AVCOMM AP222

User Manual

AVCOMM Technologies Inc.

AP222

User Manual

Copyright Notice

About This Manual

This user manual is intended to guide a professional installer to install and to configure the AP222. 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 AP222.

Disclaimer

Avcomm 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 problem arise which are not covered sufficiently for the user's purposes, the matter should be referred to Avcomm. 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. Avcomm assumes no responsibility for its use by the third parties.

Avcomm Online Technical Services

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

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

AP222 is a smart solution for smart city and IIoT applications as a LTE/Wi-Fi dual radio field router, or simply a single high speed Wi-Fi AP. The router supports LTE to Wi-Fi redundancy and auto offload to guarantee high speed. RS232/422/485 port can connect to local serial devices over cellular and Ethernet network to safeguard cyber security, security features such as Firewall, OpenVPN, GRE tunnel are supported. The embedded MQTT and RESTful API enables public cloud integration such as AWS or Azure. The private cloud platform ATMS and ATMS OTA can also be setup for instant and secured access to receive data or manage devices remotely.

This Industrial Compact router also can be smartly configured by AVCOMM advanced management utility, Web Browser, SNMP, SSH, Telnet and Command Line Interface.

Excellent security features also provided, such as Firewall, Demilitarized Zone (DMZ), Port Forwarding, HTTPs, SSH for Telnet security, and many other security features. All these features in order to ensure the secure data communication.

AVCOMM' Industrial Compact router is designed to provide fast, secure, and more stable network. One advantage that makes it a powerful router is that it equips with wireless redundancy technologies such as LTE to Wi-Fi redundancy and auto offload to guarantee high speed. Besides, IEC 61000-6-2 / 61000-6-4 Heavy Industrial and CE marking, rugged enclosure and -40~70°C wide operating temperature range, all these features guarantee stable performance of AP222 for data transmission for Wayside and ITS Application. The embedded MQTT and RESTful API enable public cloud integration such as AWS or Azure. The private cloud platform ATMS and ATMS OTA can also be setup for instant and secured access to receive data or manage devices remotely.

Model Name	Description
AP222-WLAN-LTE	Industrial Wireless IIoT Field Routing Gateway，2FE+1COM, SD, 802.11b/g/n WLAN, LTE-E, 1SIM, FDD B1/3/5/7/8/20, TDD B38/40/41,2 个 10/100Base-TX RJ45，1 WLAN+1 LAN，1 DB9 RS232/422/485，1×SIM＆1×MicroSD，9~30VDC，-40˚C~70˚C，IP30
AP222-WLAN	Industrial Wireless IIoT Field Routing Gateway,2FE+1COM, SD, 802.11b/g/n WLAN，2*10/100Base-TX RJ45，1 WLAN+1 LAN，1 DB9 RS232/422/485，1× SIM＆1×MicroSD，9~30VDC，-40˚C~70˚C，IP30
AP222-LTE	Industrial Wireless IIoT Field Routing Gateway,2FE+1COM, SD, LTE-E, 1SIM, FDD B1/3/5/7/8/20, TDD B38/40/41,2 个 10/100Base-TX RJ45，1 WLAN+1 LAN，1 DB9 RS232/422/485，1×SIM＆1×MicroSD，9~30VDC，-40˚C~70˚C，IP30

1.2 MAJOR FEATURES

Below are the major features of AP222

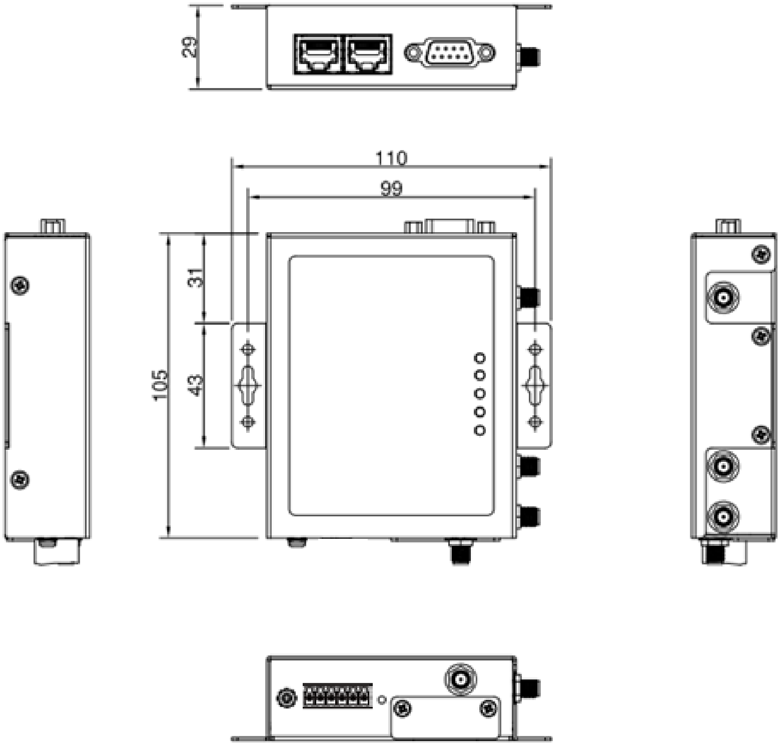
- 2 x 10/100MBase-TX RJ45, Auto Negotiation, Auto MDI/MDI-X, supports routing and bridging mode
- LTE Cat.4, 2T2R MIMO provides 150M downlink and 50M uplink
- Support NBIoT + M1
- IEEE 802.11b/g/n for 2.4G 2T2R MIMO delivers up to 300Mbps throughput
- RS232/422/485 full functions for serial over LTE/Wi-Fi/Ethernet data switching
- Supports one Digital Input to detect signal from the sensors or button and one Digital Output for Alarm
- Advanced network management features: IPv4, SNMP v1/v2c/v3/Trap, MIB II, Entity MIB, DHCP server/client, DHCP relay, TFTP, ARP response over 802.2 LLC SNAP, Proxy ARP, DNS (client/proxy), private MIB.
- Cellular Configuration: Radio on/off, 2G, 3G and 4G modes configurable, SIM Security, Connection Status, Cellular to Eth-WAN Redundancy
- Cellular to WLAN Auto Offload and advanced WLAN settings
- Serial communication: TCP Server/TCP Client/UDP mode, MODBUS RTU mode, TCP Alive check
- Advanced Security system by Firewall, DMZ, HTTPs, SSH, IEEE 802.1X/RADIUS, HTTPs Login and SSH Telnet
- 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
- Steel Metal with Aluminum for heat dissipation
- Wide range operating temperature -40~70˚C
- IP30 ingress protection

2. HARDWARE INSTALLATION

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

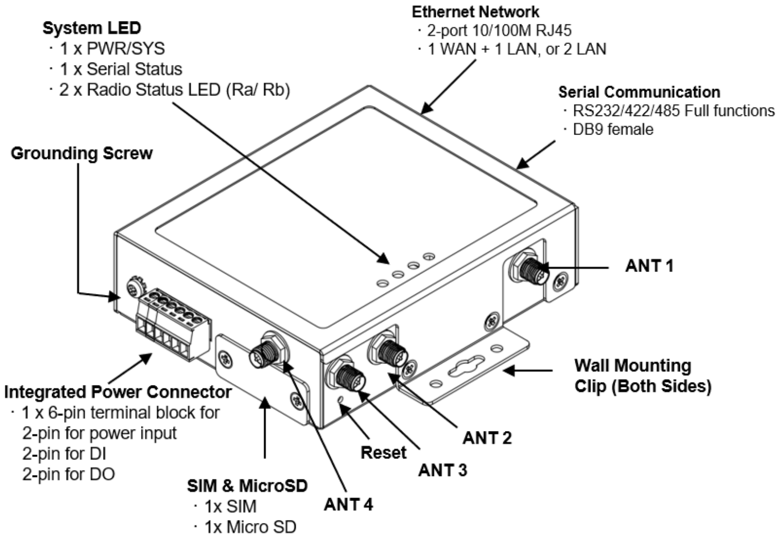
2.1 HARDWARE DIMENSION

Dimensions of AP222: 86 x 105 x 29mm (W x D x H) / without DIN Rail Clip

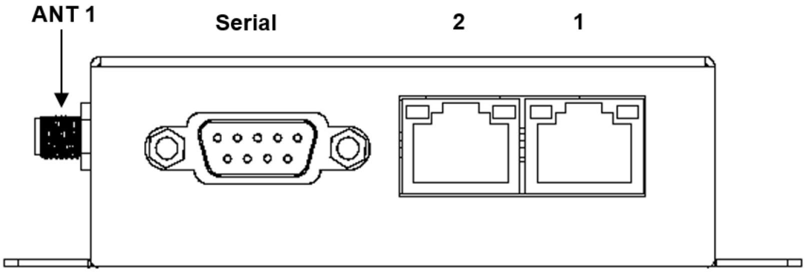


Interfaces

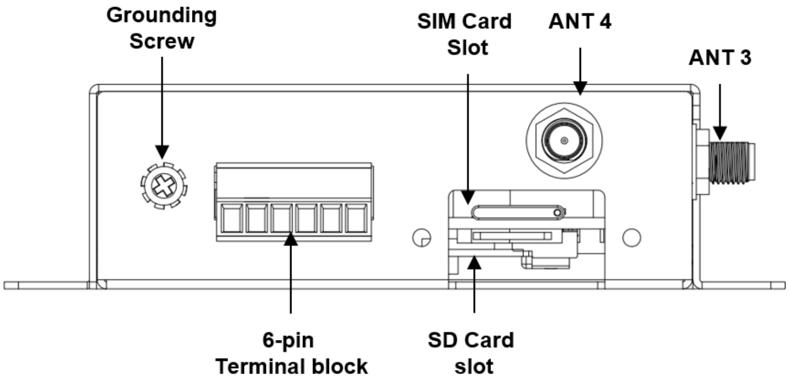
The interfaces from AP222 routers include 2 Ethernet ports (10/100 Base-TX, RJ45, Router Mode: 1 WAN + 1 LAN, Bridge Mode: 2 LAN), 1 x RS232/422/485 full functions, System LED, 1 x 6- Pin Removable Terminal Block Connector (2 Pins for V+/V- , 2 Pins for DI, 2 Pins for DO), 1 x chassis grounding screw , 1 x Nano SIM Socket 1 x Micro SD, 1 x Reset Bottom, 4 x SMA Socket. On the side of the device, there are Wall mount that can be installed with DIN rail bracket.



Top Panel



Bottom Panel

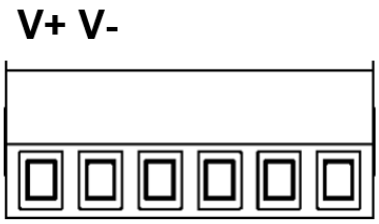


2.2 INSTALLATION

After unpacking the box, follow the steps below in order to properly connect the device. For better Wi-Fi performance, put the device in a clearly visible spot, as obstacles such as walls and doors hinder the signal. Assemble router by attaching the necessary antennas and inserting the SIM card.

2.3 WIRING THE POWER INPUTS

Power Input port in the router provides a set power input connection on the terminal block. On the picture below is the power connector.



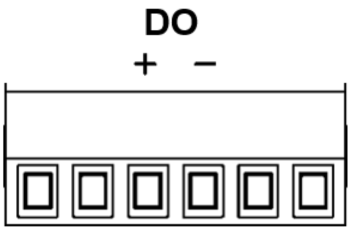
Wiring the Power Input

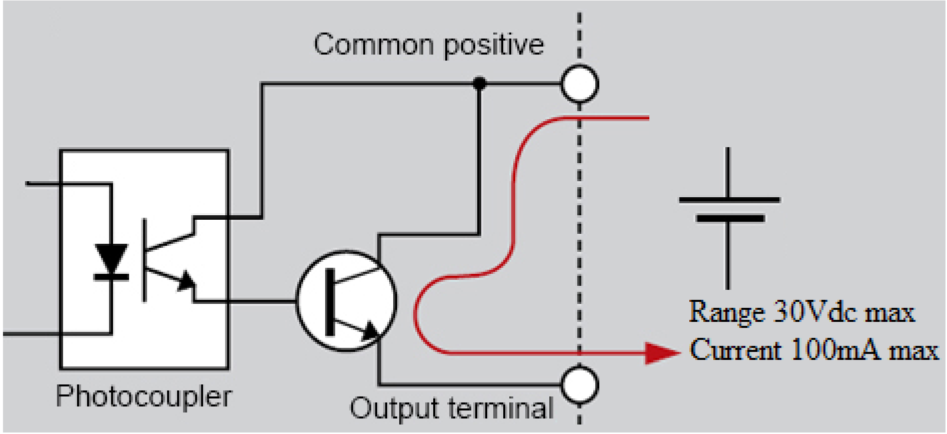
1. Insert the positive and negative wires into the V+ and V- contact on the terminal block connector.
2. Tighten the wire-clamp screws to prevent the power wires from being loosened.
3. Connect the power wires to suitable DC Switching type power supply. The input DC voltage should be in the range of 9V DC to DC 30V DC.

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

2.4 WIRING THE DIGTIAL OUTPUT (DO)

The digital output of the 2-pin terminal block connector is used to detect user-configured events. The two wires attached to the fault contacts form a close circuit when a user-configured event is triggered. If a user-configured event does not occur, the fault circuit remains opened.





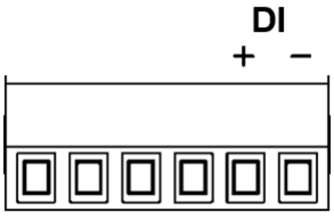
Wiring the Digital Output

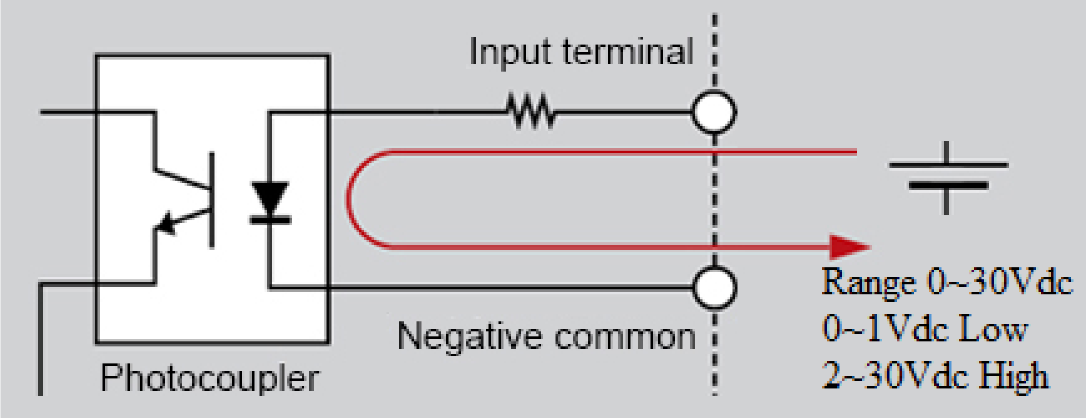
1. Insert the positive and negative wires into the DO+ and DO- contact on the terminal block connector.
2. Tighten the wire-clamp screws to prevent the wires from being loosened.

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

2.5 WIRING THE DIGTIAL INPUT (DI)

To wire the DI on the Terminal block, use screwdriver to loosen screws, insert the positive and negative wires into the DI+ and DI- contact and then tighten screws after the DI wire is connected.





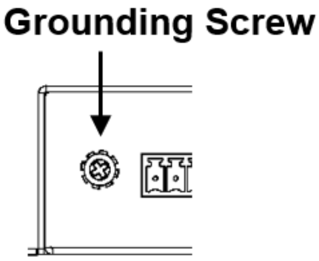
Wiring the Digital Input

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

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

2.6 CONNECTING THE GROUNDING SCREW

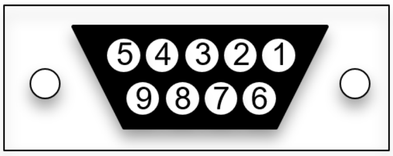
Grounding screw is located on the bottom side of the router. Grounding Screw helps limit the effects of noise due to electromagnetic interference (EMI) such as lighting or surge protection. Run the ground connection from the ground screw to the grounding surface prior to connecting devices. And tighten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



2.7 SERIAL PORT

One Full Pin RS232, RS422, RS485 with DB-9 socket

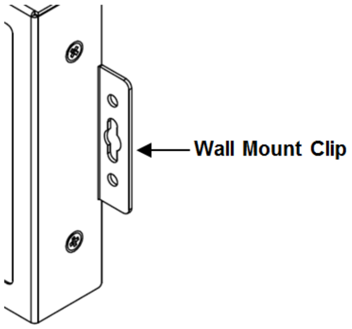
DB9 Female



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

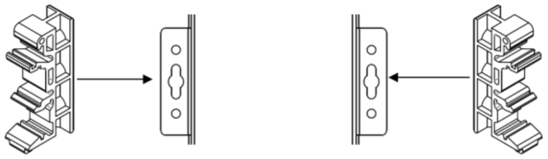
2.8 WALL MOUNTING

Two wall mounting plates are installed at the left and right side of the switch. Use the two hook holes at the corners of each wall mounting plate or the middle hole to hang the switch on the wall them then screw tightly.



2.9 DIN RAIL MOUNTING (Optional Accessory)

For the DIN Rail mount, attach the DIN Rail Clip to the two wall mount plates. Please check the Optional Accessory list.



To attach the DIN Rail Clip, screw the DIN Rail Clip to the wall mounting plates.

2.10 ANTENNA

AP222 is supported with up to 4 antenna sockets, where 3G/LTE and Wi-Fi antennas are supported. All of the antennas are connected to the router by screwing all the antennas to the SMA connector on the front panel of the router.

Wi-Fi Antenna

	Frequency	2400 ~ 2500 MHz 5150 ~ 5850 MHz
	S.W.R	<= 2.0 @ 2400 ~ 2500 MHz <= 2.0 @ 5150 ~ 5850 MHz The data is tested with 1M cable
	Peak Gain	2.5 ± 0.5 dBi @ 2400 ~ 2500 MHz 3.0 ± 0.5 dBi @ 5150 ~ 5850 MHz
	Efficiency	70 % @ 2400 ~ 2500 MHz 85 % @ 5150 ~ 5850 MHz
	Polarization	Linear
	Impedance	50 Ohm
	Connector Type	SMA
	Operational Temperature	- 40 °C ~ +65 °C

LTE Antenna

	Frequency	704 ~ 960 MHz 1710 ~ 2690 MHz
	V.S.W.R	<= 3.0
	Radiation	Omni
	Gain	2dBi
	Polarization	Linear
	Impedance	50 Ohm
	Connector Type	SMA
	Operational Temperature	- 20 °C ~ +65 °C

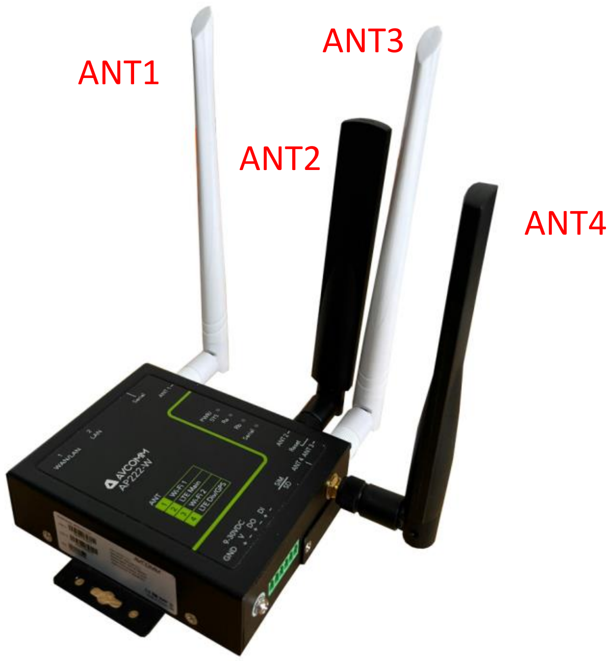
NOTE: Please refer to device stick for antenna combination of different models

Antenna Placement

	AP222-WLAN+LTE	AP222-WLAN
ANT 1	Wi-Fi 1	Wi-Fi 1
ANT 2	LTE-Main	--
ANT 3	Wi-Fi 2	Wi-Fi 2
ANT 4	LTE-DIV/GPS*	--

***** GPS support by request***

Check the picture below for the antenna installation. (take AP222-WLAN+LTE as an example)



Radio LED

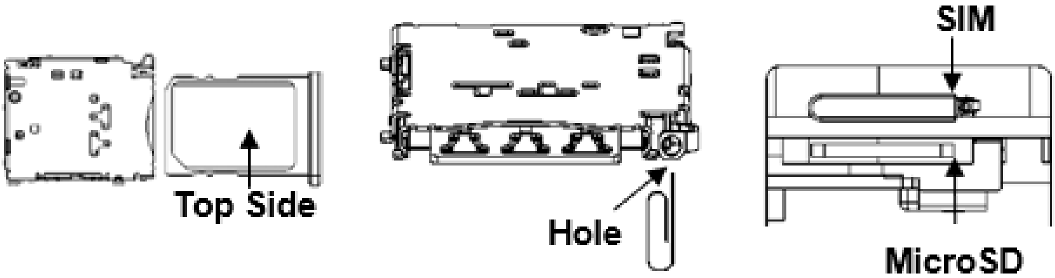
Radio	Status
Ra	4G Connection: Green On
	2/3G connection: Green Blinking
	Disconnected: Off
Rb	AP mode: Green On
	Station mode connected: Green Blinking
	Station mode/radio disable: Off

2.11 SIM /SD CARD INSTALLATION

SIM Card Slot

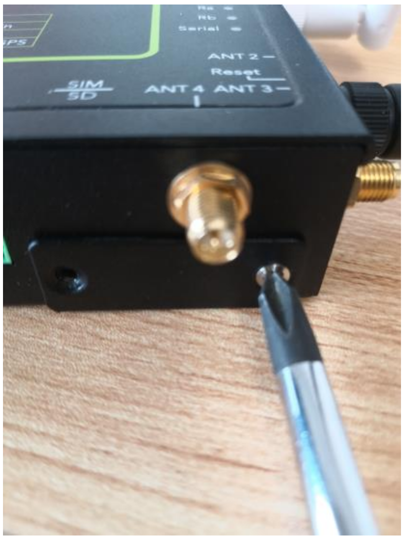
The SIM Card Slot is used to insert the cellular card.

> **WARNING:** Sim tray is fool-proof design. Push tray in wrong direction into the SIM socket could cause damage to the device

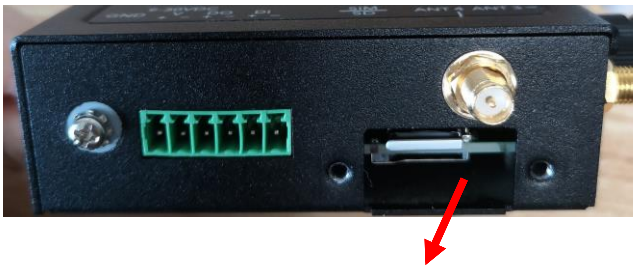


1. Turn off DC power input source before inserting the SIM Card.

2. Use screwdriver to loosen screws and remove SIM/SD cover.



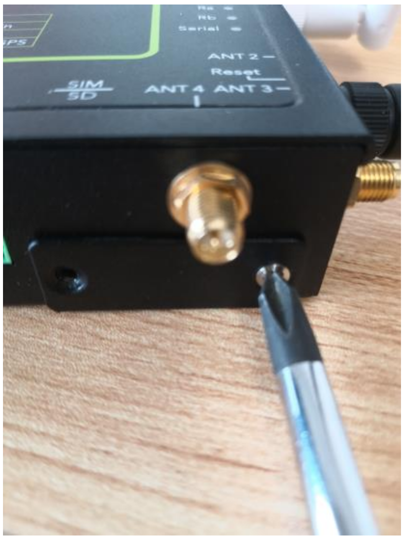
3.Insert a paper clip or a SIM-eject tool into the hole beside the SIM socket. Push in towards the device, but don't force it.



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

(When uninstall) Draw out SIM tray and uninstall SIM card.

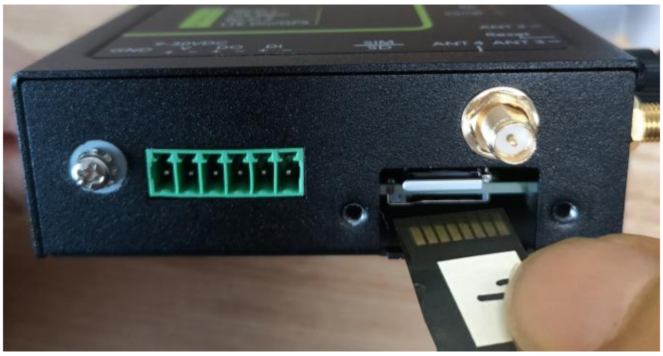
5. Insert tray back to SIM socket and reattach SIM/SD cover.



SD Card Slot

(When install) Plug MicroSD card into the socket. You will hear “click” when installed.

(When uninstall) Push in on the SD card and then remove.



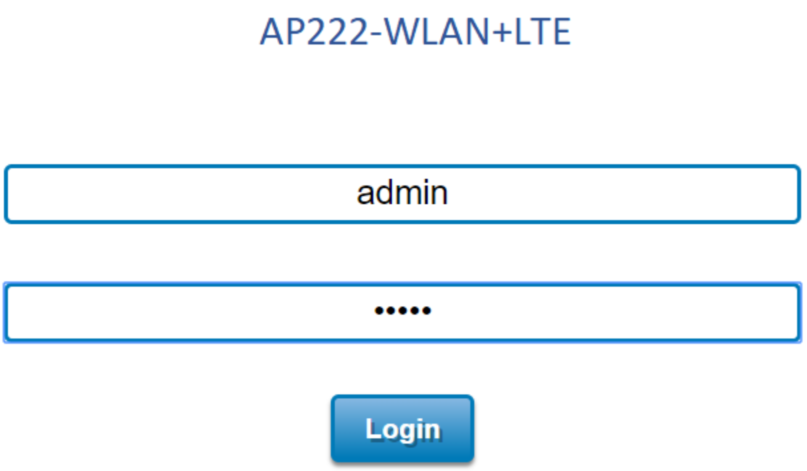
3. WEB MANAGEMENT CONFIGURATION

To access the management interface, AVCOMM 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

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

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

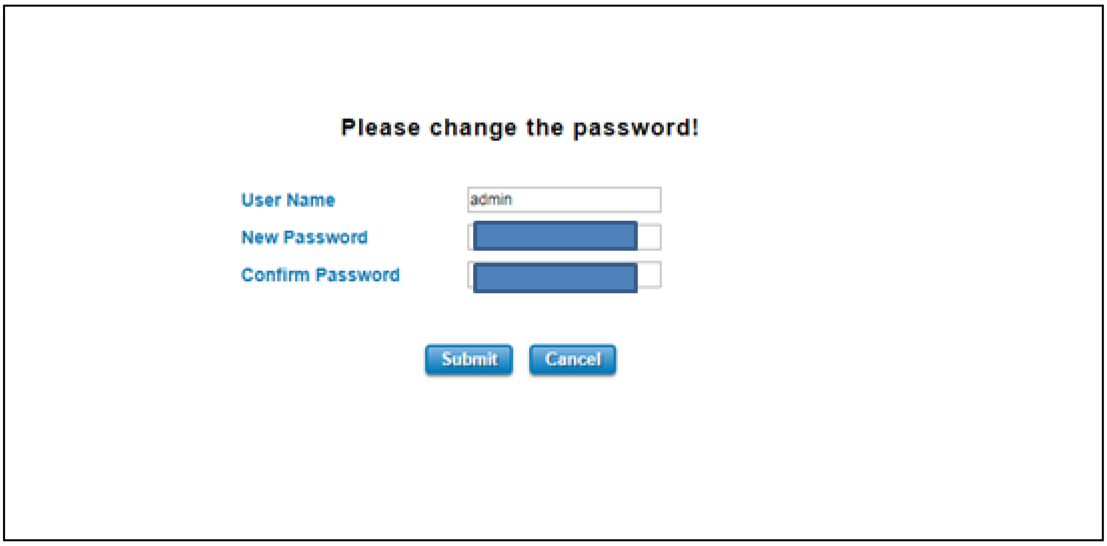


AP222-WLAN+LTE

admin

•••••

7. Type user name and the password. Default user name: **admin** and password: **admin**. Then click **Login**.
8. After user clicks Login, then user will be asked to change the default password with a new password.



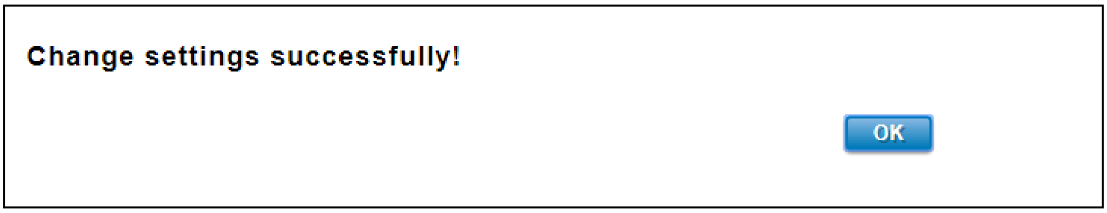
Please change the password!

User Name: admin

New Password: [redacted]

Confirm Password: [redacted]

Enter new password and Submit to apply the change.

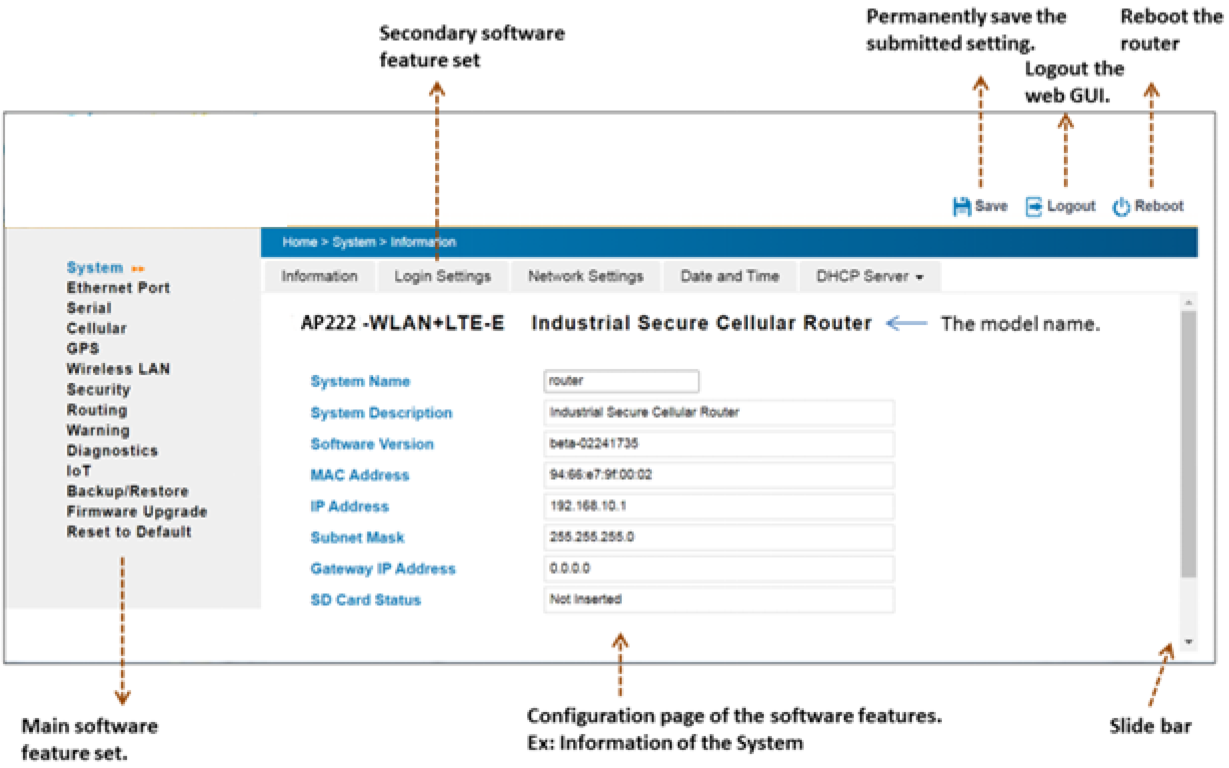


Change settings successfully!

Then re-login with the new password.

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

Web GUI Console Example 1: System Information



Secondary software feature set

Permanently save the submitted setting.

Logout the web GUI.

Reboot the router

AP222 -WLAN+LTE-E Industrial Secure Cellular Router ← The model name.

System Name: router

System Description: Industrial Secure Cellular Router

Software Version: beta-02241735

MAC Address: 94:66:e7:9f:00:02

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

Gateway IP Address: 0.0.0.0

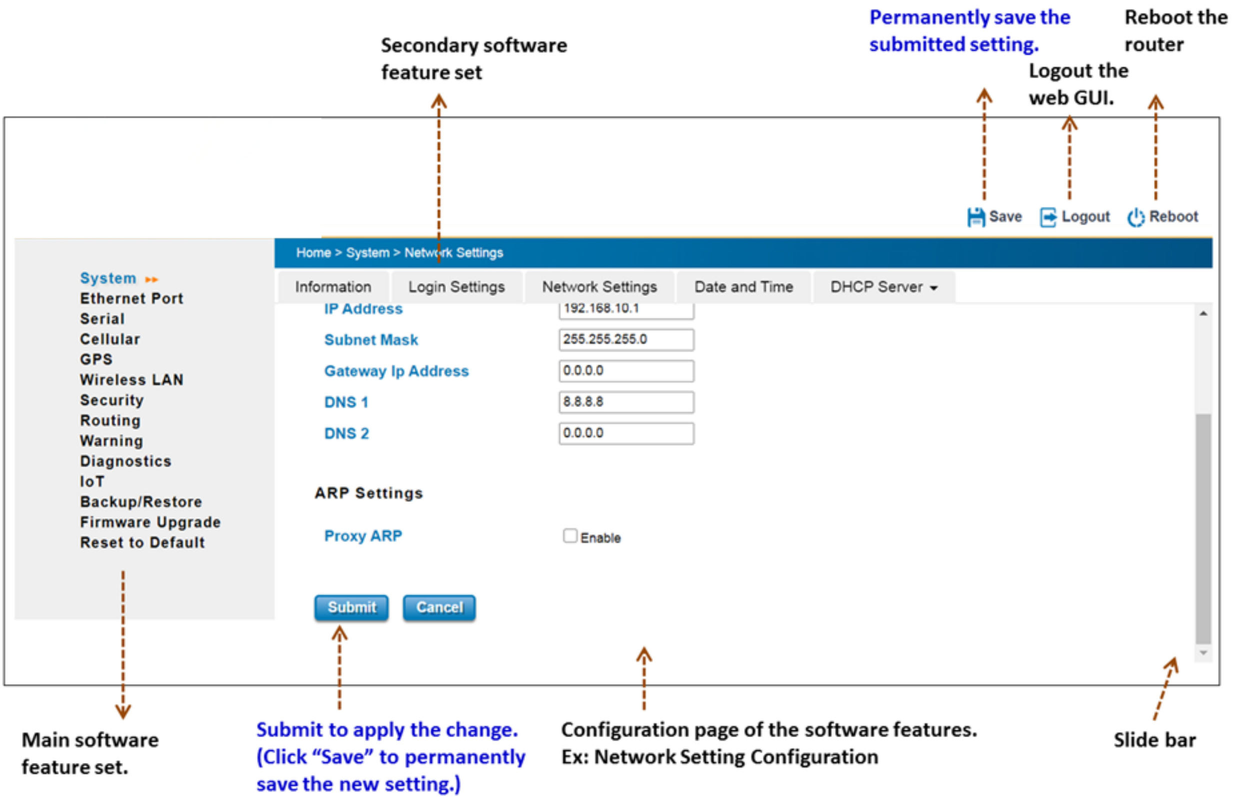
SD Card Status: Not Inserted

Main software feature set.

Configuration page of the software features.
Ex: Information of the System

Slide bar

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



Secondary software feature set
Permanently save the submitted setting.
Reboot the router
Logout the web GUI.
Save
Logout
Reboot
Home > System > Network Settings
Information
Login Settings
Network Settings
Date and Time
DHCP Server
System
Ethernet Port
Serial
Cellular
GPS
Wireless LAN
Security
Routing
Warning
Diagnostics
IoT
Backup/Restore
Firmware Upgrade
Reset to Default
Submit
Cancel
Main software feature set.
Submit to apply the change. (Click "Save" to permanently save the new setting.)
Configuration page of the software features. Ex: Network Setting Configuration
Slide bar

IP Address 192.168.10.1

Subnet Mask 255.255.255.0

Gateway Ip Address 0.0.0.0

DNS 1 8.8.8.8

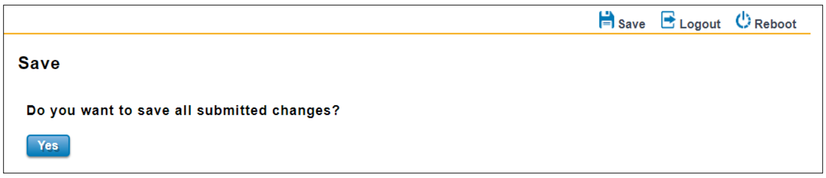
DNS 2 0.0.0.0

ARP Settings

Proxy ARP □ Enable

In this Web management for Featured Configuration, user will see all of AVCOMM Router's various configuration menus at the left side from the interface. Through this web management interface, user can configure, monitoring, and set the administration functions. The whole information used web management interface to introduce the featured functions. User can use all of the standard web-browser to configure and access the router on the network. After configured and submitted, the setting is activated immediately. However, if you want to reserve the setting after rebooting, you must click "Save" to permanently save the settings.

Notice: To save the changed settings permanently, user must click on "**Save**" at the top of the configuration page and click "**Yes**" to save all the submitted changes. Without "Save", the settings will be discarded if the switch is rebooted.



Save

Do you want to save all submitted changes?

Following topics are covered in this chapter:

3.1 System

3.2 Ethernet Port

3.3 Serial

3.4 Cellular

3.5 Wireless LAN

3.6 Security

3.7 Routing

3.8 Warning

3.9 Diagnostics

3.10 IoT

3.11 Backup and Restore

3.12 Firmware Upgrade

3.13 Reset to Defaults

3.14 Save

3.15 Logout

3.16 Reboo

3.1 SYSTEM

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

3.1.1 Information

3.1.2 Login Setting

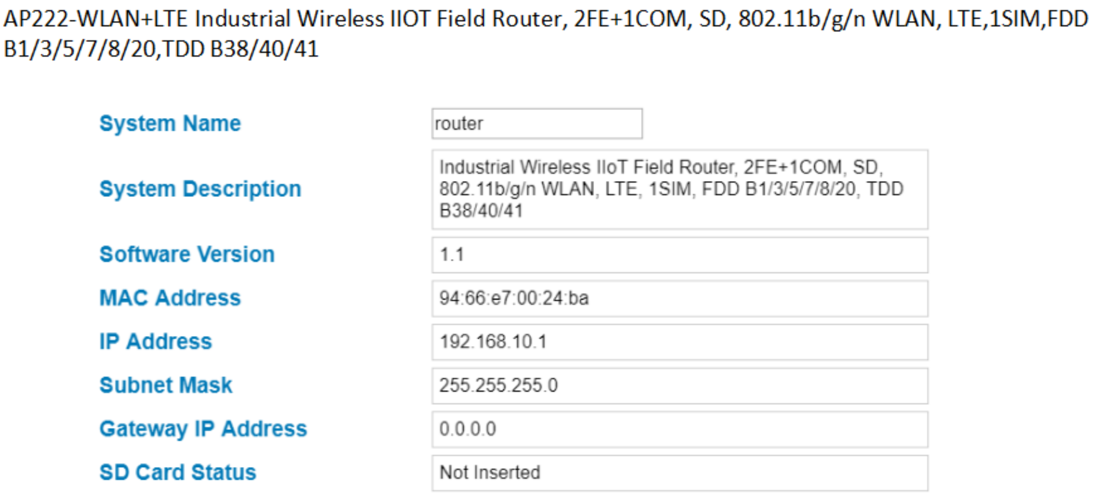
3.1.3 Network IP

3.1.4 Date and Time

3.1.5 DHCP Server

3.1.1 INFORMATION

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



AP222-WLAN+LTE Industrial Wireless IIOT Field Router, 2FE+1COM, SD, 802.11b/g/n WLAN, LTE,1SIM,FDD B1/3/5/7/8/20,TDD B38/40/41

System Name	router
System Description	Industrial Wireless IIoT Field Router, 2FE+1COM, SD, 802.11b/g/n WLAN, LTE, 1SIM, FDD B1/3/5/7/8/20, TDD B38/40/41
Software Version	1.1
MAC Address	94:66:e7:00:24:ba
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
SD Card Status	Not Inserted

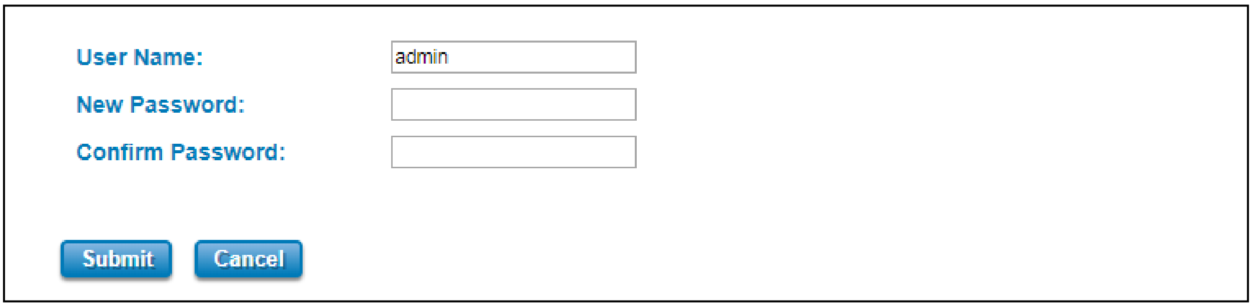
The description of the Information's interface is as below:

TERMS	DESCRIPTION
System Name	**Default: router** Set up a name to the device.

System Description	Display the name of the product.
Software Version	Display the firmware latest version that installed in the device.
MAC Address	Display the hardware's MAC address that assigned by the manufacturer.
IP Address	Display the IP Address of the device
Subnet Mask	Display the subnet mask of the device
Gateway IP Address	Display the gateway IP Address of the device
SD Card Status	Display the SD Card port status when the SD Card is inserted or not inserted.

3.1.2 LOGIN SETTING

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



User Name: admin

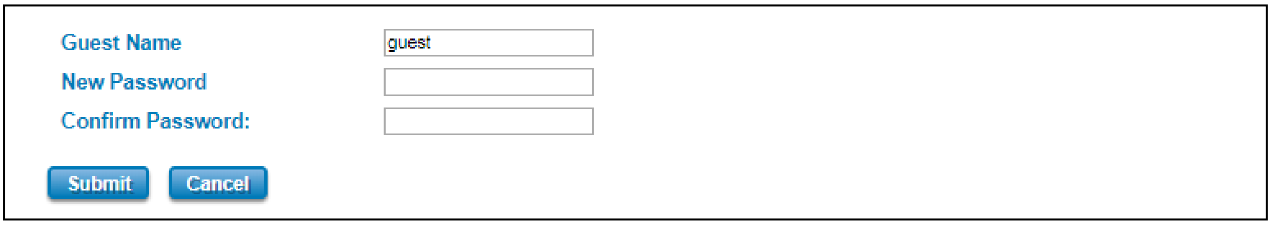
New Password:

Confirm Password:

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

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

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



Guest Name guest

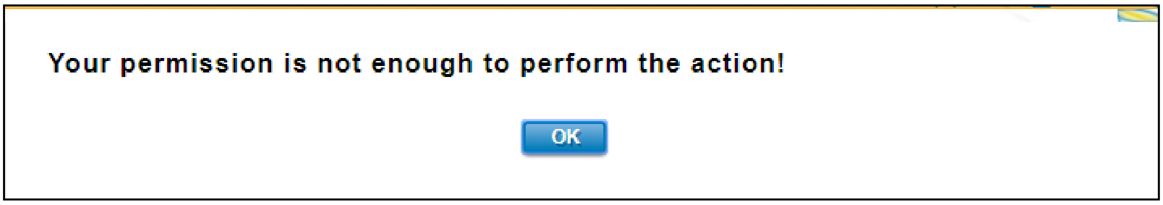
New Password

Confirm Password:

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

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

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



Your permission is not enough to perform the action!

