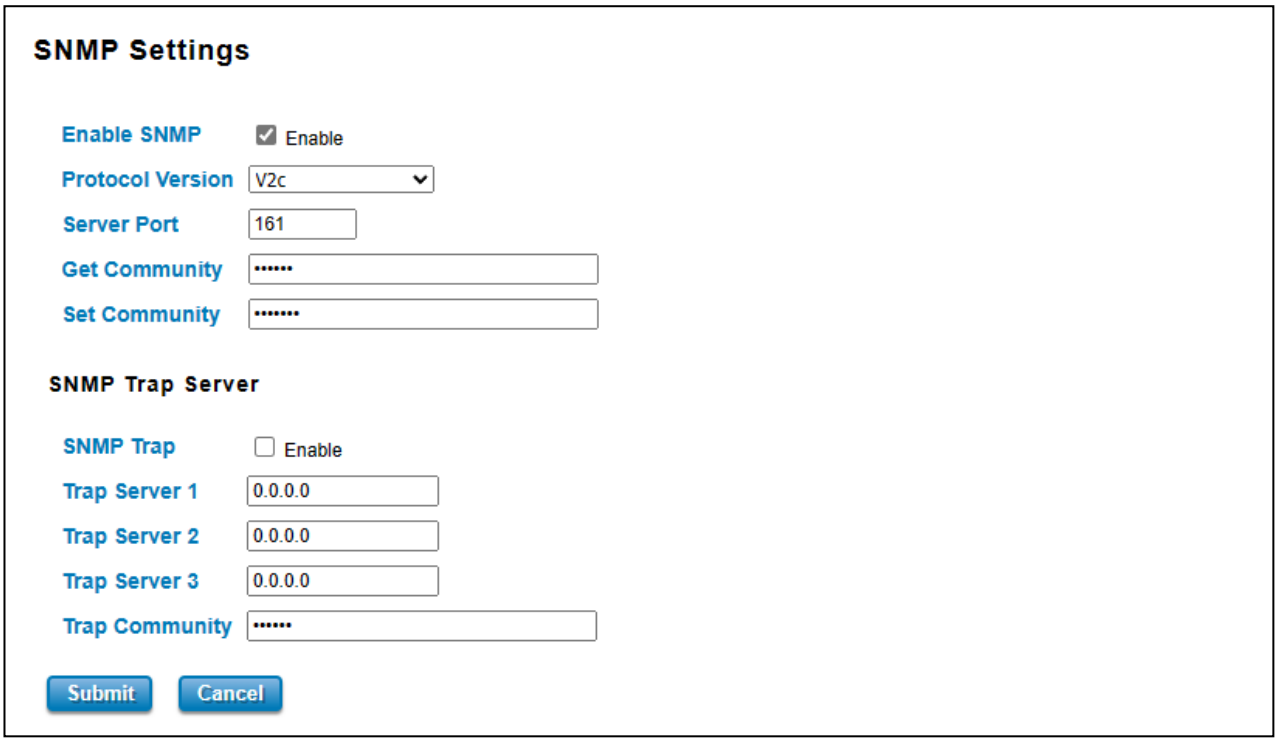


TERMS	DESCRIPTION
Authentication Failure	When the authentication fails, the system will issue the event log/email alert to the system log/SMTP server respectively.
Configuration Changed	When there are any kinds of changing in the configuration, the system will issue the event log/email alert to the system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

Click **Submit** to apply the configuration.

3.10.6 SNMP

SNMP is a standard TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates. System management software uses SNMP to allow administrators to remotely monitor and manage thousands of systems on a network, often by presenting the data gathered from monitored devices in a snapshot or dashboard view. WoMaster' Router support SNMP V2c and V3



SNMP Setting

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

SNMPv2C

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

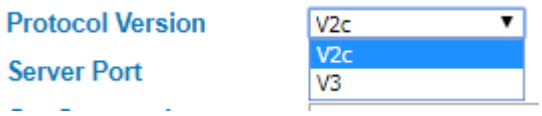
SNMP V3

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

SNMPv3 security comes primarily in 2 forms:

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

The description of the columns is as below:

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

After finishing the configuration, clicks **Submit** to activate the function.

SNMP Trap Server

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

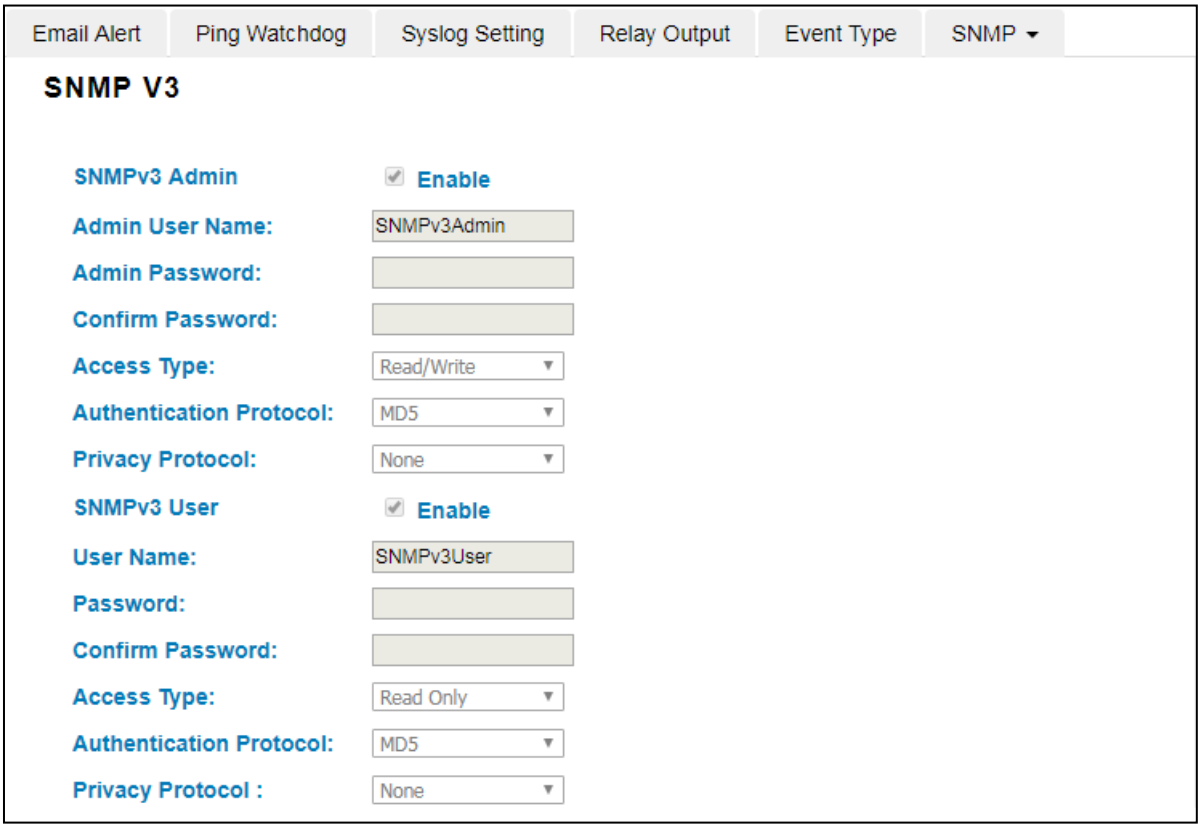
The description of the columns is as below:

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

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

SNMP V3

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

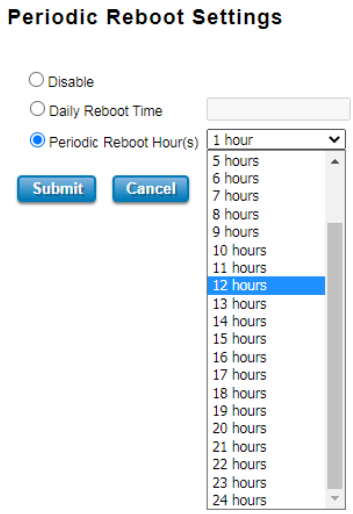


TERMS	DESCRIPTION
SNMPv3 Admin	Clicks enable to activate the function and the entries for SNMPv3 Admin.
Admin User Name	**Default: SNMPv3Admin** Set up the User Name for the SNMPv3 Admin
Admin Password	Set up the Password for the SNMPv3 Admin
Confirm Password	Confirm the Admin for the SNMPv3 Admin
Access Type	Access type for the SNMPv3 Admin, choose Read Only or Read and Write
Authentication Protocol	**Default: MD5** Provides authentication based on MD5 or SHA algorithms.
Privacy Protocol	Specify the encryption method for SNMP communication. None and DES are available. **None**: No encryption is applied.

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

3.10.7 PERIODIC REBOOT

The setting allows you reboot the device in case some un-controller error in remote site. This is one type of the watchdog feature, **it is better to configure longer period,** and **please Notice that the router will periodically reboot the router even the router works normally.** The period is configurable, allowing at Daily Reboot Time or specific time of periodic resets.

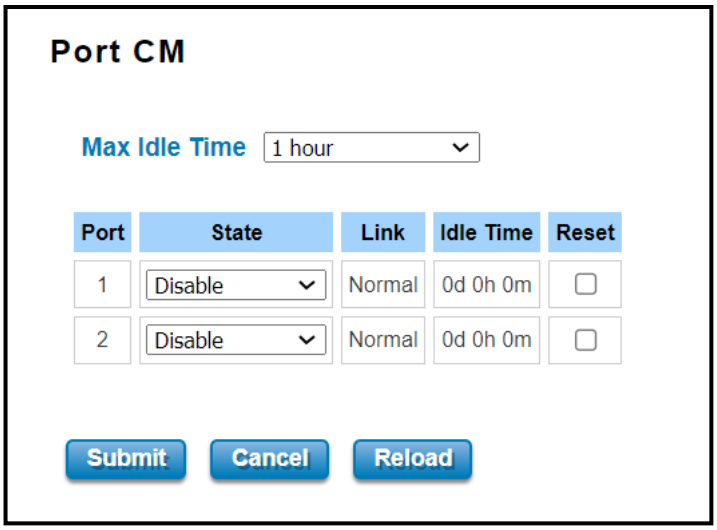


TERMS	DESCRIPTION
Disable	Disable the feature
Daily Reboot Time	Type the specific daily reboot hour time of hour/minute. The format is HH:MM, ex: 23:00
Periodic Reboot Hour(s)	Select the period time you prefer in this column.

3.10.8 Port CM

WoMaster router support the following function：

Disable ports after a certain time without activity (no device connected). Ports should be disabled after, for example, 1 week without connection of any device. This port would need to be manually activated to be recovered after this period of time.After reboot or loss power, router will keep the port is link down. So to recover access through this port, they have to reactivate it on GUI.



TERMS	DESCRIPTION
Max Idle Time	Set the max idle time.Max：4 weeks.
State	Enable/Disable the feature
Link	Show the link status.
Idle Time	Display accumulated idle time.
Reset	Reset the link status.

3.11 DIAGNOSTICS

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

Following commands are included in this group:

3.11.1 Event Logs

3.11.2 ARP Table

3.11.3 Ping

3.11.4 Trace Route

3.11.5 Network Statistic

3.11.6 Iperf

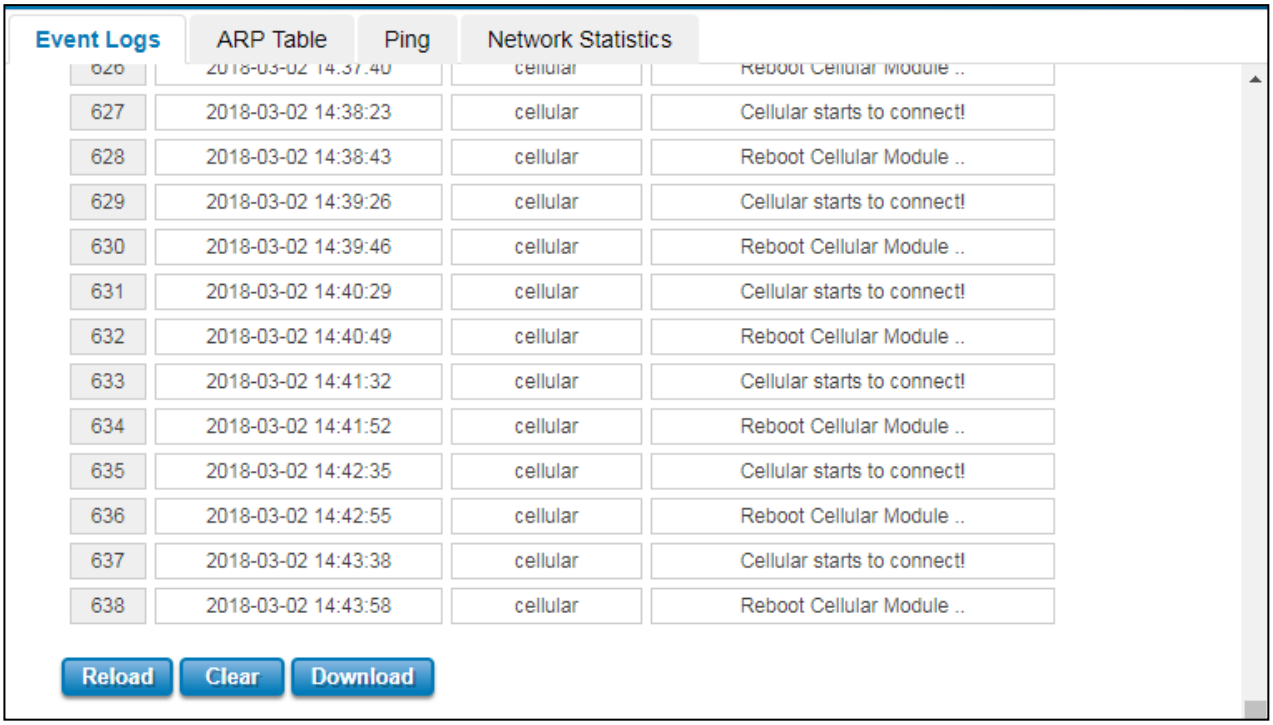
3.11.7 Netconf

3.11.8 Tcpdump

3.11.9 Client Association List

3.11.1 EVENT LOGS

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



TERMS	DESCRIPTION
#	Event index assigned to identify the event sequence.
Time	The time is updated based on how the current date and time is set in the Basic Setting page.
Source	Show the log's source.

