Industrial 4G LTE Cellular Router

ICR111WG

User Manual

Version 1.1

Table of Contents

1 Introduction

ICR111WG compact, lightweight and cost-effective **Industrial 4G LTE Cellular Routers**, are built in 2-port fast Ethernet connection as well as support 2G/3G/4G mobile networks for wired and wireless communication in harsh environments. Equipped with RS232 serial port and digital input/output interfaces, the **ICR111WG** is simple to configure and collect real-time data transmission quickly for Industrial IoT and machine-to-machine applications. The **ICR111WG** is also compliant with IEEE 802.11b/g/n Wi-Fi connectivity.

Featuring VPN Tunnels, Firewall, TR069, and SNMP Trap, **ICR111WG Industrial 4G LTE Cellular Routers** enhance highly secure authentication, encryption and management to protect your data efficiently between public and private networking. Supporting -30~+70°C wide temperature operation and flexible input voltage range of 8-48VDC for diverse environments and various applications.

ICR111WG Industrial 4G LTE Cellular Routers are suitable and reliable choices for fast deployment and easy configuration to simplify your complicated solutions and fit your services for industrial networking and smart city.

1.1 Features

- Highly reliable and secure for mission-critical cellular communications
- Compact and lightweight design with 2-port Ethernet interfaces
- Support multi-band connectivity with FDD LTE/ TDD LTE/ WCDMA/ GSM/ LTE Cat 4
- Provide IEEE 802.11b/g/n Wi-Fi standards
- Built-in micro SIM connector, RS232 serial port, and DI/DO interfaces
- Integrated detachable antenna against radio interference
- LED indicators for connection and data transmission status
- Industrial rated from -30 to +70°C for use in harsh environments
- IPv6/IPv4 dual stack and all applications are IPv6 ready
- Support serial communication protocols for rich connectivity
- Enhance security and encryption for authentication and transmission

1.2 Specifications

Cellular Interface

- Standards:
  (Please see ordering information for optional band)
  - 4G: FDD LTE, TDD LTE
  - 3G: WCDMA
  - 2G: GSM/EDGE
- LTE Data Rate: Cat 4, 150Mbps (DL), 50Mbps (UL)

Wi-Fi Interface

- Compliant with IEEE 802.11 b/g/n Wi-Fi standards
- 2.4 GHz radio band for wireless
- 2T2R 300 Mbps wireless operation rate
- Wireless security with WPA2-PSK(AES)
- Multiple SSIDs
- Wireless MAC Filtering
- Wireless client isolation

Hardware Interface

- High Performance 550 MHz SoC with 128MByte Flash
- 1 x Micro SIM Connector (push-push type)
- 1 x LAN 10/100 Mbps Ethernet port
- 1 x WAN 10/100 Mbps Ethernet port
- WPS / RESET Button
- 1 x RS232 (TXD/RXD/GND)
- 1 x DI (Non-Isolated), 1 x DO (Non-Isolated)
- 2 x SMA connectors for detachable LTE Antenna
- 2 x RP-SMA connectors for detachable Wi-Fi Antenna
- 1 x SMA connector for detachable GPS antenna

Physical Characteristics

- Enclosure：Metal Case
- Dimensions (W x H x D)：91mm x 28mm x 74mm
- Weight：250 g (0.5512 lb)
- Installation：DIN Rail / Wall Mount

LED Display

- 1 x Power LED
- 1 x Ethernet LED for each port (LAN/WAN)
- 1 x RSSI LTE LED
- 1 x Function LED (User define by Web)

Power Supply

- Power Consumption 7 Watts(Max)
- Power Input 8 ~ 48VDC

Software

- **Network Protocols:**

IPv4, IPv6, IPv4/IPv6 dual stack, DHCP server and client, PPPoE, Static IP, SNTP, GPS sync time, DNS Proxy, VRRP, OSPF, Message Queue Telemetry Transport (MQTT Broker), BGP, Flow (Modbus master ↔ MQTT client)

- **Routing/Firewall:**

NAT, Virtual Server, DMZ, MAC Filter, URL Filter, IP Filter, VLAN, Static Routing and RIP-1/2, IPS, Policy Route

- **VPN:**

OpenVPN, IPSec (3DES, AES128, AES196, AES256, MD5, SHA-1, SHA256), GRE, PPTP, L2TP

- **Wireless Connectivity:**
  WAN WiFi Client
- **Others:**

DDNS, QoS, UPnP, SMS Action, GPS Track Drawing, GPS TCP Push

- **Alarm:**

DI, DO, SMS, VPN/WAN Disconnect, SNMP Trap, E-mail, TR069

Management Software

- Web GUI for remote and local management, CLI
- Syslog monitor
- SNMP, TR069
- FOTA (Firmware over the Air)
- Remote management via SSH v2, HTTPS
- Local management via Telnet, SSH v2, HTTP/HTTPS

Environment

- Operating Temperature -30 ~ +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 301489 , FCC Part 15B Class B
- **EMS：**EN 301489
- **Vibration：**IEC60068-2-6
- **Radio：**EN 301511, EN 301908-1, EN 301908-2, EN 301908-13, EN 300328, EN 303413, EN 62311

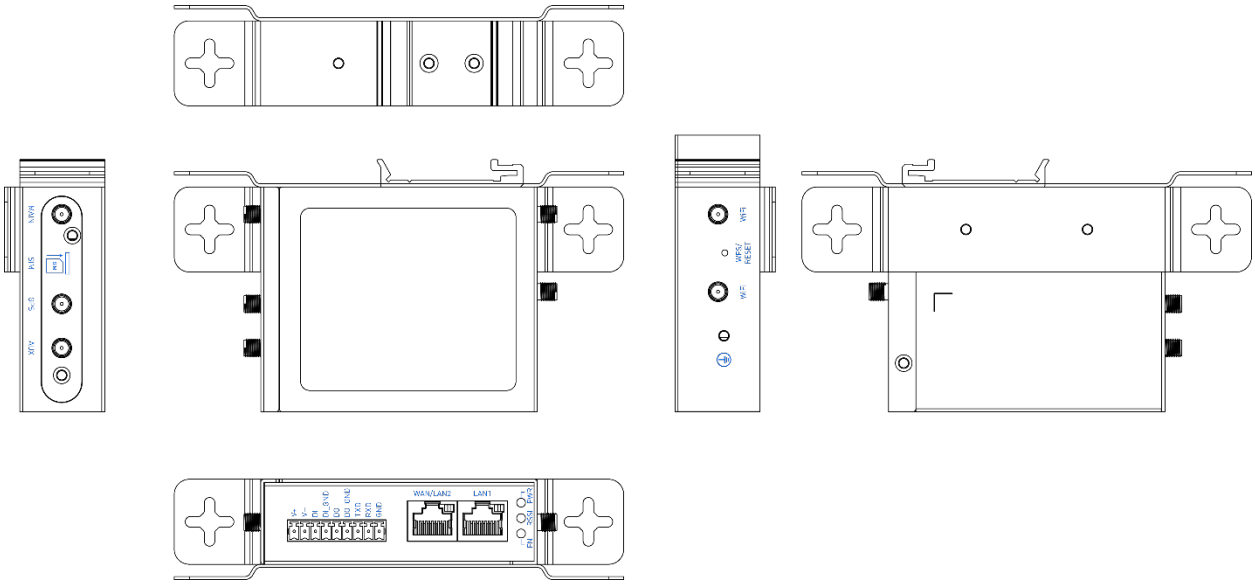
Note:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

1.3 Mechanical Dimensions



2 Hardware Installation

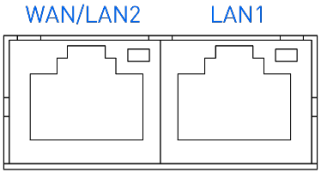
This chapter introduces how to install and connect the hardware.

2.1 LED Indicators

LED	FN	RSSI	PWR
ON	VPN Connected	High Signal	Power ON
Slow Blinking	Internet Connected / Reset	Medium Signal / Reset	N/A
Fast Blinking	System Booting / Reset to Default	Low Signal / Reset to Default	N/A
OFF	N/A	Error	Power OFF
Heart Beat	Wi-Fi Connected	WPS Processing	N/A

2.2 Ethernet Port

(1) 10/100 Mbps Ethernet LAN/WAN



The LAN and WAN interface are standard RJ45 connectors.

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

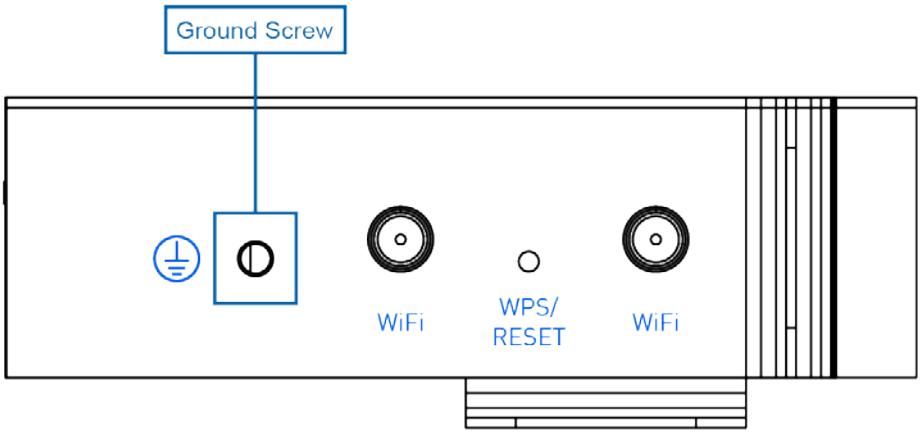
(2) LED Indicator of Ethernet Port

Each Ethernet port has one LED indicators. The Green LED indicates Link/ACT.

LED	Status	Description
Green (Link/ACT)	Off	Connection is down.
	Blink	Data is being transmitted.
	On	Connection is up.

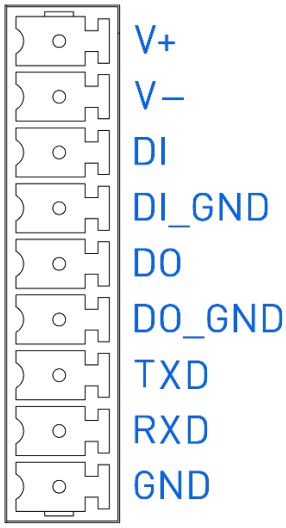
2.3 Grounding the Router

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.



(ICR111WG)

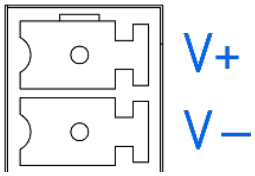
2.4 Pin Assignments



Power Input (V+, V-) / DI / DO / UART RS-232 (TXD, RXD, GND)

2.5 Connecting the Power Supply

The router requires a DC power supply in the range of 8~48V DC.



Pin	Power (8~48VDC)
V -	Negative
V+	Positive

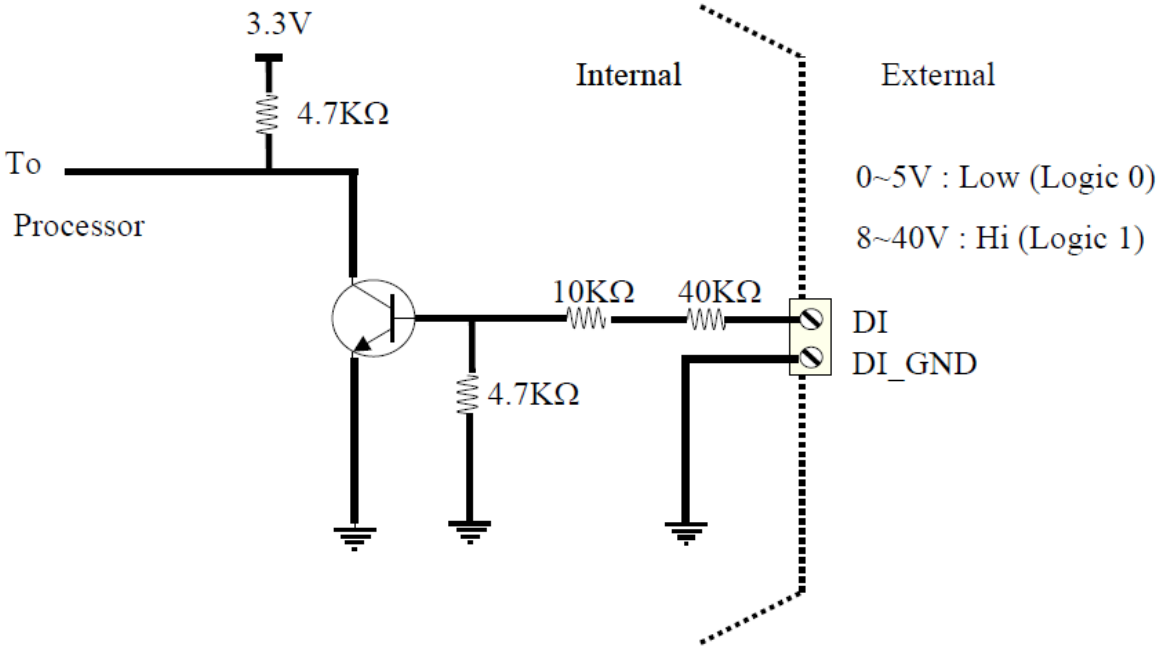
2.6 Connecting I/O Ports

(1) Digital Input (DI)

The unit has two terminals on the terminal block for the digital inputs.

Pin	Description
DI	Digital Input
DI_GND	

- DI: Low (+0 to +5V) / High (+8 to +40V)

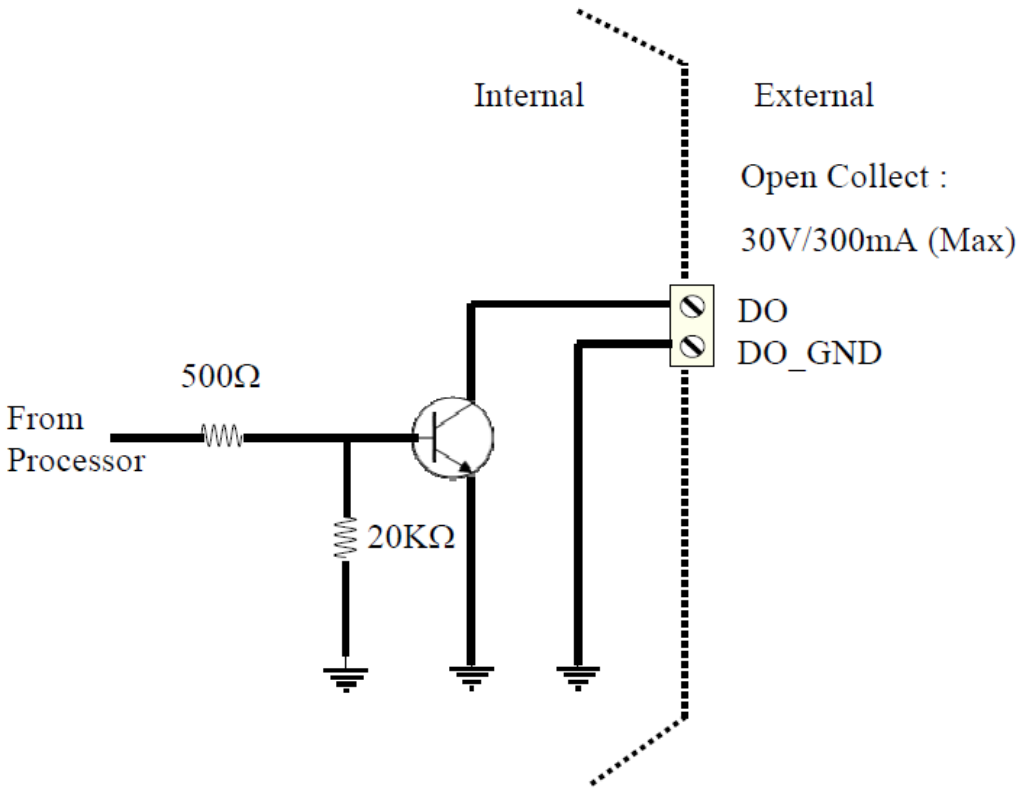


(2) Digital Output (DO)

The unit has 2 terminals on the terminal block for the digital outputs.

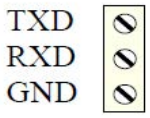
Pin	Description
DO	Digital Output
DO_GND	

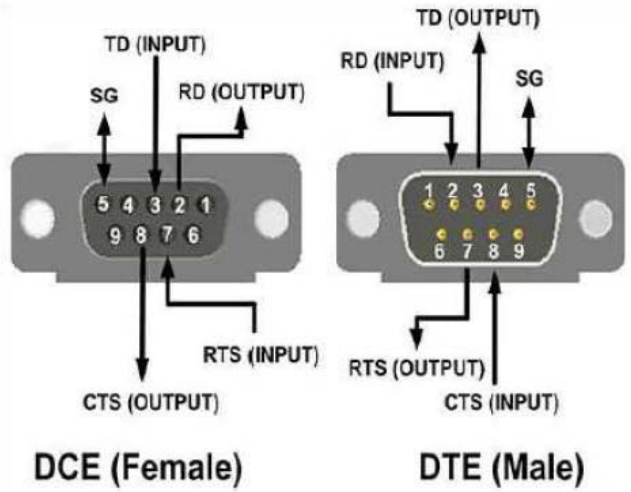
- DO: Open Collect (maximum 30V/300mA)



2.7 UART (RS-232)

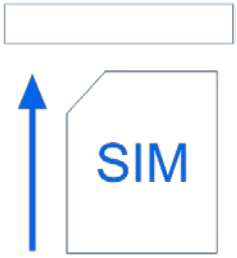
The port is a standard RS-232 signal level interface.





Pin	Signal	Direction
TXD	Transmit Data	Output
RXD	Receive Data	Input
GND	Signal Ground	-

2.8 Install the SIM Card



Insert and Remove SIM 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) Insert the SIM card with right direction. Push the SIM card in to the slot, and lightly press it to lock it in the slot.

(3) To remove the SIM card, lightly press the SIM card, and it will pop out.

2.9 Reset Button

Function	Operation
WPS Processing	Press the button less than 5 seconds.
Reset	Press the button for 5-10 seconds.
Reset to default setting	Press the button for more than 10 seconds.

2.10 External Antenna

Each unit has three antenna connectors, MAIN, GPS, AUX (SMA). For ICR111WG, there will be five antenna connectors and extra two antennas for Wi-Fi (RP-SMA). Connect the antenna to MAIN when you have only one antenna. Please tighten the connecting nut properly to ensure good connection.

(ICR111WG)

3 Configuration via Web Browser

3.1 Access the Web Configurator

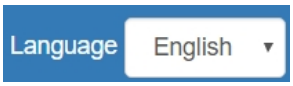
The web configuration is an HTML-based management interface for quick and easy to set up of the cellular router. Monitoring of the status, configuration and administration of the router can be done via the Web interface.

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.

Title Bar Panel > Selecting Language

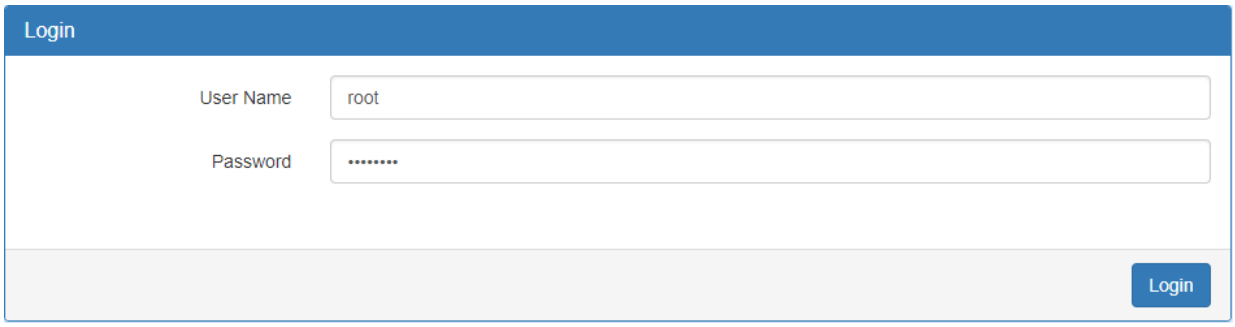
You can choose the languages, including English and Taiwan.

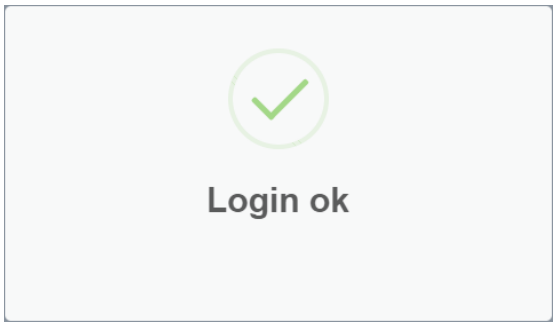


Logging in the Router

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.



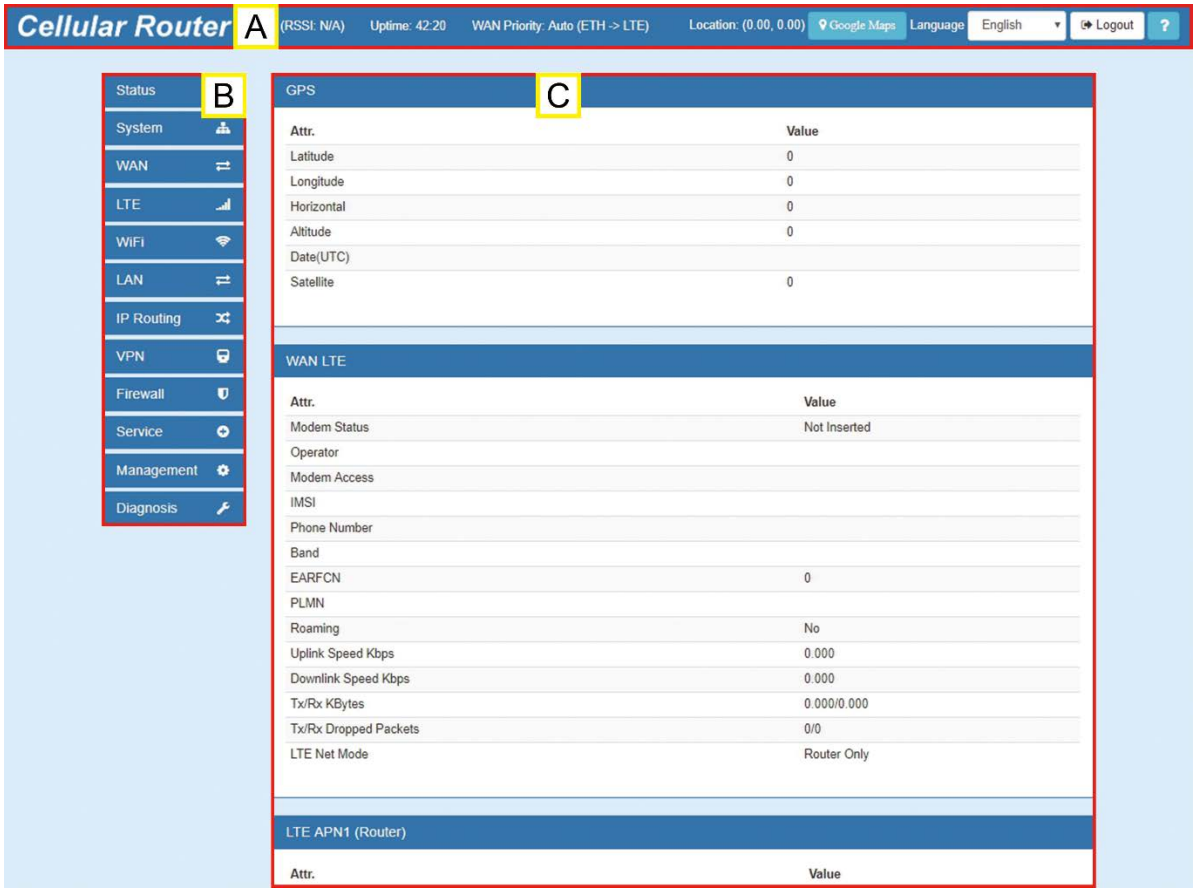


Note: After changing the User Name and Password, strongly recommend you to save them because another time when you log in, the User Name and Password have to be used the new one you changed.

3.2 Navigate the Web Configurator

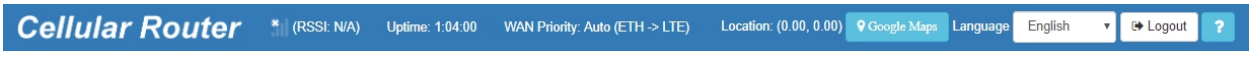
The main screen is divided into three parts as below.

A -Title Bar, B - Navigation Panel and C - Main Window.



(1) A : Title Bar

The title bar provides some useful instructions that appear the situation of router.



Title Bar	
Item	**Description**
RSSI	Show if the SIM card is inserted in the slot. If yes, RSSI (Received Signal Strength Indicator) shows the current signal strength in a wireless network and the name of telecommunication operator.
Uptime	Show the time starting turn on the router until current using.
WAN Priority	Show the three mode of WAN status, which is first to use.
Location	Show the position of router from Google Maps. ***Note:*** This function is for GPS spec.
Google Maps	Display Google Map according to location.
Language	Choose your language from the drop-down list on the upper right corner of the title bar.
Login/Logout	Click to log in or log out of the web configurator.
?	Online Manual

(2) B : Navigation Panel-Main Menu and Sub Menu

The menu items are divided into main and sub menu to configure the settings and get the status of connectivity on the navigation panel.

(3) C : Main Window

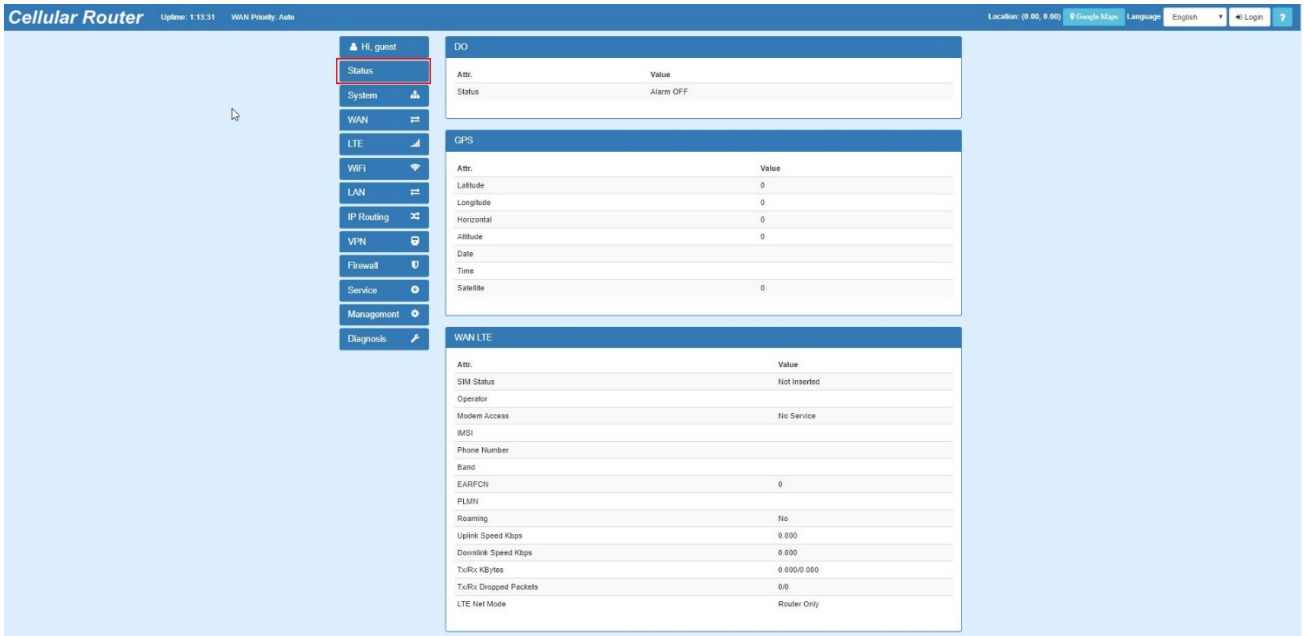
This section shows the information or setting fields from main menu and sub menu.

4 Status

When you enter the web browser in the beginning and have not log in, the first item of main menu shows your status that you are a guest. This status only can view status page without any permission to log in. The interface of main window displays the status of router to show about information, including Cellular Attribute, the current connectivity of WAN Ethernet and LAN Ethernet. If the router has GPS function, the GPS interface is shown.

Note: After logging in the system, you can set up the status of user and divide into three levels for setting user's authority, including **Super User**, **Administrator**, and **Read Only**. For Guest, this status is without any authority. All users log in or log out and they need to have Web UI log records.

Status	Super User	Administrator	Read Only	Guest
User name	system account (root/admin)	only Super User can modify	only Super User can modify	N/A
Password	configurable	configurable	configurable	N/A
Permission	● Add/Delete/Modify all users' accounts except Super User. ● Read/Write Configuration	Read/Write Configuration	only Read Configuration	N/A



Status > DO	
Item	**Description**
Attribute	
Status	• Alarm ON: DO is configured to turn on when alarm is triggered. • Alarm OFF: Alarm is configured to be disabled. • Alarm PULSE: DO is configured to pulse when alarm is triggered. • Force ON: DO is turn on by remote command. • Force OFF: DO is turn on by remote command. • Force PULSE: DO is turn pulse by remote command.

Status > GPS	
Item	**Description**
Attribute	
Latitude	Show the latitude information of location.
Longitude	Show the longitude information of location.
Horizontal	Horizontal precision:0.5-99.9
Altitude	The altitude of antenna away from the sea level (unit: m), accurate to one decimal place.
Date	UTC date when fixing position.
Time	UTC time when fixing position.
Satellite	Number of satellites.

Status > WAN LTE	
Item	**Description**
Attribute	
SIM Status	• Ready: No PIN code protection or unlock already. • Unlock: Unlock pin code protection. • Locked: Locked by pin code. • Error: SIM operation error. • Blocked: PUK needed to unlock. • Not Inserted: No SIM card. • Hardware Error: Unable to enable function. • Ignore: Ignore Specified SIM in dual SIM device.
Operator	Display the name of operator.
Modem Access	The router to access protocol type.
IMSI	The IMSI number of the SIM card.
Phone Number	The phone number of the SIM card.
Band	The current connected Band.
EARFCN	Absolute radio-frequency channel number.
PLMN	Public LAN Mobile Network ID.
Roaming	Roaming status.
Uplink Speed Kbps	Uplink Speed in Kbps.
Downlink Speed Kbps	Downlink Speed in Kbps.
Tx/Rx KBytes	Accumulated TX/RX in KBytes.

Tx/Rx Droppes Packets	TX/RX Dropped Packets.
LTE Net Mode	LTE Network Mode for both APNs.

Status > LTE APN1 (Router)	
Item	**Description**
Attribute	
IPv4 Address	WAN obtain IPv4 Address.
IPv4 Mask	WAN obtain IPv4 Mask.
Default Gateway	WAN IPv4 Default Gateway.
Connected	Yes: Connected; No: Disconnected.
IPv4 Conn Time	WAN IPv4 Connected Time.
Uplink Speed Kbps	Uplink Speed in Kbps.
Downlink Speed Kbps	Downlink Speed in Kbps.
Tx/Rx KBytes	Accumulated TX/RX in KBytes.
TX/RX Dropped Packets	TX/RX Dropped Packets.

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 > WAN Ethernet	
Item	**Description**
Attribute	
IPv4 Address	Ethernet WAN obtain IPv4 Address.
IPv4 Mask	Ethernet WAN obtain IPv4 Mask.
Default Gateway	Ethernet WAN IPv4 Default Gateway.
IPv6 Conn Time	Ethernet WAN IPv4 Connected Time.

Status > WAN WiFi	
Item	**Description**
Attribute	
IPv4 Address	WAN WiFi obtain IPv4 Address.
IPv4 Mask	WAN WiFi obtain IPv4 Mask.
Default Gateway	WAN WiFi IPv4 Default Gateway.
IPv4 Conn Time	WAN WiFi IPv4 Connected Time.
SSID	Service Set Identifier of WAN WiFi.
MAC Address	MAC Address of WAN WiFi.
Channel	The current connected Channel.

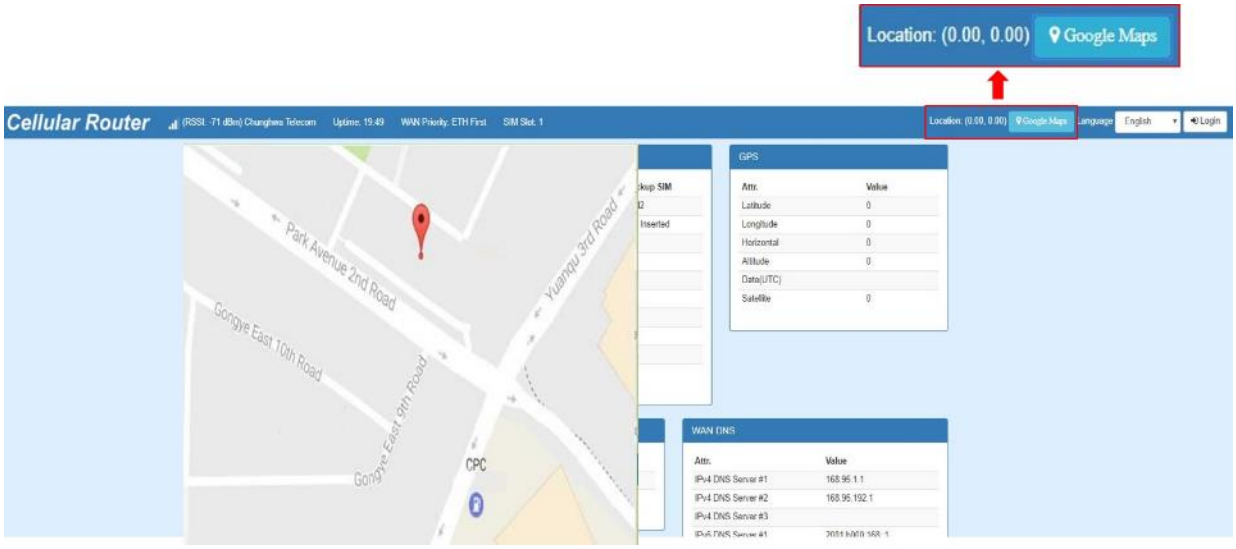
Status > LAN Ethernet	
Item	**Description**
Attribute	
IPv4 Address	LAN is assigned IPv4 Address.
IPv4 Mask	LAN is assigned IPv4 Mask.
IPv6 Address	LAN is assigned IPv6 Address.
IPv6 Conn Time	IPv6 Connected Time.
Uplink Speed Kbps	Uplink Speed in Kbps.
Downlink Speed Kbps	Downlink Speed in Kbps.
Tx/Rx KBytes	Accumulated TX/RX in KBytes.
TX/RX Dropped Packets	TX/RX Dropped Packets.

Status > WiFi AP	
Item	**Description**
Attribute	
Connected Clients	The number of connected clients.

Status > Connected VPN Connections	
Item	**Description**
Attribute	
Open VPN	Open VPN connected number.
IPSec	IPSec connected number.
GRE	GRE connected number.
PPTP Server	PPTP server connected number.
L2TP	L2TP connected number.

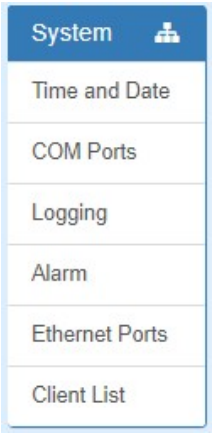
4.1 Status > GPS

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



5 Configuration > System

This system section provides you to configure the following items, including Time and Date, COM Ports, Logging, Alarm, Ethernet Ports, and Client List.



5.1 System > Time and Date

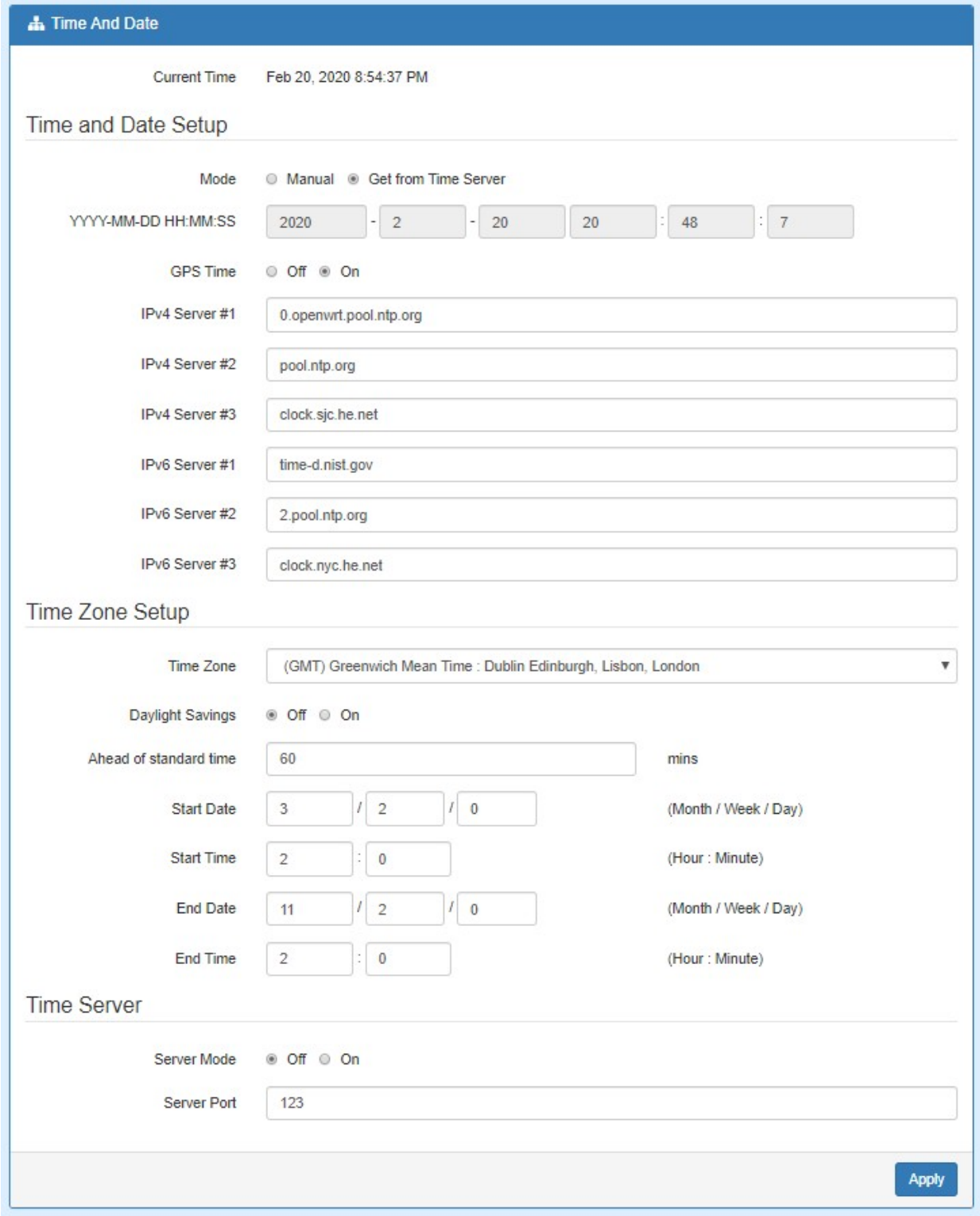
This section allows you to set up the time and date of router and NTP server. There are two modes at Time and Date Setup, including **Get from Time Server** and **Manual**. The default mode is **Get from Time Server**.

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.

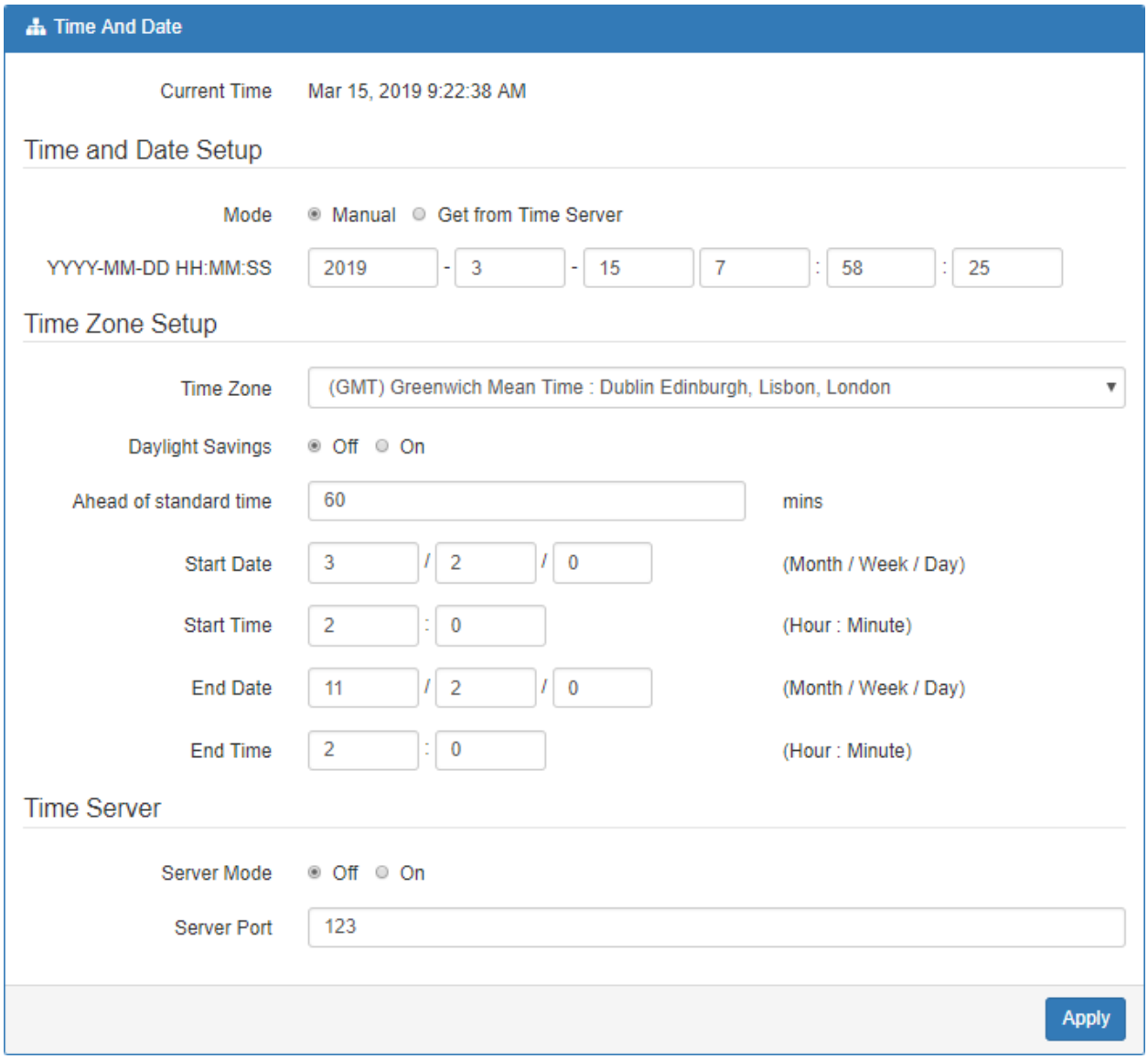
I. Get from Time Server

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


Time And Date
Current Time
Feb 20, 2020 8:54:37 PM
Time and Date Setup
Mode
Manual
Get from Time Server
YYYY-MM-DD HH:MM:SS
2020 - 2 - 20 20 : 48 : 7
GPS Time
Off
On
IPv4 Server #1
0.openwrt.pool.ntp.org
IPv4 Server #2
pool.ntp.org
IPv4 Server #3
clock.sjc.he.net
IPv6 Server #1
time-d.nist.gov
IPv6 Server #2
2.pool.ntp.org
IPv6 Server #3
clock.nyc.he.net
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)
Time Server
Server Mode
Off
On
Server Port
123
Apply

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)

System > Time Zone Setup > 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 minus.
Start Date / Start Time	Time to enter Daylight Savings duration. The Month range is 1~12. 1 - Jan. 7 - Jul. 2 - Feb. 8 - Aug. 3 - Mar. 9 - Sep. 4 - Apr. 10 - Oct. 5 - May 11 - Nov. 6 - Jun. 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.

IV. Time Server

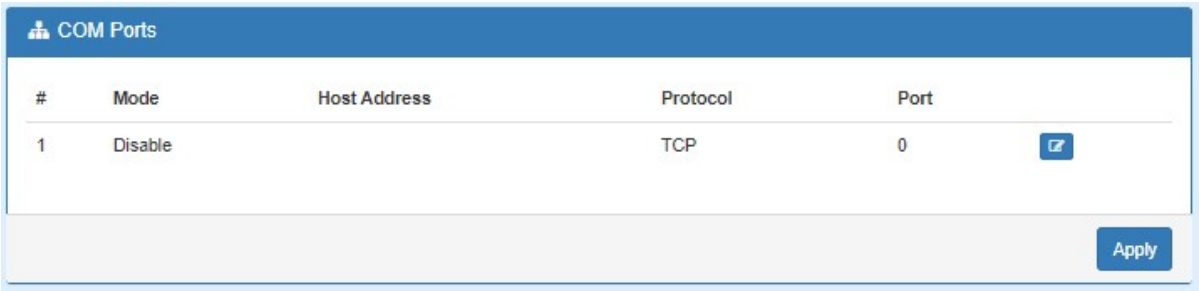
The Time server feature allows user to set a time server for LAN side client to get the time through NTP/SNTP protocol.

System > Time Server	
Item	**Description**
Server mode	Turn on/off the time server.
Server port	The UDP port listened by time server.

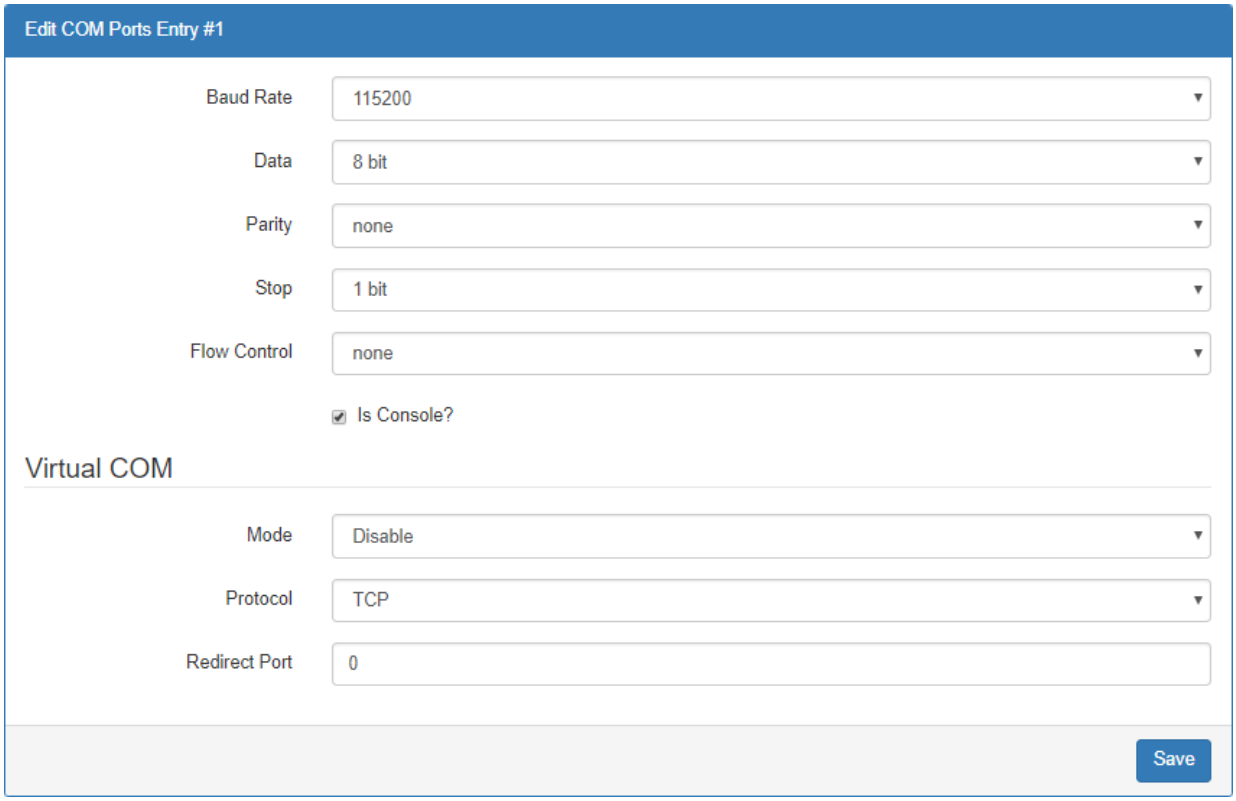
5.2 System > COM Ports

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.

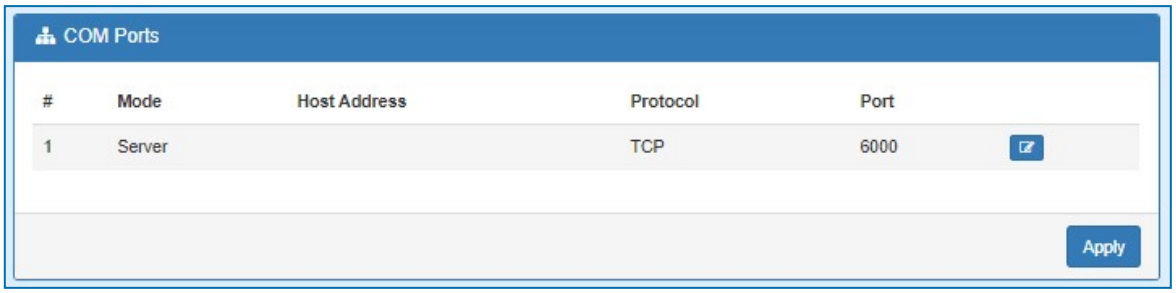
(1) The default is Disable. You can click edit button to configure your settings.



(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.



(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.

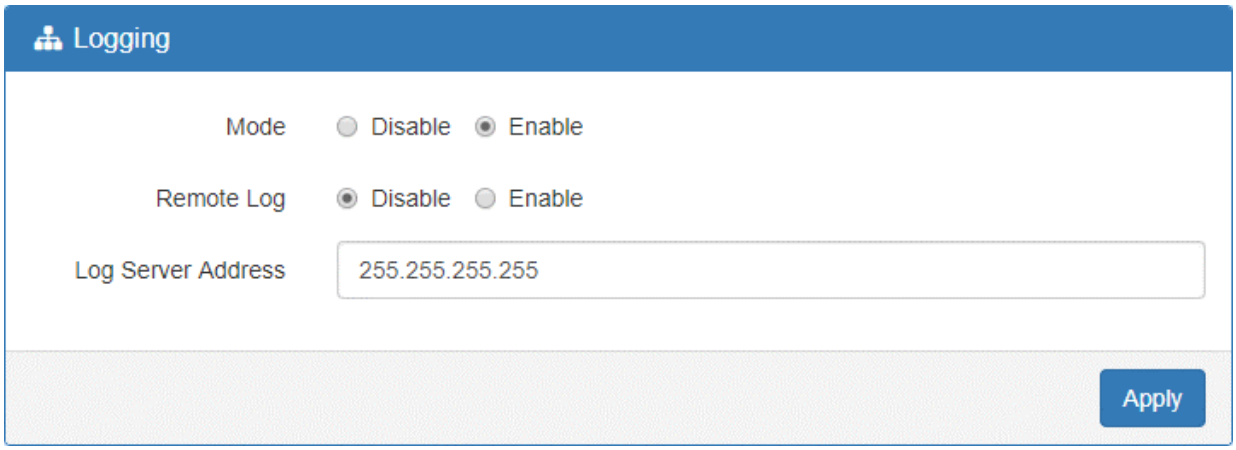
5.3 System > Logging

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

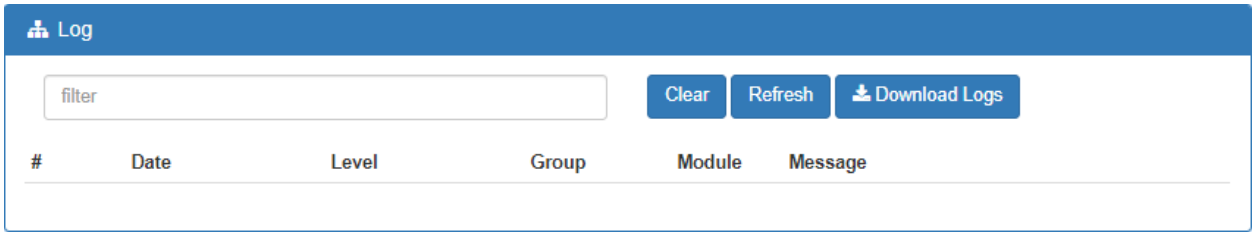
This section displays all data status.

(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.

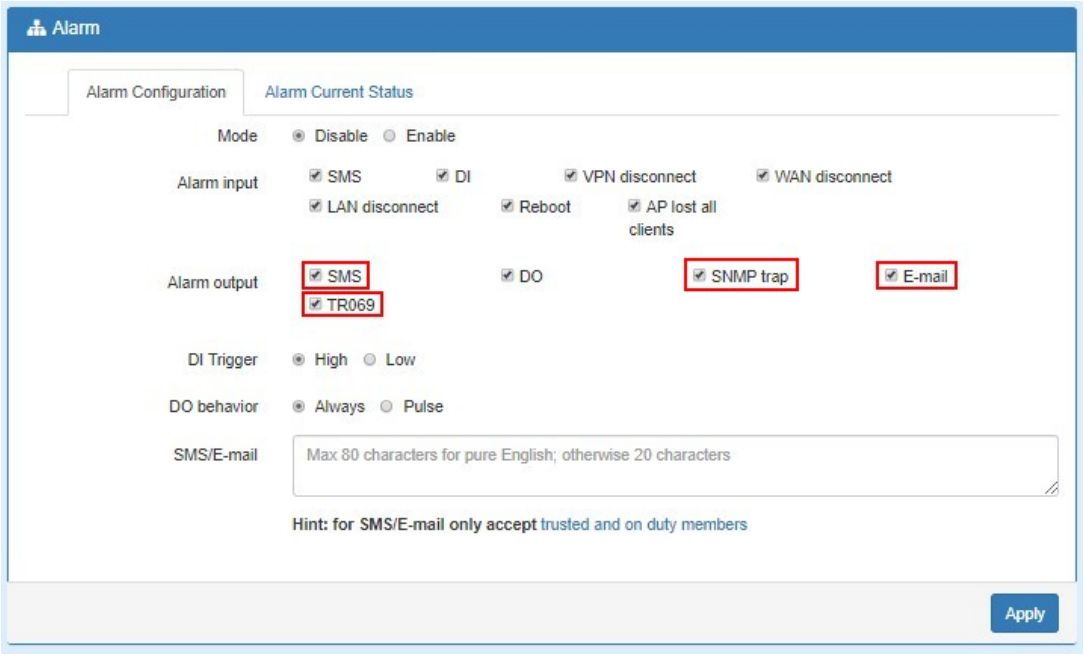
(4) When you click Download Logs, the system will download the latest data from your cellular router.



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 SMS in Alarm input/output, you need to add the trust phone number into Contracts/ On Duty.

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

(3) If you select E-Mail in Alarm output, you need to set up SMTP configuration from Service SMTP.

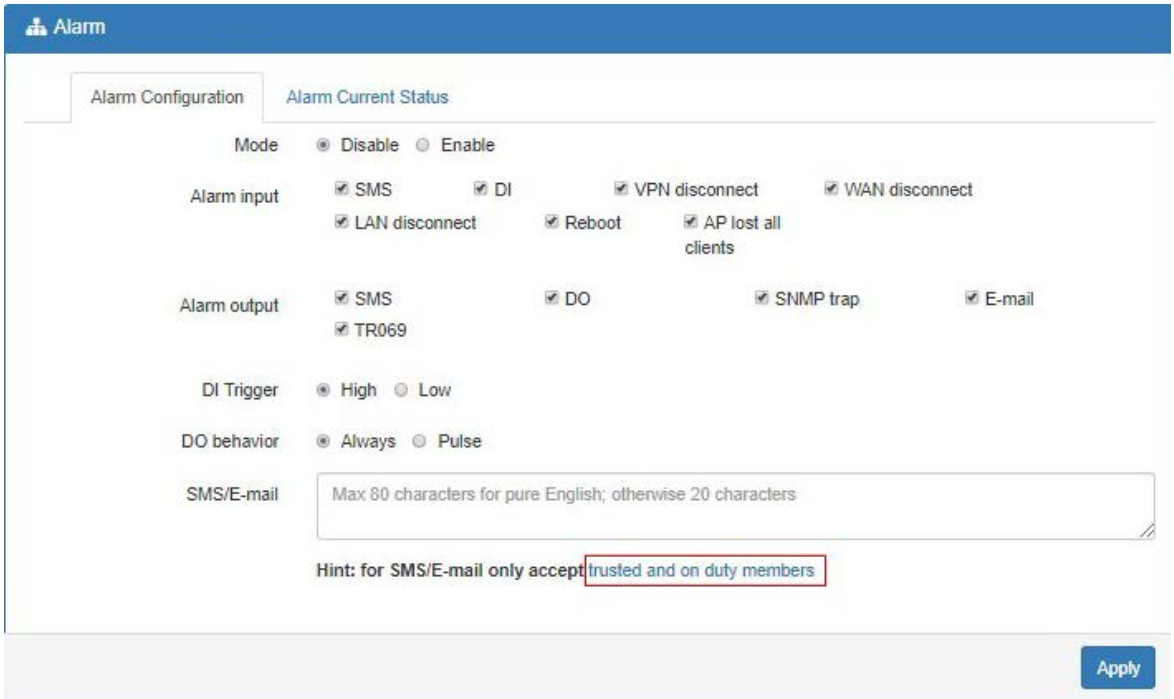
(4) If you select TR069 in Alarm output, you need to set up TR069 configuration from Service TR069.

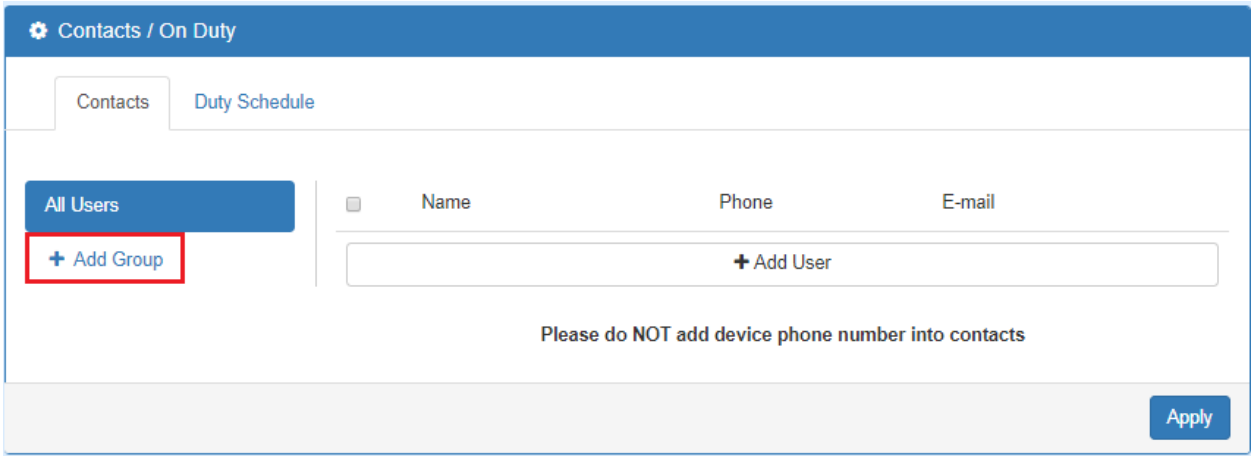
System > Alarm	
Item	**Description**
Mode	Turn on/off the Alarm configuration. Select from Disable or Enable. The default is Enable.
Alarm Input	• **SMS:** It means on duty team members on Contacts / On Duty can send SMS to the phone number of using SIM card to trigger alarm. • **DI:** IO to trigger alarm. • **VPN disconnect:** All tunnels get disconnected then trigger alarm. • **WAN disconnect:** WAN connections get disconnected then trigger alarm. • **LAN disconnect:** LAN connection get disconnected then trigger alarm. • **Reboot:** Reboot then trigger alarm.
Alarm Output	Select from SMS, DO, SNMP trap, E-mail and TR069 as alarm output.
DI Trigger	Select from High or Low. The default is High Trigger.
DO behavior	• **Always:** Pull DO high. • **Pulse:** High and Low continuously. • **Pulse Time Length:** Pulse time length (unit: mini seconds).

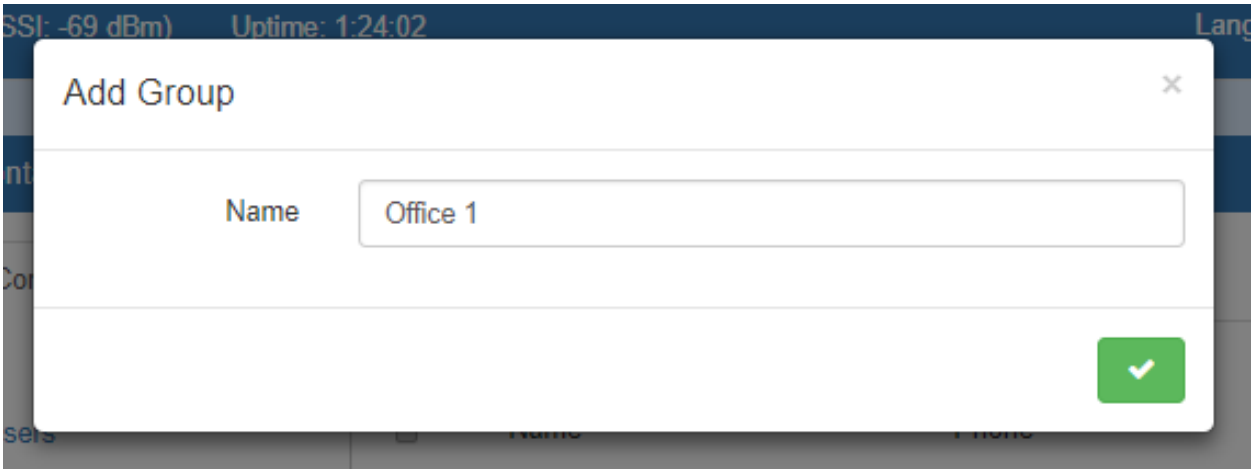
SMS/E-mail	Write your messages and the messages limit 80 pure English characters or 20 characters for other languages to deliver.

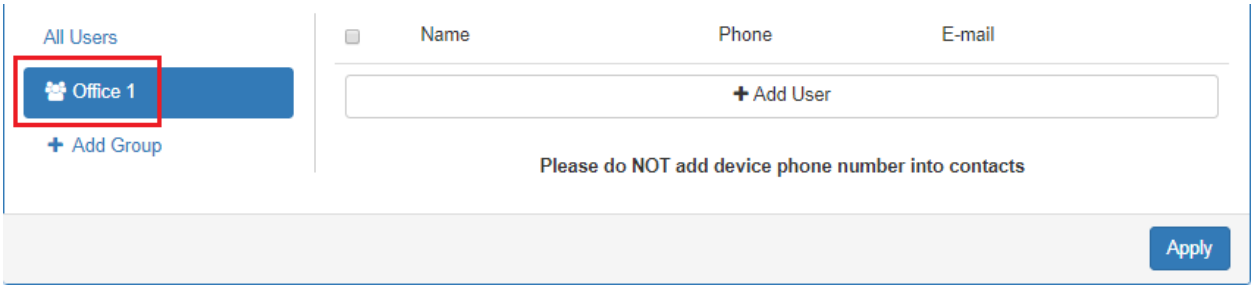
5.4.1 Alarm > Contacts > Create and name the Group

- Click **trusted and on duty members** for naming and the interface will show the group's name in the Group setting as below.

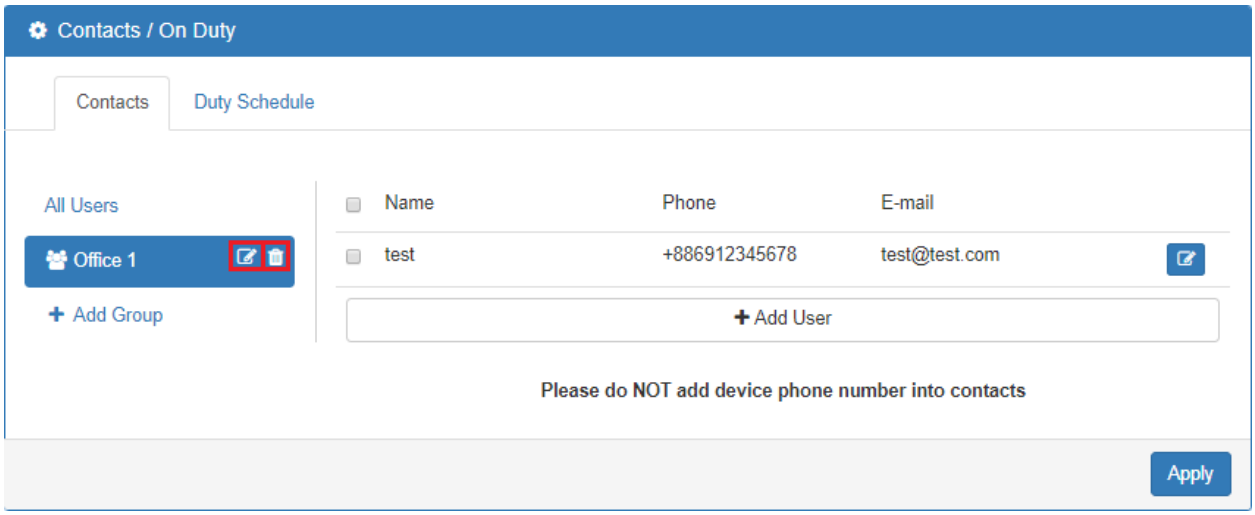






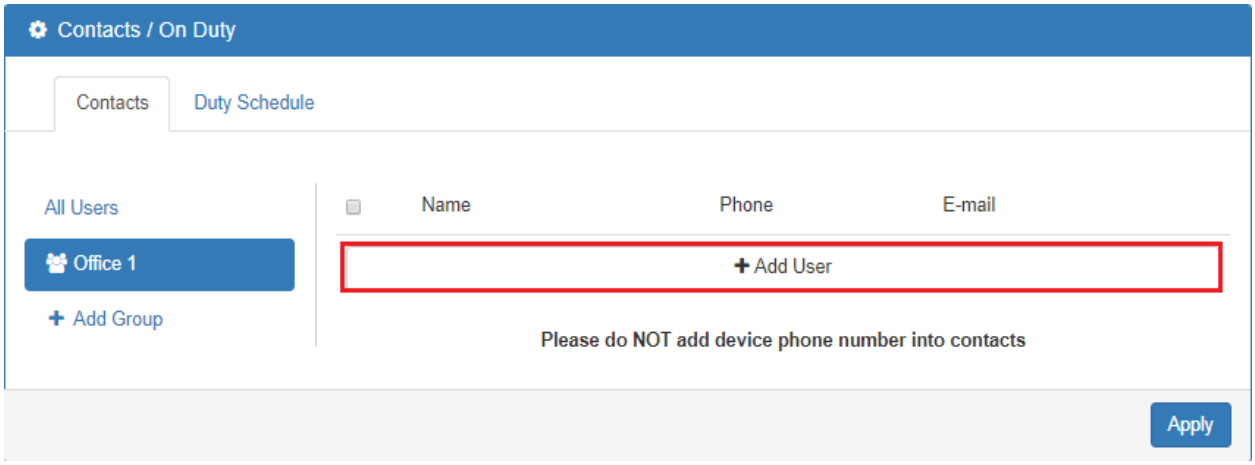


- You can click  or  button to edit or delete the group.

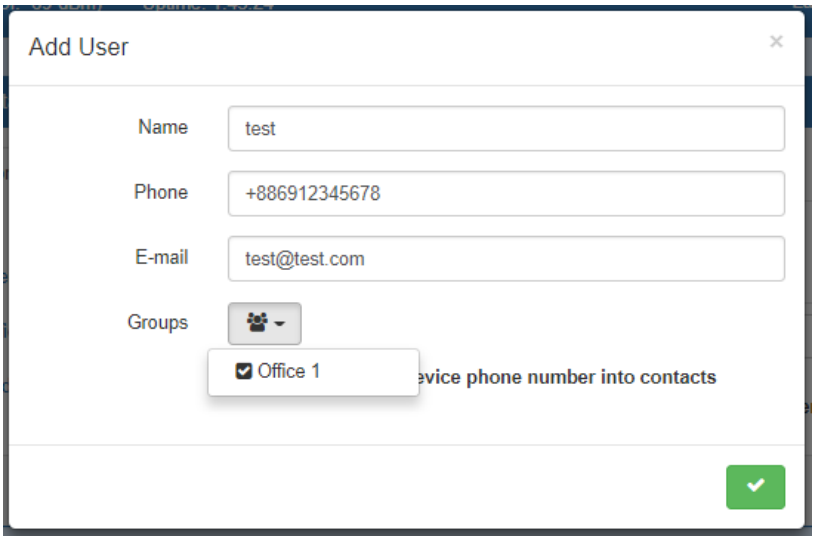


5.4.2 Alarm > Contacts > Add User

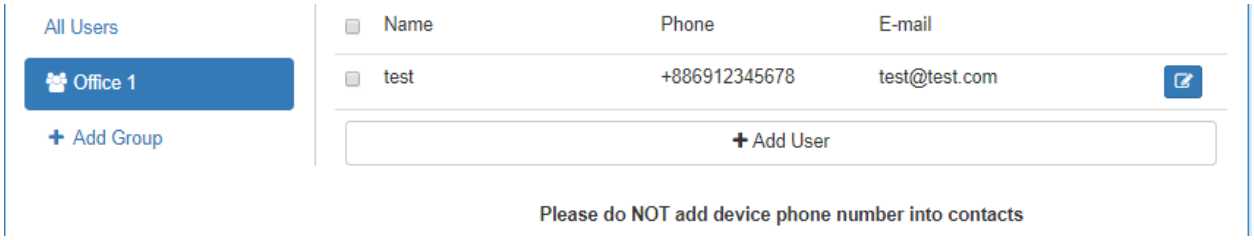
- Select your naming group and click + Add User button to add your user's information, including Name, Phone and E-mail.



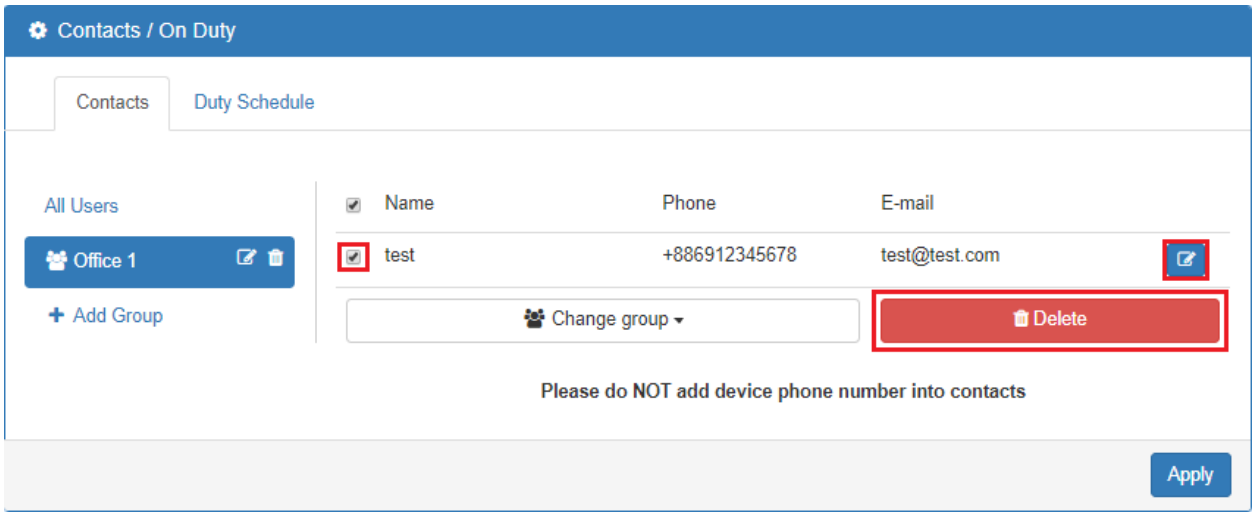
- After filling in your information for each row, chose your naming group and click  to submit your settings.



- After submitting your setting, the interface returns to Group window setting. Now you can see your naming group and the user's information that you have added.

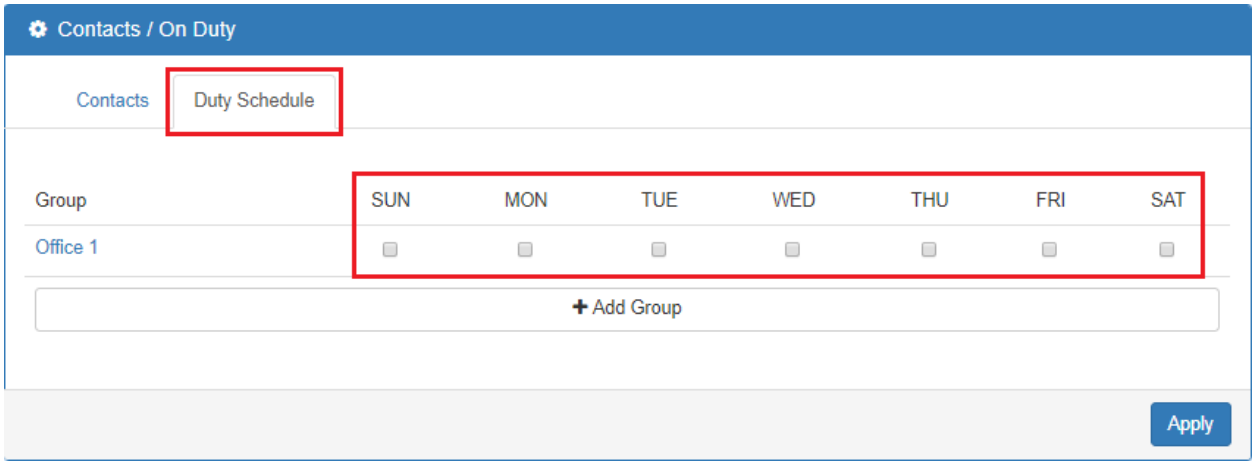


- You can click button to edit the user's information or click the check box and Delete to delete the user.



5.4.3 Alarm > Duty Schedule

- Select Duty Schedule to edit the schedule of the on duty group.

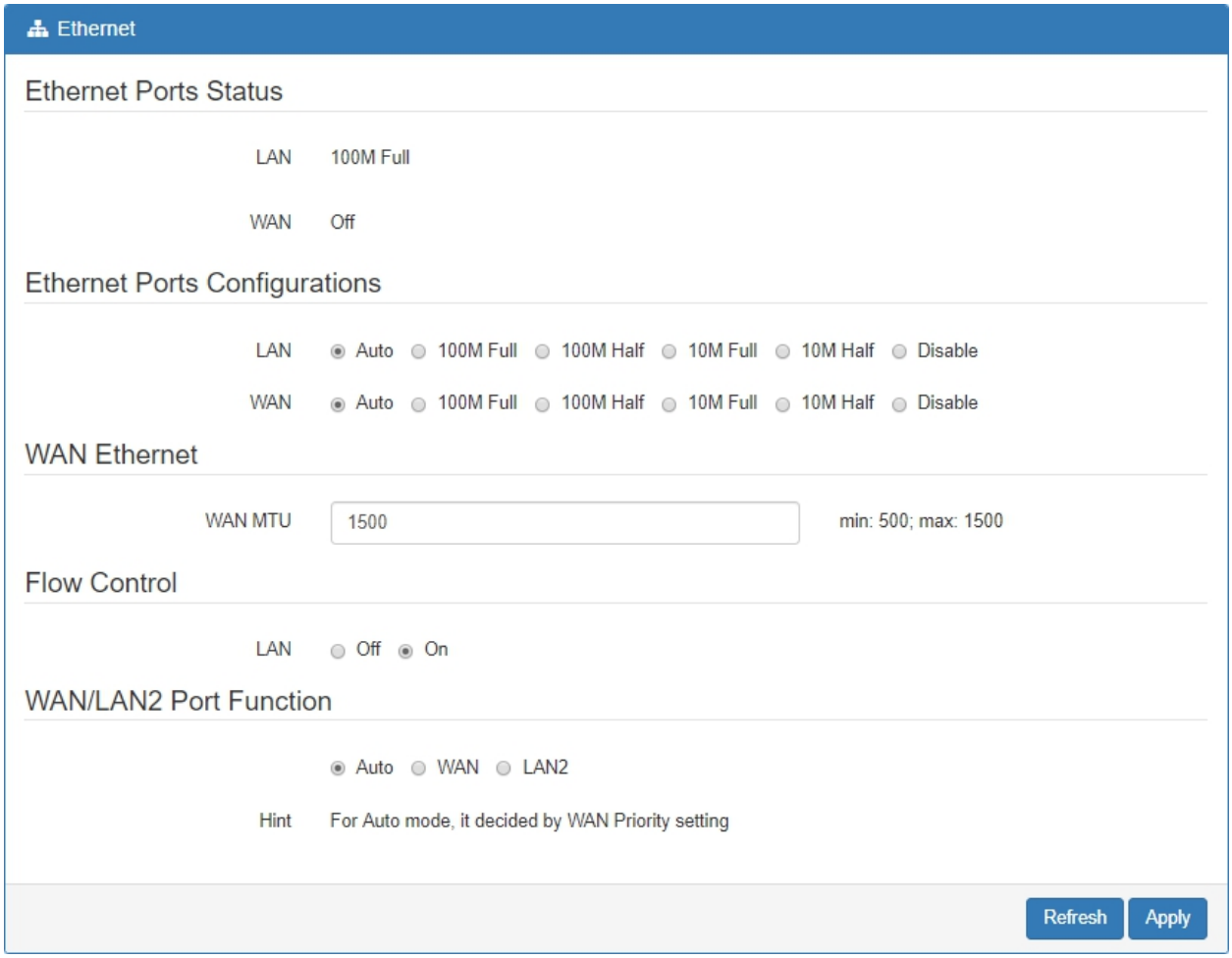


5.5 System > Ethernet Ports

This section allows you to configure the Ethernet.

