WoMaster

User Manual

COVER

SCB1000/1200 Series

Industrial Smart City Box – PoE + IIoT

Dec.14.2018 V.1.1



WOM ASIA Co., Ltd

1F., No.185-3, Kewang Rd., Longtan Dist., Taoyuan 325, Taiwan

www.womaster.eu

WoMaster

SCB1000/1200 Series

Industrial Smart City Box – PoE + IIoT

User Manual

Copyright Notice

© WoMaster. All rights reserved.

About This Manual

This user manual is intended to guide a professional installer to install and to configure the SCB1000/1200 Series. 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

COVER 1

TABLE OF CONTENTS 3

1. INTRODUCTION 6

1.1 OVERVIEW 6

1.2 MAJOR FEATURES 7

2. HARDWARE INSTALLATION 8

2.1 HARDWARE DIMENSION 8

2.2 INSTALLATION 9

2.3 WIRING THE POWER INPUTS 10

2.4 WIRING THE POWER OUTPUT 11

2.5 WIRING THE ALARM RELAY OUTPUT (DO) 12

2.6 WIRING THE DIGITAL INPUT (DI) LOW: 0~10V, HIGH: 11~30V 12

2.7 AUDIO CONNECTOR 13

2.8 POLE MOUNTING 14

2.8.1 PRE-INSTALLATION GUIDELINES FOR POLE MOUNTING 14

2.8.2 POLE MOUNTING INSTALLATION 14

2.9 ANTENNA 15

2.10 SIM CARD INSTALLATION 16

3. WEB MANAGEMENT CONFIGURATION 17

3.1 SYSTEM 18

3.1.1 INFORMATION 18

3.1.2 USER ACCOUNT 19

3.1.3 IP SETTING 20

3.1.4 DATE AND TIME 21

3.1.5 DHCP SERVER 22

3.2 ETHERNET PORT 24

3.2.1 PORT STATUS 24

3.2.2 PORT SETTING 25

3.2.3 VLAN SETTING 26

3.2.4 RATE CONTROL 28

3.2.5 TRAFFIC CONTROL 29

3.3 POWER OVER ETHERNET 30

3.3.1 PoE STATUS 30

3.3.2 PoE PORT SETTING 31

3.3.3 PoE SCHEDULE *32*
3.3.4 ALIVE CHECK *32*
3.4 QUALITY OF SERVICE (QOS) 33
3.4.1 QoS SETTING *33*
3.4.2 CoS MAPPING *34*
3.4.3 DSCP MAPPING *35*
3.5 MULTICAST 37
3.5.1 IGMP SNOOPING *37*
3.5.2 IGMP QUERY *38*
3.6 REDUNDANCY 39
3.6.1 RSTP STATUS *39*
3.6.2 ERPS SETTINGS *42*
3.6.2.1 ERPS SETTINGS 43
3.6.2.2 ERPS STATUS 45
3.6.3 VRRP *47*
3.7 SERIAL 49
3.8 CELLULAR 53
3.8.1 CELLULAR STATUS *53*
3.8.2 CELLULAR SETTING *55*
3.8.3 SIM SETTING *57*
3.8.4 DDNS SETTING *58*
3.9 GPS 59
3.9.1 GPS STATUS *59*
3.9.2 GPS SETTING *60*
3.10 WIRELESS LAN 61
3.10.1 WLAN STATUS *61*
3.10.2 WLAN SETTING *62*
3.10.3 WLAN SECURITY *73*
3.10.4 ADVANCED *76*
3.10.5 ACCESS CONTROL (AP MODE) *78*
3.10.6 RADIUS SERVER (AP MODE) *79*
3.11 SECURITY 80
3.11.1 ACCESS CONTROL *80*
3.11.2 PORT SECURITY *84*
3.11.3 OUTBOUND FIREWALL *85*
3.11.4 NAT SETTING *89*
3.11.5 OPEN VPN *91*
3.11.6 IPSEC SETTING *96*
3.12 WARNING 99
3.12.1 EMAIL ALERT *99*

3.12.2 PING WATCHDOG *100*
3.12.3 SYSLOG SETTING *101*
3.12.4 RELAY OUTPUT *101*
3.12.5 EVENT TYPE *102*
3.12.6 SNMP *103*
3.13 DIAGNOSTICS **107**
3.13.1 EVENT LOGS *107*
3.13.2 ARP TABLE *108*
3.13.3 PORT STATISTICS *109*
3.13.4 LLDP *109*
3.13.5 PING *110*
3.13.6 BATTERY CHARGE STATUS *111*
3.13.7 ASSOCIATION LIST *112*
3.14 IoT **113**
3.14.1 AWS IoT *113*
3.14.2 AZURE IoT *116*
3.14.3 PRIVATE IoT *119*
3.14.4 MODBUS DEVICE *124*
3.14.5 RMS *125*
3.15 BACKUP AND RESTORE **131**
3.16 FIRMWARE UPGRADE **132**
3.17 RESET TO DEFAULTS **133**
3.18 SAVE **133**
3.19 LOGOUT **134**
3.20 REBOOT **134**
4. REVISION HISTORY **135**

1. INTRODUCTION

1.1 OVERVIEW

The SCB1000/1200 series is an integrated Smart PoE Box for Smart City and Industrial Internet of Thing (IIoT) applications. The SCB1000 equips with two 802.3bt ultra PoE++ and two 802.3at high power PoE+ Ethernet ports for high power IP PTZ Cameras, 2 100/1000Mbps fiber ports for uplink. Besides the external interfaces, there are one gigabit WAN PoE ports, two mPCIe sockets for WIFI or Cellular, BT, LoRa…etc, IIoT expansion module.

The SCB1200 equips with more external interfaces, such as the Serial Interfaces, Digital Input, Digital Output Audio interface to connect the Speaker and Microphone, and additional internal serial port, USB and SD sockets inside the box. These interfaces are used to support each kinds of Industrial Internet of Thing application.

For field installation, the box accepts AC power input, two external 24V DC output and optional PV input for solar panels. We also offer different types solar input kit which includes solar panel, battery and charger board to avoid the risk of power shortage.

Comparing with traditional cabinet, the SCB1200 series can save you a lot of time and effort to assembly the power source, different media interfaces, wireless expansion, and software test also system adjustments. With the assembly-ready Smart City Box, you can directly install the box on roadside power tower, light tower or wall mount on the wall/roof in the field. This is the best solution for the Industrial IoT and Smart City applications.

Model Name	Description
SCB1000-AC	Industrial Smart City Box with 4GT PoE + 2GF, 1GT WAN, AC Input
SCB1200-AC	Industrial Smart City Box with 4GT PoE + 2GF, 1GT WAN, IIoT interfaces, AC Input (IIoT Interfaces: External 1xCOM,2xDI,2xDO,Voice; Internal 1GT WAN, 1xCOM, 1xUSB, 1xSD)
SCB1000-AC+Battery	Industrial Smart City Box with 4GT PoE + 2GF, 1GT WAN, AC Input, Battery Kit (Battery Kit: Typ. 48V/2.5AH Battery and AC charger board pre-installed inside.)
SCB1200-AC+Battery	Industrial Smart City Box with 4GT PoE + 2GF, 1GT WAN, IIoT interfaces, AC Input, Battery Kit (Battery Kit: Typ. 48V/2.5AH Battery and AC charger board pre-installed inside.)
SCB1000-AC+BasicSolar (By request)	Industrial Smart City Box with 4GT PoE + 2GF, 1GT WAN, AC Input, Basic Solar Kit (Basic Solar Kit: Typ. 48V/2.5AH Battery, AC/PV charger board & MC4 connector pre-installed inside.)
SCB1200-AC+BasicSolar (By request)	Industrial Smart City Box with 4GT PoE + 2GF, 1GT WAN, IIoT interfaces, AC Input, Basic Solar Kit (Basic Solar Kit: Typ. 48V/2.5AH Battery, AC/PV charger board & MC4 connector pre-installed inside.)

1.2 MAJOR FEATURES

Below are the major features of SCB1000/1200 Series:

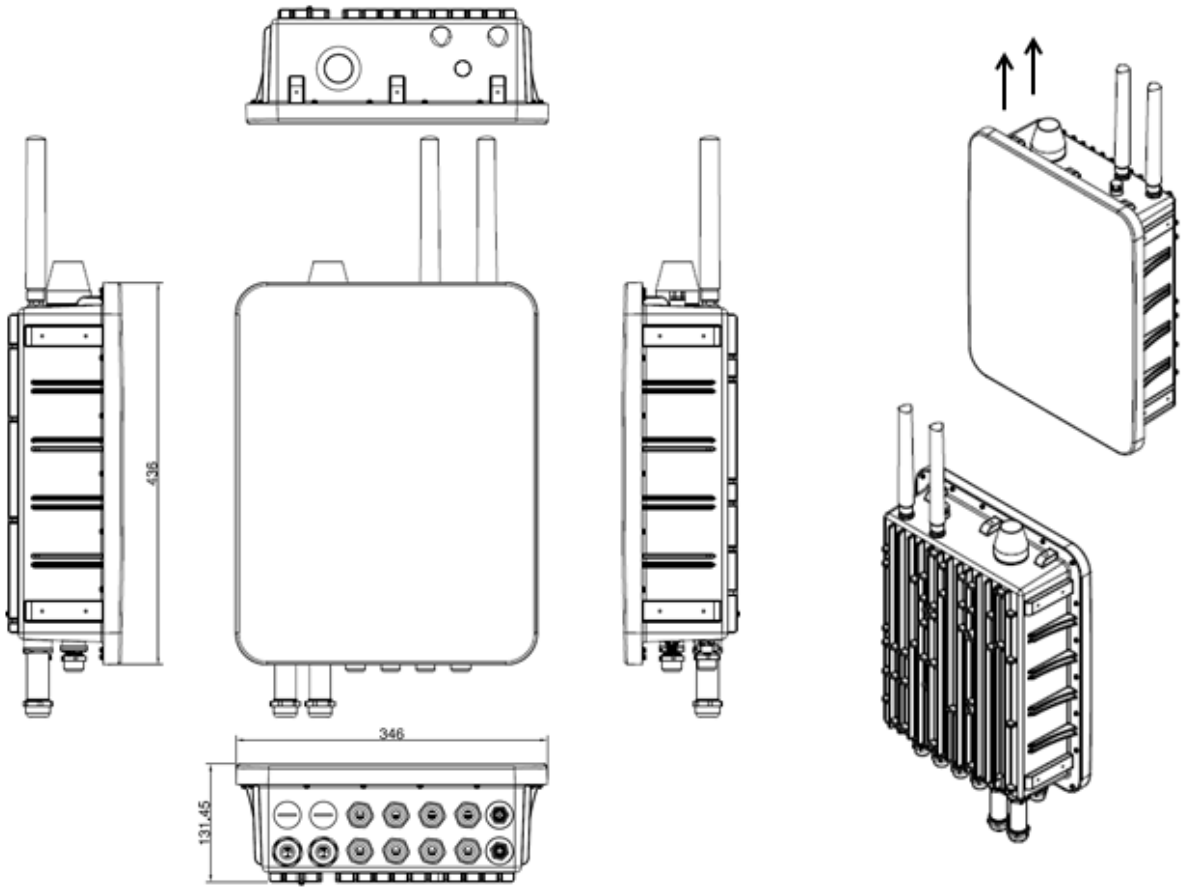
- 4 x 10/100/1000Base-T RJ45, M20 Cable Gland
  - 2 x PoE 802.3af/at,
  - 2 x PoE 802.3bt
- 2 x 100/1000Base-X SFP, M25 Cable Gland
- 1 x 10/100/1000Base-T RJ45, 802.3at/af PoE, Inside the box for Internal installation
- Advanced Network Management features:
  - IPv4, DDNS, SNMP v1/v2c/v3/Trap, LLDP, DHCP server/client, TFTP, System Log, Watchdog on IP
  - SCB1200: DI, DO, Serial, USB for Firmware upgrade, Configuration backup & restore
  - SCB Wireless Expansion: WLAN AP/CPE mode, ERPS failure to LTE redundant (P2).
- Traffic Management: 802.1Q VLAN, QoS, IGMP Snooping, Rate control, up to 10K Jumbo Frame, NAT Routing, Traffic shaping
- Redundancy Protocol: STP/RSTP, ITU-T G.8032 ERPSv2, VRRP
- Optional Wireless Expansion:
  - SCB LTE Module and Antenna Kit
    - LTE Cat.4 Cellular Module
    - LTE+GPS Antenna on the top of the box
    - 150 UL, 50M DL, FDD/TDD-LTE
  - SCB Industrial WLAN Module
    - N-Type Antenna Socket on the top of the box
    - 5G/2.4G 802.11ac/n WiFi 2T2R
- Advanced Security system by Port Security, HTTPs, SSH, Firewall (Inbound/outbound), DMZ, Port Forwarding
- VPN: IPSec and OpenVPN
- Event Notifications through E-mail, SNMP trap, and SysLog.
- Traffic Management features: NAT Routing and Traffic shaping.
- CLI interface, Web, SNMP for network Management
- Multiple event relay output for enhanced alarm control
- EN50121-4 for Industrial IoT, ITS, Railway track side application.
- IP67 Aluminum die-casting Body + Radome-ABS Cover
- Wide range operating temperature -40~60˚C
- IP67 waterproof enclosure

2. HARDWARE INSTALLATION

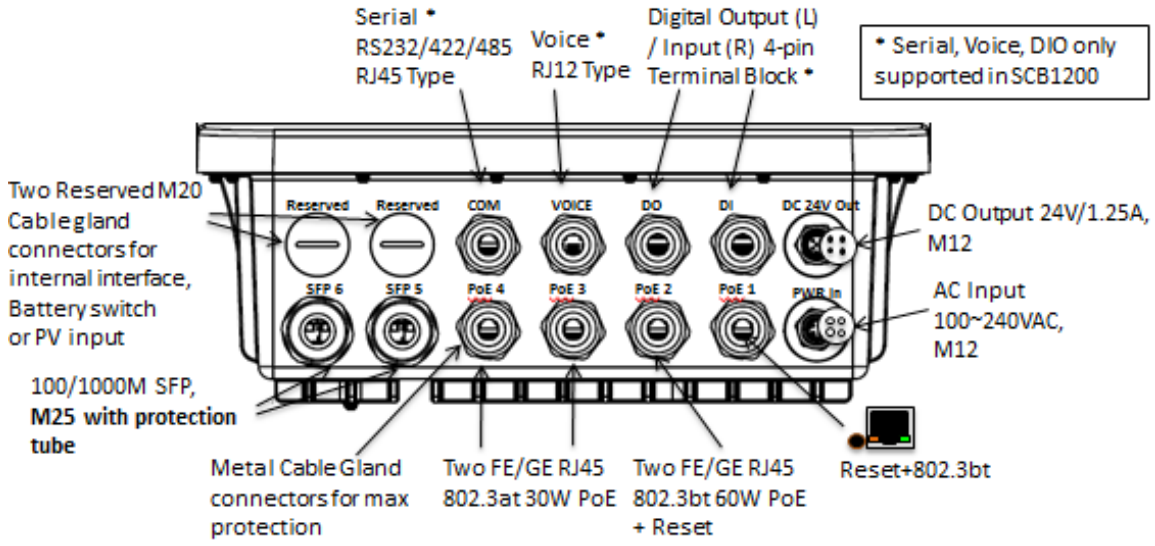
This chapter introduces hardware and contains information on installation and configuration procedures.

2.1 HARDWARE DIMENSION

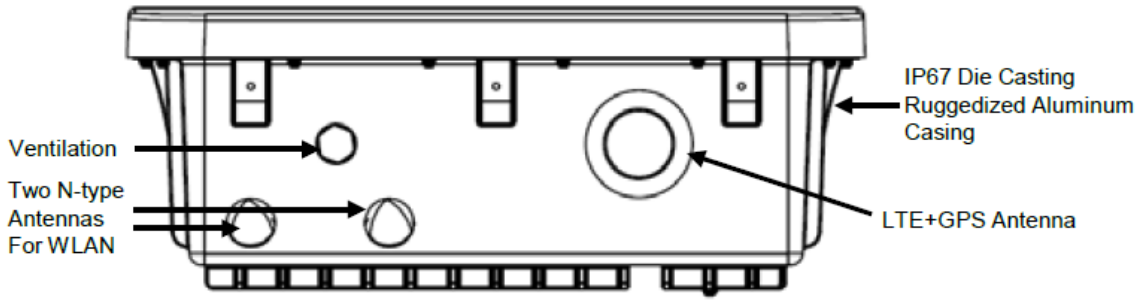
Dimensions of SCB1000/1200 Series: 346 x 406 x 142mm (W x H x D) / without Wall-mount poles



Front Panel



Back Panel



2.2 INSTALLATION

After unpack the package, follow the steps below in order to properly connect the device. For better Wi-Fi performance, put the device in a clearly visible spot.

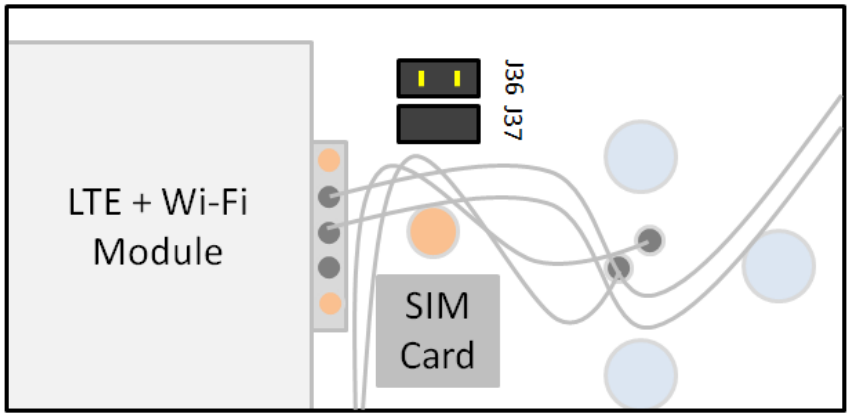
1. First, assemble the SCB by attaching the necessary Wi-Fi antennas and inserting the LTE SIM card.
2. To power up the Smart City Box, please use the power input cable that included in the package.
3. Since SCB1200 Series uses the M20 waterproof interface. Open the M20 interface, pass the cable through the M20 interface and user can start install the cable. This procedure must be applied to install all of the cables such as RJ-45, RJ-12, SFP transceiver, DO, DI and etc.

WARNING!

1. Do not use the **console connector (J19)** inside the box; it is only reserved for device maintenance by WoMaster technician. Only the authorized technicians are allowed to Use the console connector.



2. Please do not change the **power charger board jumper (J36 & J37 inside the box)**, change the jumper position will cause damaged.



WARNING, THE WARRANTY IS NOT VALID IF:

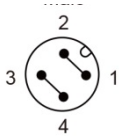
1. Open the cover without consent. Only the authorized technicians are allowed to open the cover for internal maintenance.

(Exception: User can open the SCB cover only for changing the audio jumper (2.7) and installing the LTE SIM card (2.10).

2. Install any non-certificated LTE and wireless modules.
3. If the device is damaged due to the restricted behavior.
4. The device is assembled in an unprotected environment.

2.3 WIRING THE POWER INPUTS

The power input is supported with AC model, 100~240 VAC.

Male M12 Connector	Pin	Description	Pin Color
 PWR Input L/V+ N/V-	1	V+	Red
	2		
	3	V-	Blue
	4		

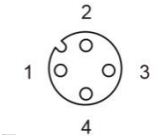
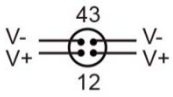
Tighten the nuts to prevent the loosening of M12 connectors.



Plug the power connector to a power source then the SCB is powered up. For European power socket, the adapter is provided.



2.4 WIRING THE POWER OUTPUT

Female M12 Connector	Power	Pin	Description	Pin Color
 DC24V Output 	1	2	V+	Brown
		3	V-	Black
	2	1	V+	White
		4	V-	Blue

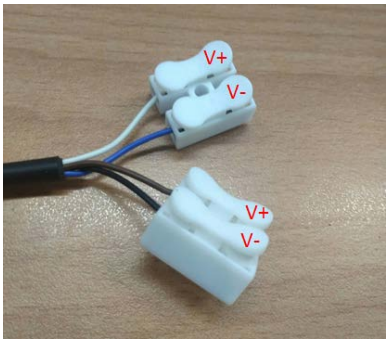
The Smart City Box Series is supported with Dual Power Outputs, 4-pin M12 power connector. This power output in this Demo Box is used to power up the CO2, temperature and humidity sensor also the alarm. And it can deliver maximum 24VDC/1.25A power output.

How to install the power output cable

1. Tighten the nuts to prevent the loosening of M12 connectors.

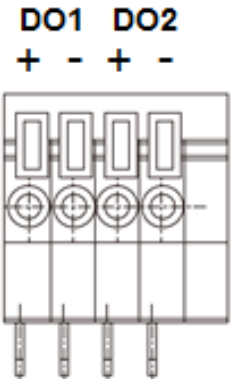


2. On the other side of the cable it has 4 pins that connected to two connectors. Below is the appearance.



2.5 WIRING THE ALARM RELAY OUTPUT (DO)

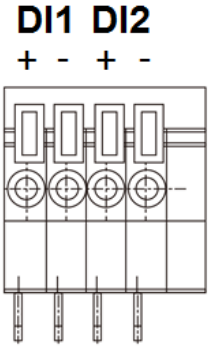
The relay output contacts are located on the front panel of the router. The relay output consists of the 2-pin terminal block connector that used to detect user-configured events. The two wires attached to the fault contacts form a close circuit when a user-configured event is triggered. If a user-configured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



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

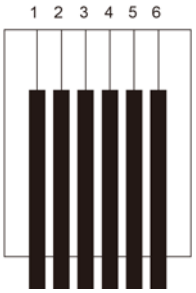
2.6 WIRING THE DIGITAL INPUT (DI) Low: 0~10V, High: 11~30V

4-pin terminal block is provided to wire the DI; the push lock connection is supported for installing the wire easily. Push the orange panel to open the contact, insert the positive and negative wires into the + and - contact and release it to lock the wire after the DI wire is inserted.



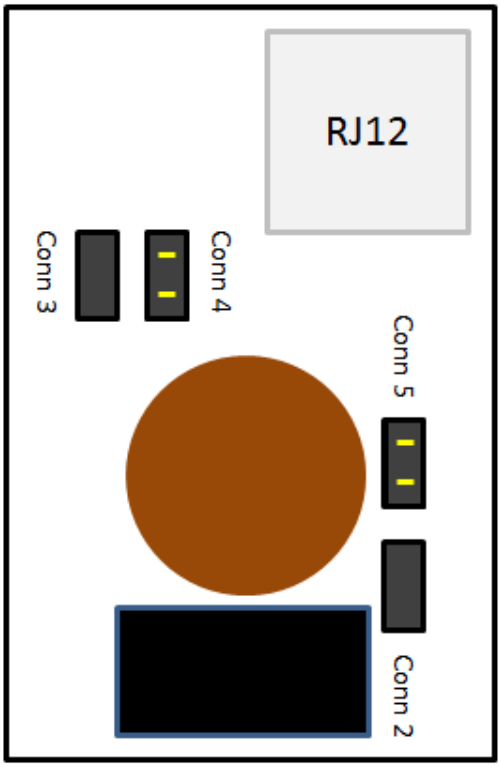
2.7 AUDIO CONNECTOR

SCB is provided with audio feature. The audio connector, it uses the RJ12 for any kind of audio adapter. To use this feature connect the RJ12 to the Voice Port. (Refer to the Appearance part).



Pin	Description
1	AGND
2	Mic L
3	Speaker Amp
4	Speaker
5	Mic R
6	Not Used

Audio Jumper (Inside the box)



Status	Description
Jumper on Conn 2, 3	Audio Amplifier Output Mode
Jumper on Conn 4, 5	Audio Codec Output Mode
	With Jumper
	Without Jumper

NOTE:

1. User needs to open the box to see the interface above.
2. Every time user changes the jumper, please make sure if the SCB is not in the powered mode.

2.8 POLE MOUNTING

The Smart City Box Series must be mounted to a pole. This section provides details for the installation.

2.8.1 PRE-INSTALLATION GUIDELINES FOR POLE MOUNTING

When installing the SCB to the pole mounting, please follow these guidelines:

• When selecting the site, consider accessibility, availability of power, signal and network cable connections, and the possibility of future expansion

• Install the SCB Series in a location where access is unobstructed

• The SCB Series operation area must have adequate ventilation

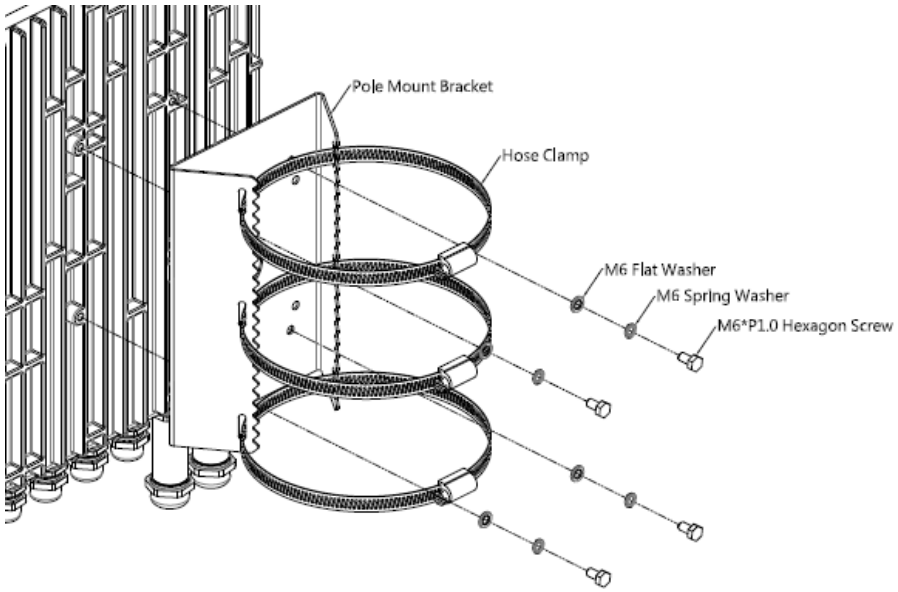
• Do not install the SCB Series on the floor, install only on a pole.

2.8.2 POLE MOUNTING INSTALLATION

The SCB Series has been designed to operate in a vertical position with the antennas are facing up and all of the connectors are facing down. User will find the required pole mount bracket to mount the SCB on a pole.

Pole Mounting kits include:

- 1 x Pole Mount Bracket
- 3 x Hose Clamps
- 4 x M6 Flat Washer
- 4 x M6 Spring Washer
- 4 x M6*P1.0 Hexagon Screw



1. Attach the pol mount bracket to the Smart City Box using the Hexagon screws. Screws provided are for general use and could not be valid for every surface. Screw all of the screws tightly.

2. Attach the bracket to the mast or pole by using the hose clamps.

2.9 ANTENNA

SCB1000/1200 Series is supported with up to 3 antenna sockets, where 3G/LTE, GPS, and Wi-Fi antennas are supported. The 3G and the GPS antennas are installed on the router, for the Wi-Fi antennas are connected to the SCB by screwing the antenna to the SMA connector on the front panel of the router.

WiFi Antenna



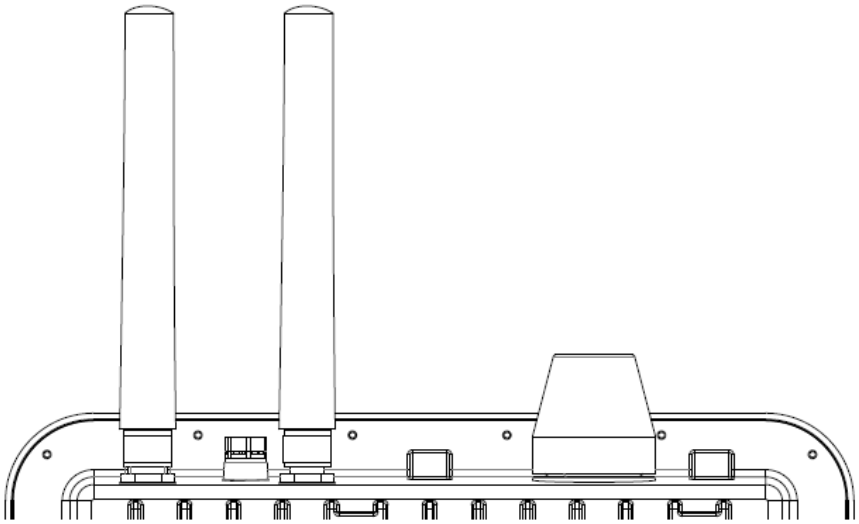
Frequency	2.4 ~ 2.5 5.X GHz
S.W.R	<= 2.0 @ 2.4~ 2.5 <= 2.5 @ 5.X GHz
Peak Gain	4 dBi @ 2400 ~ 2500 MHz 6 dBi @ 5.X GHz
Polarization	Vertical
Impedance	50 Ohm
Connector Type	Brass
Operational Temperature	- 20 °C ~ +65 °C

LTE + GPS Antenna



GPS	**Dielectric Antenna**	**Center Frequency**	1575.42±3MHz
		Bandwidth	CF±5MHz
		Polarization	RHCP
		Gain	2dBi
		V.S.W.R	<1.5
		Impedance	50 Ohm
		Axial Ratio	3dB (max)
	LNA	**Gain**	28±2dB
		Noise Figure	<1.5dB
		V.S.W.R	<2.0
LTE		**Frequency Range**	698~960MHz/1710~2690MHz
		V.S.W.R	<3.0
		Polarization	Linear
		Gain	2.0dBi
		Impedance	50 Ohm

Check the picture below for the antenna installation position.



LED Indicator

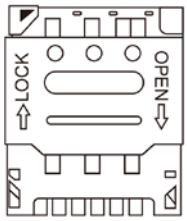
LED	Status	Description
Ethernet Port (Port1-4)	Green On	Links established
	Green Blinking	Packets transmitting/receiving
	Green Off	Link is inactive
Serial	Green Blinking	TX/RX transmission

2.10 SIM CARD INSTALLATION

SIM Card Slot

There are 2 SIM Card slots and it is located inside the box. The SIM Card Slot is used to insert the cellular card. To install the SIM Card, user needs to open the cover.

WARNING: Be careful when install the SIM Card, wrong installation procedure will cause damage.



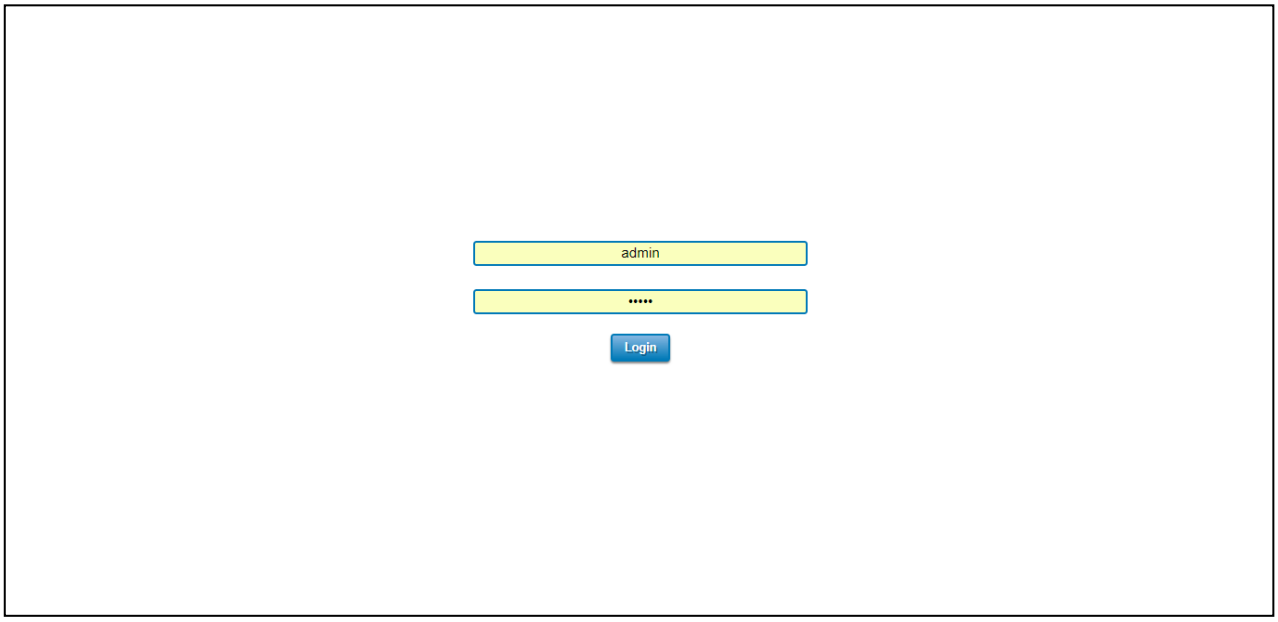
3. WEB MANAGEMENT CONFIGURATION

To access the management interface, WoMaster' router has two ways access mode through a network; they are web management and telnet management. Web interface management is the most common way and the easiest way to manage a network, through web interface management, a router interface offering status information and a subset of device commands through a standard web browser. If the network is down, another alternative to access the management interface can be used. The alternative way is by using telnet management which is offer configuration way through CLI Interface. This manual describes the procedures for Web Interface and how to configure and monitor the managed router only.

PREPARATION FOR WEB INTERFACE MANAGEMENT

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

1. Plug the DC power to the router and connect router to computer.
2. Make sure that the router default IP address is **192.168.10.1**.
3. Check that PC has an IP address on the same subnet as the router. For example, the PC and the router are on the same subnet if they both have addresses that start 192.168.10.x (Ex: **192.168.10.2)**. The subnet mask is 255.255.255.0.
4. Open command prompt and ping **192.168.10.1** to verify that the router is reachable.
5. Launch the web browser (Internet Explorer or Mozilla Firefox or Google Chrome) on the PC.
6. Type **http://192.168.10.1** (or the IP address of the router). And then press **Enter** and the login page will appear.
7. Type username and the password. Default user name: **admin** and password: **admin**. Then click **Login**.



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

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 User Account

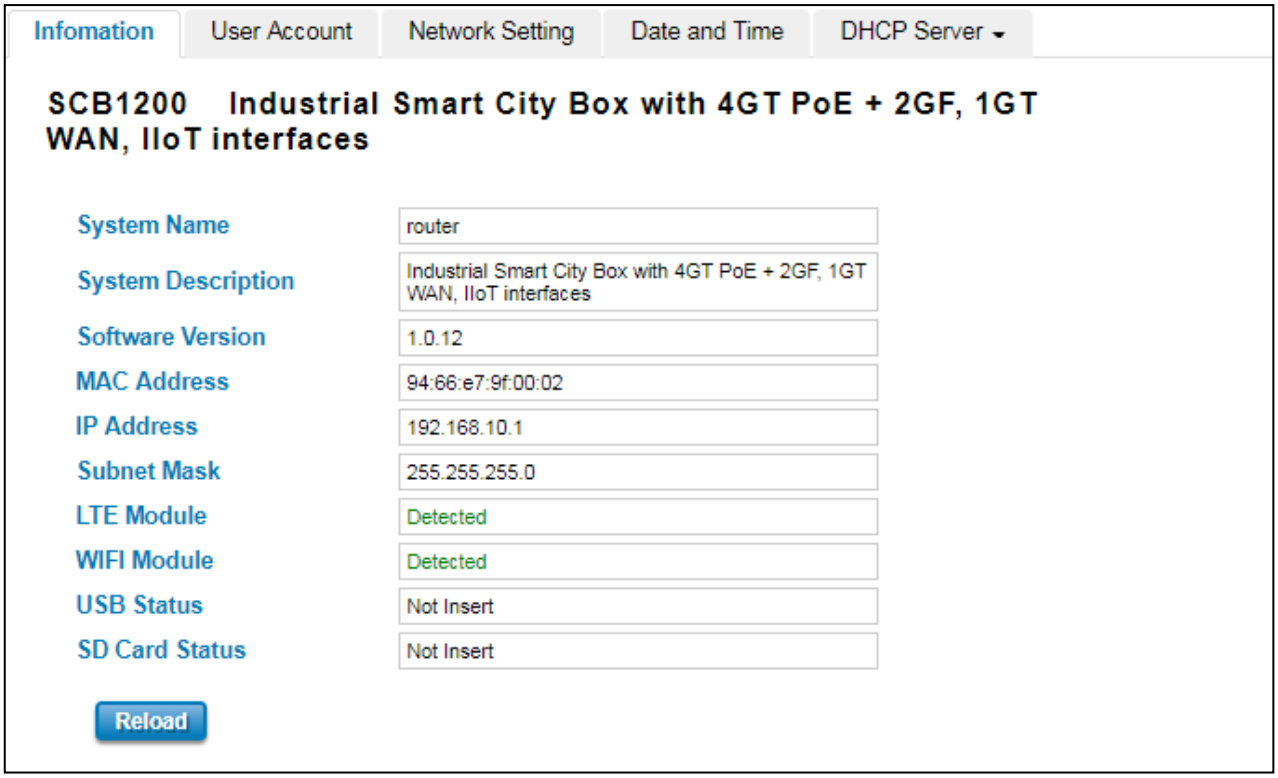
3.1.3 IP Setting

3.1.4 Date and Time

3.1.5 DHCP Server

3.1.1 INFORMATION

Information section, this section shows the basic information from the 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:

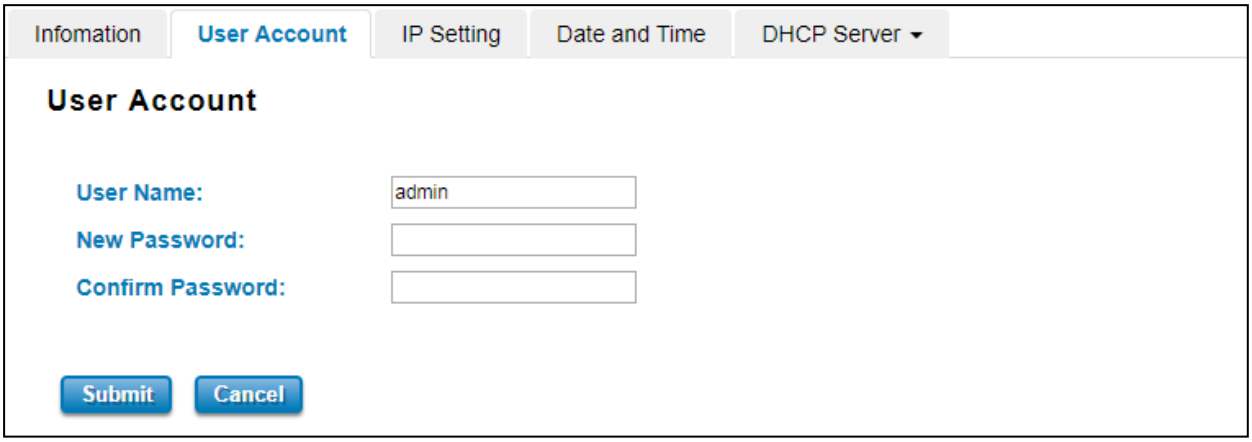
TERMS	DESCRIPTION
System Name	**Default: router** Set up a name for the device.
System Description	Display the name of the product.
Software Version	Display the firmware latest version that installed in the device.
MAC Address	Display the hardware's MAC address that assigned by the manufacturer.

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
LTE Module	Display the LTE Module status when the LTE is detected or undetected.
WIFI Module	Display the Wi-Fi Module status when the Wi-Fi is detected or undetected.

3.1.2 USER ACCOUNT

WoMaster' router supports the management accounts; with the Name default setting is **admin** and the authority allow user to configure all of configuration parameters. Below is the **User Account** section.

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



The User Account 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 confirms the new password in this section. After finished, click **Submit** to apply the changes. Don't forget to **Save** the settings. Try to re-login with the new User Name and Password.

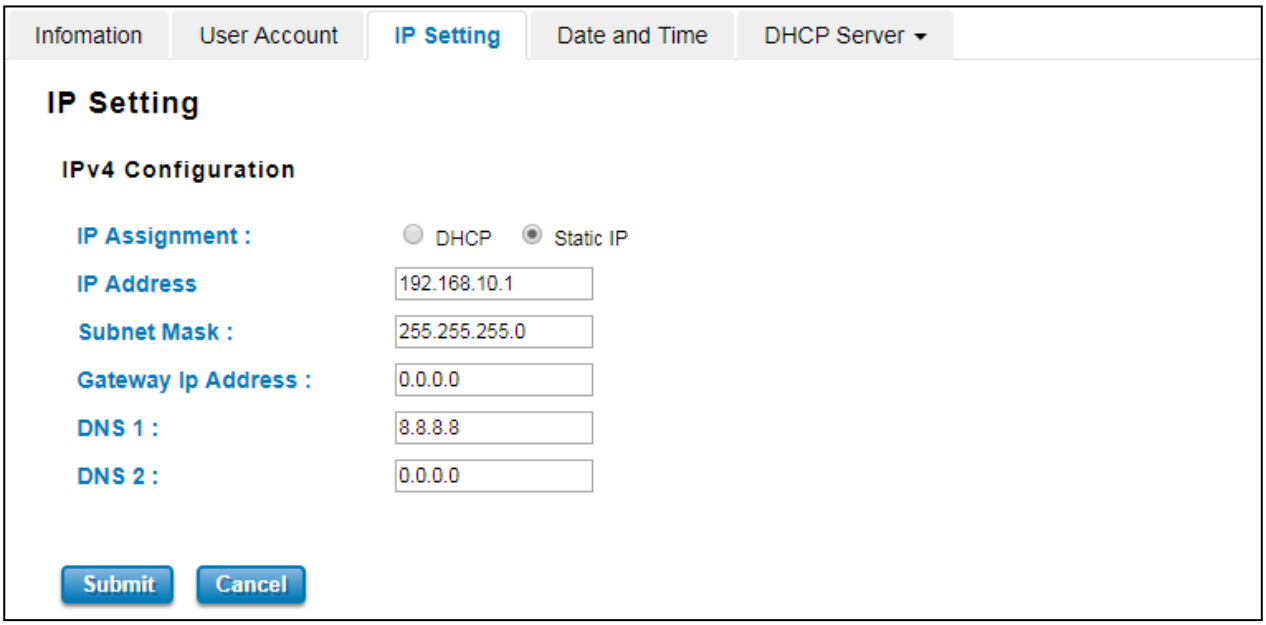
The description of the User Account interface is as below:

TERMS	DESCRIPTION
Name	**Default: admin** Key in new username here.
New Password	**Default: admin** 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.

3.1.3 IP SETTING

The IP 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.



