Industrial 4G LTE Cellular Router
ICR100G-11

User Manual

Version 1.0

Advice Electronics Ltd. Advice Building,16 Atir Yeda St., Kfar Saba, 4464321, Israel • Tel:+972-3-9000900 • advice@advice.co.il • www.advice.co.il

Table of Contents

1 Introduction

ADVICE ICR100G-11 4G LTE Cellular Router is highly reliable and secure wireless communications gateway designed for industrial networking. The **ICR100G-11** supports multi-band connectivity including FDD/TDD LTE, WCDMA and GSM for a wide range of applications and vertical machine-to-machine (M2M) markets. To enhance reliability, **ADVICE ICR100G-11** is equipped with dual SIM that support failover and roaming over to ensure uninterrupted connectivity for mission-critical cellular communications.

With flexible LAN/WAN Ethernet options, **ADVICE ICR100G-11** allows you to customize your professional applications in diverse environments. Integrated with WAN, LAN, built-in DI/DO and RS-232/RS-485 serial ports, the **ICR100G-11** also provide various serial network protocols, such as IPv6, Modbus Gateway, MQTT and VPN for enriching connectivity and security. For VPN tunnels, OpenVPN and IPSec are for reliable authentication of the network stations, data encryption and verification of data integrity. The device is administrated via web GUI, Telnet, SSH v2 and HTTP/HTTPS.

Built for secure and uninterrupted operation in harsh environments, **ADVICE ICR100G-11** supports extended operating temperature from -20 to +70°C and a flexible input voltage range of 10-32V DC. With DIN-rail mounting and IP40 housing protection, **ADVICE ICR100G-11** is an ideal cellular communications solution for heavy industrial use.

1.1 Features

- Highly reliable and secure for mission-critical cellular communications
- Provide flexible options to configure LAN/ WAN ports
- Support multi-band connectivity with FDD LTE/ TDD LTE/ WCDMA/ GSM/ LTE Cat4
- Built-in dual SIM for network redundancy
- Integrated dual detachable antenna against radio interference
- LED indicators for connection and data transmission status
- Industrial rated from -20°C to +70°C for use in harsh environments
- Metal Housing with IP40 industrial grade protection
- IPv6/IPv4 dual stack and all applications are IPv6 ready
- Support various serial communication protocols for connectivity
- Enhance security and encryption for authentication and transmission

1.2 Specifications

LTE Interface

- FDD LTE: B1/B3/B5/B7/B8/B20
- TDD LTE: B38/B40/B41
- WCDMA: B1/B5/B8
- GSM: 900/1800 MHz
- LTE Cat4

Processor & I/O Interface

- High performance 528 MHz CPU with 512 Mbytes of DDR3 memory
- 2 x SIM Card Slots
- 1 x LAN 10/100 Mbps Ethernet port (Model: M300)
- 3 x LAN 10/100 Mbps Ethernet ports (Model: M301)
- 1 x WAN 10/100 Mbps Ethernet port
- Reset Button
- Console: 1 x RS232 (9-pin Sub-D)
- 2 x SMA connectors for detachable LTE antenna
- 1 x GPS detachable antenna (Optional)
- 1 x RS485 (D+/D-)
- 1 x RS232 (TXD/RXD)
- 2 x DI, 1 x DO (Alarm +/-)

Physical Characteristics

- Enclosure：Metal Shell, IP40 Protection
- Weight：451 g (M300) / 452 g (M301)
- Dimensions (W x H x D)：60 x 110 x 106 mm
- Installation：DIN Rail (Default) or Wall Mount (Optional)

LED Display

- 1 x System status LED (Green)
- 1 x VPN status LED (Green)
- 1 x SIM1 status LED (Green)
- 1 x SIM2 status LED (Green)
- Ethernet status LEDs (Green for LINK/ACT, Yellow for SPEED)
- 2 x Mobile connection strength LEDs (Green)

Power Supply

- Power Consumption 7 Watts(Max)
- Power Input 10 ~ 32V DC

MTBF (mean time between failures)

- M300: 155,899 hrs (MIL-HDBK-217-FN2)
- M301: 148,930 hrs (MIL-HDBK-217-FN2)

Software

- **Network Protocols:**
  IPv4, IPv6, IPv4/IPv6 dual stack, DHCP server and client, PPPoE, Static IP, SNTP, GPS sync time, DNS Proxy, Modbus, VRRP, OSPF, Message Queue Telemetry Transport (MQTT Broker), BGP
- **Routing/Firewall:**
  NAT, Virtual Server, DMZ, MAC Filter, URL Filter, IP Filter, VLAN, Static Routing and RIP-1/2
- **VPN:**
  OpenVPN, IPSec (3DES, AES128, AES196, AES256, MD5, SHA-1, SHA256), GRE
- **Wireless Connectivity:**
  Two SIM for failover/ roaming over/ back up
  Two SIM data usage control
  Seamless multi WAN connections switch
- **Others:**
  DDNS, QoS, Virtual COM, UPnP
- **Alarm:**
  DI, DO, SMS, VPN/WAN Disconnect, SNMP Trap, E-mail

Management Software

- Web GUI for remote and local management, CLI
- Dual Image firmware upgrade by Web GUI
- Syslog monitor
- SNMP, TR069
- Remote management via SSH v2, HTTPS
- Local management via Telnet, SSH v2, HTTP/HTTPS

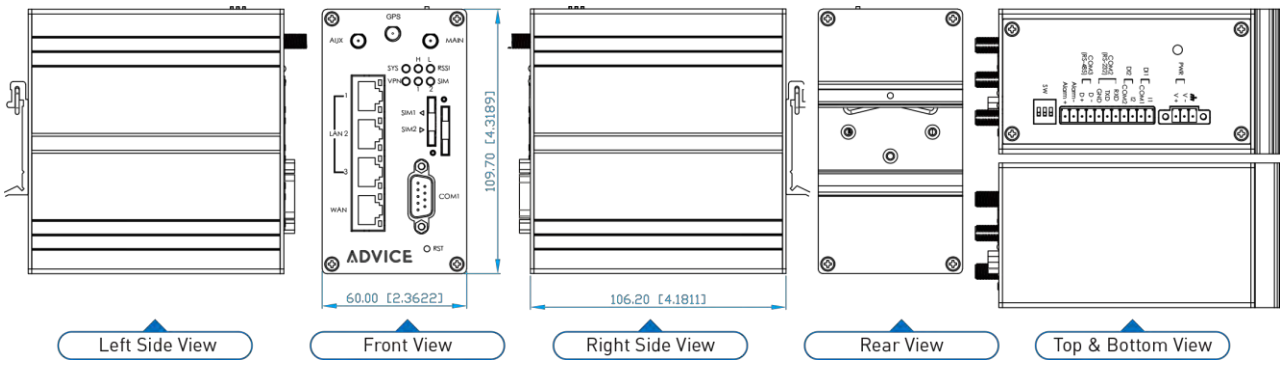
Environment

- Operating Temperature -20 ~ +70°C
- Storage Temperature -40 ~ +85°C
- Ambient Relative Humidity 10 ~ 95% (non-condensing)
- Humidity 0 ~ 95% (non-condensing)

Standards and Certifications

- **EMC**：CE, FCC
- **EMI**：EN 55032 Class A, FCC Part 15 Subpart B Class A
- **EMS**：EN 55024 / EN 61000-4-2 (ESD) Level 3 / EN 61000-4-3 (RS) Level 3 / EN 61000-4-4 (EFT) Level 4 / EN 61000-4-5 (Surge) Level 3 / EN 61000-4-6 (CS) Level 3 / EN 61000-4-8 (PFMF) Level 4 / EN 61000-4-11 / EN 61000-6-2 (Industrial) / EN 61000-6-4 (Industrial)
- **Rail Traffic**：EN50121-4
- **Vibration**：IEC60068-2-6
- **Safety**：EN60950-1
- **Highly Accelerated Life Test (HALT)**

1.3 Mechanical Dimensions



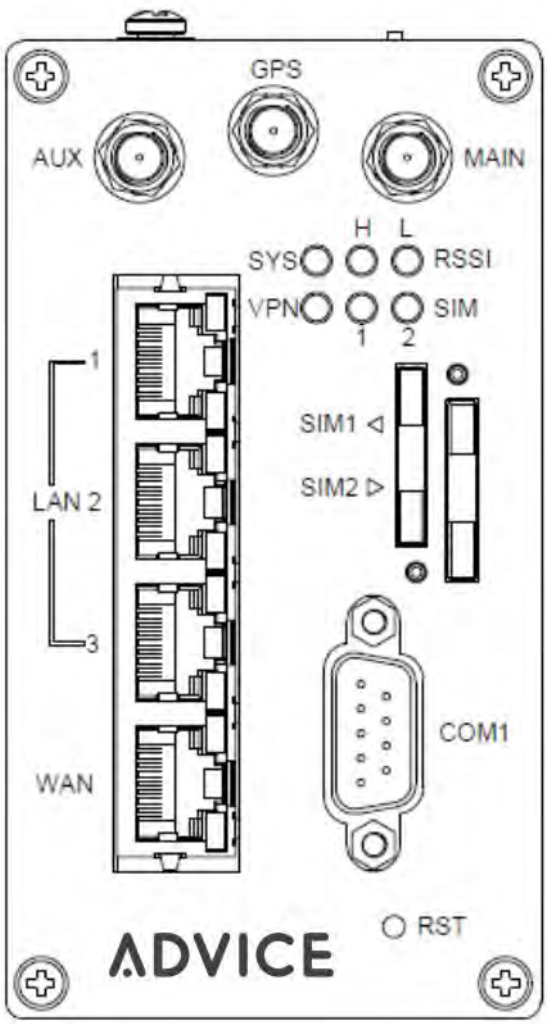
1.4 Hardware Panel Layout

This chapter describes the panel and interface layout of hardware.

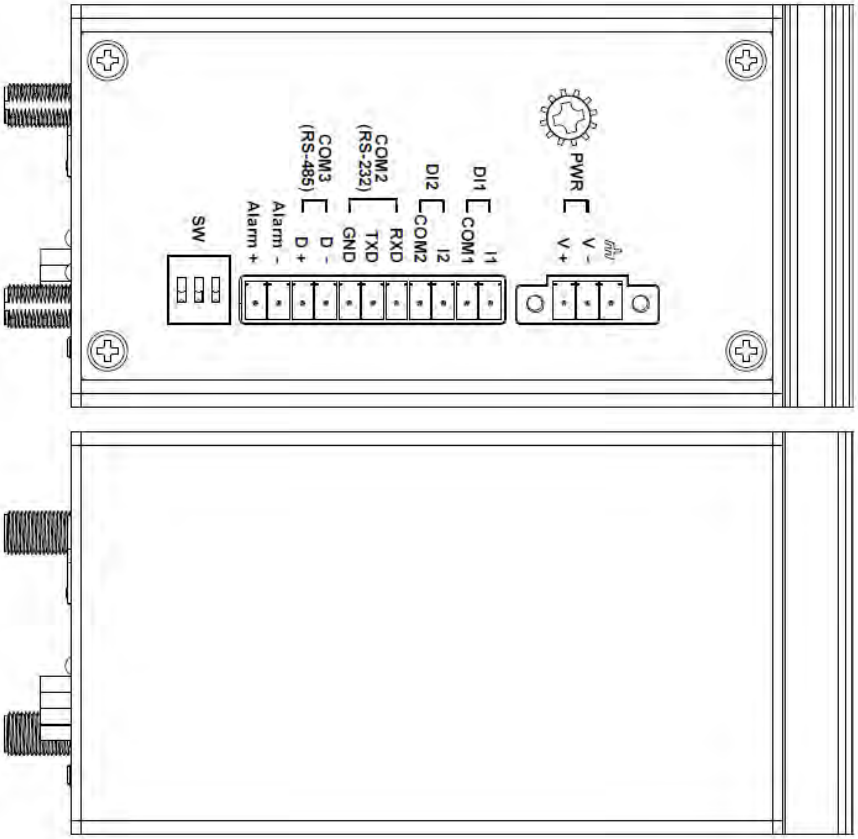
Model Name	Description
ICR100G-11	Industrial 4G LTE Cellular Router with GPS (1 x WAN + 3 x LAN + GPS)

[Front Panel View]

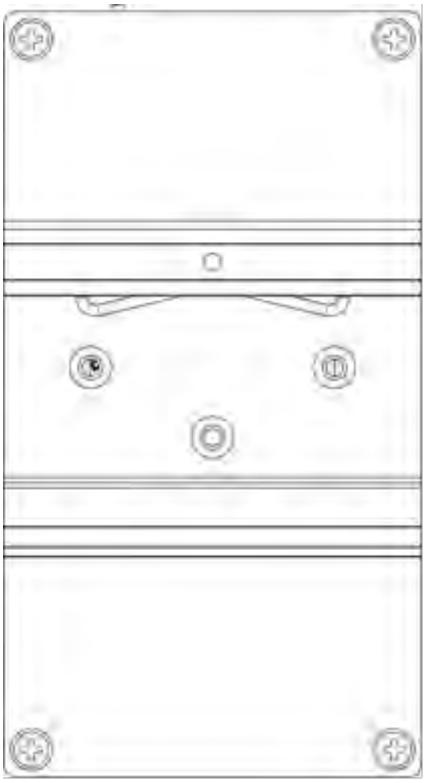
Model: ICR100G-11



[Top and Bottom View]

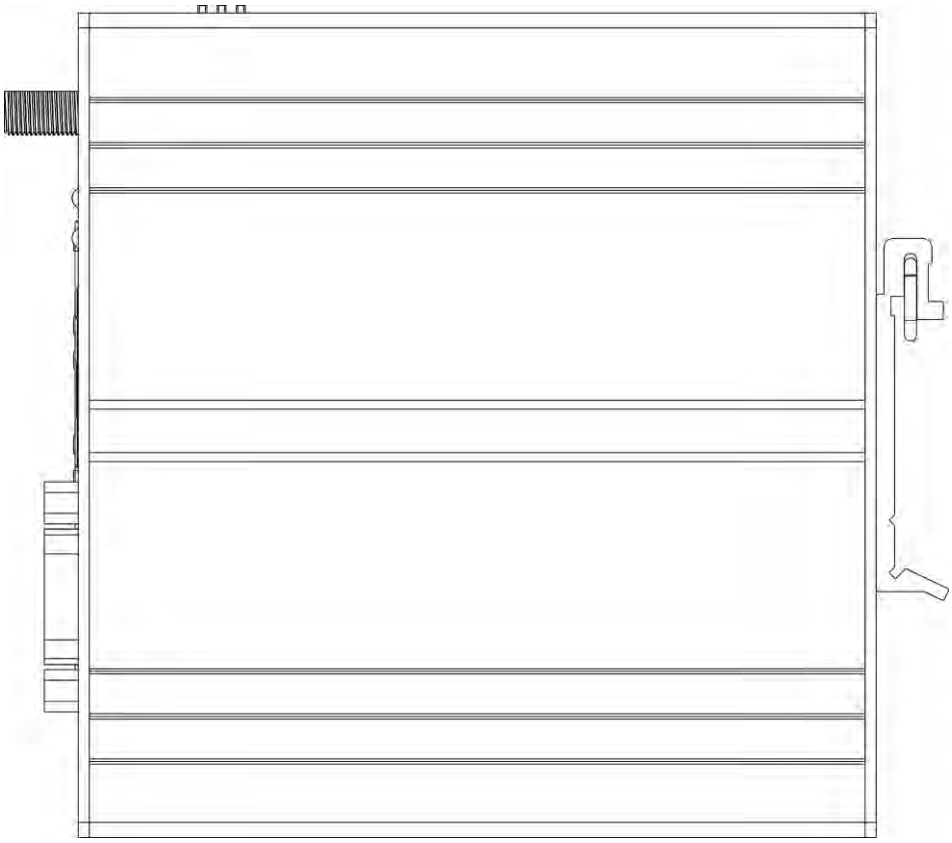


[Rear View]



[Left Side View]

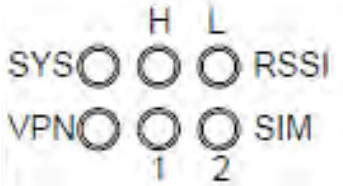
[Right Side View]



2 Hardware Installation

This chapter introduces how to install and connect the hardware.

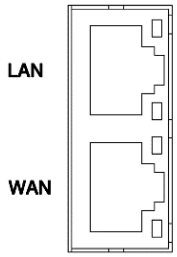
2.1 LED Indicators



LED	SYS	RSSI M~H	RSSI Low	VPN	SIM1	SIM2
ON	System UP	Normal Signal	Low Signal	VPN Connected	Connected	Connected
Slow Blinking	Booting	N/A	N/A	WAN Connected	Connecting	Connecting
Fast Blinking	N/A	N/A	N/A	N/A	Error	Error
OFF	Power Down	N/A	N/A	NO WAN Connection	Not Working	Not Working
Heart Beat	N/A	N/A	N/A	N/A	Reading	Reading

2.2 Ethernet Port

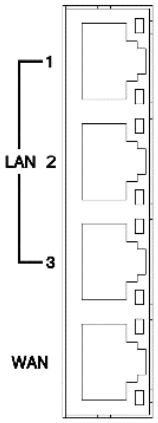
(1) 10/100 Mbps Ethernet WAN



The WAN interface is a standard RJ45 connector.

Pin	Description	Function
1	WAN TX+	10/100 Mbps WAN, TX+ Pin
2	WAN TX-	10/100 Mbps WAN, TX- Pin
3	WAN RX+	10/100 Mbps WAN, RX+ Pin
4	N/A	N/A
5	N/A	N/A
6	WAN RX-	10/100 Mbps WAN, RX- Pin
7	N/A	N/A
8	N/A	N/A

(2) 10/100 Mbps Ethernet LAN1~LAN3



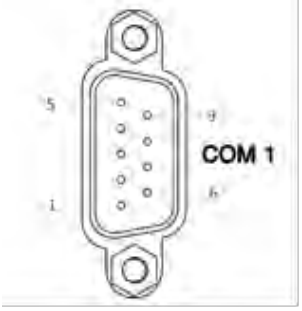
The Ethernet LAN1~3 interfaces are standard RJ45 connectors.

Pin	Description	Function
1	LAN TX+	10/100 Mbps LAN, TX+ Pin
2	LAN TX-	10/100 Mbps LAN, TX- Pin
3	LAN RX+	10/100 Mbps LAN, RX+ Pin
4	N/A	N/A
5	N/A	N/A
6	LAN RX-	10/100 Mbps LAN, RX- Pin
7	N/A	N/A
8	N/A	N/A

Each Ethernet port has two LED indicators.
The Green LED indicates Link/ACT, and the Yellow LED indicates Speed.

LED	Status	Description
Green (Link/ACT)	Off	Connection is down
	Blink	Data is being transmitted
	On	Connection is up
Yellow (Speed)	Off	10 Mbps Mode
	On	100 Mbps Mode

2.3 Serial Port COM1 (Console)

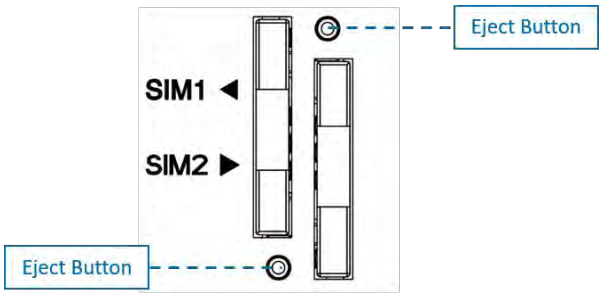


The serial port COM1 is a standard Sub-D connector.

Pin	Description	Direction
1	N/A	N/A
2	RXD	In
3	TXD	Out
4	N/A	N/A
5	GND	Ground
6	N/A	N/A
7	RTS	Out
8	CTS	In
9	N/A	N/A

2.4 Install the SIM Card

1. SIM1/SIM2 Card Drawers and Eject Buttons

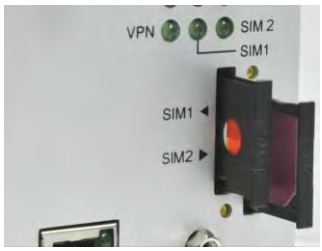


2. Insert and Remove SIM1/SIM2 Card

(1) Before inserting or removing the SIM card, ensure that the power has been turned off and the power connector has been removed from Cellular Router.

(2) Press the button with a paper clip or suitable tool to eject the SIM card from the drawer.

(3) Insert the SIM card with the contacts facing up and align it properly into the drawer. Make sure your direction of SIM Card and put it into the tray.
(4) Slide the drawer back and locks it in place.



Note:

- Please make sure the direction first. When pulling into the SIM tray without putting the correct direction, the tray will be stuck inside.
- Please turn off your router before taking the SIM card.

2.5 Reset Button

Reset button allows you to reboot the unit or restore to factory default setting.

Function	Operation
Reboot	Press the button for 1 second
Restore to factory default setting	Press the button for 5 seconds

Note:

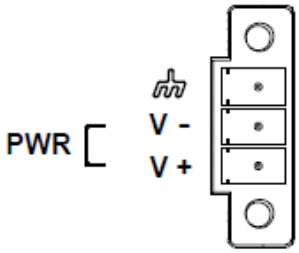
Press the Reset button and count the time around 5 seconds. The LED Indicators will be blinking to show you have activated the setting successfully.

2.6 External Antenna

Each unit has two antenna connectors (SMA), MAIN and AUX. Connect the antenna to MAIN when you have only one antenna. Please tighten the connecting nut properly to ensure good connection.

2.7 Connecting the Power Supply

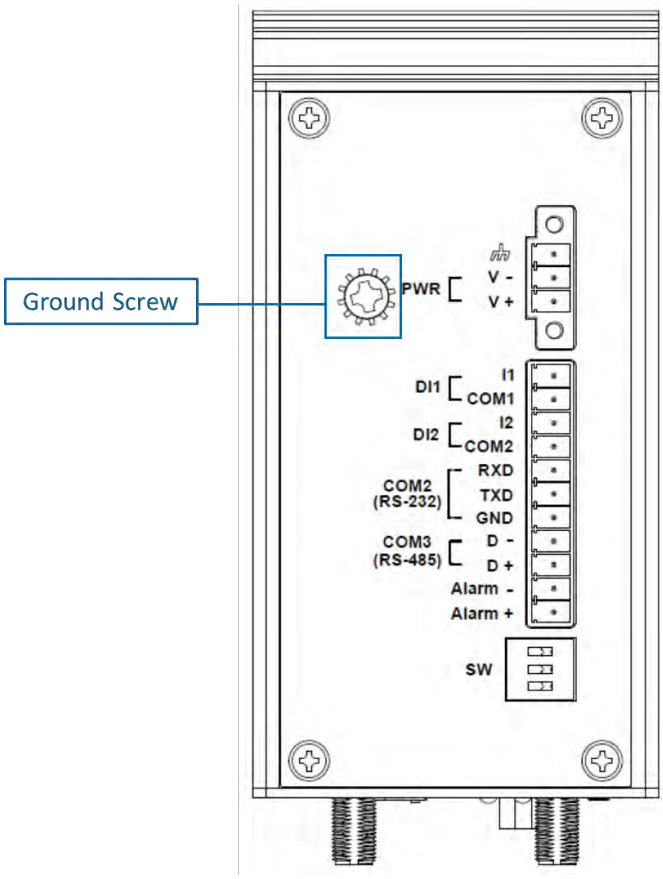
The router requires a DC power supply in the range of 10~32V DC. Please ensure all components are earthed to a common ground before connecting any wiring.



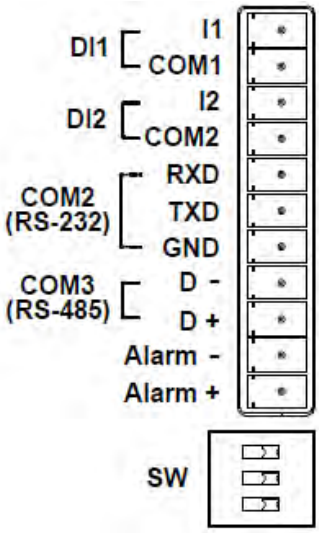
Pin	Power (10~32VDC)
⏚	FRAME GROUND
V -	Negative
V+	Positive

2.8 Grounding the Router

To prevent the noise and surge effect, please connect the router to the site ground wire by the ground screw before turning on the router.



2.9 Pin Assignments



DI1/DI2 / Alarm Contacts / COM2 (RS-232) / COM3 (RS-485)

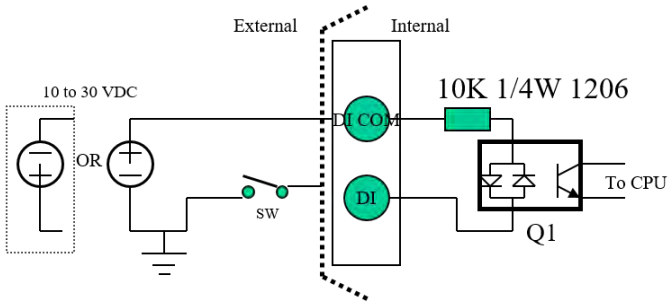
2.10 Connecting I/O Ports

(1) Digital Input DI1 & DI2

The unit has four terminals on the terminal block for the Digital inputs.

Pin	Description
DI1_I1	Digital INPUT 1
DI1_COM	Digital INPUT 1
DI2_I2	Digital INPUT 2
DI2_COM	Digital INPUT 2

Note: Q1 is a bidirectional component.



Wet Contact

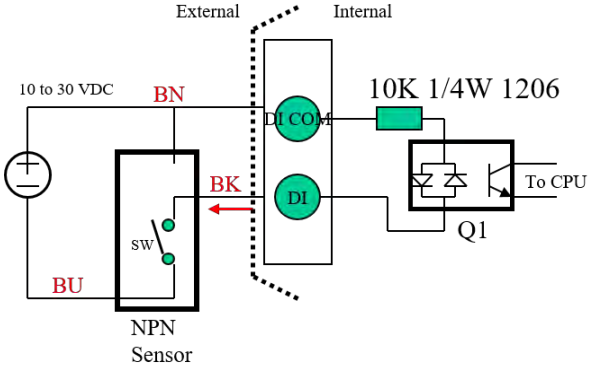
- Logic Level 1 : 10 to 30 VDC (Q1 On)
- Logic Level 0 : 0 to 3 VDC (Q1 Off)

Digital Input

- Wet Contact (Level from DI to DI COM)
  - Logic Level 1 : 10 to 30 VDC (Q1 on)
  - Logic Level 0 : 0 to 3 VDC (Q1 off)
- Wet Contact (Alarm trigger*):
  - Alarm ON* : Q1 On (SW Close)
  - Alarm Off* : Q1 off (SW Open)

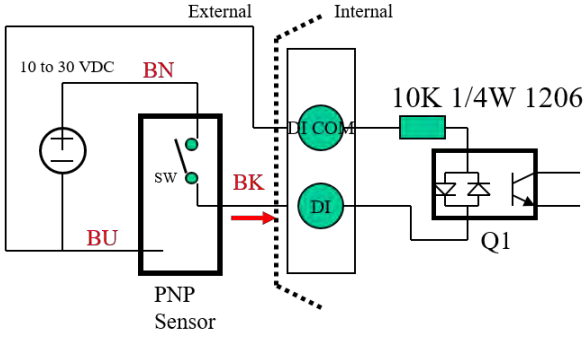
* Refer to the Alarm function on web management

* Q1 is bi-directional part



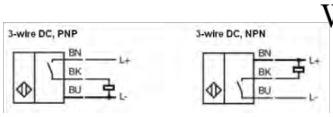
Wet Contact

- Alarm trigger* : Q1 turn on
- Alarm un-trigger* : Q1 turn off



Wet Contact

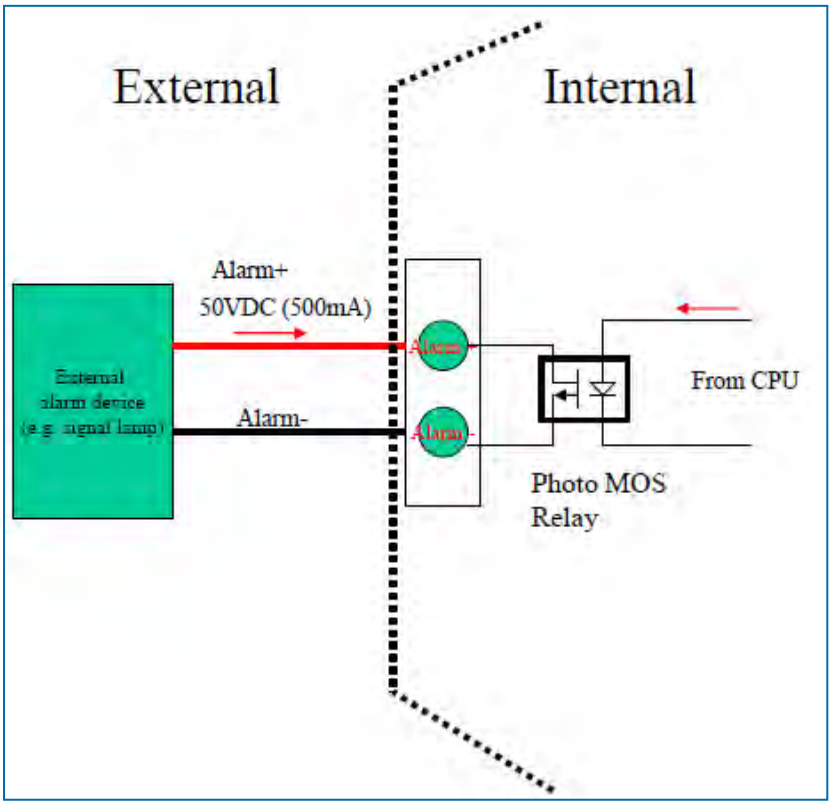
- Alarm trigger* : Q1 turn on
- Alarm un-trigger* : Q1 turn off



(2) Digital Output – Alarm Contacts

The unit has 2 terminals on the terminal block for the Alarm Contacts. Photo relay output with current capacity of 500mA/50VDC maximum.

Pin	Description
Alarm -	Alarm negative signal output
Alarm +	Alarm positive signal output



2.11 Serial Port COM2 (RS-232)

The serial port COM2 is a RS-232 interface.

Pin	Description
RXD	COM2 Serial Port, RXD Signal (INPUT)
TXD	COM2 Serial Port, TXD Signal (OUTPUT)
GND	COM2 Serial Port, Signal Ground (※)

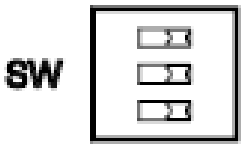
※ Both connectors (RS-232 and RS-485) have a common ground connection.

2.12 Serial Port COM3 (RS-485)

The serial port COM3 is a RS-485 interface.

Pin	Description
D -	COM3 Serial Port, Data- (B) wire
D +	COM3 Serial Port, Data+ (A) wire

2.13 DIP Switch



A built-in 120 ohm terminal resistor can be activated by DIP switch. Pull high or Pull low resistor adjustments are also available. It improves the communication on RS-485 networks for specific application.

DIP SWITCH

Switch 1 and 2 set the pull high/low resistor
Switch 3 enables or disables the termination resistor

Pull High (510 ohm) / Pull Low (510 ohm) Bias Resistor	SW 1 (Pull Low)	SW 2 (Pull High)
Enable	ON	ON
Disable (Default)	OFF	OFF

Termination Resistor (120 ohm)	SW 3
Enable	ON
Disable (Default)	OFF

3 Configuration via Web Browser

Access the Web Interface

The web configuration is an HTML-based management interface for quick and easy set up of the cellular router. Monitoring of the status, configuration and administration of the router can be done via the Web interface.

After properly connecting the hardware of cellular router as previously explained. Launch your web browser and enter http://192.168.1.1 as URL.

The default IP address and sub net-mask of the cellular router are 192.168.1.1 and 255.255.255.0. Because the cellular router acts as DHCP server in your network, the cellular router will automatically assign IP address for PC or NB in the network.

Control Panel > Selecting Language

You can choose the languages, including English and Taiwan.

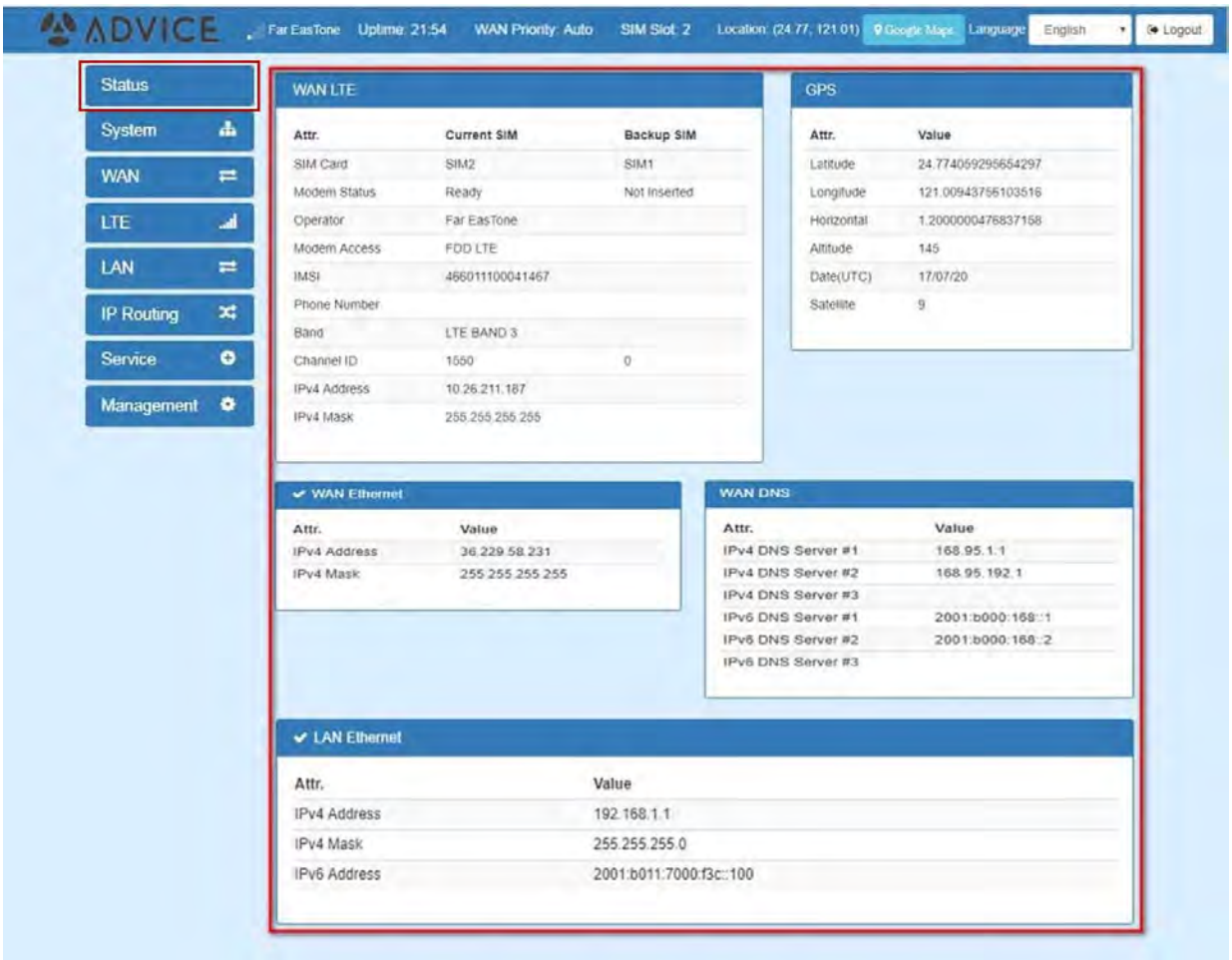
Logging in the Router

In this section, please fill in the default User Name **root** and the default Password **2wsx#EDC** and then click Login. For the system security, suggest changing them after configuration. After clicking, the interface shows Login ok.

Note: After changing the User Name and Password, strongly recommend you to save them because another time when you login, the User Name and Password have to be used the new one you changed.

4 Status

When you enter the web browser in the beginning, the interface displays the status of router to make you know about Cellular Attribute, Dual SIM information, the current connectivity of WAN Ethernet and LAN Ethernet. If you router with GPS function, the GPS interface is shown.



Status > WAN LTE	
Item	**Description**
Attribute	
SIM Card	Show the SIM card which the router work with currently: Current SIM or Backup SIM.
Modem Status	Show the status of modem.
Operator	Display the name of operator.
Modem Access	Show the router to access protocol type
IMSI	Show the IMSI number of the current SIM cards.
Phone Number	Show the phone number of the current SIM or Backup SIM.
Band	Show current connected Band.
Channel ID	Show current connected channel ID.
IPv4 Address	LTE obtain IPv4 address.

Status > WAN Ethernet	
Item	**Description**
Attribute	
IPv4 Address	Ethernet WAN obtain IPv4 Address.
IPv4 Mask	Ethernet WAN obtain IPv4 Mask.
IPv4 Mask	LTE IPv4 mask.

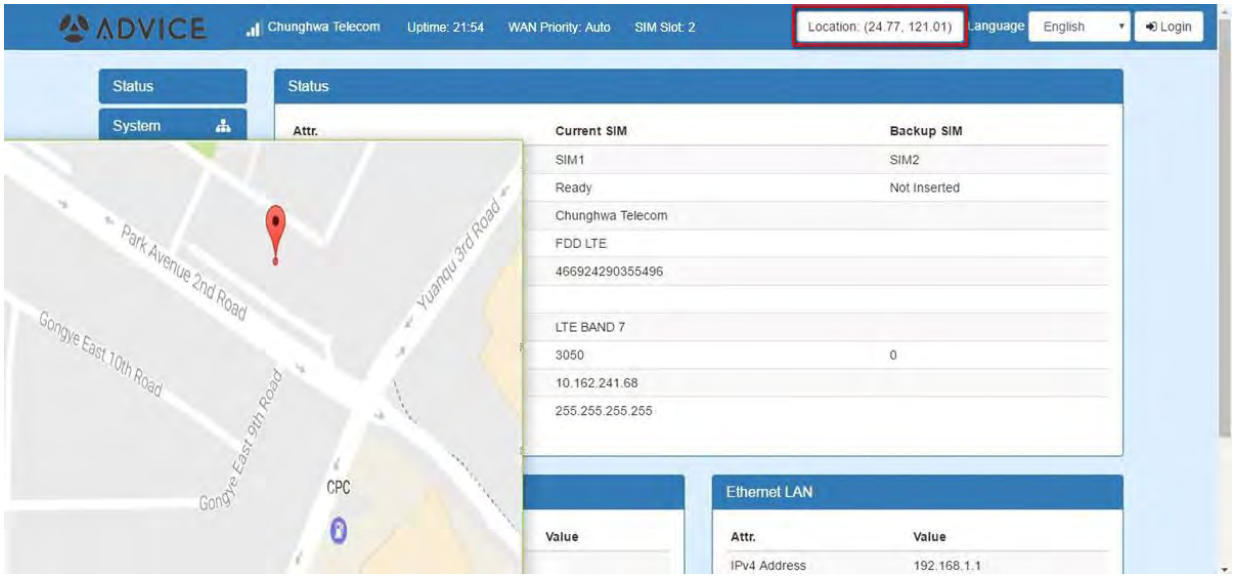
Status > LAN Ethernet	
Item	**Description**
Attribute	
IPv4 Address	Ethernet LAN is assigned IPv4 Address.
IPv4 Mask	Ethernet LAN is assigned IPv4 Mask.
IPv6 Address	Ethernet LAN is assigned IPv6 Address.

Status > WAN DNS	
Item	**Description**
Attribute	
IPv4 DNS Server #1	Show the address of IPv4 DNS Server #1.
IPv4 DNS Server #2	Show the address of IPv4 DNS Server #2.
IPv4 DNS Server #3	Show the address of IPv4 DNS Server #3.
IPv6 DNS Server #1	Show the address of IPv6 DNS Server #1.
IPv6 DNS Server #2	Show the address of IPv6 DNS Server #2.
IPv6 DNS Server #3	Show the address of IPv6 DNS Server #3.

Status > GPS	
Item	**Description**
Attribute	
Latitude	Show the latitude information of location.
Longitude	Show the longitude information of location.
Horizontal	Show the horizontal information of location.
Altitude	Show the altitude information of location.
Date(UTC)	Show the date information of location.
Satellite	Show the satellite information of location.

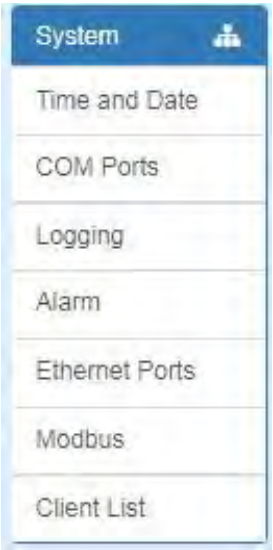
4.1 Status > GPS

For those GPS enabled router, you can see Location on the right-top banner of web interface when connecting your GPS function. After clicking this banner, a map will automatically display the current information of map according to location of router.


ADVICE
Chunghwa Telecom
Uptime: 21:54
WAN Priority: Auto
SIM Slot: 2
Location: (24.77, 121.01)
Language
English
Login
Status
System
Status
Attr.
Current SIM
Backup SIM
SIM1
SIM2
Ready
Not Inserted
Chunghwa Telecom
FDD LTE
466924290355496
LTE BAND 7
3050
0
10.162.241.68
255.255.255.255
Park Avenue 2nd Road
Yuanqu 3rd Road
Gongye East 10th Road
Gongye East 9th Road
CPC
Value
Ethernet LAN
Attr.
Value
IPv4 Address
192.168.1.1

5 Configuration > System

This system section provides you to configure the following items, including Time and Date, COM Ports, Logging, Alarm, Ethernet Ports, Modbus Static Route, RIP and GPS Config.



5.1 System > Time and Date

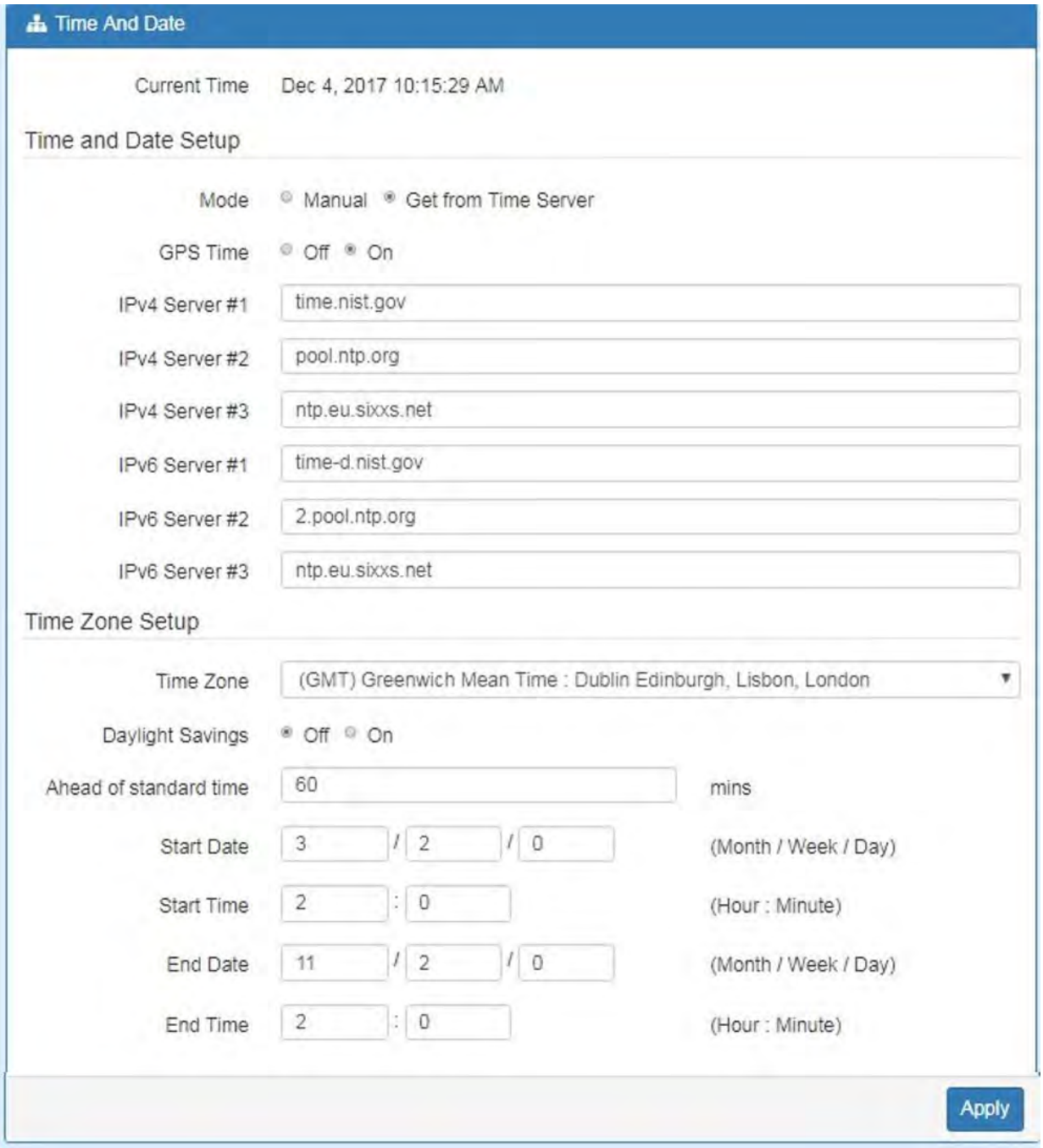
This section allows you to set up the time and date of router and NTP server. There are two modes at Time and Date Setup, including **Get from Time Server** and **Manual**. The default mode is **Get from Time Server**.

If the router has GPS function, you can turn on "**GPS Time**" for sync time from GPS server.

For **Time Zone Setup**, the **Daylight Savings Time** allows the device to forward/backward the amount of time from **Ahead of standard time** setting automatically when the time is at the **Daylight Savings** duration that you have set up before.

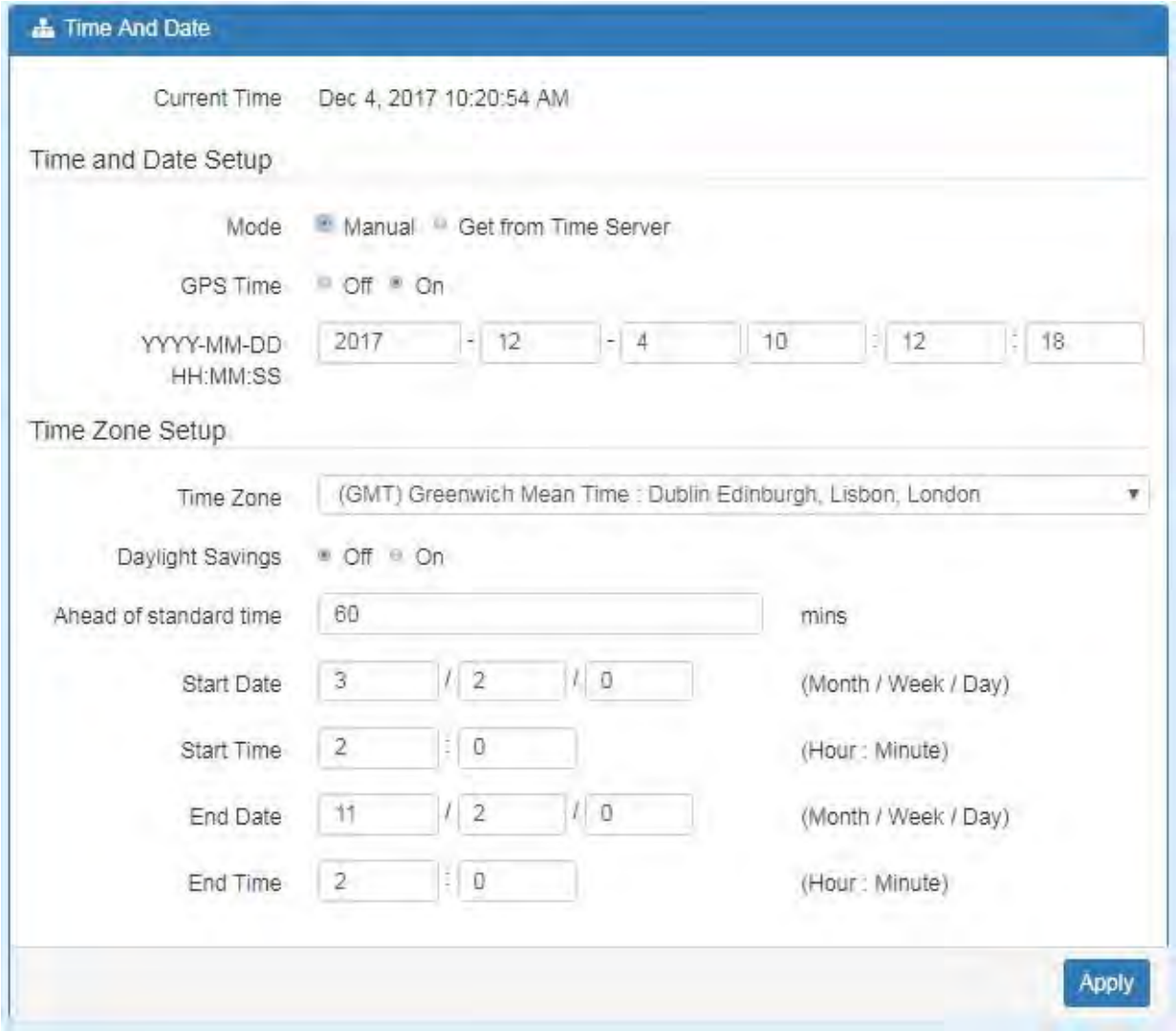
I. Get from Time Server

- Set up the time servers of IPv4 and IPv6.
- Select your local time zone.
- Click Apply to keep your configuration settings.



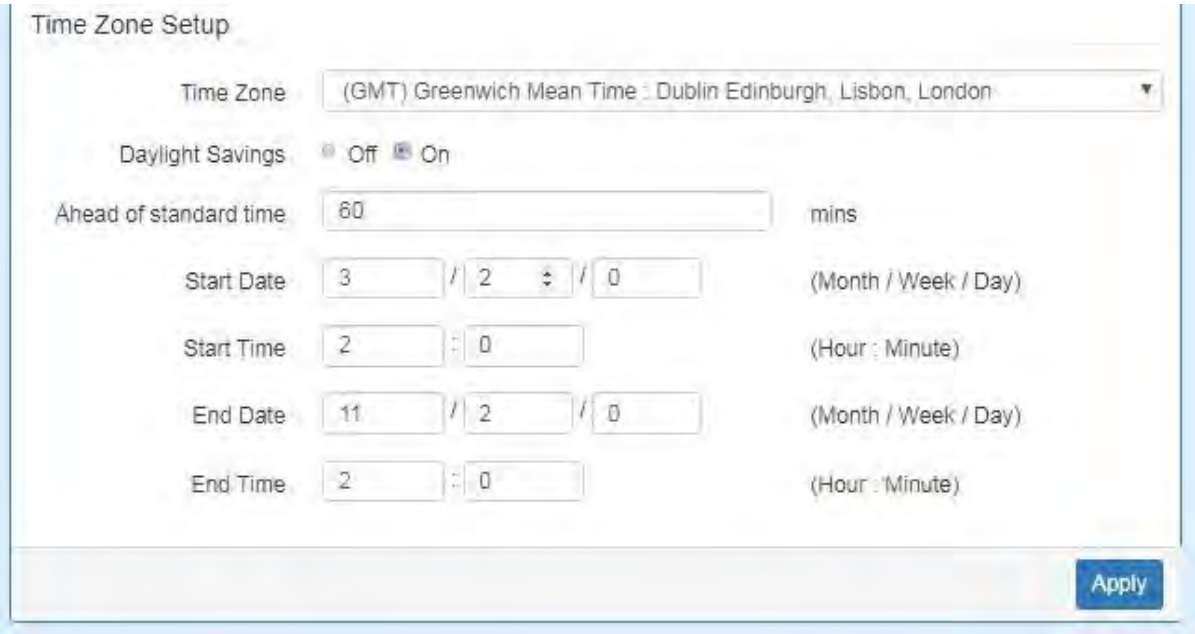
II. Manual

- Set up the information of time and date, including year, month, date, and hour, minute, and second.
- Set up your local time zone.
- Click Apply to submit your configuration changes.



III. Time Zone Setup

- Set up **Daylight Savings** as On.
- Set up **Ahead of standard time.**
- Set up the information of Start Date/Time, including Month, Week, Day, Hour and Minute.
- Set up the information of End Date/Time, including Month, Week, Day, Hour and Minute.
- Click Apply to submit your configuration changes.


Time Zone Setup
Time Zone
(GMT) Greenwich Mean Time : Dublin Edinburgh, Lisbon, London
Daylight Savings
Off
On
Ahead of standard time
60
mins
Start Date
3
2
0
(Month / Week / Day)
Start Time
2
0
(Hour : Minute)
End Date
11
2
0
(Month / Week / Day)
End Time
2
0
(Hour : Minute)
Apply

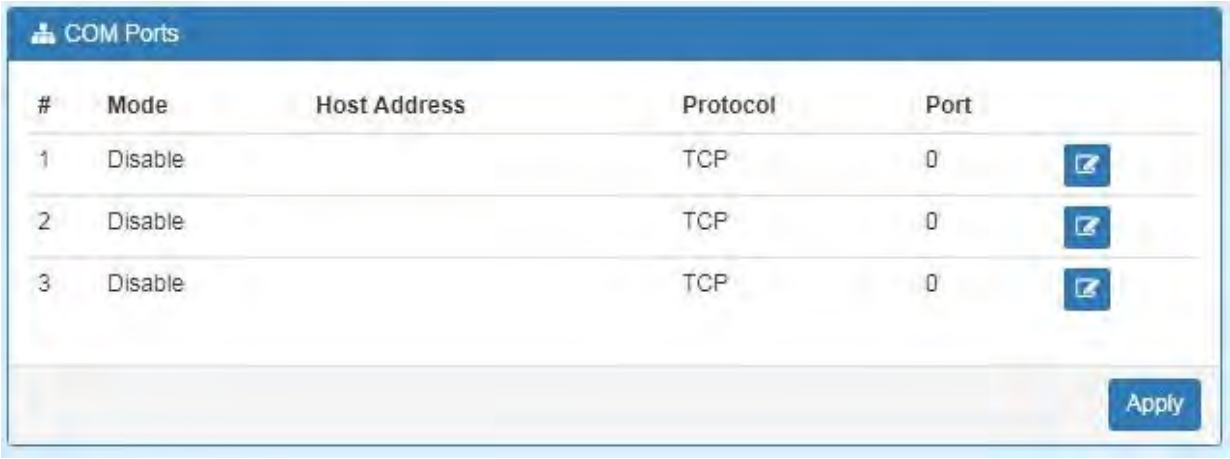
System > Time and Date->Daylight Savings	
Item	**Description**
Daylight Saving	Turn on/off the Daylight Savings feature. Select from Off or On. The default is Off.
Ahead of standard time	The forward/backward minutes when enter/leave Daylight Savings duration.Default is 60 mins.
Start Date/Start Time	Time to enter Daylight Savings duration. The Month range is 1~12; 1- Jan. 2 - Feb. 3 - Mar. 4 - Apr. 5 - May 6 - Jun. 7 - Jul. 8 - Aug. 9 - Sep. 10 - Oct. 11 - Nov. 12 - Dec. The Week range is 1~5; 1 - first week in month. 2 - second week in month 3 - third week in month 4 - fourth week in month 5 - fifth week in month The Day range is 0~6; 0 - Sunday(The start day of a week) 1- Monday 2 - Tuesday 3 - Wednesday 4 - Thursday 5 - Friday 6 - Saturday The Hour range is 0~23; The Min range is 0~59;
End Date/End Time	Time to leave Daylight Savings duration. Same with Start Date/Start Time.

5.2 System > COM Ports

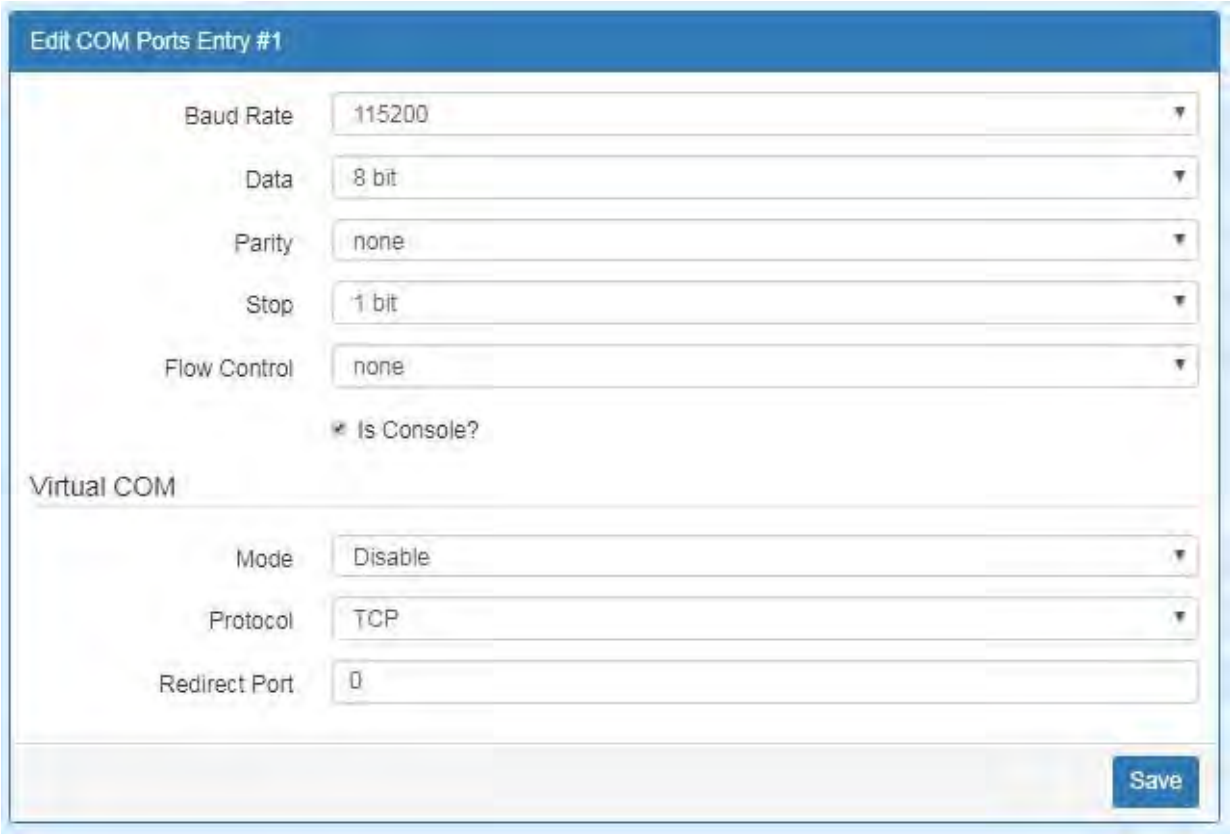
This section provides you to configure the COM port settings and remotely manage the device through the virtual COM setting. For the remote management, the managed device should be connected to the cellular router by serial interface either RS232 or RS485.

***Note*:** The COM 1 and COM 2 are RS232 interface, and the COM 3 is RS485 interface.

(1) The default is Disable. You can click edit button to configure your settings.



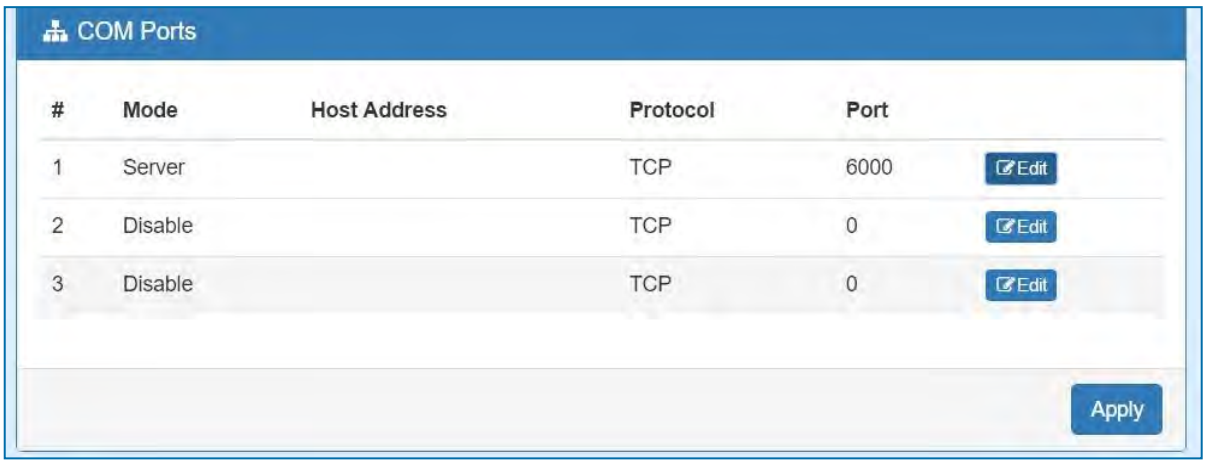
(2) Set up the configuration and Virtual COM. After configuring, click Save to confirm your settings.



(3) The console is the command-line interface (CLI) management option for cellular router. You can assign the COM port to be a management port by this option.

Note: We suggest to enable at least 1 COM port as your console port and the default console port is COM 1.

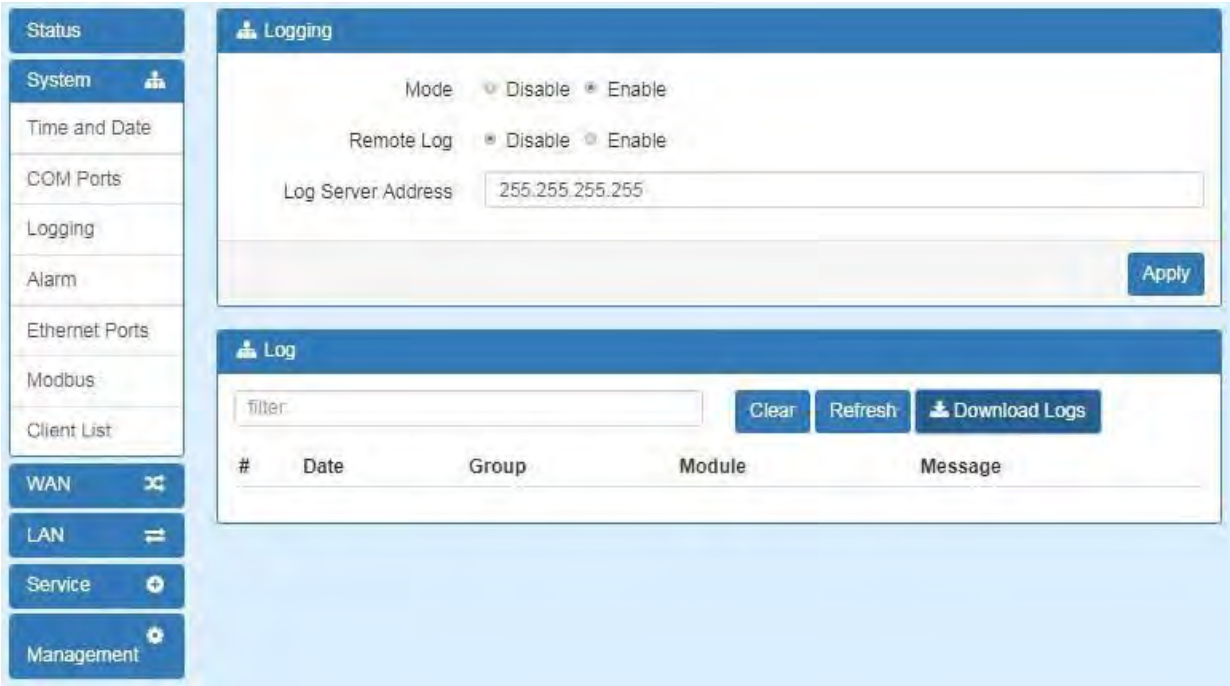
(4) The interface shows the setting information and click Apply to configure.



System > COM Ports	
Item	**Description**
Edit Configuration	
Baud Rate	Select from the current Baud Rate.
Data	Select from 7 bit or 8 bit.
Parity	Select from the information of Parity.
Stop	Select from 1 bit or 2 bit.
Flow Control	Select from none, Xon/Xoff or hardware.
Virtual COM	
Mode	Select from Disable, Server or Client.
Protocol	Select from TCP or UDP.
Host Address	The host address is only available on client mode. Specify what the domain name or IP address (IPv4 or IPv6) to be connected.
Redirect Port	● Server Mode: This network package of cellular router is on this port. ● Client Mode: The network package of remote device is on the remote host.

5.3 System > Logging

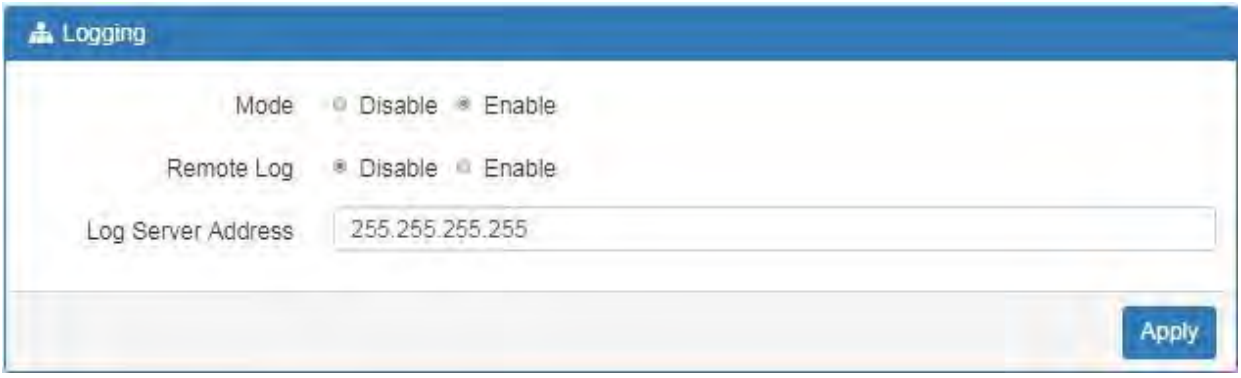
This section allows cellular router to record the data and display the status of data.



5.3.1 Logging > Logging

(1) Logging section provides you to control all logging records.

(2) Users need to select Apply to confirm your settings.



System > Logging > Logging	
Item	**Description**
Mode	Turn on/off the logging configuration. Select from Disable or Enable. The default is Enable.
Remote Log	The logging messages send to remote log or not. Select from Disable or Enable. The default is Disable.
Log Server Address	When you choose “Enable” on Remote Log, you should input IP address to save and receive all logging data. (***Note:*** This server should have installed Log software.)

5.3.2 Logging > Log

This section displays all data status.

(1) You can choose Filter function to quickly search for your data.

(2) When you click Clear, all of the data that displays on the interface will be totally cleared without any backup.

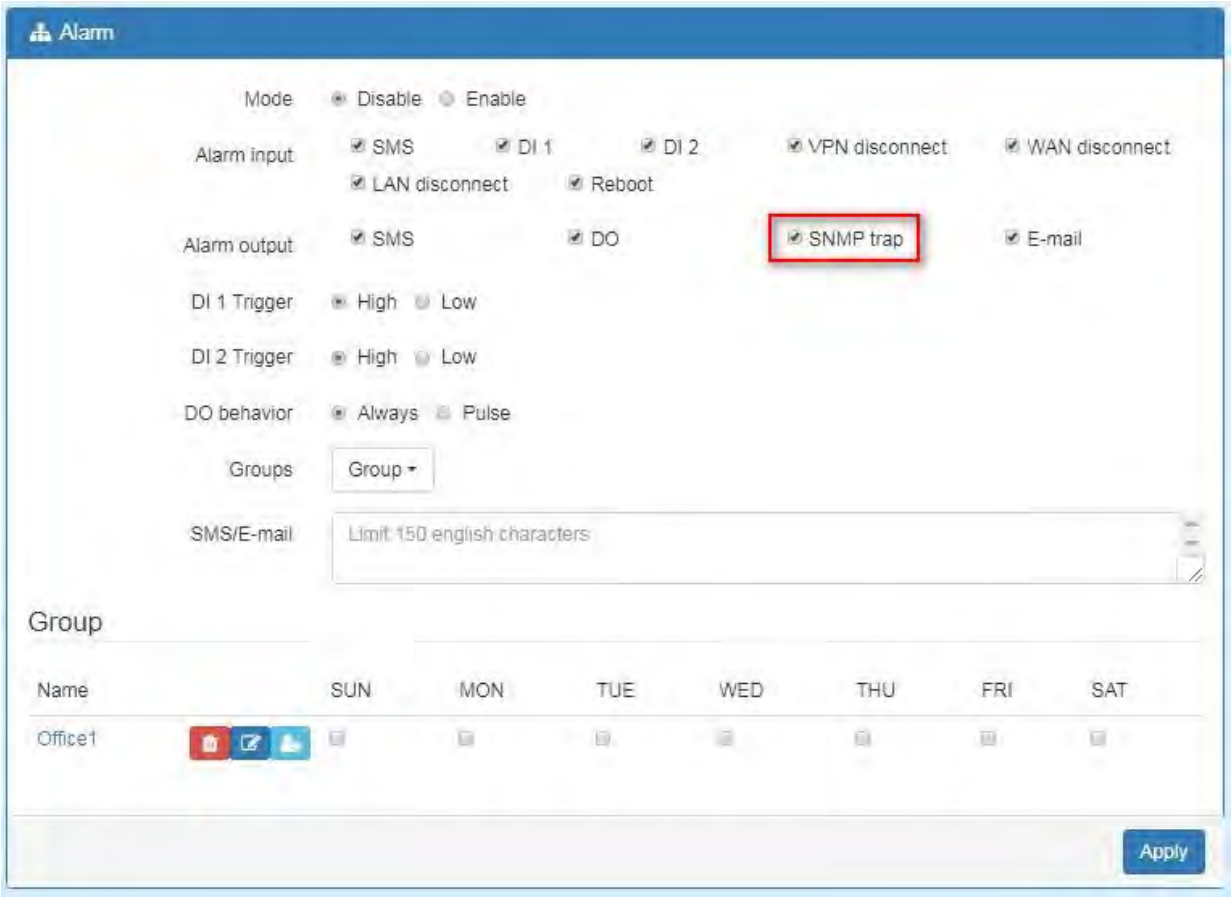
(3) When you click Refresh, the system will update and display the latest data from your cellular router.

(4) When you click Download Logs, the system will download the latest data from your cellular router.

System > Logging > Log	
Item	**Description**
Filter	Filter the required data quickly.
Date	Show the date of log for each logging data.
Group	Show the group of software functions.
Module	Show the module of group of software functions.
Message	Show the messages for each logging data.

5.4 System > Alarm

This section allows you to configure the alarm.

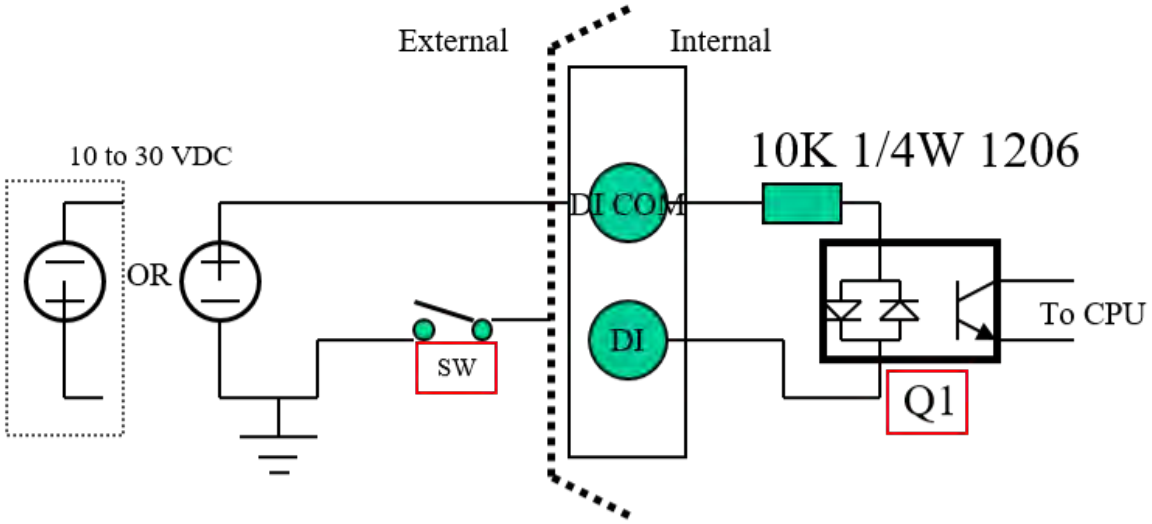


Note:

(1) If you select SNMP trap in Alarm output, you need to set up SNMP trap configuration from Service SNMP.

(2) DI trigger "High" means High Trigger. (SW is On to trigger;SW is OFF in Normal state.)

(3) DI trigger "Low" means Low Trigger. (SW is OFF to trigger;SW is ON in Normal state.)

