SkyMesh HYC-**OLTRG-101**

Outdoor 4G/LTE Router with I/O Ports

RS485 / RS232 / DI / DO

User Manual

Includes install, configuration and trouble shooting information for the broadband wireless access outdoor radio.

Version 1.1.4

Mars, 2019

HYC-OLTRG-101 ATEX & IP68

Power EIRP 2x30 dBm (2x1 Watt)

Features:

- Highly reliable and secure for mission-critical cellular communications
- Provide flexible options to configure LAN/ WAN ports
- Support multi-band connectivity with FDD LTE/ TDD LTE/ WCDMA/ GSM/ LTE Cat4
- Built-in dual SIM for network redundancy
- Dual MIMO antenna input against radio interference
- LED indicators for connection and data transmission status
- Industrial rated from -40 to +70°C for use in harsh environments
- IPv6/IPv4 dual stack and all applications are IPv6 ready
- Support various serial communication protocols for rich connectivity
- Enhance security and encryption for authentication and transmission
- IP68 Waterproof
- Option WiFi embedded
- High gain Antennas

HYC-OLTR(G)-101 4G/LTE Router is a highly reliable and secure wireless communications gateway designed for industrial networking, Operator or WISP create their own networks to share bandwidth with customers and also for marine and coastal communication applications.

It supports multi-band connectivity including FDD / TDD LTE, WCDMA and GSM for a wide range of applications and vertical machine-to-machine (M2M) markets. To enhance reliability, HUYC-OLTR(G)-101 is equipped with dual SIM that supports failover and roaming over to ensure uninterrupted connectivity for mission-critical cellular communications. With flexible LAN / WAN Ethernet options, HYC-OLTR(G)-101 series allows you to customize your professional applications in diverse environments.

It also provides enterprise-grade software features, such as Quality of Service (QoS) for traffic prioritization, IPSec, OpenVPN, Firewall security and so on.

The device is administrated via web GUI, Telnet, SSH v2 and HTTP/HTTPS. Built for secure and uninterrupted operation in harsh environments, HYC-OLTR(G)-101 series supports extended operating temperature from -40 to +70°C and a flexible input voltage range of 10-32V DC.

HYC-OLTR(G)-101 is an ideal cellular communications solution for heavy industrial use.

Specifications

FREQUENCIES	
FDD LTE	B1 / B2 / B3 / B4 / B5 / B7 / B8 / B12 / B17 / B20 / B28
TDD LTE	B38 / B40 / B41
WCDMA	B1 / B5 / B8
GSM	900 / 1800 MHz
WiFi Access Point	2402 – 2482 MHz
OUTPUT POWER	
LTE FDD	23dBm +/- 2dB up to EIRP 30dBm
LTE TDD	23dBm +/- 2dB up to EIRP 30dBm
TD-SCDMA	24dBm +/- 3dB up to EIRP 31dBm
UMTS	24dBm +/- 3dB up to EIRP 31dBm
WiFi Access Point	27dBm +/- 1.5dB up to EIRP 34dBm
INTERFACE	
SIM Cards Slots x 2	
WAN 10/100 Mbps Ethernet M12 port x 1	
LAN 10/100 Mbps Ethernet M12 port x 1	
LTE antenna N-type port x 2	
WiFi AP N-type port x 2	
GPS N-type port x 1	
DC power M12 port x 1	
Software	
Network Protocols	IPv4, IPv6, IPv4/IPv6 dual stack, DHCP server and client, PPPoE, Static IP, SNTP, DNS Proxy
Routing & Firewall	NAT, Virtual Server, DMZ, MAC filter, URL Filter, IP Filter, VLAN, Static Routing and RIP-1/2
VPN	OpenVPN, IPSec (3DES, AES128, AES196, AES256, MD5, SHA-1, SHA256)
Wireless Connectivity	Two SIM cards for failover / roaming over / back up
	Two SIM cards data usage control
	Seamless multi WAN connections switch
	WiFi Access Point for hotspot (OLTRG-101G model)
Others	DDNS, QoS, UPnP
Alarm	SMS, VPN/WAN Disconnection, SNMP Trap, E-mail
Management	
Web GUI for remote and local management, CLI	
SNMP, TR069	
ENVIRONMENT	
Operating Temperature	-40~70 ℃
Storage Temperature	-40~85 ℃
Humidity	95% non-condensing
POWER SUPPLY & CONSUMPTION	
Power consumption : 17Watts (Typical), 19Watts (Max.) Power Input : DC 24V	
PHYSICAL	
Dimension	259 (L) * 250 (W) * 75 (H) ; mm
Weight	1.8Kg
WARRANTY	
1 YEAR	
ORDERING INFORMATION	
HYC-OLTRG-101	Outdoor IP68 4G LTE Router (1 x WAN + 1 x LAN) with GPS
HYC-OLTRG-101G-20	Outdoor IP68 4G LTE Router (1 x WAN + 1 x LAN + 2.4GHz WiFi AP) with GPS
HYC-ANT-45270-MM	450 MHz – 2700 MHz Linear Omni Marine antenna

Table of Contents

1 Introduction

Hypercable OLTRG-100 series 4G/LTE 4G/LTE Router are highly reliable and secure wireless communications gateway designed for industrial networking. It supports multi-band connectivity including FDD/TDD LTE, WCDMA and GSM for a wide range of applications and vertical machine-to-machine (M2M) markets. To enhance reliability, **OLTRG-100** series are equipped with dual SIM that support failover and roaming over to ensure uninterrupted connectivity for mission-critical cellular communications.

With flexible LAN/WAN Ethernet options, **OLTRG-100** series allow you to customize your professional applications in diverse environments. Integrated with WAN, LAN, the **OLTRG-100** series also provide various network protocols, such as IPv6, MQTT and VPN for enriching connectivity and security. For VPN tunnel, OpenVPN and IPSec are for reliable authentication of the network stations, data encryption and verification of data integrity. The device is administrated via web GUI, Telnet, SSH v2 and HTTP/HTTPS.

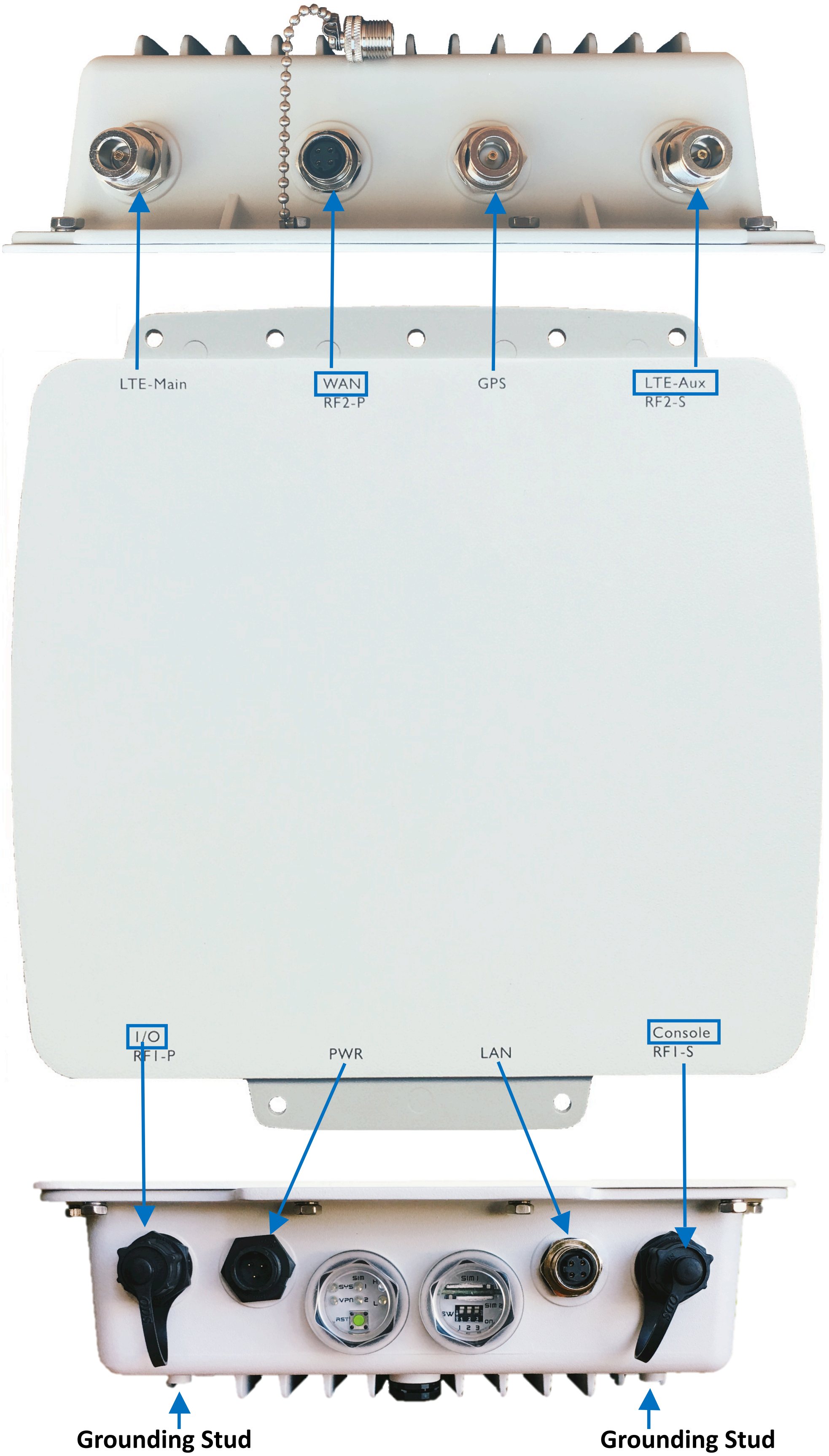
Built for secure and uninterrupted operation in harsh environments, **OLTRG-100** series support extended operating temperature from -20 to +70°C and IP-68 grade water and dust proof outdoor enclosure.

1.1 **Features**

- Highly reliable and secure for mission-critical cellular communications
- Support multi-band connectivity with FDD LTE / TDD LTE / WCDMA / GSM / LTE Cat4
- Built-in dual SIM for network redundancy
- Integrated dual detachable antenna against radio interference
- LED indicators for connection and data transmission status
- Industrial rated from -40 ~ +70°C for use in harsh environments
- IPv6 / IPv4 dual stack and all applications are IPv6 ready
- Aluminum Housing with IP-68 industrial grade protection
- Support various serial communication protocols for rich connectivity by RS232/RS485/ DI/DO

1.2 Hardware Interface

[Top Side View]



[Bottom Side View]

1.3 Hardware Interface Introduction

[Top Side View]

Interface	Description
LTE-Main	Connect to LTE antenna with N-type connector
WAN port (4 pins)	Connect to Ethernet Cable with M12 connector
GPS	Connect to GPS antenna with N-type connector
LTE-Aux	Connect to LTE antenna with N-type connector

[Bottom Side View]

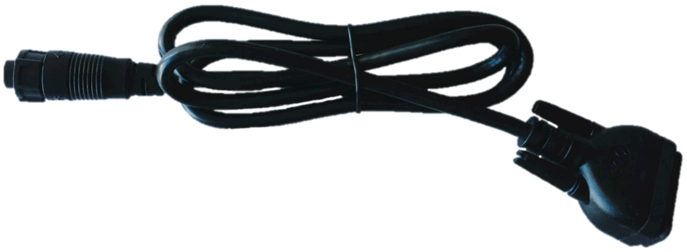
Interface	Description
I/O port (12 pins)	RS232 / RS485 / DI / DO
PWR (3 pins)	Connect to Power cable with Circle-B type connector
LAN port (4 pins)	Connect to Ethernet Cable with M12 connector
Console port (5 pins)	Connect to RS-232 Console port
LED Indicators	SYS / VPN / SIM1 / SIM2 / H (RSSI) / L (RSSI)
RST	Allows you to reboot the unit or restore to factory default setting. **Reboot -** Press the button for **1 second** **Restore to factory default setting -** Press the button for **5 seconds**
SIM1 & SIM2	Insert the Micro Sim Card (Push – Push Sim Card holder)
RF1-S	2.4GHz Wi-Fi Primary port – Connect to 2.4GHz antenna with N-type connector
Grounding stud	Connect to the ground wire with stainless screws.

Ethernet Cable with M12 connector

connector

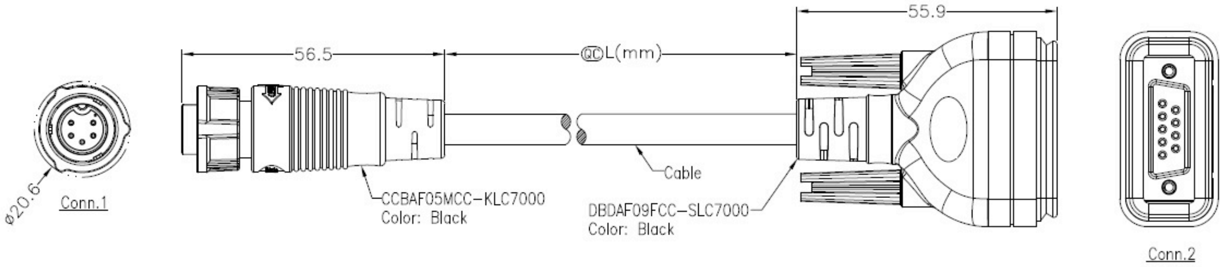
Power Cable with Circular Standard (CCB)

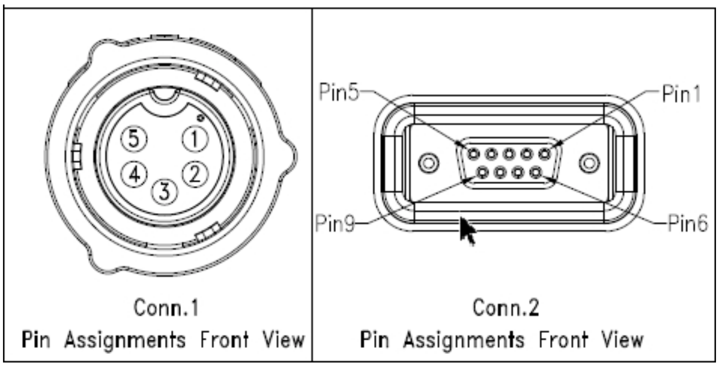
Wire color	DC Power (24V)
Yellow	Chassis Ground
White	V -
Black	V+



Console port Cable with Circular Standard (CCB) connector

■ Pin Assignment of RS-232 Cable (Com1)

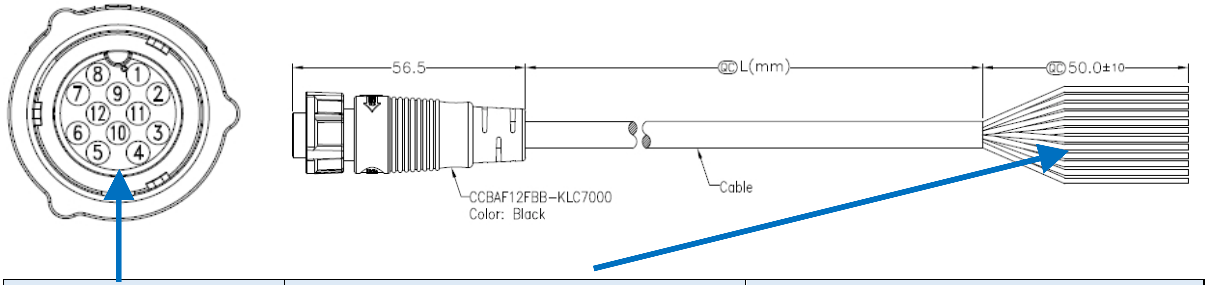




Pin of Conn.1	Pin of Conn. 2	Description
	1	N/A
2	2	RXD
1	3	TXD
	4	N/A
3	5	GND
	6	N/A
5	7	RTS
4	8	CTS
	9	N/A

I/O port Cable with Circular Standard (CCB) connector

Pin Assignment of I/O Port cable

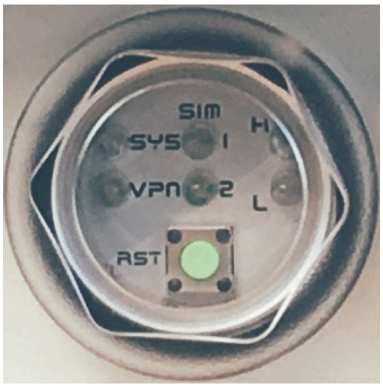


CCB 12-pin	Cable Color	Pin assignment
1	Blue	RD485 D-
2	Blue/White	RS485 D+
3	Orange	Alarm +
4	Orange/White	Alarm -
5	Green	DI2
6	Green/White	DI2_COM
7	Brown	RS232_TXD
8	Brown/White	RS232_RXD
9	Black	RS232_GND
10	Red	DI1
11	Black/White	-
12	Red/White	DI1_COM

2 Hardware Installation

This chapter introduces how to install and connect the hardware.

2.1 LED Indicators



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

2.2 Reset Button (RST)

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.

2.3 Ethernet Port

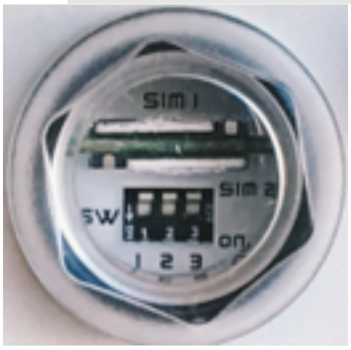
(1) 10/100 Mbps Ethernet WAN

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

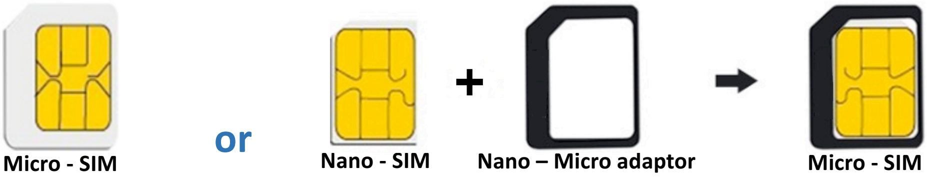
(2) 10/100 Mbps Ethernet LAN

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

2.4 Install the SIM Card (Micro-Sim)



1. Push-Push Sim Card holder for Micro-Sim Card



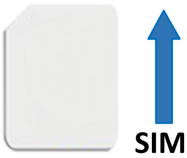
Note:

- **If you are using Nano – Micro adaptor as Micro-Sim, please use the sticker to stick the Nano Sim card and adaptor together.**

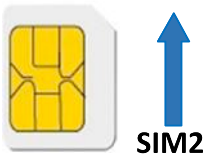
2. Insert and Remove SIM1/SIM2 Card

(1) Before inserting or removing the SIM card, ensure that the power has been turned off and the power connector has been removed from 4G/LTE Router.

(2) Insert the Micro - SIM card into the push-push Sim card holder by following instruction.



SIM1 (chip side down)



SIM2 (chip side up)

(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 insert direction is correct first. When pulling the Micro-SIM card from the tray by incorrect direction, the chip card or the tray might be damaged.**
- **Please turn off your router before insert or remove the SIM card.**

2.5 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

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

Switch 3 enables or disables the termination resistor

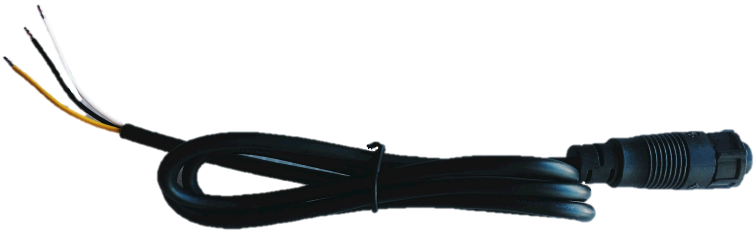
Termination Resistor (120 ohm)	**SW 3**
Enable	ON
Disable (Default)	OFF

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 24V DC. Please ensure all components are earthed to a common ground before connecting any wiring.



Wire color	DC Power (24V)
Yellow	Chassis Ground
White	V -
Black	V+

Note:

- **Please make sure the power voltage and polarization are correct and match with the wire color.**

3 Configuration via Web Browser

Access the Web Interface

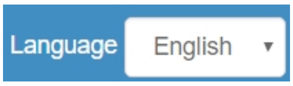
The web configuration is an HTML-based management interface for quick and easy set up of the cellular router. Monitoring of the status, configuration and administration of the router can be done via the Web interface.

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

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

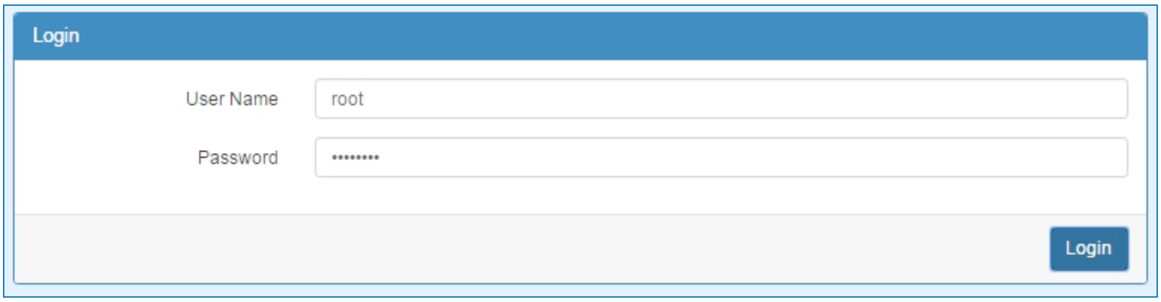
Control Panel > Selecting Language

You can choose the languages, including English and Taiwan.



