AVCOMM AP316

User Manual

AVCOMM Technologies Inc.
333 West Loop North, Suite 460 Houston, TX 77024, USA | info@avcomm.us | www.avcomm.us

AVCOMM Technologies Inc.

AP316

Industrial Cellular PoE Routing Switch

User Manual

Copyright Notice

About This Manual

This user manual is intended to guide a professional installer to install and to configure the Avcomm Industrial Cellular PoE Routing Switch. It includes procedures to assist you in avoiding unforeseen problems.

NOTE:

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

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 particular 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

The unique LTE PoE router AP316 provide ultra-resilient network by latest G.8032 ERPS v2 ring technology with 6 Giga ports, 2-port 100/1000M fiber ports, for the AP316, it is equipped with simultaneous high-speed LTE routing. The LTE can backup network in case of ring failure and works as a redundant gateway. Dual SIM standby enables auto switch to secondary cellular network if primary network disconnects. Moreover, the router offers 4 Gigabit PoE/PoE+ ports for feeding IP cam or wireless AP. Integrated firewall ensures safe data transmission. This Industrial router also can be smartly configured by Avcomm advanced management utility, Web Browser, SNMP, Telnet and Command Line Interface.

The support of OpenVPN, IPsec, and L2TP provides security to the gateway. For the best traffic control, the device management side features have been utilized: NAT Routing, Traffic shaping, 1:1 NAT, and NAPT (SNAT/DNAT).

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 to ensure the secure data communication.

The embedded MQTT and RESTful API enables public cloud integration such as AWS or Azure. The private cloud platform ATMS can also be setup for instant and secured access to track location and video surveillance over cloud.

AP316 is designed to provide fast, secure, and more stable network. Besides, IEC 61000-6-2 / 61000-6-4 Heavy Industrial and wayside EN50121-4 EMC certified design, rugged enclosure and -40~75°C wide operating temperature range, also NEMA TS2 compliance for ITS application all of these features guarantee stable performance of AP316.

Model Name	Description
AP316-WLAN-SFP	Industrial Wireless Ring Network IIoT Routing POE Gateway,802.11 b/g/n WLAN Cat. 4. 2x2 MIMO,4G/3G/2G, 4-Port Gigabit POE Plus 2-Port Gigabit SFP, ITU standard ring redundancy protocol, under 50ms protection and recovery switch, dual power 46 to 57VDC, -40°C to 75°C, IP30
AP316-LTE-SFP	Industrial Wireless Ring Network IIoT Routing POE Gateway, LTE CAT.4, 2x2 MIMO,4G/3G/2G, 4-Port Gigabit POE Plus 2-Port Gigabit SFP, ITU Standard Ring Redundancy Protocol, Protection and Recovery Switching below 50ms, Dual Power 46 to 57VDC, To 40 ° C to 75 ° C, IP30

1.2 Major Features

Below are the major features of AP316:

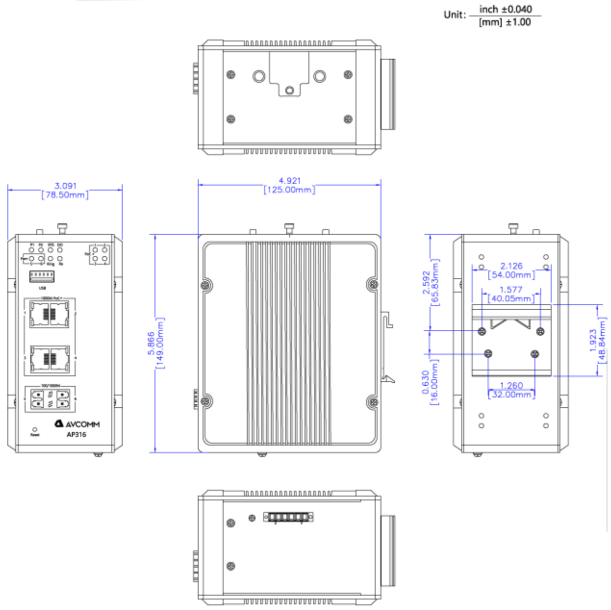
- 4-port Gigabit PoE plus 2-port Gigabit SFP, high flexibility for selecting cable types and distances
- LTE Cat.4, 2x2 MIMO, 150M downlink and 50M uplink
- 4G/3G/2G full cellular network compatibility LTE-E: FDD B1/3/5/7/8/20; TDD B38/40/41 LTE-CN: FDD B1/3/5/8; TDD B38/39/40/41 LTE-U: FDD B2/B4/B12
- Advanced network management features: IPv4/IPv6, DDNS, SNMP v1/v2c/v3/Trap, MIB II, Entity MIB, MIBs, DHCP server/client, DHCP relay*, TFTP, System Log, ARP response over 802.2 LLC SNAP, Proxy ARP, DNS (client/proxy)
- Cellular Configuration: Radio on/off, 4G LTE/3G HSPA Configuration, SIM Security, Connection Status, Cellular to Eth-WAN Redundancy, GPS positioning (by model)
- Redundancy Protocol technology: ITU-T G.8032 v1/v2 Ethernet Ring Protection Switching (ERPS) and Rapid Spanning Tree Protocol (RSTP)
- Cloud Management Service: Support Amazon AWS & Microsoft Azure cloud service, support proprietary ATMS cloud service. Interactive monitoring dashboard and map shows the status, signal strength, location etc.
- Advanced Security system by OpenVPN, IPsec, Firewall, DMZ, Port Forwarding, HTTPs Login and SSH Telnet
- VPN: IPsec, OpenVPN, L2TP*
- Traffic Management features: NAT Routing, Traffic shaping, 1:1 NAT, NAPT (SNAT/DNAT).
- CLI interface, Web, SNMP, Telnet for network Management
- Steel Metal with Aluminum for heat dissipation
- Effective heat dissipation design for operating in -40~75ºC environments
- IP30 ingress protection

2. Hardware Installation

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

2.1 Hardware Dimension

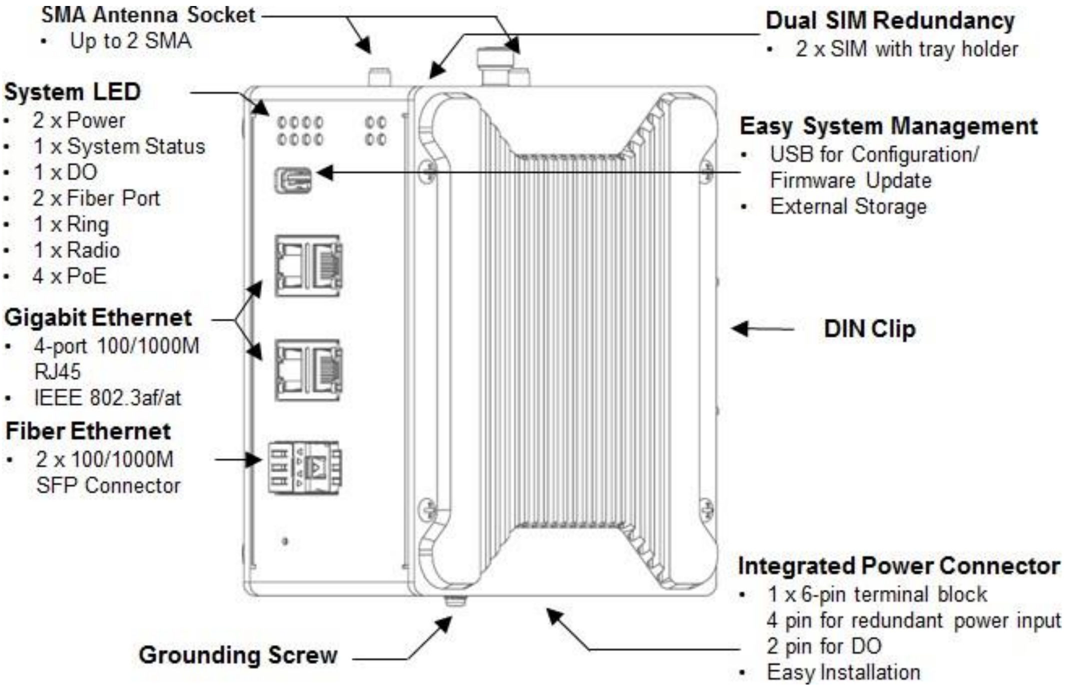
Dimensions of AP316: 78.5 x 149 x 125 (W x H x D) / without DIN Rail Clip



- ➢ Front Panel Layout

The front panel from AP316 router include 4 ports Giga Ethernet (100/1000 Base-T, RJ45) with PoE feature, 2 Fiber Ports (100/1000MBase SFP), System LED, USB for configuration/firmware management, 1 x6-pin terminal block connector (4 pin for power inputs and 2 pin for DO alarm), 2 SIM card slots (LTE router), and 1 chassis grounding screw. AP316 is provided with 2 antenna sockets for LTE module.

AP316



2.2 Installation

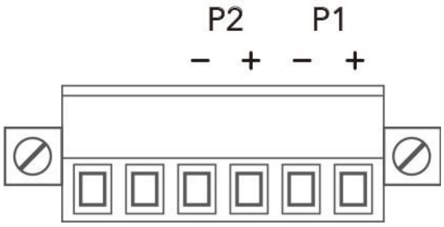
After unpack the box, follow the steps below in order to properly connect the device. For better LTE performance, put the device in a clearly visible spot, as obstacles such as walls and doors hinder the signal.

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

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

2.3 Wiring the Power Inputs

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



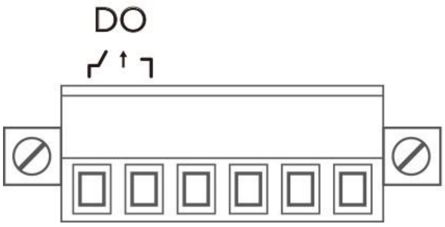
➢ Wiring the Power Input

- Insert the positive and negative wires into the V+ and V- contact on the terminal block connector.
- Tighten the wire-clamp screws to prevent the power wires from being loosened.
- Connect the power wires to suitable DC Switching type power supply. The input DC voltage should be 48VDC(46~57VDC, 50~57VDC suggested for IEEE802.3at).

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 the connections were well established.

2.4 Wiring the Alarm Relay Output (DO)

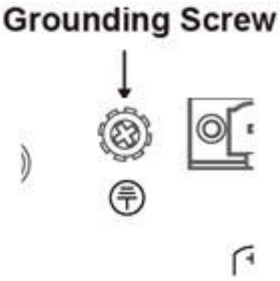
The relay output contacts are located on the front panel of the router. The relay output consists of the 2-pin terminal block connector that used to detect user-configured events. The two wires attached to the fault contacts form a close circuit when a user-configured event is triggered. If a user-configured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



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

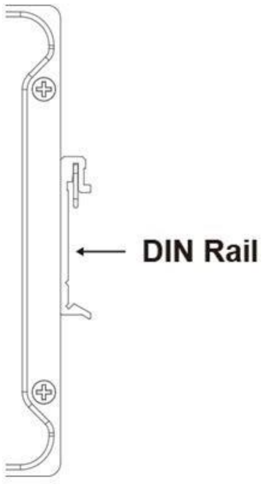
2.5 Connecting the Grounding Screw

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



2.6 DIN Rail Mounting

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



To mount the router on DIN Rail track, do the following instruction:

- Insert the top side of DIN Rail track into the slot of DIN Rail clip.
- Lightly clip the bottom of DIN-Rail to the track and make sure it attached well.
- To remove the device from the track, reverse the steps.

2.7 Antenna

AP316 is supported with up to 2 antenna sockets, where 3G/LTE antenna is supported. All the antennas are connected to the router by screwing all the antennas to the SMA connector on the front panel of the router.

LTE Antenna

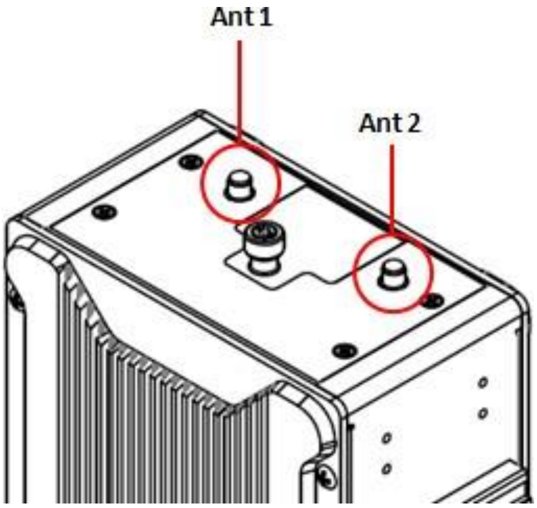
	Frequency	704 ~ 960 MHz 1710 ~ 2690 MHz
	V.S.W.R	<= 3.0
	Radiation	Omni
	Gain	2dBi
	Polarization	Vertical
	Impedance	50 Ohm
	Connector Type	Brass
	Operational Temperature	- 20 °C ~ +65 °C

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

Antenna Placement

Antenna	AP316
Ant 1	LTE-Main
Ant 2	LTE- Aux

Check the picture below for the antenna installation.



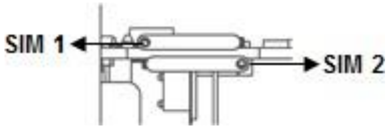
Radio LED

LED	LTE Status
Ra	SIM detected: Green On SIM not detected: Off
Rb	2/3G connection: Green On Not 2/3G connection: Off
Rc	4G connection: Green On Not 4G connection: Off

2.8 SIM/SD Card Installation

➢ SIM Card Slot

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



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

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.

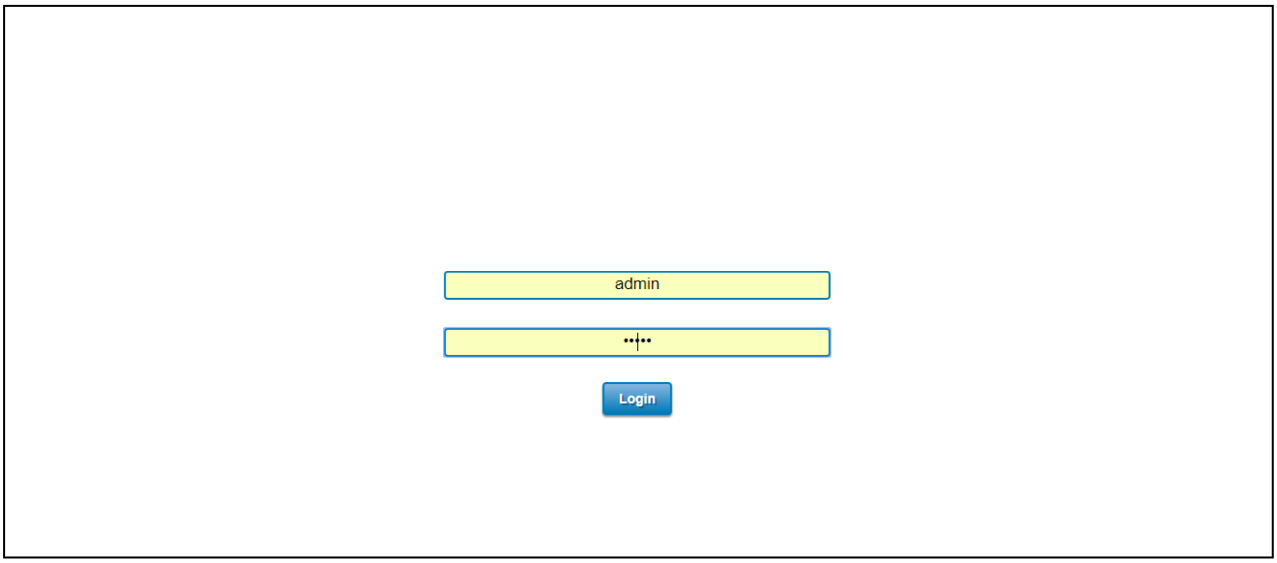
➢ Preparation for web interface management

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

- Plug the DC power to the router and connect router to computer.
- Make sure that the router default IP address is **192.168.10.1**.
- 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.
- Open command prompt and ping **192.168.10.1** to verify that the router is reachable.
- Launch the web browser (Internet Explorer or Mozilla Firefox or Google Chrome) on the PC.
- Type **http://192.168.10.1** (or the IP address of the router). And then press **Enter** and the login page

will appear.

- Type username and the password. Default username: **admin** and password: **admin**. Then click **Login**.



admin

••|••

In this Web management for Featured Configuration, user will see all Avcomm Cellular Router's various configuration menus at the left side from the interface. Through this web management interface, user can configure, monitoring, and set the administration functions. The whole information used web management interface to introduce the featured functions. User can use all the standard web-browser to configure and access the router on the network.

Following topics are covered in this chapter:

3.1 System
3.2 Ethernet Port
3.3 Power Over Ethernet
3.4 Quality of Service (QoS)
3.5 Multicast
3.6 Redundancy
3.7 Cellular
3.8 GPS
3.9 Security
3.10 Routing
3.11 Warning
3.12 Diagnostics
3.13 IoT
3.14 Backup and Restore
3.15 Firmware Upgrade
3.16 Reset to Defaults
3.17 Save
3.18 Logout

3.19 Reboot

3.20 Avcomm MIB

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:

3.21 Information

3.22 Login Setting

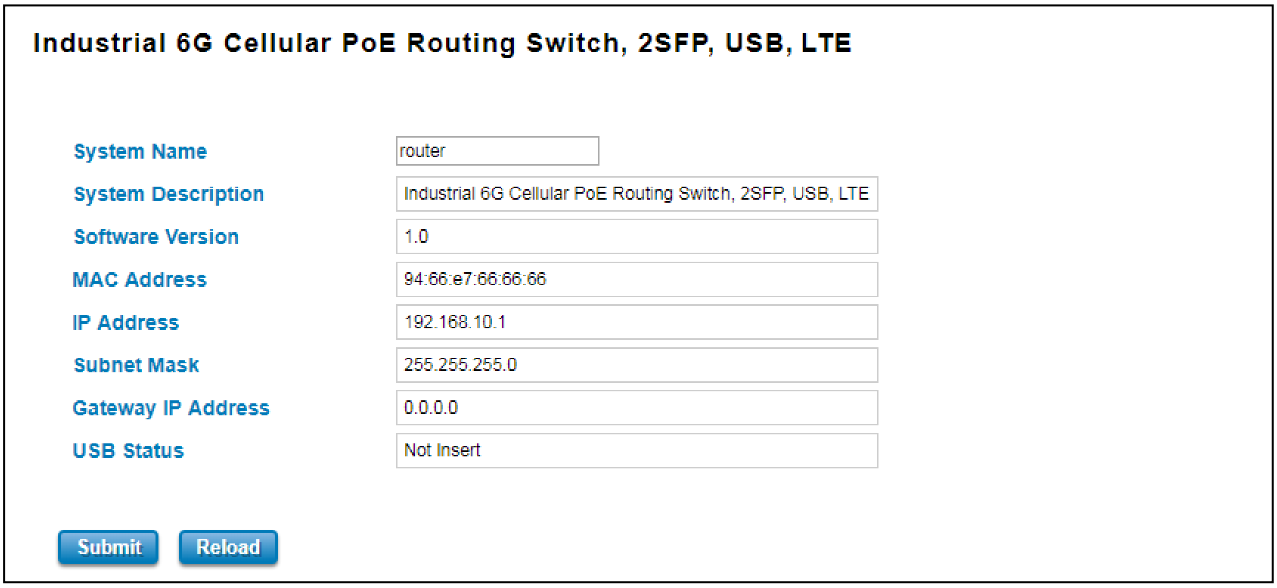
3.23 Network IP

3.24 Date and Time

3.25 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 it shows the Cellular Status and LAN Settings information. The figure below shows the interface of the Information section.



Industrial 6G Cellular PoE Routing Switch, 2SFP, USB, LTE

System Name	router
System Description	Industrial 6G Cellular PoE Routing Switch, 2SFP, USB, LTE
Software Version	1.0
MAC Address	94:66:e7:66:66:66
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
USB Status	Not Insert

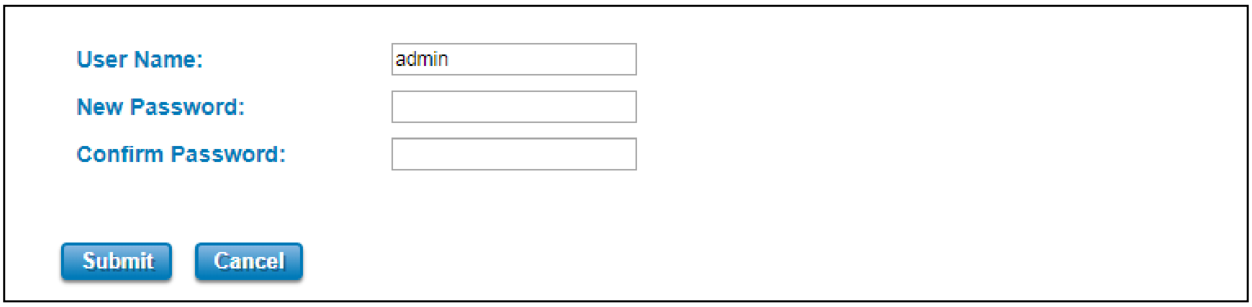
The description of the Information's interface is as below:

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
USB Status	Display the USB port status when the USB is plugged or unplugged.

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 levels, 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.**



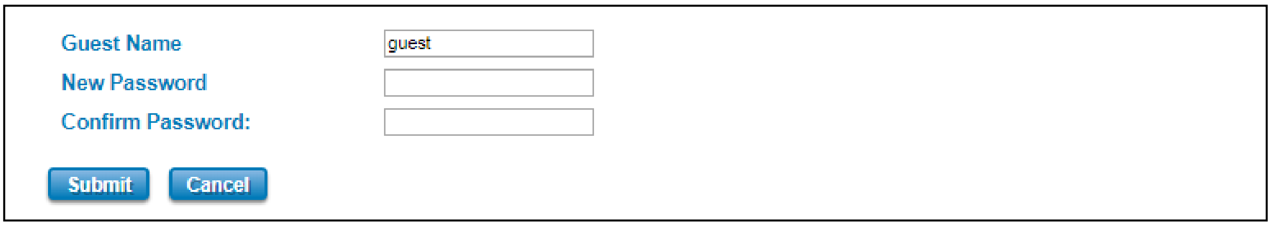
User Name: admin
New Password:
Confirm Password:

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 managementlogin. 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 Username and Password.

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

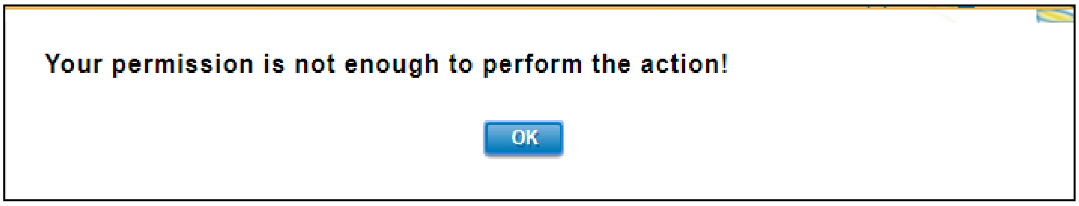
With the Name default setting is **guest** and the authority allow user to read only all of configuration parameters.



Guest Name guest
New Password
Confirm Password:

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

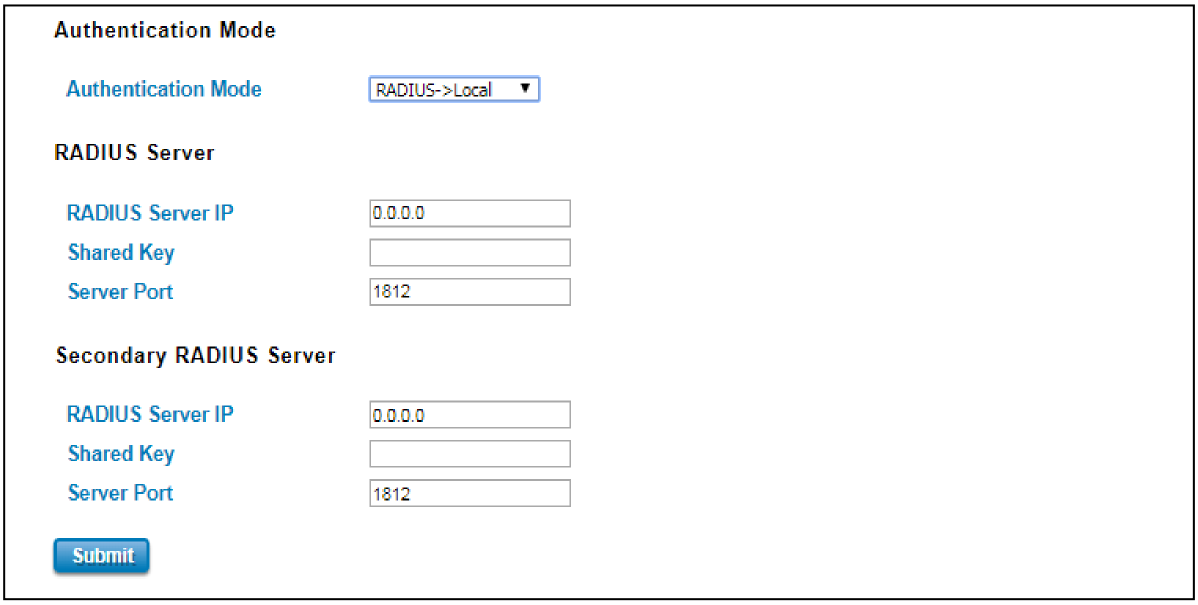
After finishing configure the Username and Password, click on Submit to apply the configuration. Don't forget to Save the configuration.

➢ Authentication Mode

The 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. 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:

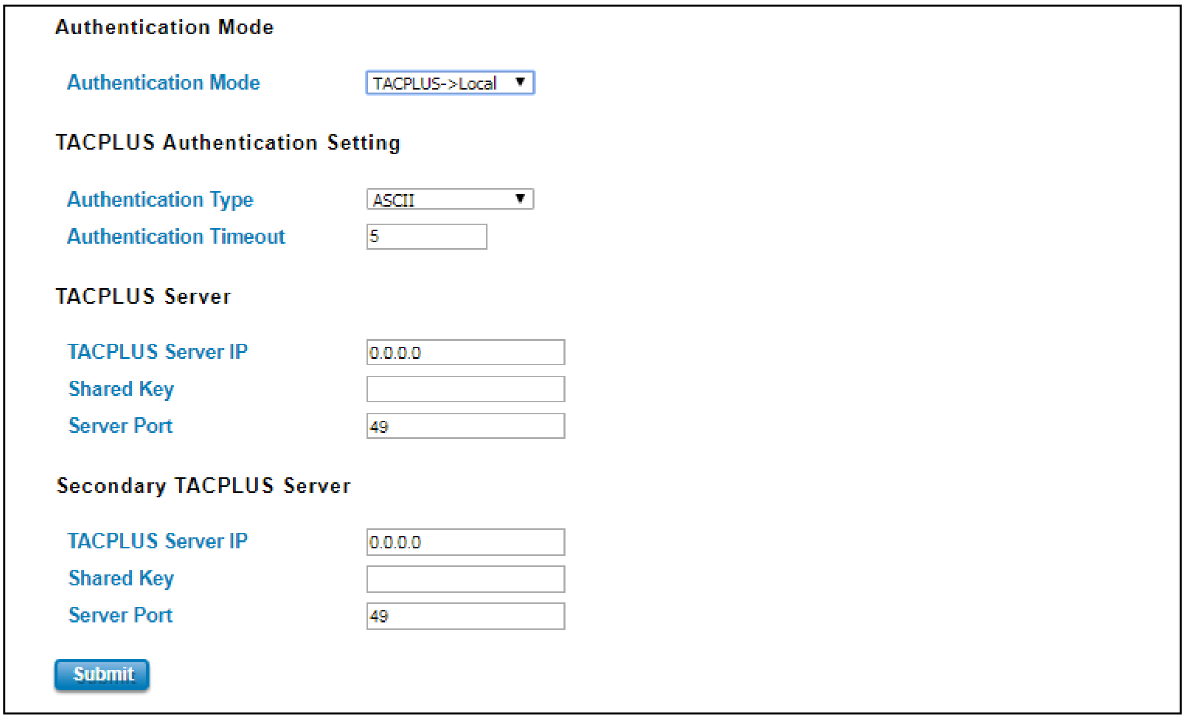
- Enter the IP address of the RADIUS server in **Server IP Address**
- Enter the **Shared Secret** of the RADIUS server
- Enter the **Server port** if necessary, by default RADIUS server listens to port 1812
- Click **Submit**

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:

- Select the **Authentication Type.**
- Enter the **Authentication Timeout** in seconds.
- Enter the IP address of the TACACS+ server in **Server IP Address.**
- Enter the **Shared Secret** of the TACACS+ server.

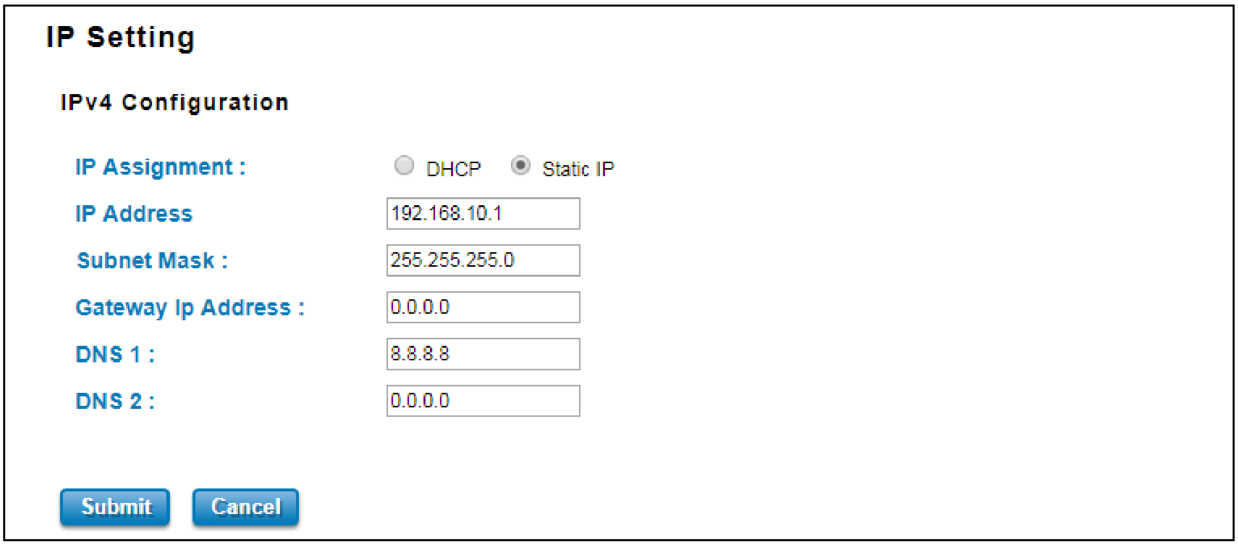
- Enter the **Server port** if necessary, by default TACACS+ server listens to port 49.
- Click Submit

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

3.1.3 Network Setting

The Network Setting section allows users to configure both IPv4 values for management access over the network. 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:

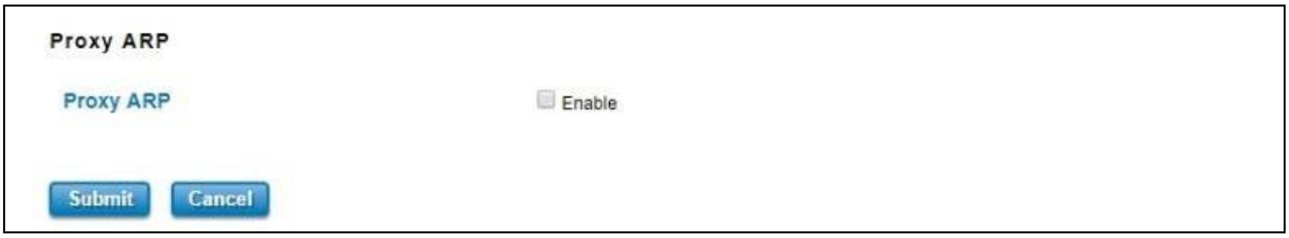
Terms	Description
IP Assignment	User can select to DHCP or Static IP to activate the function. **DHCP:** Select DHCP to activate DHCP Client Function, no need to assign IPAddress and received IP Address from DHCP Server. **Static IP:** Select Static IP to configure the IP configuration manually
IP Address	**Default: 192.168.10.1** Set up the IP address reserved by User network for User device. If DHCPClient function is enabled, no need to assign an IP address to device as itwill 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 isenabled, 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.



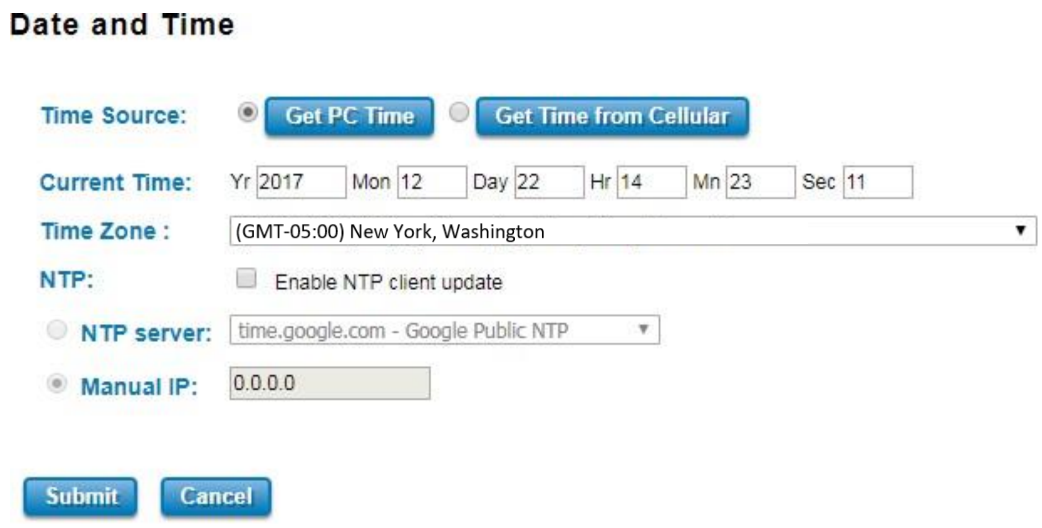
Proxy ARP

Proxy ARP ☐ Enable

Check the box to enable the function of Proxy ARP. Click Submit to apply 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.