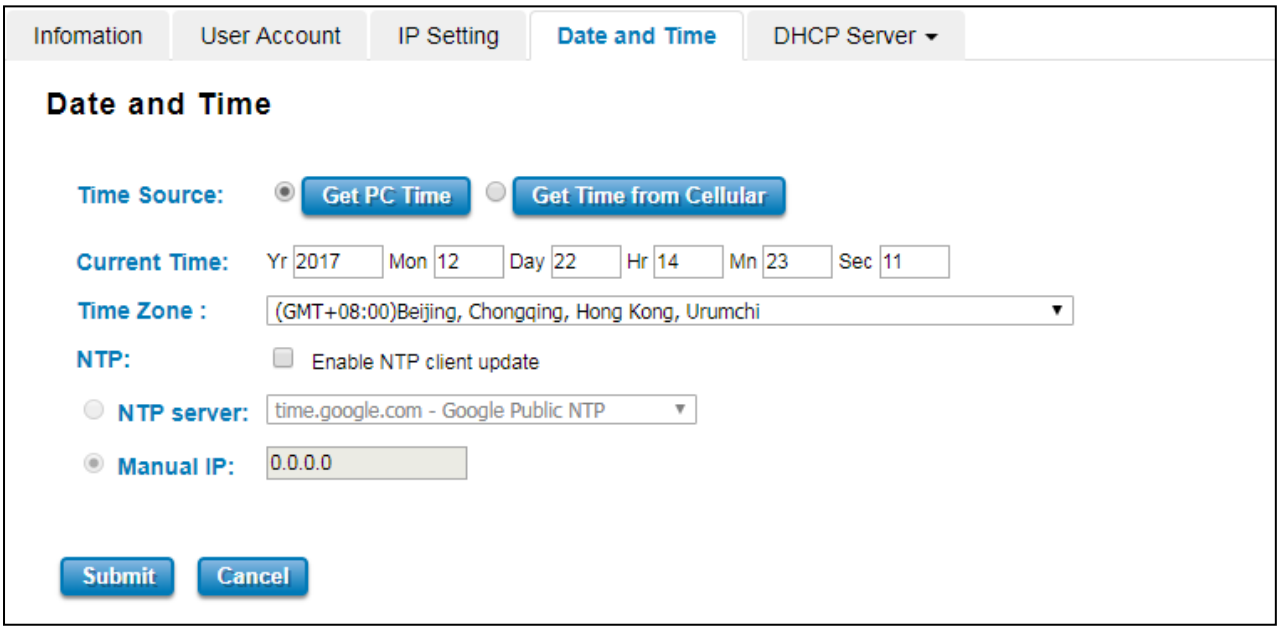
The IPv4 Configuration includes the router's IP address and subnet mask, as well as the IP address of the default gateway. In addition, input cells are provided for the IP addresses of a 1st and 2nd DNS server. Configure the managed router's IP settings. The figure above shows the user interface of IPv4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

The description of the columns is as below:

TERMS	DESCRIPTION
IP Assignment	Select to DHCP or Static 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's network for user's 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.

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:

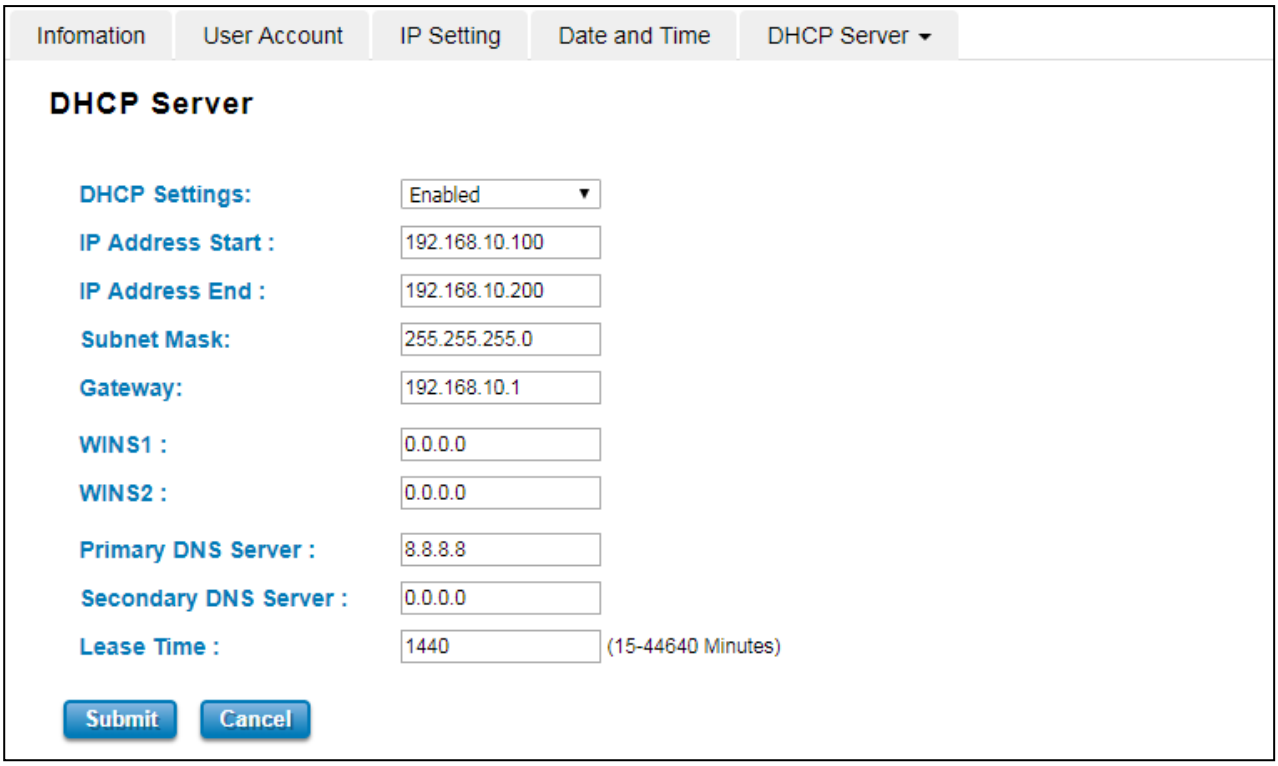
TERMS	DESCRIPTION
Current Time	User can configure time by input it manually. User also can click the **Get PC Time or Get Time from Cellular** to get the time setting. Get PC Time: get the time the PC Get Time from Cellular: get the time from the cellular network.
Time Zone	Choose the Time Zone section 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 Server** dropdown list or select **Manual IP** to manually input the IP address of available time server. ***Make sure that the device also has the internet connection.**

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

3.1.5 DHCP SERVER

DHCP Server Setting

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



The description of the columns is as below:

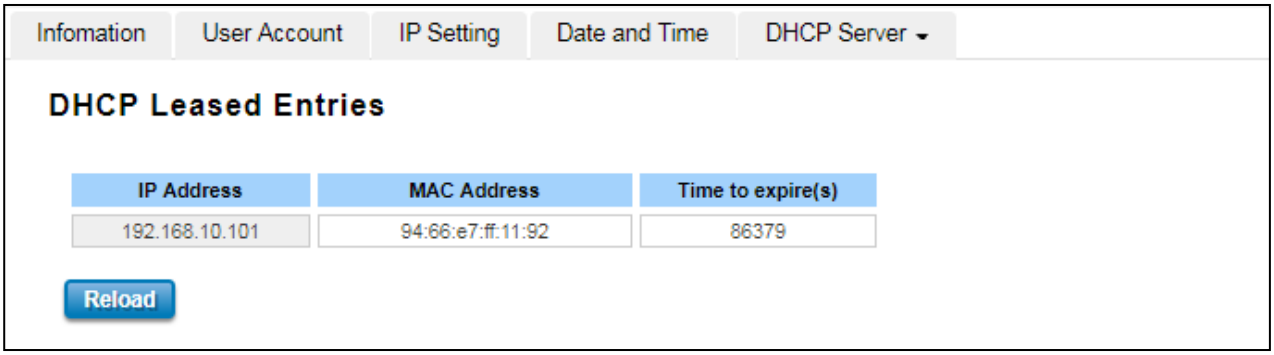
TERMS	DESCRIPTION
DHCP Setting	Select to **Enable** or **Disable** to activate and deactivate DHCP Server function.
IP Address Start	Assign the IP Address Start range.
IP Address End	Assign the IP Address End range.
Subnet Mask	**Default: 255.255.255.0** Assign the subnet mask for the IP address here for DHCP Server.
Gateway	Assign the gateway for the router here for DHCP Server.
WIN S1	Enter WINS Server 1 IP address
WIN S2	Enter WINS Server 2 IP address
Primary DNS Server	Enter Primary DNS Server that used in user network.
Secondary DNS Server	Enter Secondary DNS Server that used in user network.
Lease Time	**Default: 1440** The maximum length of time for the IP address lease. Enter the Lease time in minutes. (Lease Time range: 15-44640 minutes)

The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set user computers to be DHCP clients by setting their TCP/IP settings to “Obtain an IP Address Automatically.” When

user turns the computers on, they will automatically load the proper TCP/IP settings provided by the router. If User manually assigns IP addresses to User computers or devices, make sure the IP addresses are outside of this range or User may have an IP conflict. After finished configuring, click on **Submit** to activate the configuration.

DHCP Leased Entries

The figure below shows the **DHCP Leased Entries.** It will show the MAC and IP address that was assigned by router. Click the **Refresh** button to refresh the list.



The description of the columns is as below:

TERMS	DESCRIPTION
IP Address	IP address that was assigned by router.
MAC Address	The MAC Address of the network interface that was used to acquire the lease.
Time to expire(s)	Remains time for the IP address from DHCP Server leased

3.2 ETHERNET PORT

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

Following items are included in this group:

3.2.1 Port Status

3.2.2 Port Setting

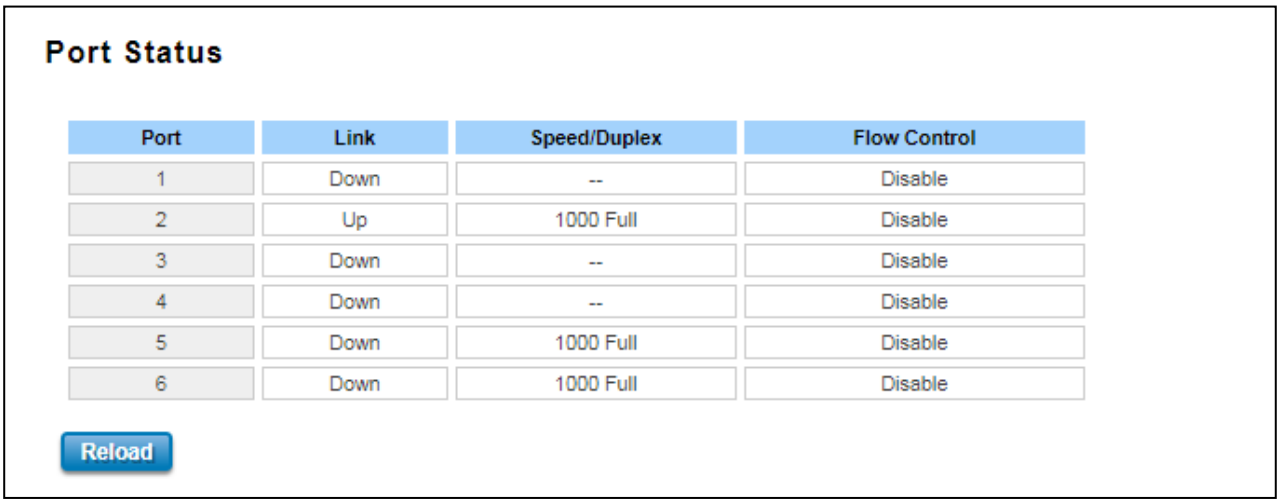
3.2.3 VLAN Setting

3.2.4 Rate Control

3.2.5 Traffic Control

3.2.1 PORT STATUS

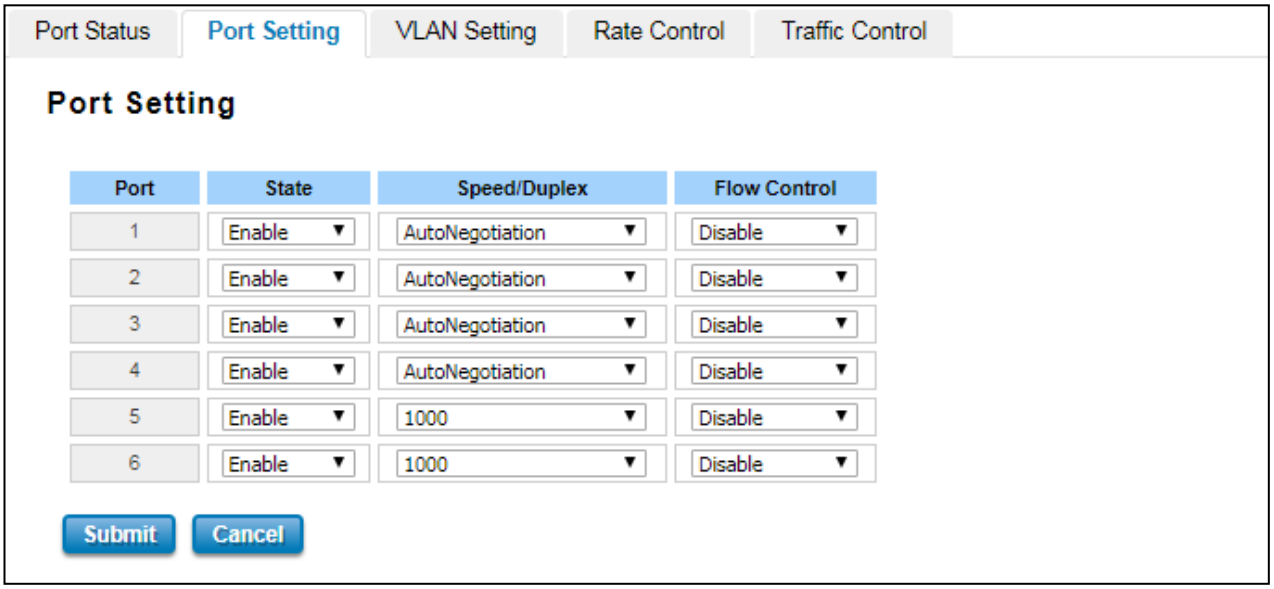
Port Status provides current port status, such as the Port number, Link status if the port is up or down, show the speed/duplex for each port and the flow control.



3.2.2 PORT SETTING

Port Settings section allows users to enable or disable each port function; state the speed/duplex of each port; and enable or disable the flow control of the port.

The description of the columns is as below:



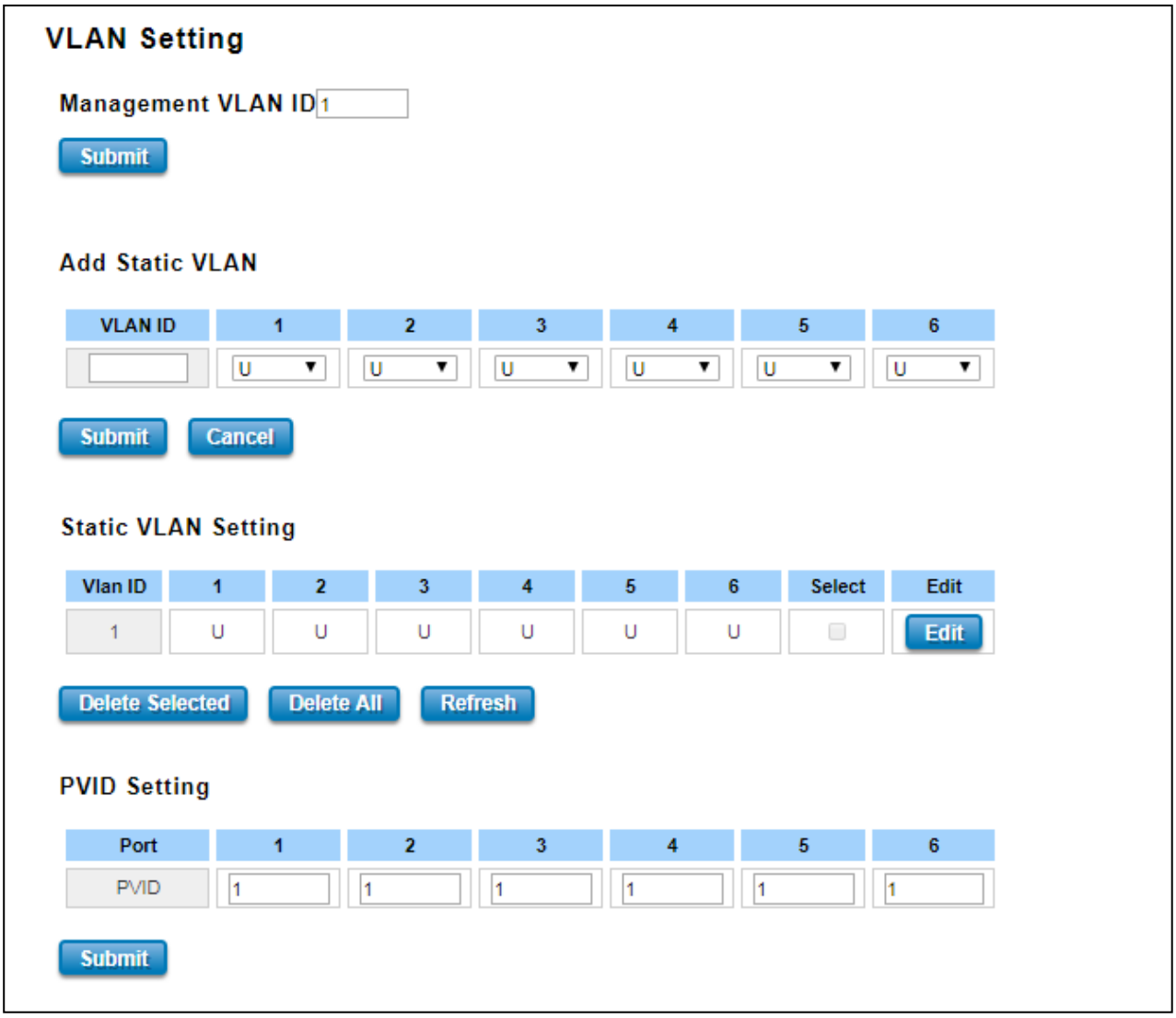
TERMS	DESCRIPTION
Port	Shows port number
State	**Default: Enable** Enable or disable a port
Speed/Duplex	**Default: AutoNegotiation** Users can set the bandwidth of each port as Auto-negotiation, 100 full,100 half,10 full,10 half mode for **Giga Ethernet Port 1~4**. For **Fiber Port 5~6:** it can be set to 100 or 1000.
Flow Control	**Default: Disable** **Enable** means that User needs to activate the flow control function in order to let the flow control of that corresponding port on the switch to work. **Disable** means that User doesn't need to activate the flow control function, as the flow control of that corresponding port on the switch will work anyway.

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

3.2.3 VLAN SETTING

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

The description of the columns is as below:



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

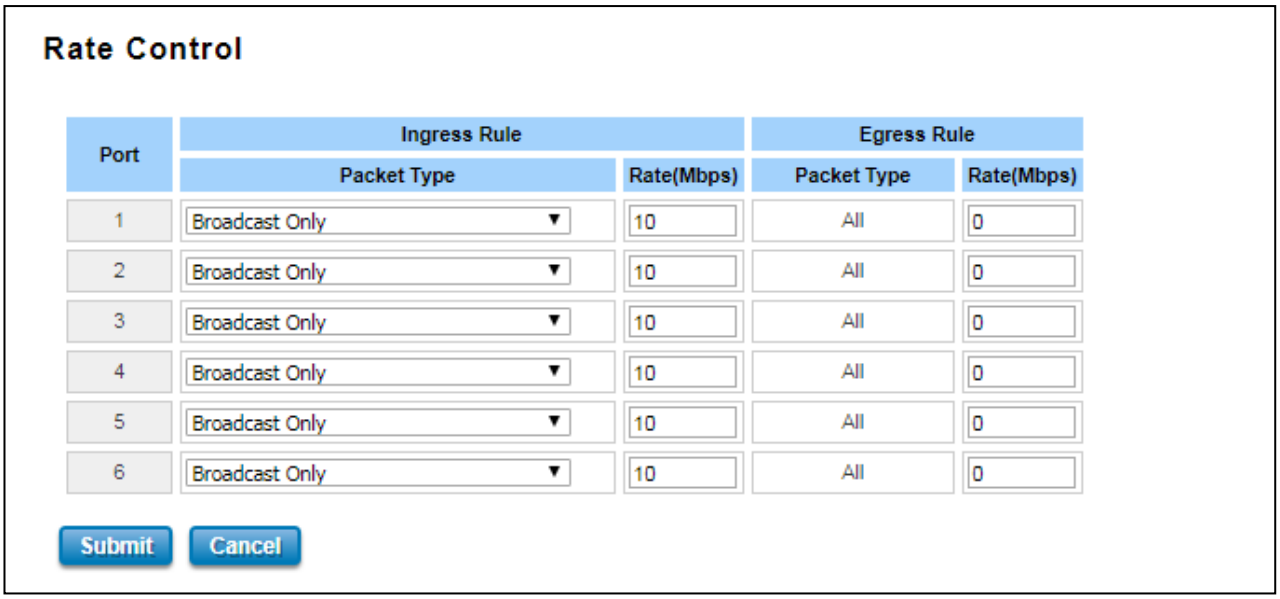
The steps to create a new VLAN: Type in Add Static VLAN section, and click **Submit** to create a new VLAN. Then User can see the new VLAN in the Static VLAN Setting table. After created the VLAN, the status of the VLAN will remain in Unused until User adds ports to the VLAN.

NOTE:

1. Before User changed the management VLAN ID by Web and Telnet, remember that the port attached by the administrator should be the member port of the management VLAN; otherwise the administrator can't access the switch via the network.
2. WoMaster switch supports max 256 groups VLAN.

3.2.4 RATE CONTROL

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



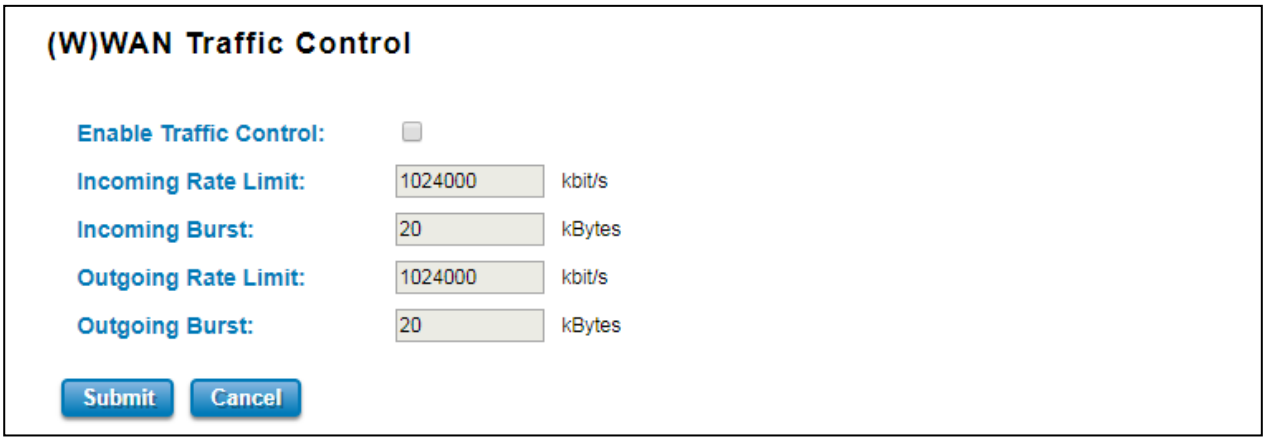
The description of the columns is as below:

TERMS	DESCRIPTION
Packet Type	Select the packet type that wanted to filter.
Ingress	The packet types of the Ingress Rule listed here include **Broadcast Only** / **Broadcast and multicast** / **Broadcast, Multicast and Unknown Unicast / Broadcast and Unknown Unicast** or **All**.
Egress	The packet types of the Egress Rule (outgoing) only support **all** packet types.
Rate (Ingress & Egress)	**Default value Ingress: 10 Mbps** **Default value Egress: 0 Mbps (**0 stands for disabling the rate control for the port.**)** Valid values are from 1Mbps-1000Mbps for Giga Ethernet ports. The step of the rate is 1 Mbps.

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

3.2.5 TRAFFIC CONTROL

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



The description of the columns is as below:

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

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

3.3 POWER OVER ETHERNET

Power over Ethernet has become increasingly popular due in large part to the reliability provided by PoE Ethernet switches that supply the necessary power to Powered Devices (PD) when AC power is not readily available or cost-prohibitive to provide locally. WoMaster industrial DIN Rail PoE Switch compliant with IEEE 802.3af and IEEE 802.3at. All of WoMaster switches adapt 4-Port PoE injectors in port 1 to port 4, each port with the ability to deliver 30 - 60W to compatible IEEE 802.3at standard and provides 100W power budget for all systems.

Power over Ethernet can be used with:

• Surveillance cameras

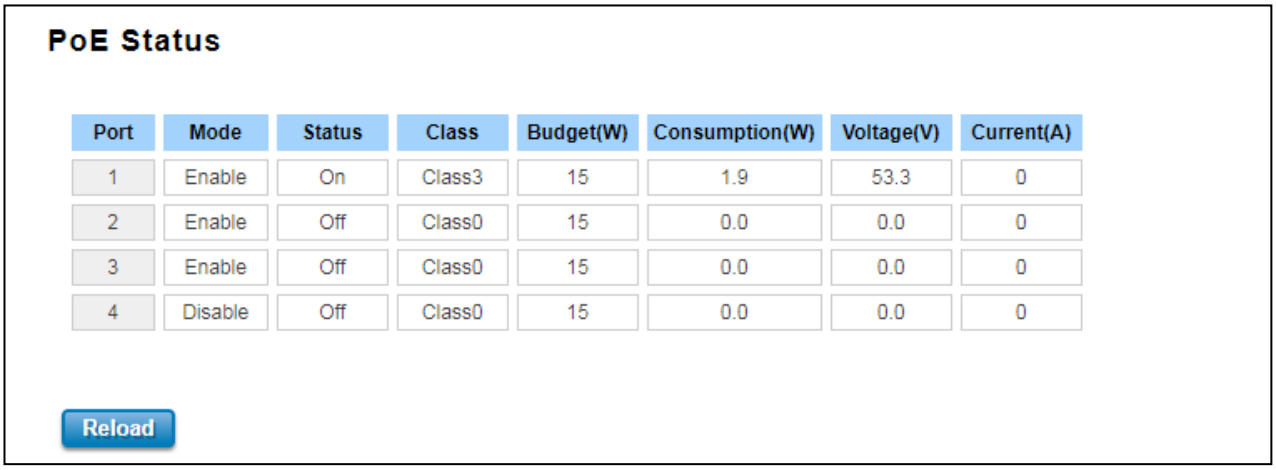
• Security I/O sensors

• Industrial wireless access points

• Emergency IP phones

3.3.1 PoE STATUS

The PoE Status page shows the system PoE status and the operating status of each PoE Port. The information includes PoE mode, Operation status, and PD class, Power Consumption, Voltage, and Current. For example, in the figure below, Port 1 was enabled and is supplying power to a Class 3 Powered Device (PD) indicated under the Classification column. The PD device is rated at 53.3V and 0A. The total power consumption for this PD is 1.9 W with Budget 15W. To check the status of the PoE port, please click on the Reload button.



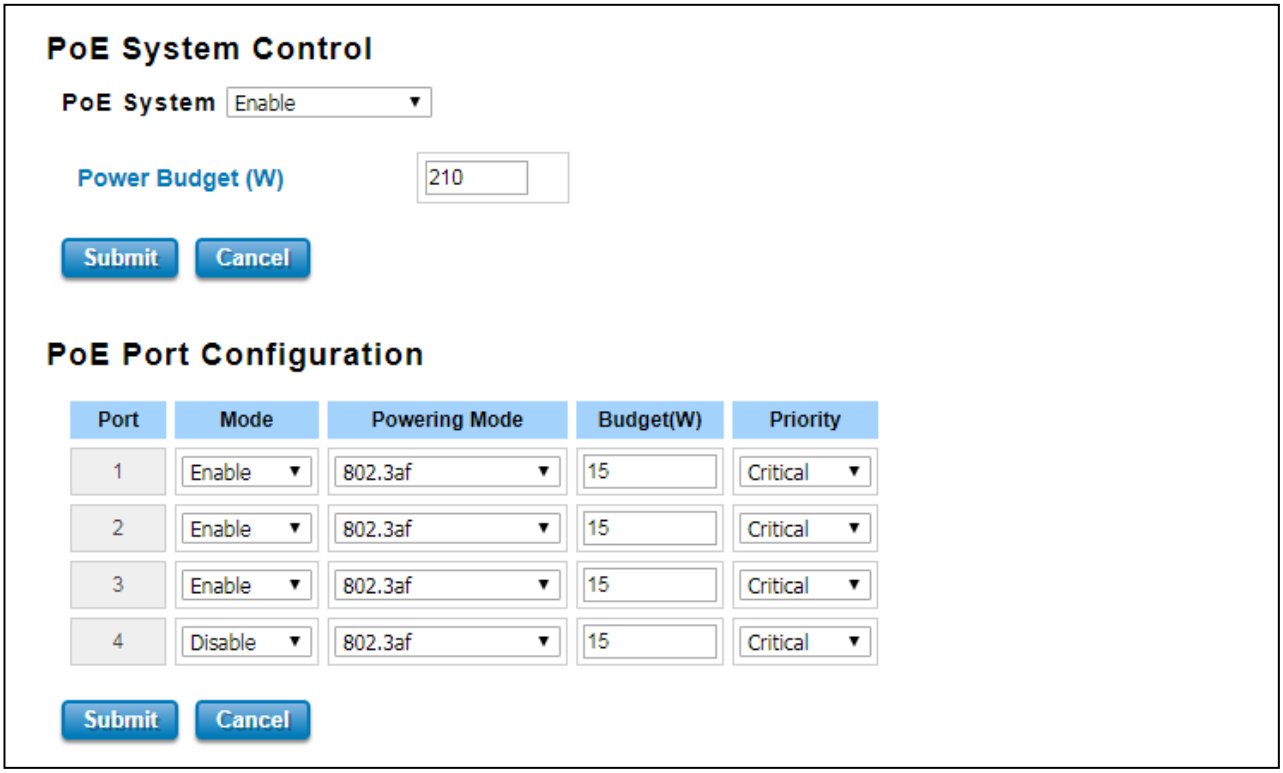
The description of the columns is as below:

TERMS	DESCRIPTION
Mode	Enable/Disable/Schedule Indicates the PoE port status
Status	**Default: Off** PoE status is included Off, Powering, and Searching. Off – PoE is inactive. Powering – PoE is enabled and powering the PD. Searching – Searching the PD which needs the power.
Class	Indicates the PD included in which PoE class.
Budget(W)	Indicates the actual Budget value for PoE port

Consumption (W)	Indicates the actual Power consumed value for PoE port
Voltage (V)	Indicates the actual Voltage consumed value for PoE port
Current (A)	Indicates the actual Current consumed value for PoE port

3.3.2 PoE PORT SETTING

The figure below is **PoE Port Setting** interface. In this section, user can enable or disable the PoE function, configure the Powering mode, the budget mode, and the set the budget. After finished configuring the settings, click on **Submit** to save the configuration.



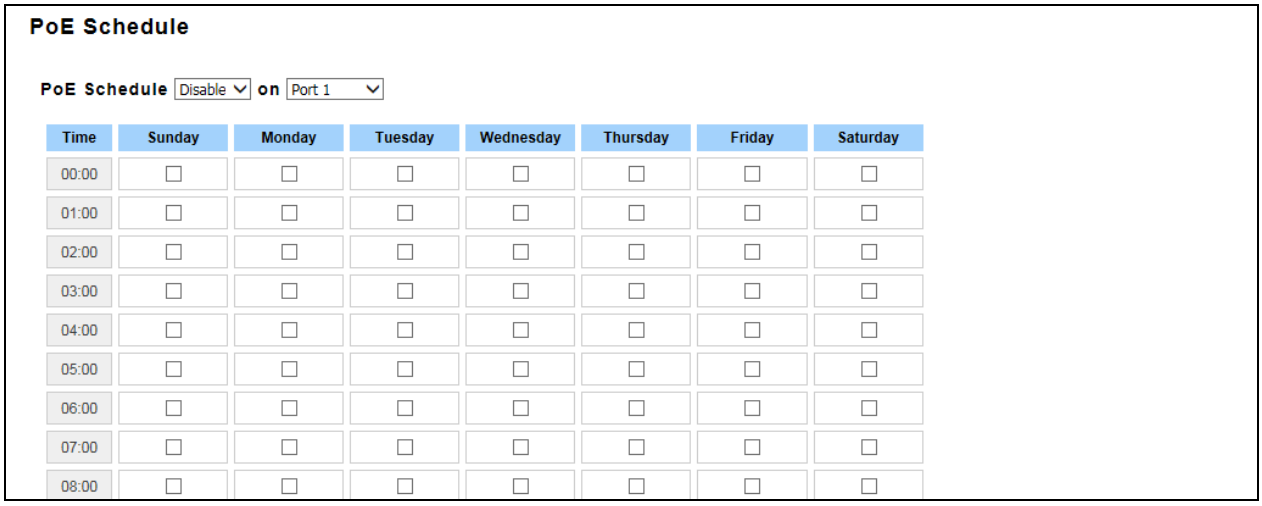
The description of the columns is as below:

TERMS	DESCRIPTION
Mode	Enable/Disable/Schedule port's PoE function.
Powering Mode	**Port 1 – 2:** 802.3af, 802.3bt (4-pair), and forced mode. **Port 3 – 4:** 802.3af, 802.3at (2-event), and forced mode. ***Forced mode will ignore the classification behaviors, uses the forced mode carefully.**
Budget (W)	Allows user assign the budget control in this field.
Priority	Allows user to set the priority to deliver the PoE from Critical, High, and Low.

If the system PoE consumption is over the system budget control, the PoE system will turn off low priority port PoE function, until the consumption becomes smaller than the system budget. After finished configuring the settings, click on **Submit** to save the configuration.

3.3.3 PoE SCHEDULE

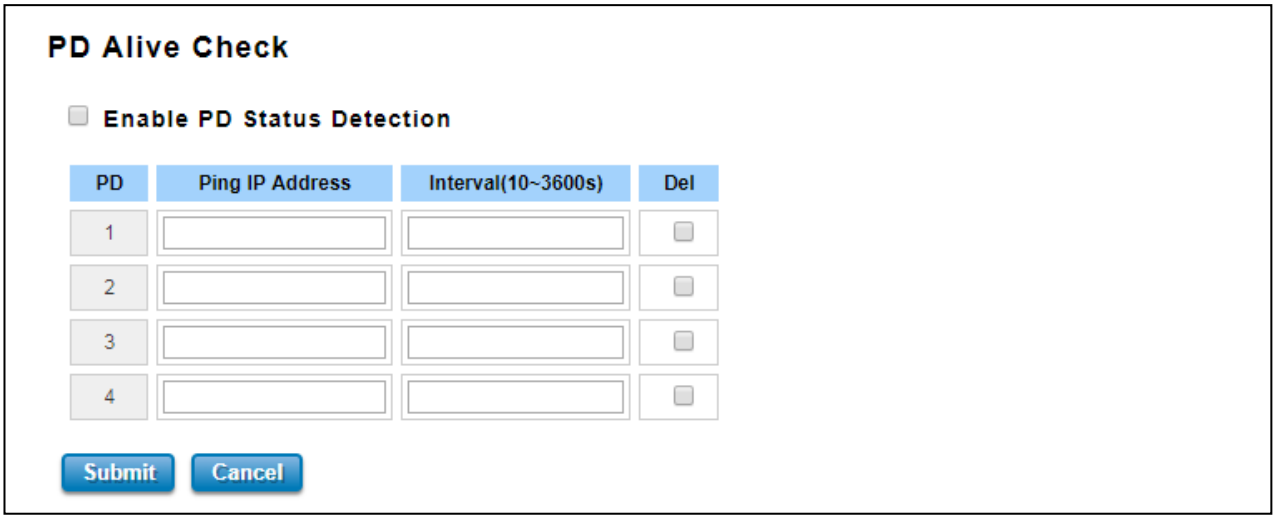
For energy saving or power recycle powered devices, the PoE managed switch's **PoE schedule** interface allows users to appoint any date and time to enable or disable PoE functions for each PoE port. User needs to configure **PoE Scheduling** and select a target port manually to enable this function. The figure below is PoE Schedule interface.



The PoE schedule supports hourly and weekly base PoE schedule configuration. **Enable** and select the target port and marking the time frame, then click **Submit** to activate the PoE scheduling function on selected port.

3.3.4 ALIVE CHECK

PD Alive Check



WoMaster's Switches support a useful function that helps user to maintain the PD's status and help to save the maintenance time and money. Once user defined this function, the PoE Switch will request PD system and turn-off PoE power if PD system does not echo the request. After the duration time (interval time), the PoE switch will start request PD again. The description of the columns is as below:

TERMS	DESCRIPTION
Ping IP address	PD's IP-address that installed on the port.
Interval (10-3600s)	User measured the PD system boots duration time. *Most of PD system – IP camera will take at least 40~50 seconds. Here, we

	suggest that user sets the cycle time to 90 seconds.
Delete	Delete PD's IP-address that

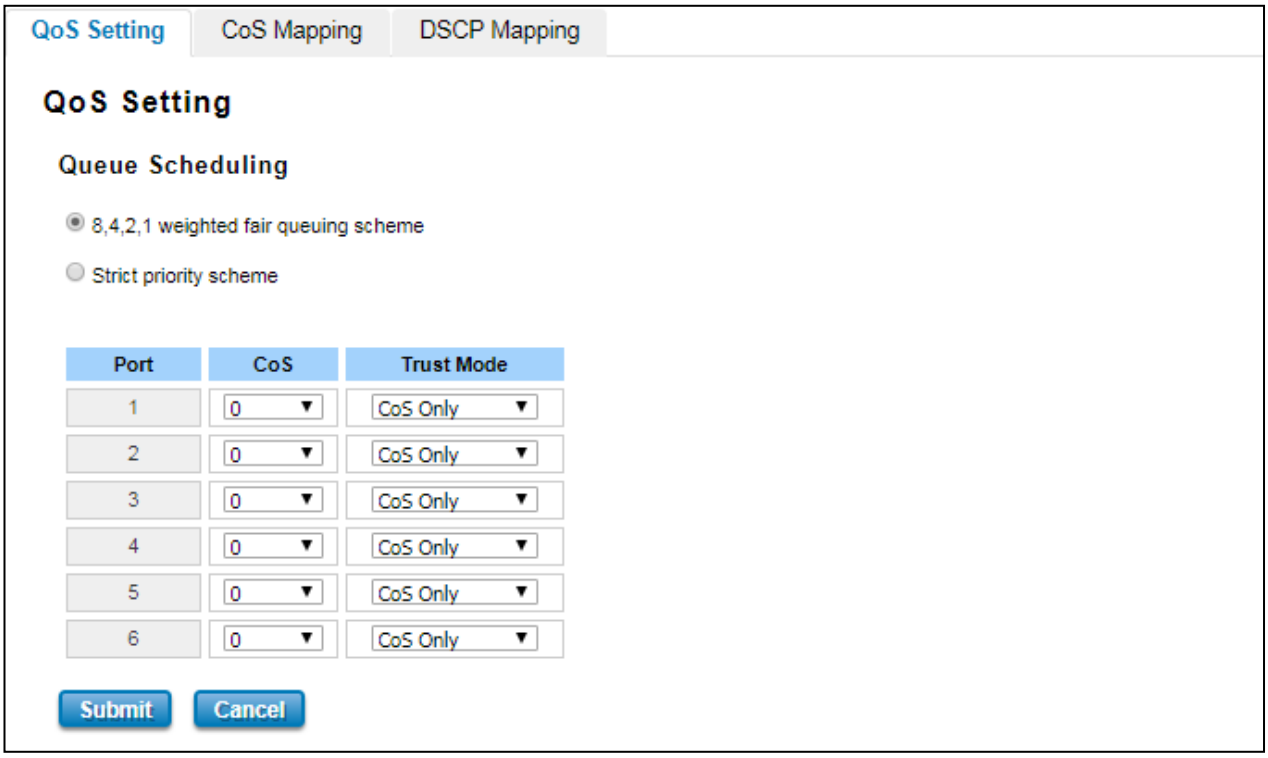
After finished configuring the settings, click on **Submit** to save the configuration.

3.4 QUALITY of SERVICE (QoS)

Quality of Service (QoS) is the ability of the switch to provide different priority to different applications, users or data flows, or to guarantee a certain level of performance to a data flow. QoS guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications. QoS can also help to reduce traffic problems and control the traffic by delivering the highest priority first. This section allows the user to configure Quality of Service settings for each port by configuring the priorities in order to provide a smooth data traffic.

3.4.1 QoS SETTING

The figure below shows QoS Setting.



Queue Scheduling

User may select the Queue Scheduling rule:

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

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

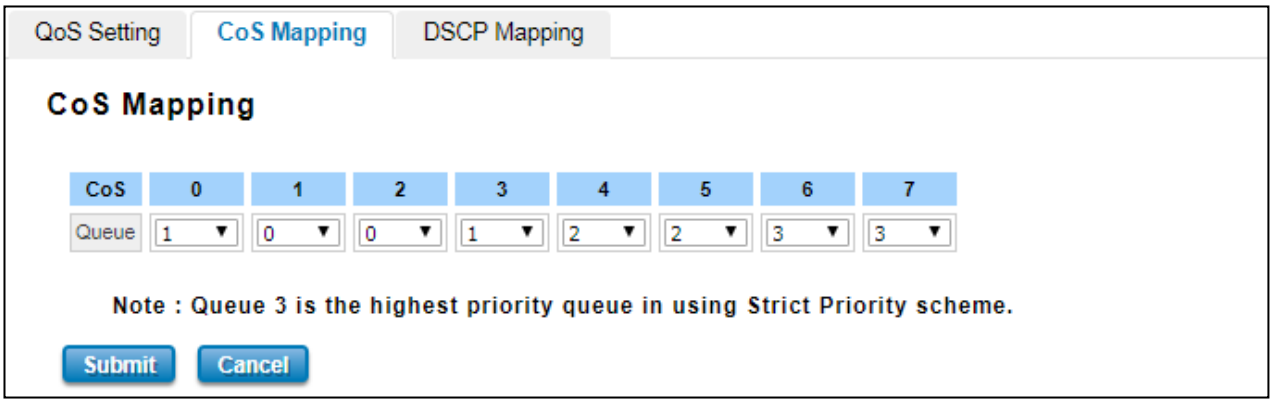
TERMS	DESCRIPTION
CoS	Indicate default port priority value for untagged or priority-tagged frames.

Trust Mode	**Default: COS Only** Indicate Queue Mapping types for User to select.
COS Only	Port priority will only follow COS-Queue Mapping User has assigned.
DSCP Only	Port priority will only follow DSCP-Queue Mapping User has assigned.
COS First	Port priority will follow COS-Queue Mapping first, and then DSCP-Queue Mapping rule.
DSCP First	Port priority will follow DSCP-Queue Mapping first, and then COS-Queue Mapping rule.