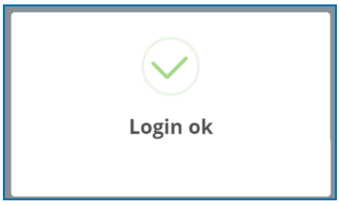
Logging in the Router

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



User Name root

Password ••••••••

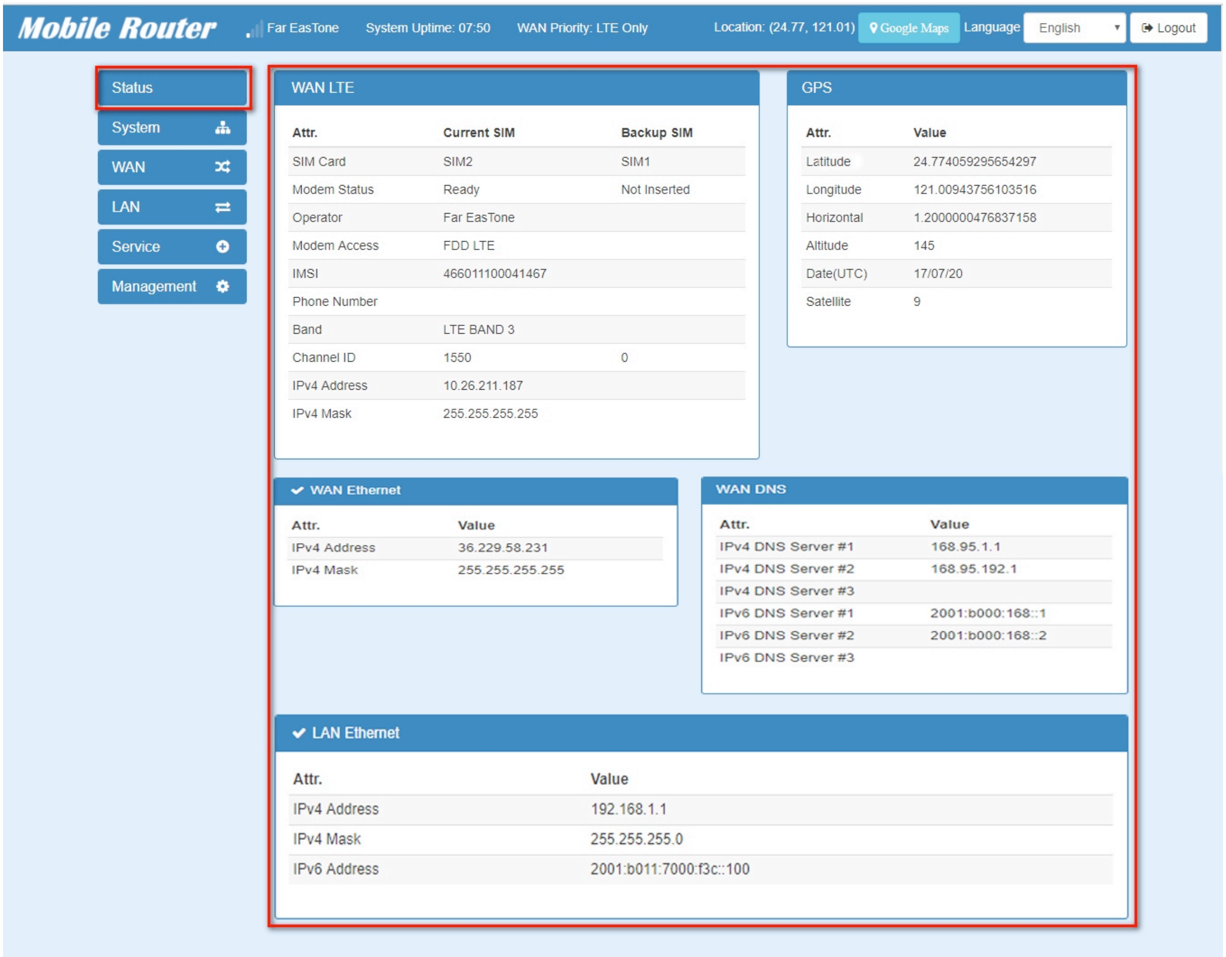


Login ok

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

4 Status

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



WAN LTE

Attr.	Current SIM	Backup SIM
SIM Card	SIM2	SIM1
Modem Status	Ready	Not Inserted
Operator	Far EasTone	
Modem Access	FDD LTE	
IMSI	466011100041467	
Phone Number		
Band	LTE BAND 3	
Channel ID	1550	0
IPv4 Address	10.26.211.187	
IPv4 Mask	255.255.255.255	

GPS

Attr.	Value
Latitude	24.774059295654297
Longitude	121.00943756103516
Horizontal	1.2000000476837158
Altitude	145
Date(UTC)	17/07/20
Satellite	9

✓ WAN Ethernet

Attr.	Value
IPv4 Address	36.229.58.231
IPv4 Mask	255.255.255.255

WAN DNS

Attr.	Value
IPv4 DNS Server #1	168.95.1.1
IPv4 DNS Server #2	168.95.192.1
IPv4 DNS Server #3	
IPv6 DNS Server #1	2001:b000:168::1
IPv6 DNS Server #2	2001:b000:168::2
IPv6 DNS Server #3	

✓ LAN Ethernet

Attr.	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	2001:b011:7000:f3c::100

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

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

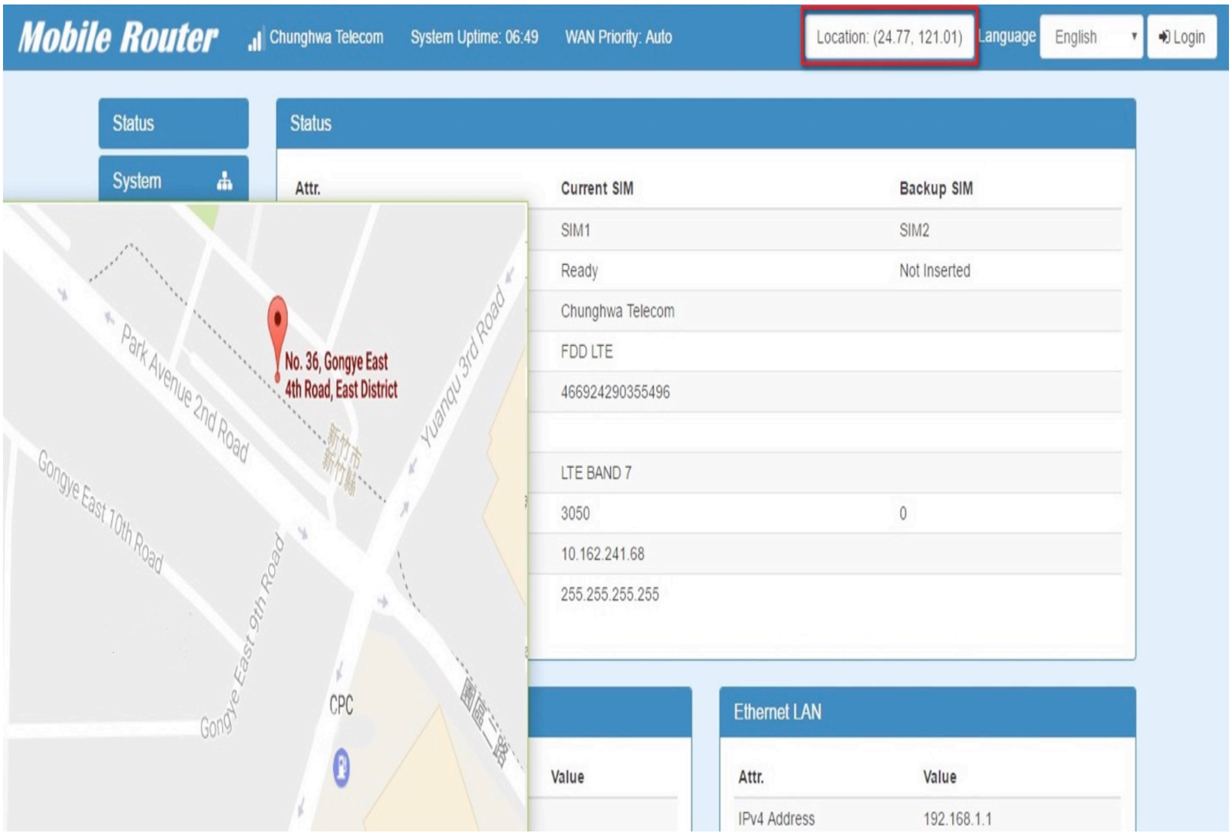
Status > LAN Ethernet	
Item	**Description**
Attribute	
IPv4 Address	Ethernet LAN is assigned IPv4 Address.
IPv4 Mask	Ethernet LAN is assigned IPv4 Mask.
IPv6 Address	Ethernet LAN is assigned IPv6 Address.

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

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

4.1 **Status > GPS**

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



Mobile Router | Chunghwa Telecom | System Uptime: 06:49 | WAN Priority: Auto | Location: (24.77, 121.01) | Language | English | Login

Status

Attr.	Current SIM	Backup SIM
	SIM1	SIM2
	Ready	Not Inserted
	Chunghwa Telecom	
	FDD LTE	
	466924290355496	
	LTE BAND 7	
	3050	0
	10.162.241.68	
	255.255.255.255	

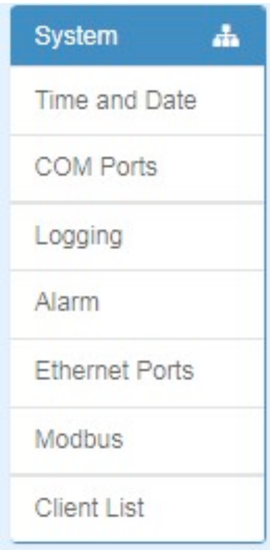
	Value

Ethernet LAN

Attr.	Value
IPv4 Address	192.168.1.1

5 Configuration > System

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



5.1 System > Time and Date

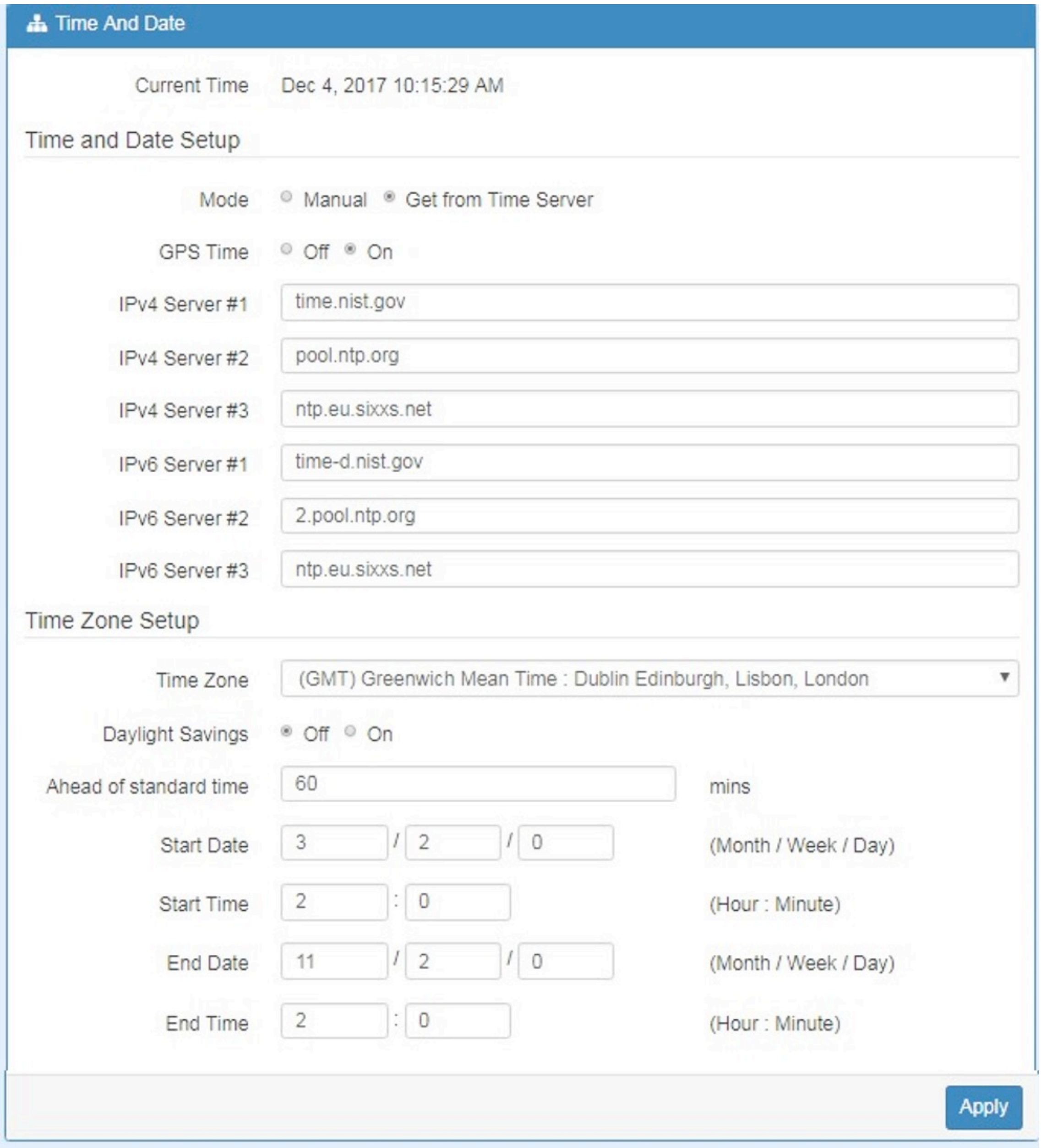
This section allows you to set up the time and date of router and NTP server. There are two modes at Time and Date Setup, including **Get from Time Server** and **Manual**. The default mode is **Get from Time Server**.

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

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

I. **Get from Time Server**

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



Time And Date

Current Time Dec 4, 2017 10:15:29 AM

Time and Date Setup

Mode ○ Manual ● Get from Time Server

GPS Time ○ Off ● On

IPv4 Server #1 time.nist.gov

IPv4 Server #2 pool.ntp.org

IPv4 Server #3 ntp.eu.sixxs.net

IPv6 Server #1 time-d.nist.gov

IPv6 Server #2 2.pool.ntp.org

IPv6 Server #3 ntp.eu.sixxs.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)

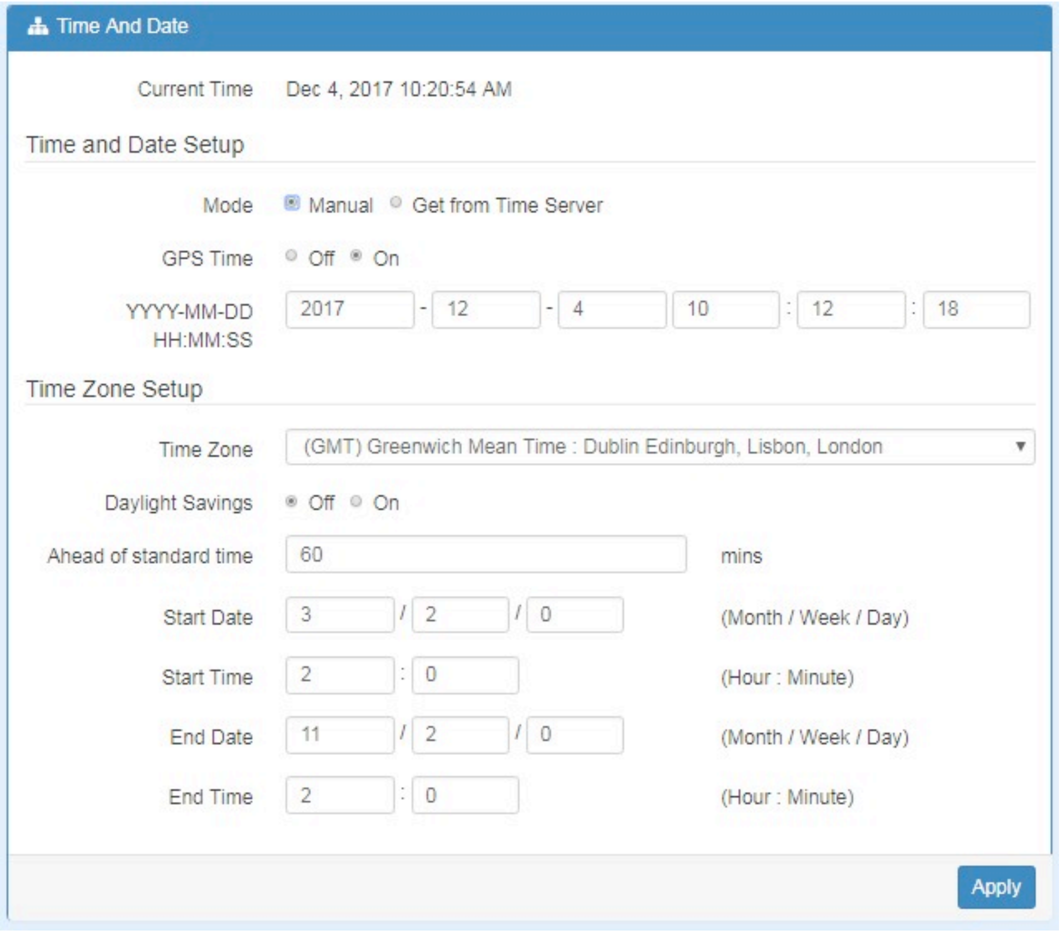
Start Time 2 : 0 (Hour : Minute)

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

End Time 2 : 0 (Hour : Minute)

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.



Time And Date

Current Time: Dec 4, 2017 10:20:54 AM

Time and Date Setup

Mode: ● Manual ○ Get from Time Server

GPS Time: ○ Off ● On

YYYY-MM-DD HH:MM:SS: 2017 - 12 - 4 10 : 12 : 18

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)

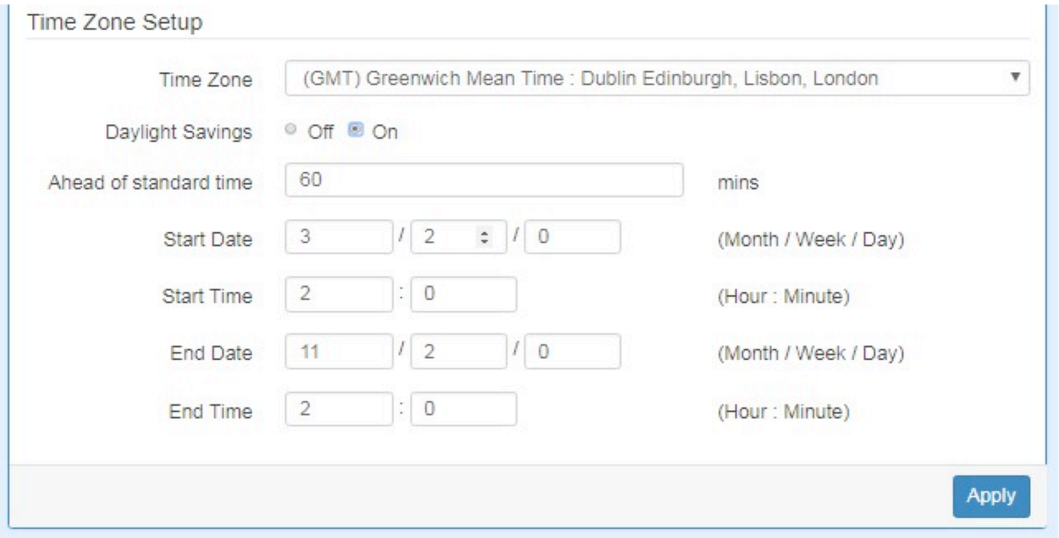
Start Time: 2 : 0 (Hour : Minute)

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

End Time: 2 : 0 (Hour : Minute)

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)

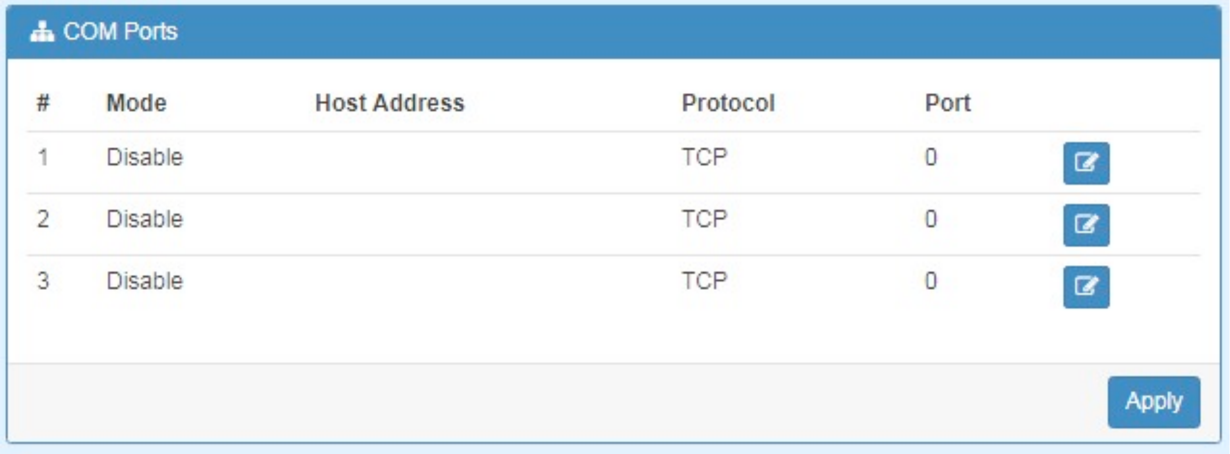
System > Time and Date->Daylight Savings	
Item	**Description**
Daylight Saving	Turn on/off the Daylight Savings feature. Select from Off or On. The default is Off.
Ahead of standard time	The forward/backward minutes when enter/leave Daylight Savings duration.Default is 60 mins.
Start Date/Start Time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

5.2 **System > COM Ports**

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

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

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

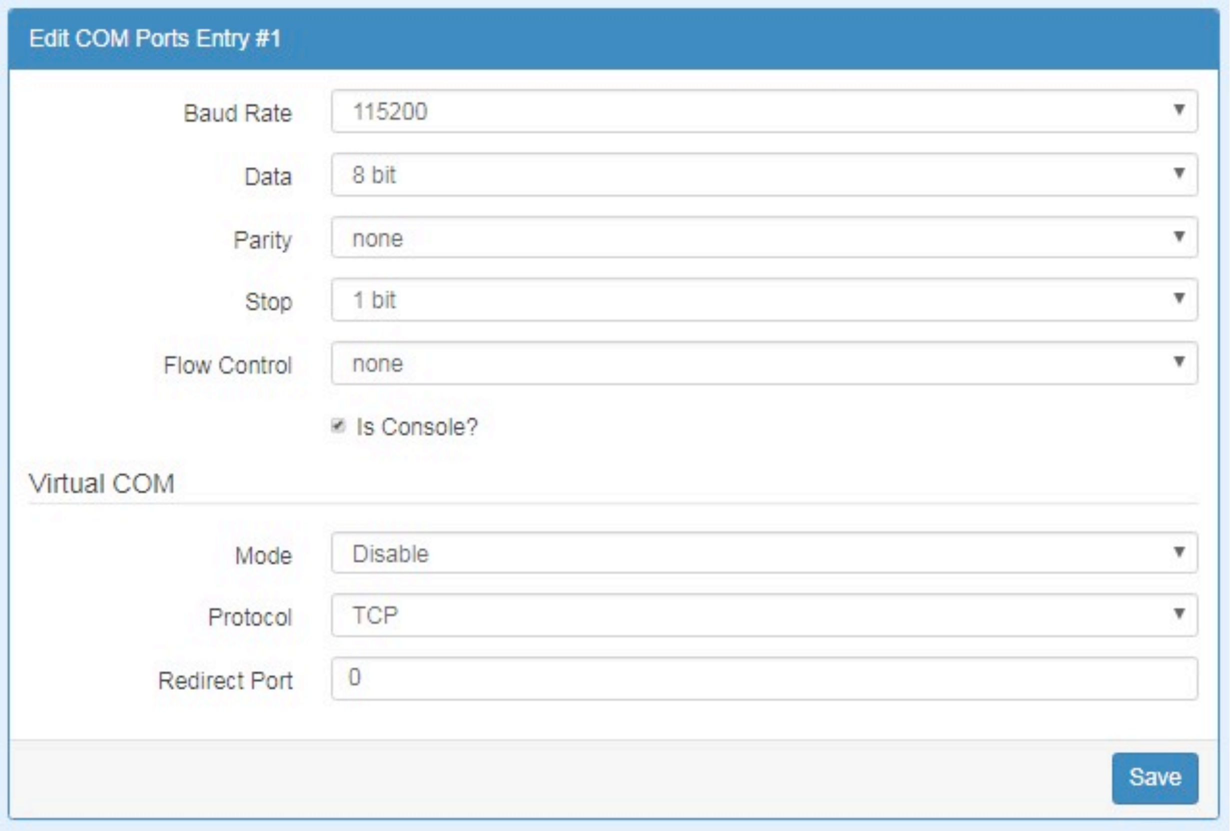


COM Ports

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

Apply

(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

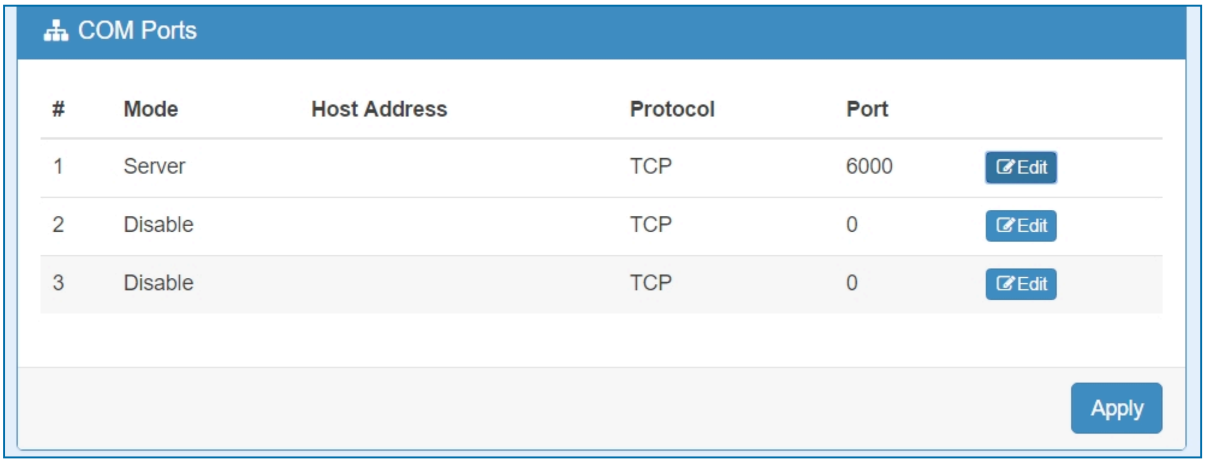
Mode	Disable ▾
Protocol	TCP ▾
Redirect Port	0

