WoMaster

User Manual

WA212BP

Outdoor Waterproof Long Range Wireless AP

July. 2020 V.1.0

WOM ASIA Co., Ltd
4F., No.86-2, Yiwen 1st St., Taoyuan Dist., Taoyuan 330, Taiwan

www.womaster.eu

WoMaster

WA212BP

Industrial Compact LTE/Wi-Fi Router

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

WA212BP is a high performance, 802.11n compliant, IP55 waterproof outdoor wireless AP/ Router with wireless coverage reaching up to 2km. It equips with highly sensitive, high power, and high gain 2T2R MIMO antennas that bring data rate up to 300Mbps. The dual Ethernet ports support NAT Routing and firewall/VPN connectivity. One Ethernet port receives PoE power input, and the other Ethernet port delivers PoE power output. A web-based GUI provides easy and secure management, as well as the firmware upgrade. The mini USB port can be used to add cellular dongles. WA212BP is an ideal entry-level high-speed long-range wireless communication solution for outdoor applications.

Model Name	Description
WA212BP-E	Industrial Wireless 802.11n AP/Client/Bridge,IP55, Embedded 11dBi antenna, 2 Ethernet ports, 24V Passive PoE with EU plug
WA212BP-U	Industrial Wireless 802.11n AP/Client/Bridge,IP55, Embedded 11dBi antenna, 2 Ethernet ports, 24V Passive PoE with US plug

1.2 Major Features

Below are the major features of WA212BP

High Throughput and Extended Range Wireless Communication

- Compliant with IEEE 802.11n with 2T2R MIMO and data rate up to 300Mbps
- Long wireless transmission distance up to 2 km
- Dual Ethernet wire connection allows to expand the wireless range without bandwidth lost.
- PoE pass-through to deliver power for AP or IP cam

High power, High gain, and Smart RF management

- External Power Amplify reaches Max. 29dBm output power and -96dBm Rx sensitivity
- Directional High-Gain 11dBi Panel Antenna Inside
- Optional 5G Radio with external antenna socket
- Supports AP, Client, WDS AP/Client, multiple SSID for Point to Point/Multiple Points connectivity

Easy and WLAN Secure management

- TTPs/ SNMP v3/ CLI management
- Built-in WPA, WPA2/ 802.1X/ Firewall security
- Multiple operating modes: Wireless AP/Client/Bridge for different applications

Dual Ethernet Routing with Enhanced Cyber Security

- Dual Ethernet port supports one LAN port, one WAN port Router mode or Bridge mode.
- NAT, Firewall, VPN is available in Router mode.
- 1:1 NAT, port forwarding and NAPT for local traffic protection
- Support Firewall for inbound/outbound traffic, port forwaring
- OpenVPN Server/Client
- Support L2TP with PPP, PAP, CHAP(LCP, IPCP)
- Support GRE tunnel
- HTTPs/SSH secure login
- Support TACACS+ multi-user authentication for privileged user management

Industrial IoT LAN & Cloud Management

- ARP response over 802.2 LLC SNAP
- Support MQTTS, CoAP protocol, ready to use AWS/Azure and Private Cloud Agent for cloud management
- Diagnostic tool includes Ping, TFTP, SNMP Trap, E-mail Alert and System Log
- WoMaster Software Utilities

Rugged Design for Wayside installation

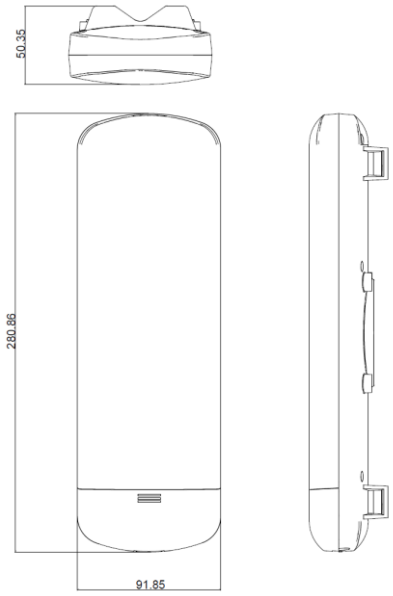
- Outdoor waterproof IP55 enclosure
- -30~60°C operating temp. & 24V PoE input
- Easy Pole mount installation for wayside, Port, Airport, Factory & Building applications

2. Installation

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

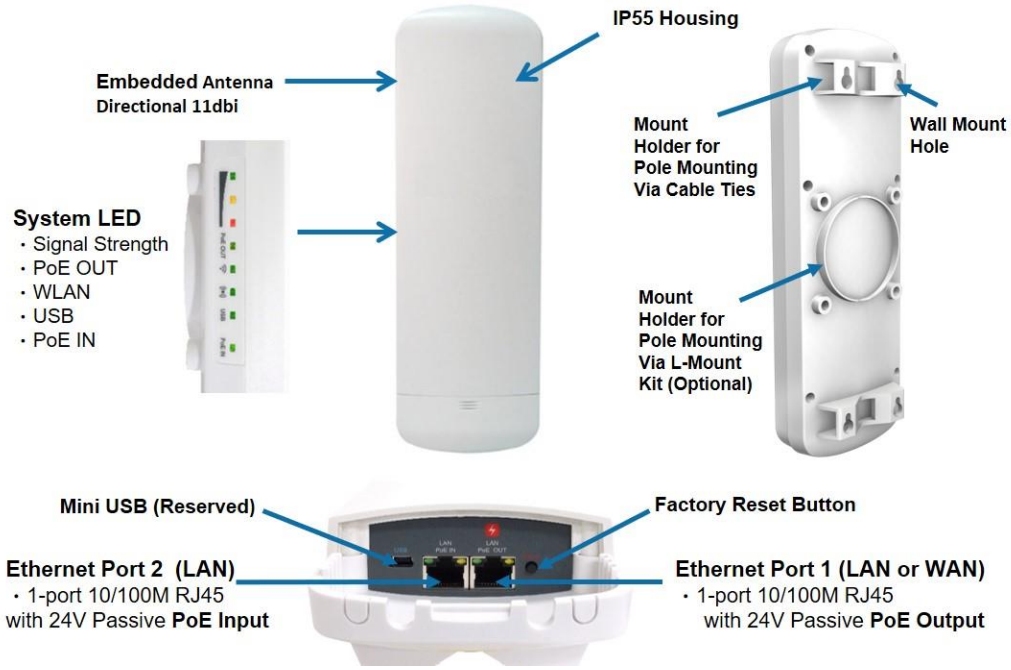
2.1 Dimension

Dimensions of WA212BP: 280.86 x 91.85 x 50.35mm (D x W x H)



Interfaces

The interfaces from WA212BP AP include 2 Ethernet ports with passive PoE 24V (10/100 Base-TX, RJ45, Router Mode: 1 WAN + 1 LAN, Bridge Mode: 2 LAN), System LED, 1 x Mini USB (Reserved by request), Embedded 11dBi Directional Antenna.



2.2 Package List

Standard package includes:

1x Product Unit
1x 24VDC PoE Injector
2x Power cord (EU or US)
2x UV Resistant Nylon Cable Tie for Pole Mounting
1x Quick Installation Guide

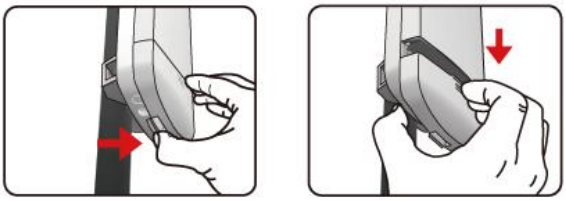
Optional accessory: 1 x Adjustment L-Mount kits for Pole Mounting

2.3 Interface Installation

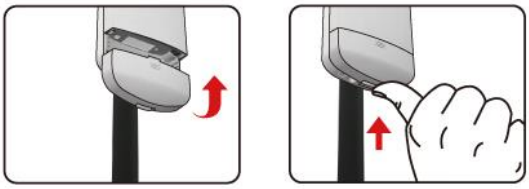
After unpacking the box, follow the steps below in order to properly connect the device. For better Wi-Fi performance, put the device in a clearly visible spot, as obstacles such as walls and doors hinder the signal. If you are using two AP to build a network, make sure that two AP are placed face to face.

Establish the connection

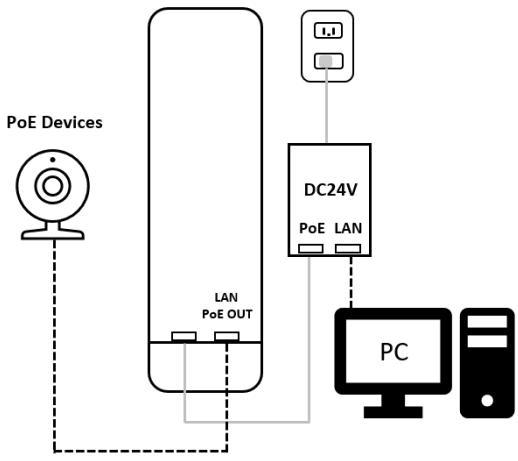
1. The bottom of the AP is a movable cover. Grab the cover and pull it back harder to take it out.



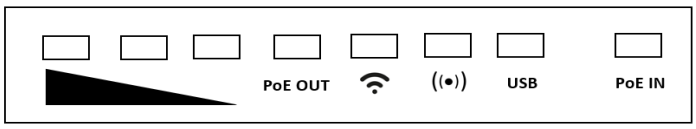
2. Plug a standard Ethernet cable into the **RJ45 PoE IN LAN port**
3. Slide the cover back and press down the lock button to seal the bottom of the Access Point.



4. Connect power cord to the PoE injector.
5. Install Ethernet cable between PoE IN LAN port of AP and PoE port of PoE injector.
6. Connect the power plug to a power socket. The Access Point will be powered up immediately.
7. Install Ethernet cable between LAN port of PoE injector and PC/NB, **whenever proceeding WebGUI configuration.**
8. Plug Ethernet cable into **PoE OUT LAN port**, if you need to connect a PoE device.



2.4 LED Indication



LED	Status	Description
Signal Strength	Green	Excellent
	Yellow	Good
	Red	Weak
PoE OUT	Green On	Link Established
	Off	Link is inactive
WLAN	Green On	WLAN enabled
	Green Blinking	Packets transmitting/receiving
	Off	WLAN disabled
((•))	-	Reserve
USB	-	Reserve
PoE IN	Green On	Link Established
	Off	Link is inactive

2.5 Mounting

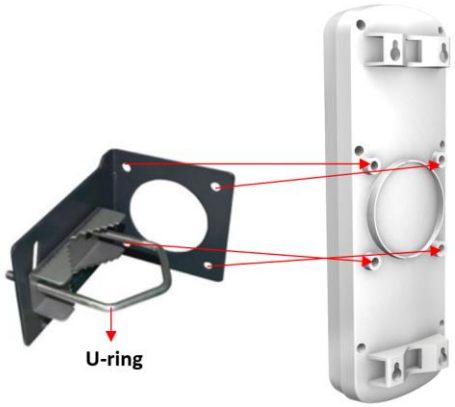
Pole mounting by cable tie

1. Place cable ties through the slots on back of AP.
2. Adjust the direction of AP for the best signal.
3. Attach the cable tie tightly to the pole and ensure AP will not fall.

Pole mounting by L-mount kits (optional)

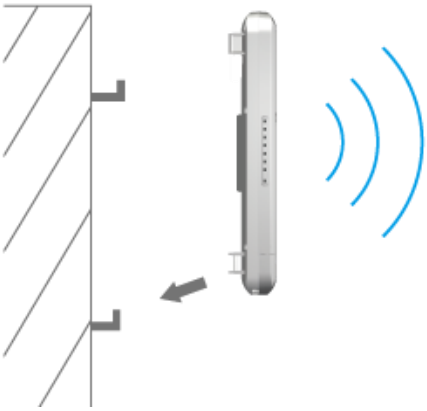
1. Use 4 screws to assemble the L-shaped mounting bracket on the back of the AP.
2. Attach the AP on the pole by using U-ring.
3. You can adjust the angle of AP up and down 45 degrees.

Note: U-ring can be attached to a pole with diameter less than 70mm.



Wall mounting

There are four wall mount holes on the back of AP, hang the AP on wall through it.



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.

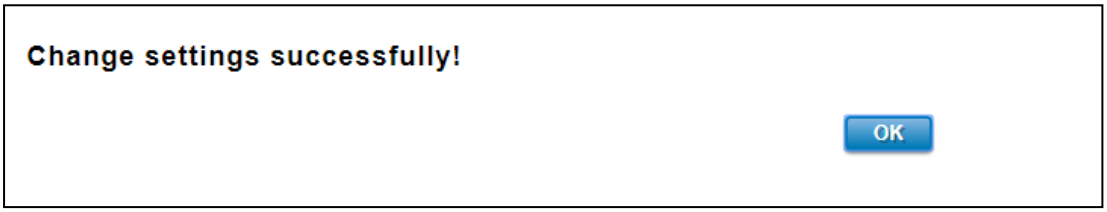
PREPARATION FOR WEB INTERFACE MANAGEMENT

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

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. Default user name: **admin** and password: **admin**. Then click **Login**.
8. After user clicks 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.

In this Web management for Featured Configuration, user will see all of WoMaster 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

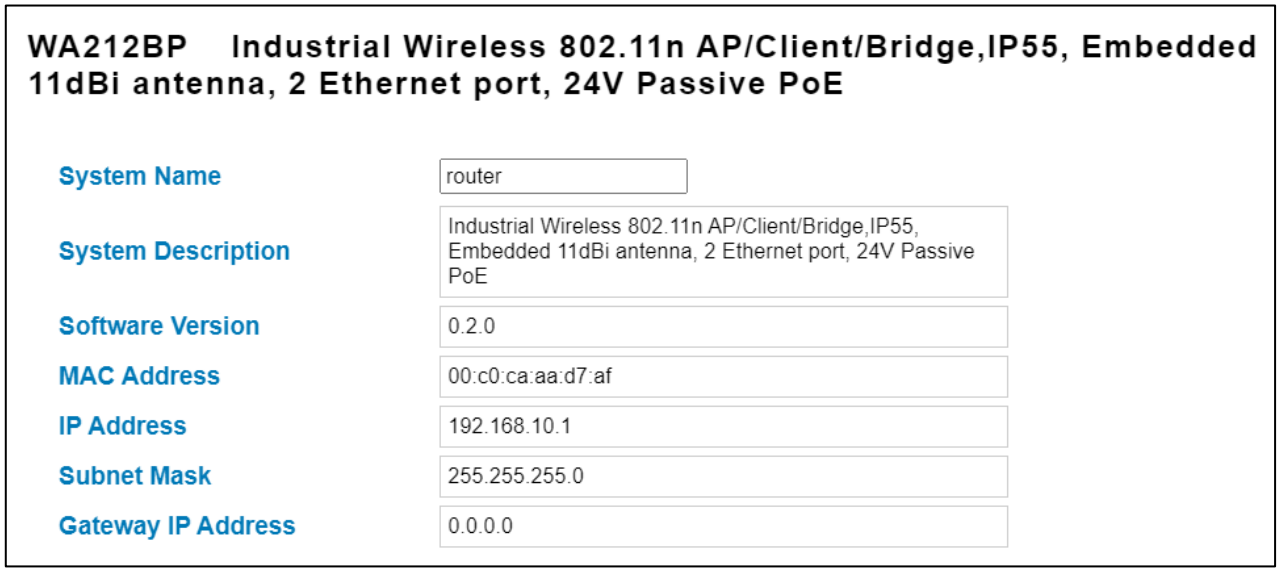
3.1.3 Network IP

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.

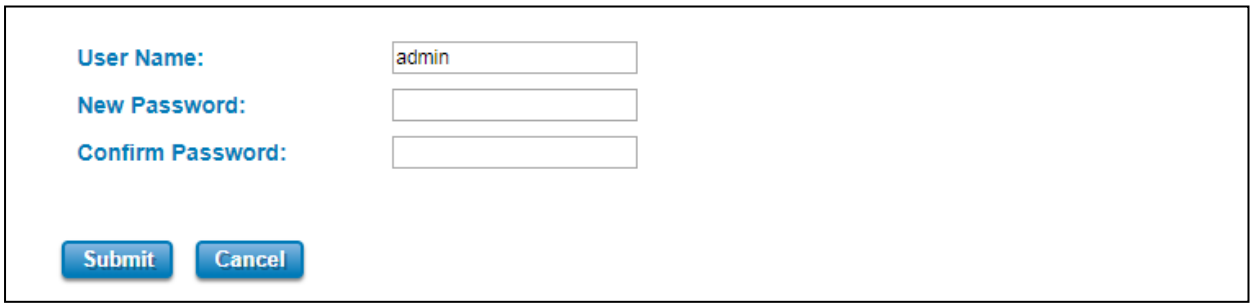


The description of the Information's interface is as below:

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

3.1.2 Login Setting

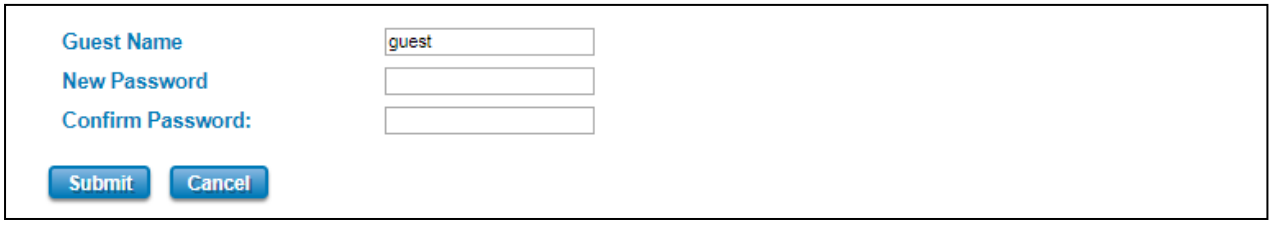
WoMaster' router supports Login Setting that has several authentication methods. It is supported with TACACS+, Radius, and Multi-User Authentication. This Login Setting consists of two level, admin and guest. Where the admin level, it has the privilege to read and write and for the guest level the privilege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

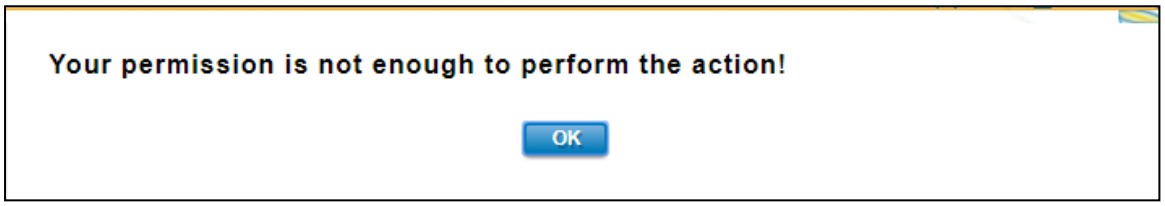
The Login Setting interface describes how to configure the system username and password for the web management login. To change the Name and Password, user just needs to input a new Name and New Password then confirm the new password in this section. Try to re-login with the new User Name and Password.

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.

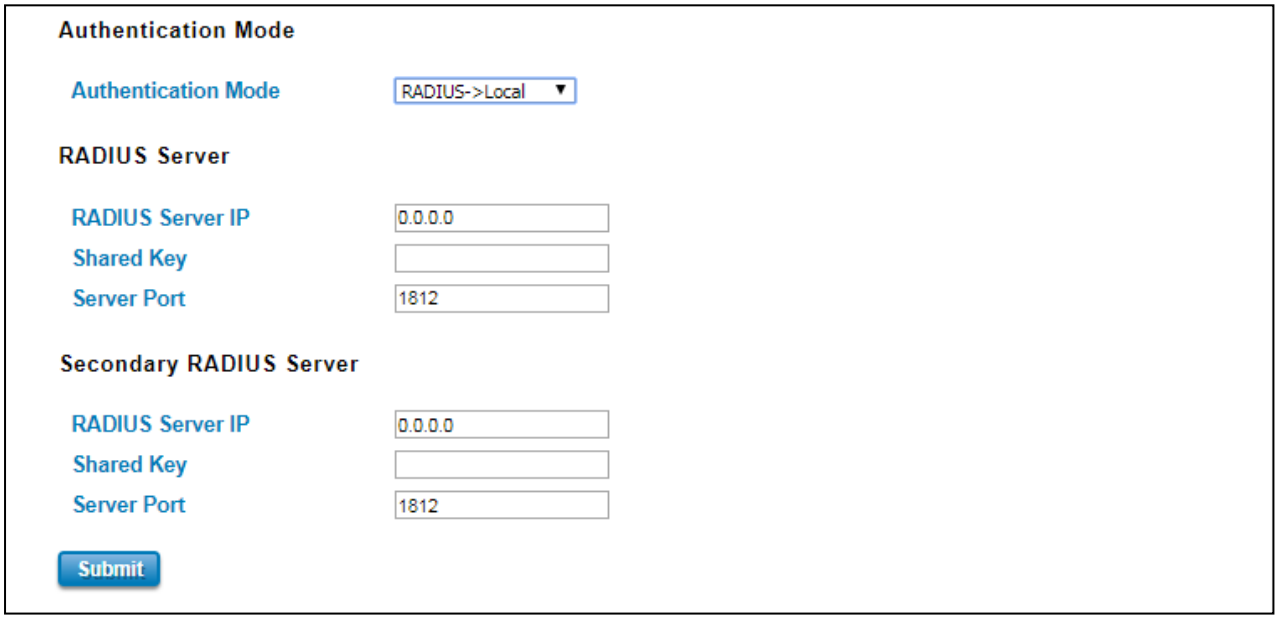
User Authentication Mode

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.



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

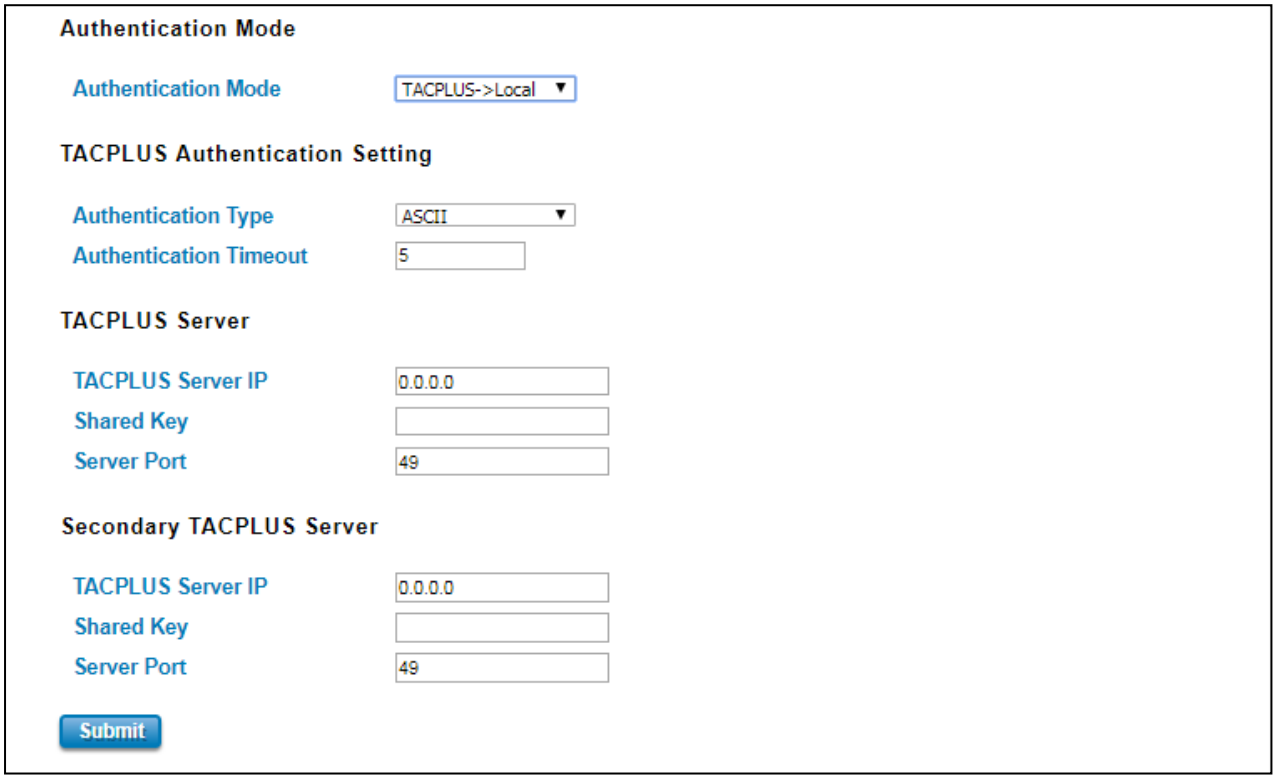
d. Click **Submit**

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:

a. Select the **Authentication Type.**

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

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

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

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

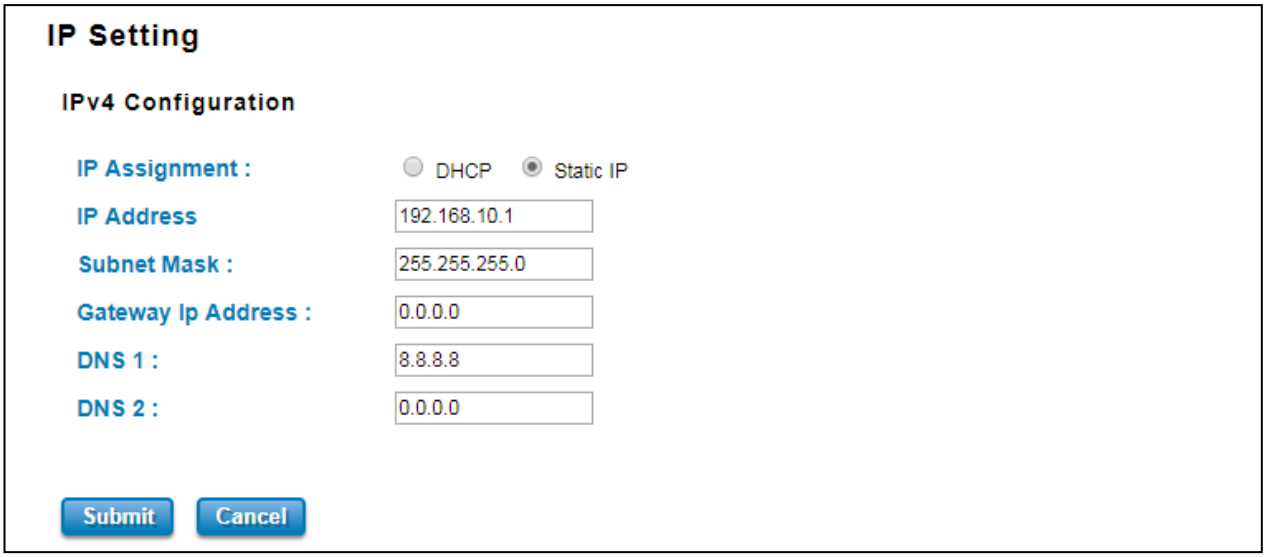
f. Click **Submit**

The description of the 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

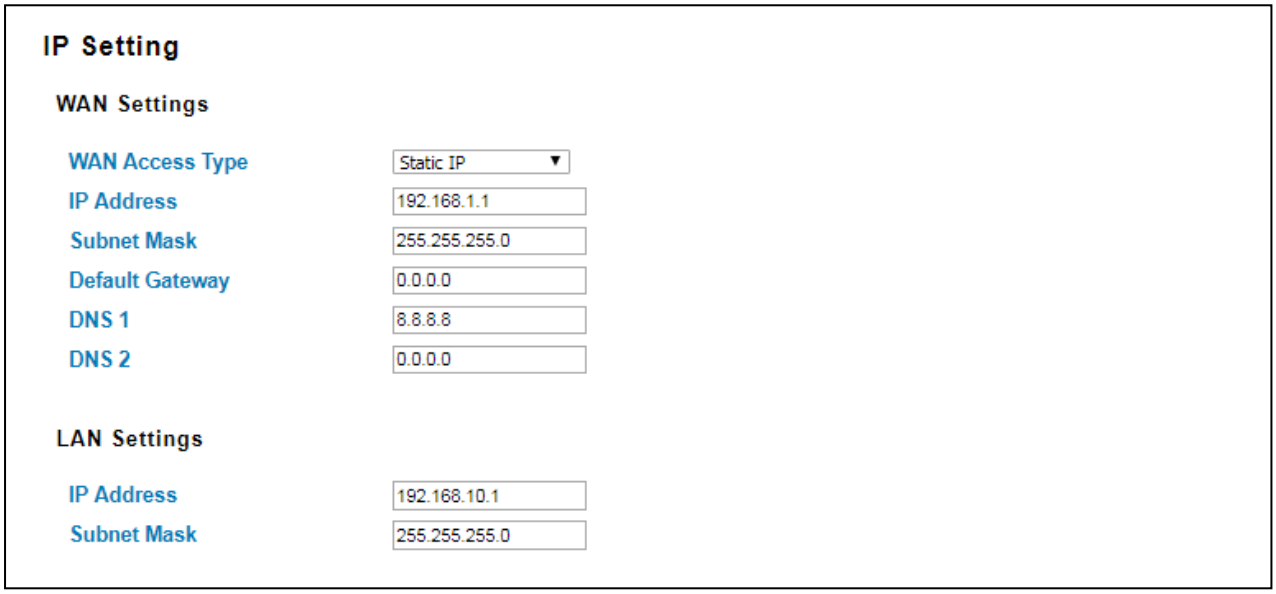
The Network Setting section allows users to configure both IPv4 values for management access over the network. WoMaster' router supports IPv4, and can be managed through either of these address types. Below is the IP Setting interface for **Bridge Mode**.