For Flow Control, it allows you to configure the Ethernet and solve unstable throughput under heavy loading. Sending 64 Bytes with bandwidth 100M bps traffic to LAN and WAN at the same time, the throughput may drop to zero at either side. When the system is very busy or buffer is exhausted, the flow control packet will be sent out to indicate that the link party has stopped to send the packet to system. The flow control packet will be sent out again once the system goes back to normal to indicate the link party that it can send packet again.

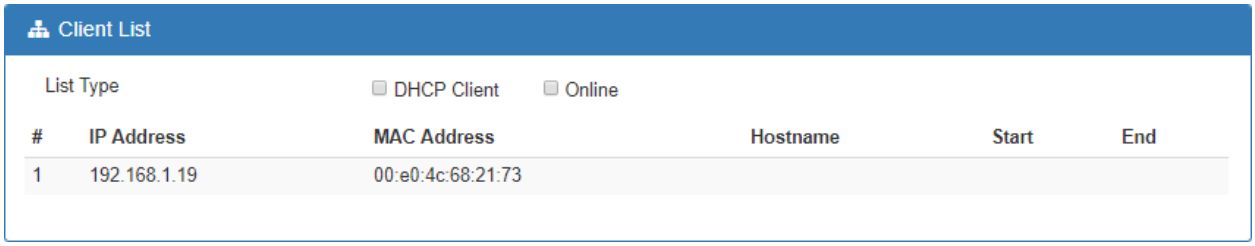
Note: The LAN port of Ethernet has different layout based on which router model you use.



System > Ethernet Ports	
Item	**Description**
Ethernet Ports Status	Show the connectivity status of LAN and WAN.
Ethernet Ports Configurations	Select from Auto, 100M Full, 100M Half, 10M Full, 10M Half and Disable.
WAN Ethernet	MTU is the Maximum Transmission Unit that can be sent over the WAN Ethernet interface. It allows users to adjust the MTU size to fit into their existing network environment.
Flow Control	Allow users to control the traffic ingress from Ethernet LAN or WAN.
WAN/LAN2 Port Function	Allow users to setup the WAN/LAN2 Port function as Auto, LAN, or WAN.

5.6 System > Client List

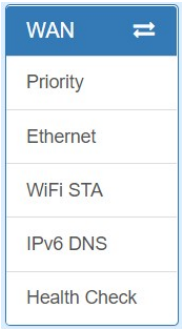
This section allows you to understand how many devices have been connected and their status from the router. There are two types, one is **DHCP Client** and the other is **Online**. The default is both types to show all status when the router is on DHCP Client and Online.



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.

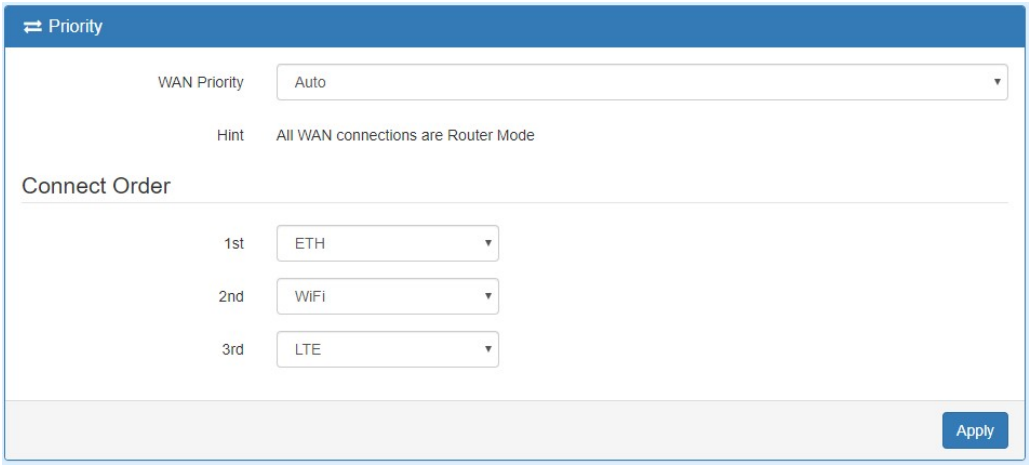
6 Configuration > WAN

This section allows you to configure WAN, including Priority, Ethernet and IPv6 DNS.



6.1 WAN > Priority

You can set up the priority of WAN. The default is Auto.



WAN > Priority	
Item	**Description**
Priority	• **Auto:** Please specify the connection order. • **LTE Only:** Only use LTE connection. • **ETH Only:** Only use WAN Ethernet connection. • **WiFi Only:** Only use WAN WiFi connection.
Connect Order	• **1st:** The first priority of wan interface for connection. • **2nd:** The second priority of wan interface for connection. • **3rd:** The 3rd priority of wan interface for connection.
LTE Net Mode	The priority is **LTE Only**. • **Bridge Only:** APN1 acts as bridge for internet access. • **Router Only:** APN1 acts as router for internet access.
WiFi Mode	The priority is **WiFi Only**. • **Bridge Only:** WiFi station acts as bridge for internet access. • **Router Only:** WiFi station acts as router for internet access.

6.2 WAN > Ethernet

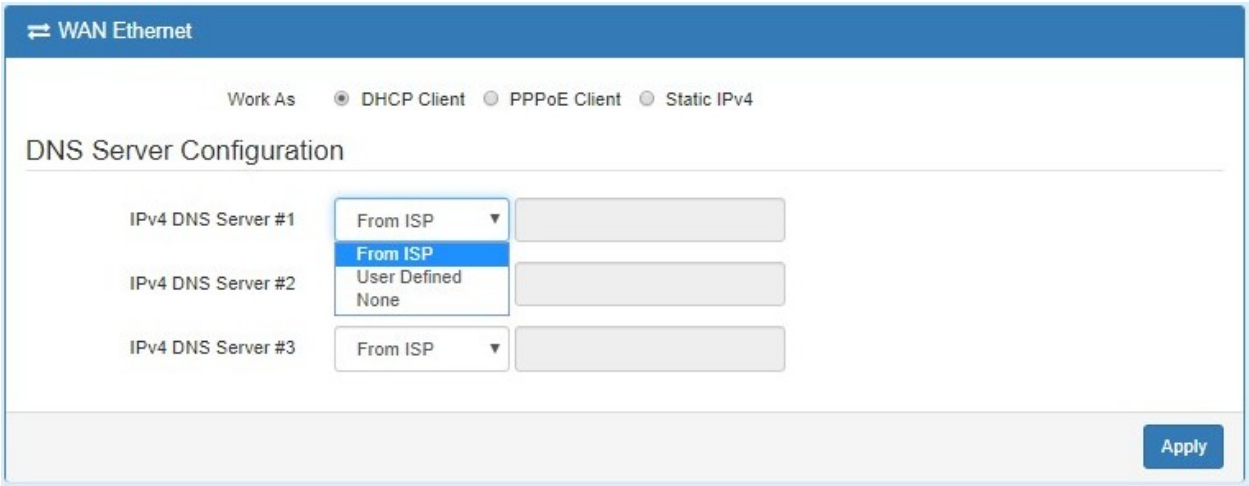
6.2.1 WAN Ethernet Configuration

This section provides three options to obtain the IP of WAN Ethernet. The options include **DHCP Client**, **PPPoE Client** and **Static IPv4.** The default is DHCP Client.

WAN > Ethernet	
Item	**Description**
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.

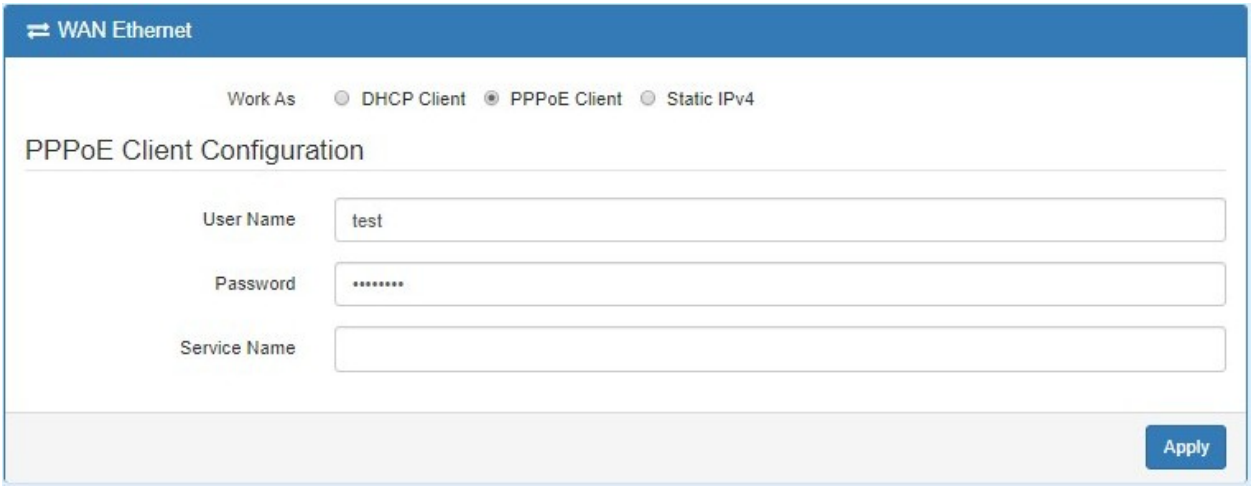
When selecting "**DHCP Client"**, you can set up DNS Server Configuration.

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.

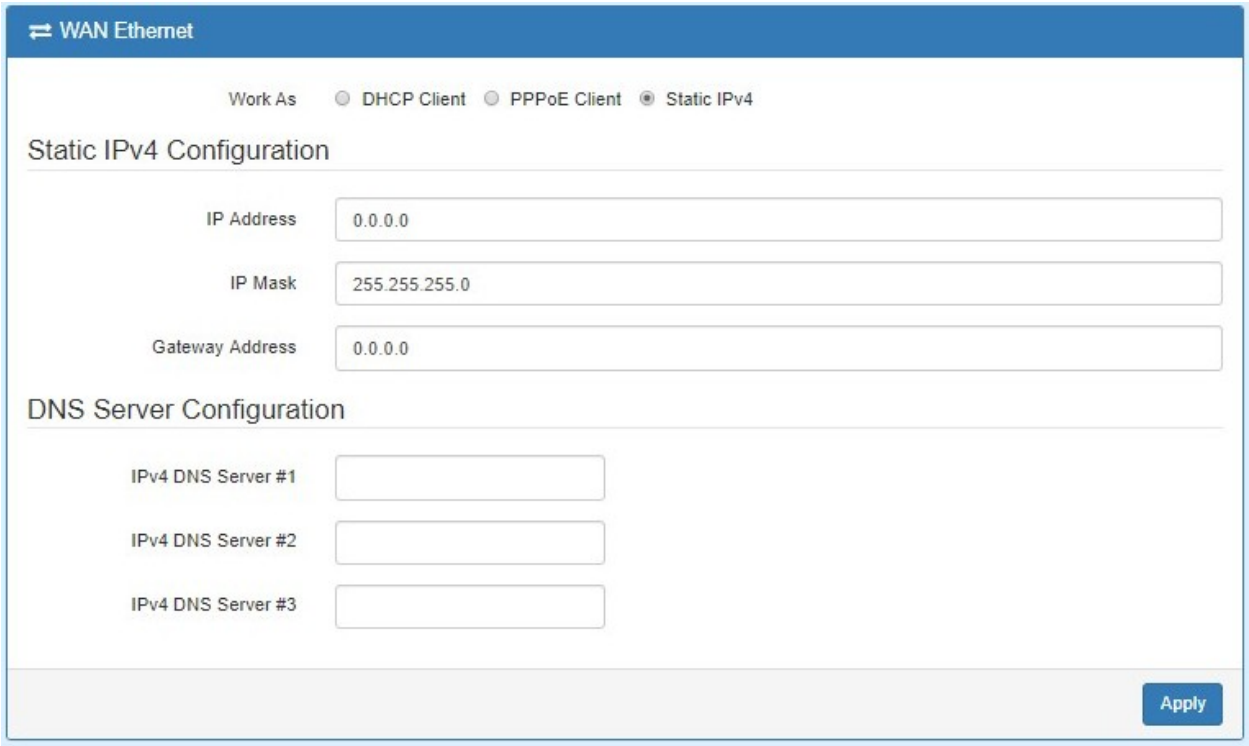


WAN > Ethernet > DHCP Client	
Item	**Description**
IPv4 DNS Server #1 **IPv4 DNS Server #2** **IPv4 DNS Server #3**	● Each setting DNS Server has three options, including From ISP, User Defined and None. ● When you select From ISP, the IPv4 DNS server IP is obtained from ISP. ● When you select User Defined,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



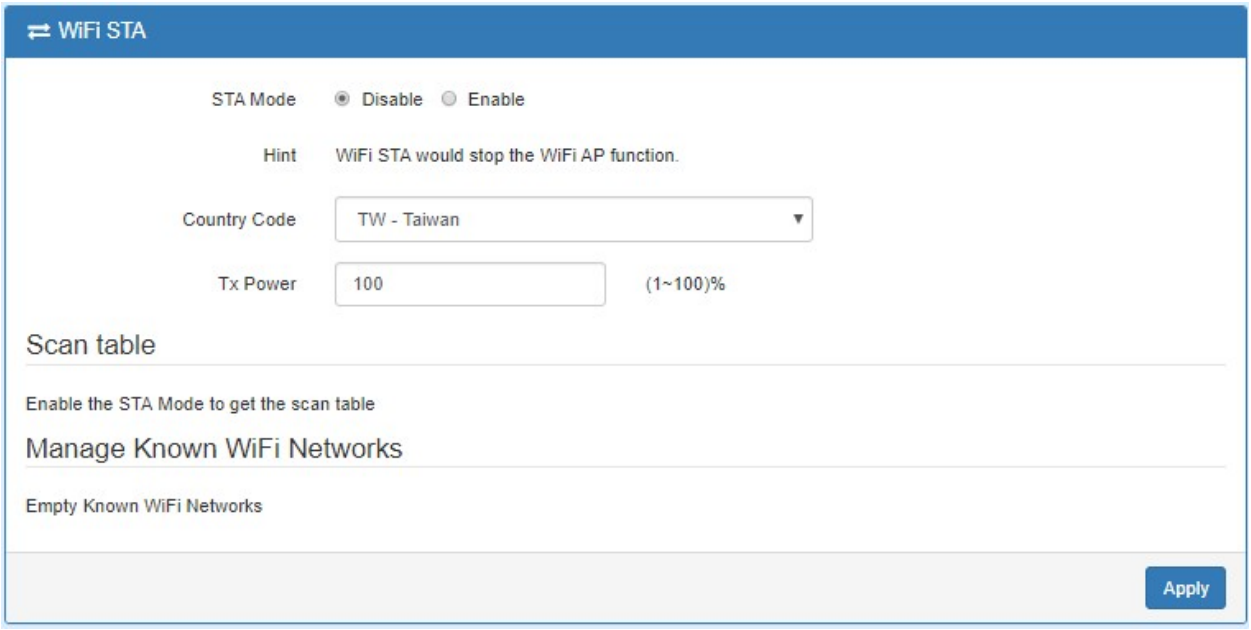
When you select **Static IPv4**, the interface shows the information of configuration, including IP Address, IP Mask and Gateway Address.



WAN > Ethernet > Static IPv4	
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.

6.3 WAN > WiFi STA

Station (STA) mode is used to connect to a Wi-Fi network established by an access point.



WAN > WiFi STA	
Item	**Description**
STA Mode	Disable or Enable this feature.
Tx Power	The TX power setting specifies the strength of the signal.
Scan Table	
Scan	List AP information that can be scanned.
Connect	Connect to your chosen Wireless Access Point.
Manage Known WiFi Networks	
Connect	Connect to your chosen Wireless Access Point.
Delete	Delete your choice of Wireless Access Point.

6.4 WAN > IPv6 DNS

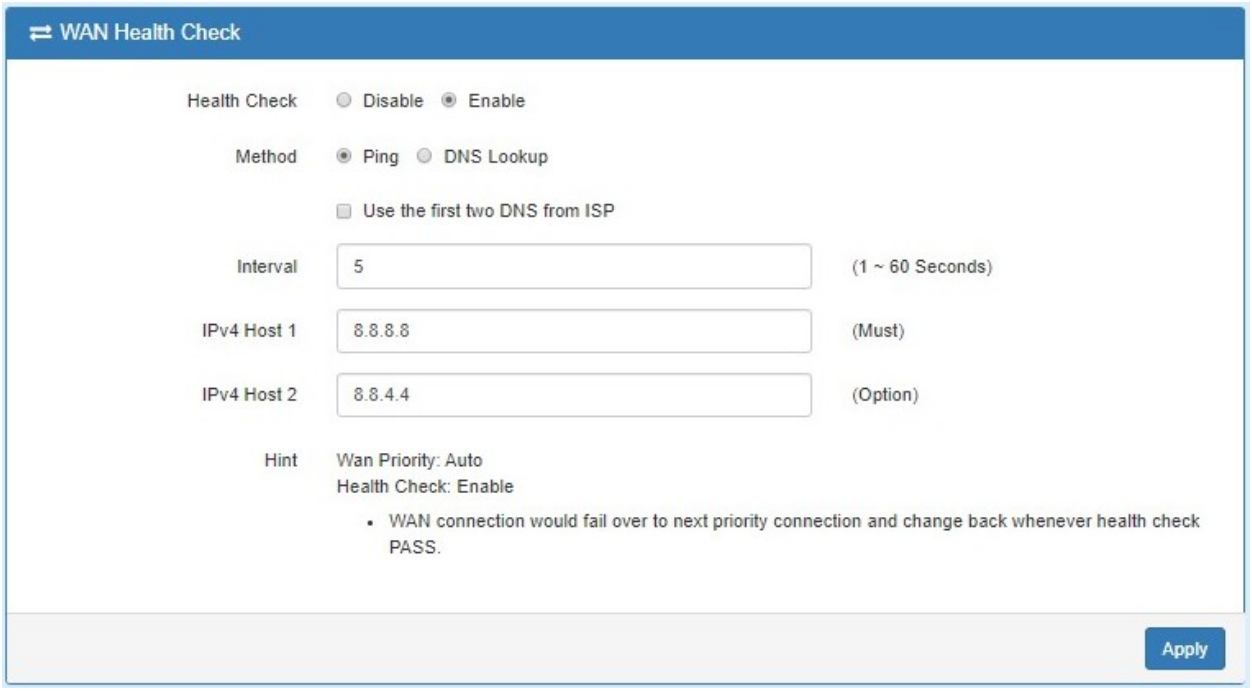
This section allows you to set up IPv6 DNS Server Configuration.

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.

6.5 Health Check

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 WAN **“Health Check**” and the system would switch to LTE connection and switch back whenever Ethernet is able to access internet again.



WAN > Health Check	
Item	**Description**
Health Check	● Select from Disable or Enable. The default is Enable. ● When Disable is chosen, the connection will NOT be treated as down of IP routing error.
Method	This setting specifies the health check method for the WAN connection. This Value can be PING, DNS Lookup. The default is Ping. DNS Lookup: Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result.
Use the first two DNS from ISP	● If this setting is checked, the first two DNS from ISP will be DNS lookup targets for checking a connection health. ● If this setting is not checked, Host 1 must be filled, while a value for Host 2 is optional.
Interval	The interval is from 1 to 60 seconds.
IPv4 Host 1	Input the address of IPv4 Host 1. Host1 must be filled.
IPv4 Host 2	Input the address of IPv4 Host 2. Host2 is optional.
LTE Keep Alive	Enable LTE Keep Alive to continue to send health check packages to avoid no network traffic cause operation kick out the connection.
LTE Keep Interval	LTE Keep Alive interval is from 1 to 60 seconds.
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.

WAN LTE

Attr.	Value
SIM Status	Ready
Operator	Chunghwa Telecom
Modem Access	FDD LTE
IMSI	466924202684767
Phone Number	
Band	LTE BAND 3
EARFCN	1750
PLMN	46692
Roaming	No
Uplink Speed Kbps	0.000
Downlink Speed Kbps	0.000
Tx/Rx KBytes	35.000/31.000
Tx/Rx Dropped Packets	0/0
LTE Net Mode	Router Only

✔ WAN Ethernet

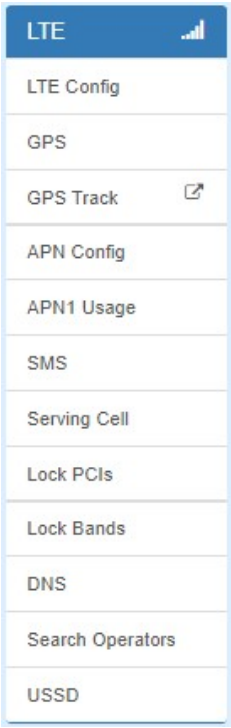
Attr.	Value
IPv4 Address	192.168.0.164
IPv4 Mask	255.255.255.0
Default Gateway	192.168.0.250
IPv4 Conn Time	15:59

LAN Ethernet

Attr.	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	2001:b400:e331:614c::1
IPv6 Conn Time	15:50
Uplink Speed Kbps	0.000
Downlink Speed Kbps	0.000
Tx/Rx KBytes	262.000/0.000
Tx/Rx Dropped Packets	0/0

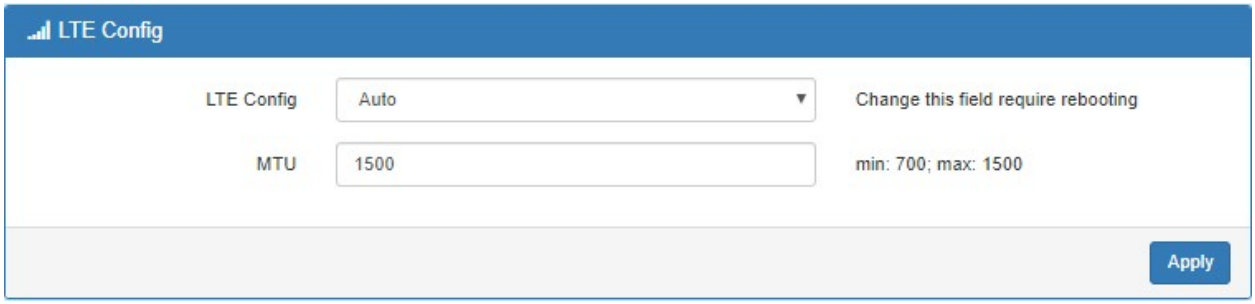
7 Configuration > LTE

This section allows you to configure LTE Config, GPS, GPS Track, APN Config, APN1 Usage, SMS, Serving Cell, Lock PCIs, Lock Bands, DNS, Search Operators, and USSD.



7.1 LTE > LTE Config

You can set up the LTE Configuration.



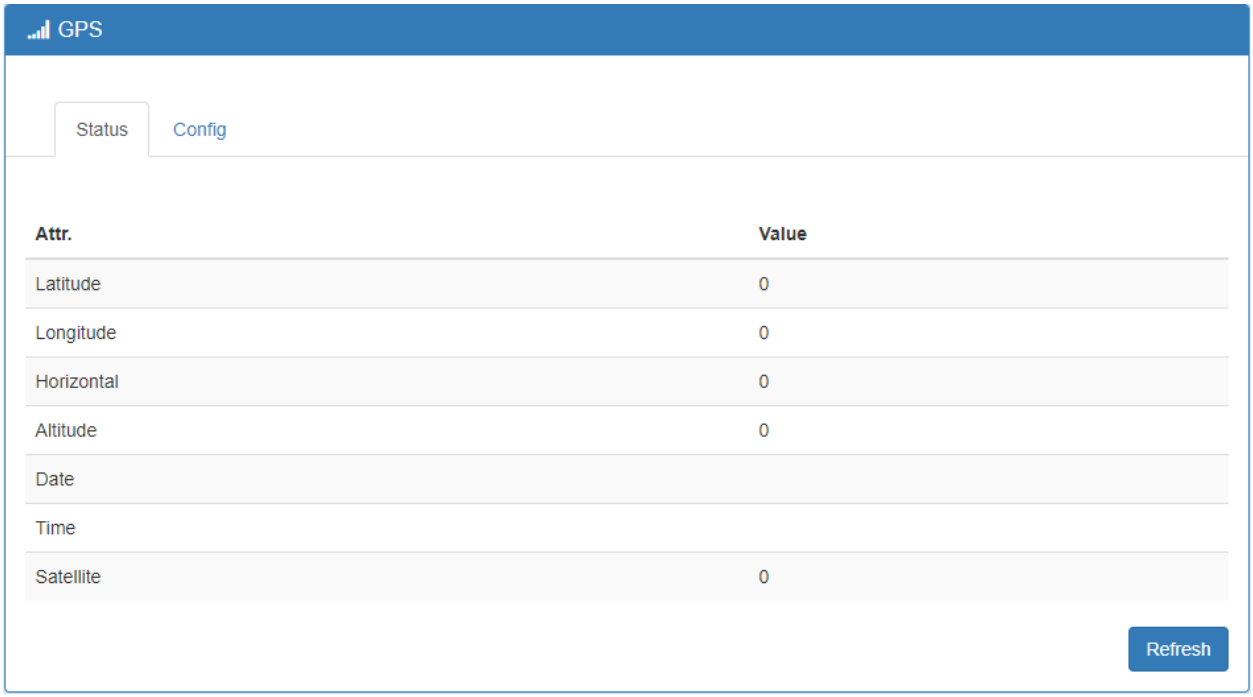
LTE > LTE Config	
Item	**Description**
LTE Config	• **Auto:** Automatically connect the possible band. • **4G Only:** Connect to 4G network only. • **3G Only:** Connect to 3G network only. • **2G Only:** Connect to 2G network only.
MTU	MTU is the Maximum Transmission Unit that can be sent over the LTE interface. It allows user to adjust the MTU size to fit into their existing network environment.

7.2 LTE > GPS

This section allows you to get GPS status and set the GPS configuration to report the location.

7.2.1 Status

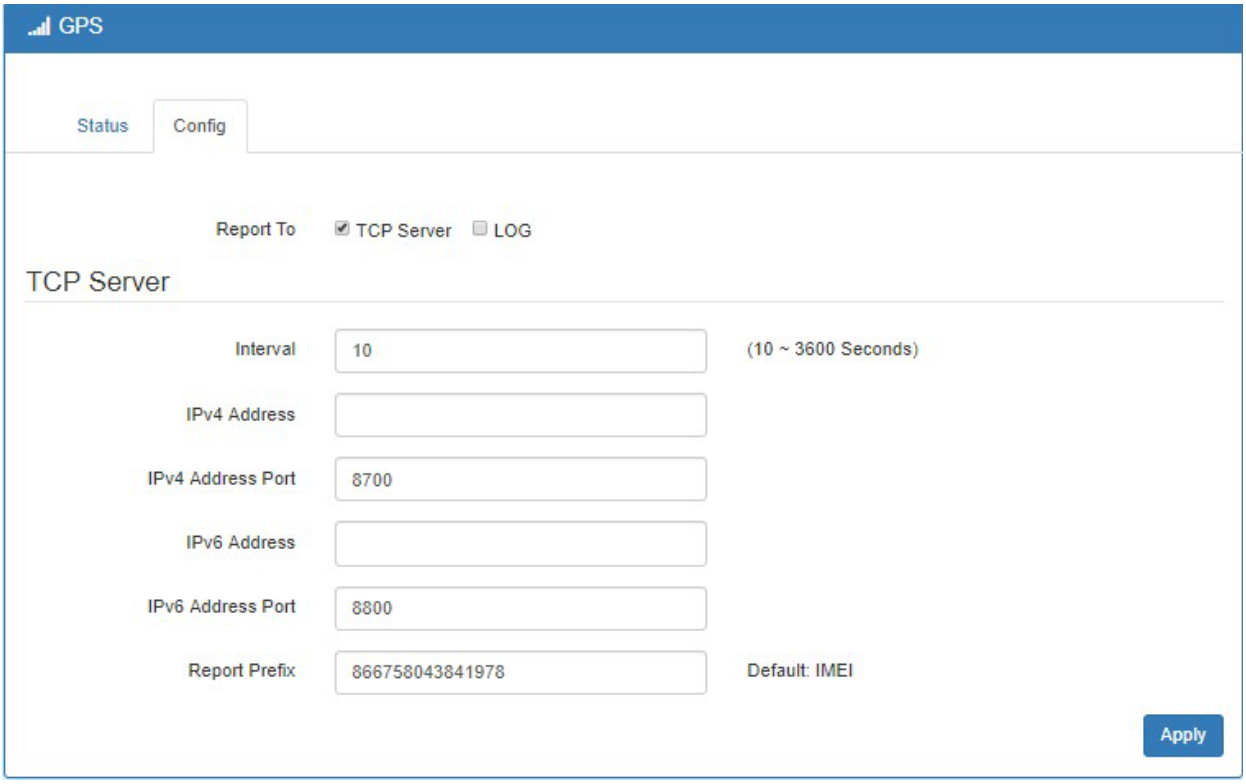
In the status tab, it shows the current device location.



LTE > GPS > Status	
Item	**Description**
Latitude	Latitude
Longitude	Longitude
Horizontal	Horizontal precision:0.5-99.9
Altitude	The altitude of antenna away from the sea level(unit: m), accurate to one decimal place
Date	UTC date when fixing position
Time	UTC time when fixing position
Satellite	Number of satellites

7.2.2 Config

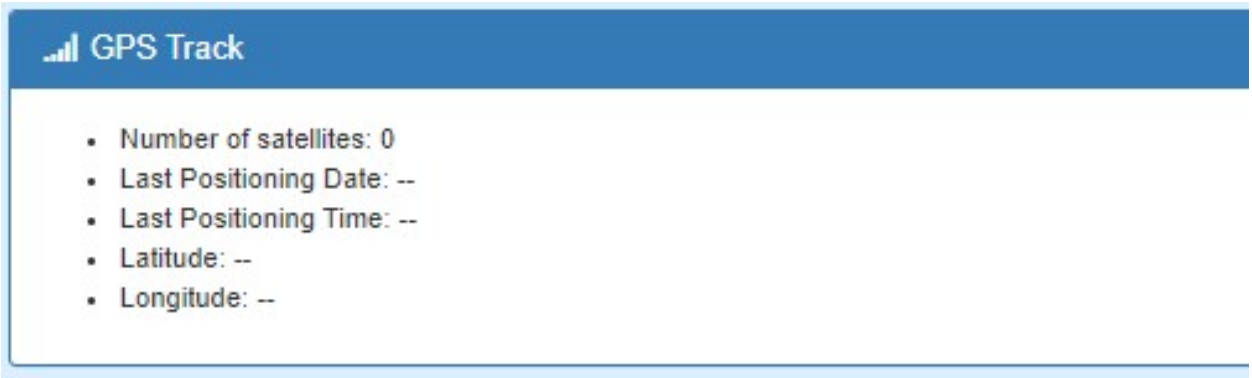
This section allows you to set up GPS configuration and send out GPS location to TCP Server or display in log.



LTE > GPS > Config	
Item	**Description**
Report to	Select from TCP Server and LOG.
Internal	Query GPS interval.
IPv4 Address	GPS IPv4 TCP Server Address.
IPv4 Address Port	GPS IPv4 TCP Server Port.
IPv6 Address	GPS IPv6 TCP Server Address.
IPv6 Address Port	GPS IPv6 TCP Server Port.
Report Prefix	Identification for GPS Track.

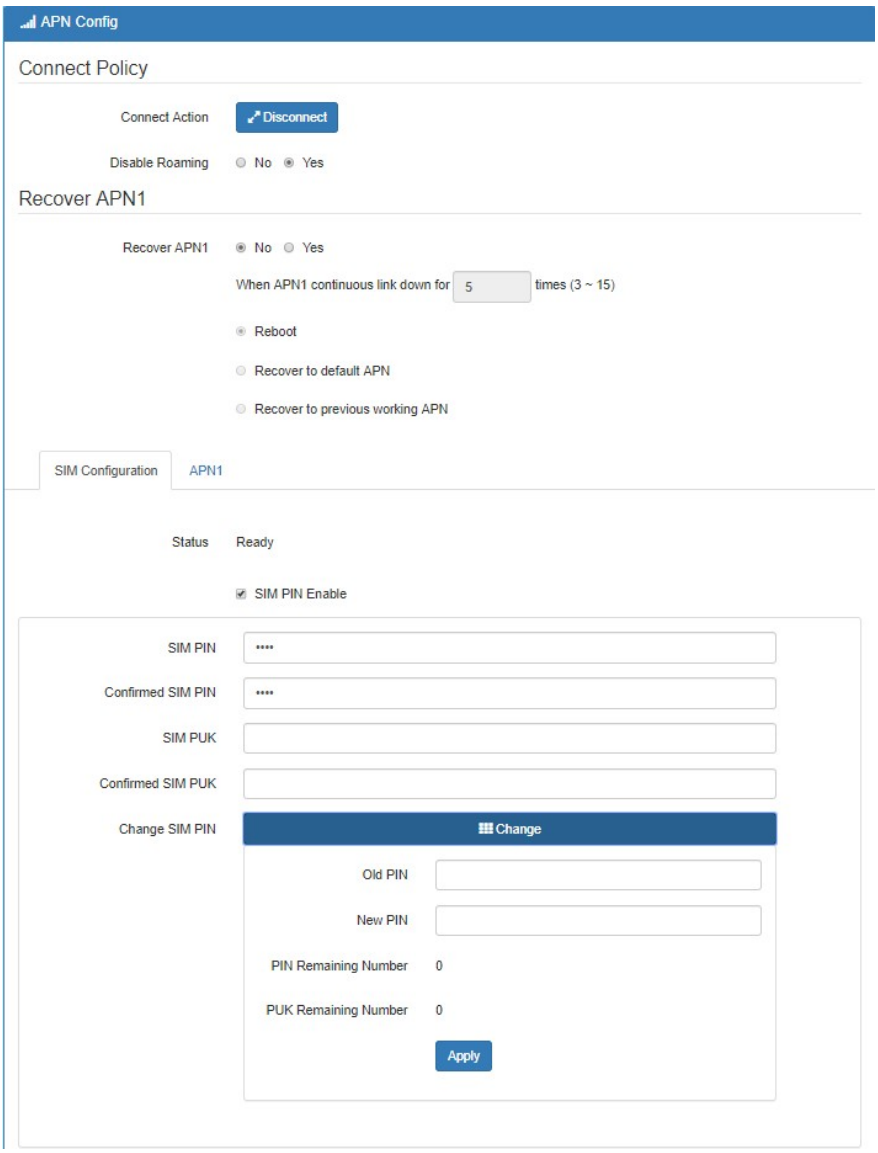
7.3 LTE > GPS Track

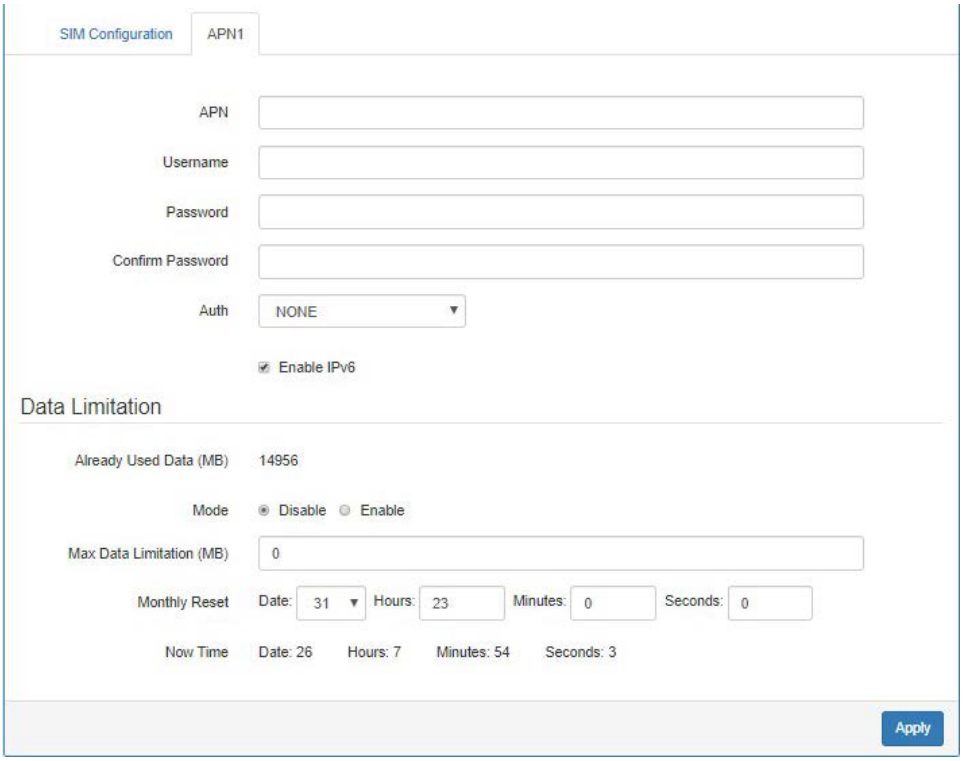
This section allows you to see the GPS Track.



7.4 LTE > APN Config

This section allows you to set APN Configuration. It includes Connect Policy, Recover APN1, SIM Configuration, APN1 and Data Limitation.



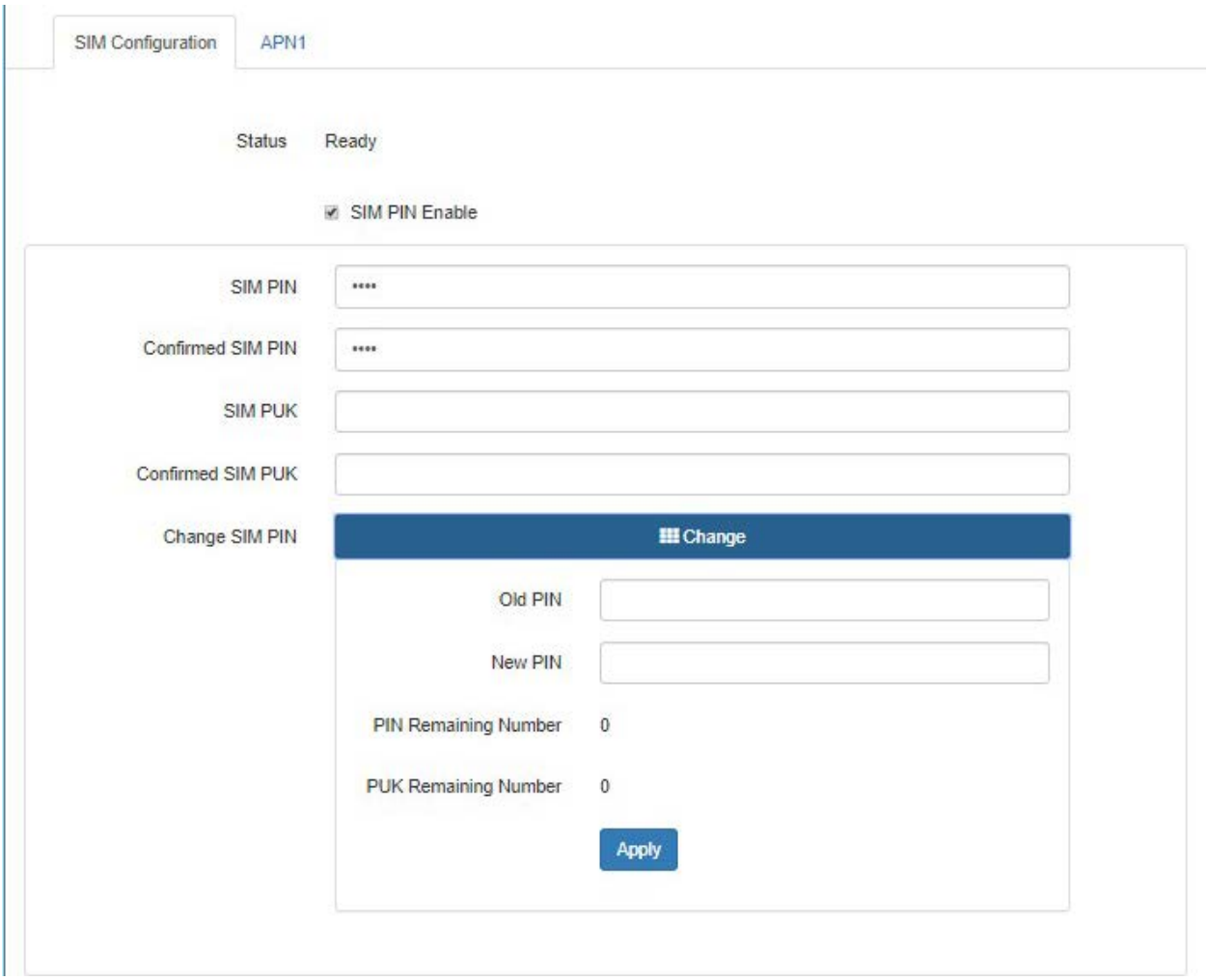


LTE > APN Config	
Item	**Description**
Connect Policy	
Connect Action	• **Disconnect:** When getting connection, the Disconnect button appear. After manually click Disconnect, the system would not automatically get connection until next reboot. • **Connect:** After manually disconnect, it will show Connect button. Click to get connection or reboot the device to make it automatically connect.
Disable Roaming	• **No:** Make connection even the device is in roaming state. • **Yes:** No connection when the device in roaming state.
Recover APN1	
Recover APN1	• **No:** Not to recover when APN1 is continuous link down. • **Yes:** Recover APN1 by using specified method.
When APN1 continuous link down for xx times.	When link down number reach the specified number then the system will proceed recover action. • **Reboot:** Reboot the system. • **Recover to default APN:** Replace active APN by using factory default APN. • **Recover to previous working APN:** Replace active APN by using previous working APN.
SIM Configurations	
Status	Display the status of SIM Card.
SIM PIN Enable	• Enable to display SIM PIN setting. • Disable to hide SIM PIN setting.
SIM PIN	A password personal identification number (PIN) for ordinary use to

	protect your SIM card.
Confirmed SIM PIN	Double confirm SIM PIN password.
SIM PUK	If user input the wrong SIM PIN more than 3 times, the user needs another password personal unblocking code (PUK) for PIN unlocking. Please check your operator for forgotten PUK number.
Confirmed SIM PUK	Double confirm SIM PUK.
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).
Old PIN	Please input the current SIM PIN code.
New PIN	Please input the newly update SIM PIN.
PIN remaining number	Display the allowed remaining PIN retry number.
PUK remaining number	Display the allowed remaining PUK retry number.
APN1	
APN	The Access Point Name (APN) is the name of the setting that set up a connection to the gateway between your carrier's cellular network and the public Internet. Leaving it empty will search internally database automatically by SIM card for connection.
Username	Username for authentication. The username can be input by user or the system will search from internal database if the APN setting is empty.
Password	Password for authentication. The password can be input by user or the system will search from internal database if the APN setting is empty.
Confirm Password	Double confirm password.
Auth: (None/PAP/CHAP)	If Auth mode is not None, most servers require username and password above.
Enable IPv6	If IPv6 is not selected, then only pure IPv4 connection.
Data Limitation	
Mode	Turn on/off the Data Limitation to disable or enable.
Already Used Data (MB)	Display current used Data since last reset.
Max Data Limitation (MB)	Configure maximum Data Limitation.
Monthly Reset	Set up the reset time during the month.
Now Time	Show the current time of system.

7.4.1 SIM Configuration

- **SIM PIN:** If you have configured SIM PIN code into SIM card, please type SIM PIN code in Dual SIM configuration to make unlock successfully.
- **SIM PUK:** If you have 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.
- **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).



7.5 LTE > APN1 Usage

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:

It displays accumulated real-time Download/Upload/Total MB for 10 seconds period.

(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	0	0	0
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	129	34	163
8	0	0	0

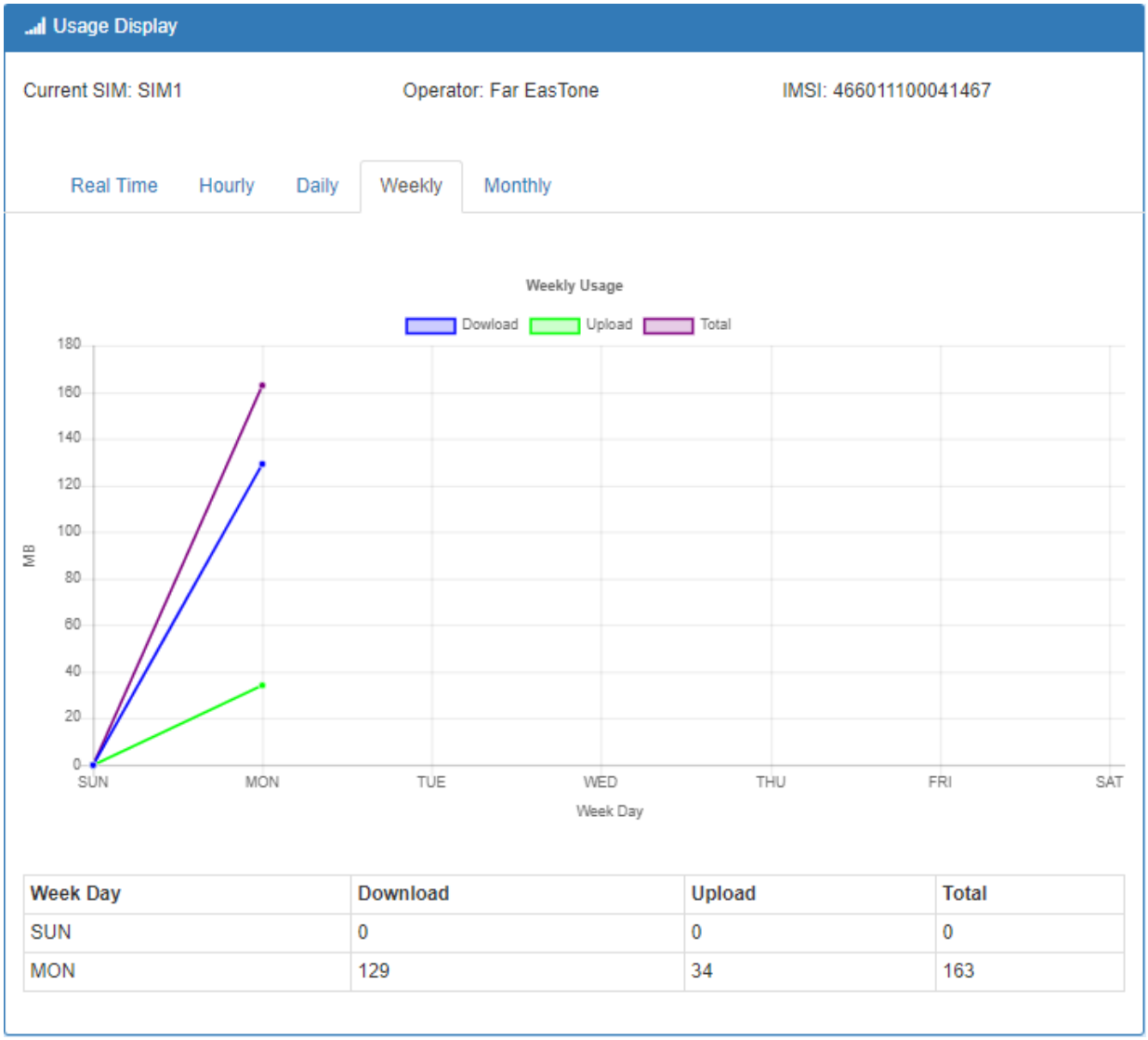
(3) Daily Usage:

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
7	0	0	0
8	0	0	0
9	0	0	0
10	0	0	0
11	129	34	163

(4) Weekly Usage:

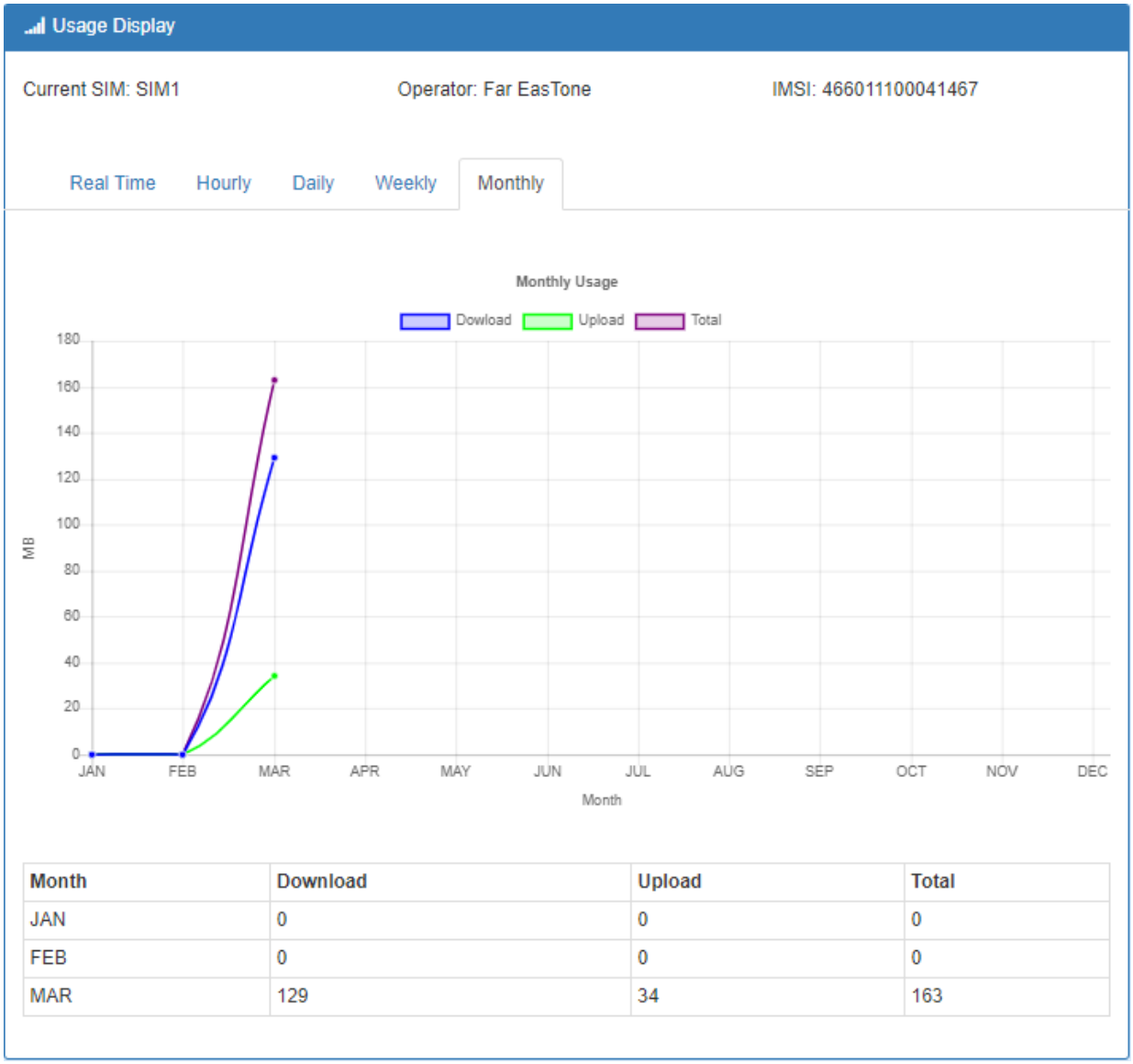
It displays Download/Upload/Total MB per day in one week for current using SIM card and the view window size is 7 days.



Week Day	Download	Upload	Total
SUN	0	0	0
MON	129	34	163

(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.

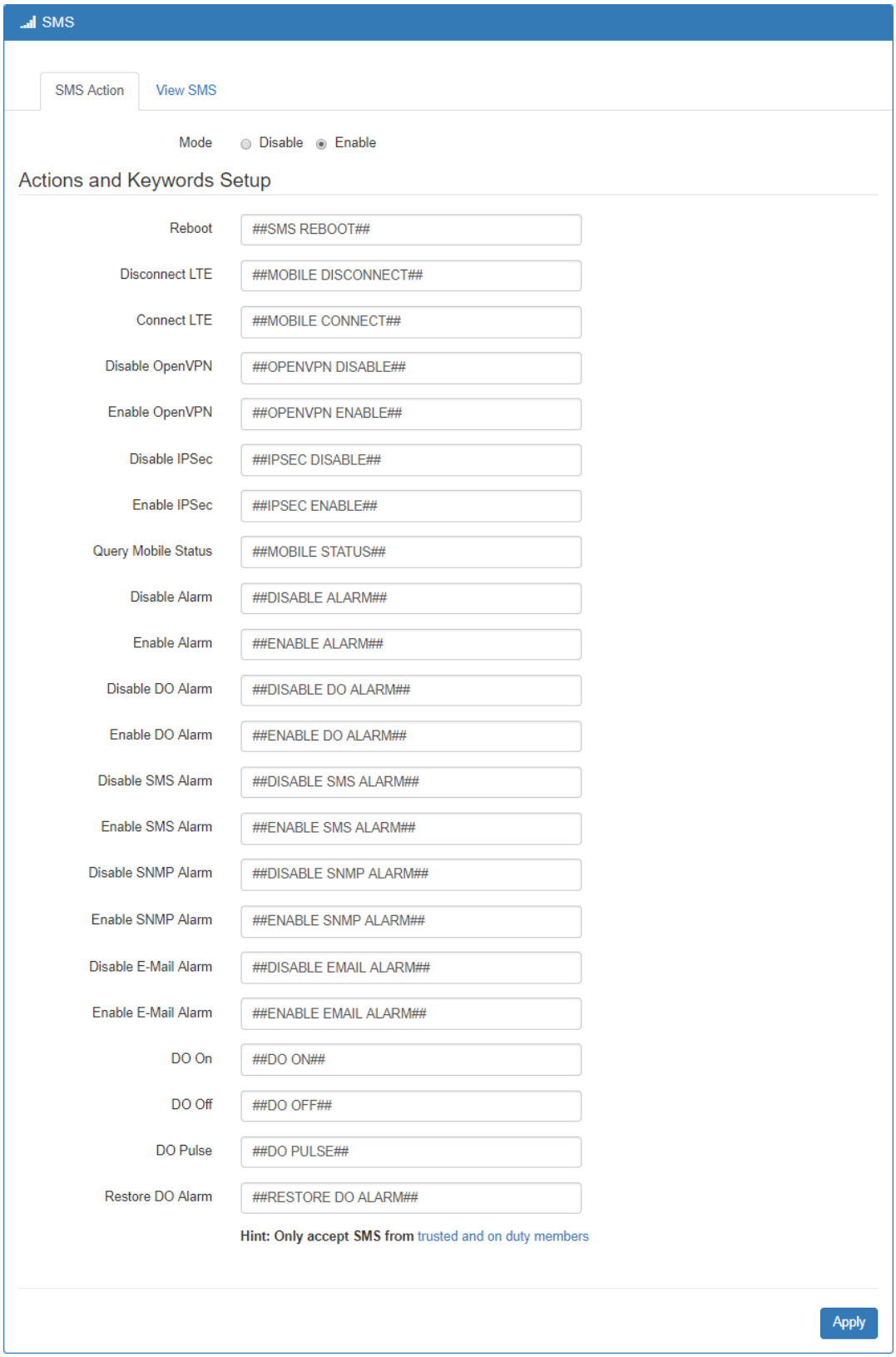


Month	Download	Upload	Total
JAN	0	0	0
FEB	0	0	0
MAR	129	34	163

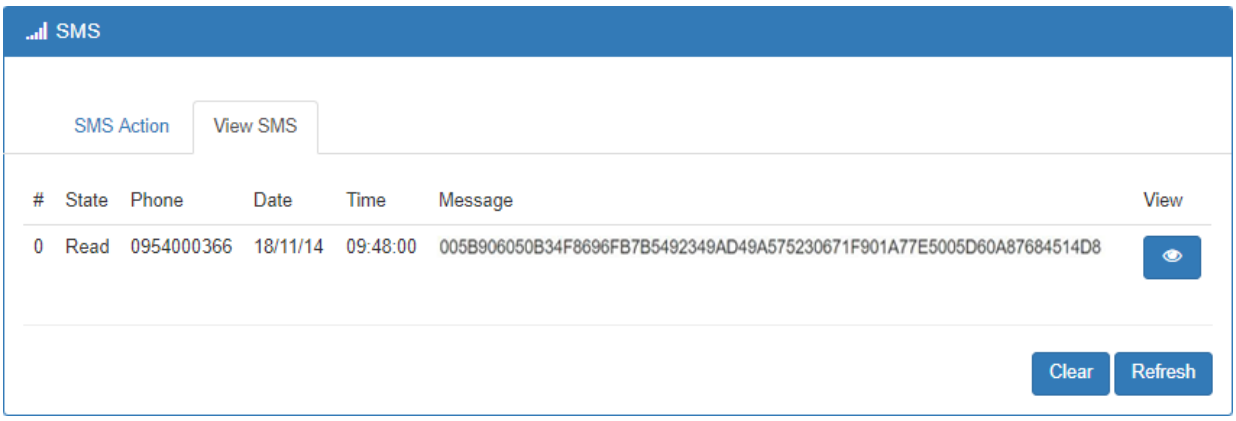
7.6 LTE > SMS

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

(1) When enabling **SMS Action**, it allows trust phone number which in **trusted and on duty members** list by sending key words SMS to trigger device setting/action/query status.



(2) **View SMS** 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, Clear **button** to clear all messages, and Refresh **button** to reload all messages.



7.7 LTE > Serving Cell

This section displays all parameters, including the following items:

Serving Cell

Attr.	Value
Rate	LTE
RSRP	-84
RSRQ	-10
SINR	7
RSCP	
ECIO	0
Cell Identity	318565-31
eNB ID	318565
Cell ID	31
PCI ID	95
EARFCN	3650
UL Bandwidth	10MHz
DL Bandwidth	10MHz
RSSI	-57 dBm
State	NOCONN
Band	LTE BAND 8

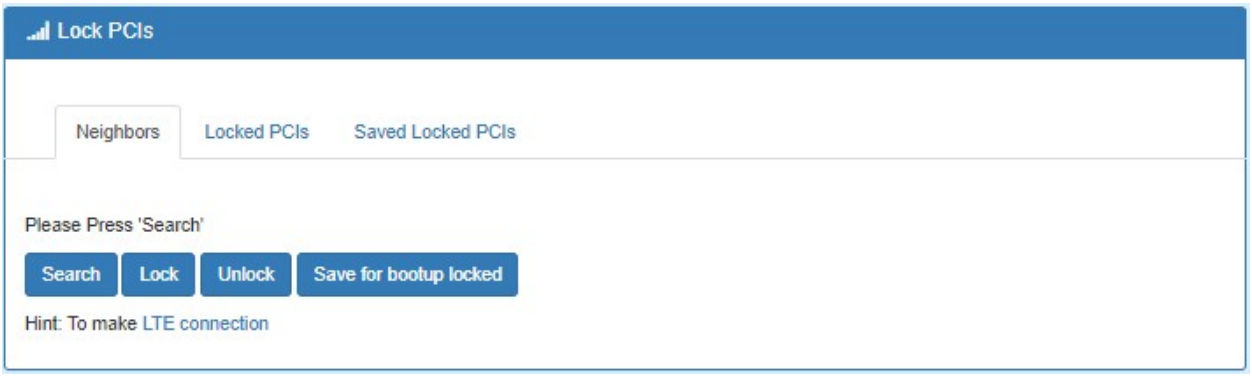
Refresh

LTE > Serving Cell	
Item	**Description**
RSRP	Reference Signal Received Power.
RSRQ	Reference Signal Received Quality.
SINR	The value of SINR (Signal to Interference plus Noise Ratio).
RSCP	The Received Signal Code Power Level of the cell that was scanned.
ECIO	Carrier to noise ratio in dB = measured Ec/Io value in dB.
Cell Identity	eNB ID (20 Bits) + Cell ID (8 Bits).
eNB ID	eNB ID.
Cell ID	Cell ID.
PCI ID	Physical Cell ID.
EARFCN	The E-UTRA-ARFCN of the cell that was scanned.
UL Bandwidth	Up Link Bandwidth.
DL Bandwidth	Down Link Bandwidth.
RSSI	Received Signal Strength Indication.
State	Connection State.
Band	Connected Band.

7.8 LTE > Lock PCIs

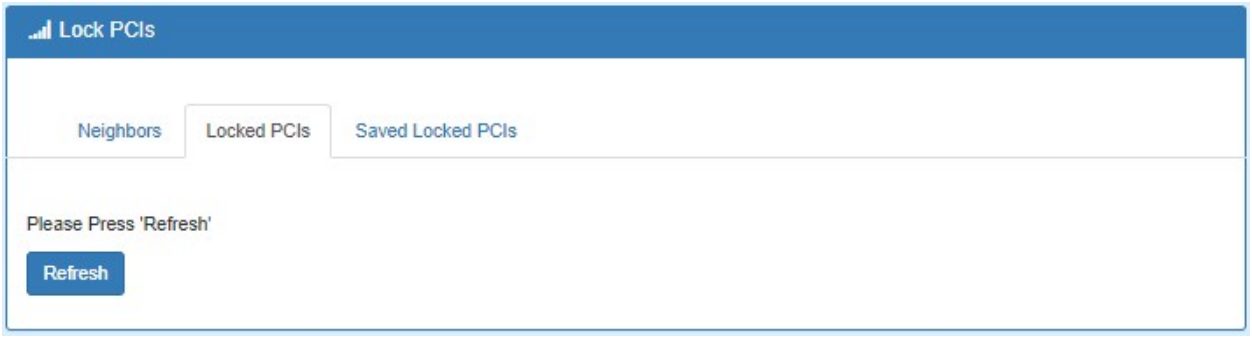
This section allows you to set Lock PCIs. It includes Neighbors, Locked PCIs, Saved Locked PCIs.

(1) Neighbors

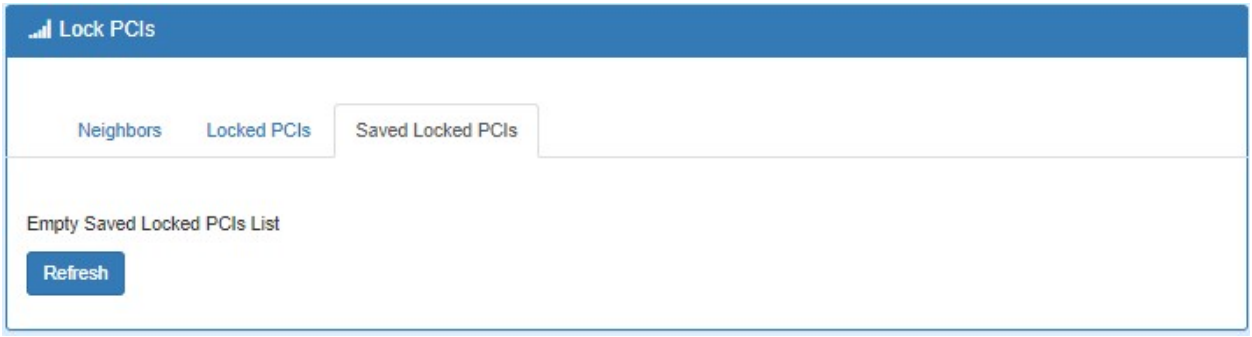


LTE > Lock PCIs > Neighbors	
Item	**Description**
Search	Search Neighbors from the Air for further action.
Lock	Select multiple PCI (Physical Cell ID) from Neighbor List to lock.
Unlock	Unlock all.
Save for bootup locked	Save selected lock PCIs for next boot up.

(2) Locked PCIs: Click **Refresh** button to display all locked PCI (Physicall Cell ID) information.

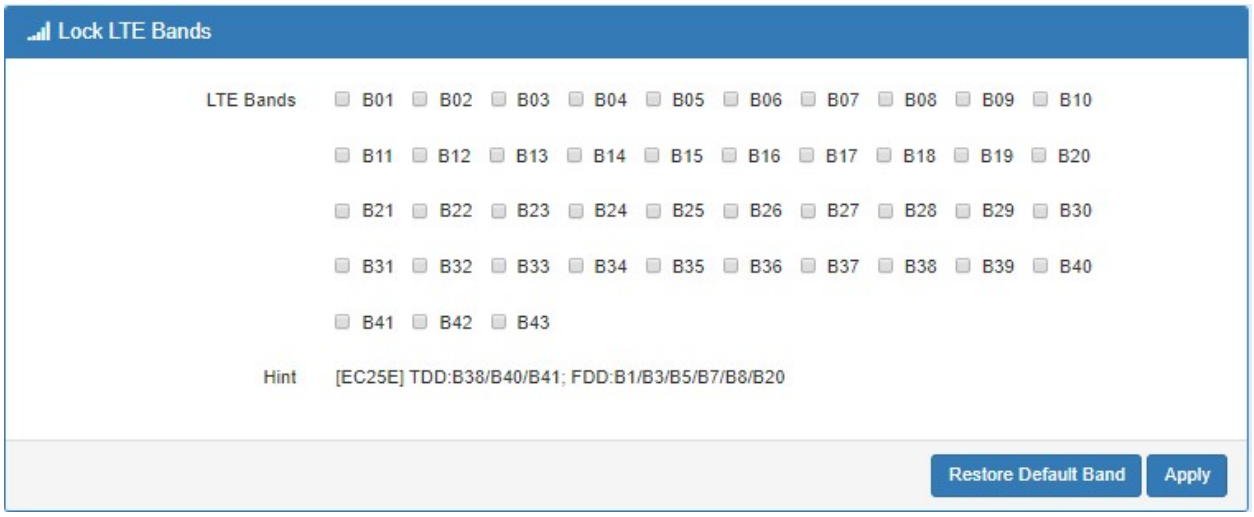


(3) Saved Locked PCIs: Click **Refresh** button to display all saved locked PCI (Physicall Cell ID) information.



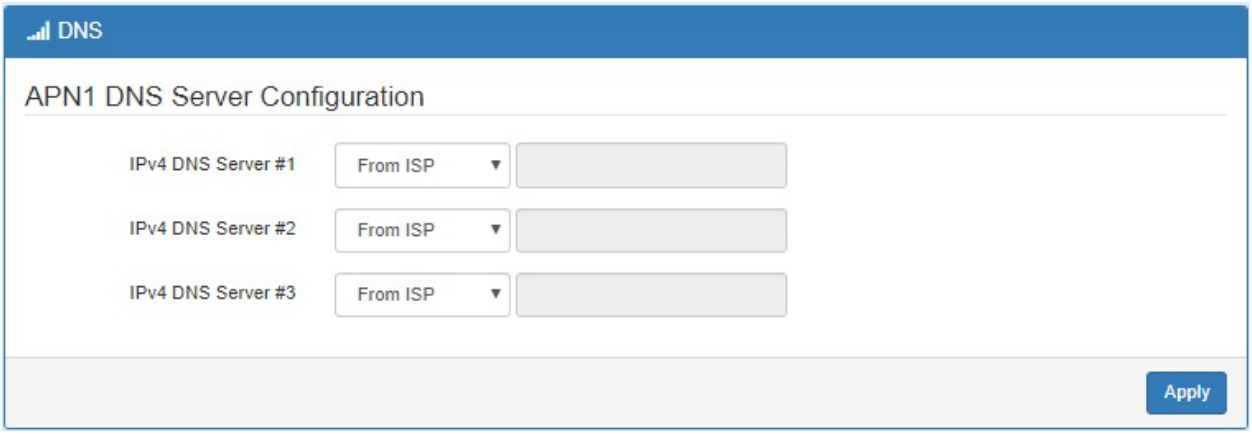
7.9 LTE > Lock Bands

Please check Hint for module support bands and then select your desired multiple bands to lock for use. It allows you to restore your default bands.



7.10 LTE > DNS

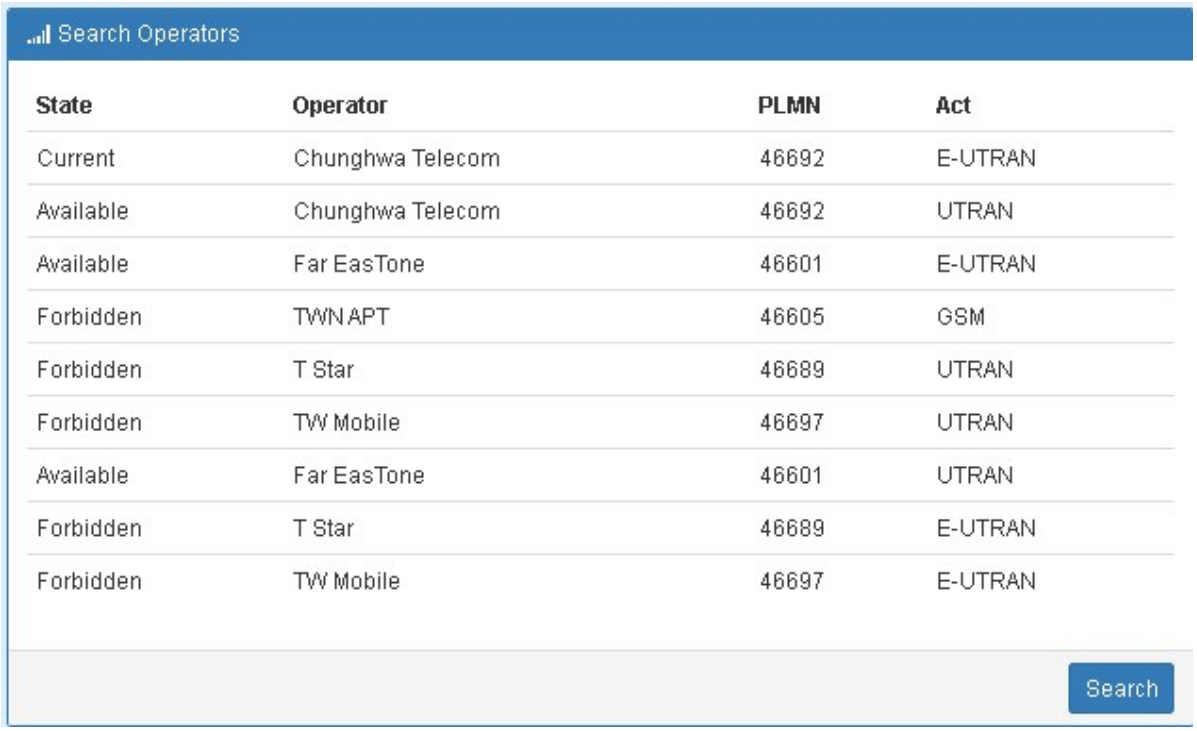
This section allows you to set LTE specific DNS setting.



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

7.11 Search Operators

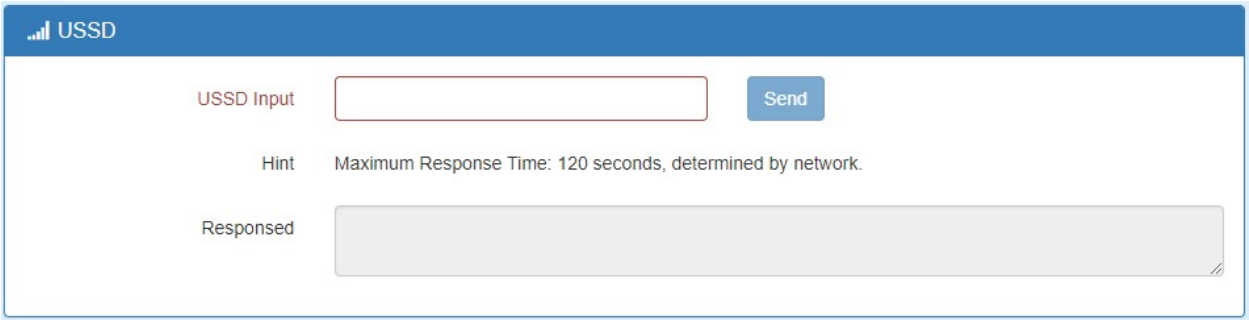
This section is to search the operators and get the status.



LTE > Search Operators	
Item	**Description**
STATE	• Current: Current connection. • Available: Possible connection. • Forbidden: Forbidden connection.
OPERATOR	Operator Name.
PLMN	Public Land Mobile Network ID.
ACT	3GPP Technology.

7.12 LTE > USSD

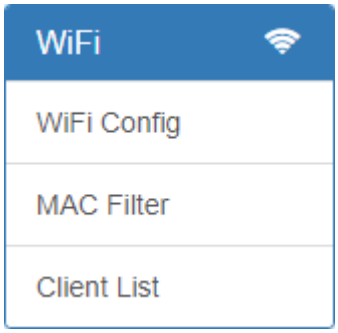
This section is to send USSD and get the response from the operator.



LTE > USSD	
Item	**Description**
USSD Input	Input the USSD you want to send.
Responded	The response from operator according your USSD.

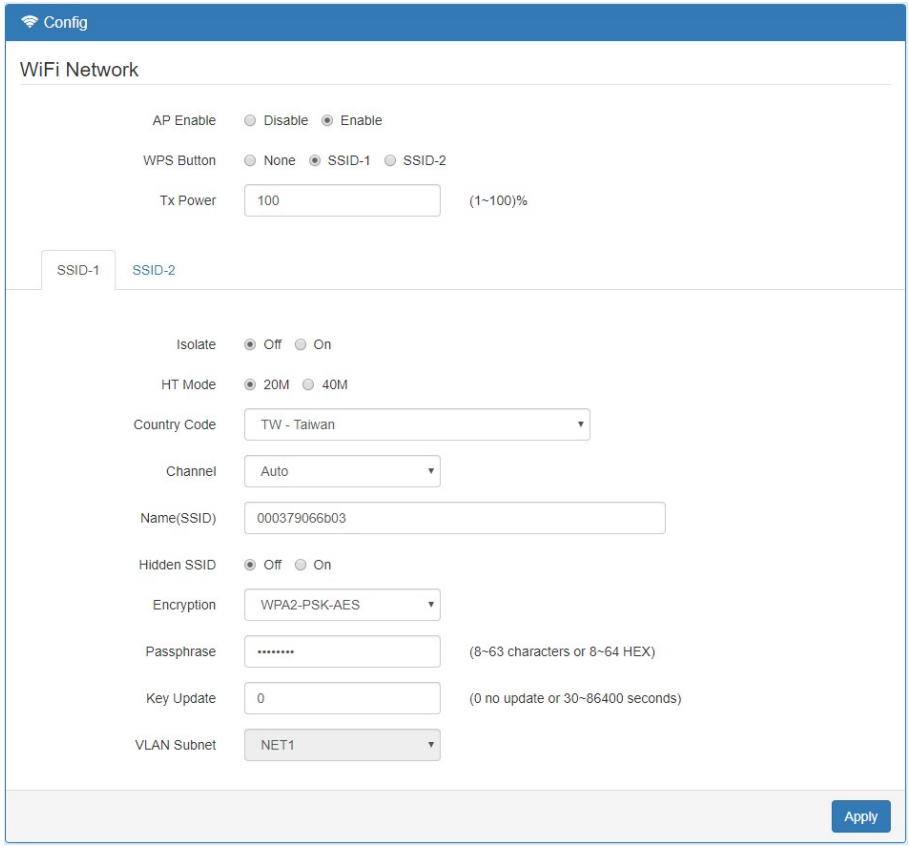
8 Configuration > WiFi

This section allows you to configure WiFi and it is used for ICR111WG model.



8.1 WiFi > WiFi Config

This section allows you to set up the Wi-Fi configuration.

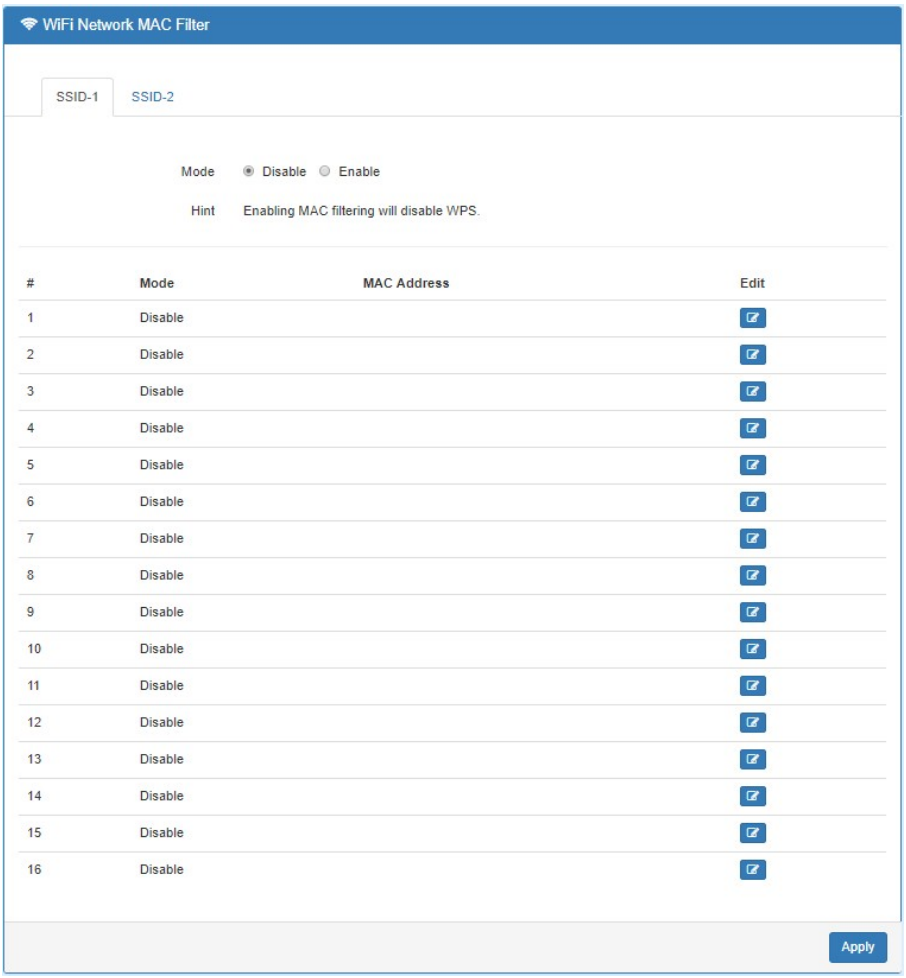


WiFi > Config	
Item	**Description**
AP Enable	Turn on/off the Wi-Fi Network. Select from Disable or Enable. The default is Enable.
WPS Button	Hardware button for WPS. Select the SSID you want to bind.
Tx Power	The TX power setting specifies the strength of the signal.
Enable	Turn on/off the SSID Network. Select from Disable or Enable.
Isolate	Isolation is a technique for preventing mobile devices connected to

WiFi > Config	
Item	**Description**
	an AP from communicating directly with each other.
HT Mode (HT Capability)	• 20M: Only 20MHz Operation is supported. • 40M: Both 20MHz and 40MHz Operation is supported.
Country Code	Select Country Area for supported Channels
Channel	Auto (Automatically select the best channel) or manually select channel number.
Name(SSID)	SSID is Wi-Fi identification. The maximum length is 32.
Hidden SSID	SSID hiding is the process of hiding the network name from being publicly broadcast.
Encryption	None or WPA2-PSK-AES.
Passphrase	Strings with a legal length of 8 to 63 or a length of 64 should belong to [0-9 A-F a-f].
Key Update	0 means no update or 30~86400 seconds update period.
VLAN Subnet	Select the VLAN Subnet you want to bind.