Save

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

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

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

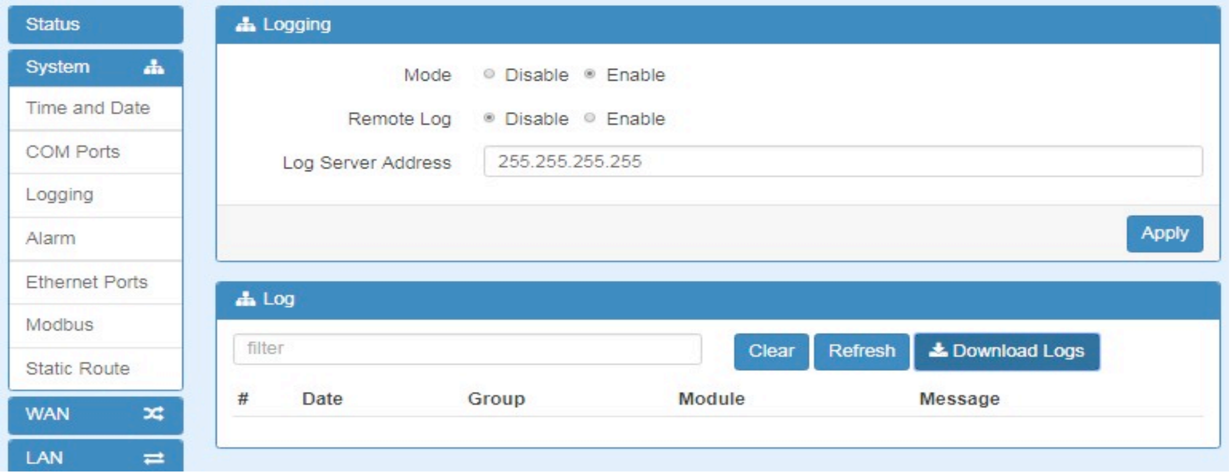


#	Mode	Host Address	Protocol	Port	
1	Server		TCP	6000	Edit
2	Disable		TCP	0	Edit
3	Disable		TCP	0	Edit

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.



Mode ○ Disable ● Enable

Remote Log ● Disable ○ Enable

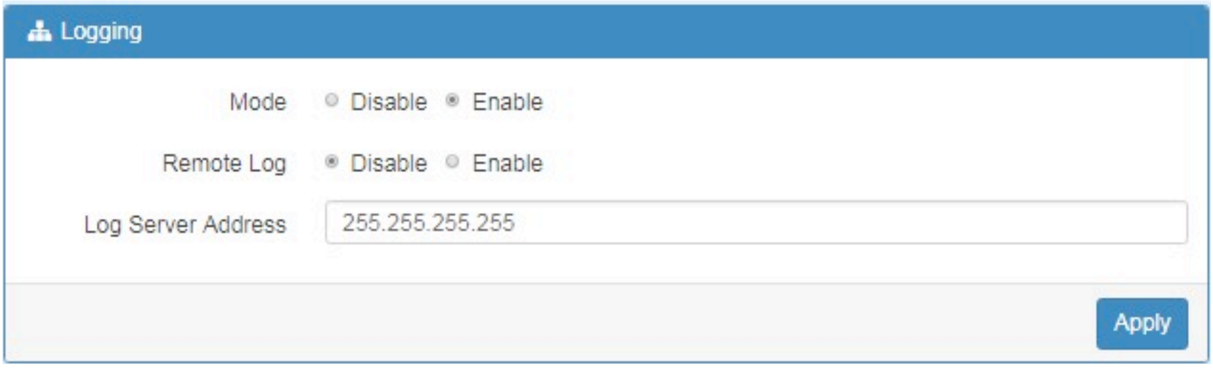
Log Server Address 255.255.255.255

#	Date	Group	Module	Message

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.



Logging

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

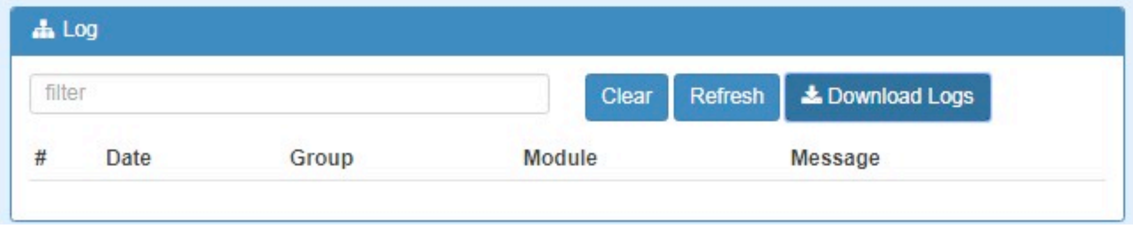
This section displays all data status.

(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.



Log

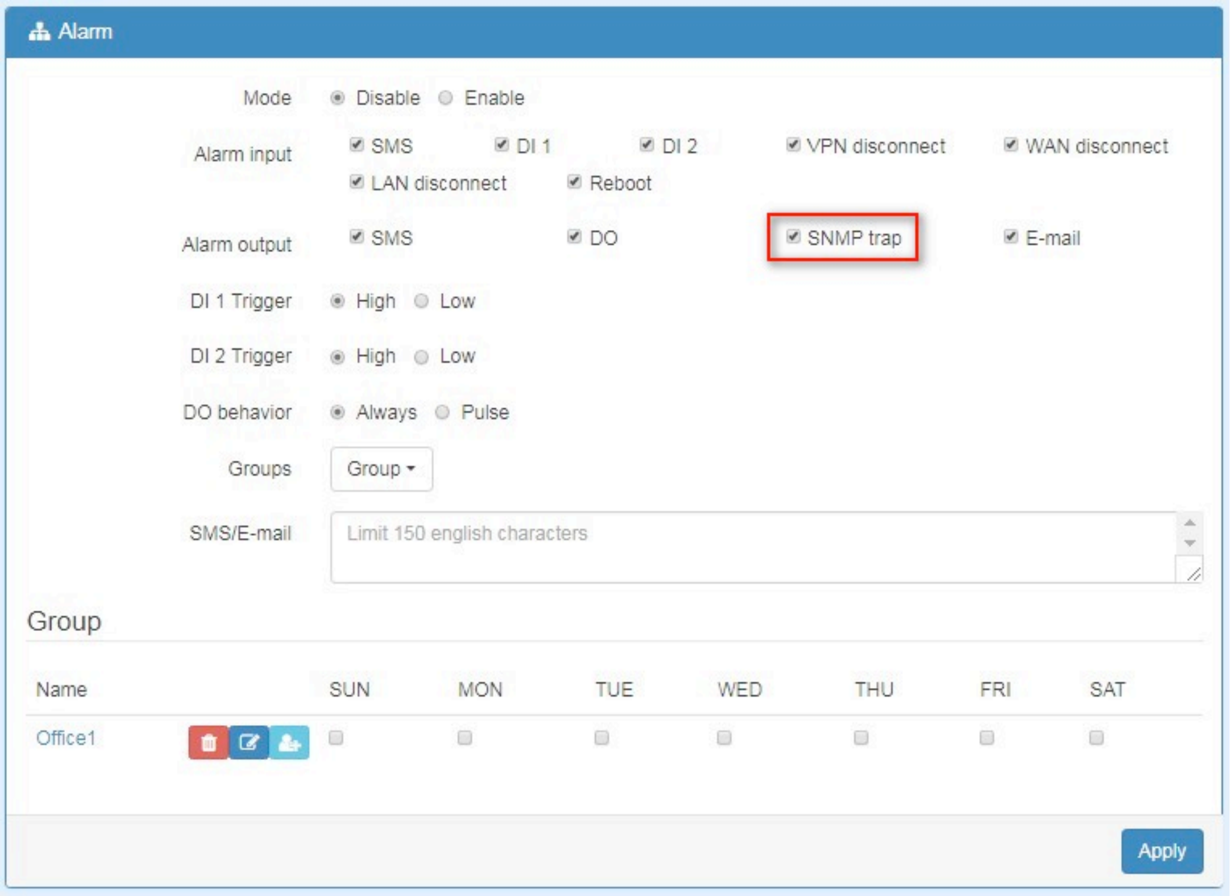
filter

#	Date	Group	Module	Message

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

DI 1 Trigger ● High ○ Low

DI 2 Trigger ● High ○ Low

DO behavior ● Always ○ Pulse

Groups: Group ▾

SMS/E-mail: Limit 150 english characters

Group

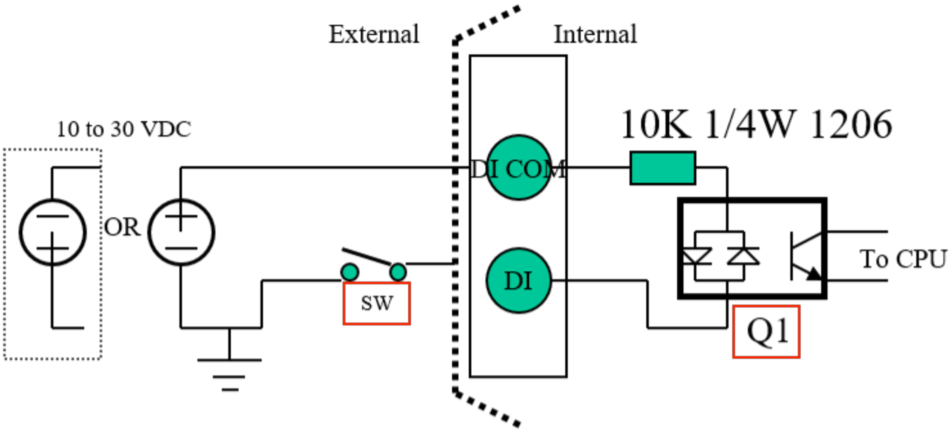
Name		SUN	MON	TUE	WED	THU	FRI	SAT
Office1		□	□	□	□	□	□	□

Note:

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

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

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

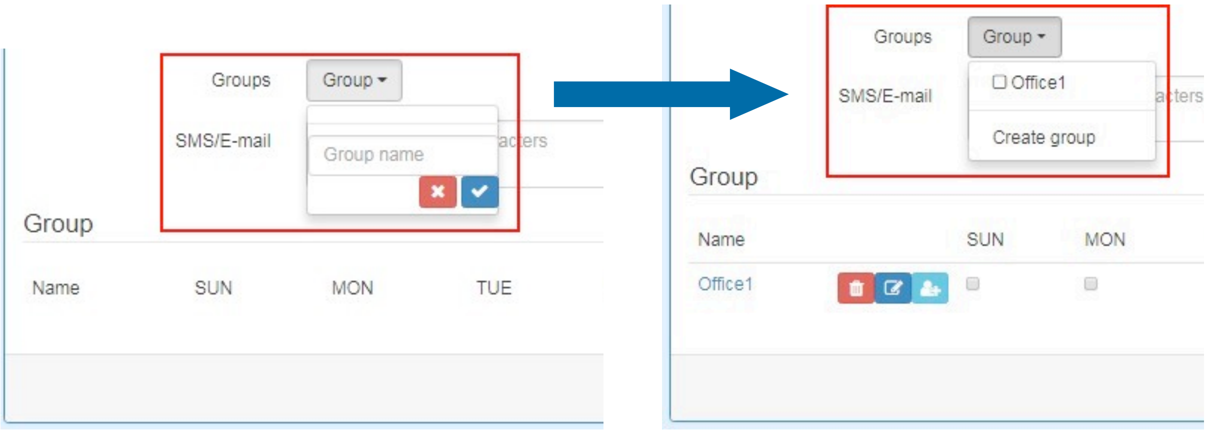


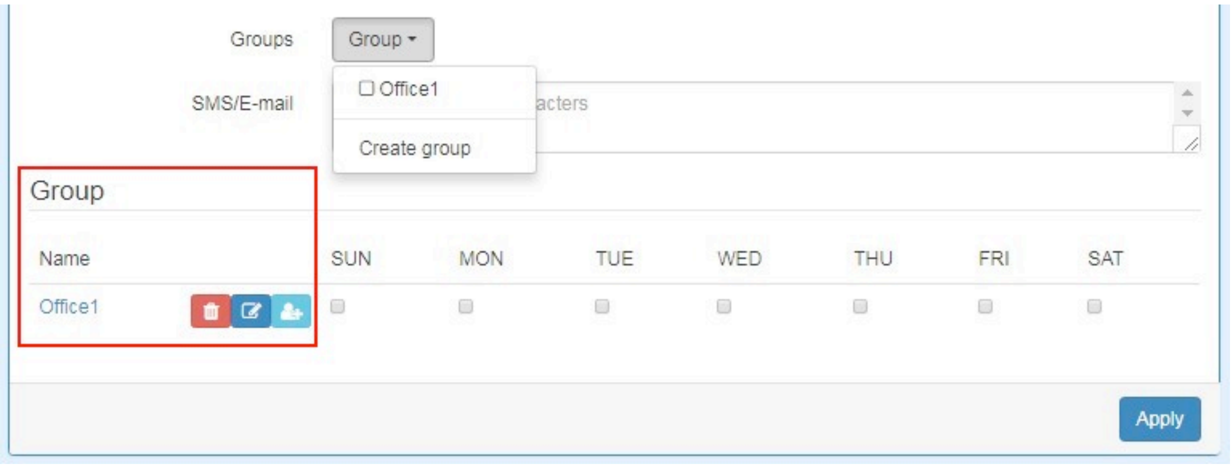
System > Alarm	
Item	**Description**
Mode	Turn on/off the Alarm configuration. Select from Disable or Enable. The default is Enable.
Alarm Input	Select from SMS, DI 1, DI 2, VPN disconnect and WAN disconnect as input to trigger alarm. ● **SMS:** It means team members on selected week day can send SMS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

5.4.1 Alarm > Name Group

(1) How to create your group

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





Groups: Group ▾

☐ Office1

Create group

SMS/E-mail: acters

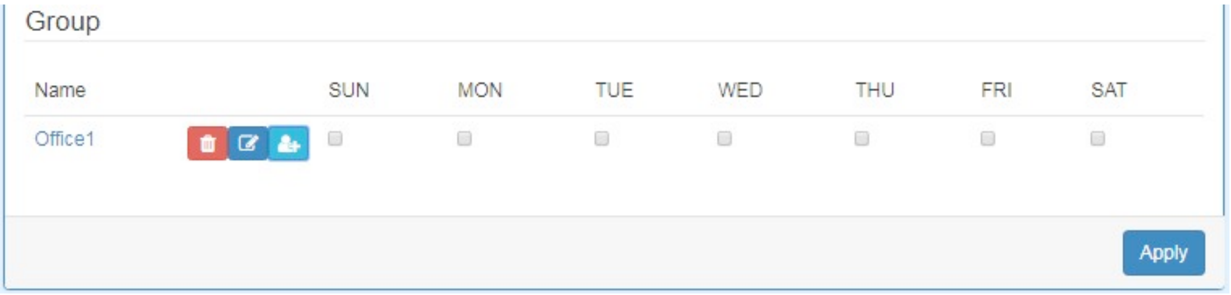
Group

Name	SUN	MON	TUE	WED	THU	FRI	SAT
Office1	☐	☐	☐	☐	☐	☐	☐

5.4.2 Alarm > Edit User

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

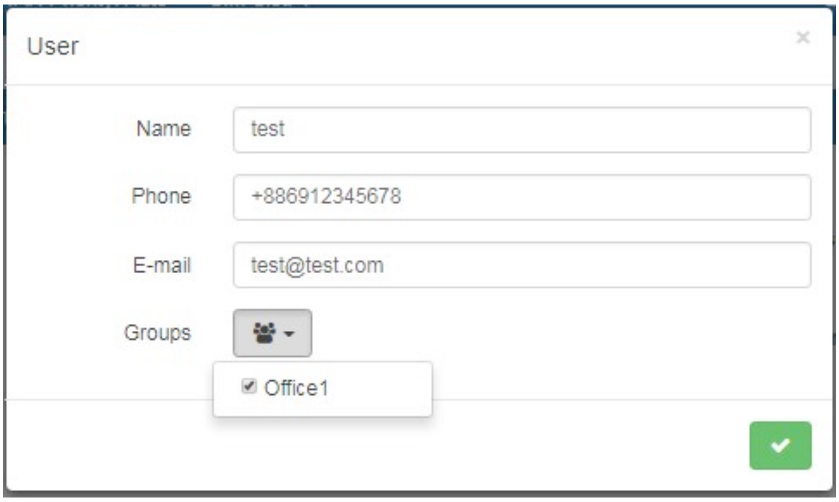
- Select your naming group and click Add button to edit your user's information, including Name, Phone and E-mail.



Group

Name	SUN	MON	TUE	WED	THU	FRI	SAT
Office1	☐	☐	☐	☐	☐	☐	☐

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



User

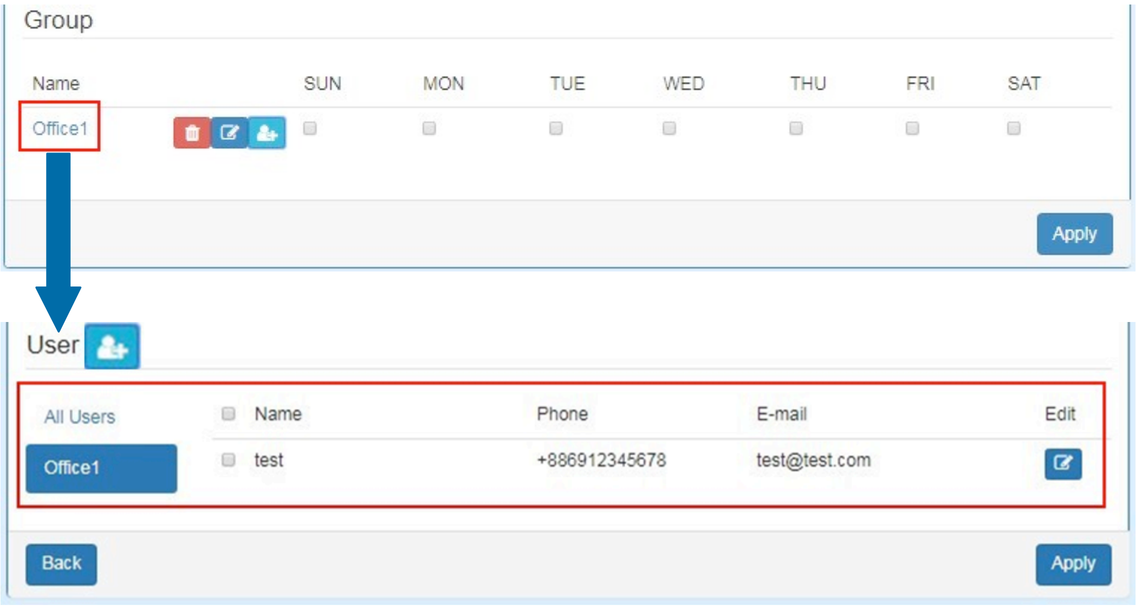
Name: test

Phone: +886912345678

E-mail: test@test.com

Groups: ☑ Office1

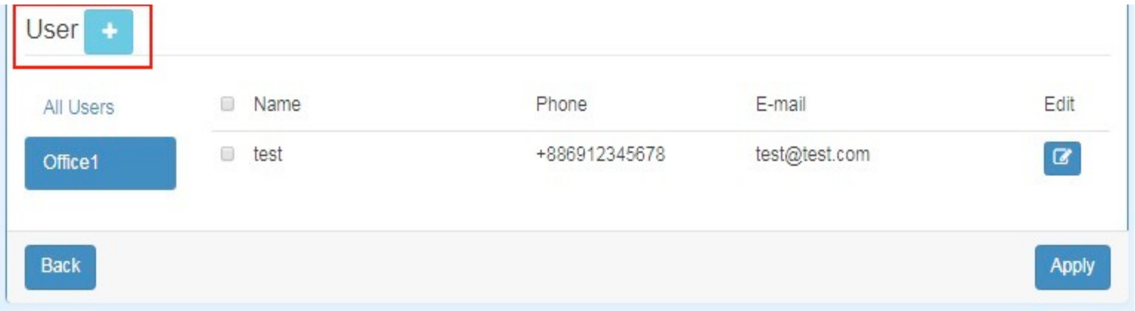
- After submitting your setting, the interface returns to Group window setting. Please click your naming group to show the user's information that you have edited.