The description of the columns is as below:

TERMS	DESCRIPTION
IP Assignment	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.
Gateway IP Address	**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 IP Setting interface for the **Router Mode w**here 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.
Gateway IP Address	**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.

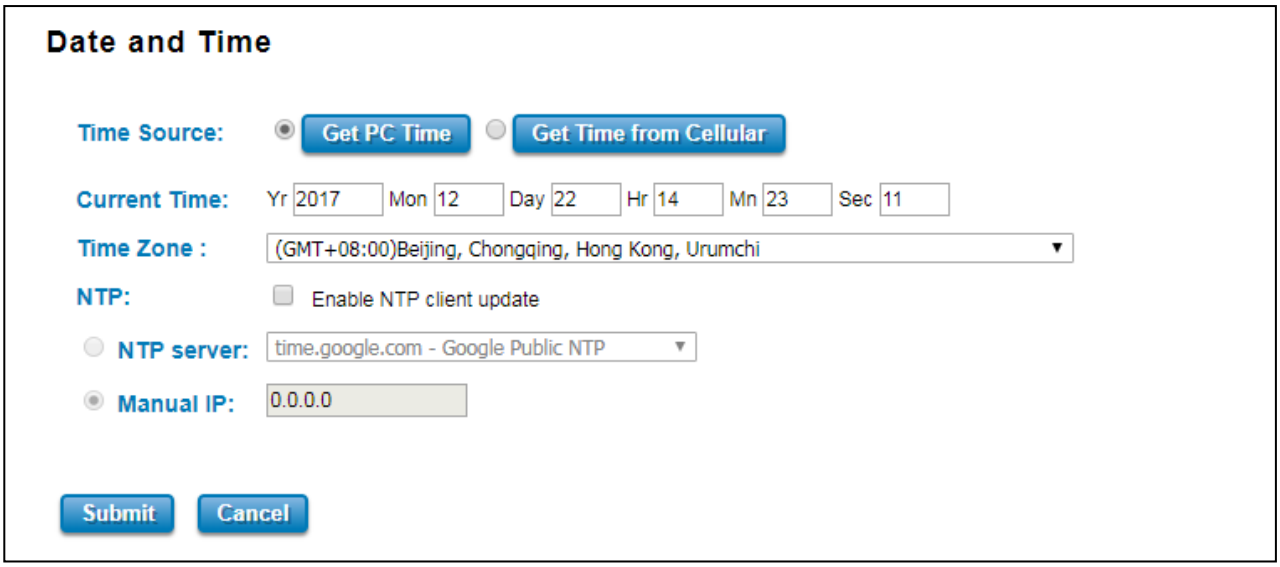
When Proxy ARP is enabled, if the router receives an ARP request for which it has a route to the target (destination) IP address, the router responds by sending a Proxy ARP reply packet containing its own MAC address. The host that sent the ARP request then sends its packets to the router, which forwards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

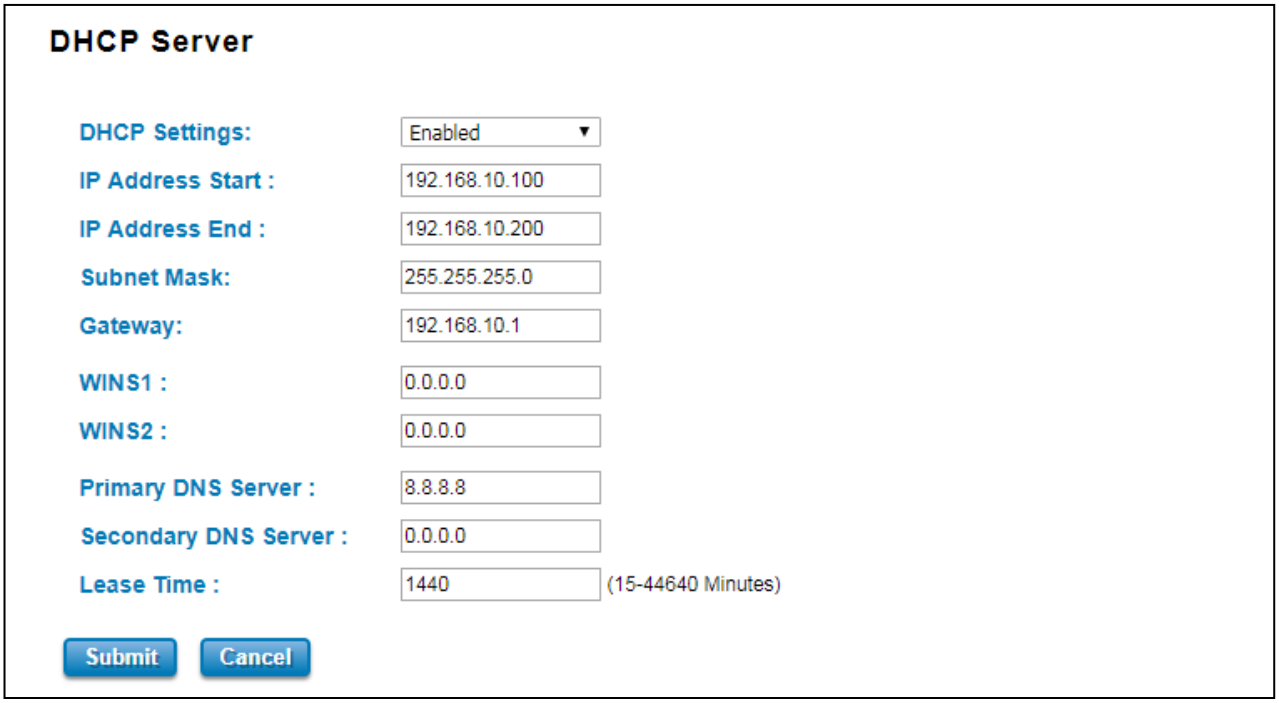
NTP	**Enable NTP Client update** by checking this box. Select the time server from the **NTP Serve**r dropdown list or select **Manual IP** to manually input the IP address of available time server. ***Make sure that the device also has the internet connection.**

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:

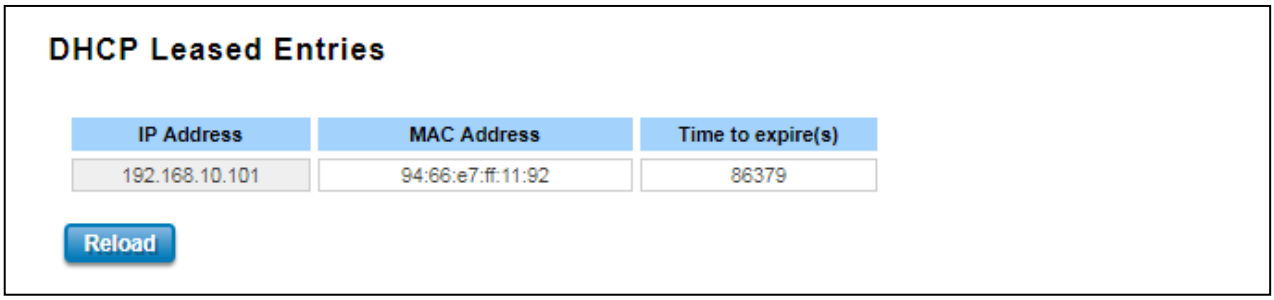
TERMS	DESCRIPTION
DHCP Setting	Select to **Enable** or **Disable** to activate and deactivate DHCP Server function.
IP Address Start	Assign the IP Address Start range.
IP Address End	Assign the IP Address End range.
Subnet Mask	**Default: 255.255.255.0** Assign the subnet mask for the IP address here 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.

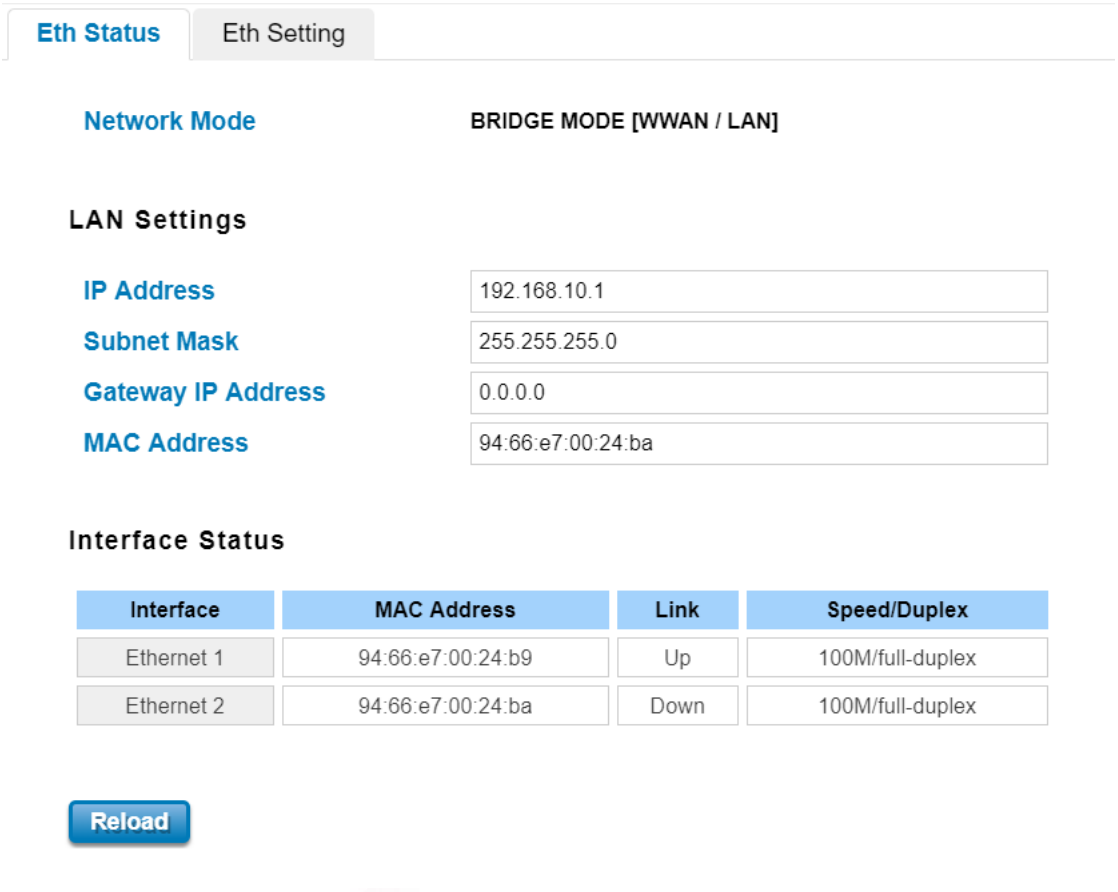
Following items are included in this group:

3.2.1 Ethernet Status

3.2.2 Ethernet Setting

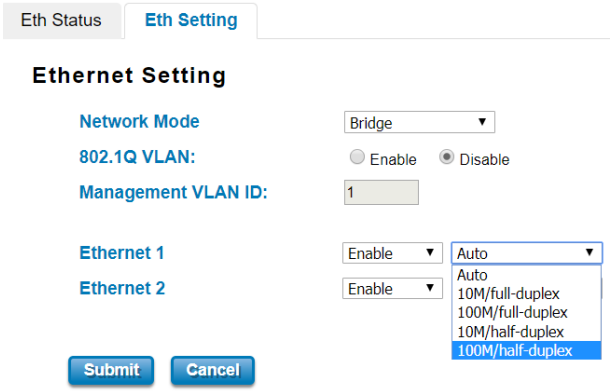
3.2.1 Ethernet Status

Ethernet Status section allows users to see the current status from the Ethernet such as Network Mode, LAN Settings, and also the Interface Status.



The description of the columns is as below:

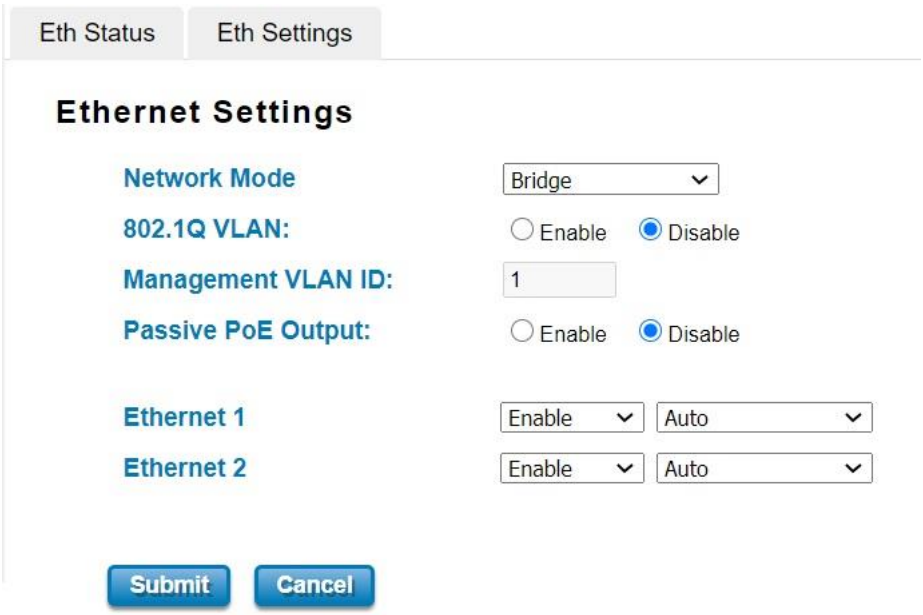
TERMS	DESCRIPTION
Network Mode	Shows network mode from the router **(Bridge or Router)**

IP Address	Display the IP address reserved by User network for User router
Subnet Mask	Display the subnet mask for the IP address.
Gateway IP Address	Display the gateway that assigned to the router.
MAC Address	Display the hardware's MAC Address that assigned by the manufacturer.
Interface	Display the Ethernet interface
MAC Address	Display the port MAC Address
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 **Ethernet Port 1~2** 

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

3.2.2 Ethernet Setting

Use this page to configure the Ethernet setting such as the Host Name, Network Mode and the speed / duplex for the Ethernet port.



The description of the Ethernet Setting page is as below:

TERMS	DESCRIPTION
Network Mode	**Default: Bridge** Select Bridge mode and Router mode depends on the application. Bridge mode and Router mode have the same setting interface. When the Router mode is selected, then the device will change to router mode and the interface for port 1 (PoE OUT) would be WAN interface and port 2 (PoE IN) would be LAN interface.
802.1Q VLAN	**Default: Disable** Choose enable to activate the function.
Management VLAN	**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.
Passive PoE Output	**Default: Disable** Choose enable to activate the function.
Ethernet 1 ~ 2	**Default: Enable** **Default: Auto / Auto-Negotiation** Configure the Speed/Duplex of the port Ethernet 1 ~ 2. Users can set the bandwidth of each port as Auto-negotiation, 100 full, 100 half, 10 full, 10 half mode.

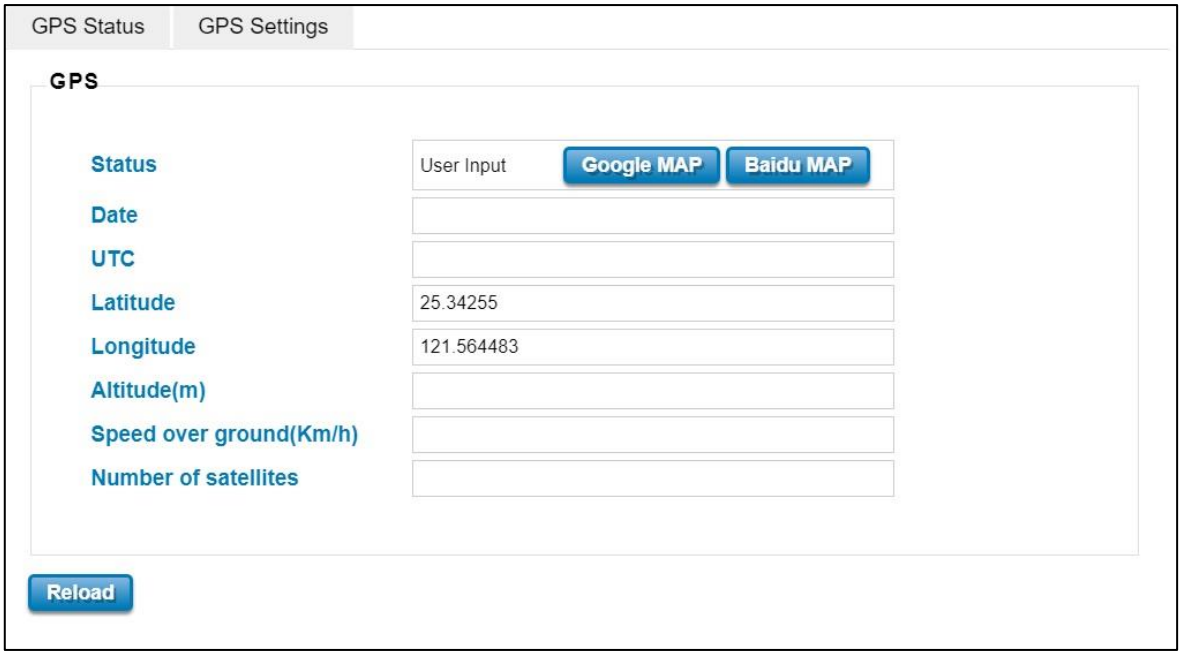
Click **Submit** to apply the configuration that just made.

3.3 GPS

This GPS section has the function to show the current position of the device. It could help the technician to track the device location.

3.3.1 GPS Status

GPS status is always disable since user need to manually input GPS coordinates in GPS settings page.



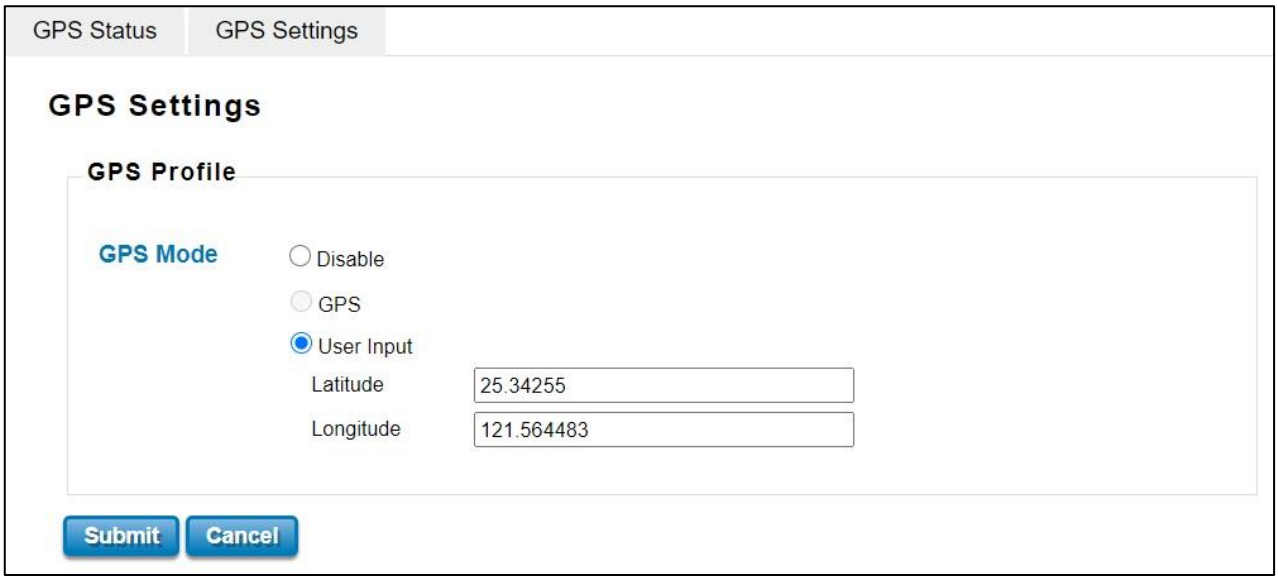
The description of the columns is as below:

TERMS	DESCRIPTION
Status	Display the GPS interface status User Input or Disable. The default is Disable.
Date	No display.
UTC	No display.
Latitude	Display the latitude of the coordinate.
Longitude	Display the longitude of the coordinate.
Altitude(m)	No display.
Speed over ground(Km/h)	No display.
Number of satellites	No display.

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.

3.3.2 GPS Setting

In this GPS Setting section, user can input the latitude and Longitude of the device by manual. After the data be entered in, the GPS status will show User Input and MAP button.(refer the picture in 3.3.1 GPS STATUS)

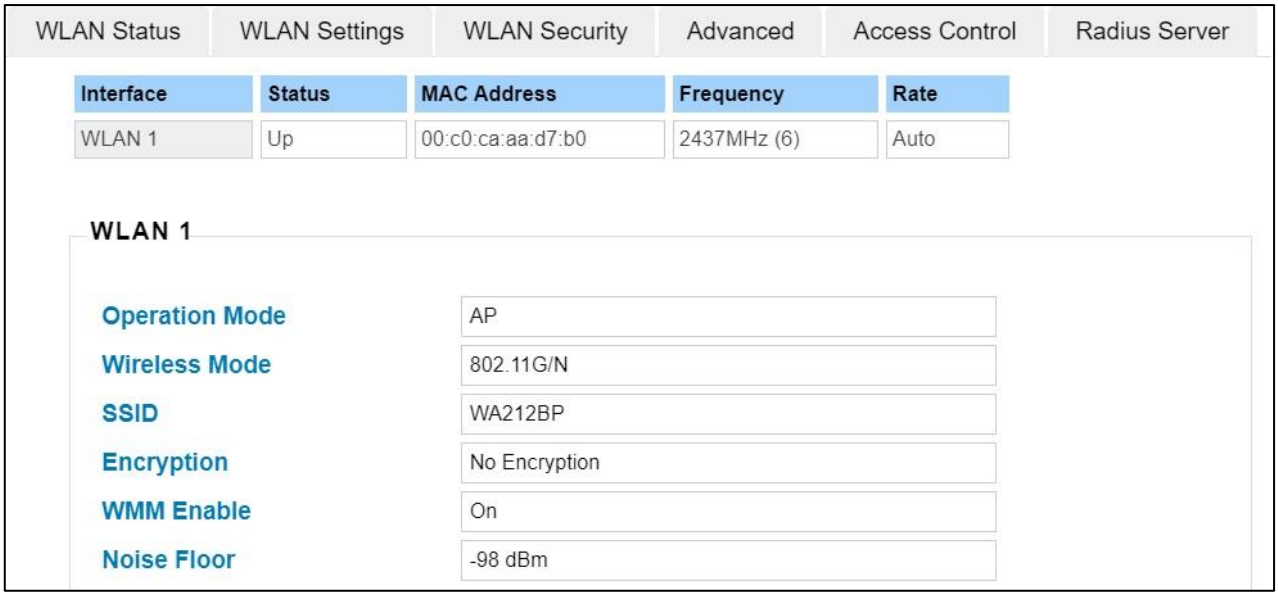

GPS Status
GPS Settings
GPS Settings
GPS Profile
GPS Mode
Disable
GPS
User Input
Latitude
25.34255
Longitude
121.564483
Submit
Cancel

3.4 Wireless LAN

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, Access Control and Radius Server.

3.4.1 WLAN Status

The figure below shows the WLAN status.