8.2 WiFi > MAC Filter

This section allows you to set up MAC Filter.

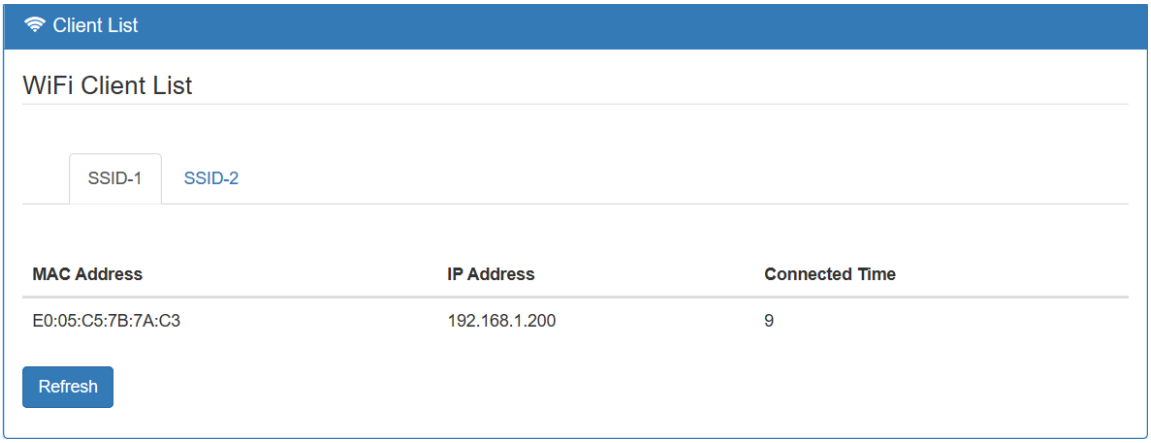


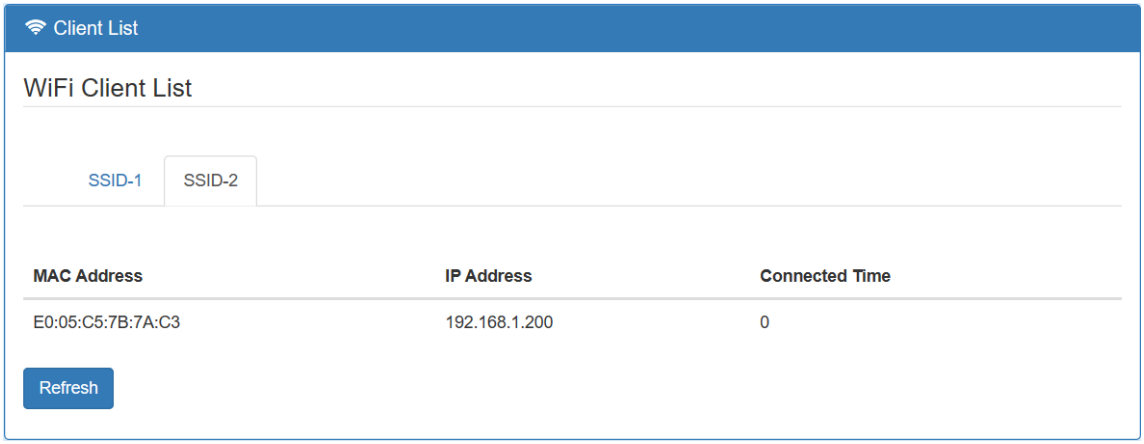
After clicking edit button, you can edit your MAC address.

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

8.3 WiFi > Client List

This section allows you to see all the Connected WiFi Client List.

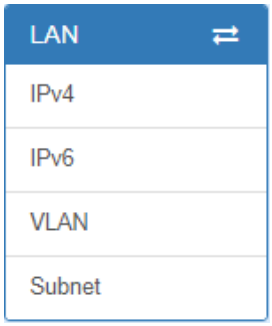




WiFi > Client List	
Item	**Description**
MAC Address	MAC Address
IP Address	Client IP Address
Connected Time	Connected Time in Seconds.

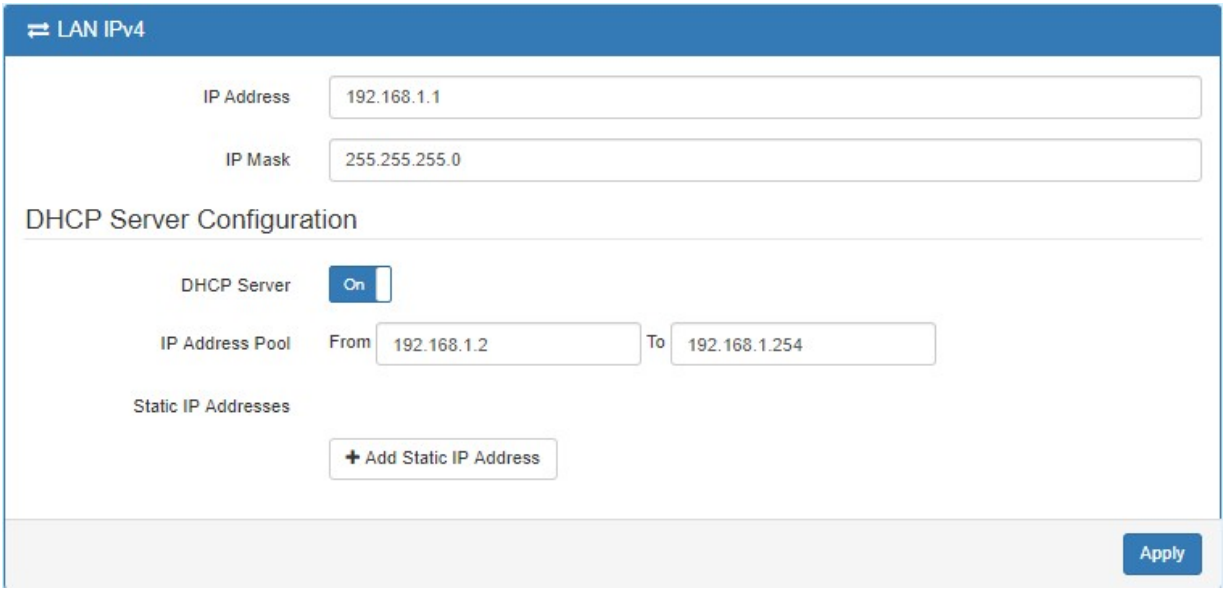
9 Configuration > LAN

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



9.1 LAN > IPv4

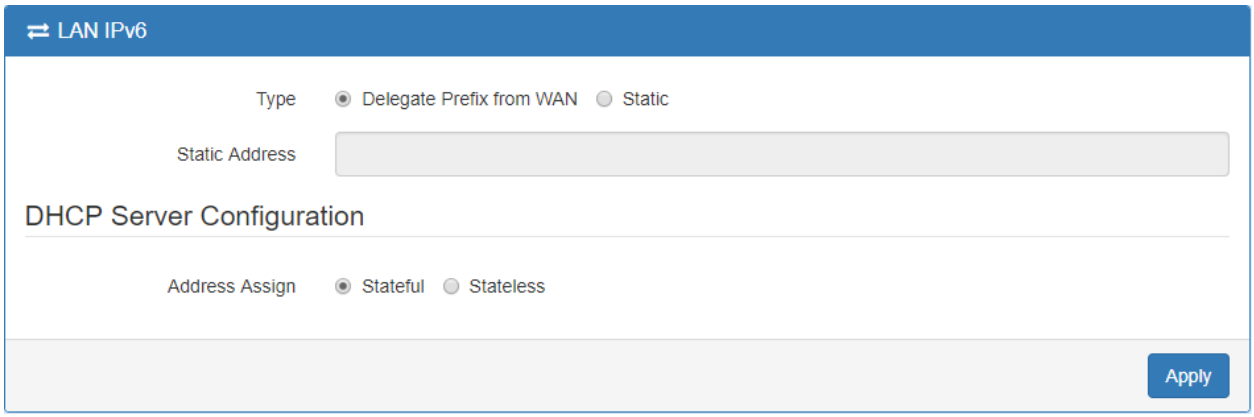
Set up your IP Address and IP Mask. Also, fill in the information of DHCP Server Configuration.



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.
Static IP Addresses	DHCP server support static IP address assignment. The static IP address can be added by clicking the **+Add Static IP Address button**. Each static IP consist of mode (on/off), MAC and IP address. • Mode: Turn on/off the static IP address. • MAC: The MAC address of target host or PC. • IP: The desired IP address for target host or PC.

9.2 LAN > IPv6

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



LAN > IPv6	
Item	**Description**
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.
Static Address	You need to input the static address when you select the static type.
DHCP Server Configuration	
Address Assign	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. • **Stateful**: The cellular router uses IPv6 stateful auto configuration. The LAN IPv6 clients can obtain IPv6 addresses through DHCPv6.

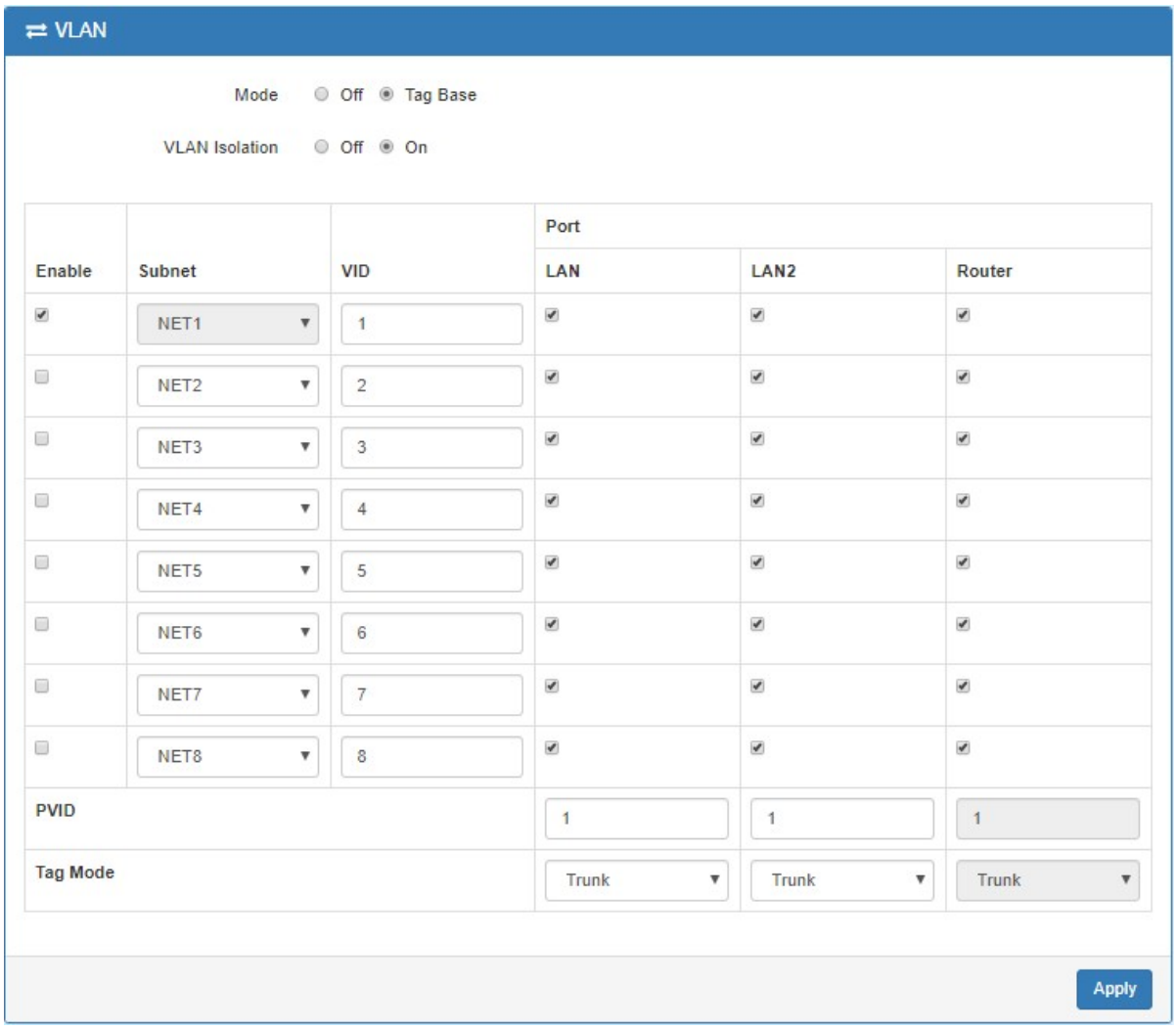
9.3 LAN > VLAN

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.

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

The **VLAN Isolation** function allows administrator to separate the different Subnet (VLAN). When

it is **on**, the different Subnet (VLAN) user cannot communication each other.



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 window will show the Subnet window from the LAN catalogue.)

There are two ports for Tag Base Mode, including LAN and LAN2. And one Router port which is a gate allows those ports to access internet or the router. The PVID and Tag Mode are for LAN and LAN2 ports. The PVID provides the untagged devices to communicate with third-party devices.

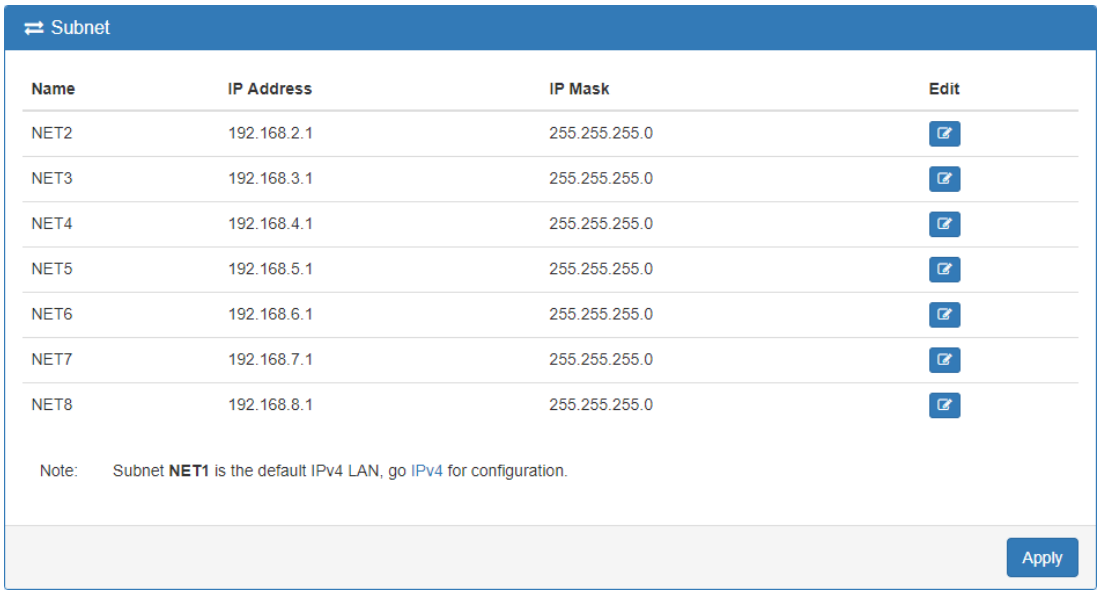
(***Note:*** The untagged devices mean not to support 802.1p VLANs.)

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.

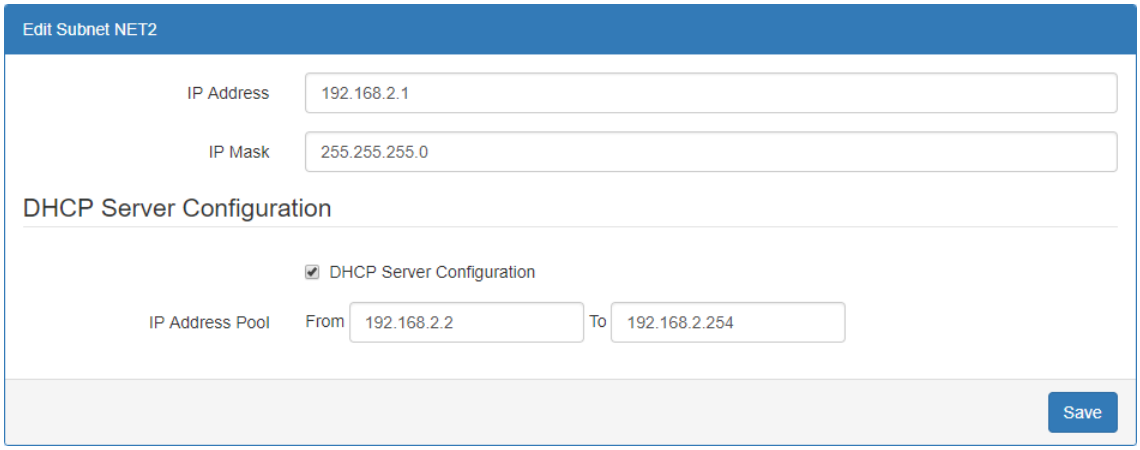
LAN > VLAN (1-port LANs)	
Item	**Description**
Mode	The VLAN mode is Off or Tag Base (802.1p VLAN).
VLAN Isolation	The VLAN Isolation is Off or On.
Enable	The assigned row of settings are enabled.
Subnet	Set up the IP address, IP mask and DHCP server.
VID	The VLAN ID range is from 1 to 4094.
Port	The port is shown to assign the port to a VLAN which the device is connected from LAN, LAN2 and Router.
PVID	• The PVID range from 1 to 4094. • Set up 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.

9.4 LAN > Subnet

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



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

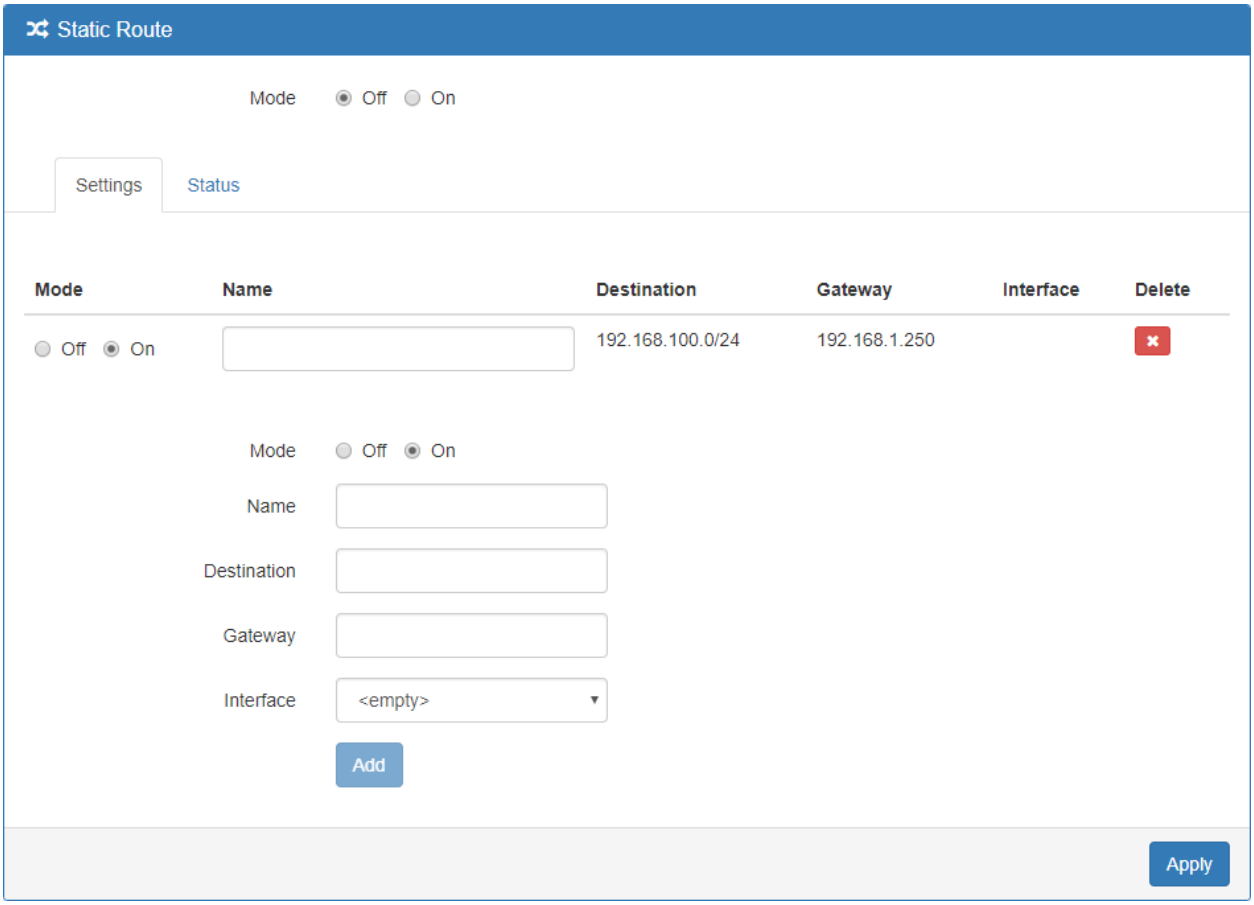


10 IP Routing

This section allows you to configure the Static Route, Policy Route, RIP, OSPF, and BGP.

10.1 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.



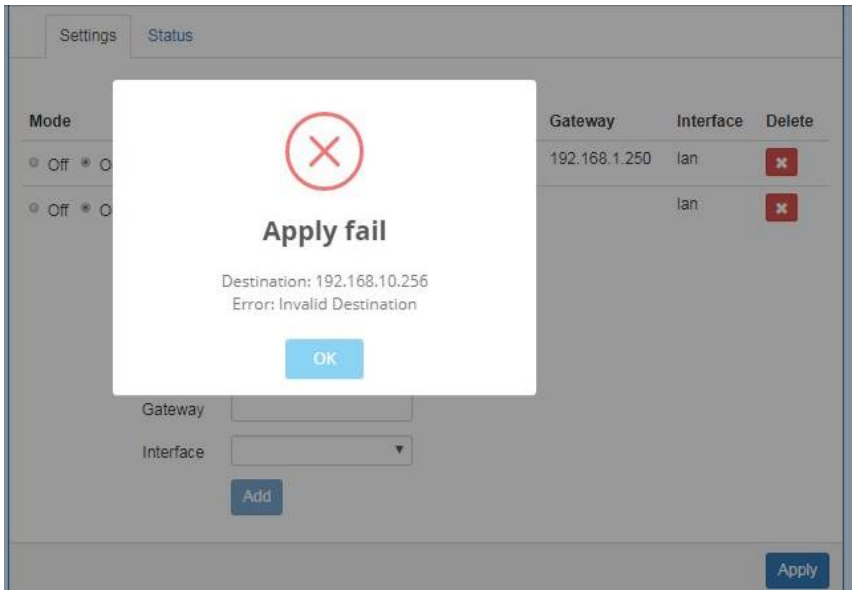
IP Routing > Static Route > Settings	
Item	**Description**
Mode	The setting is for full network. Select from Off or On.
Settings	
Mode	The setting is for the specific network. Select from Off or On.
Name	Set up each name for your running host or network.

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.

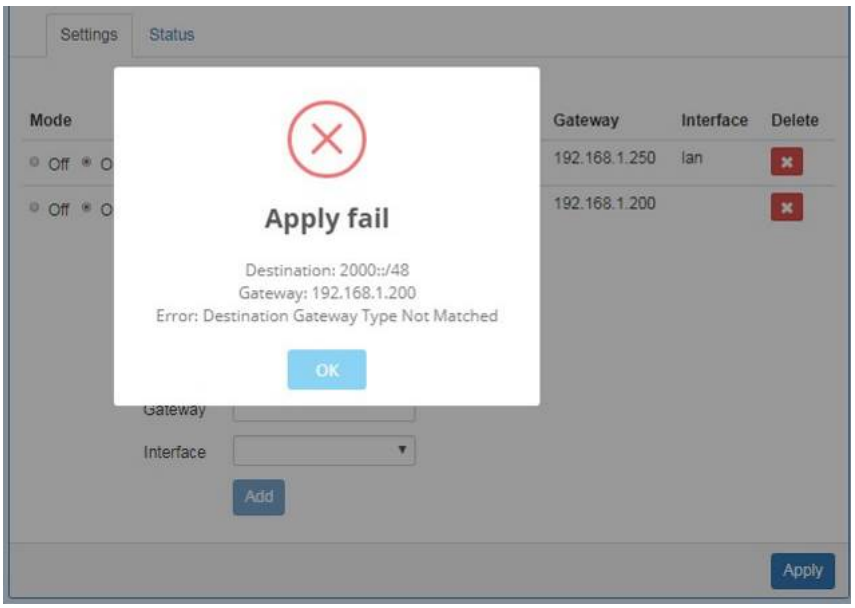
Note:

- 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.

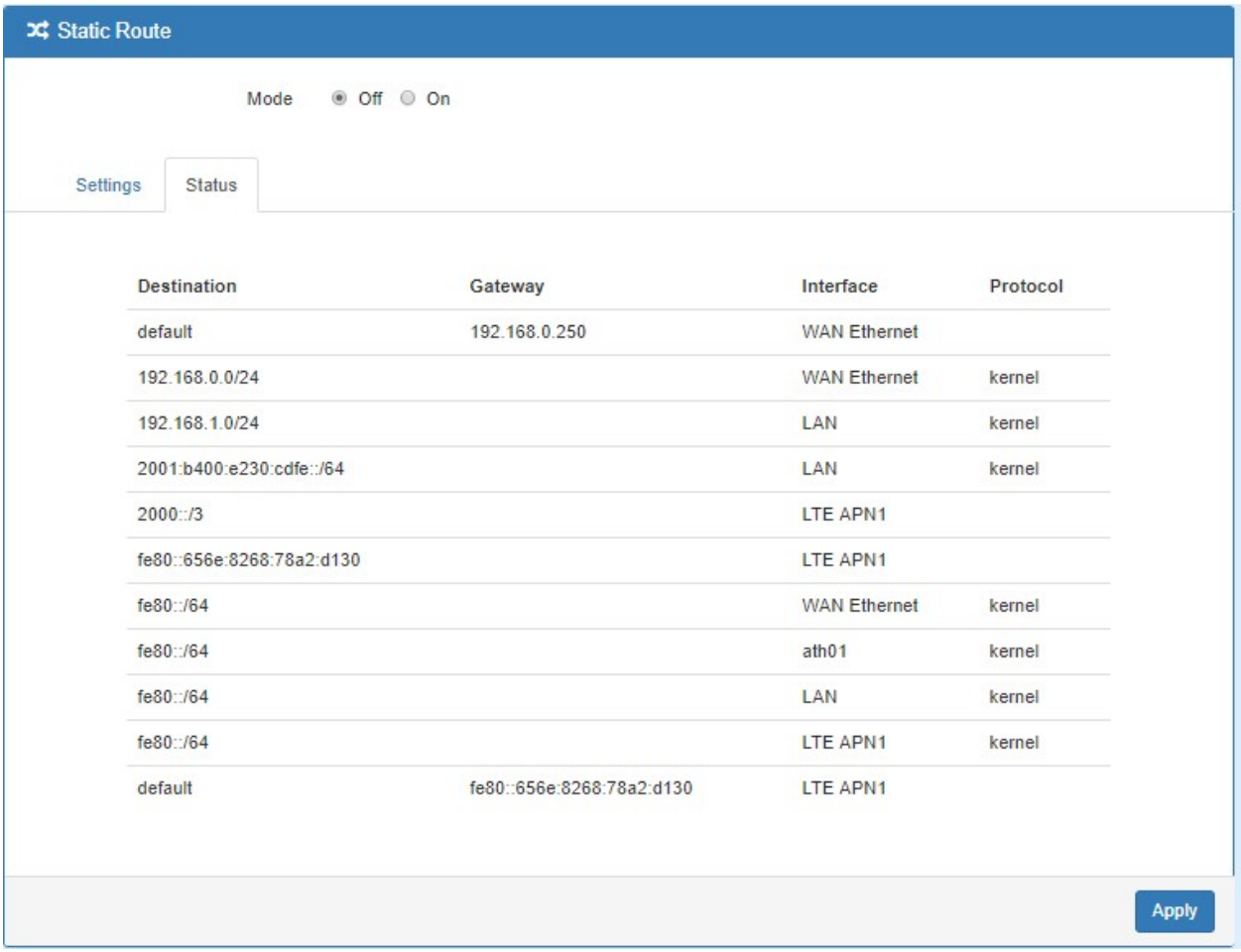
(1) Input the invalid format of destination. The interface is shown in Apply fail to notice.



(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.

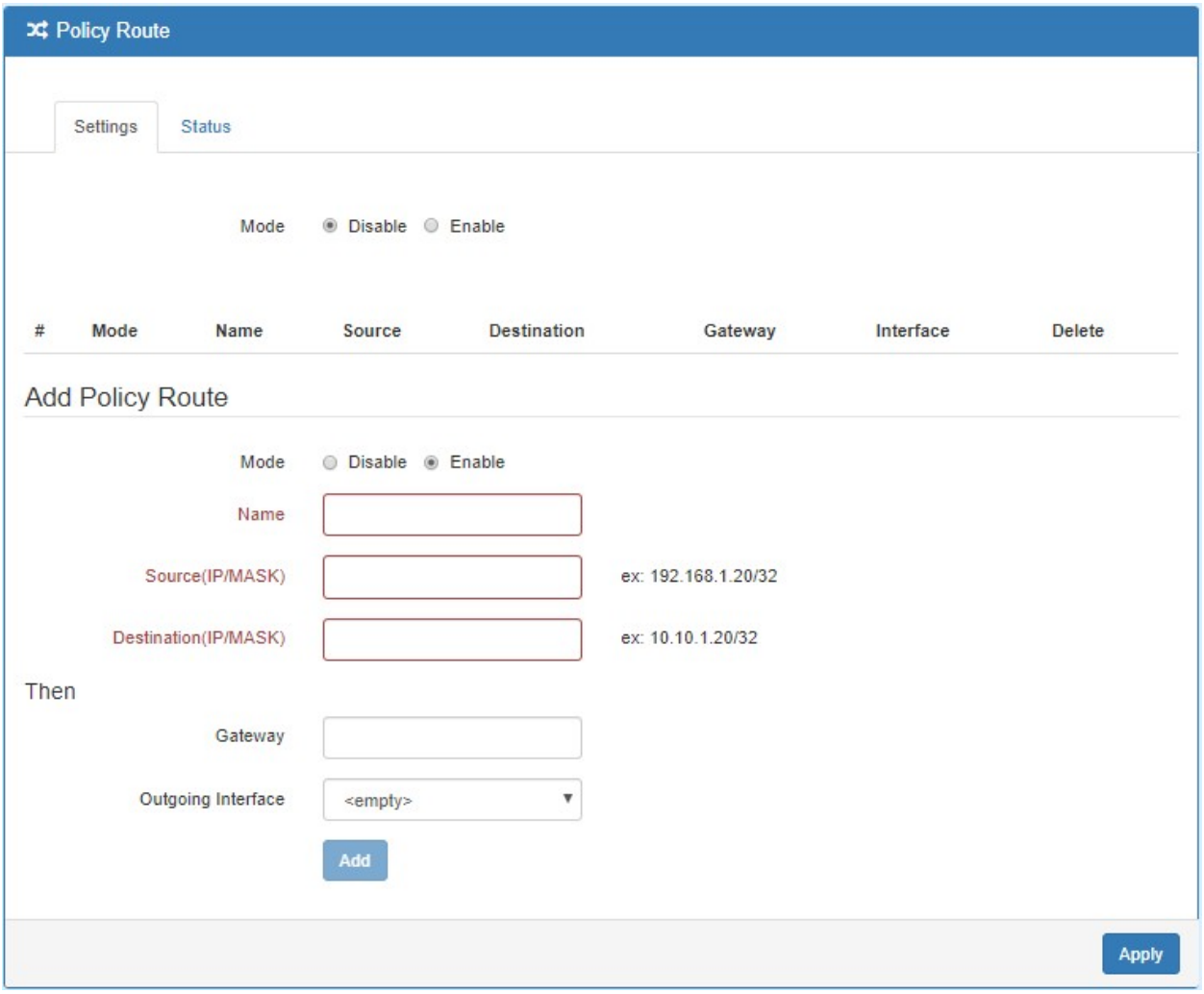


IP Routing > Static Route > Status	
Item	**Description**
Mode	The setting is open for full network. Select from Off or On.
Status	
Destination	Show the status of destination from the setting section.
Gateway	Show the status of gateway from the setting section.
Interface	Show the status of interface from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

10.2 Policy Route

This section allows you to set up the settings and get the status for Policy Route.

Note: Policy Route is only enabled on active interfaces, but it is disabled on deactivated interfaces automatically.



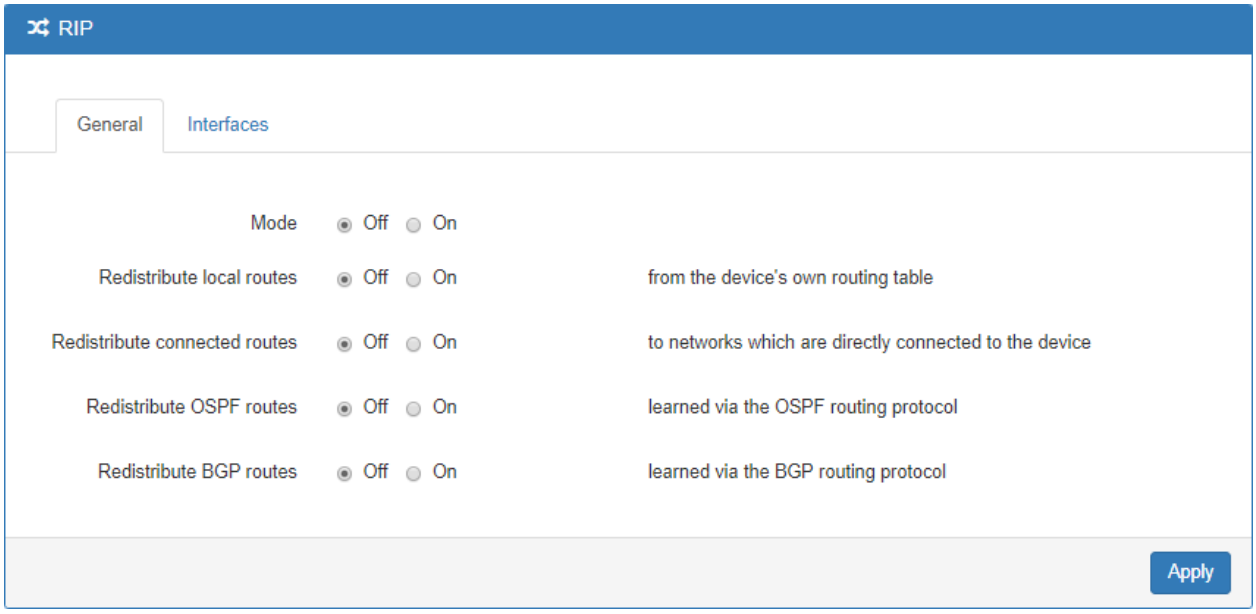
IP Routing > Policy Route	
Item	**Description**
Mode	The setting is for full network. Select from Disable or Enable.
Settings	
Mode	The setting is for the specific network. Select from Disable or Enable.
Name	Set up each name for your running host or network.
Source(IP/MASK)	Fill in the source of a specific IP/MASK from network.
Destination (IP/MASK)	Fill in the destination of a specific IP/MASK from network.
Gateway	Fill in the gateway address of your router.
Outgoing Interface	Select the interface from LAN or Ethernet.

10.3 IP Routing > RIP

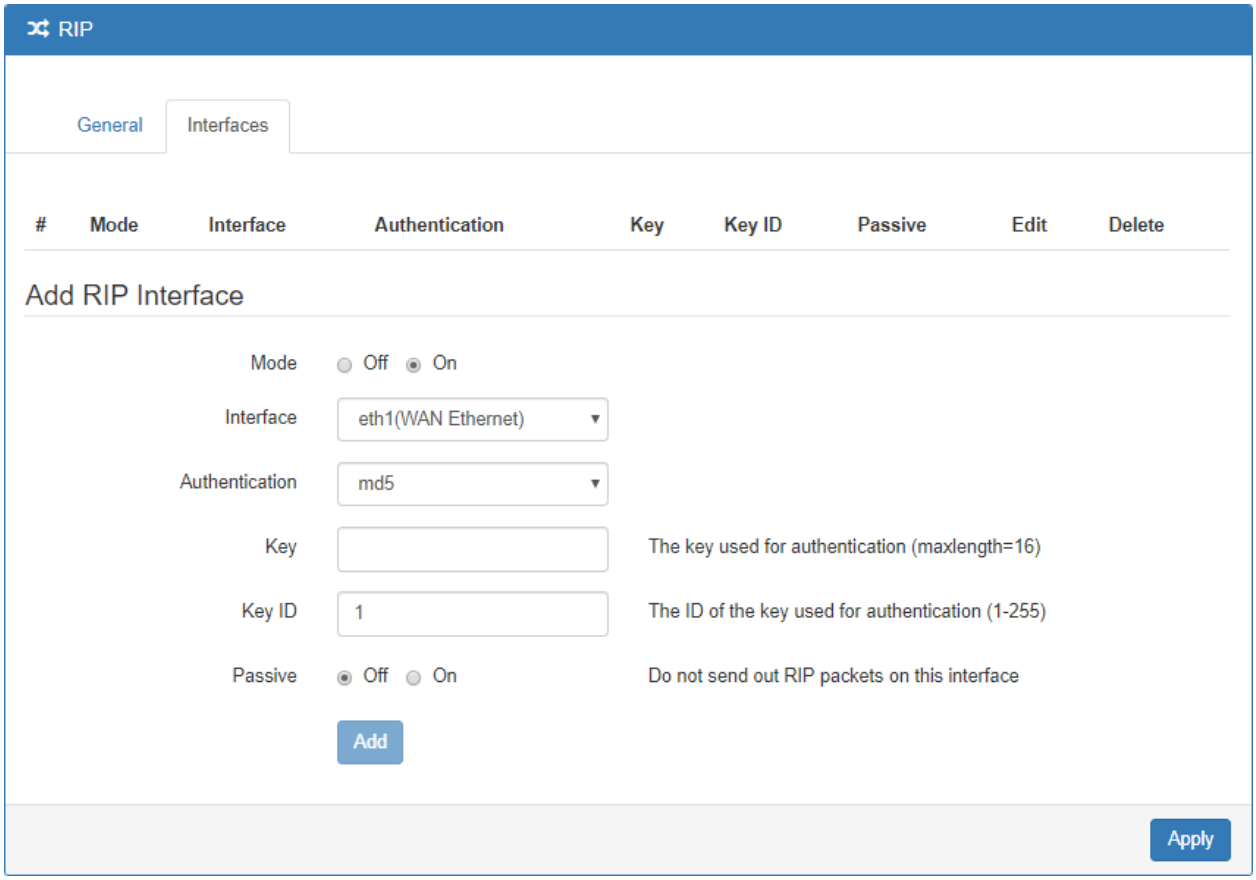
This section allows you to configure RIP and select the mode from Disable or Enable. The default is Disable.

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.
Redistribute OSPF routes	Select from Off or On to open or close redistribute OSPF routes.
Redistribute BGP routes	Select from Off or On to open or close redistribute BGP routes.

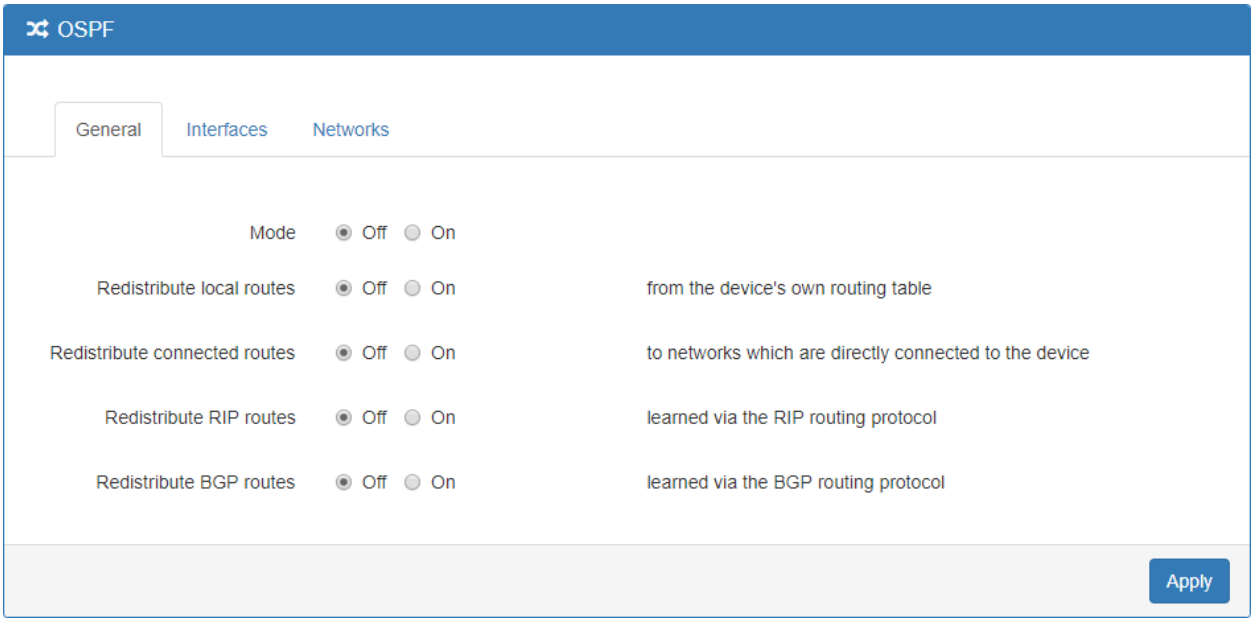


IP Routing > RIP > Interfaces	
Item	**Description**
Interfaces	
Mode	Select from **Off** or **On** to use or not to use the RIP function in the interface.
Interface	Select from **eth1 (WAN Ethernet)** or **LAN**.
Authentication	Select from **none** or **md5** to approve authentication. ***Note:*** Please 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.

10.4 IP Routing > OSPF

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

(1) General Configuration



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

(2) Interfaces Configuration

There are 2 parts for OSPF Interfaces configuration.

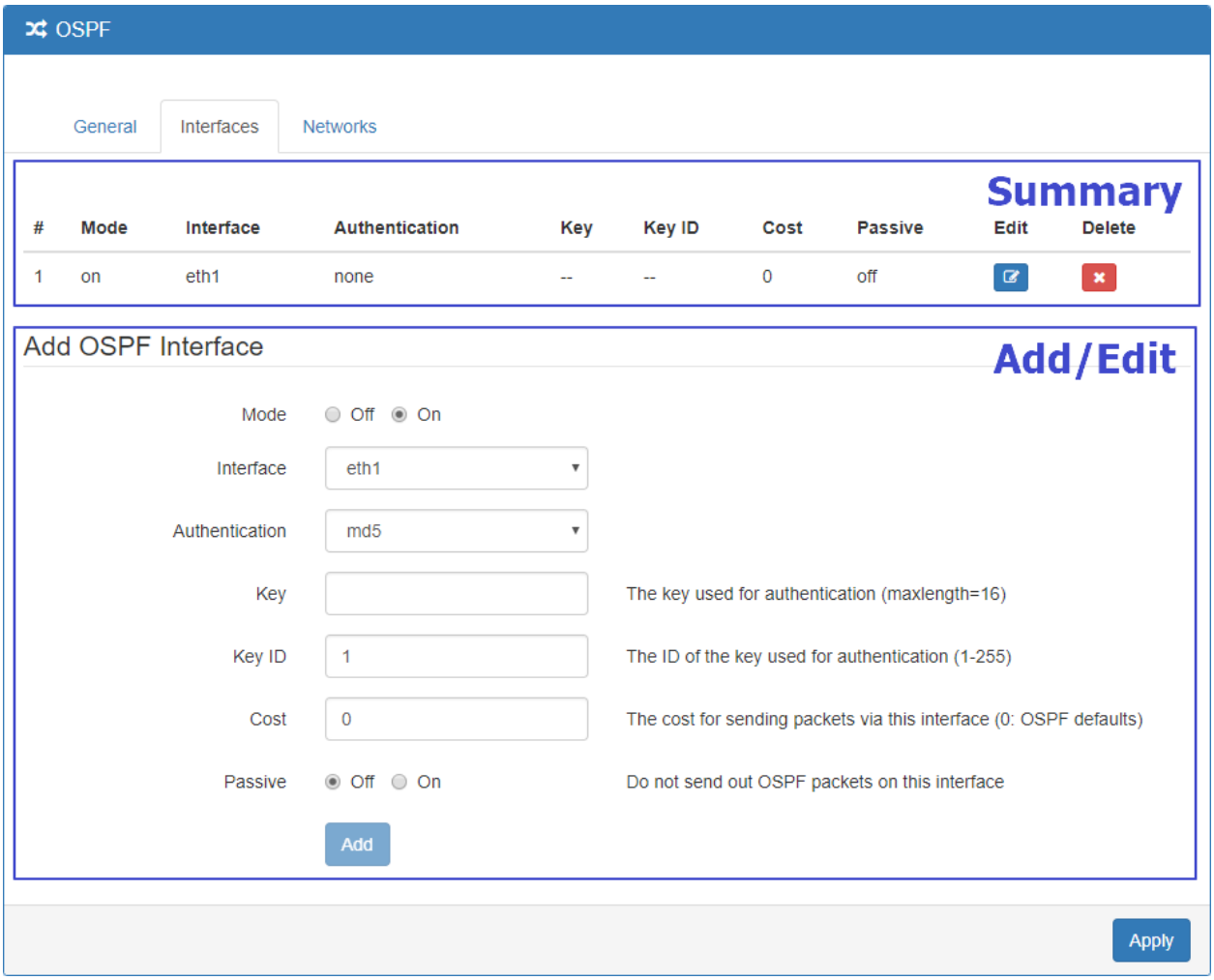
- OSPF Interfaces Summary

  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**
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

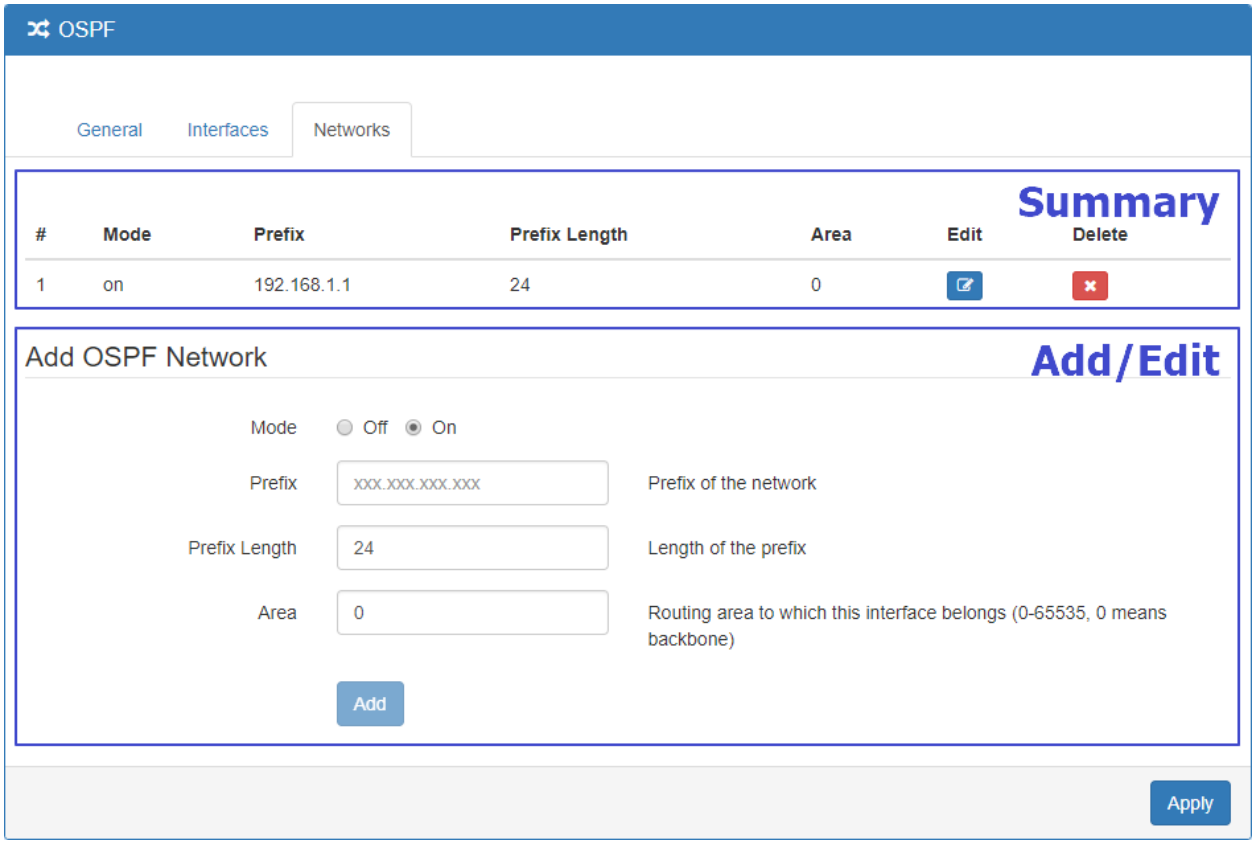
There are 2 parts for OSPF Networks configuration.

- 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.

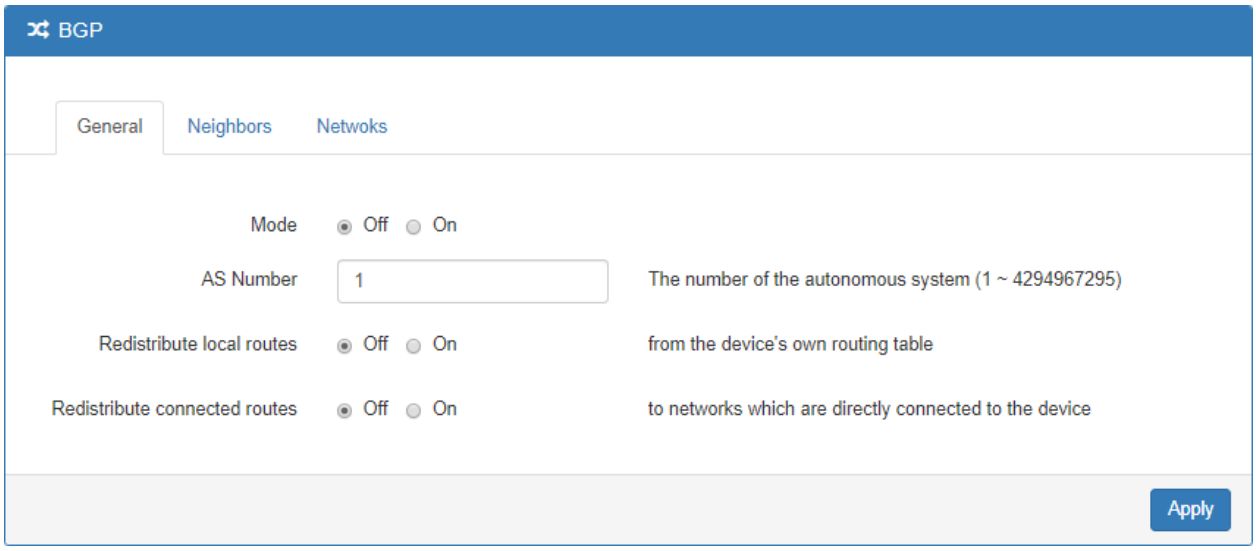


IP Routing > OSPF > Networks	
Item	**Description**
Mode	Select from **Off** or **On** to enable the network setting.
Prefix	Set Prefix of the network
Prefix Length	Set Length of the prefix
Area	Routing area to which this interface belongs (0-65535, 0 means backbone)

10.5 IP Routing > BGP

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

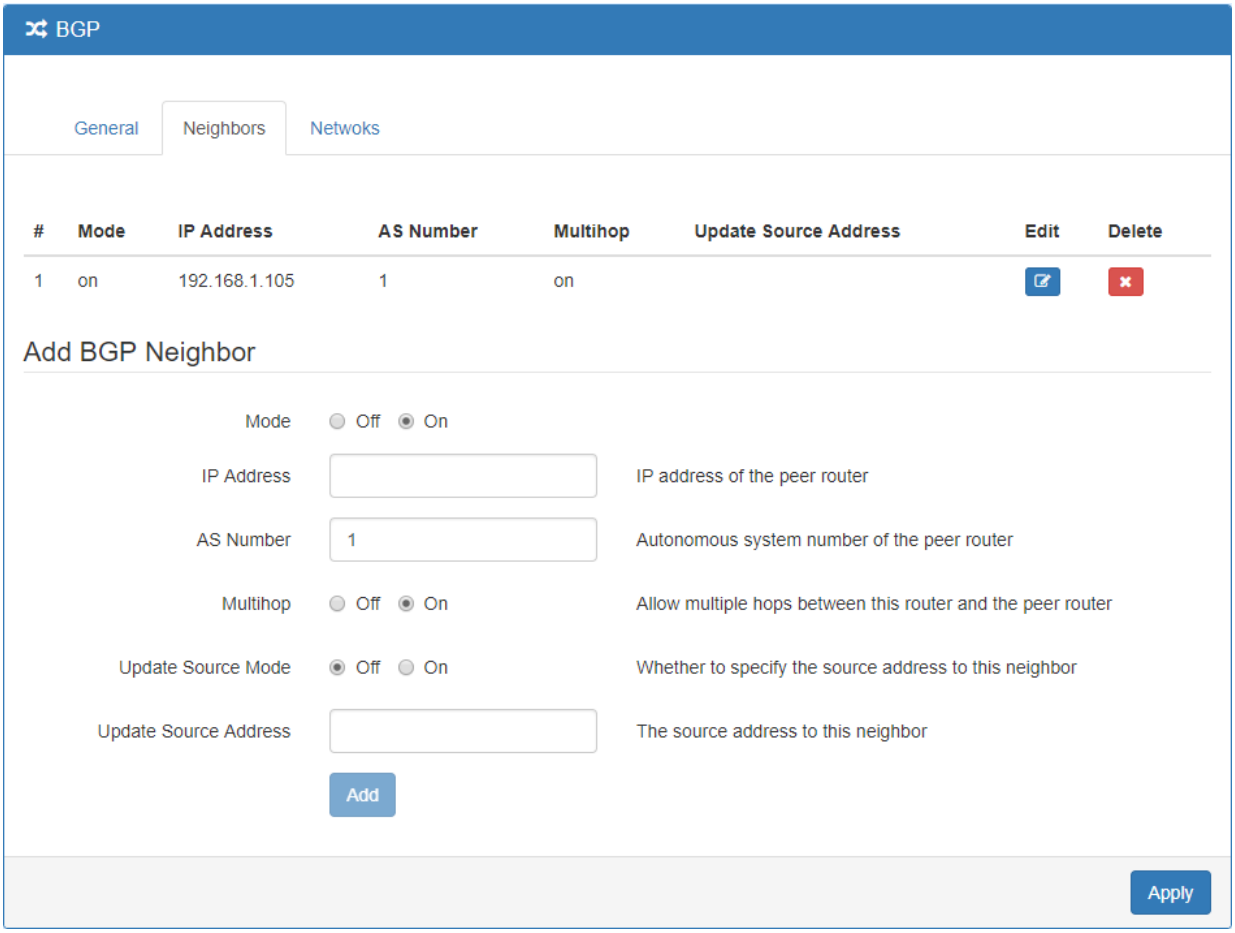
(1) General Configuration



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.

(2) Neighbor Configuration

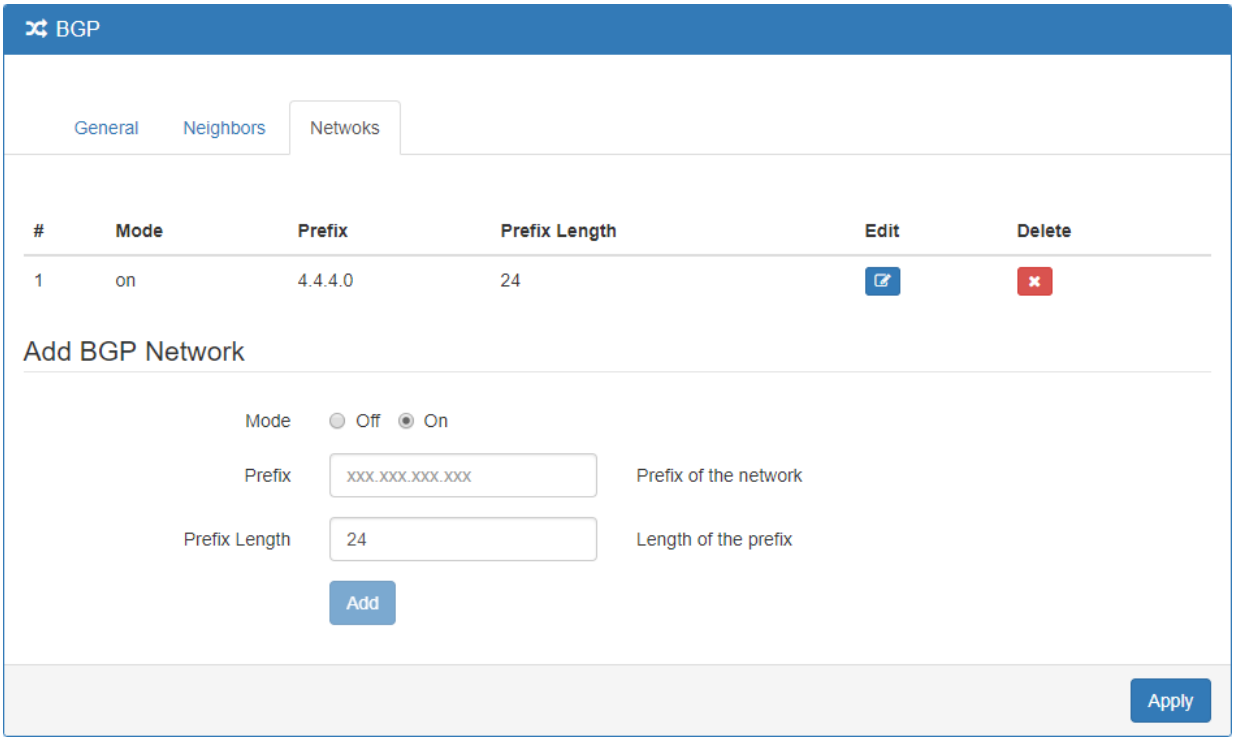
The neighbors sub configuration is used to configure all the BGP routers to peer with and the maximum neighbors is 16.



IP Routing > BGP > Neighbors	
Item	**Description**
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.
Update Source Mode	Whether to specify the source address to this neighbor.
Update Source Address	The source address to this neighbor.

(3) Networks Configuration

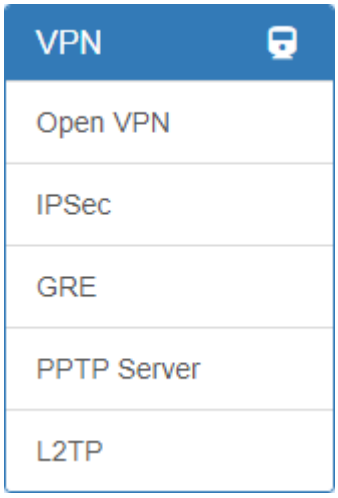
The networks sub configuration allows to add IP network prefixes that shall be distributed via BGP in addition to the networks that are redistributed from other sources as defined on the general sub configuration and the maximum neighbors is 16.



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

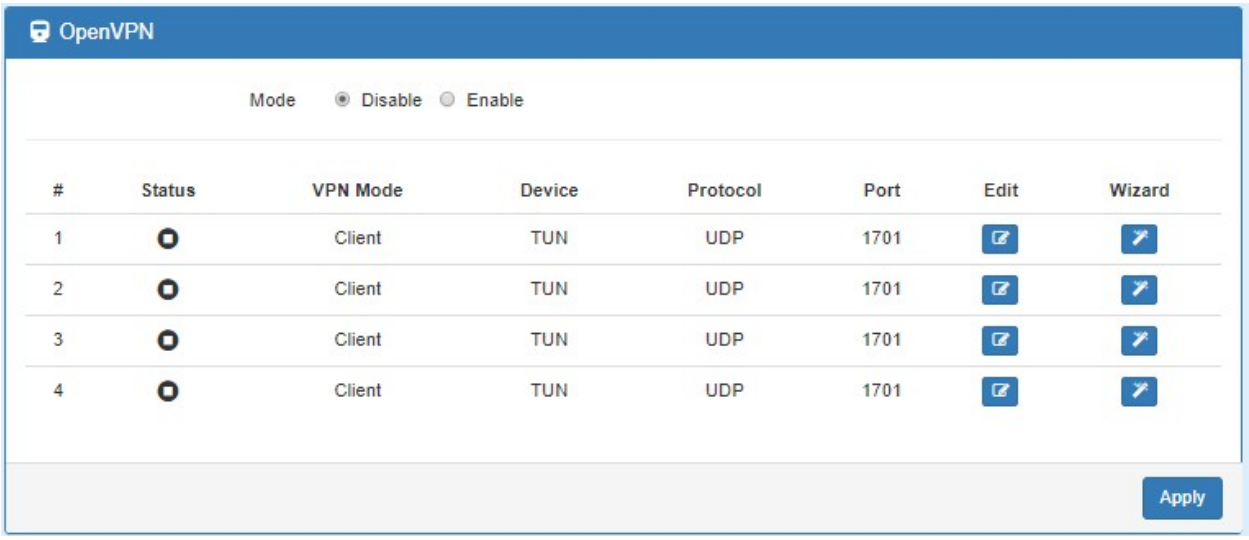
11 Configuration > VPN

This section allows you to configure Open VPN, IPsec, GRE, PPTP Server, and L2TP.



11.1 VPN > Open VPN

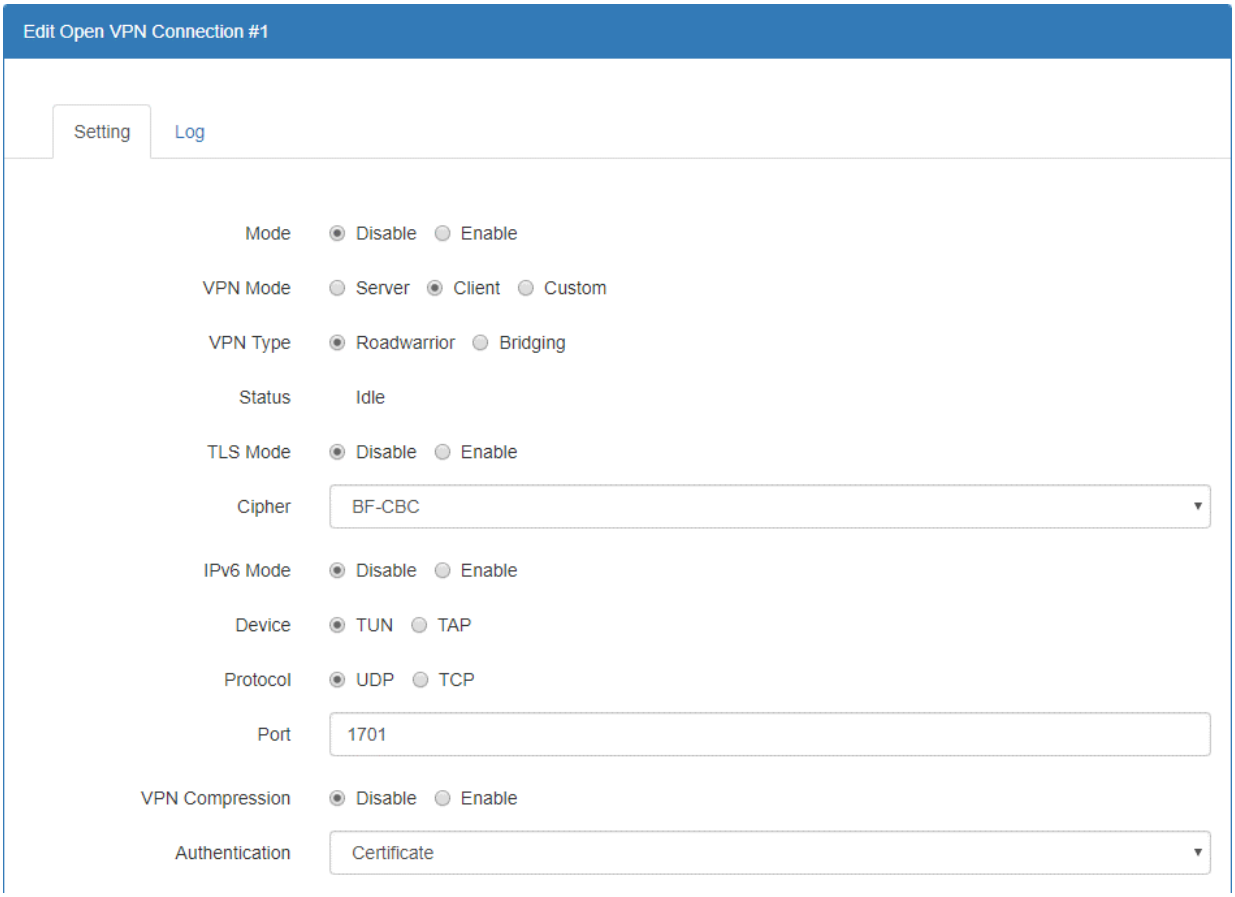
This section allows you to set up the connection of Open VPN. The default mode is Disable. From **Log** tab, the interface will show the status of connection to make you follow the situation whenever it is successful or fail connection.



11.1.1 Open VPN Common Setting

(1) Click button to edit Open VPN Connection.

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



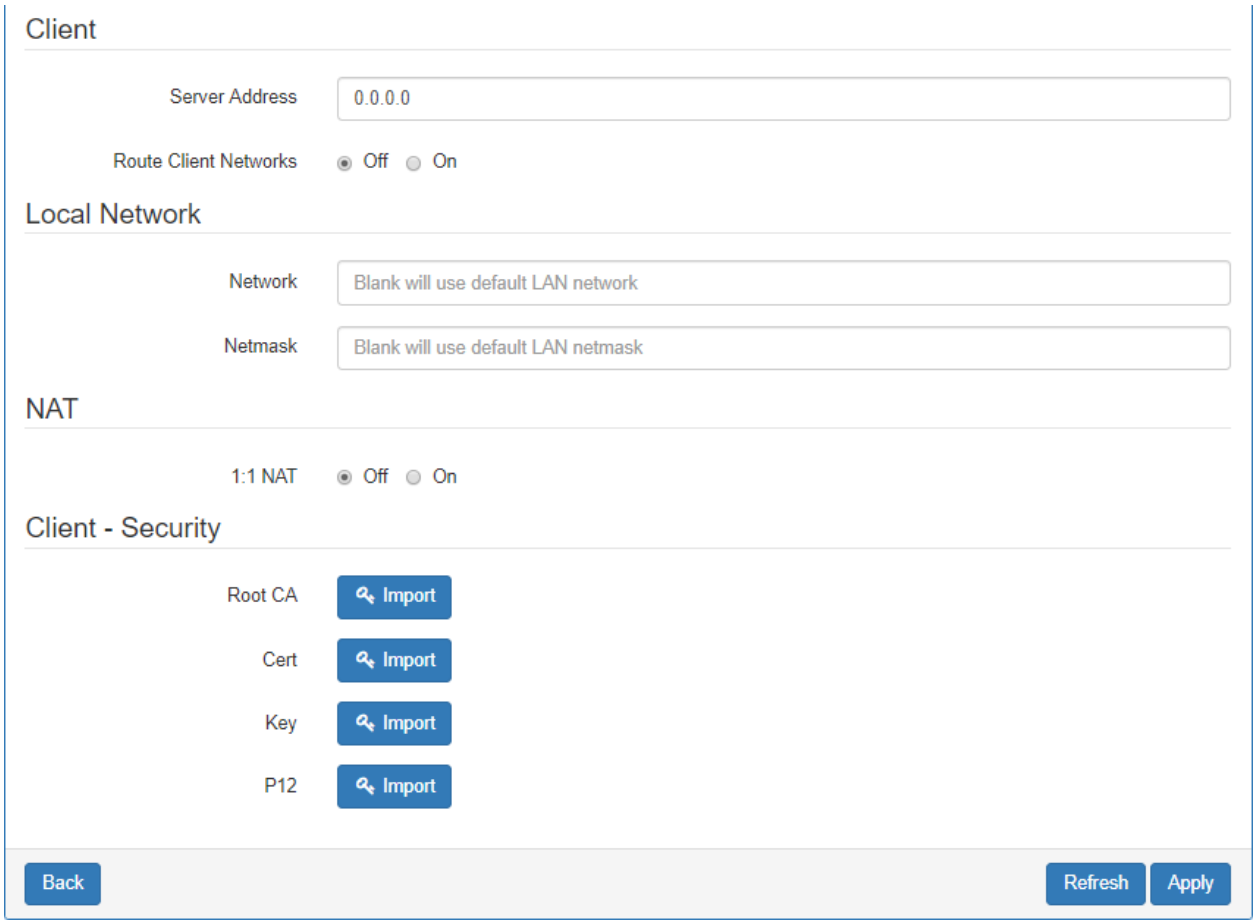
VPN > Open VPN > Setting	
Item	**Description**
Mode	Turn on/off Open VPN to select Disable or Enable.
VPN Mode	• **Server:** Tick to enable Open VPN server tunnel. • **Client:** Tick to enable Open VPN client tunnel. The default is Client. • **Custom:** This option allows user to use the .ovpn configuration file to quickly set up VPN tunnel with third-party server or use the Open VPN advanced options to be compatible with other servers.
VPN Type	• Roadwarrior (**default**) • **Bridging:** Bridging the VPN tunnel and LAN/VLAN
Status	Display the status of Open VPN.
TLS Mode	Select from Disable or Enable for data security. The default is Disable.
Cipher	The Open VPN 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 Open VPN 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.

11.1.2 Open VPN Client Setting

Select option "**Client**" from VPN Mode, and this section allows you configure the **Open VPN client route** and authentication files.

The files could be imported by clicking Import button and the file should be downloaded from Open VPN server.



VPN > Open VPN > Client VPN Mode	
Item	**Description**
Client	
Server Address	Fill in WAN IP of Open VPN 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.
Local Network	
Network	The local network exported by OpenVPN. When keeping this option blank, the OpenVPN will export the LAN network automatically.
Netmask	The local netmask exported by OpenVPN. When keeping this option blank, the OpenVPN will export the LAN netmask automatically.
NAT	

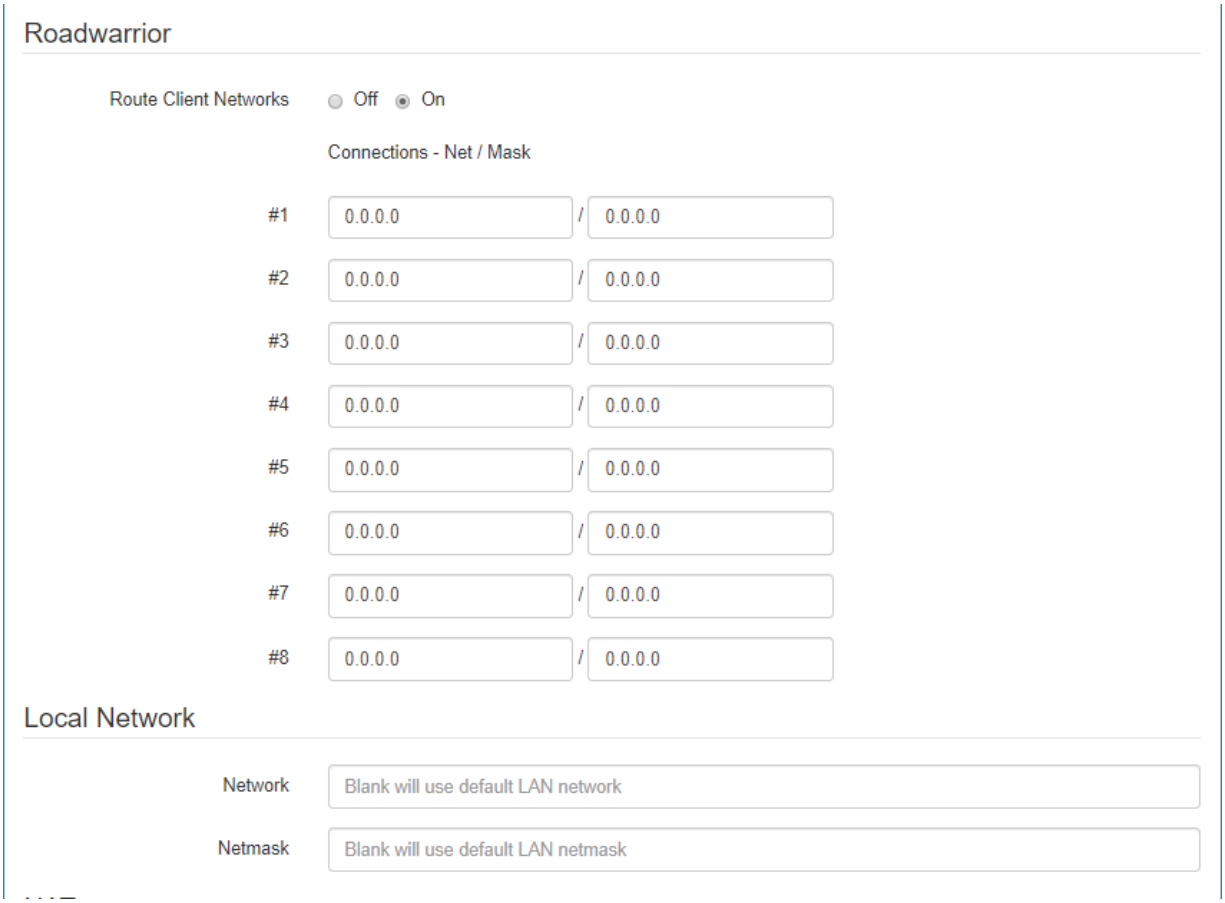
1:1 NAT	• Tick to enable NAT Traversal for Open VPN. This item must be enabled when the router under NAT environment. • Select from Off or On. • When two routers' LAN Subnet are same and create Open VPN tunnels, this function should be turned on.
Client-Security	
Root CA	The Certificate Authority file of Open VPN server could be downloaded from Open VPN server.
Cert	The certification file is for Open VPN client, which could be downloaded from Open VPN server.
Key	The private key file is for Open VPN client, which could be downloaded from Open VPN server.
P12	The PKCS#12 file is for Open VPN client, which could be downloaded from Open VPN server.

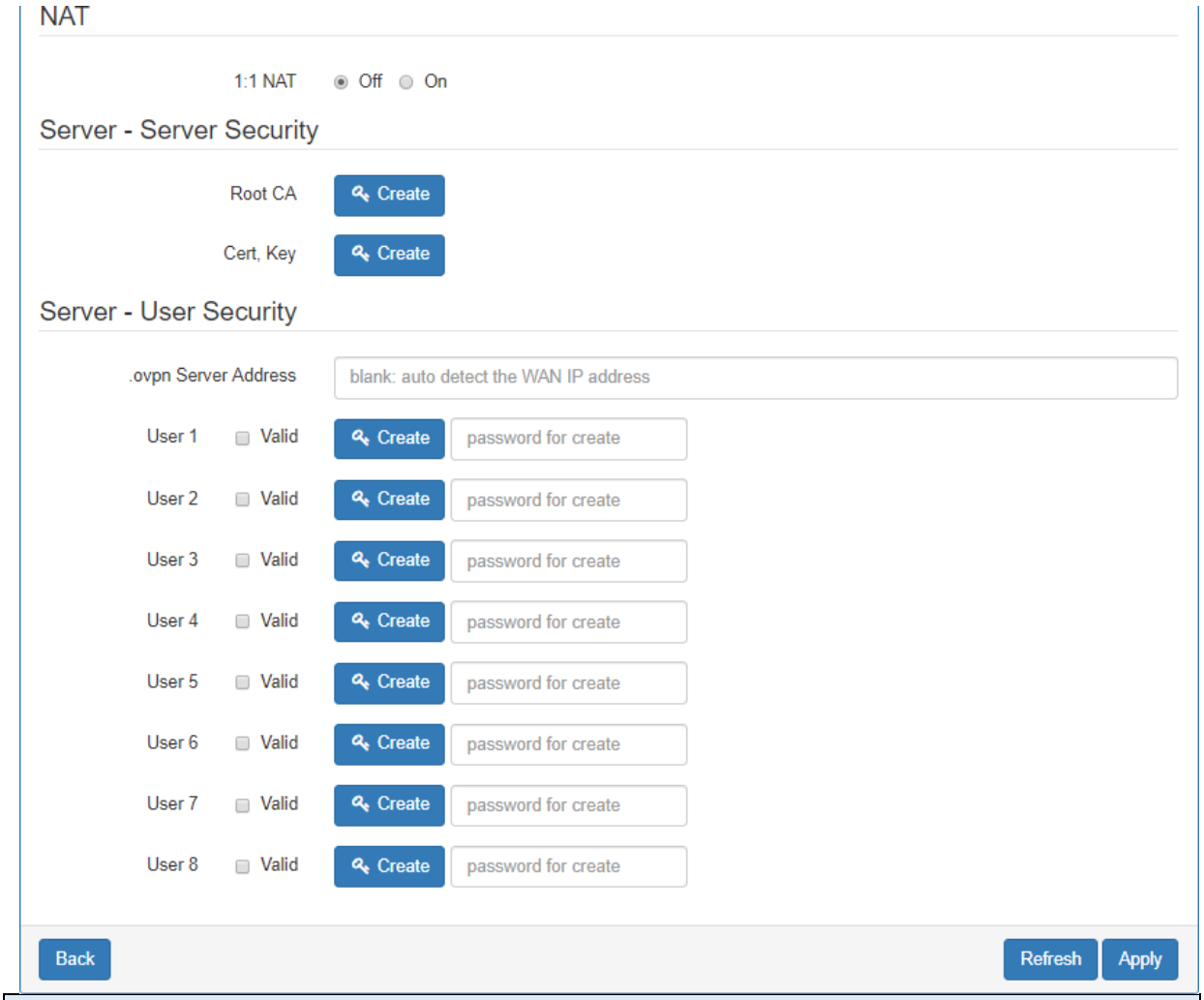
11.1.3 Open VPN Server Setting

Select option "**Server"** from VPN Mode, and this section allows you to configure the **server status of VPN Mode**.

Note: When selecting the On option of Route Client Networks, the Open VPN server will route the client traffic or not.

You should fill in the client IP and netmask when this option is enabled.