The description of the Login Setting interface is as below:

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

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

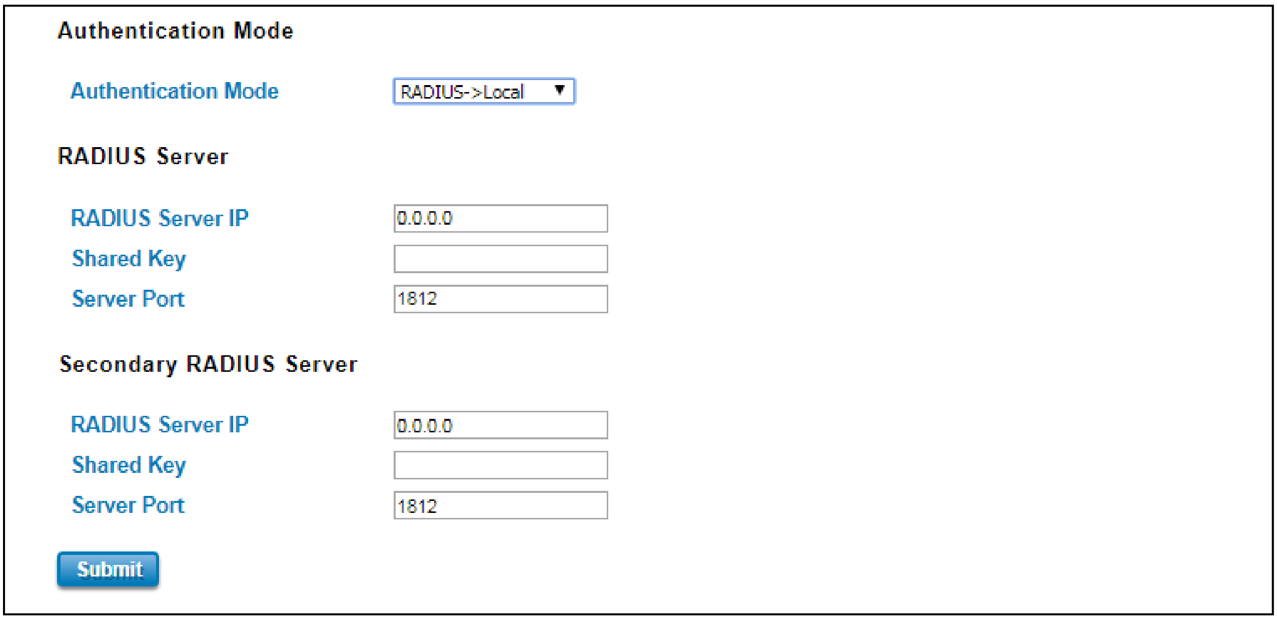
User Authentication Mode

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

RADIUS

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

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



Authentication Mode

Authentication Mode: RADIUS->Local

RADIUS Server

RADIUS Server IP: 0.0.0.0

Shared Key:

Server Port: 1812

Secondary RADIUS Server

RADIUS Server IP: 0.0.0.0

Shared Key:

Server Port: 1812

How to set up a RADIUS server:

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

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

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

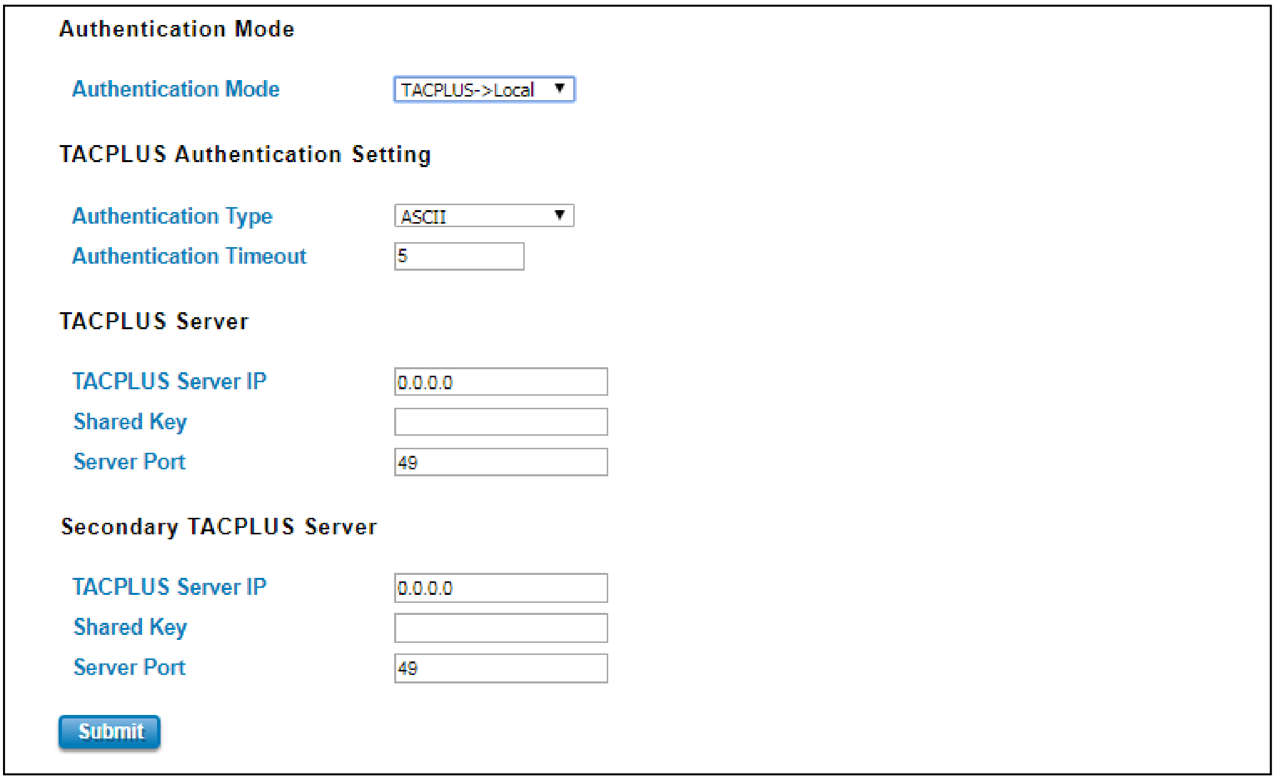
d. Click **Submit**

The description of the RADIUS Authentication interface is as below:

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

TACACS+

The Terminal Access Controller Access Control System (TACACS+) security protocol is a recent protocol developed by Cisco. It provides detailed accounting information and flexible administrative control over the authentication and authorization processes. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide authentication, authorization, and accounting services independently. Below is the interface for TACPLUS and TACPLUS to Local authentication mode. For the TACPLUS to Local mode, the authentication will try remote authentication first, falling back to local authentication mode if remote mode fails or cannot be reached.



Authentication Mode

Authentication Mode: TACPLUS->Local

TACPLUS Authentication Setting

Authentication Type: ASCII

Authentication Timeout: 5

TACPLUS Server

TACPLUS Server IP: 0.0.0.0

Shared Key:

Server Port: 49

Secondary TACPLUS Server

TACPLUS Server IP: 0.0.0.0

Shared Key:

Server Port: 49

How to set up a TACACS+ server:

a. Select the **Authentication Type.**

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

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

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

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

f. Click **Submit**

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

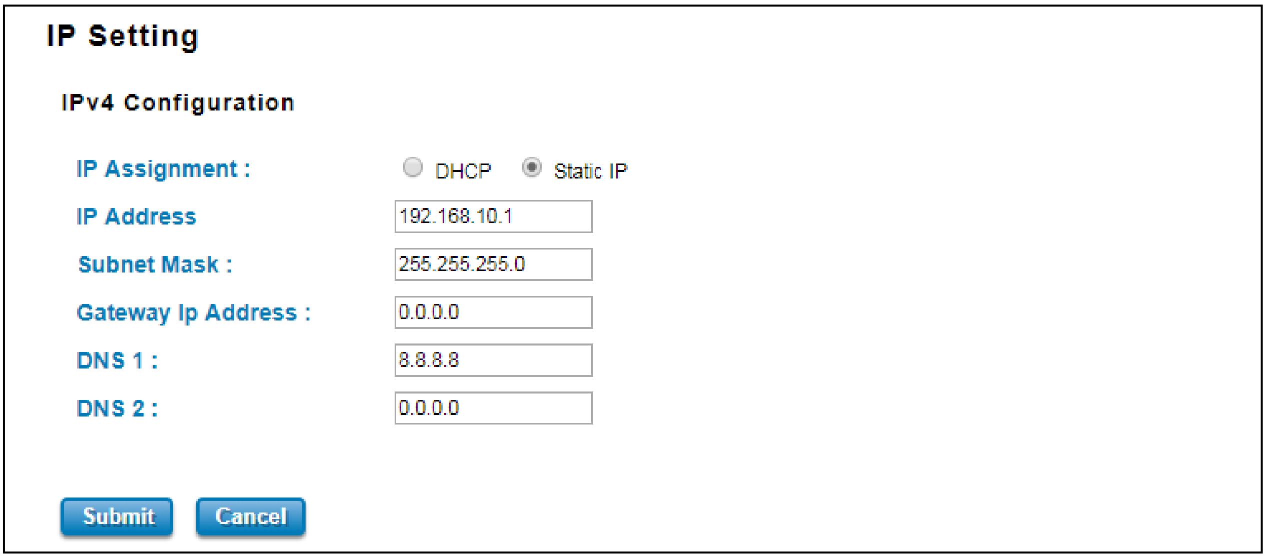
TERMS	DESCRIPTION
Authentication Type	**Default: ASCII** Select the authentication type to authenticate to the server.
Authentication Timeout	**Default: 5** The maximum number of seconds allowed establishing a TCP connection between the device and the TACACS+ server. If the server cannot be reached within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

	and the TACACS+ server. The shared key must match the encryption used on the TACACS+ server.
Server Port	Set communication port of an external TACACS+ server as the authentication database. The general value is 49

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

3.1.3 NETWORK SETTING

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



IP Setting

IPv4 Configuration

IP Assignment : ○ DHCP ● Static IP

IP Address 192.168.10.1

Subnet Mask : 255.255.255.0

Gateway Ip Address : 0.0.0.0

DNS 1 : 8.8.8.8

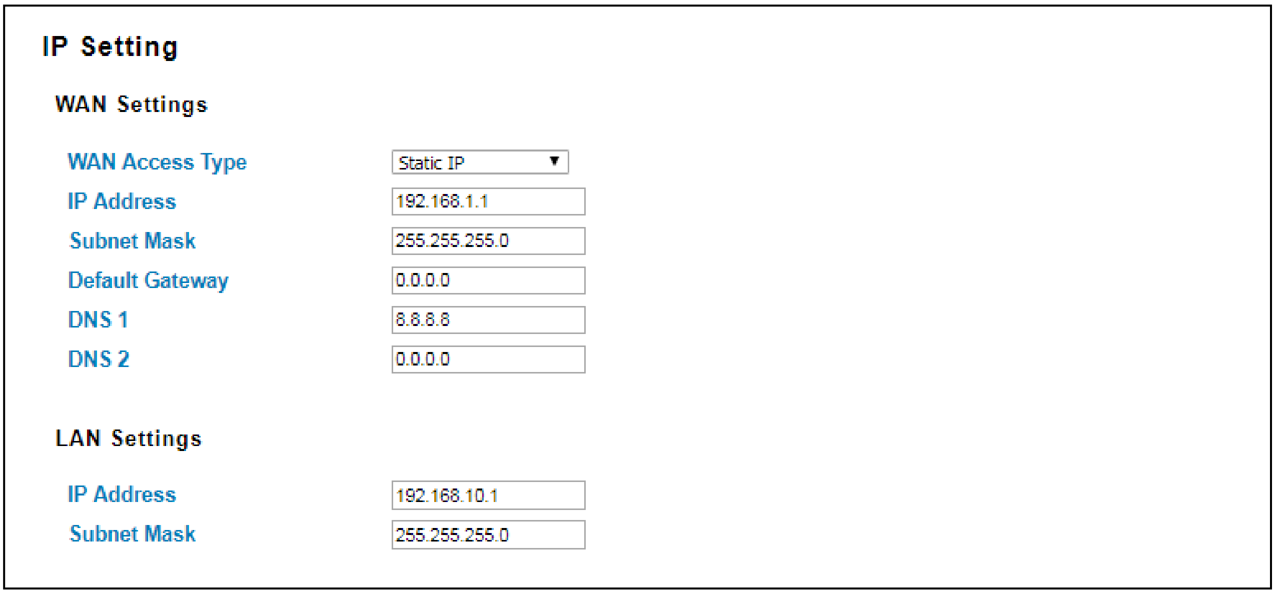
DNS 2 : 0.0.0.0

The description of the columns is as below:

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

DNS 2	Specifies the IP address of the DNS server 2 that used in user network.

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



IP Setting

WAN Settings

WAN Access Type: Static IP

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS 1: 8.8.8.8

DNS 2: 0.0.0.0

LAN Settings

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

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

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

TERMS	DESCRIPTION
WAN Access Type	User can select to DHCP Client or Static IP to activate the function. **DHCP Client:** Select DCHP Client to activate DHCP Client Function, no need to assign IP Address and received IP Address from DHCP Server. **Static IP:** Select Static IP to configure the IP configuration manually
IP Address	**Default: 192.168.1.1** Set up the IP address reserved by User network for User device. If DHCP Client function is enabled, no need to assign an IP address to device as it will be overwritten by DHCP server and shown here.
Subnet Mask	**Default: 255.255.255.0** Assign the subnet mask for the IP address here. If DHCP Client function is enabled, no needs to assign the subnet mask.
Gateway IP Address	**Default: 0.0.0.0.** Assign the gateway for the device here.
DNS 1	Specifies the IP address of the DNS server 1 that used in user network.

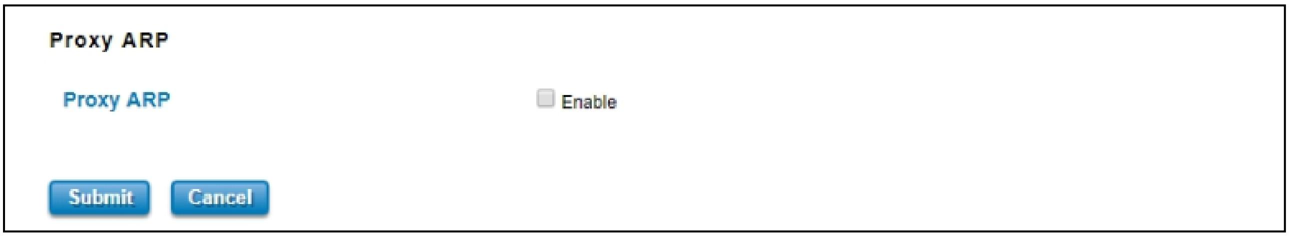
DNS 2	Specifies the IP address of the DNS server 2 that used in user network.

Proxy ARP

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

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

Below is the interface.



Proxy ARP

Proxy ARP ☐ Enable

Check the box to enable the function of Proxy ARP.

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

3.1.4 DATE AND TIME

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

The description of the columns is as below:

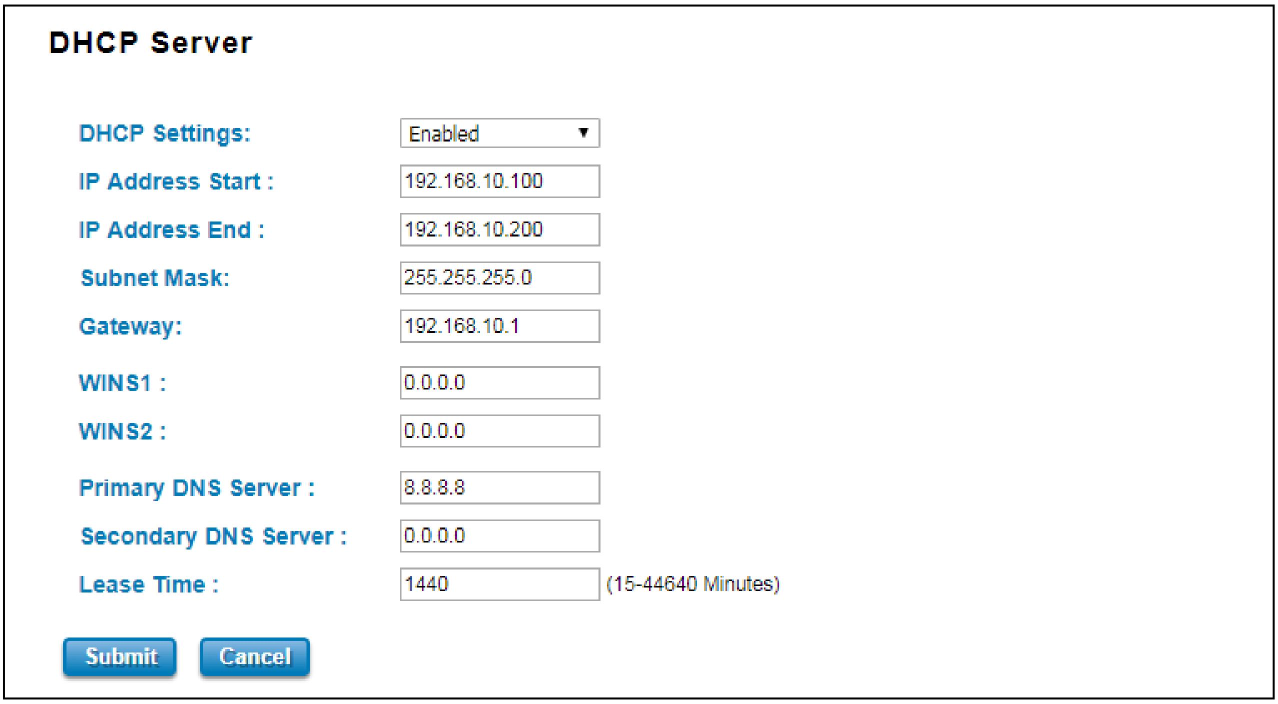
TERMS	DESCRIPTION
Current Time	User can configure time by input it manually. User also can click the **Get PC Time or Get Time from Cellular** to get the time setting. Get PC Time: get the time the PC Get Time from Cellular: get the time from the cellular network.
Time Zone	Choose the Time Zone section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

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

3.1.5 DHCP SERVER

DHCP Server Setting

AVCOMM 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



DHCP Server

DHCP Settings: Enabled

IP Address Start : 192.168.10.100

IP Address End : 192.168.10.200

Subnet Mask: 255.255.255.0

Gateway: 192.168.10.1

WINS1 : 0.0.0.0

WINS2 : 0.0.0.0

Primary DNS Server : 8.8.8.8

Secondary DNS Server : 0.0.0.0

Lease Time : 1440 (15-44640 Minutes)

The description of the columns is as below:

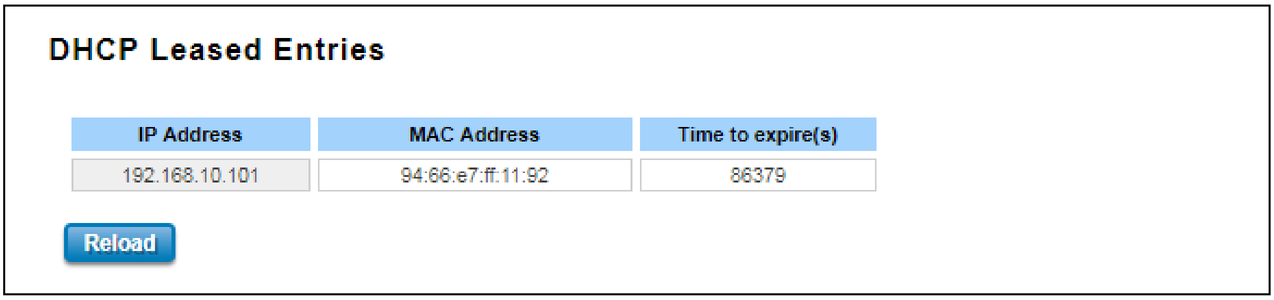
TERMS	DESCRIPTION
DHCP Setting	Select to **Enable** or **Disable** to activate and deactivate DHCP Server function.
IP Address Start	Assign the IP Address Start range.
IP Address End	Assign the IP Address End range.
Subnet Mask	**Default: 255.255.255.0** Assign the subnet mask for the IP address here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

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

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

DHCP Leased Entries

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



DHCP Leased Entries

IP Address	MAC Address	Time to expire(s)
192.168.10.101	94:66:e7:ff:11:92	86379

The description of the columns is as below:

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

3.2 ETHERNET PORT

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

Following items are included in this group:

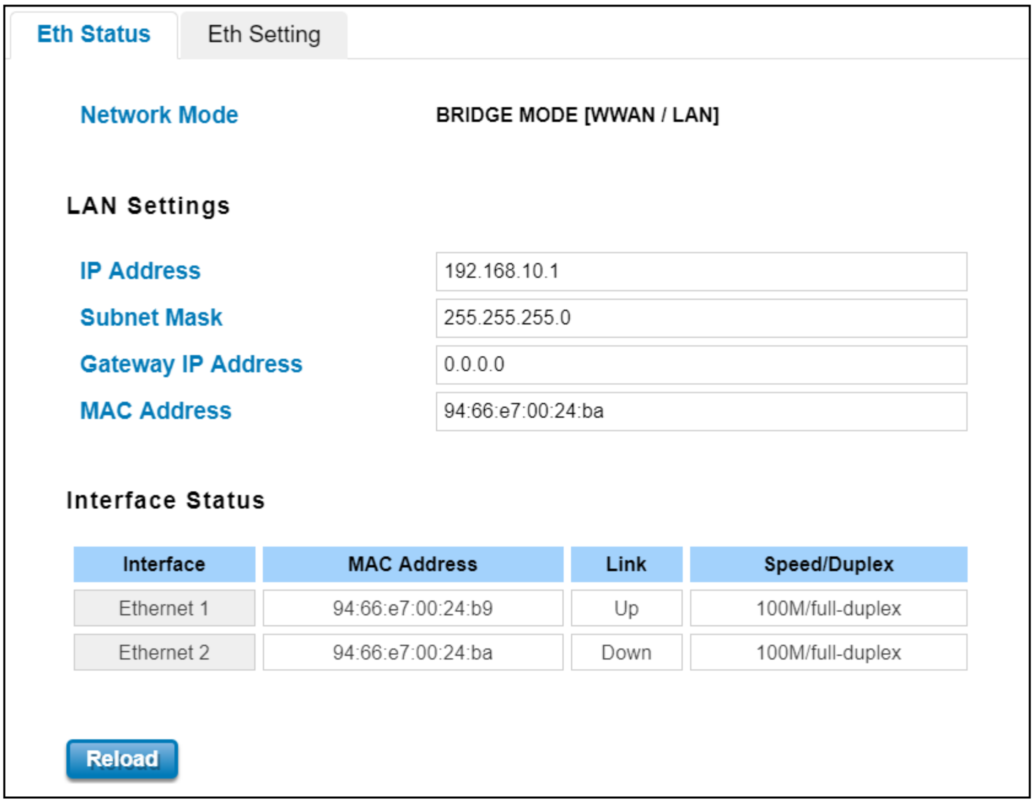
3.2.1 Ethernet Status

3.2.2 Ethernet Setting

3.2.3 Traffic Control

3.2.1 ETHERNET STATUS

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



Network Mode BRIDGE MODE [WWAN / LAN]

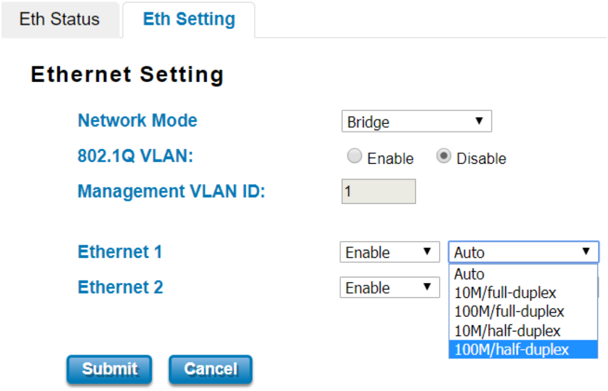
LAN Settings

IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
MAC Address	94:66:e7:00:24:ba

Interface Status

Interface	MAC Address	Link	Speed/Duplex
Ethernet 1	94:66:e7:00:24:b9	Up	100M/full-duplex
Ethernet 2	94:66:e7:00:24:ba	Down	100M/full-duplex

The description of the columns is as below:

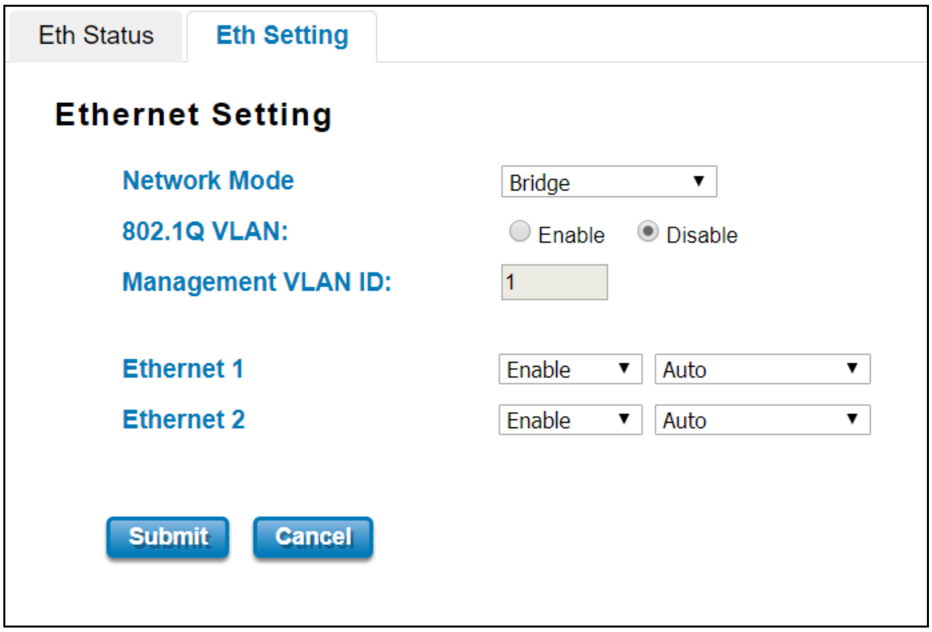
TERMS	DESCRIPTION
Network Mode	Shows network mode from the router **(Bridge or Router)**
IP Address	Display the IP address reserved by User network for User router
Subnet Mask	Display the subnet mask for the IP address.
Gateway IP Address	Display the gateway that assigned to the router.
MAC Address	Display the hardware's MAC Address that assigned by the manufacturer.
Interface	Display the Ethernet interface
MAC Address	Display the port MAC Address
Link	Display the Ethernet status, whether it is Link Up or Link Down.
Speed/Duplex	**Default: N/A** Show the Speed/Duplex for each port, such as 10 full,10 half,100 full,100 half mode for **Ethernet Port 1~2**  Ethernet Setting Network Mode: Bridge 802.1Q VLAN: ○ Enable ● Disable Management VLAN ID: 1 Ethernet 1: Enable, Auto Ethernet 2: Enable Auto / 10M/full-duplex / 100M/full-duplex / 10M/half-duplex / 100M/half-duplex Submit Cancel

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

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

3.2.2 ETHERNET SETTING

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



Ethernet Setting

Network Mode: Bridge

802.1Q VLAN: ○ Enable ● Disable

Management VLAN ID: 1

Ethernet 1: Enable, Auto

Ethernet 2: Enable, Auto

The description of the Ethernet Setting page is as below:

TERMS	DESCRIPTION
Network Mode	**Default: Bridge** Select Bridge mode and Router mode depends on the application. Bridge mode and Router mode have the same setting interface. When the Router mode is selected, then the device will change to router mode and the interface for port 1 would be WAN interface and port 2 would be LAN interface.
802.1Q VLAN	**Default: Disable** Choose enable to activate the function. *The feature is only applied for management Vlan in current firmware.
Management VLAN	**Default: 1** The switch supports management VLAN. The management VLAN ID is the VLAN ID of the CPU interface so that only member ports of the management VLAN can ping and access the switch. Note: After enabled the management VLAN ID, please note that only the device within the same VLAN can access the router's management interface.
Ethernet 1 ~ 2	**Default: Enable** **Default: Auto / Auto-Negotiation** Configure the Speed/Duplex of the port Ethernet 1 ~ 2. Users can set the bandwidth

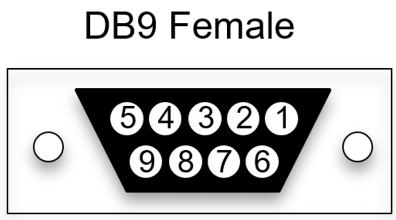
	of each port as Auto-negotiation, 100 full, 100 half, 10 full, 10 half mode.

After finishing configure the setting, click on **Submit** to apply the configuration. Click “**Save -> Save to Flash”** to permanently save the configuration.

3.3 SERIAL

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

Below is the pin assignment



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

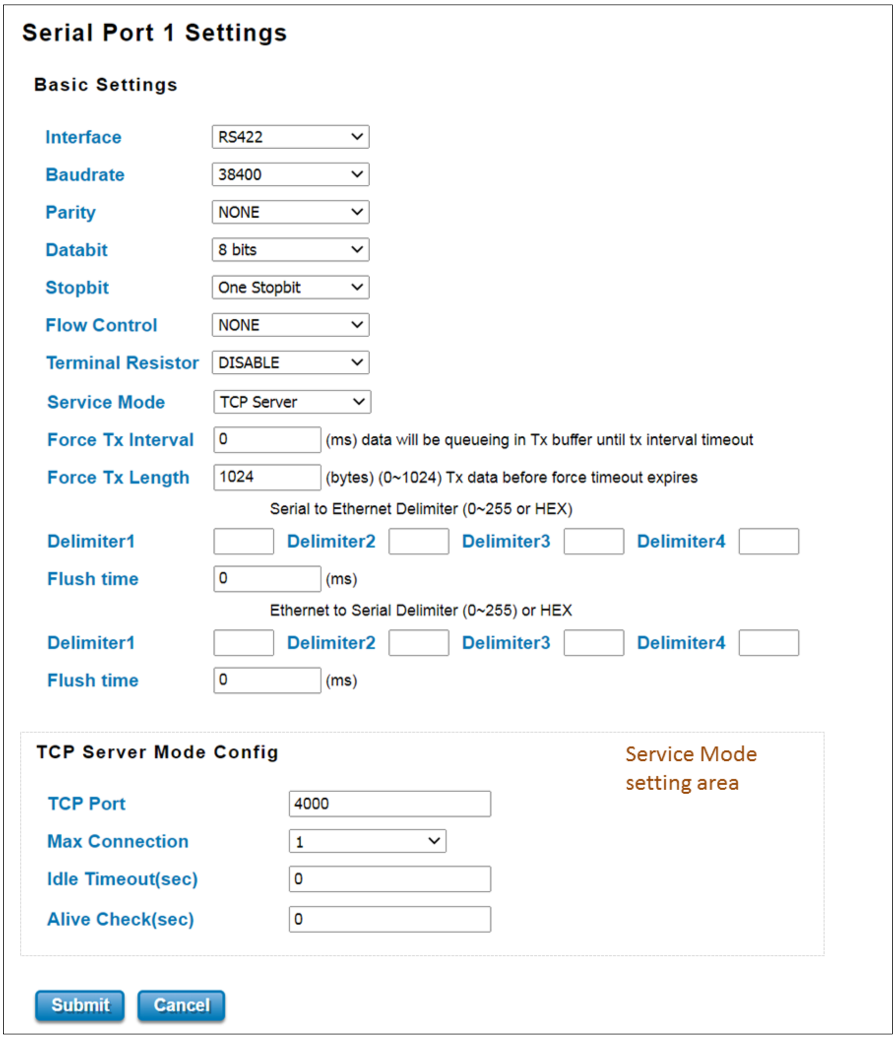
RS-232 is the most common serial interface and used to ship as a standard component on most Windows-compatible desktop computers. Now it is more common to use RS-232 over USB using a converter. RS-232 only allows for one transmitter and one receiver on each line. RS-232 also uses a Full-Duplex transmission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

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

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

Serial

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



Serial Port 1 Settings

Basic Settings

Interface	RS422
Baudrate	38400
Parity	NONE
Databit	8 bits
Stopbit	One Stopbit
Flow Control	NONE
Terminal Resistor	DISABLE
Service Mode	TCP Server
Force Tx Interval	0 (ms) data will be queueing in Tx buffer until tx interval timeout
Force Tx Length	1024 (bytes) (0~1024) Tx data before force timeout expires

Serial to Ethernet Delimiter (0~255 or HEX)

Delimiter1 ____ Delimiter2 ____ Delimiter3 ____ Delimiter4 ____

Flush time 0 (ms)

Ethernet to Serial Delimiter (0~255) or HEX

Delimiter1 ____ Delimiter2 ____ Delimiter3 ____ Delimiter4 ____

Flush time 0 (ms)

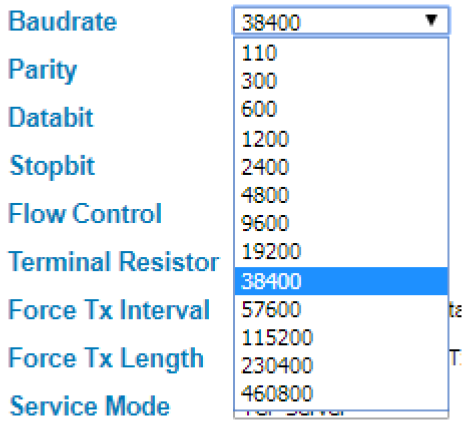
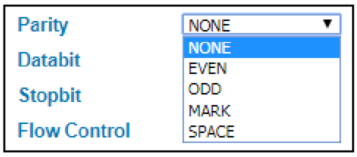
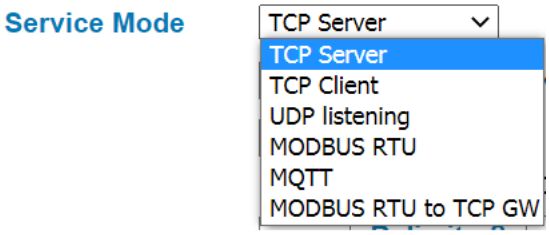
TCP Server Mode Config

Service Mode setting area

TCP Port	4000
Max Connection	1
Idle Timeout(sec)	0
Alive Check(sec)	0

The description of the columns is as below:

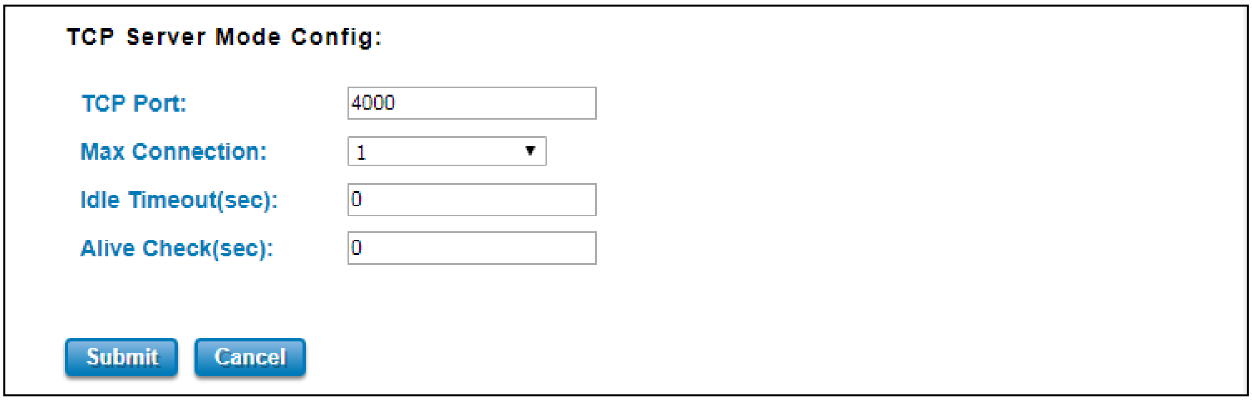
TERMS	DESCRIPTION
Interface	**Default : RS422** Choose and change the interface type from the drop down list. The serial port supports the RS232, RS422, RS485-2w, and RS485-4w.
Baudrate	**Default: 38400** Serial baud rate, a speed measurement of communication. It indicates the number of bit transfers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

	 Baudrate Parity Databit Stopbit Flow Control Terminal Resistor Force Tx Interval Force Tx Length Service Mode 38400 110 300 600 1200 2400 4800 9600 19200 38400 57600 115200 230400 460800
Parity	**Default: NONE** Set parity bit of serial data.  Parity Databit Stopbit Flow Control NONE NONE EVEN ODD MARK SPACE For even and odd parity, the serial port will set the parity bit (the last bit after the data bits) to a value to ensure that the transmission has an even or odd number of logic high bits. Mark and space parity does not actually check the data bits, but simply sets the parity bit high for marked parity or low for spaced parity.
Databit	**Default: 8 bits** Indicates the number of bits in a transmitted data package.
Stopbit	**Default: One Stopbit** The stop bit follows the data and parity bits in serial communication. It indicates the end of transmission.
Flow Control	**Default: NONE** Flow control manages data flow between devices in a network to ensure it is processed efficiently. Too much data arriving before a device is prepared to manage it causes lost or retransmitted data.
Terminal Resistor	**Default: Disable** Enable to prevent serial signal reflection.
Service Mode	 Service Mode TCP Server TCP Server TCP Client UDP listening MODBUS RTU MQTT MODBUS RTU to TCP GW You can select the "Service" mode, TCP Server, TCP Client, UDP listening, Modbus RTU, MQTT or Modbus RTU to TCP GW here and change the corresponding settings at the bottom of this page.
Force TX Interval	**Default: 0 (ms)**

	Force TX interval time is to specify the timeout when no data has been transmitted and queue data before the time interval is expired.
Force TX Length	**Default: 1024 (bytes)** To specify the length of the data before Force timeout expires.
Serial to Ethernet	**Delimiter**: User can define max. 4 delimiters (0~255, Hex) for each way. The data will be held until Flush Time is expired. 0 means disable. The factory default is 0. **Flush Time**: The received data will be queued in the buffer until all the delimiters are matched. When the Flush Time is expired the data will be sent.
Ethernet to Serial	**Delimiter**: User can define max. 4 delimiters (0~255, Hex) for each way. The data will be held until Flush Time is expired. 0 means disable. The factory default is 0. **Flush Time**: The received data will be queued in the buffer until all the delimiters are matched. When the Flush Time is expired the data will be sent.

The other section from this Serial page is corresponding Service Mode Configuration.

This page allows user to configure the basic settings of **TCP Server** Mode.



TCP Server Mode Config:

TCP Port: 4000

Max Connection: 1

Idle Timeout(sec): 0

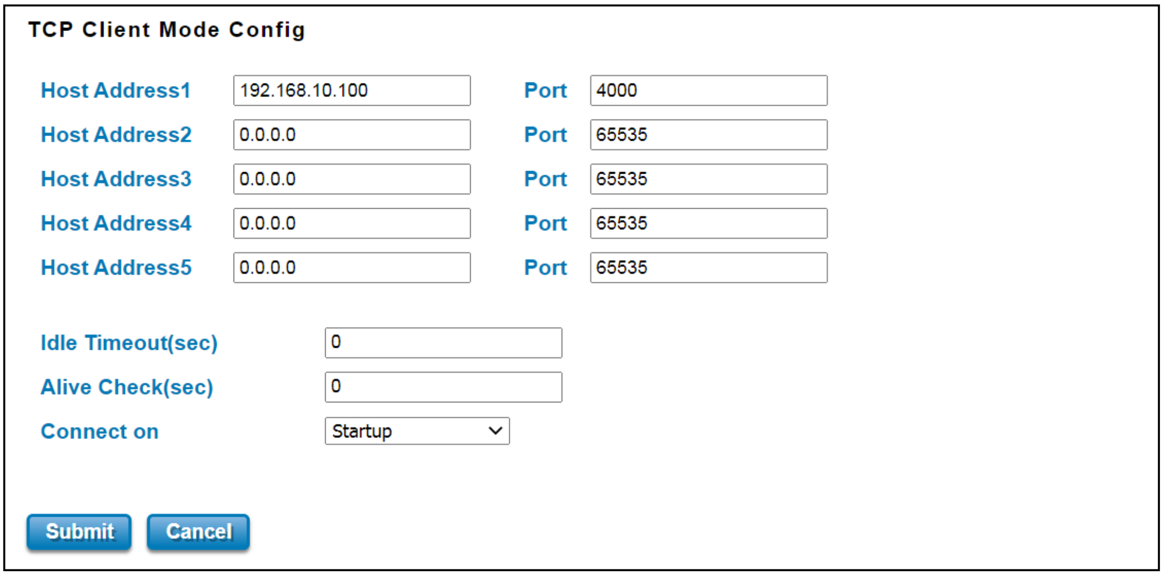
Alive Check(sec): 0

The description of the columns is as below:

TERMS	DESCRIPTION
TCP Port	**Default: 4000** 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.

This page allows user to configure the basic settings of **TCP Client** Mode.



TCP Client Mode Config

Host Address1	192.168.10.100	Port	4000
Host Address2	0.0.0.0	Port	65535
Host Address3	0.0.0.0	Port	65535
Host Address4	0.0.0.0	Port	65535
Host Address5	0.0.0.0	Port	65535

Idle Timeout(sec): 0

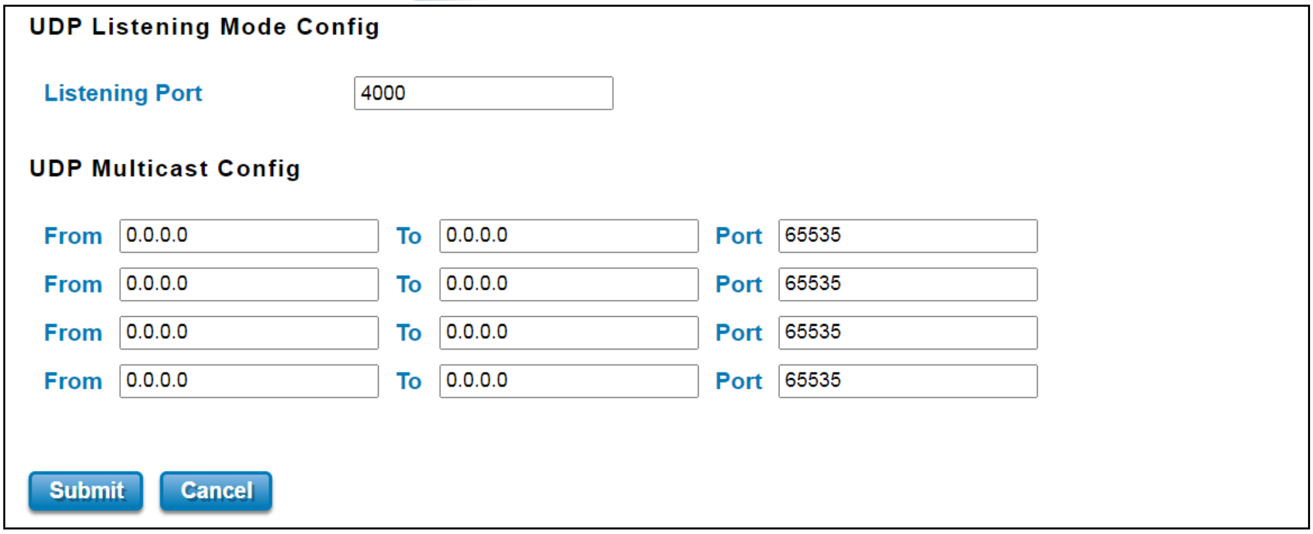
Alive Check(sec): 0

Connect on: Startup

The description of the columns is as below:

TERMS	DESCRIPTION
Host Address	Type the target host address here.
TCP Port	Assign the available TCP port number according to the TCP server. The port number of TCP Server and TCP Client should be the same.
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.
Connect on	Select connect on "**Startup**" or "**Any Character**" occurs.

This page allows user to configure the basic settings of **UDP Listening** Mode.



UDP Listening Mode Config

Listening Port: 4000

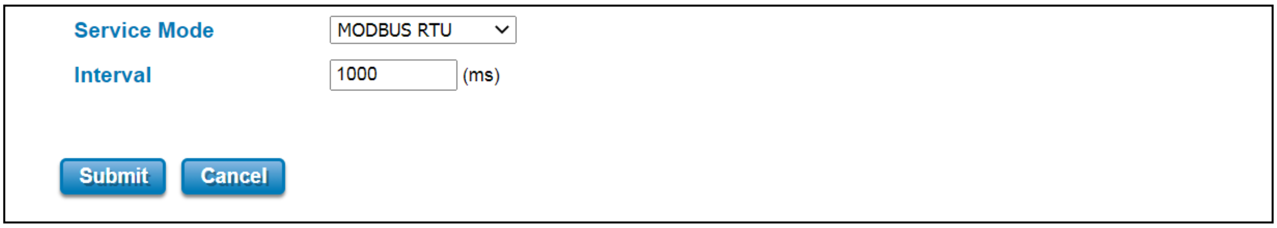
UDP Multicast Config

From	0.0.0.0	To	0.0.0.0	Port	65535
From	0.0.0.0	To	0.0.0.0	Port	65535
From	0.0.0.0	To	0.0.0.0	Port	65535
From	0.0.0.0	To	0.0.0.0	Port	65535

The description of the columns is as below:

TERMS	DESCRIPTION
Listening Port	Default: 4000 Type the listening port of the UDP listening state.
Host Address	Type the target range host addresses “From…To…”.
TCP Port	Assign the available USP listening port number. The port number of both ends should be the same.

This page allows user to configure the basic settings of **Modbus RTU** Mode.