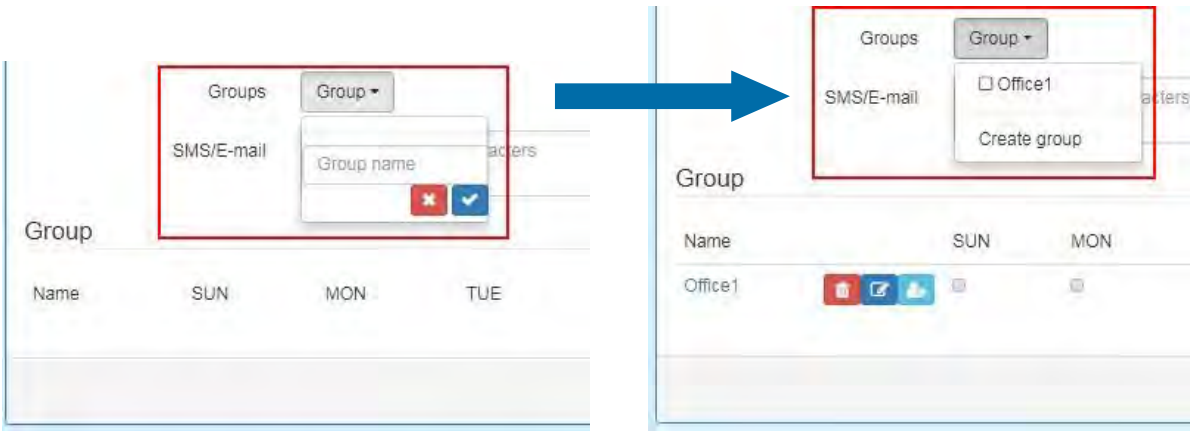


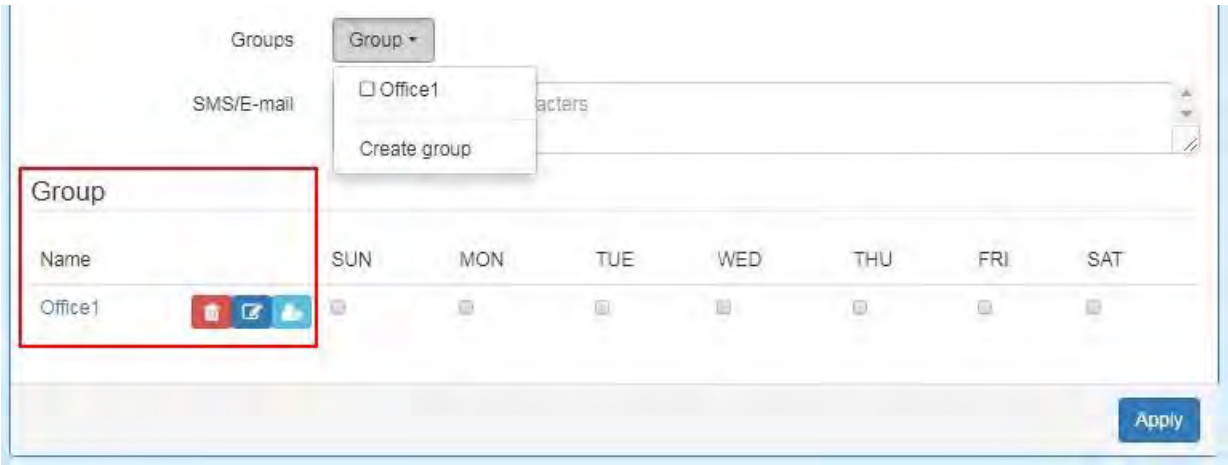
System > Alarm	
Item	**Description**
Mode	Turn on/off the Alarm configuration. Select from Disable or Enable. The default is Enable.
Alarm Input	Select from SMS, DI 1, DI 2, VPN disconnect and WAN disconnect as input to trigger alarm. ● **SMS:** It means team members on selected week day can send SMS to the phone number of using SIM card to trigger alarm. ● **DI 1/2:** IO high to trigger alarm. ● **VPN disconnect:** All tunnels get disconnected then trigger alarm. ● **WAN disconnect:** All WAN connections get disconnected then trigger alarm.
Alarm Output	Select from SMS, DO, SNMP trap and E-mail as alarm output.
DI 1 Trigger	Select from High or Low. The default is High Trigger. ● **High:** SW is On to trigger. ● **Low:** SW is OFF to trigge.
D1 2 Trigger	Select from High or Low. The default is High Trigger.
DO behavior	● **Always:** Pull DO high. ● **Pulse:** High and Low continuously.
Groups	Create your contact phone book for each group and edit your information for each user.
SMS/E-mail	Write your messages and the messages limit 150 English characters to deliver.

5.4.1 Alarm > Name Group

(1) How to create your group

- Name a group： Click **Group** for naming and the interface will show the group's name in the Group setting as below.

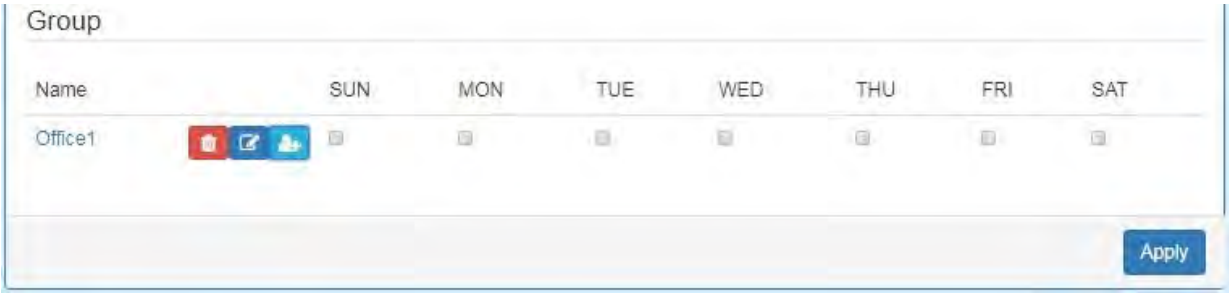




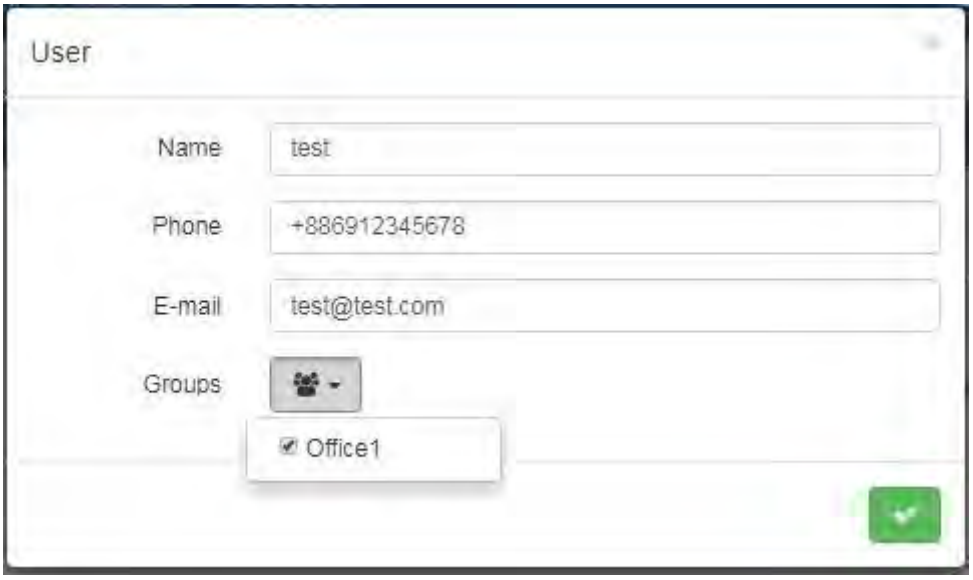
5.4.2 Alarm > Edit User

(2) How to edit each user's information in every group

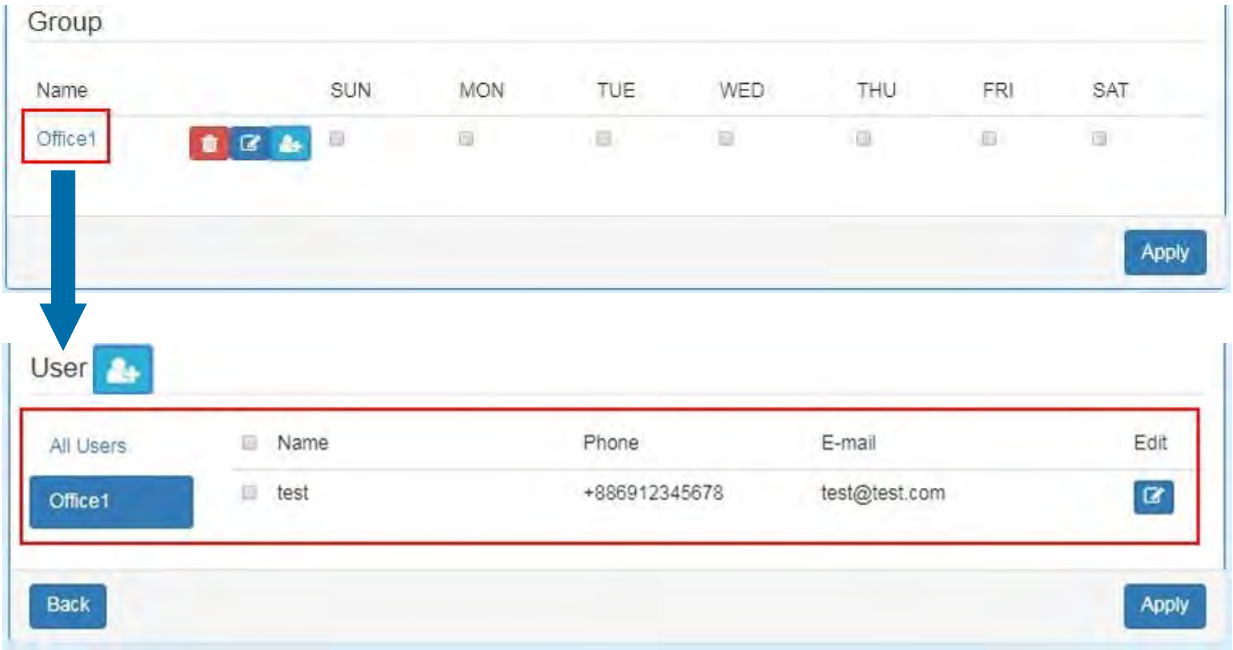
- Select your naming group and click  Add button to edit your user's information, including Name, Phone and E-mail.



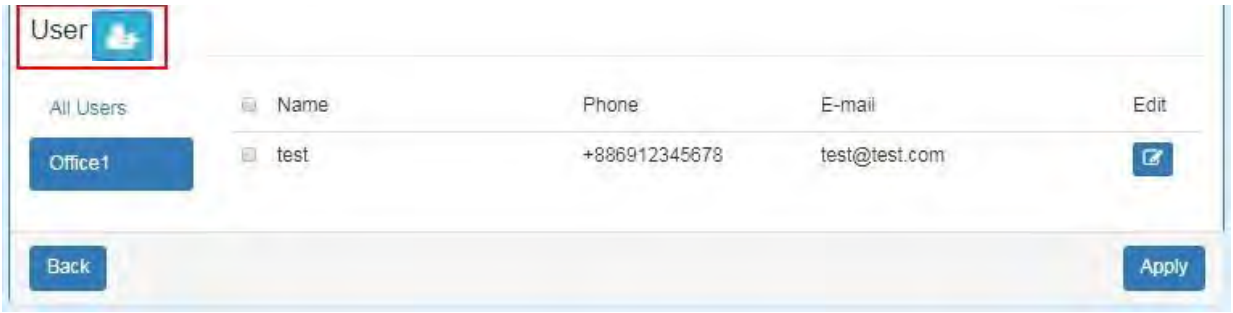
- After filling in your information for each row, chose your naming group and click  to submit your settings.



- After submitting your setting, the interface returns to Group window setting. Please click your naming group to show the user's information that you have edited.

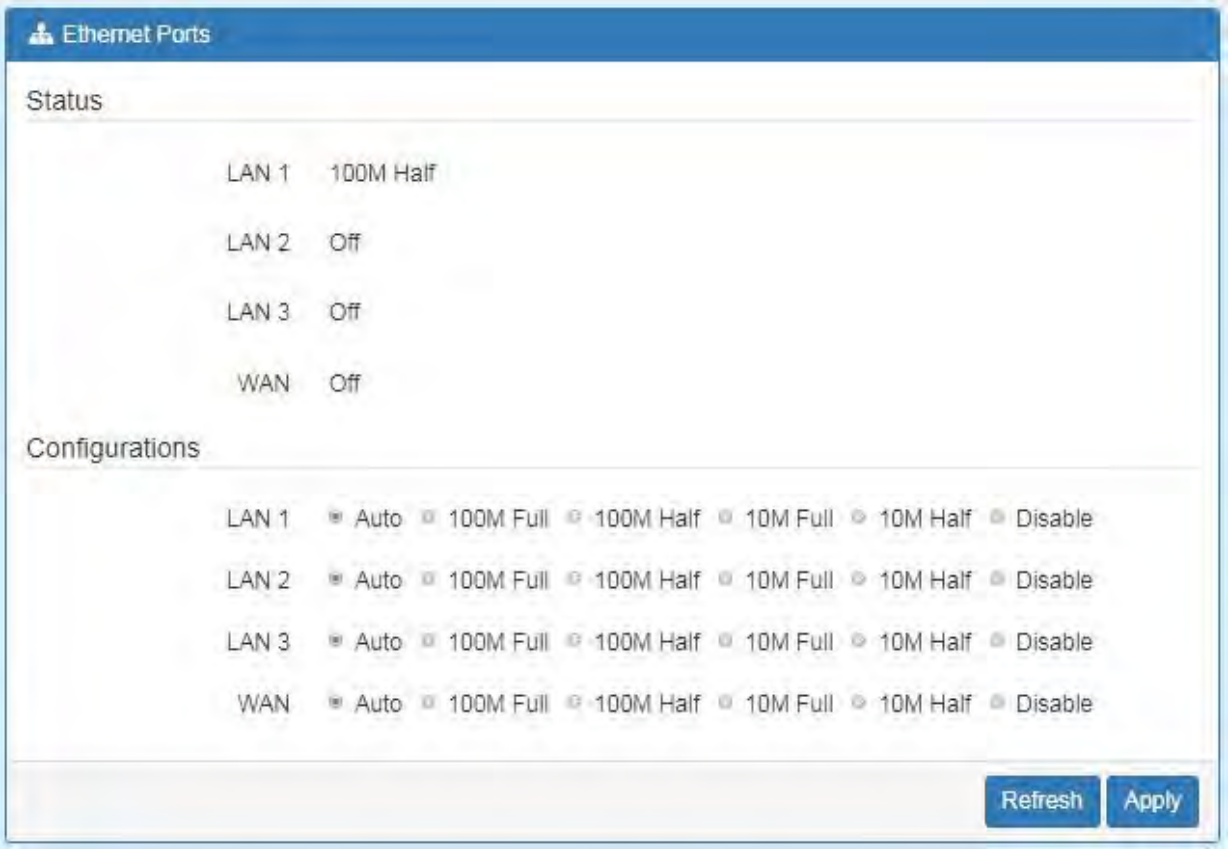


- You can click button to add the new user's information.



5.5 System > Ethernet Ports

This section allows you to configure the Ethernet Ports.

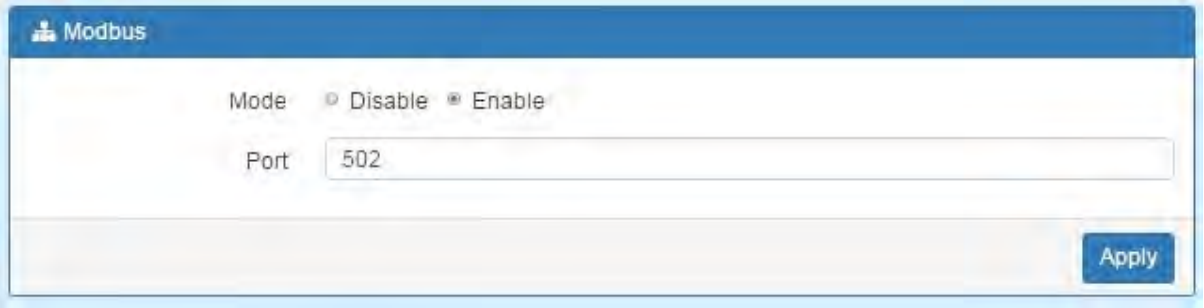


System > Ethernet Ports	
Item	**Description**
Status	Show the connectivity status of LAN and WAN.
Configurations	Select from Auto, 100M Full, 100M Half, 10M Full, 10M Half and Disable.

5.6 System > Modbus

This section allows you to configure the Modbus.

Note: This configuration is for Modbus TCP and the function is only for COM 3 (RS485).

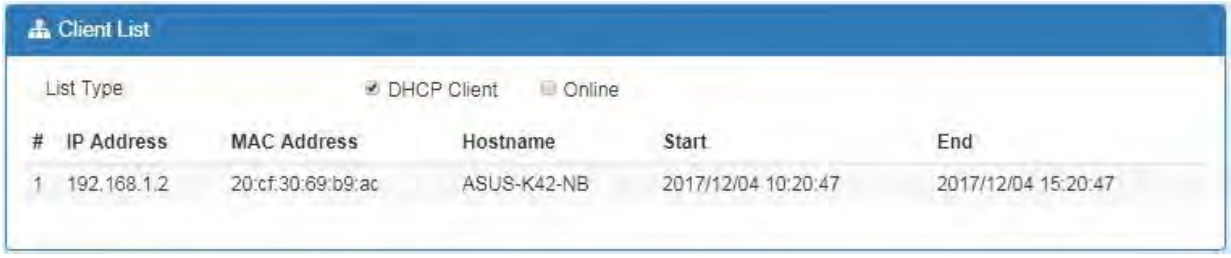


System > Modbus	
Item	**Description**
Mode	Select from Disable or Enable.
Port	The listening port of Modbus TCP.

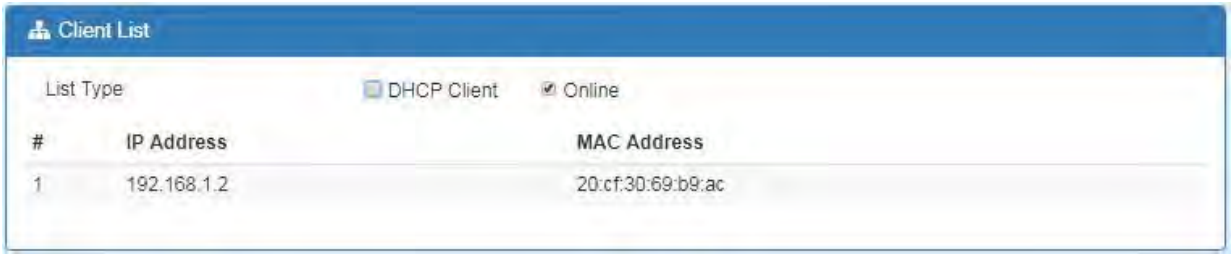
5.7 System > Client List

This section allows you to understand how many devices have been connected and their status from the router. There are two types, one is **DHCP Client** and the other is **Online**. The default is both types to show all status when the router is on DHCP Client and Online.

For **DHCP Client** type, the information shows IP address, MAC address, Hostname and the expiry time of IP (Start/End).



For **Online** type, the information shows IP address and MAC address when the client is online.



System > Client List	
Item	**Description**
List Type	• **DHCP Client:** List all clients' information when it is via DHCP. • **Online:** List the information when it is online.

6 Configuration > WAN

This section allows you to configure WAN, including Priority, LTE Config, Dual SIM, Ethernet and DNS.

6.1 WAN > Priority

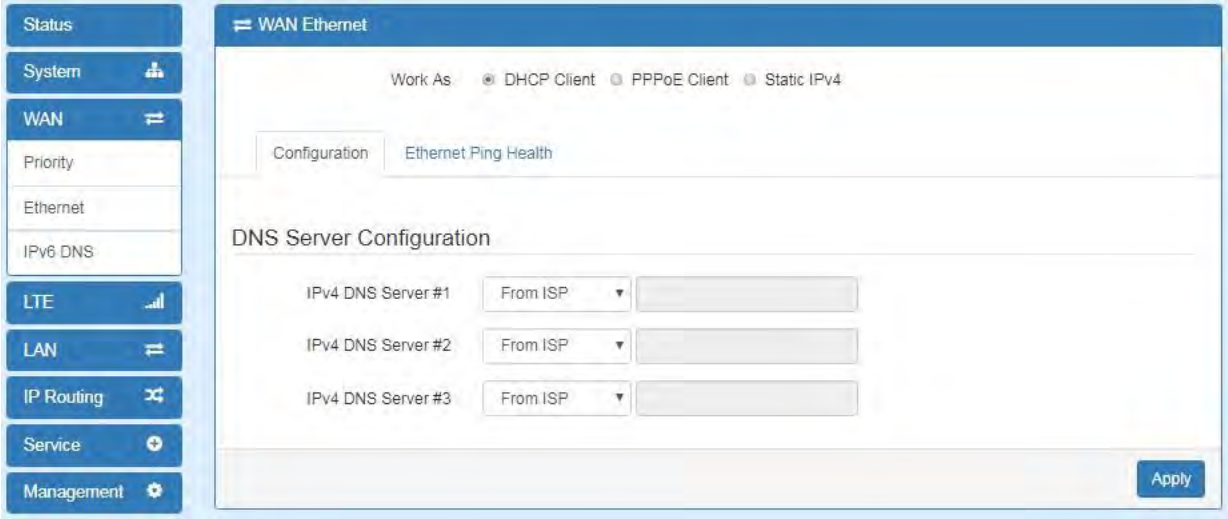
You can set up the priority of WAN.

WAN > Priority	
Item	**Description**
Priority	• Auto: WAN Ethernet is first priority and second priority is LTE. The default is Auto. • LTE Only: The priority is only LTE. • ETH Only: The priority is only Ethernet.

6.2 WAN > Ethernet

6.2.1 WAN Ethernet Configuration

This section provides three options, including **DHCP Client**, **PPPoE Client** and **Static IPv4.** The default is DHCP Client.

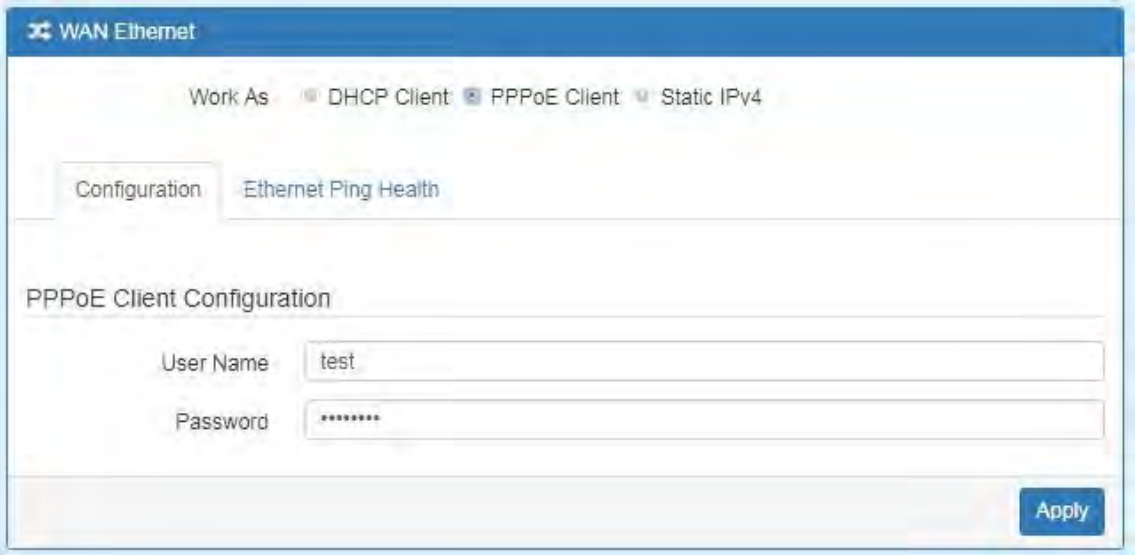


WAN > Ethernet	
Item	**Description**
WAN Ethernet	There are three options to obtain the IP of WAN Ethernet. ● **DHCP Client:** DHCP server-assigned IP address, netmask, gateway, and DNS. ● **PPPoE Client:** Your ISP will provide you with a username and password. This option is typically used for DSL services. ● **Static IPv4:** User-defined IP address, netmask, and gateway address.

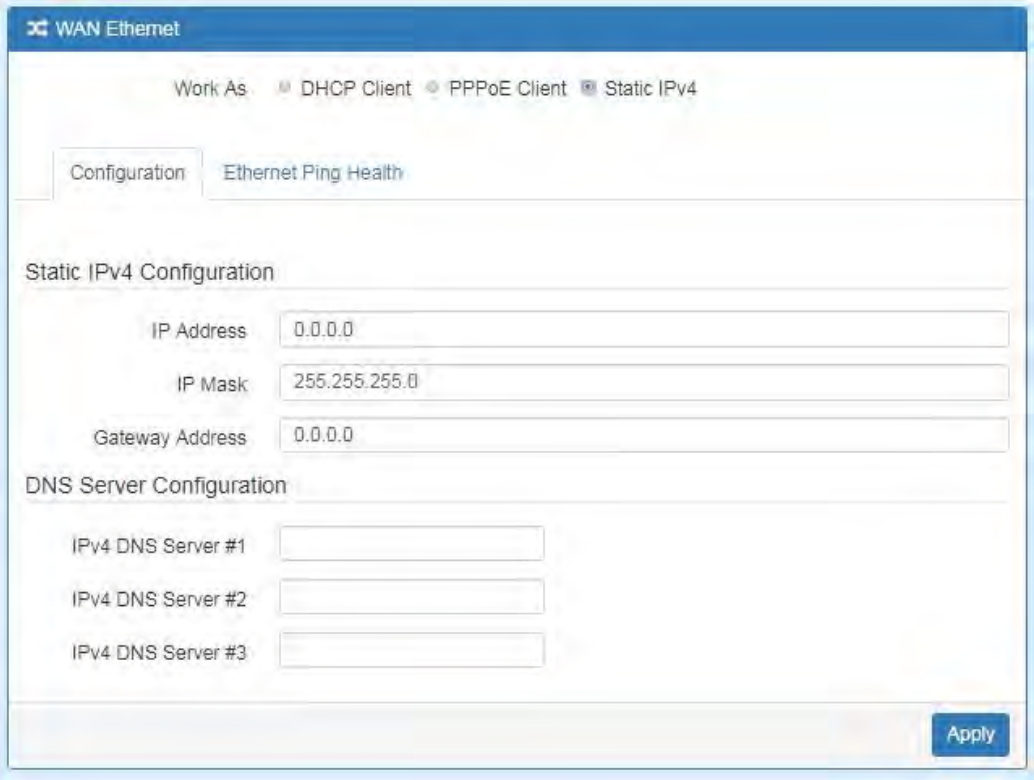
When selecting "**DHCP Client"**, you can set up DNS Server Configuration.
For IPv4 DNS Server, it provides three options to set up and each option has provided with "From ISP", "User Defined" and "None" to configure.

WAN > Ethernet	
Item	**Description**
IPv4 DNS Server #1 **IPv4 DNS Server #2** **IPv4 DNS Server #3**	● Each setting DNS Server has three options, including From ISP, User Defined and None. ● When you select From ISP, the IPv4 DNS server IP is obtained from ISP. ● When you select User Defined, the IPv4 DNS server IP is input by user.

When you select **PPPoE Client**, the interface shows the item of configuration to fill in your User Name and Password.



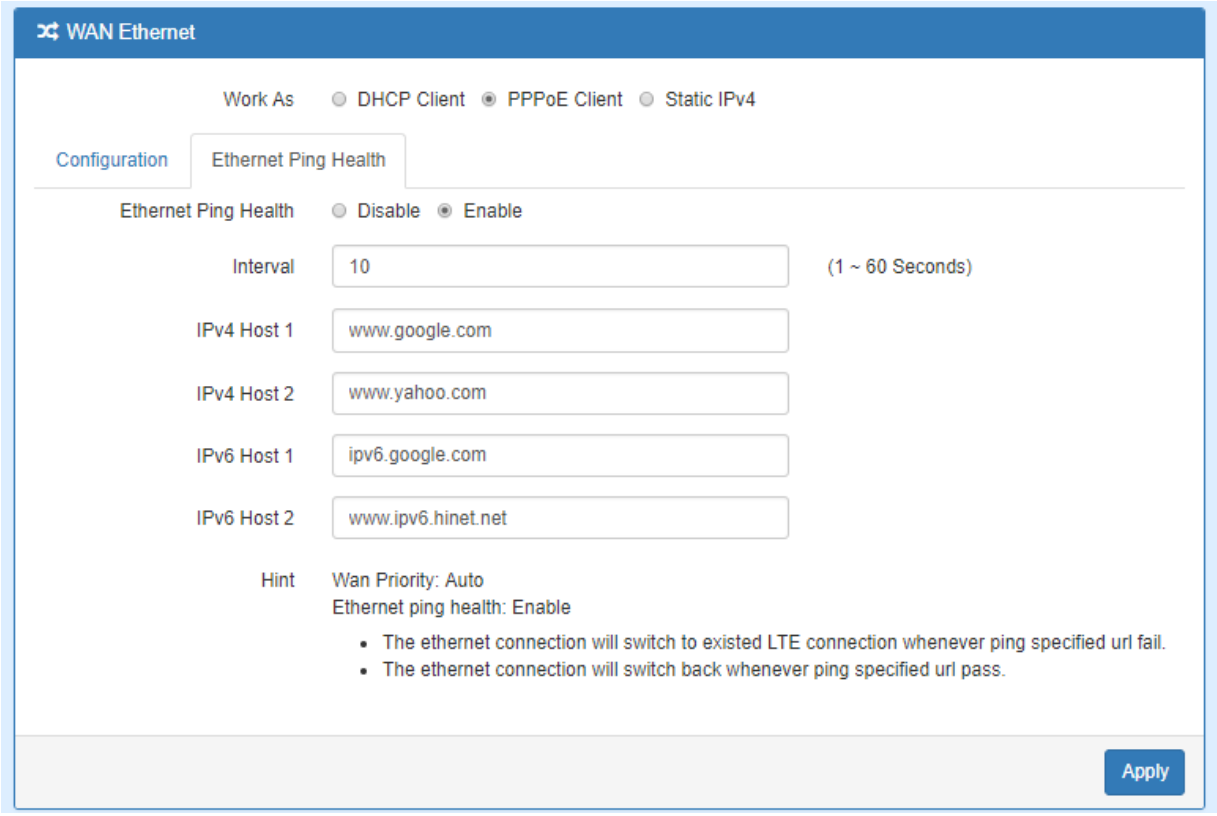
When you select **Static IPv4**, the interface shows the information of configuration, including IP Address, IP Mask and Gateway Address.



WAN > Ethernet	
Item	**Description**
Static IPv4 Configuration	
IP Address	Fill in the IP Address.
IP Mask	Fill in the IP Mask.
Gateway Address	Fill in Gateway Address.
DNS Server Configuration	
IPv4 DNS Server #1 **IPv4 DNS Server #2** **IPv4 DNS Server #3**	The IPv4 DNS server IP is input by user.

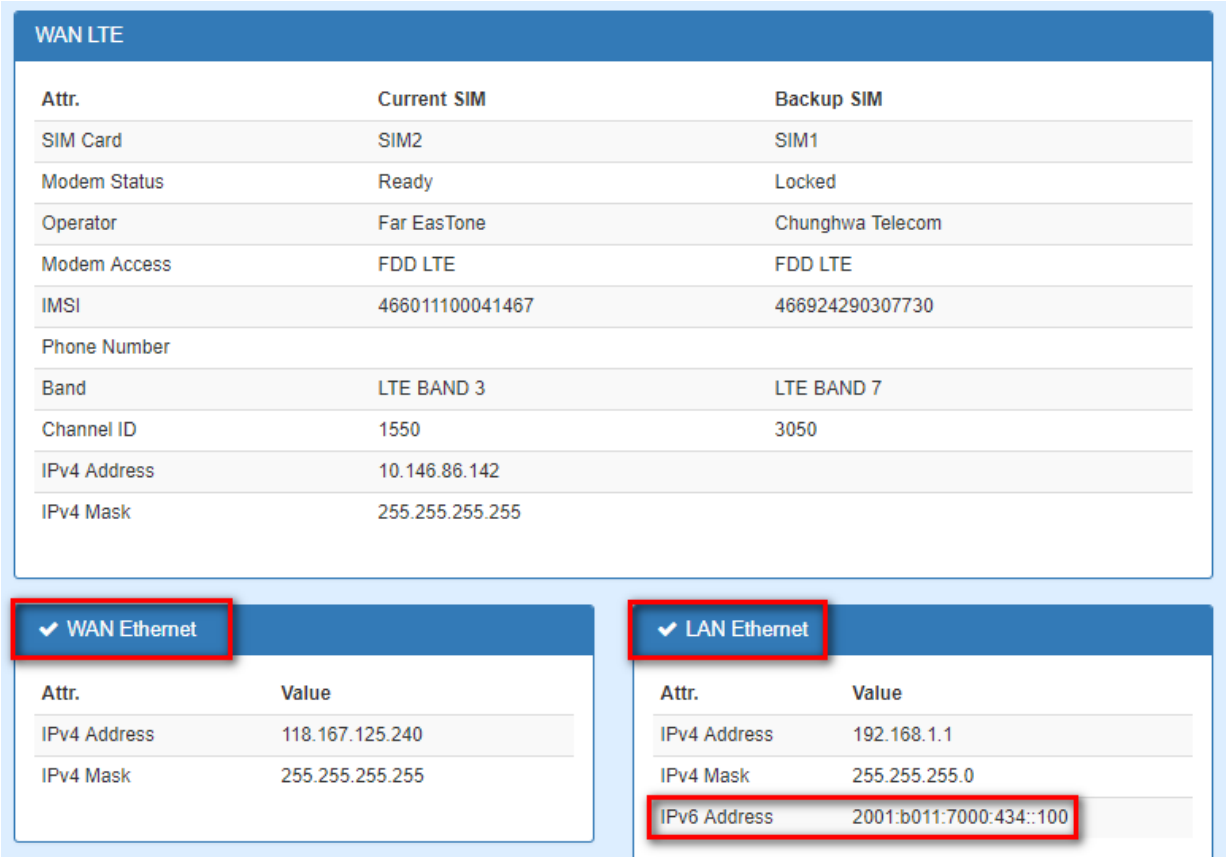
6.2.2 Ethernet Ping Health

If you configure "**WAN Priority**" to "**Auto**" mode, the system would choose the cost effective connection first such as Ethernet. However in case the Ethernet connection exist but it is unable to access internet; you can enable "**Ethernet Ping Health**" and the system would switch to LTE connection and switch back whenever Ethernet is able to access internet again.



WAN > Ethernet > Ethernet Ping Health	
Item	**Description**
Ethernet Ping Health	Select from Disable or Enable. The default is Enable.
Interval	The interval is from 1 to 60 seconds.
IPv4 Host 1	Input the address of IPv4 Host 1.
IPv4 Host 2	Input the address of IPv4 Host 2.
IPv6 Host 1	Input the address of IPv6 Host 1.
IPv6 Host 2	Input the address of IPv6 Host 2.
Hint	Show the usage descriptions.

In addition, you can check which WAN is actually using from "**Status**" page. The interface will be shown **check mark** (✓ symbol) on the connection title. For IPv6 address, the status will be displayed on LAN Etherent Interface when IPv6 is using as WAN connection.



6.3 WAN > IPv6 DNS

This section allows you to set up IPv6 DNS Server Configuration.

For IPv6 DNS Server, it provides three options to set up and each option has provided with "From ISP", "User Defined" and "None" to configure.

WAN > IPv6 DNS	
Item	**Description**
DNS Server Configuration	
IPv6 DNS Server #1 **IPv6 DNS Server #2** **IPv6 DNS Server #3**	• Each setting DNS Server has three options, including From ISP, User Defined and None. • When you select From ISP, the IPv6 DNS server IP is obtained from ISP. • When you select User Defined, the IPv6 DNS server IP is input by user.

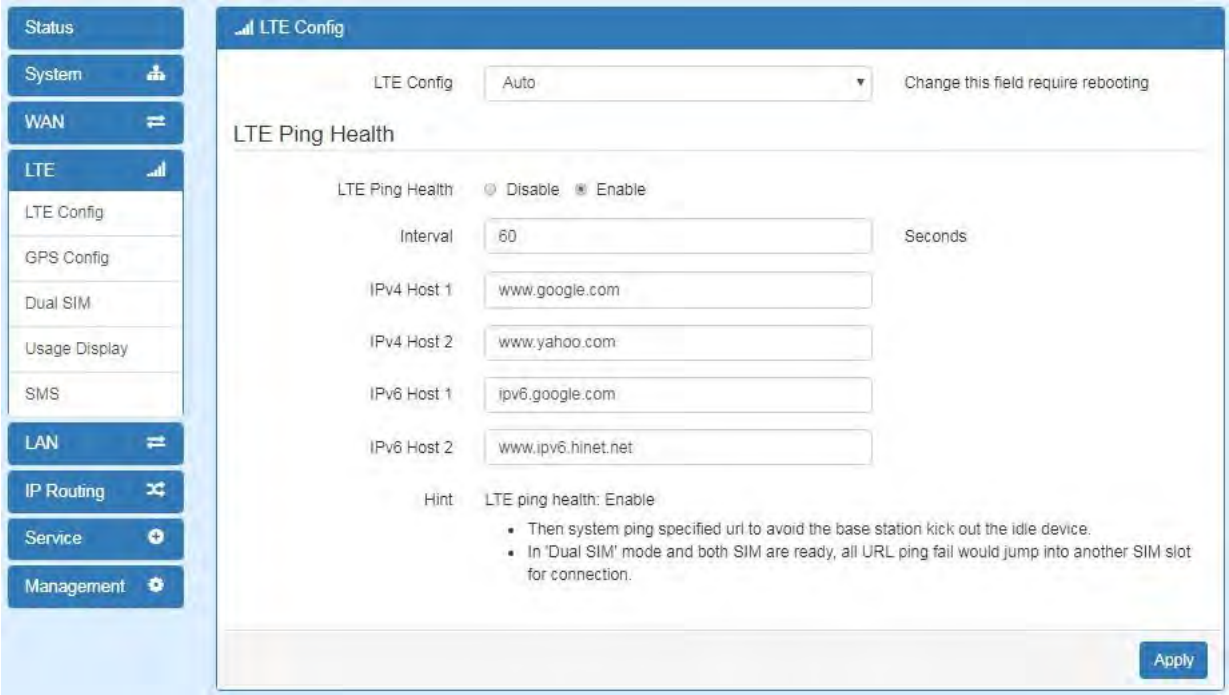
7 Configuration > LTE

This section allows you to configure LTE Config, GPS Config, Dual SIM, Usage Display and SMS.

7.1 LTE > LTE Config

7.1.1 LTE Configuration

You can set up the LTE Configuration and LTE Ping Health.



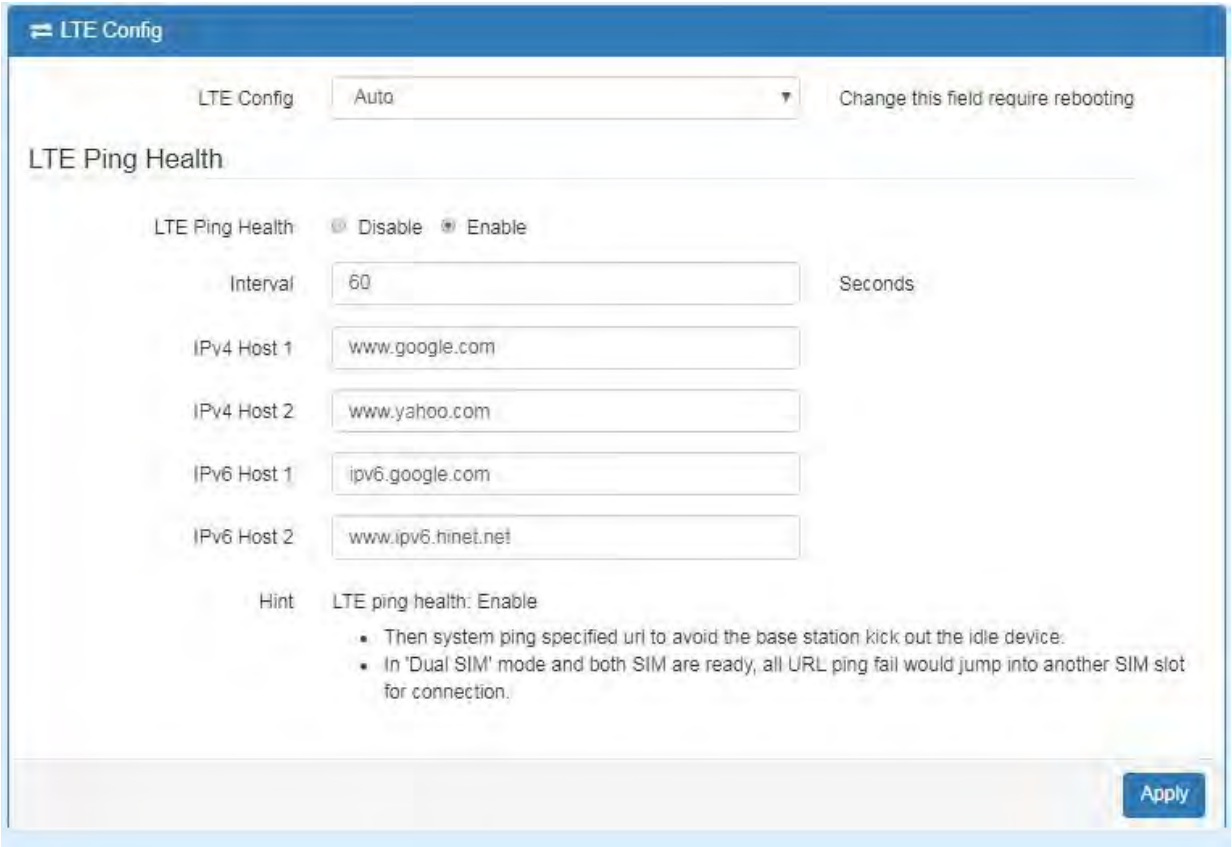
For LTE Configuration, you can select from Auto, 4G Only, 3G Only or 2G Only.

LTE > LTE Config	
Item	**Description**
Auto	Automatically connect the possible band.
4G Only	Connect to 4G network only.
3G Only	Connect to 3G network only.
2G Only	Connect to 2G network only.

7.1.2 LTE Ping Health

For LTE connection, you can enable "**LTE Ping Health**" to keep alive to avoid base station kicking out the device in idle time.

Note: In '**Dual SIM**' mode and both SIM are ready, all URL ping fail would jump into another SIM slot for connection.



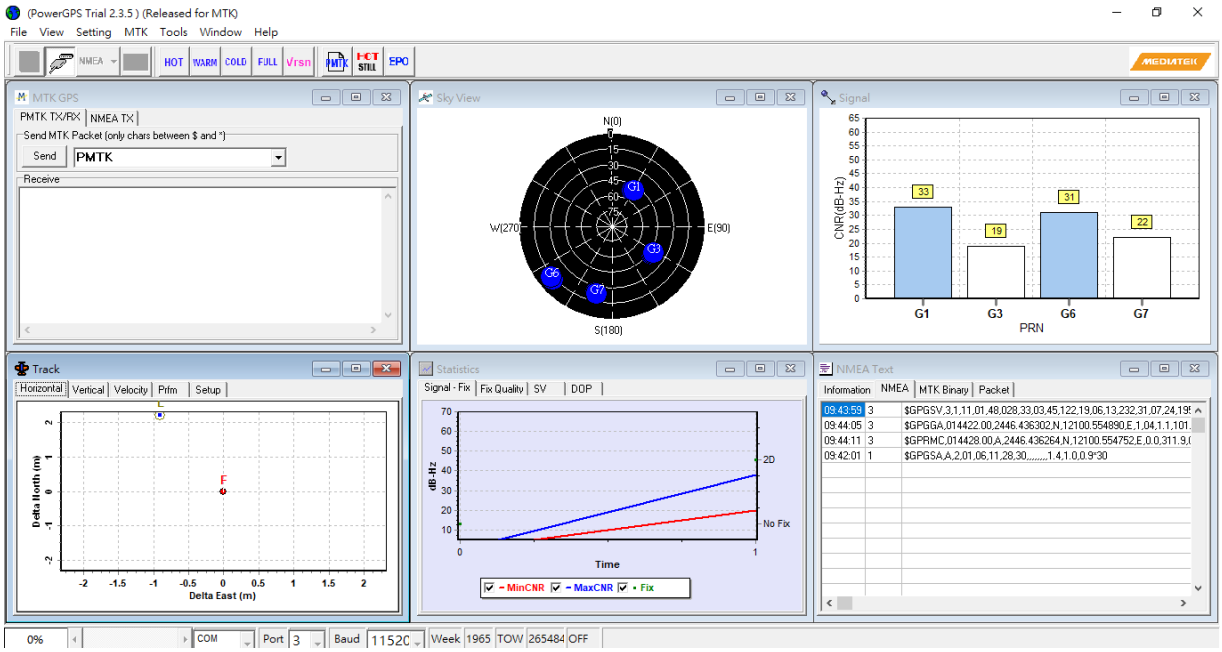
LTE > LTE Config > LTE Ping Health	
Item	**Description**
LTE Ping Health	Select from Disable or Enable.
Interval	Input the interval seconds of ping.
IPv4 Host 1	Input the address of IPv4 Host 1.
IPv4 Host 2	Input the address of IPv4 Host 2.
IPv6 Host 1	Input the address of IPv6 Host 1.
IPv6 Host 2	Input the address of IPv6 Host 2.
Hint	Show the usage descriptions.

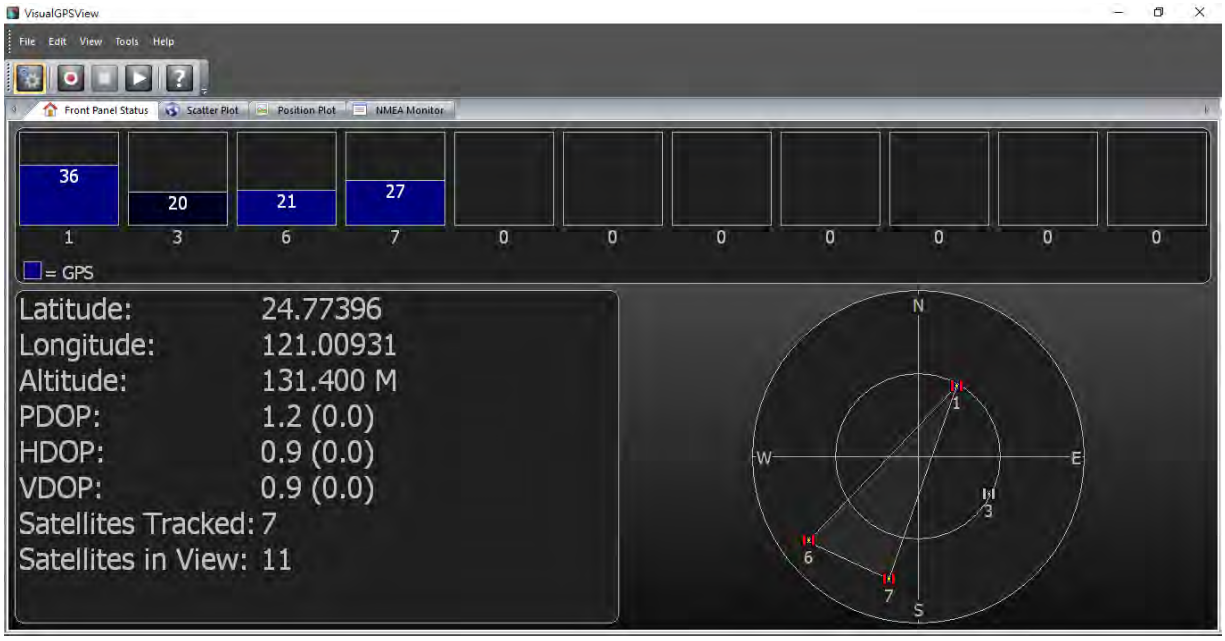
7.2 LTE > GPS Config

This section allows you to set up GPS Configuration and connect RS232 from the used router to have more detailed information for your specific purpose.

LTE > GPS Config	
Item	**Description**
Report to	Select from RS232 and LOG.
COM Port	Select from COM1 and COM2.
NMEA Type	Select from GSV, GGA, RMC and GSA.

For example, you can use some software depending on your requirements and activate the GPS Configuration to display what information you need from your selecting software.



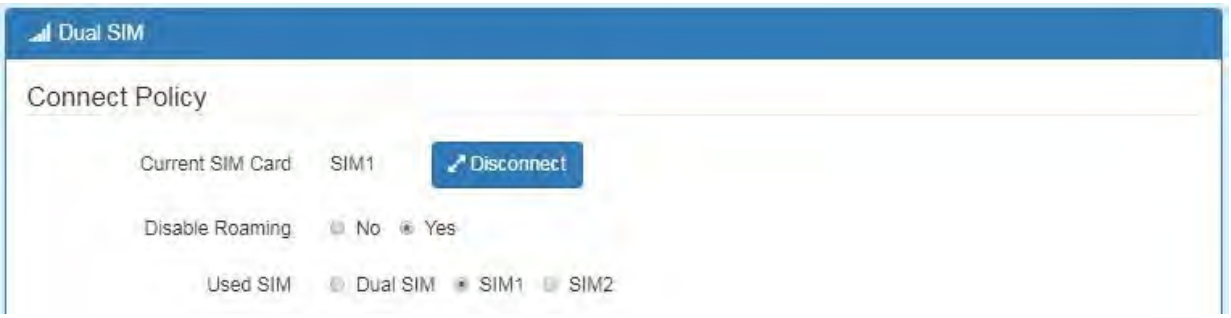


7.3 LTE > Dual SIM

This section allows you to understand the status of connectivity for Dual SIM, SIM1 and SIM2. The **Used SIM** item has three options and the default is on Dual SIM when first connection. The **Connect Retry Number** field can set up the re-connecting time if your one of the SIM cards on Dual SIM mode can't connect successfully. The default of Connect Retry Number is 3 minutes.

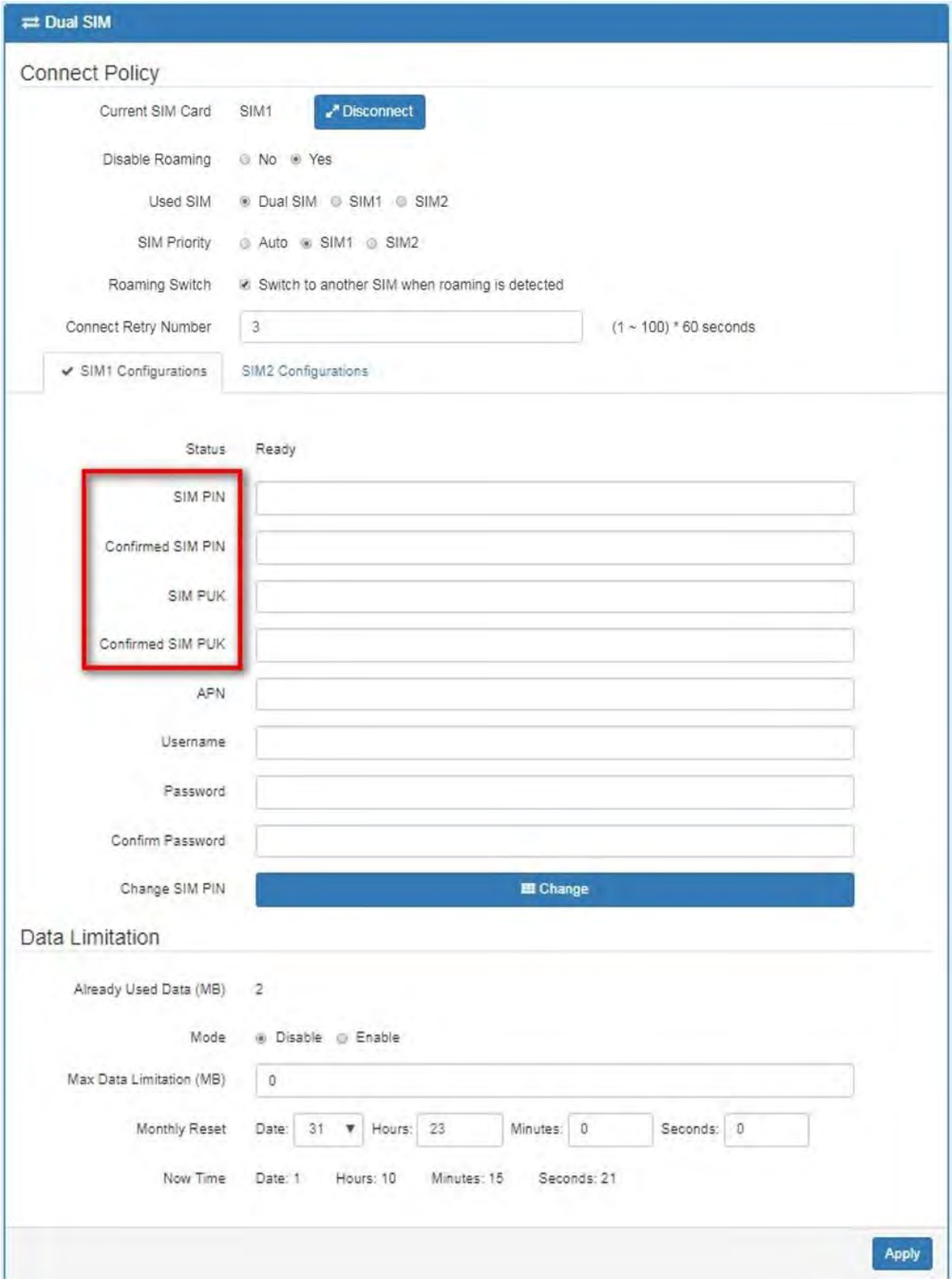
For **Roaming Switch**, it means Switch to another SIM when roaming is detected. System will switch SIM slot when current SIM is in roaming state and another SIM slot is in READY state.

If you have selected either SIM1 or SIM2 for the **Used SIM** to connect, the **Roaming Switch** and **Connect Retry Number** would not to be shown in the interface.

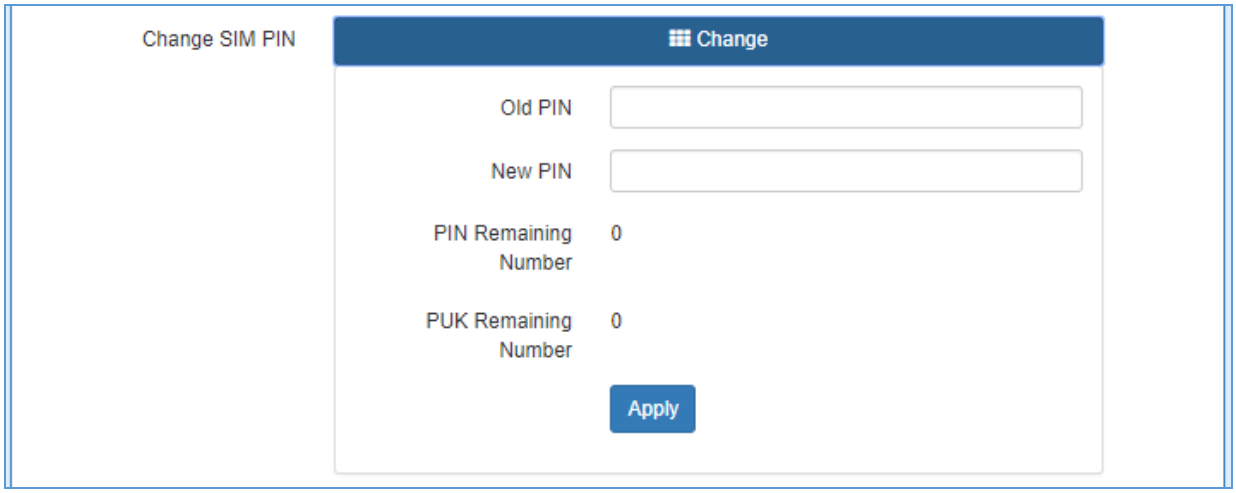


You can set up the SIM cards, SIM1 Configurations or SIM2 Configurations.

- **SIM PIN:** If you has configured SIM PIN code into SIM card, please type SIM PIN code in Dual SIM configuration to make unlock successfully.
- **SIM PUK:** If you has typed wrong SIM PIN code and retried more than 3 times, the SIM Card will become the blocked mode. In this case, you have to type PUK and new SIM code to unlock SIM Card.

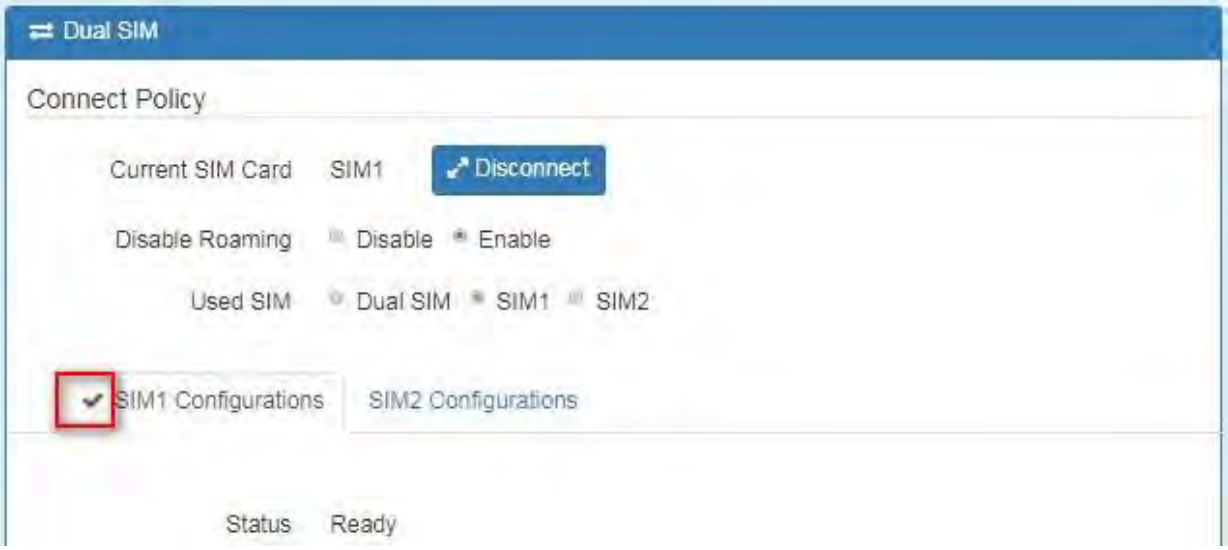

Dual SIM
Connect Policy
Current SIM Card
SIM1
Disconnect
Disable Roaming
No
Yes
Used SIM
Dual SIM
SIM1
SIM2
SIM Priority
Auto
SIM1
SIM2
Roaming Switch
Switch to another SIM when roaming is detected
Connect Retry Number
3
(1 ~ 100) * 60 seconds
SIM1 Configurations
SIM2 Configurations
Status
Ready
SIM PIN
Confirmed SIM PIN
SIM PUK
Confirmed SIM PUK
APN
Username
Password
Confirm Password
Change SIM PIN
Change
Data Limitation
Already Used Data (MB)
2
Mode
Disable
Enable
Max Data Limitation (MB)
0
Monthly Reset
Date:
31
Hours:
23
Minutes:
0
Seconds:
0
Now Time
Date: 1
Hours: 10
Minutes: 15
Seconds: 21
Apply

- **Change SIM PIN**：If you want to change SIM PIN code, you can click Change button and type old SIM PIN code and new SIM PIN code. Please aware not to exceed the retry number (PIN remaining number and PUN remaining number).



Note:

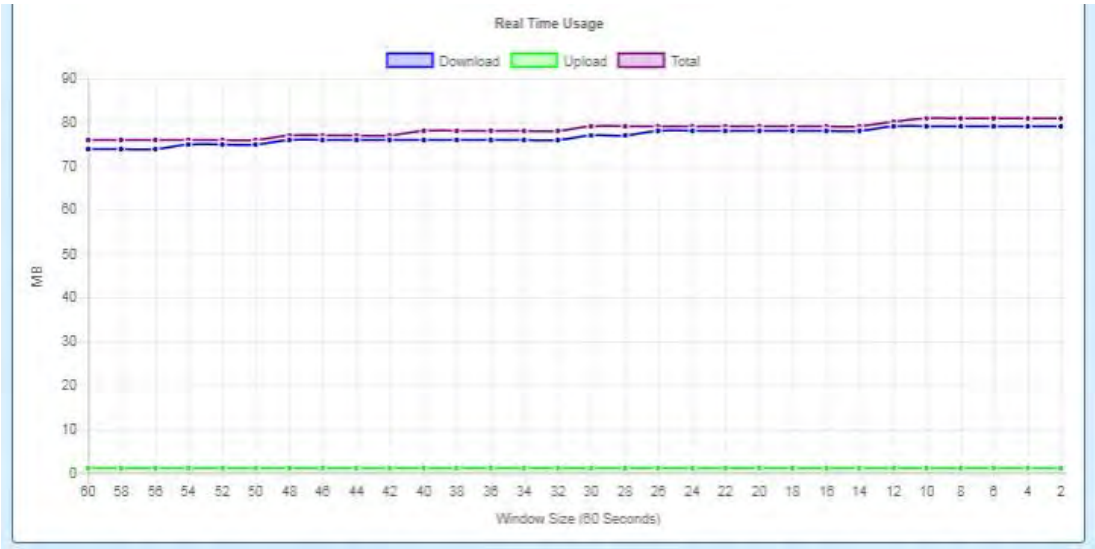
The interface will be shown the tick symbol at the same time when each SIM Card has been connected.



LTE > Dual SIM	
Item	**Description**
Connect Policy	
Current SIM Card	Display which SIM slot is using.
Status of SIM Card Connectivity	● **Connect:** After manually disconnect, user can only click Connect button to get connection or reboot the device to make it automatically connect. ● **Disconnect:** If there is one SIM slot get connection, the Disconnect button appear. After manually click Disconnect, the system would not automatically get connection until next reboot.
Disable Roaming	● **Disable:** SIM gets connection even it is in roaming state. ● **Enable:** SIM would not get connection when in roaming state.
Used SIM	Three options to show SIM Card's used status, including Dual SIM, SIM1 and SIM2.
SIM Priority	Three options to set the priority for SIM Card, including Auto, SIM1 and SIM2. To set up the first link SIM slot from Dual SIM mode with two SIM cards.
Roaming Switch	Switch to another SIM when roaming is detected. System will switch SIM slot when current SIM is in roaming state and another SIM slot is in READY state.
Connect Retry Number	Entry the time when SIM card starts to activate. This option is only for Dual SIM mode.
SIM1 Configurations or SIM2 Configurations	
Status	Display the status of Dual SIM.
SIM PIN	Configure PIN code to unlock SIM PIN.
Confirmed SIM PIN	Confirm PIN code.
SIM PUK	Fill in PUK to unlock SIM Card after typing more than 3 times.
Confirmed SIM PUK	Confirm SIM PUK.
APN	APN can be input by user or the system will search from internal database if APN is blank.
Username	The username can be input by user or the system will search from internal database if the username is blank.
Password	The password can be input by user or the system will search from internal database if the password is blank.
Confirm Password	Fill in your changed password.
Change SIM PIN	Change your old SIM PIN code into new SIM PIN code.
Data Limitation	
Mode	Turn on/off the Data Limitation to disable or enable.
Already Used Data (MB)	Display current used throughput since last reset.
Max Data Limitation (MB)	Configure max throughput.
Monthly Reset	Set up the reset time during the month.
Now Time	Show the current time of system.

7.4 LTE > Usage Display

This section shows the status of **current SIM card**, **operator**, **IMSI** and the charts for **Real Time**, **Hourly**, **Daily**, **Weekly**, and **Monthly**.



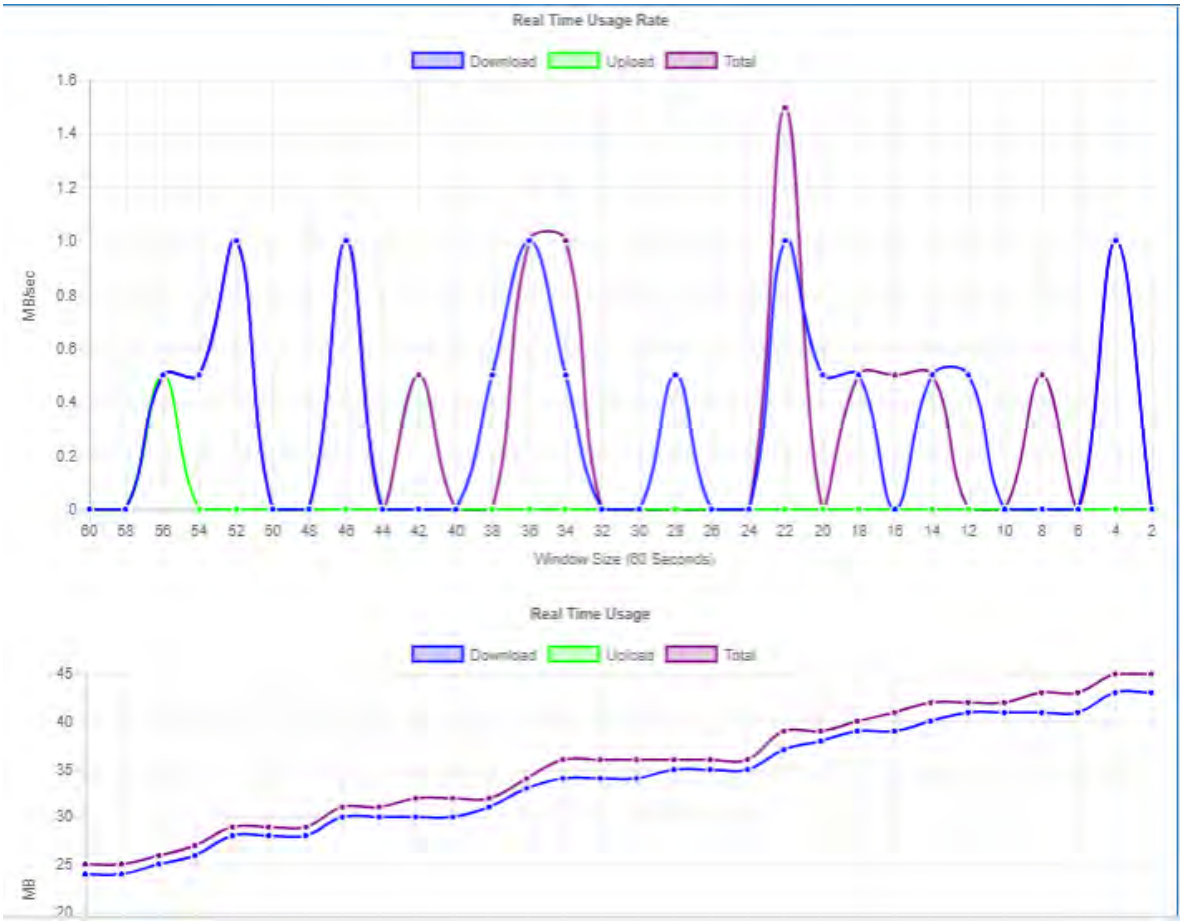
(1) Real-Time Usage:

- **Real-Time Usage Rate:**

It displays real-time Download/Upload/Total MB per seconds for current using SIM card and the view window size is 60 seconds.

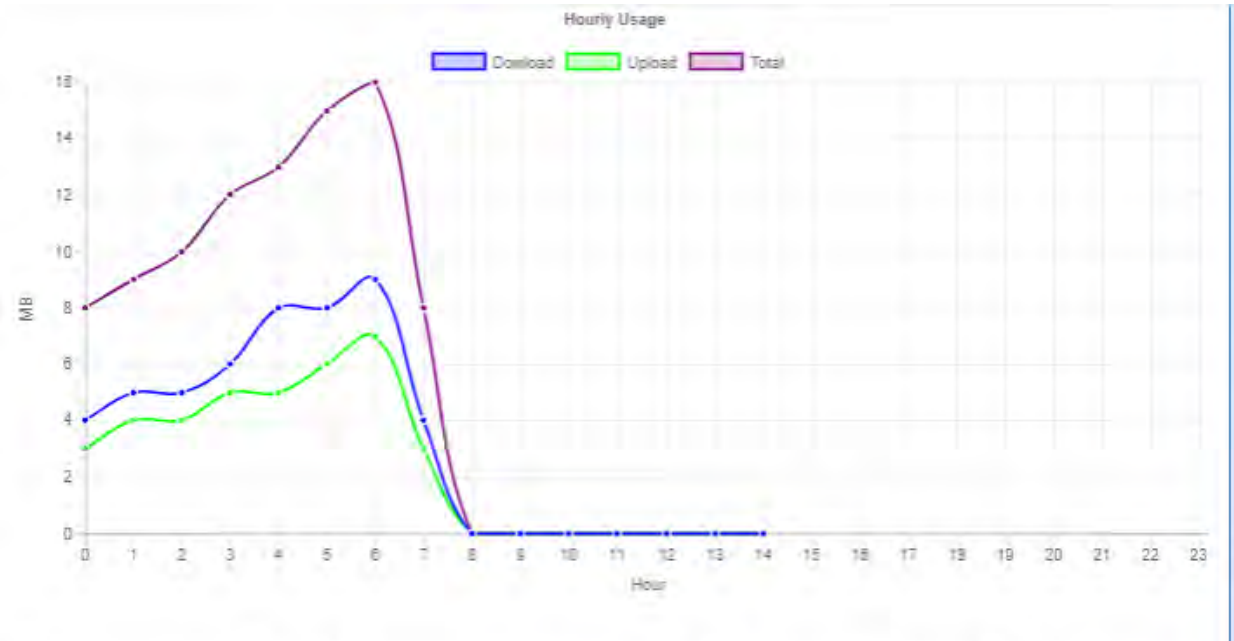
- **Real-Time Usage:**

It displays accumulated real-time Download/Upload/Total MB per seconds for current using SIM card and the view window size is 60 seconds.



(2) Hourly Usage:

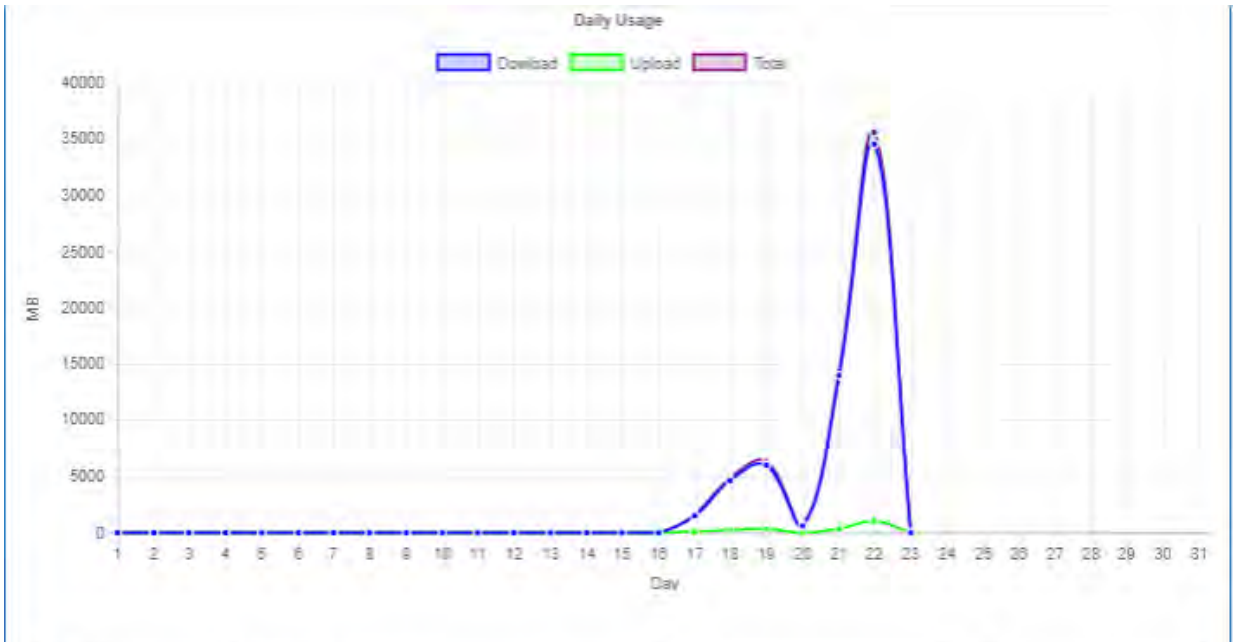
It displays Download/Upload/Total MB per hour in one day for current using SIM card and the view window size is 24 hours.



Hour	Download	Upload	Total
0	4	3	8
1	5	4	9
2	5	4	10
3	6	5	12
4	8	5	13
5	8	6	15

(3) Daily Usage:

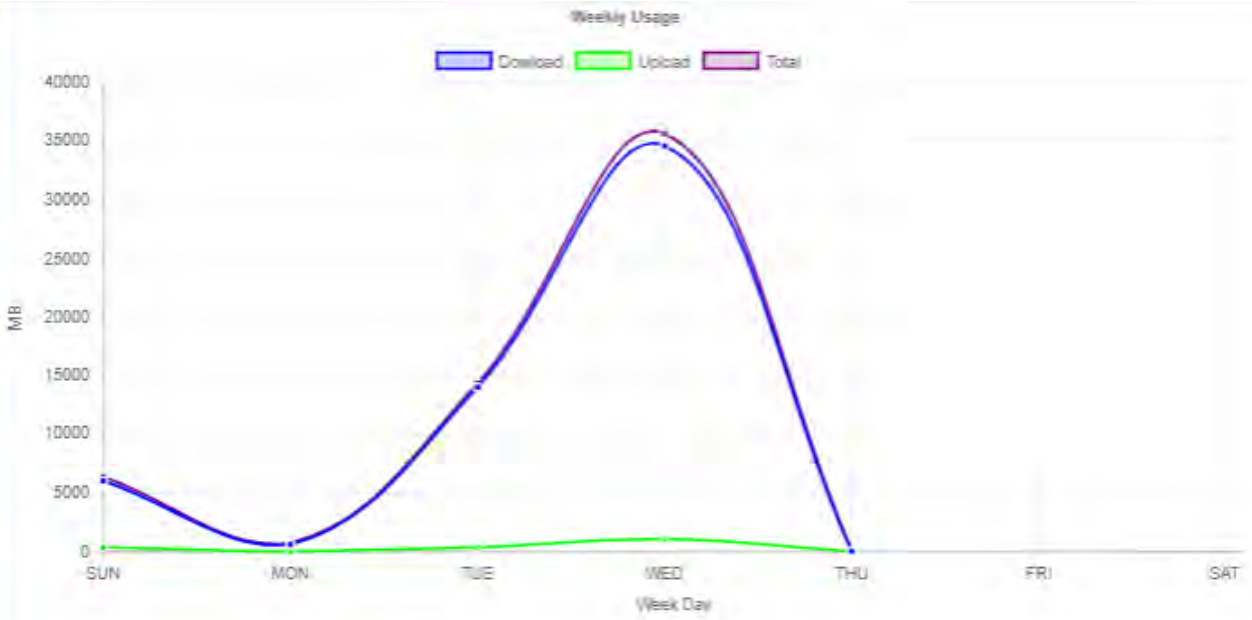
It displays Download/Upload/Total MB per day in one month for current using SIM card and the view window size is 31 days.