Message	Show the record status.

Click **Reload** to refresh the table. Click **Clear** to remove the entire event logs list. User may download the event logs file by click **Download**.

3.11.2 ARP TABLE

Basically, WoMaster device is supported with two types of ARP which is the standard ARP and ARP with 802.2 LLC Type 2. Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions. The other ARP feature is ARP with 802.2 LLC Type 2 is the new level of ARP where the device will response the request of 802.2 snap ARP on the Ethernet port and not support sending the request of 802.2 snap ARP. Below is the Data format.

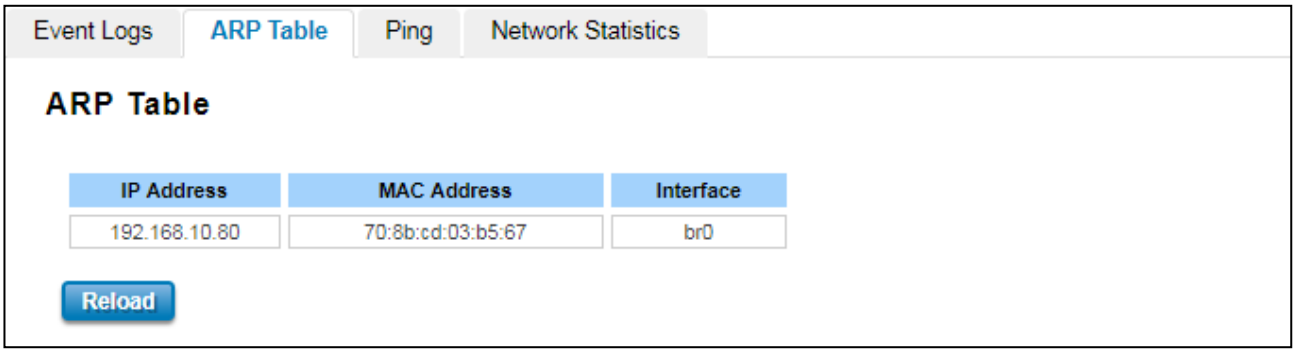
Data Format

Protocol Header:

802.3 + 802.2 LLC + 802.2 snap

|- (DS + SA + Len) -|- DSAP + SSAP + CTRL -|- Org + type

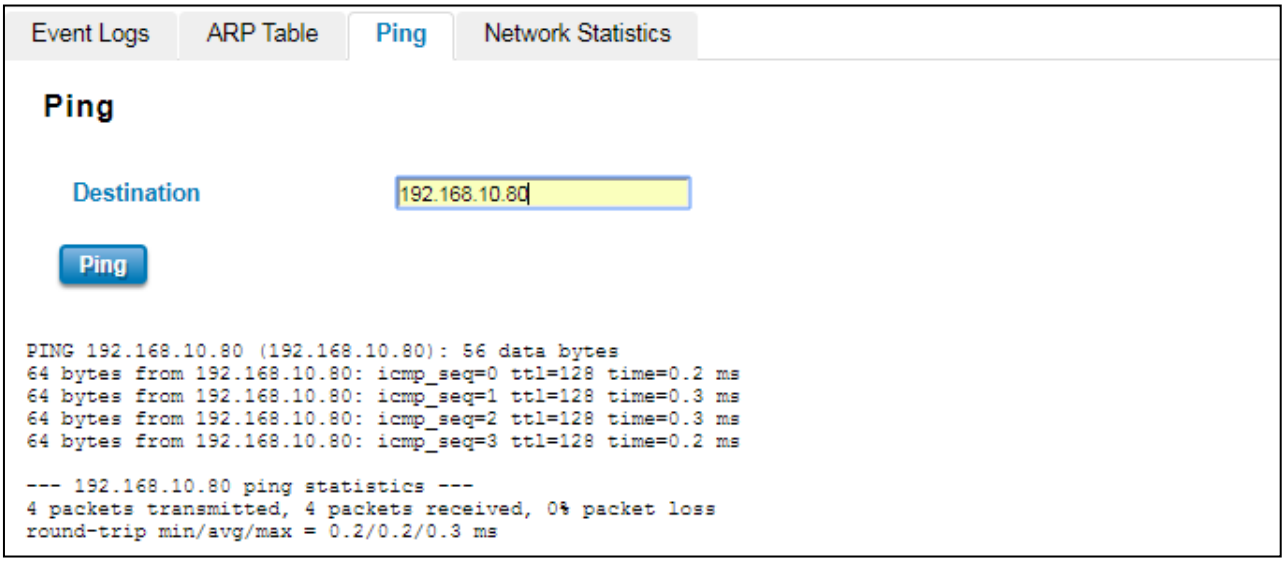
This page shows the routers active ARP table. An ARP table contains recently cached MAC addresses of every immediate device that was communicating with the router.



Click on **Reload** to change the value.

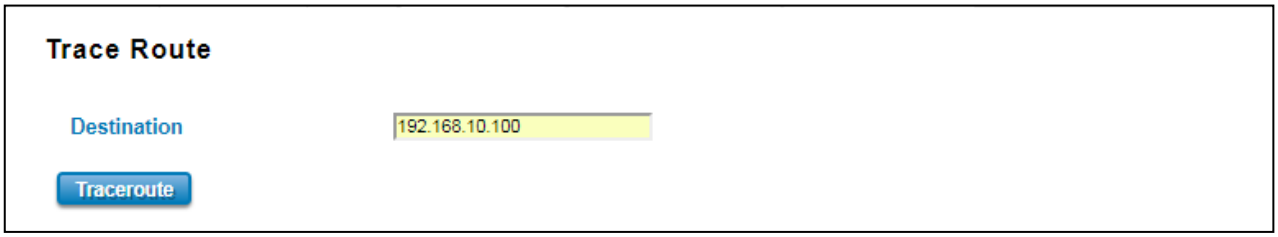
3.11.3 PING

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

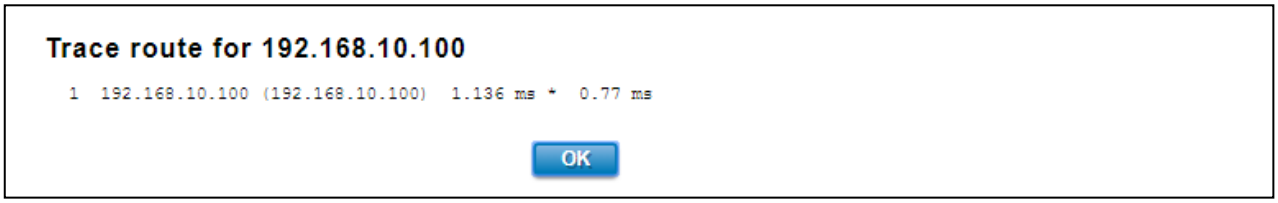


3.11.4 TRACE ROUTE

Traceroute is a diagnostics tool for displaying the route (path) and measuring transit delays of packets across an Internet IP network. Log containing route information will be shown after few seconds. Enter the destination IP Address then click traceroute to start the process.

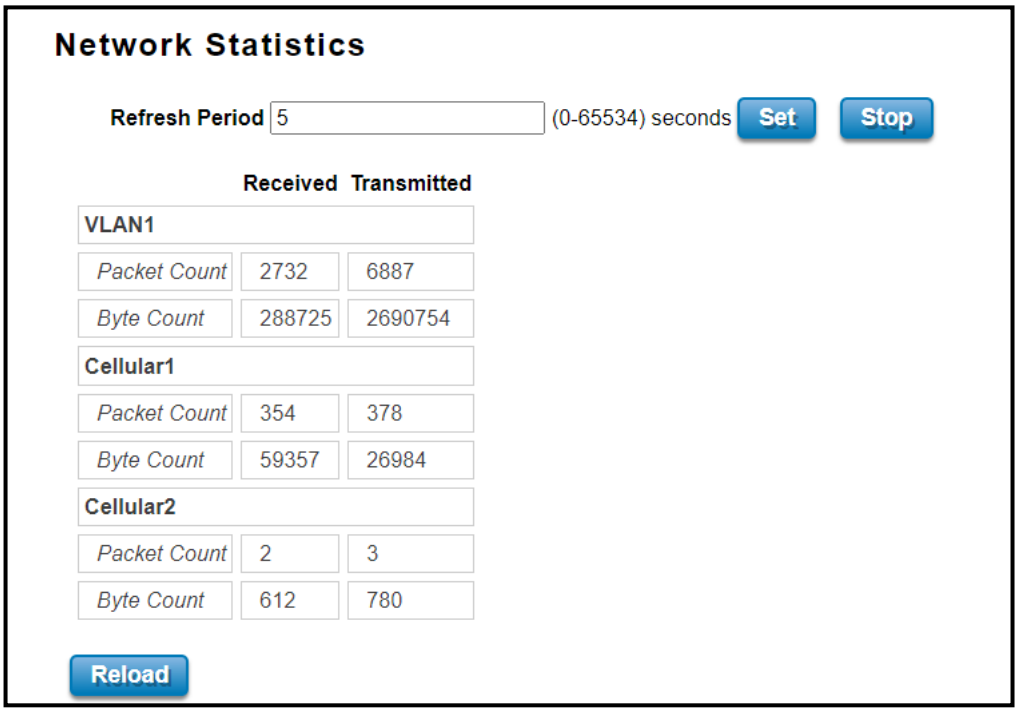


It will start search the route and measuring the transit delays of the packet.



3.11.5 NETWORK STATISTICS

This section shows about the packet data that transmitted or received regarding the Ethernet and Cellular activity. The Cellular packets include Wi-Fi and 2G/3G/LTE transmission.



Click on **Reload** to refresh the table.

The description of the columns is as below:

TERMS	DESCRIPTION
Refresh Period	**Default: 5** To set the Poll Interval time setting with range from 0 to 65534. (second)
Set	To set new Interval time. Stop the old Poll Interval first before set the new interval.
Stop	To stop Polling Interval, this action can be executed when user wants to change the poll interval time.

3.11.6 Iperf

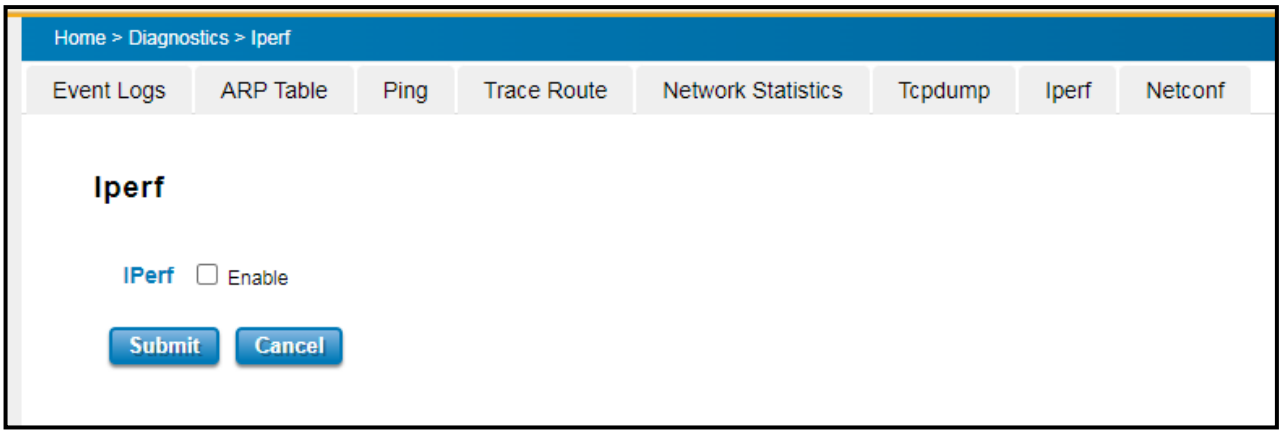
Iperf is a software tool that is used to measure the bandwidth performance of a network connection. It is designed to allow network administrators, engineers, and researchers to assess the maximum achievable data transfer rates between two hosts connected over a network.