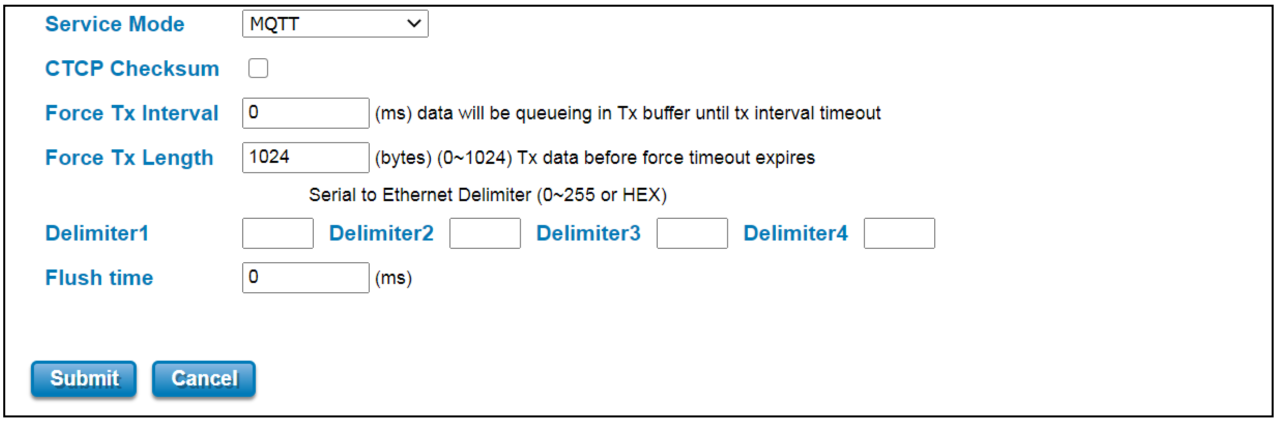


Service Mode: MODBUS RTU

Interval: 1000 (ms)

You Can configure the polling Interval here. The time unit is in milli-second.

This page allows user to configure the basic settings of **MQTT** Mode.



Service Mode: MQTT

CTCP Checksum: □

Force Tx Interval: 0 (ms) data will be queueing in Tx buffer until tx interval timeout

Force Tx Length: 1024 (bytes) (0~1024) Tx data before force timeout expires

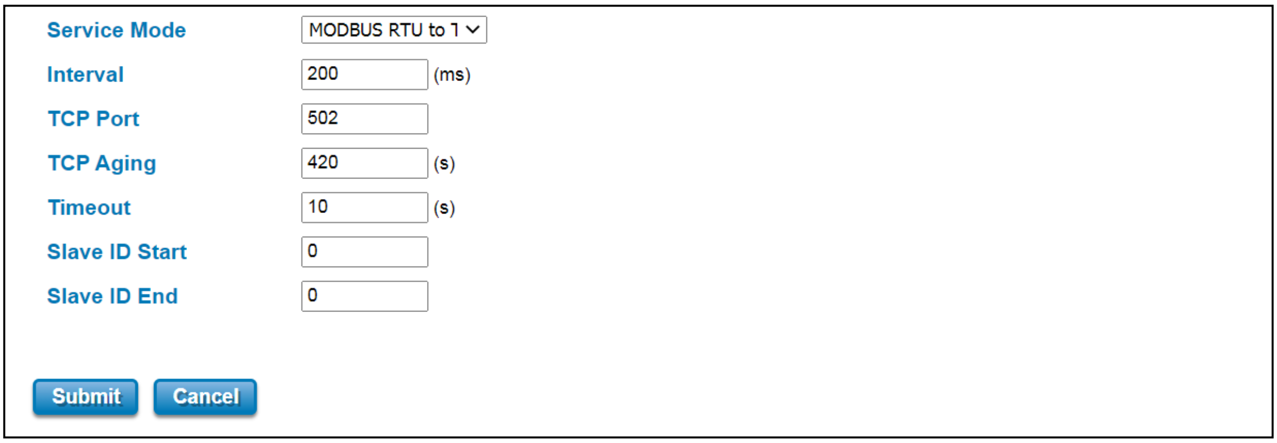
Serial to Ethernet Delimiter (0~255 or HEX)

Delimiter1: Delimiter2: Delimiter3: Delimiter4:

Flush time: 0 (ms)

The meaning of the “Force TX Interval”, “Force TX Length”, “Delimiter” and “Flush Time” are the same as other service mode.

This page allows user to configure the basic settings of Modbus RTU to TCP GW Mode.



Service Mode	MODBUS RTU to T
Interval	200 (ms)
TCP Port	502
TCP Aging	420 (s)
Timeout	10 (s)
Slave ID Start	0
Slave ID End	0

The description of the columns is as below:

TERMS	DESCRIPTION
Interval	The time interval of the transmit.
TCP Port	Assign the available TCP port number according to the TCP server. The port number of TCP Server and TCP Client should be the same.
TCP Aging	The TCP aging time of the transmitting.
Timeout	The Timeout time of the transmitting.
Slave ID Start	The start slave ID once you connect couple slave serial devices.
Slave ID End	The End slave ID once you connect couple slave serial devices.

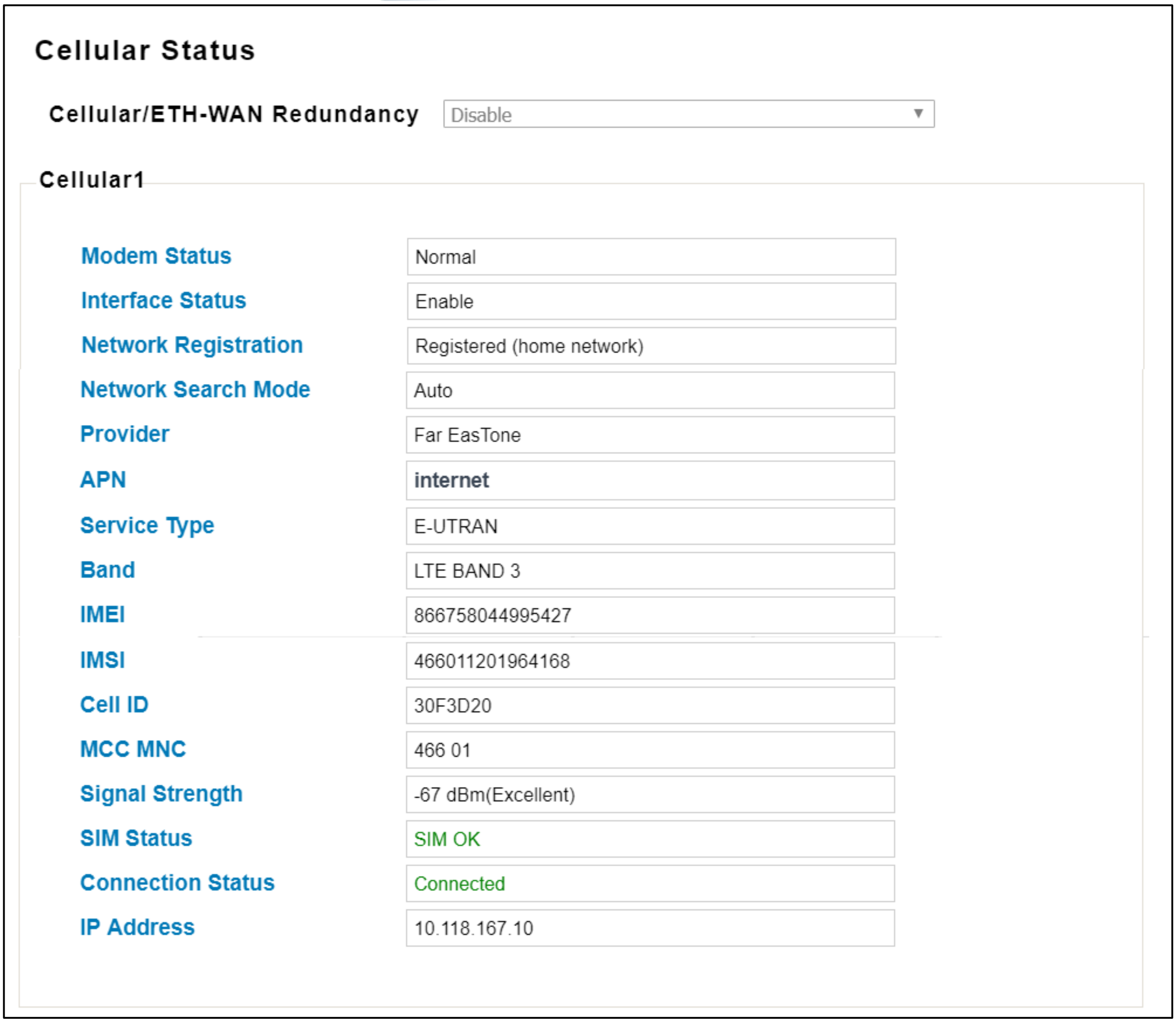
After finishing configure any of the above setting, click on **"Submit"** to apply the configuration. Click "**Save -> Save to Flash**" to permanently save the configuration.

3.4 CELLULAR

This Cellular page provides the Cellular Status; configure Cellular Setting and configure SIM Setting.

3.4.1 CELLULAR STATUS

The figure below shows Cellular Status.



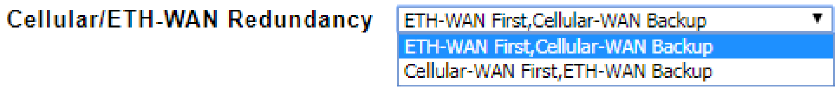
Cellular Status

Cellular/ETH-WAN Redundancy: Disable

Cellular1

Modem Status	Normal
Interface Status	Enable
Network Registration	Registered (home network)
Network Search Mode	Auto
Provider	Far EasTone
APN	internet
Service Type	E-UTRAN
Band	LTE BAND 3
IMEI	866758044995427
IMSI	466011201964168
Cell ID	30F3D20
MCC MNC	466 01
Signal Strength	-67 dBm(Excellent)
SIM Status	SIM OK
Connection Status	Connected
IP Address	10.118.167.10

The description of the columns is as below:

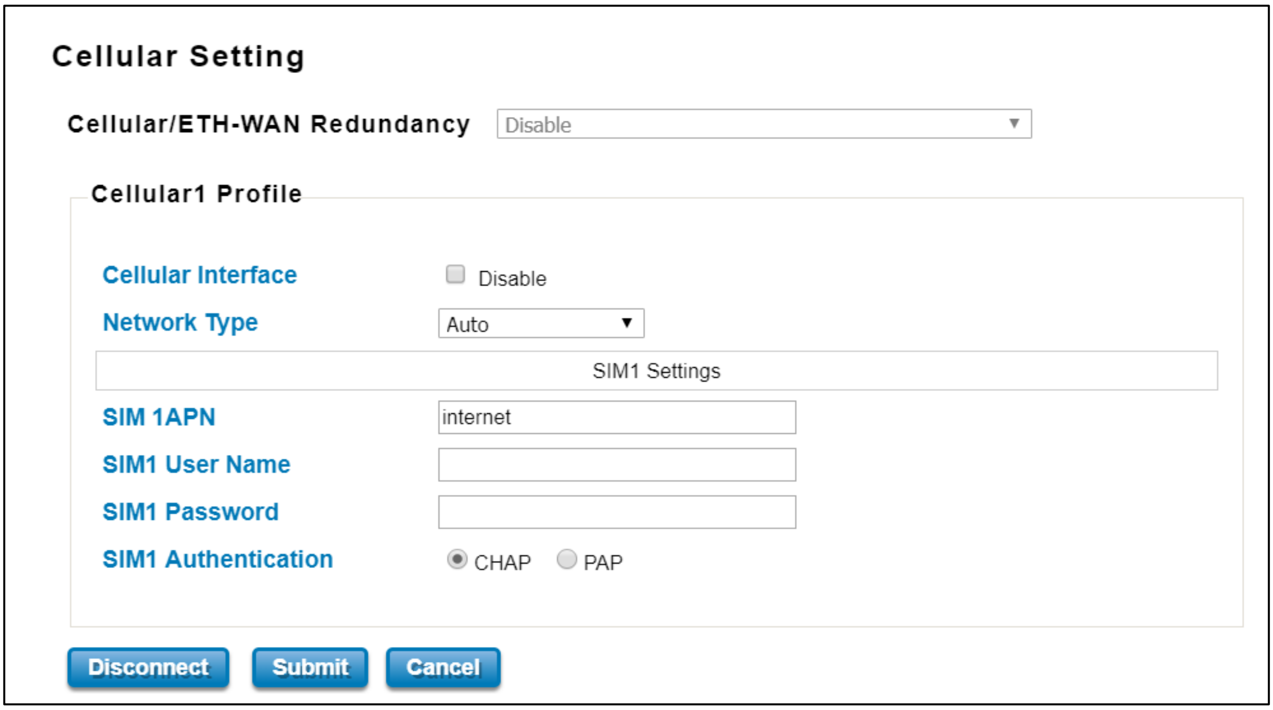
TERMS	DESCRIPTION
Cellular/ETH.WAN Redundancy	**Default: Disabled** User can choose the redundancy mode:  Cellular/ETH-WAN Redundancy: ETH-WAN First,Cellular-WAN Backup ETH-WAN First,Cellular-WAN Backup Cellular-WAN First,ETH-WAN Backup **ETH-WAN First, Cellular-WAN Backup**: by choosing this mode, the 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 Registration	Display the status of the network registration
Network Search Mode	Display the network search mode (Auto, 2G Only, 3G Only and LTE Only)
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)
IMSI	Display the International Mobile Subscriber Identity (IMSI)
Cell ID	Display the Cell Identity (CID)
MCC MNC	Display the Mobile Country Code (MCC) and Mobile Network Code (MNC)
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.

3.4.2 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, Network Type, SIM APN, User Name, Password and the Authentication mode.

The figure below is the interface of AP222



Cellular Setting

Cellular/ETH-WAN Redundancy: Disable

Cellular1 Profile

Cellular Interface: □ Disable

Network Type: Auto

SIM1 Settings

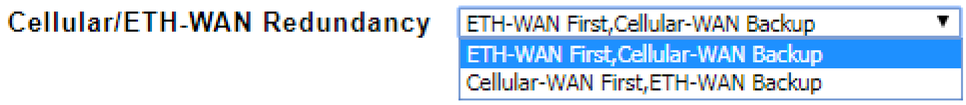
SIM 1APN: internet

SIM1 User Name:

SIM1 Password:

SIM1 Authentication: ● CHAP ○ PAP

The description of the columns is as below:

TERMS	DESCRIPTION
Cellular/ETH.WAN Redundancy	**Default: Disabled** User can choose the redundancy mode:  Cellular/ETH-WAN Redundancy: ETH-WAN First,Cellular-WAN Backup ETH-WAN First,Cellular-WAN Backup Cellular-WAN First,ETH-WAN Backup **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.
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 APN	Set the APN of the ISP.
SIM1 User Name	Set the User Name
SIM1 Password	Set the password.
SIM1 Authentication	Choose CHAP or PAP mode for the authentication mode. **CHAP**: Challenge Handshake Authentication Protocol, With CHAP, the authenticator (i.e. the server) sends a randomly generated ``challenge'' string to the client, along with its

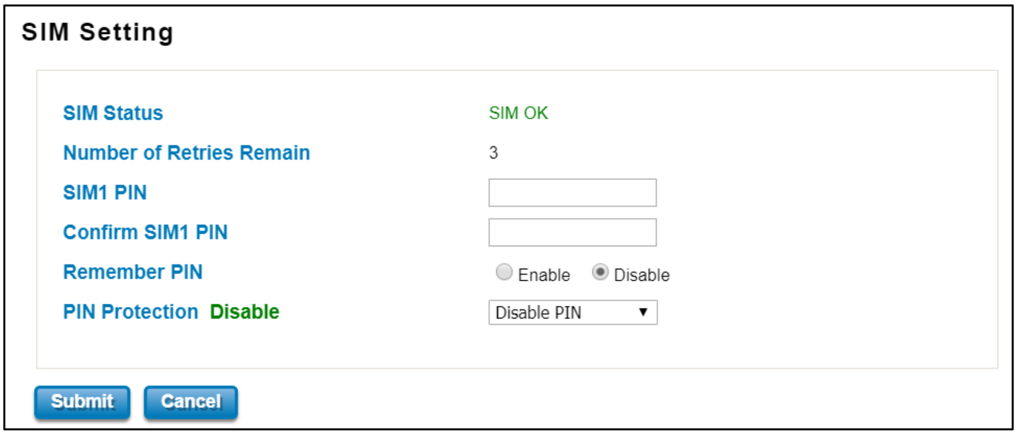
	hostname. **PAP**: Password Authentication Protocol, PAP works basically the same way as the normal login procedure. The authenticates itself by sending a user name and a password to the server

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

3.4.3 SIM SETTING

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

The figure below belongs to AP222:



SIM Setting

SIM Status	SIM OK
Number of Retries Remain	3
SIM1 PIN	
Confirm SIM1 PIN	
Remember PIN	○ Enable ● Disable
PIN Protection Disable	Disable PIN ▼

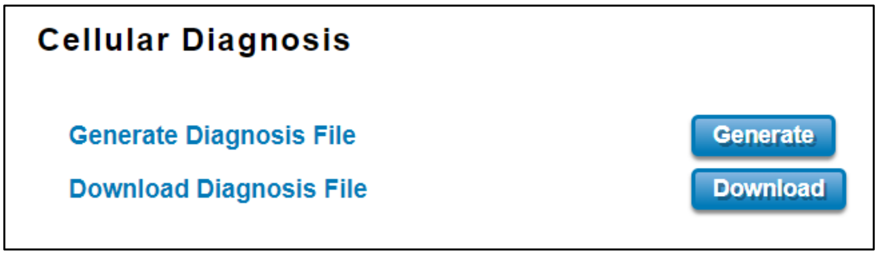
TERMS	DESCRIPTION
SIM Status	Show the installed SIM Status. **SIM OK:** The SIM card is okay to use. **SIM not inserted:** The SIM card is not inserted. **SIM PIN Locked:** The SIM card is locked due to PIN error. It may be caused by error typing PIN password many times. **WARNING:** SIM PUK Locked status 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 PIN	Enter new SIM1 PIN numbers
Confirm SIM1 PIN	Confirm the new SIM1 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.

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

3.4.4 Cellular Diag

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



Cellular Diagnosis

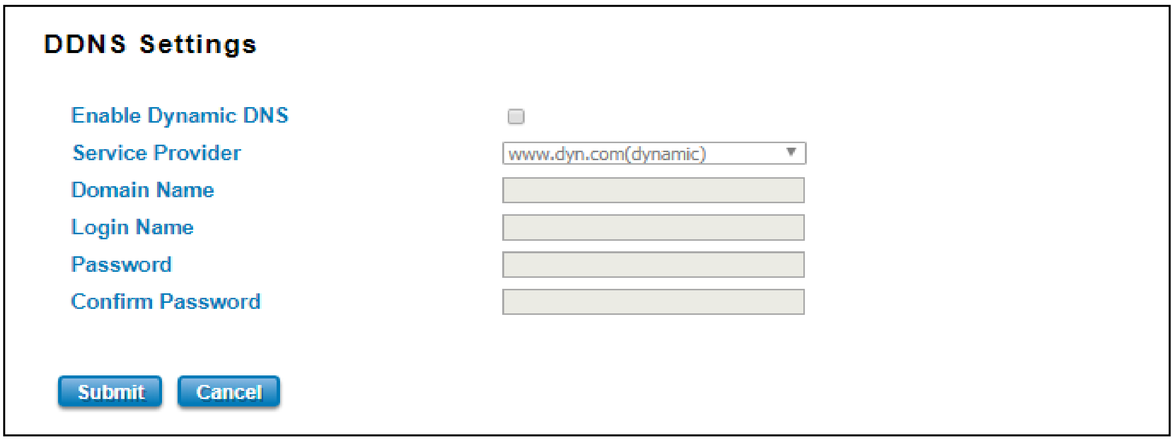
Generate Diagnosis File — Generate

Download Diagnosis File — Download

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

3.4.5 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.



DDNS Settings

Enable Dynamic DNS ☐

Service Provider: www.dyn.com(dynamic)

Domain Name

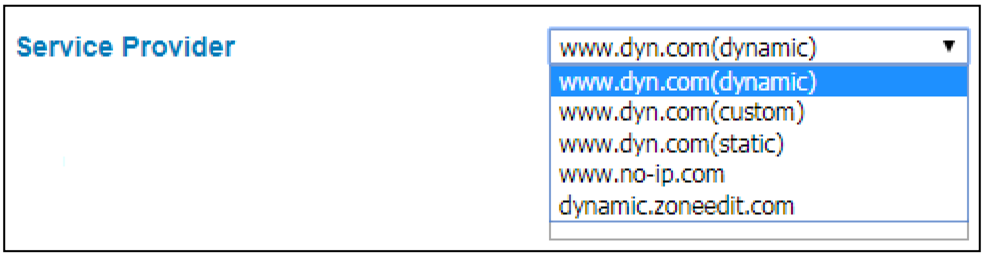
Login Name

Password

Confirm Password

Submit Cancel

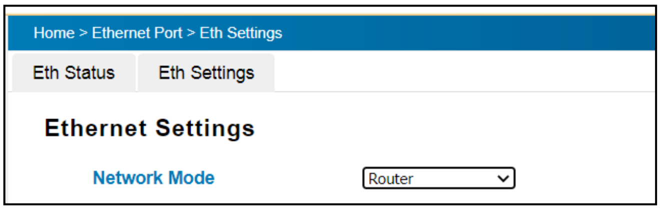
TERMS	DESCRIPTION
Enable Dynamic DNS	Check the box to enable the function
Service Provider	Select the Domain service provider from the list.

	 Service Provider: www.dyn.com(dynamic) www.dyn.com(dynamic) www.dyn.com(custom) www.dyn.com(static) www.no-ip.com dynamic.zoneedit.com
Domain Name	Enter the domain name
Login Name	Enter Login Name that used when applying the domain name
Password	Enter Password that used when applying the domain name
Confirm Password	Enter the Password once again to confirm.

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

3.4.5 Cellular/WAN Redundancy

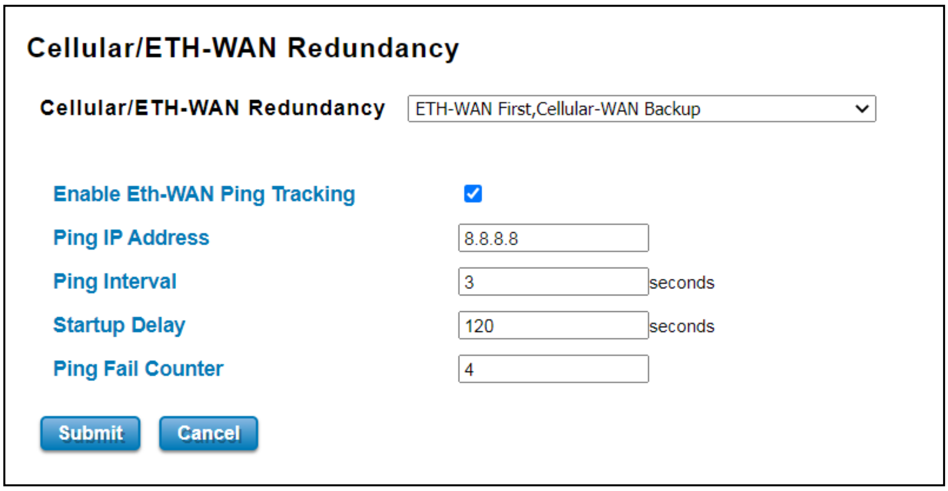
The feature allows user setup the WAN to Cellular redundancy while Ethernet-WAN port link down or unexpected failure, the cellular is activated automatically. Before enabled the feature, you should enabled the Ethernet Setting in Router mode, which means the two Ethernet ports are separated to different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



Ethernet Settings

Network Mode: Router

The Cellular/Eth-WAN Redundancy setup page:



Cellular/ETH-WAN Redundancy

Cellular/ETH-WAN Redundancy: ETH-WAN First,Cellular-WAN Backup

Enable Eth-WAN Ping Tracking: ☑

Ping IP Address: 8.8.8.8

Ping Interval: 3 seconds

Startup Delay: 120 seconds

Ping Fail Counter: 4

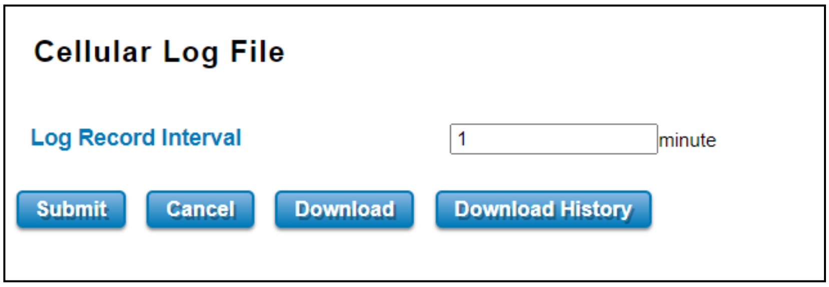
The description of the columns is as below:

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

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

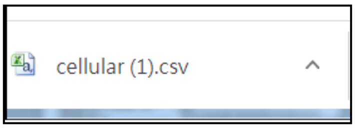
3.4.6 Save SD log

The feature allows the router to save the Cellular Diagnostic log to SD card, you can define how often to save the log by "Log Record Interval", you can also download the log file by click "Download".


Cellular Log File

Log Record Interval: 1 minute

After click "Download", you will see the "cellular(x).csv" in the below of the Web GUI.



3.4.7 SMS Remote Control

User can send the SMS message to reboot the router from the cellphone. The SMS message format is "**User Name, Password, reboot**". For example: "**admin, Admin@123, reboot**".

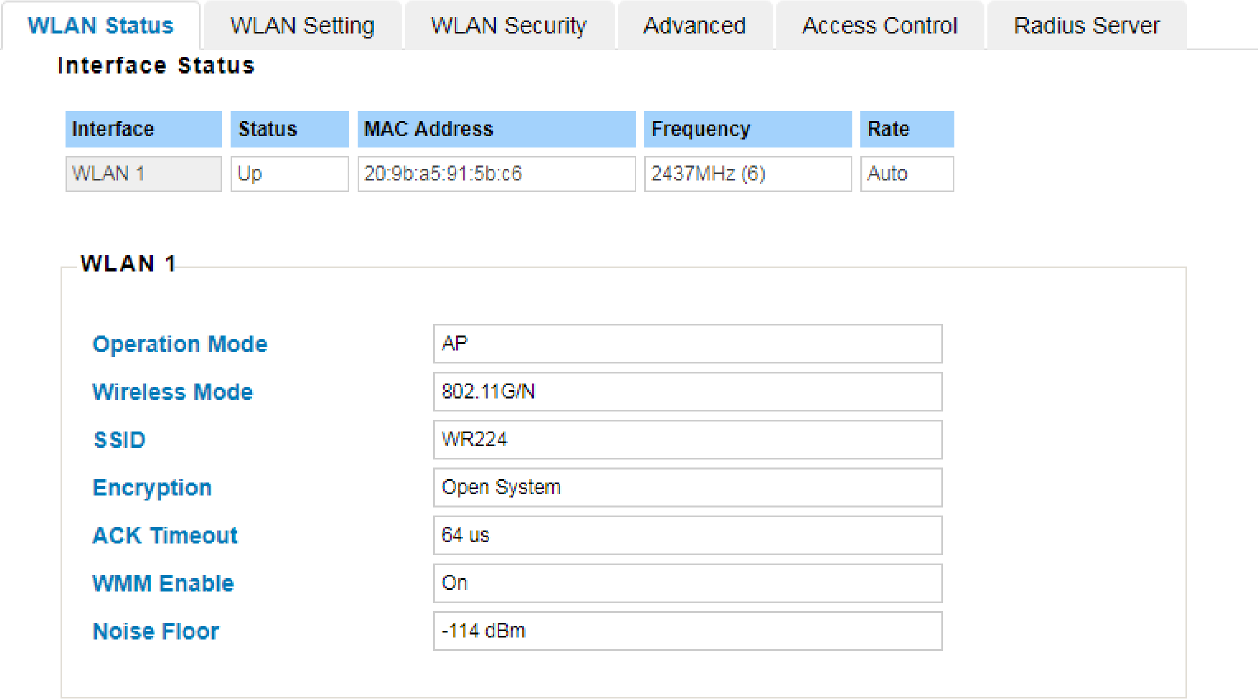
Note: The router support SMS message to reboot router currently, if you have other need, please contact our Sales/Service div., we can discuss this by project need.

3.5 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.

3.5.1 WLAN STATUS

The figure below shows the WLAN status.



Interface Status

Interface	Status	MAC Address	Frequency	Rate
WLAN 1	Up	20:9b:a5:91:5b:c6	2437MHz (6)	Auto

WLAN 1

Operation Mode	AP
Wireless Mode	802.11G/N
SSID	WR224
Encryption	Open System
ACK Timeout	64 us
WMM Enable	On
Noise Floor	-114 dBm

The description of the columns is as below:

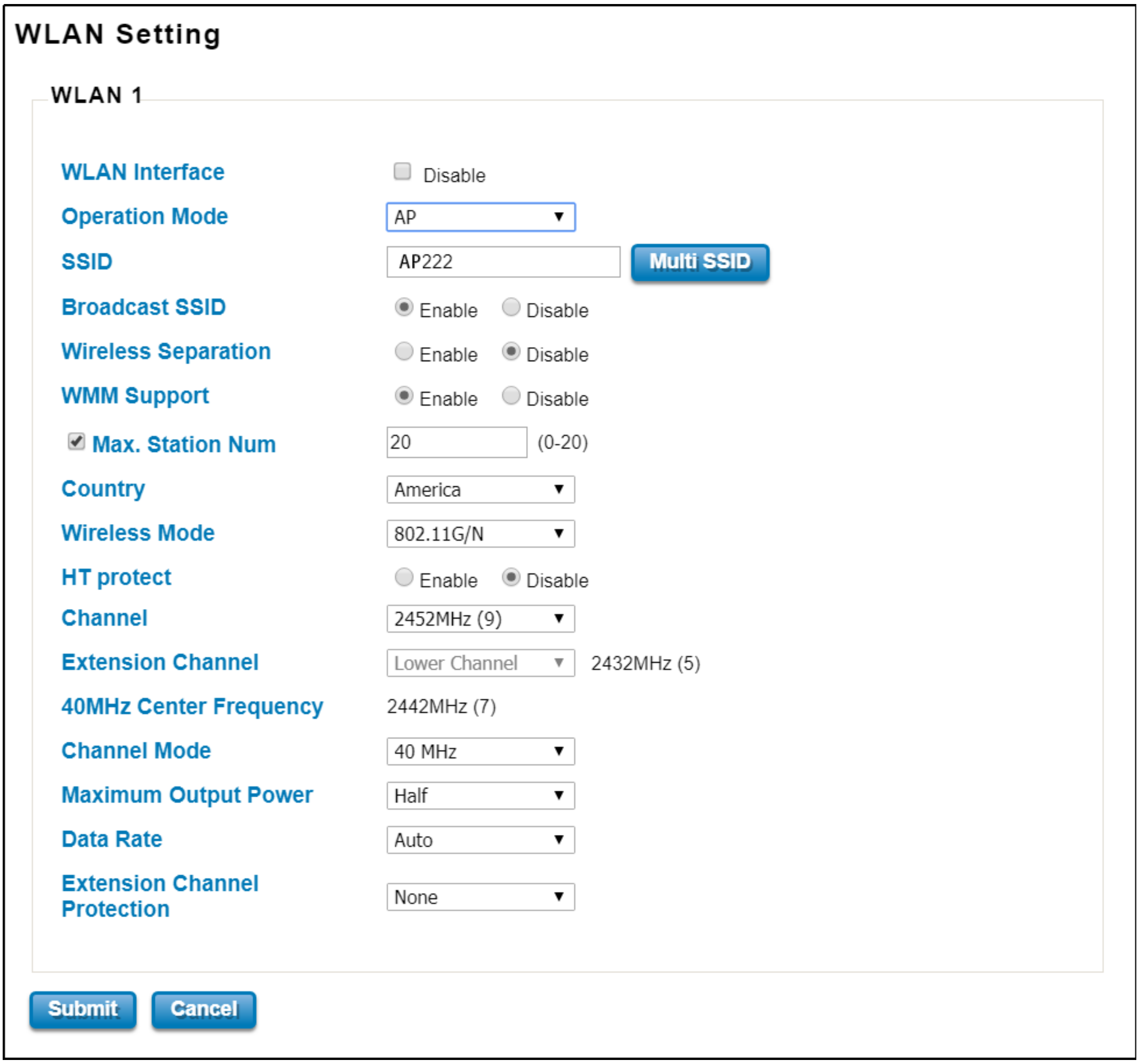
TERMS	DESCRIPTION
Operation Mode	Display the current operating modes on the device
Wireless Mode	Display the current wireless mode
SSID	Display the primary name of the SSID
Encryption	Display the encryption mode.
ACK Timeout	The ACK timeout time
WMM Enable	Display the status of the WMM support.
Noise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

3.5.2 WLAN SETTING

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

AP

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



WLAN Setting

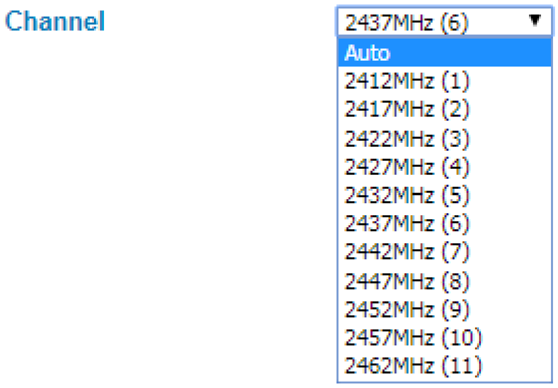
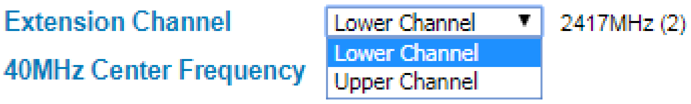
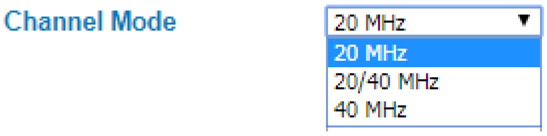
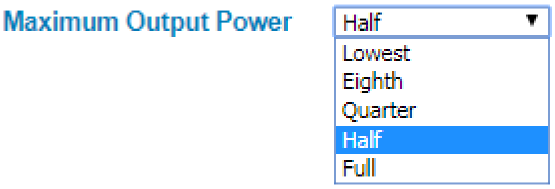
WLAN 1

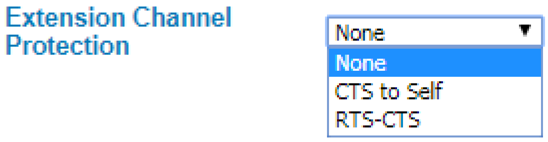
WLAN Interface	□ Disable
Operation Mode	AP
SSID	AP222 [Multi SSID]
Broadcast SSID	● Enable ○ Disable
Wireless Separation	○ Enable ● Disable
WMM Support	● Enable ○ Disable
☑ Max. Station Num	20 (0-20)
Country	America
Wireless Mode	802.11G/N
HT protect	○ Enable ● Disable
Channel	2452MHz (9)
Extension Channel	Lower Channel 2432MHz (5)
40MHz Center Frequency	2442MHz (7)
Channel Mode	40 MHz
Maximum Output Power	Half
Data Rate	Auto
Extension Channel Protection	None

The description of the columns is as below:

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

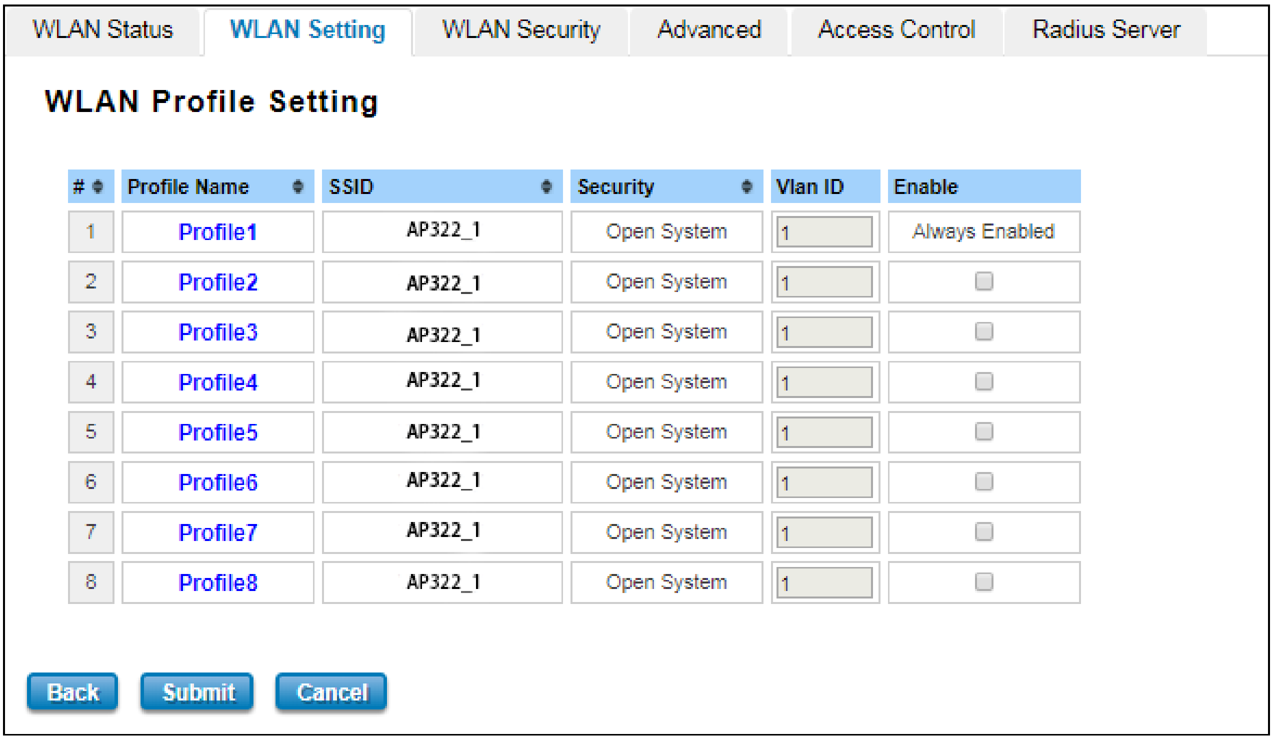
Wireless Separation	**Default: Disable** Under the AP mode, enable it to prevent one wireless device from directly communicating with another on the same AP
WMM Support	**Default: Enable** A subset of the WLAN specification that enhances quality of service (QoS) on a network by prioritizing data packets onto four categories. Ranging from highest priority to lowest, these categories are: ● **Voice**: Giving voice packets the highest priority enables concurrent Voice over IP (VoIP) calls with minimal latency and the highest quality possible. ● **Video**: By placing video packets in the second tier, WMM prioritizes it over all other data traffic. ● **Best effort**: Best effort data packets consist of those originating from legacy devices or from applications or devices that lack QoS standards. **Background**: Background priority encompasses file downloads, print jobs and other traffic that does not suffer from increased latency.
Max Station Number	**Default: 20 (0-20)** Set the maximum number of station that can communicate with the access point.
Country	Select your country or region
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has a different configuration. For each wireless mode, it has the specific frequency and it has different basic setting.. Wireless Mode 802.11G/N 802.11B Only 802.11G Only 802.11G/N
HT Protect	**Default: Disabled** Select Enabled to activate the High Throughput protect to ensure HT transmission with MAC mechanism.
Channel	**Default: 2437MHz (6)** Select the proper channel, each country has different band user may select the channel based on the situation. Or select auto to automatically set the channel.

	 Channel: 2437MHz (6) Auto 2412MHz (1) 2417MHz (2) 2422MHz (3) 2427MHz (4) 2432MHz (5) 2437MHz (6) 2442MHz (7) 2447MHz (8) 2452MHz (9) 2457MHz (10) 2462MHz (11)
Extension Channel	**Default: Lower Channel 2417MHz (2)**  Extension Channel: Lower Channel 2417MHz (2) 40MHz Center Frequency This option would be appeared when user select the Channel Mode to 20/40MHz or 40MHz. To put range for the frequency, it provides the Lower Channel (2417MHz (2)) with the 40MHz center frequency is 2427MHz (4) and Upper Channel (2457MHz (10)) with the 40MHz center frequency is 2447MHz (8).
Channel Mode	**Default: 20MHz**  Channel Mode: 20 MHz There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user select 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequency, and for the 40MHz, it provides bigger data rate and received the 40MHz frequency. But basically, if the transmission happened between the AP and the client, both AP and client can have the negotiation phase about the frequency.
Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna.  Maximum Output Power: Half
Data Rate	**Default: Auto** Select the specific data rate in order to control the transmission rate. **Auto** is preferred rate, the access point will automatically select the highest

	available rate to transmit. User may select the low rate when there is no great demand for transmission speed, for long distance transmission.
Extension Channel Protection	 Extension Channel Protection: None None CTS to Self RTS-CTS Select from the dropdown list option between **CTS-Self or RTS-CTS** to avoid conflict with other wireless network and to improve the ability of the device to catch all the wireless transmissions. By activating this function it may decrease wireless network performance.

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

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



WLAN Profile Setting

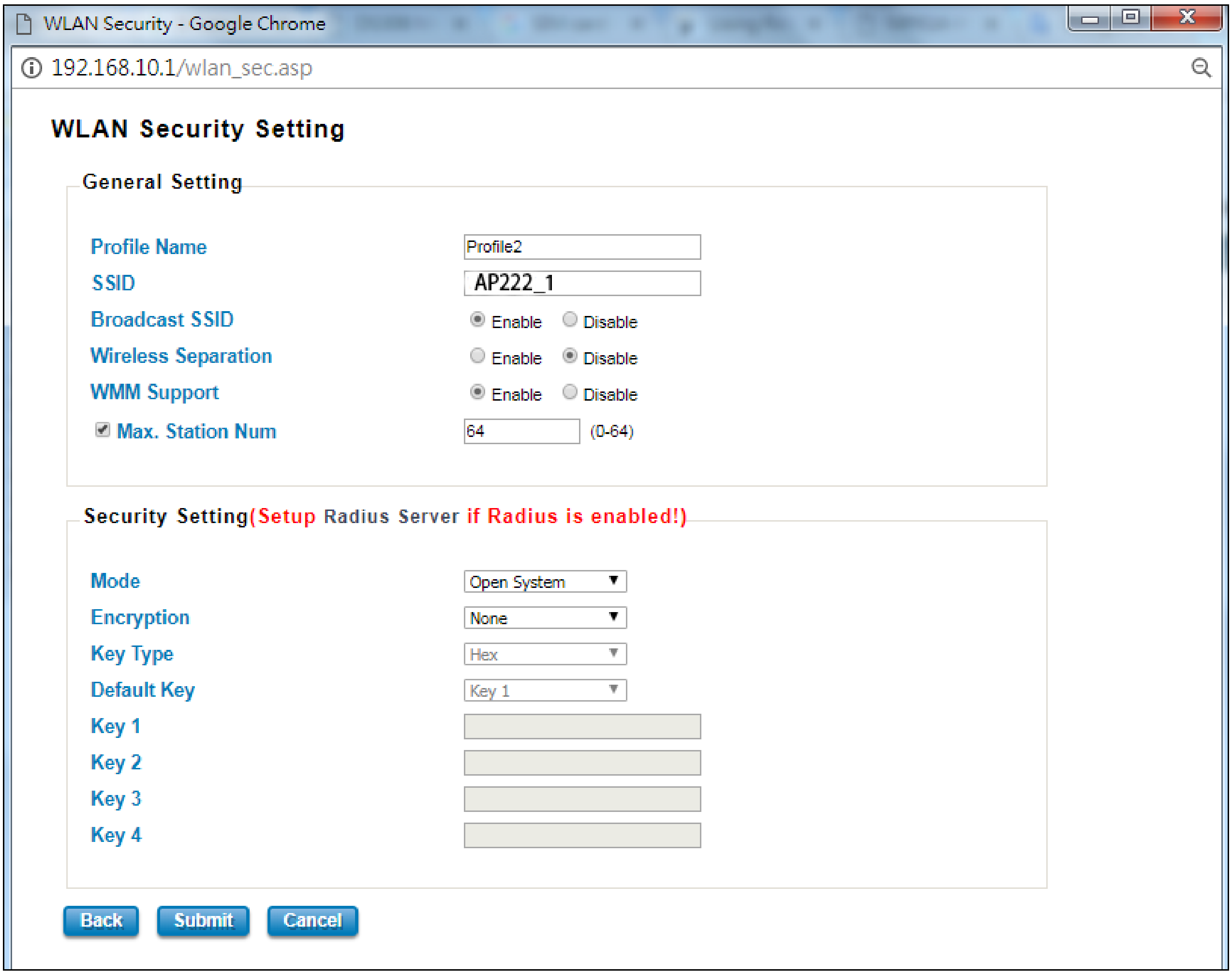
#	Profile Name	SSID	Security	Vlan ID	Enable
1	Profile1	AP322_1	Open System	1	Always Enabled
2	Profile2	AP322_1	Open System	1	□
3	Profile3	AP322_1	Open System	1	□
4	Profile4	AP322_1	Open System	1	□
5	Profile5	AP322_1	Open System	1	□
6	Profile6	AP322_1	Open System	1	□
7	Profile7	AP322_1	Open System	1	□
8	Profile8	AP322_1	Open System	1	□

The description of the column is as below:

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

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

The Multi SSID section shows the configuration page where the Profile1 always enabled. In this section, user may configure each Profile by check the box to enable the Profile and then click the profile name to open the configuration page for specific Profile. The figure below is the pop-up WLAN Security configuration page for each Profile. In this configuration page, user can configure the AP profile, divide the AP connection and set the security setting by put the encryption mode and set the key or password to access the AP. Refers to the WLAN Security Section for more description (3.5.3).