Date and Time

Time Source: ● Get PC Time ○ Get Time from Cellular

Current Time: Yr 2017 Mon 12 Day 22 Hr 14 Mn 23 Sec 11

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

NTP: □ Enable NTP client update

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

● Manual IP: 0.0.0.0

The description of the columns is as below:

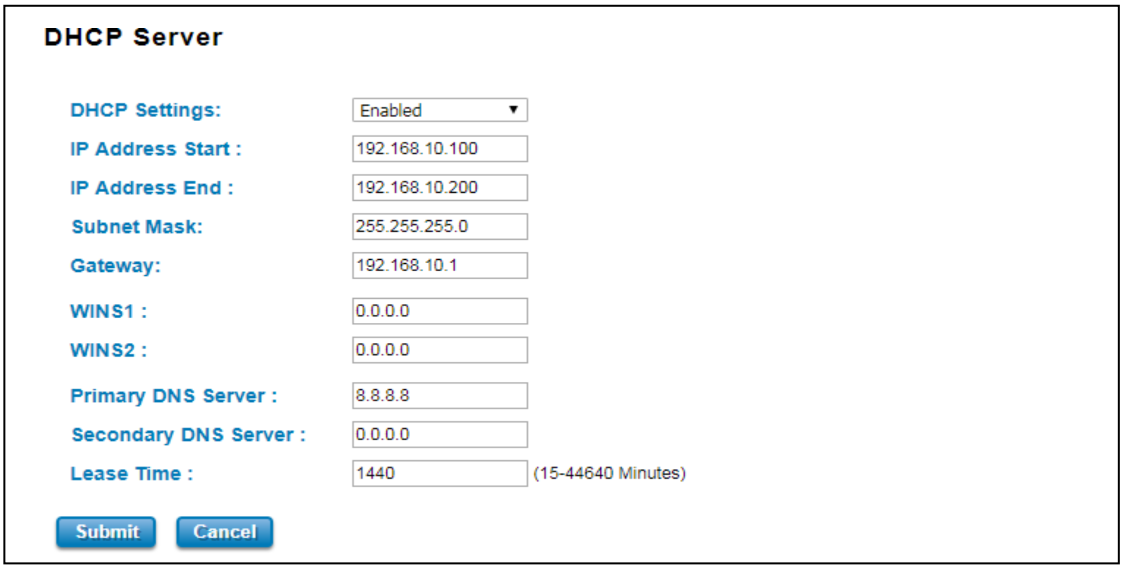
Terms	Description
Current Time	User can configure time by input it manually. User also can click the **Get PCTime or Get Time from Cellular** to get the time setting. Get PC Time: get the time the PC Get Time from Cellular: get the time from the cellular network.
Time Zone	Choose the Time Zone section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

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

3.1.5 DHCP Server

➢ DHCP Server Setting

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)

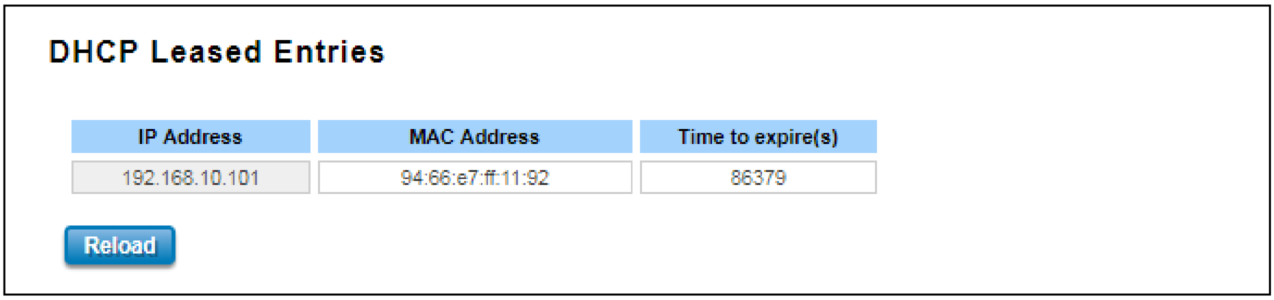
The description of the columns is as below:

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 inminutes. (Lease Time range: 15-44640 minutes)

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

➢ DHCP Leased Entries

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



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:

3.26 Port Status

3.27 Port Setting

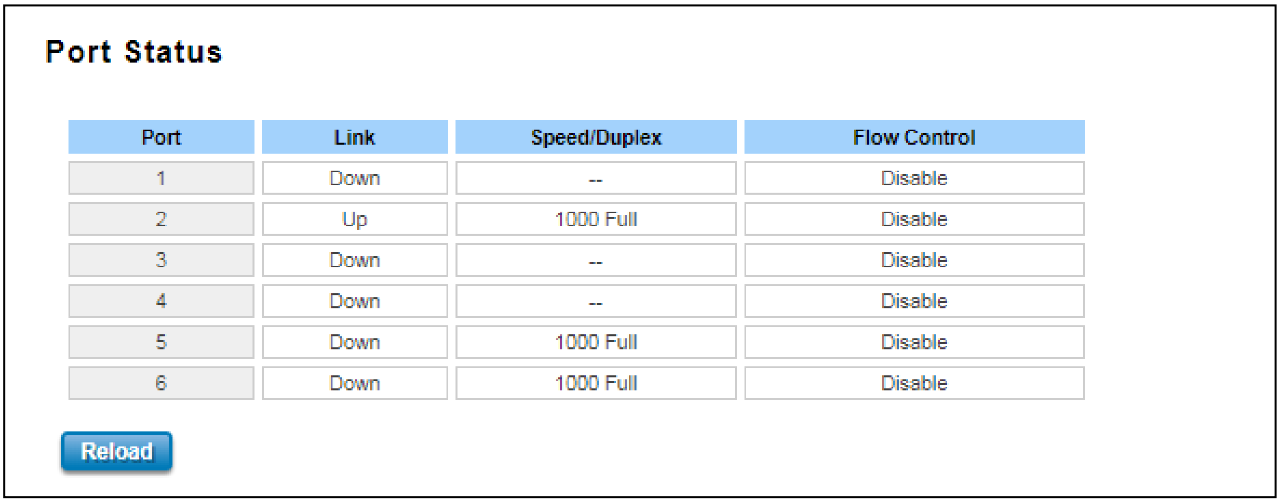
3.28 VLAN Setting

3.29 Rate Control

3.30 Traffic Control

3.2.1 Port Status

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

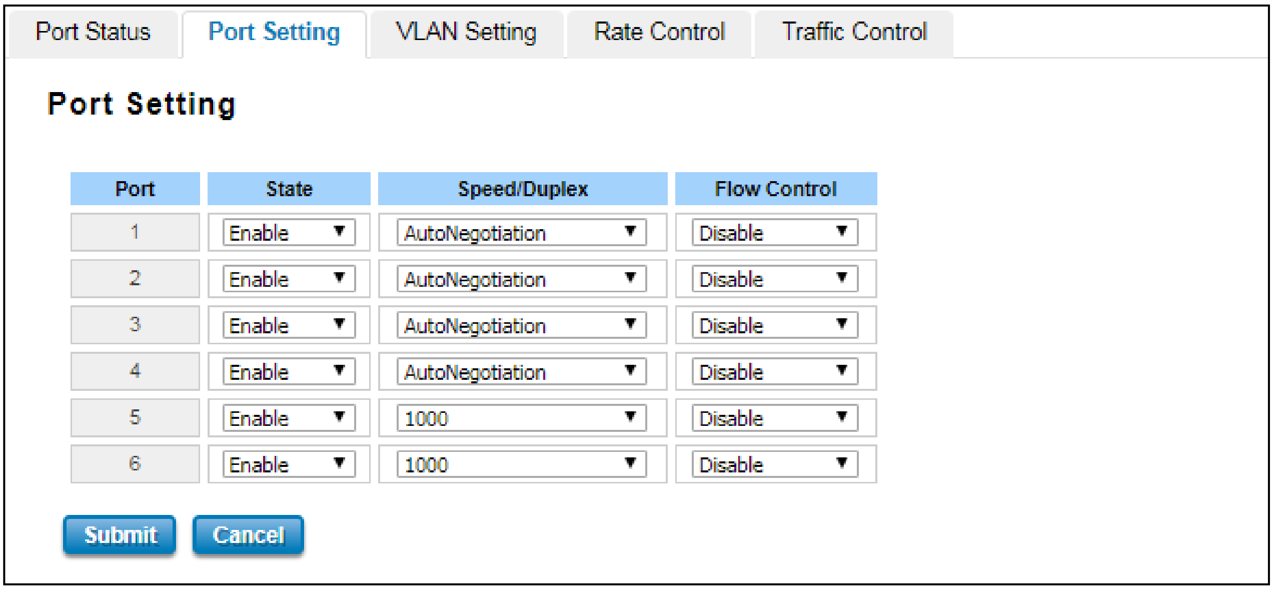


Port Status

Port	Link	Speed/Duplex	Flow Control
1	Down	--	Disable
2	Up	1000 Full	Disable
3	Down	--	Disable
4	Down	--	Disable
5	Down	1000 Full	Disable
6	Down	1000 Full	Disable

3.2.2 Port Setting

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



Port Setting

Port	State	Speed/Duplex	Flow Control
1	Enable	AutoNegotiation	Disable
2	Enable	AutoNegotiation	Disable
3	Enable	AutoNegotiation	Disable
4	Enable	AutoNegotiation	Disable
5	Enable	1000	Disable
6	Enable	1000	Disable

The description of the columns is as below:

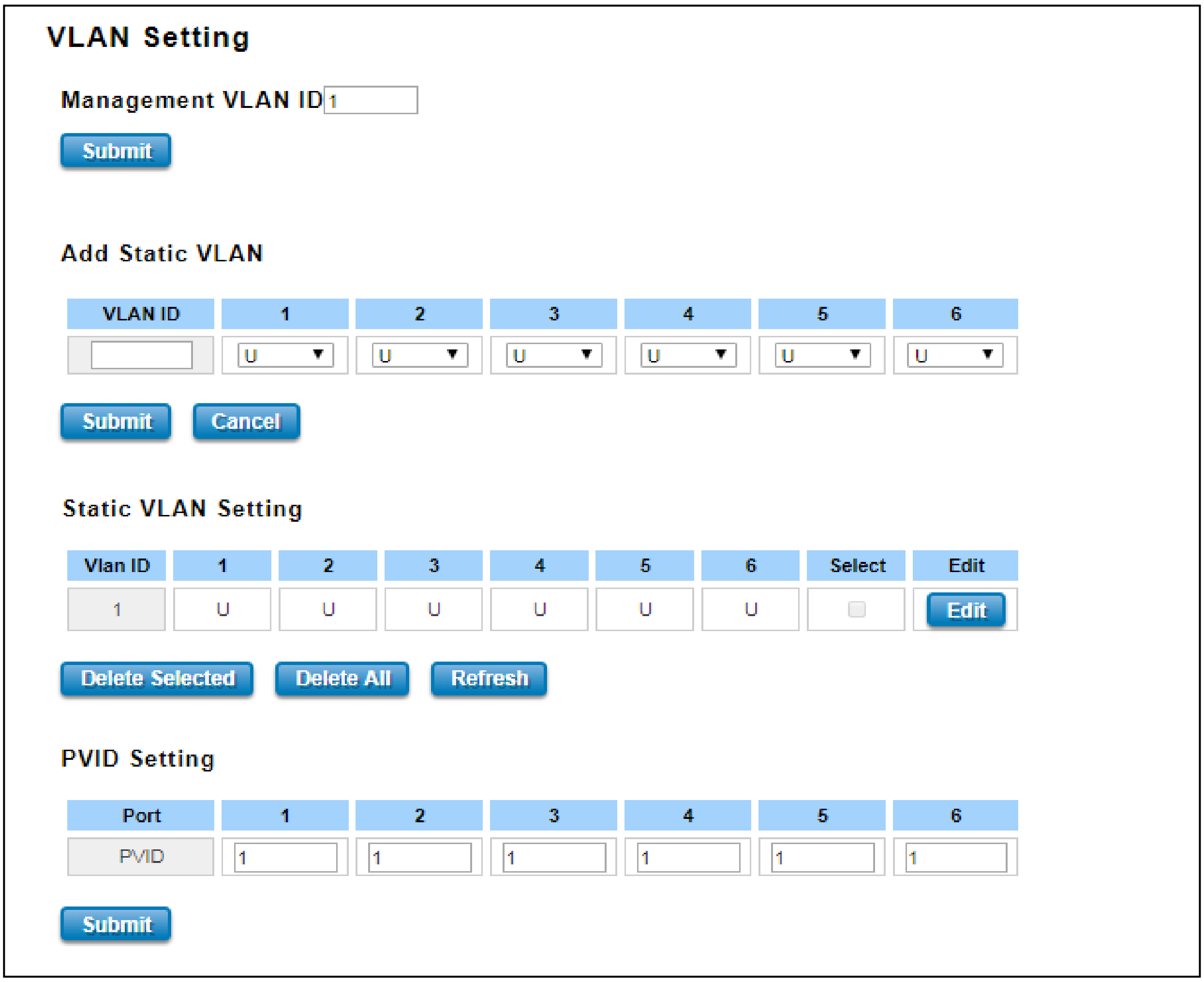
Terms	Description
Port	Shows port number
State	**Default: Enable** Enable or disable a port
Speed/Duplex	**Default: Auto Negotiation** Users can set the bandwidth of each port as Auto-negotiation(1000), 100 full,100 half,10 full,10 half mode for **Giga Ethernet Port 1~4**. For **Fiber Port 5~6:** it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

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

3.2.3 VLAN Setting

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

The description of the columns is as below:



VLAN Setting

Management VLAN ID 1

Submit

Add Static VLAN

VLAN ID	1	2	3	4	5	6
	U ▼	U ▼	U ▼	U ▼	U ▼	U ▼

Submit Cancel

Static VLAN Setting

Vlan ID	1	2	3	4	5	6	Select	Edit
1	U	U	U	U	U	U	□	Edit

Delete Selected Delete All Refresh

PVID Setting

Port	1	2	3	4	5	6
PVID	1	1	1	1	1	1

Submit

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

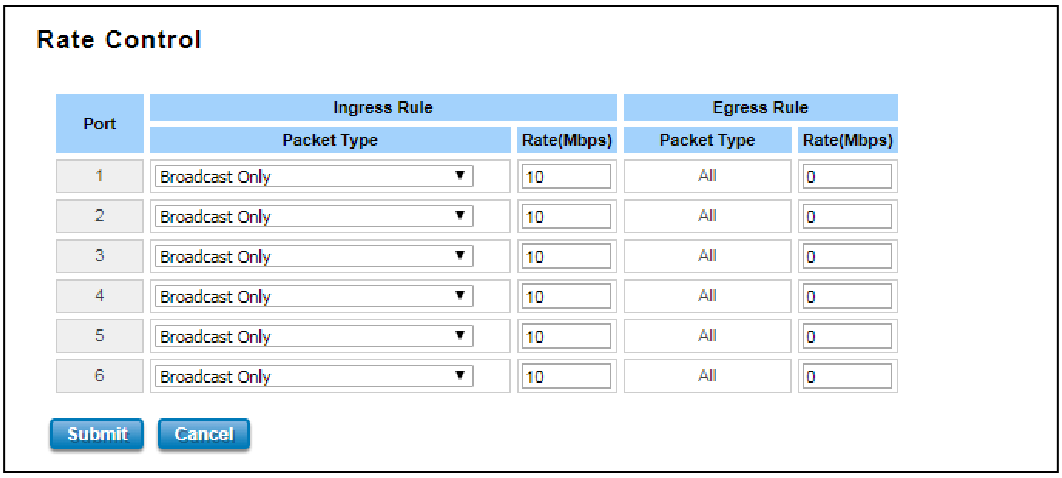
The steps to create a new VLAN: Type in Add Static VLAN section and click Submit to create a new VLAN. Then User can see the new VLAN in the Static VLAN Setting table. After created the VLAN, the status of the VLAN will remain in Unused until User adds ports to the VLAN.

NOTE:

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

3.2.4 Rate Control

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



Rate Control

Port	Ingress Rule		Egress Rule	
	Packet Type	Rate(Mbps)	Packet Type	Rate(Mbps)
1	Broadcast Only ▼	10	All	0
2	Broadcast Only ▼	10	All	0
3	Broadcast Only ▼	10	All	0
4	Broadcast Only ▼	10	All	0
5	Broadcast Only ▼	10	All	0
6	Broadcast Only ▼	10	All	0

The description of the columns is as below:

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

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

3.3 Power Over Ethernet

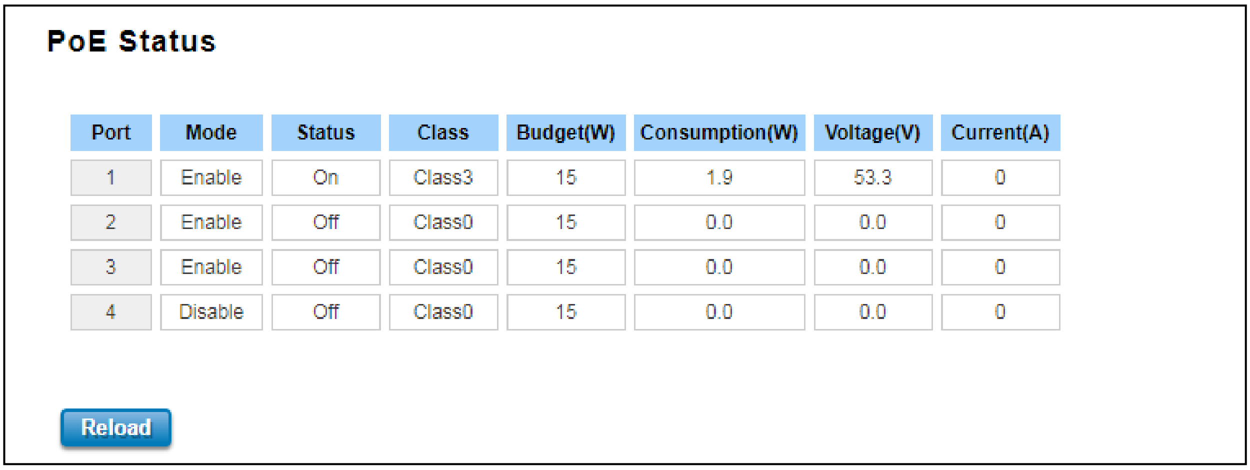
Power over Ethernet has become increasingly popular due in large part to the reliability provided by PoE Ethernet switches that supply the necessary power to Powered Devices (PD) when AC power is not readily available or cost-prohibitive to provide locally. Avcomm router compliant with IEEE 802.3af and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

Power over Ethernet can be used with:

- Surveillance cameras
- Security I/O sensors
- Industrial wireless access points
- Emergency IP phones

3.3.1 PoE Status

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



PoE Status

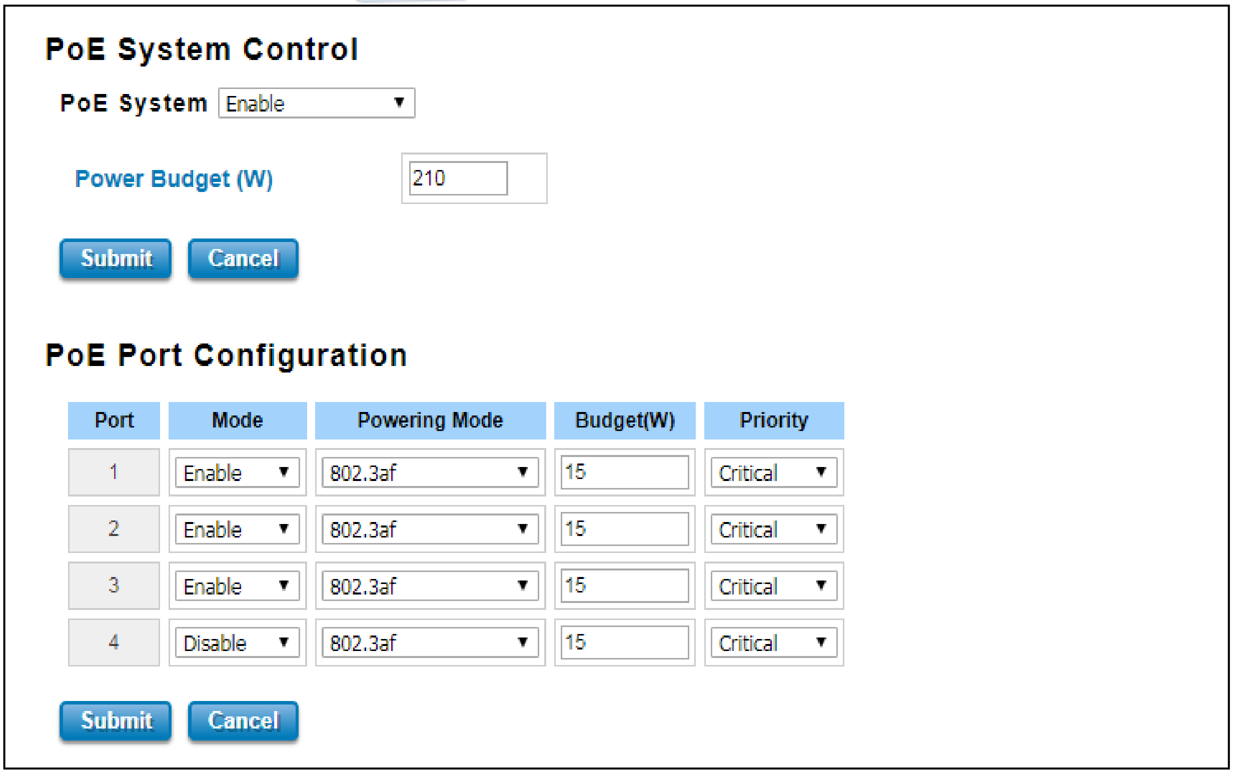
Port	Mode	Status	Class	Budget(W)	Consumption(W)	Voltage(V)	Current(A)
1	Enable	On	Class3	15	1.9	53.3	0
2	Enable	Off	Class0	15	0.0	0.0	0
3	Enable	Off	Class0	15	0.0	0.0	0
4	Disable	Off	Class0	15	0.0	0.0	0

The description of the columns is as below:

Terms	Description
Mode	Enable/Disable/Schedule Indicates the PoE port status
Status	**Default: Off** PoE status is included Off, Powering, and Searching.Off – PoE is inactive. Powering – PoE is enabled and powering the PD. Searching – Searching the PD which needs the power.
Class	Indicates the PD included in which PoE class.
Budget(W)	Indicates the actual Budget value for PoE port
Consumption (W)	Indicates the actual Power consumed value for PoE port
Voltage (V)	Indicates the actual Voltage consumed value for PoE port
Current (A)	Indicates the actual Current consumed value for PoE port

3.3.2 PoE Port Setting

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



PoE System Control

PoE System: Enable

Power Budget (W): 210

PoE Port Configuration

Port	Mode	Powering Mode	Budget(W)	Priority
1	Enable	802.3af	15	Critical
2	Enable	802.3af	15	Critical
3	Enable	802.3af	15	Critical
4	Disable	802.3af	15	Critical

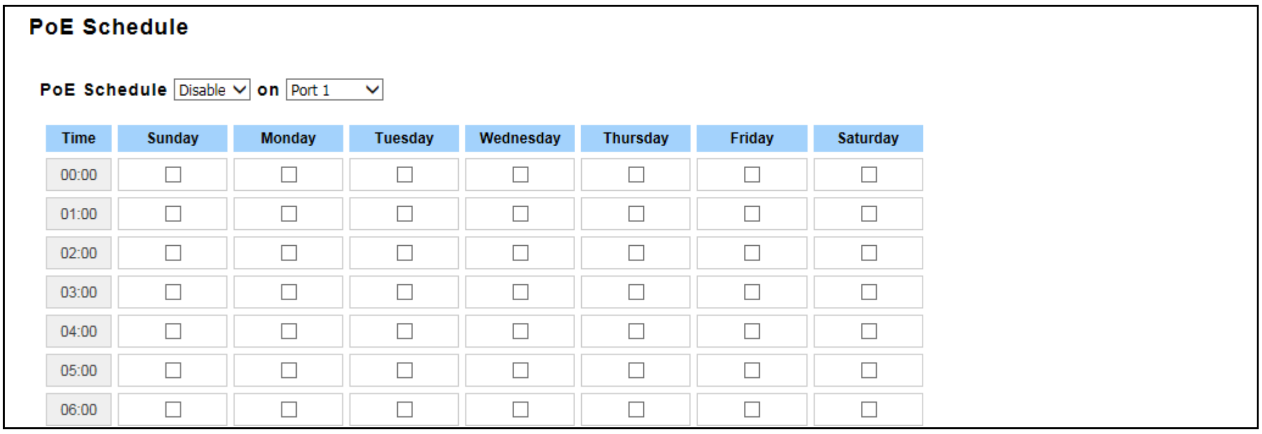
The description of the columns is as below:

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

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

3.3.3 PoE Schedule

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



PoE Schedule

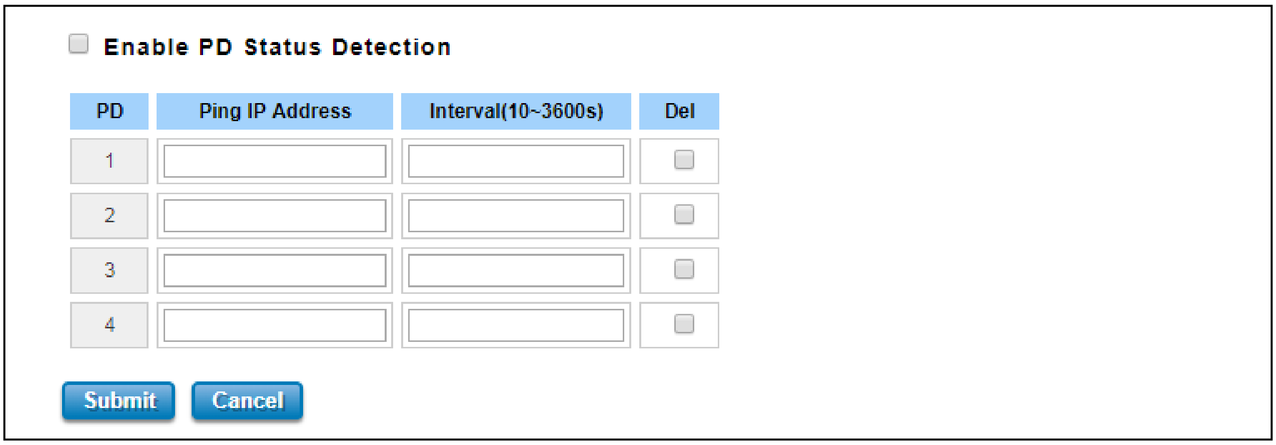
PoE Schedule [Disable] on [Port 1]

Time	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00	□	□	□	□	□	□	□
01:00	□	□	□	□	□	□	□
02:00	□	□	□	□	□	□	□
03:00	□	□	□	□	□	□	□
04:00	□	□	□	□	□	□	□
05:00	□	□	□	□	□	□	□
06:00	□	□	□	□	□	□	□

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

3.3.4 Alive Check

➢ PD Alive Check



□ **Enable PD Status Detection**

PD	Ping IP Address	Interval(10~3600s)	Del
1			□
2			□
3			□
4			□

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

Terms	Description
Ping IP address	PD's IP-address that installed on the port.
Interval (10-3600s)	User measured the PD system boots duration time. *Most of PD system – IP camera will take at least 40~50 seconds. Here, we suggest that user sets the cycle time to 90 seconds.
Delete	Delete PD's IP-address that

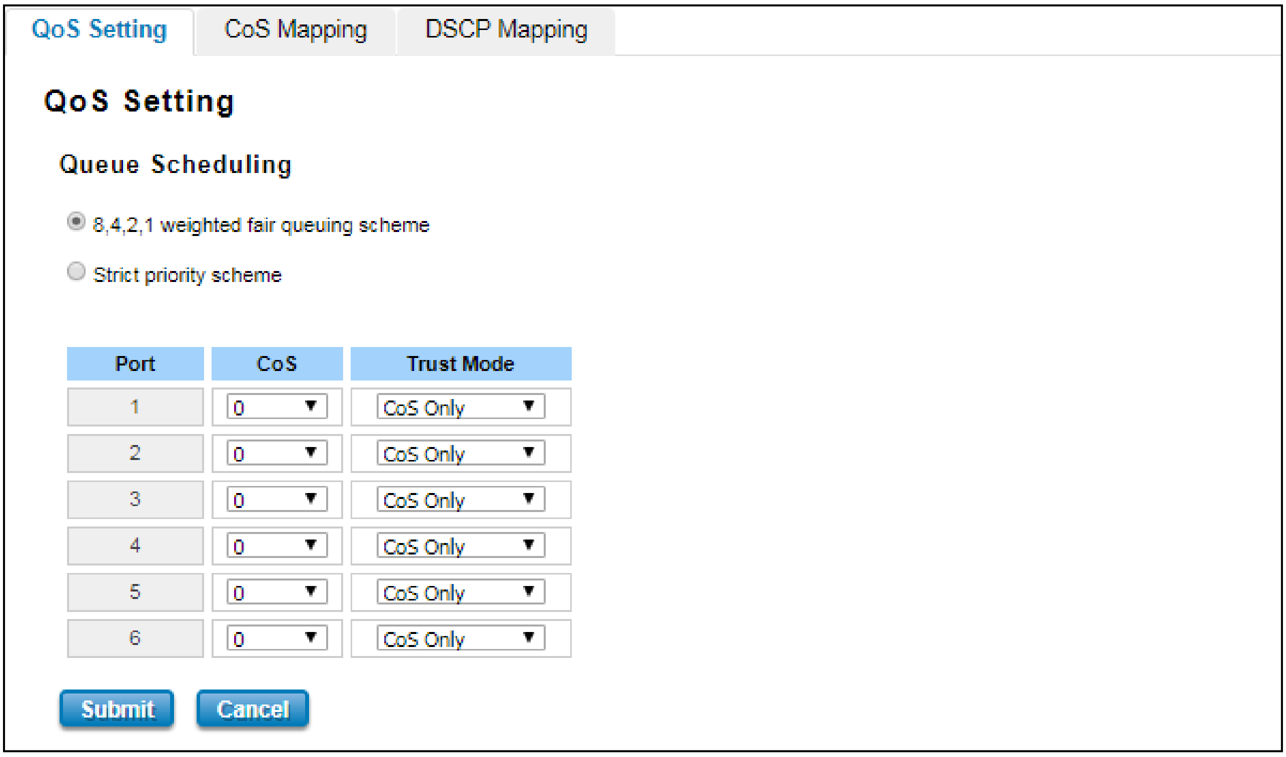
After finished configuring the settings, click on **Submit** to save the configuration

3.4 Quality of Service (QoS)

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

3.4.1 QoS Setting

The figure below shows QoS Setting.



QoS Setting

Queue Scheduling

● 8,4,2,1 weighted fair queuing scheme

○ Strict priority scheme

Port	CoS	Trust Mode
1	0	CoS Only
2	0	CoS Only
3	0	CoS Only
4	0	CoS Only
5	0	CoS Only
6	0	CoS Only

- Queue Scheduling

User may select the Queue Scheduling rule:

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

Use a strict priority scheme: The priority here is always the higher queue will be processed first, except the higher queue is empty.

The description of the columns is as below:

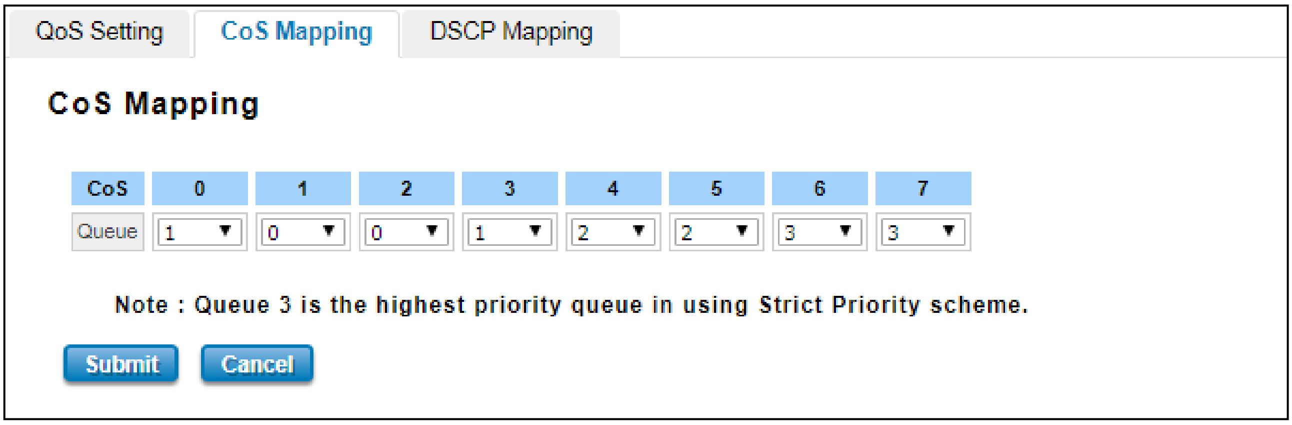
Terms	Description
CoS	Indicate default port priority value for untagged or priority-tagged frames.
Trust Mode	**Default: COS Only** Indicate Queue Mapping types for User to select.

COS Only	Port priority will only follow COS-Queue Mapping User has assigned.
DSCP Only	Port priority will only follow DSCP-Queue Mapping User has assigned.
COS First	Port priority will follow COS-Queue Mapping first, and then DSCP-Queue Mapping rule.
DSCP First	Port priority will follow DSCP-Queue Mapping first, and then COS-Queue Mapping rule.

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

3.4.2 CoS Mapping

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



CoS Mapping

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

Note : Queue 3 is the highest priority queue in using Strict Priority scheme.

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

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

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

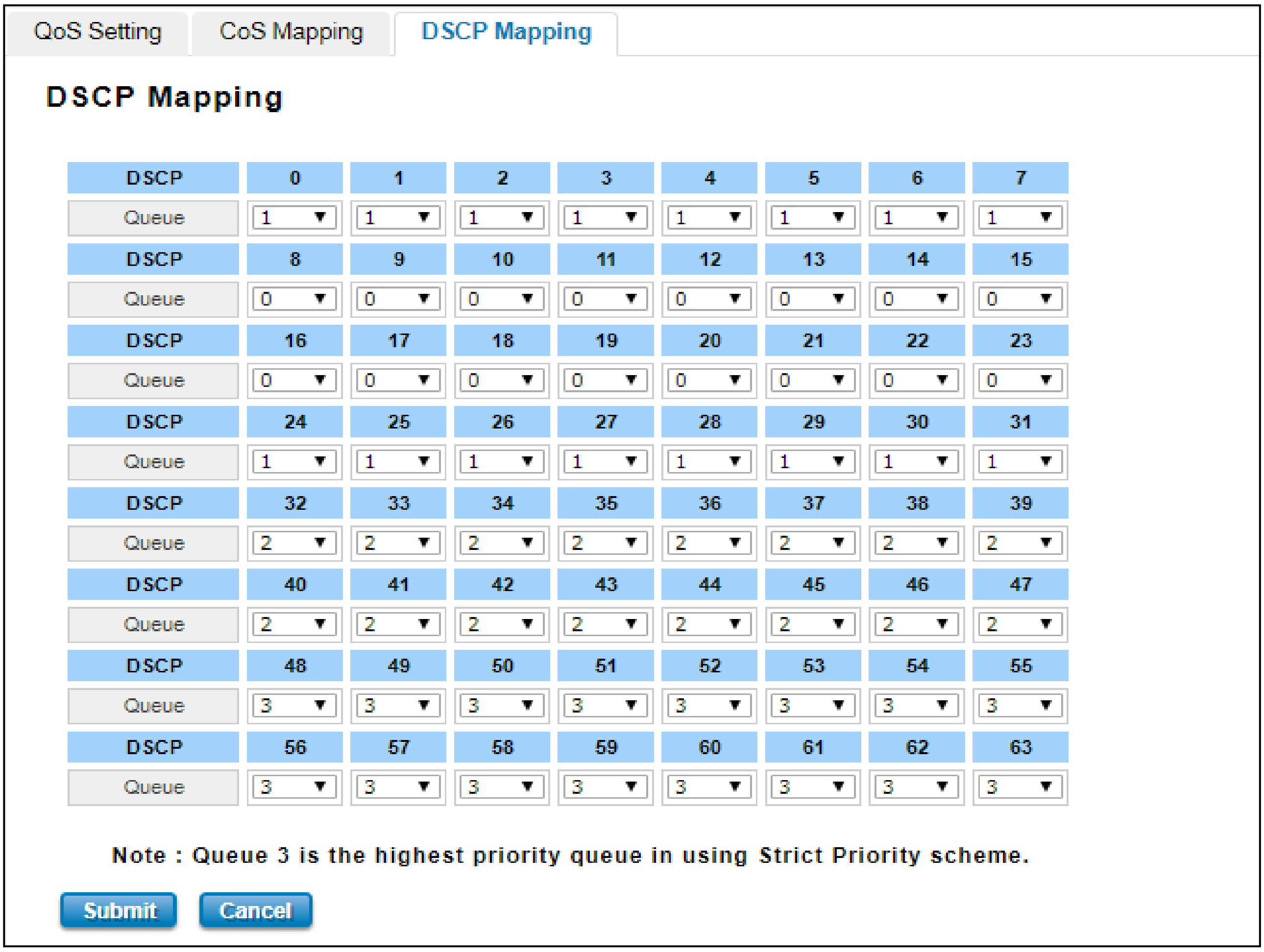
For the step in configuration

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

2. Click the Submit button.

3.4.3 DSCP Mapping

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



DSCP Mapping

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

Note : Queue 3 is the highest priority queue in using Strict Priority scheme.

After configuration, press Submit to enable the settings.