Day	Download	Upload	Total
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0

(4) Weekly Usage:

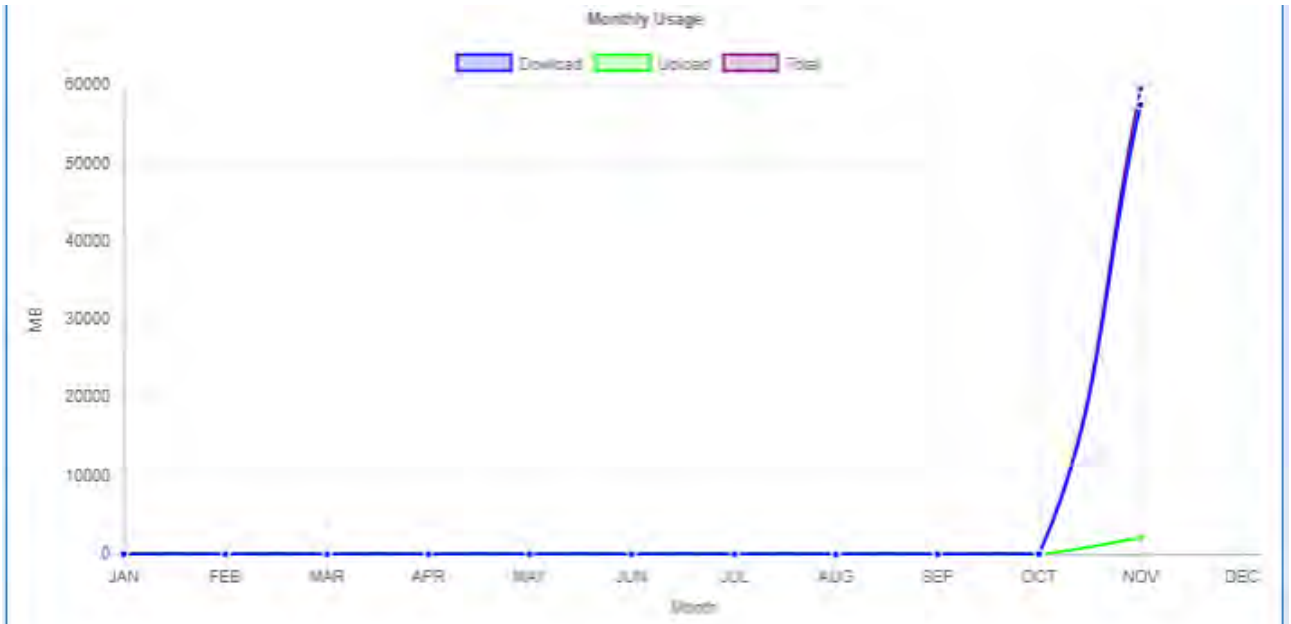
It displays Download/Upload/Total MB per day in one week for current using SIM card and the view window size is 7 days.



Week Day	Download	Upload	Total
SUN	5955	360	6316
MON	611	36	648
TUE	13928	386	14315
WED	34595	995	35591
THU	27	21	49

(5) Monthly Usage:

It displays Download/Upload/Total MB per month in one year for current using SIM card and the view window size is 12 months.

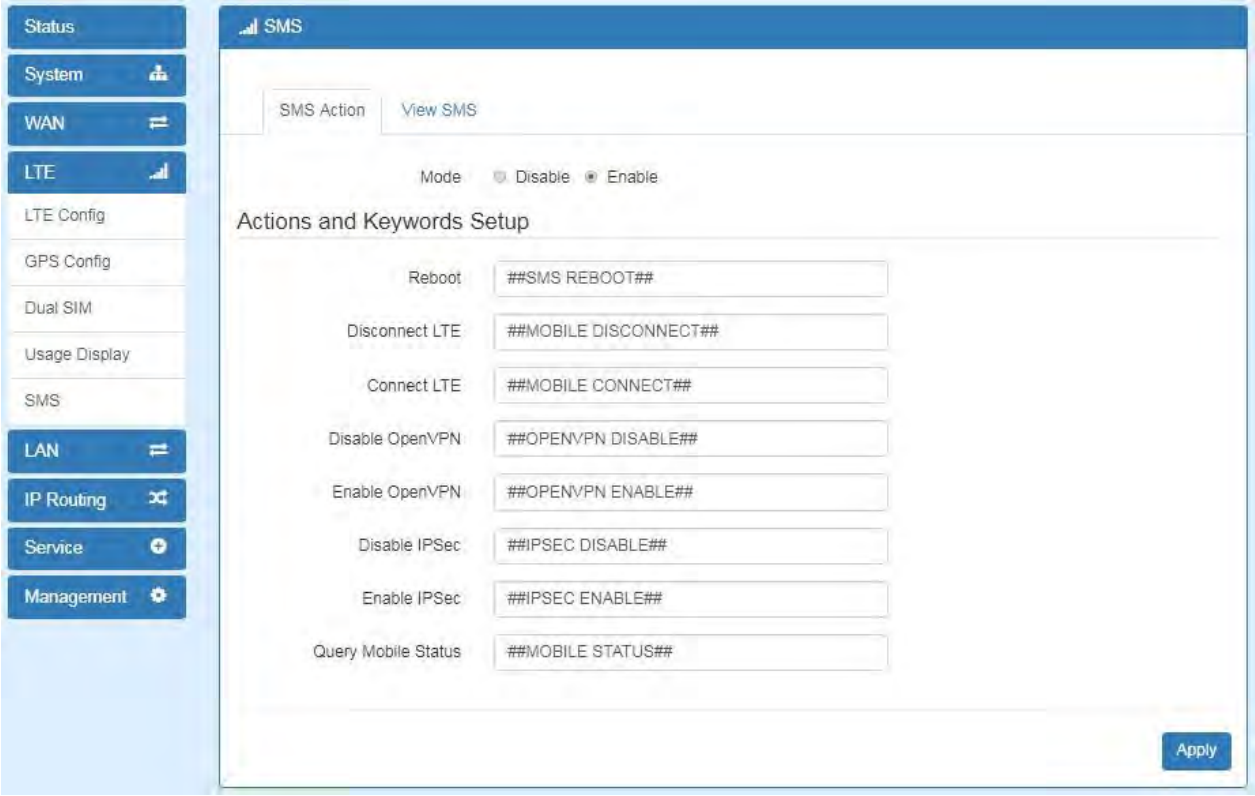


Month	Download	Upload	Total
JAN	0	0	0
FEB	0	0	0
MAR	0	0	0
APR	0	0	0
MAY	0	0	0
JUN	0	0	0

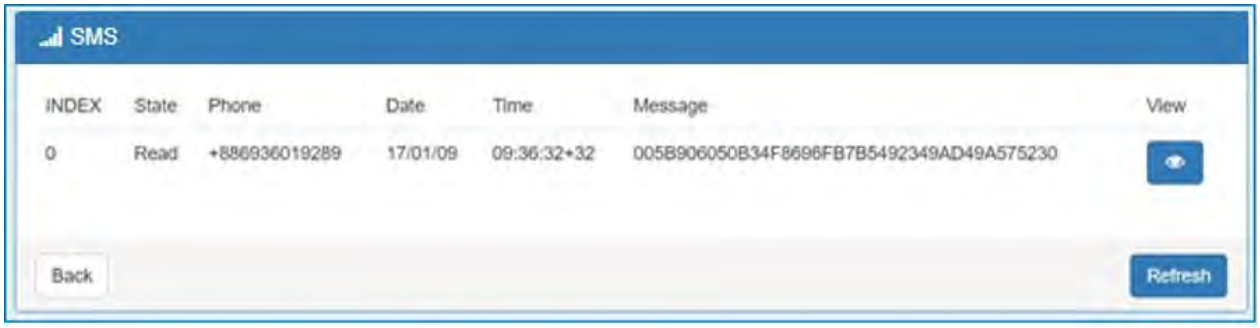
7.5 LTE > SMS

This section provides two settings, one is **SMS Action** and the other is **View SMS**.

(1) When enabling **SMS Action**, it allows you by sending key words SMS to trigger device setting/action/query status.

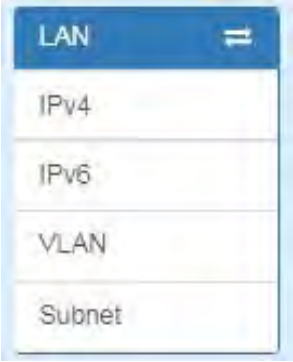


(2) For **View SMS**, this section allows you to review the information of SMS that you have received, including the state, phone and date and time. You can click **view button** to review all messages.



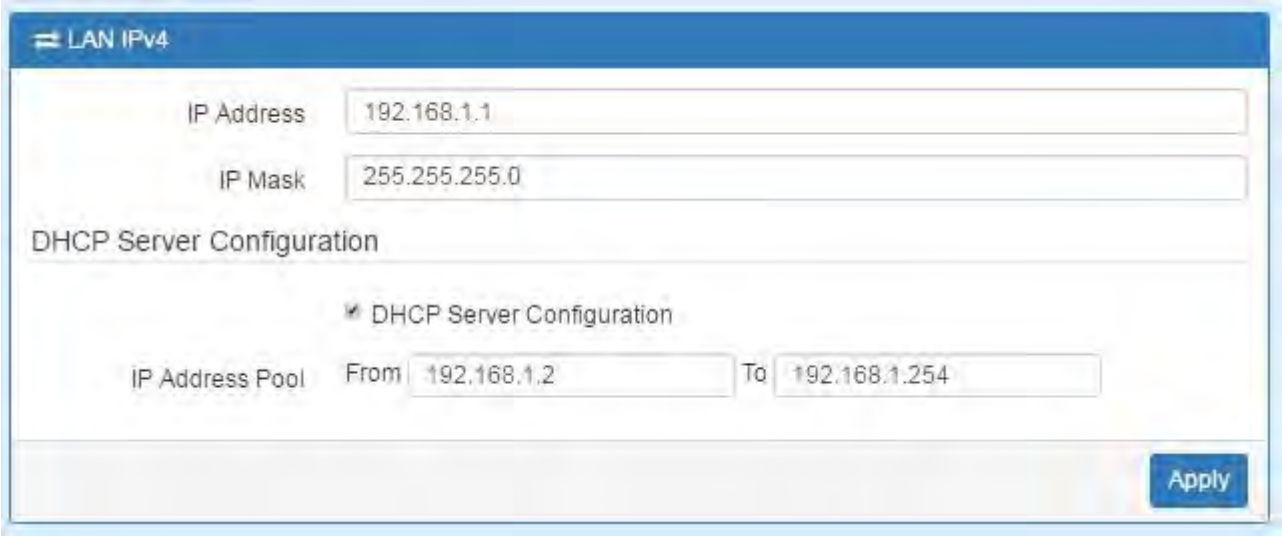
8 Configuration > LAN

This section allows you to configure LAN IPv4, LAN IPv6, VLAN and Subnet.



8.1 LAN > IPv4

Set up your IP Address and IP Mask. Also, fill in the information of DHCP Server Configuration.



LAN > IPv4	
Item	**Description**
LAN IPv4	• IP Address:192.168.1.1 • IP Mask:255.255.255.0 Both of them are default, you can change them according to your local IP Address and IP Mask.
DHCP Server Configuration	• Turn on/off DHCP Server Configuration. • Enable to make router can lease IP address to DHCP clients which connect to LAN.
IP Address Pool	• Define the beginning and the end of the pool of IP addresses which will lease to DHCP clients.

8.2 LAN > IPv6

Select your type of IPv6, which shows **Delegate Prefix from WAN** or **Static,** and then set up DHCP Server Configuration, including Address Assign, DNS Assign and DNS Server.

LAN > IPv6	
Item	**Description**
LAN IPv6	• This section provides two types, including **Delegate Prefix from WAN** and **Static**. • **Static Address**: You need to input the static address when you select the static type.
Delegate Prefix from WAN	• Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
Static	• Select this option to configure a fixed IPv6 address for the cellular router's LAN IPv6 address.
Address Assign Setup	Select how you obtain an IPv6 address: • **Stateless**: The cellular router uses IPv6 stateless auto configuration. RADVD (Router Advertisement Daemon) is enabled to have the cellular router send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 clients. • **Stateful**: The cellular router uses IPv6 stateful auto configuration. The LAN IPv6 clients can obtain IPv6 addresses through DHCPv6.

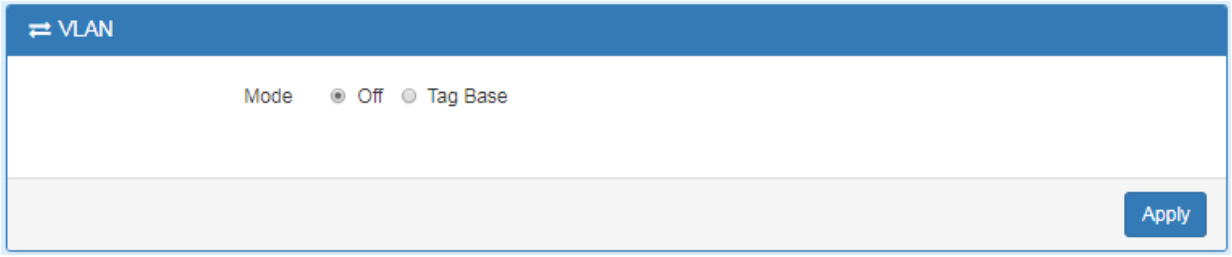
8.3 LAN > VLAN

This section allows you to set up VLAN that provides a network segmentation system to distinguish the LAN clients and separate them into different LAN subnet for enhancing security and controlling traffic.

There are two router models based on the numbers of LAN ports to have two setting types of VLAN and communicate with your devices, one is **1-port LAN** and the other is **3-port LANs**.

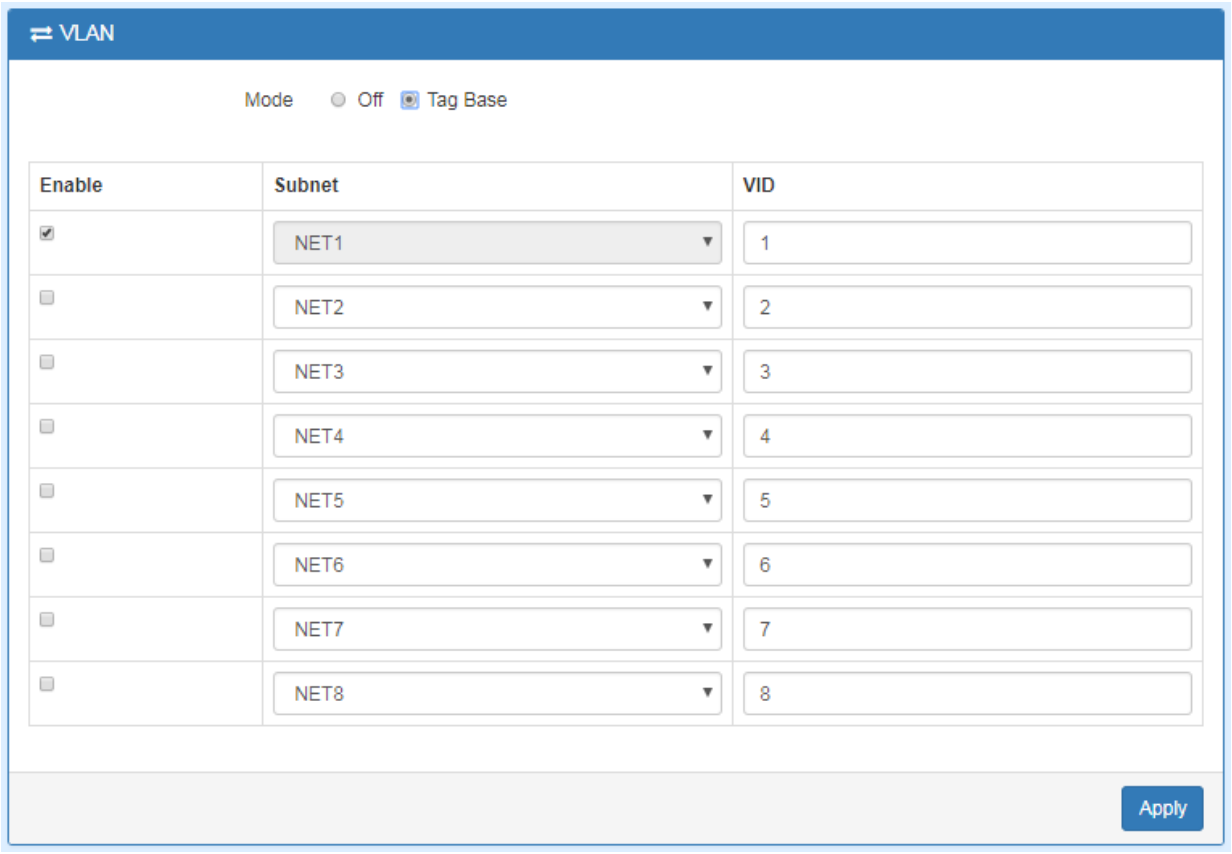
- Type 1:

For **1-port LAN** router model, you can use the **Type 1** to configure VLAN. First, the **VLAN Mode** allows you to select **Off** or **Tag Base (802.1p)**.

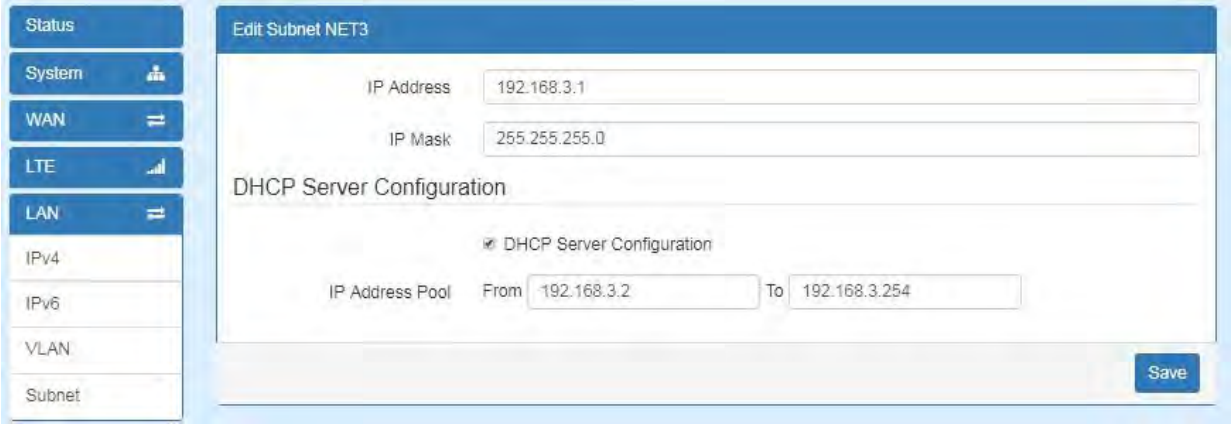


When VLAN Mode is set to **Tag Base**, the VLAN setting window will appear as shown below.

For each row, the settings can be enabled or disabled by checkbox and select the **Subnet** and the **VLAN ID (VID)**. The **Subnet** sets up the IP address and IP mask for the router so this router can communicate with the third party by this IP address and IP mask on this VLAN. (***Note:*** The NET1 can't remove it and fixes in the first row.)



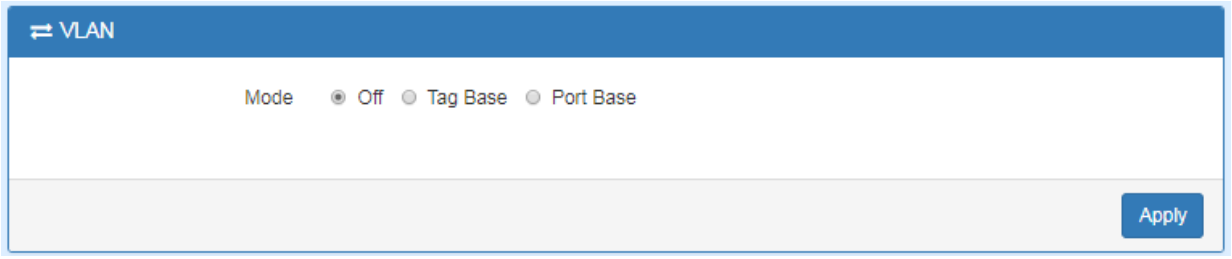
Furthermore, the **Subnet** provides DHCP Server function to allow the third party for the same VLAN to get IP address and IP mask. Therefore, you do not need to configure manually. (***Note:*** The subnet information will show the Subnet window from the LAN catalogue.)



LAN > VLAN (1-port LANs)	
Item	**Description**
Mode	● The VLAN mode is Off or Tag Base (802.1p VLAN).
Enable	● The assigned row of setting are enabled.
Subnet	● The subnet provides IP address and IP mask for the router.
VID	● The VLAN ID range is from 1 to 4094.

- Type 2:

For **3-port LANs**, the **VLAN Mode** allows you to select **Off, Tag Base (802.1p)** or **Port Base.**



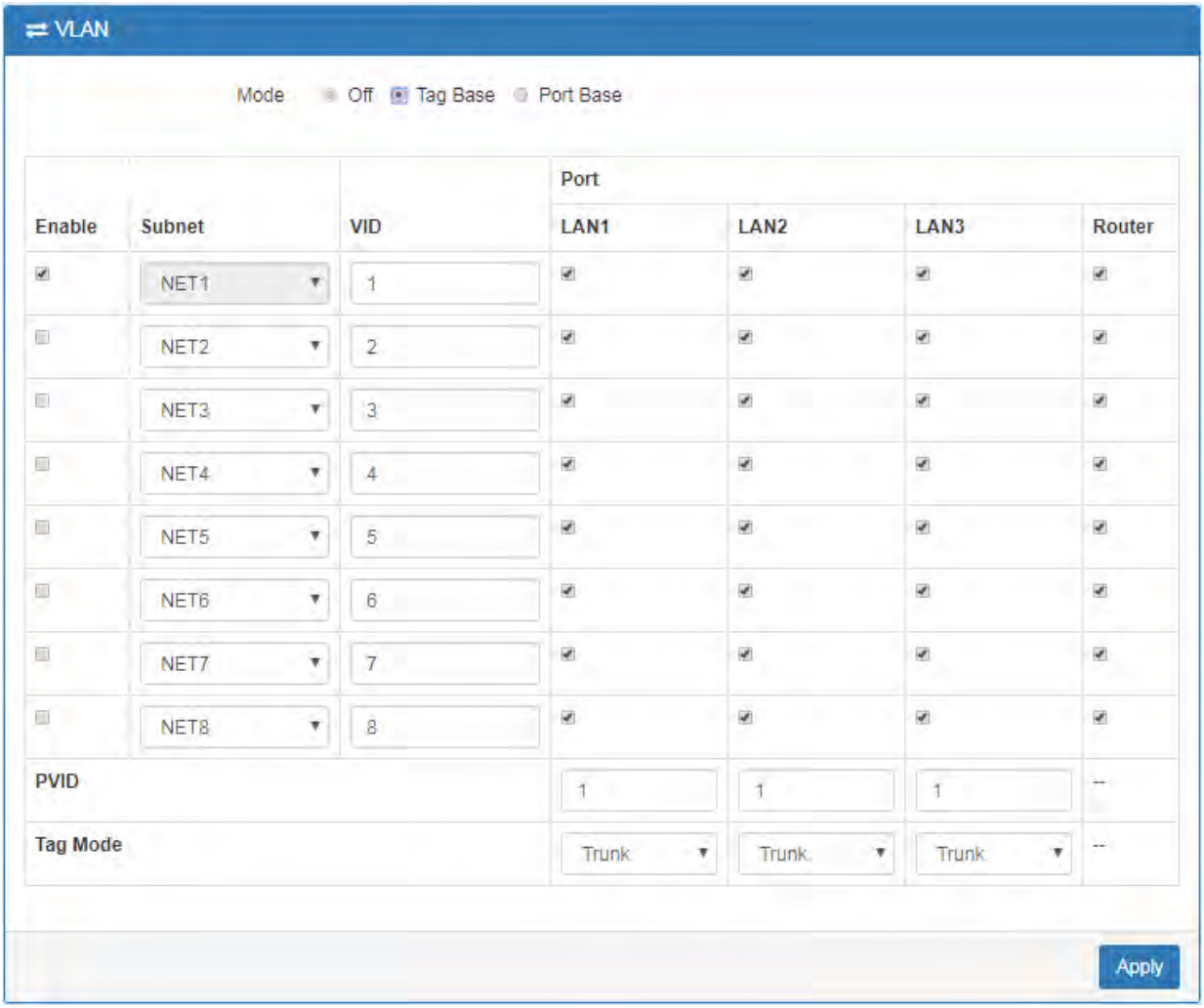
When VLAN Mode is set to **Tag Base**, the VLAN setting window will appear as shown below.

For each row, the settings can be enabled or disabled by checkbox and select the **Subnet** and the **VLAN ID (VID)**. The **Subnet** sets up the IP address and IP mask for the router so this router can communicate with the third party by this IP address and IP mask on this VLAN. (***Note:*** The NET1 can't remove it and fixes in the first column.)

Furthermore, the **Subnet** provides DHCP Server function to allow the third party for the same VLAN to get IP address and IP mask. Therefore, you do not need to configure manually. (***Note:*** The subnet information will show the Subnet window from the LAN catalogue.)

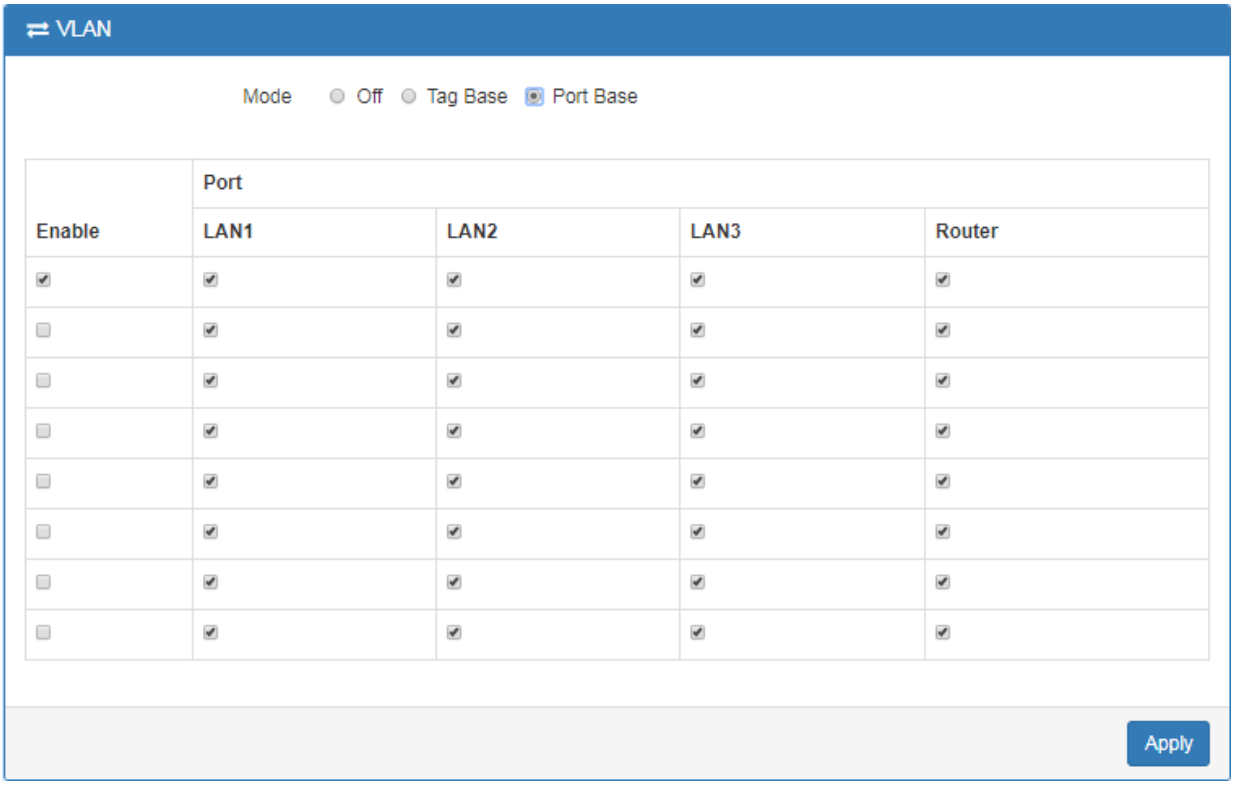
There are three ports for **Tag Base Mode**, including LAN1, LAN2 and LAN3. And one **Router port** which is a gate allows those ports to access internet or the router. The **PVID** and **Tag Mode** are for LAN1, LAN2 and LAN3 ports. The **PVID** provides the untagged devices to communicate with third-party devices. (***Note:*** The untagged devices mean not to support 802.1p VLANs.)

The **Tag Mode** can be **Trunk** or **Access**. The **Trunk** allows to carry multiple 802.1p VLANs traffic. The **Access** allows the untagged devices to communicate with a specific 802.1p VLAN by assigned **PVID**.



LAN > VLAN (3-port LANs) > Tag Base	
Item	**Description**
Mode	The VLAN mode is Off or Tag Base (802.1p VLAN).
Enable	The assigned row of settings are enabled.
Subnet	Sets the IP address, IP mask and DHCP server.
VID	The VLAN ID range is from 1 to 4094.
Port	The port is shown to assign the port to a VLAN which the device is connected from LAN 1, LAN2, LAN3 and Router.
PVID	● The PVID range from 1 to 4094 ● Sets the default VLAN ID for untagged devices connected to the port.
Tag Mode	● The **Trunk** port setting is connected to another 802.1p VLAN aware switch or device. ● The **Access** port setting is connected to a single untagged device.

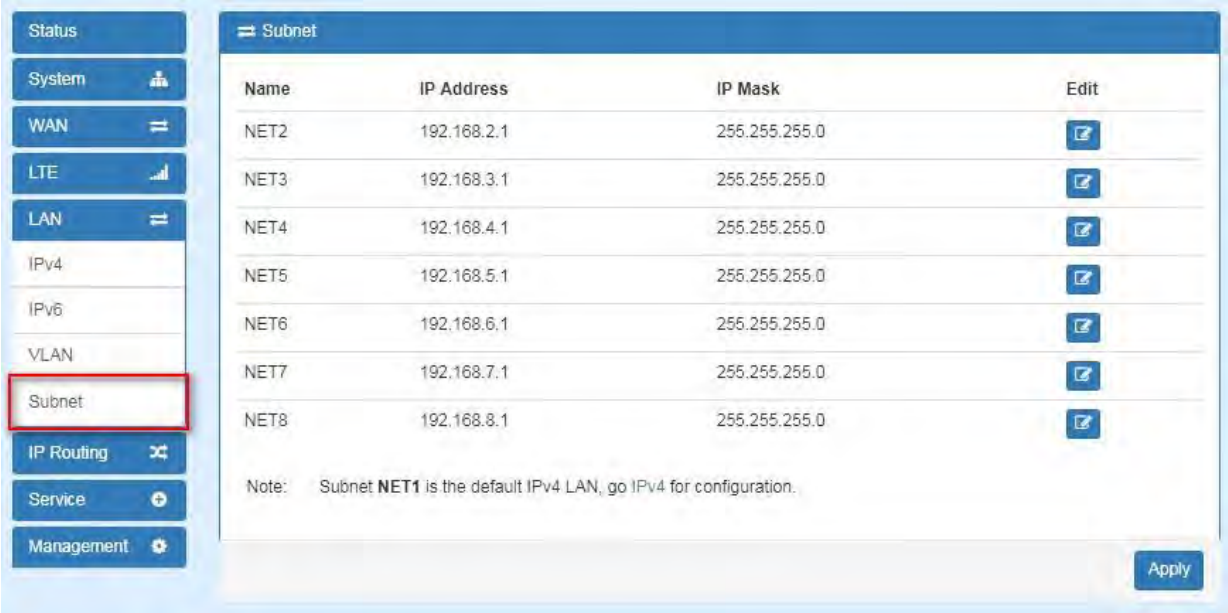
When VLAN Mode is set to **Port Base**, the VLAN setting window will appear as shown below. For each row, the settings can be enabled or disabled by checkbox and assign the port to communicate each other. There are three ports for **Port Base Mode**, including LAN1, LAN2 and LAN3. And one **Router port** which is a gate allows those ports to access internet or the router.



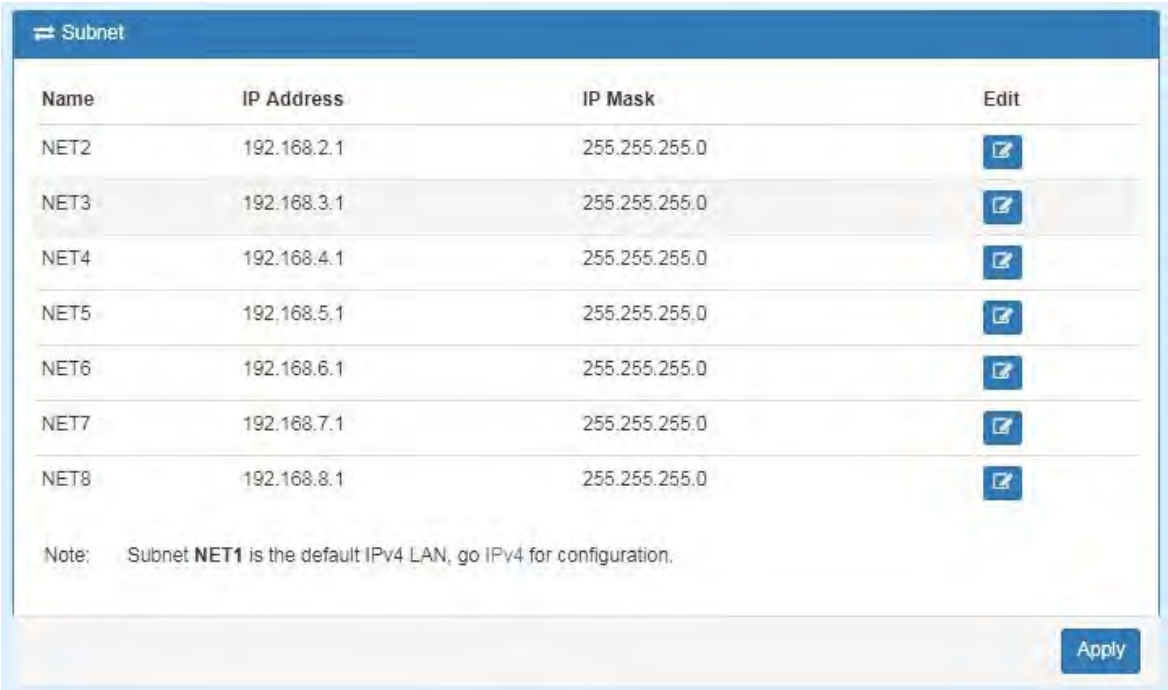
LAN > VLAN (3-port LANs) > Port Base	
Item	**Description**
Mode	The VLAN mode is Off, Tag Base (802.1p VLAN) or Port Base.
Enable	The assigned row of setting are enabled.
Port	The port is shown to assign the port to a VLAN which the device is connected from LAN 1, LAN2, LAN3 and Router.

8.4 LAN > Subnet

This section allows you to get the information of IP Address and IP Mask and edit for the Subnets from DHCP Server Configuration.



This **Subnet** setting is the same with LAN->IPv4 setting and follows with Tag Base Mode of VLAN to enable the function.

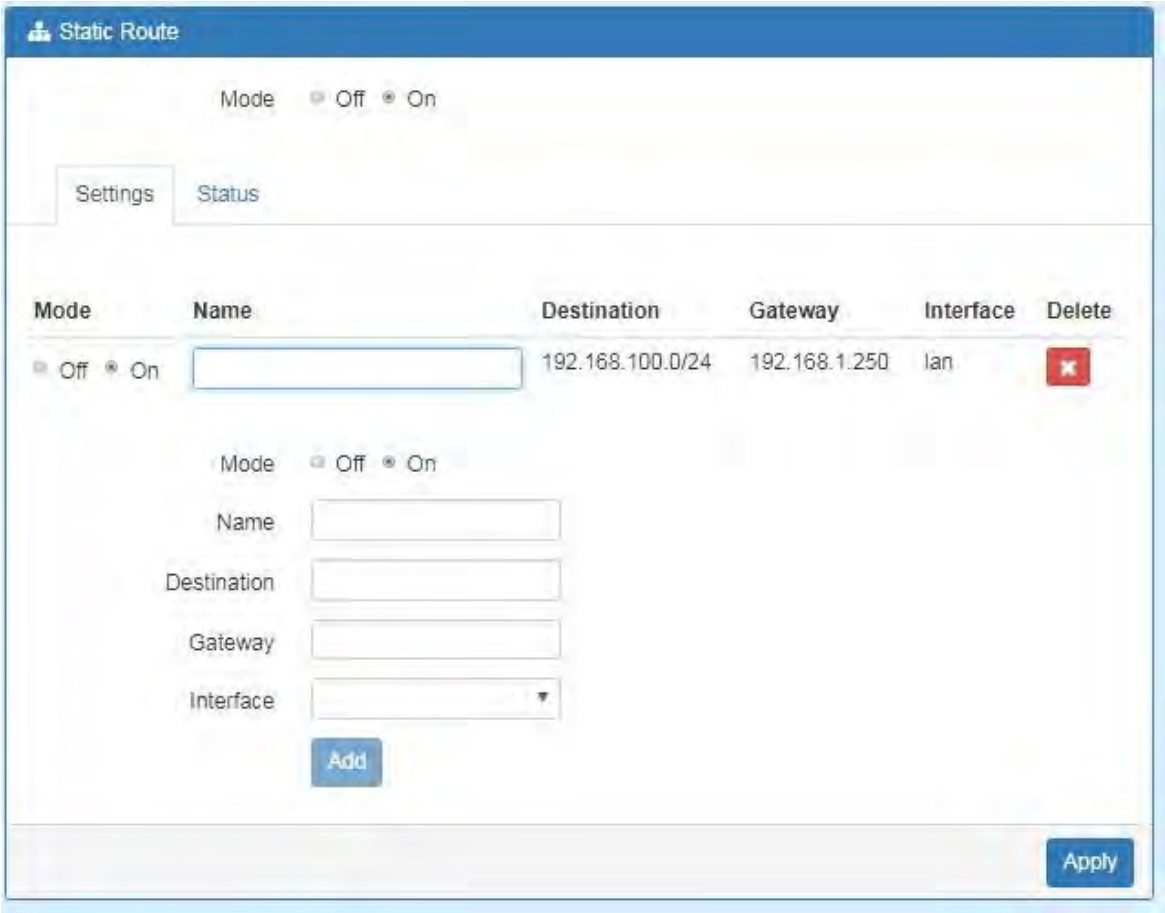


9 IP Routing

This section allows you to configure the Static Route and RIP.

9.1 IP Routing > Static Route

This section allows you to configure the Static Route. A static route is a pre-determined path that network information must follow to reach a specific host or network.

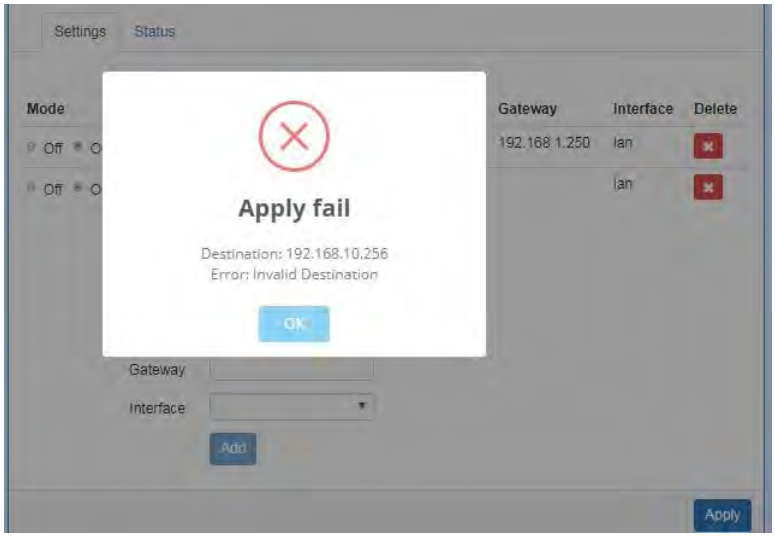


IP Routing > Static Route	
Item	**Description**
Mode	The setting is for full network. Select from Off or On.
Settings	
Mode	The setting is for the specific network. Select from Off or On.
Name	Set up each name for your running host or network.
Destination	Fill in the destination of a specific subnet or IP from network.
Gateway	Fill in the gateway address of your router.
Interface	Select the interface from LAN or Ethernet.

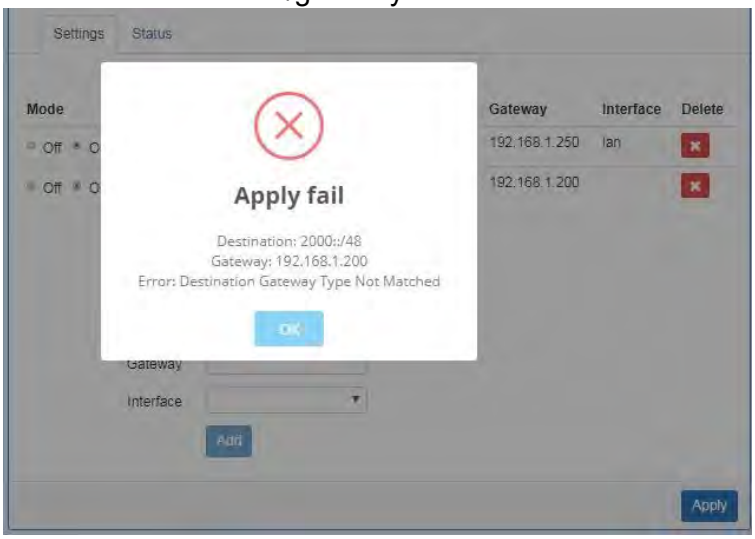
Note:

- The destination field is required to fill in. The format of destination is IPv4 or IPv6.
- The address of gateway or the type of interface can be chosen one or both to fill in the field.
- There are two fail situations when you fill in the incorrect type for the field.

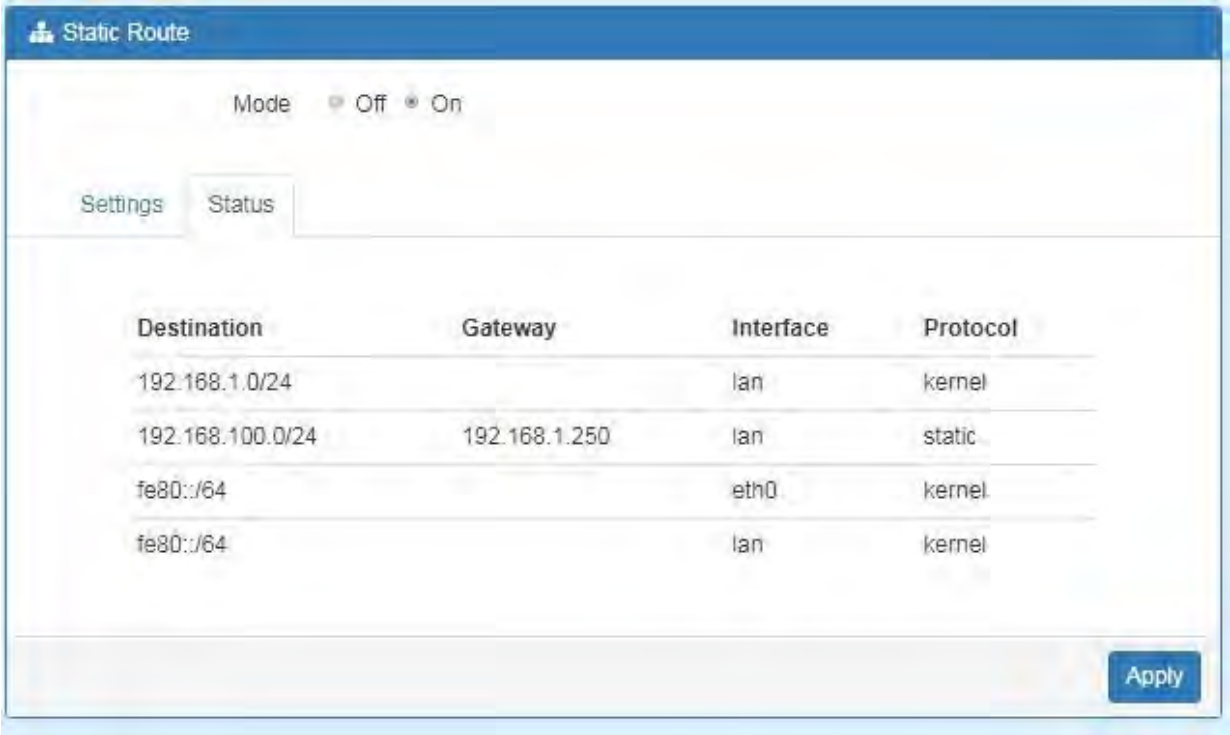
(1) Input the invalid format of destination. The interface is shown in Apply fail to notice.



(2) Input the IP address of destination/gateway from IPv4 and IPv6 at the same time. The interface is shown in Apply fail to notice. You should select either IPv4 or IPv6 as the address of destination/gateway.



The status tab shows the information from the settings of static route.



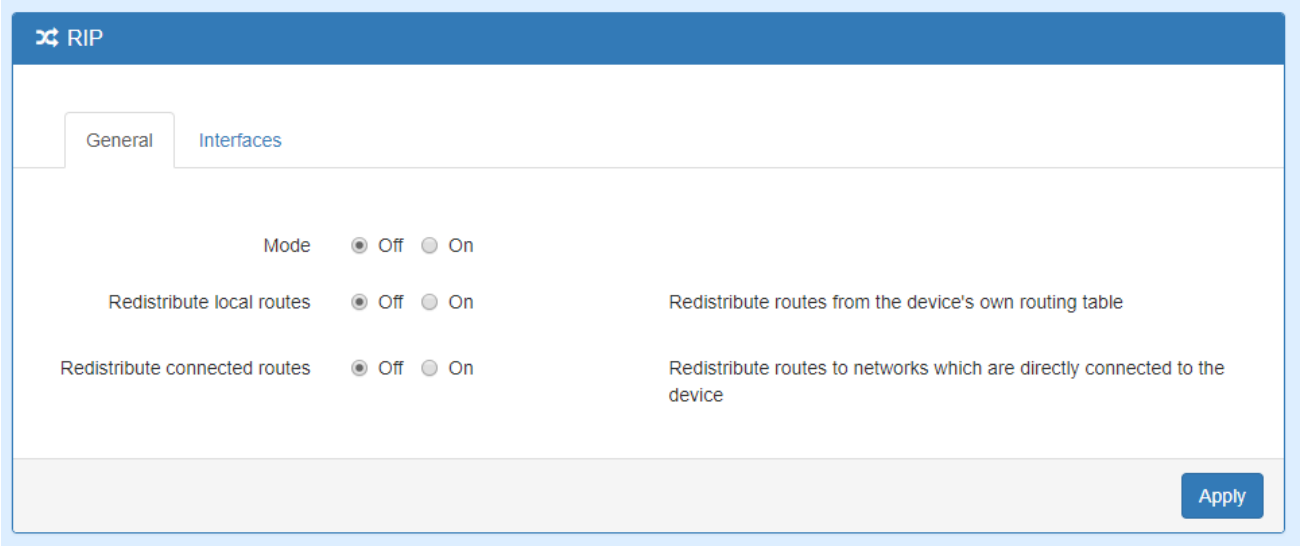
IP Routing > Static Route	
Item	**Description**
Mode	The setting is open for full network. Select from Off or On.
Status	
Destination	Show the status of destination from the setting section.
Gateway	Show the status of gateway from the setting section.
Interface	Show the status of interface from the setting section.
Protocol	Show the status of protocol from the setting section.

9.2 IP Routing > RIP

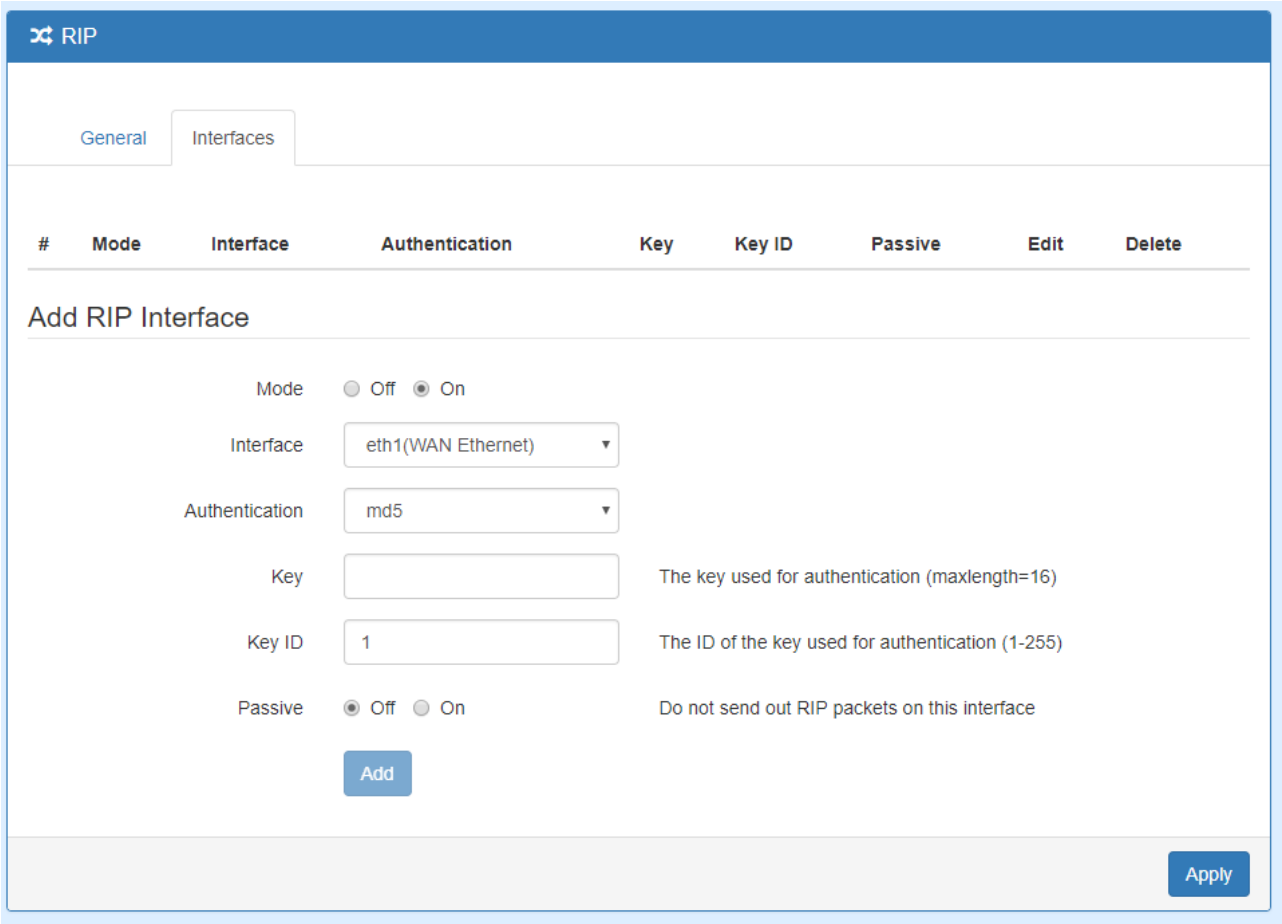
This section allows you to configure RIP and select the mode from Disable or Enable. The default is Disable.

Note:

RIP (Routing Information Protocol, RFC 2453) is an Interior Gateway Protocol (IGP) and is commonly used in internal networks. It allows a router to exchange its routing information automatically with other routers, and allows it to dynamically adjust its routing tables and adapt to changes in the network.



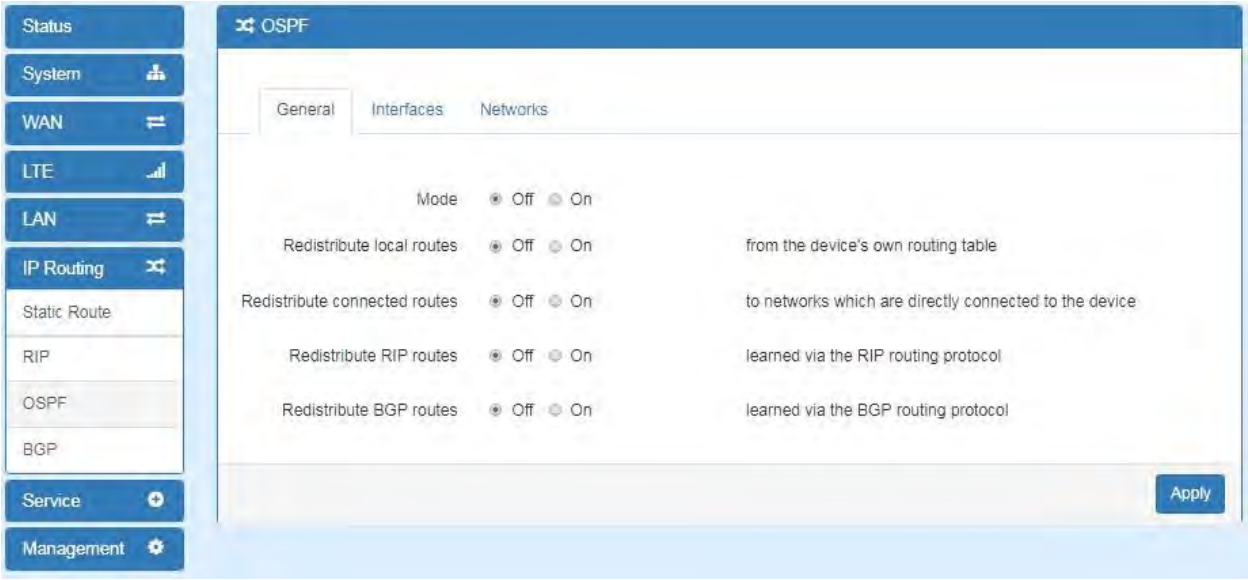
IP Routing > RIP > General	
Item	**Description**
General	
Mode	Select from Off or On to open or close RIP function.
Redistribute local routes	Select from Off or On to open or close redistribute local routes.
Redistribute connected routes	Select from Off or On to open or close redistribute connected routes.



IP Routing > RIP > Interfaces	
Item	**Description**
Interfaces	
Mode	Select from **Off** or **On** to use or not to use the RIP function in the interface.
Interface	Select from **eth1(WAN Ethernet)** or **LAN**.
Authentication	Select from **none** or **md5** to approve authentication. ***Note:*** Please offer **Key** and **Key ID** when you select **md5** to use HMAC-MD5.
Key	The key used for authentication (maxlength=16).
Key ID	The ID of the key used for authentication (1-255).
Passive	Select from **Off** or **On** to send out or not to send out RIP packets on this interface.

9.3 IP Routing > OSPF

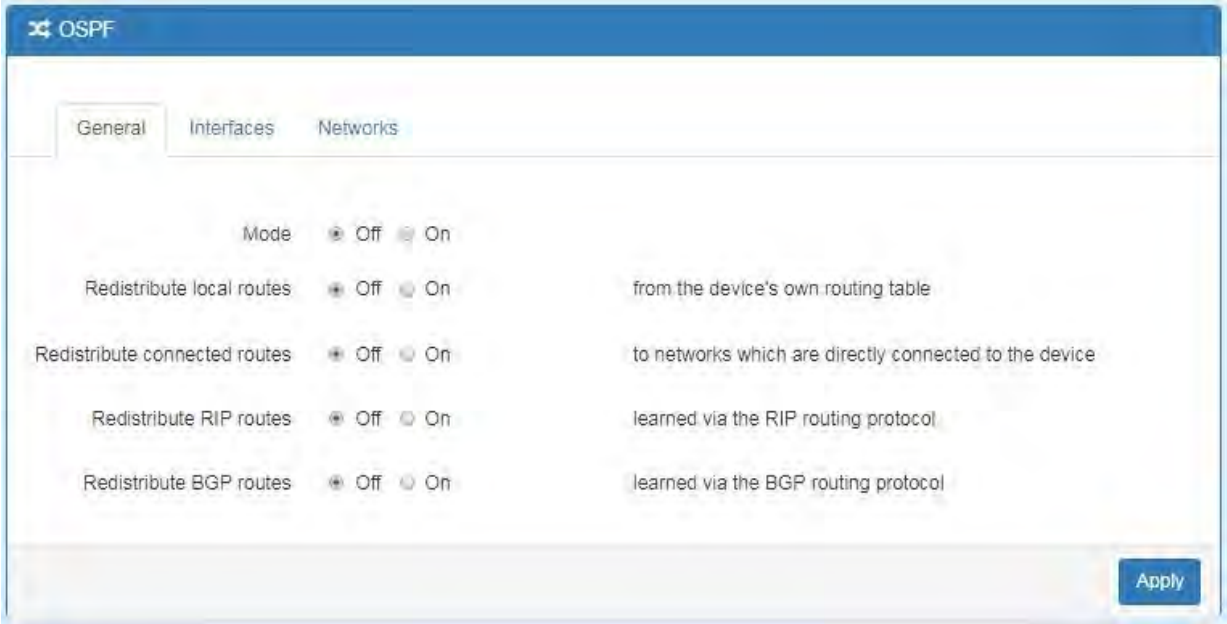
This section allows you to set up **OSPF** with three sub configurations, including General, Interfaces and Networks configuration.



(1) General Configuration

You can have these settings for General configuration.

- Mode
- Redistribute local routes
- Redistribute connected routes
- Redistribute RIP routes
- Redistribute BGP routes



IP Routing > OSPF > General	
Item	**Description**
General	
Mode	● Off：OSPF function is off. ● On：OSPF function is on.
Redistribute local routes	● Off：Not redistribute local routes from the device's own routing table. ● On: Redistribute local routes from the device's own routing table.
Redistribute connected routes	● Off：Not redistribute connected routes to networks which are directly connected to the device. ● On: Redistribute connected routes to networks which are directly connected to the device.
Redistribute RIP routes	● Off: Not redistribute RIP routes learned via the RIP routing protocol. ● On: Redistribute RIP routes learned via the RIP routing protocol.
Redistribute BGP routes	● Off: Not redistribute BGP routes learned via the RIP routing protocol. ● On: Redistribute BGP routes learned via the RIP routing protocol.

(2) Interfaces Configuration

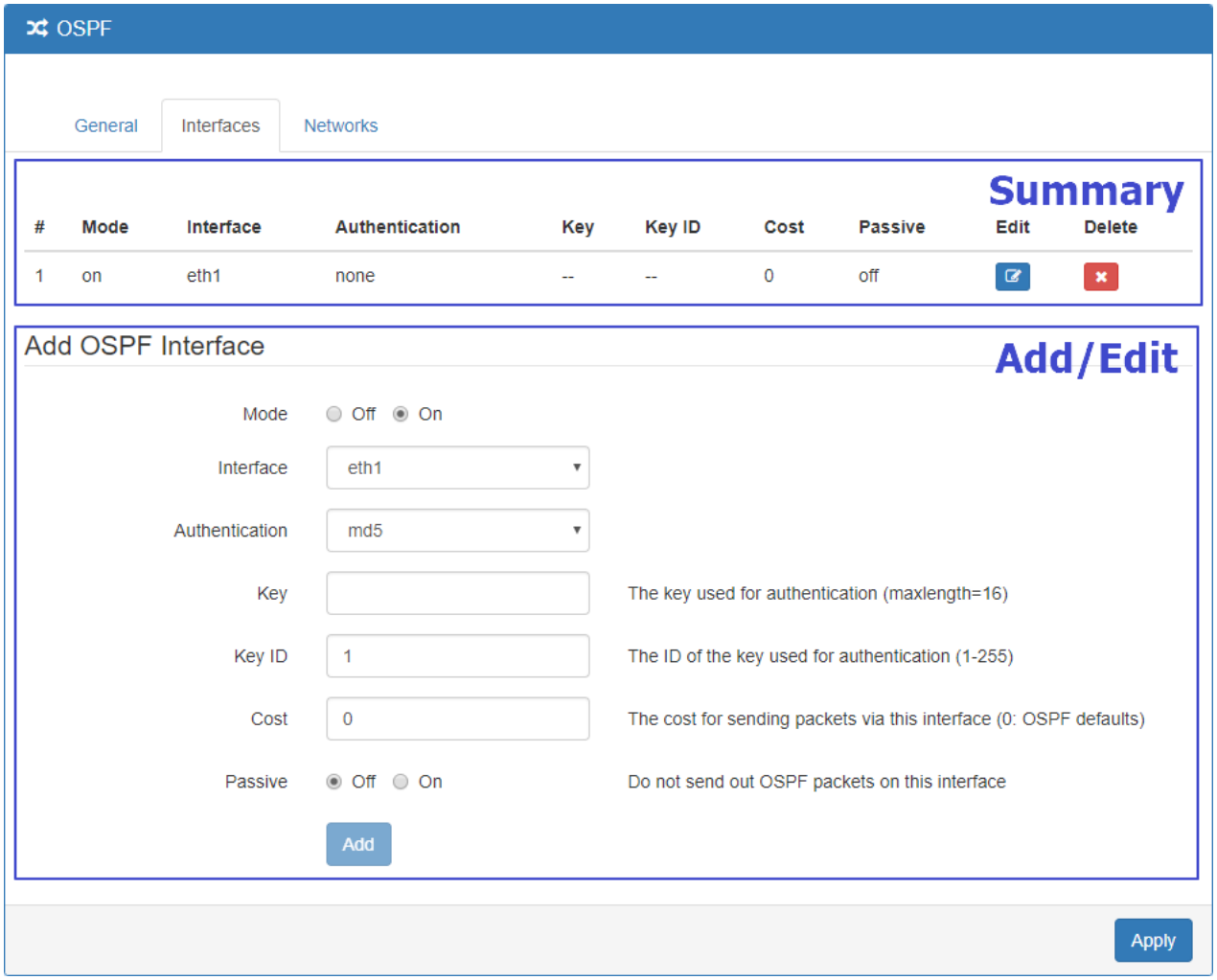
There are 2 parts for OSPF Interfaces configuration.

- OSPF Interfaces Summary

  Click **Edit** button to edit the existed interface.

  Click **Delete** button to delete the existed interface.
- Add/Edit OSPF Interface

  Note: This interface can be added at maximum is 2.



IP Routing > OSPF > Interfaces	
Item	**Description**
Interfaces	
Mode	Select from **Off** or **On** to use or not to use the OSPF function in the interface.
Interface	Select from **eth1(WAN Ethernet)** or **LAN**.
Authentication	Select from **none** or **md5** to approve authentication. ***Note:*** Please offer **Key** and **Key ID** when you select **md5** to use HMAC-MD5.
Key	The key used for authentication (maxlength=16).
Key ID	The ID of the key used for authentication (1-255).
Cost	The cost for sending packets via this interface (0: OSPF defaults).
Passive	Select from **Off** or **On** to send out or not to send out OSPF packets on this interface.

(3) Networks Configuration

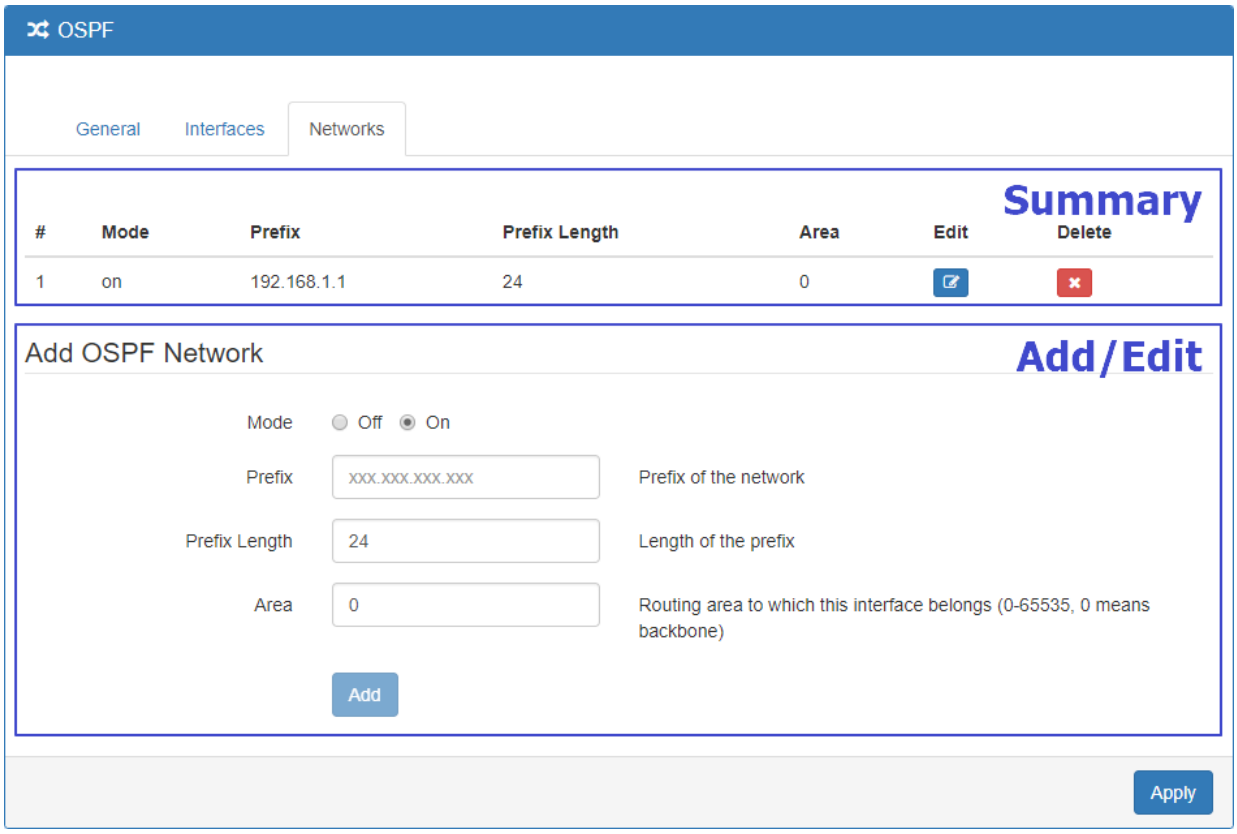
There are 2 parts for OSPF Networks configuration.

- OSPF Networks Summary

  You can edit and delete the existed OSPF networks.

- OSPF Networks Add/Edit

This sub configuration is used to configure all the networks, the maximum is 2.

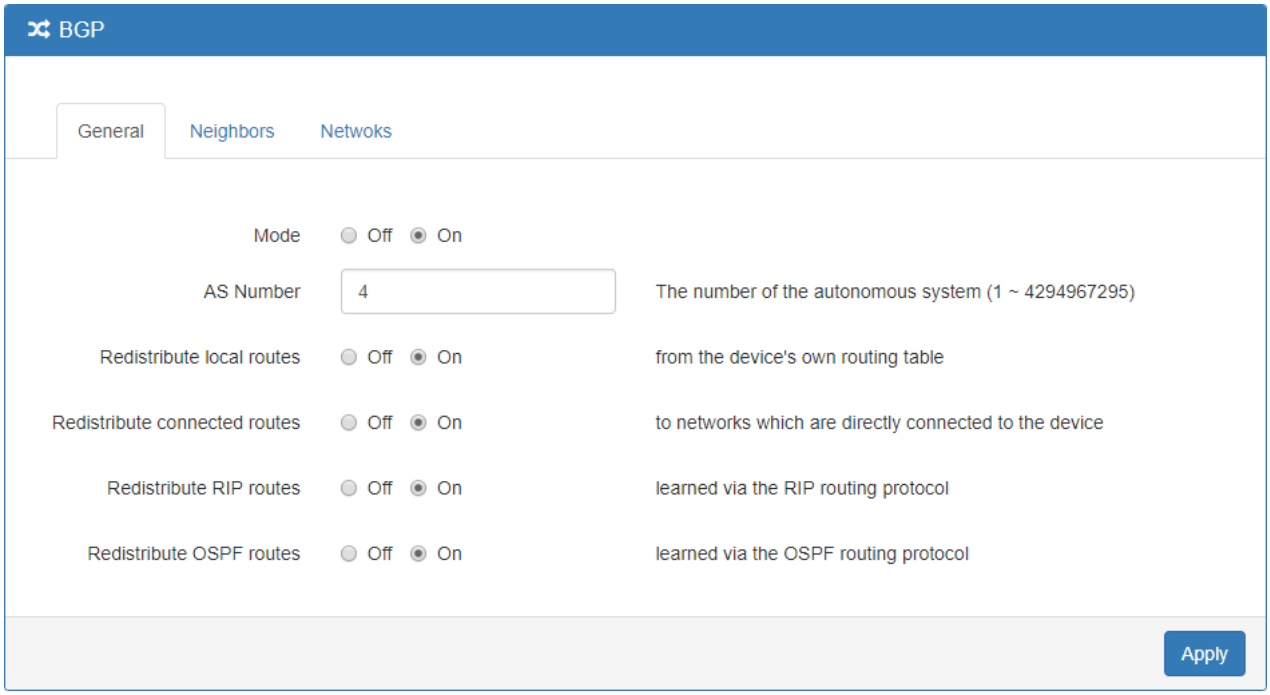


IP Routing > OSPF > Networks	
Item	**Description**
Networks	
Mode	Select from **Off** or **On** to enable the network setting.
Prefix	Set Prefix of the network
Prefix Length	Set Length of the prefix
Area	Routing area to which this interface belongs (0-65535, 0 means backbone)

9.4 IP Routing > BGP

This section allows you to set up **BGP** with three sub configurations, including General, Neighbors and Networks configuration.

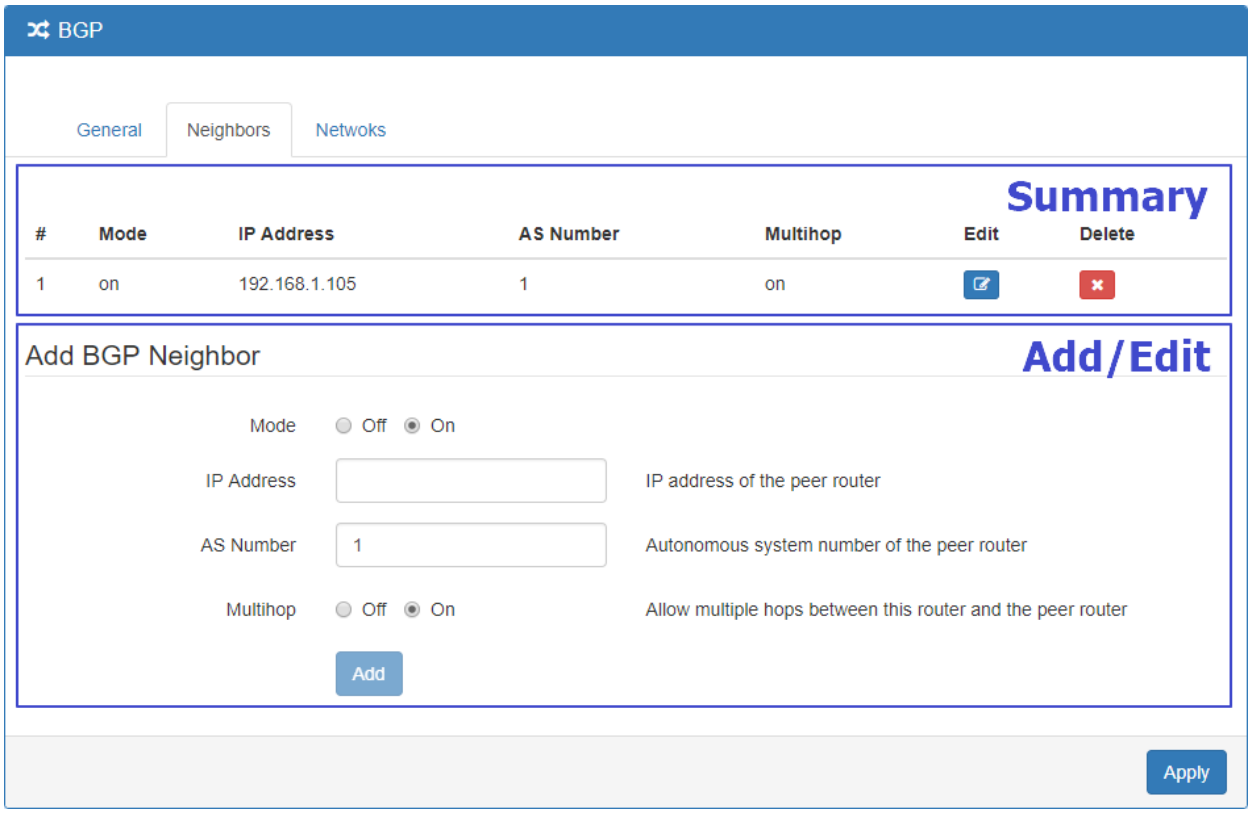
(1) General Configuration



IP Routing > BGP > General	
Item	**Description**
General	
Mode	• Off：BGP function is off. • On：BGP function is on.
AS Number	The number of the autonomous system (1 ~ 4294967295)
Redistribute local routes	• Off：Not redistribute local routes from the device's own routing table. • On ：Redistribute local routes from the device's own routing table.
Redistribute connected routes	• Off：Not redistribute connected routes to networks which are directly connected to the device. • On：Redistribute connected routes to networks which are directly connected to the device.
Redistribute RIP routes	• Off：Not redistribute RIP routes learned via the RIP routing protocol. • On：Redistribute RIP routes learned via the RIP routing protocol.
Redistribute OSPF routes	• Off：Not redistribute OSPF routes learned via the OSPF routing protocol. • On：Redistribute OSPF routes learned via the OSPF routing protocol.