WLAN Security - Google Chrome

192.168.10.1/wlan_sec.asp

WLAN Security Setting

General Setting

Profile Name	Profile2
SSID	AP222_1
Broadcast SSID	● Enable ○ Disable
Wireless Separation	○ Enable ● Disable
WMM Support	● Enable ○ Disable
☑ Max. Station Num	64 (0-64)

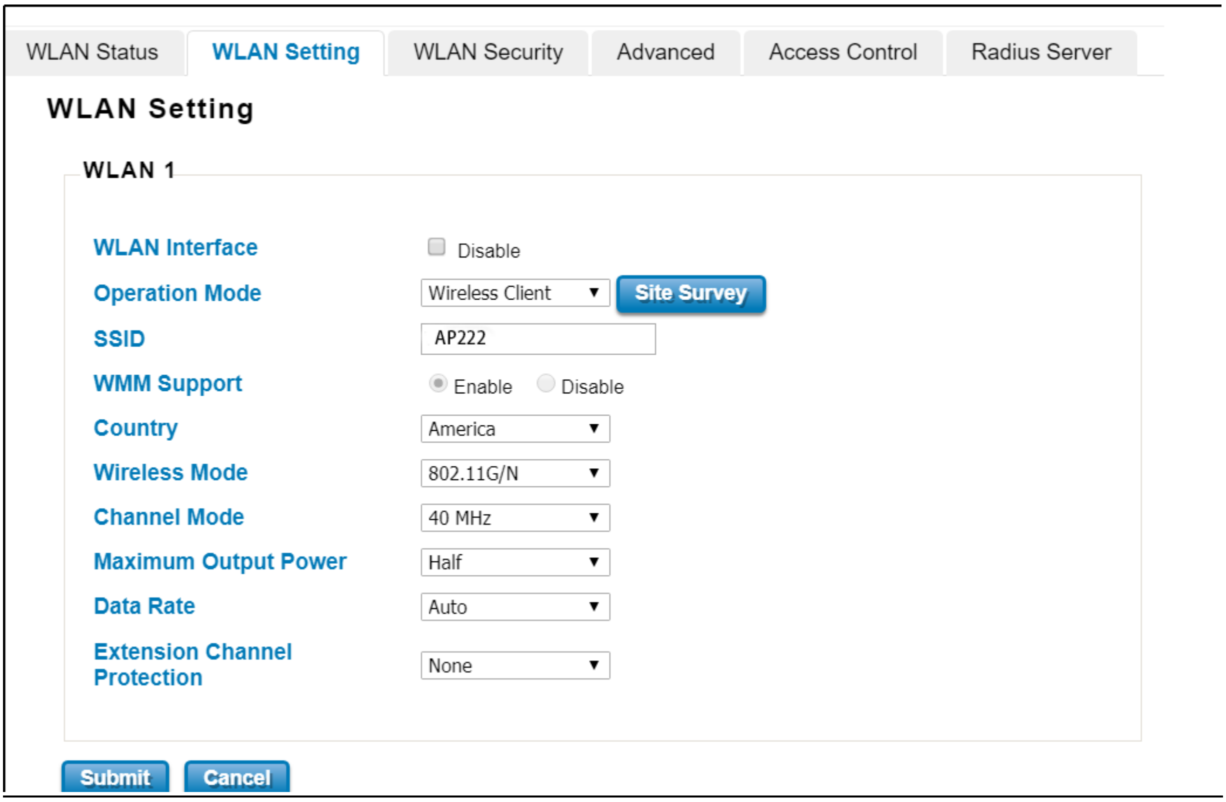
Security Setting(Setup Radius Server if Radius is enabled!)

Mode	Open System
Encryption	None
Key Type	Hex
Default Key	Key 1
Key 1	
Key 2	
Key 3	
Key 4	

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

Wireless Client

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



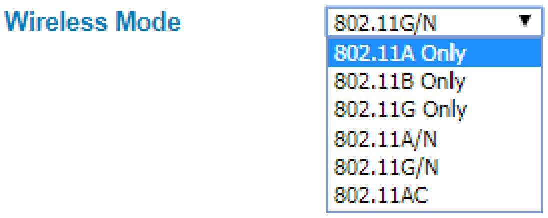
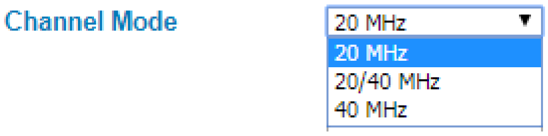
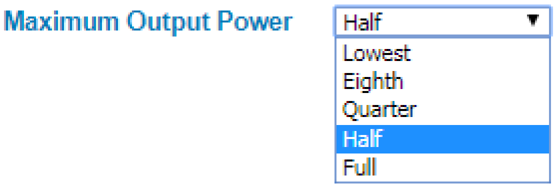
WLAN Setting

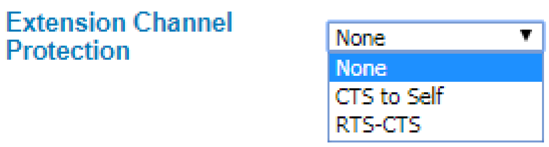
WLAN 1

WLAN Interface	□ Disable
Operation Mode	Wireless Client
SSID	AP222
WMM Support	● Enable ○ Disable
Country	America
Wireless Mode	802.11G/N
Channel Mode	40 MHz
Maximum Output Power	Half
Data Rate	Auto
Extension Channel Protection	None

The description of the columns is as below:

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

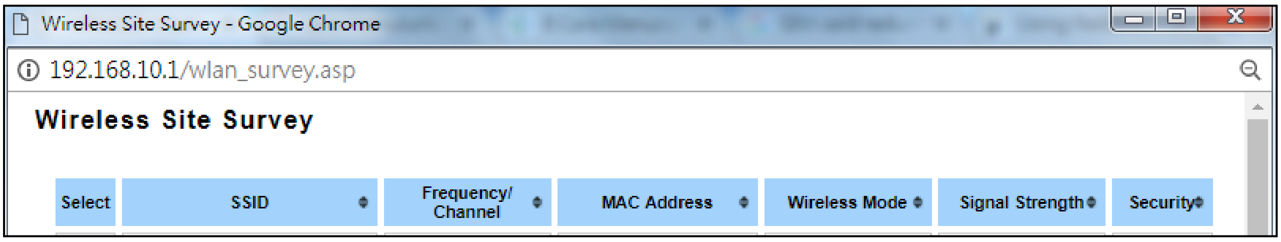
	over all other data traffic. ● **Best effort**: Best effort data packets consist of those originating from legacy devices or from applications or devices that lack QoS standards. **Background**: Background priority encompasses file downloads, print jobs and other traffic that does not suffer from increased latency.
Country	Select your country or region
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has a different configuration. For each wireless mode, it has a specific frequency and it has different basic setting..  Wireless Mode 802.11G/N 802.11A Only 802.11B Only 802.11G Only 802.11A/N 802.11G/N 802.11AC
Channel Mode	**Default: 20MHz**  Channel Mode 20 MHz There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user select 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequency, and for the 40MHz, it provides bigger data rate and received the 40MHz frequency. But basically, if the transmission happened between the AP and the client, both AP and client can have the negotiation phase about the frequency.
Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna.  Maximum Output Power Half
Data Rate	**Default: Auto** Select the specific data rate in order to control the transmission rate. **Auto** is preferred rate; the access point will automatically select the highest available rate to transmit. User may select lower rate when there is no great demand for transmission speed, for long distance transmission.

Extension Channel Protection	 Extension Channel Protection None None CTS to Self RTS-CTS 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.

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

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.



Wireless Site Survey - Google Chrome

192.168.10.1/wlan_survey.asp

Wireless Site Survey

Select	SSID	Frequency/ Channel	MAC Address	Wireless Mode	Signal Strength	Security

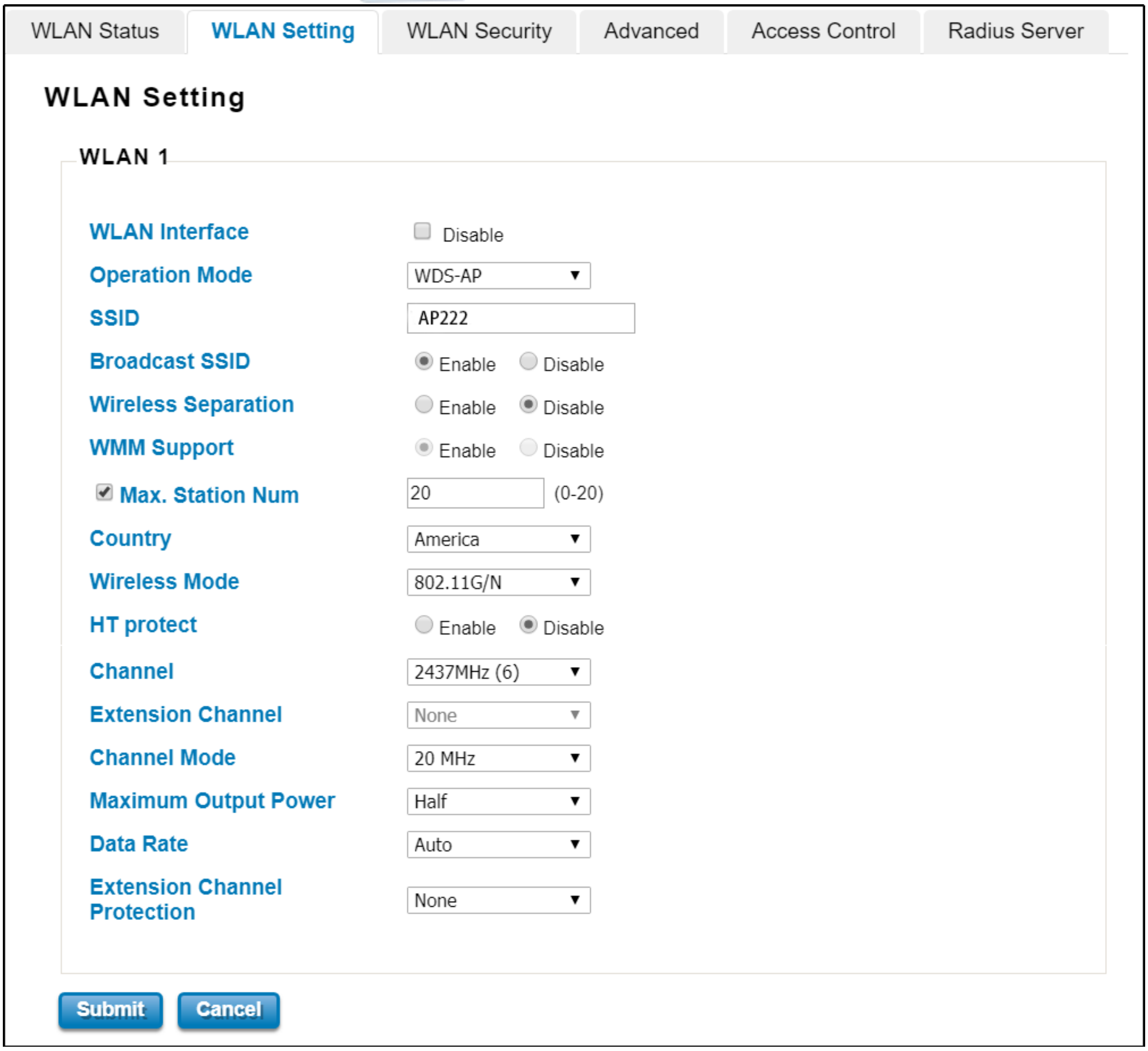
The description of the columns is as below:

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.



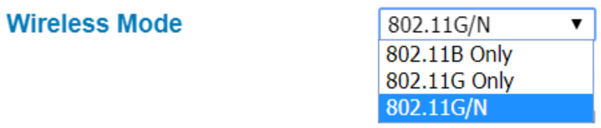
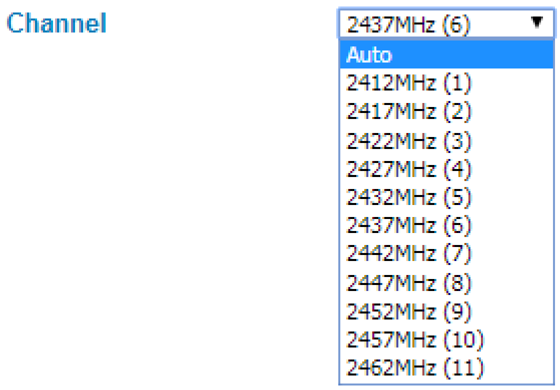
WLAN Setting

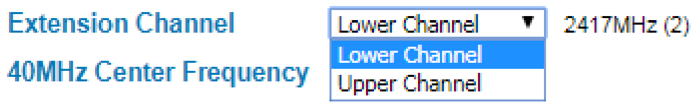
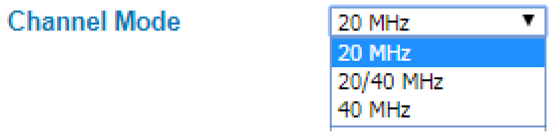
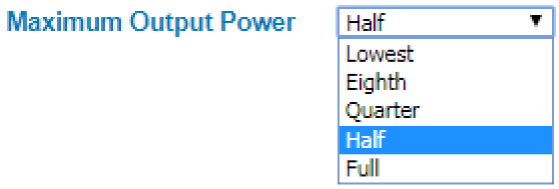
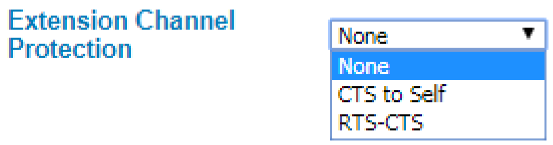
WLAN 1

WLAN Interface	□ Disable
Operation Mode	WDS-AP ▼
SSID	AP222
Broadcast SSID	● Enable ○ Disable
Wireless Separation	○ Enable ● Disable
WMM Support	● Enable ○ Disable
☑ Max. Station Num	20 (0-20)
Country	America ▼
Wireless Mode	802.11G/N ▼
HT protect	○ Enable ● Disable
Channel	2437MHz (6) ▼
Extension Channel	None ▼
Channel Mode	20 MHz ▼
Maximum Output Power	Half ▼
Data Rate	Auto ▼
Extension Channel Protection	None ▼

The description of the columns is as below:

TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless function.
Operation Mode	Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	**Default: model name** Input the primary name of the access point.
Broadcast SSID	**Default: Enabled.** By enabling the broadcast SSID, it makes the AP can be accessed and searched by the clients, and for the security concern by disabling this broadcaset SSID, the network will be hidden in order to prevent any malicious attack.
Wireless Separation	**Default: Disable** Under the AP mode, enable it to prevent one wireless device from directly communicating with another on the same AP
WMM Support	**Default: Enable**

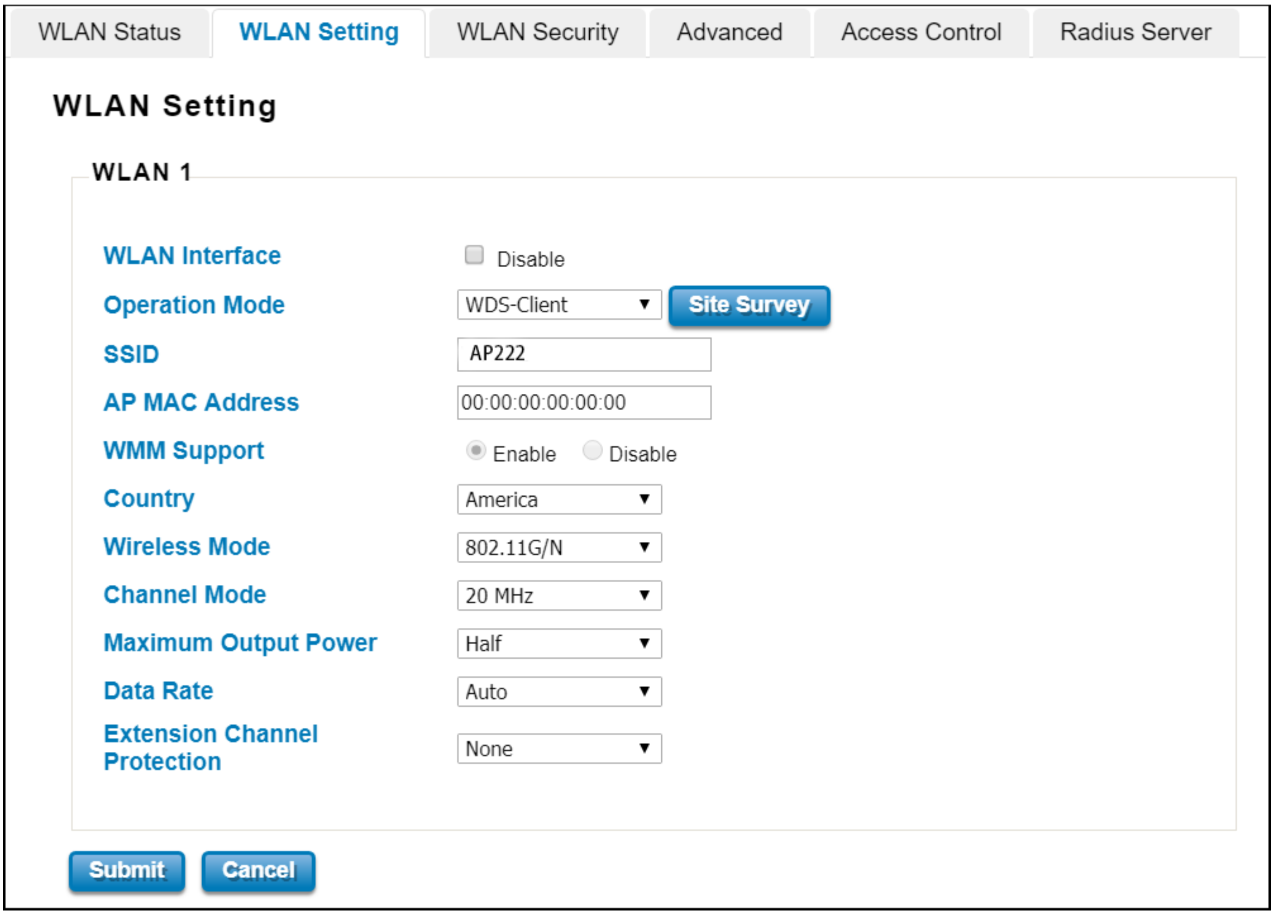
	A subset of the WLAN specification that enhances quality of service (QoS) on a network by prioritizing data packets onto four categories. Ranging from highest priority to lowest, these categories are: ● **Voice**: Giving voice packets the highest priority enables concurrent Voice over IP (VoIP) calls with minimal latency and the highest quality possible. ● **Video**: By placing video packets in the second tier, WMM prioritizes it over all other data traffic. ● **Best effort**: Best effort data packets consist of those originating from legacy devices or from applications or devices that lack QoS standards. **Background**: Background priority encompasses file downloads, print jobs and other traffic that does not suffer from increased latency.
Max Station Number	**Default: 20 (0-20)** Set the maximum number of station that can communicate with the access point.
Country	Select your country or region
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has different configuration. For each wireless mode, it has specific frequency and it has different basic setting.  Wireless Mode 802.11G/N
HT Protect	**Default: Disabled** Select Enabled to activate the High Throughput protect to ensure HT transmission with MAC mechanism.
Channel	**Default: 2437MHz (6)** Select the proper channel, each country has different band user may select the channel based on the situation. Or select auto to automatically set the channel.  Channel 2437MHz (6) Auto 2412MHz (1) 2417MHz (2) 2422MHz (3) 2427MHz (4) 2432MHz (5) 2437MHz (6) 2442MHz (7) 2447MHz (8) 2452MHz (9) 2457MHz (10) 2462MHz (11)
Extension Channel	**Default: Lower Channel 2417MHz (2)**

	 Extension Channel 40MHz Center Frequency Lower Channel Lower Channel Upper Channel 2417MHz (2) This option would be appeared when user select the Channel Mode to 20/40MHz or 40MHz. To put range for the frequency, it provides the Lower Channel (2417MHz (2)) with the 40MHz center frequency is 2427MHz (4) and Upper Channel (2457MHz (10)) with the 40MHz center frequency is 2447MHz (8).
Channel Mode	**Default: 20MHz**  There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user select 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequency, and for the 40MHz, it provides bigger data rate and received the 40MHz frequency. But basically, if the transmission happened between the AP and the client, both AP and client can have the negotiation phase about the frequency.
Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna.  Maximum Output Power Half Lowest Eighth Quarter Half Full
Data Rate	**Default: Auto** Select the specific data rate in order to control the transmission rate. **Auto** is preferred rate; the access point will automatically select the highest available rate to transmit. User may select the low rate when there is no great demand for transmission speed, for long distance transmission.
Extension Channel Protection	 Extension Channel Protection None None CTS to Self RTS-CTS Select from the dropdown list option between **CTS-Self or RTS-CTS** to avoid conflict with other wireless network and to improve the ability of the device to catch all the wireless transmissions. By activating this function it may decrease wireless network performance.

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

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.



WLAN Setting

WLAN 1

WLAN Interface: □ Disable

Operation Mode: WDS-Client ▼ Site Survey

SSID: AP222

AP MAC Address: 00:00:00:00:00:00

WMM Support: ● Enable ○ Disable

Country: America ▼

Wireless Mode: 802.11G/N ▼

Channel Mode: 20 MHz ▼

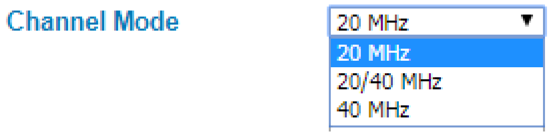
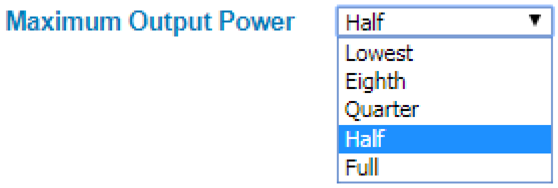
Maximum Output Power: Half ▼

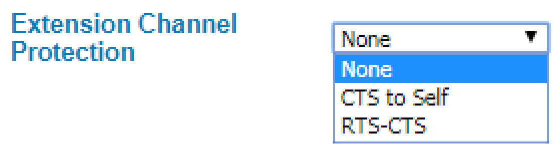
Data Rate: Auto ▼

Extension Channel Protection: None ▼

The description of the columns is as below:

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

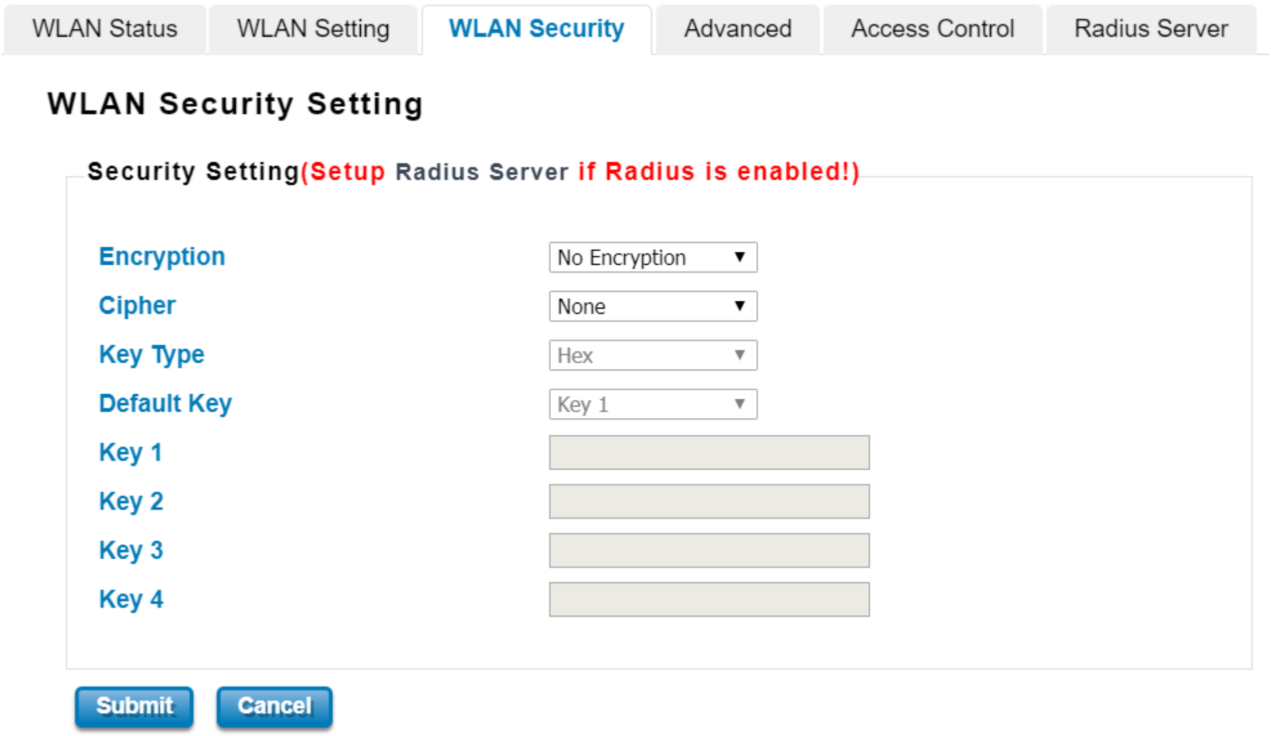
	● **Voice**: Giving voice packets the highest priority enables concurrent Voice over IP (VoIP) calls with minimal latency and the highest quality possible. ● **Video**: By placing video packets in the second tier, WMM prioritizes it over all other data traffic. ● **Best effort**: Best effort data packets consist of those originating from legacy devices or from applications or devices that lack QoS standards. **Background**: Background priority encompasses file downloads, print jobs and other traffic that does not suffer from increased latency.
Country	Select your country or region
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has a different configuration. For each wireless mode, it has a specific frequency and it has different basic setting. Wireless Mode 802.11G/N 802.11B Only 802.11G Only 802.11G/N
Channel Mode	**Default: 20MHz**  Channel Mode 20 MHz There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user select 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequency, and for the 40MHz, it provides bigger data rate and received the 40MHz frequency. But basically, if the transmission happened between the AP and the client, both AP and client can have the negotiation phase about the frequency.
Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna.  Maximum Output Power Half
Data Rate	**Default: Auto** Select the specific data rate in order to control the transmission rate. **Auto** is preferred rate, the access point will automatically select the highest available rate to transmit. User may select the low rate when there is no great demand for transmission speed, for long distance transmission.

Extension Channel **Protection**	 Extension Channel Protection: None Select from the dropdown list option between **CTS-Self or RTS-CTS** to avoid conflict with other wireless network and to improve the ability of the device to catch all the wireless transmissions. By activate this function it may decrease wireless network performance.

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

3.5.3 WLAN SECURITY

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



WLAN Security Setting

Security Setting(Setup Radius Server if Radius is enabled!)

Encryption: No Encryption

Cipher: None

Key Type: Hex

Default Key: Key 1

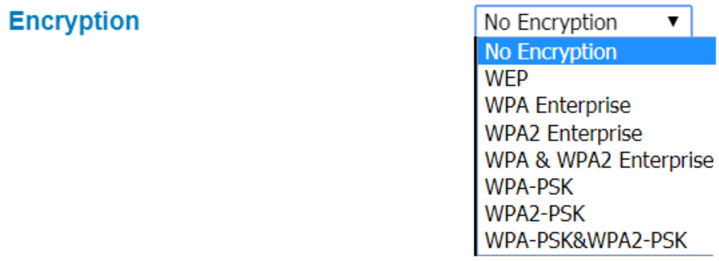
Key 1:

Key 2:

Key 3:

Key 4:

The description of the columns is as below:

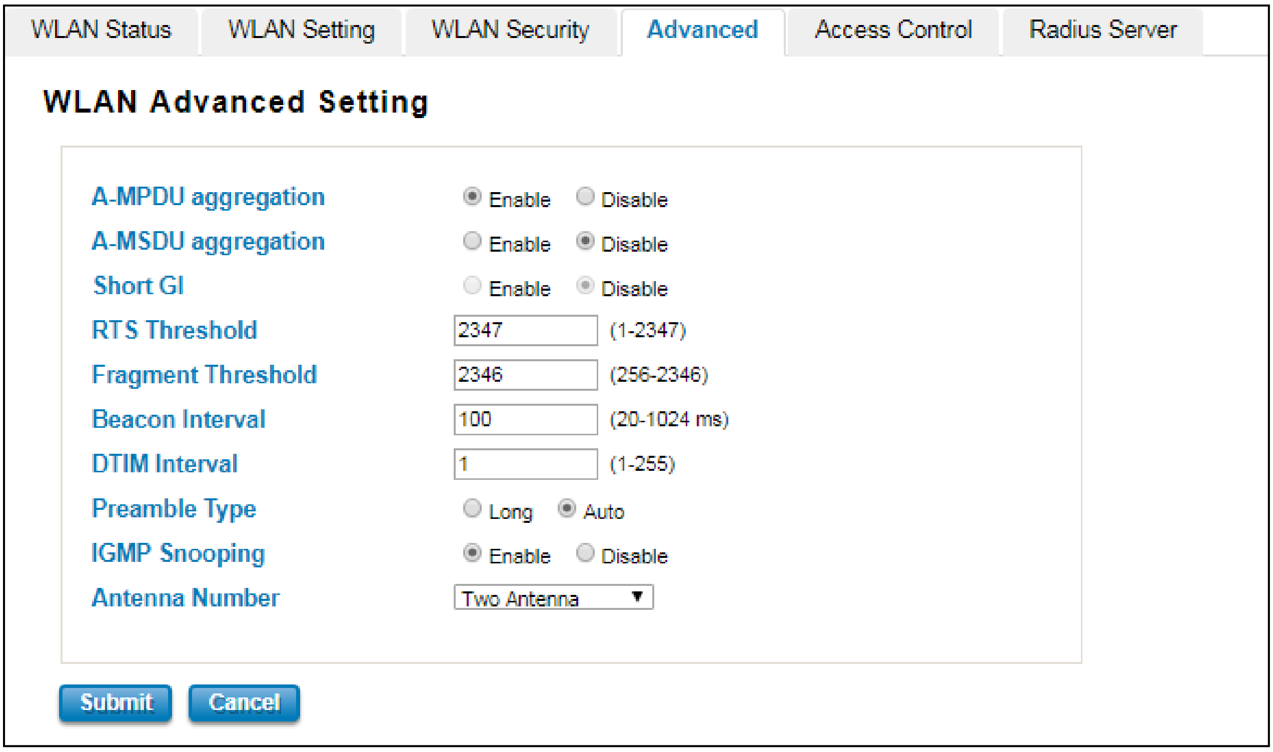
TERMS	DESCRIPTION
Encryption	**Default: No Encryption**  Encryption: No Encryption No Encryption WEP WPA Enterprise WPA2 Enterprise WPA & WPA2 Enterprise WPA-PSK WPA2-PSK WPA-PSK&WPA2-PSK

	No Encryption: It allows any device to join the network without security checks. **WEP**: Data encryption and key are required for the authentication. **WPA Enterprise**: With warrant (username, password and etc.) offered by user, this kind of authentication can be realized with specific RADIUS server. **WPA2 Enterprise**: A new version of WPA, only clients that supported with WPA2 can apply this security function. The AES encryption RADIUS server is required. **WPA & WPA2 Enterprise**: AES & TKIP encryption and RADIUS server is required. **WPA-PSK**: A simplified WPA mode that no need to specify the authentication server. It can be called as WPA Pre-Shared Key, a user just needs to enter a key in each WLAN node. The data encryption is only TKIP. **WPA2-PSK**: A new version of WPA, only clients that supported with WPA2 can apply this security function. The data encryption can only be AES and WPA Pre-Share Key is required. **WPA-PSK&WPA2-PSK**: The data encryption will be AES & TKIP and WPA Pre-Share Key is required.
Cipher	Configure the data encryption mode. ● **None**: Available only when the authentication type is an open system. ● **64 bits WEP**: It is made up of 10 hexadecimal numbers. ● **128 bits WEP**: It is made up of 26 hexadecimal numbers. ● **TKIP**: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK. ● **AES**: Advanced Encryption Standard, it is usually co-used with WPA2-PSK.
Key Type	**Default: Hex** WEP can be configured with a 64-bit or 128-bit Shared Key (hexadecimal or ASCII). As defined, hexadecimal number is represented by 0-9, A-F or a-f; ASCII is represented by 0-9, A-F, a-f or punctuation. Each one consists of two-digit hexadecimal.
Default Key	**Default: Key 1** Set the specific default key.
Key 1~4	Enter the specific encryption key.

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

3.5.4 ADVANCED

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



WLAN Advanced Setting

A-MPDU aggregation	● Enable ○ Disable
A-MSDU aggregation	○ Enable ● Disable
Short GI	○ Enable ● Disable
RTS Threshold	2347 (1-2347)
Fragment Threshold	2346 (256-2346)
Beacon Interval	100 (20-1024 ms)
DTIM Interval	1 (1-255)
Preamble Type	○ Long ● Auto
IGMP Snooping	● Enable ○ Disable
Antenna Number	Two Antenna ▼

The description of the columns is as below:

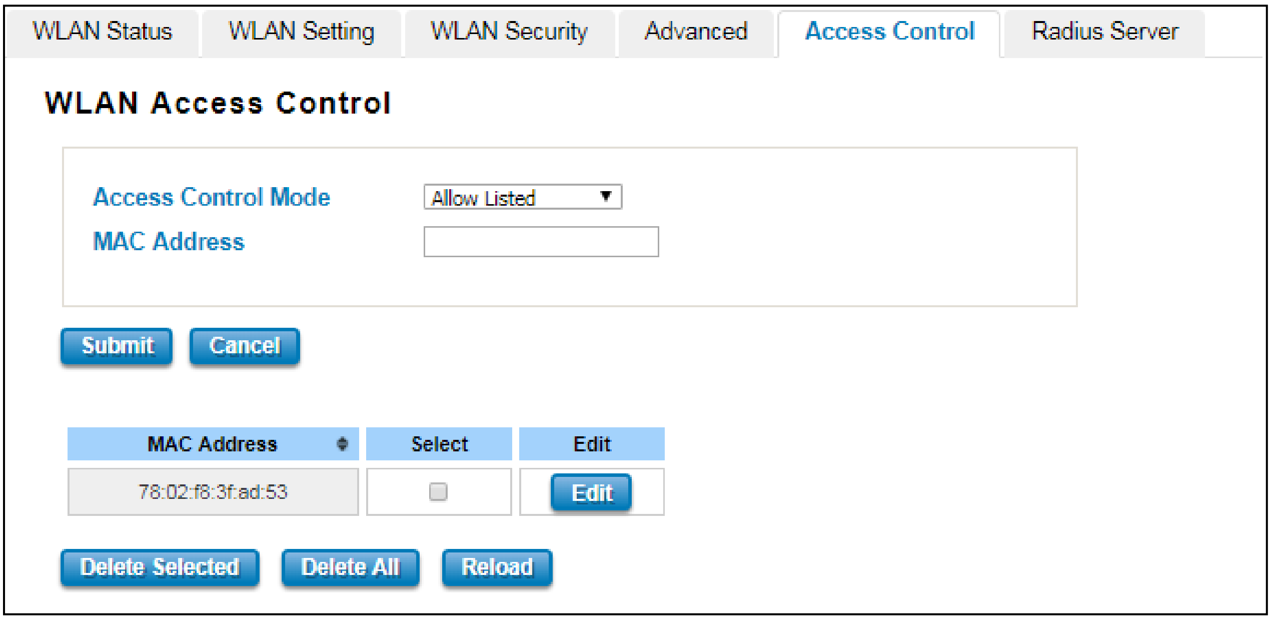
TERMS	DESCRIPTION
A-MPDU/A-MSDU aggregation	For the AP mode, by enabling this function the data rate of the AP could be enhanced greatly, Do not enable this function if the wireless clients don’t support A-MPDU/A-MSDU aggregation.
Short GI	Enable this function to obtain better data rate. (careful with compatibility issue)
RTS Threshold	**Default: 2347 (1-2347)** Basically, it is about the transmission process between the AP and the end station. When the AP sends Request to Send frames to station and it will do the negotiation process about sending the data frame. When the station receives an RTS frame, the station will respond with send back Clear to Send frame to confirm the right to start transmission.
Fragment Threshold	**Default: 2346 (256-2436)** Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance.
Beacon Interval	**Default: 100ms (20-1024 ms)** Specify the interval to broadcast packets.
DTIM Interval	**Default: 1 (1-255)** Delivery Traffic Indication Message interval is an additional message added

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

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

3.5.5 ACCESS CONTROL (AP MODE)

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



WLAN Access Control

Access Control Mode: Allow Listed ▼

MAC Address:

MAC Address	Select	Edit
78:02:f8:3f:ad:53	□	Edit

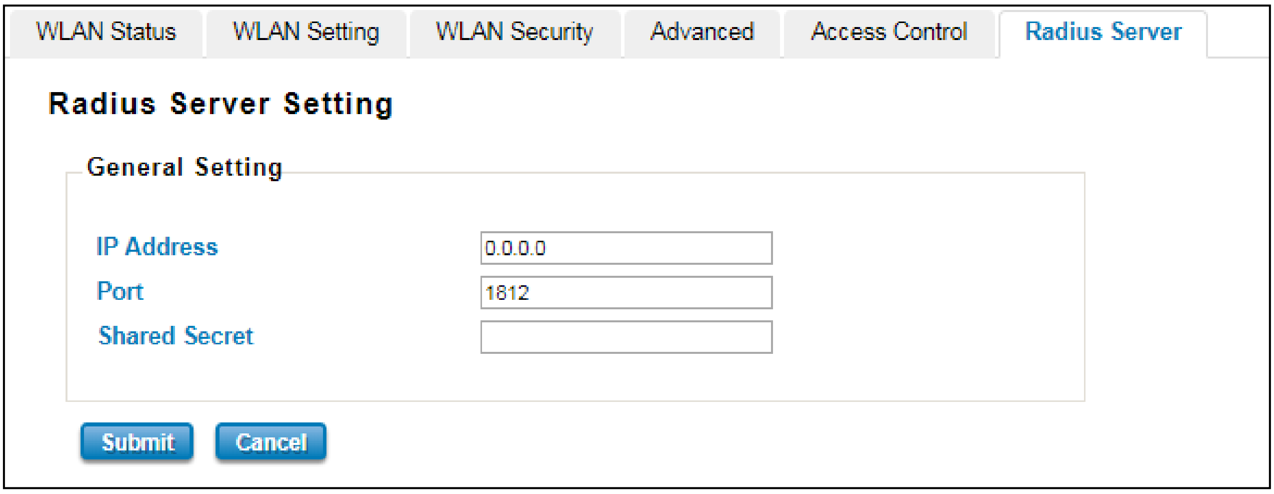
The description of the columns is as below:

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

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

3.5.6 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.



Radius Server Setting

General Setting

IP Address 0.0.0.0

Port 1812

Shared Secret

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**

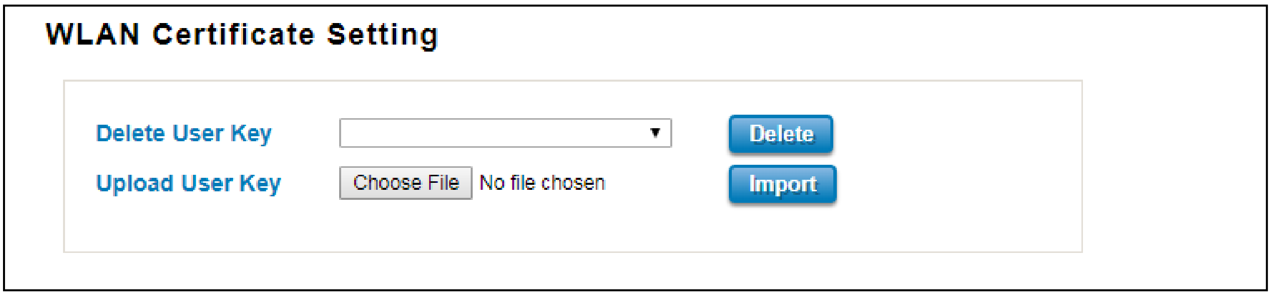
The description of the RADIUS Authentication interface is as below:

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).

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

3.5.7 CERTIFICATE FILE (CLIENT MODE)

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



WLAN Certificate Setting

Delete User Key

Upload User Key No file chosen

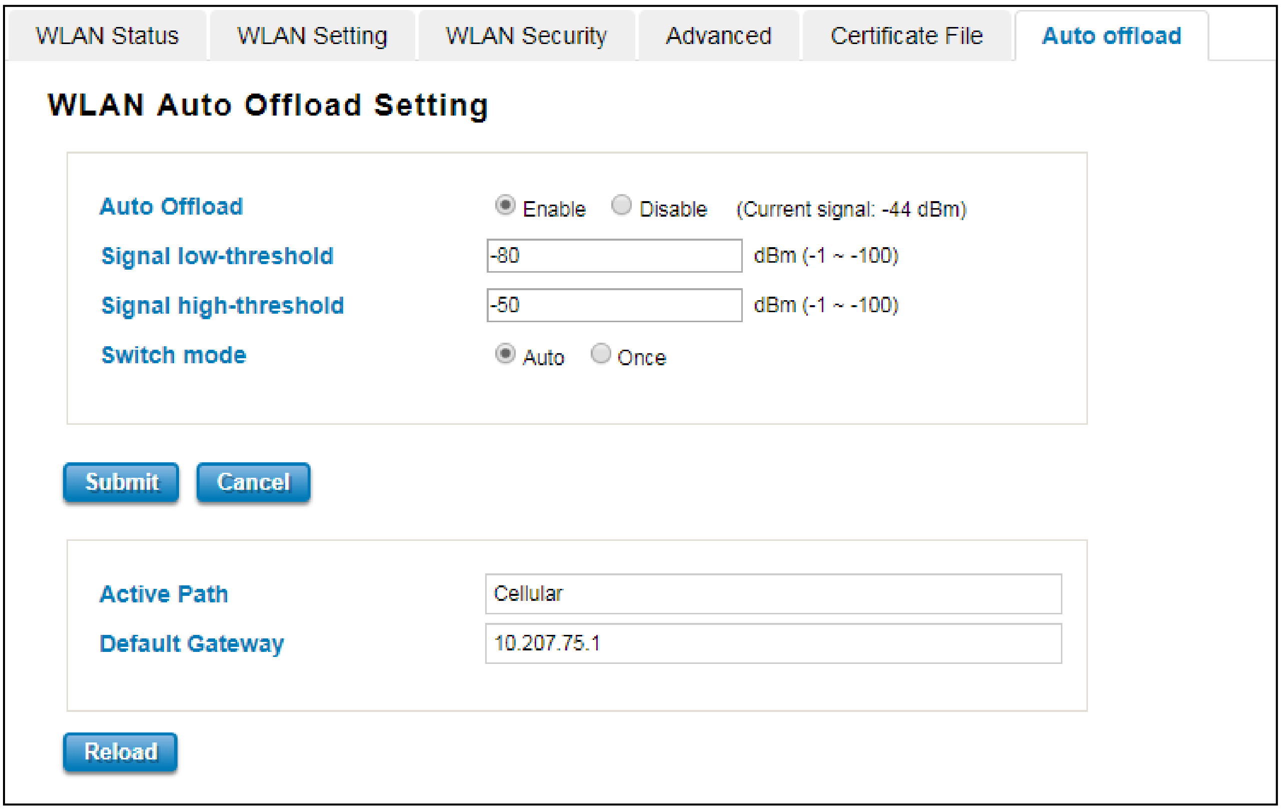
The description of the columns is as below:

TERMS	DESCRIPTION
Delete User Key	Delete the selected certificate

Upload User Key	Upload a certificate file from a specified file location

3.5.8 AUTO OFFLOAD (CLIENT MODE)

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



WLAN Auto Offload Setting

Auto Offload ● Enable ○ Disable (Current signal: -44 dBm)

Signal low-threshold -80 dBm (-1 ~ -100)

Signal high-threshold -50 dBm (-1 ~ -100)

Switch mode ● Auto ○ Once

Active Path Cellular

Default Gateway 10.207.75.1

The description of the interface is as below:

TERMS	DESCRIPTION
Auto Offload	Default: Disable Enable or Disable Auto Offload feature. This feature can be activated when the Wi-Fi is configured as the client mode and the Cellular interface is established. And it will show the current signal strength.
Signal low-threshold	**Default: -80 dBm (Range: -1 ~ -100 dBm)** When signal strength is lower than the upper range, then the connection will be directed to Cellular.
Signal high-threshold	**Default: -50 dBm (Range: -1 ~ -100 dBm)** When signal strength is higher than the upper range, then the connection will be directed to Wi-Fi.
Switch mode	**Default: Auto** When user chooses the **Auto mode**, the connection will automatically switch

	to the stronger signal between Wi-Fi or Cellular. If user chooses to **Once mode**, it means the connection will switch to the stronger signal once between Wi-Fi or Cellular and will stay at the connection even there were a stronger signal appear.
Active Path	Show the current active path between Wireless or Cellular.
Default Gateway	Show the default gateway IP Address.