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

3.4.2 CoS MAPPING

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



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

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

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

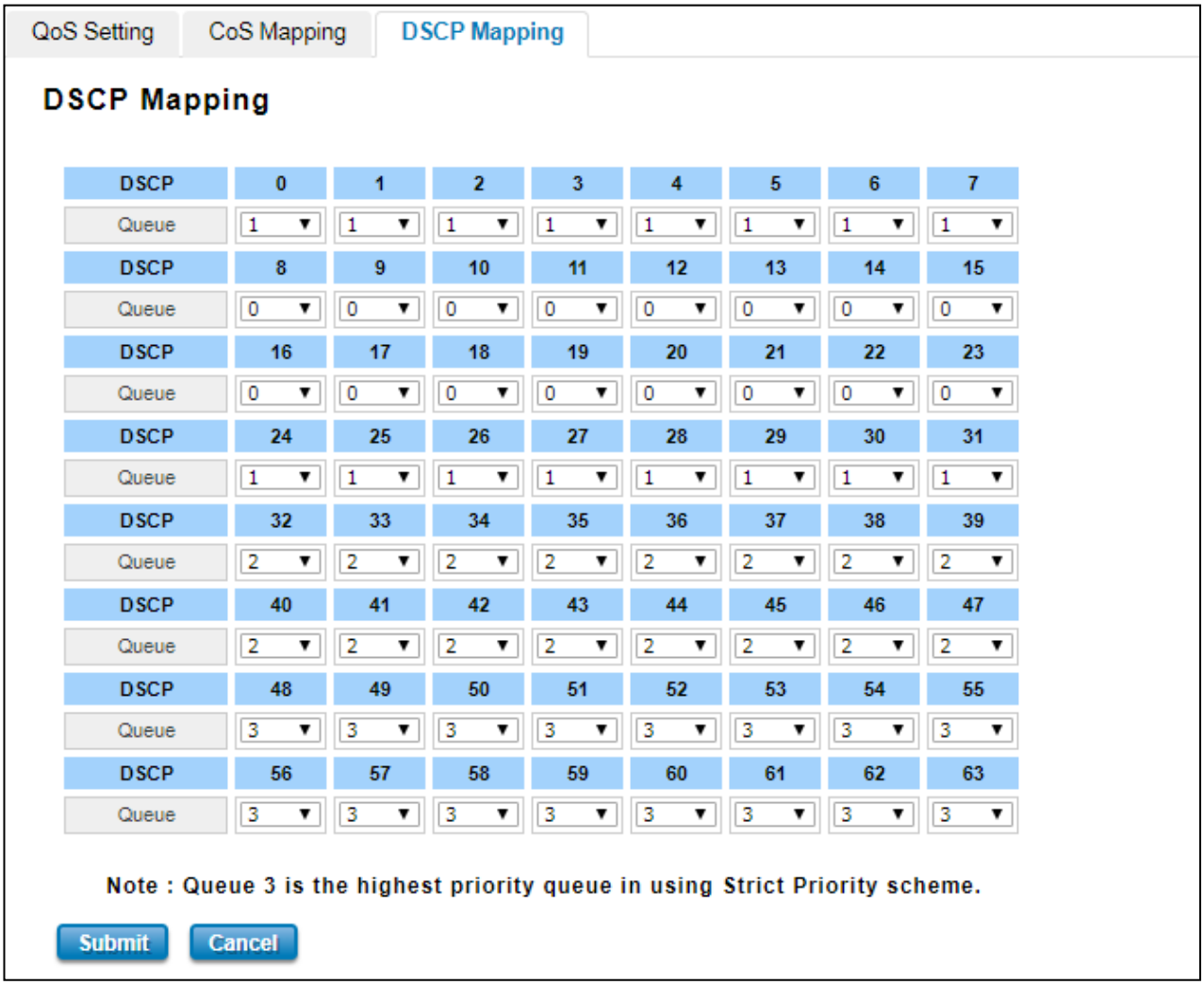
For the step in configuration

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

2. Click the Submit button.

3.4.3 DSCP MAPPING

This page is to assign DSCP priorities to different Queues. The WoMaster switch only supports 4 physical queues, Lowest, Low, Middle and High that represent by number 0 ~ 3. Users should assign how to map DSCP value to the level of the physical queue. Users can freely change the mapping table to follow the upper layer 3 switch or routers' DSCP setting.



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

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

3.5 MULTICAST

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

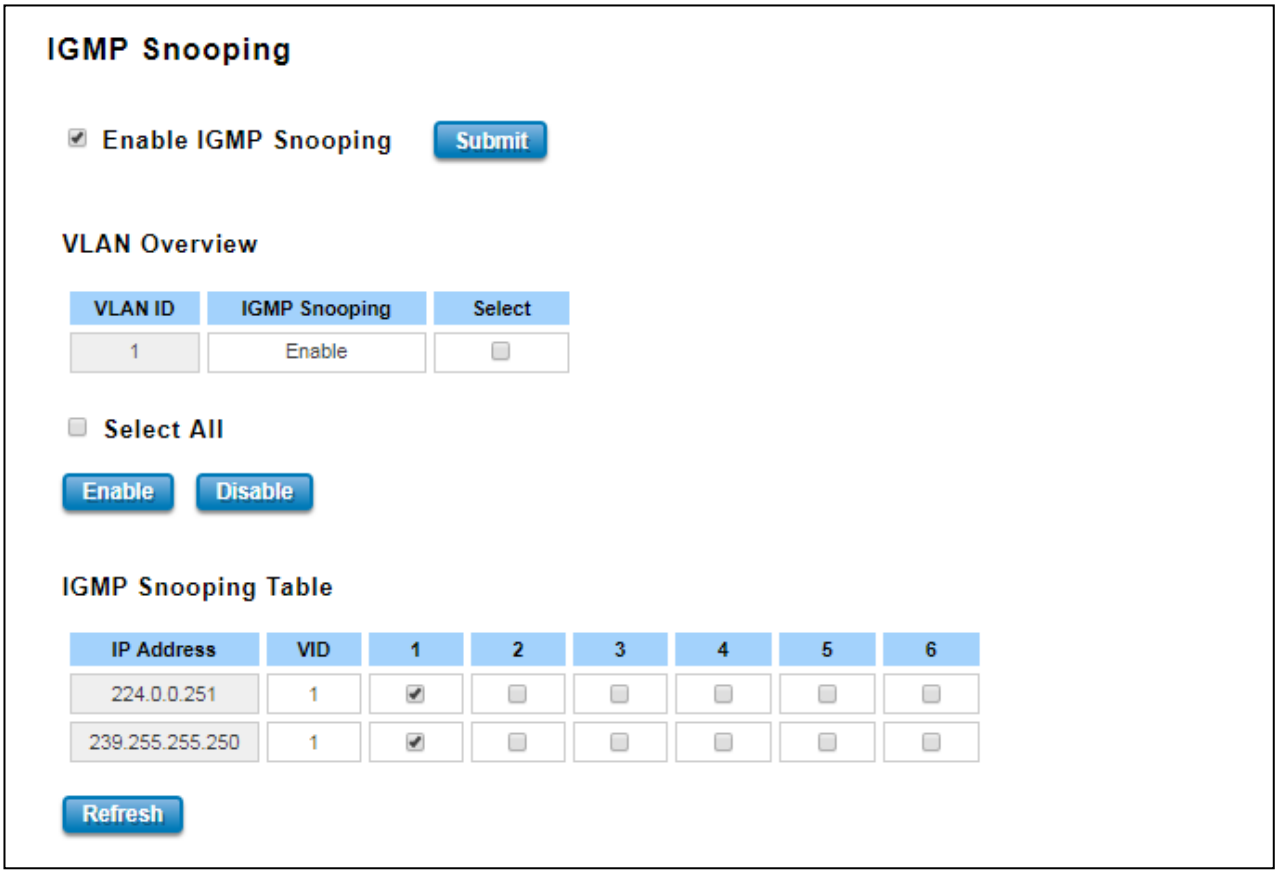
Following sections are included in this group:

3.5.1 IGMP Snooping

3.5.2 IGMP Query

3.5.1 IGMP SNOOPING

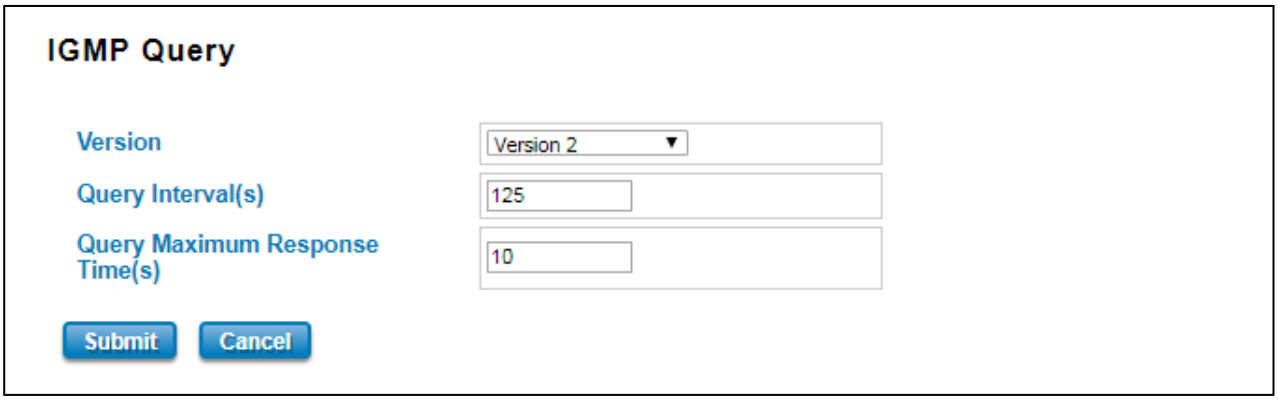
This page is to enable IGMP Snooping feature. After enabling the feature, user may assign IGMP Snooping function to specific VLAN, and the IGMP Snooping table will show the specific multicast group from dynamic learnt or manual input. By enabling IGMP Snooping allows the ports to detect IGMP queries,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



3.5.2 IGMP QUERY

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

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



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

TERMS	DESCRIPTION
Version	**Default: Disable** **V1** means IGMP V1 General Query **V2** means IGMP V2 General Query.
Query Interval(s)	**Default: 125** The interval period of querier to send the query.
Query Maximum Response Time (s)	**Default: 10** The response time for querier detects to confirm there are no more directly connected group members on a LAN.

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

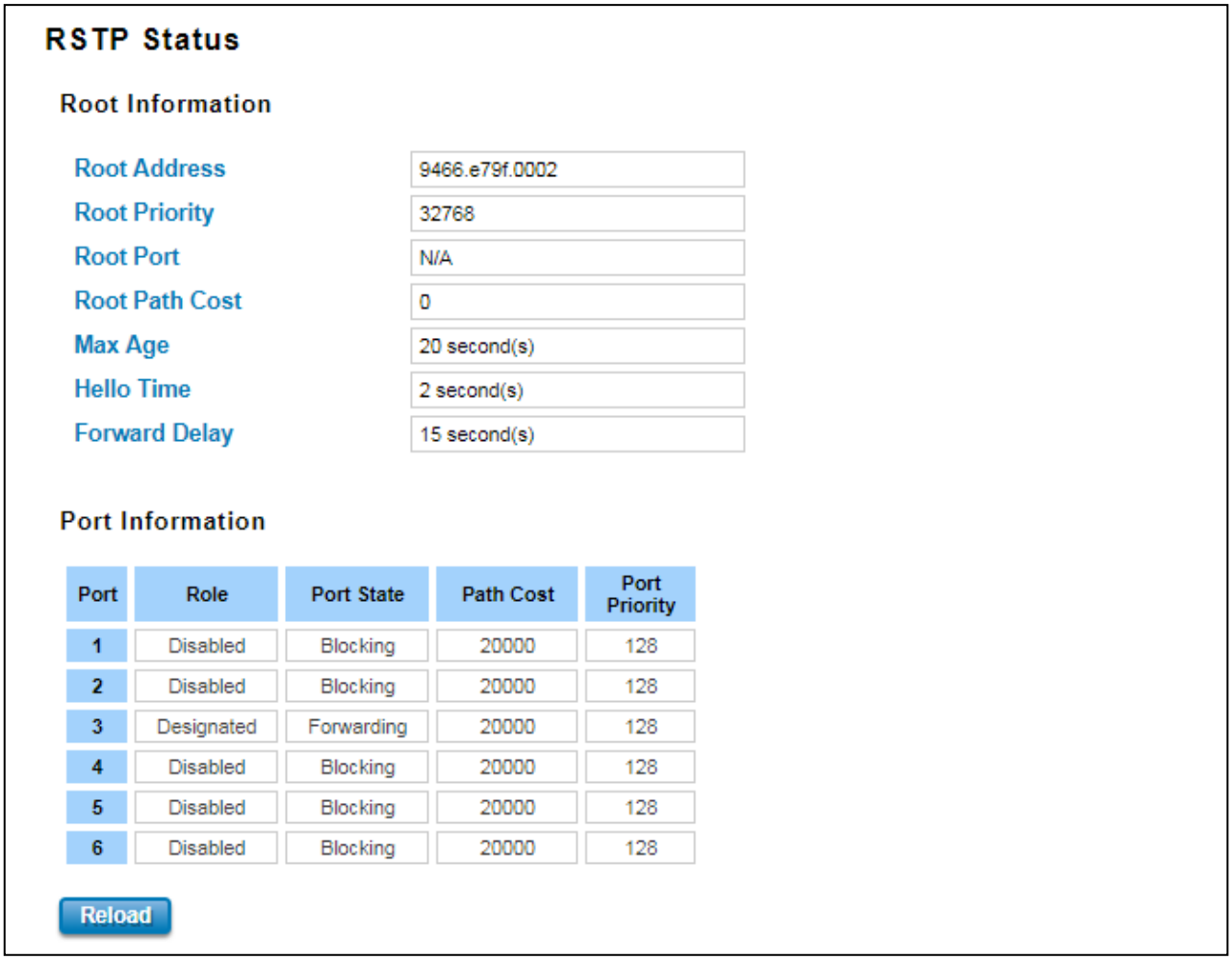
3.6 REDUNDANCY

Redundancy role of the network is to help protect critical links against failure, protects against network loops, and keeps network downtime at a minimum. Sustainable, uninterrupted data communication network is critical for industrial applications. Network Redundancy allows user to set up redundant loops in the network to provide a backup data transmission route in the event that a cable is inadvertently disconnected or damaged. This switch supports Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP). This is a particularly important feature for industrial applications since it could take several minutes to locate the disconnected or severed cable.

3.6.1 RSTP STATUS

RSTP Status

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

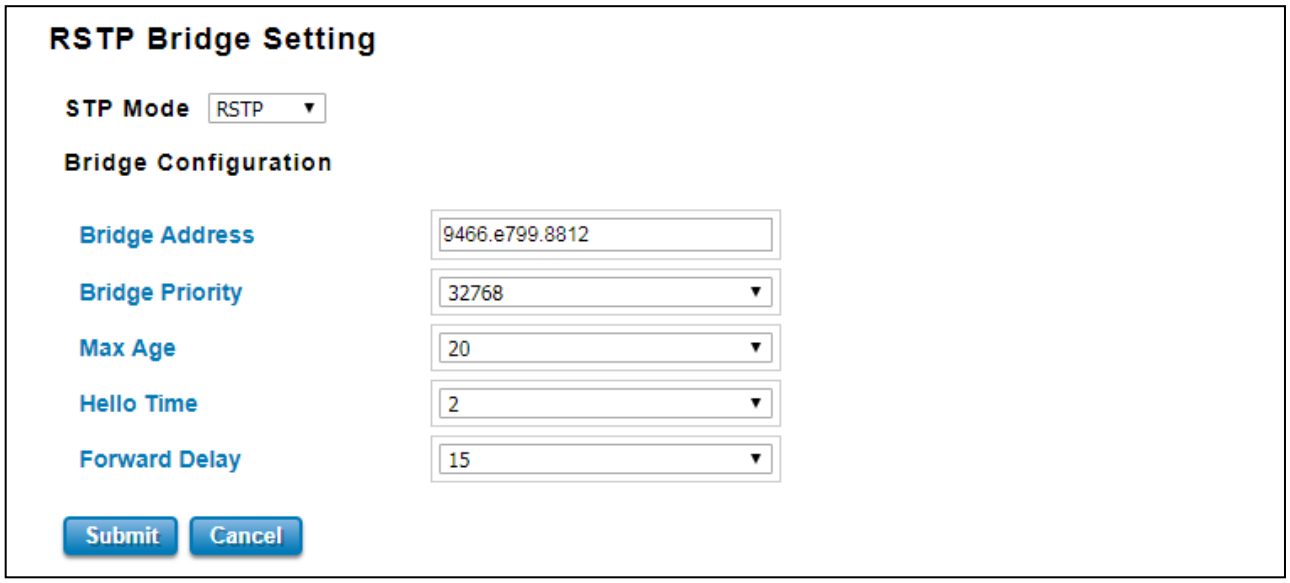


Root Information: User can see root Address, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root switch.

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

RSTP Bridge Setting

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



Spanning Tree Protocol (STP)

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

Rapid Spanning Tree Protocol (RSTP)

If the destination from a switch is more than one path, it will lead to looping condition that can generate broadcast storms in a network. The spanning tree was created to combat the negative effects of message loops in switched networks. A spanning tree algorithm is used to automatically sense whether a switch has more than one way to communicate with a node. It will then select the best path, and block the other path. Spanning Tree Protocol (STP) introduced a standard method to accomplish this. Rapid Spanning Tree Protocol (RSTP) was adopted and represents the evolution of STP, providing much faster spanning tree convergence after a topology change.

Bridge Configuration

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

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

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

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

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

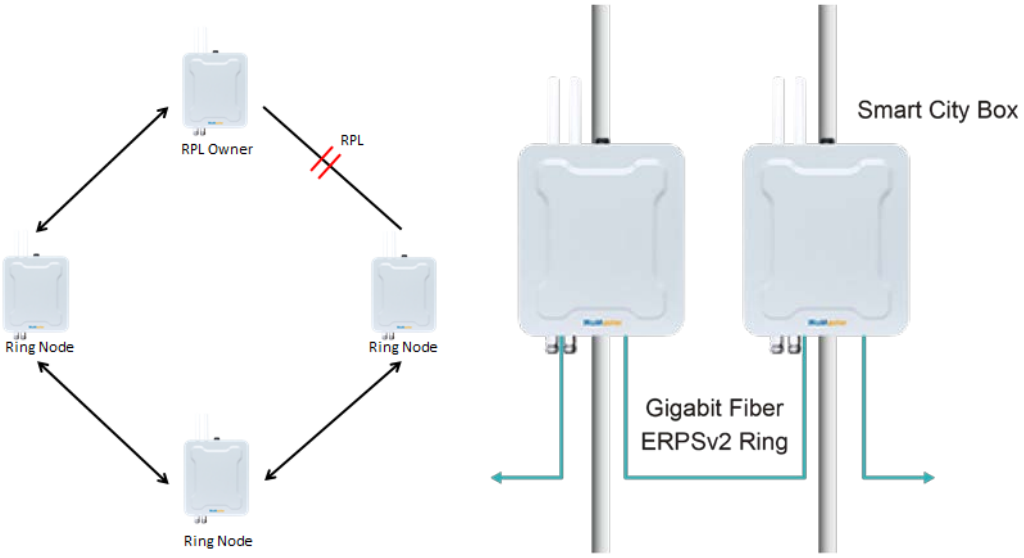
Forward Delay Time (4-30): Enter a value between 4 and 30 seconds. This value is the time that a port waits before changing from Spanning Tree Protocol learning and listening states to forwarding state.

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

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

3.6.2 ERPS SETTINGS

Ethernet Ring Protection Switching (ERPS) is a protocol for Ethernet layer network rings. The protocol specifies the protection mechanism for sub-50ms delay time. The ring topology provides multipoint connectivity economically by reducing the number of links. ERPS provides highly reliable and stable protection in the ring topology, and it never forms loops, which can affect network operation and service availability.

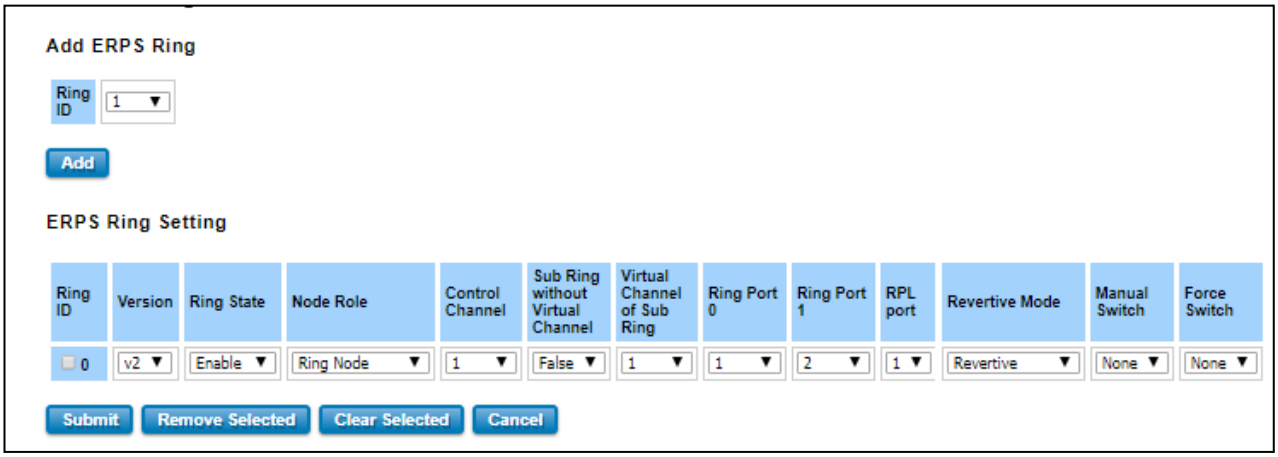


The figure above shows that each Ethernet Ring Node is connected to other Ethernet Ring Nodes that participating in the same Ethernet Ring using two independent links. In the Ethernet ring, loops can be avoided by guaranteeing that traffic may flow on all but one of the ring links at any time. This particular link is called Ring Protection Link (RPL). A control message called Ring Automatic Protection Switch (R-APS) coordinates the activities of switching on/off the RPL. Under normal conditions, this link is blocked by the Owner Node. Thus, loops can be avoided by this mechanism. In case an Ethernet ring failure occurs, one designated Ethernet Ring Node called the RPL Owner Node will be responsible for unblocking its end of the RPL to allow RPL to be used as a backup link. The RPL is the backup link when one link failure occurs.

WoMaster managed switches provide a number of Ethernet ring protocol. The ERPS/Ring section is subdivided into two menus, which are: ERPS Setting and ERPS Status.

3.6.2.1 ERPS SETTINGS

Add ERPS Ring



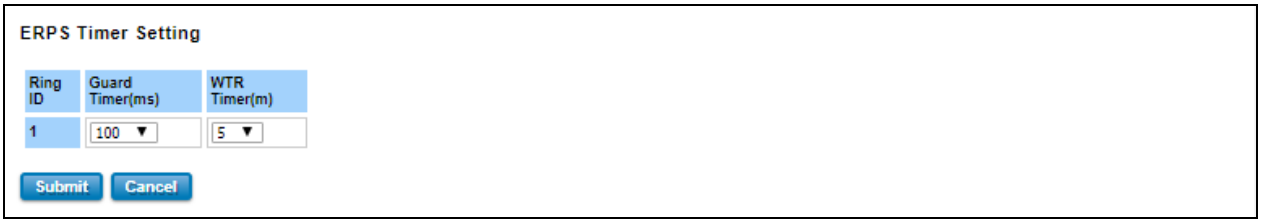
Add ERPS Ring is a section to add the Ring ID of the created Protection group; it must be an integer value between 0 and 31. The maximum numbers of ERPS Protection Groups that can be created are 32. Click the ID of a Protection group to enter the configuration page. After click Add button, one line will be directly created in the **ERPS Ring Setting** section. The ERPS Ring Setting section is a table that used to set up the ERPS Ring configuration.

Below is the description table.

TERMS	DESCRIPTION
Ring ID	Display the Ring ID
Version	ERPS Protocol Version - v1 or v2.
Ring State	**Default: Disable** Enable - Ring Status is enable Disable - Ring Status is disable
Node Role	It can be either RPL owner or RPL Neighbor or Ring Node.
Control Channel	**Default: 1** Control channel is implemented using a VLAN. Each ERP instance uses a tag-based VLAN for sending and receiving R-APS messages. (1-4094)
Sub Ring without Virtual Channel	**Default: False** **True** – If doesn't have any virtual channel **False** – If have a virtual channel
Virtual Channel of Sub Ring	**Default: 1** Sub-rings can have a virtual channel on the interconnected node. Choose the number based on the VLANs Range (1-4094)
Ring Port 0	This will create a Port 0 of the switch in the Ring. Choose the port number that belongs to Ring port 0
Ring Port 1	This will create Port 1 of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance. Choose the port

	number that belongs to Ring port 1
RPL Port	This allows user to select the east port or west port as the RPL block.
Revertive Mode	**Default: Revertive** **Revertive mode**, after the conditions causing a protection switch has been cleared; the traffic channel is restored to the working transport entity, which is, blocked on the RPL. In **Non-Revertive mode**, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.
Manual Switch	**Default: None** In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued. Choose 0 or 1, refers to Ring Port 0 or Ring Port 1
Force Switch	**Default: None** Forced Switch command forces a block on the ring port where the command is issued. Choose 0 or 1, refers to Ring Port 0 or Ring Port 1

ERPS Timer Setting



TERMS	DESCRIPTION
Guard Timer (ms)	Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2000 ms, with a default value of 100 ms.
WTR Timer (m)	The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes with a default value of 5 minutes.

3.6.2.2 ERPS STATUS

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

ERPS Status

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

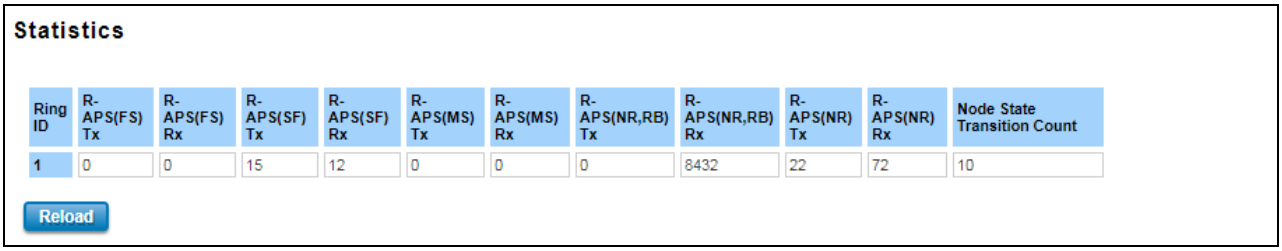
TERMS	DESCRIPTION
Ring ID	Display the Ring ID
Version	ERPS Protocol Version - v1 or v2.
Ring State	**Default: Disable** Enabled - Ring Status is enable Disabled - Ring Status is disable
Node State	Status from the **Ring is Idle, Protection** or **Pending.**
Node Role	It can be either **RPL owner** or **RPL Neighbor** or **Ring Node.**
Control Channel	Control Channel is referred to the VLANs number (1-4094)
Sub Ring without Virtual Channel	**Default: False** **True** – If have a virtual channel **False** – If doesn't have any virtual channel
Virtual Channel of Sub Ring	**Default: 1** Sub-rings can have a virtual channel on the interconnected node. Choose the number based on the VLANs Range (1-4094)
Ring Port 0	The status from the port Link up/link down and Forwarding/Blocking
Ring Port 1	The status from the port Link up/link down and Forwarding/Blocking
RPL Port	The port status as the RPL block.
Revertive Mode	**Default: Revertive** **Revertive mode**, after the conditions causing a protection switch has been cleared; the traffic channel is restored to the working transport entity, which is, blocked on the RPL. In **Non-Revertive mode**, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.
Manual Switch	Status from the Ring Port 0 and 1 or None
Force Switch	Status from the Ring Port 0 and 1 or None

Timer Status

Timer Status

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

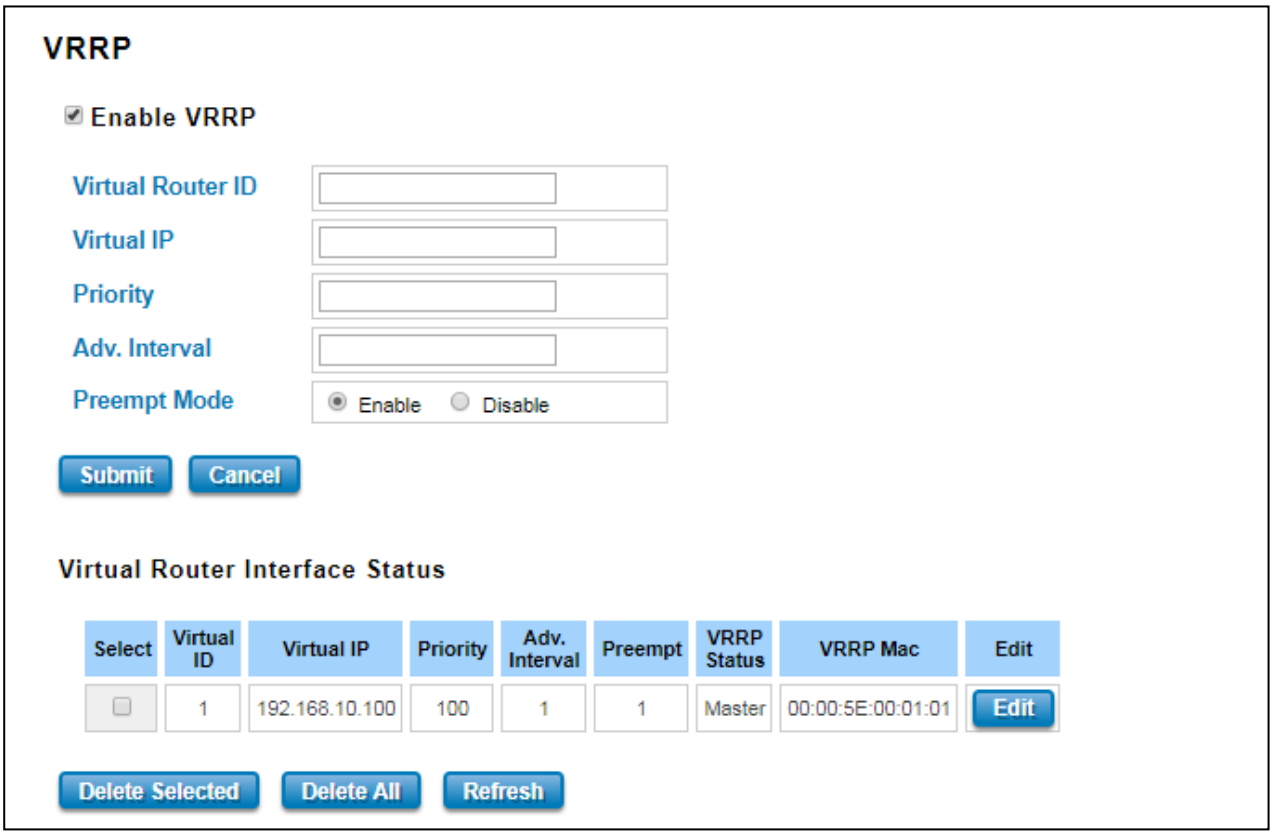
TERMS	DESCRIPTION
Ring ID	Display the Ring ID.
WTR Timer State	Running or not Running status.
WTR Timer Period (minute)	WTR timeout in milliseconds.
WTR Timer Remain (ms)	Remaining WTR timeout in milliseconds.
WTB Timer State	Running or not Running status.
WTB Timer Period (ms)	WTB timeout in milliseconds.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



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

3.6.3 VRRP

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



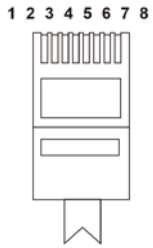
TERMS	DESCRIPTION
Select	Select the interface for the VRRP domain.
Virtual ID	This is a virtual ID range from 1~255. The switches within the same VRRP domain should have the same Virtual ID.
Virtual IP	This is the virtual IP of the VRRP domain. This is the Gateway IP of the clients.
Priority	The priority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

Adv. Interval	This field indicates how often the VRRP switches exchange the VRRP settings.
Preempt	While the VRRP Master link is failure, the VRRP Backup will take over its job immediately. However, while the VRRP master link is recovered, who should be the Master? The Preempt decide whether the VRRP master should be recovered or not. While the Preempt is **Enable** and the interface is VRRP Master, the interface will be recovered. While the Preempt is **Disable** and the interface is VRRP Master, there is no change while the link is recovered. The VRRP backup acts as the Master before restarting the switches.
VRRP Status	While the VRRP Master link is failure, the VRRP Backup will take over its job immediately
VRRP MAC	This field indicates the VRRP MAC in this configuration entry.
Edit	Click this button then the selected row can be edited.

3.7 SERIAL

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

Below is the pin definition

RJ45		RS-232	RS-422/485 (4 wire)	RS-485 (2 wire)
	1	DSR		
	2	RTS		
	3		GND	
	4	TxD	RX+	
	5	RxD	TX+	Data+
	6	DCD	TX-	Data-
	7	CTS		
	8	DTR	RX-	

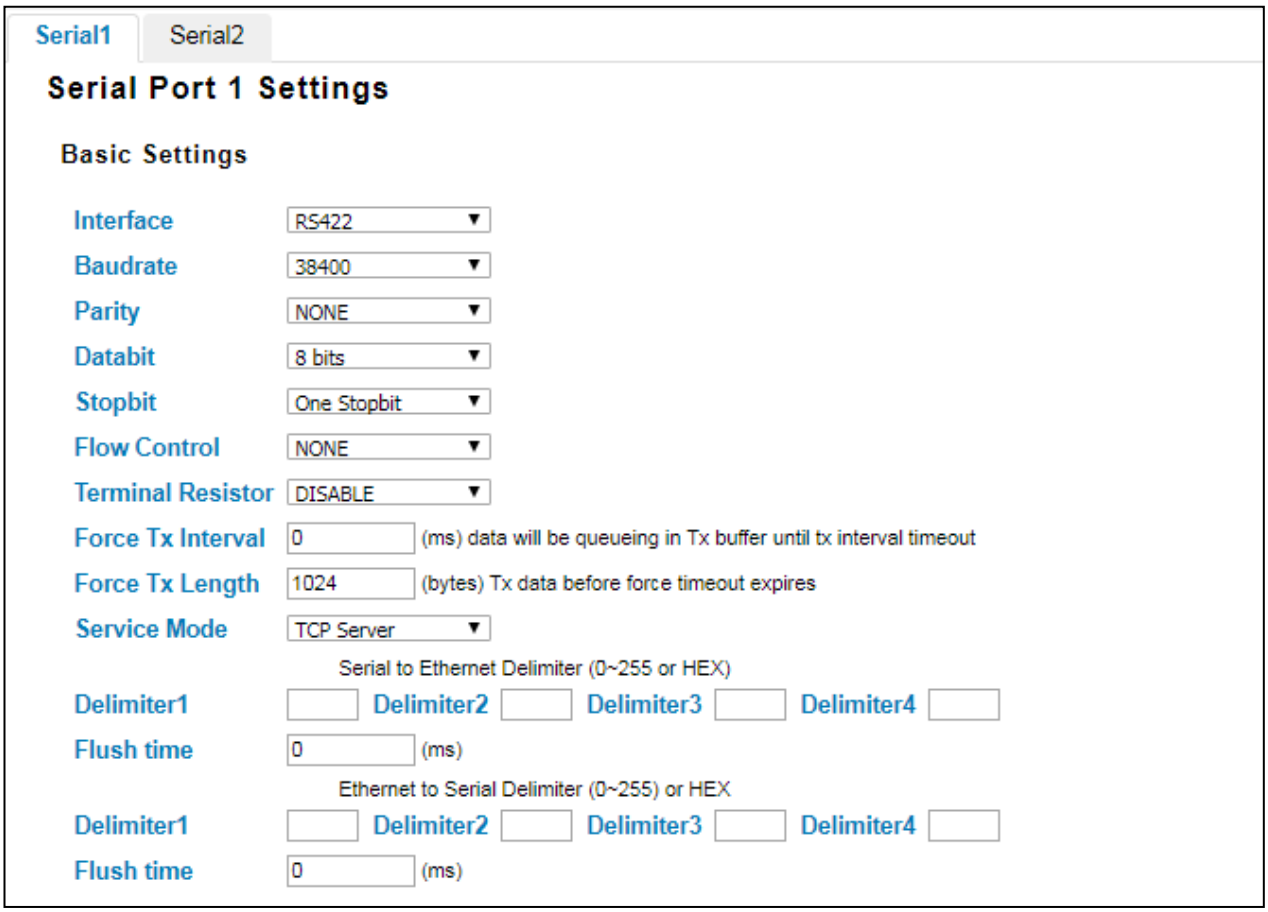
RS-232 is the most common serial interface and used to ship as a standard component on most Windows-compatible desktop computers. Now it is more common to use RS-232 over USB using a converter. RS-232 only allows for one transmitter and one receiver on each line. RS-232 also uses a Full-Duplex transmission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

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

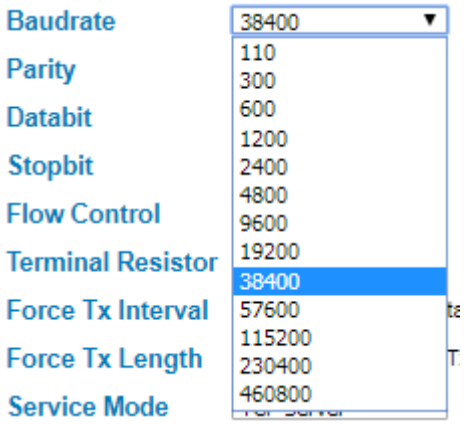
RS-485 is a superset of RS-422 and expands on the capabilities. RS-485 was made to address the multi-drop limitation of RS-422, allowing up to 32 devices to communicate through the same data line. Both RS-485 and RS-422 have multi-drop capability, but RS-485 allows up to 32 devices and RS-422 has a limit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

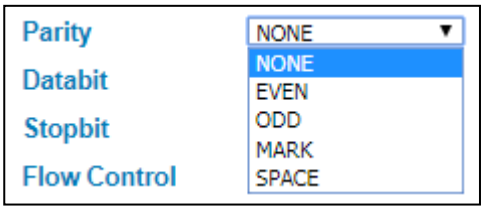
Serial 1 & 2

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

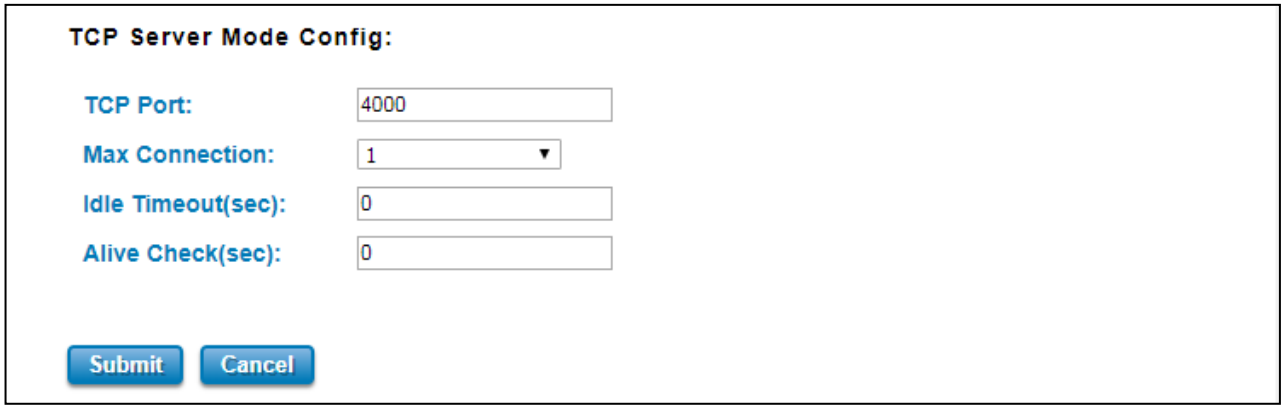


The description of the columns is as below:

TERMS	DESCRIPTION
Interface	**Default : RS422** Choose and change the interface type from the drop down list. The serial port supports the RS232, RS422, RS485-2w, and RS485-4w.
Baudrate	**Default: 38400** Serial baud rate, a speed measurement of communication. It indicates the number of bit transfers per second. 

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

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



The description of the columns is as below:

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

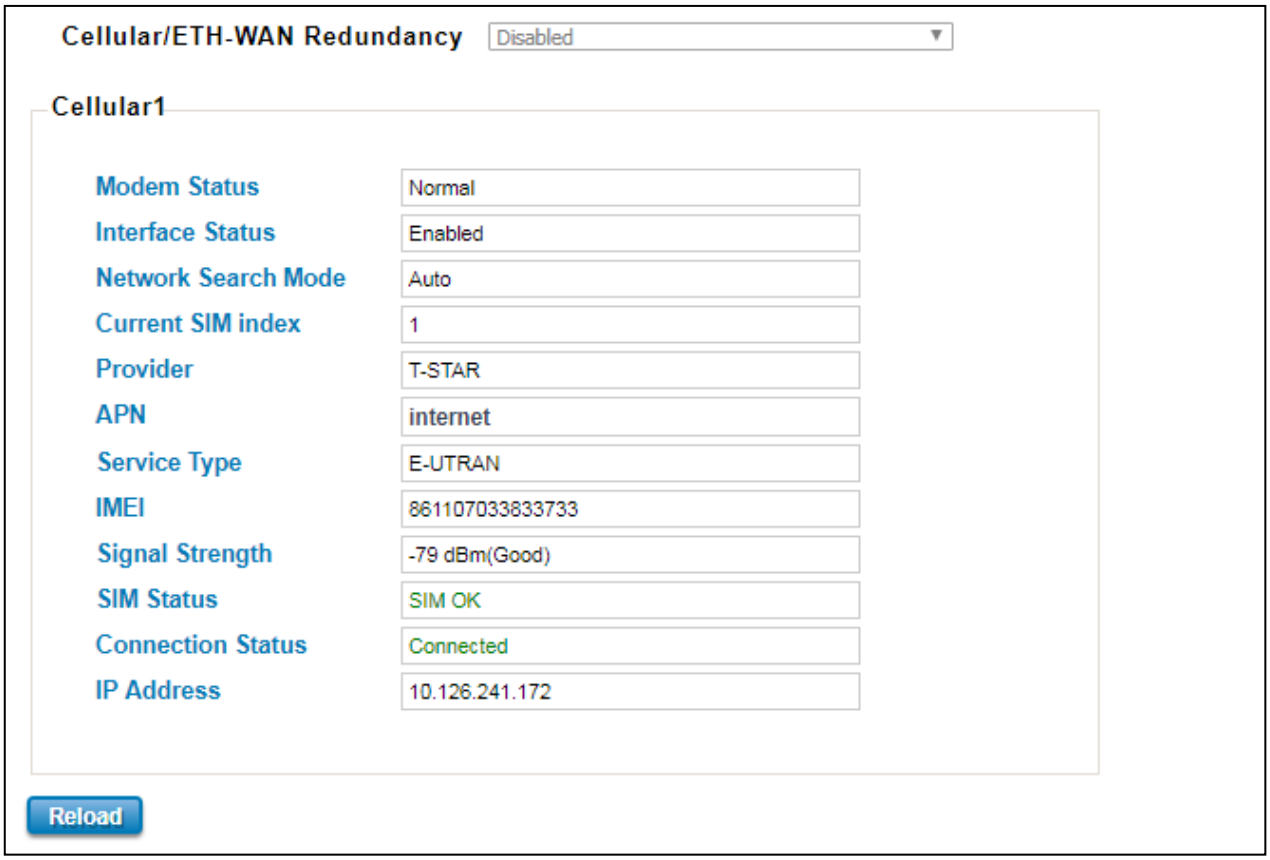
3.8 CELLULAR

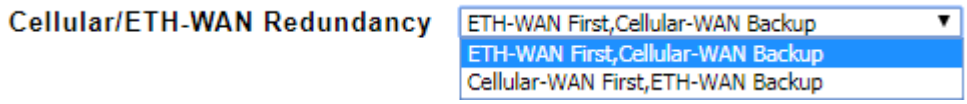
This Cellular page provides the Cellular Status; configure Cellular Setting, and configure SIM Setting. This SCB device is supported with redundant SIM or Dual SIM Card tray holder; user can choose SIM1 or SIM2 for the main SIM Card.