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

3.5 Multicast

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

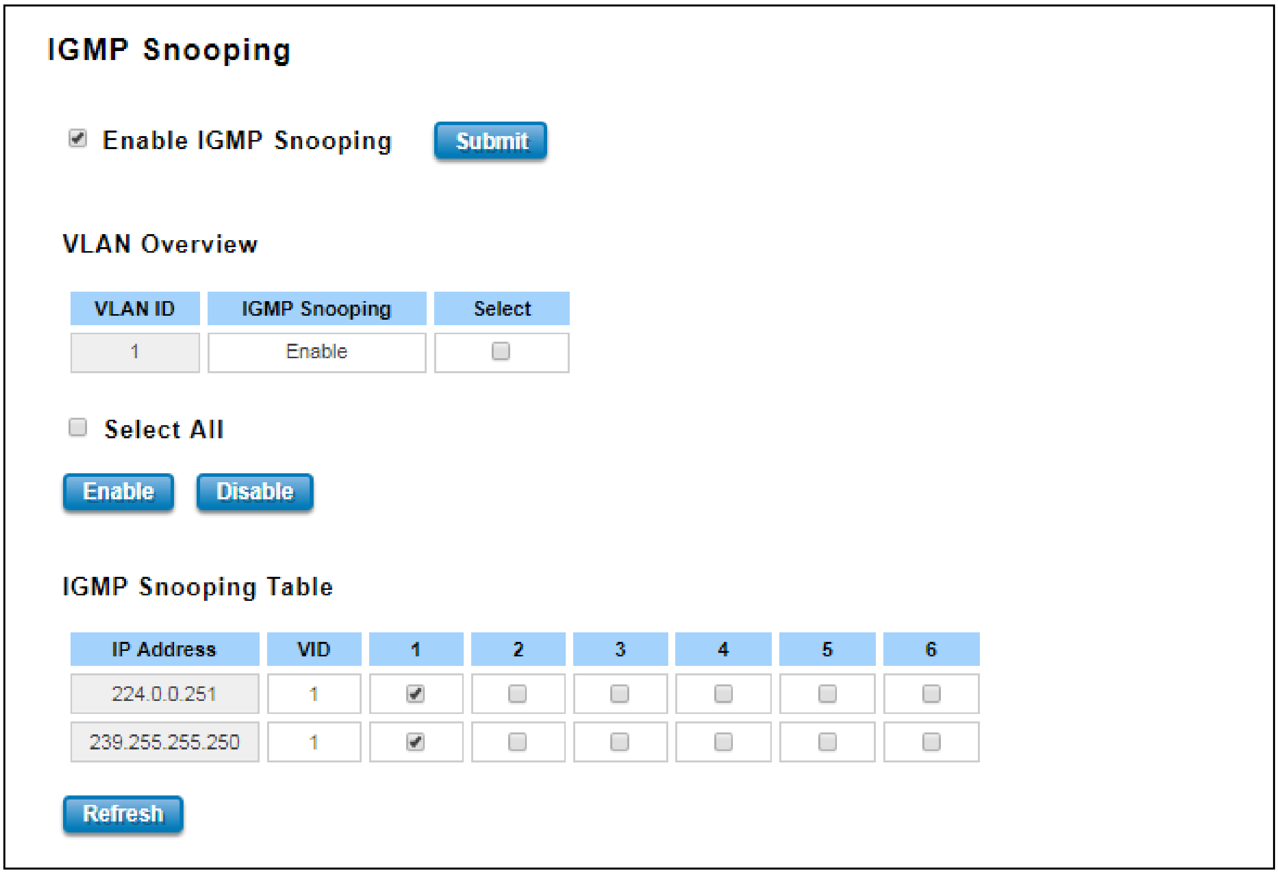
Following sections are included in this group:

3.1.1 IGMP Snooping

3.1.2 IGMP Query

3.5.1 IGMP Snooping

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



IGMP Snooping

☑ Enable IGMP Snooping

VLAN Overview

VLAN ID	IGMP Snooping	Select
1	Enable	□

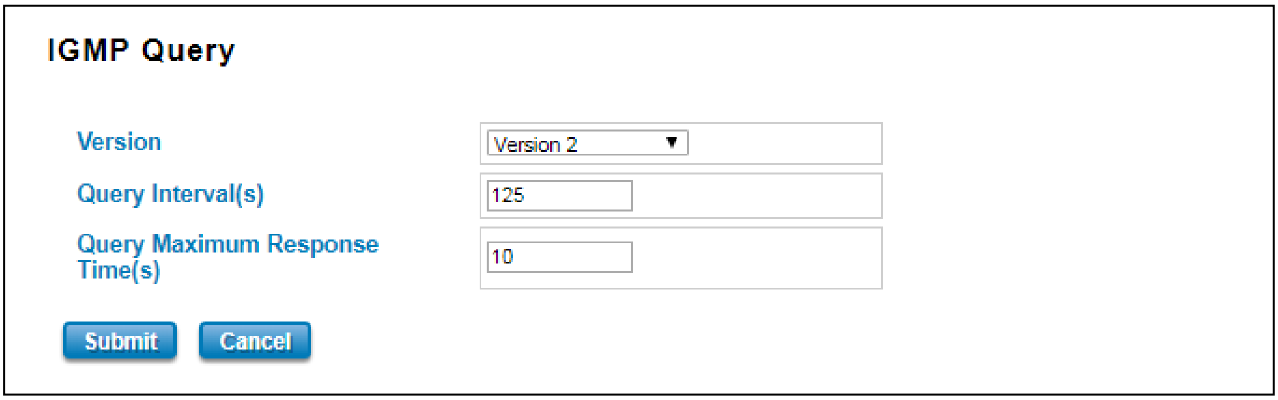
□ Select All

IGMP Snooping Table

IP Address	VID	1	2	3	4	5	6
224.0.0.251	1	☑	□	□	□	□	□
239.255.255.250	1	☑	□	□	□	□	□

3.5.2 IGMP Query

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



IGMP Query

Version: Version 2

Query Interval(s): 125

Query Maximum Response Time(s): 10

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

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

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

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

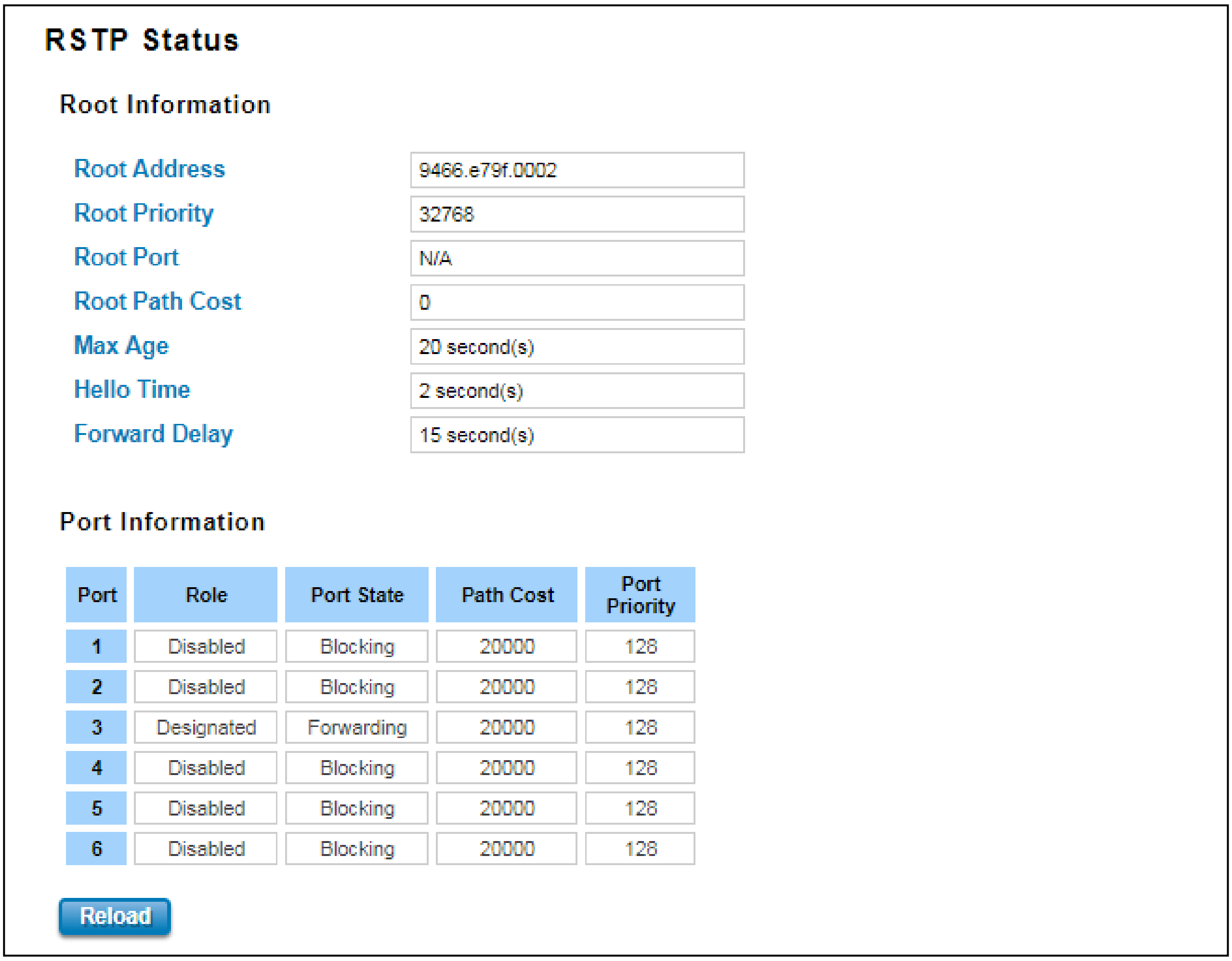
3.6 Redundancy

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

3.6.1 RSTP Status

➢ RSTP Status

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



RSTP Status

Root Information

Root Address	9466.e79f.0002
Root Priority	32768
Root Port	N/A
Root Path Cost	0
Max Age	20 second(s)
Hello Time	2 second(s)
Forward Delay	15 second(s)

Port Information

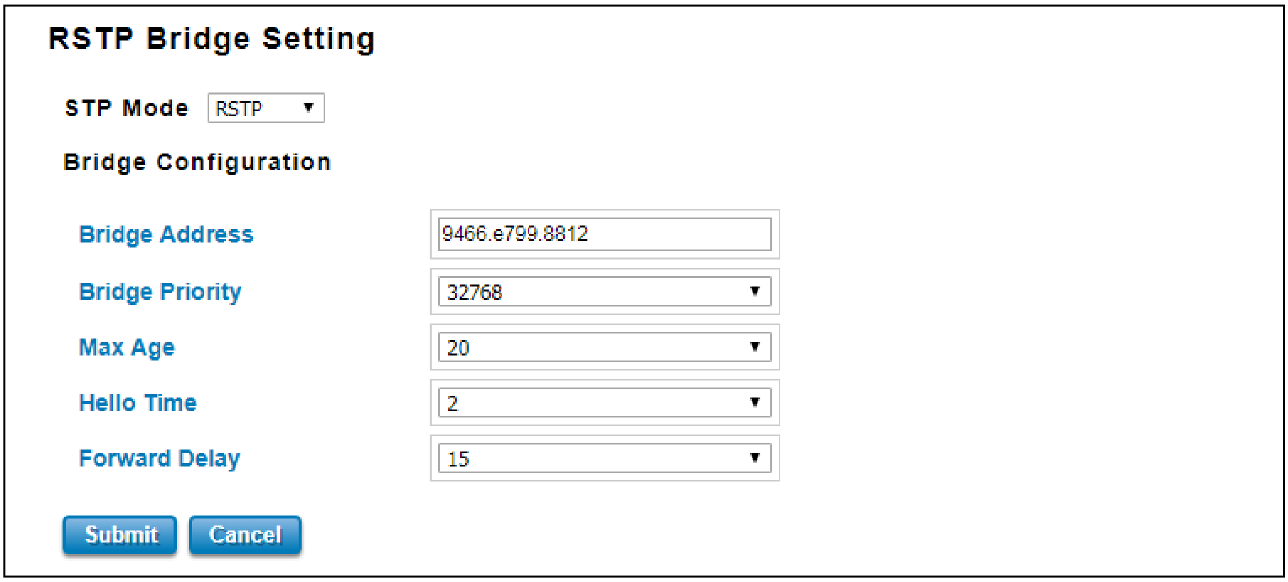
Port	Role	Port State	Path Cost	Port Priority
1	Disabled	Blocking	20000	128
2	Disabled	Blocking	20000	128
3	Designated	Forwarding	20000	128
4	Disabled	Blocking	20000	128
5	Disabled	Blocking	20000	128
6	Disabled	Blocking	20000	128

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

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

➢ RSTP Bridge Setting

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



RSTP Bridge Setting

STP Mode: RSTP

Bridge Configuration

Bridge Address	9466.e799.8812
Bridge Priority	32768
Max Age	20
Hello Time	2
Forward Delay	15

➢ Spanning Tree Protocol (STP)

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

➢ Rapid Spanning Tree Protocol (RSTP)

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

➢ Bridge Configuration

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

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

NOTE:

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

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

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

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

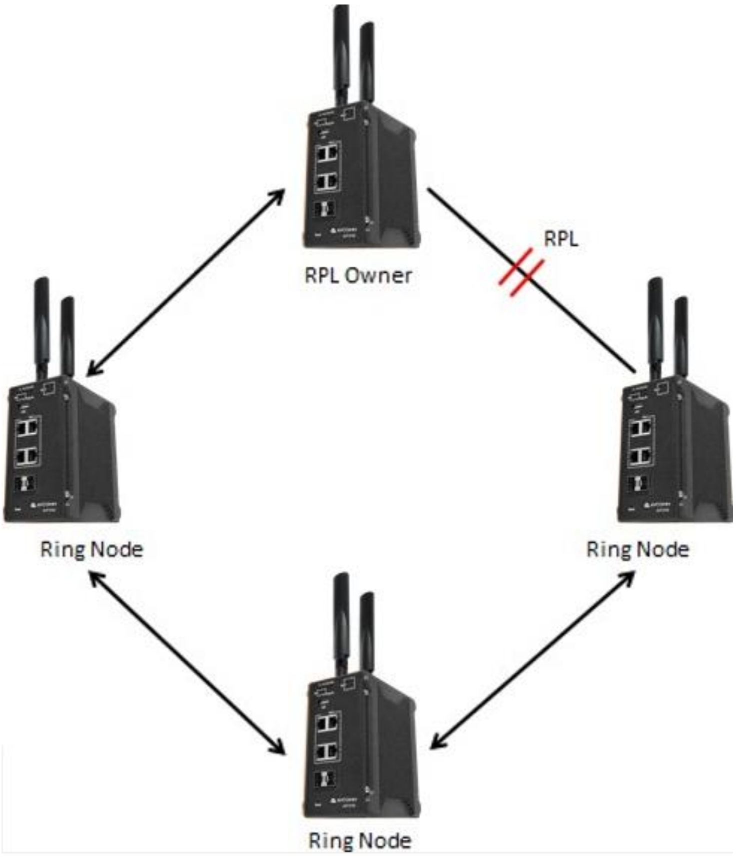
Once user has completed user configuration, click on Submit to apply user settings.

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

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

3.6.2 ERPS Settings

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

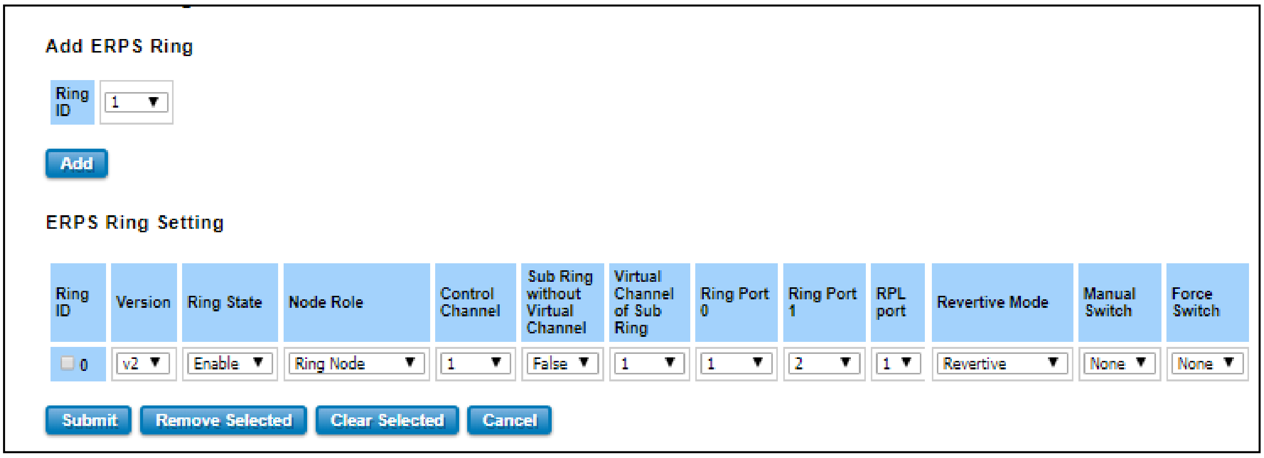


The figure above shows that each Ethernet Ring Node is connected to other Ethernet Ring Nodes that participating in the same Ethernet Ring using two independent links. In the Ethernet ring, loops can be avoided by guaranteeing that traffic may flow on all but one of the ring links at any time. This particular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

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

3.6.2.1 ERPS Settings

Add ERPS Ring



Add ERPS Ring

Ring ID: 1 ▼

ERPS Ring Setting

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

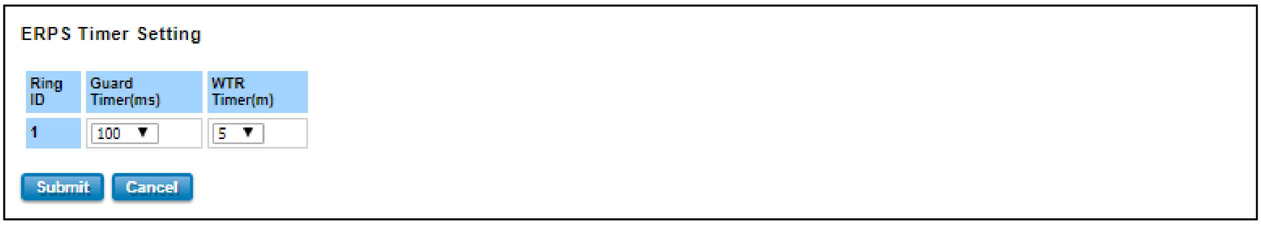
Add ERPS Ring is a section to add the Ring ID of the created Protection group; it must be an integer value between 0 and 31. The maximum numbers of ERPS Protection Groups that can be created are 32. Click the ID of a Protection group to enter the configuration page. After click Add button, one line will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

Below is the description table.

Terms	Description
Ring ID	Display the Ring ID
Version	ERPS Protocol Version - v1 or v2.
Ring State	**Default: Disable** Enable - Ring Status is enable Disable - Ring Status is disable
Node Role	It can be either RPL owner or RPL Neighbor or Ring Node.
Control Channel	**Default: 1** Control channel is implemented using a VLAN. Each ERP instance uses a tag-basedVLAN for sending and receiving R-APS messages. (1-4094)

Sub Ring without Virtual Channel	**Default: False** **True** – If doesn't have any virtual channel **False** – If have a virtual channel
Virtual Channel of Sub Ring	**Default: 1** Sub-rings can have a virtual channel on the interconnected node. Choose the numberbased on the VLANs Range (1-4094)
Ring Port 0	This will create a Port 0 of the switch in the Ring. Choose the port number that belongs to Ring port 0
Ring Port 1	This will create Port 1 of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance. Choose the port number that belongs to Ring port 1
RPL Port	This allows user to select the east port or west port as the RPL block.
Revertive Mode	**Default: Revertive** **Revertive mode**, after the conditions causing a protection switch has been cleared; the traffic channel is restored to the working transport entity, which is, blocked on theRPL. In **Non-Revertive mode**, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.
Manual Switch	**Default: None** In the absence of a failure or FS, Manual Switch command forces a block on the ringport where the command is issued. Choose 0 or 1, refers to Ring Port 0 or Ring Port 1
Force Switch	**Default: None** Forced Switch command forces a block on the ring port where the command is issued.Choose 0 or 1, refers to Ring Port 0 or Ring Port 1

- ERPS Timer Setting



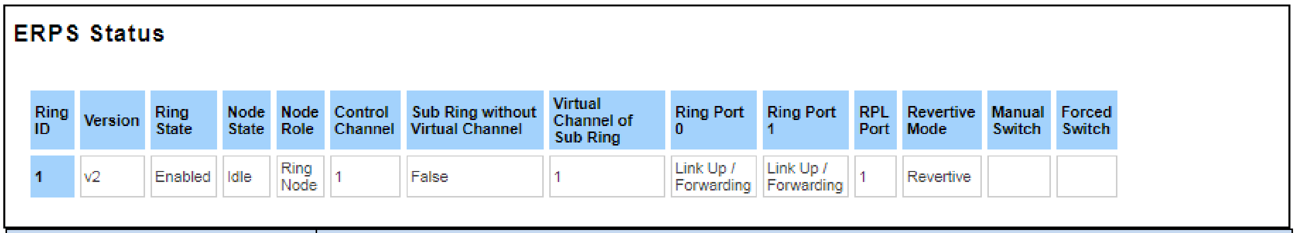
ERPS Timer Setting

Ring ID	Guard Timer(ms)	WTR Timer(m)
1	100 ▼	5 ▼

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

3.6.2.2 ERPS Status

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



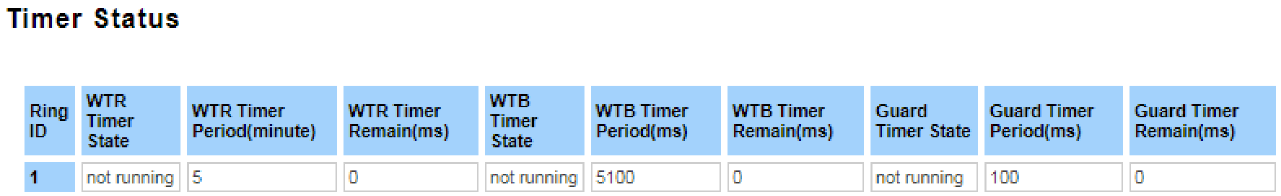
ERPS Status

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

Terms	Description
Ring ID	Display the Ring ID
Version	ERPS Protocol Version - v1 or v2.
Ring State	**Default: Disable** Enabled - Ring Status is enable Disabled - Ring Status is disable
Node State	Status from the **Ring is Idle, Protection** or **Pending.**
Node Role	It can be either **RPL owner** or **RPL Neighbor** or **Ring Node.**
Control Channel	Control Channel is referred to the VLANs number (1-4094)
Sub Ring without Virtual Channel	**Default: False** **True** – If have a virtual channel **False** – If doesn’t have any virtual channel
Virtual Channel of Sub Ring	**Default: 1** Sub-rings can have a virtual channel on the interconnected node. Choose the numberbased on the VLANs Range (1-4094)
Ring Port 0	The status from the port Link up/link down and Forwarding/Blocking
Ring Port 1	The status from the port Link up/link down and Forwarding/Blocking
RPL Port	The port status as the RPL block.
Revertive Mode	**Default: Revertive** **Revertive mode**, after the conditions causing a protection switch has been cleared; thetraffic channel is restored to the working transport entity, which is, blocked on the RPL.In **Non-Revertive mode**, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.

Manual Switch	Status from the Ring Port 0 and 1 or None
Force Switch	Status from the Ring Port 0 and 1 or None

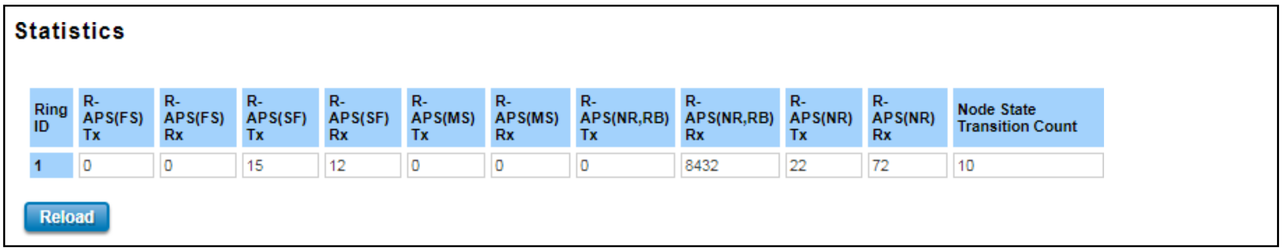
- Timer Status



Timer Status

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

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



Statistics

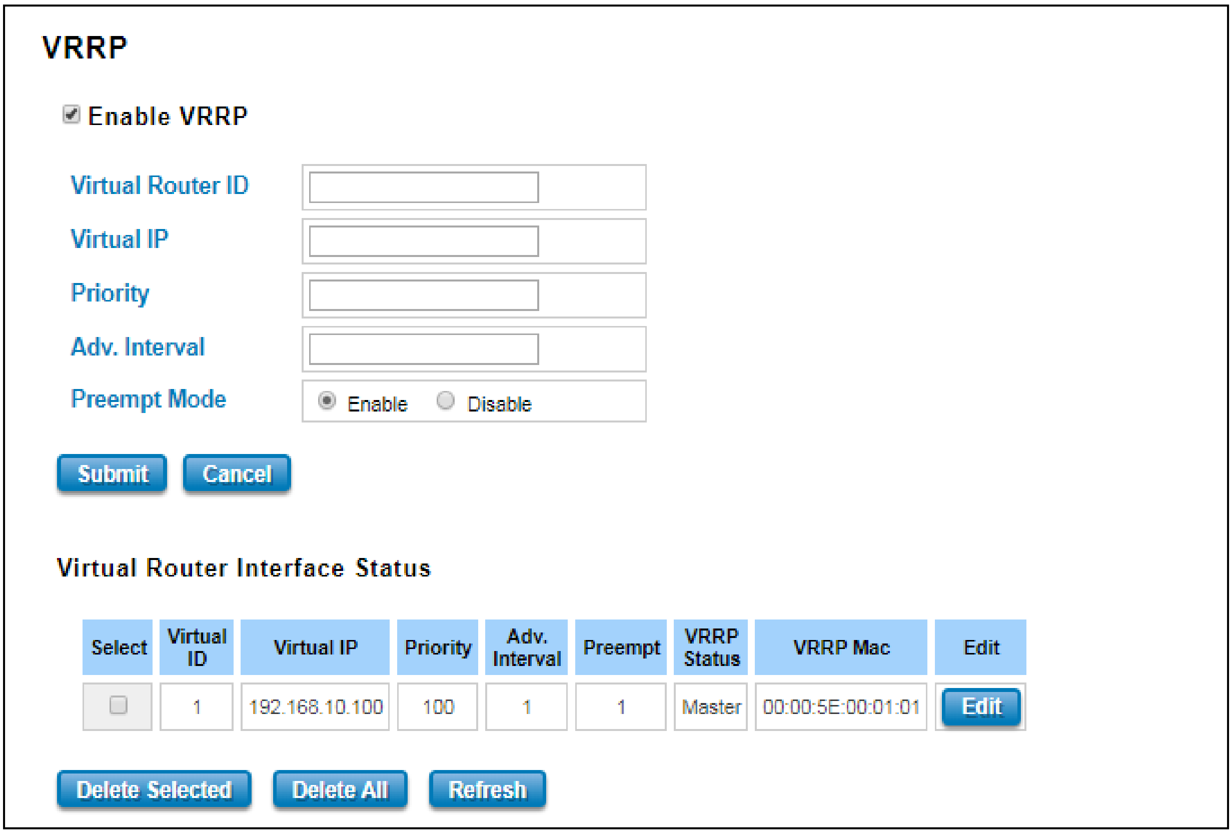
Ring ID	R-APS(FS) Tx	R-APS(FS) Rx	R-APS(SF) Tx	R-APS(SF) Rx	R-APS(MS) Tx	R-APS(MS) Rx	R-APS(NR,RB) Tx	R-APS(NR,RB) Rx	R-APS(NR) Tx	R-APS(NR) Rx	Node State Transition Count
1	0	0	15	12	0	0	0	8432	22	72	10

Terms	Description
Ring ID	Display the Ring ID.
R-APS(FS) Tx	The number of R-APS messages with Forced Switch (FS) being sent.
R-APS(FS) Rx	The number of R-APS messages with Forced Switch (FS) being received.
R-APS(SF) Tx	The number of R-APS messages with Signal Fail (SF) being sent.
R-APS(SF) Rx	The number of R-APS messages with Signal Fail (SF) being received.
R-APS(MS) Tx	The number of R-APS messages with Manual Switch (MS) being sent.
R-APS(MS) Rx	The number of R-APS messages with Manual Switch (MS) being received.
R-APS(NR, RB) Tx	The number of R-APS messages with a No Request, RPL Blocked (NR, RB) being sent.
R-APS(NR, RB) Rx	The number of R-APS messages with a No Request, RPL Blocked (NR, RB) being received.
R-APS(NR) Tx	The number of R-APS messages with a No Request (NR) being sent.
R-APS(NR) Rx	The number of R-APS messages with a No Request (NR) being received.

Node State Transition Count	The number of state transition that detected in the Ring.

3.6.3 VRRP

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



VRRP

☑ Enable VRRP

Virtual Router ID	
Virtual IP	
Priority	
Adv. Interval	
Preempt Mode	● Enable ○ Disable

Virtual Router Interface Status

Select	Virtual ID	Virtual IP	Priority	Adv. Interval	Preempt	VRRP Status	VRRP Mac	Edit
□	1	192.168.10.100	100	1	1	Master	00:00:5E:00:01:01	Edit

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

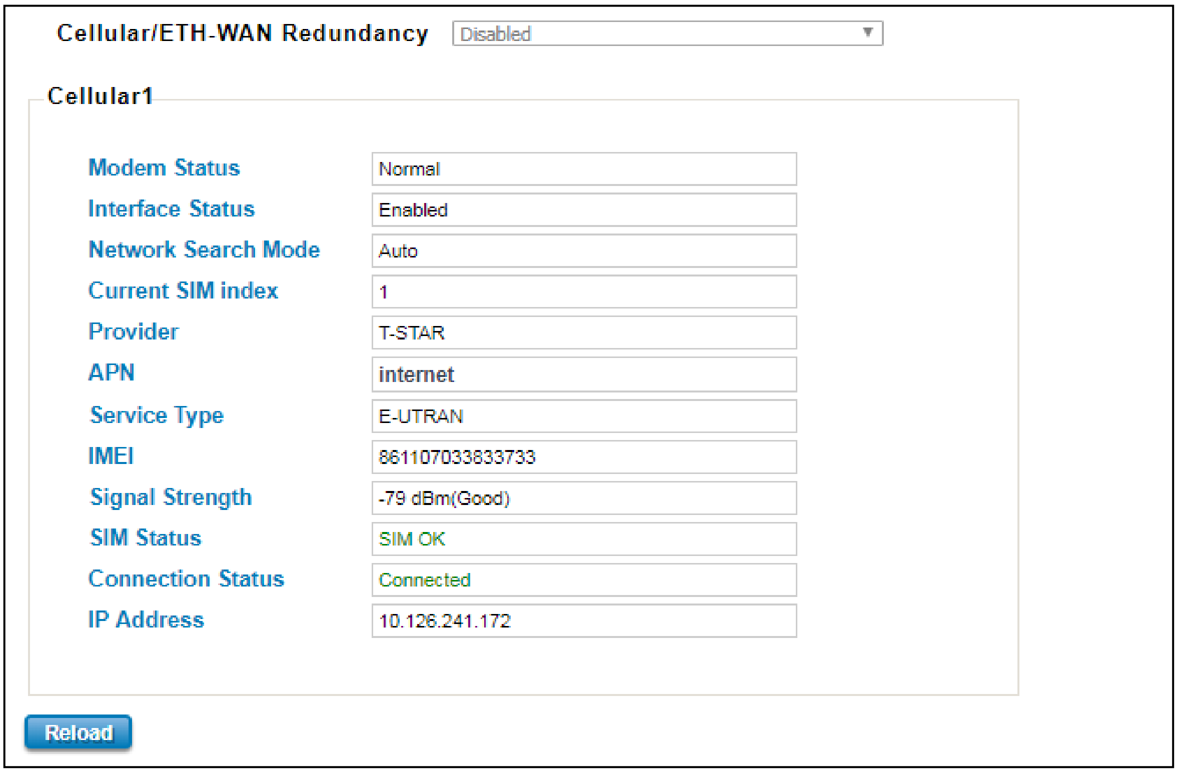
Adv. Interval	This field indicates how often the VRRP switches exchange the VRRP settings.
Preempt	While the VRRP Master link is failure, the VRRP Backup will take over its job immediately. However, while the VRRP master link is recovered, who shouldbe the Master? The Preempt decide whether the VRRP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

3.7 Cellular

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

3.7.1 Cellular Status

The figure below shows Cellular Status.

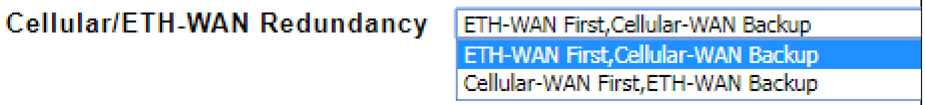


Cellular/ETH-WAN Redundancy: Disabled

Cellular1

Modem Status	Normal
Interface Status	Enabled
Network Search Mode	Auto
Current SIM index	1
Provider	T-STAR
APN	internet
Service Type	E-UTRAN
IMEI	861107033833733
Signal Strength	-79 dBm(Good)
SIM Status	SIM OK
Connection Status	Connected
IP Address	10.126.241.172

The description of the columns is as below:

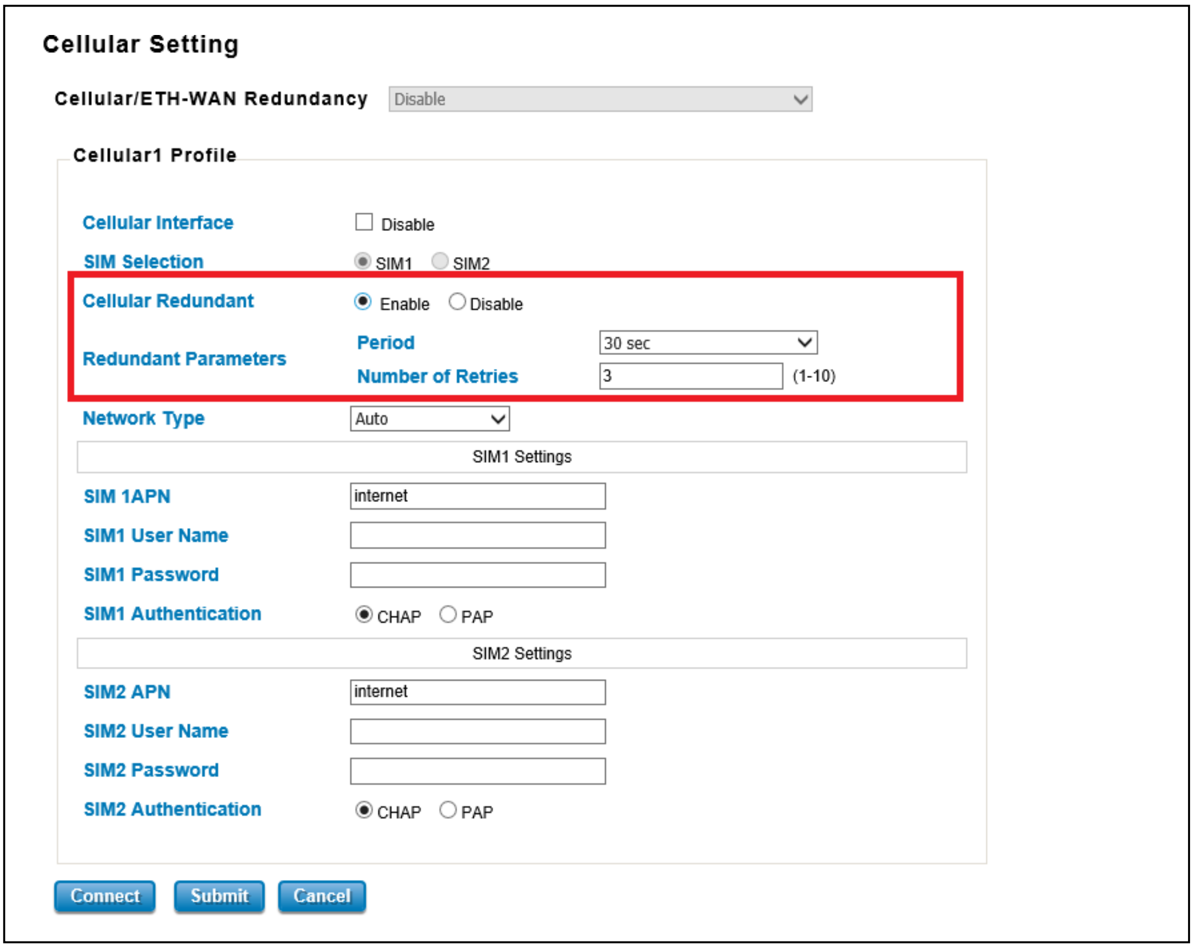
Terms	Description
Cellular/ETH.WAN Redundancy	**Default: Disabled** User can choose the redundancy mode: Cellular/ETH-WAN Redundancy ETH-WAN First,Cellular-WAN Backup ETH-WAN First,Cellular-WAN Backup Cellular-WAN First,ETH-WAN Backup **ETH-WAN First, Cellular-WAN Backup**: by choosing this mode, the 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 Search Mode	Display the network search mode (Auto, 2G Only, 3G Only and LTE Only)
Current SIM Index	Display the current in used SIM card (1 or 2)
Provider	Display the ISP that user used.
APN	Every ISP has a specific APN (Access Point Name) assigned to its cellular network. The system can read this name from the SIM card.
Service Type	The connected ISP will update the service type here. The possible types are GSM – 2G,UMTS – 3G, GSM W/EGPRS, UTRAN W/HSDPA (download), UTRAN W/HSUPA(upload), UTRAN W/HSDPA and HSUPA(download & upload), E-UTRAN - LTE , No Service(default value)
IMEI	Display the International Mobile Equipment Identity (IMEI)
Signal Strength	The signal strength to the remote connected base station. If the signal strength shows low,please change the device location or mounting the antenna in better location. Below are the signal strength definitions in our system:0 dBm (Default value while no connection) -113 dBm or less (Low) -111 dBm (Medium) -109…-53 dBm (Good) -51 dBm or greater (Excellent) -Not known or not detectable

SIM Status	Show the installed SIM Status. **SIM OK:** The SIM card is okay to use. **SIM not inserted:** The SIM card is not inserted. **SIM PIN Locked:** The SIM card is locked due to PIN error. It may be caused by errortyping 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.

3.7.2 Cellular Setting

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

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



Cellular Setting

Cellular/ETH-WAN Redundancy: Disable

Cellular1 Profile

Cellular Interface: □ Disable

SIM Selection: ● SIM1 ○ SIM2

Cellular Redundant: ● Enable ○ Disable

Redundant Parameters: Period: 30 sec; Number of Retries: 3 (1-10)

Network Type: Auto

SIM1 Settings

SIM 1APN: internet

SIM1 User Name:

SIM1 Password:

SIM1 Authentication: ● CHAP ○ PAP

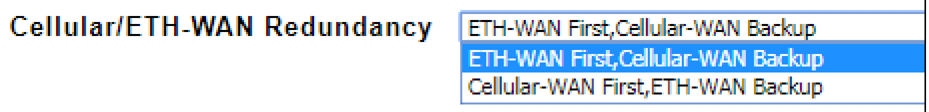
SIM2 Settings

SIM2 APN: internet

SIM2 User Name:

SIM2 Password:

SIM2 Authentication: ● CHAP ○ PAP

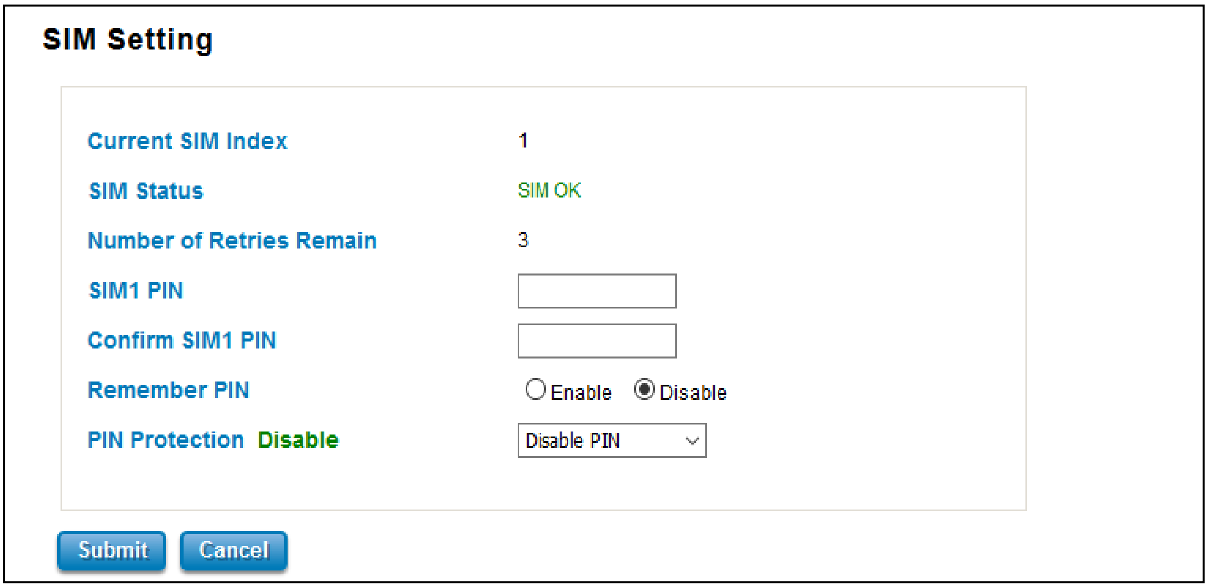
Terms	Description
Cellular/ETH.WAN Redundancy	**Default: Disabled** User can choose the redundancy mode: Cellular/ETH-WAN Redundancy ETH-WAN First,Cellular-WAN Backup ETH-WAN First,Cellular-WAN Backup Cellular-WAN First,ETH-WAN Backup **ETH-WAN First, Cellular-WAN Backup**: by choosing this mode, the 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.
SIM Selection	**Default: SIM1** User can select the SIM card 1 or 2 that want to be activated or used.
Cellular Redundant	**Default: Disable** By enable this function, the SIM redundant function will be activated. The main function of this feature is to have the backup SIM if the main SIM card is unable to use or have a problem connection. **Redundant Parameters** configuration appears after the user enables the function. **Period:** Set the period time to read the SIM card, if the SIM card cannot be read then it will directly change to the other SIM card. The default value is 30 Seconds. **Number of Entries:** Set the number of entries to give the remaining trial to read the SIM card. The default value is 3.
Network Type	Set the Network Type, the option would be:**Auto: Search the network automatically 2G Only: only receive the 2G signal.** **3G Only: only receive the 3G signal.** **LTE Only: only receive LTE/4G signal.**
SIM1/2 APN	Set the APN of the ISP.
SIM1/2 User Name	Set the User Name
SIM1/2 Password	Set the password.