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

3.6 SECURITY

AVCOMM 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:

3.6.1 Access Control

3.6.2 Outbound Firewall

3.6.3 NAT Setting

3.6.4 OpenVPN

3.6.5 L2TP Setting

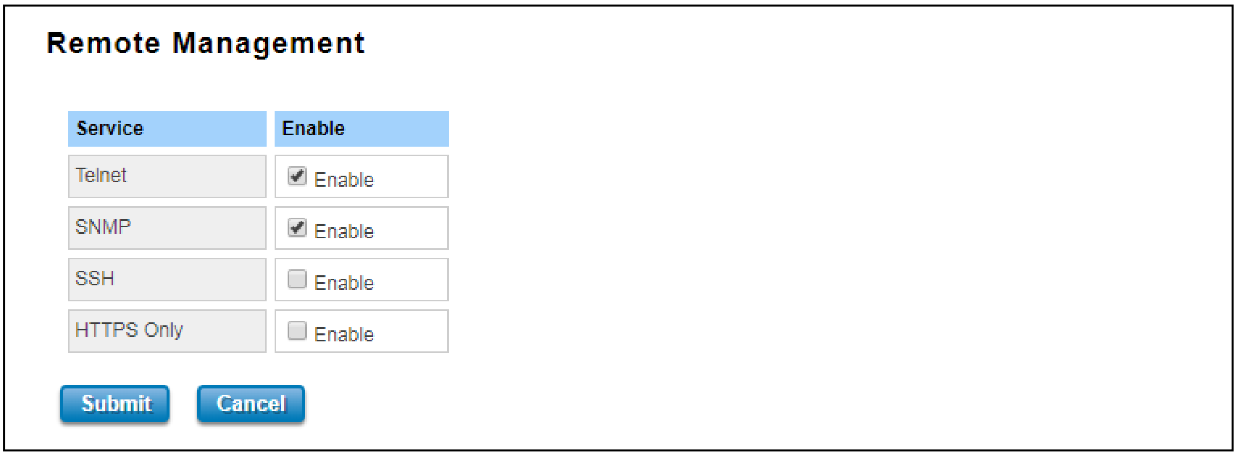
3.6.6 GRE Setting

3.6.1 ACCESS CONTROL

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

Remote Management

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



Remote Management

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

The description of the columns is as below:

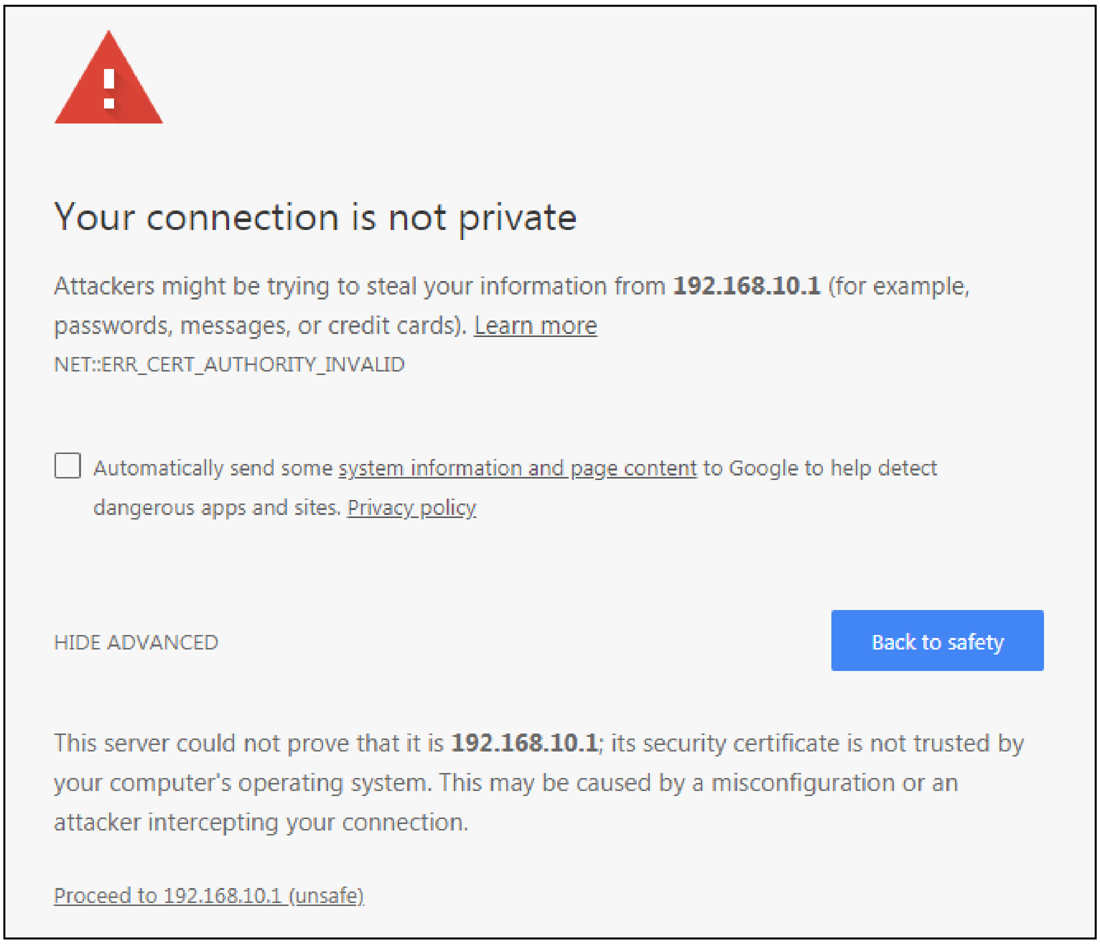
TERMS	DESCRIPTION
Telnet	Allows the user to remotely login and manage the device by Telnet. When user doesn't enable it, the connection through telnet will not allow.

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

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

HTTPS Only

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



Your connection is not private

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

NET::ERR_CERT_AUTHORITY_INVALID

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

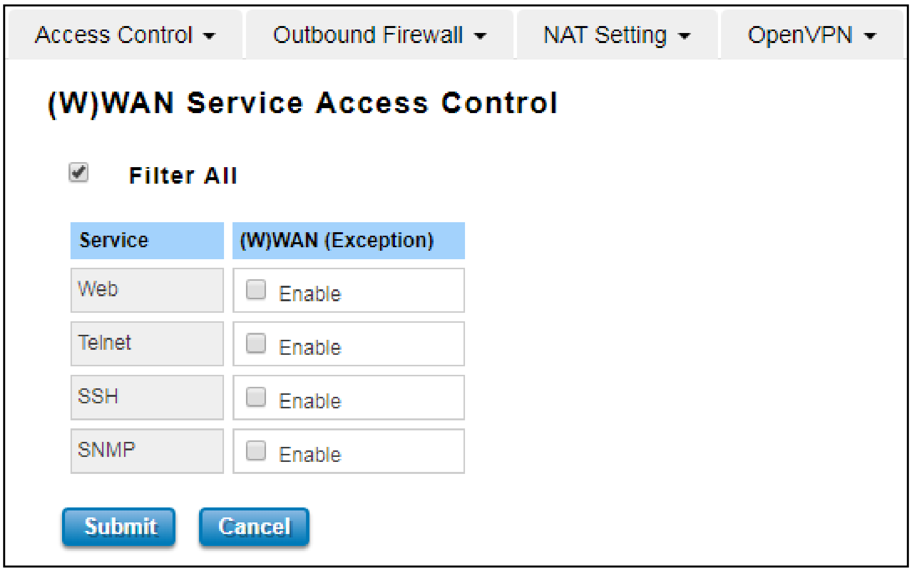
This server could not prove that it is **192.168.10.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.10.1 (unsafe)

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

WAN Access

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



(W)WAN Service Access Control

☑ Filter All

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

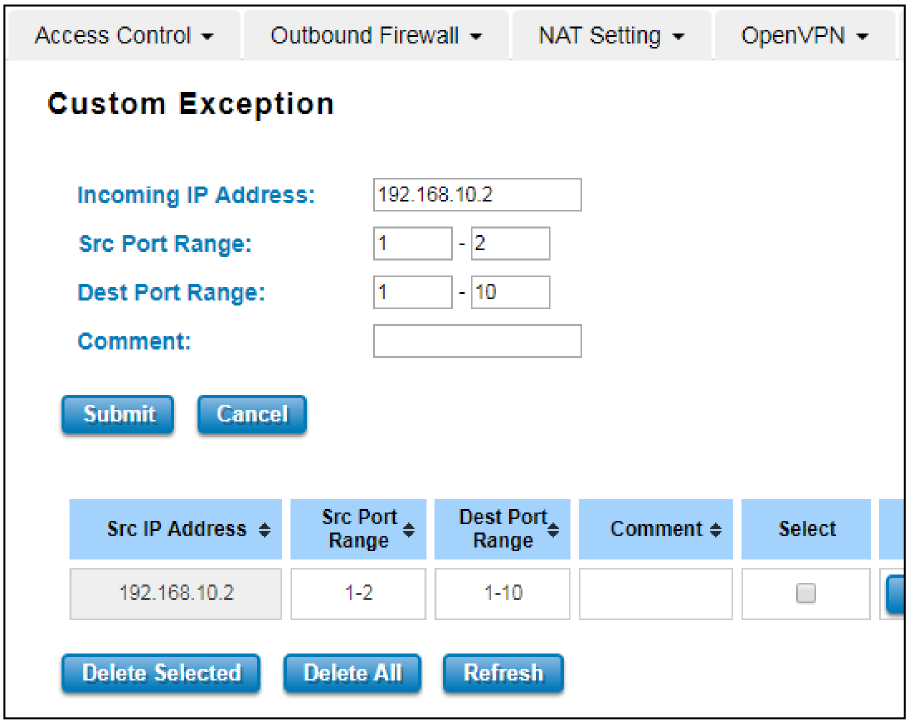
The description of the columns is as below:

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

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

Custom Exception

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



Custom Exception

Incoming IP Address: 192.168.10.2

Src Port Range: 1 - 2

Dest Port Range: 1 - 10

Comment:

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

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.

3.6.2 OUTBOUND FIREWALL

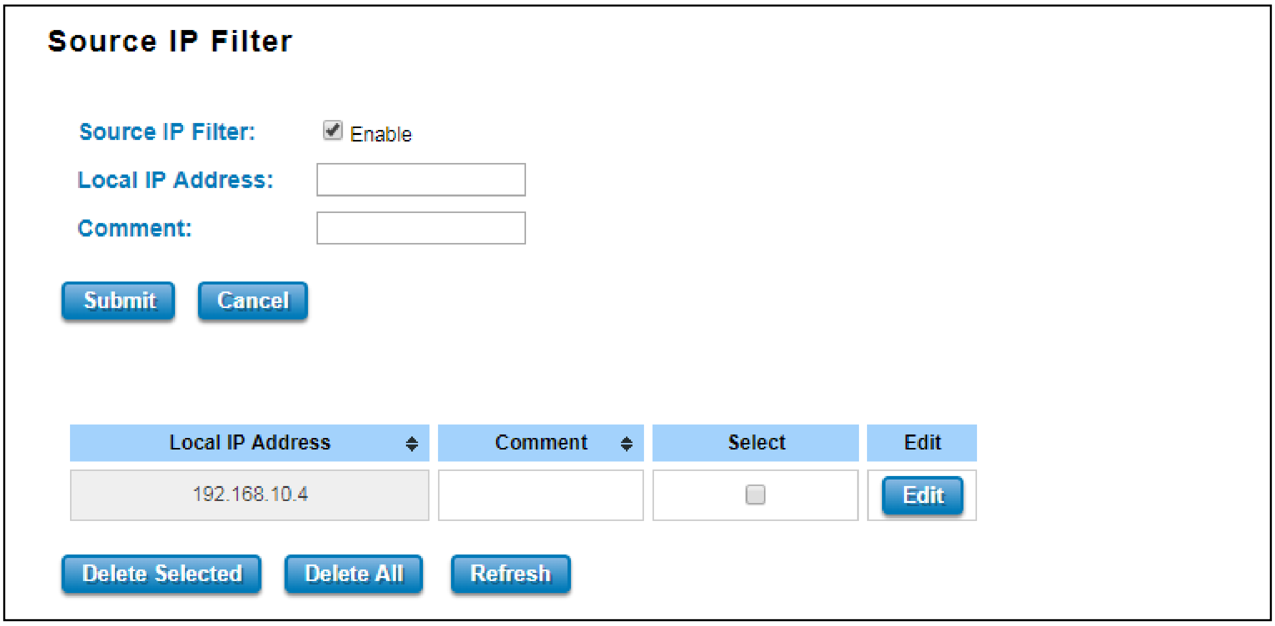
AVCOMM' router has different types firewall settings, user can enable the setting, configure the rules. The following section is Outbound Firewall Settings pages where user can configure the Outbound Firewall setting.

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.



Source IP Filter

Source IP Filter: ☑ Enable

Local IP Address:

Comment:

Local IP Address	Comment	Select	Edit
192.168.10.4		□	Edit

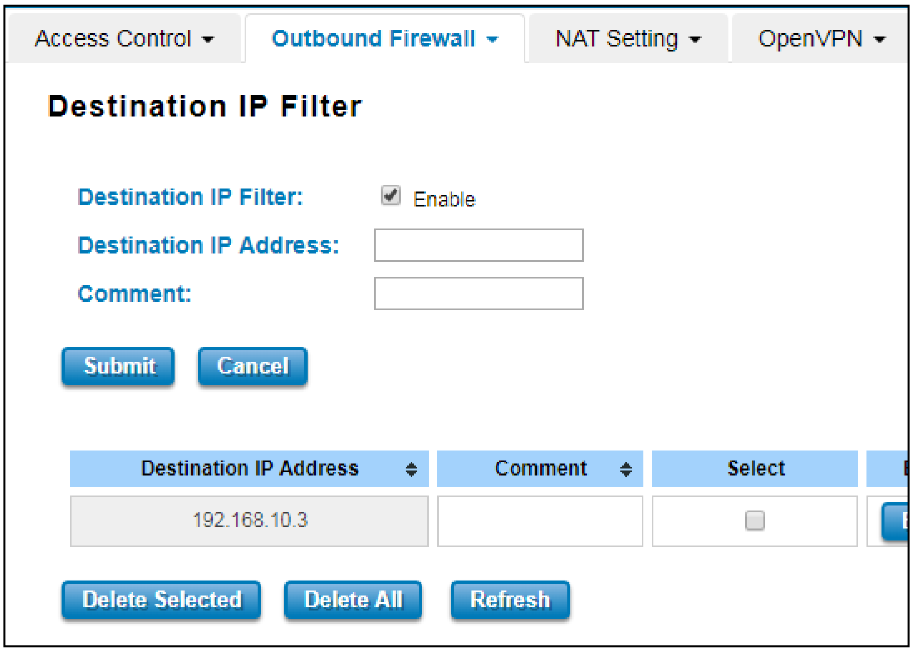
The description of the columns is as below:

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

Click **Refresh** to refresh the table

Dest IP Filter

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



Destination IP Filter

Destination IP Filter: ☑ Enable

Destination IP Address:

Comment:

Destination IP Address	Comment	Select
192.168.10.3		□

The description of the columns is as below:

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

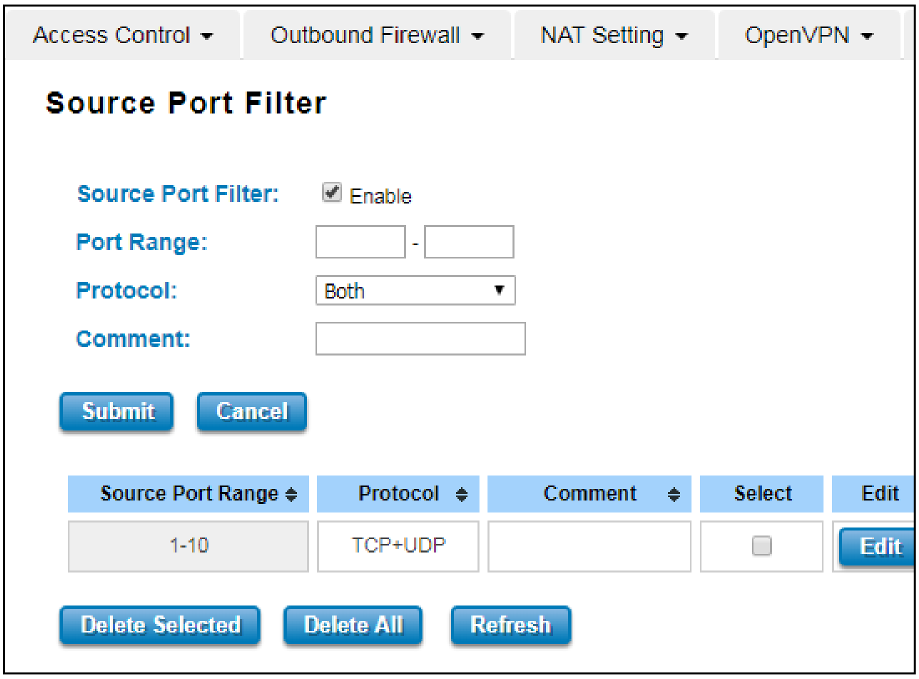
Click **Refresh** to refresh the table

Src Port Filter

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

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

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



Source Port Filter

Source Port Filter: ☑ Enable

Port Range: ___ - ___

Protocol: Both

Comment:

Source Port Range	Protocol	Comment	Select	Edit
1-10	TCP+UDP		□	Edit

The description of the columns is as below:

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

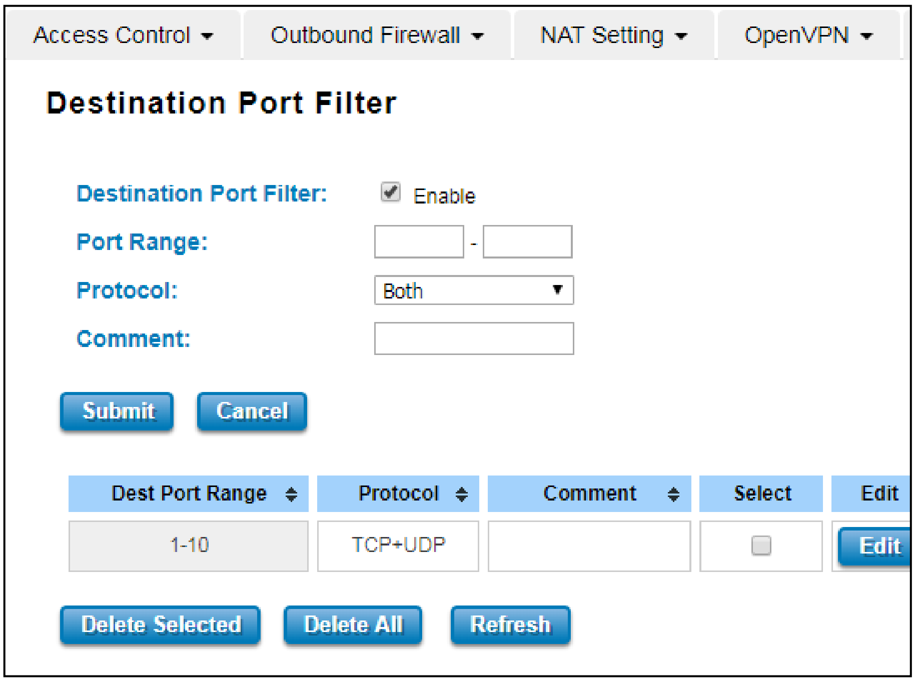
Click **Refresh** to refresh the table

Dest Port Filter

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

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

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



Destination Port Filter

Destination Port Filter:	☑ Enable
Port Range:	-
Protocol:	Both
Comment:	

Dest Port Range	Protocol	Comment	Select	Edit
1-10	TCP+UDP		□	Edit

The description of the columns is as below:

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

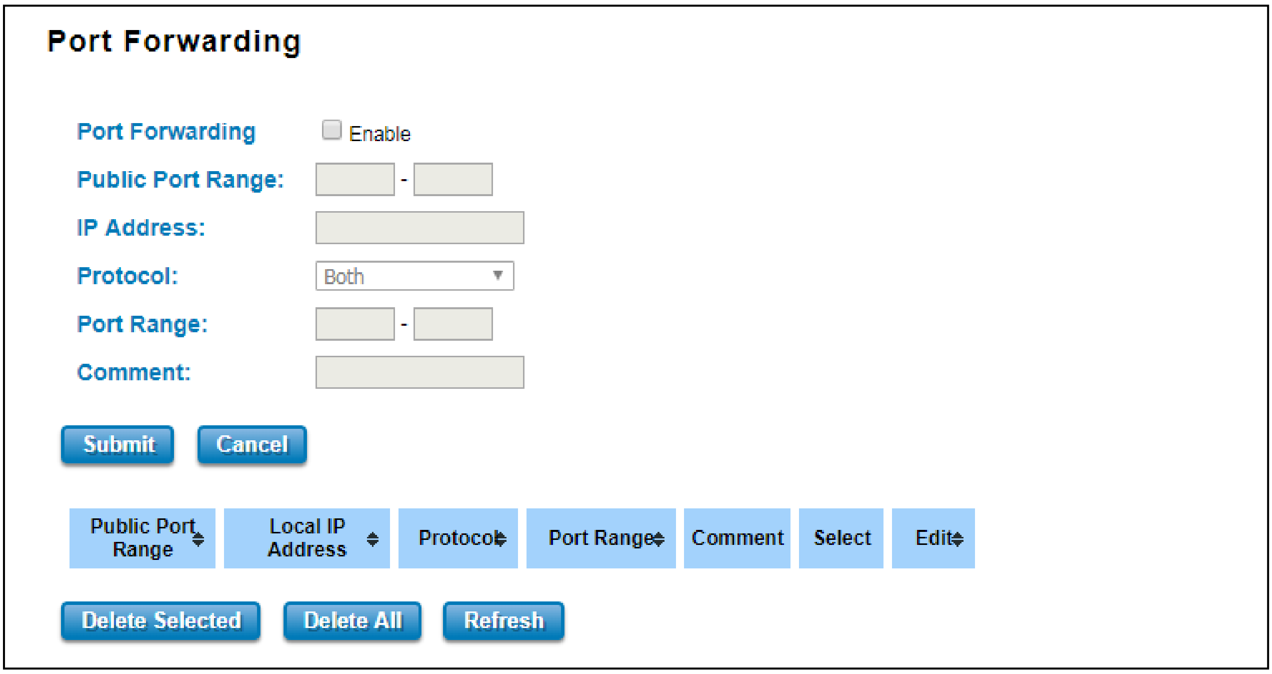
Click **Refresh** to refresh the table

3.6.3 NAT SETTING

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

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

Port Forwarding



Port Forwarding

Port Forwarding ☐ Enable

Public Port Range: -

IP Address:

Protocol: Both

Port Range: -

Comment:

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

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

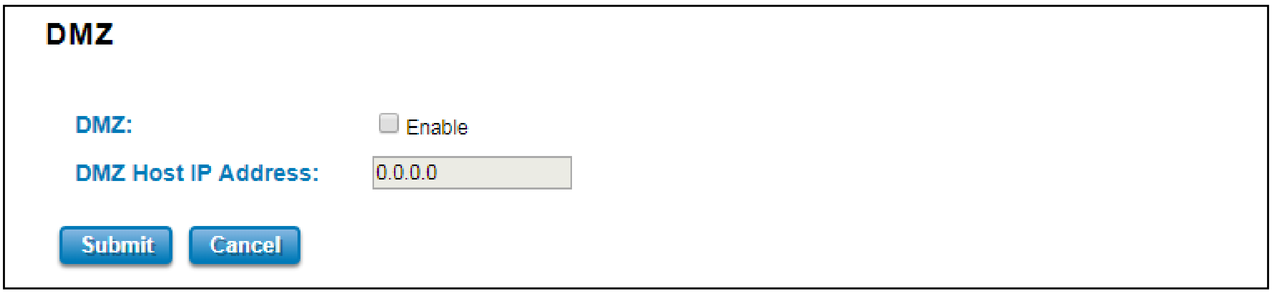
The description of the columns is as below:

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

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

DMZ

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



DMZ

DMZ: □ Enable

DMZ Host IP Address: 0.0.0.0

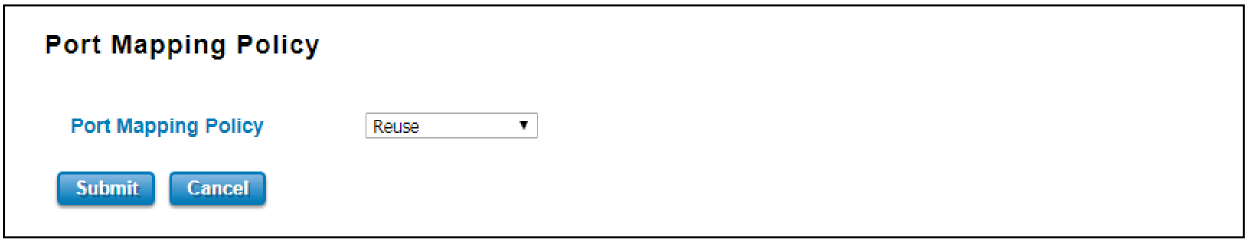
Click **Enable** to activate the function and assign the IP address of **DMZ Host IP Address**. This is the DMZ computer's IP address. Click Submit to activate the function.

The description of the columns is as below:

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

Port Mapping Policy

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



Port Mapping Policy

Port Mapping Policy: Reuse

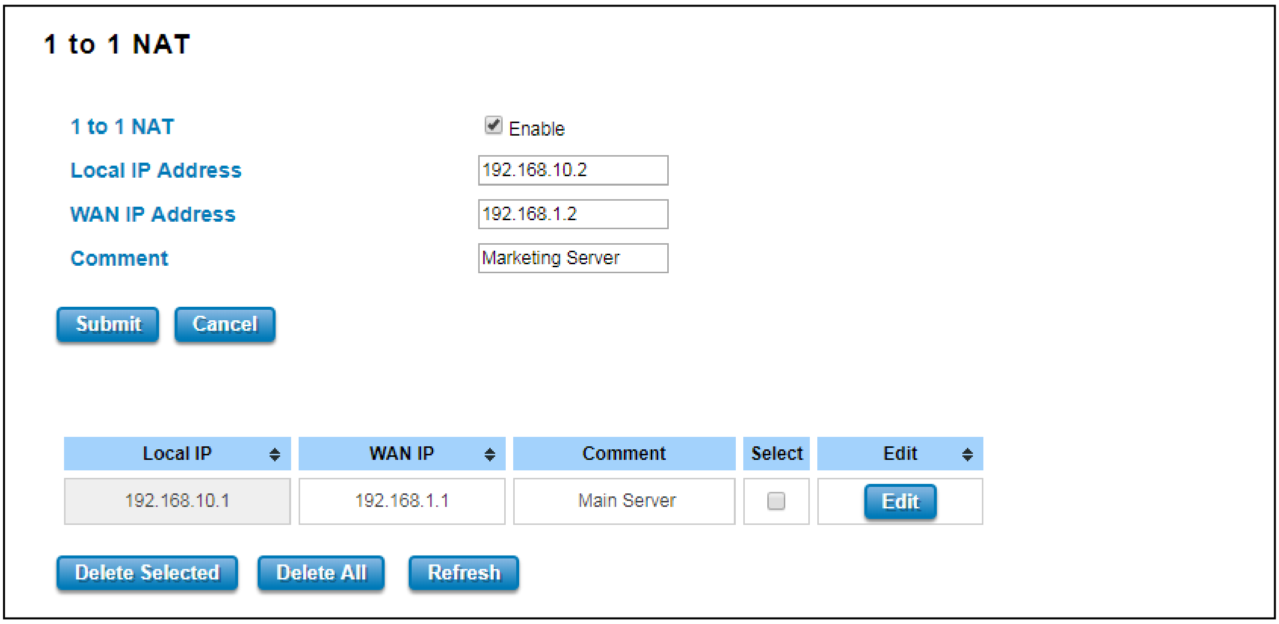
The description of the columns is as below:

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.

1 to 1 NAT

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



1 to 1 NAT

1 to 1 NAT	☑ Enable
Local IP Address	192.168.10.2
WAN IP Address	192.168.1.2
Comment	Marketing Server

Local IP	WAN IP	Comment	Select	Edit
192.168.10.1	192.168.1.1	Main Server	□	Edit

The description of the columns is as below:

TERMS	DESCRIPTION
1 to 1 NAT	Check the box to enable the function
Local IP Address	The target local IP Address
WAN IP Address	The incoming IP Address that coming through the WAN
Comment	Enter a comment

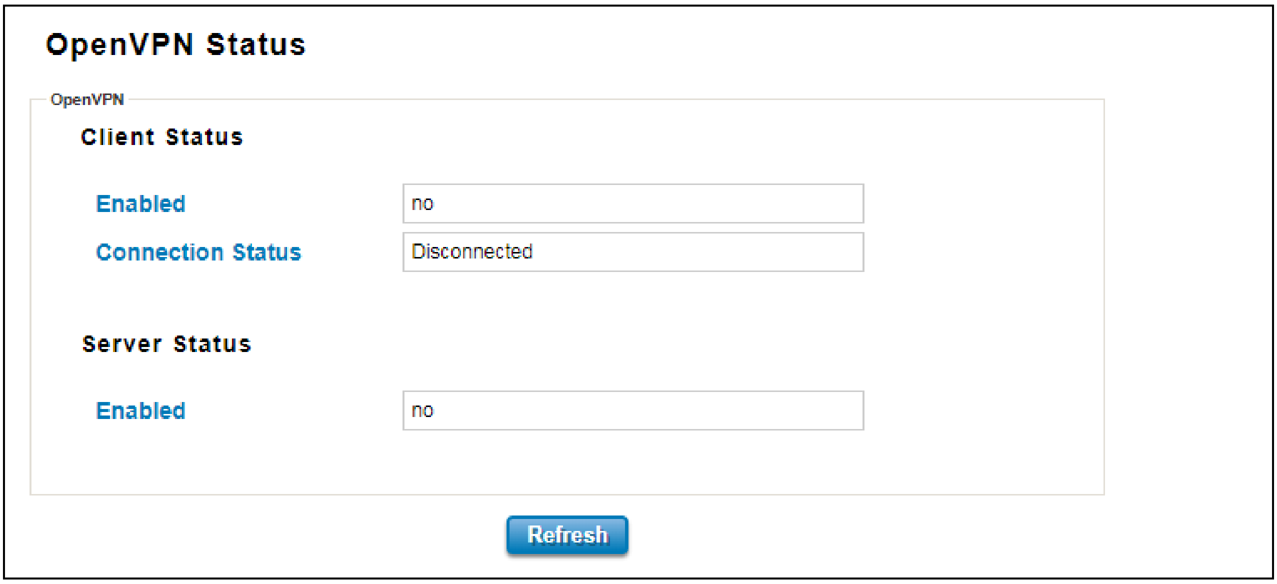
Click **Submit** to apply the configuration.

3.6.4 OPEN VPN

AVCOMM 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.



OpenVPN Status

OpenVPN

Client Status

Enabled: no

Connection Status: Disconnected

Server Status

Enabled: no

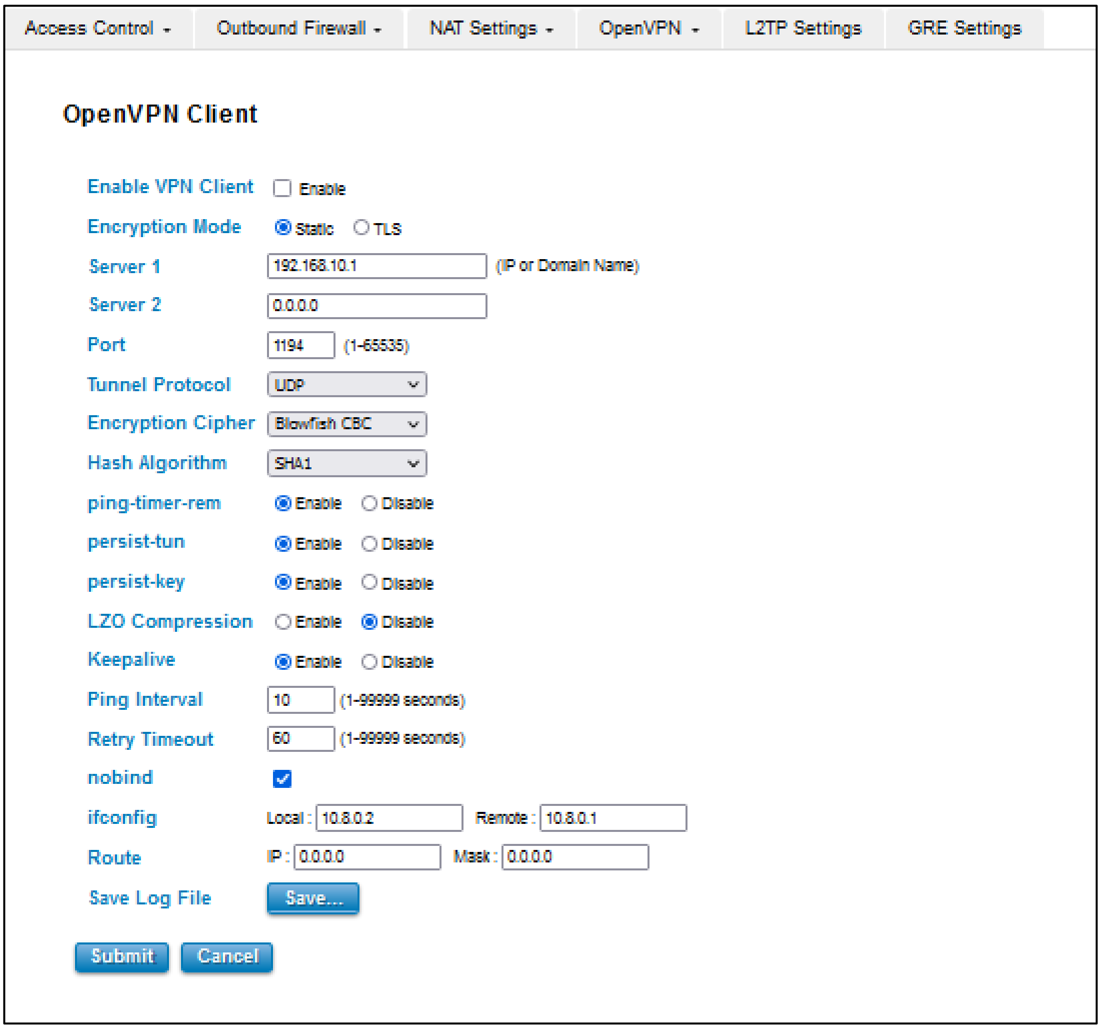
The description of the columns is as below:

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

Click **Refresh** to update the information.

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.



OpenVPN Client

Enable VPN Client ☐ Enable

Encryption Mode ● Static ○ TLS

Server 1 192.168.10.1 (IP or Domain Name)

Server 2 0.0.0.0

Port 1194 (1-65535)

Tunnel Protocol UDP

Encryption Cipher Blowfish CBC

Hash Algorithm SHA1

ping-timer-rem ● Enable ○ Disable

persist-tun ● Enable ○ Disable

persist-key ● Enable ○ Disable

LZO Compression ○ Enable ● Disable

Keepalive ● Enable ○ Disable

Ping Interval 10 (1-99999 seconds)

Retry Timeout 60 (1-99999 seconds)

nobind ☑

ifconfig Local : 10.8.0.2 Remote : 10.8.0.1

Route IP : 0.0.0.0 Mask : 0.0.0.0

Save Log File

The description of the columns is as below:

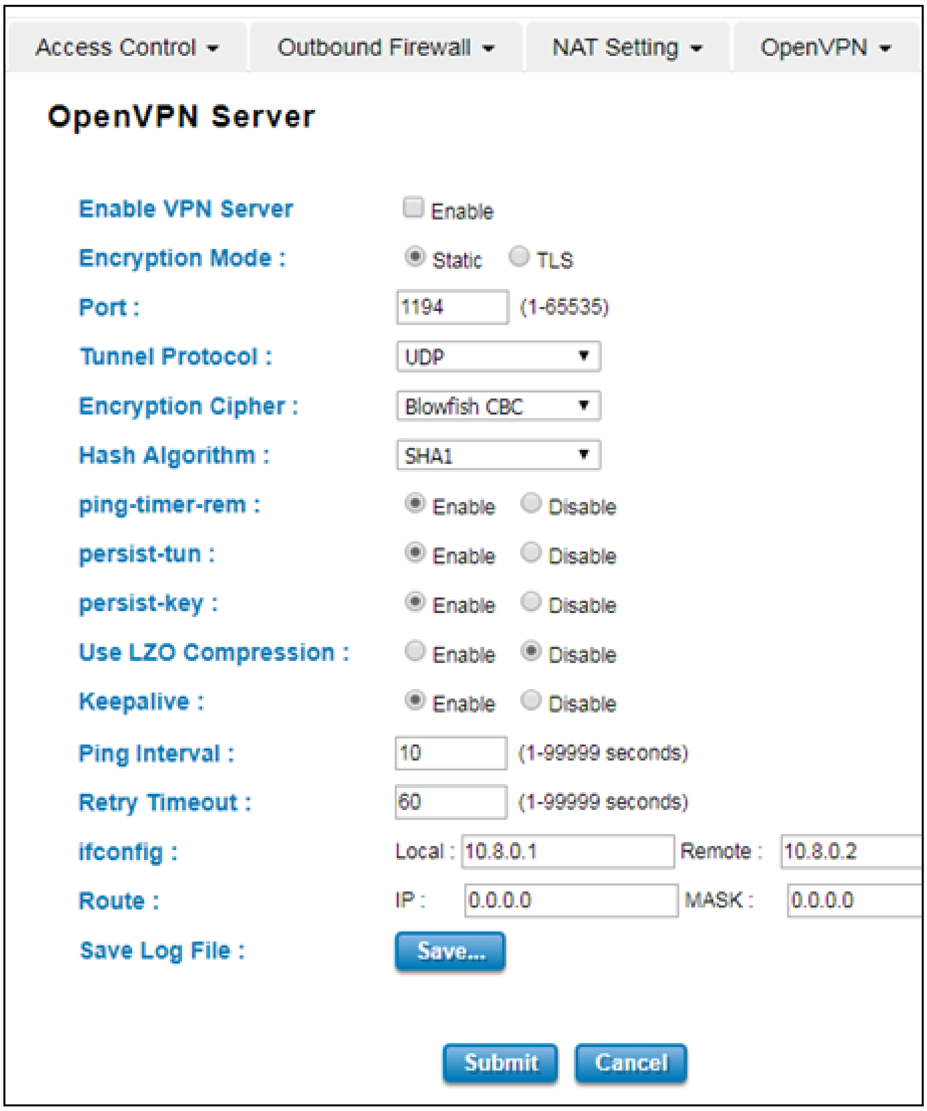
TERMS	DESCRIPTION
Enable VPN Client	Select Enable to activate the VPN Client function
Encryption Mode	Choose the Encryption Mode Static Key: Use a pre-shared static key. TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server 1	Type the IP Address of the VPN Server
Server 2	Type the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

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

Click **Submit** to apply the configuration.

OpenVPN Server

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



OpenVPN Server

Enable VPN Server: □ Enable

Encryption Mode : ● Static ○ TLS

Port : 1194 (1-65535)

Tunnel Protocol : UDP

Encryption Cipher : Blowfish CBC

Hash Algorithm : SHA1

ping-timer-rem : ● Enable ○ Disable

persist-tun : ● Enable ○ Disable

persist-key : ● Enable ○ Disable

Use LZO Compression : ○ Enable ● Disable

Keepalive : ● Enable ○ Disable

Ping Interval : 10 (1-99999 seconds)

Retry Timeout : 60 (1-99999 seconds)

ifconfig : Local : 10.8.0.1 Remote : 10.8.0.2

Route : IP : 0.0.0.0 MASK : 0.0.0.0

Save Log File :

The description of the columns is as below:

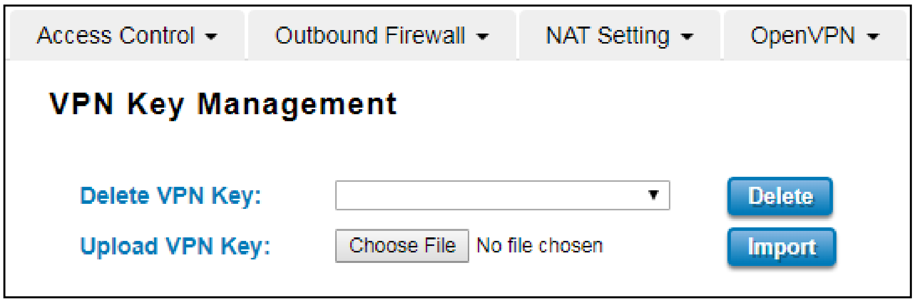
TERMS	DESCRIPTION
Enable VPN Server	Select Enable to activate the VPN Server function
Encryption Mode	Choose the Encryption Mode Static Key: Use a pre-shared static key. TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server 1	Type the IP Address of the VPN Server
Server 2	Type the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

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

Click **Submit** to apply the configuration.

OpenVPN Certificate

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



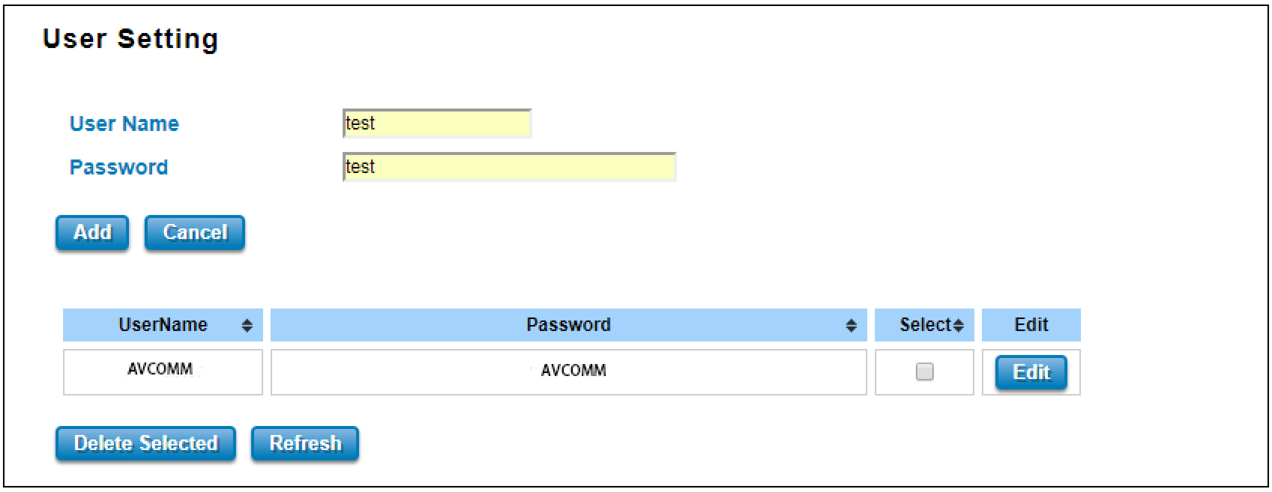
VPN Key Management

Delete VPN Key: Delete

Upload VPN Key: Choose File No file chosen Import

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



User Setting

User Name: test

Password: test

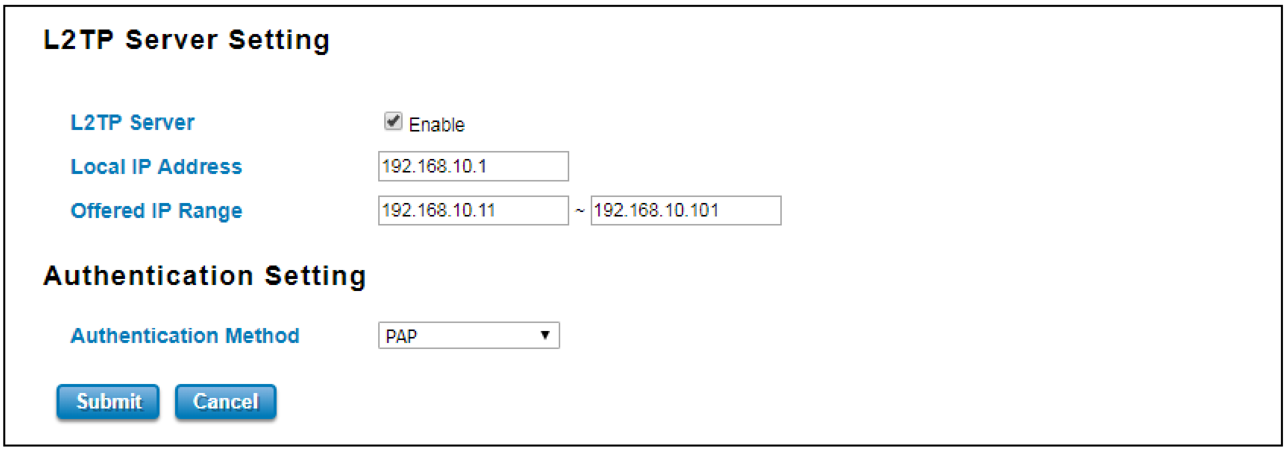
Add Cancel

UserName	Password	Select	Edit
AVCOMM	AVCOMM	□	Edit

Delete Selected Refresh

3.6.5 L2TP SETTING

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



L2TP Server Setting

L2TP Server ☑ Enable

Local IP Address 192.168.10.1

Offered IP Range 192.168.10.11 ~ 192.168.10.101

Authentication Setting

Authentication Method PAP

The description of the column is as below:

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

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

Below is the User Setting for the L2TP Authentication connection.

