Industrial 4G LTE Cellular Router

M300 / M301
M300-G / M301-G / M301-TG
M301-TPG / M301-GW

User Manual

Version 1.1.8

Table of Contents

1 Introduction

Industrial 4G LTE Cellular Router series are highly reliable and secure wireless communications gateway designed for enabling mission-critical applications and enhancing machine-to-machine connectivity for Industrial Internet of Things (IIoT).

1.1 Features

- Highly reliable and secure for mission-critical cellular communications
- Provide flexible options to configure LAN/ WAN ports
- Support multi-band connectivity with FDD LTE/ TDD LTE/ WCDMA/ GSM/ LTE Cat 4
- Provide IEEE 802.11 b/g/n Wi-Fi standards (M301-GW)
- Built-in dual SIM for network redundancy
- Equipped with DI/DO and RS-232/RS-485 serial ports
- Integrated dual detachable antenna against radio interference
- LED indicators for connection and data transmission status
- A flexible input voltage range of 10-32V DC
- Industrial rated from -40°C to +75°C for use in harsh environments (M301-TG/M301-TPG)
- Metal Housing with IP40 industrial grade protection
- IPv6/IPv4 dual stack and all applications are IPv6 ready
- Support various serial communication protocols for connectivity
- Enhance security and encryption for authentication and transmission

1.2 Specifications

Cellular Interface

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

Wi-Fi Interface (M301-GW)

- Compliant with IEEE 802.11 b/g/n Wi-Fi standards
- 2.4 GHz - 2.484 GHz radio band for wireless
- 1T1R 150 Mbps wireless operation rate
- Wireless security with WPA-PSK, WPA2-PSK support
- Multiple SSIDs
- Wireless MAC Filtering
- Wireless client isolation

Processor & I/O Interface

- High performance 528 MHz CPU with 512 Mbytes of DDR3 memory
- 2 x SIM Card Slots
- 1 x LAN 10/100 Mbps Ethernet port (M300/M300-G)
- 3 x LAN 10/100 Mbps Ethernet ports (M301/M301-G/M301-TG/M301-TPG/M301-GW)
- 1 x WAN 10/100 Mbps Ethernet port
- 1 x WAN 10/100 Mbps Ethernet port with IEEE 802.3at/af PoE PD (M301-TPG)
- Reset Button
- Console: 1 x RS232 (9-pin Sub-D)
- 2 x SMA connectors for detachable LTE antenna
- 1 x GPS detachable antenna (M300-G/M301-G/M301-TG/M301-TPG/M301-GW)
- 1 x RP-SMA for Wi-Fi antenna (M301-GW)
- 1 x RS485 (D+/D-)
- 1 x RS232 (TXD/RXD)
- 2 x DI, 1 x DO (Alarm +/-)

Physical Characteristics

- Enclosure：Aluminum Case
- Housing：IP40 Protection
- Weight：
  - 451 g (M300/M300-G)
  - 452 g (M301/M301-G/M301-TG/M301-TPG/M301-GW)
- Dimensions (W x H x D)：60 x 110 x 106 mm
- Installation：DIN Rail (Default) or Wall Mount (Optional)

LED Display

- 1 x System status LED (Green)
- 1 x VPN status LED (Green) (M300/M301/M300-G/M301-G/M301-TG/M301-TPG)
- 1 x FN status LED (Green) (M301-GW)
- 1 x SIM1 status LED (Green)
- 1 x SIM2 status LED (Green)
- Ethernet status LEDs
  (Green for LINK/ACT, Yellow for SPEED)
- 2 x Mobile connection strength LEDs (Green)

Power Supply

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

MTBF (Mean Time Between Failures)

- M300/M300-G: 155,899 hrs. (MIL-HDBK-217-FN2)
- M301/M301-G/M301-TG/M301-TPG/M301-GW:
  148,930 hrs. (MIL-HDBK-217-FN2)

Software

- **Network Protocols:**

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

- **Routing/Firewall:**

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

- **VPN:**

Open VPN, IPsec (3DES, AES128, AES196, AES256, MD5, SHA-1, SHA256), GRE, PPTP, L2TP

- **Wireless Connectivity:**

Two SIM for failover/ roaming over/ back up
Two SIM data usage control
Seamless multi WAN connections switch

- **Others:**

DDNS, QoS, Virtual COM, UPnP

- **Alarm:**

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

Management Software

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

Environment

- Operating Temperature -20 ~ +70°C (M300/M301/M300-G/M301-G/M301-GW)
- Operating Temperature -40 ~ +75°C (M301-TG/M301-TPG)
- Storage Temperature -40 ~ +85°C
- Ambient Relative Humidity 10 ~ 95% (non-condensing)
- Humidity 0 ~ 95% (non-condensing)

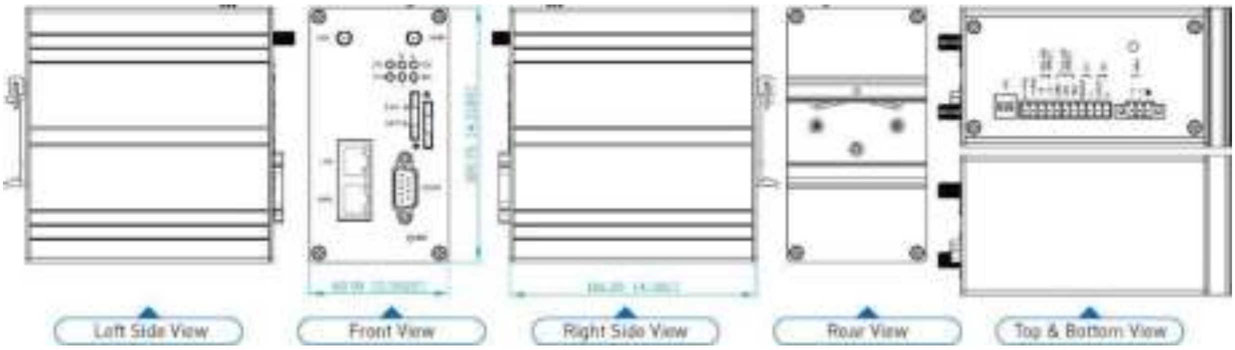
Standards and Certifications

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

1.3 Mechanical Dimensions

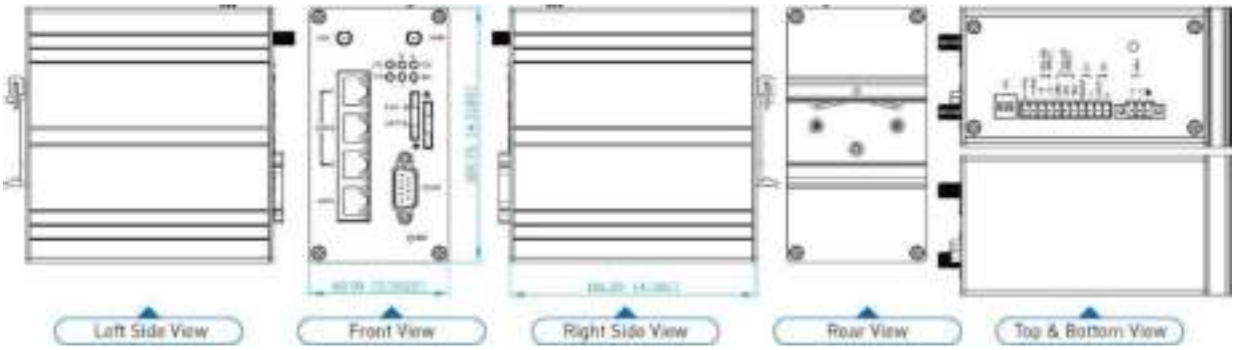
(1) M300 model:

1 x WAN, 1 x LAN, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, -20 ~ +70°C



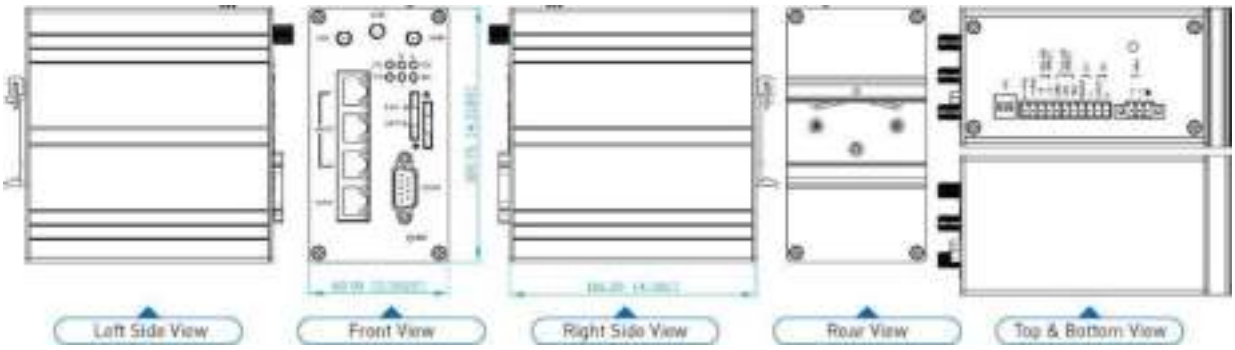
(2) M301 model:

1 x WAN, 3 x LANs, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, -20 ~ +70°C



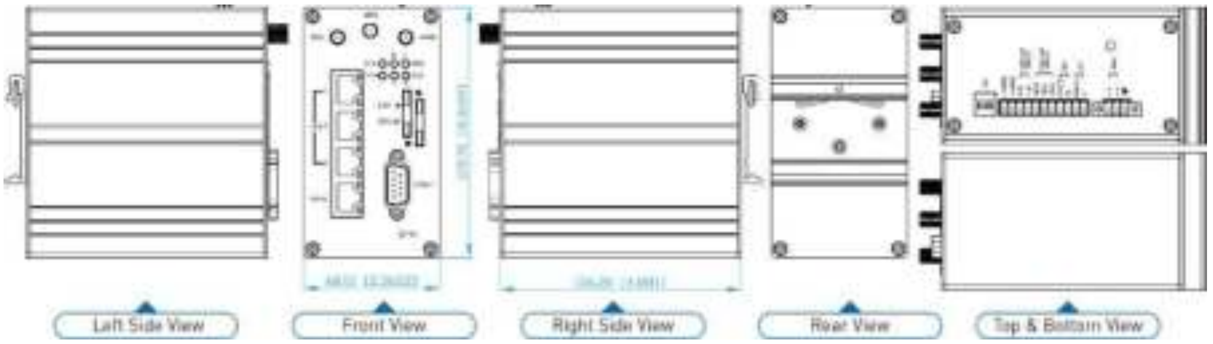
(3) M300-G model:

1 x WAN, 1 x LAN, 1 x GPS, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, -20 ~ +70°C



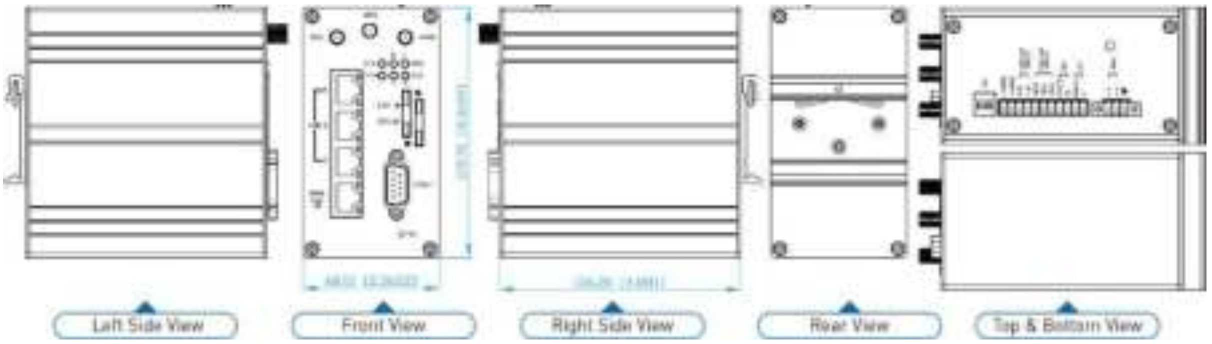
(4) M301-G / M301-TG model:

1 x WAN, 3 x LANs, 1 x GPS, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, -20 ~ +70°C (M301-G), -40 ~ +75°C (M301-TG)



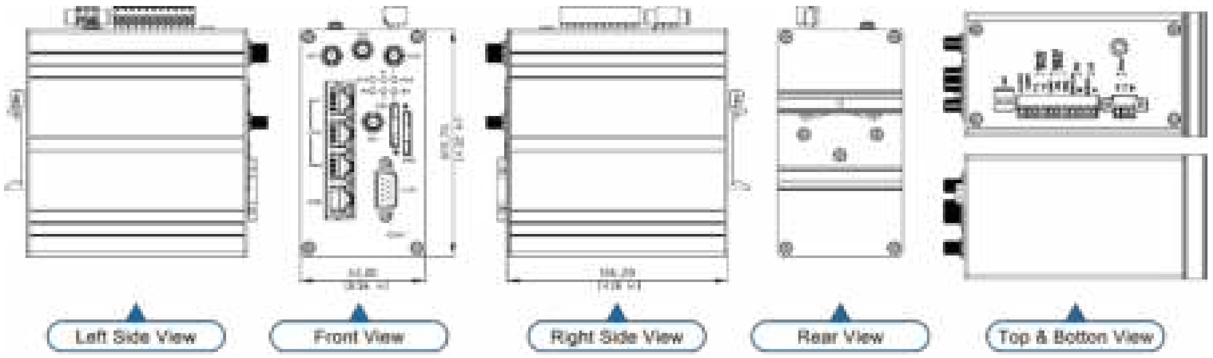
(5) M301-TPG model:

1 x WAN with IEEE 802.3at/af PoE PD, 3 x LANs, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, 1 x GPS, -40 ~ +75°C



(6) M301-GW model:

1 x WAN, 3 x LANs, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, 1 x GPS, 1 x Wi-Fi, -20 ~ +70°C



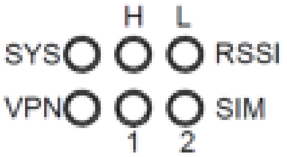
1.4 Ordering Information

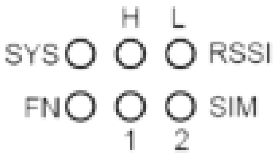
Model Name	Description
M300	Industrial 4G LTE Cellular Router (1 x WAN, 1 x LAN, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, -20 ~ +70°C)
M301	Industrial 4G LTE Cellular Router (1 x WAN, 3 x LANs, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, -20 ~ +70°C)
M300-G	Industrial 4G LTE Cellular Router (1 x WAN, 1 x LAN, 1 x GPS, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, -20 ~ +70°C)
M301-G	Industrial 4G LTE Cellular Router (1 x WAN, 3 x LANs, 1 x GPS, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, -20 ~ +70°C)
M301-TG	Industrial 4G LTE Cellular Router (1 x WAN, 3 x LANs, 1 x GPS, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, -40 ~ +75°C)
M301-TPG	Industrial 4G LTE Cellular Router (1 x WAN with IEEE 802.3at/af PoE PD, 3 x LANs, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, 1 x GPS, -40 ~ +75°C)
M301-GW	Industrial 4G LTE Cellular Router (1 x WAN, 3 x LANs, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, 1 x GPS, 1 x Wi-Fi, -20 ~ +70°C)

2 Hardware Installation

This chapter introduces how to install and connect the hardware.

2.1 LED Indicators



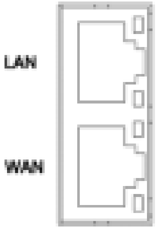


(M301-GW)

LED	SYS	RSSI High	RSSI Low	VPN	SIM1	SIM2	FN (M301-GW)
ON	System UP	Normal Signal	Low Signal	VPN Connected	Connected	Connected	VPN Connected
Slow Blinking	Booting	N/A	N/A	WAN Connected	Connecting	Connecting	WAN Connected
Fast Blinking	N/A	N/A	N/A	N/A	Error	Error	N/A
OFF	Power Down	N/A	N/A	NO WAN Connection	Not Working	Not Working	NO WAN Connection
Heart Beat	N/A	N/A	N/A	N/A	Reading	Reading	WiFi Connected

2.2 Ethernet Port

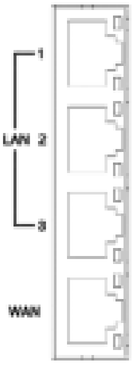
(1) 10/100 Mbps Ethernet LAN/WAN (M300/M300-G model)



The LAN and WAN interface are standard RJ45 connectors.

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

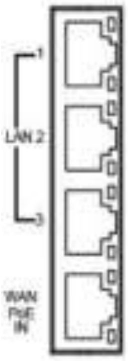
(2) 10/100 Mbps Ethernet LAN1~LAN3/WAN (M301/M301-G/M301-TG model)



The Ethernet LAN1~3 and WAN interfaces are standard RJ45 connectors.

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

(3) 10/100 Mbps Ethernet LAN1~LAN3/WAN (M301-TPG model)



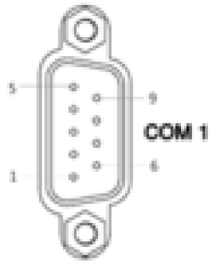
The Ethernet LAN1~3 interfaces are standard RJ45 connectors. The WAN interface is a standard RJ45 connector with IEEE 802.3at/af PoE PD.

(4) LED Indicator of Ethernet Port

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

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

2.3 Serial Port COM1 (Console-RS232)

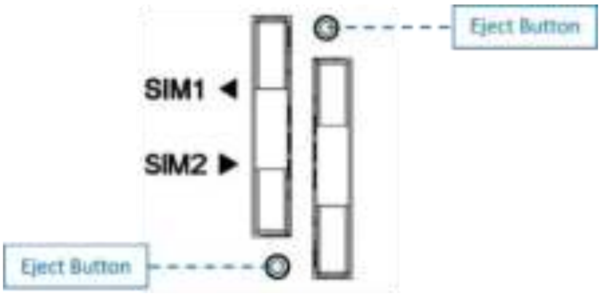


The serial port COM1 is a standard Sub-D connector.

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

2.4 Install the SIM Card

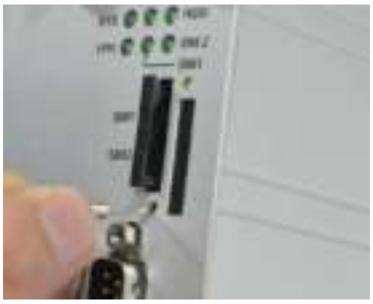
1. SIM1/SIM2 Card Drawers and Eject Buttons

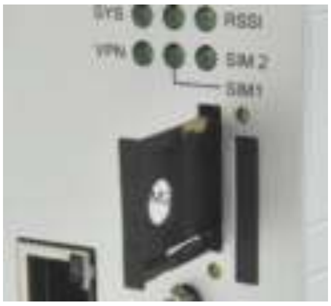


2. Insert and Remove SIM1/SIM2 Card

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

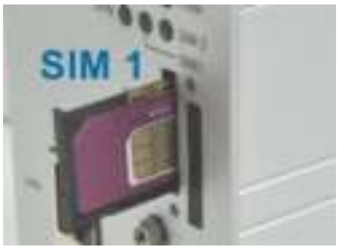
(2) Press the button with a paper clip or suitable tool to eject the SIM card from the drawer.

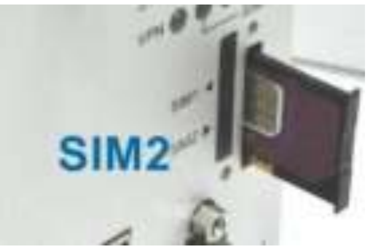




(3) Insert the SIM card with the contacts facing up and align it properly into the drawer. Make sure your direction of SIM Card and put it into the tray.

(4) Slide the drawer back and locks it in place.





Note:

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

2.5 Reset Button

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

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

Note:

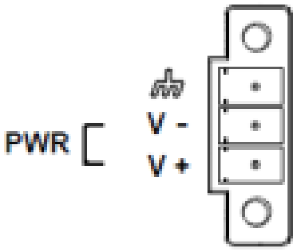
Press the Reset button and count the time around 5 seconds. The LED Indicators will be blinking to show you have activated the setting successfully.

2.6 External Antenna

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

2.7 Connecting the Power Supply

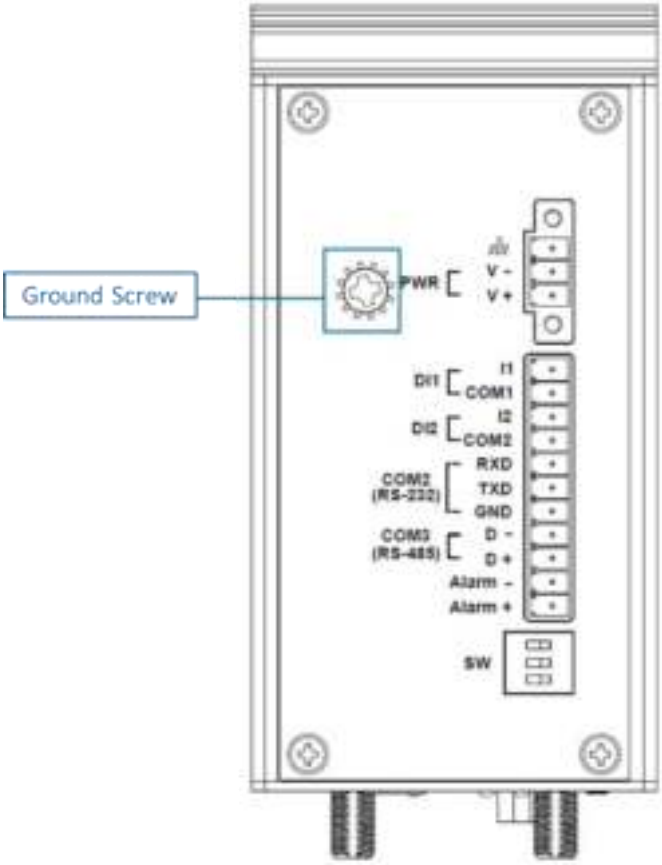
The router requires a DC power supply in the range of 10~32V DC. Please ensure all components are earthed to a common ground before connecting any wiring.



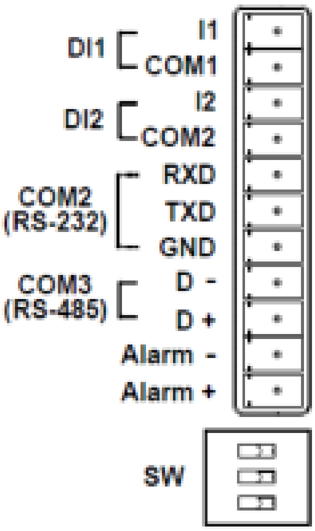
Pin	**Power (10~32VDC)**
⏚	FRAME GROUND
V -	Negative
V+	Positive

2.8 Grounding the Router

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



2.9 Pin Assignments



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

2.10 Connecting I/O Ports

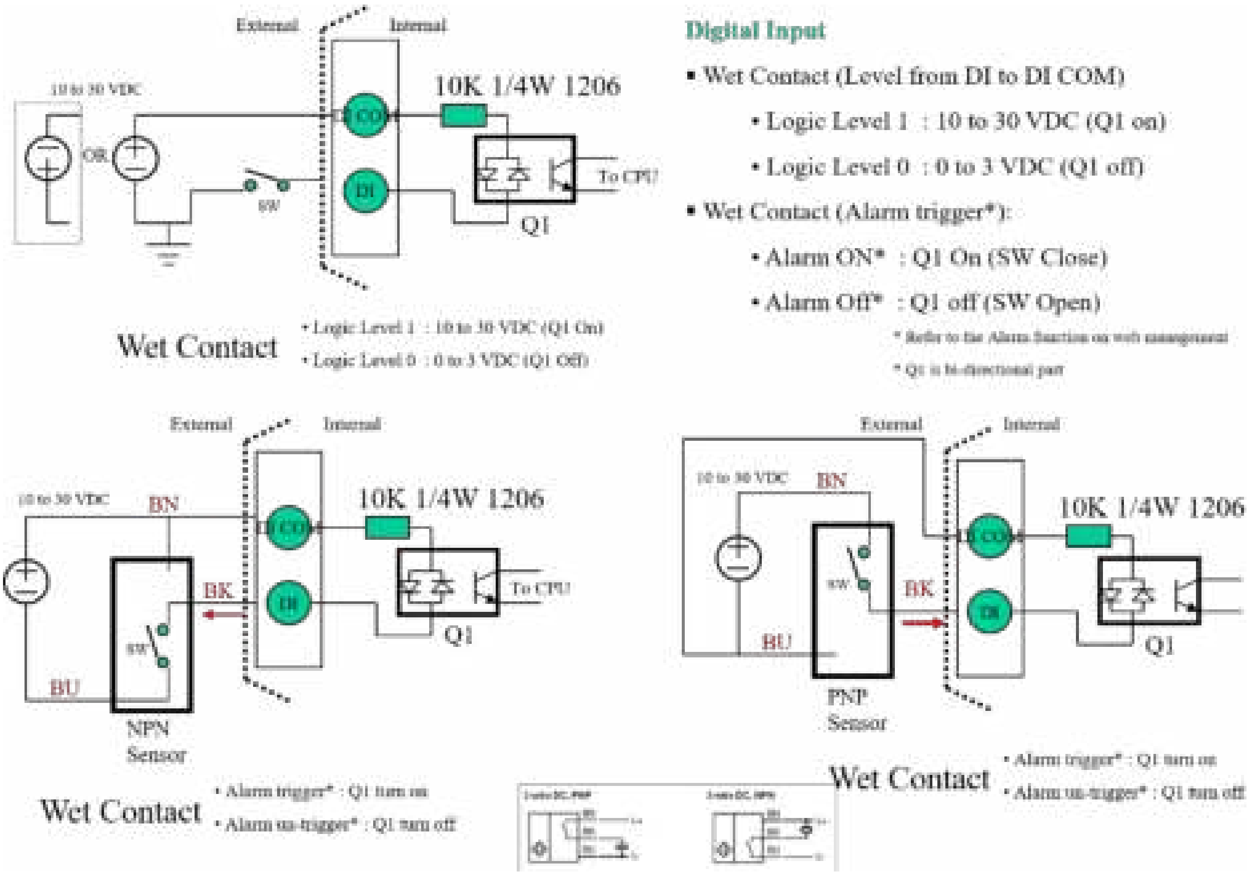
(1) Digital Input DI1 & DI2

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

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

- INPUT : +10 to +30V for state "1" (Q1 On)
- INPUT : +0 to +3V for state "0" (Q1 Off)

Note: Q1 is a bidirectional component.



Digital Input

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

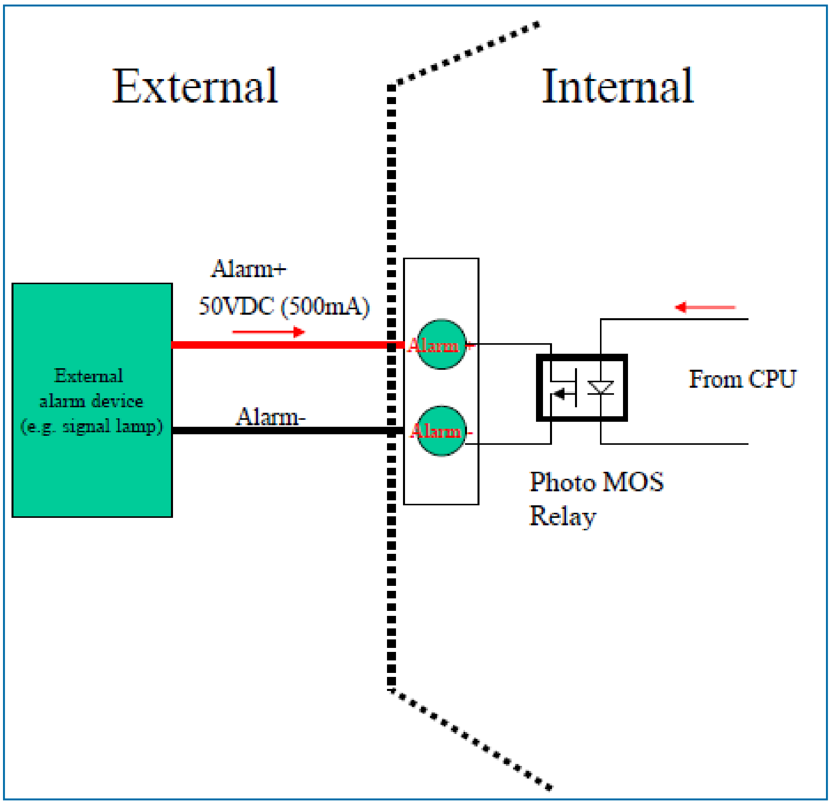
* Refer to the Alarm function on web management

* Q1 is bi-directional part

(2) Digital Output – Alarm Contacts

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

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



2.11 Serial Port COM2 (RS-232)

The serial port COM2 is a RS-232 interface.

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

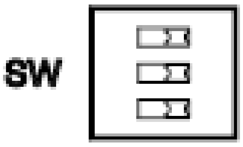
※ Both connectors (RS-232 and RS-485) have a common ground connection.

2.12 Serial Port COM3 (RS-485)

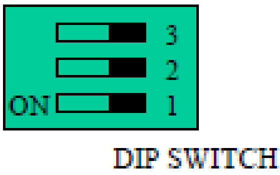
The serial port COM3 is a RS-485 interface.

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

2.13 DIP Switch



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



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

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

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

3 Configuration via Web Browser

3.1 Access the Web Configurator

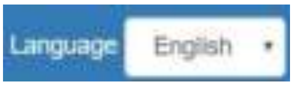
The web configuration is an HTML-based management interface for quick and easy set up of the cellular router. Monitoring of the status, configuration and administration of the router can be done via the Web interface.

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

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

Title Bar Panel > Selecting Language

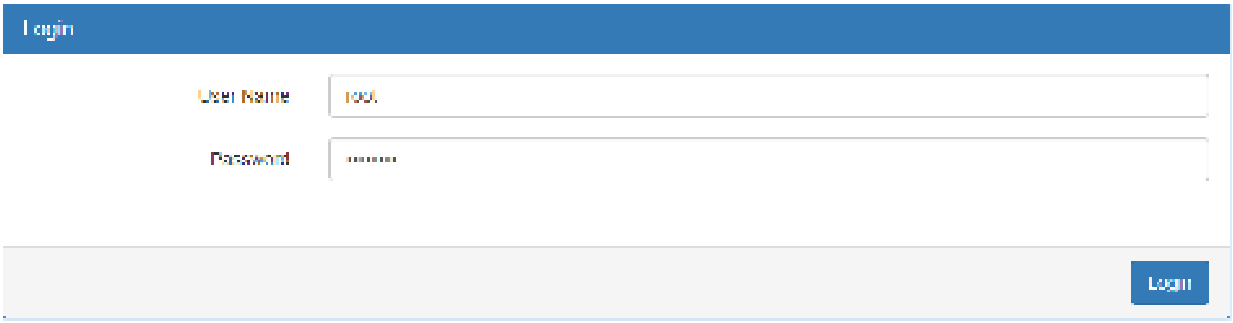
You can choose the languages, including English and Taiwan.



Logging in the Router

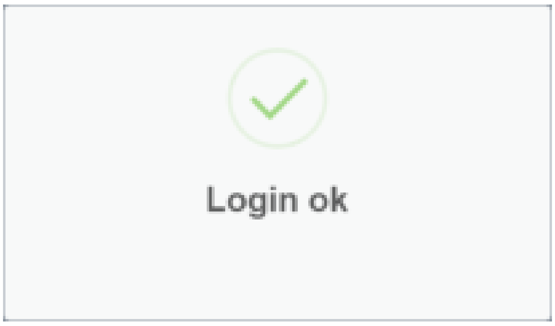
In this section, please fill in the default User Name **root** and the default Password **2wsx#EDC** and then click Login. For the system security, suggest changing them after configuration.

After clicking, the interface shows Login ok.



User Name root

Password ....

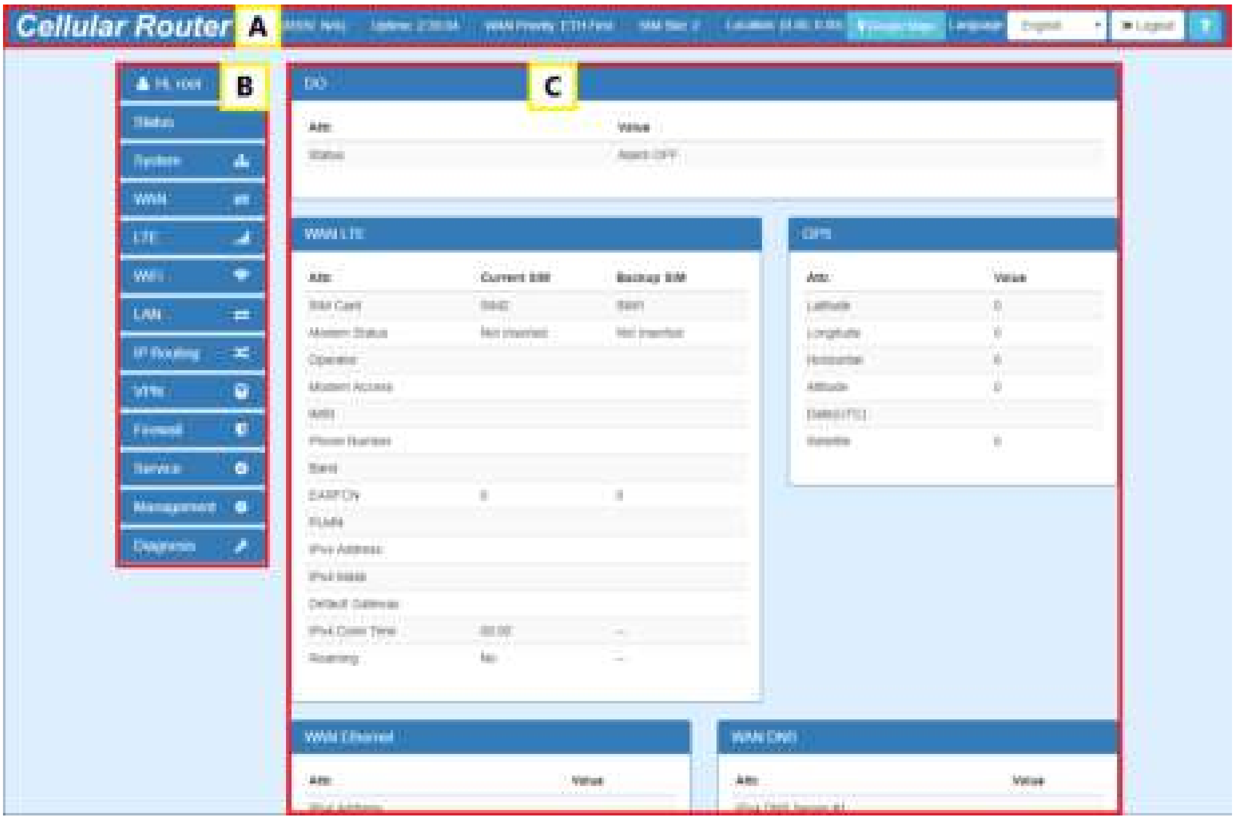


Note: After changing the User Name and Password, strongly recommend you to save them because another time when you login, the User Name and Password have to be used the new one you changed.

3.2 Navigate the Web Configurator

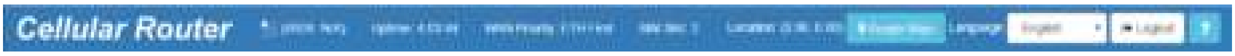
The main screen is divided into three parts as below.

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.
SIM Slot	Show the current using of SIM Slot that inserts into SIM1 or SIM2.
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

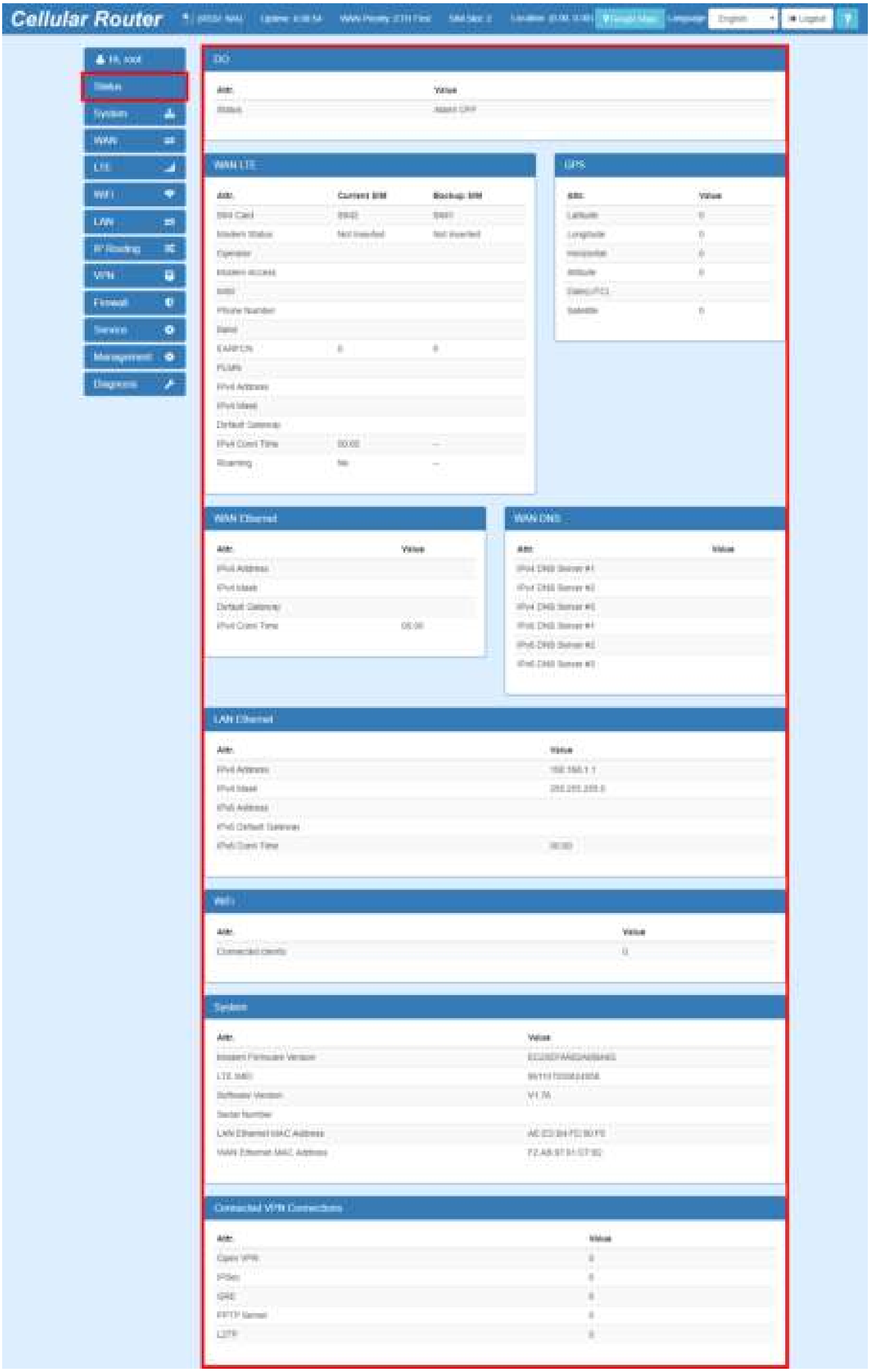
This section shows the information or setting fields from main menu and sub menu.

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, Dual SIM information, 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



DO

Attr.	Value
Status	Attach CPF

WAN LTE

Attr.	Current SIM	Backup SIM
SIM Card	SIM2	SIM1
Modem Status	Not Inserted	Not Inserted
Operator		
Modem access		
IMSI		
Phone Number		
Band		
EARFCN	0	0
PLMN		
IPv4 Address		
IPv4 Mask		
Default Gateway		
IPv4 Conn Time	00:00	--
Roaming	No	--

GPS

Attr.	Value
Latitude	0
Longitude	0
Horizontal	0
Altitude	0
Date(UTC)	-
Satellite	0

WAN Ethernet

Attr.	Value
IPv4 Address	
IPv4 Mask	
Default Gateway	
IPv4 Conn Time	00:00

WAN DNS

Attr.	Value
IPv4 DNS Server #1	
IPv4 DNS Server #2	
IPv4 DNS Server #3	
IPv6 DNS Server #1	
IPv6 DNS Server #2	
IPv6 DNS Server #3	

LAN Ethernet

Attr.	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	
IPv6 Default Gateway	
IPv6 Conn Time	00:00

Wi-Fi

Attr.	Value
Connected clients	0

System

Attr.	Value
Modem Firmware Version	EC25EFAR02A09M4G
LTE IMEI	861107030824058
Software Version	V1.76
Serial Number	
LAN Ethernet MAC Address	AE:C3:B4:FC:9D:FE
WAN Ethernet MAC Address	F2:A8:97:91:57:9D

Connected VPN Connections

Attr.	Value
Open VPN	0
IPSec	0
GRE	0
PPTP Server	0
L2TP	0

Status > DO	
Item	**Description**
Attribute	
Alarm OFF	Alarm configured to be disabled.
Alarm ON	Alarm configured to be enabled.
Alarm PULSE	Alarm configured to be enabled and DO in pulse mode.
Force ON	DO is force ON and in always mode by SMS/HTTPS.
Force OFF	DO is force OFF by SMS/HTTPS.
Force PULSE	DO is force ON and in pulse mode by SMS/HTTPS.

Status > WAN LTE	
Item	**Description**
Attribute	
WAN LTE	The status of LTE.
Operator	Display the name of operator.
Modem Access	Show the router to access protocol type.
IMSI	Show the IMSI number of the current SIM cards.
Phone Number	Show the phone number of the current SIM or Backup SIM.
Band	Show current connected Band.
EARFCN	Absolute radio-frequency channel number.
PLMN	Public LAN Mobile Network ID.
IPv4 Address	LTE obtain IPv4 address.
IPv4 Mask	LTE IPv4 mask.
Default Gateway	LTE WAN IPv4 Default Gateway.
IPv4 Conn Time	LTE WAN IPv4 Connected Time.
Roaming	Roaming status.

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.
IPv4 Conn Time	Ethernet WAN IPv4 Connected Time.

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 > LAN Ethernet	
Item	**Description**
Attribute	
IPv4 Address	Ethernet LAN is assigned IPv4 Address.
IPv4 Mask	Ethernet LAN is assigned IPv4 Mask.
IPv6 Address	Ethernet LAN is assigned IPv6 Address.
IPv6 Conn Time	IPv6 Connected Time.

Status > WiFi	
Item	**Description**
Attribute	
Connected Clients	Show the clients who have connected to the device.

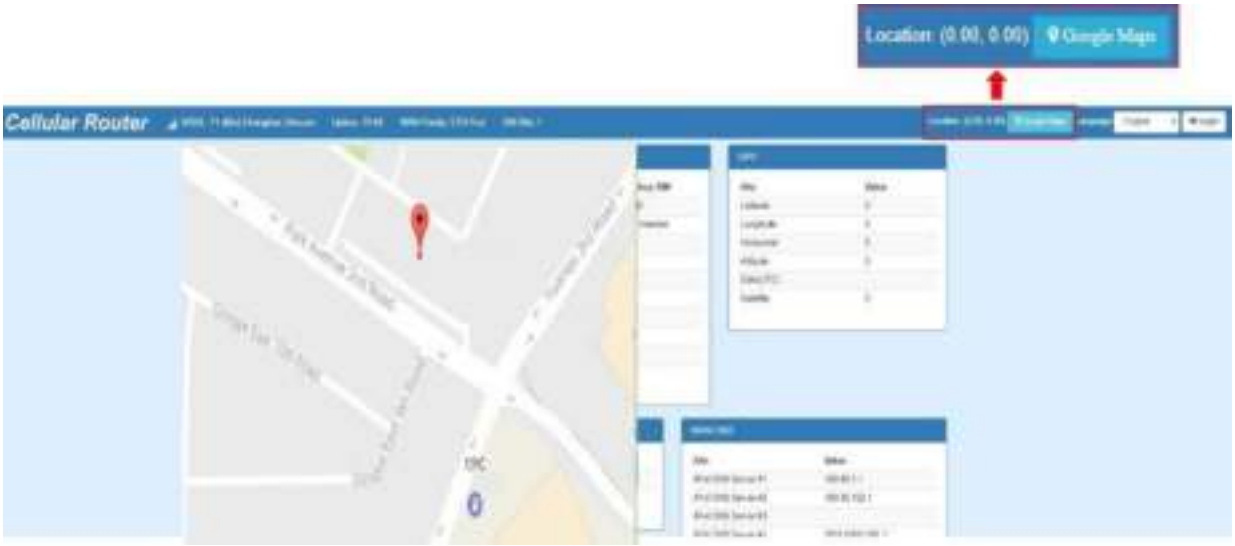
Status > GPS	
Item	**Description**
Attribute	
Latitude	Show the latitude information of location.
Longitude	Show the longitude information of location.
Horizontal	Show the horizontal information of location.
Altitude	Show the altitude information of location.
Date (UTC)	Show the date information of location.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

Status > System	
Item	**Description**
Attribute	
Modem Firmware Version	Show the modem firmware version of the device.
LTE IMEI	Show the IMEI - International Mobile Equipment Identity.
Software Version	Show the software version currently running on the device.
Serial Number	Show the serial number of the device.
LAN Ethernet MAC Address	Show the MAC address of LAN interface.
WAN Ethernet MAC Address	Show the MAC address of WAN interface.

Status > Connected VPN Connection	
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.

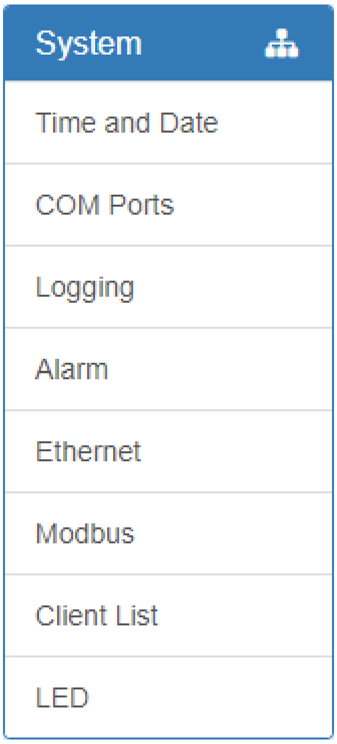
4.1 Status > GPS

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, Modbus, and Client List.



5.1 System > Time and Date

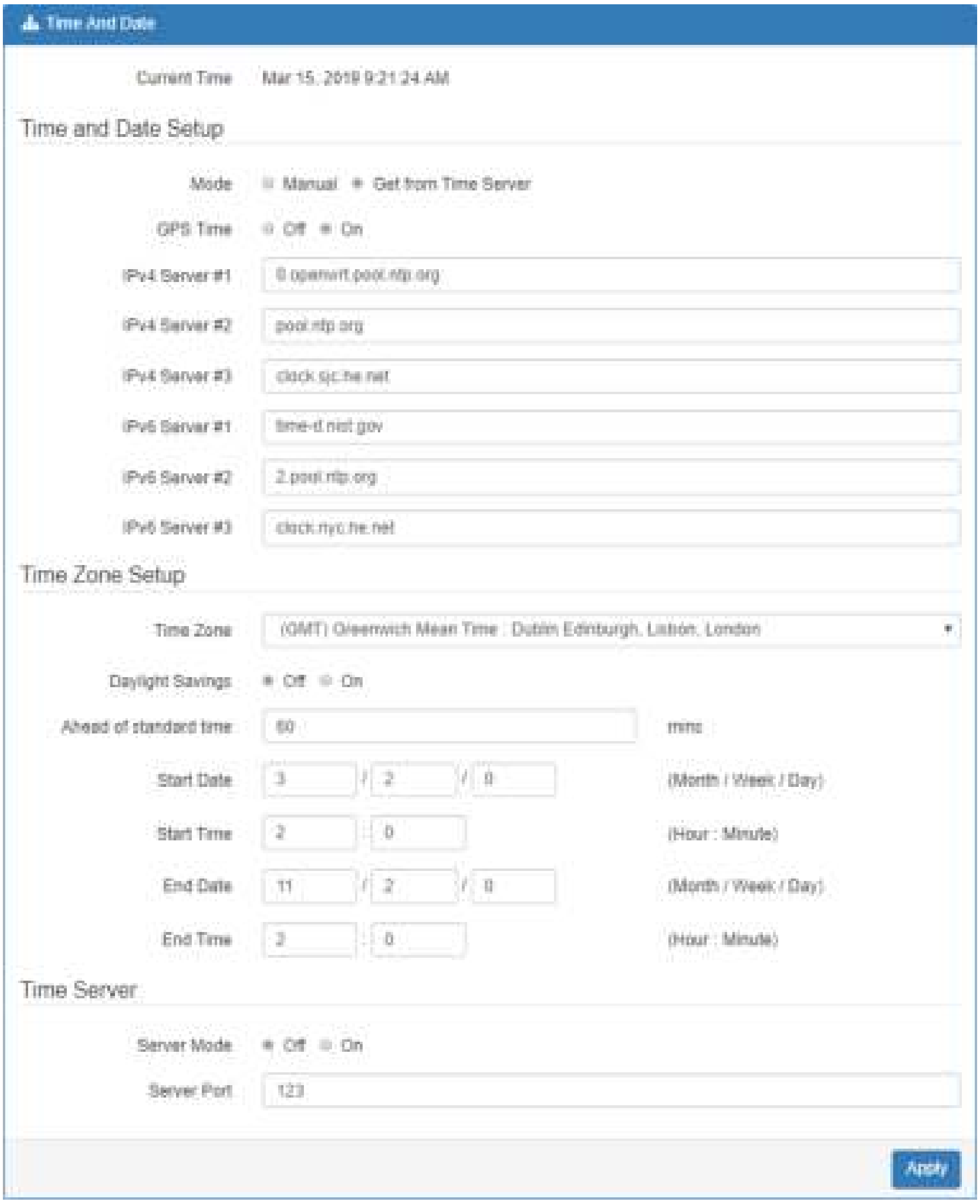
This section allows you to set up the time and date of router and NTP server. There are two modes at Time and Date Setup, including **Get from Time Server** and **Manual**. The default mode is **Get from Time Server**.

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: Mar 15, 2019 9:21:24 AM

Time and Date Setup

Mode: ○ Manual ● Get from Time Server

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)

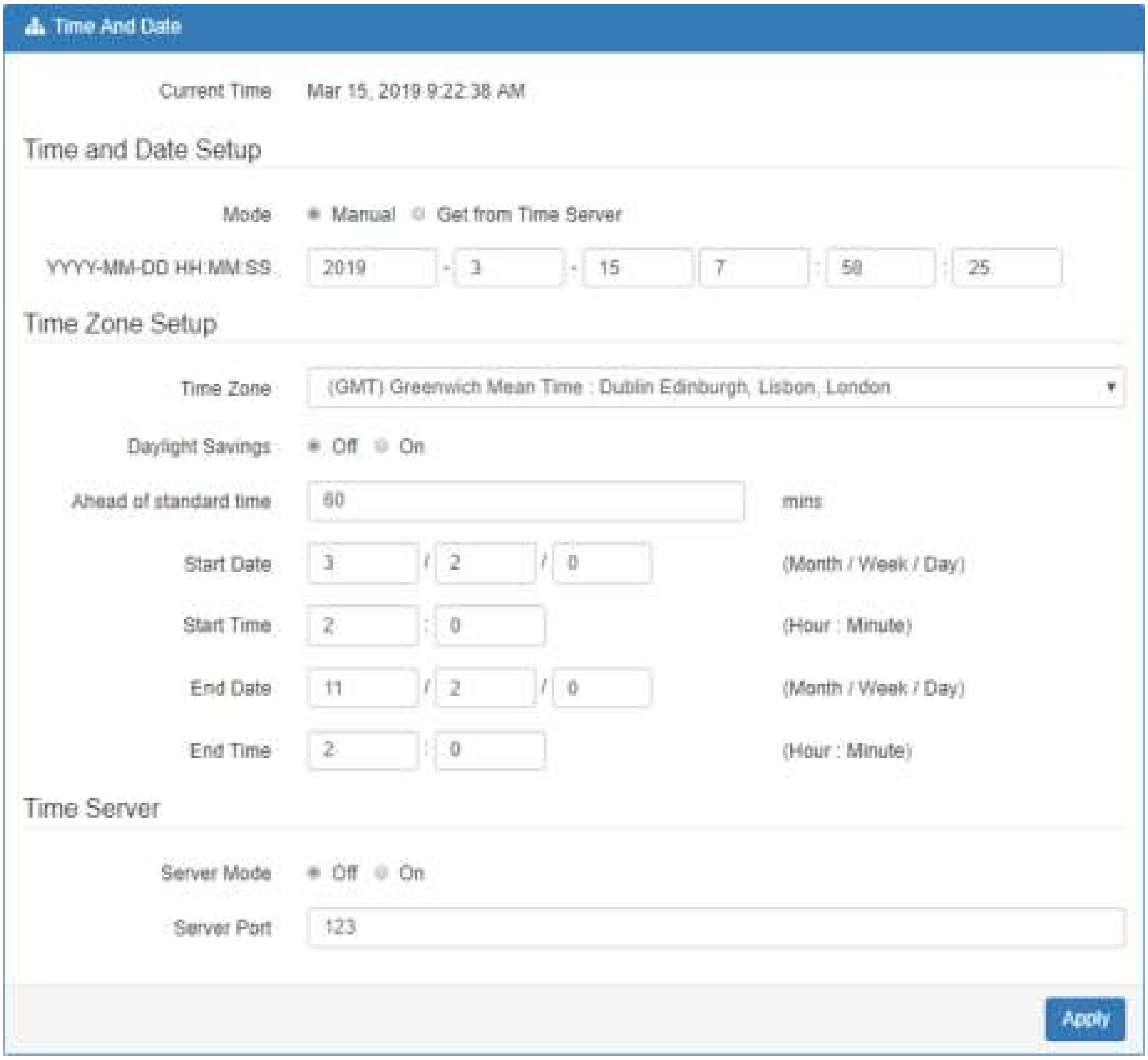
Time Server

Server Mode: ● Off ○ On

Server Port: 123

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.



Current Time Mar 15, 2019 9:22:38 AM

Time and Date Setup

Mode ● Manual ○ Get from Time Server

YYYY-MM-DD HH:MM:SS 2019 - 3 - 15 7 : 58 : 25

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)

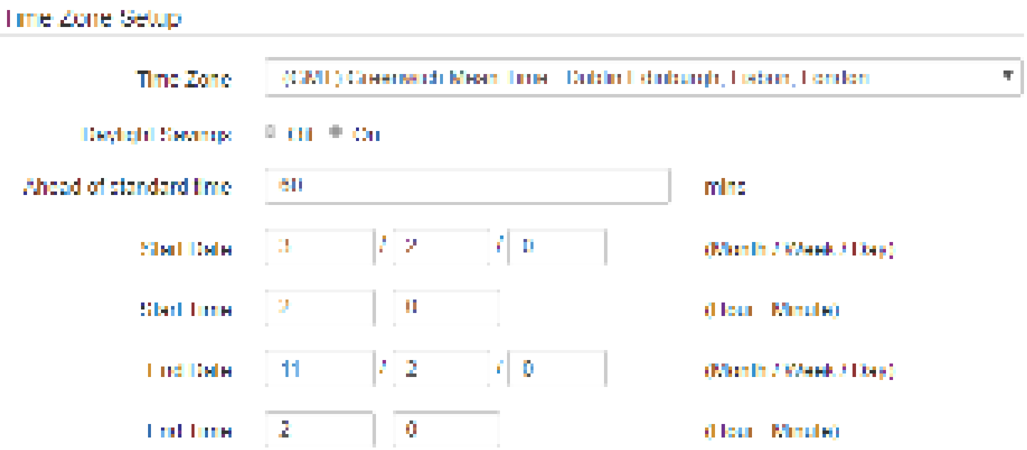
Time Server

Server Mode ● Off ○ On

Server Port 123

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)

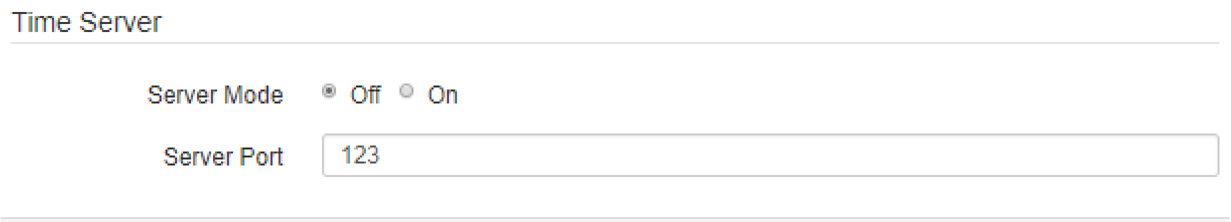
End Date: 11 / 2 / 0 (Month / Week / Day)

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.



Time Server

Server Mode ● Off ○ On

Server Port 123

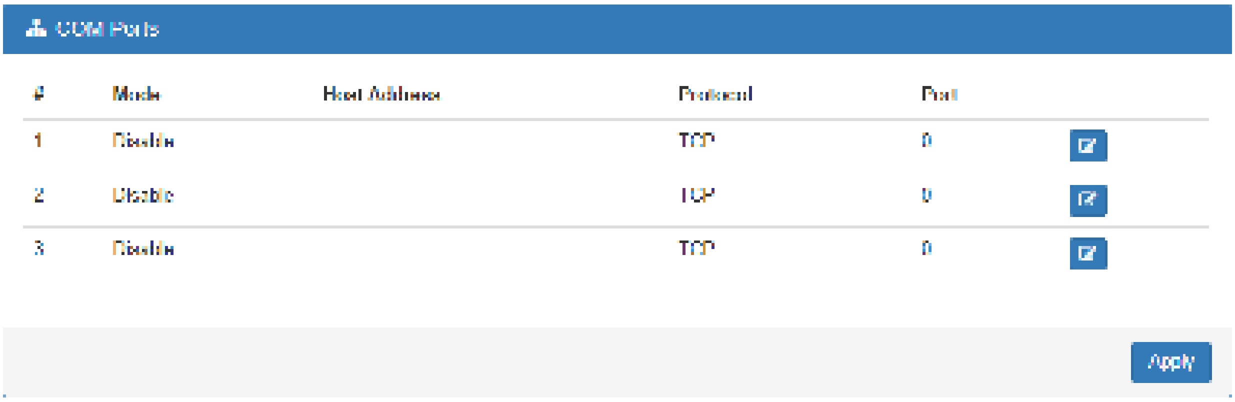
System > Time Server	
Item	**Description**
Server mode	Turn on/off the time server.
Server port	The UDP port listened by time server.

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 either RS232 or RS485.

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

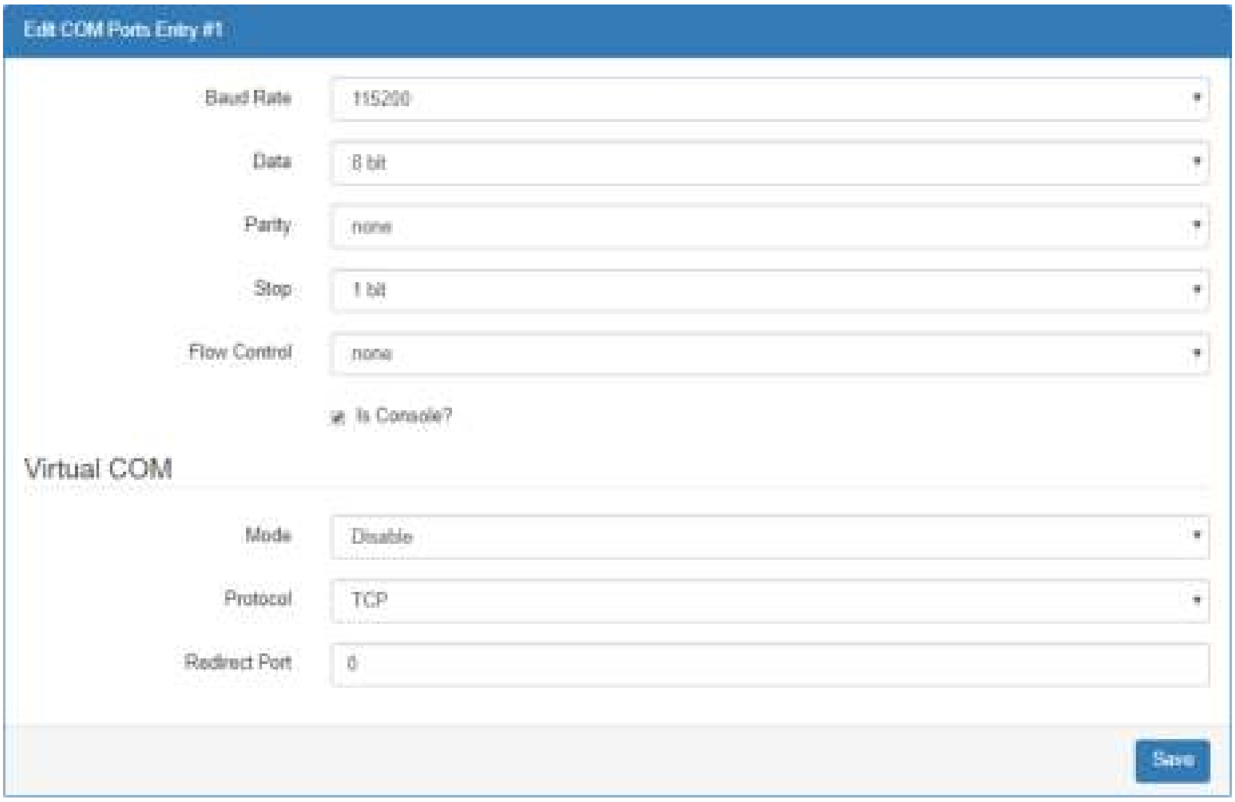
(1) The default is Disable. You can click ✎ edit button to configure your settings.



COM Ports

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

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



Edit COM Ports Entry #1

Baud Rate: 115200

Data: 8 bit

Parity: none

Stop: 1 bit

Flow Control: none

☑ Is Console?

Virtual COM

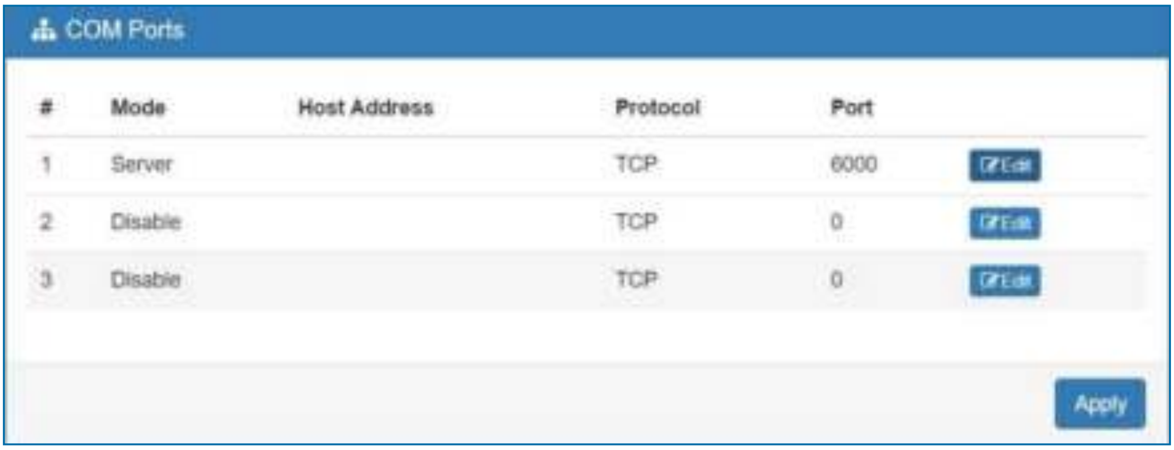
Mode: Disable

Protocol: TCP

Redirect Port: 0

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

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



COM Ports

#	Mode	Host Address	Protocol	Port	
1	Server		TCP	6000	Edit
2	Disable		TCP	0	Edit
3	Disable		TCP	0	Edit

(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.

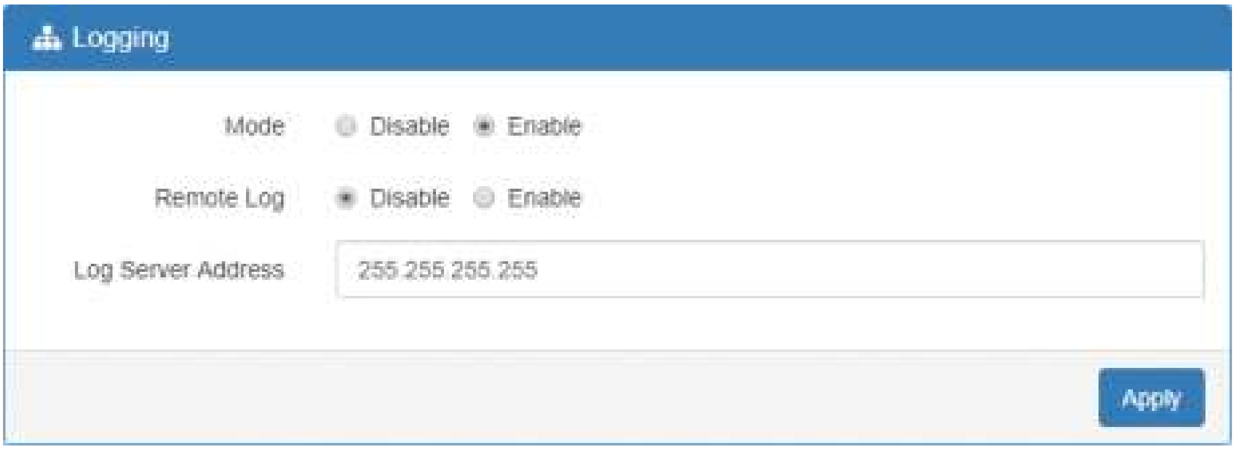
5.3 System > Logging

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.



Mode ○ Disable ● Enable

Remote Log ● Disable ○ Enable

Log Server Address 255.255.255.255

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

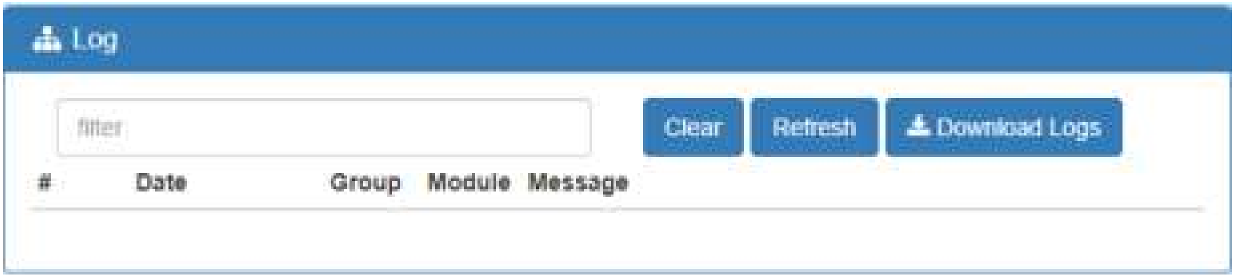
This section displays all data status.

(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.

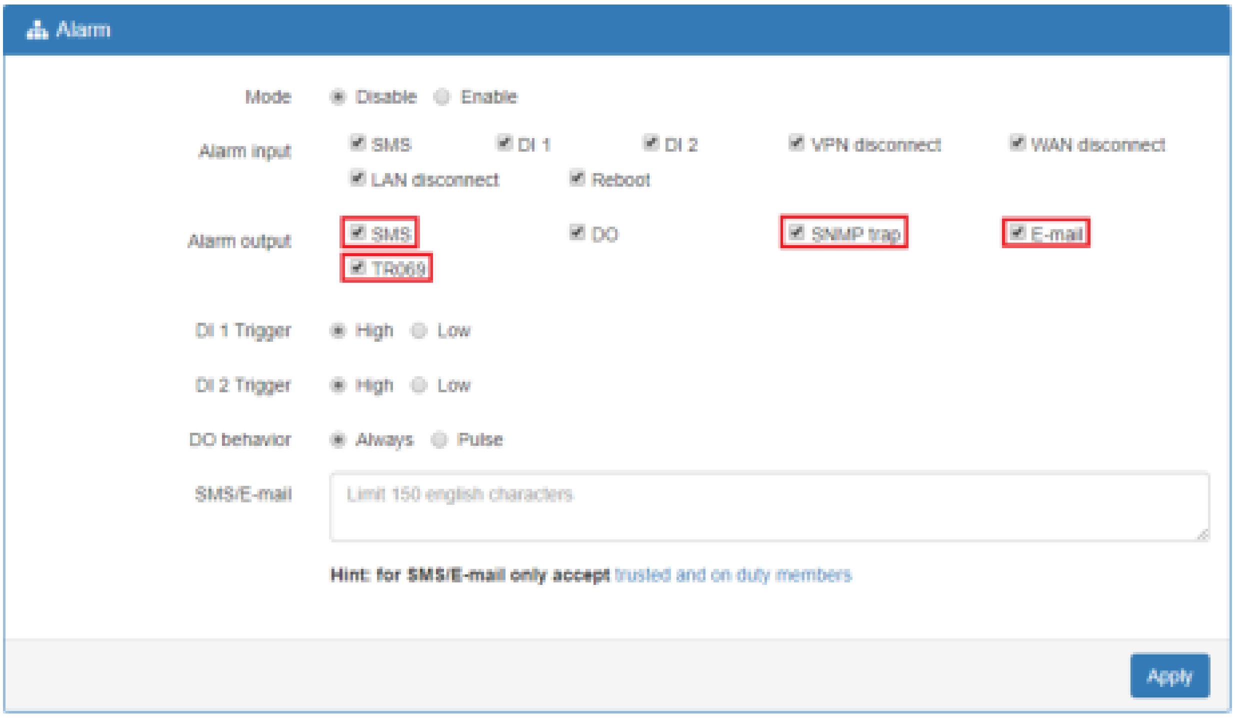
(4) When you click Download Logs, the system will download the latest data from your cellular router.



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.



Alarm

Mode: ● Disable ○ Enable

Alarm input: ☑ SMS ☑ DI 1 ☑ DI 2 ☑ VPN disconnect ☑ WAN disconnect ☑ LAN disconnect ☑ Reboot

Alarm output: ☑ SMS ☑ DO ☑ SNMP trap ☑ E-mail ☑ TR069

DI 1 Trigger: ● High ○ Low

DI 2 Trigger: ● High ○ Low

DO behavior: ● Always ○ Pulse

SMS/E-mail: Limit 150 english characters

Hint: for SMS/E-mail only accept trusted and on duty members

Apply

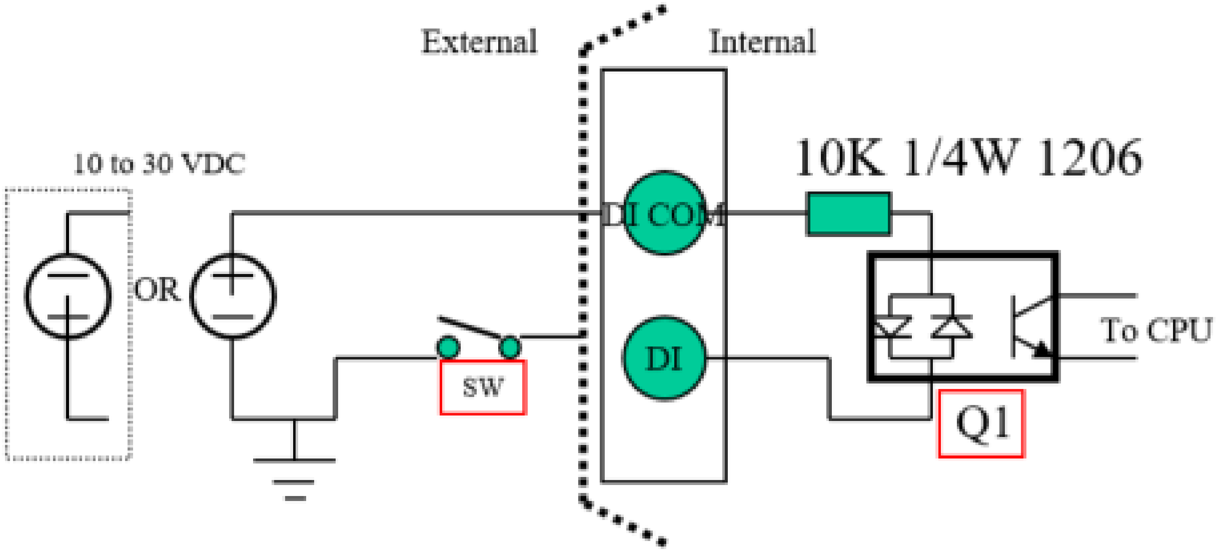
Note:

(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.

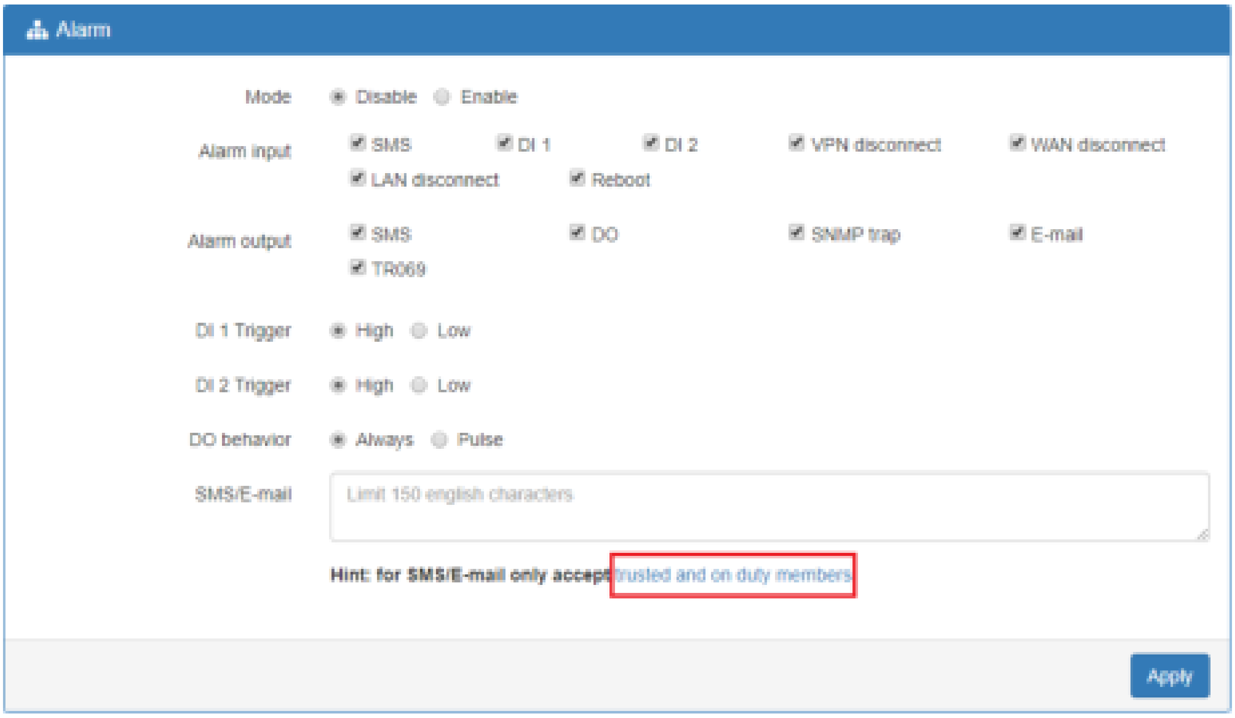
(4) If you select TR069 in Alarm output, you need to set up TR069 configuration from Service TR069.



System > Alarm	
Item	**Description**
Mode	Turn on/off the Alarm configuration. Select from Disable or Enable. The default is Enable.
Alarm Input	Select from SMS, DI 1, DI 2, VPN disconnect and WAN disconnect as input to trigger alarm. ● **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 1/2:** 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 and E-mail as alarm output.
DI 1 / 2 Trigger	Select from High or Low. The default is High Trigger. ● **High:** SW is On to trigger. ● **Low:** SW is OFF to trigge.
DO behavior	● **Always:** Pull DO high. ● **Pulse:** High and Low continuously. ● **Pulse Time Length:** Pulse time length (mini seconds).
SMS/E-mail	Write your messages and limit 150 English characters for the messages 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.



Alarm

Mode ● Disable ○ Enable

Alarm input ☑ SMS ☑ DI 1 ☑ DI 2 ☑ VPN disconnect ☑ WAN disconnect ☑ LAN disconnect ☑ Reboot

Alarm output ☑ SMS ☑ DO ☑ SNMP trap ☑ E-mail ☑ TR069

DI 1 Trigger ● High ○ Low

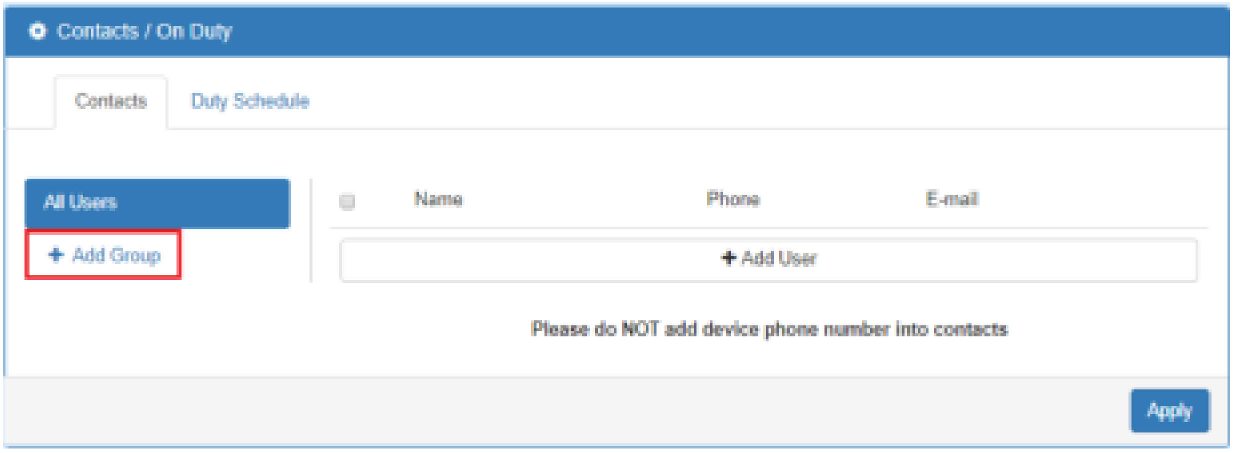
DI 2 Trigger ● High ○ Low

DO behavior ● Always ○ Pulse

SMS/E-mail: Limit 150 english characters

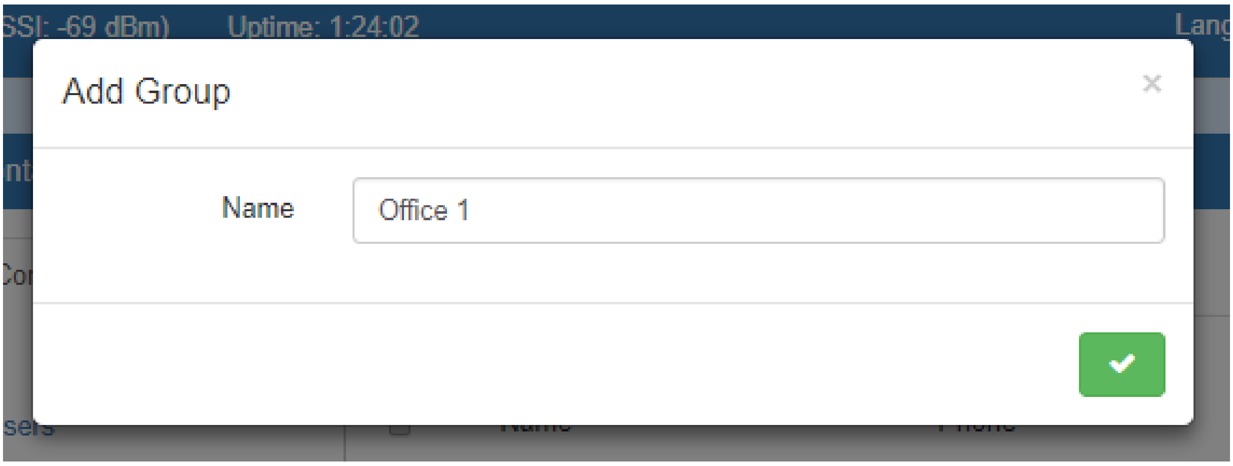
Hint: for SMS/E-mail only accept trusted and on duty members

Apply

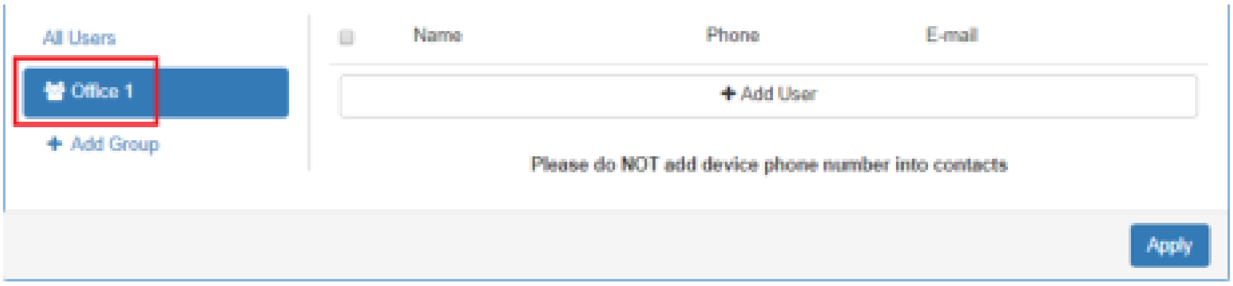


□	Name	Phone	E-mail

Please do NOT add device phone number into contacts



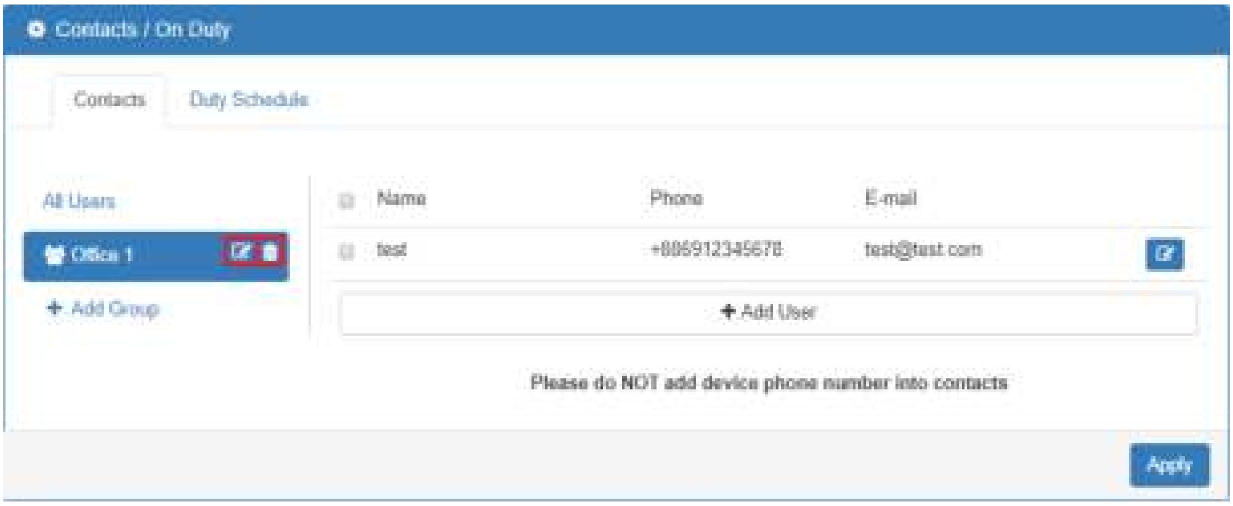
Name: Office 1



□	Name	Phone	E-mail

Please do NOT add device phone number into contacts

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

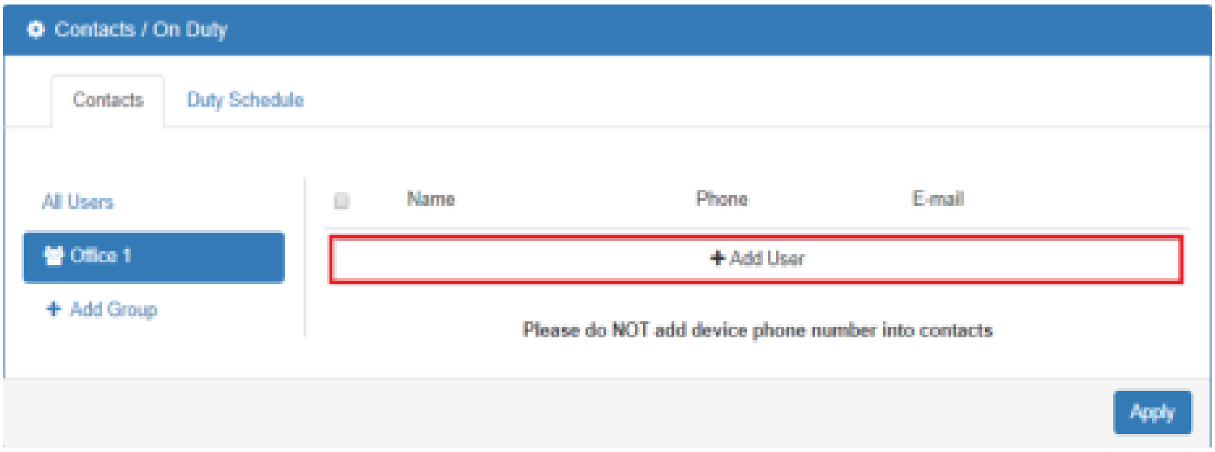


□	Name	Phone	E-mail
□	test	+886912345678	test@test.com

Please do NOT add device phone number into contacts

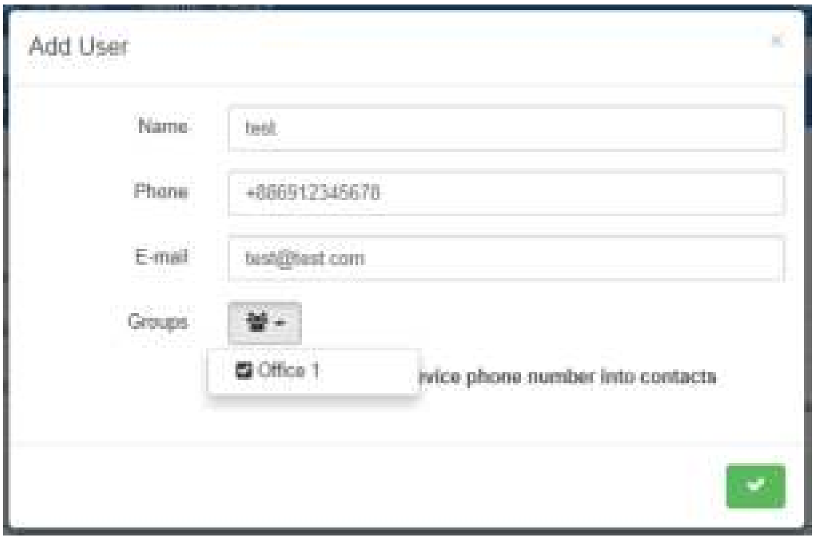
5.4.2 Alarm > Contacts > Add User

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



Please do NOT add device phone number into contacts

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



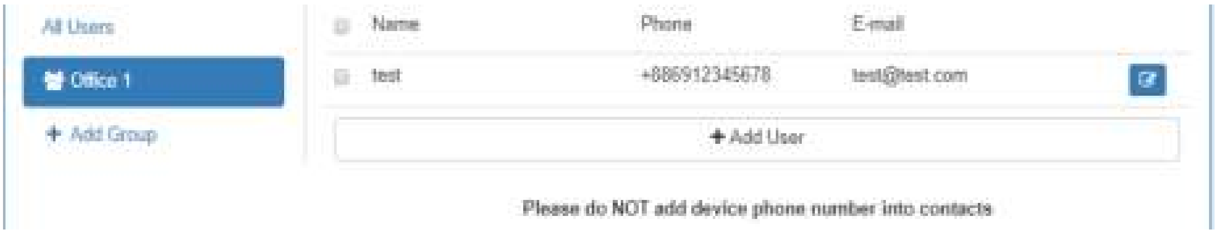
Name: test

Phone: +886912345678

E-mail: test@test.com

…vice phone number into contacts

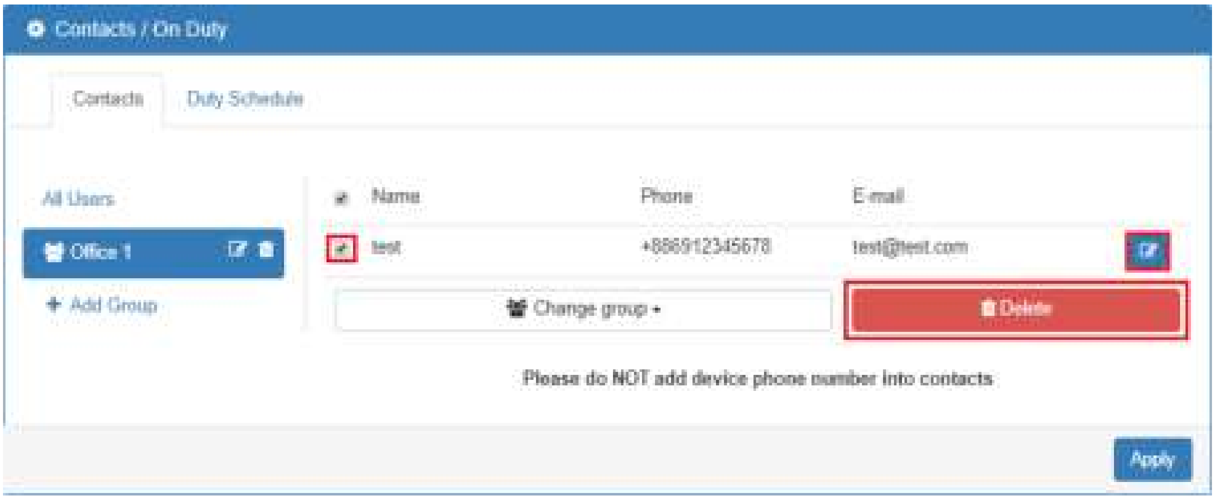
- After submitting your setting, the interface returns to Group window setting. Now you can see your naming group and the user's information that you have added.



□	Name	Phone	E-mail
□	test	+886912345678	test@test.com

Please do NOT add device phone number into contacts

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

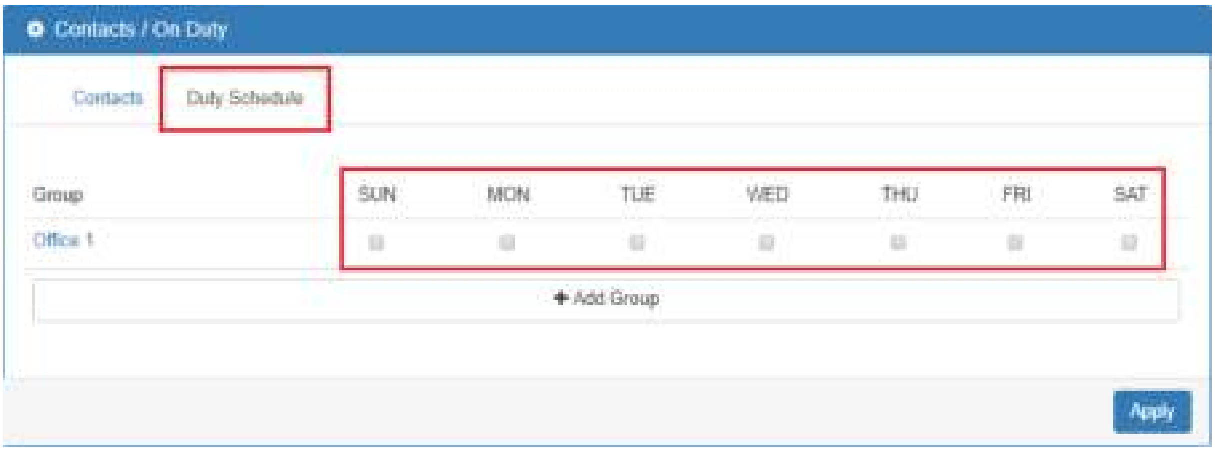


☑	Name	Phone	E-mail
☑	test	+886912345678	test@test.com

Please do NOT add device phone number into contacts

5.4.3 Alarm > Duty Schedule

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



Group	SUN	MON	TUE	WED	THU	FRI	SAT
Office 1	□	□	□	□	□	□	□

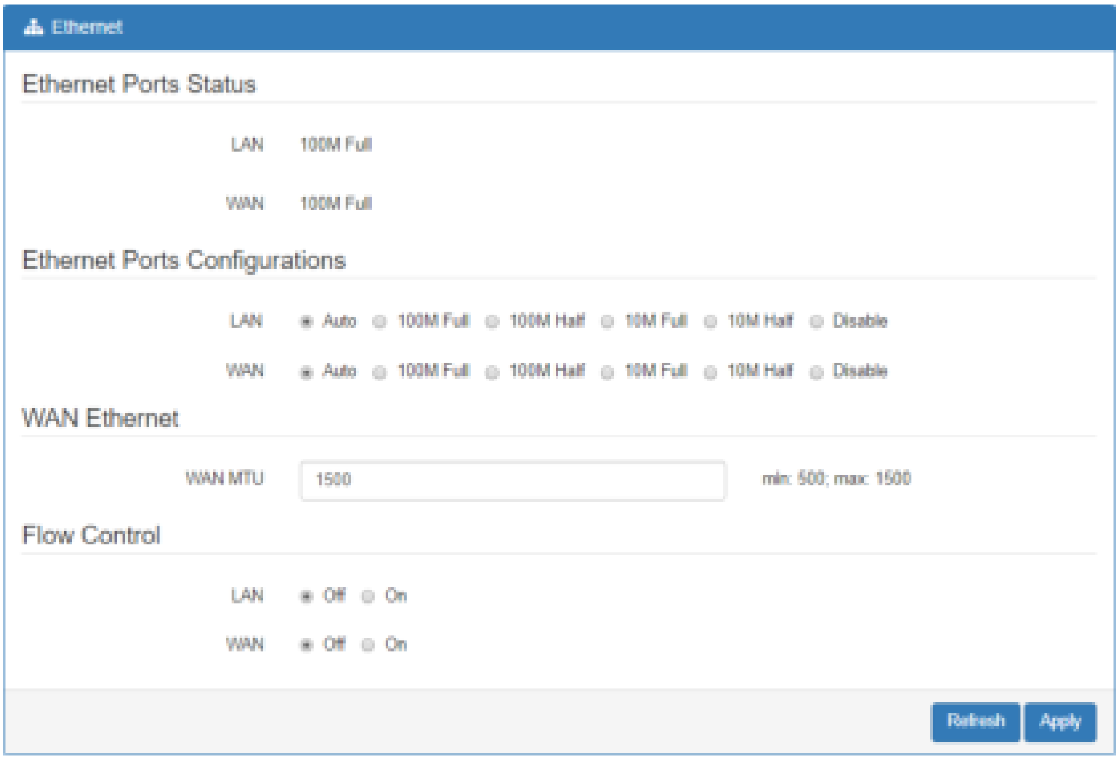
5.5 System > Ethernet

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.

- For one LAN port (M300/M300-G/)



Ethernet Ports Status

LAN 100M Full

WAN 100M Full

Ethernet Ports Configurations

LAN ● Auto ○ 100M Full ○ 100M Half ○ 10M Full ○ 10M Half ○ Disable

WAN ● Auto ○ 100M Full ○ 100M Half ○ 10M Full ○ 10M Half ○ Disable

WAN Ethernet

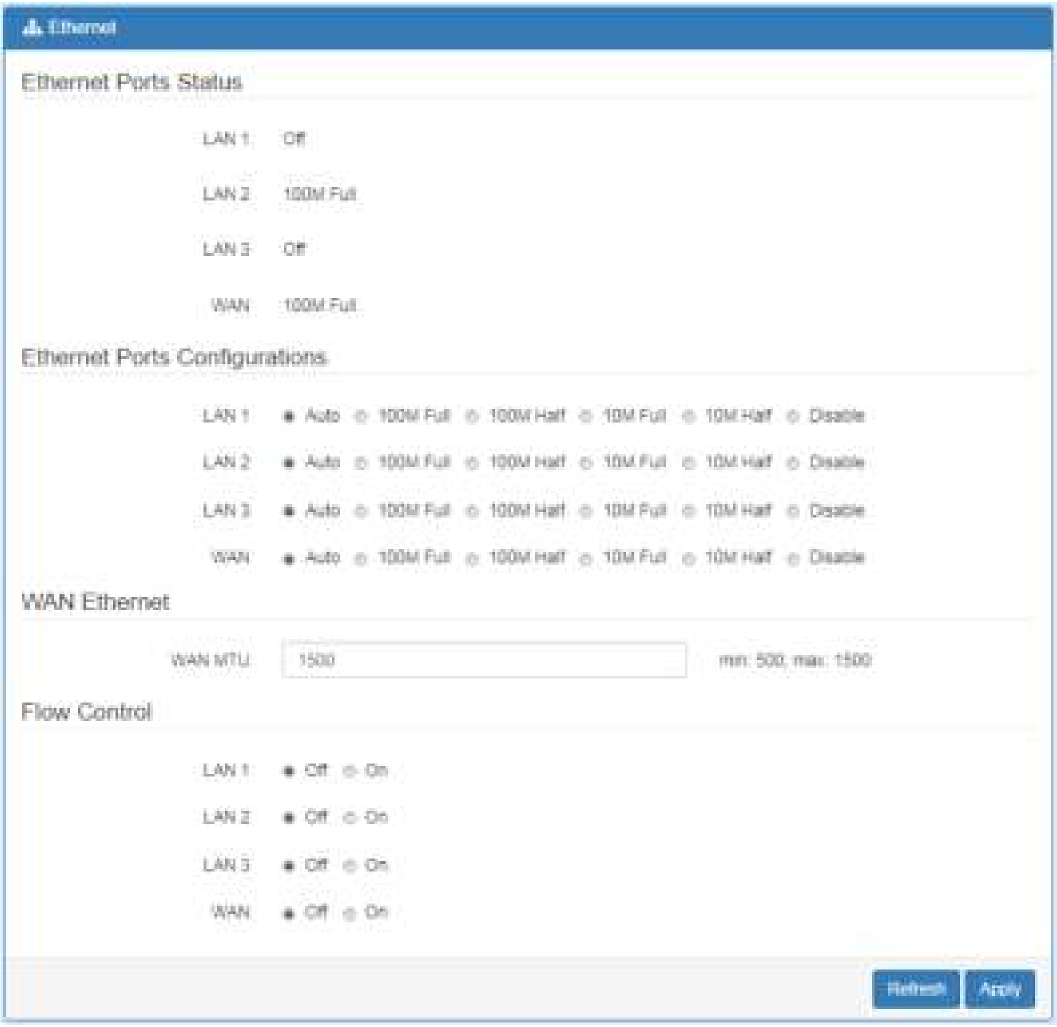
WAN MTU 1500 min: 500; max: 1500

Flow Control

LAN ● Off ○ On

WAN ● Off ○ On

- For three LAN ports (M301/M301-G/M301-TG/M301-TPG/M301-GW)



Ethernet Ports Status

LAN 1 Off

LAN 2 100M Full

LAN 3 Off

WAN 100M Full

Ethernet Ports Configurations

LAN 1 ● Auto ○ 100M Full ○ 100M Half ○ 10M Full ○ 10M Half ○ Disable

LAN 2 ● Auto ○ 100M Full ○ 100M Half ○ 10M Full ○ 10M Half ○ Disable

LAN 3 ● Auto ○ 100M Full ○ 100M Half ○ 10M Full ○ 10M Half ○ Disable

WAN ● Auto ○ 100M Full ○ 100M Half ○ 10M Full ○ 10M Half ○ Disable

WAN Ethernet

WAN MTU 1500 min: 500; max: 1500

Flow Control

LAN 1 ● Off ○ On

LAN 2 ● Off ○ On

LAN 3 ● Off ○ On

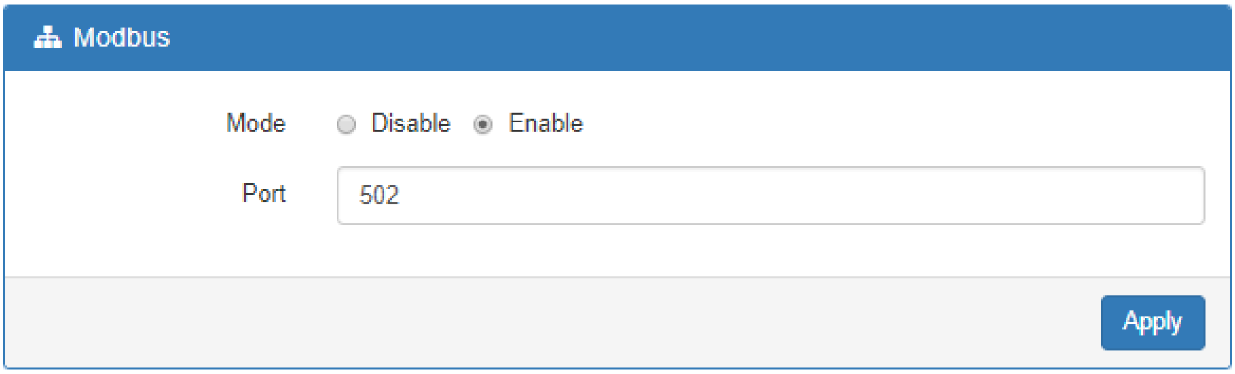
WAN ● Off ○ On

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 user to control the traffic ingress from Ethernet LAN or WAN.

5.6 System > Modbus

This section allows you to configure the Modbus.

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



Mode ○ Disable ● Enable

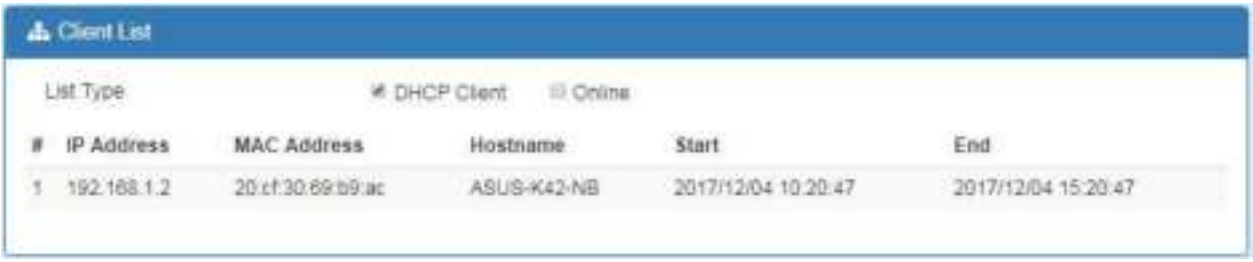
Port 502

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

5.7 System > Client List

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

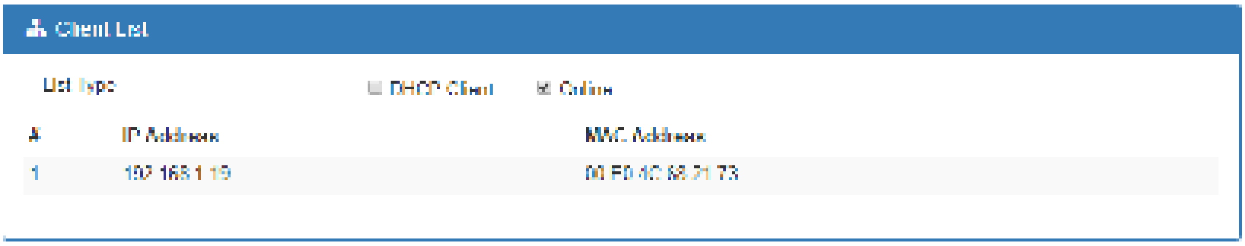
For **DHCP Client** type, the information shows IP address, MAC address, Hostname and the expiry time of IP (Start/End).



List Type ☑ DHCP Client ☐ Online

#	IP Address	MAC Address	Hostname	Start	End
1	192.168.1.2	20:cf:30:69:b9:ac	ASUS-K42-NB	2017/12/04 10:20:47	2017/12/04 15:20:47

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



Client List

List Type ☐ DHCP Client ☑ Online

#	IP Address	MAC Address
1	192.168.1.19	00:E0:4C:68:21:73

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.

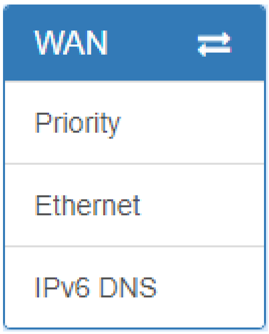
5.8 System > LED

This section allows you to set up the function led.

System > Client List	
Item	**Description**
Function LED	● **Default:** - **ON:** VPN connected. - **Slow Blinking:** WAN connected. - **OFF:** No WAN connection. ● **WiFi AP:** - **Heart Beat Blinking:** WiFi clients connected and it takes precedence. - Otherwise as default behavior.

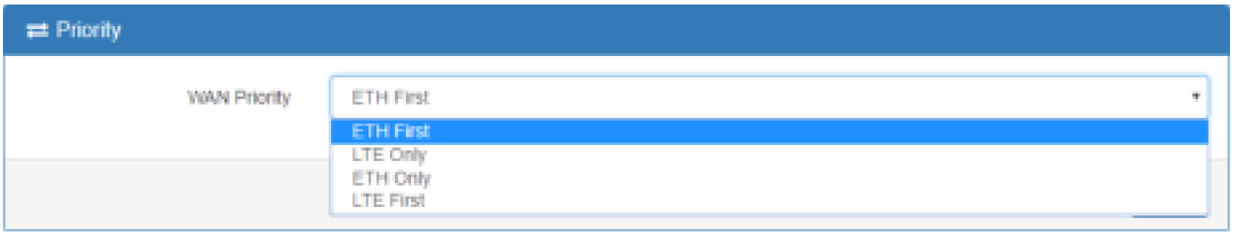
6 Configuration > WAN

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.

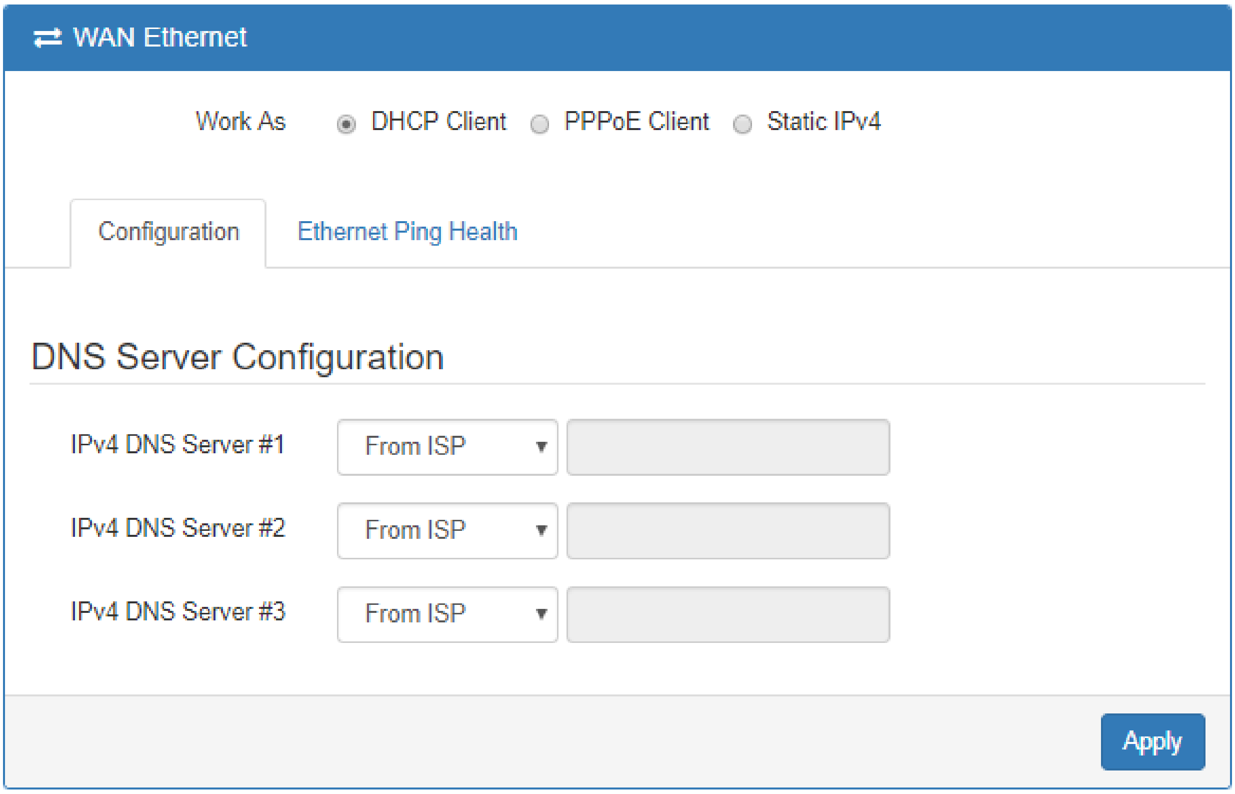


WAN > Priority	
Item	**Description**
Priority	● **ETH First:** WAN Ethernet is first priority and the second priority is LTE. The default is ETH First. ● **LTE Only:** The priority is only LTE. ● **ETH Only:** The priority is only Ethernet. ● **LTE First:** WAN LTE is first priority and the second priority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

6.2 WAN > Ethernet

6.2.1 WAN Ethernet Configuration

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



WAN Ethernet

Work As ● DHCP Client ○ PPPoE Client ○ Static IPv4

DNS Server Configuration

IPv4 DNS Server #1: From ISP

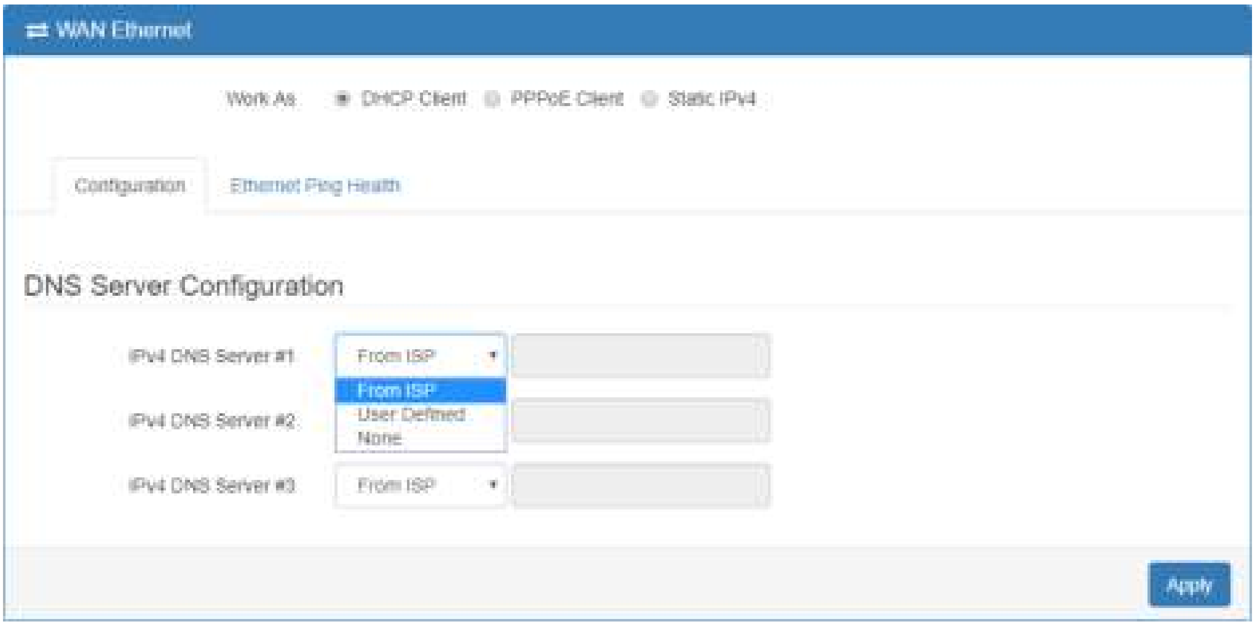
IPv4 DNS Server #2: From ISP

IPv4 DNS Server #3: From ISP

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

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

For IPv4 DNS Server, it provides three options to set up and each option has provided with “From ISP”, “User Defined” and “None” to configure.