3.8.1 CELLULAR STATUS

The figure below shows Cellular Status.

The description of the columns is as below:



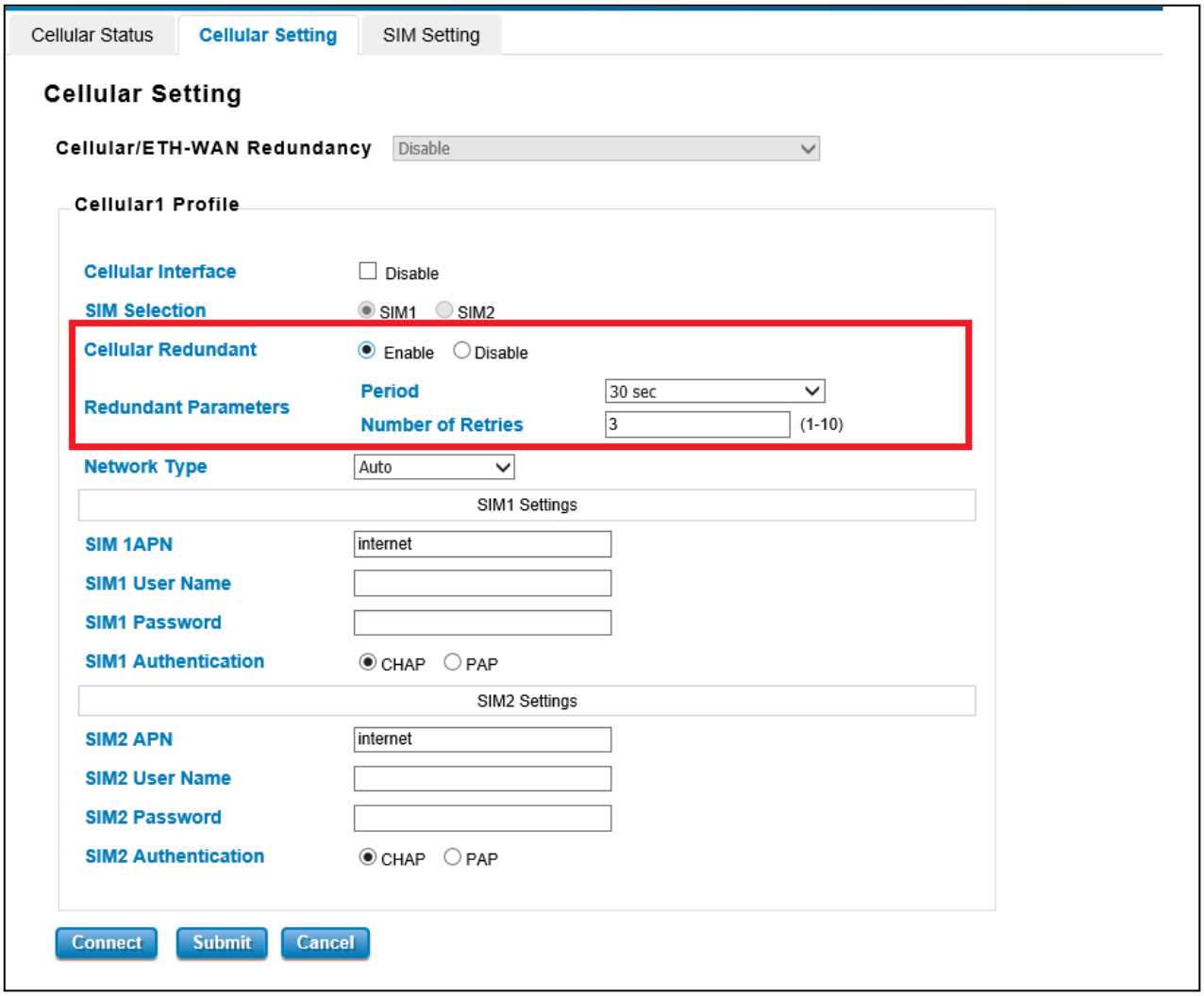
TERMS	DESCRIPTION
Cellular/ETH.WAN Redundancy	**Default: Disabled** User can choose the redundancy mode:  **ETH-WAN First, Cellular-WAN Backup**: by choosing this mode, the redundancy mode would be like prioritize the ETH-WAN connection; if the ETH-WAN connection has a problem then the Cellular-WAN would be the backup connection. **Cellular-WAN First, ETH-WAN Backup**: by choosing this mode, the redundancy mode would be like prioritize the Cellular-WAN connection; if the Cellular-WAN connection has a problem then the ETH-WAN would be the backup connection.

Modem Status	Display the modem status
Interface Status	Display the Cellular interface status Enabled or Disabled
Network Search Mode	Display the network search mode (Auto, 2G Only, 3G Only and LTE Only)
Current SIM Index	Display the current in used SIM card (1 or 2)
Provider	Display the ISP that user used.
APN	Every ISP has a specific APN (Access Point Name) assigned to its cellular network. The system can read this name from the SIM card.
Service Type	The connected ISP will update the service type here. The possible types are GSM – 2G, UMTS – 3G, GSM W/EGPRS, UTRAN W/HSDPA (download), UTRAN W/HSUPA(upload), UTRAN W/HSDPA and HSUPA(download & upload), E-UTRAN - LTE , No Service(default value)
IMEI	Display the International Mobile Equipment Identity (IMEI)
Signal Strength	The signal strength to the remote connected base station. If the signal strength shows low, please change the device location or mounting the antenna in better location. Below are the signal strength definitions in our system: 0 dBm (Default value while no connection) -113 dBm or less (Low) -111 dBm (Medium) -109…-53 dBm (Good) -51 dBm or greater (Excellent) -Not known or not detectable
SIM Status	Show the installed SIM Status. **SIM OK:** The SIM card is okay to use. **SIM not inserted:** The SIM card is not inserted. **SIM PIN Locked:** The SIM card is locked due to PIN error. It may be caused by error typing PIN password many times. **SIM PUK Locked:** The SIM Card PUK is locked due to PIN error after user three times input the wrong password. Contact the ISP to resolve the issue.
Connection Status	**Connection Status:** **Connected:** The cellular interface is connected. **Not Connected:** The cellular interface is not connected.
IP Address	The IP Address assigned by the ISP. While the cellular is connected, the IP address will display here.

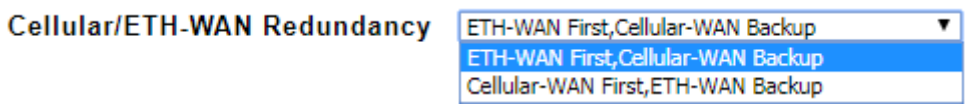
3.8.2 CELLULAR SETTING

This section displays the Cellular Setting configuration page and also in this configuration page user may activate the redundant SIM function. In this section, user may configure the Cellular Interface, SIM Selection, Cellular Redundant, Network Type, SIM1/2 APN, User Name, Password and the Authentication mode.

The figure below is the interface of SCB Web GUI that included the Dual SIM function and the SIM Redundancy function:



The description of the columns is as below:

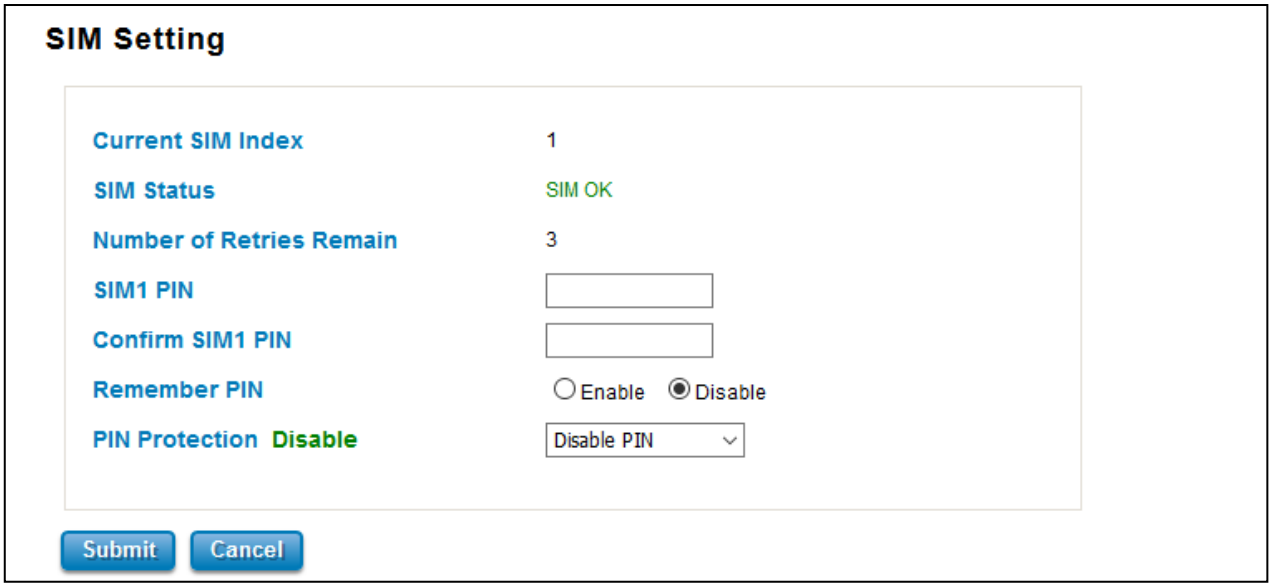
TERMS	DESCRIPTION
Cellular/ETH.WAN Redundancy	**Default: Disabled** User can choose the redundancy mode:  **ETH-WAN First, Cellular-WAN Backup**: by choosing this mode, the redundancy mode would be like prioritize the ETH-WAN connection; if the ETH-WAN connection has a problem then the Cellular-WAN would be the backup connection. **Cellular-WAN First, ETH-WAN Backup**: by choosing this mode, the redundancy mode would be

	like prioritize the Cellular-WAN connection; if the Cellular-WAN connection has a problem then the ETH-WAN would be the backup connection.
Cellular Interface	To enable or disable the cellular interface. Click check to disable the function.
SIM Selection	**Default: SIM1** User can select the SIM card 1 or 2 that want to be activated or used.
Cellular Redundant	**Default: Disable** By enable this function, the SIM redundant function will be activated. The main function of this feature is to have the backup SIM if the main SIM card is unable to use or have a problem connection. **Redundant Parameters** configuration appears after the user enables the function. **Period:** Set the period time to read the SIM card, if the SIM card cannot be read then it will directly change to the other SIM card. The default value is 30 Seconds. **Number of Entries:** Set the number of entries to give the remaining trial to read the SIM card. The default value is 3.
Network Type	Set the Network Type, the option would be: **Auto: Search the network automatically** **2G Only: only receive the 2G signal.** **3G Only: only receive the 3G signal.** **LTE Only: only receive LTE/4G signal.**
SIM1/2 APN	Set the APN of the ISP.
SIM1/2 User Name	Set the User Name
SIM1/2 Password	Set the password.
SIM1/2 Authentication	Choose CHAP or PAP mode for the authentication mode. **CHAP**: Challenge Handshake Authentication Protocol, With CHAP, the authenticator (i.e. the server) sends a randomly generated ``challenge'' string to the client, along with its hostname. **PAP**: Password Authentication Protocol, PAP works basically the same way as the normal login procedure. The authenticates itself by sending a username and a password to the server

Click **Submit** to apply the configuration.

3.8.3 SIM SETTING

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

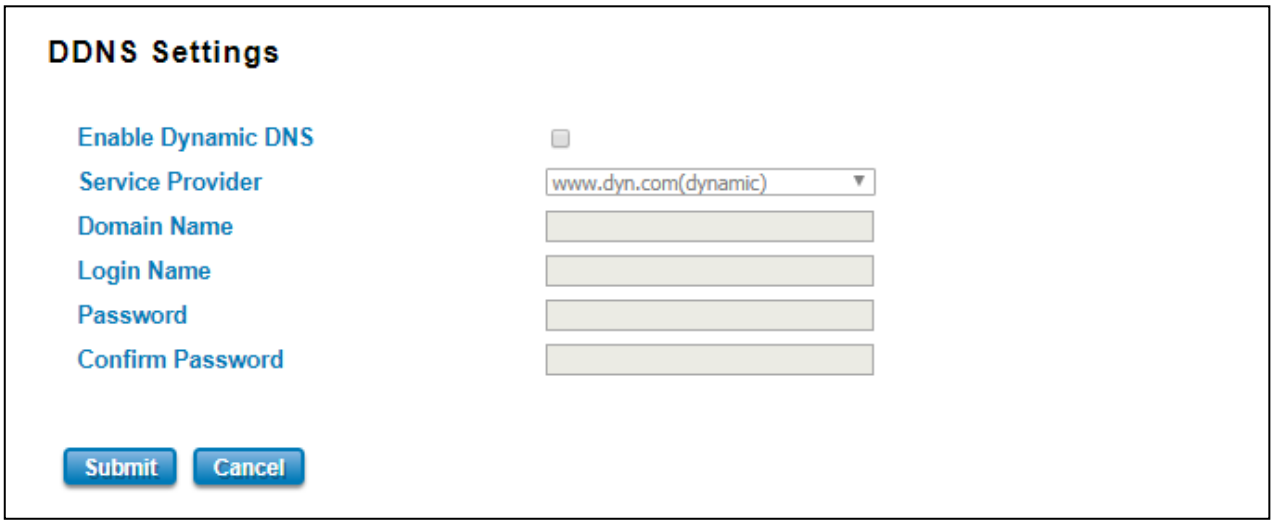


TERMS	DESCRIPTION
Current SIM Index	Display the current in used SIM Card slot (1 / 2)
SIM Status	Show the installed SIM Status. **SIM OK:** The SIM card is okay to use. **SIM not inserted:** The SIM card is not inserted. **SIM PIN Locked:** The SIM card is locked due to PIN error. It may be caused by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

Click **Submit** to apply the configuration.

3.8.4 DDNS SETTING

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



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

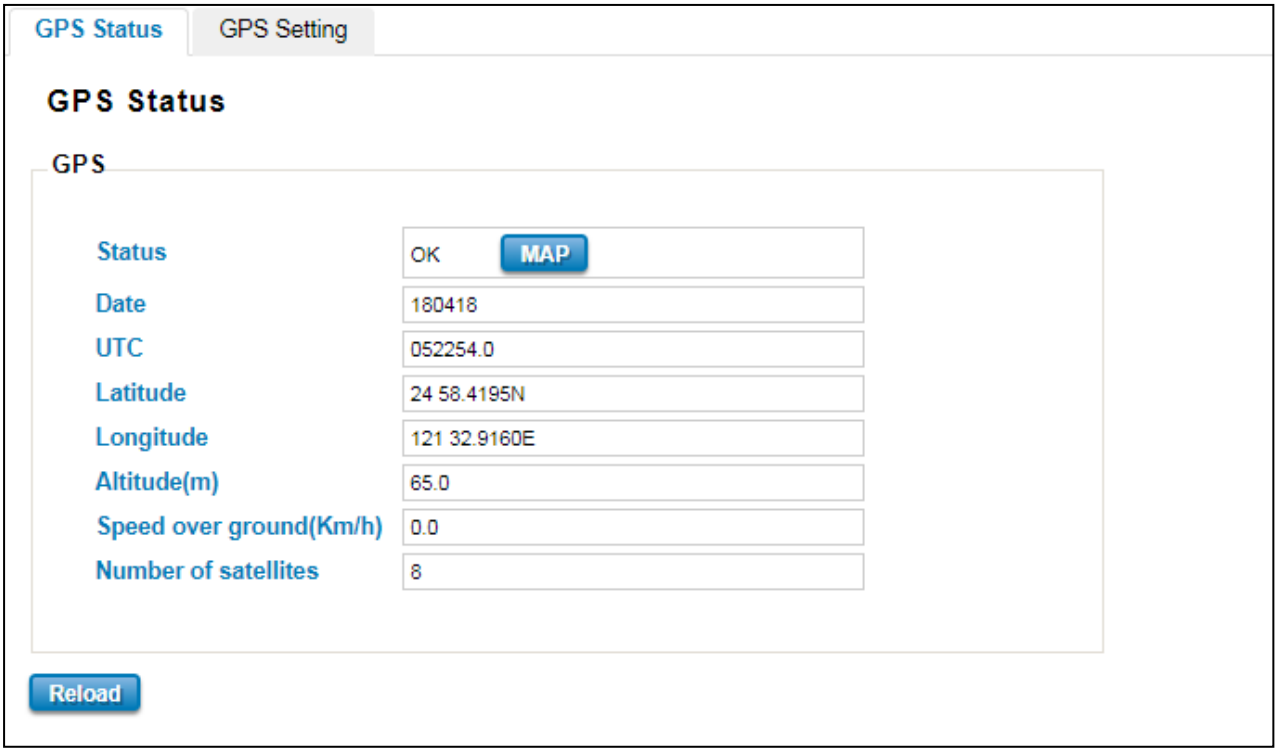
Click **Submit** to apply the configuration.

3.9 GPS

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

3.9.1 GPS STATUS

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

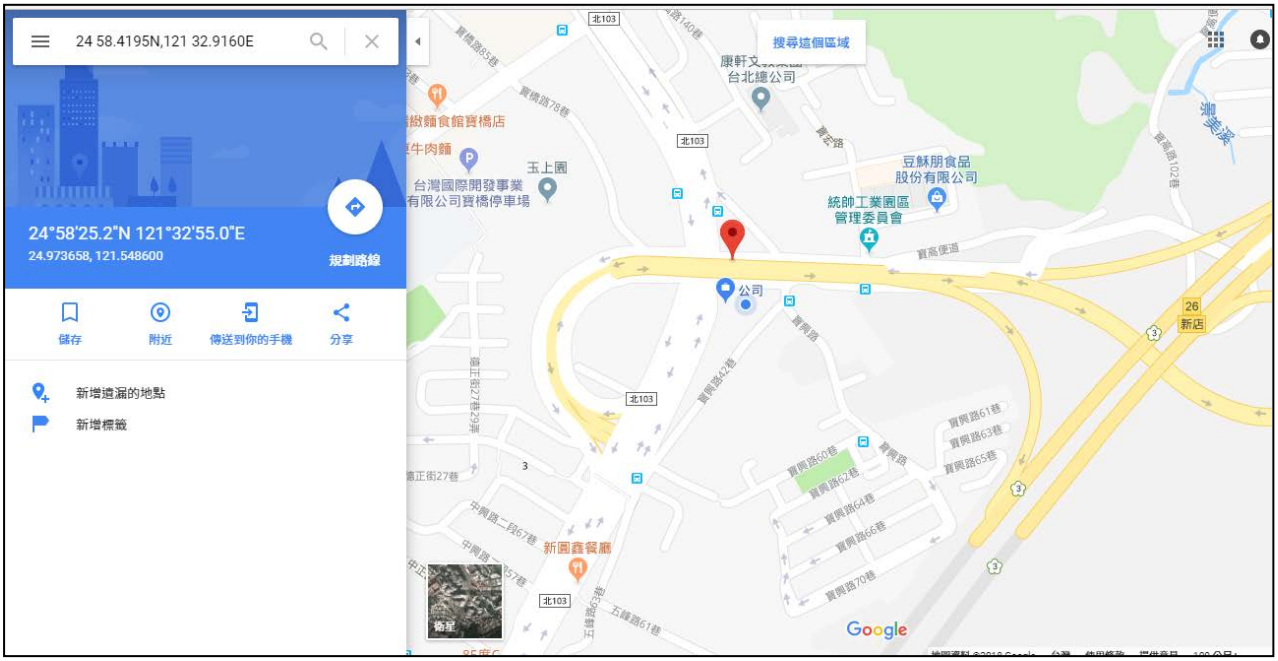


The description of the columns is as below:

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

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

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



3.9.2 GPS SETTING

In this GPS Setting section, user can disable the GPS Interface by check the Disable. After user disables the function the GPS Status will show disabled status for the GPS function.

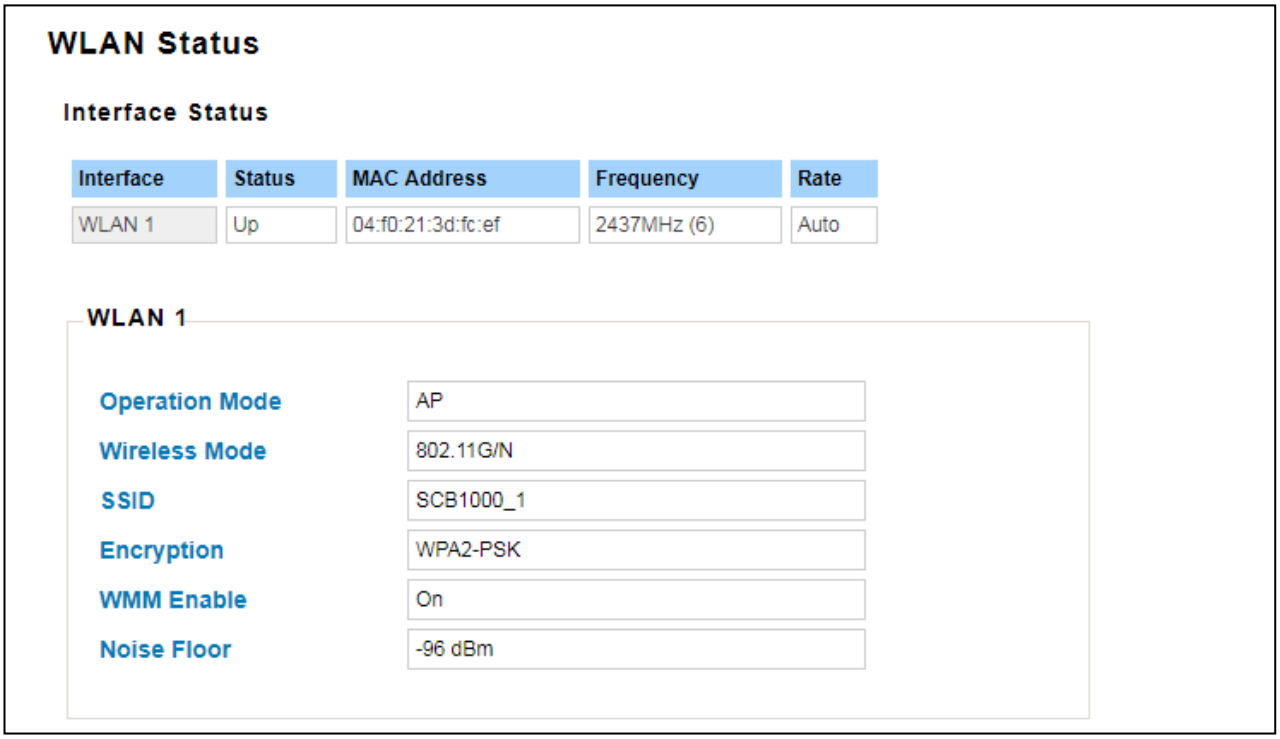


3.10 WIRELESS LAN

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 and the Auto Offload.

3.10.1 WLAN STATUS

The figure below shows the WLAN status.



The description of the columns is as below:

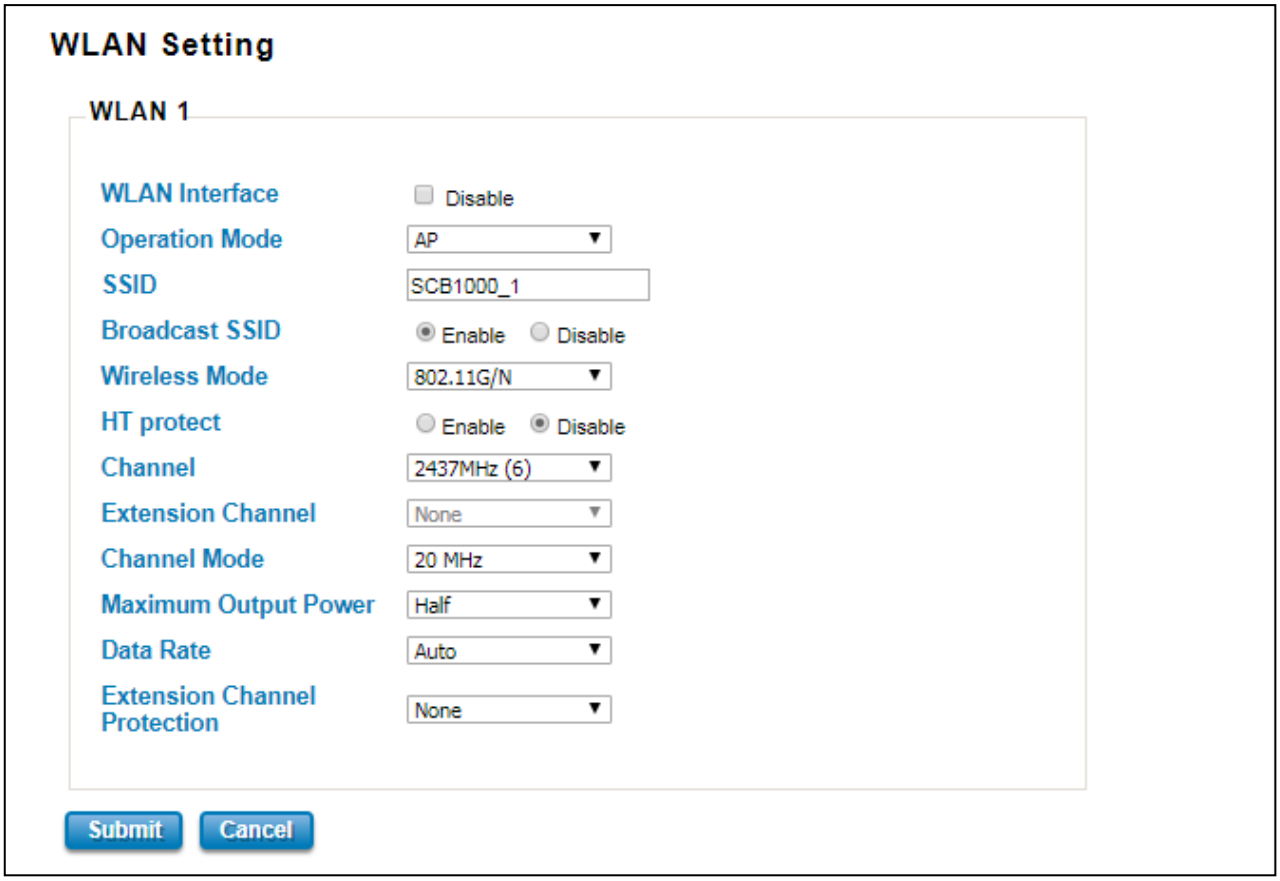
TERMS	DESCRIPTION
Operation Mode	Display the current operating modes on the device
Wireless Mode	Display the current wireless mode
SSID	Display the primary name of the SSID
Encryption	Display the encryption mode.
WMM Enable	Display the status of the WMM support.
Noise Floor	Display the background noise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

3.10.2 WLAN SETTING

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

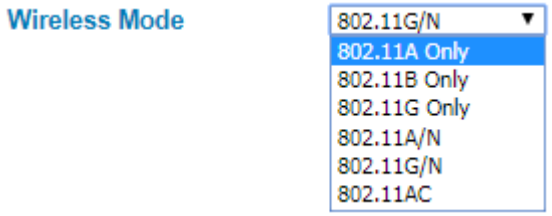
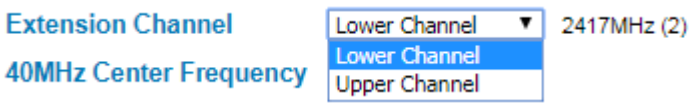
AP

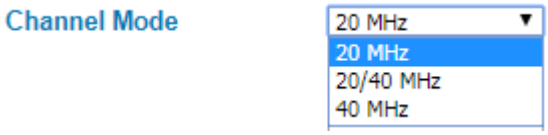
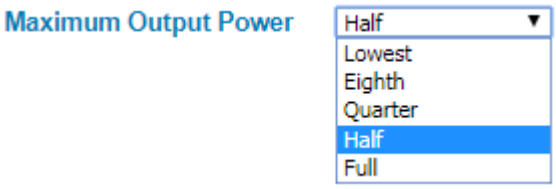
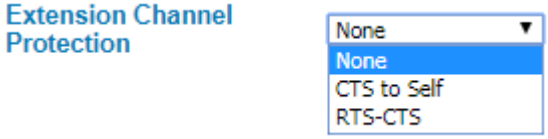
The Access Point mode, it establishes a wireless connection, receives from wireless clients and provides connection for wireless client devices, the client can search and connect to several the access points. In AP mode interface, user can configure the SSID name, Enable or Disable Broadcast SSID, select 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: SCB1000_1** Input the primary name of the access point.
Broadcast SSID	**Default: Enabled.**

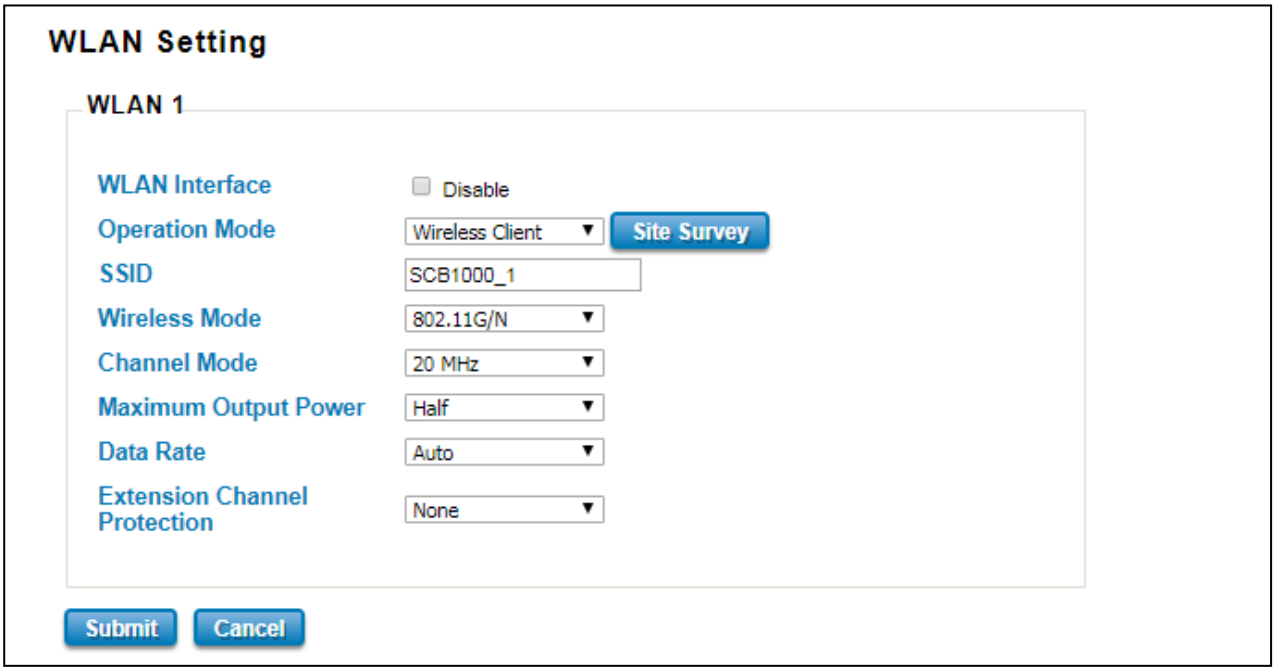
	By enabling the broadcast SSID, it makes the AP can be accessed and searched by the clients, and for the security concern by disabling this broadcast SSID, the network will be hidden in order to prevent any malicious attack.
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different 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 feature 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 appear when user selects 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 selects 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequencies, 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.

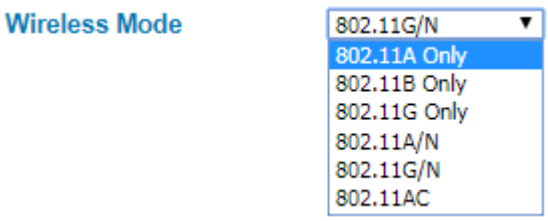
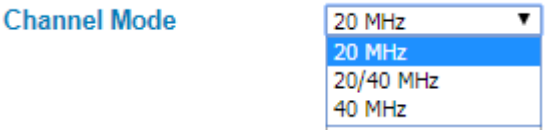
Click **Submit** to apply the configuration

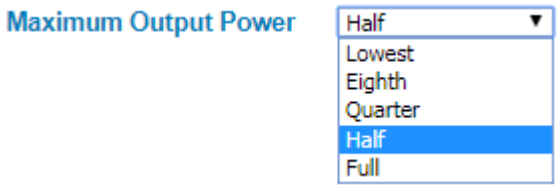
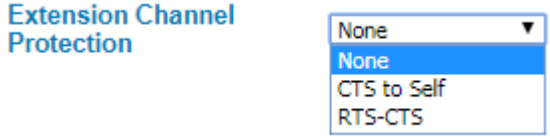
Wireless Client

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



The description of the columns is as below:

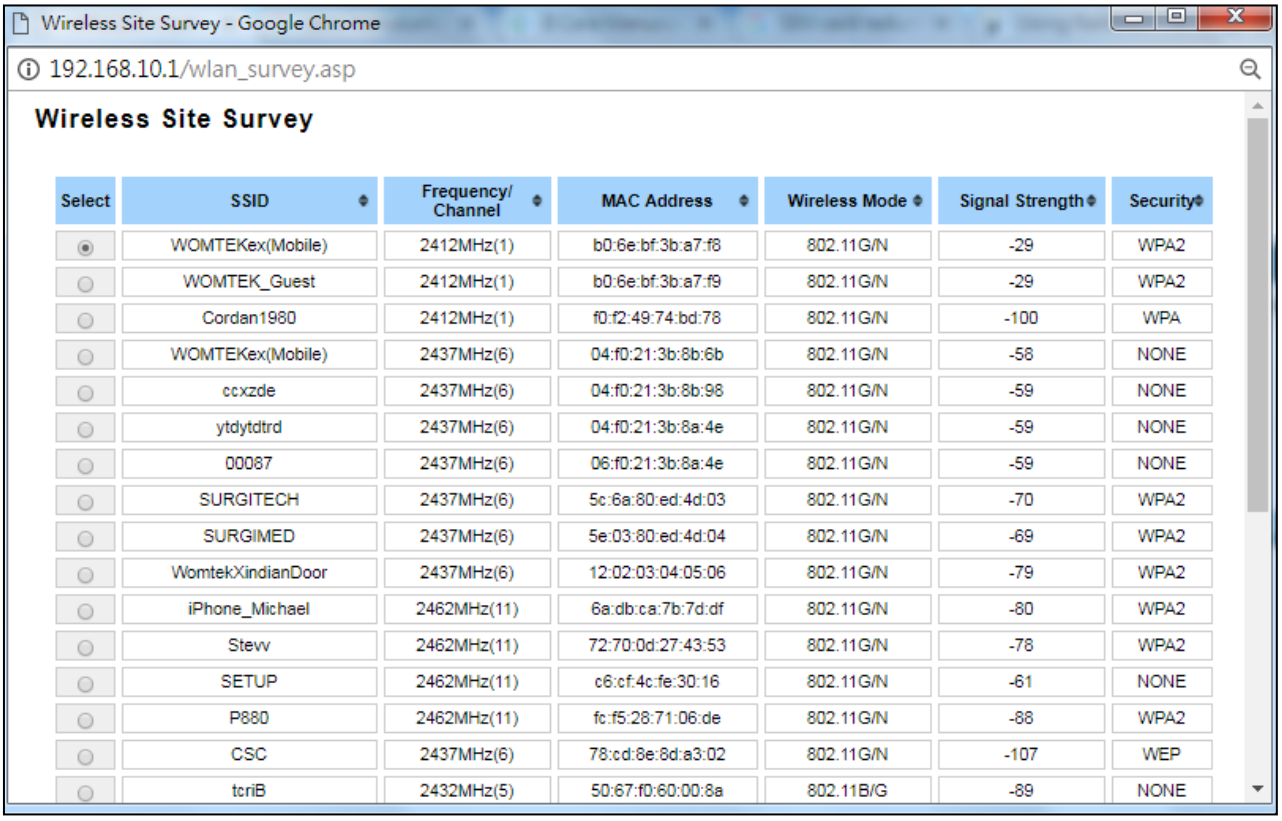
TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless functions.
Operation Mode	Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP, and WDS-Client)
SSID	**Default: SCB1000_1** Input the primary name of the access point.
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has a different configuration. For each wireless mode, it has a specific frequency and it has different basic setting. 
Channel Mode	**Default: 20MHz** 

	There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user selects 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequencies, 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 lower rate when there is no great demand for transmission speed, for long distance transmission.
Extension Channel Protection	 Select from the drop down list option between **CTS-Self or RTS-CTS** to avoid conflict with other wireless network and to improve the ability of the device to catch all the wireless transmissions. By activating this function, it may decrease wireless network performance.

Click **Submit** to apply the configuration

Wireless Site Survey (Wireless Client & WDS-Client)

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



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

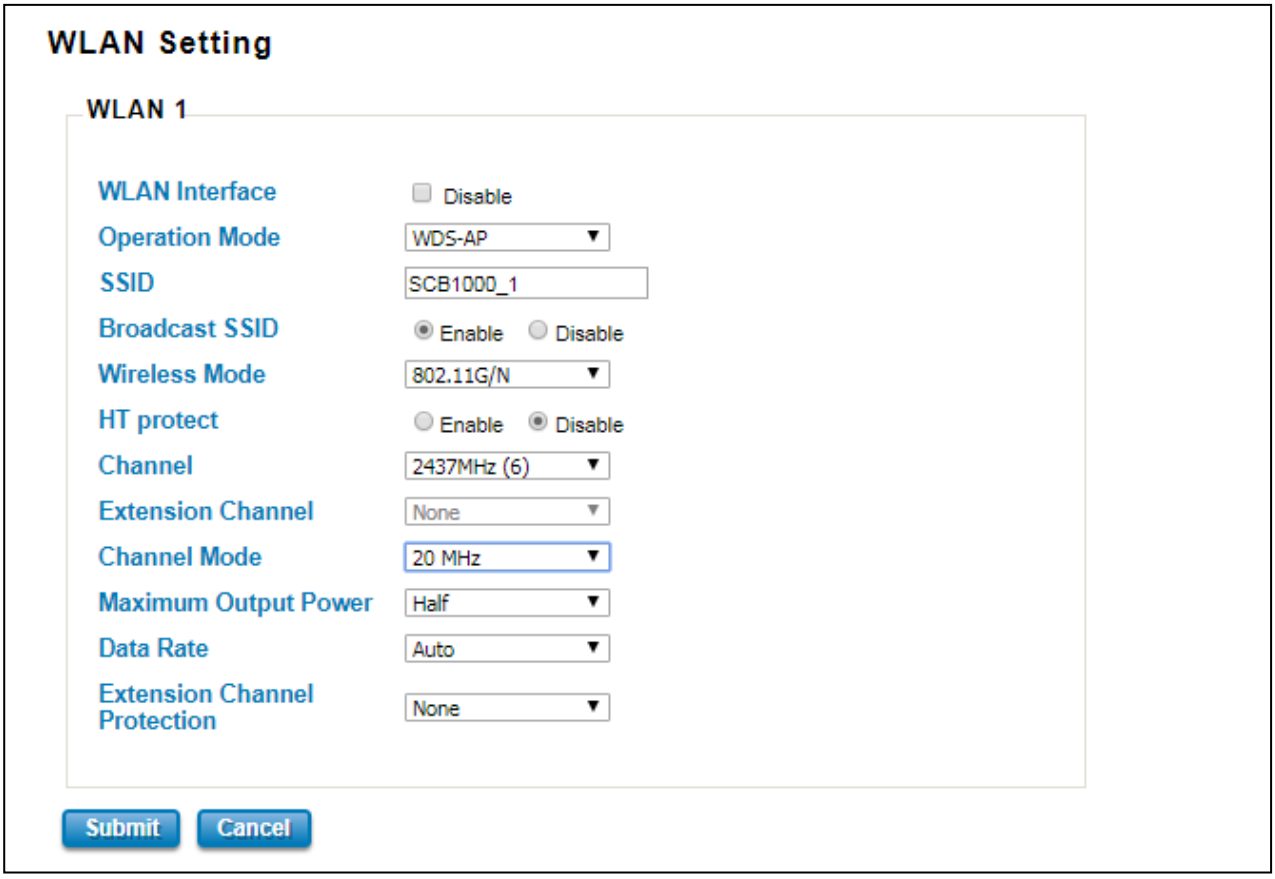
The description of the columns is as below:

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

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

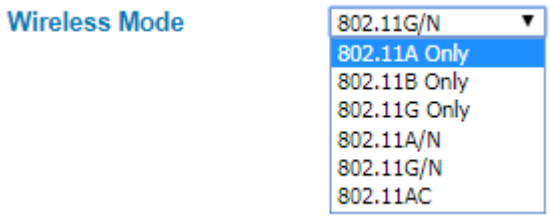
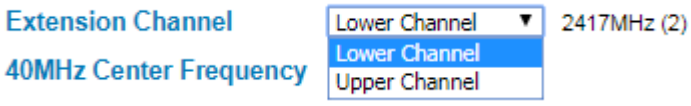
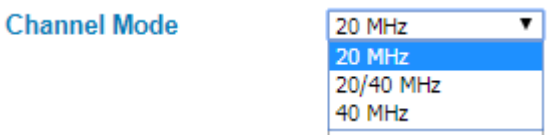
WDS-AP

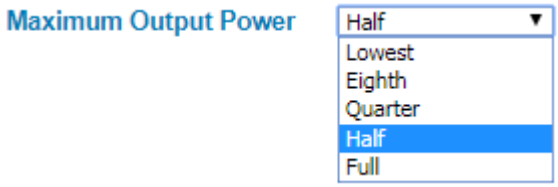
The WDS-AP mode usually implements the Point to Point (P2P) connection, so the access point should be WDS-AP and the wireless client should be WDS-Client. So in this case, the AP just can share the connection to the specific wireless client that has its MAC Address. But WDS-AP can be a repeater to provide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



The description of the columns is as below:

TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless function.
Operation Mode	Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	**Default: SCB1000_1** Input the primary name of the access point.
Broadcast SSID	**Default: Enabled.** By enabling the broadcast SSID, it makes the AP can be accessed and searched by the clients, and for the security concern by disabling this broadcast SSID, the network will be hidden in order to prevent any malicious attack.
Wireless 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

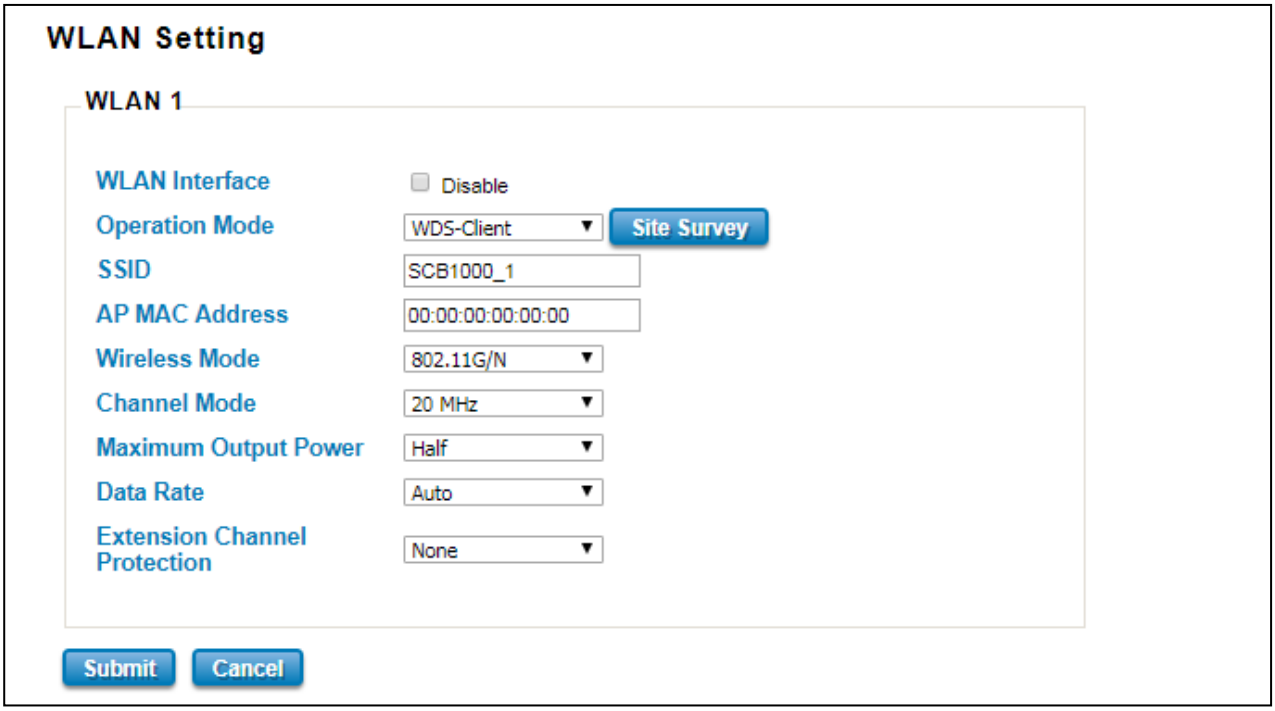
	different basic setting. 
HT Protect	**Default: Disabled** Select Enabled to activate the High Throughput protect to ensure HT transmission with MAC mechanism.
Channel	**Default: 2437MHz (6)** Select the proper channel, each country has different band user may select the channel based on the situation. 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 frequencies, 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.