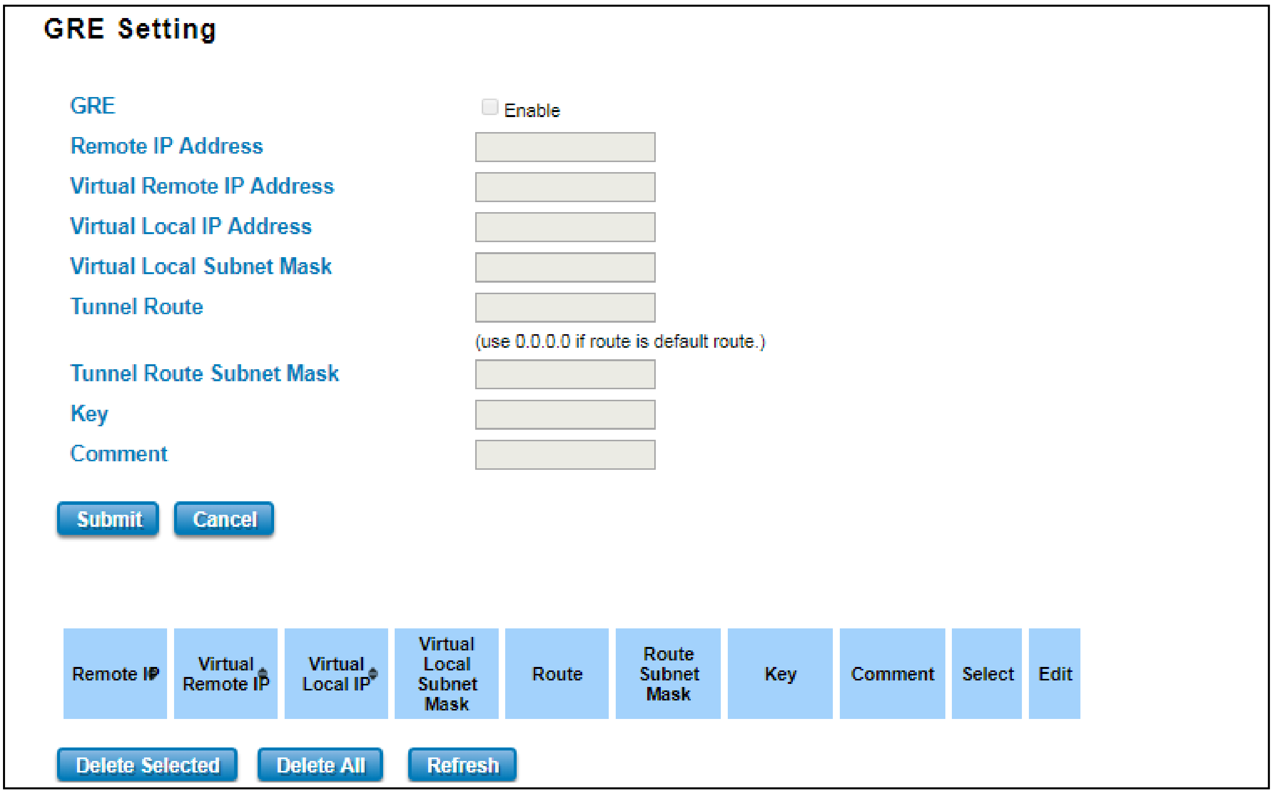
The description of the column is as below:

TERMS	DESCRIPTION
User Name	Username for L2TP connection
Password	Password for L2TP connection
Select	Select the list on the table, so user can press **Edit** or **Delete Selected** to delete.

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

3.6.6 GRE SETTING

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



GRE Setting

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

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

The description of the column is as below:

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

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

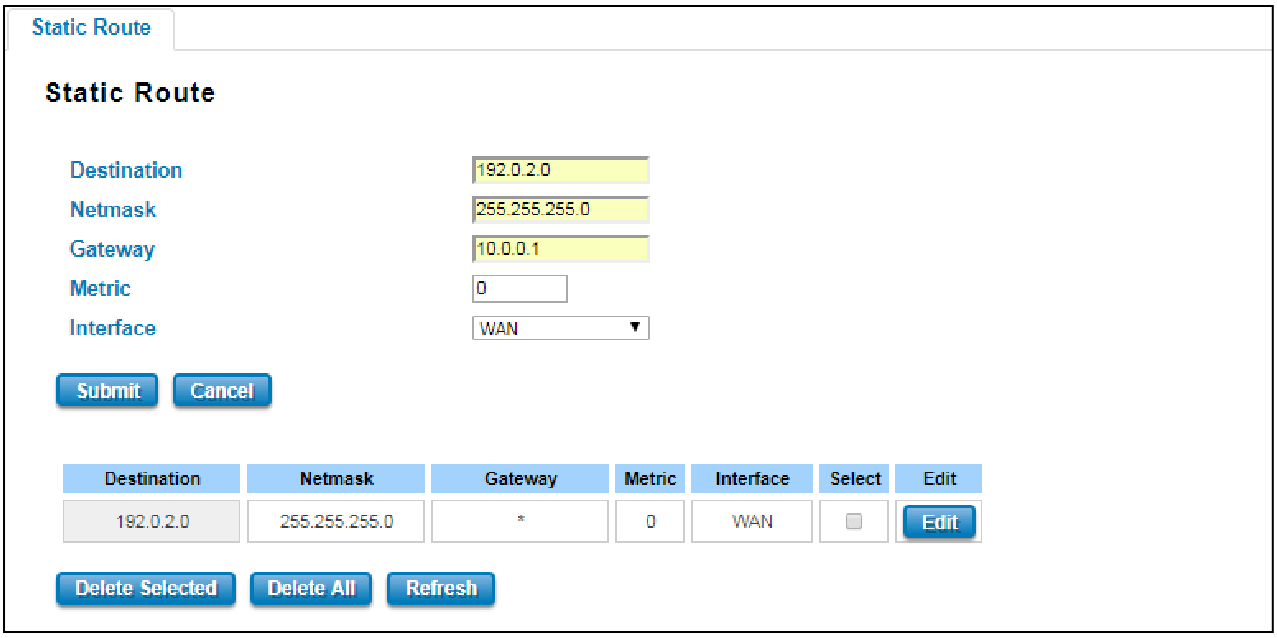
3.7 ROUTING

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

3.7.1 STATIC ROUTE

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

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



Static Route

Destination	192.0.2.0
Netmask	255.255.255.0
Gateway	10.0.0.1
Metric	0
Interface	WAN

Destination	Netmask	Gateway	Metric	Interface	Select	Edit
192.0.2.0	255.255.255.0	*	0	WAN	☐	Edit

The description of the column is as below:

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

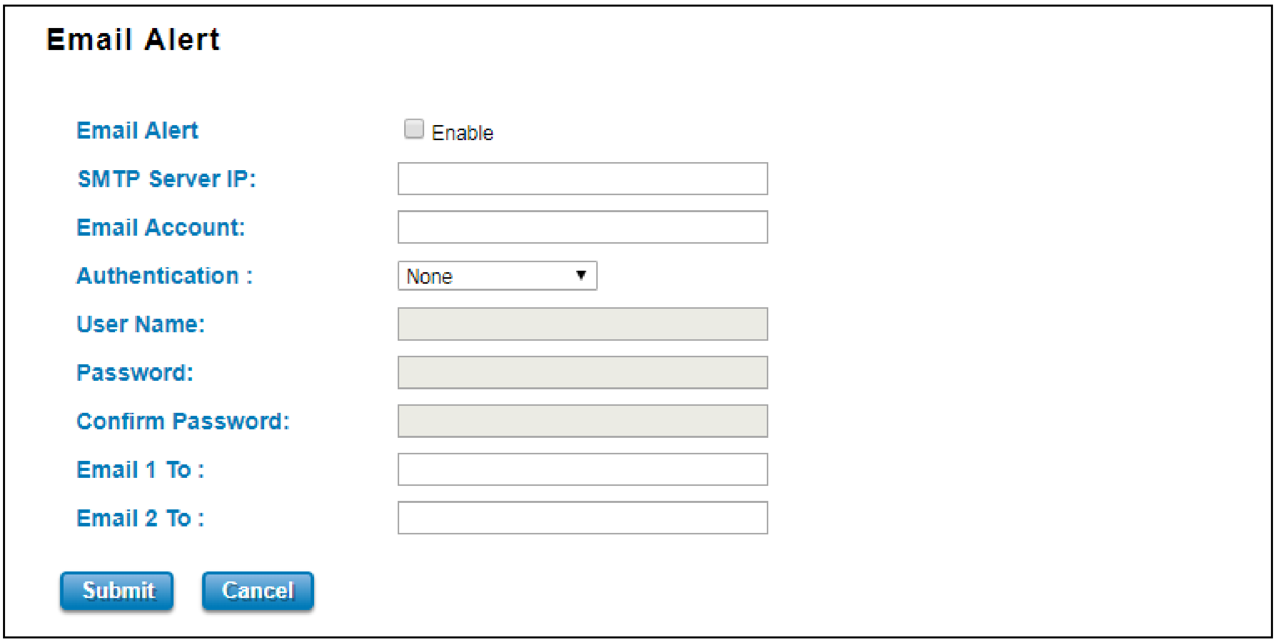
Click the **Refresh** button to refresh the list.

3.8 WARNING

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

3.8.1 EMAIL ALERT

AVCOMM 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.



Email Alert

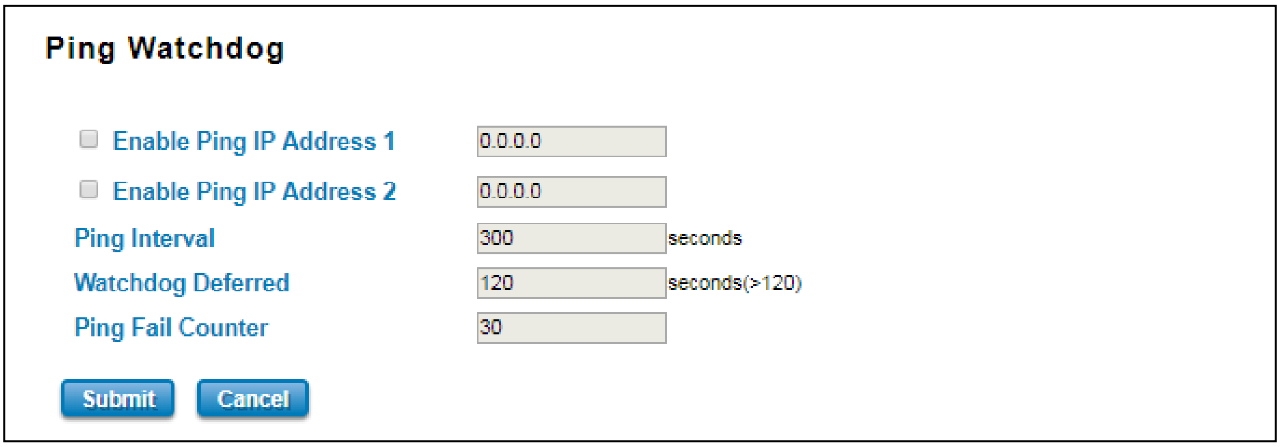
Email Alert	☐ Enable
SMTP Server IP:	
Email Account:	
Authentication :	None ▼
User Name:	
Password:	
Confirm Password:	
Email 1 To :	
Email 2 To :	

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.

3.8.2 PING WATCHDOG



Ping Watchdog

□ Enable Ping IP Address 1 0.0.0.0

□ Enable Ping IP Address 2 0.0.0.0

Ping Interval 300 seconds

Watchdog Deferred 120 seconds(>120)

Ping Fail Counter 30

Ping Watchdog is a feature that helps AVCOMM' 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, AVCOMM provides two target IP Addresses, in order if the other IP Address cannot be reached, so there is another backup IP address. There are two conditions in this Ping Watchdog section, the first one is when the device continuously ping the target IP and in the end, it can reach one of the target IPs the device would not reboot. But if both targets IPs cannot be reached, the device will start counting the Ping Fail Counter time till it can be reached. If it is unable to ping the target IP address, this device will automatically reboot. After User finishes configuring the settings, click on **Submit** to apply User configuration.

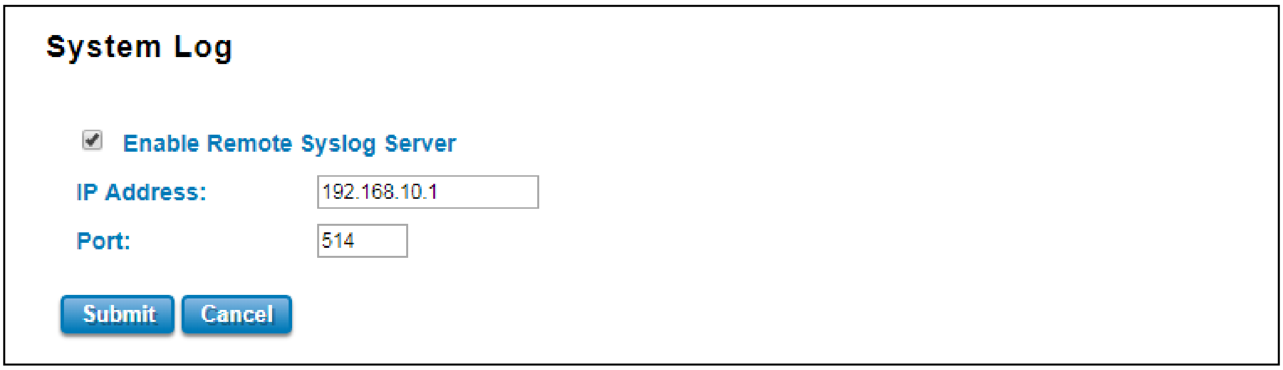
The description of the columns is as below:

TERMS	DESCRIPTION
Enable Ping IP Address 1	Clicks enable to activate the feature. Set the first IP Address to check if the device is alive or not
Enable Ping IP Address 2	Clicks enable to activate the feature. Set the second IP Address to check if the device is alive or not
Ping Interval	**Default: 300 (seconds)** Set the interval timer to Ping the remote device. Every 300 seconds the device will try to ping the target IP.
Watchdog Deferred	**Default: 120 (seconds) >120** The device needs time to boot, the startup delay use to buffer to prevent the device continue to reboot itself.
Ping Fail Counter	**Default: 30** When the remaining Ping Fail Counter reach to 0 or reach the failure count, the device will reboot.

Click **Submit** to apply the configuration.

3.8.3 SYSLOG SETTING

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



System Log

☑ Enable Remote Syslog Server

IP Address: 192.168.10.1

Port: 514

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

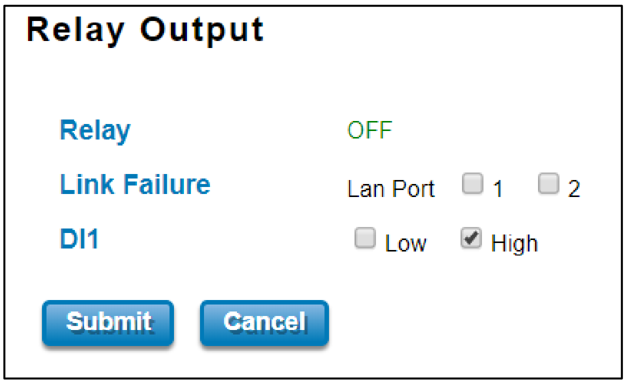
The condition or term described as following table.

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.

3.8.4 RELAY OUTPUT

AVCOMM' router provides 1 Digital Output. The Digital Output configuration interface has shown as below:



Relay Output

Relay OFF

Link Failure Lan Port □ 1 □ 2

DI1 □ Low ☑ High

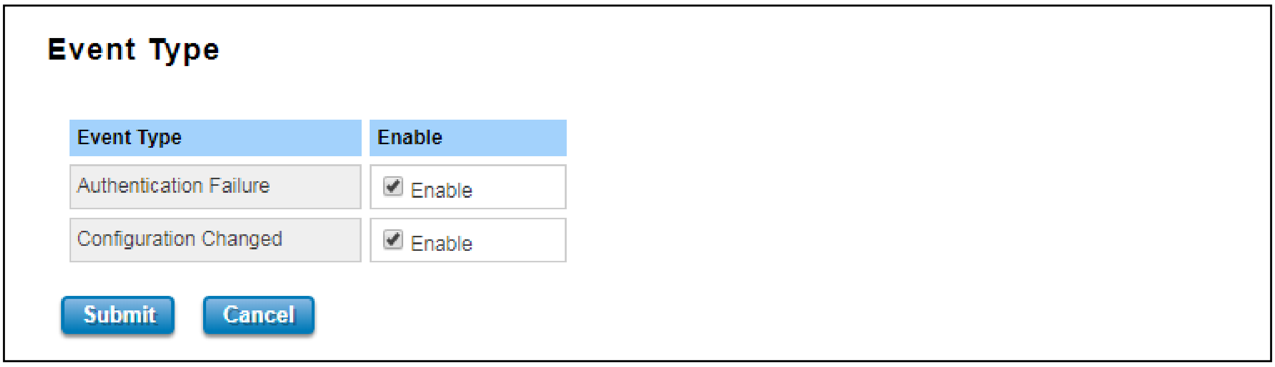
The condition or term described as following table.

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

3.8.5 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.



Event Type

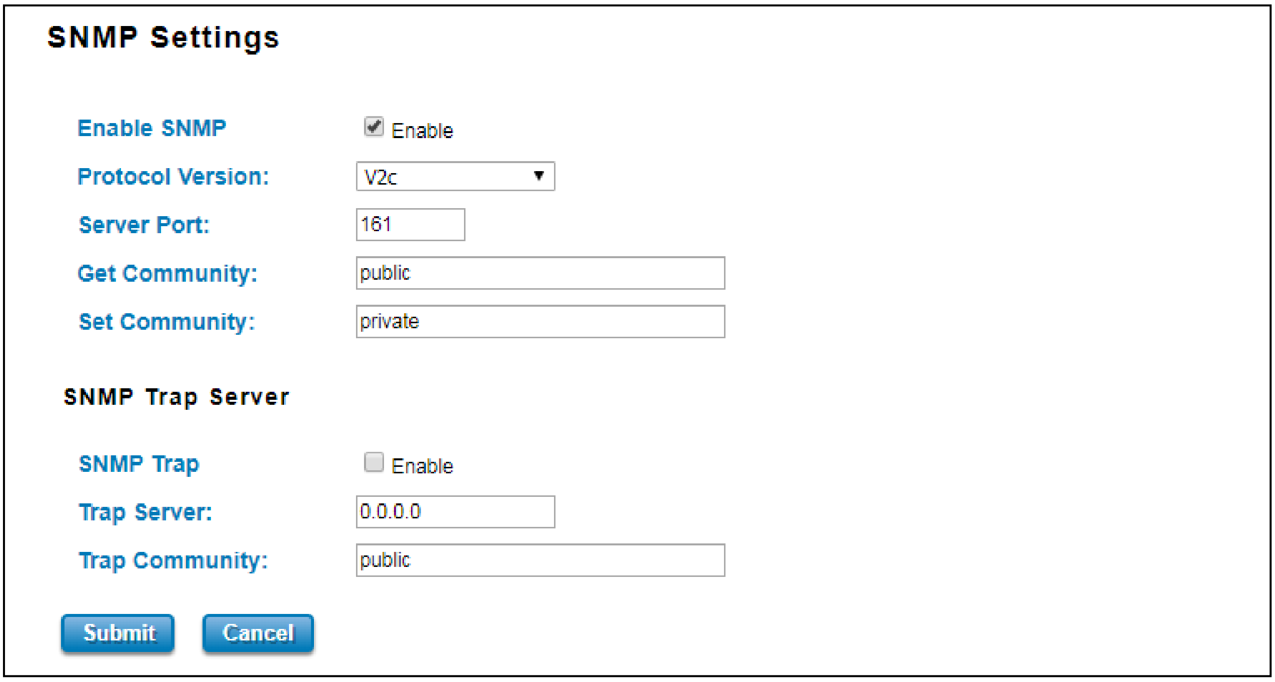
Event Type	Enable
Authentication Failure	☑ Enable
Configuration Changed	☑ Enable

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.

3.8.6 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. AVCOMM' Router support SNMP V2c and V3



SNMP Settings

Enable SNMP	☑ Enable
Protocol Version:	V2c ▾
Server Port:	161
Get Community:	public
Set Community:	private

SNMP Trap Server

SNMP Trap	□ Enable
Trap Server:	0.0.0.0
Trap Community:	public

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.

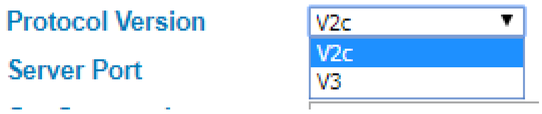
SNMP V3

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.  Protocol Version V2c Server Port V2c V3
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:

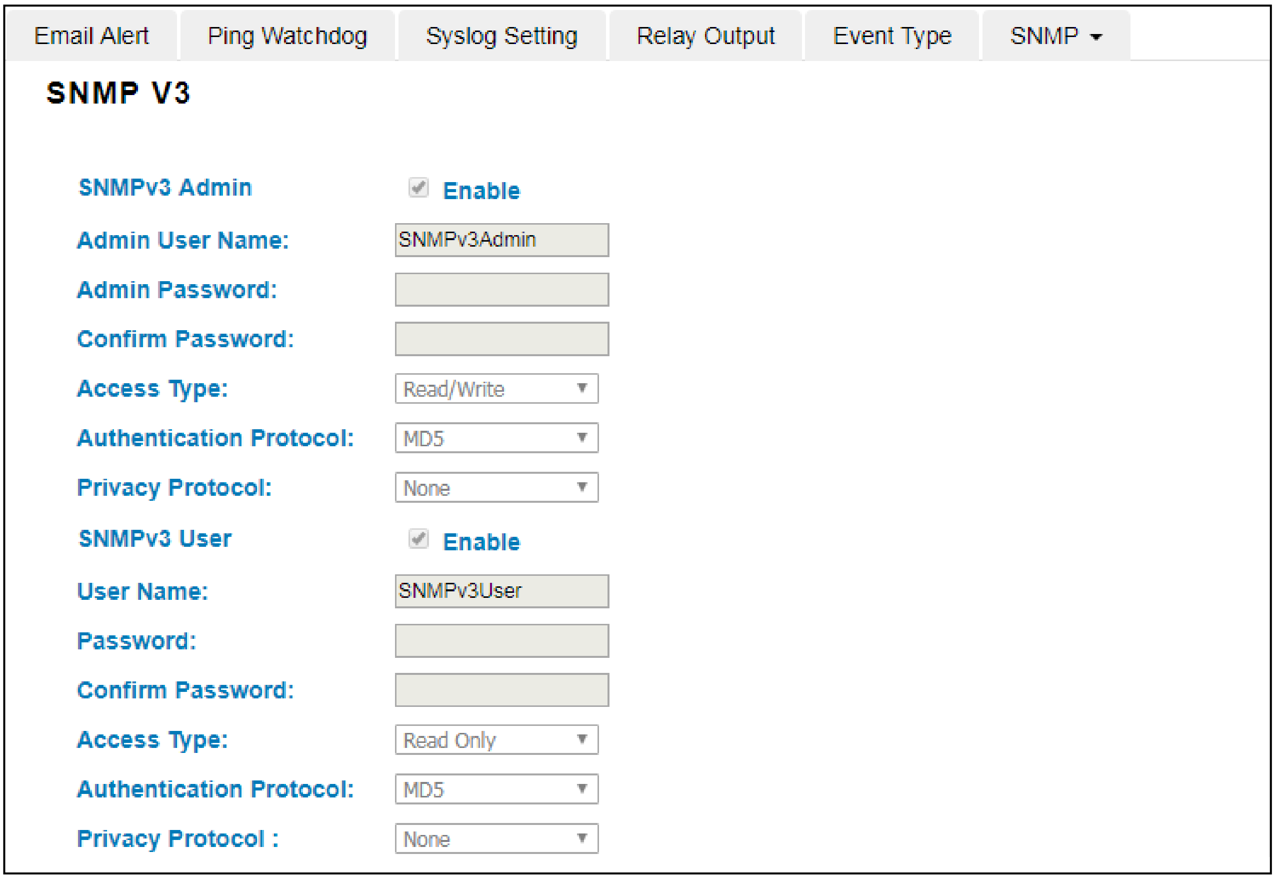
TERMS	DESCRIPTION

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.



SNMP V3

SNMPv3 Admin ☑ Enable
Admin User Name: SNMPv3Admin
Admin Password:
Confirm Password:
Access Type: Read/Write
Authentication Protocol: MD5
Privacy Protocol: None
SNMPv3 User ☑ Enable
User Name: SNMPv3User
Password:
Confirm Password:
Access Type: Read Only
Authentication Protocol: MD5
Privacy Protocol : None

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.

3.9 DIAGNOSTICS

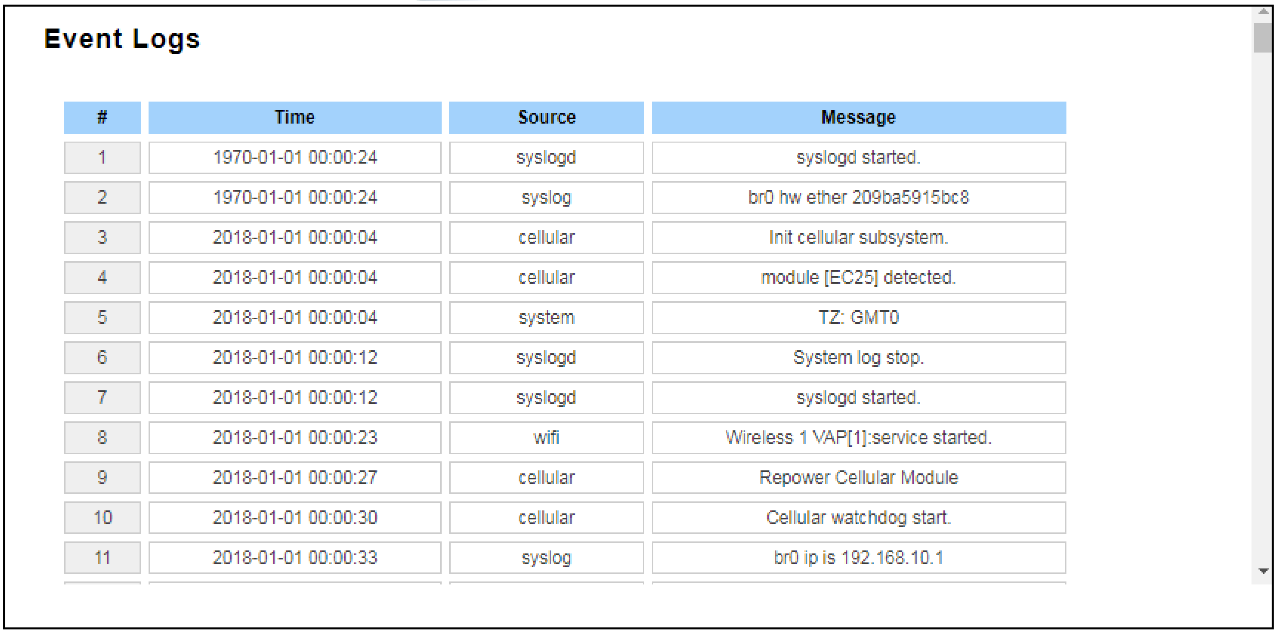
AVCOMM Router provides several types of features for User to monitor the status of the router or diagnostic for User to check the problem when encountering problems related to the router.

Following commands are included in this group:

3.9.1 Event Logs
3.9.2 ARP Table
3.9.3 Ping
3.9.4 Traceroute
3.9.5 Network Statistic
3.9.6 Client Association List

3.9.1 EVENT LOGS

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



Event Logs

#	Time	Source	Message
1	1970-01-01 00:00:24	syslogd	syslogd started.
2	1970-01-01 00:00:24	syslog	br0 hw ether 209ba5915bc8
3	2018-01-01 00:00:04	cellular	Init cellular subsystem.
4	2018-01-01 00:00:04	cellular	module [EC25] detected.
5	2018-01-01 00:00:04	system	TZ: GMT0
6	2018-01-01 00:00:12	syslogd	System log stop.
7	2018-01-01 00:00:12	syslogd	syslogd started.
8	2018-01-01 00:00:23	wifi	Wireless 1 VAP[1]:service started.
9	2018-01-01 00:00:27	cellular	Repower Cellular Module
10	2018-01-01 00:00:30	cellular	Cellular watchdog start.
11	2018-01-01 00:00:33	syslog	br0 ip is 192.168.10.1

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**.

3.9.2 ARP TABLE

Basically, AVCOMM 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.

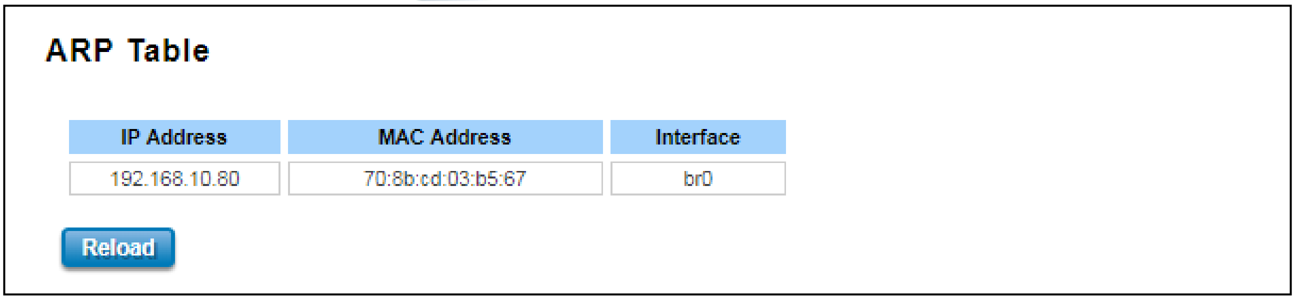
Data Format

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.



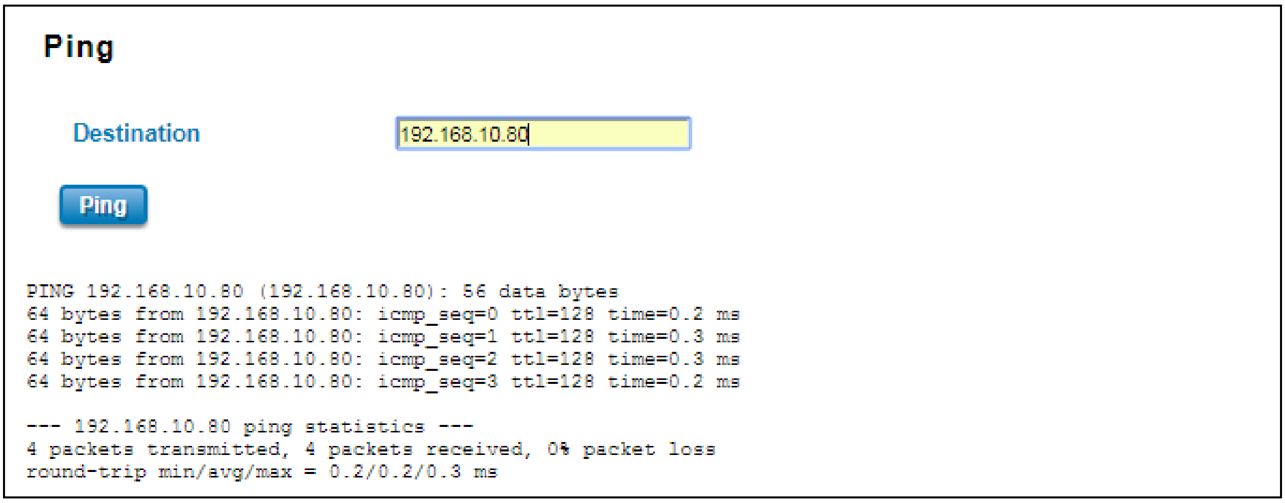
ARP Table

IP Address	MAC Address	Interface
192.168.10.80	70:8b:cd:03:b5:67	br0

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

3.9.3 PING

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



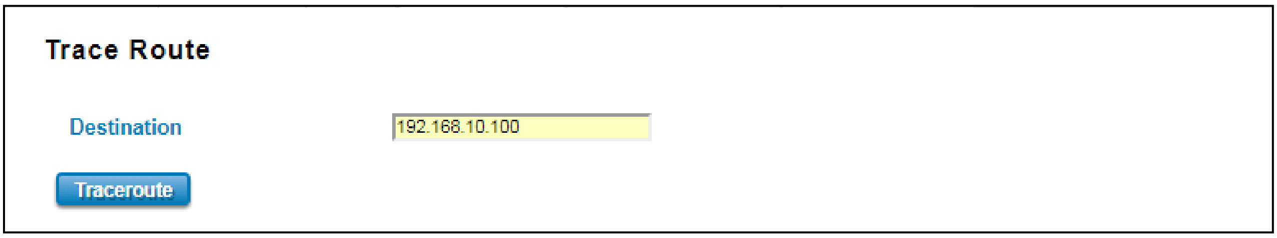
Ping

Destination: 192.168.10.80

```
PING 192.168.10.80 (192.168.10.80): 56 data bytes
64 bytes from 192.168.10.80: icmp_seq=0 ttl=128 time=0.2 ms
64 bytes from 192.168.10.80: icmp_seq=1 ttl=128 time=0.3 ms
64 bytes from 192.168.10.80: icmp_seq=2 ttl=128 time=0.3 ms
64 bytes from 192.168.10.80: icmp_seq=3 ttl=128 time=0.2 ms

--- 192.168.10.80 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.3 ms
```

3.9.4 TRACEROUTE

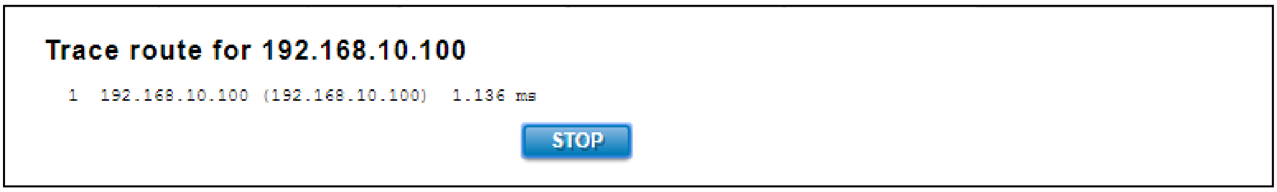
Traceroute is a diagnostics tool for displaying the route (path) and measuring transit delays of packets across an Internet IP network. Log containing route information will be shown after few seconds. Enter the destination IP Address then click traceroute to start the process.



Trace Route

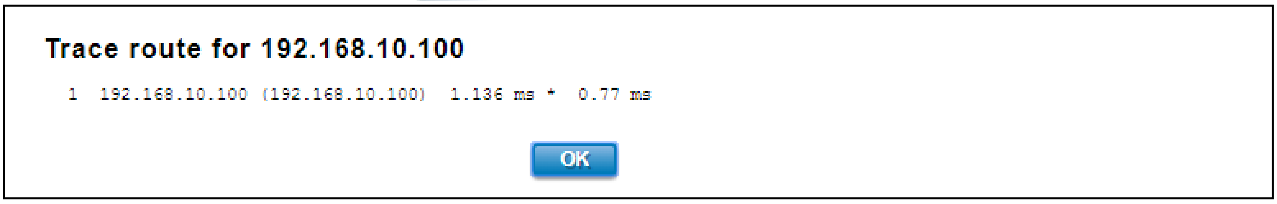
Destination: 192.168.10.100

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



Trace route for 192.168.10.100

```
1  192.168.10.100 (192.168.10.100)  1.136 ms
```

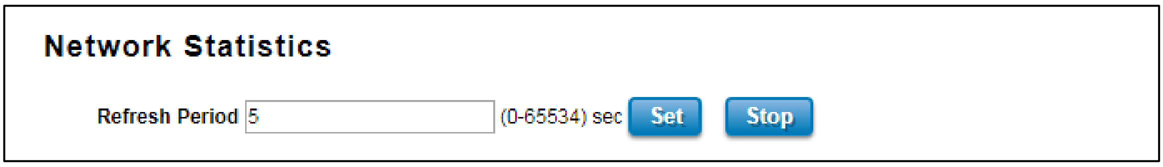


Trace route for 192.168.10.100

```
1  192.168.10.100 (192.168.10.100)  1.136 ms *  0.77 ms
```

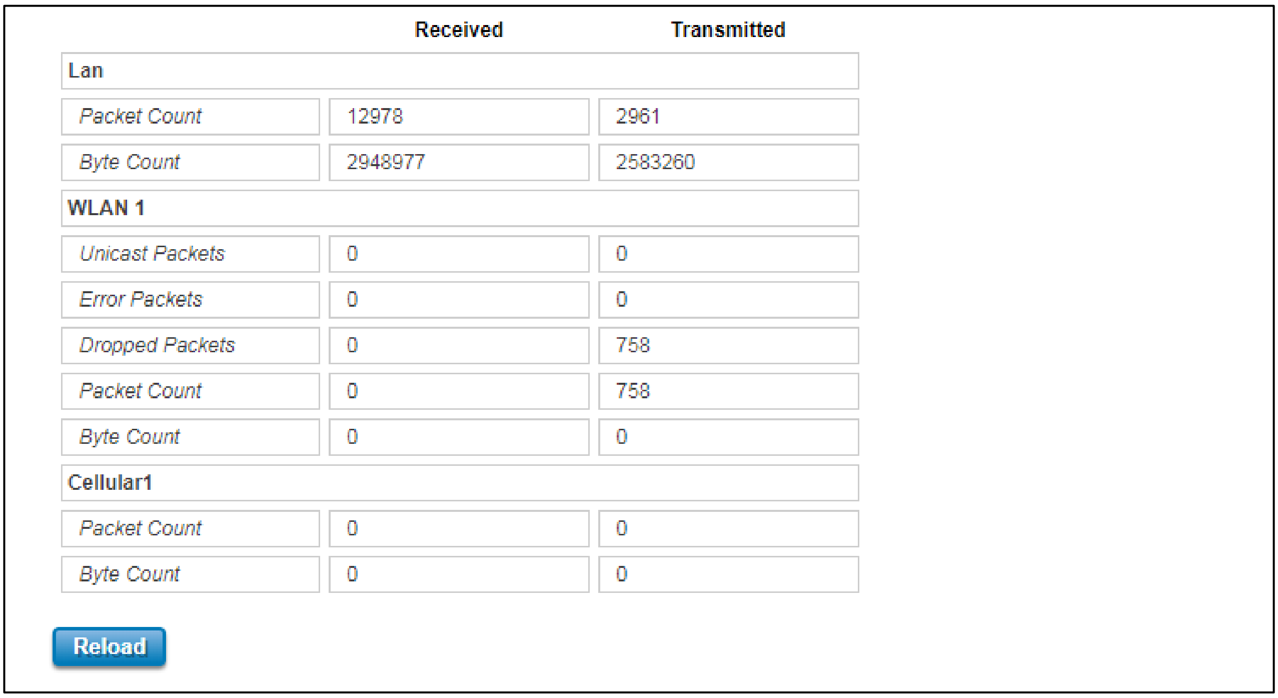
3.9.5 NETWORK STATISTICS

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



Network Statistics

Refresh Period 5 (0-65534) sec



	Received	Transmitted
Lan		
Packet Count	12978	2961
Byte Count	2948977	2583260
WLAN 1		
Unicast Packets	0	0
Error Packets	0	0
Dropped Packets	0	758
Packet Count	0	758
Byte Count	0	0
Cellular1		
Packet Count	0	0
Byte Count	0	0

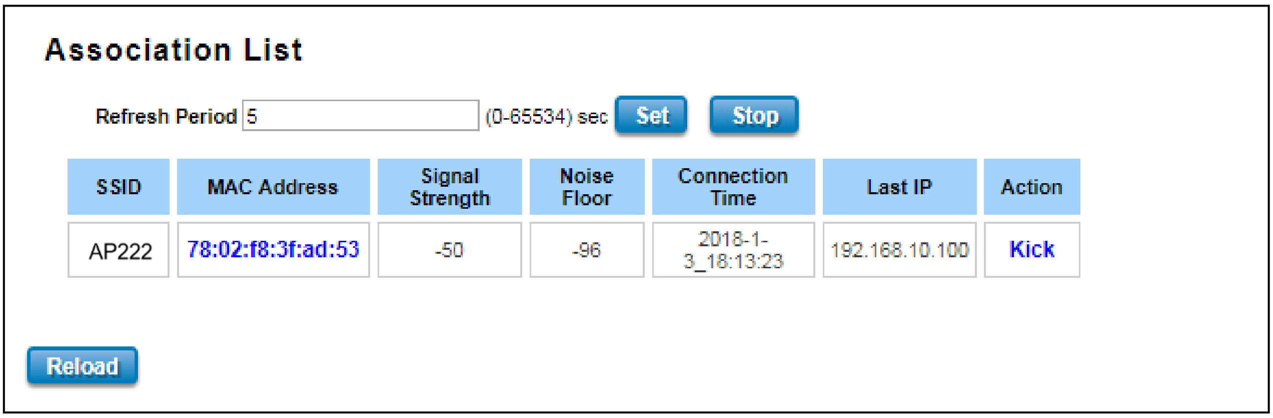
Click on **Reload** to refresh the table.

The description of the columns is as below:

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

3.9.6 CLIENT ASSOCIATION LIST

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



Association List

Refresh Period 5 (0-65534) sec

SSID	MAC Address	Signal Strength	Noise Floor	Connection Time	Last IP	Action
AP222	78:02:f8:3f:ad:53	-50	-96	2018-1-3_18:13:23	192.168.10.100	Kick

Click **Reload** to refresh the list.

The description of the columns is as below:

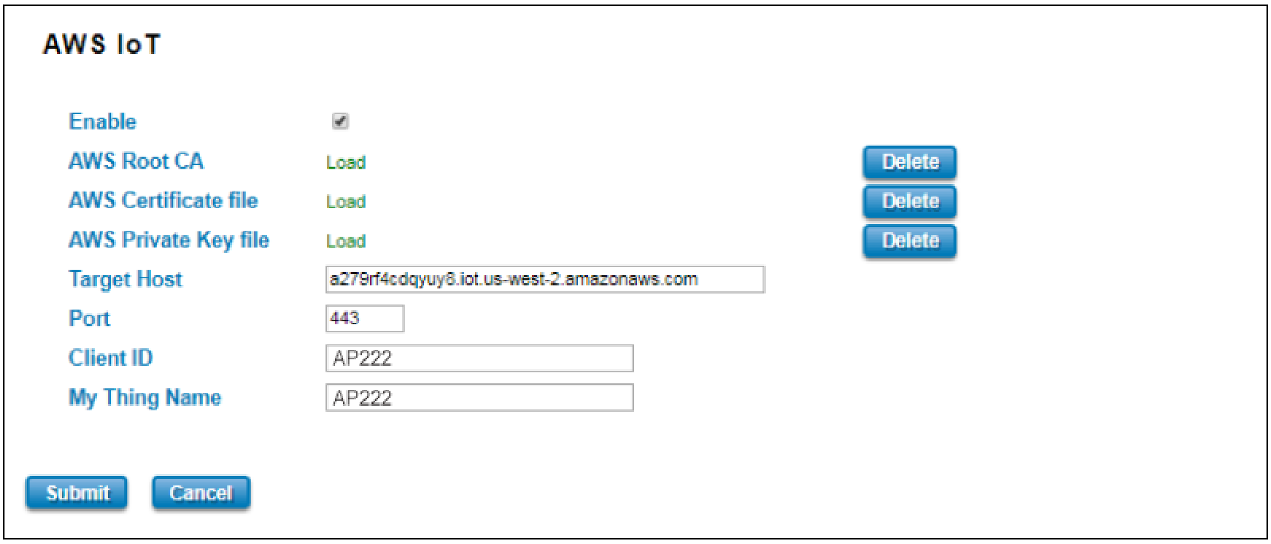
TERMS	DESCRIPTION
SSID	Display the primary name of the SSID that available on the network.
MAC Address	Display the MAC Address that connected to the AP.
Signal Strength	Display the connection signal strength.
Noise Floor	Display the background noise level.
Connection Time	Display the time when the client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

3.10 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. AVCOMM Industrial Router is supported with private clouds ATMS 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.