(2) Neighbor Configuration

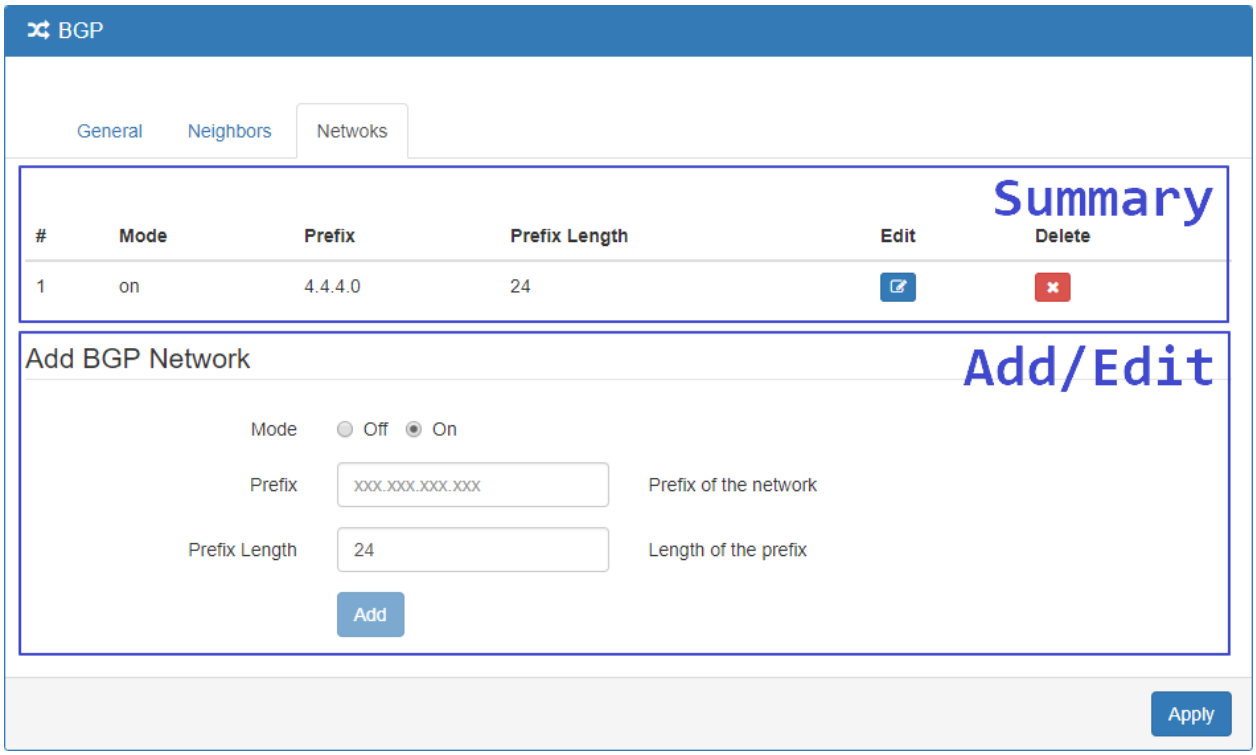
The neighbors sub configuration is used to configure all the BGP routers to peer with and the maximum neighbors is 16.



IP Routing > BGP > Neighbor	
Item	**Description**
Neighbor	
Mode	Select from **Off** or **On** to enable the neighbor setting
IP Address	Set IP address of the peer router
AS Number	Autonomous system number of the peer router
Multihop	Allow multiple hops between this router and the peer router

(3) Networks Configuration

The networks sub configuration allows to add IP network prefixes that shall be distributed via BGP in addition to the networks that are redistributed from other sources as defined on the general sub configuration and the maximum neighbors is 16.



IP Routing > BGP > Networks	
Item	**Description**
Networks	
Mode	Select from **Off** or **On** to enable the network
Prefix	Set Prefix of the network
Prefix Length	Set Length of the prefix

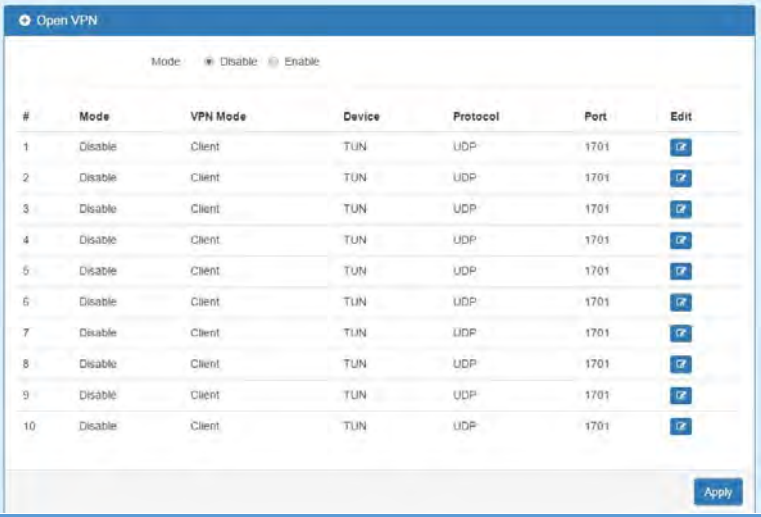
10 Configuration > Service

This section allows you to configure OpenVPN, IPSec, Port Forwarding, Dynamic DNS, DMZ, SNMP, IP Filter, MAC Filter, URL Filter, VRRP, MQTT, UPnP, SMTP, NAT, IP Alias and GRE.

10.1 Service > Configuration OpenVPN

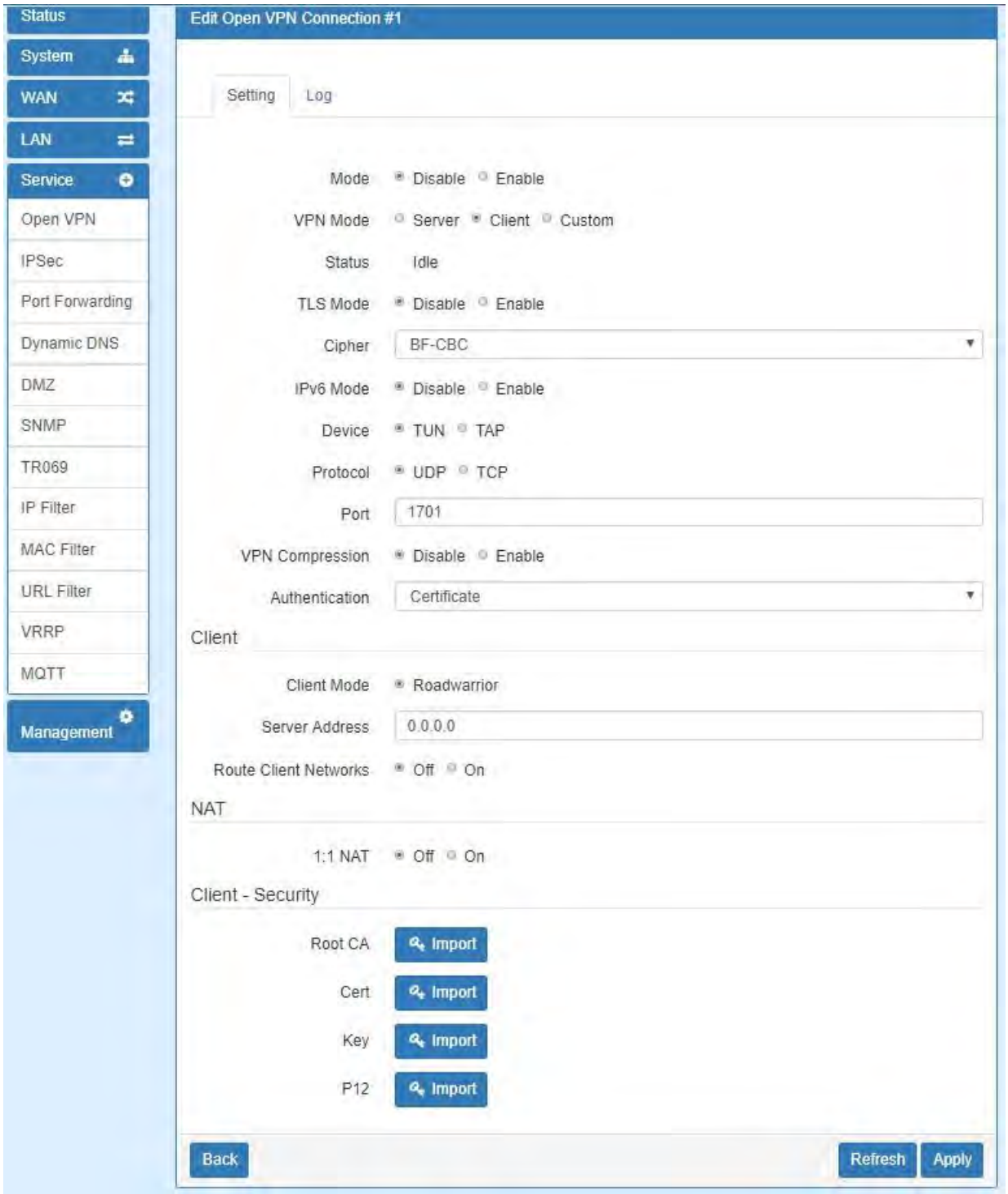
10.1.1 Edit OpenVPN Connection

(1) This section allows you to configure the OpenVPN parameters. The default mode is Disable. Click button to edit OpenVPN Connection.



#	Mode	VPN Mode	Device	Protocol	Port	Edit
1	Disable	Client	TUN	UDP	1701	
2	Disable	Client	TUN	UDP	1701	
3	Disable	Client	TUN	UDP	1701	
4	Disable	Client	TUN	UDP	1701	
5	Disable	Client	TUN	UDP	1701	
6	Disable	Client	TUN	UDP	1701	
7	Disable	Client	TUN	UDP	1701	
8	Disable	Client	TUN	UDP	1701	
9	Disable	Client	TUN	UDP	1701	
10	Disable	Client	TUN	UDP	1701	

(2) From **Setting** tab, you can set up the connection of OpenVPN.

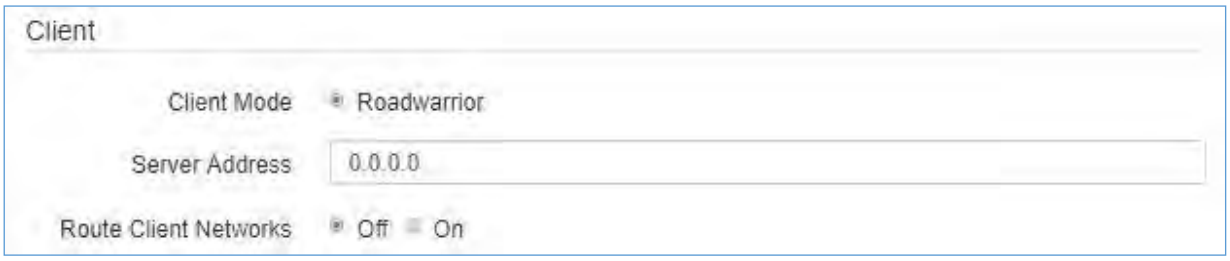


(3) From **Log** tab, the interface will be shown the status of connection to make you follow the suitation whenever is successful or fail connection.

Service > OpenVPN	
Item	**Description**
Mode	Turn on/off OpenVPN to select Disable or Enable.
VPN Mode	● Server: Tick to enable OpenVPN server tunnel. ● Client: Tick to enable OpenVPN client tunnel. The default is Client. ● Custom: This option allows user to use the .ovpn configuration file to quickly set up VPN tunnel with third-party server or use the OpenVPN advanced options to be compatible with other servers.
Status	Display the status of OpenVPN.
TLS Mode	Select from Disable or Enable for data security. The default is Disable.
Cipher	The OpenVPN format of data transmission.
IPv6 Mode	Select from Disable or Enable. The default is Disable.
Device	Select from TUN or TAP. The default is TUN.
Protocol	Select from UDP or TCP Client which depends on the application. The default is UDP.
Port	Enter the listening port of remote side OpenVPN server.
VPN Compression	Select Disable or Enable to compress the data stream. The default is Disable.
Authentication	● Select from two different kinds of authentication ways: Certificate or pkcs#12 Certificate. ● The pkcs#12 option is only available on the VPN client mode.

10.1.2 Set up OpenVPN Client

This section allows you configure the **OpenVPN client** route and authentication files. The files could be imported by clicking Import button and the file should be downloaded from OpenVPN server.

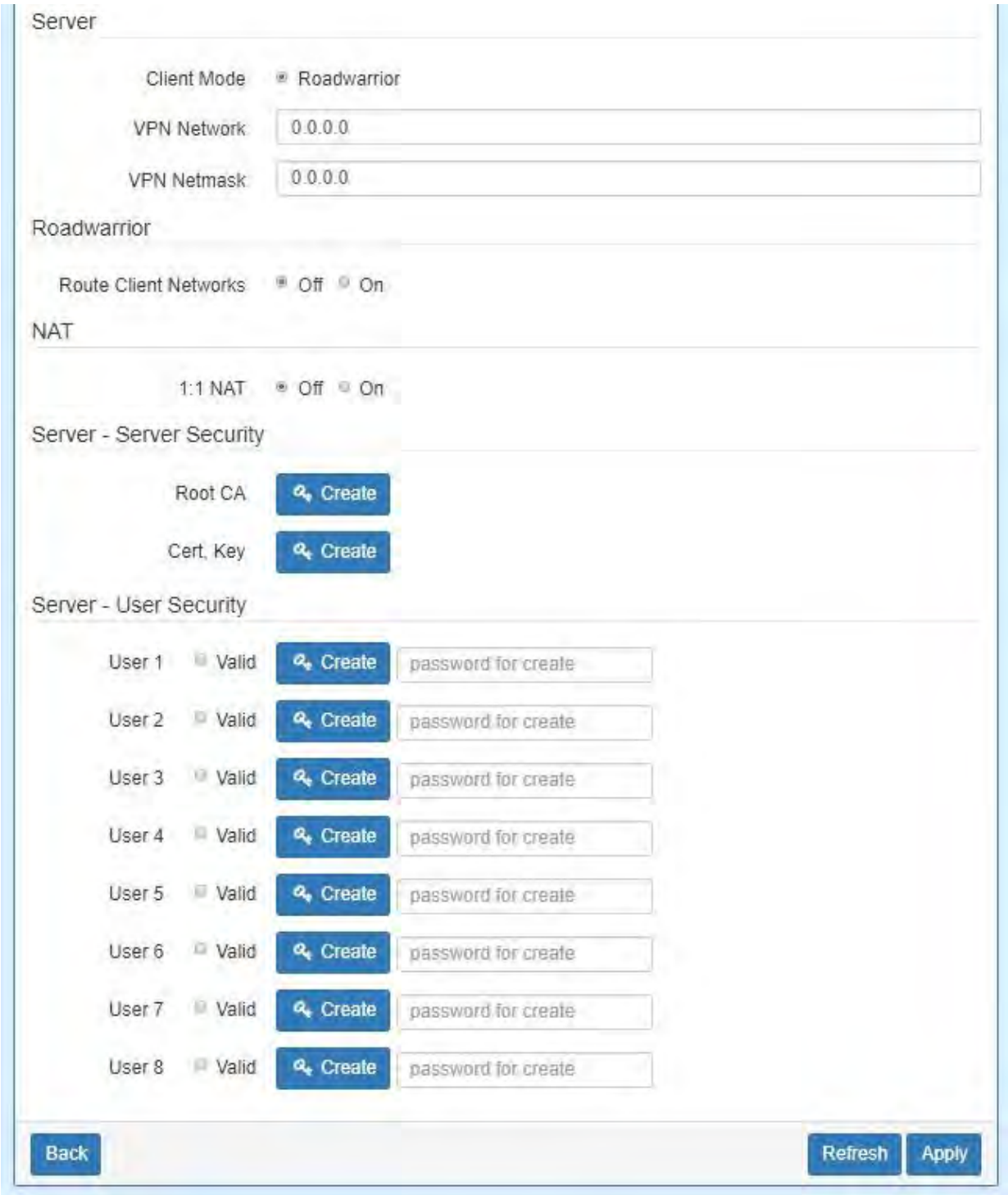


Service > OpenVPN > Client VPN Mode	
Item	**Description**
Client	
Client Mode	Only support the Roadwarrior mode.
Server Address	Fill in WAN IP of OpenVPN server.
Route Client Networks	Select from Off or On. This setting needs to match the server side. When enabled, the cellular router will auto apply the properly routing rules.
NAT	
1:1 NAT	• Tick to enable NAT Traversal for OpenVPN. This item must be enabled when the router under NAT environment. • Select from Off or On. • When two routers' LAN Subnet are same and create OpenVPN tunnels, this function should be turned on.
Client-Security	
Root CA	The Certificate Authority file of OpenVPN server could be downloaded from OpenVPN server.
Cert	The certification file is for OpenVPN client, which could be downloaded from OpenVPN server.
Key	The private key file is for OpenVPN client, which could be downloaded from OpenVPN server.
P12	The PKCS#12 file is for OpenVPN client, which could be downloaded from OpenVPN server.

10.1.3 Set up OpenVPN Server

This section allows you to configure the **server status of VPN Mode**.

Note: When selecting the On option of Route Client Networks, the OpenVPN server will route the client traffic or not. You should fill in the client IP and netmask when this option is enabled.



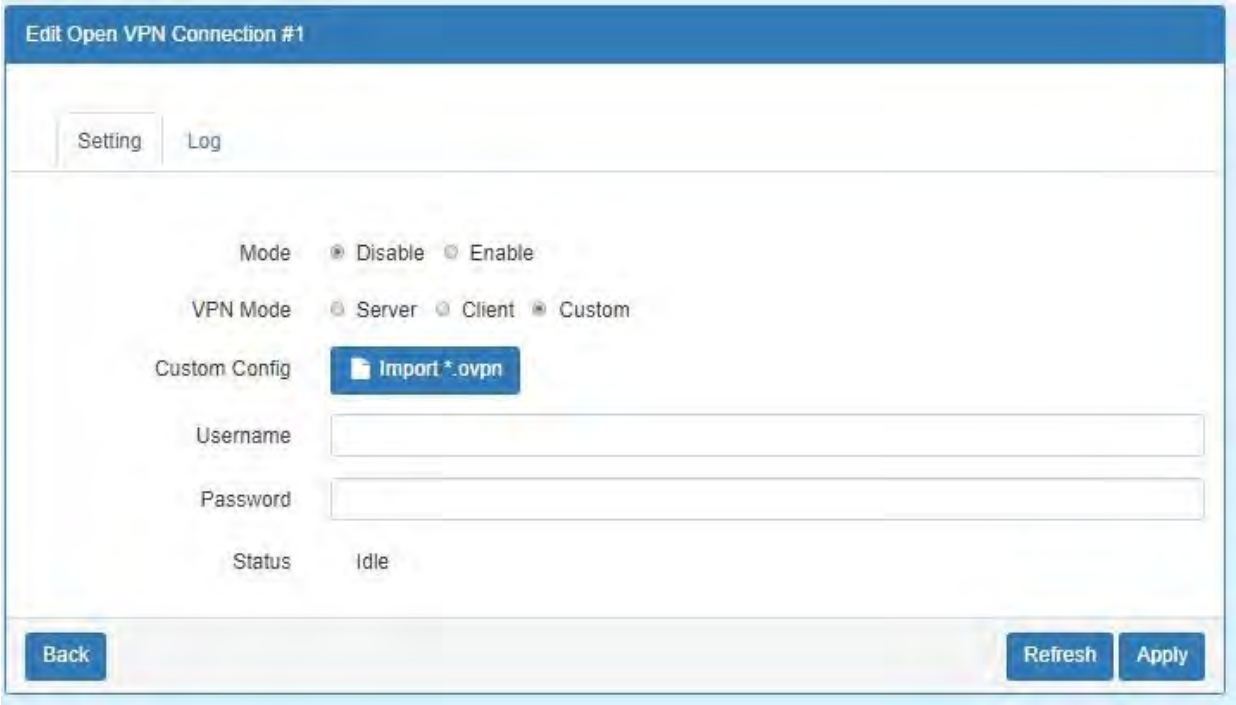
Service > OpenVPN > Server VPN Mode	
Item	**Description**
Server	
Client Mode	Only support the Roadwarrior mode.
VPN Network	The network ID for OpenVPN virtual network.
VPN Netmask	The netmask for OpenVPN virtual network.
Roadwarrior: Route Client Networks	Select from Off or On. The OpenVPN server will route the client traffic or not. User should fill in the client IP and netmask when this option is enabled.
NAT	
1:1 NAT	● Tick to enable NAT Traversal for OpenVPN. This item must be enabled when router under NAT environment. ● Select from Off or On. The default is Off. ● When two routers' LAN Subnet are same and create OpenVPN tunnels, this function is turned on.
Server- Server Security	
Root CA	Create Root CA key.
Cert, Key and DH	Create Cert, Key and DH key.
Server- User Security	
User 1 - User 8	According to your requirement, you can create different kinds of user security key from User 1 to User 8.

10.1.4 Set up OpenVPN Custom

For **Custom of VPN Mode**, this section helps you use the .ovpn configuration file to quickly set up VPN tunnel with third-party server or use the OpenVPN advance options to be compatible with other servers.

Note:

- When clicking the Import button, you can import third-party OpenVPN configuration that find out from Internet and save the document into your server or PC. After importing the file, the interface will show  button to click  for displaying the information and to click  for downloading the file.
- For third-party OpenVPN configuration, suggest from http://www.vpngate.net/en/



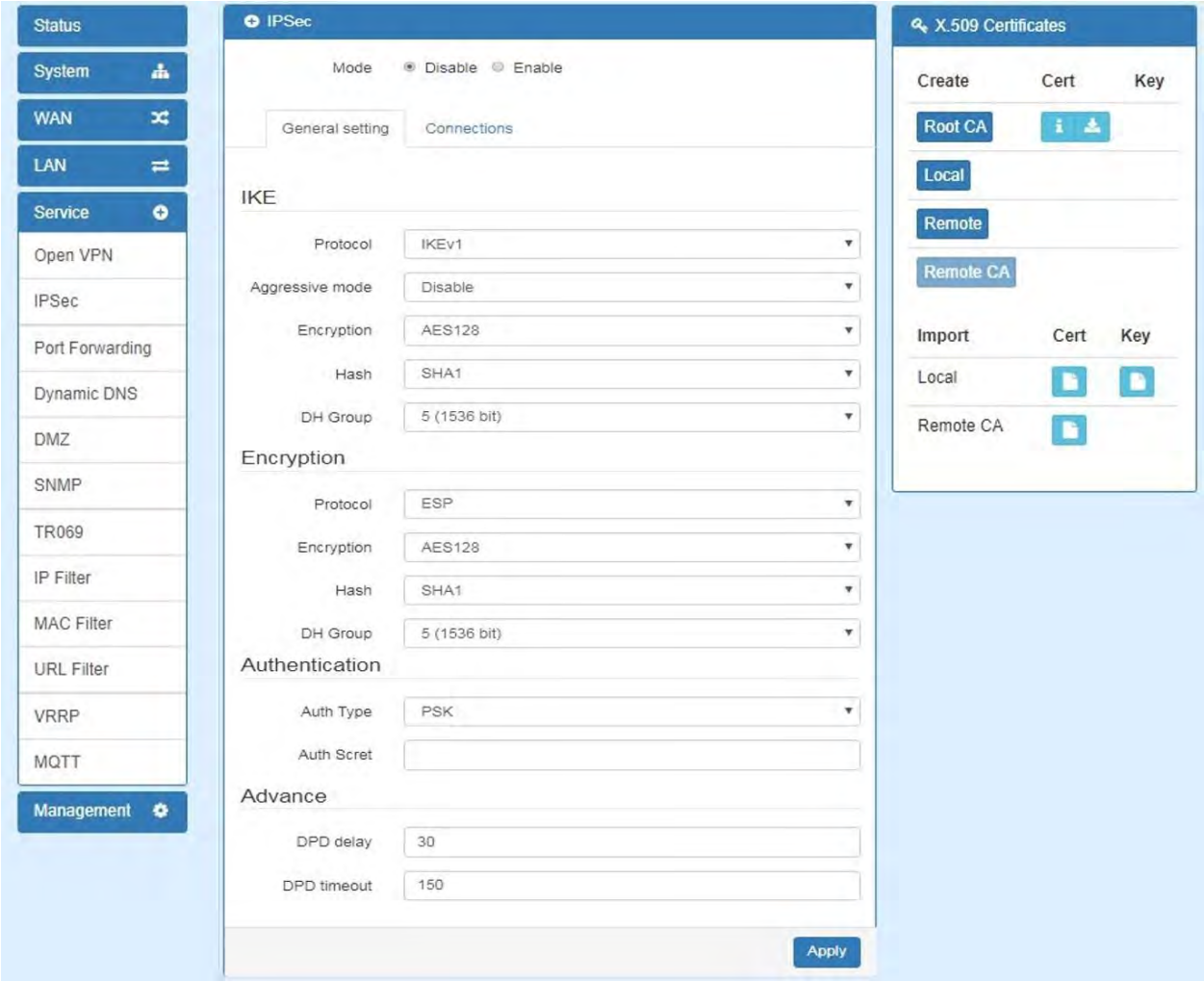
Service > OpenVPN > Custom VPN Mode	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
VPN Mode	Select from custom mode.
Custom Config	Import OpenVPN configuration.
Username	Fill in the username if the imported file has already set up the username.
Password	Fill in the password if the imported file has already set up the password.
Status	Display the connection status of OpenVPN, such as IP address and the connected time.

10.2 Service > Configuration IPSec

This section allows you to set up IPSec Tunnel. The seting has two tags, General setting and Connections.

10.2.1 IPSec > General setting

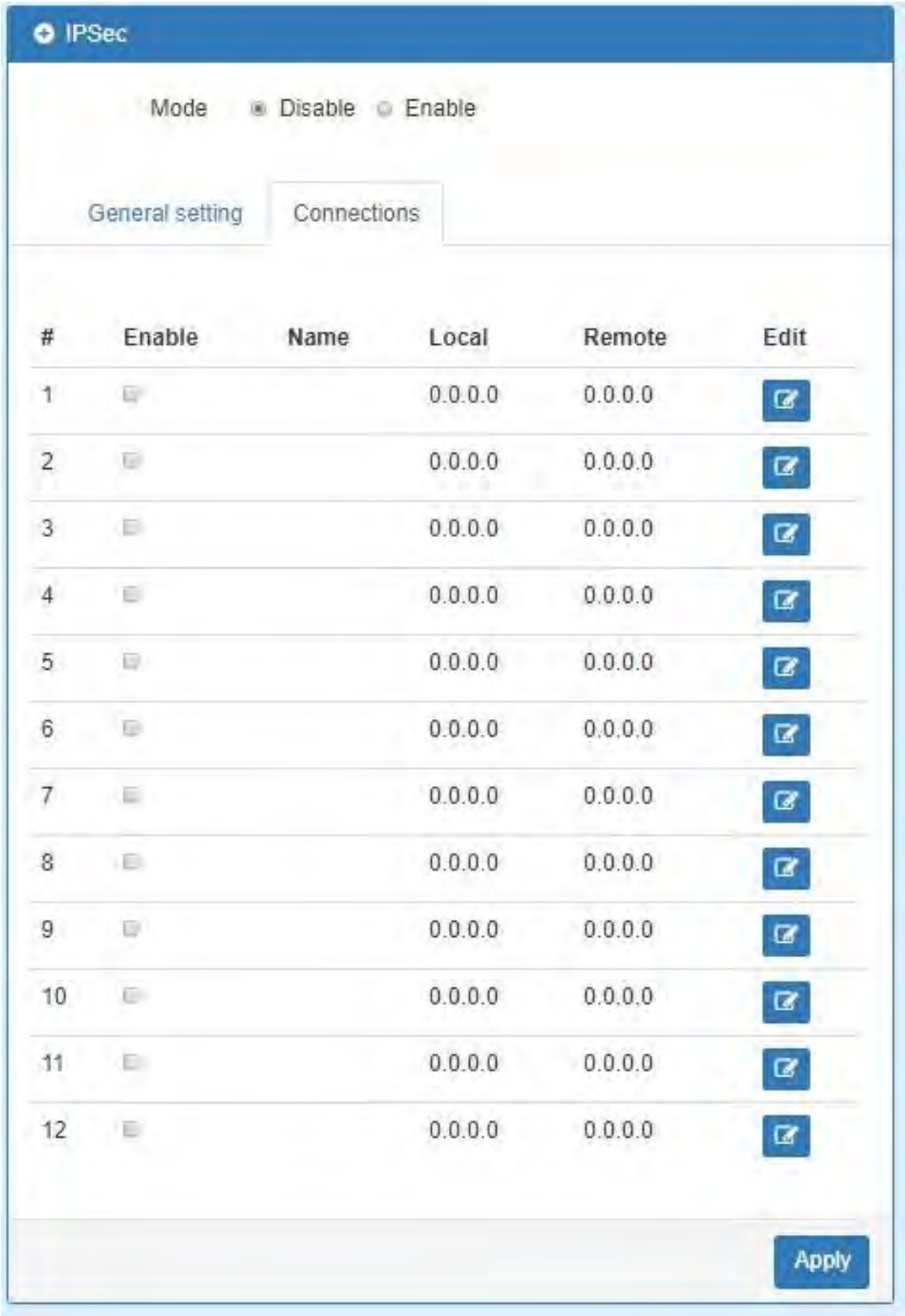
For **General setting**, you can set up **IKE**, **Encryption** and **Authentication**. The General setting for the local and remote side should be the same when using Net-to-Net application.

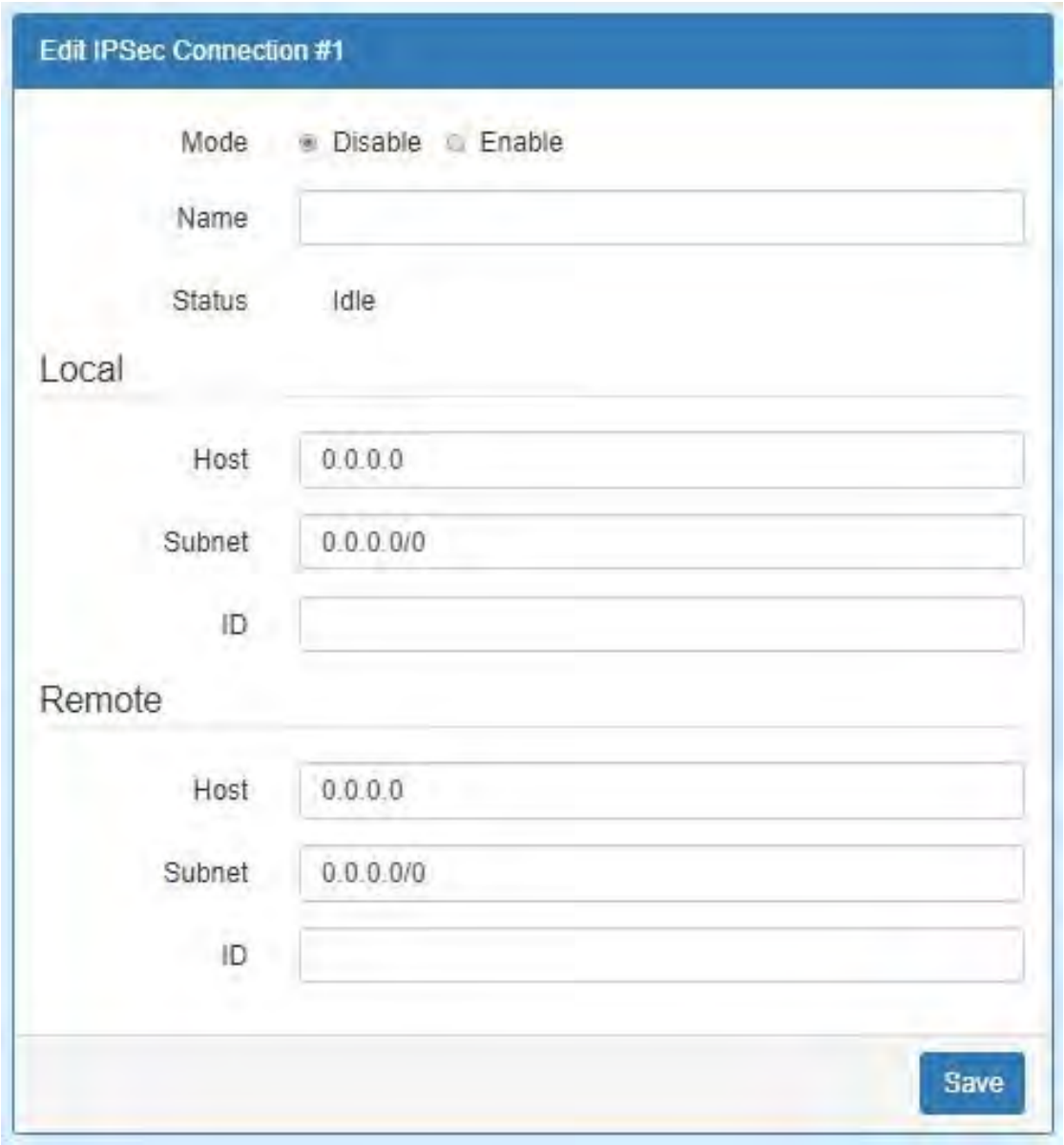


Service > IPSec > General setting	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
IKE	
Protocol	Select from IKEv1 or IKEv2.
Aggressive mode	Select from Enable or Disable (default). (**Note:** The Aggressive mode is for IKEv2.)
Encryption	Select from AES128 (default), AES192, AES256 or 3DES.
Hash	Select from MD5, SHA1 (default) or SHA256.
DH Group	Select from 1(768 bit), 2(1024 bit), 5(1536 bit) (default)、14(2048 bit)、15(3072 bit)、16(4096 bit)、17(6144 bit) or 18(8192 bit).
Encryption	
Protocol	Select from ESP.
Encryption	Select from AES128 (default), AES192, AES256, 3DES or DES.
Hash	Select from MD5, SHA1 (default) or SHA256.
DH Group	Select from off, 1(768 bit), 2(1024 bit), 5(1536 bit) (default)、14(2048 bit)、15(3072 bit)、16(4096 bit)、17(6144 bit) or 18(8192 bit).
Authentication	
Auth Type	Select from PSK (default) or RSA. (**Note:** The EAP-TLS is for IKEv2.)
Auth Scret	The password is for PSK authentication type.
Advance	
DPD delay (Deed Peer Detection)	Define the period time interval to detect dead peers. The default is 30 seconds.
DPD timeout (Deed Peer Detection)	Define the timeout interval, after which all connections to a peer are deleted in case of inactivity. The default is 150 seconds.

10.2.2 IPSec > Connections

For **Connections** tab, the web UI provides the overview for each connection. Click button to edit IPSec connection and set up the local and remote side.


IPSec
Mode
Disable
Enable
General setting
Connections
Enable Name Local Remote Edit
1 0.0.0.0 0.0.0.0
2 0.0.0.0 0.0.0.0
3 0.0.0.0 0.0.0.0
4 0.0.0.0 0.0.0.0
5 0.0.0.0 0.0.0.0
6 0.0.0.0 0.0.0.0
7 0.0.0.0 0.0.0.0
8 0.0.0.0 0.0.0.0
9 0.0.0.0 0.0.0.0
10 0.0.0.0 0.0.0.0
11 0.0.0.0 0.0.0.0
12 0.0.0.0 0.0.0.0
Apply



Service > IPSec > Connections	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Name	Fill in the name of IPSec Tunnel.
Status	Display the connection status of IPSec.
Local	
Host	Fill in the WAN IP of cellular router.
Subnet	Fill in the subnet for the LAN of cellular router.
ID	The connection ID of IPSec local side.
Remote	
Host	Fill in the granted remote IP. If no limitation, keep blank.
Subnet	Fill in the granted remote subnet. If no limitation, keep blank.
ID	The connection ID of IPSec Remote side.

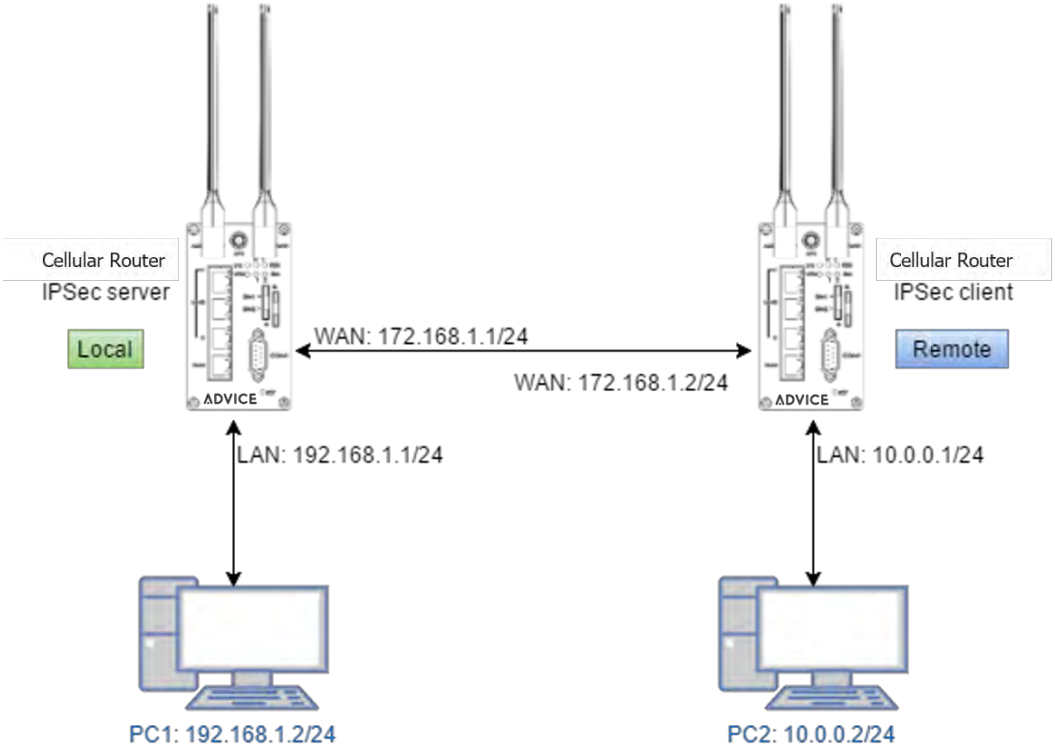
10.2.3 IPSec > The setting of X.509 Certificates

The interface shows the setting items of X.509 Certificates.

- You need to create the IPSec Security Keys by clicking Create button, including Root CA, Local, Remote and Remote CA. E.g. To create Root CA file, click the Root CA button.
- For the IPSec connection, the client should set up properly Root CA, Local, Remote and Remote CA key and cert files. The files could be downloaded by clicking Download button after the file genearted.
- You can import the files of local and remote CA from the server.

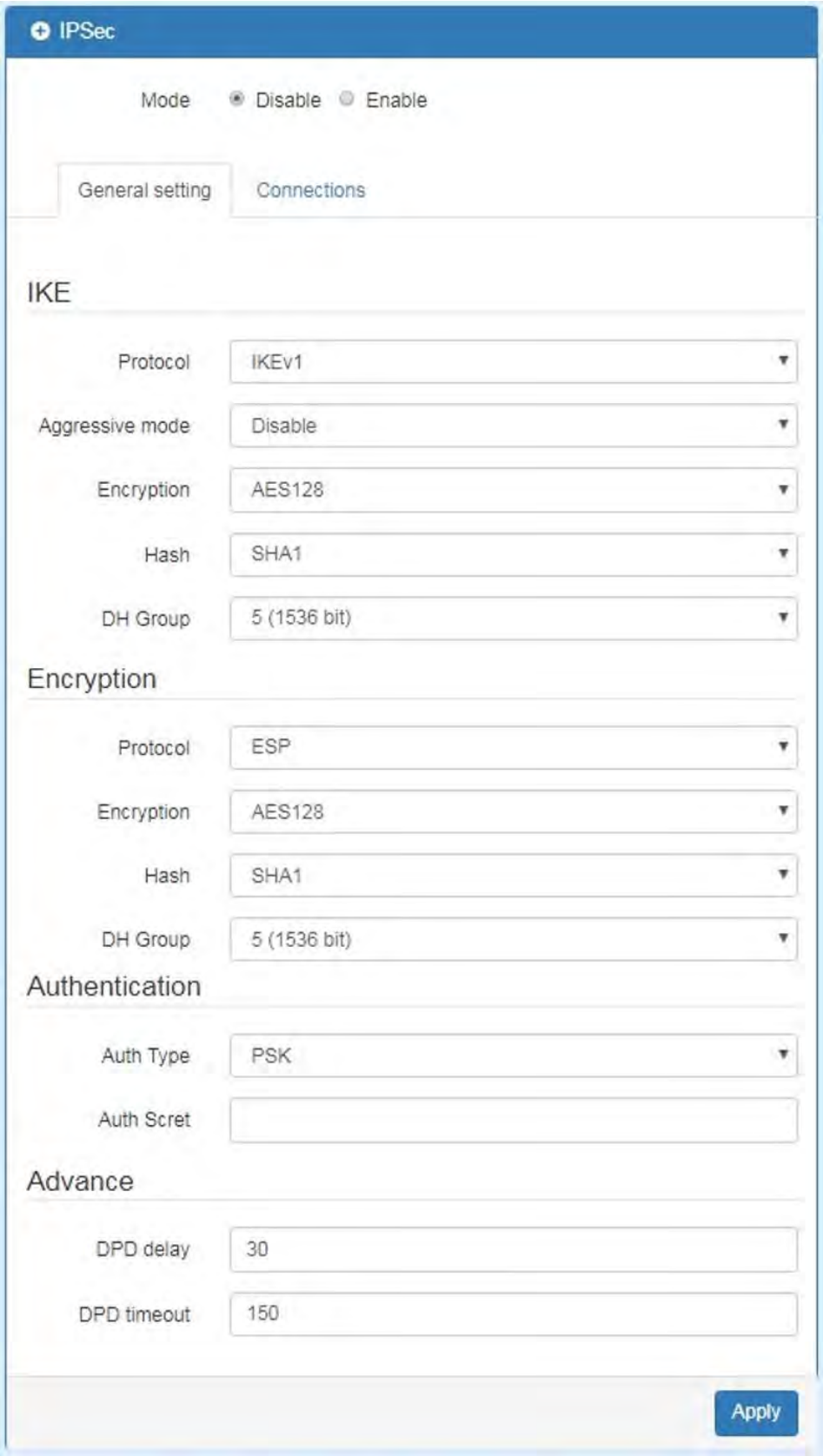
10.2.4 IPSec > Net-to-Net Configuration

In this case, the IPSec VPN tunnel uses the two LAN side subnet clouds and makes them communicate each other. There are two part settings for the Cellular router IPSec feature.



General setting

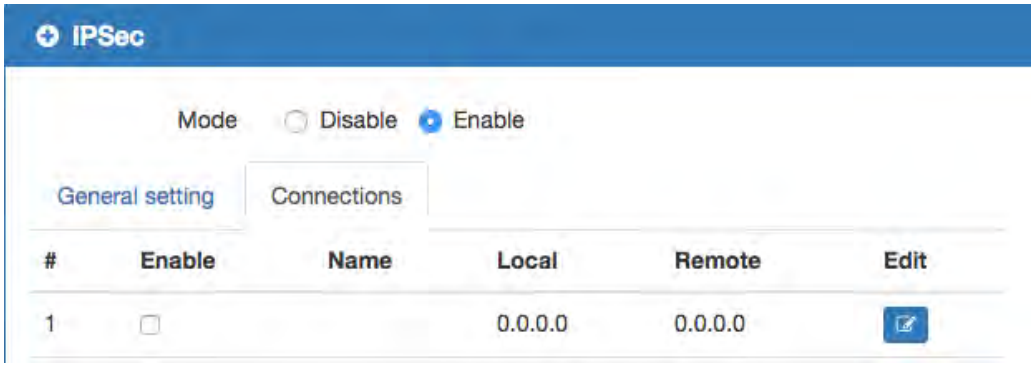
The first part is the general setting, it provides the IPSec basic setting and authentication configuration. The psk (Pre-shared key) is as an authentication option to simplify the progress. The general setting for the local and remote side should be used the same setting.



Connections Setting

The second part is the connection setting, you can configure the local and the remote side setting for each connection.

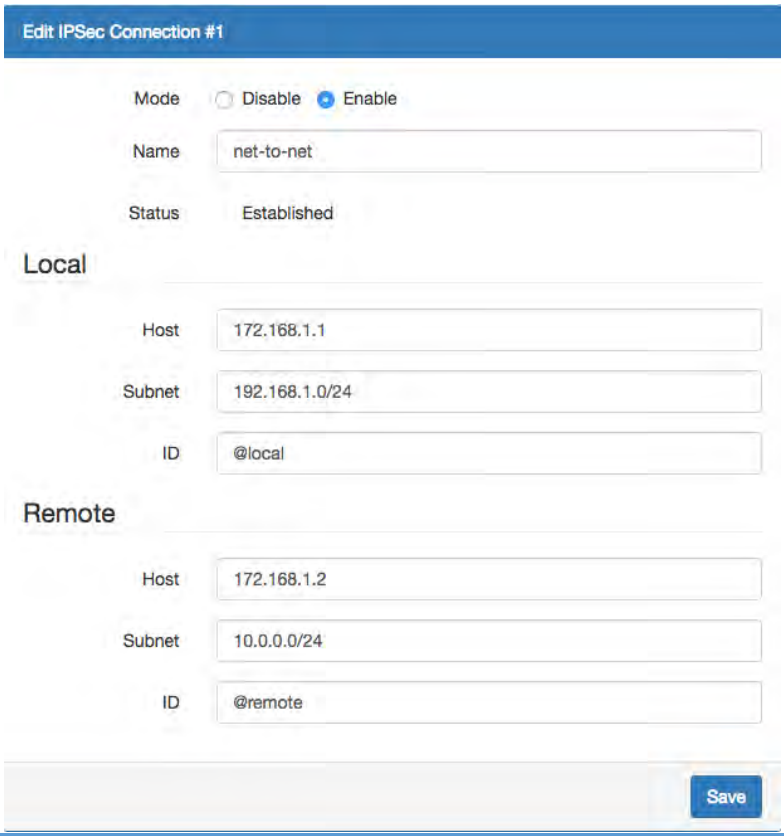
For the Net-to-Net scenario, you can configure the information of **Host**, **Subnet** and **ID** for the local and remote side. In this case, the #1 connection is edited from connections tab for setting up the Net-to-Net configuration.



- Local Side

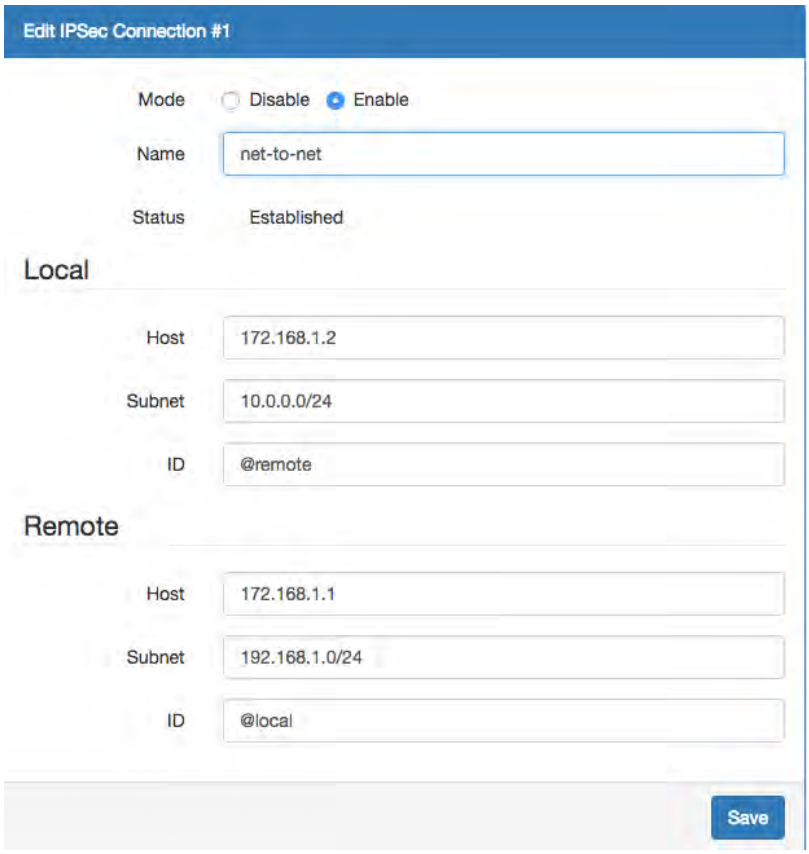
First, fill up the local Host and Subnet fields by the network information of IPSec server.
And, use the network information of IPSec client to fill up the remote setting.
Then, specify the ID for the both sides.
In this case, the IDs for the local and remote side are named as @local and @remote respectively.

Note: The ID should be started with @ symbol. The above settings will make the traffic between 192.168.1.0/24 and 10.0.0.0/24. They can be forwarded by IPSec tunnel.



- Remote Side

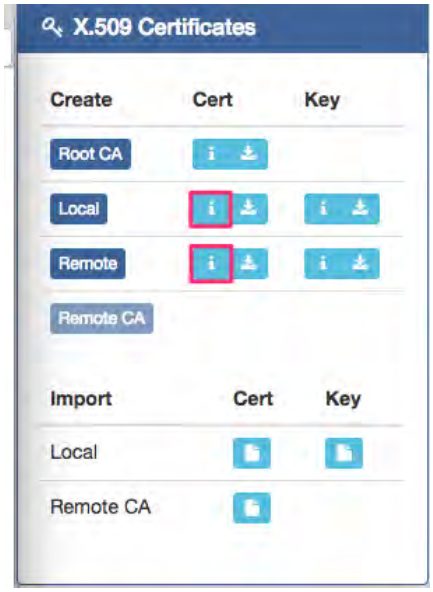
The setting for remote side is similar to Local Side. Just swap the local settings with the remote setting.

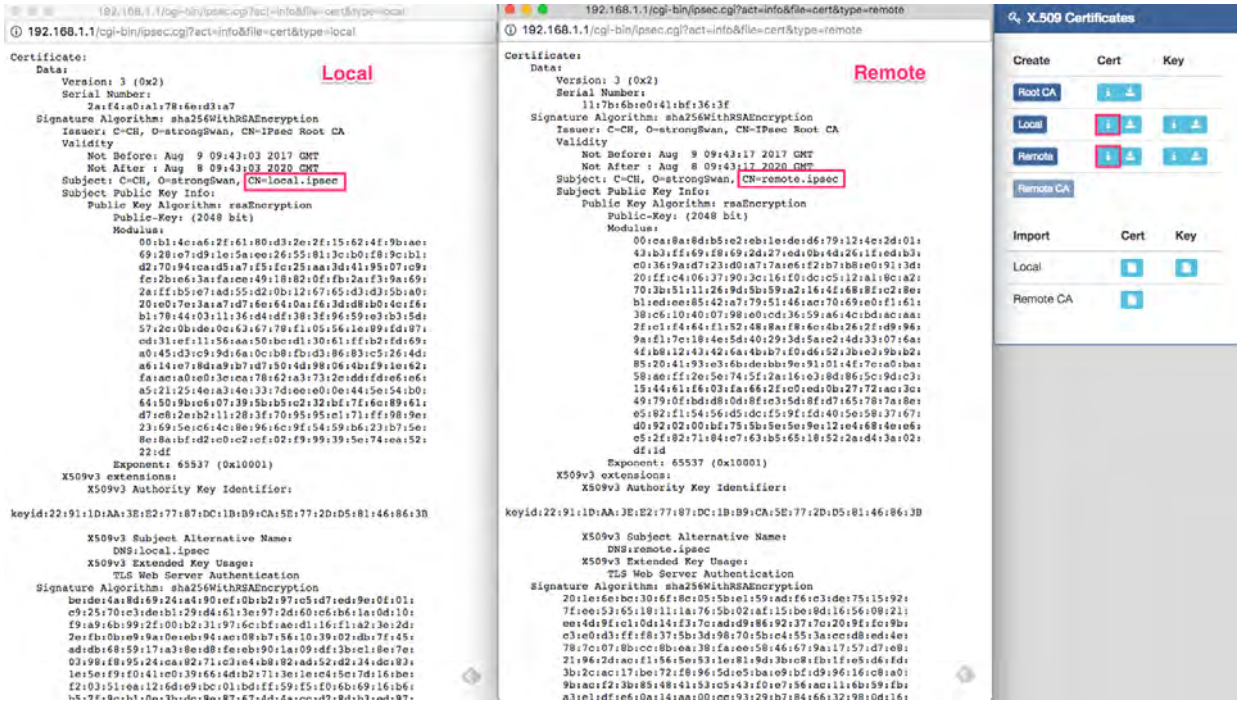


Net-to-Net (Pre-shared key)

When the **rsa** authentication is used, there will have some different with psk. In the **rsa** authentication, the **id** of connections is corresponded with the certificate **CN** field for the both sides.

For the Cellular router IPSec certificate generation, it generates the local and remote side certificates with **@local.ipsec** and **@remote.ipsec**. (The certificate information can be queried by  the information button.)





Import Certificate

For the IPSec remote side, it requires the certificates from local side to authenticate the IPSec connection. Thus, you need to download the Root CA, remote cert and key from local side. And, import them to the remote side.

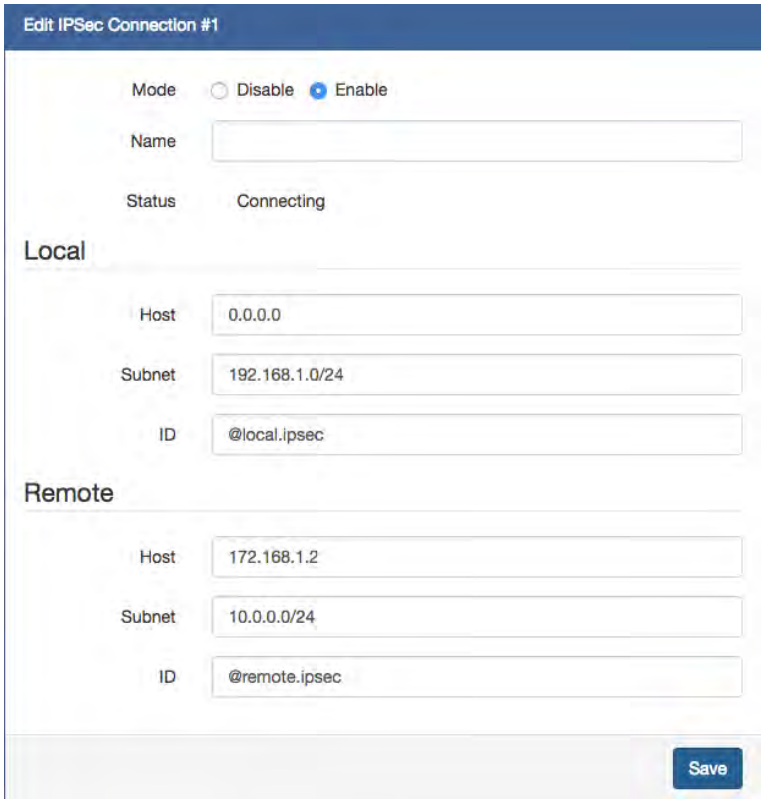
The mapping is as below:

1. Root CA (Local side) -> Import Remote CA (Remote side)
2. Remote Cert (Local side) -> Import Local Cert (Remote side)
3. Remote Key (Local side) -> Import Local Key (Remote side)

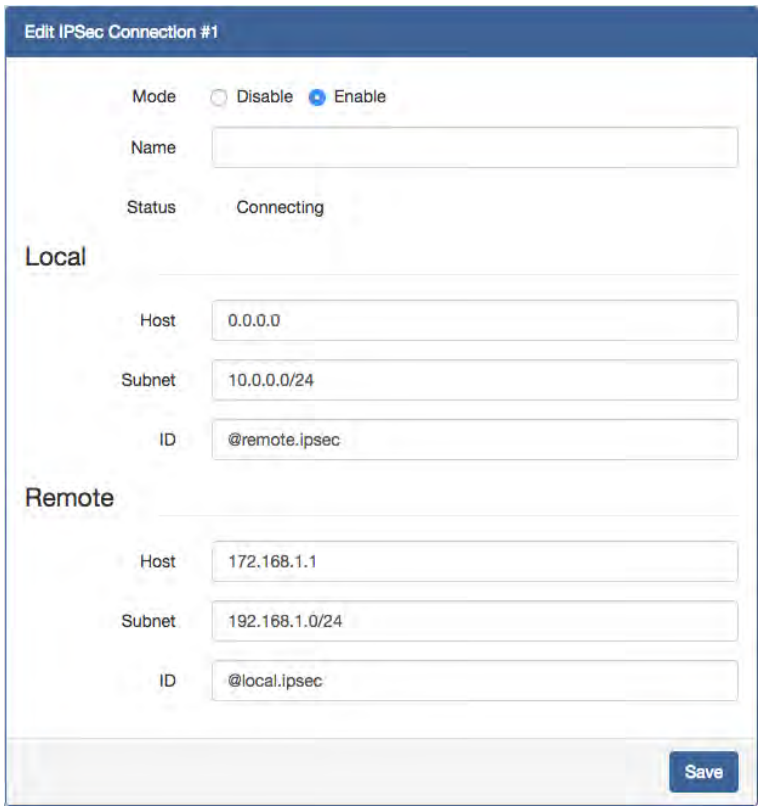
For Connection setting, the mapping of connection IDs like the following table.

Certificate	IPSec local side	IPSec remote side
Local	@local.ipsec	@remote.ipsec
Remote	@remote.ipsec	@local.ipsec

Local Side



Remote Side

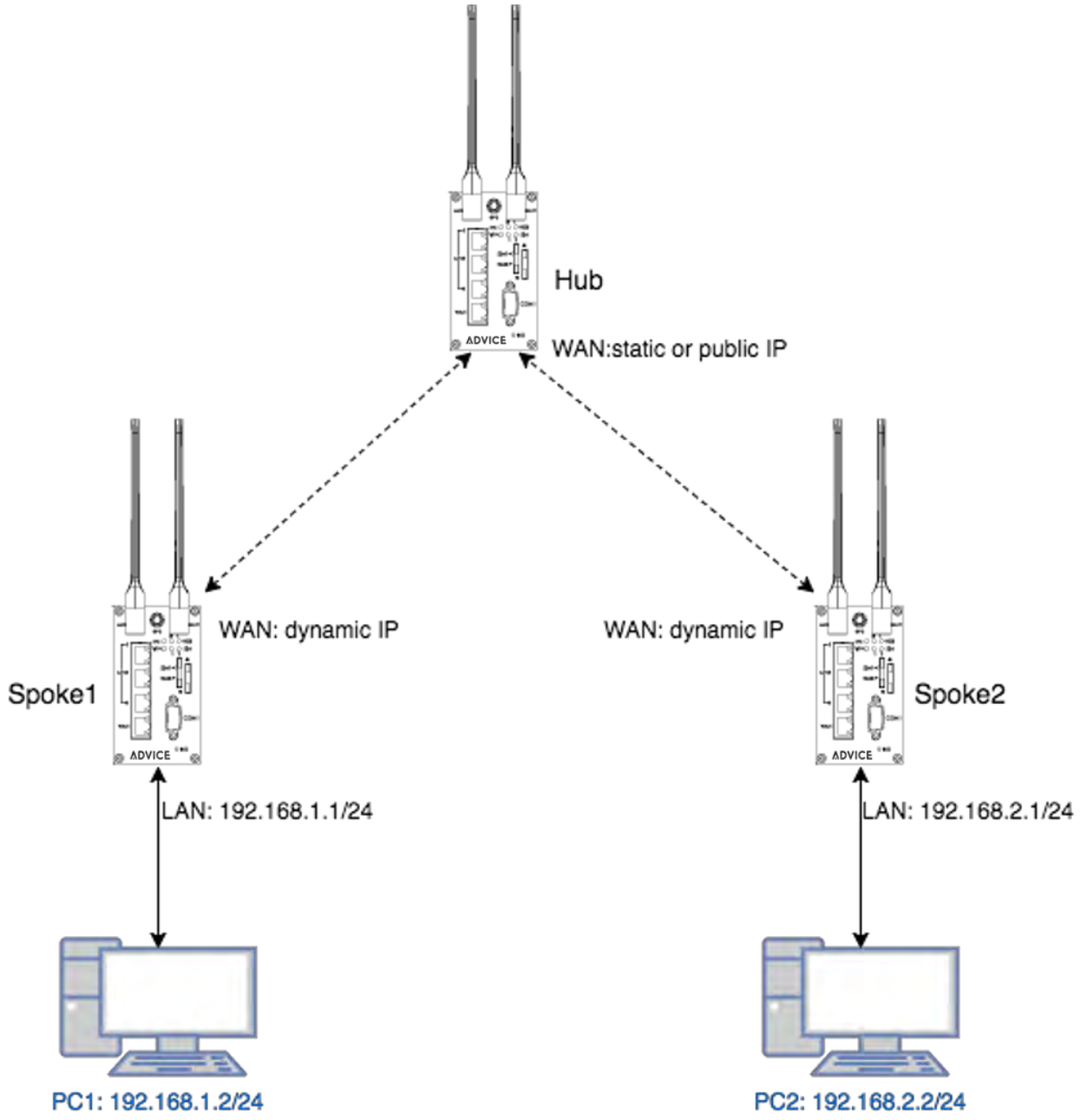


10.2.5 IPSec > Hub-Spoke Topology

This section explains how to sets Hub-Spoke Topology. Connect two (or more) gateways to a central one.

This requires one connection between each spoke and the central hub (**n - 1** connections for **n** gateways)

For example, we use three gateways to setup this topology. It should like the following figure.



After some configuration setup, the PC1 and PC2 could communicate each other through the Hub gateway.

Note:

(1)This example should be running under the pre-shared key authentication.

(2)This example will cause the cellular router internet traffic loss (Only handle IPSec VPN traffic)

- **Hub configuration**

In this example, we have two spoke on the topology. Thus, the Hub needs to setup two IPSec connections for each spoke.

The settings should be like the following table.

Attribute	Hub's conn 1	Hub's conn 2
Local host		
Local subnet	0.0.0.0/0	0.0.0.0/0
Local id		
Remote host		
Remote subnet	192.168.1.0/24	192.168.2.0/24
Remote id		

- **Spoke configuration**

In this example, the spoke gateways only need to setup one IPSec connection.

The setting needs to correspond the hub gateway settings, it should be like the following table.

Attribute	Hub's conn 1	Hub's conn 2
Local host		
Local subnet	192.168.1.0/24	192.168.2.0/24
Local id		
Remote host	Hub's WAN IP	Hub's WAN IP
Remote subnet	0.0.0.0/0	0.0.0.0/0
Remote id		

Note: The Remote subnet **0.0.0.0/0**, it will make the all traffic into the IPSec VPN tunnel.

10.3 Service > Configuration Port Forwarding

This section allows you to set up Port Forwarding and click edit button to configure.

Port Forwarding

Mode Disable Enable

#	Mode	Description	Protocol	Edit
1	Disable	ssh	TCP	
2	Disable		TCP	
3	Disable		TCP	
4	Disable		TCP	
5	Disable		TCP	
6	Disable		TCP	
7	Disable		TCP	
8	Disable		TCP	
9	Disable		TCP	
10	Disable		TCP	
11	Disable		TCP	
12	Disable		TCP	
13	Disable		TCP	
14	Disable		TCP	
15	Disable		TCP	
16	Disable		TCP	

Apply

Edit Port Forwarding Entry #1

Mode Disable Enable

Description ssh

Protocol TCP UDP

Source Port Begin 22

Source Port End 22

Destination IP 0.0.0.0

Destination Port Begin 22

Destination Port End 0

Save

Service > Port Forwarding	
Item	**Description**
Mode	Turn on/off Port Forwarding to select Disable or Enable. The default is Disable.
Description	Descript the name of Port Forwarding.
Protocol	Select from UDP or TCP Client which depends on the application.
Source Port Begin	Fill in the beginning of source port.
Source Port End	Fill in the end of source port.
Destination IP	Fill in the current private destination IP.
Destination Port Begin	Fill in the beginning of private destination port.
Destination Port End	Fill in the end of private destination port.

10.4 Service > Dynamic DNS

This section allows you to set up Dynamic DNS.

Service > Dynamic DNS	
Item	**Description**
Mode	Turn on/off this function to select Disable or Enable. The default is Disable.
Service Provider	Select the Service Provider of Dynamic DNS.
Host Name	Fill in your registered Host Name from Service Provider.
Token ID	Fill in your Token ID from Service Provider.
Host Secret ID	Fill in your Secret ID from Service Provider.
Username	Fill in your registered username from Service Provider.
Password	Fill in your registered password from Service Provider.
Update Period Time (Sec)	Fill in “0” to mean 30 days.

Note: There are five options of Service Provider as below to explain the information.

Service Provider	dynv6.com
Host Name	Register hostname, e.g. tester.dynv6.net
Token ID	The token ID, e.g. v_ABjMMQxeAnWv5UwtuVn1QBriynzq

Service Provider	www.nsupdate.info
Host Name	Register hostname, e.g. tester.nsupdate.info
Host Secret ID	The Host Secret ID, e.g. e2AMDsLmVF

Service Provider	www.duckdns.org
Host Name	Register hostname, e.g. tester.duckdns.org
Token ID	The token ID, e.g.12345678-de49-4e97-a33c-98b159aead2b

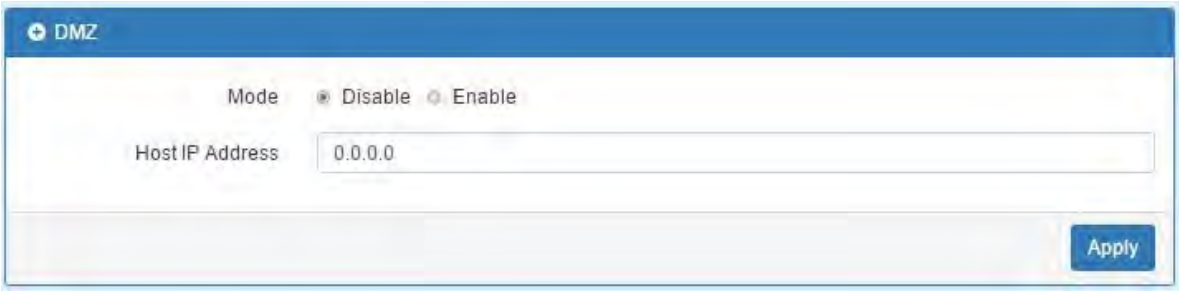
Service Provider	no-ip.com
Host Name	Register hostname, e.g. tester.hopto.org
Username	Register username.
Password	Register password.

Service provider	freedns.afraid.org
Host Name	Register hostname, e.g. tester.mooo.com
Username	Register username.
Password	Register password.

Service provider	dyndns.org
Host Name	Register hostname, e.g. tester.dyns.com
Username	Register username.
Password	Register password.

10.5 Service > DMZ

This section allows you to set the DMZ configuration.

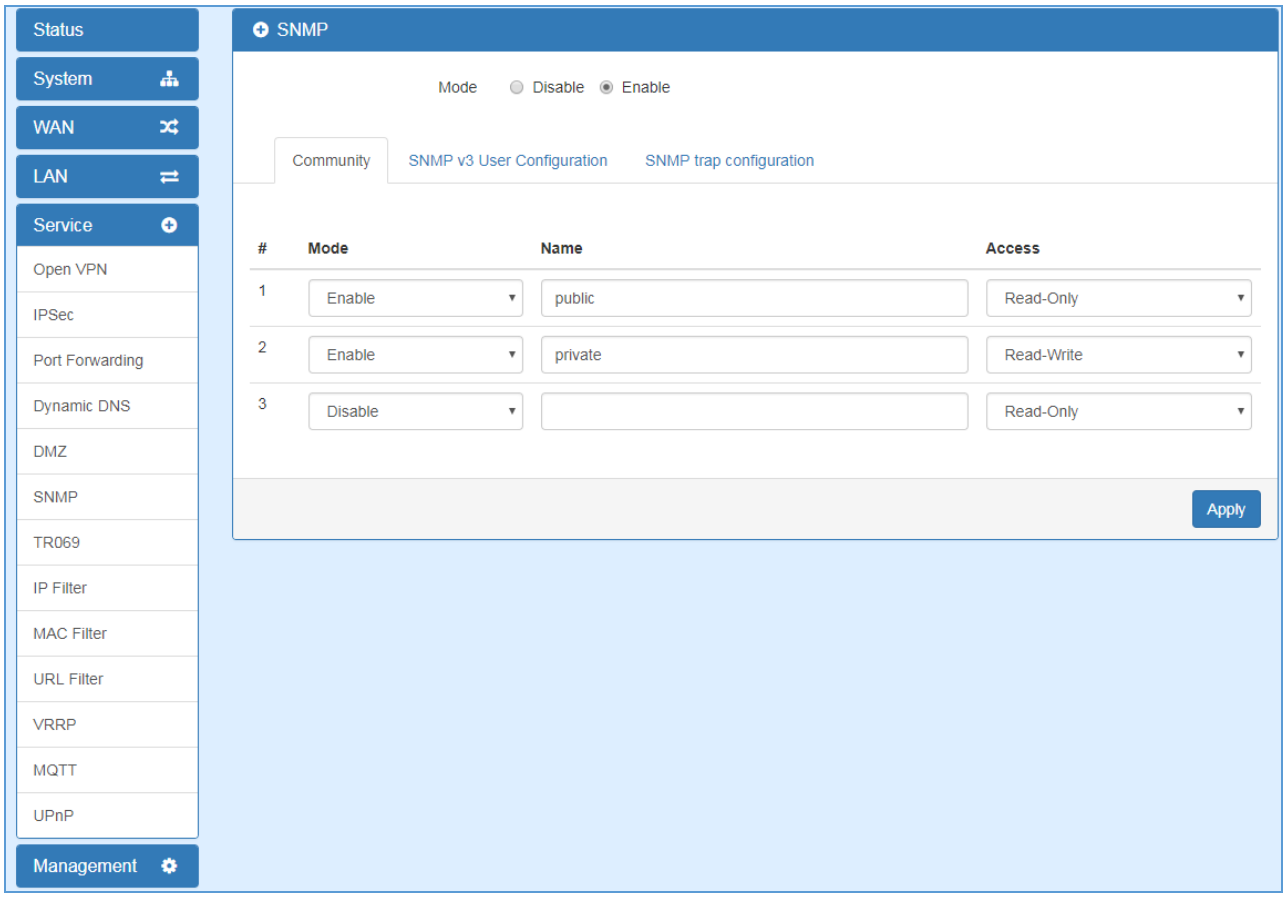


Service > DMZ	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Host IP Address	Fill in your Host IP Address.

10.6 Service > SNMP

10.6.1 SNMP configuration

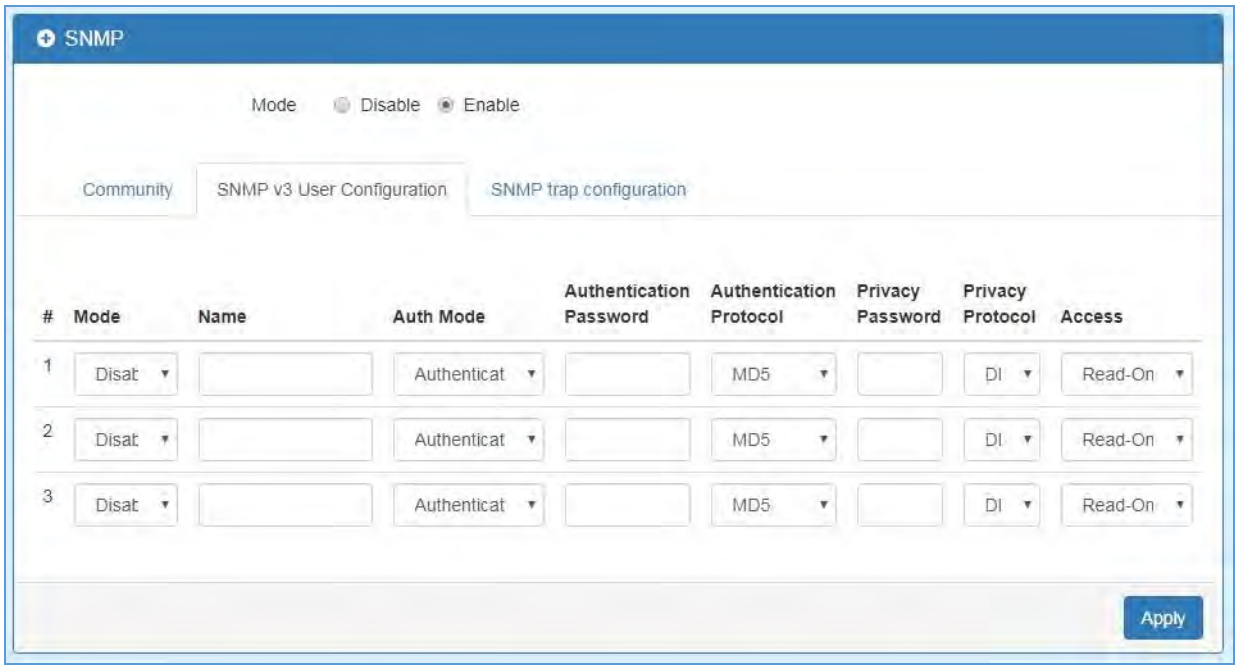
This section allows you to set the SNMP configuration.



Service > SNMP > Community	
Item	**Description**
Mode	Select from Disable or Enable to configure SNMP.
Community	Configure community setting with three options, including # 1, # 2 and #3.
Mode	Select from Disable or Enable.
Name	Name each community.
Access	Select from Read-Only or Read-Write.

10.6.2 SNMP v3 User configuration

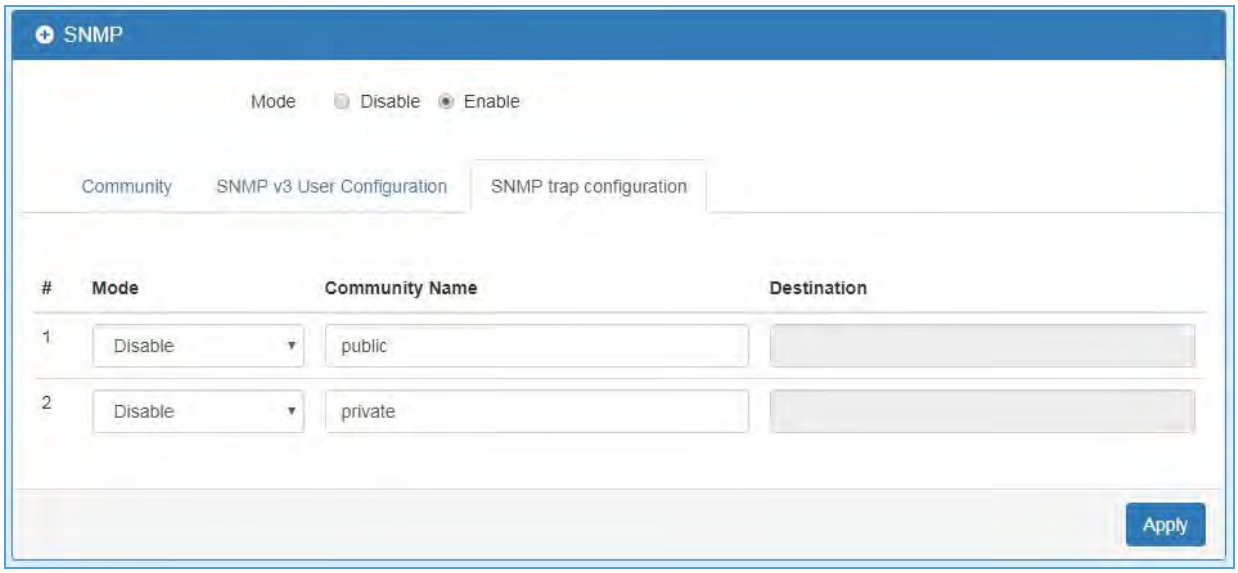
For SNMP version 3, you need to register authentication and allow a receiver that confirm the packet was not modified in transit. There are three options to set up SNMP v3 configuration.