Work As ● DHCP Client ○ PPPoE Client ○ Static IPv4

DNS Server Configuration

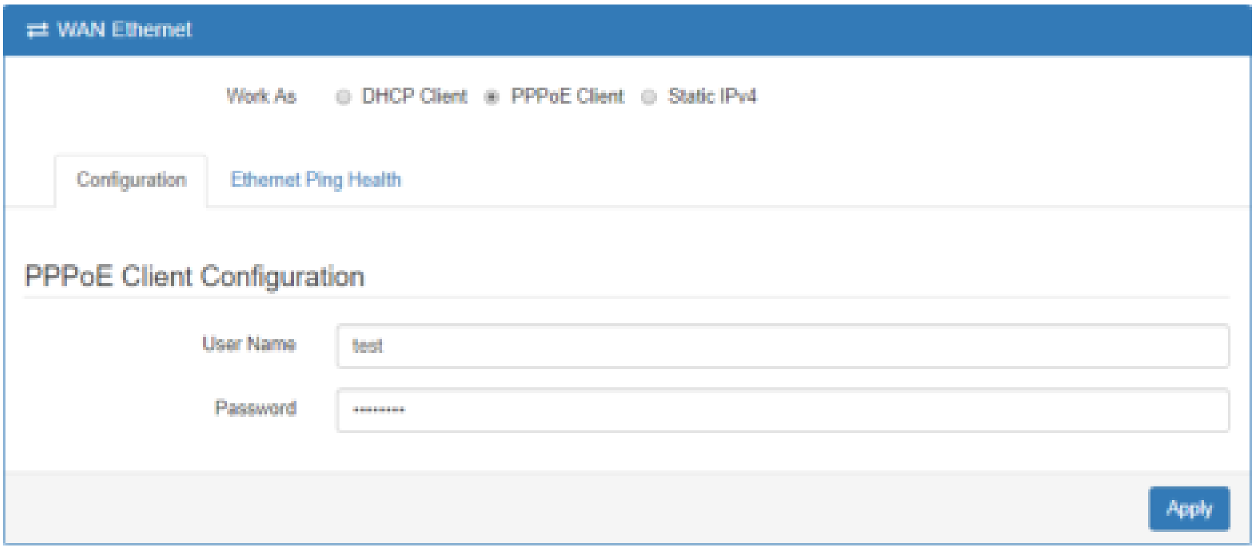
IPv4 DNS Server #1: From ISP

IPv4 DNS Server #2

IPv4 DNS Server #3: From ISP

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.



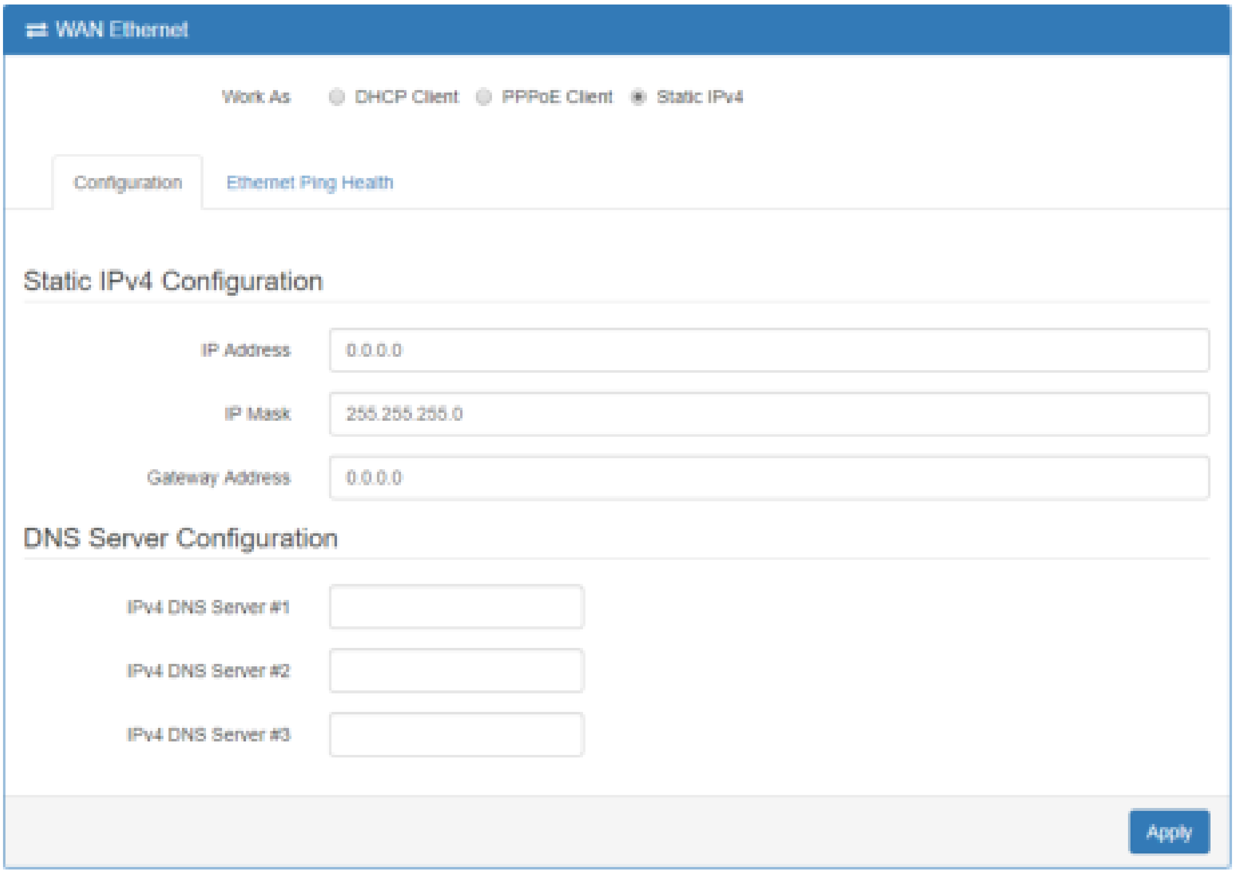
Work As ○ DHCP Client ● PPPoE Client ○ Static IPv4

PPPoE Client Configuration

User Name: test

Password: ••••••••

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



Work As ○ DHCP Client ○ PPPoE Client ● Static IPv4

Static IPv4 Configuration

IP Address 0.0.0.0

IP Mask 255.255.255.0

Gateway Address 0.0.0.0

DNS Server Configuration

IPv4 DNS Server #1

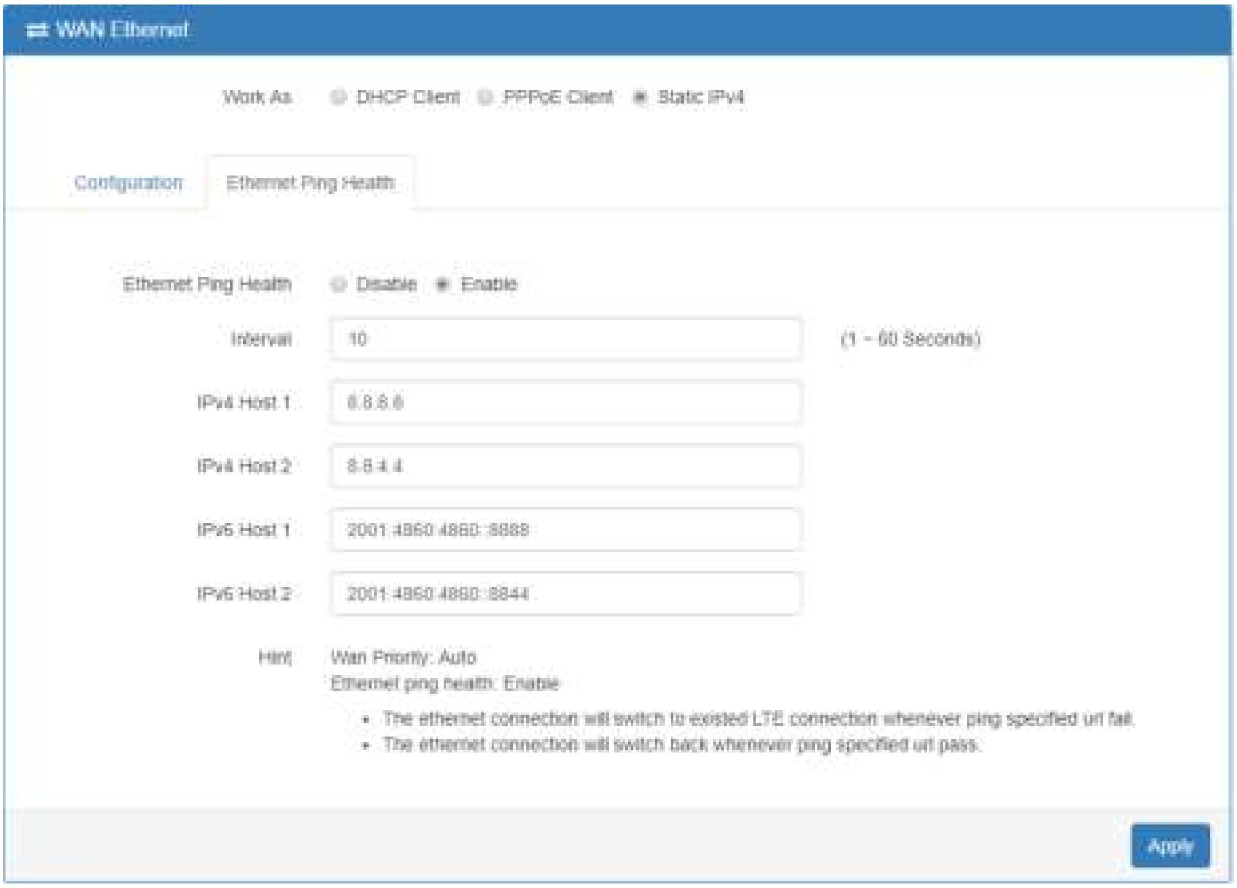
IPv4 DNS Server #2

IPv4 DNS Server #3

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.

6.2.2 Ethernet Ping Health

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



WAN Ethernet

Work As ○ DHCP Client ○ PPPoE Client ● Static IPv4

Configuration | Ethernet Ping Health

Ethernet Ping Health ○ Disable ● Enable

Interval: 10 (1 ~ 60 Seconds)

IPv4 Host 1: 8.8.8.8

IPv4 Host 2: 8.8.4.4

IPv6 Host 1: 2001:4860:4860::8888

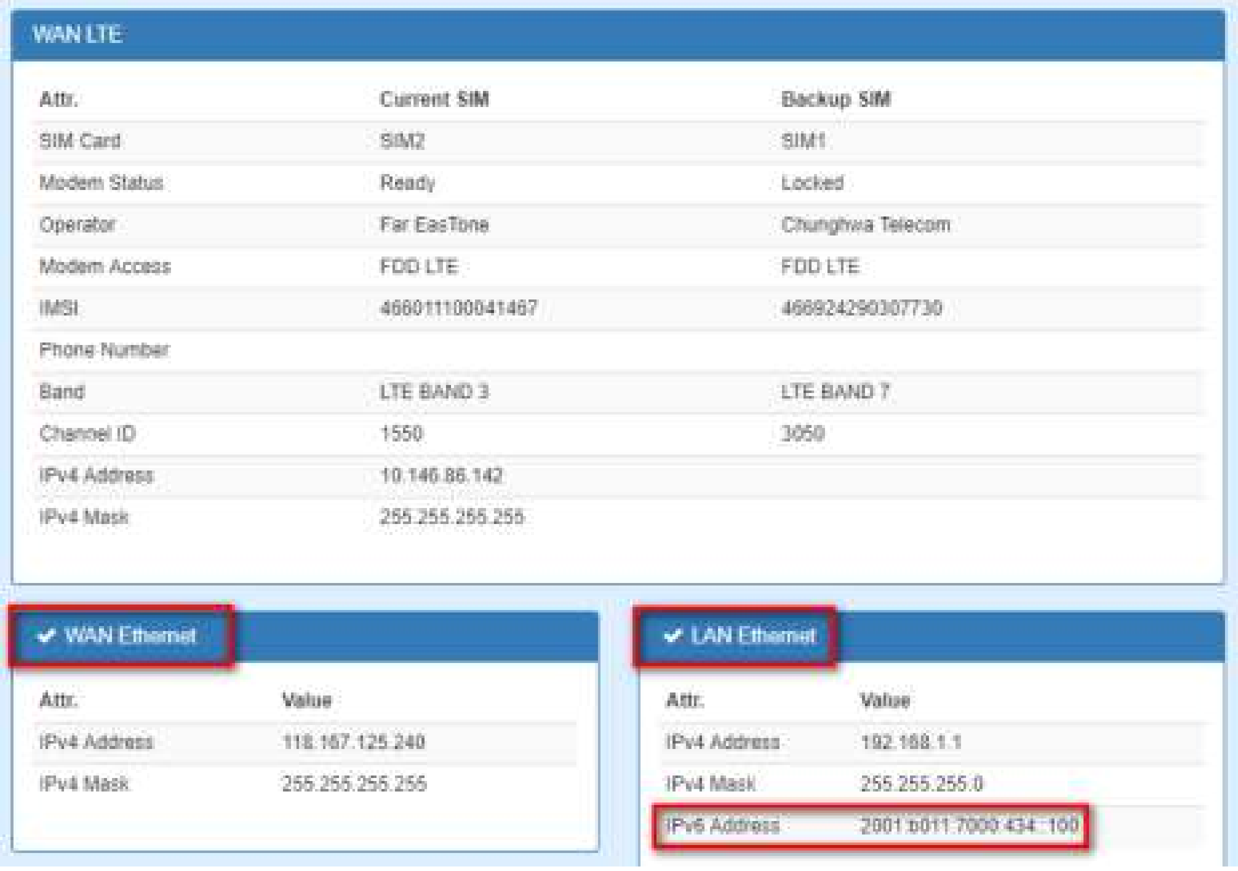
IPv6 Host 2: 2001:4860:4860::8844

Hint: Wan Priority: Auto
Ethernet ping health: Enable

- The ethernet connection will switch to existed LTE connection whenever ping specified url fail.
- The ethernet connection will switch back whenever ping specified url pass.

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

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



WAN LTE

Attr.	Current SIM	Backup SIM
SIM Card	SIM2	SIM1
Modem Status	Ready	Locked
Operator	Far EasTone	Chunghwa Telecom
Modem Access	FDD LTE	FDD LTE
IMSI	466011100041467	466924290307730
Phone Number		
Band	LTE BAND 3	LTE BAND 7
Channel ID	1550	3050
IPv4 Address	10.146.86.142	
IPv4 Mask	255.255.255.255	

✓ WAN Ethernet

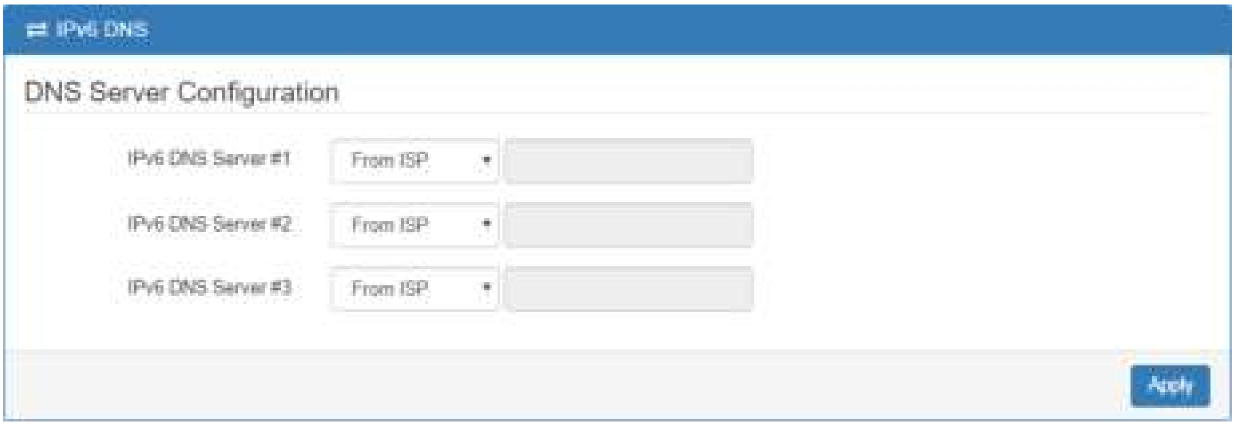
Attr.	Value
IPv4 Address	118.167.125.240
IPv4 Mask	255.255.255.255

✓ LAN Ethernet

Attr.	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	2001:b011:7000:434::100

6.3 WAN > IPv6 DNS

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



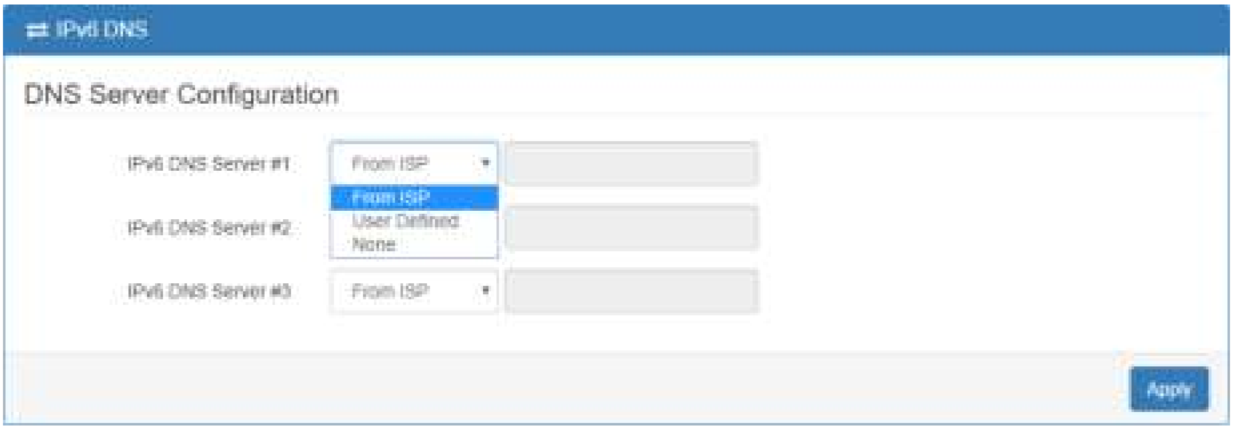
DNS Server Configuration

IPv6 DNS Server #1 From ISP

IPv6 DNS Server #2 From ISP

IPv6 DNS Server #3 From ISP

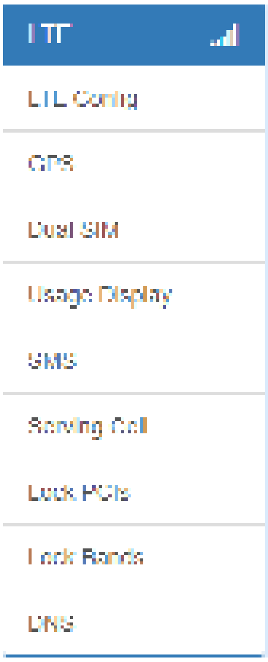
For IPv6 DNS Server, it provides three options to set up and each option has provided with “From ISP”, “User Defined” and “None” to configure.



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

7 Configuration > LTE

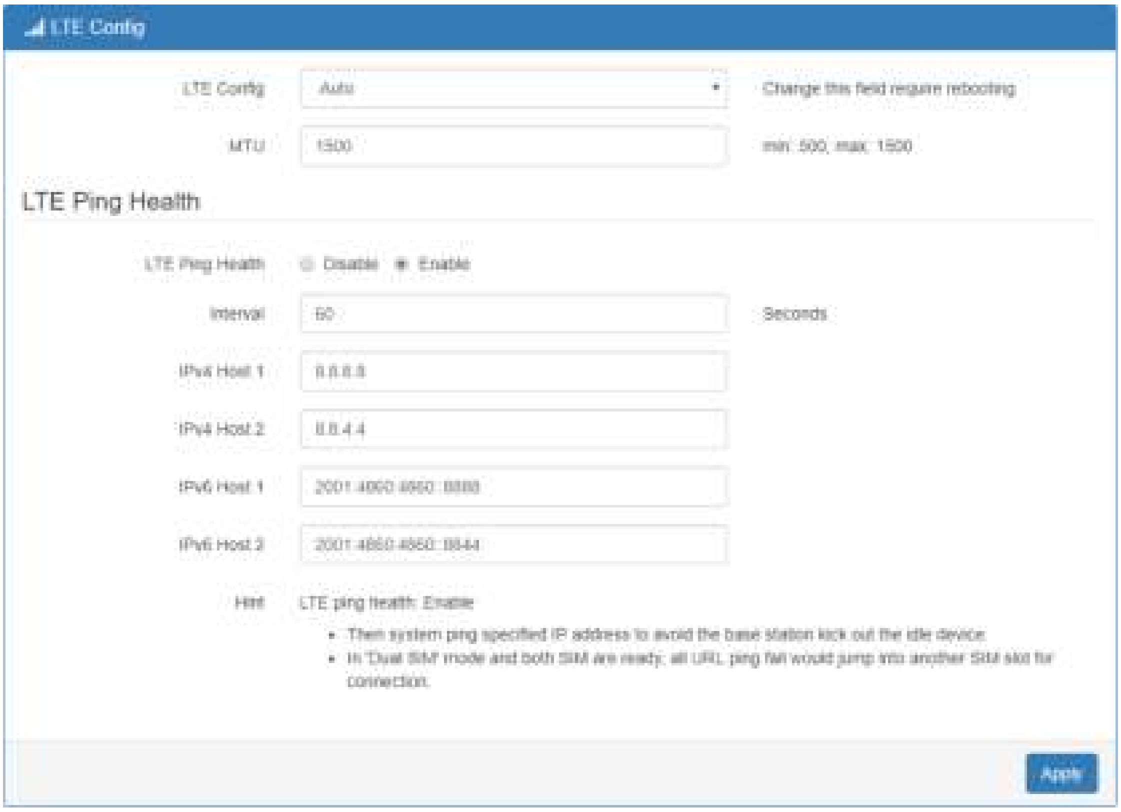
This section allows you to configure LTE Config, GPS Config, Dual SIM, Usage Display, SMS, Engineer Info, and DNS.



7.1 LTE > LTE Config

7.1.1 LTE Configuration

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



LTE Config

LTE Config: Auto — Change this field require rebooting

MTU: 1500 — min: 500, max: 1500

LTE Ping Health

LTE Ping Health: ○ Disable ● Enable

Interval: 60 Seconds

IPv4 Host 1: 8.8.8.8

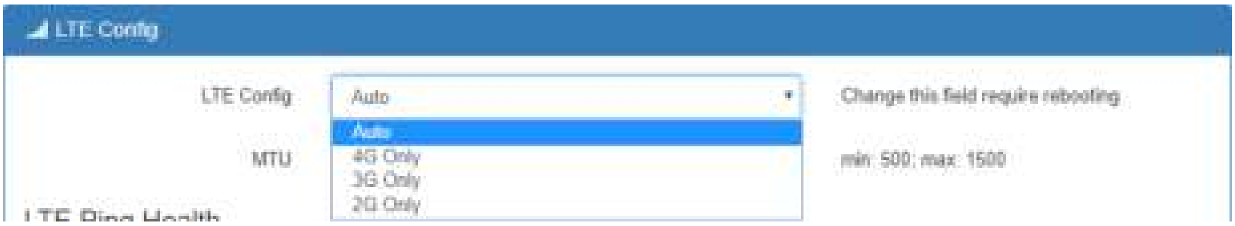
IPv4 Host 2: 8.8.4.4

IPv6 Host 1: 2001:4860:4860::8888

IPv6 Host 2: 2001:4860:4860::8844

Hint: LTE ping health: Enable

- Then system ping specified IP address to avoid the base station kick out the idle device.
- In 'Dual SIM' mode and both SIM are ready, all URL ping fail would jump into another SIM slot for connection.



LTE Config: Auto

Change this field require rebooting

MTU

min: 500; max: 1500

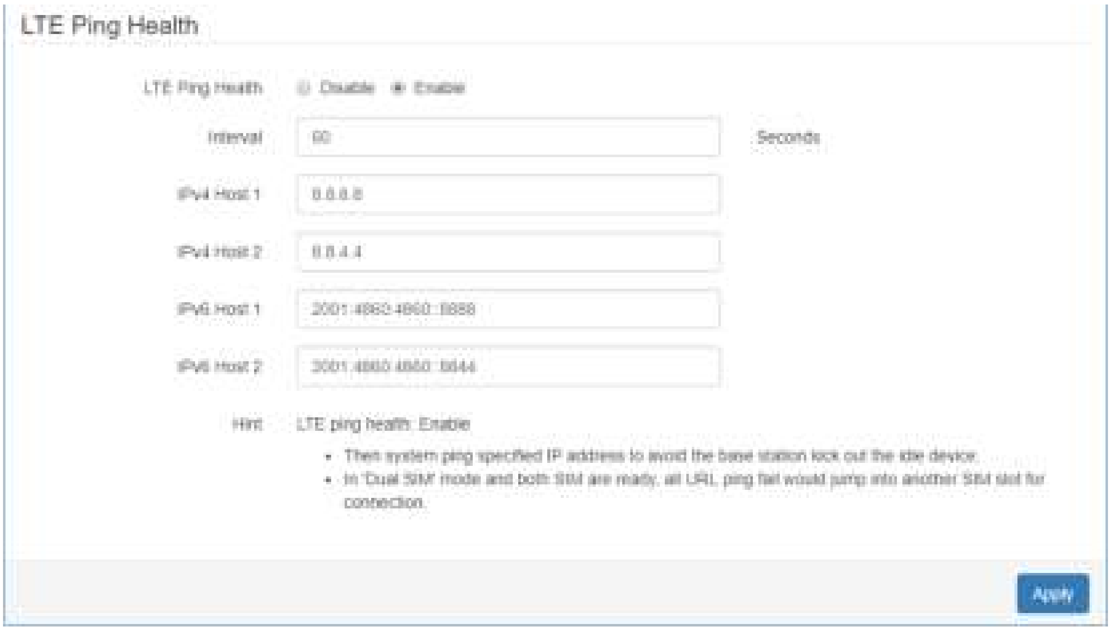
LTE Ping Health

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.

7.1.2 LTE Ping Health

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

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



LTE Ping Health

LTE Ping Health: ○ Disable ● Enable

Interval: 60 Seconds

IPv4 Host 1: 8.8.8.8

IPv4 Host 2: 8.8.4.4

IPv6 Host 1: 2001:4860:4860::8888

IPv6 Host 2: 2001:4860:4860::8844

Hint: LTE ping health: Enable

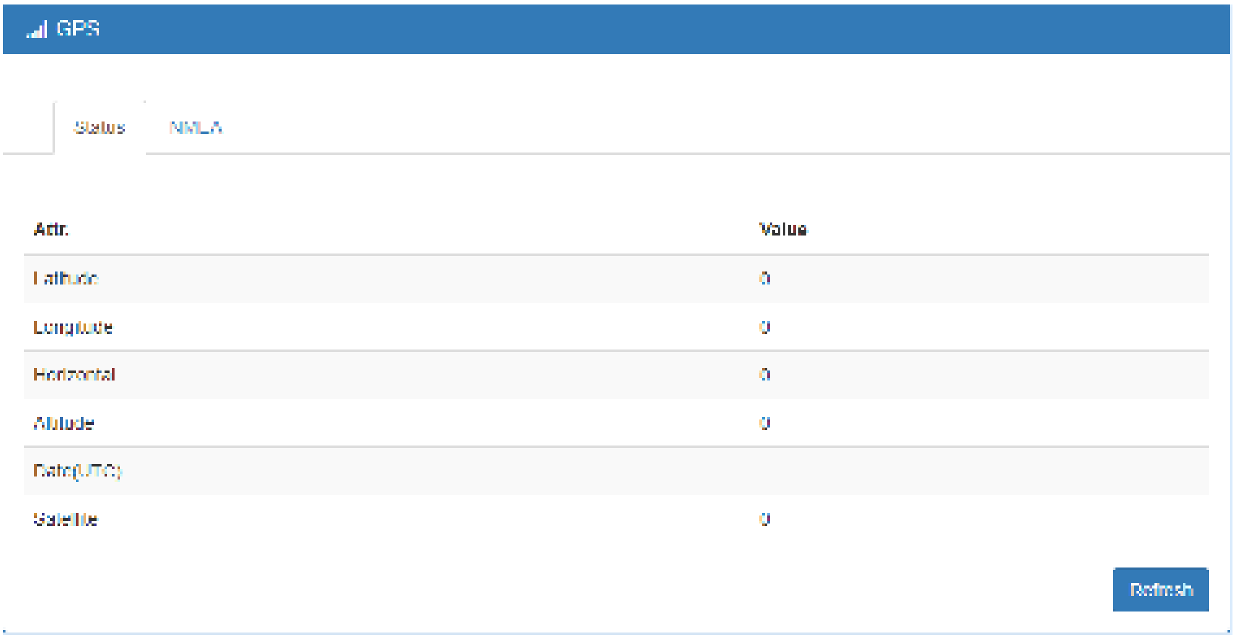
- Then system ping specified IP address to avoid the base station lock out the idle device.
- In 'Dual SIM' mode and both SIM are ready, all URL ping fail would jump into another SIM slot for connection.

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

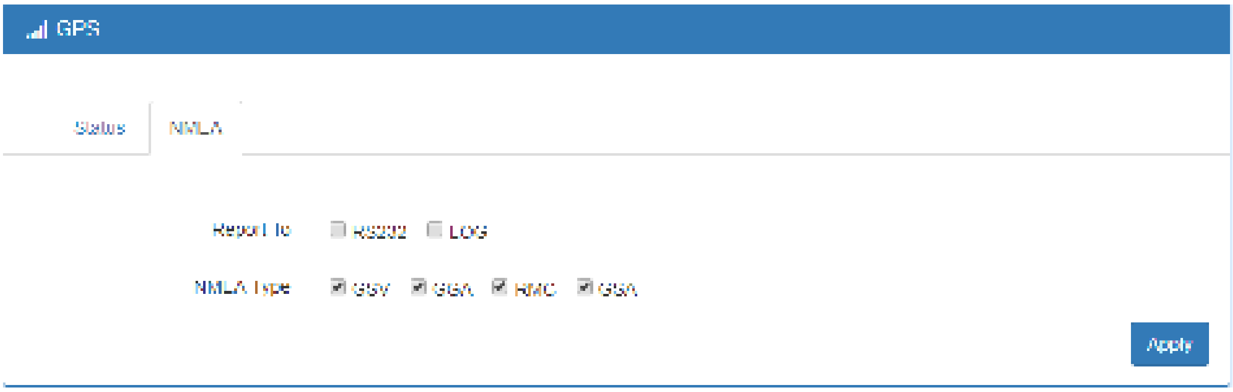
IPv4 Host 2	Input the address of IPv4 Host 2.
IPv6 Host 1	Input the address of IPv6 Host 1.
IPv6 Host 2	Input the address of IPv6 Host 2.
Hint	Show the usage descriptions.

7.2 LTE > GPS

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



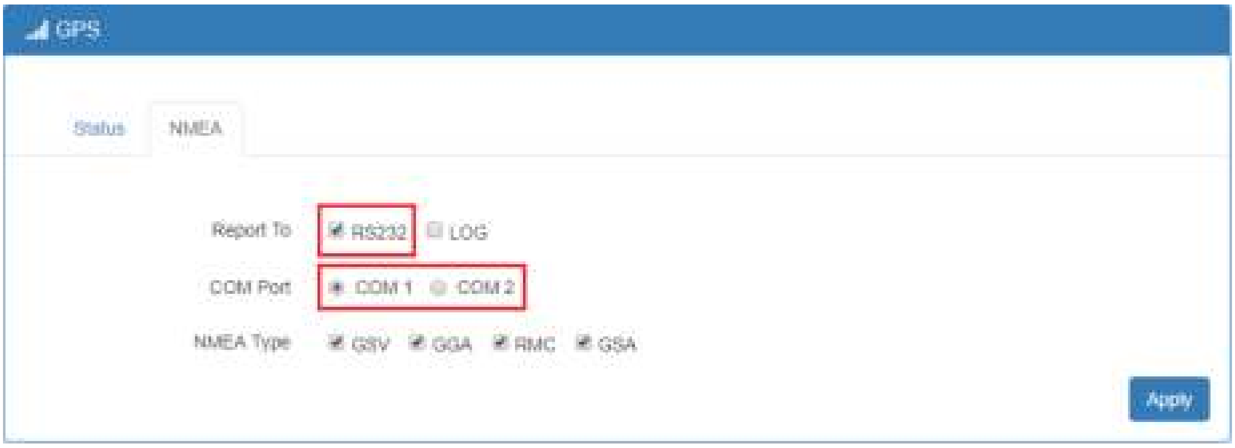
Attr.	Value
Latitude	0
Longitude	0
Horizontal	0
Altitude	0
Date(UTC)	
Satellite	0



Report To ☐ RS232 ☐ LOG

NMEA Type ☑ GSV ☑ GGA ☑ RMC ☑ GSA

Note: You have to select **RS232** item and the interface shows the options of COM Port.



GPS

Status | NMEA

Report To ☑ RS232 □ LOG

COM Port ● COM 1 ○ COM 2

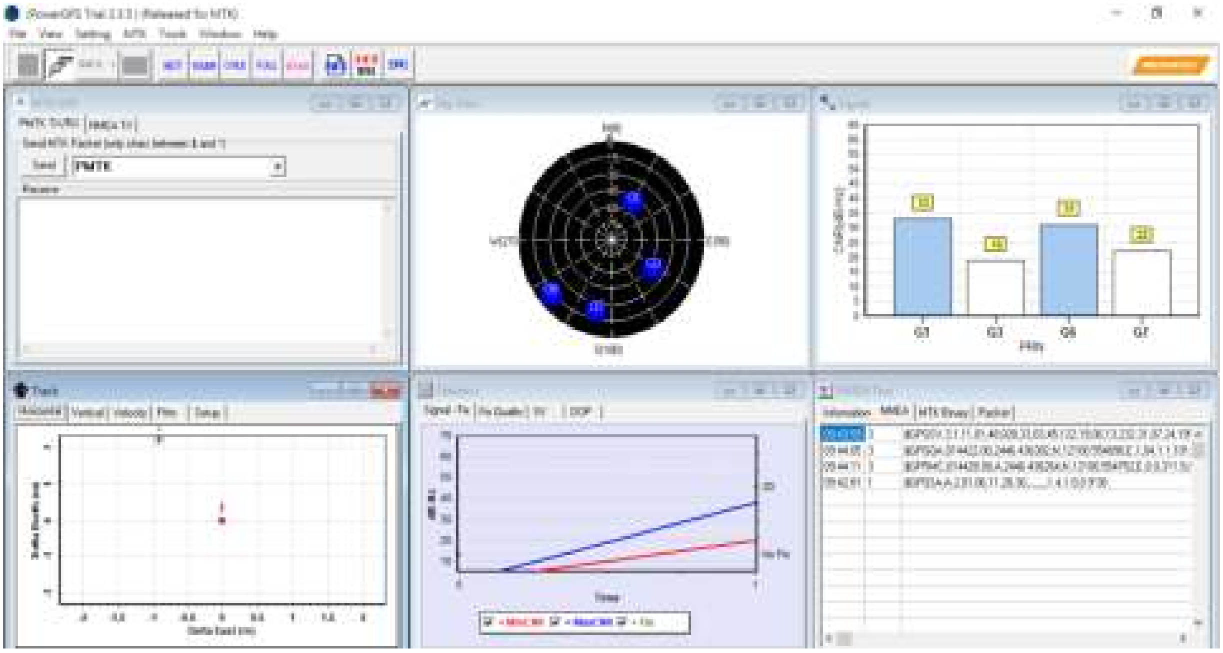
NMEA Type ☑ GSV ☑ GGA ☑ RMC ☑ GSA

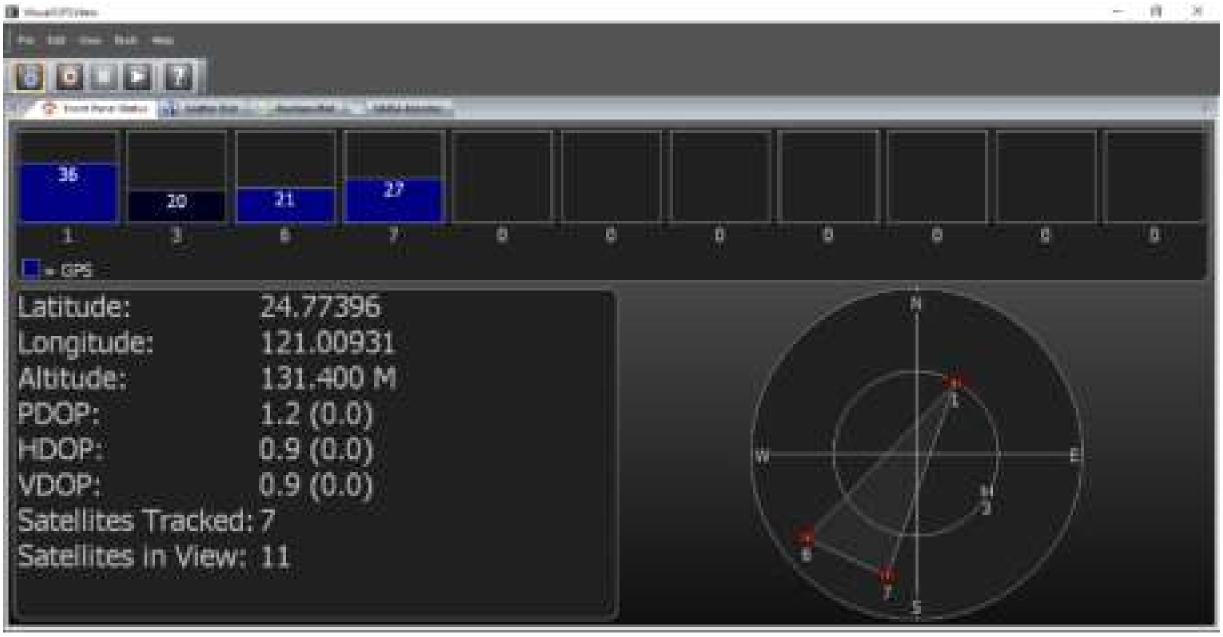
Apply

You can download software from internet and activate the GPS Configuration to display what information you need from your software.

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

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

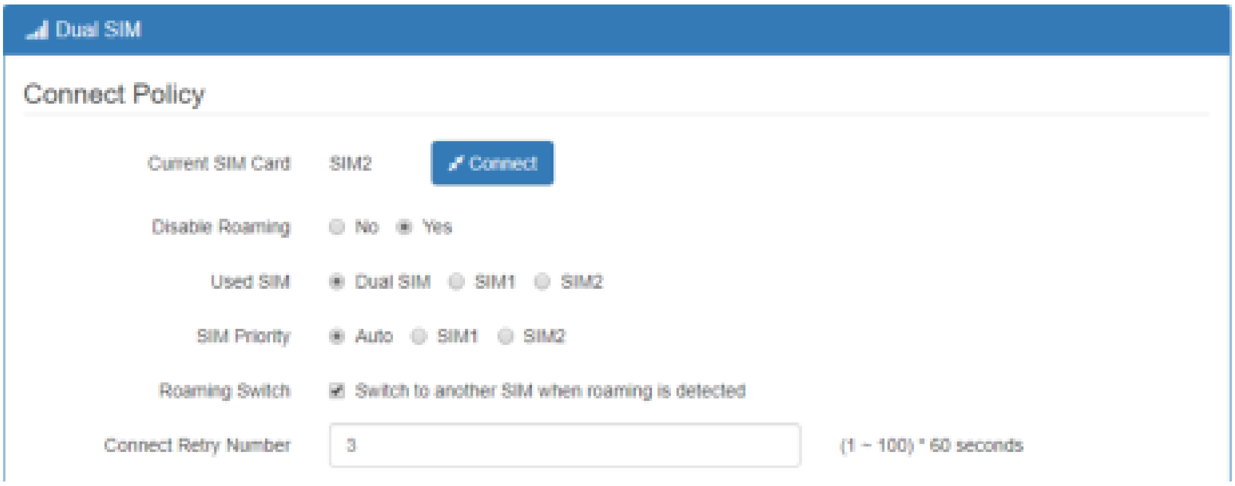




Latitude: 24.77396
Longitude: 121.00931
Altitude: 131.400 M
PDOP: 1.2 (0.0)
HDOP: 0.9 (0.0)
VDOP: 0.9 (0.0)
Satellites Tracked: 7
Satellites in View: 11

7.3 LTE > Dual SIM

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



Dual SIM

Connect Policy

Current SIM Card: SIM2 [Connect]

Disable Roaming: ○ No ● Yes

Used SIM: ● Dual SIM ○ SIM1 ○ SIM2

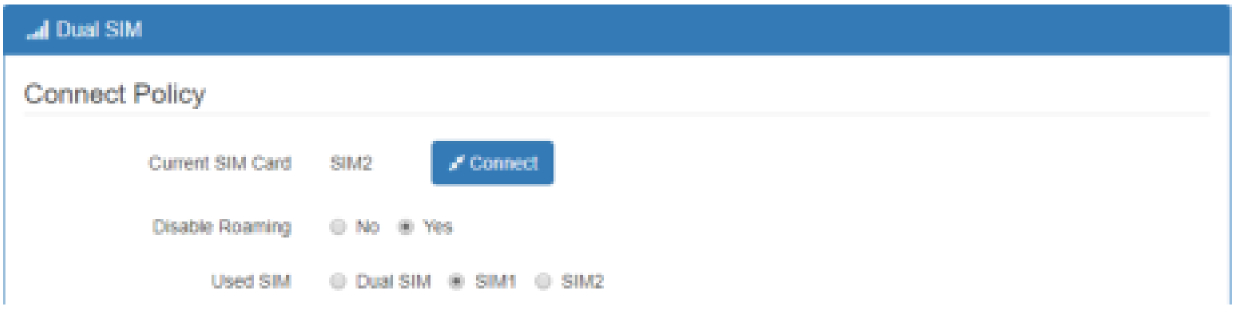
SIM Priority: ● Auto ○ SIM1 ○ SIM2

Roaming Switch: ☑ Switch to another SIM when roaming is detected

Connect Retry Number: 3 (1 ~ 100) * 60 seconds

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

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



Dual SIM

Connect Policy

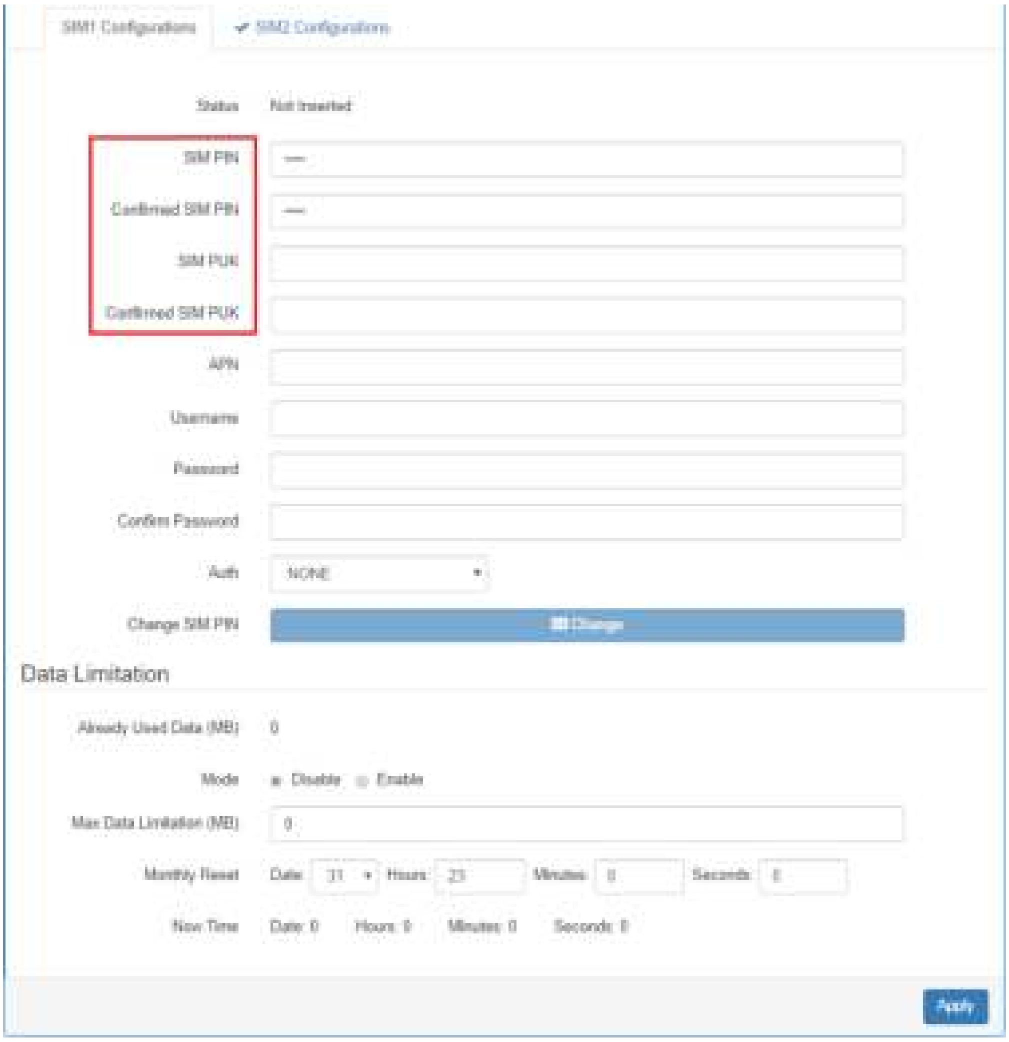
Current SIM Card SIM2

Disable Roaming ○ No ● Yes

Used SIM ○ Dual SIM ● SIM1 ○ SIM2

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

- **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.



Status Not Inserted

SIM PIN ----

Confirmed SIM PIN ----

SIM PUK

Confirmed SIM PUK

APN

Username

Password

Confirm Password

Auth NONE

Change SIM PIN

Data Limitation

Already Used Data (MB) 0

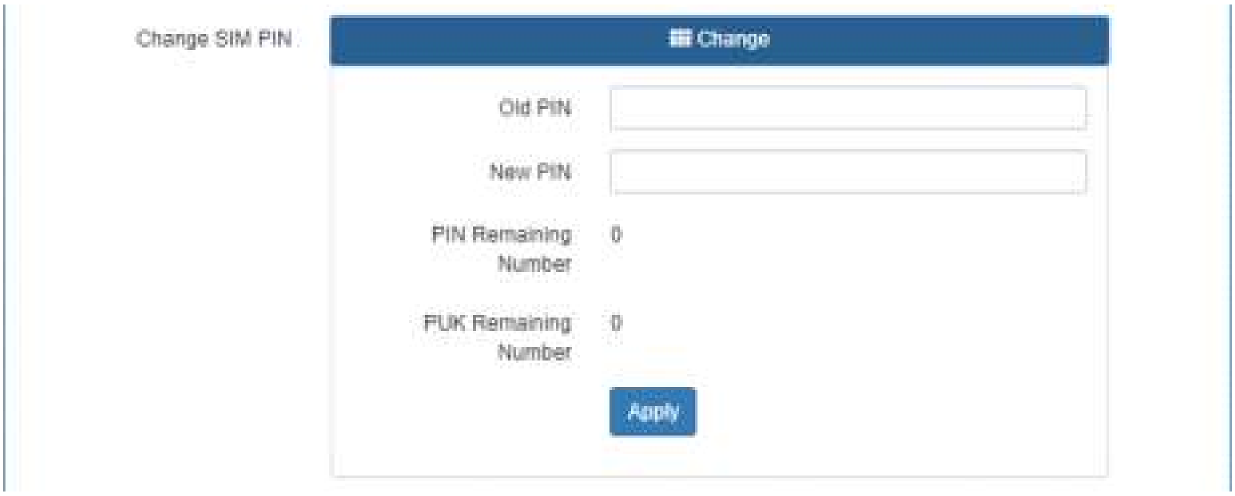
Mode ● Disable ○ Enable

Max Data Limitation (MB) 0

Monthly Reset Date 31 Hours 23 Minutes 0 Seconds 0

Now Time Date: 0 Hours: 0 Minutes: 0 Seconds: 0

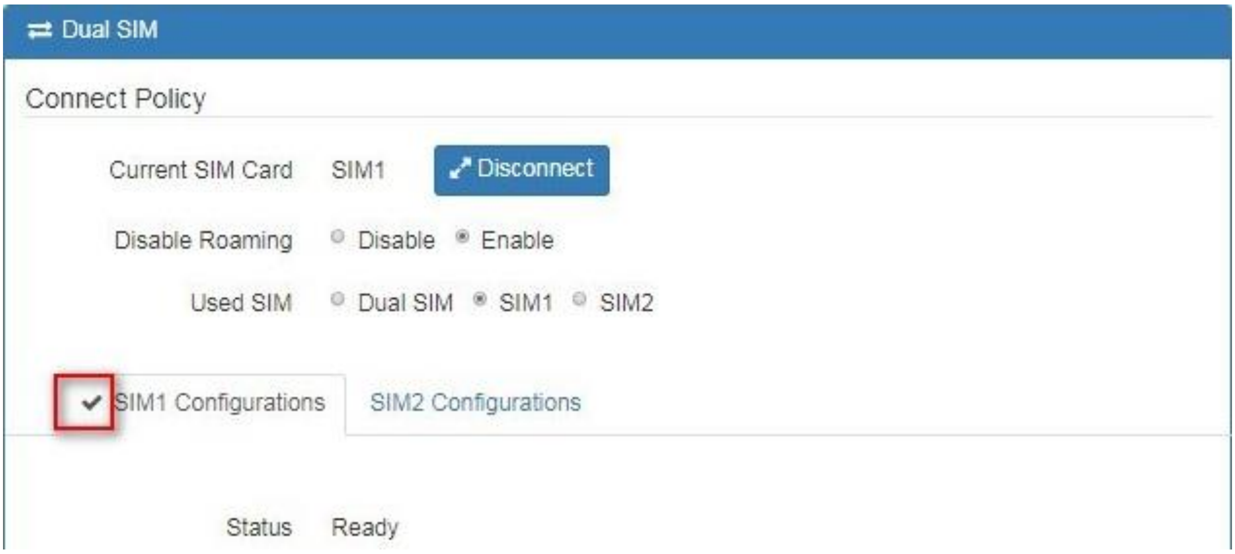
- **Change SIM PIN：** If you want to change SIM PIN code, you can click Change button and type old SIM PIN code and new SIM PIN code. Please aware not to exceed the retry number (PIN remaining number and PUN remaining number).



Change SIM PIN
Change
Old PIN
New PIN
PIN Remaining Number 0
PUK Remaining Number 0

Note:

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



Dual SIM

Connect Policy

Current SIM Card SIM1

Disable Roaming ○ Disable ● Enable

Used SIM ○ Dual SIM ● SIM1 ○ SIM2

✓ SIM1 Configurations SIM2 Configurations

Status Ready

LTE > Dual SIM	
Item	**Description**
Connect Policy	
Current SIM Card	Display which SIM slot is using.
Status of SIM Card Connectivity	● **Connect:** After manually disconnect, user can only click Connect button to get connection or reboot the device to make it automatically connect. ● **Disconnect:** If there is one SIM slot get connection, the Disconnect button appear. After manually click Disconnect, the system would not automatically get connection until next reboot.
Disable Roaming	● **NO:** Make the connection even the device is in roaming state. ● **YES:** No connection when the device in roaming state.
Used SIM	● **Dual SIM:** Automatically switch SIM card when the current SIM card fail to make connection. ● **SIM1:** Only use SIM1 card slot. ● **SIM2:** Only use SIM2 card slot.
SIM Priority	● **Dual SIM:** Automatically switch SIM card when the current SIM card fail to make connection. ● **SIM1:** Use SIM1 card slot as the first priority for connection. ● **SIM2:** Use SIM2 card slot as the first priority for connection.
Roaming Switch	Switch to another SIM when roaming is detected. System will switch SIM slot when current SIM is in roaming state and another SIM slot is in READY state.
Connect Retry Number	After timeout, the router attempts to switch another SIM Slot. The default timeout is three minutes. This option is only for Dual SIM mode.
SIM1 or SIM2 Configurations	
Status	Display the status of Dual SIM.
SIM PIN	A personal identification number (PIN) for ordinary use to protect your SIM card.
Confirmed SIM PIN	Double confirm SIM PIN.
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.
APN	The Access Point Name (APN) is the name for the settings to set up a connection to the gateway between your carrier's cellular network and the Public Internet. Leave it empty will search internally database automatically by SIM card for connection; however, please notice APN1 and APN2 must be manually configured different setting while concurrently use.
Username	The username can be input by user or the system will search from internal database if the username is blank.

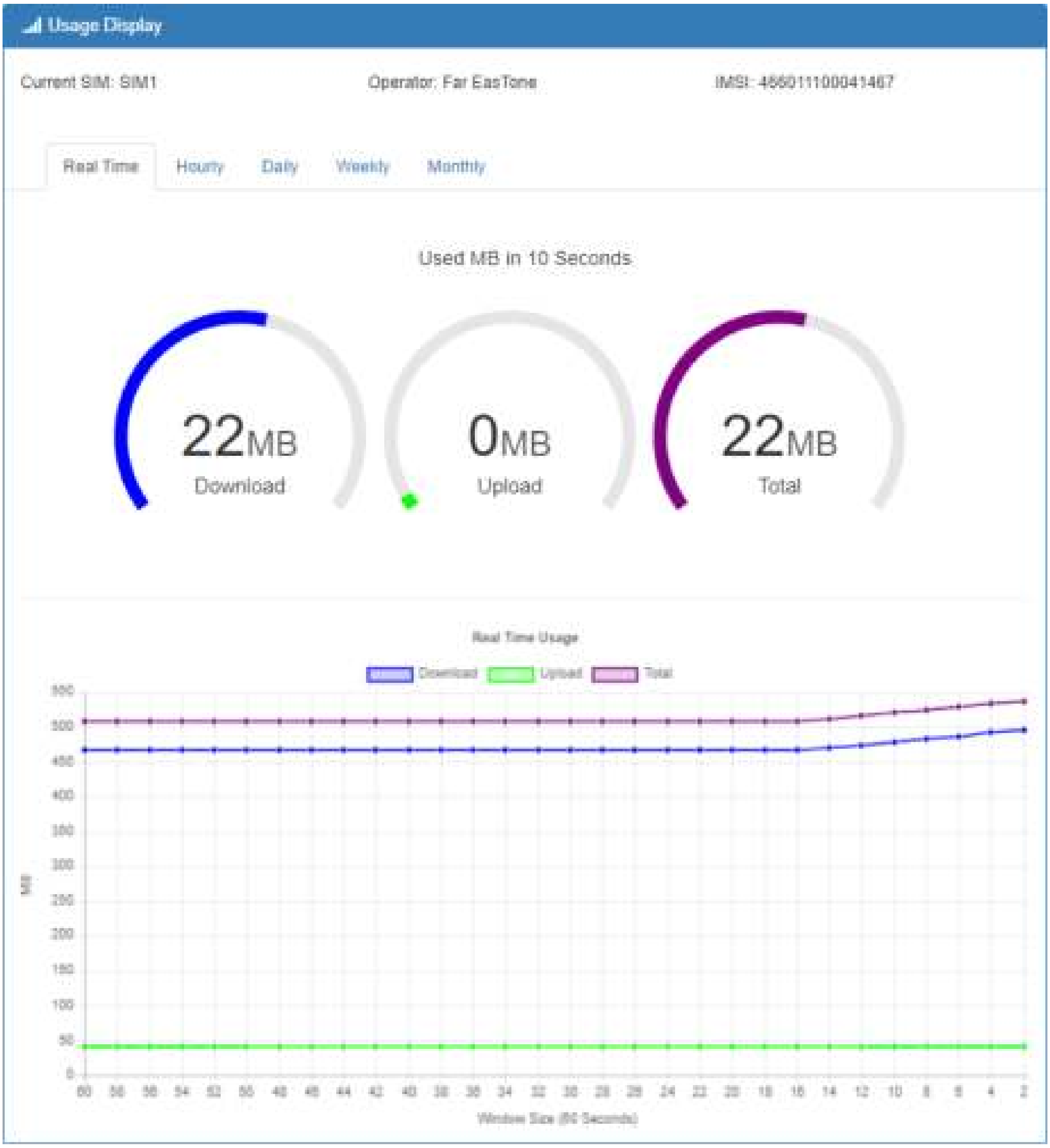
Password	The password can be input by user or the system will search from internal database if the password is blank.
Confirm Password	Double confirm password.
Auth (NONE/PAP/CHAP)	Configure Authentication mode with three modes, including NONE, PAP, and CHAP. If Auth mode is not None, most servers require username and password above.
Change SIM PIN	When you change the SIN PIN, 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 code.
PIN remaining number	Display the allowed remaining PIN code retry number.
PUK remaining number	Display the allowed remaining PUK code retry number.
Data Limitation	
Mode	Turn on/off the Data Limitation to disable or enable.
Already Used Data (MB)	Display current used throughput since last reset.
Max Data Limitation (MB)	Configure max throughput.
Monthly Reset	Set up the reset time during the month.
Now Time	Show the current time of system.

7.4 LTE > Usage Display

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

(1) Real-Time Usage:

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



Usage Display

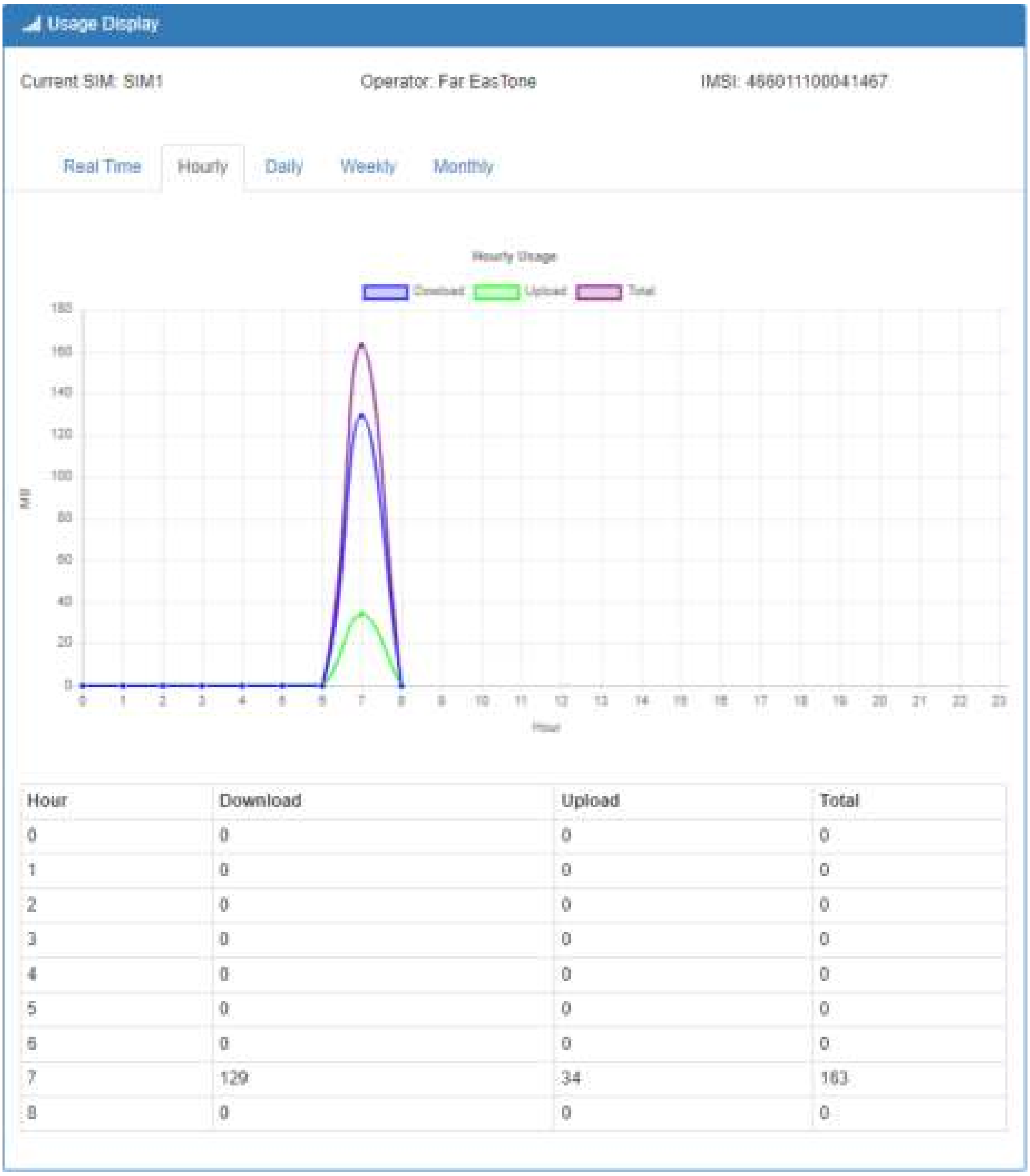
Current SIM: SIM1

Operator: Far EasTone

IMSI: 466011100041467

(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.



Current SIM: SIM1

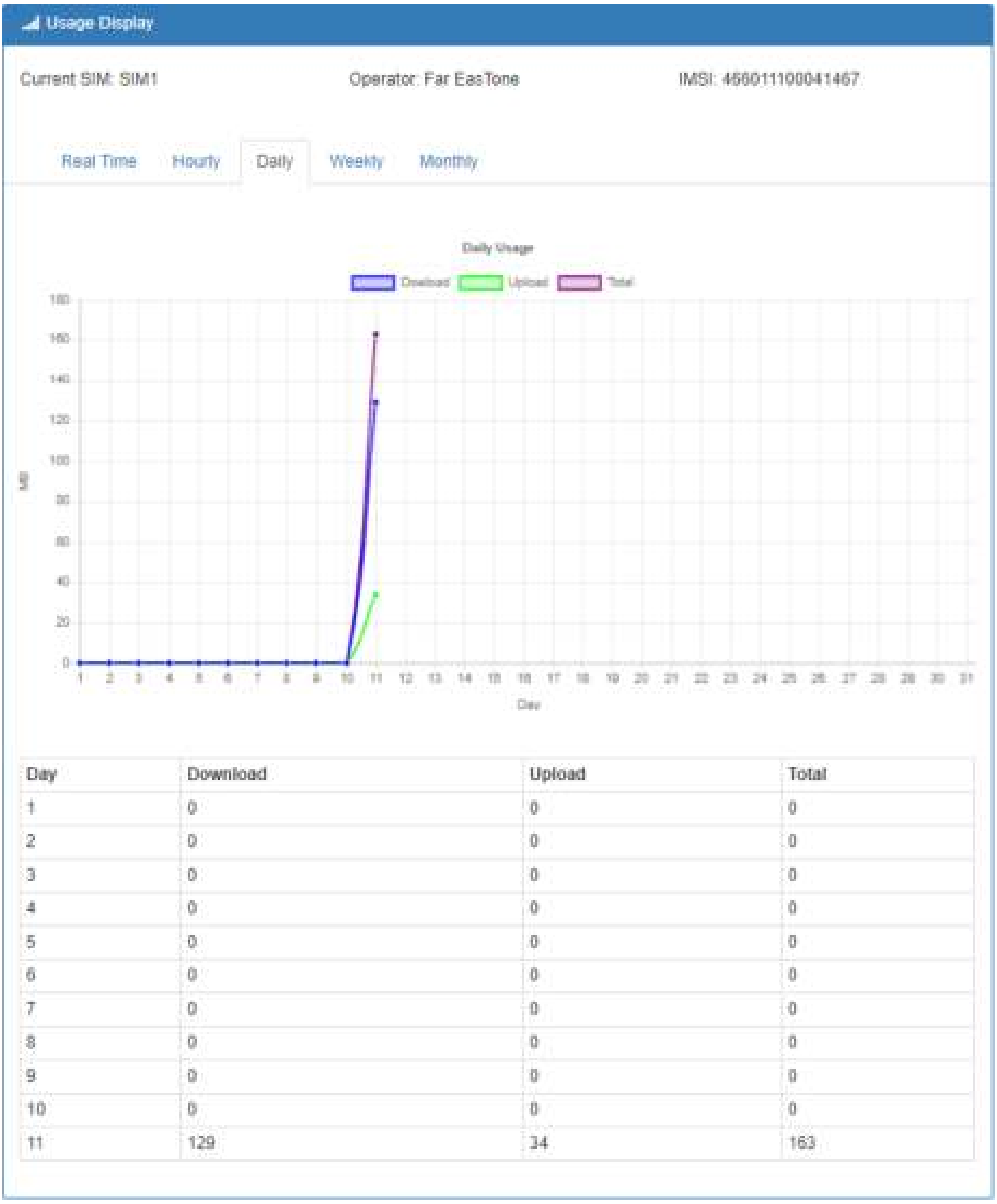
Operator: Far EasTone

IMSI: 466011100041467

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.



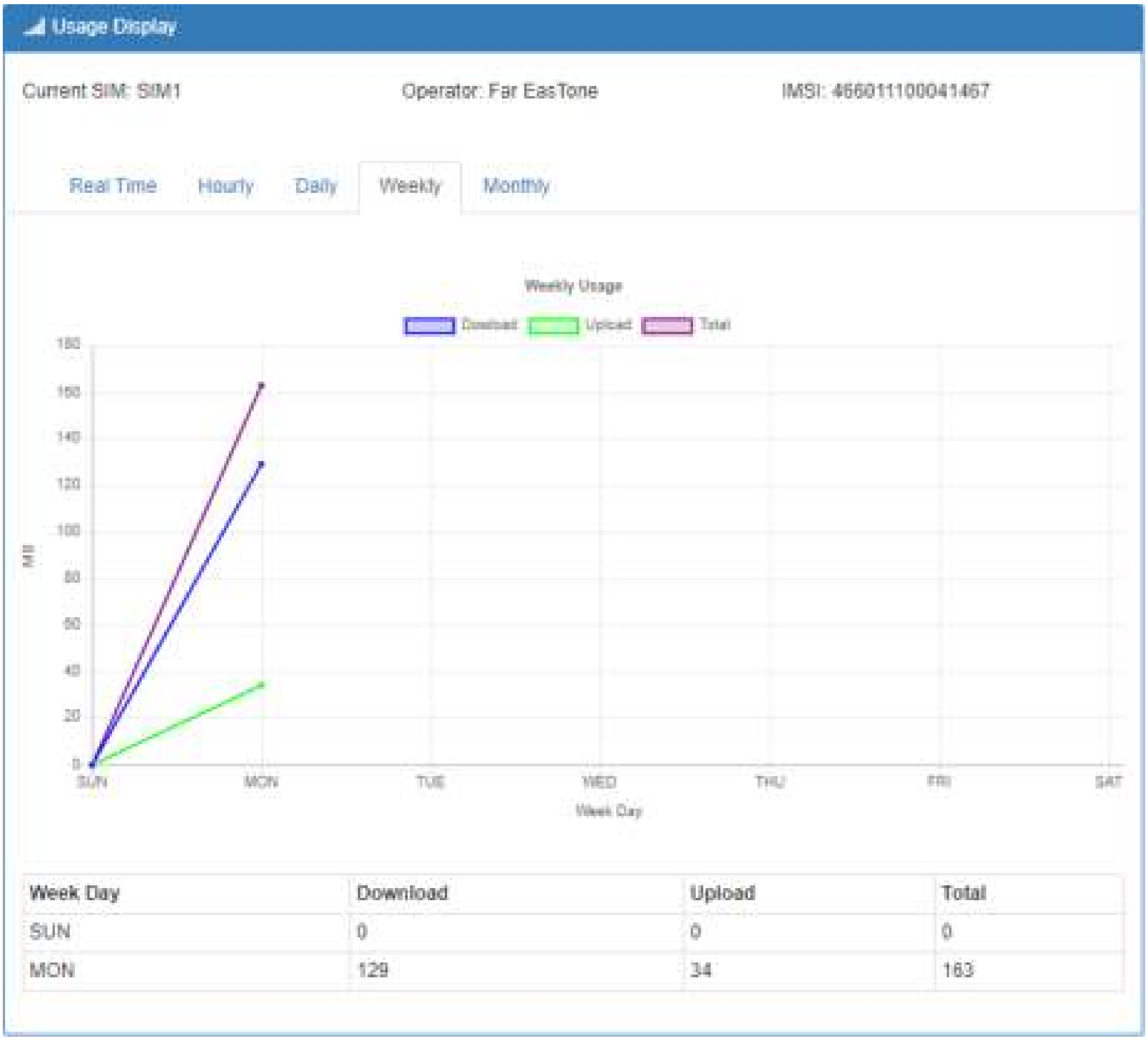
Usage Display

Current SIM: SIM1 Operator: Far EasTone IMSI: 466011100041467

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.



Current SIM: SIM1

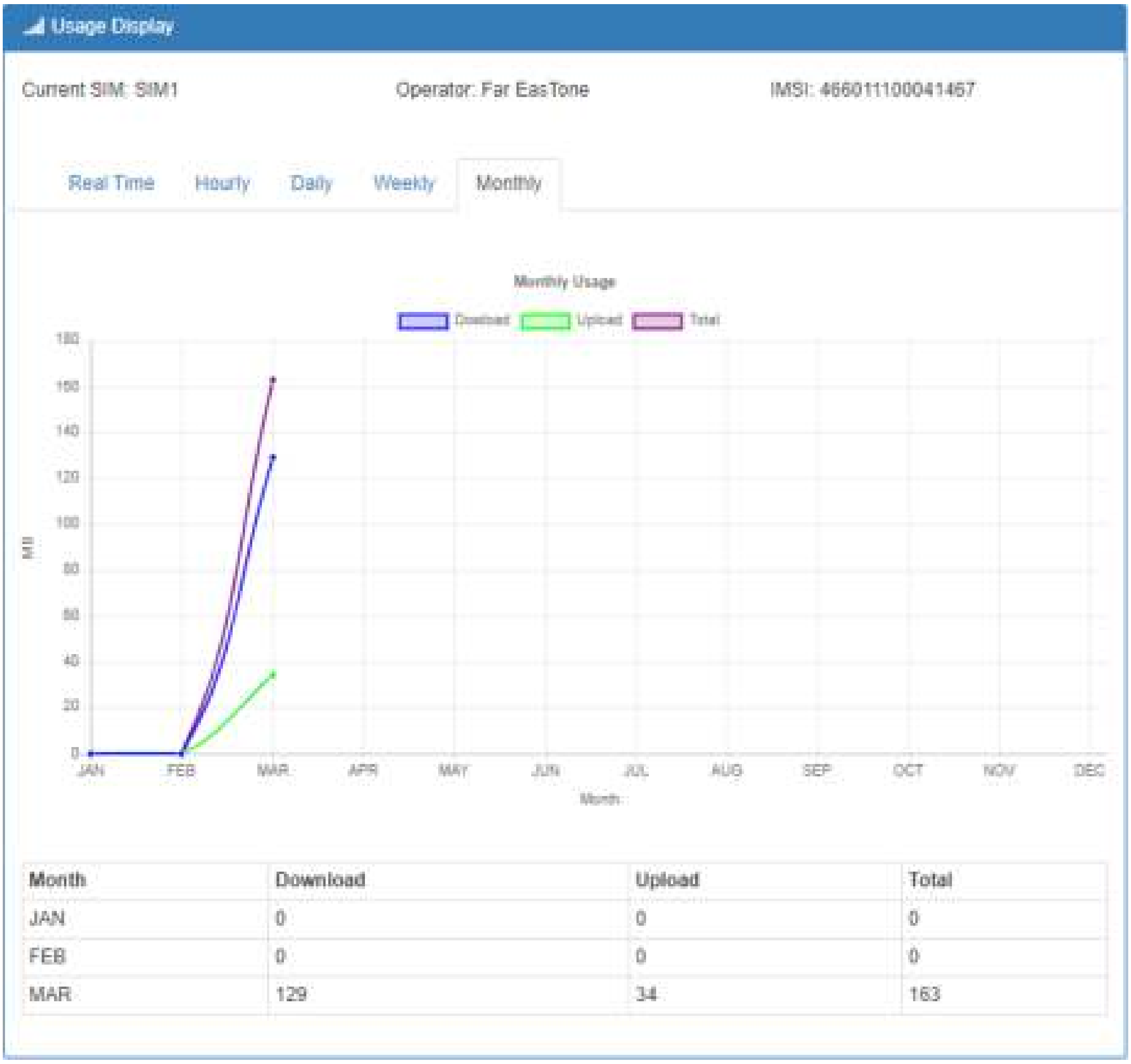
Operator: Far EasTone

IMSI: 466011100041467

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.



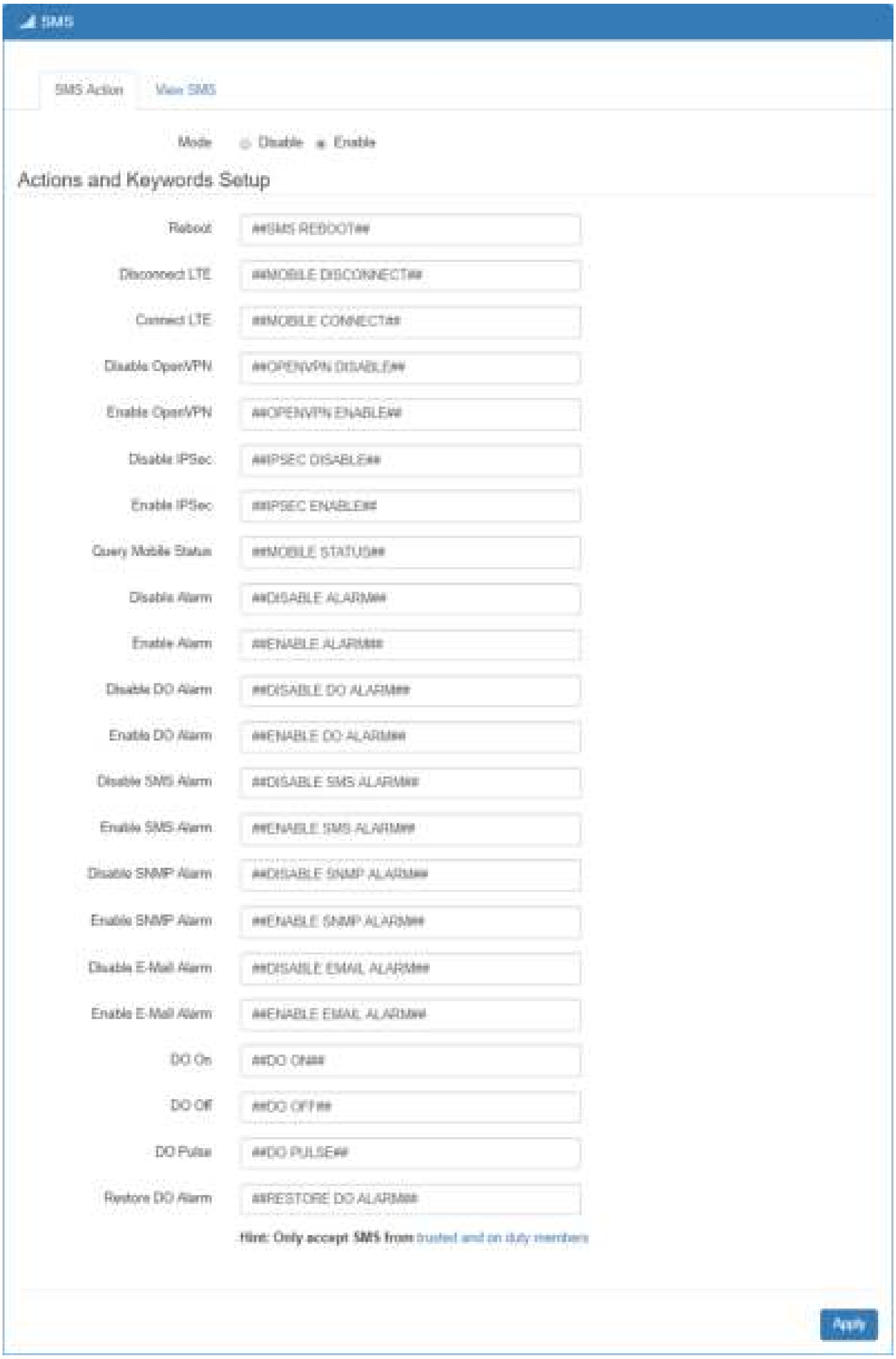
Current SIM: SIM1 Operator: Far EasTone IMSI: 466011100041467

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

7.5 LTE > SMS

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

(1) When enabling **SMS Action**, it allows trust phone number which in **Contacts/On Duty** list by sending key words SMS to trigger device setting/action/query status.



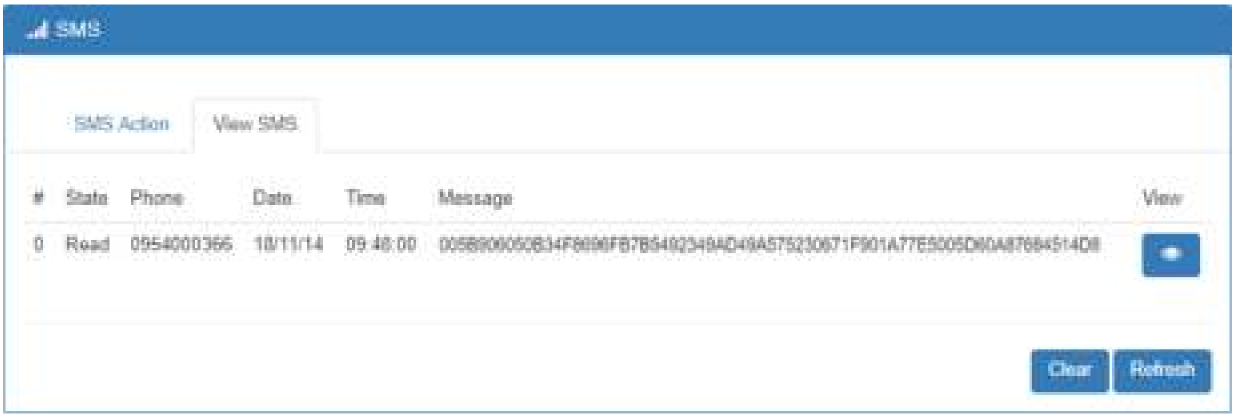
Mode ○ Disable ● Enable

Actions and Keywords Setup

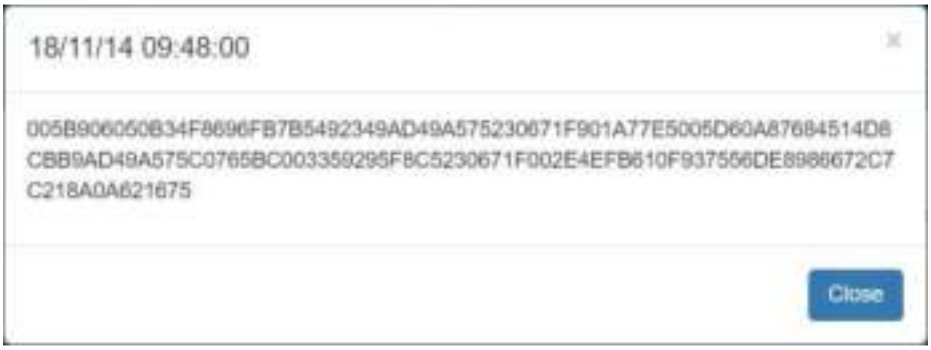
Reboot	##SMS REBOOT##
Disconnect LTE	##MOBILE DISCONNECT##
Connect LTE	##MOBILE CONNECT##
Disable OpenVPN	##OPENVPN DISABLE##
Enable OpenVPN	##OPENVPN ENABLE##
Disable IPSec	##IPSEC DISABLE##
Enable IPSec	##IPSEC ENABLE##
Query Mobile Status	##MOBILE STATUS##
Disable Alarm	##DISABLE ALARM##
Enable Alarm	##ENABLE ALARM##
Disable DO Alarm	##DISABLE DO ALARM##
Enable DO Alarm	##ENABLE DO ALARM##
Disable SMS Alarm	##DISABLE SMS ALARM##
Enable SMS Alarm	##ENABLE SMS ALARM##
Disable SNMP Alarm	##DISABLE SNMP ALARM##
Enable SNMP Alarm	##ENABLE SNMP ALARM##
Disable E-Mail Alarm	##DISABLE EMAIL ALARM##
Enable E-Mail Alarm	##ENABLE EMAIL ALARM##
DO On	##DO ON##
DO Off	##DO OFF##
DO Pulse	##DO PULSE##
Restore DO Alarm	##RESTORE DO ALARM##

Hint: Only accept SMS from trusted and on duty members

(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.



#	State	Phone	Date	Time	Message	View
0	Read	0954000366	18/11/14	09:48:00	005B906050B34F8696FB7B5492349AD49A575230671F901A77E5005D60A87684514D8	👁

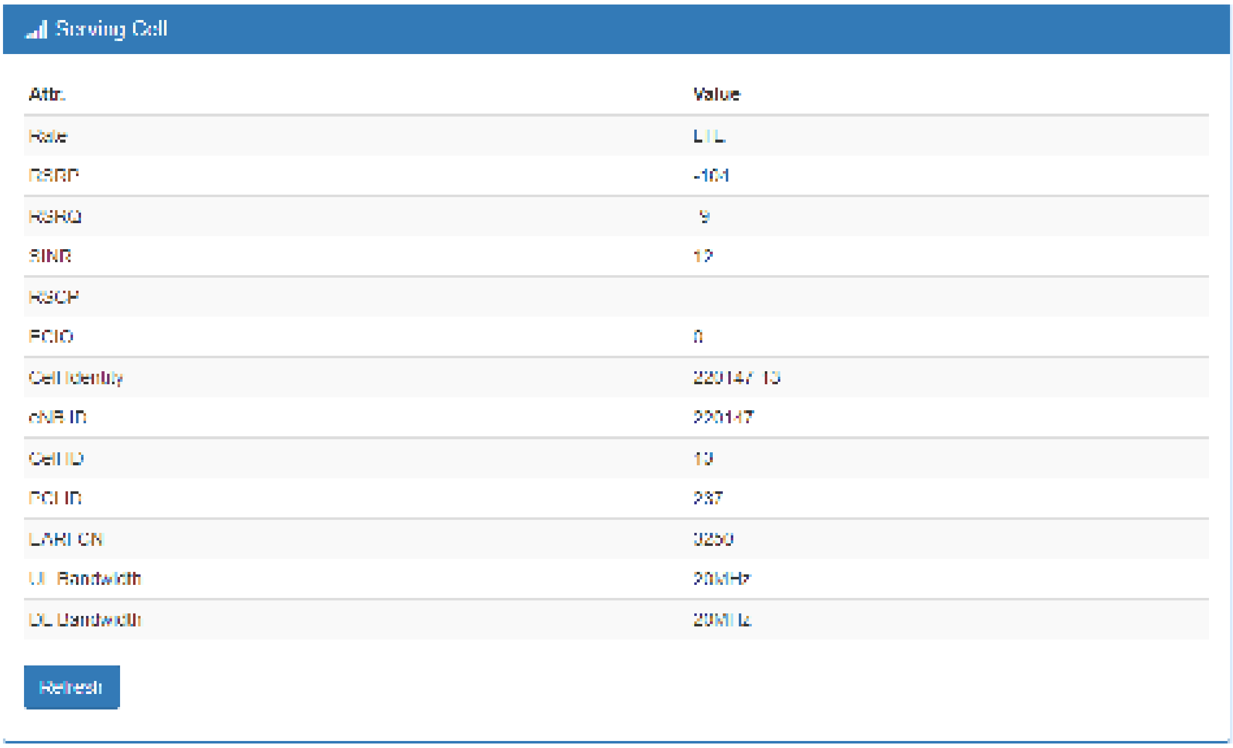


18/11/14 09:48:00

005B906050B34F8696FB7B5492349AD49A575230671F901A77E5005D60A87684514D8
CBB9AD49A575C0765BC003359295F8C5230671F002E4EFB610F937556DE8986672C7
C218A0A621675

7.6 LTE > Serving Cell

This section displays all parameters, including the following items:



Serving Cell

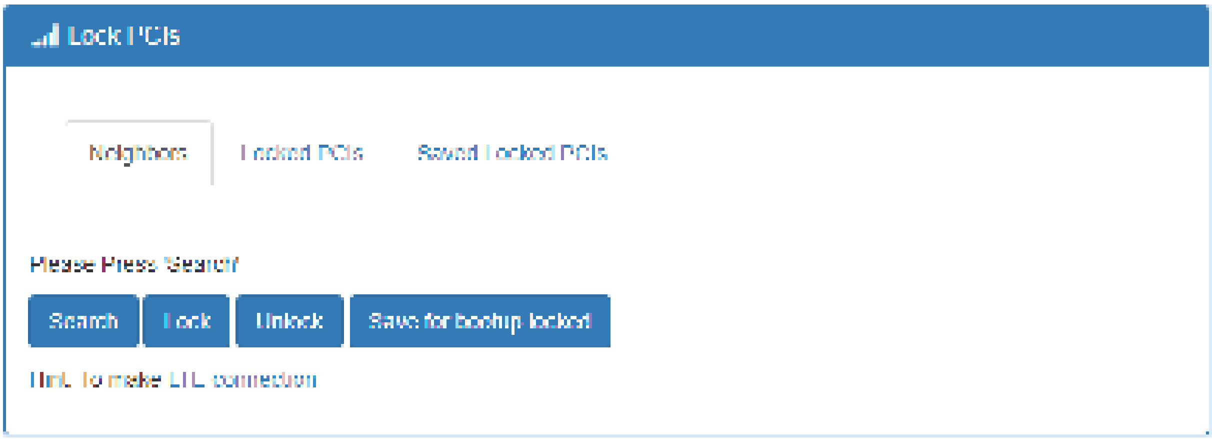
Attr.	Value
Rate	LTE
RSRP	-104
RSRQ	-9
SINR	12
RSCP	
ECIO	0
Cell Identity	220147-13
eNB ID	220147
Cell ID	13
PCI ID	287
EARFCN	3250
UL Bandwidth	20MHz
DL Bandwidth	20MHz

LTE > Serving Cell	
Item	**Description**
RSRP	Reference Signal Received Power.
RSRQ	Reference Signal Received Quality.
SINR	Loarithmic value of SINR.
RSCP	The Received Signal Code Power Level of the cell that was scanned.
ECIO	Carrier to noise ratio in dB = measured Ec/lo 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.

7.7 LTE > Lock PCIs

This section allows you to search neighbors, lock/unlock PCIs and save locked PCIs.

7.7.1 Neighbors



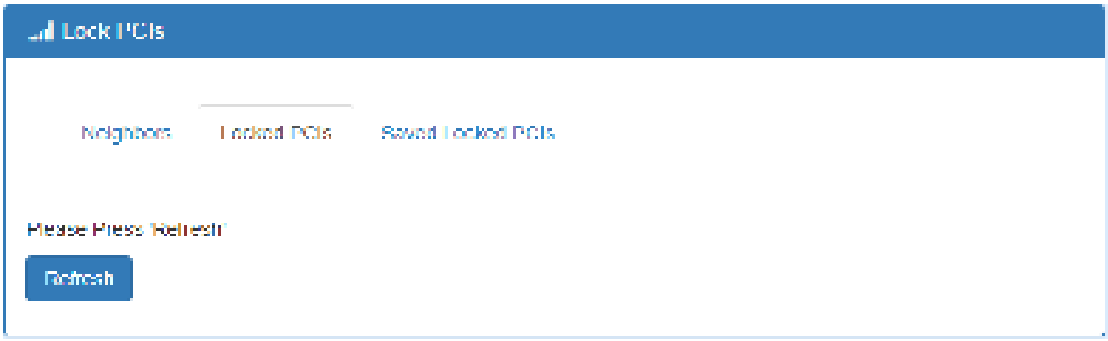
Please Press 'Search'

Hint: To make LTE connection

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

7.7.2 Locked PCIs

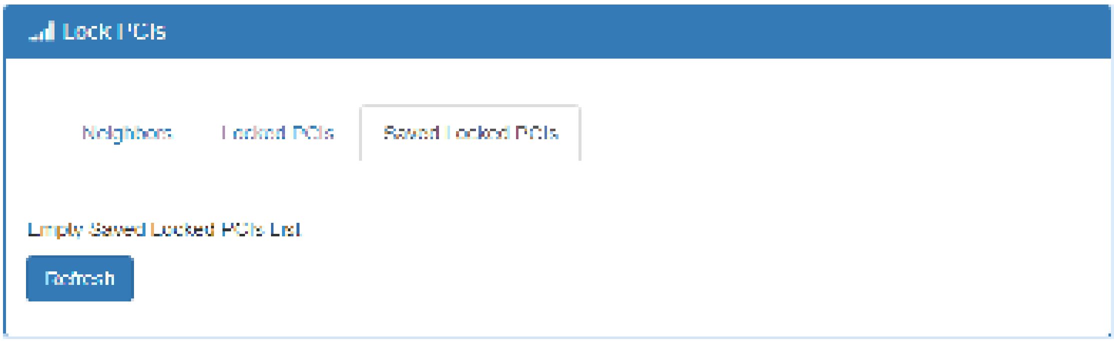
Click Refresh button to get all the most recent locked PCIs (Physical Cell ID) information.



Please Press 'Refresh'

7.7.3 Saved Locked PCIs

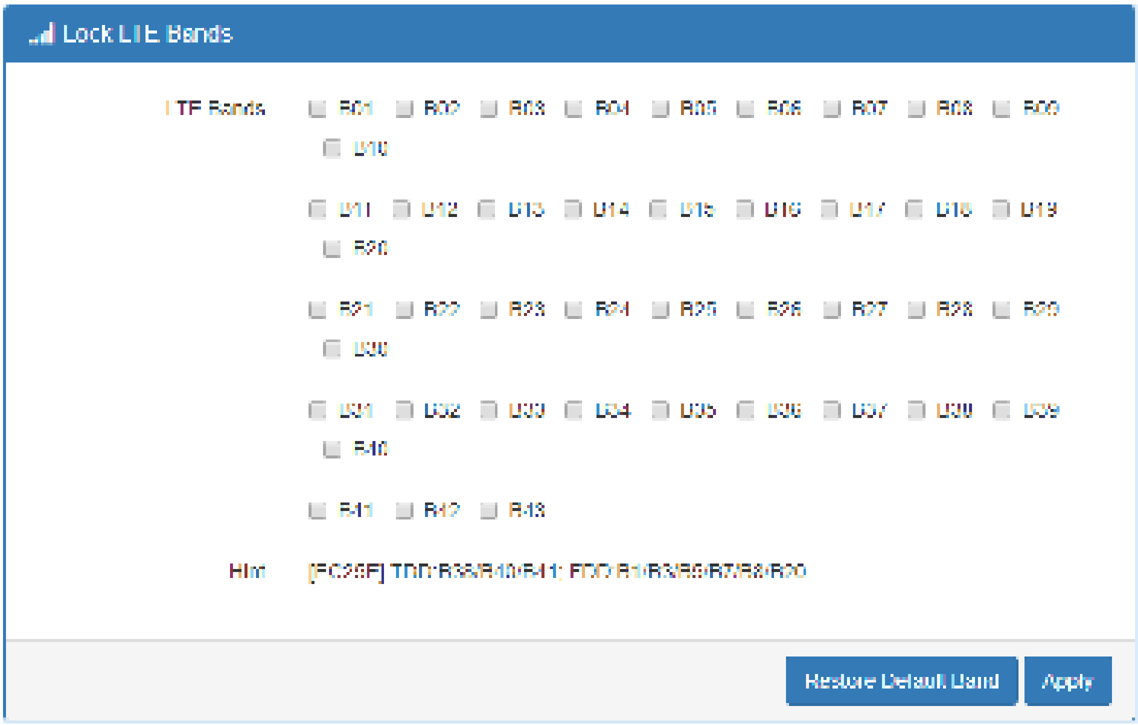
Click Refresh button to get all the most recent saved locked PCIs (Physical Cell ID) information.



Empty Saved Locked PCIs List

7.8 LTE > Lock Bands

Please check Hint for module support bands and then select your desired multiple bands to lock for use.

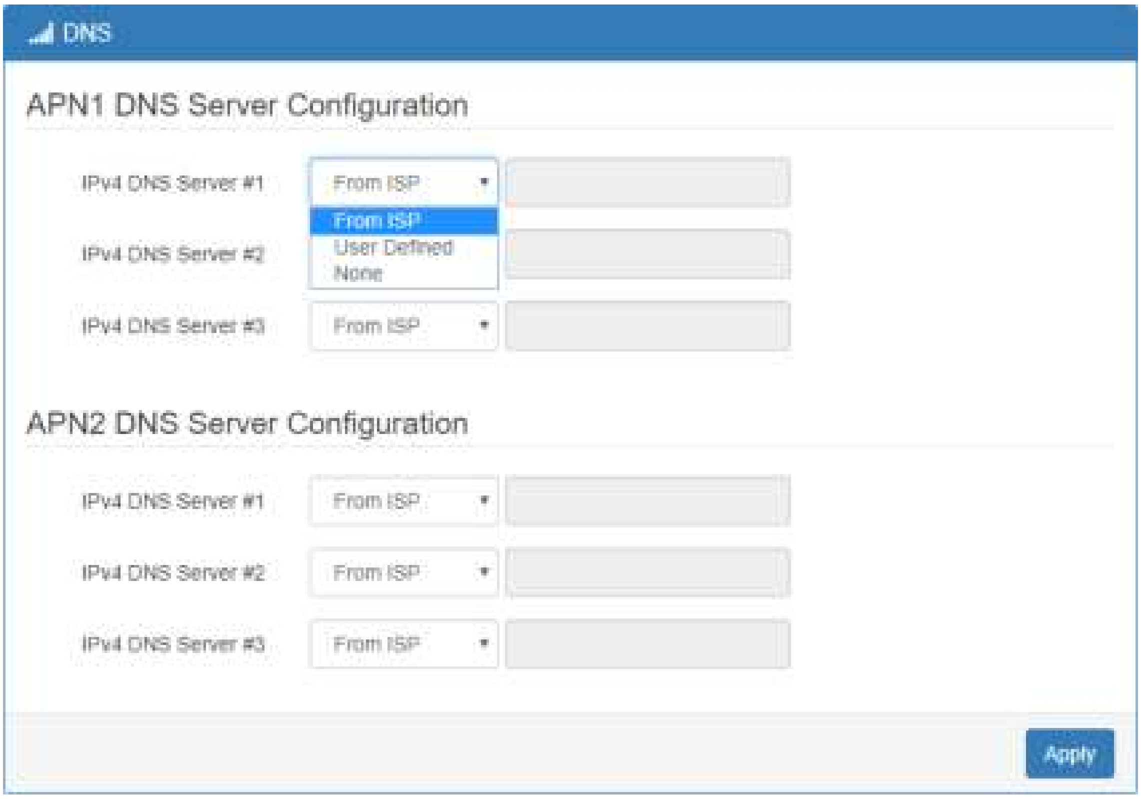


LTE Bands □ B01 □ B02 □ B03 □ B04 □ B05 □ B06 □ B07 □ B08 □ B09 □ B10
□ B11 □ B12 □ B13 □ B14 □ B15 □ B16 □ B17 □ B18 □ B19 □ B20
□ B21 □ B22 □ B23 □ B24 □ B25 □ B26 □ B27 □ B28 □ B29 □ B30
□ B31 □ B32 □ B33 □ B34 □ B35 □ B36 □ B37 □ B38 □ B39 □ B40
□ B41 □ B42 □ B43

Hint [EC25E] TDD:B38/B40/B41; FDD:B1/B3/B5/B7/B8/B20

7.9 LTE > DNS

This section allows you to setup LTE specific DNS setting.



APN1 DNS Server Configuration

IPv4 DNS Server #1: From ISP

IPv4 DNS Server #2

IPv4 DNS Server #3: From ISP

APN2 DNS Server Configuration

IPv4 DNS Server #1: From ISP

IPv4 DNS Server #2: From ISP

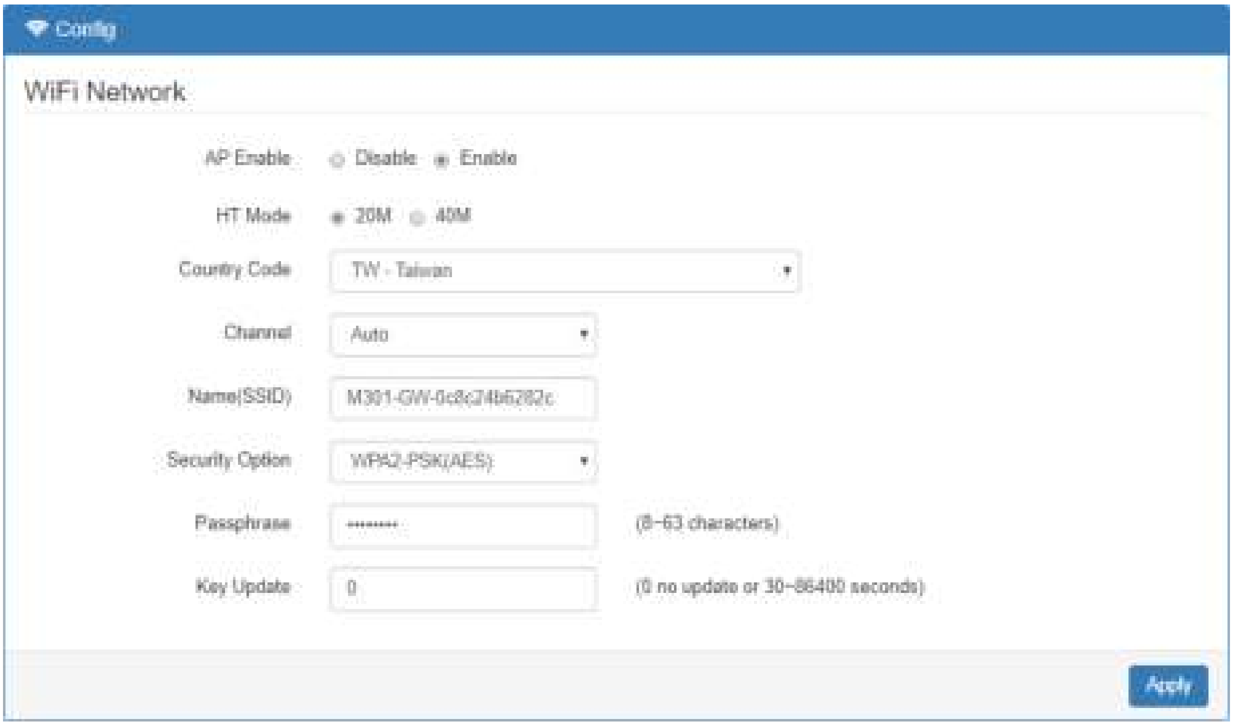
IPv4 DNS Server #3: From ISP

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.

8 Configuration > WiFi (M301-GW)

8.1 WiFi > WiFi Config

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



AP Enable: ○ Disable ● Enable

HT Mode: ● 20M ○ 40M

Country Code: TW - Taiwan

Channel: Auto

Name(SSID): M301-GW-0c8c24b6282c

Security Option: WPA2-PSK(AES)

Passphrase: ········· (8~63 characters)

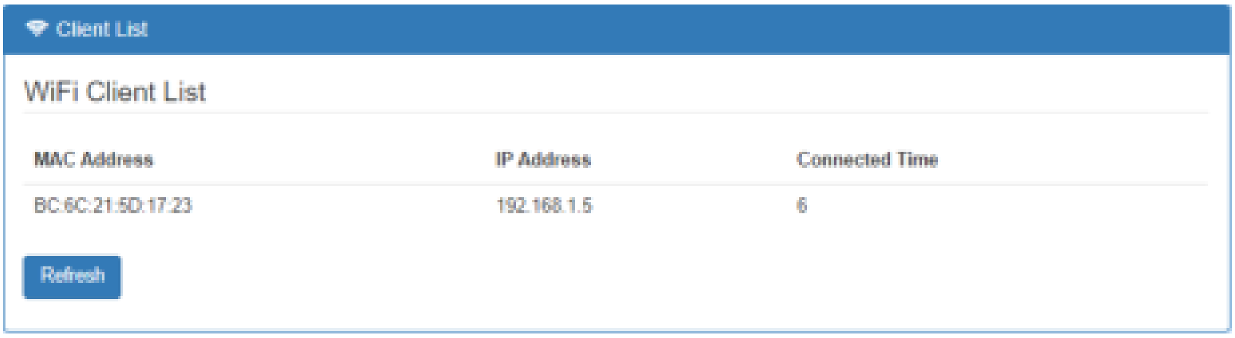
Key Update: 0 (0 no update or 30~86400 seconds)

Item	Description
AP Enable	Turn on/off the Wi-Fi Network. Select from Disable or Enable. The default is Enable.
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
Name(SSID)	SSID is Wi-Fi identification. The maximum length is 32
Channel	Auto (Automatically select the best channel) or manually select channel number.

Item	Description
Security Option	None / WPA-PSK(TKIP) / WPA-PSK(AES) / WPA2-PSK (TKIP) / WPA2-PSK(AES)/ WPA2(MIX).
Passphrase	The legal length is 8 ~ 63. The string should belong to [0-9 A-F a-f].
Key Update	0 means no update or 30~86400 seconds update period.

8.2 WiFi > Client List

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



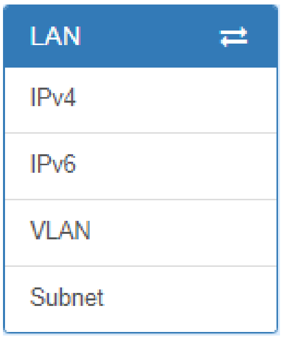
WiFi Client List

MAC Address	IP Address	Connected Time
BC:6C:21:5D:17:23	192.168.1.5	6

Item	Description
MAC Address	MAC Address
IP Address	Client IP Address
Connected Time	Connected Time in Seconds.

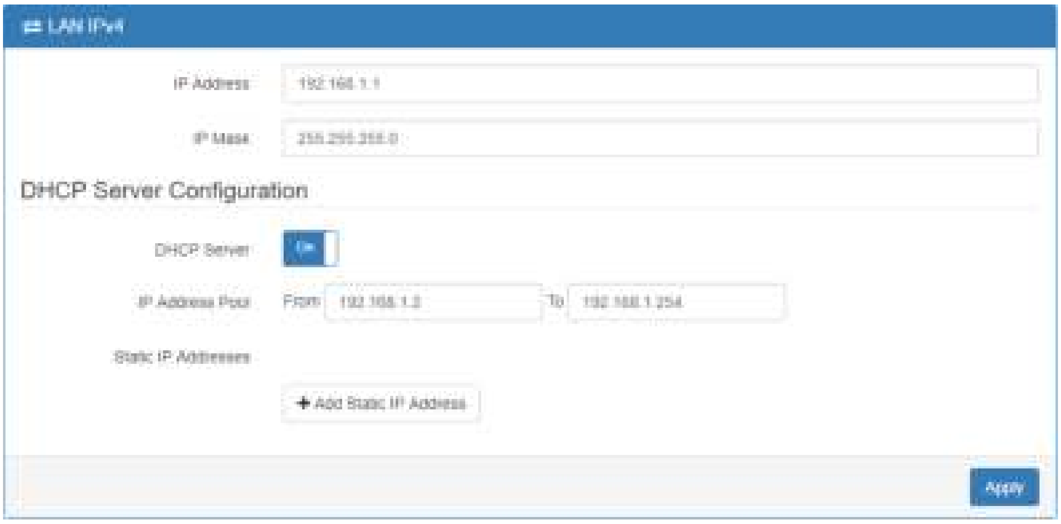
9 Configuration > LAN

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.



IP Address 192.168.1.1

IP Mask 255.255.255.0

DHCP Server Configuration

DHCP Server On

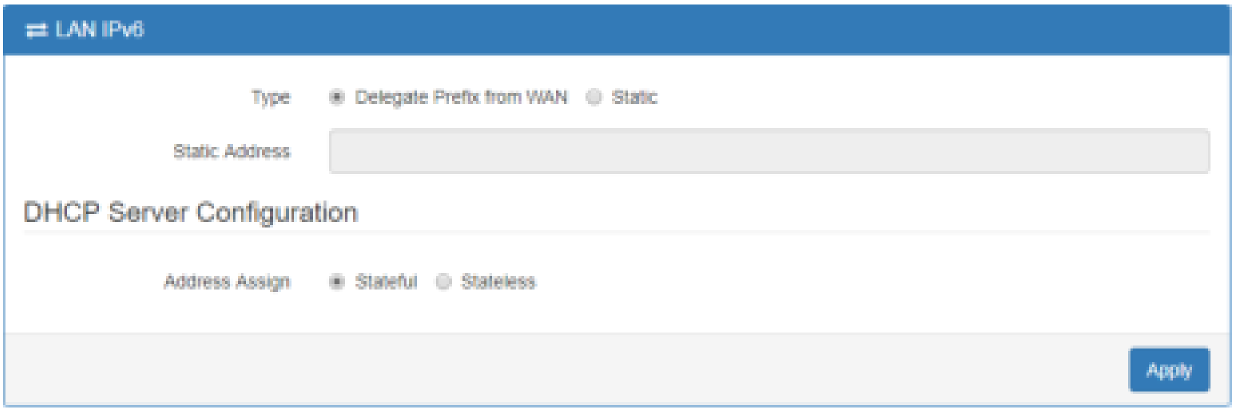
IP Address Pool From 192.168.1.2 To 192.168.1.254

Static IP Addresses

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, including Address Assign, DNS Assign and DNS Server.



LAN IPv6

Type ● Delegate Prefix from WAN ○ Static

Static Address

DHCP Server Configuration

Address Assign ● Stateful ○ Stateless

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.

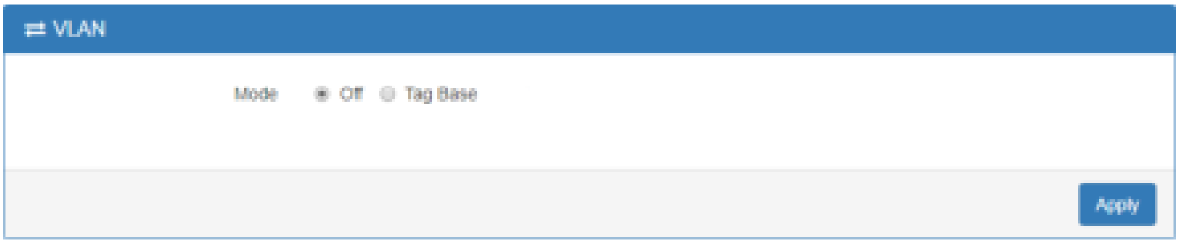
9.3 LAN > VLAN

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.

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

- Type 1:

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

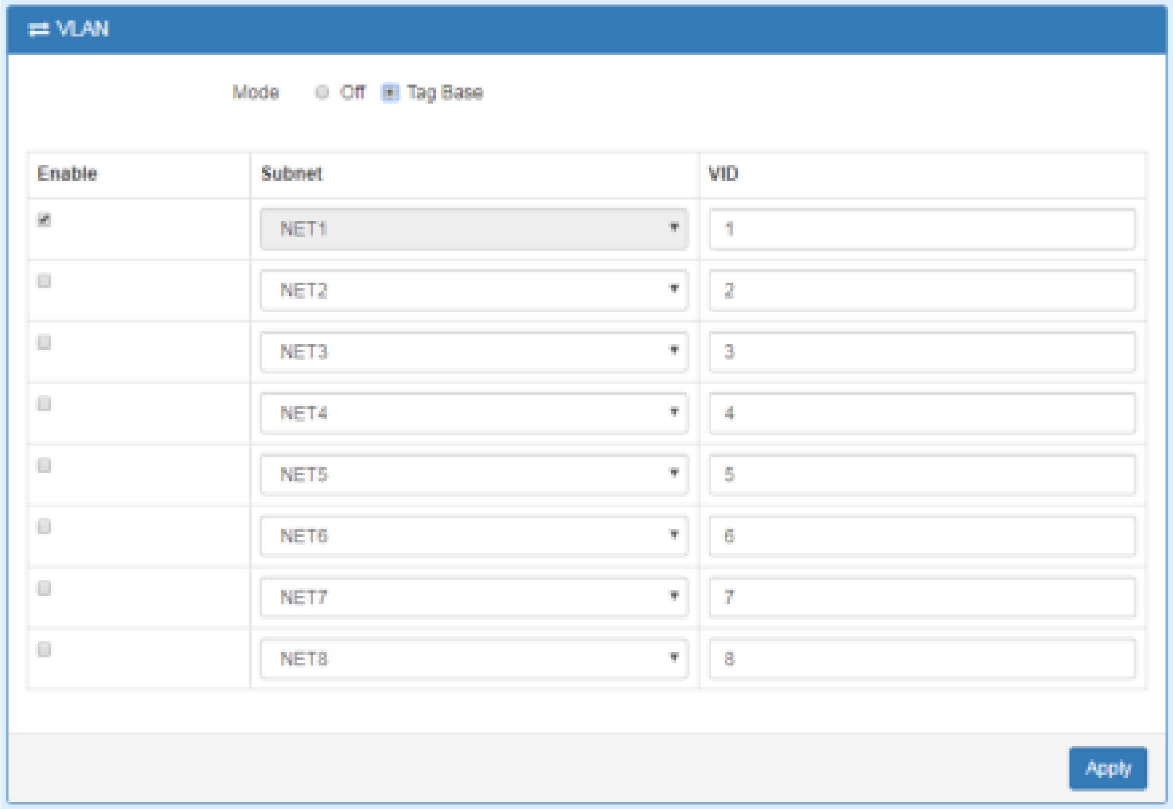


⇄ VLAN

Mode ● Off ○ Tag Base

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

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



⇄ VLAN

Mode ○ Off ● Tag Base

Enable	Subnet	VID
☑	NET1	1
□	NET2	2
□	NET3	3
□	NET4	4
□	NET5	5
□	NET6	6
□	NET7	7
□	NET8	8

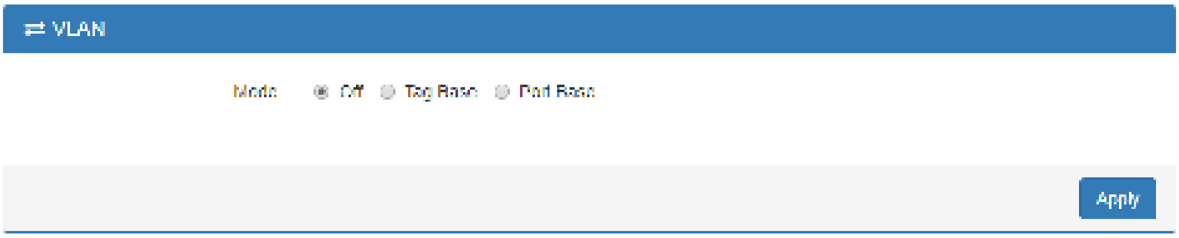
Furthermore, the **Subnet** provides DHCP Server function to allow the third party for the same VLAN to get IP address and IP mask. Therefore, you do not need to configure manually.

(***Note:*** The subnet information window will show from **LAN > Subnet**.)

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

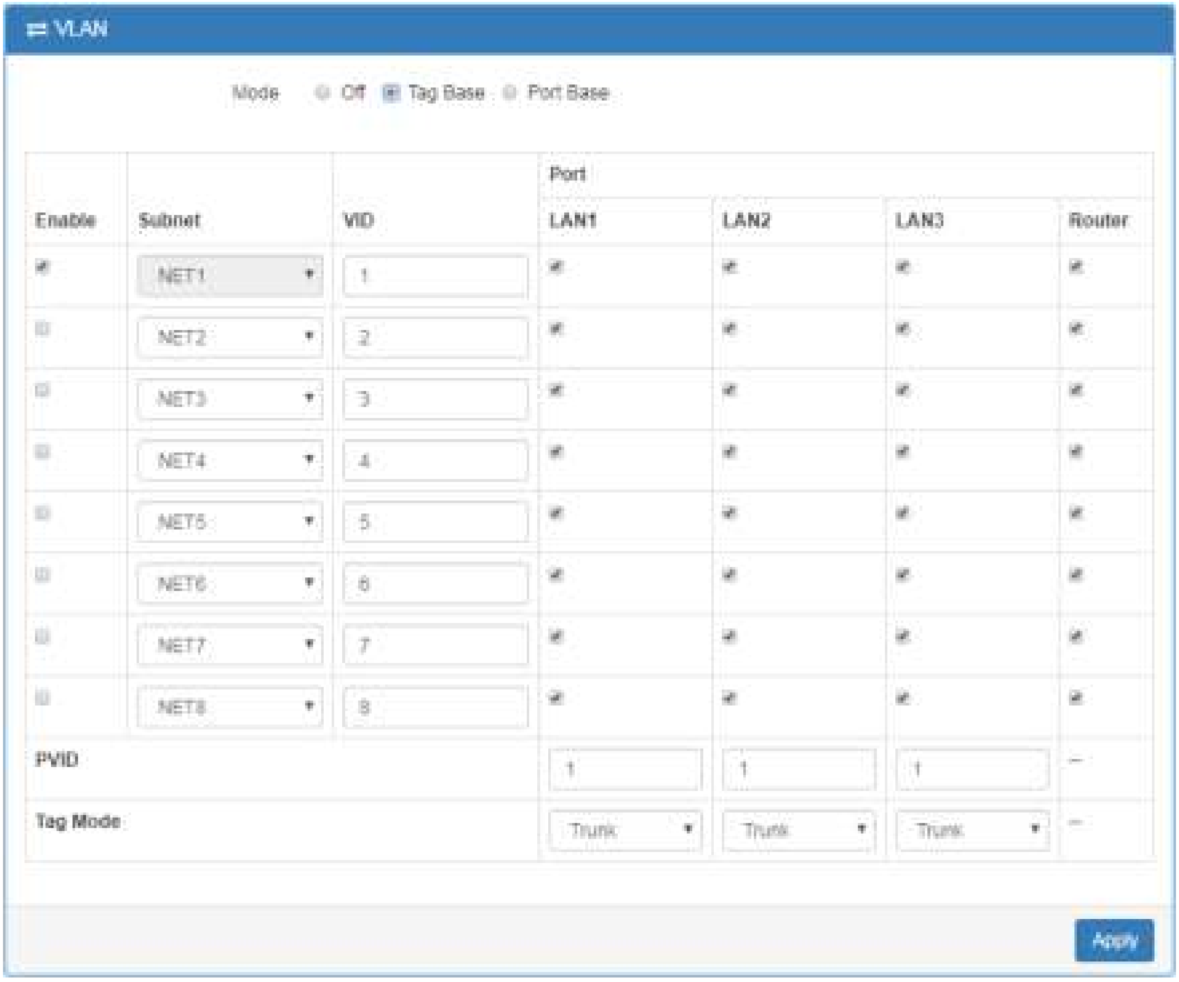
- Type 2:

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



Mode ● Off ○ Tag Base ○ Port Base

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



Mode ○ Off ● Tag Base ○ Port Base

			Port			
Enable	Subnet	VID	LAN1	LAN2	LAN3	Router
☑	NET1	1	☑	☑	☑	☑
□	NET2	2	☑	☑	☑	☑
□	NET3	3	☑	☑	☑	☑
□	NET4	4	☑	☑	☑	☑
□	NET5	5	☑	☑	☑	☑
□	NET6	6	☑	☑	☑	☑
□	NET7	7	☑	☑	☑	☑
□	NET8	8	☑	☑	☑	☑
PVID			1	1	1	—
Tag Mode			Trunk	Trunk	Trunk	—

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.