Iperf operates by establishing a connection between two hosts using the User Datagram Protocol (UDP) and then transmitting and receiving data packets across the connection. It measures various metrics such as the total amount of data transferred, the transfer rate, and the round-trip time (RTT) of the packets.

Iperf supports various options and configurations that allow users to customize the test according to their specific requirements. For example, users can specify the size of the data packets, the number of packets to transmit, and the duration of the test. Additionally, Iperf can be used in both client-server and peer-to-peer configurations, allowing

users to test different network scenarios.

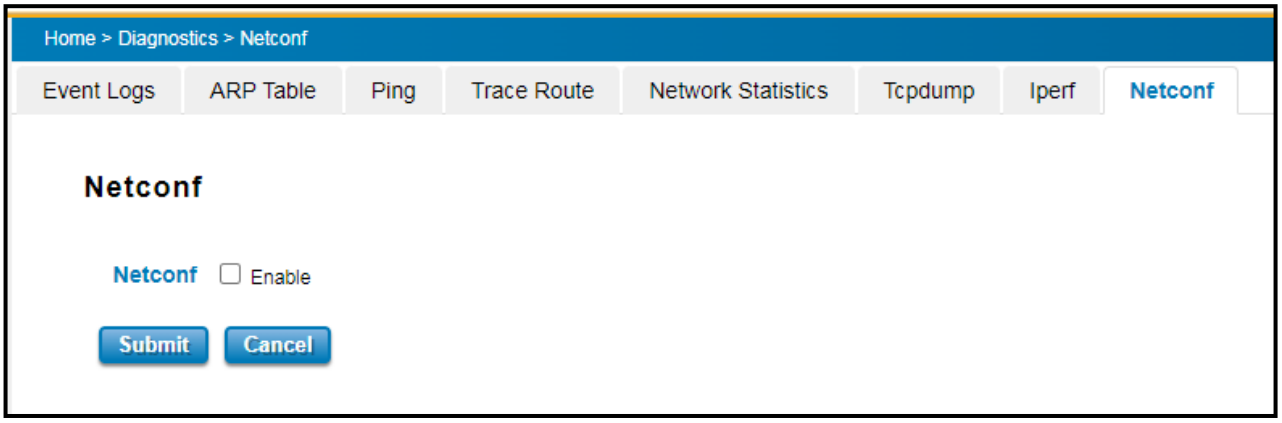
Iperf is widely used in network engineering and research due to its flexibility, accuracy, and ability to provide detailed performance reports. It is particularly useful for testing network links, evaluating network upgrades, and conducting network capacity planning. Iperf is freely available as open-source software and is supported on multiple operating systems, making it a popular choice for network performance testing.



3.11.7 Netconf

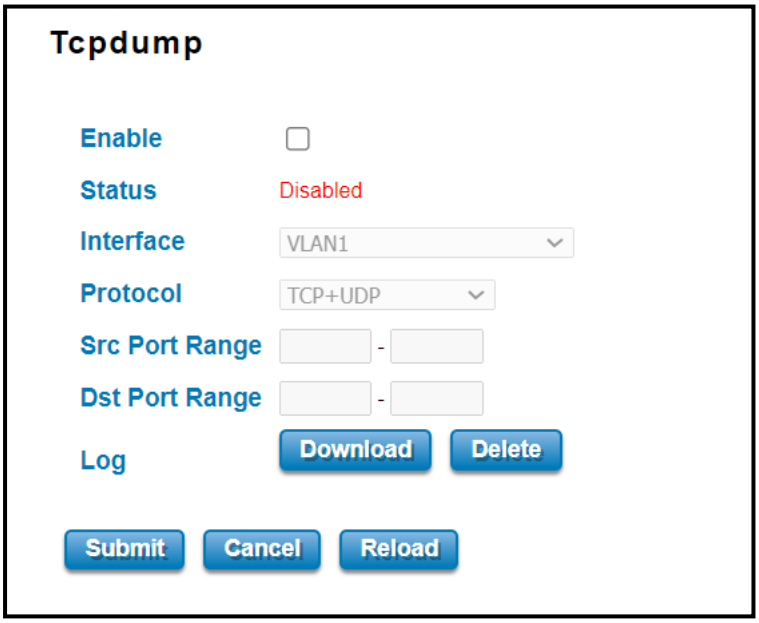
Netconf (Network Configuration Protocol) is a protocol used to manage and configure complex network devices in a vendor-agnostic manner. It was developed to address the limitations of the traditional command-line interface (CLI) for network configuration, which is often inefficient and does not provide a complete representation of the network device's configuration.

Netconf provides a standardized way to access and modify the configuration of network devices, including routers, switches, and firewalls. It allows network administrators to view, edit, and delete device configurations using a well-defined protocol. Netconf communication is encrypted and authenticated to ensure secure device communication.



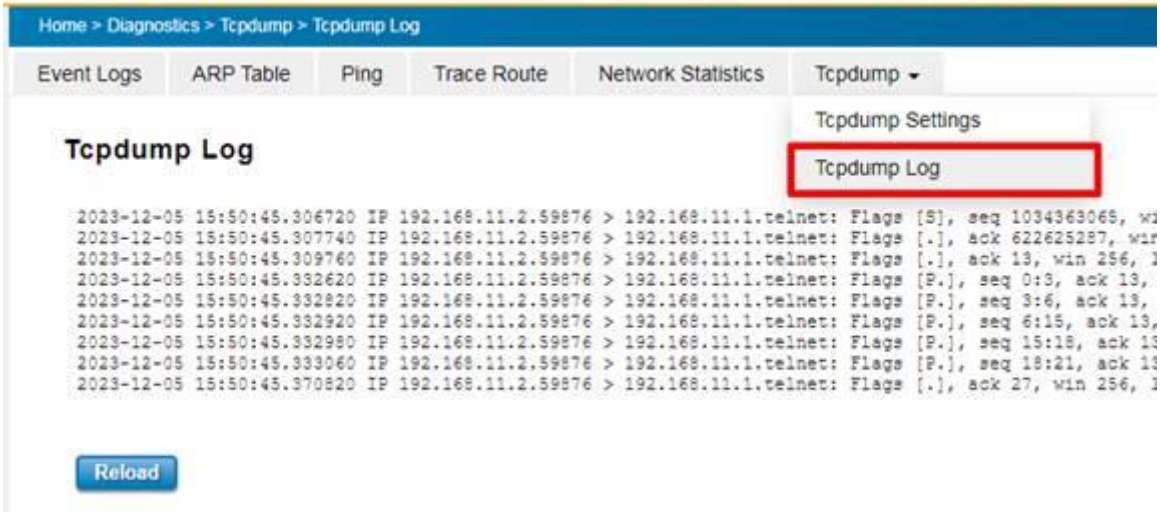
3.11.8 Tcpdump

WoMaster router can support Tcpdump function.Tcpdump is a packet analysis tool that allows users to capture and analyze network packets, troubleshoot connection issues, and identify potential security issues. It is a highly flexible program that can be used to filter data based on criteria such as network layer, protocol, host, network, or port.



Click **Reload** to refresh the list.

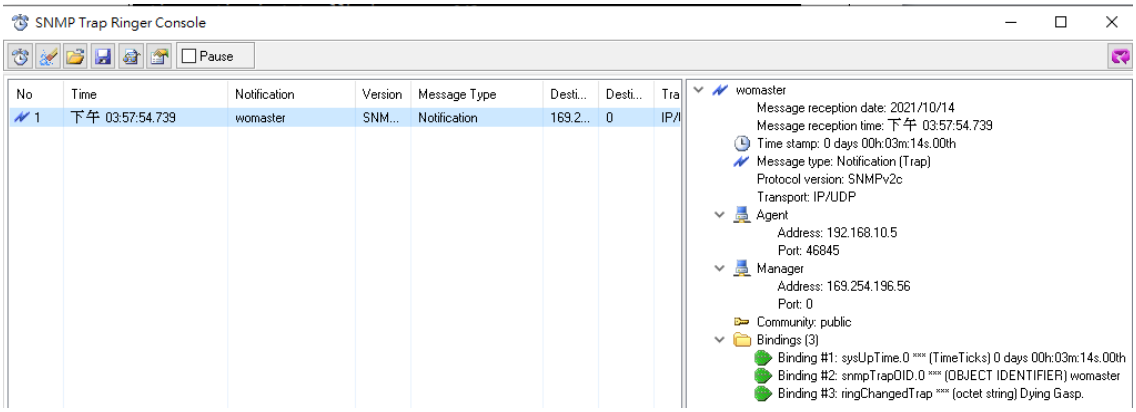
After enabling Tcpdump function, check the TCPDUMP in real-time on the web interface.



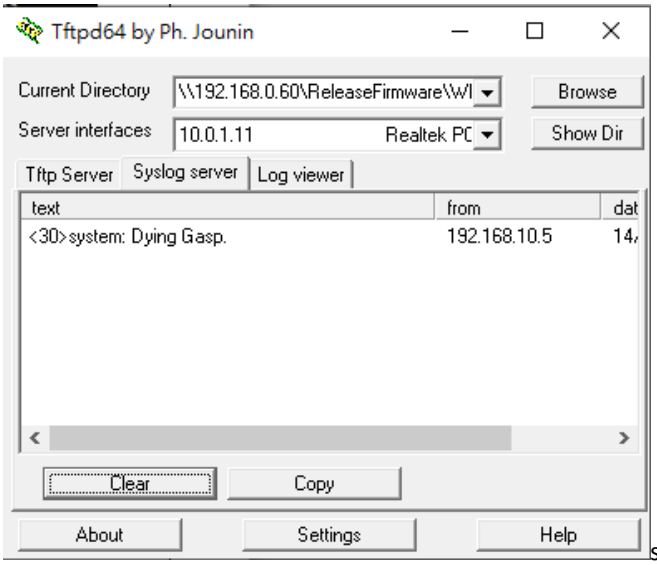
3.11.9 DYING GASP

A dying gasp is a message sent by the router to indicate that the router has lost power. It's also known as "last gasp". The dying gasp is enabled in the router which supports dying gasp hardware and software feature. To see the dying gasp, you MUST configure the target Syslog Server or SNMP Trap server. Then it has possibility of sending a last gasp event to the specific server while power supply loss.

Below figures show the example of SNMP trap and syslog events.



SNMP Trap



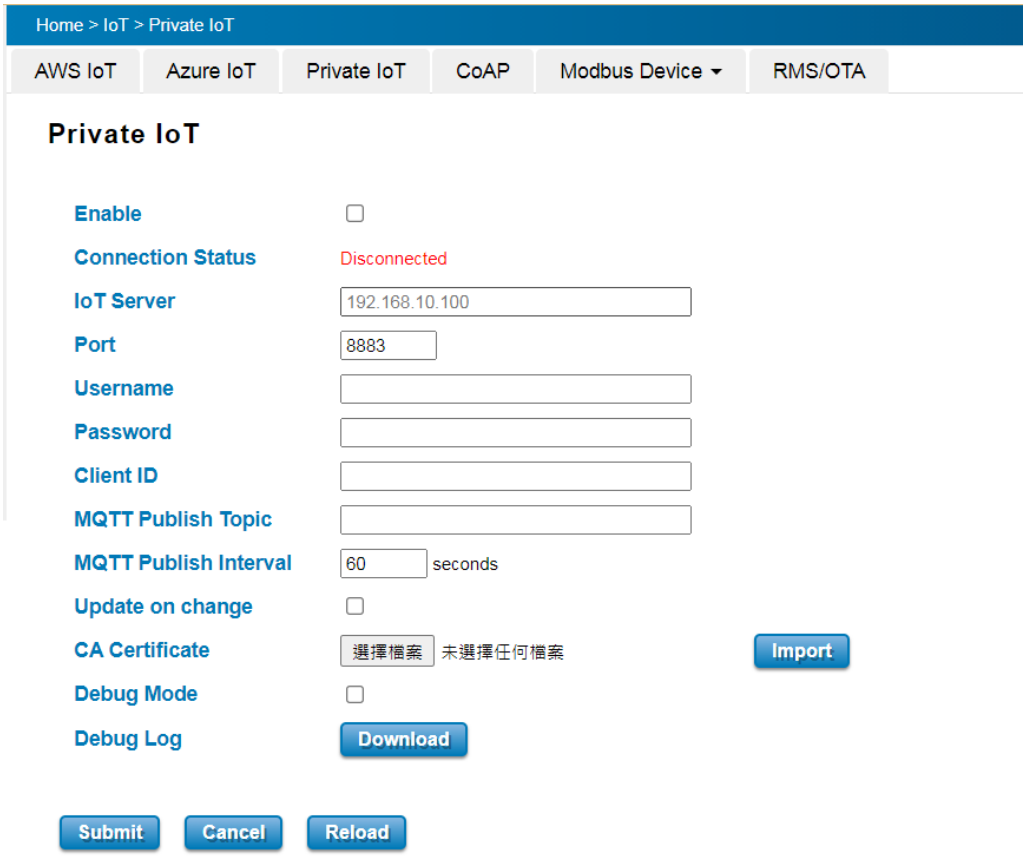
syslog

3.12 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.