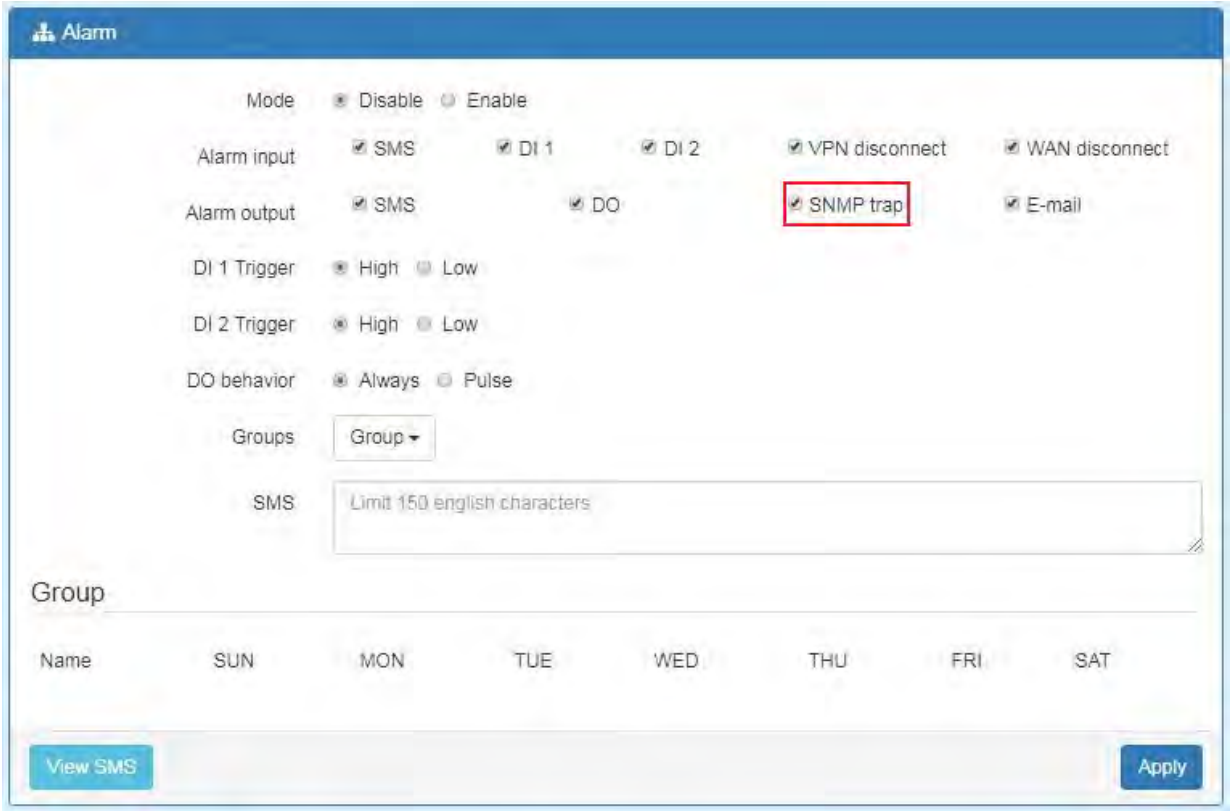


Service > SNMP > SNMP v3 User configuration	
Item	**Description**
Mode	Select from Disable or Enable to configure SNMP. The default is Disable.
Name	Fill in your name.
Auth Mode	Select from Authentication or Privacy.
Authentication Password	Fill in your authentication password.
Authentication Protocol	Select from MD5 or SHA.
Privacy Password	Fill in your privacy password.
Privacy Protocol	Select from DES or AES.
Access	Select from Read-Only or Read-Write.

10.6.3 SNMP trap configuration

This section allows you to set up the SNMP trap configuration when you select the SNMP trap function from Alarm output of system for your router. With SNMP trap setting, you can know the status of remote device.

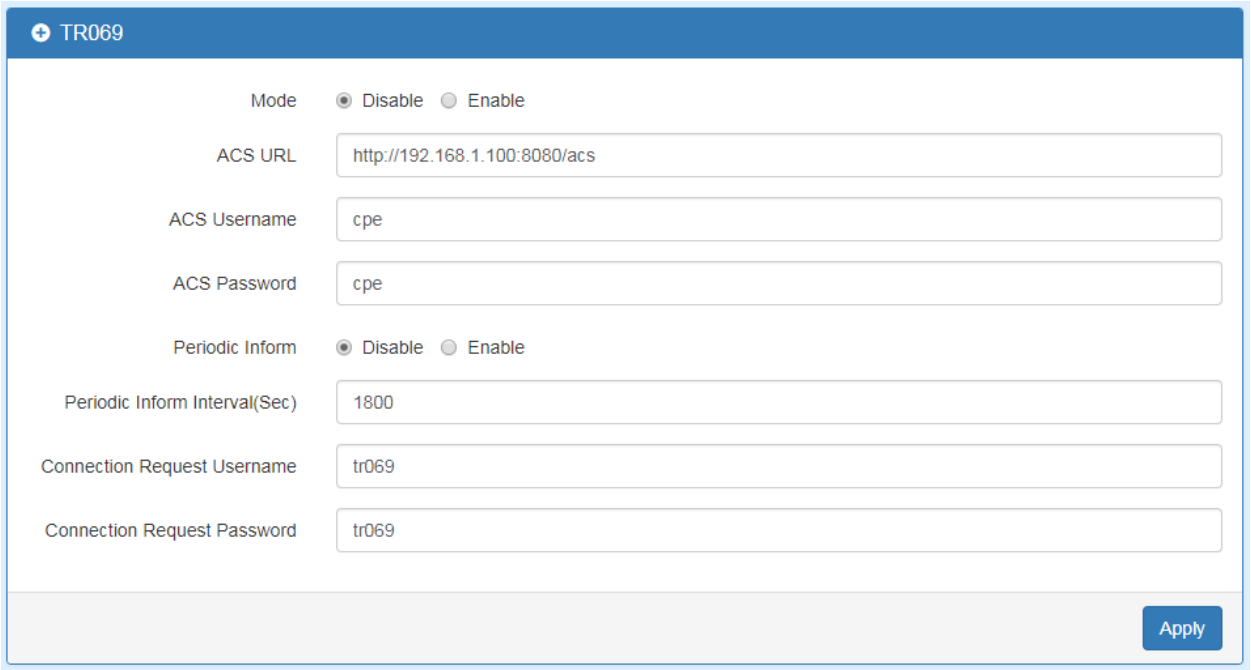




Service > SNMP > SNMP trap configuration	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Community Name	Fill in your community name.
Destination	The destination (domain name/IP) of remote SNMP trap server.

10.7 Service > TR069

This section allows you to set up TR069 client configuration. You can get information how to install TR069 Server (GenieACS Installation) from the application configuration chapter.



Service > TR069	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
ACS URL	Fill in the URL address of ACS (Auto-Configuration Server).
ACS Username	Fill in the ACS username to authenticate the CPE (this router) when connecting to the ACS.
ACS Password	Fill in the ACS password to authenticate the CPE (this router) when connecting to the ACS.
Periodic Inform	Select from Disable or Enable. The default is Disable. The CPE reports the status to the ACS when enabling a period of time set.
Periodic Inform Interval(Sec)	Fill in the periodic time. The CPE reports to ACS the status according to your duration in seconds of the interval set.
Connection Request Username	Fill in the connection request username to authenticate the ACS if the ACS attempts to communicate with the CPE connecting.
Connection Request Password	Fill in the connection request password to authenticate the ACS if the ACS attempts to communicate with the CPE connecting.

10.8 Service > IP Filter

This section allows you to configure IP Filter. After clicking button, you can edit your IP protocol, source/port and destination/port.

IP Filter

Mode ◉ Disable ○ Enable

#	Mode	Protocol	Source / Port	Destination / Port	Edit
1	Disable	All	0.0.0.0 --	0.0.0.0 --	
2	Disable	All	0.0.0.0 --	0.0.0.0 --	
3	Disable	All	0.0.0.0 --	0.0.0.0 --	
4	Disable	All	0.0.0.0 --	0.0.0.0 --	
5	Disable	All	0.0.0.0 --	0.0.0.0 --	
6	Disable	All	0.0.0.0 --	0.0.0.0 --	
7	Disable	All	0.0.0.0 --	0.0.0.0 --	
8	Disable	All	0.0.0.0 --	0.0.0.0 --	
9	Disable	All	0.0.0.0 --	0.0.0.0 --	
10	Disable	All	0.0.0.0 --	0.0.0.0 --	
11	Disable	All	0.0.0.0 --	0.0.0.0 --	
12	Disable	All	0.0.0.0 --	0.0.0.0 --	
13	Disable	All	0.0.0.0 --	0.0.0.0 --	
14	Disable	All	0.0.0.0 --	0.0.0.0 --	
15	Disable	All	0.0.0.0 --	0.0.0.0 --	
16	Disable	All	0.0.0.0 --	0.0.0.0 --	

Apply

(1) The default is Disable Mode as the following interface.

Service > IP Filter	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Protocol	Select from All, ICMP, TCP or UDP.
Source IP	Fill in your source IP address.
Source Port	Fill in your source port.
Destination IP	Fill in your destination IP address.
Destination Port	Fill in your destination port.

(2) When selecting Enable Mode, the protocol is TCP. The source IP has IPv4 and IPv6 setting formats.

(3) For Source IP, there are three types to input your source IP that depends on your requirement, including single IP, IP with Mask or giving a range of IP. The following table provides some examples.

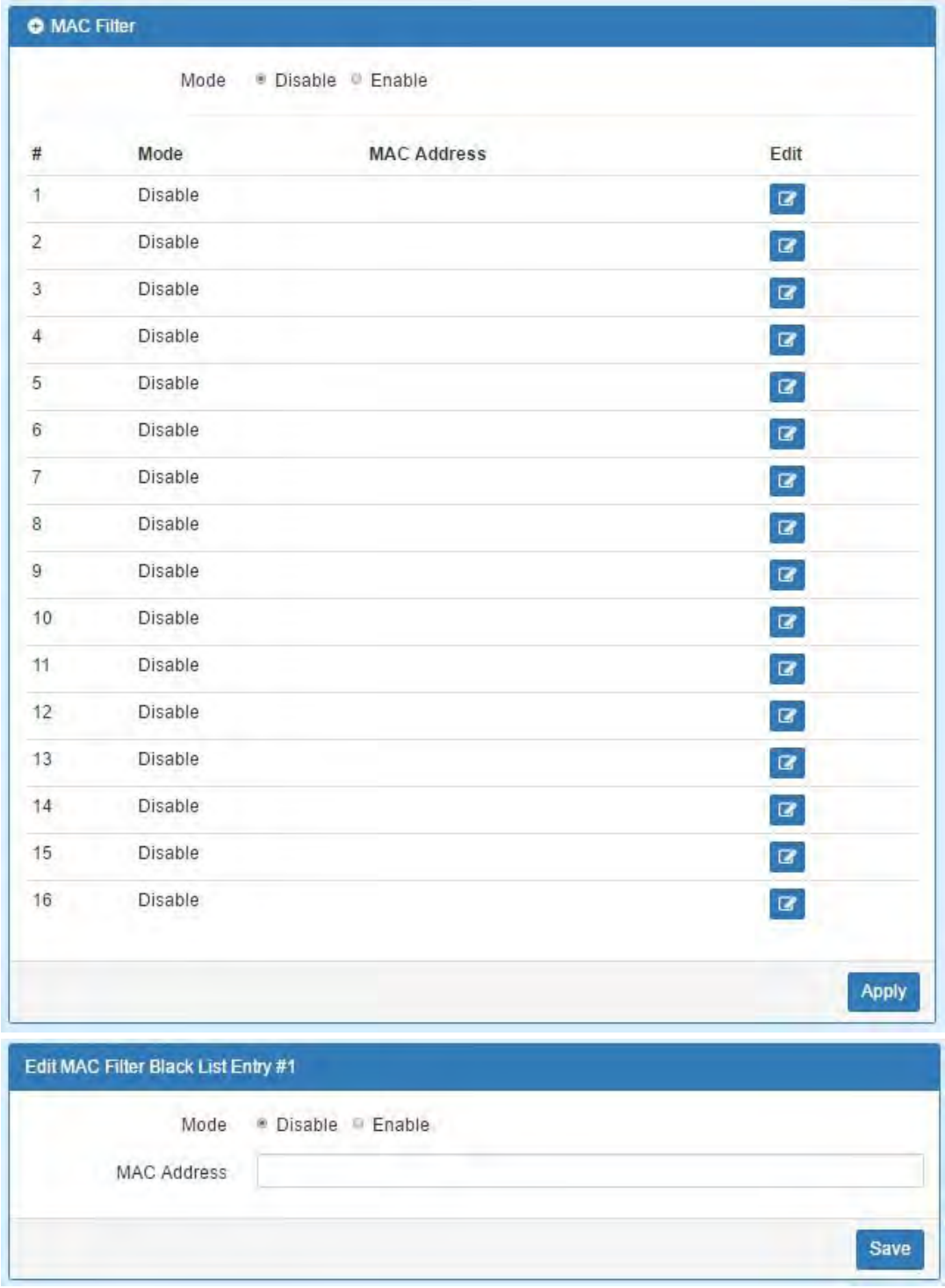
Service > Edit IP Filter > Source IP			
IP Format	**Single IP**	**IP with Mask**	**Ranged IP**
IPv4	192.168.0.123	192.168.1.0/24 192.168.1.0/255.255.255.	192.168.1.1-192.168.1.123
IPv6	2607:f0d0:1002:51::4	2607:f0d0:1002:51::0/64	2607:f0d0:1002:51::4- 2607:f0d0:1002:51::aaaa
Note: Setting up a range of IP, please use **–** hyphen symbol to mark your ranged IP.			

(4) For Source Port, there are two types to input your source port that depends on your requirement, including single port (e.g.1234) or giving a range of ports (e.g.1234:5678).

Note: Setting up a range of source ports, please use **:** colon symbol to mark your ranged ports.

10.9 Service > MAC Filter

This section allows you to set up MAC Filter. After clicking button, you can edit your MAC address.

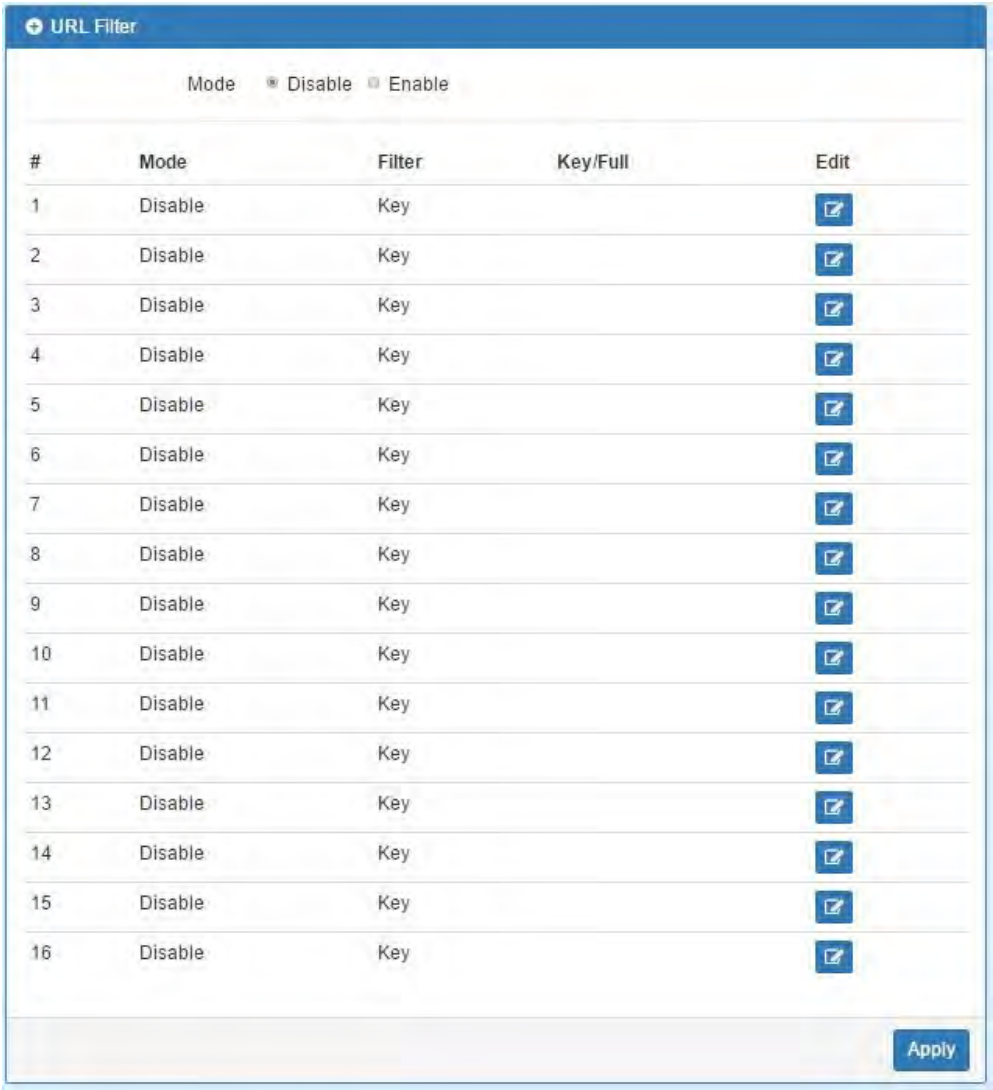


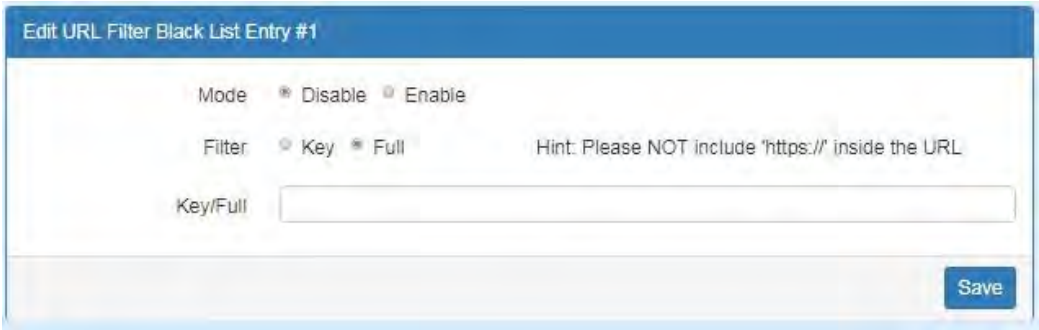
Service > MAC Filter	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
MAC Address	Fill in your MAC address.

Note: Setting up MAC address, please use **:** colon symbol (e.g. xx : xx : xx: xx) or **–** hyphen symbol to mark (e.g. xx- xx–xx-xx).

10.10 Service > URL Filter

This section allows you to set up URL Filter. After clicking button, you can edit the type of filter and information.



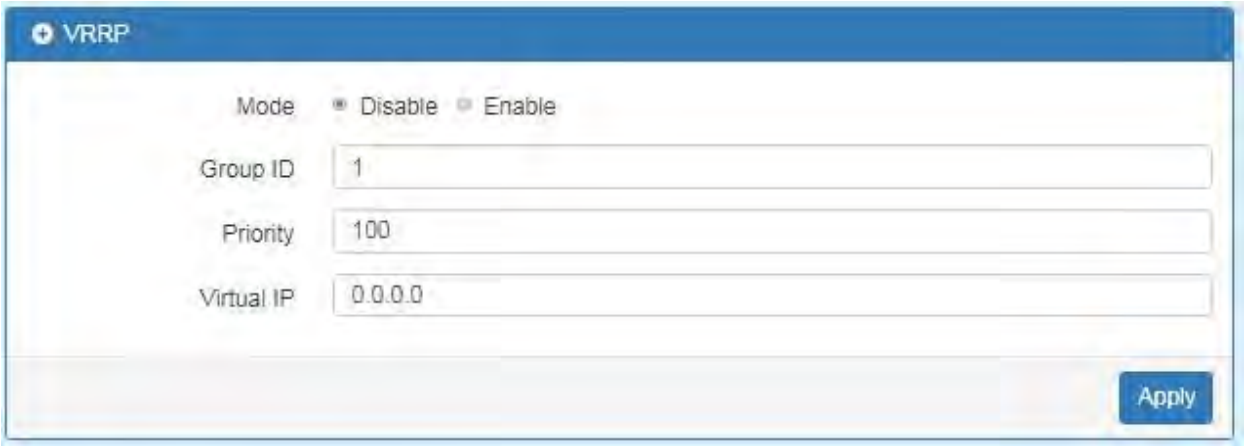


Note: Please not include “https://” for the URL address in the **Full** Filter.

Service > URL Filter	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Filter	Select from Key or Full. The default is Key.
Key/Full	Fill in your Key/Full information.

10.11 Service > VRRP

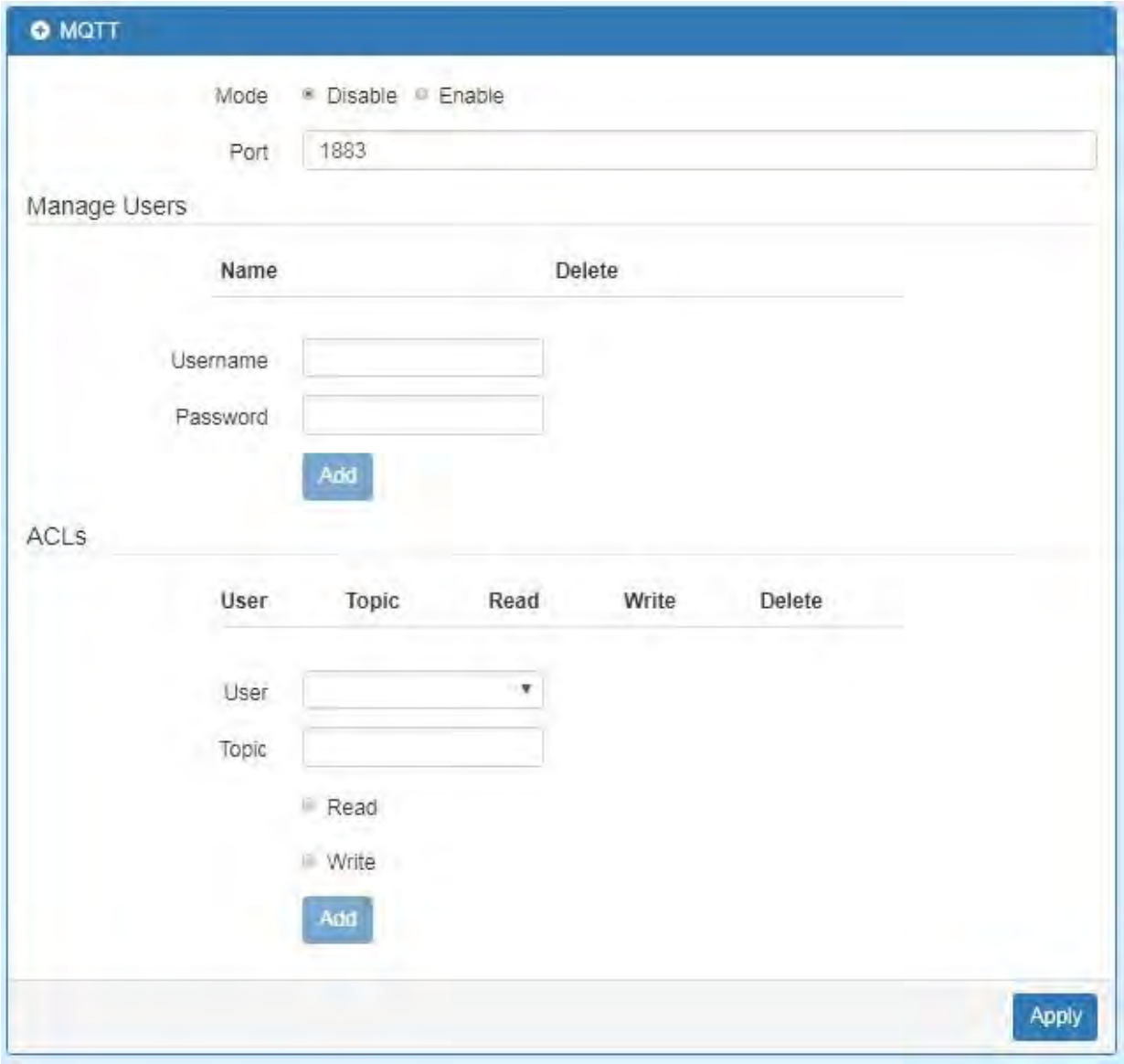
This section allows you to configure VRRP.



Service > VRRP	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Group ID	Specify which VRRP group of this router belong to (1-255). The default is 1.
Priority	Enter the priority value from 1 to 254. The larger value has higher priority. The default is 100.
Virtual IP	● Each router in the same VRRP group must have the same virtual IP address. The default is 0.0.0.0. ● This virtual IP address must belong to the same address range as the real IP address of the interface.

10.12 Service > MQTT

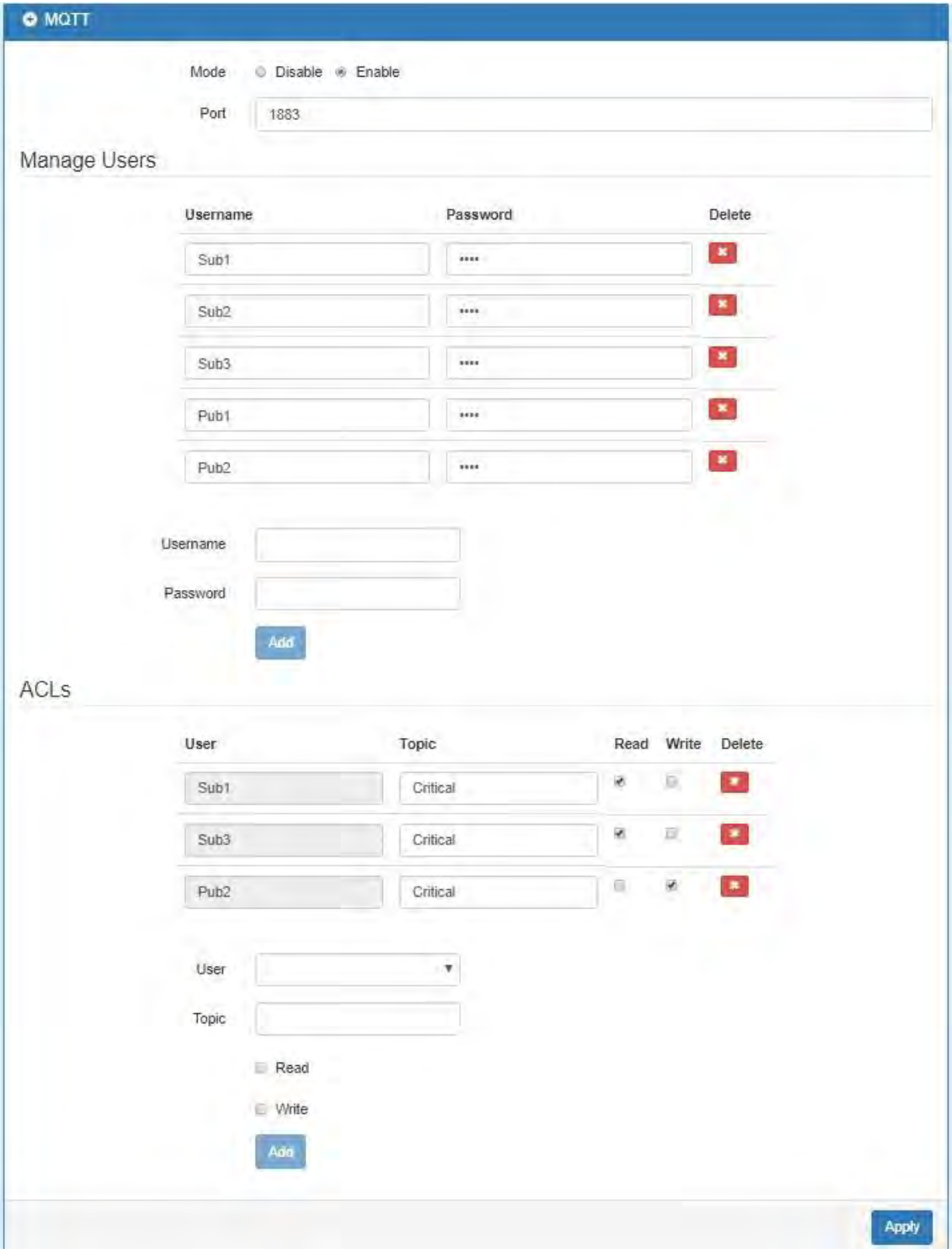
This section makes you configure MQTT which allows the MQTT client to send the message within specific topic or channel. By default, the router does not allow anonymous to read/write the MQTT topic or channel. Thus, you need to create the account with username and password for MQTT client in the web UI.



Service > MQTT	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Port	Fill in the port number of MQTT application.
Manage Users	Create the users and show all users' names. Allow each user to delete their name.
Username	Fill in the username of manage user.
Password	Fill in the password of manage user.
ACLs	Allow to specify what topic should be limited.
User	Select the users and identify their authority to read or write the MQTT topic/channel.
Topic	Name the topic of MQTT message.

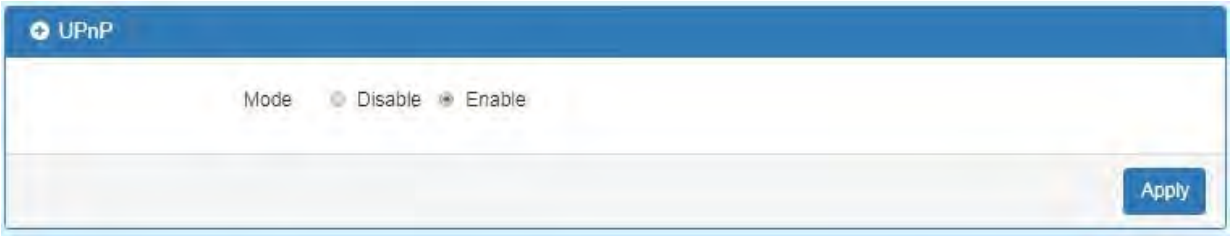
Take for example, the interface is shown as below.

The Manage Users section will show all users that you create. Moreover, each user can use the delete button to delete it. For the ACL control, user can specify what topic should be limited. In this case, we set up the publisher **pub1** to write the critical topic. Additionally, we also allow the subscribers **sub1** and **sub3** to read the critical topic. Thus, only the sub1 and sub3 can receive it when **pub1** sending the message.



10.13 Service > UPnP

This section allows you to set up UPnP confirguration to select the mode from Disable or Enable. The default UPnP is enabled for the cellular router.



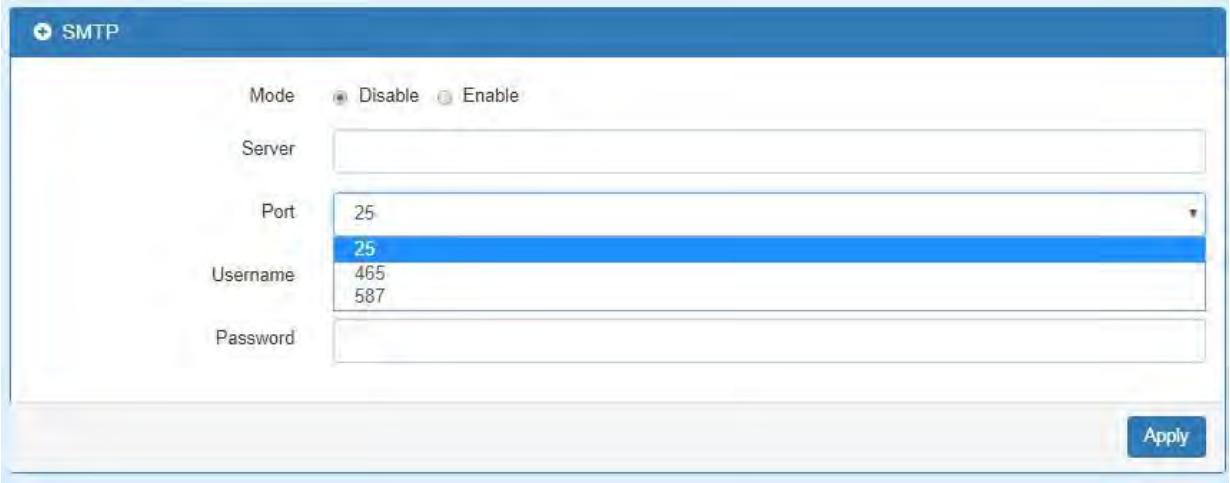
Note:

UPnP™ (Universal Plug and Play) is a set of protocols that allows a PC to automatically discover other UPnP devices (anything from an Internet gateway device to a light switch), retrieve an XML description of the device and its services, control the device, and subscribe to real-time event notification.

PCs using UPnP can retrieve the cellular router's WAN IP address, and automatically create NAT port maps. This means that applications that support UPnP, and are used with UPnP enabled cellular router, will not need application layer gateway support on the cellular router to work through NAT.

10.14 Service > SMTP

This section provides you to send your email for the server. For instance, the email will be sent to notify when the Alarm has a nofitication by the server.



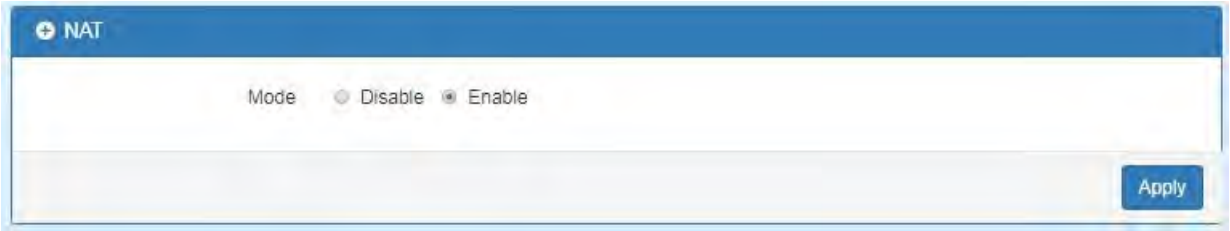
Service > SMTP	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Server	The email will be sent through the server.
Port	There are three ports for SMTP communication between mail servers. ● **Port 25**：Use TCP port 25 without encryption. ● **Port 465**：SMTP connections secured by SSL. ● **Port 587**：SMTP connections secured by TLS.
Username/Password	Fill in your username and password as the same your server.

10.15 Service > NAT

This section allows you to set NAT configuration.

When NAT is on, the router will replace the source private IP address by its Internet public address for outgoing packets, and replace the destination Internet public address by private IP address for incoming packets.

When NAT is off, the router will send the source LAN private IP address for outgoing packets and allow to receive the destination LAN private IP address for incoming packets.

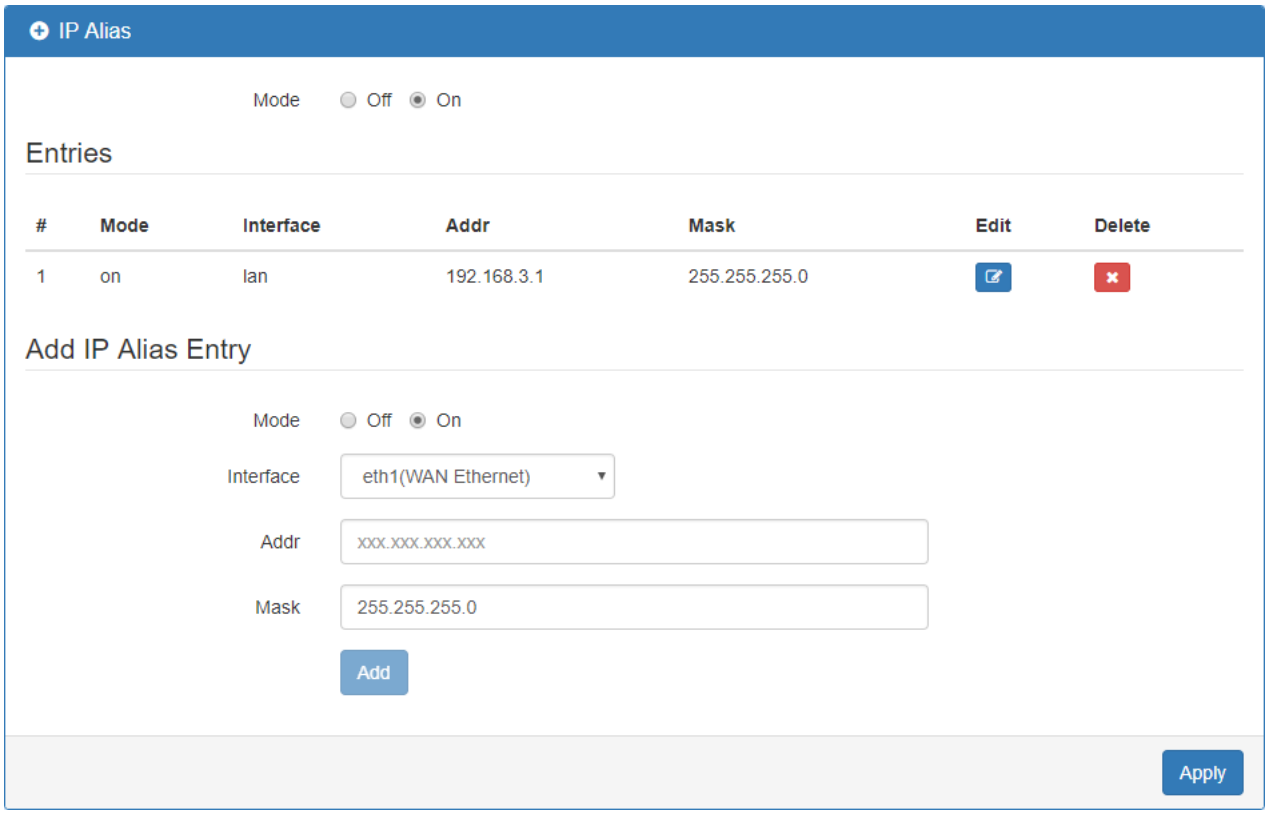


10.16 Service > IP Alias

This section allows you to set **IP Alias** configuration.

IP Alias is associating more than one IP address to a network interface. With IP Alias, one node on a network can have multiple connections to a network, each serving a different purpose.

IP Alias can be used to provide multiple network addresses on a single physical interface.



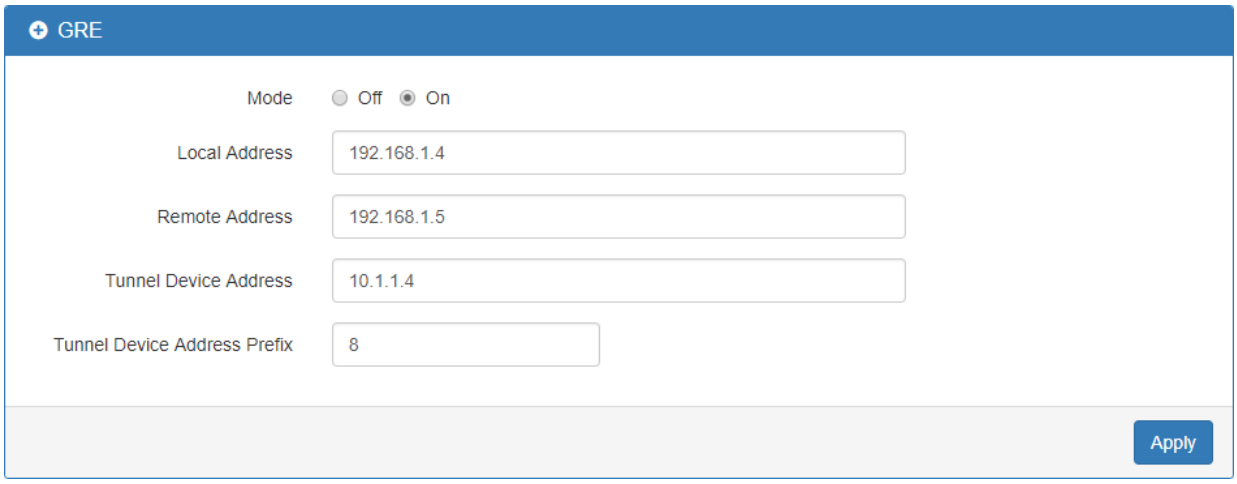
Service > IP Alias	
Item	**Description**
Mode	Select from Off or On to enable the IP Alias.
Entries	The setting can be edited or deleted the existed entries.
Add/Edit IP Alias Entry	● Mode: select from Off or On to use or not use this entry. ● Interface: the interface you want to provide the additional address. ● Addr: the IP address. ● Mask: the network mask.

10.17 Service > GRE

This section allows you to set GRE configuration. The default mode is off.

Generic Routing Encapsulation (GRE) is one of the available tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.

The GRE Mode is on.



Service > IP Alias	
Item	**Description**
Mode	Select from Off or On to enable GRE.
Local Address	Set local address of the GRE tunnel.
Remote Address	Set remote address of the GRE tunnel.
Tunnel Device Address	Set IP address of this GRE tunnel device.
Tunnel Device Address Prefix	Set Prefix of the Tunnel Device Address.

11 Management

This section provides you to manage the router, set up your administration and know about the status of current software and firmware. Also, you can back up and restore the configuration.

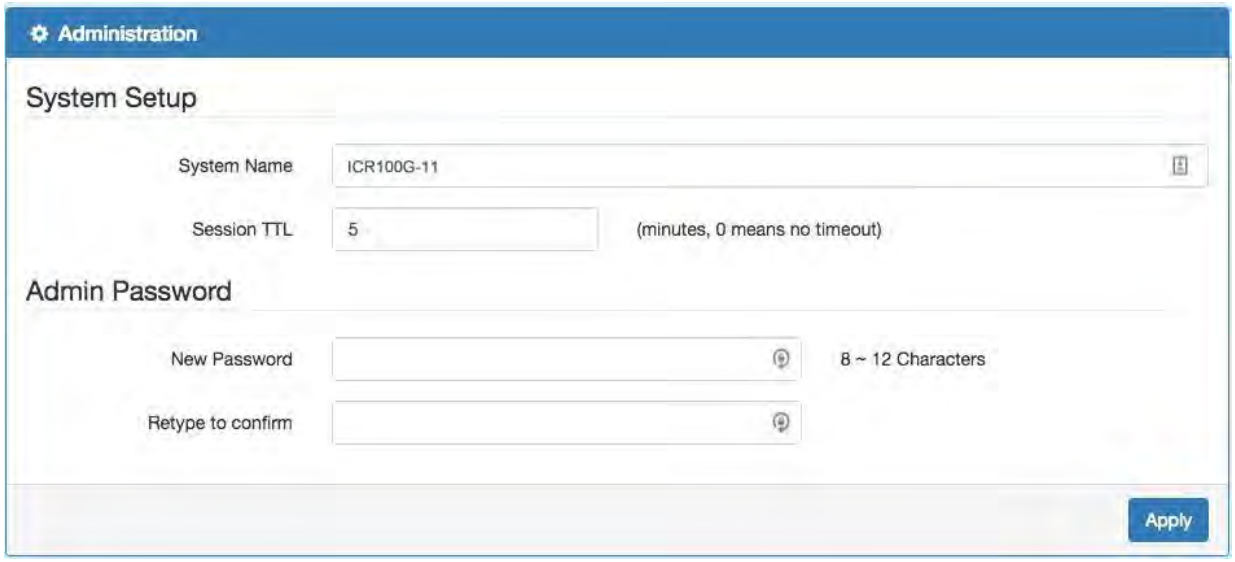
11.1 Identification

This section allows you to confirm the profile of router, current software, firmware version and system uptime.

Management > Identification	
Item	**Description**
Host Name	Show the host name of cellular router.
MAC Address	Show the MAC address.
Software Version	Show the current software version.
Software MCSV	Show the current software MCSV.
Hardware MCSV	Show the current hardware MCSV.
Modem Firmware Version	Show the current firmware version.
IMEI	Show the IMEI (International Mobile Equipment Identity number).
Uptime	Show the current system uptime.

11.2 Administration

This section allows you to set up the name of system and change your new password. For the Session TTL, you can set up what duration of time will be logout. If you don't need to have this timeout limitation, you can fill in "0"(Zero).



11.3 Firmware

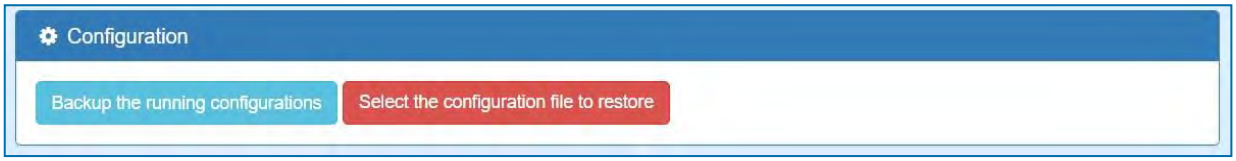
This section provides you to upgrade the firmware of router.

(1) Click Select the firmware to upgrade button to choose your current firmware version in your PC.
(2) Select Upgrade button to update.
(3) After upgrading successfully, the router will reboot automatically.

11.4 Configuration

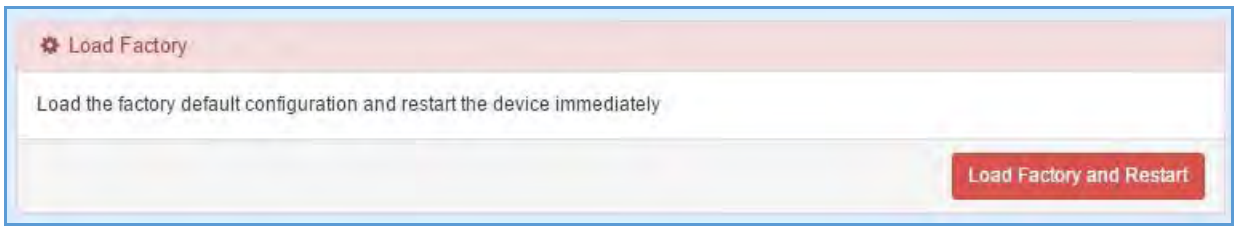
This section supports you to export or import the configuration file.

(1) Click Backup the running configurations button to export your current configurations.
(2) Click Select the configuration file to restore button to import the configuration file.



11.5 Load Factory

This section supports you to load the factory default configuration and restart the device immediately. You can click the Load Factory and Restart button.



11.6 Restart

This section allows you to click Restart button and the router will restart immediately.

12 Configuration Applications

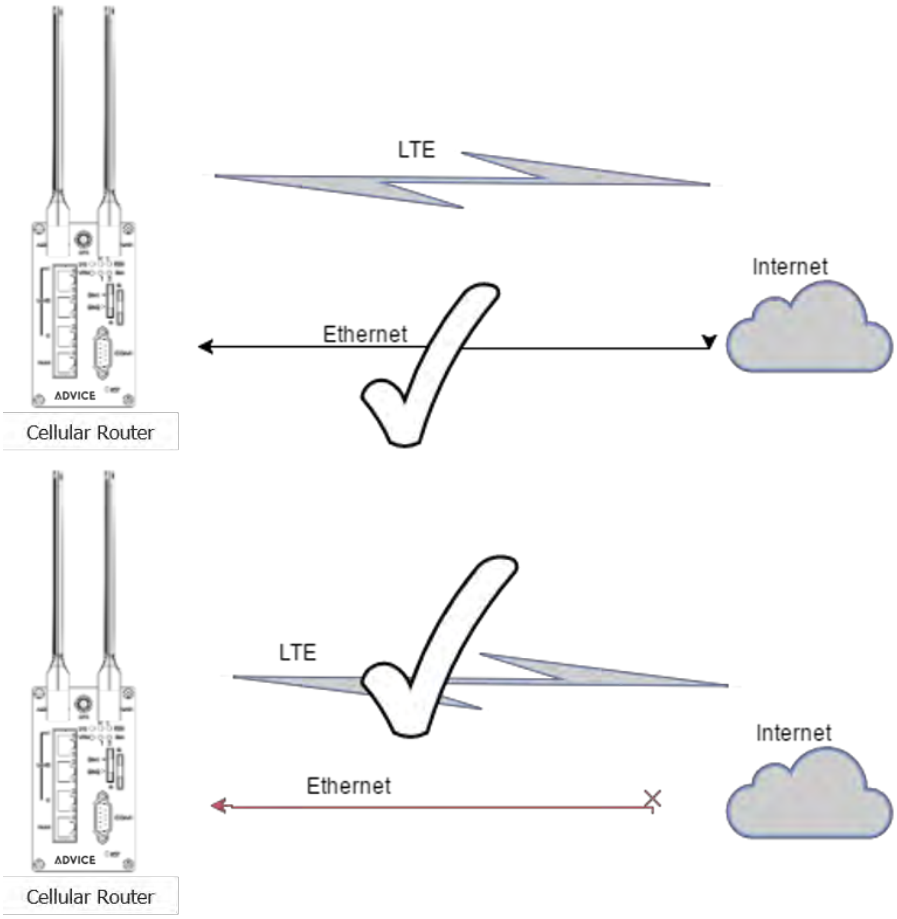
This section explains specific examples how to configure your applications.

12.1 WAN Priority

You can select from Auto, LTE Only or ETH Only.

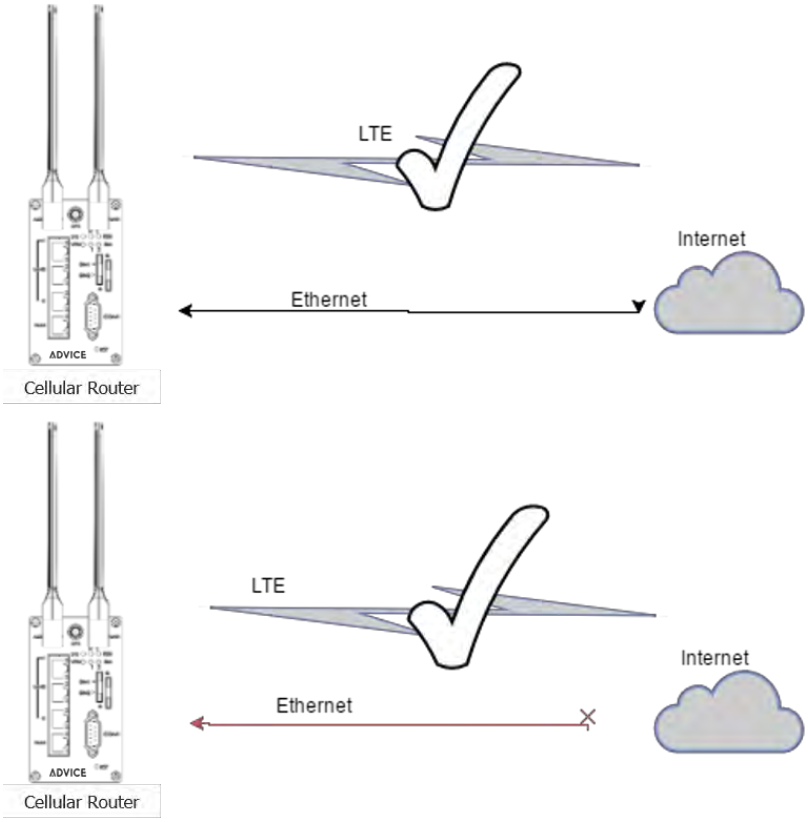
(1) WAN Priority > Auto:

In case both Ethernet and LTE can access Internet, the router would route network packages through Ethernet. The reason is Ethernet that is low price and stable.
However, in case Ethernet is unplug or not able to access Internet (check by ping), the router would route network packages through LTE network.



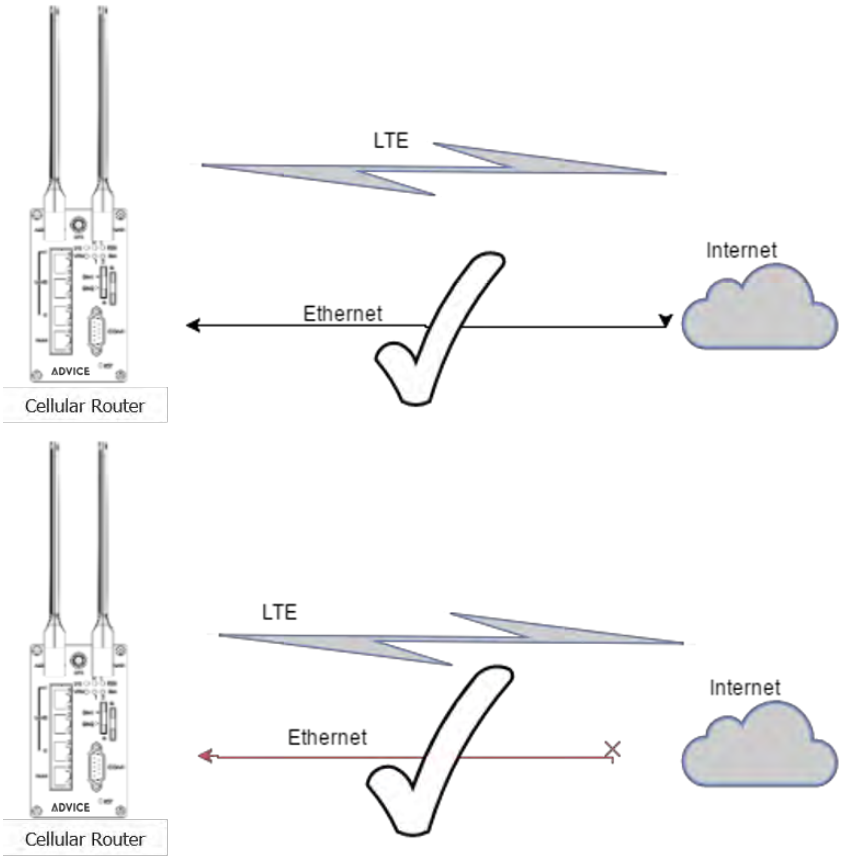
(2) WAN Priority > LTE Only:

In this mode, the router only routes network packages through LTE.



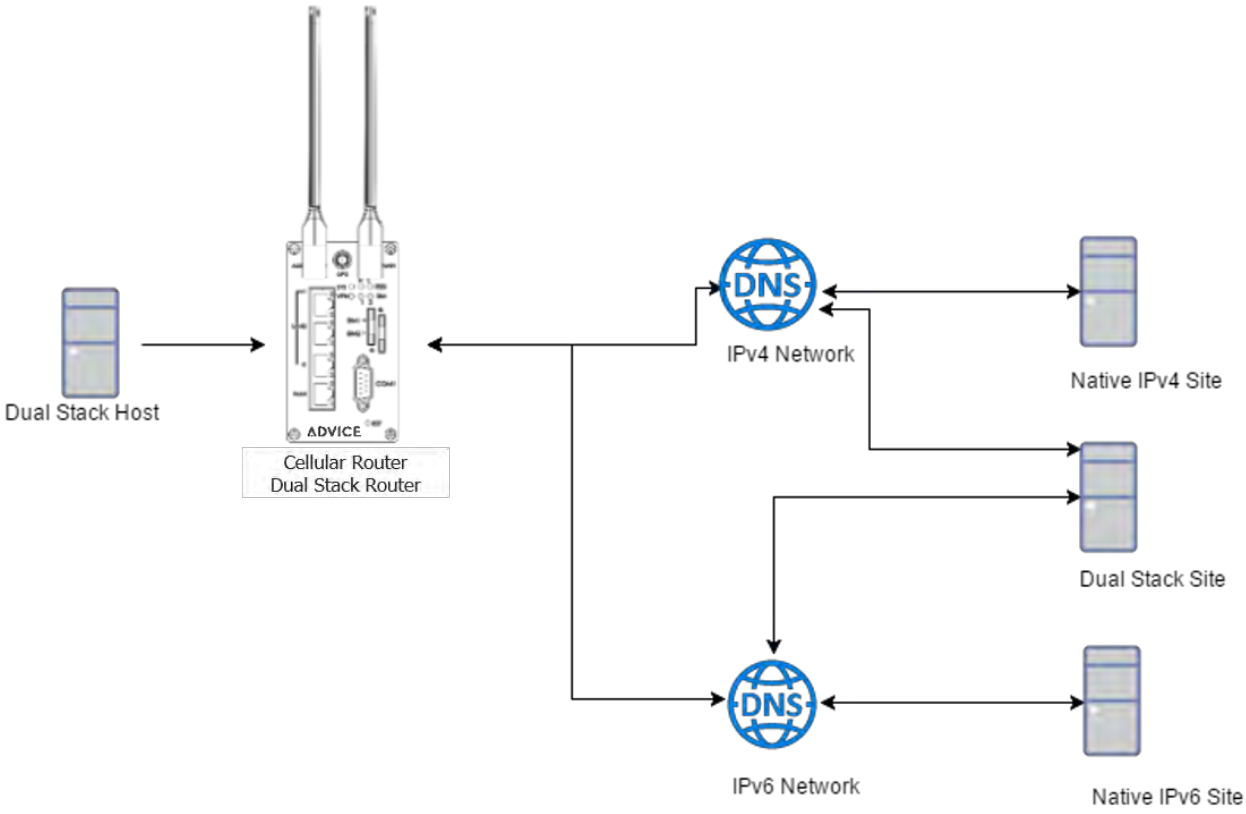
(3) WAN Priority > ETH Only:

In this mode, the router only routes network packages through Ethernet.



12.2 LAN > IPv4/IPv6 Dual Stack

The router supports IPv4/IPv6 dual stack by default, it means IPv4 packages route to IPv4 network and IPv6 route to IPv6 network.



Since IPv6 is global IP, there is no NAT between WAN site and LAN site. One device only needs one global IPv6. There is IPv6 firewall protection in the router by default. Only the IPv6 packages come from LAN site device and got reply back.

Status

Attr.	Current SIM	Backup SIM
SIM Card	SIM1	SIM2
Modem Status	Ready	Not Inserted
Operator	Chunghwa Telecom	
Modem Access	FDD LTE	
IMSI	466924290307730	
Phone Number		
Band	LTE BAND 7	
Channel ID	3050	0
IPv4 Address	10.167.236.11	
IPv4 Mask	255.255.255.255	

Ethernet WAN

Attr.	Value
IPv4 Address	192.168.11.176
IPv4 Mask	255.255.255.0

Ethernet LAN

Attr.	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	2001:b021:4a::100

The router automatically detects IPv6 environment and query IP. After the IP is obtained successfully, it will distribute to LAN site hosts.

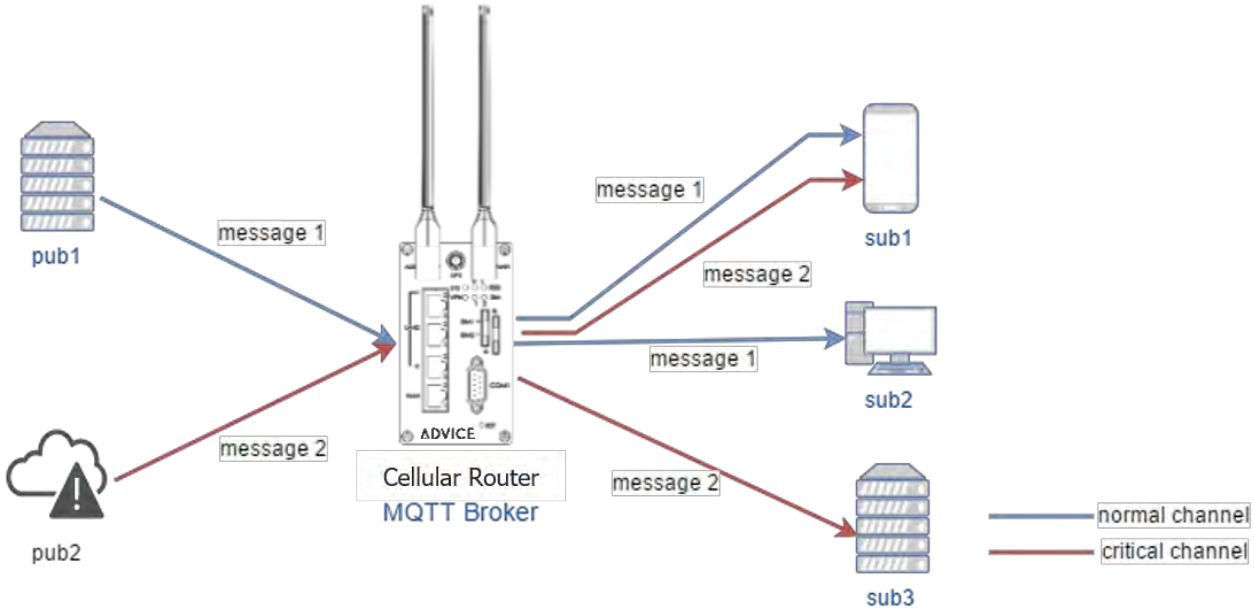
Command Prompt (1)

```
C:\>ipconfig  /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : PCI-borchen-LAB
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Blue:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller #2
   Physical Address. . . . . . . . . : 00-E0-4C-68-00-FD
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:b400:e335:e5ca::101(Preferred)
   Lease Obtained. . . . . . . . . . : Thursday, March 15, 2018 1:15:07 PM
   Lease Expires . . . . . . . . . . : Thursday, March 15, 2018 1:17:06 PM
   Link-local IPv6 Address . . . . . : fe80::8c61:e319:2e70:1140%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, March 15, 2018 11:22:20 AM
   Lease Expires . . . . . . . . . . : Thursday, March 15, 2018 6:14:00 PM
   Default Gateway . . . . . . . . . : fe80::c2e:43ff:fe0d:4743%15
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 620814412
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-04-D3-75-D8-50-E6-C3-63-BD

   DNS Servers . . . . . . . . . . . : fe80::c2e:43ff:fe0d:4743%15
                                       192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\>_
```

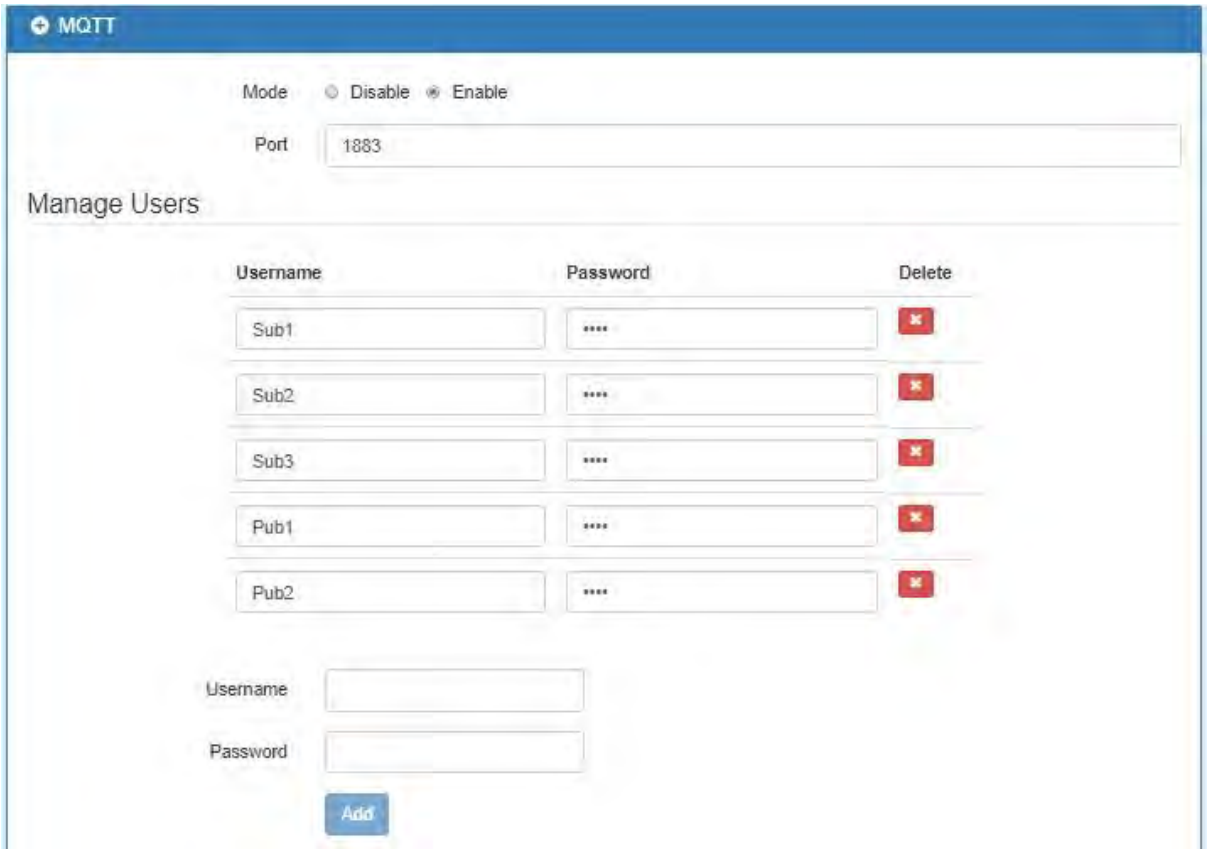
12.3 MQTT Broker

The cellular router provides the MQTT broker feature which allow the MQTT client sending the message within specific topic (channel).

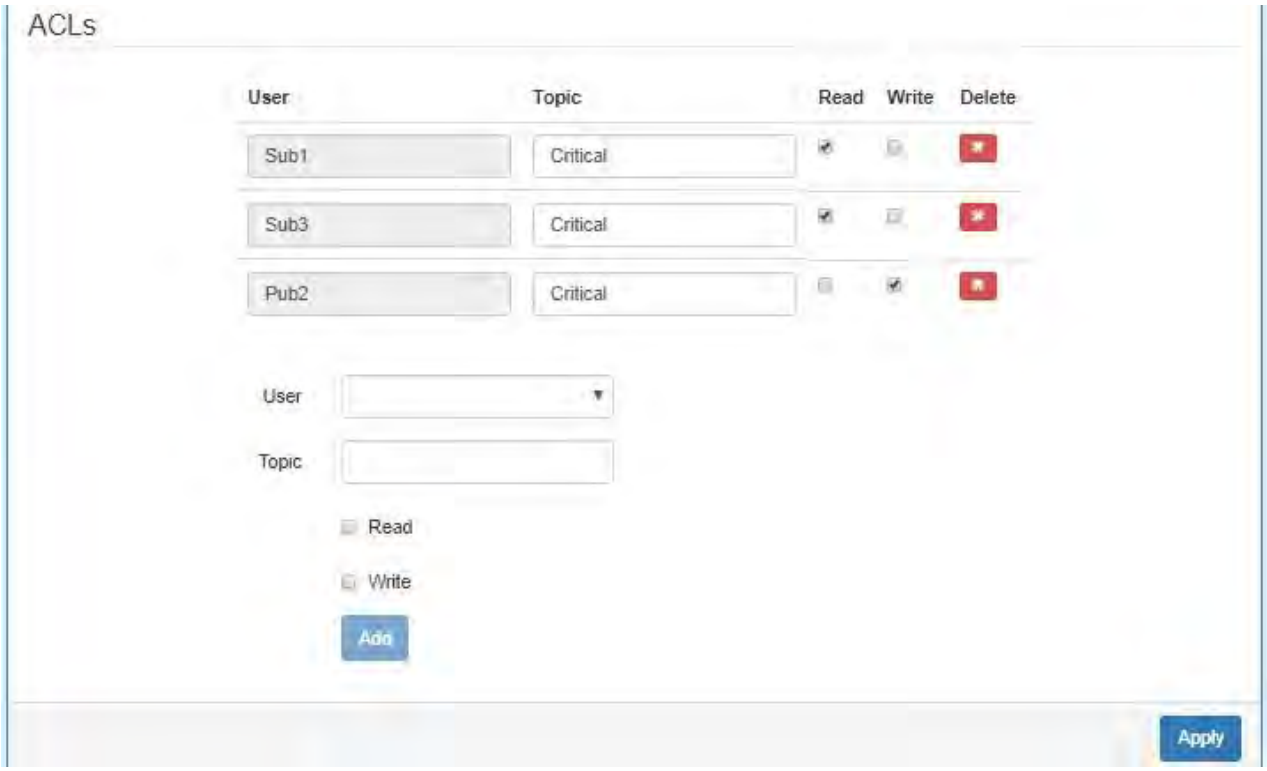
By default, the cellular router does not allow anonymous to read/write the MQTT topic (channel).



Thus, you need to create the account with username and password for MQTT client in the web UI.

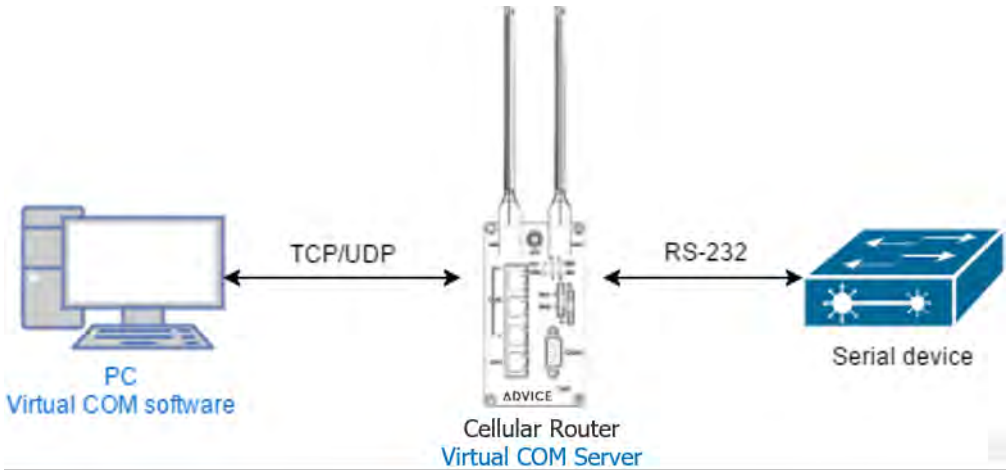


The **Manage Users** section will show all created users. Each user can use the **delete** button to delete it. For the ACL control, you can specify what topic should be limited.
For example, we set the publisher **pub1** to write the critical topic.
Additionally, we also the subscribers **sub1** and **sub3** can read the critical topic.
Thus, when **pub1** is sending the message only the **sub1**, the **sub3** can receive it.



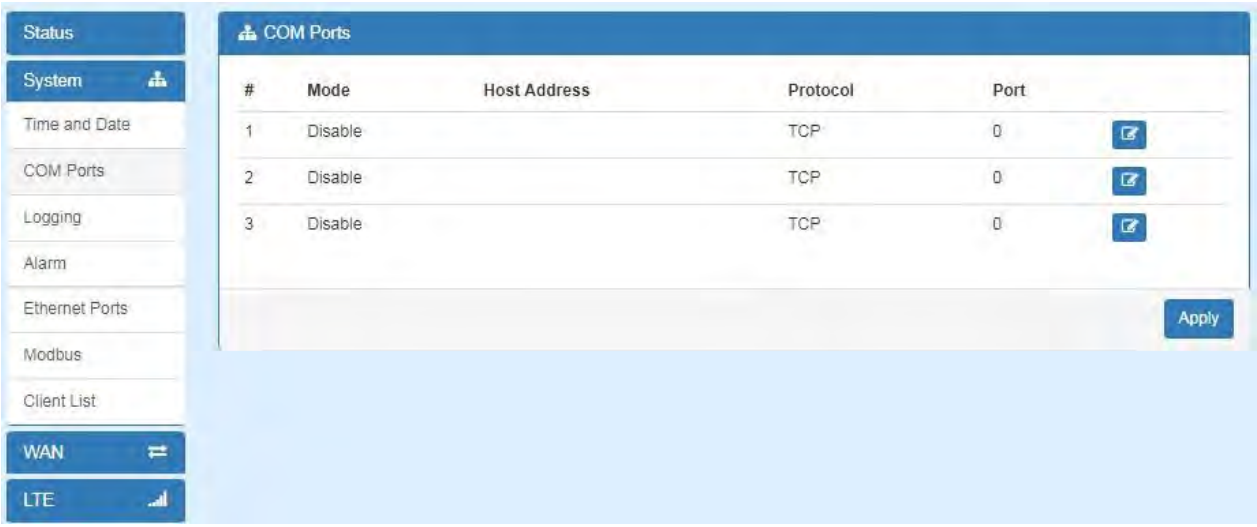
12.4 Virtual COM > Remote Management

You can access the remote serial device (e.g. Console) by the Virtual COM server feature.
When you set up the above environment, use the Virtual COM software (e.g. USR-VCOM) to simulate the COM device. After the simulation, the user can use the terminal tool (e.g. putty, tera term) to access the remote serial device Console.

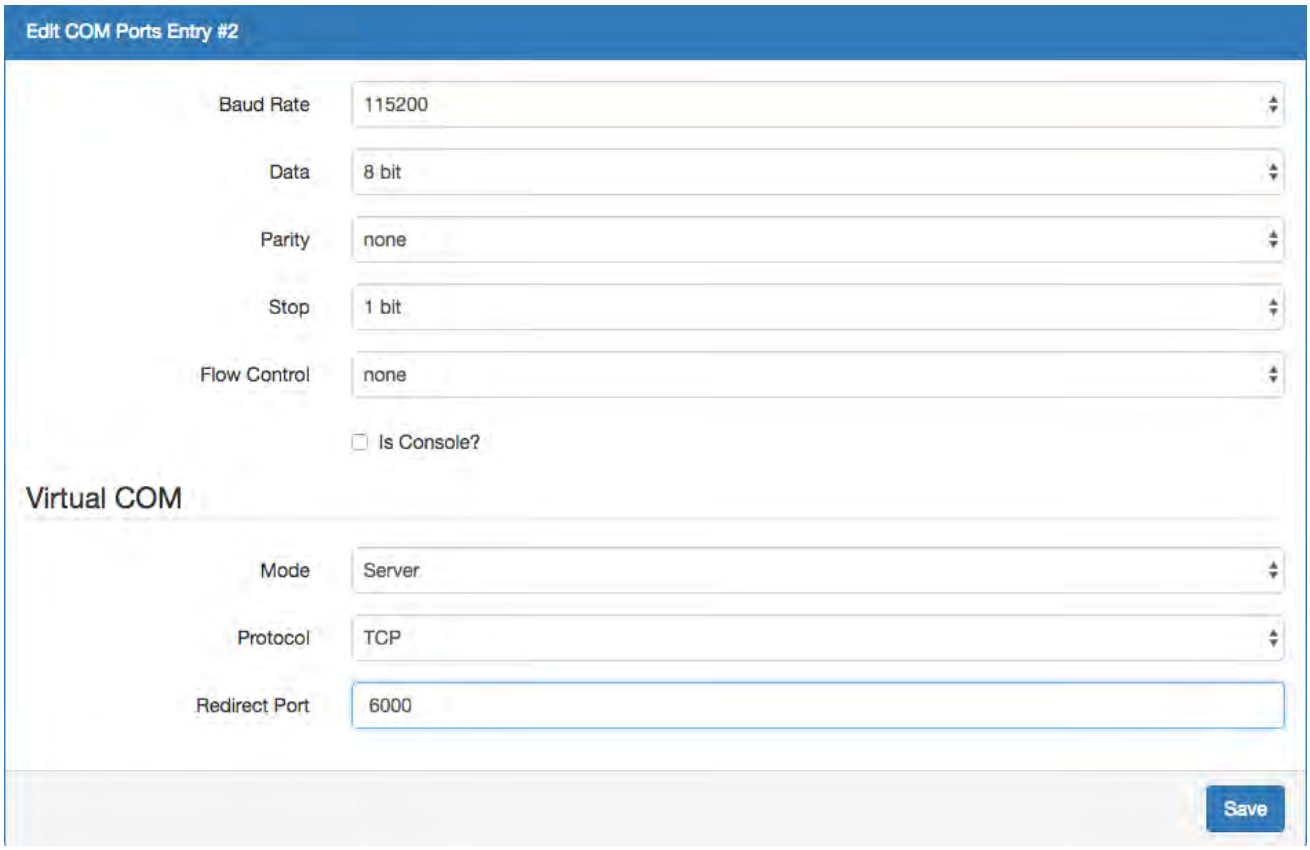


- **How to set up**

The router provides RS-232 (COM1, COM2) and RS-458 (COM3). You can choose one serial port to connect the device. For example, if you use COM2 to connect the serial device, you need to adjust the setting like baud rate, date bits to fit the device. You can use the web UI to set up the serial settings and open the Virtual COM server feature for COM2.
First, you need to navigate to the **System -> COM ports**. The web UI shows the following picture.