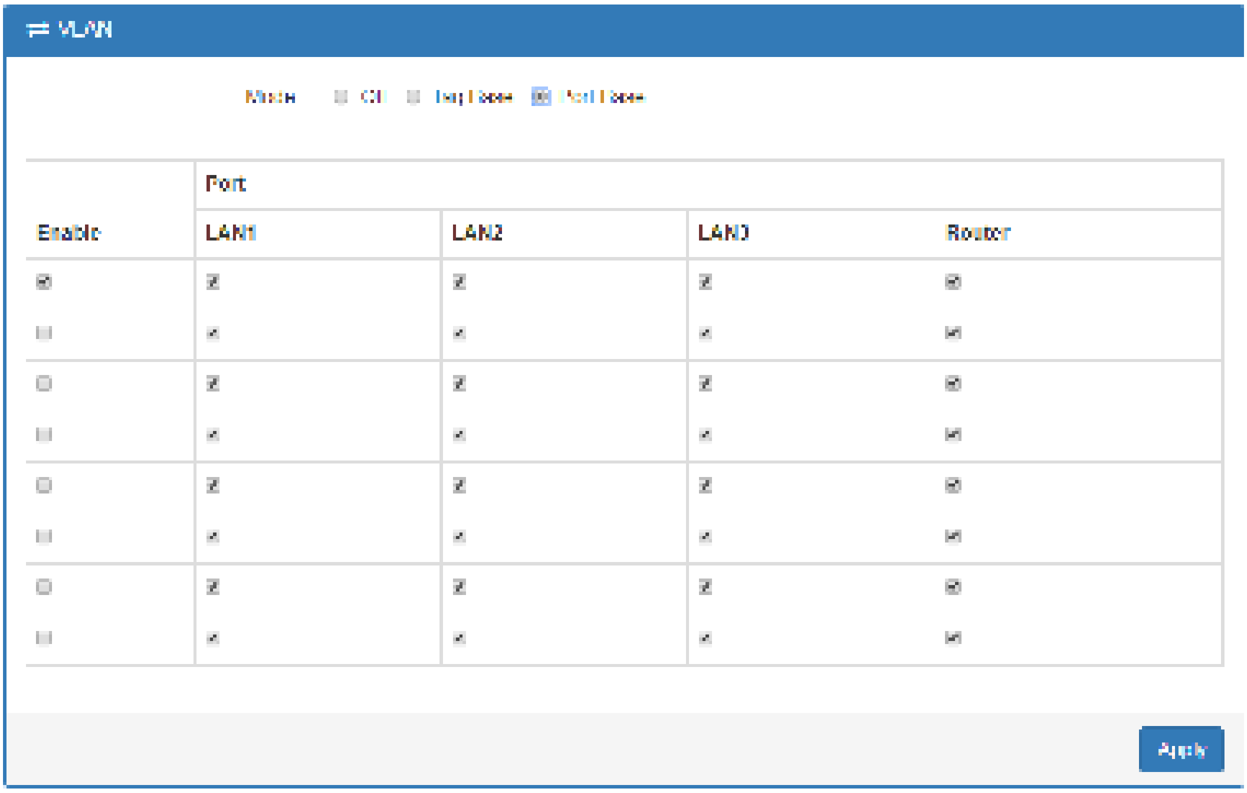
(***Note:*** The subnet information will show the Subnet window from the LAN catalogue.)

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

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

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

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

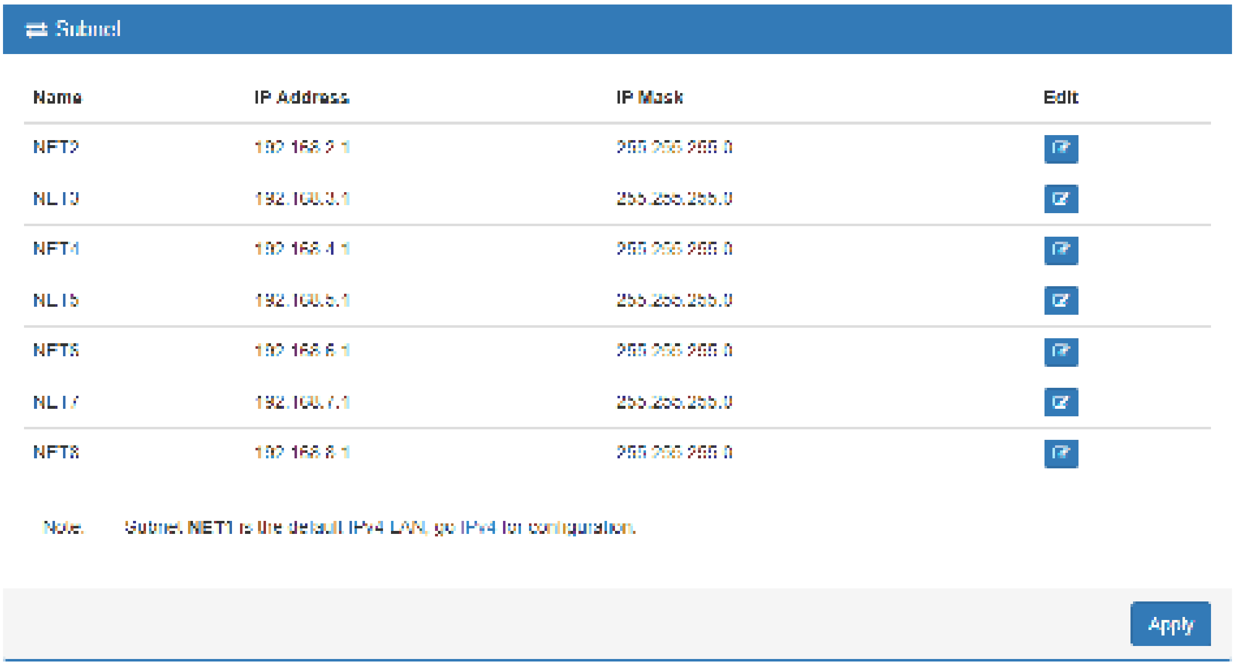


For each row, the settings can be enabled or disabled by checkbox and assign the port to communicate each other. There are three ports for **Port Base Mode**, including LAN1, LAN2 and LAN3. And one **Router port** which is a gate allows those ports to access internet or the router.

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

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.

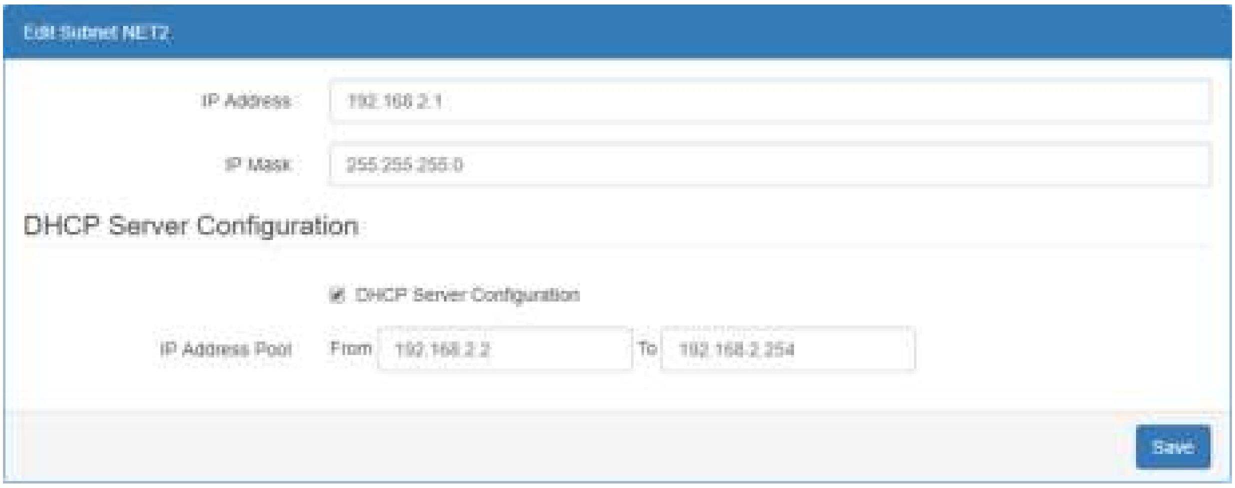


⇄ Subnet

Name	IP Address	IP Mask	Edit
NET2	192.168.2.1	255.255.255.0	✎
NET3	192.168.3.1	255.255.255.0	✎
NET4	192.168.4.1	255.255.255.0	✎
NET5	192.168.5.1	255.255.255.0	✎
NET6	192.168.6.1	255.255.255.0	✎
NET7	192.168.7.1	255.255.255.0	✎
NET8	192.168.8.1	255.255.255.0	✎

Note: Subnet NET1 is the default IPv4 LAN, go IPv4 for configuration.

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



Edit Subnet NET2

IP Address: 192.168.2.1

IP Mask: 255.255.255.0

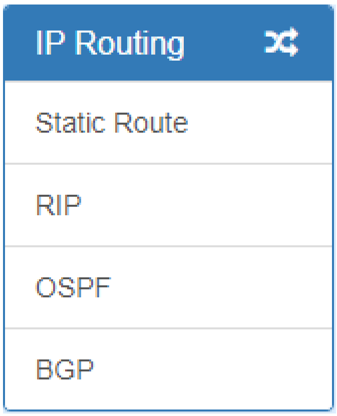
DHCP Server Configuration

☑ DHCP Server Configuration

IP Address Pool: From 192.168.2.2 To 192.168.2.254

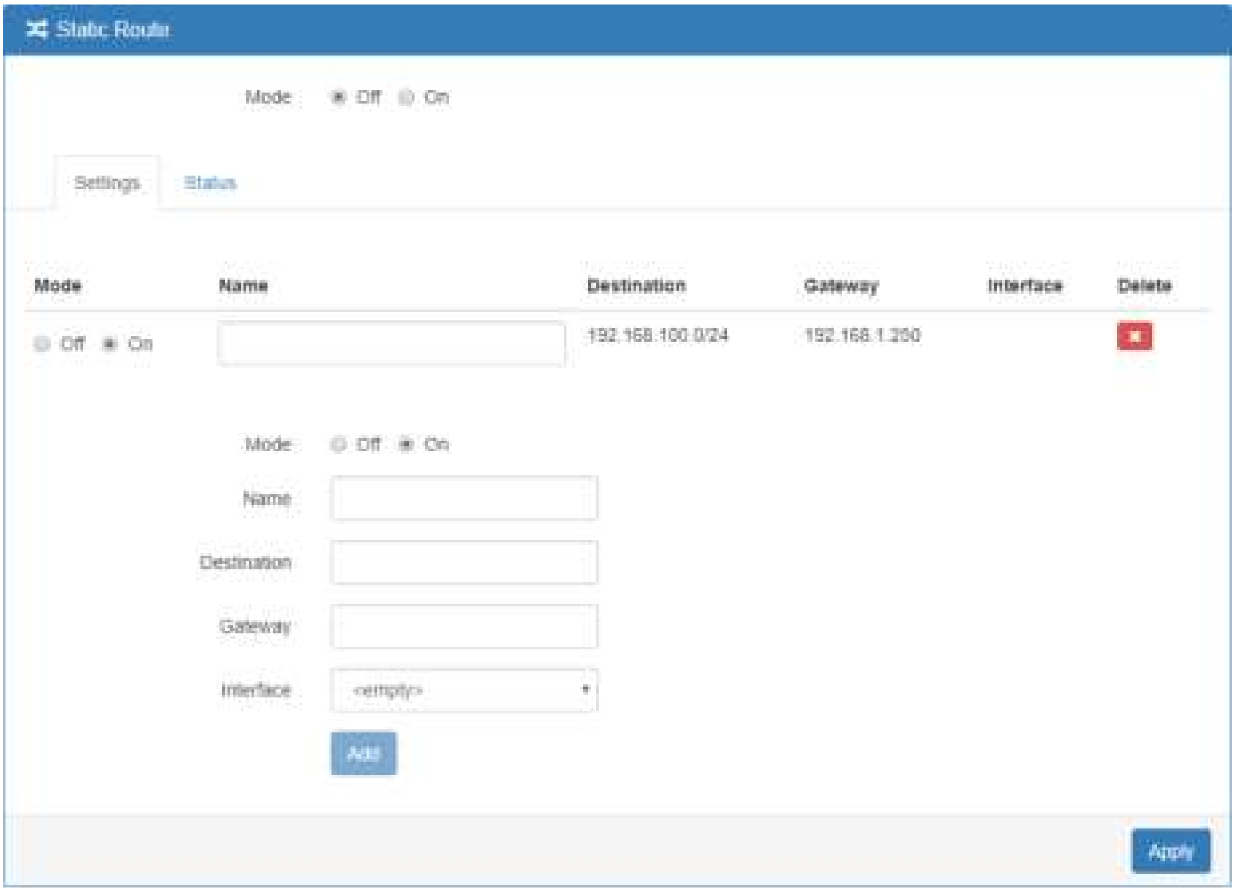
10 IP Routing

This section allows you to configure the Static 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.



Mode ● Off ○ On

Mode	Name	Destination	Gateway	Interface	Delete
○ Off ● On		192.168.100.0/24	192.168.1.200		✖

Mode ○ Off ● On

Name

Destination

Gateway

Interface <empty>

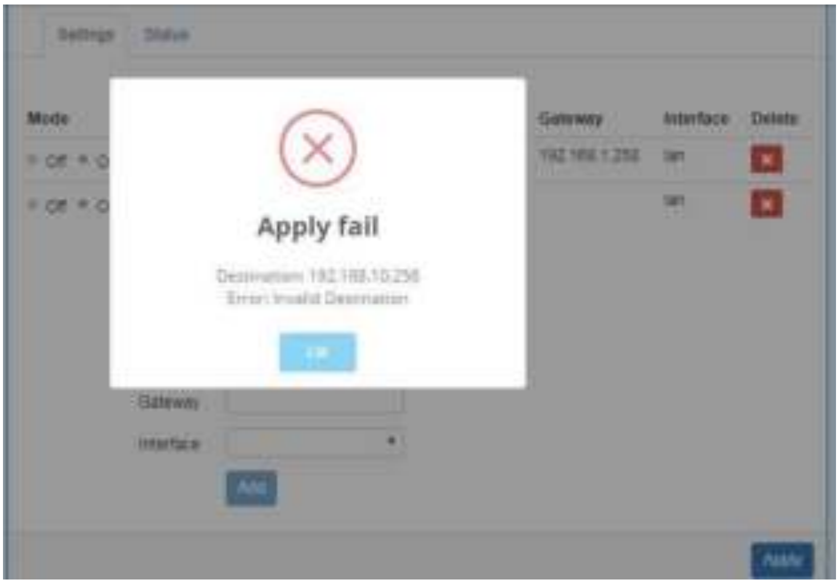
IP Routing > Static Route > Settings	
Item	**Description**
Mode	The setting is for full network. Select from Off or On.
Settings	
Mode	The setting is for the specific network. Select from Off or On.

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.

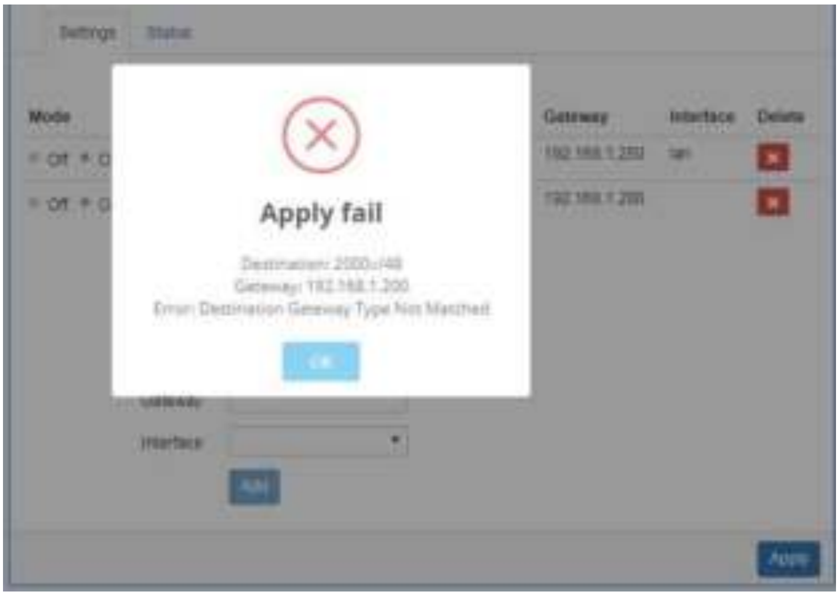
(1) Input the invalid format of destination. The interface is shown in Apply fail to notice.



Apply fail

Destination: 192.168.10.256
Error: Invalid Destination

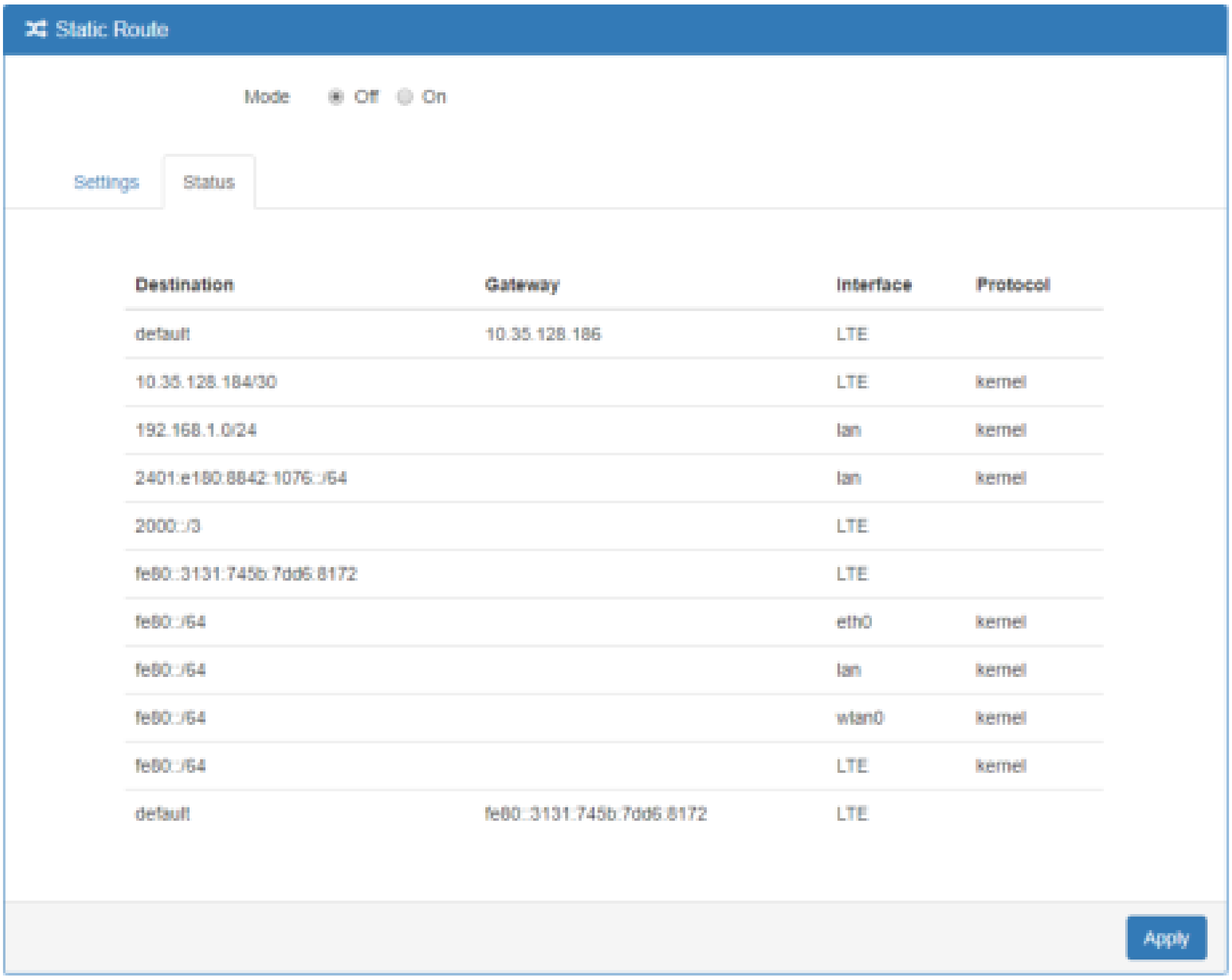
(2) Input the IP address of destination/gateway from IPv4 and IPv6 at the same time. The interface is shown in Apply fail to notice. You should select either IPv4 or IPv6 as the address of destination/gateway.



Apply fail

Destination: 2000::/48
Gateway: 192.168.1.200
Error: Destination Gateway Type Not Matched

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



Mode ● Off ○ On

Destination	Gateway	Interface	Protocol
default	10.35.128.186	LTE	
10.35.128.184/30		LTE	kernel
192.168.1.0/24		lan	kernel
2401:e180:8842:1076::/64		lan	kernel
2000::/3		LTE	
fe80::3131:745b:7dd6:8172		LTE	
fe80::/64		eth0	kernel
fe80::/64		lan	kernel
fe80::/64		wlan0	kernel
fe80::/64		LTE	kernel
default	fe80::3131:745b:7dd6:8172	LTE	

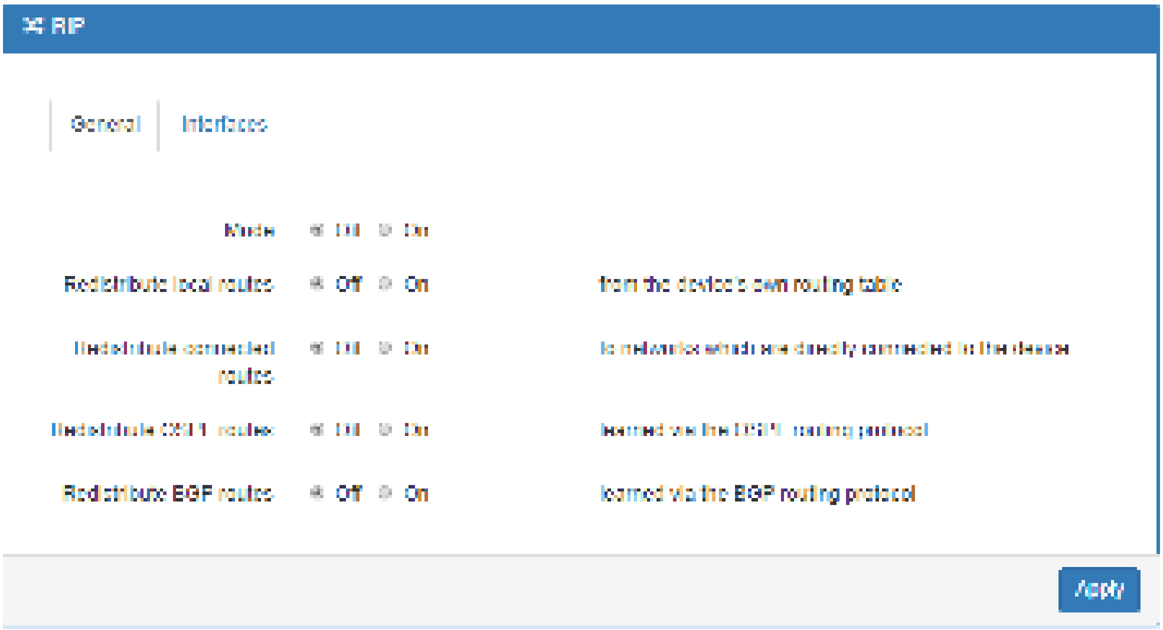
IP Routing > Static Route > Status	
Item	**Description**
Mode	The setting is open for full network. Select from Off or On.
Status	
Destination	Show the status of destination from the setting section.
Gateway	Show the status of gateway from the setting section.
Interface	Show the status of interface from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

10.2 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.



Mode ● Off ○ On

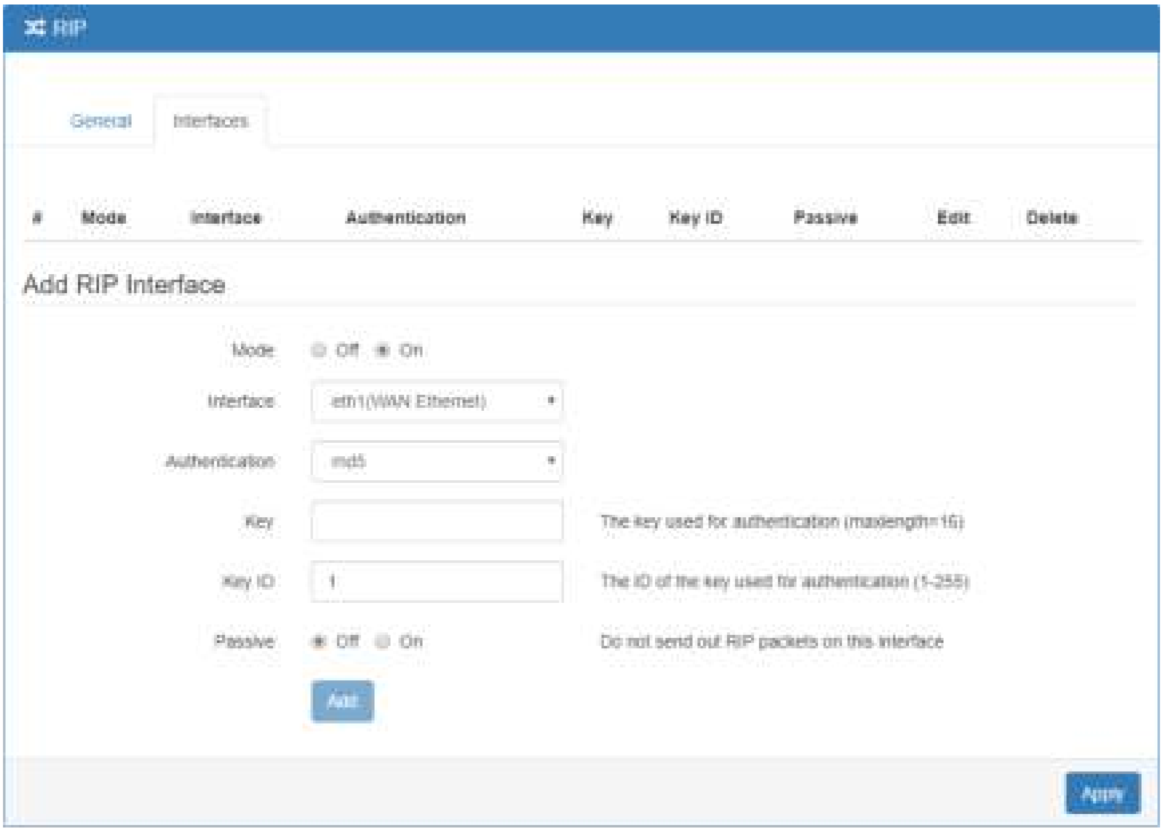
Redistribute local routes ● Off ○ On from the device's own routing table

Redistribute connected routes ● Off ○ On to networks which are directly connected to the device

Redistribute OSPF routes ● Off ○ On learned via the OSPF routing protocol

Redistribute BGP routes ● Off ○ On learned via the BGP routing protocol

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.



#	Mode	Interface	Authentication	Key	Key ID	Passive	Edit	Delete

Add RIP Interface

Mode ○ Off ● On

Interface eth1(WAN Ethernet)

Authentication md5

Key The key used for authentication (maxlength=16)

Key ID 1 The ID of the key used for authentication (1-255)

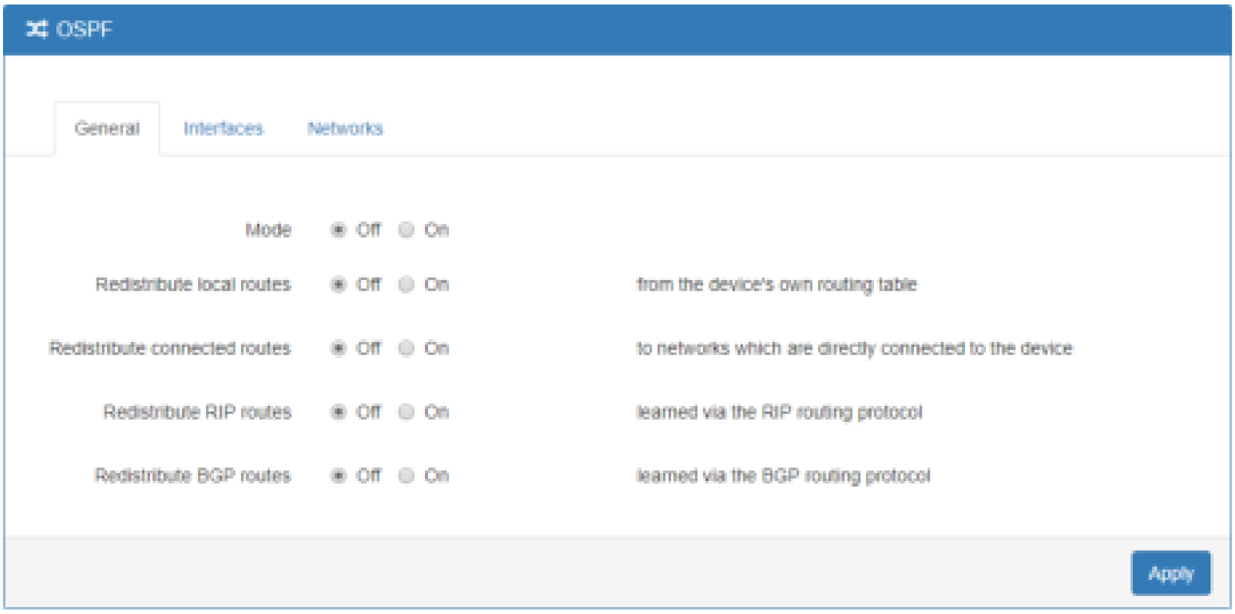
Passive ● Off ○ On Do not send out RIP packets on this interface

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.

10.3 IP Routing > OSPF

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

(1) General Configuration



Mode ● Off ○ On

Redistribute local routes ● Off ○ On from the device's own routing table

Redistribute connected routes ● Off ○ On to networks which are directly connected to the device

Redistribute RIP routes ● Off ○ On learned via the RIP routing protocol

Redistribute BGP routes ● Off ○ On learned via the BGP routing protocol

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

	● On: Redistribute connected routes to networks which are directly connected to the device.
Redistribute RIP routes	● Off: Not redistribute RIP routes learned via the RIP routing protocol. ● On: Redistribute RIP routes learned via the RIP routing protocol.
Redistribute BGP routes	● Off: Not redistribute BGP routes learned via the RIP routing protocol. ● On: Redistribute BGP routes learned via the RIP routing protocol.

(2) Interfaces Configuration

There are 2 parts for OSPF Interfaces configuration.

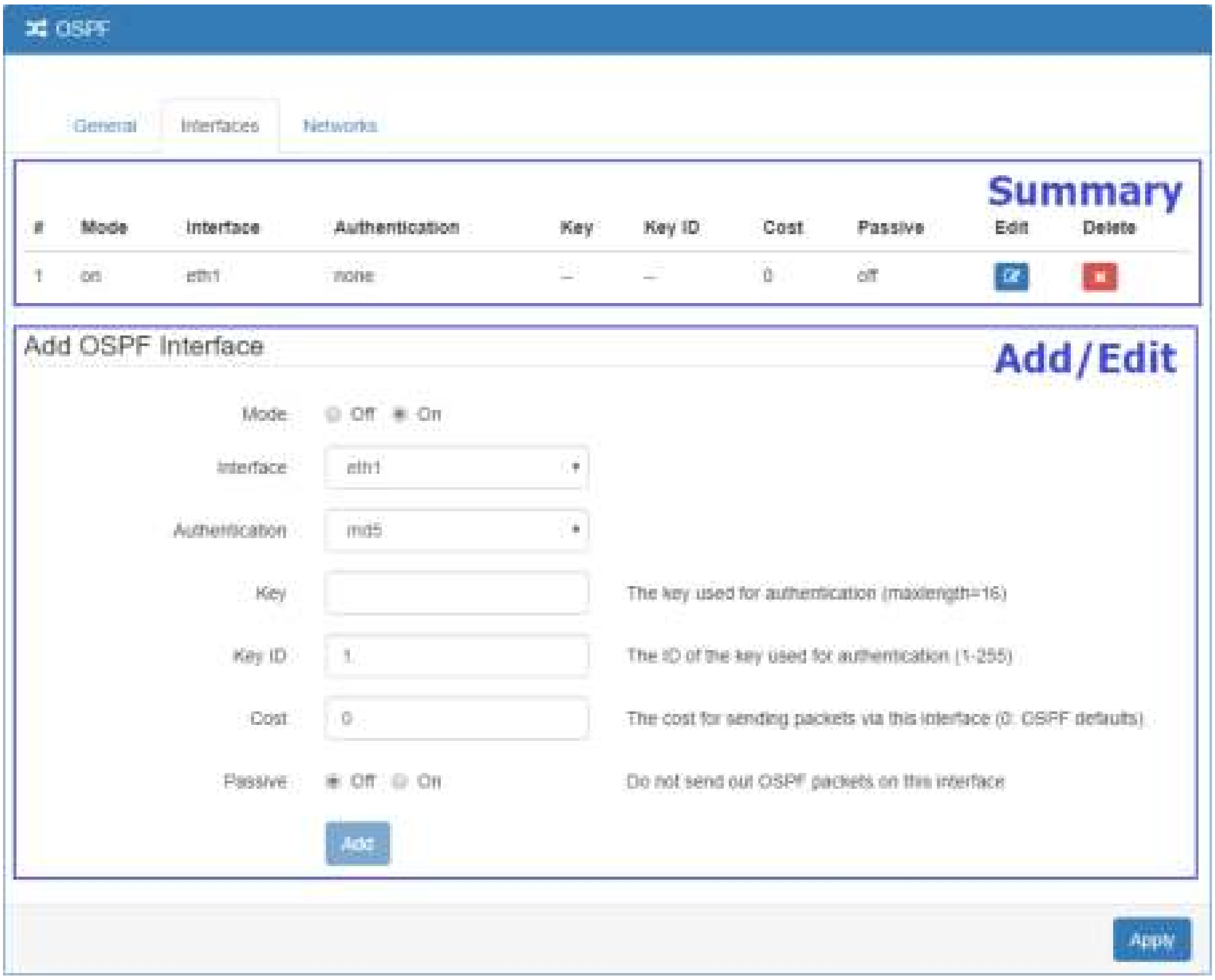
- OSPF Interfaces Summary

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

  Click **Delete** button to delete the existed interface.

- Add/Edit OSPF Interface

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



#	Mode	Interface	Authentication	Key	Key ID	Cost	Passive	Edit	Delete
1	on	eth1	none	–	–	0	off		

Add OSPF Interface

Mode	○ Off ● On	
Interface	eth1	
Authentication	md5	
Key		The key used for authentication (maxlength=16)
Key ID	1	The ID of the key used for authentication (1-255)
Cost	0	The cost for sending packets via this interface (0: OSPF defaults)
Passive	● Off ○ On	Do not send out OSPF packets on this interface

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

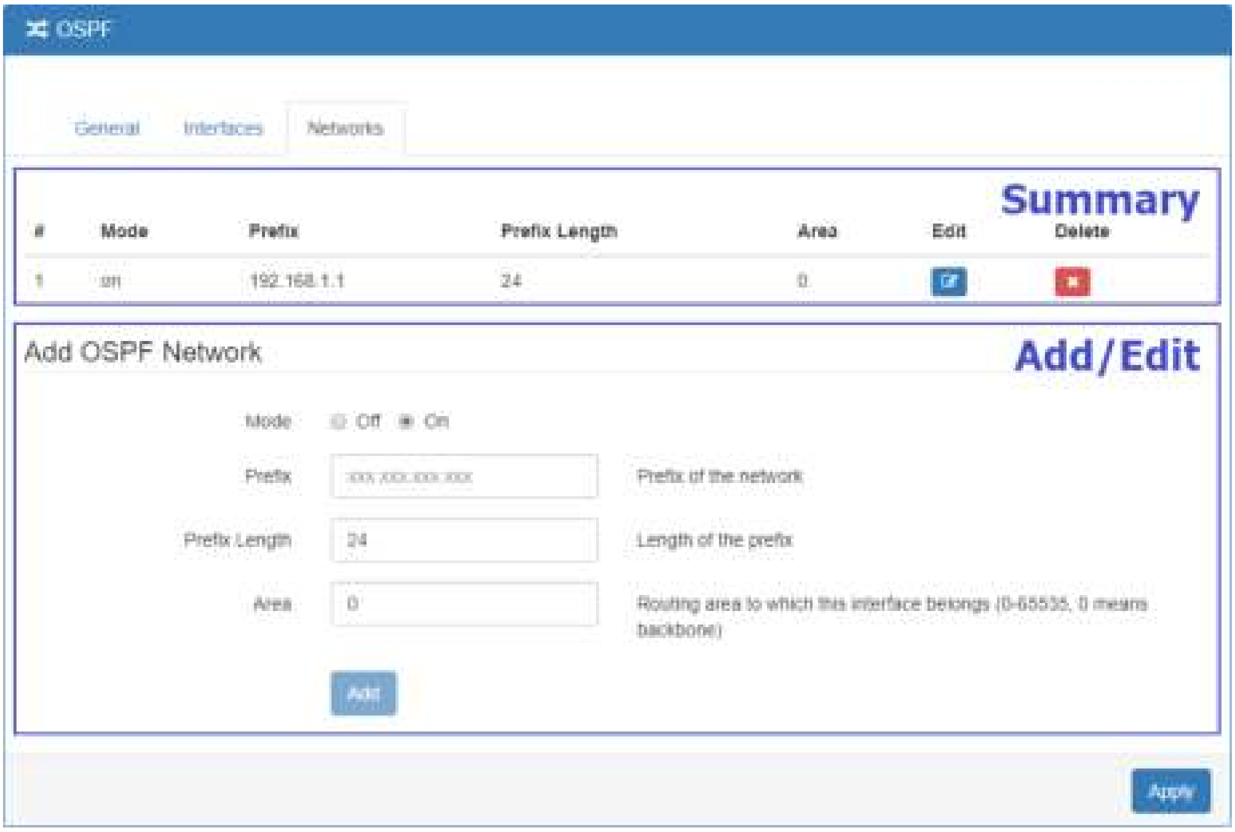
There are 2 parts for OSPF Networks configuration.

- 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.



#	Mode	Prefix	Prefix Length	Area	Edit	Delete
1	on	192.168.1.1	24	0	✎	✖

Add OSPF Network

Mode ○ Off ● On

Prefix xxx.xxx.xxx.xxx Prefix of the network

Prefix Length 24 Length of the prefix

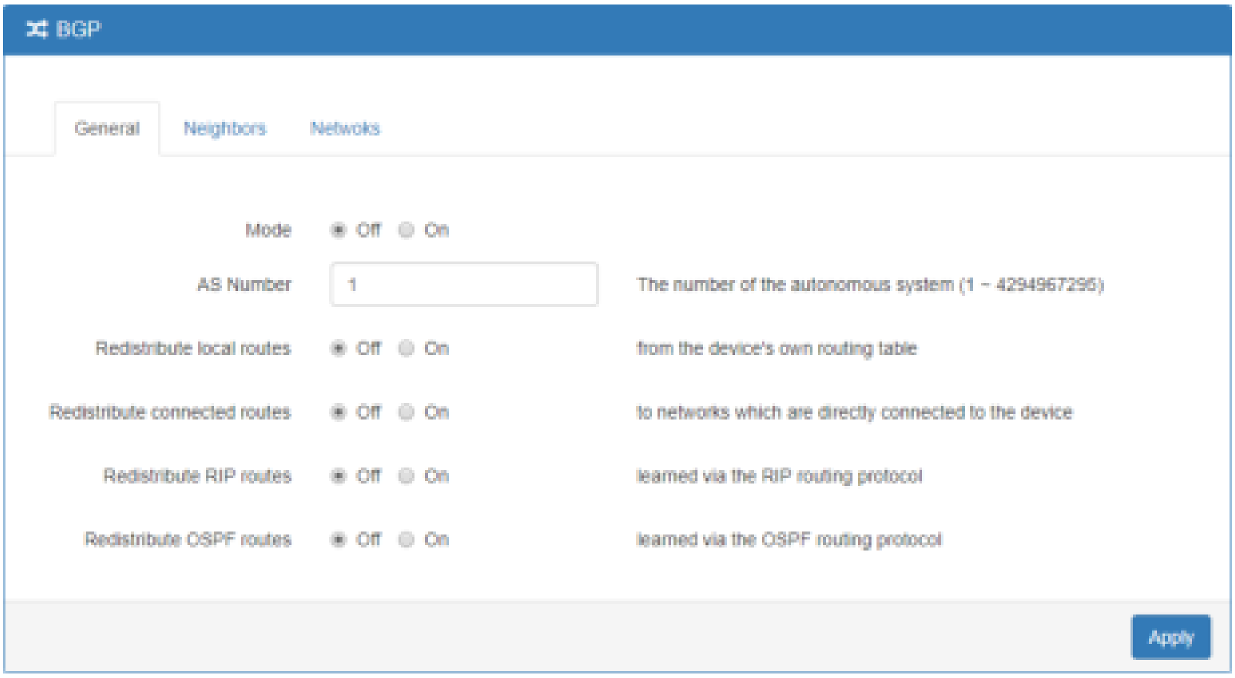
Area 0 Routing area to which this interface belongs (0-65535, 0 means backbone)

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)

10.4 IP Routing > BGP

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

(1) General Configuration



Mode ● Off ○ On

AS Number 1 — The number of the autonomous system (1 ~ 4294967295)

Redistribute local routes ● Off ○ On — from the device's own routing table

Redistribute connected routes ● Off ○ On — to networks which are directly connected to the device

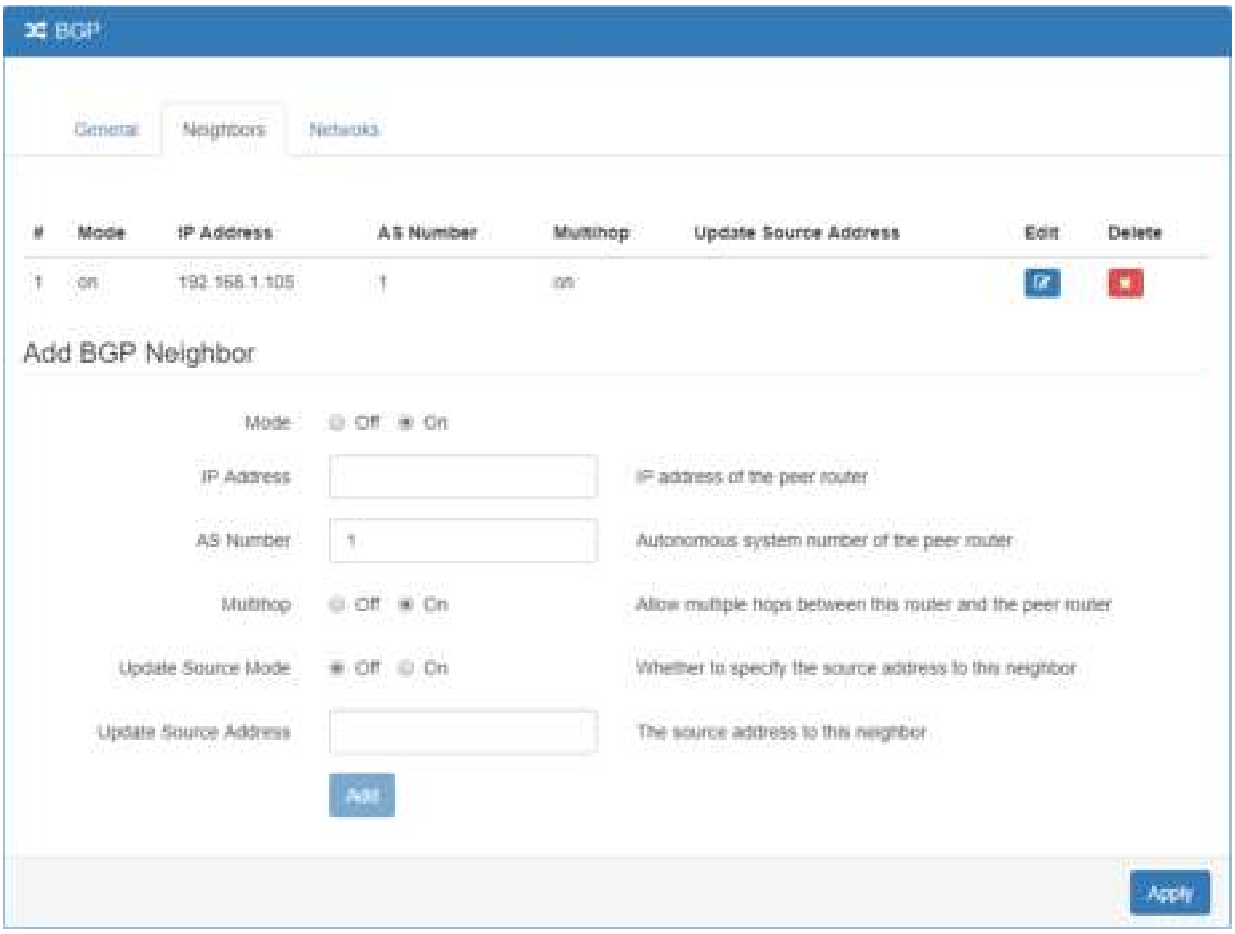
Redistribute RIP routes ● Off ○ On — learned via the RIP routing protocol

Redistribute OSPF routes ● Off ○ On — learned via the OSPF routing protocol

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

(2) Neighbor Configuration

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



#	Mode	IP Address	AS Number	Multihop	Update Source Address	Edit	Delete
1	on	192.168.1.105	1	on			

Add BGP Neighbor

Mode ○ Off ● On

IP Address — IP address of the peer router

AS Number 1 — Autonomous system number of the peer router

Multihop ○ Off ● On — Allow multiple hops between this router and the peer router

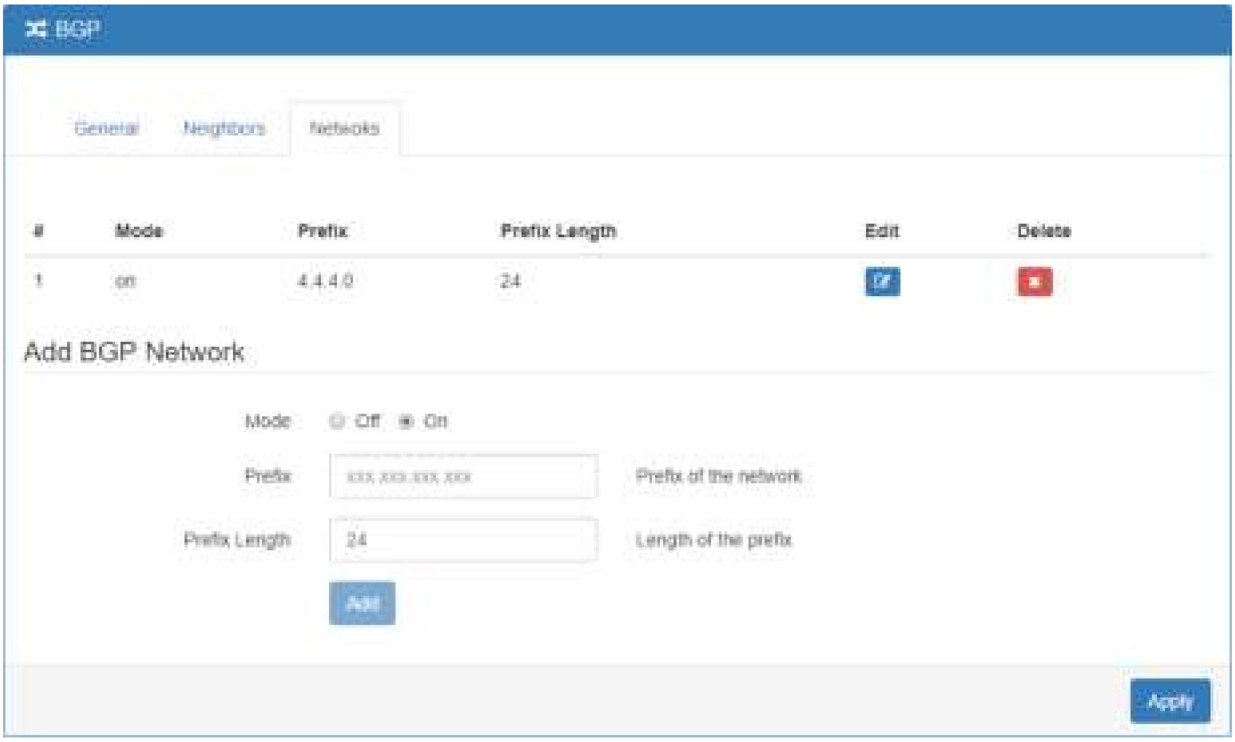
Update Source Mode ● Off ○ On — Whether to specify the source address to this neighbor

Update Source Address — The source address to this neighbor

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.



#	Mode	Prefix	Prefix Length	Edit	Delete
1	on	4.4.4.0	24	✎	✖

Add BGP Network

Mode ○ Off ● On

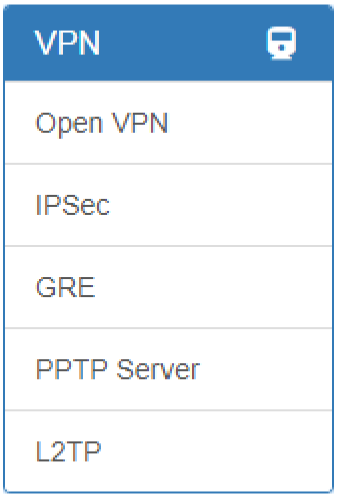
Prefix xxx.xxx.xxx.xxx Prefix of the network

Prefix Length 24 Length of the prefix

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.

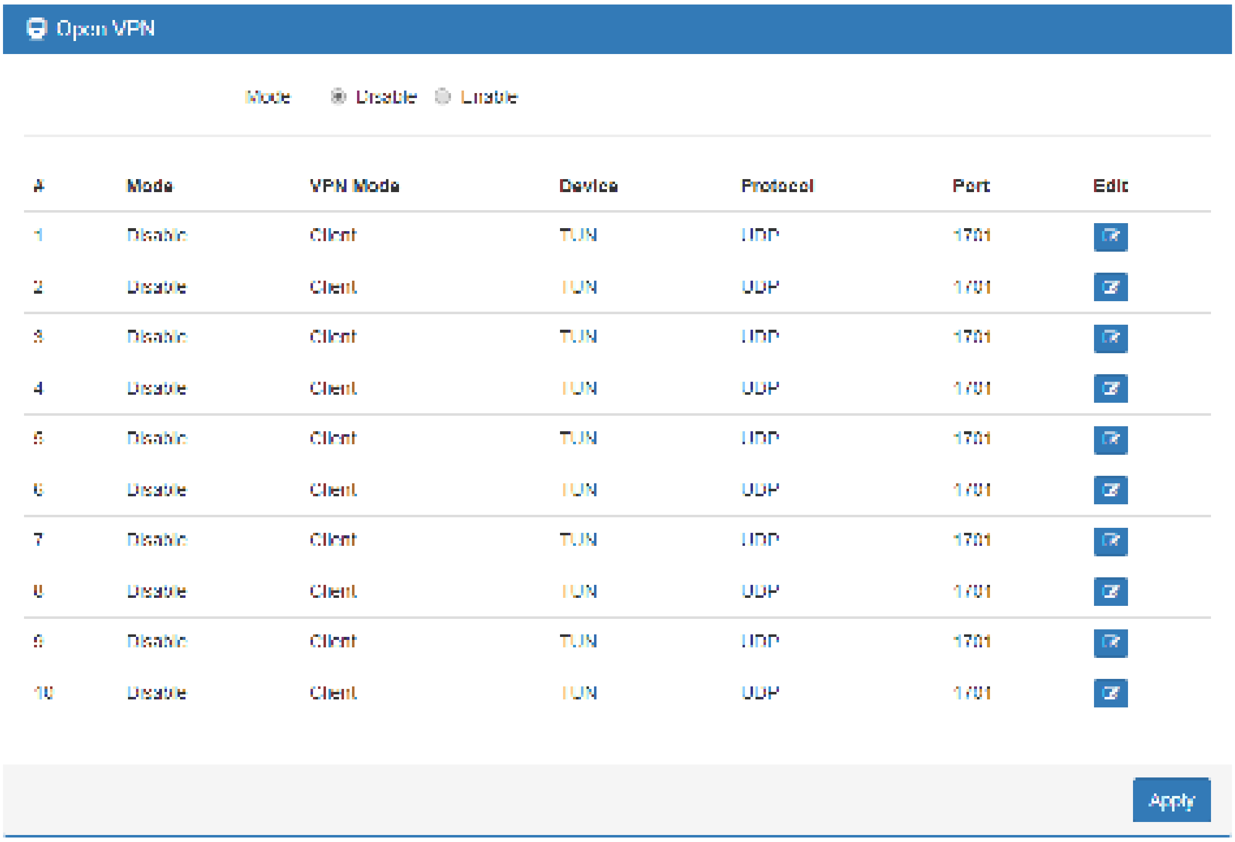

VPN

- Open VPN
- IPSec
- GRE
- PPTP Server
- L2TP

11.1 VPN > Open VPN

11.1.1 Open VPN Common Setting

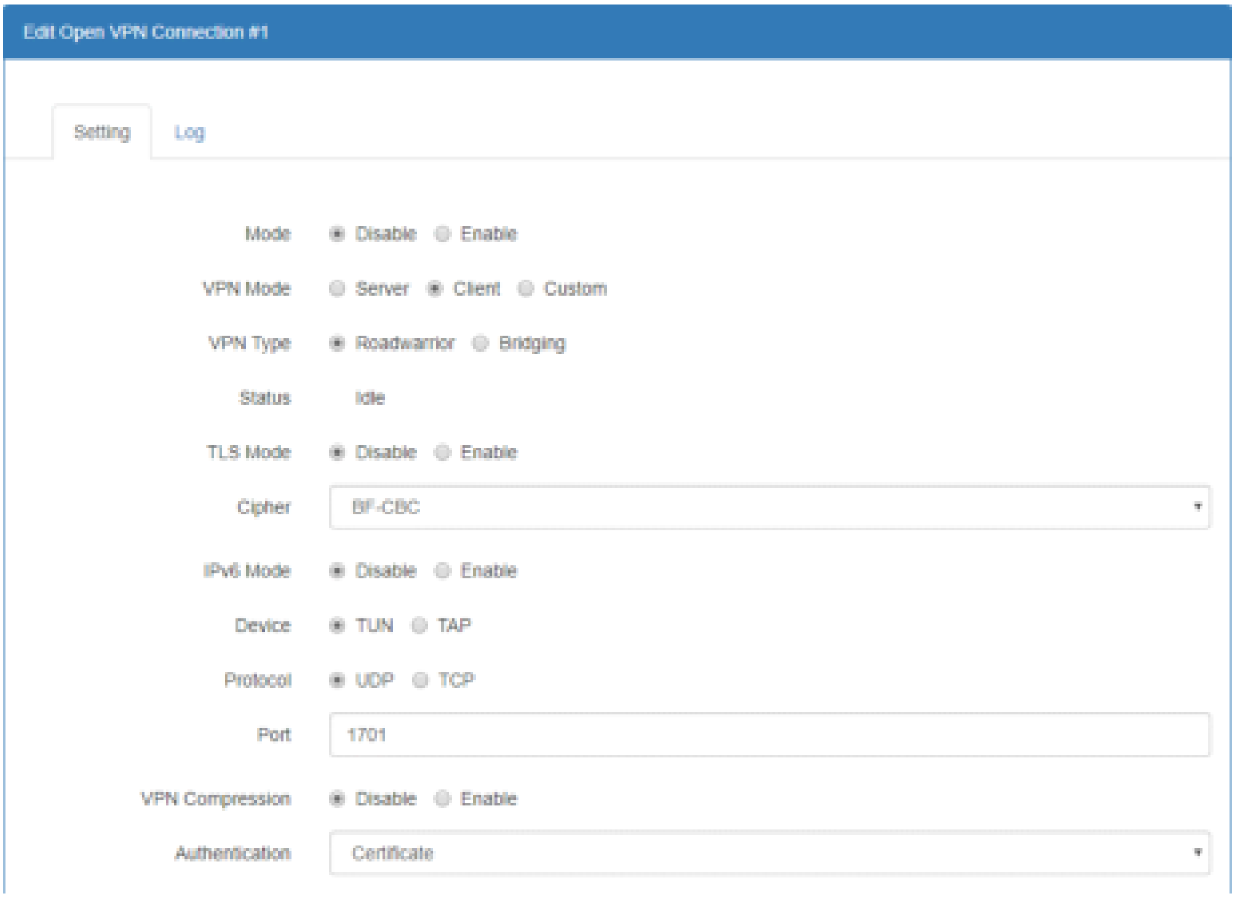
(1) This section allows you to configure the Open VPN parameters. The default mode is Disable. Click ✎ button to edit Open VPN Connection.


Open VPN

Mode ● Disable ○ Enable

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

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



Edit Open VPN Connection #1

Setting | Log

Mode: ● Disable ○ Enable

VPN Mode: ○ Server ● Client ○ Custom

VPN Type: ● Roadwarrior ○ Bridging

Status: Idle

TLS Mode: ● Disable ○ Enable

Cipher: BF-CBC

IPv6 Mode: ● Disable ○ Enable

Device: ● TUN ○ TAP

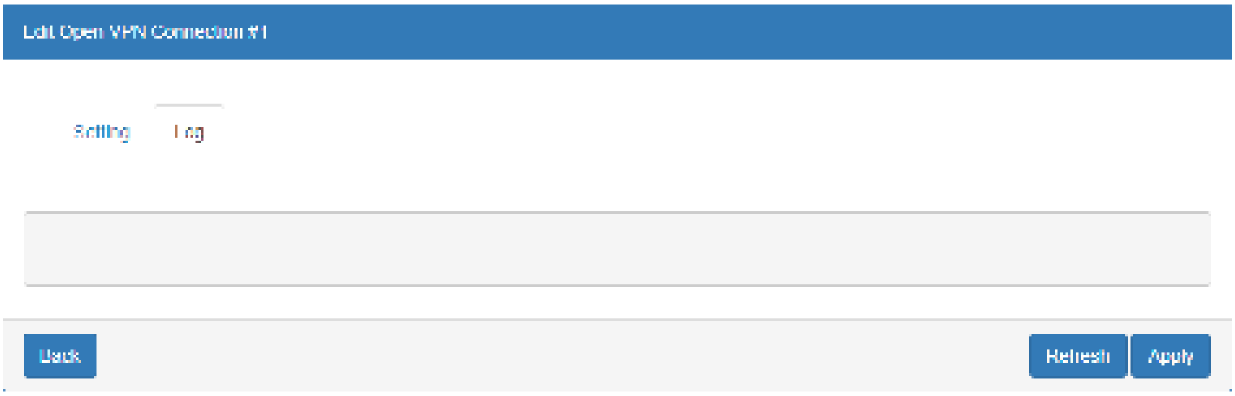
Protocol: ● UDP ○ TCP

Port: 1701

VPN Compression: ● Disable ○ Enable

Authentication: Certificate

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



Edit Open VPN Connection #1

Setting | Log

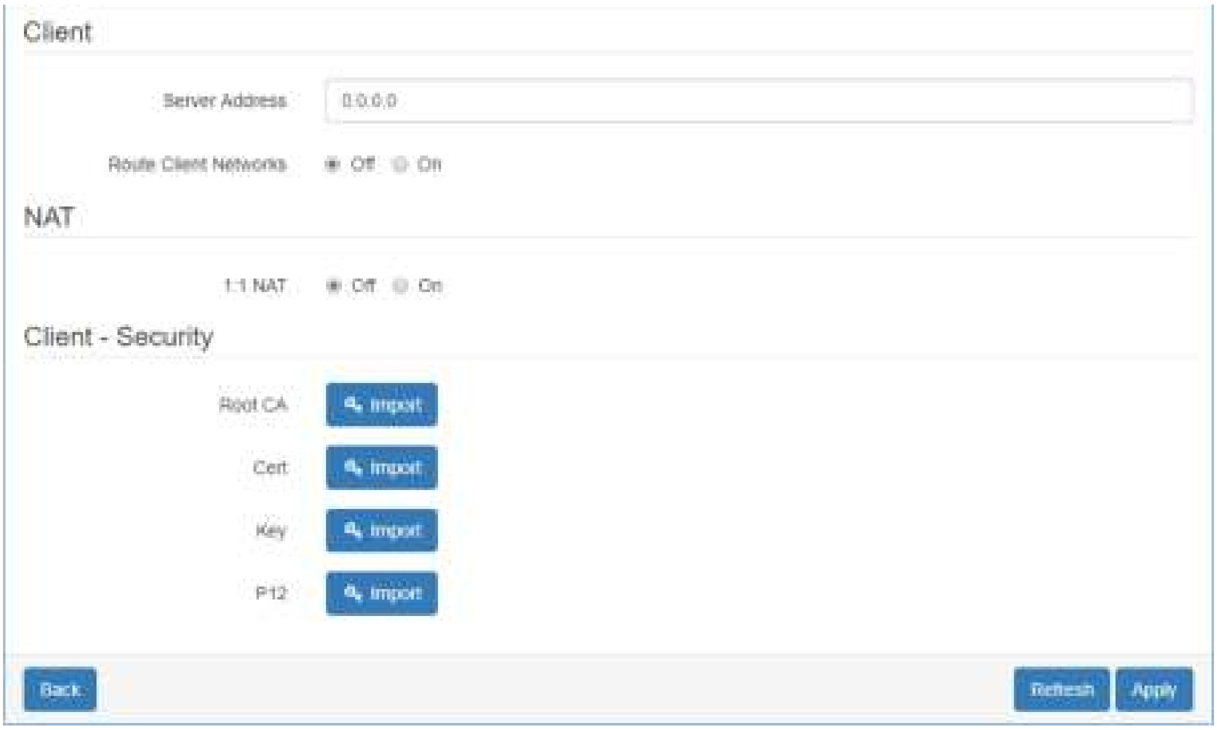
VPN > Open VPN > Setting	
Item	**Description**
Mode	Turn on/off Open VPN to select Disable or Enable.
VPN Mode	● **Server:** Tick to enable Open VPN server tunnel. ● **Client:** Tick to enable Open VPN client tunnel. The default is Client. ● **Custom:** This option allows user to use the .ovpn configuration 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.



Client

Server Address: 0.0.0.0

Route Client Networks: ● Off ○ On

NAT

1:1 NAT: ● Off ○ On

Client - Security

Root CA

Cert

Key

P12

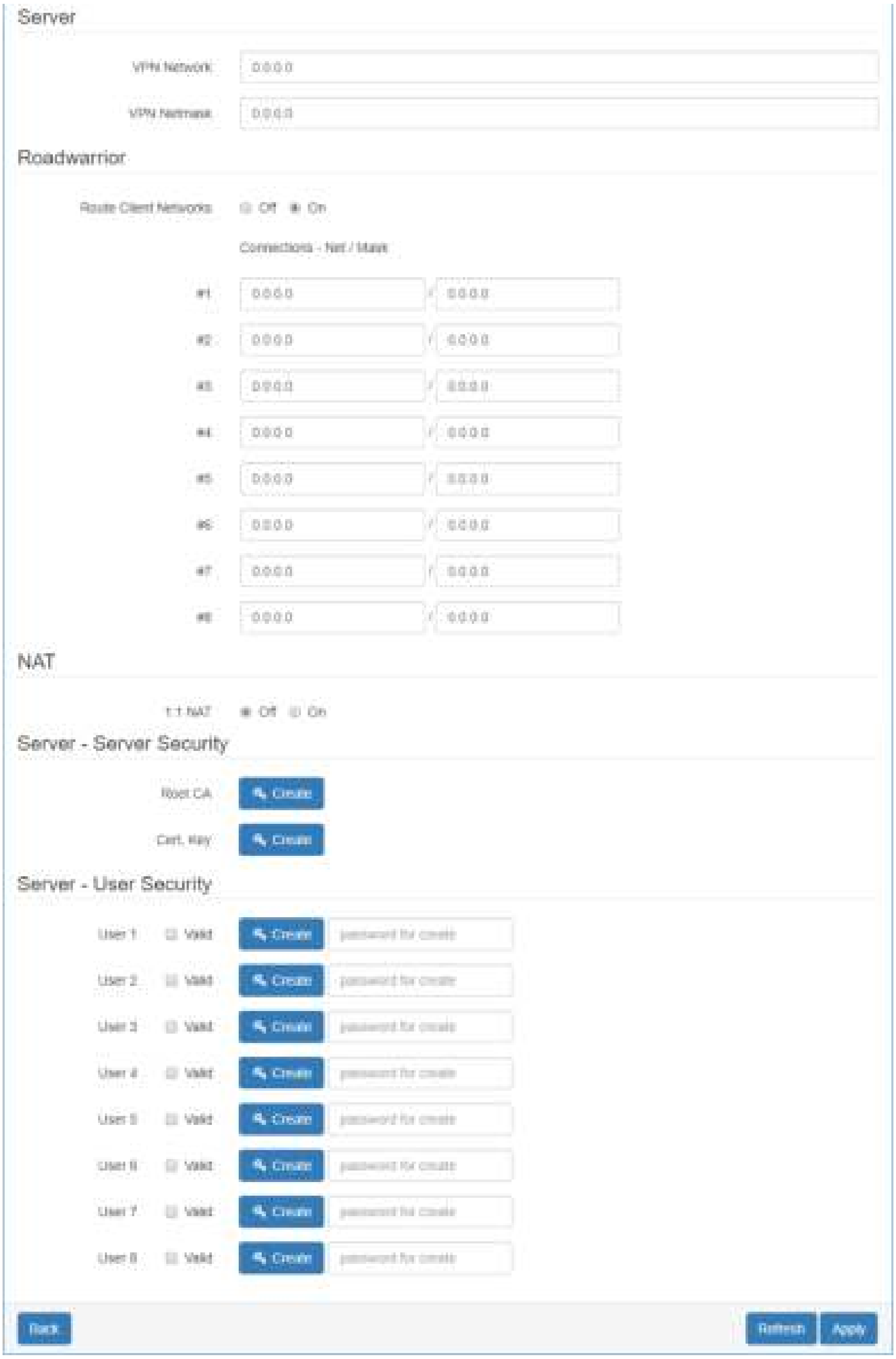
VPN > Open VPN > Client VPN Mode	
Item	**Description**
Client	
Server Address	Fill in WAN IP of Open VPN server.
Route Client Networks	Select from Off or On. This setting needs to match the server side. When enabled, the cellular router will auto apply the properly routing rules.
NAT	
1:1 NAT	● Tick 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.



Server

VPN Network: 0.0.0.0

VPN Netmask: 0.0.0.0

Roadwarrior

Route Client Networks: ○ Off ● On

Connections - Net / Mask

#1	0.0.0.0	/ 0.0.0.0
#2	0.0.0.0	/ 0.0.0.0
#3	0.0.0.0	/ 0.0.0.0
#4	0.0.0.0	/ 0.0.0.0
#5	0.0.0.0	/ 0.0.0.0
#6	0.0.0.0	/ 0.0.0.0
#7	0.0.0.0	/ 0.0.0.0
#8	0.0.0.0	/ 0.0.0.0

NAT

1:1 NAT: ● Off ○ On

Server - Server Security

Root CA: Create

Cert. Key: Create

Server - User Security

User 1	□ Valid	Create	password for create
User 2	□ Valid	Create	password for create
User 3	□ Valid	Create	password for create
User 4	□ Valid	Create	password for create
User 5	□ Valid	Create	password for create
User 6	□ Valid	Create	password for create
User 7	□ Valid	Create	password for create
User 8	□ Valid	Create	password for create

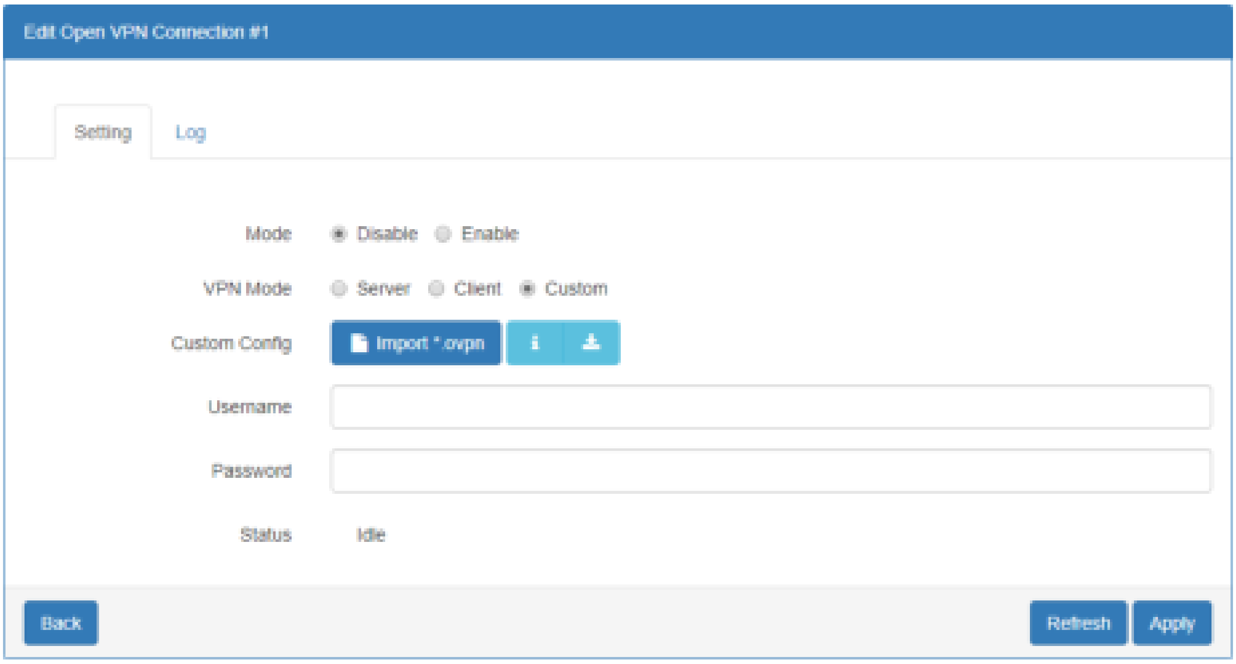
VPN > Open VPN > Server VPN Mode	
Item	**Description**
Server	
VPN Network	The network ID for Open VPN virtual network.
VPN Netmask	The netmask for Open VPN virtual network.
Roadwarrior: **Route Client Networks**	Select from Off or On. The Open VPN server will route the client traffic or not. User should fill in the client IP and netmask when this option is enabled.
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 Import *.ovpn 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 ℹ ⬇ button. Click ℹ for displaying the information and ⬇ for downloading the file.
- For third-party Open VPN configuration, suggest from http://www.vpngate.net/en/


Edit Open VPN Connection #1

Setting | Log

Mode ● Disable ○ Enable

VPN Mode ○ Server ○ Client ● Custom

Custom Config: Import *.ovpn

Username

Password

Status Idle

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 seting 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

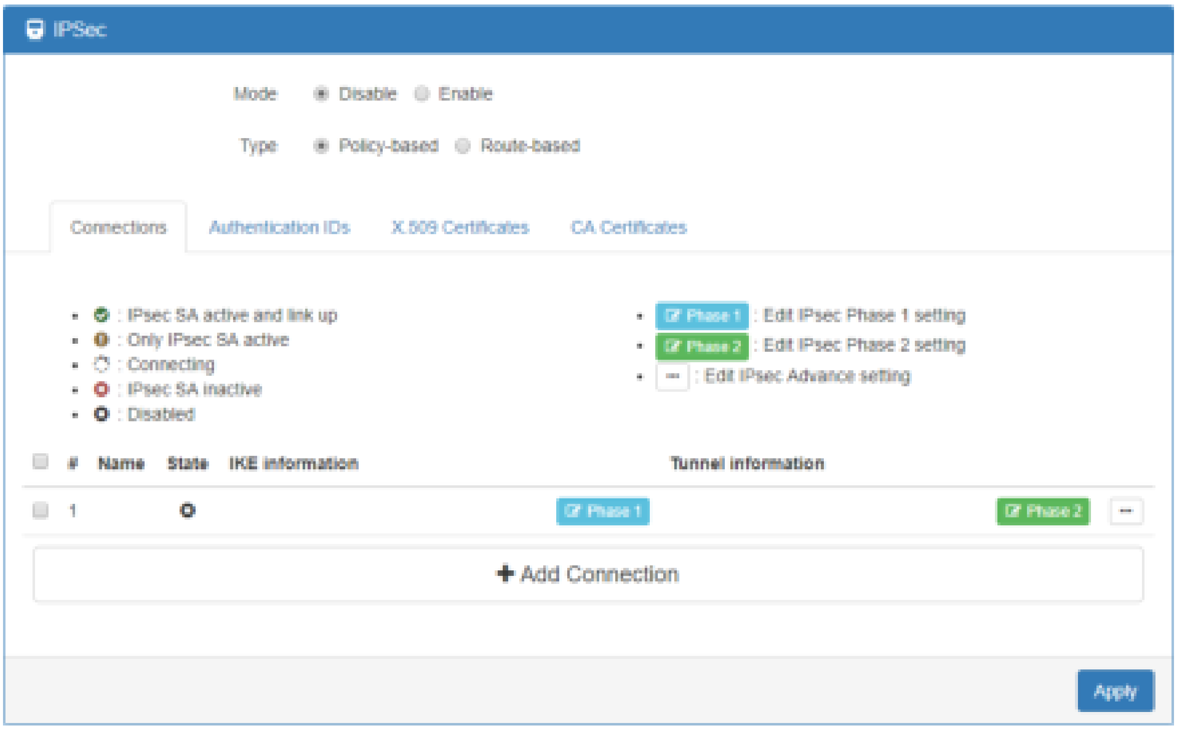
Type ● Policy based ○ Route based

VPN > IPsec > General setting	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Type	Select from Policy-based or Route-based. The default is Policy-based. ● Policy-based: transmit traffic that meet the IPsec phase 2 local/remote subnet. ● Route-based: transmit traffic that match routing table.

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.



IPSec

Mode ● Disable ○ Enable

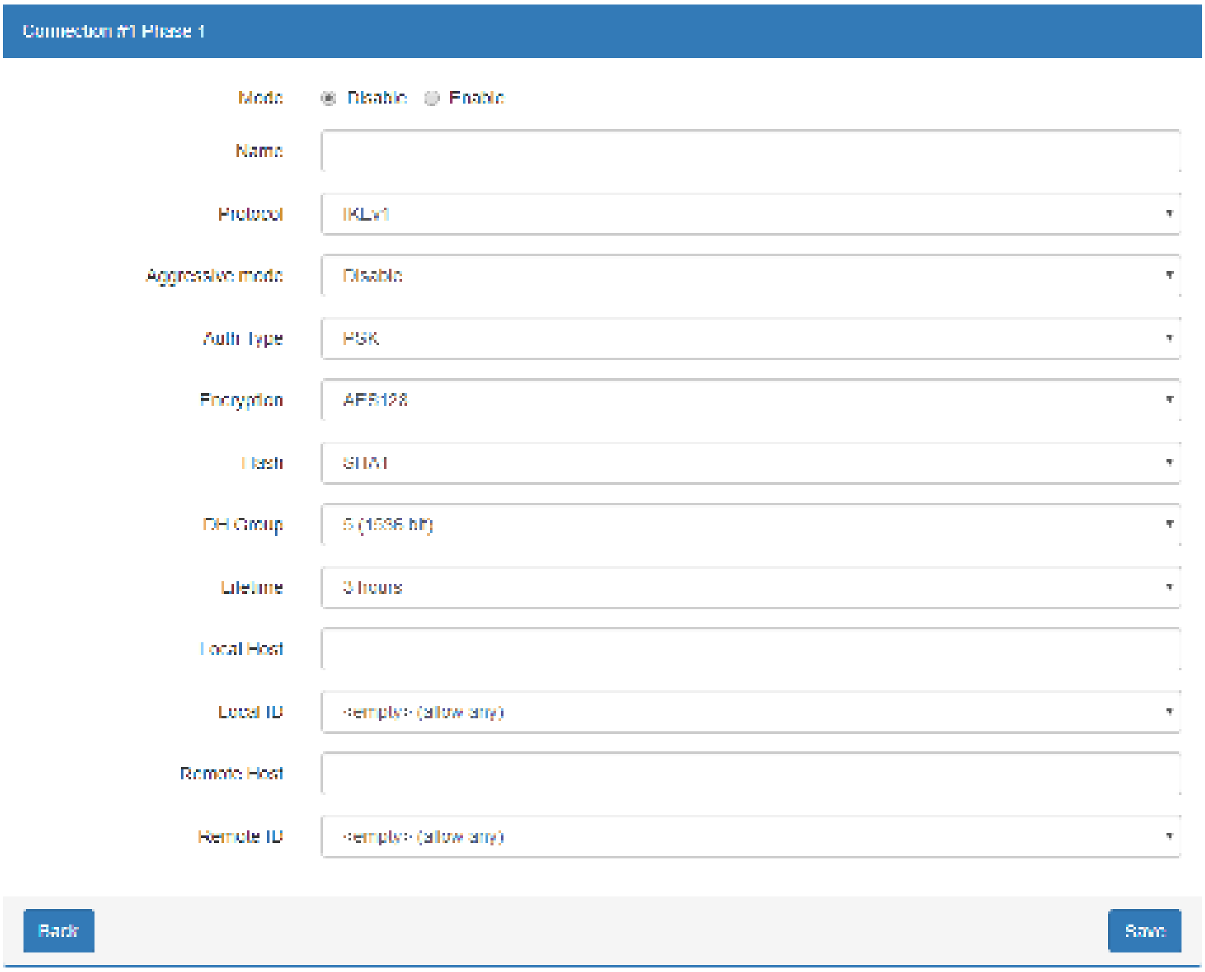
Type ● Policy-based ○ Route-based

- ● : IPsec SA active and link up
- ● : Only IPsec SA active
- ○ : Connecting
- ● : IPsec SA inactive
- ● : Disabled

- Phase 1 : Edit IPsec Phase 1 setting
- Phase 2 : Edit IPsec Phase 2 setting
- ··· : Edit IPsec Advance setting

□	#	Name	State	IKE information	Tunnel information		
□	1		●	Phase 1		Phase 2	···

(1) IPsec Phase 1 Setting



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)

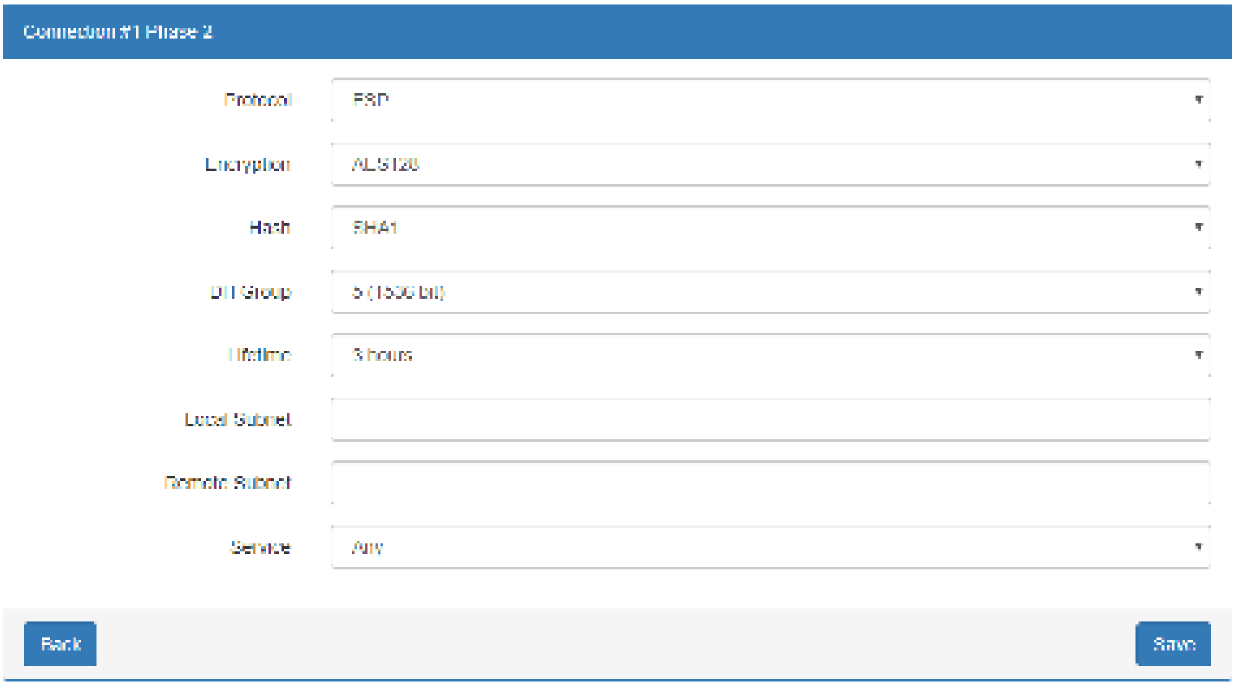
Remote Host

Remote ID <empty> (allow any)

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



Connection #1 Phase 2

Protocol: ESP

Encryption: AES128

Hash: SHA1

DH Group: 5 (1536 bit)

Lifetime: 3 hours

Local Subnet:

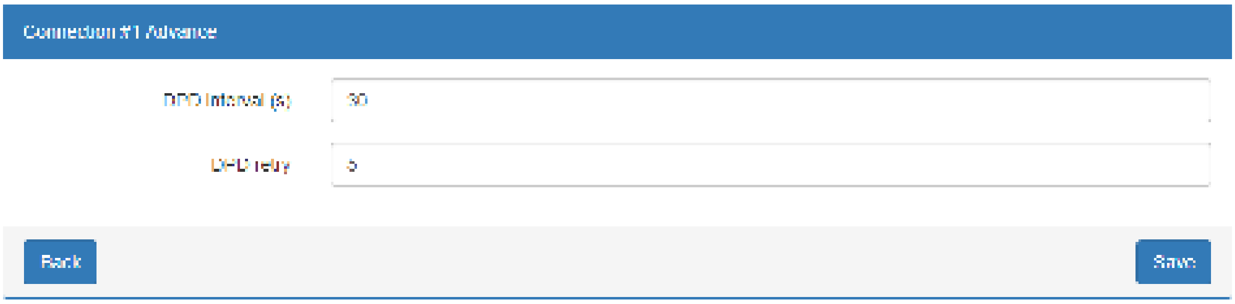
Remote Subnet:

Service: Any

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: (1) This option only work on Policy-based IPsec VPN type. (2) This option will be setup as 0.0.0.0/0 automatically on IPsec Route-based VPN. (3) This option will be omitted when the service option is L2TP. (For host-to-host connection only)
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:*** (1) This option only work on Policy-based IPsec VPN type. (2) This option will be setup as 0.0.0.0/0 automatically on IPsec Route-based VPN. (3) This option will be omitted when the service option is L2TP. (for host-to-host connection only)
Service	Restrict the VPN traffic to the particular protocol only. Select from the Any, TCP, UDP or L2TP.

(3) IPsec Advance Setting



Connection #1 Advance

DPD interval (s): 30

DPD retry: 5

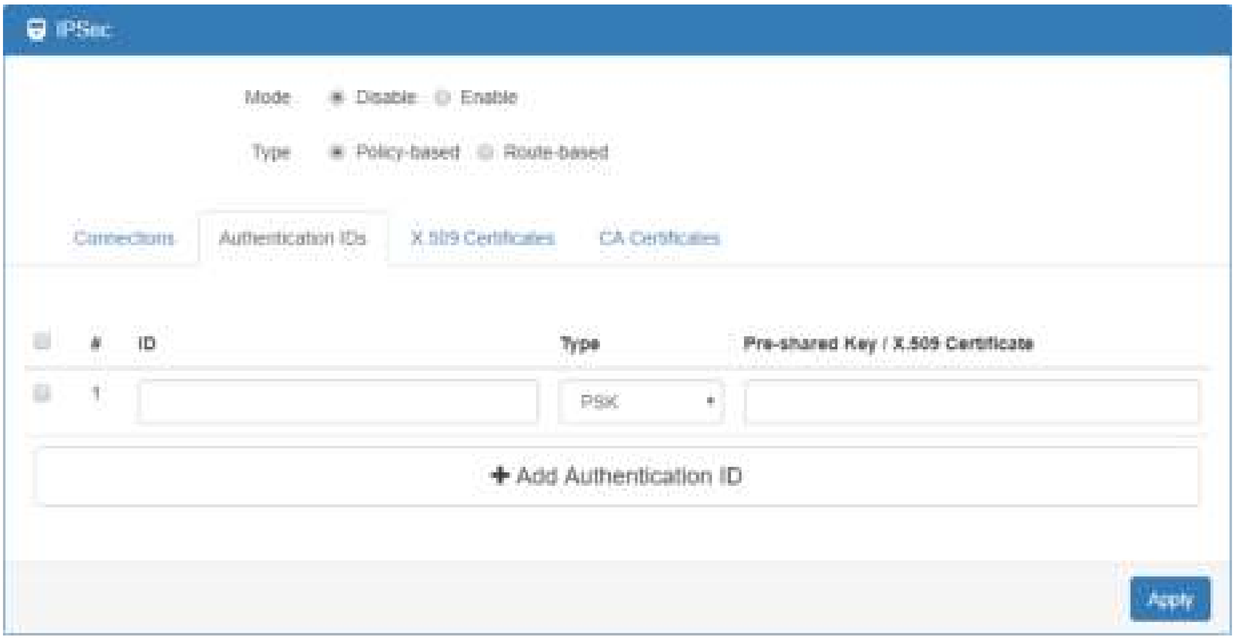
VPN > IPsec > Connections > Advance Setting	
Item	**Description**
DPD interval	The period time interval to detect dead peers. The default is 30 seconds.
DPD retry	The max number of retry of dead peer detection. The default is 5 times.

11.2.2 IPsec > Authentication IDs

This section provides the authenticaion 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.



IPSec

Mode ● Disable ○ Enable

Type ● Policy-based ○ Route-based

□	#	ID	Type	Pre-shared Key / X.509 Certificate
□	1		PSK	

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.

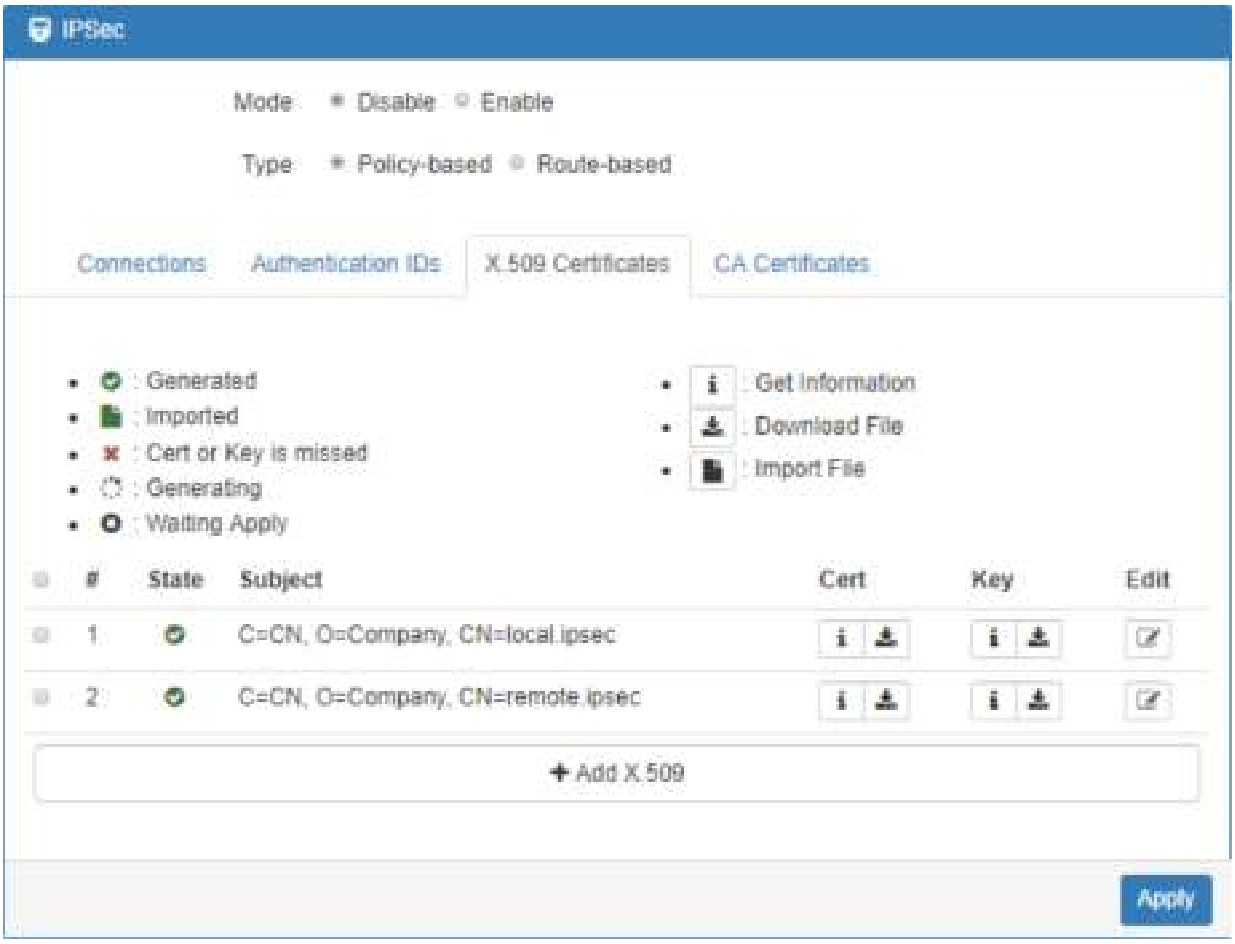
VPN > IPsec > Authentication IDs				
#	**ID**	**Type**	**Pre-shared Key / X.509 Certificate**	**Comment**
1		PSK	password	The default password for the PSK connections.
2	remote.IPsec	PSK	2wsx#EDC	The password only for the PSK connection with **remote.IPsec** ID. Normally, this case will be used to authenticate peer gateway.
3	local.IPsec	PSK		The identification for the connection. Normally, this case will be used to announe 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**.



IPSec

Mode ● Disable ○ Enable

Type ● Policy-based ○ Route-based

- ✓ : Generated
- ▮ : Imported
- ✖ : Cert or Key is missed
- ◌ : Generating
- ○ : Waiting Apply

- i : Get Information
- ⬇ : Download File
- ▮ : Import File

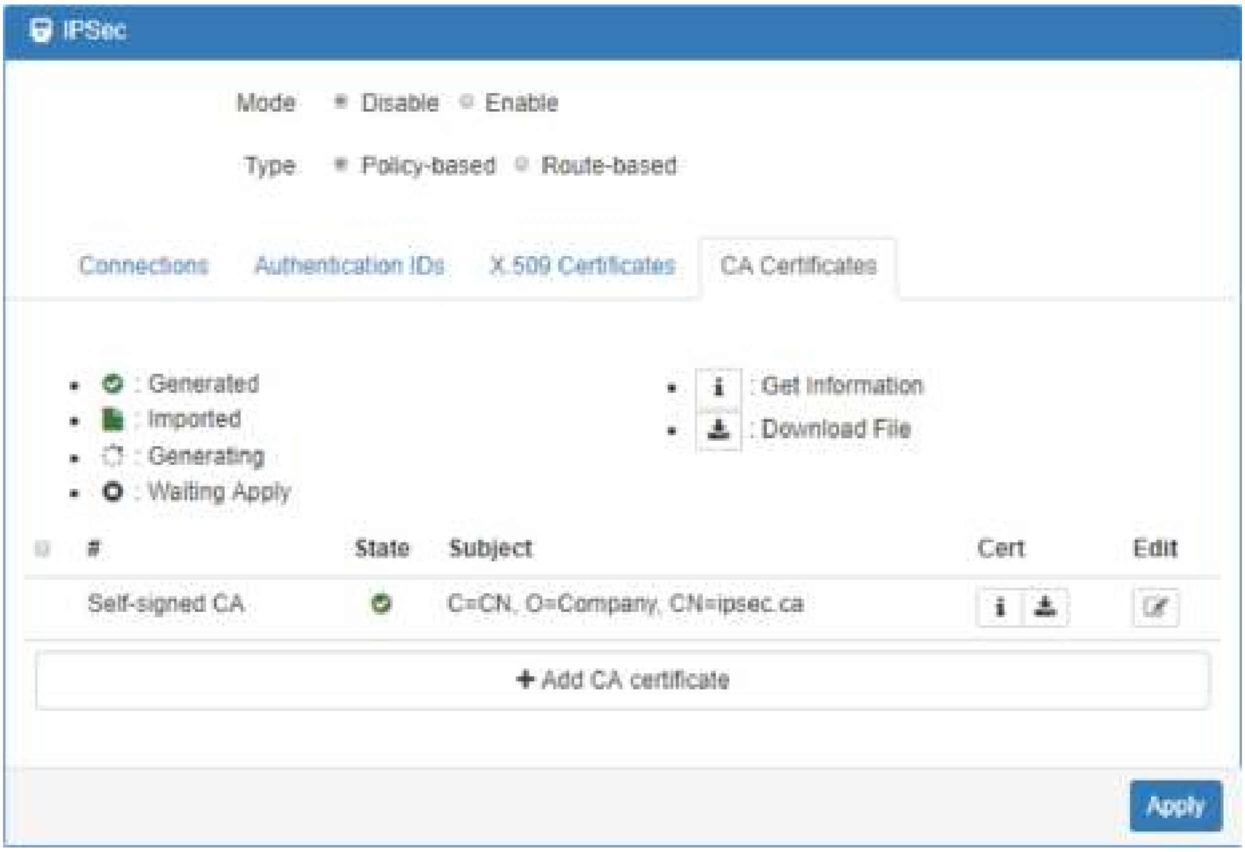
□	#	State	Subject	Cert	Key	Edit
□	1	✓	C=CN, O=Company, CN=local.ipsec	i ⬇	i ⬇	✎
□	2	✓	C=CN, O=Company, CN=remote.ipsec	i ⬇	i ⬇	✎

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.


IPSec

Mode ● Disable ○ Enable

Type ● Policy-based ○ Route-based

- ✓ : Generated
- ▨ : Imported
- ◌ : Generating
- ○ : Waiting Apply

- ℹ : Get Information
- ⭳ : Download File

□	#	State	Subject	Cert	Edit
	Self-signed CA	✓	C=CN, O=Company, CN=ipsec.ca	ℹ ⭳	✎

Certificate Generation

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

To generate the self-signed CA certificate:

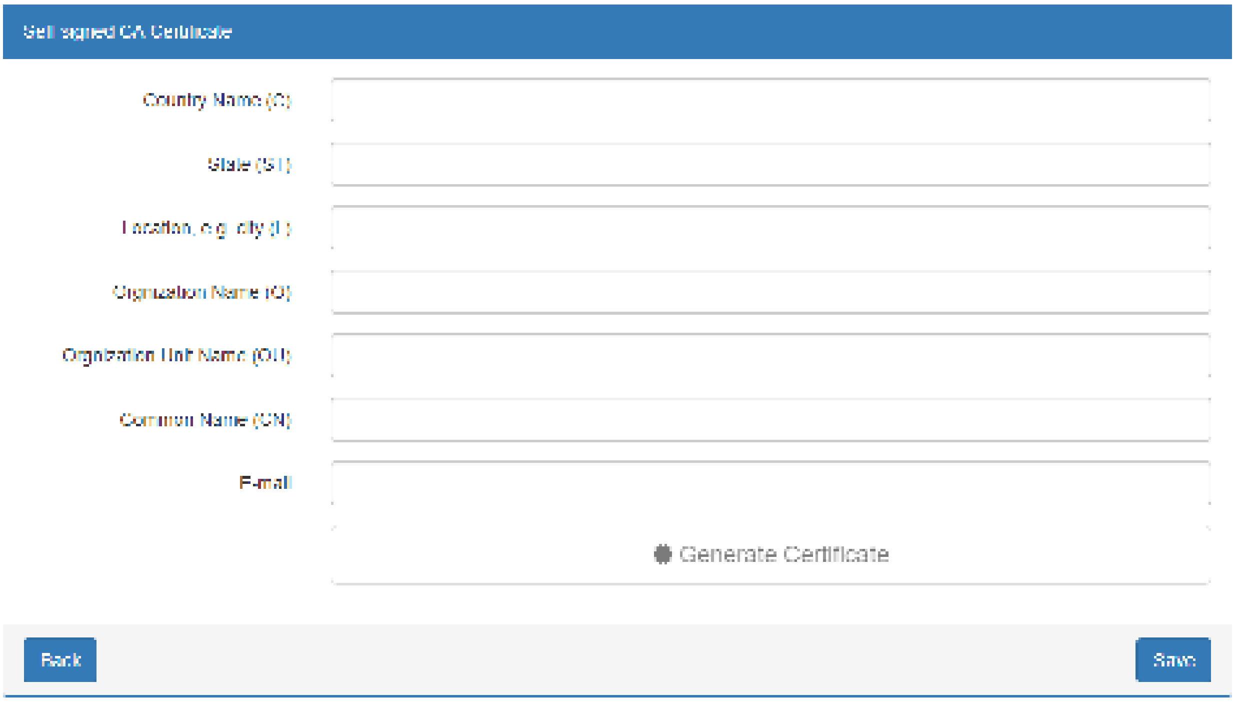
1. Navigate to CA Certificates tab.
2. Click the ✎ edit button to navigate the **Certificate Setting** page.
3. Fill up the informations of the CA certificate.
4. Click the Generate Certificate button and Save.
5. Click the Apply button to apply the changes.

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 informations 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
Orgnization Name	The orgnization name. e.g. company-name This option is required for certificate generation.
Orgnization Unit Name	The orgnization 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 support 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 shown 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 balnk 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.

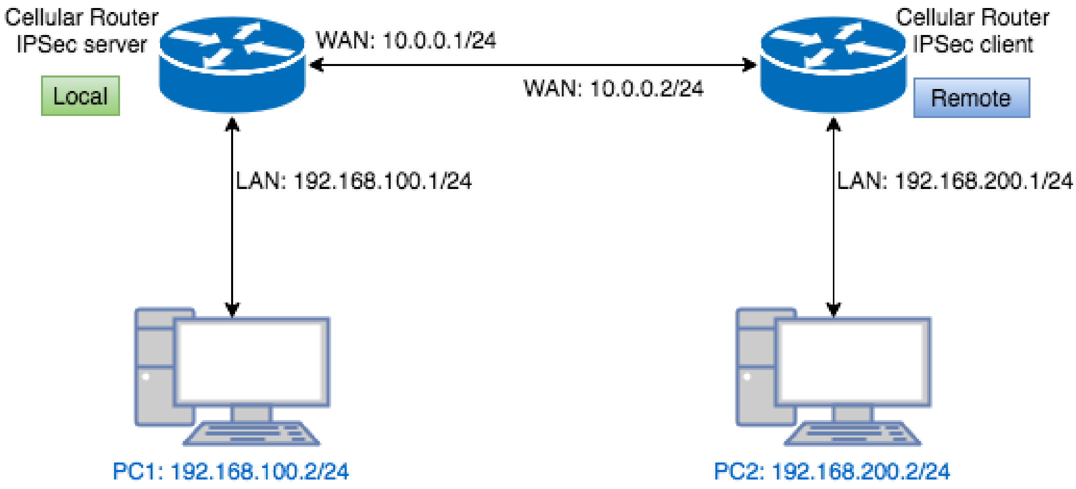
How to download the certificate

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.