Name		SUN	MON	TUE	WED	THU	FRI	SAT
Office1		□	□	□	□	□	□	□

		Name	Phone	E-mail	Edit
All Users	□	Name	Phone	E-mail	Edit
Office1	□	test	+886912345678	test@test.com	

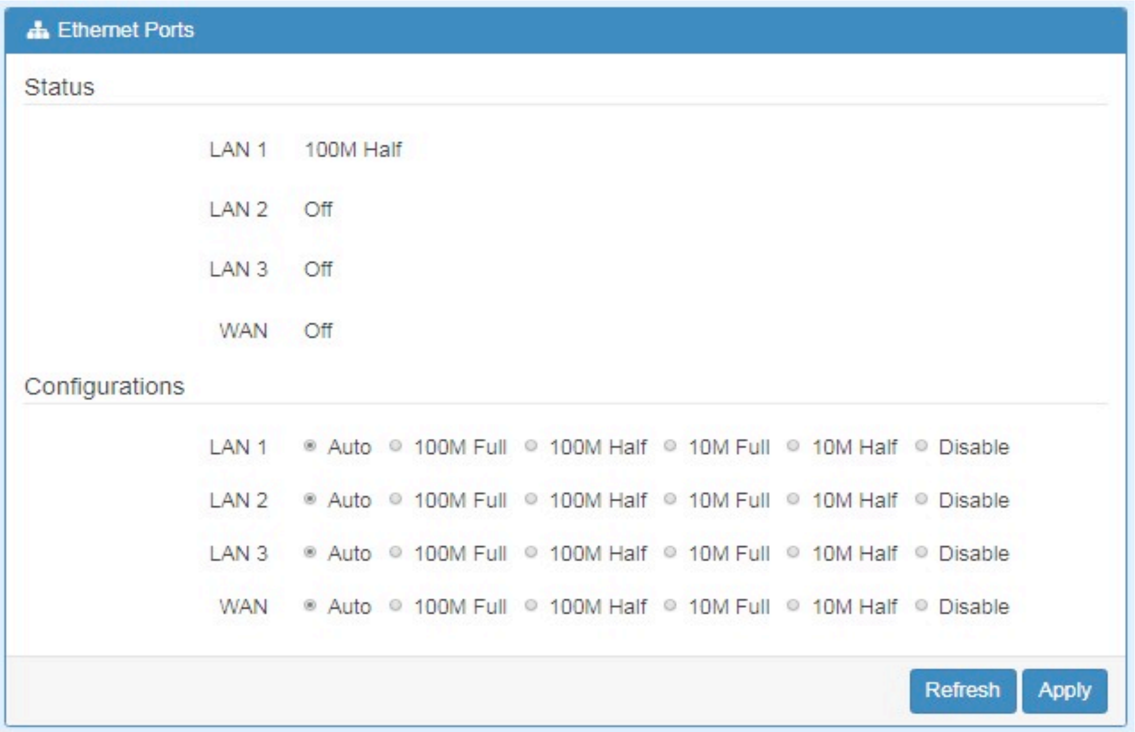
- You can click button to add the new user's information.



		Name	Phone	E-mail	Edit
All Users	□	Name	Phone	E-mail	Edit
Office1	□	test	+886912345678	test@test.com	

5.5 System > Ethernet Ports

This section allows you to configure the Ethernet Ports.



Status

LAN 1	100M Half
LAN 2	Off
LAN 3	Off
WAN	Off

Configurations

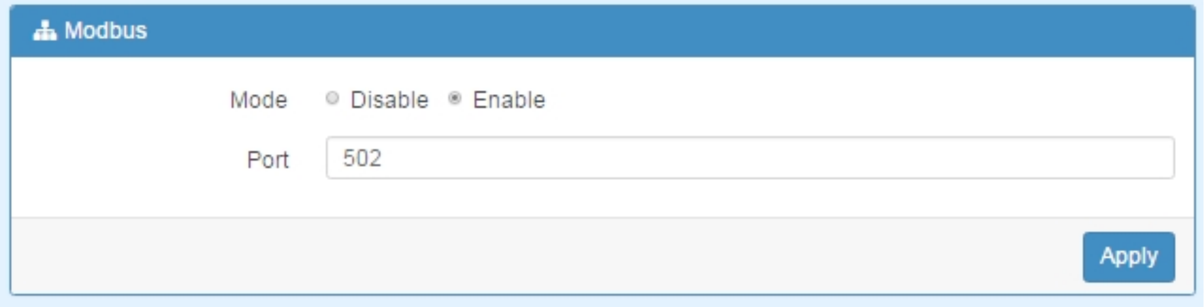
LAN 1	● Auto	○ 100M Full	○ 100M Half	○ 10M Full	○ 10M Half	○ Disable
LAN 2	● Auto	○ 100M Full	○ 100M Half	○ 10M Full	○ 10M Half	○ Disable
LAN 3	● Auto	○ 100M Full	○ 100M Half	○ 10M Full	○ 10M Half	○ Disable
WAN	● Auto	○ 100M Full	○ 100M Half	○ 10M Full	○ 10M Half	○ Disable

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

5.6 System > Modbus

This section allows you to configure the Modbus.

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



Mode ○ Disable ● Enable

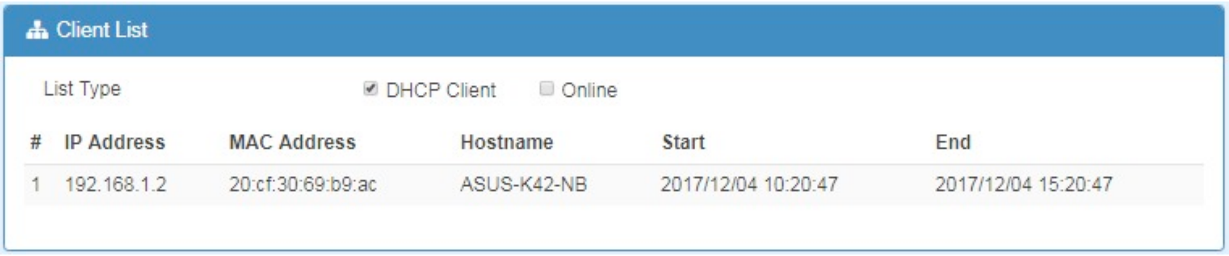
Port 502

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.

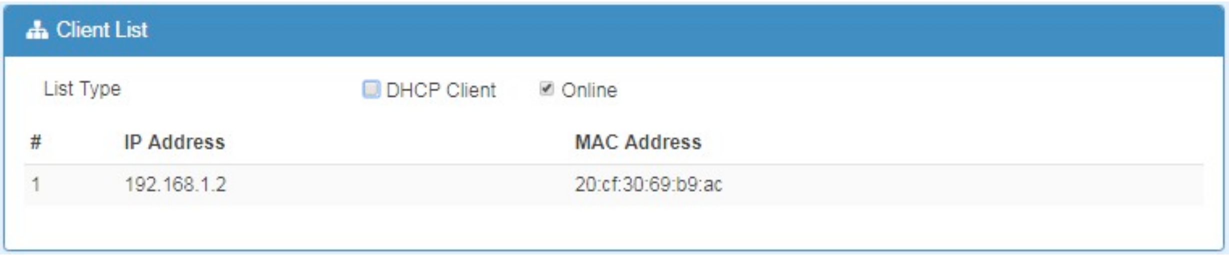
For **DHCP Client** type, the information shows IP address, MAC address, Hostname and the expiry time of IP (Start/End).



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

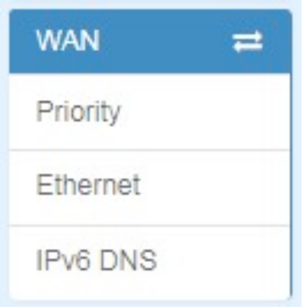
List Type □ DHCP Client ☑ Online

#	IP Address	MAC Address
1	192.168.1.2	20:cf:30:69:b9:ac

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

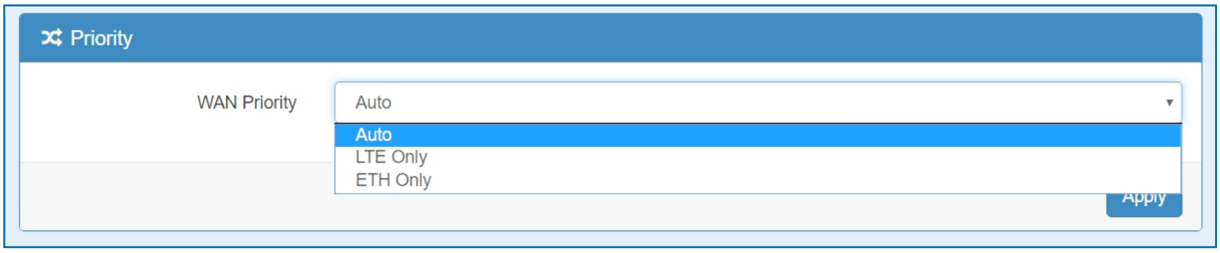
6 Configuration > WAN

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



6.1 WAN > Priority

You can set up the priority of WAN.



WAN Priority: Auto

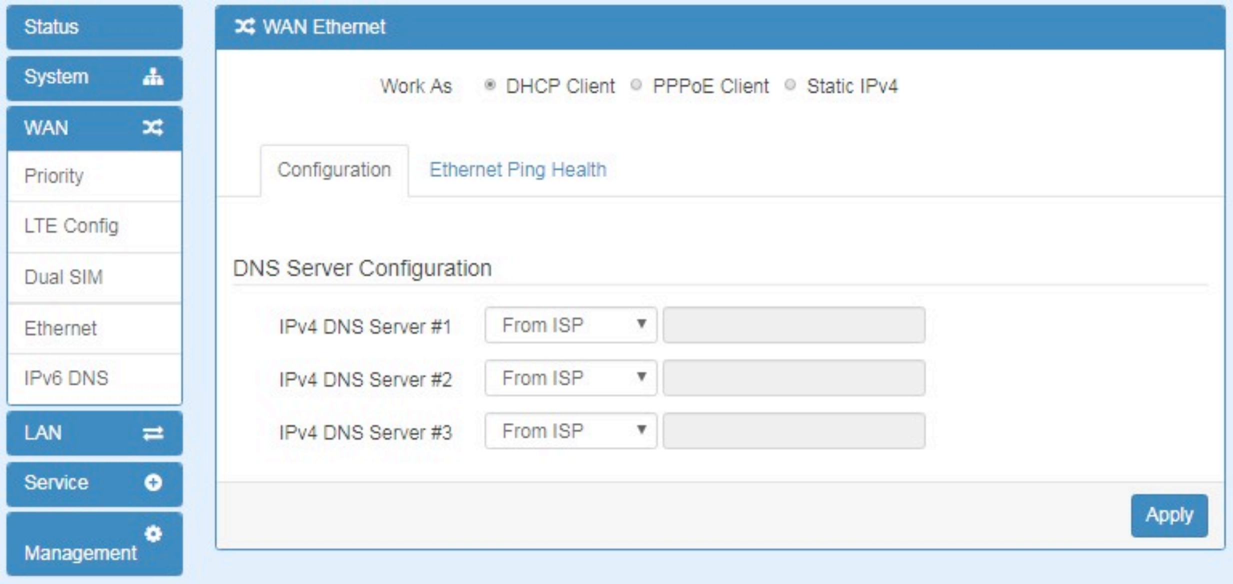
- Auto
- LTE Only
- ETH Only

6.2 WAN > Ethernet

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

6.2.1 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

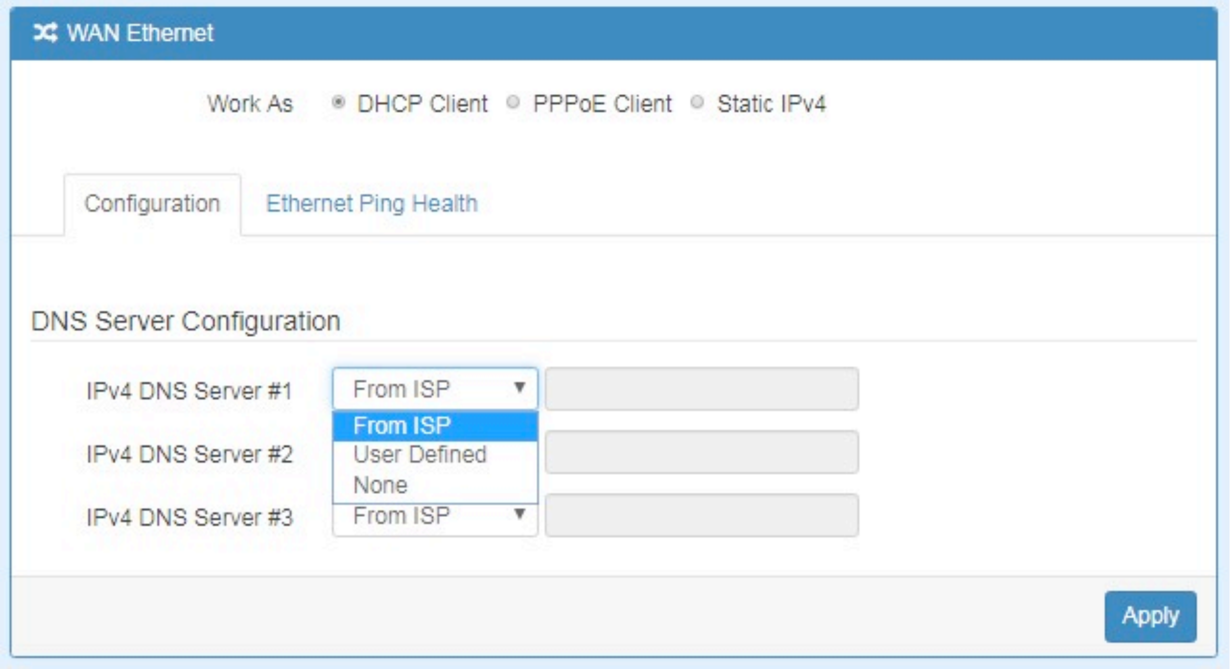
Configuration | Ethernet Ping Health

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.



WAN Ethernet

Work As ● DHCP Client ○ PPPoE Client ○ Static IPv4

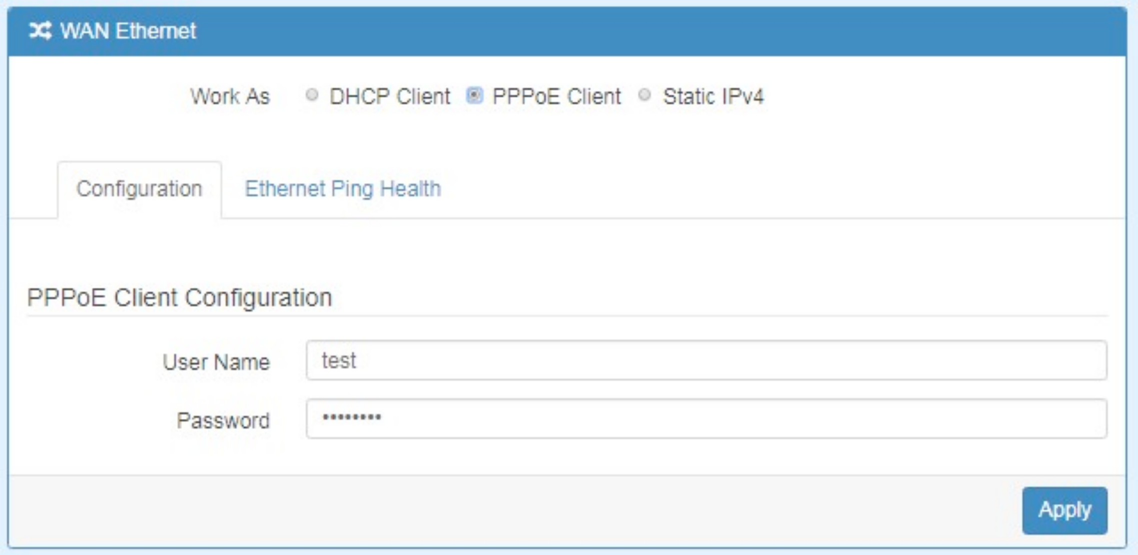
Configuration | Ethernet Ping Health

DNS Server Configuration

IPv4 DNS Server #1: From ISP
IPv4 DNS Server #2
IPv4 DNS Server #3: From ISP

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

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



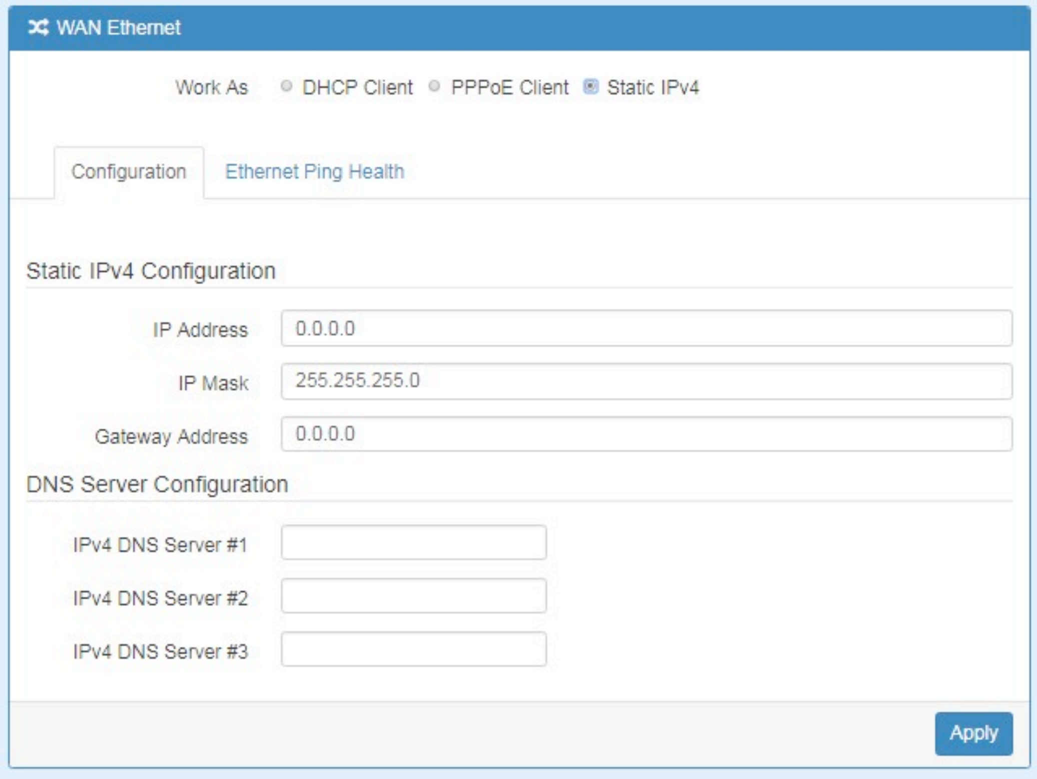
Work As ○ DHCP Client ● PPPoE Client ○ Static IPv4

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

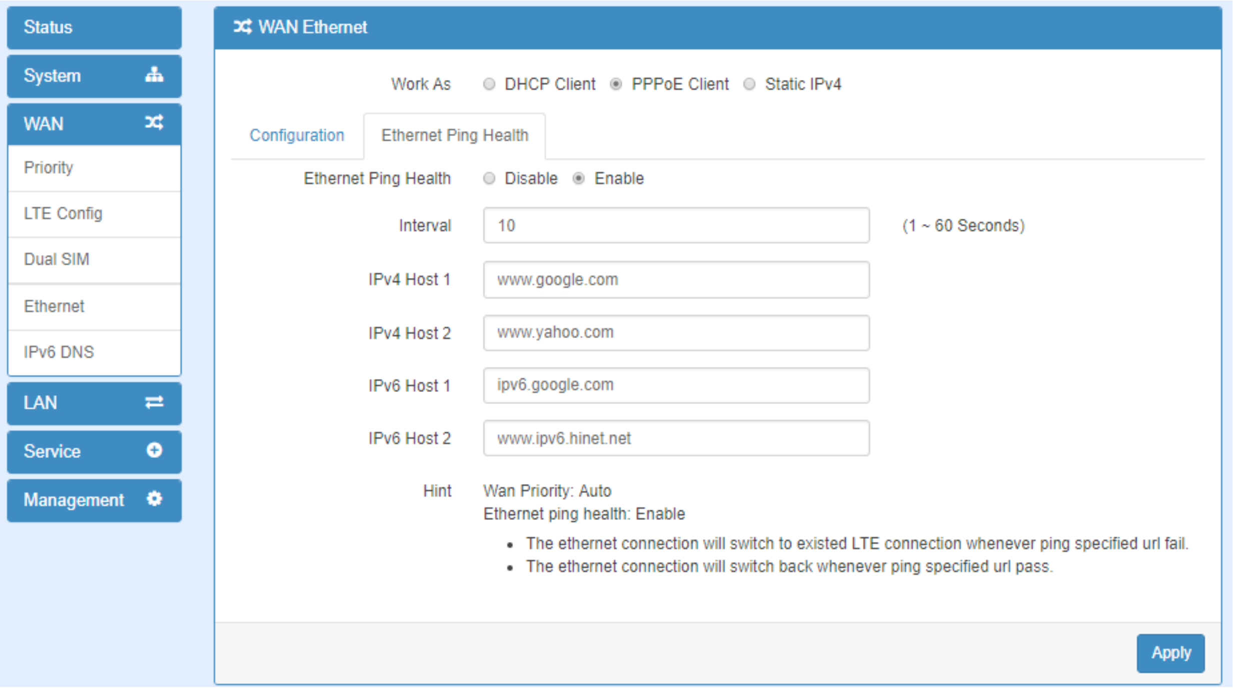
IPv4 DNS Server #2

IPv4 DNS Server #3

WAN > Ethernet	
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.