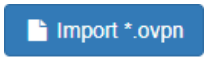
VPN > Open VPN > Server VPN Mode	
Item	**Description**
Server	
VPN Network	The network ID for Open VPN virtual network.
VPN Netmask	The netmask for Open VPN virtual network.
Roadwarrior: Route Client Networks	Select from Off or On. The Open VPN server will route the client traffic or not. User should fill in the client IP and netmask when this option is enabled.
Local Network	
Network	The local network exported by OpenVPN. When keeping this option blank, the OpenVPN will export the LAN network automatically.
Netmask	The local netmask exported by OpenVPN. When keeping this option blank, the OpenVPN will export the LAN netmask automatically.
NAT	
1:1 NAT	• Tick to enable NAT Traversal for Open VPN. 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 Open VPN 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.

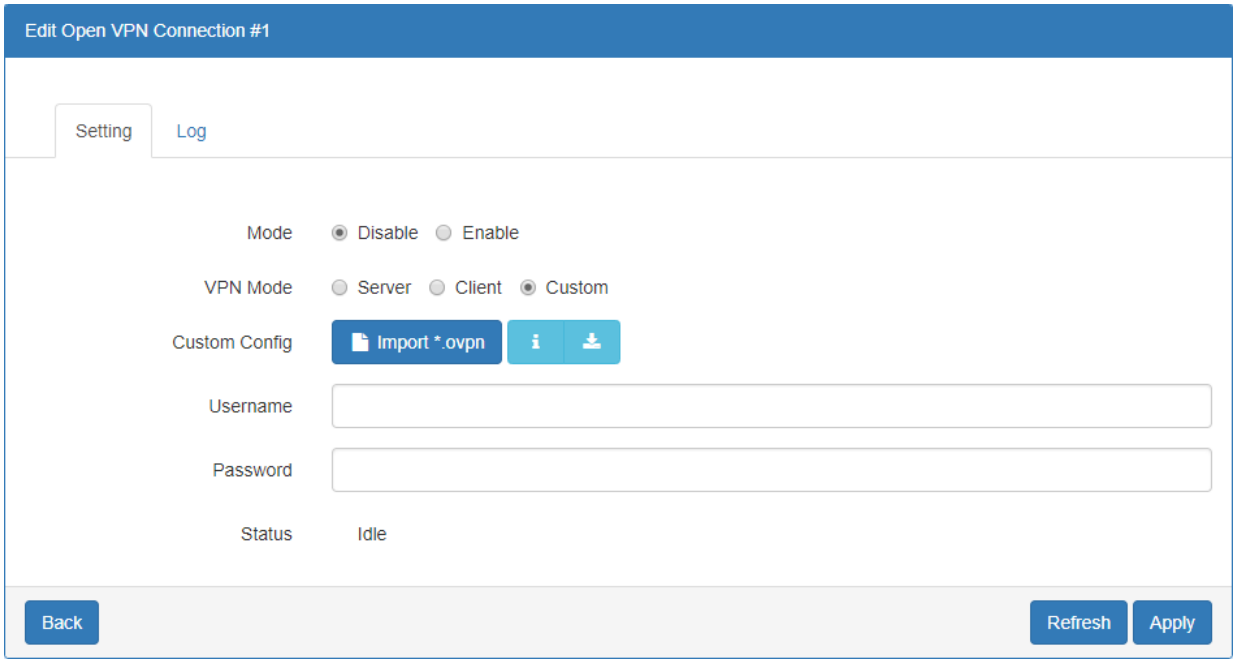
11.1.4 Set up Open VPN Custom

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 Open VPN advance options to be compatible with other servers.

Note:

- When clicking the 

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



VPN > Open VPN > Custom VPN Mode	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
VPN Mode	Select from custom mode.
Custom Config	Import Open VPN 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 Open VPN, such as IP address and the connected time.

11.2 VPN > IPsec

This section allows you to set up IPsec Tunnel. The setting has four tags, Connections, Authentication IDs, X.509 Certificates, and CA Certificates.

For the IPsec connection which be authenticated by **pre-shared key**, it only need to setup the **Connections** and **Authentication IDs.** For the IPsec connection which be authenticated by **RSA or TLS**, the settings must cover the four parts.

Mode ◉ Disable ○ Enable

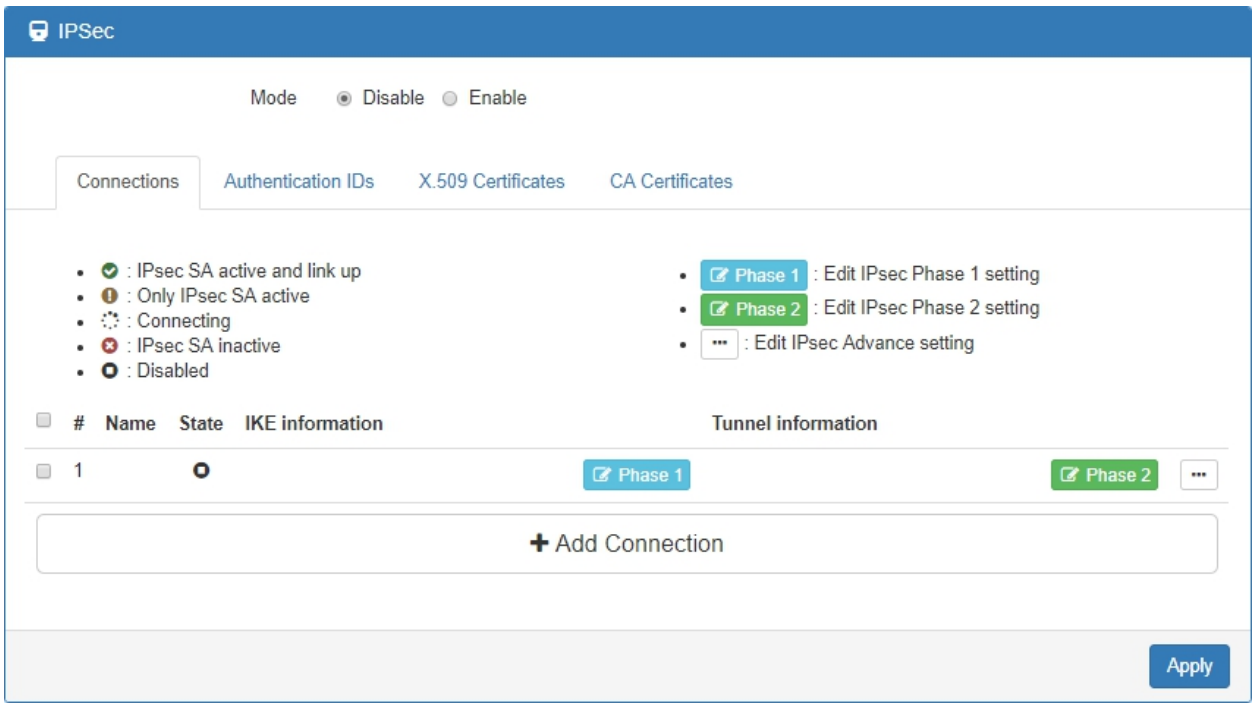
Type ◉ Policy-based ○ Route-based

VPN > IPsec > General setting	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.

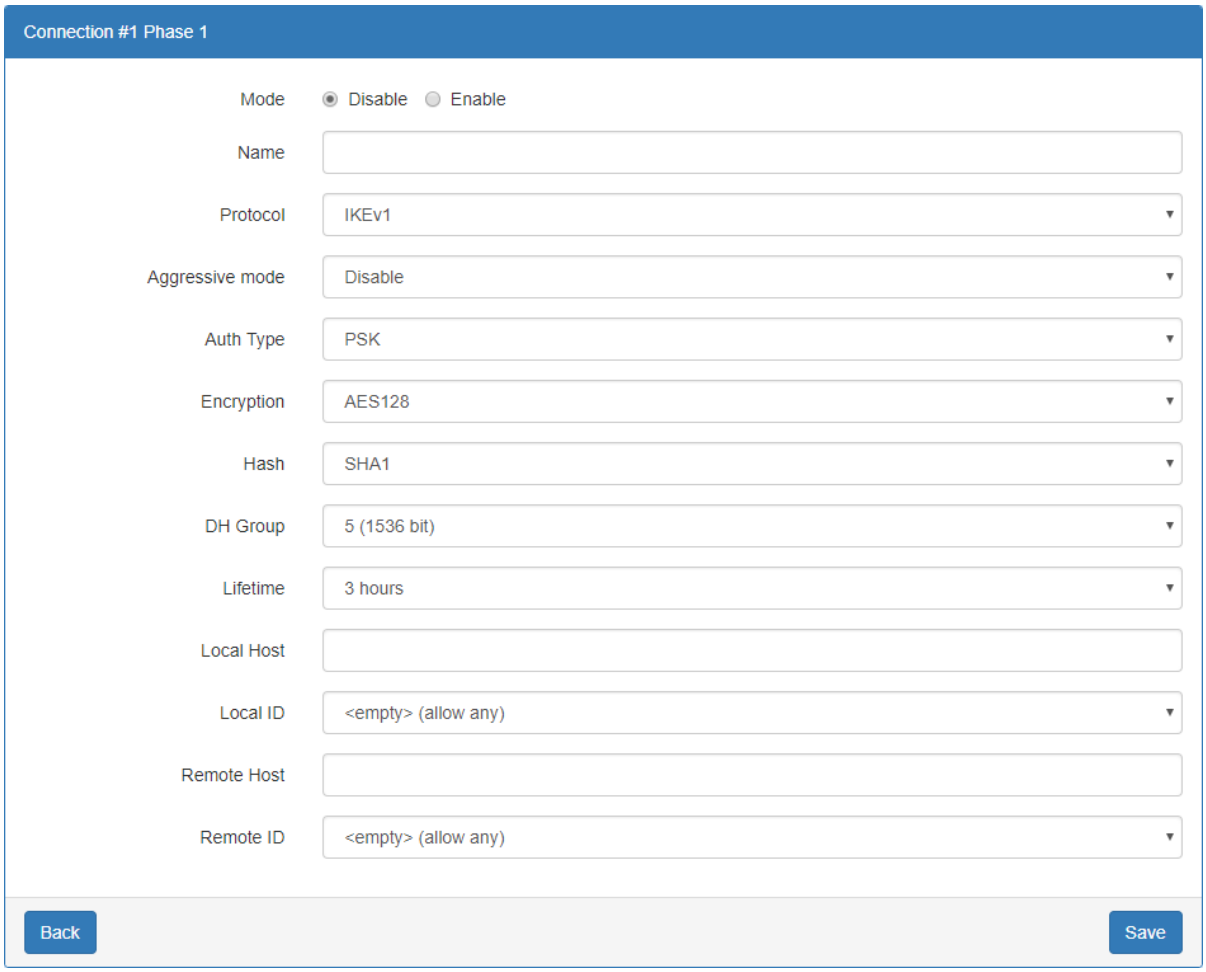
11.2.1 IPsec > Connections

This section provides the information of the IPsec connections. Each connection will show the **State**, **IKE information** and **Tunnel information**.

- In the default setting, the list of connections is empty. You can create the new connection by click + Add Connection button.
- For the edit, you can click the Phase 1 and Phase 2 buttons to edit IPsec phase 1 and phase 2 setting respectively.
- For the advance settings, like Dead Peer Detection, a.k.a DPD, you can click the ··· button to edit it.



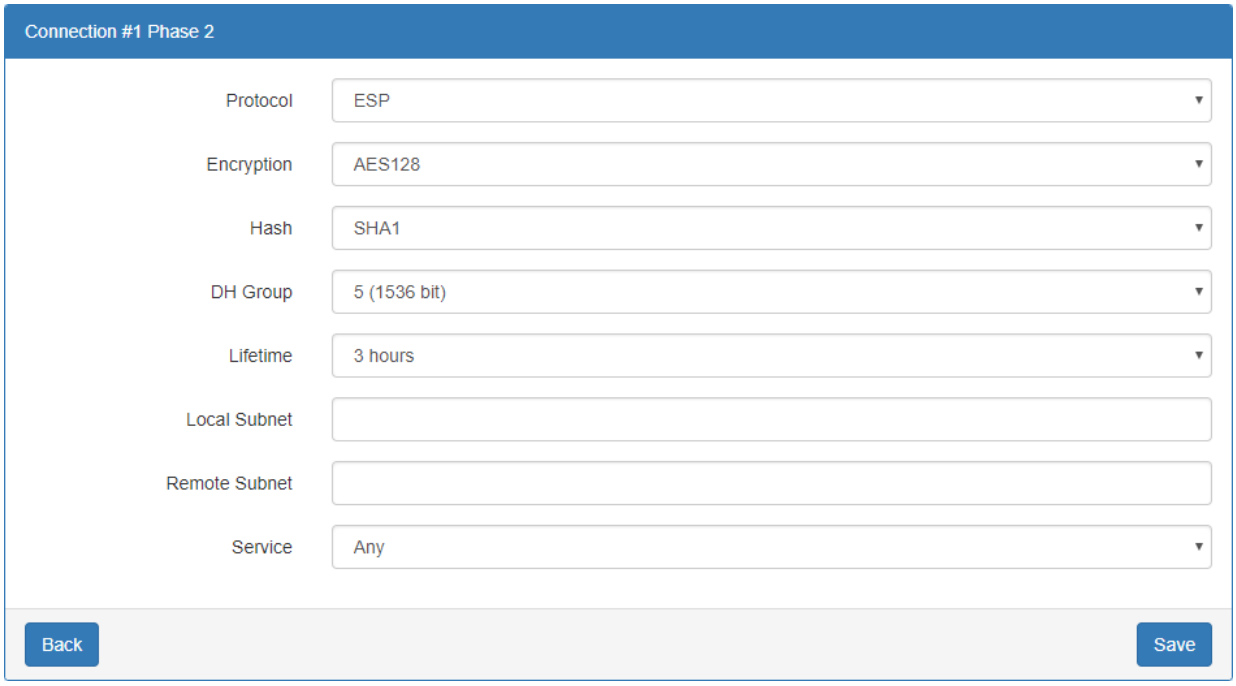
(1) IPsec Phase 1 Setting



VPN > IPsec > Connections > Phrase 1 setting	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Name	Short name or description.
Protocol	Select from IKEv1 or IKEv2. The default is IKEv1.
Aggressive mode	Select from Disable or Enable. The default is Disable. When this option be enabled, the connection will be running on IKEv1 Aggressive mode. (***Note:*** This option only work on IKEv1.)
Auth Type	Select from PSK (default), RSA, EAP-TLS. (***Note:*** The EAP-TLS is for IKEv2 only.)
Encryption	The encryption algorithm. Select from AES128 (default), AES192, AES256 or 3DES.
Hash	The integrity algorithm. Select from MD5, SHA1 (default) or SHA256.
DH Group	The Diffie Hellman 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).
Lifetime	The length of the keying channel of a connection. Select from 30 minutes, 1 hour, 2 hours, 3 hours, 6 hours, 12 hours or 24 hours.
Local Host	The IP address of the router's public network interface.

	If this value is blank, the connection will automatically detect the correct IP address.
Local ID	The identification for authentication on local peer. Select from the created authentication IDs or empty.
Remote Host	The IP address of the peer gateway's public network interface. If this value is blank, the connection will act the server role to wait the incoming request.
Remote ID	The identification for authentication on remote peer. Select from the created authentication IDs or empty.

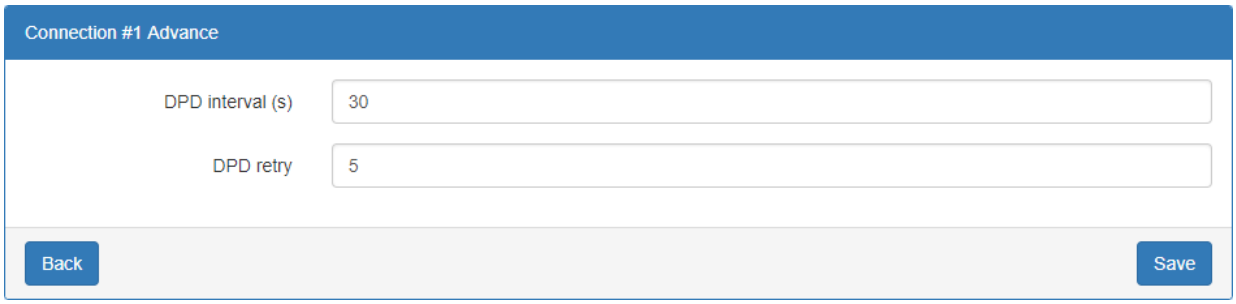
(2) IPsec Phase 2 Setting



VPN > IPsec > Connections > Phrase 2 setting	
Item	**Description**
Protocol	Only support ESP.
Encryption	The encryption algorithm. Select from AES128 (default), AES192, AES256 or 3DES.
Hash	The integrity algorithm. Select from MD5, SHA1 (default) or SHA256.
DH Group	The Diffie Hellman 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).
Lifetime	The length of a particular instance of a connection. Select from 30 minutes, 1 hour, 2 hours, 3 hours, 6 hours, 12 hours or 24 hours.
Local Subnet	The private subnet behind the router. The available formats are A.B.C.D, A.B.C.D/M, A.B::C.D or A.B::C.D/M If this value is blank, the connection will set it as the “Local Host” of Phase 1 setting. ***Note:*** This option only work on Policy-based IPsec VPN type.
Remote Subnet	The private subnet behind the peer gateway. The available formats are A.B.C.D, A.B.C.D/M, A.B::C.D or A.B::C.D/M

	If this value is blank, the connection will set it as the “Remote Host” of Phase 1 setting. ***Note:*** This option only work on Policy-based IPsec VPN type.
Service	Restrict the VPN traffic to the particular protocol only. Select from the Any, TCP, UDP or L2TP.

(3) IPsec Advance Setting



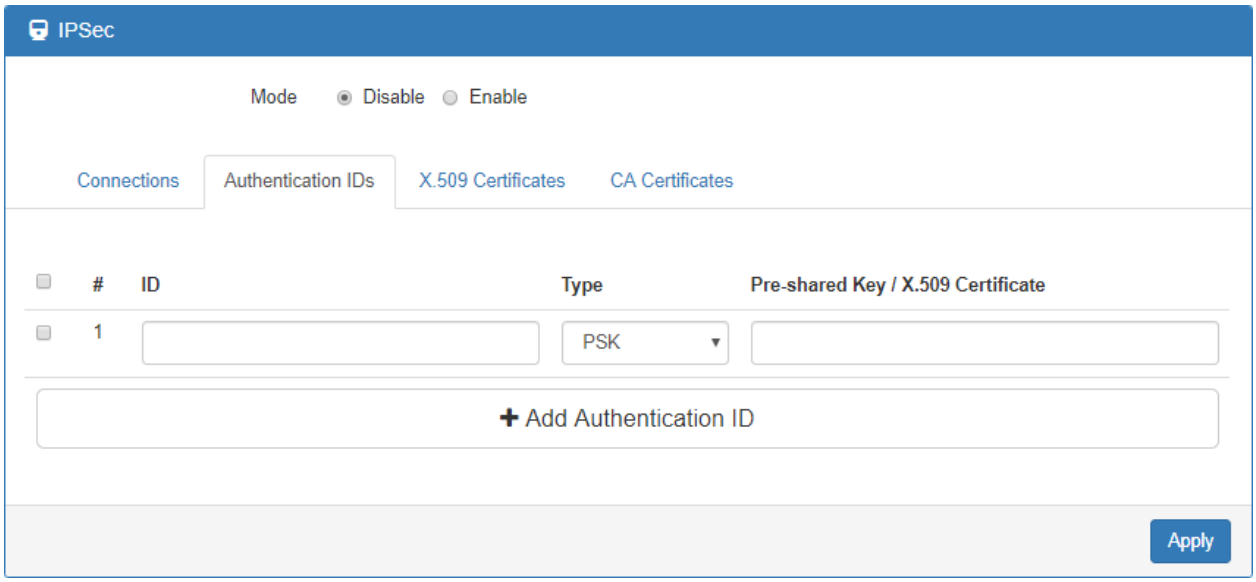
VPN > IPsec > Connections > Advance Setting	
Item	**Description**
DPD interval	The period time interval to detect dead peers. The default is 30 seconds.
DPD retry	The max number of retry of dead peer detection. The default is 5 times.

11.2.2 IPsec > Authentication IDs

This section provides the authentication ID set to authenticate the IPsec connections.

In the default setting, the list of authentication ID is empty. You can create the new authentication ID by click + Add Authentication ID button.

Note: Please apply the changes before editing the **connection** settings.



VPN > IPsec > Authentication IDs	
Item	**Description**
ID	The identification for authentication. It only work on PSK type.
Type	Select from PSK or RSA. The default is PSK. ● PSK: Use the pre-shared key to authenticate the connection. ● RSA: Use the certificate to authenticate the connection.
Pre-shared Key / X.509 Certificate	The X.509 certificate for authentication. The certificate could be generated or imported by X.509 Certificates section.

According to the above options, there are some combinations to authenticate the IPsec connection.

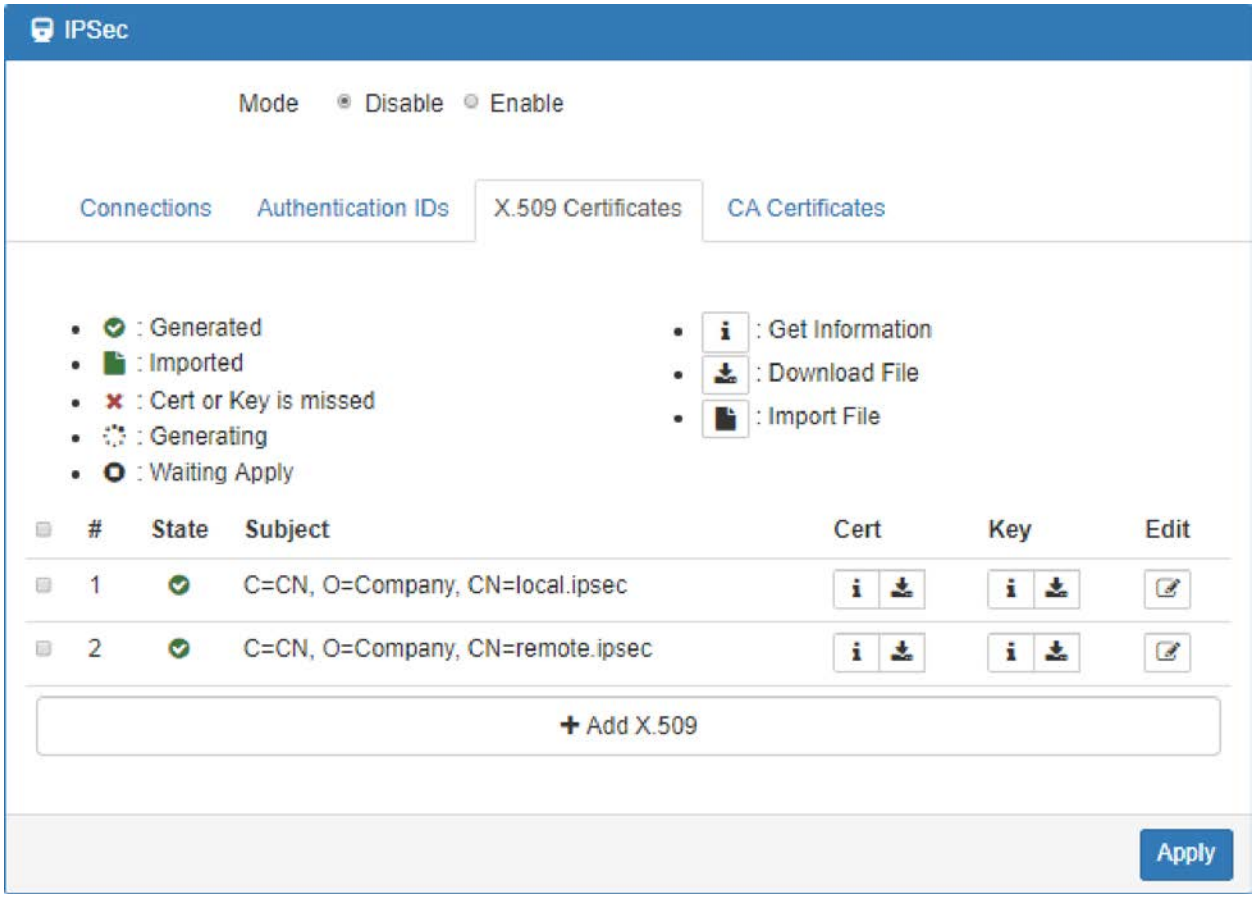
VPN > IPsec > Authentication IDs				
#	**ID**	**Type**	**Pre-shared Key / X.509 Certificate**	**Comment**
1		PSK	password	The default password for the PSK connections.
2	remote.ipsec	PSK	2wsx#EDC	The password only for the PSK connection with **remote.IPsec** ID. Normally, this case will be used to authenticate peer gateway.
3	local.ipsec	PSK		The identification for the connection. Normally, this case will be used to announce the ID of the router.
4	test	RSA	**created X.509**	The ID field will be omitted, and use the common name(CN) of X.509 as the ID field.

11.2.3 IPsec > X.509 Certificates

This section provides the certificates setting which could be used by IPsec authentication ID.

Each certificate will show the **State** and **Subject** information and provide the controlling buttons to let user import, download or edit the certificate/key files.

Note: Please apply the changes before editing the **Authentication IDs settings**.

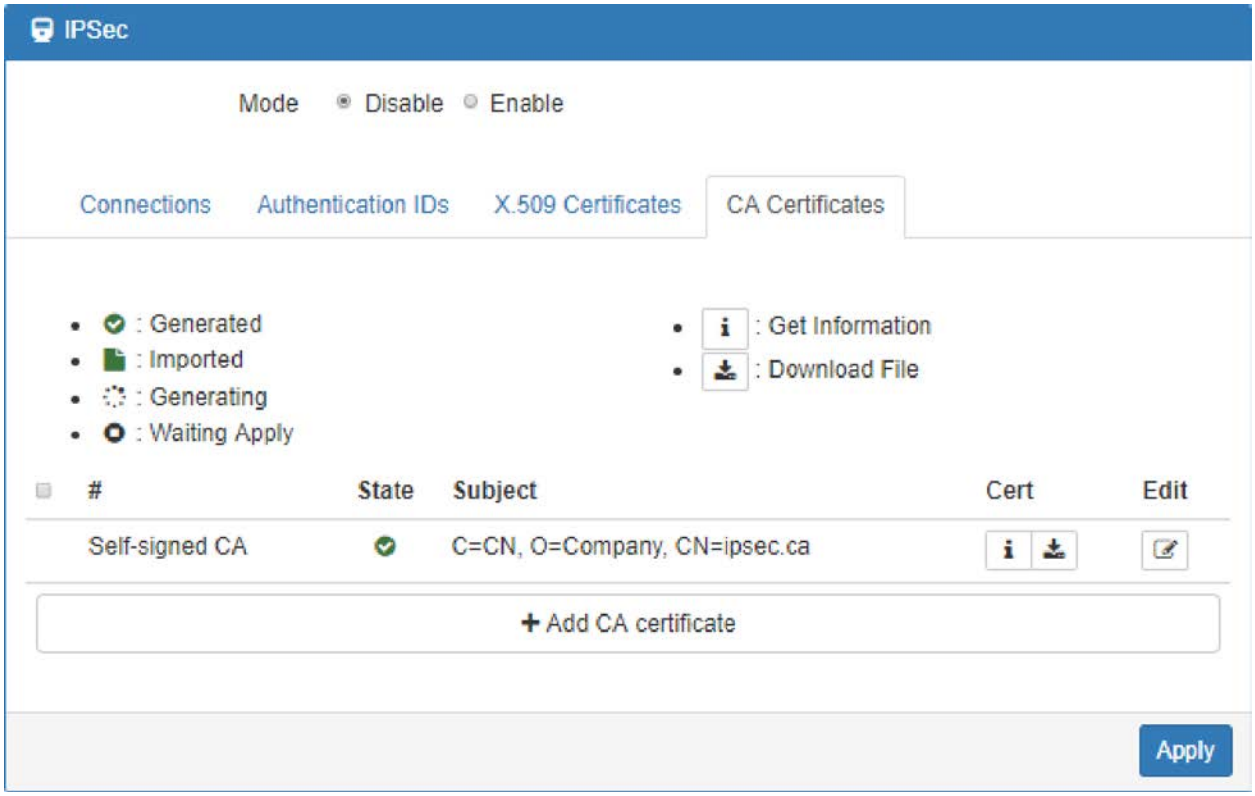


11.2.4 IPsec > CA Certificates

This section provides the CA certificates setting which could check whether the X.509 certificate is valid or not.

There is one self-signed CA (generated by the router), and it supports the user import the self-signed CAs to the router. The self-signed CA will help the router to verify the self-signed X.509 certificate which is imported on X.509 Certificates section.

Each CA certificate will show the **State** and **Subject** information and provide the controlling buttons to let user could download or edit the certificate / key files.



Certificate Generation

There are two kinds of certificate generated by router, one is self-signed CA, the other is X.509.

To generate the self-signed CA certificate:

1. Navigate to CA Certificates tab.
2. Click the edit button to navigate the **Certificate Setting** page.
3. Fill up the information of the CA certificate.
4. Click the Generate Certificate button and Save.
5. Click the Apply button to apply the changes.

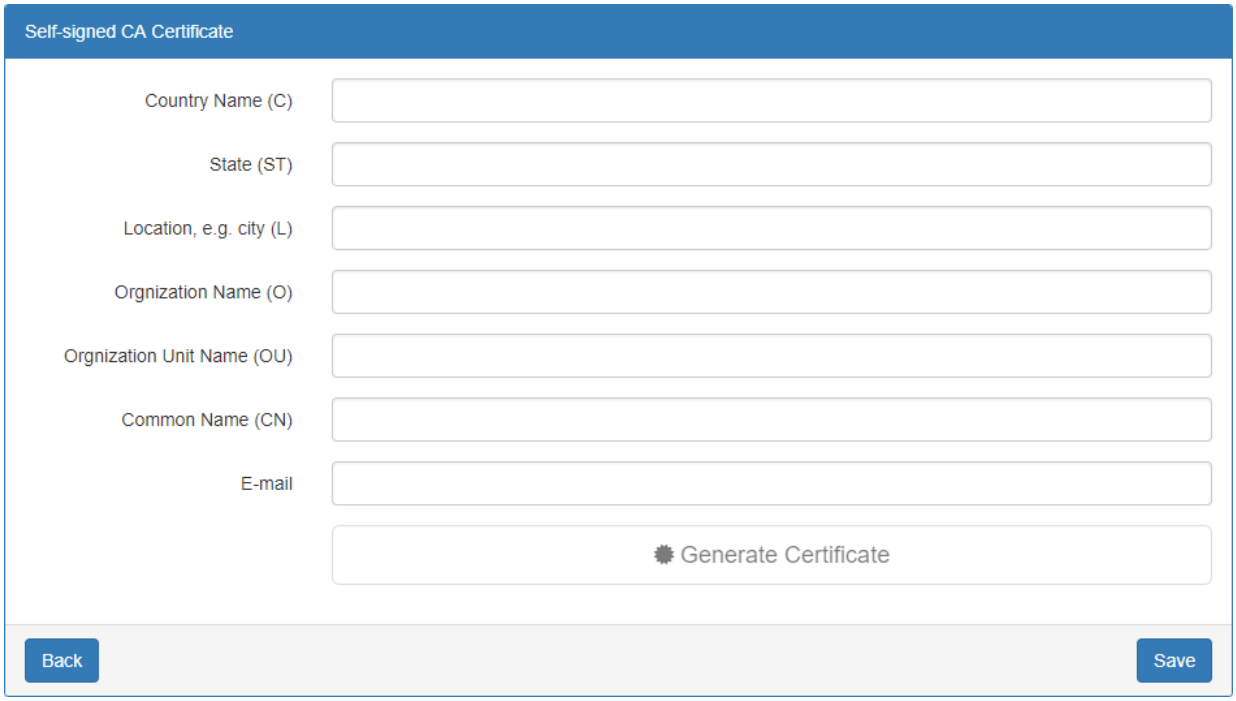
To generate the X.509 certificate:

1. Make sure the self-signed CA certificate generated.
2. Navigate to X.509 Certificates tab.
3. Add the new X.509 certificate by + Add X.509 button. (If it's not existed.)

4. Click the Edit button to navigate the **Certificate Setting** page.
5. Fill up the information of the X.509 certificate.
6. Click the Generate Certificate button and Save.
7. Click the Apply button to apply the changes.

Certificate Setting

VPN > IPsec > CA Certificates	
Item	**Description**
Country Name	The 2-letter country code. e.g. US This option is required for certificate generation.
State	The state name. e.g. Some-State
Location	The location name. e.g. city-name
Organization Name	The organization name. e.g. company-name This option is required for certificate generation.
Organization Unit Name	The organization unit name.
Common Name	The host name associated with the certificate. e.g. example.com This option is required for certificate generation.
E-mail	The maintainer's E-mail.



Certificate Importing

Same as the **Certificate Generation**, the router supports the CA and X.509 certificate importing.

To import the CA certificate:

1. Navigate to CA Certificates tab.
2. Click the + Add CA certificate button.
3. Select the CA certificate file from browser window.
4. When the file be selected and everything all right, the newly CA certificate will show the CA certificate list with **Imported** state.

To import the X.509 certificate:

1. Navigate to X.509 Certificates tab.
2. Click the + Add X.509 button. The list will pop up the blank X.509 entry.
3. Click the Cert Import button.
4. Select the X.509 certificate file from browser window.
5. When the file be selected and everything all right, the state should be **Cert or Key is missed**.
6. Click the **Key Import** button.
7. Select the X.509 key file from browser window.
8. When the state shown **Imported**, the importing procedure is completed.

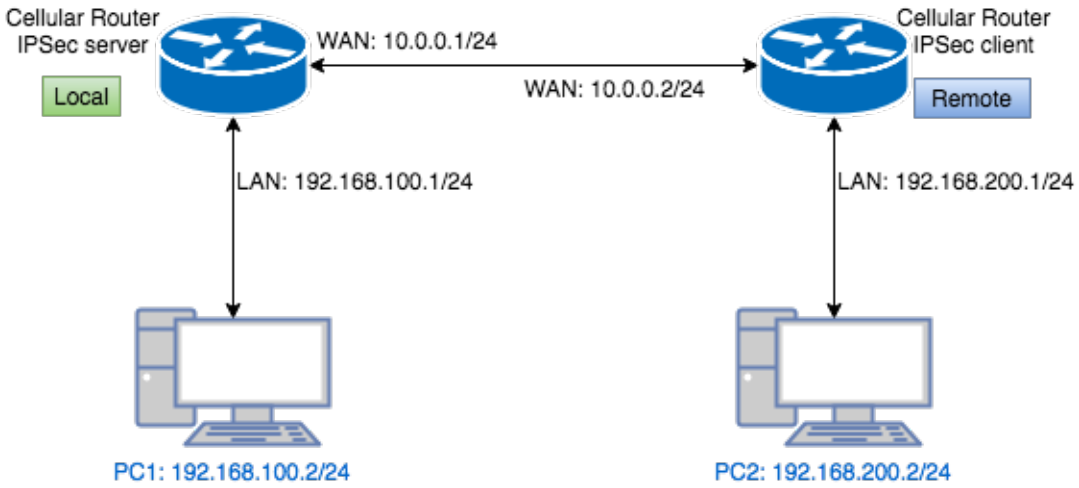
Download the certificate

If the certificate is generated or imported, there will be the download button to download each certificate and key file.

Note: When the connection is authenticated by RSA or EAP-TLS, the user must download the X.509 certificate, key and CA certificate, and import the files to the remote gateway.

11.2.5 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.

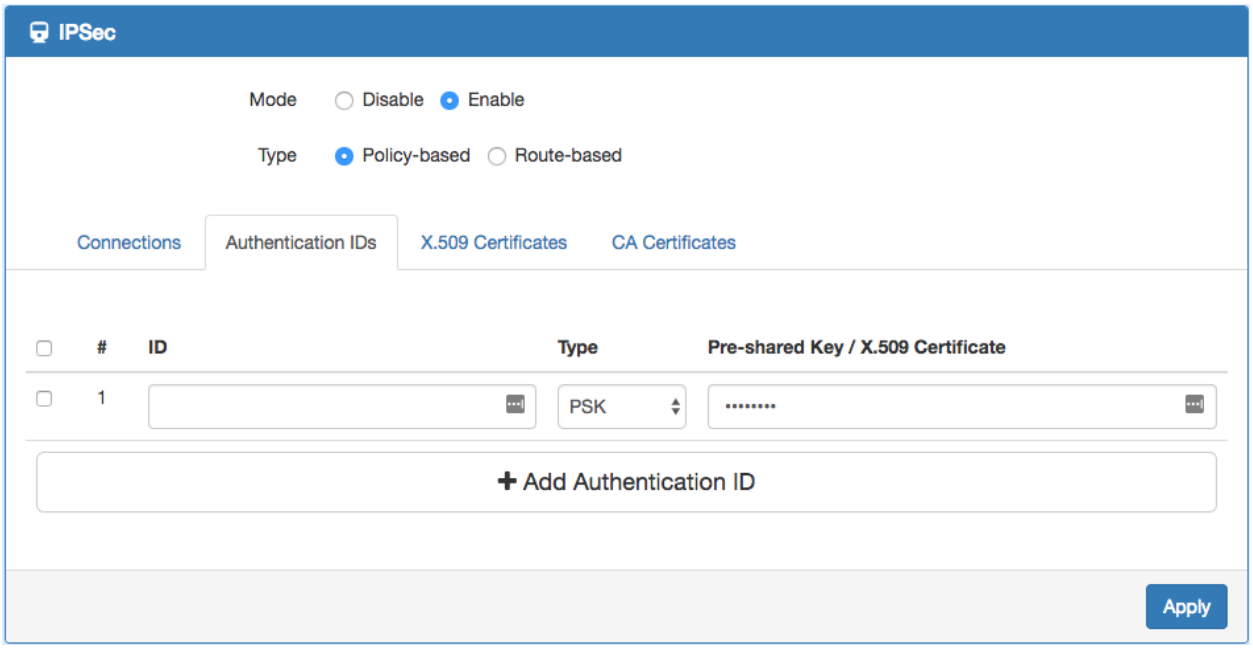


- **Pre-shared Key authentication**

Configure Net-to-Net VPN Server

1. Change **Mode** from Disable to **Enable**.
2. Navigate to the Authentication IDs tab.
3. Add the authentication ID
   - Keep **ID** as blank, **Type** as **PSK** and fill the password to **Pre-shared Key** field.
4. Apply the changes
5. Navigate to the Connections tab.

6. Add IPsec connection
   (1) Edit the phase 1 setting
   (2) Change **Mode** from Disable to **Enable**.
   (3) Save the changes.
   (4) Edit the phase 2 setting
   (5) Fill up the **Local Subnet** and **Remote Subnet**.
      - e.g. Local Subnet: 192.168.100.0/24, Remote Subnet: 192.168.200.0/24
   (6) Save the changes
7. Apply the changes



Connection #1 Phase 1

Mode	○ Disable ● Enable
Name	
Protocol	IKEv1
Aggressive mode	Disable
Auth Type	PSK
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	3 hours
Local Host	
Local ID	<empty> (allow any)
Remote Host	
Remote ID	<empty> (allow any)

Back Save

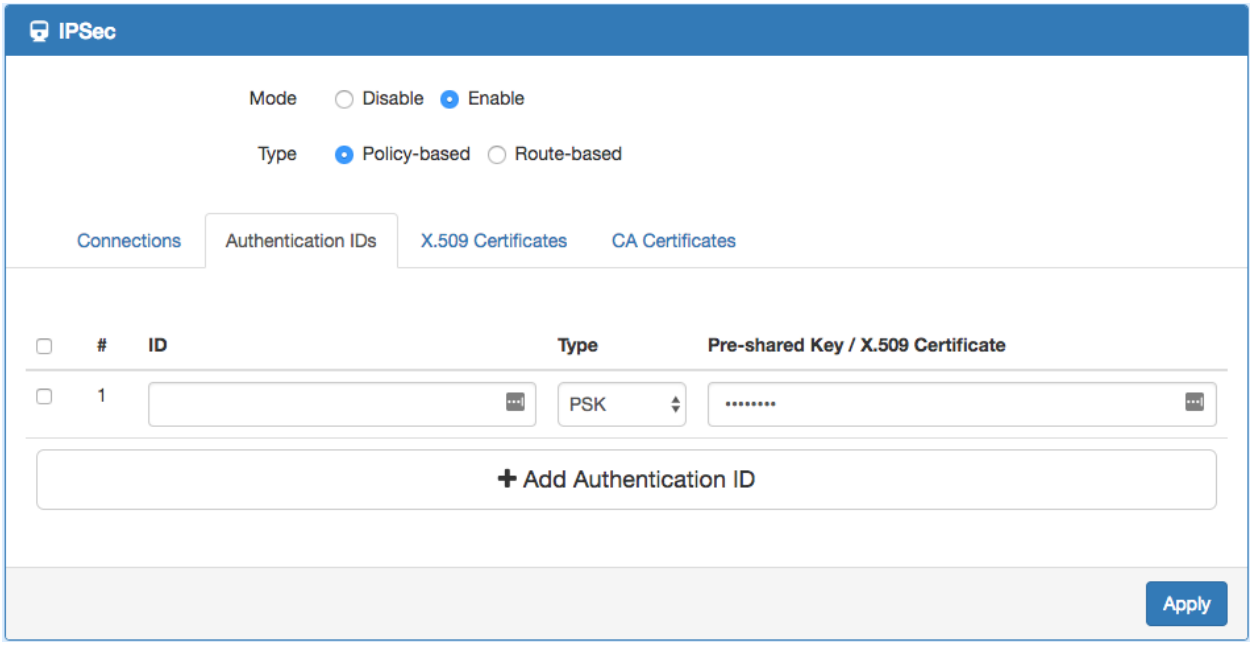
Connection #1 Phase 2

Protocol	ESP
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	2 hours
Local Subnet	192.168.100.0/24
Remote Subnet	192.168.200.0/24
Service	Any

Back Save

Configure Net-to-Net VPN Client

1. Change **Mode** from Disable to **Enable**.
2. Navigate to the Authentication IDs tab.
3. Add the authentication ID
   - Keep **ID** as blank, **Type** as **PSK** and fill the password to **Pre-shared Key** field.
4. Apply the changes
5. Navigate to the Connections tab.
6. Add IPsec connection
   (1) Edit the **phase 1** setting
   (2) Change **Mode** from Disable to **Enable**.
   (3) Fill the IP address of VPN server to **Remote Host** Field.
   - e.g. Remote Host: 10.0.0.1
   (4) Save the changes
   (5) Edit the **phase 2** setting
   (6) Fill up the **Local Subnet** and **Remote Subnet**.
   - e.g. Local Subnet: 192.168.200.0/24, Remote Subnet: 192.168.100.0/24
   (7) Save the changes
7. Apply the changes



Connection #1 Phase 1

Mode	○ Disable ● Enable
Name	
Protocol	IKEv1
Aggressive mode	Disable
Auth Type	PSK
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	3 hours
Local Host	
Local ID	<empty> (allow any)
Remote Host	10.0.0.1
Remote ID	<empty> (allow any)

Back Save

Connection #1 Phase 2

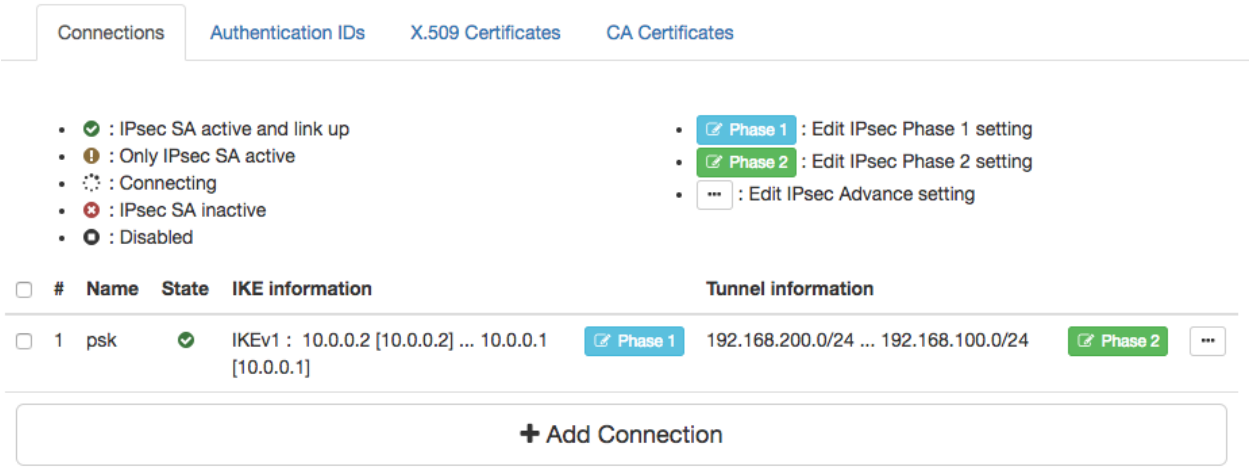
Protocol	ESP
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	2 hours
Local Subnet	192.168.200.0/24
Remote Subnet	192.168.100.0/24
Service	Any

Back Save

IPsec Net-to-Net with Pre-shared Key result

- Server

- Client

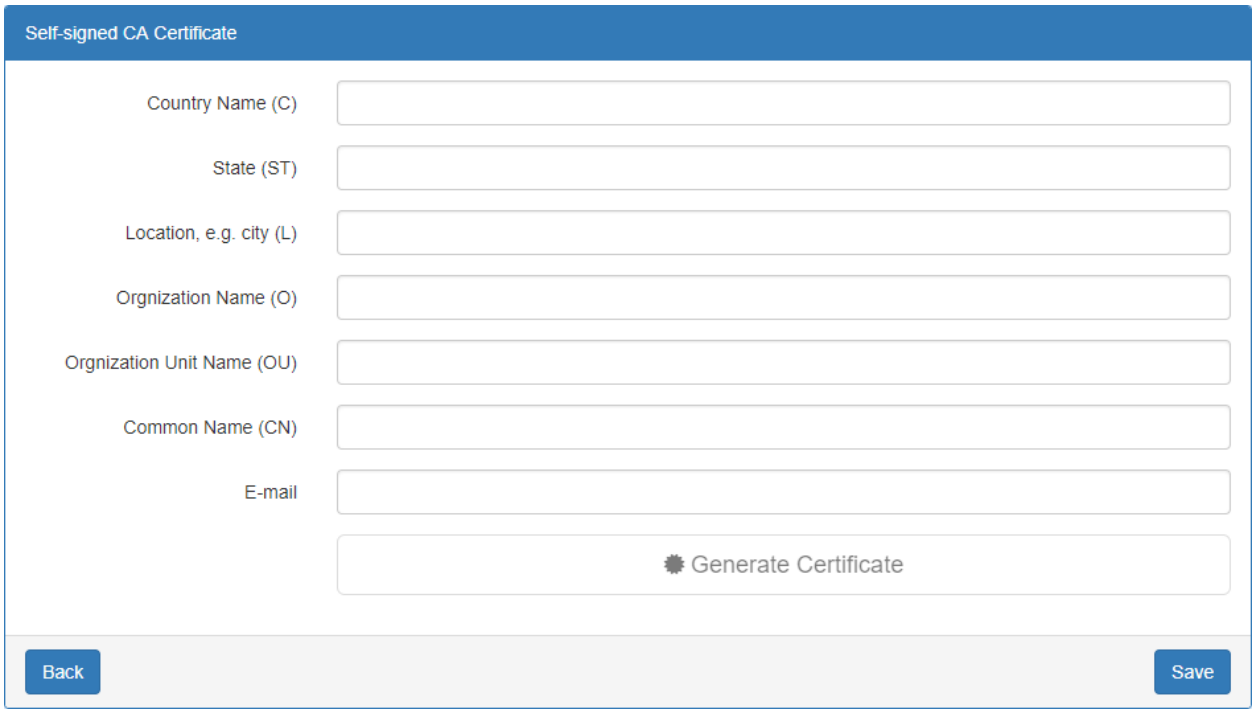


- **RSA authentication - Server**

Prepare the self-signed CA certificate

1. Navigate to the CA Certificates tab.
2. Edit the self-signed CA. (Skip it if the self-signed CA is generated.)
   (1) Fill the information of the self-signed CA
   (2) **Country Name**: CN
   (3) **Organization Name**: Company
   (4) **Common Name**: IPsec.ca
   (5) Click the Generate Certificate button
   (6) Save the changes
3. The **State** of self-signed CA will be **Waiting Apply**
4. Apply the changes

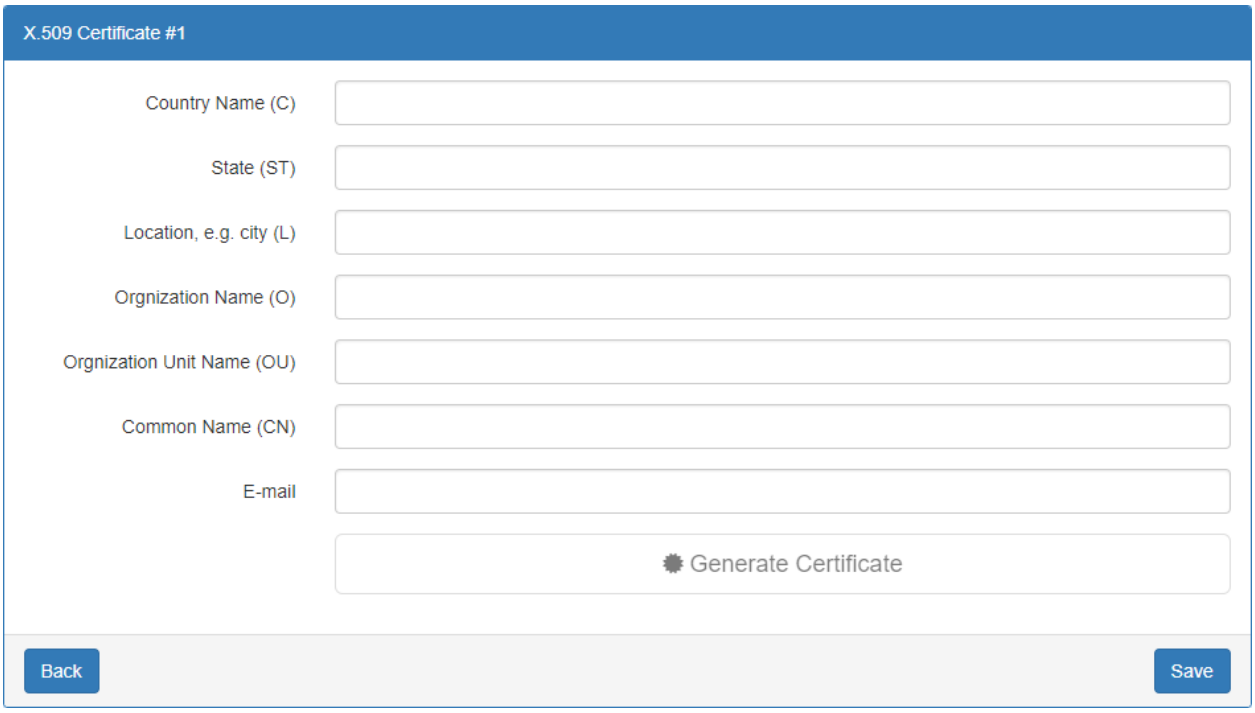
5. Waiting for the **State** of self-signed CA become generated
6. Refresh the page

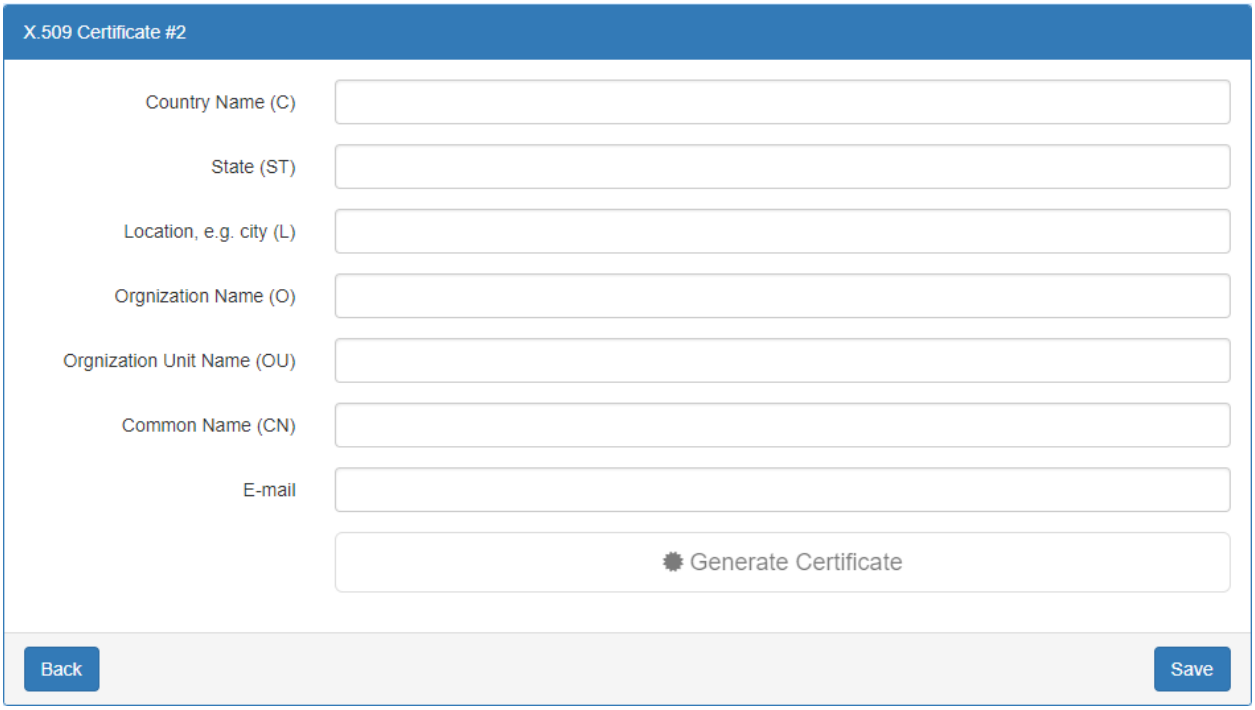


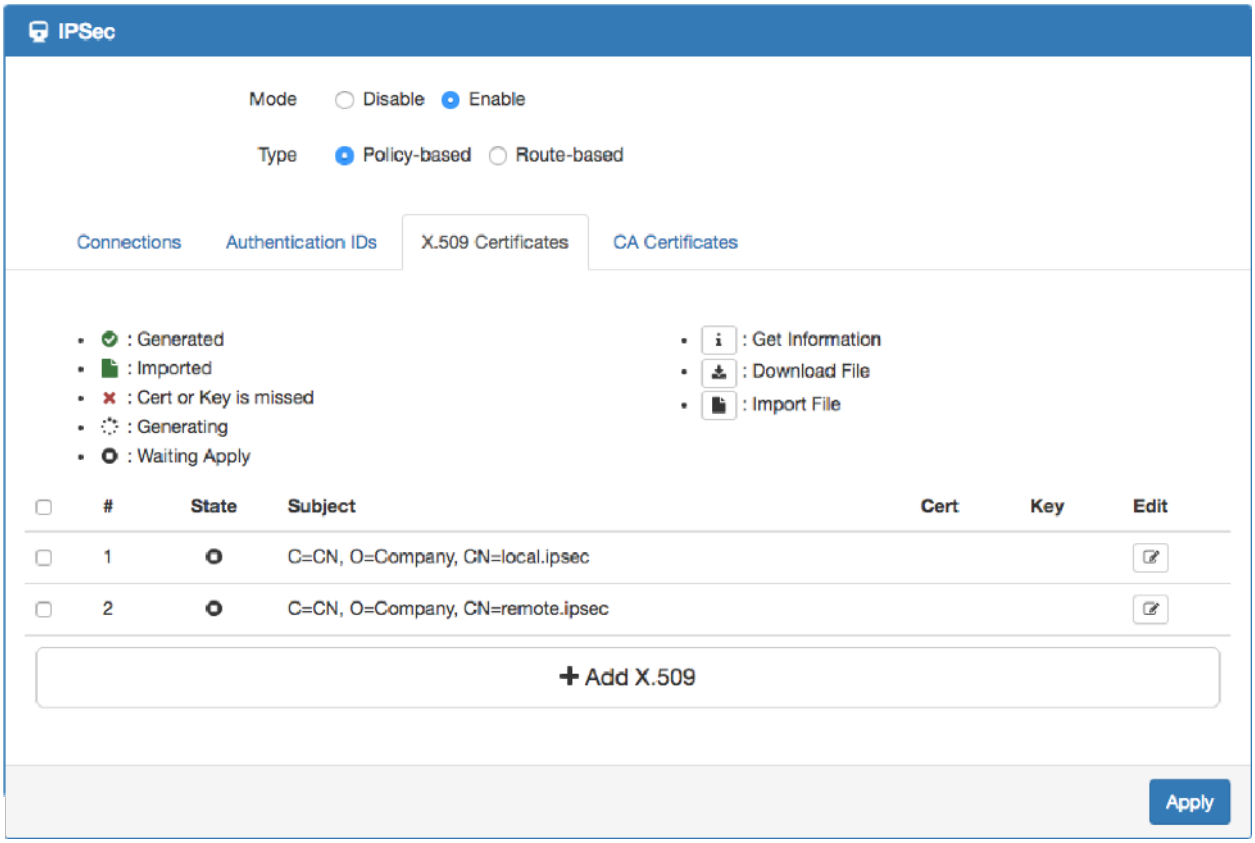
Prepare the X.509 certificates

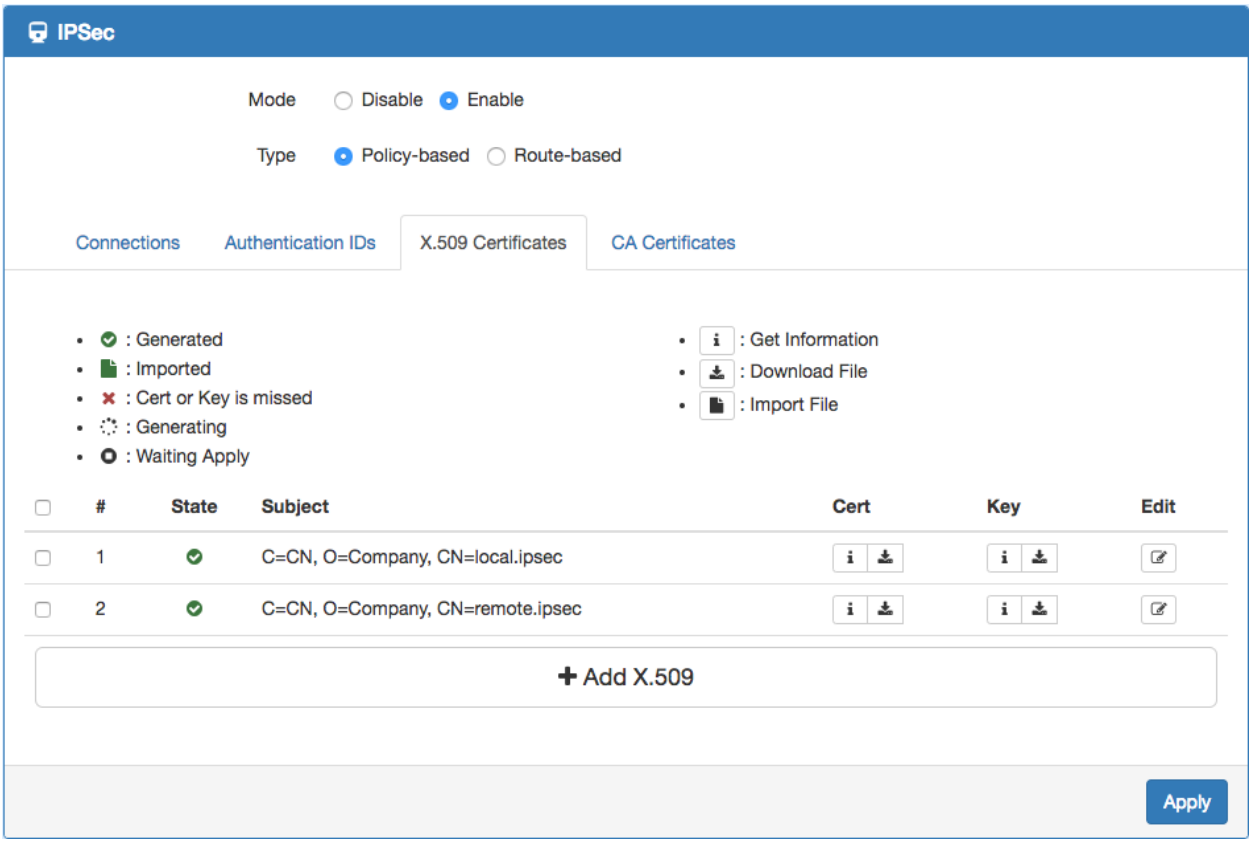
1. Navigate to the X.509 Certificates tab.
2. Click the add button to add the X.509 certificate
3. Edit the newly X.509 certificate for the local router.
   (1) Fill the information of the X.509 certificate
   (2) **Country Name**: CN
   (3) **Organization Name**: Company
   (4) **Common Name**: local.IPsec
   (5) Click the Generate Certificate button
   (6) Save the changes
4. Click the add button to add the X.509 certificate
5. Edit the newly X.509 certificate for the remote router.
   (1) Fill the information of the X.509 certificate
   (2) **Country Name**: CN
   (3) **Organization Name**: Company
   (4) **Common Name**: remote.IPsec
   (5) Click the Generate Certificate button
   (6) Save the changes
6. Apply the changes

7. Waiting for the **State** of X.509 Certificate become generated



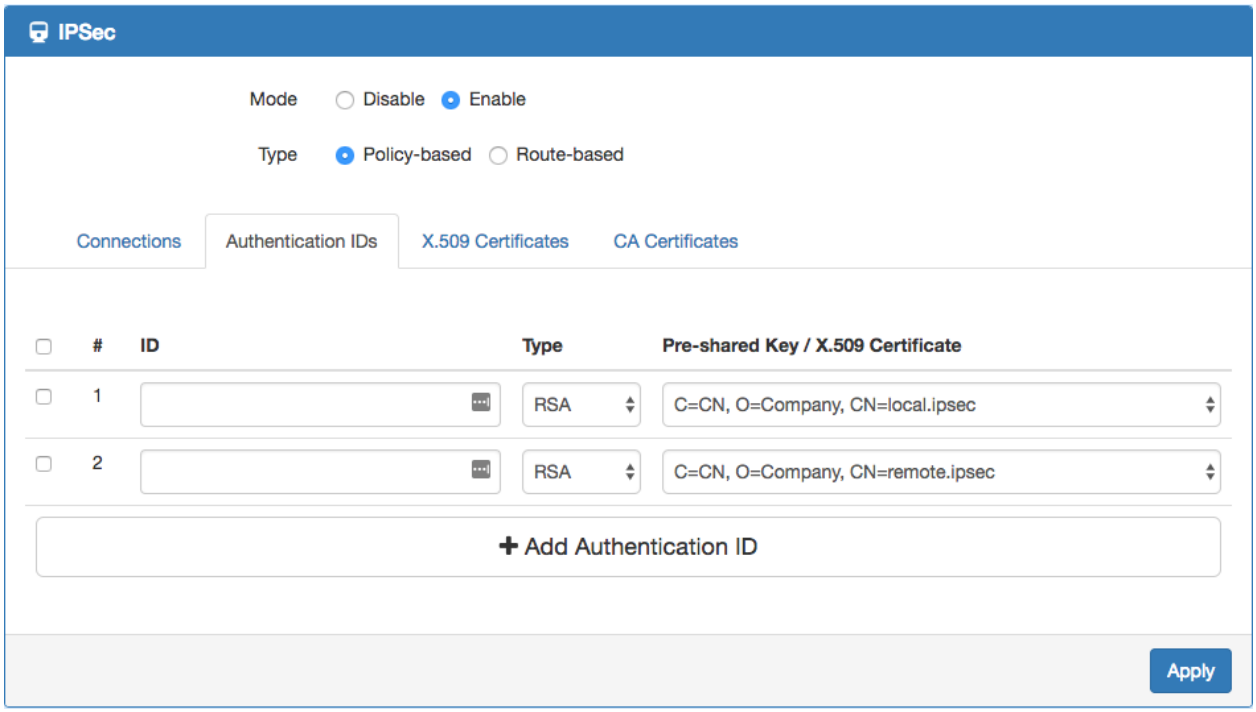



IPSec
Mode
Disable
Enable
Type
Policy-based
Route-based
Connections
Authentication IDs
X.509 Certificates
CA Certificates
: Generated
: Imported
: Cert or Key is missed
: Generating
: Waiting Apply
: Get Information
: Download File
: Import File
State Subject Cert Key Edit
1 C=CN, O=Company, CN=local.ipsec
2 C=CN, O=Company, CN=remote.ipsec
+ Add X.509
Apply


IPSec
Mode
Disable
Enable
Type
Policy-based
Route-based
Connections
Authentication IDs
X.509 Certificates
CA Certificates
: Generated
: Imported
: Cert or Key is missed
: Generating
: Waiting Apply
: Get Information
: Download File
: Import File
State Subject Cert Key Edit
1 C=CN, O=Company, CN=local.ipsec
2 C=CN, O=Company, CN=remote.ipsec
+ Add X.509
Apply

Prepare the authentication IDs

1. Navigate to the Authentication IDs tab.
2. Add tow authentication IDs
   - Keep first one's **ID** as blank, **Type** as **RSA** and select the **C=CN, O=Company, CN=local.IPsec** X.509 certificate.
   - Keep second one's **ID** as blank, **Type** as **RSA** and select the **C=CN, O=Company, CN=remote.IPsec** X.509 certificate.
3. Apply the changes



Setup the connection on VPN server

1. Change **Mode** from Disable to **Enable**.
2. Navigate to the Connections tab.
3. Add IPsec connection
   (1) Edit the phase 1 setting
   (2) Change **Mode** from Disable to **Enable**.
   (3) Change **Auth Type** from PSK to **RSA**.
   (4) Change the **Local ID** and select the **local.IPsec (RSA)** authentication ID.
   (5) Save the changes
   (6) Edit the phase 2 setting
   (7) Fill up the **Local Subnet** and **Remote Subnet**.
      - e.g. Local Subnet: 192.168.100.0/24, Remote Subnet: 192.168.200.0/24
   (8) Save the changes

4. Apply the changes

Connection #1 Phase 1

Mode	○ Disable ● Enable
Name	
Protocol	IKEv1
Aggressive mode	Disable
Auth Type	RSA
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	3 hours
Local Host	
Local ID	ID#1: local.ipsec (RSA)
Remote Host	
Remote ID	<empty> (allow any)

Back Save

Connection #1 Phase 2

Protocol	ESP
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	3 hours
Local Subnet	192.168.100.0/24
Remote Subnet	192.168.200.0/24
Service	Any

Back Save

- **RSA authentication – Client**

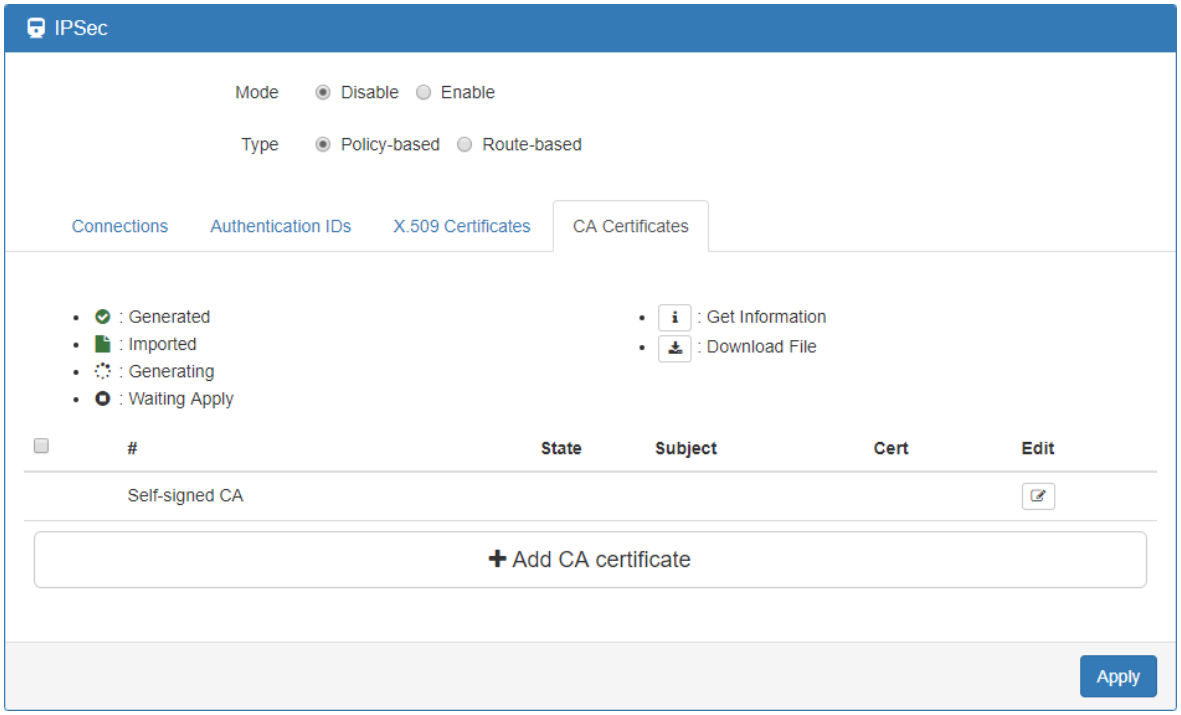
Prerequisite for VPN Client with RSA authentication

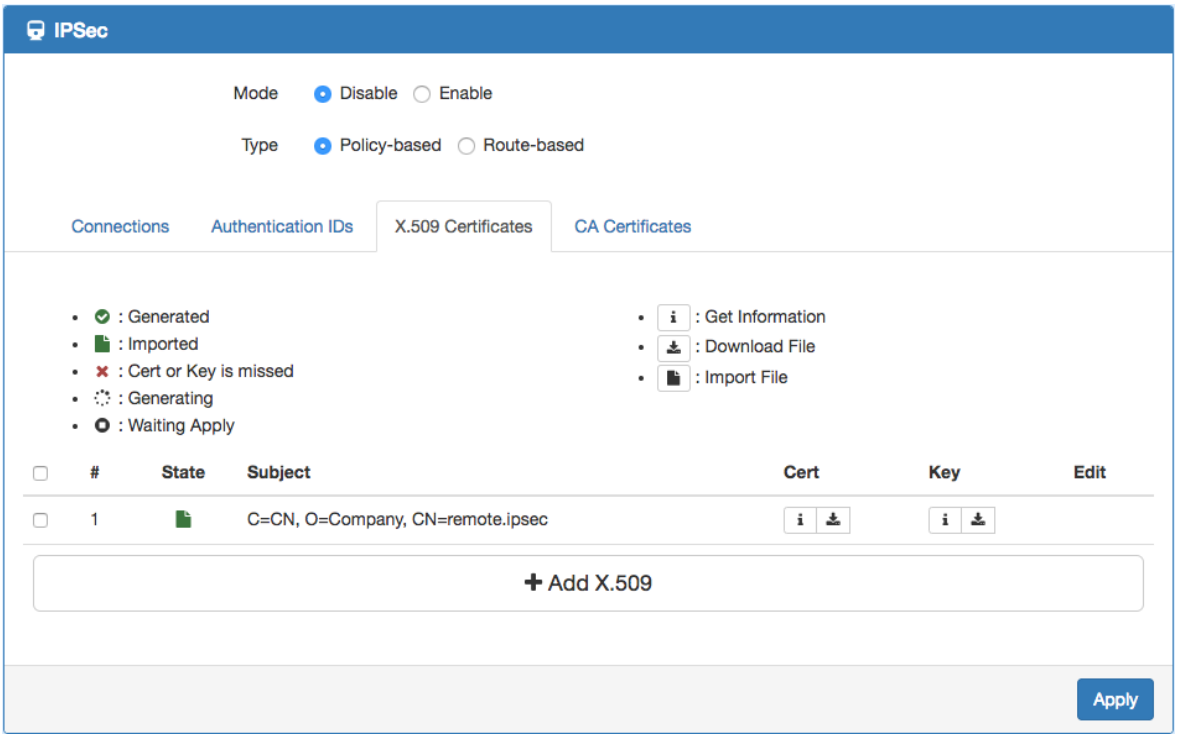
1. The self-signed CA certificate which generated by VPN server
2. The X.509 certificate and key for remote router which generated by VPN server

These files could be downloaded from VPN server. The detail could reference " How to download the certificate section " of user manual.

Import the CA certificate and the X.509 certificate

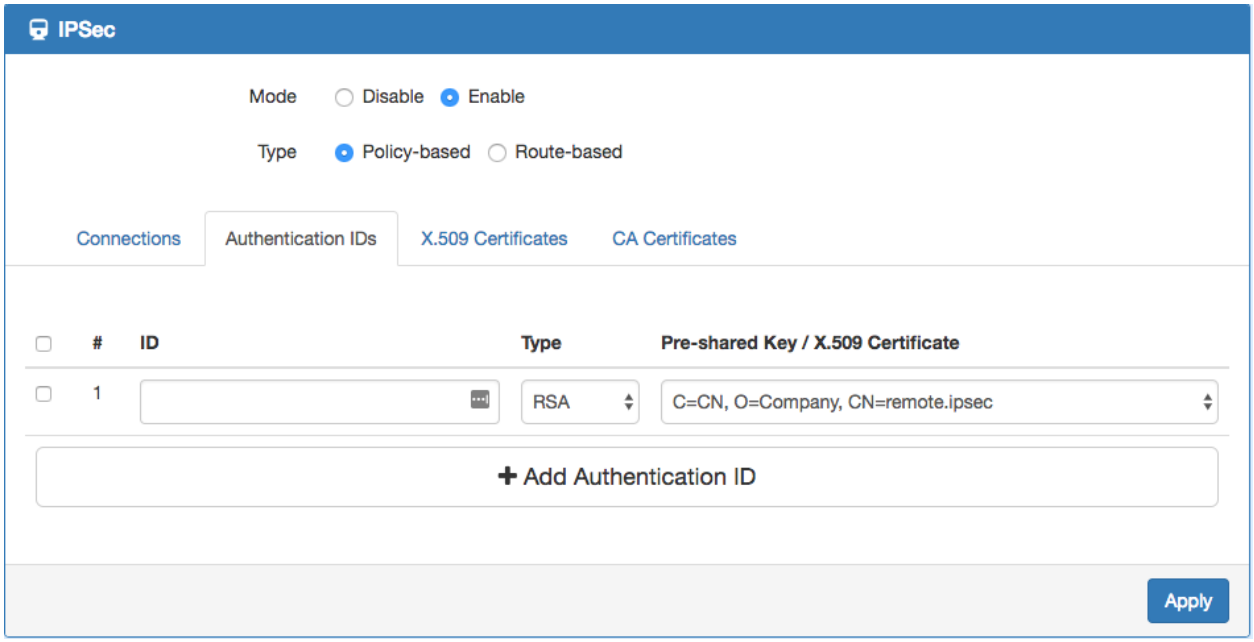
Please refer the **Certificate Importing** section of user manual to import the required files.