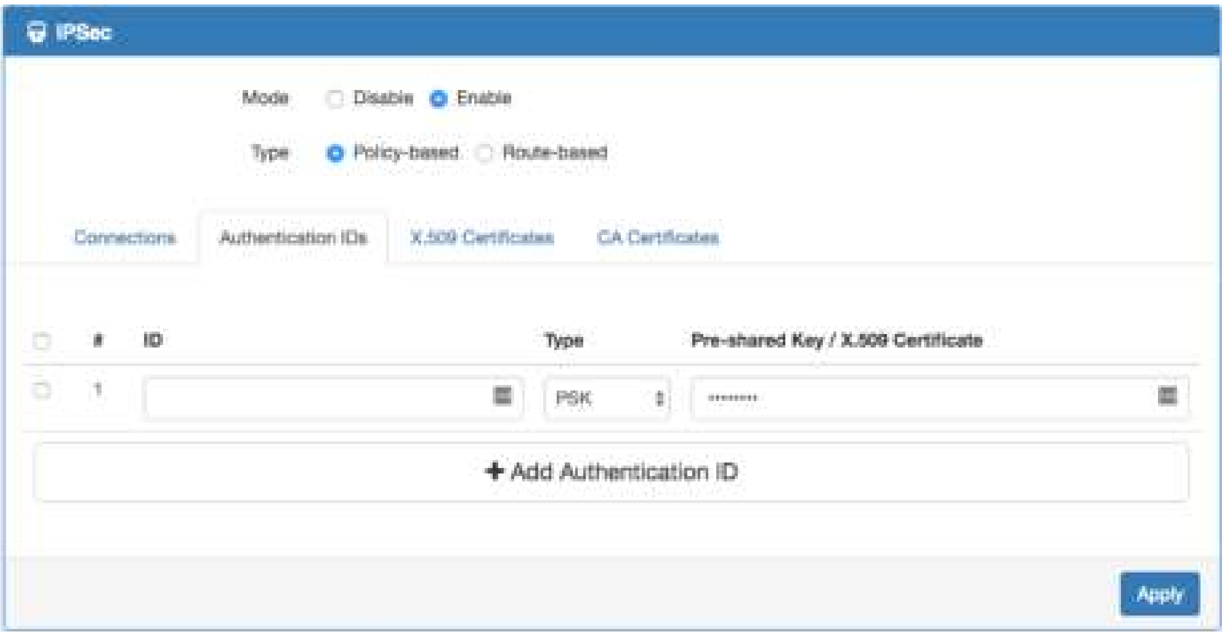


- **Pre-shared Key authentication**

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

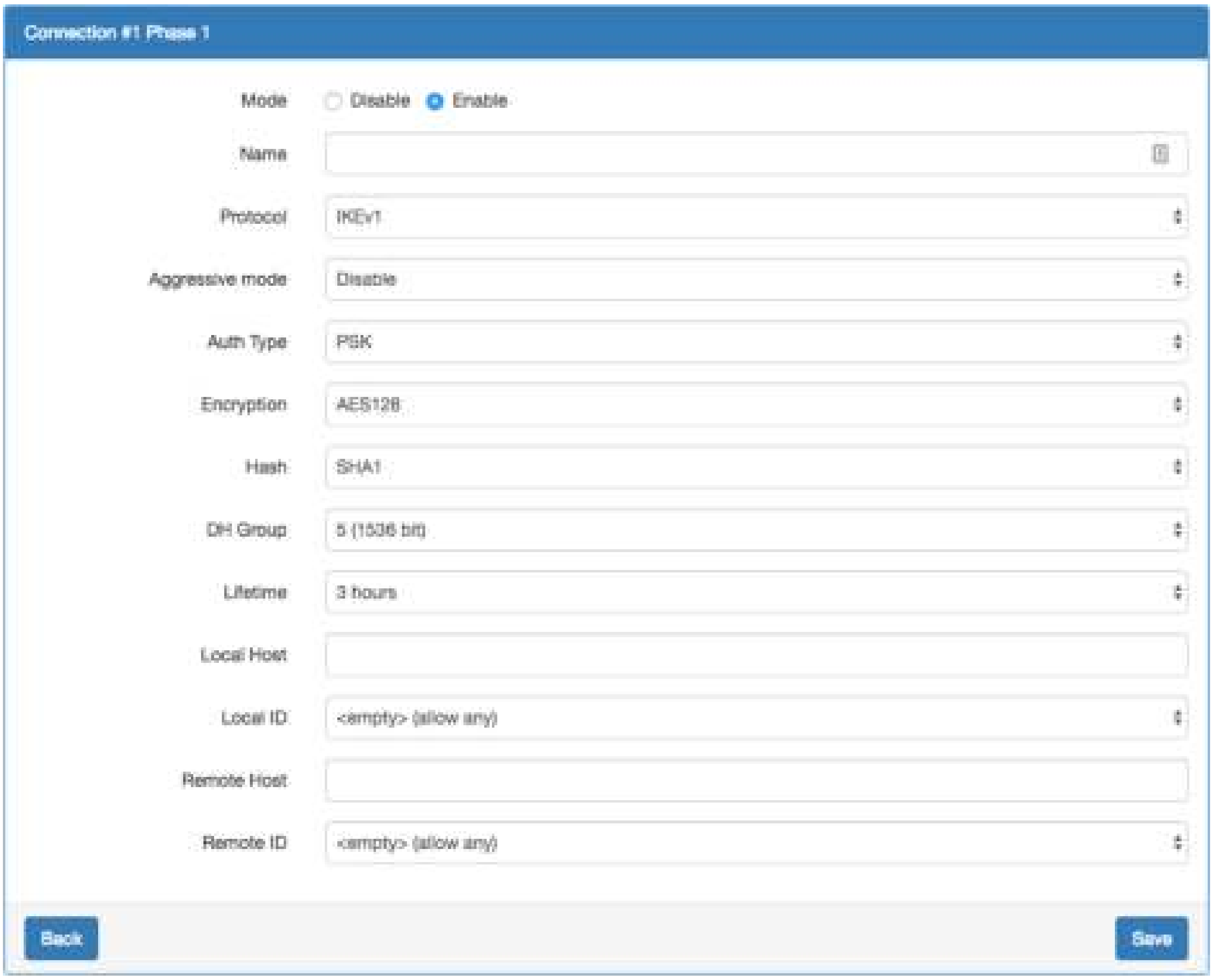
5. Navigate to the Connections tab.
6. Add IPsec connection
   (1) Edit the phase 1 setting
   (2) Change **Mode** from Disable to **Enable**.
   (3) Save the changes.
   (4) Edit the phase 2 setting
   (5) Fill up the **Local Subnet** and **Remote Subnet**.
      - e.g. Local Subnet: 192.168.100.0/24,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



Mode ○ Disable ● Enable

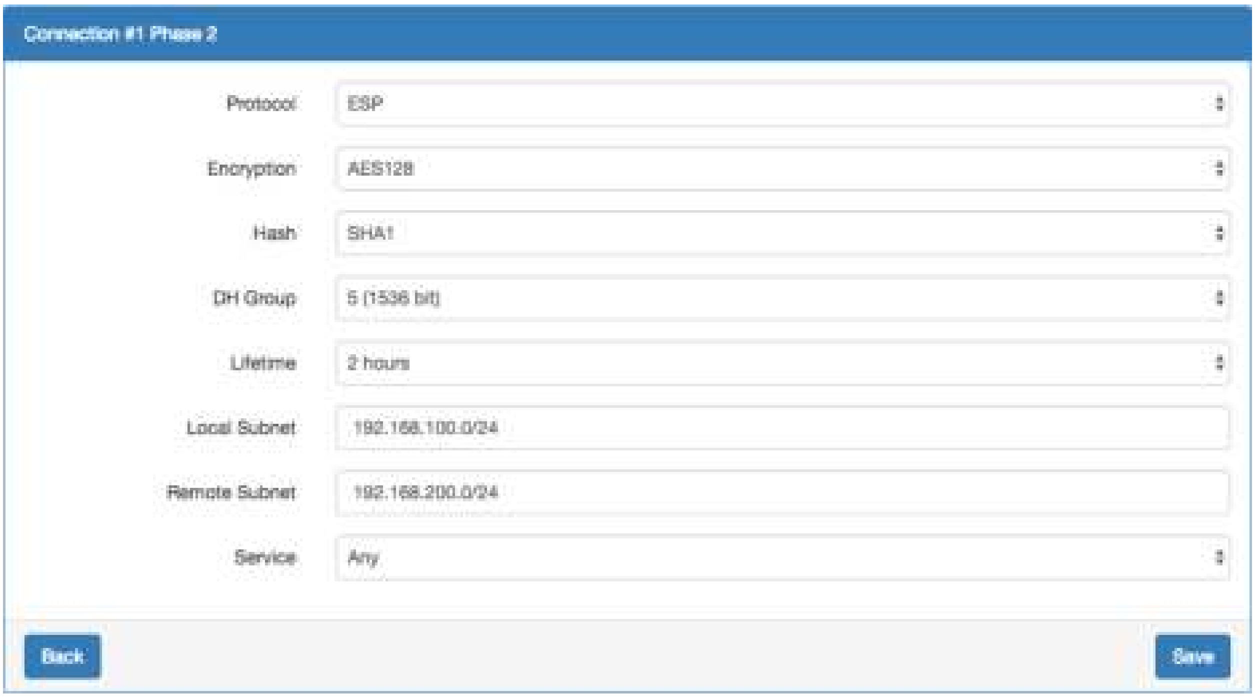
Type ● Policy-based ○ Route-based

□	#	ID	Type	Pre-shared Key / X.509 Certificate
□	1		PSK	********



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)

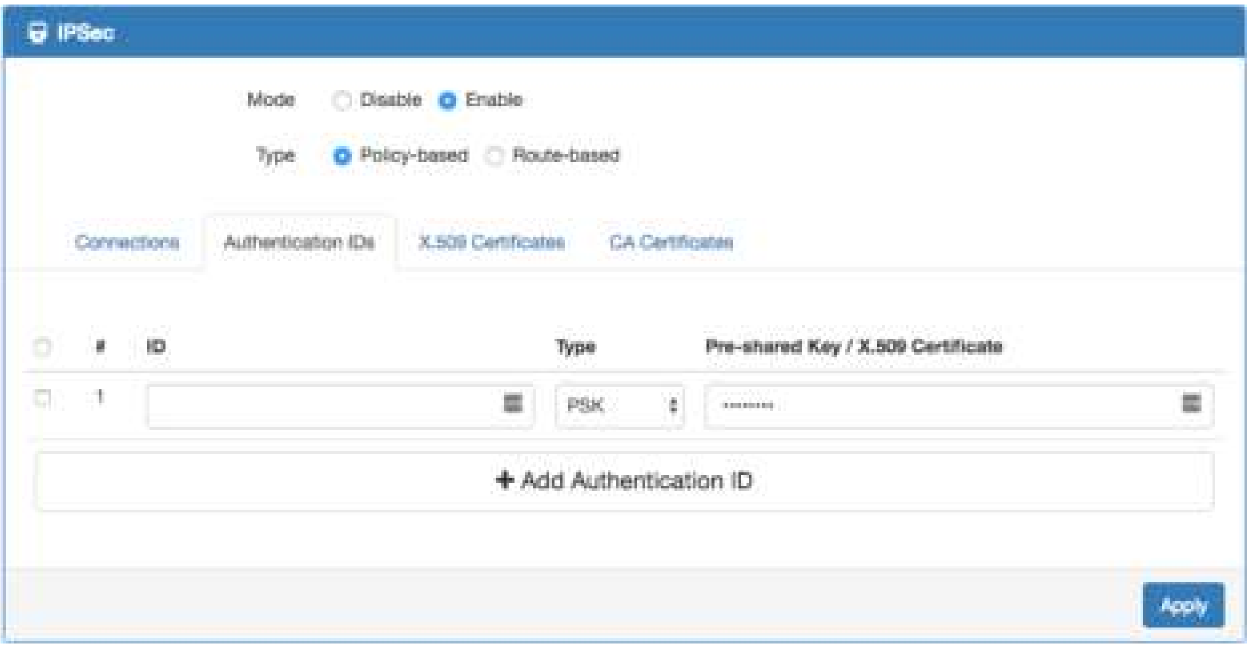


Connection #1 Phase 2

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

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



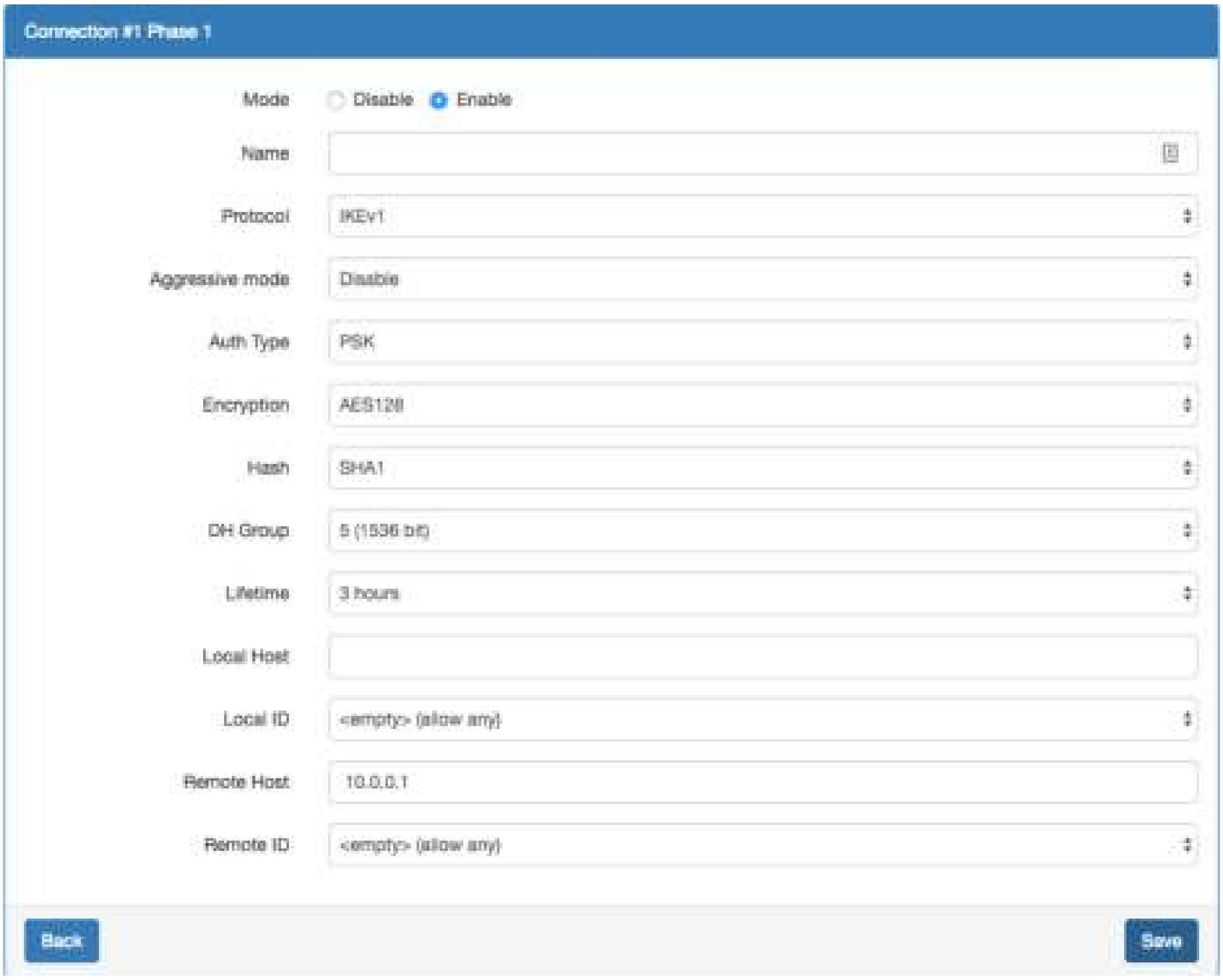
IPSec

Mode ○ Disable ● Enable

Type ● Policy-based ○ Route-based

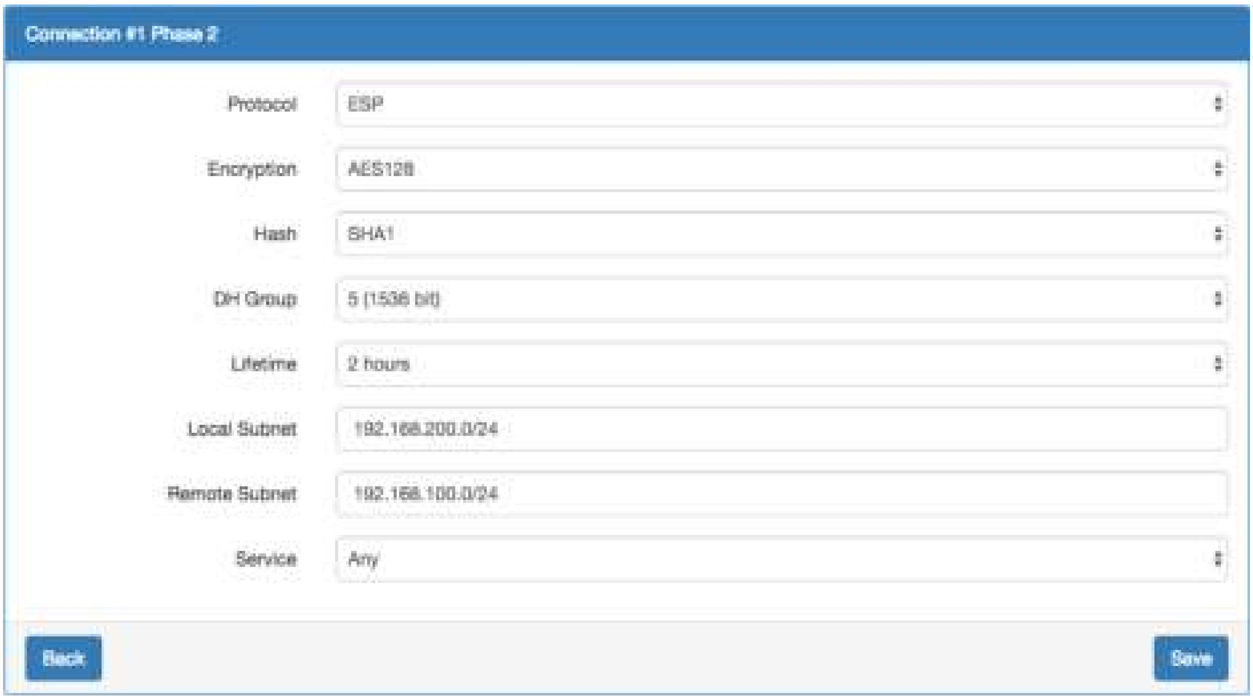
Connections | Authentication IDs | X.509 Certificates | CA Certificates

□	#	ID	Type	Pre-shared Key / X.509 Certificate
□	1		PSK	••••••••



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)

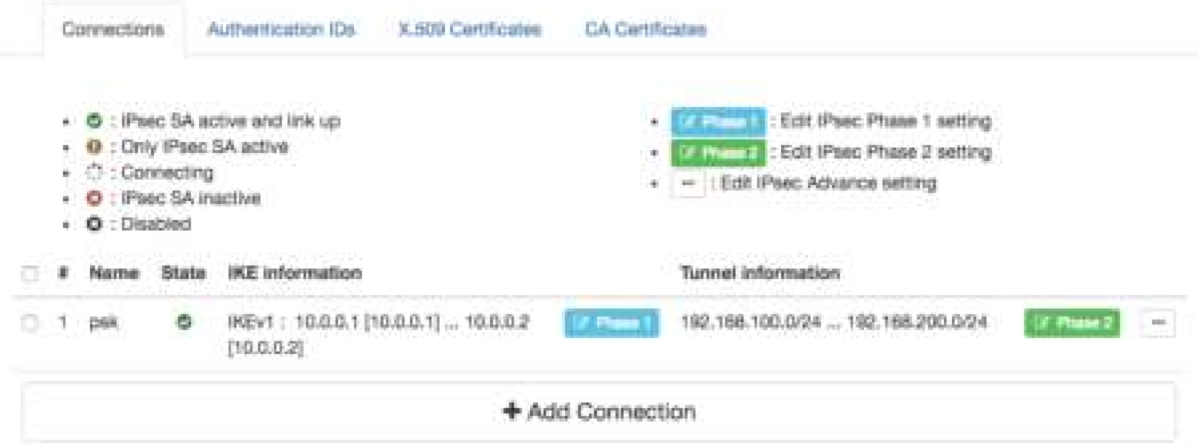


Connection #1 Phase 2

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

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

- Server



Connections | Authentication IDs | X.509 Certificates | CA Certificates

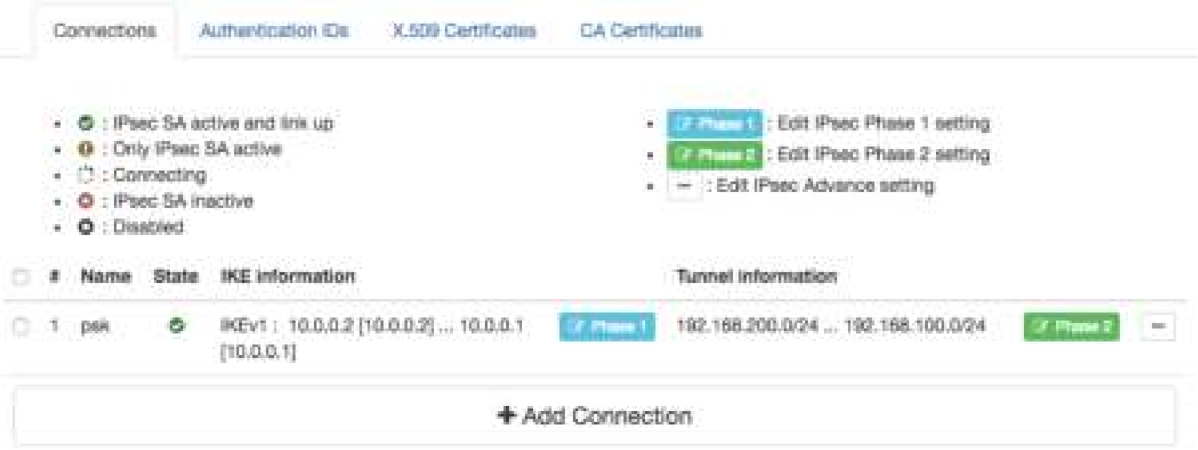
- ● : IPsec SA active and link up
- ● : Only IPsec SA active
- ○ : Connecting
- ● : IPsec SA inactive
- ● : Disabled

- Phase 1 : Edit IPsec Phase 1 setting
- Phase 2 : Edit IPsec Phase 2 setting
- — : Edit IPsec Advance setting

□	#	Name	State	IKE information		Tunnel information		
□	1	psk	●	IKEv1 : 10.0.0.1 [10.0.0.1] ... 10.0.0.2 [10.0.0.2]	Phase 1	192.168.100.0/24 ... 192.168.200.0/24	Phase 2	—

+ Add Connection

- Client



Connections | Authentication IDs | X.509 Certificates | CA Certificates

- ● : IPsec SA active and link up
- ● : Only IPsec SA active
- ○ : Connecting
- ● : IPsec SA inactive
- ● : Disabled

- Phase 1 : Edit IPsec Phase 1 setting
- Phase 2 : Edit IPsec Phase 2 setting
- — : Edit IPsec Advance setting

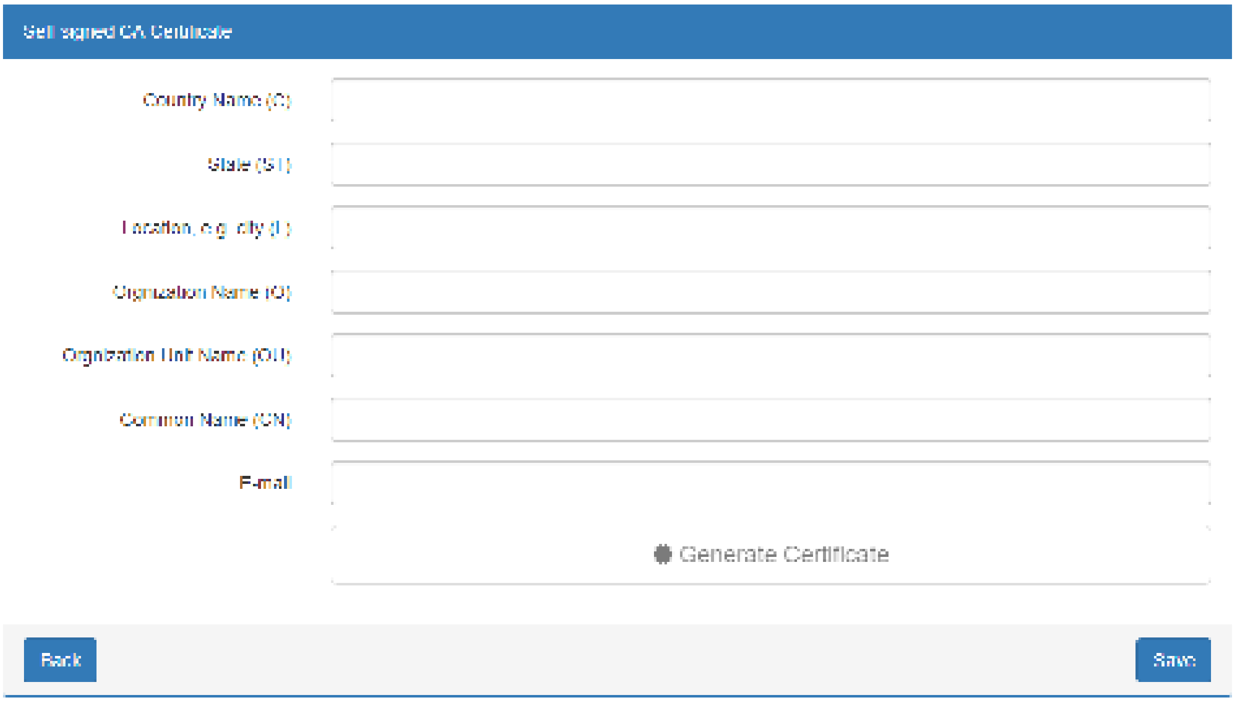
□	#	Name	State	IKE information		Tunnel information		
□	1	psk	●	IKEv1 : 10.0.0.2 [10.0.0.2] ... 10.0.0.1 [10.0.0.1]	Phase 1	192.168.200.0/24 ... 192.168.100.0/24	Phase 2	—

+ Add Connection

- **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) **Orgnization 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



Self-signed CA Certificate

Country Name (C)

State (ST)

Location, e.g. city (L)

Orgnization Name (O)

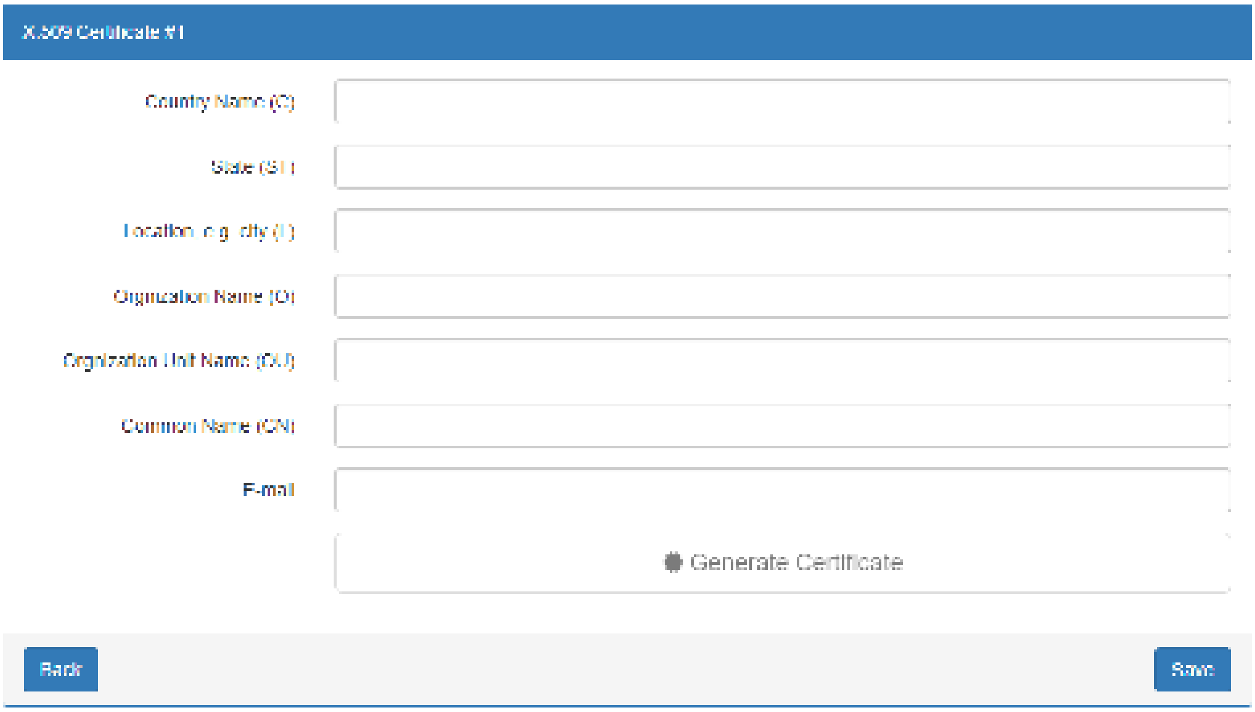
Orgnization Unit Name (OU)

Common Name (CN)

E-mail

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) **Orgnization 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) **Orgnization 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



X.509 Certificate #1

Country Name (C)

State (ST)

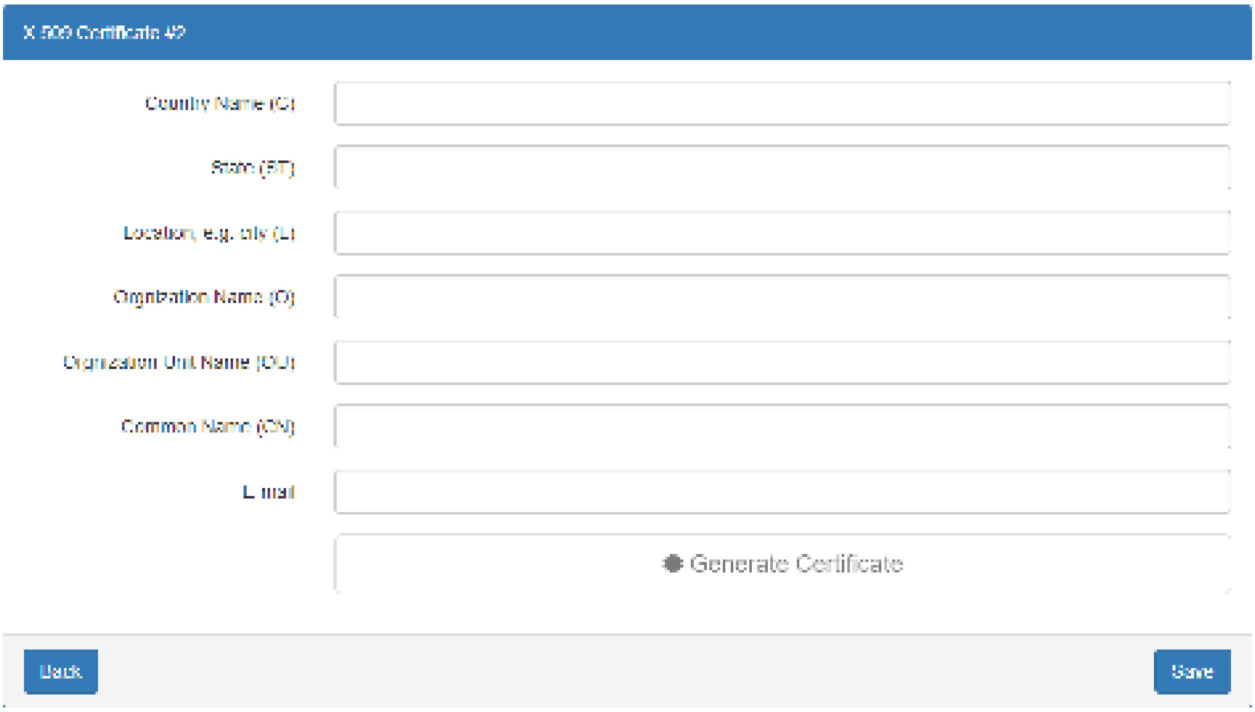
Location, e.g. city (L)

Orgnization Name (O)

Orgnization Unit Name (OU)

Common Name (CN)

E-mail



X.509 Certificate #2

Country Name (C)

State (ST)

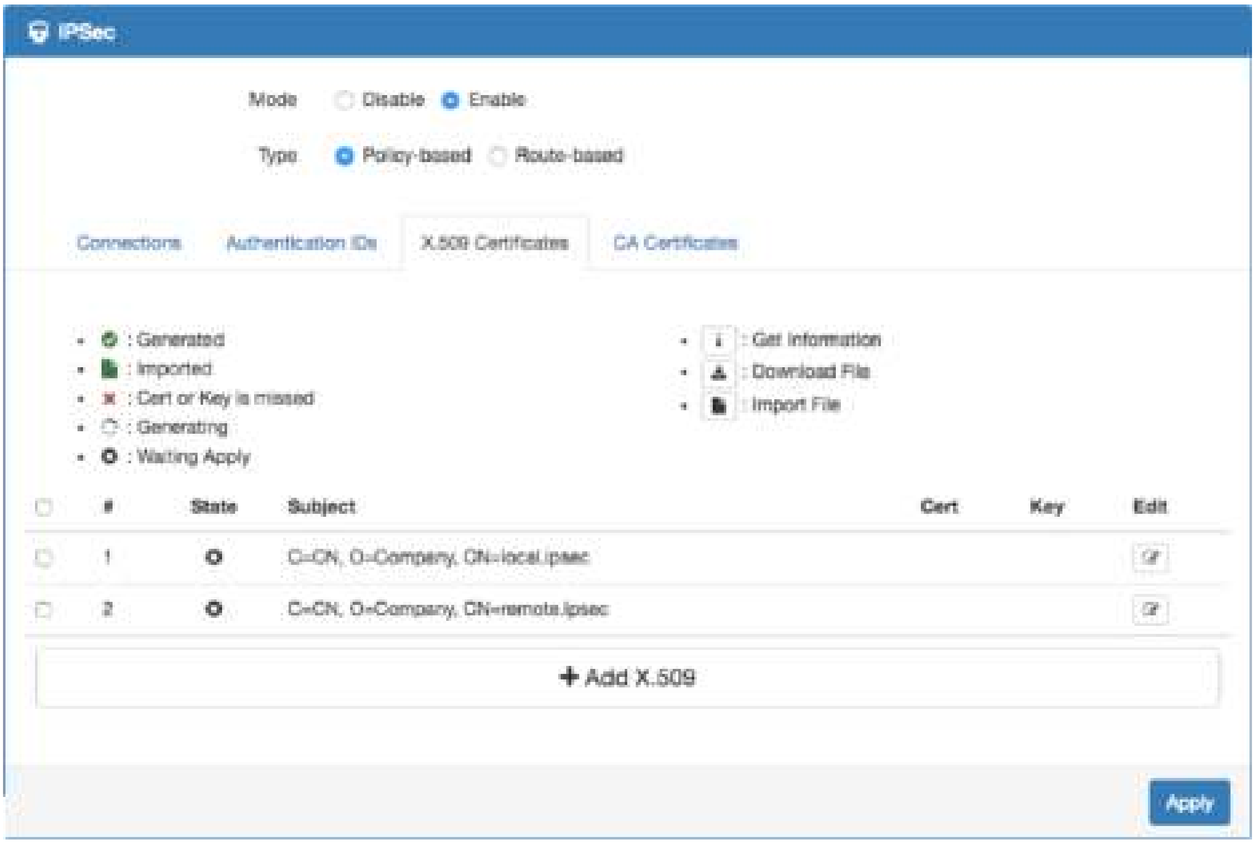
Location, e.g. city (L)

Orgnization Name (O)

Orgnization Unit Name (OU)

Common Name (CN)

E-mail



IPSec

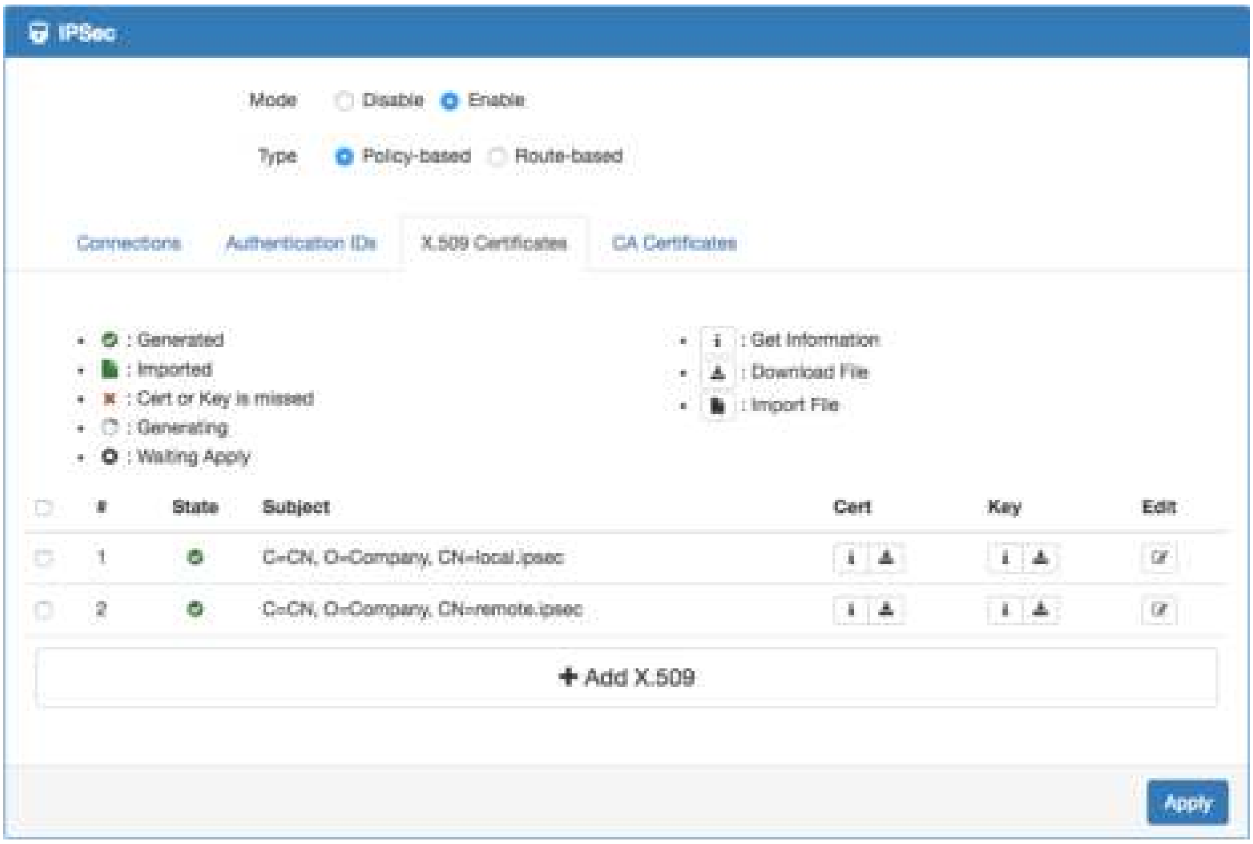
Mode ○ Disable ● Enable

Type ● Policy-based ○ Route-based

- ✓ : Generated
- ▮ : Imported
- ✗ : Cert or Key is missed
- ◌ : Generating
- ⚙ : Waiting Apply

- i : 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			✎



IPSec

Mode ○ Disable ● Enable

Type ● Policy-based ○ Route-based

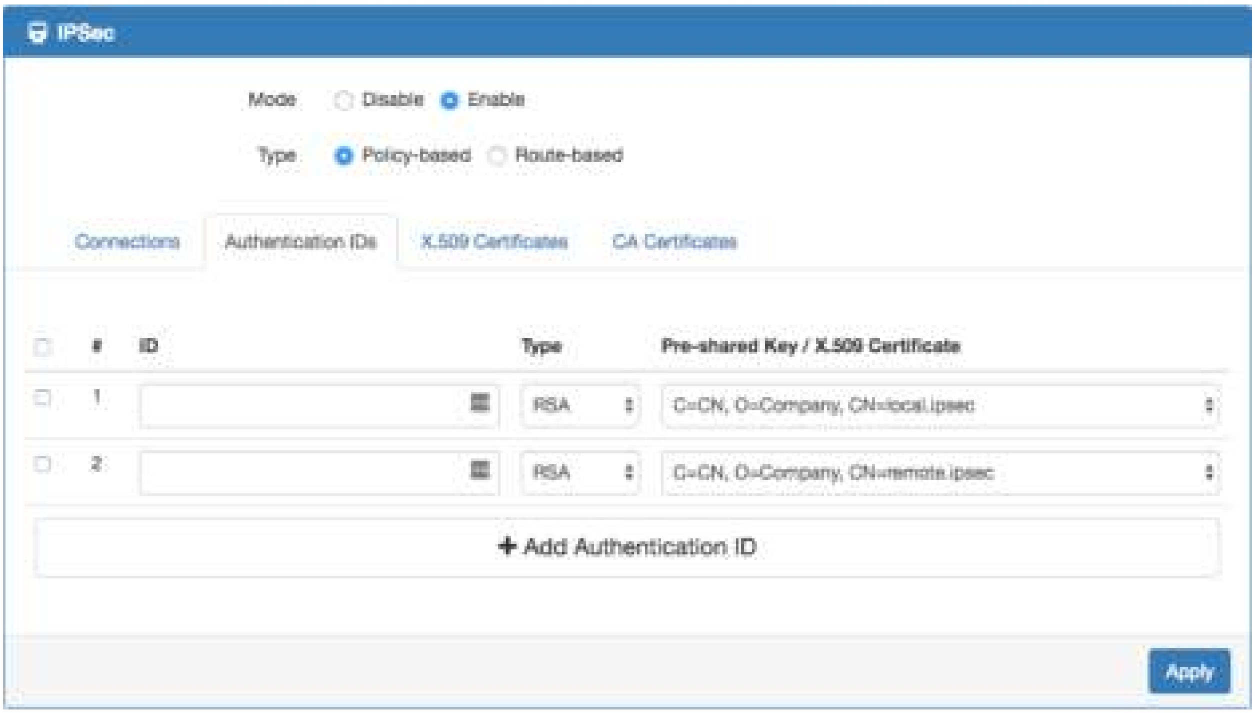
- ✓ : Generated
- ▮ : Imported
- ✗ : Cert or Key is missed
- ◌ : Generating
- ⚙ : Waiting Apply

- i : Get Information
- ⬇ : Download File
- ▮ : Import File

□	#	State	Subject	Cert	Key	Edit
□	1	✓	C=CN, O=Company, CN=local.ipsec	i ⬇	i ⬇	✎
□	2	✓	C=CN, O=Company, CN=remote.ipsec	i ⬇	i ⬇	✎

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



IPSec

Mode ○ Disable ● Enable

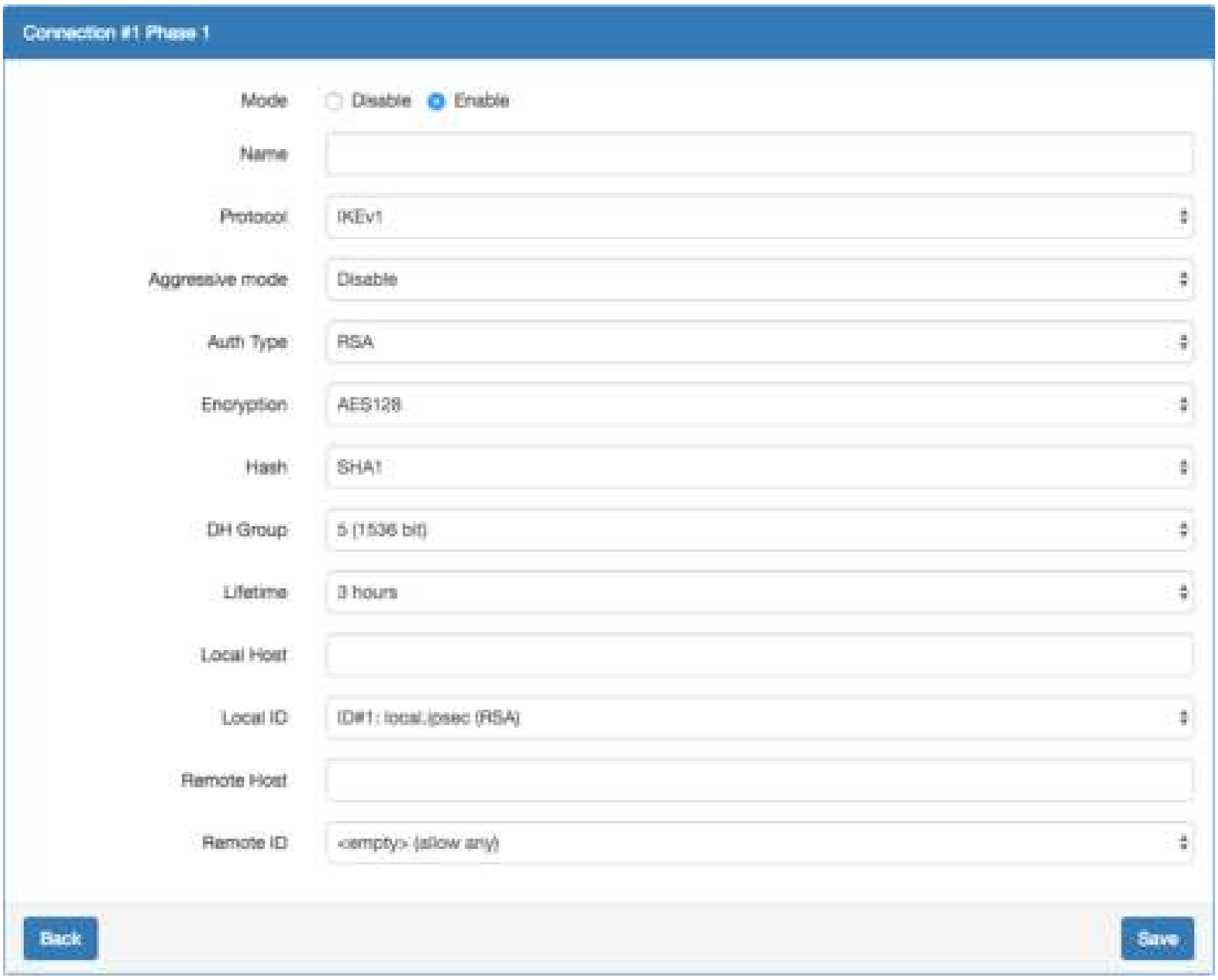
Type ● Policy-based ○ Route-based

□	#	ID	Type	Pre-shared Key / X.509 Certificate
□	1		RSA	C=CN, O=Company, CN=local.ipsec
□	2		RSA	C=CN, O=Company, CN=remote.ipsec

Setup the connection on VPN server

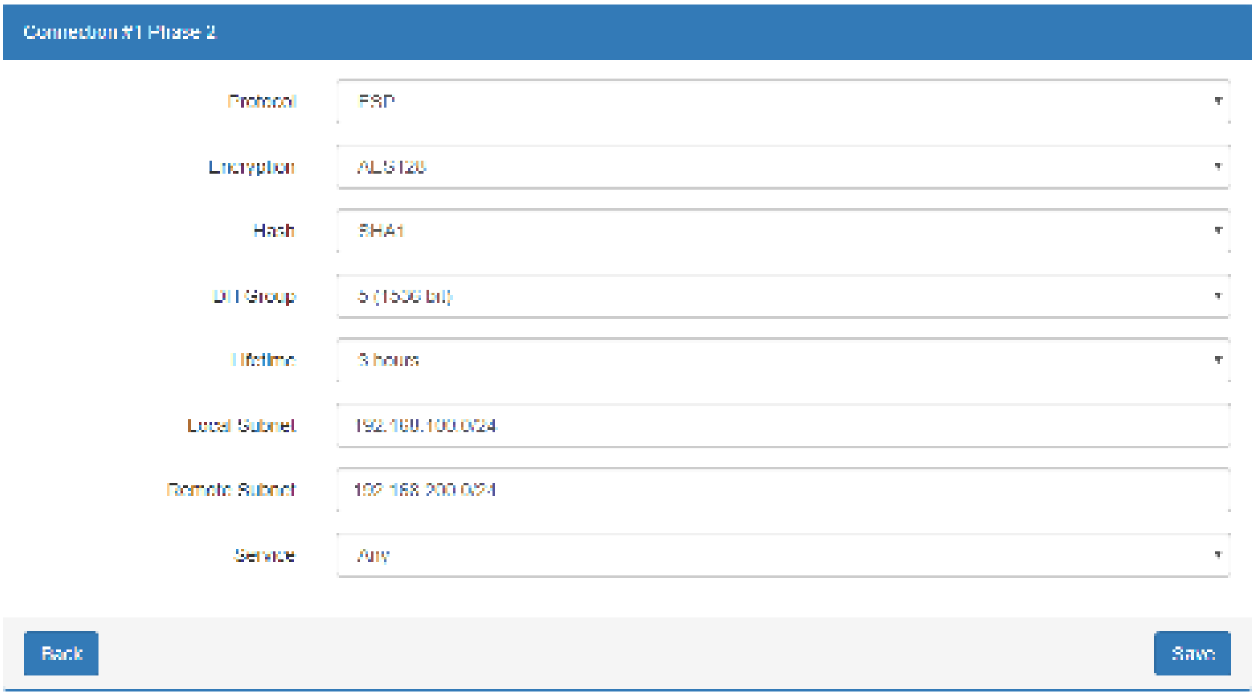
1. Change **Mode** from Disable to **Enable**.
2. Navigate to the Connections tab.
3. Add IPsec connection
   (1) Edit the phase 1 setting
   (2) Change **Mode** from Disable to **Enable**.
   (3) Change **Auth Type** from PSK to **RSA**.
   (4) Change the **Local ID** and select the **local.IPsec (RSA)** authenticaion 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)



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

- **RSA authentication – Client**

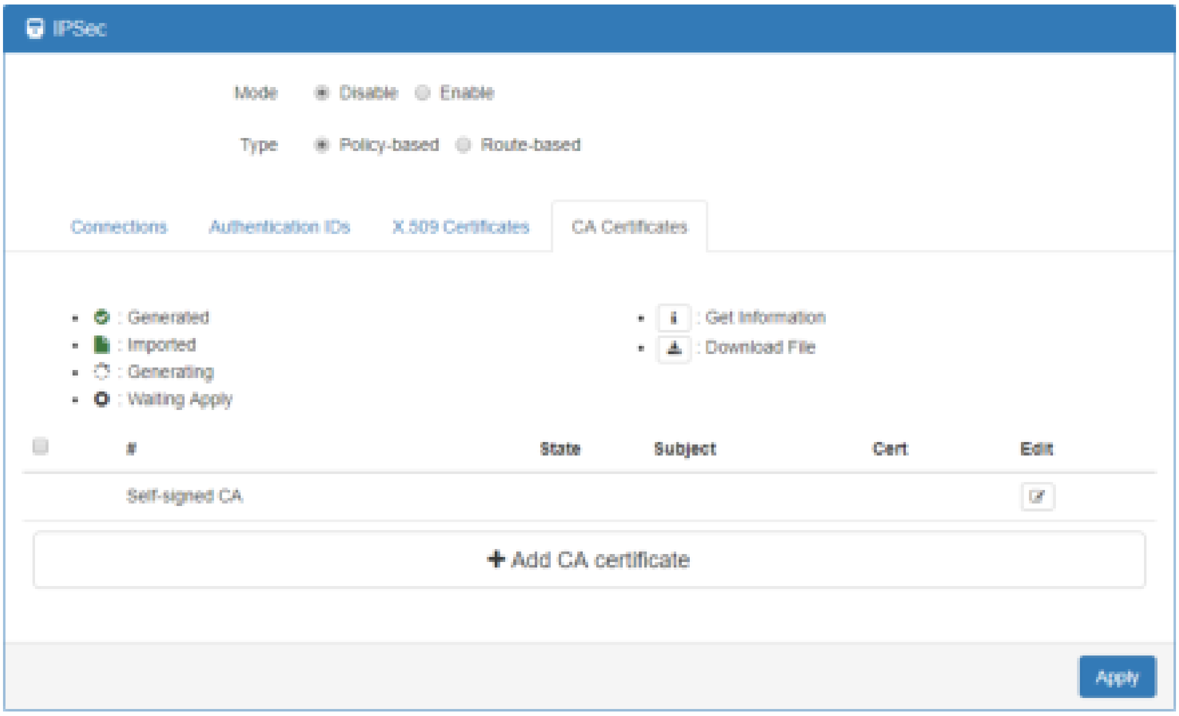
Prerequisite for VPN Client with RSA authentication

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.



IPSec

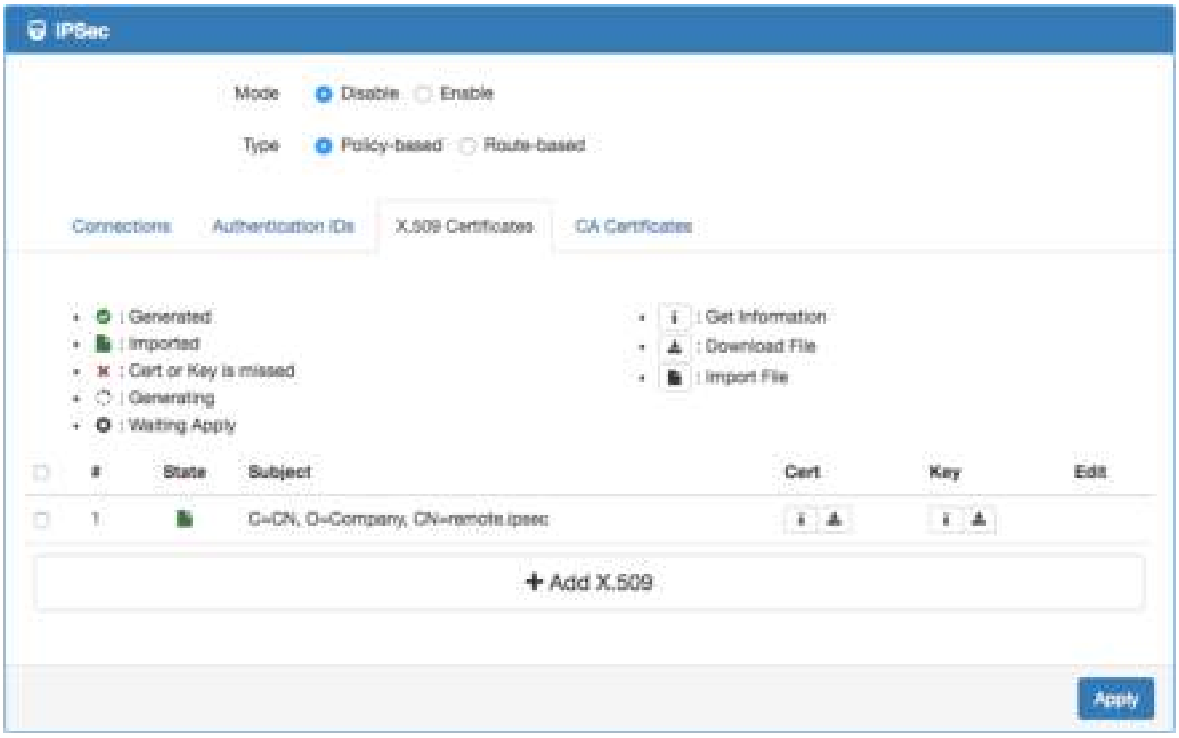
Mode ● Disable ○ Enable

Type ● Policy-based ○ Route-based

- ✓ : Generated
- ▮ : Imported
- ◌ : Generating
- ⚙ : Waiting Apply

- i : Get Information
- ⭳ : Download File

□	#	State	Subject	Cert	Edit
	Self-signed CA				✎



IPSec

Mode ● Disable ○ Enable

Type ● Policy-based ○ Route-based

- ✓ : Generated
- ▮ : Imported
- ✗ : Cert or Key is missed
- ◌ : Generating
- ⚙ : Waiting Apply

- i : Get Information
- ⭳ : Download File
- ▮ : Import File

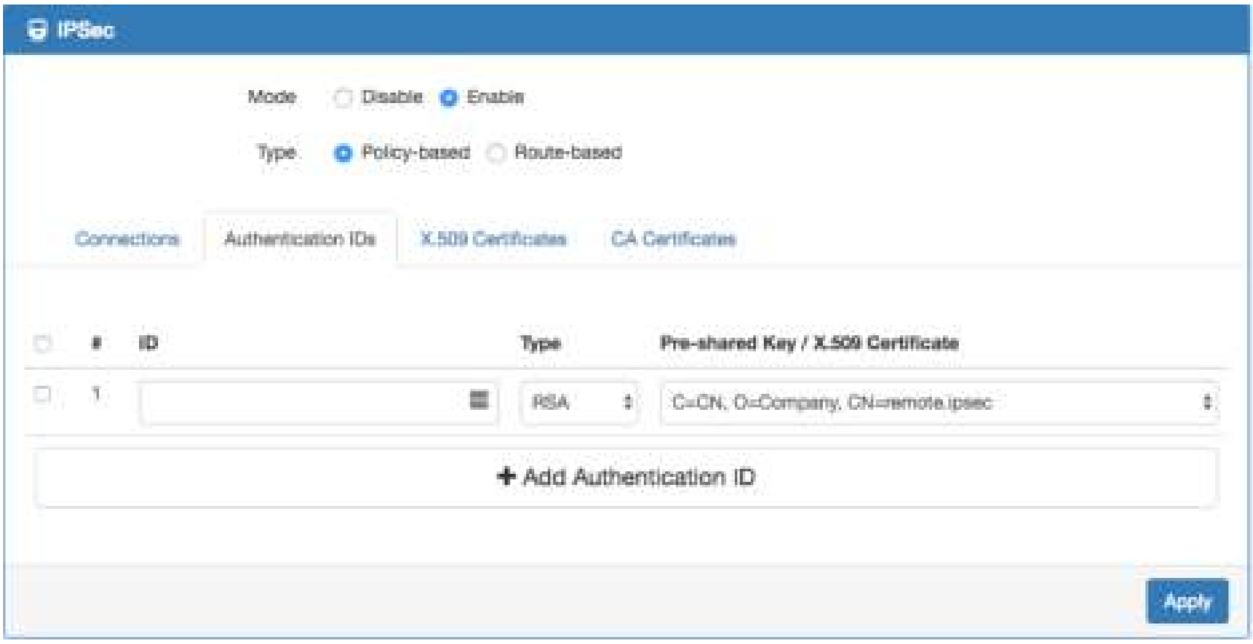
□	#	State	Subject	Cert	Key	Edit
□	1	▮	C=CN, O=Company, CN=remote.ipsec	i ⭳	i ⭳	

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)** authenticaion 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



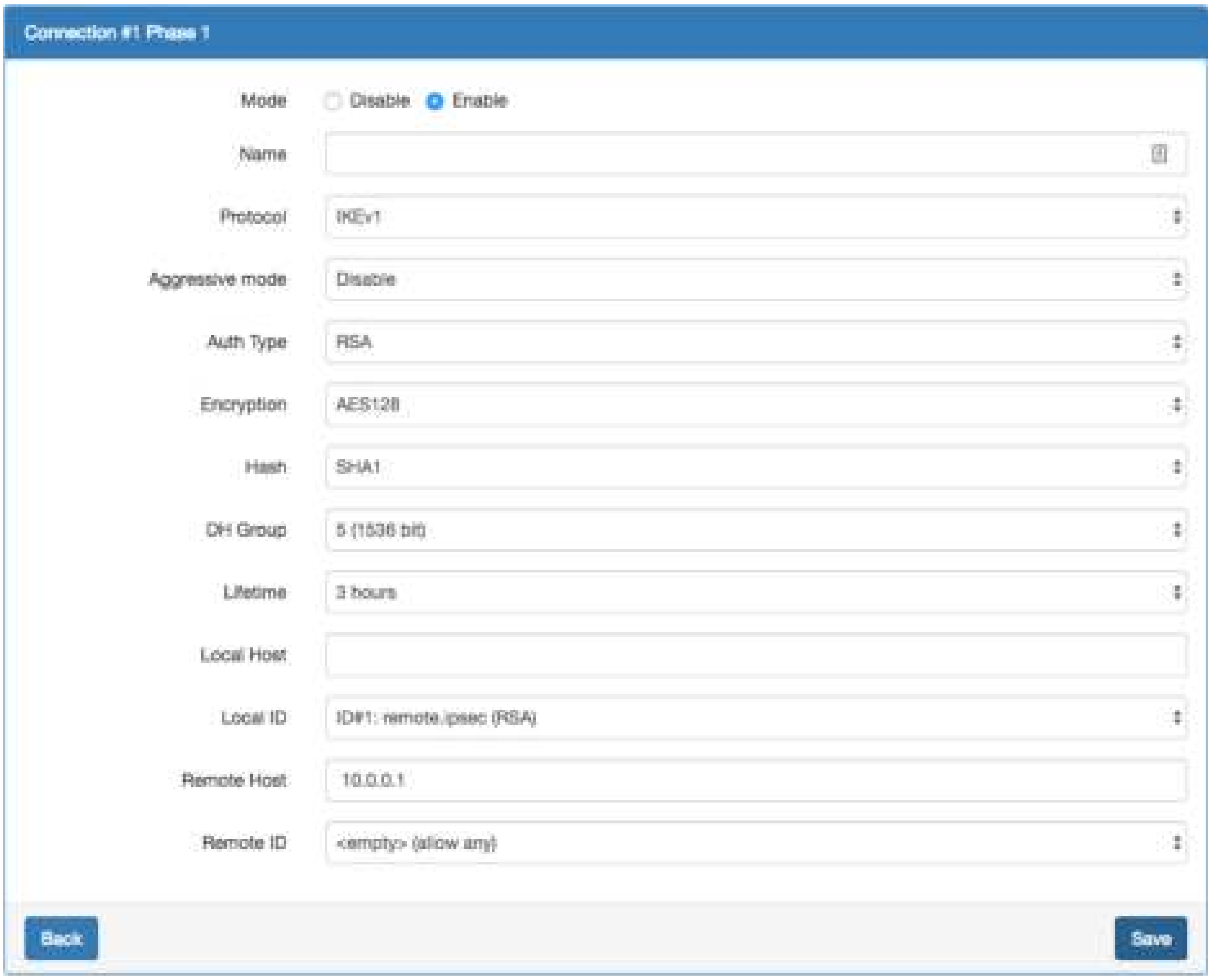
IPSec

Mode ○ Disable ● Enable

Type ● Policy-based ○ Route-based

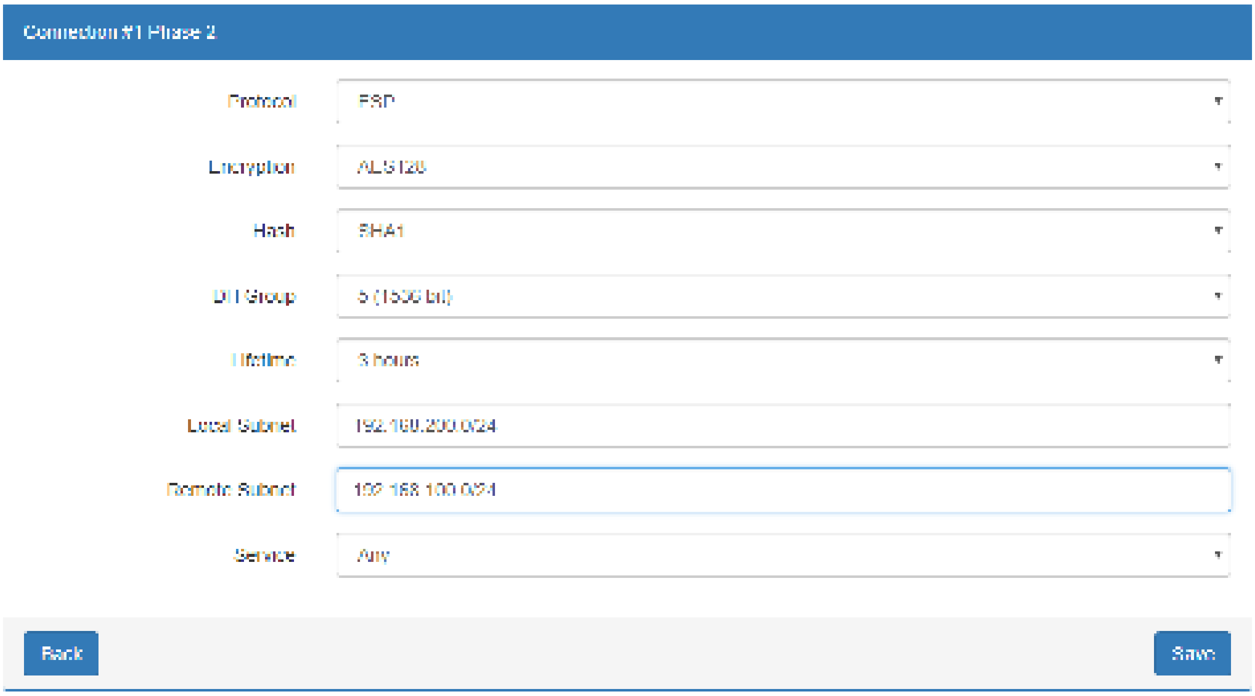
Connections | Authentication IDs | X.509 Certificates | CA Certificates

□	#	ID	Type	Pre-shared Key / X.509 Certificate
□	1		RSA	C=CN, O=Company, CN=remote.ipsec



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)

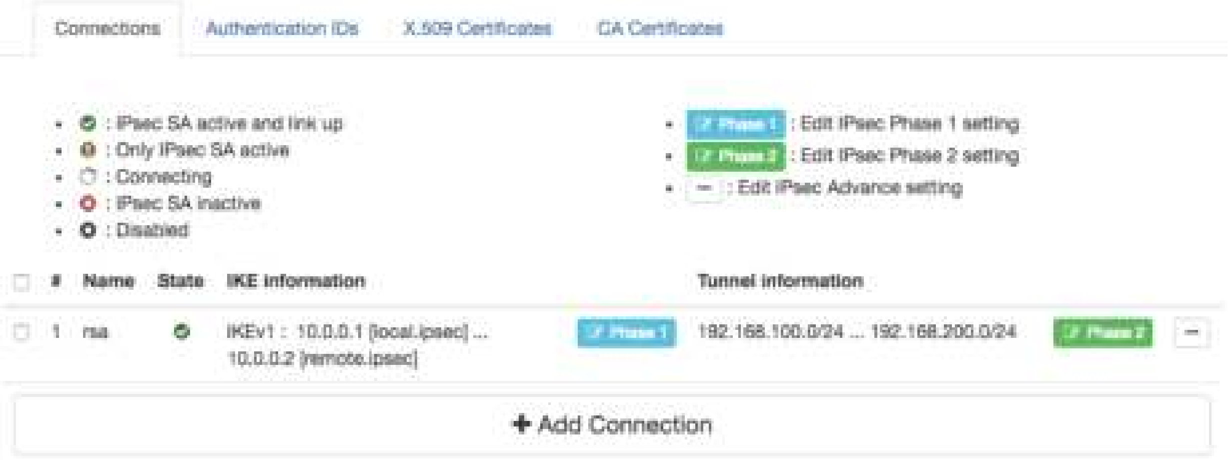


Connection #1 Phase 2

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

● IPsec Net-to-Net with RSA authentication result

- Server

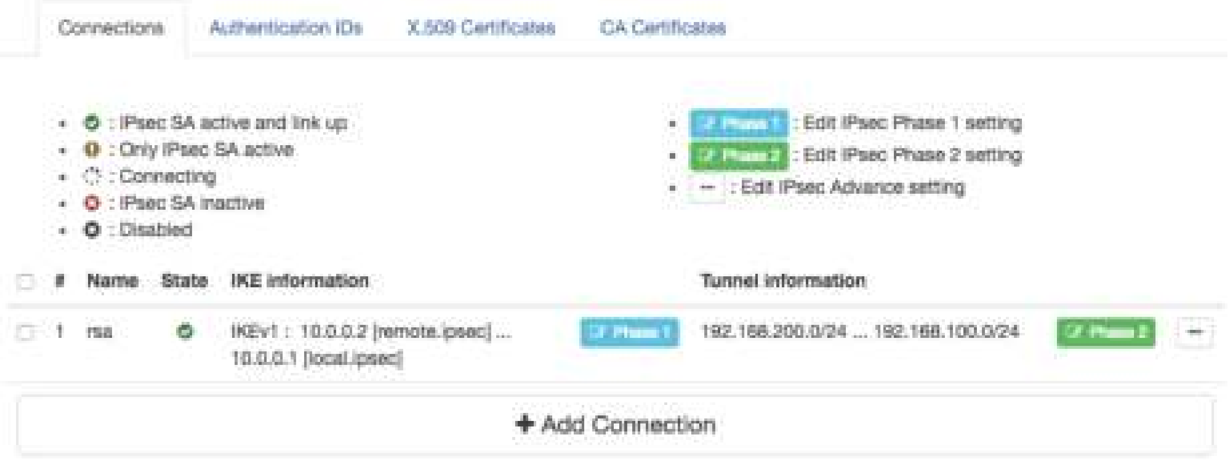


- ● : IPsec SA active and link up
- ● : Only IPsec SA active
- ○ : Connecting
- ● : IPsec SA inactive
- ● : Disabled

- Phase 1 : Edit IPsec Phase 1 setting
- Phase 2 : Edit IPsec Phase 2 setting
- − : Edit IPsec Advance setting

□	#	Name	State	IKE information		Tunnel information		
□	1	rsa	●	IKEv1 : 10.0.0.1 [local.ipsec] ... 10.0.0.2 [remote.ipsec]	Phase 1	192.168.100.0/24 ... 192.168.200.0/24	Phase 2	−

- Client



- ● : IPsec SA active and link up
- ● : Only IPsec SA active
- ○ : Connecting
- ● : IPsec SA inactive
- ● : Disabled

- Phase 1 : Edit IPsec Phase 1 setting
- Phase 2 : Edit IPsec Phase 2 setting
- − : Edit IPsec Advance setting

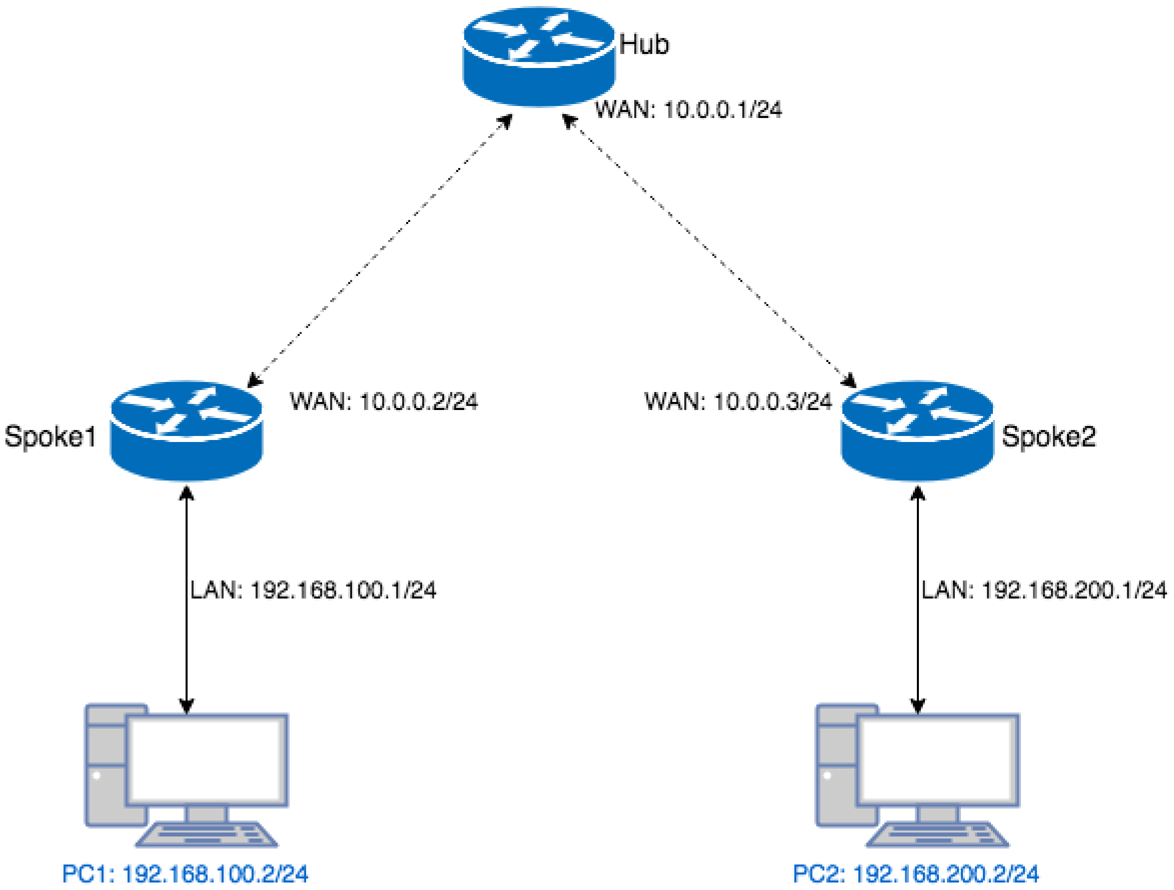
□	#	Name	State	IKE information		Tunnel information		
□	1	rsa	●	IKEv1 : 10.0.0.2 [remote.ipsec] ... 10.0.0.1 [local.ipsec]	Phase 1	192.168.200.0/24 ... 192.168.100.0/24	Phase 2	−

11.2.6 IPsec > Hub-Spoke Topology

This section explains how to set Hub-Spoke Topology and connect two (or more) gateways to a central one.

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

For example, in the Hub-and-Spoke topology, we want to send the essential traffic through IPsec VPN tunnel. Thus, we will set the Route-based VPN and Static Route to handle this situation. The Route-based VPN will redirect the traffic which is matching the routing table only to IPsec VPN tunnel.



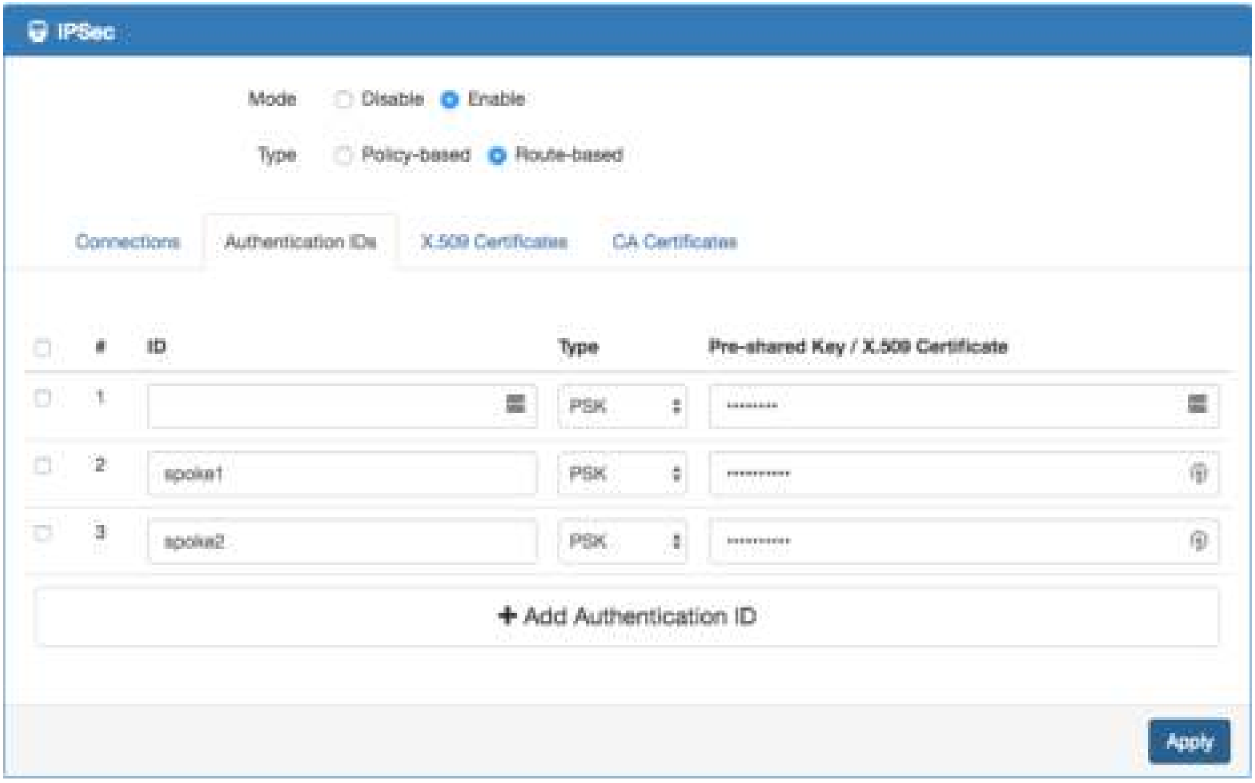
After setting some configurations, the PC1 and PC2 could communicate each other through the Hub gateway.

- ## Hub configuration

Hub IPsec configuration

In this example, we have two spokes on the topology. Thus, the Hub needs to set two IPsec connections for each spoke.

1. Change **Mode** from Disable to **Enable**.
2. Change Type from Policy-based to Route-based.
3. Navigate to the Authentication IDs tab.
4. Add the default pre-shared key
   - **ID:** (The ID is blank.)
   - **Type:** PSK
   - **Pre-shared Key:** defaultpsk
5. Add the authentication ID for Spoke 1
   - **ID**: spoke1
   - **Type**: PSK
   - **Pre-shared Key**: testspoke1
6. Add the authentication ID for **Spoke 2**
   - **ID**: spoke2
   - **Type**: PSK
   - **Pre-shared Key**: testspoke2
7. Apply the changes
8. Navigate to the Connections tab
9. Add IPsec connection for **Spoke 1**
   (1) Edit the **phase 1** setting
   (2) Change **Mode** from Disable to **Enable**
   (3) Change the **Remote ID** and select the **spoke1 (PSK)** authentication ID
   (4) Save the changes
10. Add IPsec connection for **Spoke 2**
   (1) Edit the **phase 1** setting
   (2) Change **Mode** from Disable to **Enable**.
   (3) Change the **Remote ID** and select the **spoke2 (PSK)** authentication ID
   (4) Save the changes
11. Apply the changes

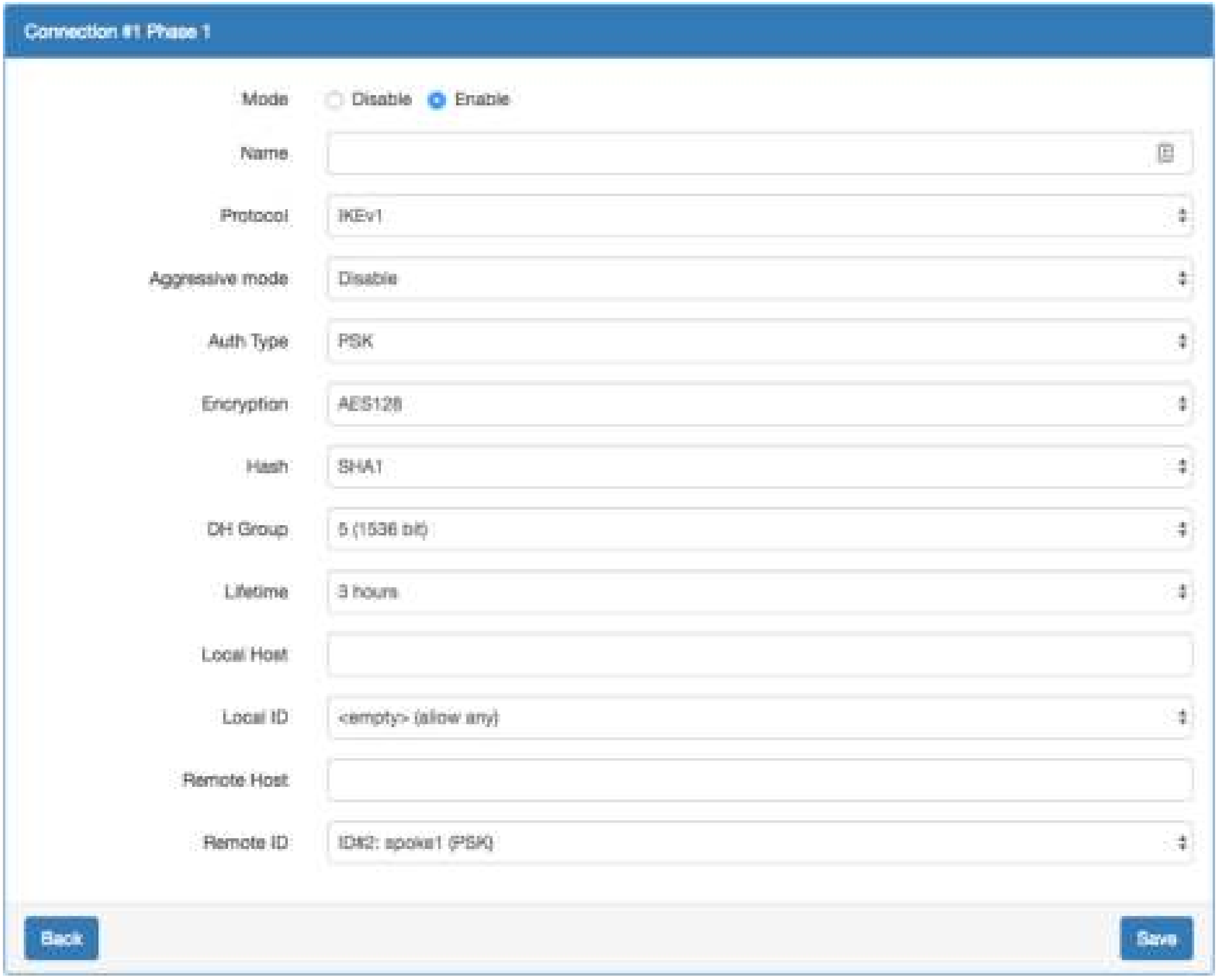


IPSec

Mode ○ Disable ● Enable

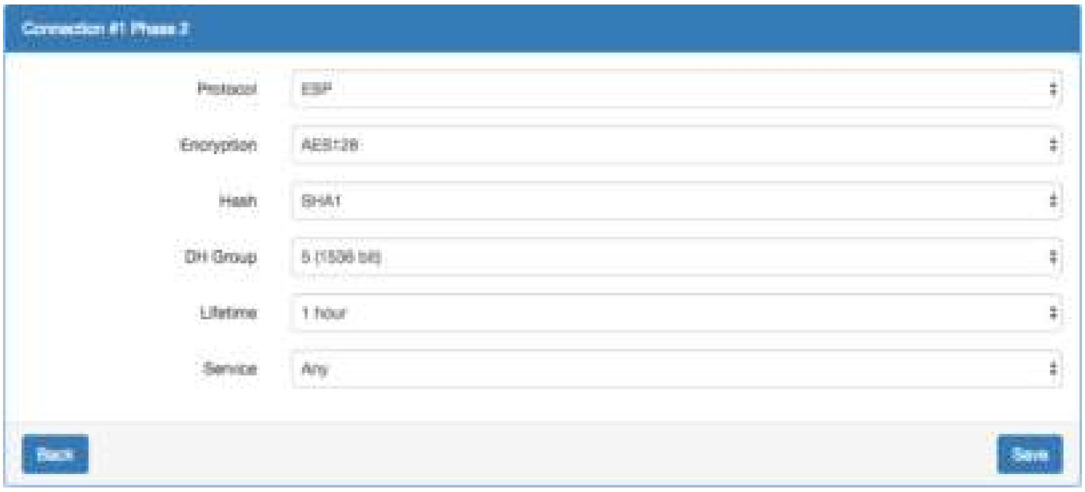
Type ○ Policy-based ● Route-based

□	#	ID	Type	Pre-shared Key / X.509 Certificate
□	1		PSK	••••••••
□	2	spoke1	PSK	••••••••••
□	3	spoke2	PSK	••••••••••



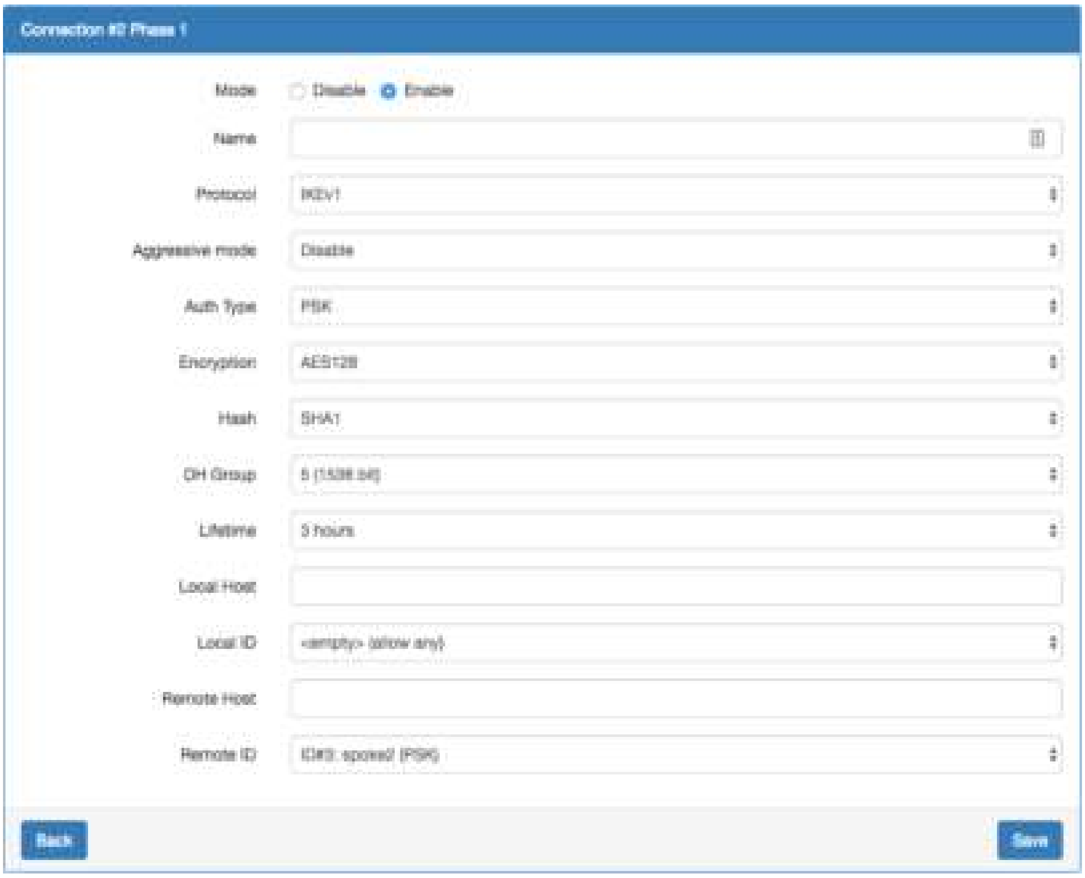
Connection #1 Phase 1

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	ID#2: spoke1 (PSK)



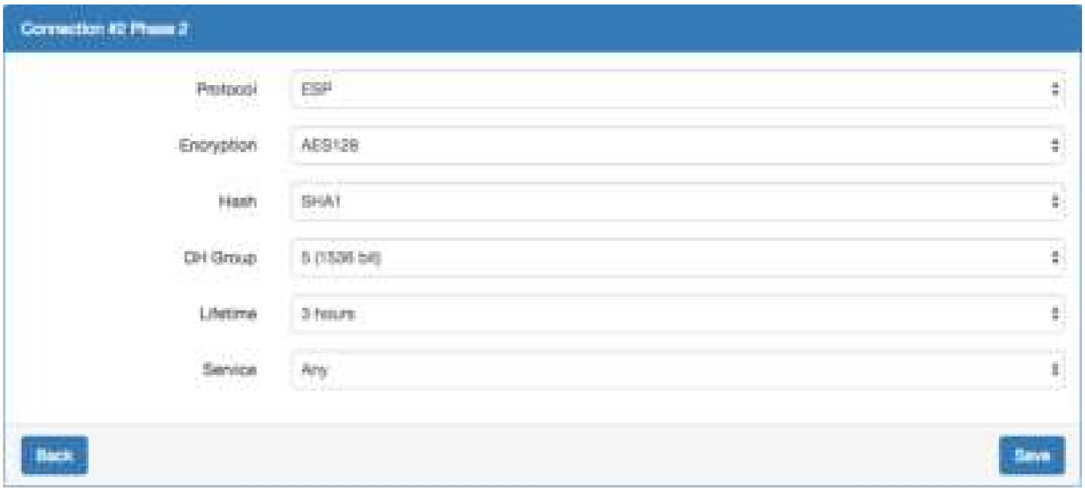
Connection #1 Phase 2

Protocol	ESP
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	1 hour
Service	Any



Connection #2 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	ID#3: spoke2 (PSK)

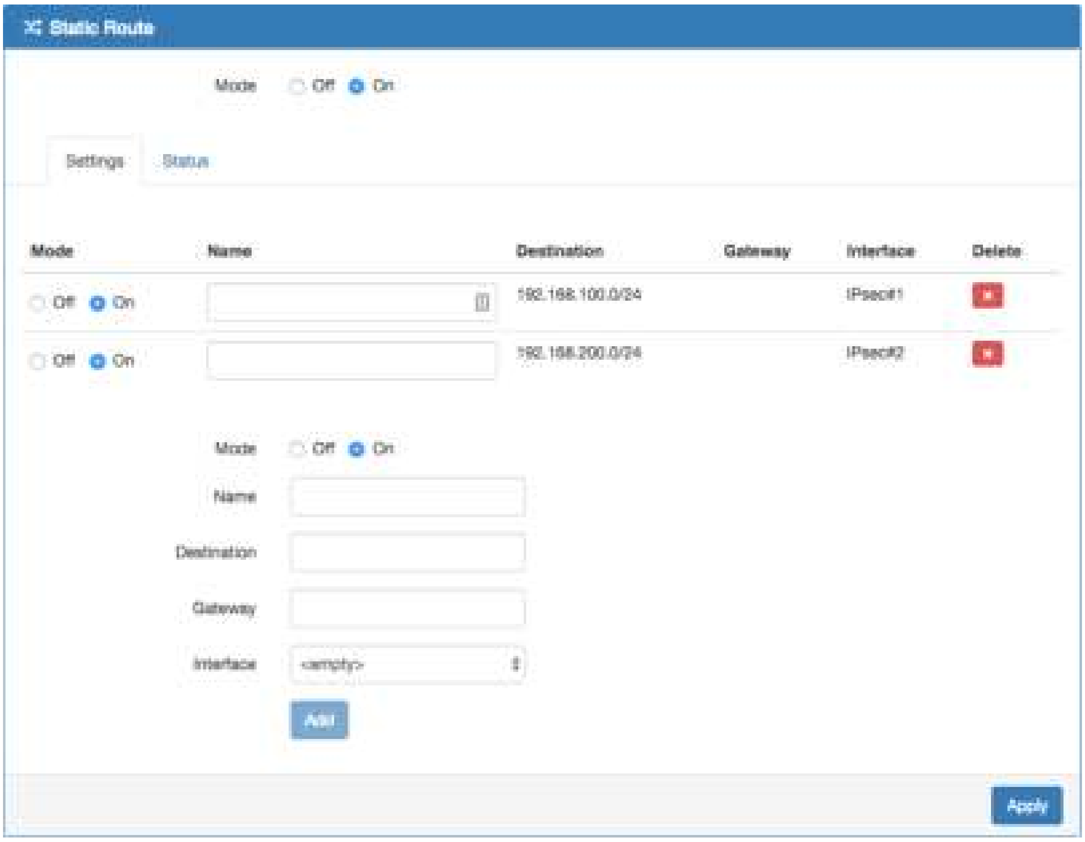


Connection #2 Phase 2

Protocol	ESP
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	3 hours
Service	Any

- **Hub Static Route configuration**

1. Navigate to the IP Routing > Static Route page
2. Add the static route for IPsec **Spoke 1** connection
   - **Mode**: On
   - **Destination**: 192.168.100.0/24
   - **Interface**: Select the IPsec interface by connection number
   - e.g. If your IPsec connection is **#1** then the interface should be **IPsec#1**.
3. Add the static route for IPsec **Spoke 2** connection
   - **Mode**: On
   - **Destination**: 192.168.200.0/24
   - **Interface**: Select the IPsec interface by connection number
   - e.g. If your IPsec connection is **#2** then the interface should be **IPsec#2**.
4. Apply the changes



Mode ○ Off ● On

Mode	Name	Destination	Gateway	Interface	Delete
○ Off ● On		192.168.100.0/24		IPsec#1	✕
○ Off ● On		192.168.200.0/24		IPsec#2	✕

Mode ○ Off ● On

Name

Destination

Gateway

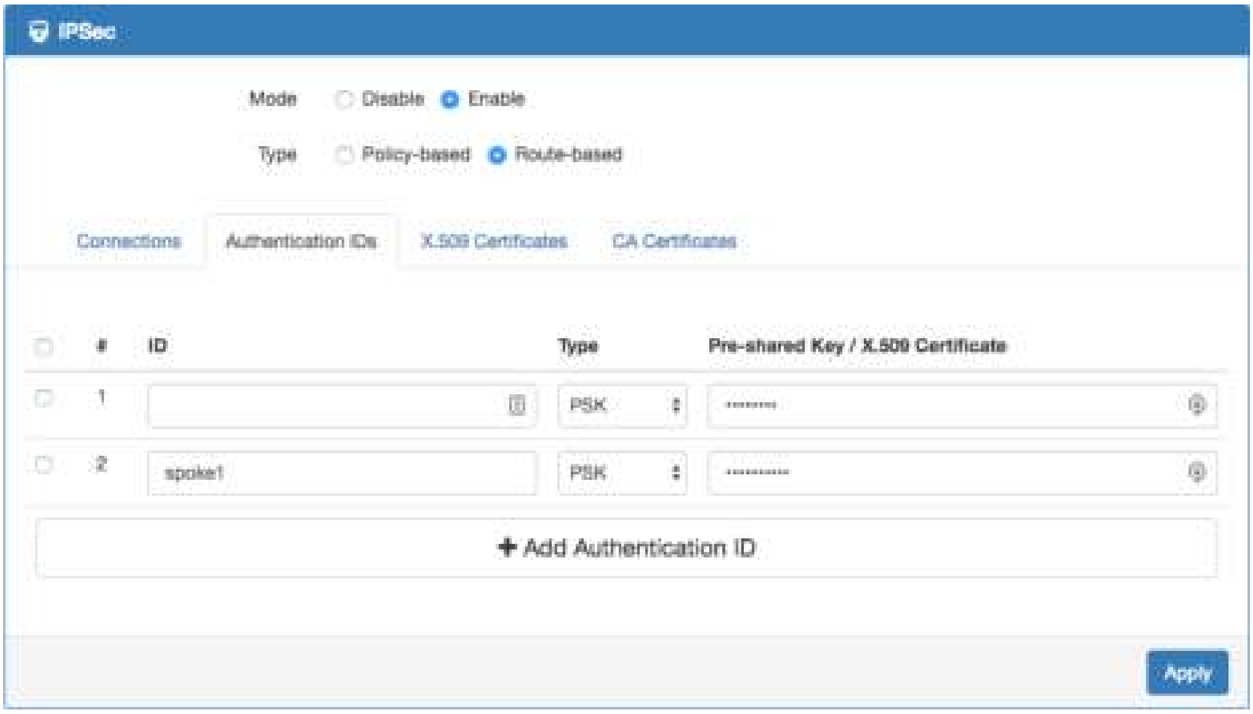
Interface <empty>

- **Spoke 1 configuration**

Spoke 1 IPsec configuration

1. Change **Mode** from Disable to **Enable**.
2. Change Type from Policy-based to **Route-based**.
3. Navigate to the Authentication IDs tab.
4. Add default pre-shared key
   (1) **ID:**
   (2) **Type:** PSK
   (3) **Pre-shared Key:** defaultpsk
5. Add one authentication ID
   (4) **ID**: spoke1
   (5) **Type**: PSK
   (6) **Pre-shared Key**: testspoke1
6. Apply the changes
7. Navigate to the Connections tab.
8. Add IPsec connection
   (7) Edit the **phase 1** setting
   (8) Change **Mode** from Disable to **Enable**.
   (9) Change the **Local ID** and select the **spoke1 (PSK)** authenticaion ID.
   (10) Fill the IP address of VPN server to **Remote Host** field.
   - e.g. Remote Host: 10.0.0.1

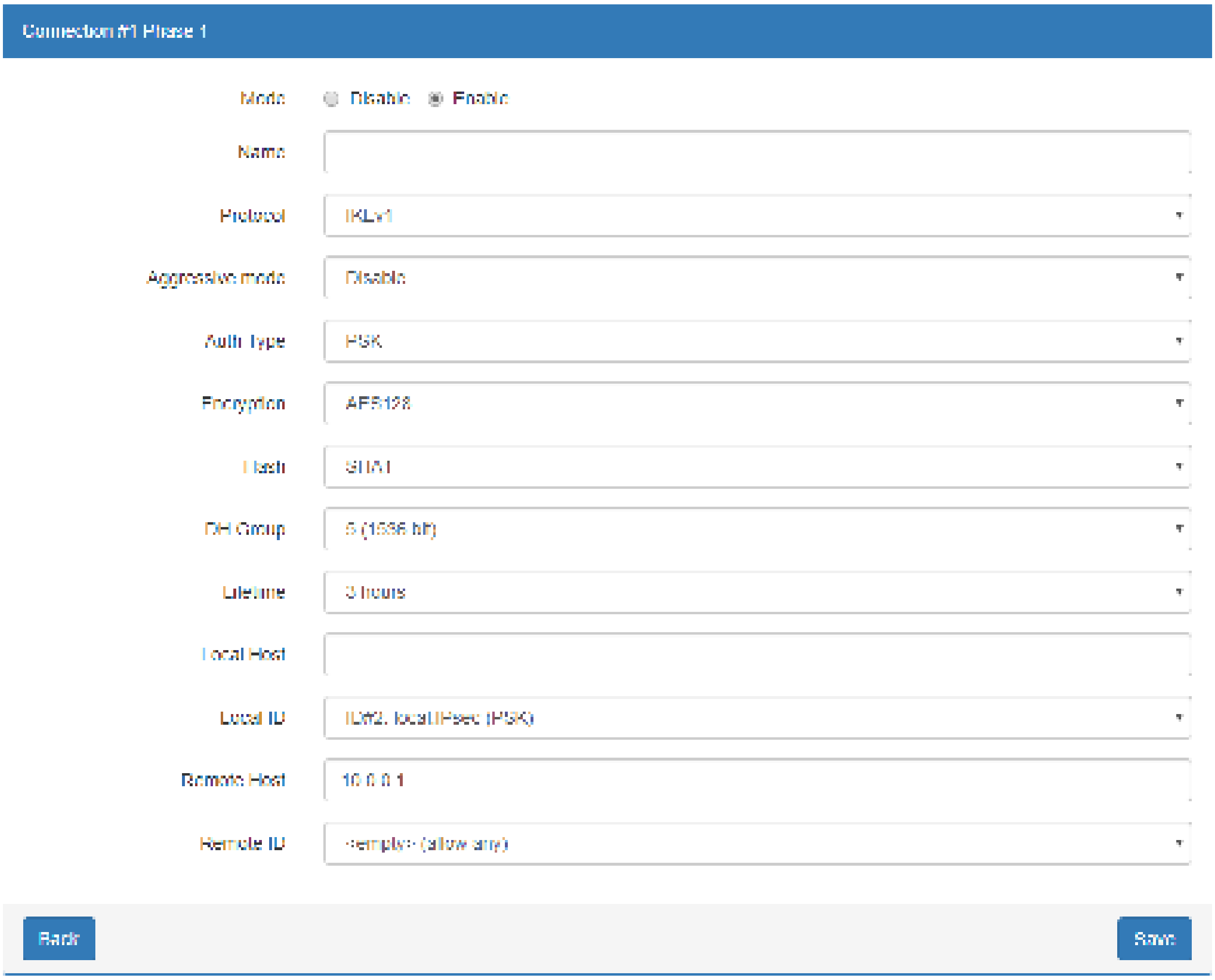
   (11) Save the changes
9. Apply the changes



Mode ○ Disable ● Enable

Type ○ Policy-based ● Route-based

☐	#	ID	Type	Pre-shared Key / X.509 Certificate
☐	1		PSK	••••••••
☐	2	spoke1	PSK	••••••••••

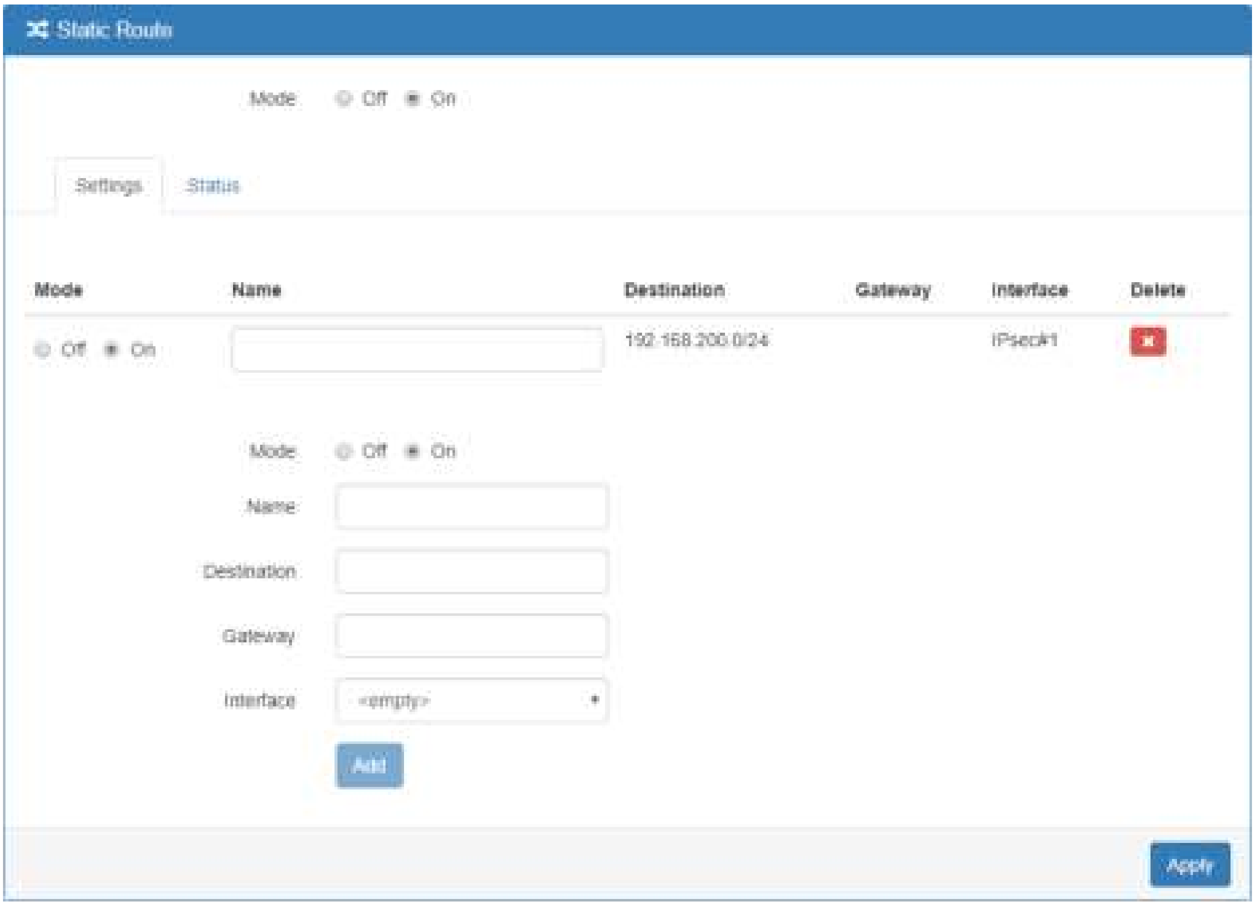


Connection #1 Phase 1

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	ID#2: local IPsec (PSK)
Remote Host	10.0.0.1
Remote ID	<empty> (allow any)

Spoke 1 Static Route configurtation

1. Navigate to the **IP Routing** > **Static Route** page
2. Add the static route for IPsec connection
   - **Mode**: On
   - **Destination**: 192.168.200.0/24
   - **Interface**: Select the IPsec interface by connection number
   - e.g. If your IPsec connection is **#1** then the interface should be **IPsec#1**.
3. Apply the changes



Static Route

Mode ○ Off ● On

Mode	Name	Destination	Gateway	Interface	Delete
○ Off ● On		192.168.200.0/24		IPsec#1	✖

Mode ○ Off ● On

Name

Destination

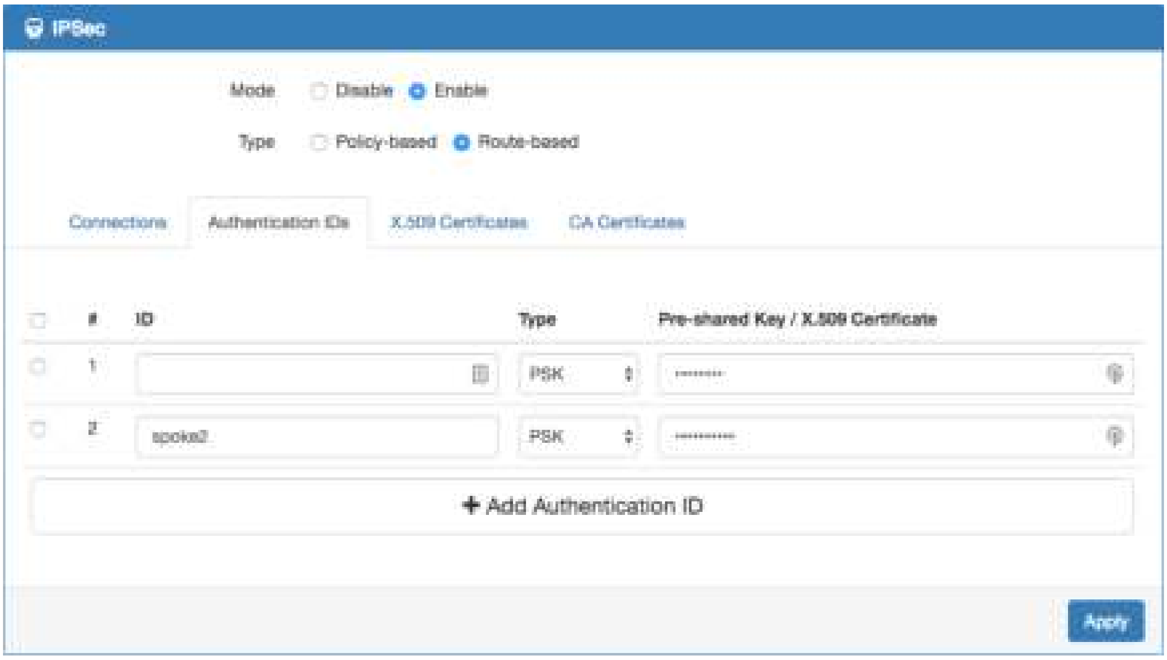
Gateway

Interface <empty>

- **Spoke 2 configuration**

Spoke 2 IPsec configuration

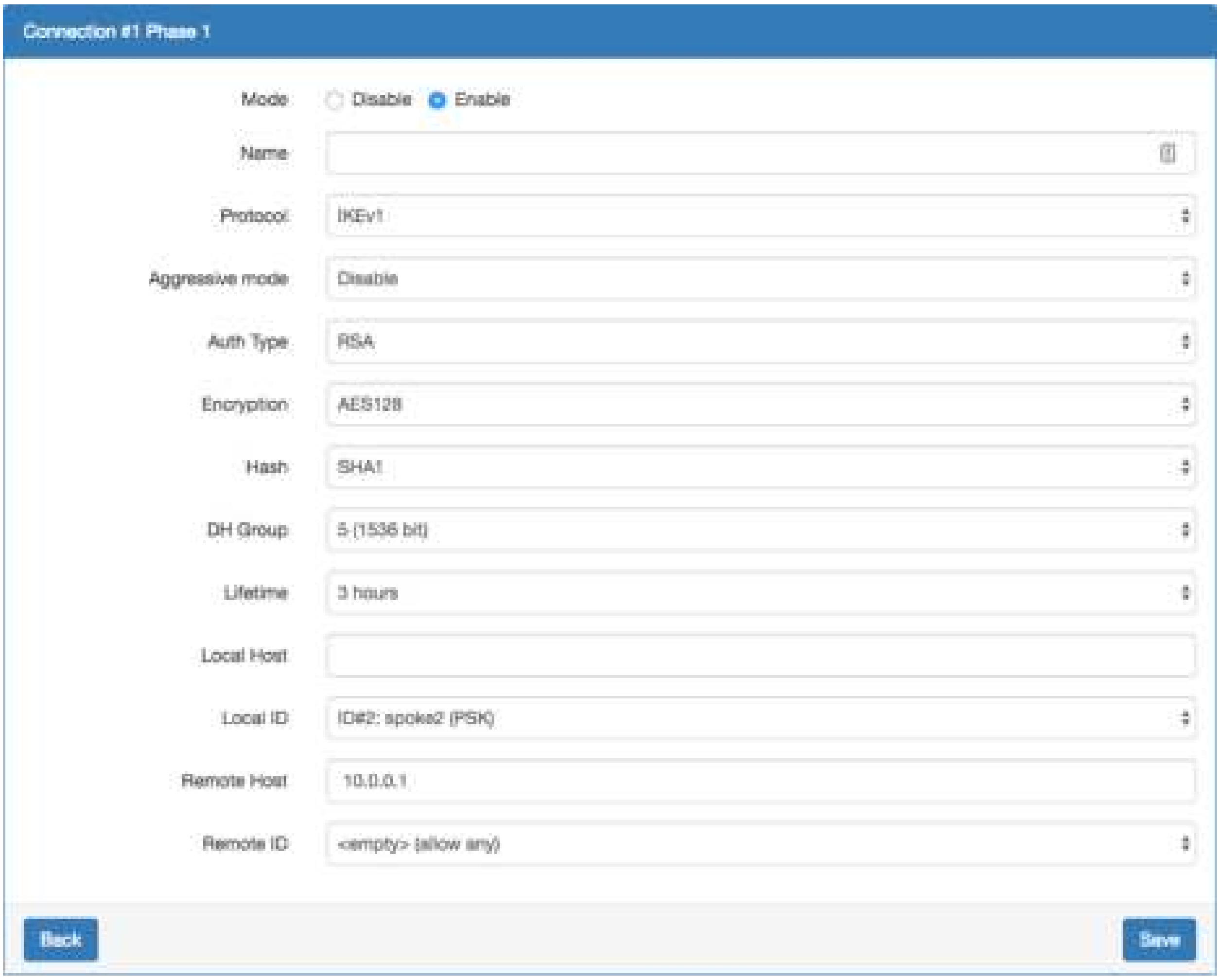
1. Change **Mode** from Disable to **Enable**.
2. Change **Type** from Policy-based to **Route-based**.
3. Navigate to the Authentication IDs tab.
4. Add default pre-shared key
   - **ID:** (The ID is blank.)
   - **Type:** PSK
   - **Pre-shared Key:** defaultpsk
5. Add one authentication ID
   - **ID**: spoke2
   - **Type**: PSK
   - **Pre-shared Key**: testspoke2
6. Apply the changes
7. Navigate to the Connections tab.
8. Add IPsec connection
   (1) Edit the **phase 1** setting
   (2) Change **Mode** from Disable to **Enable**.
   (3) Change the **Local ID** and select the **spoke2 (PSK)** authenticaion ID.
   (4) Fill the IP address of VPN server to **Remote Host** field.
   - e.g. Remote Host: 10.0.0.1
   (5) Save the changes
9. Apply the changes



Mode ○ Disable ● Enable

Type ○ Policy-based ● Route-based

□	#	ID	Type	Pre-shared Key / X.509 Certificate
□	1		PSK	·········
□	2	spoke2	PSK	··········

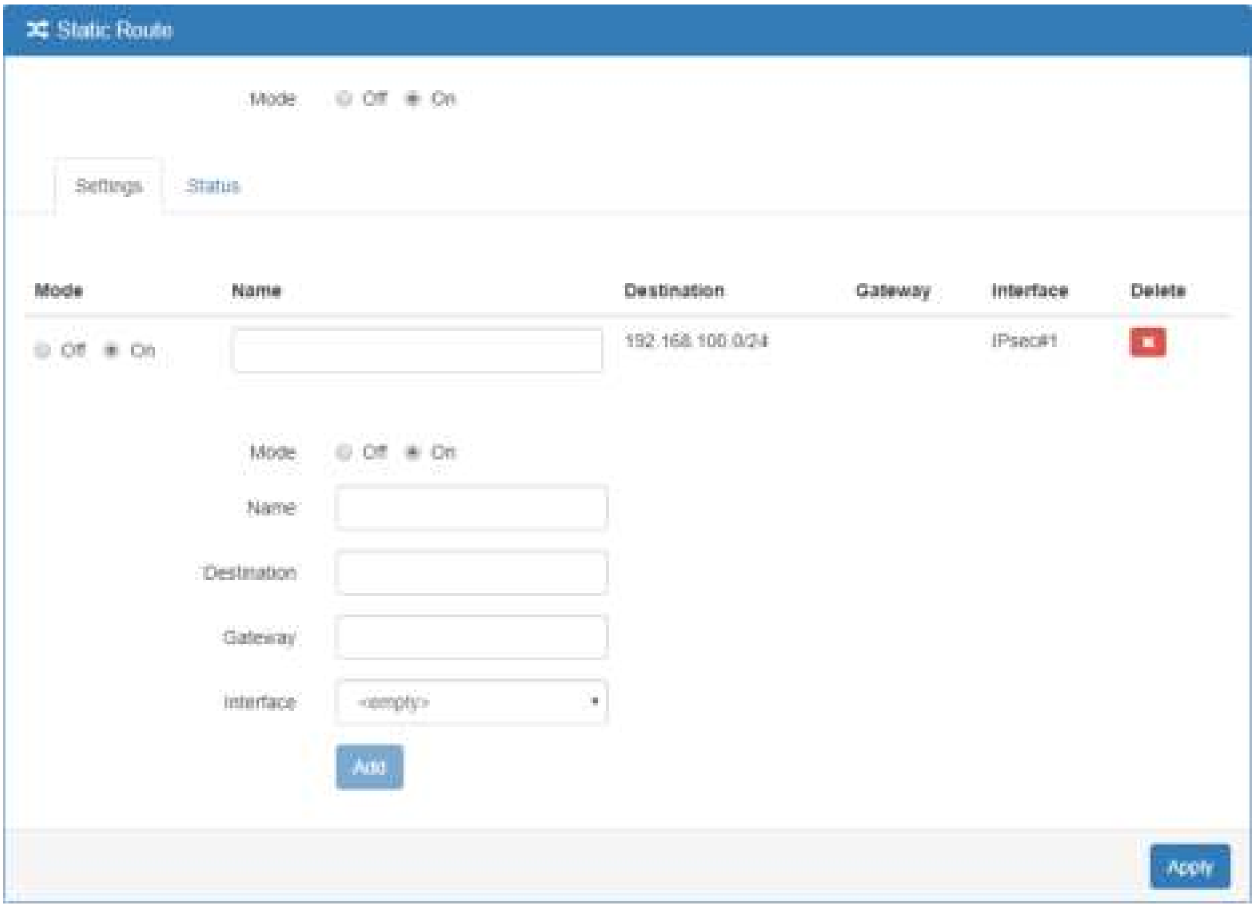


Connection #1 Phase 1

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#2: spoke2 (PSK)
Remote Host	10.0.0.1
Remote ID	<empty> (allow any)

Spoke 2 Static Route configurtation

1. Naviagte to the IP Routing > Static Route page
2. Add the static route for IPsec connection
   - Mode: On
   - Destination: 192.168.100.0/24
   - Interface: Select the IPsec interface by connection number
   - e.g. If your IPsec connection is #1 then the interface should be IPsec#1.
3. Apply the changes

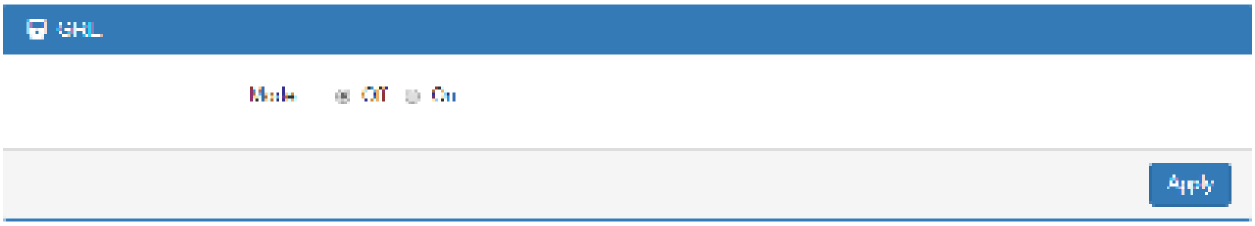


Mode	Name	Destination	Gateway	Interface	Delete
○ Off ● On		192.168.100.0/24		IPsec#1	✖

11.3 VPN > GRE

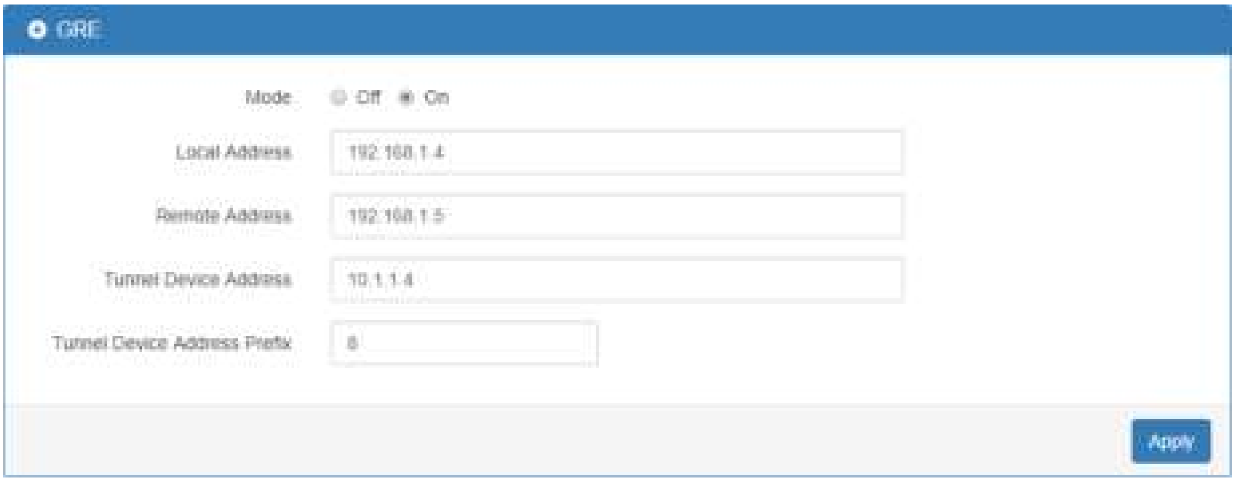
This section allows you to set GRE configuration. The default mode is off.

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.



Mode ● Off ○ On

The GRE Mode is on.



Mode ○ Off ● On

Local Address 192.168.1.4

Remote Address 192.168.1.5

Tunnel Device Address 10.1.1.4

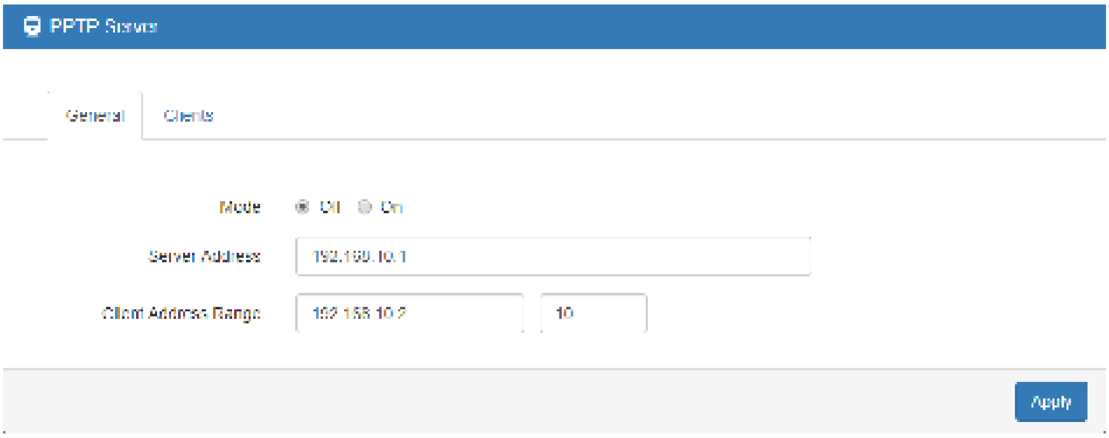
Tunnel Device Address Prefix 8

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.

11.4 VPN > PPTP Server

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

(1) General Configuration



Mode ● Off ○ On

Server Address 192.168.10.1

Client Address Range 192.168.10.2 10

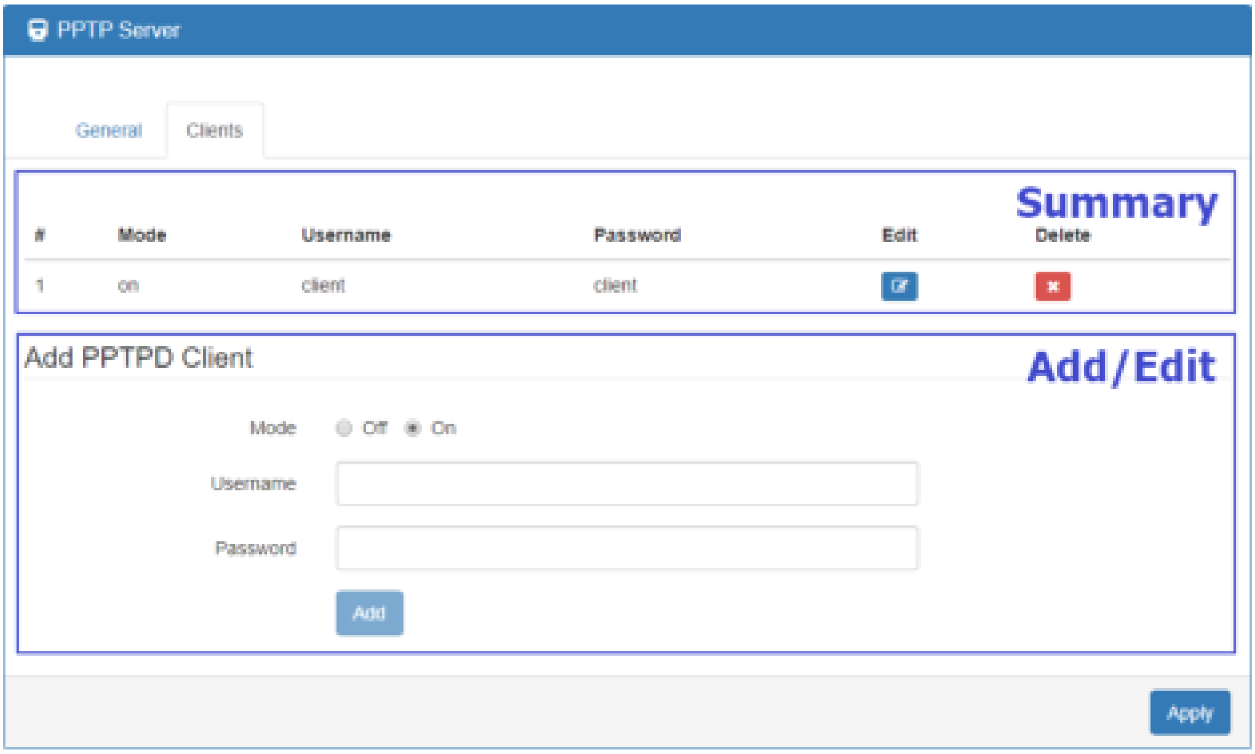
VPN > PPTP Server > General	
Item	**Description**
Mode	Select from Off or On to enable PPTP Server.
Server Address	IP addresses to be used at the local end of the tunneled PPP links between the server and the client.
Client Address Range	A list of IP addresses to assign to remote PPTP clients.

(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.



PPTP Server

General | Clients

Summary

#	Mode	Username	Password	Edit	Delete
1	on	client	client		✖

Add PPTPD Client

Add/Edit

Mode ○ Off ● On

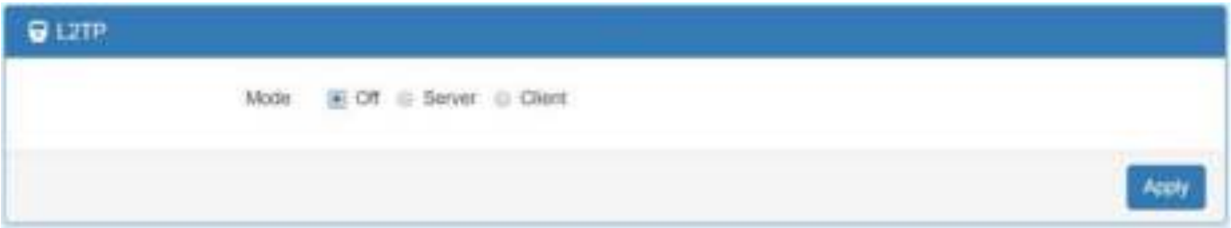
Username

Password

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) Genernal Mode: The defualt mode is Off as shown in the following interface.