3.12.1 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.



The description of the columns is as below:

TERMS	DESCRIPTION
Enable	Enable the WoM IoT function
Connection Status	The connection status between the router and IoT server.

IoT Server	Enter the specific IoT Server.
Port	Specify the specific port of the IoT server.
User Name	Enter the user name.
Password	Enter the password of the user name.
Client ID	Enter the client ID that has been registered.
MQTT Publish Topic	Specify the MQTT Topic
MQTT Publish Interval	The interval time to update the data.
Update on change	**Default: Uncheck** Check the box to keep update the data. The router will check whether the system and Modbus info from serial port is updated or not, if the value is changed, the router will pubish the data to IoT Server.
CA Certificate	The function from this certificate file is to create an encrypted MQTT communication. User can apply the CA file from the cloud server. For example, you can get this file together when download the ThingsMaster server file. **Note. This field only supports in ThingsMaster v1.1**
Debug Mode	Enable/Disable the debug mode. Default is Uncheck.
Debug Log	You can download the log for debugging.

Click **Submit** to apply the configuration.

HOW TO ESTABLISH AND CONNECT TO THE THINGSMASTER CLOUD SERVER

1. Download and install VMware Workstation Player.

Please click the link below.

https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/14_0

2. Download the server file from the link that sent by the Sales.

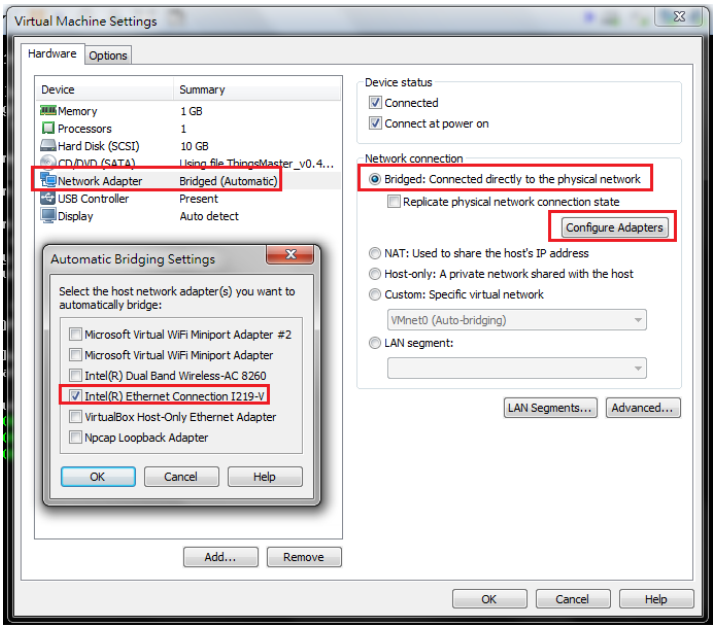
3. Open a Virtual Machine from disk and import.

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

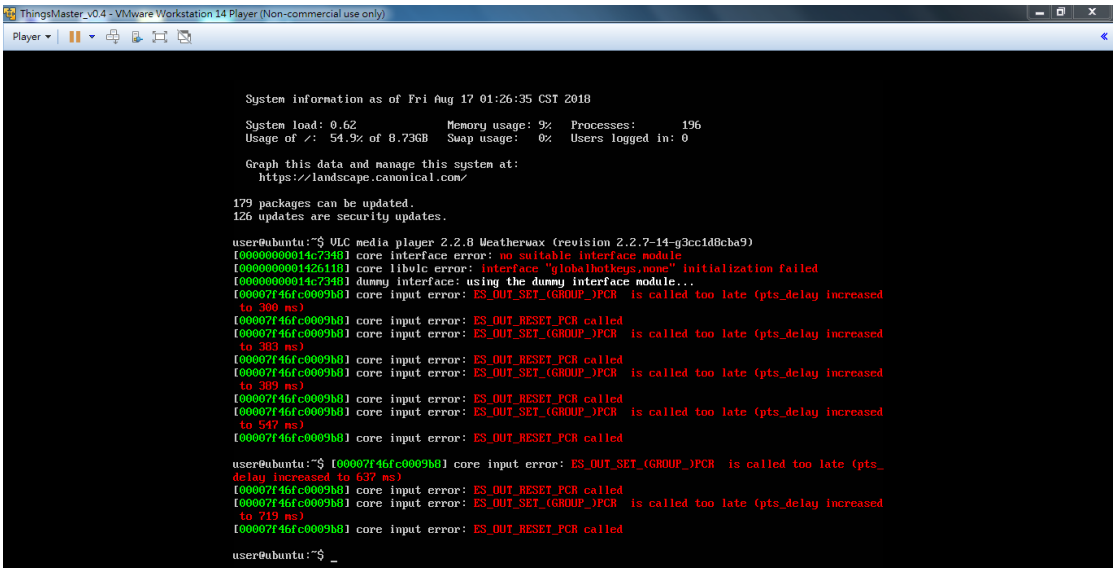
4. Configure network adapter of ThingsMaster VM to make sure that the laptop or the computer can ping the Virtual Machine.

- 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.



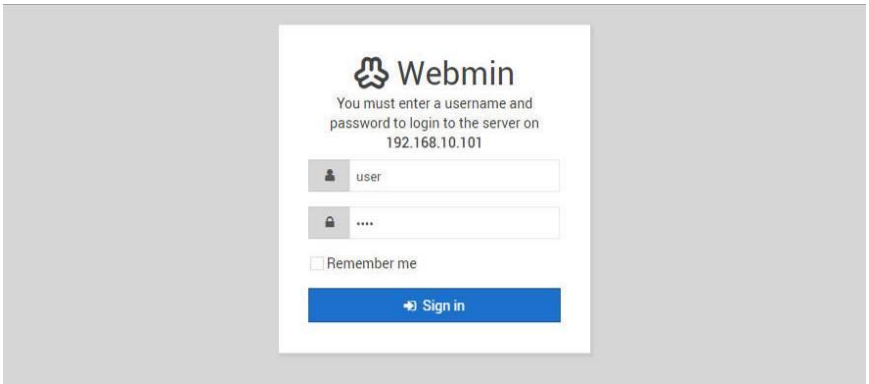
5. Start the Virtual Machine, wait till the starting process is done then the ThingsMaster is established.



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

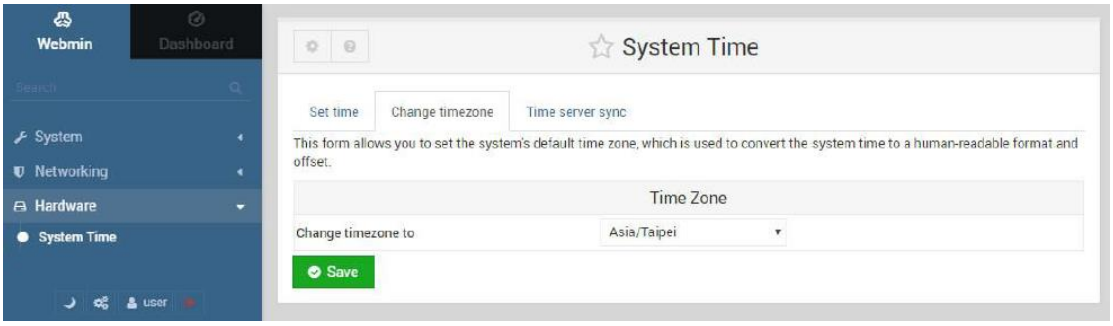
User Name/Password: user/user



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.

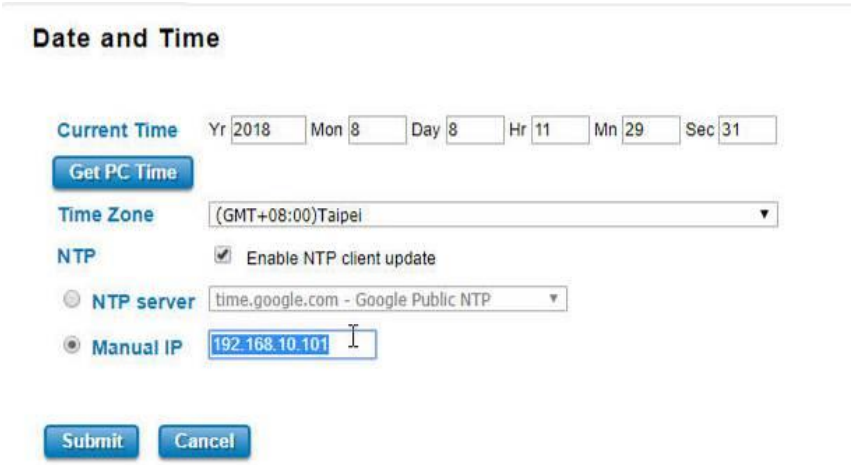
Please adjust the time and change time zone of the VM first. User can configure it from the Webmin interface. Go to Hardware -> System Time -> Set Time -> Change Time Zone



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.

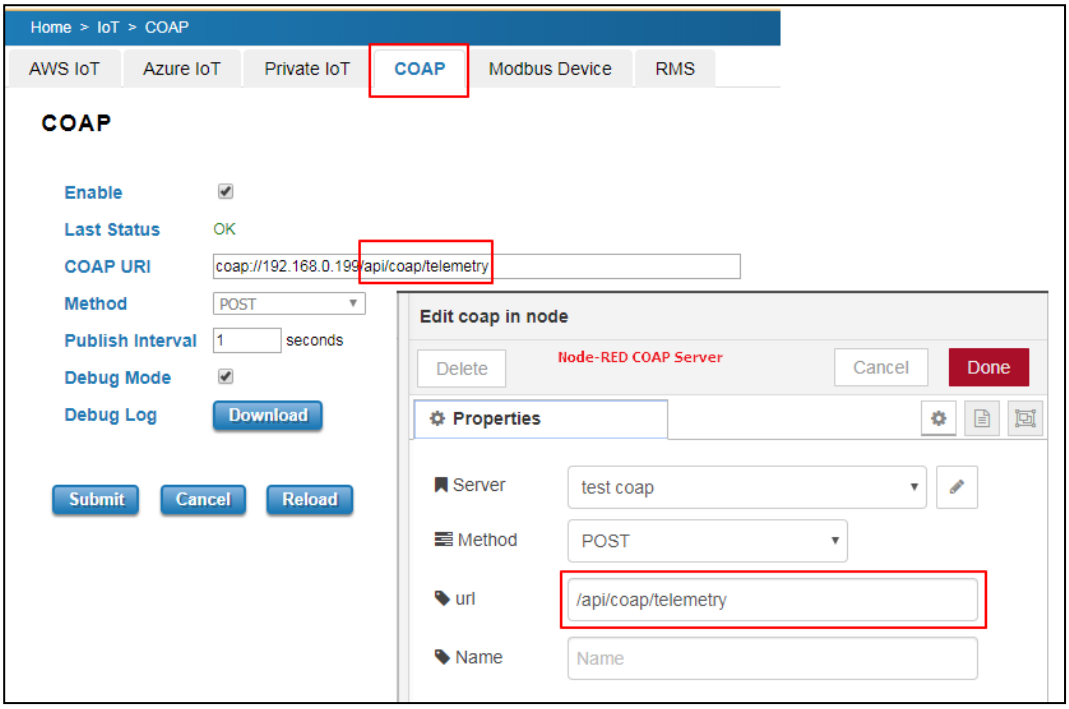
- Enable the NTP Client from the Web GUI -> choose the Manual IP -> enter the server IP Address (192.168.10.101)



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

3.12.2 CoAP

This page allows the user to configure the CoAP (**Constrained Application Protocol)** server settings.