SIM1/2 Authentication	Choose CHAP or PAP mode for the authentication mode. **CHAP**: Challenge Handshake Authentication Protocol, With CHAP, the authenticator (i.e. the server) sends a randomly generated ``challenge" string to the client, along with its hostname. **PAP**: Password Authentication Protocol, PAP works basically the same way as the normal loginprocedure. The authenticates itself by sending a username and a password to the server

Click Submit to apply the configuration.

3.7.3 SIM Setting

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



SIM Setting

Current SIM Index	1
SIM Status	SIM OK
Number of Retries Remain	3
SIM1 PIN	
Confirm SIM1 PIN	
Remember PIN	○ Enable ● Disable
PIN Protection Disable	Disable PIN

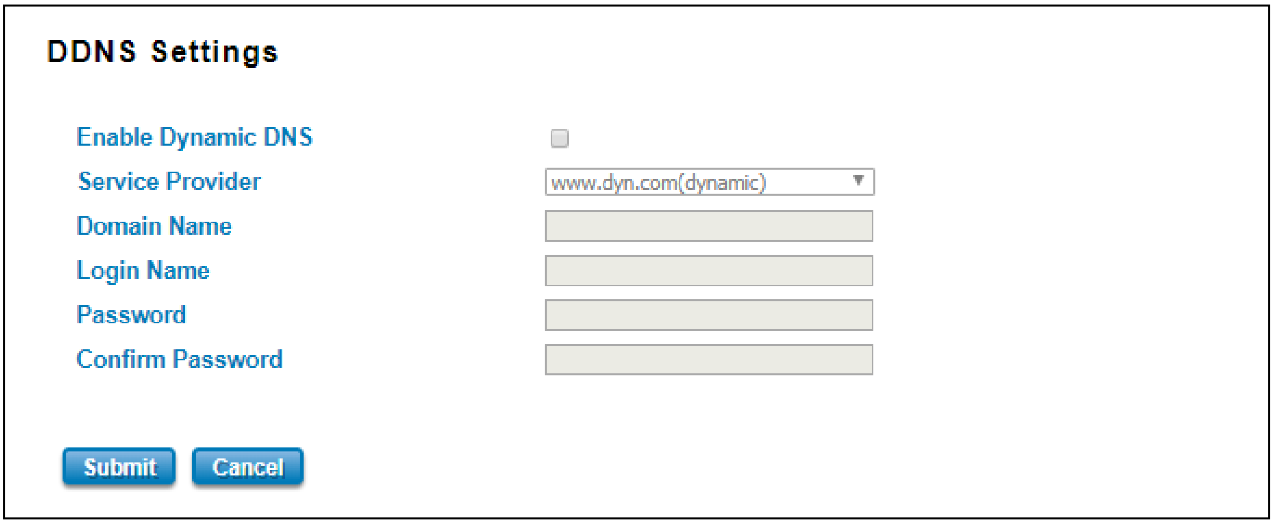
Terms	Description
Current SIM Index	Display the current in used SIM Card slot (1 / 2)
SIM Status	Show the installed SIM Status. **SIM OK:** The SIM card is okay to use. **SIM not inserted:** The SIM card is not inserted. **SIM PIN Locked:** The SIM card is locked due to PIN error. It may be causedby error typing PIN password many times. **WARNING:** SIM PUK Locked status will appear when the SIM Card PUK islocked due to PIN error after user three times input the wrong password.Contact the ISP to resolve the issue.

Number of Retries Remain	Display the remaining chance to enter the PIN numbers.
SIM1/2 PIN	Enter new SIM1/2 PIN numbers
Confirm SIM1/2 PIN	Confirm the new SIM1/2 PIN numbers
Remember PIN	Click enable to save the PIN numbers
PIN Protection	Activate the PIN protection feature. Choose the mode from the drop list. **Disable PIN**: Disable the PIN Protection feature **Enable PIN**: Activate the PIN Protection feature **Change PIN**: Change the PIN number, make sure user type the new PINNumber first at the SIM1 PIN textbox.

Click **Submit** to apply the configuration.

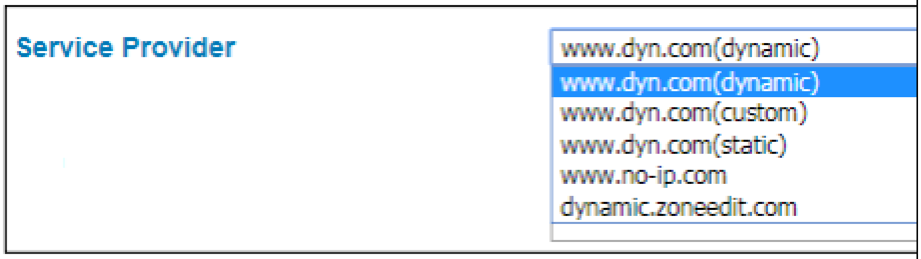
3.7.4 DDNS Setting

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



DDNS Settings

Enable Dynamic DNS	□
Service Provider	www.dyn.com(dynamic) ▼
Domain Name	
Login Name	
Password	
Confirm Password	

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.

Click **Submit** to apply the configuration.

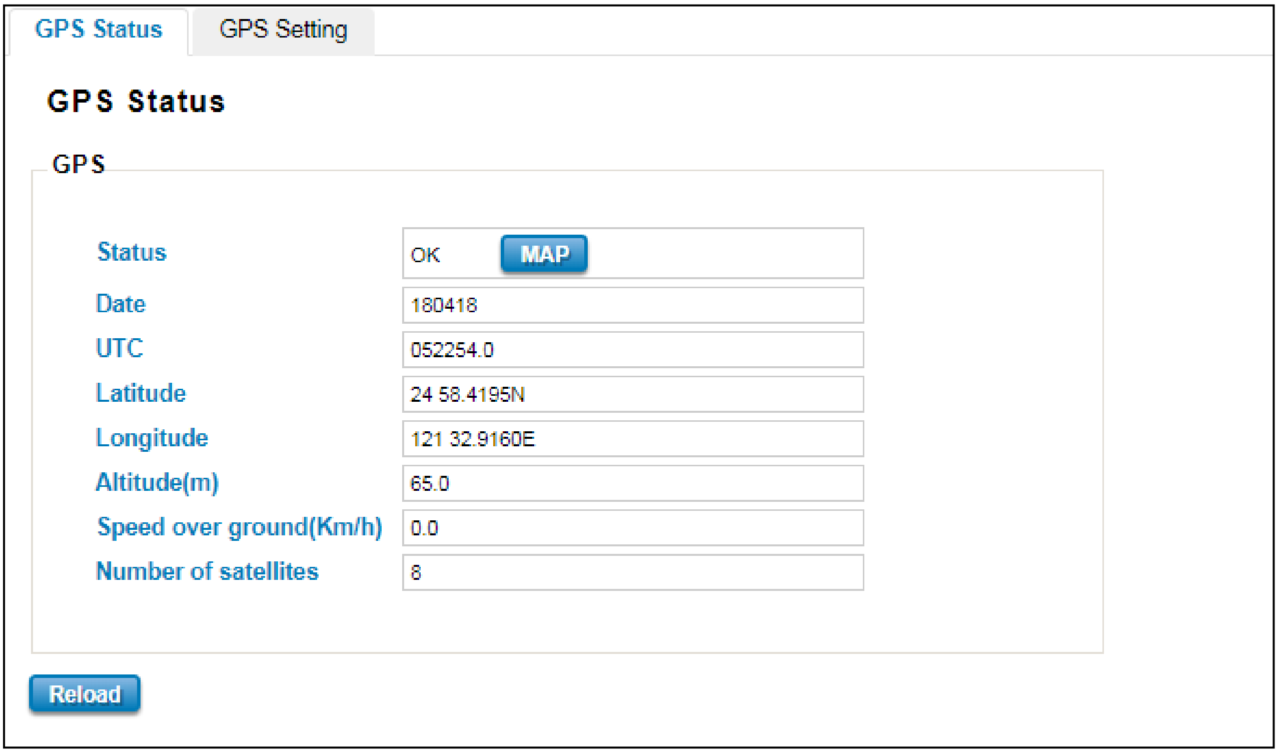
3.8 GPS

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

Whether user is navigating a position in a crowded city, a vast desert, or a dense forest, utilizing multiple GNSS systems can help the device stays connected and centered.

3.8.1 GPS Status

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



GPS Status

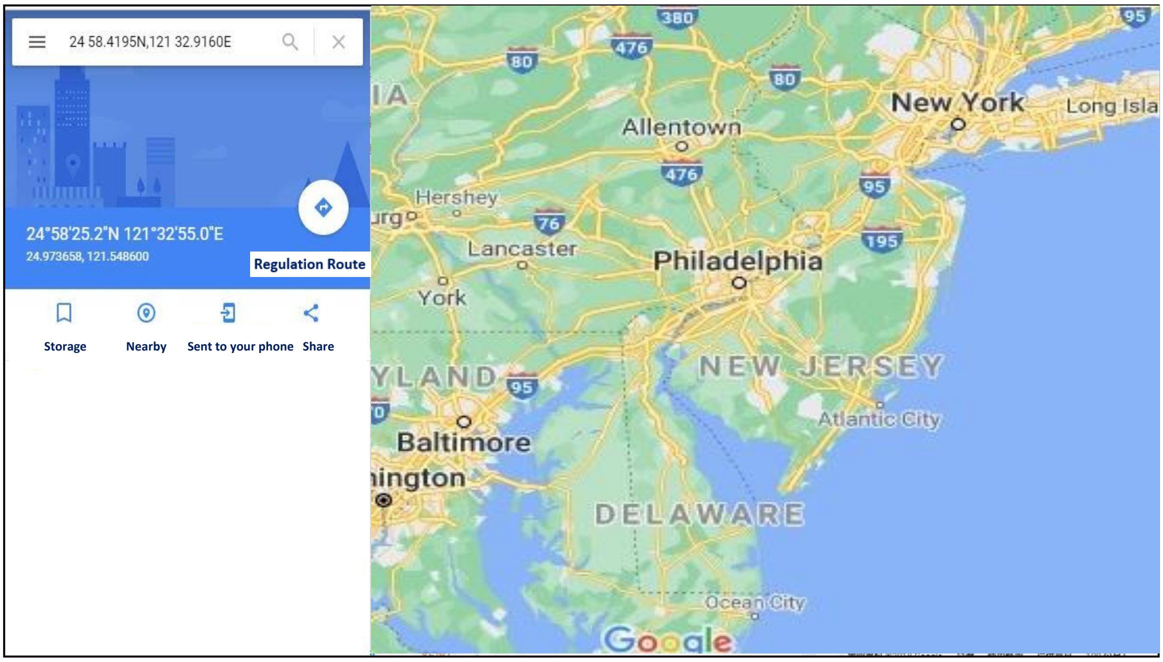
GPS

Status	OK
Date	180418
UTC	052254.0
Latitude	24 58.4195N
Longitude	121 32.9160E
Altitude(m)	65.0
Speed over ground(Km/h)	0.0
Number of satellites	8

The description of the columns is as below:

Terms	Description
Status	Display the GPS interface status OK or Disabled
Date	Display the current date.
UTC	Display the Coordinated Universal Time (UTC)
Latitude	Display the latitude of the coordinate
Longitude	Display the longitude of the coordinate
Altitude(m)	Display the altitude of the coordinate show the height or distance of an object from sea level.
Speed over ground(Km/h)	Display the speed over ground.
Number of satellites	Display the number of satellites that help to fix the position (Minimum 4 satellites).

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

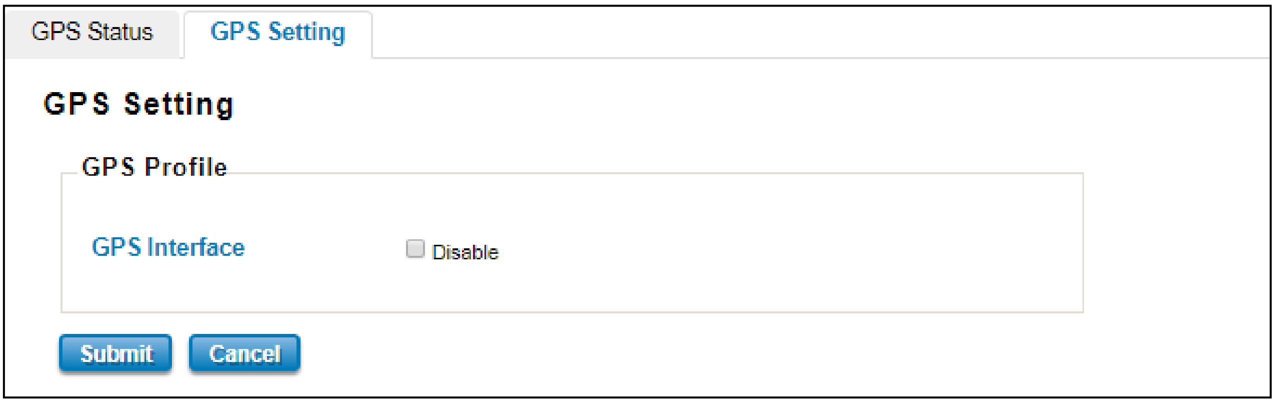


24 58.4195N,121 32.9160E

24°58'25.2"N 121°32'55.0"E
24.973658, 121.548600

3.8.2 GPS Setting

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



GPS Setting

GPS Profile

GPS Interface □ Disable

3.9 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:

3.1.3 Access Control

3.1.4 Port Security

3.1.5 Outbound Firewall

3.1.6 NAT Setting

3.1.7 OpenVPN

3.1.8 IPSec Setting

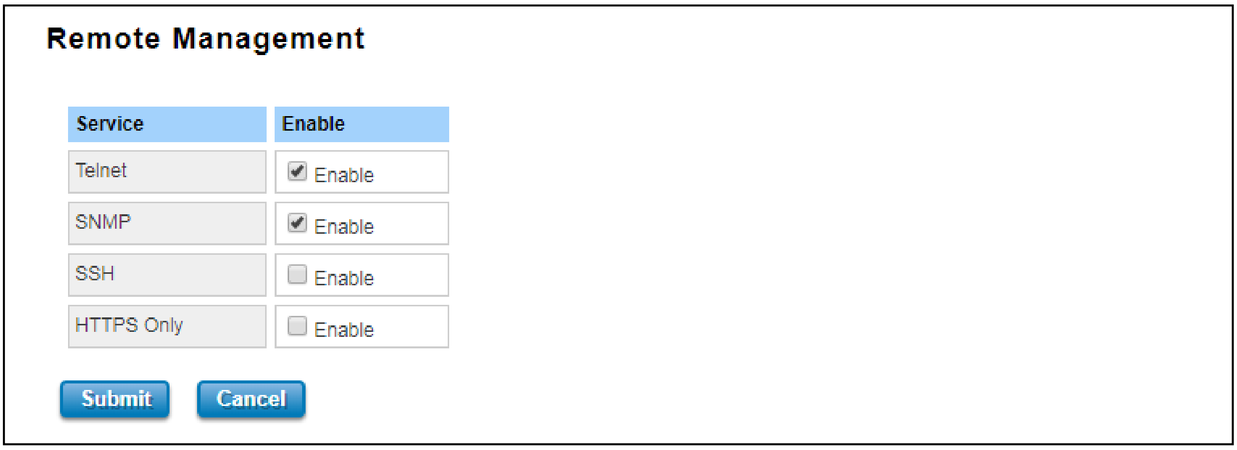
3.1.9 L2TP Setting

3.9.1 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

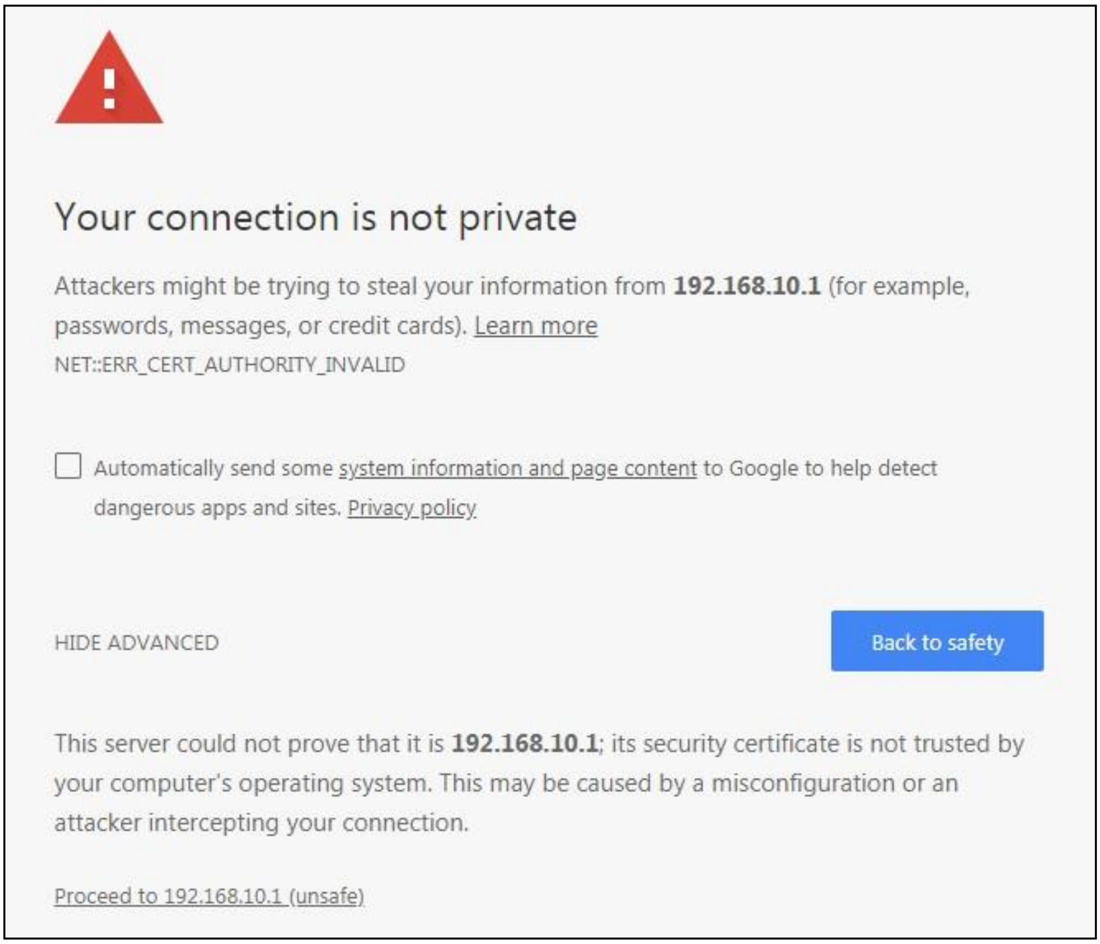
The description of the columns is as below:

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

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

➢ HTTPS Only

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



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

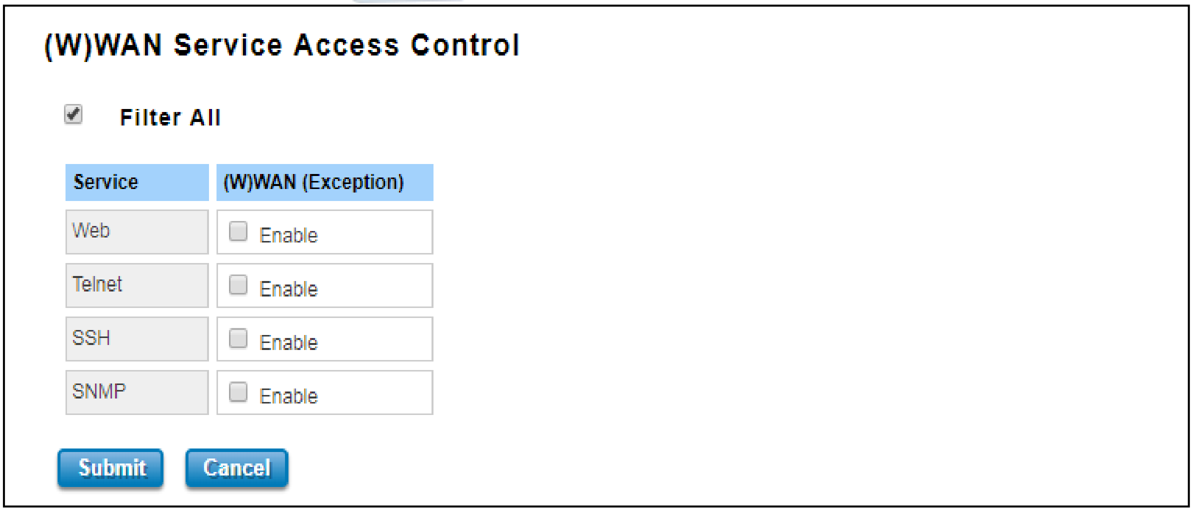
This server could not prove that it is **192.168.10.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.10.1 (unsafe)

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

➢ WAN Access

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



(W)WAN Service Access Control

☑ Filter All

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

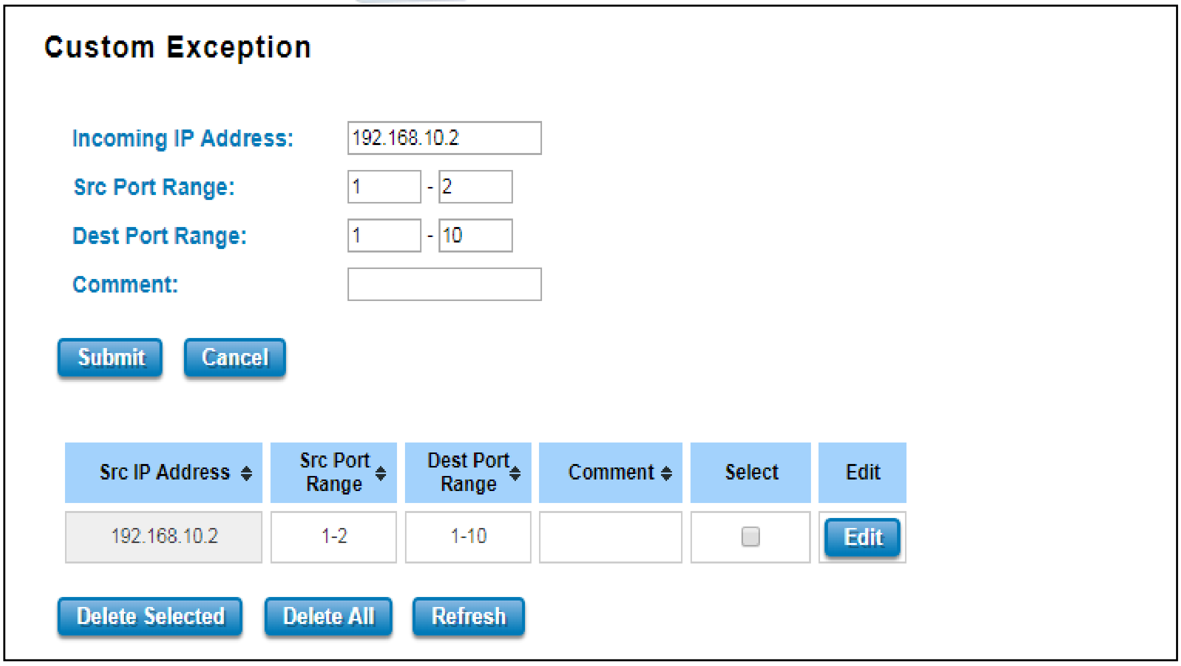
The description of the columns is as below:

Terms	Description
Filter All	By select Filter All, it will block all external access from WAN interface tothe 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	Edit
192.168.10.2	1-2	1-10		□	Edit

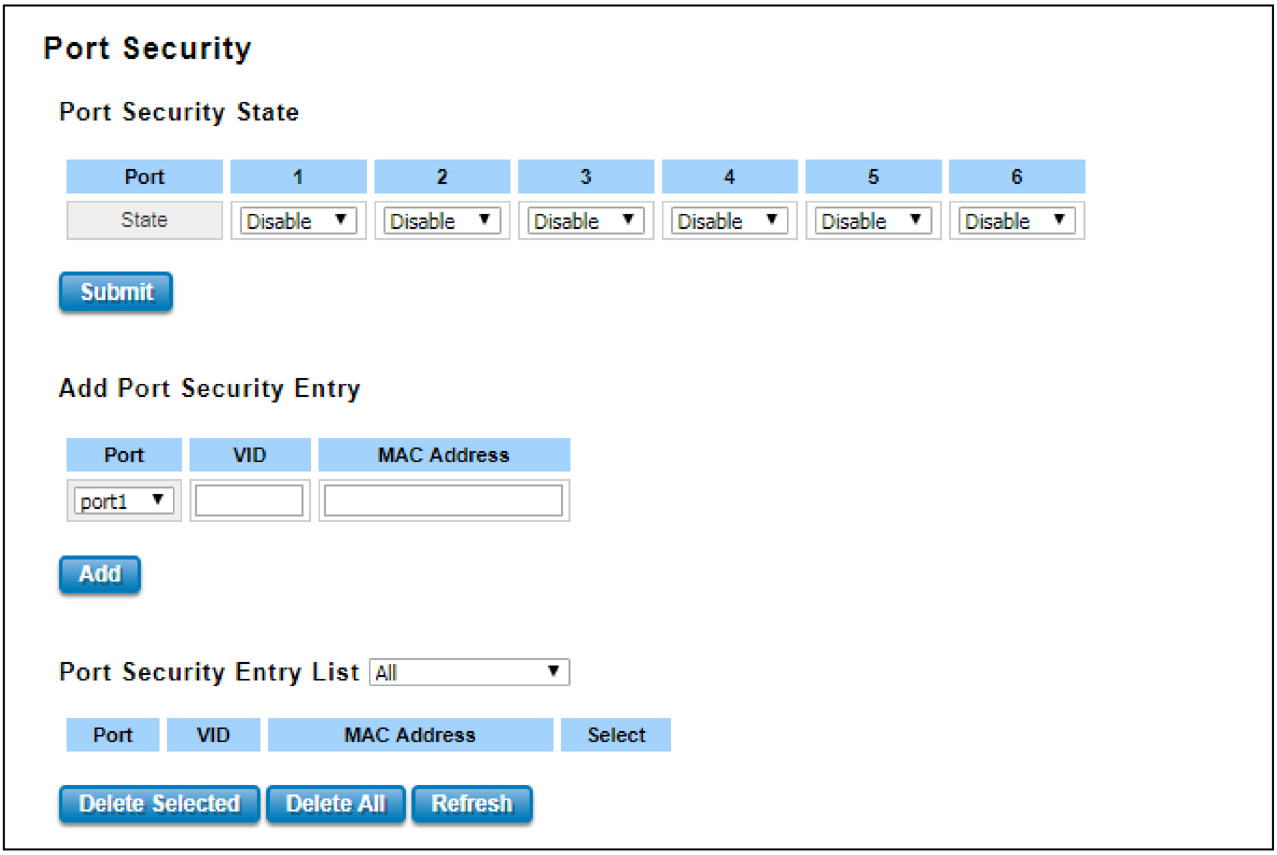
The description of the columns is as below:

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

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

3.9.2 Port Security

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



Port Security

Port Security State

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

Add Port Security Entry

Port	VID	MAC Address
port1		

Port Security Entry List All

Port	VID	MAC Address	Select

The description of the columns is as below:

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

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

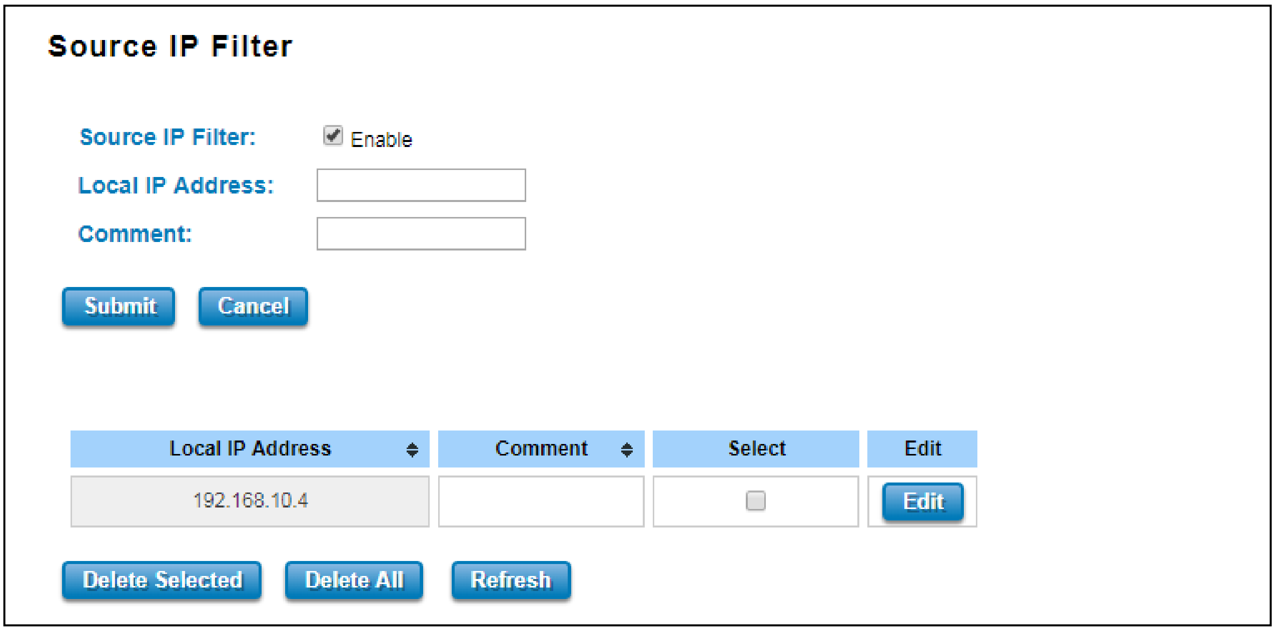
3.9.3 Outbound Firewall

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

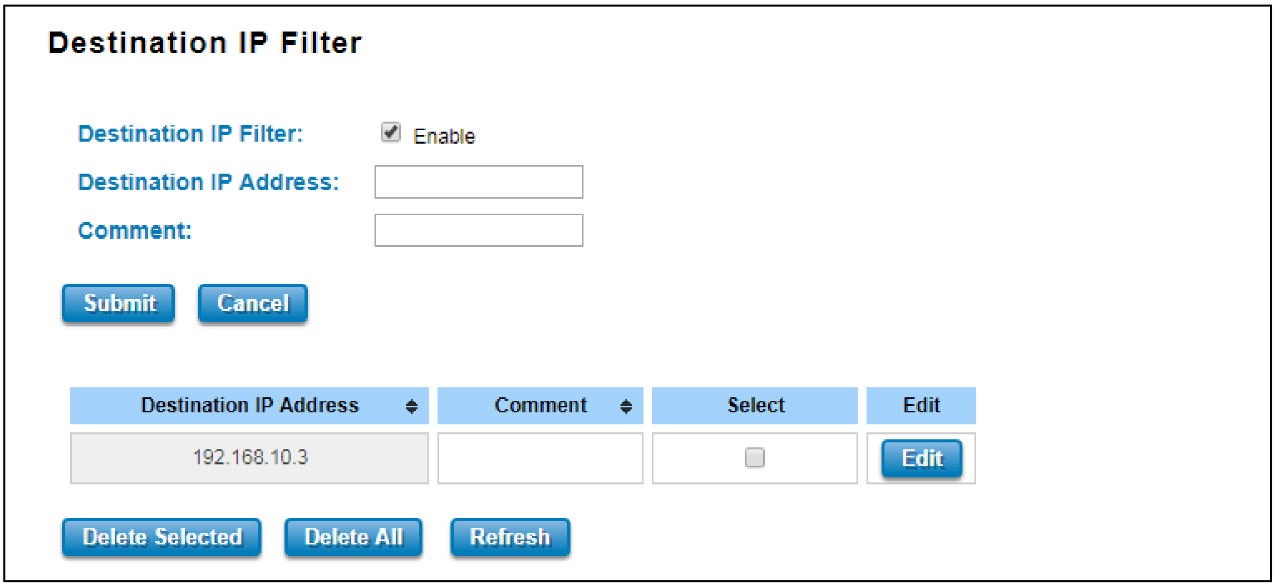
The description of the columns is as below:

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 the list.
Edit	Click edit to modify the parameters

Click **Refresh** to refresh the table

➢ Dest IP Filter

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



Destination IP Filter

Destination IP Filter: ☑ Enable

Destination IP Address:

Comment:

Destination IP Address	Comment	Select	Edit
192.168.10.3		□	Edit

The description of the columns is as below:

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

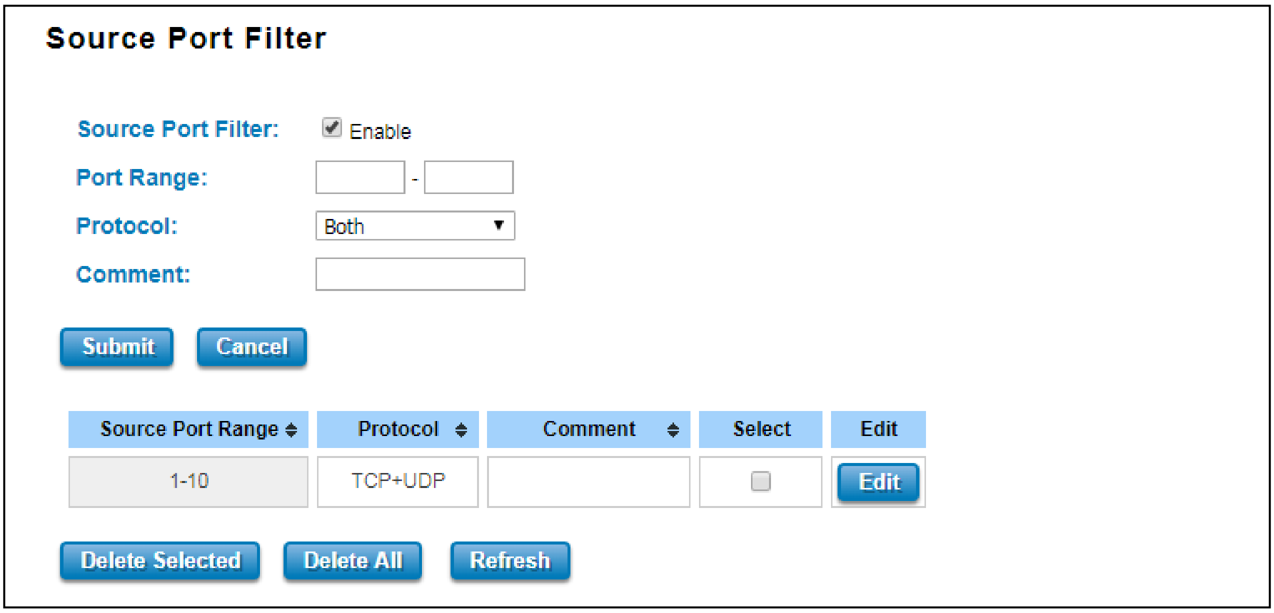
Click **Refresh** to refresh the table

➢ Src Port Filter

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

Select Enable Source Port filtering, type the Port Range of below Protocol type, the protocol type can be UDP, TCPor 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 the list.
Edit	Click edit to modify the parameters

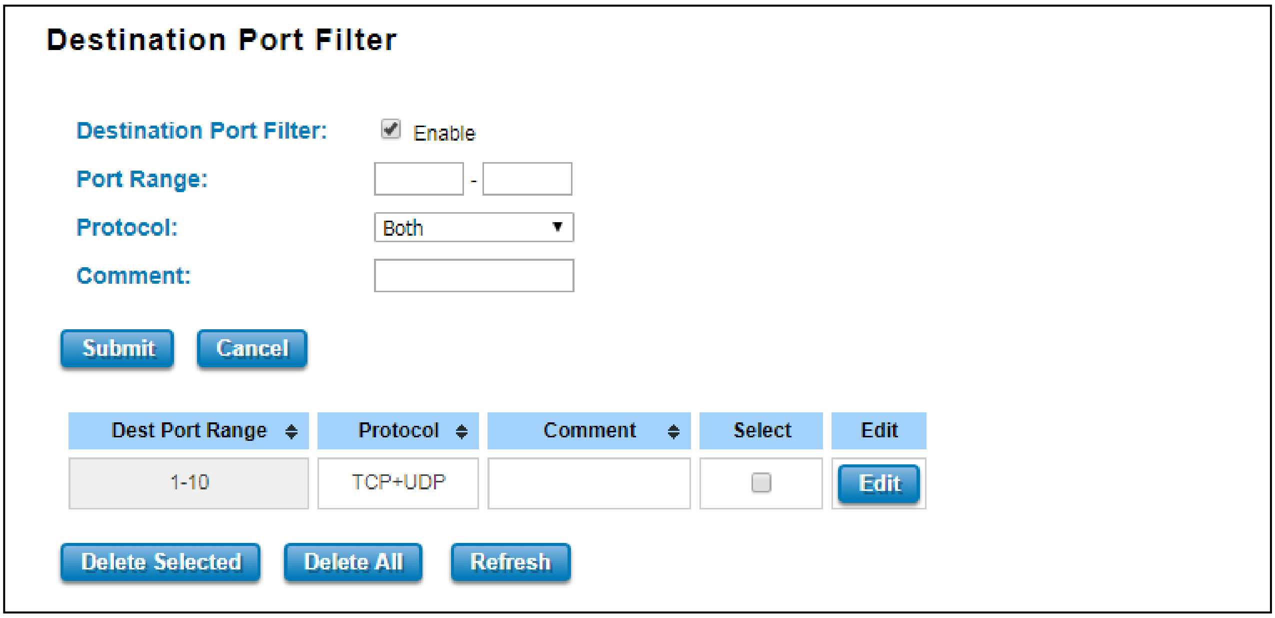
Click **Refresh** to refresh the table

- Dest Port Filter

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

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

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



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:

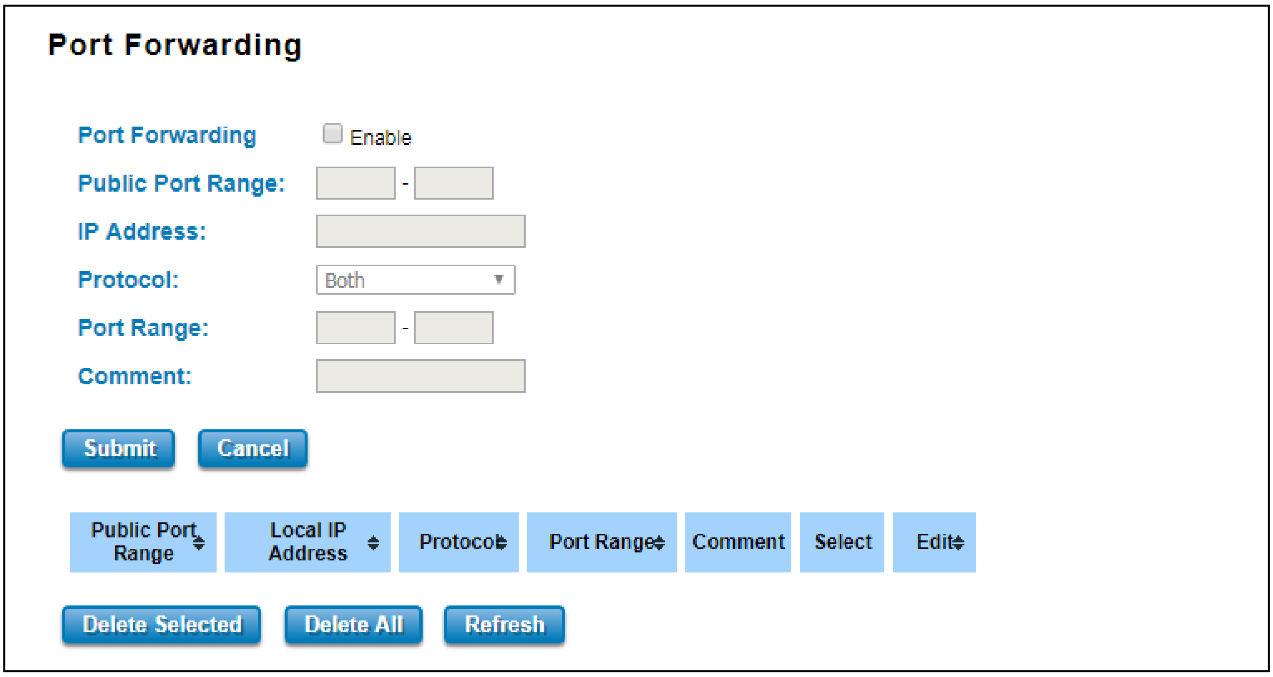
Terms	Description
Dest Port Range	Display the Destination Port Range (Range is from 1 to 65535)
Protocol	Display the protocol that has been chosen by the user.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete the list.
Edit	Click edit to modify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

Click **Refresh** to refresh the table

3.9.4 NAT Setting

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

➢ Port Forwarding



Port Forwarding

Port Forwarding □ Enable

Public Port Range: -

IP Address:

Protocol: Both

Port Range: -

Comment:

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.