Work As ○ DHCP Client ● PPPoE Client ○ Static IPv4

Ethernet Ping Health ○ Disable ● Enable

Interval: 10 (1 ~ 60 Seconds)

IPv4 Host 1: www.google.com

IPv4 Host 2: www.yahoo.com

IPv6 Host 1: ipv6.google.com

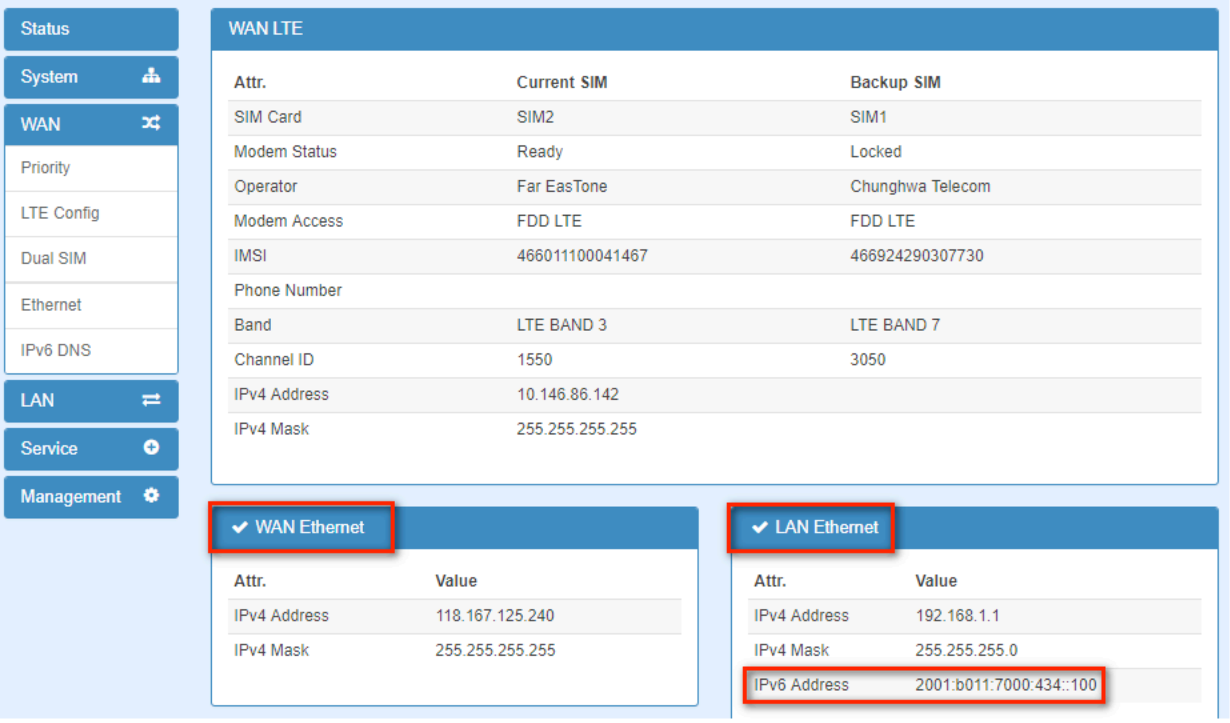
IPv6 Host 2: www.ipv6.hinet.net

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

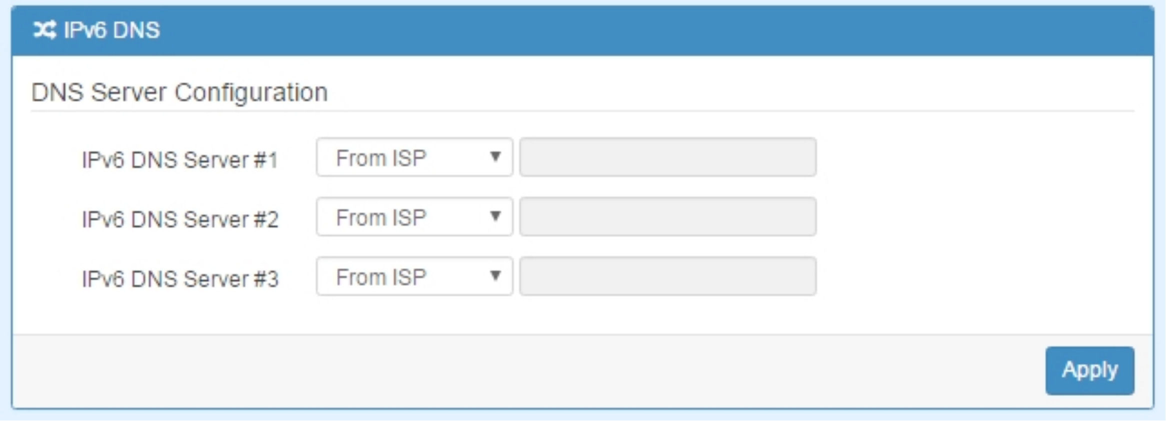
Attr.	Value
IPv4 Address	118.167.125.240
IPv4 Mask	255.255.255.255

✓ 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.



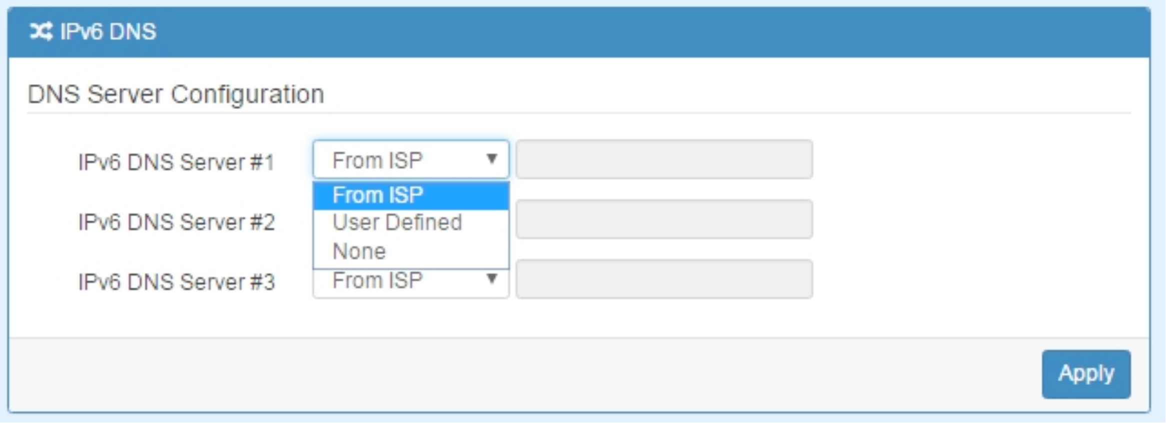
DNS Server Configuration

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.



DNS Server Configuration

IPv6 DNS Server #1 From ISP

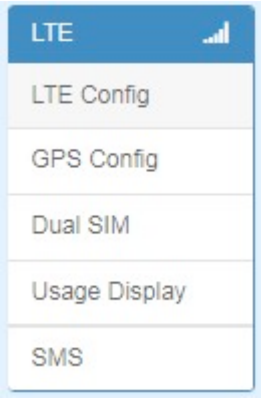
IPv6 DNS Server #2

IPv6 DNS Server #3 From ISP

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

7 Configuration > LTE

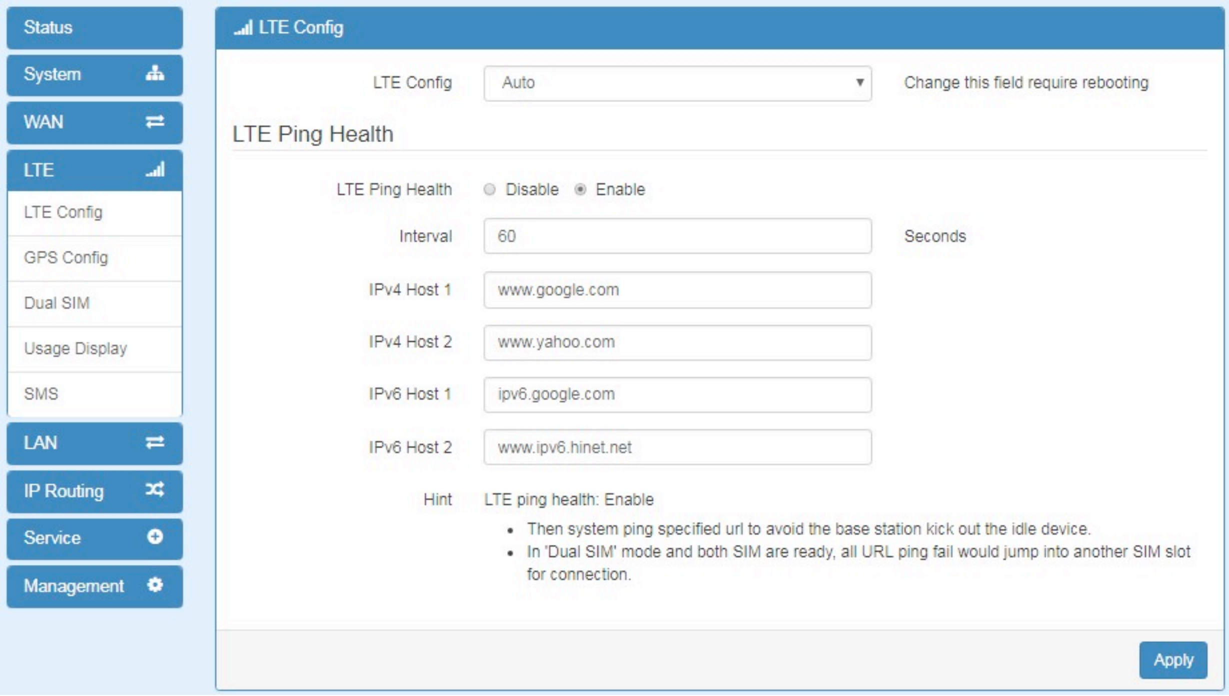
This section allows you to configure LTE Config, GPS Config, Dual SIM, Usage Display and SMS.



7.1 LTE > LTE Config

7.1.1 LTE Configuration

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



LTE Config

LTE Config: Auto ▾ Change this field require rebooting

LTE Ping Health

LTE Ping Health: ○ Disable ● Enable

Interval: 60 Seconds

IPv4 Host 1: www.google.com

IPv4 Host 2: www.yahoo.com

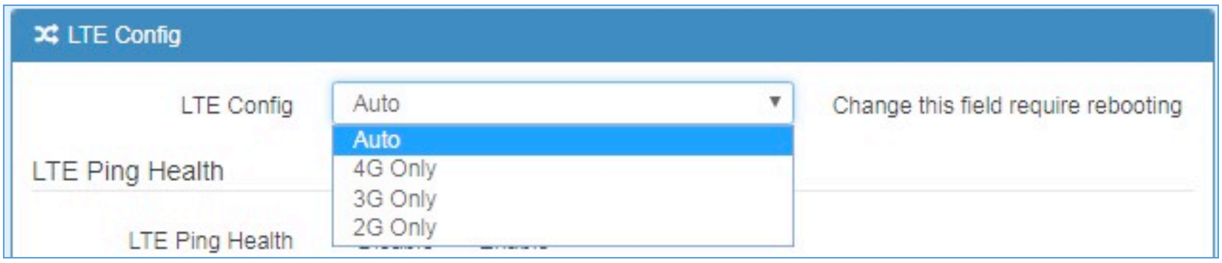
IPv6 Host 1: ipv6.google.com

IPv6 Host 2: www.ipv6.hinet.net

Hint: LTE ping health: Enable

- Then system ping specified url 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.

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

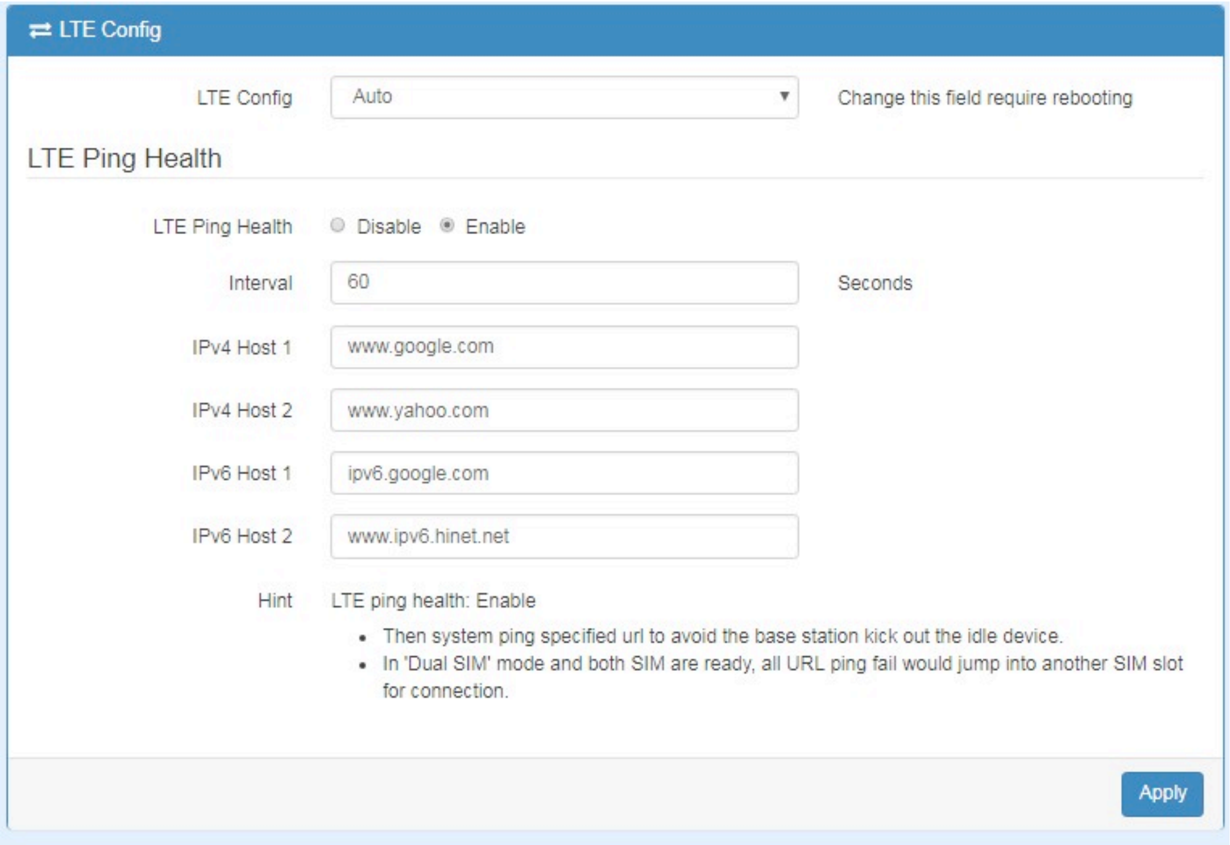


LTE > LTE Config	
Item	**Description**
Auto	Automatically connect the possible band.
4G Only	Connect to 4G network only.
3G Only	Connect to 3G network only.
2G Only	Connect to 2G network only.

7.1.2 LTE Ping Health

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

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



LTE Config: Auto ▾ Change this field require rebooting

LTE Ping Health

LTE Ping Health ○ Disable ● Enable

Interval: 60 Seconds

IPv4 Host 1: www.google.com

IPv4 Host 2: www.yahoo.com

IPv6 Host 1: ipv6.google.com

IPv6 Host 2: www.ipv6.hinet.net

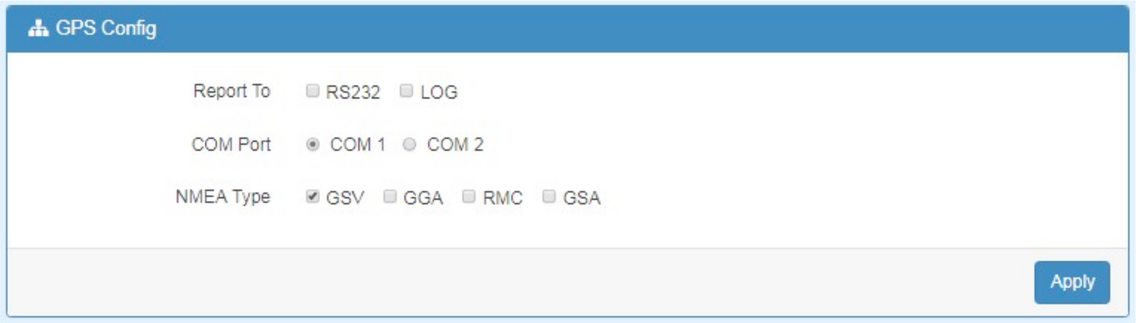
Hint: LTE ping health: Enable

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

7.2 LTE > GPS Config

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



GPS Config

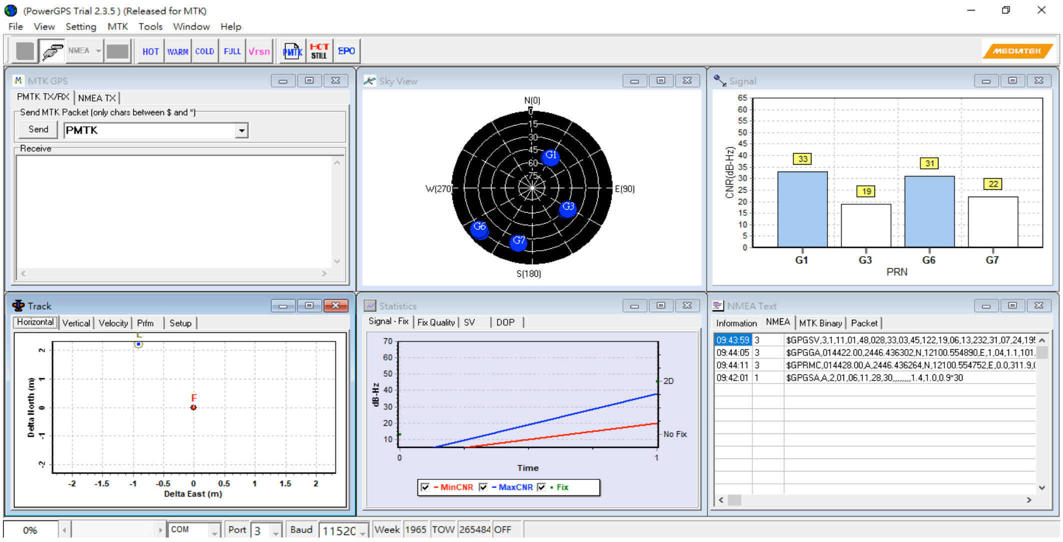
Report To □ RS232 □ LOG

COM Port ● COM 1 ○ COM 2

NMEA Type ☑ GSV □ GGA □ RMC □ GSA

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.

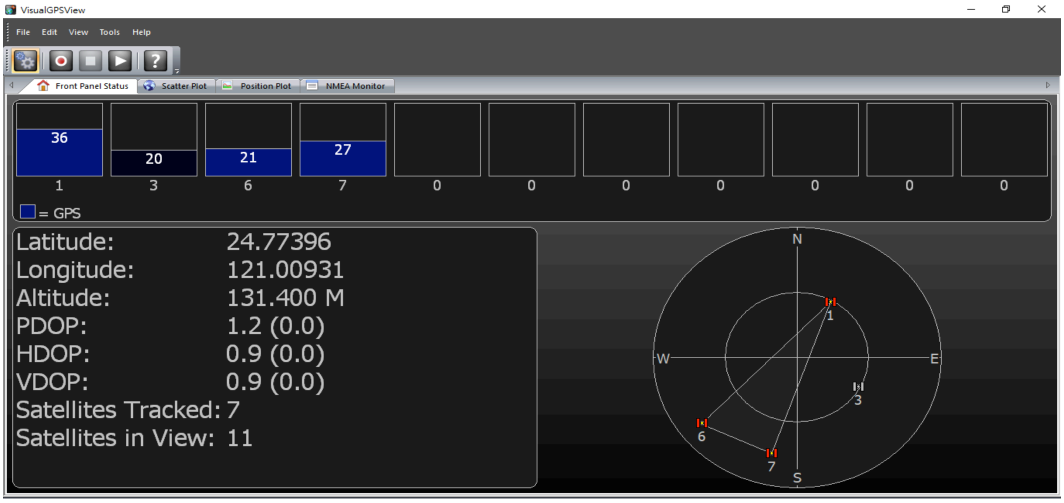
For example, you can use some software depending on your requirements and activate the GPS Configuration to display what information you need from your selecting software.



(PowerGPS Trial 2.3.5) (Released for MTK)
File View Setting MTK Tools Window Help
HOT WARM COLD FULL Vrsn PMTK EPO
MEDIATEK
MTK GPS
PMTK TX/RX NMEA TX
Send MTK Packet (only chars between $ and *)
Send PMTK
Receive
Sky View
N(0) E(90) S(180) W(270)
G1 G3 G6 G7
Signal
CNR(dB-Hz)
33 19 31 22
G1 G3 G6 G7
PRN
Track
Horizontal Vertical Velocity Pfm Setup
Delta North (m)
Delta East (m)
Statistics
Signal - Fix Fix Quality SV DOP
dB-Hz
Time
2D
No Fix
MinCNR MaxCNR Fix
NMEA Text
Information NMEA MTK Binary Packet

```
09:43:59 3 $GPGSV,3,1,11,01,48,028,33,03,45,122,19,06,13,232,31,07,24,195
09:44:05 3 $GPGGA,014422.00,2446.436302,N,12100.554890,E,1,04,1.1,101.
09:44:11 3 $GPRMC,014428.00,A,2446.436264,N,12100.554752,E,0.0,311.9,0
09:42:01 1 $GPGSA,A,2,01,06,11,28,30,,,,,,,,1.4,1.0,0.9*30
```

0% COM Port 3 Baud 11520 Week 1965 TOW 265484 OFF

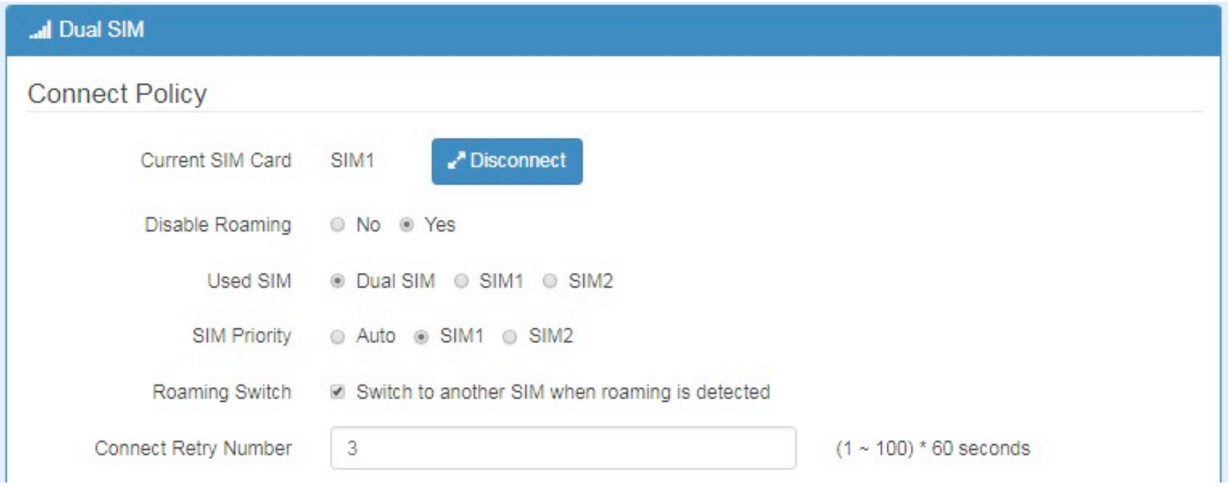


VisualGPSView
File Edit View Tools Help
Front Panel Status Scatter Plot Position Plot NMEA Monitor
36 20 21 27
1 3 6 7 0 0 0 0 0 0 0
= GPS
N S E W
1 3 6 7

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: SIM1 [Disconnect]