Setup the connection on VPN client

1. Change **Mode** from Disable to **Enable**.
2. Navigate to the Authentication IDs tab.
3. Add one authentication ID
   - Keep second one's ID as blank, Type as RSA and select the C=CN, O=Company, CN=remote.IPsec X.509 certificate.
4. Apply the changes
5. Navigate to the Connections tab.
6. Add IPsec connection
   (1) Edit the **phase 1** setting
   (2) Change **Mode** from Disable to **Enable**.
   (3) Change **Auth Type** from PSK to **RSA**.
   (4) Change the **Local ID** and select the **remote.IPsec (RSA)** authentication ID.
   (5) Fill the IP address of VPN server to **Remote Host** field.
      - e.g. Remote Host: 10.0.0.1
   (6) Save the changes
   (7) Edit the **phase 2** setting
   (8) Fill up the **Local Subnet** and **Remote Subnet**.
      - e.g. Local Subnet: 192.168.200.0/24, Remote Subnet: 192.168.100.0/24
   (9) Save the changes
7. Apply the changes



ADVICE

Connection #1 Phase 1

Mode	○ Disable ● Enable
Name	
Protocol	IKEv1
Aggressive mode	Disable
Auth Type	RSA
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	3 hours
Local Host	
Local ID	ID#1: remote.ipsec (RSA)
Remote Host	10.0.0.1
Remote ID	<empty> (allow any)

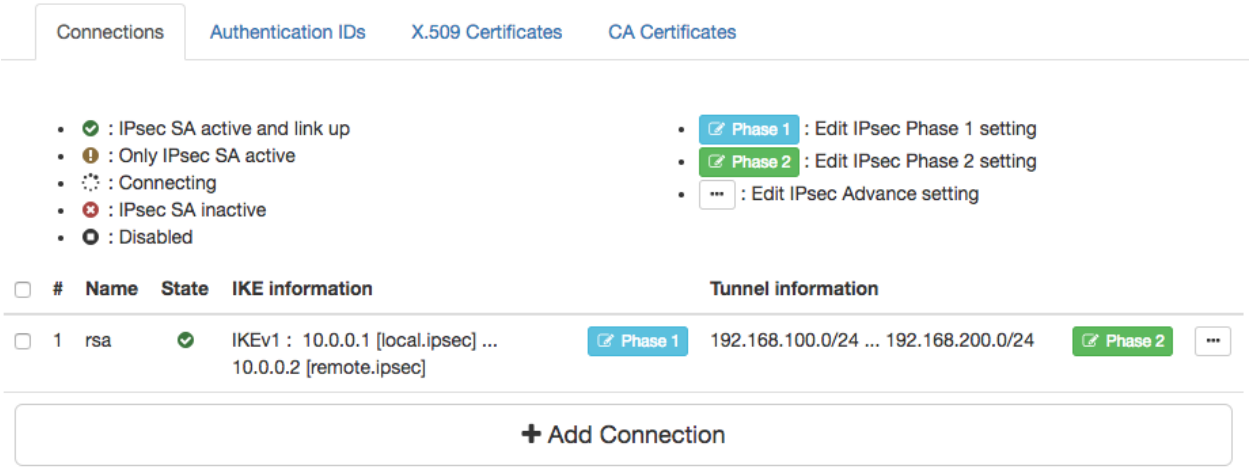
Back Save

Connection #1 Phase 2

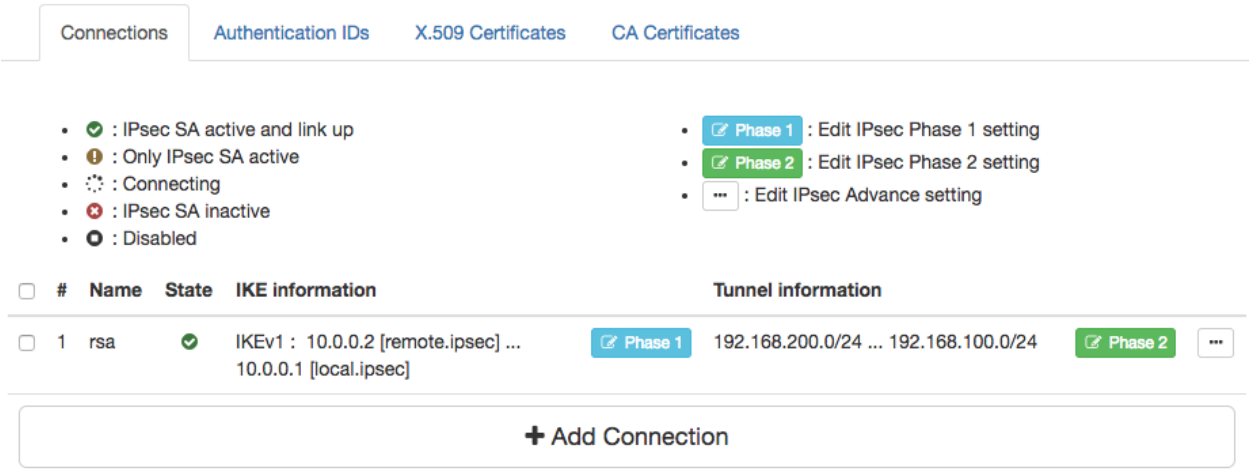
Protocol	ESP
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	3 hours
Local Subnet	192.168.200.0/24
Remote Subnet	192.168.100.0/24
Service	Any

Back Save

- **IPsec Net-to-Net with RSA authentication result**
  - Server



  - Client



11.3 VPN > GRE

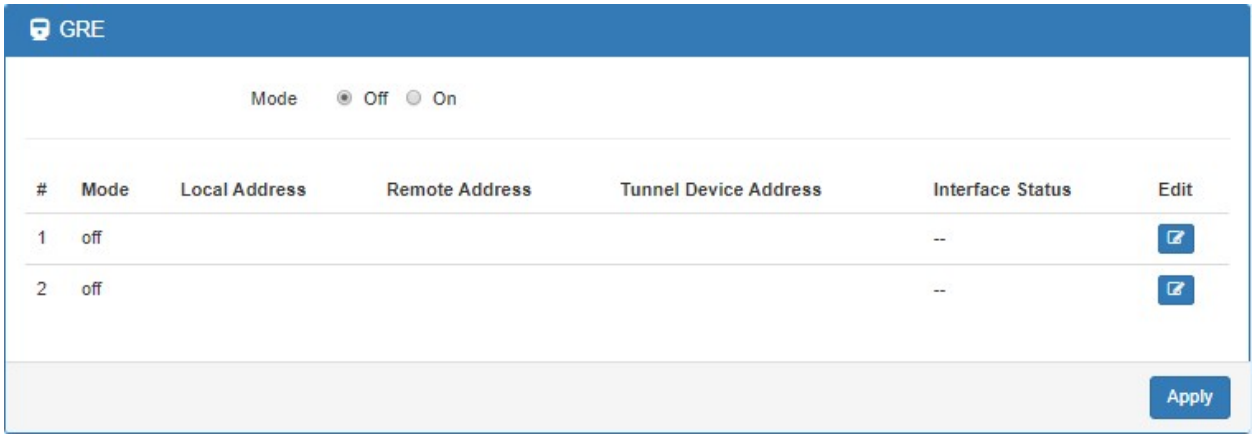
This section allows you to set **GRE configuration**. The default mode is off.

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.

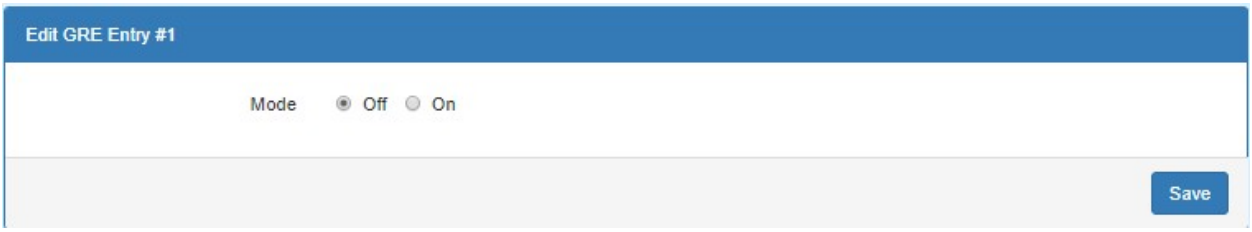
- GRE Tunnel interface comes up as soon as it is configured.
- Local endpoint does not bring the interface down if the remote endpoint is unreachable.
- No way to determine problems in the intervening network.
- Keepalives are used to solve this issue.

The GRE Tunnel Keepalive feature provides the capability of configuring keepalive packets to be sent over IP-encapsulated GRE tunnels. You can specify the rate at which keepalives will be sent and the number of times that a device will continue to send keepalive packets without a response before the interface becomes inactive. GRE keepalive packets may be sent from both sides of a tunnel or from just one side.

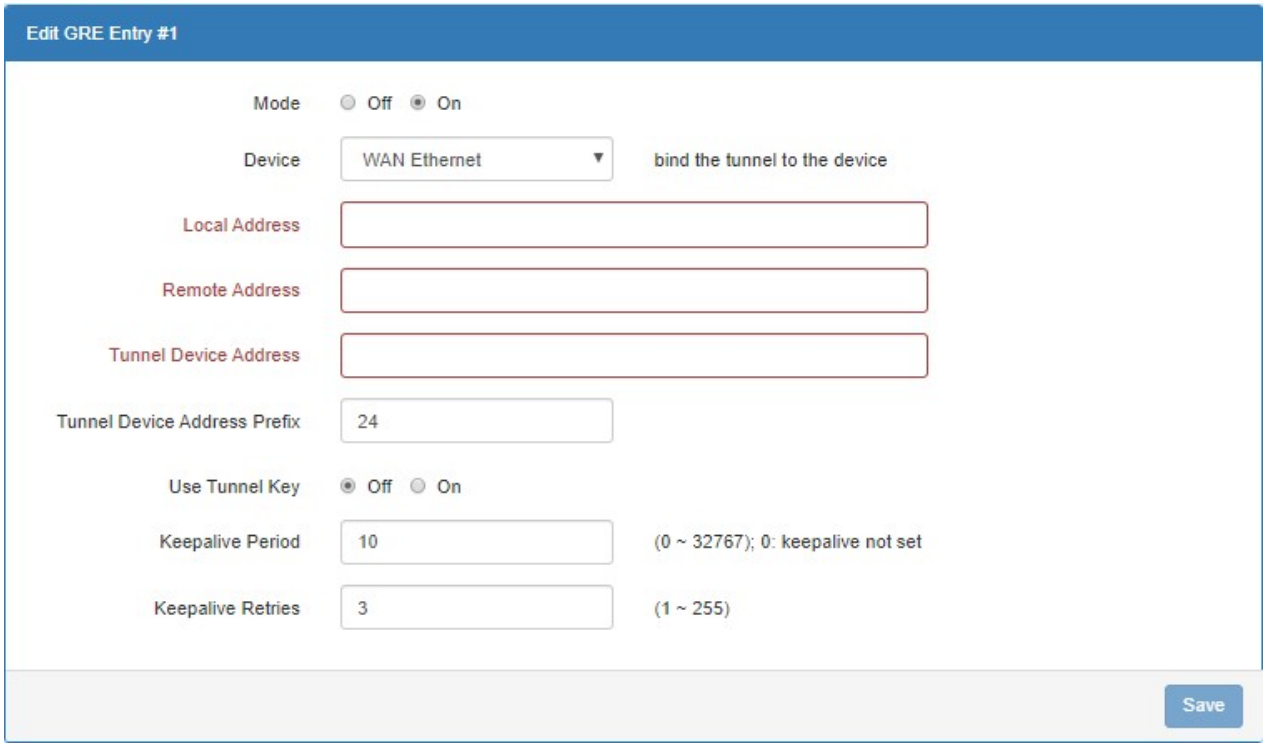
There are 2 entry for user to configure, please press Edit button.



While clicking Edit button, it shows Off or On mode. Please select On to display setting items.



The GRE Mode is On.

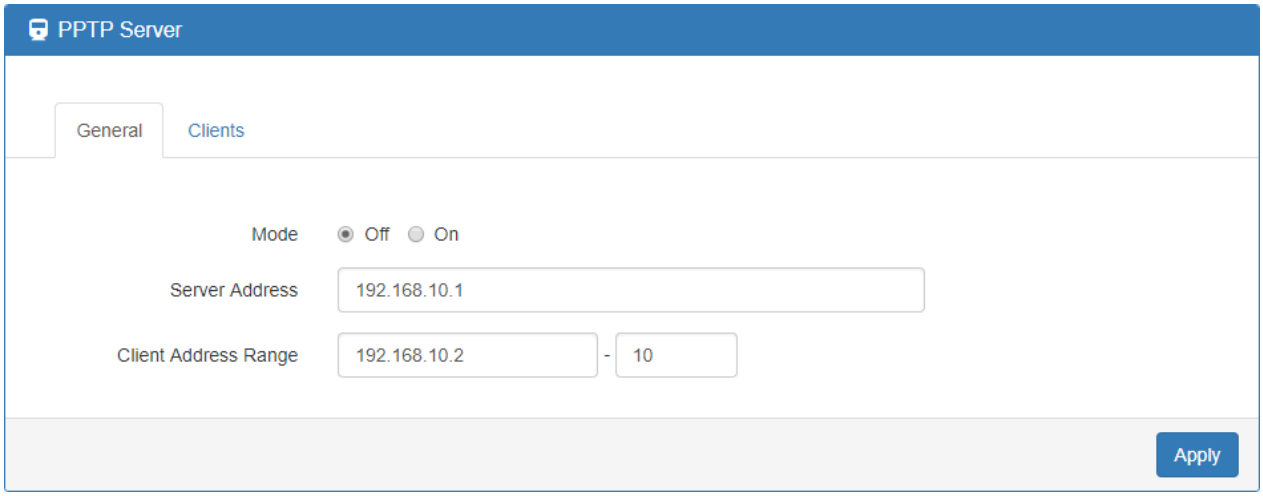


VPN > GRE	
Item	**Description**
Mode	Select from Off or On to enable GRE.
Local Address	Set local address of the GRE tunnel.
Remote Address	Set remote address of the GRE tunnel.
Tunnel Device Address	Set IP address of this GRE tunnel device.
Tunnel Device Address Prefix	Set Prefix of the Tunnel Device Address.
Use Tunnel Key	Whether to use the key for identifying an individual traffic flow within a tunnel.
Tunnel Key Number	The number of the tunnel key; default is '1234'.
Keepalive Period	(0 ~ 32767); 0: keepalive not set.
Keepalive Retries	1 ~ 255.

11.4 VPN > PPTP Server

This section provides 2 sub configurations, including General Configuration and Clients Configuration.

(1) General Configuration



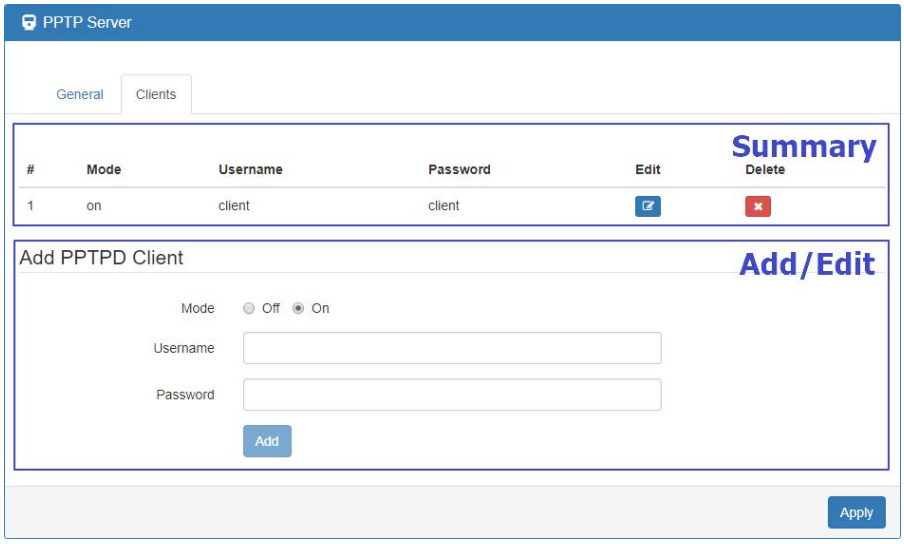
VPN > PPTP Server > General	
Item	**Description**
Mode	Select from Off or On to enable PPTP Server.
Server Address	IP addresses to be used at the local end of the tunneled PPP links between the server and the client.
Client Address Range	A list of IP addresses to assign to remote PPTP clients.

(2) Clients Configuration

There are two parts for Clients configuration.

- Summary part: User can delete and edit the existed PPTP clients.
- Add/Edit part:

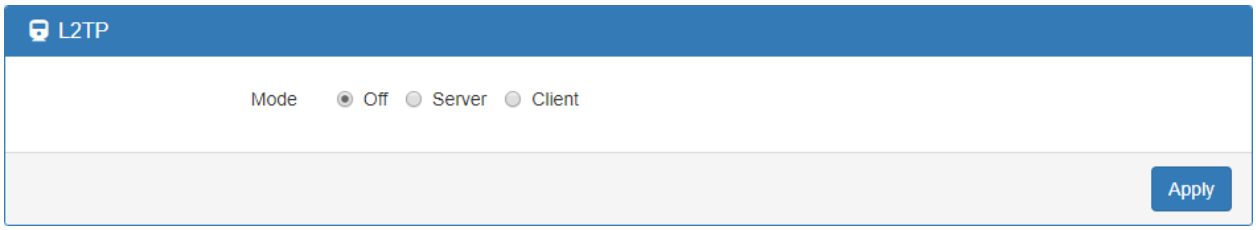
VPN > PPTP Server > Clients	
Item	**Description**
Mode	Select from Off or On to set the client setting.
Username	The username of this client.
Password	The password of this client.



11.5 VPN > L2TP

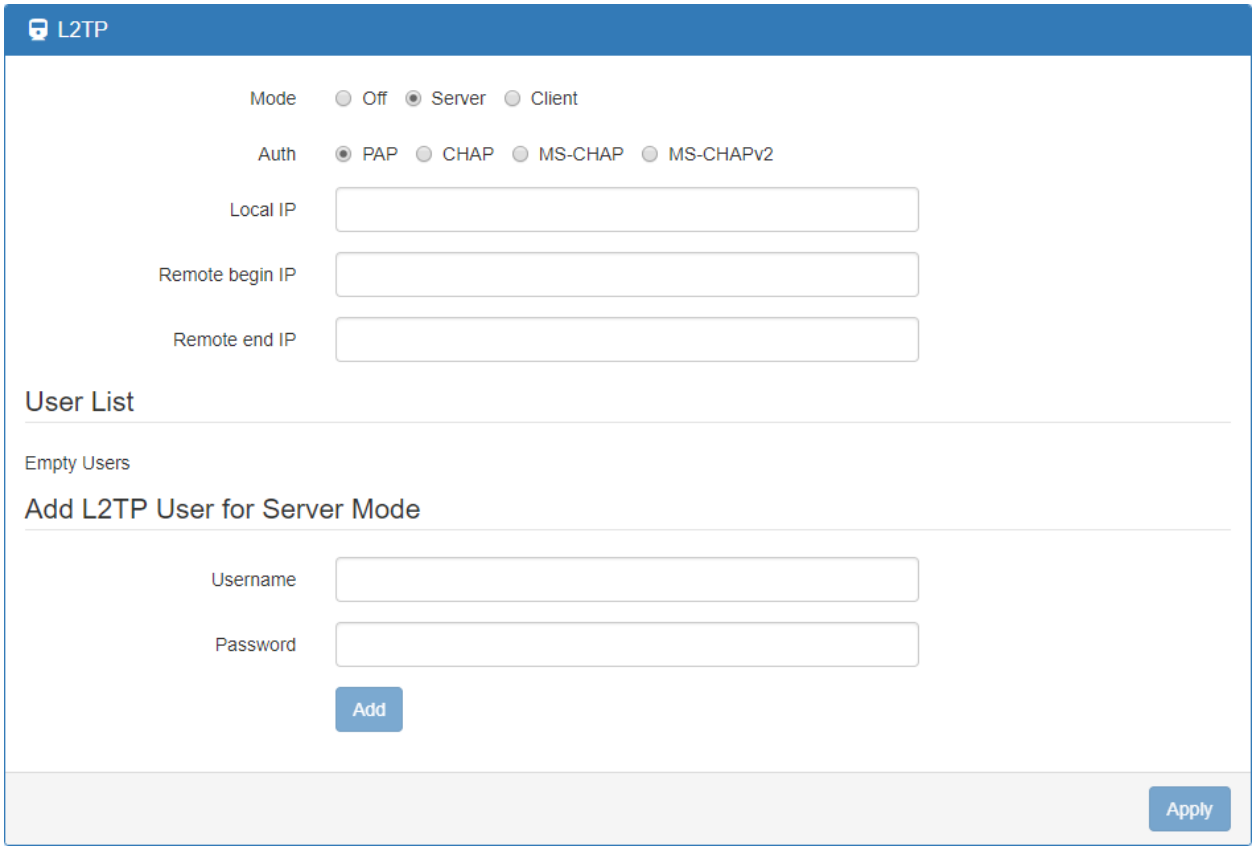
This section allows you to set up L2TP and provides three modes for configuration, including Off, Server, and Client Mode.

(1) General Mode: The default mode is Off as shown in the following interface.



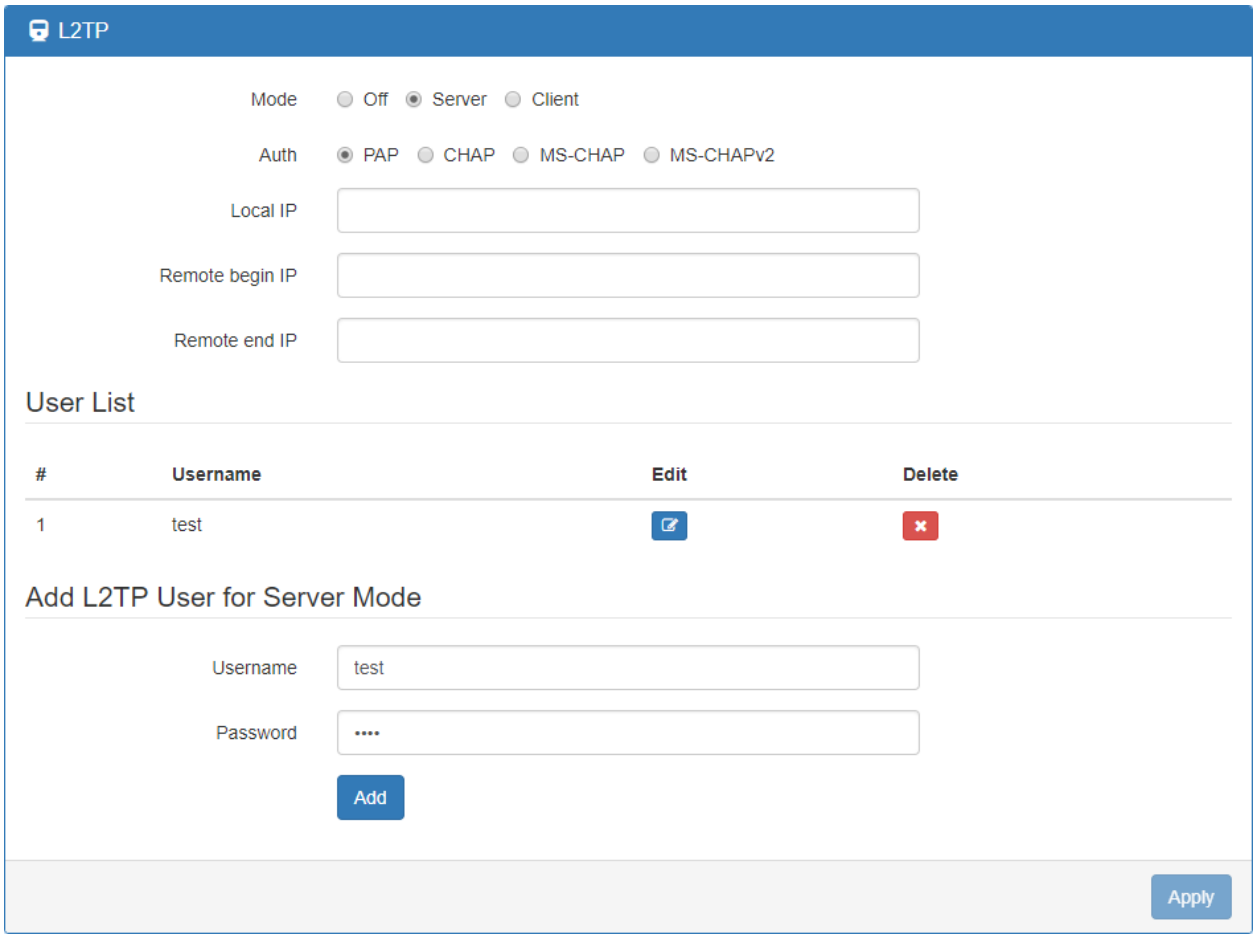
(2) Server Mode:

Choose the Server mode and the interface will be changed as below.



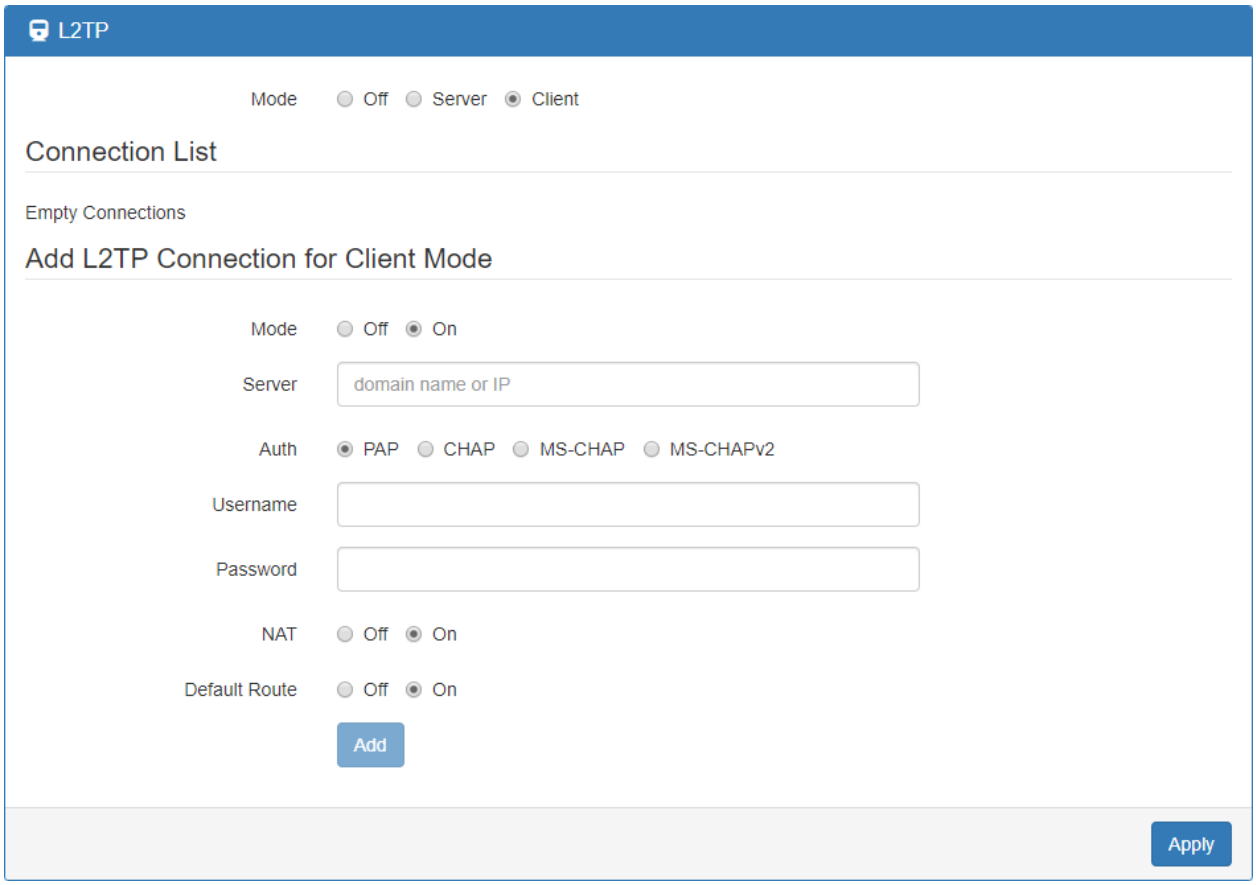
VPN> L2TP > Server Mode	
Item	**Description**
Mode	Select from Off or On to set the client setting.
Auth	The authentication method for L2TP connection. Available options: PAP, CHAP, MS-CHAP, MS-CHAPv2
Local IP	The virtual IP for L2TP server.
Remote begin IP	The begin address of L2TP client's IP pool.
Remote end IP	The end address of L2TP client's IP pool.
Username	The L2TP client's username. Could be used to add the newly client or update existed client.
Password	The L2TP client's password. Could be used to add the newly client or update existed client.

Fill in the username and password and click the Add button, you can create the L2TP client and manage them under server mode.



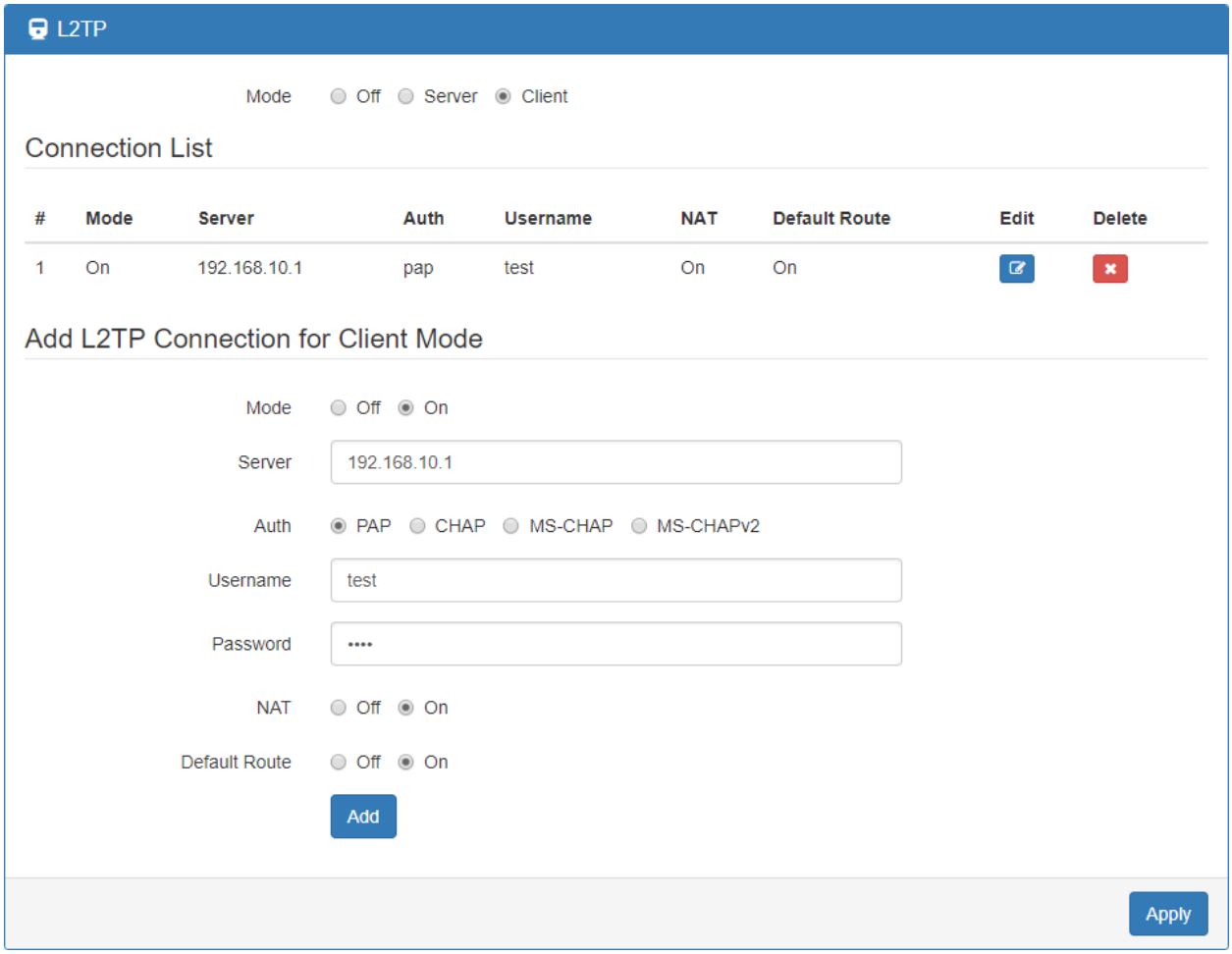
(3) Client Mode:

Choose the Client mode and the interface will be changed as below.



VPN> L2TP > Client Mode	
Item	**Description**
Mode	Turn on/off this L2TP connection
Server	The L2TP server address or hostname.
Auth	The authentication method for L2TP connection. Should same as L2TP server's auth type.
Username	The username for L2TP authentication.
Password	The password for L2TP authentication.
NAT	Turn on to translate the LAN subnet IP to L2TP virtual IP.
Default route	Turn on to redirect all traffic to L2TP tunnel.

Fill in the required parameters and click the Add button to create the L2TP connection and manage the L2TP connection under client mode.



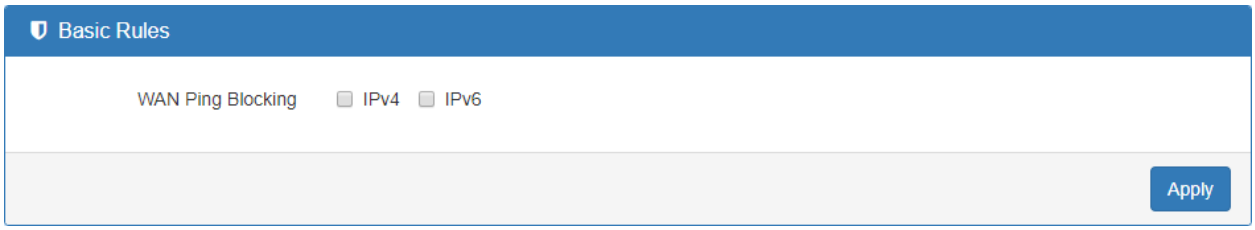
Click the button and edit the parameters to update the L2TP connection.

12 Configuration > Firewall

This section allows you to configure Basic Rules, Port Forwarding, DMZ, IP Filter, MAC Filter, URL Filter, NAT and IPS.

12.1 Firewall > Basic Rules

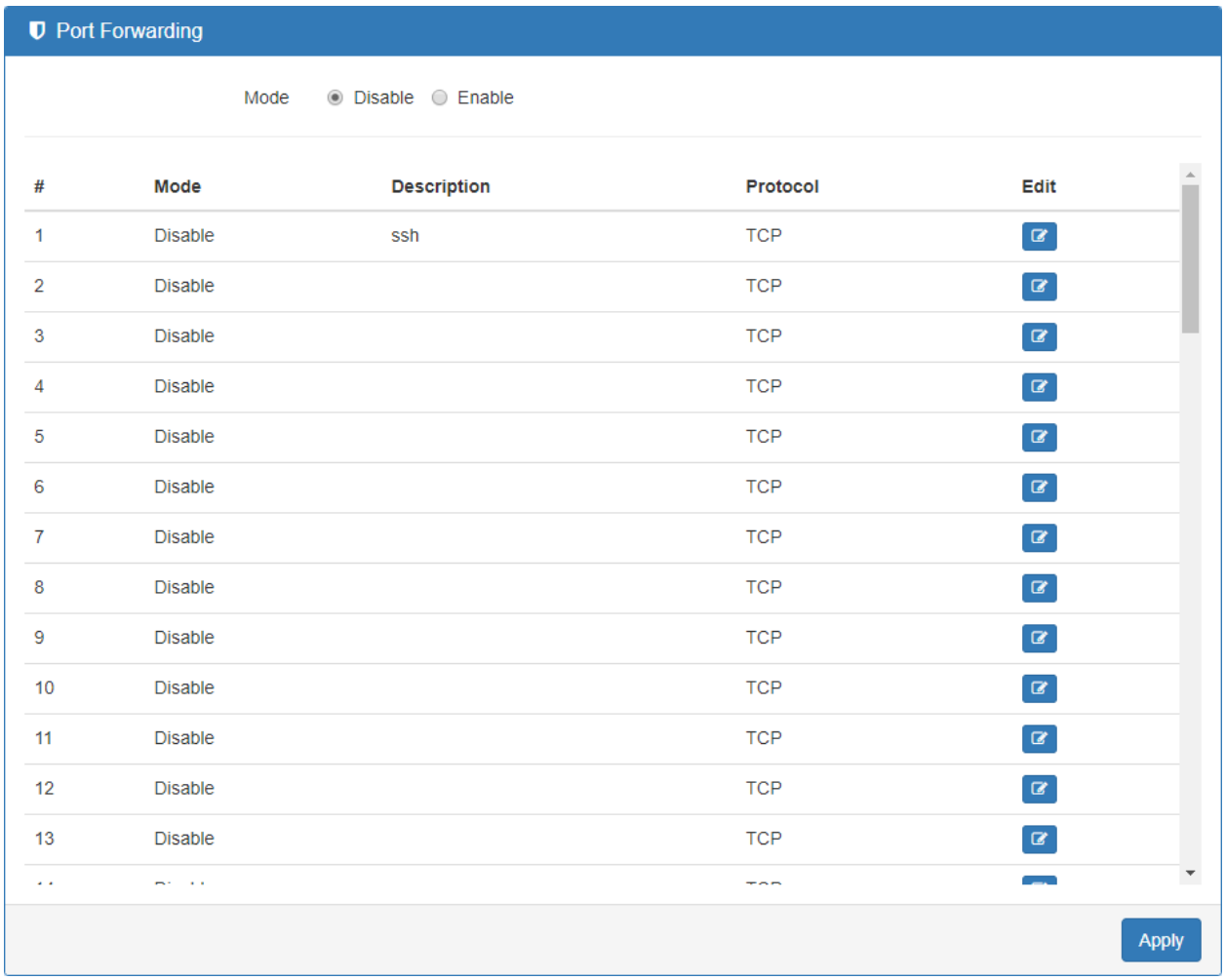
This section allows you to set the Basic Rules configuration.

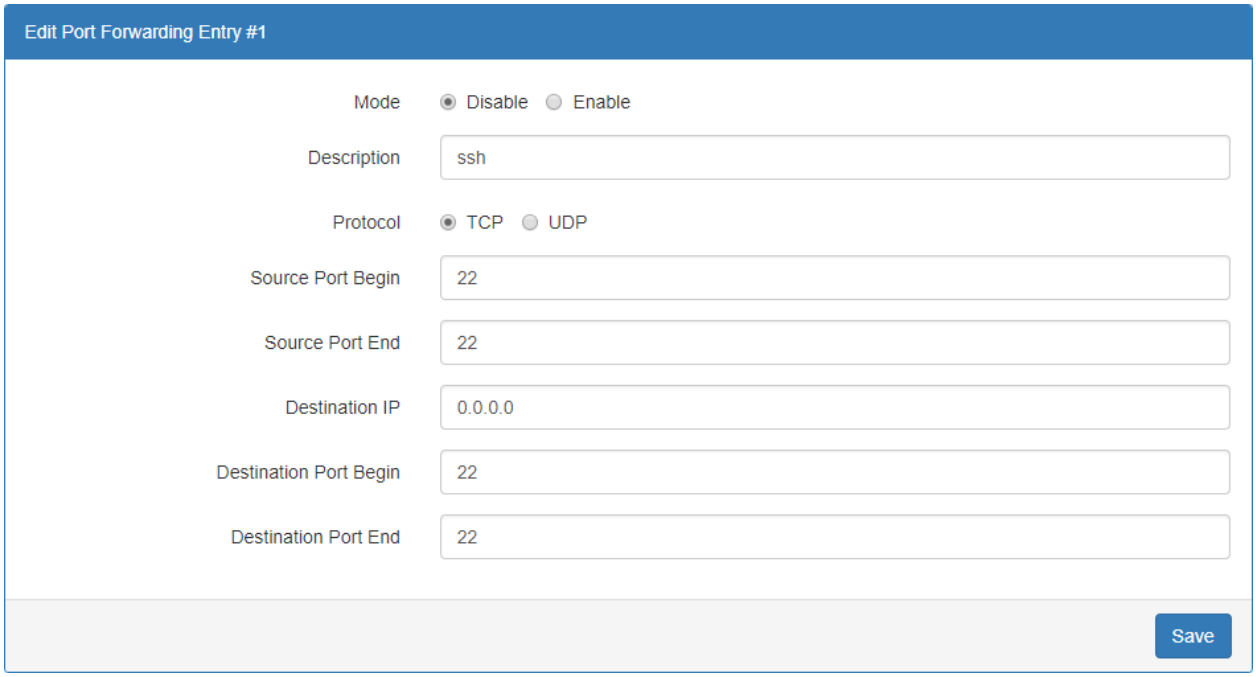


Firewall > Basic Rules	
Item	**Description**
WAN Ping Blocking	Check IPv4 or IPv6 for blocking

12.2 Firewall > Port Forwarding

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

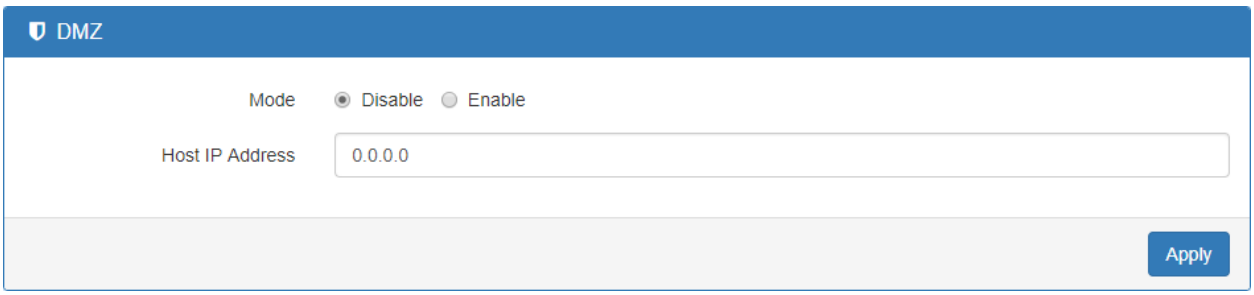




Firewall > Port Forwarding	
Item	**Description**
Mode	Turn on/off Port Forwarding to select Disable or Enable. The default is Disable.
Description	Descript the name of Port Forwarding.
Protocol	Select from UDP or TCP Client which depends on the application.
Source Port Begin	Fill in the beginning of 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.

12.3 Firewall > DMZ

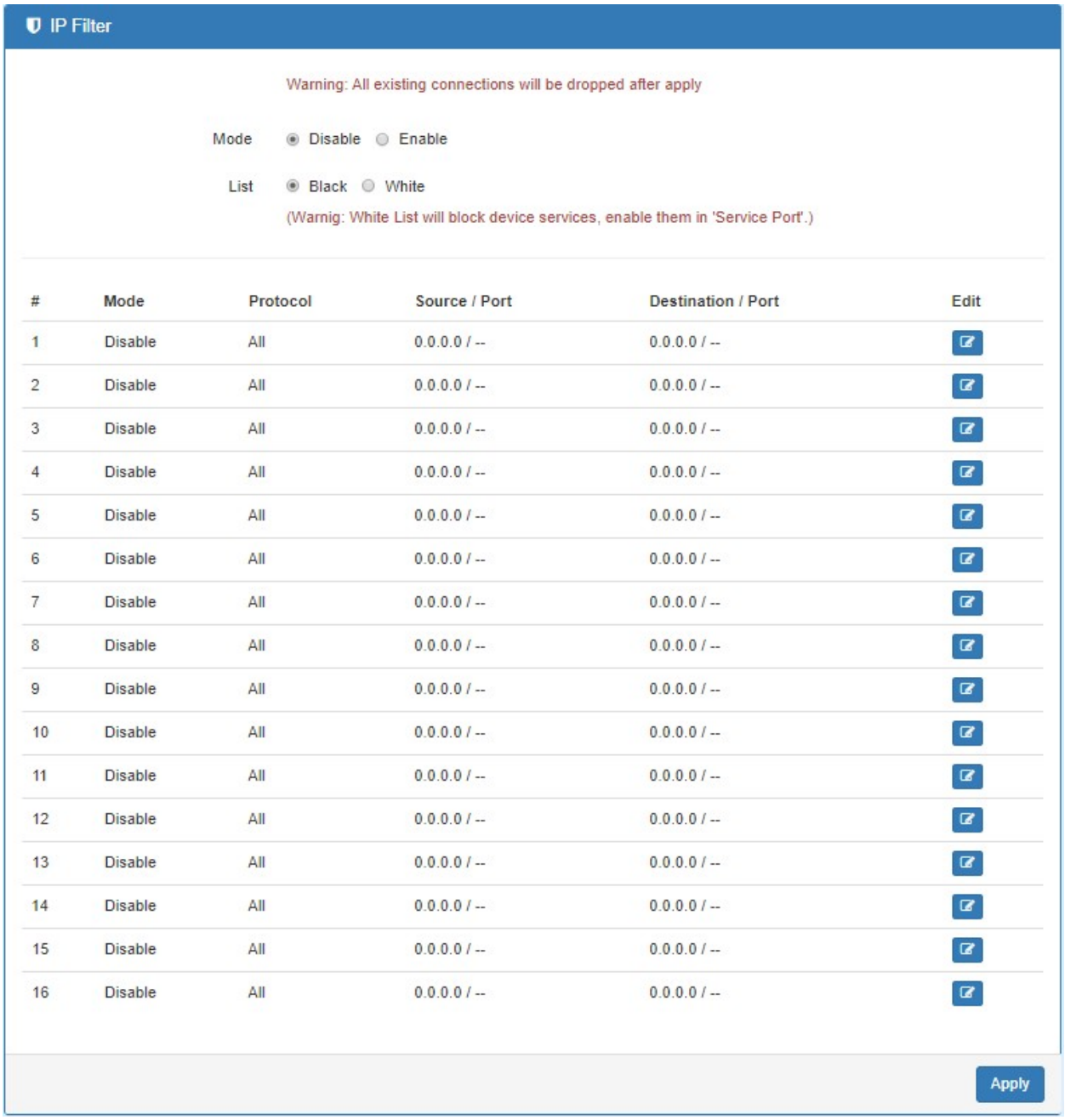
This section allows you to set the DMZ configuration.



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

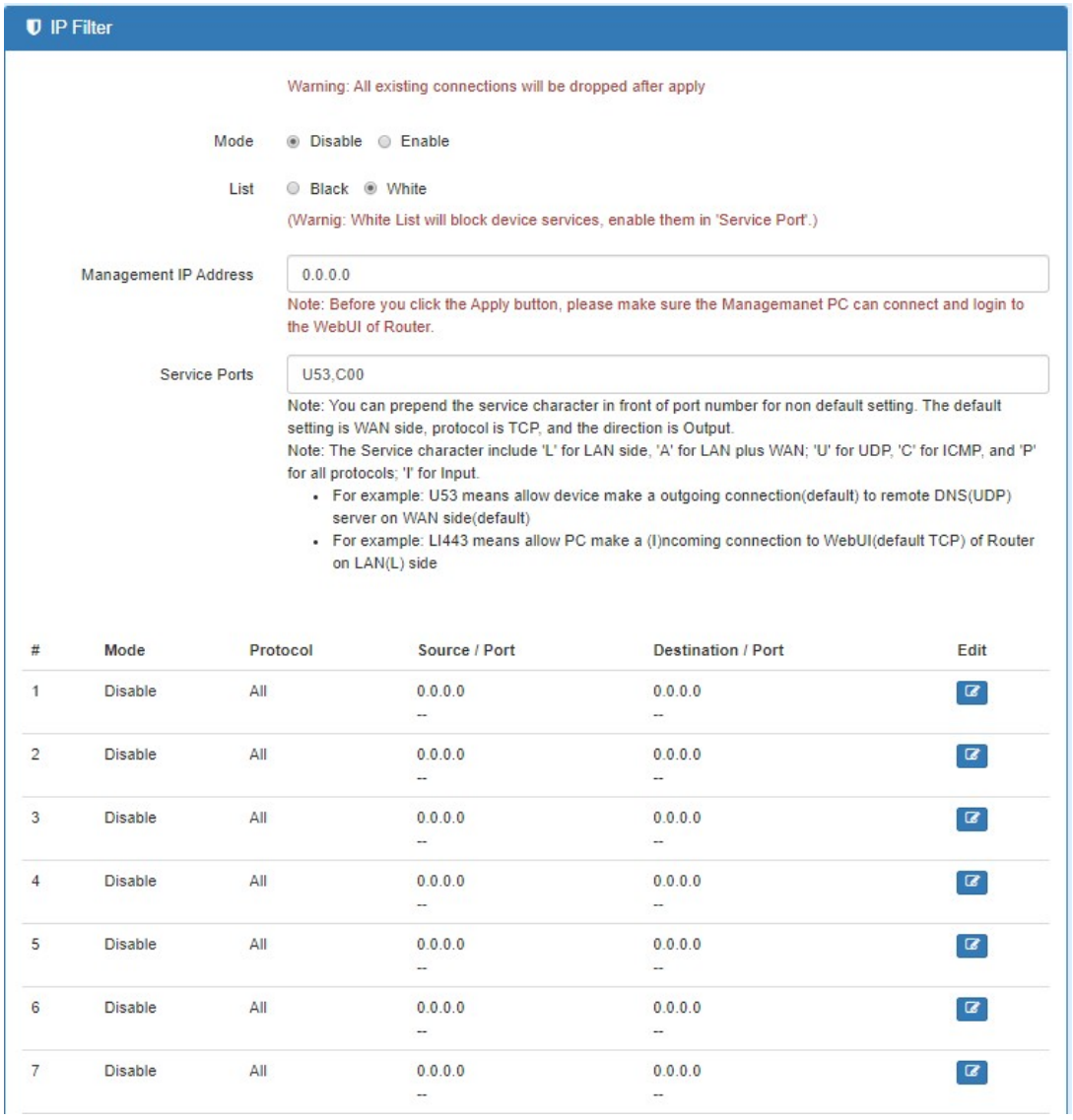
12.4 Firewall > IP Filter

This section allows you to configure IP Filter. After clicking button, you can edit your IP protocol, source/port and destination/port. The default is **Disable** mode and **Black** list.



#	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 / --	

- **Black List:** When set as Black List, the specific IP address/port in rule will be blocked.
- **White List:** When set as White List, the specific IP address/port in rule will be accepted.



Management IP Address:

For White List only. Since White List will block all user communication except those has been assigned by rules, it is better to assign a specific IP address for the administrator to access the Router which is Management IP Address.

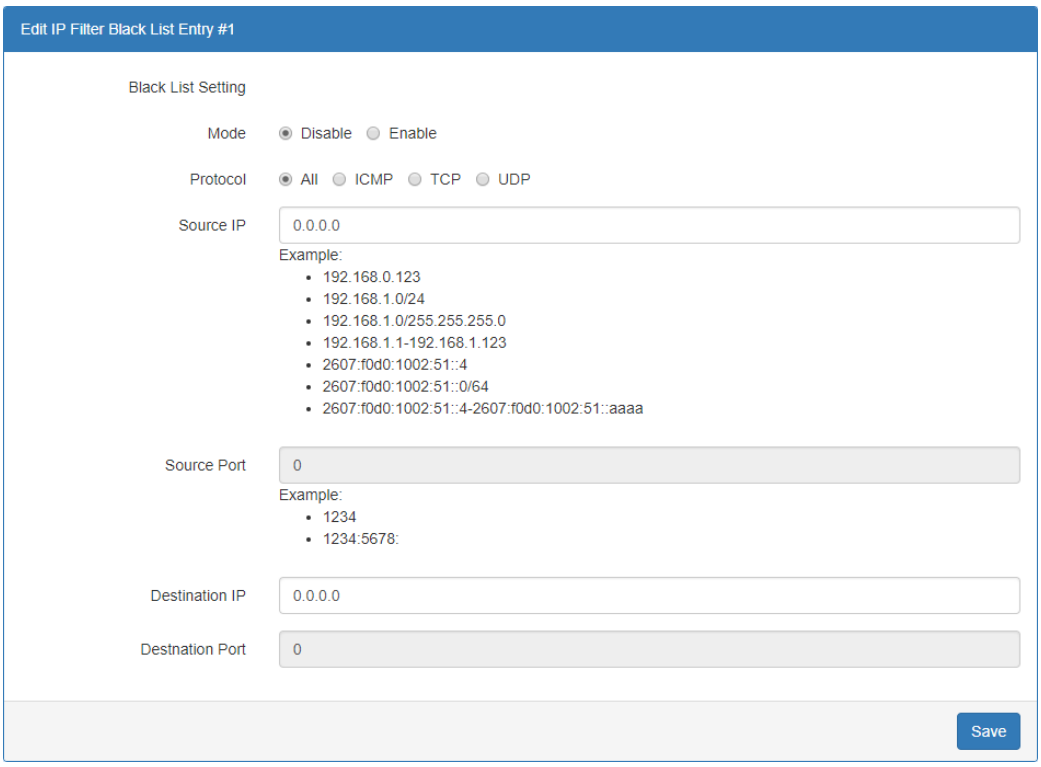
Service Ports:

For White List only. The setting is specified for Router access only. The user can set it to allow Router access outside WAN or inside LAN Service. For example, access outside WAN DNS service. It also allows user to access Router service from outside WAN or inside LAN. For example, access Router Web service.

Edit Black/White List

(1) Click button to edit Black/White list.

(2) The default is **Disable** mode as the following interface (Black/White).



Firewall > 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.

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

(4) 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.

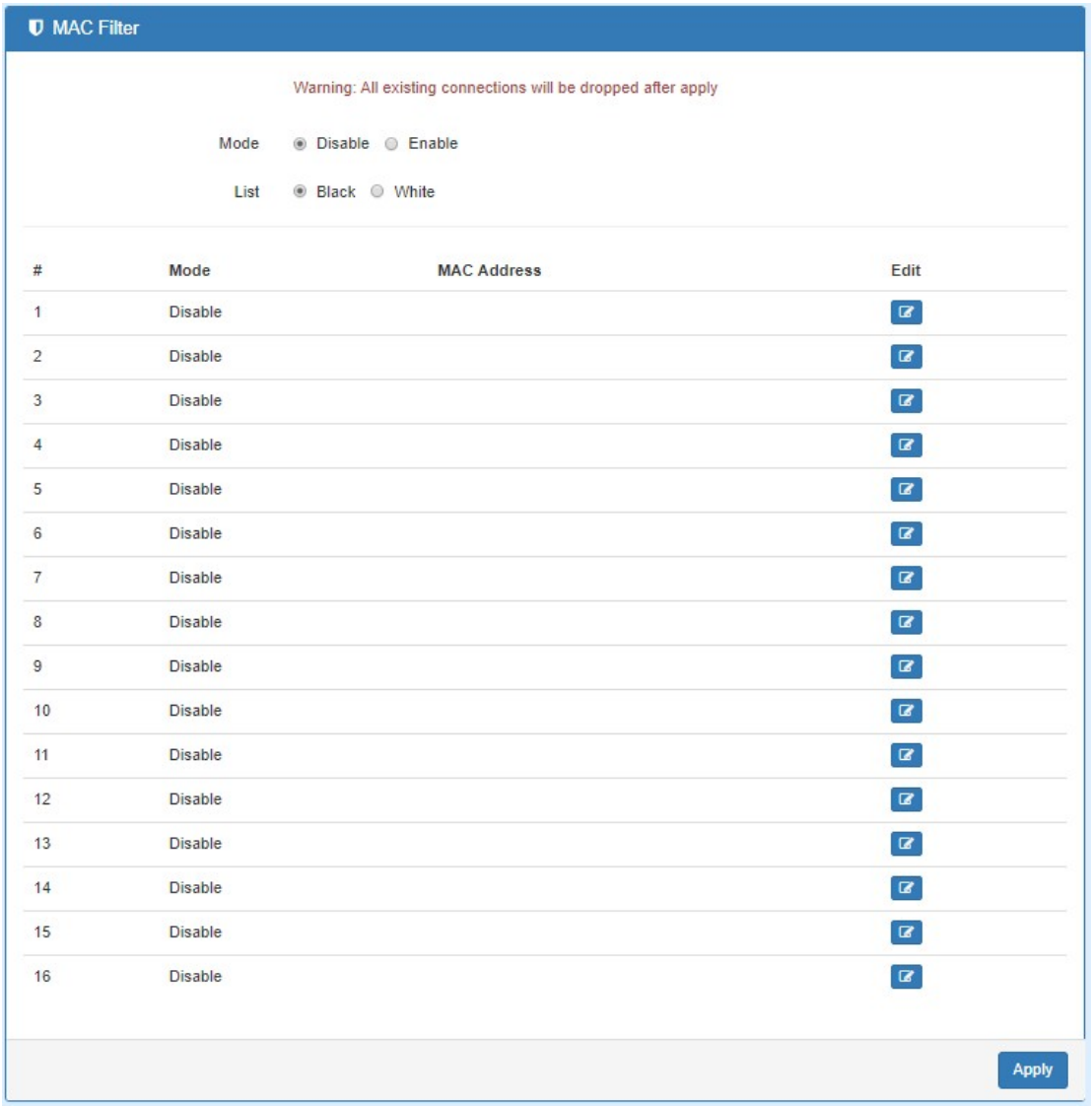
Firewall > Edit IP Filter > Source IP			
IP Format	**Single IP**	**IP with Mask**	**Ranged IP**
IPv4	192.168.0.123	192.168.1.0/24 192.168.1.0/255.255.255.	192.168.1.1- 192.168.1.123
IPv6	2607:f0d0:1002:51::4	2607:f0d0:1002:51::0/64	2607:f0d0:1002:51::4- 2607:f0d0:1002:51::aaaa
Note: Setting up a range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

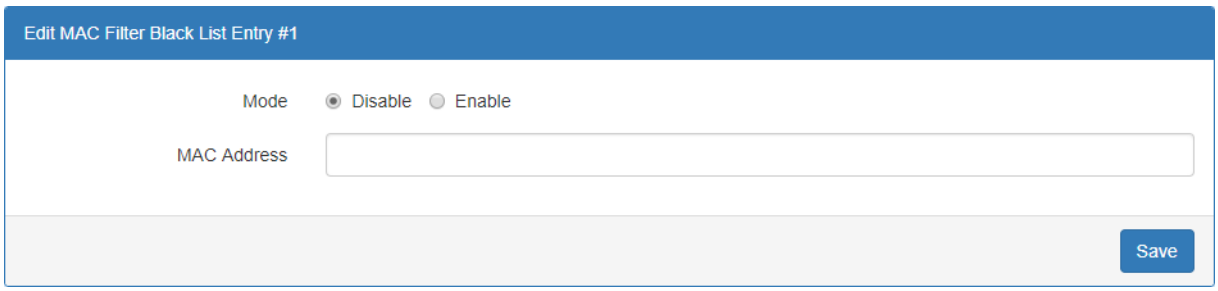
(5) For Source Port, there are two types to input your source port that depends on your requirement, including single port (e.g.1234) or giving a range of ports (e.g.1234:5678).

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

12.5 Firewall > 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).

12.6 Firewall > URL Filter

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

URL Filter

Warning: All existing connections will be dropped after apply

Mode ◉ Disable ○ Enable

#	Mode	Filter	Key/Full	Edit
1	Disable	Key		
2	Disable	Key		
3	Disable	Key		
4	Disable	Key		
5	Disable	Key		
6	Disable	Key		
7	Disable	Key		
8	Disable	Key		
9	Disable	Key		
10	Disable	Key		
11	Disable	Key		
12	Disable	Key		
13	Disable	Key		
14	Disable	Key		
15	Disable	Key		
16	Disable	Key		

Apply

Edit URL Filter Black List Entry #1

Mode ○ Disable ◉ Enable

Filter ○ Key ◉ Full

Key/Full tw.yahoo.com

Hint About the 'Full' filter:

- Please NOT include 'http://' or 'https://' inside the URL
- It only works at LTE Net Modes 'Router Only' and 'Dual Router'

Save

Note: Please not include "**https://**" or "**http://**" for the URL address in the **Full** Filter.

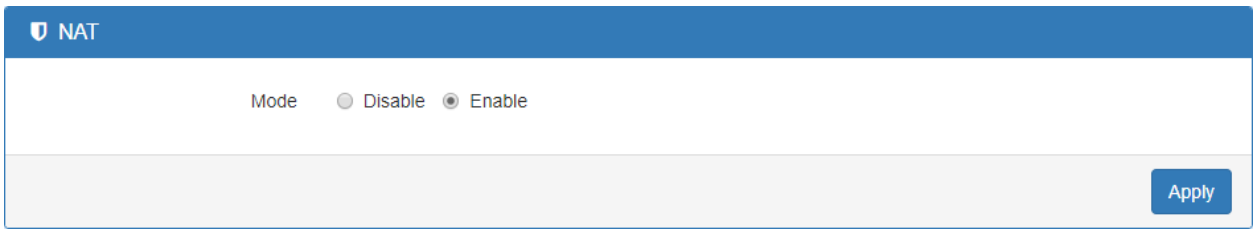
Firewall > URL Filter	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Filter	Select from Key or Full. The default is Key.
Key / Full	Fill in your Key / Full information.

12.7 Firewall > NAT

This section allows you to set NAT configuration.

When NAT mode is **Enable**, 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.

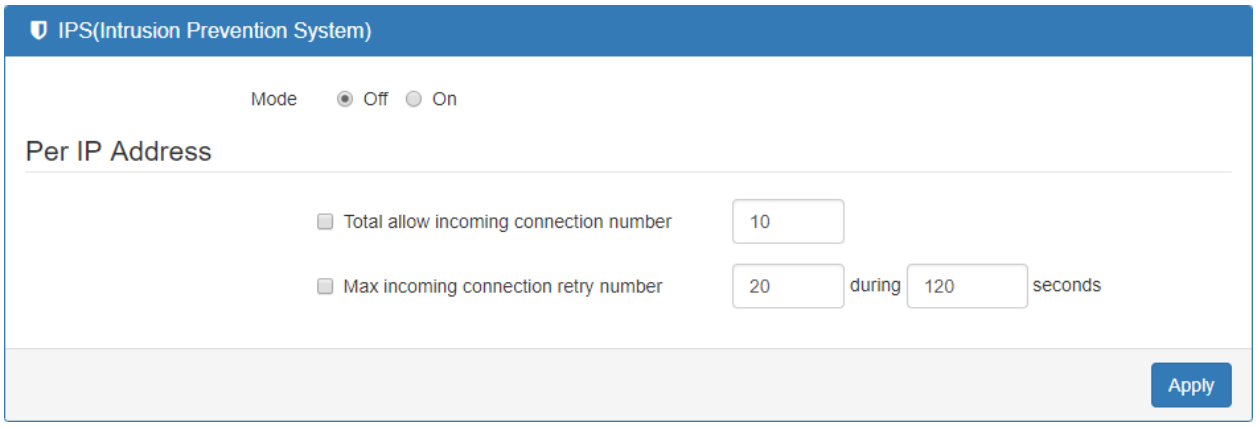
When NAT mode is **Disable**, the router will send the source LAN private IP address for outgoing packets and allow to receive the destination LAN private IP address for incoming packets.



12.8 Firewall > IPS

This section allows you to set IPS configuration. IPS prevents the system from being attacked by the Internet.

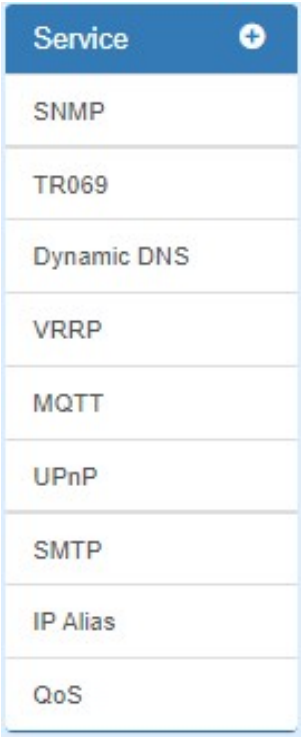
The system allows to limit the max incoming connection number from WAN per source IP address to prevent system resource exhausted. Also, the system allows to limit the max incoming connection retry number during a specific time period from WAN per source IP address to prevent too many unexpected connections retry event from causing system busy.



Firewall > IPS	
Item	**Description**
Mode	Turn on / off IPS function (default: Off)
Total allow incoming connection number	Select the checkbox to enable or disable the function. The default number is 10.
Max incoming connection retry number	Select the checkbox to enable or disable the function. The default number is 20.
Duration time	The default time is 120 seconds.

13 Configuration > Service

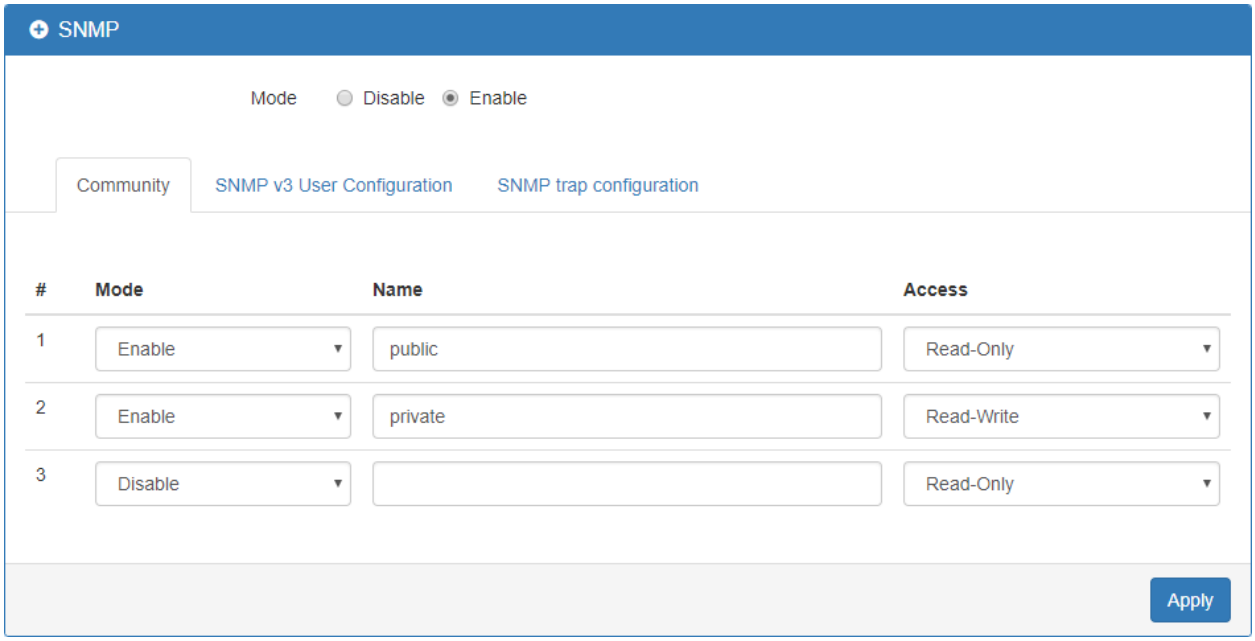
This section allows you to configure the SNMP, TR069, Dynamic DNS, VRRP, MQTT, UPnP, SMTP, IP Alias, and QoS.



13.1 Service > SNMP

This section allows you to set the SNMP configuration.

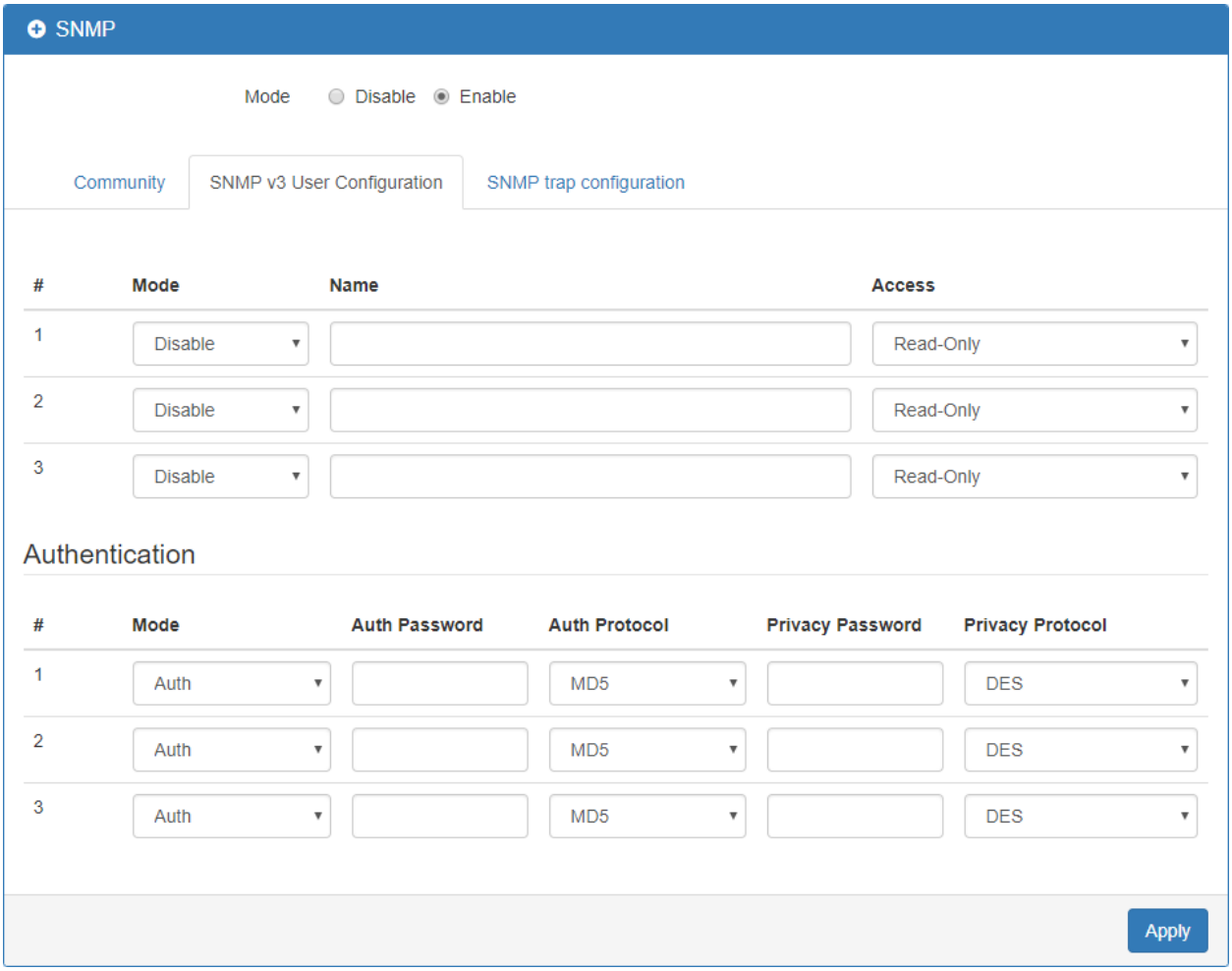
13.1.1 Community



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.

13.1.2 SNMP v3 User Configuration

For SNMP v3 User Configuration, 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.

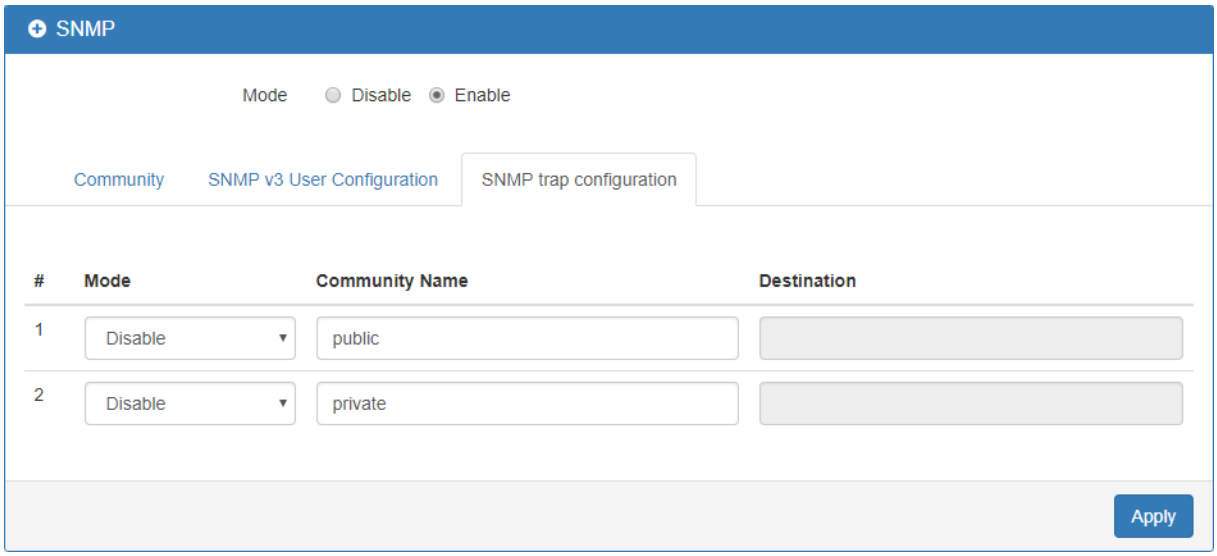


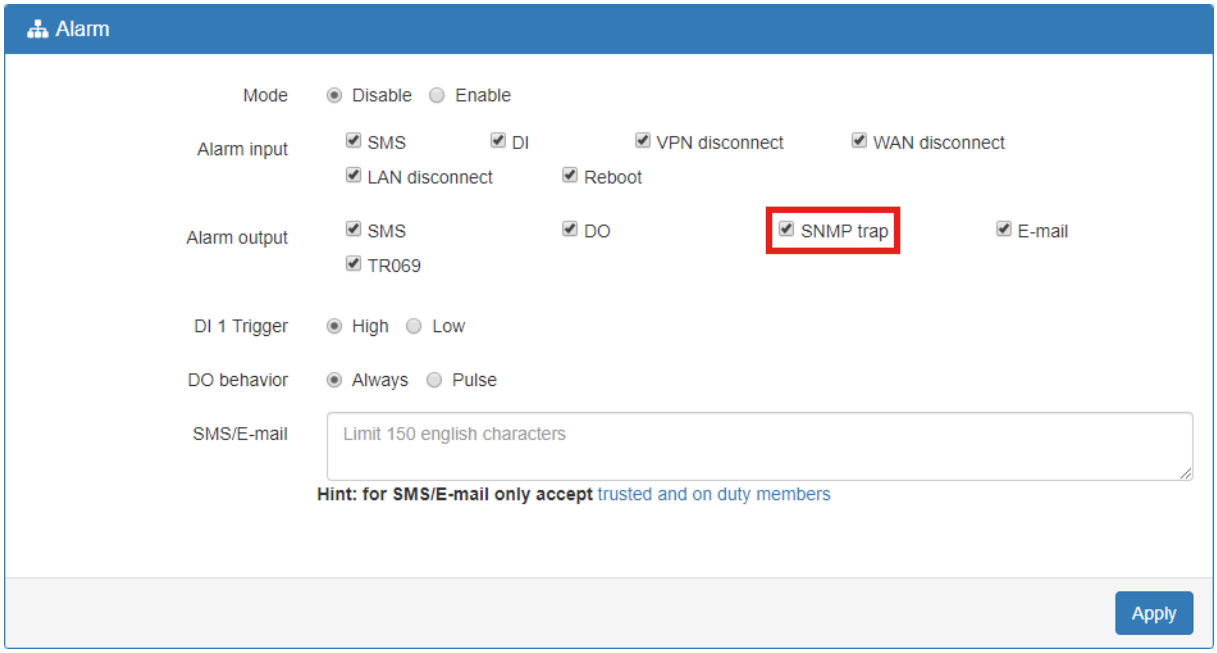
Service > SNMP > SNMP v3 User configuration	
Item	**Description**
Mode	Select from Disable or Enable to configure SNMP. The default is Disable.
Name	Fill in your name.
Auth Mode	Select from Authentication or Privacy.
Authentication Password	Fill in your authentication password.
Authentication Protocol	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.

13.1.3 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.

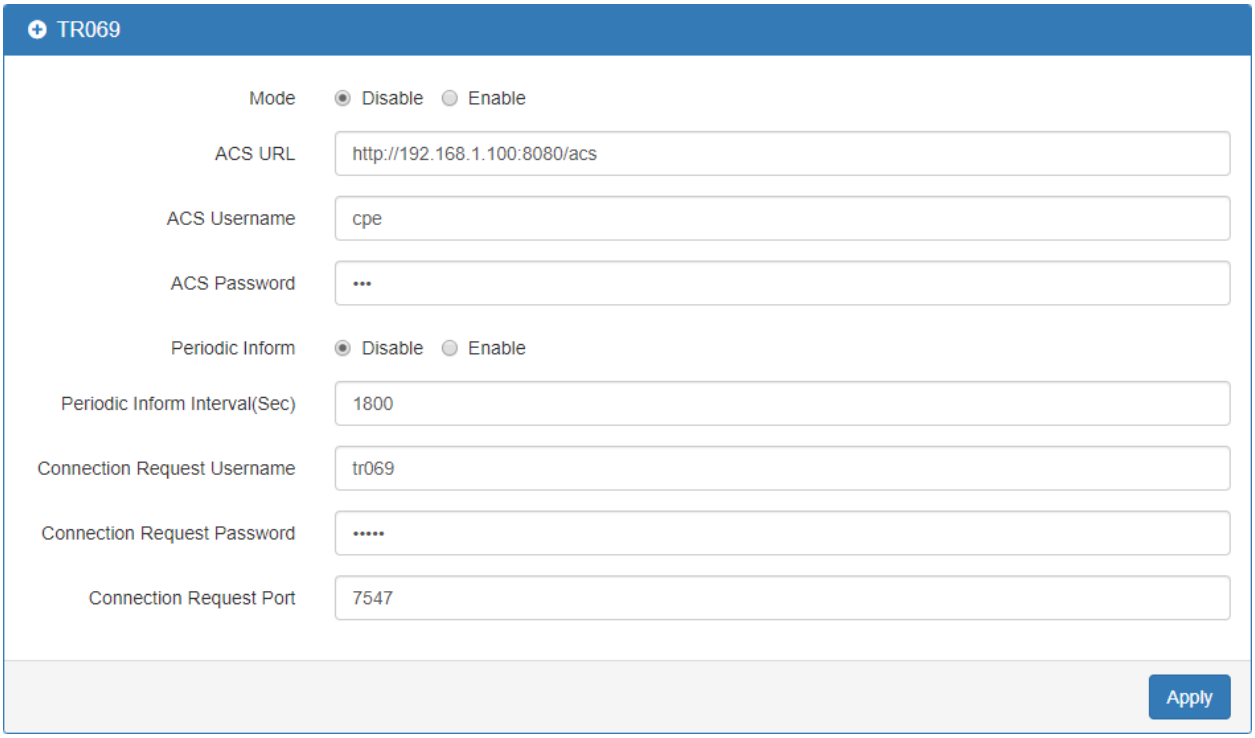




Service > SNMP > SNMP trap configuration	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Community Name	Fill in your community name.
Destination	The destination (domain name/IP) of remote SNMP trap server.

13.2 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.
Connection Request Password	Fill in the connection request password to authenticate the ACS if the ACS attempts to communicate with the CPE.
Connection Request Port	Fill in the connection request port to authenticate the ACS if the ACS attempts to communicate with the CPE.

13.3 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.
IP Address Selection	Select either Internet IP or WAN IP.

Note: There are six 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

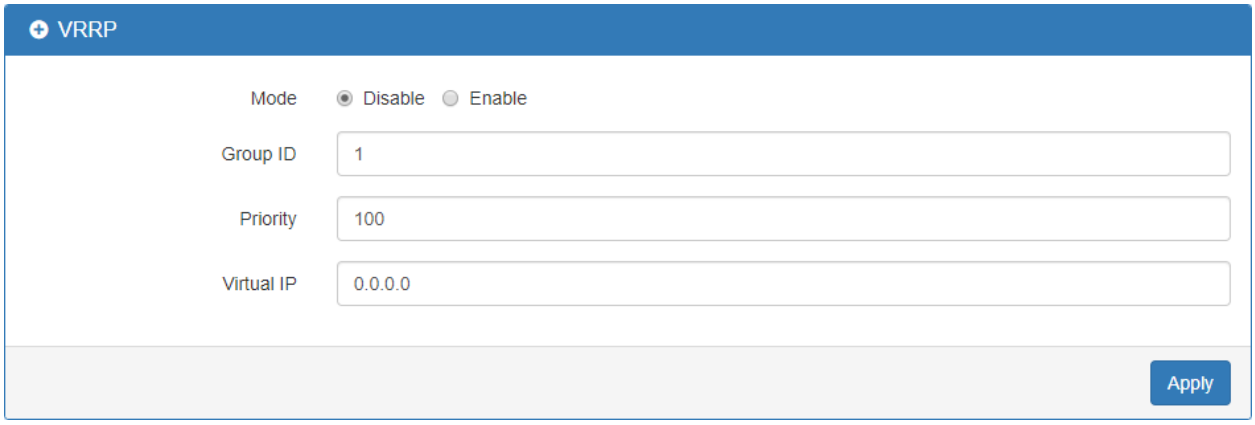
Service Provider	**no-ip.com**
Host Name	Register hostname, e.g. tester.hopto.org
Username	Register username.
Password	Register password.

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.