The description of the columns is as below:

TERMS	DESCRIPTION
Enable	Check the box to enable the function.
Last Status	Shows the results of last update to CoAP server
COAP URI	Specify the URI (**U**niform **R**esource **L**ocator) address of CoAP server. The figure above show example configuration in WebGUI & NodeRed.
Method	Support “POST” method. Other methods can be supported by request.
Publish Interval	**Default: 10 (Seconds)** Specify the interval (in seconds) between each upload
Debug Mode	Check to enable debug mode for CoAP connection.
Debug Log	Download log for problem analysis between device and CoAP server

The following shows example of CoAP payload. Contact WoMaster salesperson for customized payload.

CoAP payload:

{ "modelname": "WR222-WLAN+LTE", "devicename": "router", "version": "1.1.1", "mac address": "94:66:e7:00:24:be", "serial number": "N/A", "IPADD": "192.168.10.22", "status": "normal" , "latitude": "25.034", "longitude": "121.5641" , "act": 2, "rssi": -75, "rscp": -79, "ecio": -12 , "di1":"0" , "lte_rx": 0.00 , "lte_tx": 0.00 , "lte_bytes":0, "CO2":1, "Temperature":2}

CoAP content-format: application/json

Key-value format:

Key is always a string, while value can be either string, Boolean, double or long.

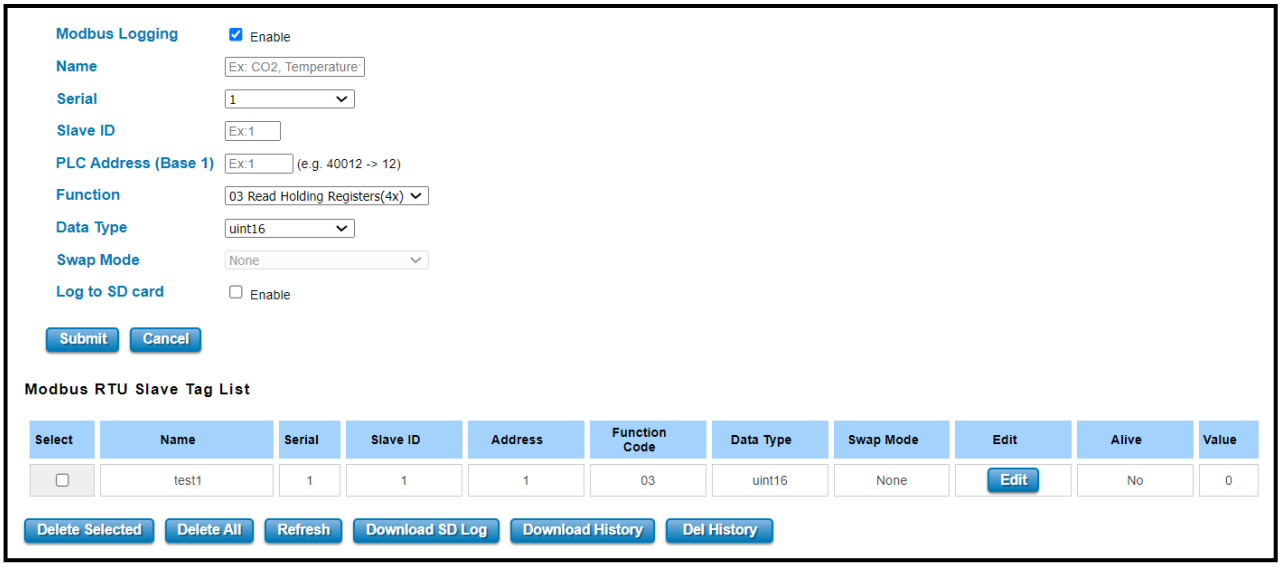
{"stringKey":"String1", "booleanKey":true, "doubleKey":10.0, "longKey":20}

3.12.3 Modbus Device

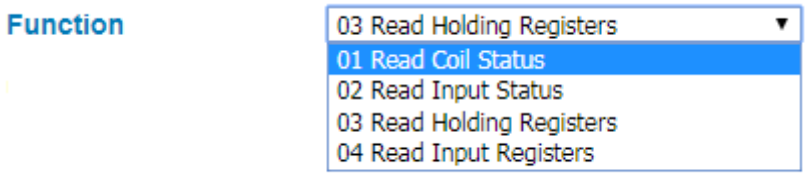
Modbus Logging

This page allows the user to configure the Modbus connection, so that the device will be connected to the device.

Any kind of sensor should have their own information please check their information.

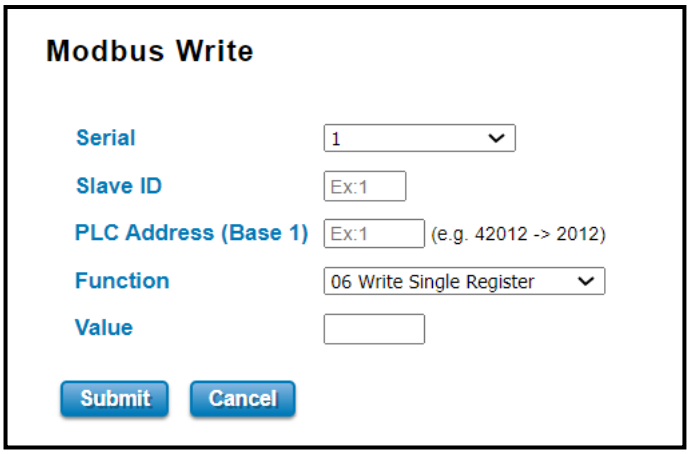


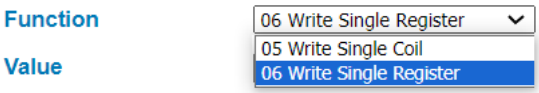
The description of the columns is as below:

TERMS	DESCRIPTION
Modbus Logging	Check the box to enable the function.
Name	Enter the Modbus name
Serial	Select the correct serial port.
Slave ID	Enter the Slave ID that belongs to the device
PLC Address	Enter the address that belongs to the device.
Function	
Data Type	**Default: Uint32** Select the Data Type
Swap mode	If need,select the swap mode:ABCD--->CDAB
Log to SD card	Save the log to SD card.
Alive	The Alive status of the target Protocol/PLC address of the connected sensor.
Value	The Value of the target Protocol/PLC address the router read from the sensor.

Modbus Write

This page provide the modbus write function.

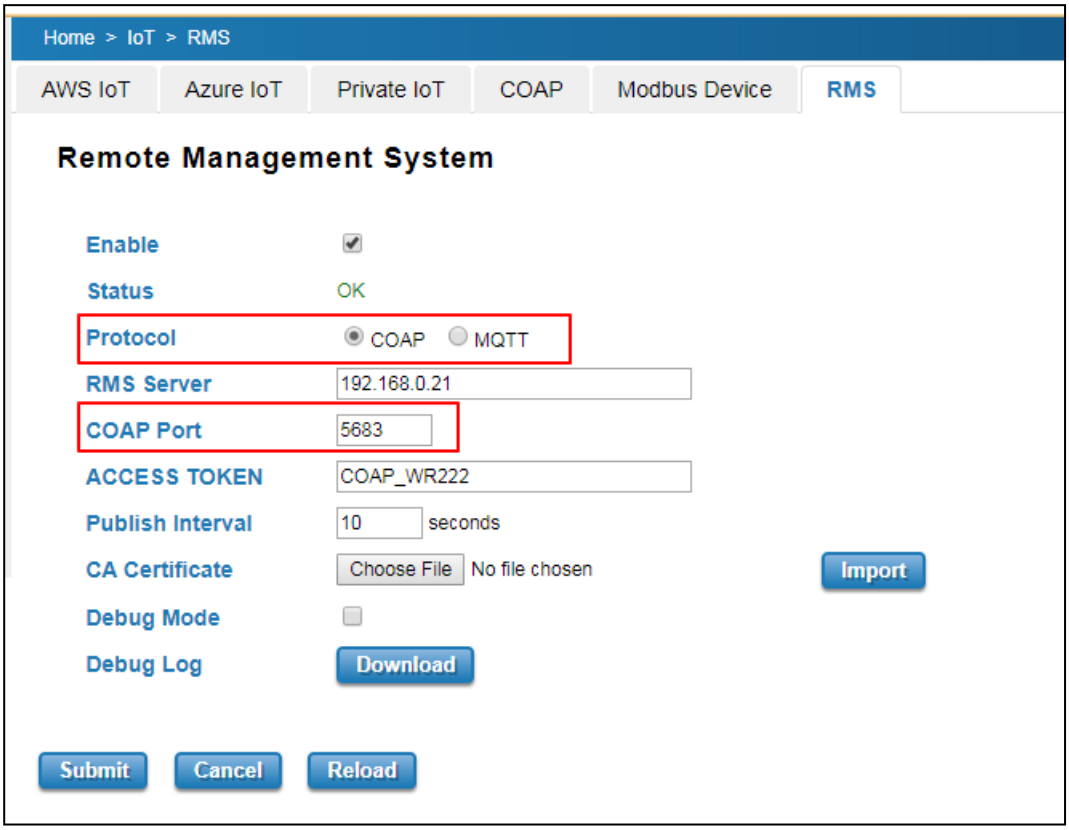


TERMS	DESCRIPTION
Serial	Select the correct serial port.
Slave ID	Enter the Slave ID that belongs to the device
PLC Address	Enter the address that belongs to the device.
Function	
value	Enter the value

Click Submit to apply the configuration

3.12.4 RMS/OTA

This page allows the user to configure the RMS (**R**emote **M**anagement **S**ystem) server. The page is used only for WoMaster ThingsMaster



The description of the columns is as below:

TERMS	DESCRIPTION
Enable	Check the box to enable the RMS function.
Status	Show the connection status between device and RMS server
Protocol	Select protocol for uploaded payload. CoAP and MQTT are supported. Contact WoMaster salesperson for other protocols.
RMS Server	Enter the RMS Server IP Address
CoAP Port	Specify connection port of selected upload protocol.
ACCESS TOKEN	Generate the token from ThingsMaster RMS; this access token is used to access the device by ThingsMaster Cloud.
Publish Interval	**Default: 10 (Seconds)** Specify the interval (in seconds) between each upload.
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 OTA v1.0.0 and later version.**
Debug Mode	Check to enable debug mode for CoAP connection.
Debug Log	Download log for problem analysis between device and CoAP server