Disable Roaming: ○ No ● Yes

Used SIM: ● Dual SIM ○ SIM1 ○ SIM2

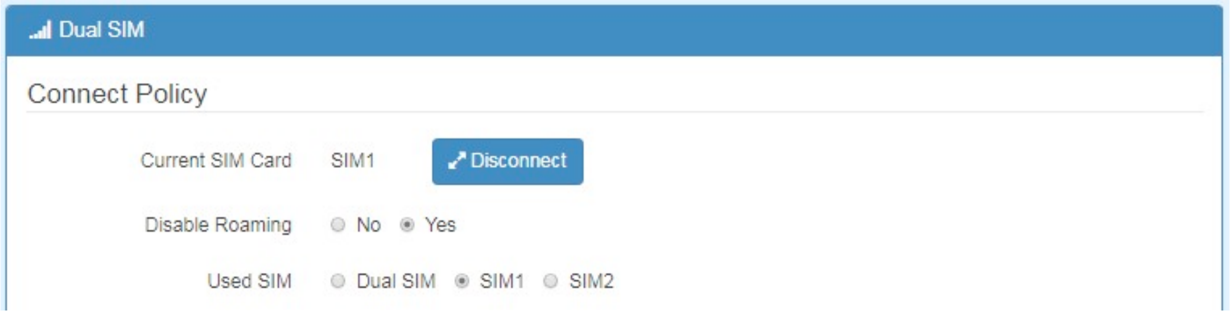
SIM Priority: ○ Auto ● SIM1 ○ SIM2

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

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

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

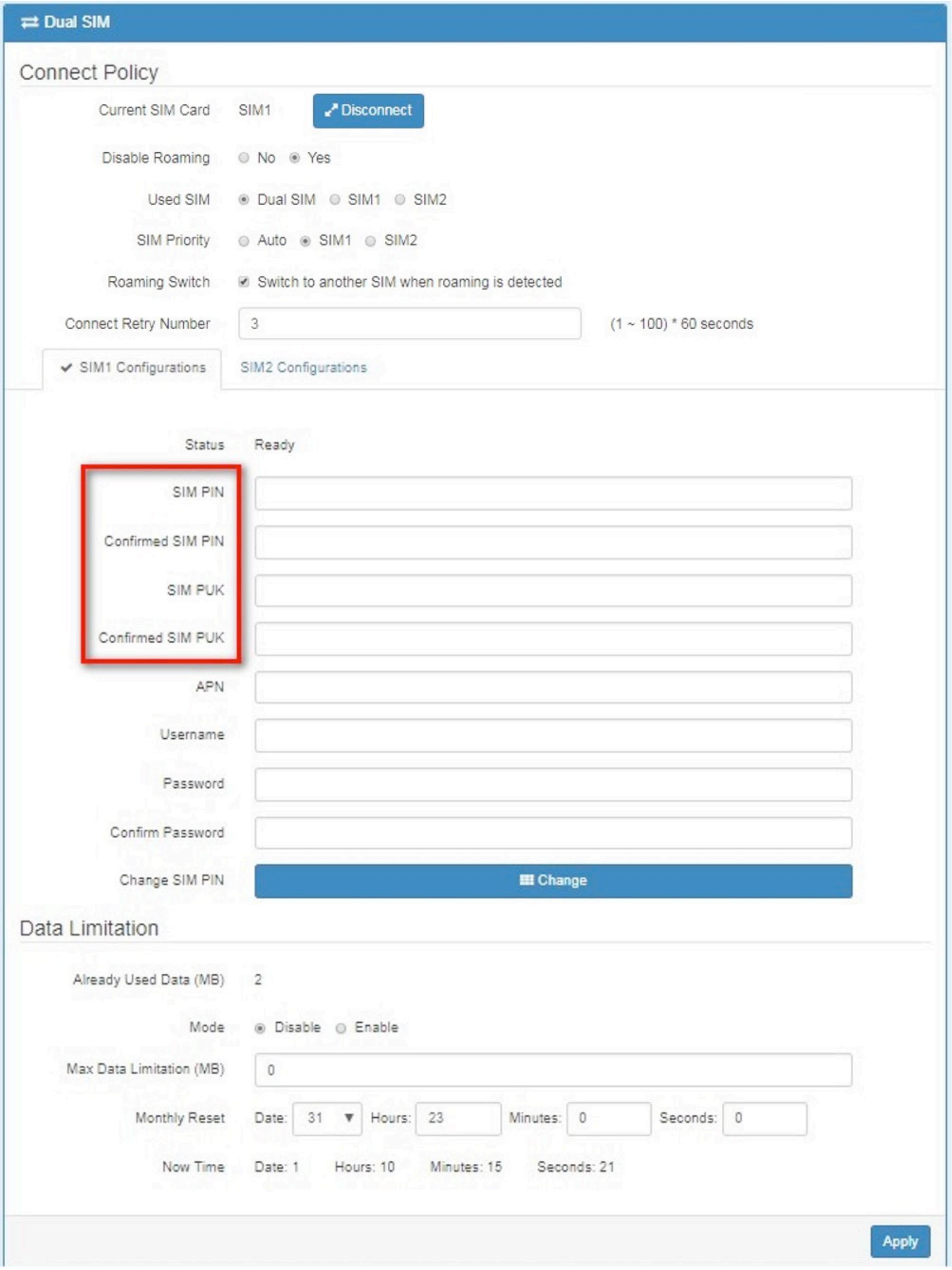
Current SIM Card: SIM1 [Disconnect]

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



⇄ Dual SIM

Connect Policy

Current SIM Card: SIM1

Disable Roaming: ○ No ● Yes

Used SIM: ● Dual SIM ○ SIM1 ○ SIM2

SIM Priority: ○ Auto ● SIM1 ○ SIM2

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

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

✓ SIM1 Configurations | SIM2 Configurations

Status: Ready

SIM PIN:

Confirmed SIM PIN:

SIM PUK:

Confirmed SIM PUK:

APN:

Username:

Password:

Confirm Password:

Change SIM PIN: Change

Data Limitation

Already Used Data (MB): 2

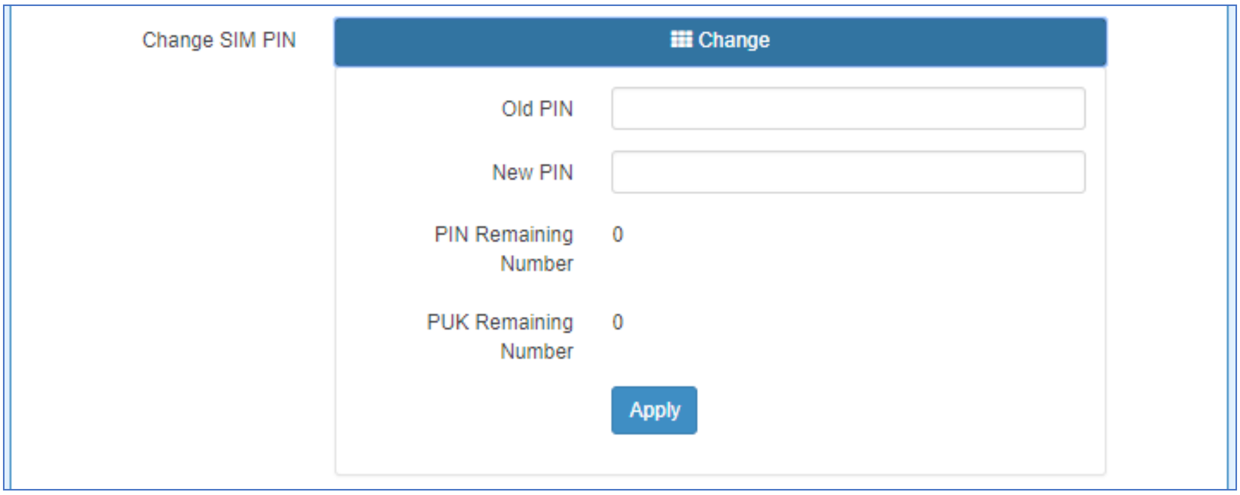
Mode: ● Disable ○ Enable

Max Data Limitation (MB): 0

Monthly Reset: Date: 31 ▼ Hours: 23 Minutes: 0 Seconds: 0

Now Time: Date: 1 Hours: 10 Minutes: 15 Seconds: 21

- **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).

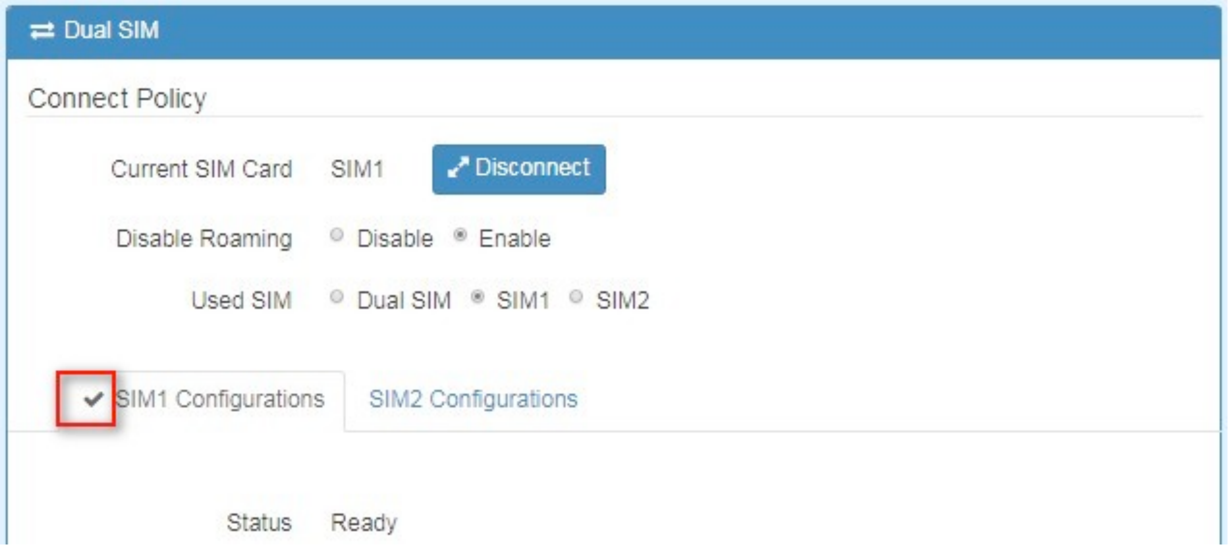


Change SIM PIN

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

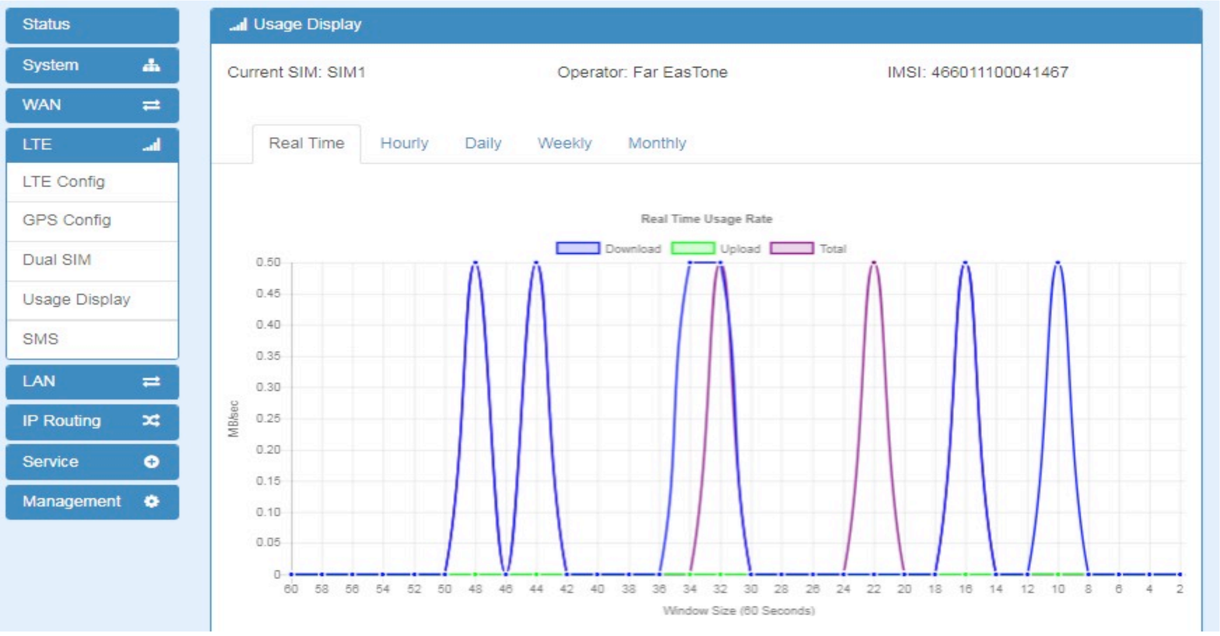
Used SIM ○ Dual SIM ● SIM1 ○ SIM2

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

7.4 TE > Usage Display

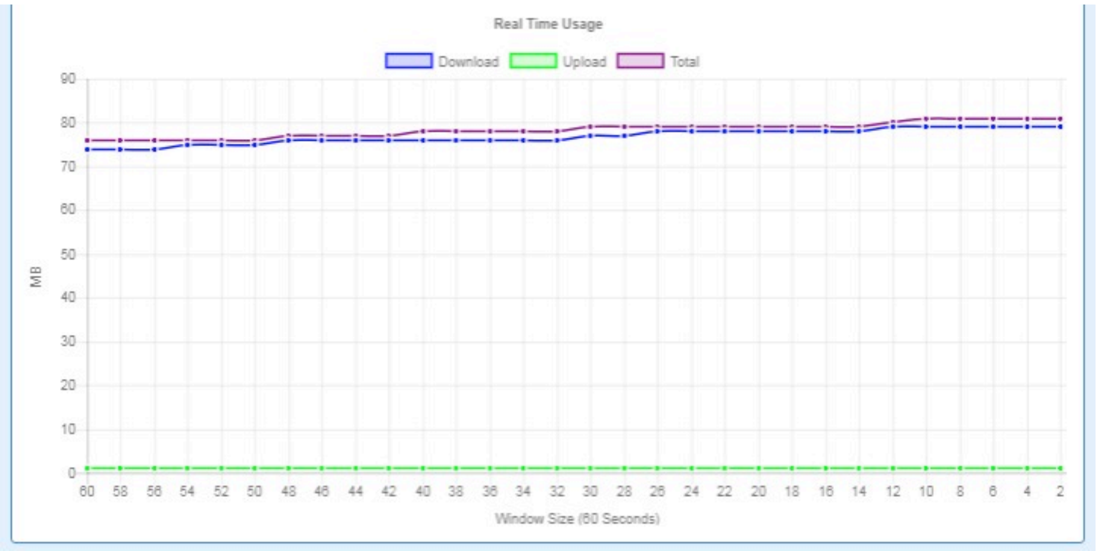
This section shows the status of **current SIM card**, **operator**, **IMSI** and the charts for **Real Time**, **Hourly**, **Daily**, **Weekly**, and **Monthly**.



Current SIM: SIM1

Operator: Far EasTone

IMSI: 466011100041467



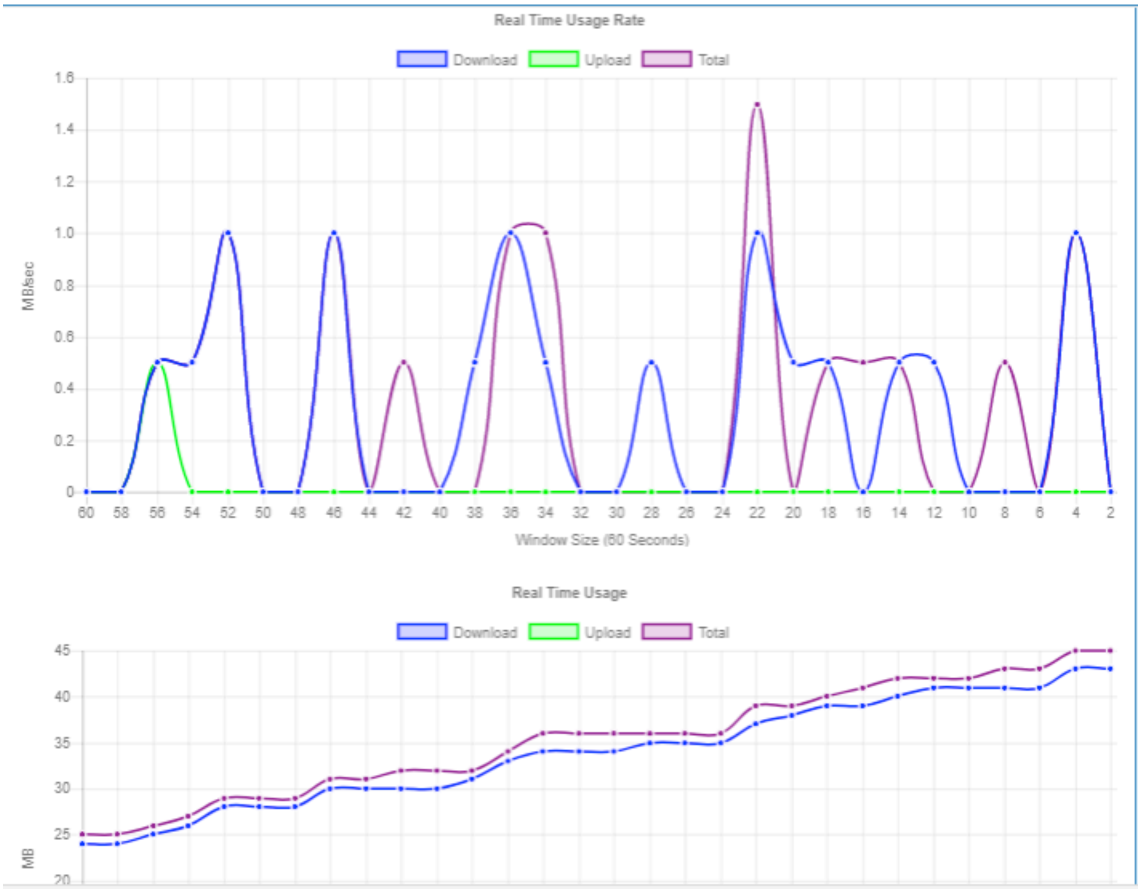
(1) Real-Time Usage:

- **Real-Time Usage Rate:**

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

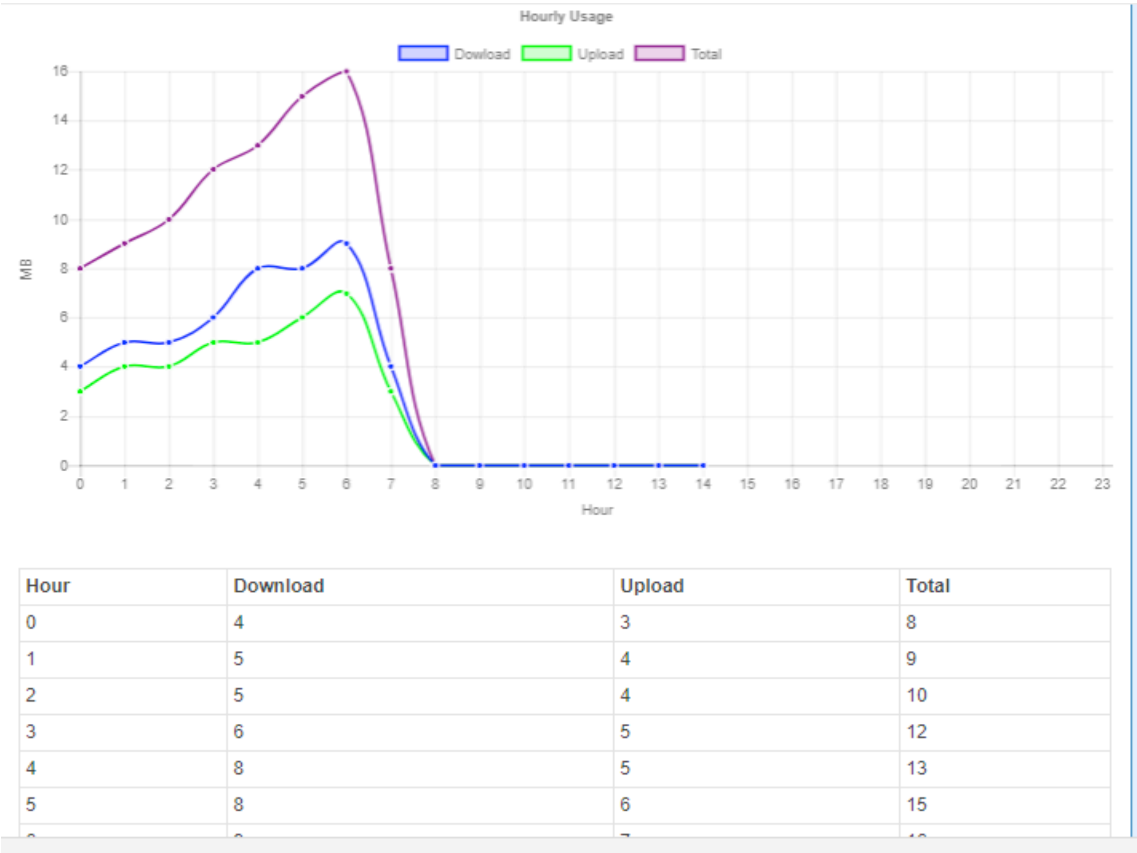
- **Real-Time Usage:**

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



(2) Hourly Usage:

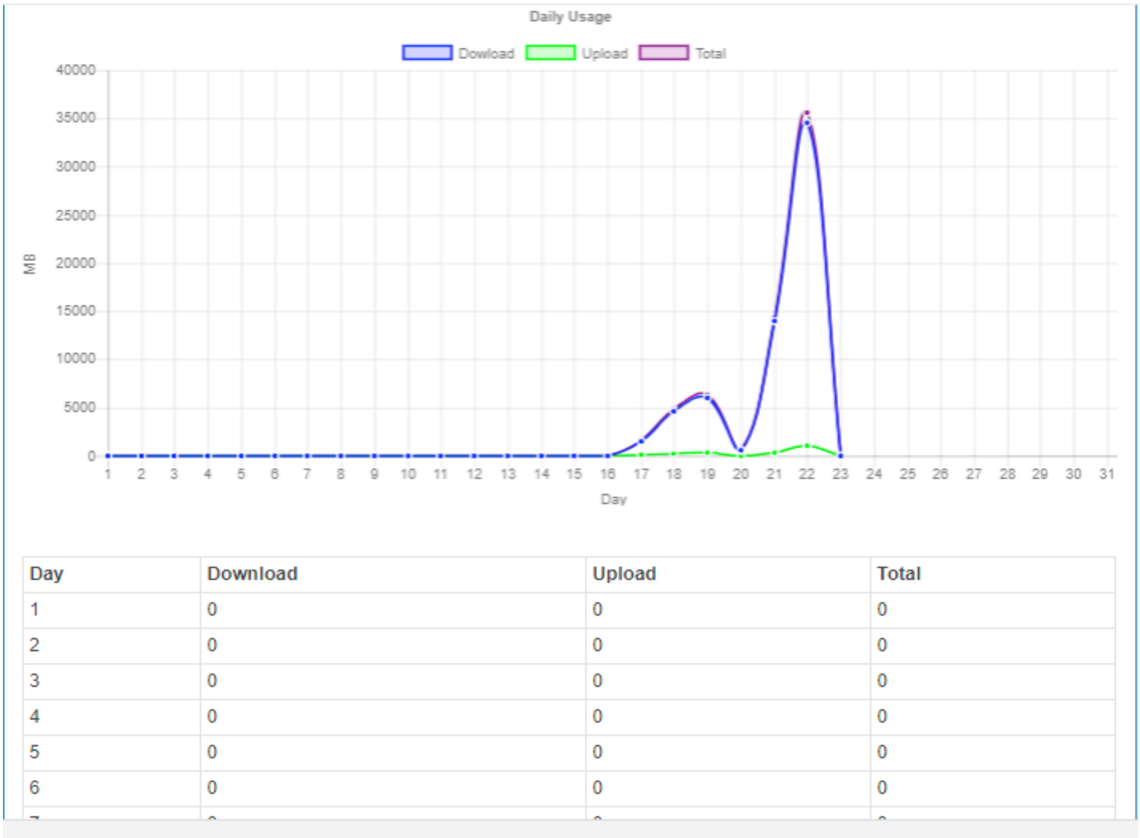
It displays Download/Upload/Total MB per hour in one day for current using SIM card and the view window size is 24 hours.