The description of the columns is as below:

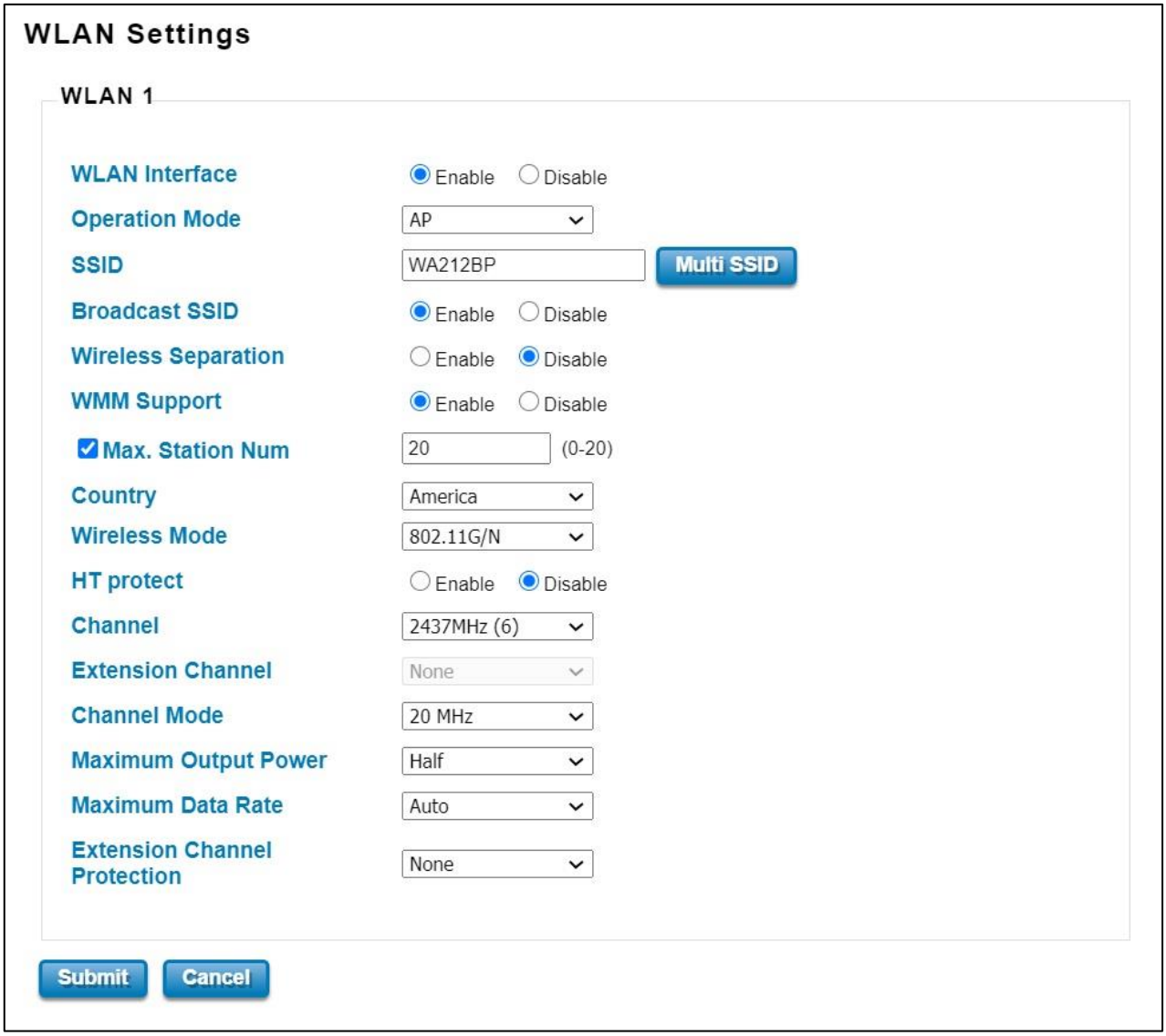
TERMS	DESCRIPTION
Operation Mode	Display the current operating modes on the device
Wireless Mode	Display the current wireless mode
SSID	Display the primary name of the SSID
Encryption	Display the encryption mode.
WMM Enable	Display the status of the WMM support.
Noise Floor	Display the background noise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

3.4.2 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.

3.4.2.1 AP Mode

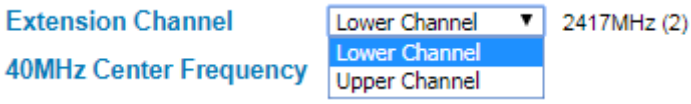
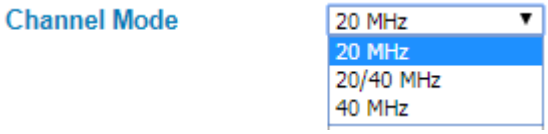
The Access Point mode, it establishes a wireless connection, receive from wireless clients and provide connection for wireless client devices, the client can search and connect to several the access points. In AP mode interface, user can configure the SSID name, Enable or Disable Broadcast SSID, select 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.

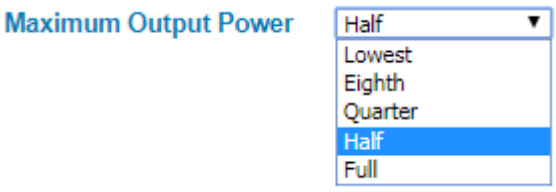
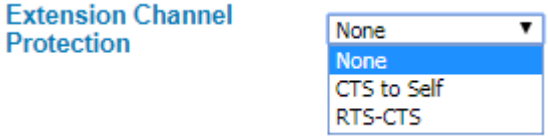


The description of the columns is as below:

TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless

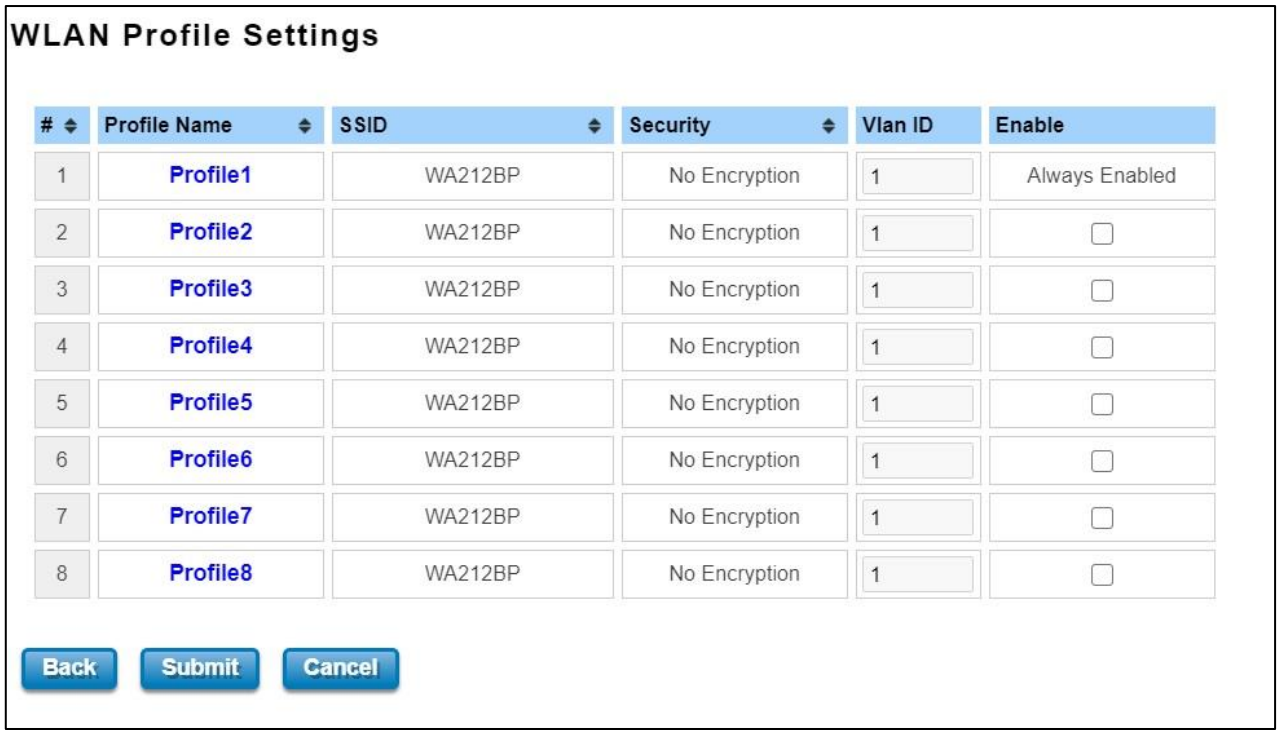
	functions.
Operation Mode	**Default: AP** Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	**Default: model name** Input the primary name of the access point.
Broadcast SSID	**Default: Enabled.** By enabling the broadcast SSID, it makes the AP can be accessed 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: Disable** Under the AP mode, enable it to prevent one wireless device from directly communicating with another on the same AP
WMM Support	**Default: Enable** A subset of the WLAN specification that enhances quality of service (QoS) on a network by prioritizing data packets onto four categories. Ranging from highest priority to lowest, these categories are: ● **Voice**: Giving voice packets the highest priority enables concurrent Voice over IP (VoIP) calls with minimal latency and the highest quality possible. ● **Video**: By placing video packets in the second tier, WMM prioritizes it over all other data traffic. ● **Best effort**: Best effort data packets consist of those originating from legacy devices or from applications or devices that lack QoS standards. **Background**: Background priority encompasses file downloads, print jobs and other traffic that does not suffer from increased latency.
Max Station Number	**Default: 20 (0-20)** Set the maximum number of station that can communicate with the access point.
Country	Select your country or region
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. 
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**  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.

	
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	 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.

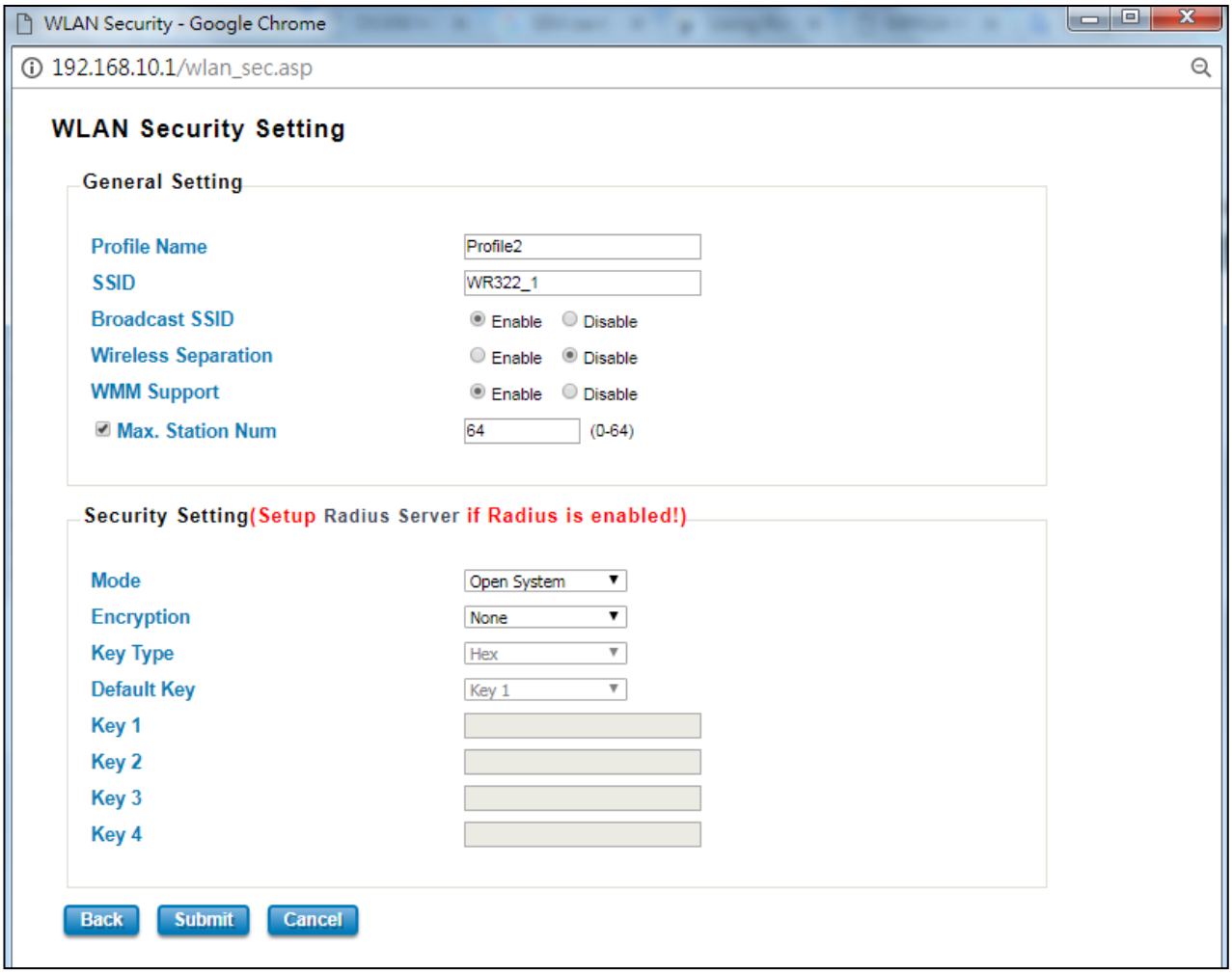


The description of the column is as below:

TERMS	DESCRIPTION
Profile Name	Display the available WLAN Profile name
SSID	Display the SSID Name.
Security	Display the current security mode for the Wireless 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

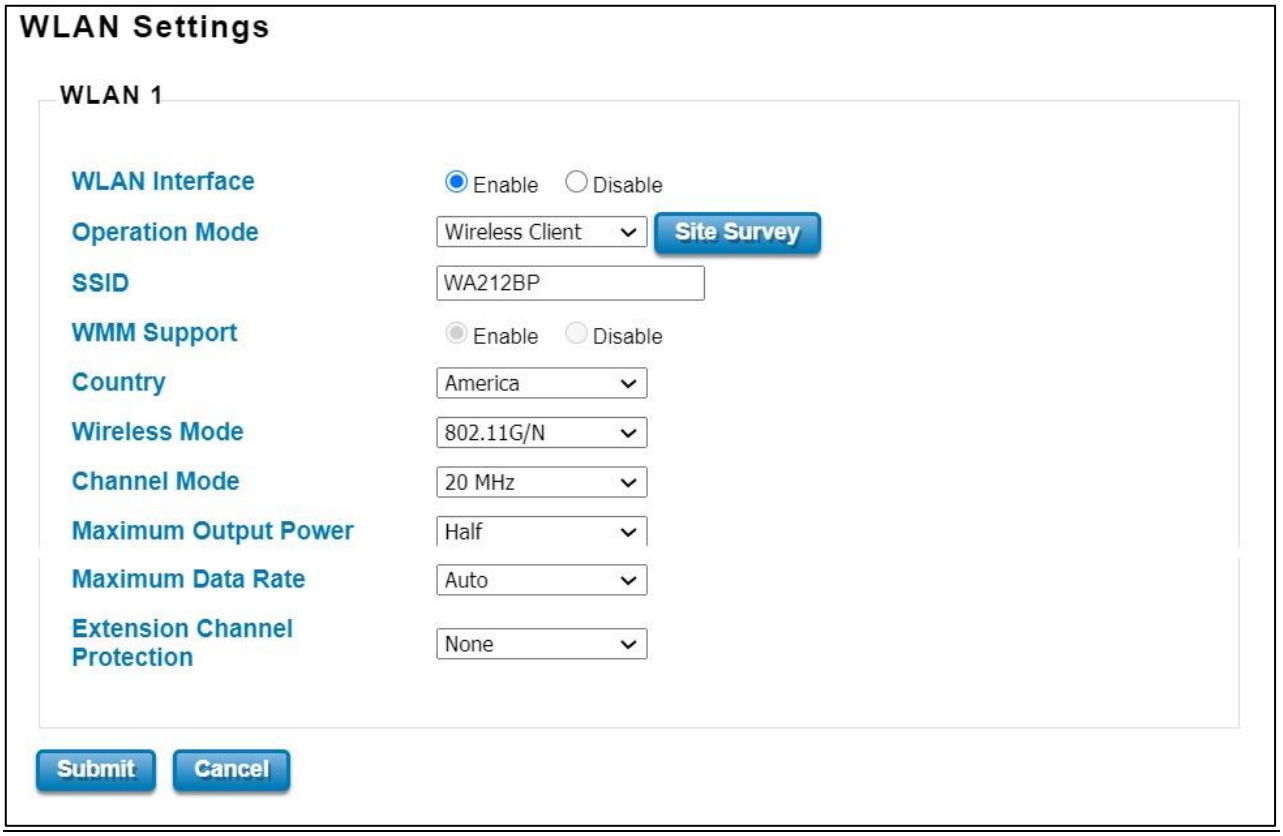
The Multi SSID section shows the configuration page where the Profile1 always enabled. In this section, user may configure each Profile by check the box to enable the Profile and then click the profile name to open the configuration page for specific Profile. The figure below is the pop-up WLAN Security 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 (3.4.3).



Click **Submit** to apply the configuration

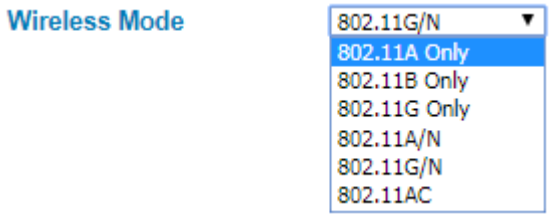
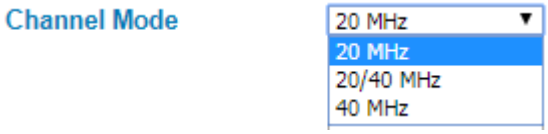
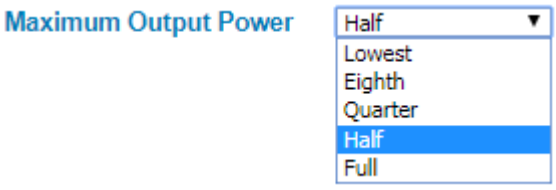
3.4.2.2 Client Mode

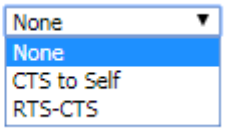
Wireless Client mode, in this mode the device is able to connect to the Access Point and join the wireless network around the device that opens the connection. User can find the best connection for the AP by click the **Site Survey** and the AP list will appear.



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: model name** Input the primary name of the access point.
WMM Support	**Default: Enable** A subset of the WLAN specification that enhances quality of service (QoS) on a network by prioritizing data packets onto four categories. Ranging from highest priority to lowest, these categories are: ● **Voice**: Giving voice packets the highest priority enables concurrent Voice over IP (VoIP) calls with minimal latency and the highest quality possible. ● **Video**: By placing video packets in the second tier, WMM prioritizes it

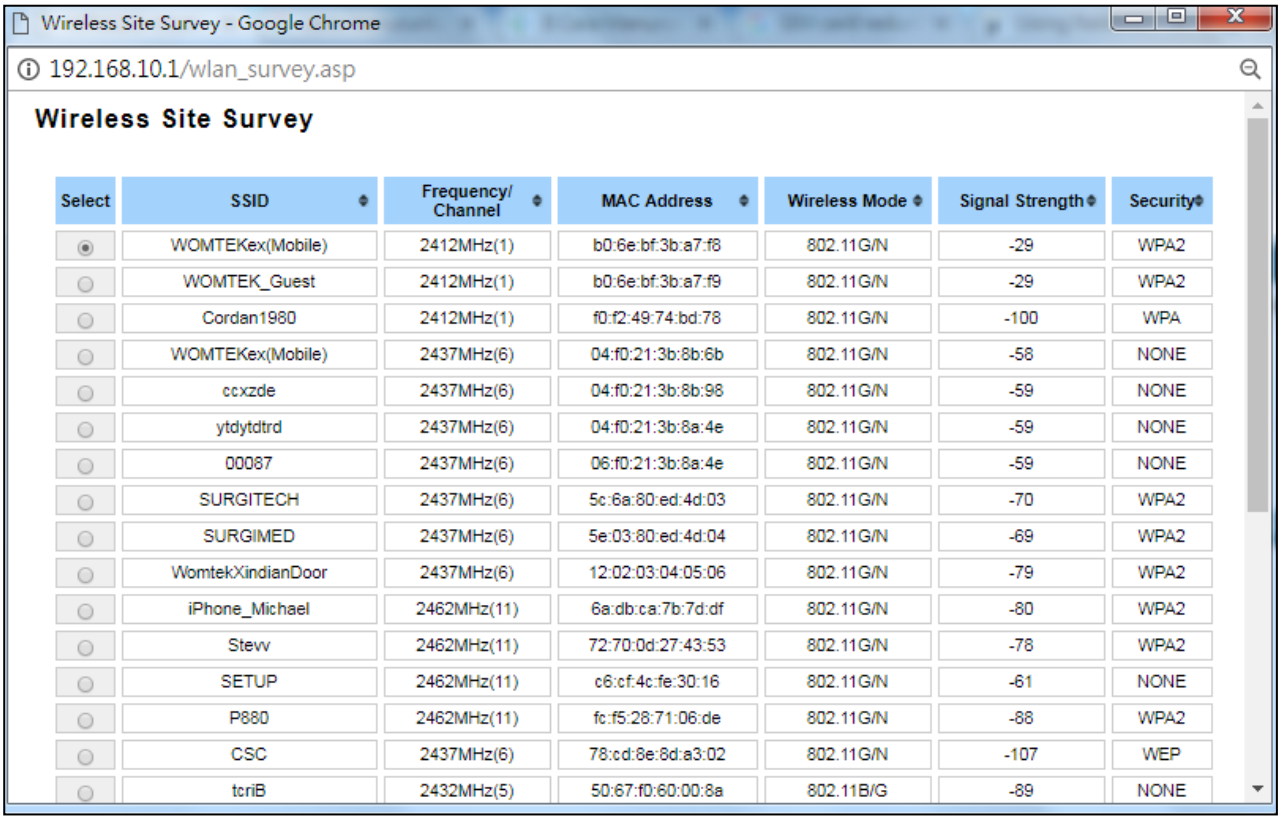
	over all other data traffic. ● **Best effort**: Best effort data packets consist of those originating from legacy devices or from applications or devices that lack QoS standards. **Background**: Background priority encompasses file downloads, print jobs and other traffic that does not suffer from increased latency.
Country	Select your country or region
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 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. 
Maximum 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	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

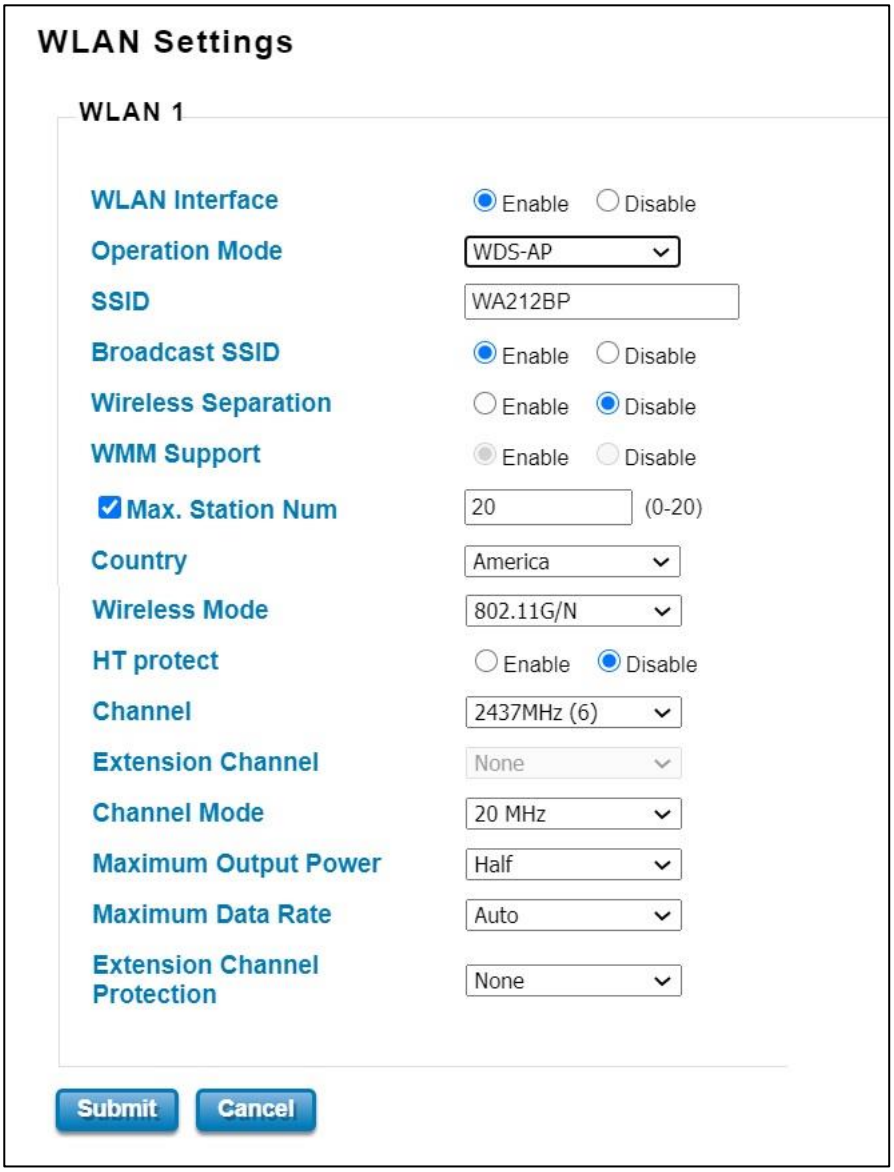
The description of the columns is as below:

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.

3.4.2.3 WDS AP Mode

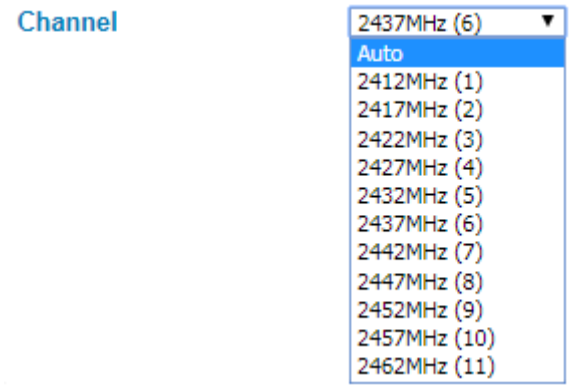
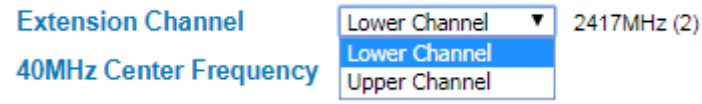
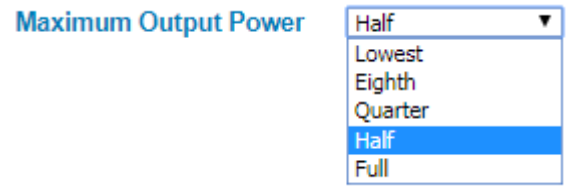
The WDS-AP mode usually implements the Point to Point (P2P) connection, so the access point should be WDS-AP and the wireless client should be WDS-Client. So in this case, the AP just can share the connection to the specific wireless client that has its MAC Address. But WDS-AP can be a repeater to provide 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 function.
Operation Mode	Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	**Default: model name** 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 broadcaset SSID, the network will be hidden in order to prevent any malicious attack.
Wireless Separation	**Default: Disable** Under the AP mode, enable it to prevent one wireless device from directly communicating with another on the same AP
WMM Support	**Default: Enable** A subset of the WLAN specification that enhances quality of service (QoS) on a network by prioritizing data packets onto four categories. Ranging from highest priority to lowest, these categories are: ● **Voice**: Giving voice packets the highest priority enables concurrent Voice over IP (VoIP) calls with minimal latency and the highest quality possible. ● **Video**: By placing video packets in the second tier, WMM prioritizes it over all other data traffic. ● **Best effort**: Best effort data packets consist of those originating from legacy devices or from applications or devices that lack QoS standards. **Background**: Background priority encompasses file downloads, print jobs and other traffic that does not suffer from increased latency.
Max Station Number	**Default: 20 (0-20)** Set the maximum number of station that can communicate with the access point.
Country	Select your country or region
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has different configuration. For each wireless mode, it has 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.