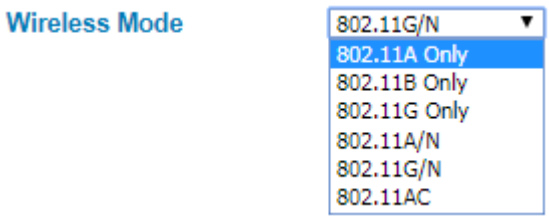
Click **Submit** to apply the configuration

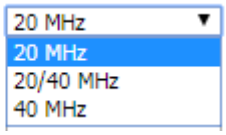
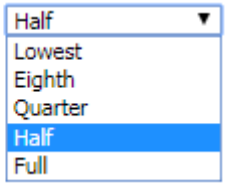
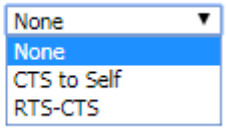
WDS-Client

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



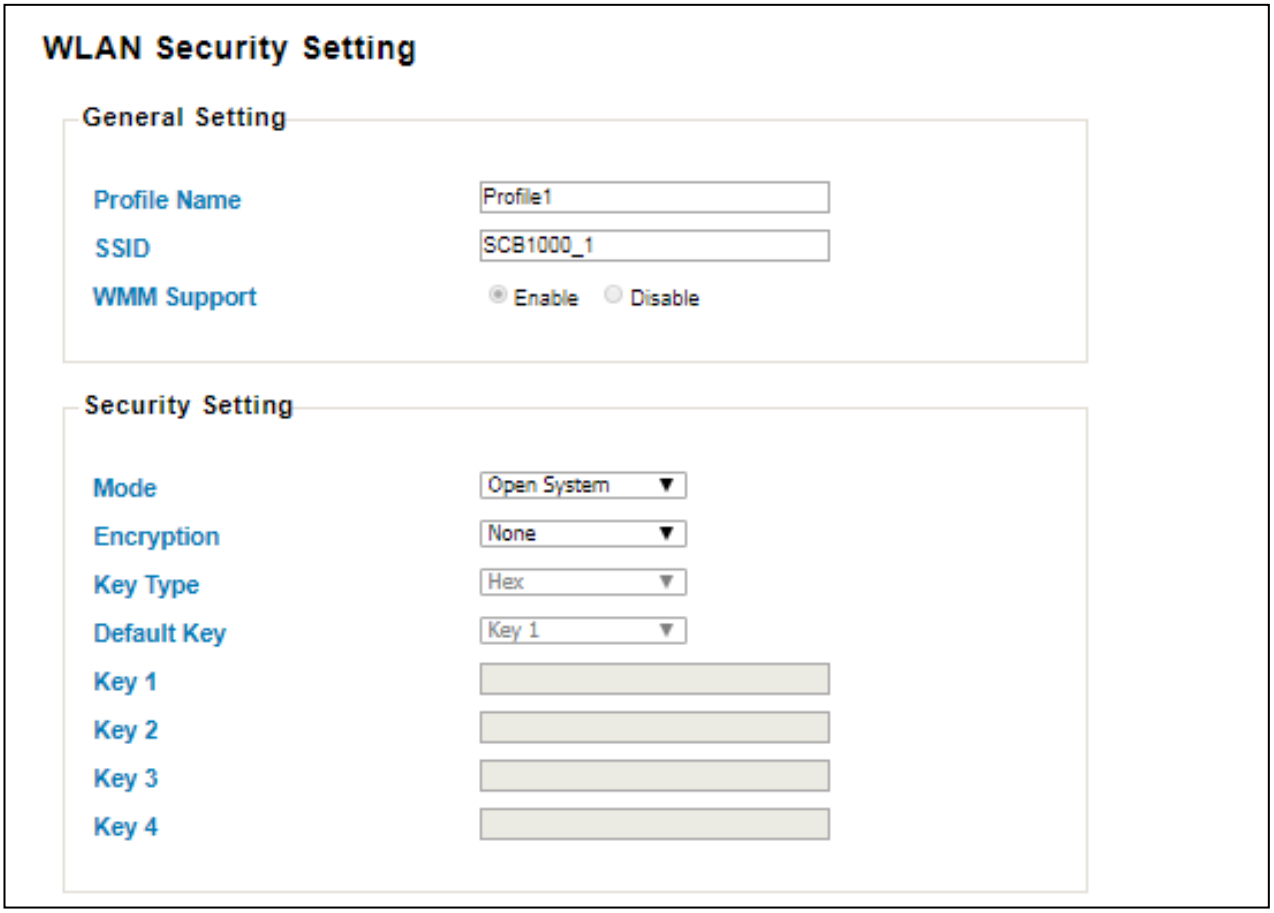
The description of the columns is as below:

TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless functions.
Operation Mode	Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	**Default: SCB1000_1** Input the primary name of the access point.
AP MAC Address	**Default: 00:00:00:00:00:00** Set the specific AP MAC Address of the WDS-AP.
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has a different configuration. For each wireless mode, it has a specific frequency and it has different basic setting. 
Channel Mode	**Default: 20MHz**

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

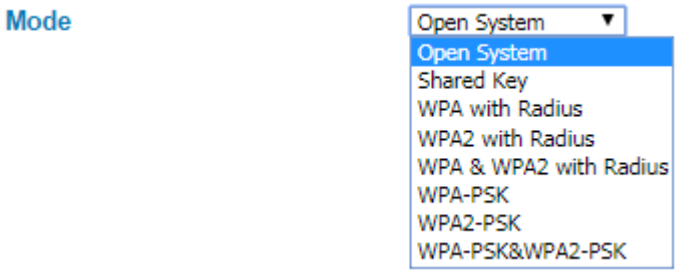
3.10.3 WLAN SECURITY

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



The description of the columns is as below:

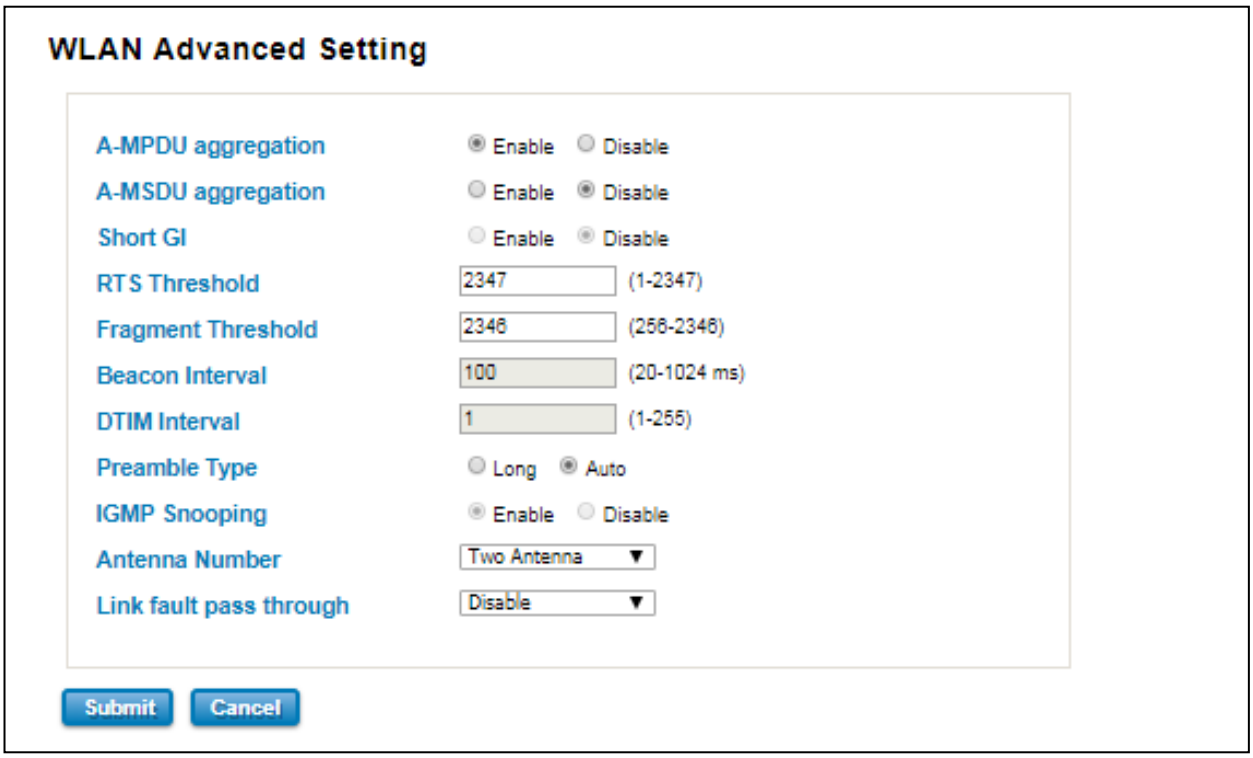
TERMS	DESCRIPTION
Profile Name	**Default: Profile1** **Set the profile name for the Access Point.**
SSID	**Default: SCB1000_1** Set the Service Set Identifier name, this ID can be recognized by the Client when the WLAN connection is established**.**
Broadcast SSID	**Default: Enabled.** By enabling the 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: 64 (0-64)** Set the maximum number of station that can communicate with the access point.
Mode	**Default: Open System**  **Open System**: It allows any device to join the network without security checks. **Shared Key**: Data encryption and key are required for the authentication. **WPA with RADIUS**: With warrant (username, password and etc.) offered by user, this kind of authentication can be realized with specific RADIUS server. **WPA2 with RADIUS**: 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 with RADIUS**: 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 can 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.
Encryption	Configure the data encryption mode. ● **None**: Available only when the authentication type is an open system. ● **64 bits WEP**: It is made up of 10 hexadecimal numbers. ● **128 bits WEP**: It is made up of 26 hexadecimal numbers. ● **TKIP**: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK. ● **AES**: Advanced Encryption Standard, it is usually co-used with WPA2-PSK.
Key Type	**Default: Hex** WEP can be configured with a 64-bit or 128-bit Shared Key (hexadecimal or ASCII). As defined, hexadecimal number is represented by 0-9, A-F or a-f; ASCII is represented by 0-9, A-F, a-f or punctuation. Each one consists of two-digit hexadecimal.
Default Key	**Default: Key 1** Set the specific default key.
Key 1~4	Enter the specific encryption key.

3.10.4 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 user does not need to change the default setting except user knows 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 by sending 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 provides two antenna sockets. User can configure One Antenna or Two Antenna. Please refer to the Antenna Placement table to connect the antenna correctly.

3.10.5 ACCESS CONTROL (AP MODE)

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

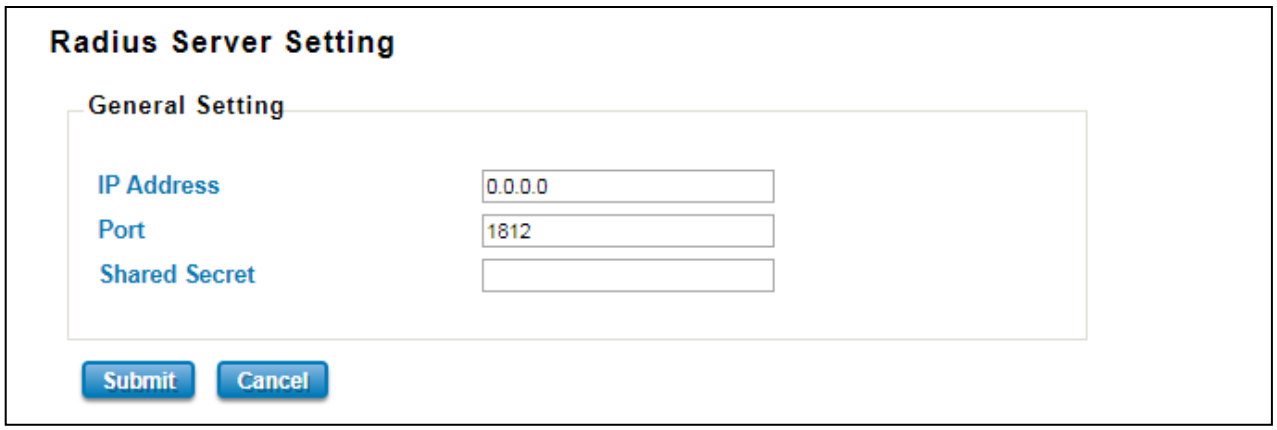


The description of the columns is as below:

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

3.10.6 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).

3.11 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:

3.11.1 Access Control

3.11.2 Port Security

3.11.3 Outbound Firewall

3.11.4 NAT Setting

3.11.5 OpenVPN

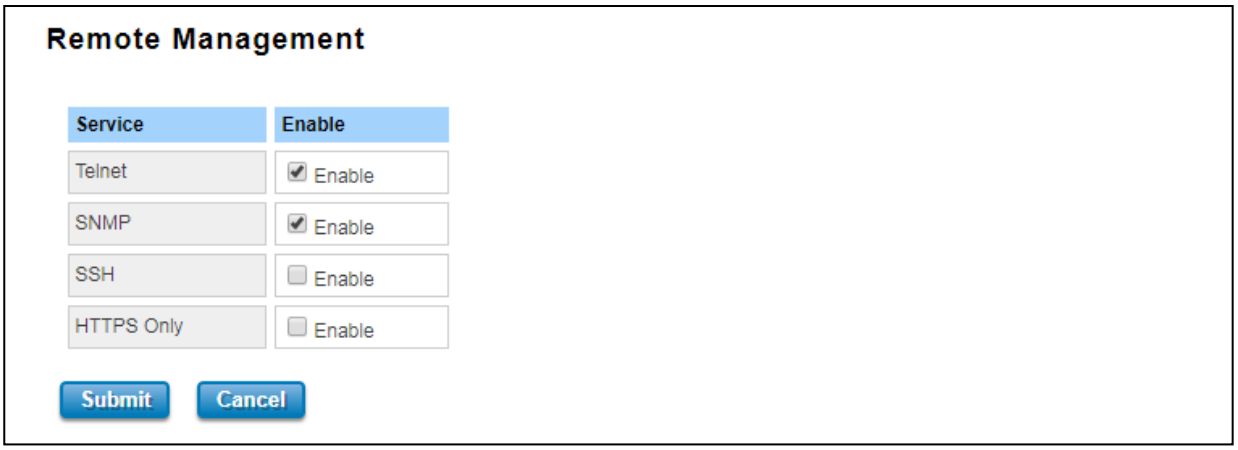
3.11.6 IPSec Setting

3.11.1 ACCESS CONTROL

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

Remote Management

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



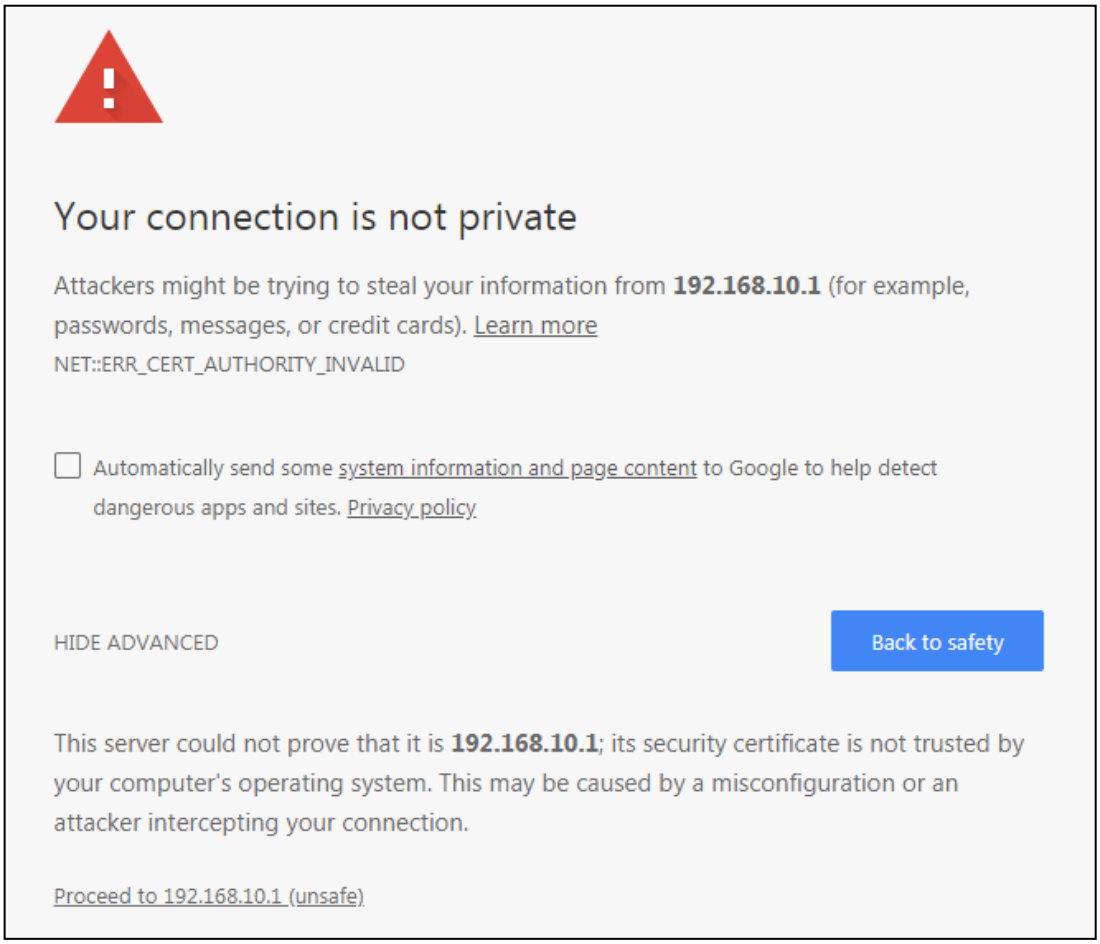
The description of the columns is as below:

TERMS	DESCRIPTION
Telnet	Allows the user to remotely login and access 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 access 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 access 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 access 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 website, 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 accesses the device in order to provide a secure access. The picture above is the warning message about the digital certificate and user just needs to accept this warning by click **"Proceed to 192.168.10.1 (unsafe)"**.

WAN Access

When user changes the device to **router mode (Port 1 – WAN interface)** then the WAN Access feature can be activated. This feature is about the exception to access the device through the WAN interface for security concern. So that the access or the traffic that coming through the WAN interface can be limited as required. The user may choose the **Filter All** functions to block all access from the WAN interface or enable the exception options, then the router allows user to remotely access to the router from WAN interface.



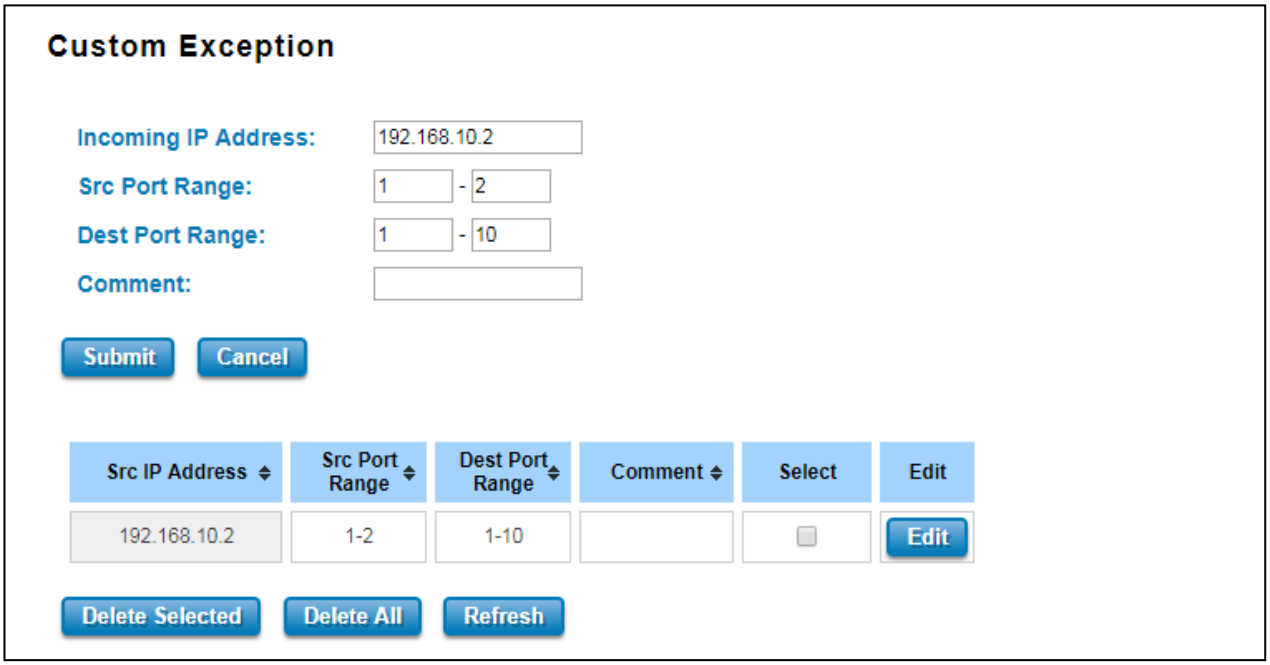
The description of the columns is as below:

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

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

Custom Exception

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



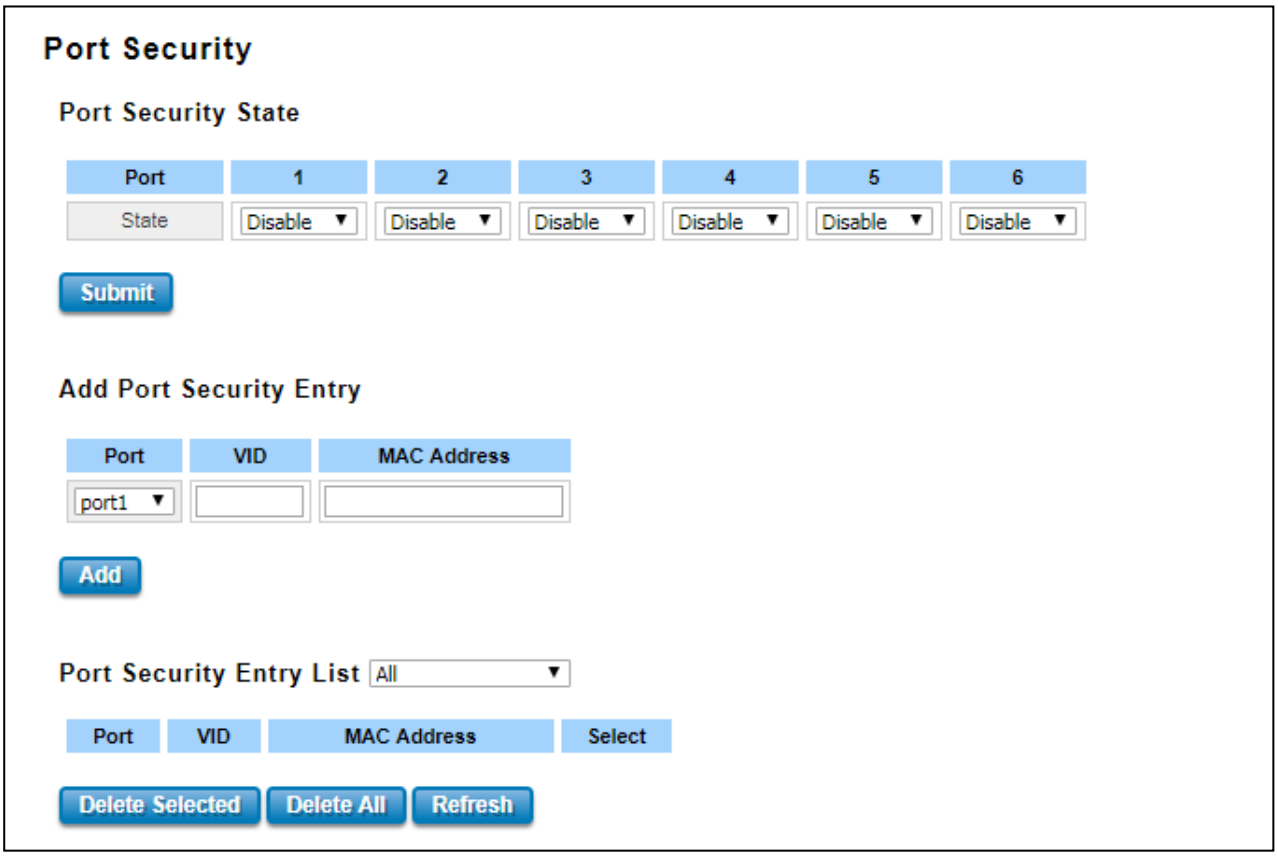
The description of the columns is as below:

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

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

3.11.2 PORT SECURITY

Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. By using Port Security feature user allowed denying any kind of accesses from unidentified MAC Address. Only the MAC addresses that listed in Port Security List that can access the switch and do the transmission. Through this method user may avoid any kind of attacks from hackers.



The description of the columns is as below:

TERMS	DESCRIPTION
Port Security State	**Default: Disable** Change Port Security State of the port to Enable first.
Add Port Security Entry	Select the port, and type VLAN ID and MAC address. Format of the MAC address is xxxx.xxxx.xxxx. Ex: 9466.e79f.5678. Max volume of one port is 10. So the system can accept 100 Port Security MAC addresses in total.
Show Port Security List	This table shows User those enabled port security entries. User can click on **Delete Selected/ Delete All** to delete the entry.

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

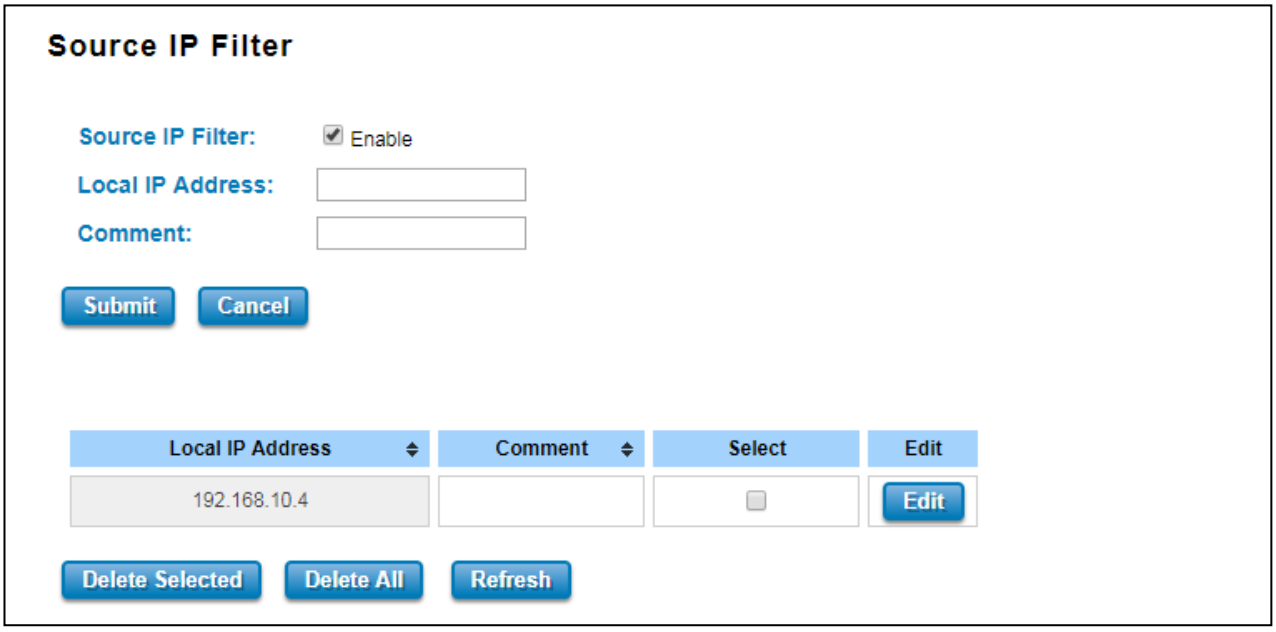
3.11.3 OUTBOUND FIREWALL

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

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

Src IP Filter

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



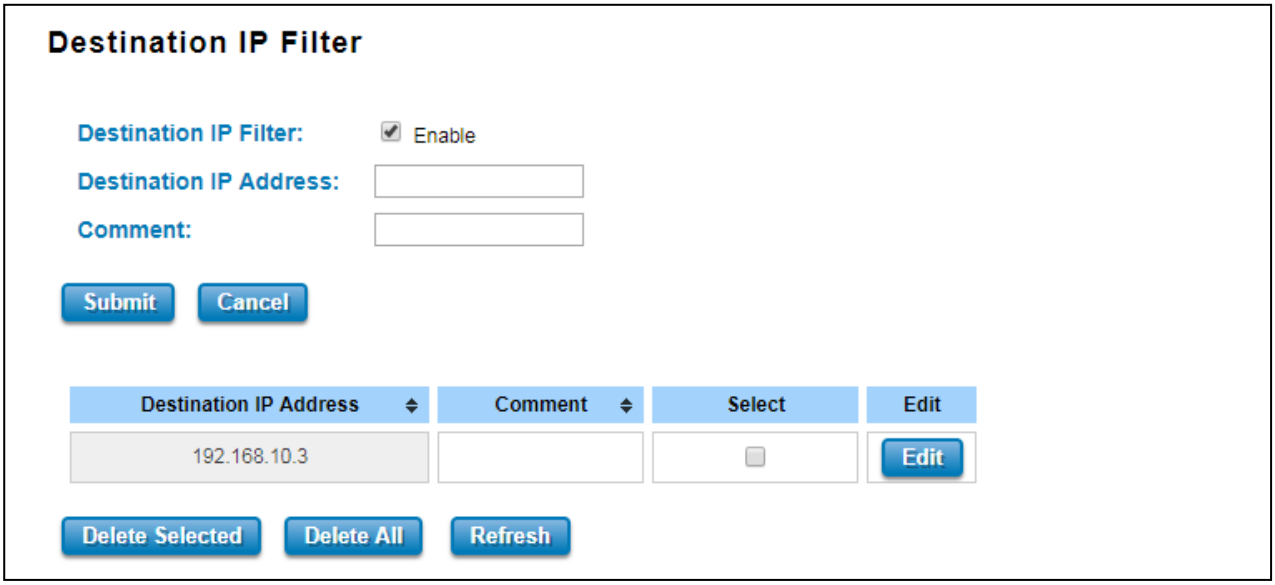
The description of the columns is as below:

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 the list.
Edit	Click edit to modify the parameters

Click **Refresh** to refresh the table

Dest IP Filter

By entries the 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 the list.
Edit	Click edit to modify the parameters

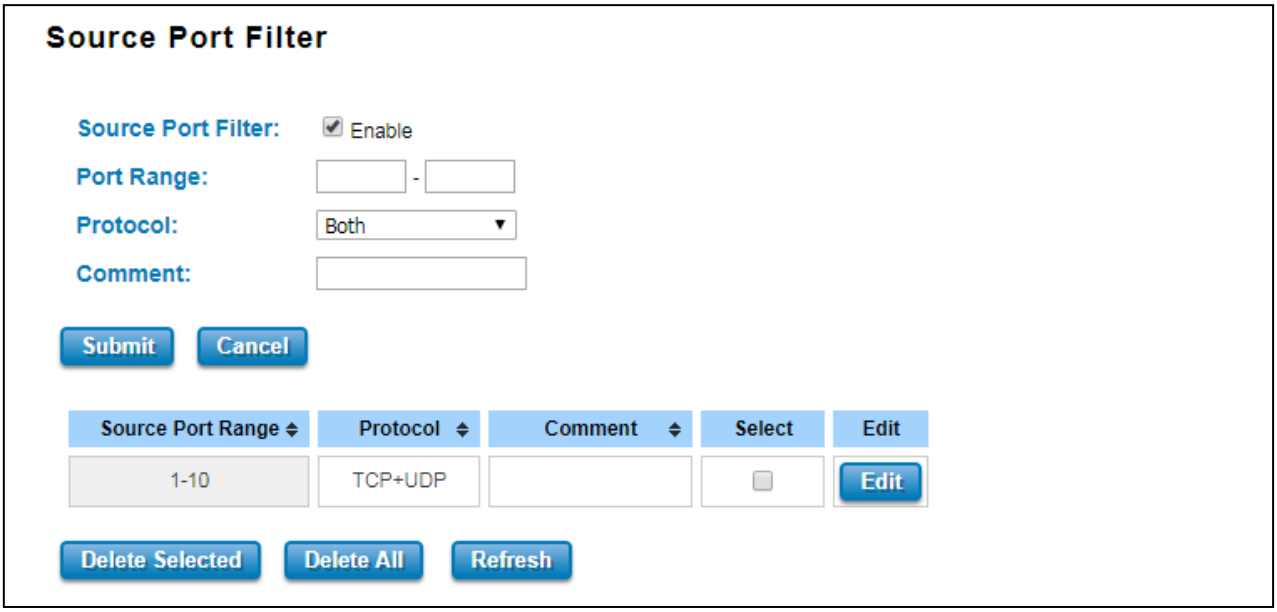
Click **Refresh** to refresh the table

Src Port Filter

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

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

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



The description of the columns is as below:

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

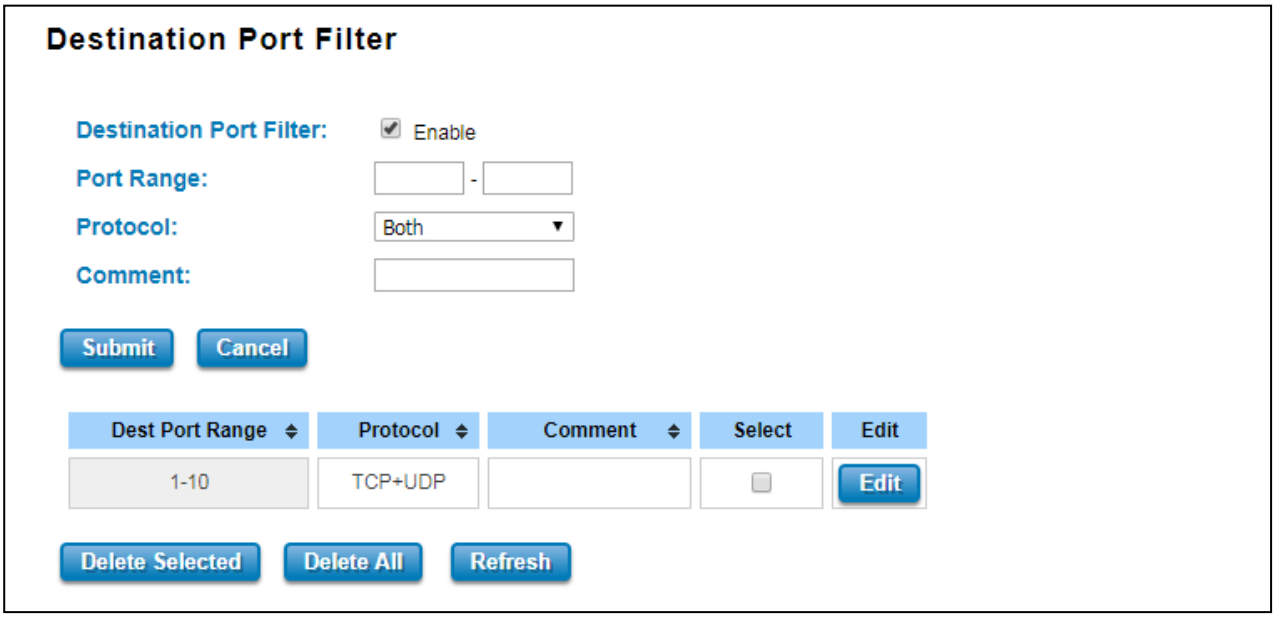
Click **Refresh** to refresh the table

Dest Port Filter

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

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

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



The description of the columns is as below:

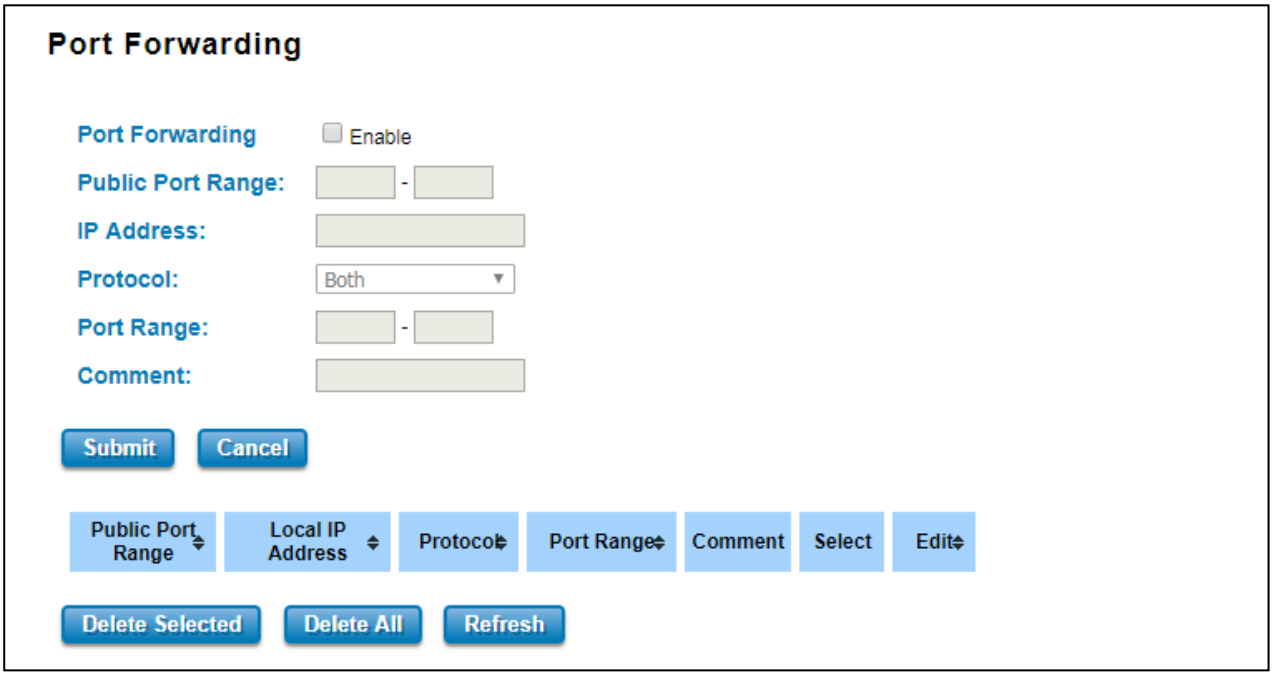
TERMS	DESCRIPTION
Dest Port Range	Display the Destination Port Range (Range is from 1 to 65535)
Protocol	Display the protocol that has been chosen by the user.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete the list.
Edit	Click edit to modify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

Click **Refresh** to refresh the table

3.11.4 NAT SETTING

Network Address Translation is the process where a network device, usually a firewall, assigns a public address to a device or group of devices inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economic and security purposes. The simple type of NAT provides one to one translation of IP address. It can be used to interconnect two IP networks, normally one network is for Local Area Network and the other network is for Wide Area Network/Internet. To configure the NAT Setting, the **Port Forwarding, DMZ** and **NAT Setting** configuration pages are provided in this section.