You can click the **Edit** button to configure COM2 setting. The configuration UI shows the following picture.



The configuration UI provides the serial setting and the Virtual COM setting.

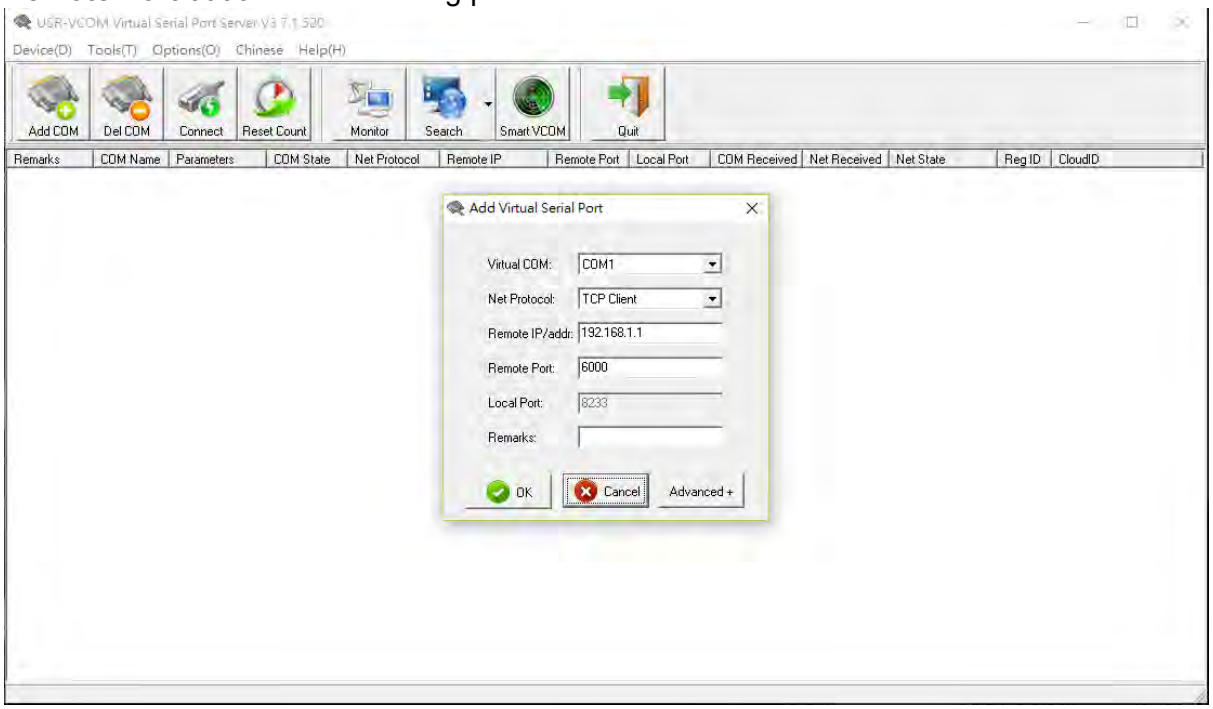
(1) For the serial setting, you need to change the setting like baud rate to fit the connected device.

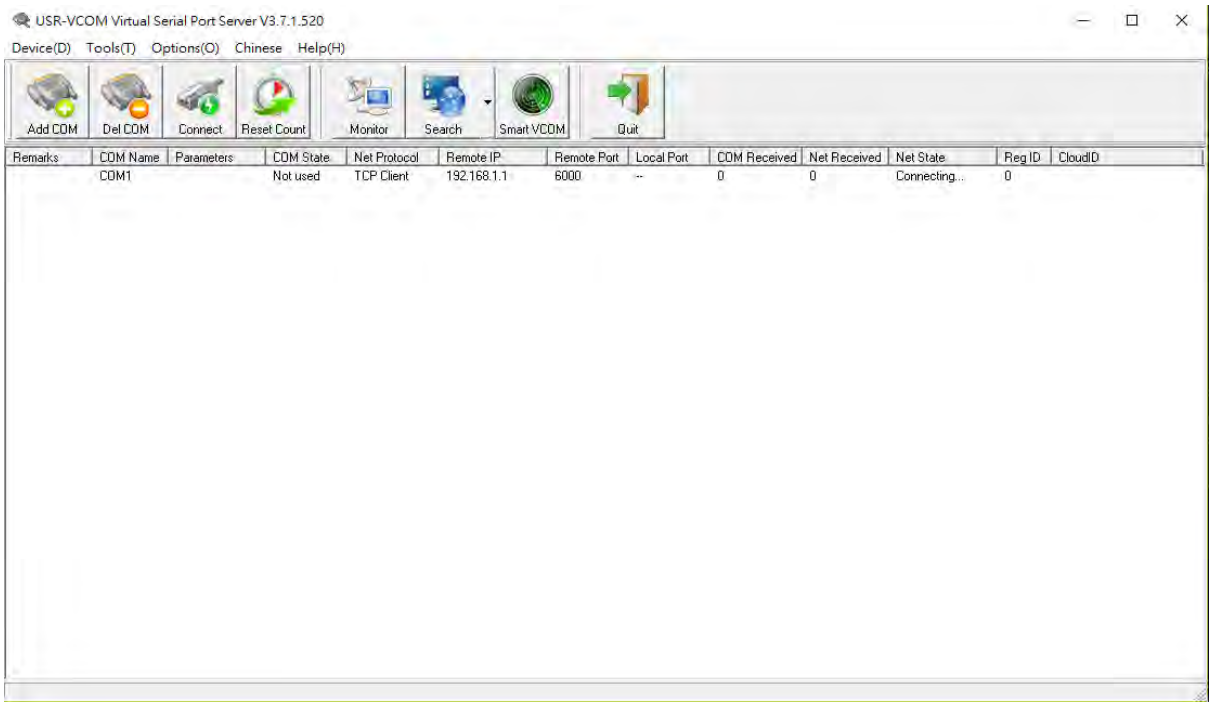
(2) For the Virtual COM, you need to change the mode to **Server** and specify the **Protocol**, **Port** to reach the remote management feature. (Note: In this case, we use the **TCP** and port **6000** to be the Virtual COM server settings.)

(3) Click the **Close** and the **Apply** button. If all settings are correct, the web UI will display **Apply OK**.

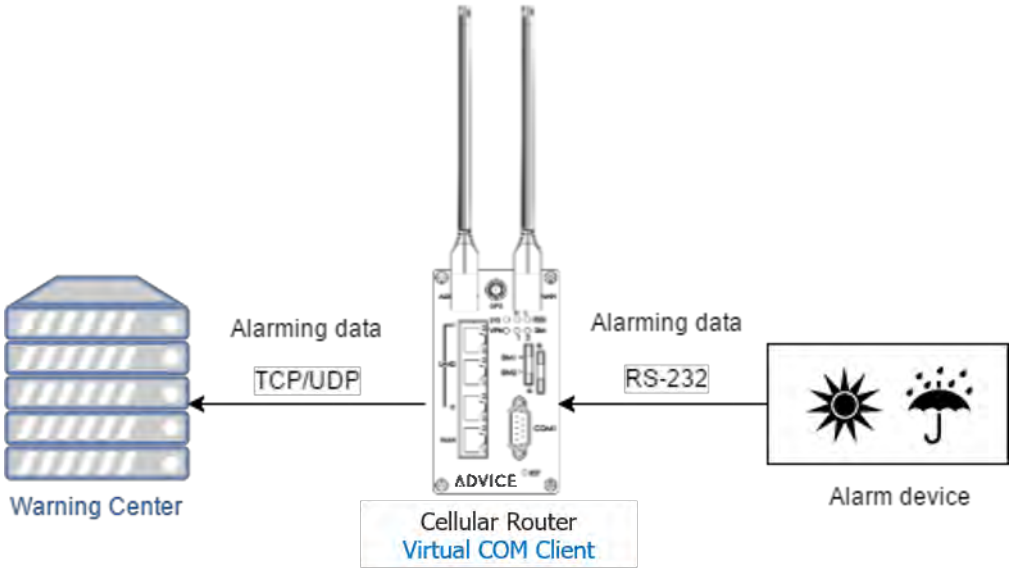
(4) Then you can open the Virtual COM software on PC. (Note: In this case, we use the USR-VCOM to be the Virtual COM software.)

(5) And set up the virtual serial port by **192.168.1.1** (The default is LAN IP), **TCP client** and **Remote Port 6000** as the following picture.



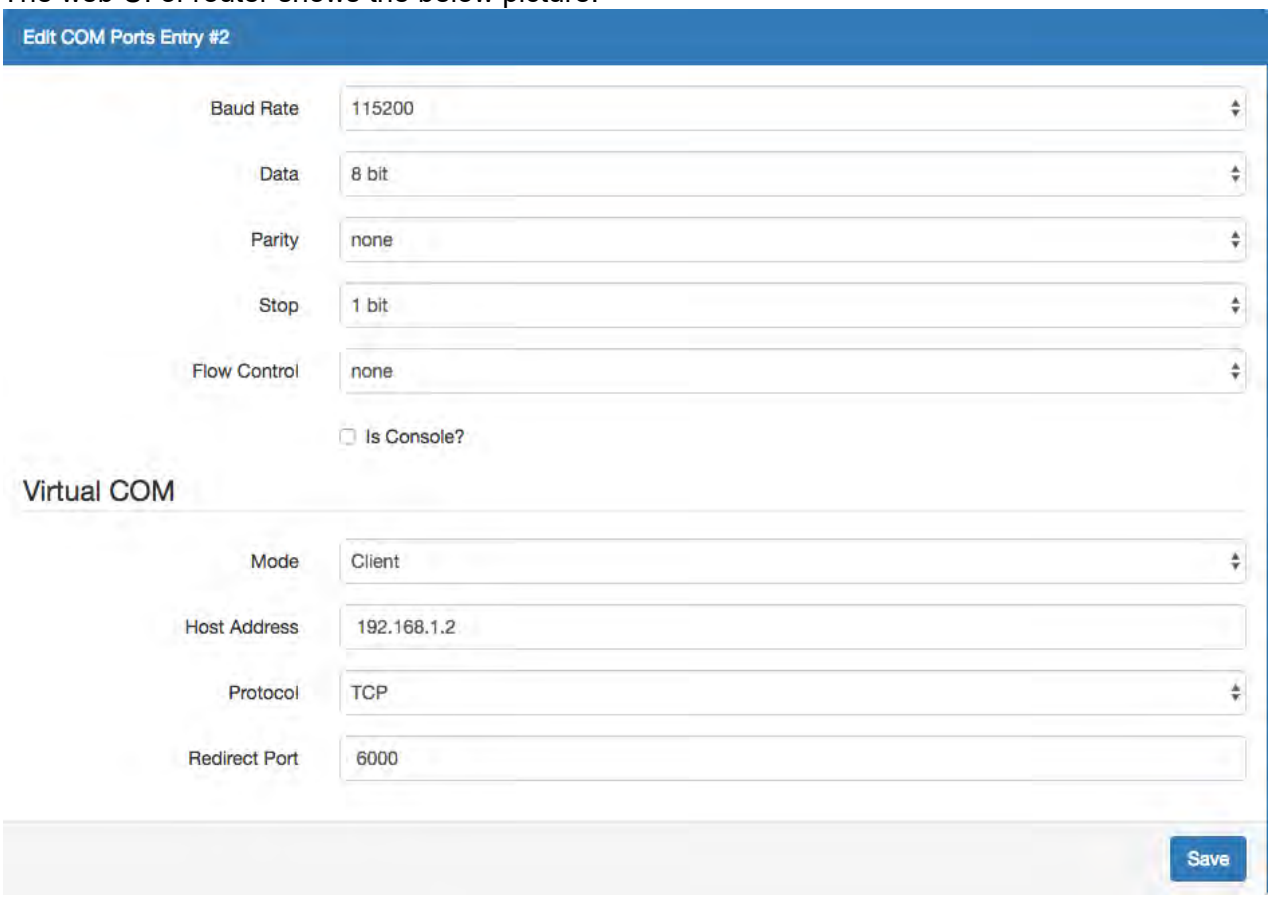


12.5 Virtual COM > Remote Alarm



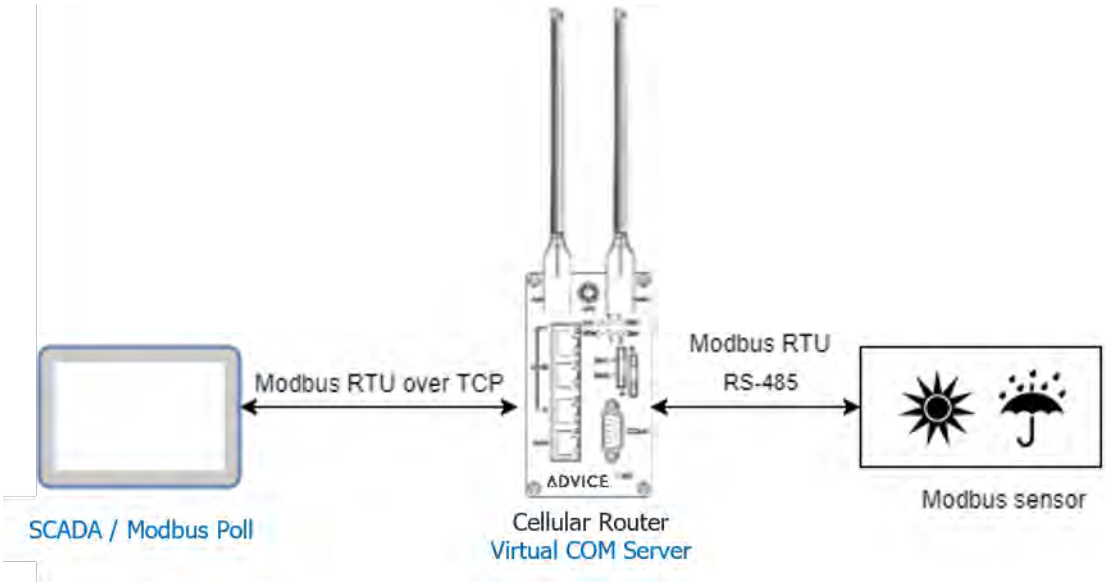
When the router connected with the alarm device, the alarming data from the device can be forwarded by the router to the warning center. Same as the remote management, the serial settings of connected COM port need to be configured properly. And the virtual should be opened and run as **Client** mode. Also, you need to specify the **remote host** and the **port**.

The web UI of router shows the below picture.

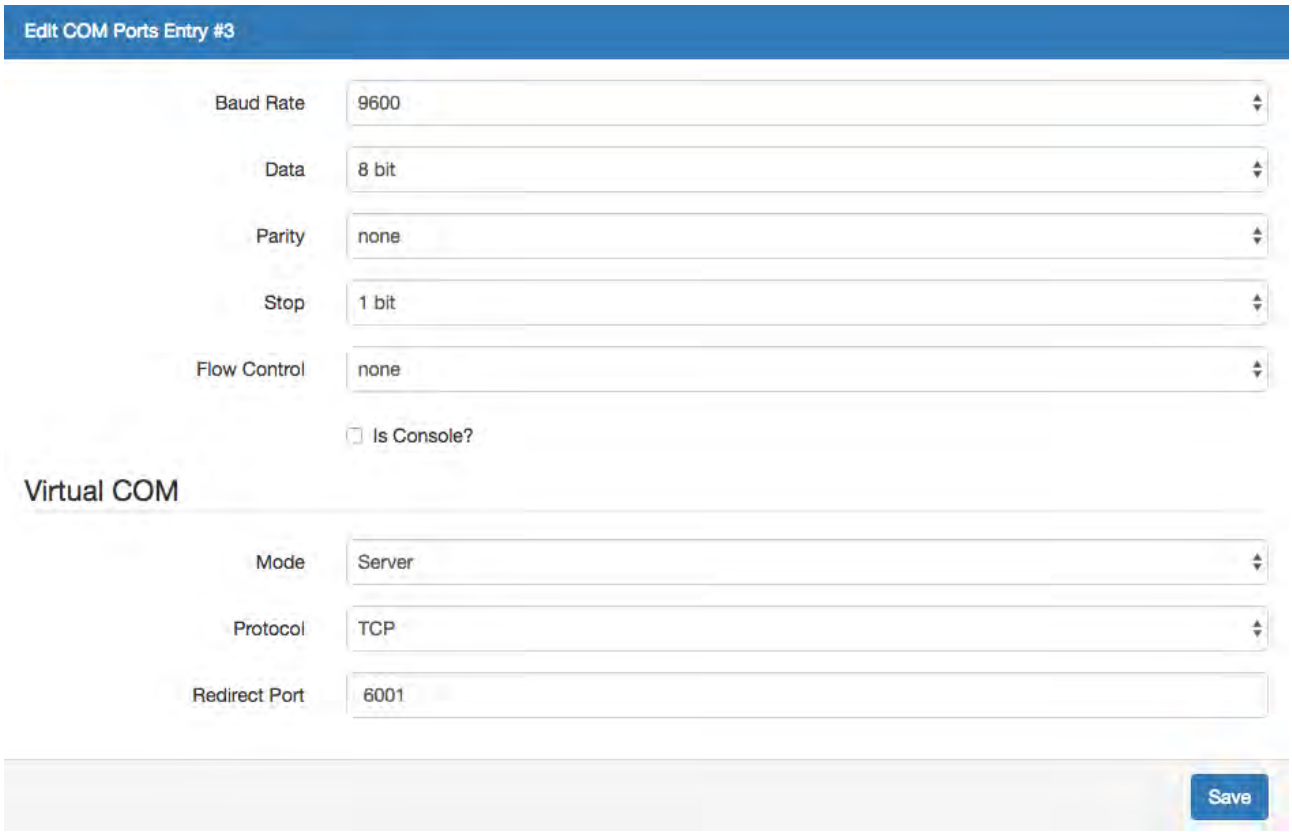


After the above setup, the warning center will receive the data when the alarm device sent the data/message.

12.6 Virtual COM > Modbus RTU over TCP

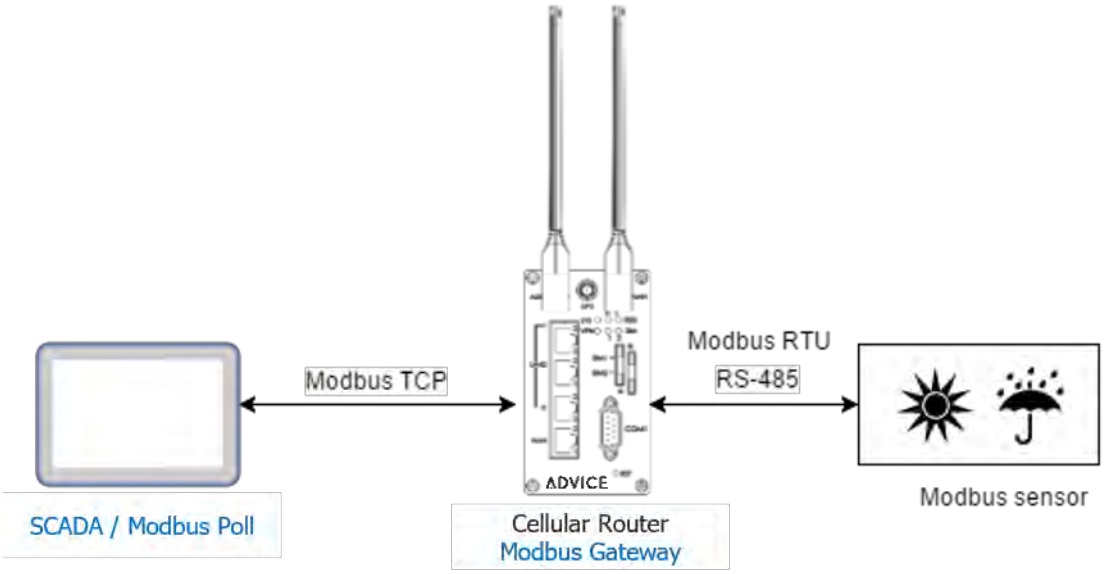


For the industrial products, the Modbus protocol is the most popular industrial control protocol. If the Modbus software/SCADA supported the Modbus RTU over TCP, the Virtual COM server feature of router could handle it. You need to configure the RS-485(COM3) like the remote management (serial settings, Virtual COM settings).

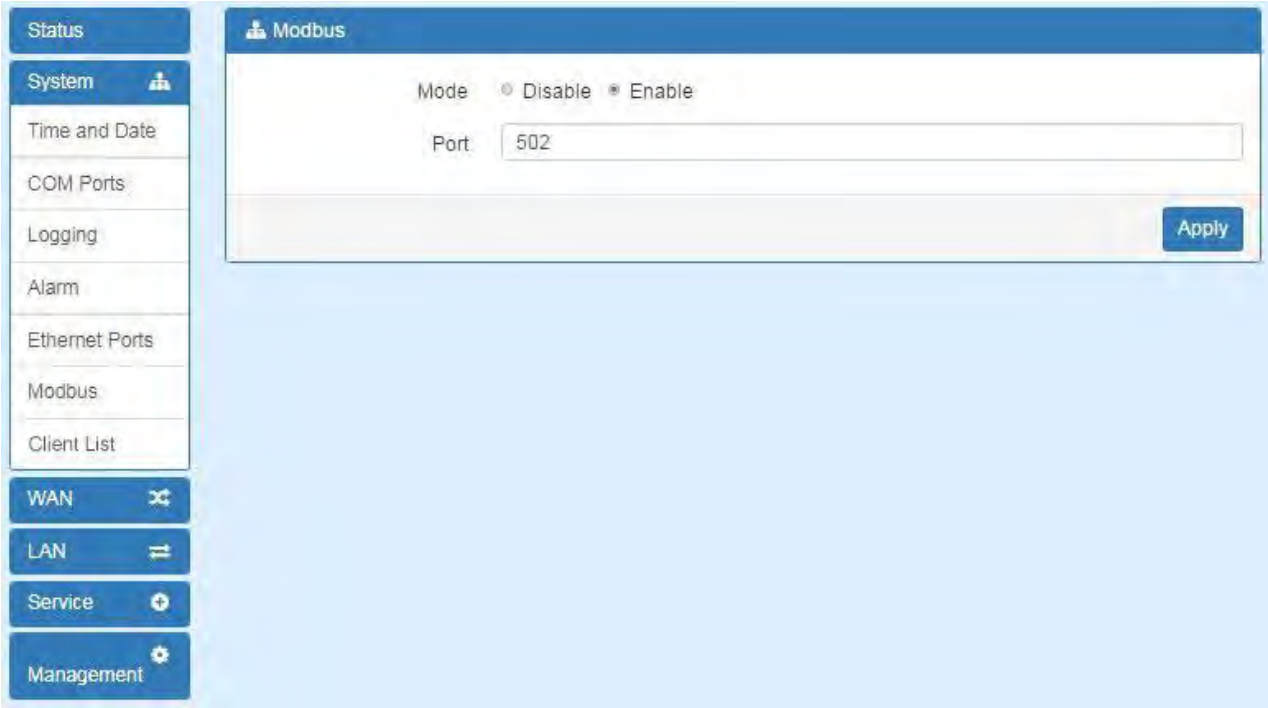


After above setup, you can use the Modbus software which supported the Modbus RTU over TCP to control the Modbus sensor/device.

12.7 Modbus Gateway



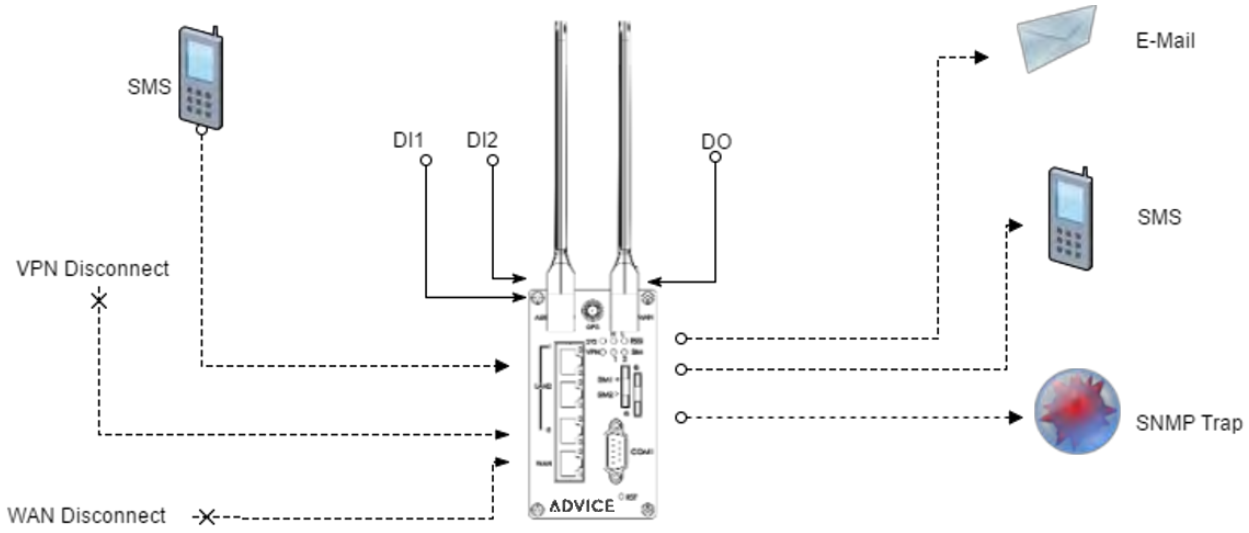
The Modbus gateway feature of router could convert the Modbus TCP to the Modbus RTU protocol and send it to the connected RS-485 device. This feature depends on the COM3 setting, you need to configure the serial setting in the **System -> COM ports** web UI and set up this feature in the **System -> Modbus** web UI.



After above setup, the Modbus software can use the Modbus TCP protocol to control the Modbus sensor/device.

12.8 Alarm Configuration

After you enable alarm, all the selected alarm input events would trigger selected alarm output.

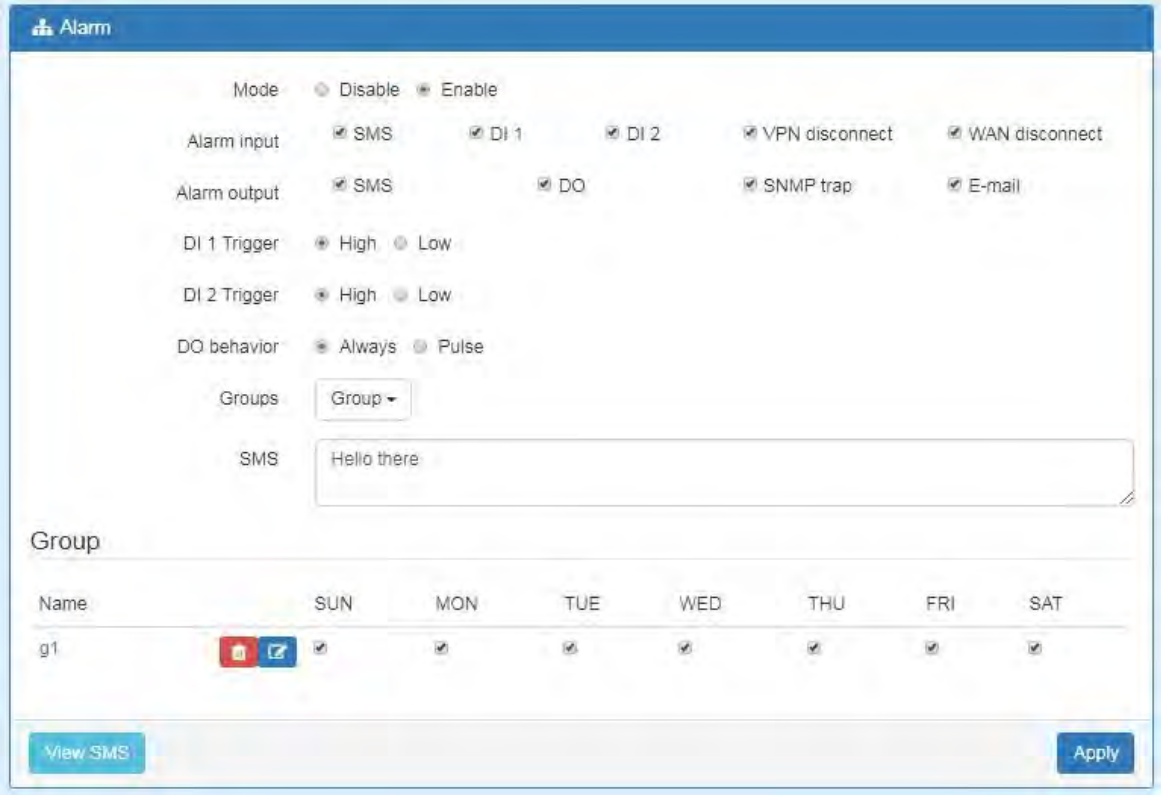


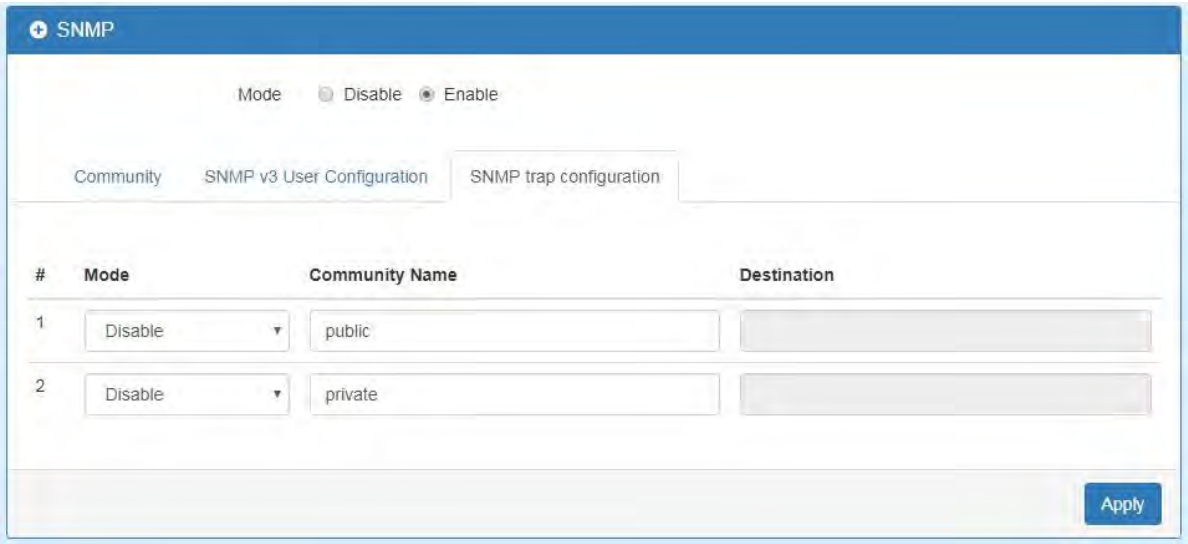
(1) Alarm Input:

- The alarm would be triggered when DI1/DI2 show(s) high signal.
- The user's phone number is in device contact phone book can send a SMS to device SIM card to trigger alarm.
- VPN / WAN disconnect would trigger alarm no matter which interface is currently using.

(2) Alarm Output:

- In case of SMS is selected then only user's phone number is in selected group and on selected working day would receive alarm SMS.
- In case of DO is selected, please make sure your DO is connected to your alarm device.
- In case of SNMP trap is selected, please make sure you enable SNMP trap (Service→SNMP) and fill our server IP.





12.9 OpenVPN Configuration

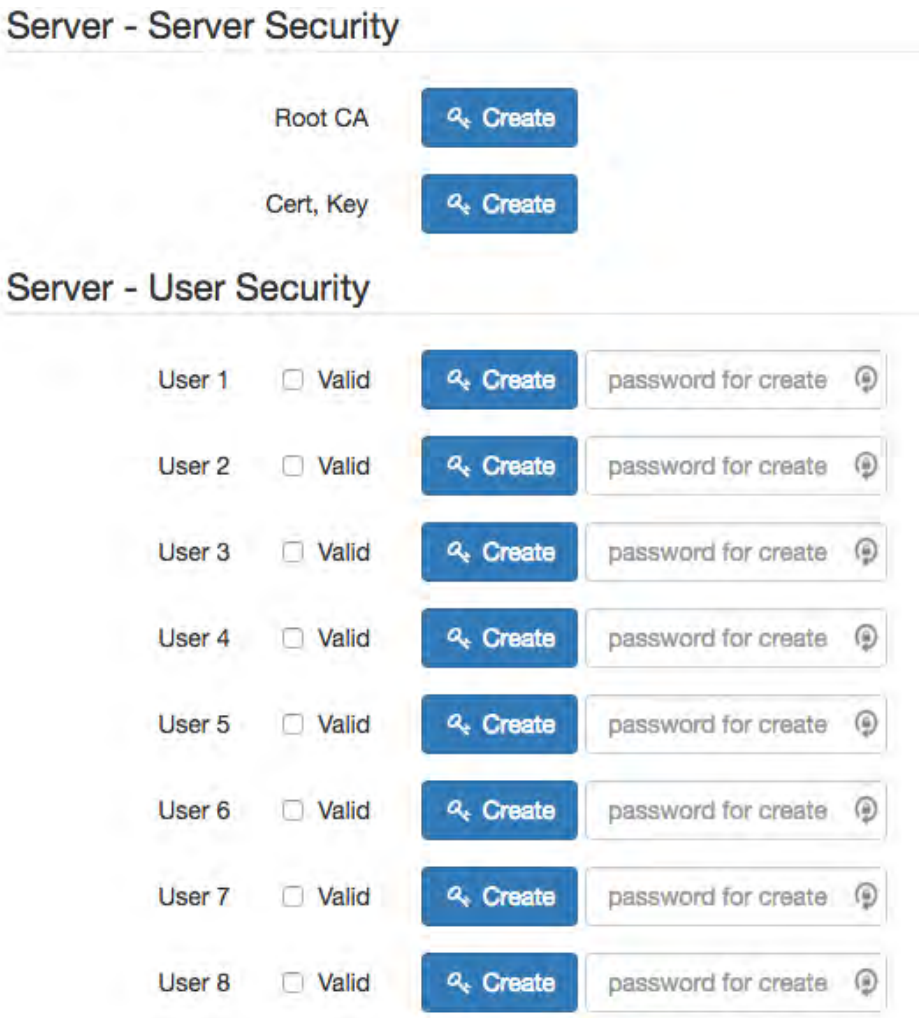
Generic setup

For OpenVPN configuration, use the certificate to authenticate the VPN connection.

Thus, you need to generate the required files for OpenVPN server or import the required file to OpenVPN client.

12.9.1 OpenVPN Server Mode

OpenVPN server certificate generation

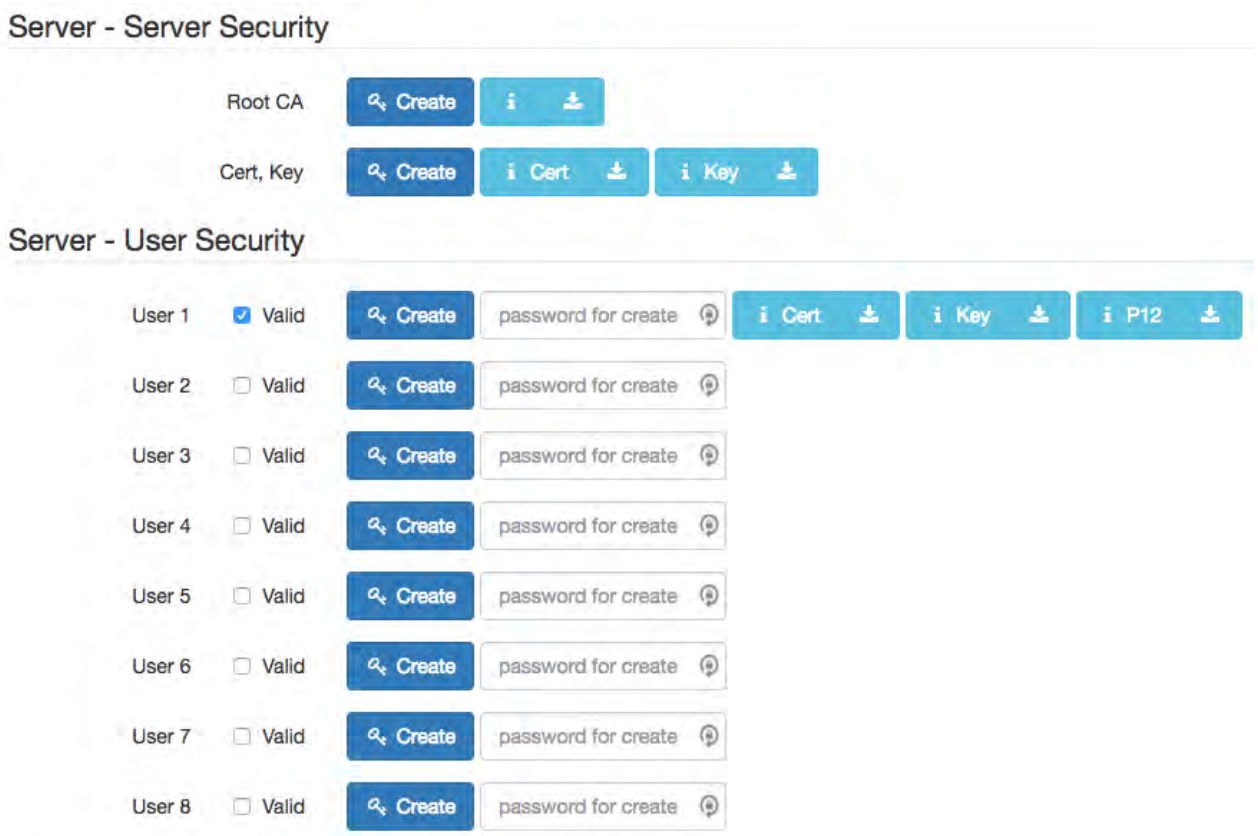


For the OpenVPN server mode, the OpenVPN web UI provides the buttons to generate the required files. The files include **Root CA**, **Cert**, **Key** and **OpenVPN** client files. The file will be generated when you click the corresponded **Create** button.

Note: The **Cert**, **Key** generation will takes around 10 minutes.

To generate the OpenVPN client files, you need to type the password to create it.

The password will be used in the OpenVPN client when the client use **PKCS#12** to authenticate the VPN connection. After the generation, the web UI shows the below picture.



And you can click the info button to show the detail for each files, or click the download button to download the file to PC.

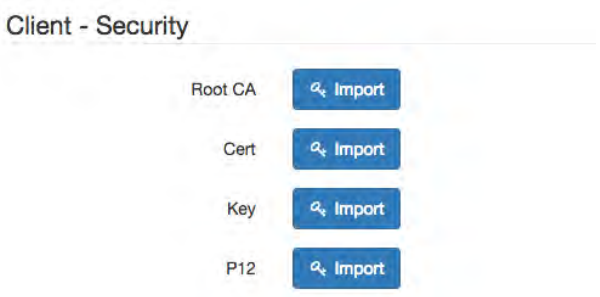
12.9.2 OpenVPN Client Mode

OpenVPN client certificate import

For the OpenVPN client mode, the OpenVPN web UI provides the buttons to import the required files.The OpenVPN client can use the **Root CA**, **User Key** and **User Cert** files from OpenVPN server to authenticate the VPN tunnel. Or just only use the **PKCS#12 (P12)** file from OpenVPN server to authenticate it.

Note: The PKCS#12 files will contain the Root CA, User Key and User Cert.

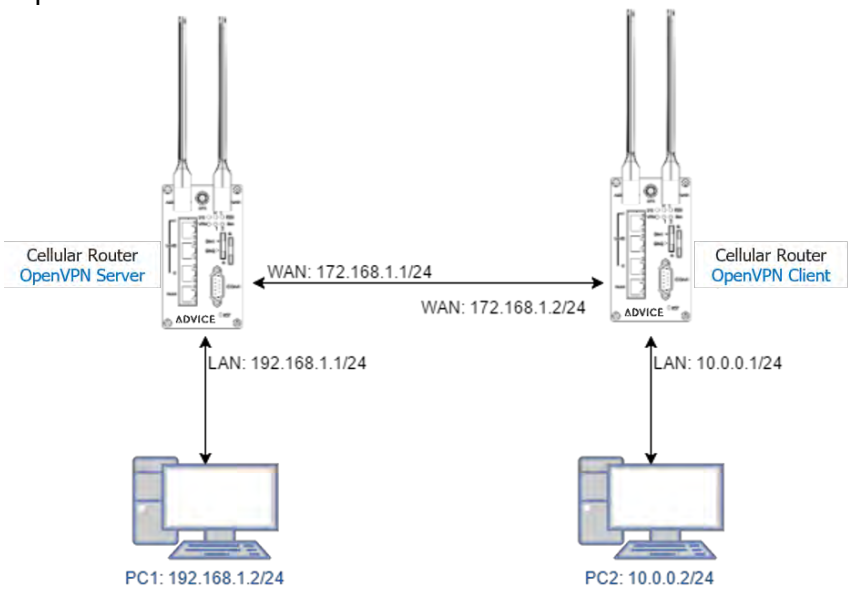
When the files are imported, the web UI is as shown in the right-bottom picture.



Same as OpenVPN server part, you can use the info/download buttons to get the information of file or download the file to PC.

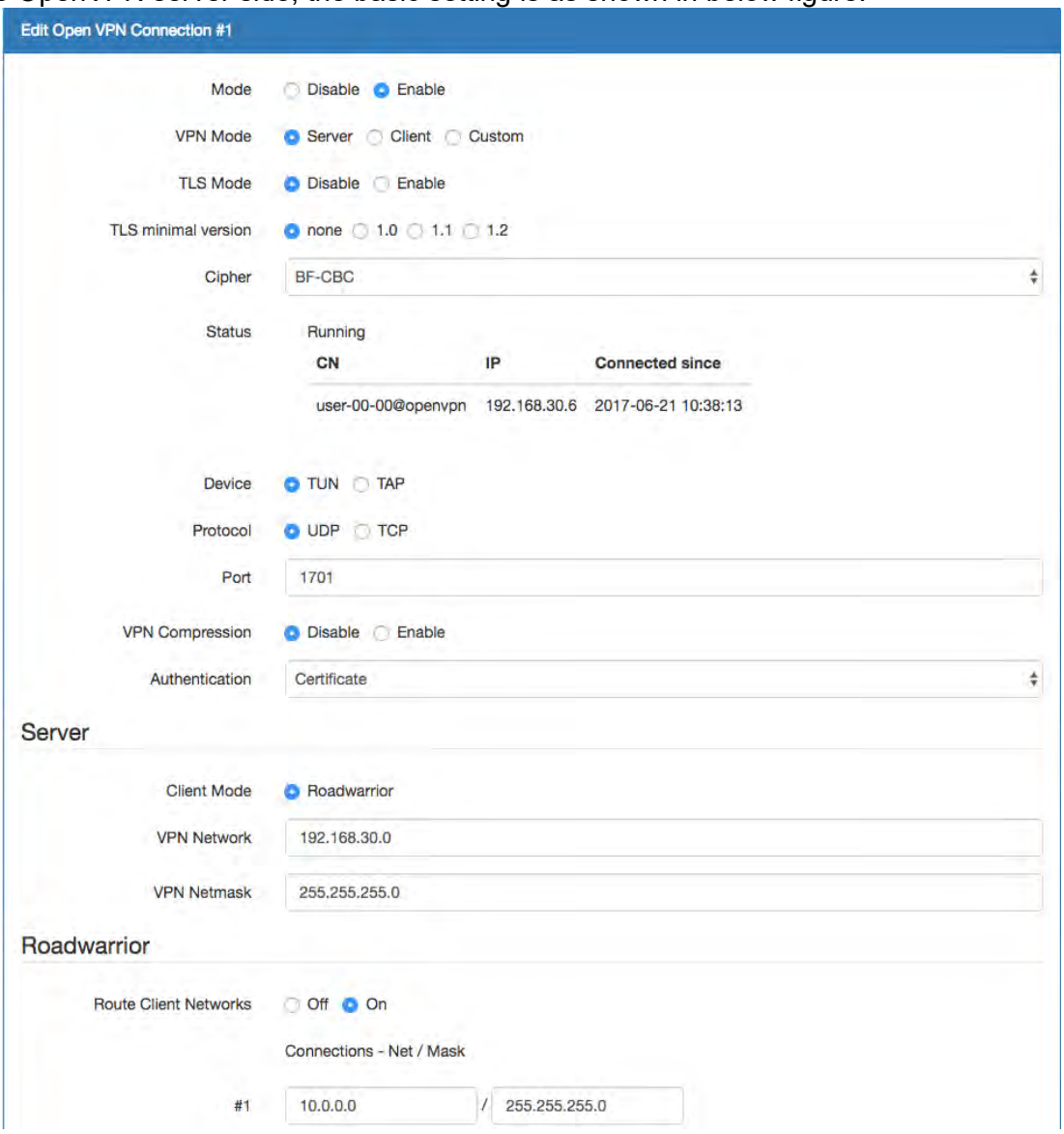
12.9.3 OpenVPN Net-to-Net

You can use the OpenVPN VPN tunnel to make the PC1 and PC2 communicate each other.



(1) OpenVPN server configuration

For the OpenVPN server side, the basic setting is as shown in below figure.



The **VPN Network** and **VPN Netmask** are required fields.

Note: The **VPN Network** should be network ID (e.g. **192.168.30.1** is invalid setting.)

When PC1 and PC2 communicate each other, the Route Client Networks should be enabled. And add the LAN information of OpenVPN client side, in this case the **#1** route will be **10.0.0.0** and **255.255.255.0**

Note: The **#1** route means the routing information for **User 1**.

If all settings set up properly, the web UI will show the **Apply OK** and the OpenVPN server status should be **Running**. When OpenVPN Client mode is connected, the status will show the information which client is connected, IP address and connected time.

Status	Running		
	CN	**IP**	**Connected since**
	user-00-00@openvpn	192.168.30.6	2017-06-21 10:38:13

In the status, the **CN** field will indicate which client is connected and the **user-00-00@openvpn** value is from the **User 1** certificate information. You can check it by clicking the information button, the web UI will display the window as the below figure.

192.168.1.1/cgi-bin/openvpn.cgi?act=info&file=cert&type=user&conn_id=0&user_i...

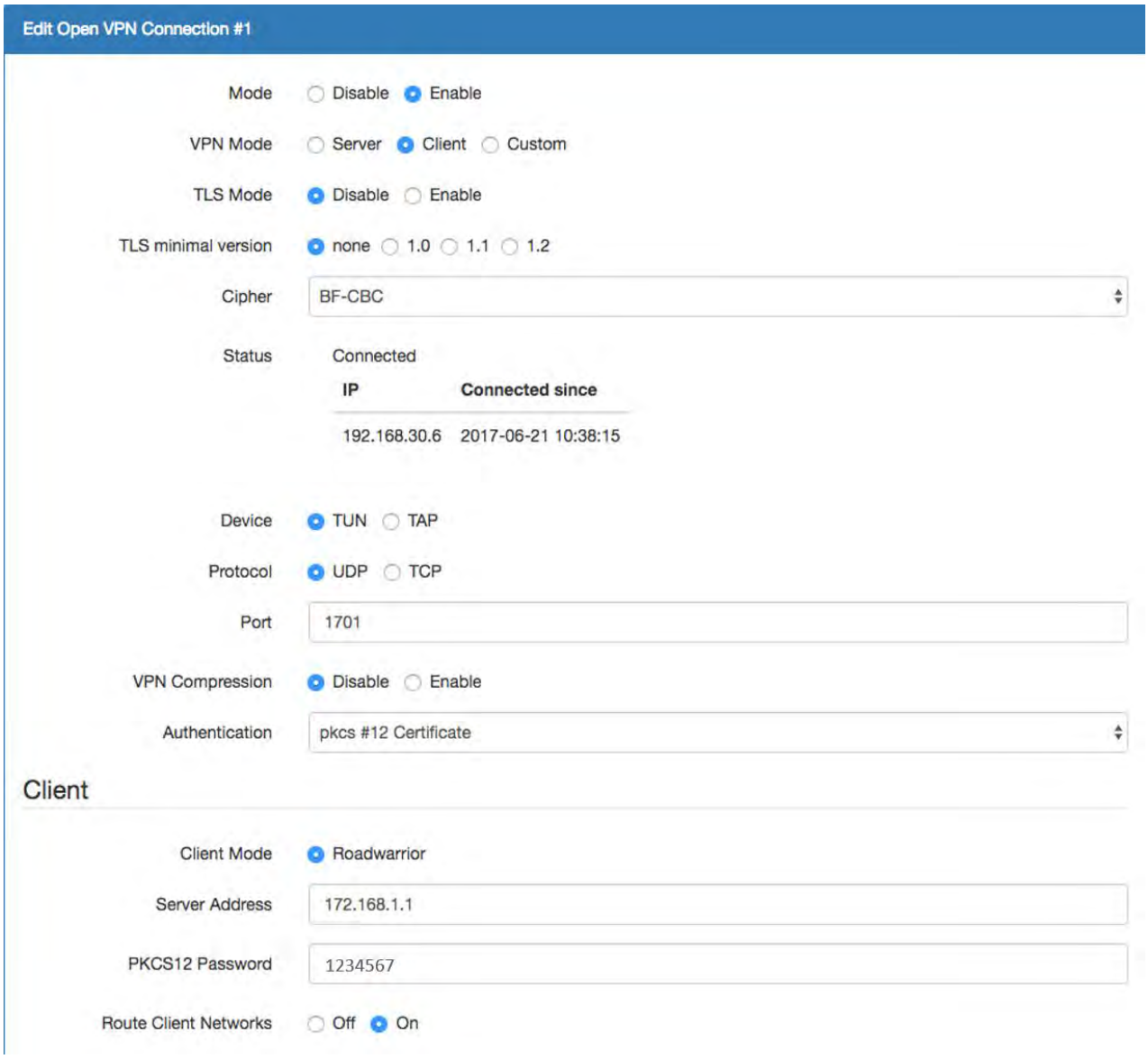
192.168.1.1/cgi-bin/openvpn.cgi?act=info&file=cert&type=user&conn_id=0&user_id...

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CH, O=strongSwan, CN=OpenVPN
        Validity
            Not Before: May  9 06:34:08 2017 GMT
            Not After : May  7 06:34:08 2027 GMT
        Subject: C=CH, O=strongSwan, CN=user-00-00@openvpn
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ac:b1:ca:c7:74:18:70:ed:71:88:9e:c4:ba:d1:
                    c4:09:52:b8:11:d7:17:00:e4:dd:e5:a7:f4:e1:f6:
                    1c:10:b5:0c:d2:27:e7:f8:63:cb:e2:30:78:6c:ab:
                    e3:eb:bd:08:a0:64:ed:1c:6d:97:8f:75:be:21:0d:
                    47:1f:ca:66:6e:52:a8:c2:40:98:01:21:73:73:b5:
                    62:c7:ab:a7:39:6b:94:7b:db:b4:a4:45:33:39:00:
                    5b:92:f6:05:4c:18:e1:7d:1b:0b:35:ed:3b:da:0e:
                    1c:f3:0e:db:04:e0:90:53:da:f5:87:91:d9:af:0f:
                    3d:82:c3:12:ec:4a:e2:ed:77:d9:ca:89:2a:73:c9:
                    e7:4f:a3:97:ff:97:f1:c4:f0:de:12:c0:ae:12:73:
                    3f:63:30:dd:e8:87:97:59:34:e7:a7:1f:a0:53:c5:
                    b1:f6:4d:10:2f:96:bd:f1:80:cc:62:5a:66:d8:30:
                    29:c6:f3:fa:7a:69:4a:6a:67:0b:85:e7:8f:76:a4:
                    fc:47:af:e5:1e:76:96:1c:f0:2b:64:d7:d0:02:50:
                    63:43:ae:65:ad:88:73:b0:19:67:08:a4:60:6a:f1:
                    03:93:62:f1:e3:0a:b3:70:82:dc:8b:85:a4:95:98:
                    fb:f5:f8:81:2b:a5:55:8a:f7:1c:15:41:c2:f5:8b:
                    ae:ed
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
         54:fd:09:0b:23:5b:d1:22:e3:17:1e:de:5c:48:1c:30:30:c7:
         01:d8:6d:46:f4:91:4c:84:16:35:ea:79:91:67:dc:91:63:88:
         6a:23:7b:fe:8c:e0:93:14:a1:1e:1d:32:c2:22:84:af:22:ff:
         a9:9d:2f:aa:b2:0c:8b:86:c3:bc:46:8e:9d:5c:f8:55:39:91:
         cc:03:17:40:e9:d5:bb:df:e9:34:aa:89:71:f7:ea:1c:78:78:
         99:38:ba:7b:ec:d7:de:1a:d0:a0:07:58:cc:8a:4a:cc:2e:54:
         b3:d9:46:03:8e:58:cb:ef:de:95:61:01:33:9f:40:4c:cb:1b:
         3e:3e:70:4a:07:62:8c:d4:f0:53:86:42:c7:13:30:a8:3a:76:
         d3:bf:9d:33:7b:50:c3:98:fd:f0:ed:2a:c3:00:b8:dc:e0:80:
         a9:4b:0c:e1:ad:fc:32:76:03:b8:2f:9f:2a:d1:bb:1b:e7:cb:
         62:d2:63:be:7c:21:ac:b5:91:14:55:96:fc:67:94:cc:1f:7b:
         82:12:e6:84:da:fe:12:3e:73:bf:62:bb:1a:14:57:45:ce:28:
         95:e1:1f:d9:86:cb:36:c6:4d:b8:04:af:f6:0e:f4:f4:31:ba:
         6d:ef:cc:75:bc:0e:db:19:c7:c2:2c:b3:62:60:c2:88:d9:a3:
         cf:d4:8b:25
-----BEGIN CERTIFICATE-----
MIIC5zCCAc8CAQEwDQYJKoZIhvcNAQELBQAwNDELMAkGA1UEBhMCQ0gxEzARBgNV
BAoMCnN0cm9uZ1N3YW4xEDAOBgNVBAMMB09wZW5WUE4wHhcNMTcwNTA5MDYzNDA4
WhcNMjcwNTA3MDYzNDA4WjA/MOswCOYDVOOGEwJDSDETMBEGA1UECgwKc3Rvb25n
```

The CN information of user certificate is as shown in the subject field.

(2) OpenVPN client configuration

For the OpenVPN client side, the basic setting is as below figure.

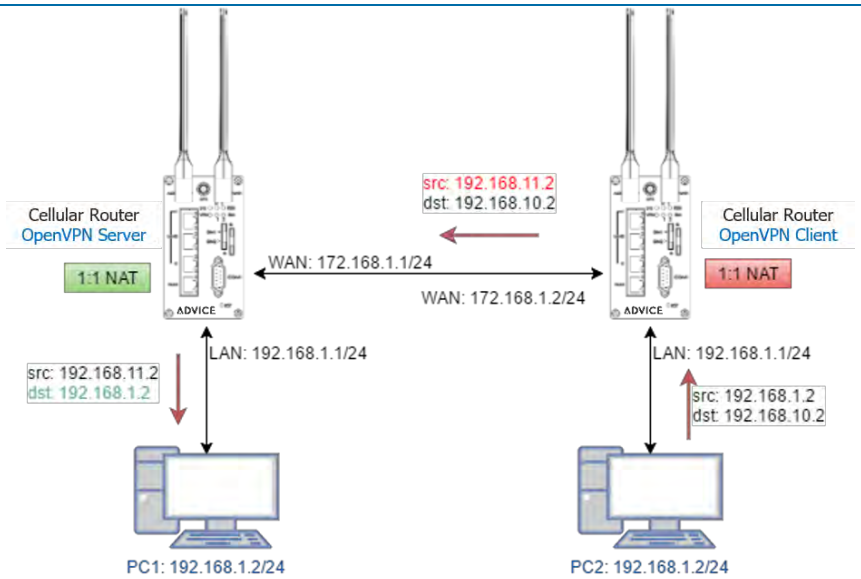


The **Server Address** is required field, which indicate the OpenVPN server address which OpenVPN client try to connect. And the **PKCS12 Password** only works when selected the **pkcs #12 Certificate** authentication option.

This option require the P12 file which generated from Generic Setup OpenVPN server part.
The password also be set on the Generic Setup OpenVPN server part.
If you use the Certificate authentication option, the OpenVPN client will require the **Root CA**, **User cert** and **User key** files.

Same as the OpenVPN server configuration part, OpenVPN client web UI also provides the status information. When all settings set up properly, the status will change from **Idle** to **Running**. When OpenVPN tunnel is created, the status shows **Connected** and the information for IP address and the time.

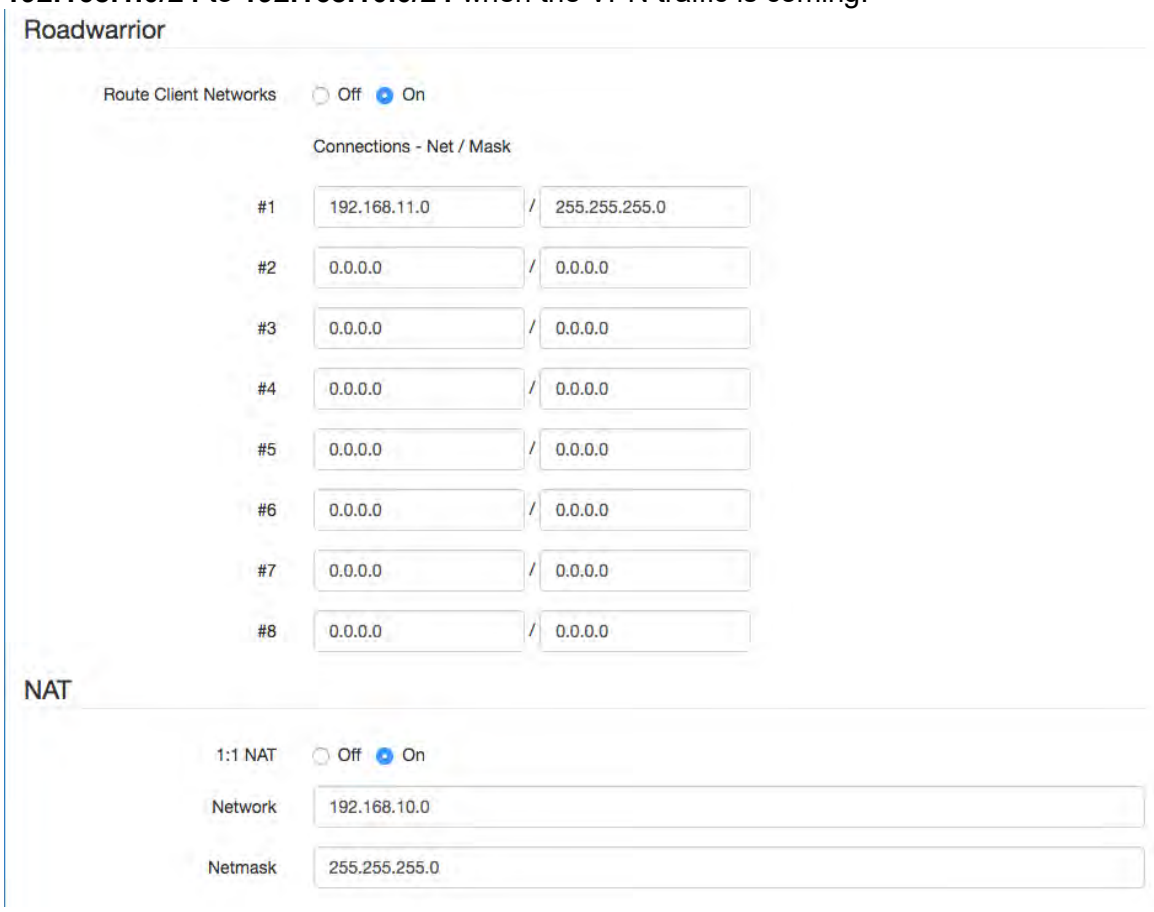
12.9.4 OpenVPN 1:1 NAT



For the net-to-net part, the OpenVPN server LAN network and the OpenVPN client LAN network are different. But some time, the LAN network will be same for both sides.

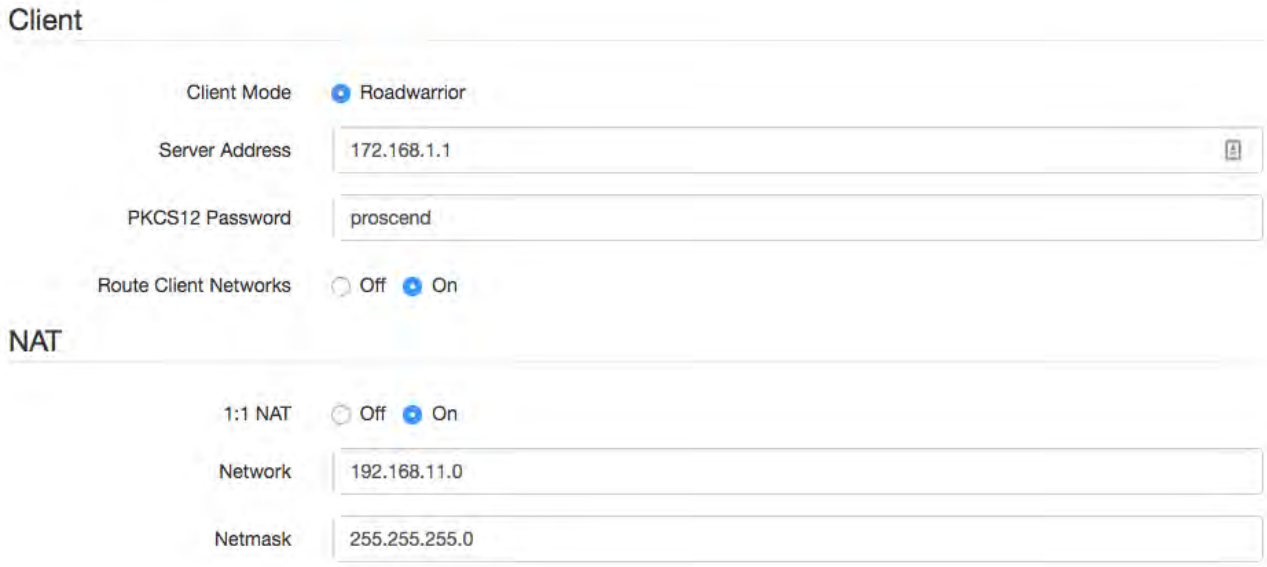
When this situation occurred, the routing rules will be ambiguous that will result in the PC1 and the PC2 can't communicate each other. Thus, the router OpenVPN provides the 1:1 NAT feature. The feature will convert the conflict subnet to different subnet. In this case, you can use 1:1 NAT feature to convert the OpenVPN server and client side LAN network.

For the OpenVPN server side, we fill up the Network be **192.168.10.0** and Netmask **255.255.255.0**. The setting will make the router convert the OpenVPN server side LAN network from **192.168.1.0/24** to **192.168.10.0/24** when the VPN traffic is coming.

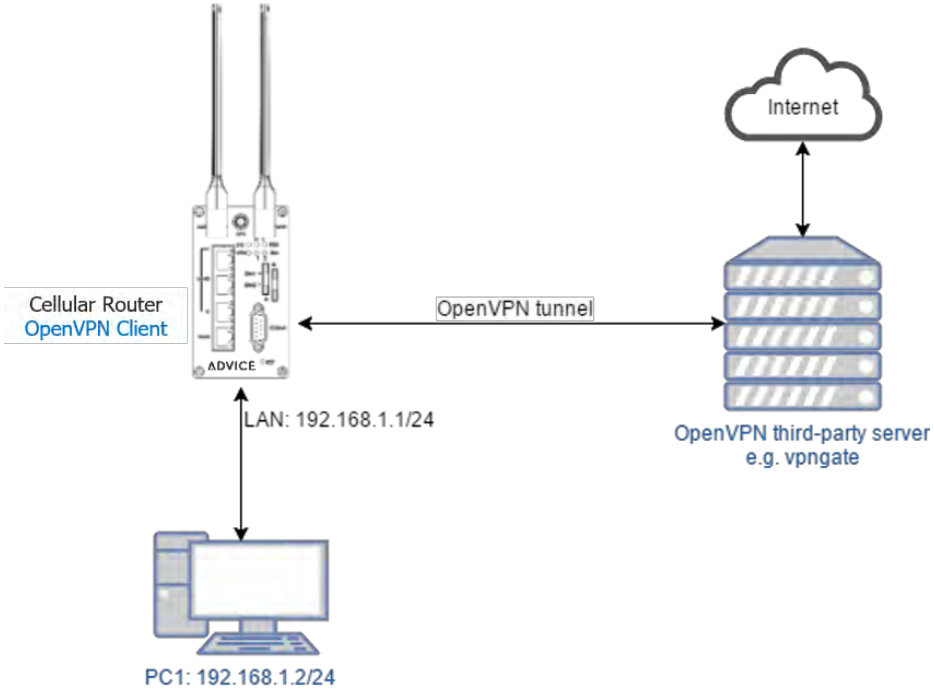


For the OpenVPN client side, same as server side but we fill up the Network as **192.168.11.0**.

The setting will make router convert the OpenVPN client side LAN network from **192.168.1.0/24** to **192.168.11.0/24** when the VPN traffic is coming.



12.9.5 OpenVPN with third-party server

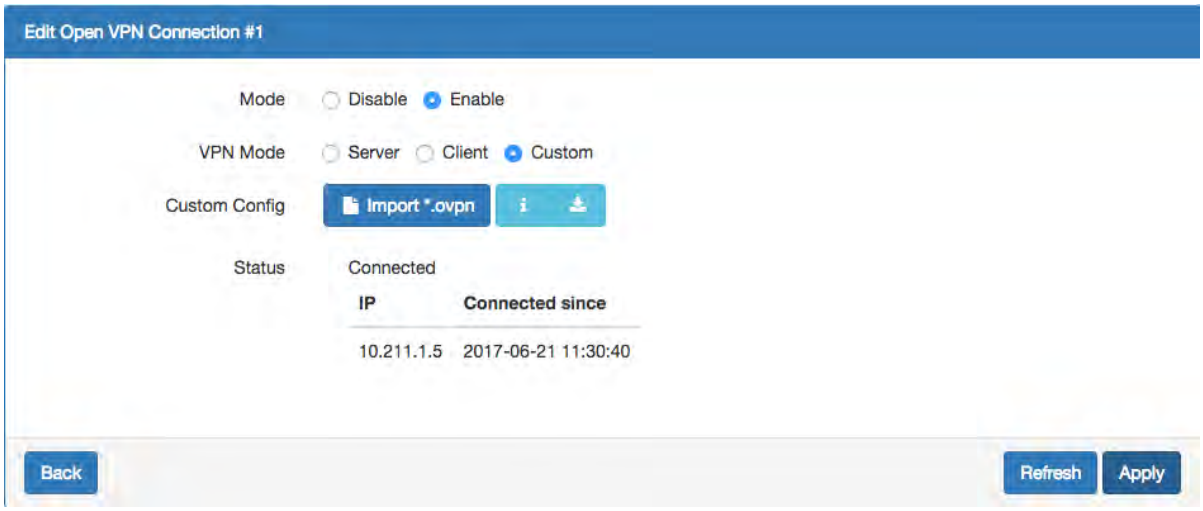


A VPN enables you to send and receive data across shared networks.

For some users, they will use the VPN to access the limited network service from the different country. But normally, the third-party OpenVPN server will provide the **.ovpn** configuration files for the OpenVPN client. The **.ovpn** is hard to convert to the cellular router OpenVPN client configuration. So, we provide the **Custom** mode to make the user can easy use the **.ovpn** to set up the cellular router OpenVPN client. The **Custom** mode provide the import button to allow user import the third-party OpenVPN server **.ovpn** configurations file.

For example, use the Japan OpenVPN server which provided by http://www.vpngate.net/en/ .
Firstly, download the .ovpn configuration files from vpngate.net.

Additionally, use the OpenVPN custom import button to import it. The result is as the below figure. If the **.ovpn** configuration file is correct, the web UI will show **Apply OK**.



If the third-party OpenVPN server is reachable, the VPN tunnel will be established.

When the OpenVPN VPN tunnel is established, the status shows **Connected** and the information for IP address and the time. In this moment, the PC1 can visit the http://www.vpngate.net and the web UI should indicate the PC1 in the Japan at now as the below figure.

12.9.6 Install OpenVPN Access Server on Docker

OpenVPN Access Server on Docker installation

OpenVPN Access Server is a full featured secure network tunneling VPN software solution that integrates OpenVPN server capabilities, enterprise management capabilities, simplified OpenVPN Connect UI, and OpenVPN Client software packages that accommodate Windows, MAC, Linux, Android, and iOS environments. OpenVPN Access Server supports a wide range of configurations, including secure and granular remote access to internal network and/ or private cloud network resources and applications with fine-grained access control.

All OpenVPN Access Server downloads come with 2 free client connections for testing purposes.

$15.00 License Fee Per Client Connection Per Year. Support & Updates included. 10 Client minimum purchase.

The detail please look https://openvpn.net/index.php/access-server/pricing.html

Install Docker on Ubuntu 16.04 64bit

Reference: https://docs.docker.com/engine/installation/linux/docker-ce/ubuntu/

Set up the repository

```
sudo apt-get remove docker docker-engine docker.io
sudo apt-get update
sudo apt-get install \
      apt-transport-https \
      ca-certificates \
      curl \
      software-properties-common

curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
sudo add-apt-repository \
    "deb [arch=amd64] https://download.docker.com/linux/ubuntu \
    $(lsb_release -cs) \
    stable"
```

Install Docker CE

```
sudo apt-get update
sudo apt-get install docker-ce
```

Install OpenVPN Access Server by docker image

Reference: https://hub.docker.com/r/linuxserver/openvpn-as/