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

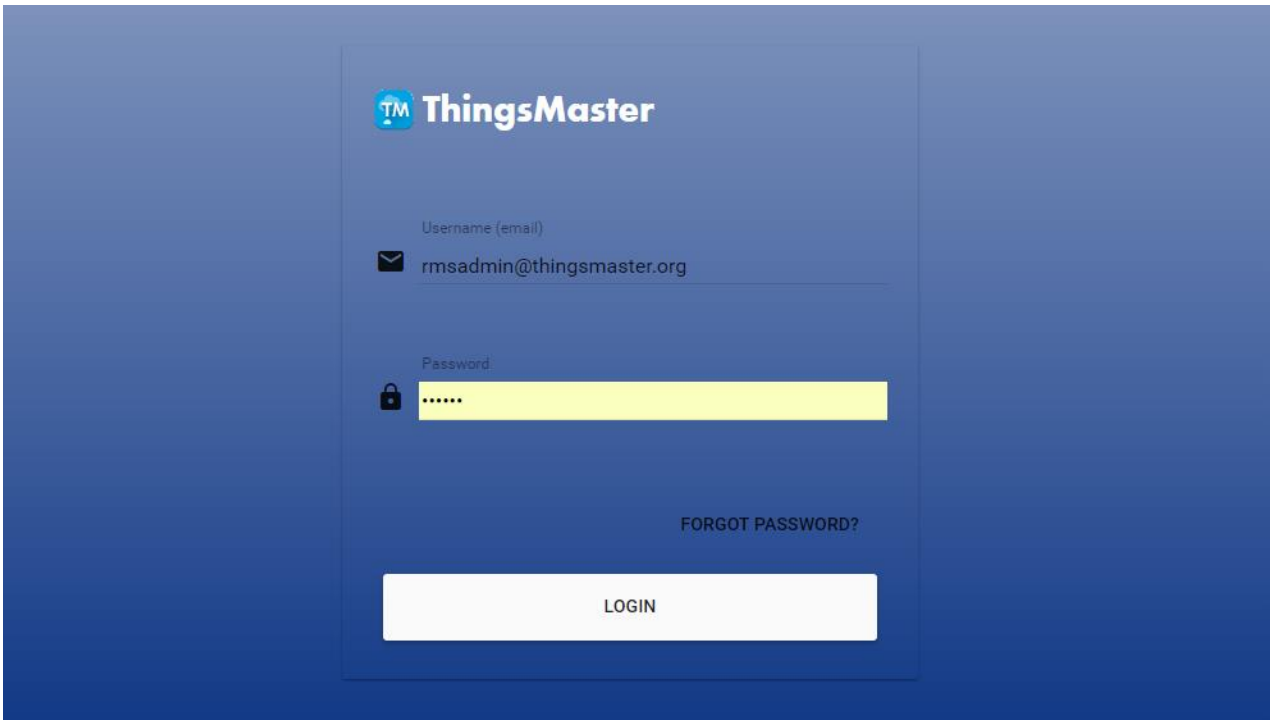
HOW TO ESTABLISH AND CONNECT TO THE THINGSMASTER RMS SERVER

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

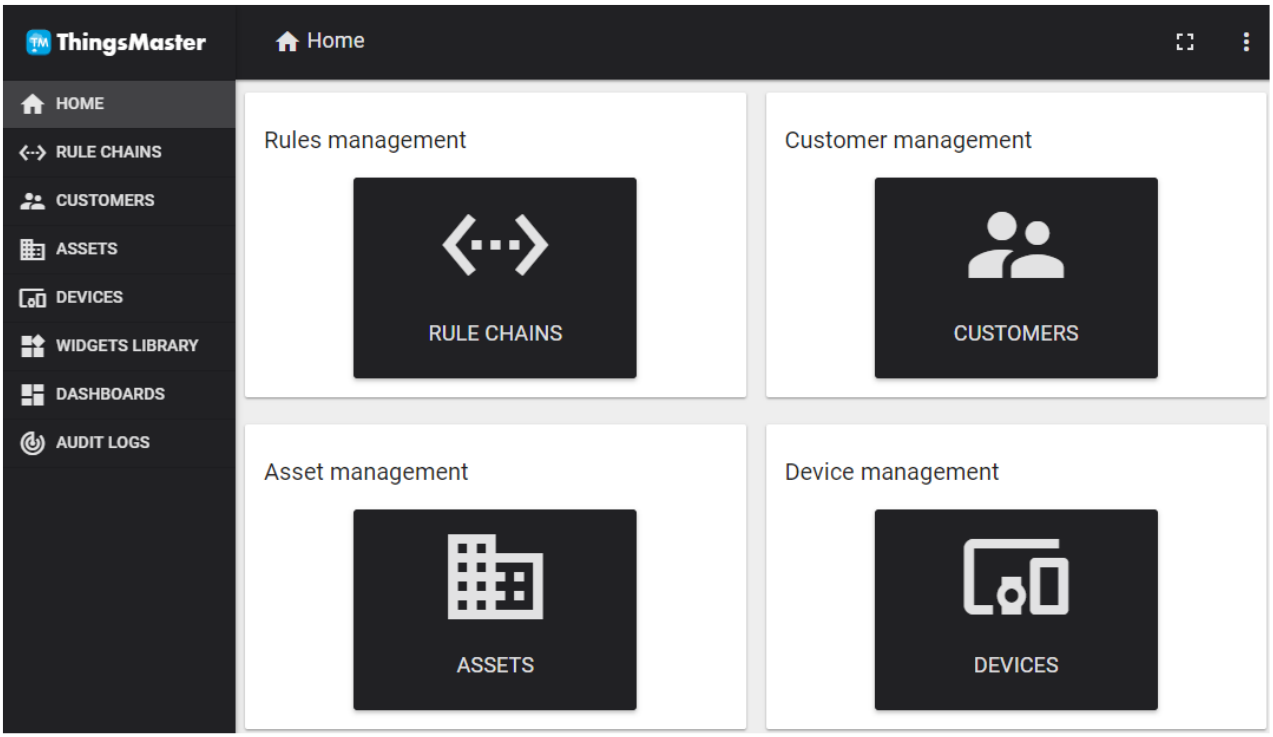
2. Login to ThingsMaster RMS, using RMS Account.

Login: <User RMS Account>

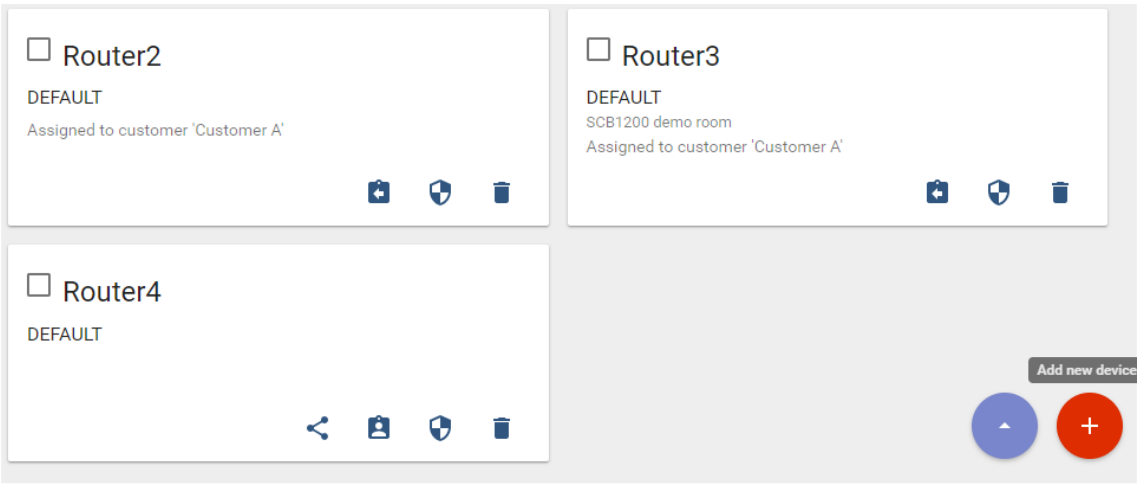
Password: <User RMS Password>



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

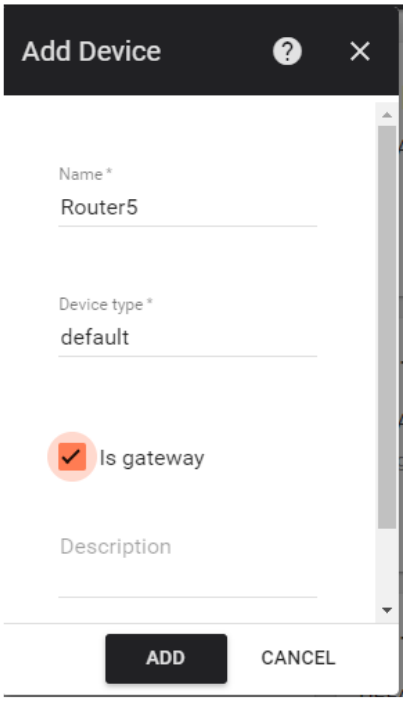


4. Add new device information, by clicking the “+” at the corner of the page.

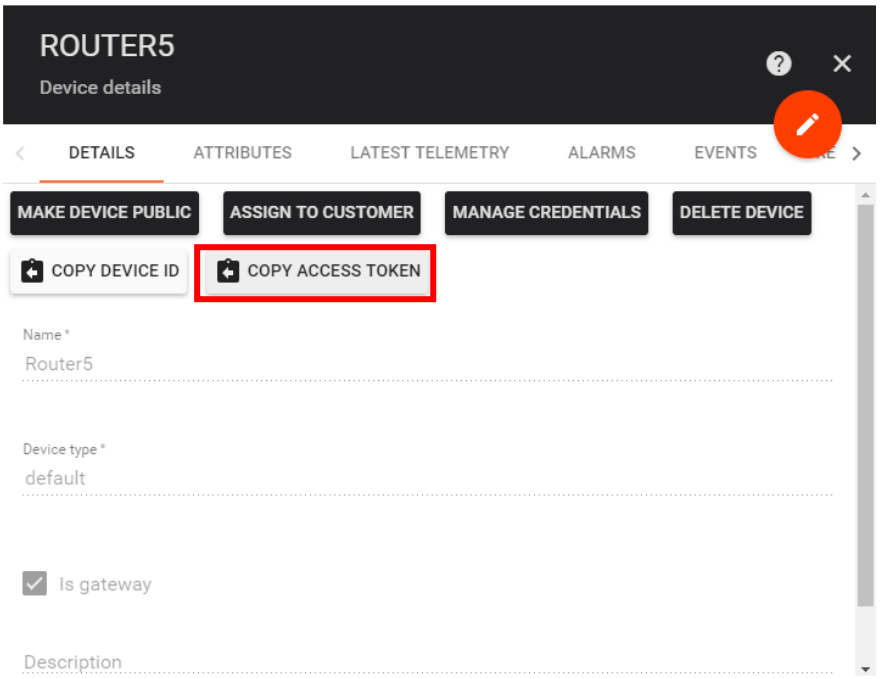


After click “+” menu then a page will pop up. Enter the device information.

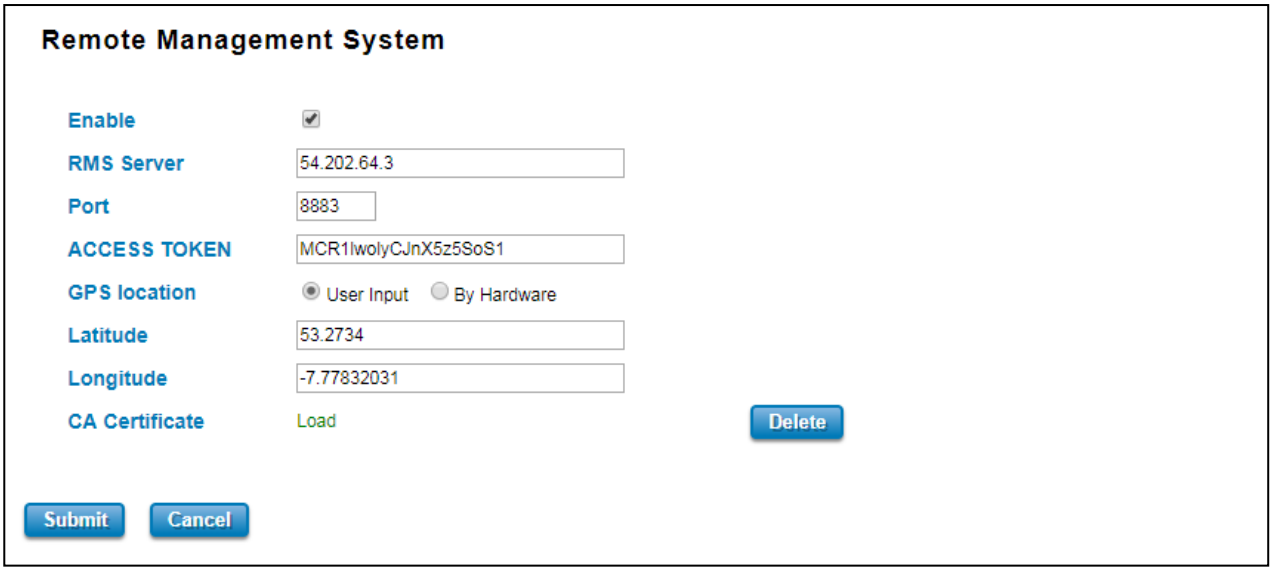
- Name: Please start the name with Router + Number.
- Device type: default
- Is gateway: check the box
- Click **Add**