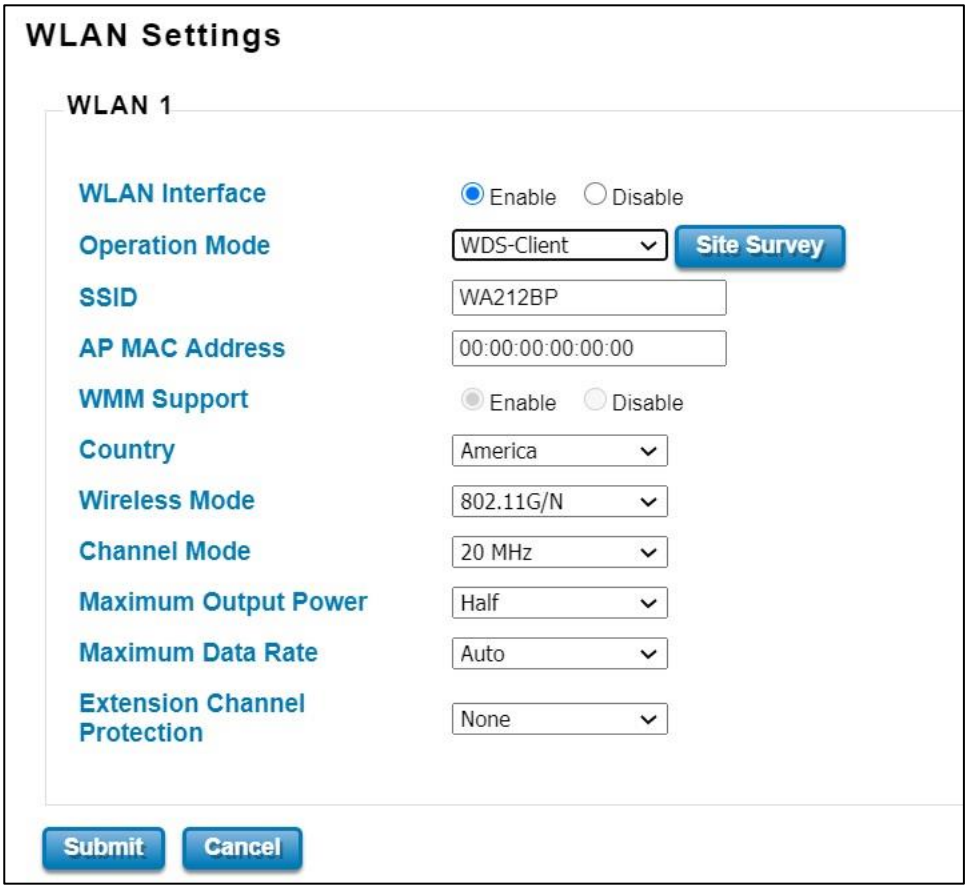
	
Extension Channel	**Default: Lower Channel 2417MHz (2)**  This option would be appeared when user select the Channel Mode to 20/40MHz or 40MHz. To put range for the frequency, it provides the Lower Channel (2417MHz (2)) with the 40MHz center frequency is 2427MHz (4) and Upper Channel (2457MHz (10)) with the 40MHz center frequency is 2447MHz (8).
Channel Mode	**Default: 20MHz**  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 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	 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

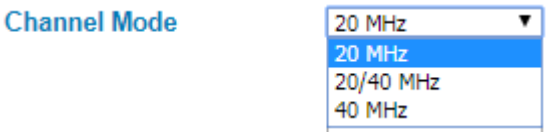
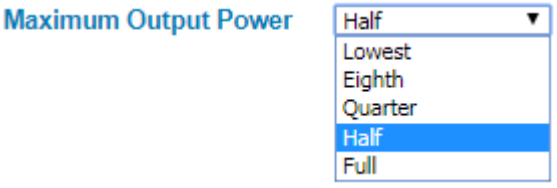
3.4.2.4 WDS Client Mode

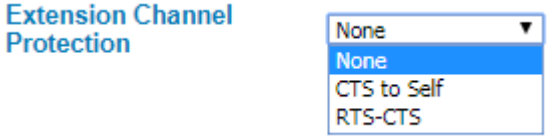
In WDS-Client mode, user must specify the specific WDS-AP's SSID and MAC address. So WDS-Client just do the transmission to the WDS-AP only. In this mode, please make sure that the configuration should be the same as the WDS-AP as well.



The description of the columns is as below:

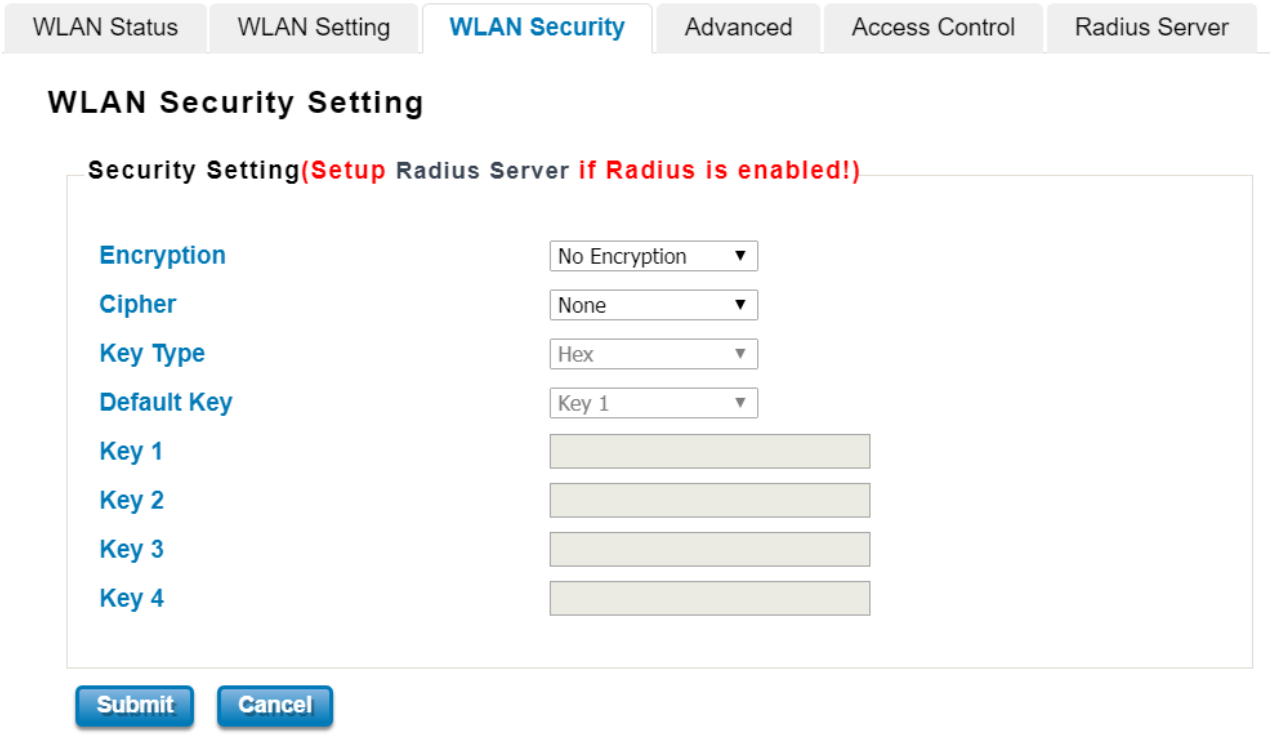
TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless functions.
Operation Mode	Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	**Default: model name** Input the primary name of the access point.
AP MAC Address	**Default: 00:00:00:00:00:00** Set the specific AP MAC Address of the WDS-AP.
WMM Support	**Default: Enable** A subset of the WLAN specification that enhances quality of service (QoS) on a network by prioritizing data packets onto four categories. Ranging from highest priority to lowest, these categories are: ● **Voice**: Giving voice packets the highest priority enables concurrent Voice over IP (VoIP) calls with minimal latency and the highest quality possible.

	● **Video**: By placing video packets in the second tier, WMM prioritizes it over all other data traffic. ● **Best effort**: Best effort data packets consist of those originating from legacy devices or from applications or devices that lack QoS standards. **Background**: Background priority encompasses file downloads, print jobs and other traffic that does not suffer from increased latency.
Country	Select your country or region
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 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. 
Maximum 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	 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.

3.4.3 WLAN Security

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



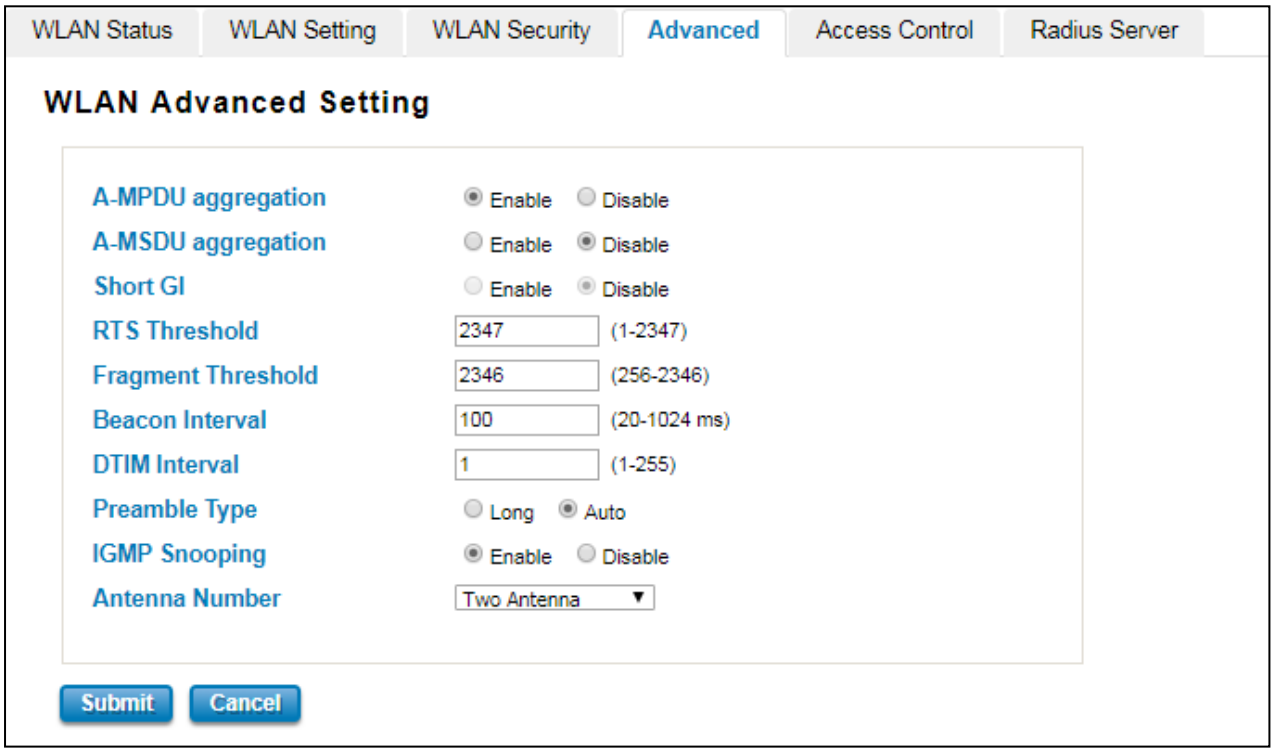
The description of the columns is as below:

TERMS	DESCRIPTION
Encryption	**Default: No Encryption** Encryption: No Encryption ▼ No Encryption WEP WPA Enterprise WPA2 Enterprise WPA & WPA2 Enterprise WPA-PSK WPA2-PSK WPA-PSK&WPA2-PSK **No Encryption**: It allows any device to join the network without security checks. **WEP**: Data encryption and key are required for the authentication. **WPA Enterprise**: With warrant (username, password and etc.) offered by user, this kind of authentication can be realized with specific RADIUS server. **WPA2 Enterprise**: A new version of WPA, only clients that supported with WPA2 can apply this security function. The AES encryption RADIUS server is required. **WPA & WPA2 Enterprise**: AES & TKIP encryption and RADIUS server is required.

	WPA-PSK: A simplified WPA mode that no need to specify the authentication server. It can be called as WPA Pre-Shared Key, a user just needs to enter a key in each WLAN node. The data encryption is only TKIP. **WPA2-PSK**: A new version of WPA, only clients that supported with WPA2 can apply this security function. The data encryption can only be AES and WPA Pre-Share Key is required. **WPA-PSK&WPA2-PSK**: The data encryption will be AES & TKIP and WPA Pre-Share Key is required.
Cipher	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.

3.4.4 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.



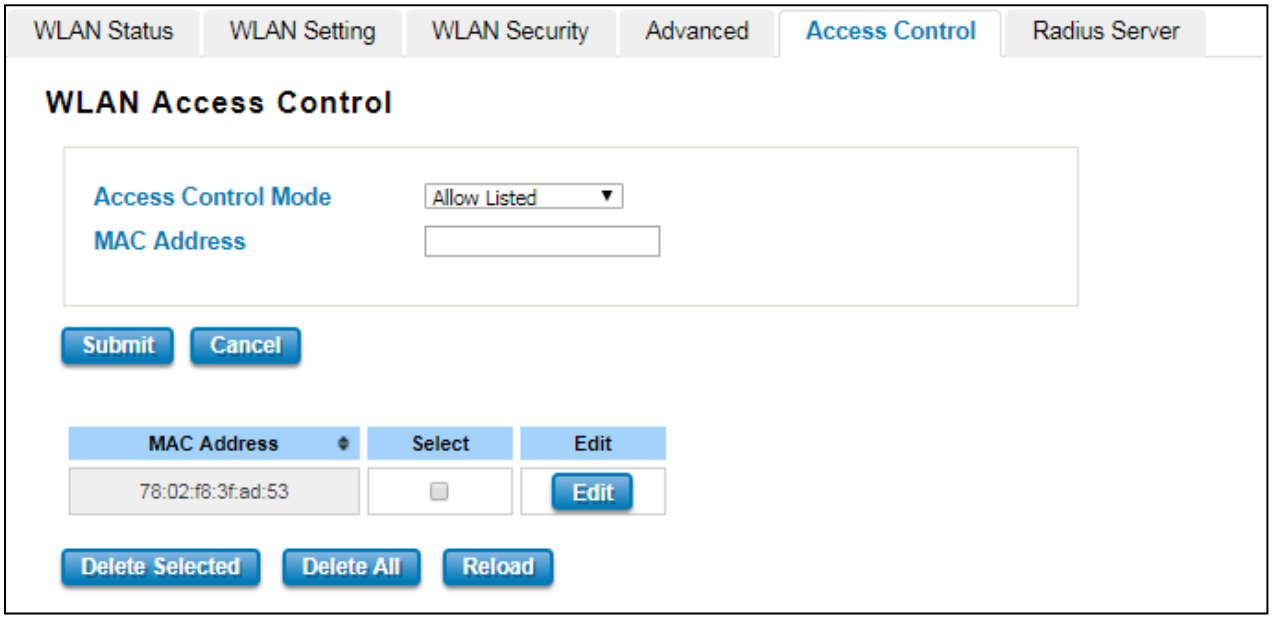
The description of the columns is as below:

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.

3.4.5 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

3.4.6 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).

3.5 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:

3.5.1 Access Control

3.5.2 Outbound Firewall

3.5.3 NAT Setting

3.5.4 OpenVPN

3.5.5 L2TP Setting

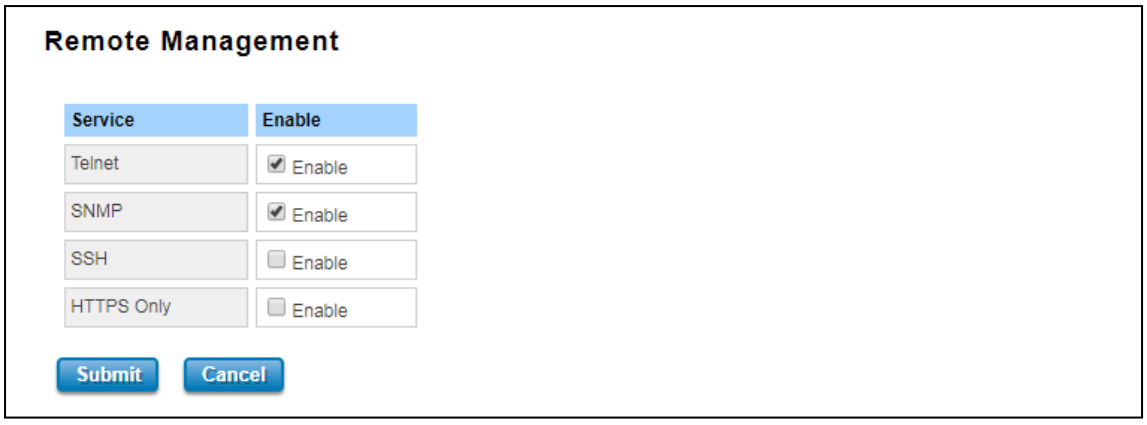
3.5.6 GRE Setting

3.5.1 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.

3.5.1.1 Remote Management

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



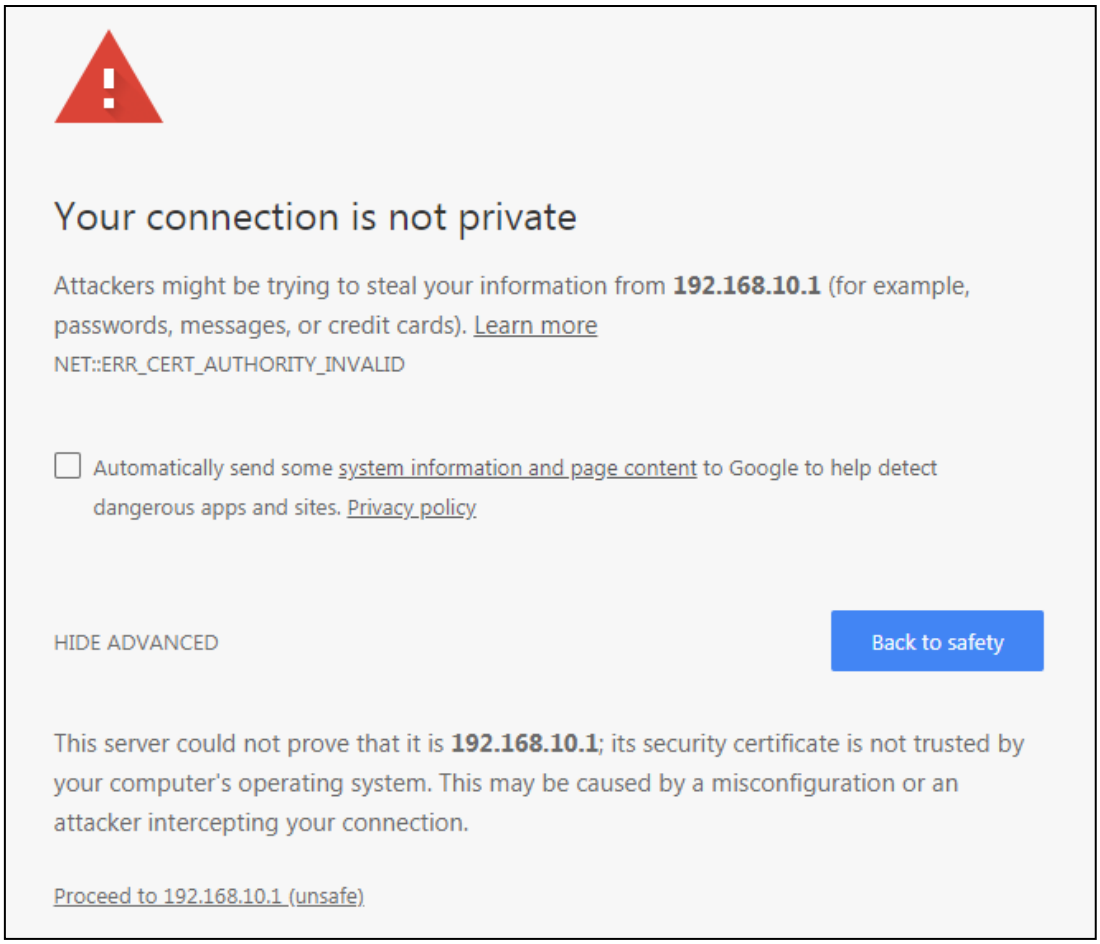
The description of the columns is as below:

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

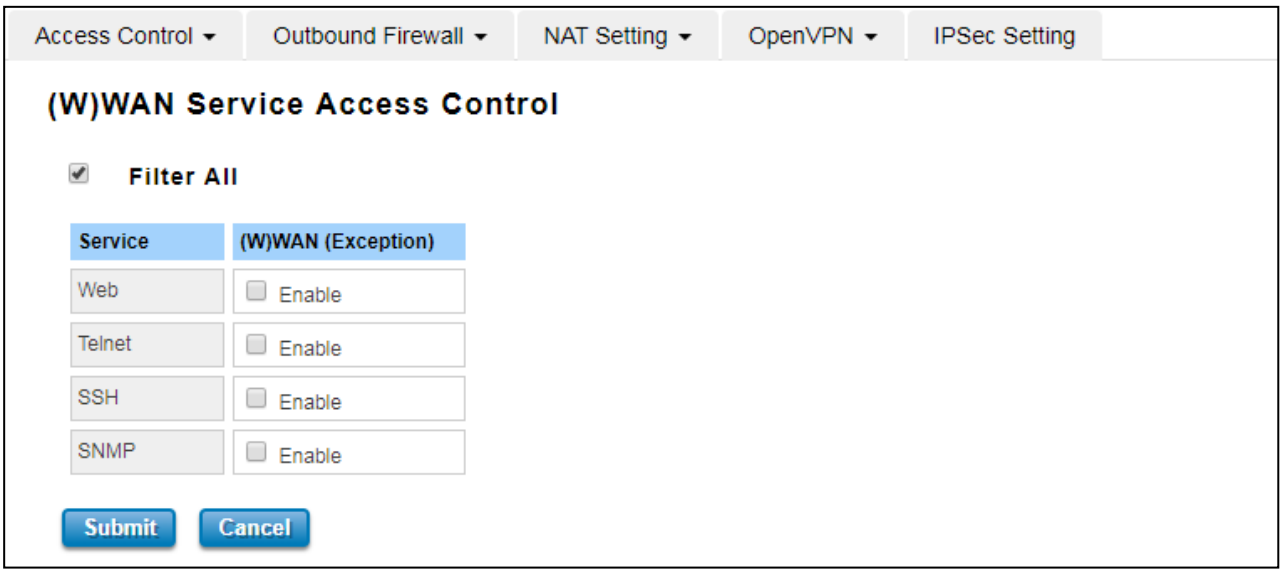
HTTP Secure is the use of the HTTP protocol over an SSL/TLS protocol. It is used primarily to protect against eavesdropping of communication between a web browser and the web site to which it is connected. This is especially important when you wish to have a secure connection over a public network such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

3.5.1.2 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.



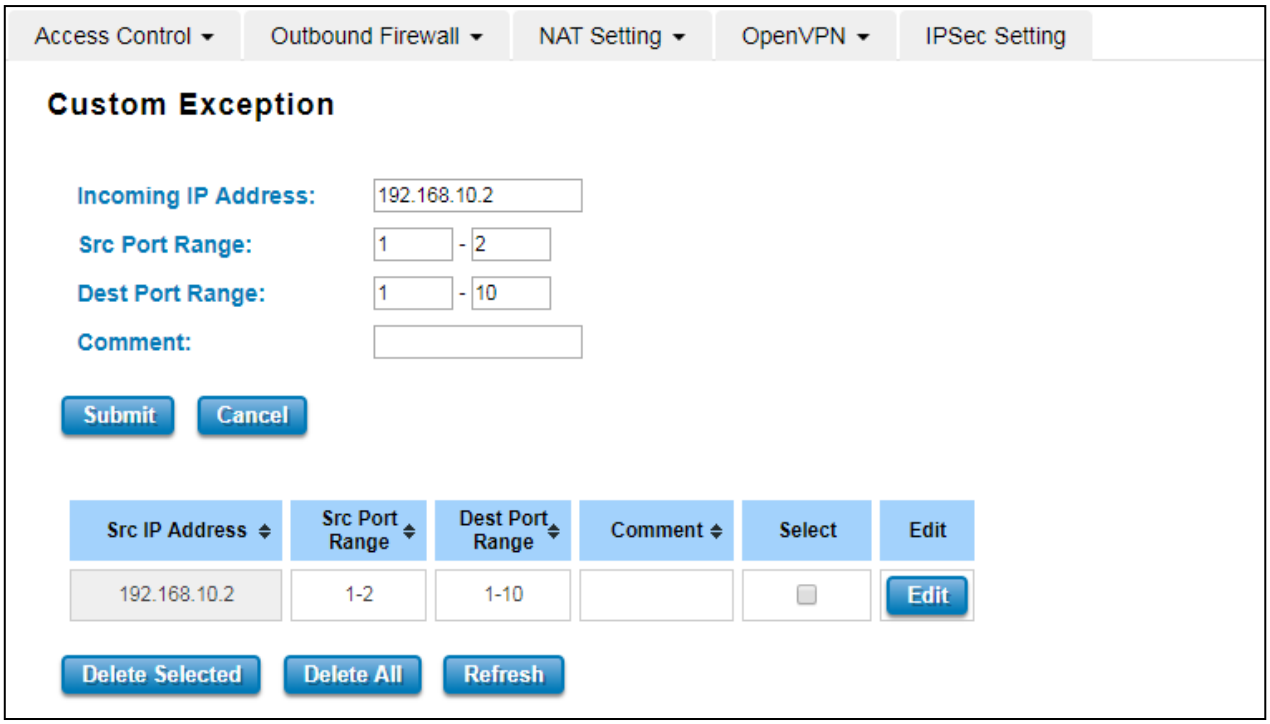
The description of the columns is as below:

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.

3.5.1.3 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.



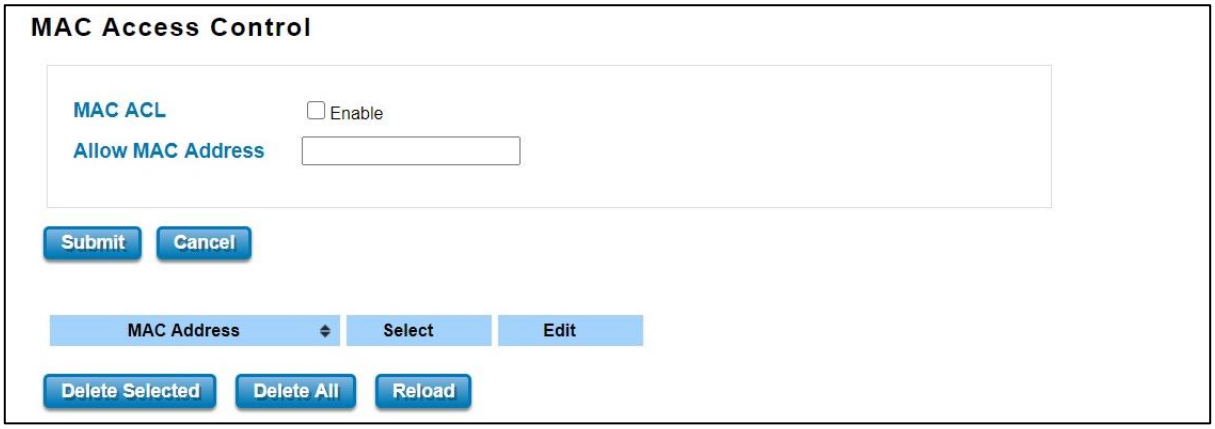
The description of the columns is as below:

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.