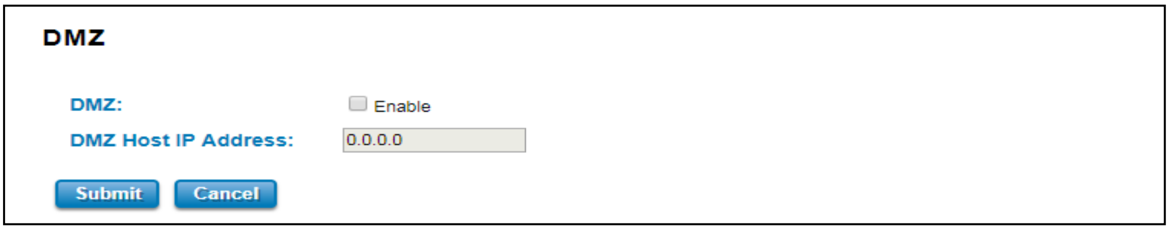
The description of the columns is as below:

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

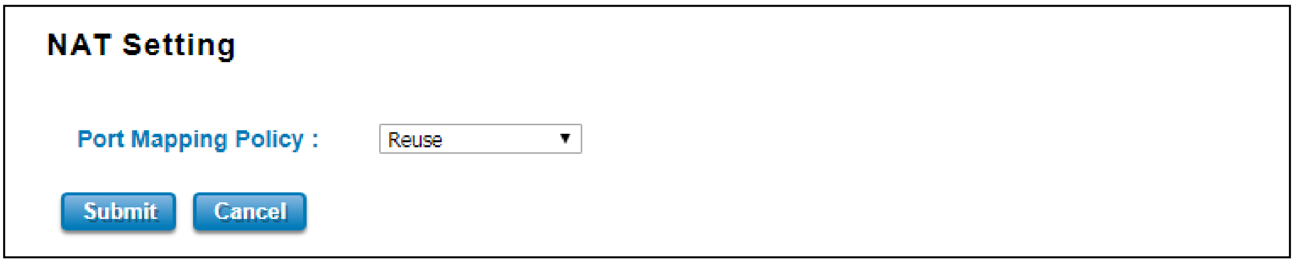
Click **Enable** to activate the function and assign the IP address of **DMZ Host IP Address**. This is the DMZ computer's IP address. Click Submit to activate the function.

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.

➢ NAT Setting

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



NAT Setting

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 sameremote device. Randomize: Change the port number every time access the remote device.

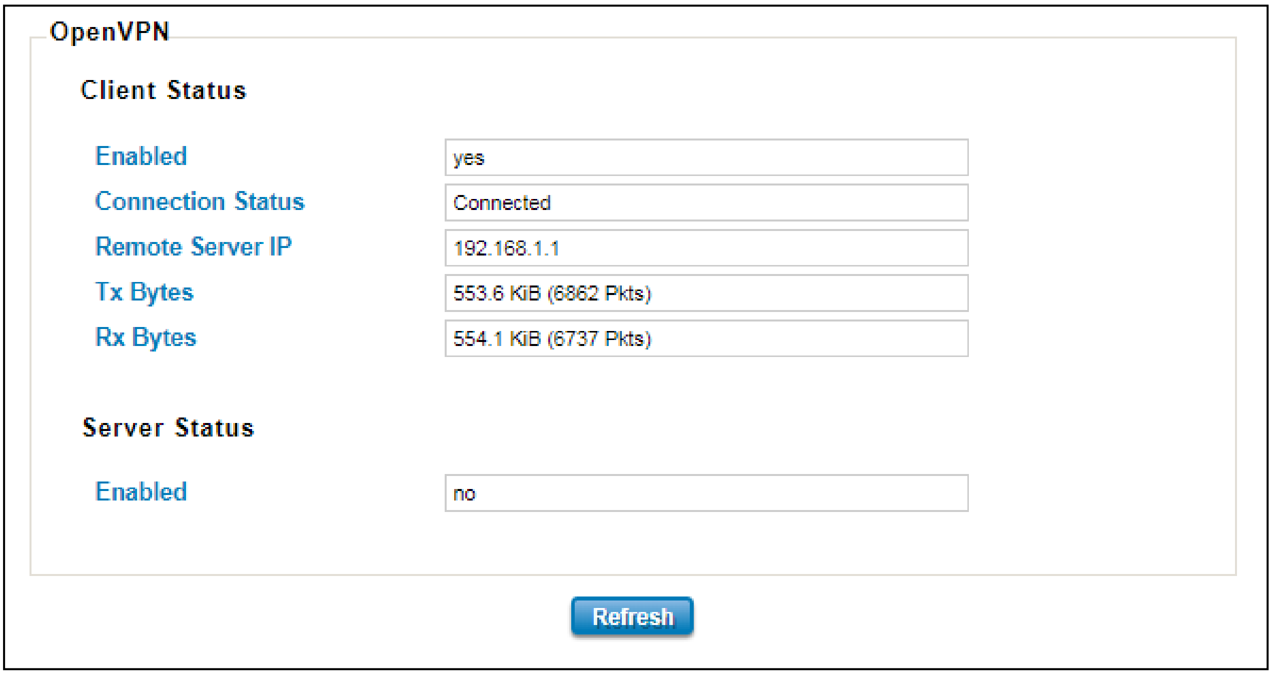
Click **Submit** to apply the configuration.

3.9.5 OpenVPN

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

Client Status

Enabled	yes
Connection Status	Connected
Remote Server IP	192.168.1.1
Tx Bytes	553.6 KiB (6862 Pkts)
Rx Bytes	554.1 KiB (6737 Pkts)

Server Status

Enabled	no

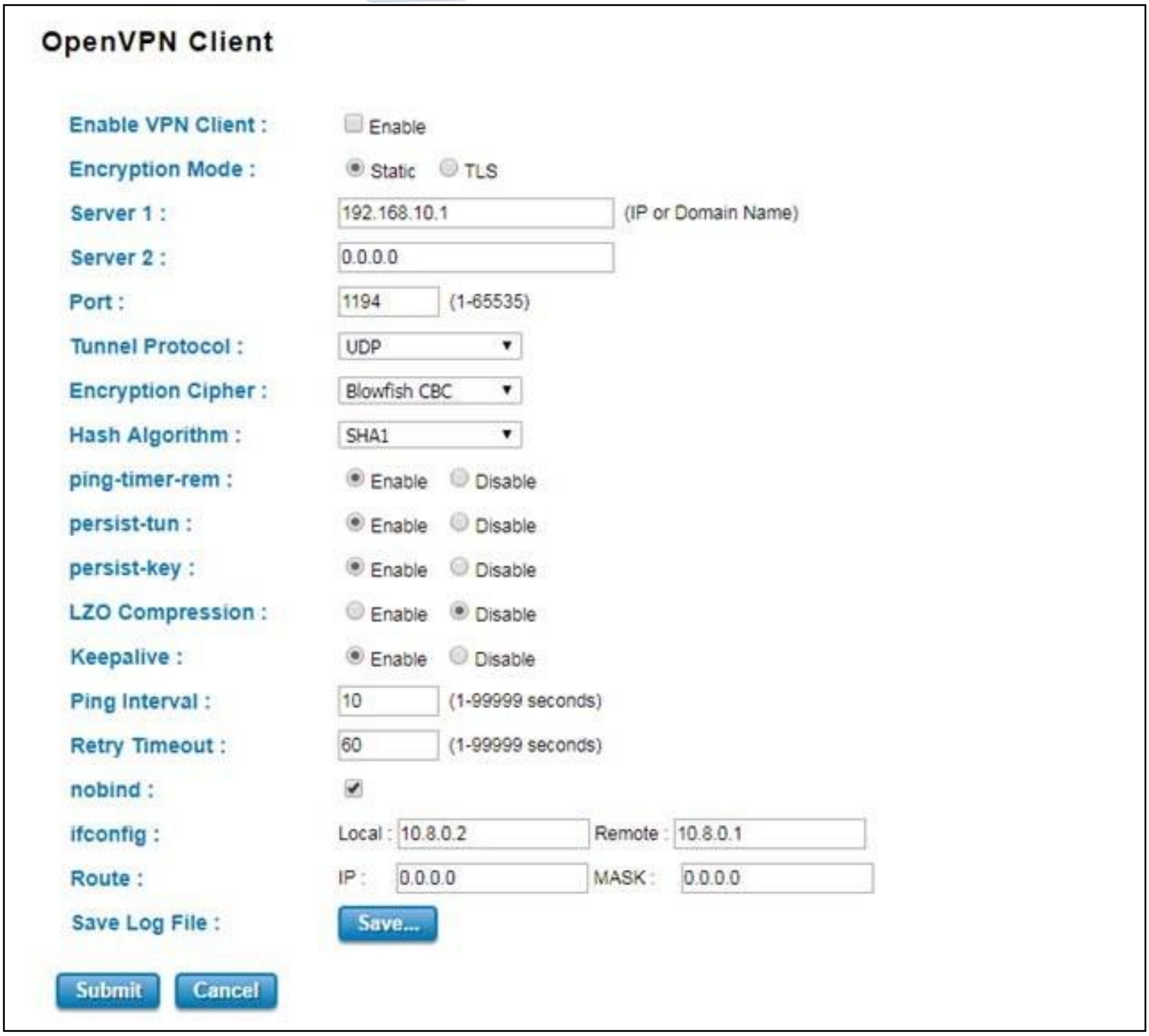
The description of the columns is as below:

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 :	Save...

The description of the columns is as below:

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

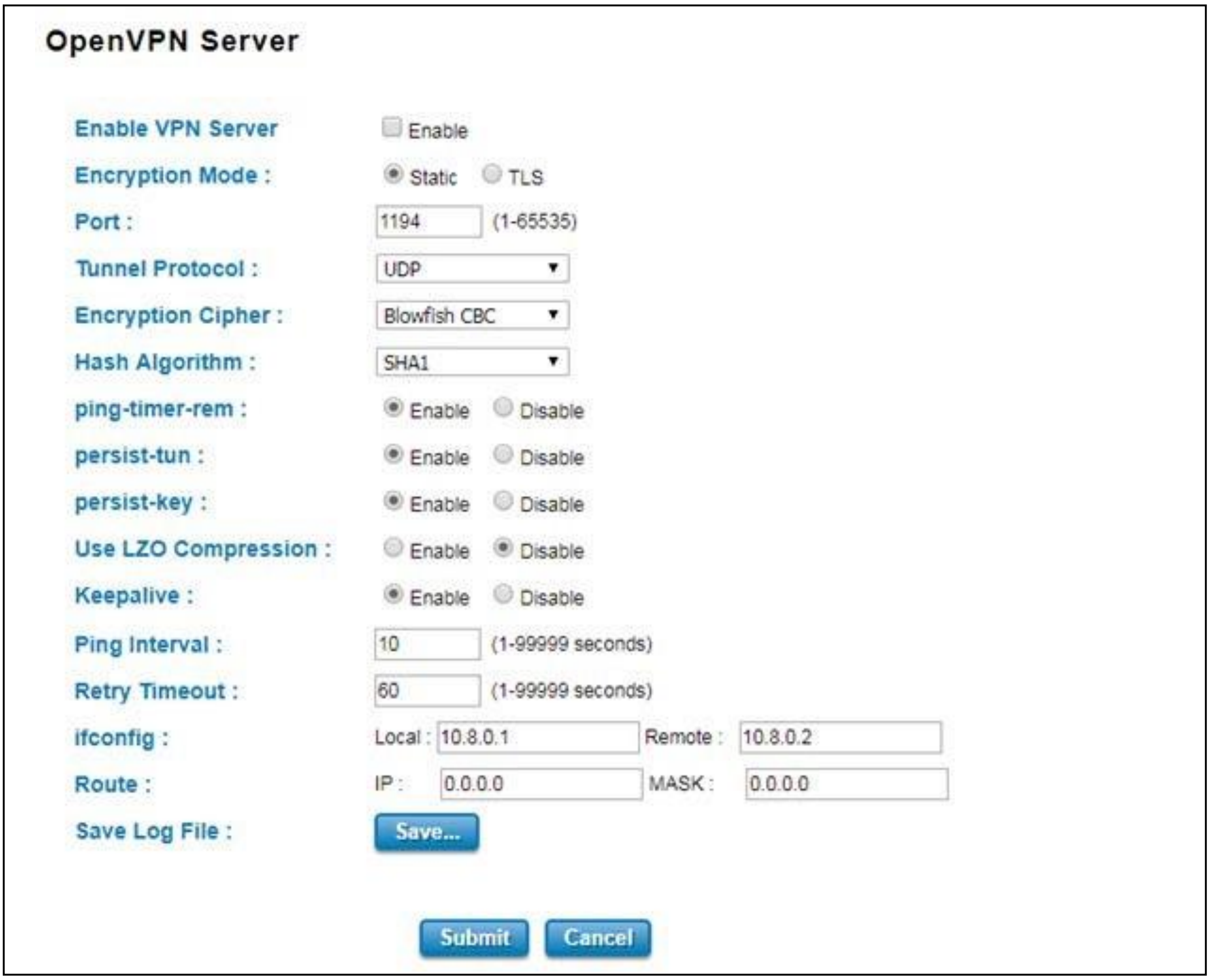
Hash Algorithm	Hash algorithm provides a method of quick access to data, including SHA1， SHA256，SHA512，MD5
Login (TLS)	**Default: Disable** Select enable to activate the login function, input the username and password.
ping-timer-rem	**Default: Enable** Select enable or disable the ping-timer-rem, to prevent unnecessary restart atserver/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 keyfirst use if the VPN restarts after Keepalive timeout.
LZO Compression	**Default: Disable** Select use LZO Compression or not, this function compresses data to decreasethe traffic but also need more CPU effort.
Keepalive	**Default: Enable** Select enable or disable Keepalive function, this function is use to detect thestatus 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.
Renegotiation Interval (TLS)	**Default: 3600** Input the renegotiation interval, the range can from 0~36000000 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 : Save...

The description of the columns is as below:

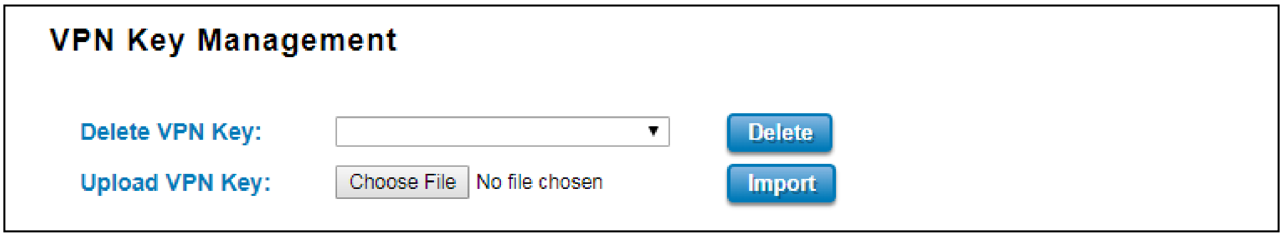
Terms	Description
Enable VPN Server	Select Enable to activate the VPN Server function
Encryption Mode	Choose the Encryption Mode Static Key: Use a pre-shared static key. TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server 1	Type the IP Address of the VPN Server
Server 2	Type the 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 portsetting. 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 unnecessaryrestart 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 useif VPN restart after Keepalive timeout.
LZO Compression	**Default: Disable** Select use LZO Compression or not, this function compresses data to decrease thetraffic, 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.
Server (TLS)	Input the server 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.
Push Route (TLS)	Input the push route IP and MASK. This brings client to send the same packets to VPN interface.
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.

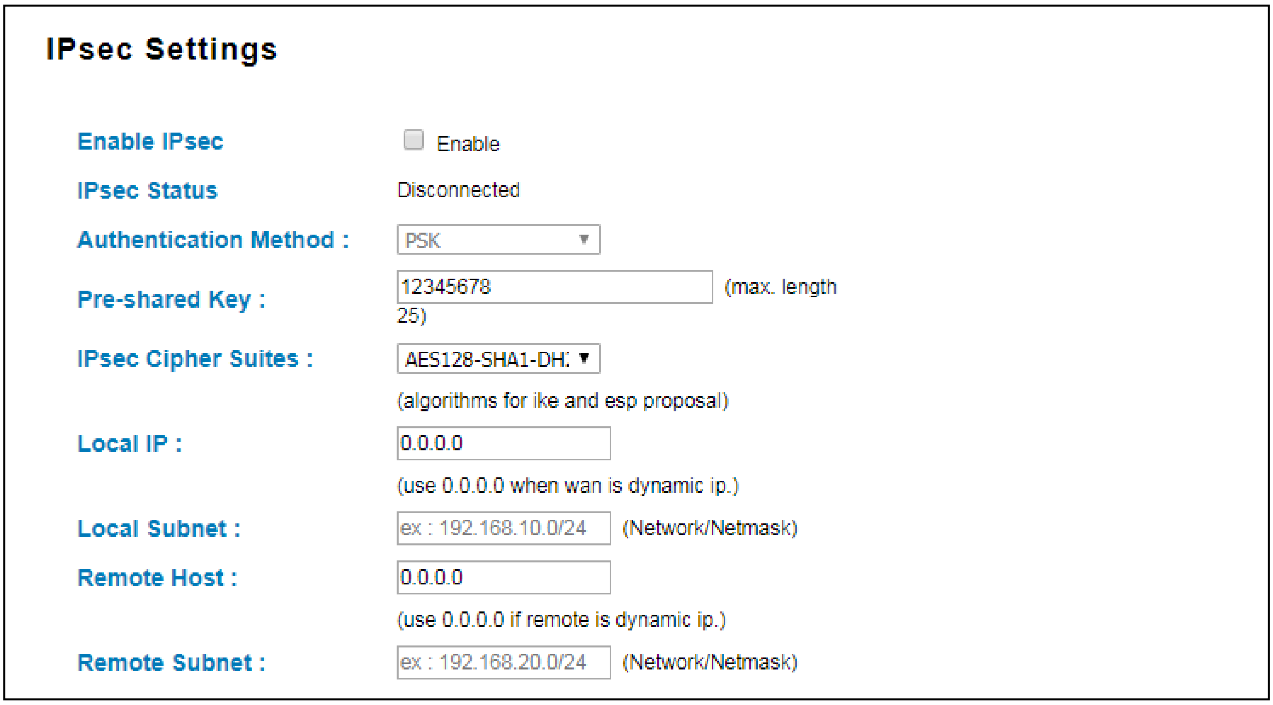


The description of the columns is as below:

Terms	Description
Delete VPN Key	Delete the selected certificate
Upload VPN Key	Upload a certificate file from a specified file location Please select correct vpn key file! Example: ca.crt, server.key, server.crt, dh1024.pem, client.key, client.crt, static.key

3.9.6 IPSEC SETTING

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



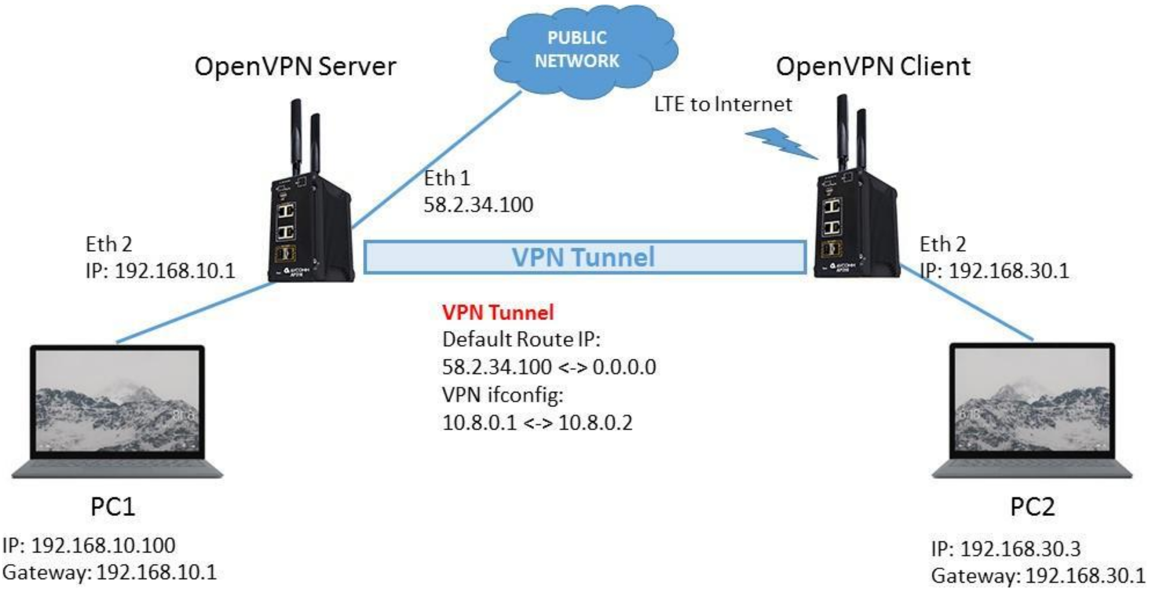
IPsec Settings

Enable IPsec	□ Enable
IPsec Status	Disconnected
Authentication Method :	PSK ▼
Pre-shared Key :	12345678 (max. length 25)
IPsec Cipher Suites :	AES128-SHA1-DH: ▼ (algorithms for ike and esp proposal)
Local IP :	0.0.0.0 (use 0.0.0.0 when wan is dynamic ip.)
Local Subnet :	ex : 192.168.10.0/24 (Network/Netmask)
Remote Host :	0.0.0.0 (use 0.0.0.0 if remote is dynamic ip.)
Remote Subnet :	ex : 192.168.20.0/24 (Network/Netmask)

The description of the columns is as below:

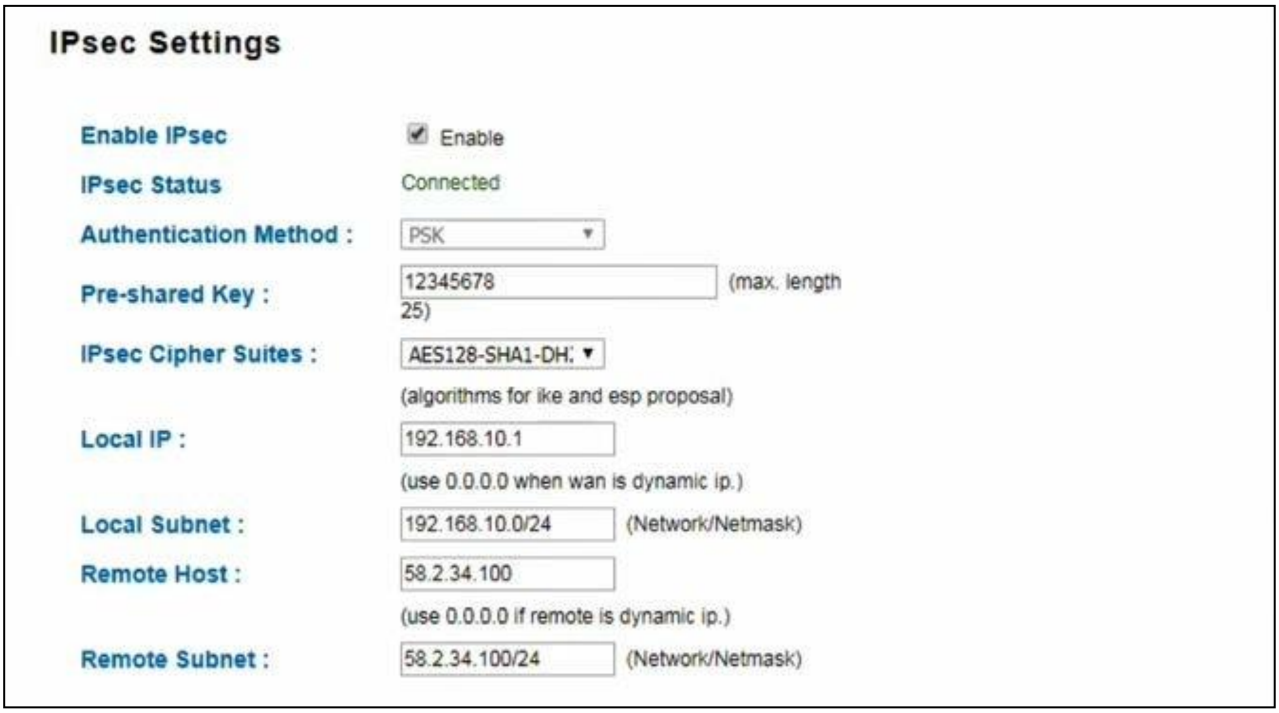
Terms	Description
Enable IPsec	Select Enable to activate the IPsec function
IPsec Status	Display the IPsec status, whether it is connected or disconnected
Authentication Method	Default: PSK Optional: Pre Shared Key or Certificate
Pre-shared key	**Default: 12345678** Set the preshared key
IPsec Cipher Suites	**Default: AES128-SHA1-DH2** Set algorithms for IKE and ESP proposal, choose AES128-SHA1-DH2, DES-SHA1-DH2,and 3DES-SHA1-DH2
Local IP	IP Address of the local side of the tunnel. (Use 0.0.0.0 when WAN is dynamic IP.)
Local Subnet	Set IPSec local protected subnet and subnet mask, i.e. 192.168.1.0/24
Remote Host	**Default: 0.0.0.0** Set IPsec Remote Host, use the default setting if remote is dynamic IP
Remote Subnet	Set IPsec Remote Protected Subnet/Subnet Netmask

Click **Submit** to apply the configuration.



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

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



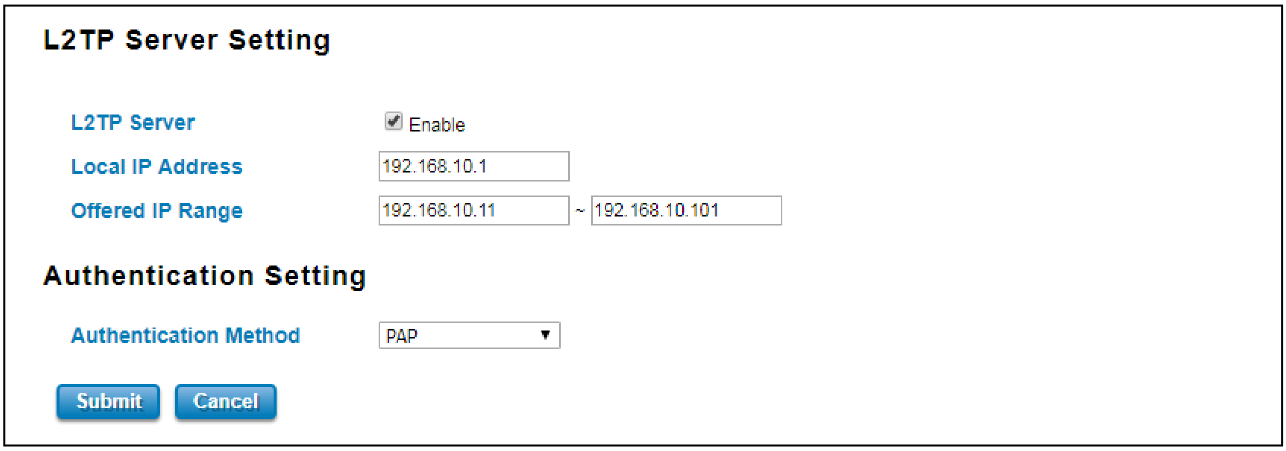
IPsec Settings

Enable IPsec	☑ Enable
IPsec Status	Connected
Authentication Method :	PSK ▾
Pre-shared Key :	12345678 (max. length 25)
IPsec Cipher Suites :	AES128-SHA1-DH; ▾ (algorithms for ike and esp proposal)
Local IP :	192.168.10.1 (use 0.0.0.0 when wan is dynamic ip.)
Local Subnet :	192.168.10.0/24 (Network/Netmask)
Remote Host :	58.2.34.100 (use 0.0.0.0 if remote is dynamic ip.)
Remote Subnet :	58.2.34.100/24 (Network/Netmask)

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

3.9.7 L2TP SETTING

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



L2TP Server Setting

L2TP Server ☑ Enable

Local IP Address 192.168.10.1

Offered IP Range 192.168.10.11 ~ 192.168.10.101

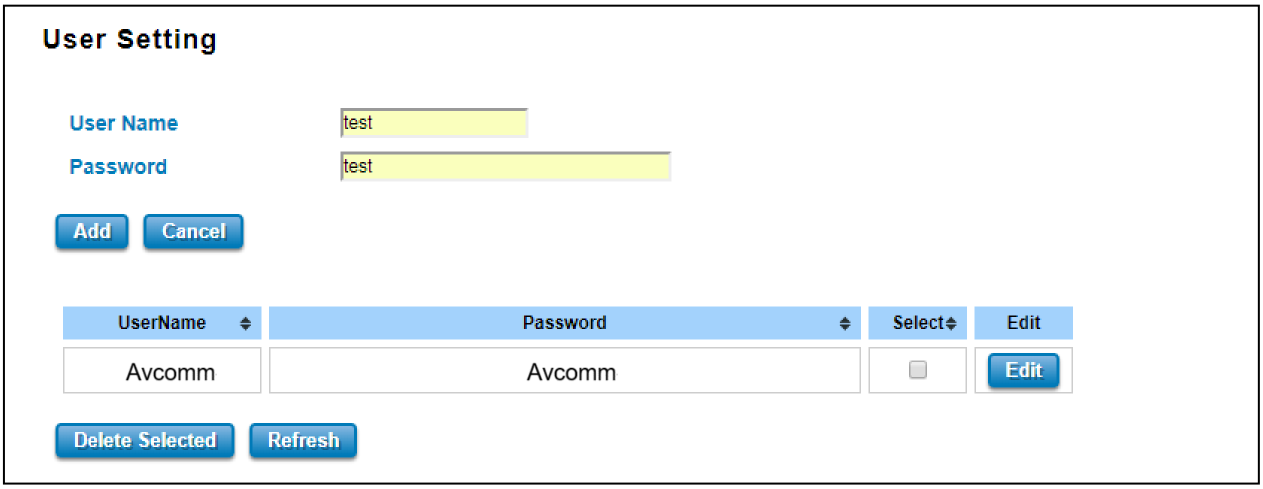
Authentication Setting

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 usingthe password authentication protocol (PAP) and challenge handshake authentication protocol (CHAP).

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



User Setting

User Name test

Password test

UserName	Password	Select	Edit
Avcomm	Avcomm	□	Edit

Below is the User Setting for the L2TP Authentication connection.

The description of the column is as below:

Terms	Description
Username	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.

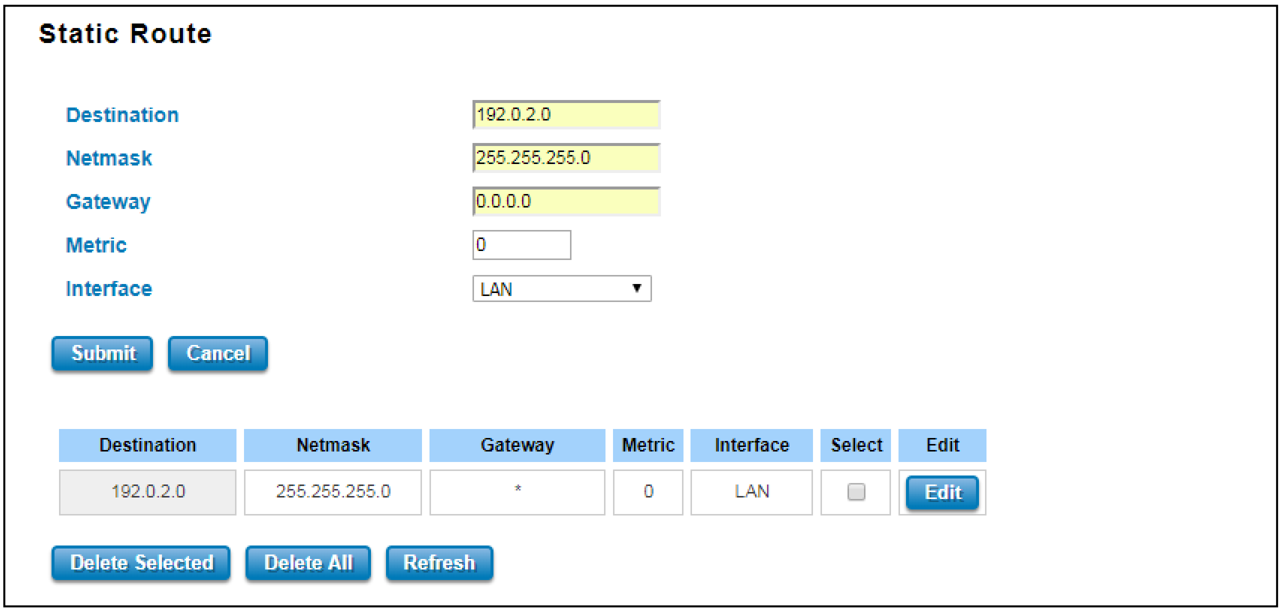
3.10 ROUTING

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.

3.10.1 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	0.0.0.0
Metric	0
Interface	LAN

Destination	Netmask	Gateway	Metric	Interface	Select	Edit
192.0.2.0	255.255.255.0	*	0	LAN	□	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 interfaces. LAN 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.

3.10.2 RIPv2

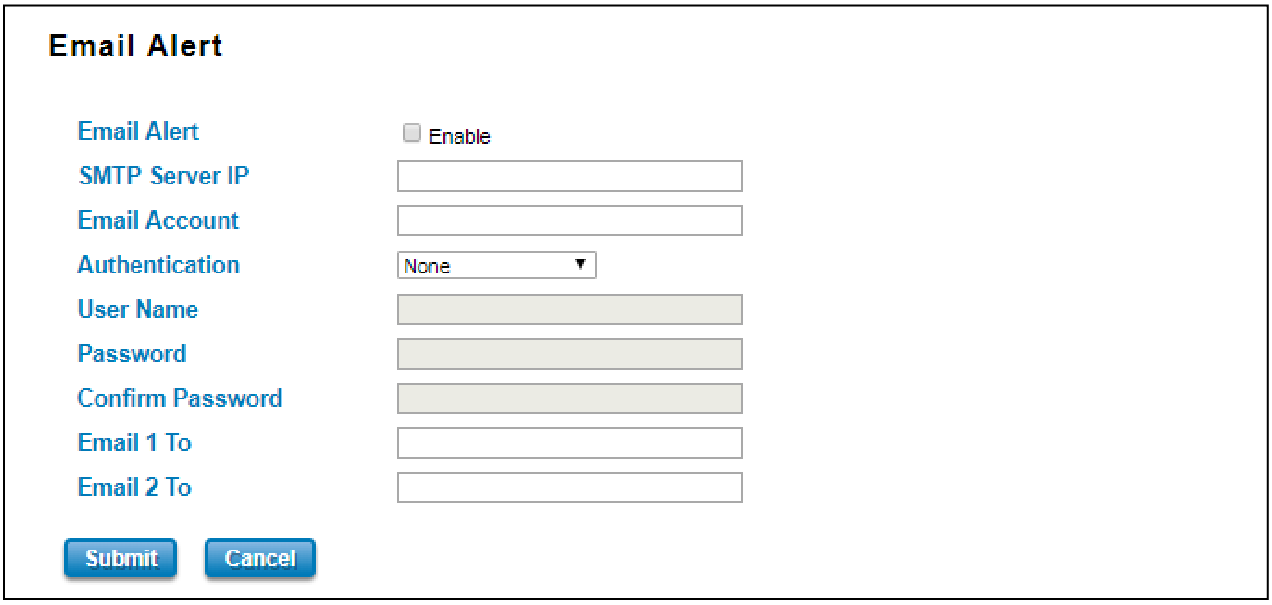
Avcomm Industrial Router is supported with RIPv2. The Routing Information Protocol (RIP) is a distance-vector, interior gateway (IGP) routing protocol used by routers to exchange routing information. RIP uses the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the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

3.11 WARNING

The switch provides several types of Warning feature for remote monitoring of end devices status or network changes.