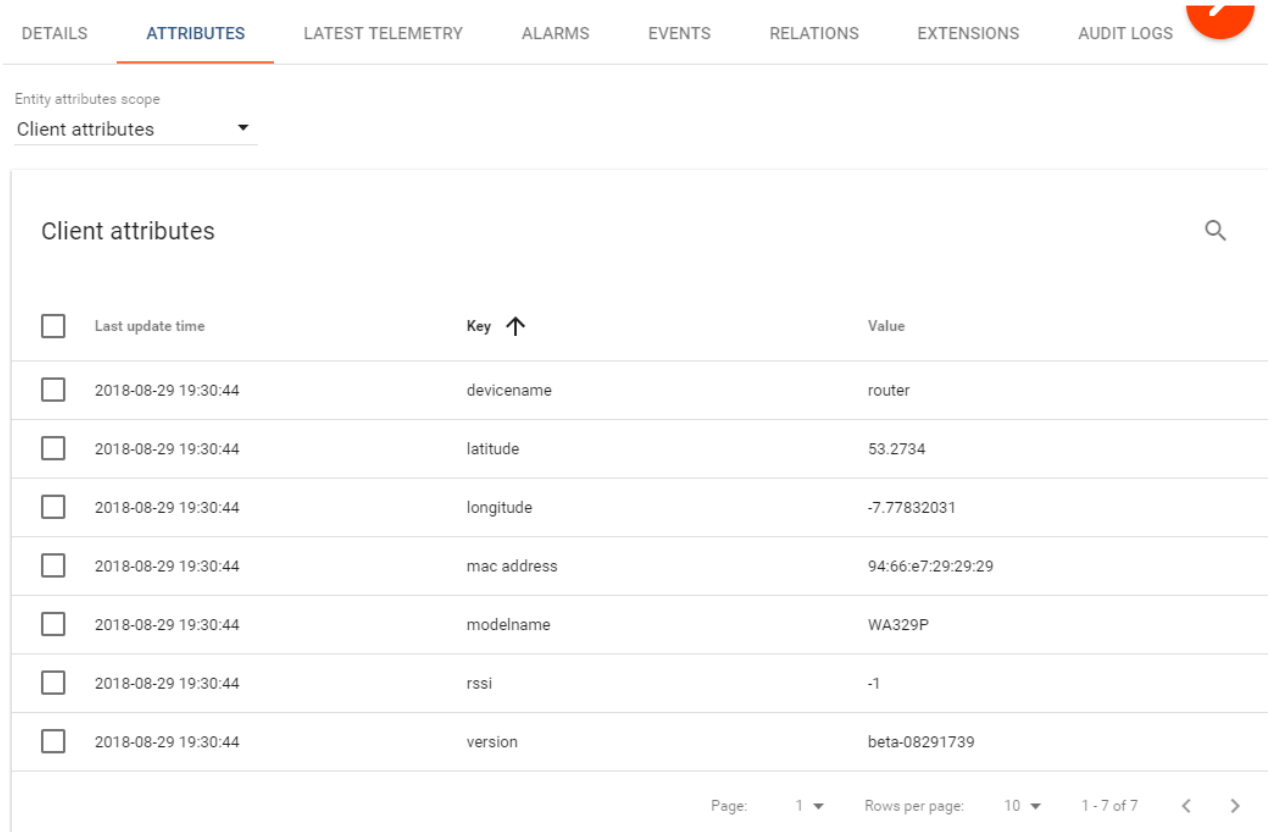
5. After the device is registered, then click on the device folder go to Details -> Click on Copy Access Token. This access token is code to link the device with the RMS Server.



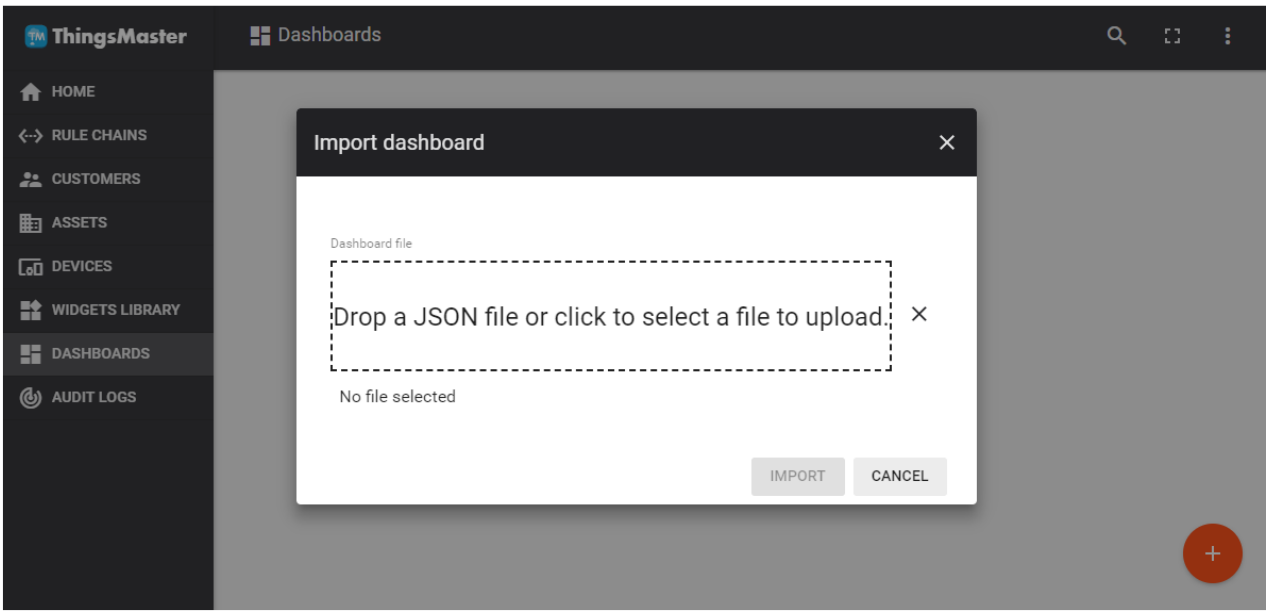
6. Go to the Web GUI -> IoT -> RMS. Paste the Access Token code to the Web GUI. And complete the configuration.



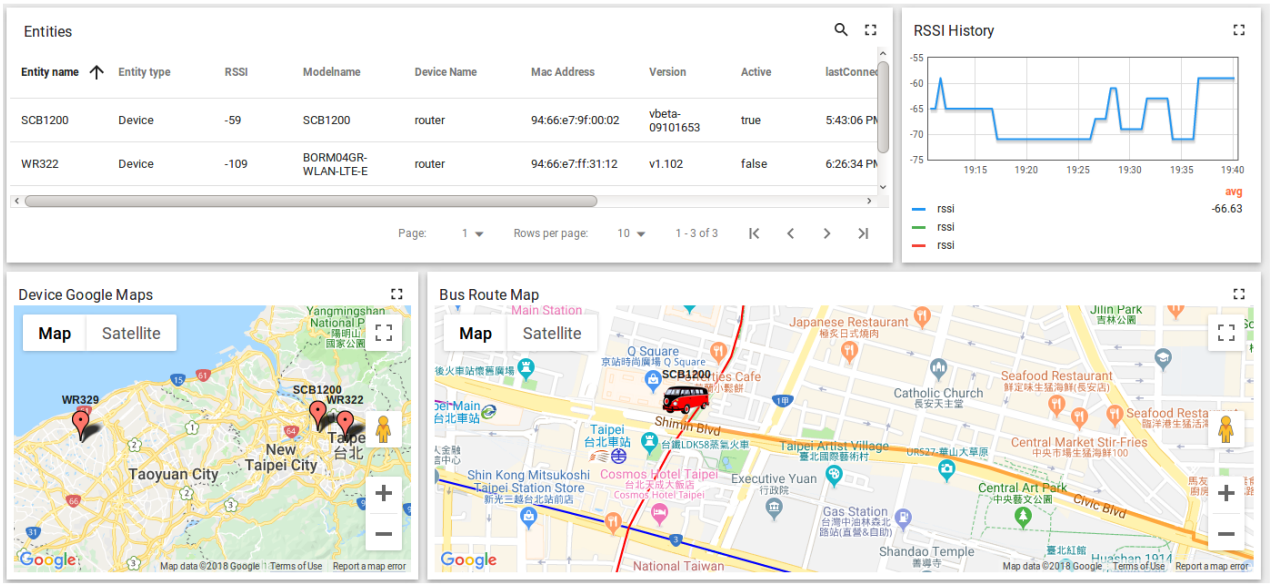
7. After the configuration is done then go back to ThingsMaster RMS Server. And then click on the newly added Router -> Attributes-> Client Attributes to see if the data has been uploaded.



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.

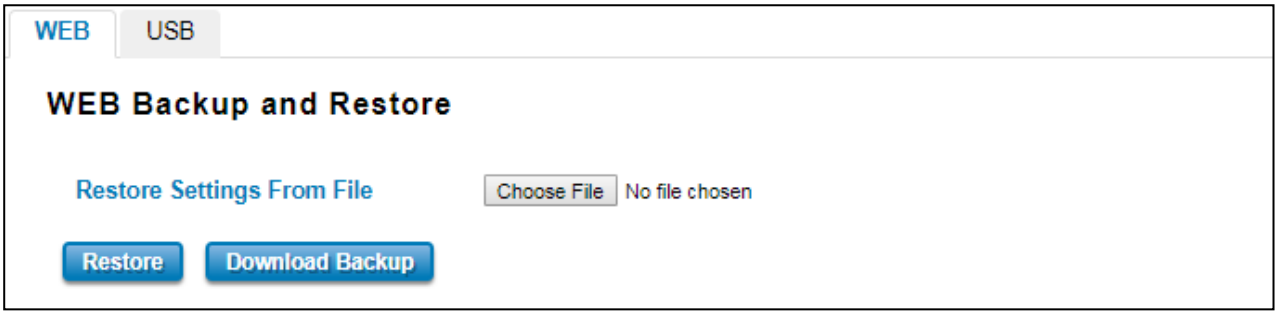


9. After the JSON file is uploaded, the dashboard will show as below:



3.13 BACKUP AND RESTORE

User can use WoMaster's Backup and Restore configuration to save and load configuration through the router. There are 2 modes for users to backup/restore the configuration file.



Web mode: In this mode, the router 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 router. This mode is only provided by Web UI while CLI is not supported. Also, this feature provides the Download Backup button in order to download the backup configuration from the router.

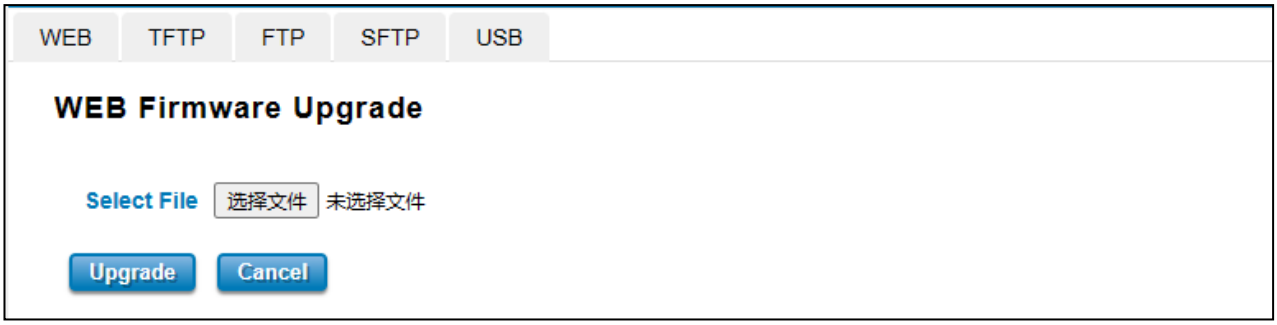
USB mode: this mode has two functions, Load Setting from File and Save Setting to USB. Load Setting from File, make sure that the USB has been inserted and it has the *.conf* file which is the backup files. After inserting the USB, the USB port will directly read the USB and then user needs to type the specific filename. Then click **Restore**. At the Save Setting to USB part, all of the configuration settings would be saved to the USB, with *.conf* as the file type by clicking the **Backup button**.

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 provides the release notes for the update as well. For technical viewpoint, WoMaster suggests user uses the latest firmware before installing the router to the customer site.

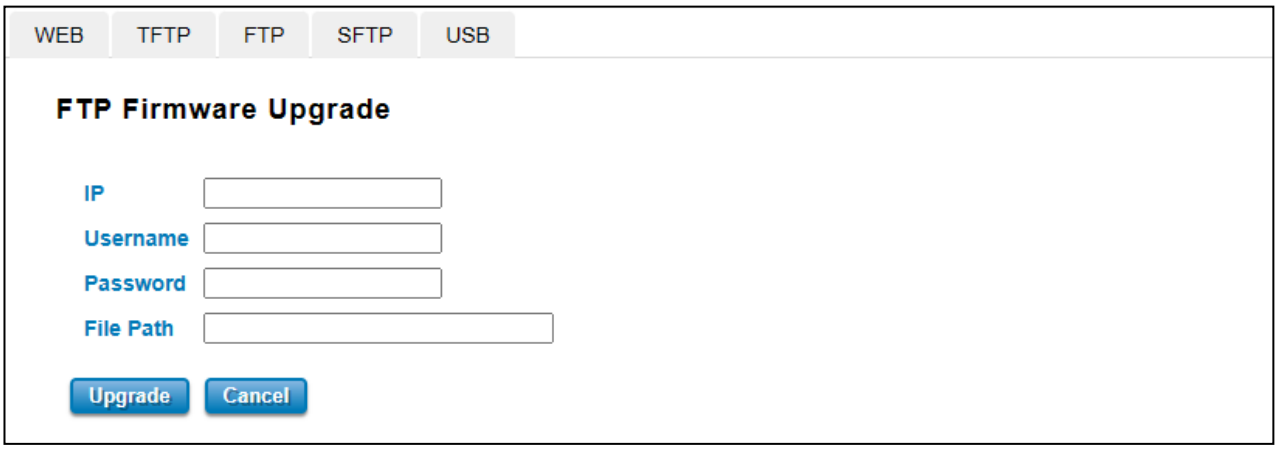
> **NOTE:** Note that the system will be automatically rebooted after User finished upgrading the new firmware. Please remind the attached network users before User performs this function.