3.5.1.4 MAC Access Control

MAC Access control is Access Control that filter traffic using information in the Layer 2 header of each packet. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at the interfaces.



The description of the columns is as below:

TERMS	DESCRIPTION
MAC ACL	Check Enable to activate the function.
Allow MAC Address	Input the MAC address you allow.

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

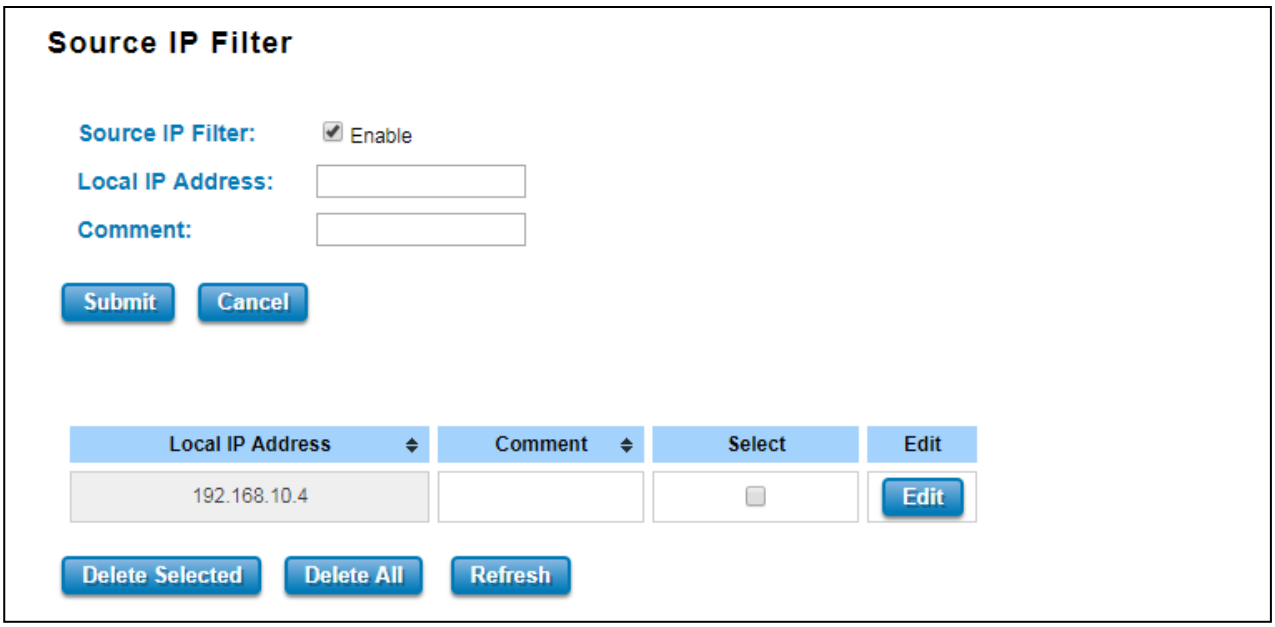
3.5.2 Outbound Firewall

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

3.5.2.1 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.



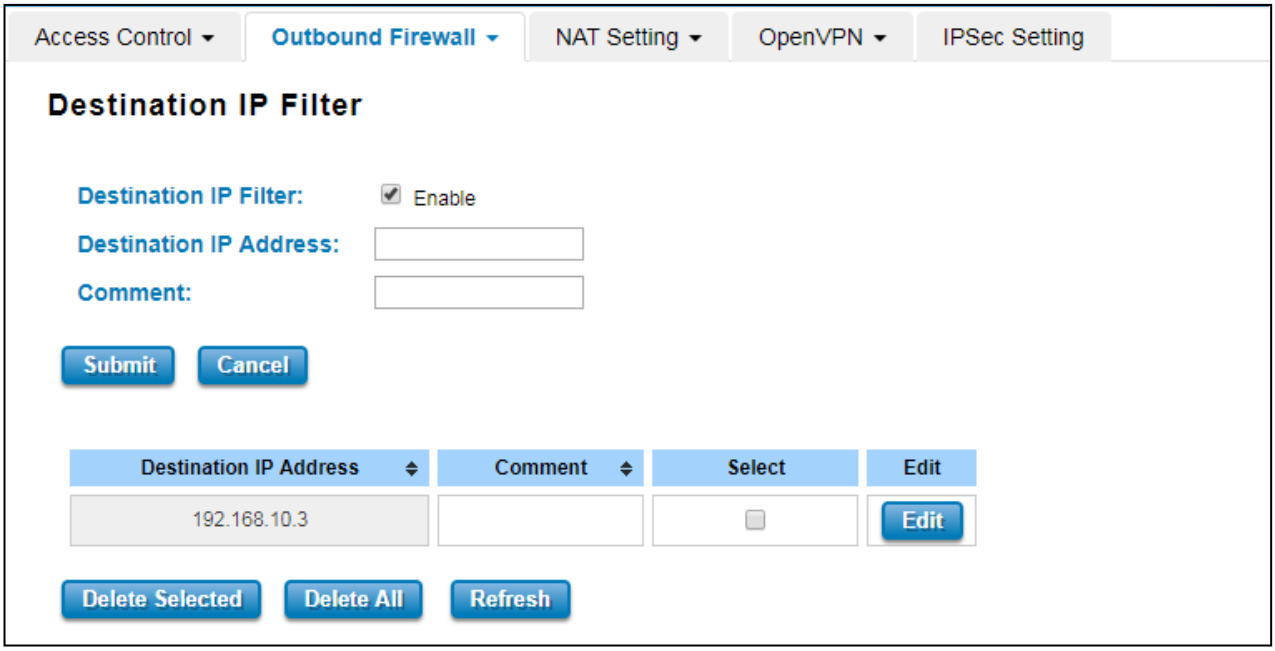
The description of the columns is as below:

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

3.5.2.2 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

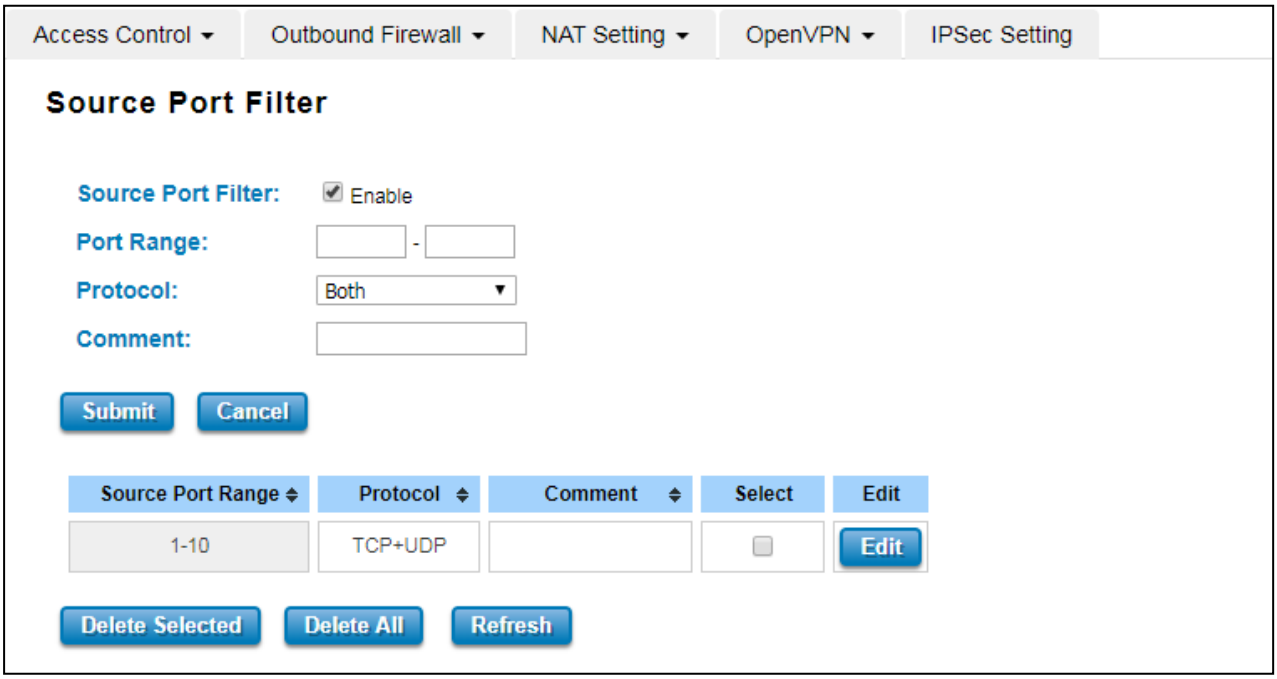
Click **Refresh** to refresh the table

3.5.2.3 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

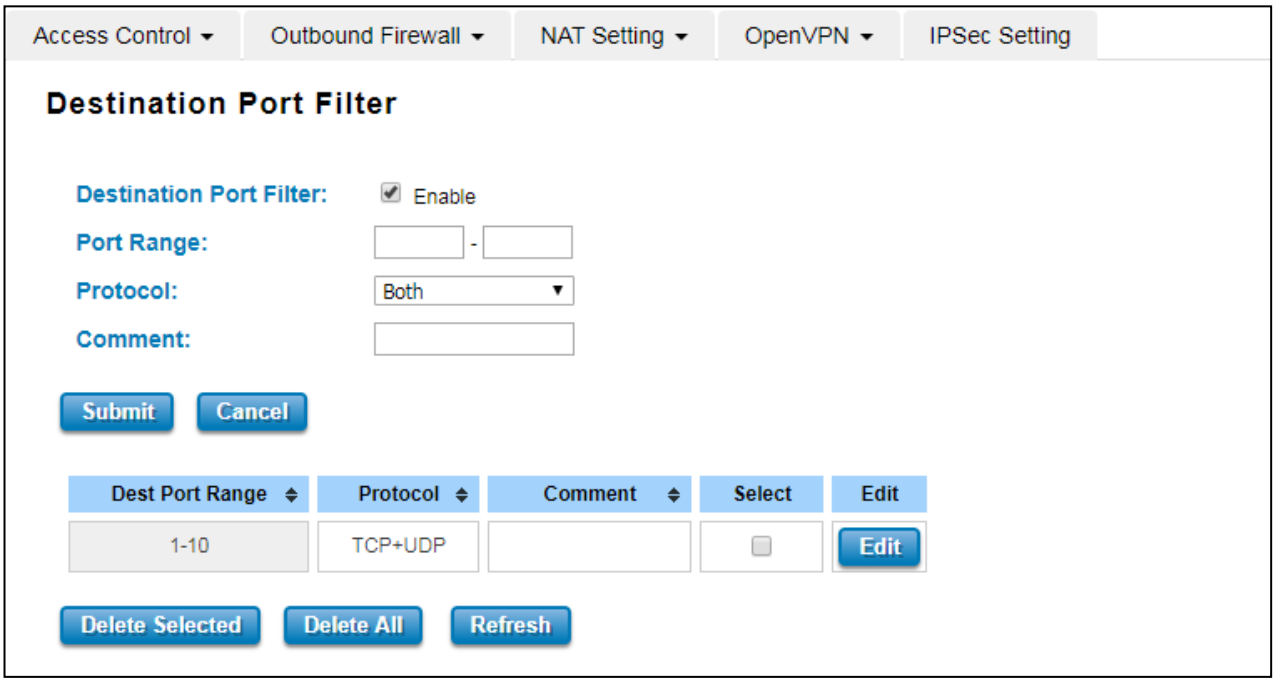
Click **Refresh** to refresh the table

3.5.2.4 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

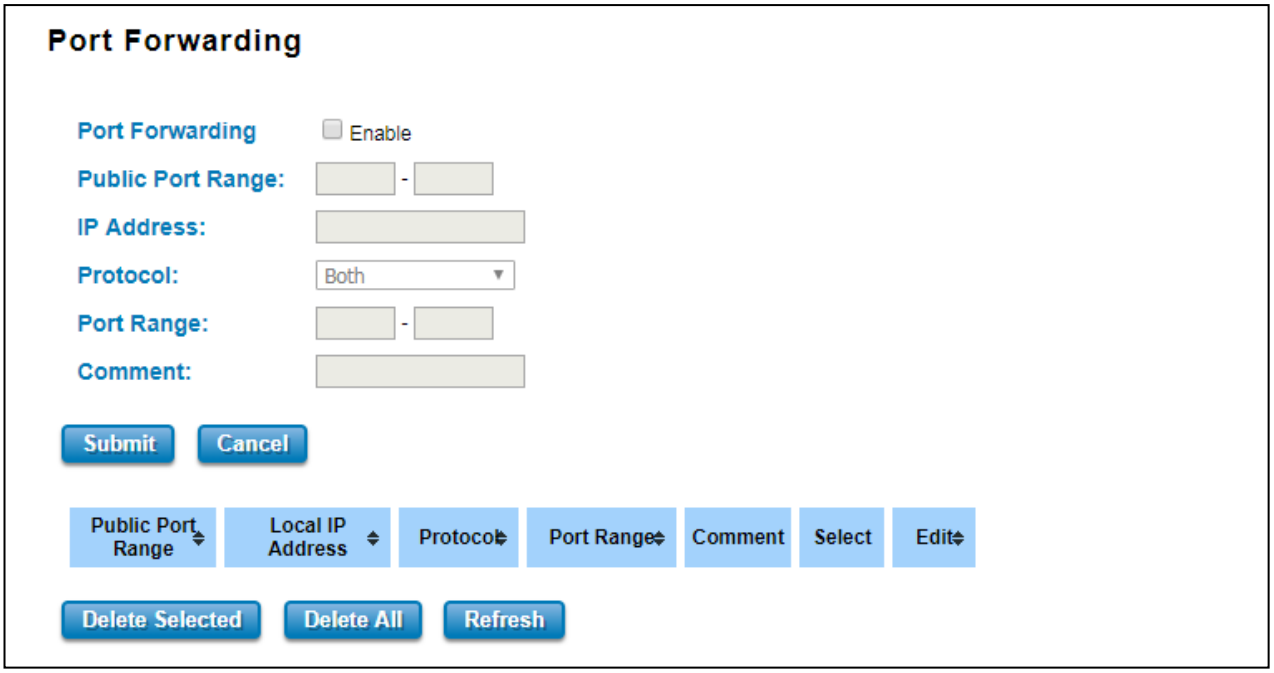
Click **Refresh** to refresh the table

3.5.3 NAT Settings

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.

3.5.3.1 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.

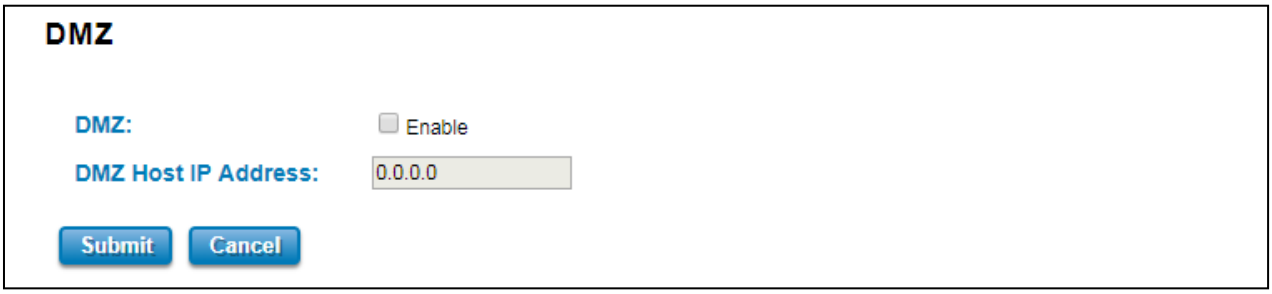
The description of the columns is as below:

TERMS	DESCRIPTION
Port Forwarding	Select Enable to activate Port Forwarding function.
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.

3.5.3.2 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.

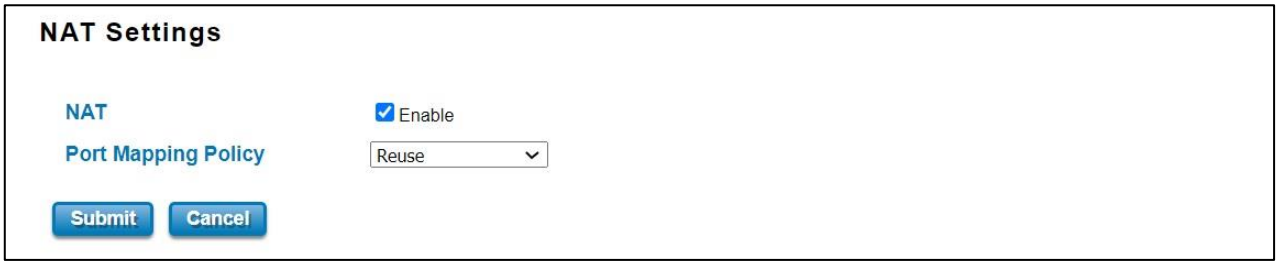


Click **Enable** to activate the function and assign the IP address of **DMZ Host IP Address**. This is the DMZ computer's IP address. Click Submit to activate the function.

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.

3.5.3.3 NAT Settings



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

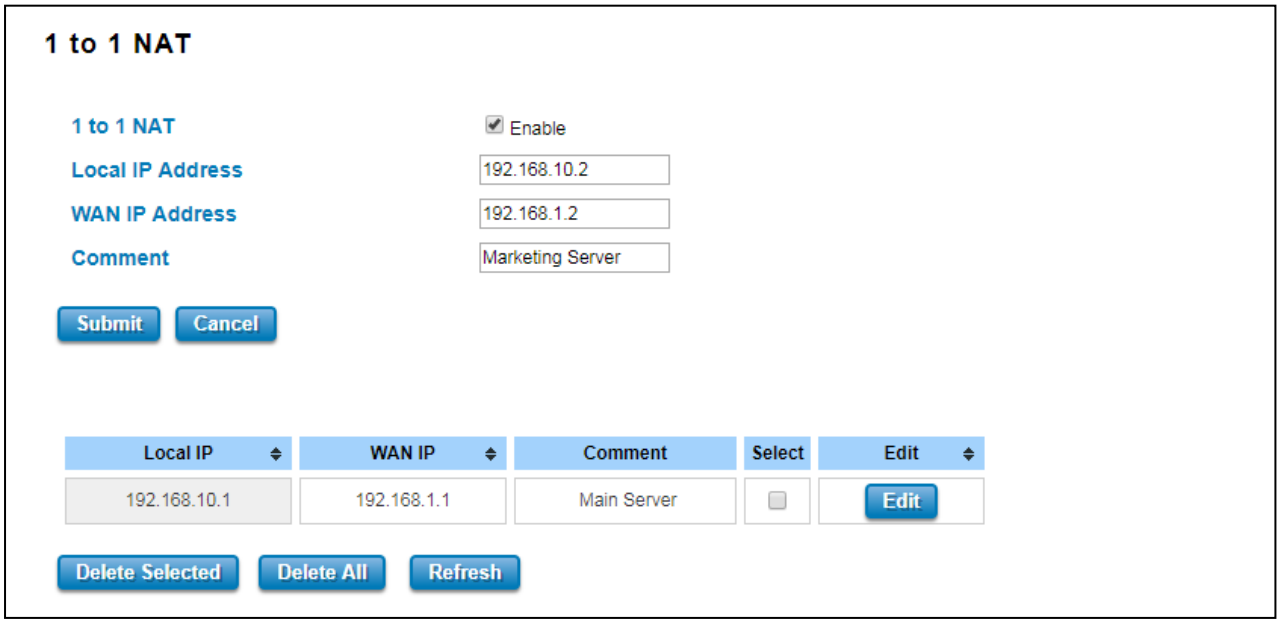
The description of the columns is as below:

TERMS	DESCRIPTION
NAT	**Default: 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.

3.5.3.4 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

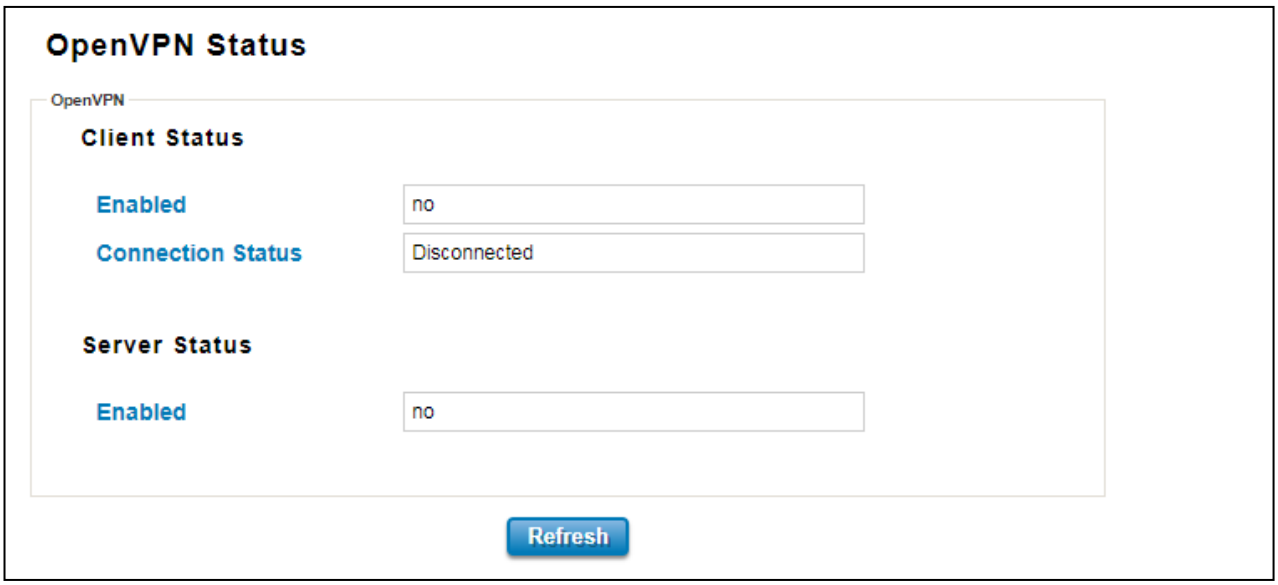
Click **Submit** to apply the configuration.

3.5.4 OpenVPN

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.

3.5.4.1 OpenVPN Status

This section shows the VPN Client and Server current status.



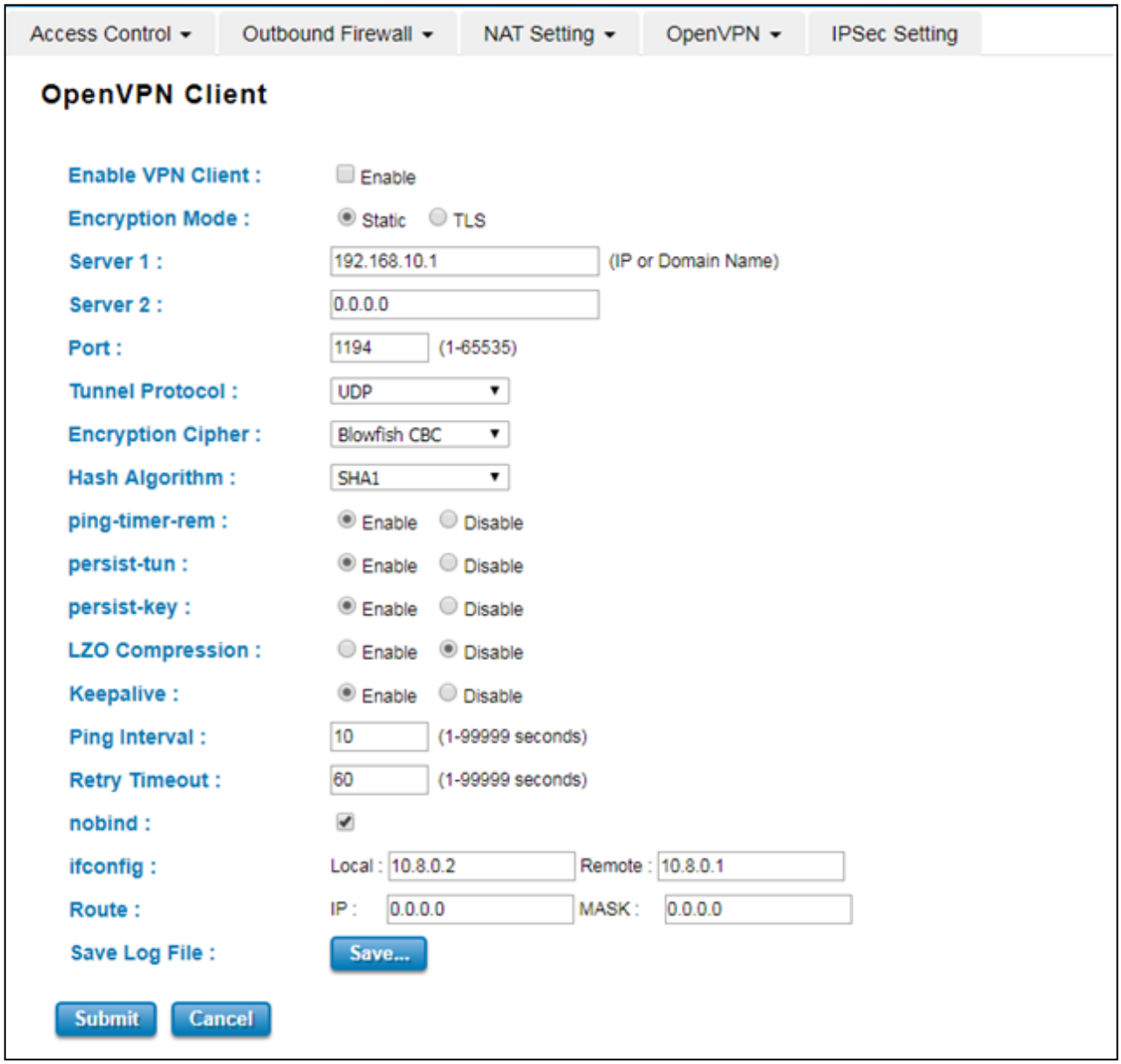
The description of the columns is as below:

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.