```
sudo mkdir -p /openvpn-as
sudo docker create --name=openvpn-as \
      -v /openvpn-as:/config \
      -e TZ="Asia/Taipei" \
      -e INTERFACE=enp3s0 \
      --net=host --privileged linuxserver/openvpn-as
sudo start openvpn-as
```

Check the OpenVPN Access Server by visiting https://<server_ip_or_domain>:943

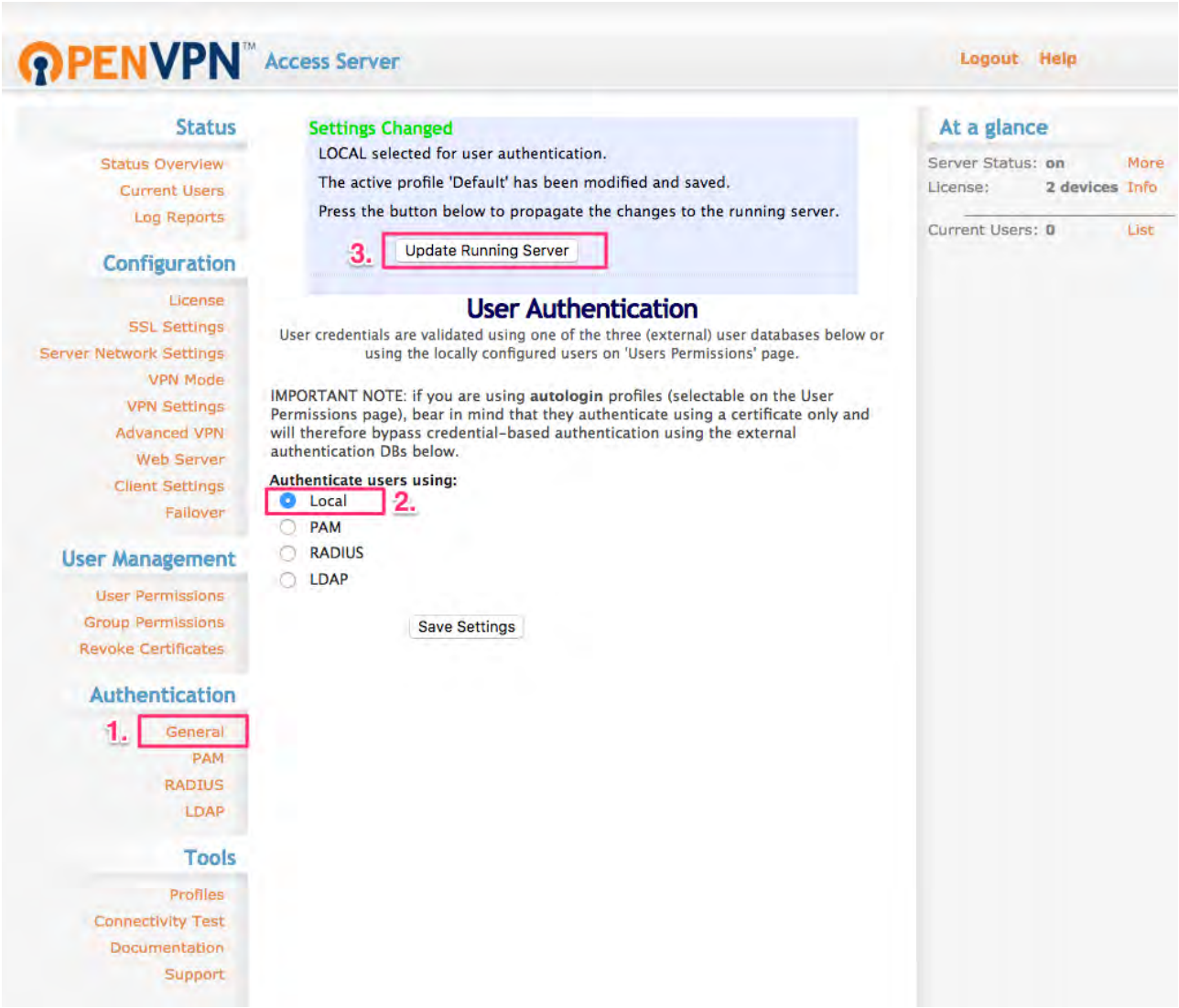
Setup OpenVPN Access Server for Cellular Router

The admin page is https://<server_ip_or_domain>:943/admin

The default administrator username and password is admin/password.

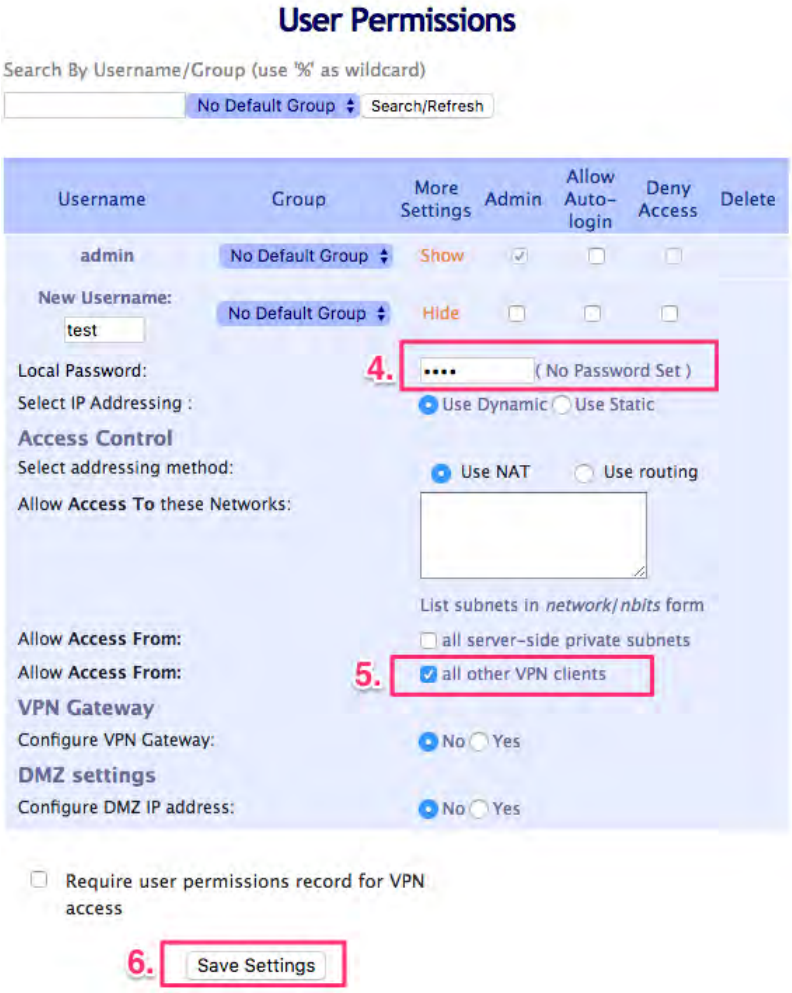
Login page:

After logged, please change the user authentication type to Local like the following figure.



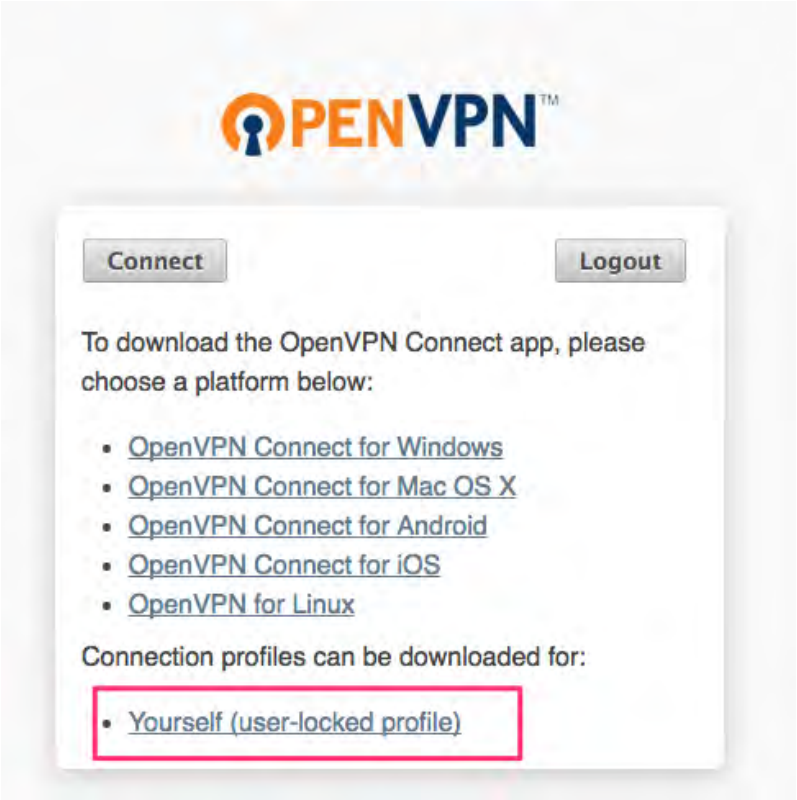
And switch to the User Permission page to create the user for Cellular Router.
(In this case, we use the test/test to be the example.)

Also check the Access From all other VPN clients to make the Cellular Router could be reachable.

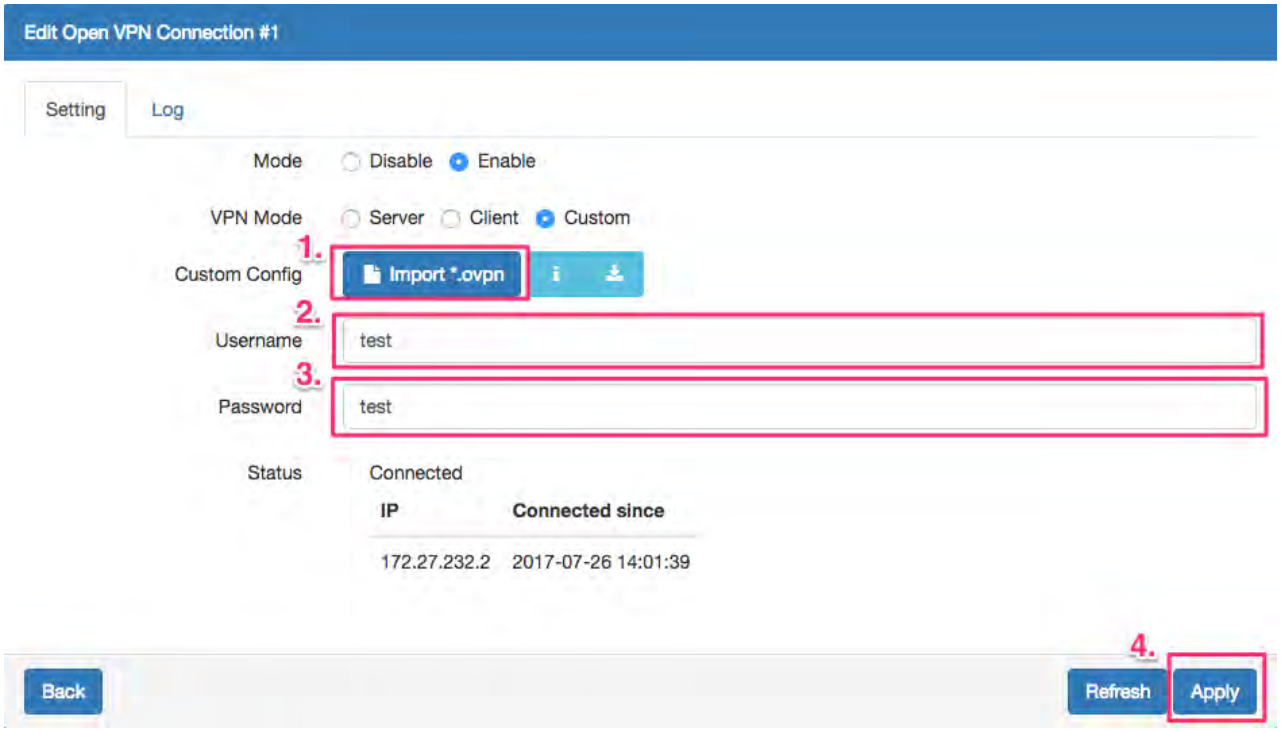


Setup Cellular Router OpenVPN client

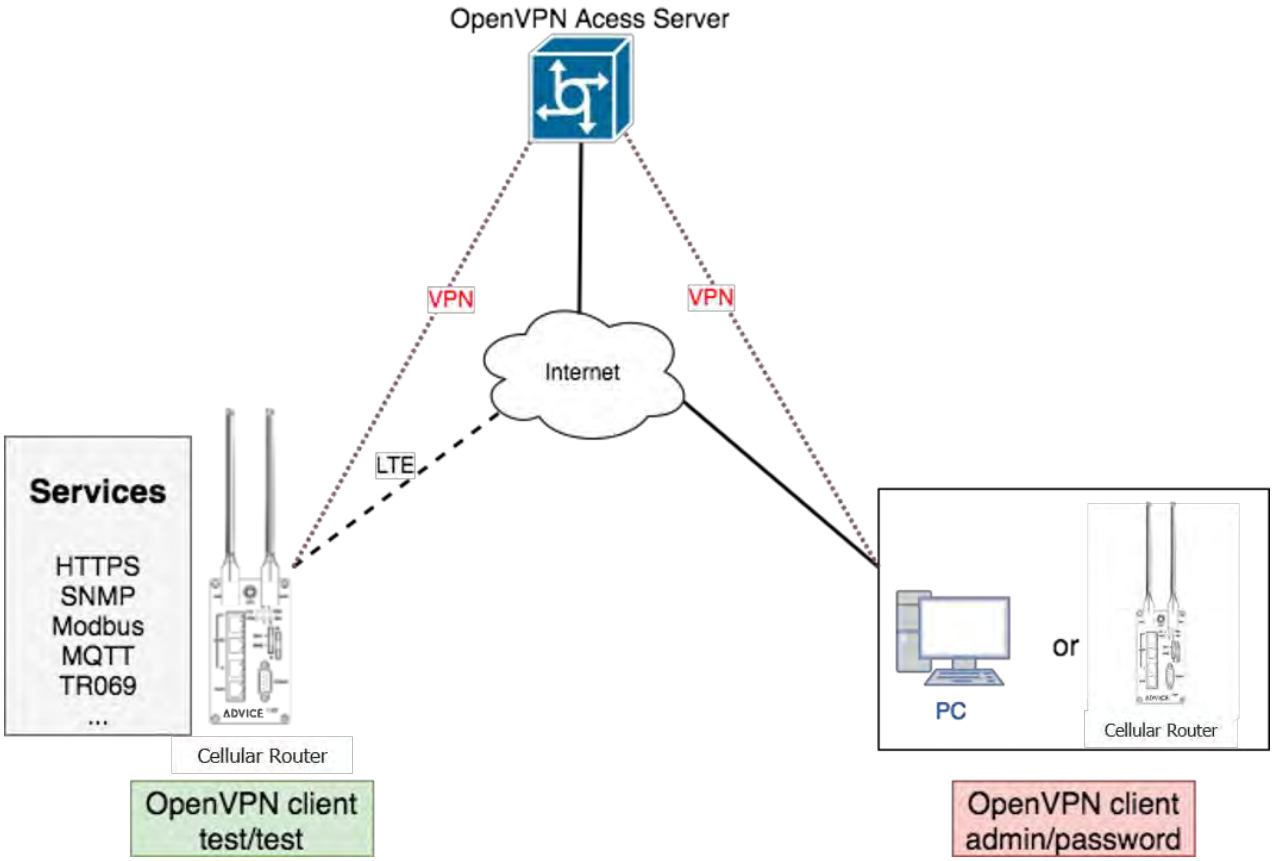
Use the user test/test to login https://<server_ip_or_domain>:943
Please make sure to change the type from Connect to Login.



After logged, please download the .ovpn configuration by click the user-locked profile.



Upload the .ovpn configuration to Cellular Router OpenVPN custom mode, and input the username and password.



When the VPN tunnel established, the Cellular Router can be managed/accessed by the other VPN clients.

12.9.7 Install Pritunl OpenVPN server on Docker

Pritunl OpenVPN server on Docker installation

Pritunl is a distributed enterprise vpn server built using the OpenVPN protocol.
Install Docker on Ubuntu 16.04 64bit
Reference: https://docs.docker.com/engine/installation/linux/docker-ce/ubuntu/

Set up the repository

```
sudo apt-get remove docker docker-engine docker.io
sudo apt-get update
sudo apt-get install \
      apt-transport-https \
      ca-certificates \
      curl \
      software-properties-common

curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
sudo add-apt-repository \
    "deb [arch=amd64] https://download.docker.com/linux/ubuntu \
    $(lsb_release -cs) \
    stable"
```

Install Docker CE

```
sudo apt-get update
sudo apt-get install docker-ce
```

Install Docker compose

```
sudo apt-get install docker-compose
```

Install Pritunl OpenVPN Server by docker compose

(1) Set up the basic environment by the following commands.

```
mkdir ~/pritunl
cd ~/pritunl
touch docker-compose.yml
```

(2) Copy and paste the following content to docker-compose.yml.

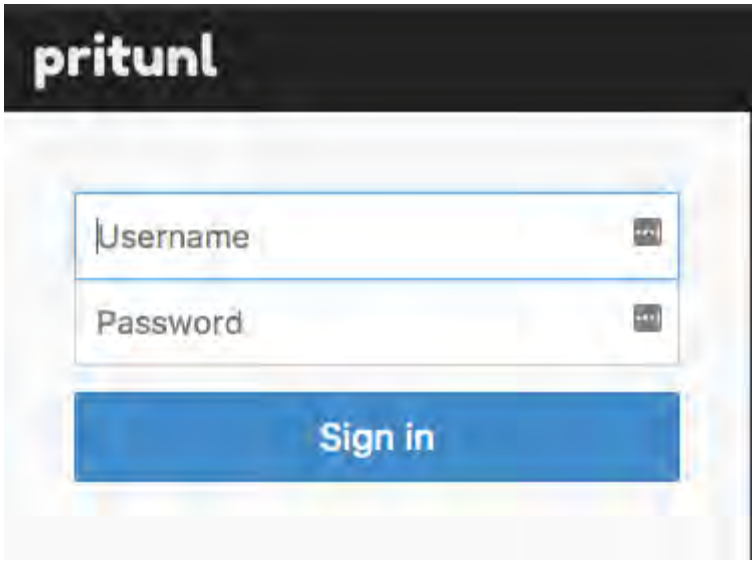
```
version: '2'
services:
   pritunl:
      image: jippi/pritunl
      volumes:
         - pritunl:/var/lib/pritunl
         - mongo:/var/lib/mongodb
      privileged: true
      network_mode: "host"
      ports:
         - "1194:1194/tcp"
         - "1194:1194/udp"
         - "80:80/tcp"
         - "443:443/tcp"

volumes:
   mongo:
   pritunl:
```

(3) Run the command docker-compose up -d to start the server
(4) Check the Pritunl OpenVPN Server by visiting https://<server_ip_or_domain>

Setup Pritunl OpenVPN Server for Cellular Router
The server will running on https://<server_ip_or_domain>.

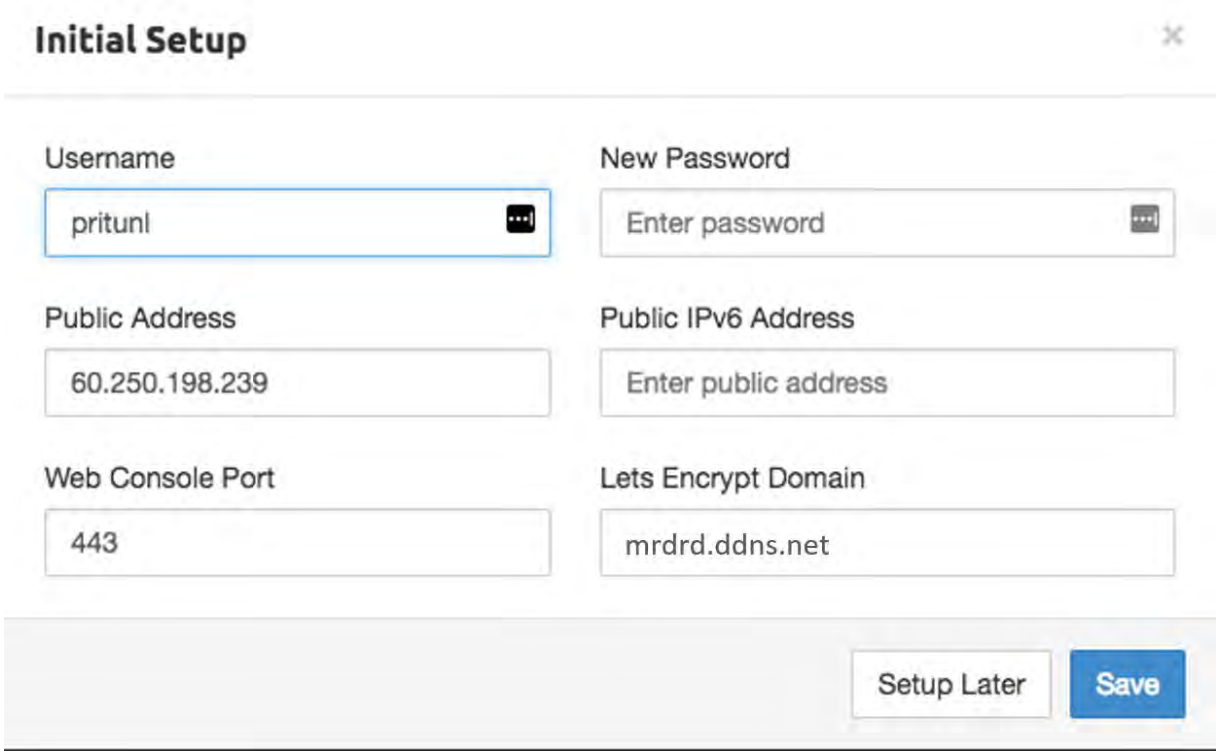
The default username/password is pritunl/pritunl.

Login Page:



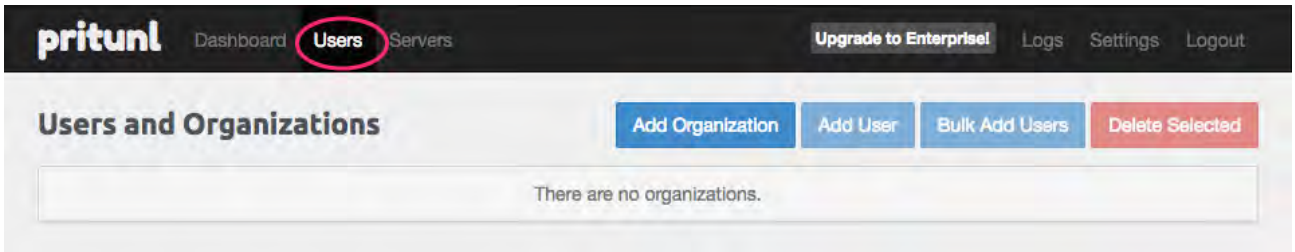
After logged, the server will ask you to do the initial setup. You can change the username and the password setting in this page.

Initial Setup:

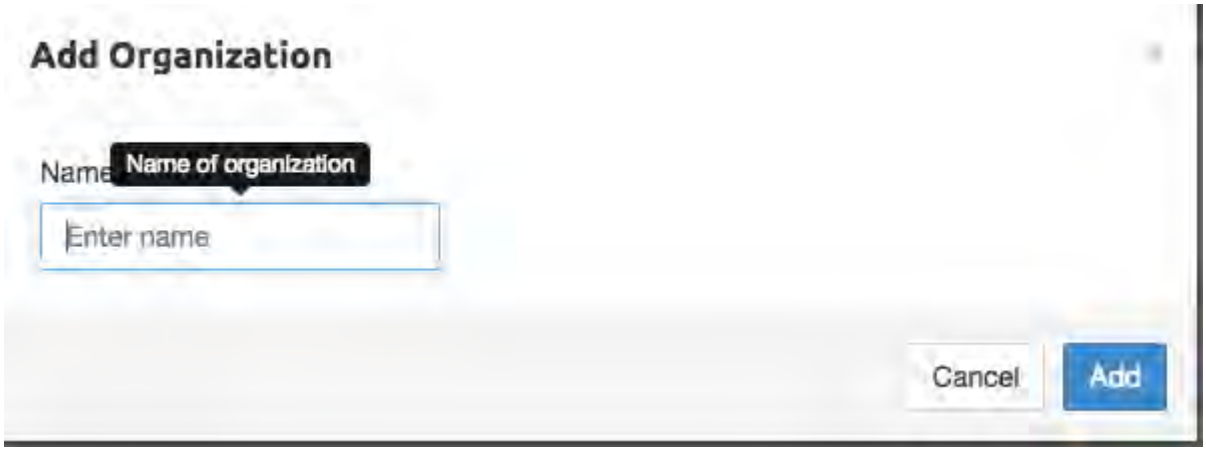


OpenVPN user setup

Please navigate to the User page to setup the OpenVPN user account.

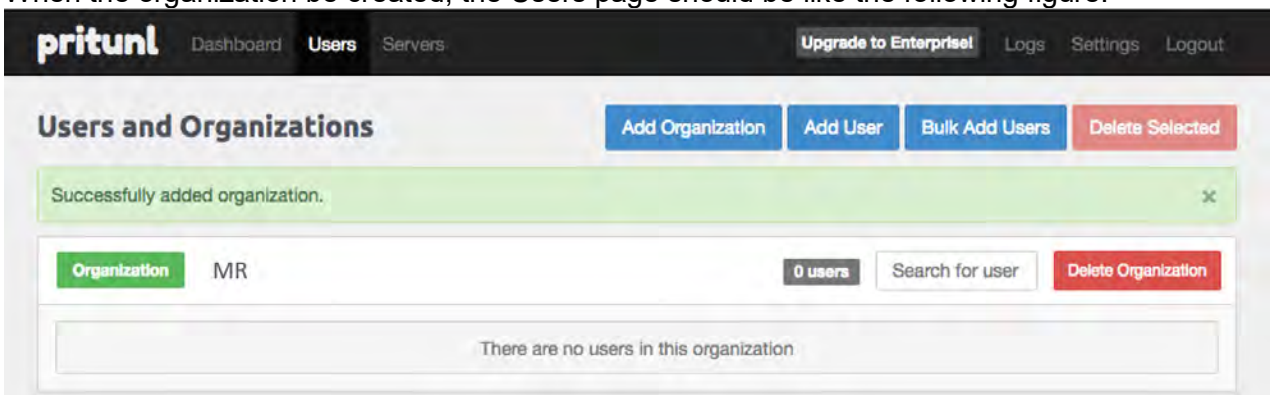


Add the organization by click the Add Organization button.

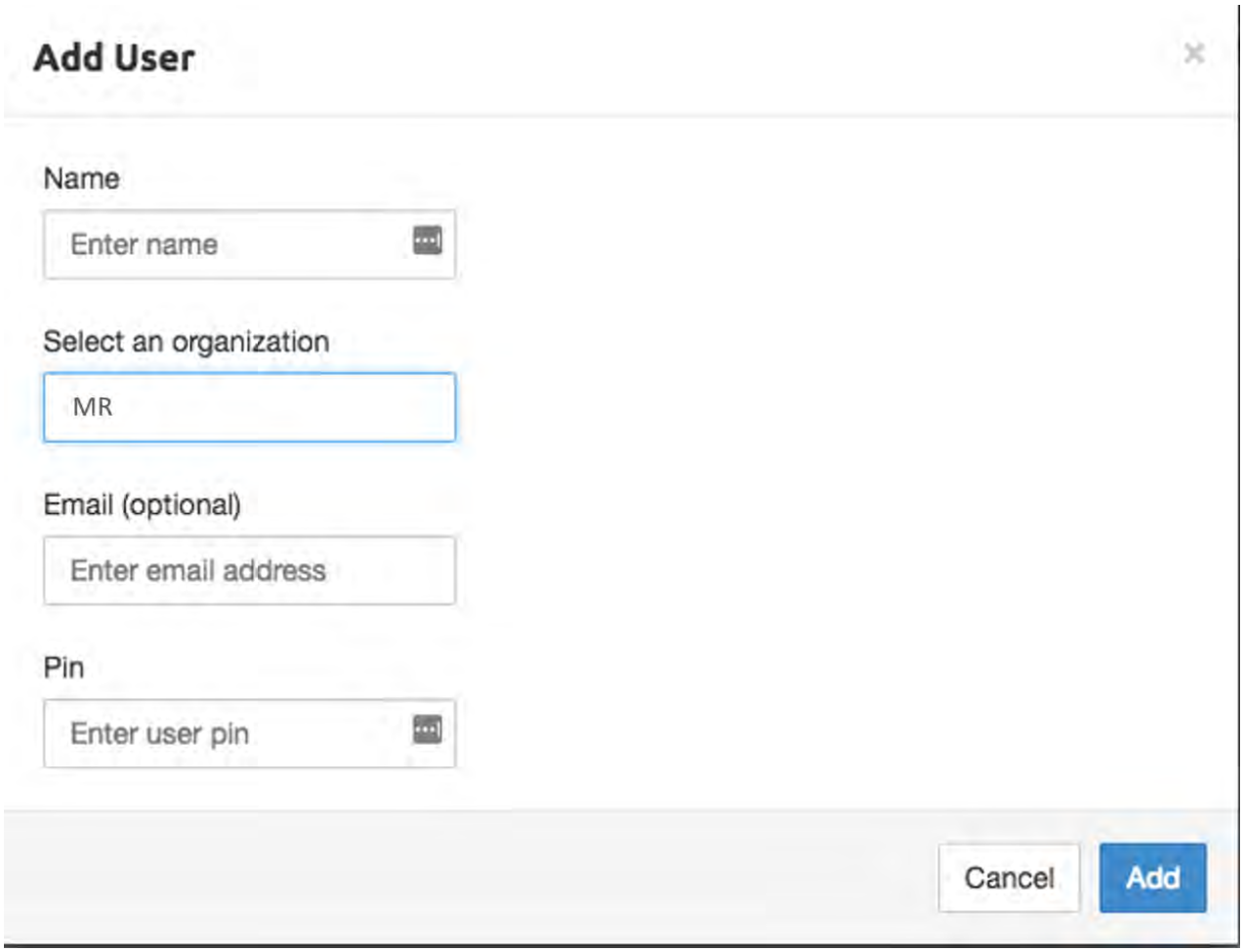


(In this document, we use the MR to be the organization example.)

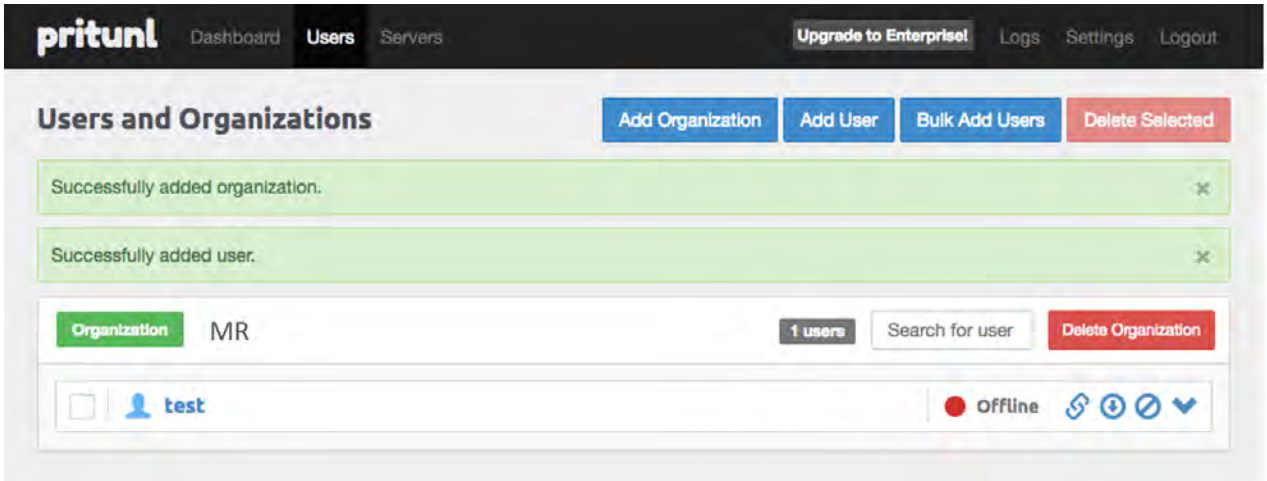
When the organization be created, the Users page should be like the following figure.



Then add the OpenVPN user by click the Add User button.

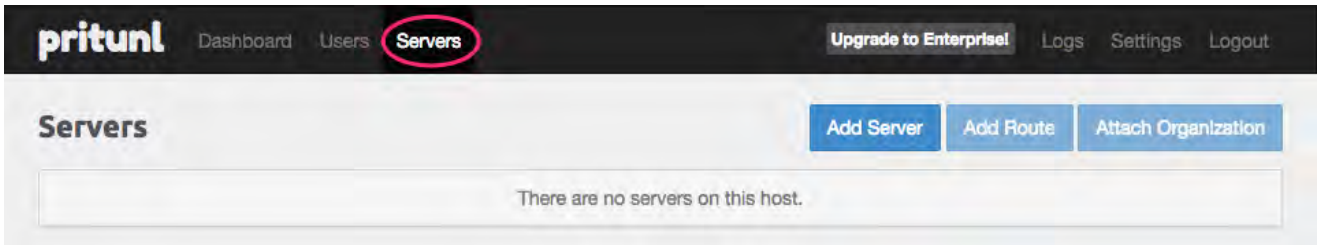


Note: In this OpenVPN server, the PIN must contain only digits.
Note: In this document, we use the test/123456 OpenVPN user to be the example.

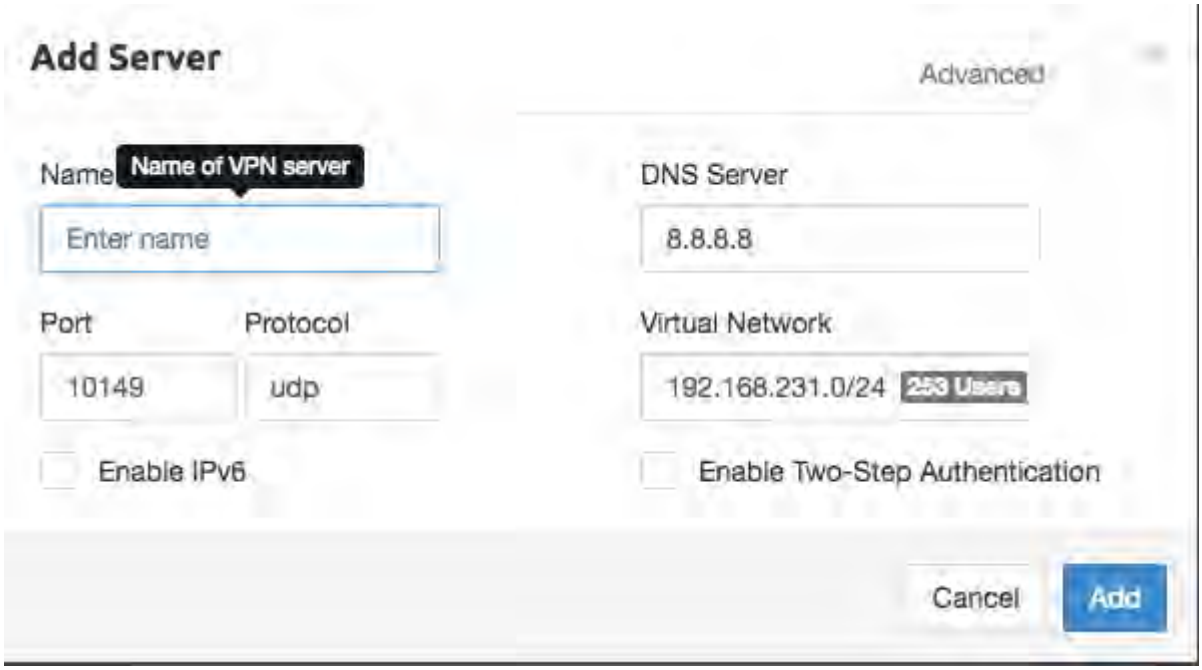


OpenVPN server setup

Please navigate to the Server page to setup the OpenVPN server.

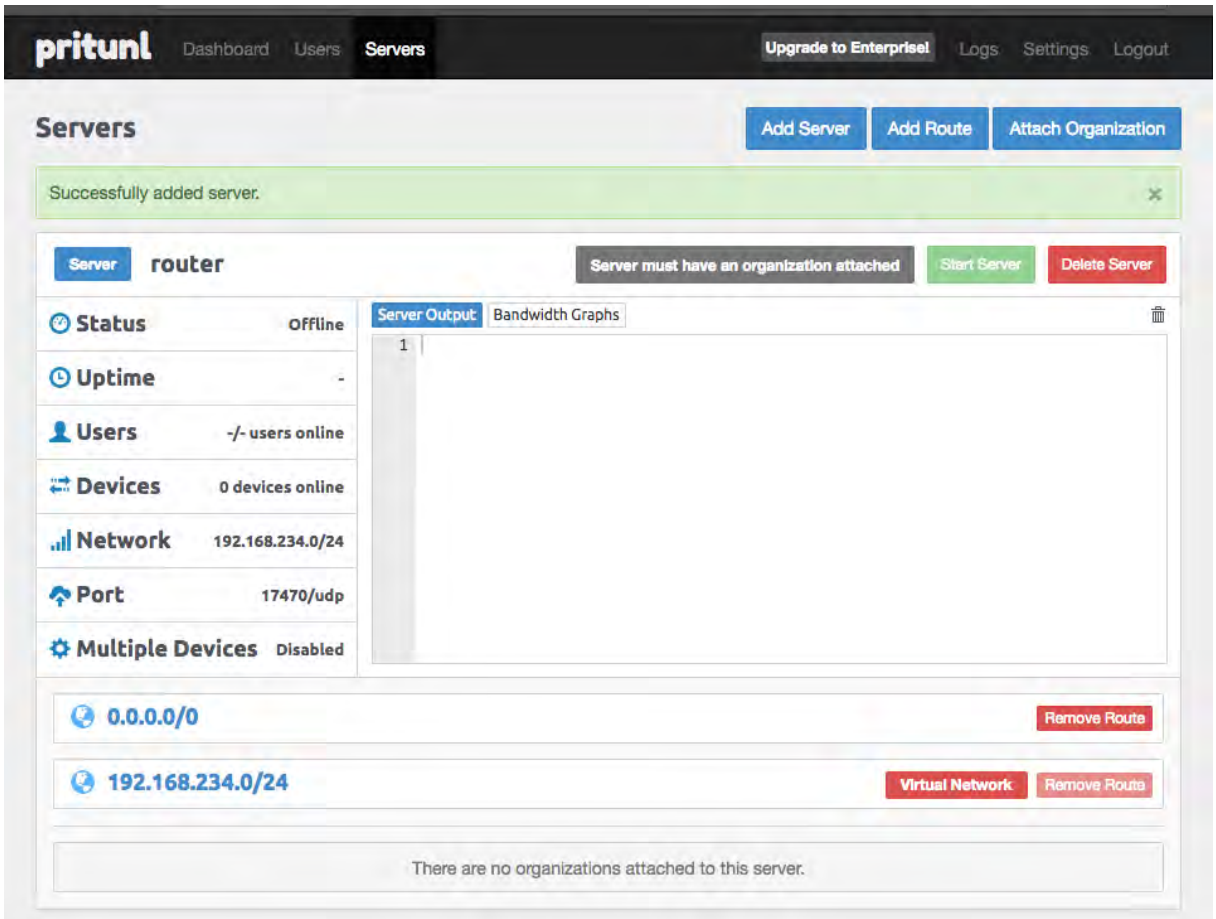


And click the Add Server button to create the OpenVPN server.

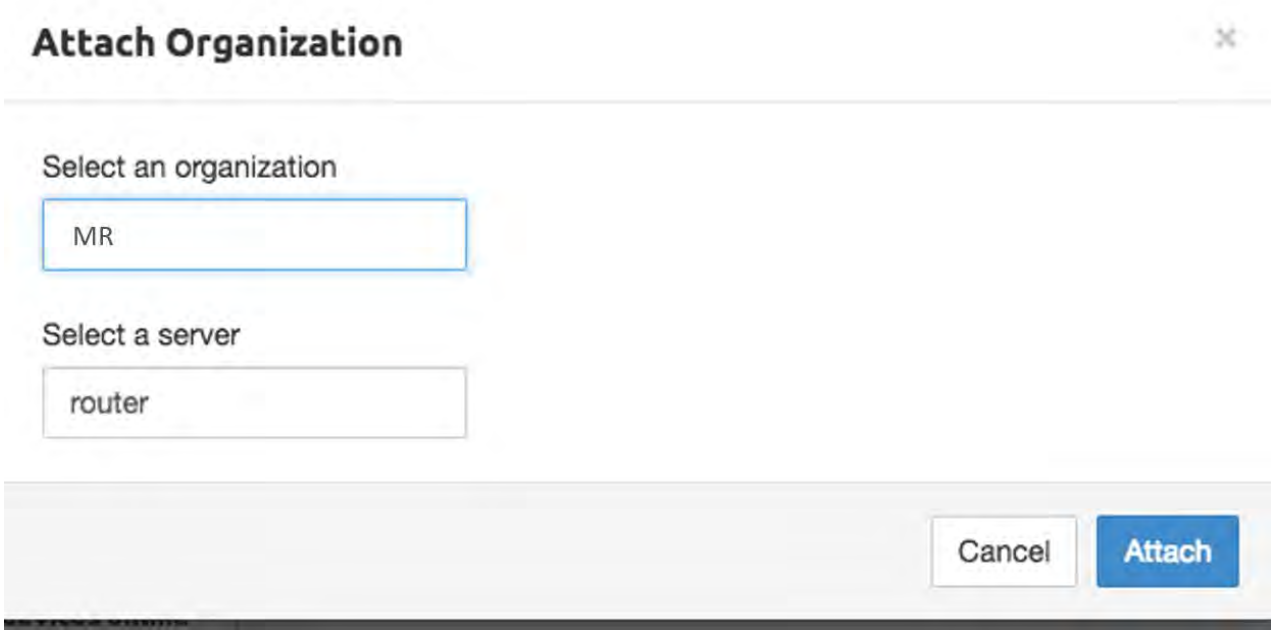


Note: Please click the Advanced tab and make sure the Inter-Client Communication be checked

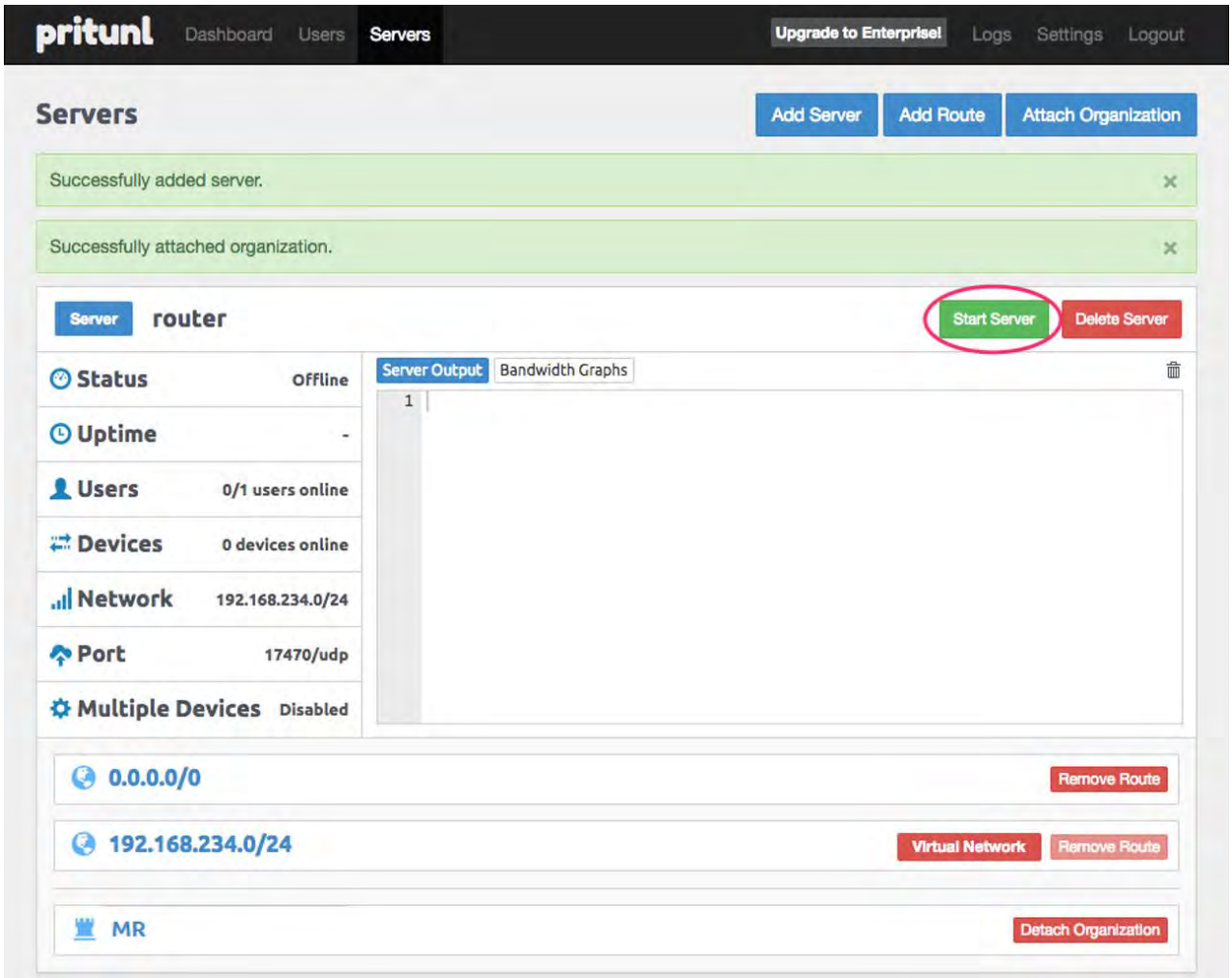
When the OpenVPN server created, the Servers page should like the following figure.



And click Attach Organization button to setup the OpenVPN server.

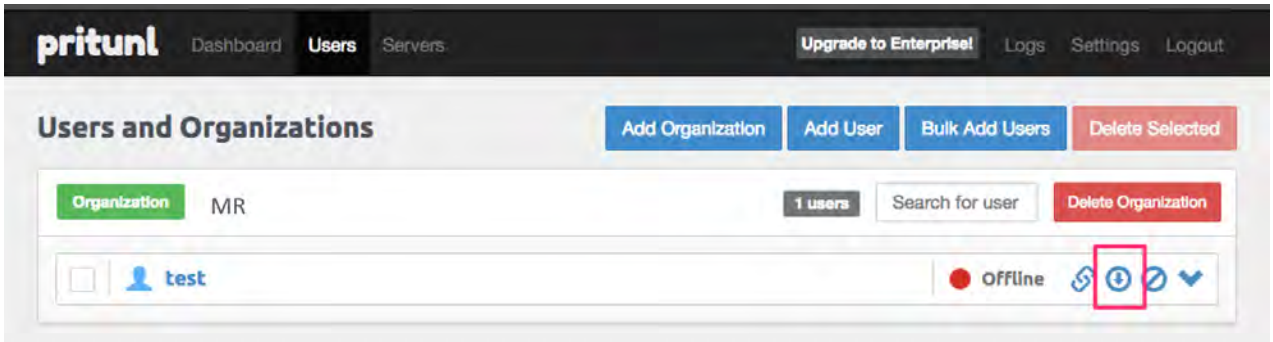


Start the OpenVPN server by click Start Server button.



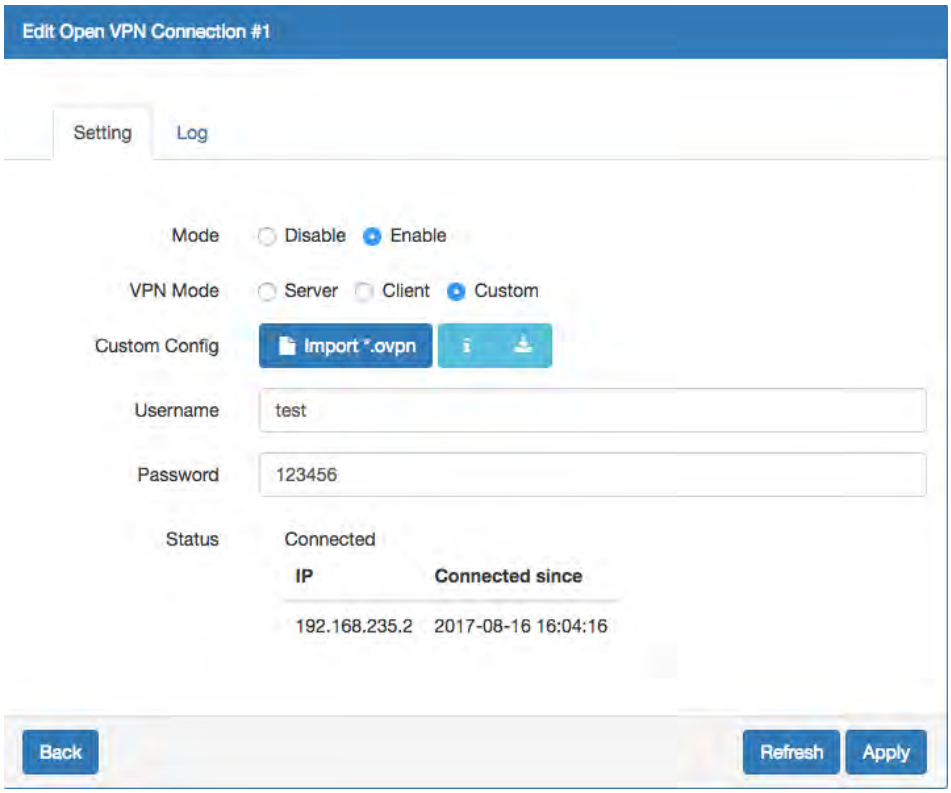
Cellular Router setup

First, please navigate to the Users page and download the user configuration file and extract it.

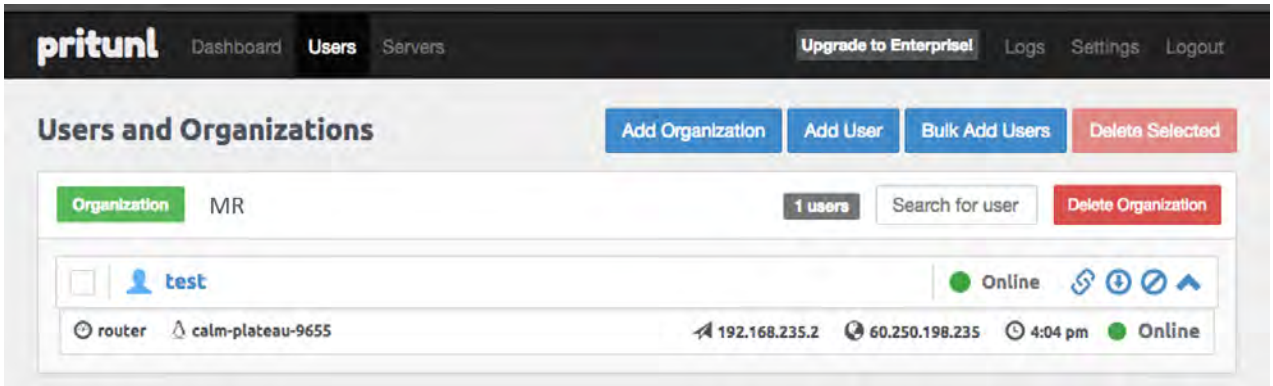


Note: In this document, you should get the MR_test_router.ovpn file.

And visit the Cellular Router OpenVPN custom page then import the .ovpn file.
Fill up the username/password which be setup in OpenVPN user setup part.

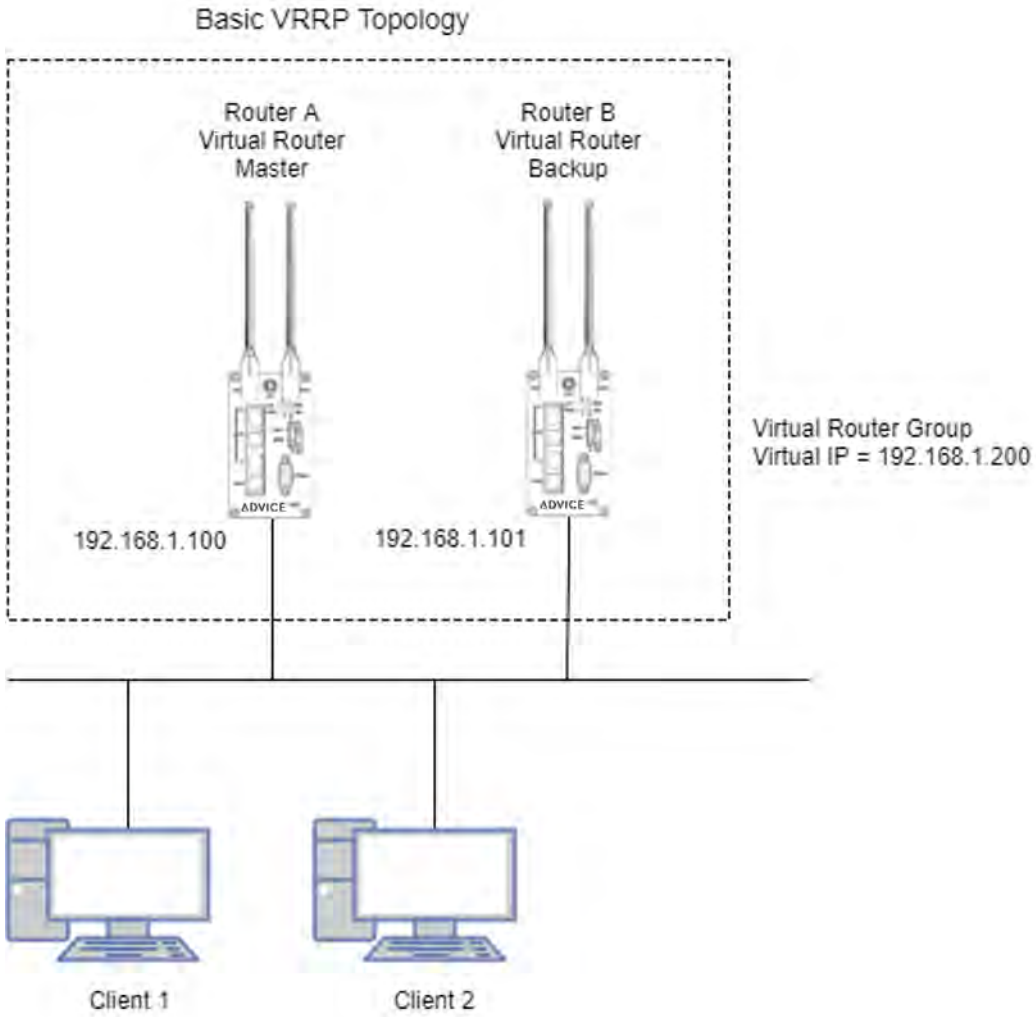


When the Cellular Router OpenVPN connected, the Pritunl OpenVPN server also update the user status.



12.10 VRRP Topology

Basic VRRP Topology



Base on this topology and VRRP Parameter settings, Router A and Router B will offer a virtual router service with virtual IP = 192.168.1.200 for the client.

12.11 TR069 Server (GenieACS Installation)

Server OS: Ubuntu 14.04 on Virtualbox

Installation:

1) Login ubuntu
2) Change to root by 'su -' and enter your root password.
3) Install required package as below command:
   >apt install gcc openssl-devel zlib-devel readline-devel sqlite-devel
4) Make a directory for application installation
   >mkdir /opt
5) Install yaml

cd /opt

```
wget http://pyyaml.org/download/libyaml/yaml-0.1.7.tar.gz
tar xvzf yaml-0.1.7.tar.gz
cd yaml-0.1.7
./configure
make && make install
```

6) Install ruby

```
cd /opt
wget http://cache.ruby-lang.org/pub/ruby/2.4/ruby-2.4.1.tar.gz
tar xvzf uby-2.4.1.tar.gz
cd ruby-2.4.1
./configure
make && make install
ruby   -v
ruby 2.4.1p111 (2017-03-22 revision 58053) [i686-linux]

cd /opt
gem install rails --no-ri --no-rdoc
gem install bundle --no-ri --no-rdoc
```

7) Install node.js

```
cd /opt
wget http://nodejs.org/dist/v8.2.1/node-v8.2.1.tar.gz
tar zxvf node-v8.2.1.tar.gz
cd node-v8.2.1
./configure
make && make install
node -v
v8.2.1
```

8) Install redis

```
cd /opt
wget http://download.redis.io/releases/redis-4.0.1.tar.gz
tar zxvf redis-4.0.1.tar.gz
cd redis-4.0.1
make
make test
All tests passed without errors!
make install
#Start redis server
redis-server
```

9) Install mongodb

```
cd /opt
wget https://fastdl.mongodb.org/linux/mongodb-linux-i686-3.3.3.tgz
tar zxvf mongodb-linux-i686-3.3.3.tgz
```

```
cd mongodb-linux-i686-3.3.3
mkdir -p /data/db
```

10) Install genieACS

```
cd /opt
git clone https://github.com/zaidka/genieacs.git
cd genieacs
npm install
npm run configure
npm run compile
```

Modify FS_HOSTNAME field in genieacs/config/config.json for device retrieve firmware file

Original configuration:

"FS_HOSTNAME" : "acs.example.com"

New configuration example.:

"FS_HOSTNAME" : "192.168.0.199"

Note: It is the place where the device firmware file stored. Generally, it is the IP address on where your GenieACS server installed.

Modify connect request username/password in genieacs/config/auth.js to stimulate connection

Original configuration:

```
function connectionRequest(deviceId, url, username, password, callback) {
    return callback(username || deviceId, password || "");
}
```

New configuration example:

```
function connectionRequest(deviceId, url, username, password, callback) {
    return callback('tr069','tr069');
}
```

Note: The hard code username/password MUST same with device's connection request username/password, otherwise the ACS stimulate connection will fail.

11) Install genieACS-Gui

```
git clone https://github.com/zaidka/genieacs-gui
cd genieacs-gui
bundle

gem install json
bundle update

rm -f db/*.sqlite3
rake db:create
RAILS_ENV=development rake db:migrate
```

```
cd /opt
cd genieacs-gui/config
cp index_parameters-sample.yml index_parameters.yml
cp parameter_renderers-sample.yml parameter_renderers.yml
cp parameters_edit-sample.yml parameters_edit.yml
cp roles-sample.yml roles.yml
cp summary_parameters-sample.yml summary_parameters.yml
cp users-sample.yml users.yml
cp graphs-sample.json.erb graphs.json.erb
```

GenieACS startup script:

```
#!/bin/sh

GENIE_PATH=/opt/genieacs/bin
GENIE_GUI_PATH=/opt/genieacs-gui

echo "start mongod."
pidof mongod
if [ $? != 0 ]; then
/opt/mongodb-linux-i686-3.3.3/bin/mongod  --dbpath  /data/db  --journal  --storageEngine=mmapv1
--fork --syslog
fi