3.11.1 Email Alert

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

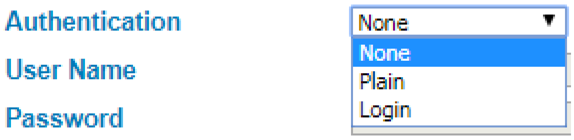


Email Alert

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

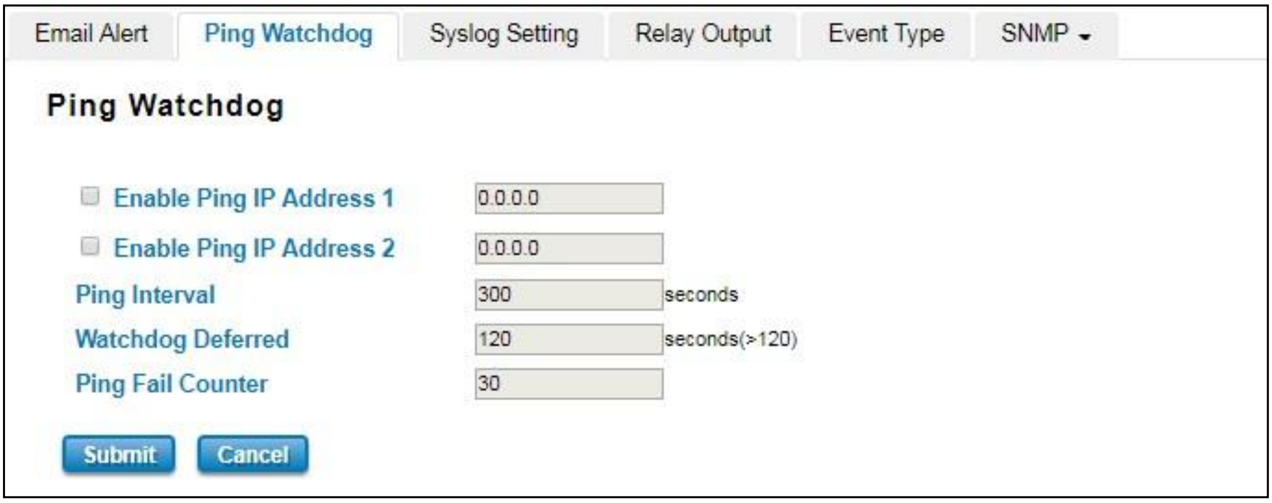
The description of the columns is as below:

Terms	Description
Email Alert	Check the box to enable the function
SMTP Server IP	Enter the IP address of the email Server

Email Account	Click on check box to enable the password
Authentication	 Authentication None ▼ User Name Password None Plain Login Choose the Authentication mode (None, Plain, Login)
Username	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 switch	
Email 1 To	The first email address to receive an email alert from the switch (Max. 40 characters)
Email 2 To	The second email address to receive an email alert from the switch (Max. 40 characters)

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

3.11.2 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 provide two target IP Addresses, in order if the other one cannot be reached there is another backup IP address. There are two conditions in this Ping Watchdog section, the first one is when the device continuously pings 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 the user configuration.

The description of the columns is as below:

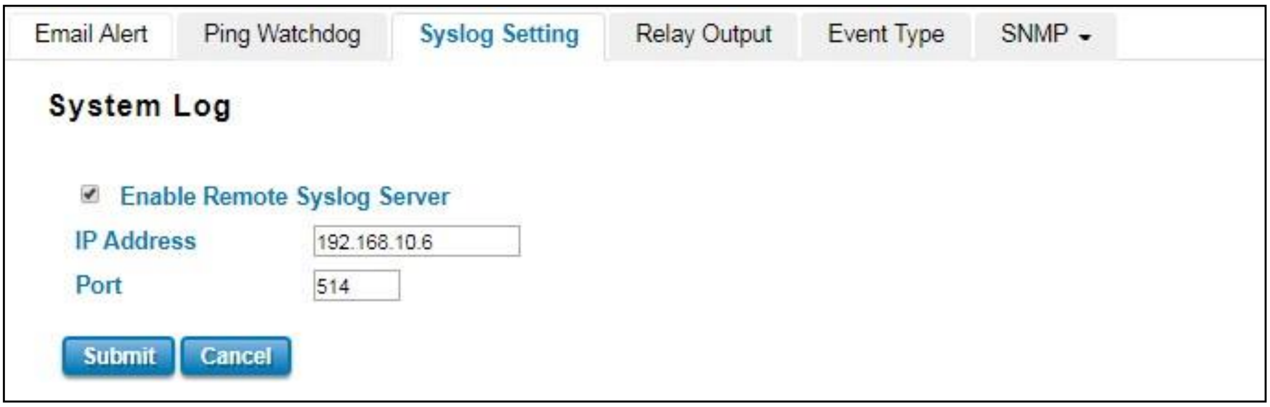
Terms	Description
Enable Ping IP Address 1	Clicks enable to activate the feature. Set the first IP Address to check if the device is alive or not
Enable Ping IP Address 2	Clicks enable to activate the feature. Set the second IP Address to check if

	the device is alive or not
Ping Interval	**Default: 300 (seconds)** Set the interval timer to Ping the remote device. Every 300 seconds thedevice 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 thedevice 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.

3.11.3 Syslog Setting

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



System Log

☑ Enable Remote Syslog Server

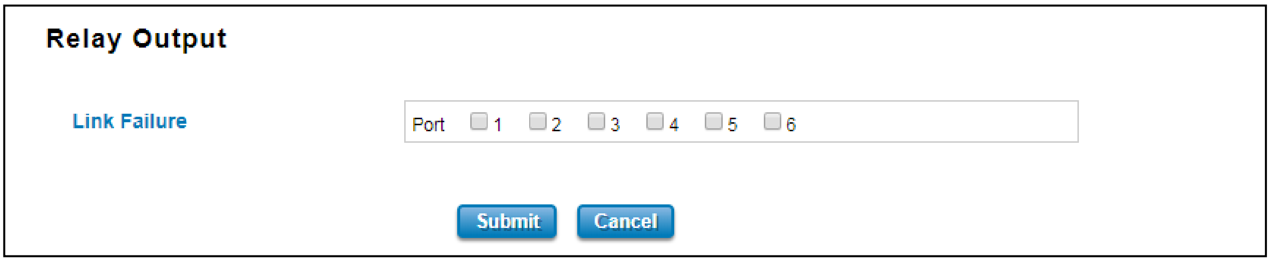
IP Address: 192.168.10.6

Port: 514

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

3.11.4 Relay Output

Avcomm switch provides 1 alarm relay output, also known as Digital Output. These settings in Relay Output section control the events that will trigger the alarm output. The discrete output is on during normal conditions and turned off in the event of an alarm condition. The Relay Output configuration interface has shown as below:



Relay Output

Link Failure: Port □1 □2 □3 □4 □5 □6

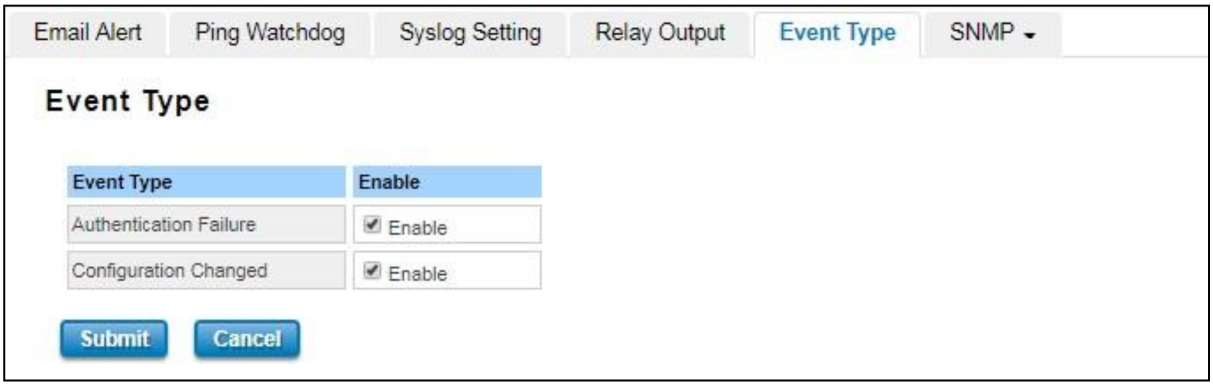
The condition or term described as the following table.

Terms	Condition	Description
Link Failure	Port number	Monitoring port link down event

The relay supports multiple event trigger function; click and select type of event and setting the detail information, and then clicks Submit to activate the relay alarm function.

3.11.5 Even Type

On this page, user can specify how the switch reacts to system events. To enable or disable the options, click the relevant check boxes of the columns. There are two basic Event Types which are Authentication Failure that related when the authentication process between your local computer and the remote device has failed and Configuration Changed that related to the any changing in configuration.



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.

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

3.11.6 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

3.11.6.1 SNMP SETTING

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

- SNMPv2C

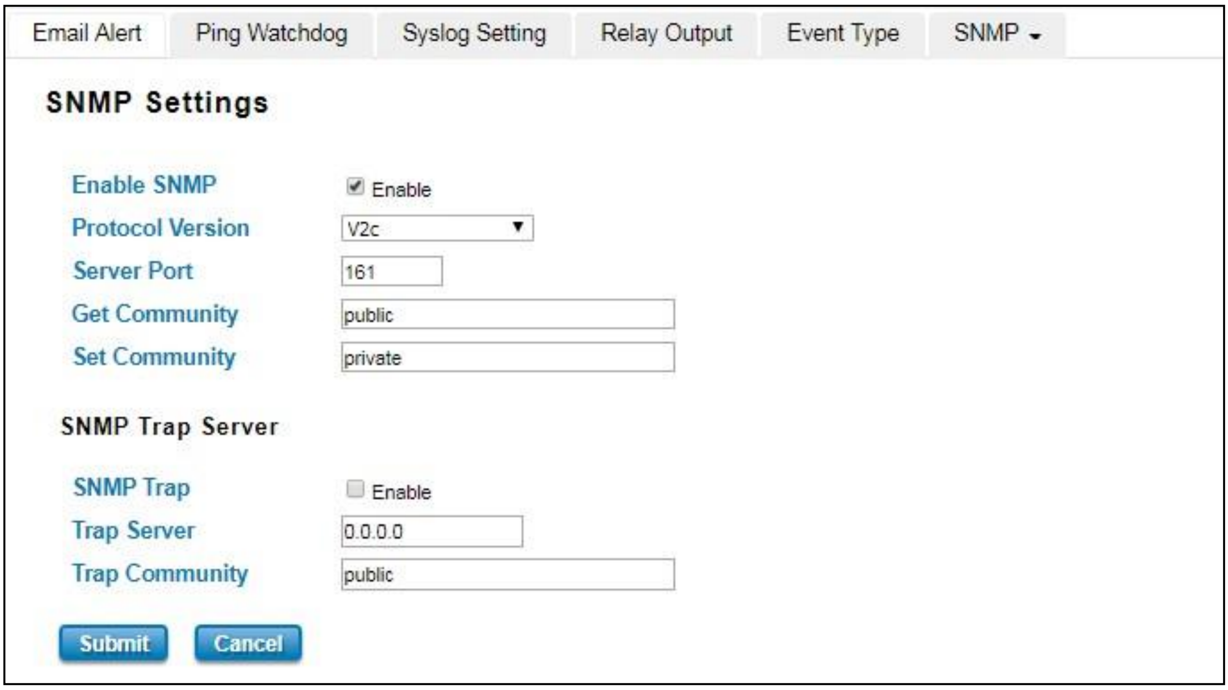
> NOTE: When User first installs the device in User network, we highly recommend user to change the community string. Since most SNMP management application uses Public and Private as their default community name, this might be the leakage of the network security.

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.



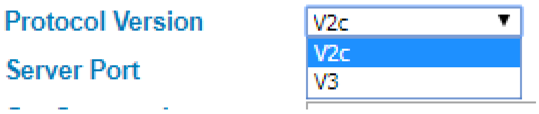
SNMP Settings

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

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 markingon 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 SNMPdata.
Set Community	**Default: private** Create the name for a group or community of administrators who can write or editSNMP data.

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

- SNMP Trap Server

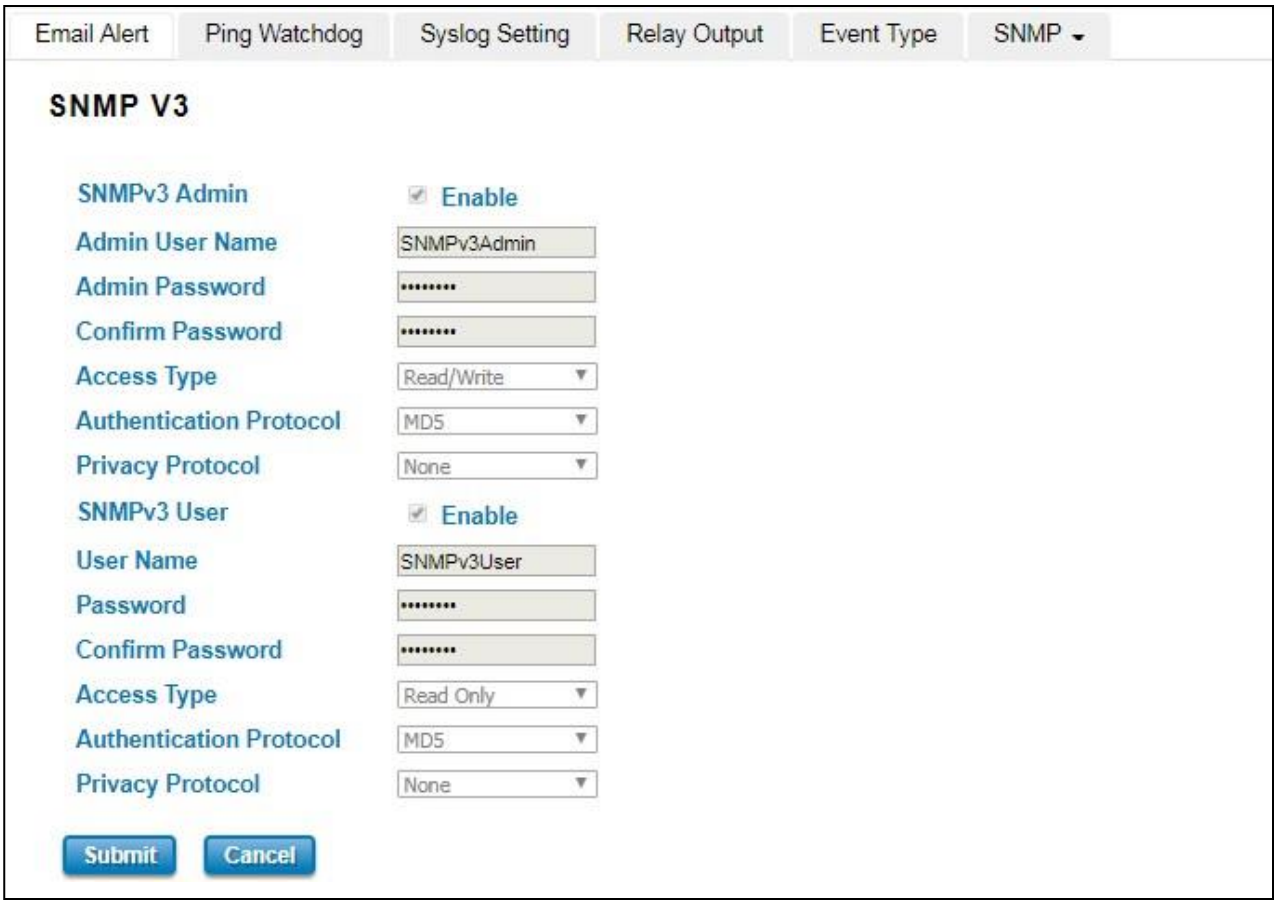
SNMP trap is the most frequently used SNMP messages. These messages are sent to the manager by an agent when an issue needs to be reported. SNMP traps are quite unique if compared to other message types, since they are the only method that can be directly initiated by an SNMP agent. The other types of messages are either initiated by theSNMP 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 toreport the events. If the the group is match then the events can be reported.

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

3.11.6.2 SNMP V3

SNMP v3 can provide more security functions when the user performs remote management through SNMP protocol. This field displays the SNMPv3 configuration page for Admin and User. If the value from Access Type is set to Read- Write, the SNMPv3 user will be able to set and retrieve parameters on the system. And if the value is set to Read Only, the SNMPv3 user will only be able to retrieve parameter information. It delivers SNMP information to the administrator with user authentication; all of data between the router and the administrator are encrypted to ensure secure communication. SNMPv3 requires an authentication level of MD5 or DES to encrypt data to enhance data security. To activate the page make sure user has already choose 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 areavailable. **None**: No encryption is applied. **DES**: Data Encryption Standard, it applies a 58-bit key to each 64-bit blockof 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 areavailable. **None**: No encryption is applied. **DES**: Data Encryption Standard, it applies a 58-bit key to each 64-bit blockof data.

3.12 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:

3.1.10Event Logs

3.1.11ARP Table

3.1.12Port Statistic

3.1.13Network Statistic

3.1.14Port Mirror

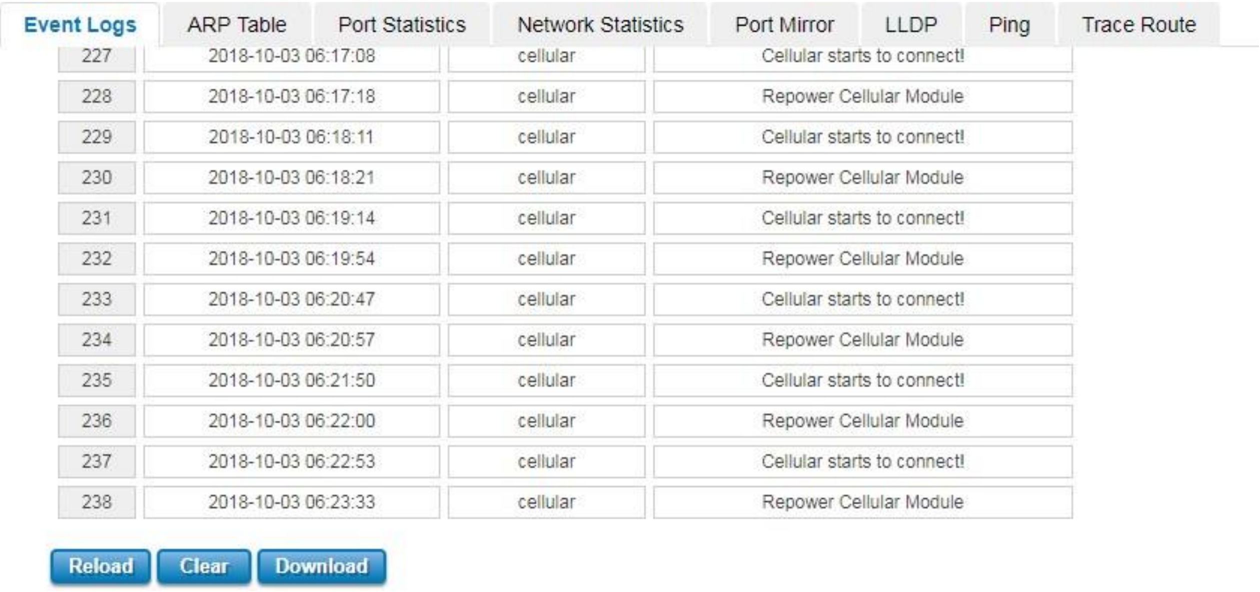
3.1.15LLDP

3.1.16Ping

3.1.17Traceroute

3.12.1 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.



227	2018-10-03 06:17:08	cellular	Cellular starts to connect!
228	2018-10-03 06:17:18	cellular	Repower Cellular Module
229	2018-10-03 06:18:11	cellular	Cellular starts to connect!
230	2018-10-03 06:18:21	cellular	Repower Cellular Module
231	2018-10-03 06:19:14	cellular	Cellular starts to connect!
232	2018-10-03 06:19:54	cellular	Repower Cellular Module
233	2018-10-03 06:20:47	cellular	Cellular starts to connect!
234	2018-10-03 06:20:57	cellular	Repower Cellular Module
235	2018-10-03 06:21:50	cellular	Cellular starts to connect!
236	2018-10-03 06:22:00	cellular	Repower Cellular Module
237	2018-10-03 06:22:53	cellular	Cellular starts to connect!
238	2018-10-03 06:23:33	cellular	Repower Cellular Module

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

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

3.12.2 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

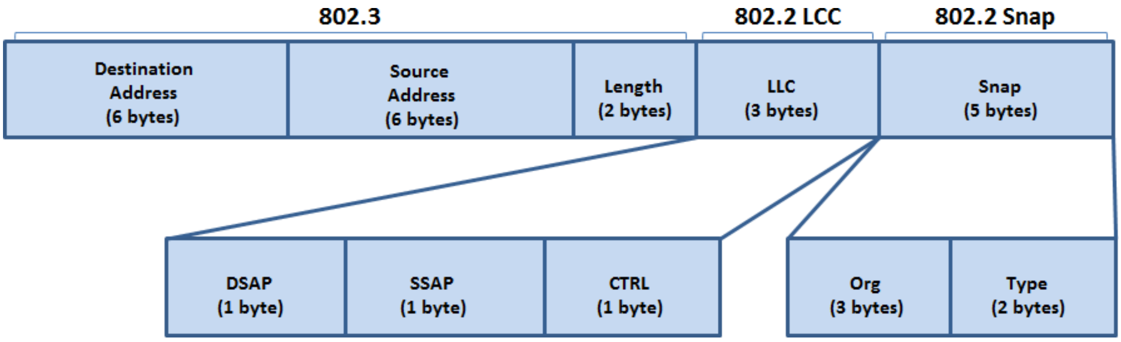
802.2 LLC Type 2 is the new level of ARP where the device will response the request of 802.2 snap ARP on the Ethernet port and not support sending the request of 802.2 snap ARP. Below is the Data format.

Data Format

Protocol Header:

802.3 + 802.2 LLC + 802.2 snap

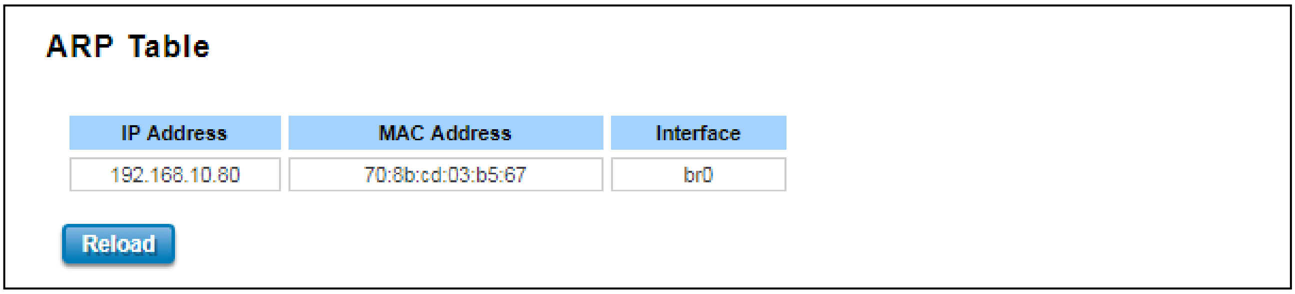
|- (DS + SA + Len) -|- DSAP + SSAP + CTRL -|- Org + type -|



Note:

LLC: Logic Link Control; DSAP - Destination Service Access Point; 1 byte, SSAP - Source Service Access Point; 1 byteSNAP: Sub-Network Access Protocol; OUI - Organization Unique ID; 3 bytes, EtherType – 2 bytes

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.



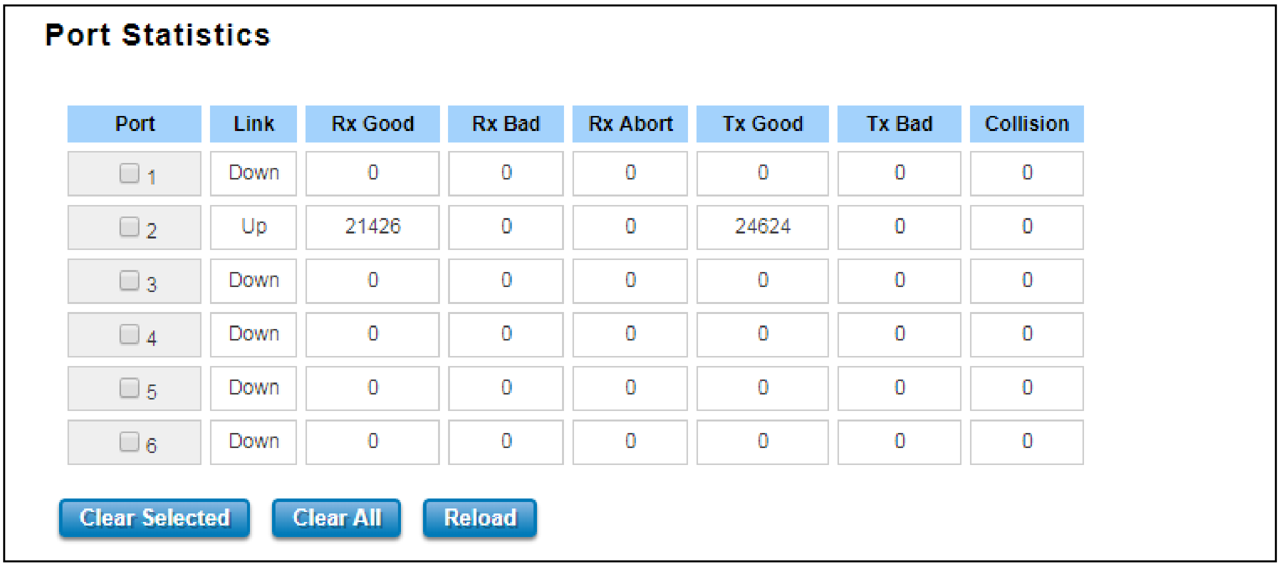
ARP Table

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

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

3.12.3 Port Statistic

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



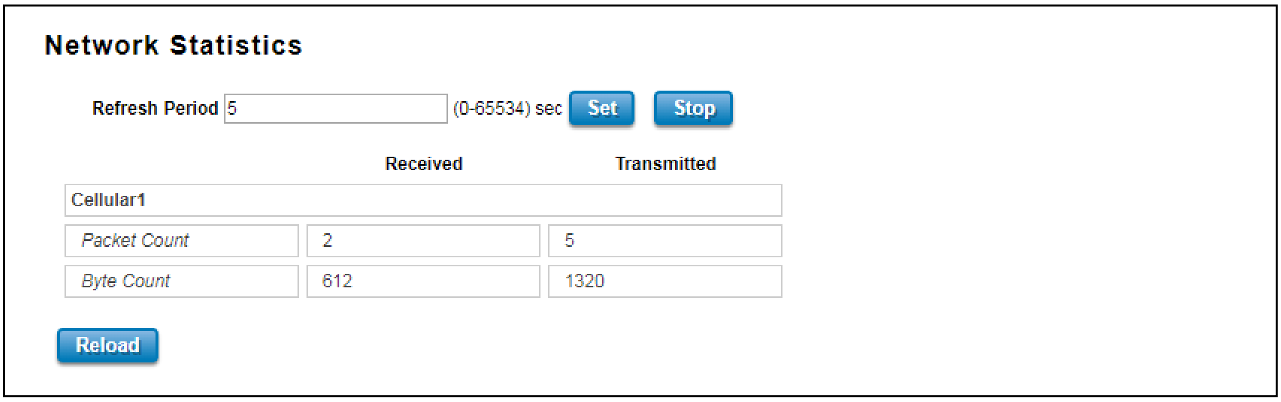
Port Statistics

Port	Link	Rx Good	Rx Bad	Rx Abort	Tx Good	Tx Bad	Collision
☐ 1	Down	0	0	0	0	0	0
☐ 2	Up	21426	0	0	24624	0	0
☐ 3	Down	0	0	0	0	0	0
☐ 4	Down	0	0	0	0	0	0
☐ 5	Down	0	0	0	0	0	0
☐ 6	Down	0	0	0	0	0	0

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

3.12.4 Network Statistics

This section shows about the packet data that transmitted or received on the router or the switch. For



Network Statistics

Refresh Period 5 (0-65534) sec

	Received	Transmitted
Cellular1		
Packet Count	2	5
Byte Count	612	1320

the AP316 it will include the Cellular activity. The Cellular packets include 2G/3G/LTE transmission.

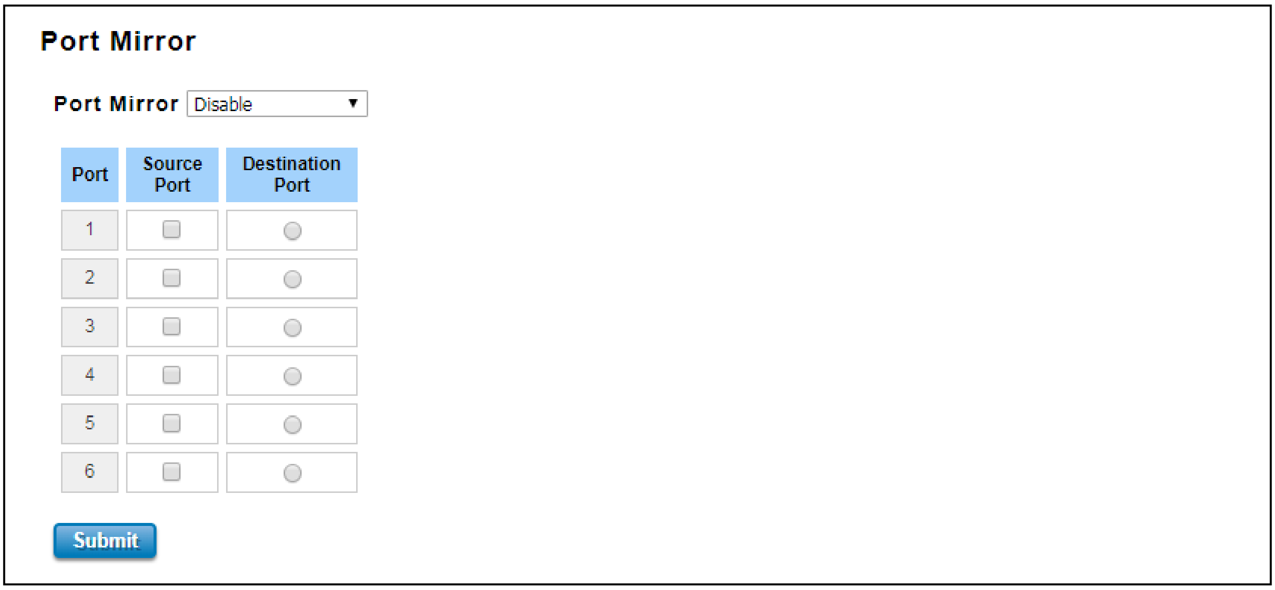
Click on **Reload** to refresh the table.

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.

3.12.5 Port Mirror

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



Port Mirror

Port Mirror: Disable

Port	Source Port	Destination Port
1	□	○
2	□	○
3	□	○
4	□	○
5	□	○
6	□	○

The configuration and settings explain as following.

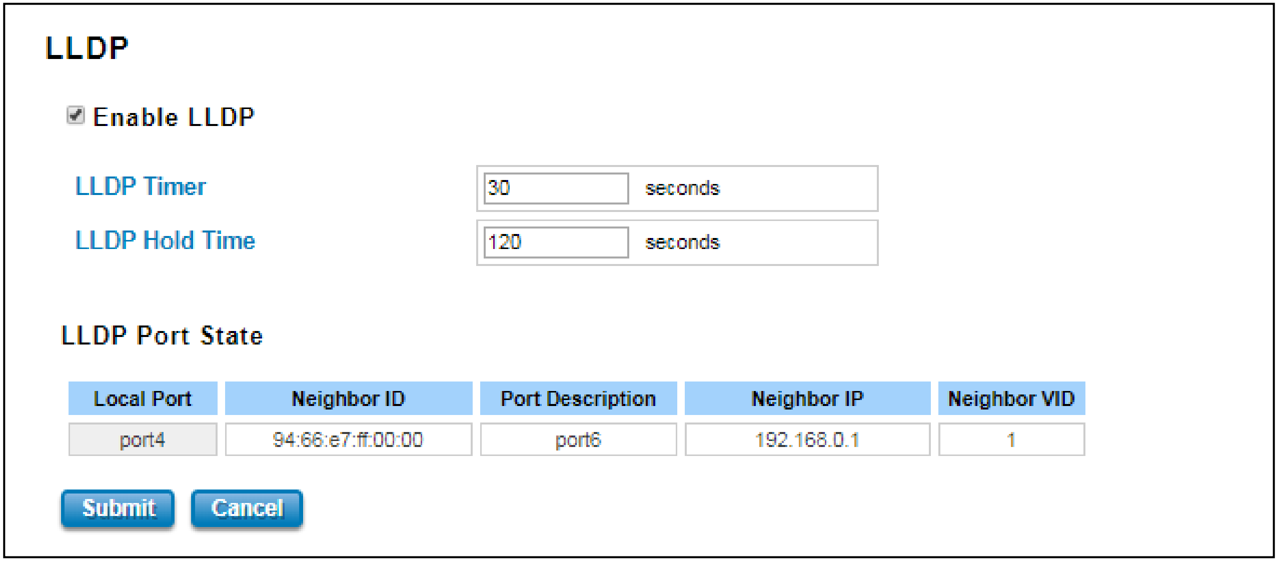
Terms	**Description**
Port Mirror	Select Enable/Disable to enable/disable Port Mirror.
Source Port	These are the ports that User wants to monitor. The traffic of all source ports will be duplicated to destination ports. User can choose a single port, or multiple ports. Click on checkbox of the Port ID,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

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

3.12.6 LLDP

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

The configuration and settings explain as follows.



LLDP

☑ Enable LLDP

LLDP Timer: 30 seconds

LLDP Hold Time: 120 seconds

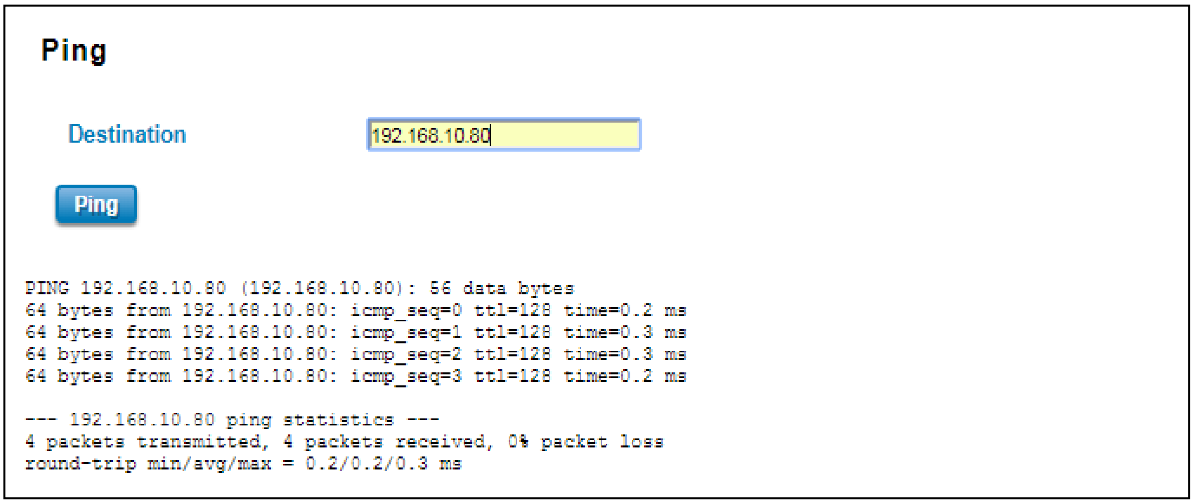
LLDP Port State

Local Port	Neighbor ID	Port Description	Neighbor IP	Neighbor VID
port4	94:66:e7:ff:00:00	port6	192.168.0.1	1

Terms	Description
Enable LLDP	Check the box to enable/disable LLDP function.
LLDP Timer	**Default: 30 seconds** The interval time of each LLDP and counts in second; the valid number is from 5 to254.
LLDP Hold time	**Default: 120 seconds** The TTL (Time To Live) timer. The LLDP state will be expired once the LLDP is not received by the hold time; the valid number is from 10 to 255.
Local port	The current port number that linked with neighbor network device.
Neighbor ID	The MAC address of neighbor device on the same network segment.
Port Description	The port number of neighbor device on the same network segment.
Neighbor IP	The IP address of neighbor device on the same network segment.
Neighbor VID	The VLAN ID of neighbor device on the same network segment.

3.12.7 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.