3.5.4.2 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:

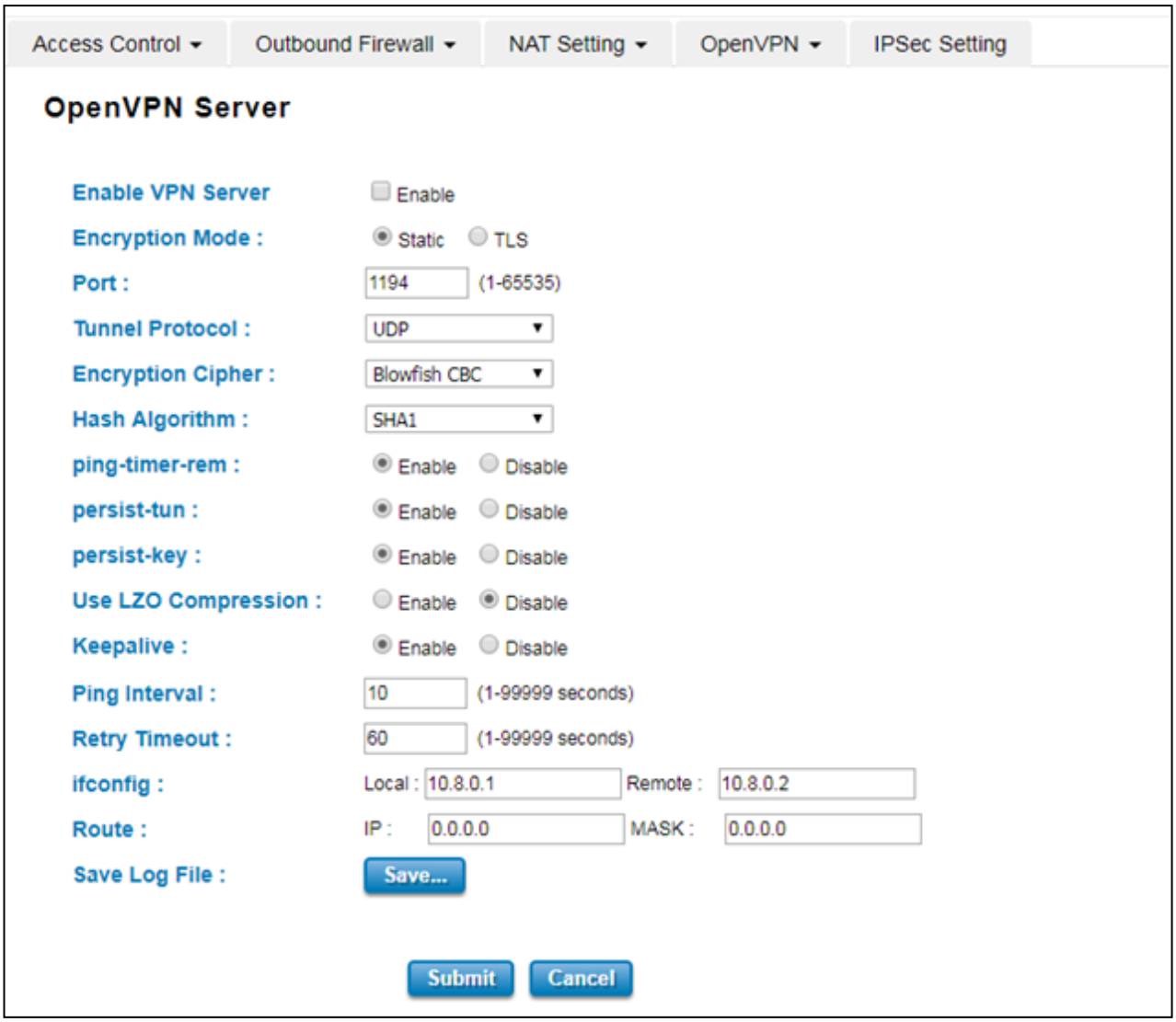
TERMS	DESCRIPTION
Enable VPN Client	Select Enable to activate the VPN Client function
Encryption Mode	Choose the Encryption Mode Static Key: Use a pre-shared static key. TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server 1	Type the IP Address of the VPN Server
Server 2	Type the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

3.5.4.3 OpenVPN Server

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



The description of the columns is as below:

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

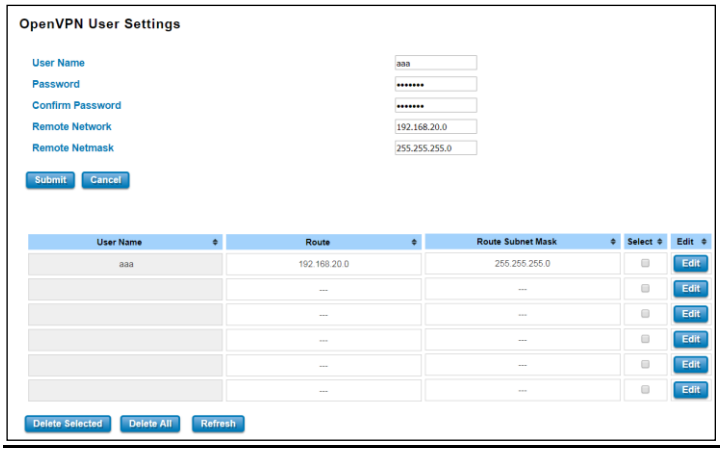
Tunnel Protocol	Choose use TCP or UDP to establish the VPN connection.
Encryption Cipher	Select the encryption cipher from Blowfish to AES in Pull-down menus.
Hash Algorithm	Hash algorithm provides a method of quick access to data, including SHA1, SHA256, SHA512, and MD5
ping-timer-rem	**Default: Enable**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

Click **Submit** to apply the configuration.

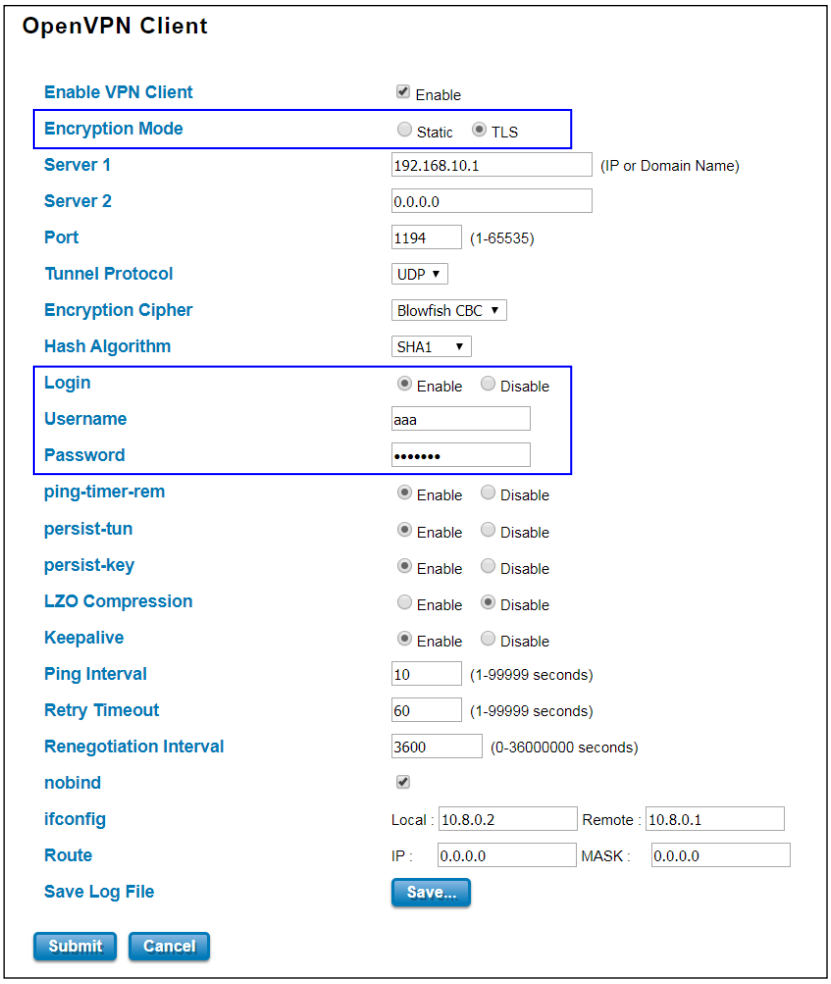
3.5.4.4 OpenVPN User

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

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



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



3.5.4.5 OpenVPN Certificate

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

Key Generation in the device

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

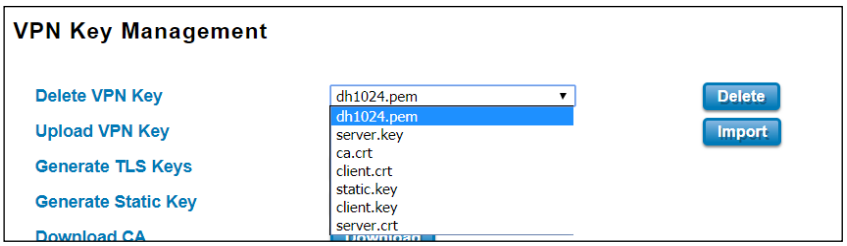
In the latest firmware, the WoMaster Secure Router Switch supports Key generation feature. Click **"Generate"** in **"Generate TLS Keys"** and **"Generate Static Key" in the Open VPN Router**, the system prompts you to wait 30 seconds to generate the key. Click "Yes" to start and wait 30 seconds. After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

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

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

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

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

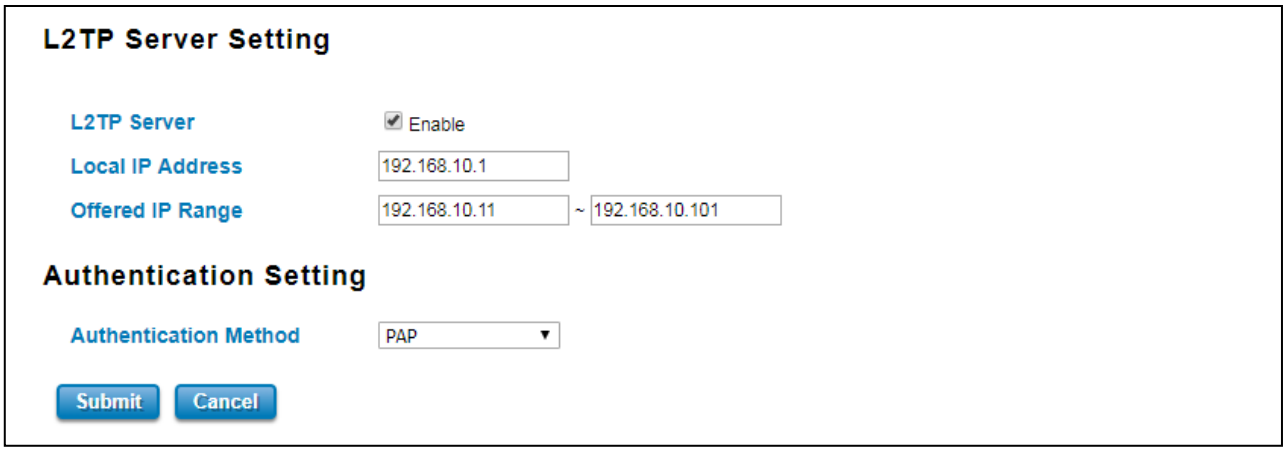


The description of the columns is as below:

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

3.5.5 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.

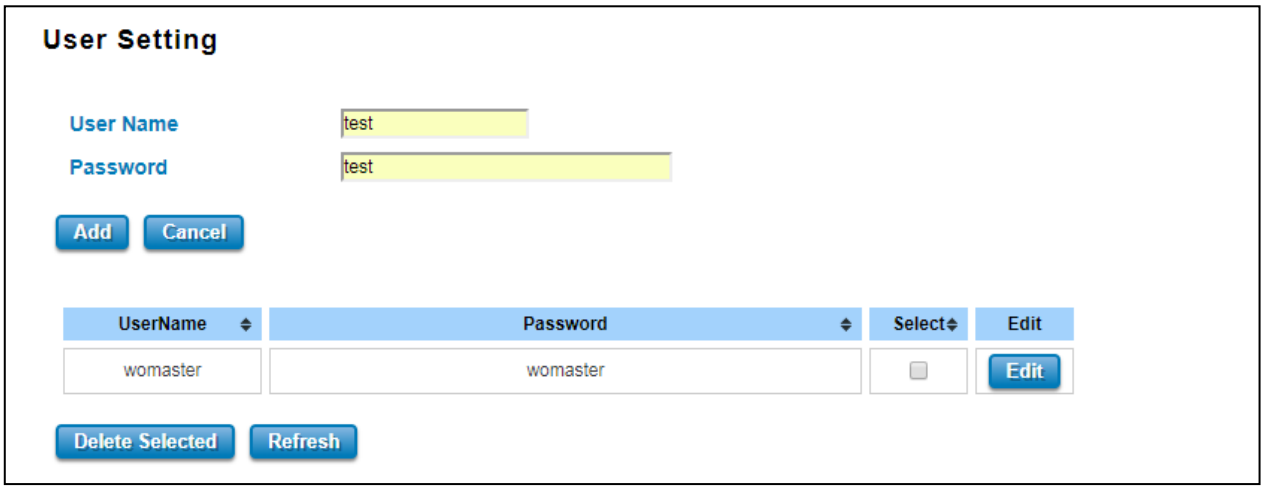


The description of the column is as below:

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:

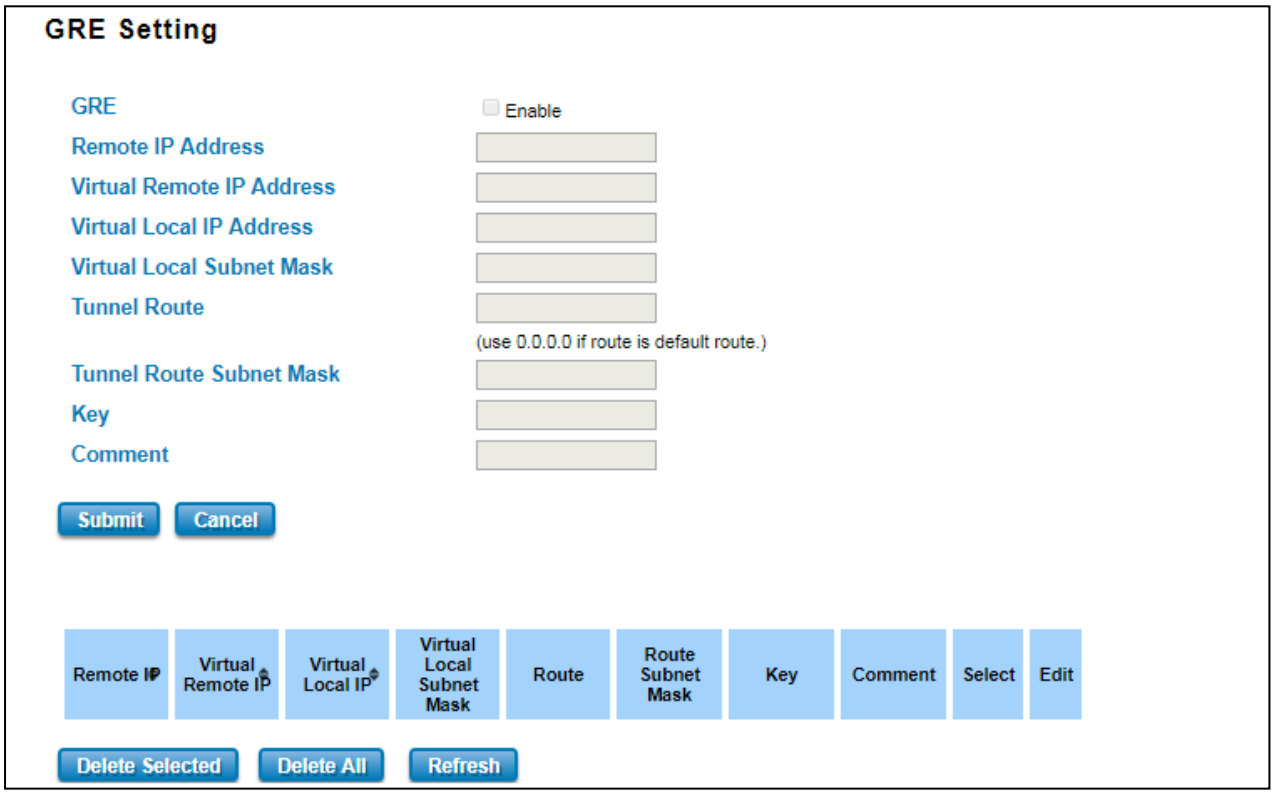
TERMS	DESCRIPTION
User Name	Username for L2TP connection

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.

3.5.6 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.

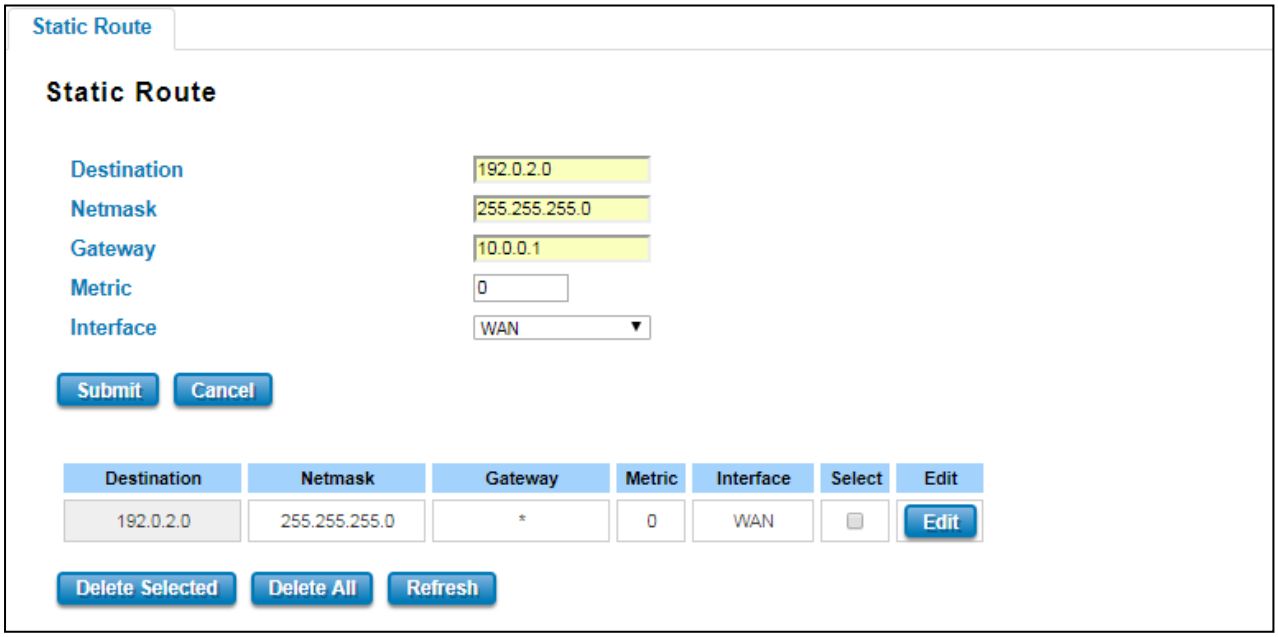
3.6 Routing

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.

3.6.1 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.

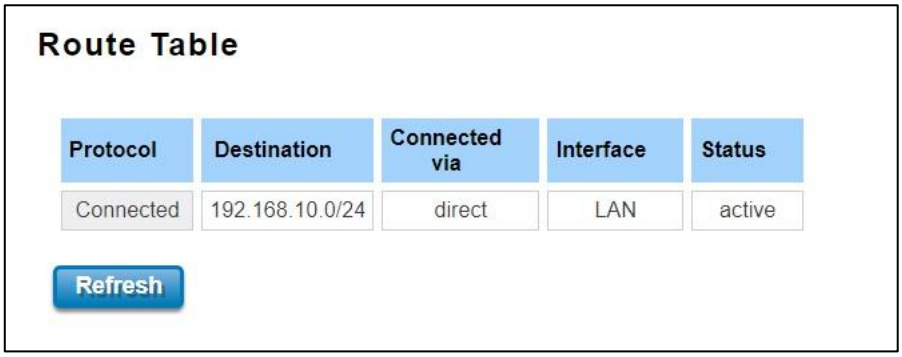


The description of the column is as below:

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.

3.6.2 Route Table



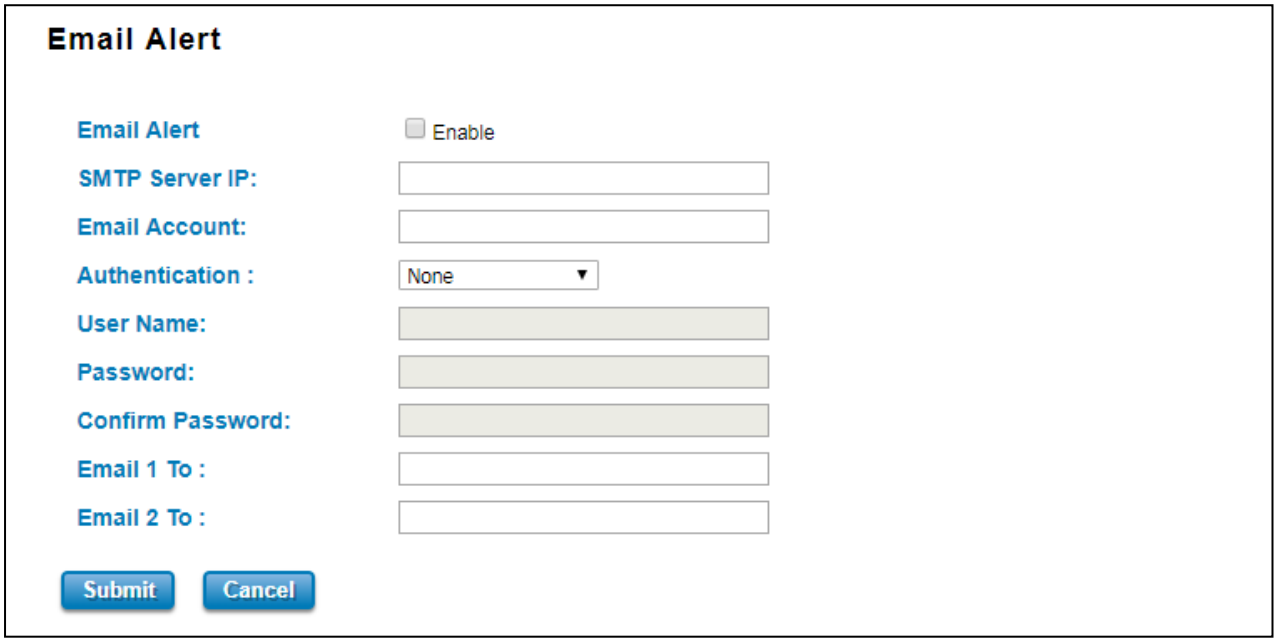
TERMS	DESCRIPTION
Protocol	The field shows the entry is a local interface or learnt from the routing protocol. The **connected** represents for the local interface. The **OSPF** shows the entry is learnt from the routing protocol, OSPF.
Destination	The destination address of static route entry.
Connected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

3.7 Warning

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

3.7.1 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.

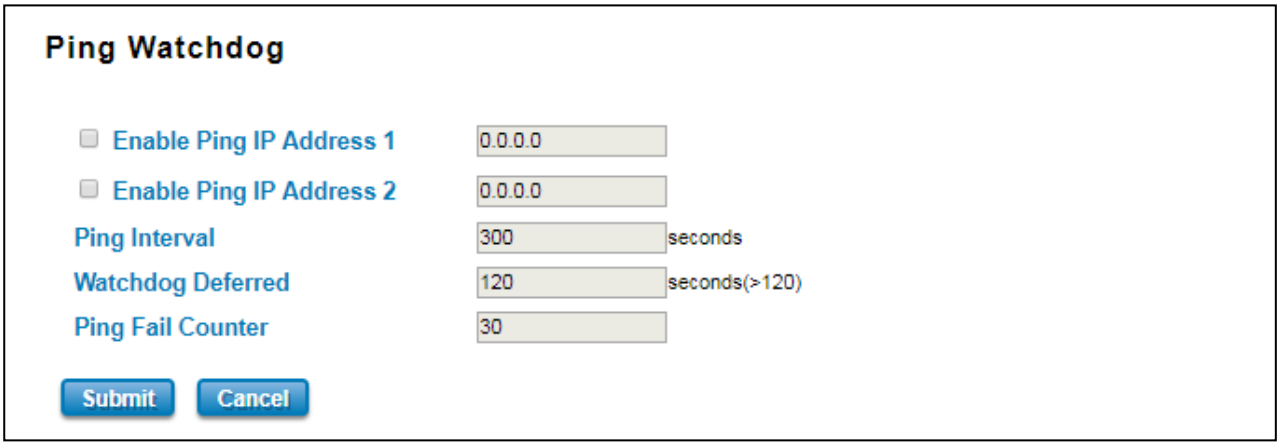


The description of the columns is as below:

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.

3.7.2 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.

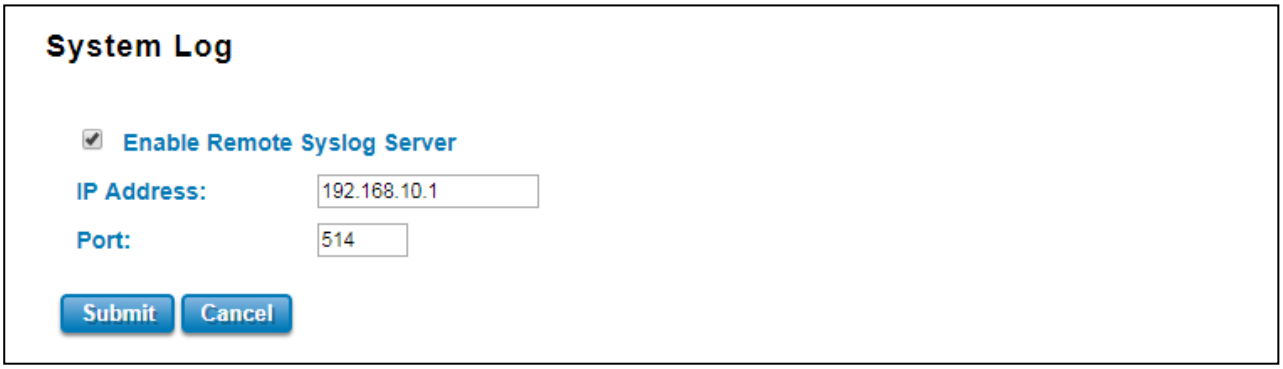
The description of the columns is as below:

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
Ping Interval	**Default: 300 (seconds)** Set the interval timer to Ping the remote device. Every 300 seconds the device will try to ping the target IP.
Watchdog Deferred	**Default: 120 (seconds) >120** The device needs time to boot, the startup delay use to buffer to prevent the device continue to reboot itself.
Ping Fail Counter	**Default: 30** When the remaining Ping Fail Counter reach to 0 or reach the failure count, the device will reboot.

Click **Submit** to apply the configuration.

3.7.3 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

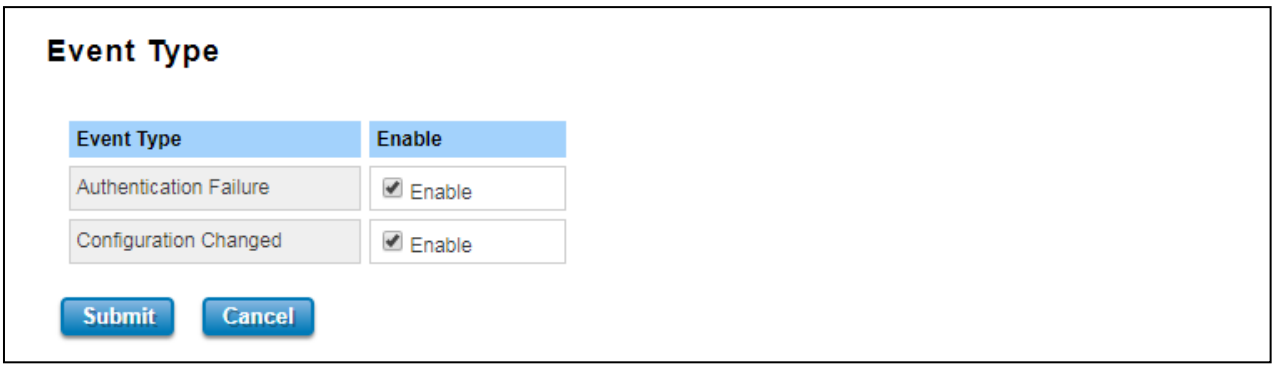
The condition or term described as following table.