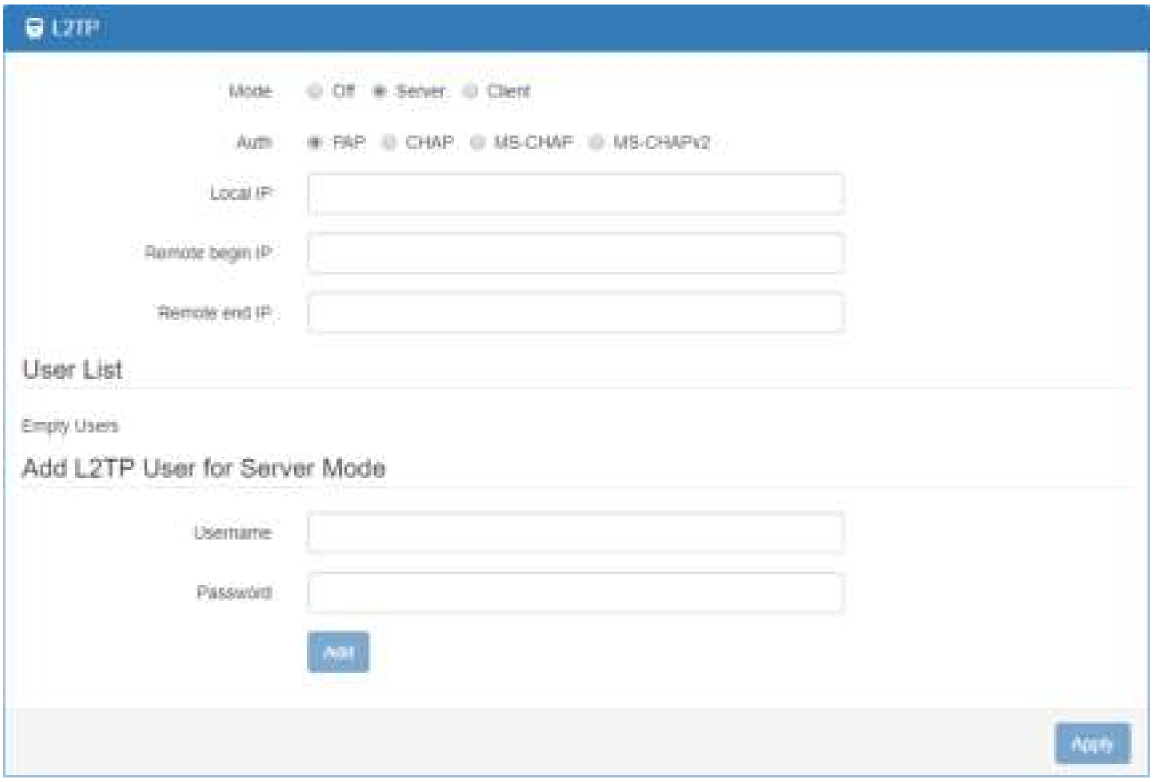


L2TP

Mode ● Off ○ Server ○ Client

(2) Server Mode:

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



L2TP

Mode ○ Off ● Server ○ Client

Auth ● PAP ○ CHAP ○ MS-CHAP ○ MS-CHAPv2

Local IP

Remote begin IP

Remote end IP

User List

Empty Users

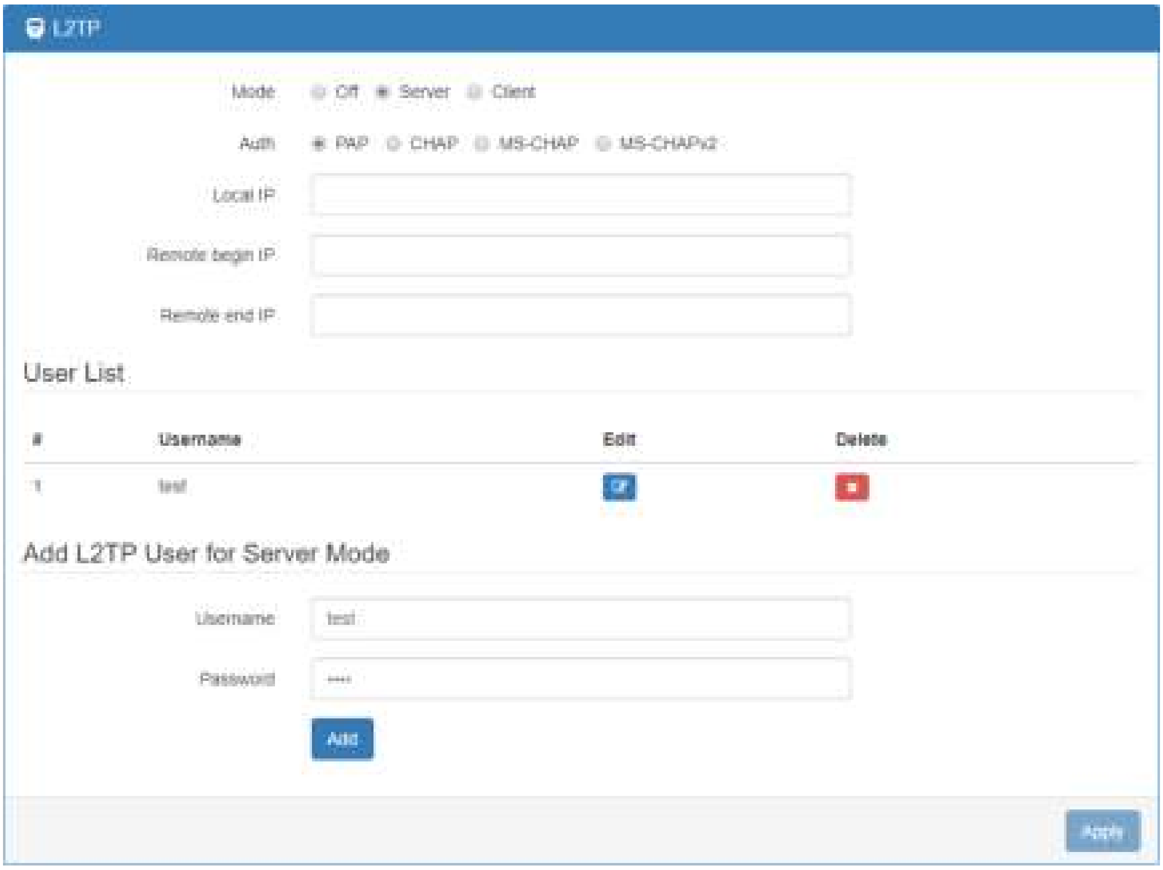
Add L2TP User for Server Mode

Username

Password

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.



L2TP

Mode ○ Off ● Server ○ Client

Auth ● PAP ○ CHAP ○ MS-CHAP ○ MS-CHAPv2

Local IP

Remote begin IP

Remote end IP

User List

#	Username	Edit	Delete
1	test	✎	✖

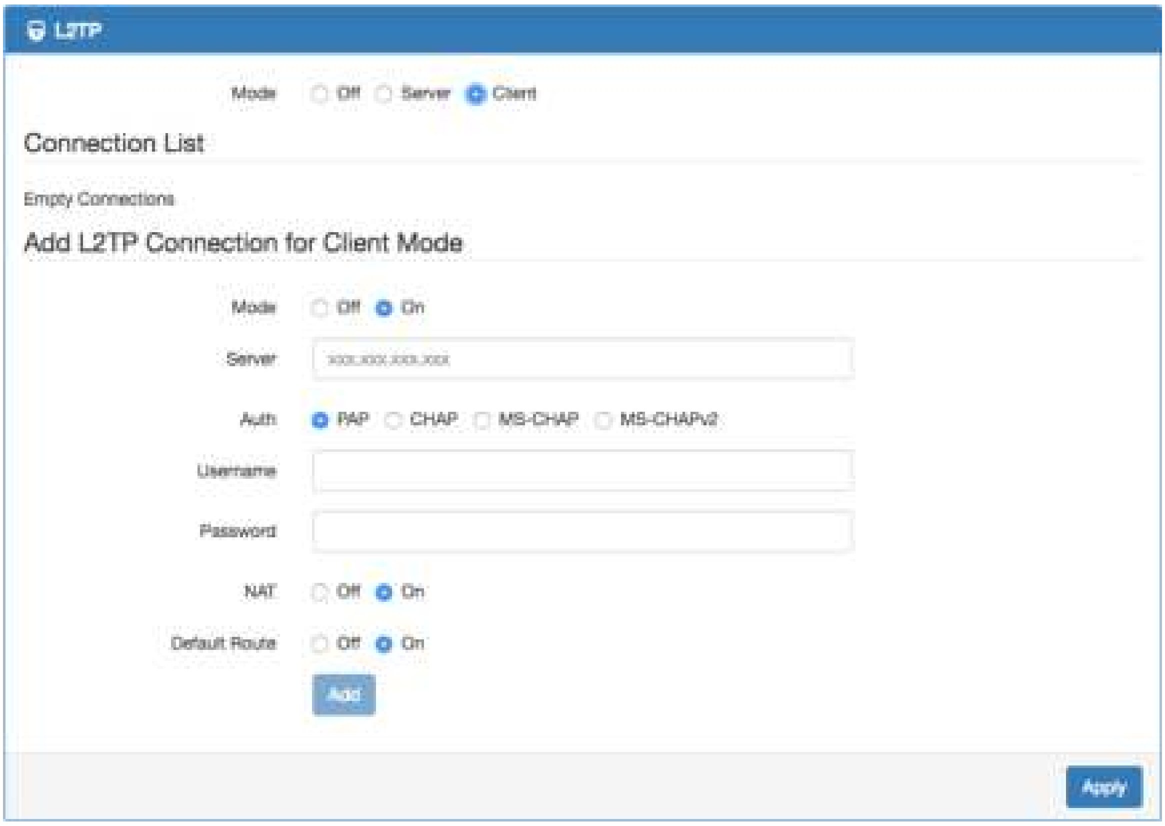
Add L2TP User for Server Mode

Username: test

Password: ••••

(3) Client Mode:

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



L2TP

Mode ○ Off ○ Server ● Client

Connection List

Empty Connections

Add L2TP Connection for Client Mode

Mode ○ Off ● On

Server: xxx.xxx.xxx.xxx

Auth ● PAP ○ CHAP ○ MS-CHAP ○ MS-CHAPv2

Username

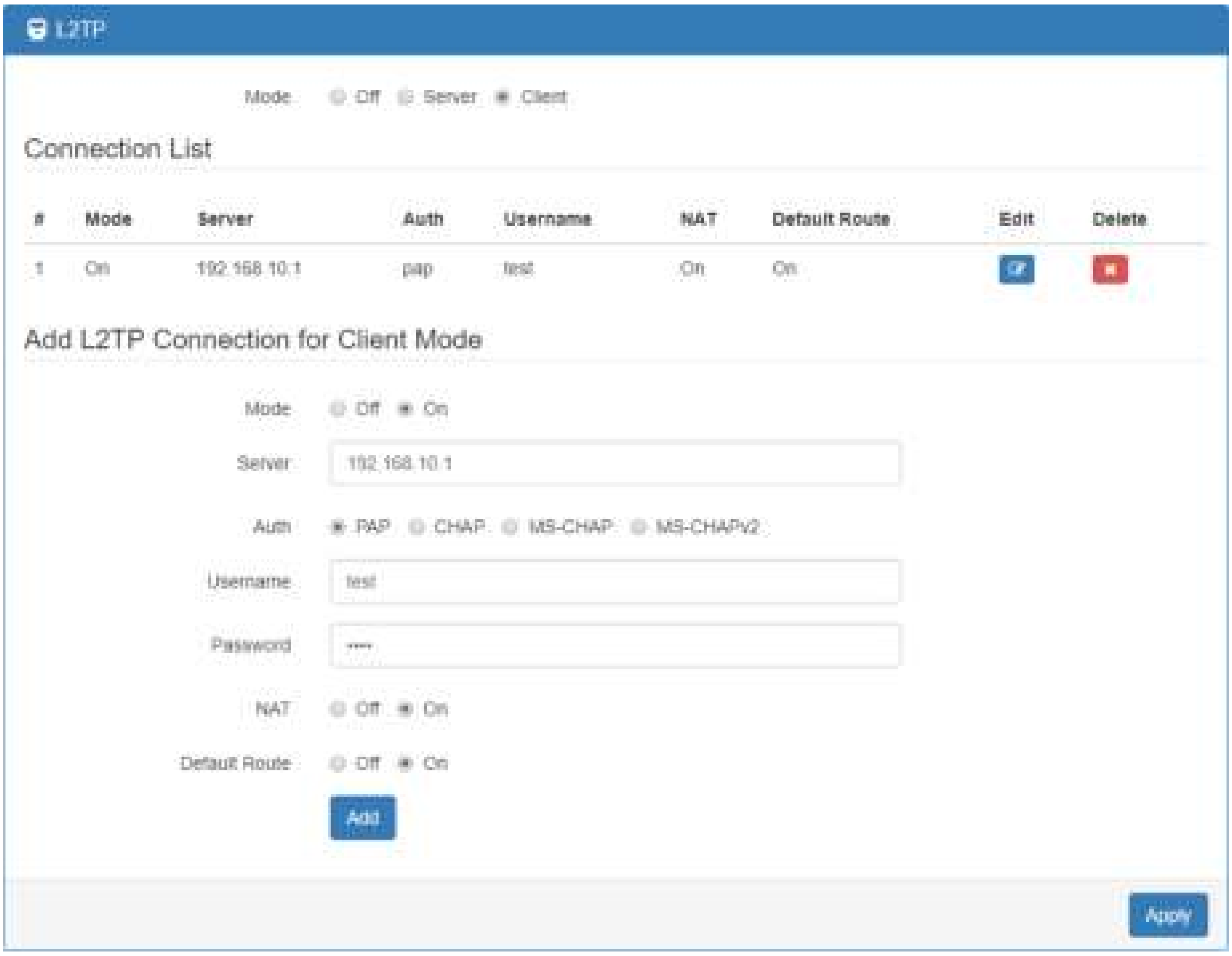
Password

NAT ○ Off ● On

Default Route ○ Off ● On

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.



L2TP

Mode ○ Off ○ Server ● Client

Connection List

#	Mode	Server	Auth	Username	NAT	Default Route	Edit	Delete
1	On	192.168.10.1	pap	test	On	On	✎	✖

Add L2TP Connection for Client Mode

Mode ○ Off ● On

Server 192.168.10.1

Auth ● PAP ○ CHAP ○ MS-CHAP ○ MS-CHAPv2

Username test

Password ••••

NAT ○ Off ● On

Default Route ○ Off ● On

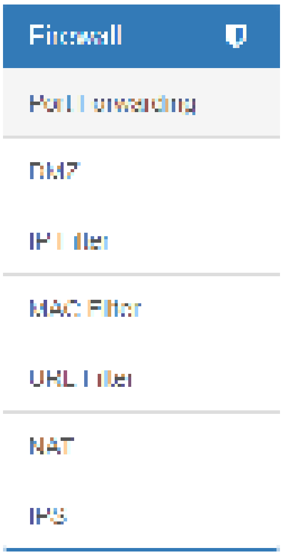
Add

Apply

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

12 Configuration > Firewall

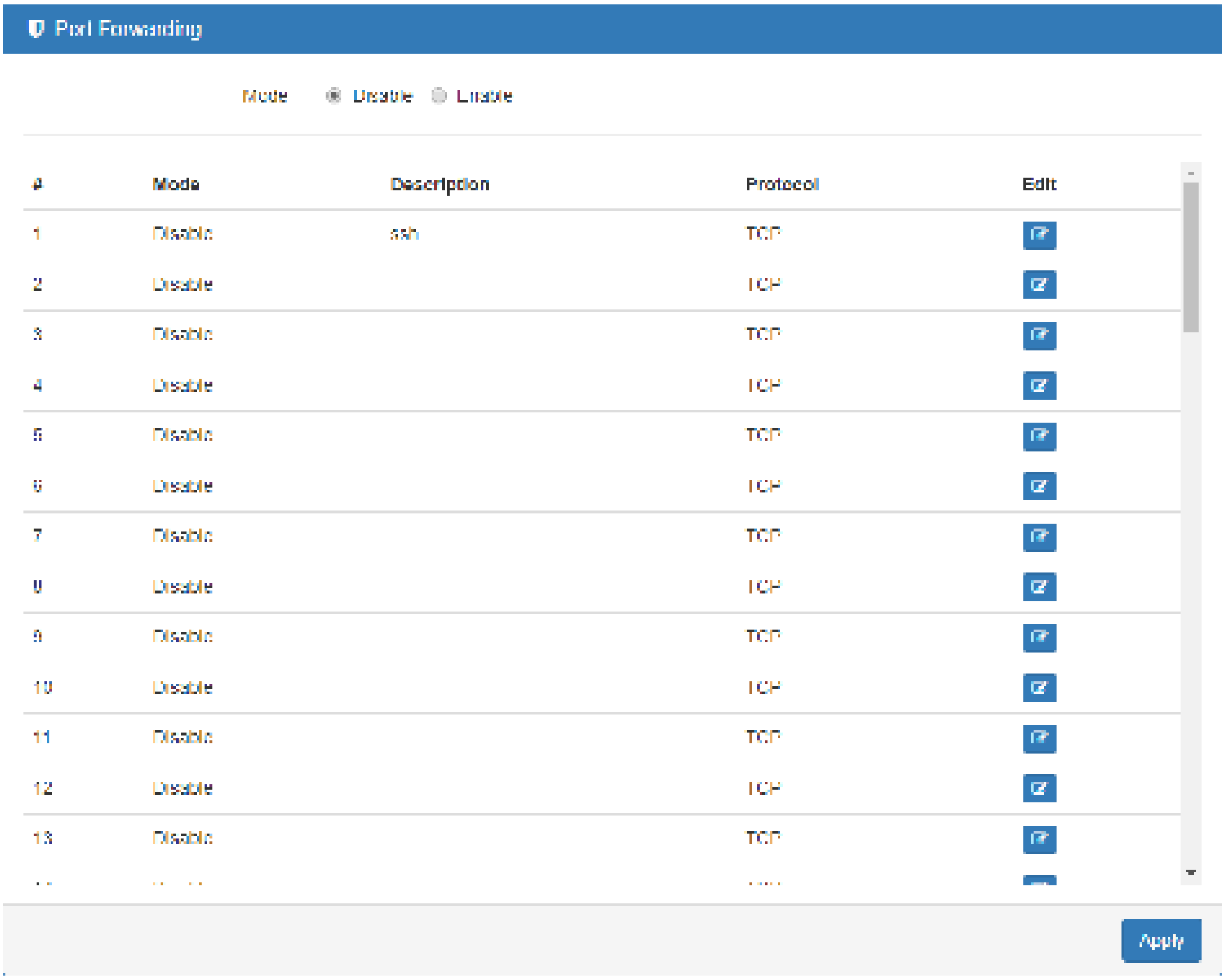
This section allows you to configurate Port Forwarding, DMZ, IP Filter, MAC Filter, URL Filter, NAT and IPS.



Firewall
- Port Forwarding
- DMZ
- IP Filter
- MAC Filter
- URL Filter
- NAT
- IPS

12.1 Firewall > Port Forwarding

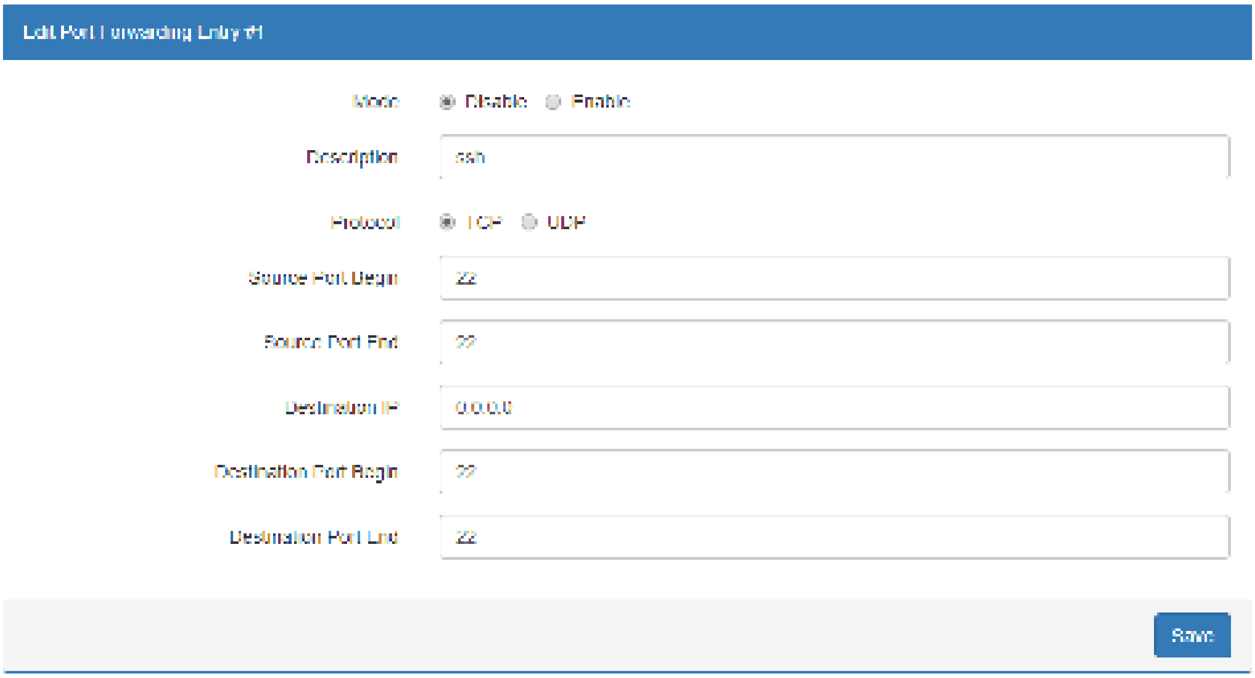
This section allows you to set up **Port Forwarding** and click ✎ edit button to configure.



Port Forwarding

Mode ● Disable ○ Enable

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



Edit Port Forwarding Entry #1

Mode ● Disable ○ Enable

Description: ssh

Protocol ● TCP ○ UDP

Source Port Begin: 22

Source Port End: 22

Destination IP: 0.0.0.0

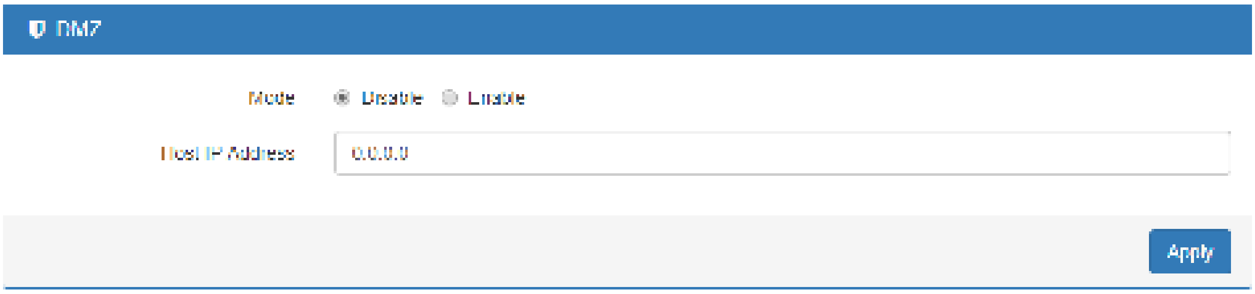
Destination Port Begin: 22

Destination Port End: 22

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.

12.2 Firewall > DMZ

This section allows you to set the DMZ configuration.



DMZ

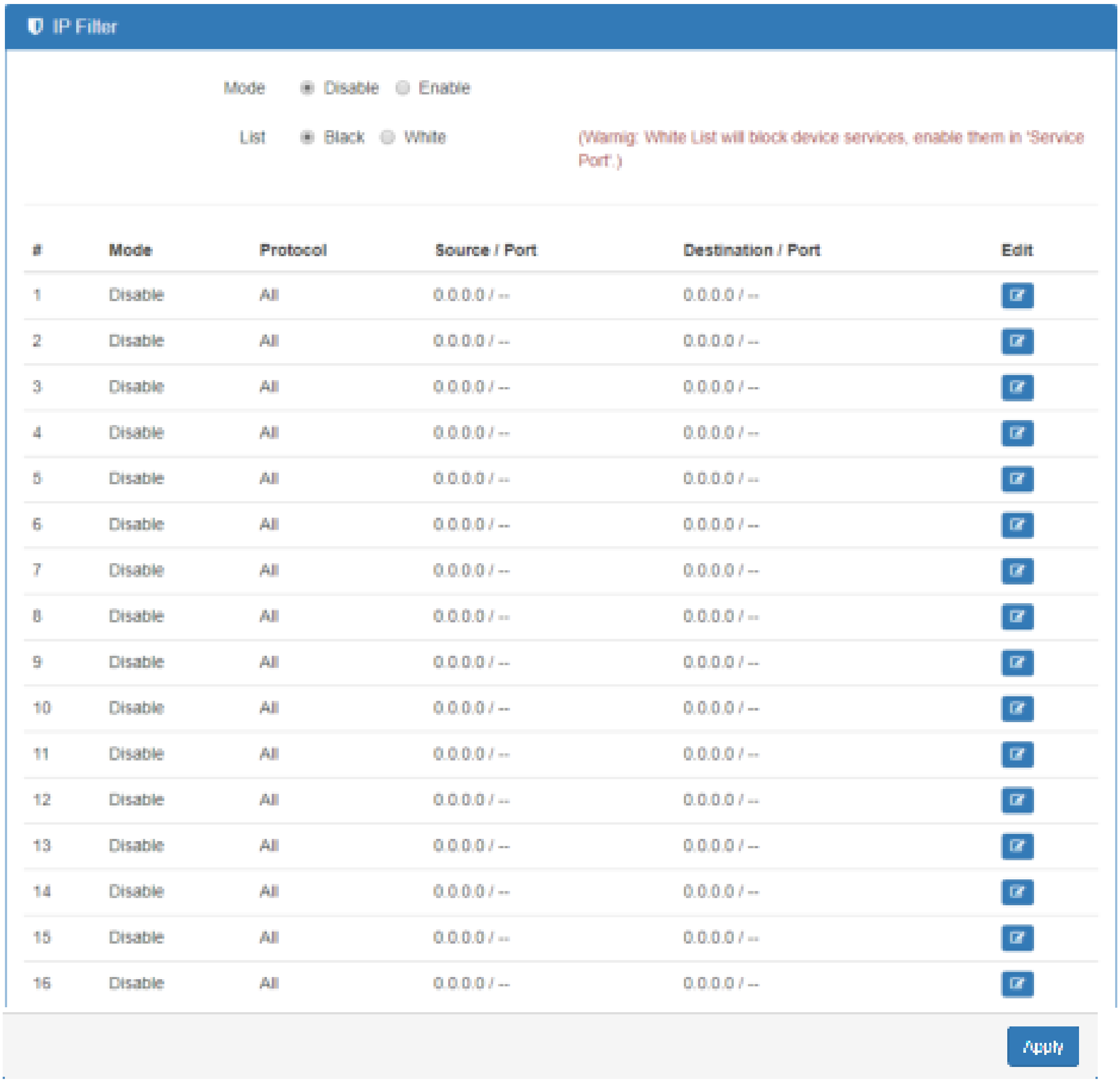
Mode ● Disable ○ Enable

Host IP Address: 0.0.0.0

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

12.3 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.



IP Filter

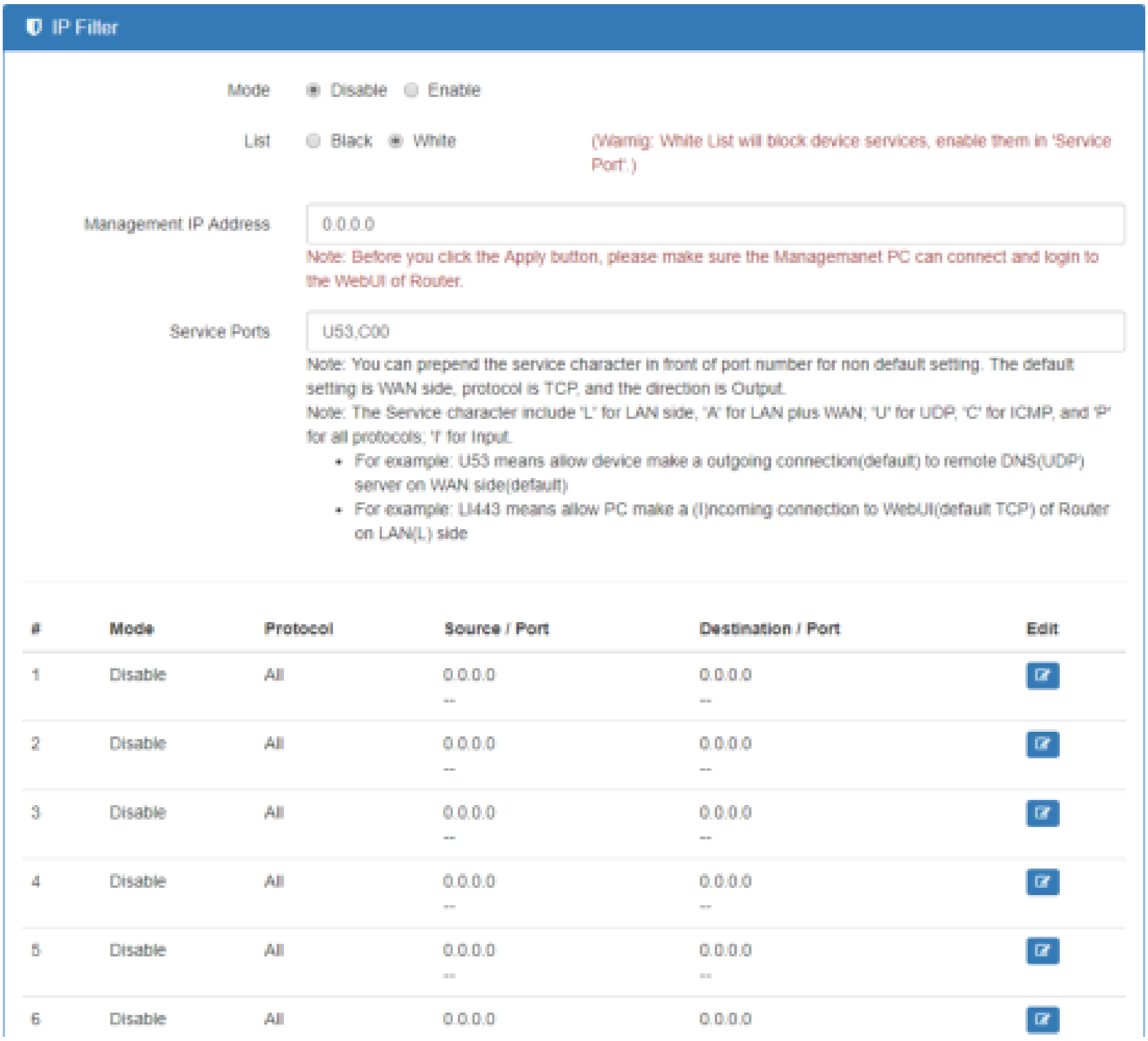
Mode ● Disable ○ Enable

List ● Black ○ White

(Warnig: White List will block device services, enable them in 'Service Port'.)

#	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.



IP Filter

Mode ● Disable ○ Enable

List ○ Black ● White (Warnig: White List will block device services, enable them in 'Service Port'.)

Management IP Address: 0.0.0.0

Note: Before you click the Apply button, please make sure the Managemanet PC can connect and login to the WebUI of Router.

Service Ports: U53,C00

Note: You can prepend the service character in front of port number for non default setting. The default setting is WAN side, protocol is TCP, and the direction is Output.

Note: The Service character include 'L' for LAN side, 'A' for LAN plus WAN; 'U' for UDP, 'C' for ICMP, and 'P' for all protocols; 'I' for Input.

- For example: U53 means allow device make a outgoing connection(default) to remote DNS(UDP) server on WAN side(default)
- For example: LI443 means allow PC make a (I)ncoming connection to WebUI(default TCP) of Router on LAN(L) side

#	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	✎

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.

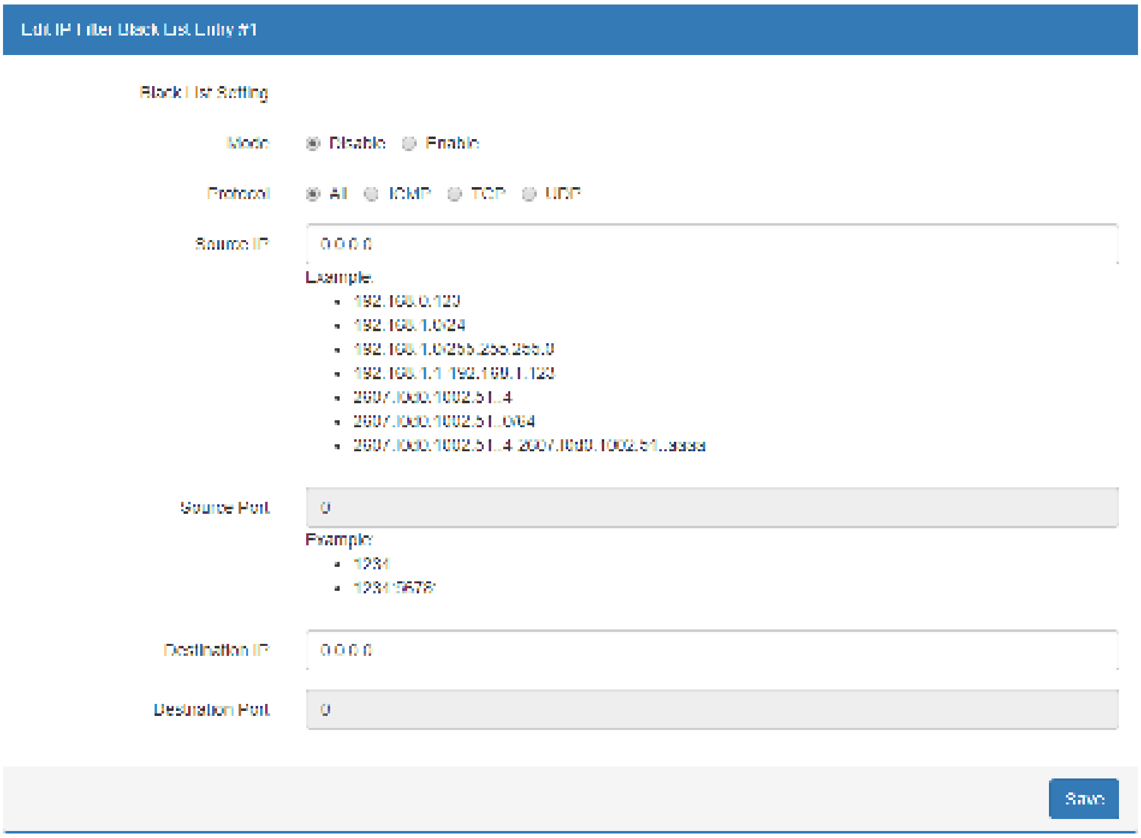
Service Ports:

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).



Edit IP Filter Black List Entry #1

Black List Setting

Mode ● Disable ○ Enable

Protocol ● All ○ ICMP ○ TCP ○ UDP

Source IP 0.0.0.0

Example:

- 192.168.0.123
- 192.168.1.0/24
- 192.168.1.0/255.255.255.0
- 192.168.1.1-192.168.1.123
- 2607:f0d0:1002:51::4
- 2607:f0d0:1002:51::0/64
- 2607:f0d0:1002:51::4-2607:f0d0:1002:51::aaaa

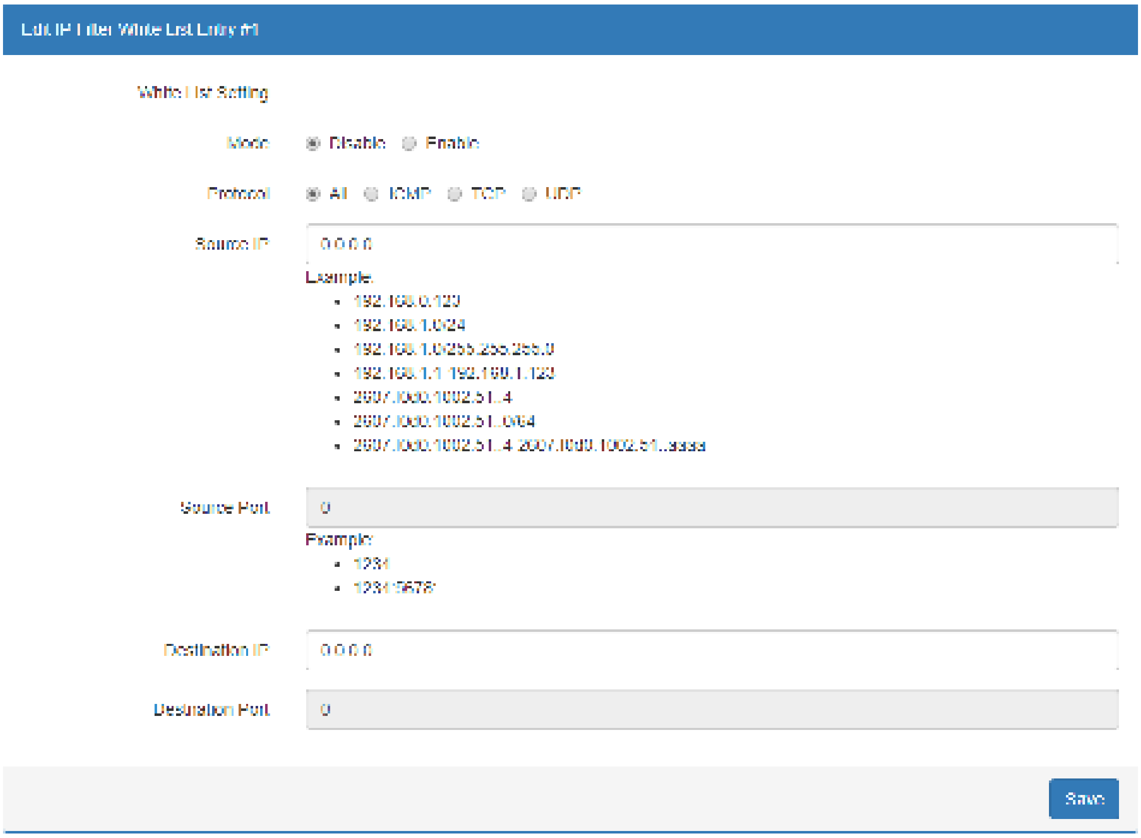
Source Port 0

Example:

- 1234
- 1234:5678

Destination IP 0.0.0.0

Destination Port 0



Edit IP Filter White List Entry #1

White List Setting

Mode ● Disable ○ Enable

Protocol ● All ○ ICMP ○ TCP ○ UDP

Source IP 0.0.0.0

Example:

- 192.168.0.123
- 192.168.1.0/24
- 192.168.1.0/255.255.255.0
- 192.168.1.1-192.168.1.123
- 2607:f0d0:1002:51::4
- 2607:f0d0:1002:51::0/64
- 2607:f0d0:1002:51::4-2607:f0d0:1002:51::aaaa

Source Port 0

Example:

- 1234
- 1234:5678

Destination IP 0.0.0.0

Destination Port 0

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.

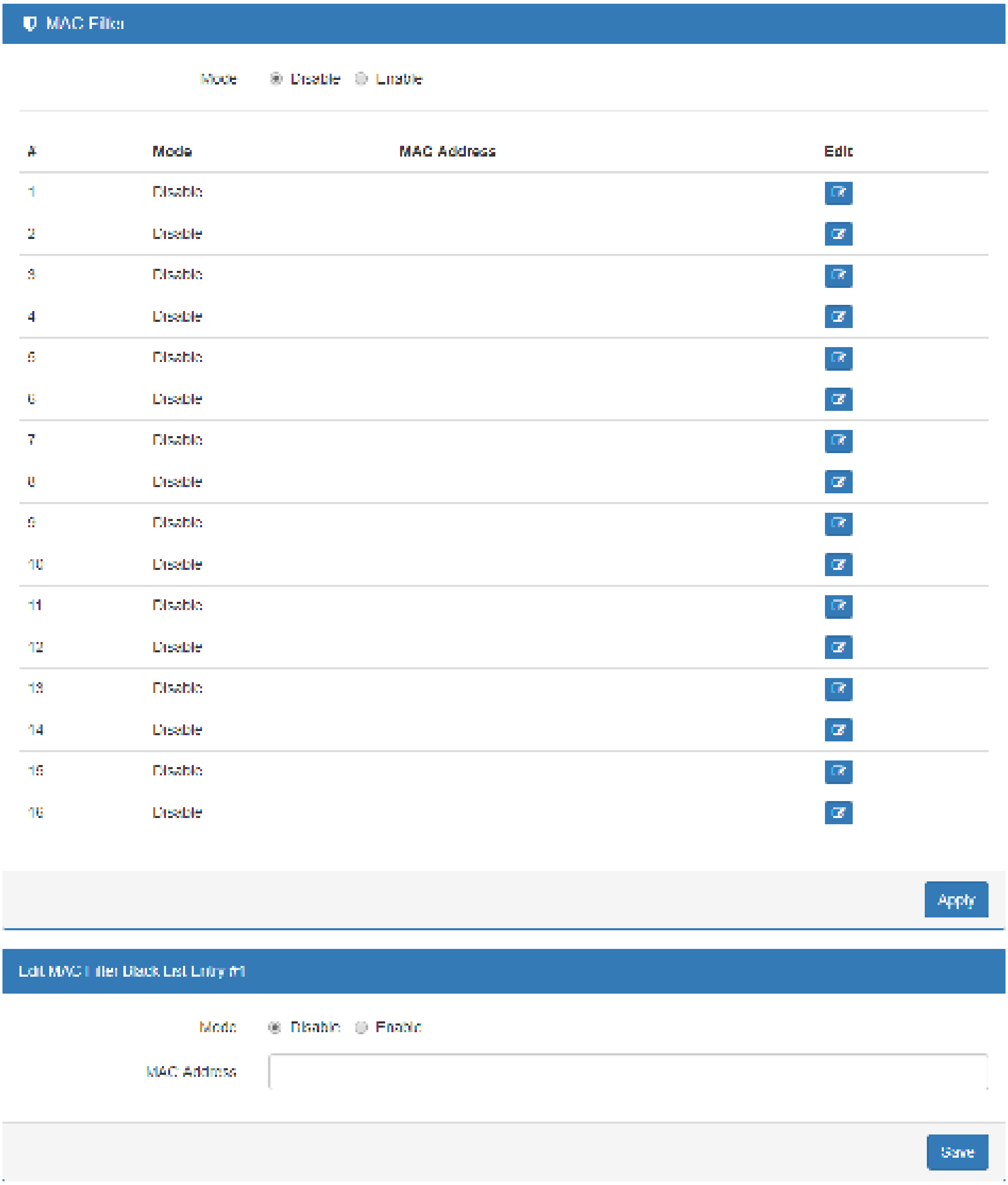
Firewall > Edit IP Filter > Source IP			
IP Format	**Single IP**	**IP with Mask**	**Ranged IP**
IPv4	192.168.0.123	192.168.1.0/24 192.168.1.0/255.255.255.	192.168.1.1- 192.168.1.123
IPv6	2607:f0d0:1002:51::4	2607:f0d0:1002:51::0/64	2607:f0d0:1002:51::4- 2607:f0d0:1002:51::aaaa
Note: Setting up a range 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.

12.4 Firewall > MAC Filter

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



MAC Filter

Mode ● Disable ○ Enable

#	Mode	MAC Address	Edit
1	Disable		✎
2	Disable		✎
3	Disable		✎
4	Disable		✎
5	Disable		✎
6	Disable		✎
7	Disable		✎
8	Disable		✎
9	Disable		✎
10	Disable		✎
11	Disable		✎
12	Disable		✎
13	Disable		✎
14	Disable		✎
15	Disable		✎
16	Disable		✎

Edit MAC Filter Black List Entry #1

Mode ● Disable ○ Enable

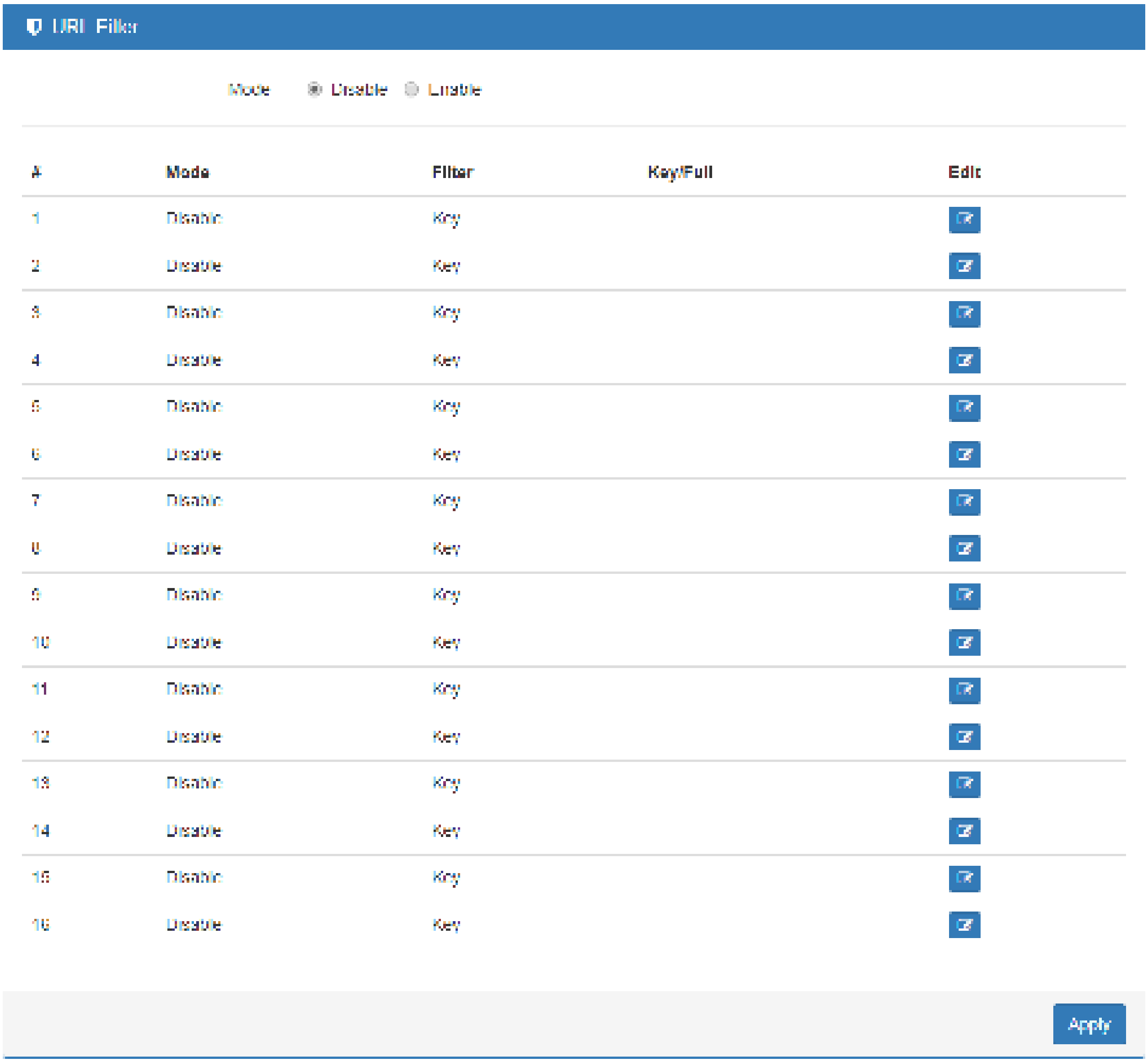
MAC Address

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).

12.5 Firewall > URL Filter

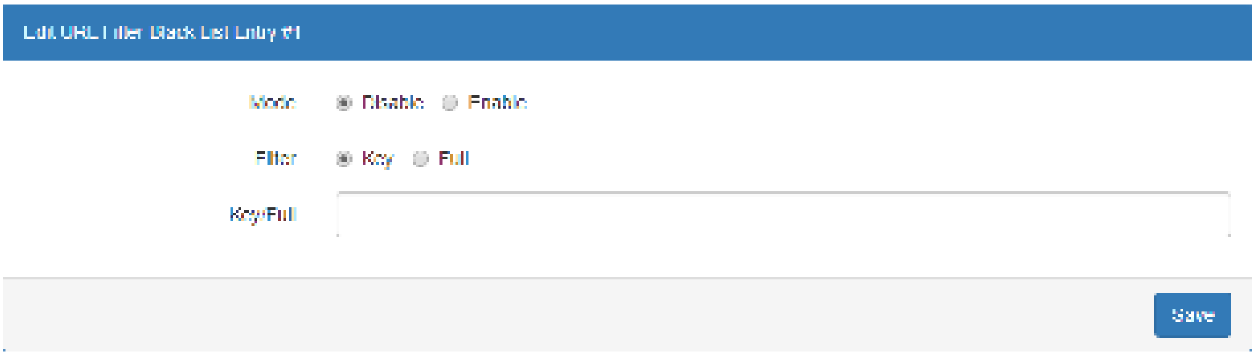
This section allows you to set up URL Filter. After clicking ✎ button, you can edit the type of filter and information.



URL Filter

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		✎



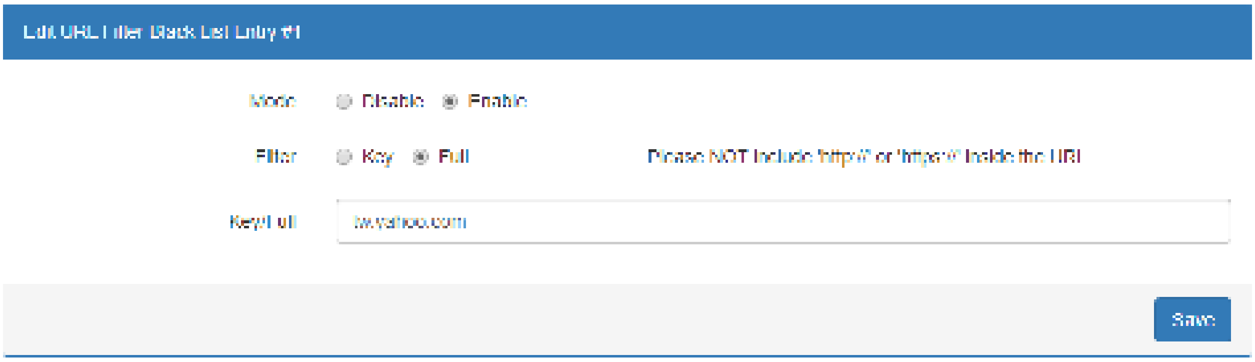
Edit URL Filter Black List Entry #1

Mode ● Disable ○ Enable

Filter ● Key ○ Full

Key/Full

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



Edit URL Filter Black List Entry #1

Mode ○ Disable ● Enable

Filter ○ Key ● Full Please NOT include 'http://' or 'https://' inside the URL

Key/Full tw.yahoo.com

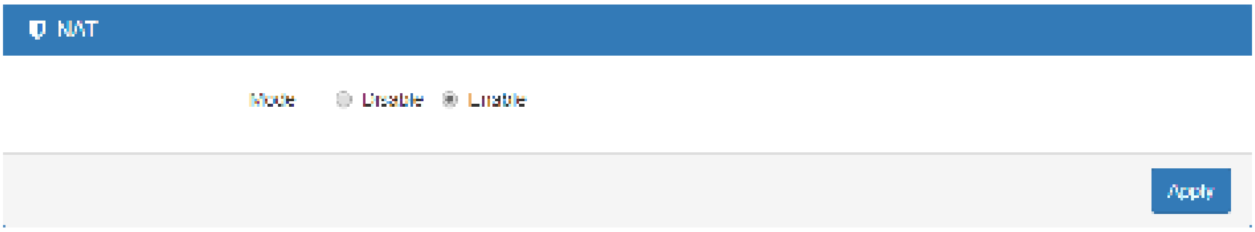
Firewall > URL Filter	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Filter	Select from Key or Full. The default is Key.
Key / Full	Fill in your Key / Full information.

12.6 Firewall > NAT

This section allows you to set NAT configuration.

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

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



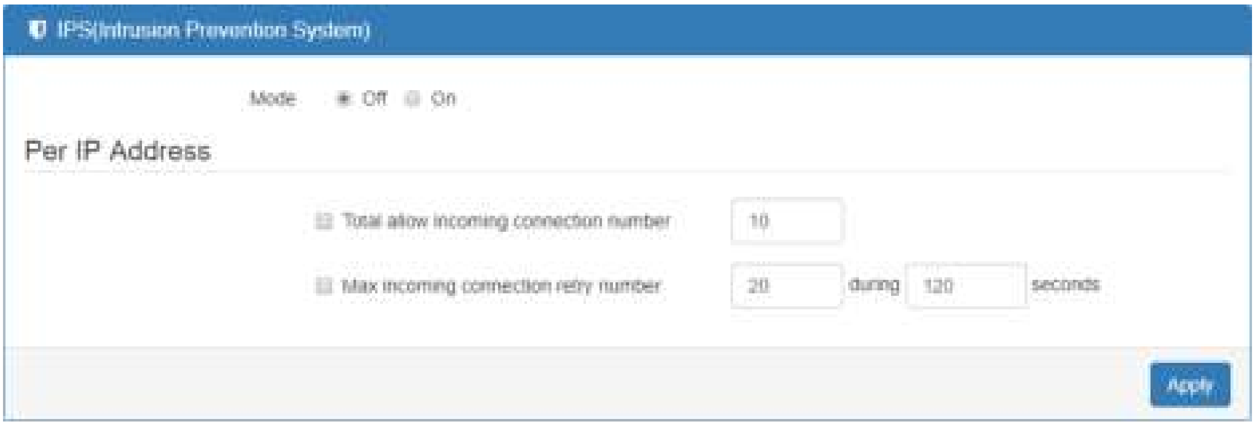
NAT

Mode ○ Disable ● Enable

12.7 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.



IPS(Intrusion Prevention System)

Mode ● Off ○ On

Per IP Address

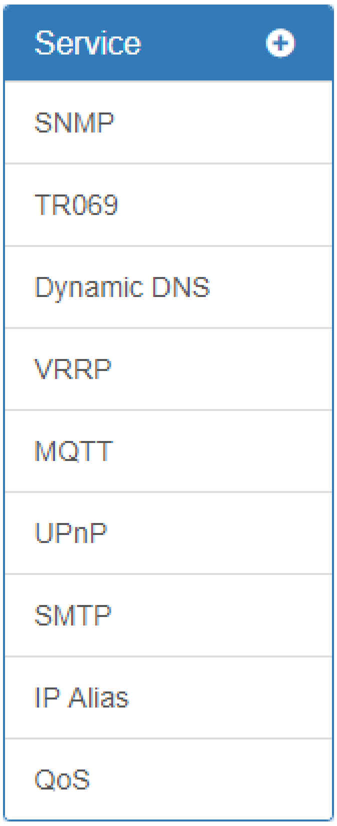
□ Total allow incoming connection number 10

□ Max incoming connection retry number 20 during 120 seconds

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

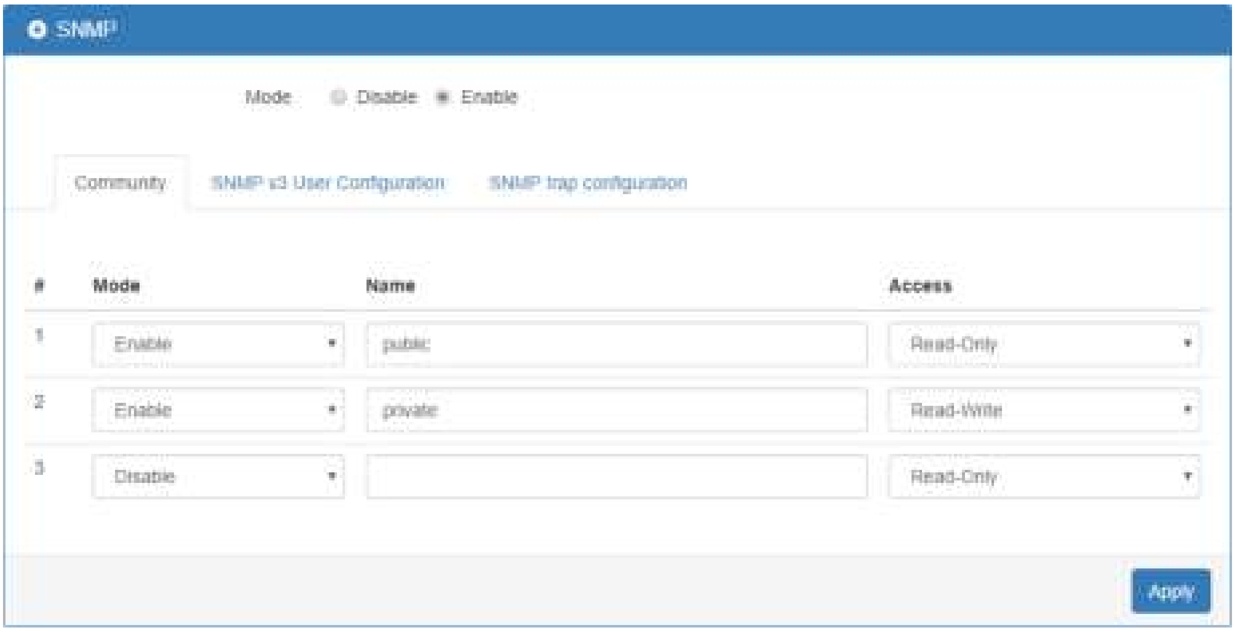
This section allows you to configure the SNMP, TR069, Dynamic DNS, VRRP, MQTT, UPnP, SMTP, and IP Alias.



13.1 Service > SNMP

13.1.1 Community

This section allows you to set the SNMP configuration.



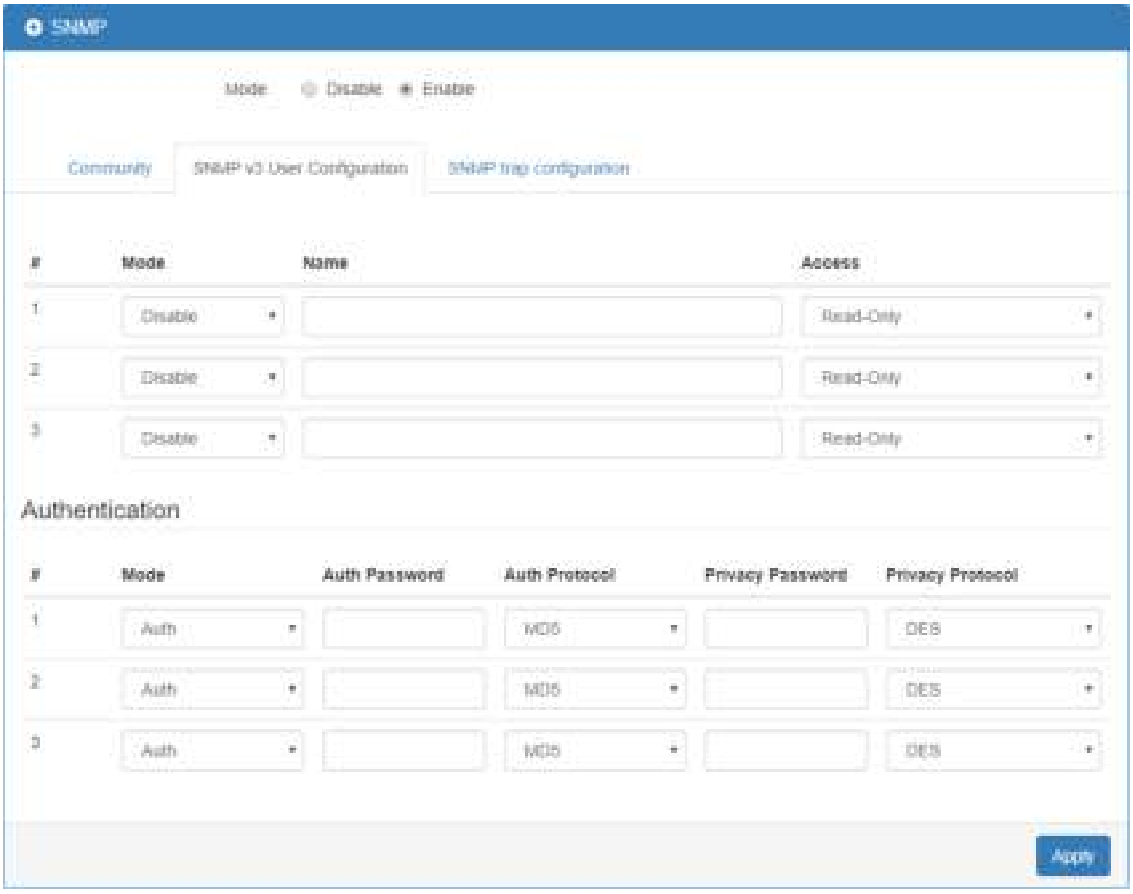
Mode ○ Disable ● Enable

#	Mode	Name	Access
1	Enable	public	Read-Only
2	Enable	private	Read-Write
3	Disable		Read-Only

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



SNMP

Mode ○ Disable ● Enable

Community | SNMP v3 User Configuration | SNMP trap configuration

#	Mode	Name	Access
1	Disable		Read-Only
2	Disable		Read-Only
3	Disable		Read-Only

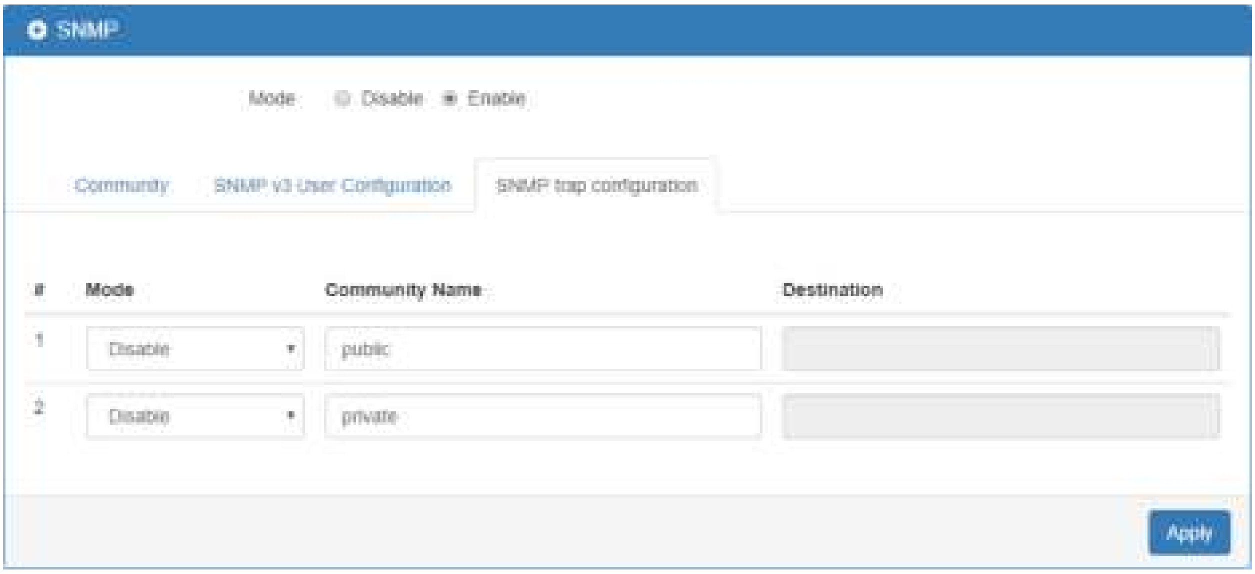
Authentication

#	Mode	Auth Password	Auth Protocol	Privacy Password	Privacy Protocol
1	Auth		MD5		DES
2	Auth		MD5		DES
3	Auth		MD5		DES

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.

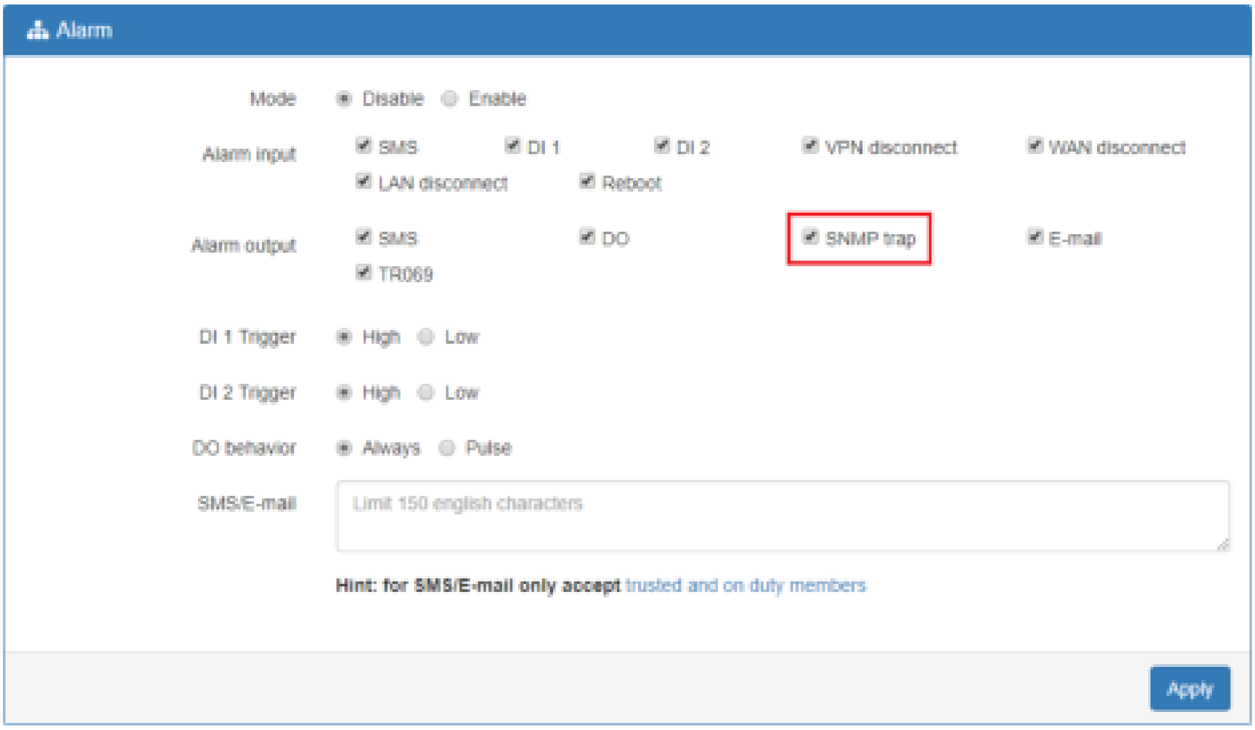
13.1.3 SNMP trap configuration

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.



Mode ○ Disable ● Enable

#	Mode	Community Name	Destination
1	Disable	public	
2	Disable	private	



Mode ● Disable ○ Enable

Alarm input ☑ SMS ☑ DI 1 ☑ DI 2 ☑ VPN disconnect ☑ WAN disconnect ☑ LAN disconnect ☑ Reboot

Alarm output ☑ SMS ☑ DO ☑ SNMP trap ☑ E-mail ☑ TR069

DI 1 Trigger ● High ○ Low

DI 2 Trigger ● High ○ Low

DO behavior ● Always ○ Pulse

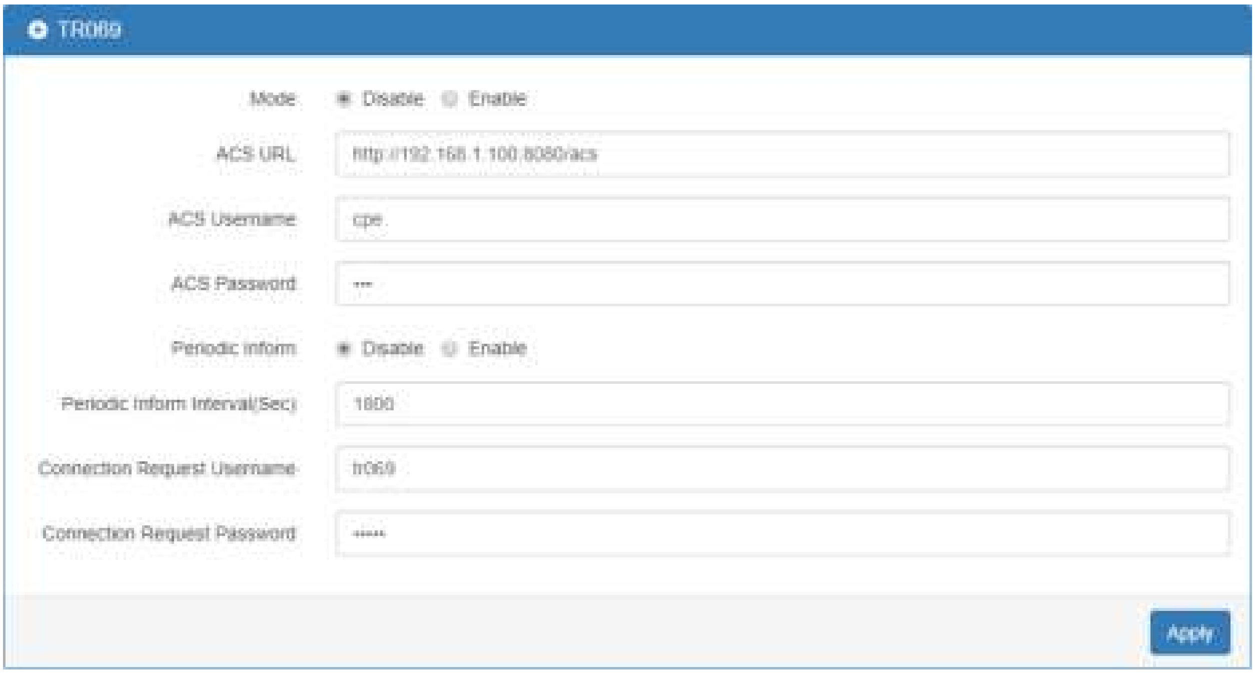
SMS/E-mail Limit 150 english characters

Hint: for SMS/E-mail only accept trusted and on duty members

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.



Mode ● Disable ○ Enable

ACS URL: http://192.168.1.100:8080/acs

ACS Username: cpe

ACS Password: ***

Periodic Inform ● Disable ○ Enable

Periodic Inform Interval(Sec): 1800

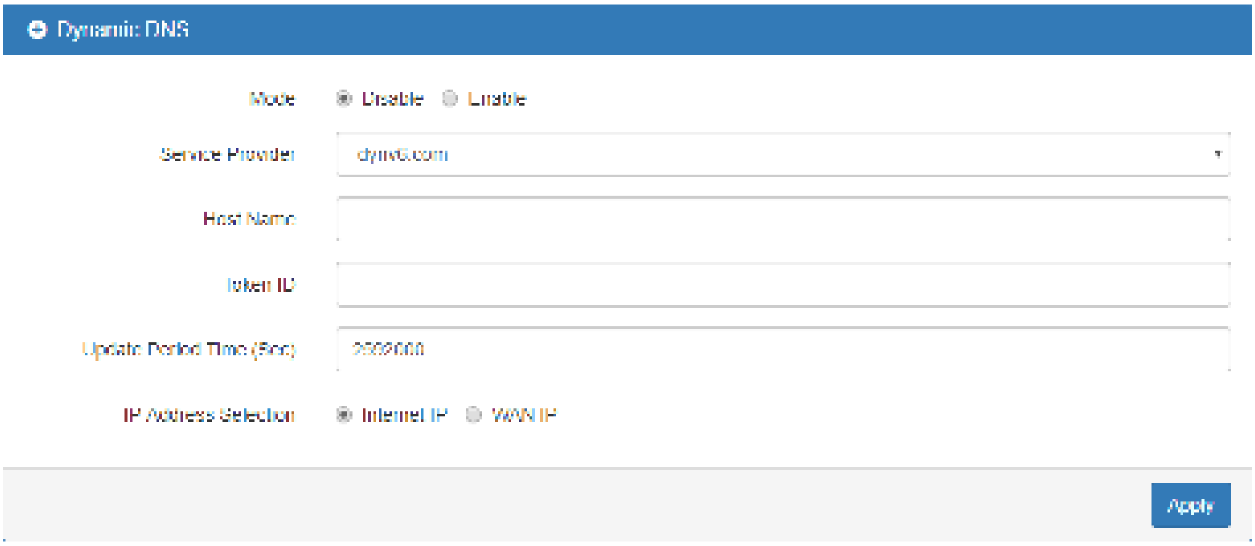
Connection Request Username: tr069

Connection Request Password: ******

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.

13.3 Service > Dynamic DNS

This section allows you to set up Dynamic DNS.



Dynamic DNS

Mode ● Disable ○ Enable

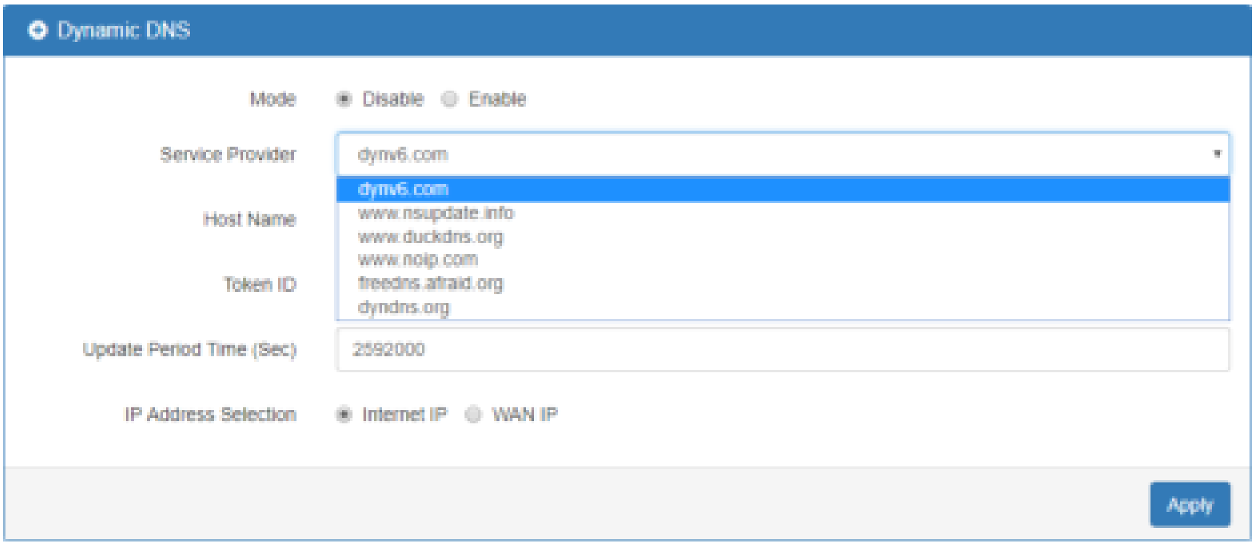
Service Provider: dynv6.com

Host Name:

Token ID:

Update Period Time (Sec): 2592000

IP Address Selection ● Internet IP ○ WAN IP



Dynamic DNS

Mode ● Disable ○ Enable

Service Provider: dynv6.com

- dynv6.com
- www.nsupdate.info
- www.duckdns.org
- www.noip.com
- freedns.afraid.org
- dyndns.org

Host Name

Token ID

Update Period Time (Sec): 2592000

IP Address Selection ● Internet IP ○ WAN IP

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

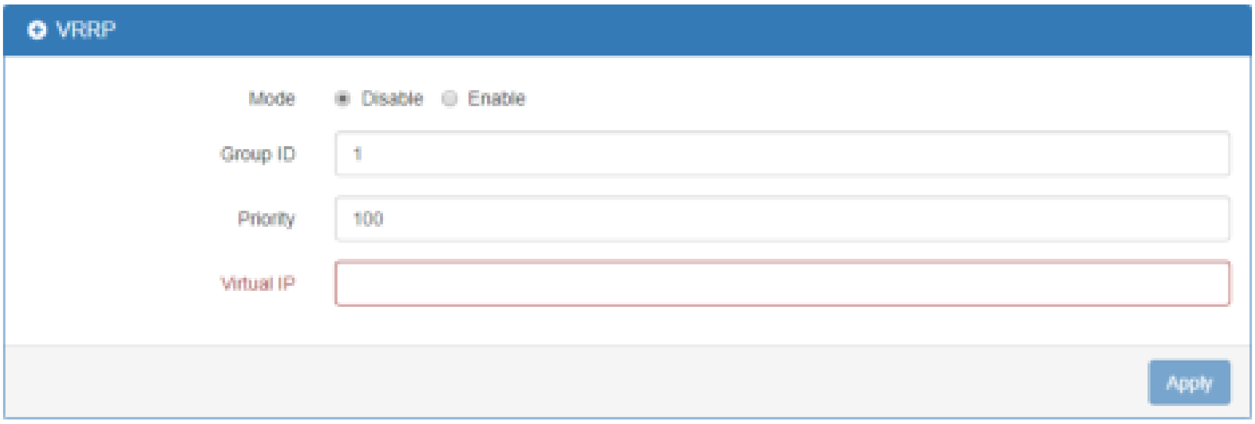
Service Provider	**no-ip.com**
Host Name	Register hostname, e.g. tester.hopto.org
Username	Register username.
Password	Register password.

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.



VRRP

Mode ● Disable ○ Enable

Group ID 1

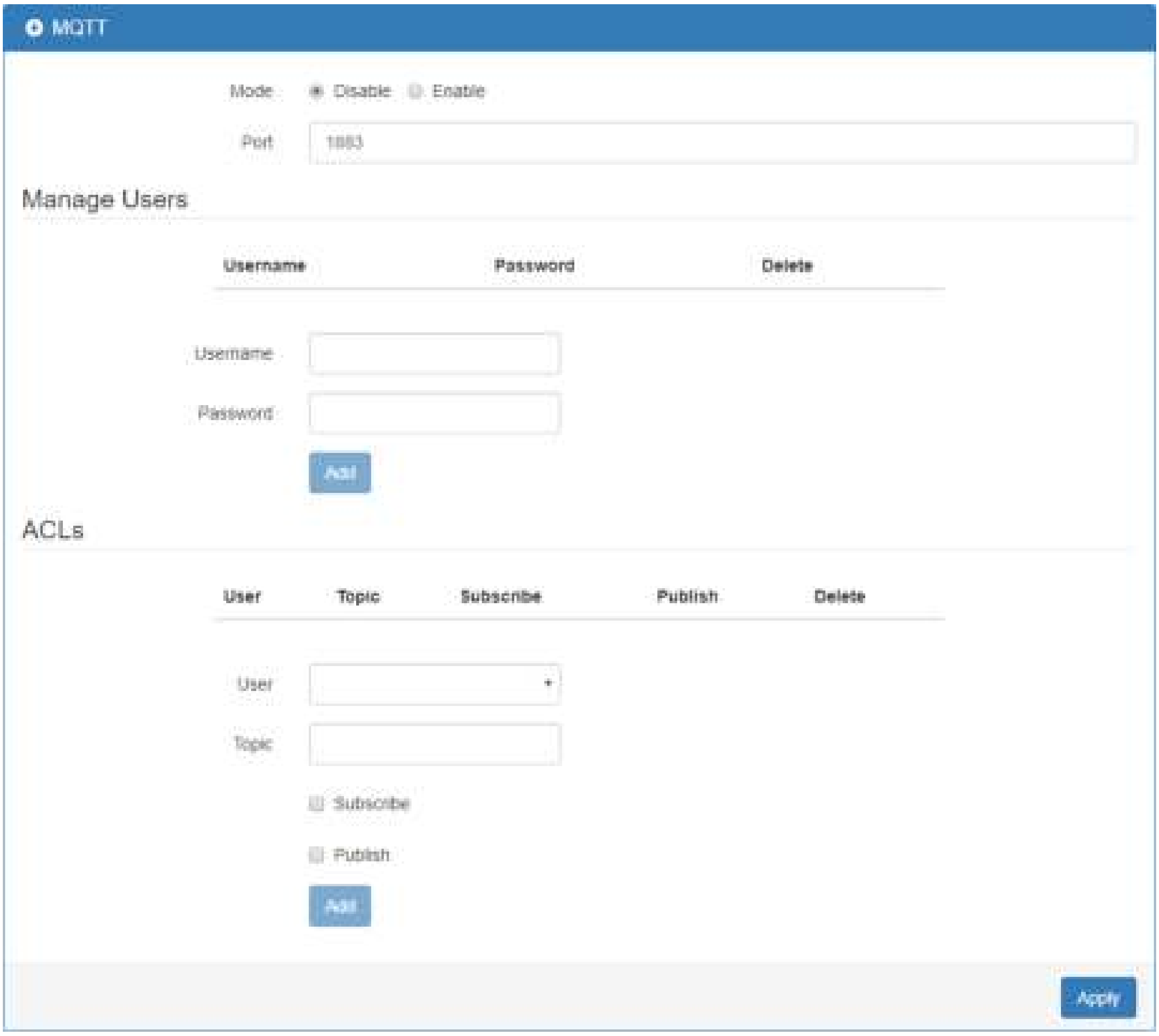
Priority 100

Virtual IP

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.



MQTT

Mode ● Disable ○ Enable

Port 1883

Manage Users

Username	Password	Delete

Username

Password

ACLs

User	Topic	Subscribe	Publish	Delete

User

Topic

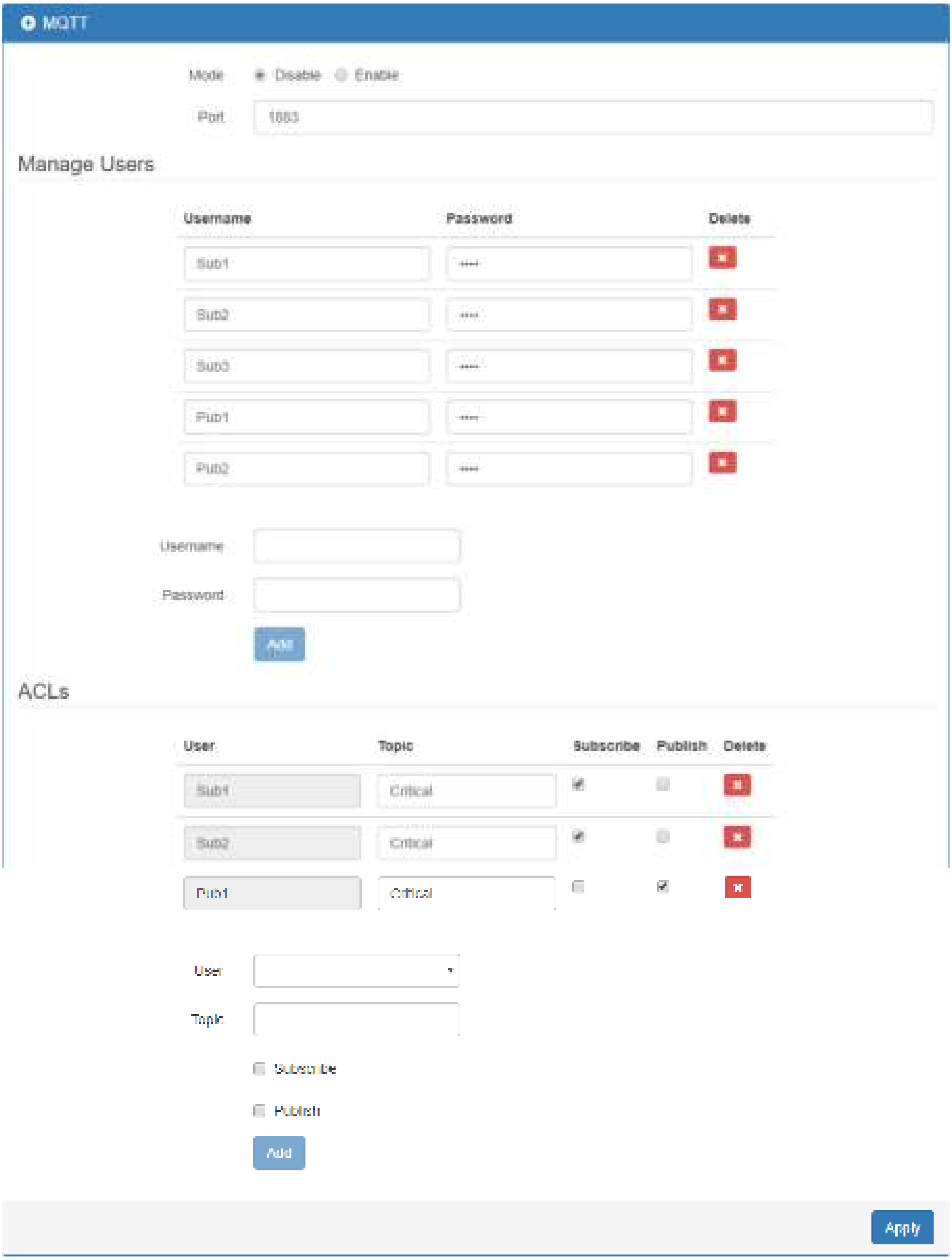
□ Subscribe

□ Publish

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.



MQTT

Mode ● Disable ○ Enable

Port 1883

Manage Users

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

Username

Password

ACLs

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

User

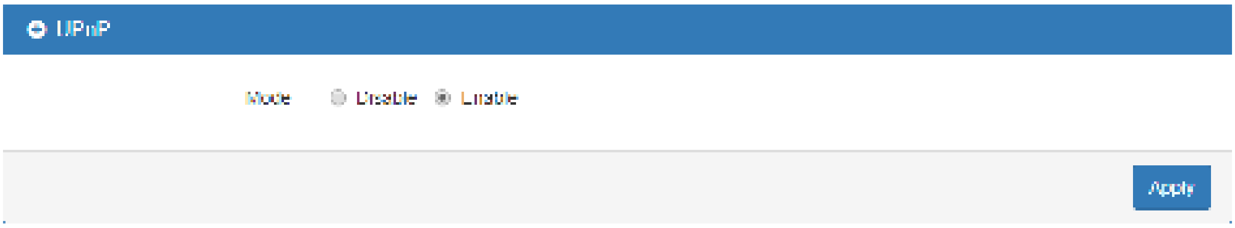
Topic

☐ Subscribe

☐ Publish

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.



UPnP

Mode ○ Disable ● Enable

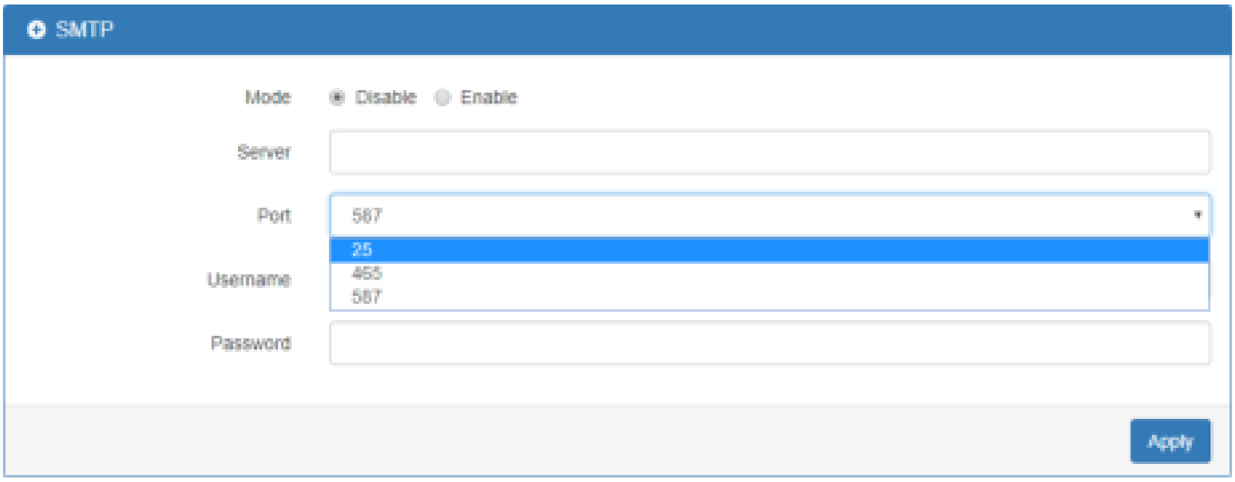
Note:

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.



SMTP

Mode ● Disable ○ Enable

Server

Port 587

Username

Password

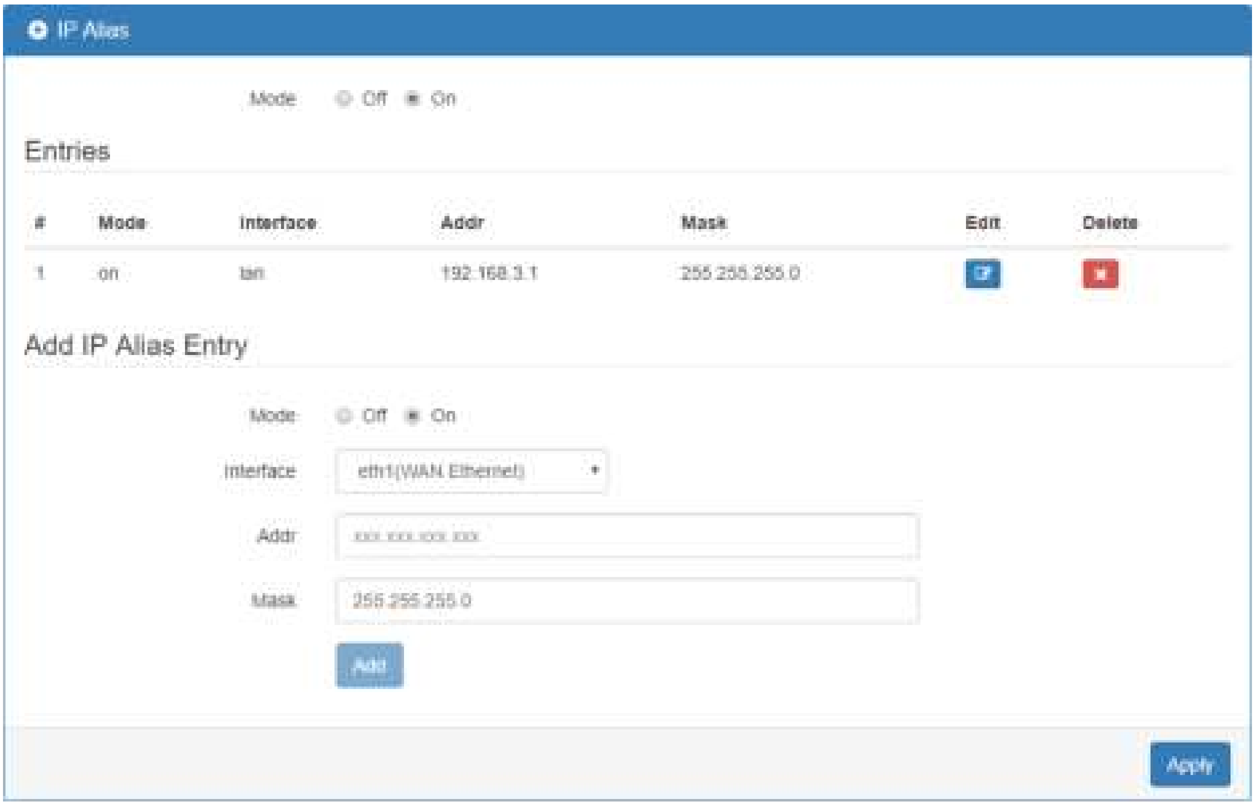
Service > SMTP	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Server	The email will be sent through the server.
Port	There are three ports for SMTP communication between mail servers. ● **Port 25**：Use TCP port 25 without encryption. ● **Port 465**：SMTP connections 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.



IP Alias

Mode ○ Off ● On

Entries

#	Mode	Interface	Addr	Mask	Edit	Delete
1	on	lan	192.168.3.1	255.255.255.0	✎	✖

Add IP Alias Entry

Mode ○ Off ● On

Interface: eth1(WAN Ethernet)

Addr: xxx.xxx.xxx.xxx

Mask: 255.255.255.0

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 Service > QoS (Quality of Service)

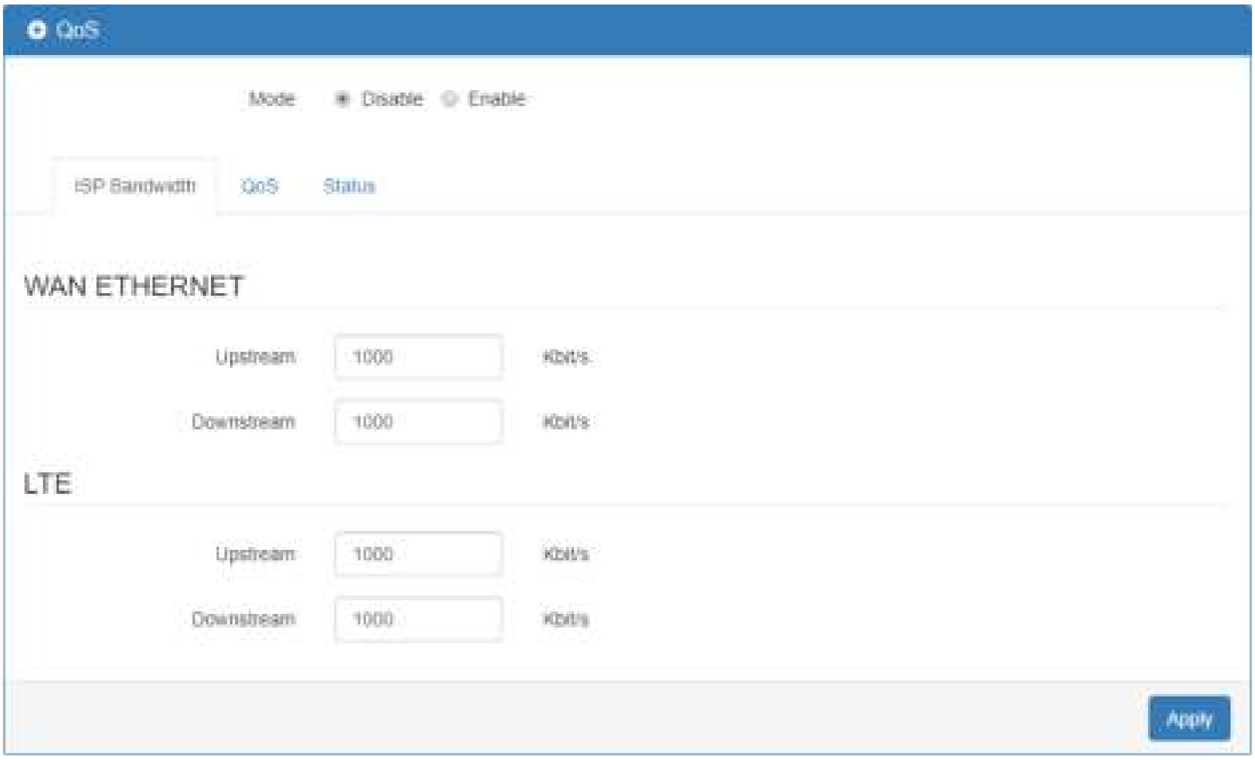
QoS (Quality of Service) refers to a network's ability to achieve maximum bandwidth and allow minimum bandwidth. It guarantees the minimum and limit the maximum bandwidth for certain class of traffic. The QoS configuration has three parts, including ISP bandwidth, QoS and Status.

- **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 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.



Mode ● Disable ○ Enable

WAN ETHERNET

Upstream 1000 Kbit/s

Downstream 1000 Kbit/s

LTE

Upstream 1000 Kbit/s

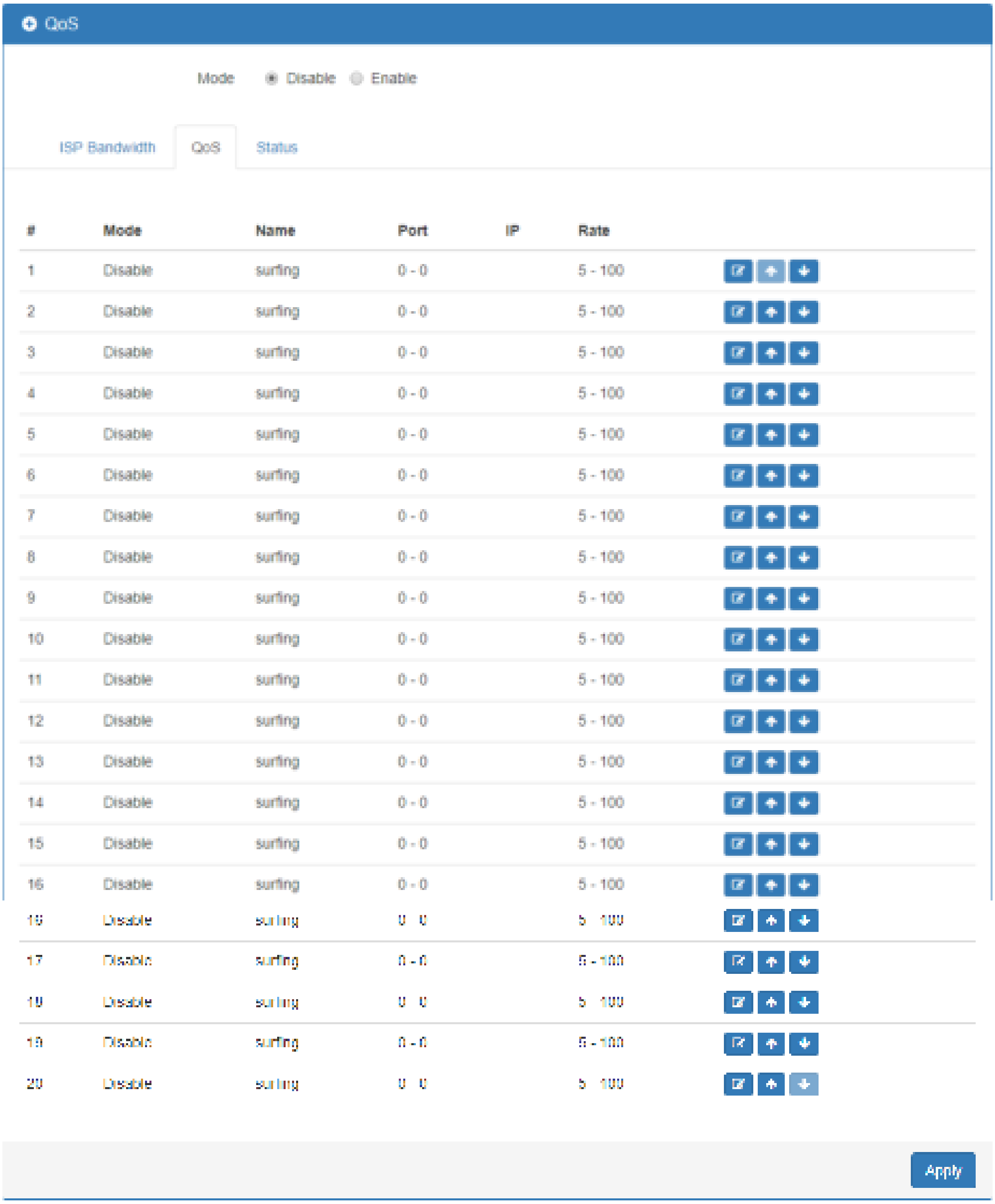
Downstream 1000 Kbit/s

13.9.2 QoS

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

✎ **botton** allows you to edit QoS Entry and configure QoS settings.

↑ ↓ **button** allows you to adjust priority of the QoS entry. The first QoS entry is the highest priority.



QoS

Mode ● Disable ○ Enable

#	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	✎ ↑ ↓
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	✎ ↑ ↓

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

1. Classify traffic by following items:

Service > QoS > Edit QoS Entry	
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.
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.

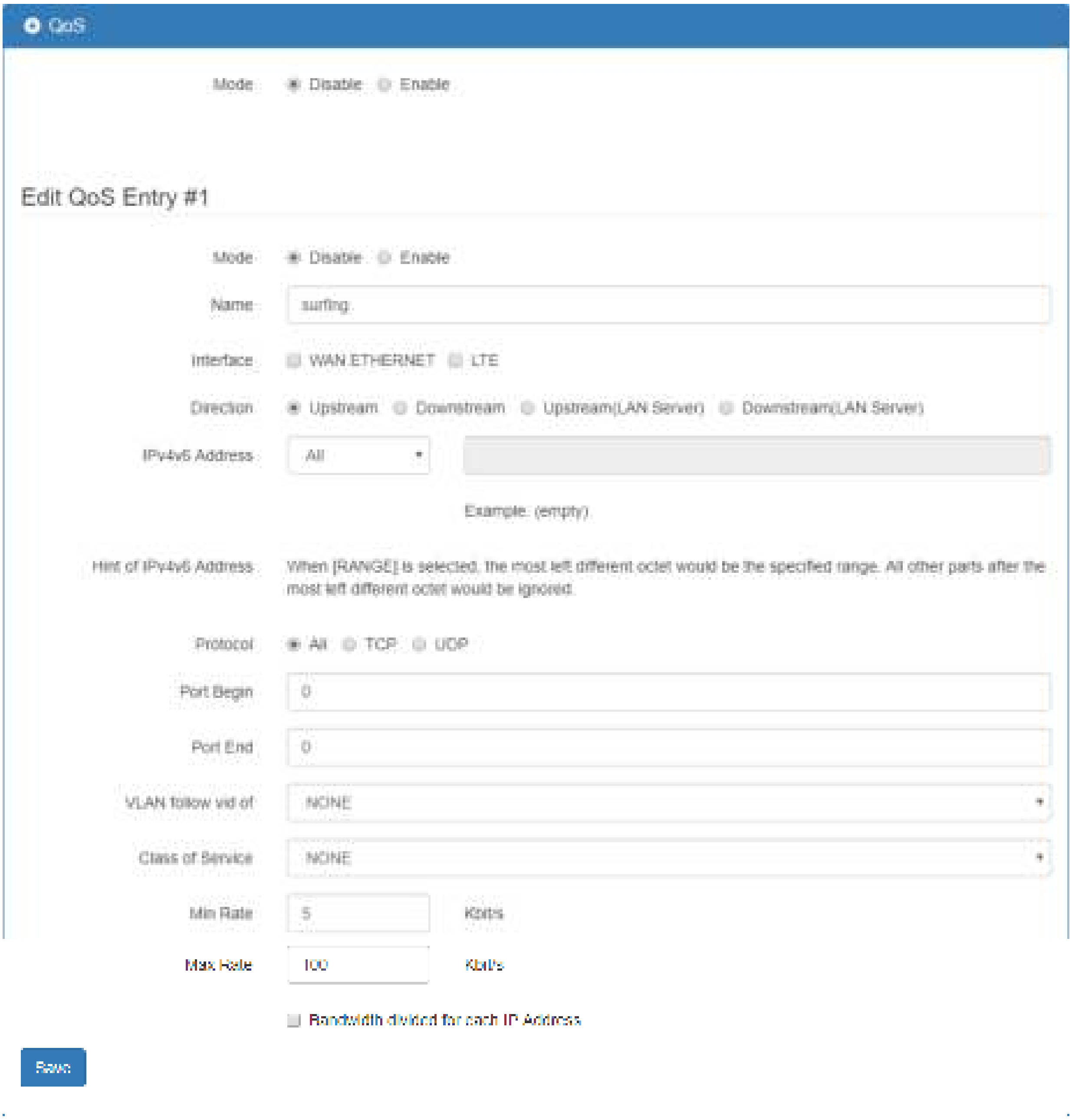
2. **Assign bandwidth by following items:**

   Min Rate / Max Rate: The unit is kilobits per second. Min Rate guarantee the minimum bandwidth and Max Rate is the limit bandwidth.

3. **Assign group IP bandwidth by following items:**

   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 also one octet, 256, from subnet mask bit to subnet mask plus eight bit.



QoS

Mode ● Disable ○ Enable

Edit QoS Entry #1

Mode ● Disable ○ Enable

Name surfing

Interface □ WAN ETHERNET □ LTE

Direction ● Upstream ○ Downstream ○ Upstream(LAN Server) ○ Downstream(LAN Server)

IPv4v6 Address All

Example: (empty)

Hint of IPv4v6 Address When [RANGE] is selected, the most left different octet would be the specified range. All other parts after the most left different octet would be ignored.

Protocol ● All ○ TCP ○ UDP

Port Begin 0

Port End 0

VLAN follow vid of NONE

Class of Service NONE

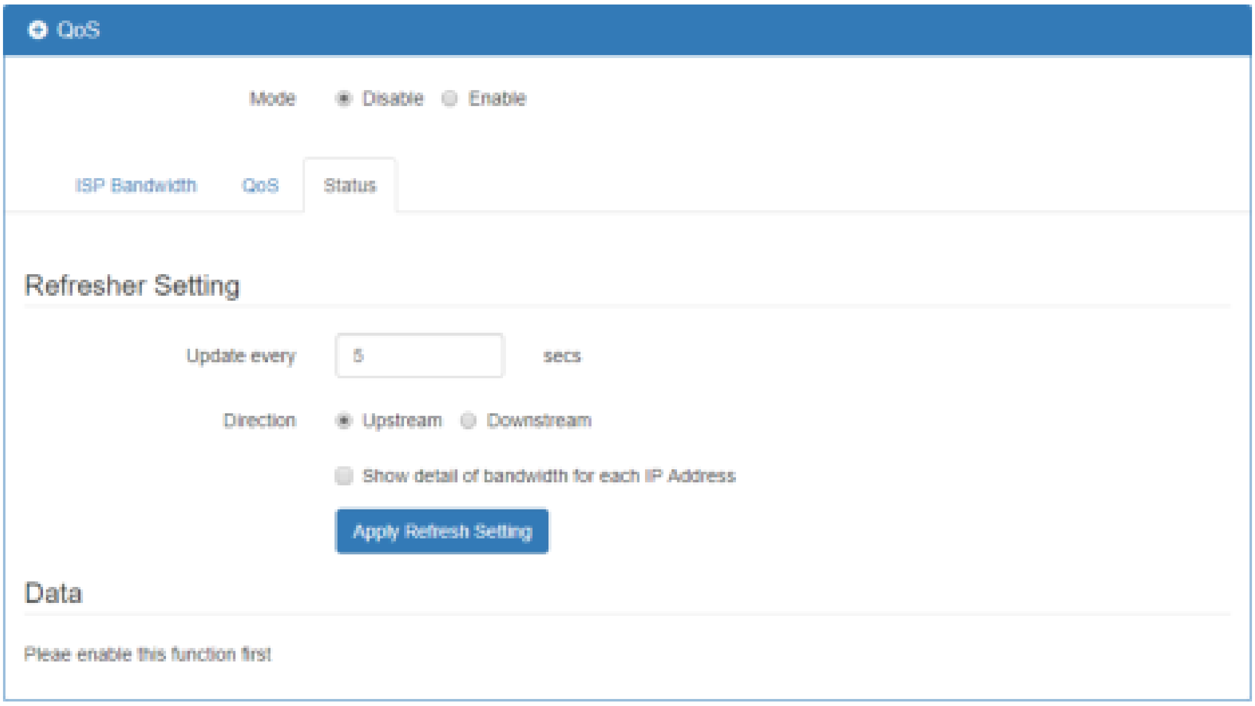
Min Rate 5 Kbits

Max Rate 100 Kbits

□ Bandwidth divided for each IP Address

13.9.3 Status

1. 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.
2. Data part is the content of bandwidth usage.



Mode ● Disable ○ Enable

Refresher Setting

Update every 5 secs

Direction ● Upstream ○ Downstream

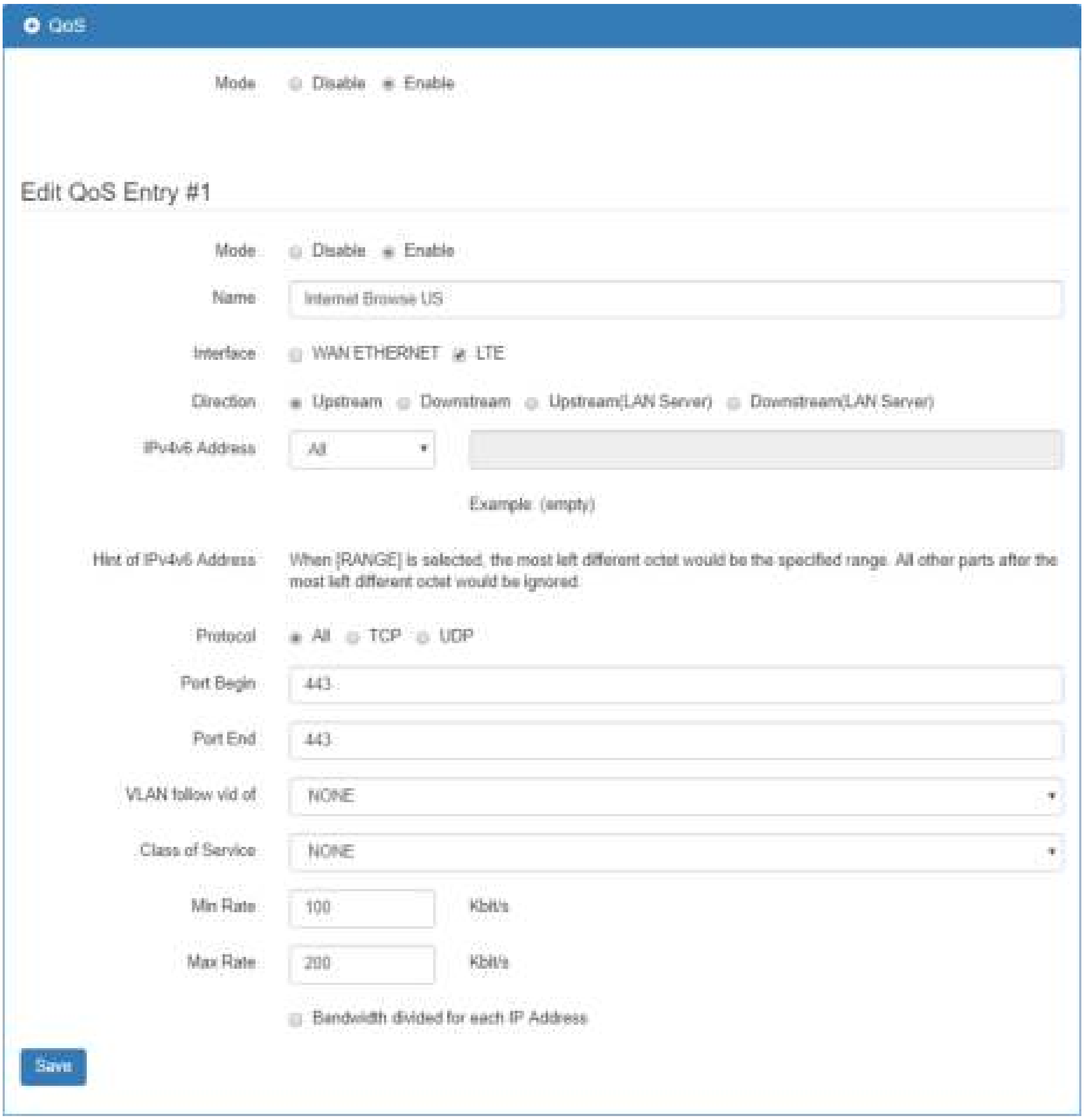
□ Show detail of bandwidth for each IP Address

Data

Pleae enable this function first

13.9.4 The case of Internet Web site access

- Step 1: Set Main Mode as **Enable**
- Step 2: Set QoS **Entry #1**
  - Step 2.1: Set Mode as **Enable**
  - Step 2.2: Set Name as **Internet Browse US**.
  - Step 2.3: Select Interface **LTE**.
  - Step 2.4: Select **Upstream**.
  - Step 2.5: Set Port Begin/End as **443/443**.
  - Step 2.6: Set Min/Max Rate as **100/200**.



QoS

Mode ○ Disable ● Enable

Edit QoS Entry #1

Mode ○ Disable ● Enable

Name: Internet Browse US

Interface ☐ WAN ETHERNET ☑ LTE

Direction ● Upstream ○ Downstream ○ Upstream(LAN Server) ○ Downstream(LAN Server)

IPv4v6 Address: All

Example: (empty)

Hint of IPv4v6 Address: When [RANGE] is selected, the most left different octet would be the specified range. All other parts after the most left different octet would be ignored.

Protocol ● All ○ TCP ○ UDP

Port Begin: 443

Port End: 443

VLAN follow vid of: NONE

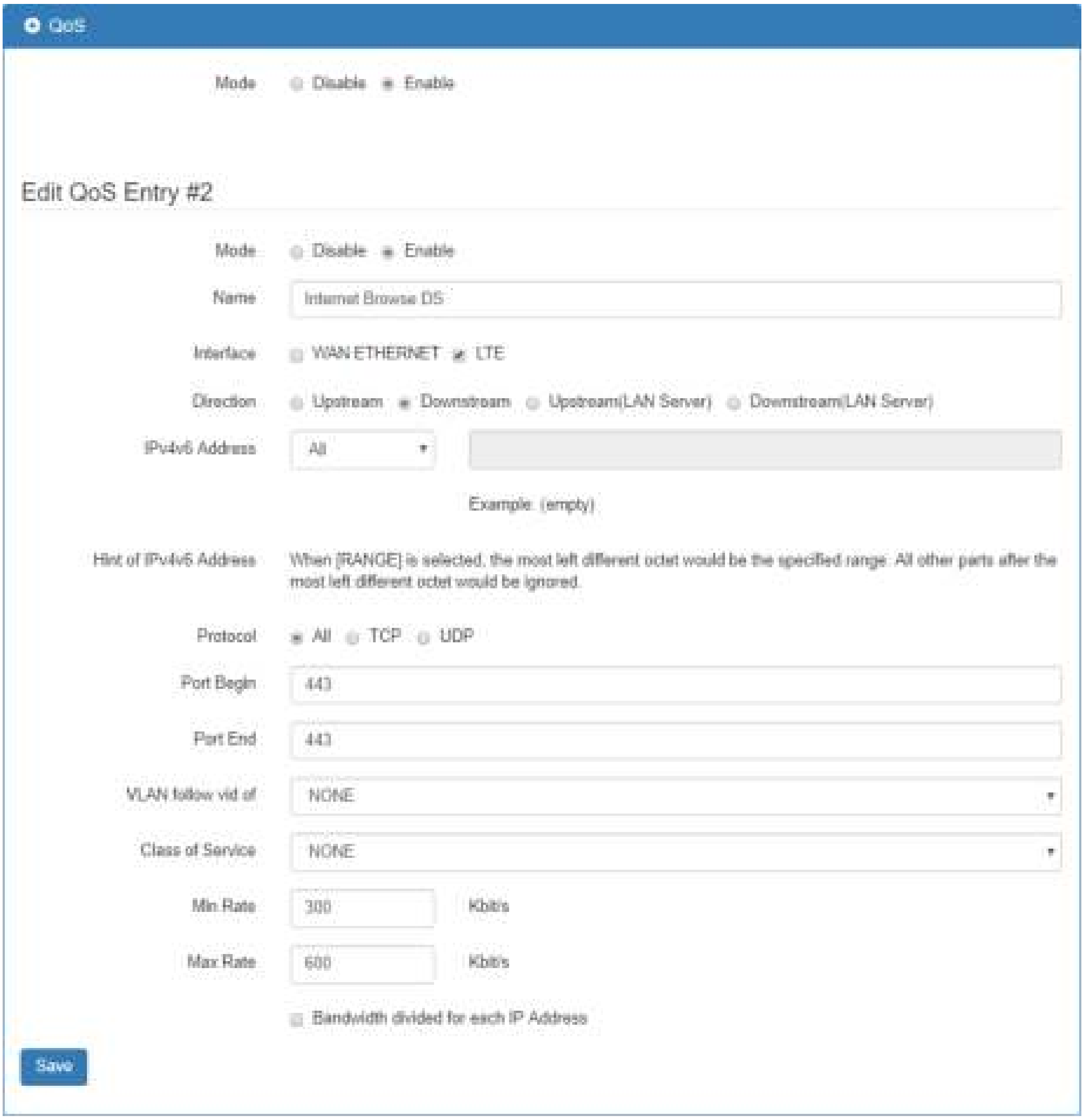
Class of Service: NONE

Min Rate: 100 Kbit/s

Max Rate: 200 Kbit/s

☐ Bandwidth divided for each IP Address

- Step 3: Set QoS **Entry #2**
  - Step 3.1: Set Mode as **Enable**
  - Step 3.2: Set Name as **Internet Browse DS**.
  - Step 3.3: Select Interface **LTE**.
  - Step 3.4: Select **Downstream**.
  - Step 3.5: Set Port Begin/End as **443/443**.
  - Step 3.6: Set Min/Max Rate as **300/600**.