3.10.1 AWS IoT

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



AWS IoT

Enable	☑	
AWS Root CA	Load	Delete
AWS Certificate file	Load	Delete
AWS Private Key file	Load	Delete
Target Host	a279rf4cdqyuy8.iot.us-west-2.amazonaws.com	
Port	443	
Client ID	AP222	
My Thing Name	AP222	

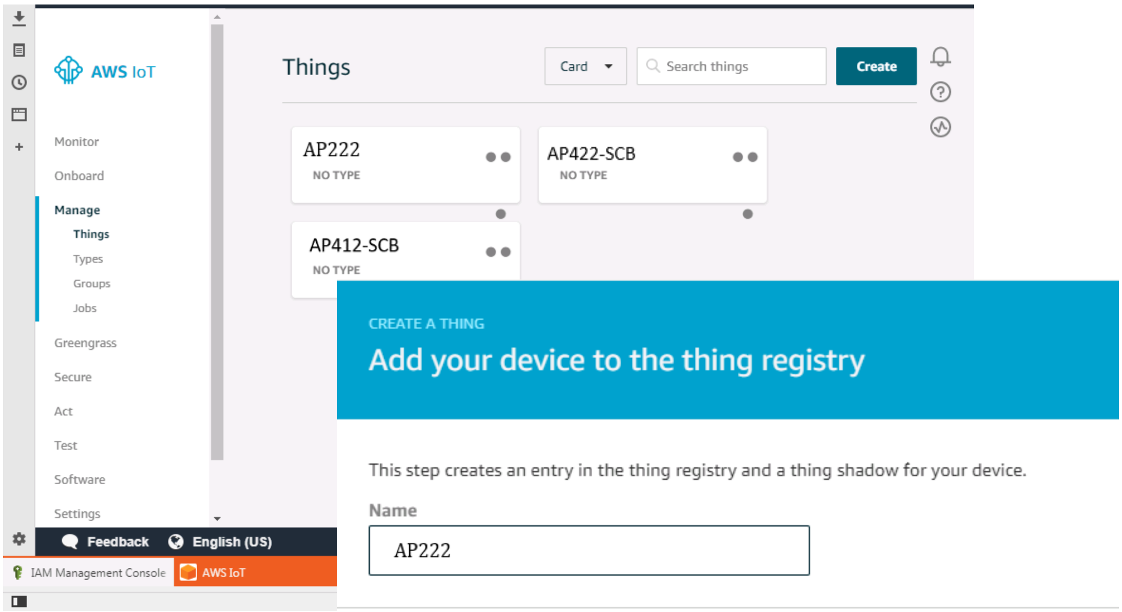
The description of the columns is as below:

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

Click **Submit** to apply the configuration.

HOW TO CONNECT THE DEVICE TO AWS

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

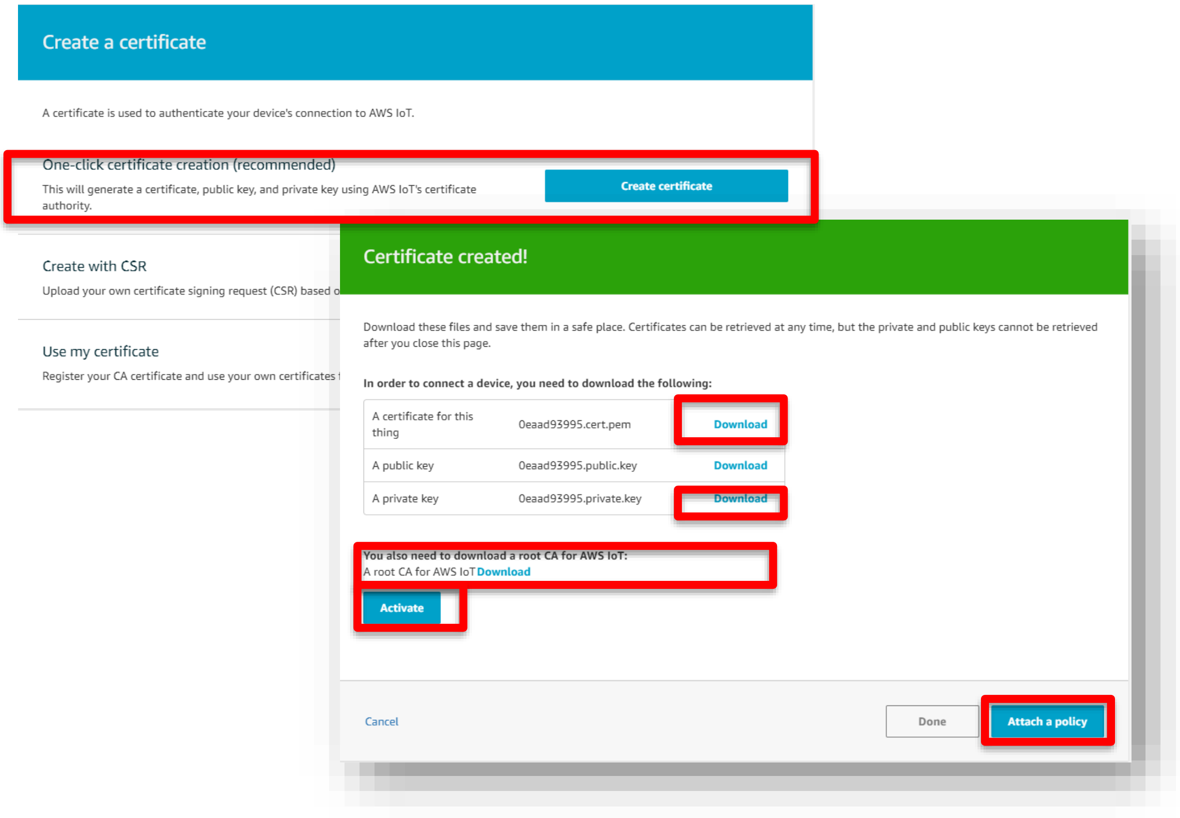


Add your device to the thing registry

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

Name: AP222

- Create and download the key or certificate.



Create a certificate

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

One-click certificate creation (recommended)
This will generate a certificate, public key, and private key using AWS IoT's certificate authority.

Create with CSR
Upload your own certificate signing request (CSR) based o

Use my certificate
Register your CA certificate and use your own certificates

Certificate created!

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

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

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

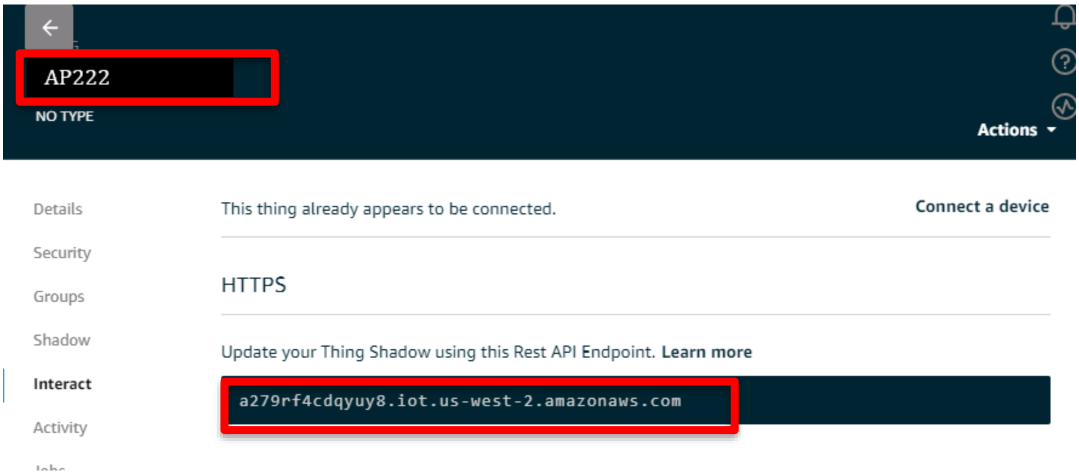
You also need to download a root CA for AWS IoT:
A root CA for AWS IoT Download

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

- Get the Target host to connect with the device.

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

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



This thing already appears to be connected.

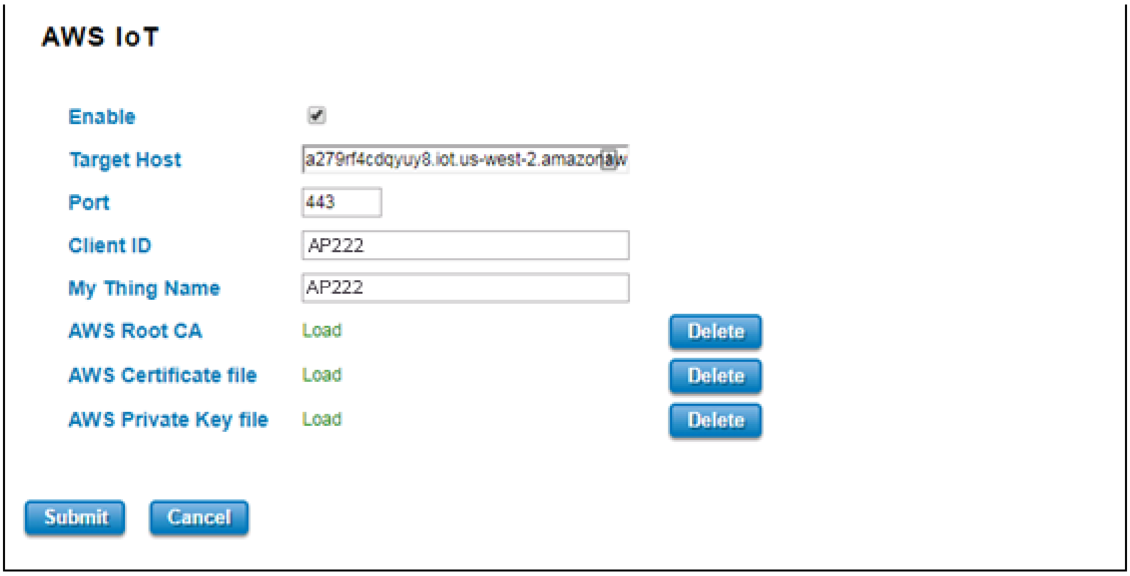
HTTPS

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

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

- Connect the device to AWS.

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



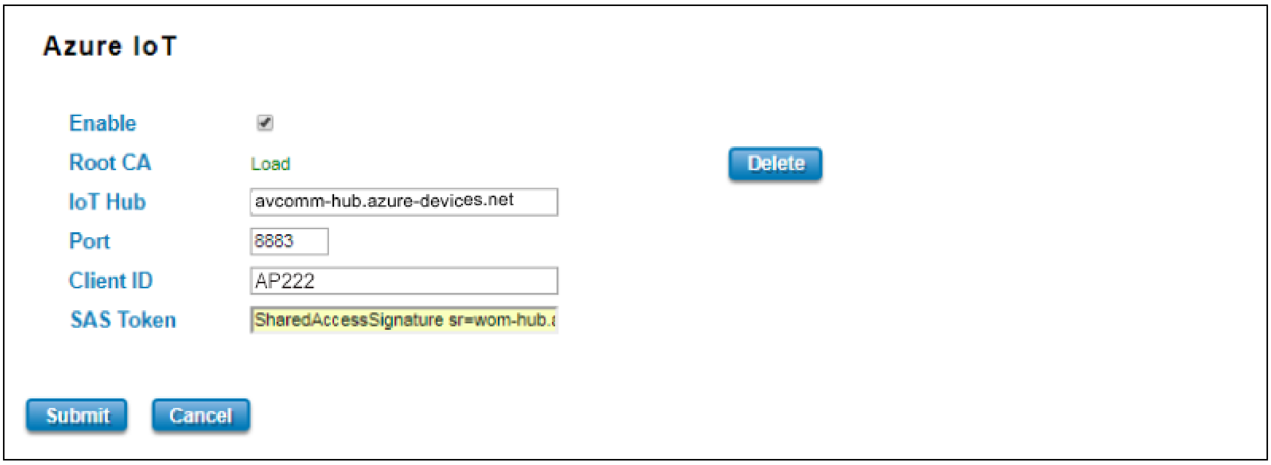
AWS IoT

Enable	☑
Target Host	a279rf4cdqyuy8.iot.us-west-2.amazonaw
Port	443
Client ID	AP222
My Thing Name	AP222
AWS Root CA	Load Delete
AWS Certificate file	Load Delete
AWS Private Key file	Load Delete

3.10.2 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.



Azure IoT

Enable ☑
Root CA Load
IoT Hub avcomm-hub.azure-devices.net
Port 8883
Client ID AP222
SAS Token SharedAccessSignature sr=wom-hub.(

- Includes the most popular communication protocols.

The description of the columns is as below:

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

Click **Submit** to apply the configuration.

HOW TO CONNECT THE DEVICE TO MICROSOFT AZURE

CREATE IOT HUB

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

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

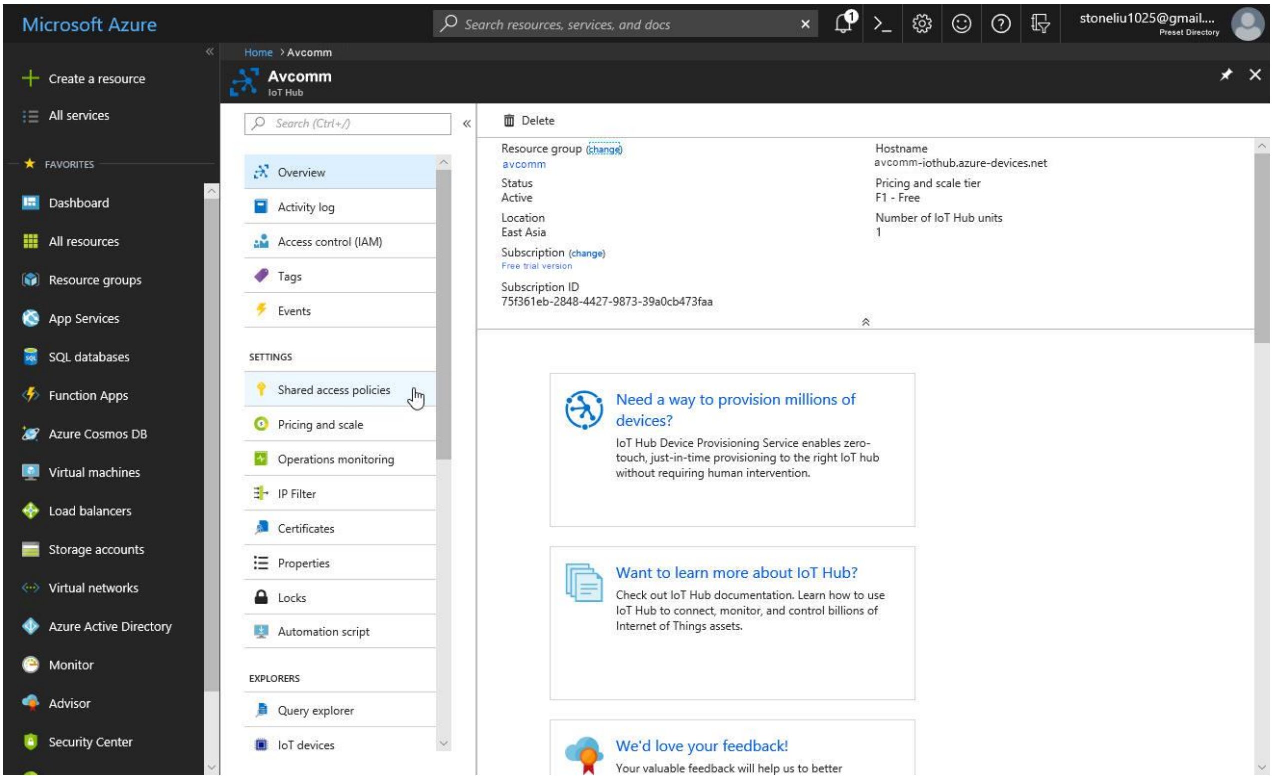
CONFIGURE THE DEVICE AS A MQTT CLIENT

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

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

User has to annotate the value of this field.

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



Resource group (change)
avcomm

Status
Active

Location
East Asia

Subscription (change)
Free trial version

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

Hostname
avcomm-iothub.azure-devices.net

Pricing and scale tier
F1 - Free

Number of IoT Hub units
1

Need a way to provision millions of devices?

IoT Hub Device Provisioning Service enables zero-touch, just-in-time provisioning to the right IoT hub without requiring human intervention.

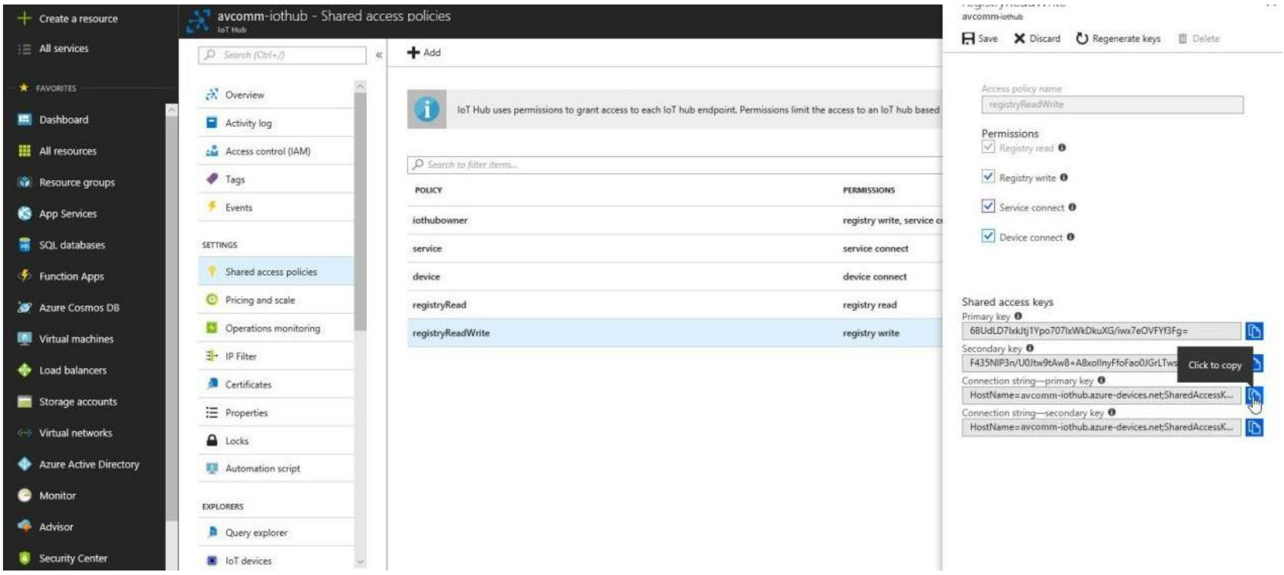
Want to learn more about IoT Hub?

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

We'd love your feedback!

Your valuable feedback will help us to better

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



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

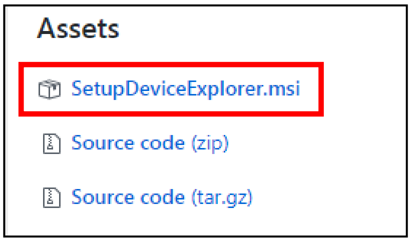
POLICY	PERMISSIONS
iothubowner	registry write, service c
service	service connect
device	device connect
registryRead	registry read
registryReadWrite	registry write

Access policy name
registryReadWrite

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

Shared access keys
Primary key
6BUdLD7lxkJtj1Ypo707lxWkDkuXG/iwx7eOVFYf3Fg=
Secondary key
F435NIP3n/U0Jtw9tAw8+A8xollnyFfoFao0JGrLTws
Connection string—primary key
HostName=avcomm-iothub.azure-devices.net;SharedAccessK...
Connection string—secondary key
HostName=avcomm-iothub.azure-devices.net;SharedAccessK...

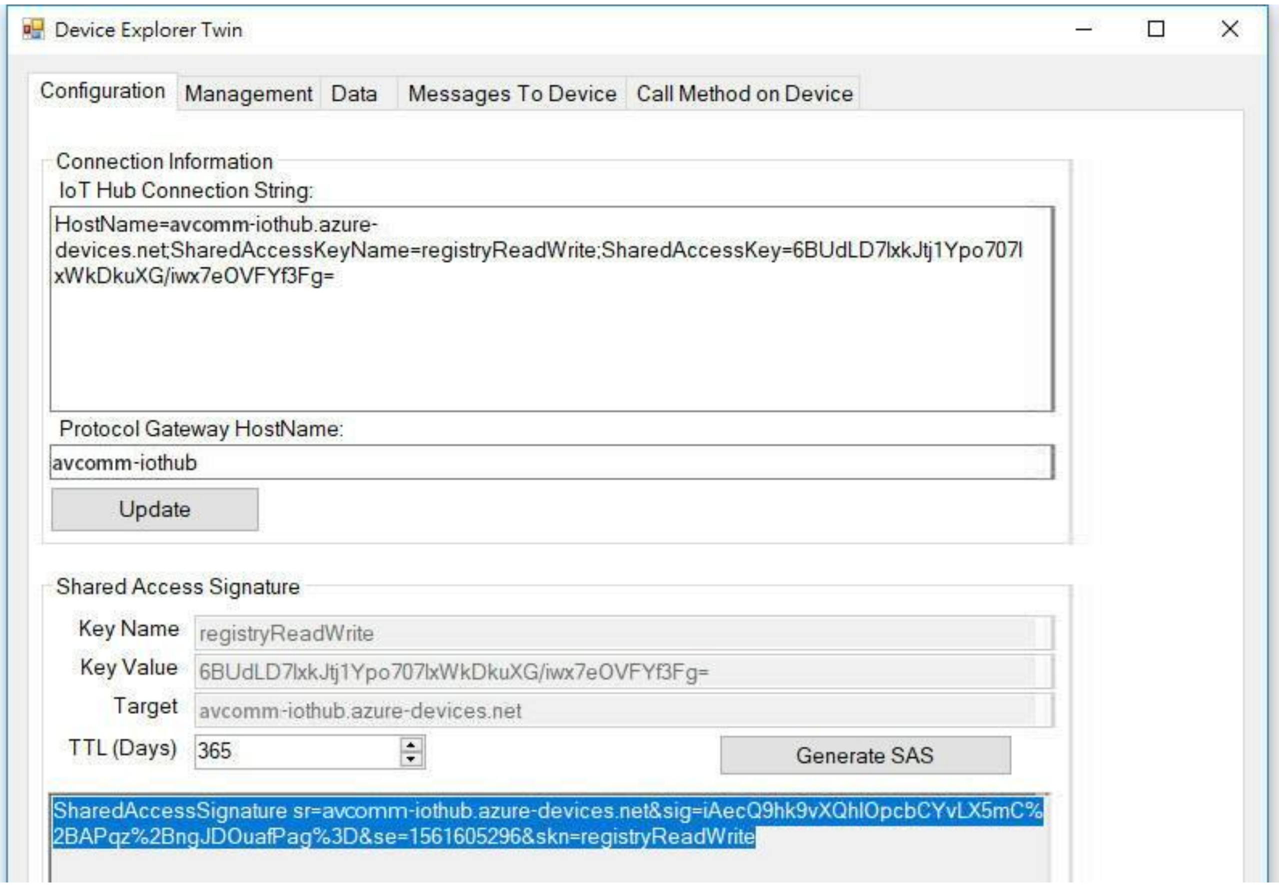
3. Download and install the Azure Device Explorer to generate the SAS Token. Go to this link to download the software: https://github.com/Azure/azure-iot-sdk-csharp/releases/download/2018-3-13/SetupDeviceExplorer.msi



Assets

- SetupDeviceExplorer.msi
- Source code (zip)
- Source code (tar.gz)

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



IoT Hub Connection String:

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

Protocol Gateway HostName: avcomm-iothub

Key Name: registryReadWrite

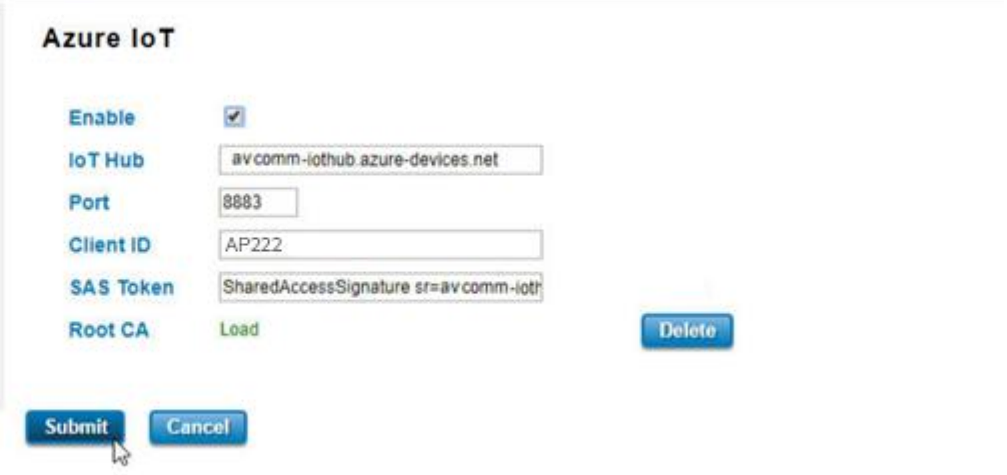
Key Value: 6BUdLD7lxkJtj1Ypo707lxWkDkuXG/iwx7eOVFYf3Fg=

Target: avcomm-iothub.azure-devices.net

TTL (Days): 365

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

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



Azure IoT

Enable ☑

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

Port: 8883

Client ID: AP222

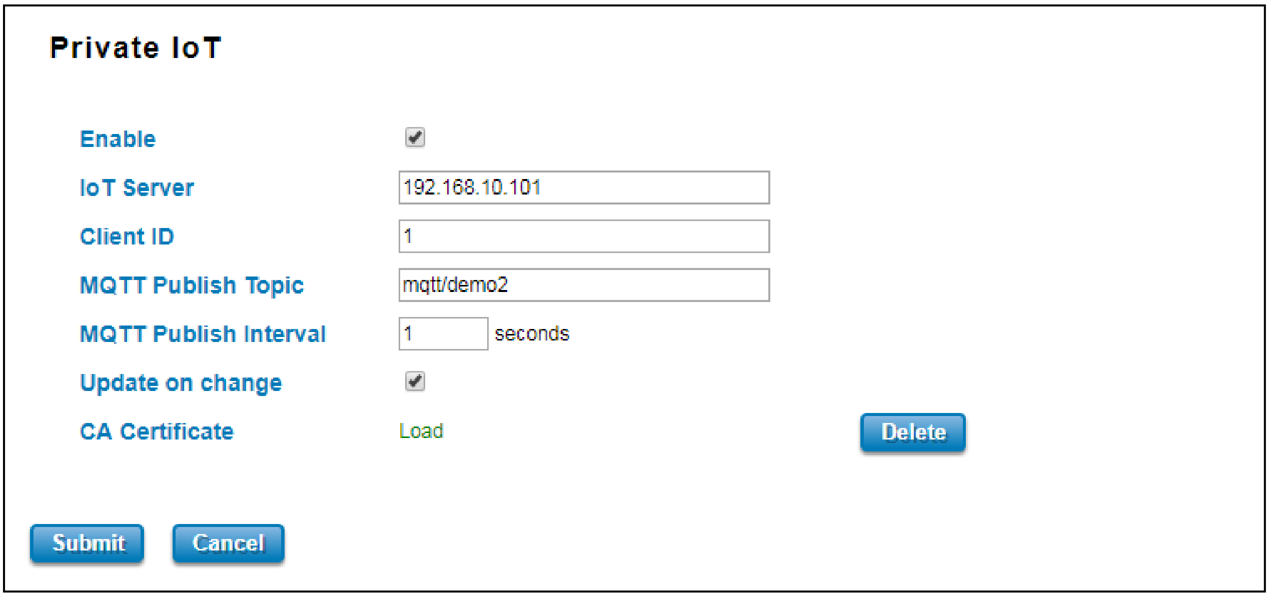
SAS Token: SharedAccessSignature sr=avcomm-ioth

Root CA: Load

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

3.10.3 Private IoT

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



Private IoT

Enable ☑

IoT Server: 192.168.10.101

Client ID: 1

MQTT Publish Topic: mqtt/demo2

MQTT Publish Interval: 1 seconds

Update on change ☑

CA Certificate: Load

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 ATMS server file. **Note. This field only supports in ATMS v1.1 and later version**

Click Submit to apply the configuration.

HOW TO ESTABLISH AND CONNECT TO THE ATMS 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

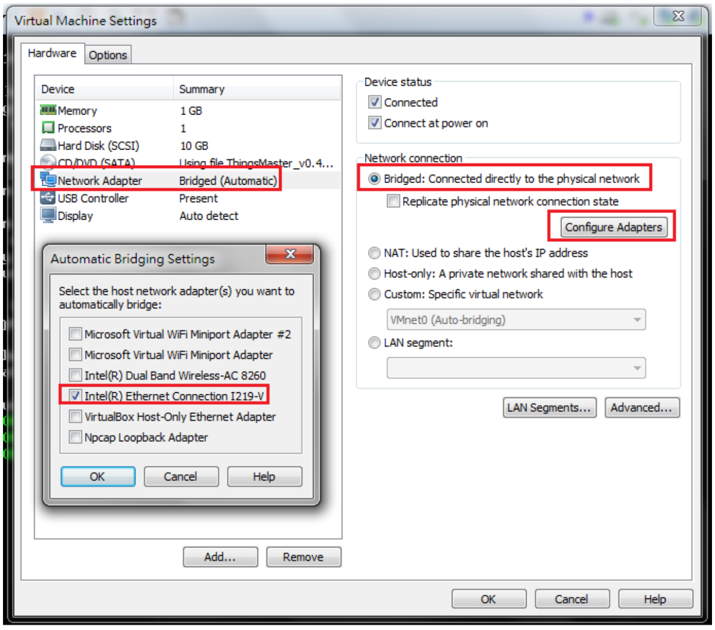
2. Download the server file from the link that sent by the sales.

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 ATMS 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.



Virtual Machine Settings

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

Device status

☑ Connected

☑ Connect at power on

Network connection

● Bridged: Connected directly to the physical network

□ Replicate physical network connection state

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

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

○ Custom: Specific virtual network

VMnet0 (Auto-bridging)

○ LAN segment:

Automatic Bridging Settings

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

□ Microsoft Virtual WiFi Miniport Adapter #2

□ Microsoft Virtual WiFi Miniport Adapter

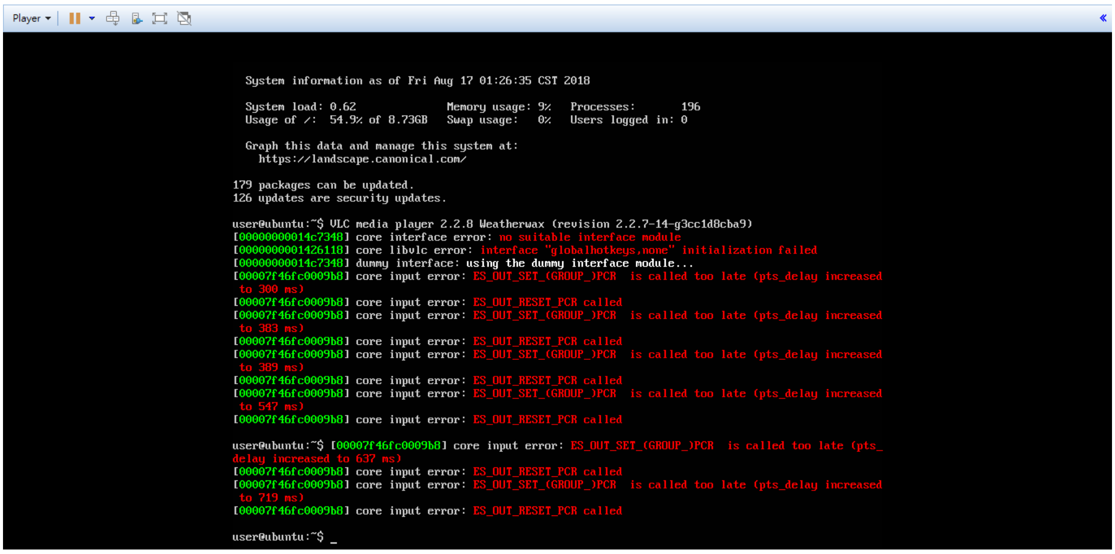
□ Intel(R) Dual Band Wireless-AC 8260

☑ Intel(R) Ethernet Connection I219-V

□ VirtualBox Host-Only Ethernet Adapter

□ Npcap Loopback Adapter

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

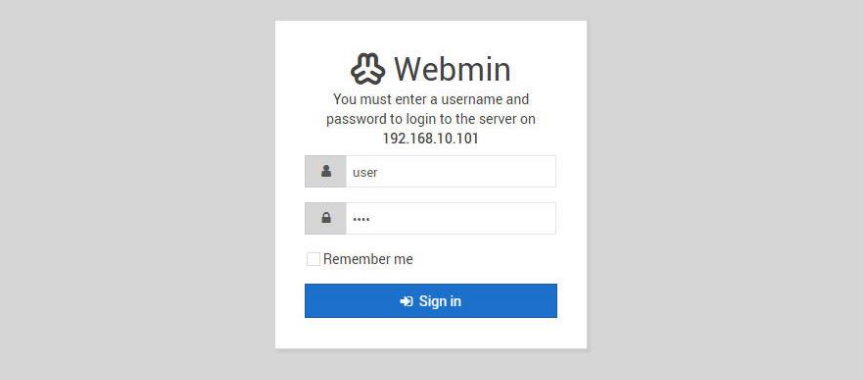


```
  System information as of Fri Aug 17 01:26:35 CST 2018

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

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

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

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

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

user@ubuntu:~$ _
```

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

Default: https://192.168.10.101:10000

User Name/Password: user/user



Webmin

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

user

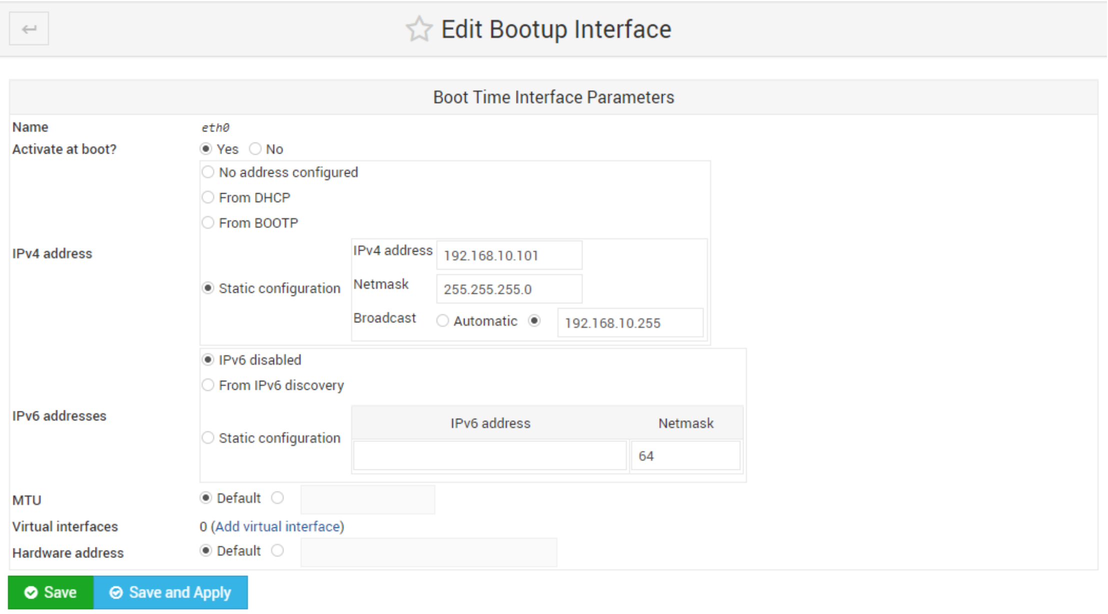
····

□ Remember me

7. Configure the IP address and Gateway (optional).

Select 'eth0' to change IP address and add default gateway if needed.

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



Edit Bootup Interface

Boot Time Interface Parameters

Name: *eth0*

Activate at boot?: ● Yes ○ No

IPv4 address:
○ No address configured
○ From DHCP
○ From BOOTP
● Static configuration — IPv4 address: 192.168.10.101; Netmask: 255.255.255.0; Broadcast: ○ Automatic ● 192.168.10.255

IPv6 addresses:
● IPv6 disabled
○ From IPv6 discovery
○ Static configuration — IPv6 address: ; Netmask: 64

MTU: ● Default ○

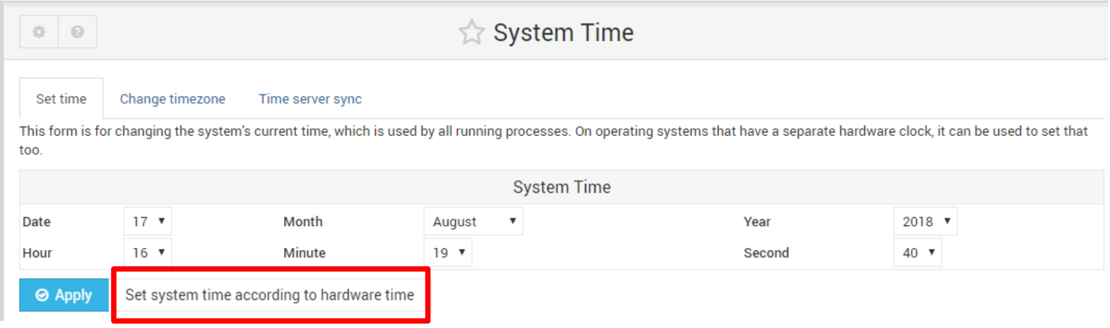
Virtual interfaces: 0 (Add virtual interface)

Hardware address: ● Default ○

8. Configure Date & Time of the ATMS 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.



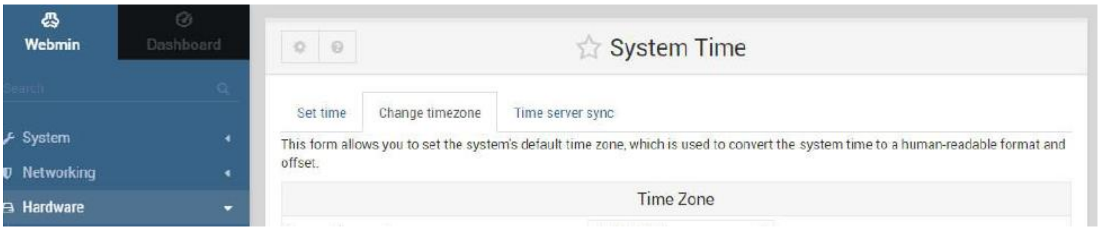
System Time

This form is for changing the system's current time, which is used by all running processes. On operating systems that have a separate hardware clock, it can be used to set that too.

System Time

Date	17	Month	August	Year	2018
Hour	16	Minute	19	Second	40

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



System Time

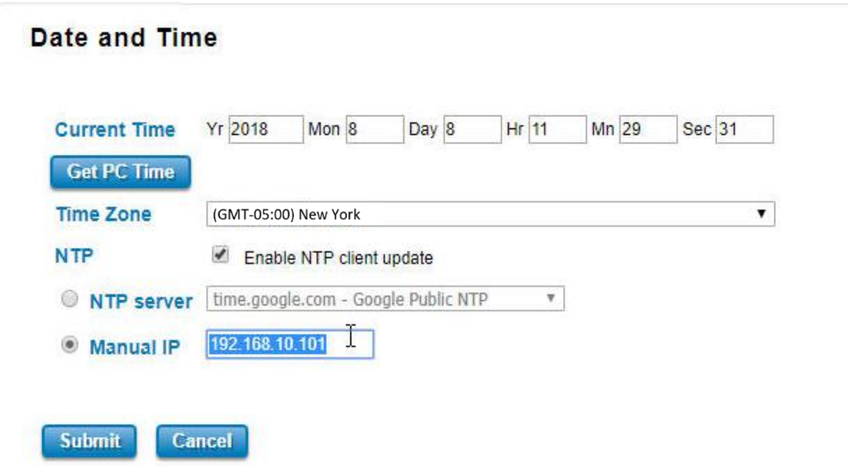
This form allows you to set the system's default time zone, which is used to convert the system time to a human-readable format and offset.

Time Zone

9. Adjust the time setting by using NTP

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

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



Date and Time

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

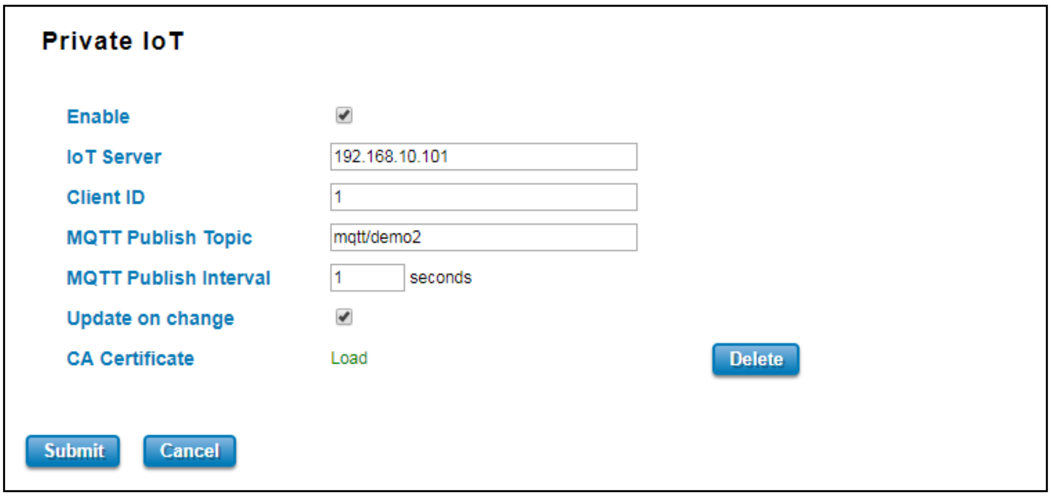
Time Zone: (GMT-05:00) New York

NTP: ☑ Enable NTP client update

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

● Manual IP: 192.168.10.101

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



Private IoT

Enable: ☑

IoT Server: 192.168.10.101

Client ID: 1

MQTT Publish Topic: mqtt/demo2

MQTT Publish Interval: 1 seconds

Update on change: ☑

CA Certificate: Load

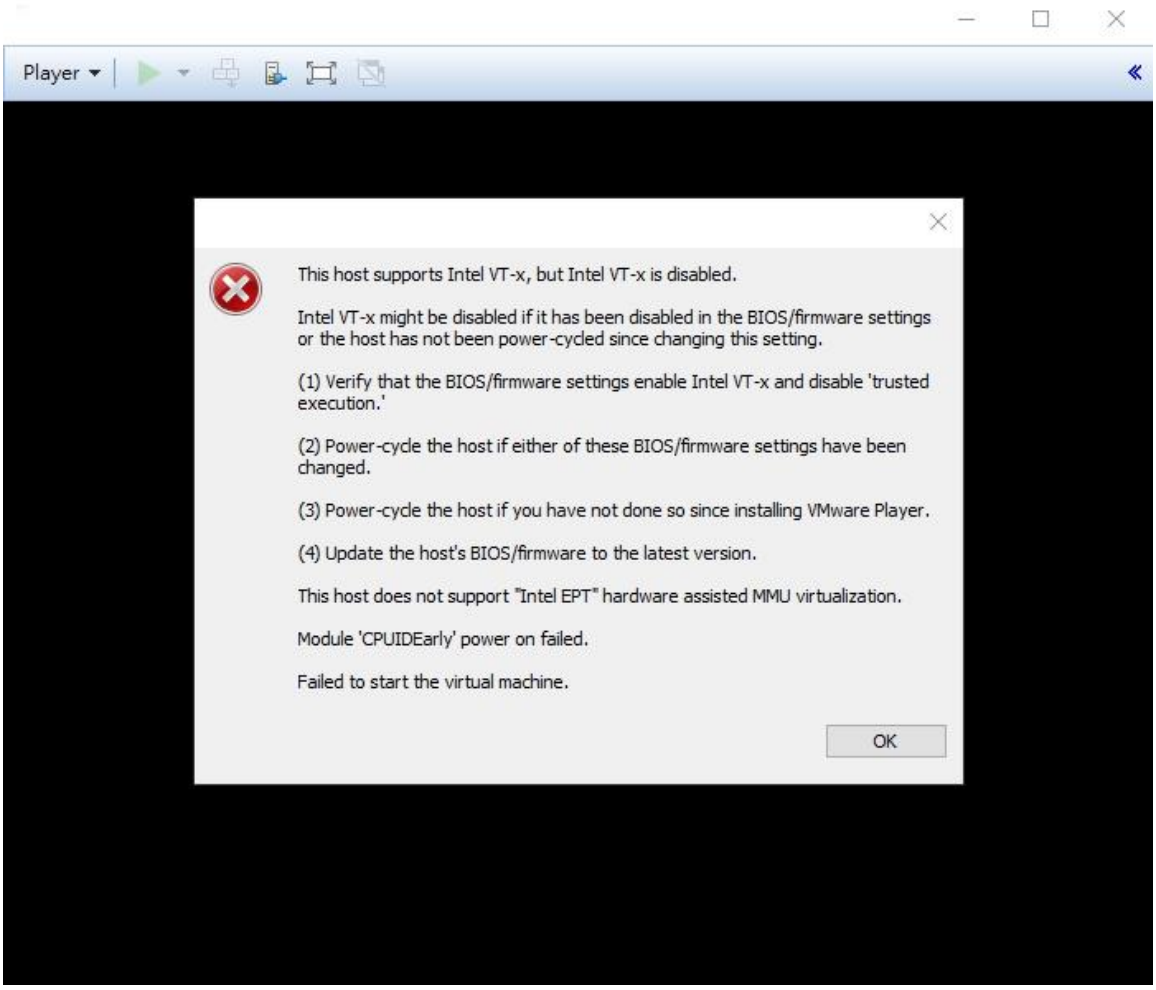
NOTE

1. Warning message about Inter VT-x

Root cause: VT-x disabled by BIOS

Please follow the instruction below:

- Reboot PC
- Enter BIOS (press ‘Delete’ key)
- Enable the VT-x feature (the location of this feature may differ according to the BIOS)



This host supports Intel VT-x, but Intel VT-x is disabled.