13.4 Service > VRRP

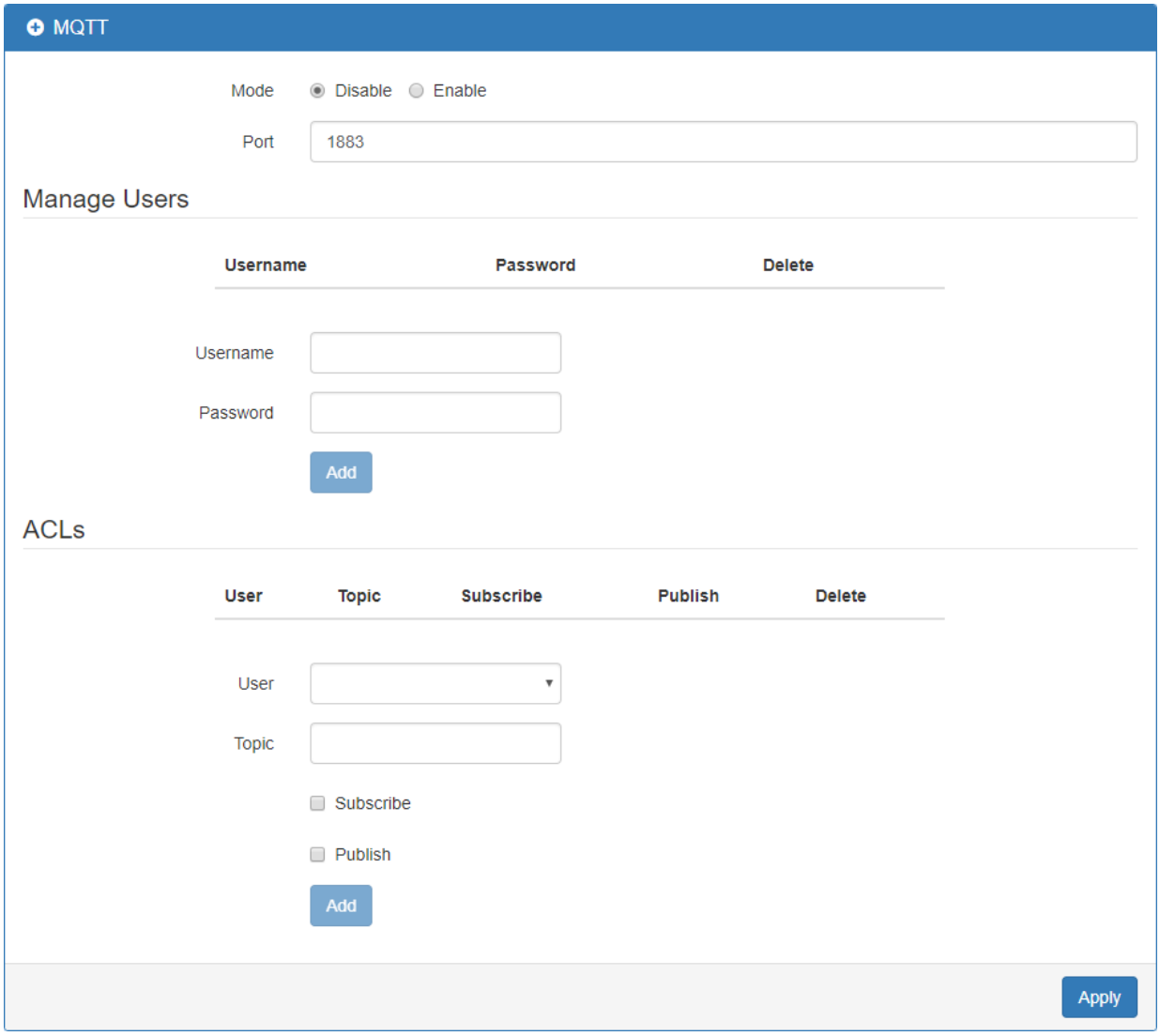
This section allows you to configure VRRP.



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.

13.5 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 **ACLs** 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 **sub2** to read the critical topic. Thus, only the sub1 and sub2 can receive it when **pub1** sending the message.

ADVICE

MQTT

Mode ◉ Disable ○ Enable

Port 1883

Manage Users

Username	Password	Delete
Sub1	••••	✖
Sub2	••••	✖
Sub3	••••	✖
Pub1	••••	✖
Pub2	••••	✖

Username

Password

Add

ACLs

User	Topic	Subscribe	Publish	Delete
Sub1	Critical	☑	☐	✖
Sub2	Critical	☑	☐	✖
Pub1	Critical	☐	☑	✖

User

Topic

☐ Subscribe

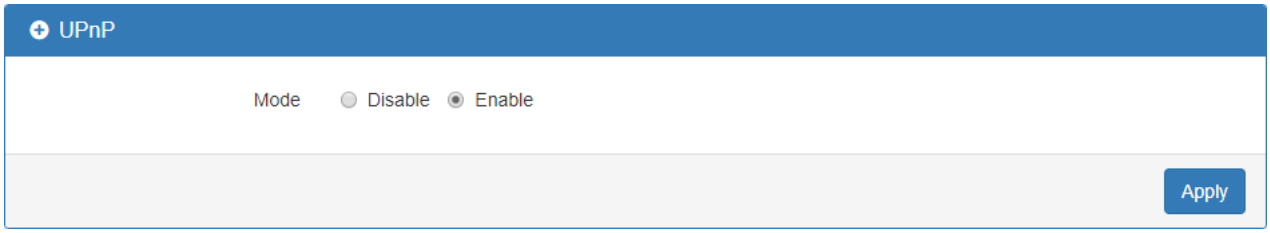
☐ Publish

Add

Apply

13.6 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.



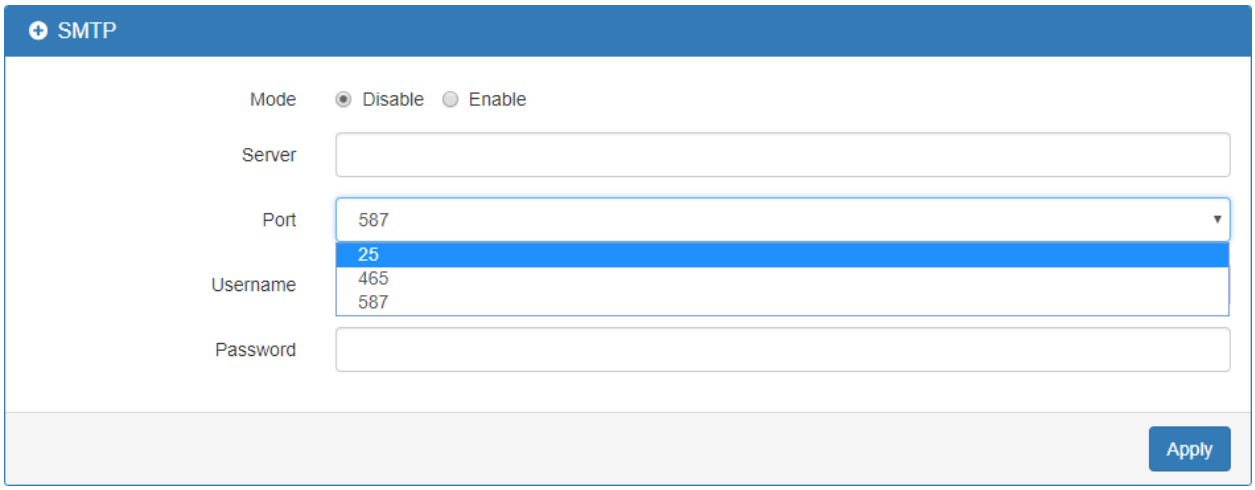
Note:

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.

13.7 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.



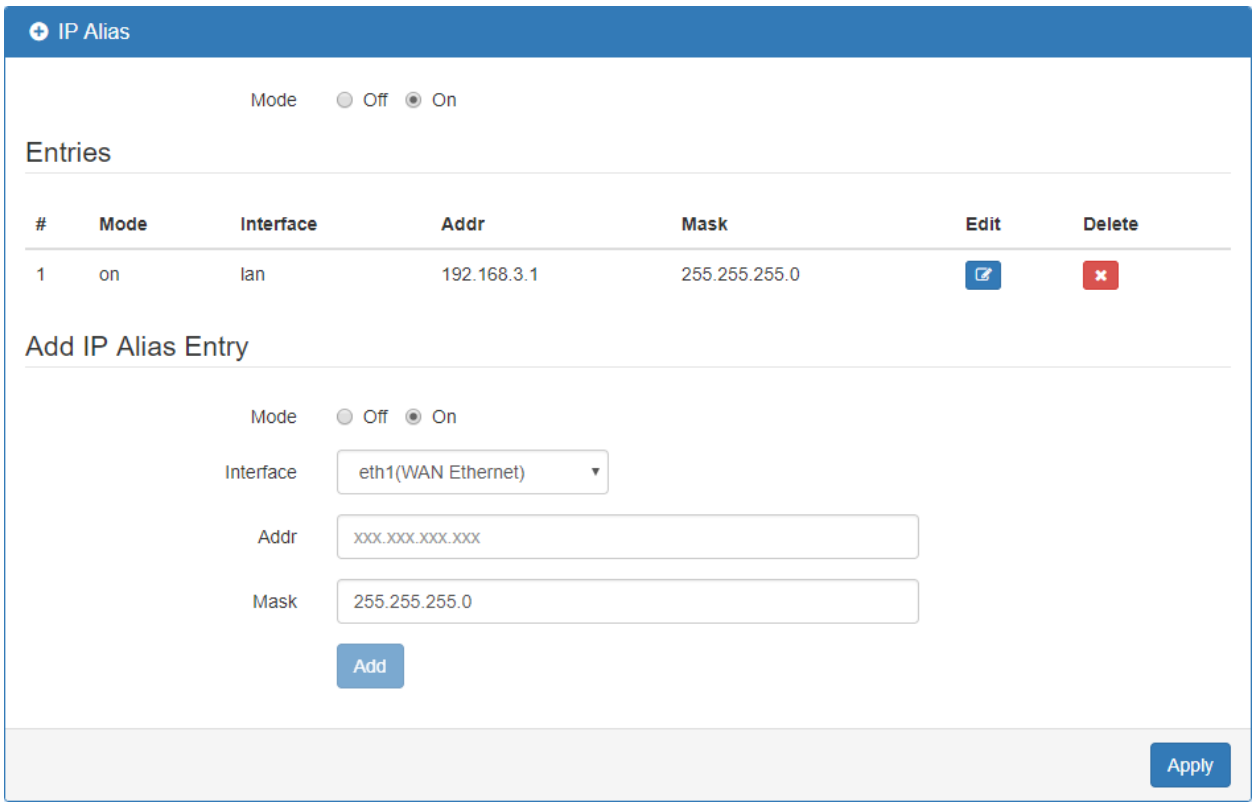
Service > SMTP	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Server	The email will be sent through the server.
Port	There are three ports for SMTP communication between mail servers. ● **Port 25**：Use TCP port 25 without encryption. ● **Port 465**：SMTP connections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

13.8 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 build multiple connections with the 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.

13.9 QoS

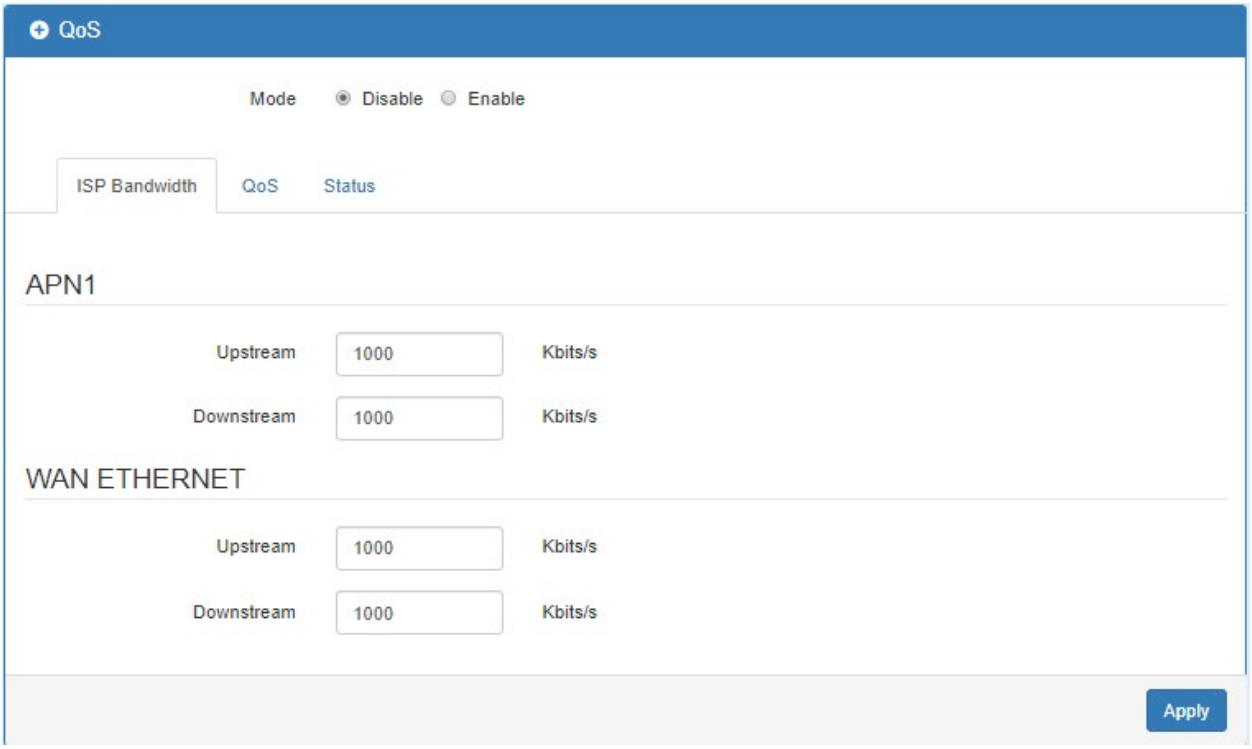
QoS (Quality of Service) refers to a network ability to achieve maximum bandwidth and allow minimum bandwidth. It guarantees the minimum and limit the maximum bandwidth for certain class of traffic. The QoS configuration has three parts, including ISP bandwidth, QoS, and Status.

- ISP bandwidth allows user to configure the max bandwidth for upstream and downstream of specific WAN interface. Upstream means from LAN to WAN. Downstream means WAN to LAN.
- QoS configuration allows user to classify the traffic. Once classified, the traffic will have the guarantee minimum and limit maximum bandwidth.
- Status allows user to monitor the dynamic bandwidth usage.

13.9.1 QoS > ISP Bandwidth

User can assign the Upstream and Downstream Bandwidth for each interface. The Bandwidth unit is kilobits per second.

To prevent guaranteed traffic loss, the assigned bandwidth is better not to exceed the real bandwidth because the allowable traffic quantity may exceed the real bandwidth.



13.9.2 QoS > QoS

You can select QoS tab to show an overall view for QoS configuration.
At right side of window, there are three buttons.

- Edit button: It allows you to edit QoS Entry and configure QoS settings.
- Up/Down arrow button: It allows you to adjust priority of the QoS entry. The first QoS entry is the highest priority.

The QoS entry configuration page has three parts for classify traffic, assign bandwidth, and group IP address bandwidth.

ADVICE

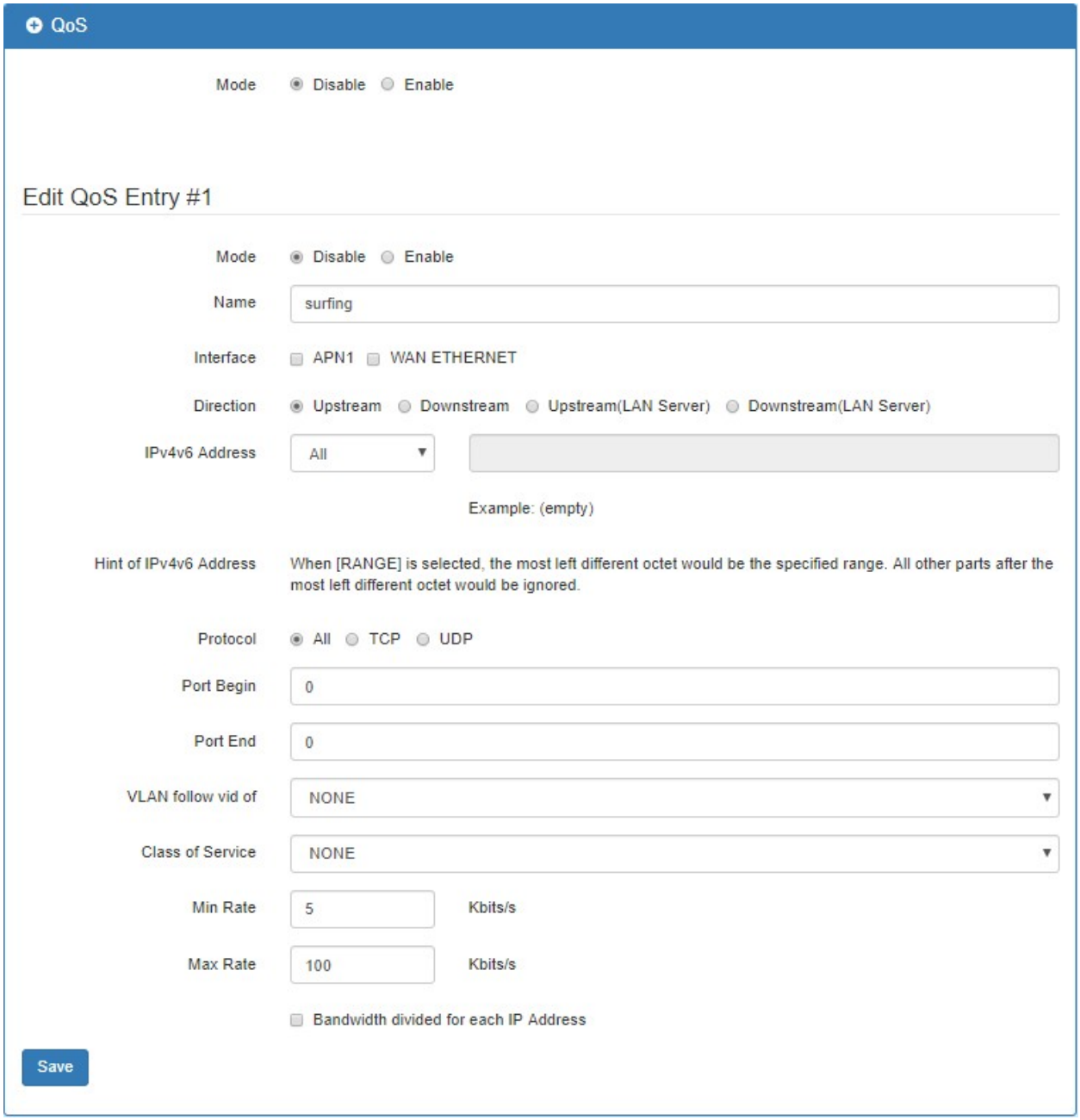
QoS

Mode ◉ Disable ○ Enable

ISP Bandwidth | QoS | Status

#	Mode	Name	Port	IP	Rate
1	Disable	surfing	0 - 0		5 - 100
2	Disable	surfing	0 - 0		5 - 100
3	Disable	surfing	0 - 0		5 - 100
4	Disable	surfing	0 - 0		5 - 100
5	Disable	surfing	0 - 0		5 - 100
6	Disable	surfing	0 - 0		5 - 100
7	Disable	surfing	0 - 0		5 - 100
8	Disable	surfing	0 - 0		5 - 100
9	Disable	surfing	0 - 0		5 - 100
10	Disable	surfing	0 - 0		5 - 100
11	Disable	surfing	0 - 0		5 - 100
12	Disable	surfing	0 - 0		5 - 100
13	Disable	surfing	0 - 0		5 - 100
14	Disable	surfing	0 - 0		5 - 100
15	Disable	surfing	0 - 0		5 - 100
16	Disable	surfing	0 - 0		5 - 100
17	Disable	surfing	0 - 0		5 - 100
18	Disable	surfing	0 - 0		5 - 100
19	Disable	surfing	0 - 0		5 - 100
20	Disable	surfing	0 - 0		5 - 100

Apply



Service > IP Alias	
Item	**Description**
Mode	Select from Disable or Enable QoS.
Name	The setting can be edited or deleted the existed entries.
Interface	The interface of QoS entry is either WAN Ethernet or LTE and both options.
Direction	• When selecting Upstream for LAN to WAN traffic, the Port Begin/End is for public server. • When selecting Downstream for WAN to LAN traffic, the Port Begin/End is for public server. • When selecting Upstream (LAN server) for WAN to LAN traffic, the Port Begin/End is for LAN server.

	• When selecting Downstream (LAN server) for LAN to WAN traffic, the Port Begin/End is for LAN server. • Downstream (LAN server) is for LAN to WAN traffic, and the Port Begin/End is for LAN server.
IPv4v6 Address	Choose four types to set address format, including All, Single, Subnet, and Range. • All is for none. • Single is for single IP address. • Subnet is for IP address with subnet mask bit. • Range is for the specified range between two IP addresses. Hint: When [RANGE] is selected, compare the difference from left to right octet and find out different octet for setting the specified range of IP address. All other parts after different octet would be ignored.
Protocol	• All is for none. • UDP is for User Datagram Protocol. • TCP is for Transmission Control Protocol.
Port Begin/Port End	the TCP/UDP service port
VLAN follow vid of	• NONE. • NET1 - NET8. Note: For NET1 to NET8, make sure the related subnet is enabled at VLAN->Tag Base. The VLAN ID, vid, will be the VID field of the related Subnet at VLAN->Tag Base.
COS (Class of Service or 802.1q)	NONE or 0~7. It is class of service for VLAN.
Min Rate/Max Rate	The unit is kilobits per second. Min Rate guarantee the minimum bandwidth and Max Rate is the limit bandwidth.
Bandwidth divided for each IP Address	When this feature is selected, the bandwidth assigned by Min Rate/Max Rate will be divided by the number of IP addresses. The available IP type is Subnet and Range. User needs to calculate the Min Rate and Max Rate for those IP addresses. The subnet mask bit in IP Type Subnet is octet boundary and the number of IP addresses is one octet too, 256, from subnet mask bit to subnet mask plus eight bit.

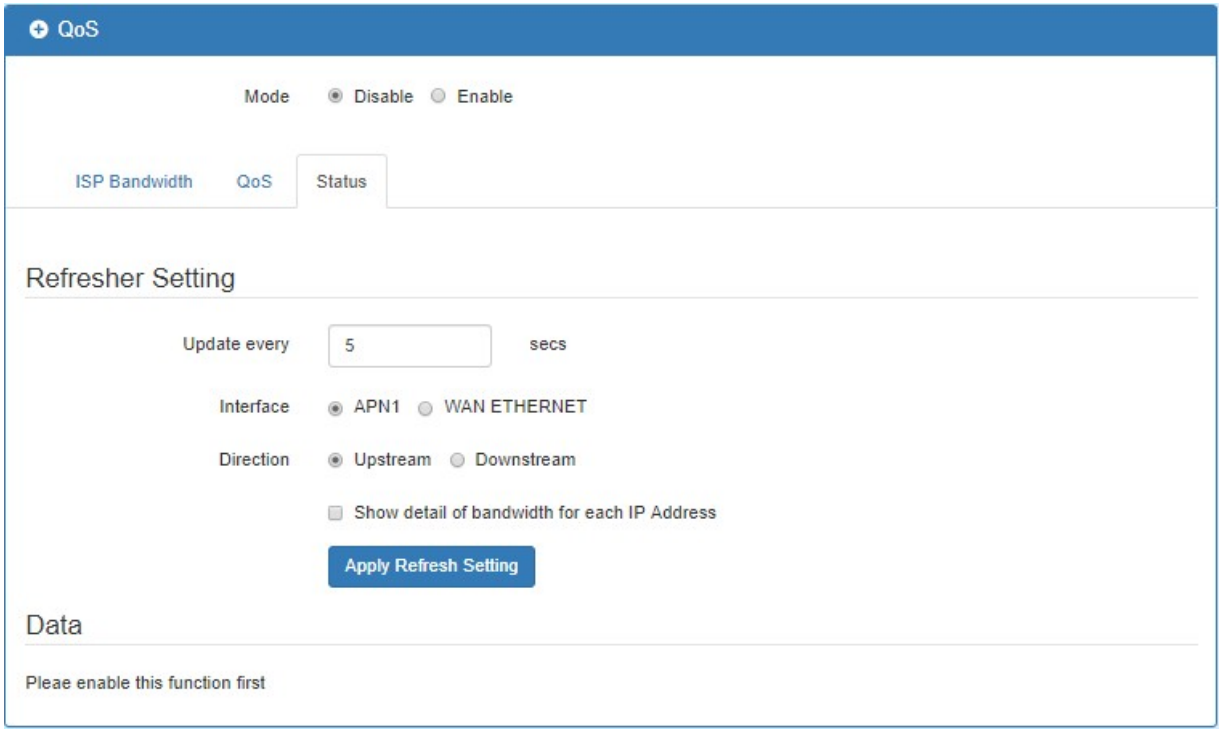
Note: To guarantee minimum bandwidth for assigning each IP, you should select **Bandwidth divided for each IP Address**.

13.9.3 QoS > Status

Refresher Setting select the showed content of bandwidth usage by following items:

- Refresh rate: how long the browser will update the showed content once.
- Direct: show Upstream or Downstream.
- Show detail bandwidth for each IP address: show the group IP bandwidth usage.
- Apply Refresh Setting button: press this button to take above new setting effect.

Data part is the content of bandwidth usage.

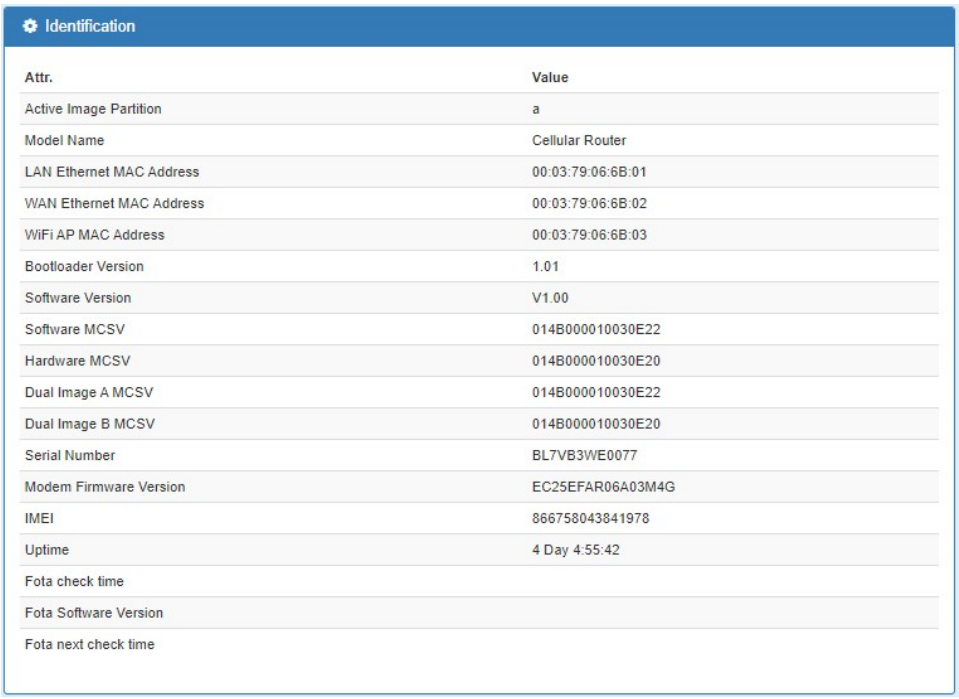


14 Configuration > Management

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.

14.1 Management > Identification

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



Identification

Attr.	Value
Active Image Partition	a
Model Name	Cellular Router
LAN Ethernet MAC Address	00:03:79:06:6B:01
WAN Ethernet MAC Address	00:03:79:06:6B:02
WiFi AP MAC Address	00:03:79:06:6B:03
Bootloader Version	1.01
Software Version	V1.00
Software MCSV	014B000010030E22
Hardware MCSV	014B000010030E20
Dual Image A MCSV	014B000010030E22
Dual Image B MCSV	014B000010030E20
Serial Number	BL7VB3WE0077
Modem Firmware Version	EC25EFAR06A03M4G
IMEI	866758043841978
Uptime	4 Day 4:55:42
Fota check time	
Fota Software Version	
Fota next check time	

Management > Identification	
Item	**Description**
Active Image Partition	Show the active image partition: a or b
Model Name	The model name of cellular router.
LAN Ethernet MAC Address	The LAN Ethernet MAC address.
WAN Ethernet MAC Address	The WAN Ethernet MAC address.
WiFi AP MAC Address	The WiFi AP MAC address.
Bootloader Version	The bootloader version of the device.
Software Version	The software version currently running on the device.
Software MCSV	Show the software MCSV of the running firmware
Hardware MCSV	Show the current hardware MCSV of the device.
Dual Image A MCSV	Show the Dual Image A MCSV.
Dual Image B MCSV	Show the Dual Image B MCSV.
Serial Number	Show the product serial number.
Modem Firmware Version	Show the modem firmware version of the device
IMEI	Show the IMEI (International Mobile Equipment Identity number).
Uptime	Show the current system uptime.
FOTA check time	Show the FOTA check time.
FOTA Software Version	Show the FOTA software version.
FOTA next check time	Show the FOTA next check time.

14.2 Management > Administration

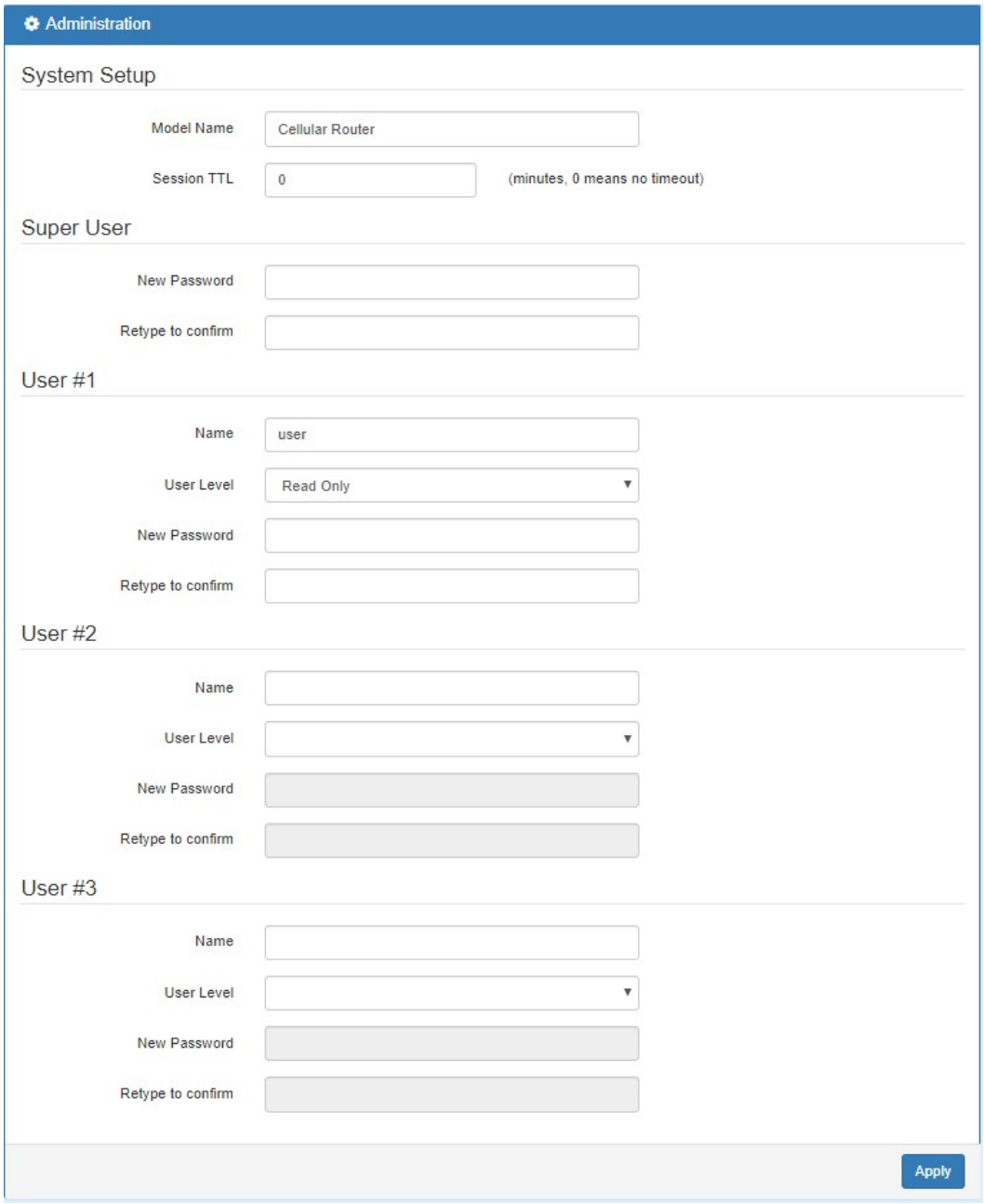
This section allows you to set up the name of the device and change your new password. For the **Session TTL**, you can set up what duration of time will be logout. If you don't need to have this timeout limitation, you can fill in "0"(Zero). The default timeout is 5 minutes.

For different users' authority, you can set up each level and password from this section.

(1) Super User can set User 1, 2 and 3 and give them different level authority:

- Level Administrator – can see and can apply each function except super user's password.
- Level Read Only – only can see the current configuration of each function.

(2) Non-super user can only edit his/her password.

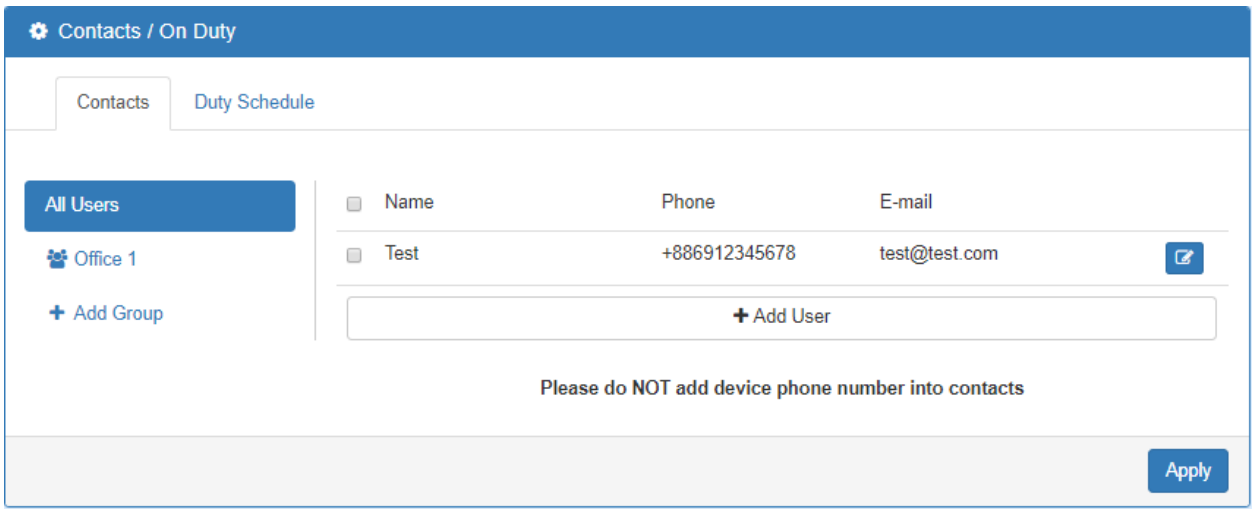


14.3 Management > Contacts / On Duty

There are two pages, **Contacts** and **Duty Schedule**. **Contacts** allows you to create the groups, and add the users. **Duty Schedule** is to select the duty date for specified groups. The on duty group members can receive alarm, perform SMS actions and input SMS alarm.

14.3.1 Contacts

You can create the groups, and add the users by Contacts.

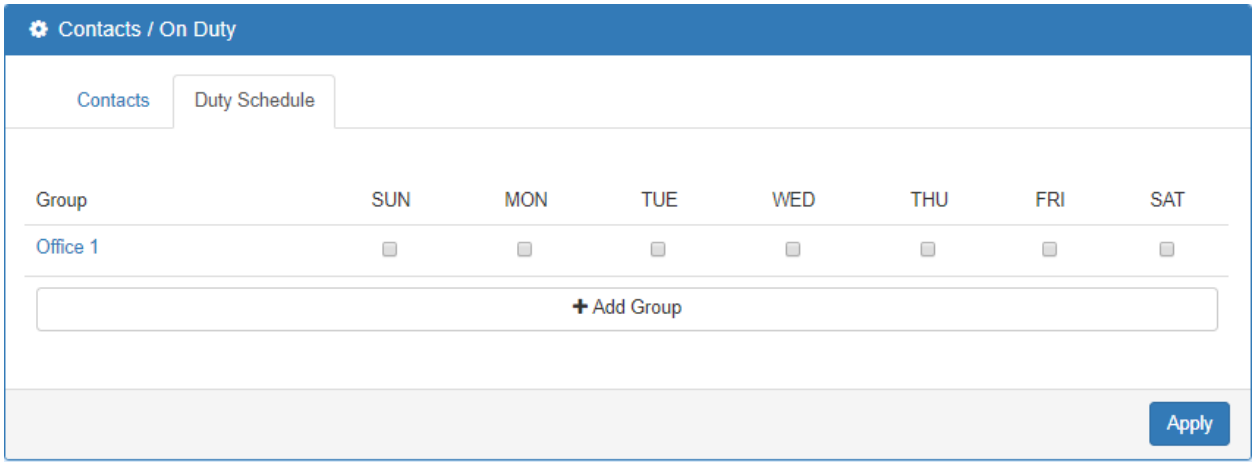


+ Add Group: Please fill out group name.

+ Add User: Please fill out Name/Phone/E-Mail/Groups.

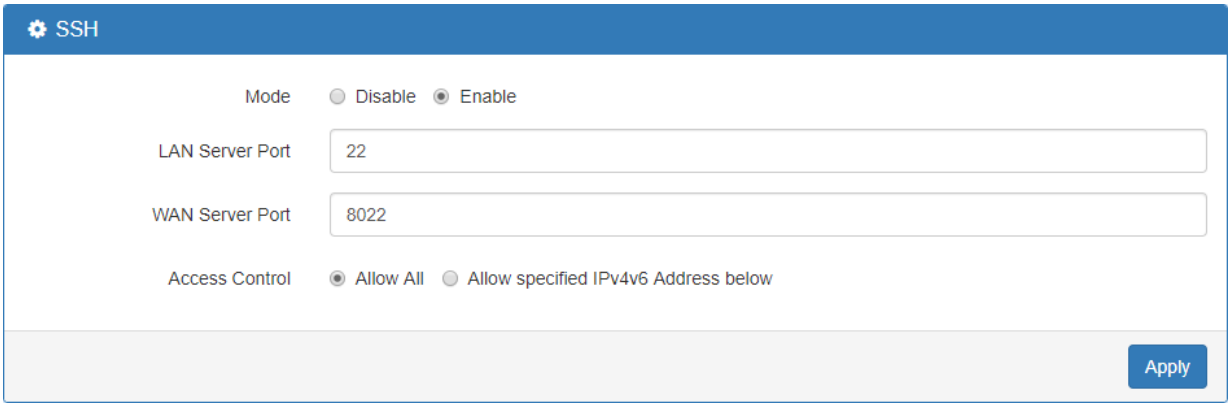
14.3.2 Duty Schedule

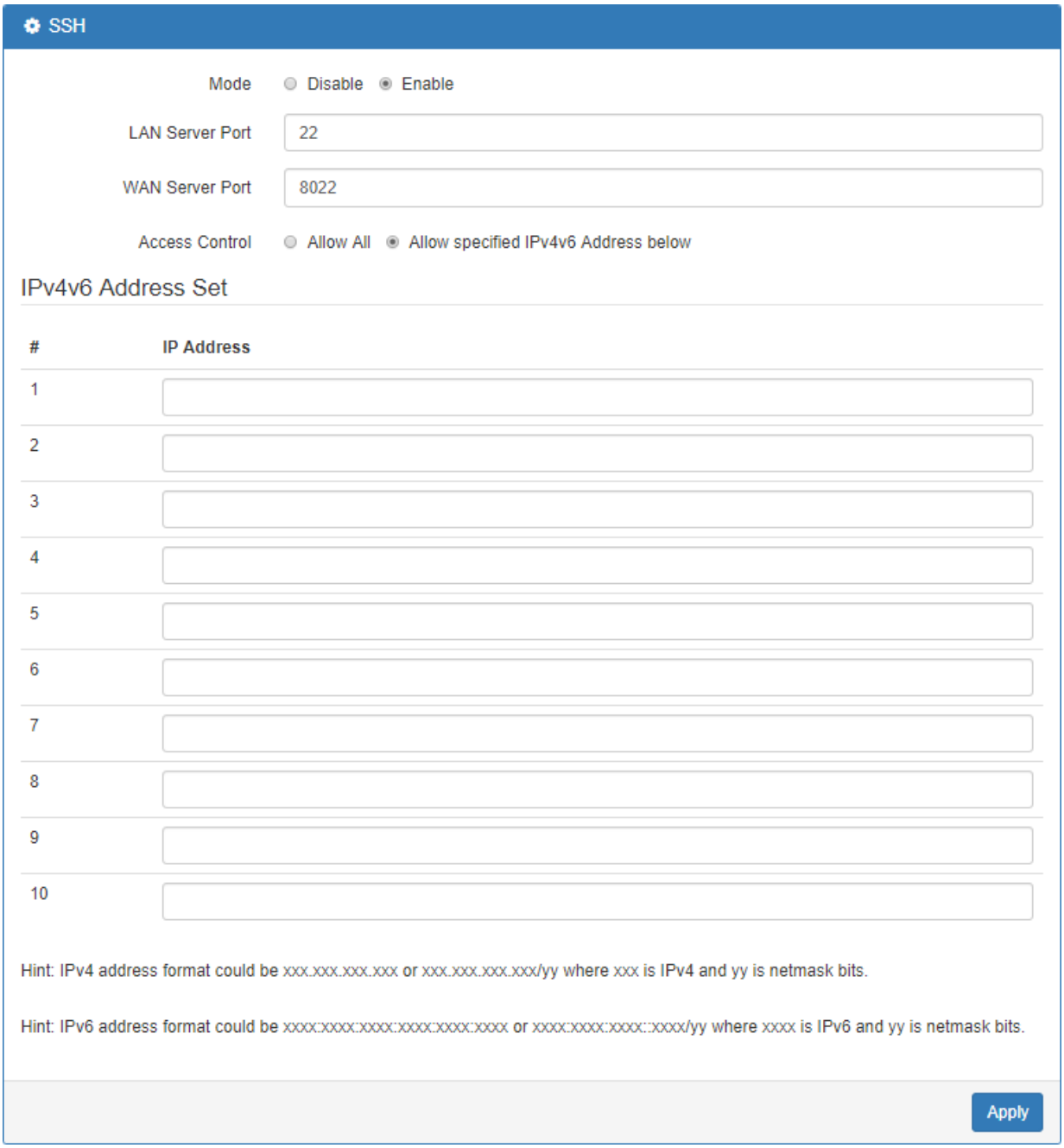
Please select duty date for every group. The trust and responsible groups can control/receive alarms and SMS.



14.4 Management > SSH

Secure Shell (SSH) allows user to configure system via a secure channel. User can configure system from either public domain or local LAN.





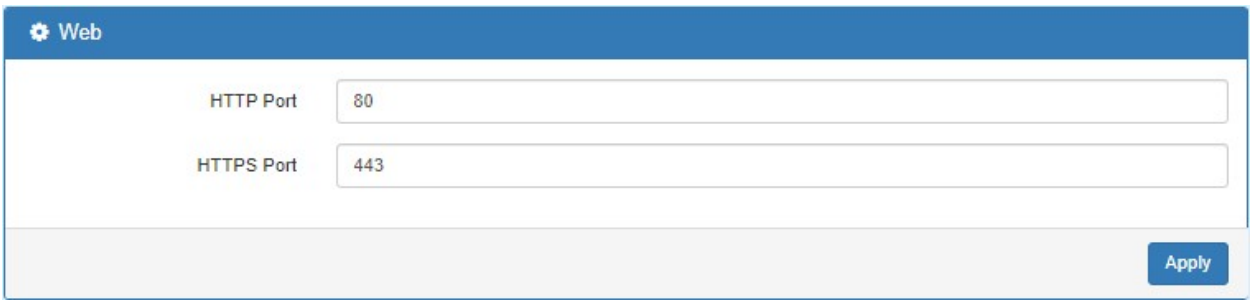
Management > SSH	
Item	**Description**
Mode	Select from Disable or Enable SSH function.
LAN Server Port	The LAN side TCP port number listened by SSH server.
WAN Server Port	The WAN side TCP port number listened by SSH server.
Access Control	• **Allow All:** Any client who own the IPv4v6 Address can reach system is able to connect system. • **Allow specified IPv4v6 Address below:** Only those configured IPv4v6 Address client are allowed to connect system.

14.5 Management > Web

This section allows user to change the HTTP port via HTTP. As long as pressing Apply, the web daemon will restart the new configuration, and you won't see the response at the web browser.

After pressing Apply button, the device will apply immediately and give you some hints "Please use new port to access latter". For example, port 3000.

Management > Web	
Item	**Description**
HTTP Port	The TCP port listened by HTTP daemon.
HTTPS Port	The TCP port listened by HTTPS daemon.



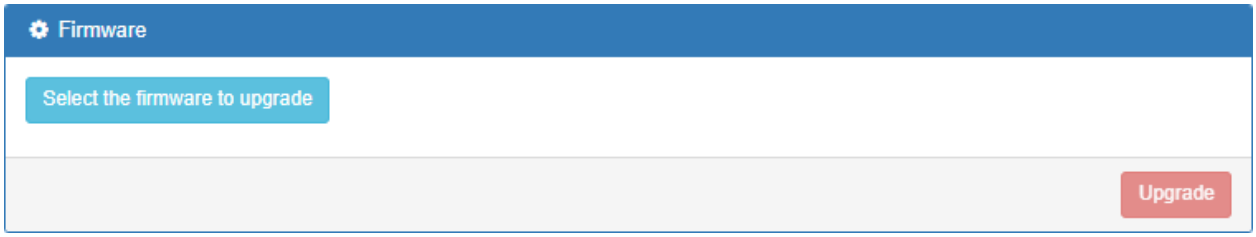
14.6 Management > Firmware

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.

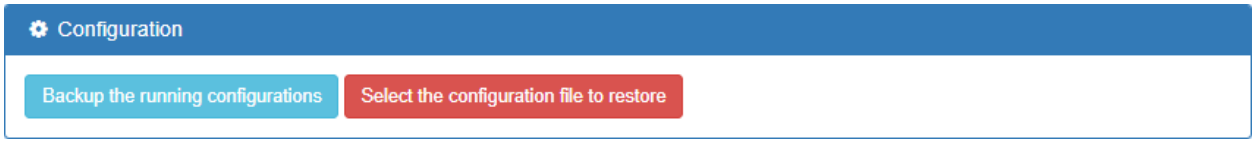
(3) After upgrading successfully, please reboot the router.



14.7 Management > Configuration

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

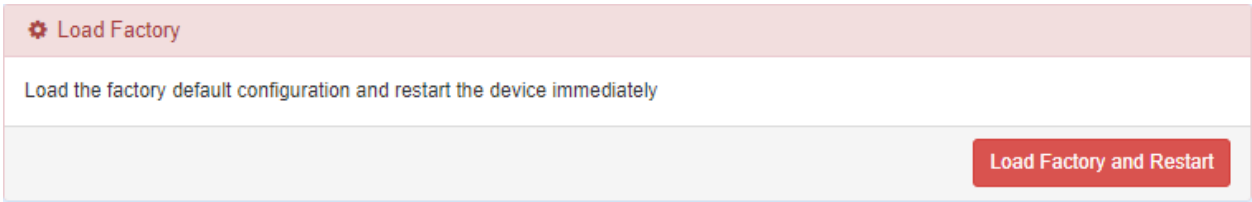
(1) Click Backup the running configurations button to export your current configurations.



(2) Click Select the configuration file to restore button to import the configuration file.

14.8 Management > 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.

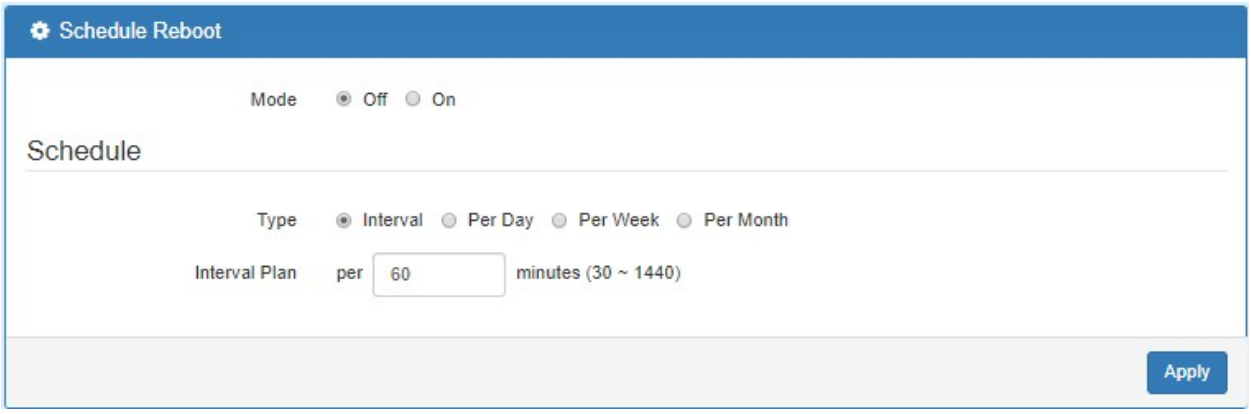


14.9 Management > Restart

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

14.10 Management > Schedule Reboot

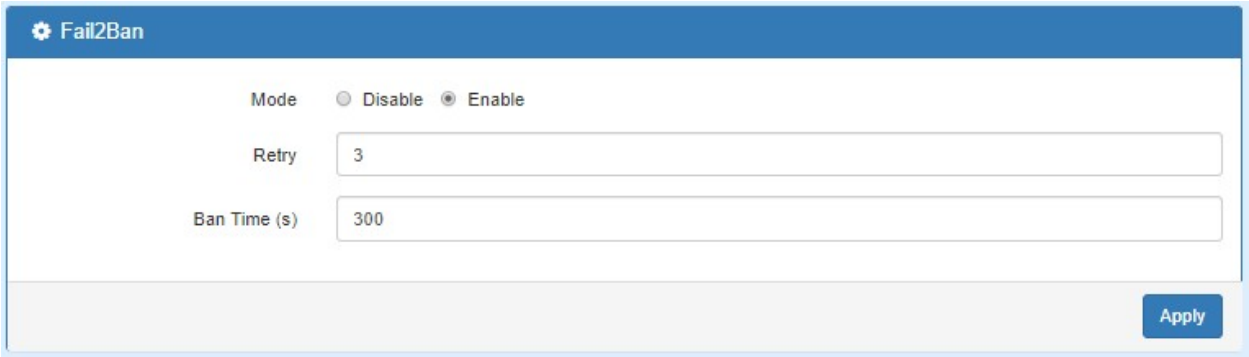
The setting allows you to schedule the reboot time regularly.



Management > Schedule Reboot	
Item	**Description**
Mode	Select the mode from Off or On. The default is Off.
Type	Schedule types include Interval, Per Day, Per Week, and Per Month.
Interval Plan	Input the interval minutes which you want to plan.

14.11 Management > Fail2Ban

Fail2Ban is an intrusion prevention feature that protects the device from brute-force login attacks.



Management > Fail2Ban	
Item	**Description**
Mode	Select from Disable or Enable. The default is Enable.
Retry	The limit for maximum login retries/attempts.
Ban Time(s)	The banned time(s) for user or IP when it exceeded the retry limit.

14.12 Management > FOTA

This section allows you to set up the Firmware Over-the-Air.

ADVICE

FOTA

Firmware Over the Air

- [ ] Enable
- [ ] Check only the new firmware version (not upgrade)
- [ ] Update backup partition image

Server URL: ftp://80.250.198.239:2121/fota_firmware.xml http://80.250.198.239:

Hint: ex:(ftp or http)://user:password@host:port/path

Schedule

Automatic: (•) Auto ( ) Custom

Custom: (•) Every day ( ) Every week

Immediately

[ ] Sun	00:00	-	01:00
[ ] Mon	00:00	-	01:00
[ ] Tue	00:00	-	01:00
[ ] Wed	00:00	-	01:00
[ ] Thu	00:00	-	01:00
[ ] Fri	00:00	-	01:00
[ ] Sat	00:00	-	01:00

Status

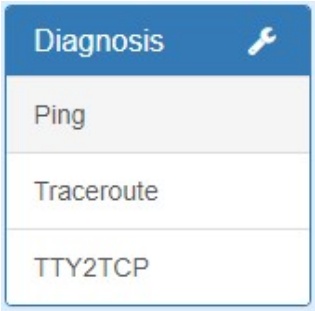
Attr.	Value
Update information server	
Firmware download server	
Fota check time	
Fota software version	
Result	
Fota next check time	

Apply

Management > FOTA	
Item	**Description**
Firmware Over the Air	
Enable	Enable or disable the FOTA function, which is Enabled by default.
Check only the new firmware version (not upgrade)	Only check, not download firmware from the server.
Update backup partition image	upgrade image to backup partition, sync two partition
Server URL	Enter custom server URL.
Schedule	
You can choose Auto or Custom, which is Auto by default.	
Auto	There are two options for automatic, every day or every week.
Custom	You can choose the time or execute it immediately
Status	Show the status information after running. Update information server, Firmware download server, FOTA check time, FOTA software version, Result, FOTA next check time.

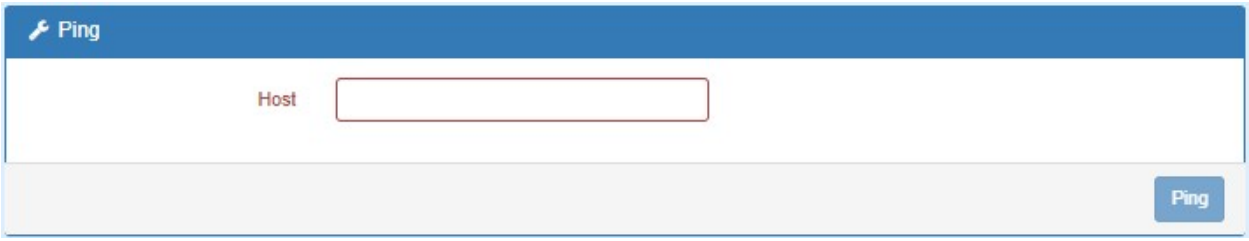
15 Configuration > Diagnosis

This section allows you to diagnose Ping,Traceroute, and TTY2TCP.



15.1 Diagnosis > Ping

Please assign the Host you want to ping.



Diagnosis > Ping	
Item	**Description**
Host	The host name or the host IP address

15.2 Diagnosis > Traceroute

Please assign the Host you want to traceroute.

Diagnosis > Ping	
Item	**Description**
Use Interface As Source	Use or not use the Interface as source
Use Interface	APN1 / APN2
Host	The host name or the host IP address

15.3 Diagnosis > TTY2TCP

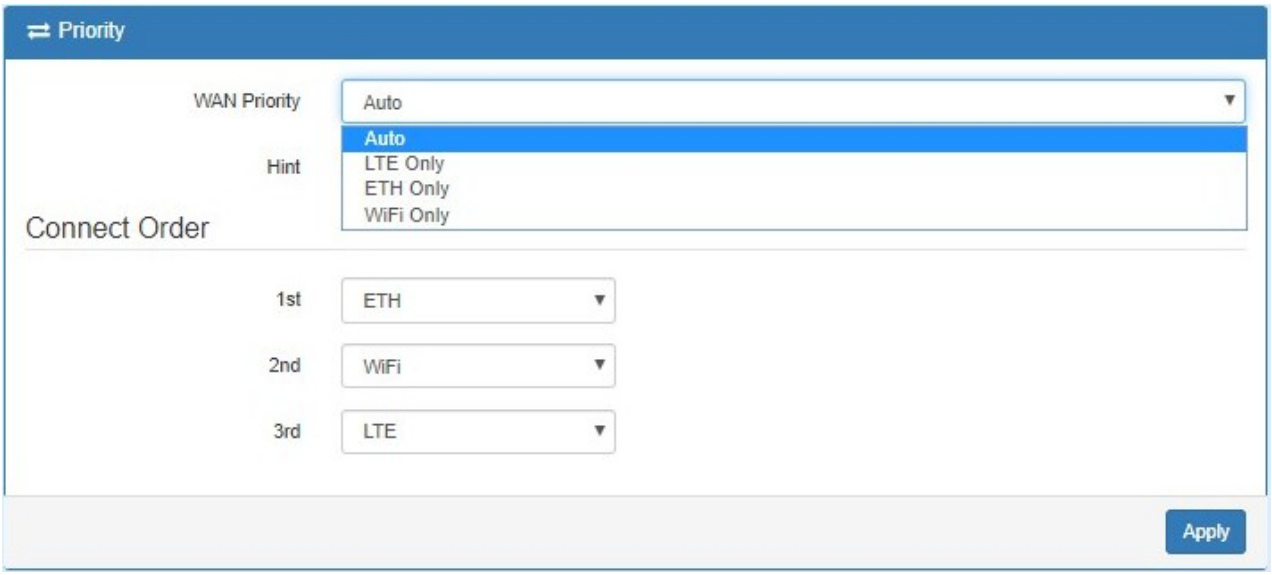
Diagnosis > TTY2TCP	
Item	**Description**
Port number	the port number to issue TTY2TCP
Start	start TTY2TCP
Stop	stop TTY2TCP

16 Configuration Applications

This section explains specific examples how to configure your applications.

16.1 WAN Priority

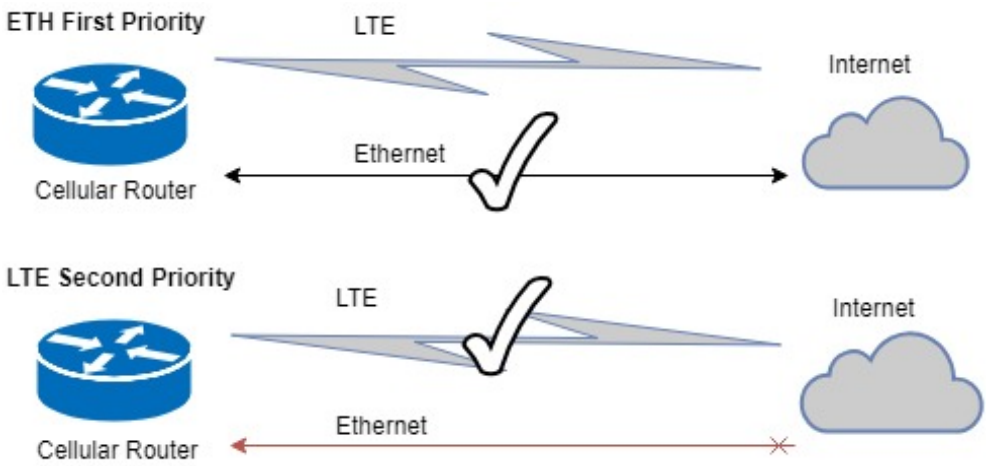
You can select from Auto, LTE Only, ETH Only or WiFi Only. Moreover, you can configure Connect Order to set up the priority.



(1) WAN Priority > ETH First:

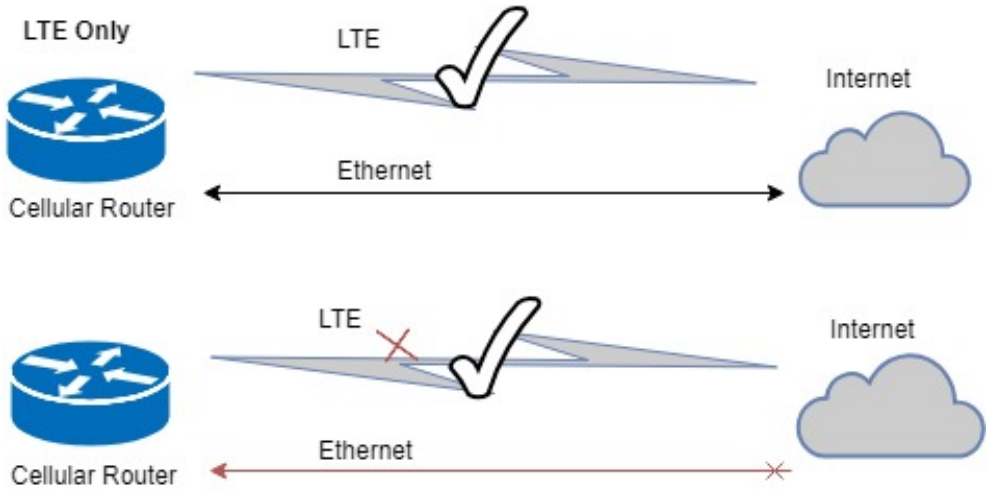
In case both Ethernet and LTE can access Internet, the router would route network packages through Ethernet. The reason is Ethernet that is low price and stable.

However, in case Ethernet is unplug or not able to access Internet (check by ping), the router would route network packages through LTE network.



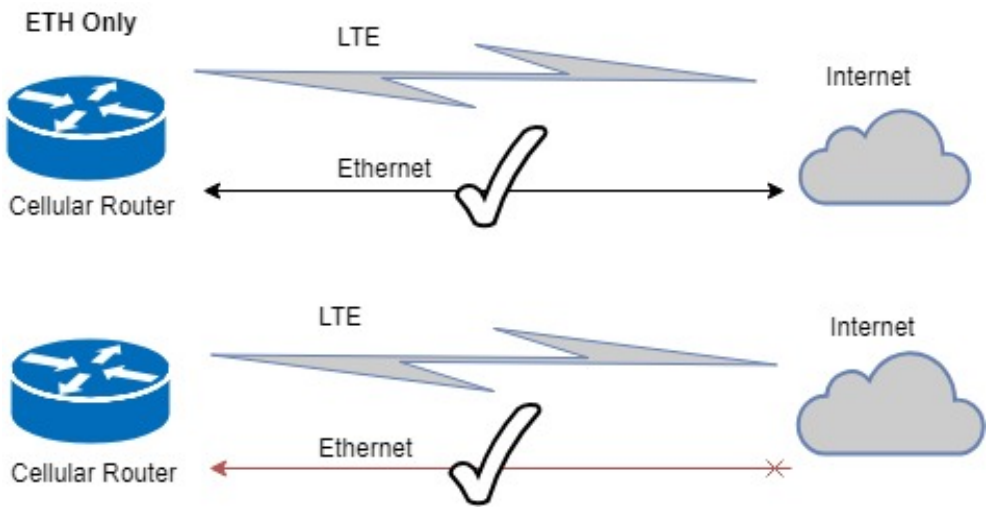
(2) WAN Priority > LTE Only:

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



(3) WAN Priority > ETH Only:

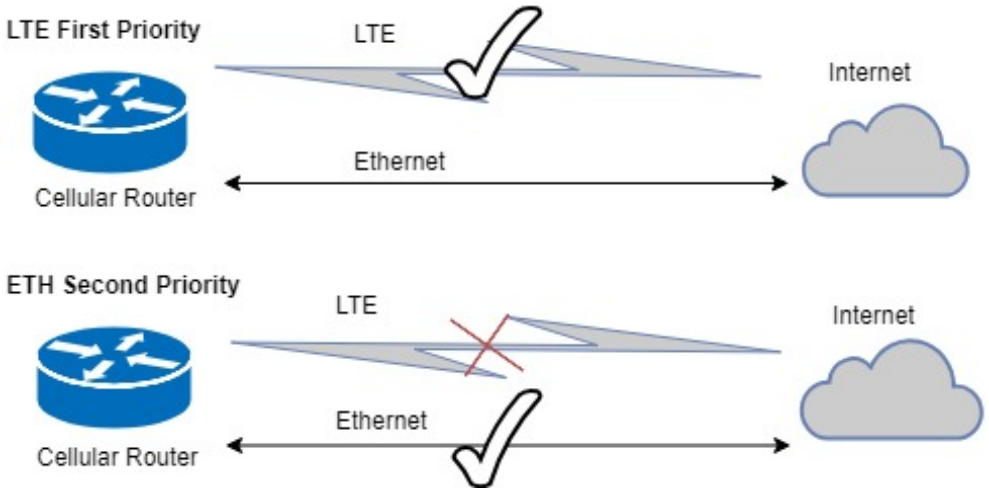
In this mode, the router only routes network packages through Ethernet.



(4) WAN Priority > LTE First:

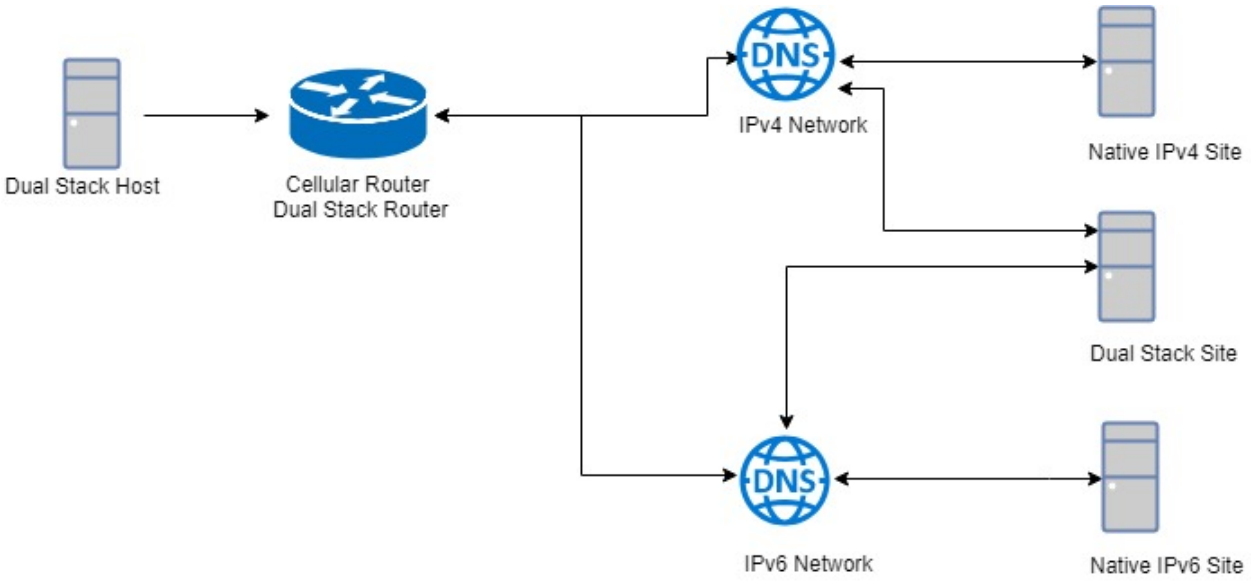
In case both Ethernet and LTE can access Internet, the router would route network packages through LTE.

However, in case LTE is unplug or not able to access Internet (check by ping), the router would route network packages through Ethernet network.



16.2 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.

LAN Ethernet

Attr.	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	2001:b400:e230:cdfe::1
IPv6 Conn Time	5 Day 3:38:09
Uplink Speed Kbps	0.000
Downlink Speed Kbps	0.000
Tx/Rx KBytes	84411.000/0.000
Tx/Rx Dropped Packets	0/0

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

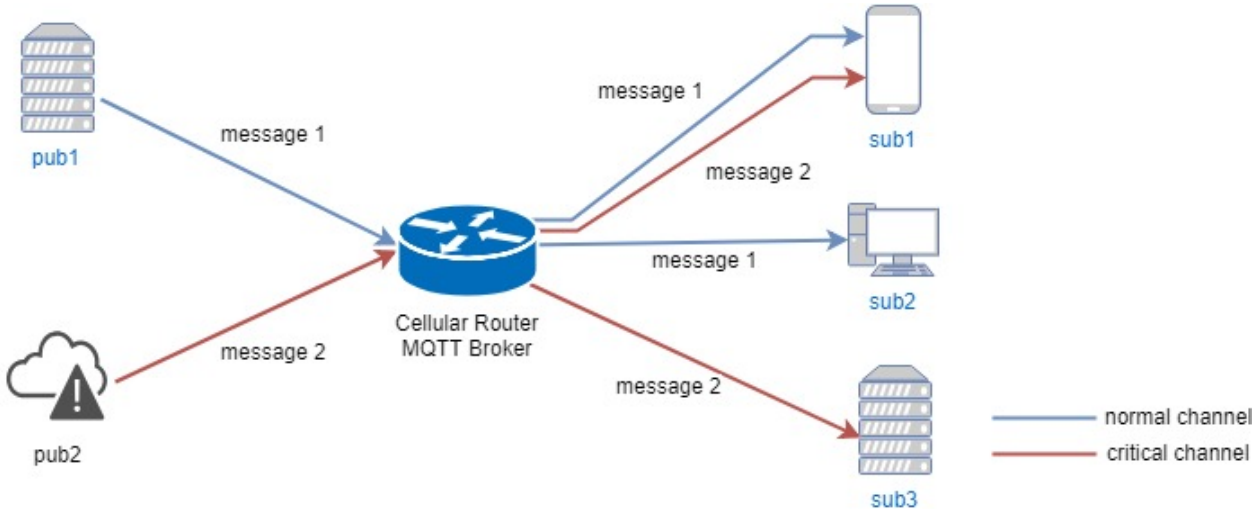
Command Prompt (1)

```
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:\>
```

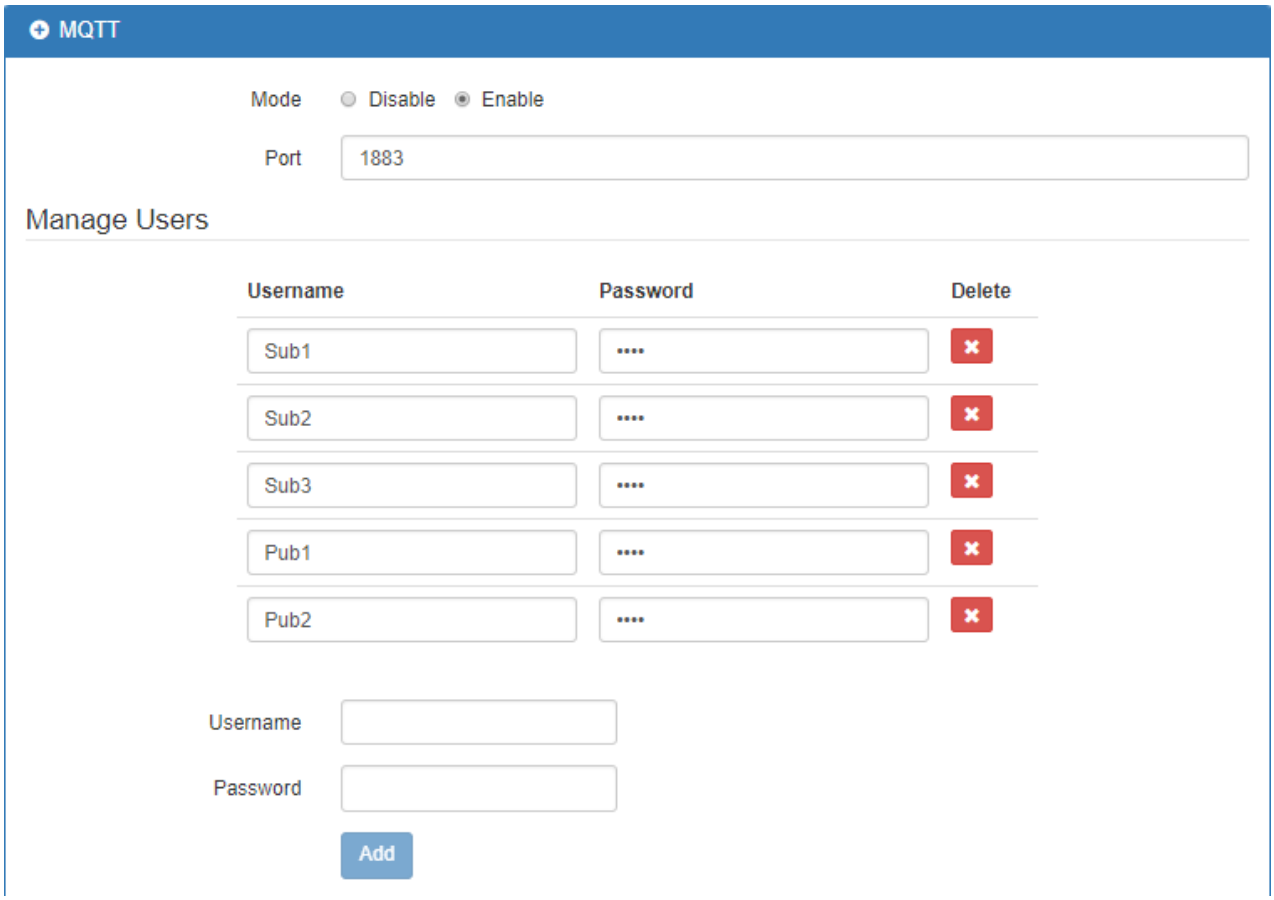
16.3 MQTT Broker

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.

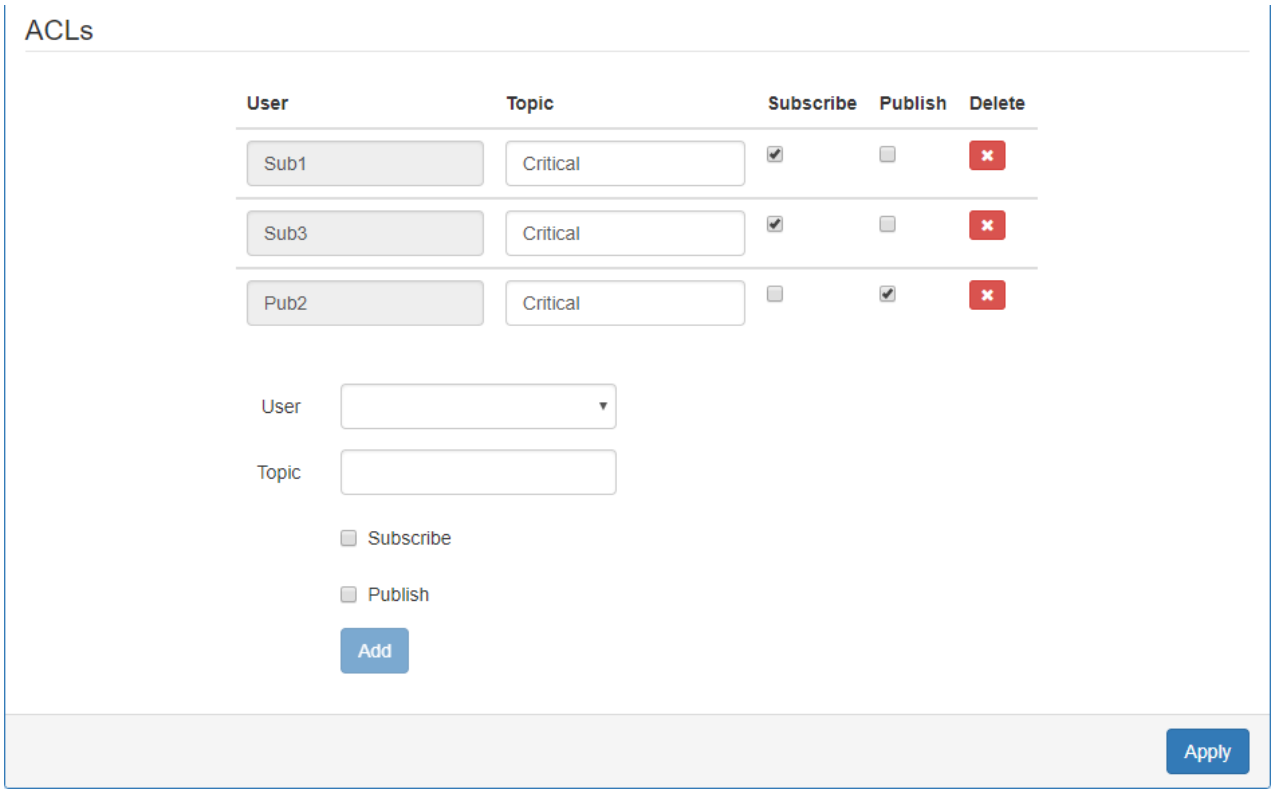


The **Manage Users** section will show all created users. Each user can use the **delete** button to delete it. For the ACL control, you can specify what topic should be limited.

For example, we set the publisher **pub2** to write the critical topic.

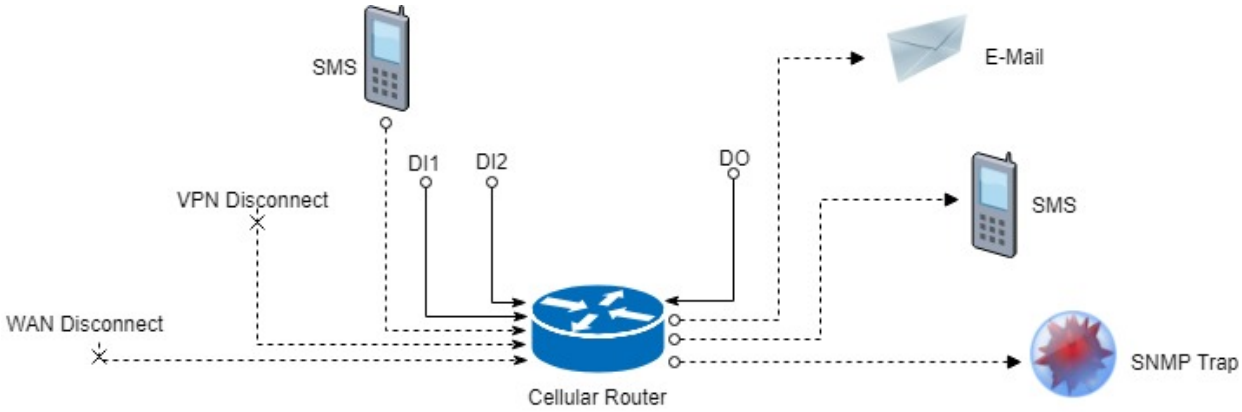
Additionally, we also the subscribers **sub1** and **sub3** can read the critical topic.

Thus, when **pub2** is sending the message only the **sub1**, the **sub3** can receive it.