QoS

Mode ○ Disable ● Enable

Edit QoS Entry #2

Mode ○ Disable ● Enable

Name: Internet Browse DS

Interface ☐ WAN ETHERNET ☑ LTE

Direction ○ Upstream ● Downstream ○ Upstream(LAN Server) ○ Downstream(LAN Server)

IPv4v6 Address: All

Example: (empty)

Hint of IPv4v6 Address: When [RANGE] is selected, the most left different octet would be the specified range. All other parts after the most left different octet would be ignored.

Protocol ● All ○ TCP ○ UDP

Port Begin: 443

Port End: 443

VLAN follow vid of: NONE

Class of Service: NONE

Min Rate: 300 Kbit/s

Max Rate: 600 Kbit/s

☐ Bandwidth divided for each IP Address

- Step 4: Apply
- Step 5: Check the internet access is ok through LTE. (Since we selected LTE interface.)
- Step 6: Start browse the internet from LAN PC.
- Step 7: Check Upstream Status.

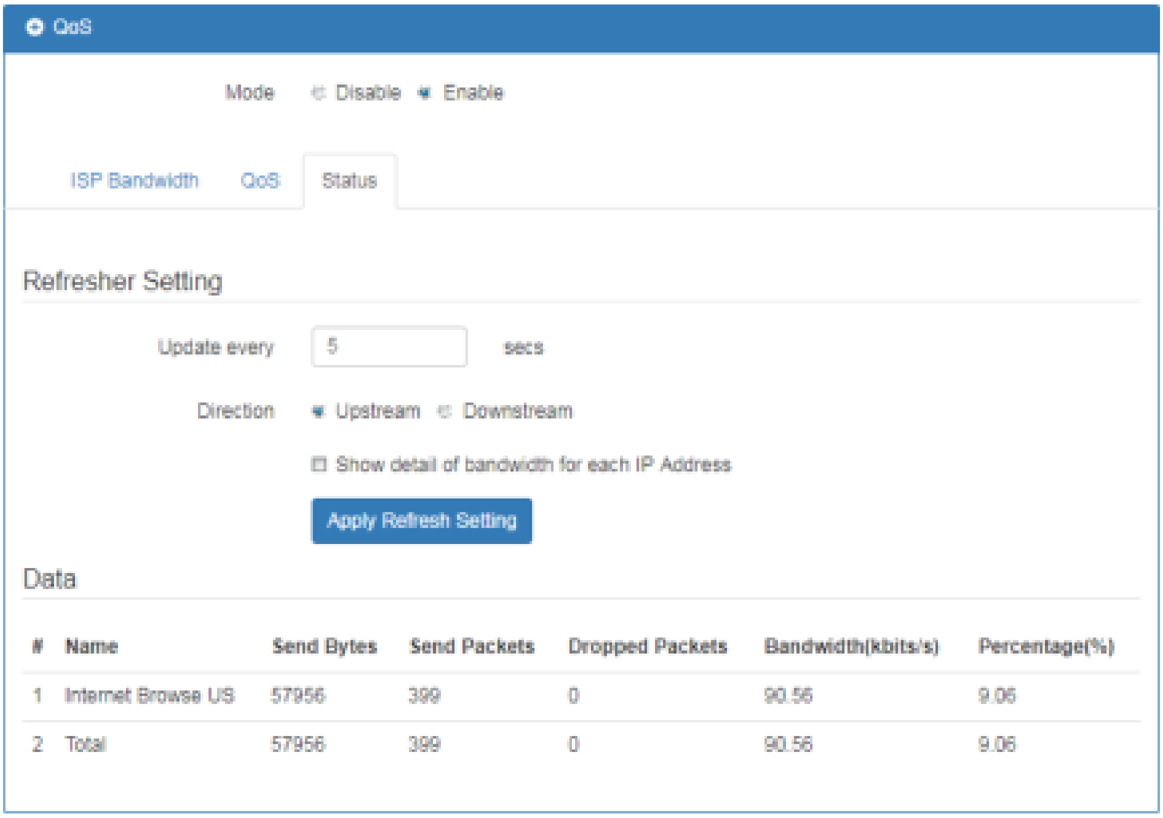
  The traffic in entry “Internet Browse US” is Upstream, LAN to WAN, and send request to public Web Server with destination port number 443.

  The base of percentage is ISP Bandwidth > LTE > Upstream setting. It is 1000 kbps in our case.

- Step 8: Check Status Downstream.

  The traffic in entry “ Internet Browse DS ” is Downstream, WAN to LAN, and send response from public Web Server with source port number 443.

  The base of percentage is ISP Bandwidth > LTE > Downstream setting. It is 1000 kbps in our example.



QoS

Mode ○ Disable ● Enable

ISP Bandwidth | QoS | Status

Refresher Setting

Update every 5 secs

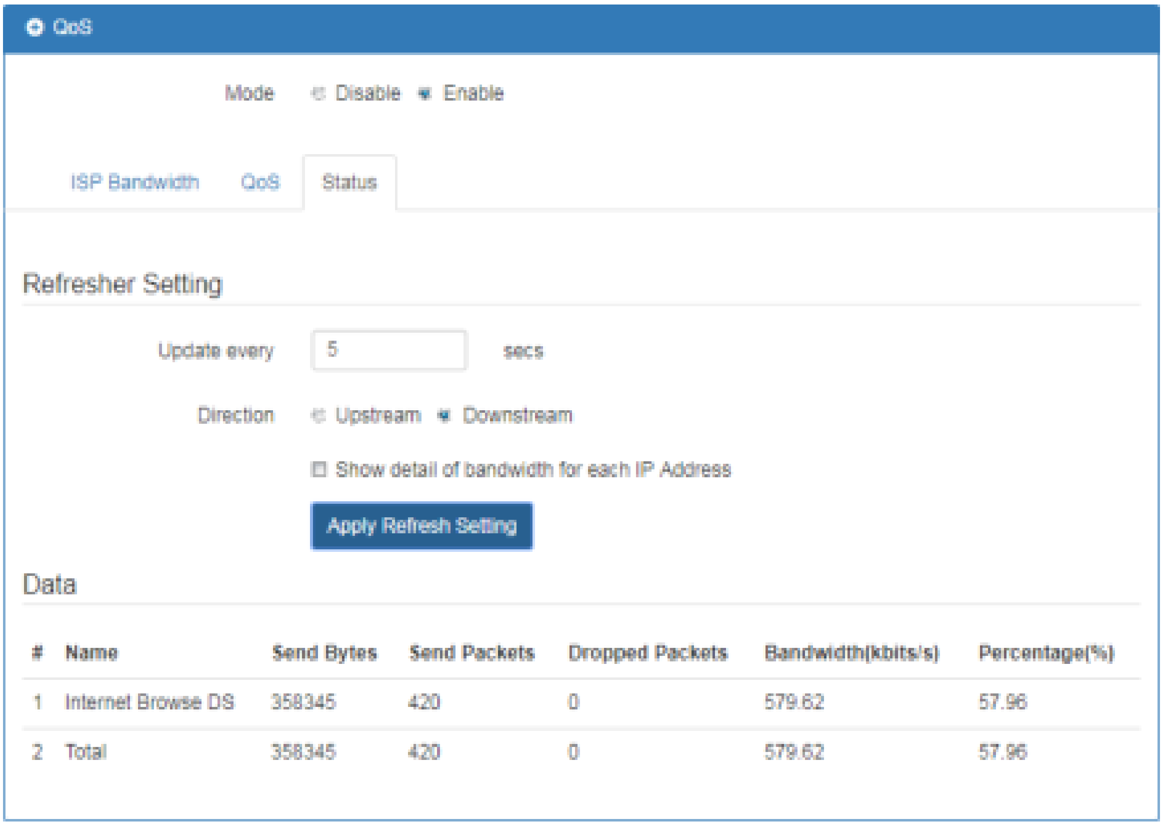
Direction ● Upstream ○ Downstream

□ Show detail of bandwidth for each IP Address

Apply Refresh Setting

Data

#	Name	Send Bytes	Send Packets	Dropped Packets	Bandwidth(kbits/s)	Percentage(%)
1	Internet Browse US	57956	399	0	90.56	9.06
2	Total	57956	399	0	90.56	9.06



QoS

Mode ○ Disable ● Enable

ISP Bandwidth | QoS | Status

Refresher Setting

Update every 5 secs

Direction ○ Upstream ● Downstream

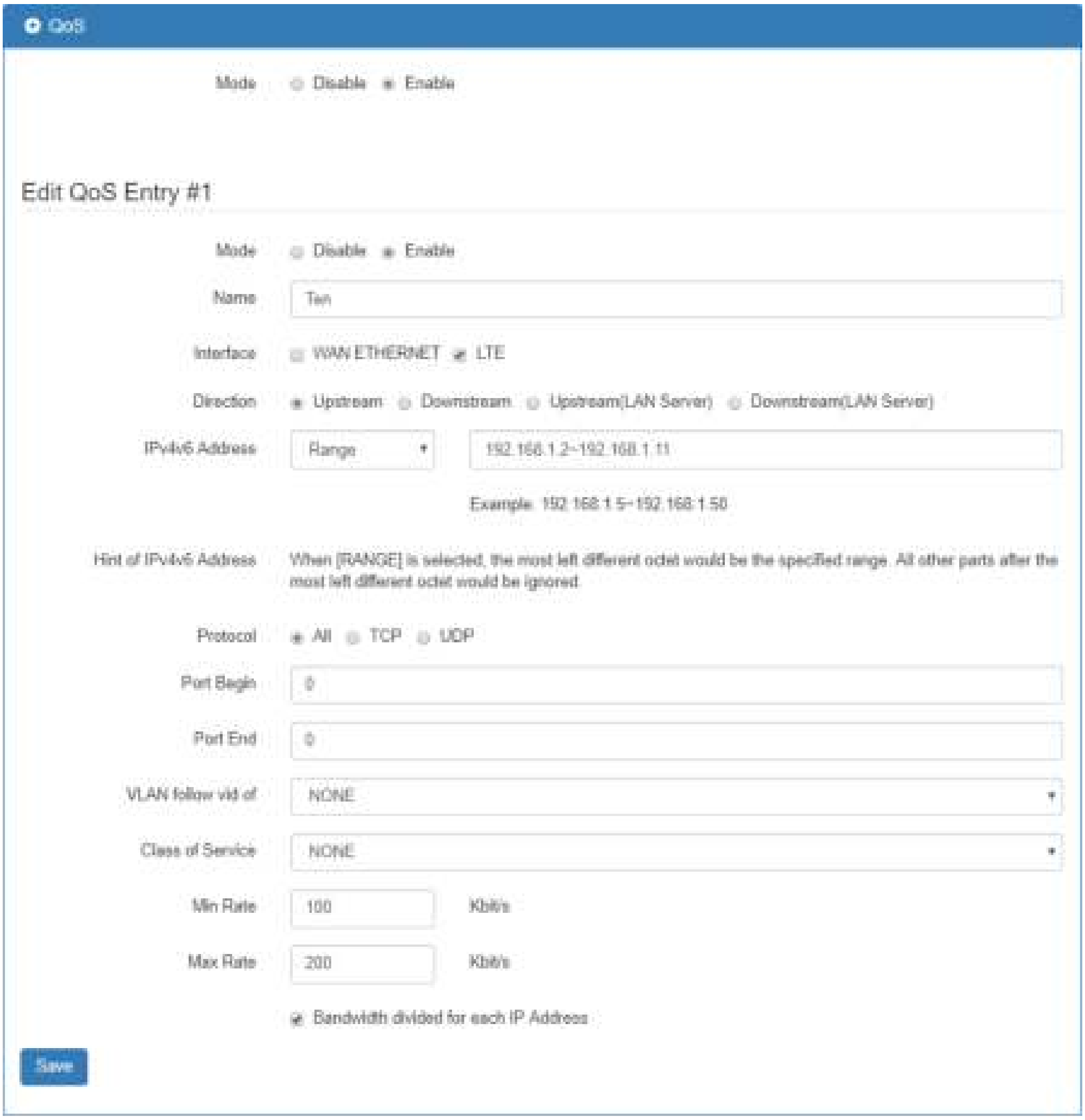
□ Show detail of bandwidth for each IP Address

Apply Refresh Setting

Data

#	Name	Send Bytes	Send Packets	Dropped Packets	Bandwidth(kbits/s)	Percentage(%)
1	Internet Browse DS	358345	420	0	579.62	57.96
2	Total	358345	420	0	579.62	57.96

13.9.5 Bandwidth divided for each IP address



QoS

Mode ○ Disable ● Enable

Edit QoS Entry #1

Mode ○ Disable ● Enable

Name: Ten

Interface ☐ WAN ETHERNET ☑ LTE

Direction ● Upstream ○ Downstream ○ Upstream(LAN Server) ○ Downstream(LAN Server)

IPv4v6 Address: Range ▾ 192.168.1.2~192.168.1.11

Example: 192.168.1.5~192.168.1.50

Hint of IPv4v6 Address: When [RANGE] is selected, the most left different octet would be the specified range. All other parts after the most left different octet would be ignored.

Protocol ● All ○ TCP ○ UDP

Port Begin: 0

Port End: 0

VLAN follow vid of: NONE ▾

Class of Service: NONE ▾

Min Rate: 100 Kbit/s

Max Rate: 200 Kbit/s

☑ Bandwidth divided for each IP Address

There are ten number of IP addresses. The most left different octet is “ 11 ” in 192.168.1.11 and “ 2 ” in 192.168.1.2, so number of IP addresses is calculated by 11 minus 2 and plus one for boundary.

The Min rate will be divided by ten, 100/10=10 kbit/s for each IP address 192.168.1.2 to 192.168.1.11.

The Max rate is same with configuration for all IP addresses, 192.168.1.2 to 192.168.1.11, since we don't want to waste the bandwidth when there is just one IP address in use. For example, if only 192.168.1.2 have traffic to send/receive, then it can use all of the 200 kbit/s.

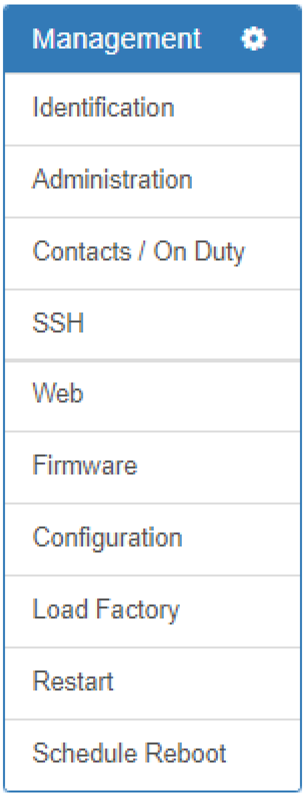
In the same case except changing IPv4v6 address field to 192.168.1.0~192.168.2.0, there are two number of IP addresses. The most left different octet is “ 2 ” in 192.168.2.0 and “ 1 ” in 192.168.1.0, so number of IP addresses is calculated by 2 minus 1 and plus one for boundary.

The Min rate will be divided by two, 100/2=50 kbit/s for IP address 192.168.2.0 and 192.168.1.0.

The Max rate is same with configuration for both IP addresses, 192.168.1.0 and 192.168.2.0, since we don't want to waste the bandwidth when there is just one IP address in using. For example, if only 192.168.1.0 have traffic to send/receive, then it can use all of the 200 kbit/s.

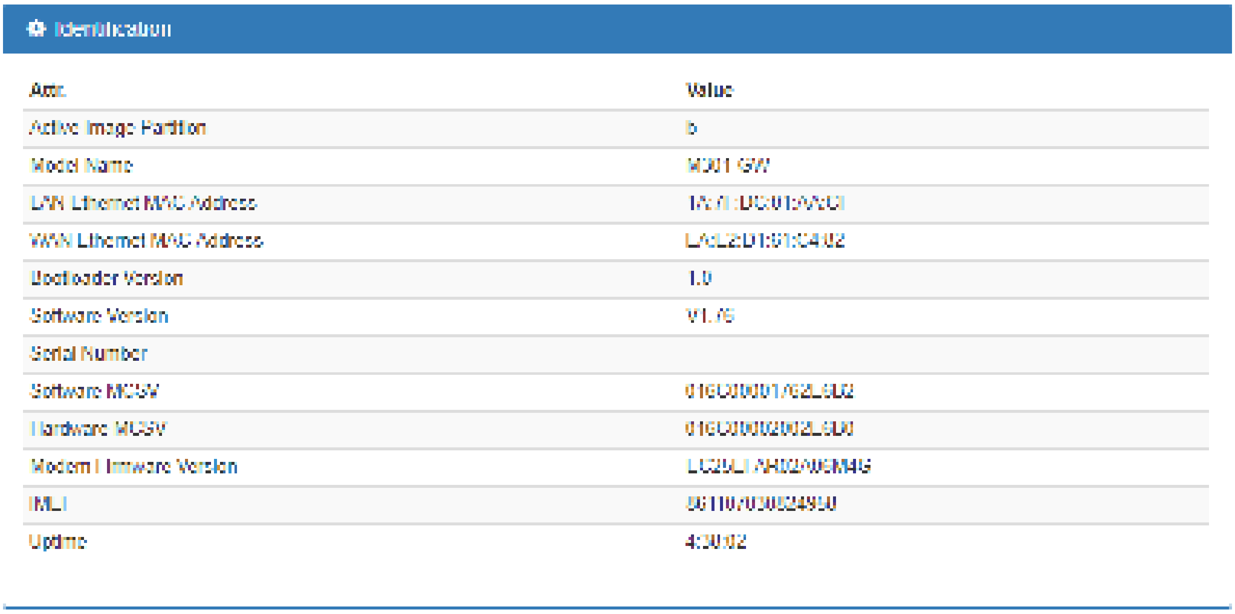
14 Configuration > Management

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.



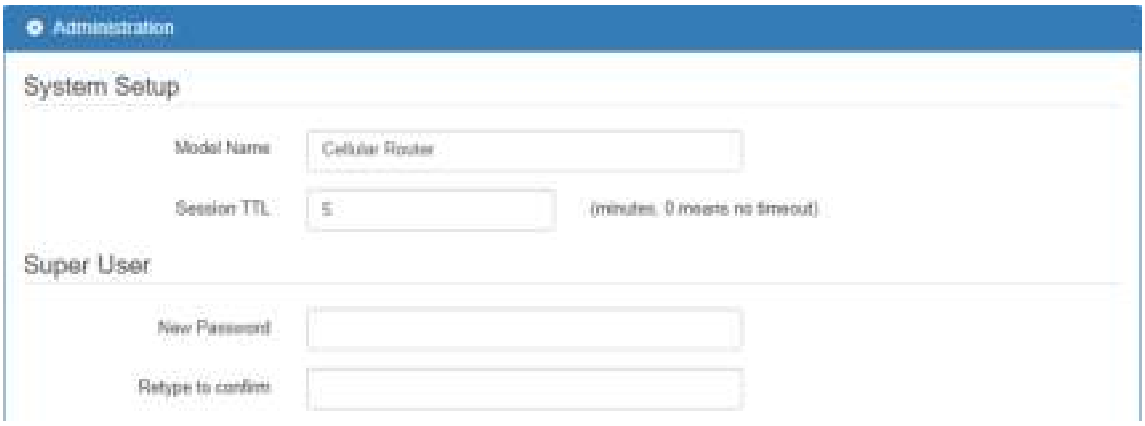
Identification

Attr.	Value
Active Image Partition	b
Model Name	M301-GW
LAN Ethernet MAC Address	[illegible]
WAN Ethernet MAC Address	EA:E2:D1:91:C4:02
Bootloader Version	1.0
Software Version	V1.76
Serial Number	
Software MCSV	01GC0000176 2L6L02
Hardware MCSV	01GC00000200 2L6L00
Modem Firmware Version	EC25EFAR02A06M4G
IMEI	861107030524950
Uptime	4:30:02

Management > Identification	
Item	**Description**
Model Name	Show the model name of cellular router.
LAN Ethernet MAC Address	Show the LAN Ethernet MAC address.
WAN Ethernet MAC Address	Show the WAN Ethernet MAC address.
Bootloader Version	Show the bootloader version currently running on the device.
Software Version	Show the software version currently running on the device
Serial Number	Show the product serial number.
Software MCSV	Show the software MCSV of the running firmware
Hardware MCSV	Show the current hardware MCSV of the device.
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.

14.2 Management > Administration

This section allows you to set up the name of router 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.



Administration

System Setup

Model Name: Cellular Router

Session TTL: 5 (minutes, 0 means no timeout)

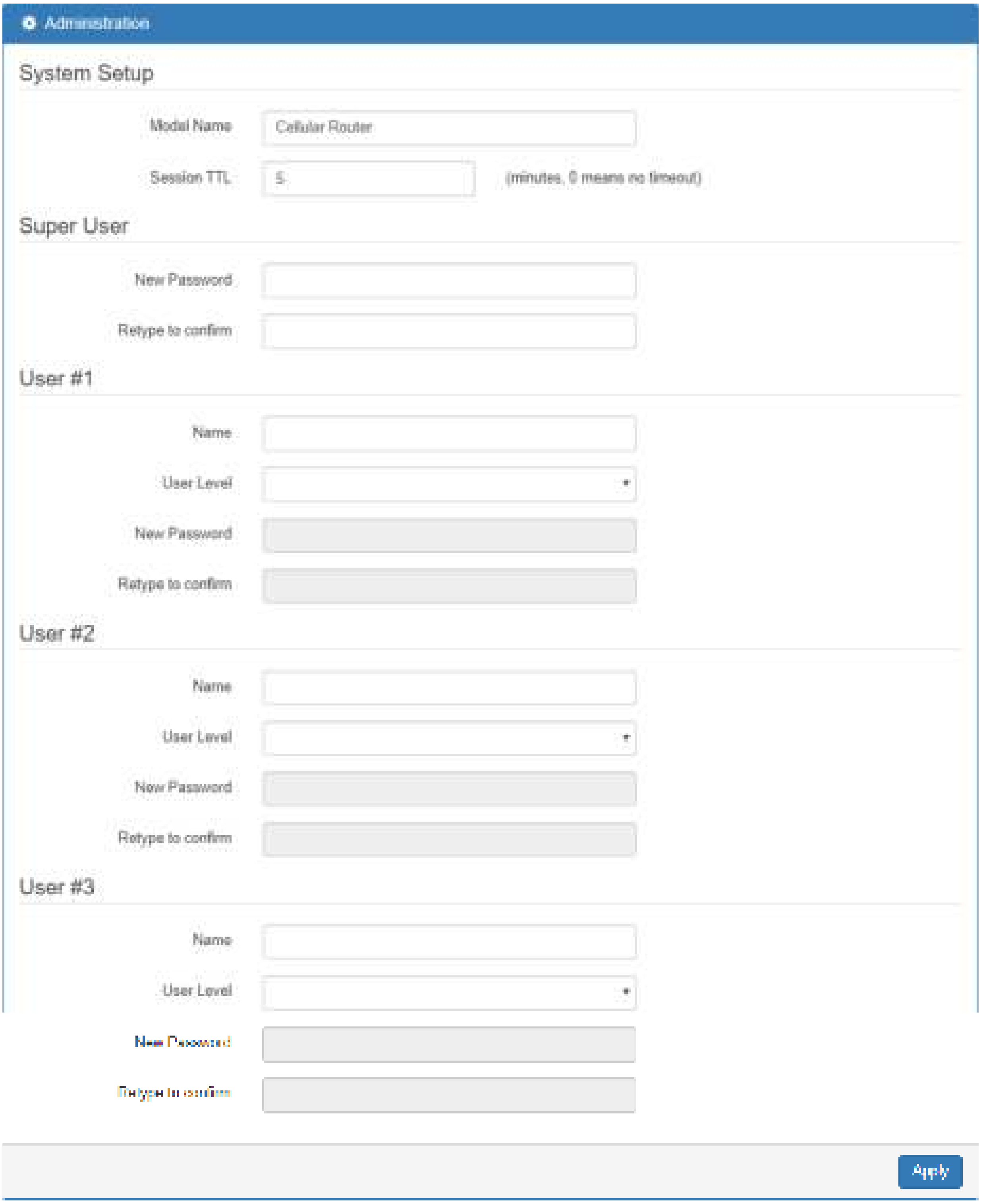
Super User

New Password:

Retype to confirm:

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.

User Level **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	(1) Add/Delete/Modify all users' accounts except Super User. (2) Read/Write Configuration	Read / Write Configuration	only Read Configuration	N/A



Administration

System Setup

Model Name: Cellular Router

Session TTL: 5 (minutes, 0 means no timeout)

Super User

New Password:

Retype to confirm:

User #1

Name:

User Level:

New Password:

Retype to confirm:

User #2

Name:

User Level:

New Password:

Retype to confirm:

User #3

Name:

User Level:

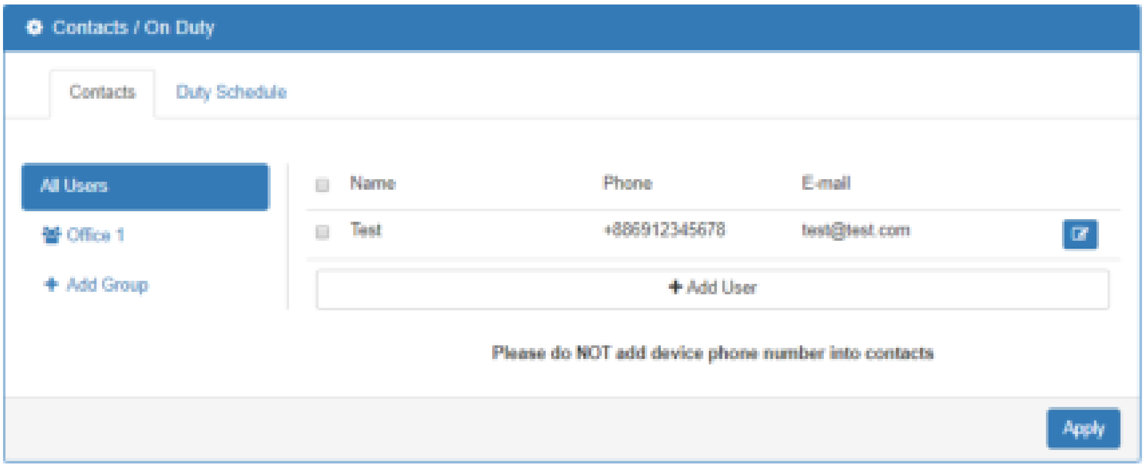
New Password:

Retype to confirm:

14.3 Management > Contacts / On Duty

This section allows you to create the groups, add the usersFor more detailed instruction, please navigate to System > Alarm.

14.3.1 Contacts



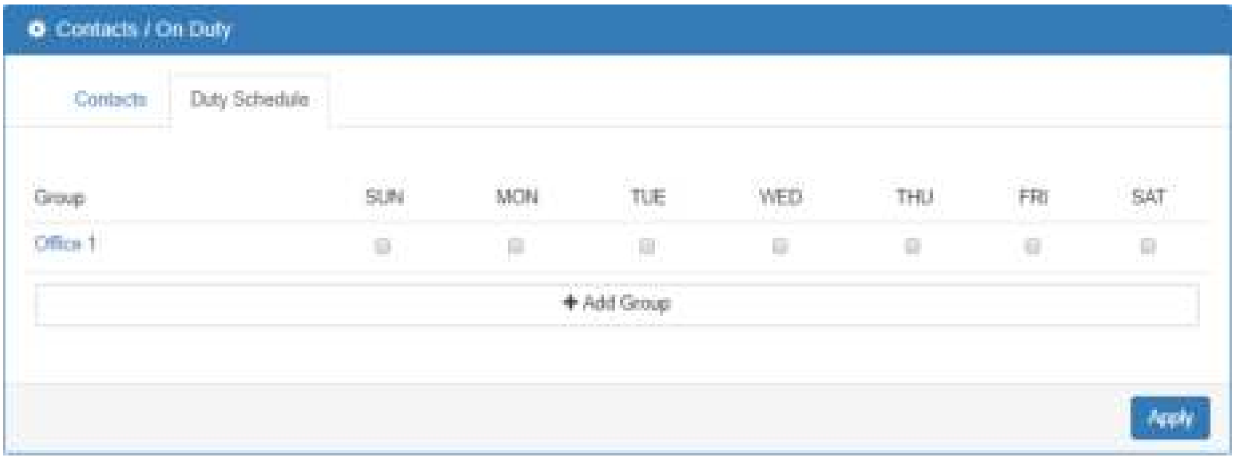
□	Name	Phone	E-mail
□	Test	+886912345678	test@test.com

Please do NOT add device phone number into contacts

+ Add Group: Please fill out group name.

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

14.3.2 Duty Schedule

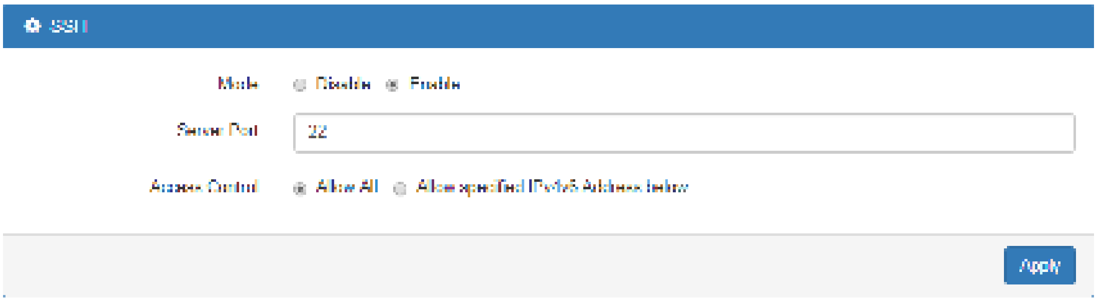


Group	SUN	MON	TUE	WED	THU	FRI	SAT
Office 1	□	□	□	□	□	□	□

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.

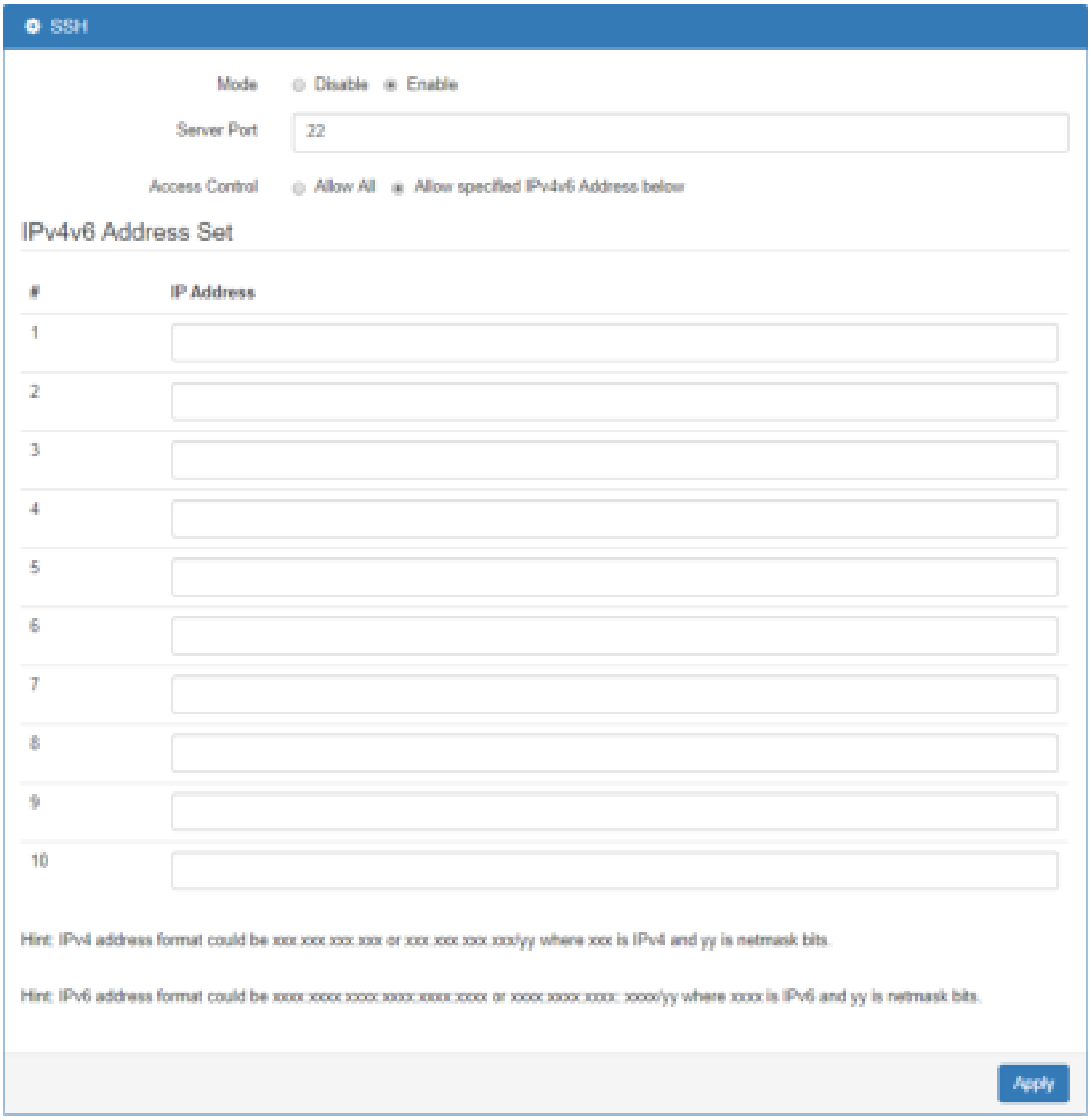


SSH

Mode: ○ Disable ● Enable

Server Port: 22

Access Control: ● Allow All ○ Allow specified IPv4v6 Address below



SSH

Mode: ○ Disable ● Enable

Server Port: 22

Access Control: ○ Allow All ● Allow specified IPv4v6 Address below

IPv4v6 Address Set

#	IP Address
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

Hint: IPv4 address format could be xxx.xxx.xxx.xxx or xxx.xxx.xxx.xxx/yy where xxx is IPv4 and yy is netmask bits.

Hint: IPv6 address format could be xxxx:xxxx:xxxx:xxxx:xxxx:xxxx or xxxx:xxxx:xxxx::xxxx/yy where xxxx is IPv6 and yy is netmask bits.

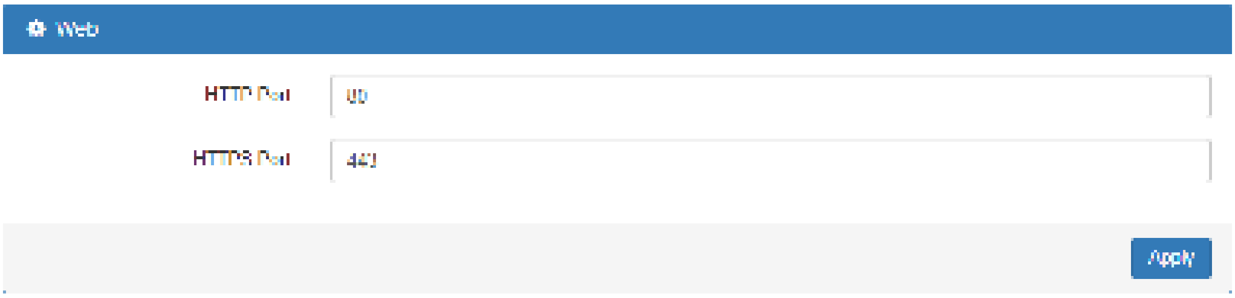
Management > SSH	
Item	**Description**
Mode	Select from Disable or Enable SSH function.
Server Port	The port number is where SSH server works on.
Access Control	● **Allow All:** Any client who own the IPv4v6 Address can reach system is able to connect system. ● **Allow specified IPv4v6 Address below:** 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.

We need a way to reply immediately and apply the configuration latter. By using fork, we can make parent process reply immediately and the child process execute the configuration.

Note: Remember close the file descriptor stdin and stdout within the child process context.

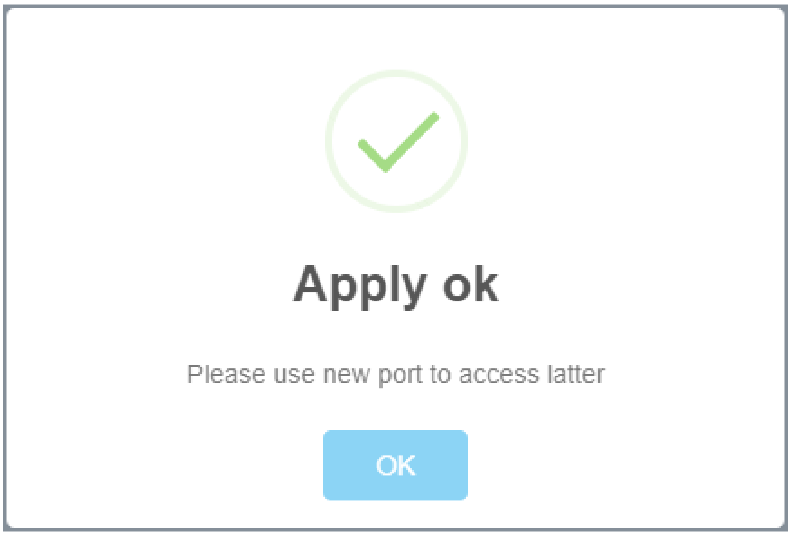


HTTP Port 80

HTTPS Port 443

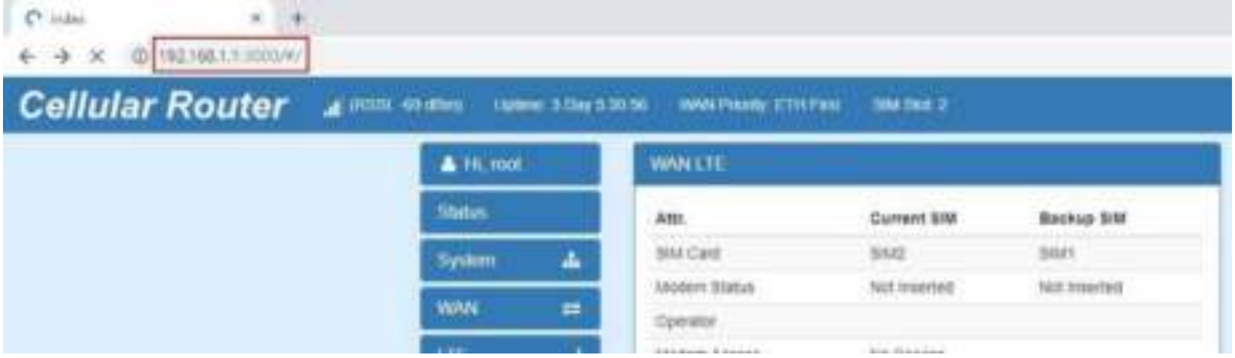
Management > Web	
Item	**Description**
HTTP Port	The TCP port listened by HTTP daemon.
HTTPS Port	The TCP port listened by HTTPS daemon.

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



Apply ok

Please use new port to access latter



Attr.	Current SIM	Backup SIM
SIM Card	SIM2	SIM1
Modem Status	Not Inserted	Not Inserted
Operator		

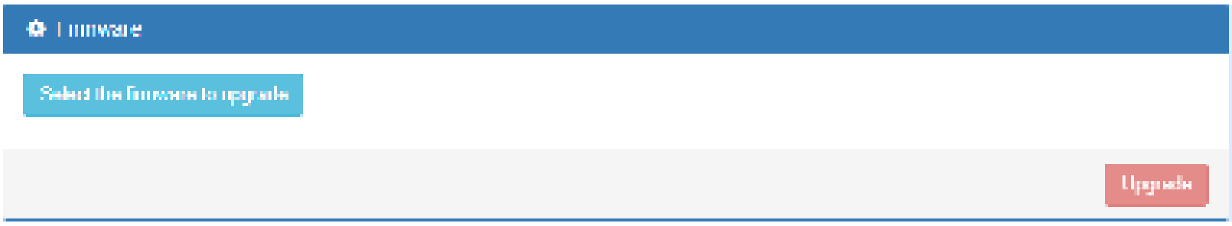
14.6 Management > Firmware

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.

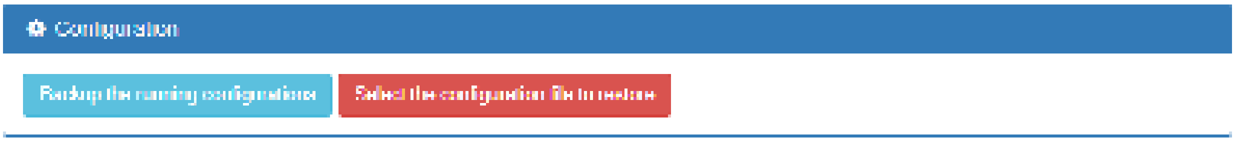
(3) After upgrading successfully, please reboot the router.



14.7 Management > Configuration

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

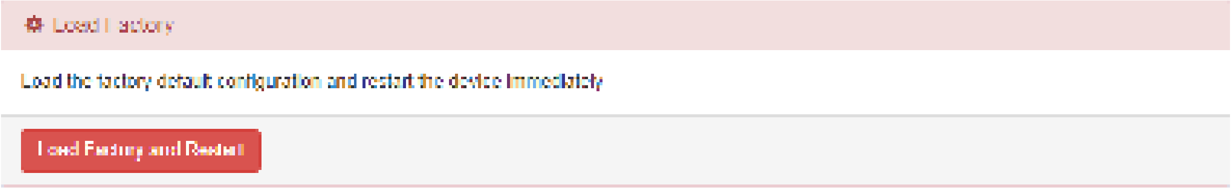
(1) Click Backup the running configurations button to export your current configurations.


Configuration
Backup the running configurations
Select the configuration file to restore

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

14.8 Management > Load Factory

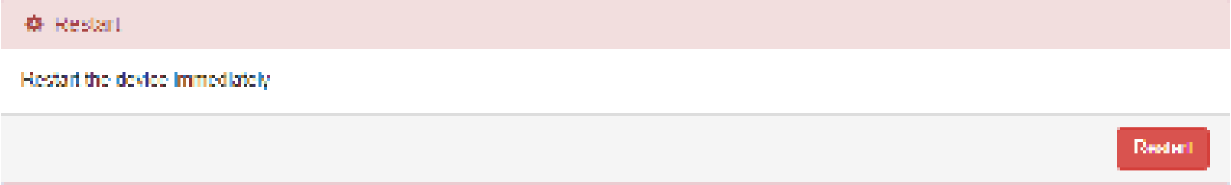
This section supports you to load the factory default configuration and restart the device immediately. You can click the Load Factory and Restart button.



Load the factory default configuration and restart the device Immediately

14.9 Management > Restart

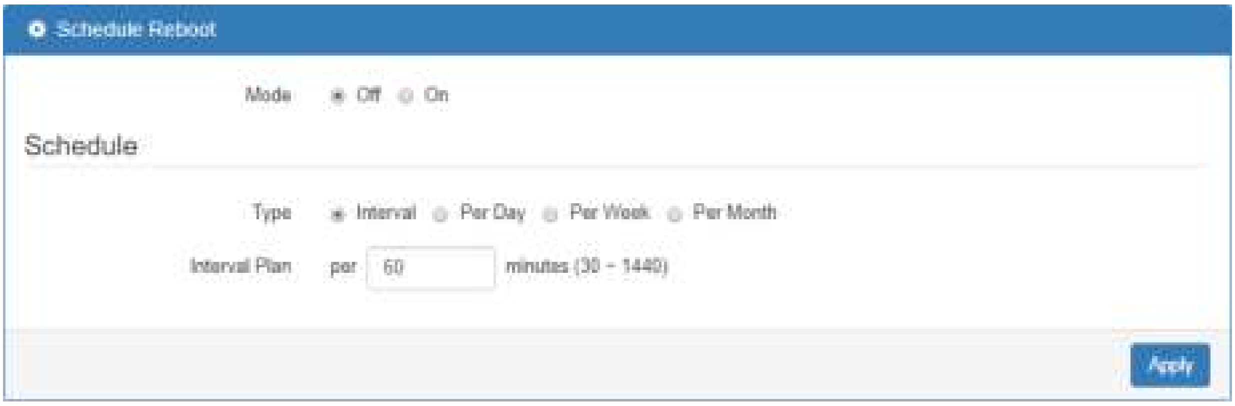
This section allows you to click Restart button and the router will restart immediately.



Restart the device Immediately

14.10 Management > Schedule Reboot

The setting allows you to schedule the reboot time regularly.



Schedule Reboot

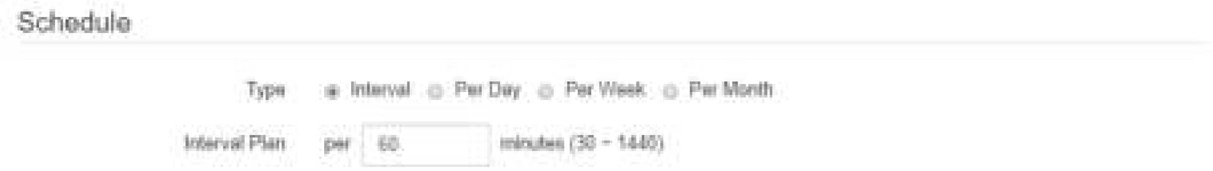
Mode ● Off ○ On

Schedule

Type ● Interval ○ Per Day ○ Per Week ○ Per Month

Interval Plan per 60 minutes (30 ~ 1440)

- **Schedule Type – Interval**

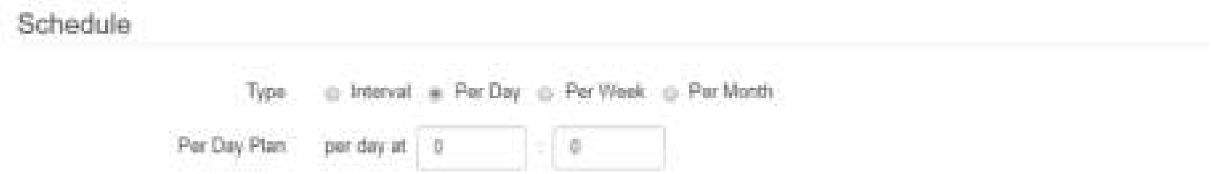


Schedule

Type ● Interval ○ Per Day ○ Per Week ○ Per Month

Interval Plan per 60 minutes (30 ~ 1440)

- **Schedule Type - Per Day**

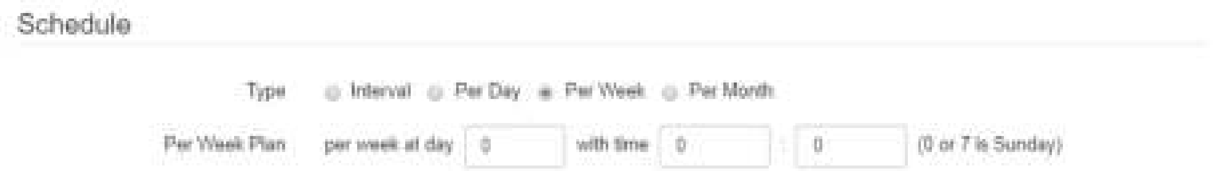


Schedule

Type ○ Interval ● Per Day ○ Per Week ○ Per Month

Per Day Plan per day at 0 : 0

- **Schedule Type - Per Week**

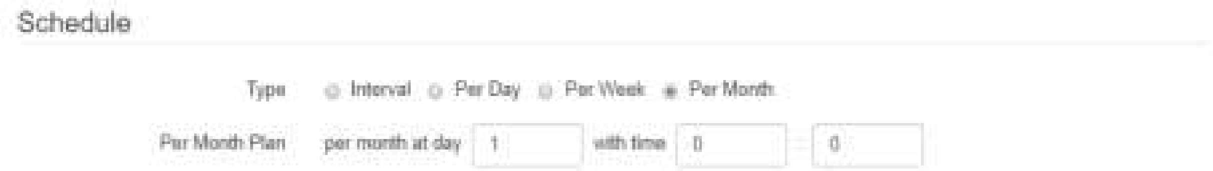


Schedule

Type ○ Interval ○ Per Day ● Per Week ○ Per Month

Per Week Plan per week at day 0 with time 0 : 0 (0 or 7 is Sunday)

- **Schedule Type - Per Month**



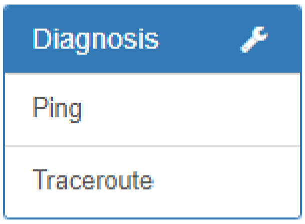
Schedule

Type ○ Interval ○ Per Day ○ Per Week ● Per Month

Per Month Plan per month at day 1 with time 0 : 0

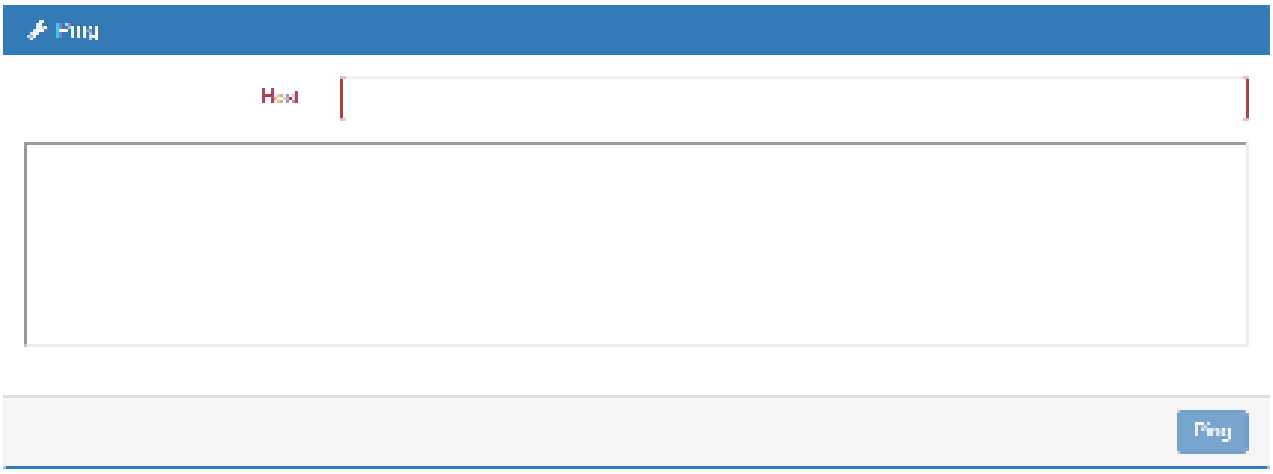
15 Configuration > Diagnosis

This section allows you to diagnose Ping and Traceroute for your Host (IP address or Domain Name).

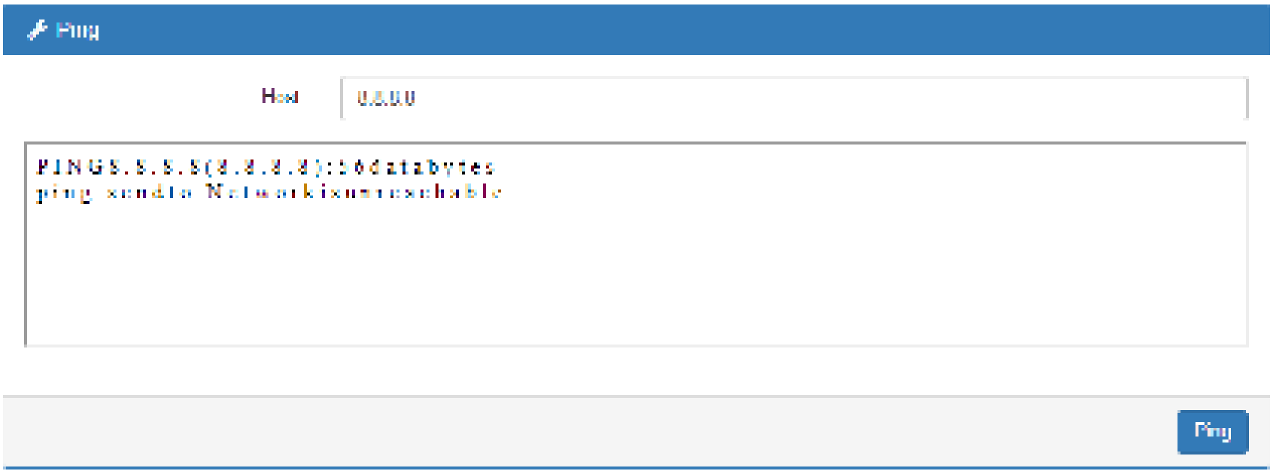


15.1 Diagnosis > Ping

Please assign the Host you want to ping.



The result of the ping is as below.

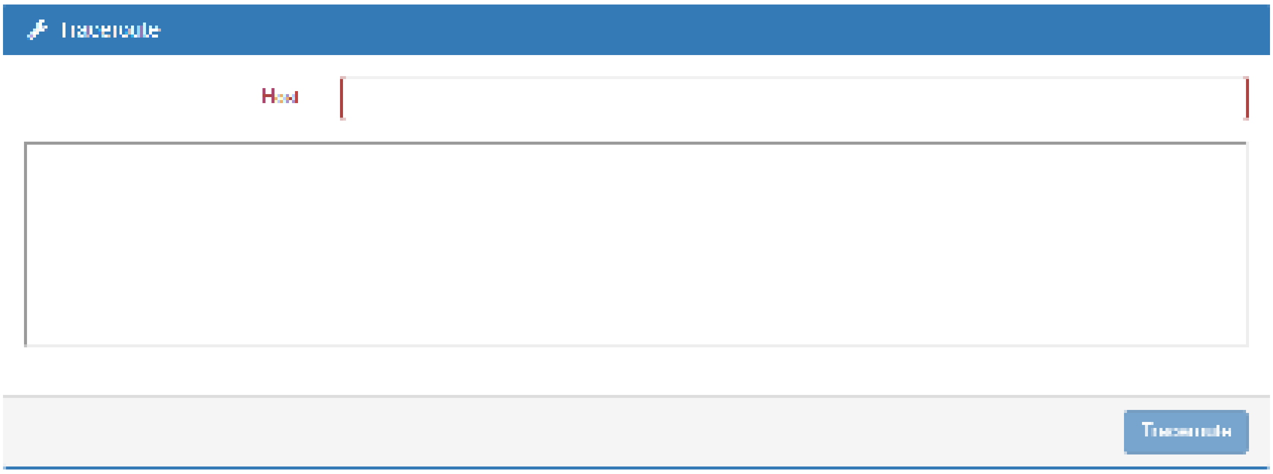


Host: 8.8.8.8

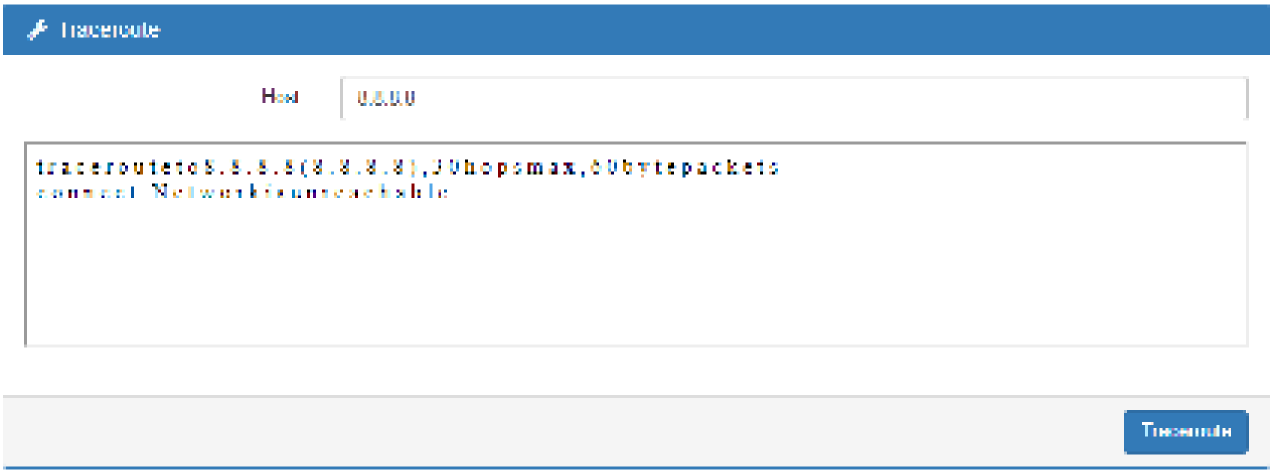
```
PING8.8.8.8(8.8.8.8):56databytes
ping sendto Networkisunreachable
```

15.2 Diagnosis > Traceroute

Please assign the Host **you want to** traceroute.



The result of the traceroute is as below.



Host: 8.8.8.8

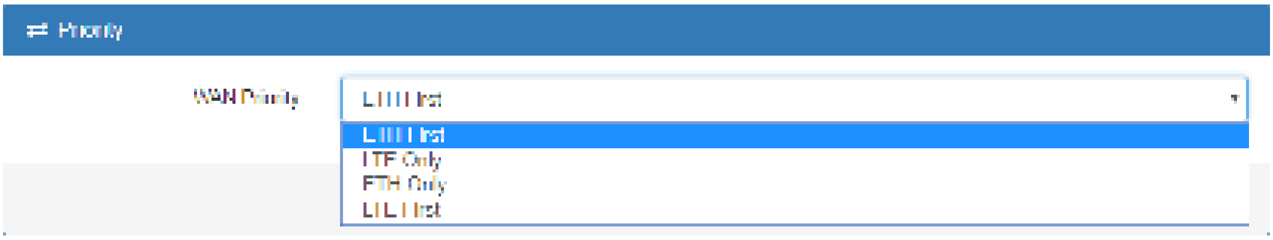
```
tracerouteto8.8.8.8(8.8.8.8),30hopsmax,60bytepackets
connect: Networkisunreachable
```

16 Configuration Applications

This section explains specific examples how to configure your applications.

16.1 WAN Priority

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



⇄ Priority

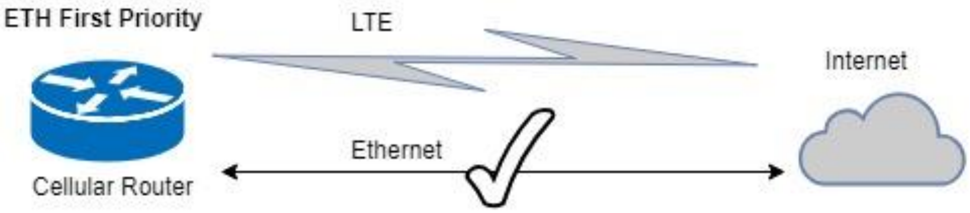
WAN Priority: ETH First ▾

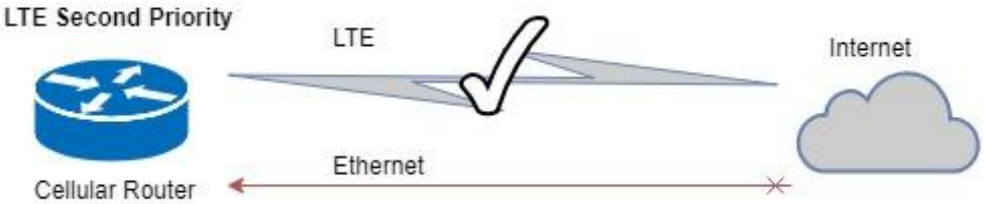
- ETH First
- LTE Only
- ETH Only
- LTE First

(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.

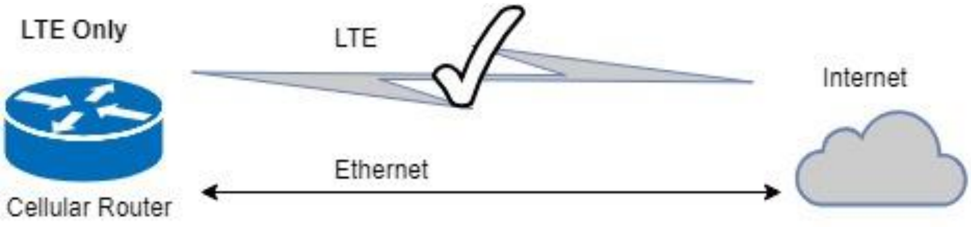
However, in case Ethernet is unplug or not able to access Internet (check by ping), the router would route network packages through LTE network.

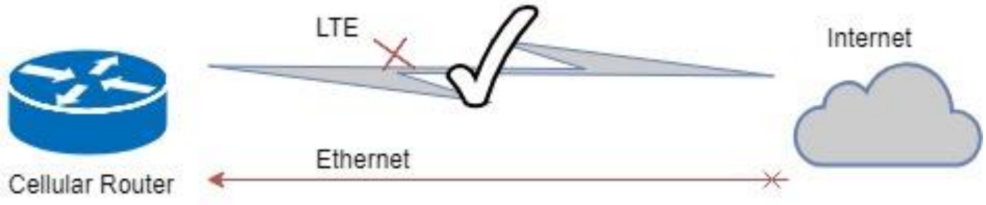




(2) WAN Priority > LTE Only:

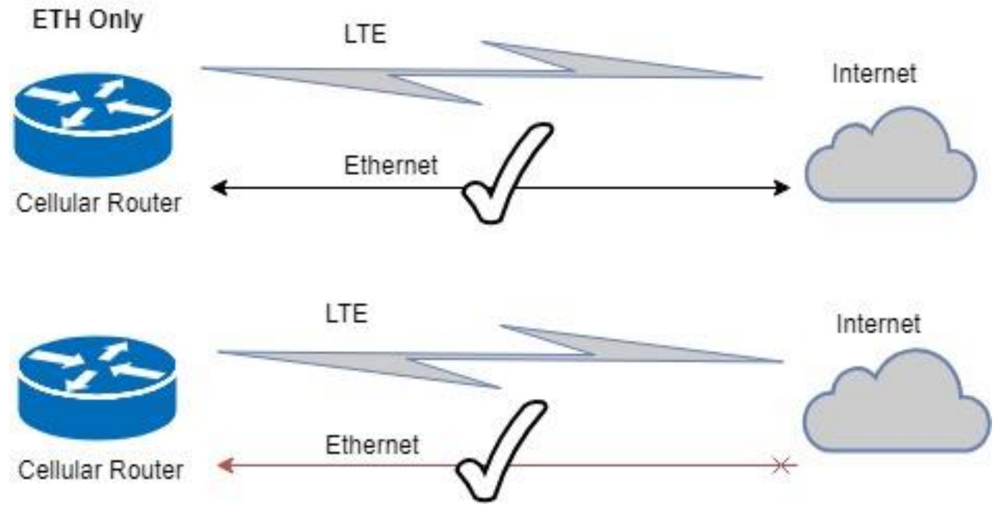
In this mode, the router only routes network packages through LTE.





(3) WAN Priority > ETH Only:

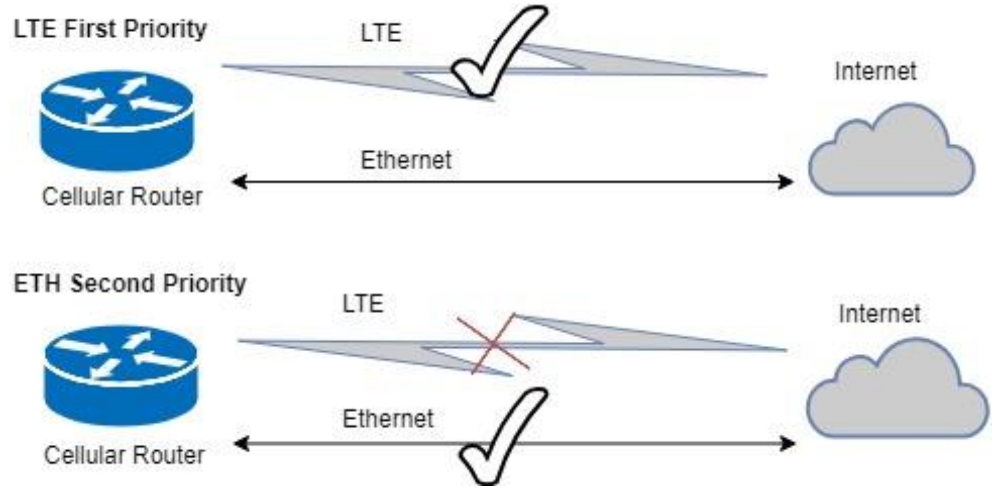
In this mode, the router only routes network packages through Ethernet.



(4) WAN Priority > LTE First:

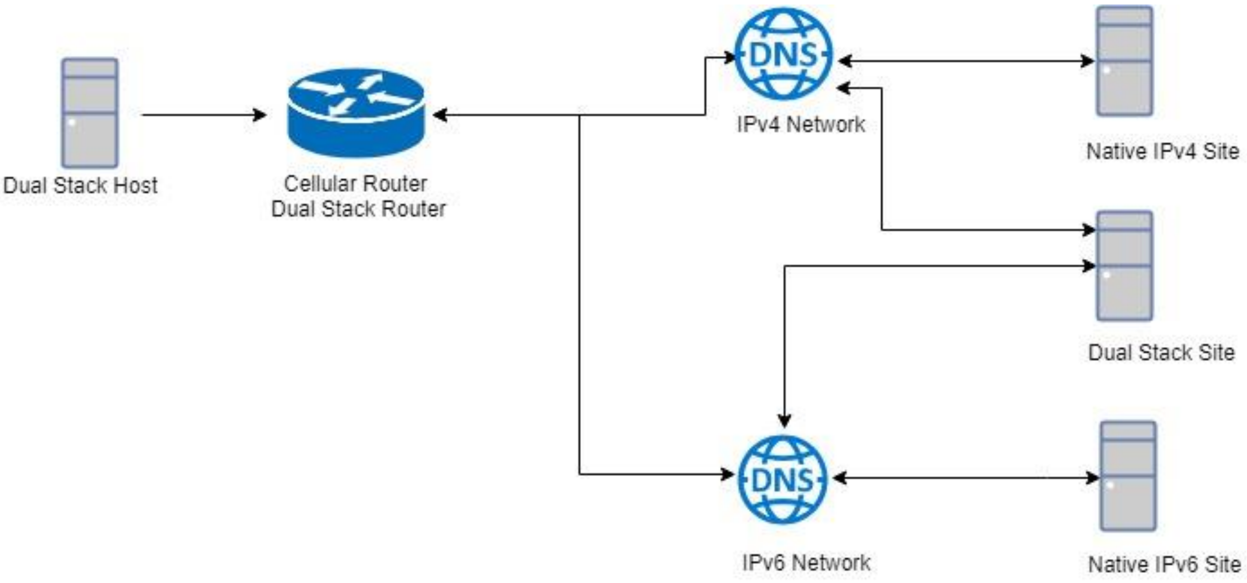
In case both Ethernet and LTE can access Internet, the router would route network packages through LTE.

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

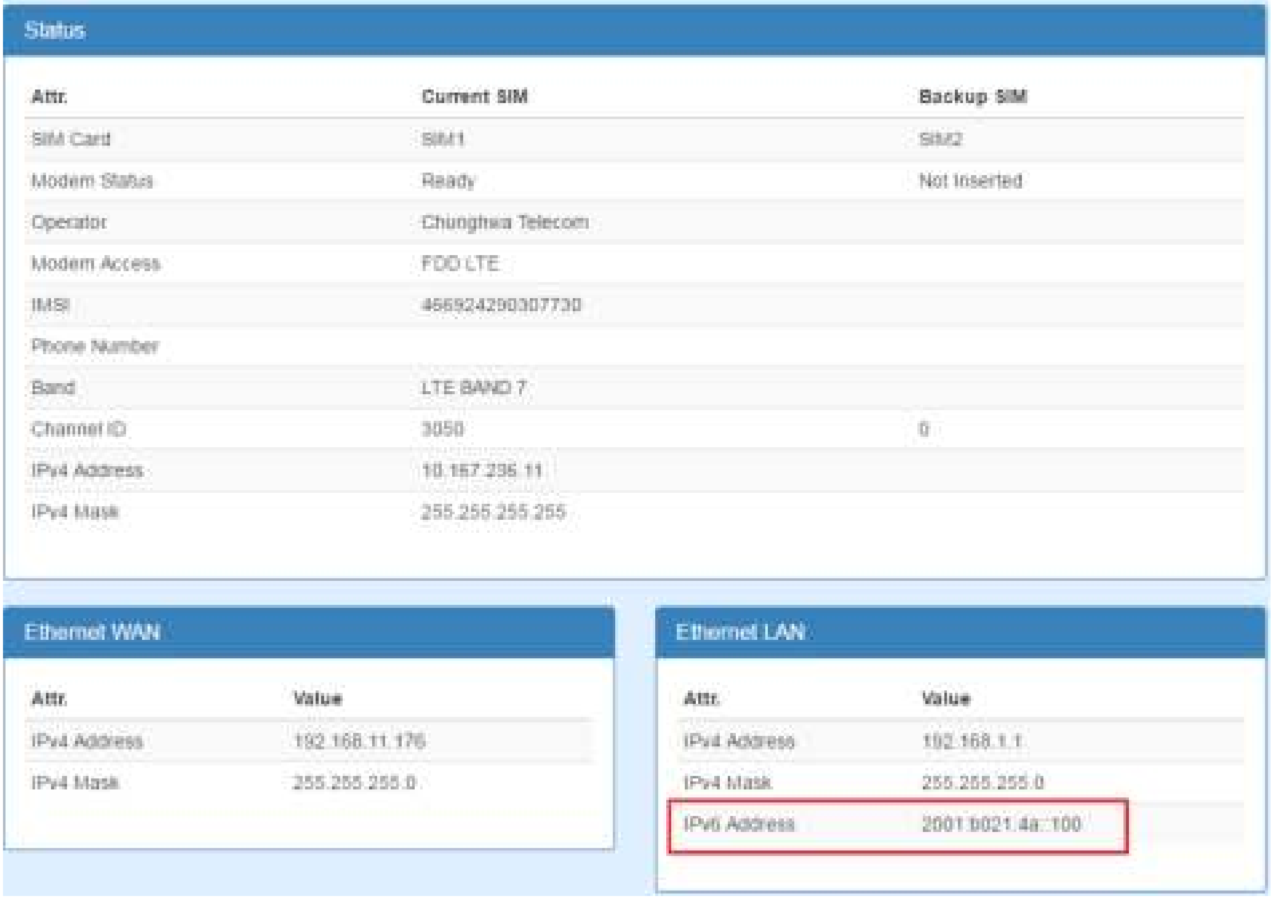


16.2 LAN > IPv4/IPv6 Dual Stack

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.



Status

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

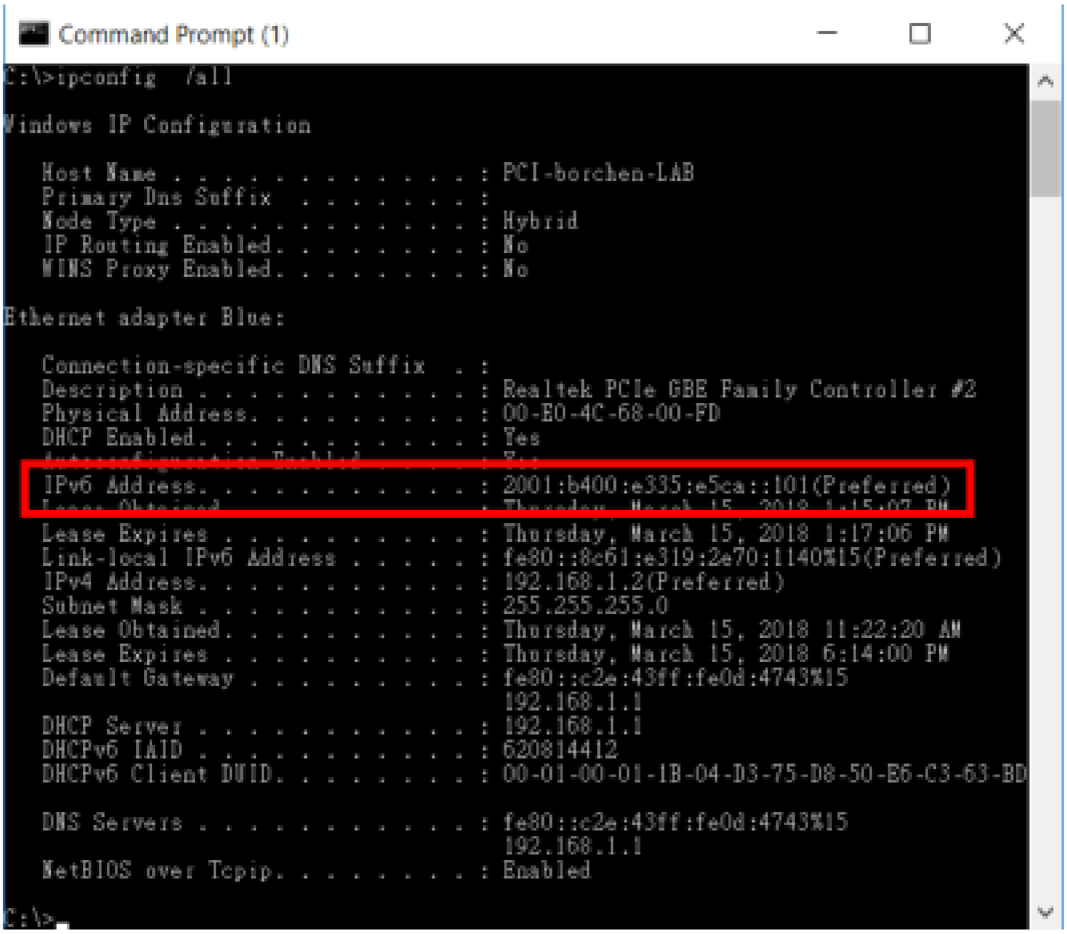
Ethernet WAN

Attr.	Value
IPv4 Address	192.168.11.176
IPv4 Mask	255.255.255.0

Ethernet LAN

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

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

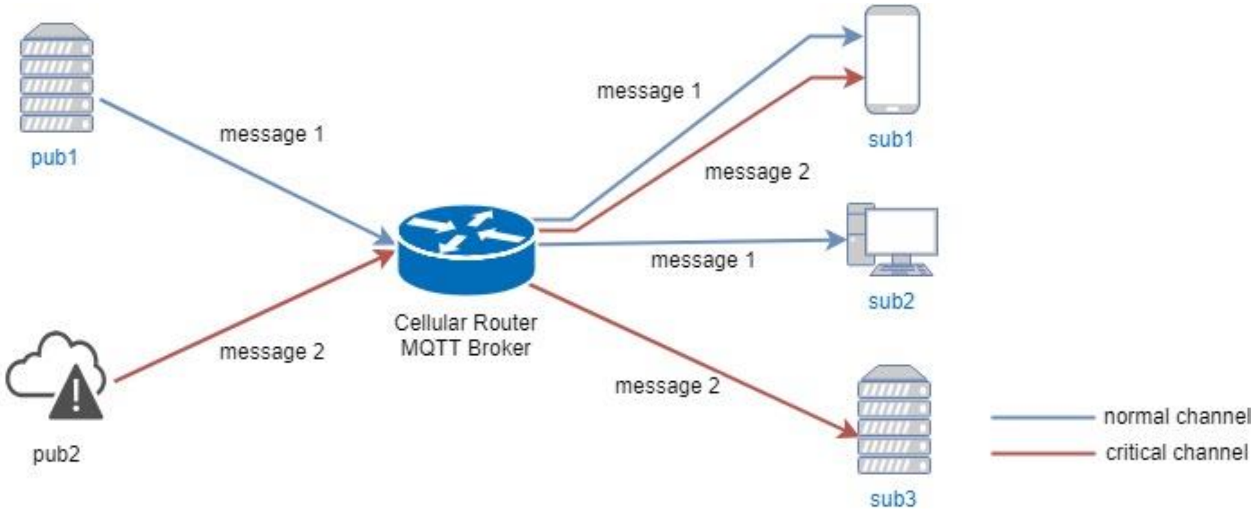


```
C:\>ipconfig  /all

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:\>
```

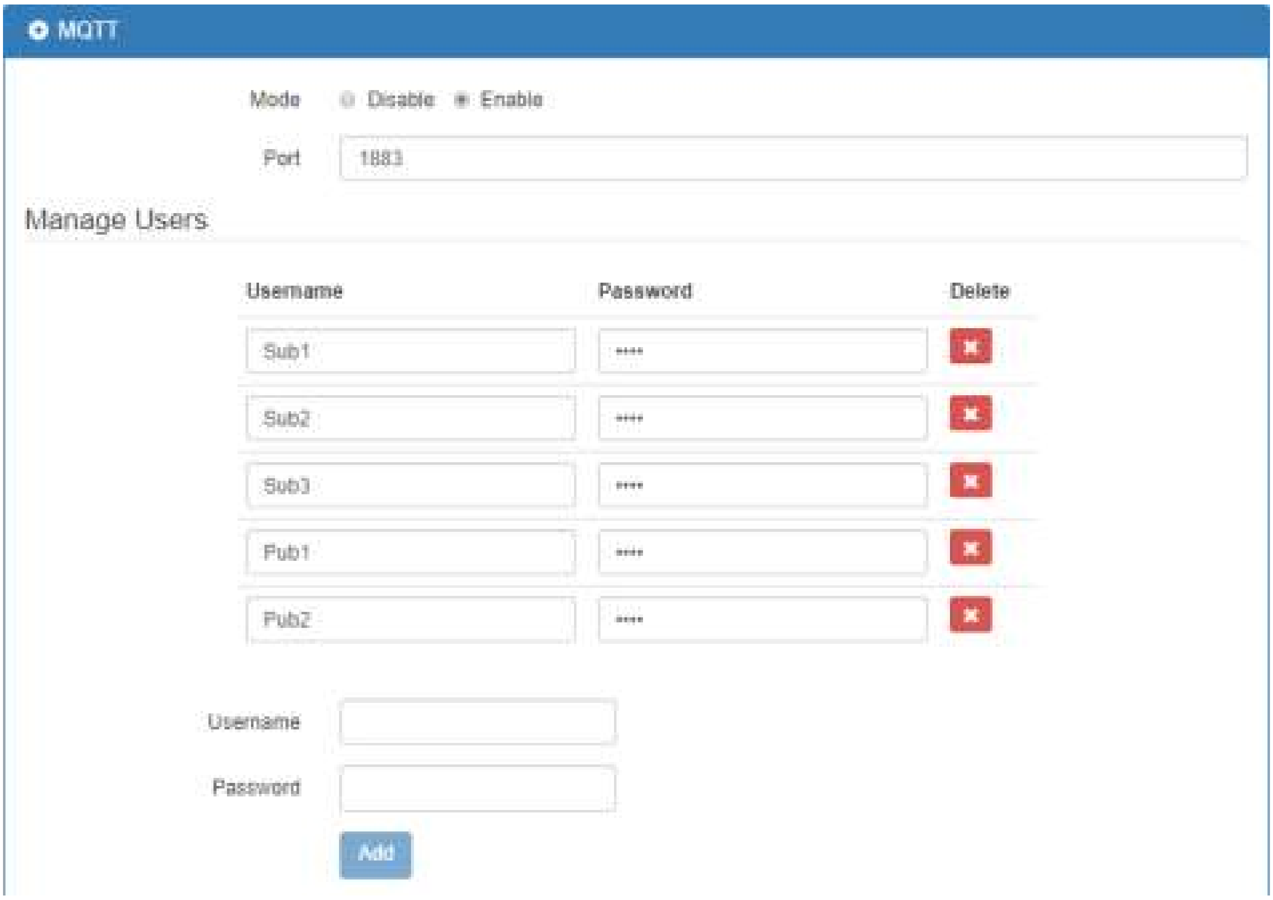
16.3 MQTT Broker

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.



MQTT

Mode ○ Disable ● Enable

Port 1883

Manage Users

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

Username

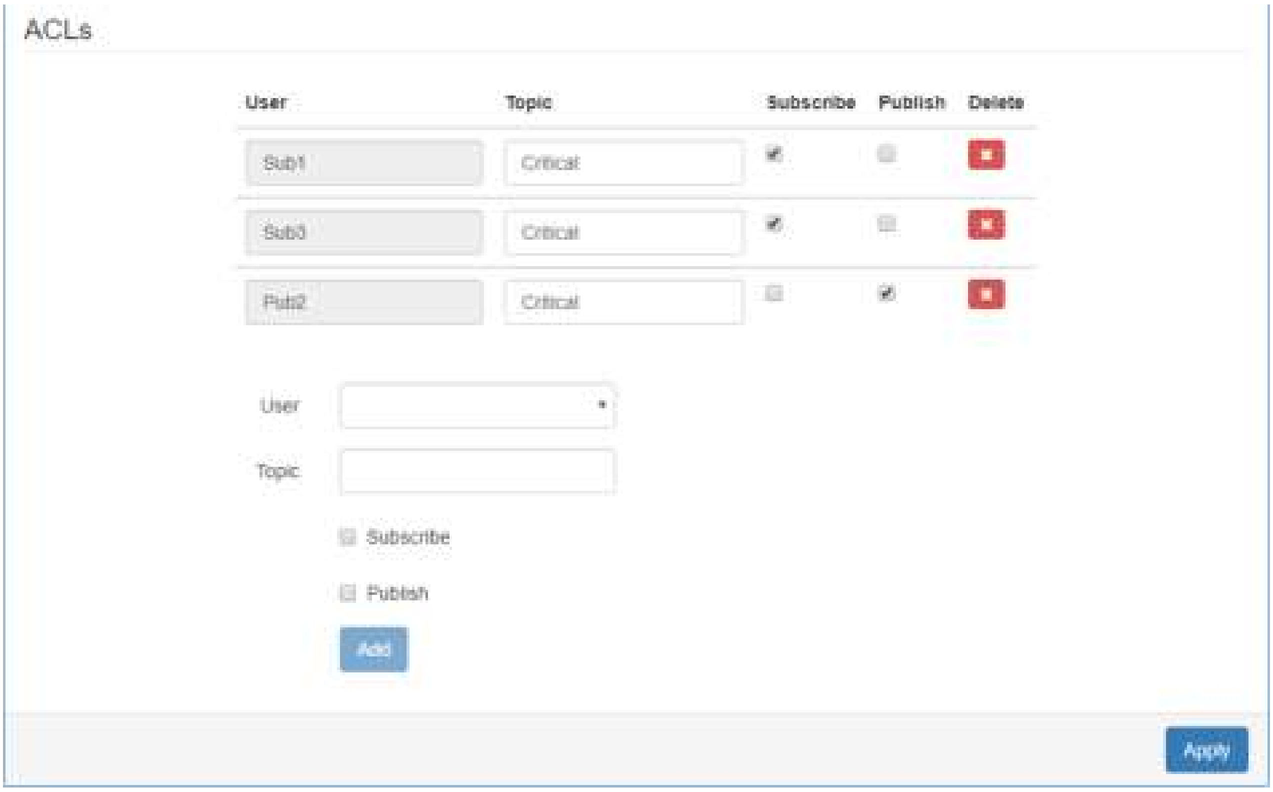
Password

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.



ACLs

User	Topic	Subscribe	Publish	Delete
Sub1	Critical	☑	□	✖
Sub3	Critical	☑	□	✖
Pub2	Critical	□	☑	✖

User

Topic

□ Subscribe

□ Publish

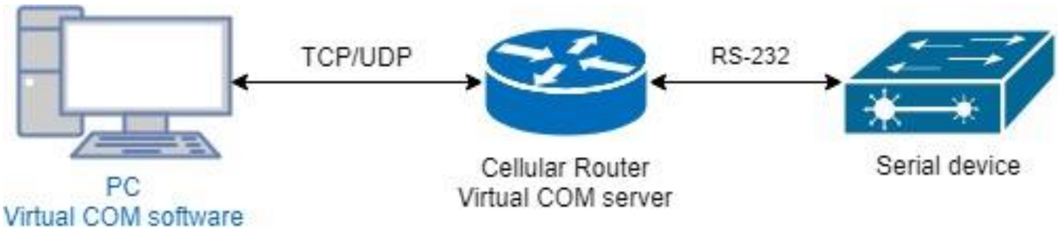
Add

Apply

16.4 Virtual COM > Remote Management

You can access the remote serial device (e.g. Console) by the Virtual COM server feature.

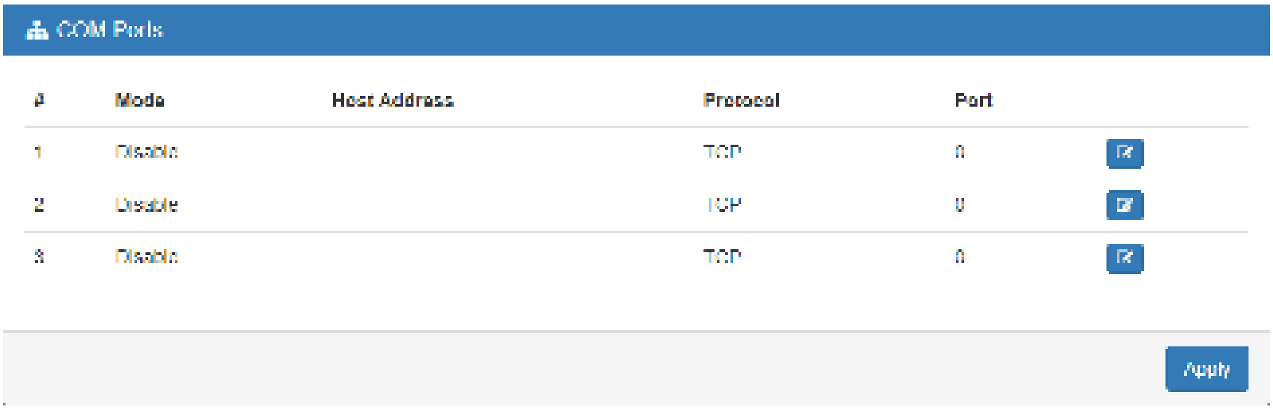
When you set up the above environment, use the Virtual COM software (e.g. USR-VCOM) to simulate the COM device. After the simulation, the user can use the terminal tool (e.g. putty, tera term) to access the remote serial device Console.



- **How to set up**

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

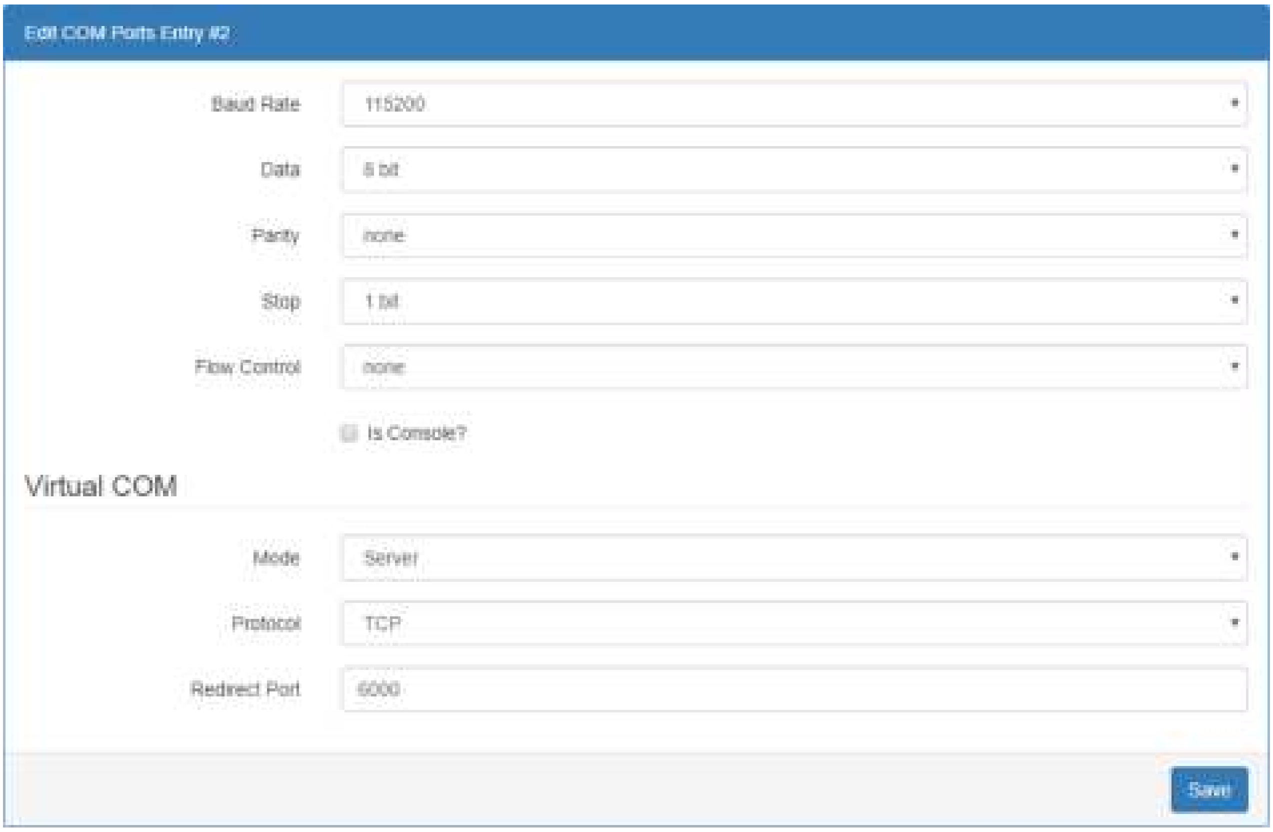
First, you need to navigate to the **System -> COM ports**. The web UI shows the following picture.



COM Ports

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

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



Edit COM Ports Entry #2

Baud Rate: 115200

Data: 8 bit

Parity: none

Stop: 1 bit

Flow Control: none

□ Is Console?

Virtual COM

Mode: Server

Protocol: TCP

Redirect Port: 6000

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

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

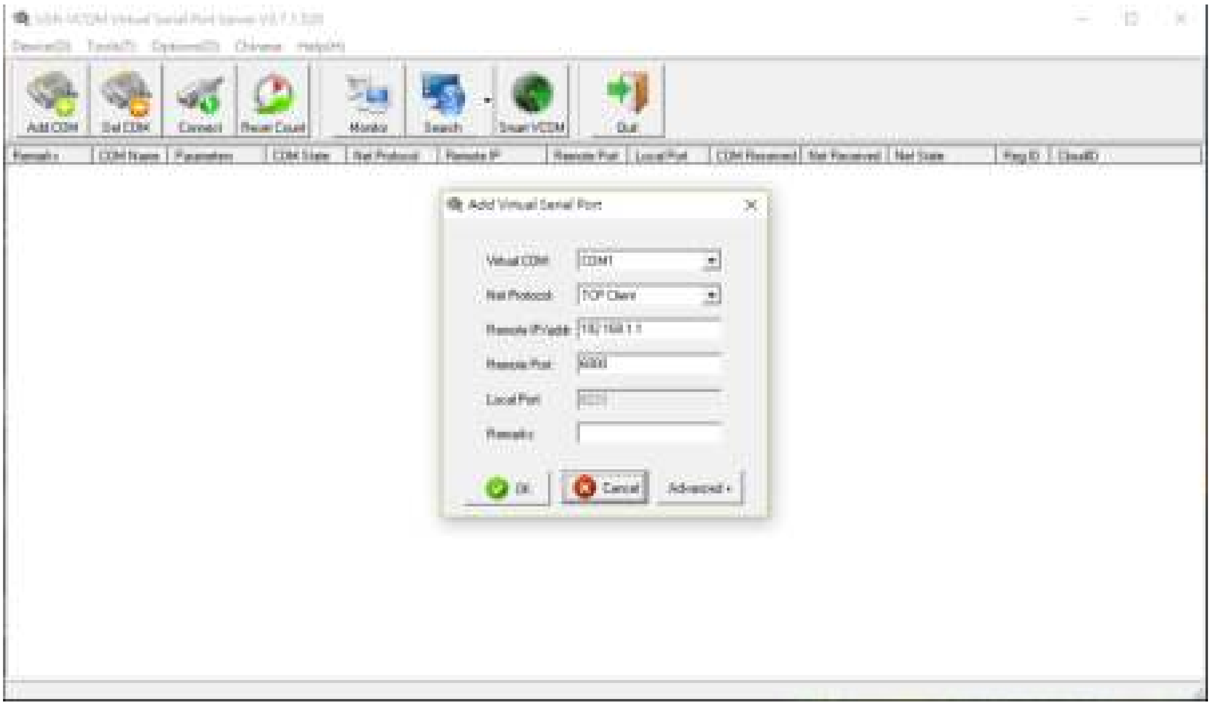
(2) For the Virtual COM, you need to change the mode to **Server** and specify the **Protocol**, **Port** to reach the remote management feature. (***Note:*** In this case, we use the **TCP** and port **6000** to be the Virtual COM server settings.)

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

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

(5) And set up the virtual serial port by **192.168.1.1** (The default is LAN IP), **TCP client** and

Remote Port 6000 as the following picture.


USR-VCOM Virtual Serial Port Server V3.7.1.520
Device(D) Tools(T) Options(O) Chinese Help(H)
Add COM
Del COM
Connect
Reset Count
Monitor
Search
Smart VCOM
Quit
Remark | COM Name | Parameters | COM State | Net Protocol | Remote IP | Remote Port | Local Port | COM Received | Net Received | Net State | Reg ID | CloudID
Add Virtual Serial Port
OK
Cancel
Advanced ›

Virtual COM: COM1

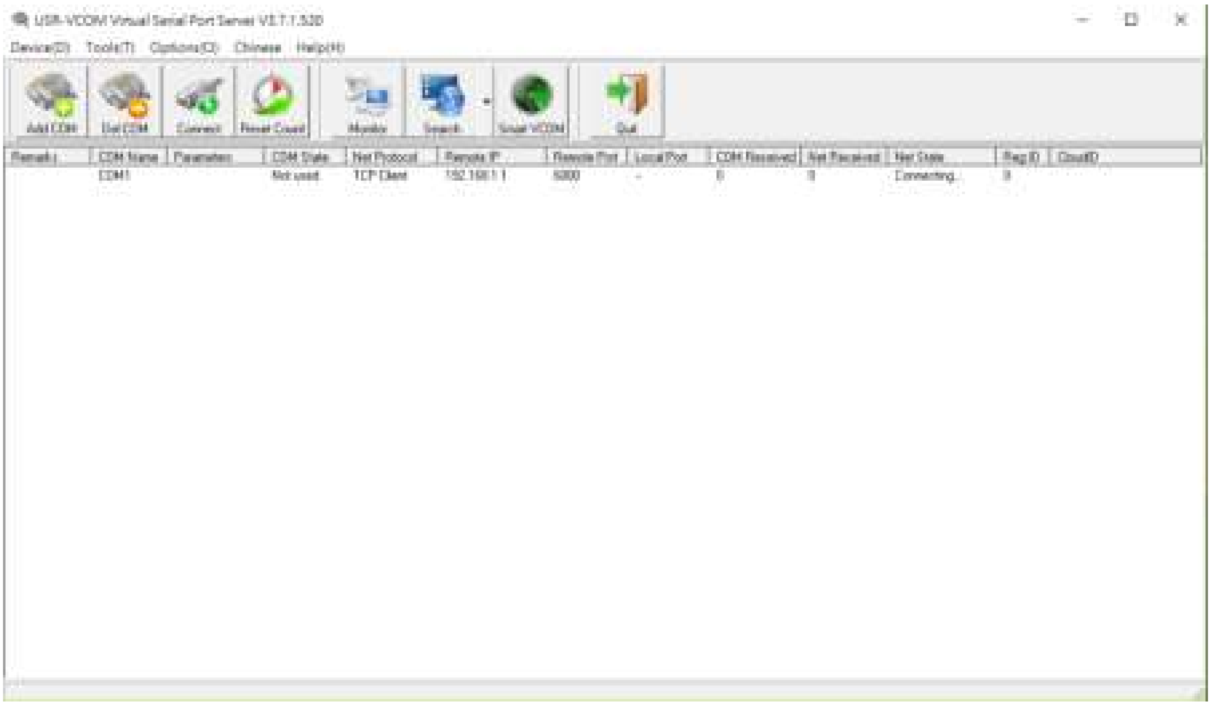
Net Protocol: TCP Client

Remote IP/addr: 192.168.1.1

Remote Port: 6000

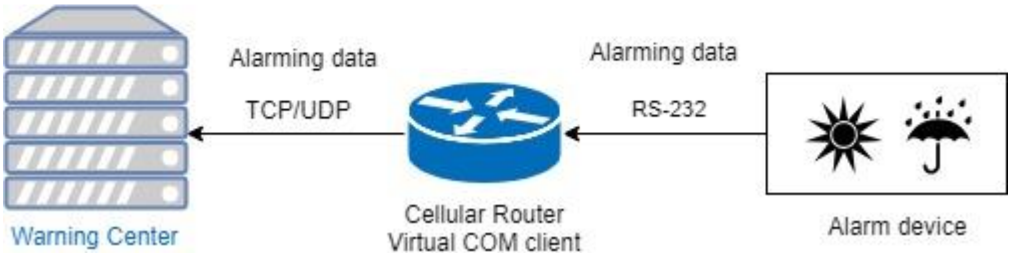
Local Port: 8231

Remarks:


USR-VCOM Virtual Serial Port Server V3.7.1.520
Device(D) Tools(T) Options(O) Chinese Help(H)
Add COM
Del COM
Connect
Reset Count
Monitor
Search
Smart VCOM
Quit

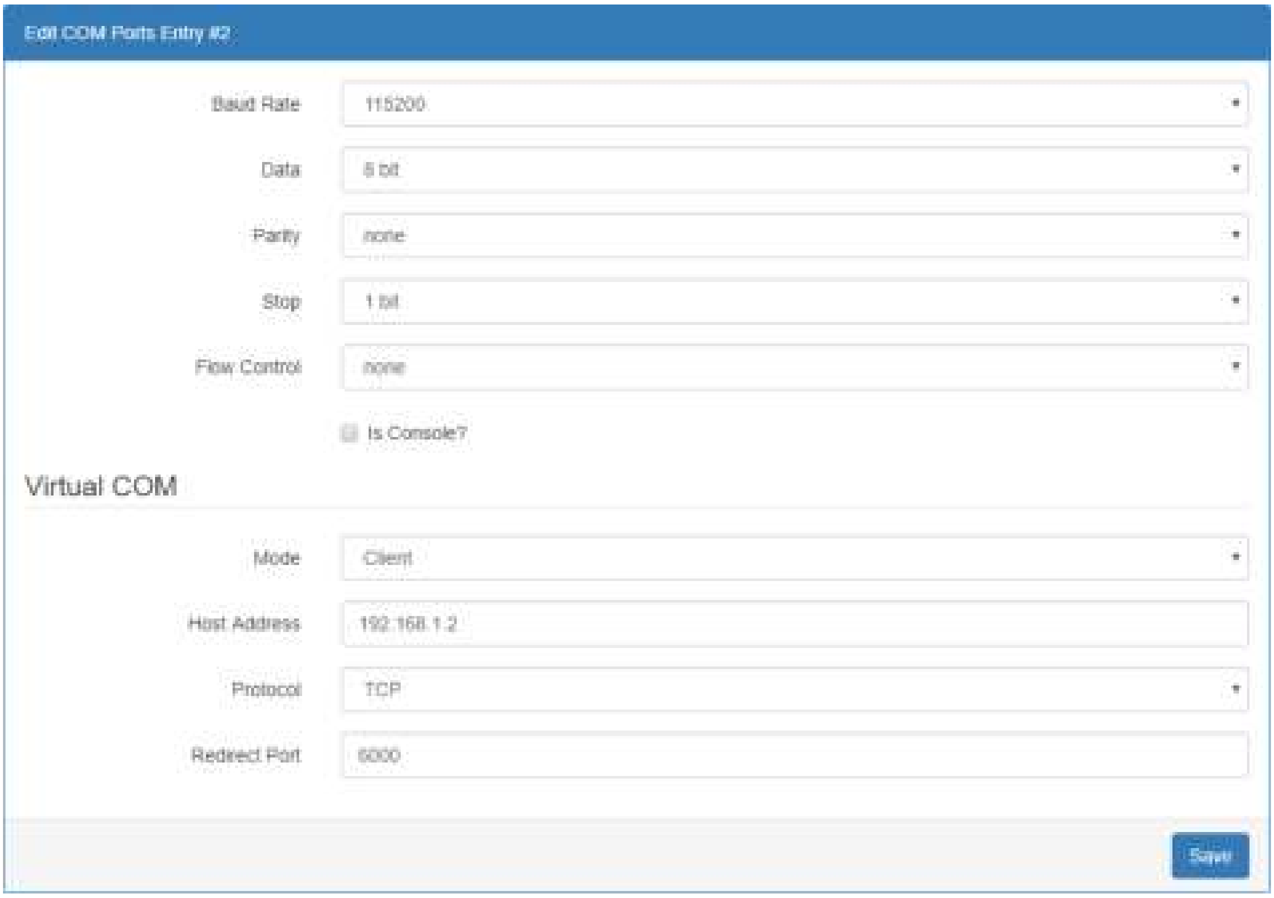
Remarks	COM Name	Parameters	COM State	Net Protocol	Remote IP	Remote Port	Local Port	COM Received	Net Received	Net State	Reg ID	CloudID
	COM1		Not used	TCP Client	192.168.1.1	6000	-	0	0	Connecting...	0	

16.5 Virtual COM > Remote Alarm



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

The web UI of router shows the below picture.



Edit COM Ports Entry #2

Baud Rate: 115200

Data: 8 bit

Parity: none

Stop: 1 bit

Flow Control: none

□ Is Console?

Virtual COM

Mode: Client

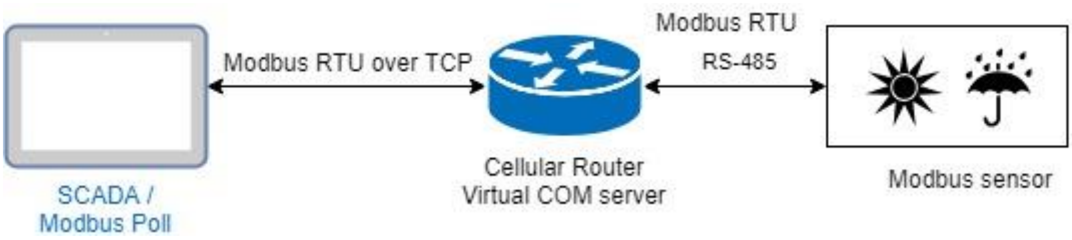
Host Address: 192.168.1.2

Protocol: TCP

Redirect Port: 6000

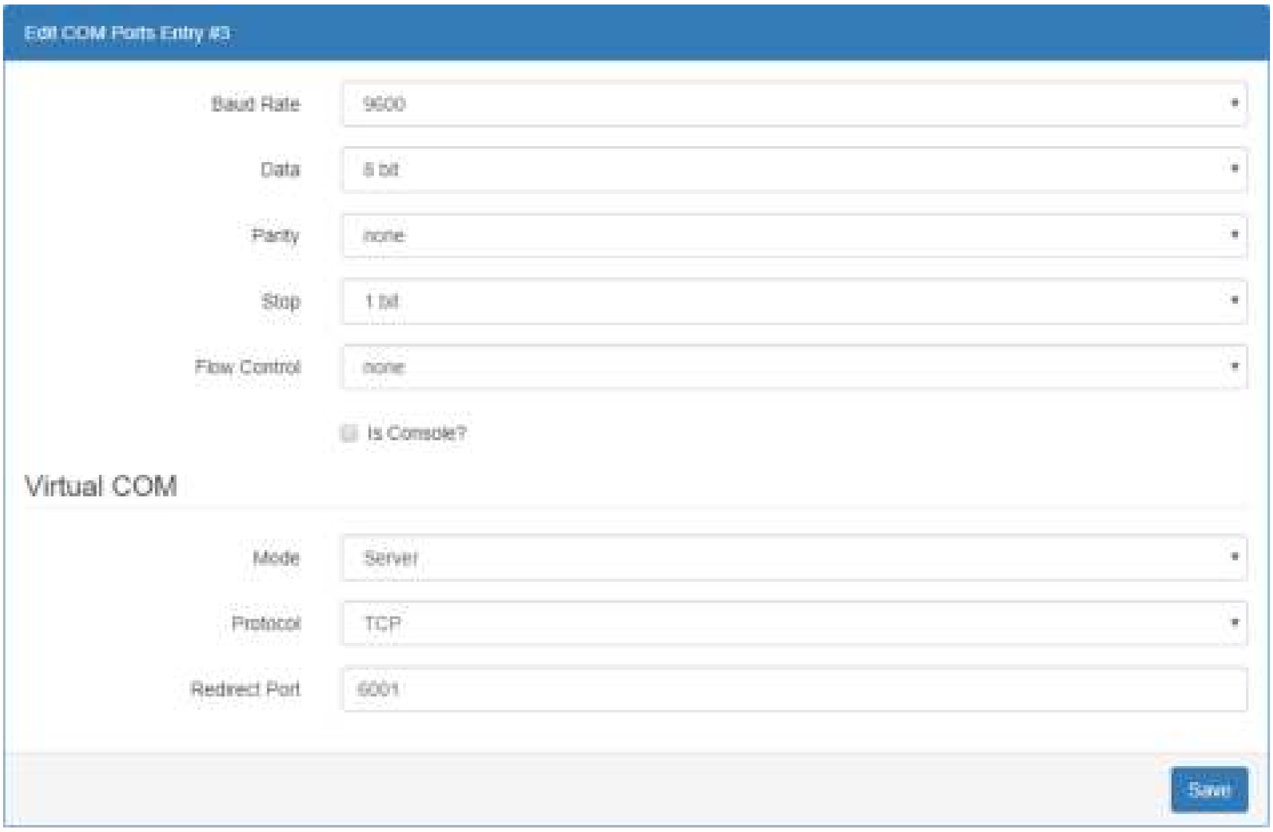
After the above setup, the warning center will receive the data when the alarm device sent the data/message.

16.6 Virtual COM > Modbus RTU over TCP



For the industrial products, the Modbus protocol is the most popular industrial control protocol.

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



Edit COM Ports Entry #3

Baud Rate	9600
Data	8 bit
Parity	none
Stop	1 bit
Flow Control	none

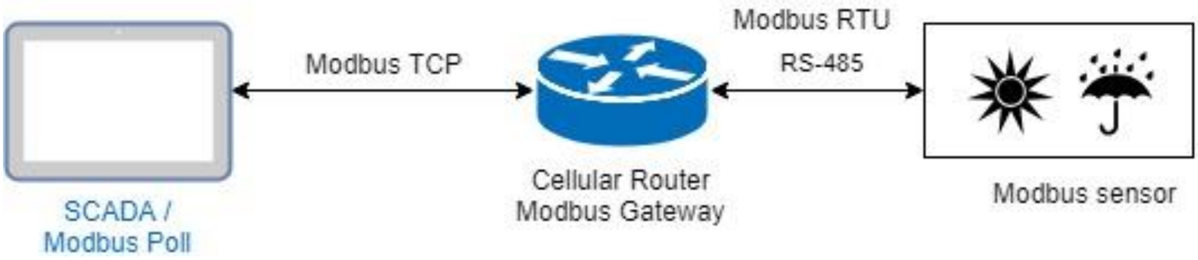
□ Is Console?