Port Forwarding



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

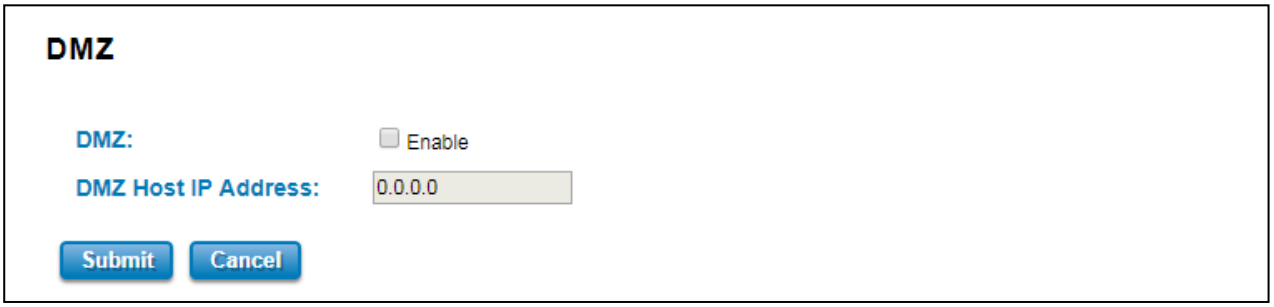
The description of the columns is as below:

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

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

DMZ

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



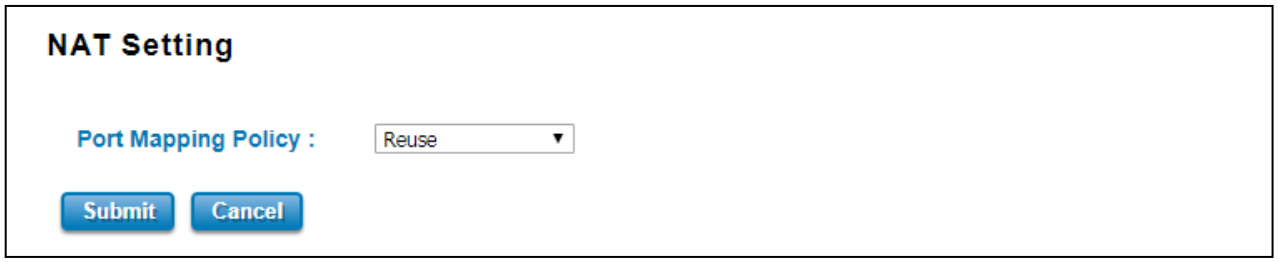
Click **Enable** to activate the function and assign the IP address of **DMZ Host IP Address**. This is the DMZ computer's IP address. Click Submit to activate the function.

The description of the columns is as below:

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

NAT Setting

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



The description of the columns is as below:

TERMS	DESCRIPTION
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.

3.11.5 OPEN VPN

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

OpenVPN Status

This section shows the VPN Client and Server current status.



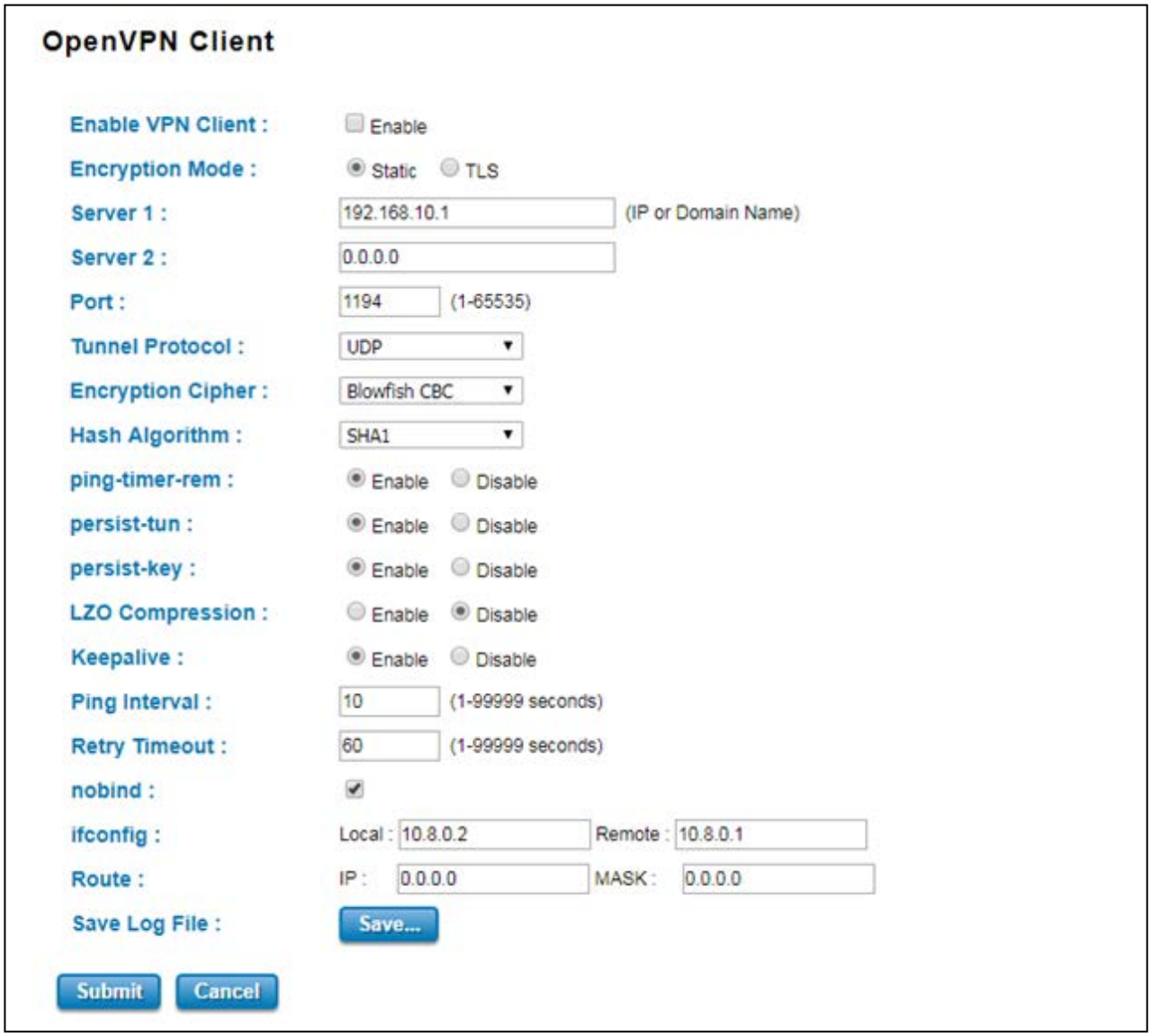
The description of the columns is as below:

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

Click **Refresh** to update the information.

OpenVPN Client

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



The description of the columns is as below:

TERMS	DESCRIPTION
Enable VPN Client	Select Enable to activate the VPN Client function
Encryption Mode	Choose the Encryption Mode Static Key: Use a pre-shared static key. TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server 1	Type the IP Address of the VPN Server
Server 2	Type the second IP Address of the VPN Server if needed.
Port	**Default: 1194**

	Input the port number that VPN service used. Please check the VPN Server port setting. The range from 1-65535.
Tunnel Protocol	Choose use TCP or UDP to establish the VPN connection.
Encryption Cipher	Select the encryption cipher from Blowfish to AES in Pull-down menus.
Hash Algorithm	Hash algorithm provides a method of quick access to data, including SHA1，SHA256，SHA512，MD5
ping-timer-rem	**Default: Enable** Select enable or disable the ping-timer-rem, to 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 the VPN restarts after Keepalive timeout.
LZO Compression	**Default: Disable** Select use LZO Compression or not, this function compresses data to decrease the traffic but also need more CPU effort.
Keepalive	**Default: Enable** Select enable or disable Keepalive function, this function is use to detect the status of connection.
Ping Interval	**Default: 10** Input the ping interval, the range can from 1~99999 seconds.
Retry Timeout	**Default: 60** Input the retry timeout, the range can from 1~99999 seconds.
nobind	Check the box to activate nobind function. With nobind function, the source ports are random.
ifconfig	Input the tunnel IP addresses that VPN use.
Route	Input the route IP and MASK. This is the target IP domain that user can access through the VPN tunnel.
Save Log File	Click Save to keep the VPN Client Log.

Click **Submit** to apply the configuration.

OpenVPN Server

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



The description of the columns is as below:

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

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

Click **Submit** to apply the configuration.

OpenVPN Certificate

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

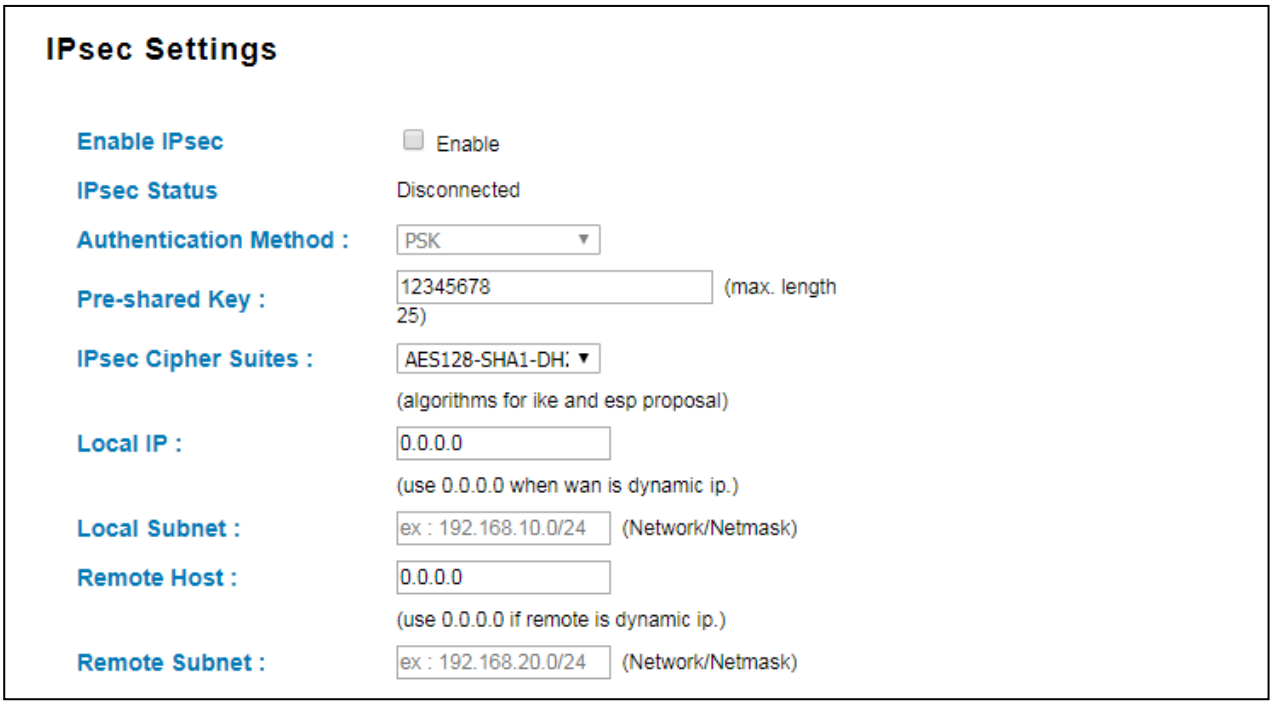


The description of the columns is as below:

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

3.11.6 IPSEC SETTING

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

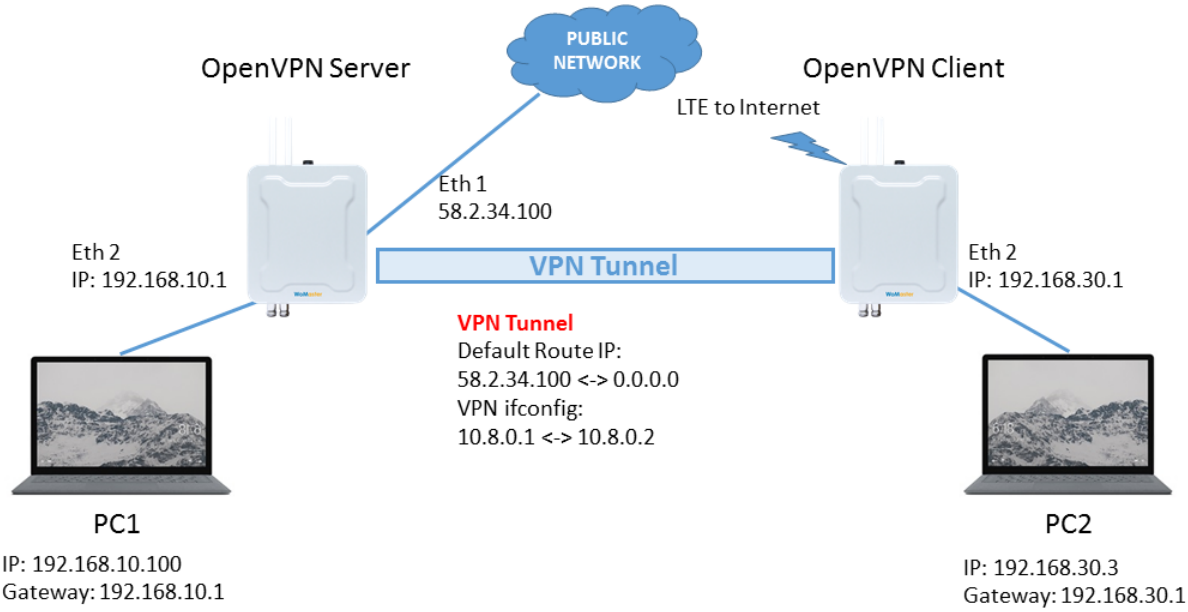


The description of the columns is as below:

TERMS	DESCRIPTION
Enable IPsec	Select Enable to activate the IPsec function
IPsec Status	Display the IPsec status, whether it is connected or disconnected
Authentication Method	Default: PSK Optional: Pre Shared Key or Certificate

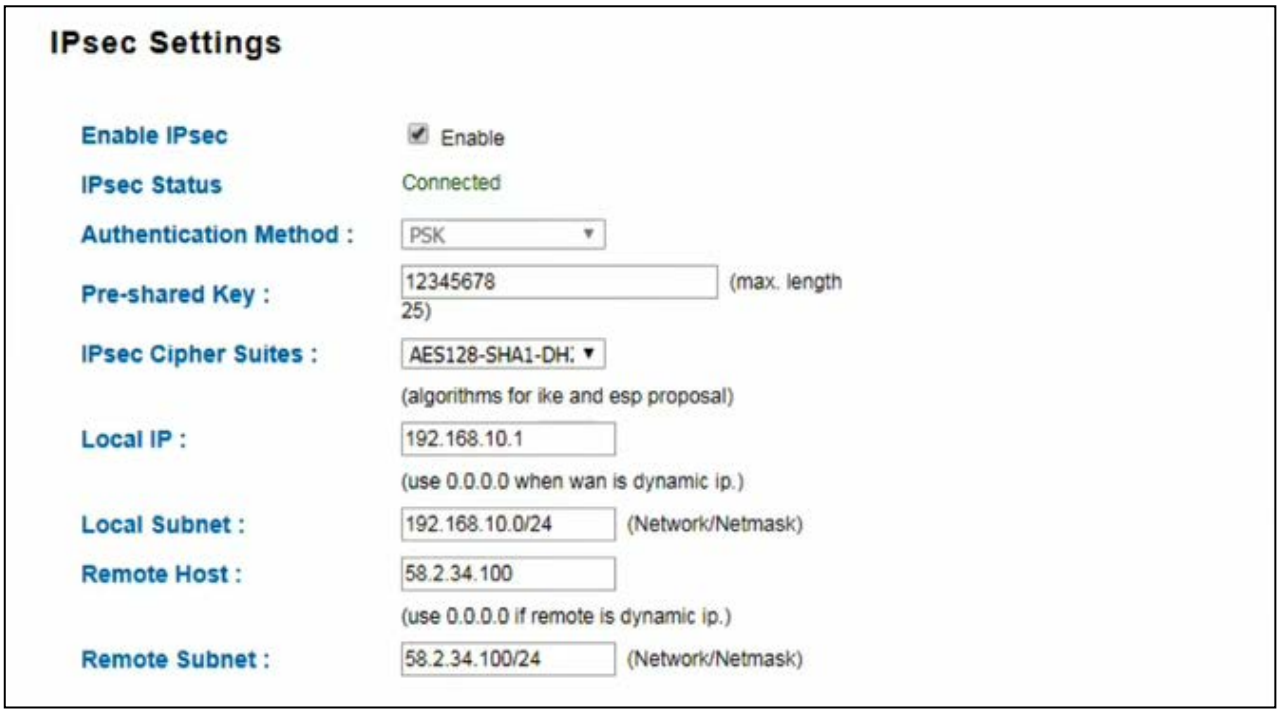
Pre-shared key	**Default: 12345678** Set the preshared key
IPsec Cipher Suites	**Default: AES128-SHA1-DH2** Set algorithms for IKE and ESP proposal, choose AES128-SHA1-DH2, DES-SHA1-DH2, and 3DES-SHA1-DH2
Local IP	IP Address of the local side of the tunnel. (Use 0.0.0.0 when WAN is dynamic IP.)
Local Subnet	Set IPSec local protected subnet and subnet mask, i.e. 192.168.1.0/24
Remote Host	**Default: 0.0.0.0** Set IPsec Remote Host, use the default setting if remote is dynamic IP
Remote Subnet	Set IPsec Remote Protected Subnet/Subnet Netmask

Click **Submit** to apply the configuration.



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

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



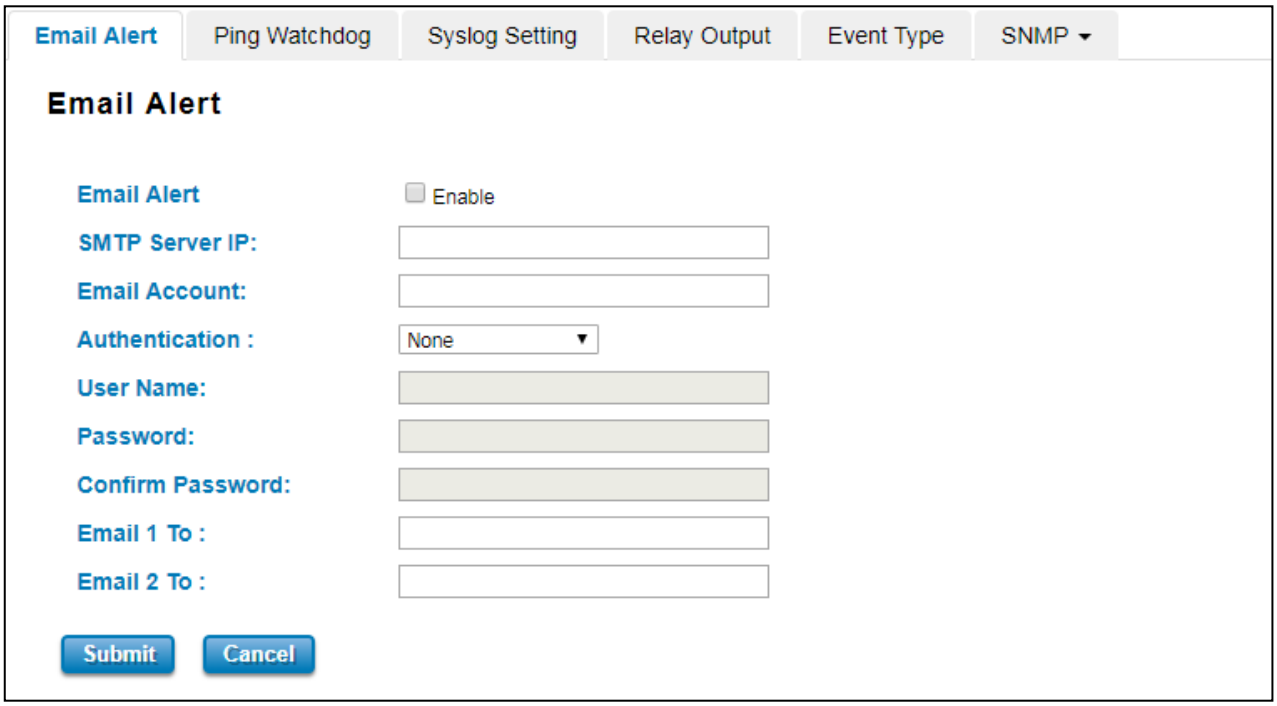
When the connection is enabled, then the IPsec status will directly change to connected status, which means that the connection is established. So that the laptop at the branch office can access the server at headquarter.

3.12 WARNING

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

3.12.1 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.

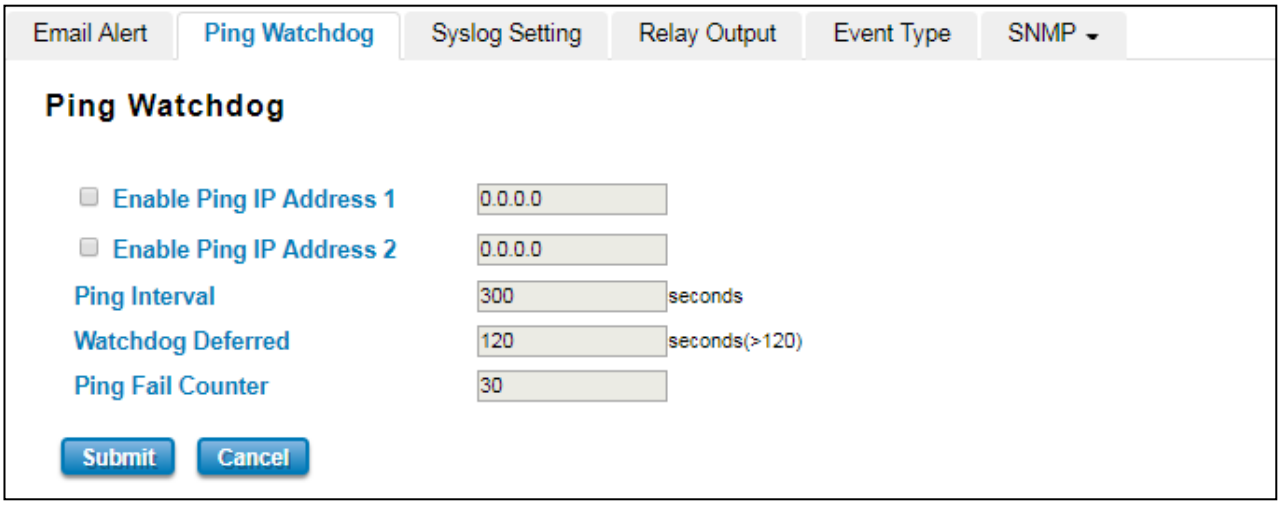


The description of the columns is as below:

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.

3.12.2 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.

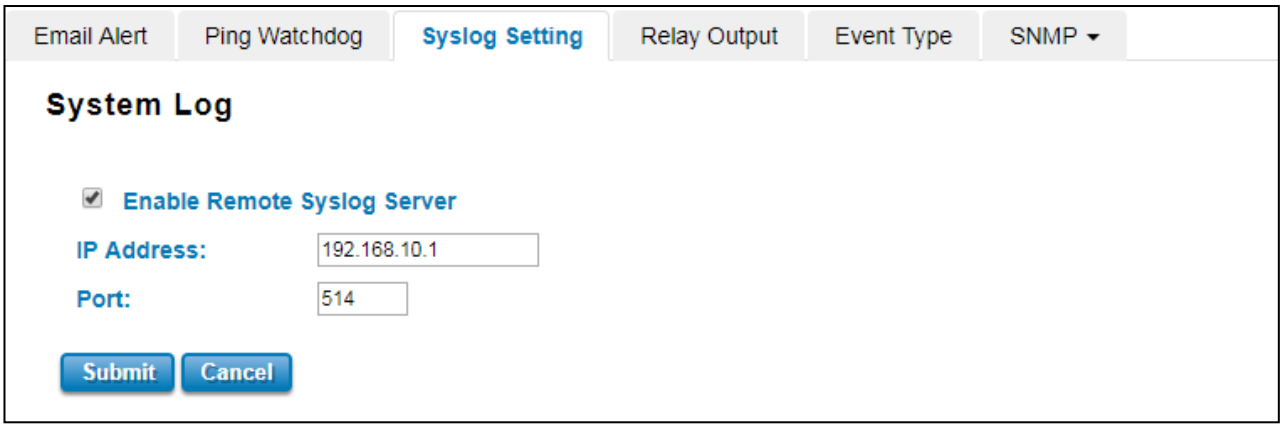
The description of the columns is as below:

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 is expired or reach the failure count, the device will reboot.

Click **Submit** to apply the configuration.

3.12.3 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

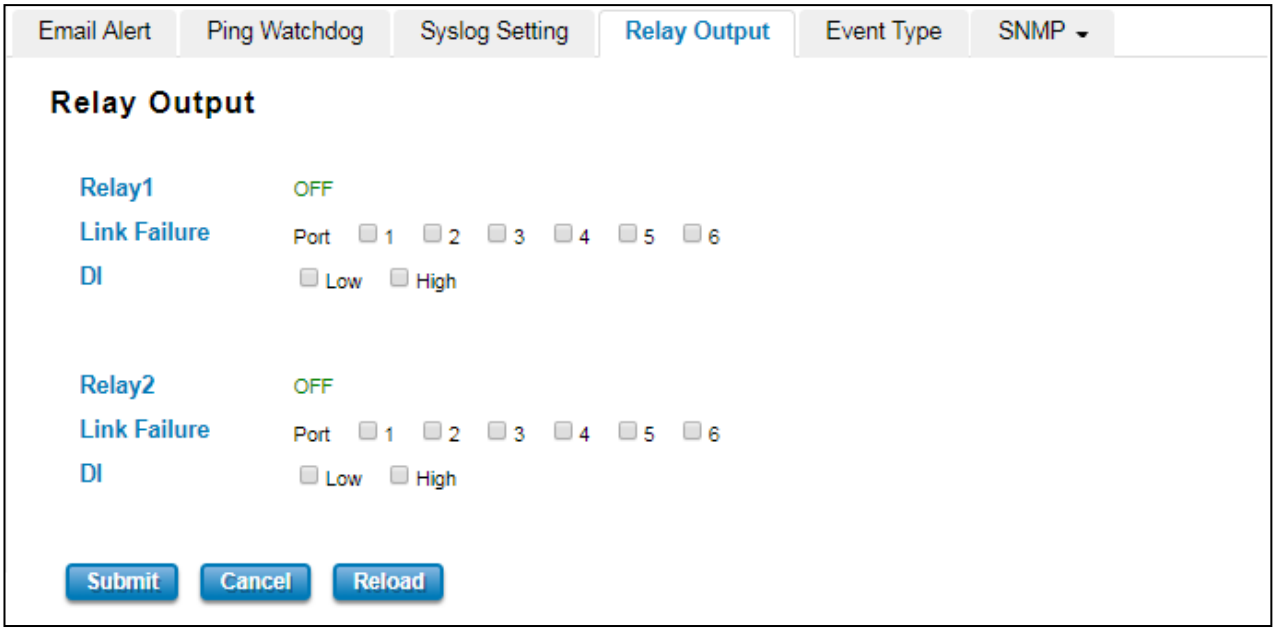
The condition or term described as following table.

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.

3.12.4 RELAY OUTPUT

WoMaster' router provides 1 alarm relay output, also known as Digital Output. These settings in Relay Output section control the events that will trigger the alarm output. The Relay Output configuration interface has shown as below:



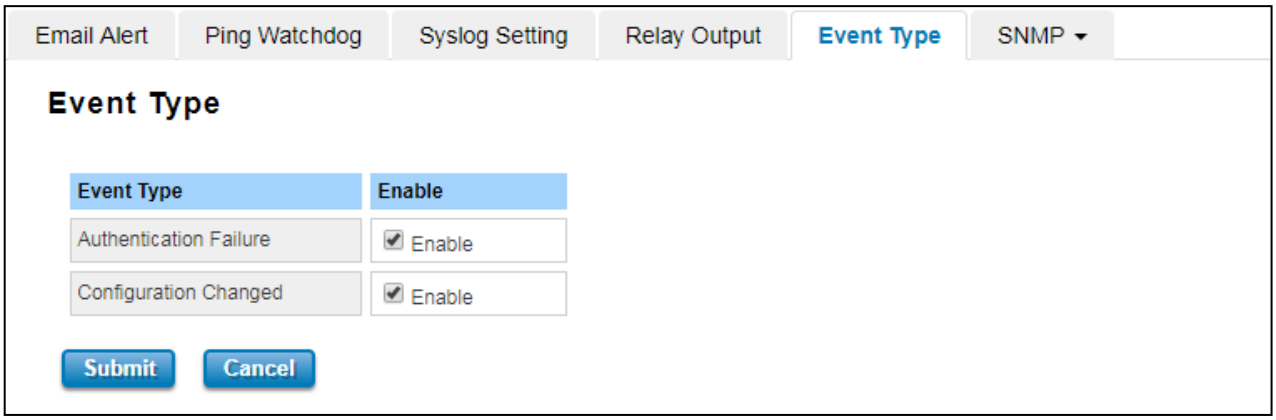
The condition or term described as following table.

TERMS	CONDITION	DESCRIPTION
Relay 1/2	ON or OFF	The status change to ON if any kind of failure is detected. OFF if the status is normal.
Link Failure	LAN Port number 1 to 6	Monitoring port link down event
DI	Low or High	Relay trigger when DI states change to Hi or Low

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

3.12.5 EVENT TYPE

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

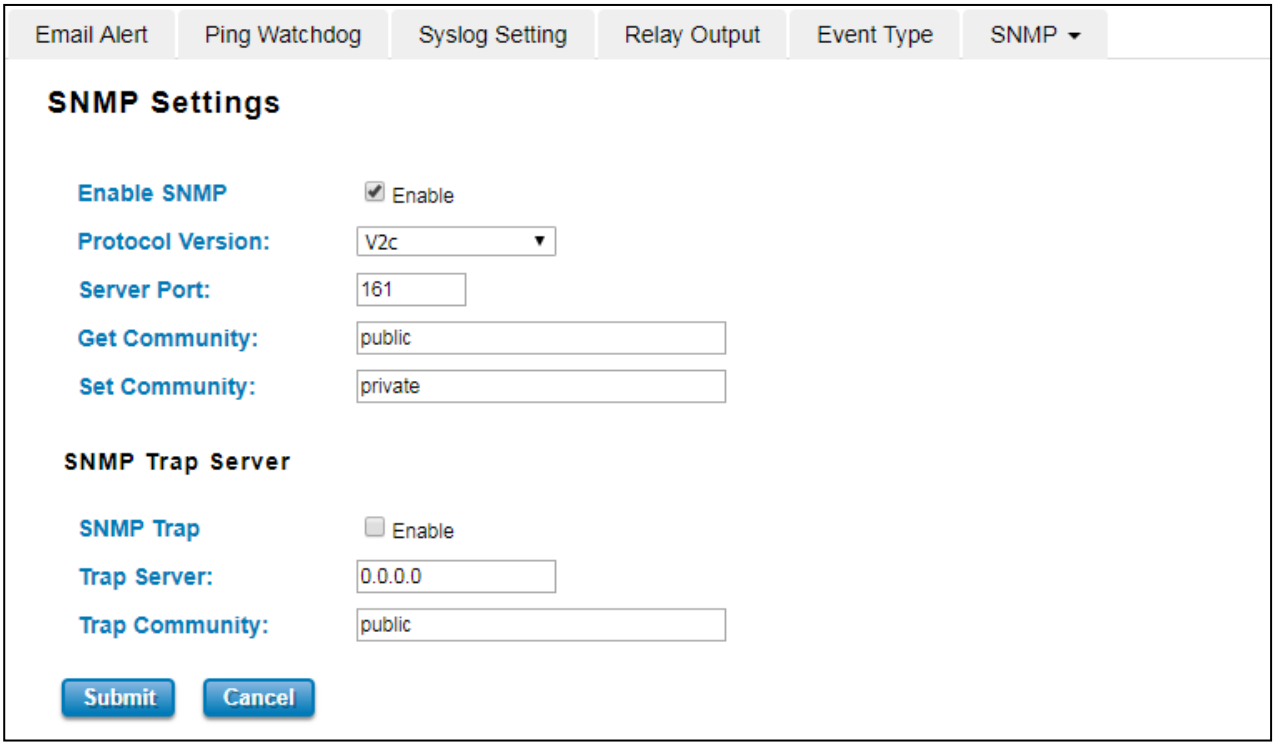


TERMS	DESCRIPTION
Authentication Failure	When the authentication fails, the system will issue the event log/email alert to the system log/SMTP server respectively.
Configuration Changed	When there are any kinds of changing in the configuration, the system will issue the event log/email alert to the system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

Click **Submit** to apply the configuration.

3.12.6 SNMP

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



SNMP Setting

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

SNMPv2C

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

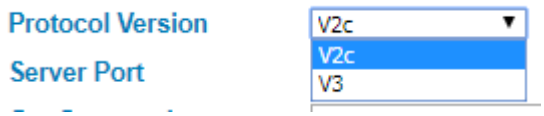
SNMP V3

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

SNMPv3 security comes primarily in 2 forms:

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

The description of the columns is as below:

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

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

SNMP Trap Server

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

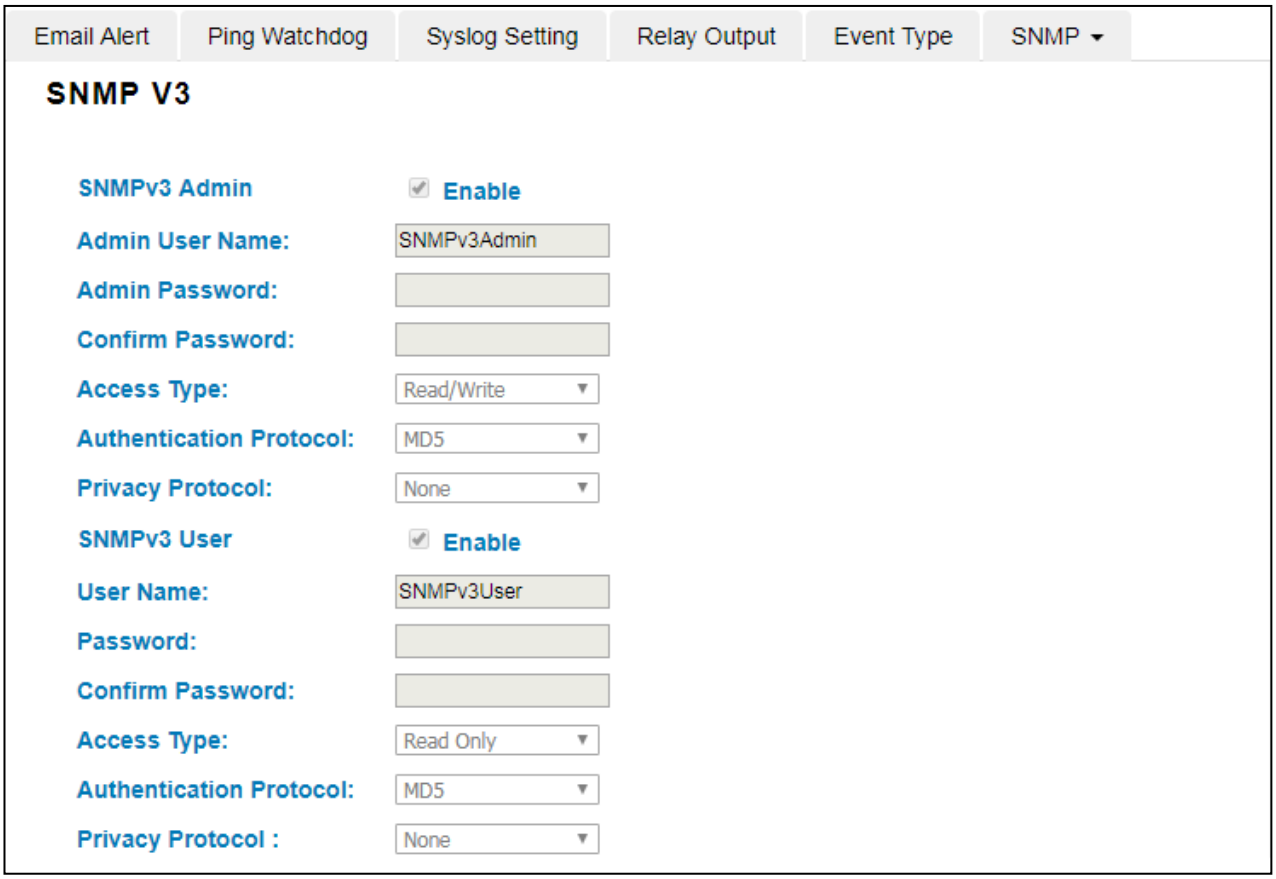
The description of the columns is as below:

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

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

SNMP V3

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



TERMS	DESCRIPTION
SNMPv3 Admin	Clicks enable to activate the function and the entries for SNMPv3 Admin.
Admin User Name	**Default: SNMPv3Admin** Set up the User Name for the SNMPv3 Admin
Admin Password	Set up the Password for the SNMPv3 Admin
Confirm Password	Confirm the Admin for the SNMPv3 Admin
Access Type	Access type for the SNMPv3 Admin, choose Read Only or Read and Write
Authentication Protocol	**Default: MD5** Provides authentication based on MD5 or SHA algorithms.
Privacy Protocol	Specify the encryption method for SNMP communication. None and DES are available.

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

3.13 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:

3.13.1 Event Logs

3.13.2 ARP Table

3.13.3 Port Statistics

3.13.4 LLDP

3.13.5 Ping

3.13.6 Battery Charge Status

3.13.7 Client Association List

3.13.1 EVENT LOGS

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

Event Logs

#	Time	Source	Message
1	2018-07-11 11:36:00	syslogd	syslogd started.
2	2018-07-11 11:36:00	syslog	br0 hw ether 9466e79f0002
3	2018-07-11 11:36:03	cellular	Init cellular subsystem.
4	2018-07-11 11:36:03	cellular	module [EC25] detected.
5	2018-07-11 11:36:03	system	TZ: GMT0
6	2018-07-11 11:36:08	syslogd	System log stop.
7	2018-07-11 11:36:08	syslogd	syslogd started.
8	2018-07-11 11:36:15	syslog	eth0 ip is 192.168.1.1
9	2018-07-11 11:36:19	wifi	Wireless 1 VAP[1]:service started.
10	2018-07-11 11:36:30	syslog	br0 ip is 192.168.10.1
11	2018-07-11 11:36:30	syslog	dns1 is 8.8.8.8
12	2018-07-11 11:36:31	system	TZ: GMT0
13	2018-07-11 11:36:31	cellular	Repower Cellular Module

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**.

3.13.2 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.

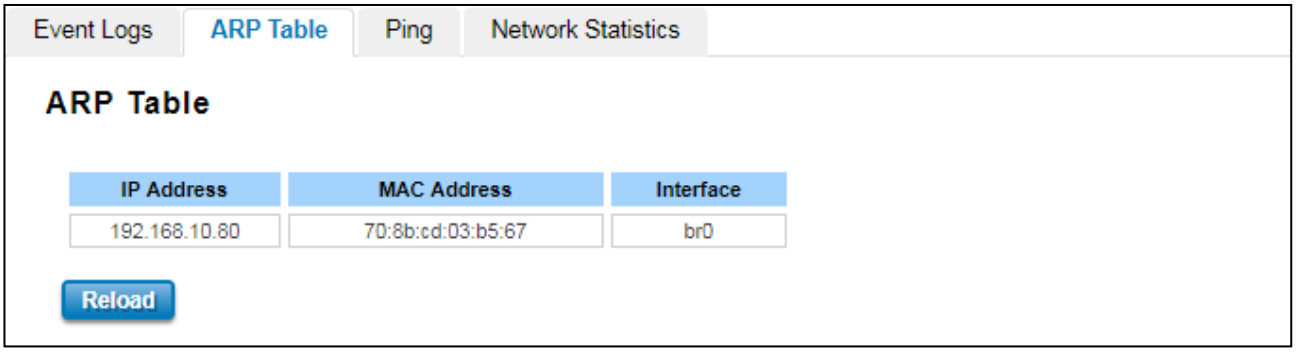
Data Format

Protocol Header:

802.3 + 802.2 LLC + 802.2 snap

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

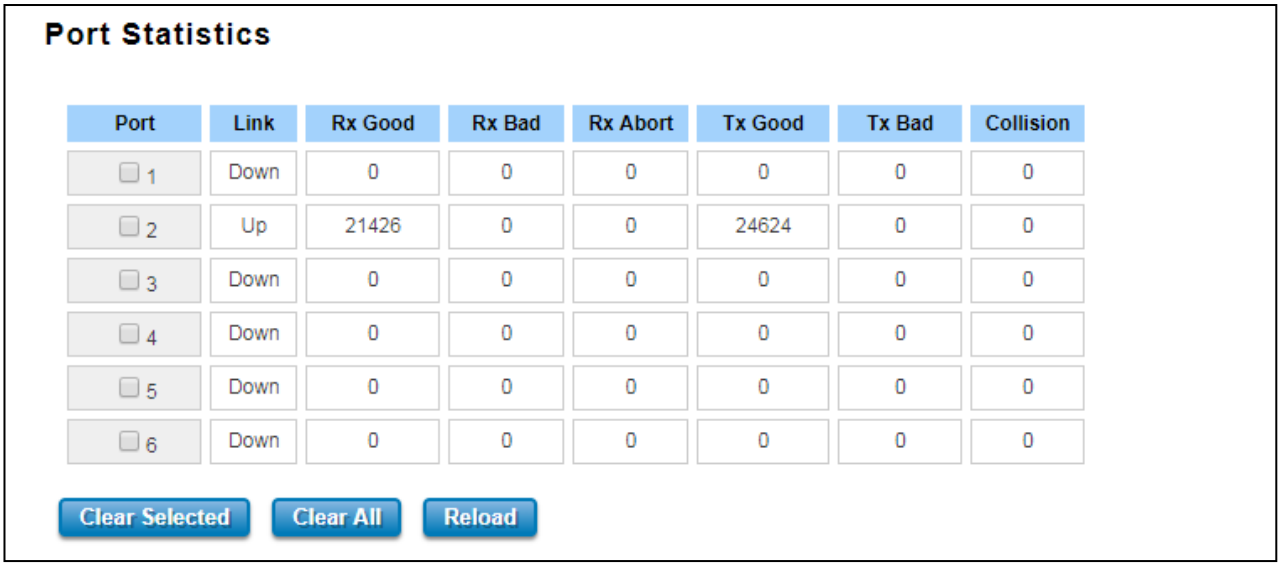
This page shows the routers active ARP table. An ARP table contains recently cached MAC addresses of every immediate device that was communicating with the router.