16.4 Alarm Configuration

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



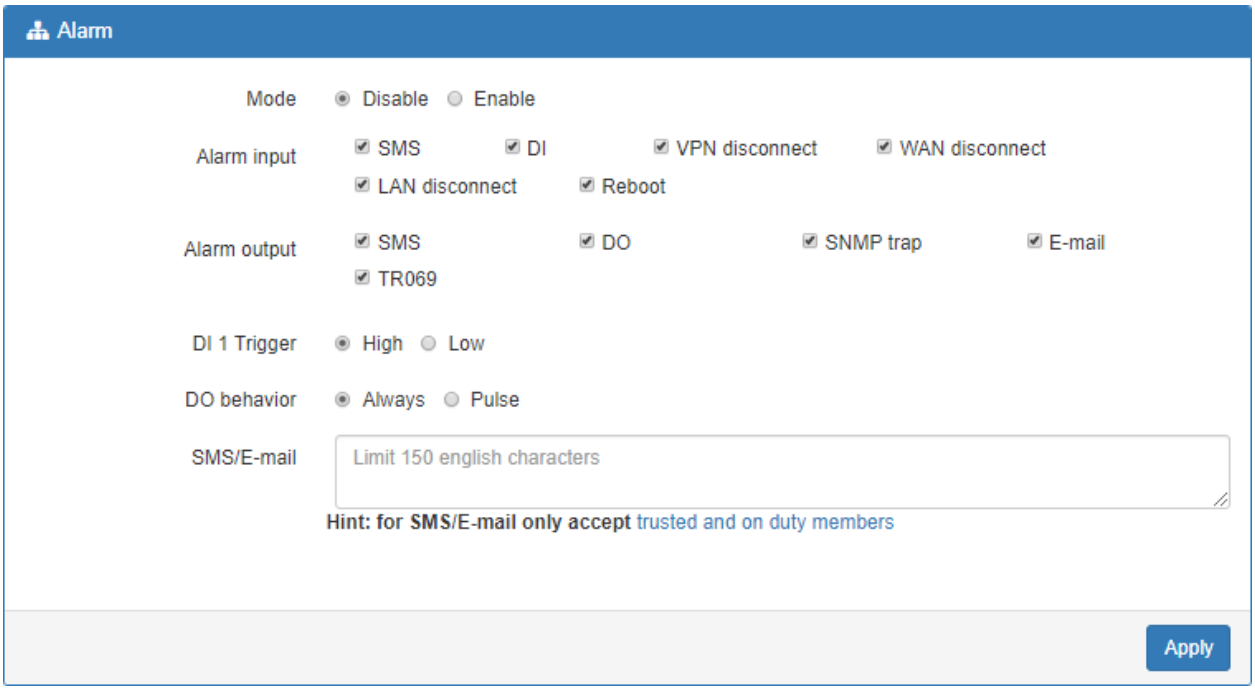
(1) Alarm Input:

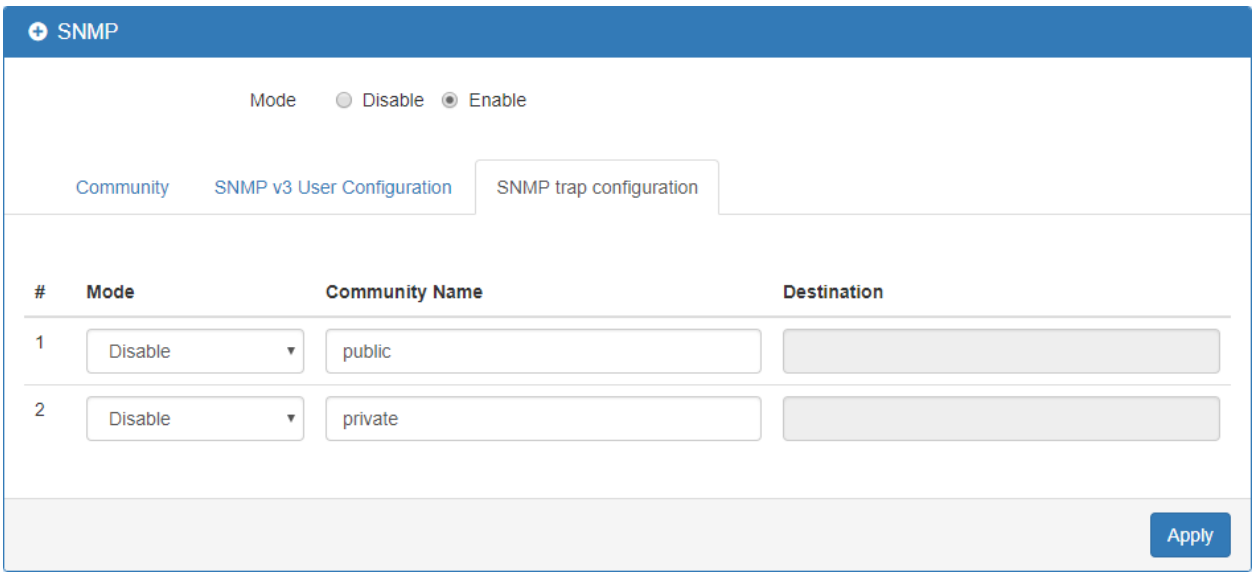
- The alarm would be triggered when DI1/DI2 show(s) high signal.
- The user's phone number is in device contact phone book can send a SMS to device SIM card to trigger alarm.
- VPN / WAN disconnect would trigger alarm no matter which interface is currently using.

(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.





16.5 Open VPN Configuration

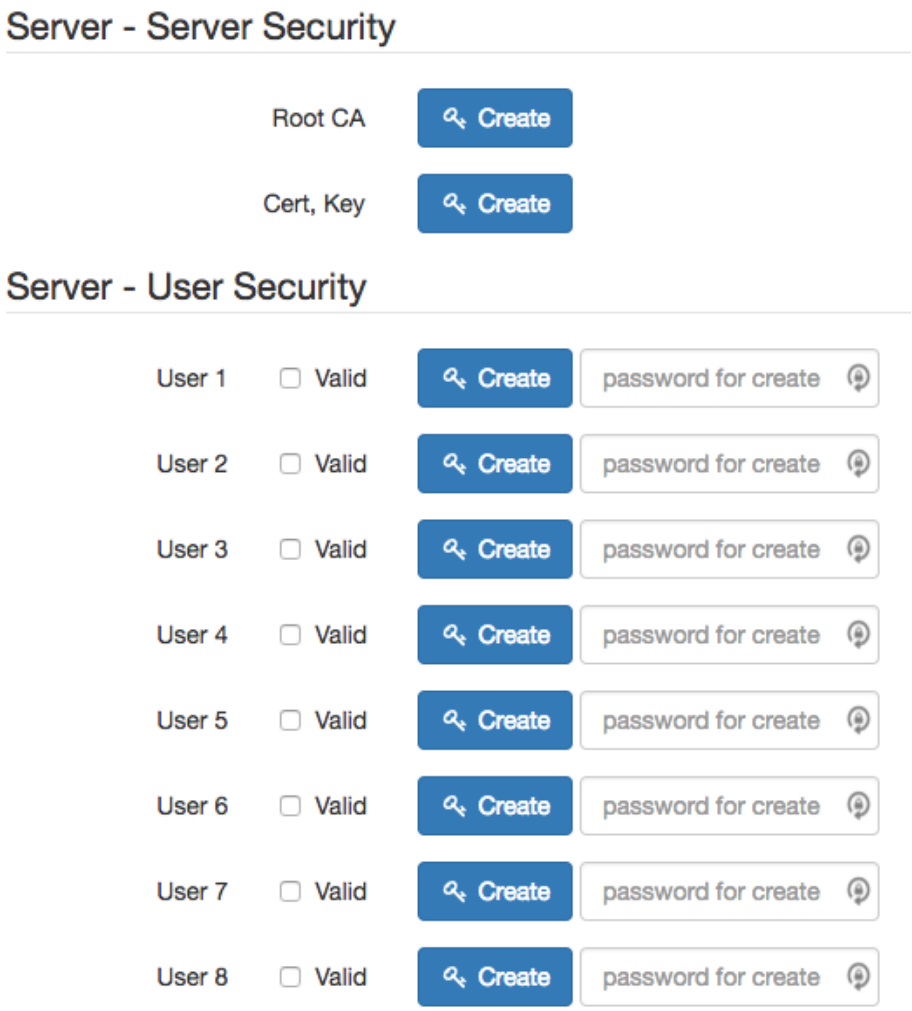
Generic setup

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

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

16.5.1 Open VPN Server Mode

Open VPN server certificate generation

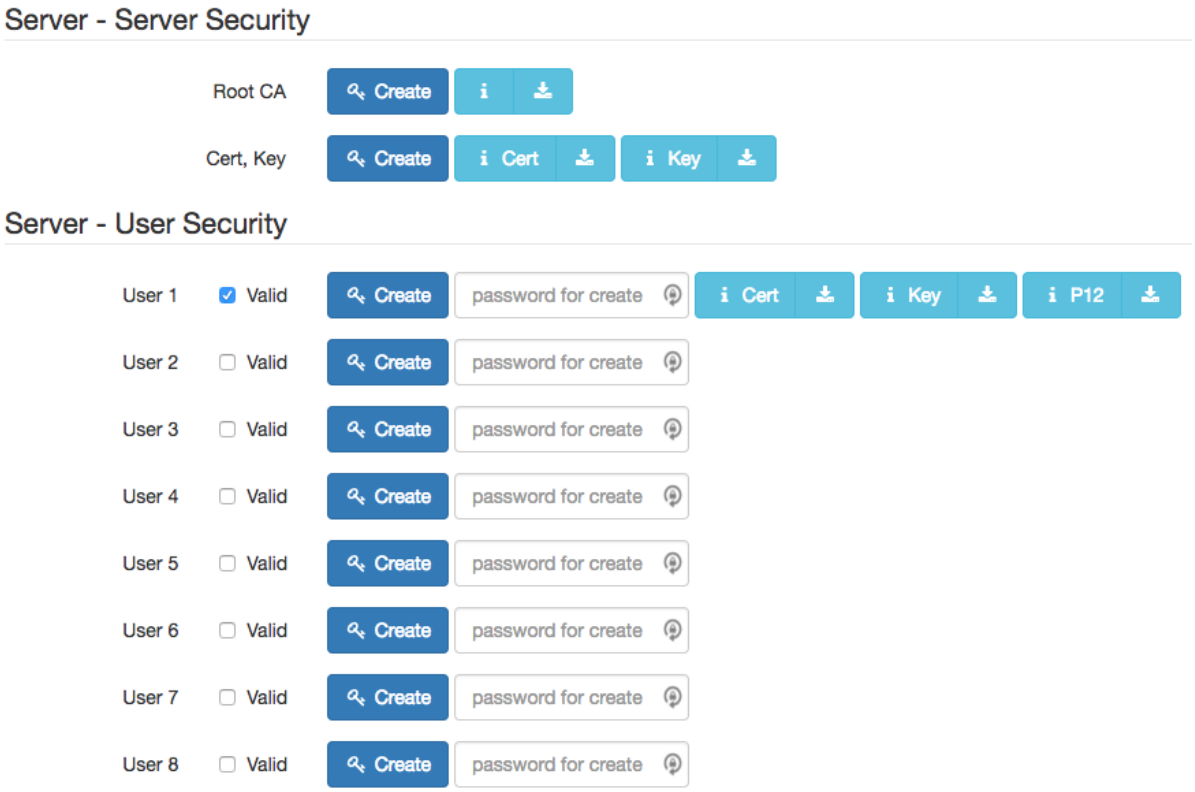


For the Open VPN server mode, the Open VPN web UI provides the buttons to generate the required files. The files include **Root CA**, **Cert**, **Key** and **Open VPN** client files. The file will be generated when you click the corresponded **Create** button.

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

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

The password will be used in the Open VPN client when the client uses **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.

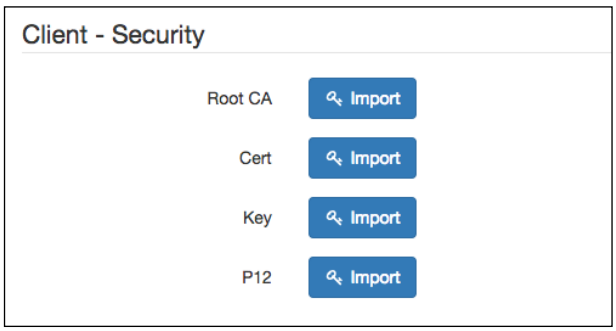
16.5.2 Open VPN Client Mode

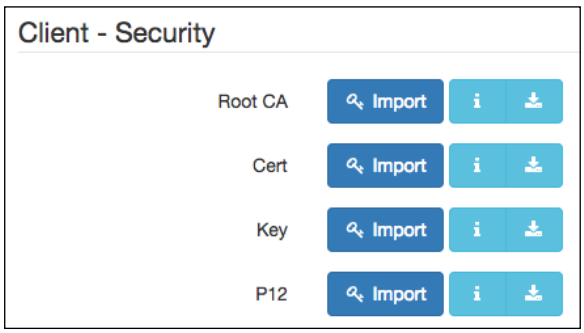
Open VPN client certificate import

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

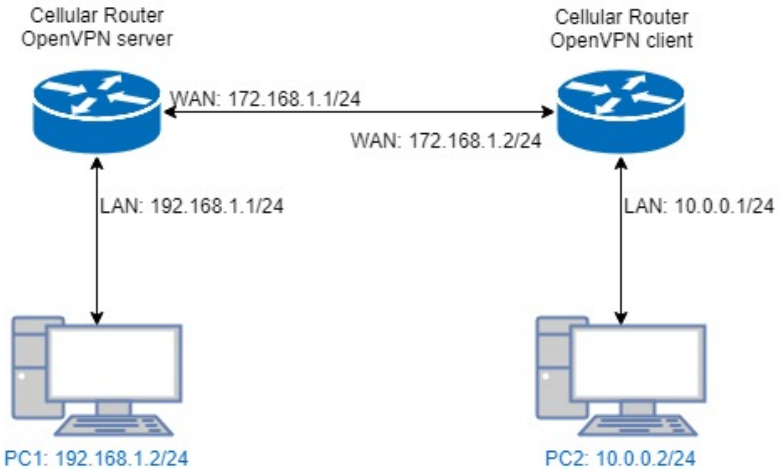




Same as Open VPN server part, you can use the info/download buttons to get the information of file or download the file to PC.

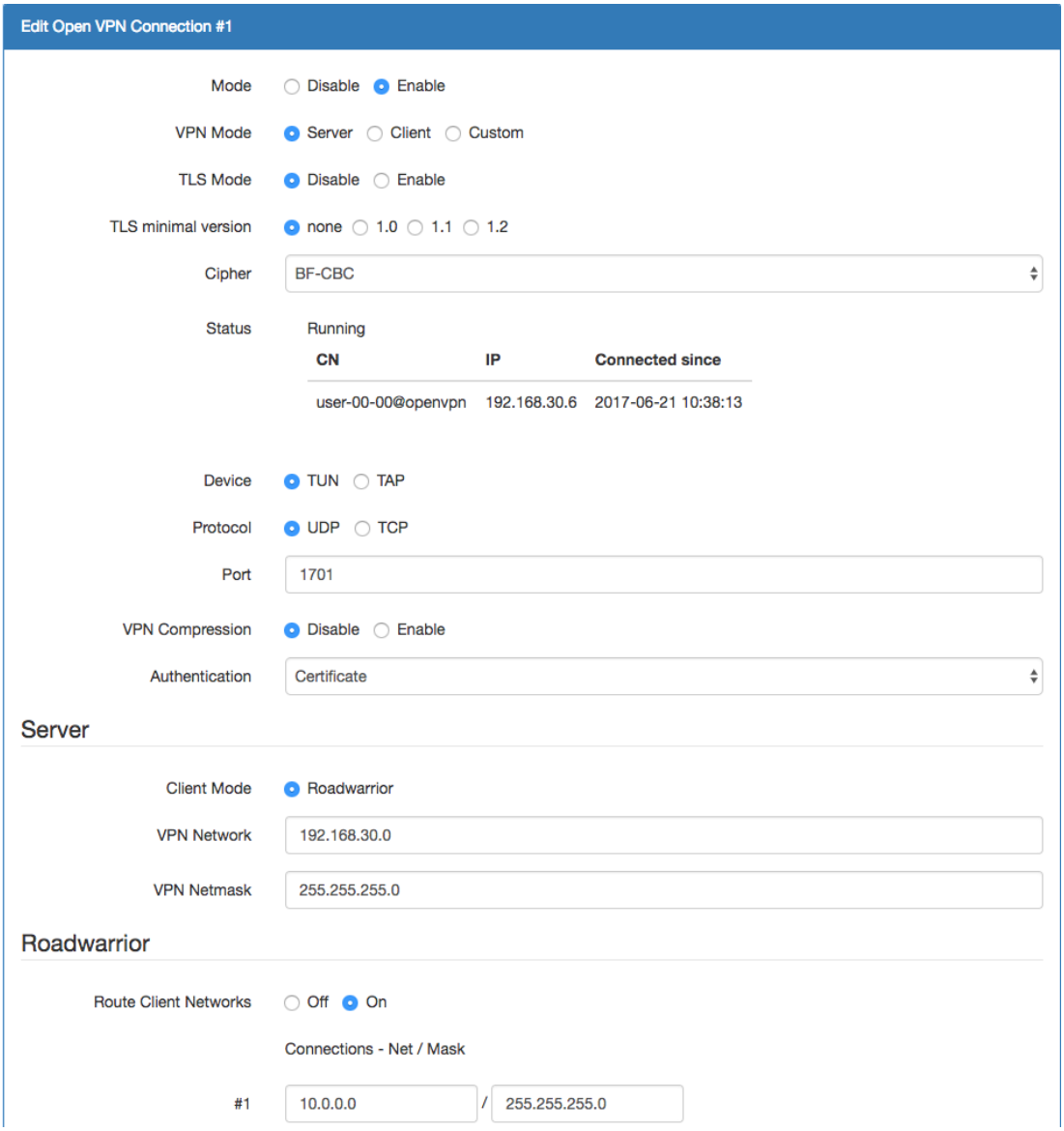
16.5.3 Open VPN Net-to-Net

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



(1) Open VPN server configuration

For the Open VPN 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 Open VPN 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 Open VPN server status should be **Running**. When Open VPN 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@Open VPN** 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...

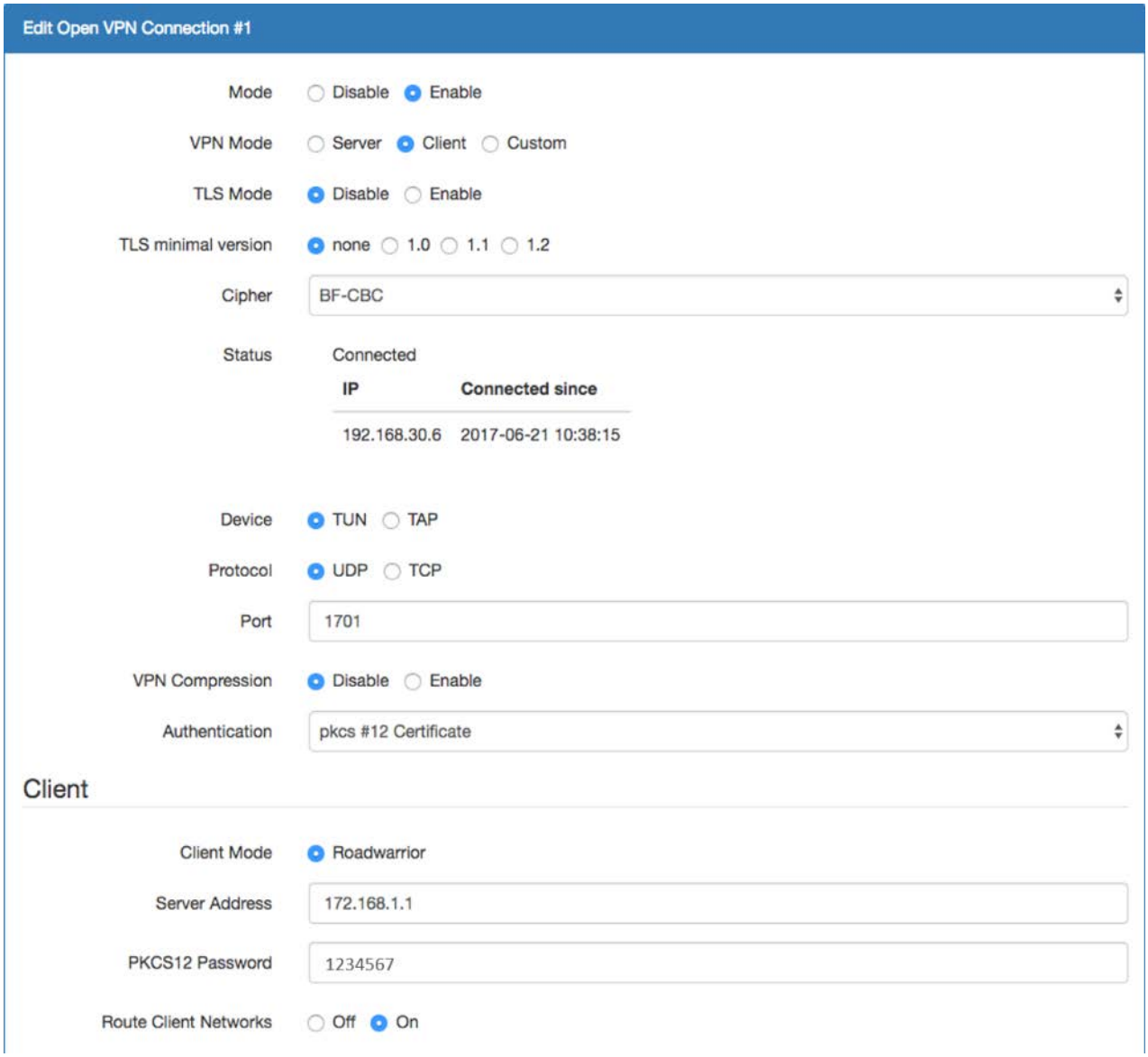
192.168.1.1/cgi-bin/openvpn.cgi?act=info&file=cert&type=user&conn_id=0&user_id...

```
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
WhcNMicwNTA3MDYzNDA4WiA/MOswCOYDVOOGEwJDSDETMBEGA1UECgwKc3Rvb25n
```

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

(2) Open VPN client configuration

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



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

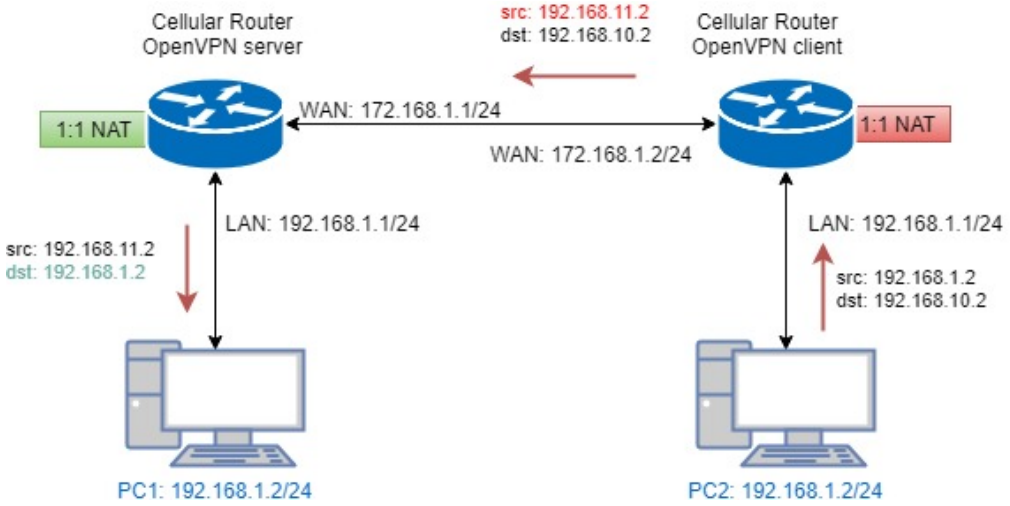
This option requires the P12 file which generated from Generic Setup Open VPN server part.

The password also be set on the Generic Setup Open VPN server part.

If you use the Certificate authentication option, the Open VPN client will require the **Root CA**, **User cert** and **User key** files.

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

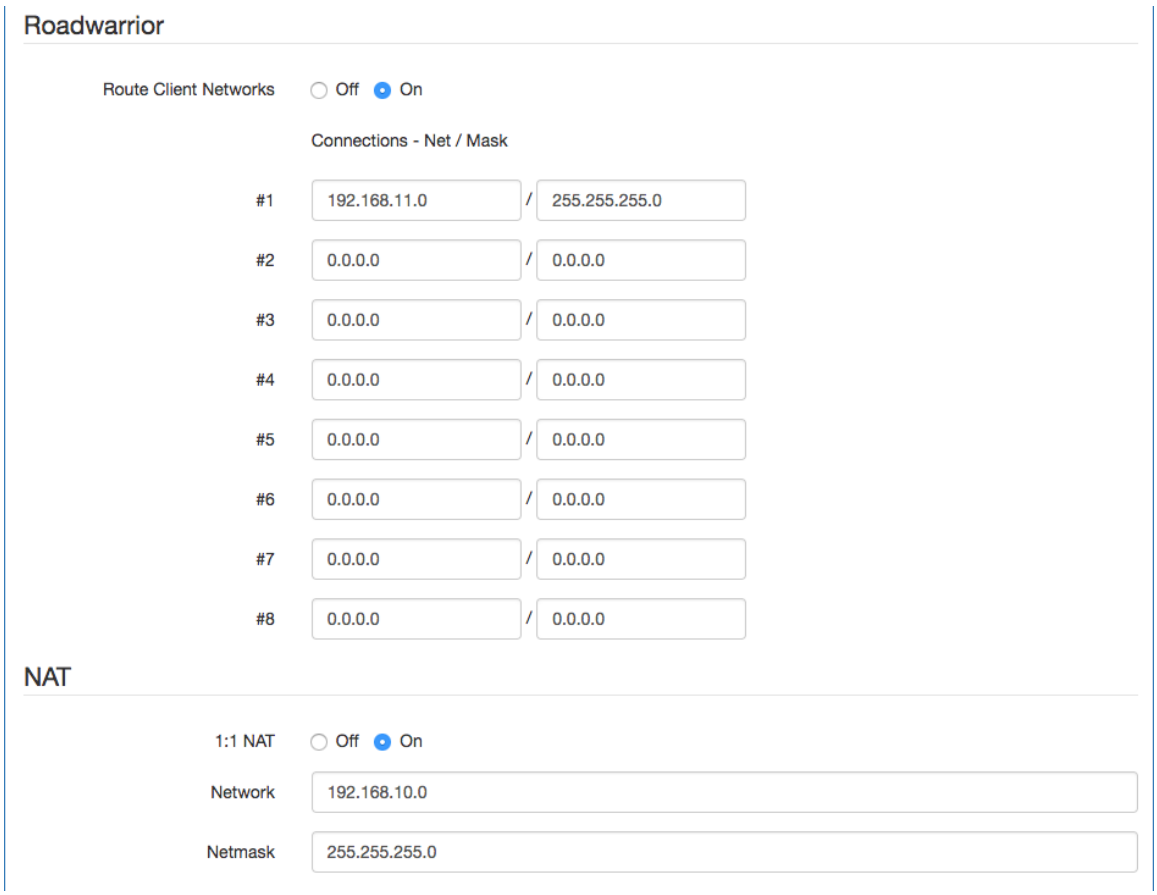
16.5.4 Open VPN 1:1 NAT



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

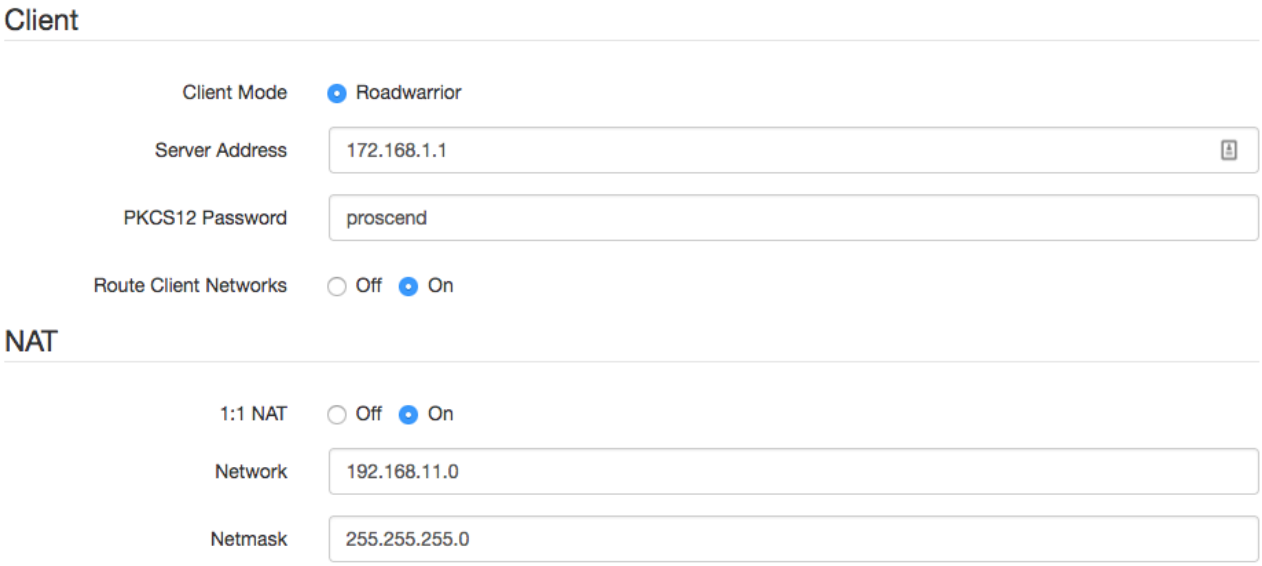
When this situation occurred, the routing rules will be ambiguous that will result in the PC1 and the PC2 can't communicate each other. Thus, the router Open VPN provides the 1:1 NAT feature. The feature will convert the conflict subnet to different subnet. In this case, you can use 1:1 NAT feature to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

For the Open VPN 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 Open VPN server side LAN network from **192.168.1.0/24** to **192.168.10.0/24** when the VPN traffic is coming.

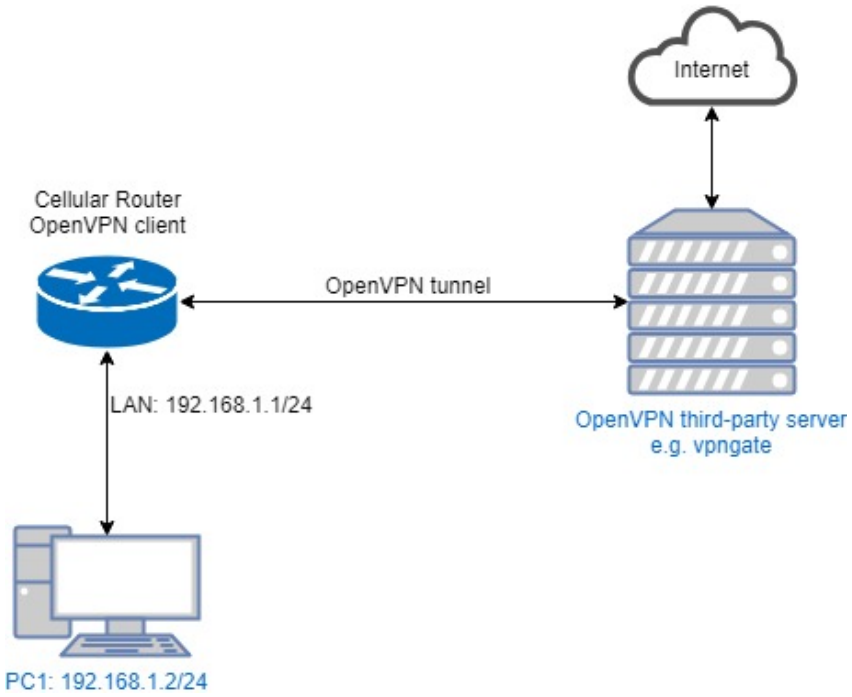


For the Open VPN client side, same as server side but we fill up the Network as **192.168.11.0**.

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



16.5.5 Open VPN with third-party server



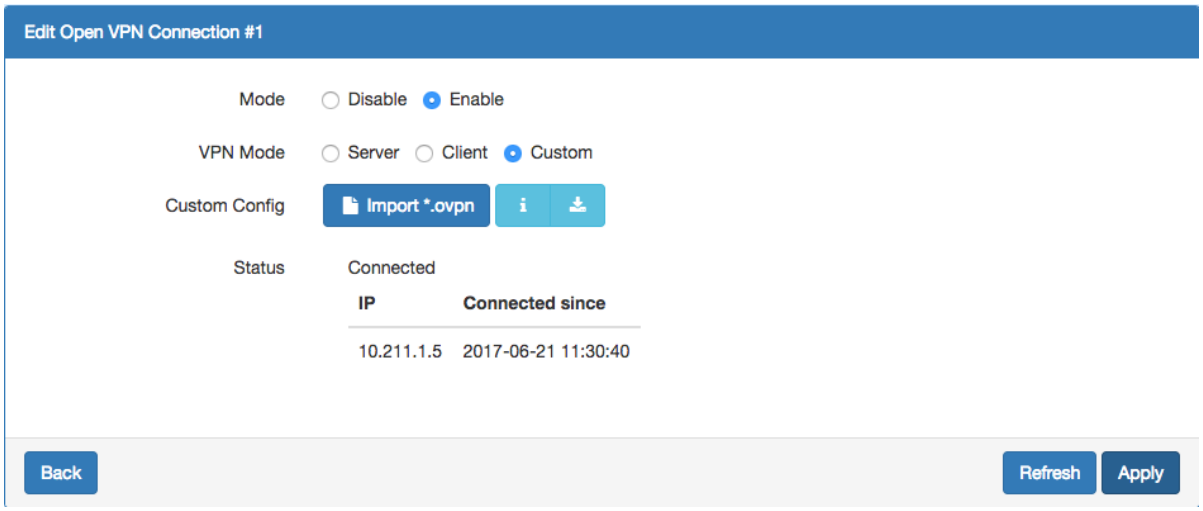
A VPN enables you to send and receive data across shared networks.

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

For example, use the Japan Open VPN server which provided by http://www.vpngate.net/en/.

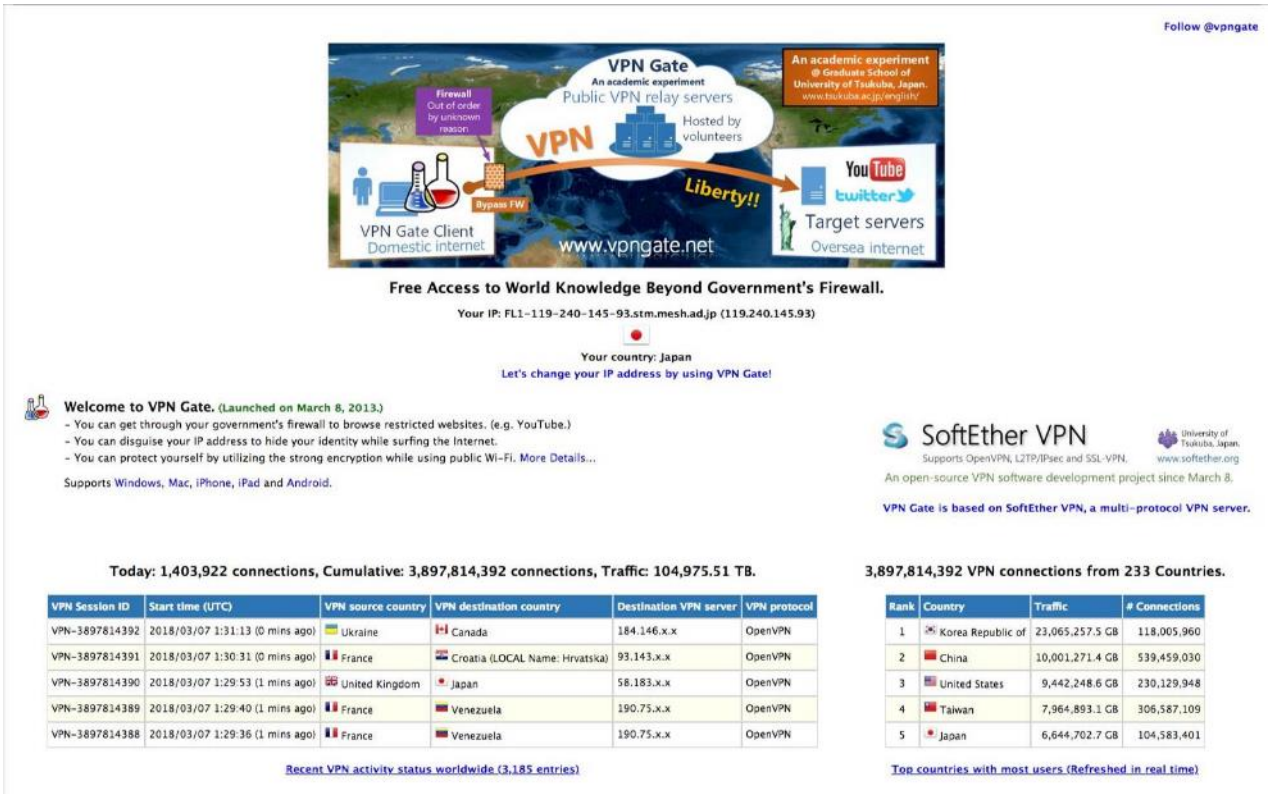
Firstly, download the ovpn configuration files from vpngate.net.

Additionally, use the Open VPN 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 Open VPN server is reachable, the VPN tunnel will be established.

When the Open VPN 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.



16.5.6 Install Open VPN Access Server on Docker

Open VPN Access Server on Docker installation

Open VPN Access Server is a full featured secure network tunneling VPN software solution that integrates Open VPN server capabilities, enterprise management capabilities, simplified Open VPN Connect UI, and Open VPN Client software packages that accommodate Windows, MAC,

Linux, Android, and iOS environments. Open VPN 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 Open VPN 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://Open VPN.net/index.php/access-server/pricing.html

Quick Installation

- **Prerequisites**
- Ubuntu 16.04
- curl or wget should be installed

Install via curl

sh -c "$(curl -fsSL https://bit.ly/2GrzYyS)"

Install via wget

sh -c "$(wget https://bit.ly/2GrzYyS -O -)"

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 Open VPN Access Server by docker image

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

sudo mkdir -p /Open VPN-as

sudo docker create --name=Open VPN-as \

-v /Open VPN-as:/config \

-e TZ="Asia/Taipei" \

-e INTERFACE=enp3s0 \

--net=host --privileged linuxserver/Open VPN-as

sudo docker start Open VPN-as

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

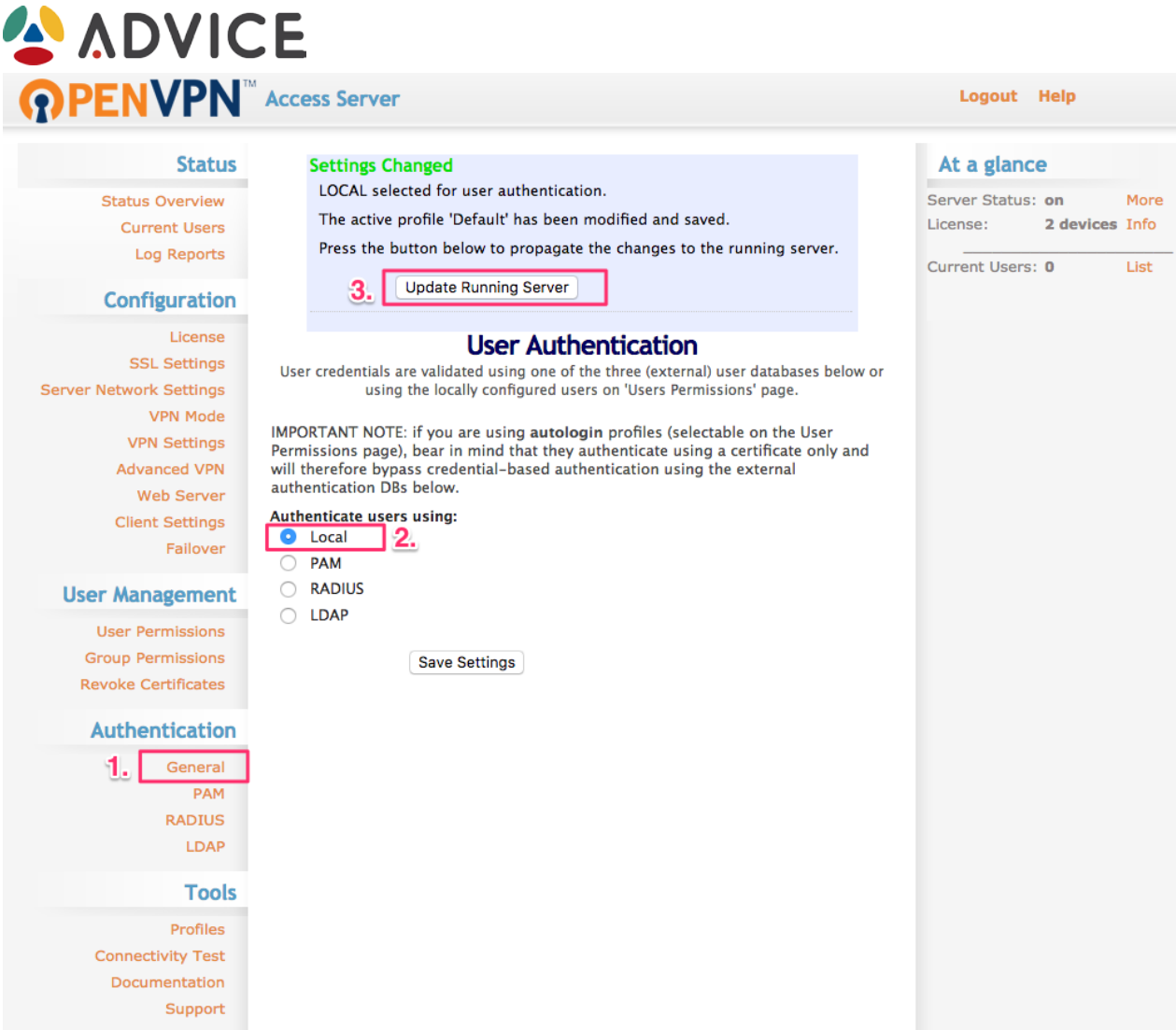
Setup Open VPN Access Server for Cellular Router

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

The default administrator username and password is admin/password.

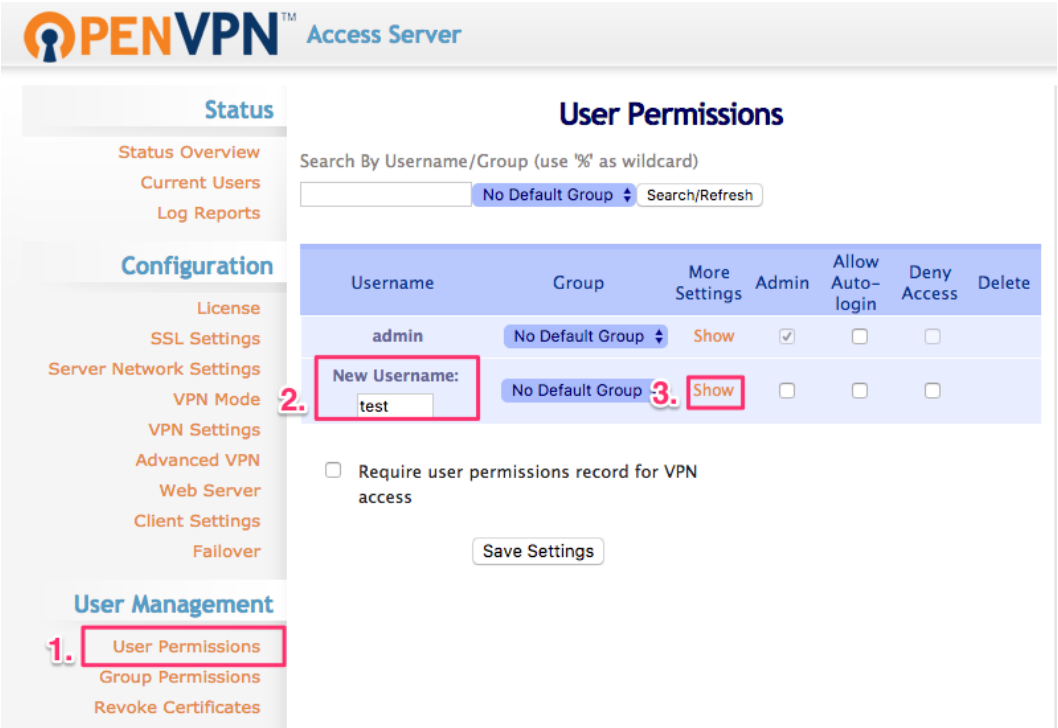
Login page:

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.)

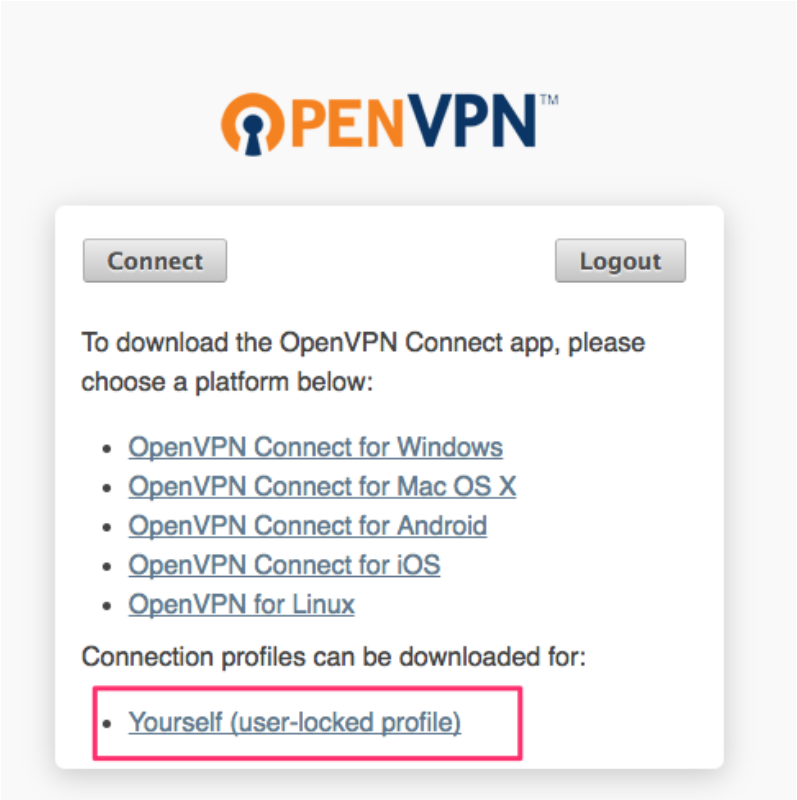


Also check the Access from all other VPN clients to make the Cellular Router could be reachable.

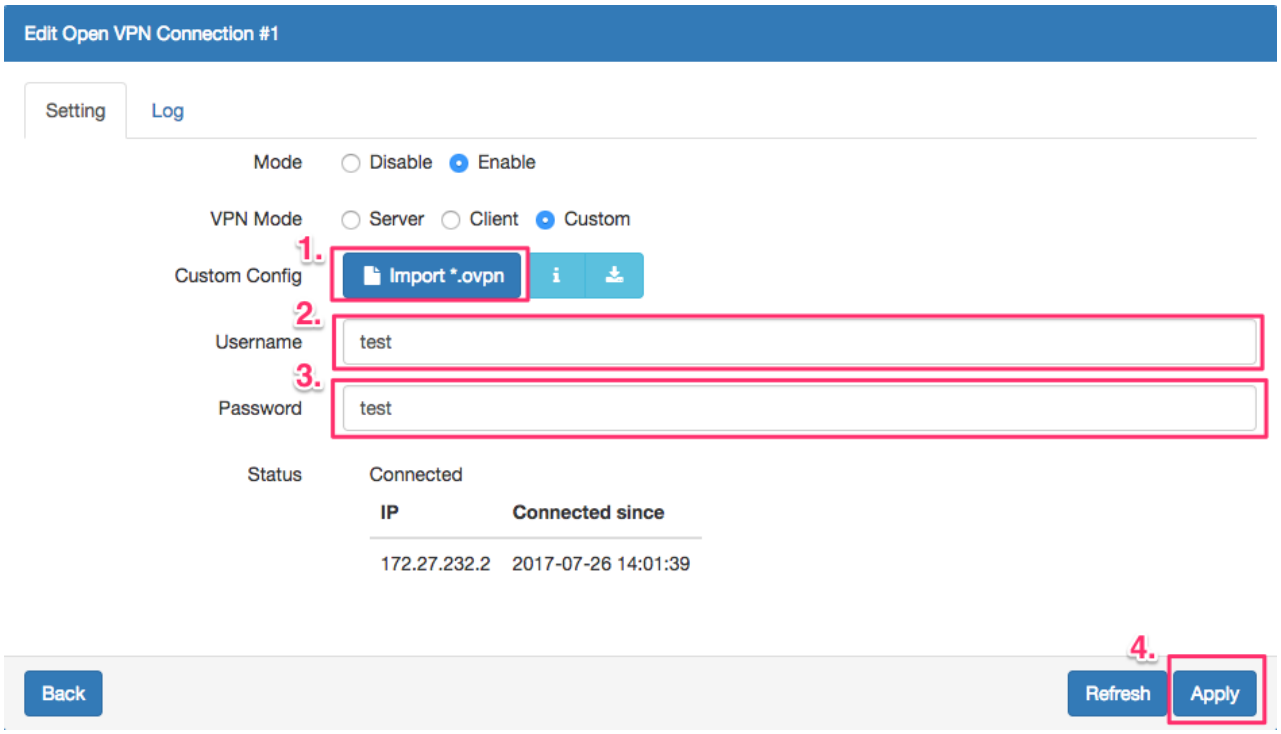
Setup Cellular Router Open VPN client

Use the user test/test to login https://<server_ip_or_domain>:943

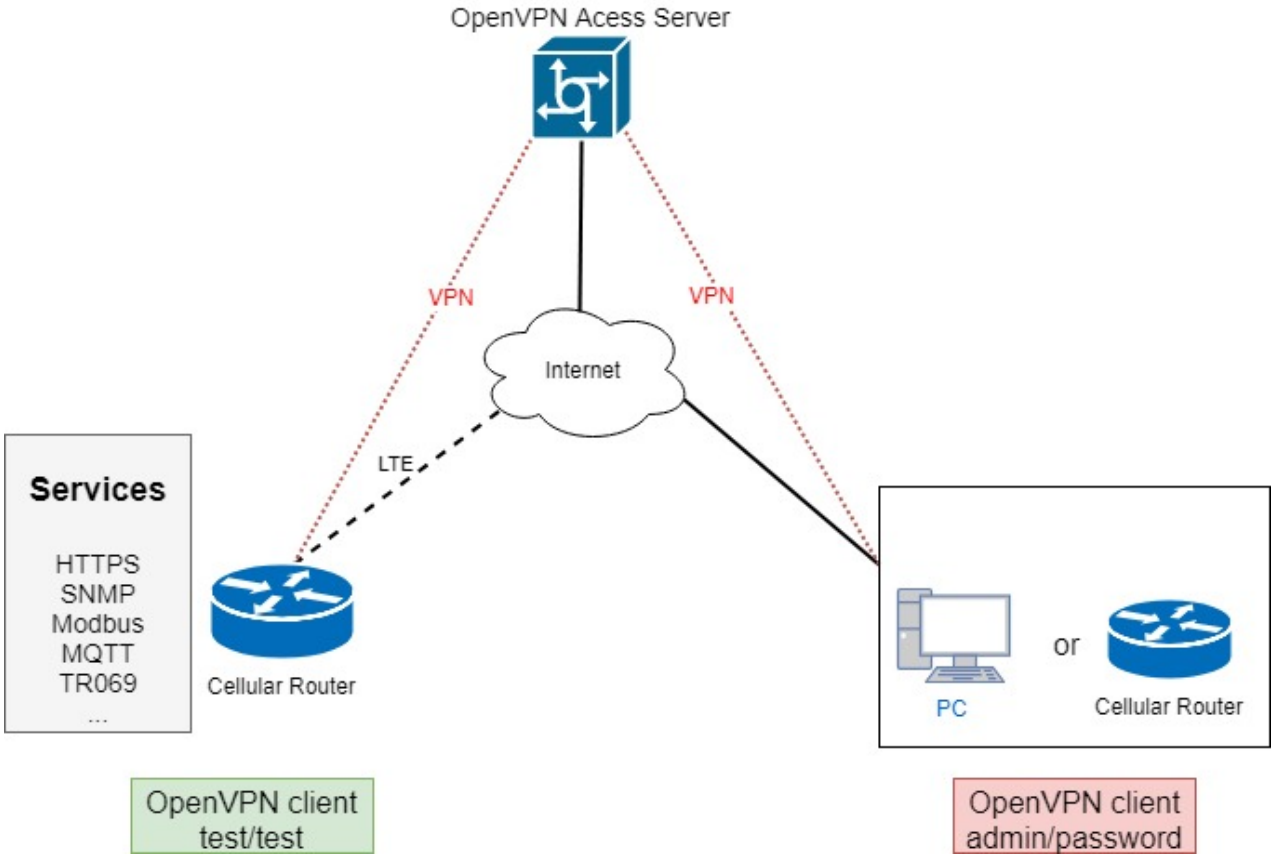
Please make sure to change the type from Connect to Login.



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



Upload the .ovpn configuration to Cellular Router Open VPN 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.

16.5.7 Install Pritunl Open VPN server on Docker

Pritunl Open VPN server on Docker installation

Pritunl is a distributed enterprise vpn server built using the Open VPN protocol.

Quick Installation

- **Prerequisites**

- Ubuntu 16.04
- curl or wget should be installed

- **Install via curl**

sh -c "$(curl -fsSL https://bit.ly/2IpJN1X)"

- **Install via wget**

sh -c "$(wget https://bit.ly/2IpJN1X -O -)"

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 Open VPN 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

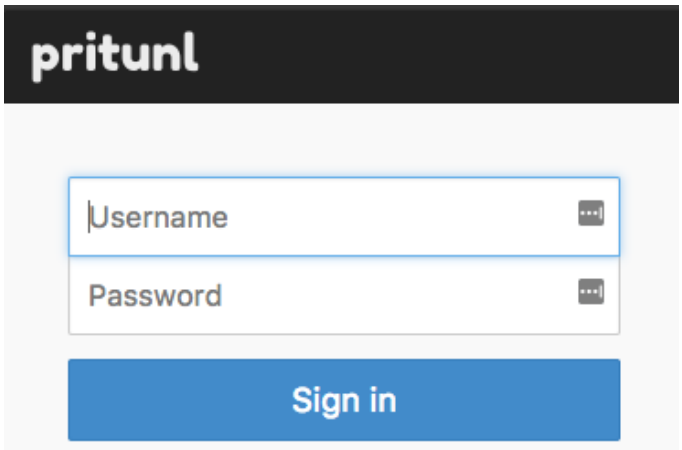
(4) Check the Pritunl Open VPN Server by visiting https://<server_ip_or_domain>

Setup Pritunl Open VPN Server for Cellular Router

The server will running on https://<server_ip_or_domain>.

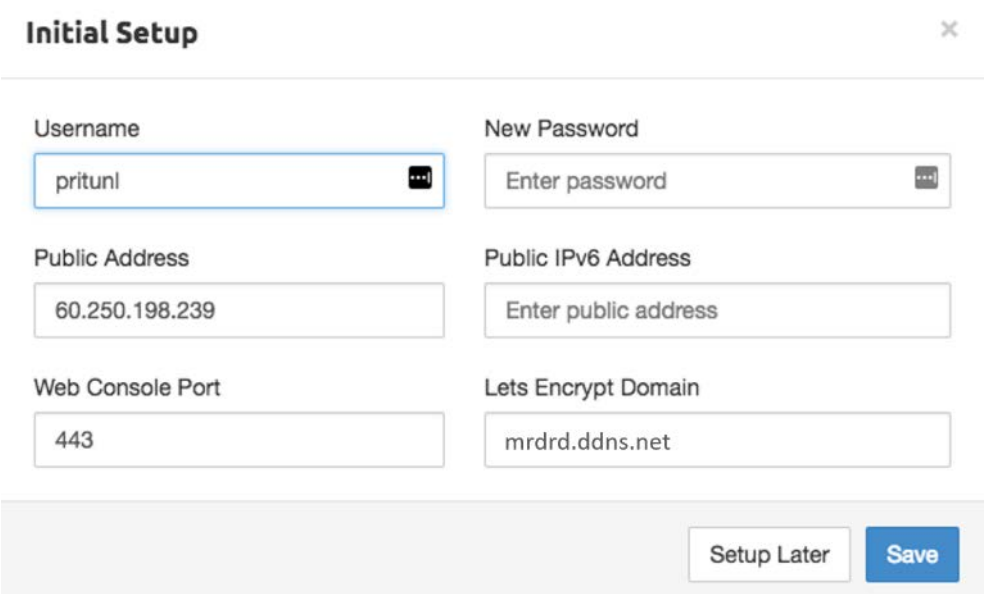
The default username/password is pritunl/pritunl.

Login Page:



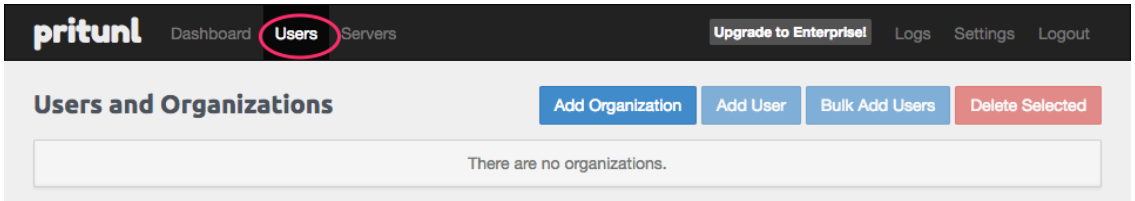
After logged, the server will ask you to do the initial setup. You can change the username and the password setting in this page.

Initial Setup:

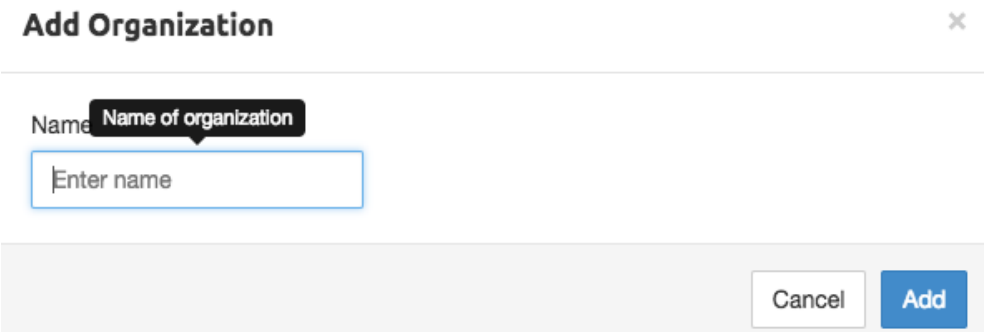


Open VPN user setup

Please navigate to the User page to setup the Open VPN user account.

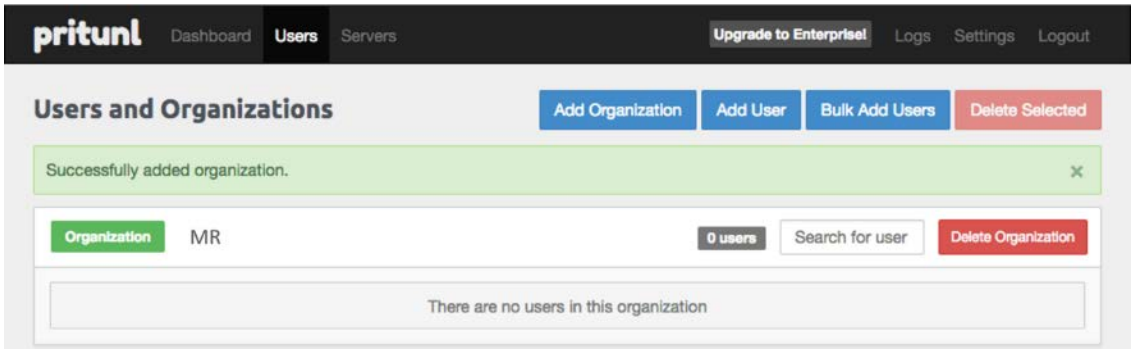


Add the organization by click the Add Organization button.

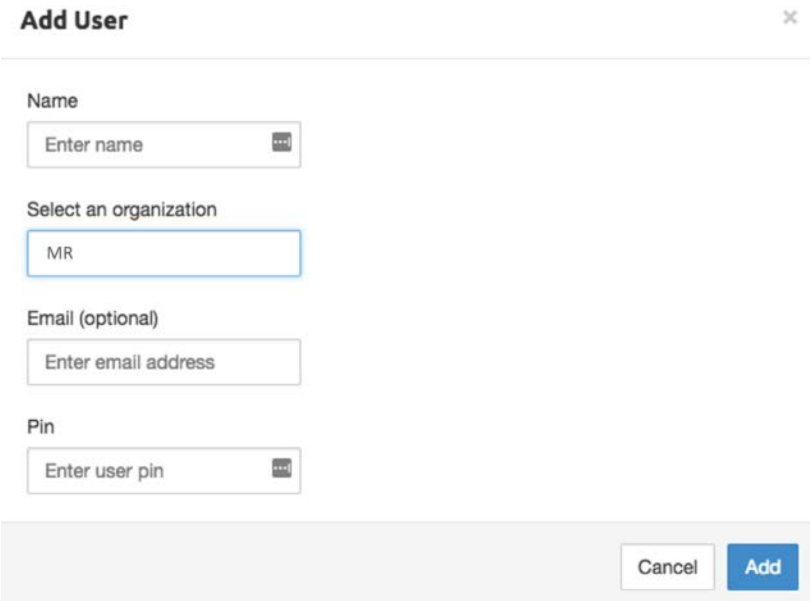


(In this document, we use the MR to be the organization example.)

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

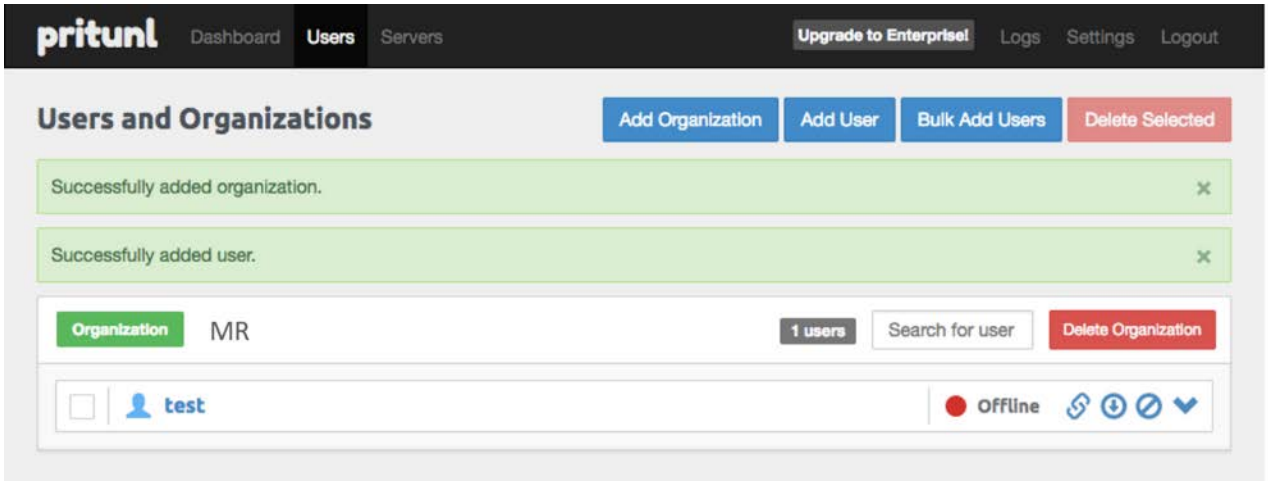


Then add the Open VPN user by click the Add User button.



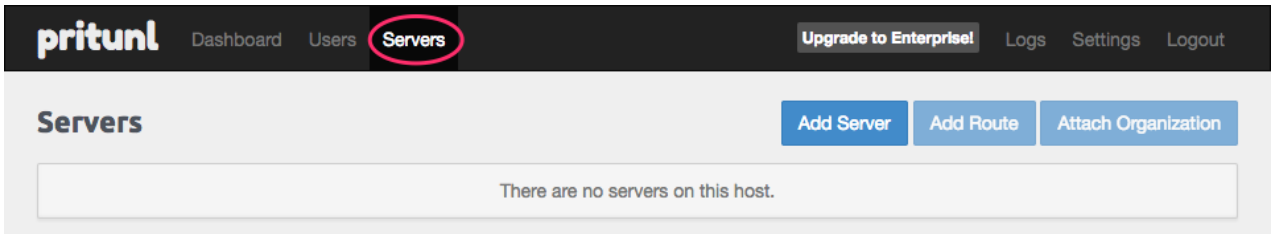
Note: In this Open VPN server, the PIN must contain only digits.

Note: In this document, we use the test/123456 Open VPN user to be the example.

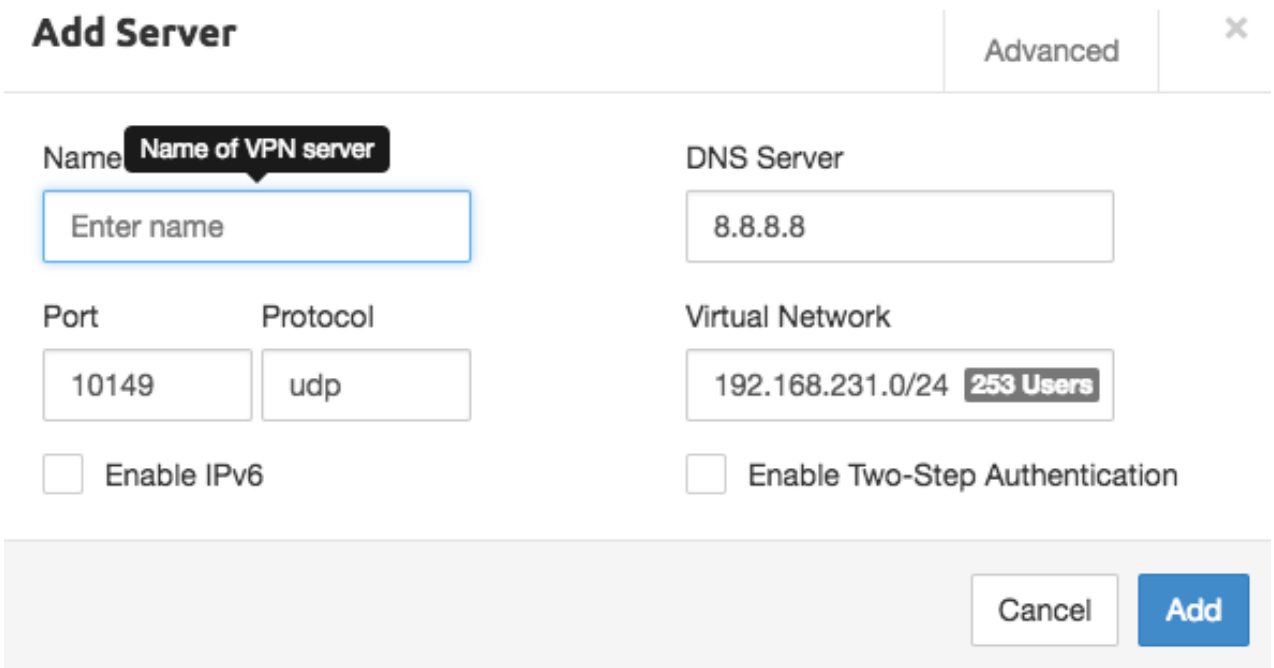


Open VPN server setup

Please navigate to the Server page to setup the Open VPN server.

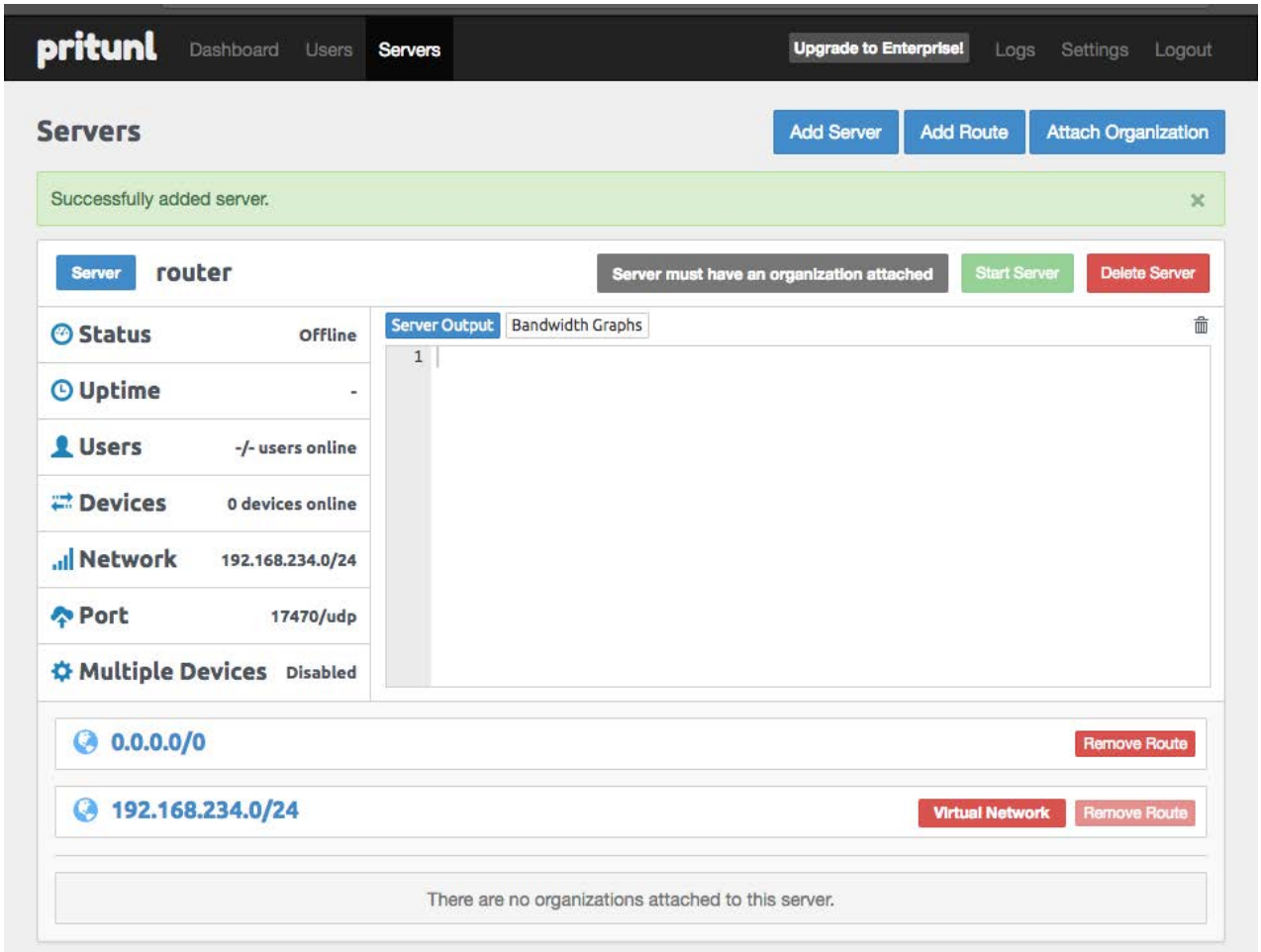


And click the Add Server button to create the Open VPN server.

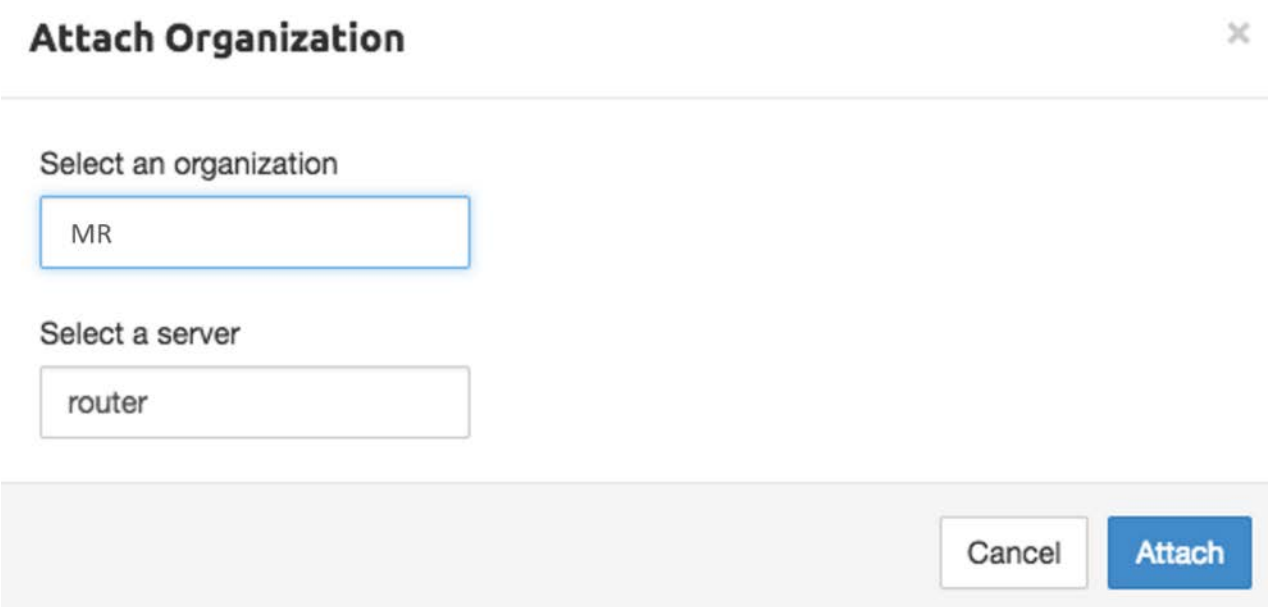


Note: Please click the Advanced tab and make sure the Inter-Client Communication be checked

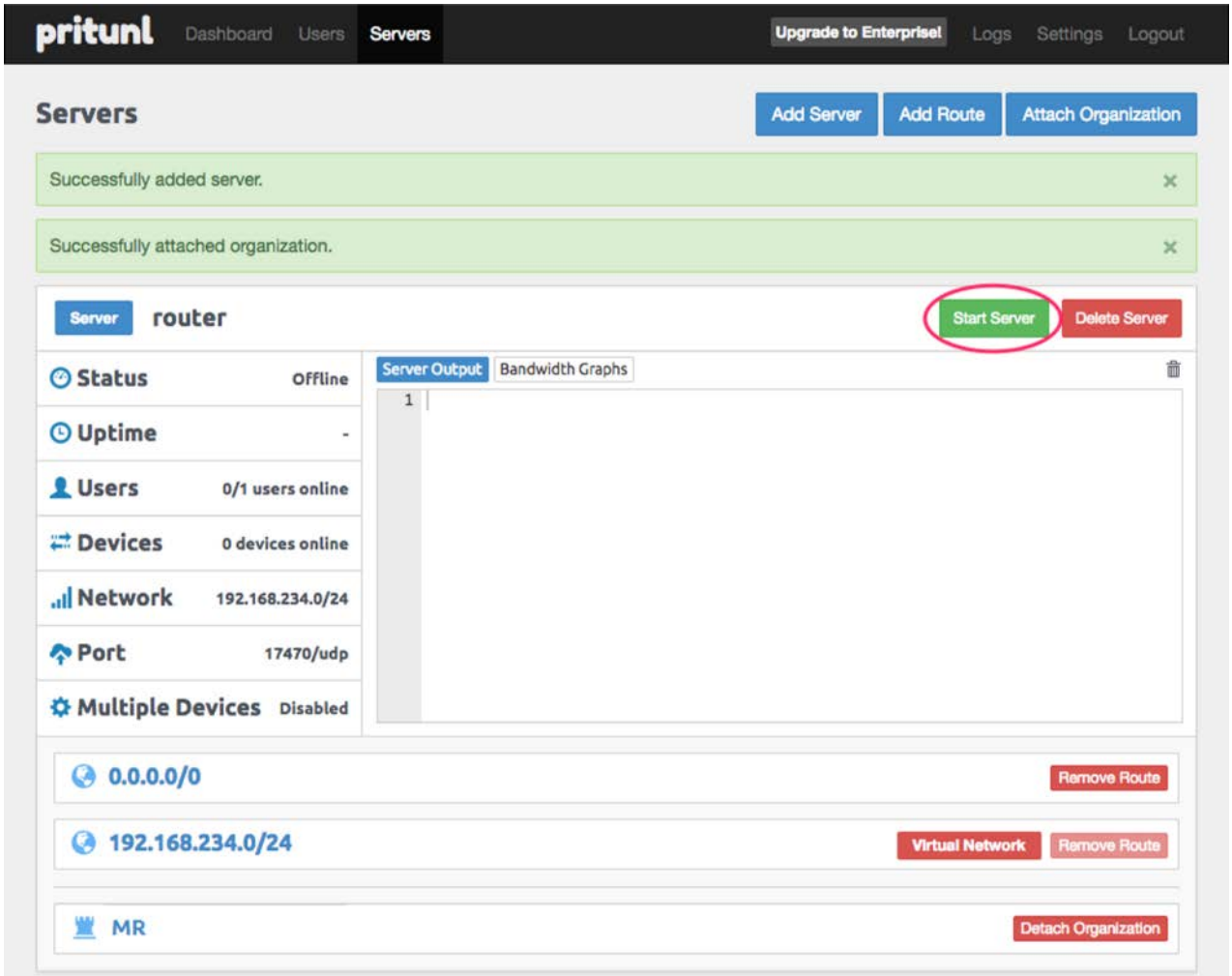
When the Open VPN server created, the Servers page should like the following figure.



And click Attach Organization button to setup the Open VPN server.

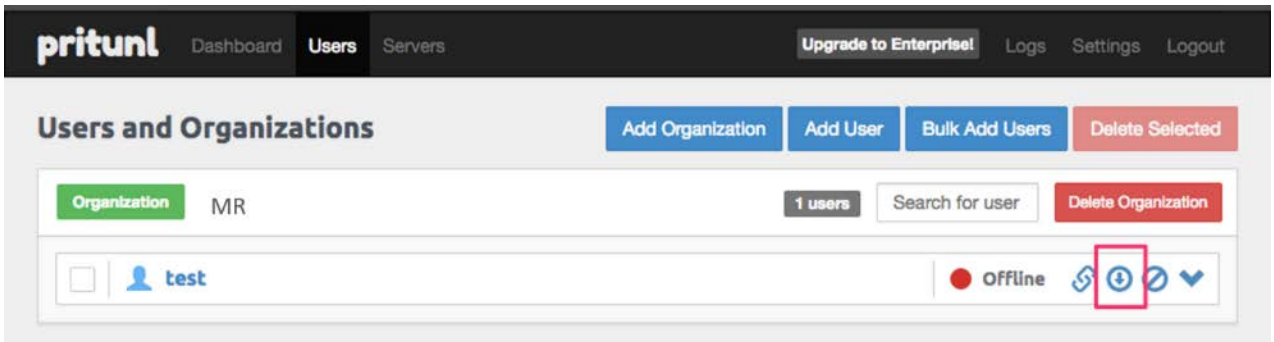


Start the Open VPN server by click Start Server button.