Virtual COM

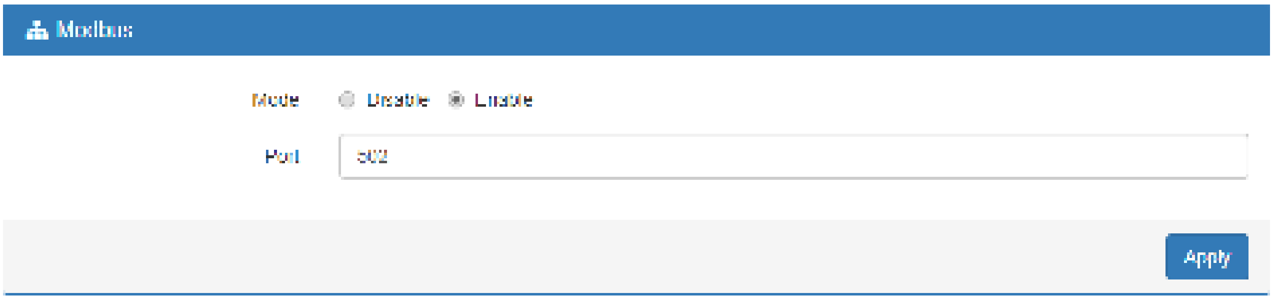
Mode	Server
Protocol	TCP
Redirect Port	6001

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

16.7 Modbus Gateway



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



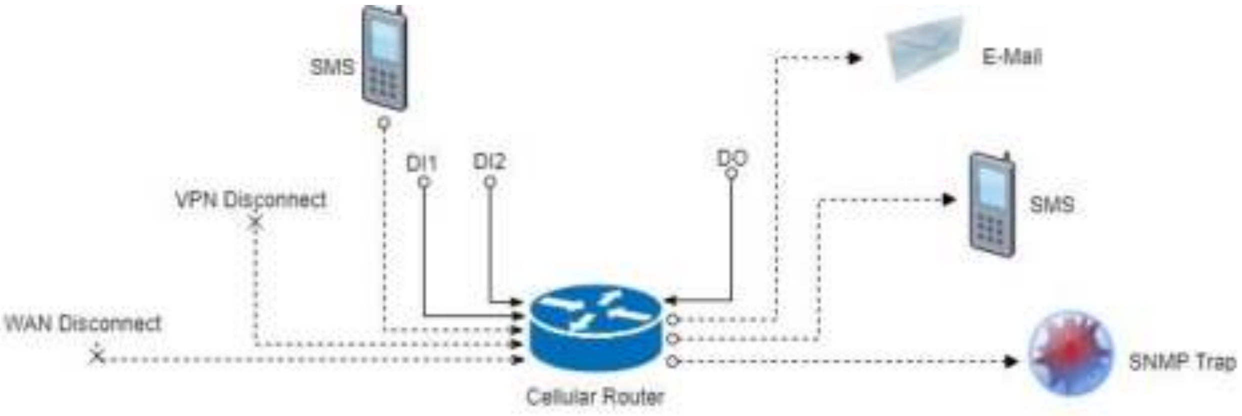
Mode ○ Disable ● Enable

Port 502

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

16.8 Alarm Configuration

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

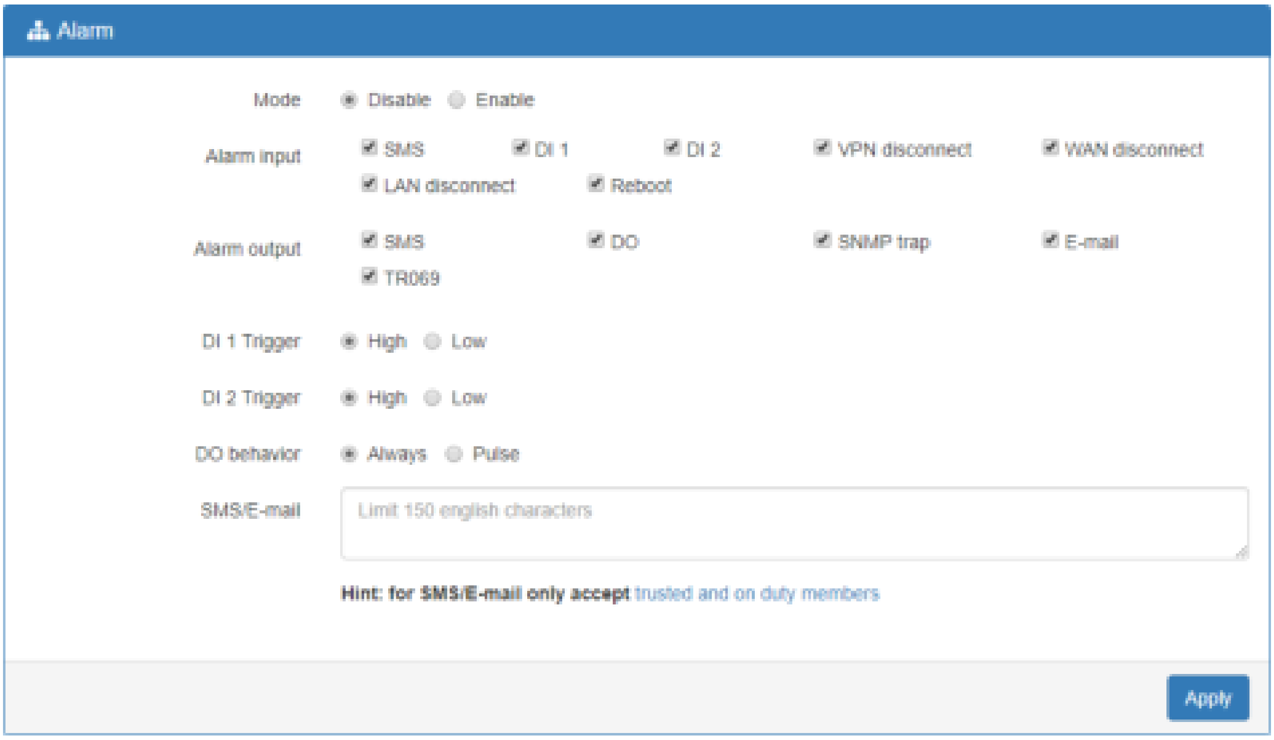


(1) Alarm Input:

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

(2) Alarm Output:

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



Alarm

Mode ● Disable ○ Enable

Alarm input ☑ SMS ☑ DI 1 ☑ DI 2 ☑ VPN disconnect ☑ WAN disconnect ☑ LAN disconnect ☑ Reboot

Alarm output ☑ SMS ☑ DO ☑ SNMP trap ☑ E-mail ☑ TR069

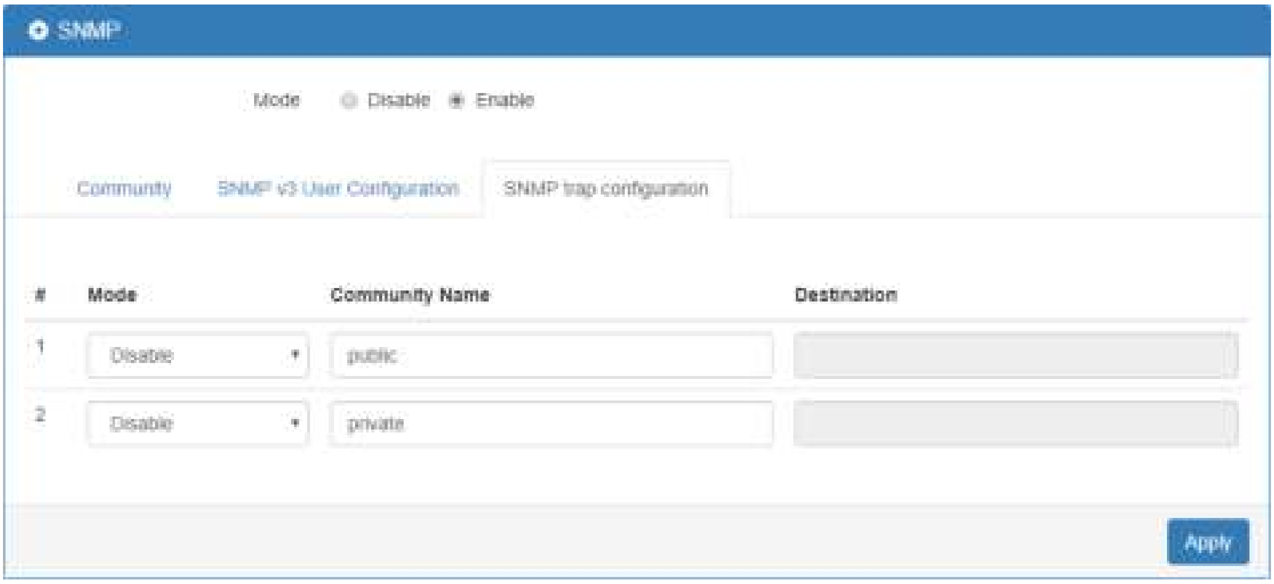
DI 1 Trigger ● High ○ Low

DI 2 Trigger ● High ○ Low

DO behavior ● Always ○ Pulse

SMS/E-mail: Limit 150 english characters

Hint: for SMS/E-mail only accept trusted and on duty members



SNMP

Mode ○ Disable ● Enable

#	Mode	Community Name	Destination
1	Disable	public	
2	Disable	private	

16.9 Open VPN Configuration

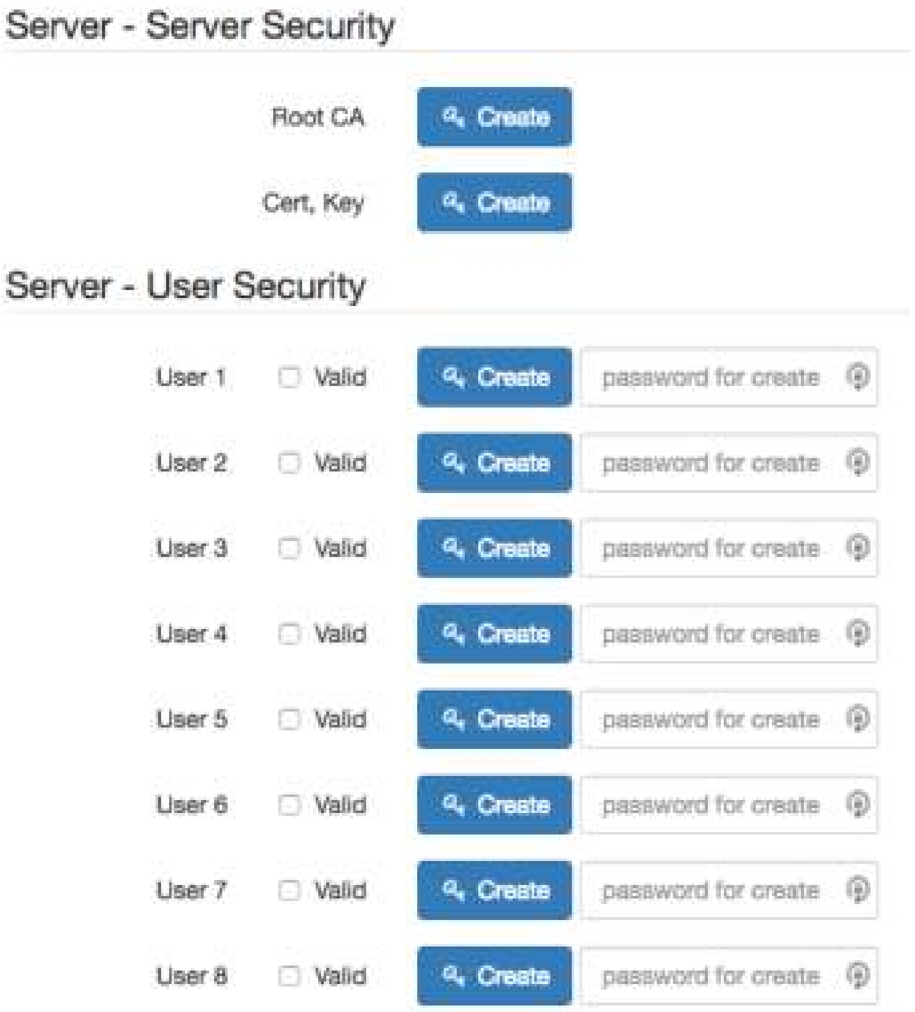
Generic setup

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.

16.9.1 Open VPN Server Mode

Open VPN server certificate generation



Server - Server Security

Root CA [Create]

Cert, Key [Create]

Server - User Security

User 1 □ Valid [Create] password for create

User 2 □ Valid [Create] password for create

User 3 □ Valid [Create] password for create

User 4 □ Valid [Create] password for create

User 5 □ Valid [Create] password for create

User 6 □ Valid [Create] password for create

User 7 □ Valid [Create] password for create

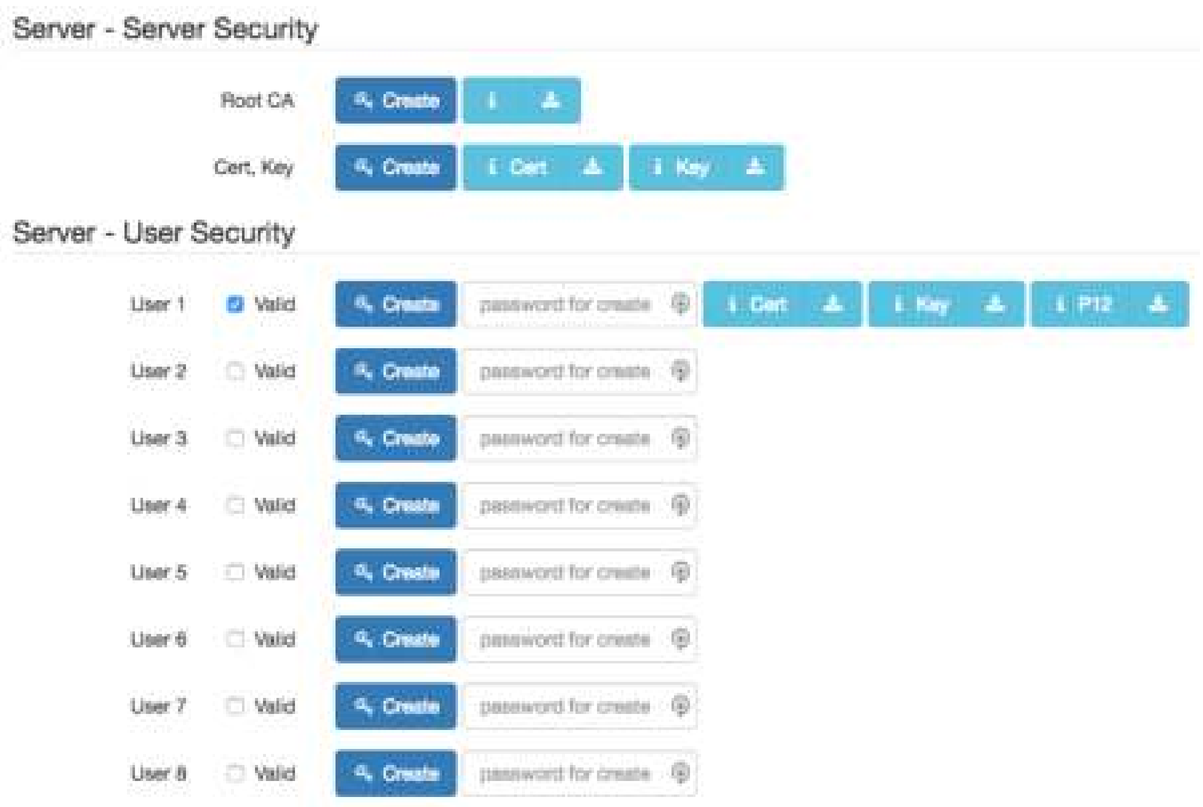
User 8 □ Valid [Create] password for create

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.

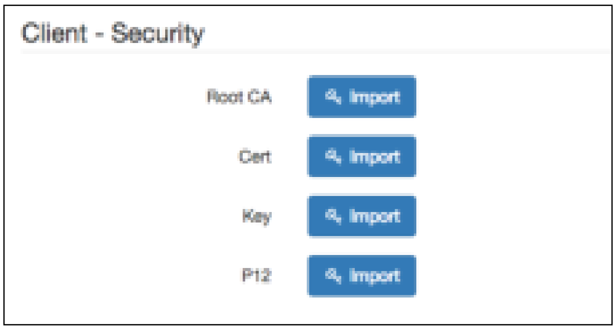
16.9.2 Open VPN Client Mode

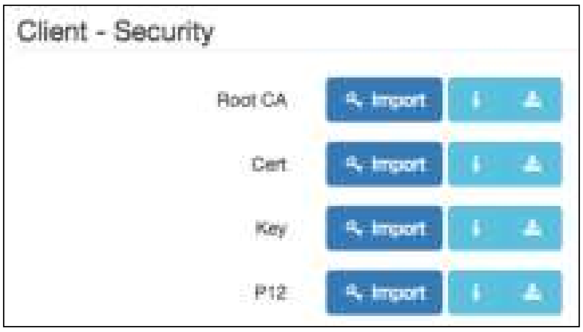
Open VPN client certificate import

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.

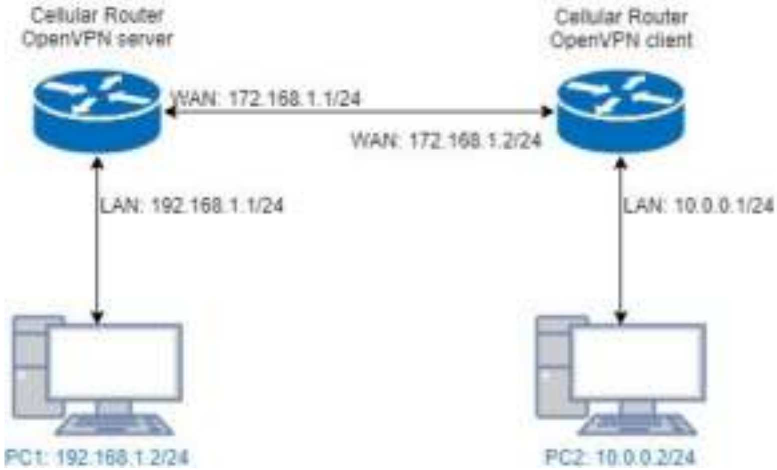




Same as Open VPN server part, you can use the info/download buttons to get the information of file or download the file to PC.

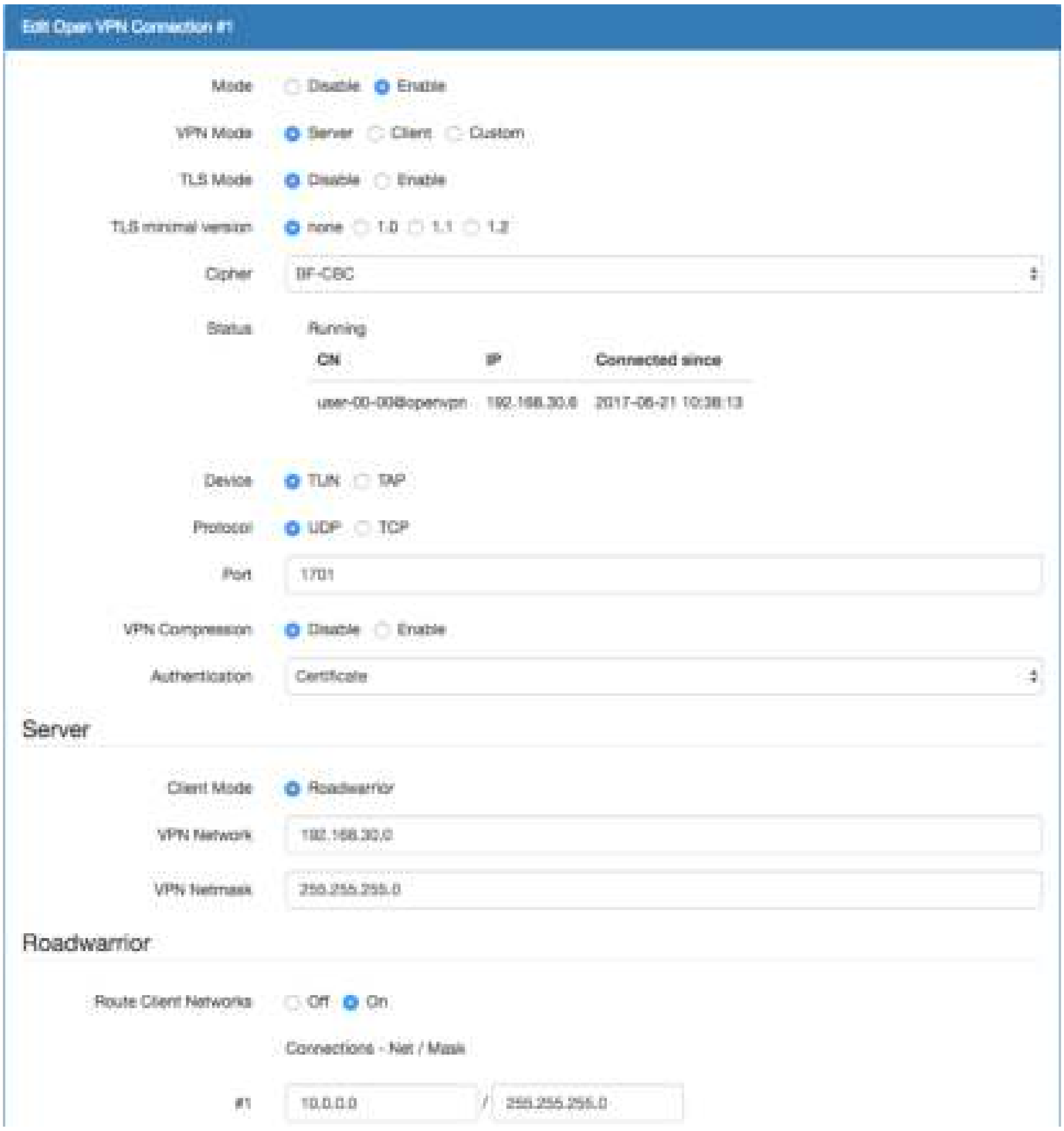
16.9.3 Open VPN Net-to-Net

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.


Edit Open VPN Connection #1

Mode ○ Disable ● Enable

VPN Mode ● Server ○ Client ○ Custom

TLS Mode ● Disable ○ Enable

TLS minimal version ● none ○ 1.0 ○ 1.1 ○ 1.2

Cipher BF-CBC

Status Running

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

Device ● TUN ○ TAP

Protocol ● UDP ○ TCP

Port 1701

VPN Compression ● Disable ○ Enable

Authentication Certificate

Server

Client Mode ● Roadwarrior

VPN Network 192.168.30.0

VPN Netmask 255.255.255.0

Roadwarrior

Route Client Networks ○ Off ● On

Connections - Net / Mask

#1 10.0.0.0 / 255.255.255.0

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

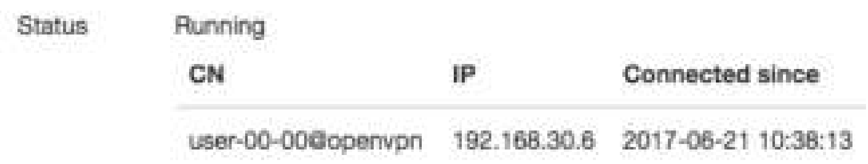
Note: The **VPN Network** should be network ID (e.g. **192.168.30.1** is invalid setting.)

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**

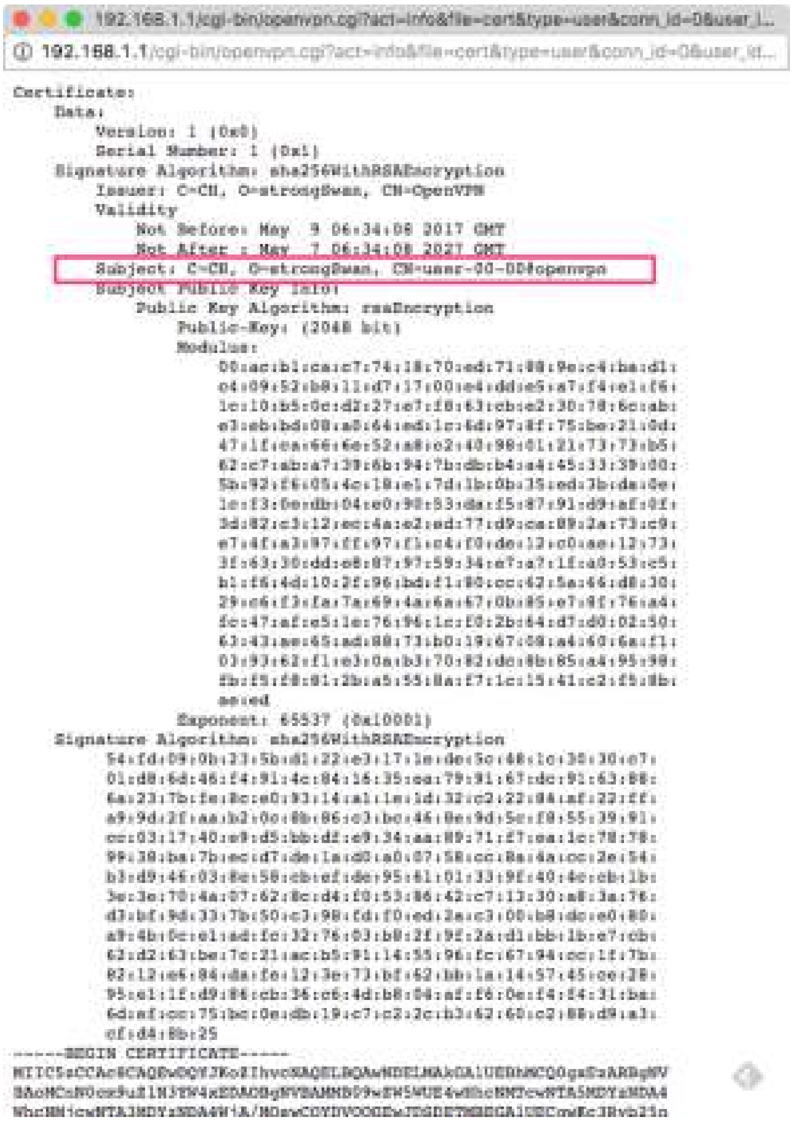
Note: The **#1** route means the routing information for **User 1**.

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...

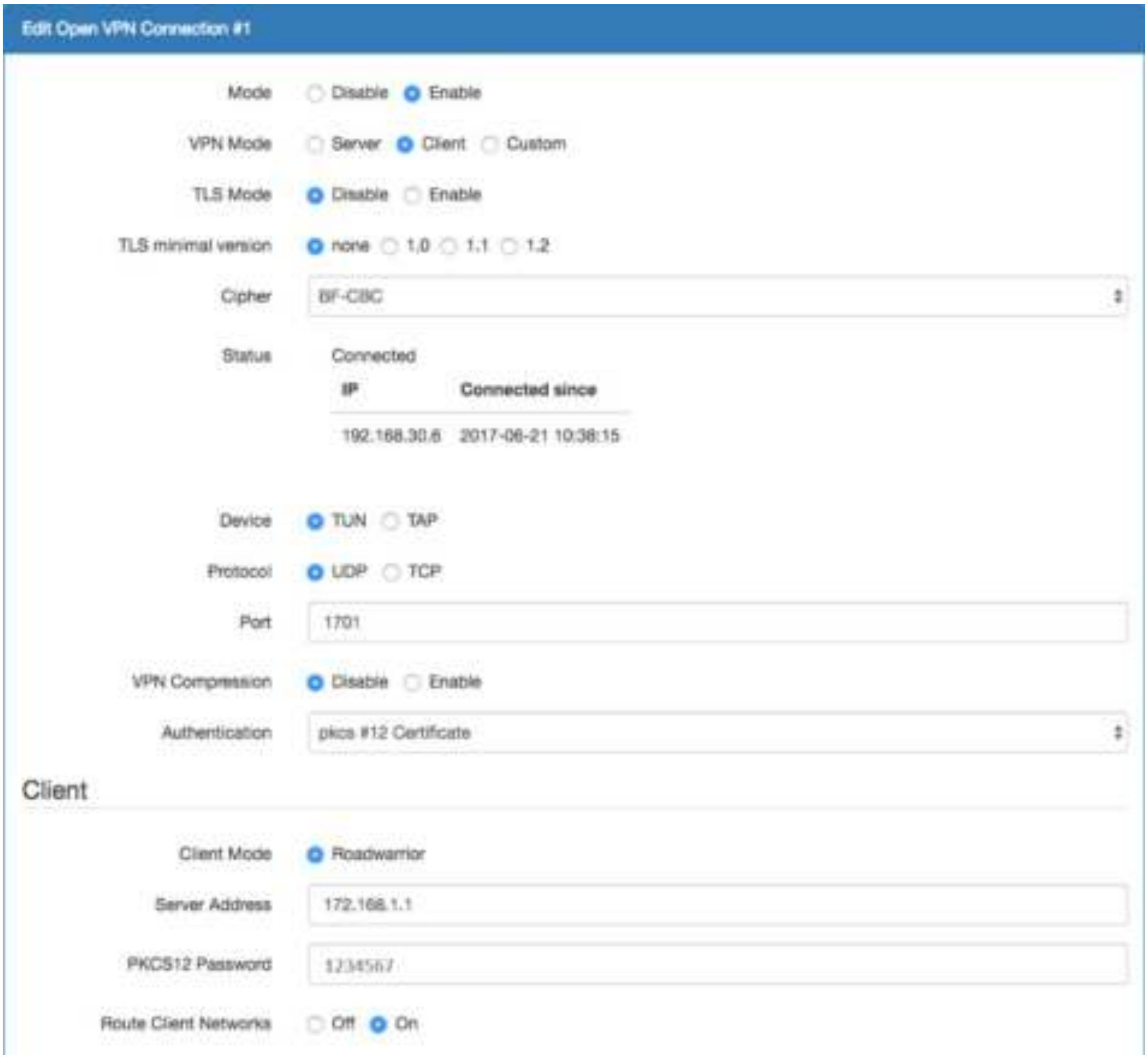
192.168.1.1/cgi-bin/openvpn.cgi?act=info&file=cert&type=user&conn_id=0&user_id...

```
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:a8:64: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:
                    1e: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:09:2a:73:c9:
                    e7:4f:a3:87: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:46: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:45: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:d2: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:2e:c3:00:b8:dc:e0:80:
         a9:4b:0c:e1:ad:fc:32:76:03:b8:2f:9f:2a:d1:bb:1b:e7:cb:
         63:d2:63:be:7c:21:ac:b5:91:14:55:96:fc:67:94:cc:1f:7b:
         82:12:e6:84:da:fc: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:af:cc:75:bc:0e:db:19:c7:c2:2c:b3:63:60:c2:88:d9:a3:
         cf:d4:8b:25
-----BEGIN CERTIFICATE-----
MIICSzCCAc8CAQEwDQYJKoZIhvcNAQELBQAwMDELMAkGA1UEBhMCQ0gxEzARBgNV
BAoMCnN0cm9uZ1N3YW4xEDAOBgNVBAMMB09wZW5WUE4wHhcNMTcwNTA5MDYzNDA4
WhcNMjcwNTA3MDYzNDA4WjA/MQswCQYDVQQGEwJDSDETMBEGA1UECgwKc3Ryb25n
```

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.



Edit Open VPN Connection #1

Mode ○ Disable ● Enable

VPN Mode ○ Server ● Client ○ Custom

TLS Mode ● Disable ○ Enable

TLS minimal version ● none ○ 1.0 ○ 1.1 ○ 1.2

Cipher BF-CBC

Status Connected

IP	Connected since
192.168.30.6	2017-06-21 10:38:15

Device ● TUN ○ TAP

Protocol ● UDP ○ TCP

Port 1701

VPN Compression ● Disable ○ Enable

Authentication pkcs #12 Certificate

Client

Client Mode ● Roadwarrior

Server Address 172.168.1.1

PKCS12 Password 1234567

Route Client Networks ○ Off ● On

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.

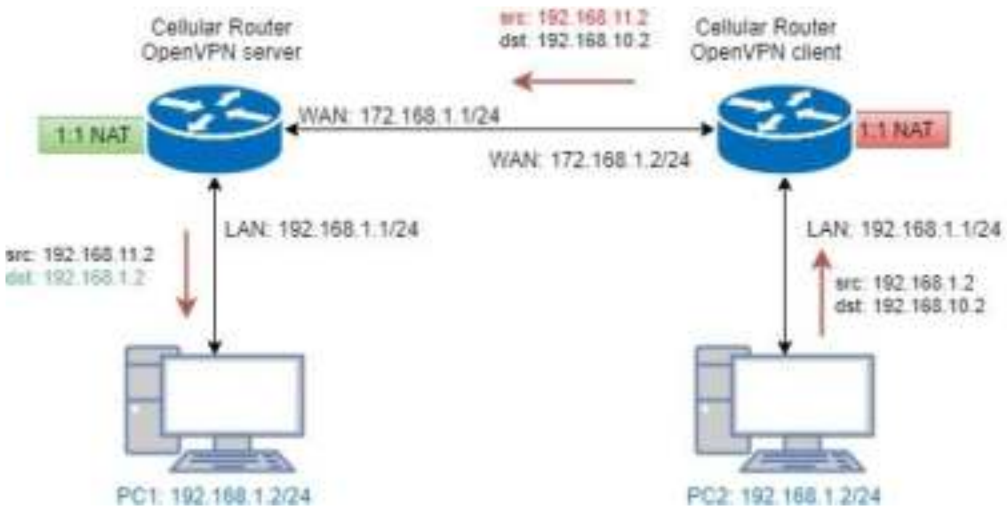
This option requires the P12 file which generated from Generic Setup Open VPN server part.

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.

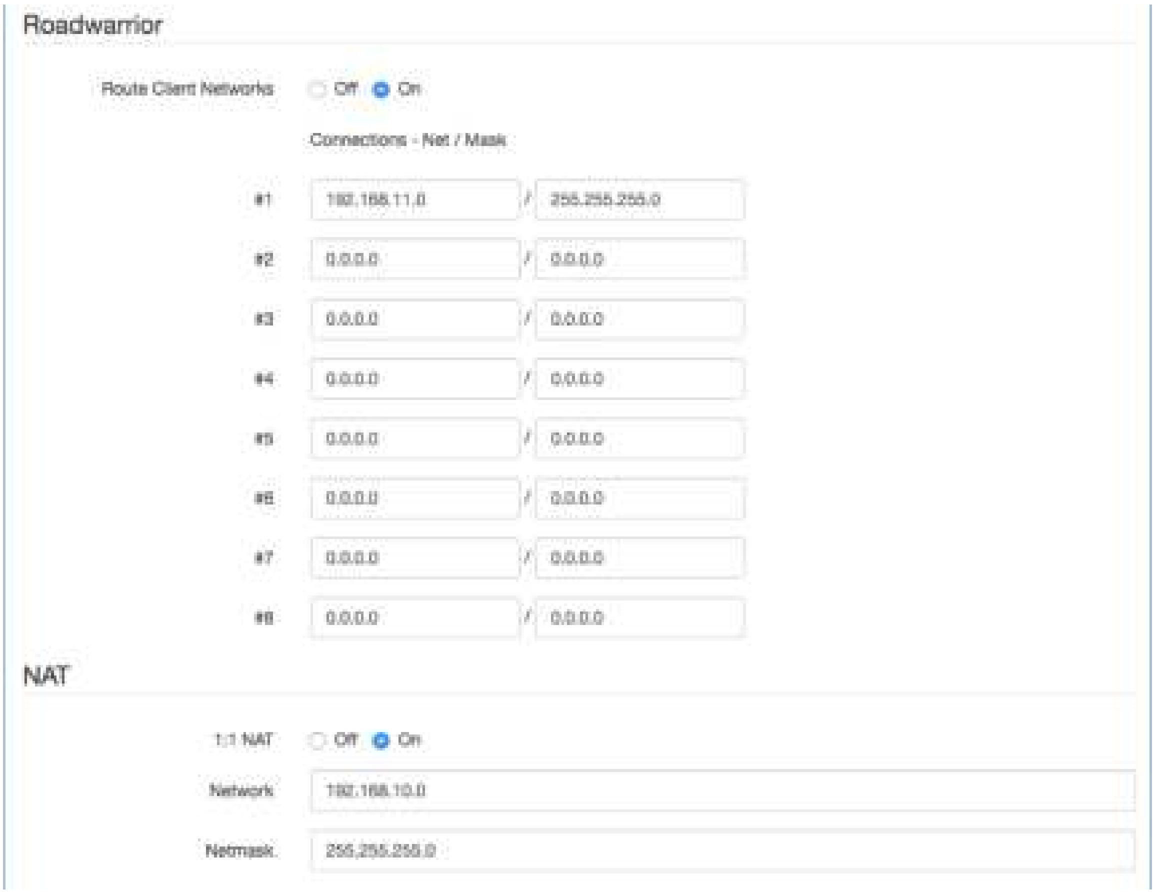
16.9.4 Open VPN 1:1 NAT



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.



Roadwarrior

Route Client Networks ○ Off ● On

Connections - Net / Mask

#1	192.168.11.0	/ 255.255.255.0
#2	0.0.0.0	/ 0.0.0.0
#3	0.0.0.0	/ 0.0.0.0
#4	0.0.0.0	/ 0.0.0.0
#5	0.0.0.0	/ 0.0.0.0
#6	0.0.0.0	/ 0.0.0.0
#7	0.0.0.0	/ 0.0.0.0
#8	0.0.0.0	/ 0.0.0.0

NAT

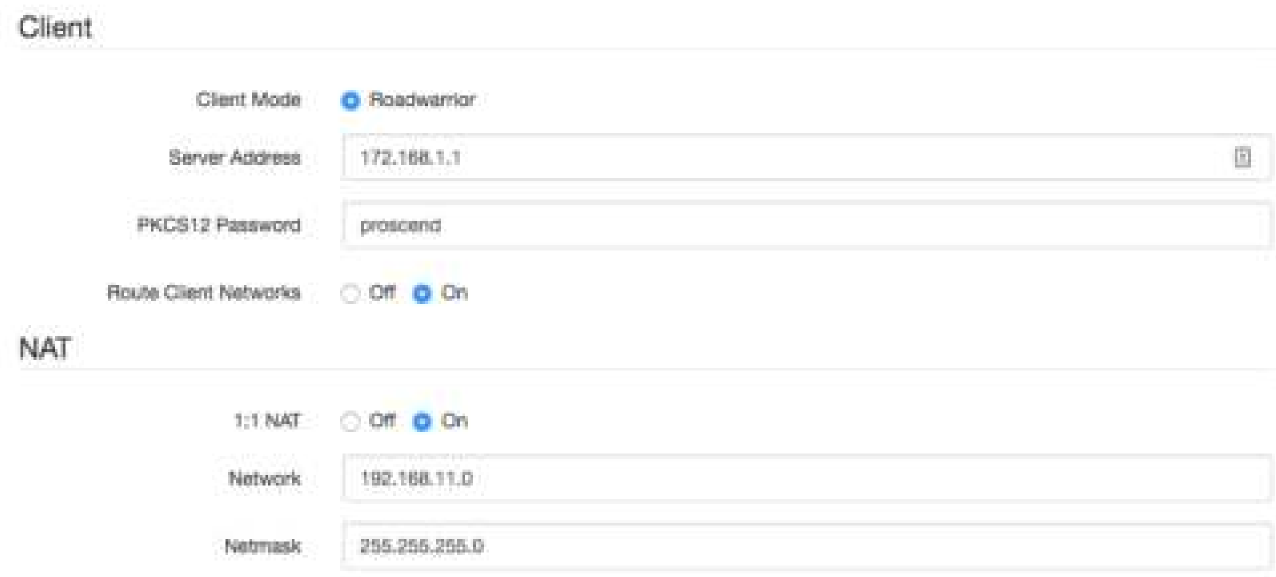
1:1 NAT ○ Off ● On

Network 192.168.10.0

Netmask 255.255.255.0

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.



Client

Client Mode ● Roadwarrior

Server Address 172.168.1.1

PKCS12 Password proscend

Route Client Networks ○ Off ● On

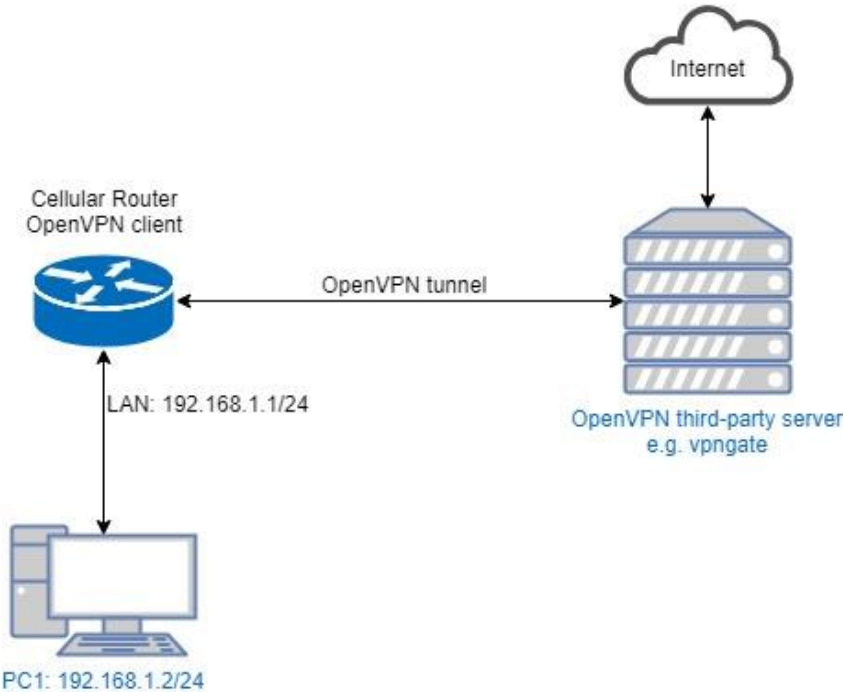
NAT

1:1 NAT ○ Off ● On

Network 192.168.11.0

Netmask 255.255.255.0

16.9.5 Open VPN with third-party server



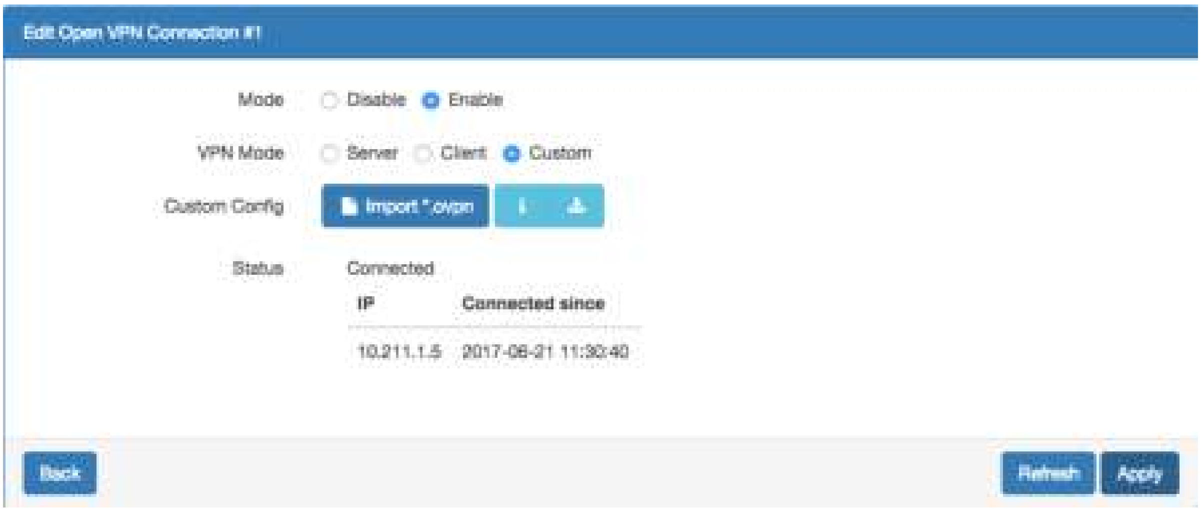
A VPN enables you to send and receive data across shared networks.

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**.



Edit Open VPN Connection #1

Mode ○ Disable ● Enable

VPN Mode ○ Server ○ Client ● Custom

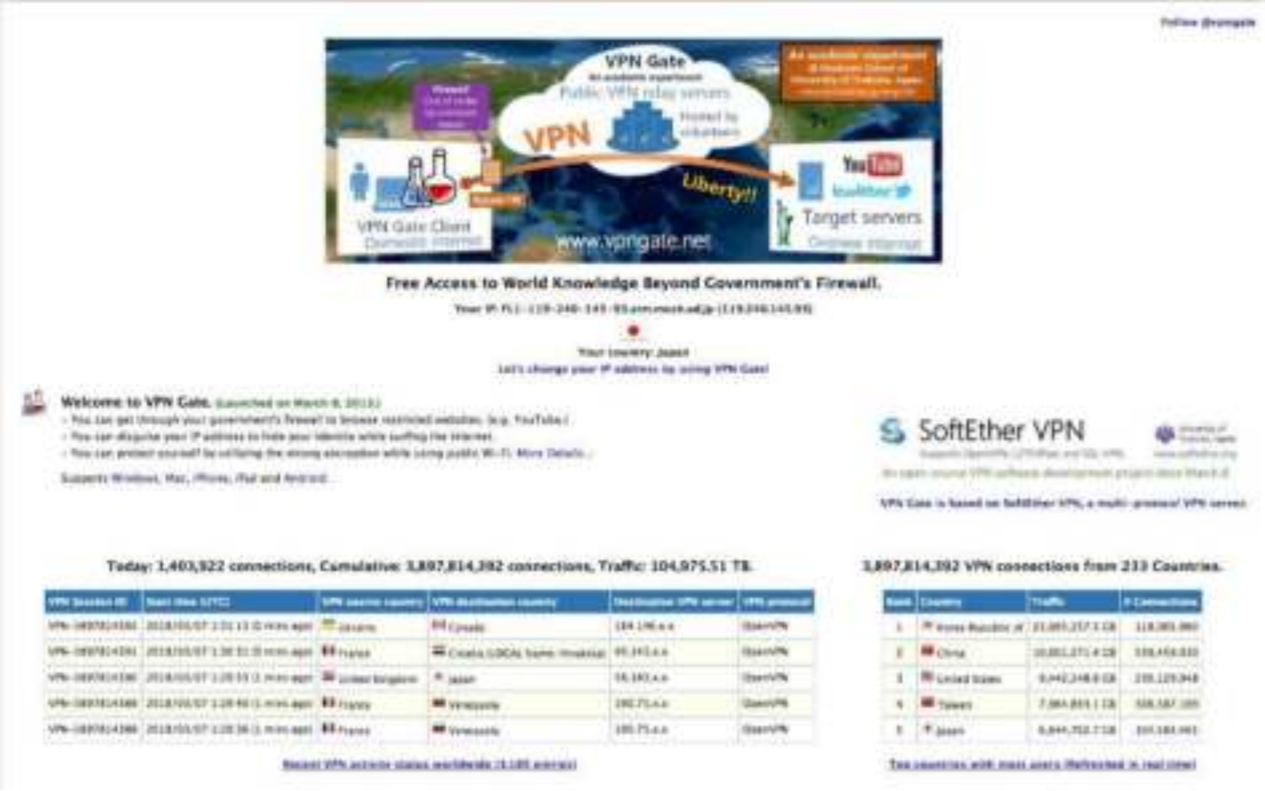
Custom Config [Import *.ovpn]

Status Connected

IP	Connected since
10.211.1.5	2017-06-21 11:30:40

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.



Free Access to World Knowledge Beyond Government's Firewall.

Your IP: [illegible]

Your country: Japan

Let's change your IP address by using VPN Gate!

Welcome to VPN Gate. [illegible]

- You can get through your government's firewall to browse restricted websites. (e.g. YouTube.)
- You can disguise your IP address to hide your identity while surfing the Internet.
- You can protect yourself by utilizing the strong encryption while using public Wi-Fi. More Details...

Supports Windows, Mac, iPhone, iPad and Android.

VPN Gate is based on SoftEther VPN, a multi-protocol VPN server.

Today: 1,403,922 connections, Cumulative: 3,897,814,392 connections, Traffic: 104,975.51 TB.

VPN Session ID	Start time (UTC)	VPN source country	VPN destination country	Destination VPN server	VPN protocol
[illegible]	[illegible]	Ukraine	Canada	[illegible]	OpenVPN
[illegible]	[illegible]	France	[illegible]	[illegible]	OpenVPN
[illegible]	[illegible]	United Kingdom	Japan	[illegible]	OpenVPN
[illegible]	[illegible]	France	Venezuela	[illegible]	OpenVPN
[illegible]	[illegible]	France	Venezuela	[illegible]	OpenVPN

Recent VPN activity status worldwide [illegible]

3,897,814,392 VPN connections from 233 Countries.

Rank	Country	Traffic	# Connections
1	Korea Republic of	[illegible]	[illegible]
2	China	[illegible]	[illegible]
3	United States	[illegible]	[illegible]
4	Taiwan	[illegible]	[illegible]
5	Japan	[illegible]	[illegible]

Top countries with most users (Refreshed in real time)

16.9.6 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
```

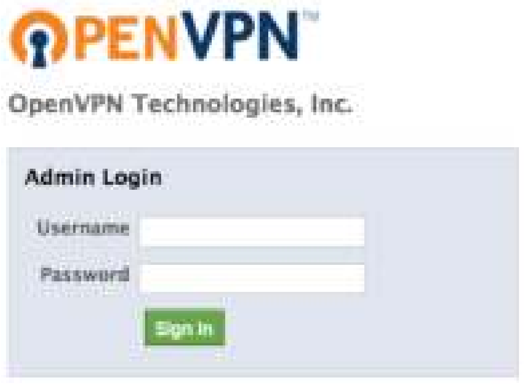
Check the Open VPN Access Server by visiting https://<server_ip_or_domain>:943

Setup Open VPN Access Server for Cellular Router

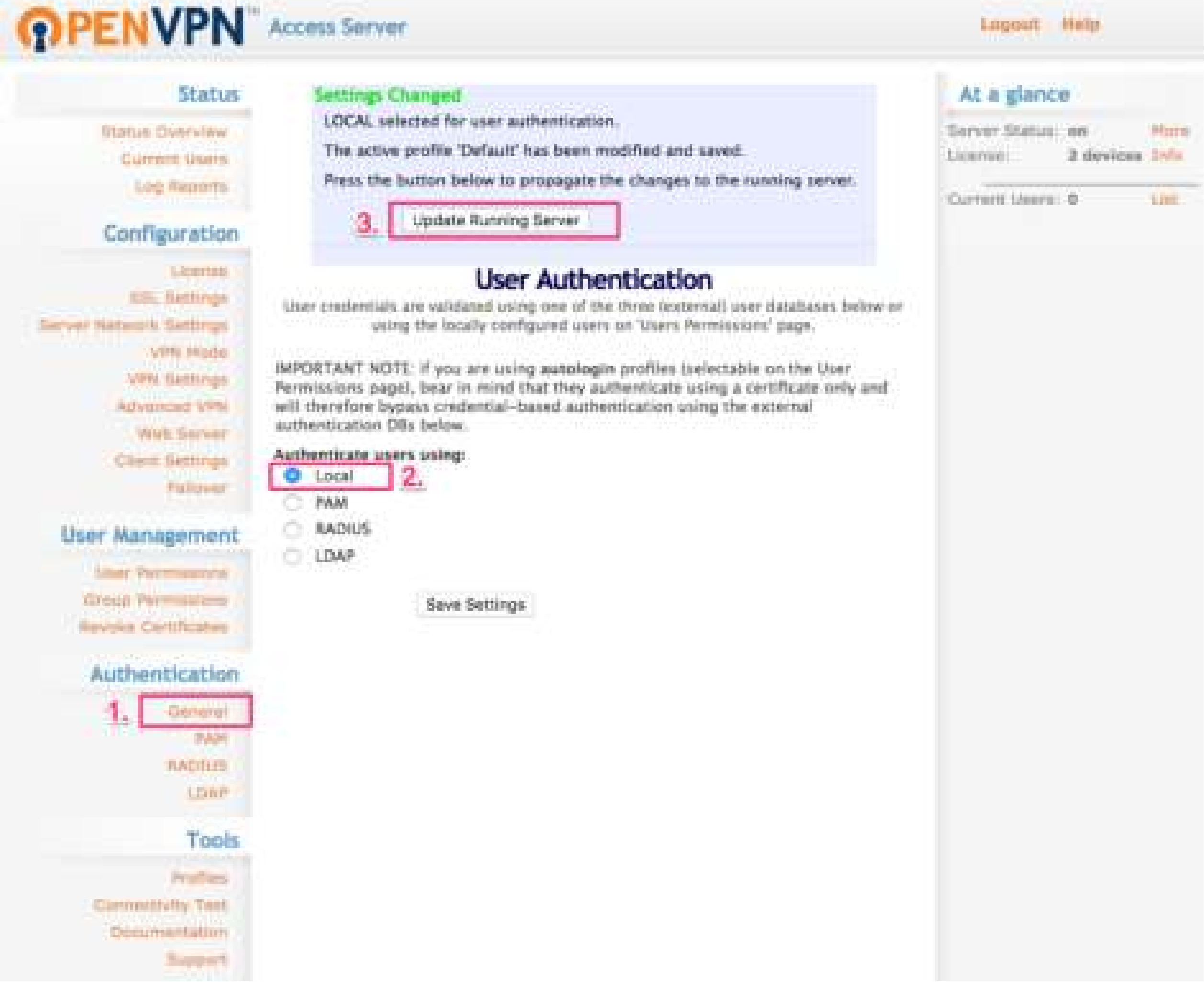
The admin page is https://<server_ip_or_domain>:943/admin

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.



Settings Changed

LOCAL selected for user authentication.

The active profile 'Default' has been modified and saved.

Press the button below to propagate the changes to the running server.

3. Update Running Server

User Authentication

User credentials are validated using one of the three (external) user databases below or using the locally configured users on 'Users Permissions' page.

IMPORTANT NOTE: If you are using **autologin** profiles (selectable on the User Permissions page), bear in mind that they authenticate using a certificate only and will therefore bypass credential-based authentication using the external authentication DBs below.

Authenticate users using:

● Local 2.

○ PAM

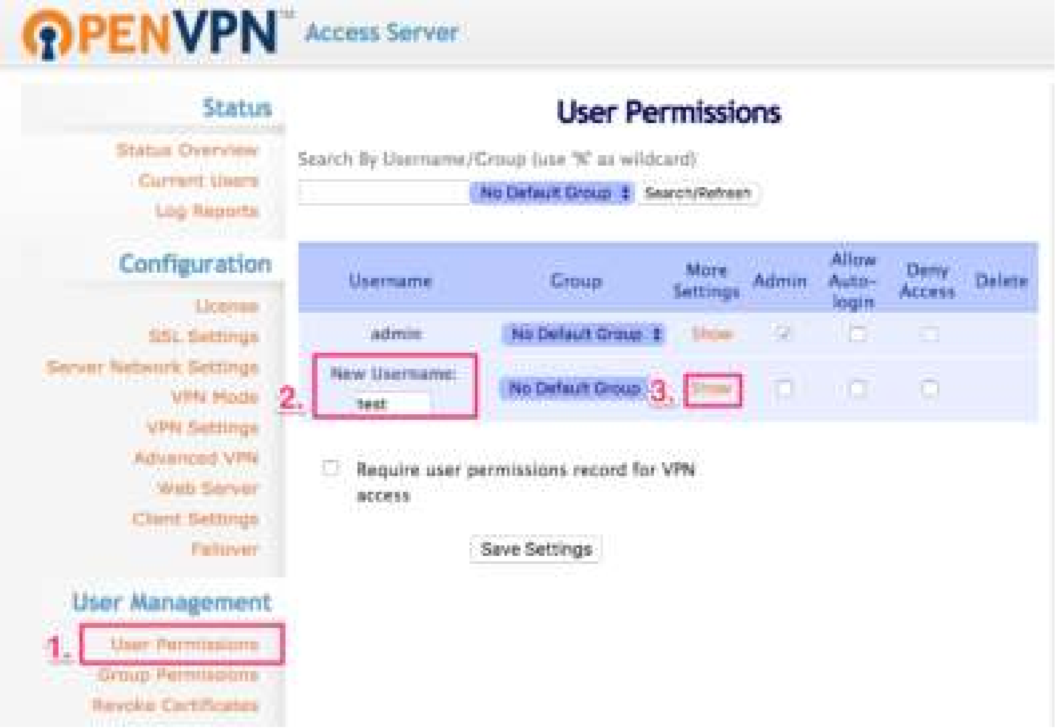
○ RADIUS

○ LDAP

Save Settings

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.)



User Permissions

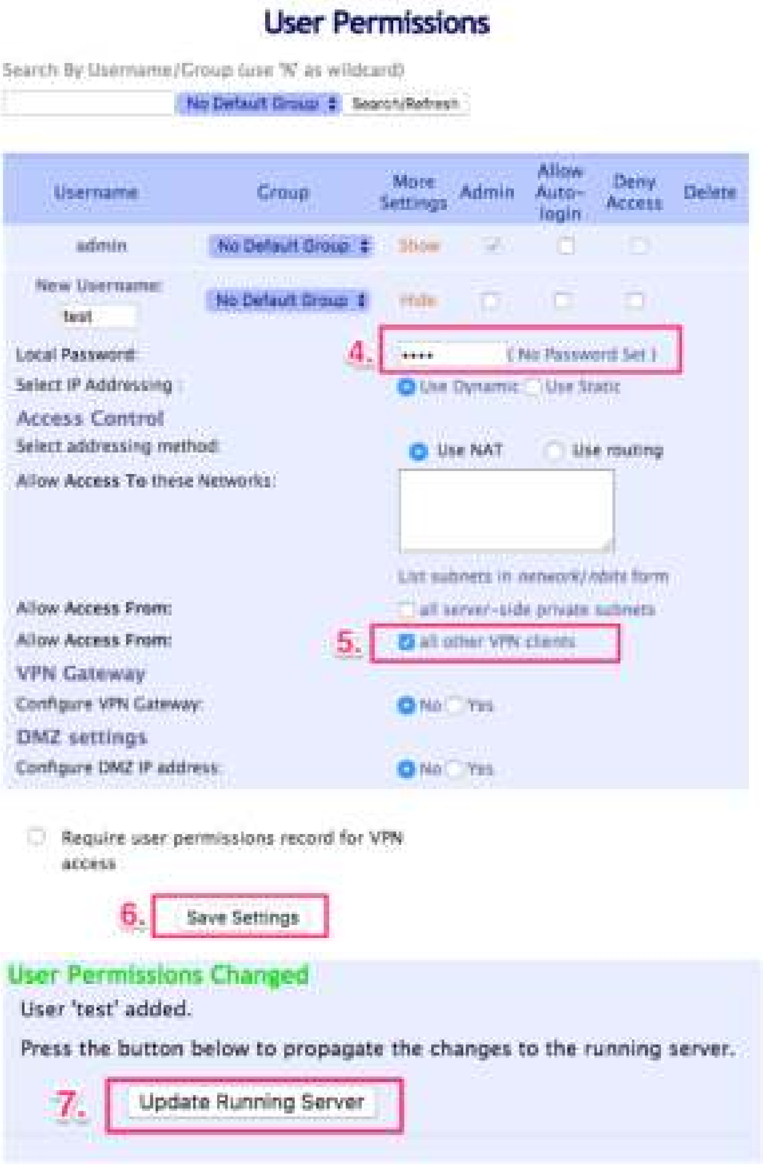
Search By Username/Group (use '%' as wildcard)

No Default Group

Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
admin	No Default Group	Show	☑	□	□	
2. New Username: test	No Default Group	3. Show	□	□	□	

□ Require user permissions record for VPN access

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



User Permissions

Search By Username/Group (use '%' as wildcard)

No Default Group | Search/Refresh

Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
admin	No Default Group	Show	✓	□	□	
New Username: test	No Default Group	Hide	□	□	□	

Local Password: 4. •••• (No Password Set)

Select IP Addressing : ● Use Dynamic ○ Use Static

Access Control

Select addressing method: ● Use NAT ○ Use routing

Allow Access To these Networks:

List subnets in network/nbits form

Allow Access From: □ all server-side private subnets

Allow Access From: 5. ☑ all other VPN clients

VPN Gateway

Configure VPN Gateway: ● No ○ Yes

DMZ settings

Configure DMZ IP address: ● No ○ Yes

□ Require user permissions record for VPN access

6. Save Settings

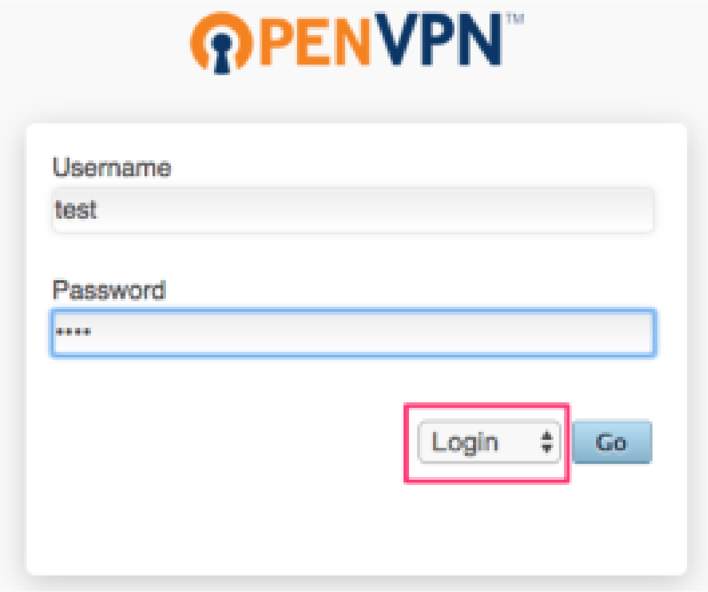
User Permissions Changed

User 'test' added.

Press the button below to propagate the changes to the running server.

7. Update Running Server

Setup Cellular Router Open VPN client



Username

test

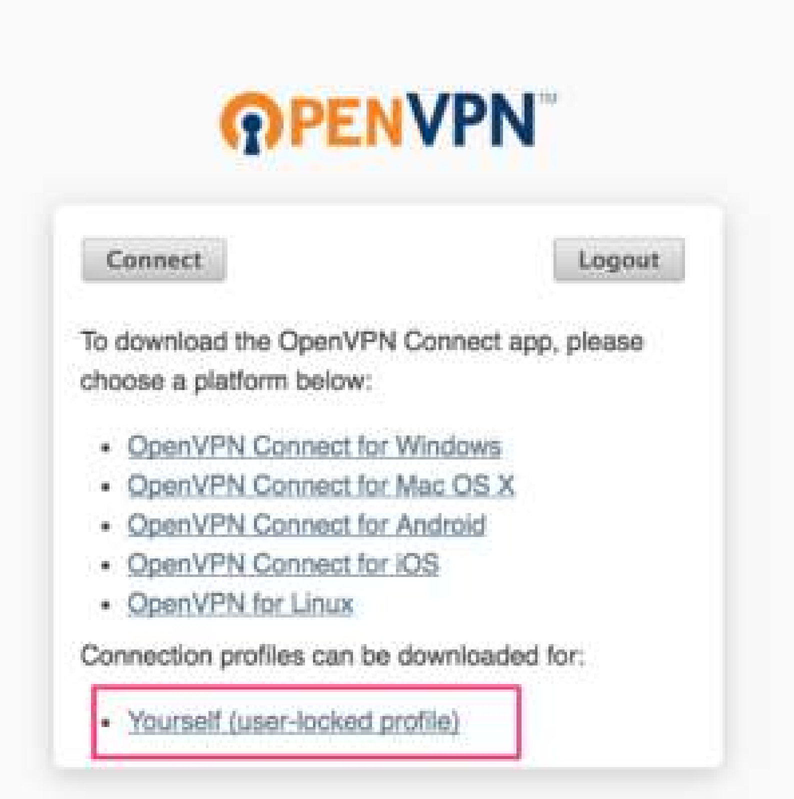
Password

••••

Login | Go

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

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



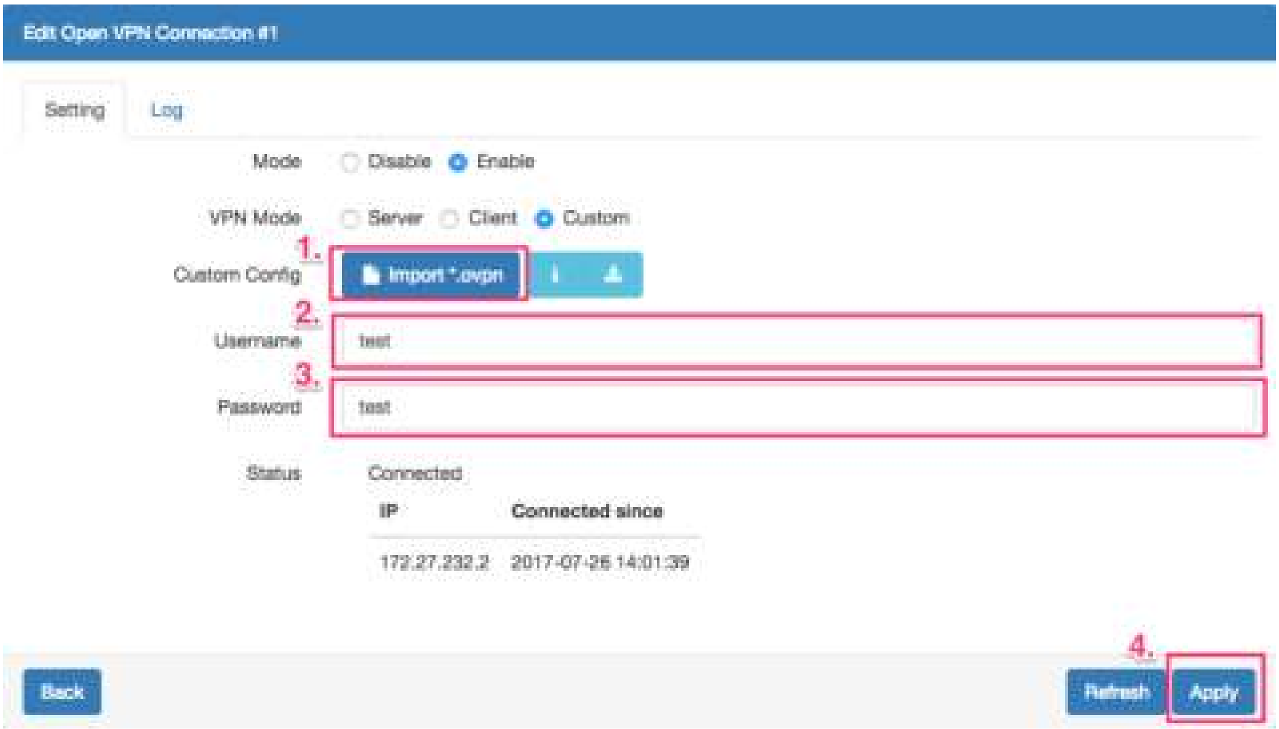
To download the OpenVPN Connect app, please choose a platform below:

- OpenVPN Connect for Windows
- OpenVPN Connect for Mac OS X
- OpenVPN Connect for Android
- OpenVPN Connect for iOS
- OpenVPN for Linux

Connection profiles can be downloaded for:

- Yourself (user-locked profile)

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



Mode ○ Disable ● Enable

VPN Mode ○ Server ○ Client ● Custom

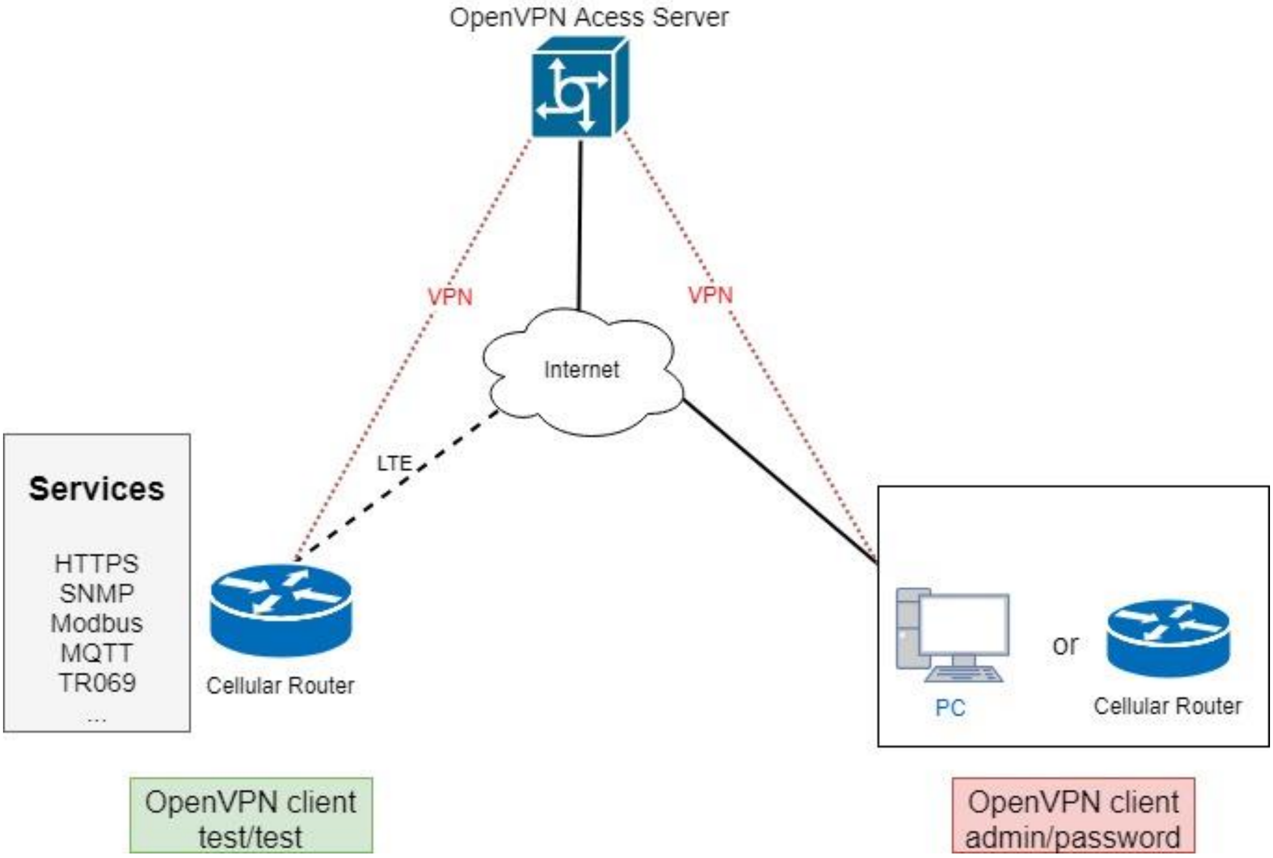
Username: test

Password: test

Status: Connected

IP	Connected since
172.27.232.2	2017-07-26 14:01:39

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.

16.9.7 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

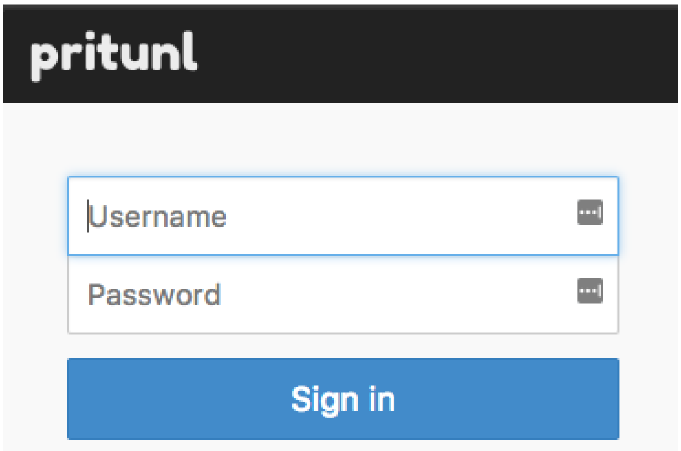
(4) Check the Pritunl Open VPN Server by visiting https://<server_ip_or_domain>

Setup Pritunl Open VPN Server for Cellular Router

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

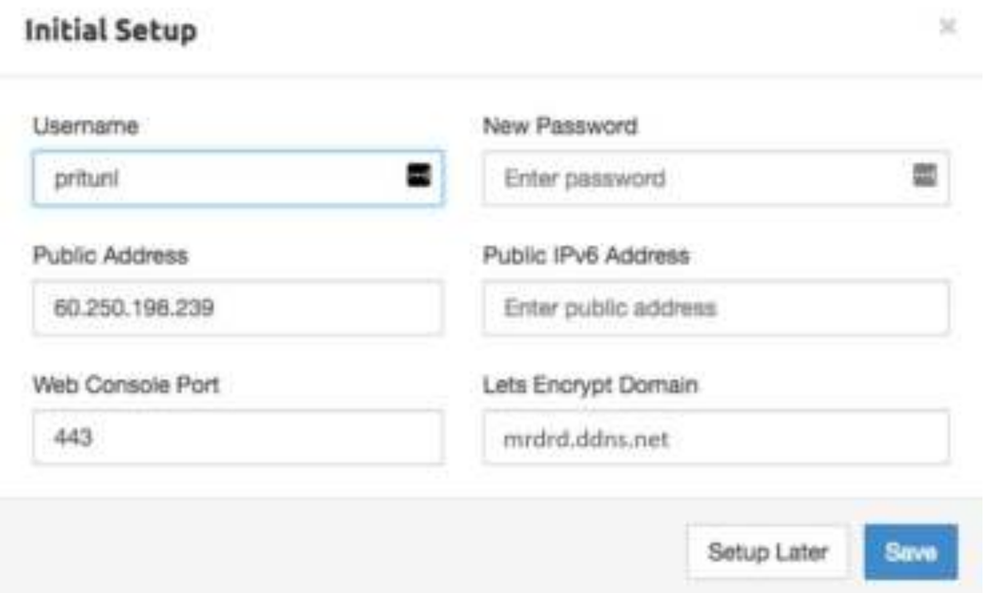
The default username/password is pritunl/pritunl.

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:


Initial Setup

Username: pritunl

New Password: Enter password

Public Address: 60.250.198.239

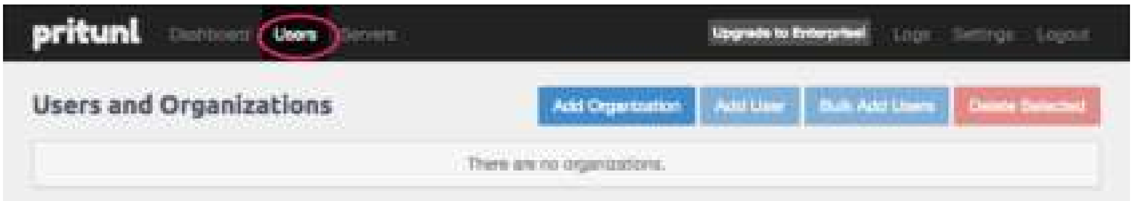
Public IPv6 Address: Enter public address

Web Console Port: 443

Lets Encrypt Domain: mrdrd.ddns.net

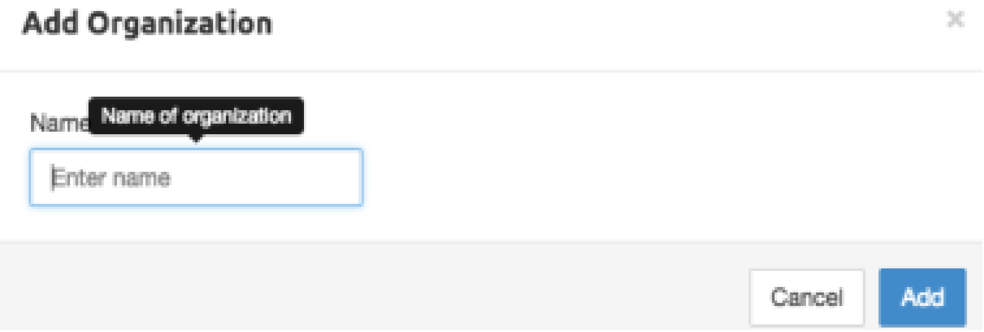
Open VPN user setup

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



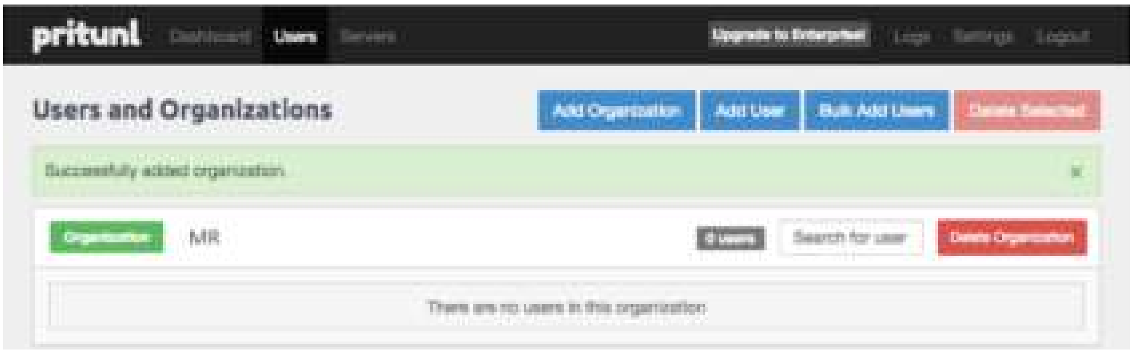
There are no organizations.

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.

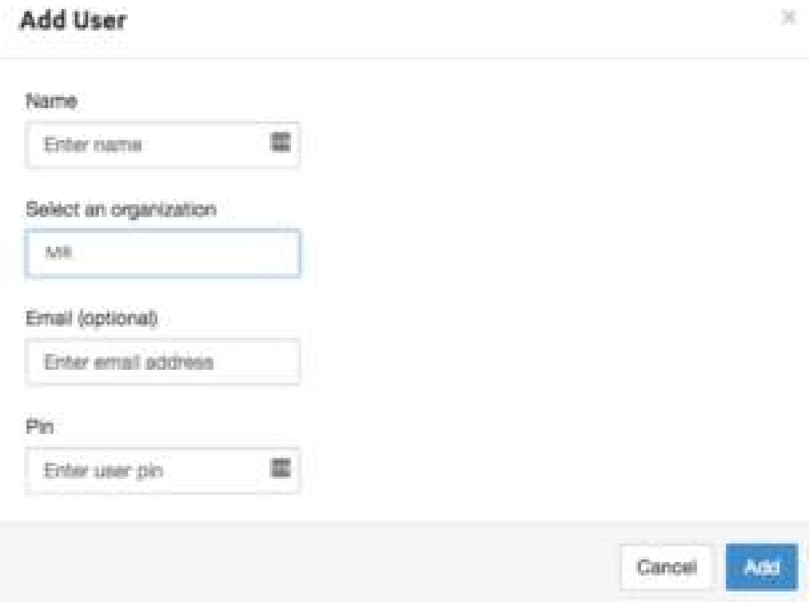


Successfully added organization.

MR

There are no users in this organization

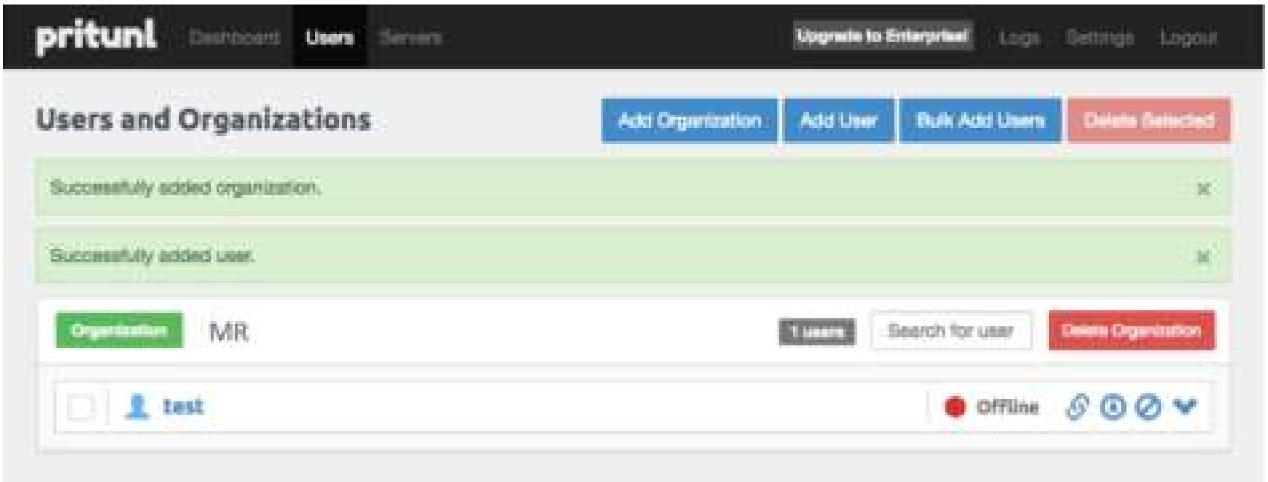
Then add the Open VPN user by click the Add User button.



Select an organization: MR

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.



Users and Organizations

Successfully added organization. ×

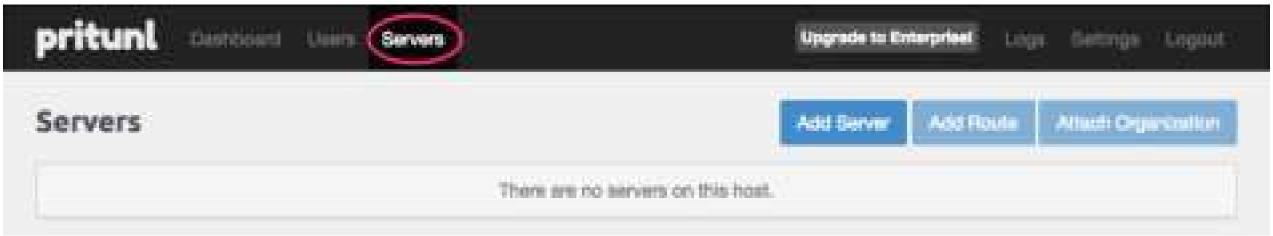
Successfully added user. ×

Organization MR 1 users Search for user

□ test ● Offline

Open VPN server setup

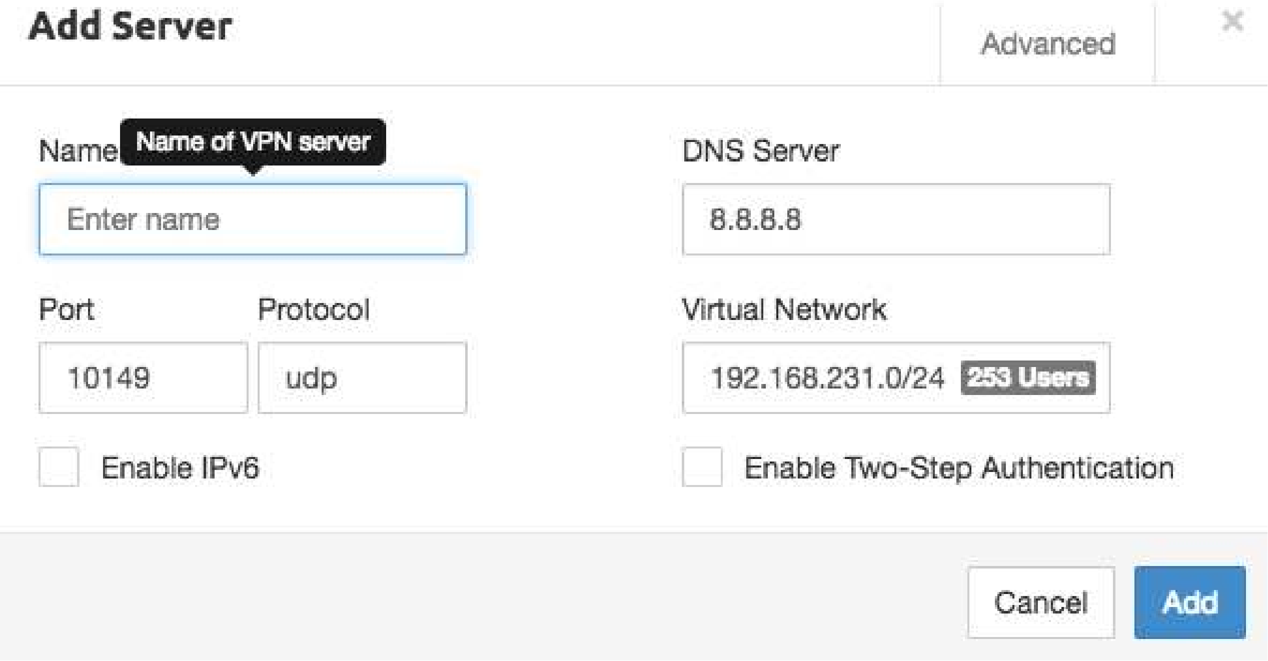
Please navigate to the Server page to setup the Open VPN server.



Servers

There are no servers on this host.

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



Add Server

Name: Enter name

DNS Server: 8.8.8.8

Port: 10149

Protocol: udp

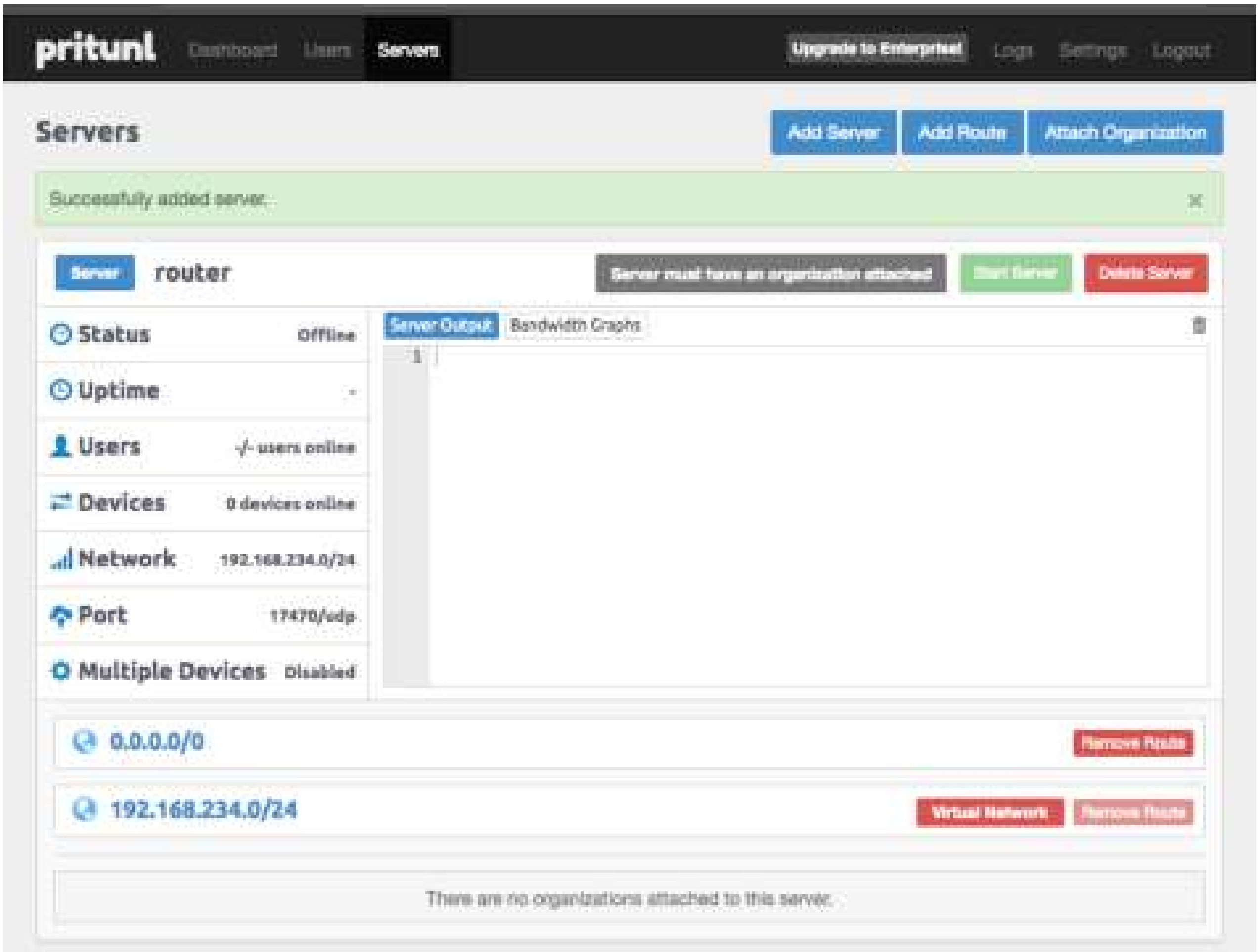
Virtual Network: 192.168.231.0/24 253 Users

□ Enable IPv6

□ Enable Two-Step Authentication

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.



Servers

Successfully added server.

router

Status Offline

Uptime -

Users -/- users online

Devices 0 devices online

Network 192.168.234.0/24

Port 17470/udp

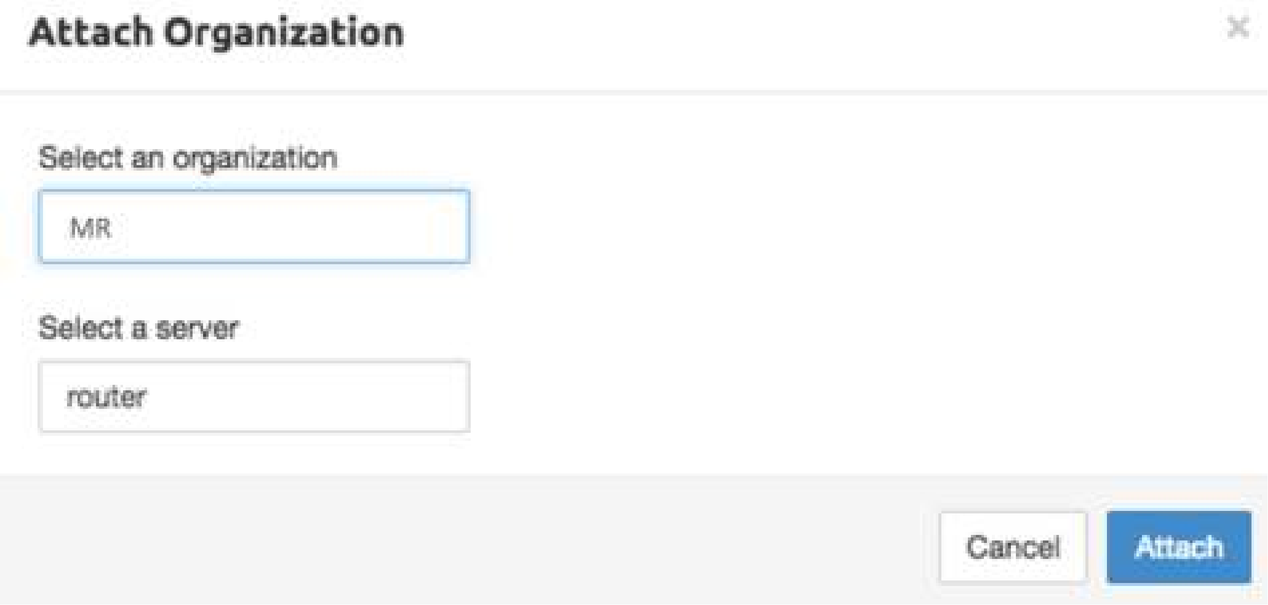
Multiple Devices Disabled

0.0.0.0/0

192.168.234.0/24

There are no organizations attached to this server.

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

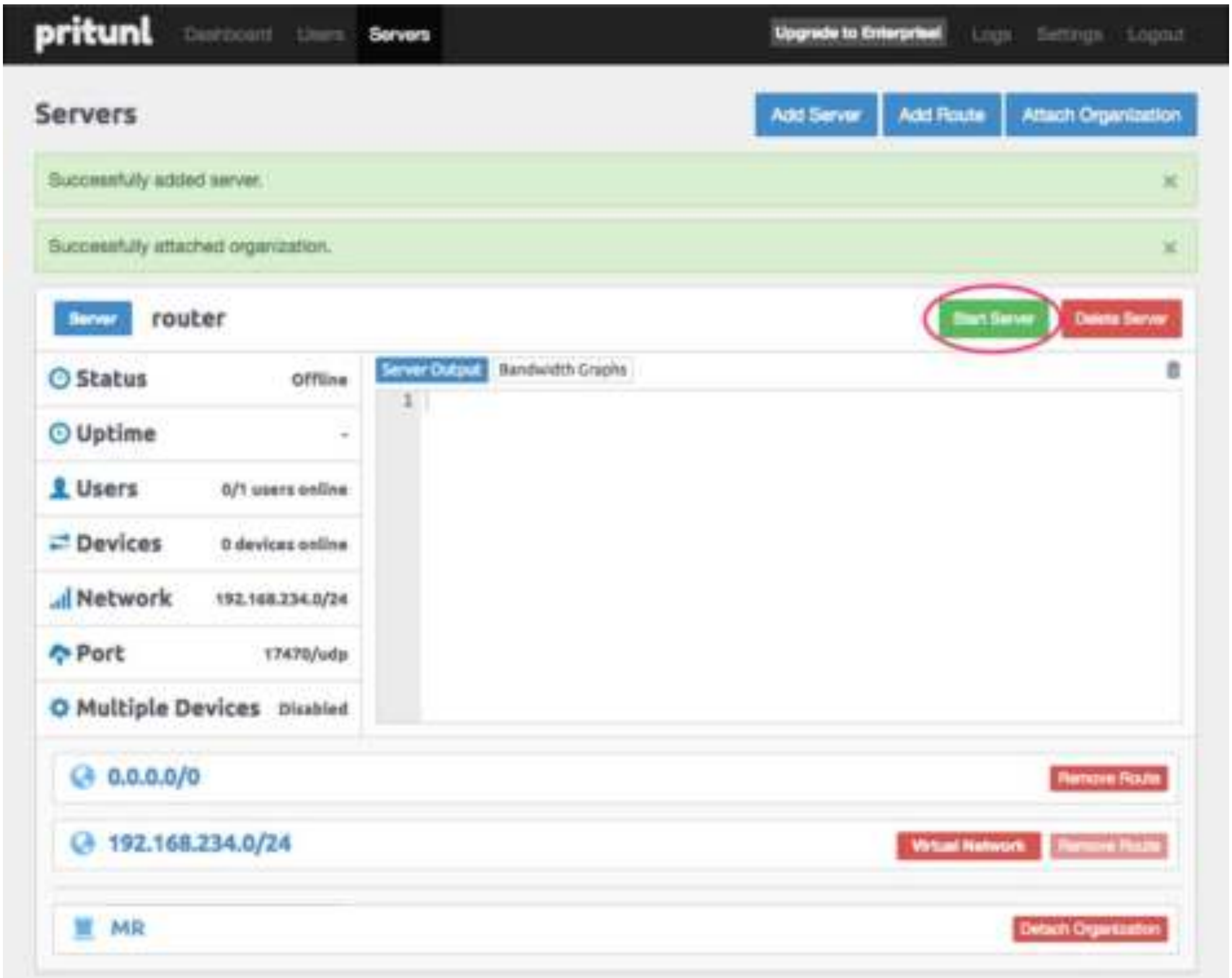


Attach Organization

Select an organization: MR

Select a server: router

Start the Open VPN server by click Start Server button.



Servers

Successfully added server.

Successfully attached organization.

router

Status Offline

Uptime -

Users 0/1 users online

Devices 0 devices online

Network 192.168.234.0/24

Port 17470/udp

Multiple Devices Disabled

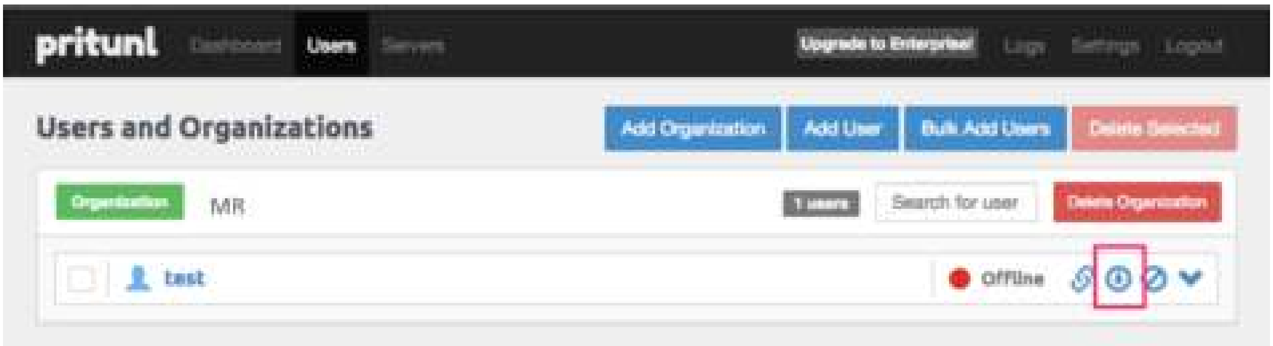
0.0.0.0/0

192.168.234.0/24

MR

Cellular Router setup

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



Users and Organizations

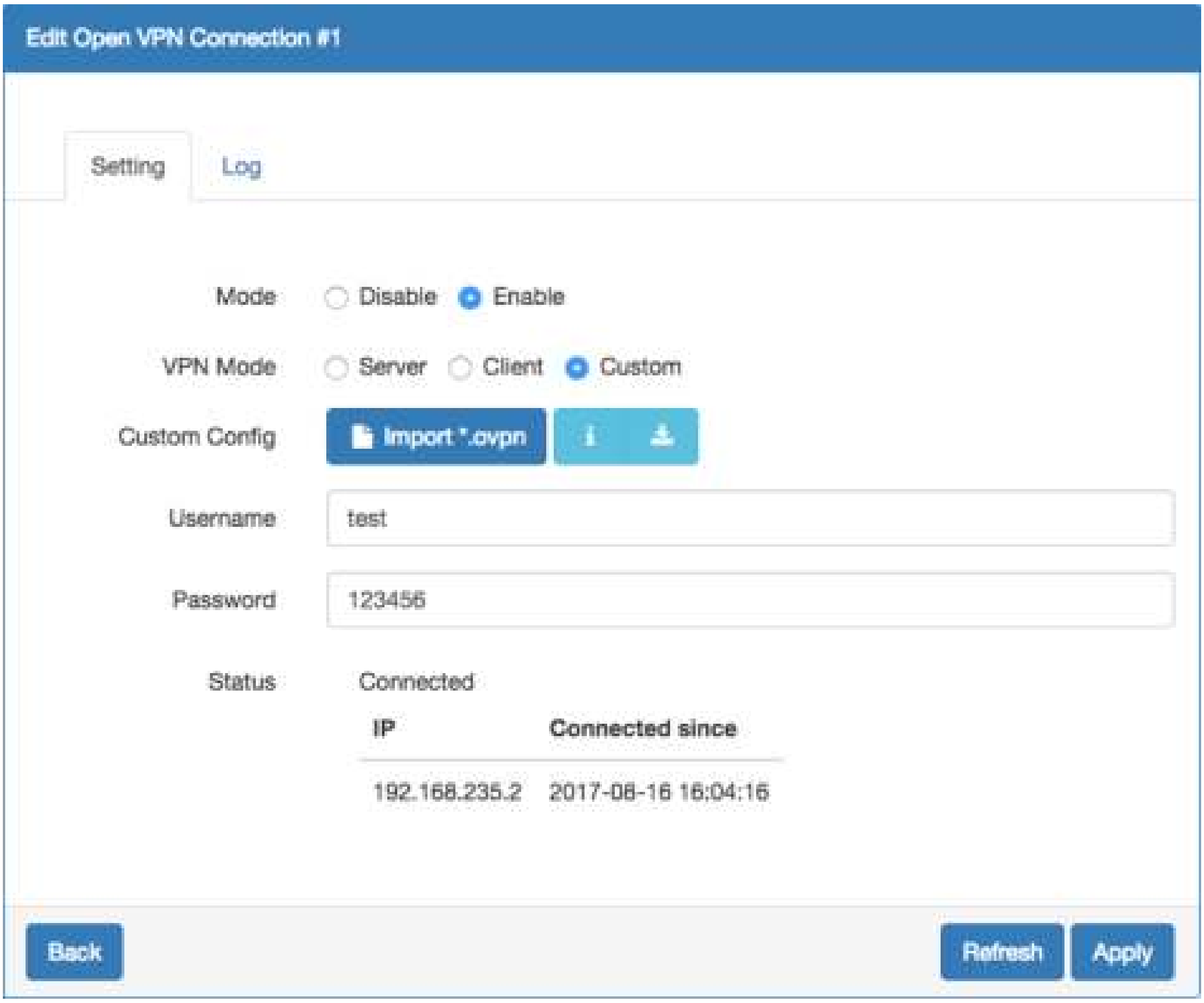
MR

test ● Offline

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.



Edit Open VPN Connection #1

Mode: ○ Disable ● Enable

VPN Mode: ○ Server ○ Client ● Custom

Custom Config

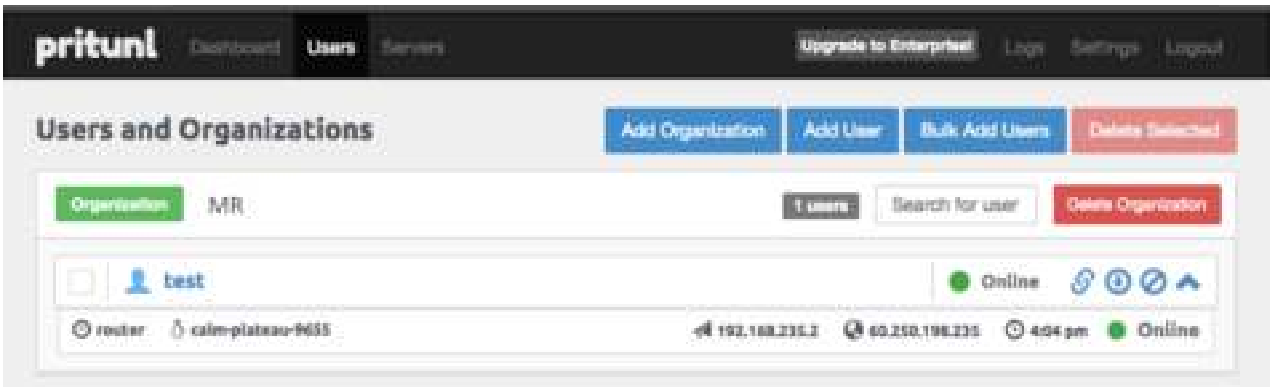
Username: test

Password: 123456

Status: Connected

IP	Connected since
192.168.235.2	2017-08-16 16:04:16

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



Users and Organizations

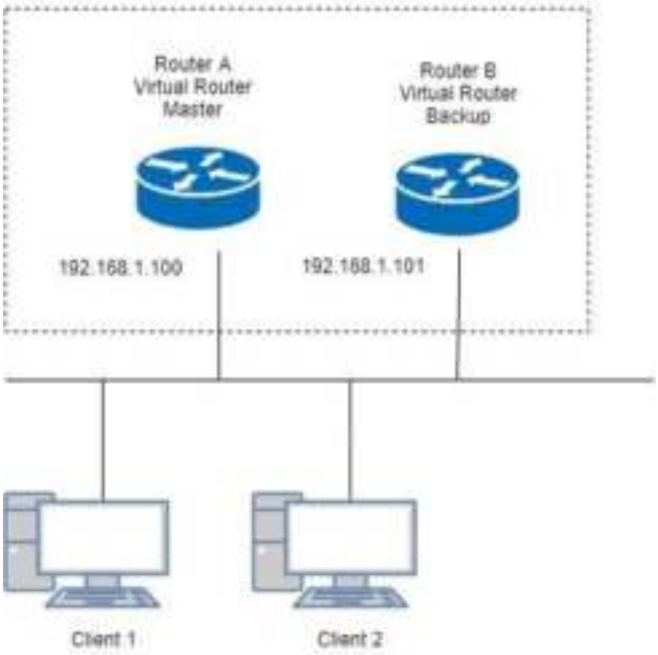
MR

test ● Online

router calm-plateau-9655 192.168.235.2 60.250.198.235 4:04 pm ● Online

16.10 VRRP Topology

Basic VRRP Topology



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

16.11 TR069 Server (GenieACS Installation)

Server OS: Ubuntu 14.04 on Virtualbox

Installation:

1) Login ubuntu
2) Change to root by 'su -' and enter your root password.
3) Install required package as below command:

```
>apt install gcc openssl-devel zlib-devel readline-devel sqlite-devel
```

4) Make a directory for application installation

```
>mkdir /opt
```

5) Install yaml

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

6) Install ruby

```
cd /opt
wget http://cache.ruby-lang.org/pub/ruby/2.4/ruby-2.4.1.tar.gz
tar xvzf uby-2.4.1.tar.gz
cd ruby-2.4.1
```

```
./configure
make && make install
ruby    -v
ruby 2.4.1p111 (2017-03-22 revision 58053) [i686-linux]
```

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

7) Install node.js

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

8) Install redis

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

9) Install mongodb

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

10) Install genieACS

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

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

Original configuration:

```
"FS_HOSTNAME" : "acs.example.com"
```

New configuration example.:

```
"FS_HOSTNAME" : "192.168.0.199"
```

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

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

Original configuration:

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

New configuration example:

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

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

11) Install genieACS-Gui

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

gem install json
bundle update

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

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

GenieACS startup script:

```
#!/bin/sh

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

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

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

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

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

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

GenieACS stop:

Ctrl-C

Usage:

1) Device Configuration

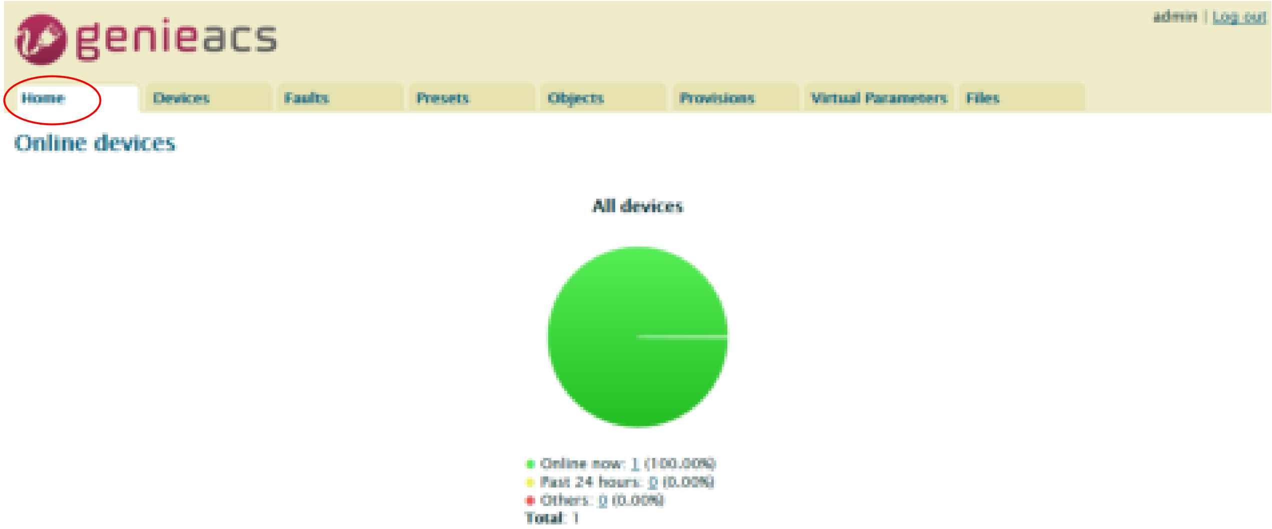
Fill in the ACS URL field as http://GenieACS server IP:7547

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

2) GenieACS Operation

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

Press Home tab to refresh Online devices status.



Online devices

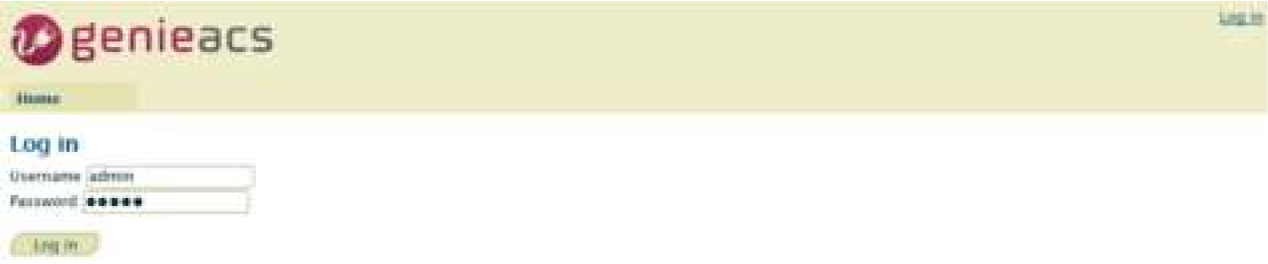
All devices

- 🟩 Online now: 1 (100.00%)
- 🟨 Past 24 hours: 0 (0.00%)
- 🟥 Others: 0 (0.00%)

Total: 1

2.1) Login

Username and Password are admin/admin.

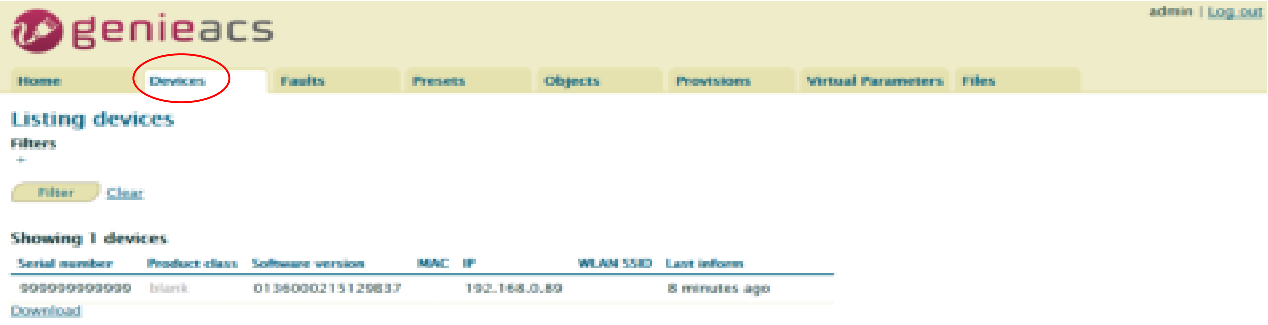


Log in

Username: admin
Password: ●●●●●

3) Device information

Press Devices tab



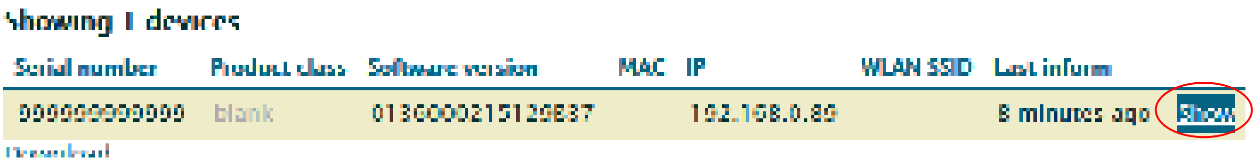
Listing devices

Filters

Showing 1 devices

Serial number	Product class	Software version	MAC	IP	WLAN SSID	Last inform
999999999999	blank	0136000215129837		192.168.0.89		8 minutes ago

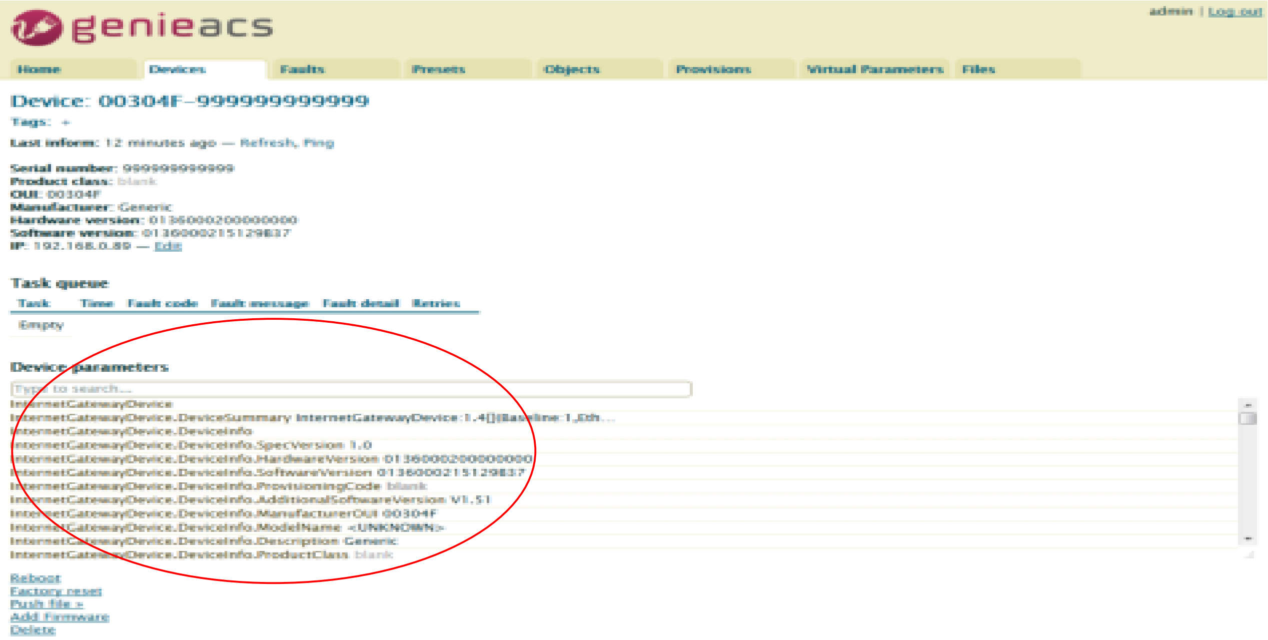
Move mouse to line end of your device, the Show link show up.



Showing 1 devices

Serial number	Product class	Software version	MAC	IP	WLAN SSID	Last inform	
999999999999	blank	0136000215129837		192.168.0.89		8 minutes ago	Show

Press Show link, the device information shows up.



Device: 00304F-999999999999

Tags: +

Last inform: 12 minutes ago — Refresh, Ping

Serial number: 999999999999
Product class: blank
OUI: 00304F
Manufacturer: Generic
Hardware version: 0136000200000000
Software version: 0136000215129837
IP: 192.168.0.89 — Edit

Task queue

Task	Time	Fault code	Fault message	Fault detail	Retries
Empty					

Device parameters

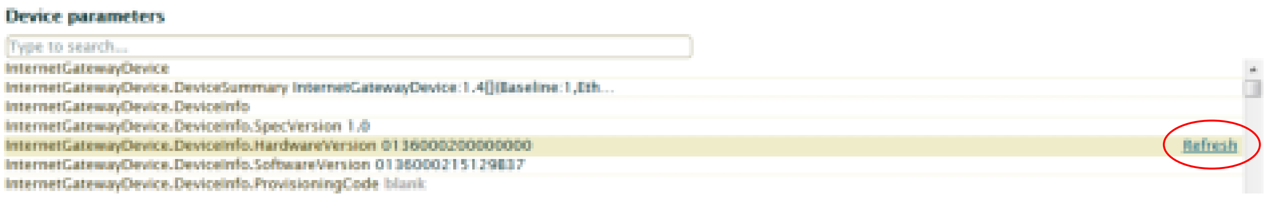
Type to search...

```
InternetGatewayDevice
InternetGatewayDevice.DeviceSummary InternetGatewayDevice:1.4[](Baseline:1,Eth...
InternetGatewayDevice.DeviceInfo
InternetGatewayDevice.DeviceInfo.SpecVersion 1.0
InternetGatewayDevice.DeviceInfo.HardwareVersion 0136000200000000
InternetGatewayDevice.DeviceInfo.SoftwareVersion 0136000215129837
InternetGatewayDevice.DeviceInfo.ProvisioningCode blank
InternetGatewayDevice.DeviceInfo.AdditionalSoftwareVersion V1.51
InternetGatewayDevice.DeviceInfo.ManufacturerOUI 00304F
InternetGatewayDevice.DeviceInfo.ModelName <UNKNOWN>
InternetGatewayDevice.DeviceInfo.Description Generic
InternetGatewayDevice.DeviceInfo.ProductClass blank
```

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



Device parameters

Type to search...

InternetGatewayDevice

InternetGatewayDevice.DeviceSummary InternetGatewayDevice:1.4[](Baseline:1,Eth...

InternetGatewayDevice.DeviceInfo

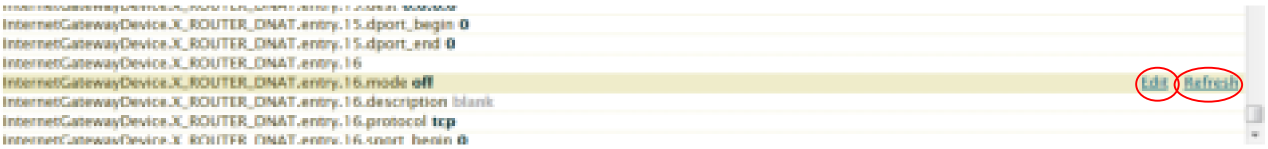
InternetGatewayDevice.DeviceInfo.SpecVersion 1.0

InternetGatewayDevice.DeviceInfo.HardwareVersion 0136000200000000

InternetGatewayDevice.DeviceInfo.SoftwareVersion 0136000215129837

InternetGatewayDevice.DeviceInfo.ProvisioningCode blank

For Readable and Writable parameter



InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dport_begin **0**

InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dport_end **0**

InternetGatewayDevice.X_ROUTER_DNAT.entry.16

InternetGatewayDevice.X_ROUTER_DNAT.entry.16.mode **off**

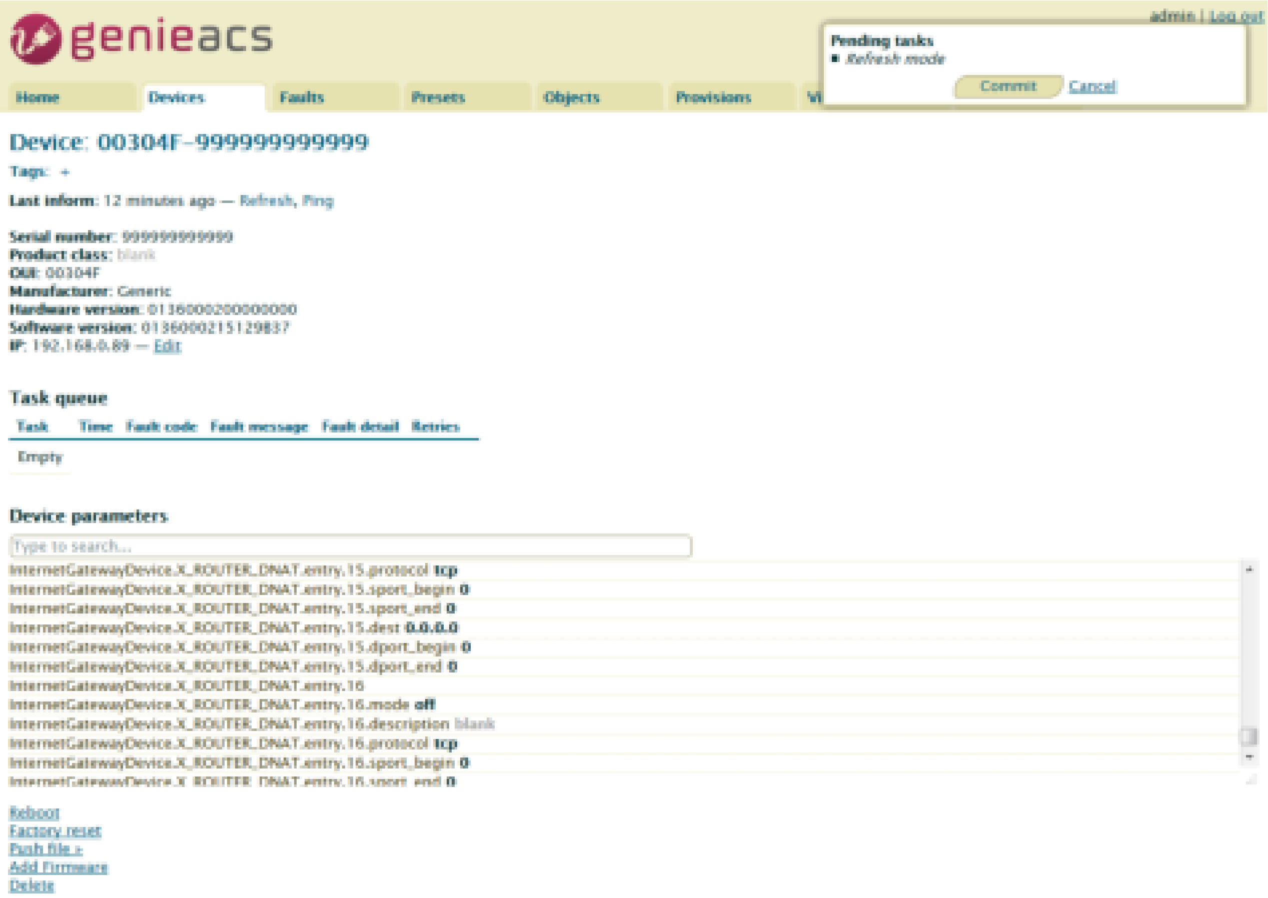
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.description blank

InternetGatewayDevice.X_ROUTER_DNAT.entry.16.protocol **tcp**

InternetGatewayDevice.X_ROUTER_DNAT.entry.16.sport_begin **0**

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.