TERMS	DESCRIPTION
Enable Remote Syslog Server	Select Enable to enable system log
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.

3.7.4 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.

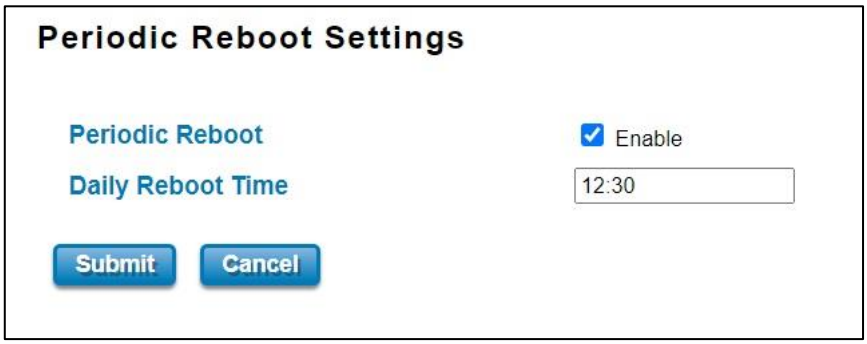


TERMS	DESCRIPTION
Authentication Failure	When the authentication fails, the system will issue the event log/email alert to the system log/SMTP server respectively.
Configuration Changed	When there are any kinds of changing in the configuration, the system will issue the event log/email alert to the system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

Click **Submit** to apply the configuration.

3.7.5 Periodic Reboot

In this page user allowed to reboots the device at a specified time. It can be used as a preventive measure.

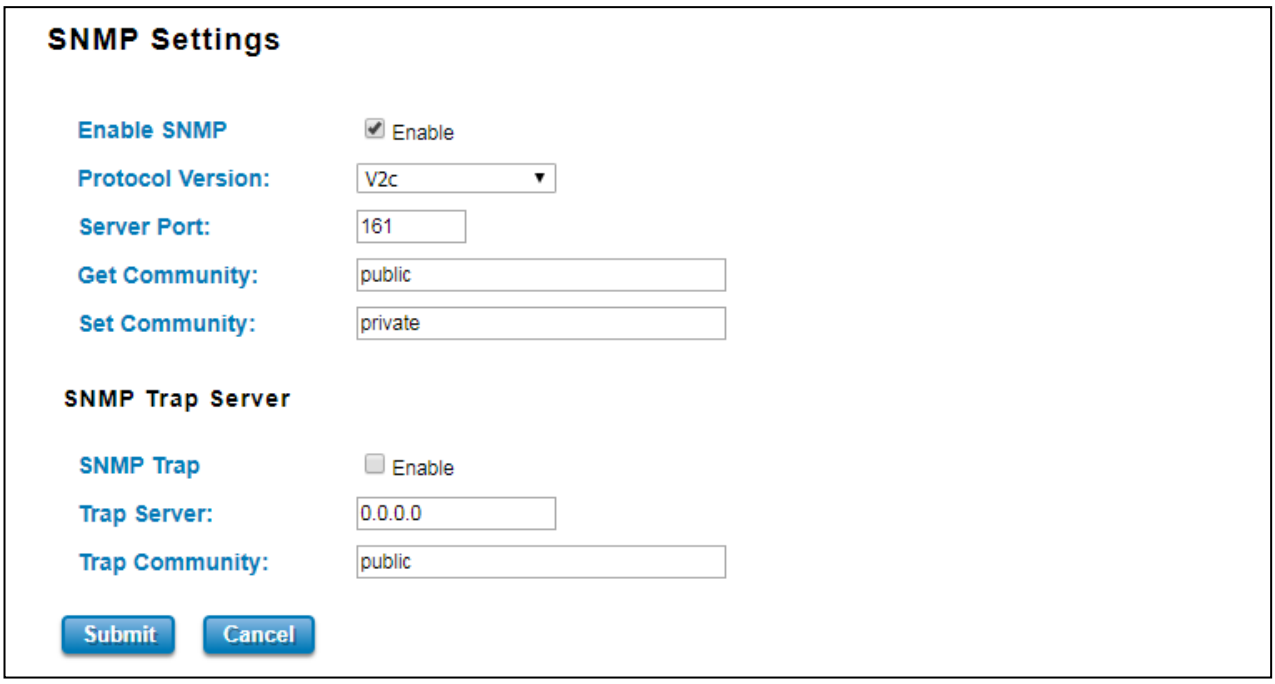


TERMS	DESCRIPTION
Periodic Reboot	Check Enable to activate the function.
Daily Reboot Time	Input HH:MM in 24 time frame.

Click **Submit** to apply the configuration.

3.7.6 SNMP

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



3.7.6.1 SNMP Setting

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

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.

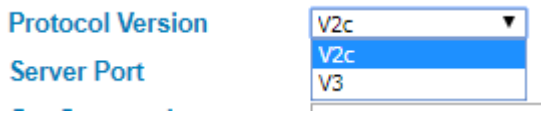
SNMP V3

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.

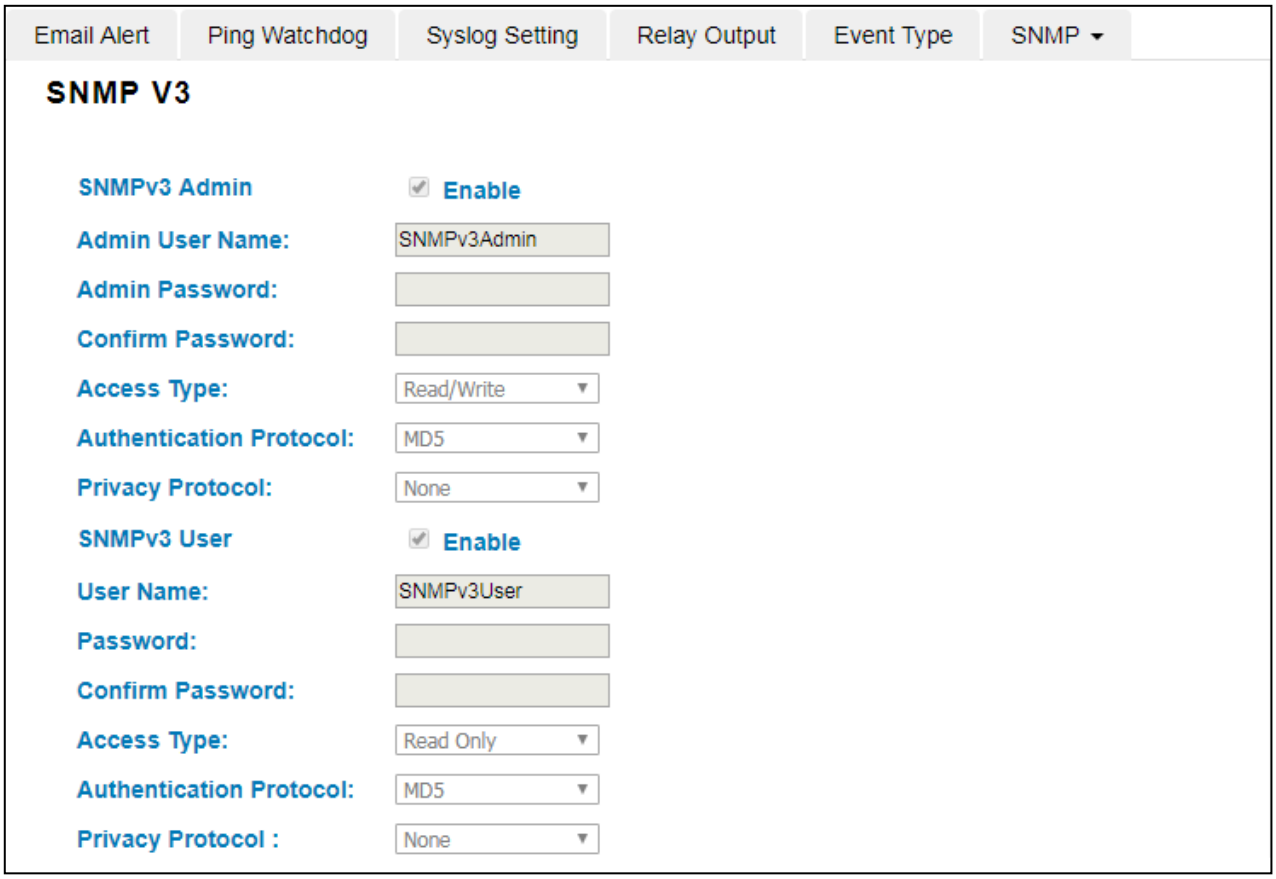
The description of the columns is as below:

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.

3.7.6.2 SNMP V3

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

3.8 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:

3.8.1 Event Logs

3.8.2 ARP Table

3.8.3 Ping

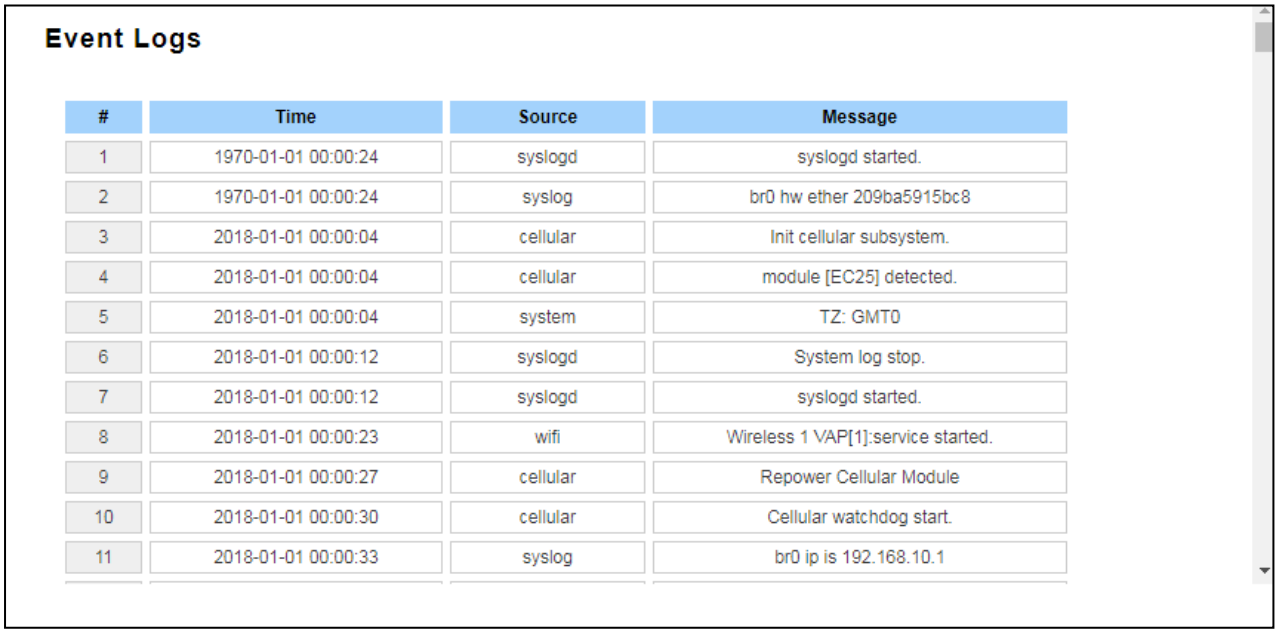
3.8.4 Trace Route

3.8.5 Network Statistic

3.8.6 Association List

3.8.1 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**.

3.8.2 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.

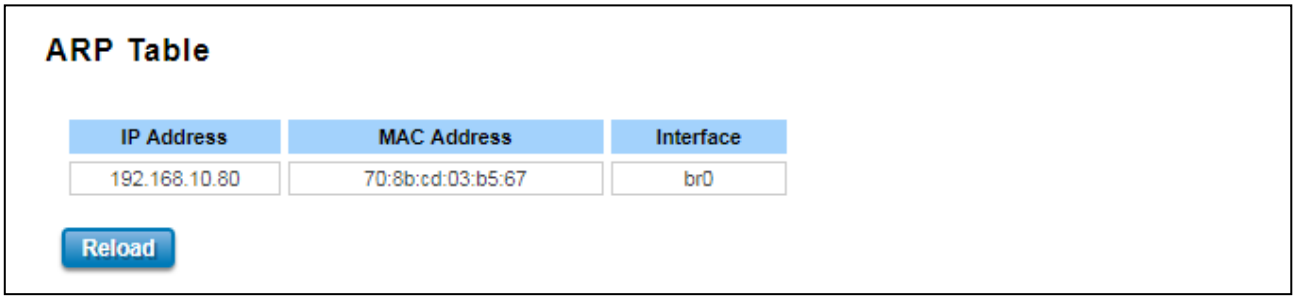
Data Format

Protocol Header:

802.3 + 802.2 LLC + 802.2 snap

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

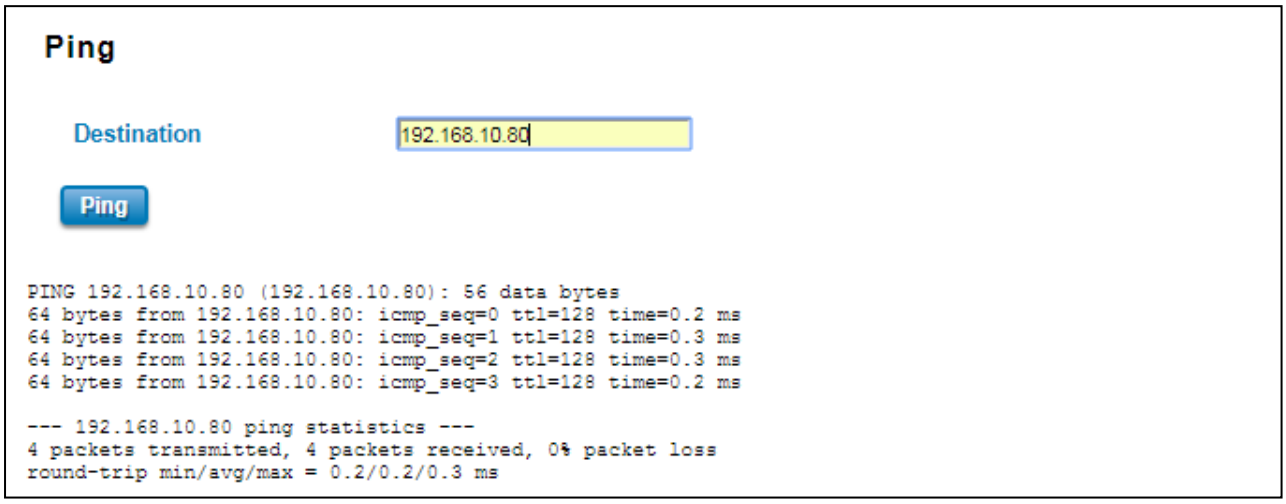
This page shows the routers active ARP table. An ARP table contains recently cached MAC addresses of every immediate device that was communicating with the router.



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

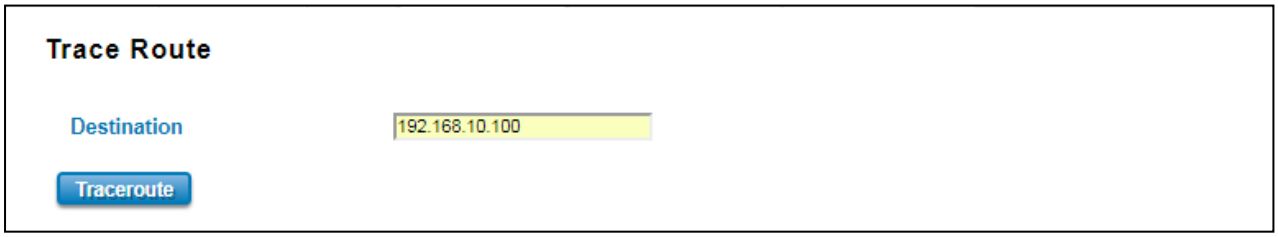
3.8.3 Ping

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.

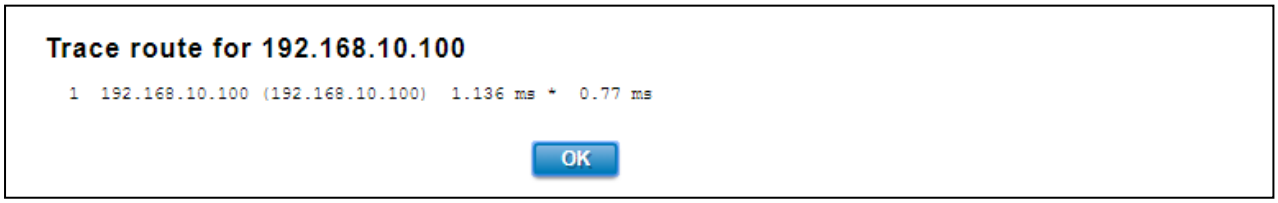


3.8.4 Trace Route

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.

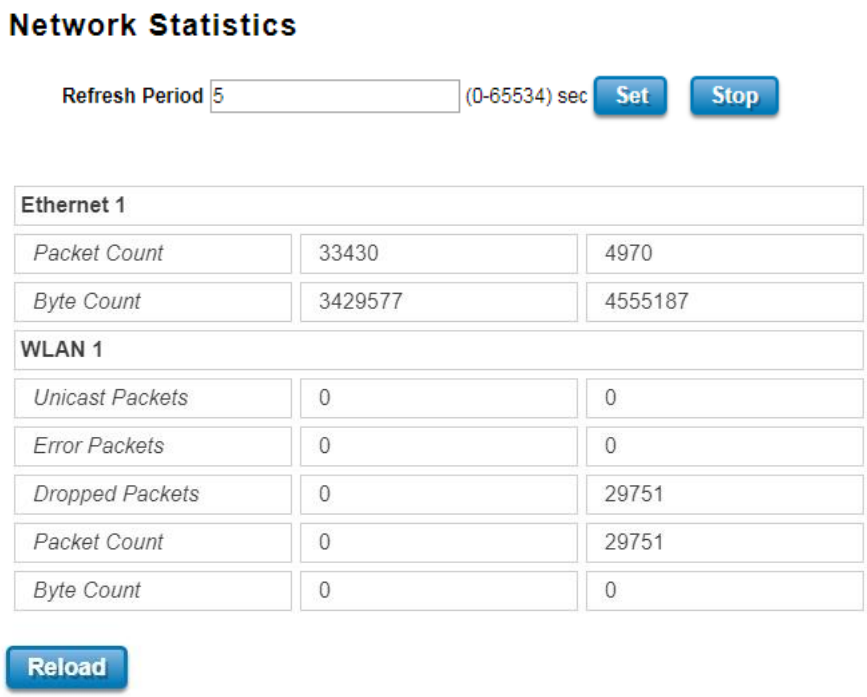


It will start search the route and measuring the transit delays of the packet.



3.8.5 Network Statistics

This section shows about the packet data that transmitted or received regarding the Ethernet and activity.



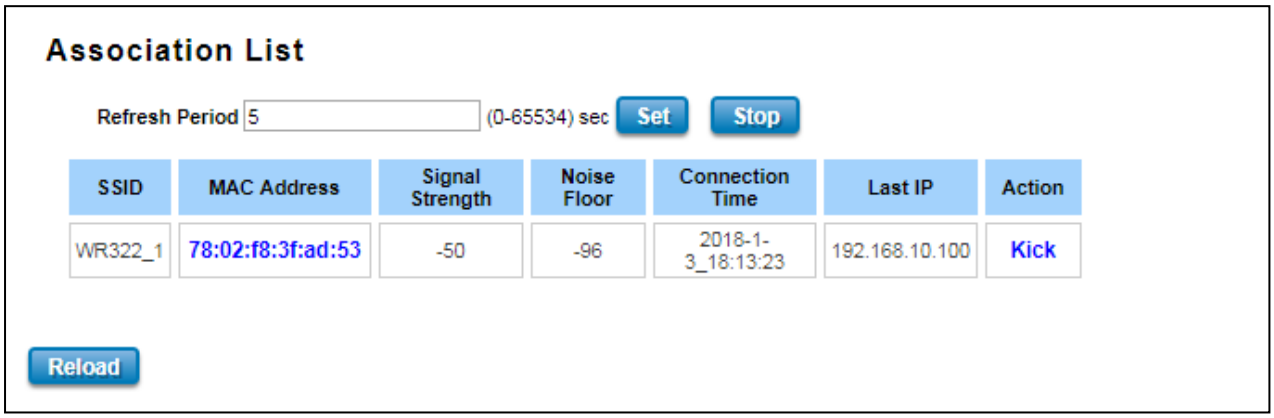
Click on **Reload** to refresh the table.

The description of the columns is as below:

TERMS	DESCRIPTION
Poll Interval	**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.

3.8.6 Association List

This Client Association List displays the current wireless connection status when there is a client that connected to the AP. It shows the SSID, MAC Address, Signal Strength, Noise Floor, Connection Time, Last IP and Action. For the security concern, in this page user can do the security action, such as **Kick** the unexpected user from the wireless networks. This page also provides the refresh function to refresh the list automatically, where user may set the refresh period for refresh the list. Click **Set** to apply the setting, click **Stop** to stop the refresh function.



Click **Reload** to refresh the list.

The description of the columns is as below:

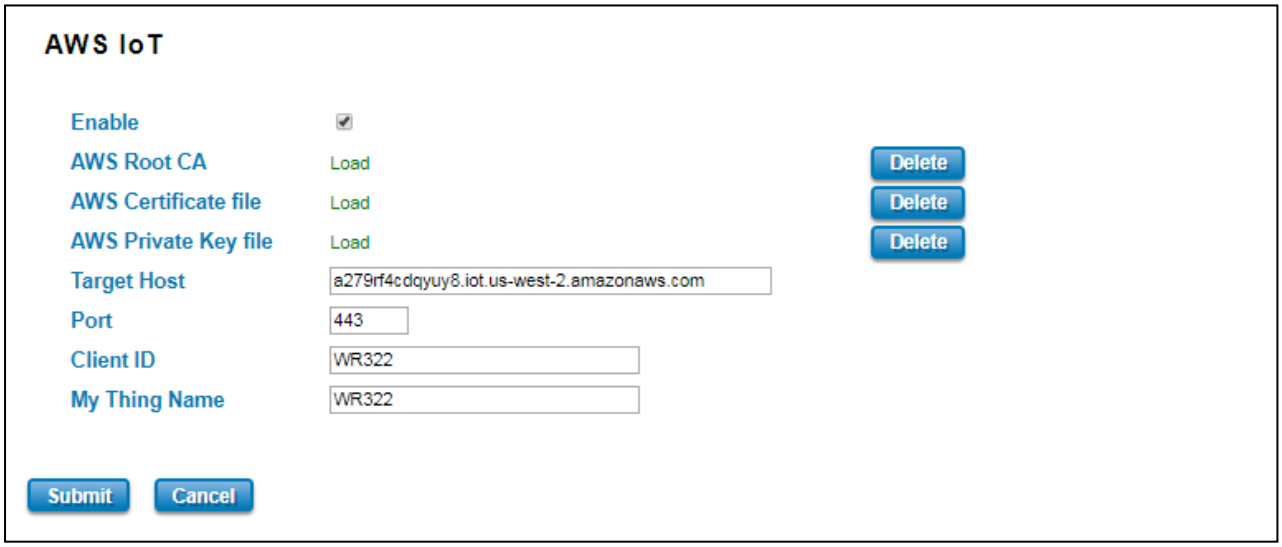
TERMS	DESCRIPTION
SSID	Display the primary name of the SSID that available on the network.
MAC Address	Display the MAC Address that connected to the AP.
Signal Strength	Display the connection signal strength.
Noise Floor	Display the background noise level.
Connection Time	Display the time when the client connected to the AP.
Last IP	Show the IP Address of the wireless client.
Action	In this section user may do an action by **kick** the unexpected wireless client.

3.9 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.

3.9.1 AWS IoT

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



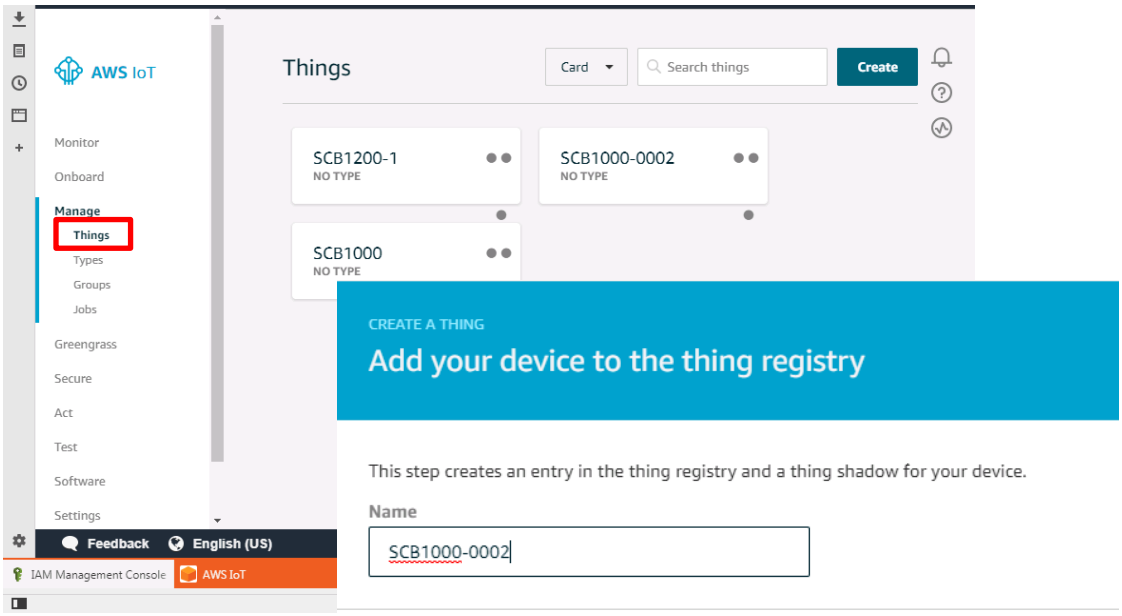
The description of the columns is as below:

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

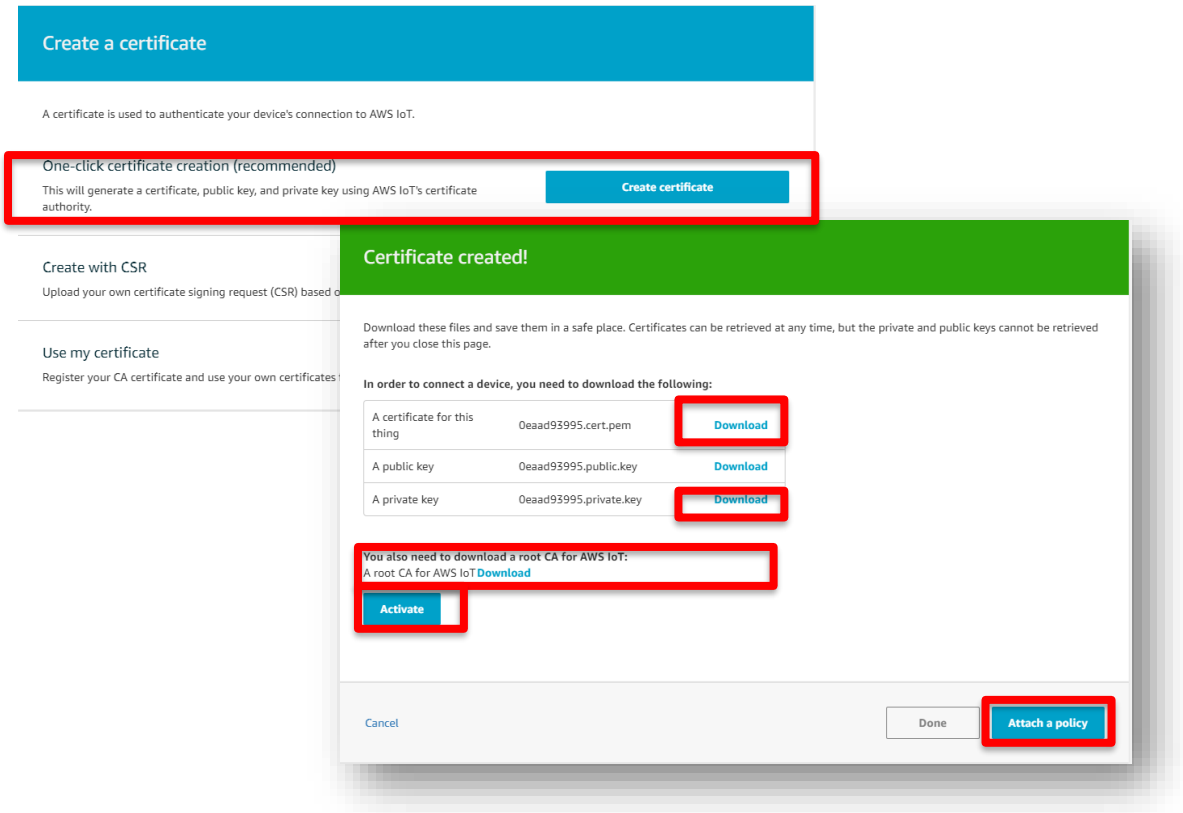
Click **Submit** to apply the configuration.