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

3.13.3 PORT STATISTICS

This page displays the number of packets that were received and sent from the port. The number of error packets can mean a duplex mismatch, incompatibilities with the port and its attached device, or faulty cables or attached devices. Any of these problems can cause slow network performance, data loss, or lack of connectivity. The statistics that can be viewed include Port, Link, Rx Good, Rx Bad, Rx Abort, Tx Good, Tx Bad and Collision.

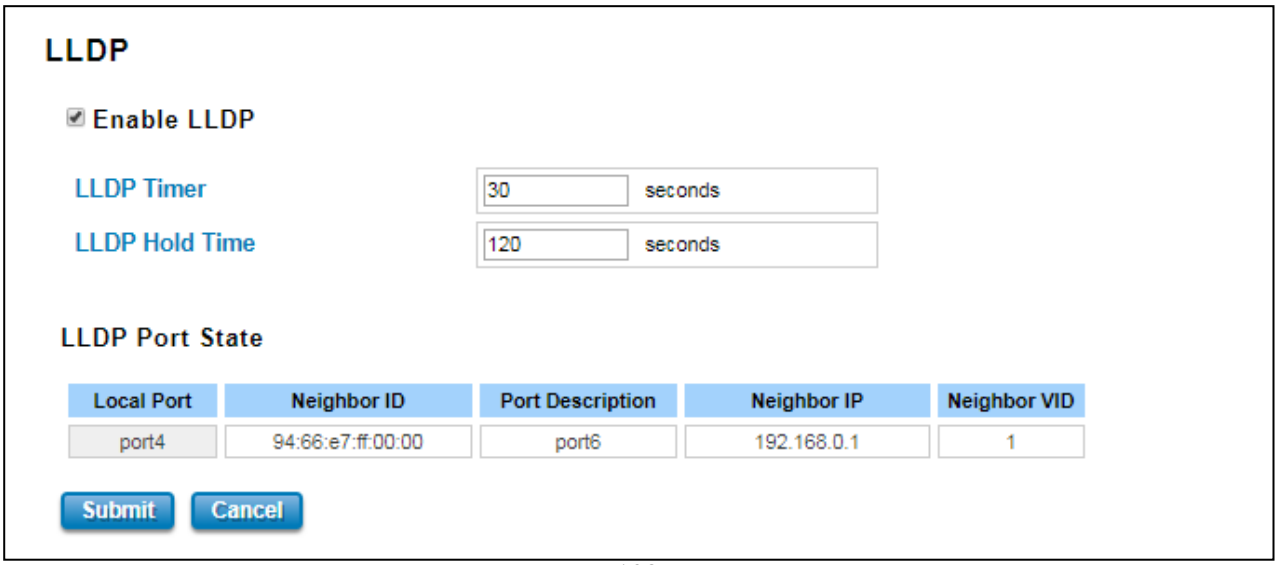


Click on **Clear Selected** to reinitialize the counts of the selected ports, and **Clear All** to reinitialize the counts of all ports. Click on **Reload** to refresh the counts.

3.13.4 LLDP

LLDP is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device, such as a WoMaster managed switch, to periodically send its system and configuration information to its neighbors. Because of this, all LLDP devices are kept informed of each other's status and configuration, and with SNMP. From the switch's web interface, User can enable or disable LLDP, and User can view each switch's neighbor-list, which is reported by its network neighbors. Most importantly, enabling the LLDP function allows to automatically display the neighbor ID and IP learnt from the connected devices.

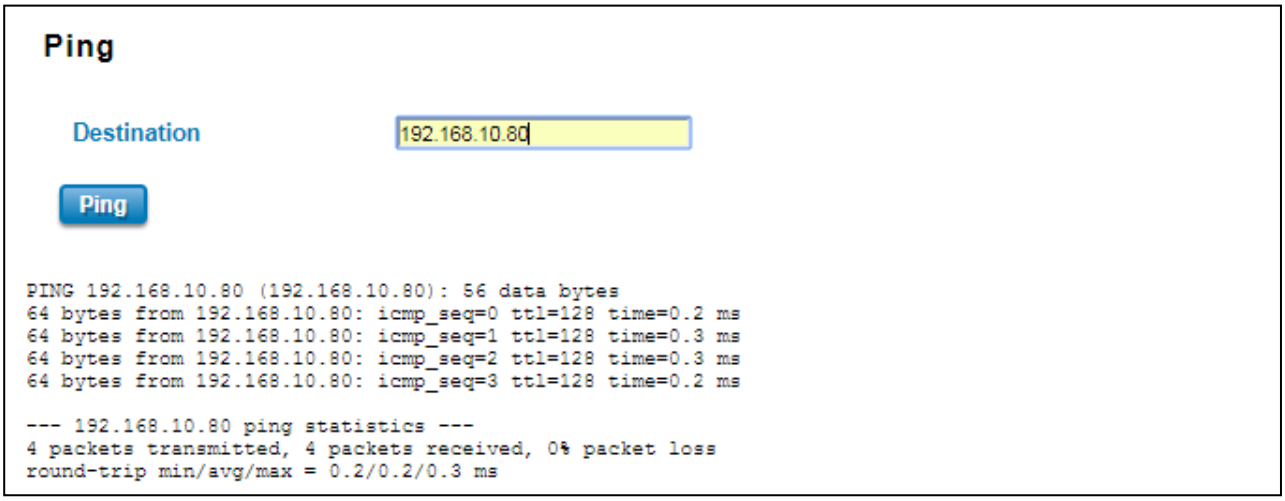
The configuration and settings explain as follows.



TERMS	DESCRIPTION
Enable LLDP	Check the box to enable/disable LLDP function.
LLDP Timer	**Default: 30 seconds** The interval time of each LLDP and counts in second; the valid number is from 5 to 254.
LLDP Hold time	**Default: 120 seconds** The TTL (Time To Live) timer. The LLDP state will be expired once the LLDP is not received by the hold time; the valid number is from 10 to 255.
Local port	The current port number that linked with neighbor network device.
Neighbor ID	The MAC address of neighbor device on the same network segment.
Port Description	The port number of neighbor device on the same network segment.
Neighbor IP	The IP address of neighbor device on the same network segment.
Neighbor VID	The VLAN ID of neighbor device on the same network segment.

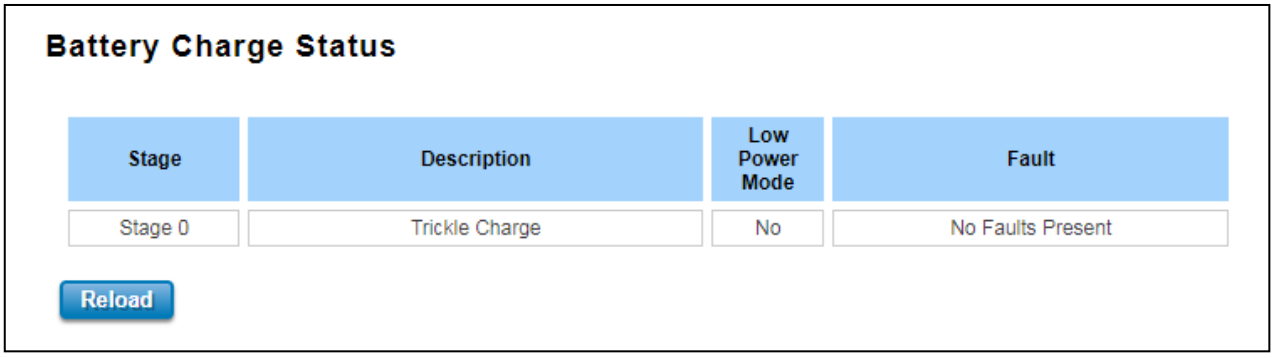
3.13.5 PING

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.



3.13.6 BATTERY CHARGE STATUS

The SCB is supported with the internal battery charger. The table below will show the user the charging status.



The battery is equipped with a switch button; you can refer to the SCB appearance to check the position. The function is to enable the battery as the backup power (Typ. 48V/2.5AH (max. 54.6V) Internal Battery). The battery will be charged automatically when user use the power input cable.



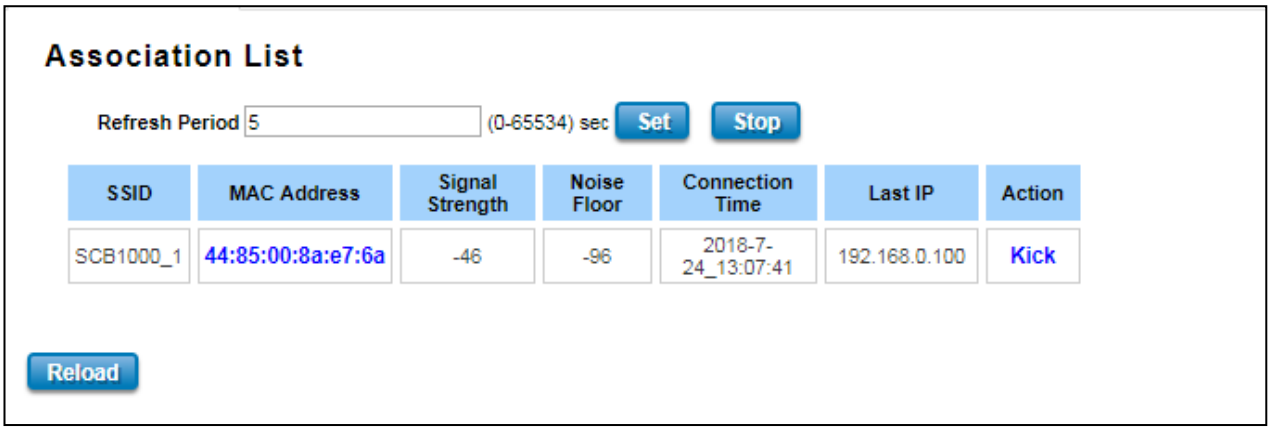
Below is the Battery Charge Status description:

TERMS	DESCRIPTION
Stage	Display the charging status stage. **S0: Trickle Change** **S1: Constant Current** **S2-1: Constant Voltage** **S2-2: Constant Voltage** **Done Charging: Done Charging**
Description	Display the stage's description.
Low Power Mode	Display the Low Power Mode is enabled or disabled. Yes means the Low Power Mode is enabled. No means the Low Power Mode is disabled.
Fault	Display the fault description. Includes: **No Faults Present** **Battery disconnected (Thermistor Disconnected)** **Invalid Battery Temperature** **Timer Fault** **Battery Under voltage**

Click **Reload** to refresh the list.

3.13.7 ASSOCIATION LIST

This 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:

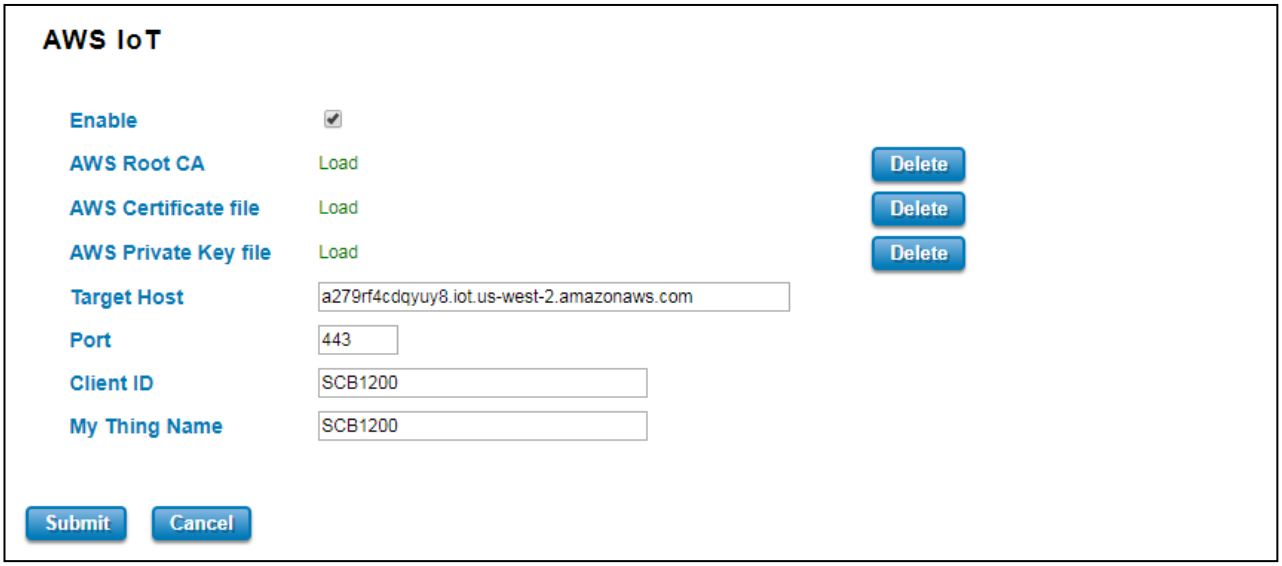
TERMS	DESCRIPTION
Refresh Period	**Default: 5** To set the Poll Interval time setting with range from 0 to 65534. (second)
Set	To set new Interval time. Stop the old Poll Interval first before setting the new interval.
Stop	To stop Polling Interval, this action can be executed when user wants to change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

3.14 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 SCB Series 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.

3.14.1 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/.



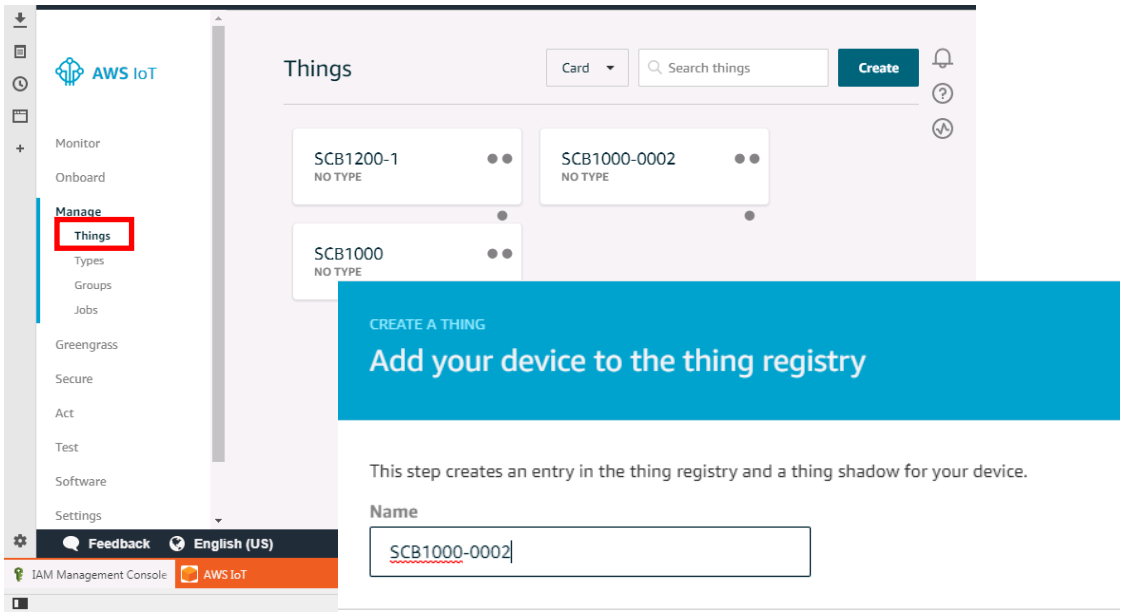
The description of the columns is as below:

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 needs to add an inbound rule on port 443.
Client ID	Enter the client ID.
My Thing Name	Enter the registered device name (Need to be the same).

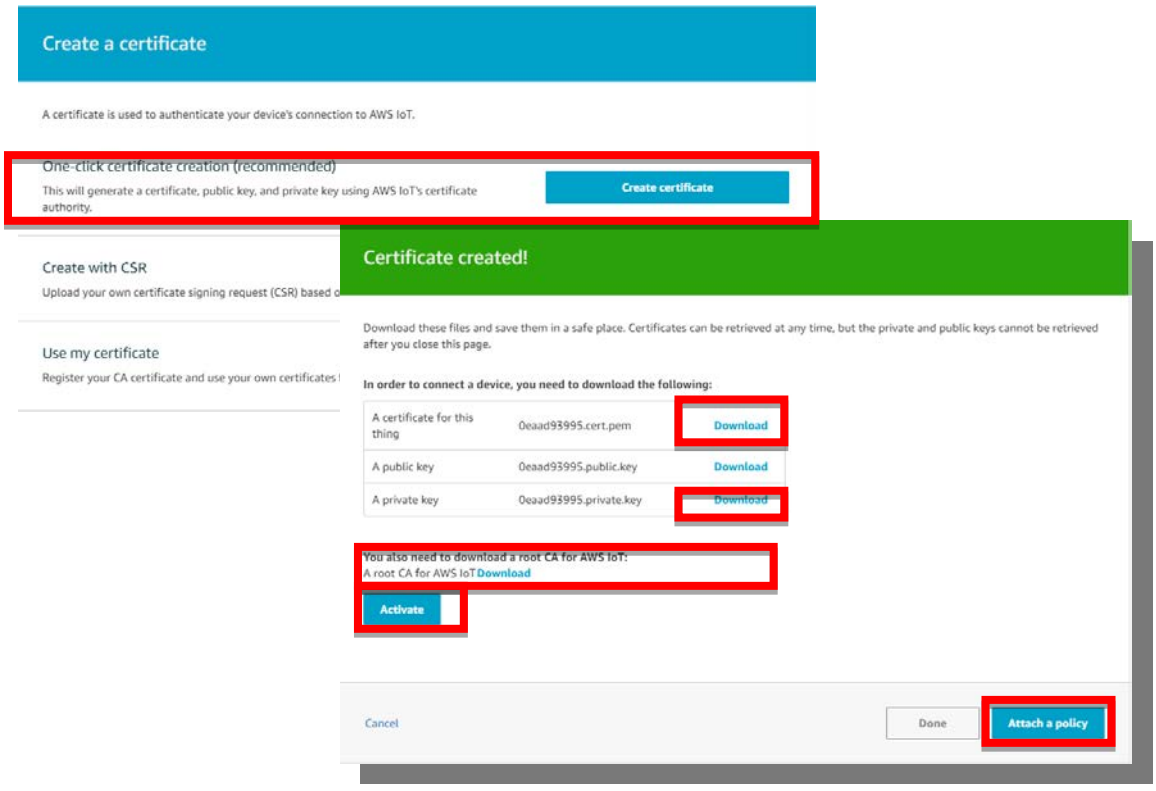
Click **Submit** to apply the configuration.

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.

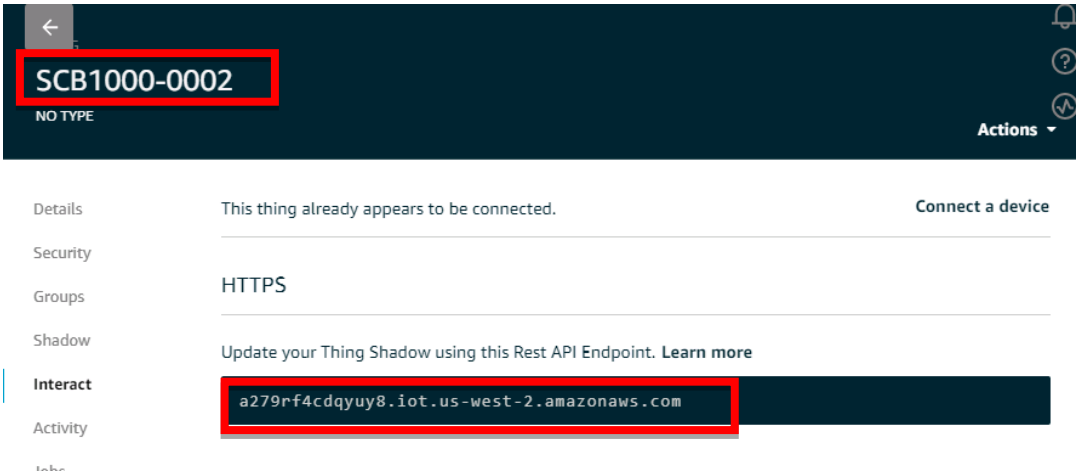


Certificate, private key, root CA is necessary. Public key is used by AWS server to authenticate with private key. The public key and private cannot be downloaded back after the user closes the page. Policy can be added later.

- Get the Target host to connect with the device.

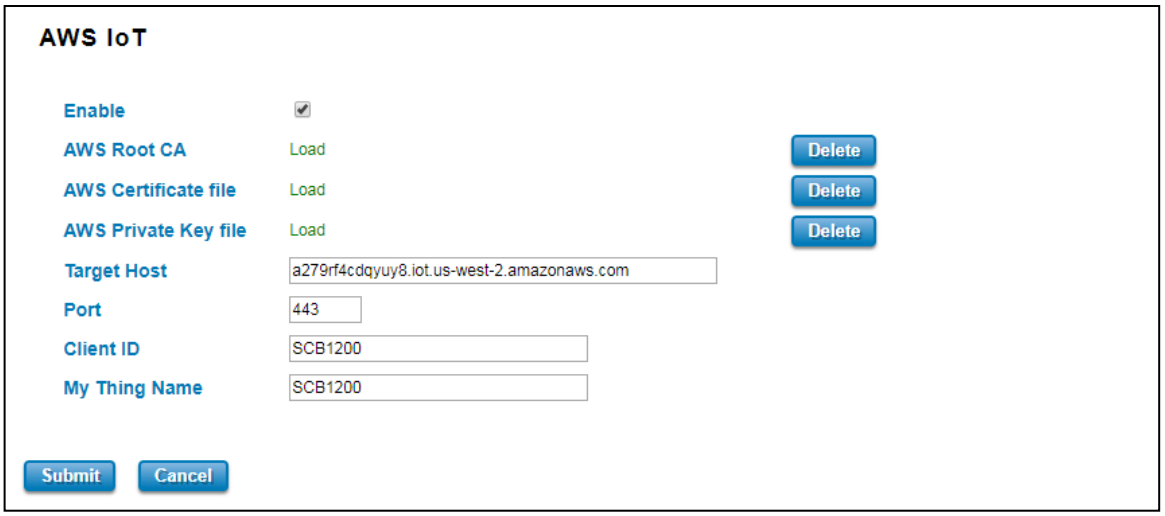
  Go to Manage -> Things -> click the device name -> Click Interact.

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



- Connect the device to AWS.

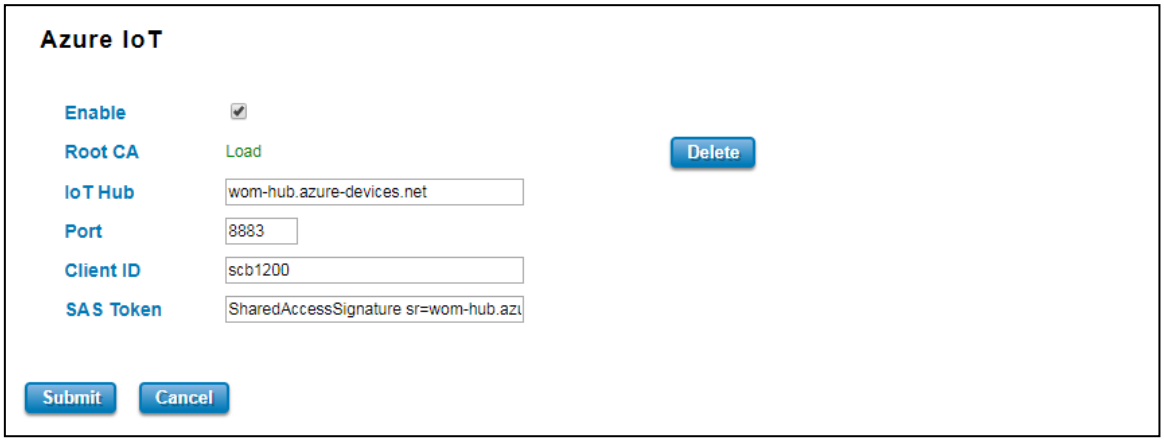
  Copy the link and paste on the Target Host field at the AWS IoT page.



3.14.2 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).

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 (IoT Configuration).

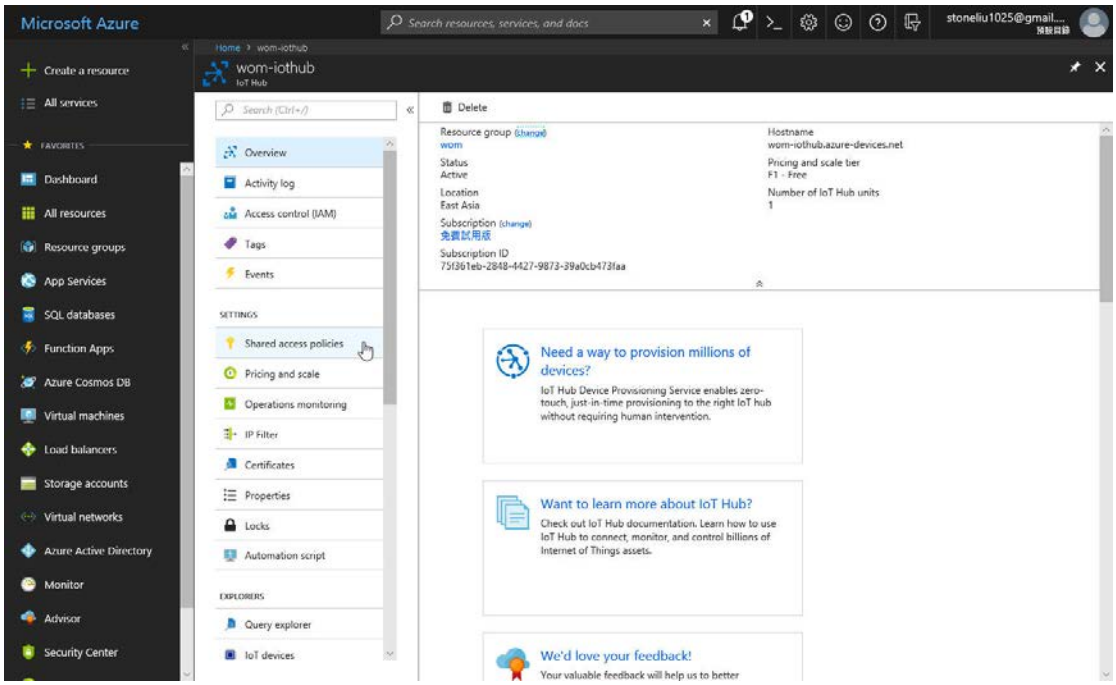
CONFIGURE THE DEVICE AS A MQTT CLIENT

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

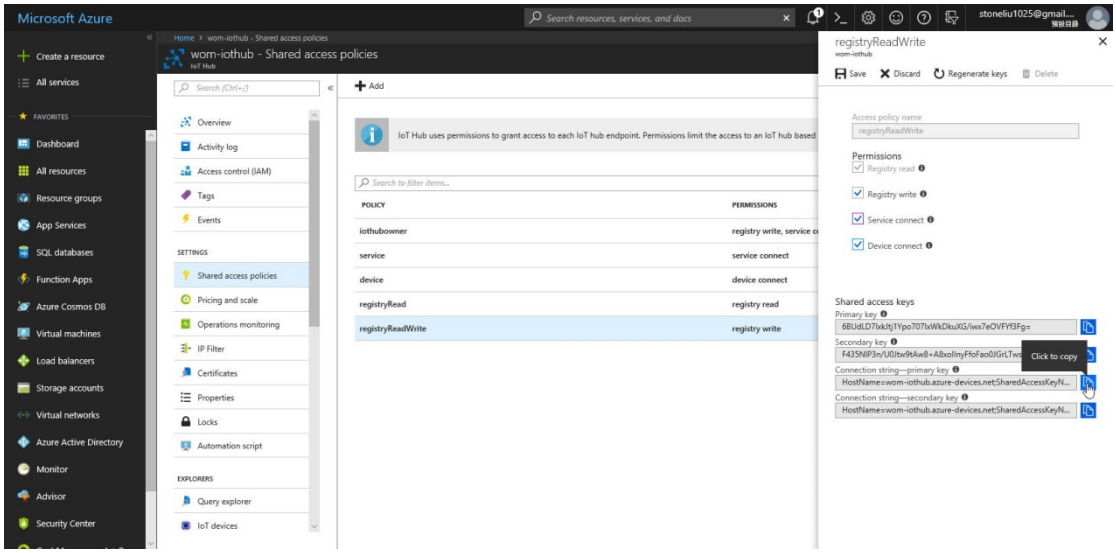
Devices > myCreatedDevice > Shared access policies > iothubowner > Connection string - primary key.

User has to annotate the value of this field.

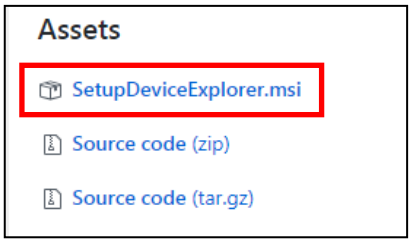
1. Get the connection string. Click the IoT Hub -> Shared access policies.



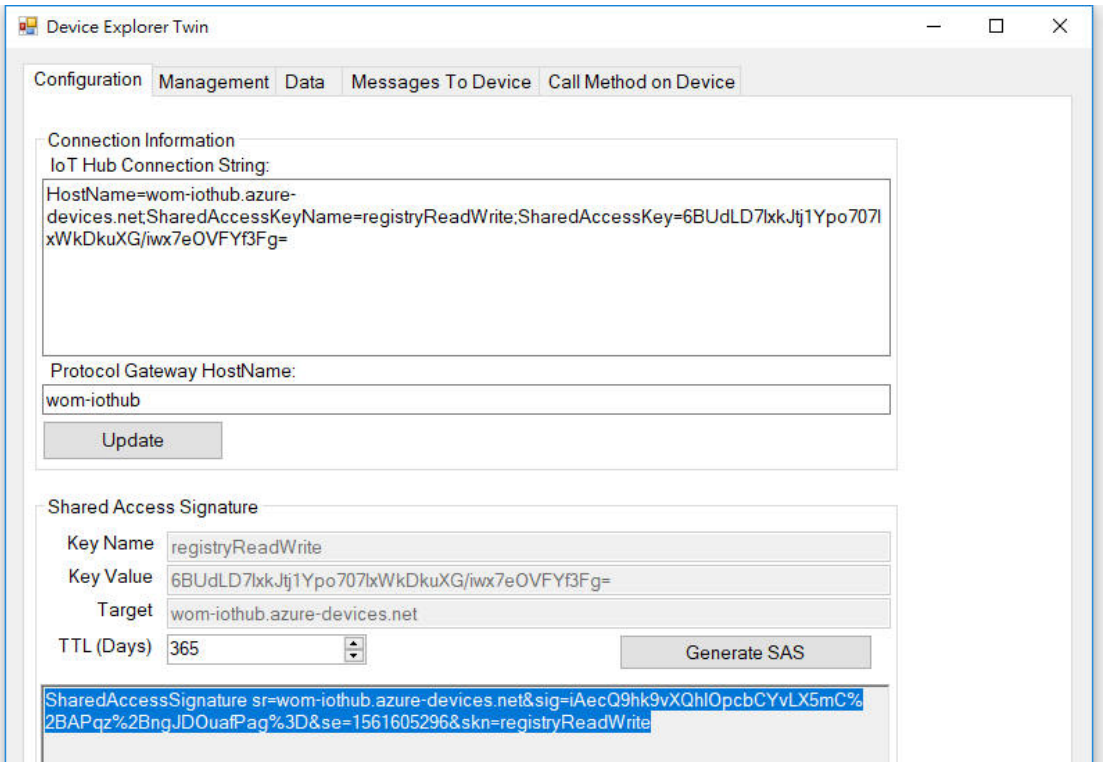
2. Click registryReadWrite -> copy the Connection string---Primary Key.



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.



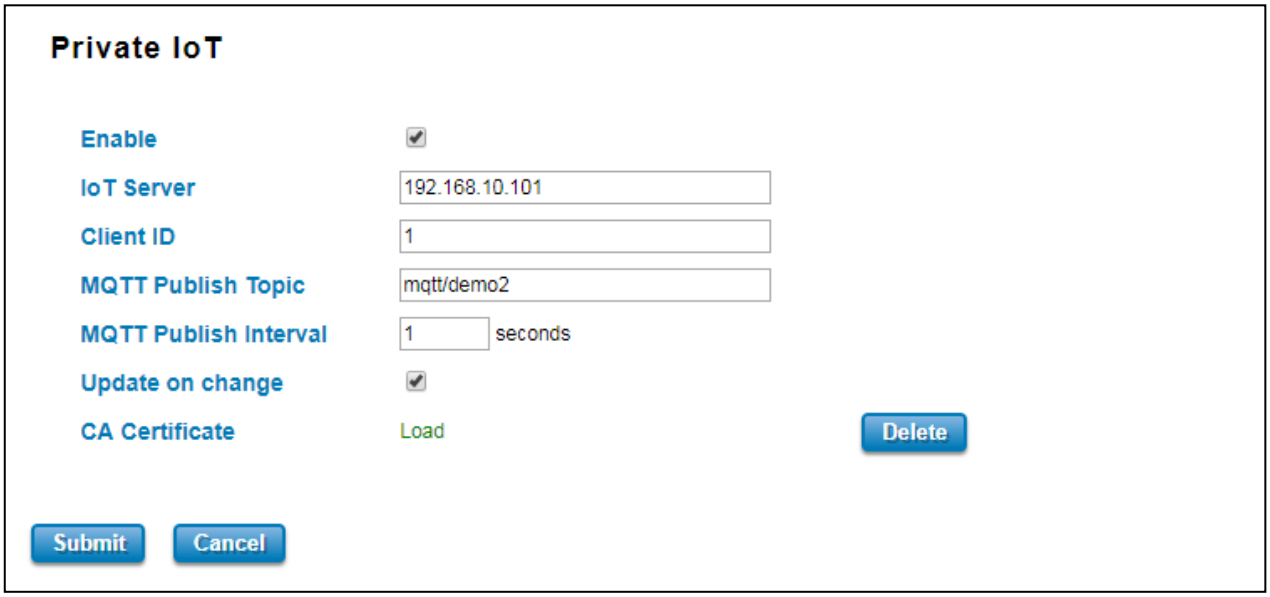
5. Configure the MQTT Client from the Web GUI. Enter the value based on the IoT Hub settings. And the device is connected to the cloud.



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

3.14.3 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 to the cloud anywhere, anytime, and seamlessly share to any authorized users.



The description of the columns is as below:

TERMS	DESCRIPTION
Enable	Enable the Private IoT function
IoT Server	Enter the specific IoT Server.
Client ID	Enter the client ID that has been registered.
MQTT Publish Topic	**Default: mqtt/demo2**

	Specify the MQTT Topic
MQTT Publish Interval	The interval time to update the data
Update on change	**Default: Uncheck** Check the box to keep update the data.
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**

Click Submit to apply the configuration.

HOW TO ESTABLISH AND CONNECT TO THE THINGSMASTER CLOUD SERVER

1. Download and install VMware Workstation Player.

Please click the link below.

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

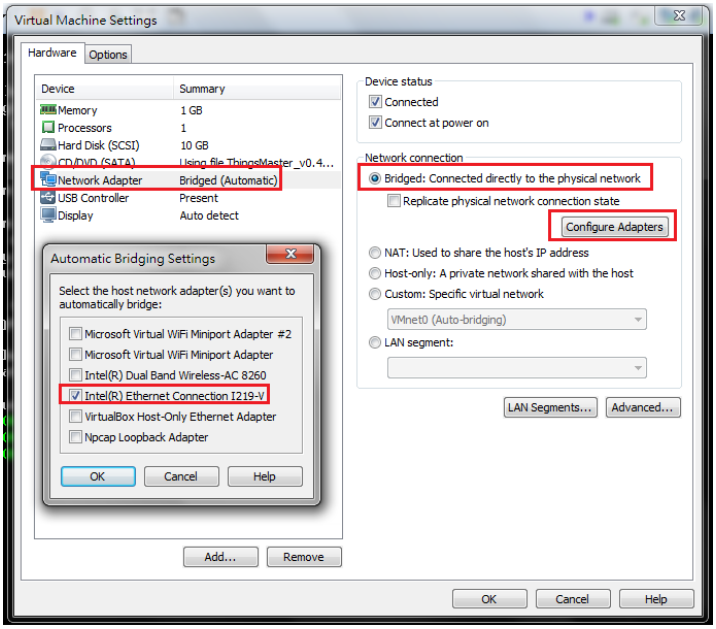
2. Download the server file from the link that sent by the sales.

3. Open a Virtual Machine from disk and import.

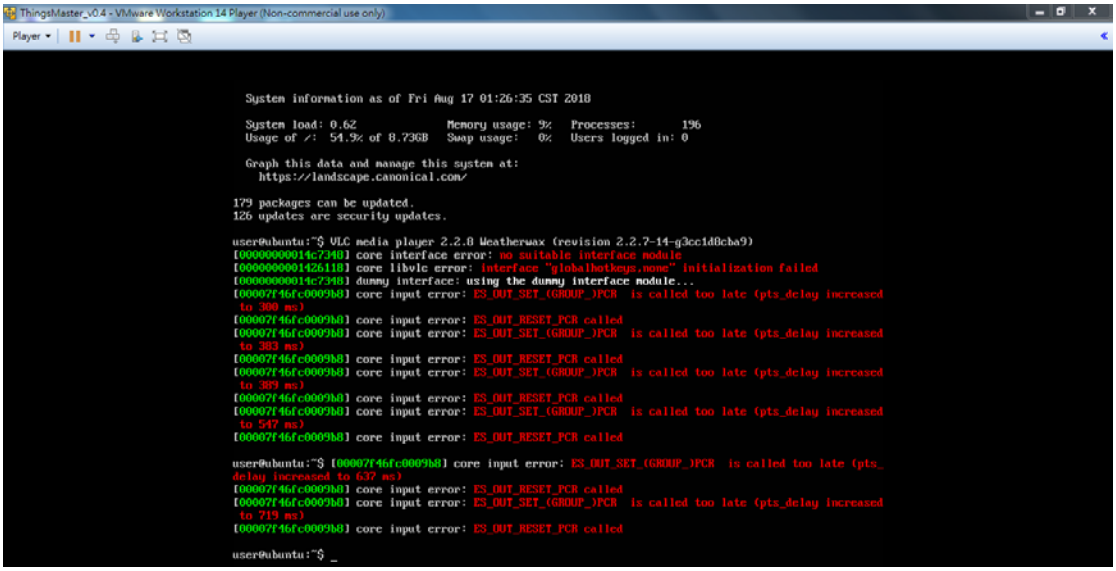
Note: Ignore the warning message, check “Do not show this message again” then click Retry.

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

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



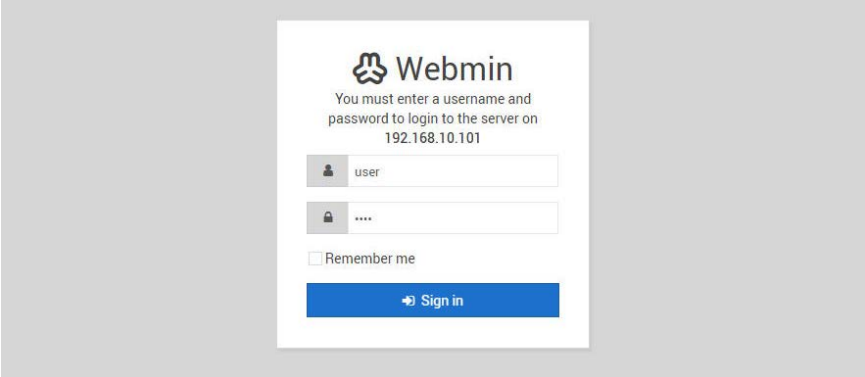
5. Start the Virtual Machine, wait till the starting process is done then the ThingsMaster is established.



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

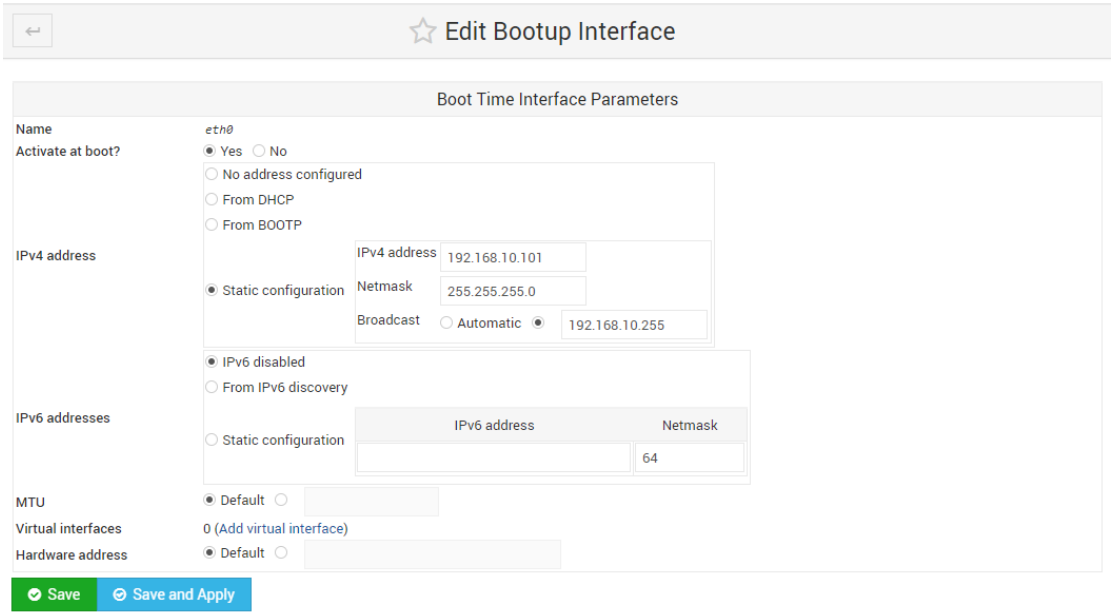
Default: https://192.168.10.101:10000

User Name/Password: user/user



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

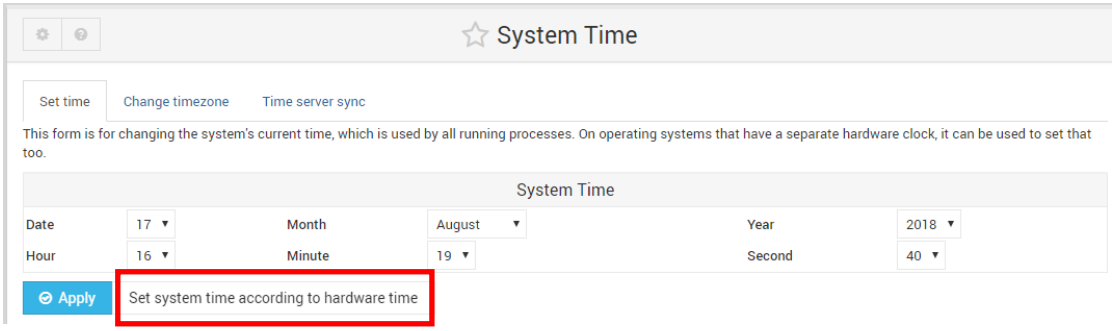
Go to Networking -> Network Configuration -> Network Interface -> Click eth0



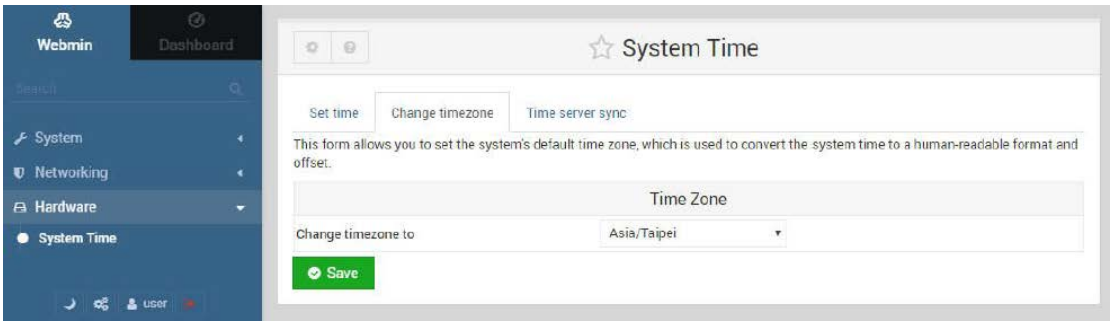
8. Configure Date & Time of the ThingsMaster Virtual Machine.