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

(3) Daily Usage:

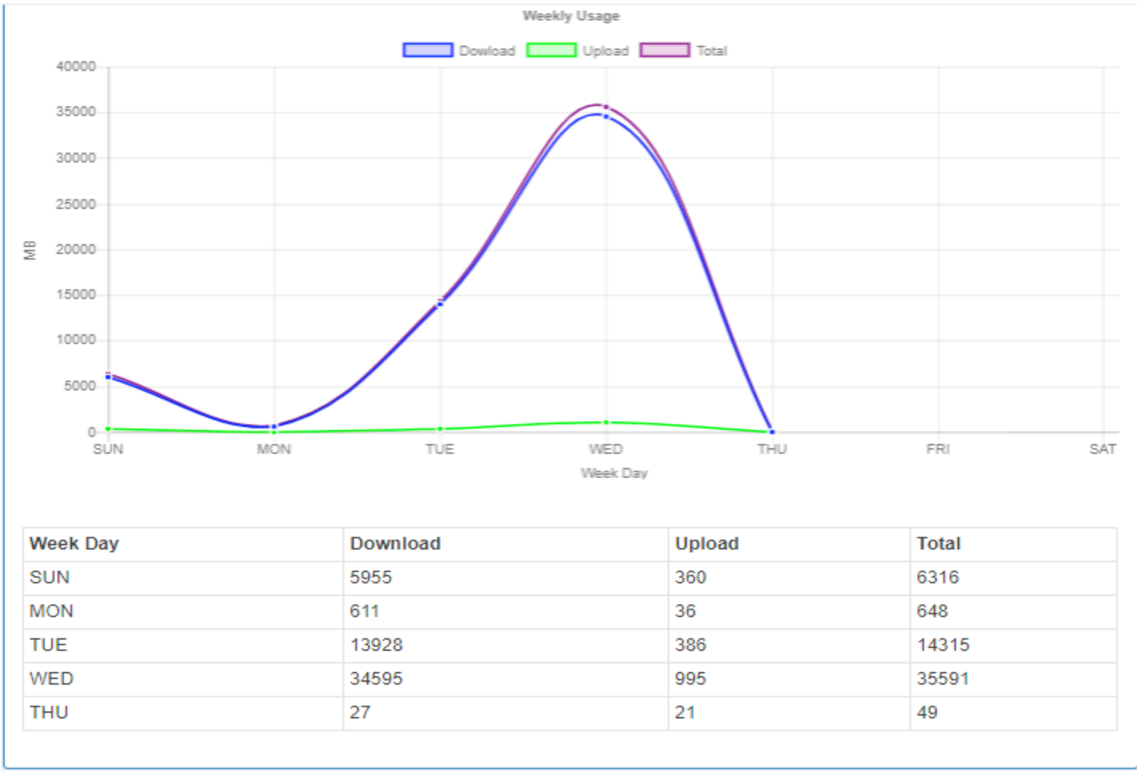
It displays Download/Upload/Total MB per day in one month for current using SIM card and the view window size is 31 days.



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

(4) Weekly Usage:

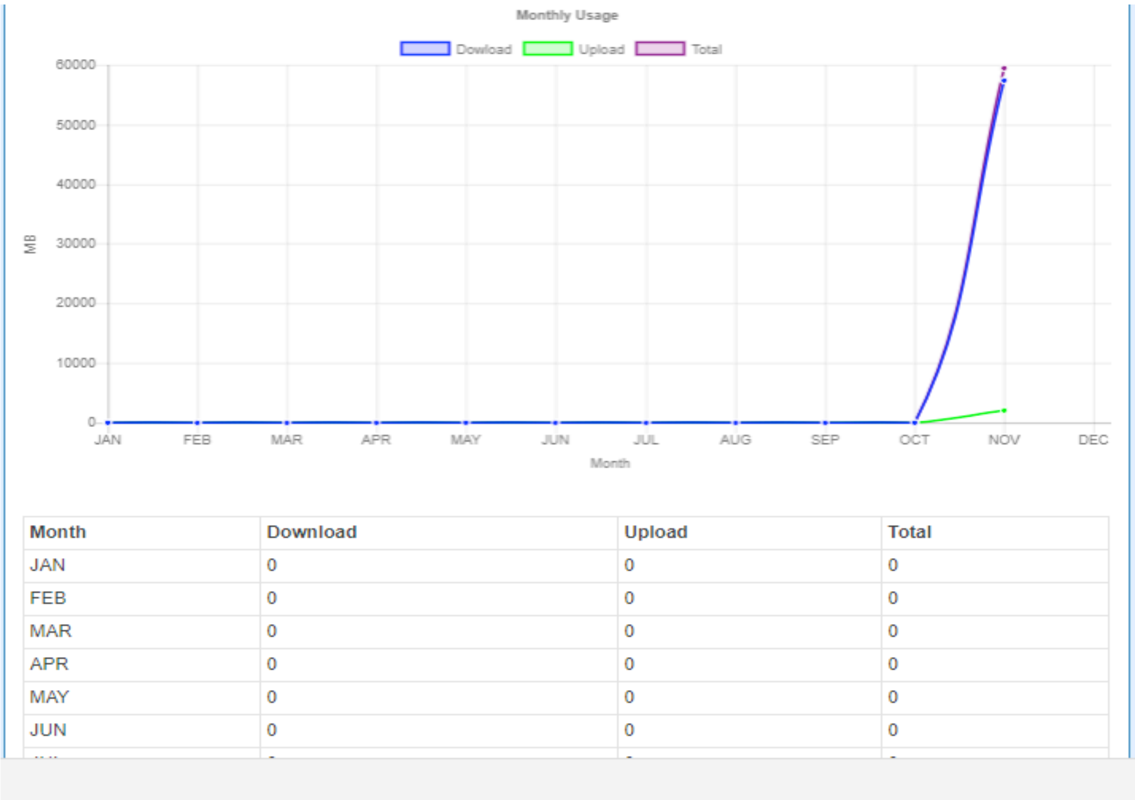
It displays Download/Upload/Total MB per day in one week for current using SIM card and the view window size is 7 days.



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

(5) Monthly Usage:

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

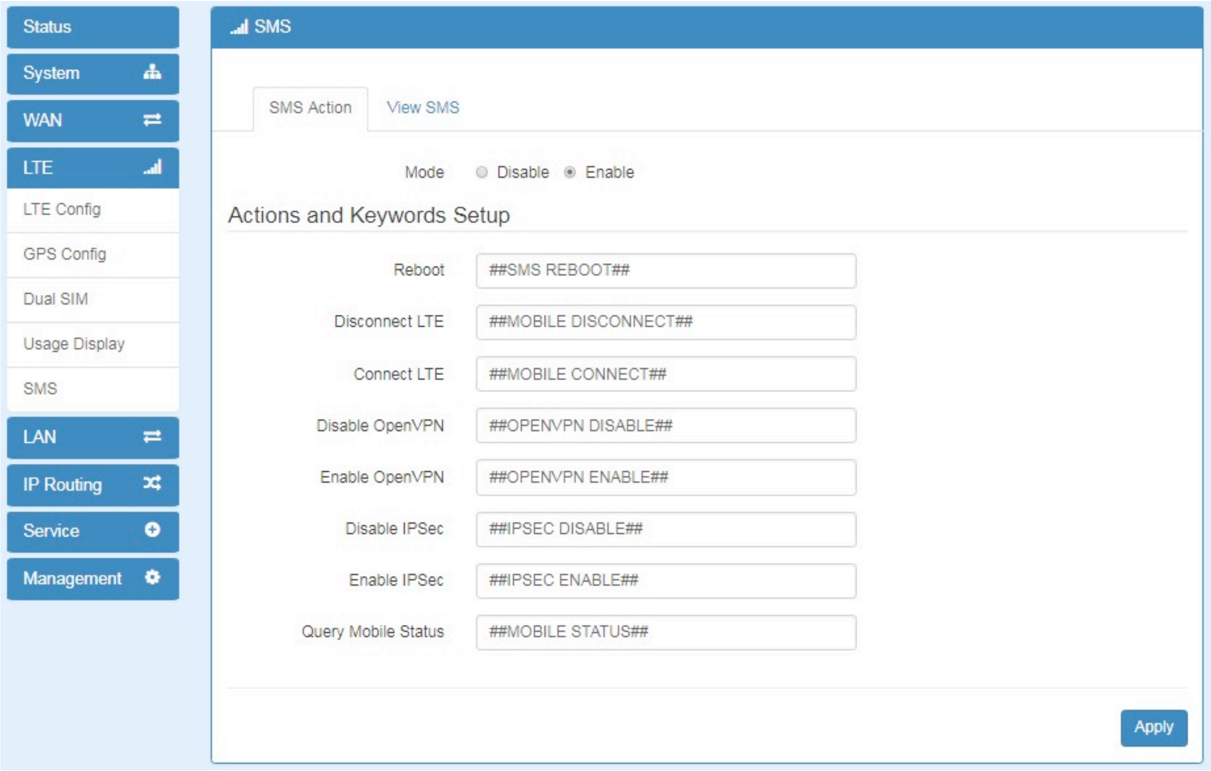


Month	Download	Upload	Total
JAN	0	0	0
FEB	0	0	0
MAR	0	0	0
APR	0	0	0
MAY	0	0	0
JUN	0	0	0

7.5 LTE > SMS

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

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

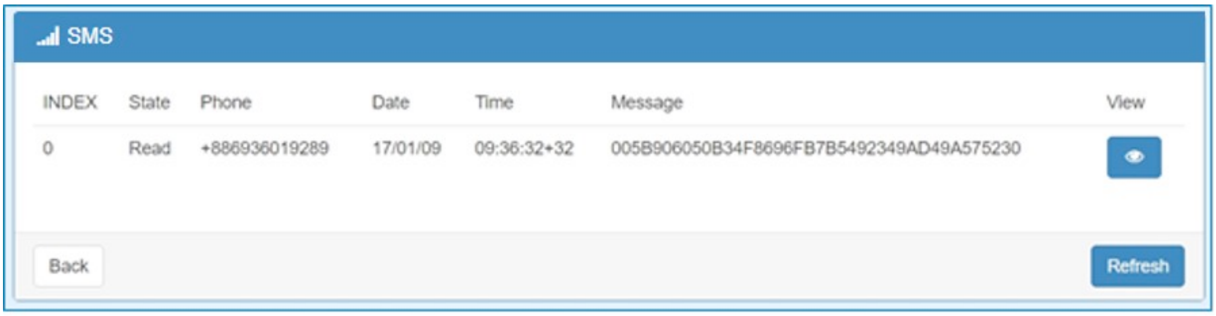


Mode ○ Disable ● Enable

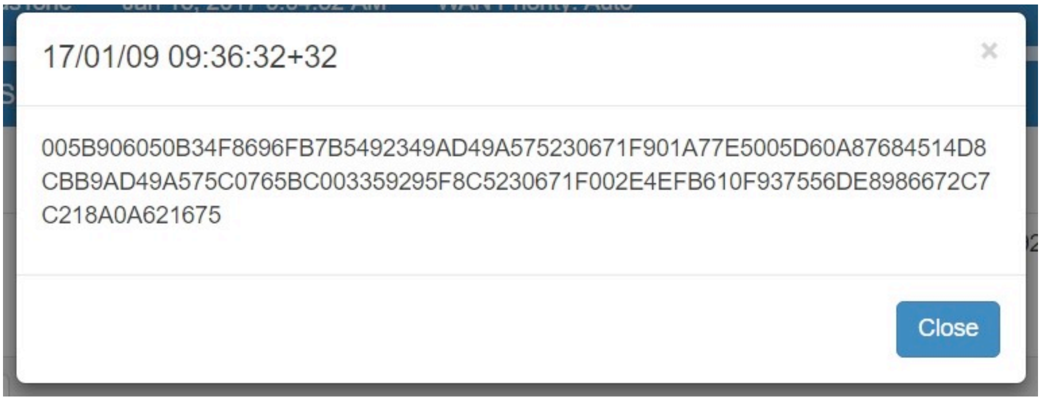
Actions and Keywords Setup

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##

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



INDEX	State	Phone	Date	Time	Message	View
0	Read	+886936019289	17/01/09	09:36:32+32	005B906050B34F8696FB7B5492349AD49A575230	

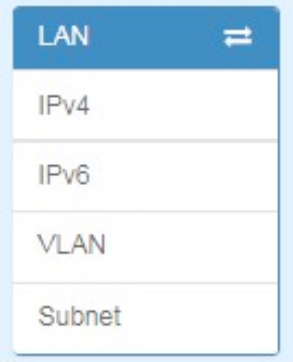


17/01/09 09:36:32+32

005B906050B34F8696FB7B5492349AD49A575230671F901A77E5005D60A87684514D8CBB9AD49A575C0765BC003359295F8C5230671F002E4EFB610F937556DE8986672C7C218A0A621675

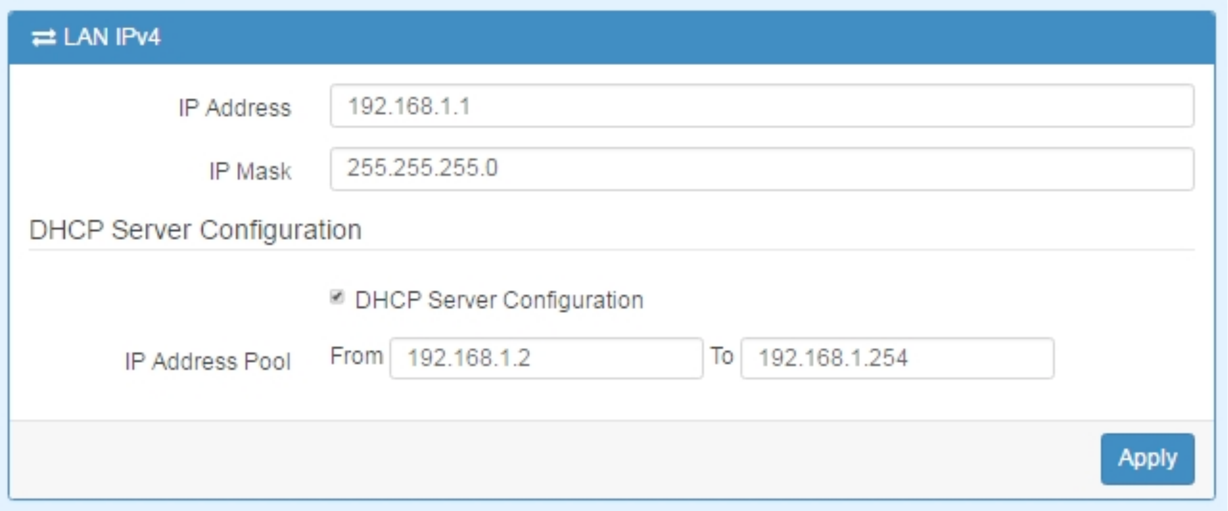
8 Configuration > LAN

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



8.1 LAN > IPv4

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



⇄ LAN IPv4

IP Address: 192.168.1.1

IP Mask: 255.255.255.0

DHCP Server Configuration

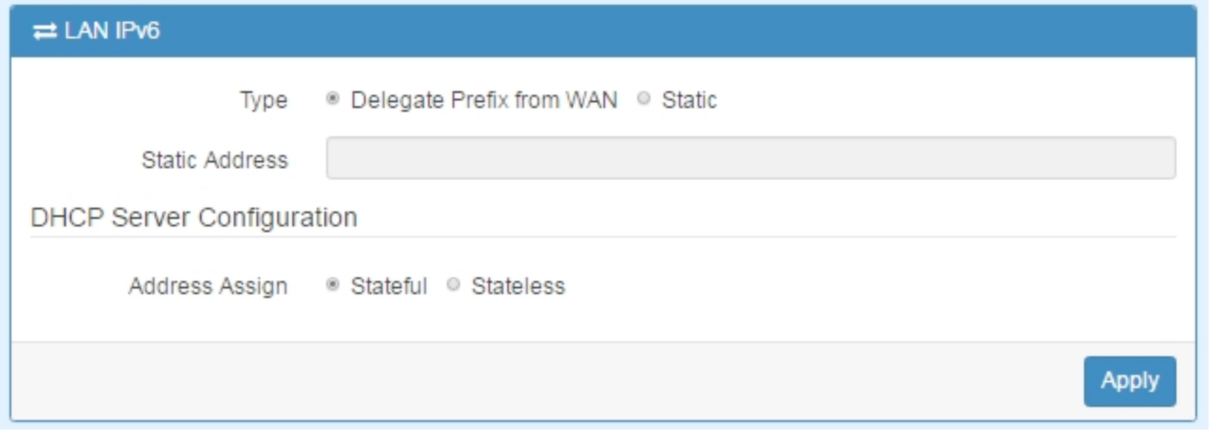
☑ DHCP Server Configuration

IP Address Pool: From 192.168.1.2 To 192.168.1.254

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

8.2 LAN > IPv6

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



⇄ LAN IPv6

Type ● Delegate Prefix from WAN ○ Static

Static Address

DHCP Server Configuration

Address Assign ● Stateful ○ Stateless

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

8.3 LAN > VLAN

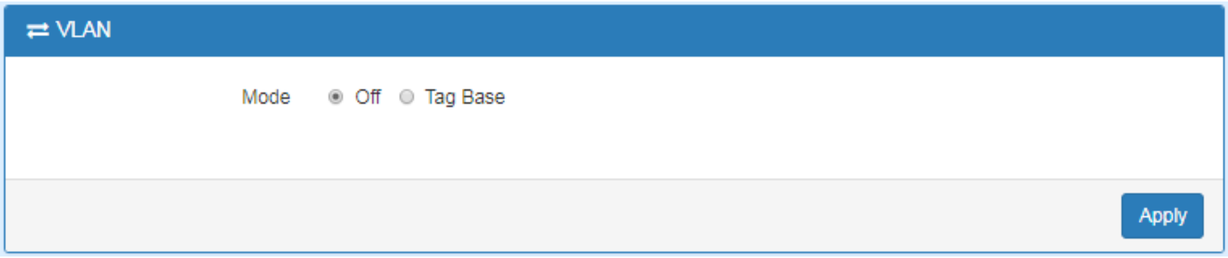
This section allows you to set up VLAN that provides a network segmentation system to distinguish the LAN clients and separate them into different LAN subnet for enhancing security and controlling traffic.

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

- Type 1:

For **1-port LAN** router model, you can use the **Type 1** to configure VLAN. First, the **VLAN**

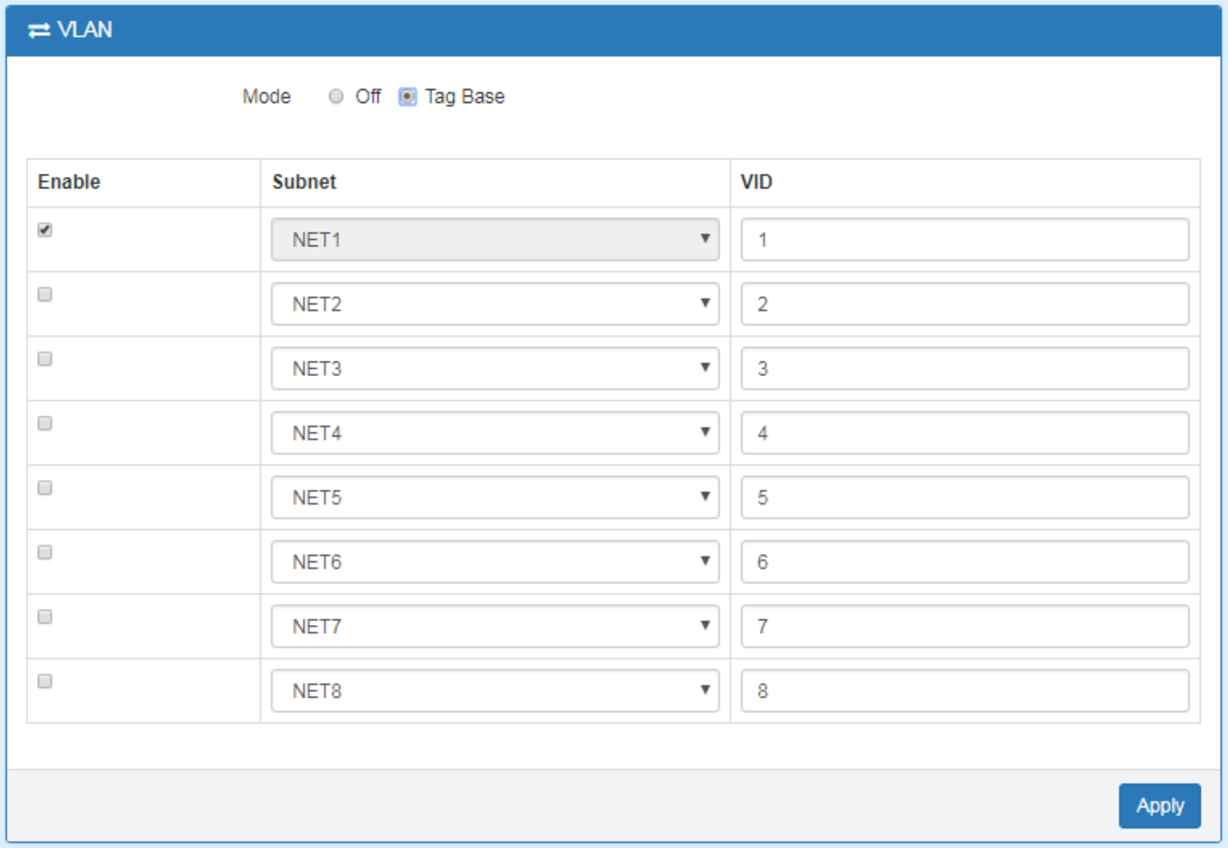
Mode allows you to select **Off** or **Tag Base (802.1p)**.