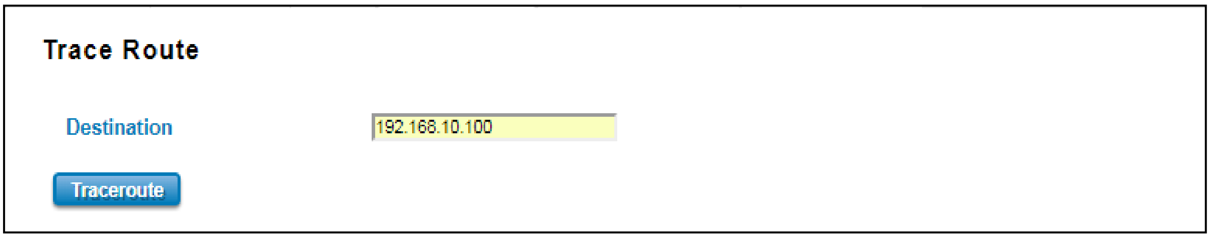
Ping

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
```

3.12.8 Traceroute

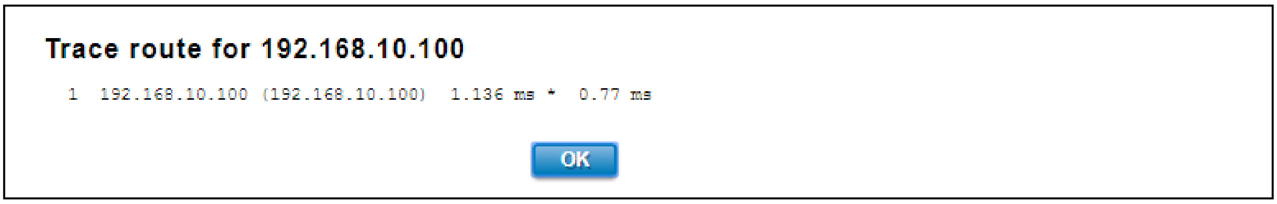
Traceroute is a diagnostics tool for displaying the route (path) and measuring transit delays of packets across an Internet IP network. Log containing route information will be shown after few seconds. Enter the destination IP Address then click traceroute to start the process.



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 *  0.77 ms
```

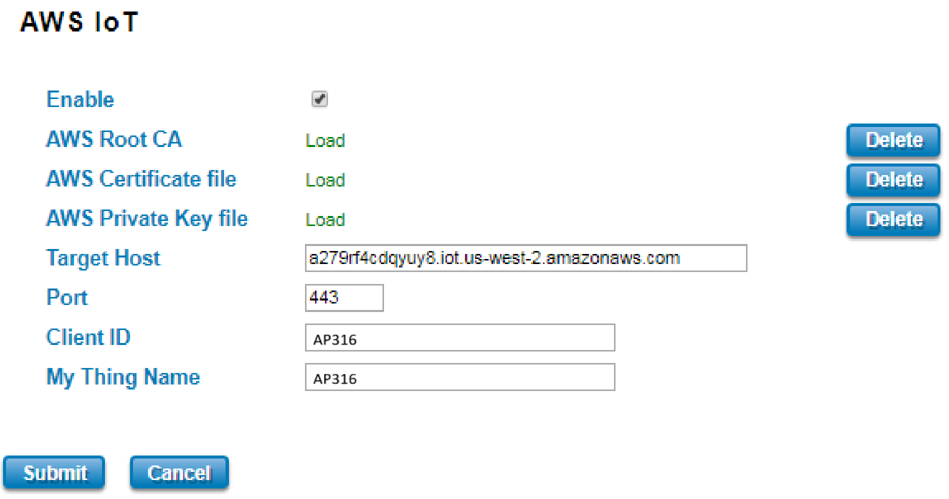
3.13 IoT

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 cloudcan be addressed in terms of securing infrastructure, information, identities, and devices.

3.13.1 AWS IoT

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

The description of the columns is as below:



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 AP316

My Thing Name AP316

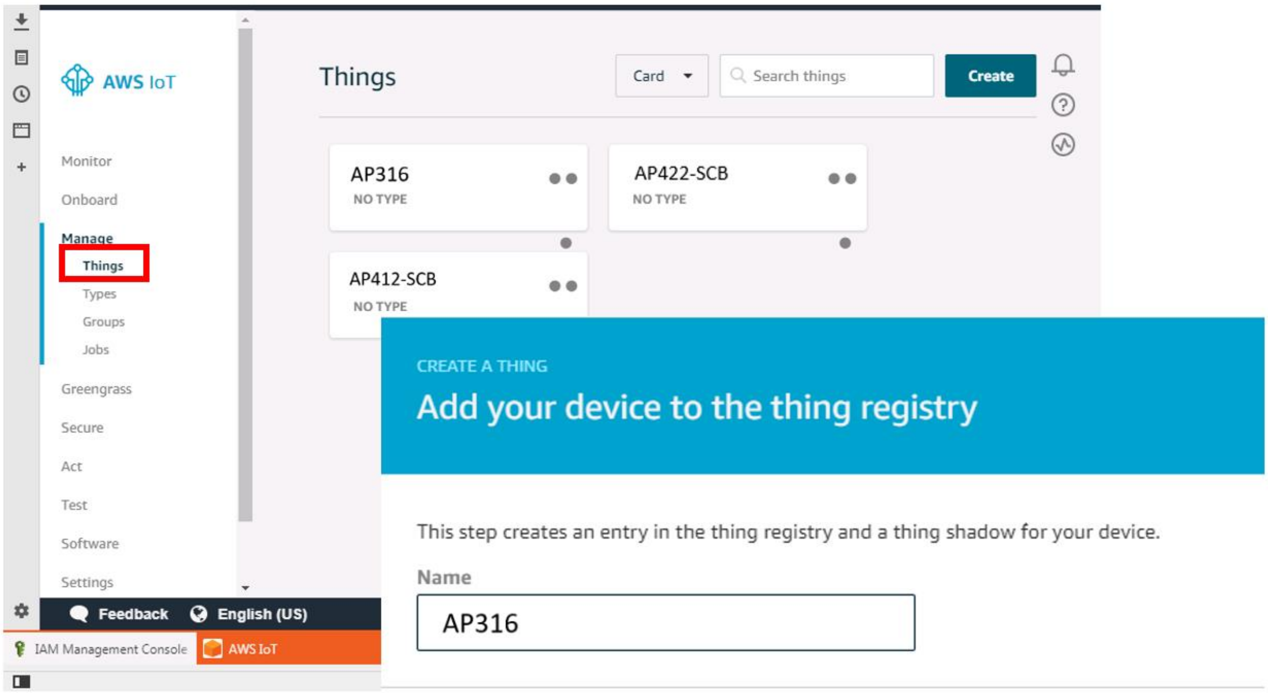
Submit Cancel

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

Click **Submit** to apply the configuration.

How to connect the device to AWS

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



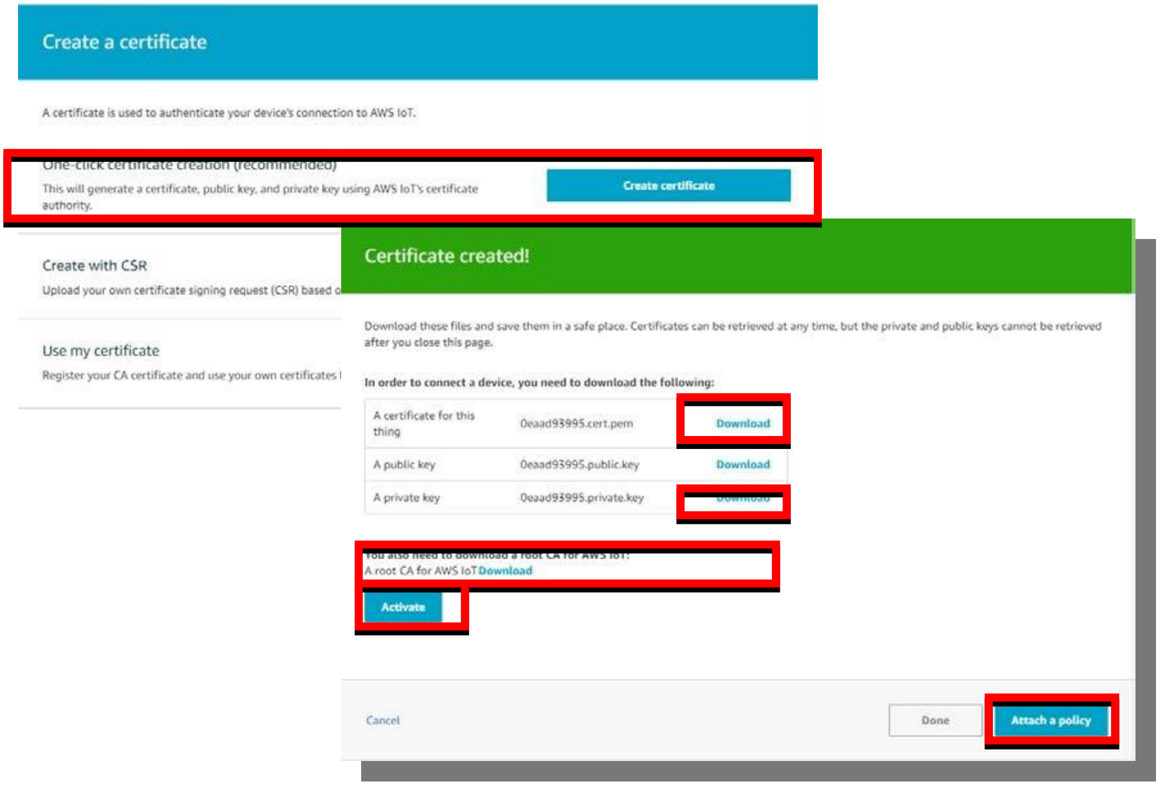
CREATE A THING

Add your device to the thing registry

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

Name: AP316

- 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 i

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:

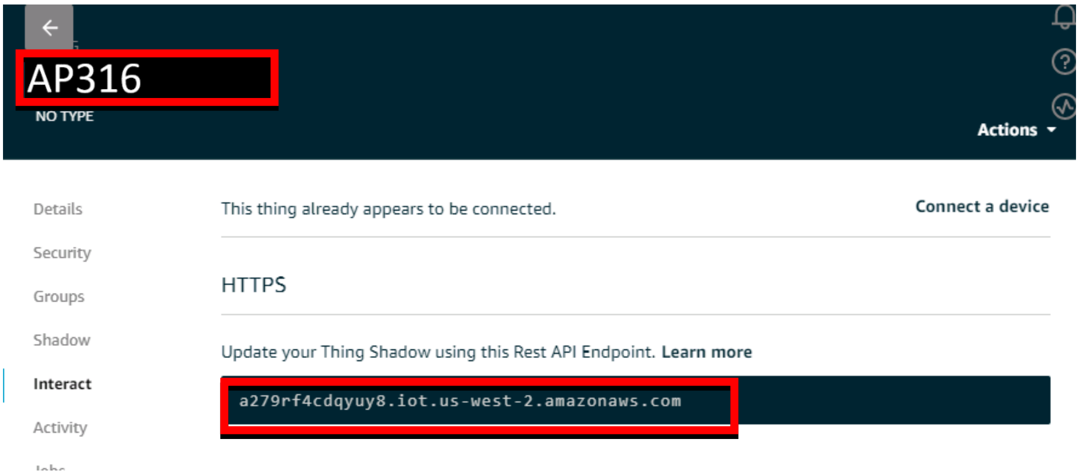
A root CA for AWS IoT Download

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 close 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.



AP316

NO TYPE

This thing already appears to be connected.

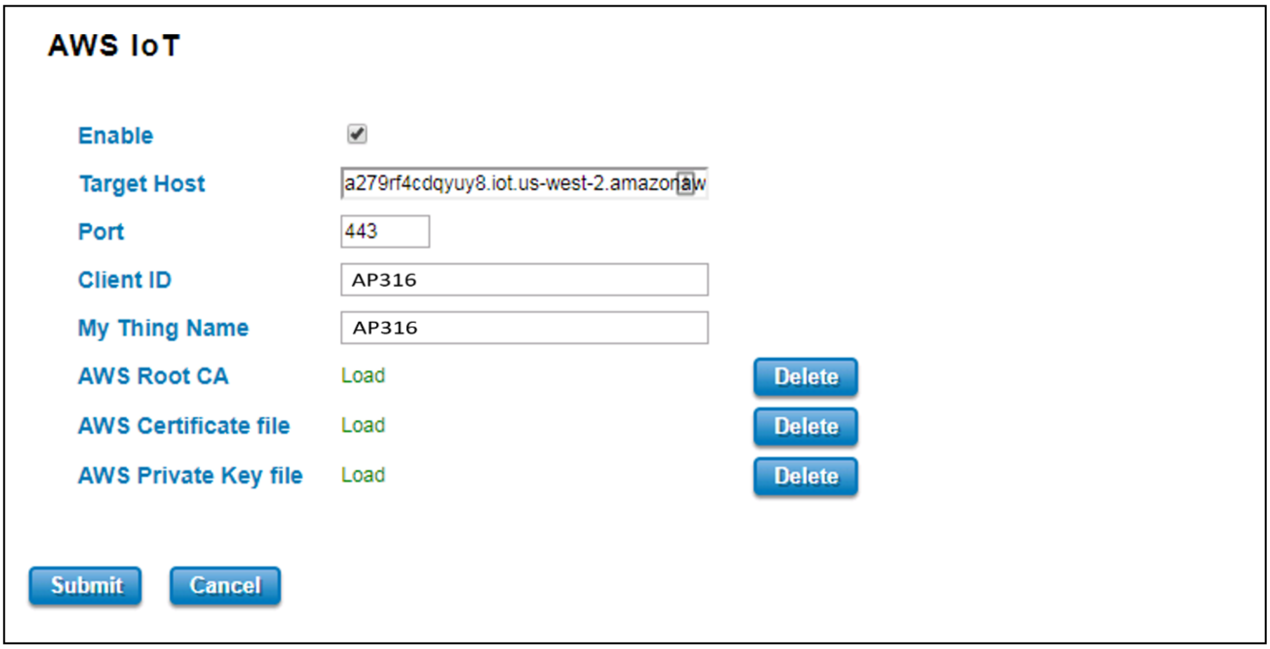
HTTPS

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

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

- Connect the device to AWS.

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



AWS IoT

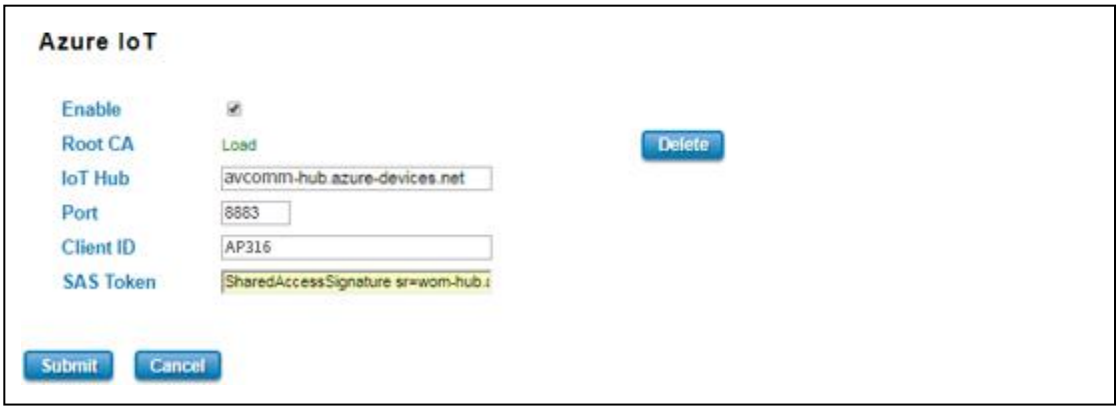
Enable	☑
Target Host	a279rf4cdqyuy8.iot.us-west-2.amazonaw
Port	443
Client ID	AP316
My Thing Name	AP316
AWS Root CA	Load
AWS Certificate file	Load
AWS Private Key file	Load

3.13.2 Azure IoT

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

- Offers reliable device-to-cloud and cloud-to-device hyper-scale messaging.
- Enables secure communications using per-device security credentials and access control.

- Includes the most popular communication protocols.



Azure IoT

Enable ☑
Root CA Load
IoT Hub avcomm-hub.azure-devices.net
Port 8883
Client ID AP316
SAS Token SharedAccessSignature sr=wom-hub.

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 userneeds 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/.

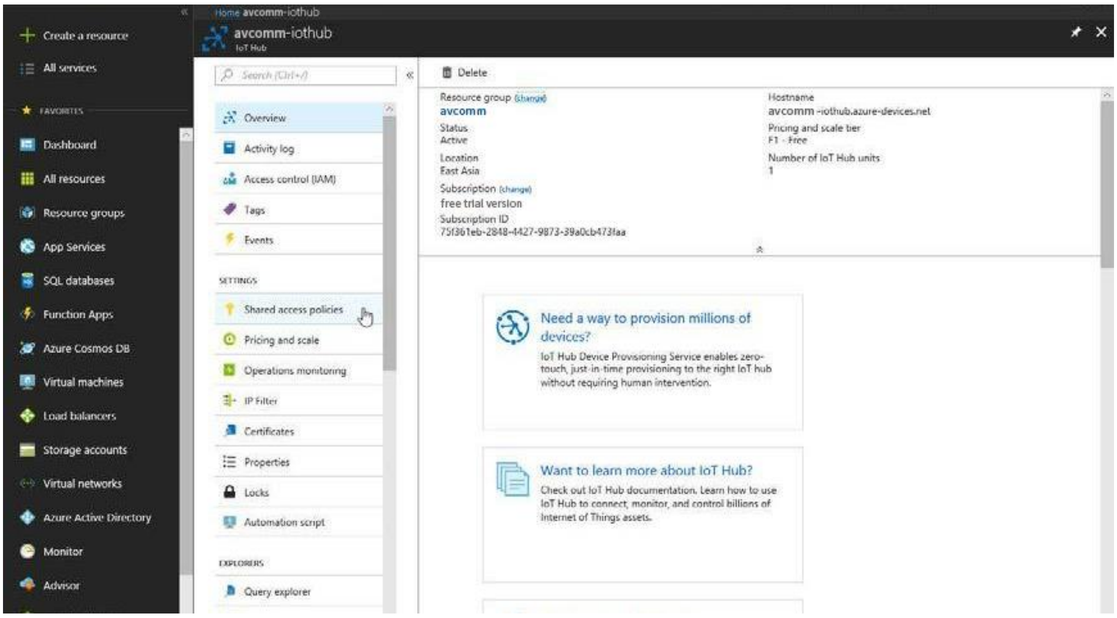
The guide explains how to create an IoT Hub and a device entity. It is important to annotate the connection string generated after creating the device entity. User will need this parameter later for the device configuration.

➢ 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.

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



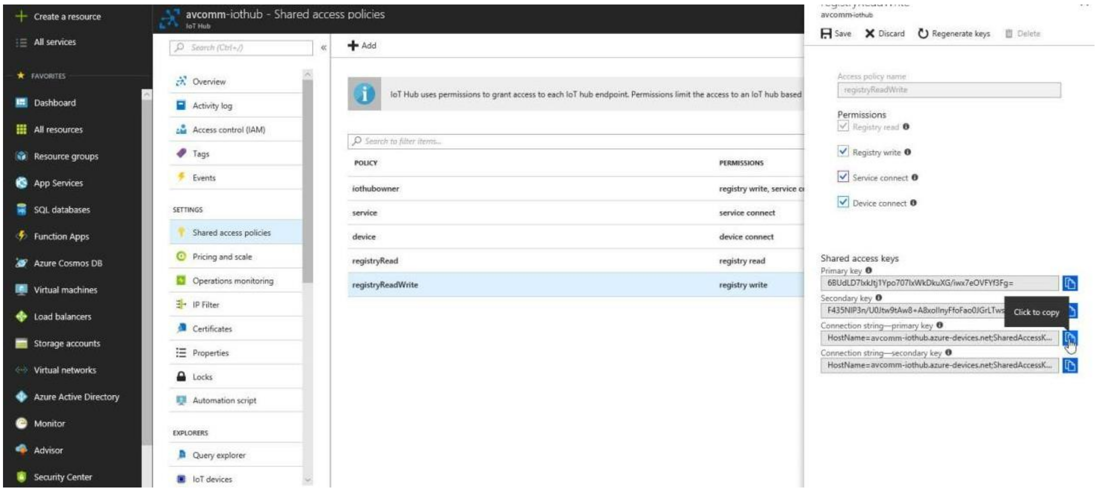
Resource group (change)
avcomm
Status
Active
Location
East Asia
Subscription (change)
free trial version
Subscription ID
75f361eb-2848-4427-9873-39a0cb473faa

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.

- 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

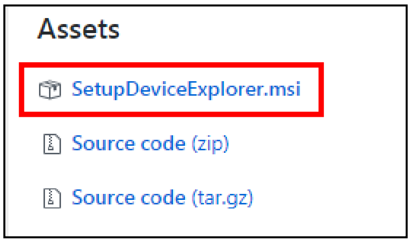
POLICY	PERMISSIONS
iothubowner	registry write, service c
service	service connect
device	device connect
registryRead	registry read
registryReadWrite	registry write

Access policy name
registryReadWrite

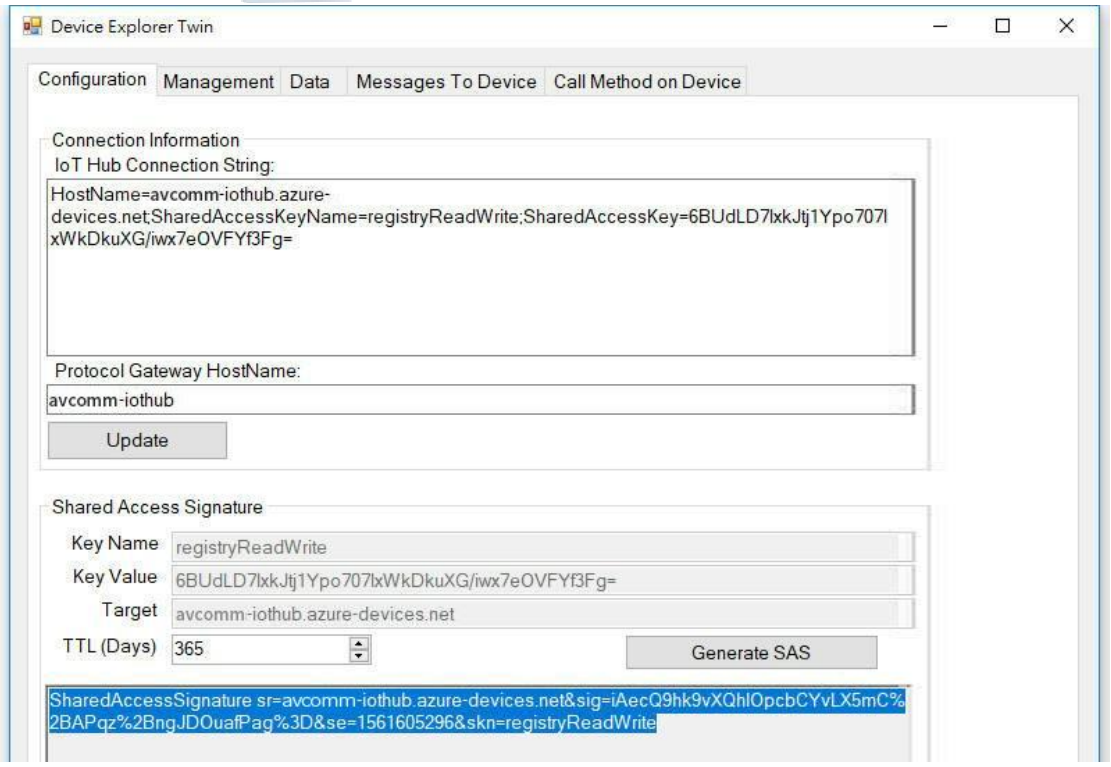
Permissions
☐ Registry read
☑ Registry write
☑ Service connect
☑ Device connect

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...

- 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/SetupDevi ceExplorer.msi



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



Connection Information

IoT Hub Connection String:

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

Protocol Gateway HostName: avcomm-iothub

Shared Access Signature

Key Name: registryReadWrite

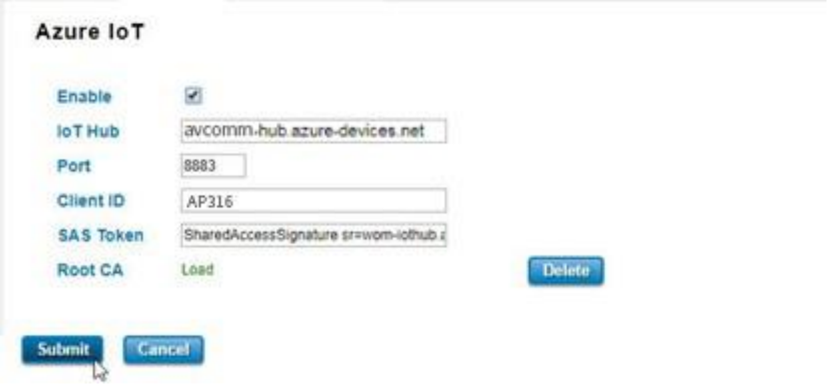
Key Value: 6BUdLD7lxkJtj1Ypo707lxWkDkuXG/iwx7eOVFYf3Fg=

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
```

- 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-hub.azure-devices.net

Port: 8883

Client ID: AP316

SAS Token: SharedAccessSignature sr=wom-iothub.a

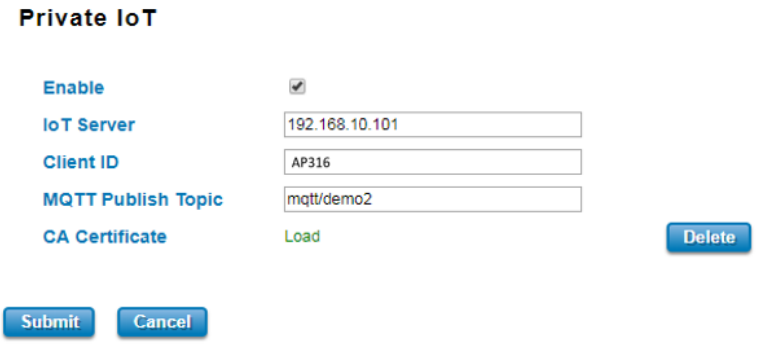
Root CA: Load

- Please find the Root CA through this link:

https://github.com/Azure/azure-iot-sdk-c/blob/master/certs/certs.c

3.13.3 Private IoT

Avcomm provides its own private 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	AP316
MQTT Publish Topic	mqtt/demo2
CA Certificate	Load

The description of the columns is as below:

Terms	Description
Enable	Enable the IoT function
IoT Server	Enter the specific IoT Server.
Client ID	Enter the client ID that has been registered.
MQTT Publish Topic	Specify the MQTT Topic
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**

Click **Submit** to apply the configuration.

➢ How to establish and connect to the ATMS cloud server

- 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

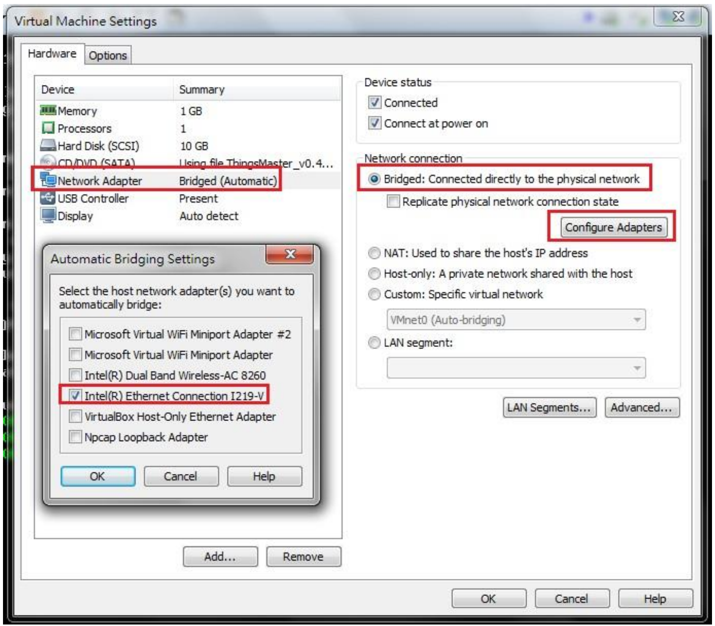
- Download the server file from the link that sent by the Sales.
- Open a Virtual Machine from disk and import.

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

- 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.

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



Virtual Machine Settings

Hardware | Options

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

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

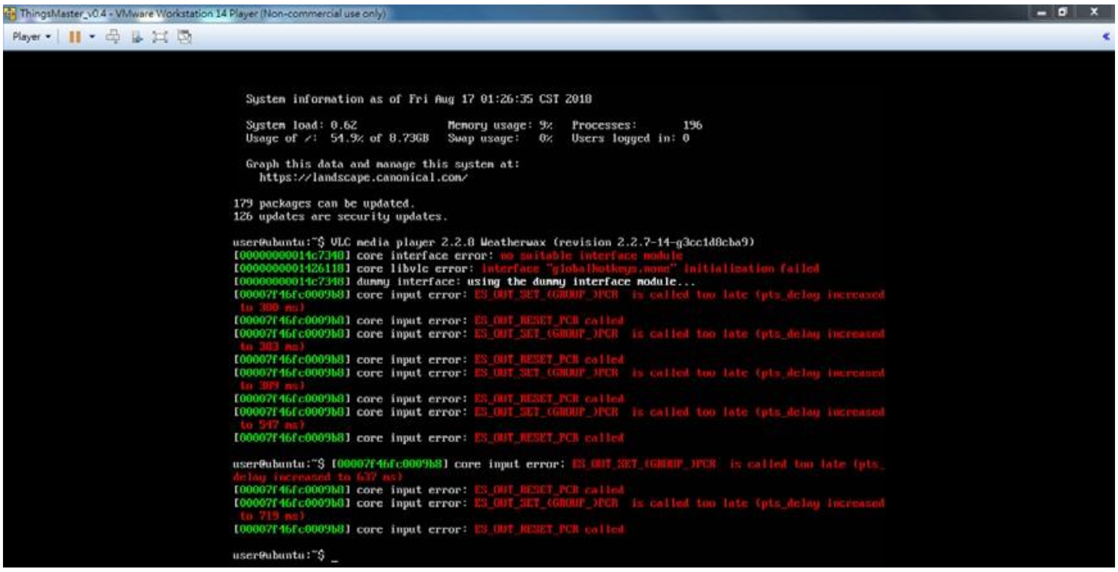
Device status

- ☑ 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:

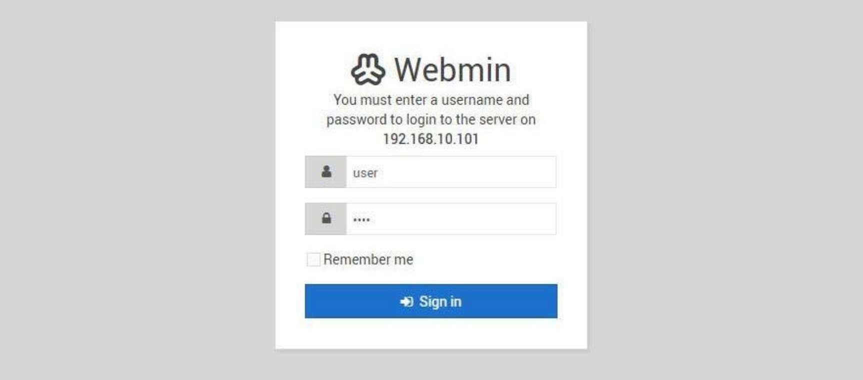
- Start the Virtual Machine, wait till the starting process is done then the ATMS is established.



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

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

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

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

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

user@ubuntu:~$ VLC media player 2.2.8 Weatherwax (revision 2.2.7-14-g3cc1d8cba9)
[00000000014c7348] core interface error: no suitable interface module
[0000000001426118] core libvlc error: interface "globalhotkeys,none" initialization failed
[00000000014c7348] dummy interface: using the dummy interface module...
[00007f46fc0009b8] core input error: ES_OUT_SET_(GROUP_)PCR  is called too late (pts_delay increased
 to 300 ms)
[00007f46fc0009b8] core input error: ES_OUT_RESET_PCR called
[00007f46fc0009b8] core input error: ES_OUT_SET_(GROUP_)PCR  is called too late (pts_delay increased
 to 303 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:~$ _
```

- Open a web browser to Login to Webmin by SSL in order to change some VM configurations.
  Default: https://192.168.10.101:10000
  Username/Password: user/user



Webmin

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

user

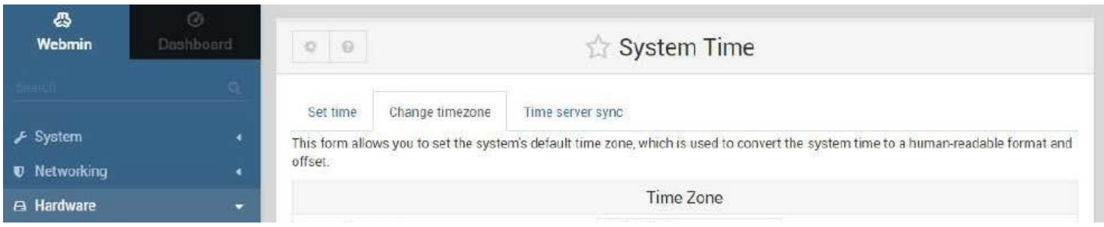
....

☐ Remember me

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

- **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 toHardware -> System Time -> Set Time -> Change Time Zone



System Time

Set time | Change timezone | Time server sync

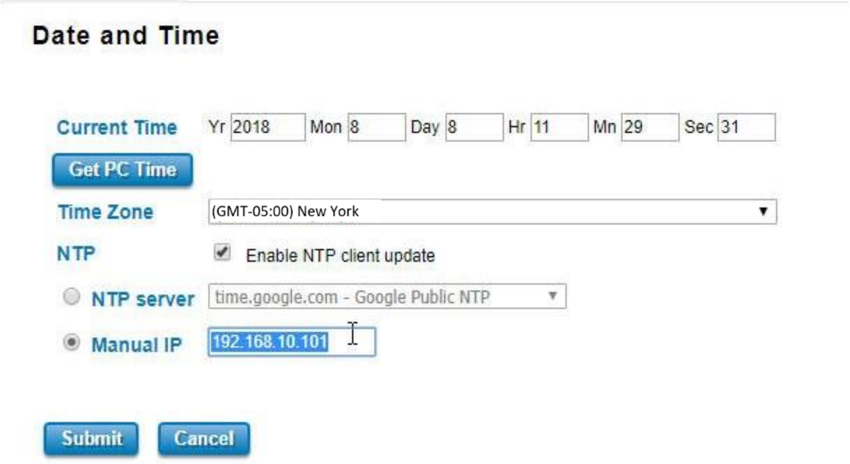
This form allows you to set the system's default time zone, which is used to convert the system time to a human-readable format and offset.

Time Zone

- 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

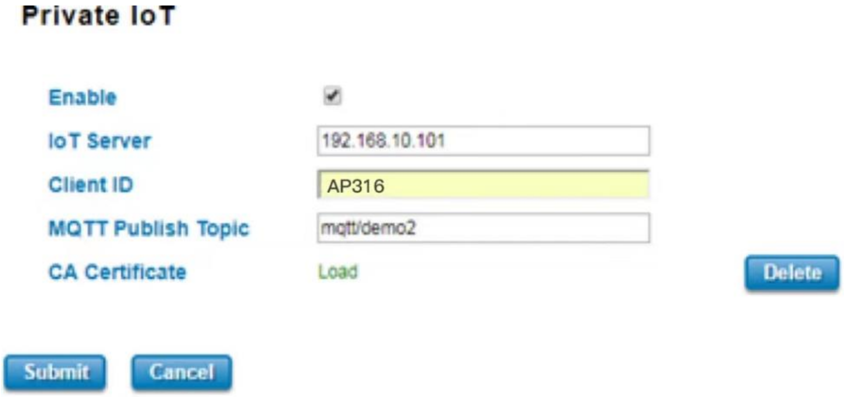
Time Zone: (GMT-05:00) New York

NTP: ☑ Enable NTP client update

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

● Manual IP: 192.168.10.101

- Enable IoT service and get connected to the ATMS



Private IoT

Enable: ☑

IoT Server: 192.168.10.101

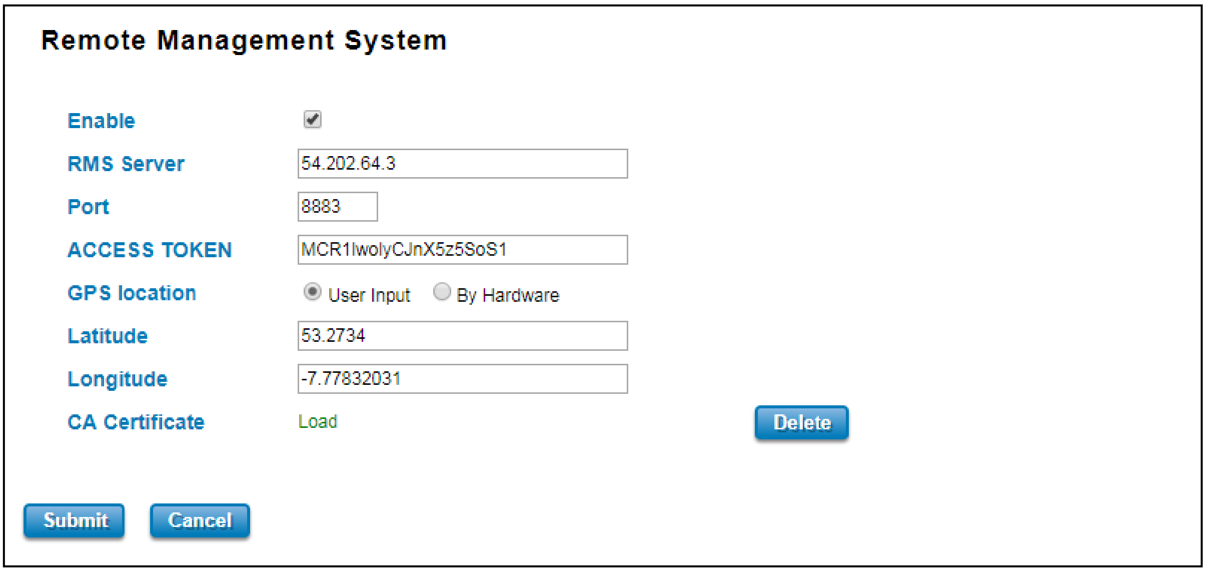
Client ID: AP316

MQTT Publish Topic: mqtt/demo2

CA Certificate: Load

3.13.4 RMS

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



Remote Management System

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

The description of the columns is as below:

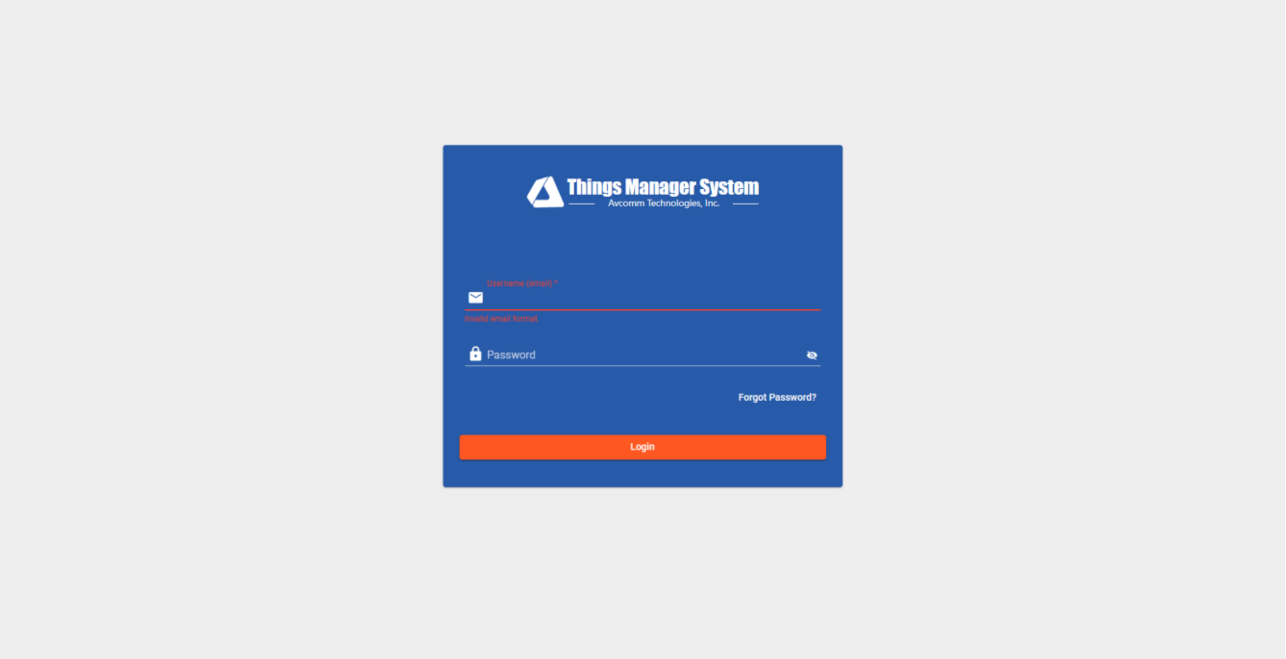
Terms	Description
Enable	Check the box to enable the RMS function.
RMS Server	Enter the RMS Server IP Address
Port	**Default: 8883**
ACCESS TOKEN	Generate the token from ATMS RMS; this access token is used to access the device.
GPS Location	**User Input**: User input the device location information.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

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

➢ How to establish and connect to the ATMS RMS server

- Contact our Sales to get the access to the ATMS RMS Account.
- Login to ATMS RMS, using RMS Account.