echo "start North Bound/RESTful Interface service."
$GENIE_PATH/genieacs-nbi &

echo "start ACS/CWMP service."
$GENIE_PATH/genieacs-cwmp &

echo "start HTTP/File streaming service."
$GENIE_PATH/genieacs-fs &

echo "start GenieACS/WebUI."
cd $GENIE_GUI_PATH
rails server -b 0.0.0.0
```

GenieACS stop:

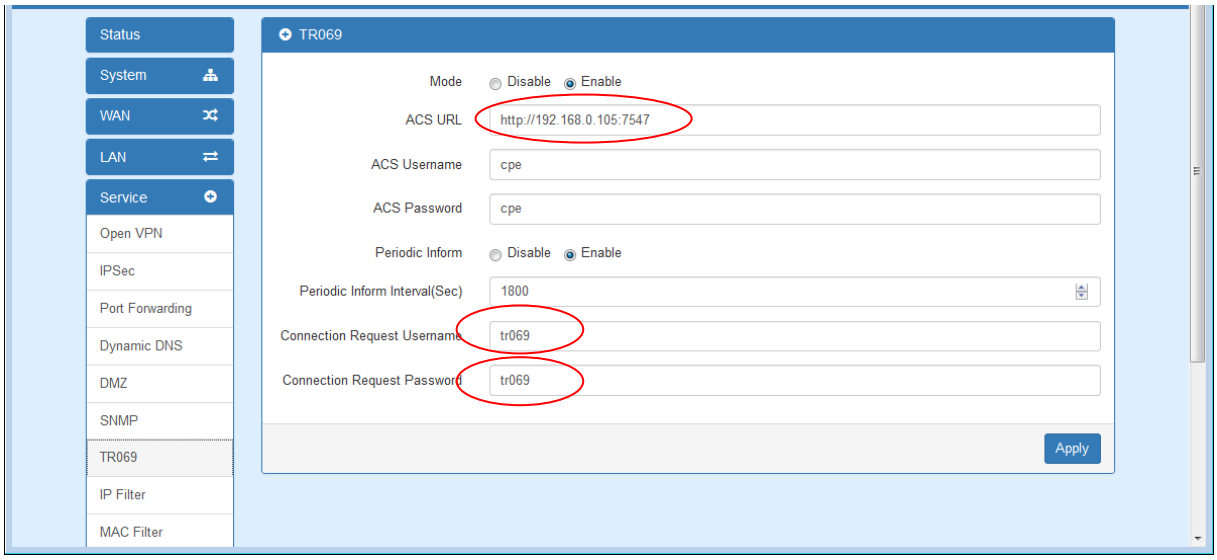
Ctrl-C

Usage:

1) Device Configuration

Fill in the ACS URL field as http://GenieACS server IP:7547

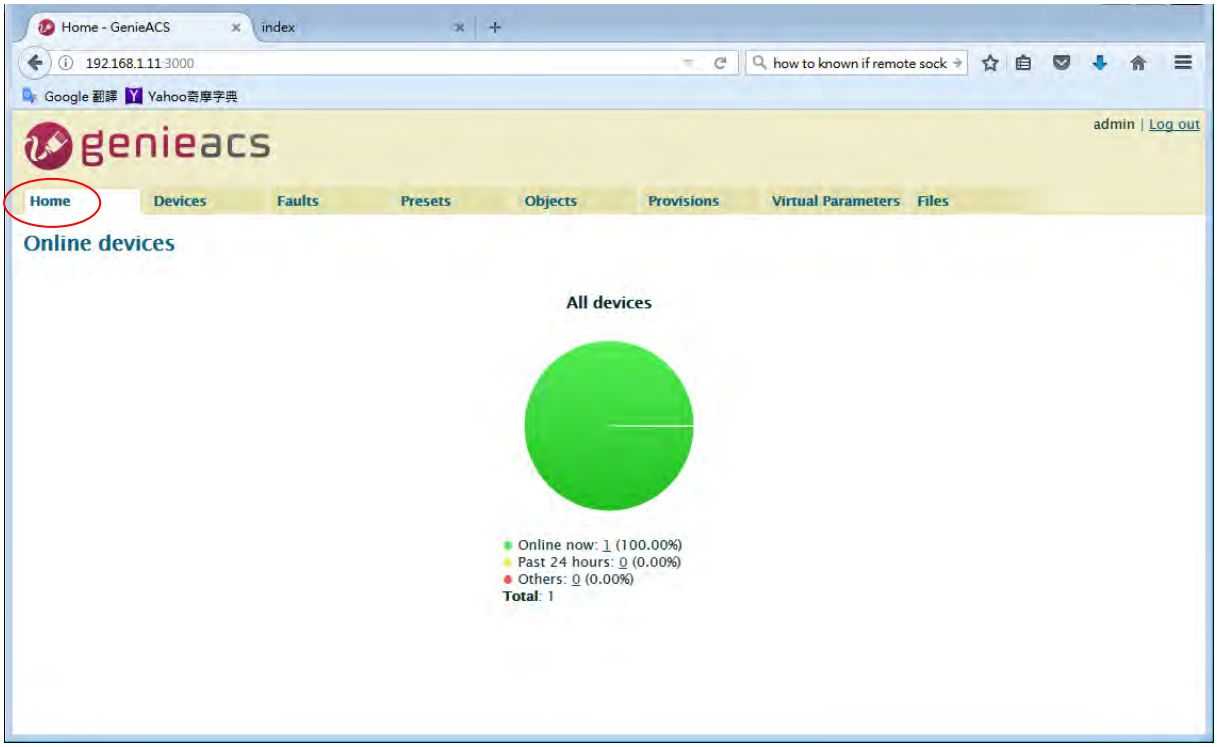
Fill in the Connection Request Username and Connection Request Password fields to same with the configuration in genieacs/config/auth.js.



2) GenieACS Operation

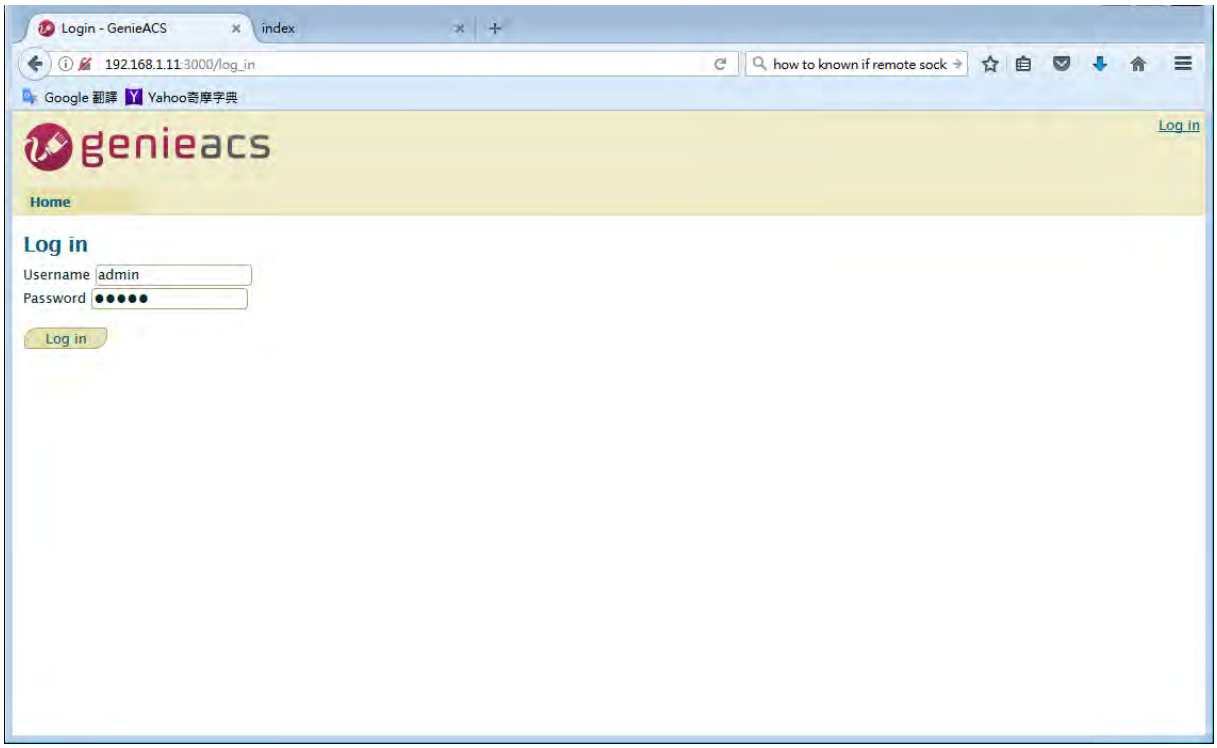
Input http://GenieACS server IP:3000 on browser url bar and Enter.

Press Home tab to refresh Online devices status.



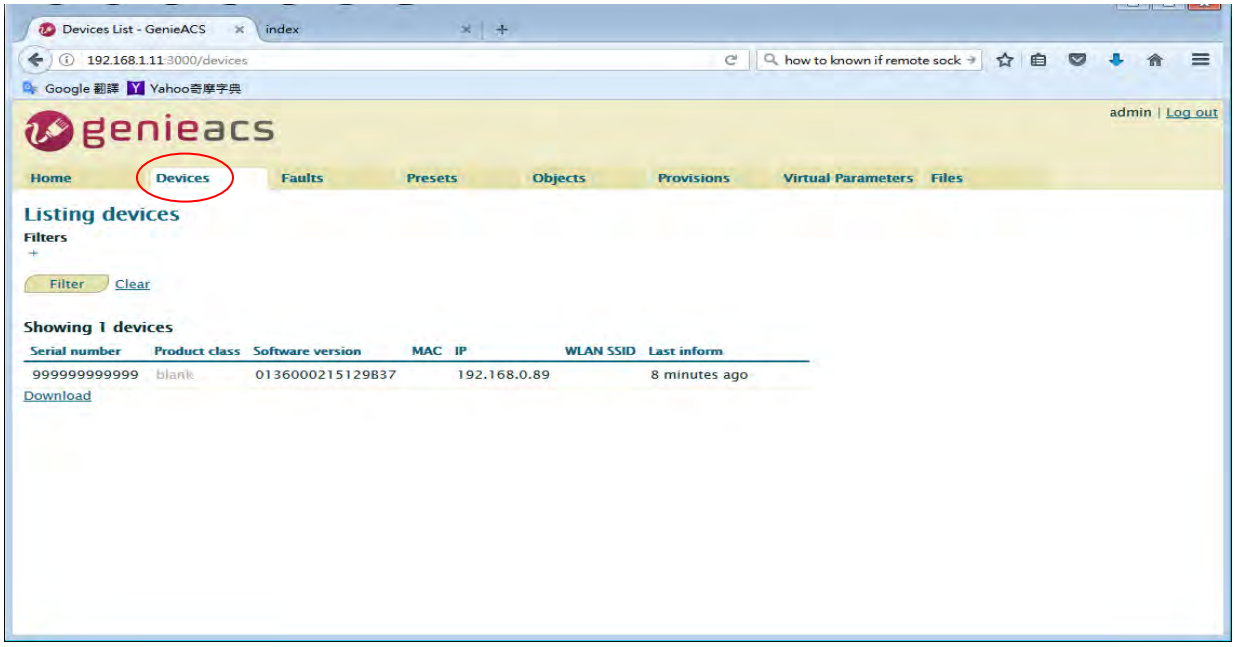
2.1) Login

Username and Password are admin/admin.

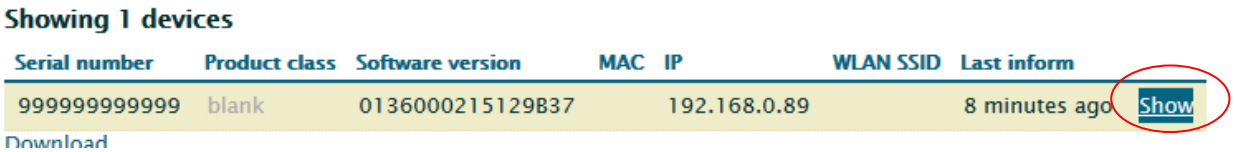


3) Device information

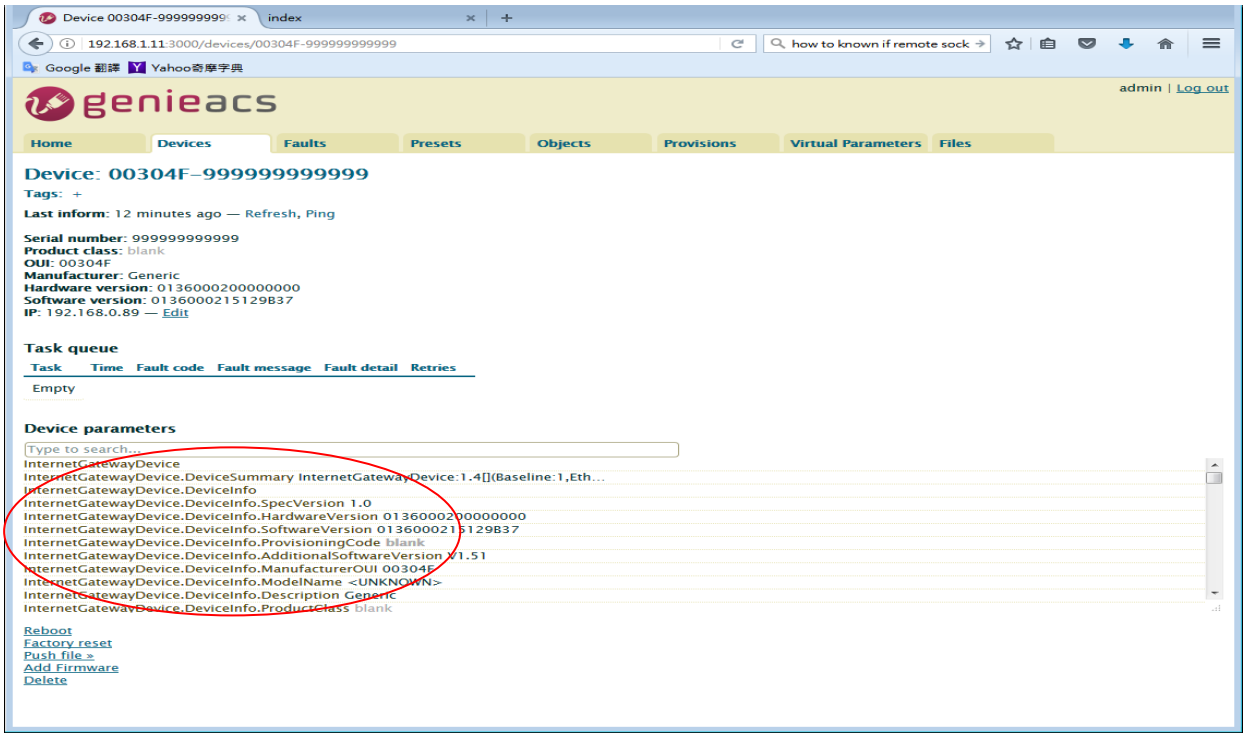
Press Devices tab



Move mouse to line end of your device, the Show link show up.



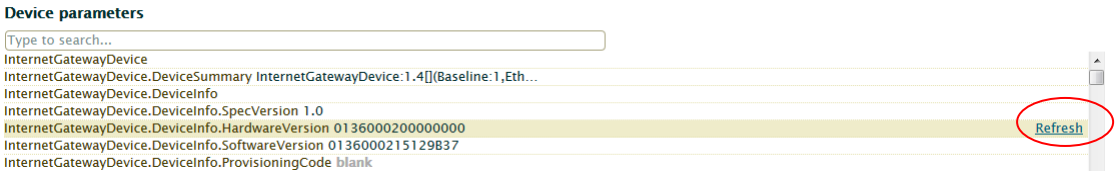
Press Show link, the device information show up.



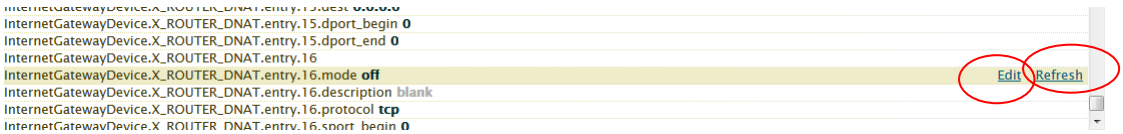
4) Access parameters

Scroll up/down on Device parameters list, the Refresh and Edit link show up at line end of parameter.

For Readable parameter

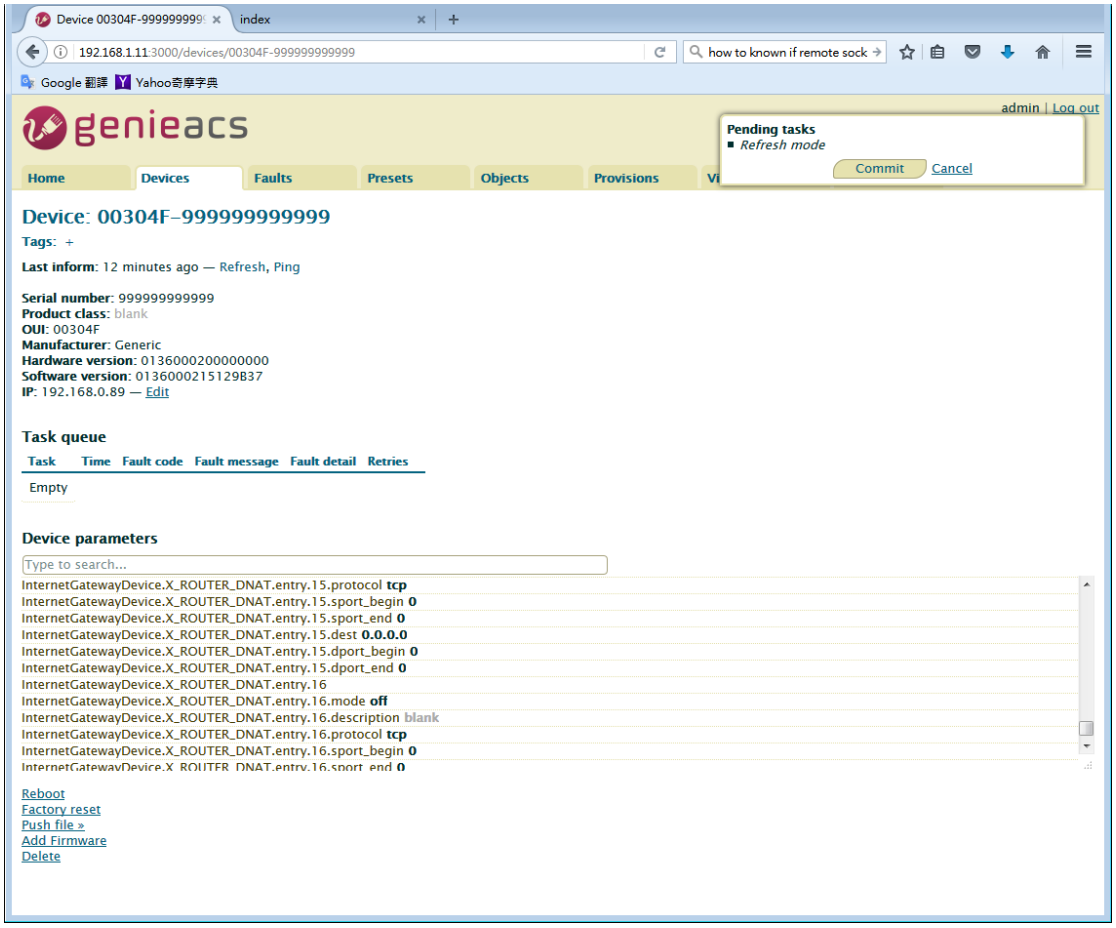


For Readable and Writable parameter



4.1) Get parameter value

Press on the Refresh link,the Pending tasks window will popup on right top to ask you to allow or Cancel this action.



Press Commit to get this parameter value.

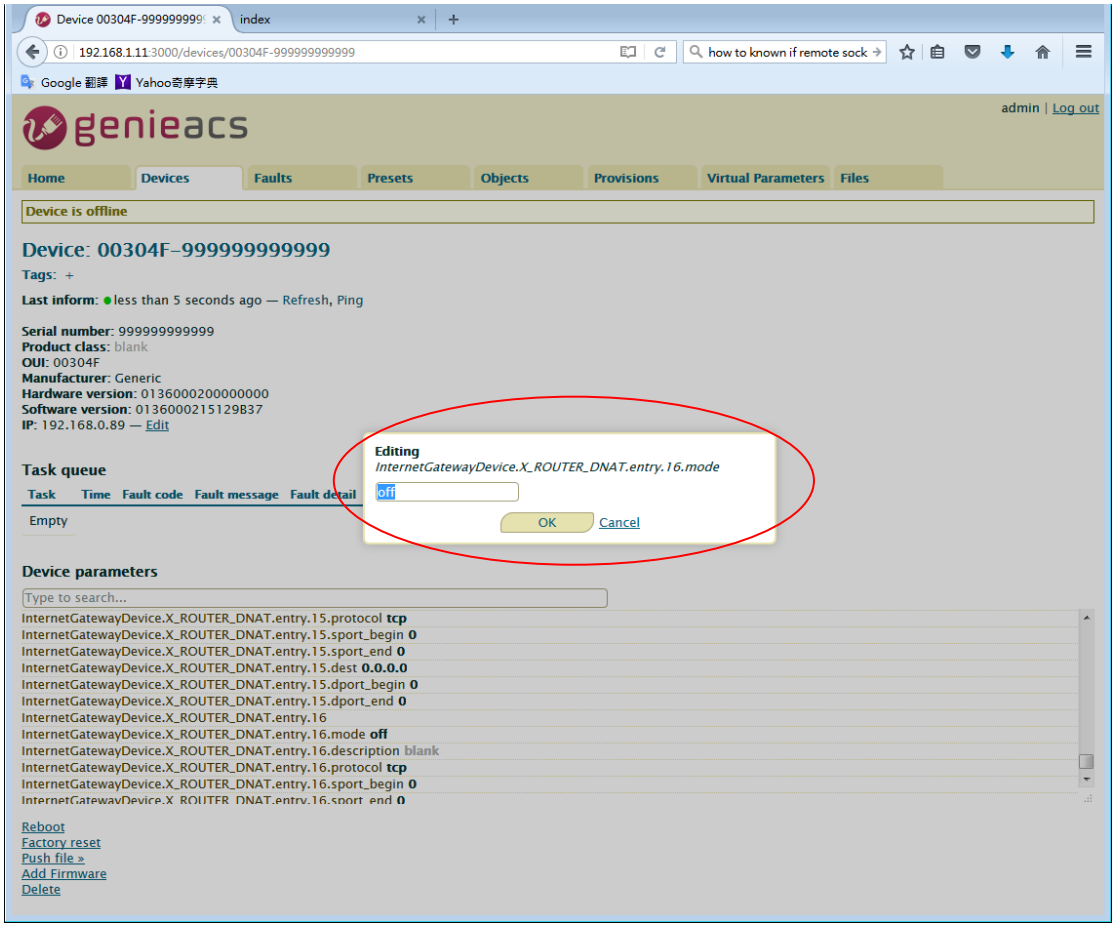
Note: *If the GenieACS can reach the device, the parameter value will be updated immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.*

Note: To update the whole tree, refresh the root parameter (InternetGatewayDevice.).

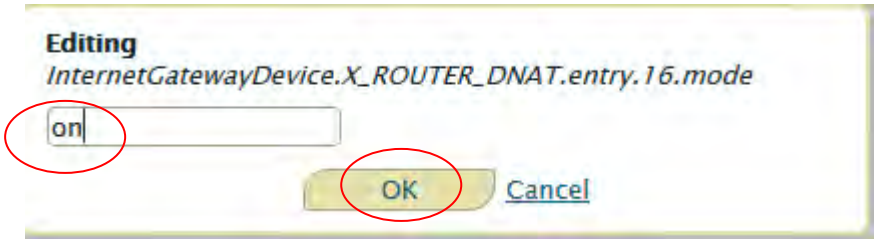
Note: To update partial tree, refresh the parent node of the partial tree.

4.2) Set parameter value

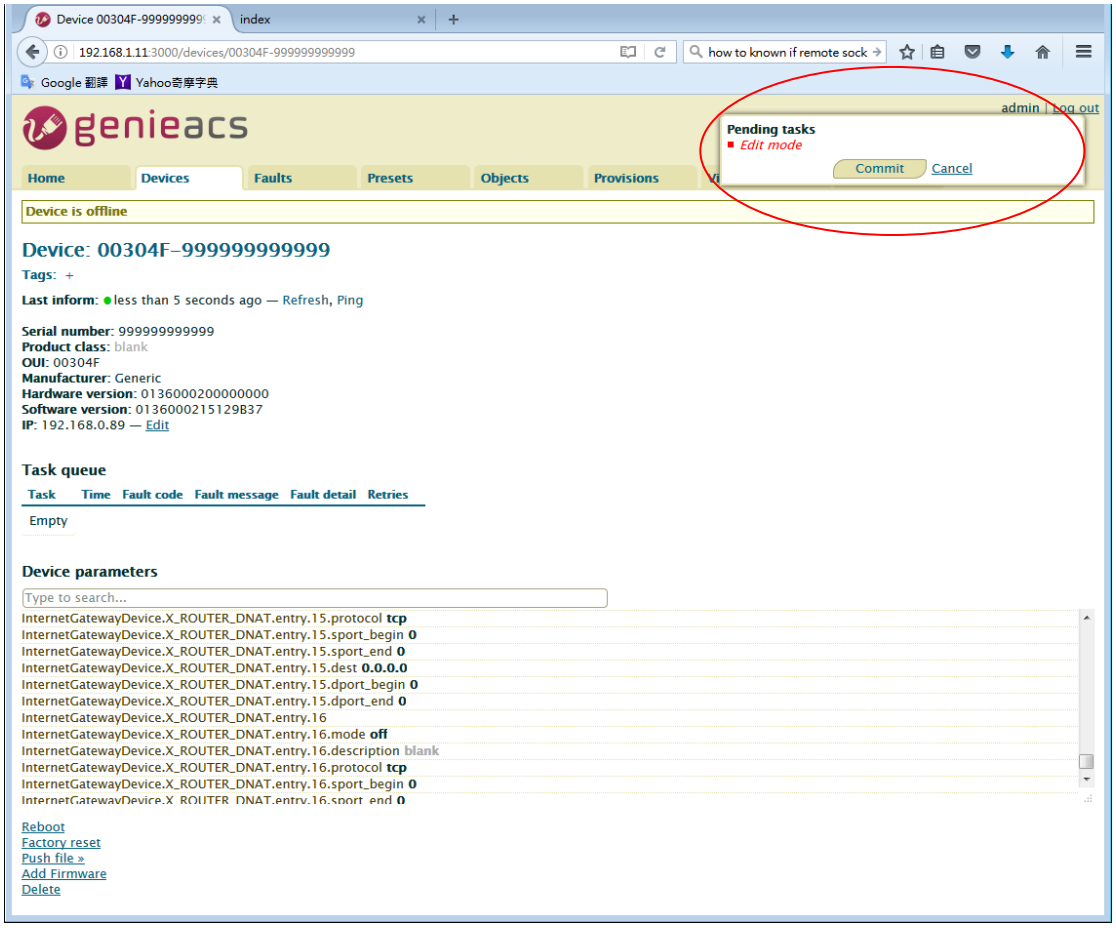
Press on the Edit link, Editing window will pop up to ask you to change the value of this parameter.



Input new value and press OK.



The Pending tasks window will pop up to ask you to allow or Cancel this action.

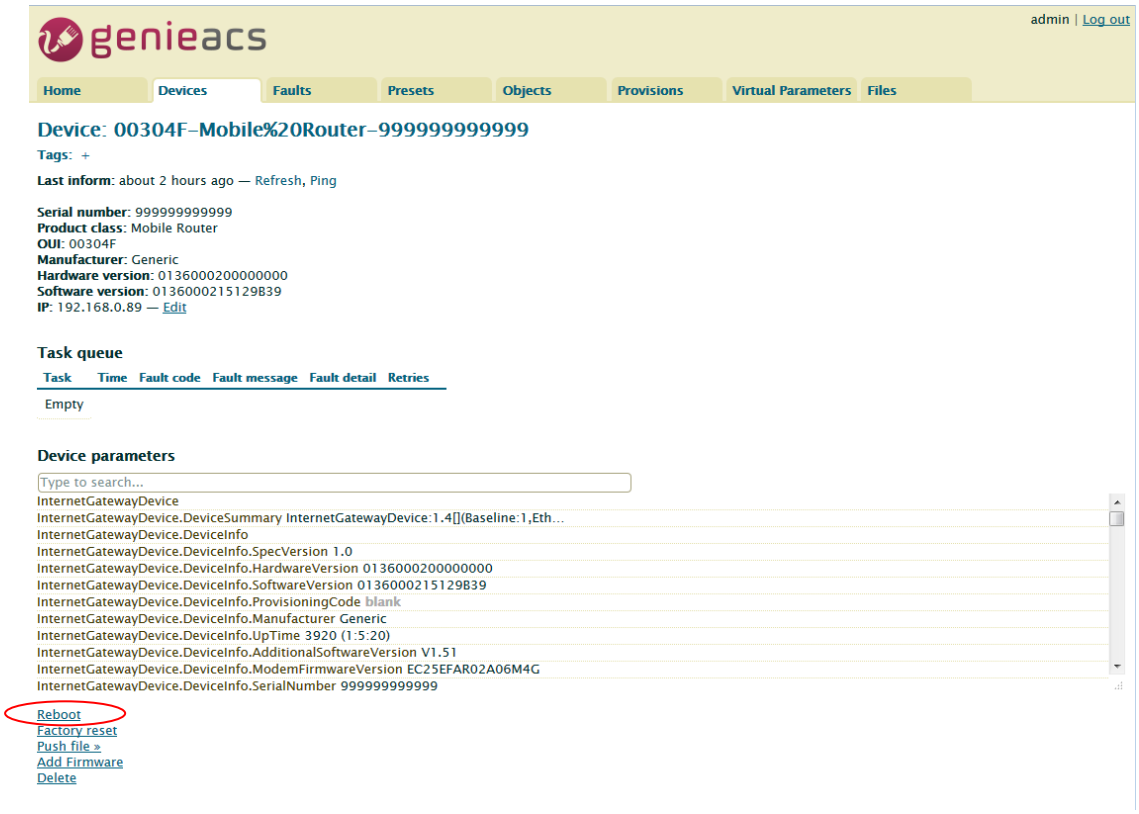


Press Commit to set this parameter value.

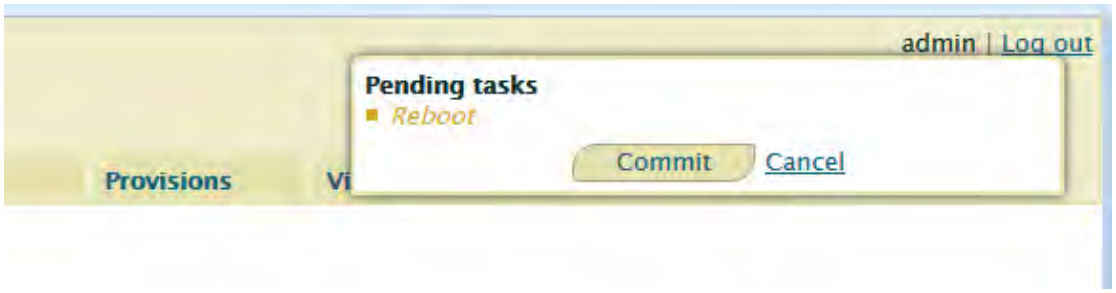
Note: *If the GenieACS can reach the device, the parameter value will be set immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.*

5) Reboot device

Press on Reboot link.



The Pending tasks window will popup to ask you to allow or Cancel this action.



Press Commit to reboot device.

Note: *If the GenieACS can reach the device, the device will reboot immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.*

6) Reset to default

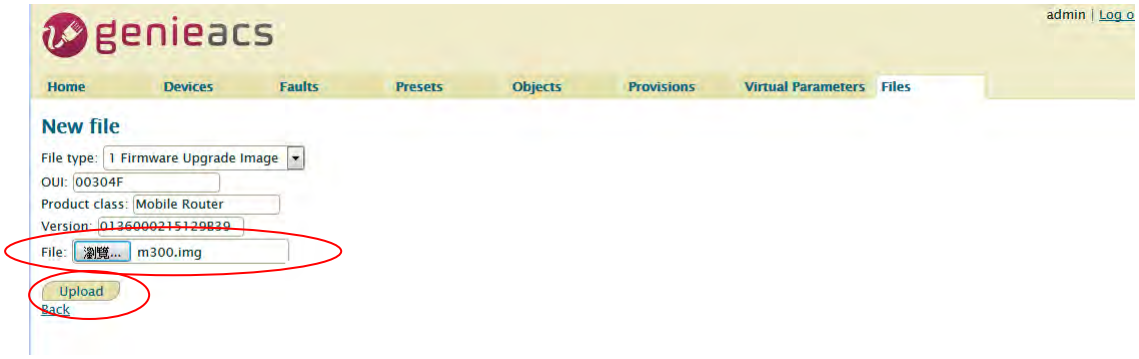
Similar to Reboot device except pressing on Factory reset link.

7) Firmware Upgrade

7.1) Upload Firmware

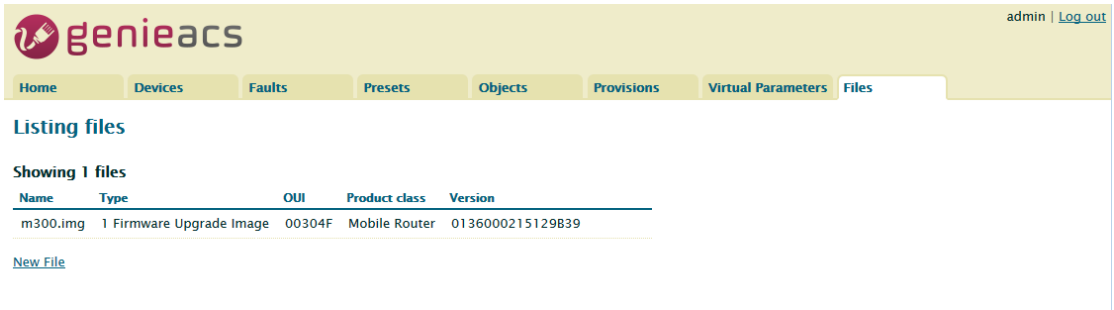
Press Add Firmware link

The link will redirect to Files tab



Press File: browse button, select the firmware, and then press Upload button.

The firmware will be added to Listing files as below.



7.2) Upgrade

Move mouse to the Push file>> link, the upgrade firmware name will pop up as below picture.

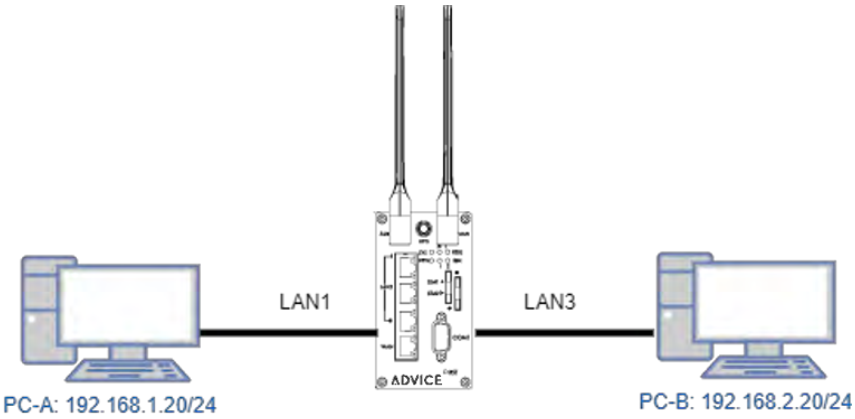
Move mouse to the upgrade firmware name and press it. The Pending tasks window will pop up to ask you to allow or Cancel this action.

Press Commit, then firmware upgrade started.

Note: *If the GenieACS can reach the device, the firmware upgrade will be started immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.*

13 Test Case Example

13.1 VLAN Topology



This VLAN Topology for **3-port LANs** shows different PCs how to configure VLAN settings with different LAN ports and has two results for this configuration.

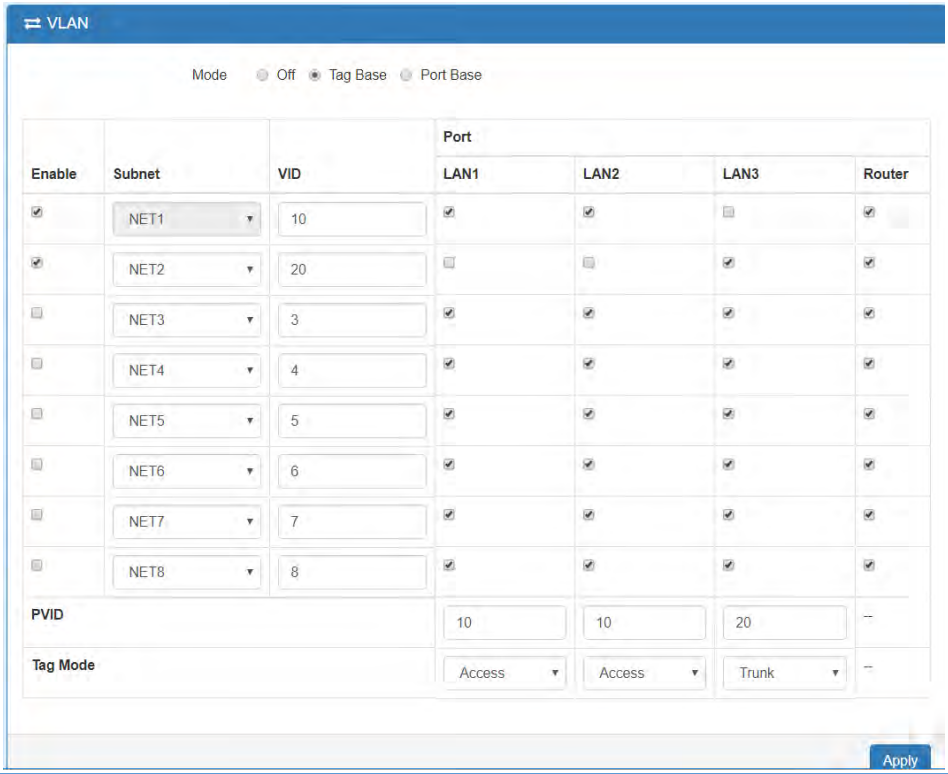
(1) PC-A sends ICMP packet to PC-B IP (192.168.2.20) and captures traffic on PC-B. Thus, PC-B will receive Tag20 traffic.

(2) PC-B sends ICMP packet to PC-A IP (192.168.1.20) and captures traffic on PC-A. Thus, PC-A will receive untag traffic.

Note:

- PC-A and PC-B are on Ubuntu OS.
- PC-A and PC-B should install vlan on Ubuntu.
- PC-A and PC-B should command this order “sudo apt-get install vlan”.

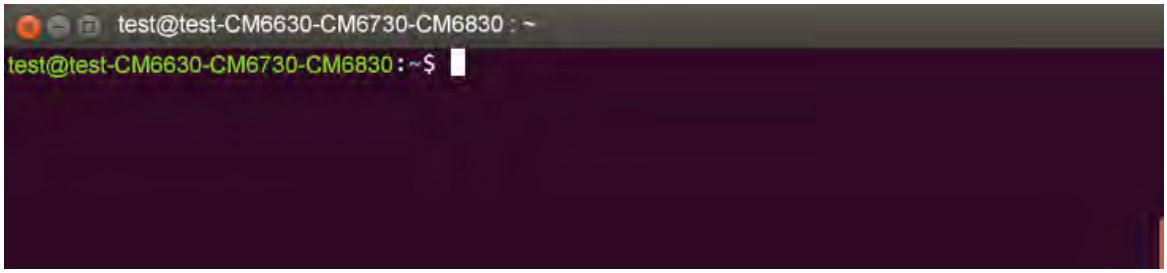
The following interface shows VLAN settings for the cellular router.



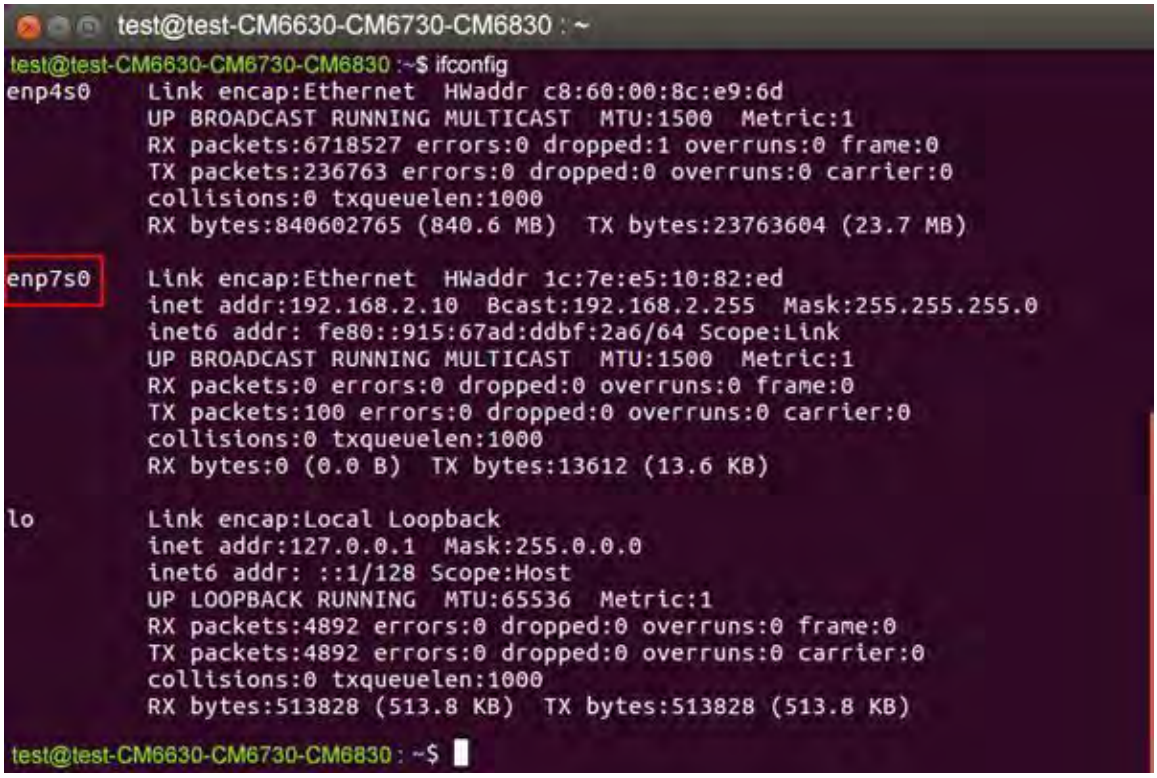
Note:

- Different PCs have different interface of network cards, like PC-A network card is eth1.10 for example 1 and PC-B network card is eth1.20 for example 2.
- How to find out the terminal and the interface of network cards based on different PCs.
  - From the following picture, you can click *the finding your computer icon* and input the terminal letters. Then, the interface will show *the terminal icon* and click to open it.

  - Next, it shows the information when you click *the terminal icon*.



  - From the following picture, it shows the interface of network card, enp7s0.



There are two examples to explain how configure VLAN settings.

Example 1: PC-A pings PC-B (Access to Trunk)

For PC-A, add default gateway and LAN's MAC to ARP.

- Load VLAN and create VLAN interface, command as below:
  - sudo modprobe 8021q
  - sudo vconfig rem eth1.20
  - sudo vconfig add eth1.10
- Configure VLAN interface as below:
  - sudo ifconfig eth1.10 192.168.1.20 netmask 255.255.255.0 up
  - sudo ifconfig eth1 0.0.0.0
- sudo route add default gw 192.168.1.1 eth1.10
- sudo arp -s 192.168.1.1 LAN's MAC
- eth1 is network interface on PC-A

Therefore, PC-B will receive Tag20 traffic when PC-A sends ICMP packet to PC-B IP (192.168.2.20) and captures traffic on PC-B.

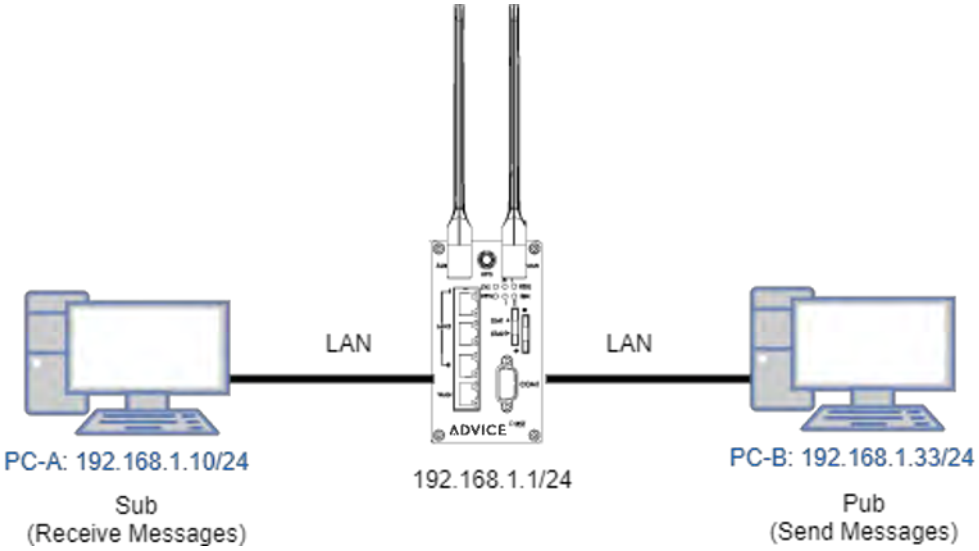
Example 2: PC-A ping PC-B (Trunk to Access)

For PC-B, add default gateway and LAN's MAC to ARP

- Load VLAN and create VLAN interface, command as below:
  - sudo modprobe 8021q
  - sudo vconfig rem eth1.10
  - sudo vconfig add eth1.20
- Configure VLAN interface as below:
  - sudo ifconfig eth1.20 192.168.2.20 netmask 255.255.255.0 up
  - sudo ifconfig eth1 0.0.0.0
- sudo route add default gw 192.168.2.1 eth1.20
- sudo arp -s 192.168.2.1 LAN's MAC
- eth1 is network interface on PC-B

Therefore, PC-A will receive untag traffic when PC-B sends ICMP packet to PC-A IP (192.168.1.20) and captures traffic on PC-A.

13.2 MQTT Topology



This MQTT Topology shows the cellular router to connect PC-A and PC-B's LANs and have two results are as below.

Expect Result:

(1) PC-A sends message to PC-B and PC-B should not receive any message.

(2) PC-B sends message to PC-A and PC-A should receive message.

Note: PC-A and PC-B should install MQTT Client software.

There is a process to explain the steps and result.

- Step1: Install mosquitto-clients on ubuntu or windows.

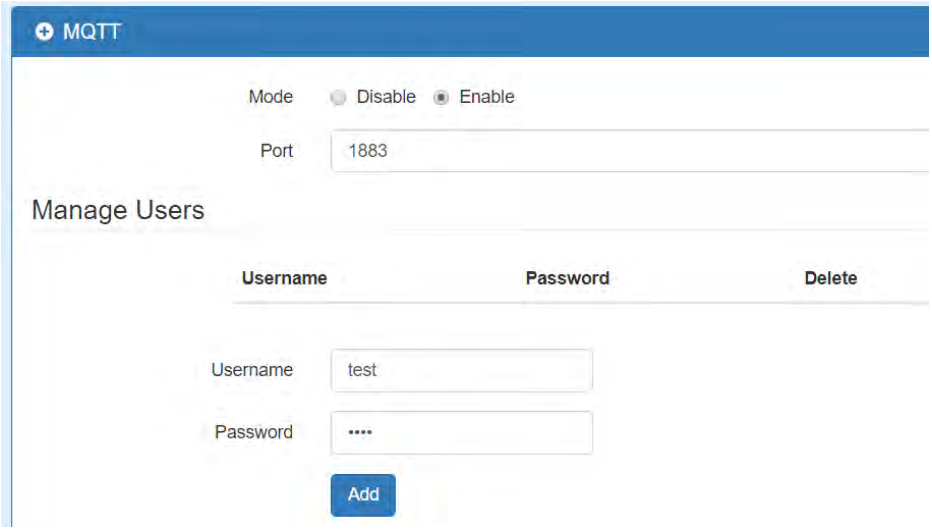
If your OS system is Ubuntu, you should install as below steps:

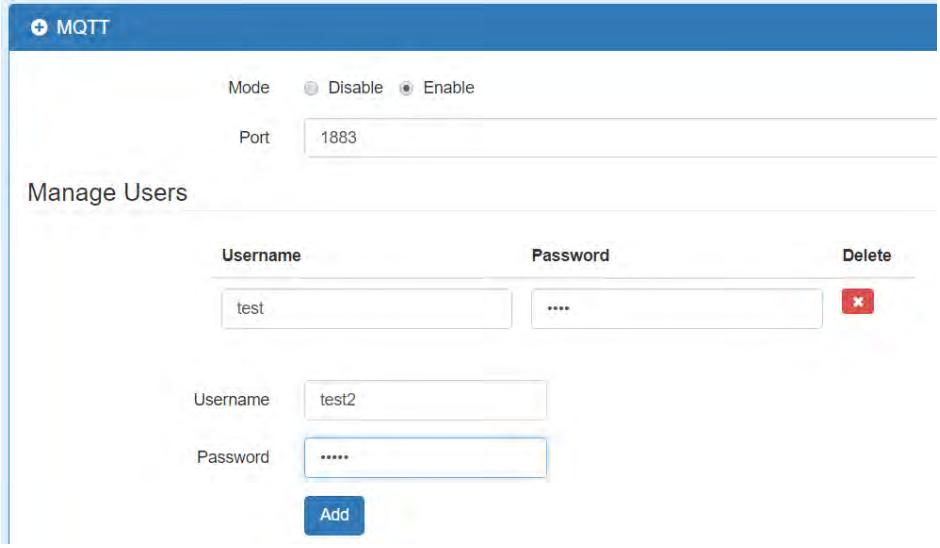
```
test@test: ~
test@test:~$ sudo apt-get install mosquitto-clients
sudo: unable to resolve host test
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  geoip-database-extra javascript-common libjs-openlayers libnghttp2-14
  libnl-route-3-200 libqgsttools-p1 libqt5multimedia5-plugins
  libqt5multimediawidgets5 libsmi2ldbl libssh-gcrypt-4 libwireshark-data
  libwiretap6 libwscodecs1 libwsutil7 linux-headers-4.10.0-28
  linux-headers-4.10.0-28-generic linux-headers-4.10.0-42
  linux-headers-4.10.0-42-generic linux-headers-4.13.0-26
  linux-headers-4.13.0-26-generic linux-image-4.10.0-28-generic
  linux-image-4.10.0-42-generic linux-image-4.13.0-26-generic
  linux-image-extra-4.10.0-28-generic linux-image-extra-4.10.0-42-generic
  linux-image-extra-4.13.0-26-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libc-ares2 libmosquitto1
The following NEW packages will be installed:
  libc-ares2 libmosquitto1 mosquitto-clients
0 upgraded, 3 newly installed, 0 to remove and 119 not upgraded.
Need to get 65.3 kB/96.4 kB of archives.
After this operation, 330 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

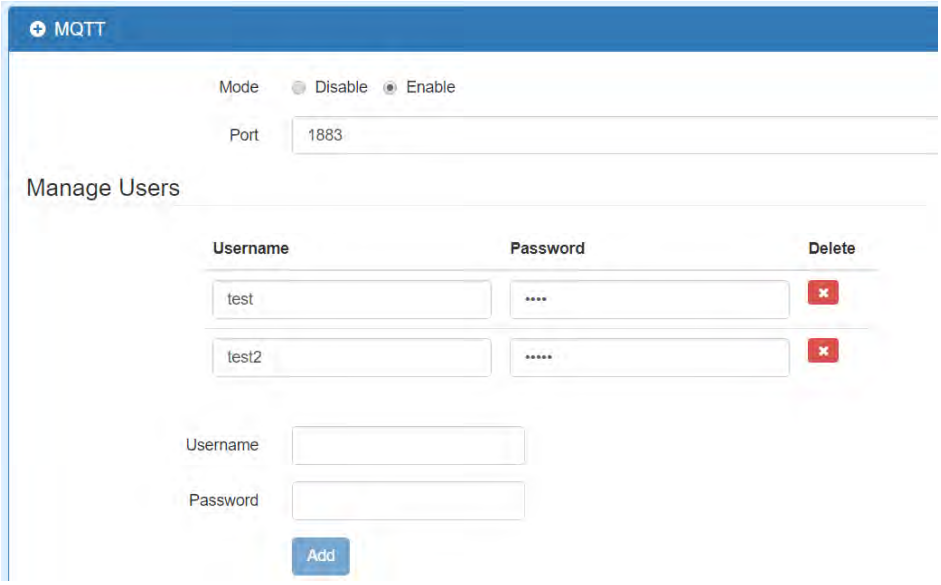
```
test@test: ~
After this operation, 330 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://tw.archive.ubuntu.com/ubuntu xenial-updates/main amd64 libc-ares2 amd
64 1.10.0-3ubuntu0.2 [34.1 kB]
Get:2 http://tw.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 libmosquit
to1 amd64 1.4.8-1ubuntu0.16.04.2 [31.3 kB]
Fetched 65.3 kB in 0s (201 kB/s)
Selecting previously unselected package libc-ares2:amd64.
(Reading database ... 319360 files and directories currently installed.)
Preparing to unpack .../libc-ares2_1.10.0-3ubuntu0.2_amd64.deb ...
Unpacking libc-ares2:amd64 (1.10.0-3ubuntu0.2) ...
Selecting previously unselected package libmosquitto1:amd64.
Preparing to unpack .../libmosquitto1_1.4.8-1ubuntu0.16.04.2_amd64.deb ...
Unpacking libmosquitto1:amd64 (1.4.8-1ubuntu0.16.04.2) ...
Selecting previously unselected package mosquitto-clients.
Preparing to unpack .../mosquitto-clients_1.4.8-1ubuntu0.16.04.2_amd64.deb ...
Unpacking mosquitto-clients (1.4.8-1ubuntu0.16.04.2) ...
Processing triggers for libc-bin (2.23-0ubuntu10) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up libc-ares2:amd64 (1.10.0-3ubuntu0.2) ...
Setting up libmosquitto1:amd64 (1.4.8-1ubuntu0.16.04.2) ...
Setting up mosquitto-clients (1.4.8-1ubuntu0.16.04.2) ...
Processing triggers for libc-bin (2.23-0ubuntu10) ...
test@test:~$
```

- Step2: Configure MQTT for the Cellular Router

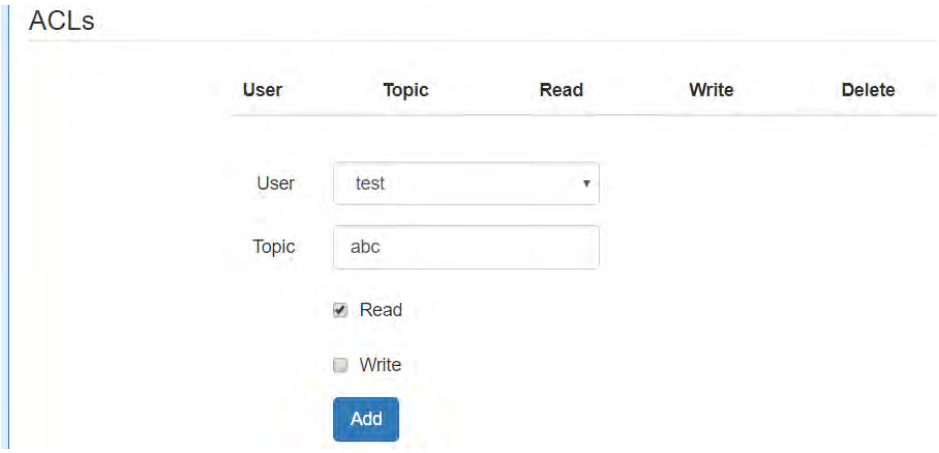
You need to add two users. For example, we create the users for test and test2.

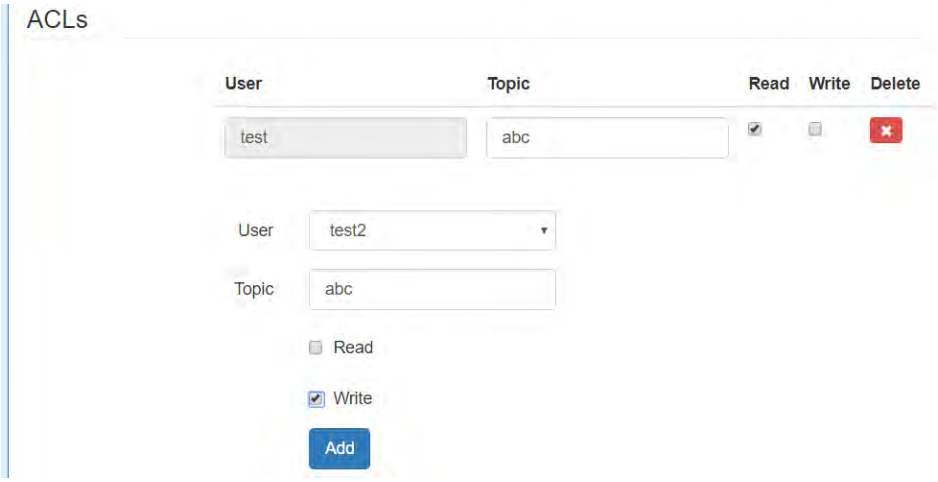


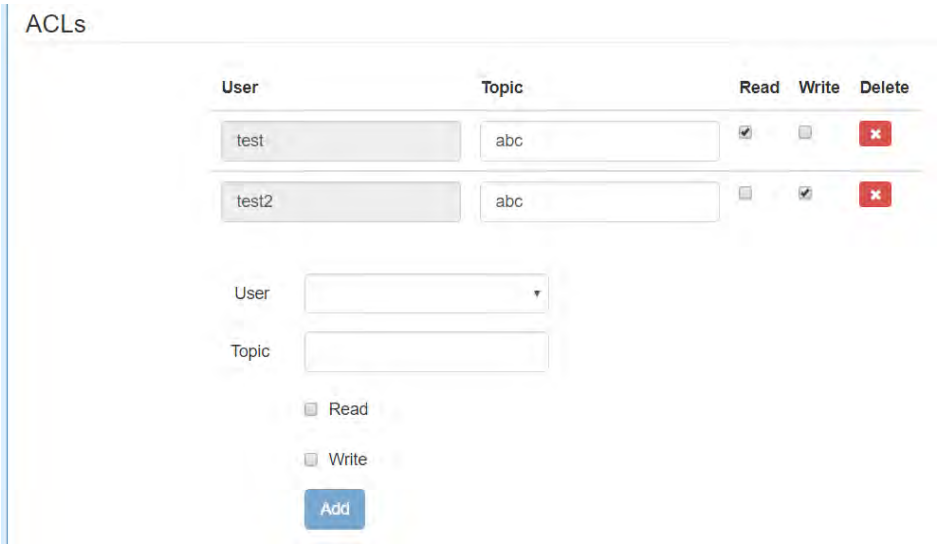




You need to add two ACLs based on the users you created. For instance, we create two ACLs for test user and test2 user.







Note:

- For Receive message command format:
  Mosquitto_sub -h <ICR100G-11 IP> -t <Topic> -u <username> -P <password>
- For Send message command format:
  Mosquitto_pub -h <ICR100G-11 IP> -t <Topic> -u <username> -P <password> -m

- Step3: There are two test MQTT examples.

Example 1: PC-A sends message to PC-B and PC-B should not receive any message.

For PC-B, command "mosquitto_sub -h 192.168.1.1 -t abc -u test2 -P test2".

```
Command Prompt (1) - mosquitto_sub  -h 192.168.1.1 -t abc -u test2 -P test2

C:\Program Files (x86)\mosquitto>ipconfig

Windows IP Configuration


Ethernet adapter Blue:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b400:e335:e5ca::101
   Link-local IPv6 Address . . . . . : fe80::8c61:e319:2e70:1140%15
   IPv4 Address. . . . . . . . . . . : 192.168.1.33
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::c2e:43ff:fe0d:4743%15
                                       192.168.1.1

C:\Program Files (x86)\mosquitto>mosquitto_sub -h 192.168.1.1 -t abc -u test2 -P test2
```

For PC-A, command "mosquitto_pub -h 192.168.1.1 -t abc -u test -P test -m test" and confirm the message on PC-B. It won't receive any message on PC-B.

```
test@test: ~
test@test:~$ ifconfig enp7s0
enp7s0    Link encap:Ethernet  HWaddr 1c:7e:e5:10:82:ed
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b400:e335:e5ca::102/128 Scope:Global
          inet6 addr: fe80::915:67ad:ddbf:2a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:34342 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4582 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9538280 (9.5 MB)  TX bytes:1065380 (1.0 MB)

test@test:~$ mosquitto_pub -h 192.168.1.1 -t abc -u test -P test -m test
test@test:~$
```


```
Command Prompt (1) - mosquitto_sub  -h 192.168.1.1 -t abc -u test2 -P test2

C:\Program Files (x86)\mosquitto>ipconfig

Windows IP Configuration


Ethernet adapter Blue:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b400:e335:e5ca::101
   Link-local IPv6 Address . . . . . : fe80::8c61:e319:2e70:1140%15
   IPv4 Address. . . . . . . . . . . : 192.168.1.33
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::c2e:43ff:fe0d:4743%15
                                       192.168.1.1

C:\Program Files (x86)\mosquitto>mosquitto_sub -h 192.168.1.1 -t abc -u test2 -P test2
```

Example 2: PC-B sends message to PC-A and PC-A should receive message.

For PC-A, command "mosquitto_sub -h 192.168.1.1 -t abc -u test -P test"

```
test@test: ~
test@test:~$ ifconfig enp7s0
enp7s0    Link encap:Ethernet  HWaddr 1c:7e:e5:10:82:ed
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b400:e335:e5ca::102/128 Scope:Global
          inet6 addr: fe80::915:67ad:ddbf:2a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50690 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4831 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10908302 (10.9 MB)  TX bytes:1150596 (1.1 MB)

test@test:~$ mosquitto_sub -h 192.168.1.1 -t abc -u test -P test
```

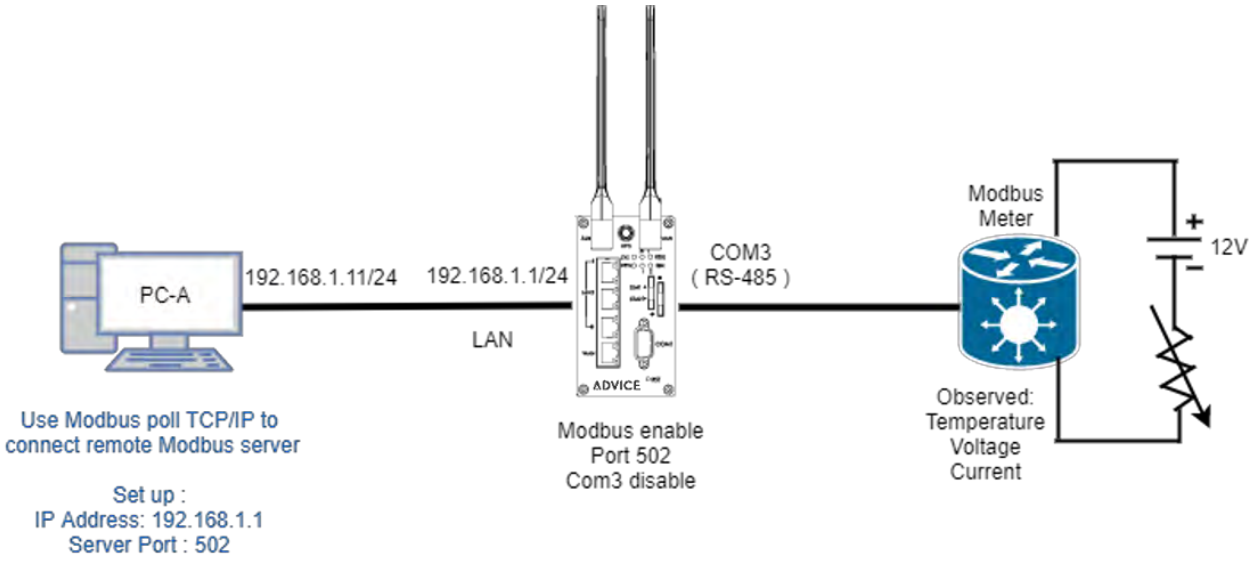
For PC-B, command "mosquitto_pub -h 192.168.1.1 -t abc -u test2 -P test2 -m test" and confirm the message on PC-A. It will receive test message on PC-A.

```
Command Prompt (1)

C:\Program Files (x86)\mosquitto>ipconfig

Windows IP Configuration


Ethernet adapter Blue:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b400:e335:e5ca::101
   Link-local IPv6 Address . . . . . : fe80::8c61:e319:2e70:1140%15
   IPv4 Address. . . . . . . . . . . : 192.168.1.33
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::c2e:43ff:fe0d:4743%15
                                       192.168.1.1

C:\Program Files (x86)\mosquitto>mosquitto_pub -h 192.168.1.1 -t abc -u test2 -P test2 -m test

C:\Program Files (x86)\mosquitto>
```

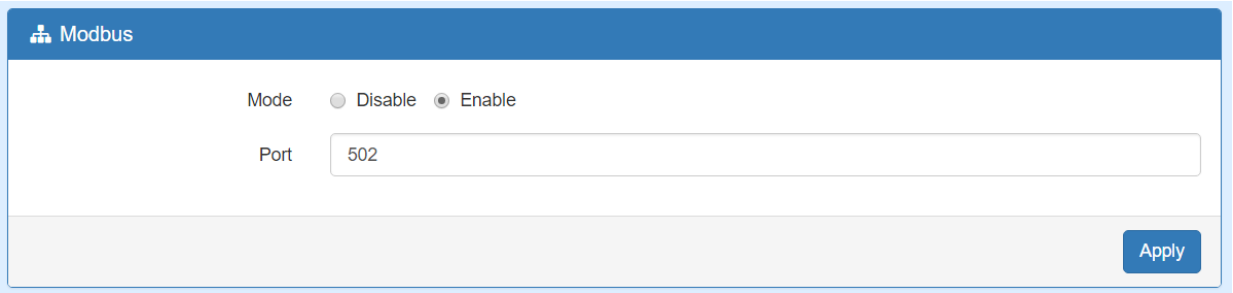
```
test@test: ~
enp7s0    Link encap:Ethernet  HWaddr 1c:7e:e5:10:82:ed
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b400:e335:e5ca::102/128 Scope:Global
          inet6 addr: fe80::915:67ad:ddbf:2a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50690 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4831 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10908302 (10.9 MB)  TX bytes:1150596 (1.1 MB)

test@test:~$ mosquitto_sub -h 192.168.1.1 -t abc -u test -P test
test
```

13.3 Modbus Topology

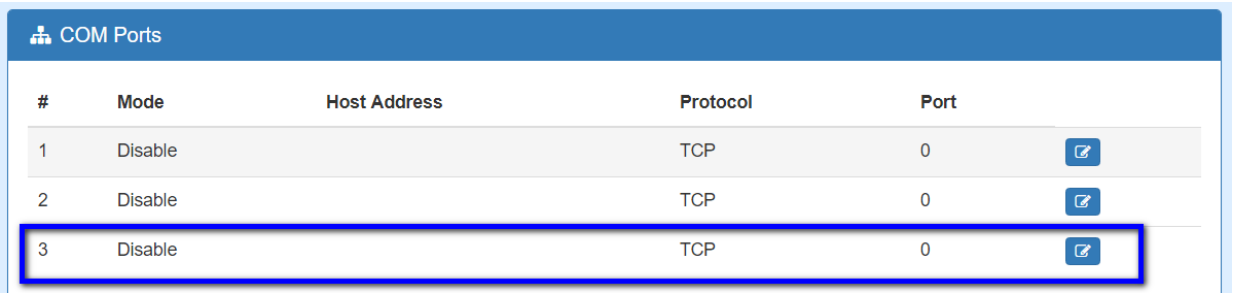
There is an example for Modbus Topology that you can configure Modbus gateway to observe the temperature, voltage and current from Modbus meter on PC-A.



The settings of Modbus is shown as below. The mode is Enable. The default port is 502.

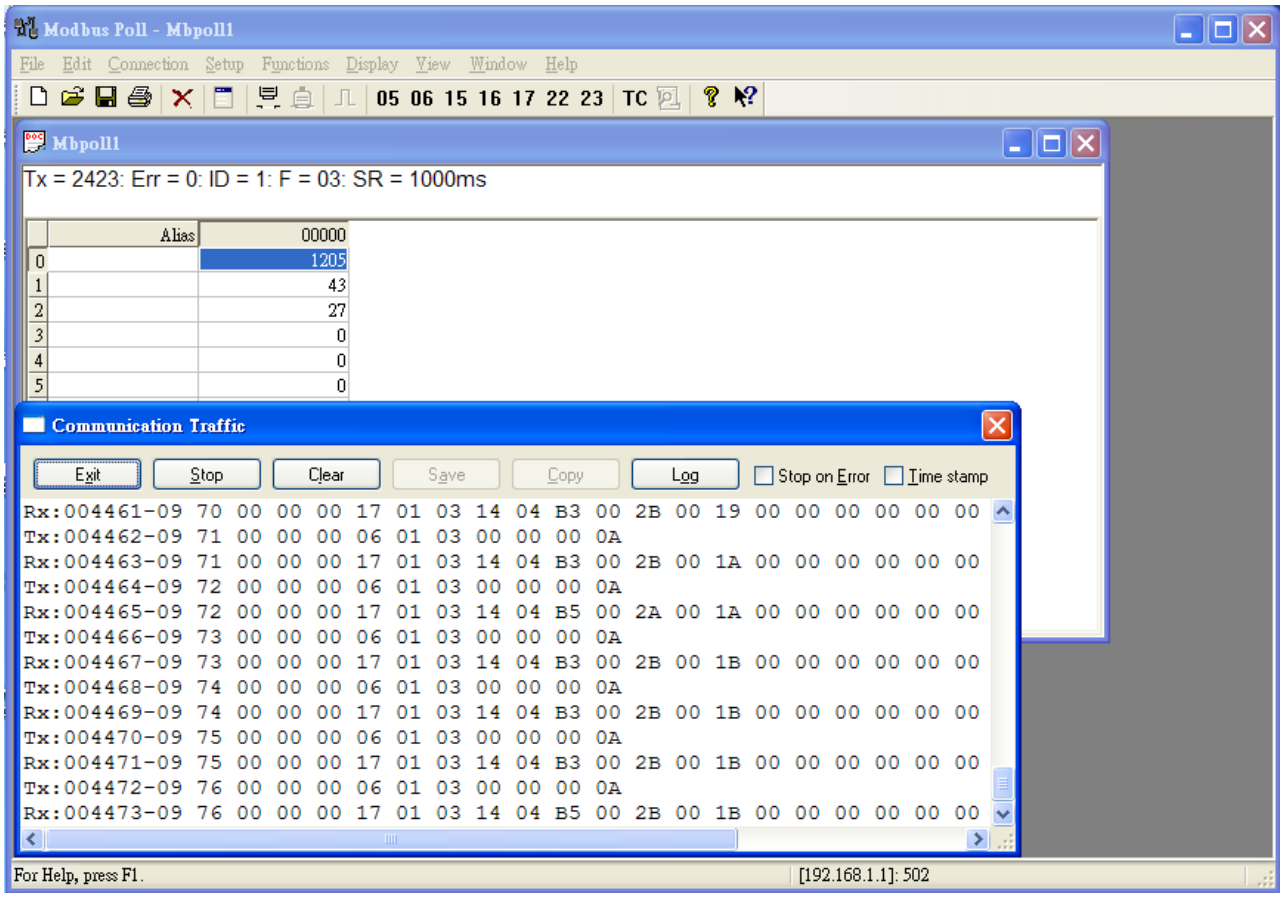


Please confirm the interface of COM Port 3 that the mode is Disable.



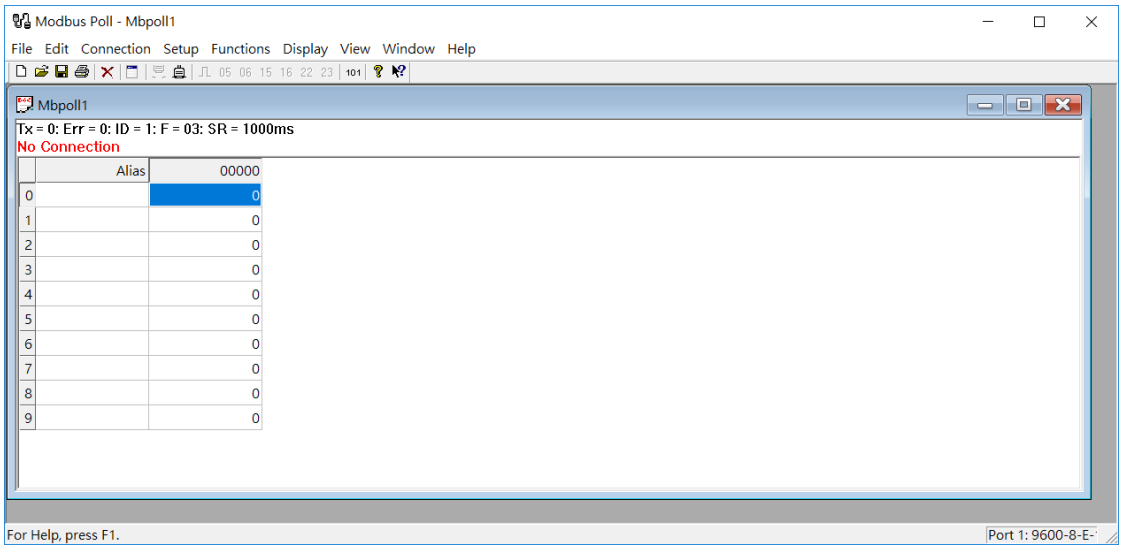
#	Mode	Host Address	Protocol	Port
1	Disable		TCP	0
2	Disable		TCP	0
3	Disable		TCP	0

Next, you can connect a meter of DC voltage and current for supporting Modbus protocol with RS-485 serial to COM Port 3 from the cellular router and know the information about temperature, voltage and current.



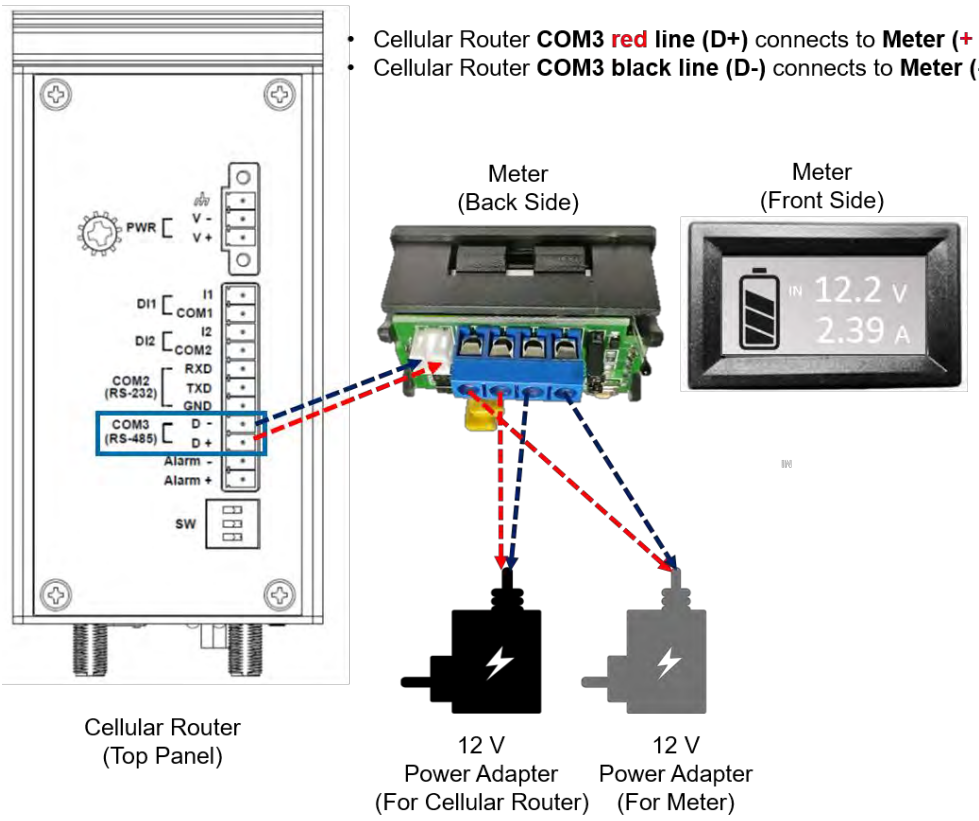
Note 1:

- There is a reference for Modbus poll software to download and install on PC.
  http://www.tucows.com/preview/502459/Modbus-Poll

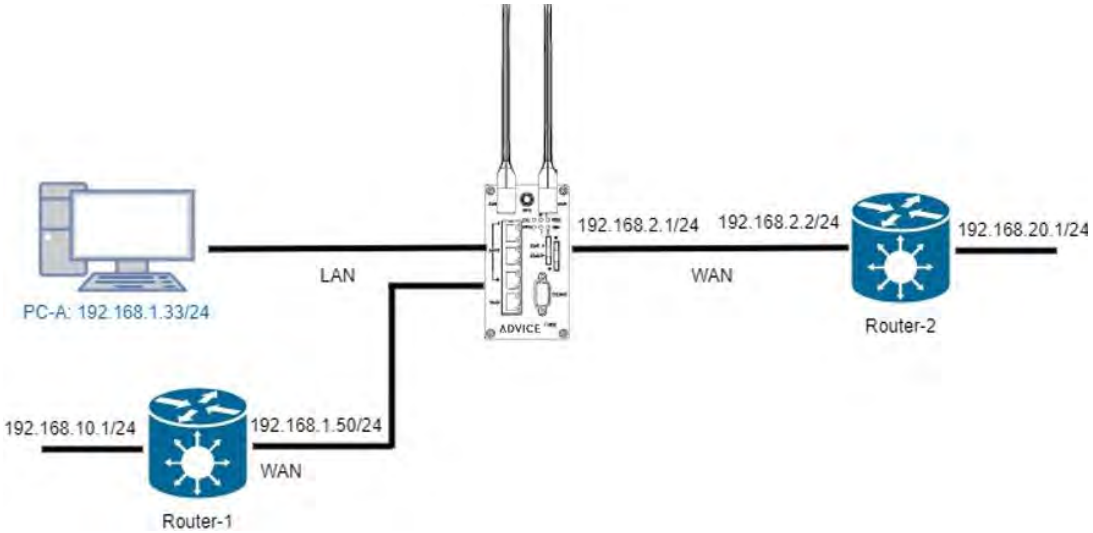


Note 2:

- You can purchase a meter of DC voltage and current supporting Modbus protocol with RS-485 serial for test and connection to COM Port 3.
- The following picture shows how connect the ports and the lines between a cellular router and a meter.



13.4 IP Routing Topology



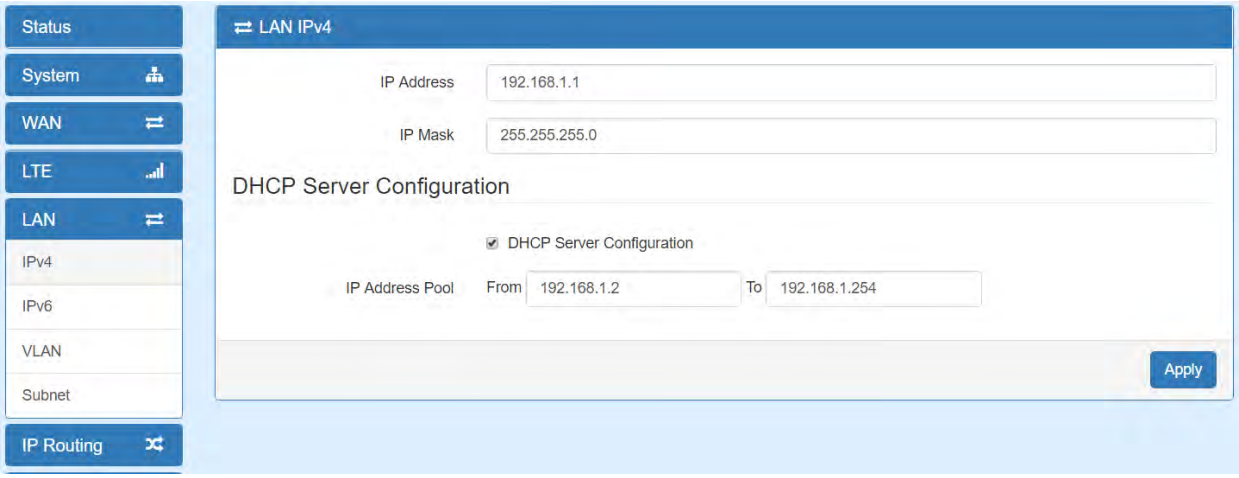
This IP Routing topology that the cellular router connects Router-1 and Router-2 will have two results.

(1) PC-A sends ICMP packet to Router-1 LAN and WAN IP and they should have response.

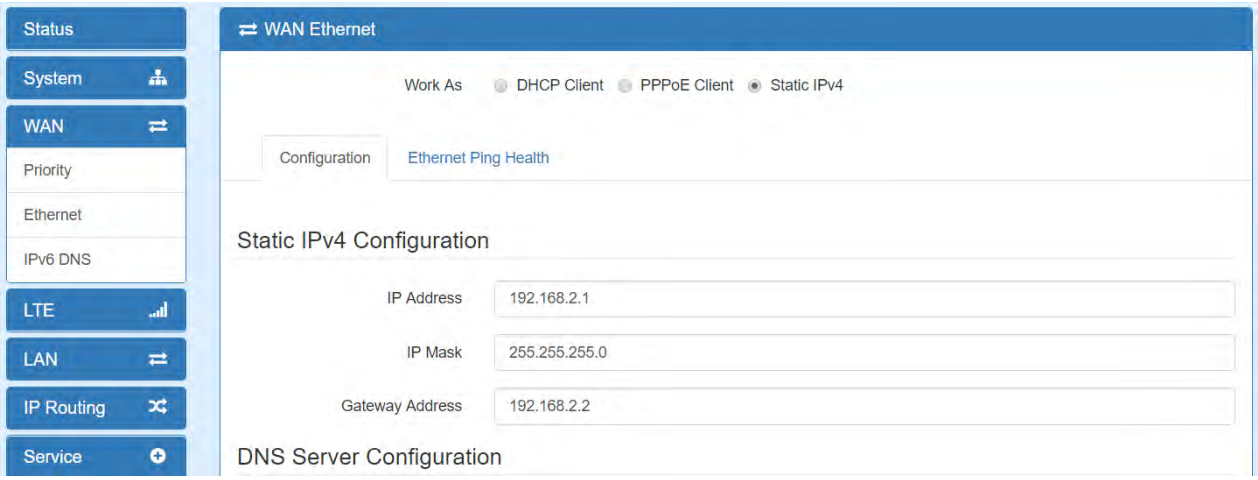
(2) PC-A sends ICMP packet to Router-2 LAN and WAN IP and they should have response.

Note: Router-1 and Router-2 are pure routers and should be supported "NAT enable / disable".

- LAN configuration:



- WAN configuration:

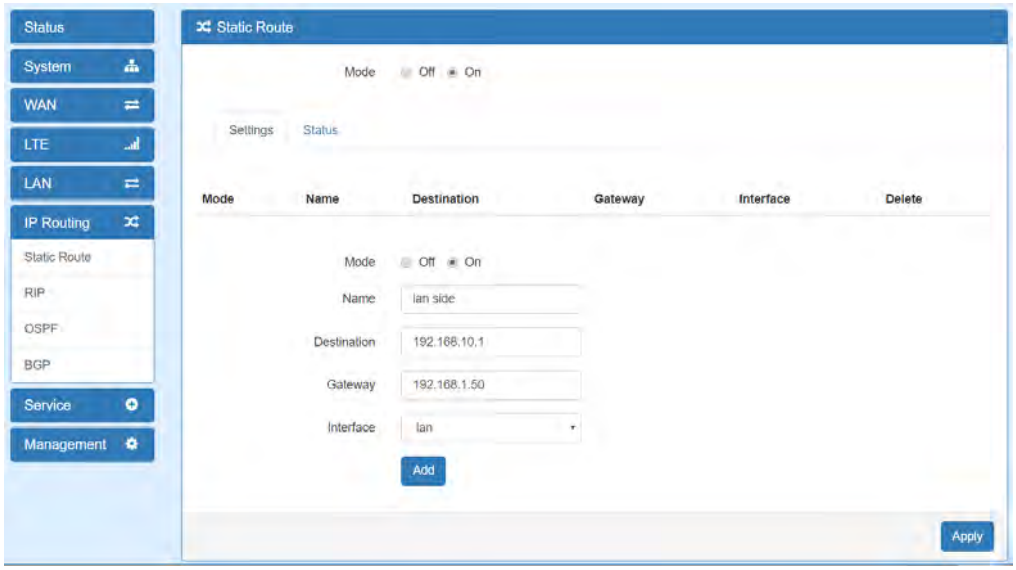


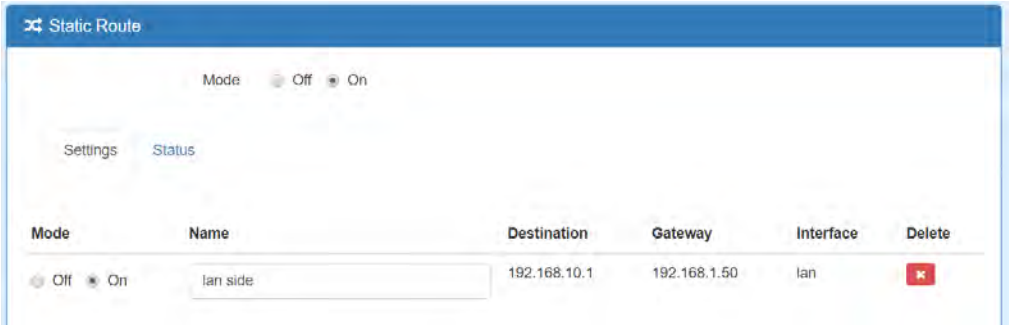
There are two examples to introduce how to work for routing.

Example 1: Add IP Routing on LAN interface

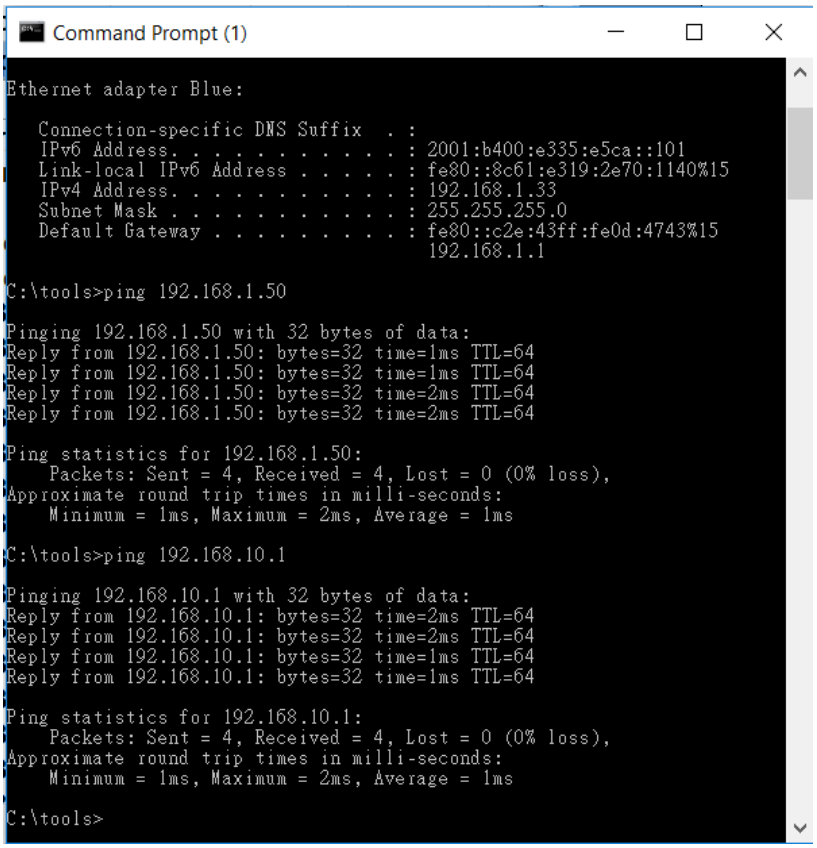
- Step 1: The cellular router for Static Route configuration
  The Mode is on at the settings section and add the routing.
- Step 2: Router-1 configuration is as below.

(1) Login to the Router-1 web site, and then "NAT disable".
(2) Configure LAN IP: 192.168.10.1
(3) Configure WAN IP: 192.168.1.50





- Result: PC-A sends ICMP packet to Router-1 LAN and WAN IP and they should have response.



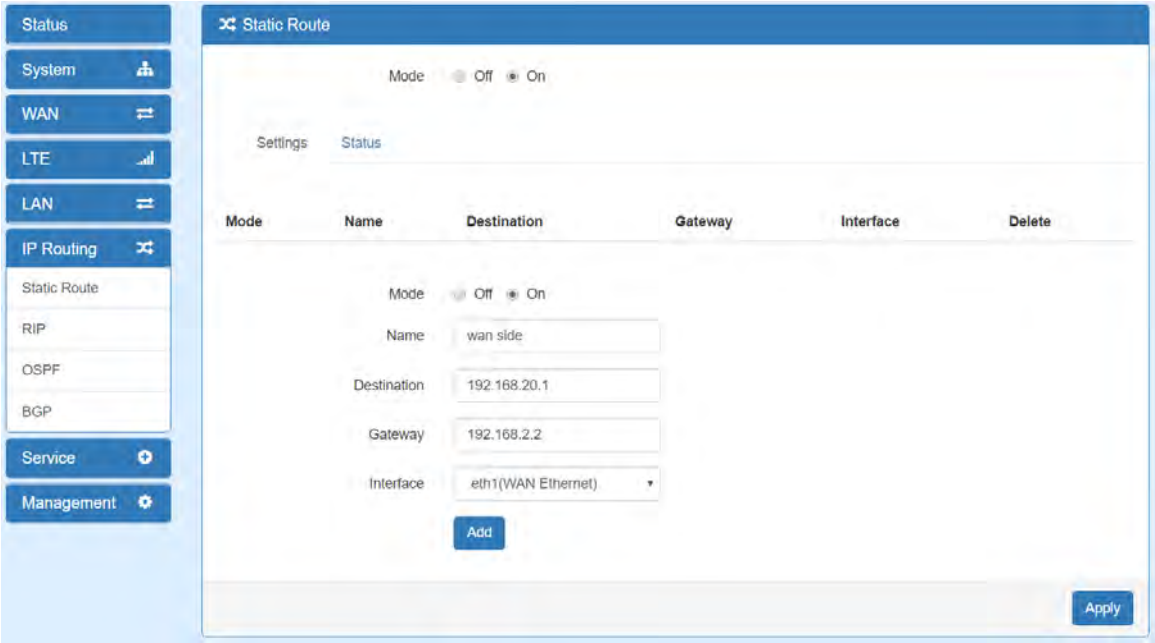
Example 2: Add IP Routing on WAN interface

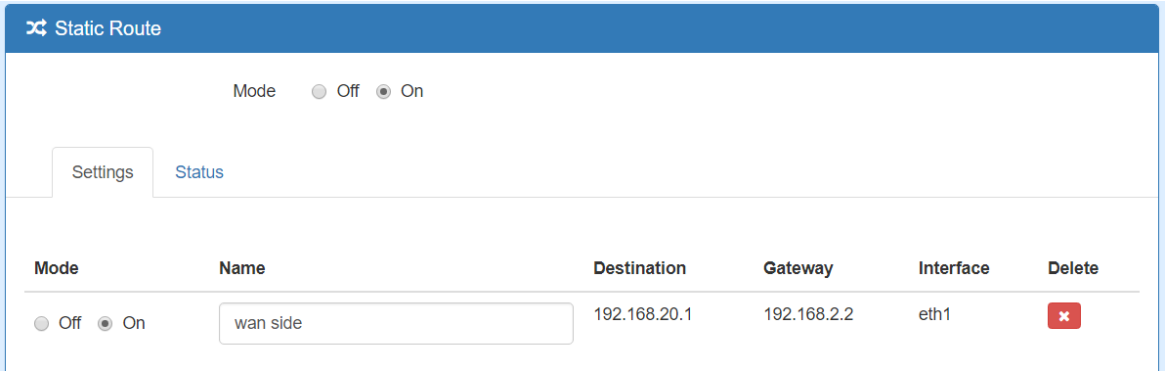
- Step1: The cellular router for Static Route configuration
  The Mode is on at the settings section and add the routing.
- Step2: Router-2 configuration is as below.

(1) Login to the Router-2 web site, and then "NAT disable".

(2) Configure LAN IP: 192.168.20.1

(3) Configure WAN IP: 192.168.2.2





- Result: PC-A sends ICMP packet to Router-2 LAN and WAN IP and they should have response.