Intel VT-x might be disabled if it has been disabled in the BIOS/firmware settings or the host has not been power-cycled since changing this setting.

(1) Verify that the BIOS/firmware settings enable Intel VT-x and disable 'trusted execution.'

(2) Power-cycle the host if either of these BIOS/firmware settings have been changed.

(3) Power-cycle the host if you have not done so since installing VMware Player.

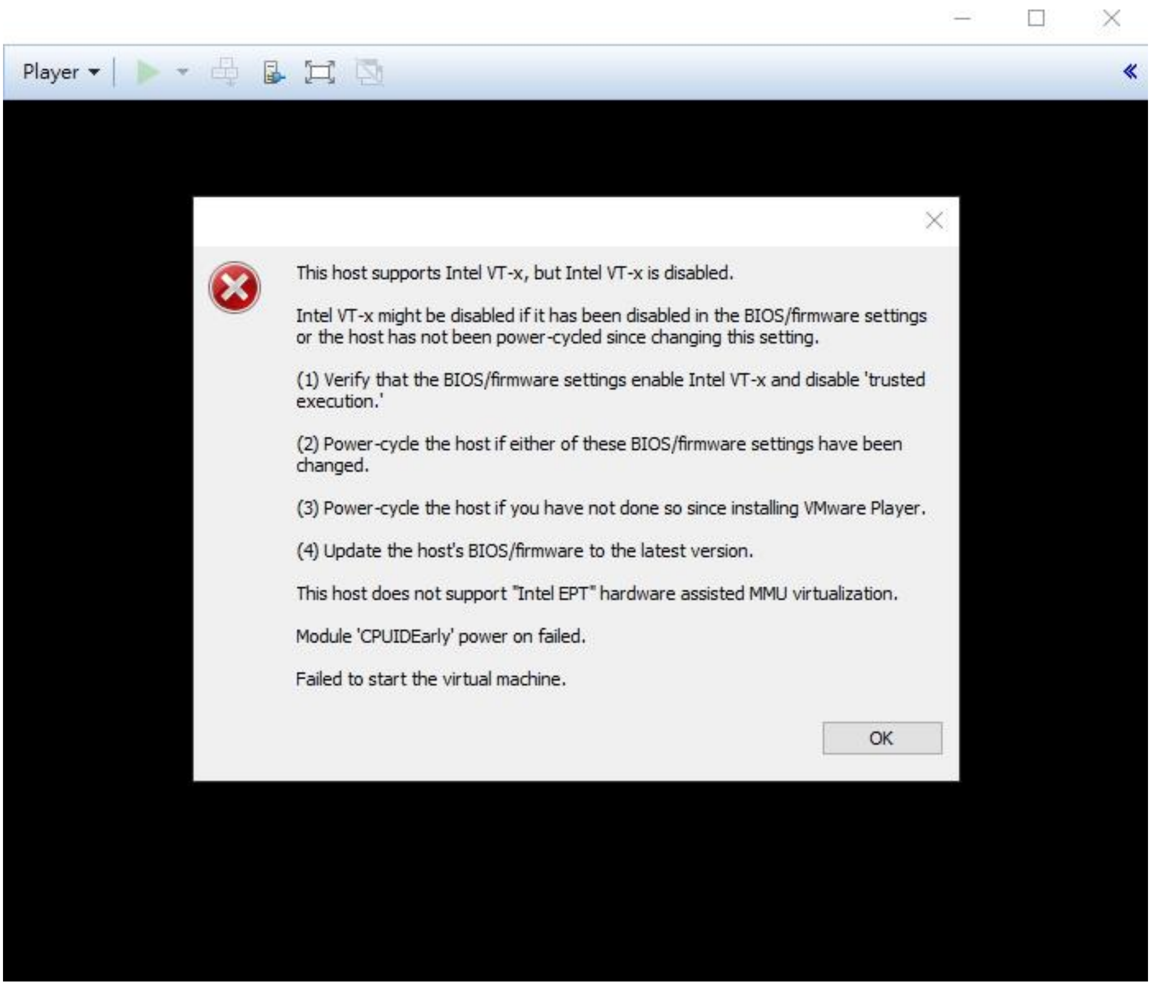
(4) Update the host's BIOS/firmware to the latest version.

This host does not support "Intel EPT" hardware assisted MMU virtualization.

Module 'CPUIDEarly' power on failed.

Failed to start the virtual machine.

2. If user has already installed other different Virtual Machine software (ex. Hyper-V, etc), it can cause the ATMS might fail to run.



This host supports Intel VT-x, but Intel VT-x is disabled.

Intel VT-x might be disabled if it has been disabled in the BIOS/firmware settings or the host has not been power-cycled since changing this setting.

(1) Verify that the BIOS/firmware settings enable Intel VT-x and disable 'trusted execution.'

(2) Power-cycle the host if either of these BIOS/firmware settings have been changed.

(3) Power-cycle the host if you have not done so since installing VMware Player.

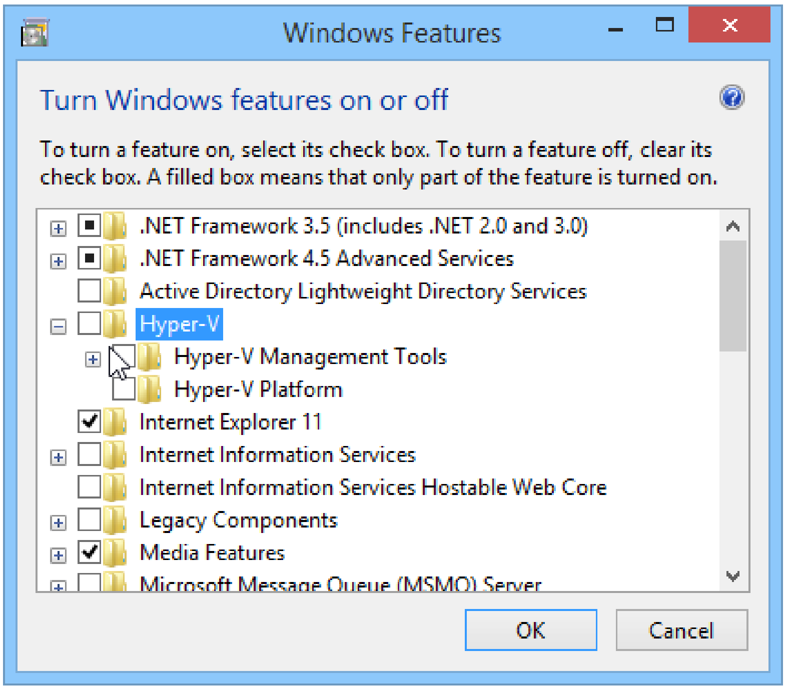
(4) Update the host's BIOS/firmware to the latest version.

This host does not support "Intel EPT" hardware assisted MMU virtualization.

Module 'CPUIDEarly' power on failed.

Failed to start the virtual machine.

Please disable/uninstall other installed Virtual Machine software. Then click OK.


Windows Features

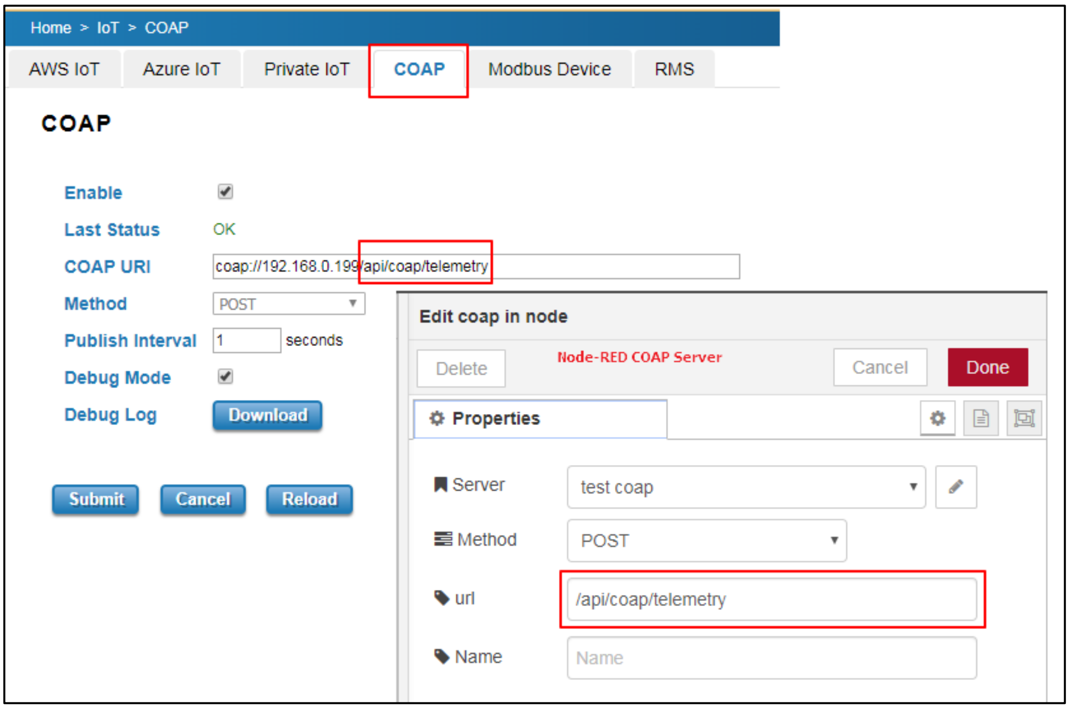
Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ■ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- ■ .NET Framework 4.5 Advanced Services
- □ Active Directory Lightweight Directory Services
- □ Hyper-V
  - □ Hyper-V Management Tools
  - □ Hyper-V Platform
- ☑ Internet Explorer 11
- □ Internet Information Services
- □ Internet Information Services Hostable Web Core
- □ Legacy Components
- ☑ Media Features
- □ Microsoft Message Queue (MSMQ) Server

3.10.4 CoAP

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



COAP

Enable ☑

Last Status OK

COAP URI coap://192.168.0.199/api/coap/telemetry

Method POST

Publish Interval 1 seconds

Debug Mode ☑

Debug Log

Server test coap

Method POST

url /api/coap/telemetry

Name Name

The description of the columns is as below:

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

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

CoAP payload:

{ "modelname": "AP222-WLAN+LTE", "devicename": "router", "version": "1.1.1", "mac address": "94:66:e7:00:24:be", "serial number": "N/A", "IPADD": "192.168.10.22", "status": "normal" , "latitude": "25.034", "longitude": "121.5641" , "act": 2, "rssi": -75, "rscp": -79, "ecio": -12 , "di1":"0" , "lte_rx": 0.00 , "lte_tx": 0.00 , "lte_bytes":0, "CO2":1, "Temperature":2}

CoAP content-format: application/json

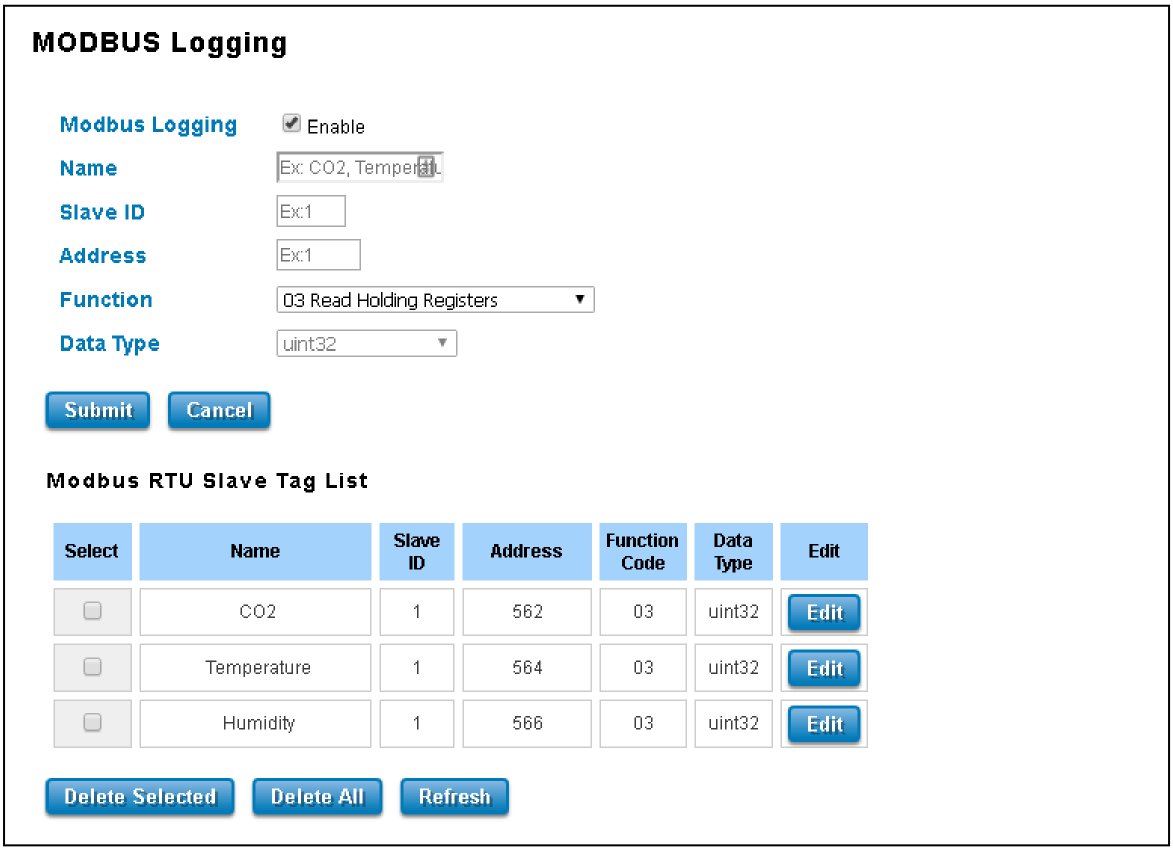
Key-value format:

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

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

3.10.5 Modbus Device

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



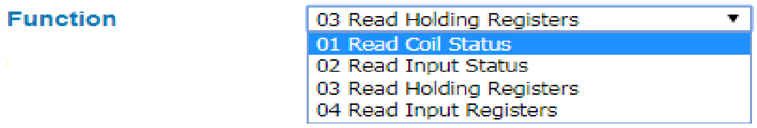
MODBUS Logging

Modbus Logging	☑ Enable
Name	Ex: CO2, Temperatu
Slave ID	Ex:1
Address	Ex:1
Function	03 Read Holding Registers ▼
Data Type	uint32 ▼

Modbus RTU Slave Tag List

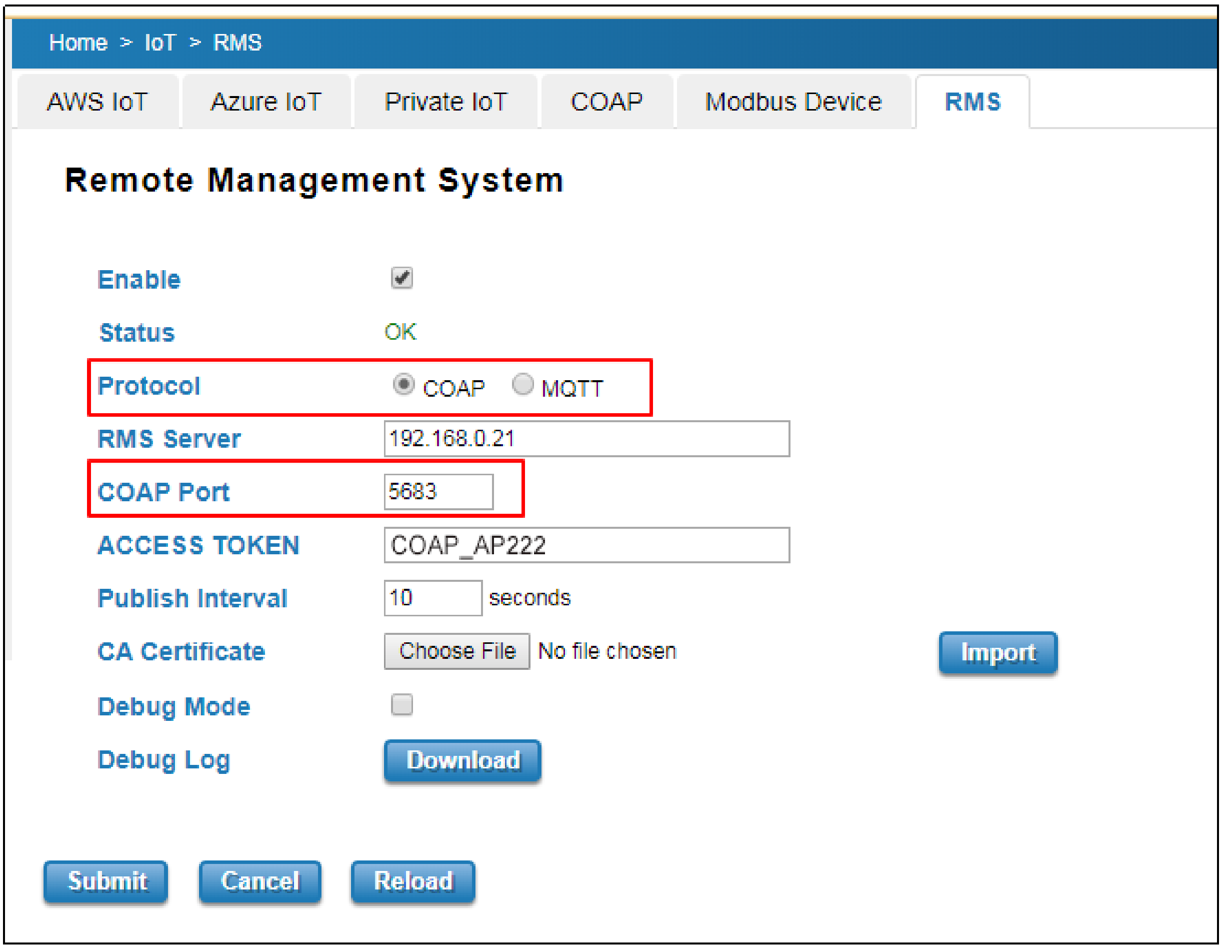
Select	Name	Slave ID	Address	Function Code	Data Type	Edit
□	CO2	1	562	03	uint32	Edit
□	Temperature	1	564	03	uint32	Edit
□	Humidity	1	566	03	uint32	Edit

The description of the columns is as below:

TERMS	DESCRIPTION
Modbus Logging	Check the box to enable the function.
Name	Enter the Modbus name
Slave ID	Enter the Slave ID that belongs to the device
Address	Enter the address that belongs to the device.
Function	 Function 03 Read Holding Registers ▼ 01 Read Coil Status 02 Read Input Status 03 Read Holding Registers 04 Read Input Registers
Data Type	**Default: Uint32** Select the Data Type
Alive	The Alive status of the target Protocol/PLC address of the connected sensor.
Value	The Value of the target Protocol/PLC address the router read from the sensor.

3.10.6 RMS

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



Home > IoT > RMS

Remote Management System

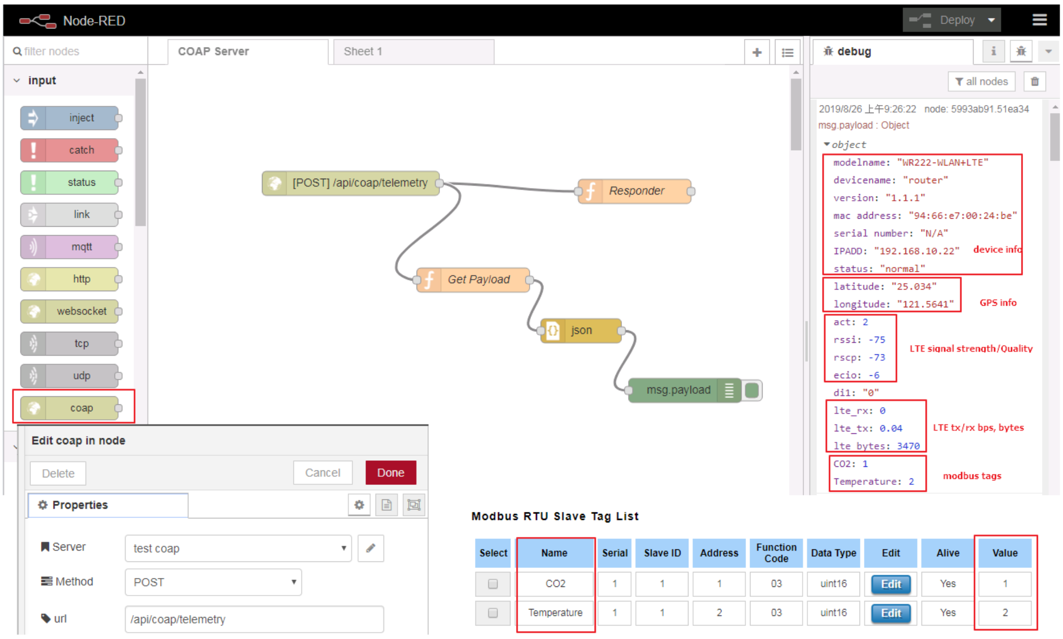
Enable	☑
Status	OK
Protocol	● COAP ○ MQTT
RMS Server	192.168.0.21
COAP Port	5683
ACCESS TOKEN	COAP_AP222
Publish Interval	10 seconds
CA Certificate	Choose File No file chosen
Debug Mode	☐
Debug Log	Download

The description of the columns is as below:

TERMS	DESCRIPTION
Enable	Check the box to enable the RMS function.
Status	Show the connection status between device and RMS server
Protocol	Select protocol for uploaded payload. CoAP and MQTT are supported. Contact AVCOMM salesperson for other protocols.
RMS Server	Enter the RMS Server IP Address
CoAP Port	Specify connection port of selected upload protocol.
ACCESS TOKEN	Generate the token from ATMS RMS; this access token is used to access the device by ATMS Cloud.
Publish Interval	**Default: 10 (Seconds)** Specify the interval (in seconds) between each upload.
CA Certificate	The function from this certificate file is to create an encrypted MQTT communication. User will get this file when download the ATMS server file. **Note. This field only supports in ATMS OTA v1.0.0 and later version.**
Debug Mode	Check to enable debug mode for CoAP connection.

Debug Log	Download log for problem analysis between device and CoAP server

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



Edit coap in node

Delete Cancel Done

Properties

Server: test coap

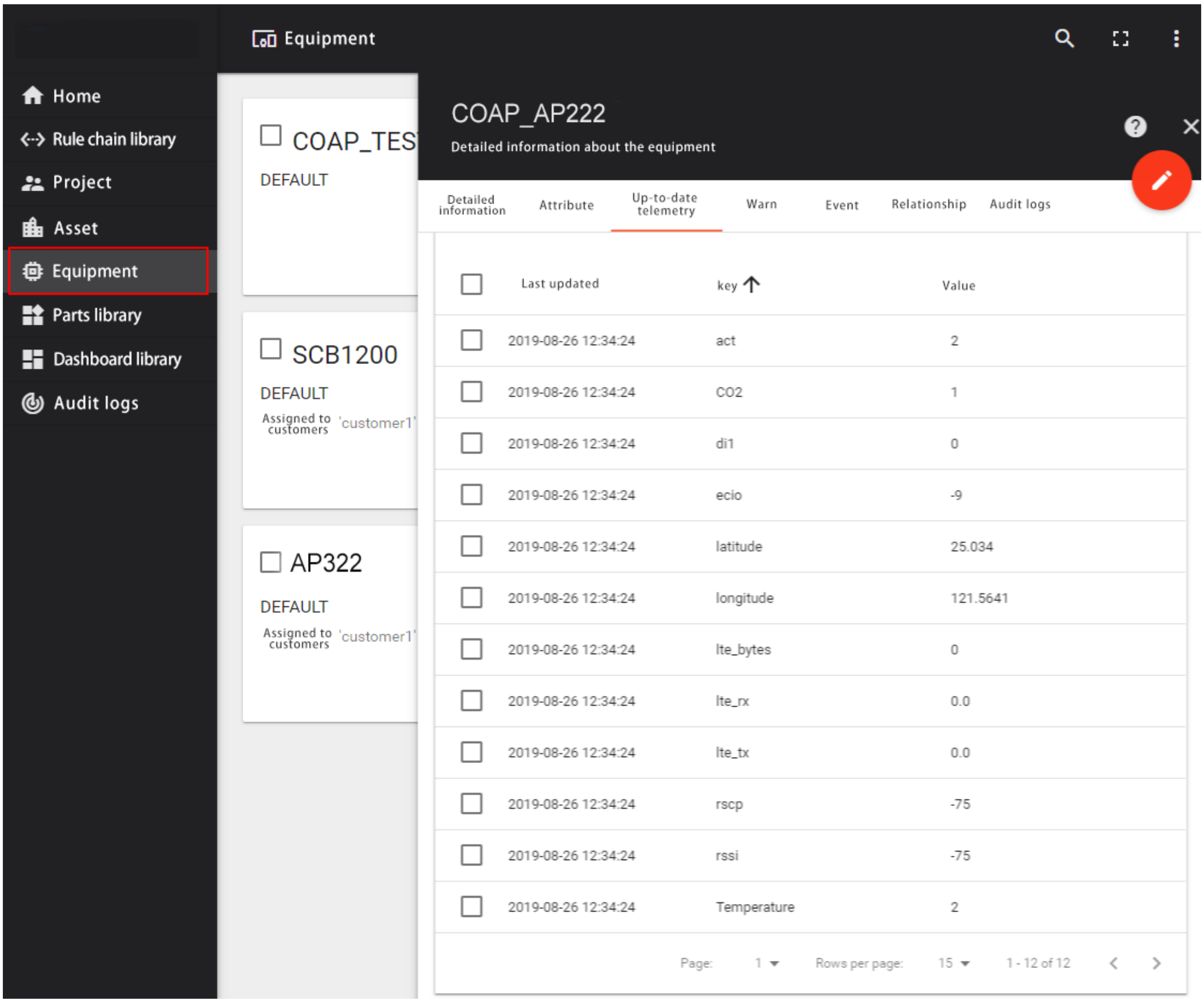
Method: POST

url: /api/coap/telemetry

```
2019/8/26 上午9:26:22   node: 5993ab91.51ea34
msg.payload : Object
▾object
  modelname: "WR222-WLAN+LTE"
  devicename: "router"
  version: "1.1.1"
  mac address: "94:66:e7:00:24:be"
  serial number: "N/A"
  IPADD: "192.168.10.22"
  status: "normal"
  latitude: "25.034"
  longitude: "121.5641"
  act: 2
  rssi: -75
  rscp: -73
  ecio: -6
  di1: "0"
  lte_rx: 0
  lte_tx: 0.04
  lte_bytes: 3470
  CO2: 1
  Temperature: 2
```

Modbus RTU Slave Tag List

Select	Name	Serial	Slave ID	Address	Function Code	Data Type	Edit	Alive	Value
□	CO2	1	1	1	03	uint16	Edit	Yes	1
□	Temperature	1	1	2	03	uint16	Edit	Yes	2



COAP_AP222

Detailed information about the equipment

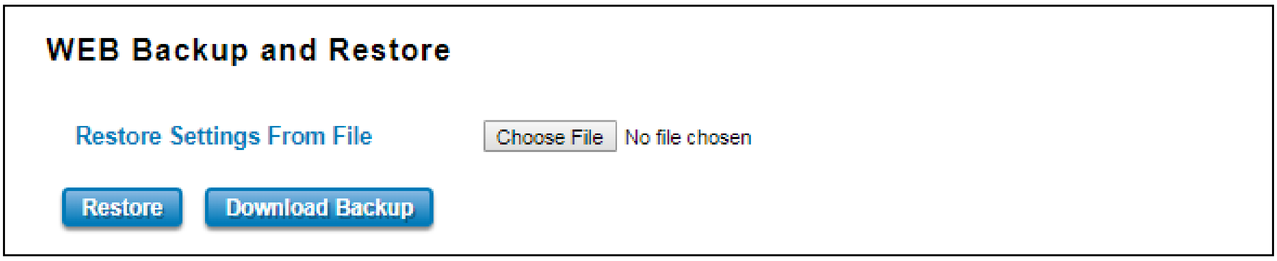
Detailed information | Attribute | Up-to-date telemetry | Warn | Event | Relationship | Audit logs

□	Last updated	key ↑	Value
□	2019-08-26 12:34:24	act	2
□	2019-08-26 12:34:24	CO2	1
□	2019-08-26 12:34:24	di1	0
□	2019-08-26 12:34:24	ecio	-9
□	2019-08-26 12:34:24	latitude	25.034
□	2019-08-26 12:34:24	longitude	121.5641
□	2019-08-26 12:34:24	lte_bytes	0
□	2019-08-26 12:34:24	lte_rx	0.0
□	2019-08-26 12:34:24	lte_tx	0.0
□	2019-08-26 12:34:24	rscp	-75
□	2019-08-26 12:34:24	rssi	-75
□	2019-08-26 12:34:24	Temperature	2

Page: 1 ▾ Rows per page: 15 ▾ 1 - 12 of 12

3.11 BACKUP AND RESTORE

User can use AVCOMM'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 Backup and Restore

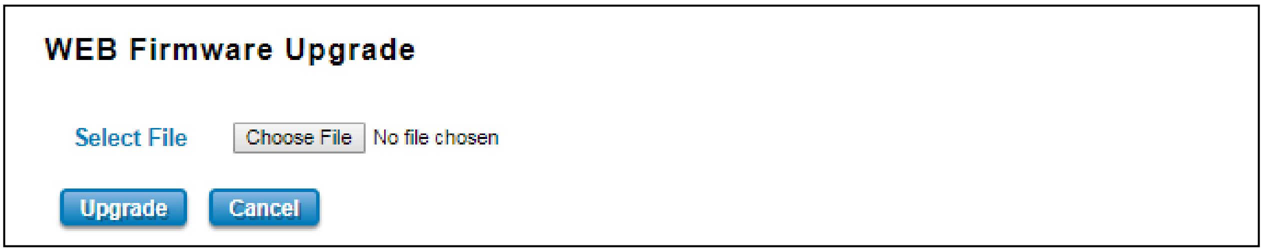
Restore Settings From File No file chosen

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.

3.12 FIRMWARE UPGRADE

AVCOMM provides the latest firmware online at www.avcomm.us The new firmware may include new features, bug fixes or other software changes. AVCOMM also provides the release notes for the update as well. For technical viewpoint, AVCOMM 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.



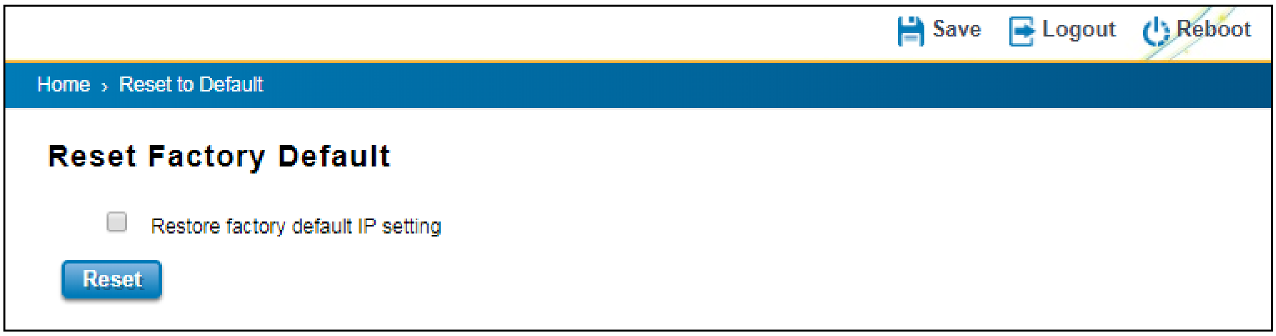
WEB Firmware Upgrade

Select File No file chosen

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.

3.13 RESET TO DEFAULTS

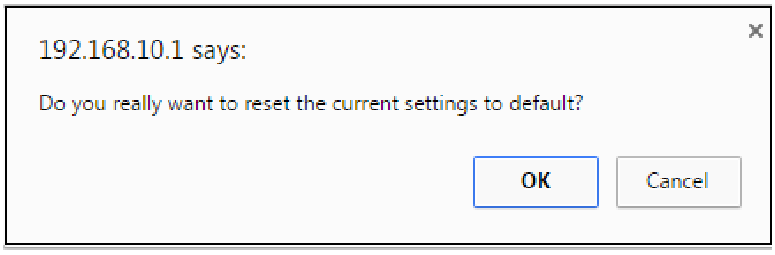
This function provides users with a quick way of restoring the AVCOMM router's configuration to factory defaults. By check the Restore Factory default IP setting, it means the IP of the device will directly change to the default IP (192.168.10.1).



Reset Factory Default

□ Restore factory default IP setting

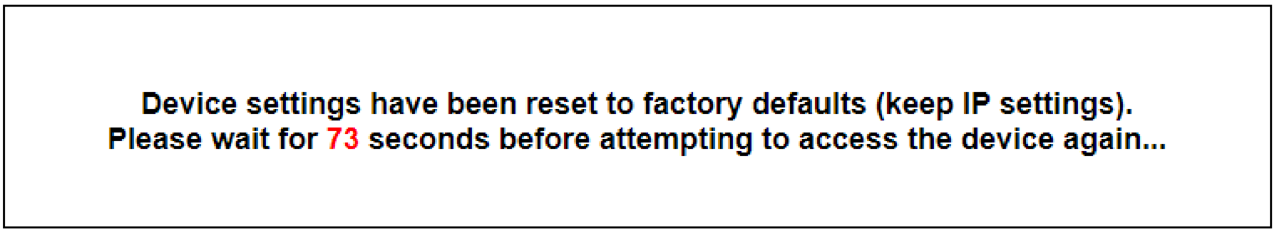
Pop-up message screen to show User that have done the command. Click on **OK** to close the screen and reboot the device.



192.168.10.1 says:

Do you really want to reset the current settings to default?

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



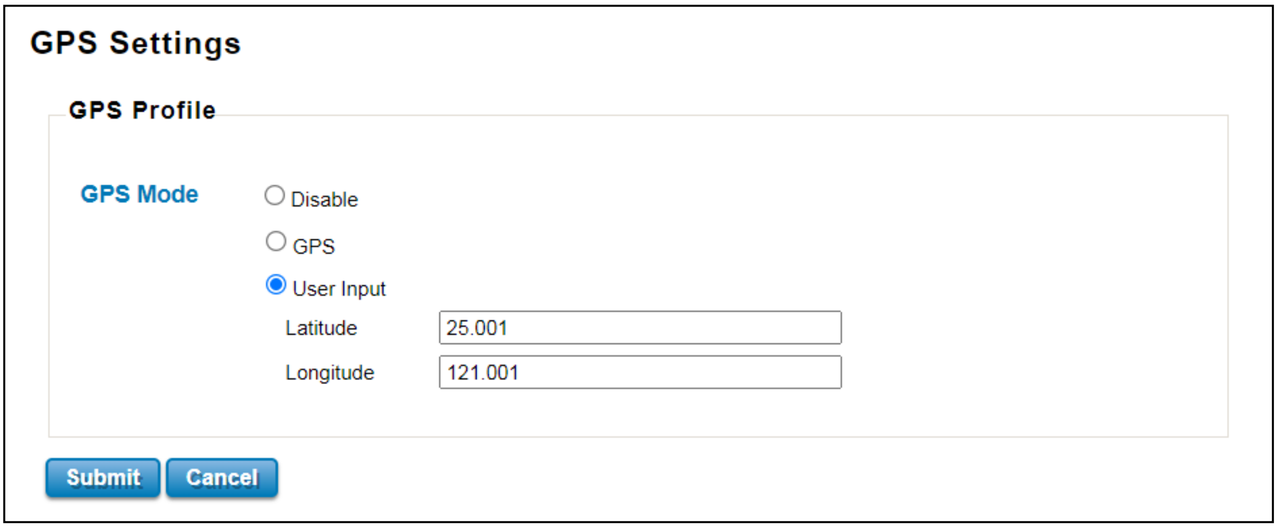
Device settings have been reset to factory defaults (keep IP settings).
Please wait for 73 seconds before attempting to access the device again...

3.14 GPS

This is a new feature allows user to configure static GPS address in web GUI.

GPS Setting:

Select the “User Input” and Type the address of “Latitude” and “Longitude”. While you enabled the IoT feature, the router can send the User Input GPS address of the router through MQTT protocol to the AWS/Azure or your private IoT cloud.

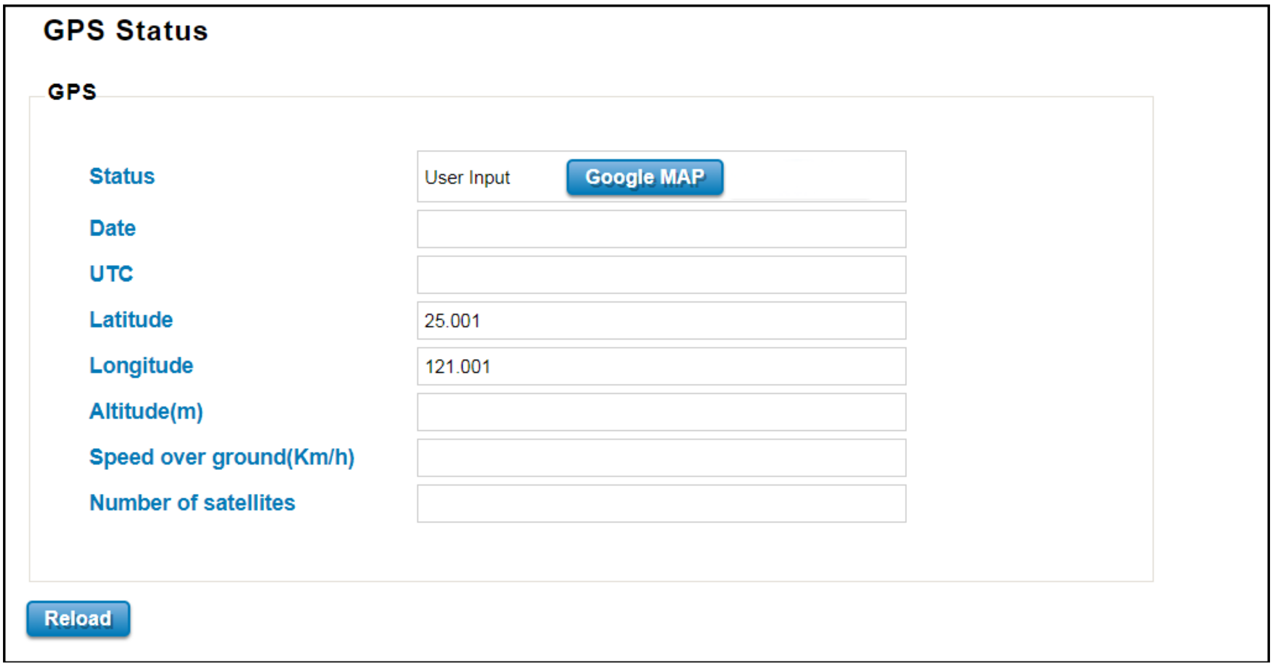


GPS Settings

GPS Profile

GPS Mode
○ Disable
○ GPS
● User Input

Latitude: 25.001
Longitude: 121.001



GPS Status

GPS

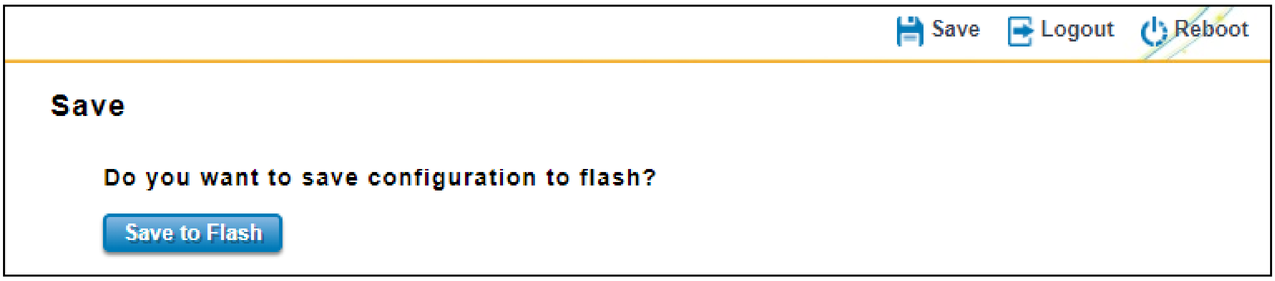
Status	User Input
Date	
UTC	
Latitude	25.001
Longitude	121.001
Altitude(m)	
Speed over ground(Km/h)	
Number of satellites	

In GPS Status, you can find the address you input. You can click “Google MAP”, then it will connect to the MAP in your computer.

Note: The standard version router doesn’t support GPS feature in hardware. If you need GPS feature, please contact our Sales, we can customize for your project need.

3.15 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.

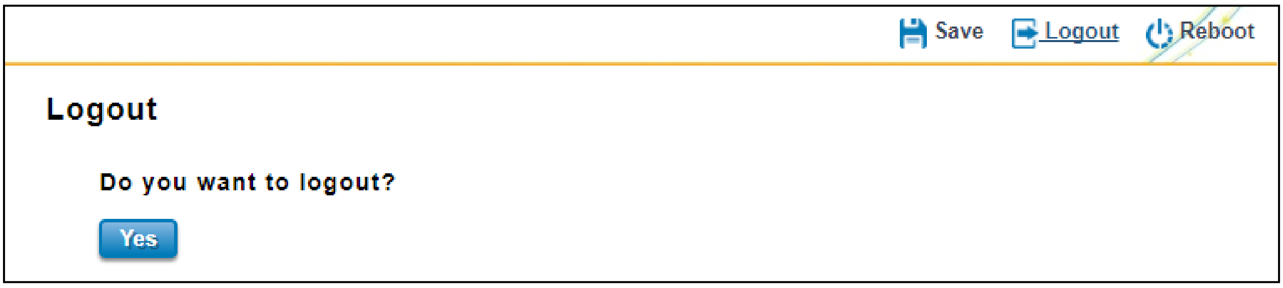


Save

Do you want to save configuration to flash?

3.16 LOGOUT

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



Logout

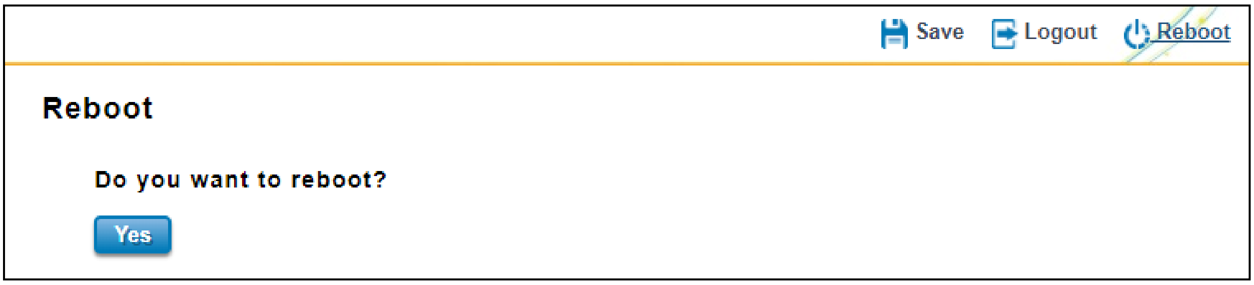
Do you want to logout?

3.17 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.



Reboot

Do you want to reboot?