There are 5 modes for users to backup/restore the configuration file.

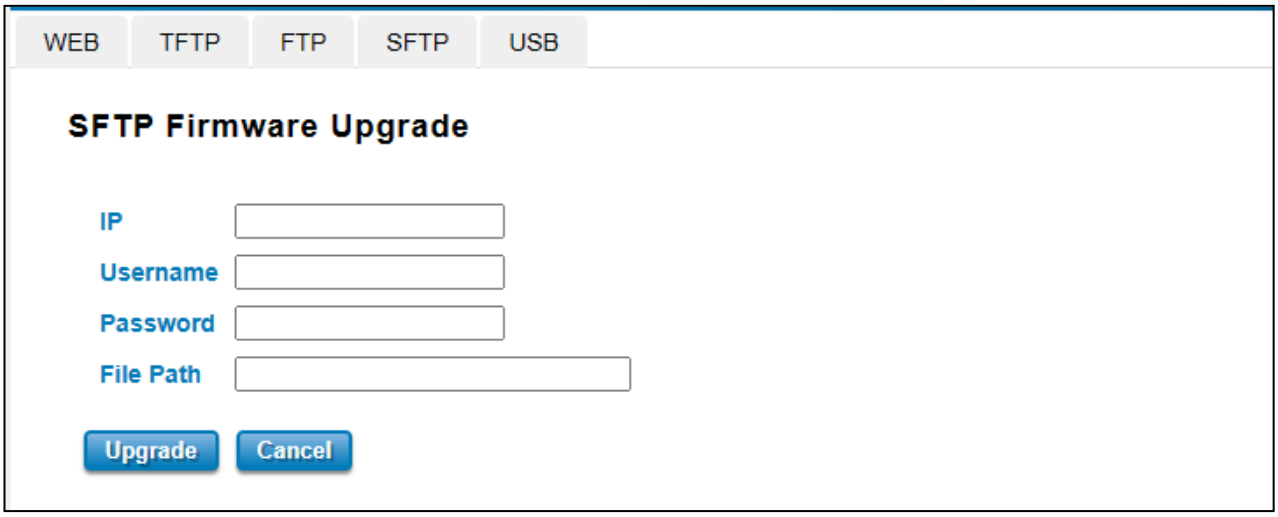


Web mode: The router acts as the file server. Users can browse the target folder and then type the file name to back-up the configuration. Users also can browse the target folder and select the existed upgrade file. This mode is only provided by Web UI while CLI is not supported.

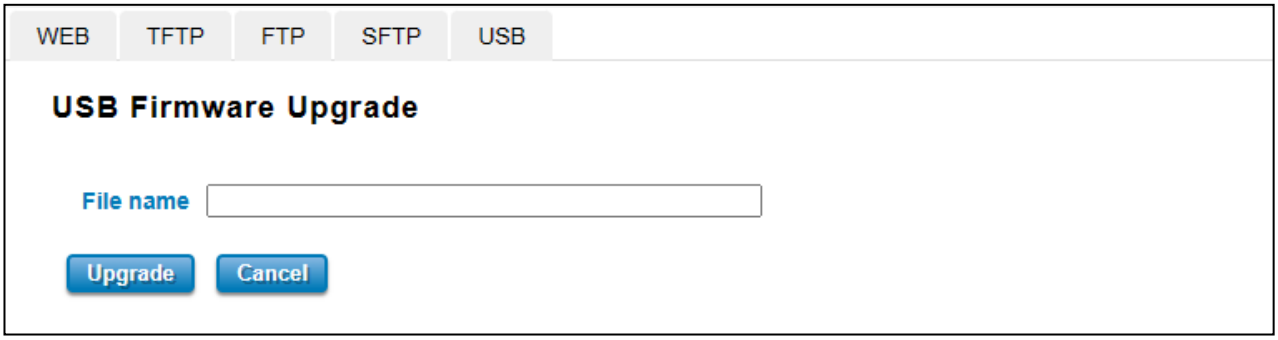
TFTP mode: After configuring the TFTP IP and Firmware file name, Then click **Upgrade**.



FTP mode: After configuring the FTP IP, Username, Password and File Path, Then click **Upgrade**.



SFTP mode: After configuring the SFTP IP, Username, Password and File Path, Then click **Upgrade**.

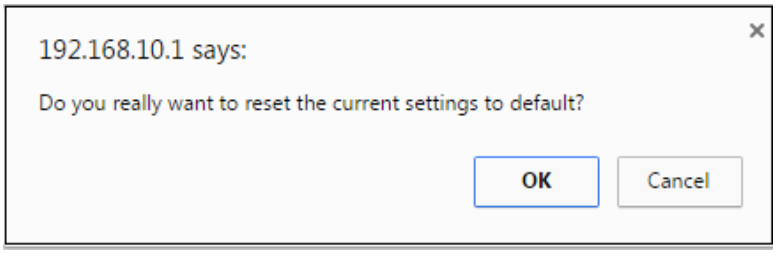


USB mode: plugged the USB device with the firmware file, then type the specific filename of the new firmware file. Then click **Upgrade**.

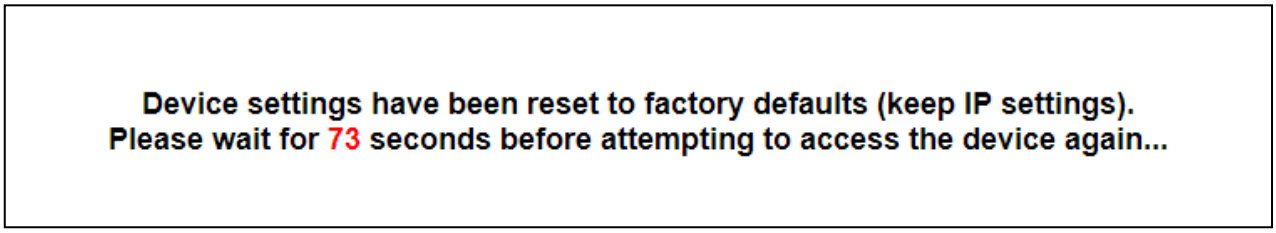
3.15 RESET TO DEFAULTS

This function provides users with a quick way of restoring the WoMaster router's configuration to factory defaults. By check the Restore Factory default IP setting, it means the IP of the device will directly change to the default IP (192.168.10.1).

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

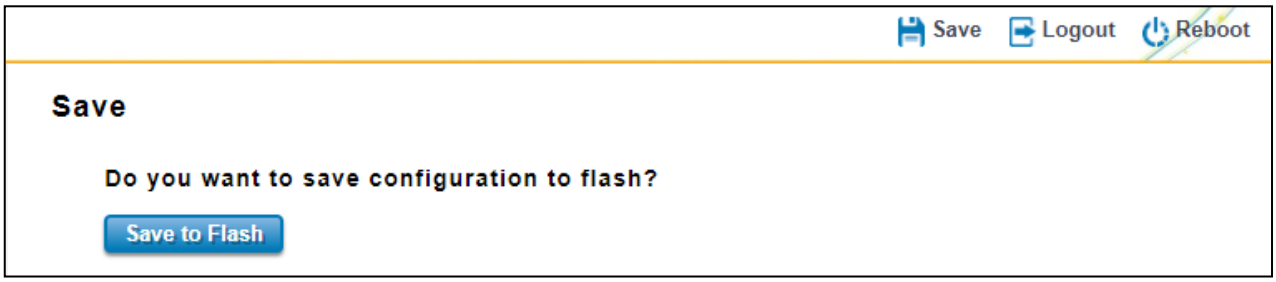


Below is the interface for resetting the device with keep the IP Settings.



3.16 SAVE

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



3.17 LOGOUT

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

3.18 REBOOT

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

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

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

3.19 WOMASTER MIB

WoMaster supports Public MIB and also provides Private MIBs for users to configure or monitor the device's configuration by SNMP. WoMaster provides Private MIB to meet up the need. The Private MIB can be found in or downloaded from WoMaster Web site (www.womaster.eu). Compile the private MIB file by SNMP tool or using WoMaster NMS, NetMaster.

Below is the Public MIB for the WoMaster Router products:

- **Bridge-MIB (RFC1493)**
- **Entity MIB (RFC4133)**
- **MIB-II (RFC1213)**

The table below is the Private MIBs and the supported model:

• WOMASTER-SWITCH-MIB • WOMASTER-POE-MIB	DP310/DS310 DP612/DS612 DS409 DP412/DS412 MP310 MP614
• WOMASTER-ROUTER-MIB • WOMASTER-SERIAL-MIB (by Hardware) • WOMASTER-CELLULAR-MIB (by Hardware) • WOMASTER-GPS-MIB (by Hardware)	SCB1000/SCB1200 WR312/WR322 WR316 DS306 WR329

4. REVISION HISTORY

Version	Description	Date	Editor
V3.0	1st released WR312G-LTE/WR322GR-2xLTE User Manual Modify from previous user manual of the WR322-2C V2.0.	2023/11/14	Orwell, Jerry, Ann
V3.1	Update Web GUI and Description: System information， Date and time， Port Forwarding， SMS Alert, SYS Remote Reboot -> SMS Remote Control, NAT Settings， IPSec Setting，PING WATCHDOG， SYSLOG SETTING， SNMP， Tcpdump， FIRMWARE UPGRADE	2024/03/28	Orwell, Jerry, Ann
	-		
	-		
	-		
	-		

APPENDIX

ENTITY MIB (RFC4133)

Object Group Name		Object Identifier	Access	Value
entPhysicalTable		1.3.6.1.2.1.47.1.1.1		
	entPhysicalIndex	1.3.6.1.2.1.47.1.1.1.1.1	Not-accessible	
	entPhysicalDescr	1.3.6.1.2.1.47.1.1.1.1.2	Read Only	Industrial Secure Cellular Router, 2GbE+2COM, 802.11ac/n WLAN, LTE-E, RSIM, GPS, FDD B1/3/5/7/8/20, TDD B38/40/41
	entPhysicalVendorType	1.3.6.1.2.1.47.1.1.1.1.3	Read Only	1.3.6.1.4.1.47114.1.1
	entPhysicalContainedIn	1.3.6.1.2.1.47.1.1.1.1.4	Read Only	0
	entPhysicalClass	1.3.6.1.2.1.47.1.1.1.1.5	Read Only	other(1)
	entPhysicalParentRelPos	1.3.6.1.2.1.47.1.1.1.1.6	Read Only	0
	entPhysicalName	1.3.6.1.2.1.47.1.1.1.1.7	Read Only	router
	entPhysicalHardwareRev	1.3.6.1.2.1.47.1.1.1.1.8	Read Only	v1.0
	entPhysicalFirmwareRev	1.3.6.1.2.1.47.1.1.1.1.9	Read Only	v1.2.3
	entPhysicalSoftwareRev	1.3.6.1.2.1.47.1.1.1.1.10	Read Only	v1.2.3
	entPhysicalMfgName	1.3.6.1.2.1.47.1.1.1.1.12	Read Only	WoMaster
	entPhysicalModelName	1.3.6.1.2.1.47.1.1.1.1.13	Read Only	WR322G-WLAN+LTE-E
	entPhysicalIsFRU	1.3.6.1.2.1.47.1.1.1.1.16	Read Only	False(2)
	entPhysicalMfgDate	1.3.6.1.2.1.47.1.1.1.1.17	Read Only	
entLastChangeTime		1.3.6.1.2.1.47.1.4.1	Read Only	

MIB-II (RFC1213)

Object Group Name		Object Identifier	Access	Value
System				
	sysDescr	1.3.6.1.2.1.1.1	Read Only	Industrial Secure Cellular Router, 2GbE+2COM, 802.11ac/n WLAN, LTE-E, GPS, 2SIM, FDD B1/3/5/7/8/20, TDD B38/40/41
	sysObjectID	1.3.6.1.2.1.1.2	Read Only	switch
	sysUpTime	1.3.6.1.2.1.1.3	Read Only	5 minutes 22 seconds (32200)
	sysContact	1.3.6.1.2.1.1.4	Read Only	0
	sysName	1.3.6.1.2.1.1.5	Read Only	WR322GR-WLAN+LTE-E
	sysLocation	1.3.6.1.2.1.1.6	Read Only	Unknown
	sysServices	1.3.6.1.2.1.1.7	Read Only	2
at		1.3.6.1.2.1.3		
atTable		1.3.6.1.2.1.3.1		
	atIfIndex	1.3.6.1.2.1.3.1.1.1	Read Only	8
	atPhysAddress	1.3.6.1.2.1.3.1.1.2	Read Only	00-99-99-99-99-99
	atNetAddress	1.3.6.1.2.1.3.1.1.3	Read Only	192.168.10.2