Pending tasks

- *Refresh mode*

Device: 00304F-999999999999

Tags: +

Last inform: 12 minutes ago — Refresh, Ping

Serial number: 999999999999

Product class: blank

OUI: 00304F

Manufacturer: Generic

Hardware version: 0136000200000000

Software version: 0136000215129837

IP: 192.168.0.89 — Edit

Task queue

Task	Time	Fault code	Fault message	Fault detail	Retries
Empty					

Device parameters

Type to search...

InternetGatewayDevice.X_ROUTER_DNAT.entry.15.protocol **tcp**

InternetGatewayDevice.X_ROUTER_DNAT.entry.15.sport_begin **0**

InternetGatewayDevice.X_ROUTER_DNAT.entry.15.sport_end **0**

InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dest **0.0.0.0**

InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dport_begin **0**

InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dport_end **0**

InternetGatewayDevice.X_ROUTER_DNAT.entry.16

InternetGatewayDevice.X_ROUTER_DNAT.entry.16.mode **off**

InternetGatewayDevice.X_ROUTER_DNAT.entry.16.description blank

InternetGatewayDevice.X_ROUTER_DNAT.entry.16.protocol **tcp**

InternetGatewayDevice.X_ROUTER_DNAT.entry.16.sport_begin **0**

InternetGatewayDevice.X_ROUTER_DNAT.entry.16.sport_end **0**

Press Commit to get this parameter value.

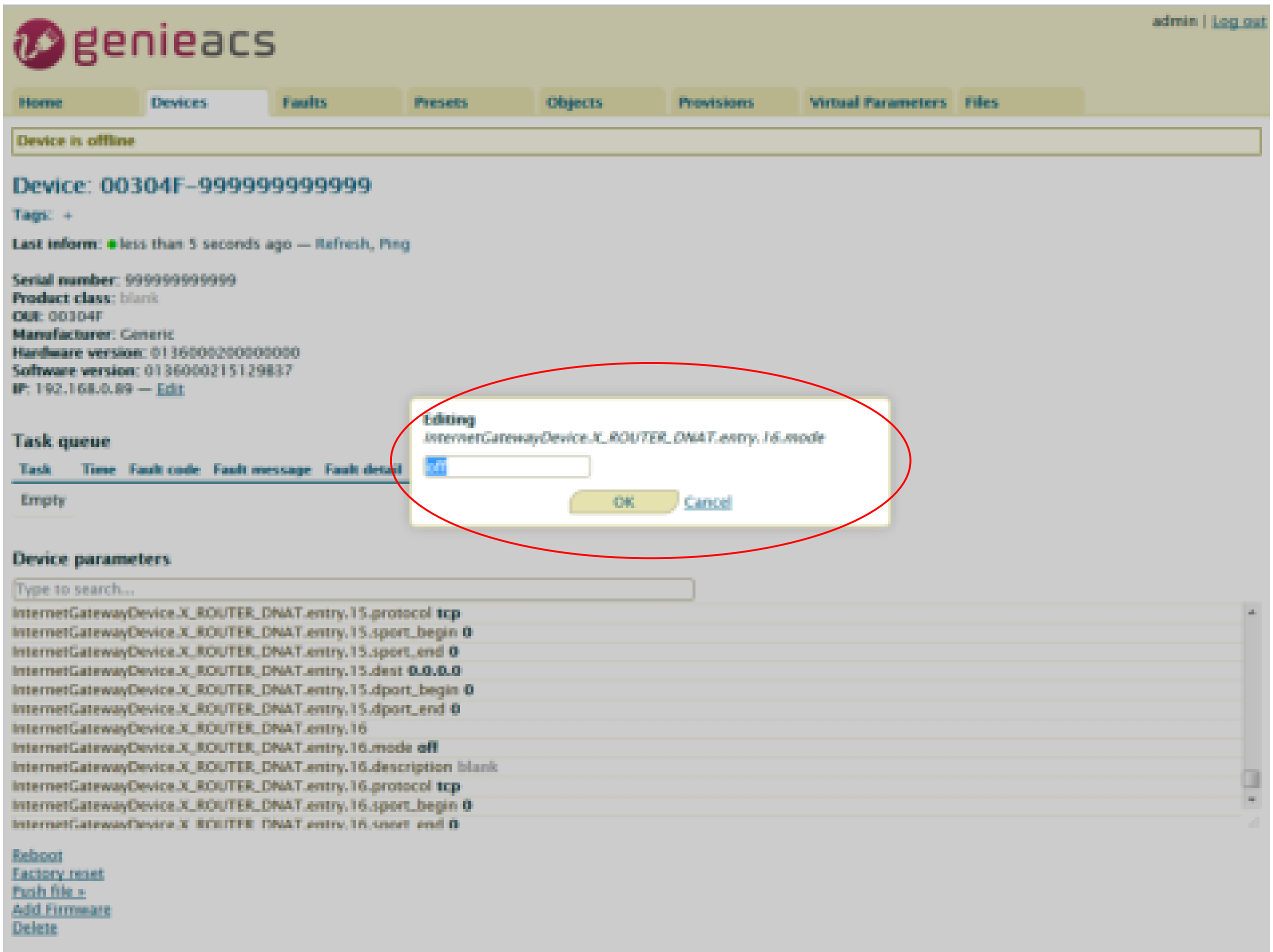
Note: *If the GenieACS can reach the device, the parameter value will be updated immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.*

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

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

4.2) Set parameter value

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



Device is offline

Device: 00304F-999999999999

Tags: +

Last inform: less than 5 seconds ago — Refresh, Ping

Serial number: 999999999999
Product class: blank
OUI: 00304F
Manufacturer: Generic
Hardware version: 0136000200000000
Software version: 0136000215129837
IP: 192.168.0.89 — Edit

Task queue

Task	Time	Fault code	Fault message	Fault detail
Empty				

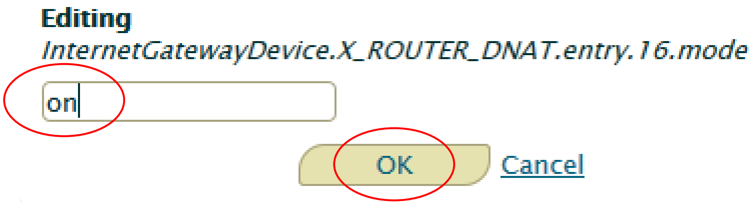
Editing
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.mode
off

Device parameters

Type to search...

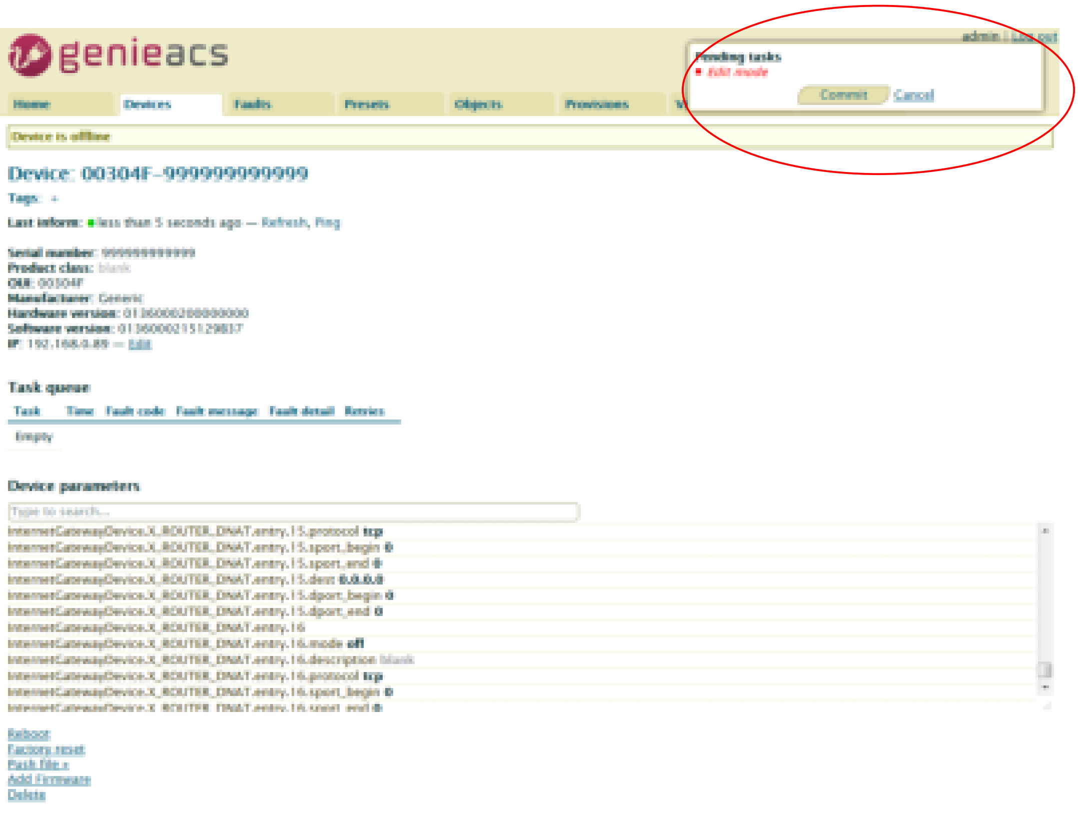
```
InternetGatewayDevice.X_ROUTER_DNAT.entry.15.protocol tcp
InternetGatewayDevice.X_ROUTER_DNAT.entry.15.sport_begin 0
InternetGatewayDevice.X_ROUTER_DNAT.entry.15.sport_end 0
InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dest 0.0.0.0
InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dport_begin 0
InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dport_end 0
InternetGatewayDevice.X_ROUTER_DNAT.entry.16
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.mode off
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.description blank
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.protocol tcp
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.sport_begin 0
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.sport_end 0
```

Input new value and press OK.



Editing
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.mode
on

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



Device is offline

Device: 00304F-999999999999

Tags: +

Last inform: less than 5 seconds ago — Refresh, Ping

Serial number: 999999999999
Product class: blank
OUI: 00304F
Manufacturer: Generic
Hardware version: 01360000200000000
Software version: 013600002151129837
IP: 192.168.0.89 — Edit

Task queue

Task	Time	Fault code	Fault message	Fault detail	Retries
Empty					

Device parameters

Type to search...

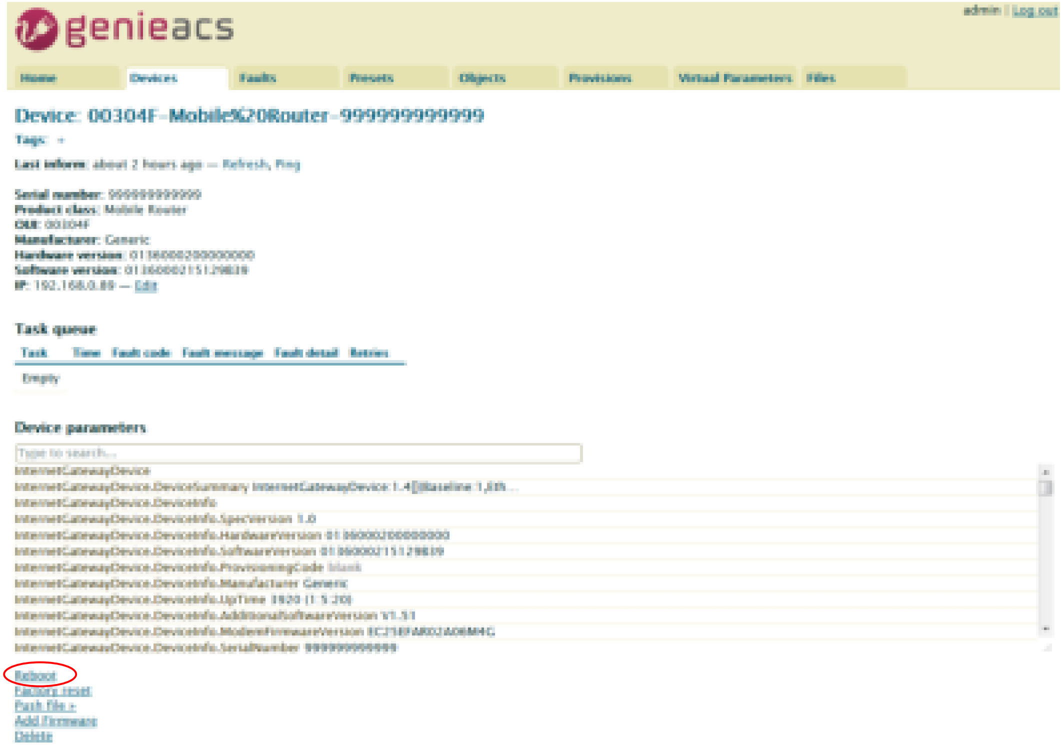
```
InternetGatewayDevice.X_ROUTER_DNAT.entry.15.protocol tcp
InternetGatewayDevice.X_ROUTER_DNAT.entry.15.sport_begin 0
InternetGatewayDevice.X_ROUTER_DNAT.entry.15.sport_end 0
InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dest 0.0.0.0
InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dport_begin 0
InternetGatewayDevice.X_ROUTER_DNAT.entry.15.dport_end 0
InternetGatewayDevice.X_ROUTER_DNAT.entry.16
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.mode off
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.description blank
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.protocol tcp
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.sport_begin 0
InternetGatewayDevice.X_ROUTER_DNAT.entry.16.sport_end 0
```

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.



Device: 00304F-Mobile%20Router-999999999999

Tags: +

Last inform: about 2 hours ago — Refresh, Ping

Serial number: 999999999999
Product class: Mobile Router
OUI: 00304F
Manufacturer: Generic
Hardware version: 01360000200000000
Software version: 013600002151129839
IP: 192.168.0.89 — Edit

Task queue

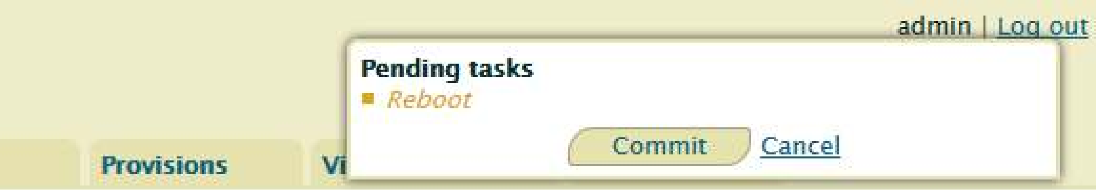
Task	Time	Fault code	Fault message	Fault detail	Retries
Empty					

Device parameters

Type to search...

```
InternetGatewayDevice
InternetGatewayDevice.DeviceSummary InternetGatewayDevice:1.4[](Baseline:1,Eth...
InternetGatewayDevice.DeviceInfo
InternetGatewayDevice.DeviceInfo.SpecVersion 1.0
InternetGatewayDevice.DeviceInfo.HardwareVersion 01360000200000000
InternetGatewayDevice.DeviceInfo.SoftwareVersion 013600002151129839
InternetGatewayDevice.DeviceInfo.ProvisioningCode blank
InternetGatewayDevice.DeviceInfo.Manufacturer Generic
InternetGatewayDevice.DeviceInfo.UpTime 1920 (1 5 20)
InternetGatewayDevice.DeviceInfo.AdditionalSoftwareVersion V1.31
InternetGatewayDevice.DeviceInfo.ModemFirmwareVersion EC21EFAR02A06M4G
InternetGatewayDevice.DeviceInfo.SerialNumber 999999999999
```

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.*

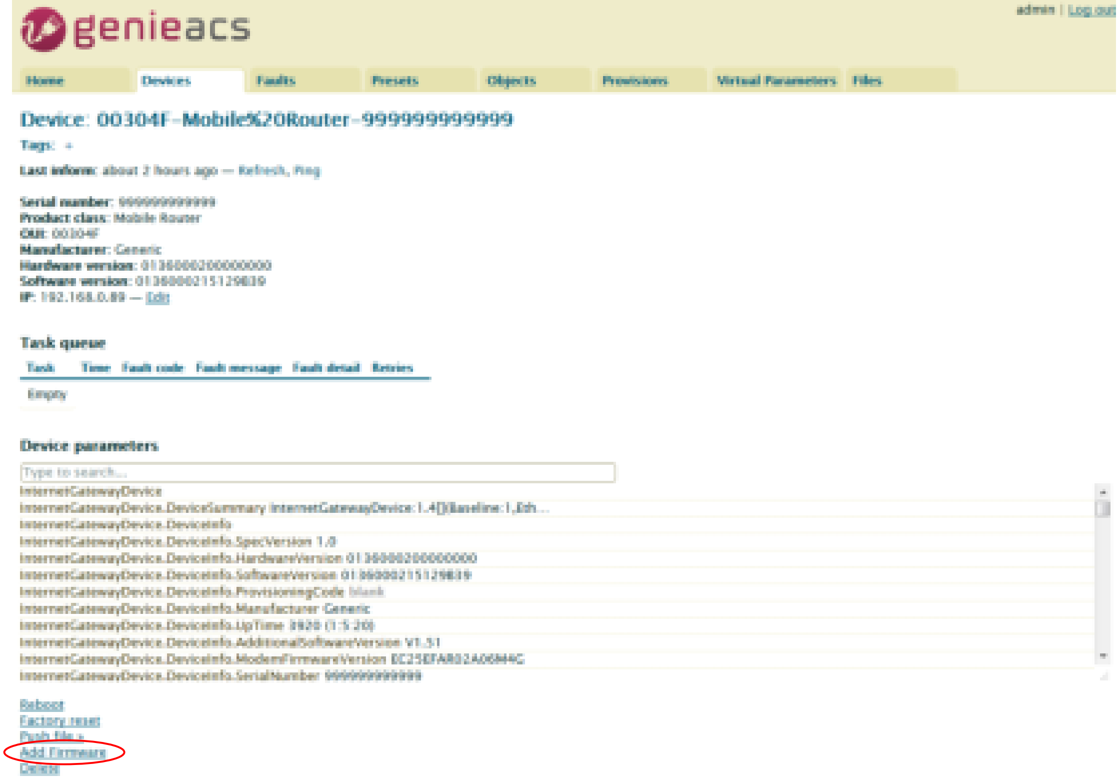
6) Reset to default

Similar to Reboot device except pressing on Factory reset link.

7) Firmware Upgrade

7.1) Upload Firmware

Press Add Firmware link



Device: 00304F-Mobile%20Router-999999999999

Tags: +

Last inform: about 2 hours ago — Refresh, Ping

Serial number: 999999999999
Product class: Mobile Router
OUI: 00304F
Manufacturer: Generic
Hardware version: 0136000200000000
Software version: 0136000215129839
IP: 192.168.0.89 — Edit

Task queue

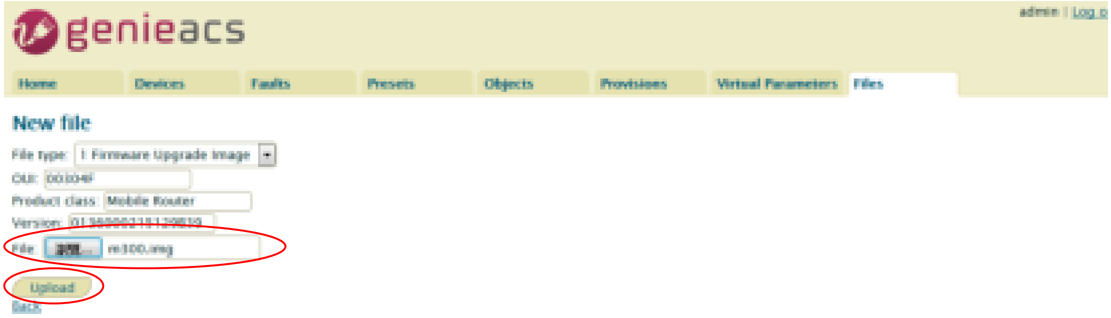
Task	Time	Fault code	Fault message	Fault detail	Retries
Empty					

Device parameters

Type to search...

```
InternetGatewayDevice
InternetGatewayDevice.DeviceSummary InternetGatewayDevice:1.4[](Baseline:1,Eth...
InternetGatewayDevice.DeviceInfo
InternetGatewayDevice.DeviceInfo.SpecVersion 1.0
InternetGatewayDevice.DeviceInfo.HardwareVersion 0136000200000000
InternetGatewayDevice.DeviceInfo.SoftwareVersion 0136000215129839
InternetGatewayDevice.DeviceInfo.ProvisioningCode blank
InternetGatewayDevice.DeviceInfo.Manufacturer Generic
InternetGatewayDevice.DeviceInfo.UpTime 3920 (1:5:20)
InternetGatewayDevice.DeviceInfo.AdditionalSoftwareVersion V1.31
InternetGatewayDevice.DeviceInfo.ModemFirmwareVersion EC25EFAR02A06M4G
InternetGatewayDevice.DeviceInfo.SerialNumber 999999999999
```

The link will redirect to Files tab



New file

File type: 1 Firmware Upgrade Image

OUI: 00304F

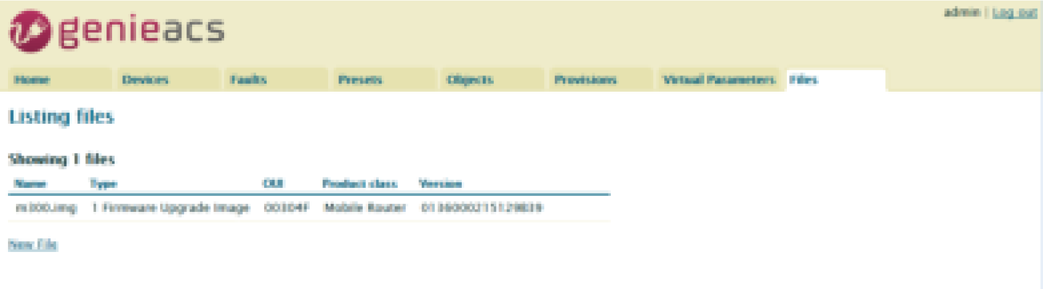
Product class: Mobile Router

Version: 0136000215129B39

File: m300.img

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

The firmware will be added to listing files as below.



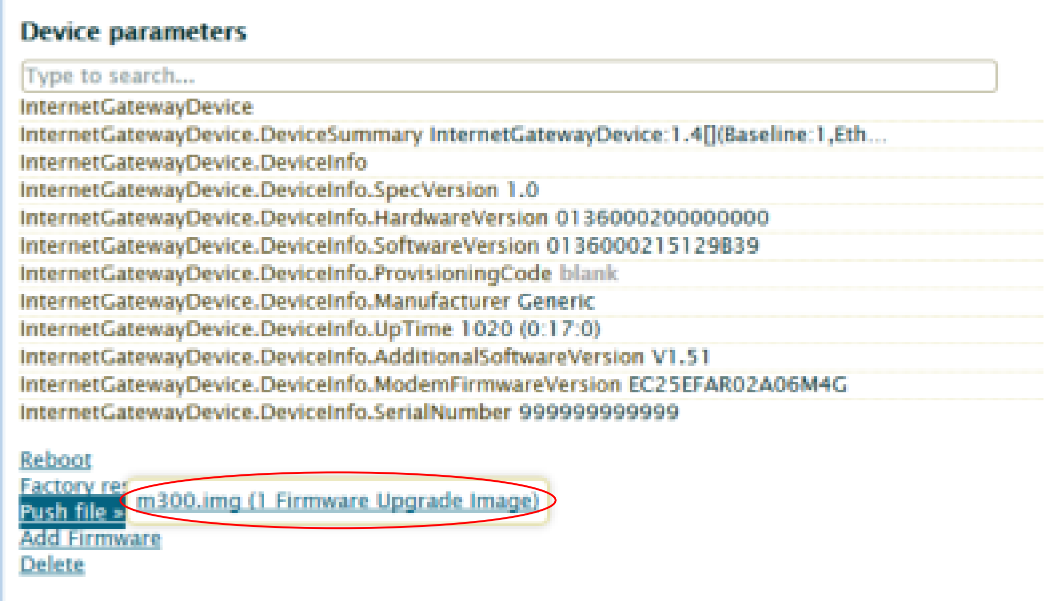
Listing files

Showing 1 files

Name	Type	OUI	Product class	Version
m300.img	1 Firmware Upgrade Image	00304F	Mobile Router	0136000215129B39

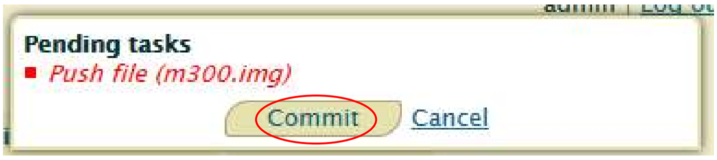
7.2) Upgrade

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


Device parameters

InternetGatewayDevice
InternetGatewayDevice.DeviceSummary InternetGatewayDevice:1.4[](Baseline:1,Eth...
InternetGatewayDevice.DeviceInfo
InternetGatewayDevice.DeviceInfo.SpecVersion 1.0
InternetGatewayDevice.DeviceInfo.HardwareVersion 0136000200000000
InternetGatewayDevice.DeviceInfo.SoftwareVersion 0136000215129B39
InternetGatewayDevice.DeviceInfo.ProvisioningCode blank
InternetGatewayDevice.DeviceInfo.Manufacturer Generic
InternetGatewayDevice.DeviceInfo.UpTime 1020 (0:17:0)
InternetGatewayDevice.DeviceInfo.AdditionalSoftwareVersion V1.51
InternetGatewayDevice.DeviceInfo.ModemFirmwareVersion EC25EFAR02A06M4G
InternetGatewayDevice.DeviceInfo.SerialNumber 999999999999

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.


Pending tasks

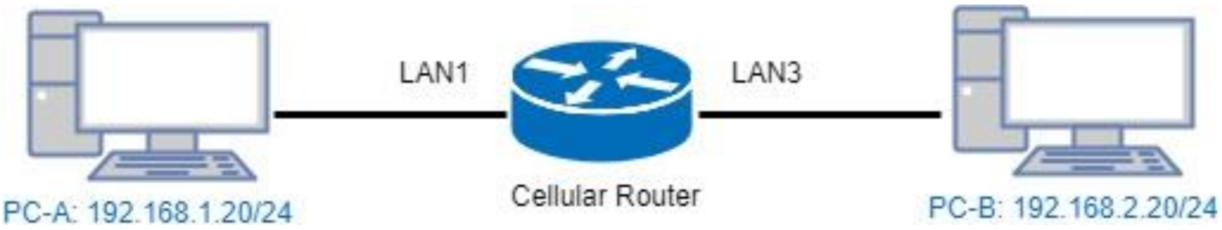
- *Push file (m300.img)*

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

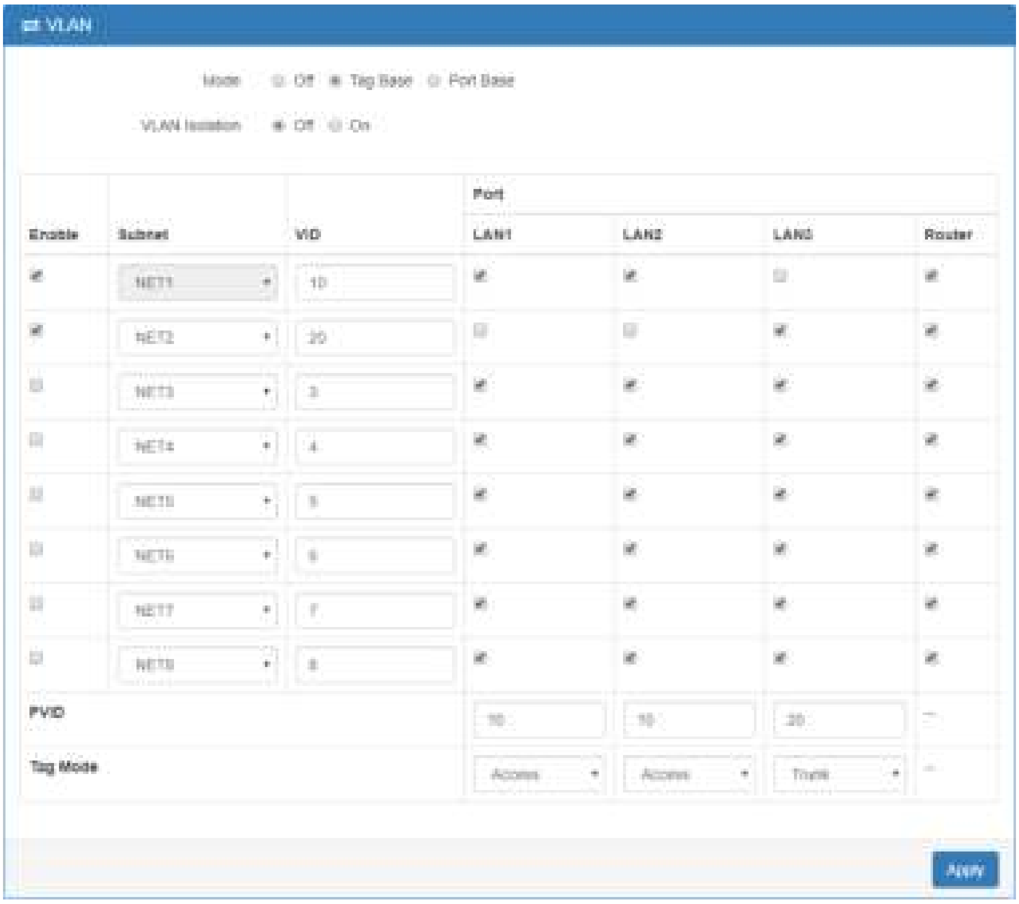
(1) PC-A sends ICMP packet to PC-B IP (192.168.2.20) and captures traffic on PC-B. Thus, PC-B will receive Tag20 traffic.

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

Note:

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

The following interface shows VLAN settings for the cellular router.



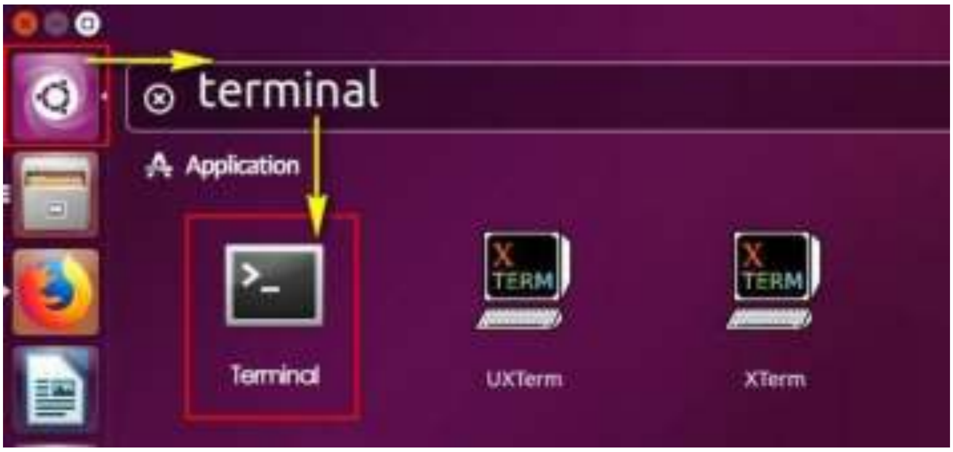
Mode ○ Off ● Tag Base ○ Port Base

VLAN Isolation ● Off ○ On

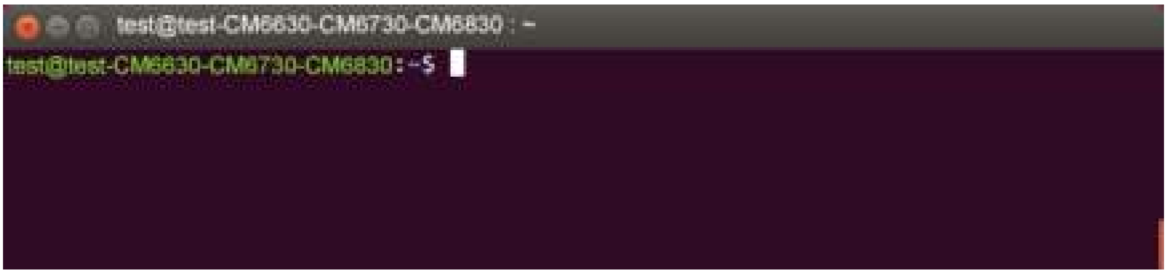
			Port			
Enable	Subnet	VID	LAN1	LAN2	LAN3	Router
☑	NET1	10	☑	☑	□	☑
☑	NET2	20	□	□	☑	☑
□	NET3	3	☑	☑	☑	☑
□	NET4	4	☑	☑	☑	☑
□	NET5	5	☑	☑	☑	☑
□	NET6	6	☑	☑	☑	☑
□	NET7	7	☑	☑	☑	☑
□	NET8	8	☑	☑	☑	☑
PVID			10	10	20	–
Tag Mode			Access	Access	Trunk	–

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.

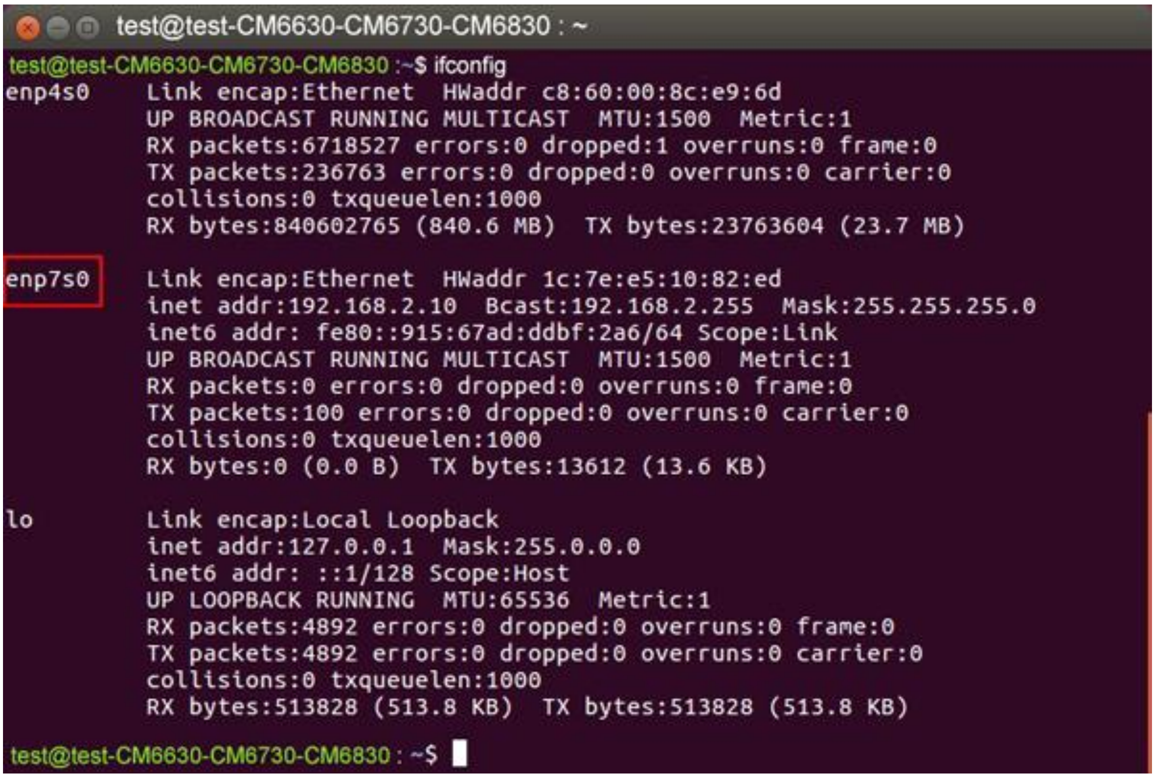


    - Next, it shows the information when you click *the terminal icon*.



```
test@test-CM6630-CM6730-CM6830 : ~
test@test-CM6630-CM6730-CM6830:~$ 
```

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



```
test@test-CM6630-CM6730-CM6830 : ~
test@test-CM6630-CM6730-CM6830 :~$ ifconfig
enp4s0    Link encap:Ethernet  HWaddr c8:60:00:8c:e9:6d
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6718527 errors:0 dropped:1 overruns:0 frame:0
          TX packets:236763 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:840602765 (840.6 MB)  TX bytes:23763604 (23.7 MB)

enp7s0    Link encap:Ethernet  HWaddr 1c:7e:e5:10:82:ed
          inet addr:192.168.2.10  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::915:67ad:ddbf:2a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:13612 (13.6 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4892 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4892 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:513828 (513.8 KB)  TX bytes:513828 (513.8 KB)

test@test-CM6630-CM6730-CM6830 : ~$ 
```

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.

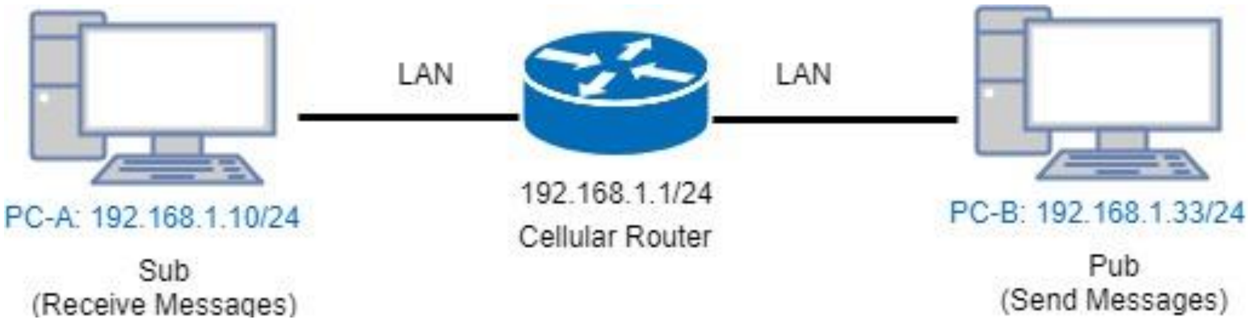
Example 2: PC-A ping PC-B (Trunk to Access)

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.

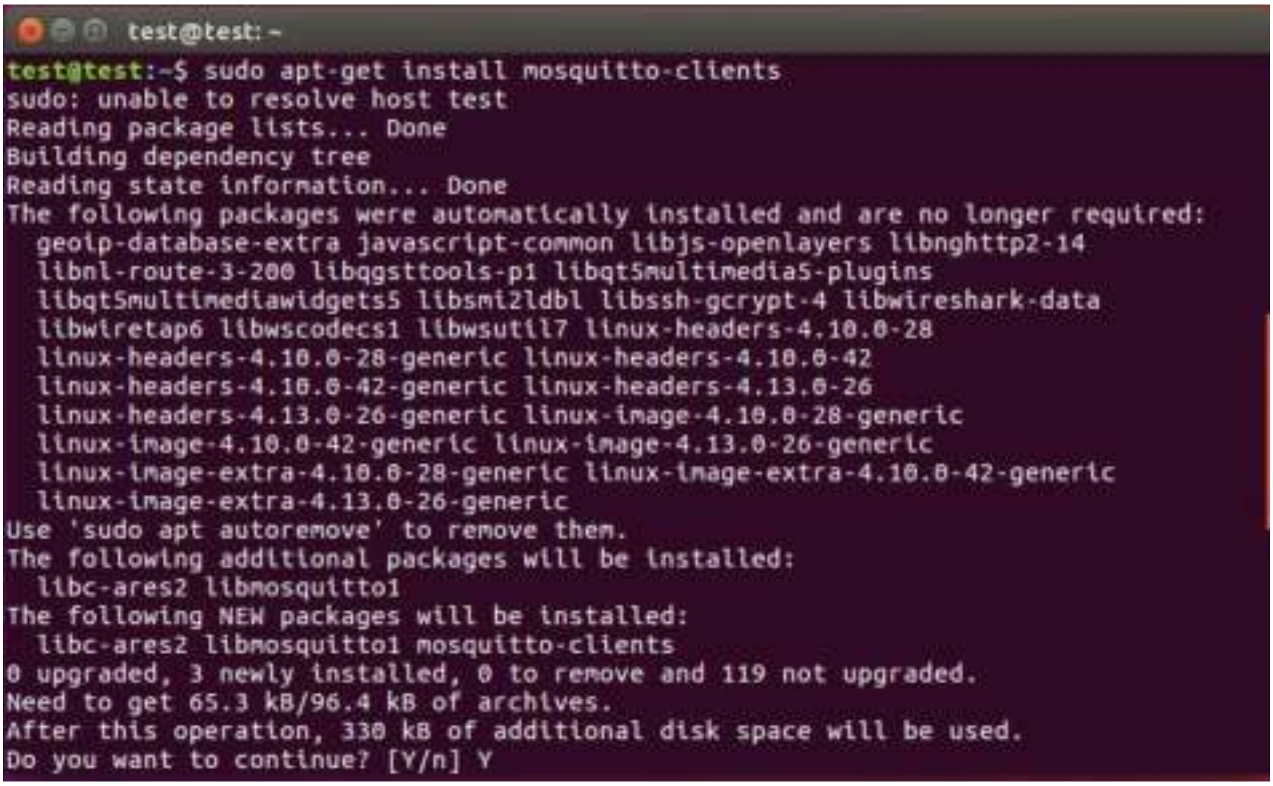
(2) PC-B sends message to PC-A and PC-A should receive message.

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

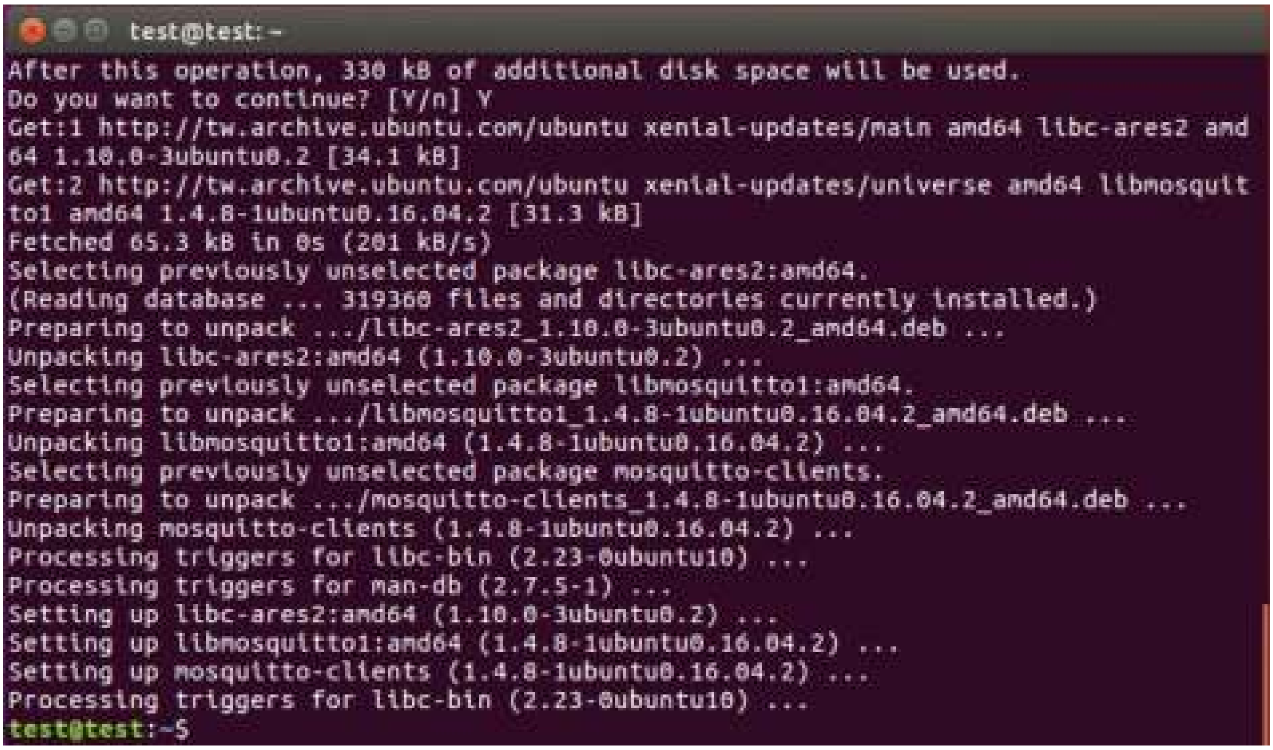
There is a process to explain the steps and result.

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

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



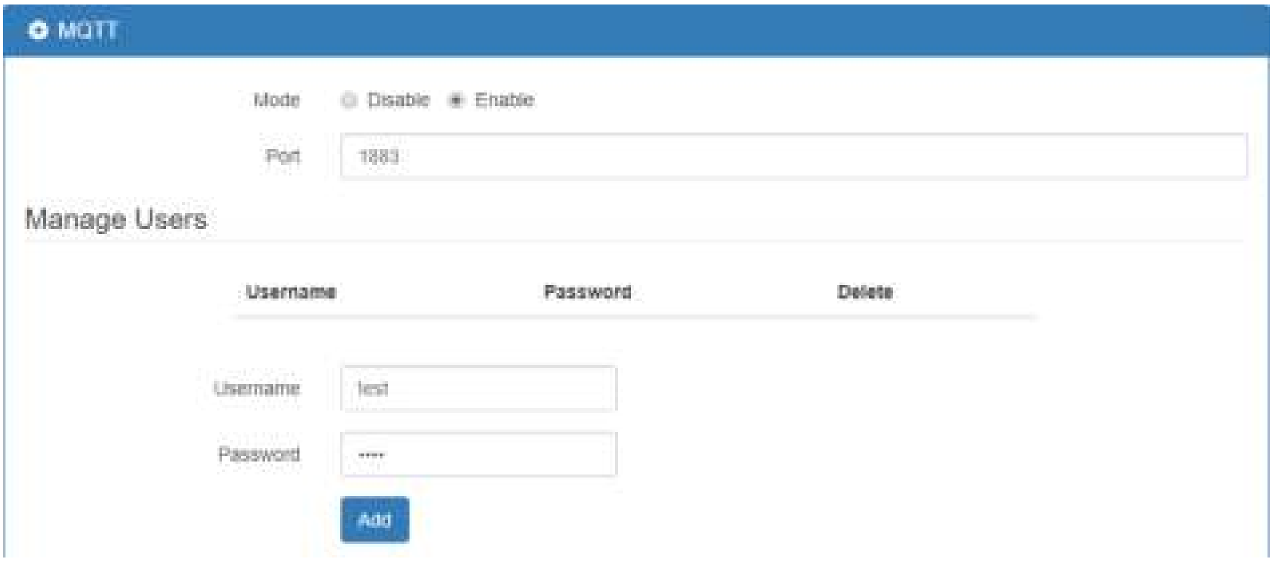
```
test@test:~$ sudo apt-get install mosquitto-clients
sudo: unable to resolve host test
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  geoip-database-extra javascript-common libjs-openlayers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



MQTT

Mode ○ Disable ● Enable

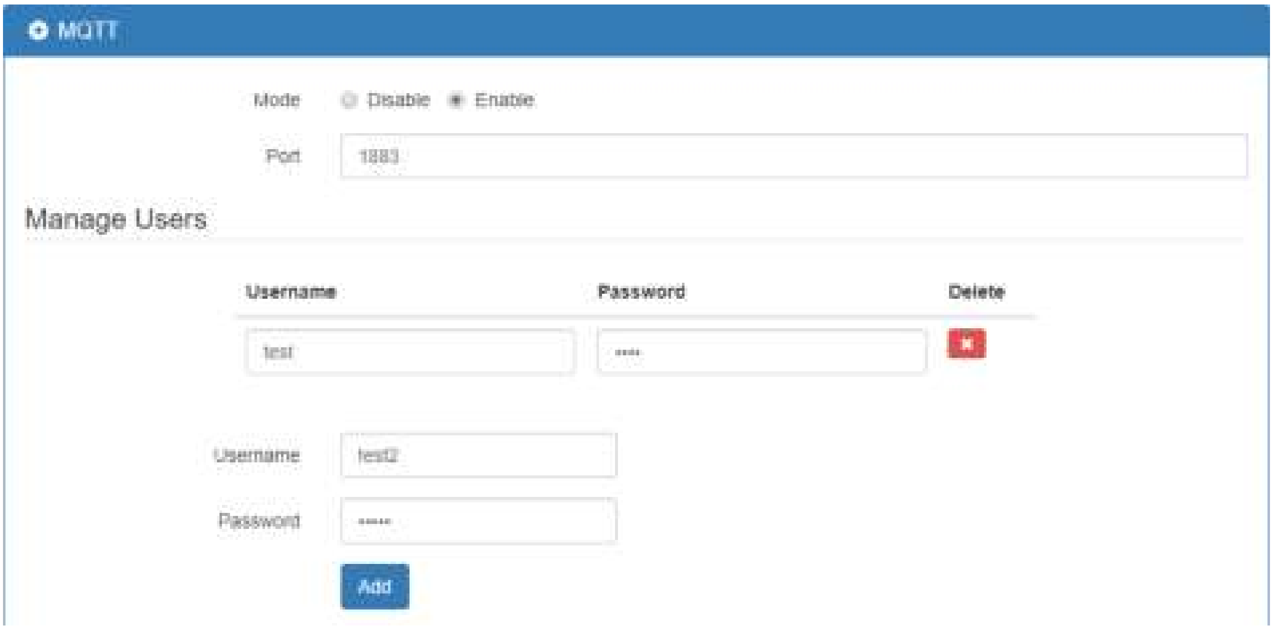
Port 1883

Manage Users

Username	Password	Delete

Username test

Password ••••



MQTT

Mode ○ Disable ● Enable

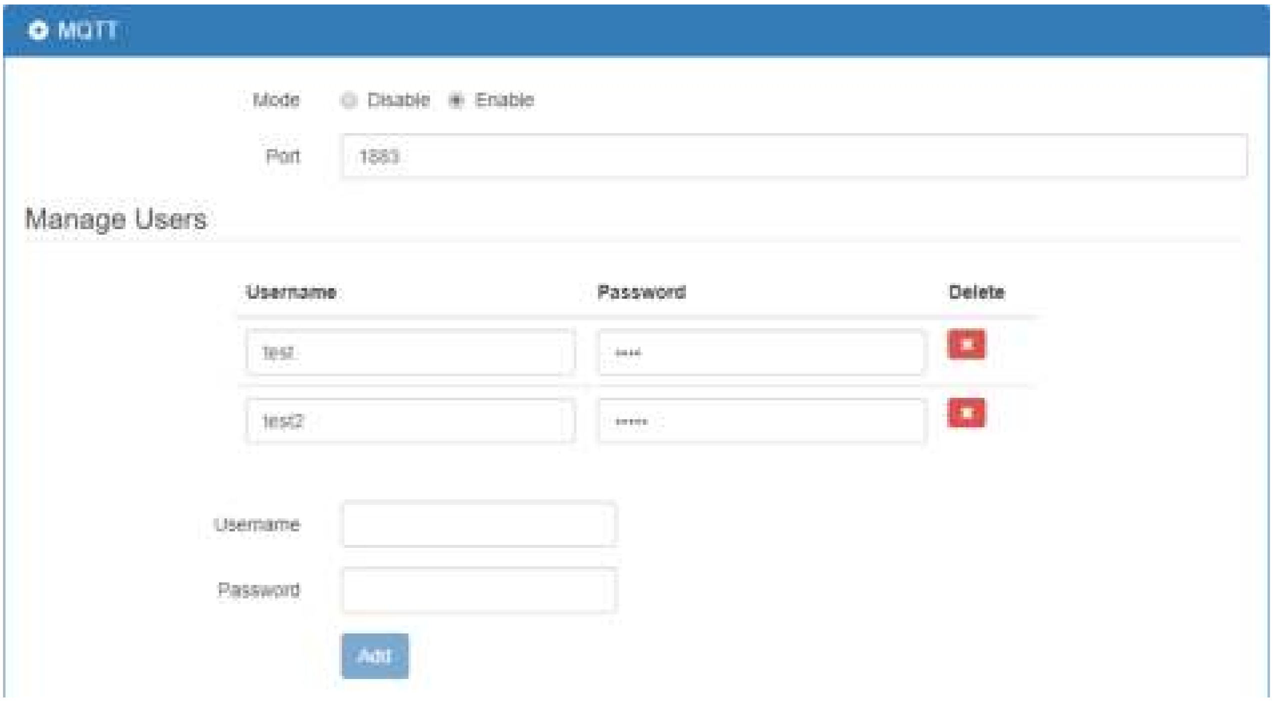
Port 1883

Manage Users

Username	Password	Delete
test	••••	✖

Username test2

Password •••••



MQTT

Mode ○ Disable ● Enable

Port 1883

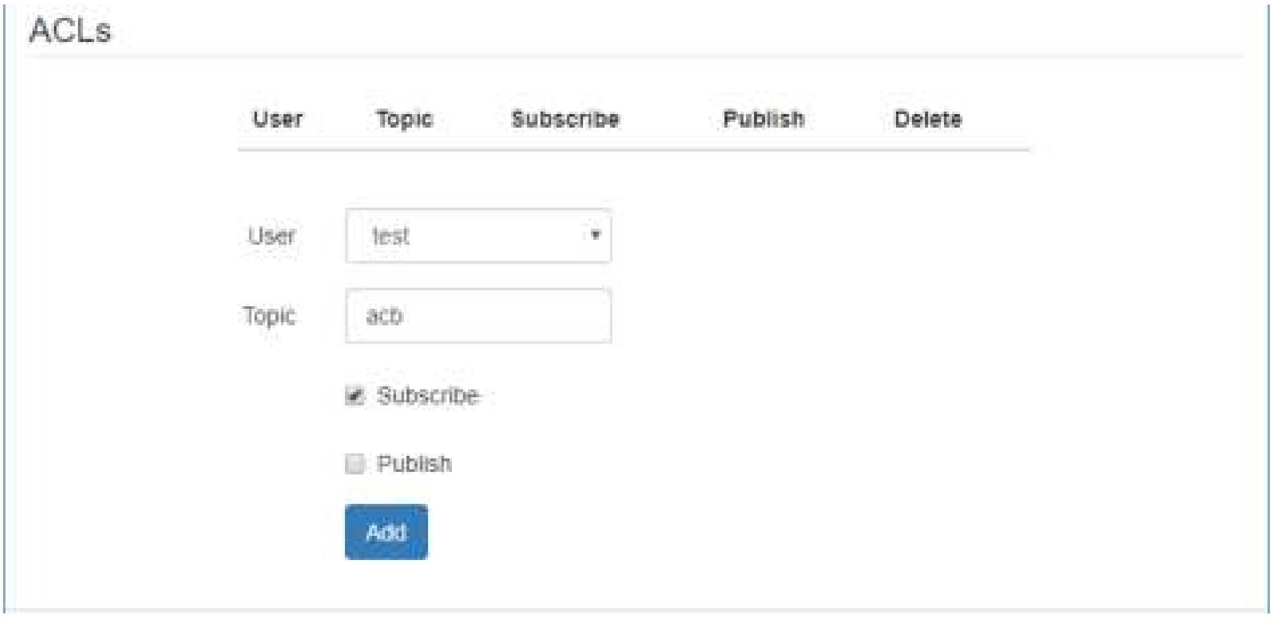
Manage Users

Username	Password	Delete
test	••••	✖
test2	•••••	✖

Username

Password

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



ACLs

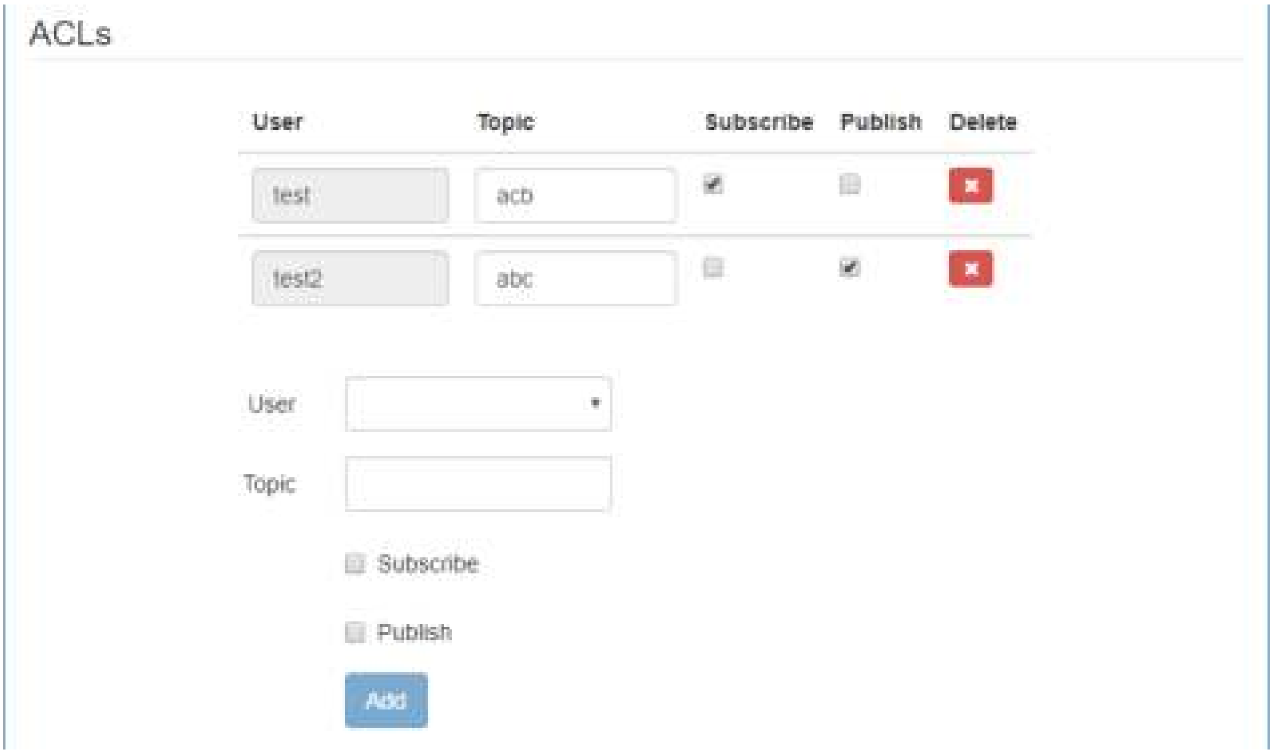
User	Topic	Subscribe	Publish	Delete

User test

Topic acb

☑ Subscribe

□ Publish



ACLs

User	Topic	Subscribe	Publish	Delete
test	acb	☑	□	✖
test2	abc	□	☑	✖

User

Topic

□ Subscribe

□ Publish

Note:

- For Receive message command format:

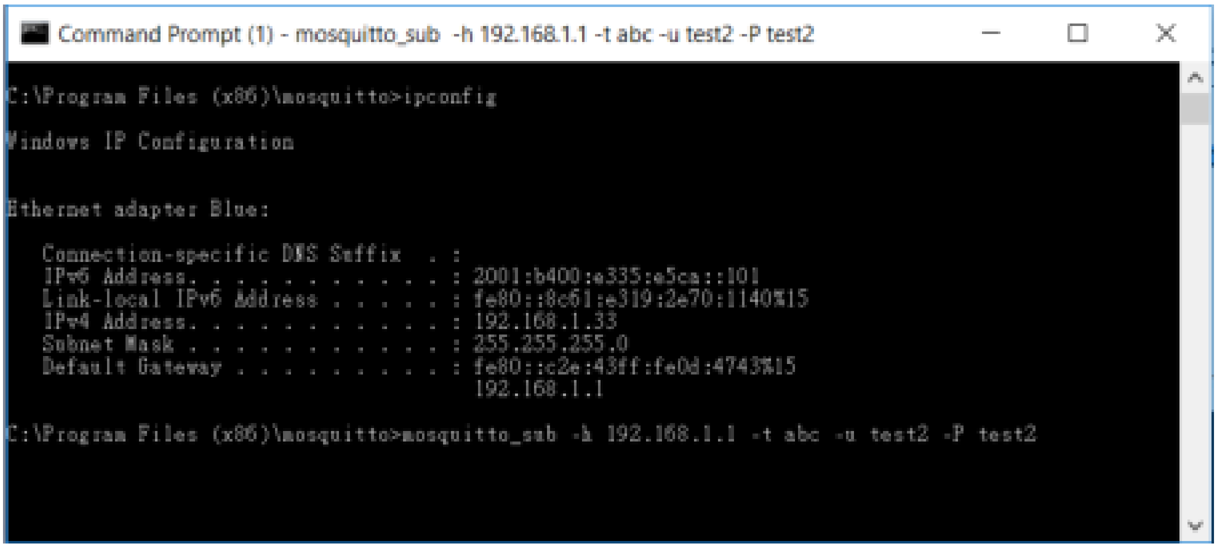
  Mosquitto_sub -h <M300 IP> -t <Topic> -u <username> -P <password>
- For Send message command format:

  Mosquitto_pub -h <M300 IP> -t <Topic> -u <username> -P <password> -m <message>

- Step3: There are two test MQTT examples.

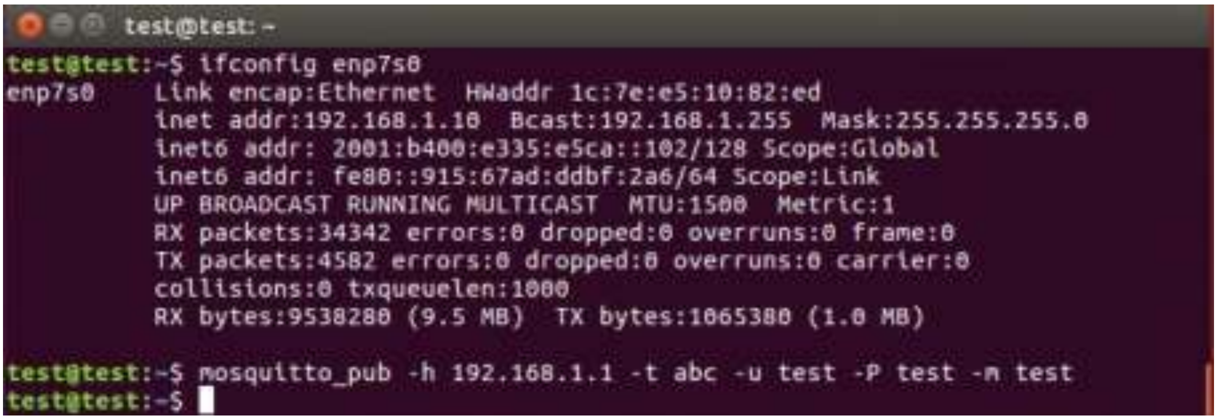
Example 1: PC-A sends message to PC-B and PC-B should not receive any message.

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

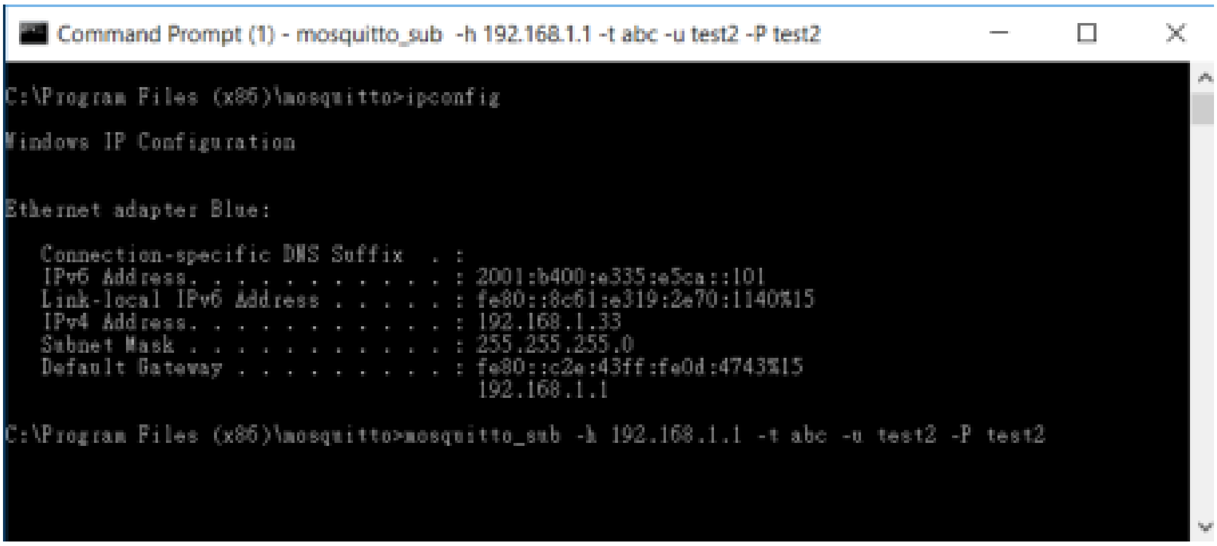

Command Prompt (1) - mosquitto_sub -h 192.168.1.1 -t abc -u test2 -P test2

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

Windows IP Configuration


Ethernet adapter Blue:

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

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

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



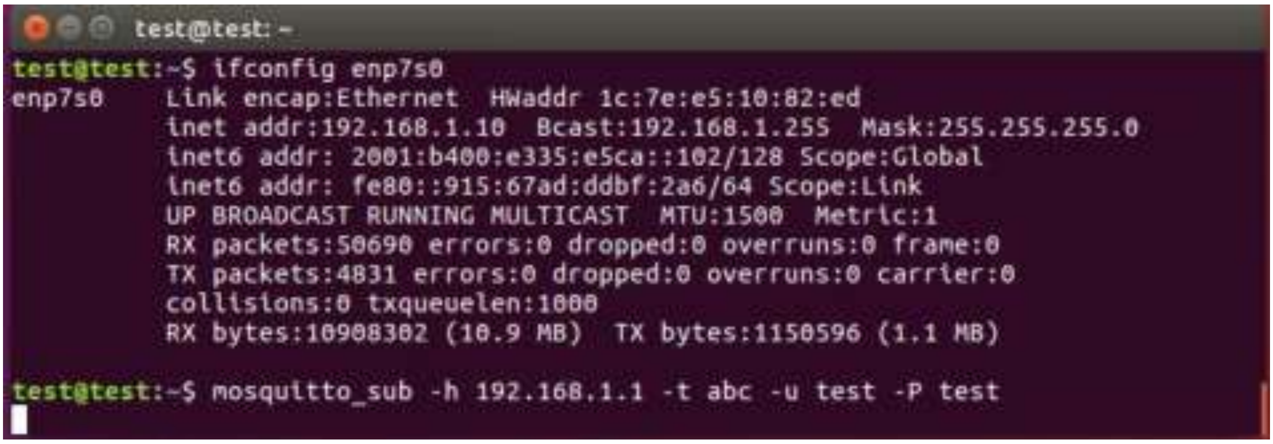
```
test@test:~$ ifconfig enp7s0
enp7s0    Link encap:Ethernet  HWaddr 1c:7e:e5:10:82:ed
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b400:e335:e5ca::102/128 Scope:Global
          inet6 addr: fe80::915:67ad:ddbf:2a6/64 Scope:Link
          UP BROADCAST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

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


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

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

Windows IP Configuration


Ethernet adapter Blue:

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

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

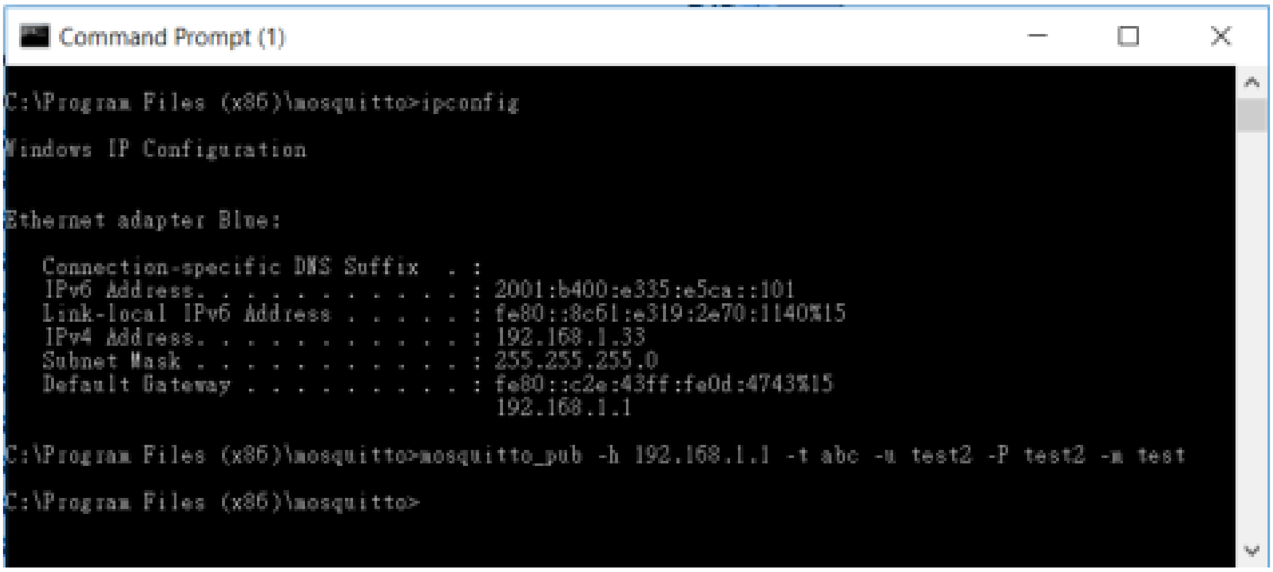
Example 2: PC-B sends message to PC-A and PC-A should receive message.

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

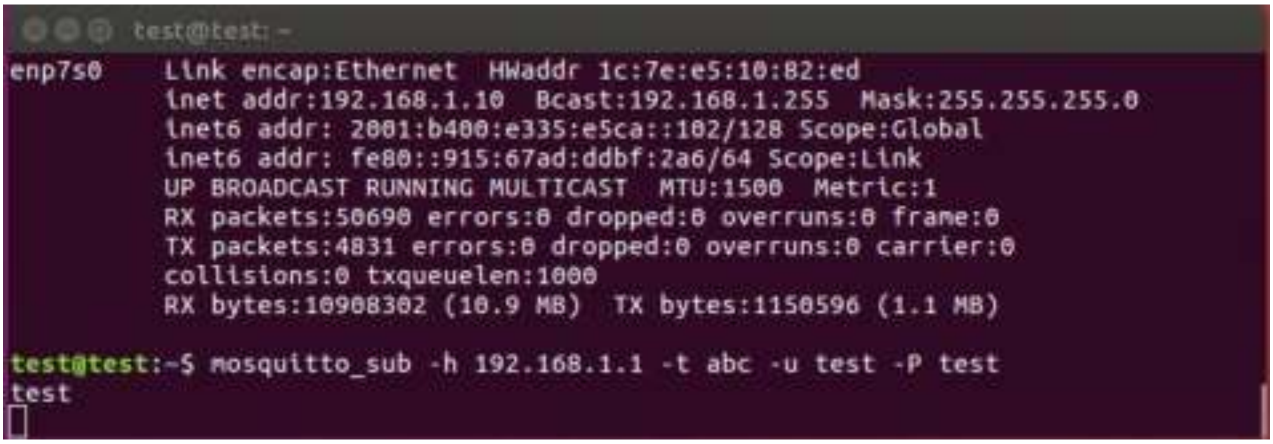


```
test@test:~$ ifconfig enp7s0
enp7s0    Link encap:Ethernet  HWaddr 1c:7e:e5:10:82:ed
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b400:e335:e5ca::102/128 Scope:Global
          inet6 addr: fe80::915:67ad:ddbf:2a6/64 Scope:Link
          UP BROADCAST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



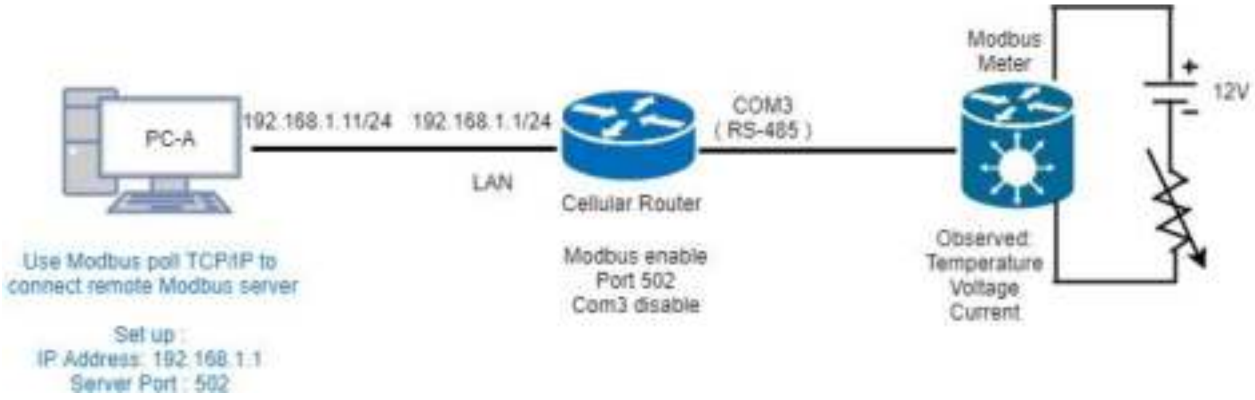
```
C:\Program Files (x86)\mosquitto>ipconfig

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>
```



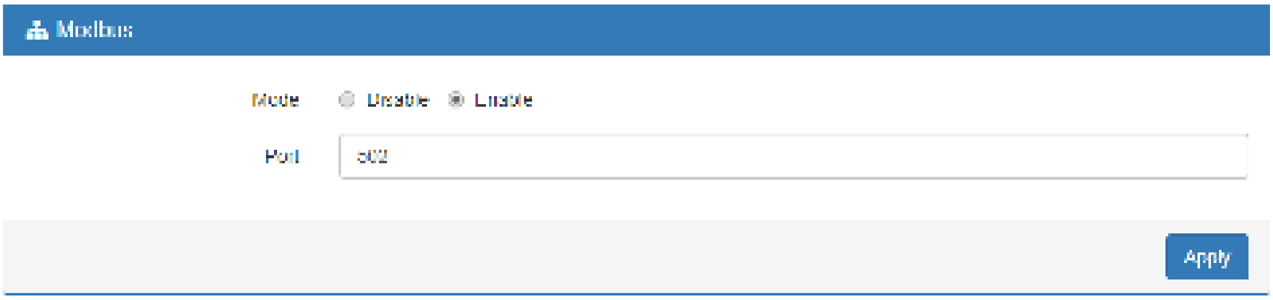
```
enp7s0    Link encap:Ethernet  HWaddr 1c:7e:e5:10:82:ed
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b400:e335:e5ca::102/128 Scope:Global
          inet6 addr: fe80::915:67ad:ddbf:2a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  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 Modbus Topology

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



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

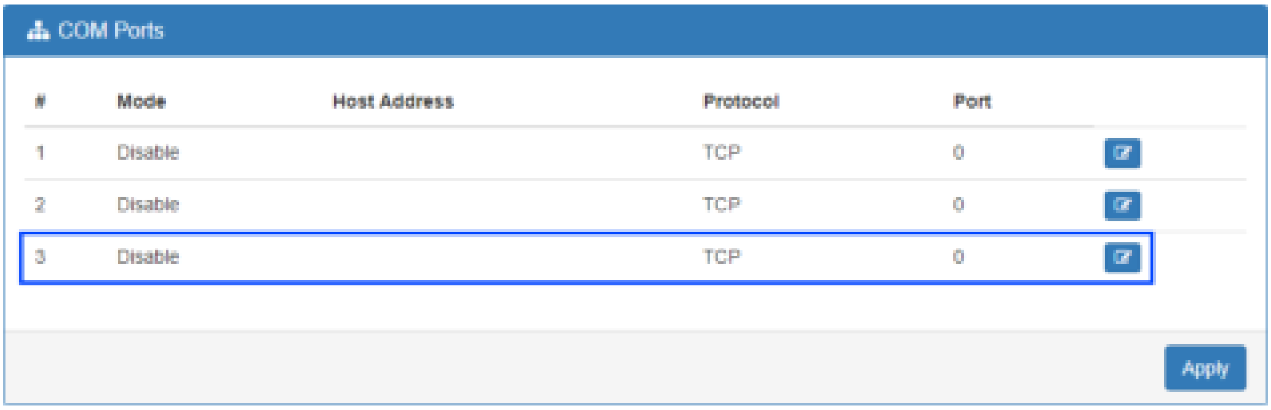


Modbus

Mode ○ Disable ● Enable

Port 502

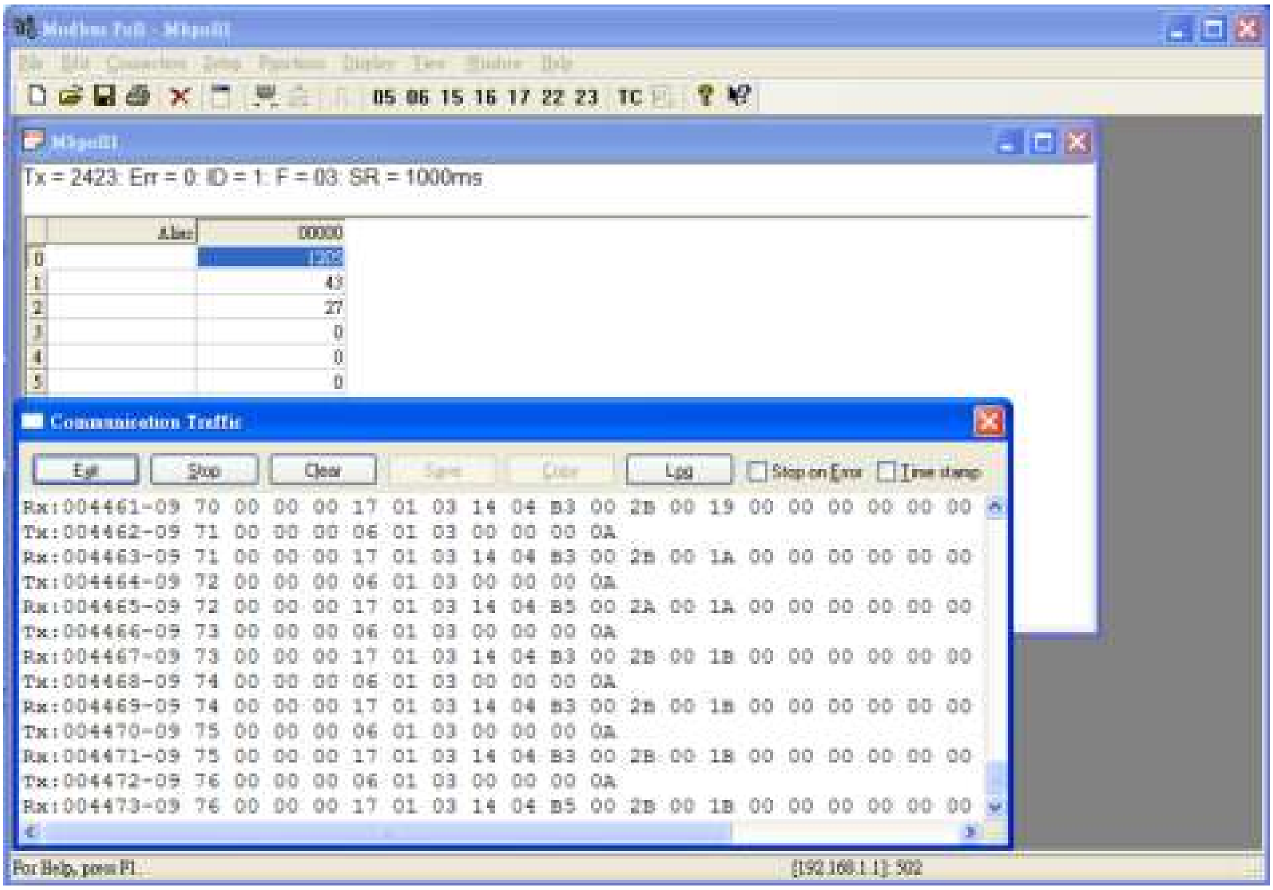
Please confirm the interface of COM Port 3 that the mode is Disable.



COM Ports

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

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



Tx = 2423: Err = 0: ID = 1: F = 03: SR = 1000ms

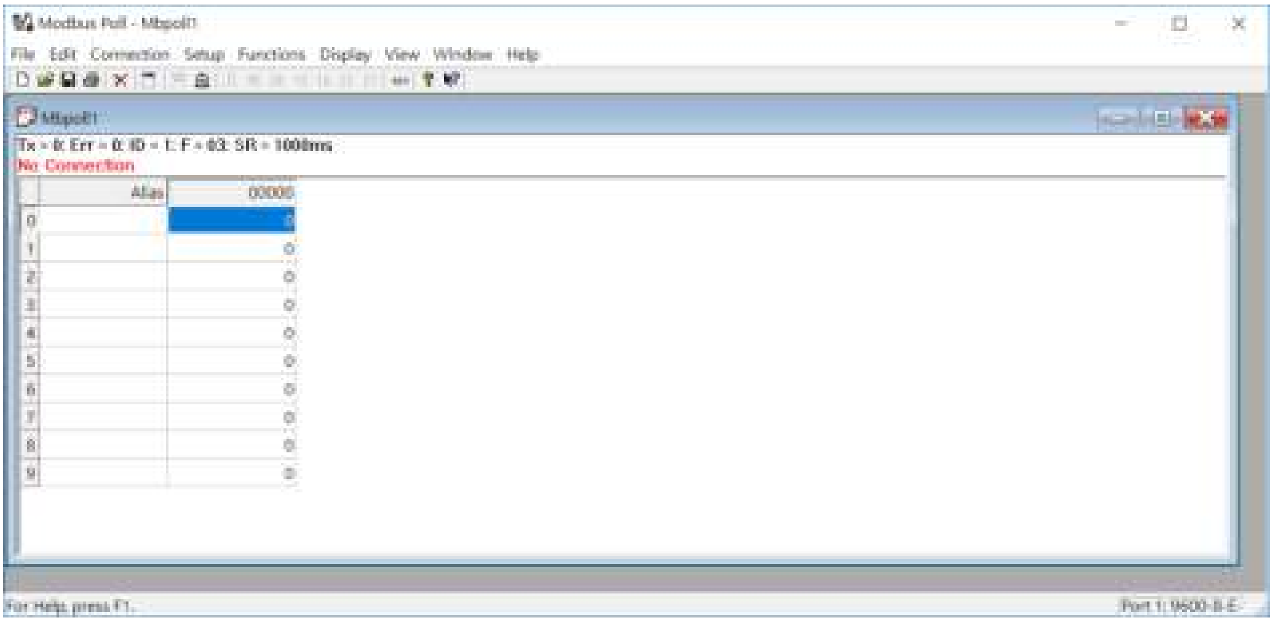
	Alias	00000
0		1202
1		43
2		27
3		0
4		0
5		0

```
Rx:004461-09 70 00 00 00 17 01 03 14 04 B3 00 2B 00 19 00 00 00 00 00 00
Tx:004462-09 71 00 00 00 06 01 03 00 00 00 0A
Rx:004463-09 71 00 00 00 17 01 03 14 04 B3 00 2B 00 1A 00 00 00 00 00 00
Tx:004464-09 72 00 00 00 06 01 03 00 00 00 0A
Rx:004465-09 72 00 00 00 17 01 03 14 04 B5 00 2A 00 1A 00 00 00 00 00 00
Tx:004466-09 73 00 00 00 06 01 03 00 00 00 0A
Rx:004467-09 73 00 00 00 17 01 03 14 04 B3 00 2B 00 1B 00 00 00 00 00 00
Tx:004468-09 74 00 00 00 06 01 03 00 00 00 0A
Rx:004469-09 74 00 00 00 17 01 03 14 04 B3 00 2B 00 1B 00 00 00 00 00 00
Tx:004470-09 75 00 00 00 06 01 03 00 00 00 0A
Rx:004471-09 75 00 00 00 17 01 03 14 04 B3 00 2B 00 1B 00 00 00 00 00 00
Tx:004472-09 76 00 00 00 06 01 03 00 00 00 0A
Rx:004473-09 76 00 00 00 17 01 03 14 04 B5 00 2B 00 1B 00 00 00 00 00 00
```

Note 1:

- There is a reference for Modbus poll software to download and install on PC.

  http://www.tucows.com/preview/502459/Modbus-Poll



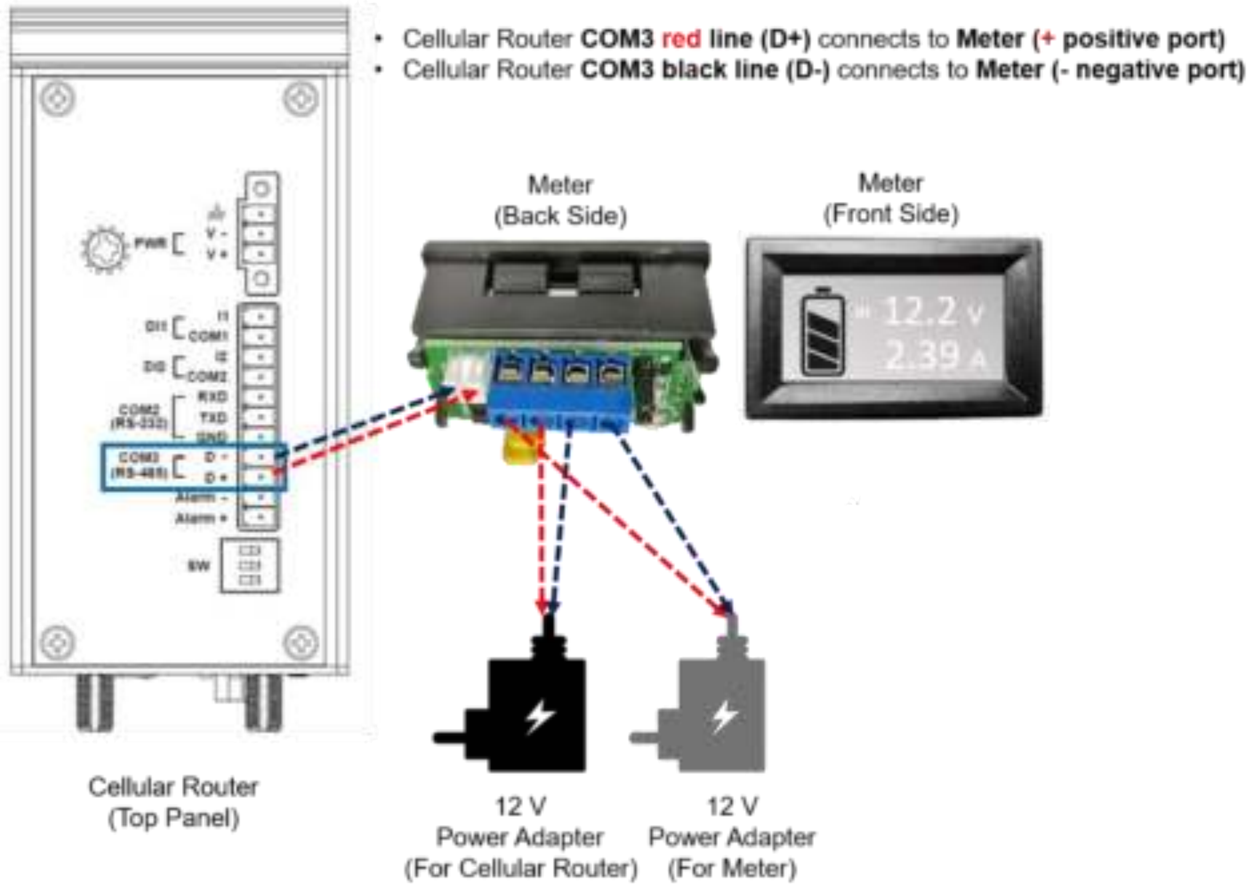
Tx = 0: Err = 0: ID = 1: F = 03: SR = 1000ms
No Connection

	Alias	00000
0		0
1		0
2		0
3		0
4		0
5		0
6		0
7		0
8		0
9		0

Note 2:

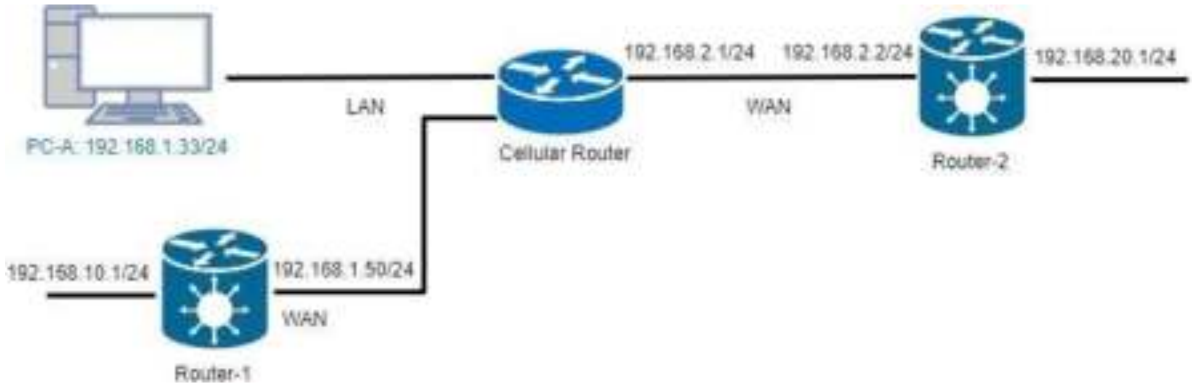
- You can purchase a meter of DC voltage and current supporting Modbus protocol with RS-485 serial for test and connection to COM Port 3.

- The following picture shows how connect the ports and the lines between a cellular router and a meter.



- Cellular Router **COM3 red line (D+)** connects to **Meter (+ positive port)**
- Cellular Router **COM3 black line (D-)** connects to **Meter (- negative port)**

17.4 IP Routing Topology



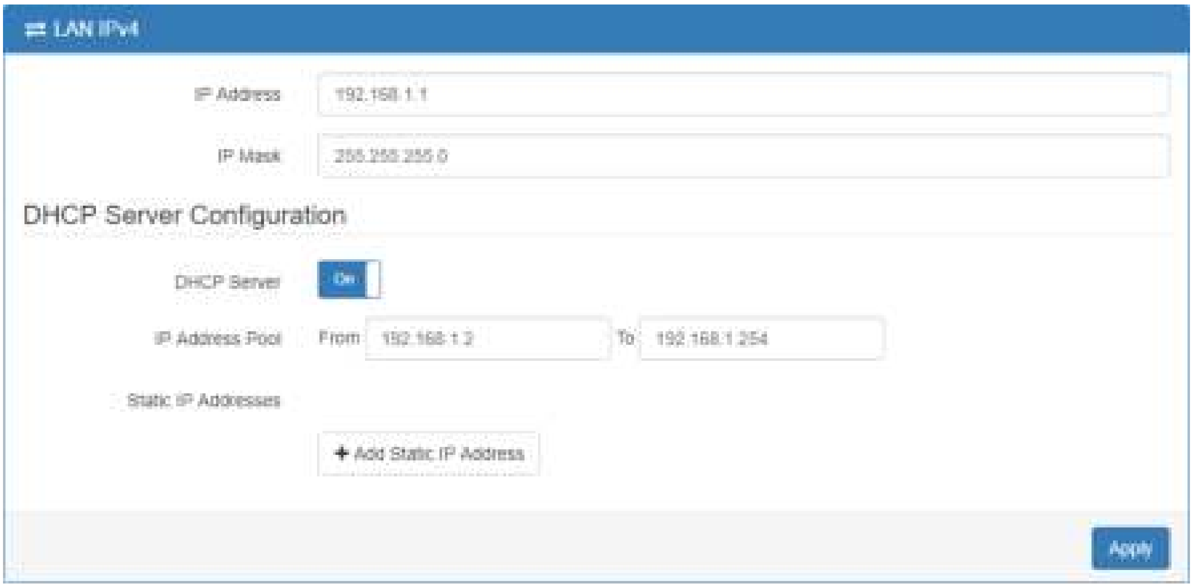
This IP Routing topology that the cellular router connects Router-1 and Router-2 will have two results.

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

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

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

- LAN configuration:



LAN IPv4

IP Address: 192.168.1.1

IP Mask: 255.255.255.0

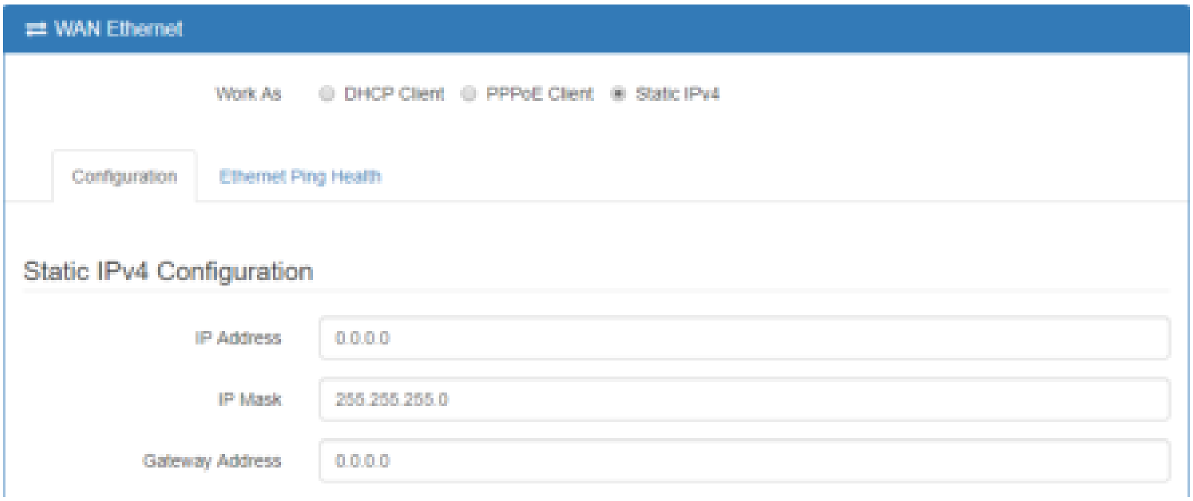
DHCP Server Configuration

DHCP Server: On

IP Address Pool: From 192.168.1.2 To 192.168.1.254

Static IP Addresses

- WAN configuration:



WAN Ethernet

Work As: ○ DHCP Client ○ PPPoE Client ● Static IPv4

Static IPv4 Configuration

IP Address: 0.0.0.0

IP Mask: 255.255.255.0

Gateway Address: 0.0.0.0

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

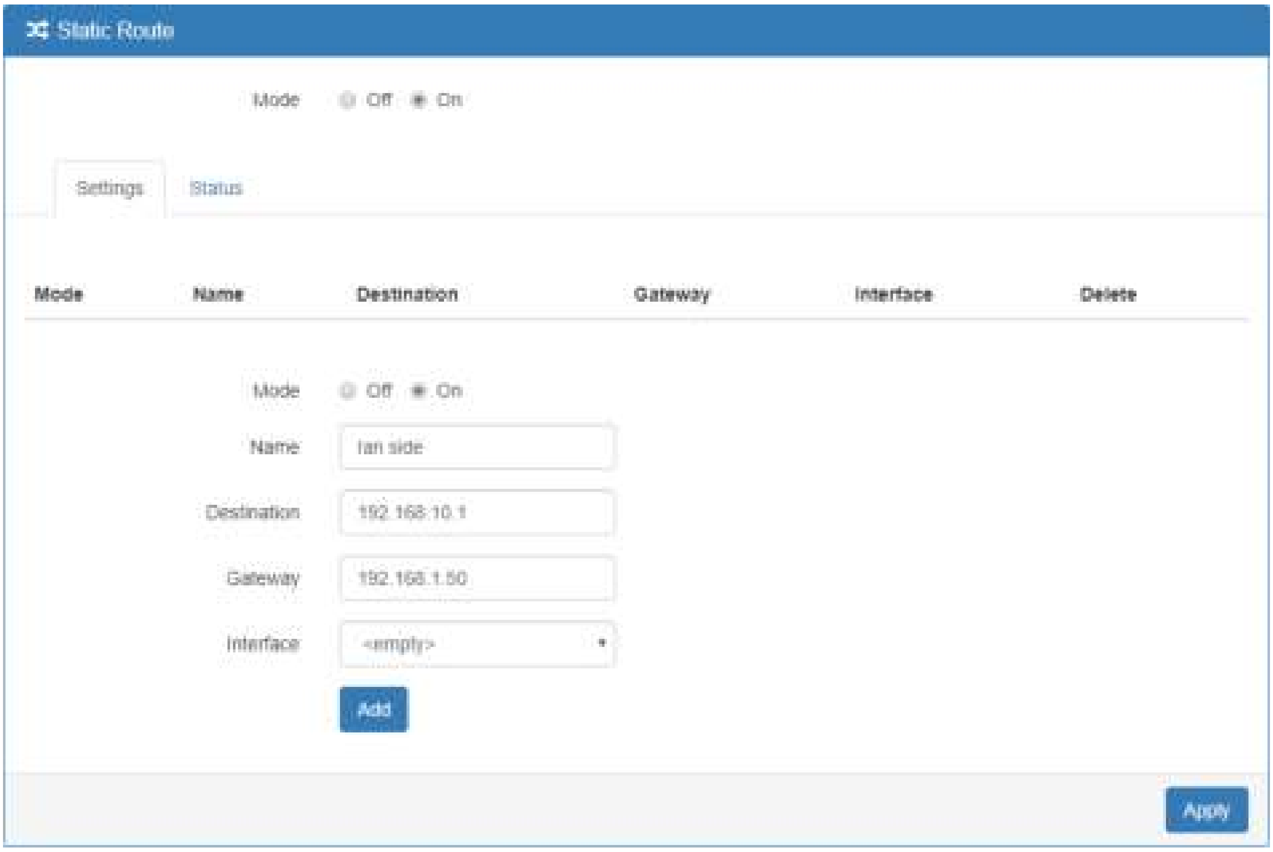
Example 1: Add IP Routing on LAN interface

- 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



Mode ○ Off ● On

Mode	Name	Destination	Gateway	Interface	Delete

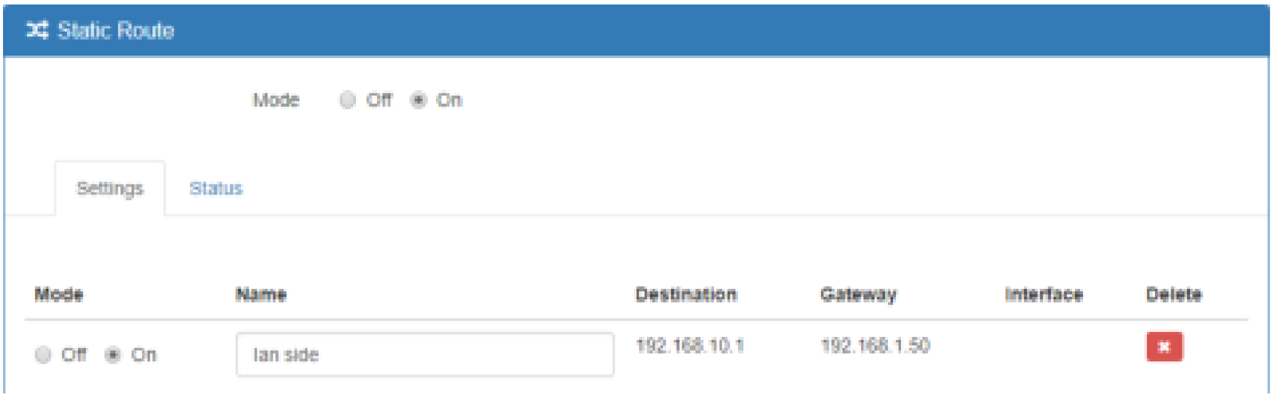
Mode ○ Off ● On

Name: lan side

Destination: 192.168.10.1

Gateway: 192.168.1.50

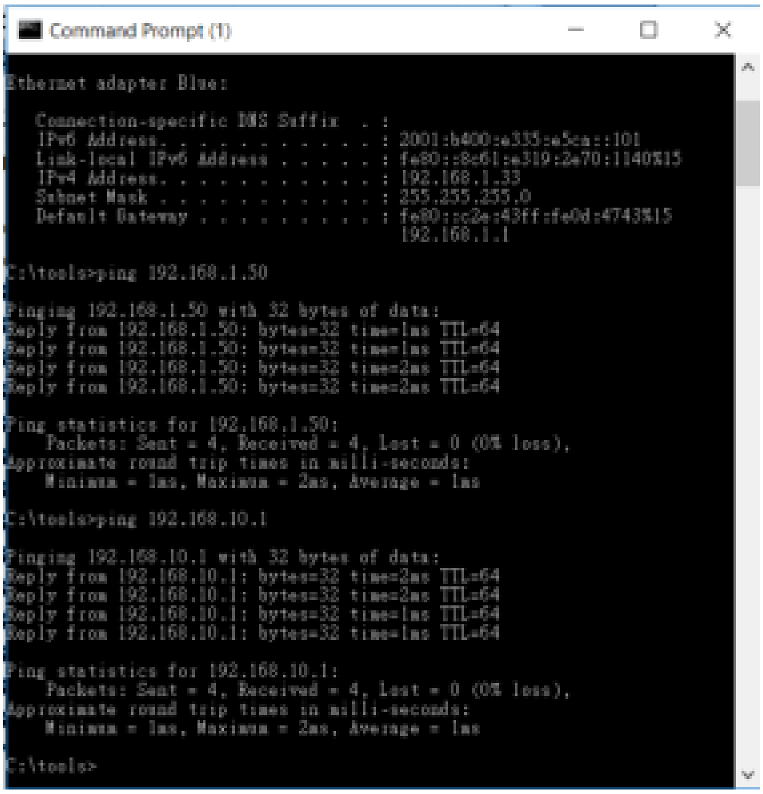
Interface: <empty>



Mode ○ Off ● On

Mode	Name	Destination	Gateway	Interface	Delete
○ Off ● On	lan side	192.168.10.1	192.168.1.50		✖

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



Command Prompt (1)

```
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:\tools>ping 192.168.1.50

Pinging 192.168.1.50 with 32 bytes of data:
Reply from 192.168.1.50: bytes=32 time=1ms TTL=64
Reply from 192.168.1.50: bytes=32 time=1ms TTL=64
Reply from 192.168.1.50: bytes=32 time=2ms TTL=64
Reply from 192.168.1.50: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\tools>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time=2ms TTL=64
Reply from 192.168.10.1: bytes=32 time=2ms TTL=64
Reply from 192.168.10.1: bytes=32 time=1ms TTL=64
Reply from 192.168.10.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\tools>
```

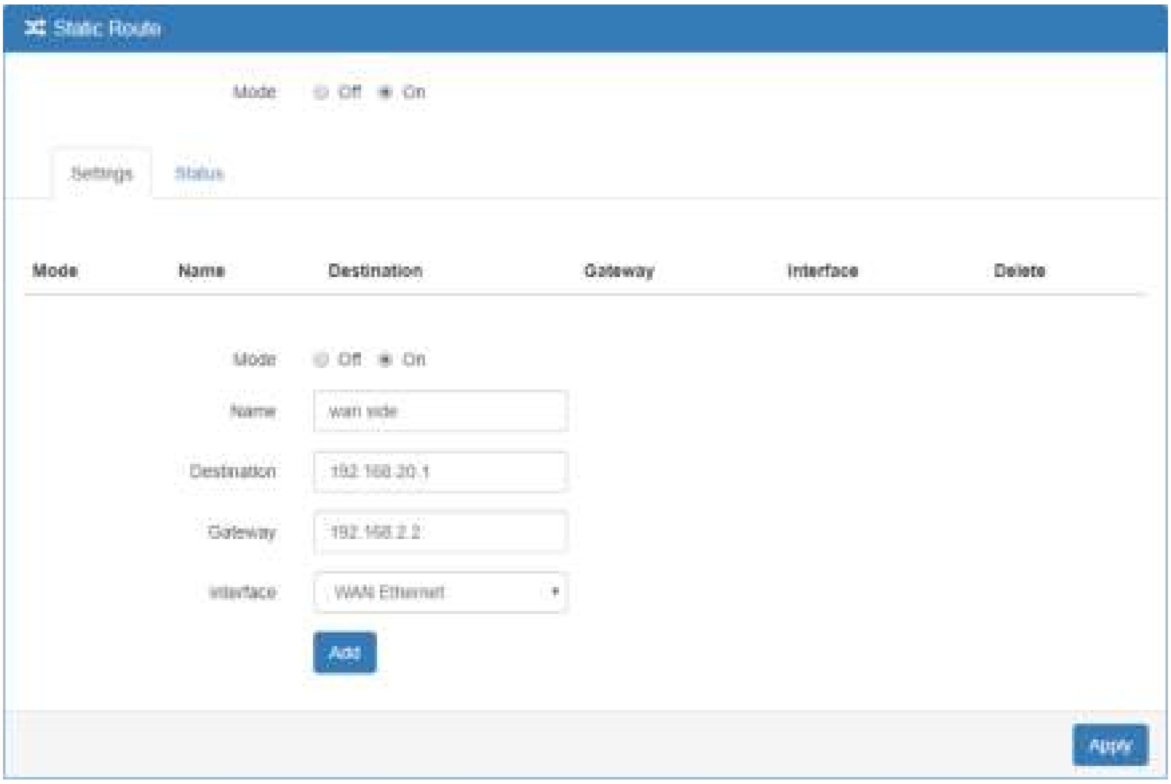
Example 2: Add IP Routing on WAN interface

- 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



Static Route

Mode ○ Off ● On

Settings | Status

Mode	Name	Destination	Gateway	Interface	Delete

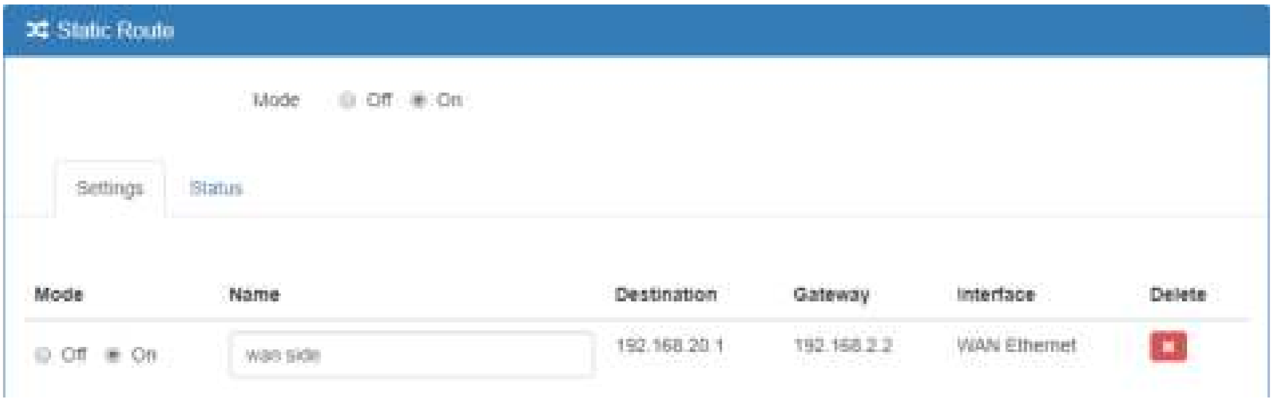
Mode ○ Off ● On

Name: wan side

Destination: 192.168.20.1

Gateway: 192.168.2.2

Interface: WAN Ethernet



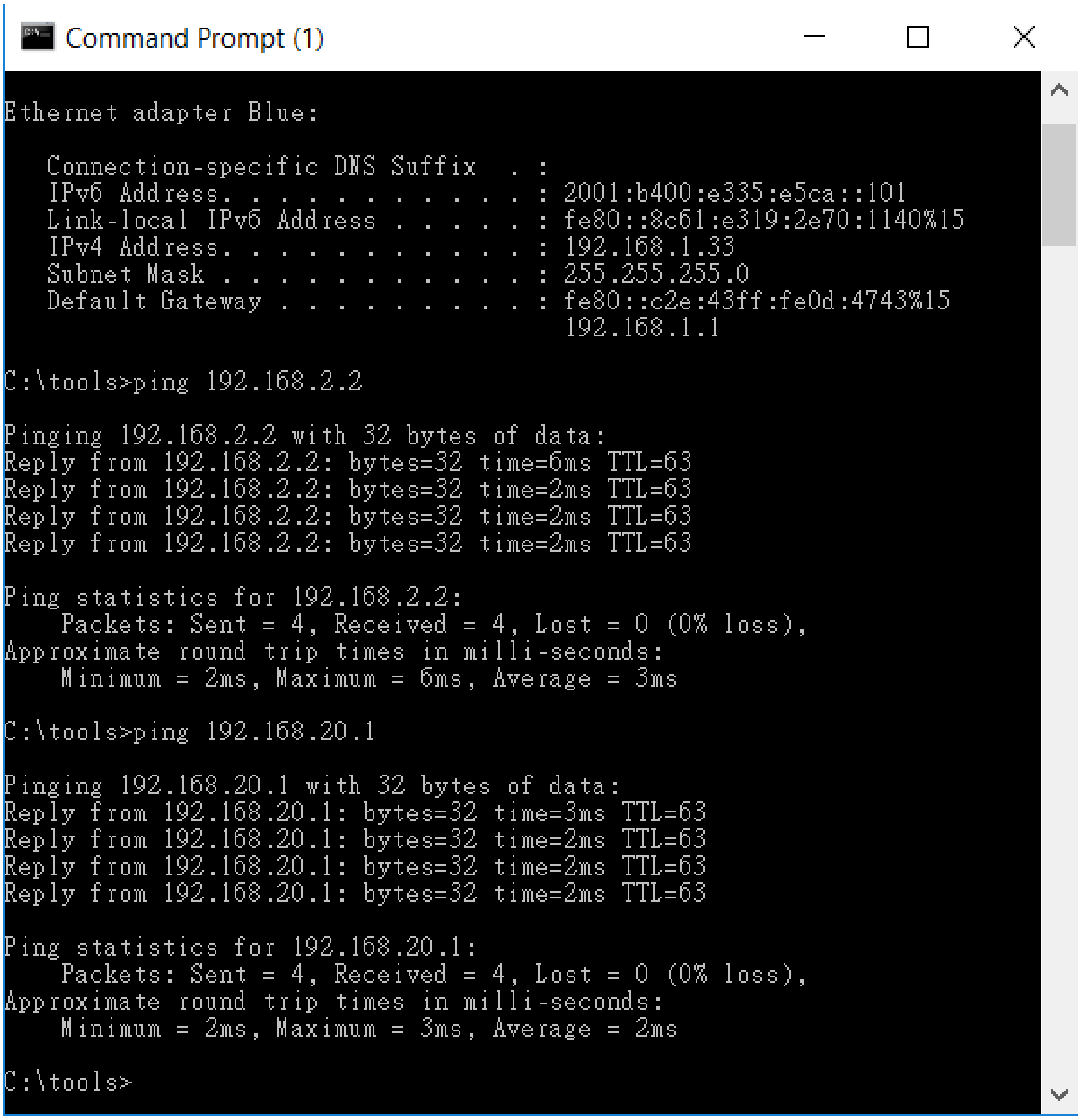
Static Route

Mode ○ Off ● On

Settings | Status

Mode	Name	Destination	Gateway	Interface	Delete
○ Off ● On	wan side	192.168.20.1	192.168.2.2	WAN Ethernet	✖

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



Command Prompt (1)

```
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:\tools>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=6ms TTL=63
Reply from 192.168.2.2: bytes=32 time=2ms TTL=63
Reply from 192.168.2.2: bytes=32 time=2ms TTL=63
Reply from 192.168.2.2: bytes=32 time=2ms TTL=63

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 6ms, Average = 3ms

C:\tools>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:
Reply from 192.168.20.1: bytes=32 time=3ms TTL=63
Reply from 192.168.20.1: bytes=32 time=2ms TTL=63
Reply from 192.168.20.1: bytes=32 time=2ms TTL=63
Reply from 192.168.20.1: bytes=32 time=2ms TTL=63

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\tools>
```