Login: <User RMS Account> Password: <User RMS Password>

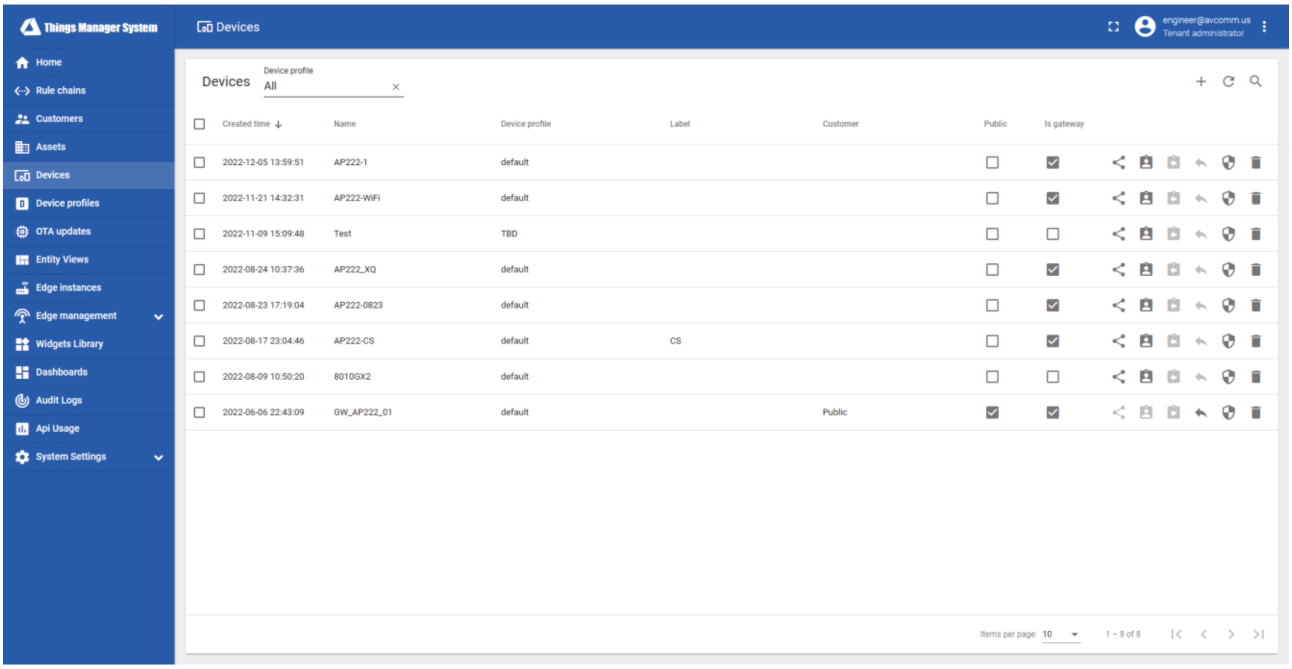


Username (email) *

Invalid email format.

Password

- Click the Device -> Device Management to register the device.

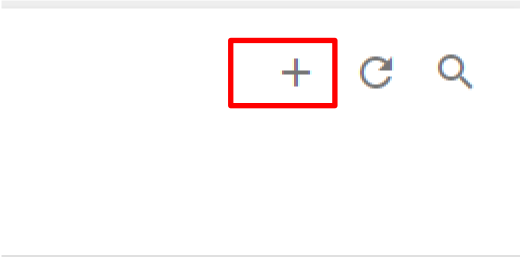


Devices Device profile: All

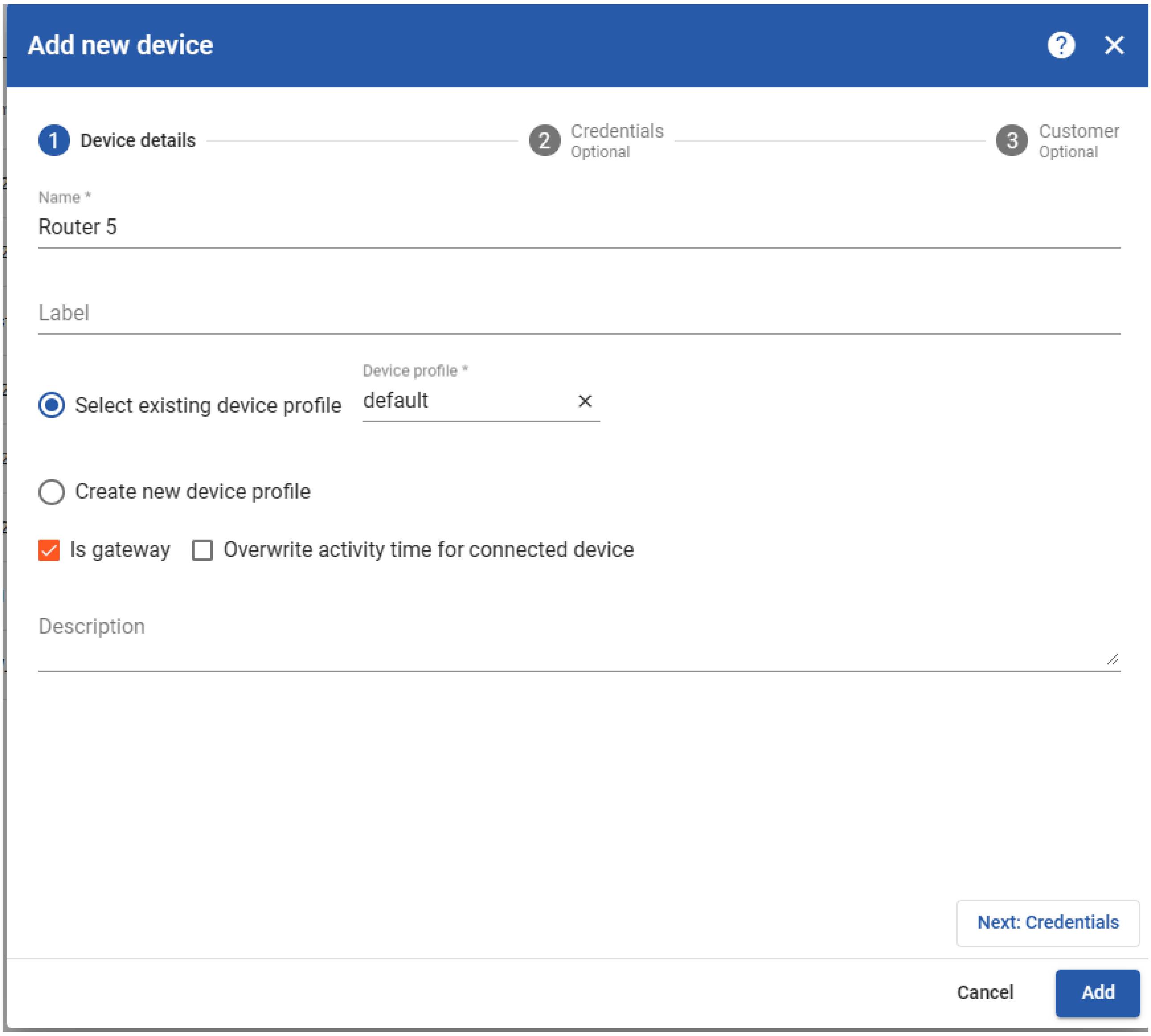
□	Created time ↓	Name	Device profile	Label	Customer	Public	Is gateway
□	2022-12-05 13:59:51	AP222-1	default			□	☑
□	2022-11-21 14:32:31	AP222-WiFi	default			□	☑
□	2022-11-09 15:09:48	Test	TBD			□	□
□	2022-08-24 10:37:36	AP222_XQ	default			□	☑
□	2022-08-23 17:19:04	AP222-0823	default			□	☑
□	2022-08-17 23:04:46	AP222-CS	default	CS		□	☑
□	2022-08-09 10:50:20	8010GX2	default			□	□
□	2022-06-06 22:43:09	GW_AP222_01	default		Public	☑	☑

Items per page: 10 1 – 8 of 8

- Add new device information, by clicking the "+" at the corner of the page.



- After click “+” menu then a page will pop up. Enter the device information.
  - Name: Please start the name with Router + Number.
  - Device type: default
  - Is gateway: check the box
  - Click **Add**



Add new device

1 Device details — 2 Credentials Optional — 3 Customer Optional

Name *
Router 5

Label

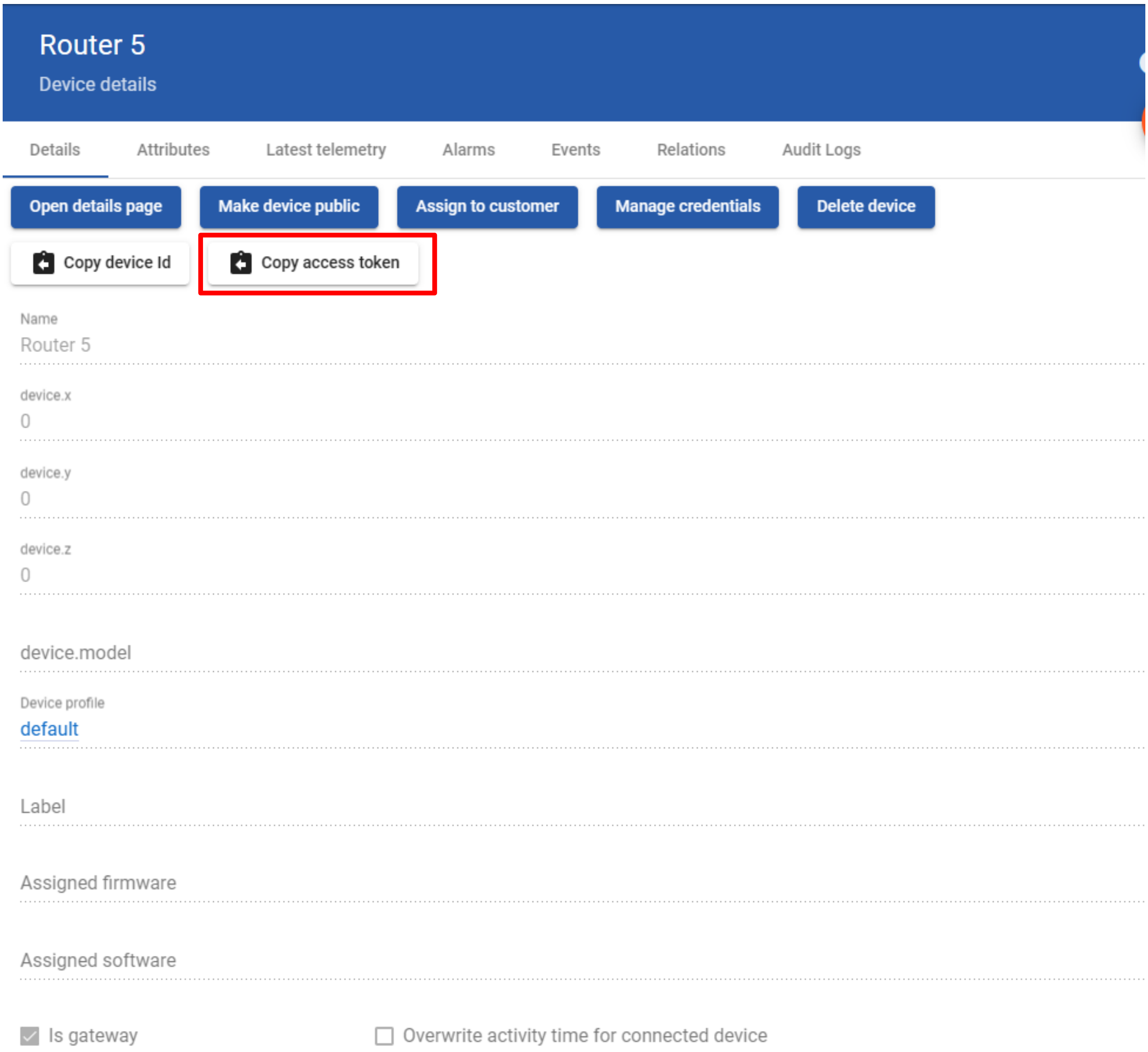
● Select existing device profile   Device profile *
default ×

○ Create new device profile

☑ Is gateway   □ Overwrite activity time for connected device

Description

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



Router 5

Device details

Name
Router 5

device.x
0

device.y
0

device.z
0

device.model

Device profile
default

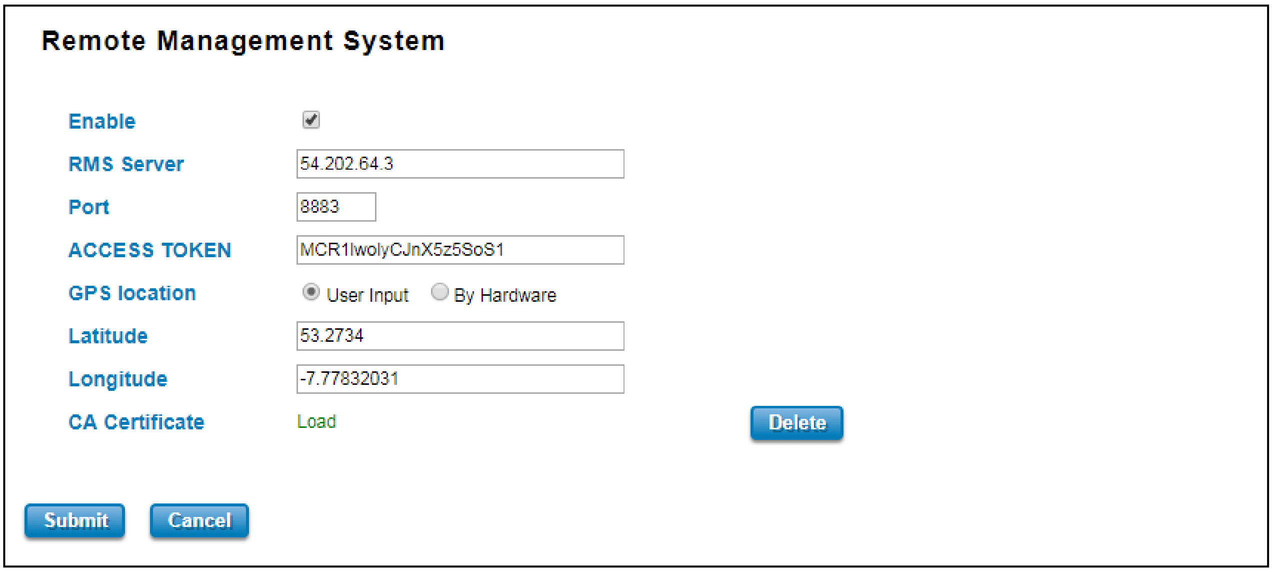
Label

Assigned firmware

Assigned software

☑ Is gateway □ Overwrite activity time for connected device

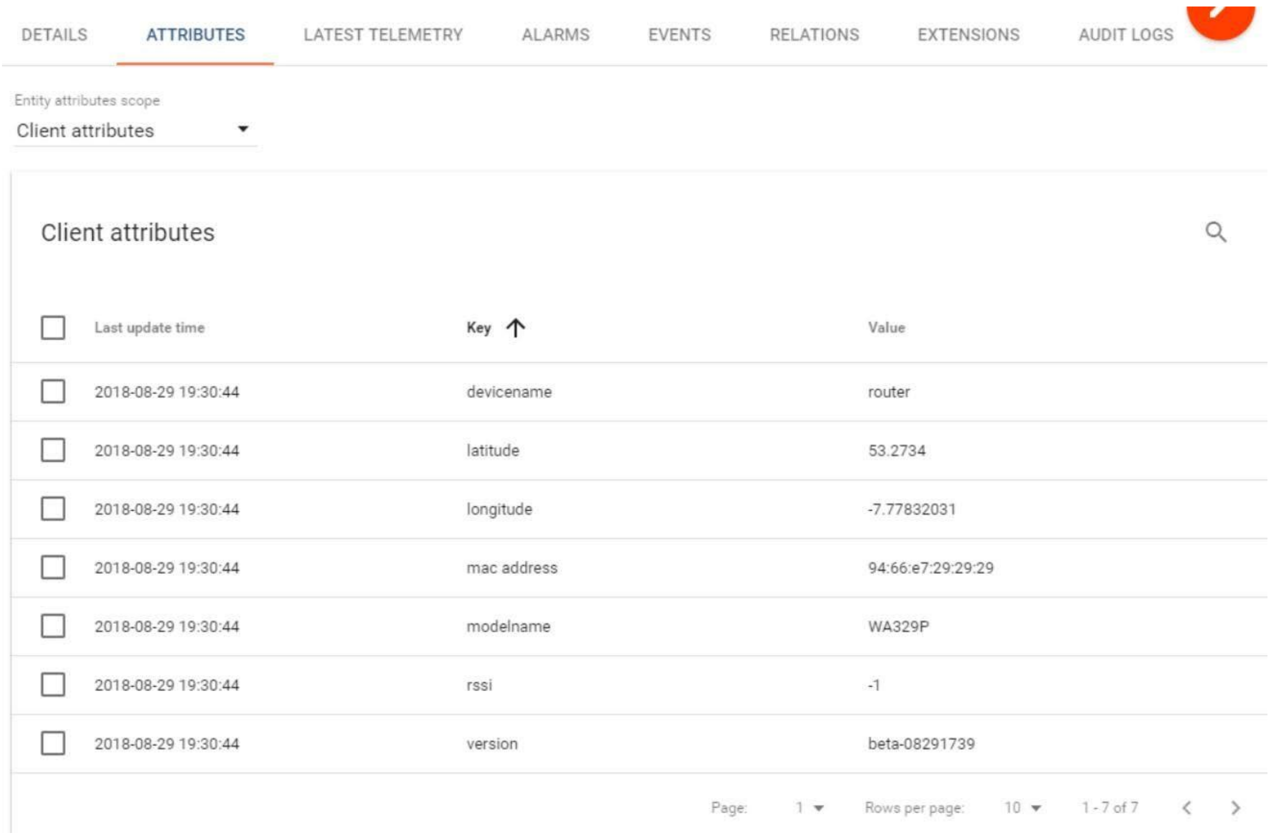
- Go to the Web GUI -> IoT -> RMS. Paste the Access Token code to the Web GUI. And complete the configuration.



Remote Management System

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

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



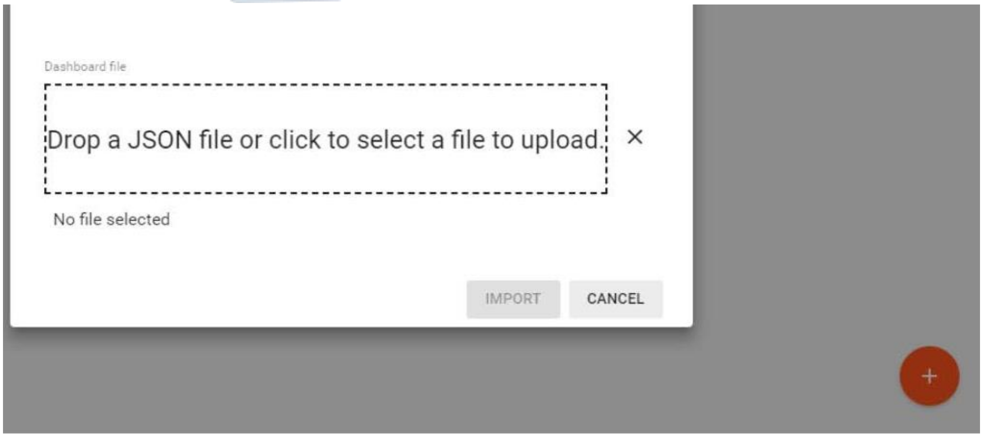
Entity attributes scope
Client attributes

Client attributes

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

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

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

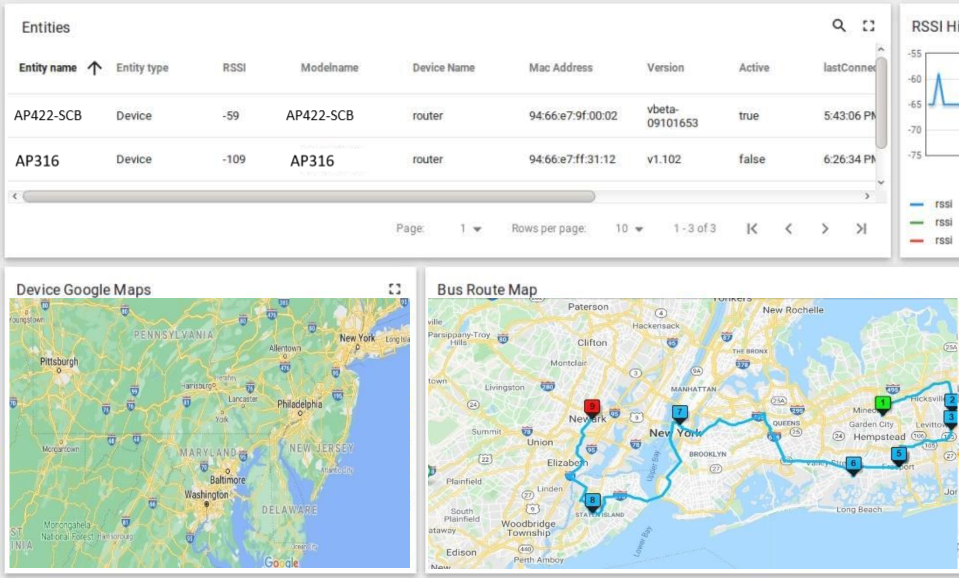


Dashboard file

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

No file selected

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



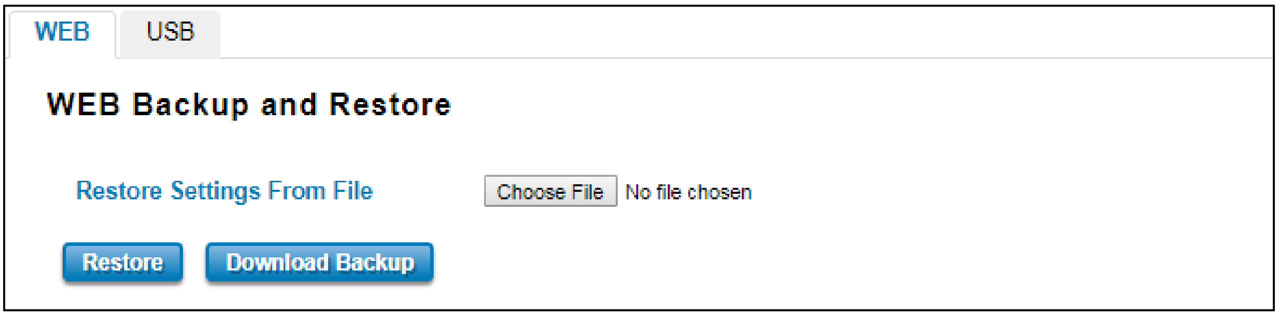
Entities

Entity name	Entity type	RSSI	Modelname	Device Name	Mac Address	Version	Active	lastConne
AP422-SCB	Device	-59	AP422-SCB	router	94:66:e7:9f:00:02	vbeta-09101653	true	5:43:06 PM
AP316	Device	-109	AP316	router	94:66:e7:ff:31:12	v1.102	false	6:26:34 PM

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

3.14 Backup and Restore ACKUP AND RESTORE

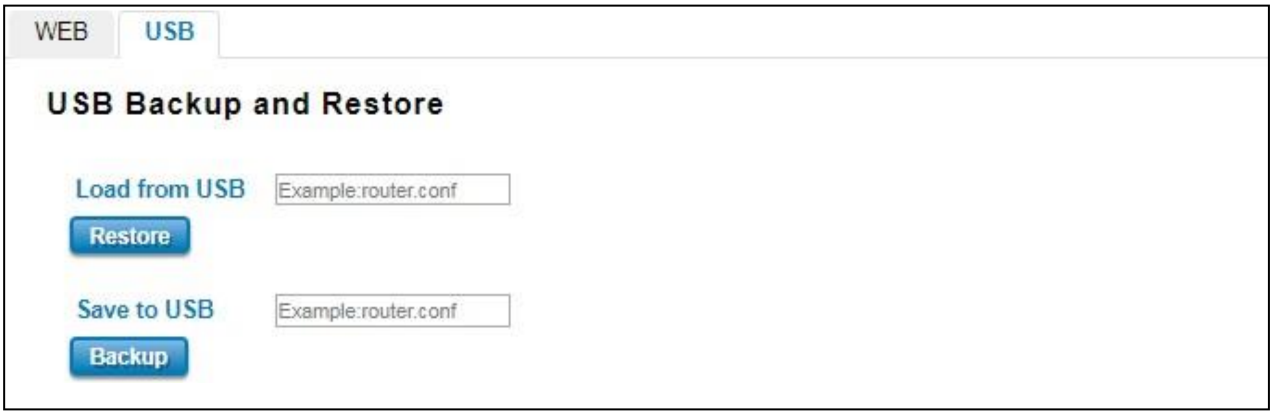
User can use Avcomm Backup and Restore configuration to save and load configuration through the router. There are 2 modes for users to backup/restore the configuration file.



WEB Backup and Restore

Restore Settings From File Choose 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.



USB Backup and Restore

Load from USB Example:router.conf

Save to USB Example:router.conf

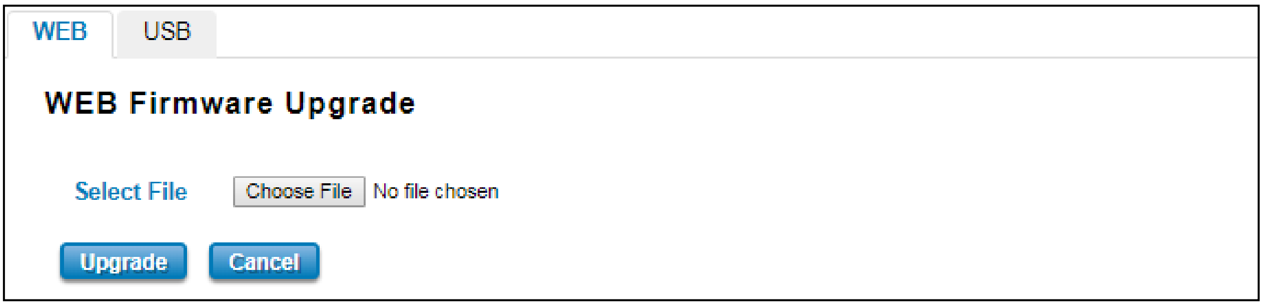
USB mode: this mode has two functions, Load Setting from File and Save Setting to USB. Load Setting from File, make sure that the USB has been inserted and it has the .conf file which is the backup files. After inserting the USB, the USB port will directly read the USB and then user needs to type the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

3.15 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.

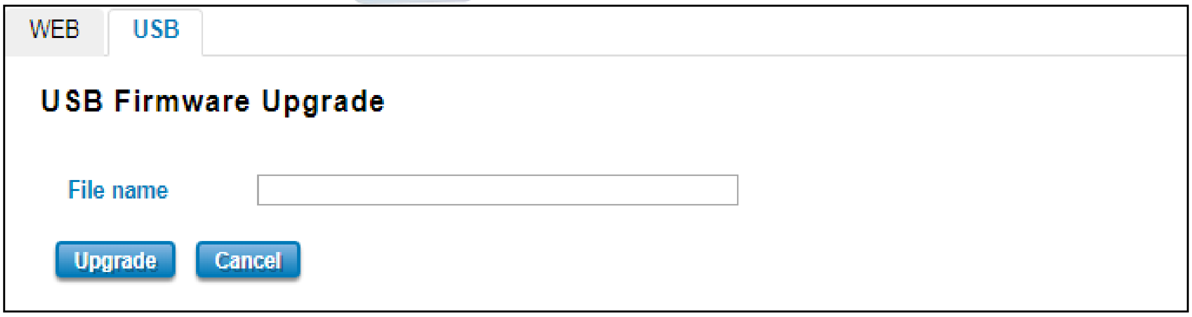
There are 2 modes for users to backup/restore the configuration file, Web mode, and USB mode.



WEB Firmware Upgrade

Select File Choose 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.



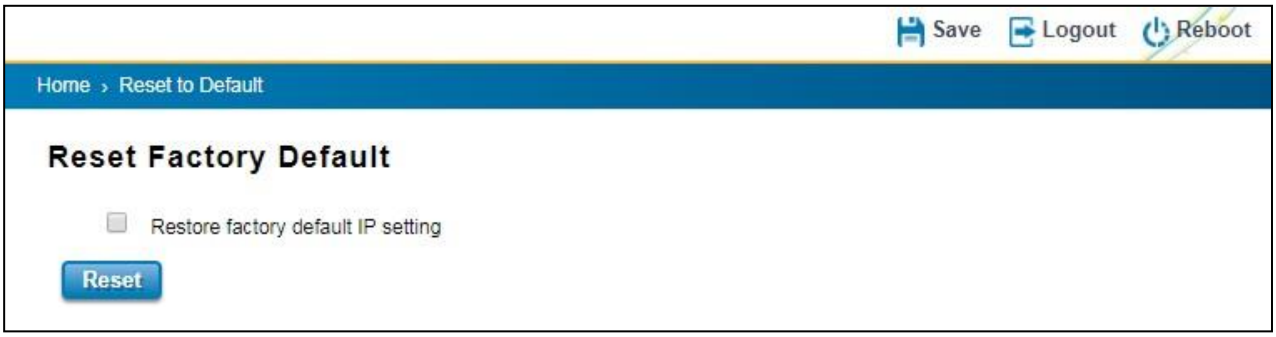
USB Firmware Upgrade

File name

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

3.16 Reset to Defaults

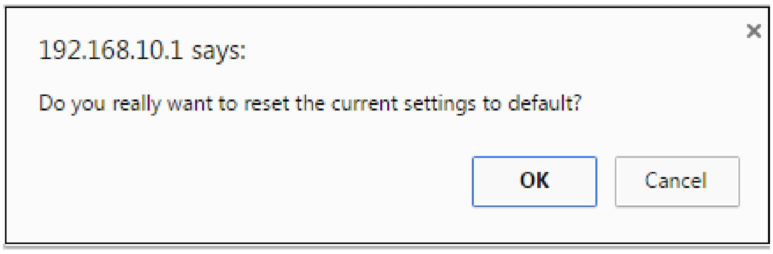
This function provides users with a quick way of restoring the Avcomm router's configuration to factory defaults. By check the Restore Factory default IP setting, it means the IP of the device will directly change to the default IP (192.168.10.1).



Reset Factory Default

□ Restore factory default IP setting

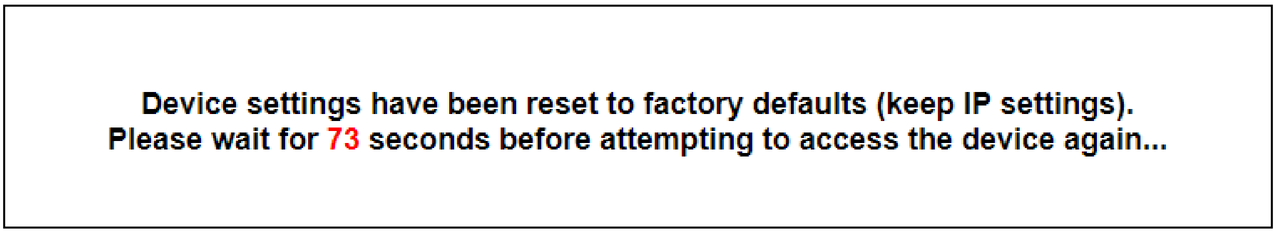
Pop-up message screen to show User that have done the command. Click on **OK** to close the screen and reboot the device.



192.168.10.1 says:

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

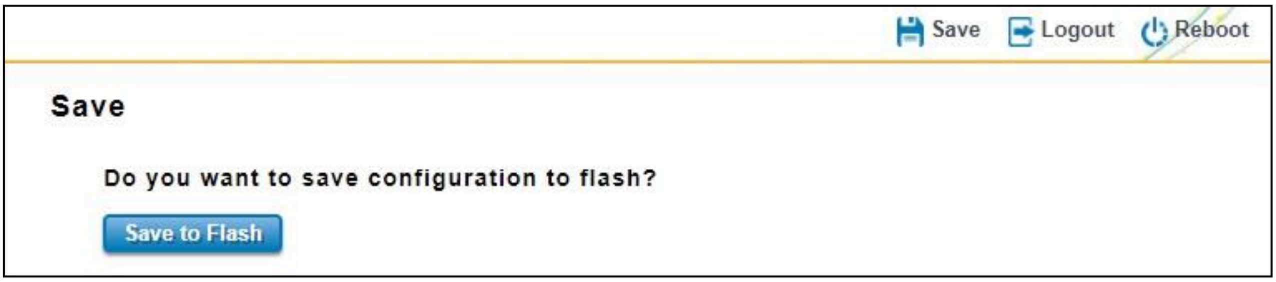
Below is the interface for resetting the device with keep the IP Settings.



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

3.17 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.

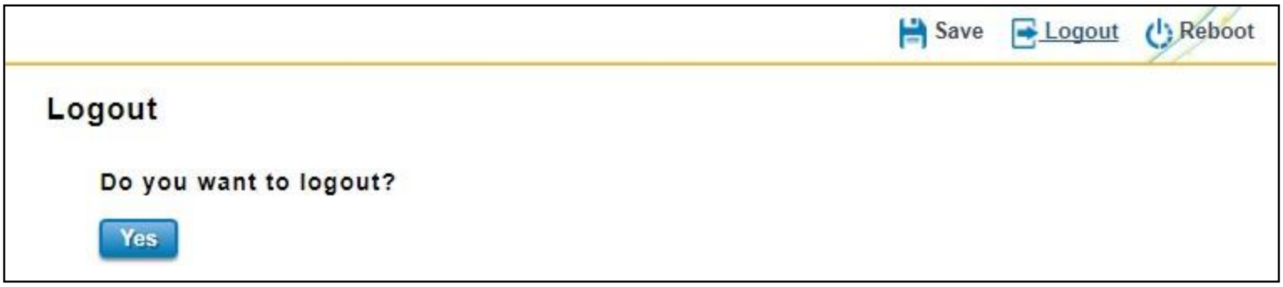


Save

Do you want to save configuration to flash?

3.18 Logout

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



Logout

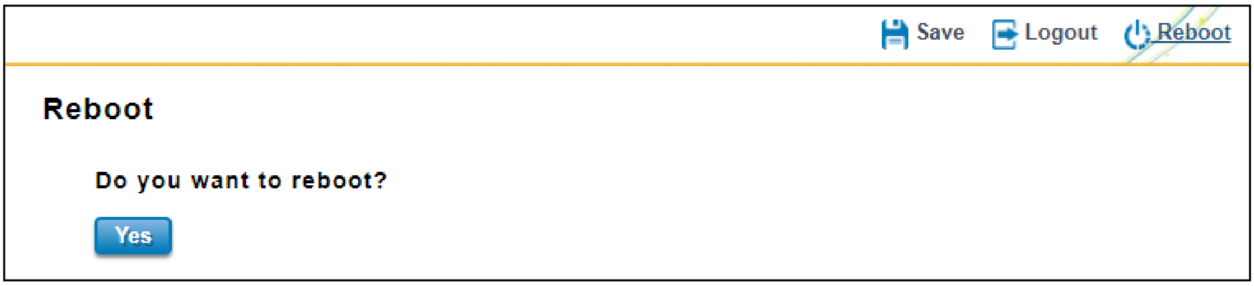
Do you want to logout?

3.19 Reboot

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

NOTE: Remember to click on Save button to save configuration settings. Otherwise, the settingsuser 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?

3.20 MIB

Avcomm provides Private MIBs for users to configure or monitor the device's configuration by SNMP. Avcomm provides Private MIB to meet up the need. Compile the private MIB file by SNMP tool or using Avcomm ANMS. The Private MIB can be found in or downloaded from Avcomm Web site (www.avcomm.us). Private MIBtree is the same as the web tree. This is easier to understand and use. If user does not familiar with standard MIB, User can directly use private MIB to manage /monitor the device.

The table below is the MIB file and the supported model:

AVCOMM-ROUTER-MIB	AP412-SCB/AP422-SCB AP322 AP316 AP329
AVCOMM-SERIAL-MIB (by Hardware)	AP422-SCB AP322
AVCOMM-CELLULAR-MIB (by Hardware)	AP316 AP329
AVCOMM-GPS-MIB (by Hardware)	AP412-SCB/AP422-SCB AP322 (GPS by request) AP316 AP329