HOW TO CONNECT THE DEVICE TO AWS

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



- Create and download the key or certificate.



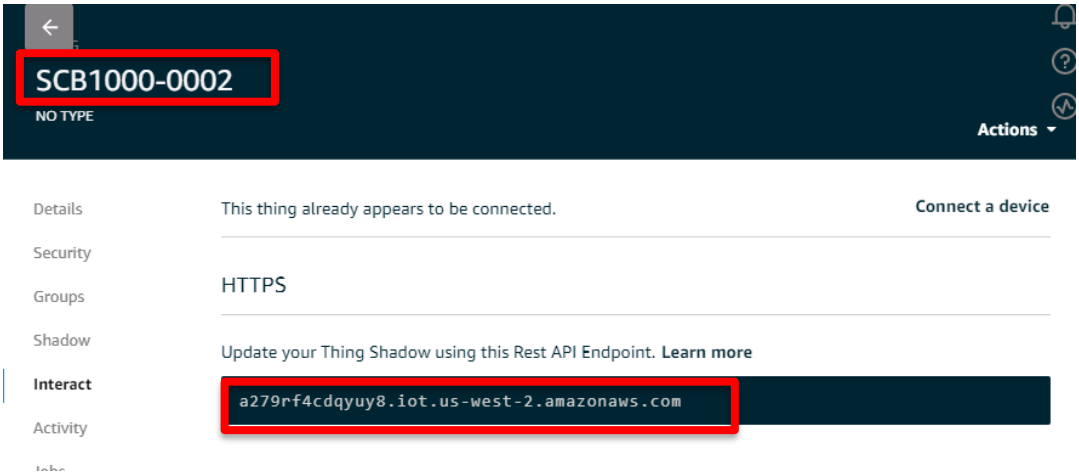
Certificate, private key, root CA is necessary. Public key is used by AWS server to authenticate with private key. The public key and private cannot be downloaded back after the user closes the page. Policy can be added

later.

- Get the Target host to connect with the device.

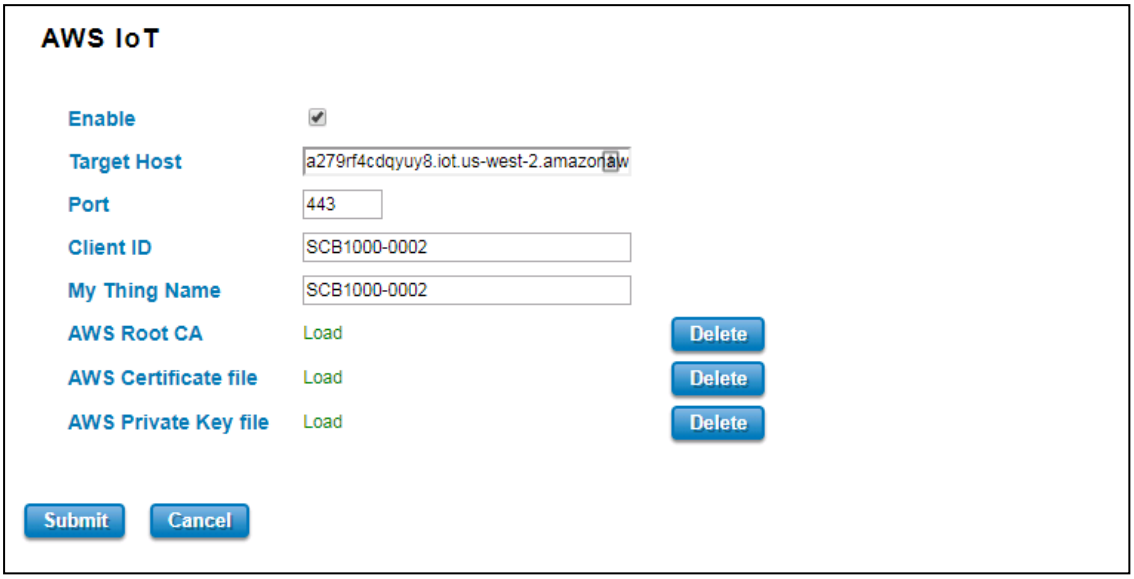
  Go to Manage -> Things -> click the device name -> Click Interact.

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



- Connect the device to AWS.

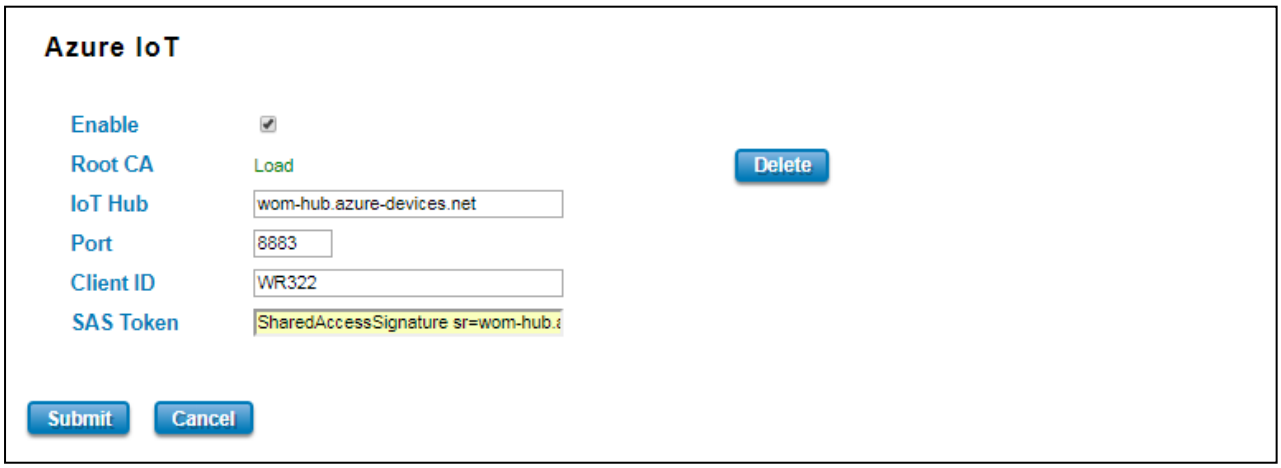
  Copy the link and paste on the Target Host field at the AWS IoT page.



3.9.2 AZURE IoT

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

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



The description of the columns is as below:

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

Click **Submit** to apply the configuration.

HOW TO CONNECT THE DEVICE TO MICROSOFT AZURE

CREATE IOT HUB

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

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

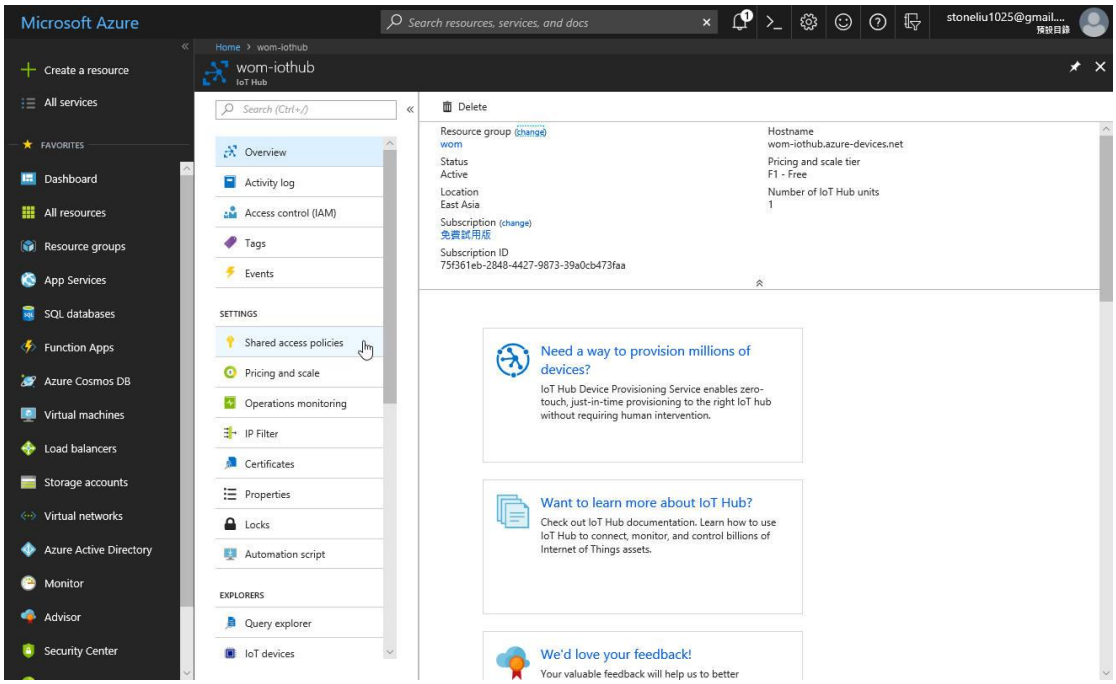
CONFIGURE THE DEVICE AS A MQTT CLIENT

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

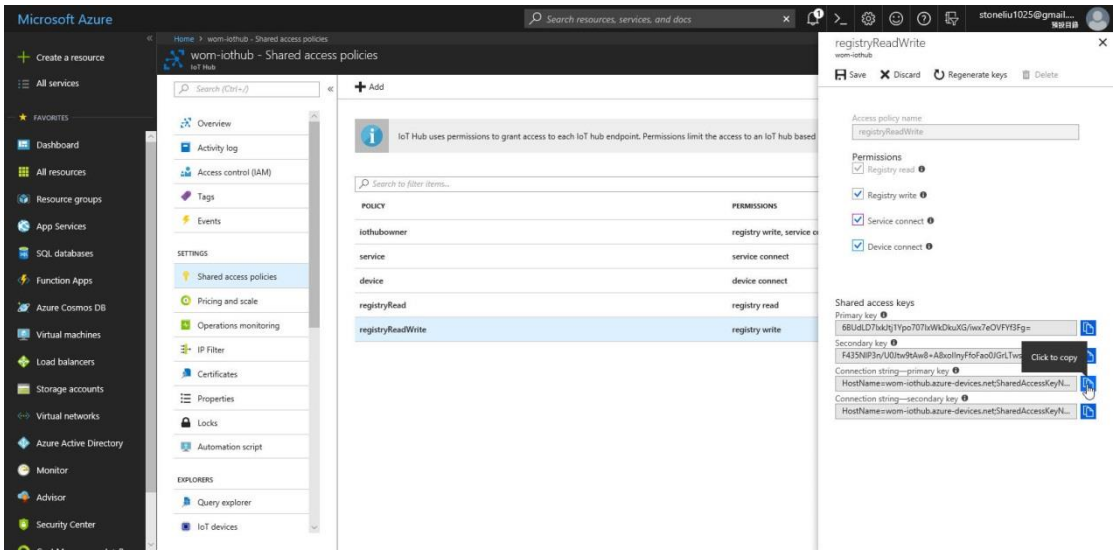
Devices > myCreatedDevice > Shared access policies > iothubowner > Connection string - primary key.

User has to annotate the value of this field.

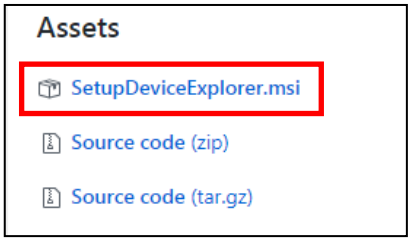
1. Get the connection string. Click the IoT Hub -> Shared access policies.



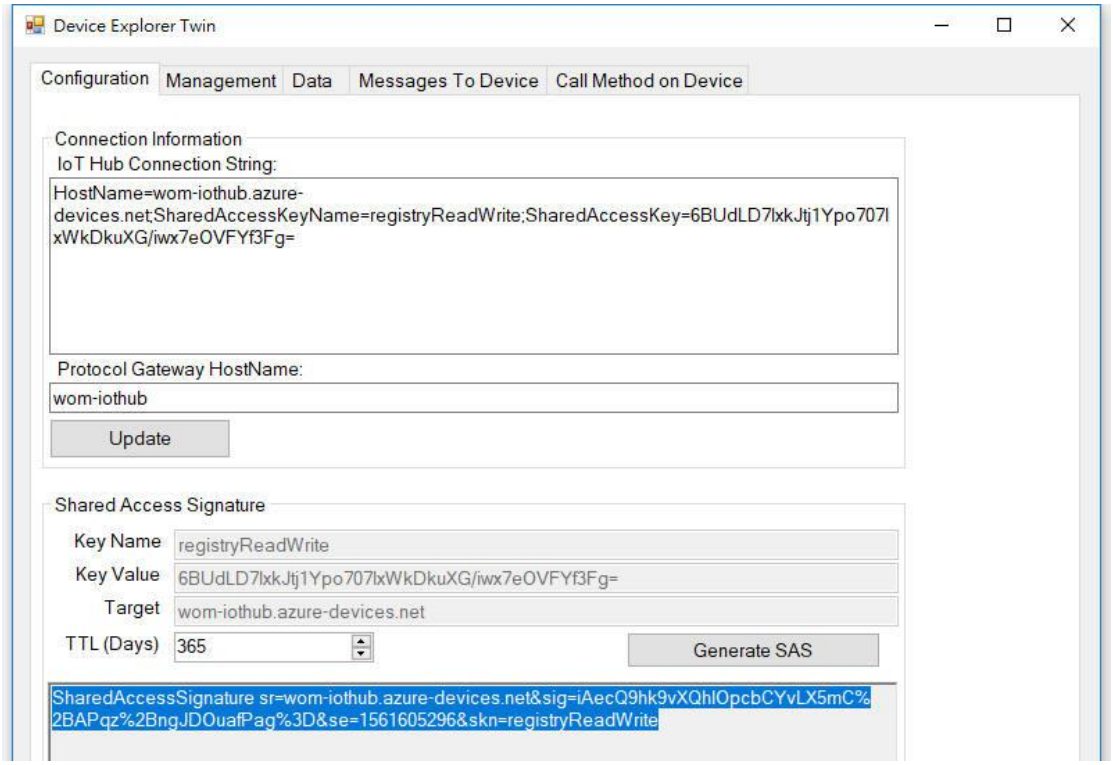
2. Click registryReadWrite -> copy the Connection string---Primary Key.



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



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



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

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

3.9.3 Private IoT

WoMaster provides its own 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.

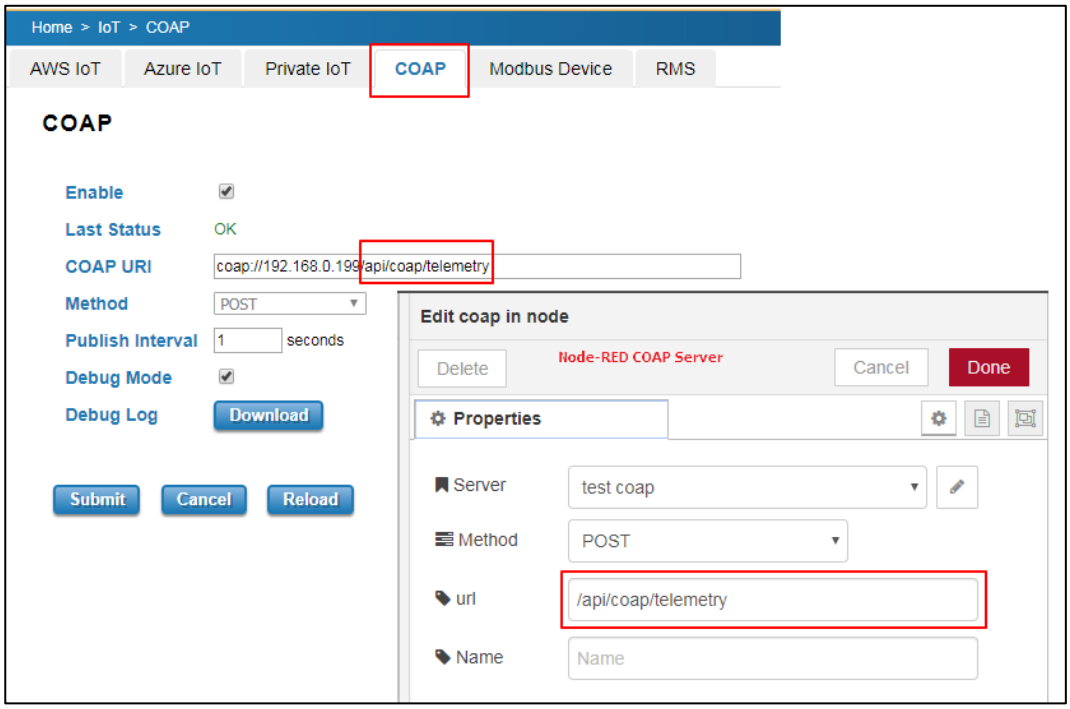
The description of the columns is as below:

TERMS	DESCRIPTION
Enable	Enable the WoM IoT function
Connection Status	Show the status of the connection between the device and ThingsMaster
IoT Server	Enter the address of Private IoT Server.
Port	Enter the port of Private IoT Server.
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 send update on when data changed.
CA Certificate	The function from this certificate file is to create an encrypted MQTT communication. User will get this file when download the ThingsMaster server file. **Note. This field only supports in ThingsMaster v1.1 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.

3.9.4 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:

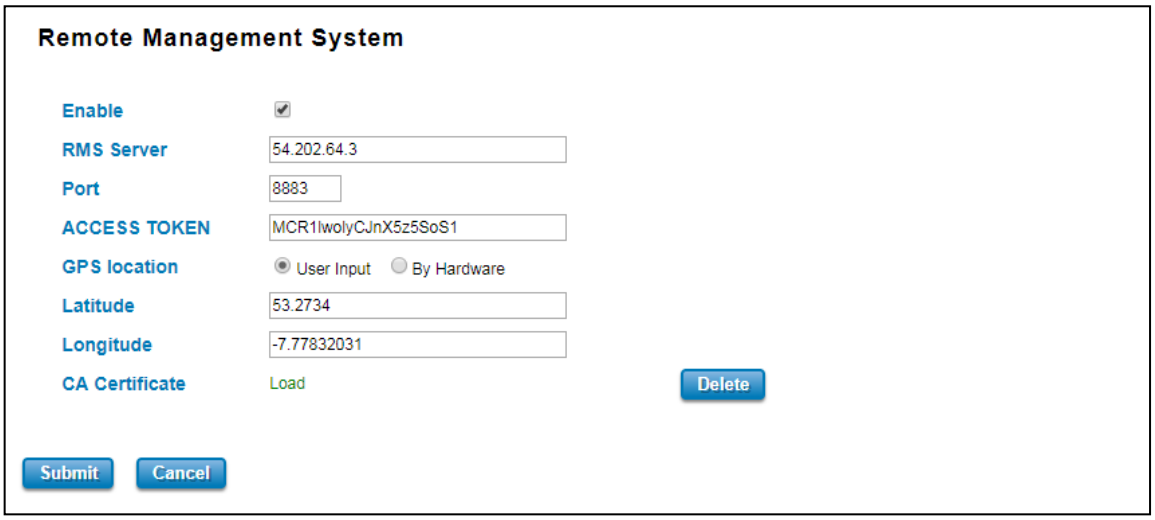
Key is always a string, while value can be either string, Boolean, double or long.

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

3.9.5 RMS/OTA

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

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



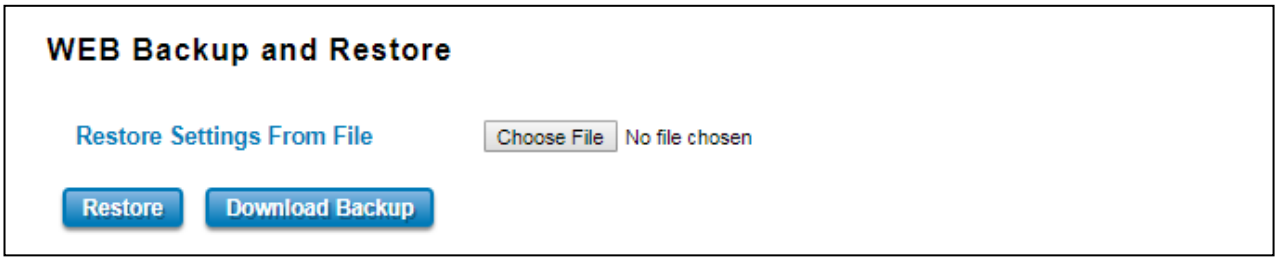
The description of the columns is as below:

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

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

3.10 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.

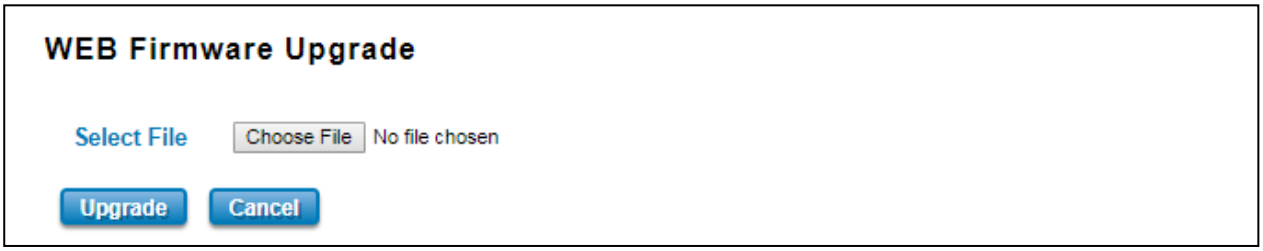


Users can browse the target folder and then type the file name to back-up the configuration. Browse the target folder and select existed configuration file to restore the configuration back to the router. This mode is only provided by Web UI while CLI is not supported. Also, this feature provides the Download Backup button in order to download the backup configuration from the router.

3.11 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.

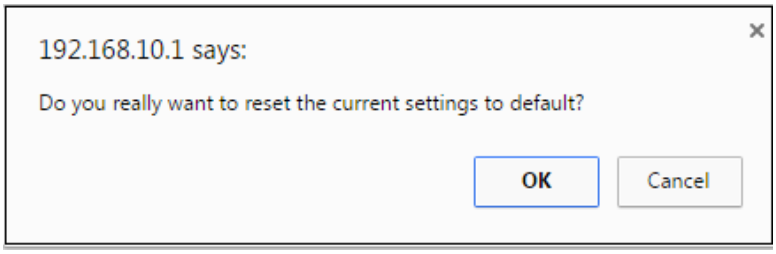


Users can browse the target folder and then type the file name to back-up the configuration. Users also can browse the target folder and select the existed upgrade file. This mode is only provided by Web UI while CLI is not supported.

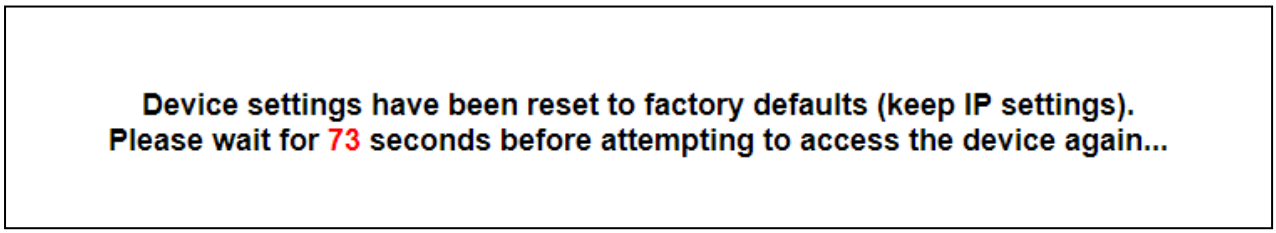
3.12 Reset to Default

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.

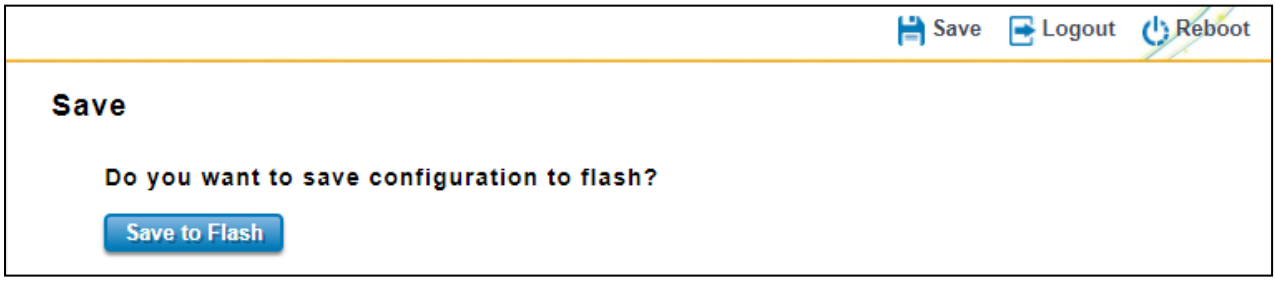


Below is the interface for resetting the device with keep the IP Settings.



3.13 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.



3.14 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.

3.15 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.

4. Revision History

Version	Description	Date	Editor
V1.0	1st released WA212BP User Manual	2020/07/31	Besser