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

Set the System time according to the hardware.



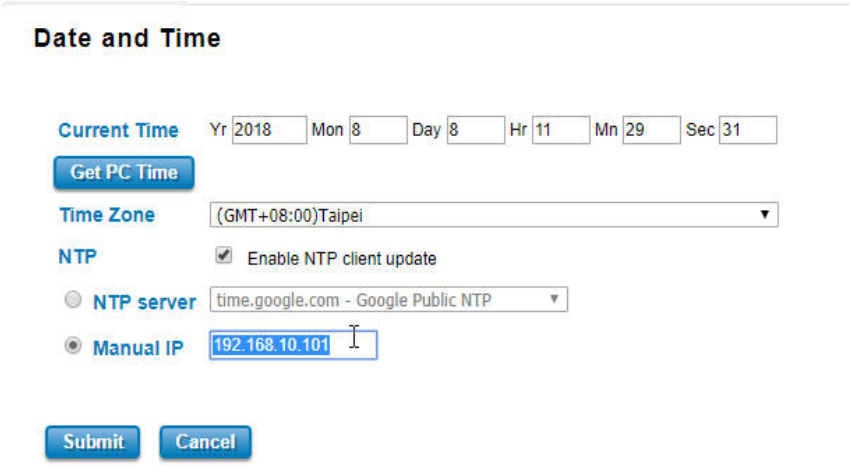
Change the time zone to current user's time zone.



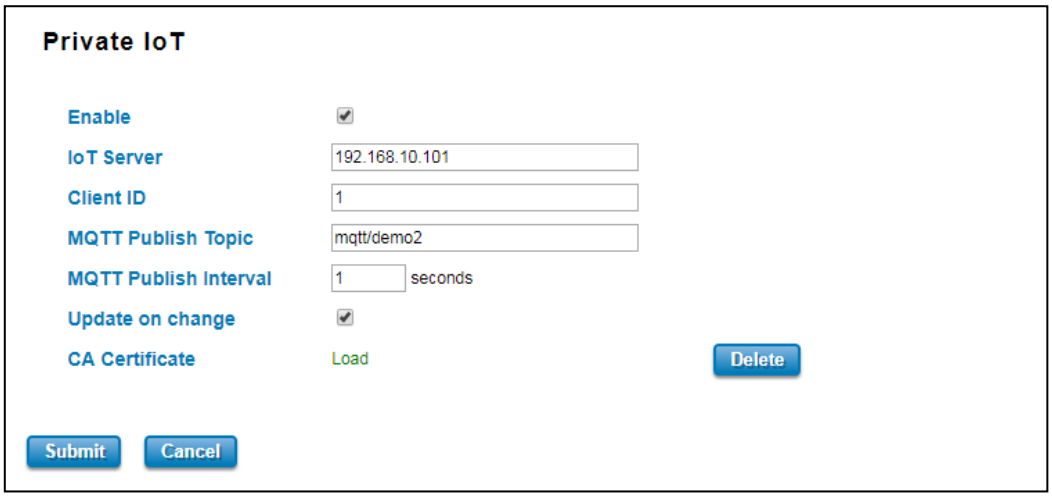
9. Adjust the time setting by using NTP

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

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

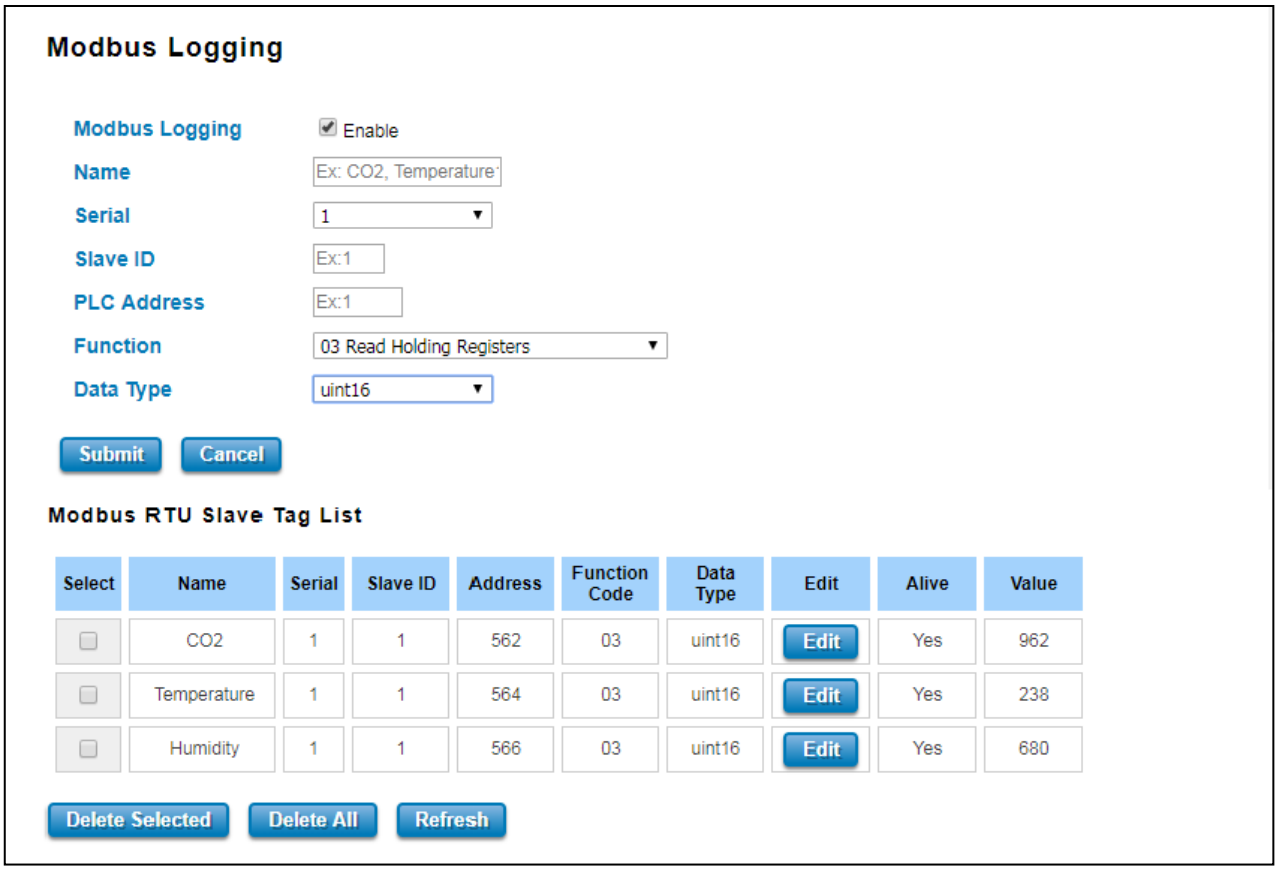


10. Enable Private IoT service and get connected to the ThingsMaster.

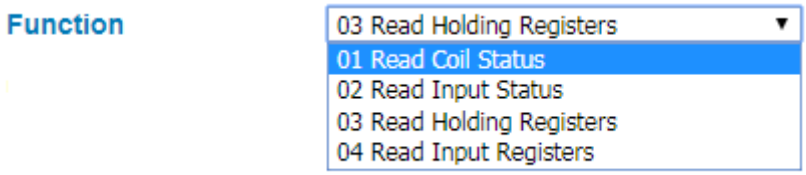


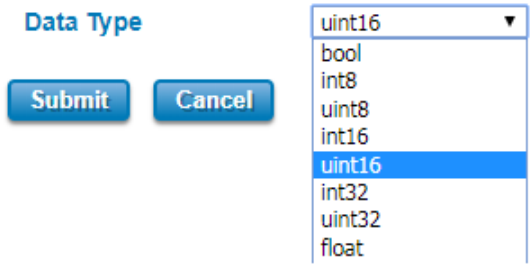
3.14.4 MODBUS DEVICE

This page allows the user to configure the Modbus connection so that the device will be connected to the SCB. Any kind of sensor should have their own information please check their information.



The description of the columns is as below:

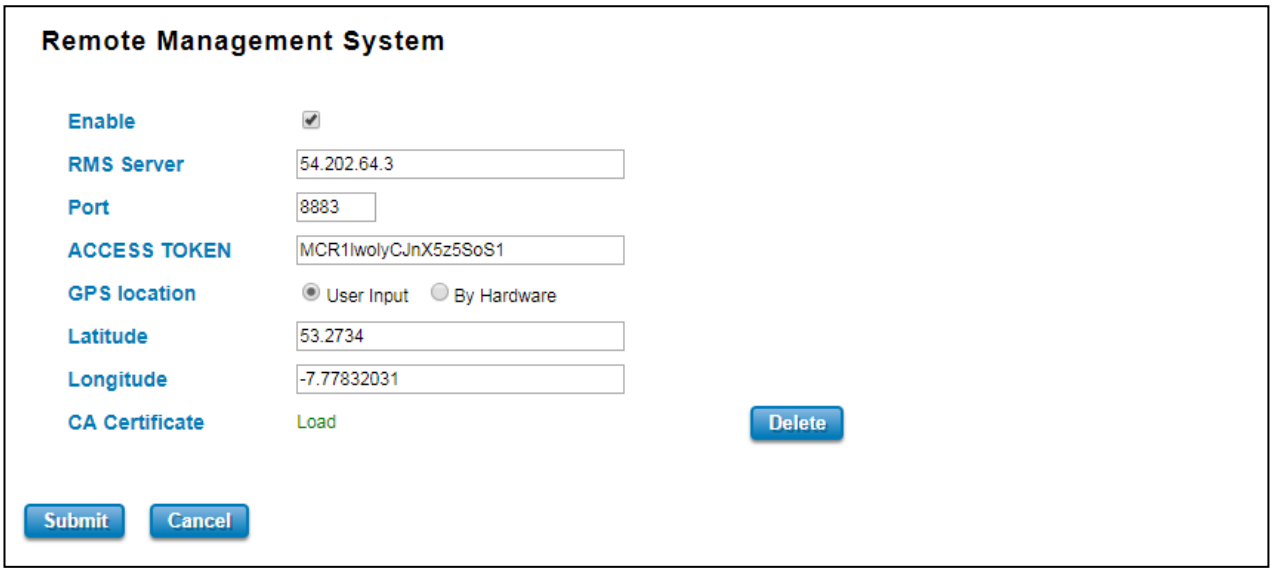
TERMS	DESCRIPTION
Modbus Logging	Check the box to enable the function.
Name	Enter the Modbus name
Serial	Select the Serial port 1 or 2. (1 – external, 2 – internal)
Slave ID	Enter the Slave ID that belongs to the device
PLC Address	Enter the PLC address that belongs to the device.
Function	
Data Type	Select the Data Type.

	
Edit	Click edit to modify the Modbus data
Alive	The Modbus device status (Yes or No)
Value	The current value from the Modbus device.

Note: User should configure the service mode to 'Modbus RTU' in serial setting page.

3.14.5 RMS

This page allows the user to configure the Remote Management System for the device, so that the device will be monitored through the ThingsMaster RMS.



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 OTA v1.0.0 and later version.**

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

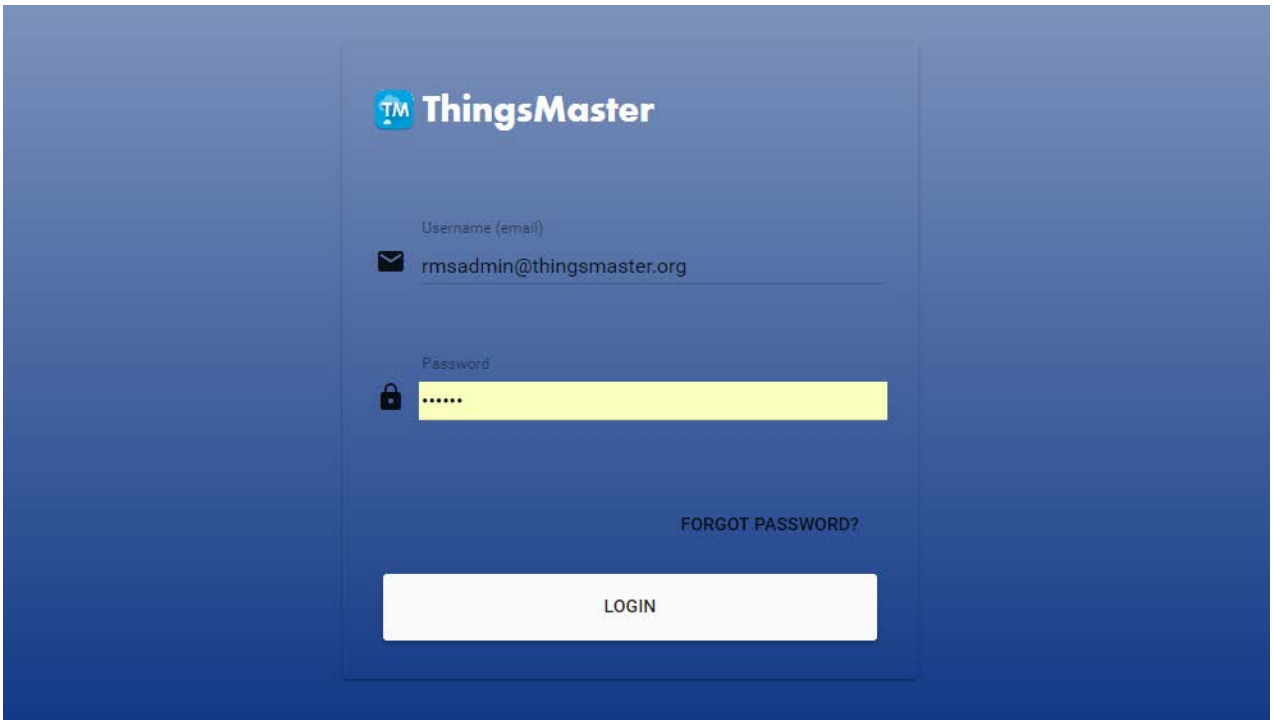
HOW TO ESTABLISH AND CONNECT TO THE THINGSMASTER RMS SERVER

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

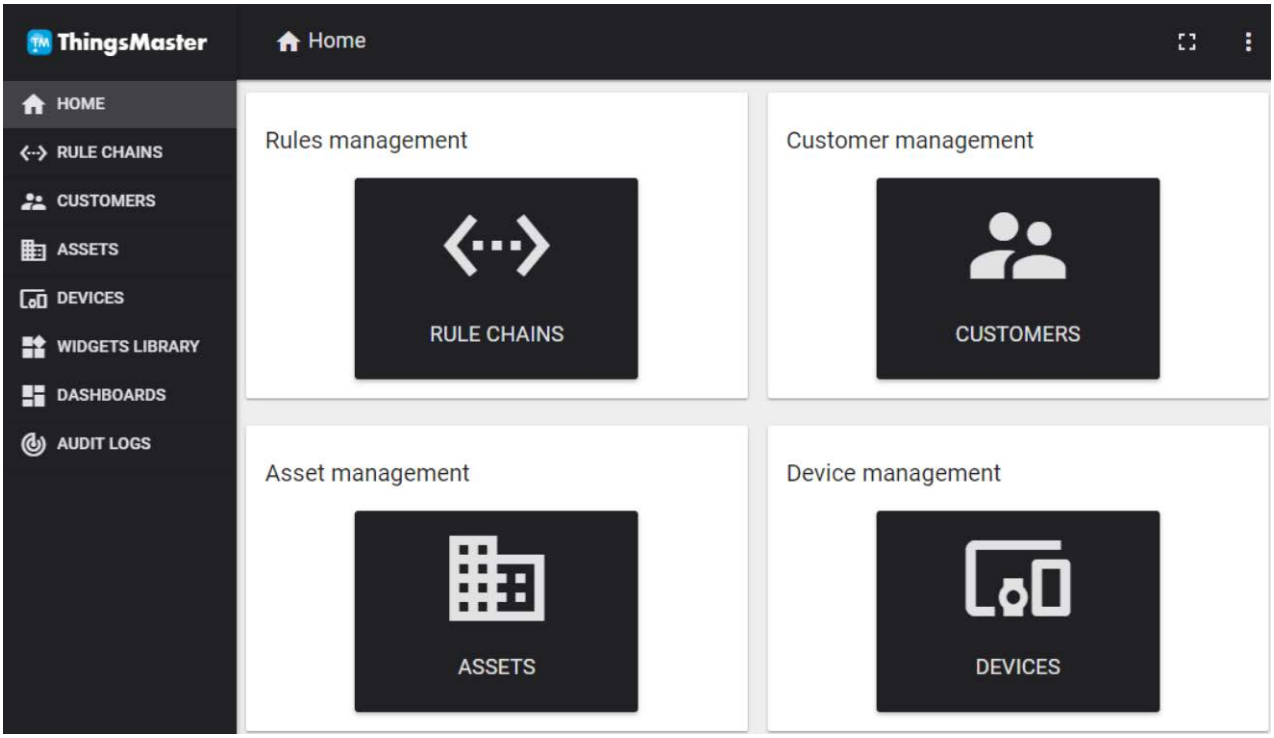
2. Login to ThingsMaster RMS, using RMS Account.

Login: <User RMS Account>

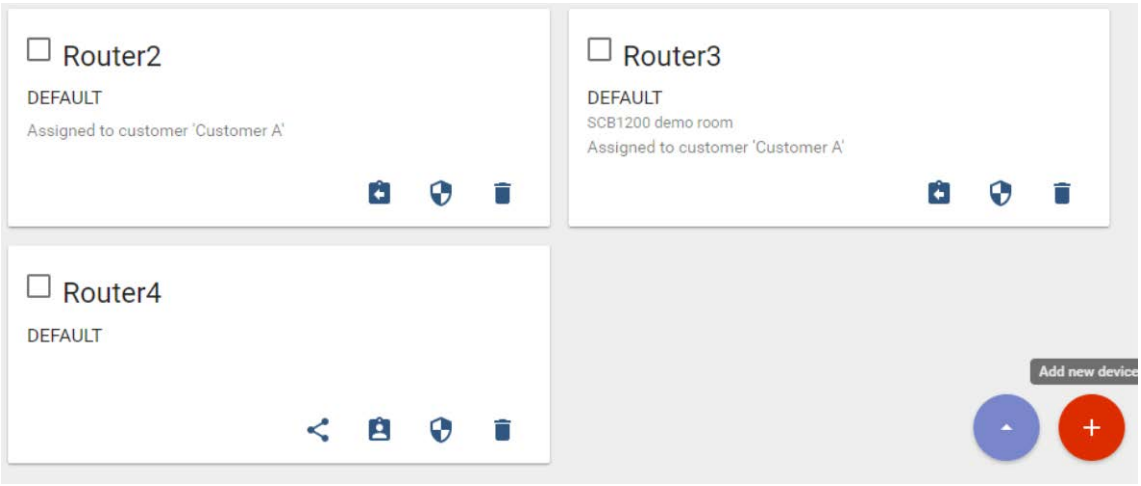
Password: <User RMS Password>



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

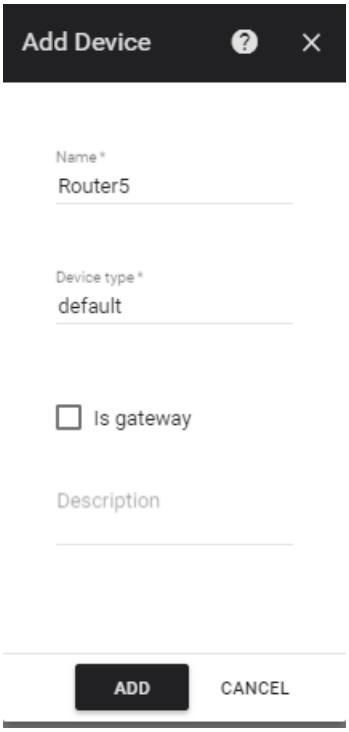


4. Add new device information, by clicking the “+” at the corner of the page.

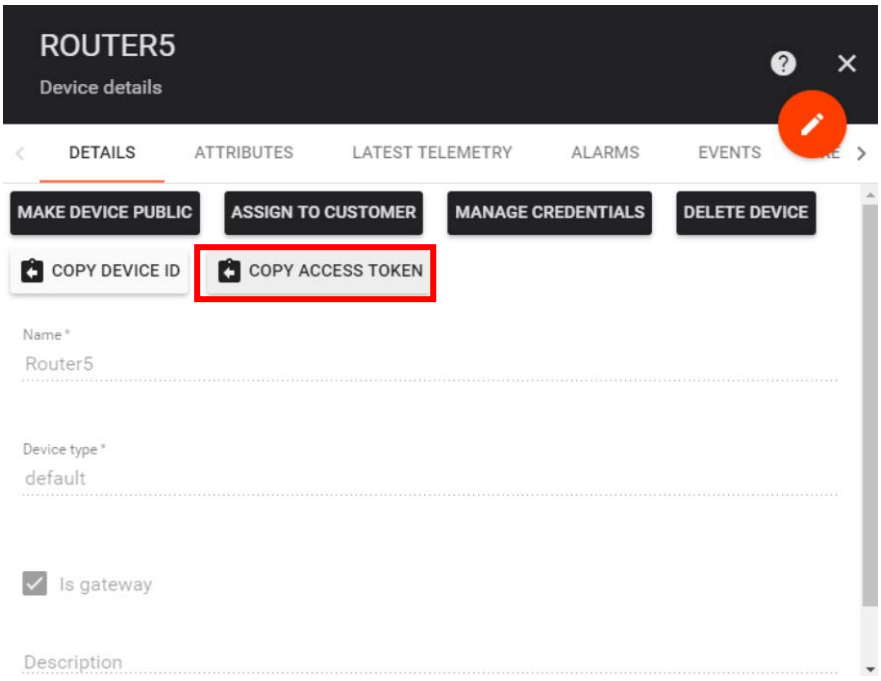


After click “+” menu then a page will pop up. Enter the device information.

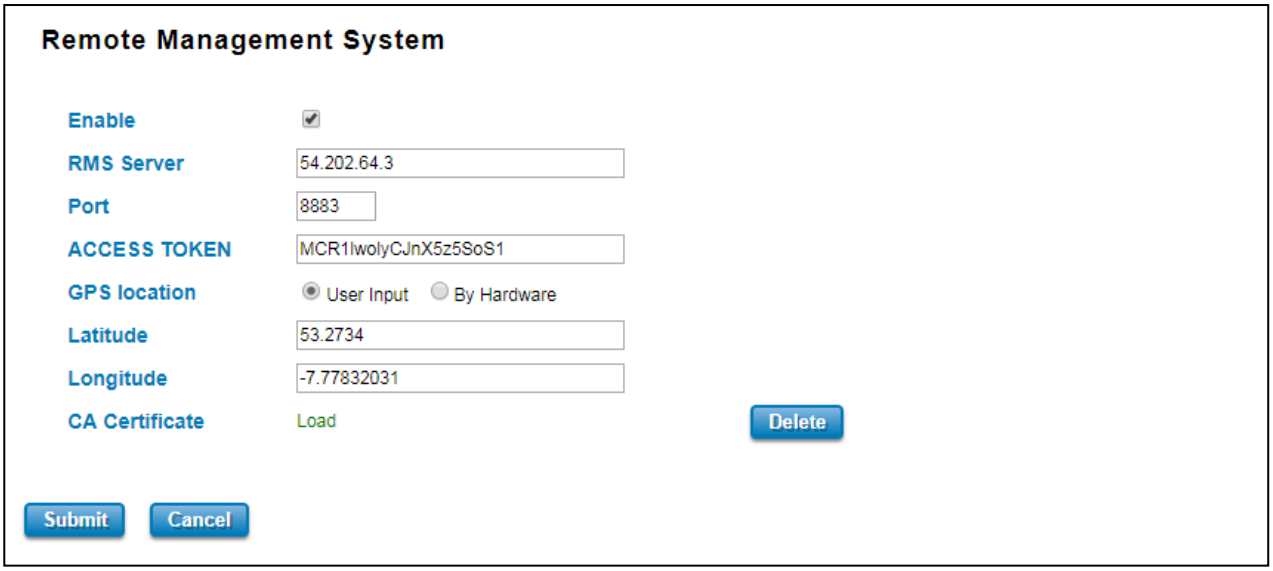
- Name: Please start the name with Router + Number.
- Device type: default
- Is gateway: check the box
- Click **Add**



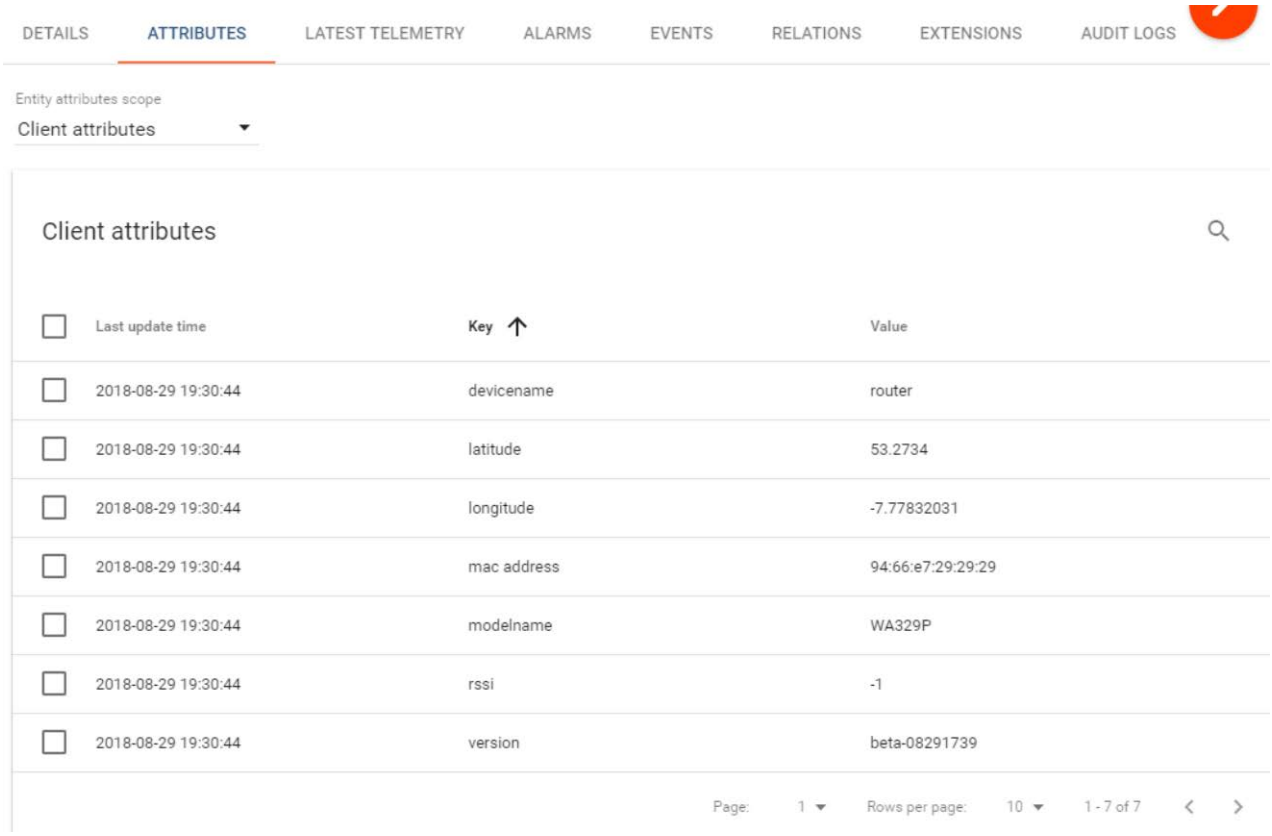
5. After the device is registered, then click on the device folder go to Details -> Click on Copy Access Token. This access token is code to link the device with the RMS Server.



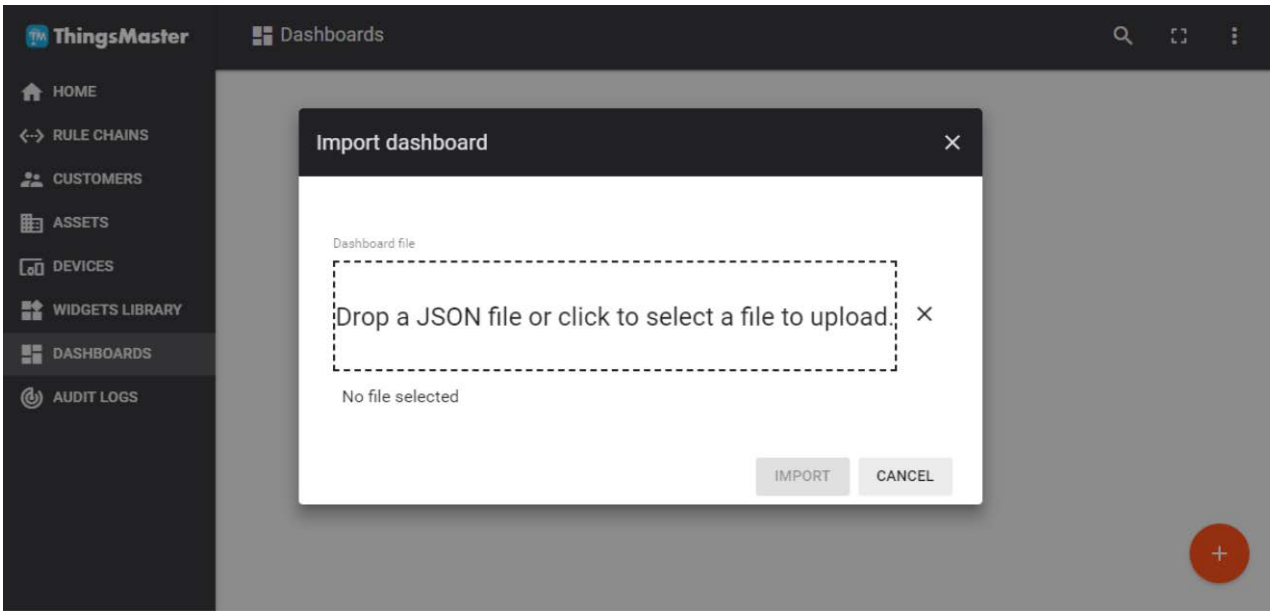
6. Go to the Web GUI -> IoT -> RMS. Paste the Access Token code to the Web GUI. And complete the configuration.



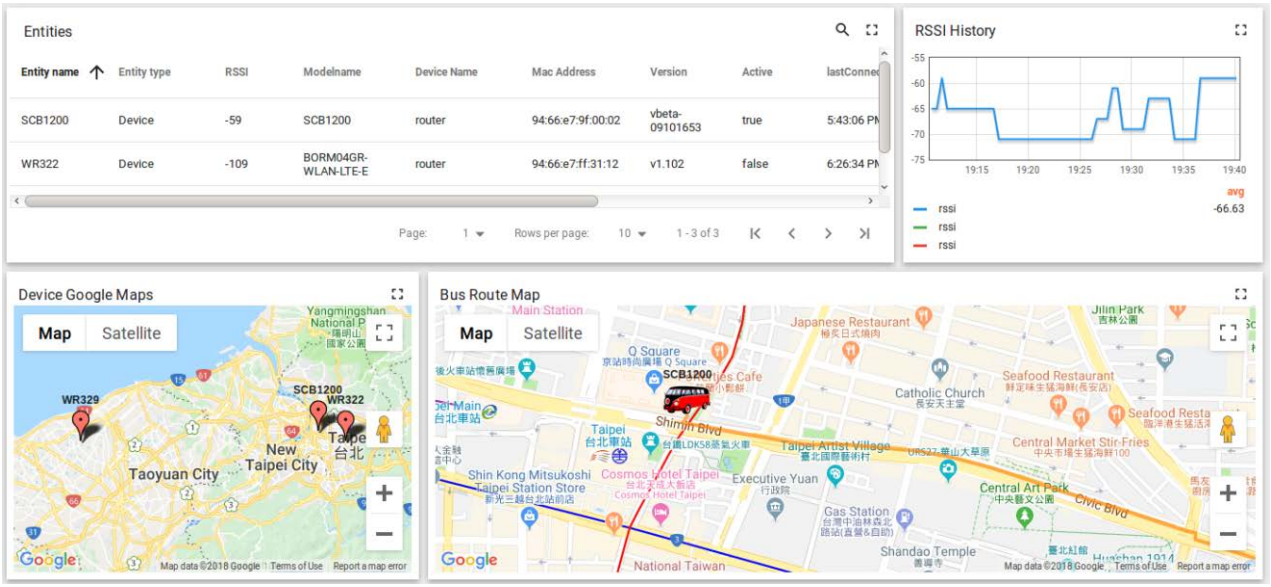
7. After the configuration is done then go back to ThingsMaster RMS Server. And then click on the newly added Router -> Attributes-> Client Attributes to see if the data has been uploaded.



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

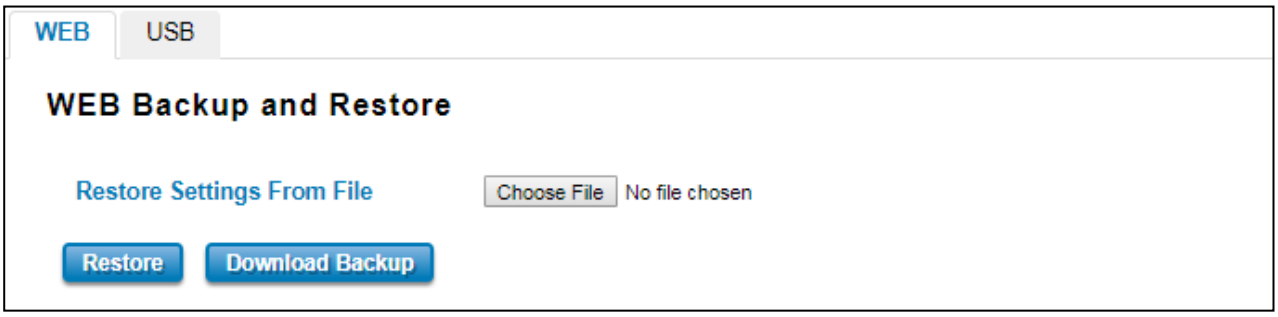


9. After the JSON file is uploaded, the dashboard will show as below:



3.15 BACKUP AND RESTORE

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



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



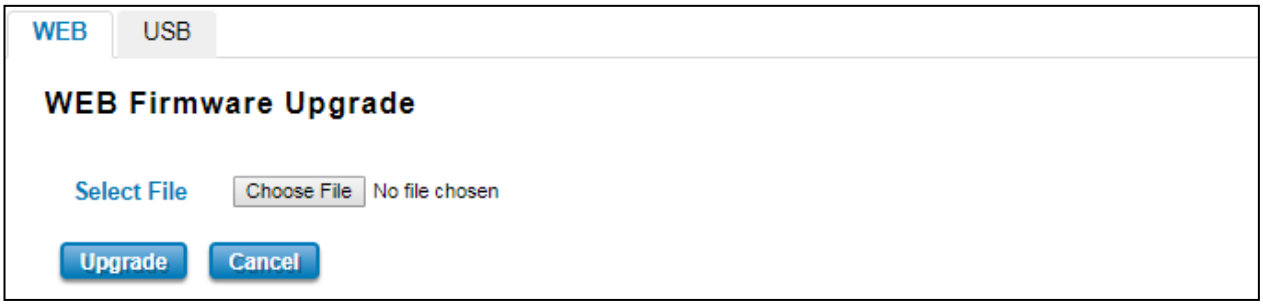
USB mode: this mode has two functions, Load Setting from File and Save Setting to USB. Load Setting from File, make sure that the USB has been inserted and it has the *.conf* file which is the backup files. After inserting the USB, the USB port will directly read the USB and then user needs to type the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

3.16 FIRMWARE UPGRADE

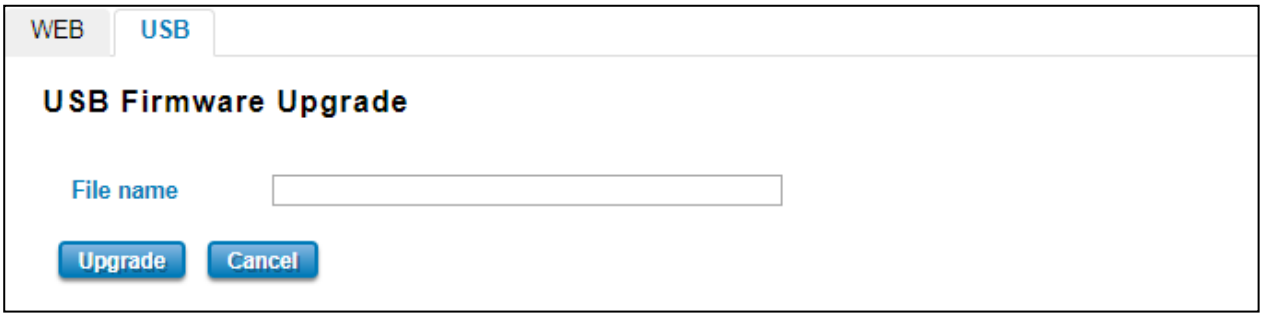
WoMaster provides the latest firmware online at www.womaster.eu. The new firmware may include new features, bug fixes or other software changes. WoMaster also provides the release notes for the update as well. For technical viewpoint, WoMaster suggests user uses the latest firmware before installing the router to the customer site.

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

There are 2 modes for users to backup/restore the configuration file, Web mode, and USB mode.



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



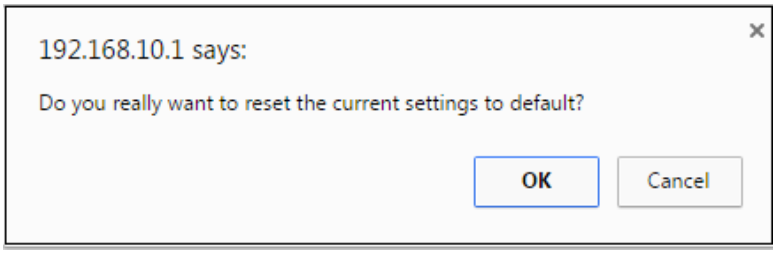
USB mode: plugged the USB device with the firmware file, then type the specific filename of the new firmware file. Then click **Upgrade**.

3.17 RESET TO DEFAULTS

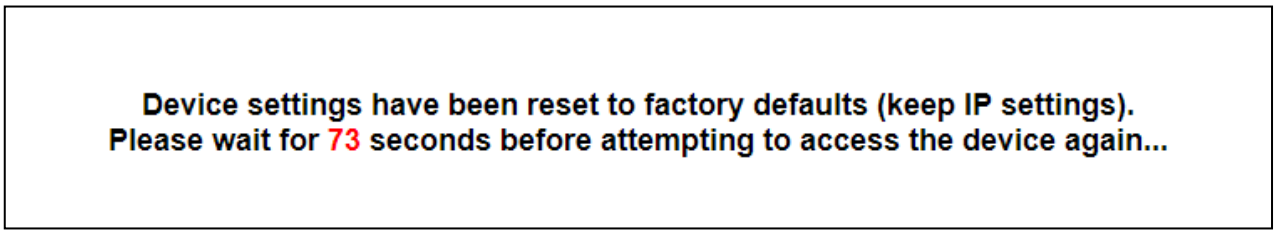
This function provides users with a quick way of restoring the WoMaster router's configuration to factory defaults. By check the Restore Factory default IP setting, it means the IP of the device will directly change to the default IP (192.168.10.1).



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

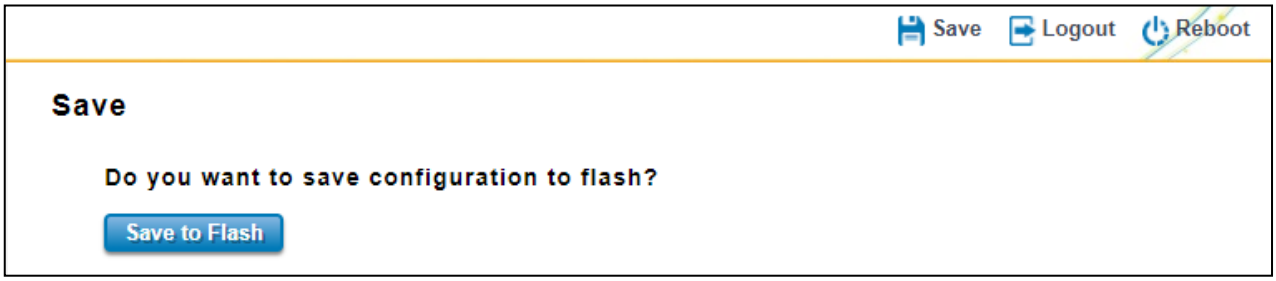


Below is the interface for resetting the device with keep the IP Settings.



3.18 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.



3.19 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.



3.20 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	Released the User Manual	21/08/2018	Yohan
V1.1	Remove the SD Card Add the cable installation (2.2) Update model name table (1.1) Update the dimension and appearance picture (2.1) Add the safety precaution for internal (2.2) Add Audio Jumper picture and table (2.7) Add the battery ON/OFF Switch description and picture (3.13.6) Update the IoT section	14/12/2018	Yohan