Cellular Router setup

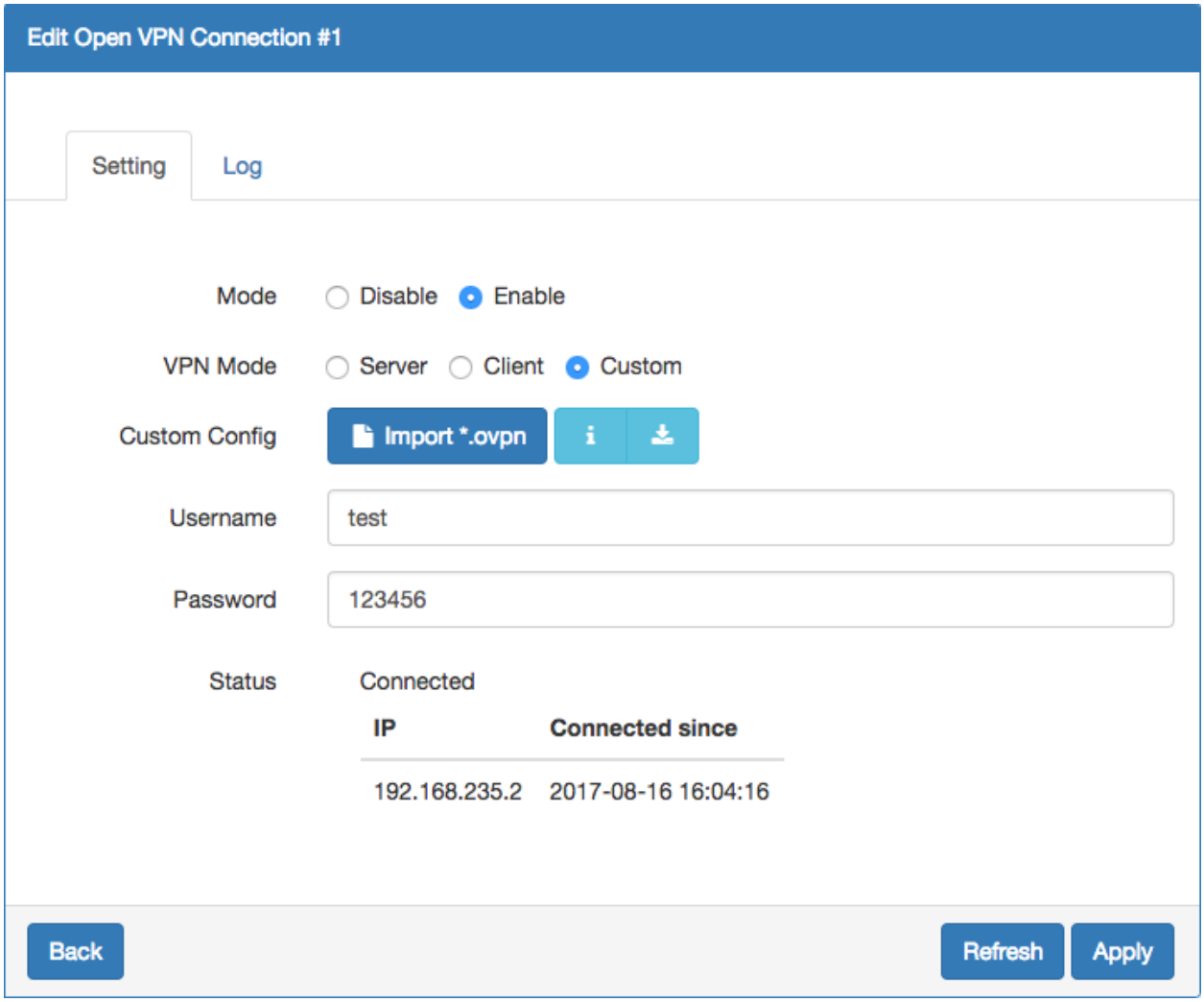
First, please navigate to the Users page and download the user configuration file and extract it.



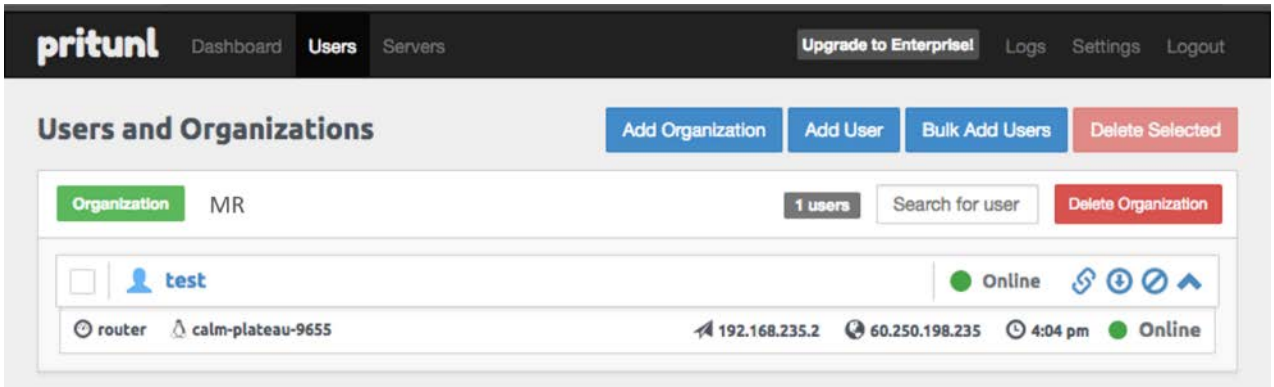
Note: In this document, you should get the MR_test_router.ovpn file.

And visit the Cellular Router Open VPN custom page then import the .ovpn file.

Fill up the username/password which be setup in Open VPN user setup part.

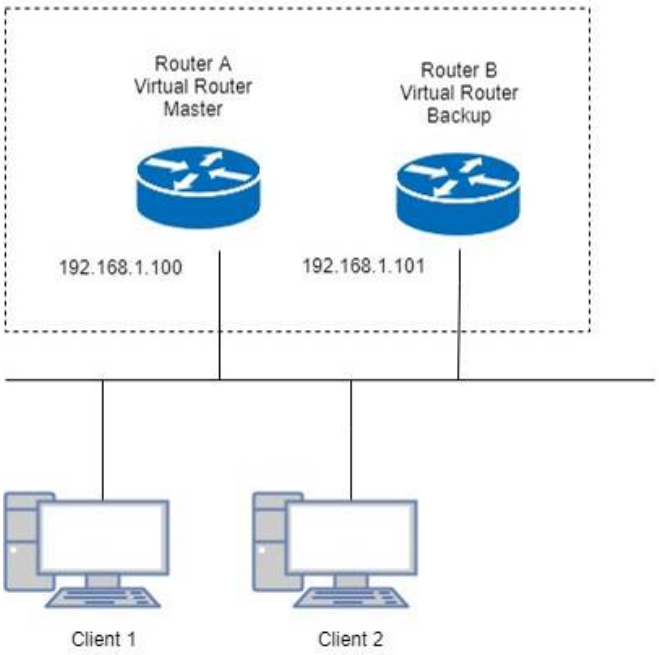


When the Cellular Router Open VPN connected, the Pritunl Open VPN server also update the user status.



16.6 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.

16.7 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

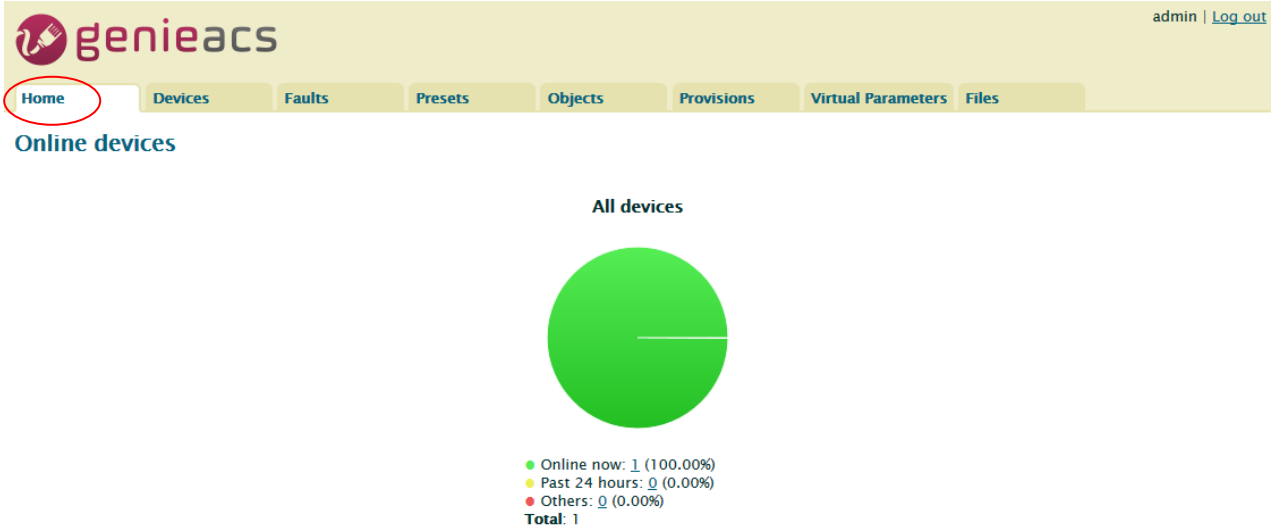
Fill in the ACS URL field as http://GenieACS server IP:7547

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

2) GenieACS Operation

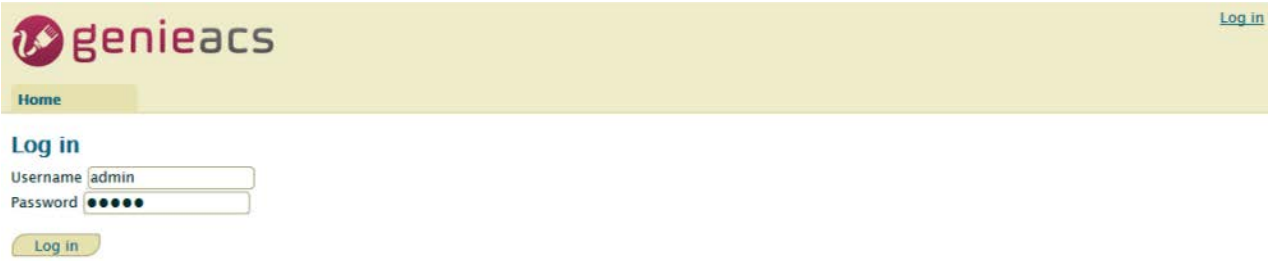
Input http://GenieACS server IP:3000 on browser url bar and Enter.

Press Home tab to refresh Online devices status.



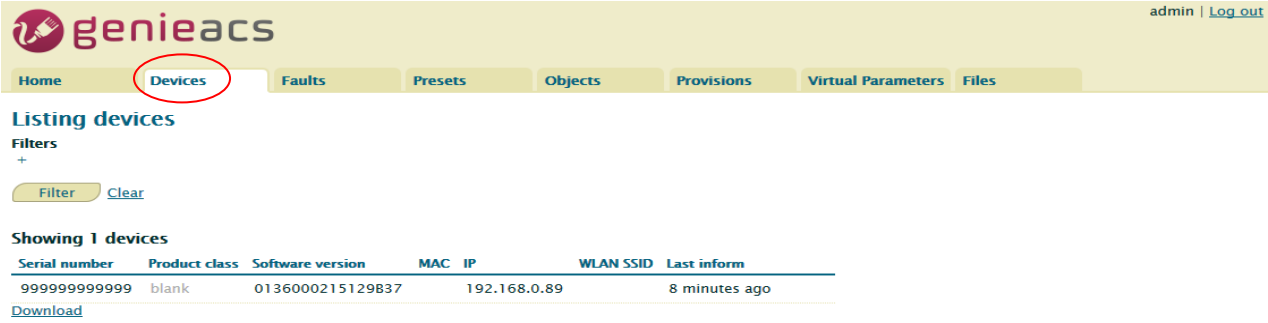
2.1) Login

Username and Password are admin/admin.

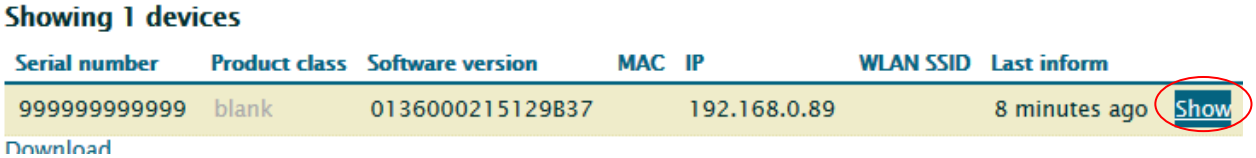


3) Device information

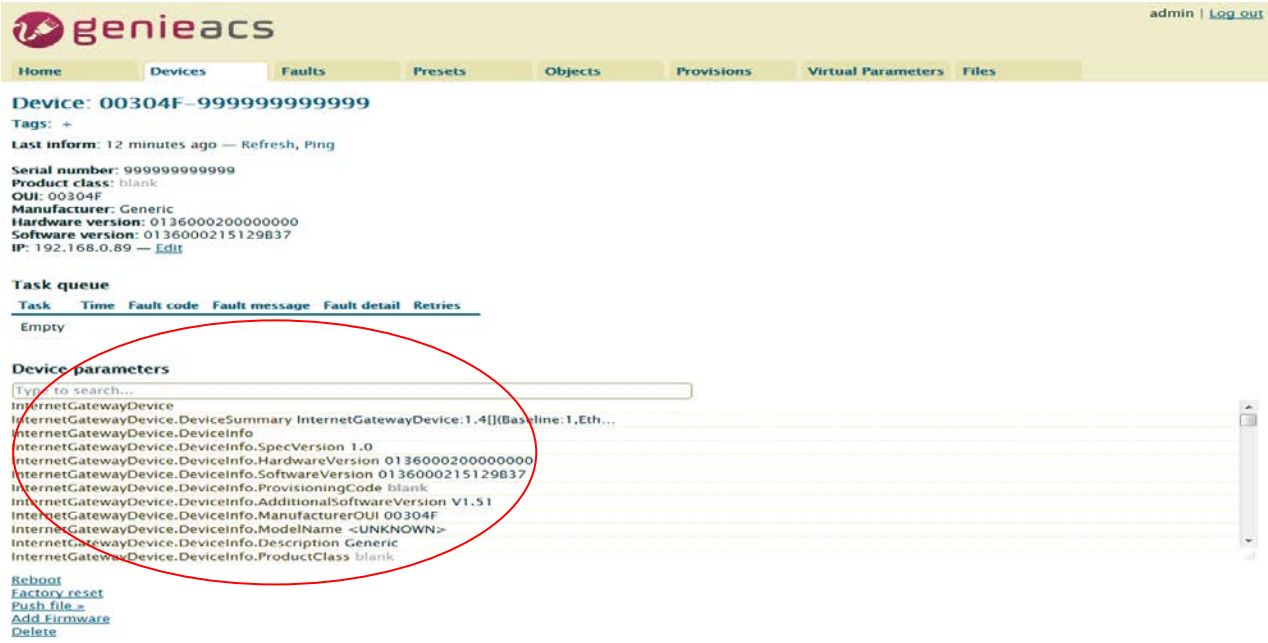
Press Devices tab



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



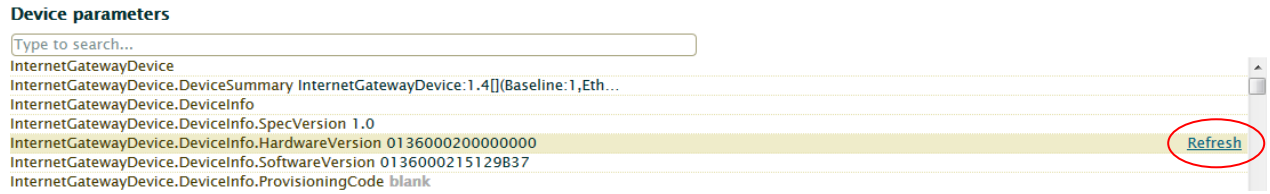
Press Show link, the device information shows up.



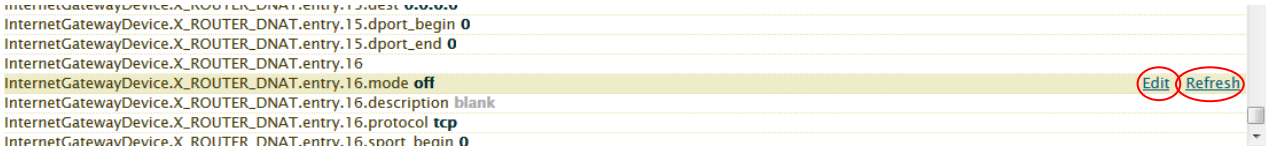
4) Access parameters

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

For Readable parameter

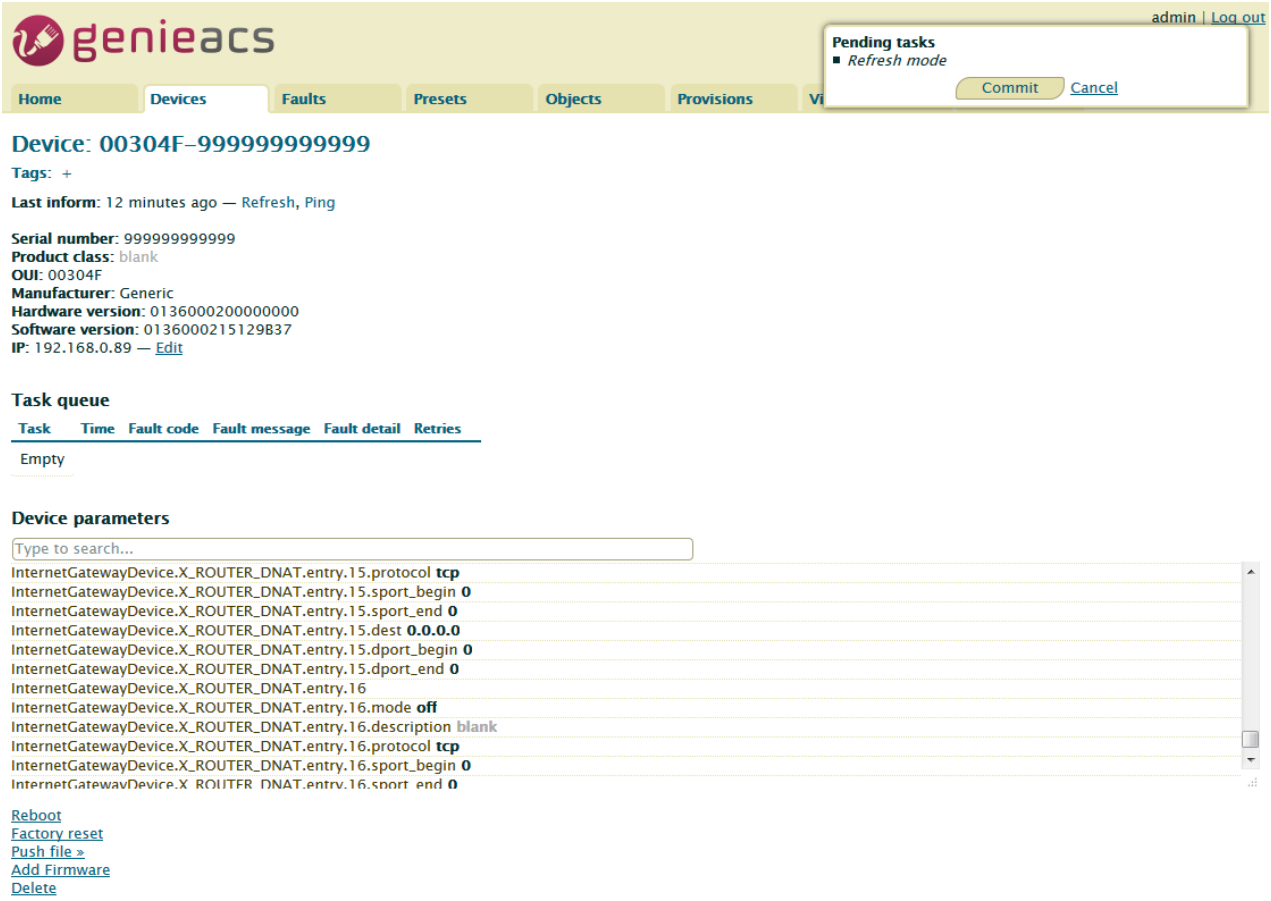


For Readable and Writable parameter



4.1) Get parameter value

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



Press Commit to get this parameter value.

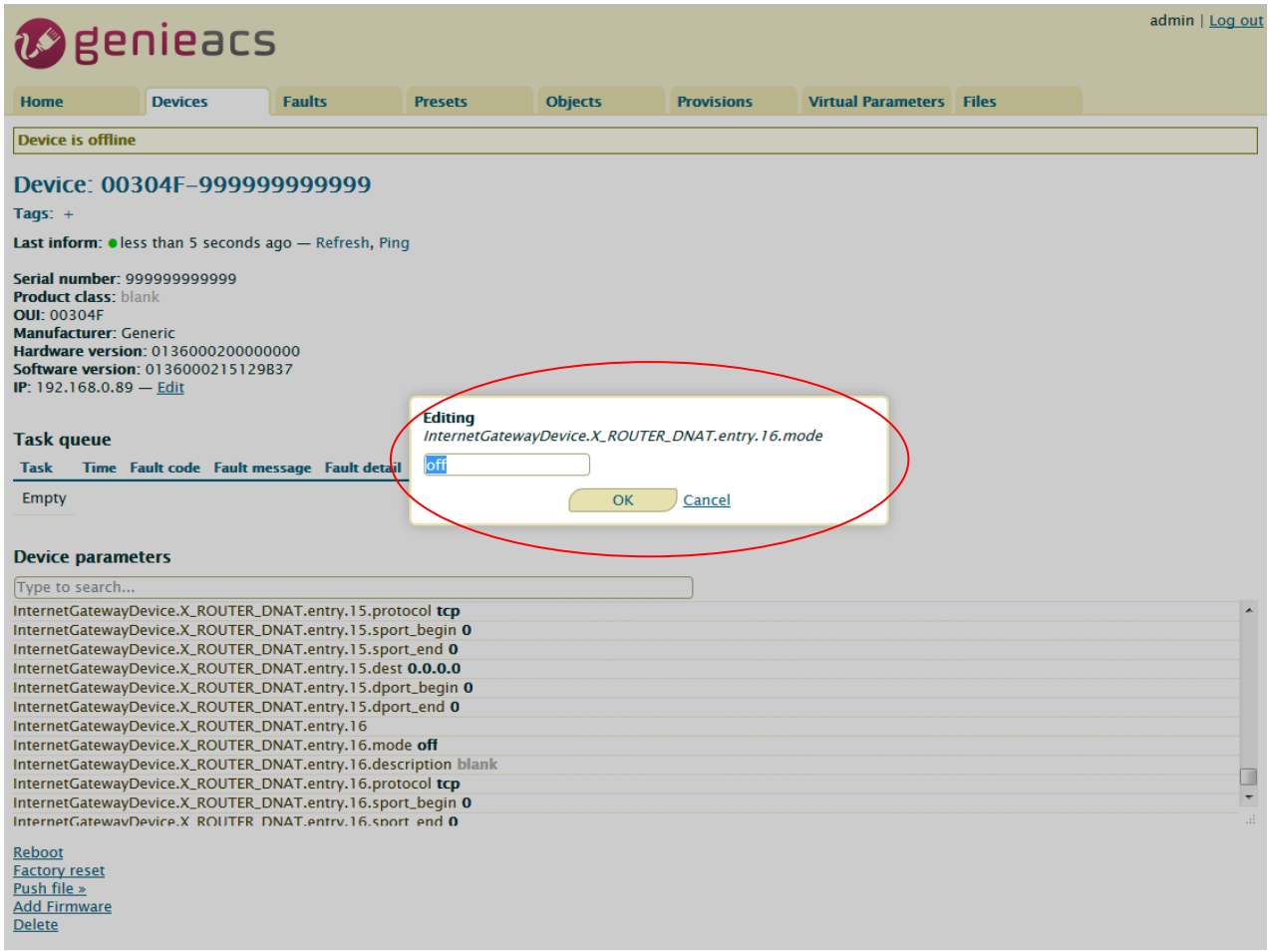
Note: *If the GenieACS can reach the device, the parameter value will be updated immediately. Otherwise, this request will be queued on Task queue list until next time device connect to*

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

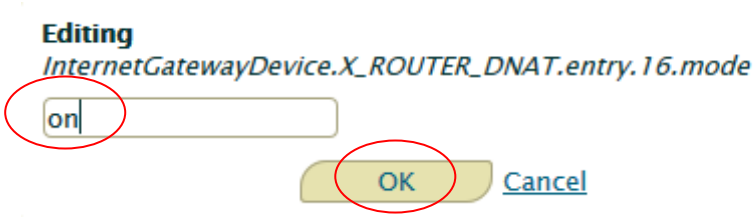
Note: To update partial tree, refresh the parent node of the partial tree.

4.2) Set parameter value

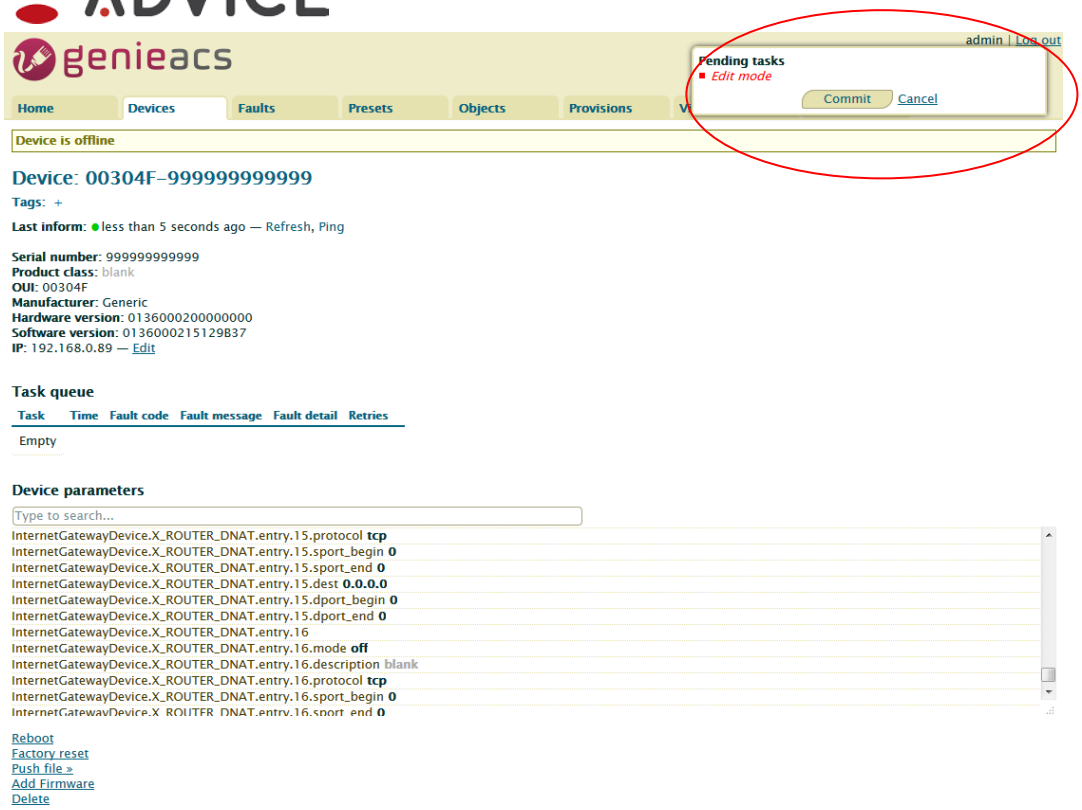
Press on the Edit link, editing window will pop up to ask you to change the value of this parameter.



Input new value and press OK.



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

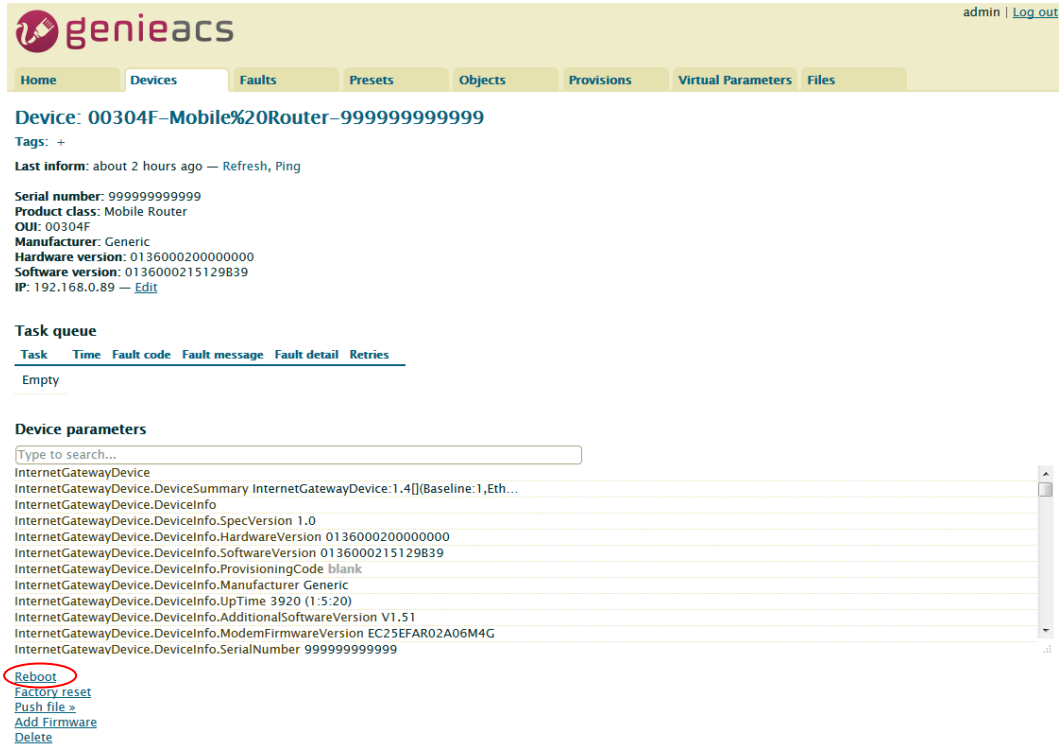


Press Commit to set this parameter value.

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 pop up 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.*

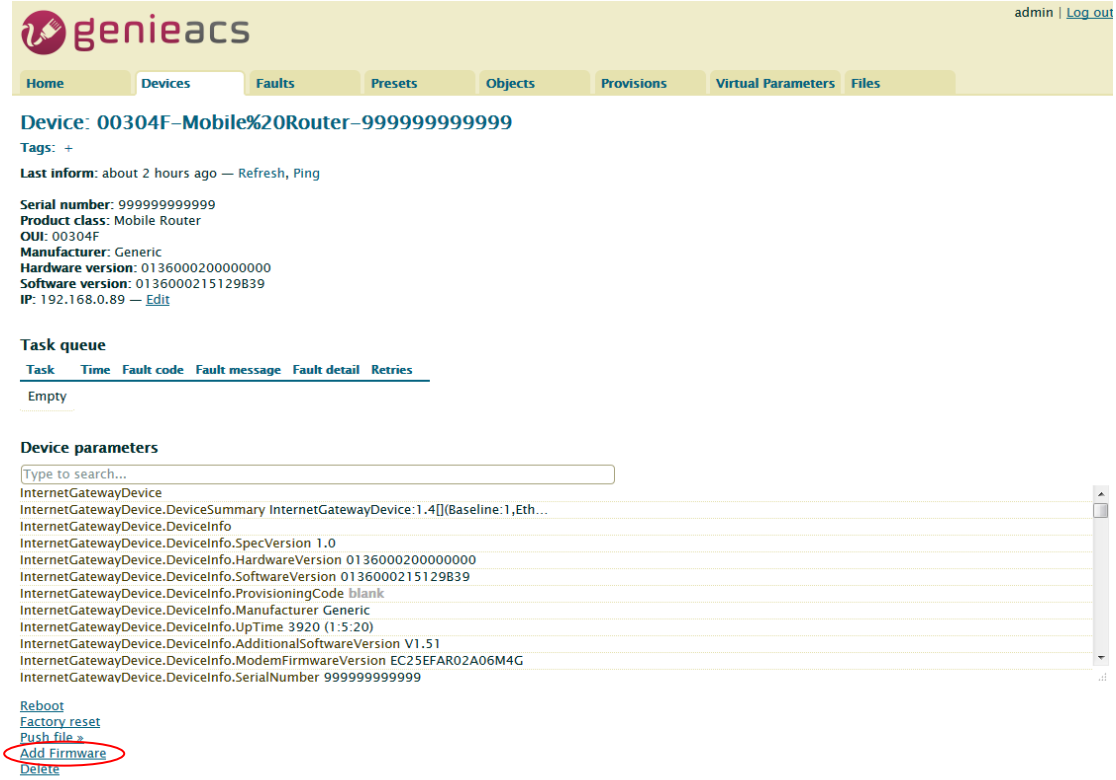
6) Reset to default

Similar to Reboot device except pressing on Factory reset link.

7) Firmware Upgrade

7.1) Upload Firmware

Press Add Firmware link



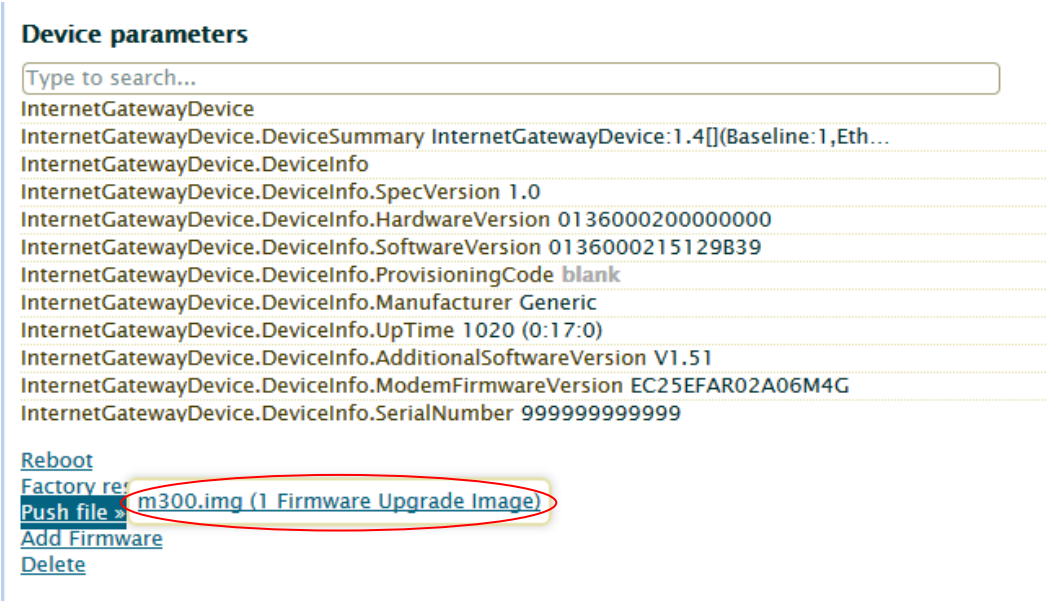
The link will redirect to Files tab

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.*

17 Test Case Example

17.1 VLAN Topology

This VLAN Topology for **2-port LANs** shows different PCs how to configure VLAN settings with different LAN ports and has two results for this configuration.

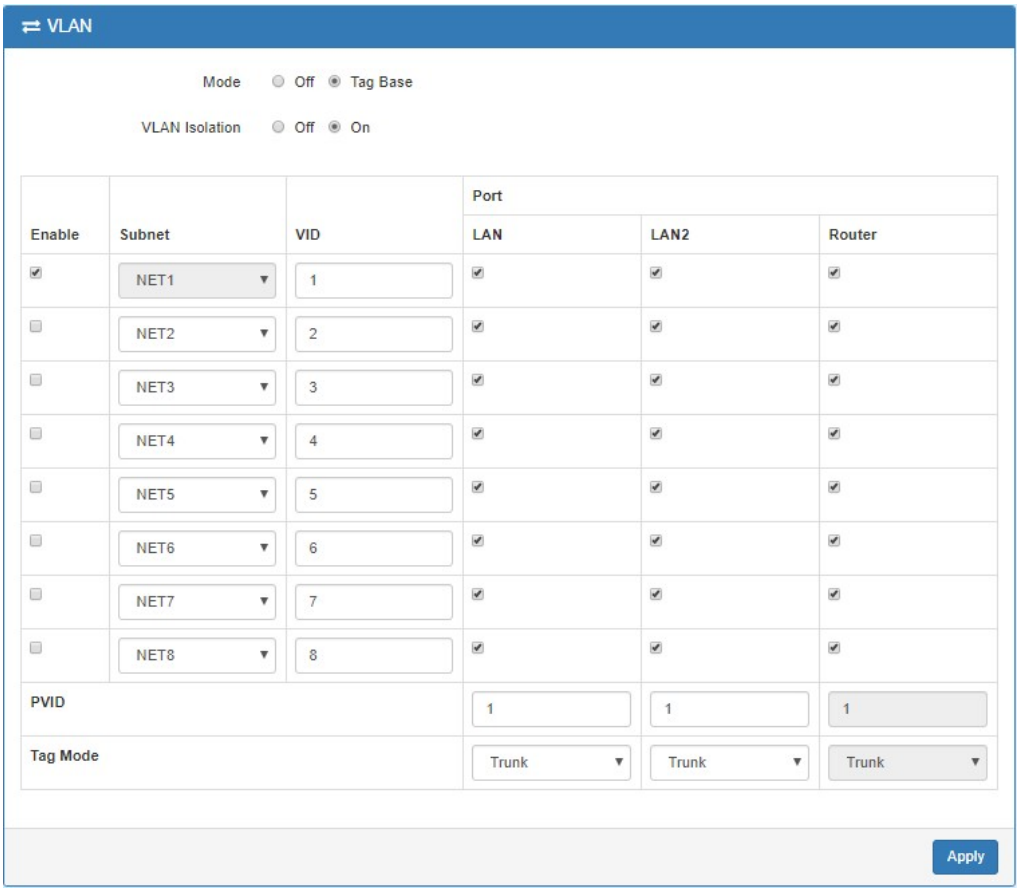
(1) PC-A sends ICMP packet to PC-B IP (192.168.2.20) and captures traffic on PC-B. Thus, PC-B will receive Tag20 traffic.

(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.

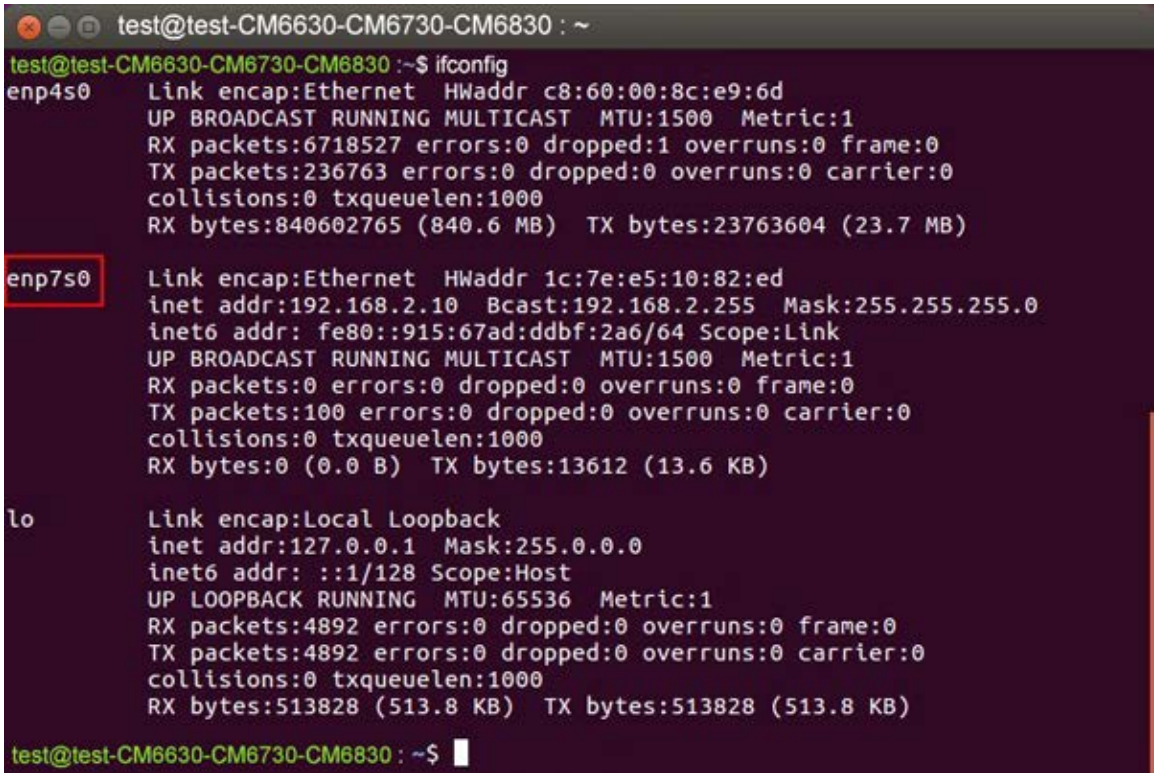


Note:

- 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.

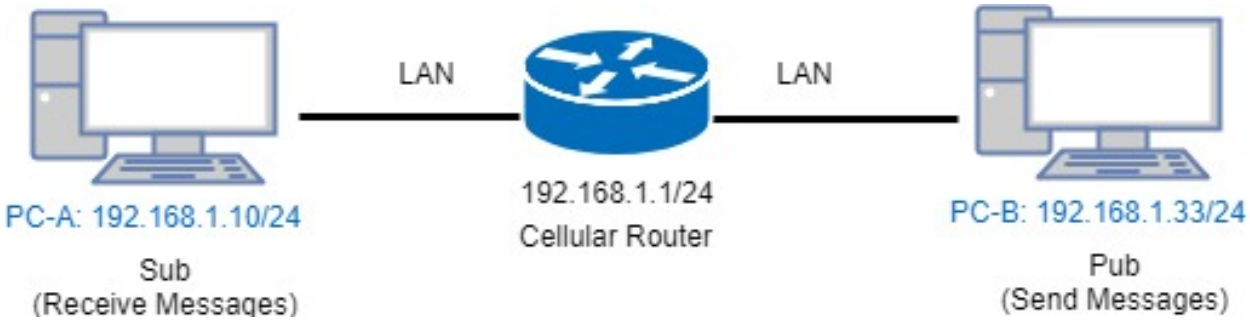
Example 2: PC-A ping PC-B (Trunk to Access)

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.

17.2 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.

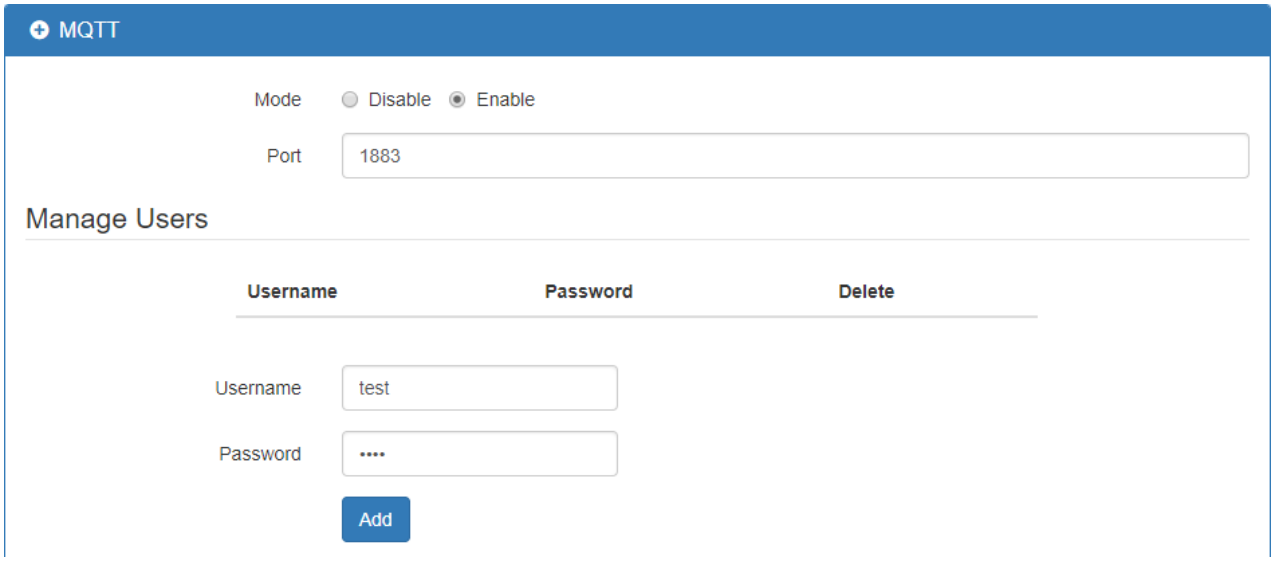
If your OS system is Ubuntu, you should install as below steps:

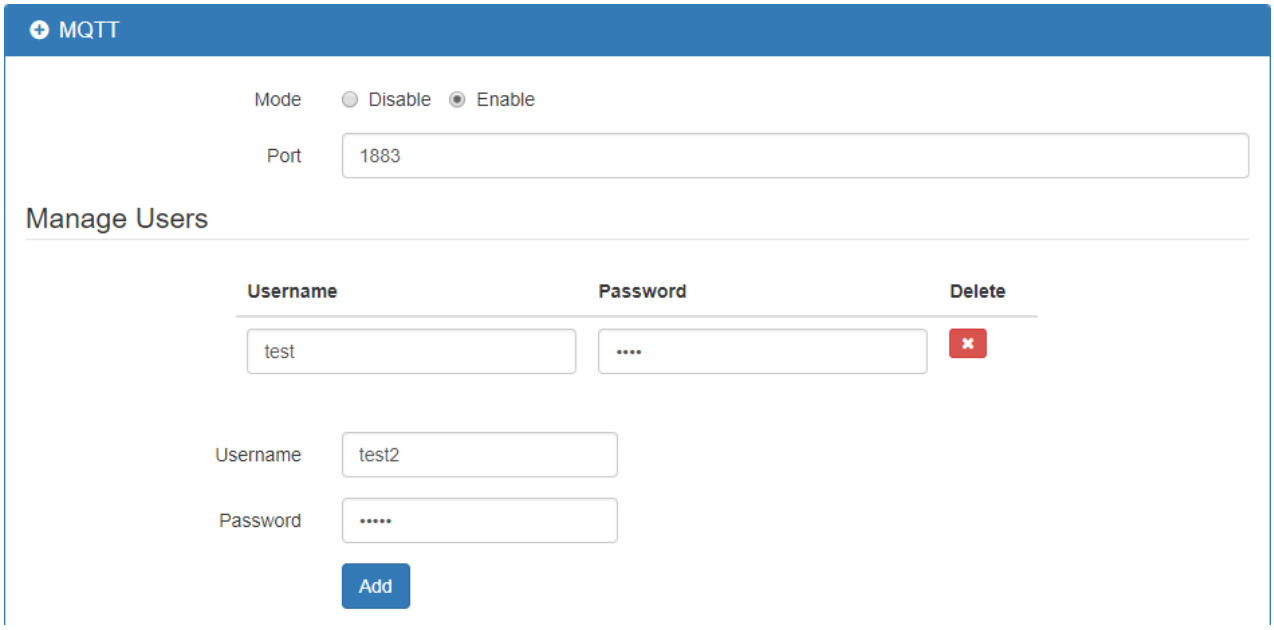
```
test@test: ~
test@test:~$ sudo apt-get install mosquitto-clients
sudo: unable to resolve host test
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  geoip-database-extra javascript-common 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
```

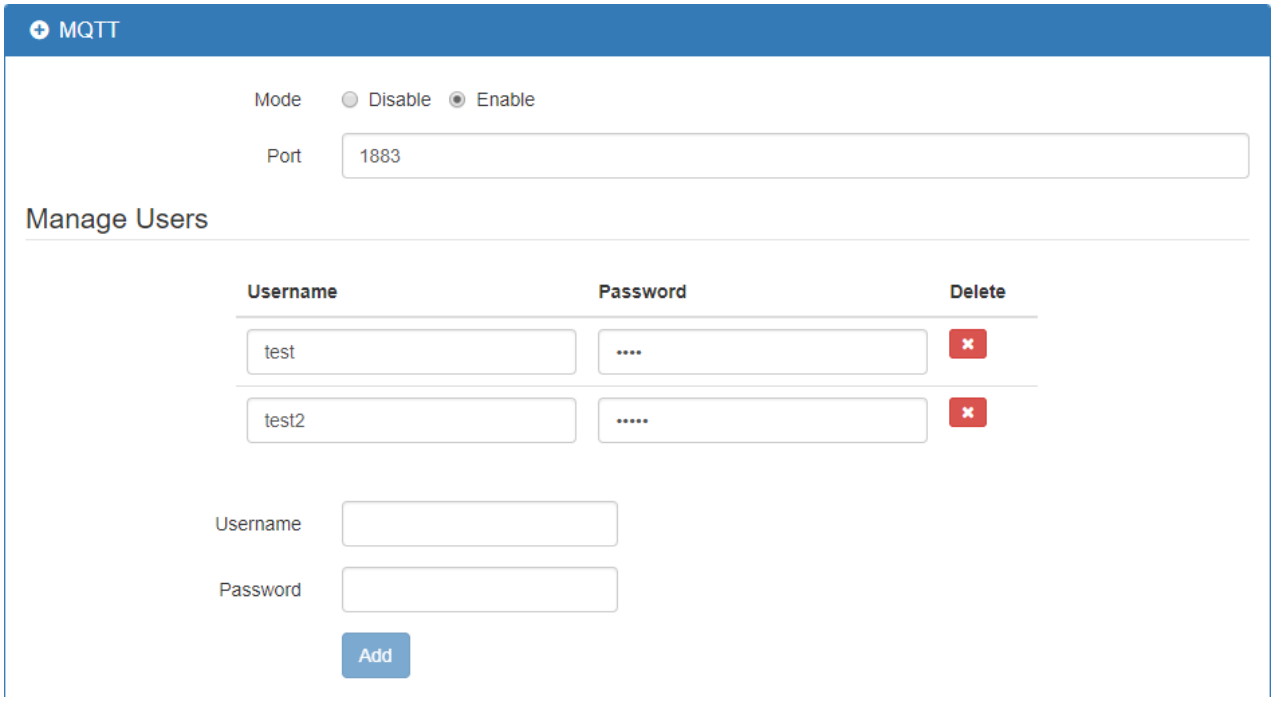
```
test@test: ~
After this operation, 330 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://tw.archive.ubuntu.com/ubuntu xenial-updates/main amd64 libc-ares2 amd
64 1.10.0-3ubuntu0.2 [34.1 kB]
Get:2 http://tw.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 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

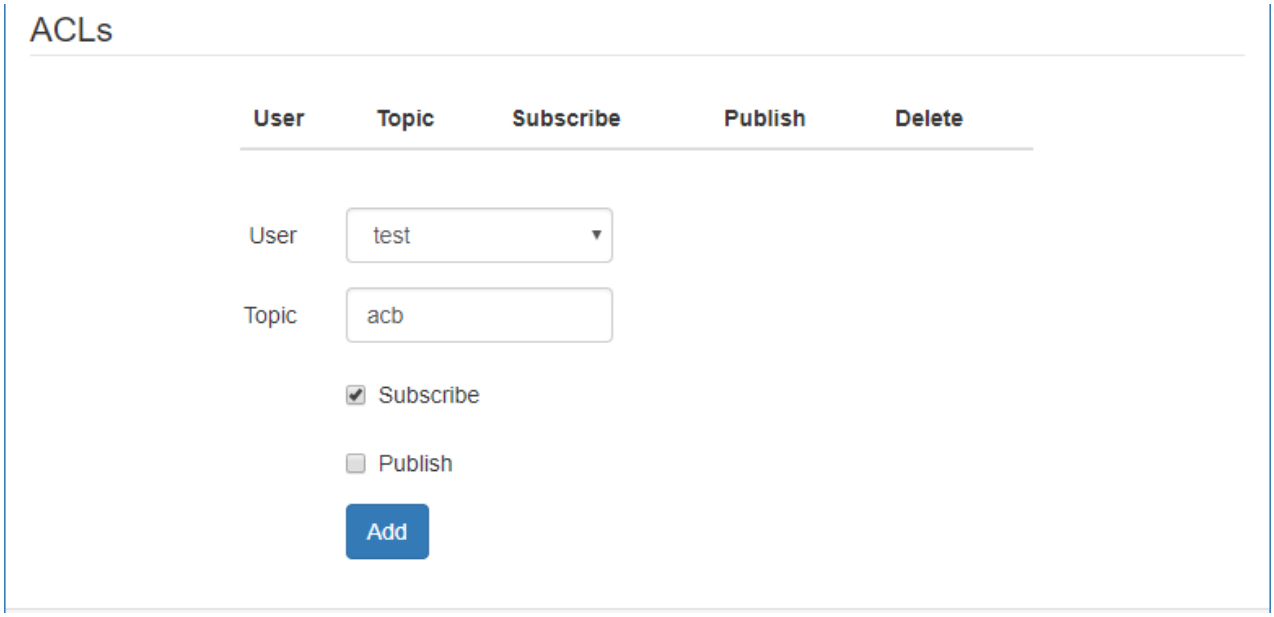
You need to add two users. For example, we create the users for test and test2.

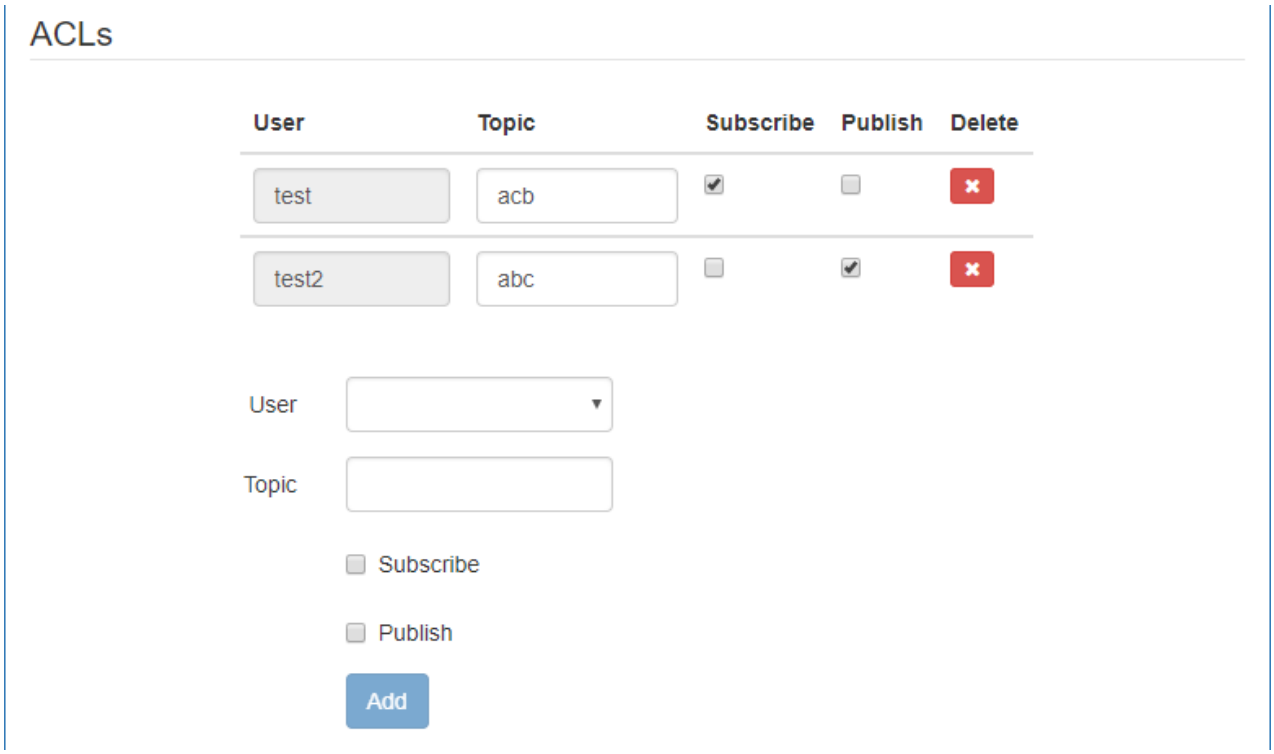






You need to add two ACLs based on the users you created. For instance, we create two ACLs for test user and test2 user.





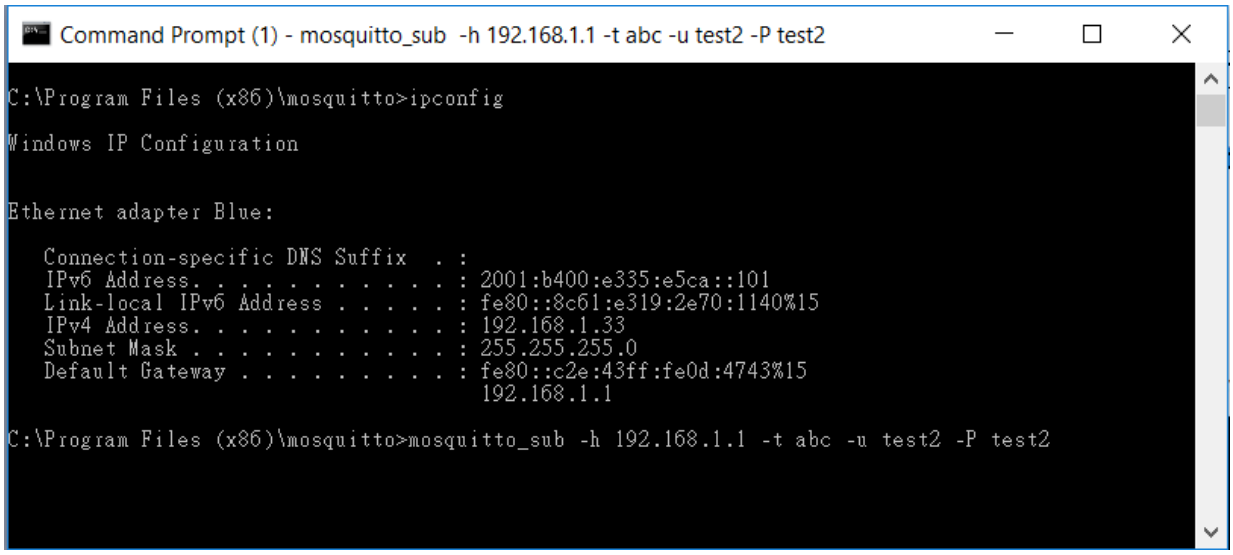
Note:

- For Receive message command format:
  Mosquitto_sub -h <M300 IP> -t <Topic> -u <username> -P <password>
- For Send message command format:
  Mosquitto_pub -h <M300 IP> -t <Topic> -u <username> -P <password> -m <message>

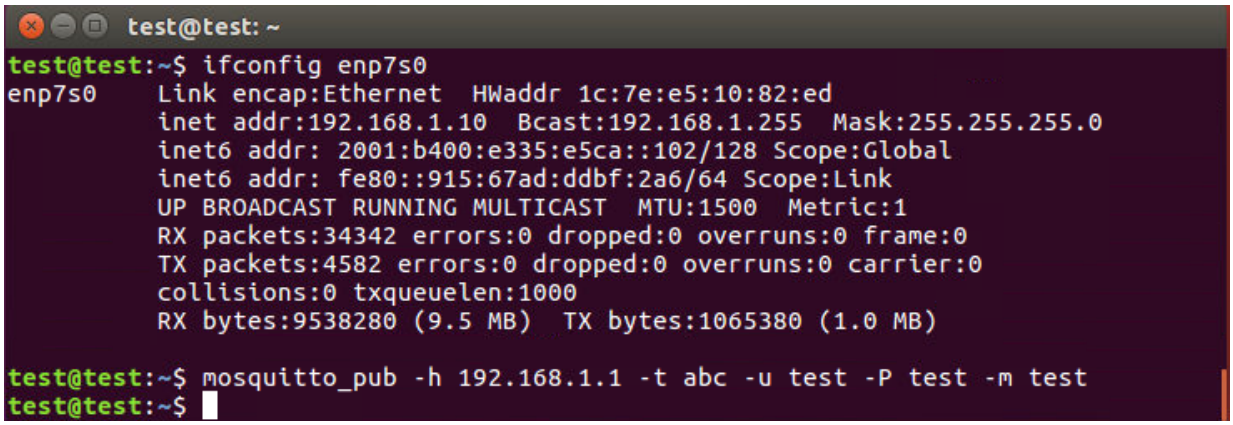
- Step3: There are two test MQTT examples.

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".



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.



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"

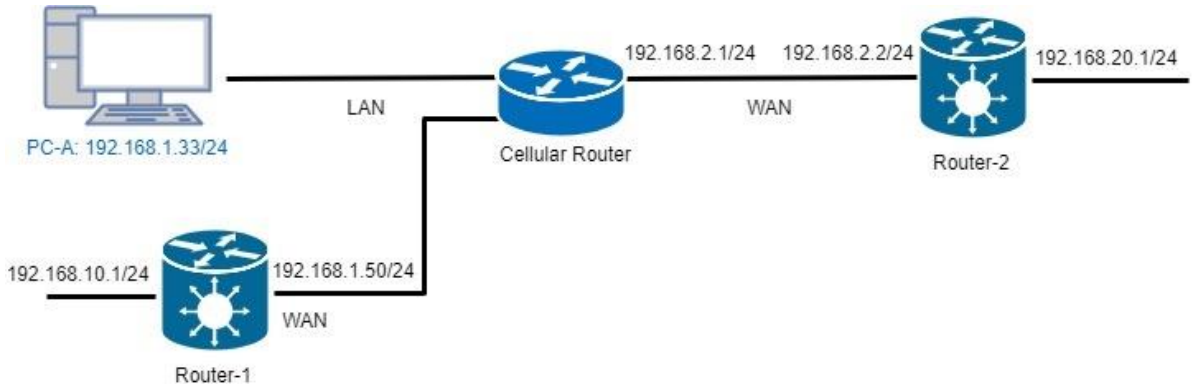
```
test@test: ~
test@test:~$ ifconfig enp7s0
enp7s0    Link encap:Ethernet  HWaddr 1c:7e:e5:10:82:ed
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b400:e335:e5ca::102/128 Scope:Global
          inet6 addr: fe80::915:67ad:ddbf:2a6/64 Scope:Link
          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
```

17.3 IP Routing Topology



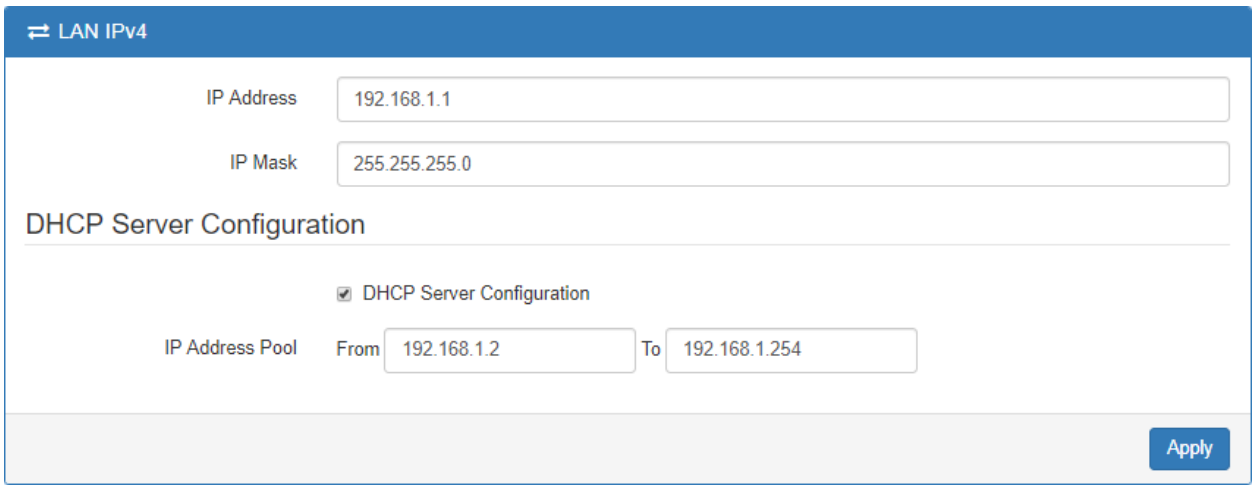
This IP Routing topology that the cellular router connects Router-1 and Router-2 will have two results.

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

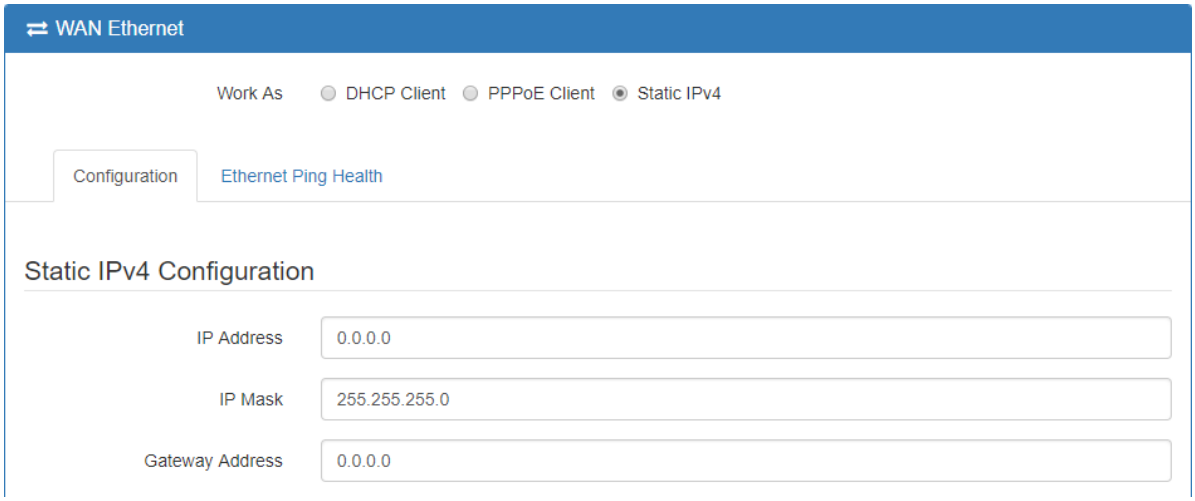
(2) PC-A sends ICMP packet to Router-2 LAN and WAN IP and they should have response.

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

- LAN configuration:



- WAN configuration:

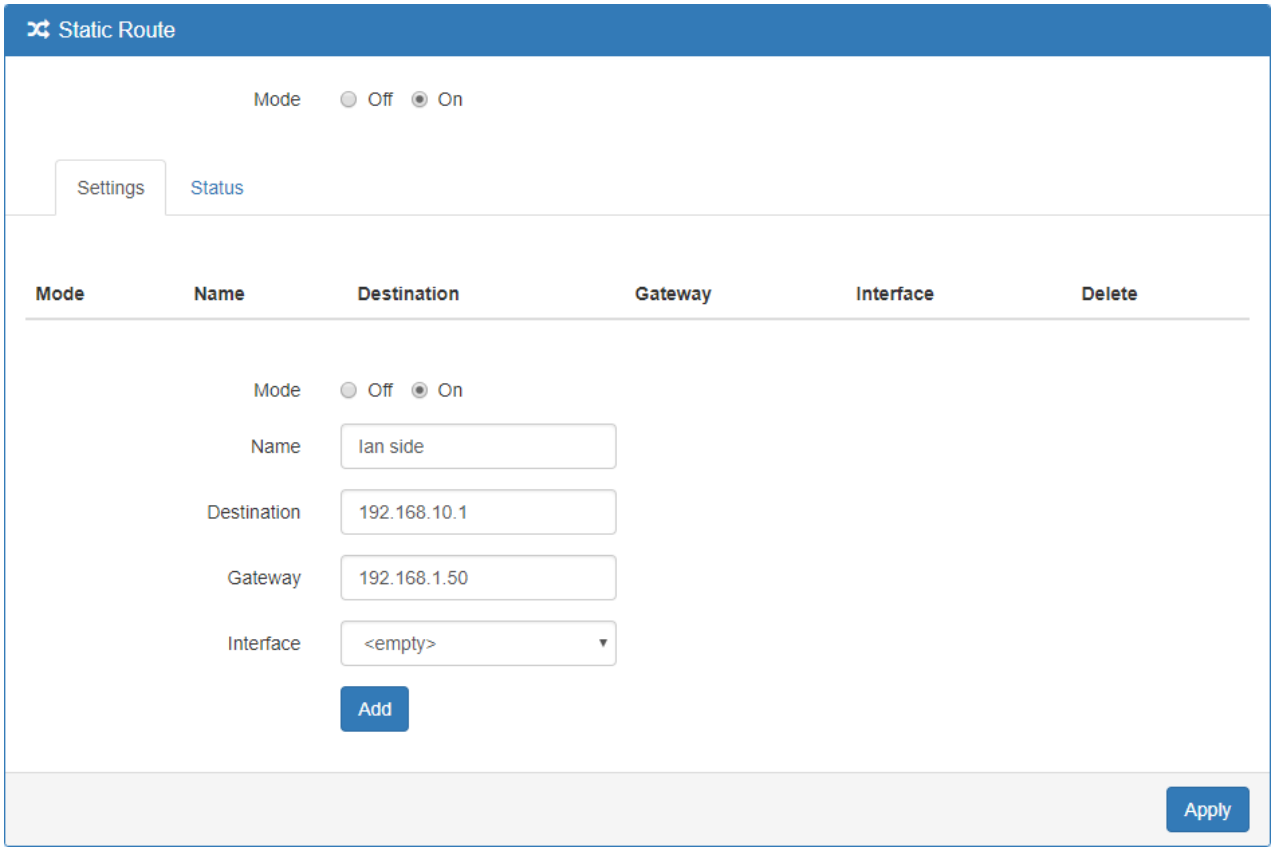


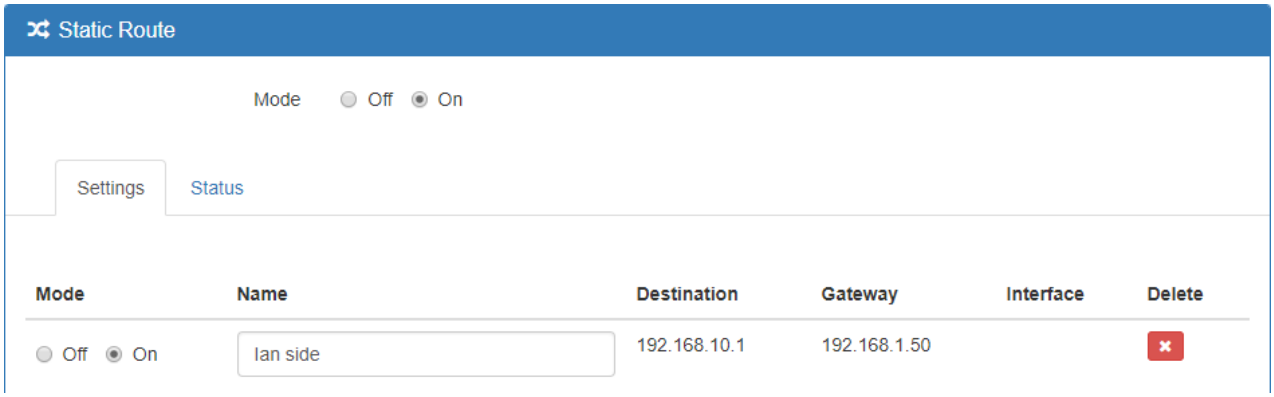
There are two examples to introduce how to work for routing.

Example 1: Add IP Routing on LAN interface

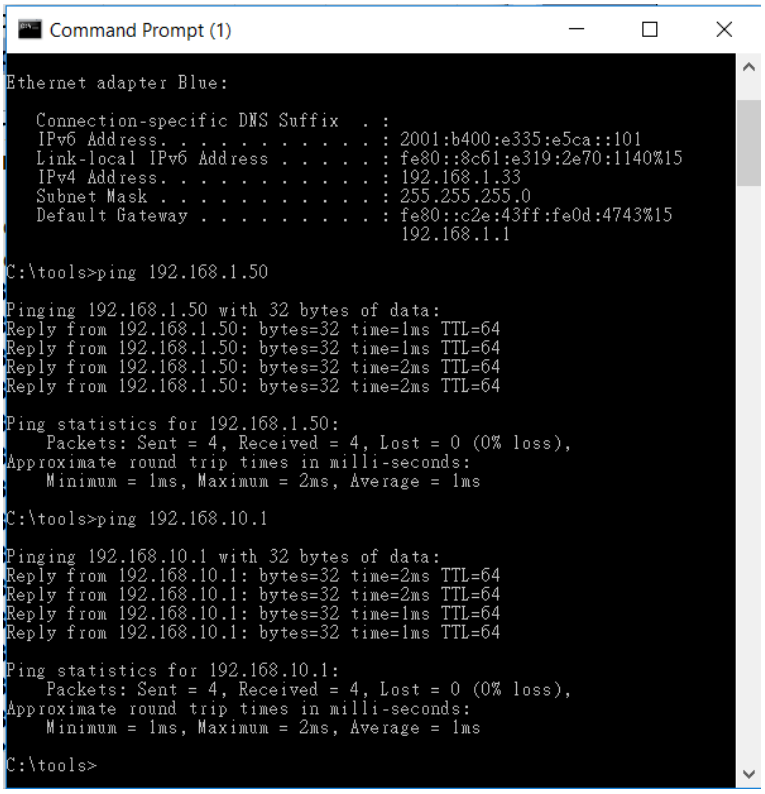
- Step 1: The cellular router for Static Route configuration
  The Mode is on at the settings section and add the routing.
- Step 2: Router-1 configuration is as below.

(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.



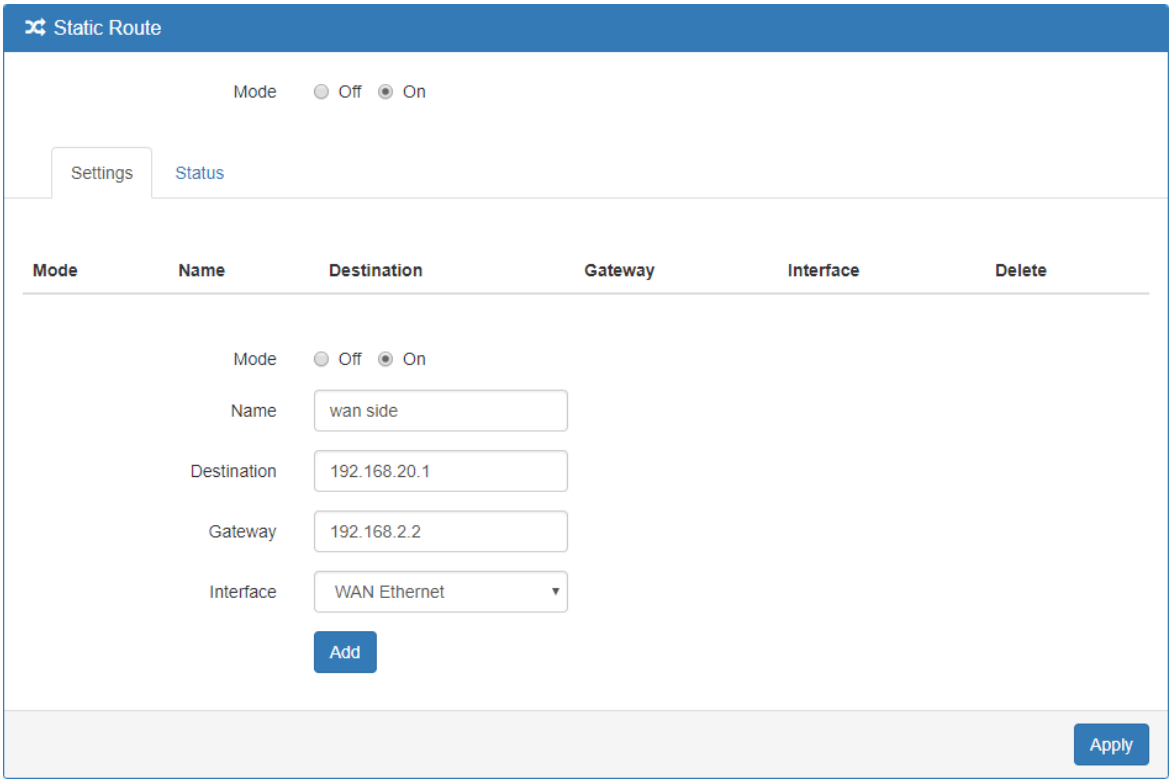
Example 2: Add IP Routing on WAN interface

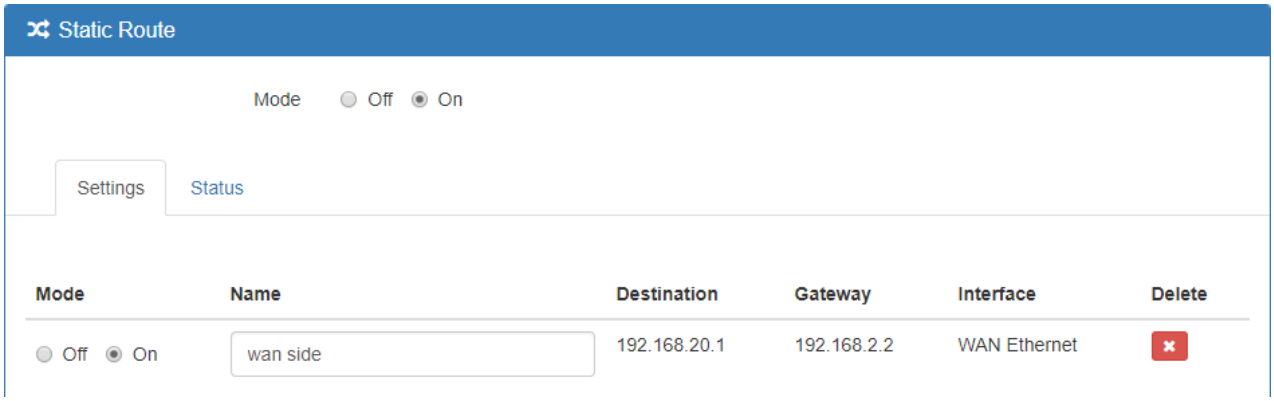
- Step1: The cellular router for Static Route configuration
  The Mode is on at the settings section and add the routing.
- Step2: Router-2 configuration is as below.

(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.