Mode ● Off ○ Tag Base

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

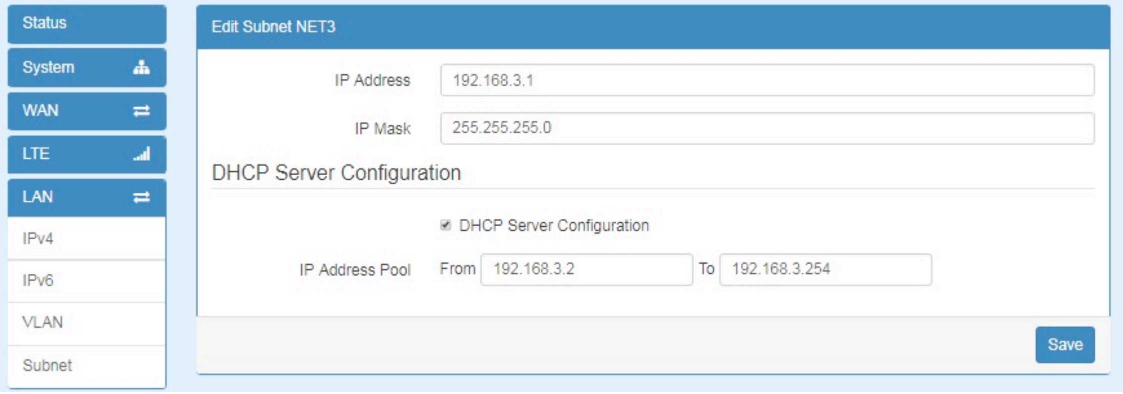
For each row, the settings can be enabled or disabled by checkbox and select the **Subnet** and the **VLAN ID (VID)**. The **Subnet** sets up the IP address and IP mask for the router so this router can communicate with the third party by this IP address and IP mask on this VLAN. (***Note:*** The NET1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



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 will show the Subnet window from the LAN catalogue.)



Edit Subnet NET3

IP Address: 192.168.3.1

IP Mask: 255.255.255.0

DHCP Server Configuration

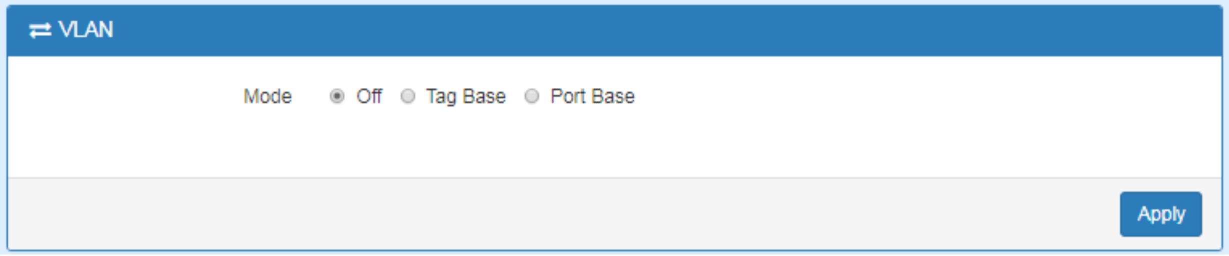
☑ DHCP Server Configuration

IP Address Pool From 192.168.3.2 To 192.168.3.254

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

- Type 2:

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


⇄ VLAN

Mode ● Off ○ Tag Base ○ Port Base

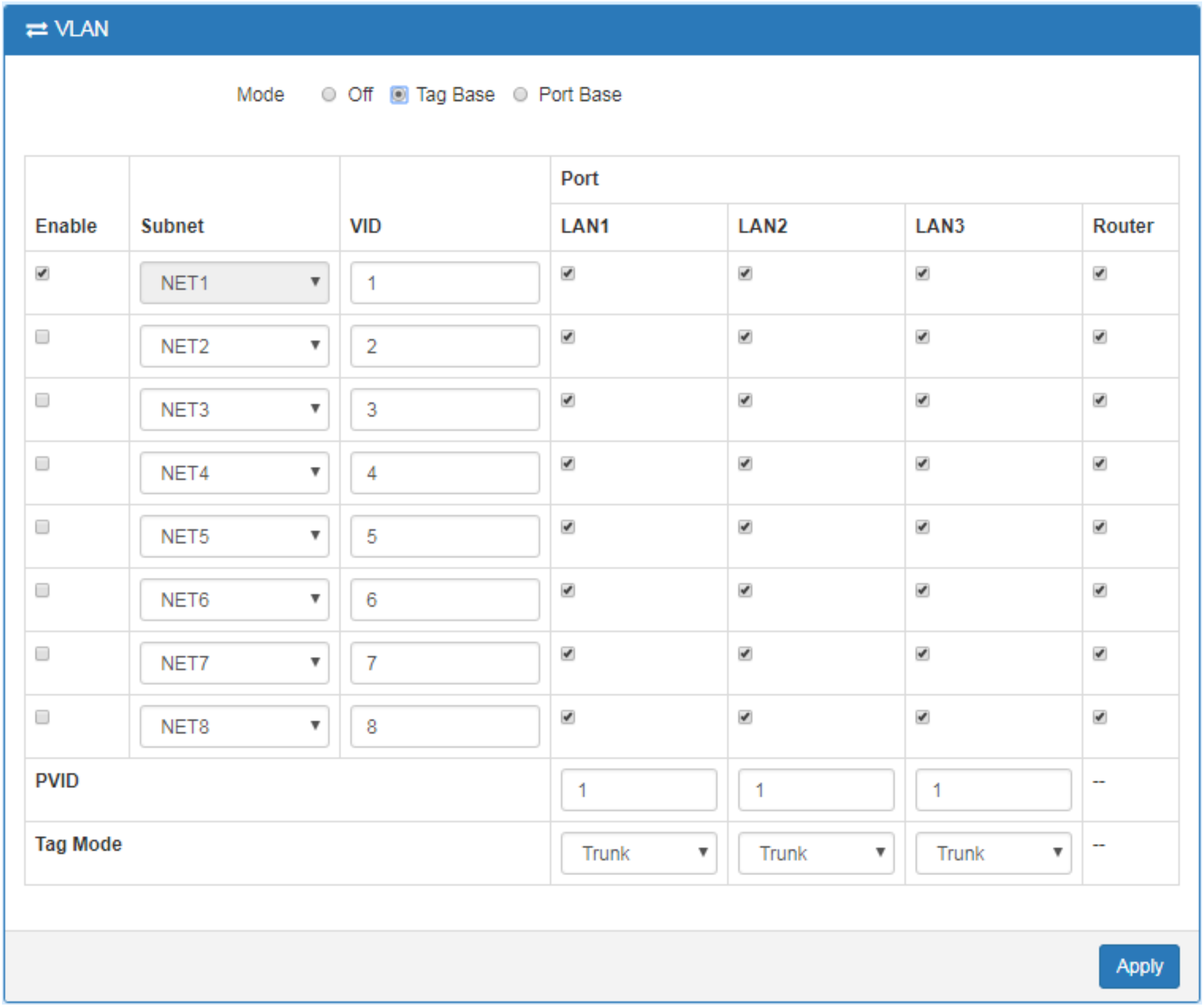
When VLAN Mode is set to **Tag Base**, the VLAN setting window will appear as shown below.

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

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

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

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



⇄ VLAN

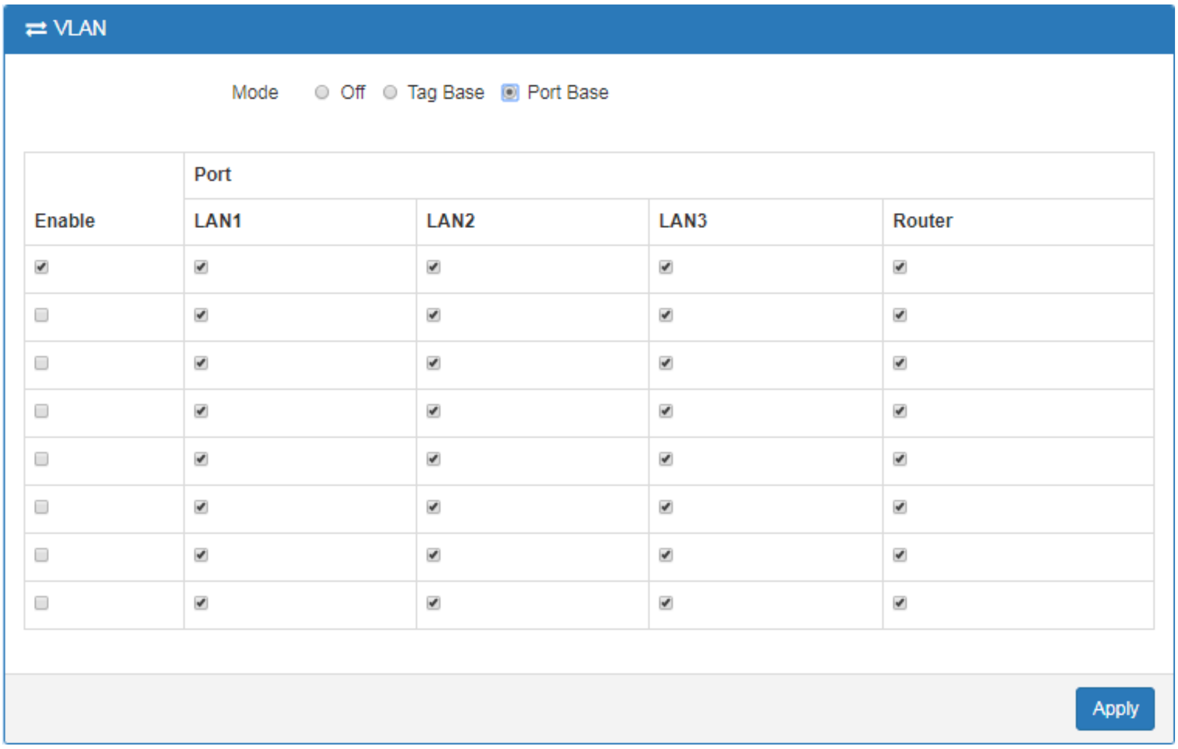
Mode ○ Off ● Tag Base ○ Port Base

Enable	Subnet	VID	Port 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 ▾	--

Apply

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

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



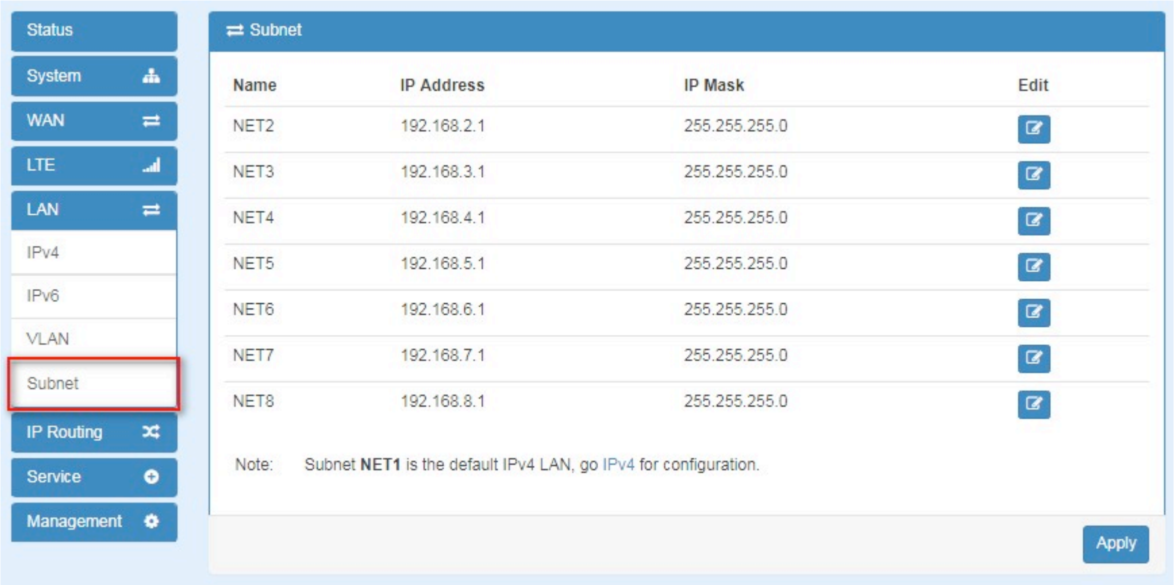
Mode ○ Off ○ Tag Base ● Port Base

	Port			
Enable	LAN1	LAN2	LAN3	Router
☑	☑	☑	☑	☑
□	☑	☑	☑	☑
□	☑	☑	☑	☑
□	☑	☑	☑	☑
□	☑	☑	☑	☑
□	☑	☑	☑	☑
□	☑	☑	☑	☑
□	☑	☑	☑	☑

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

8.4 LAN > Subnet

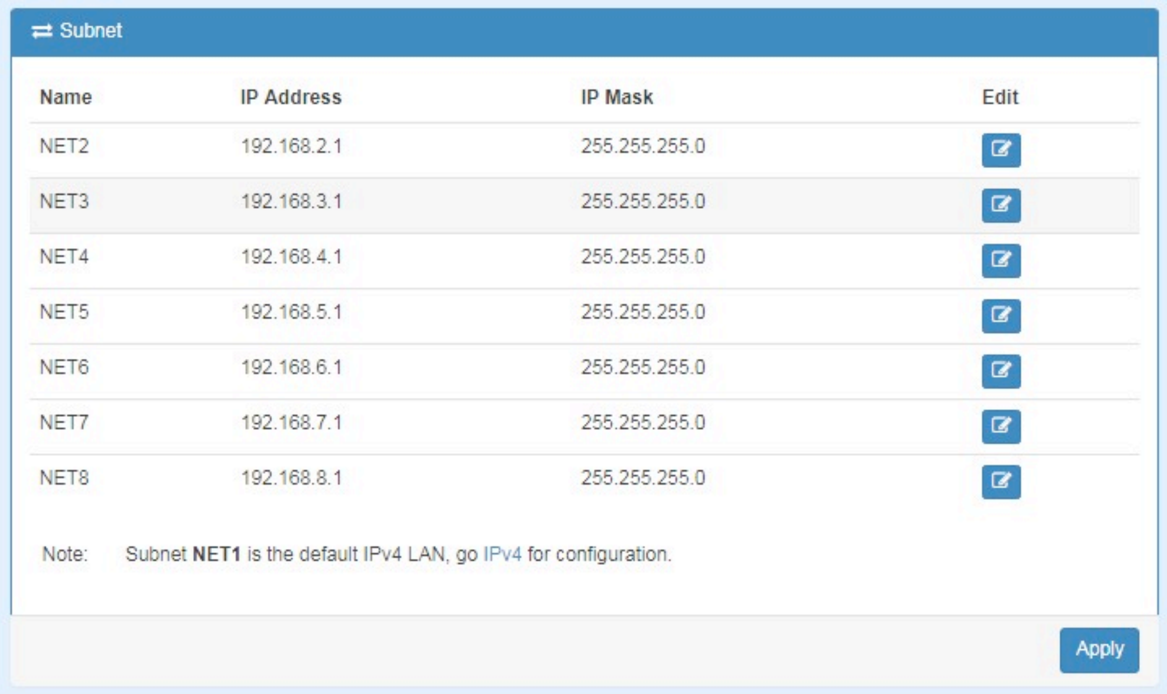
This section allows you to get the information of IP Address and IP Mask and edit for the Subnets from DHCP Server Configuration.



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.

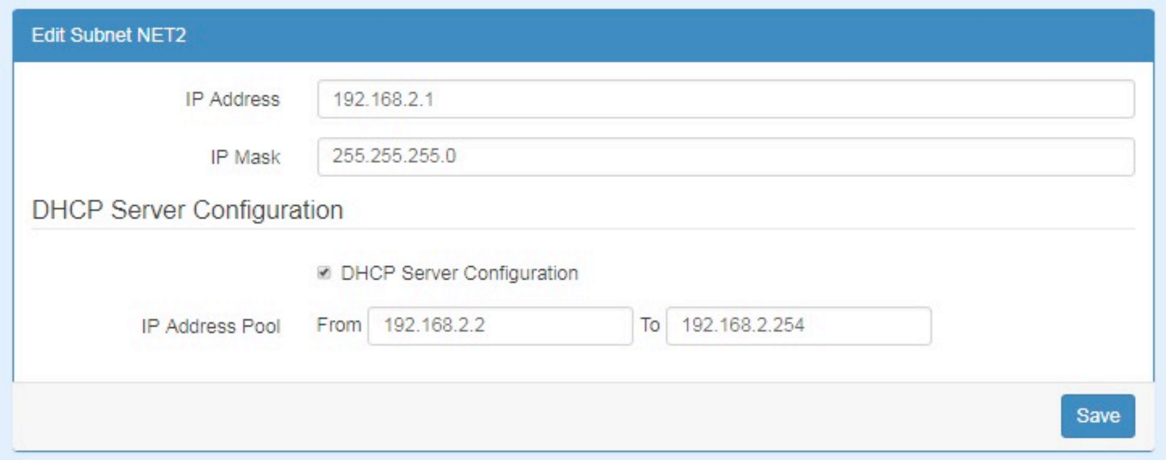
This **Subnet** setting is the same with LAN->IPv4 setting and follows with Tag Base Mode of VLAN to enable the function.



⇄ 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.



Edit Subnet NET2

IP Address: 192.168.2.1

IP Mask: 255.255.255.0

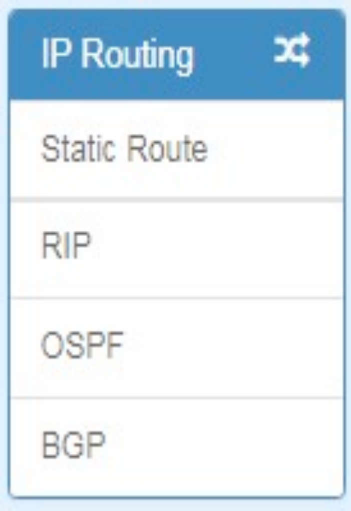
DHCP Server Configuration

☑ DHCP Server Configuration

IP Address Pool: From 192.168.2.2 To 192.168.2.254

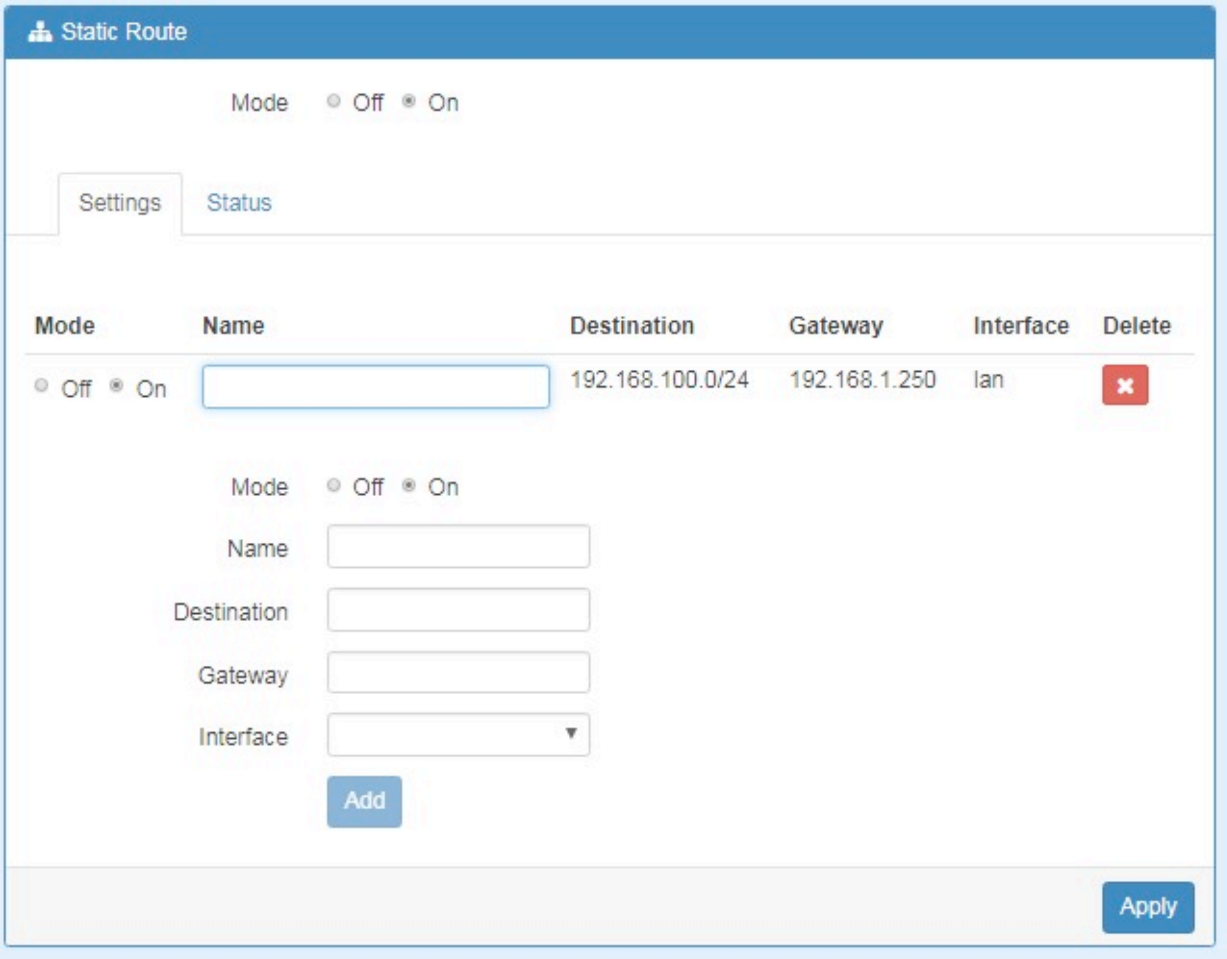
9 IP Routing

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



9.1 IP Routing > Static Route

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



Mode ○ Off ● On

Mode	Name	Destination	Gateway	Interface	Delete
○ Off ● On		192.168.100.0/24	192.168.1.250	lan	✖

Mode ○ Off ● On

Name

Destination

Gateway

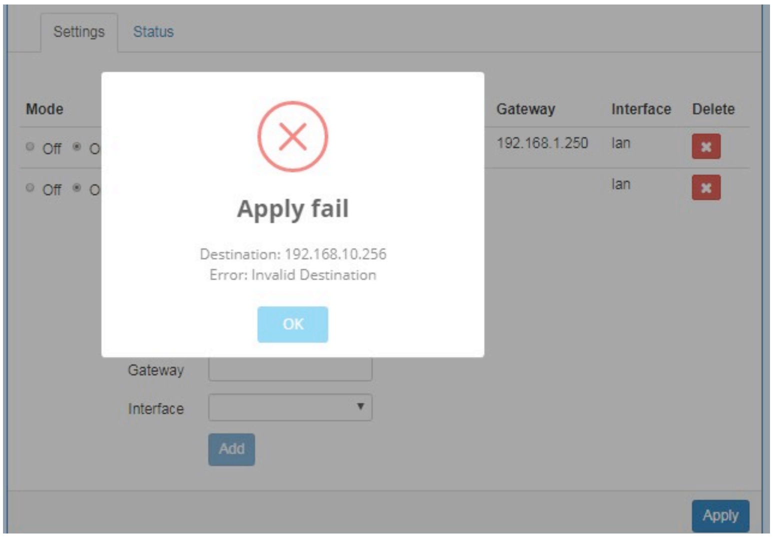
Interface ▾

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

Note:

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

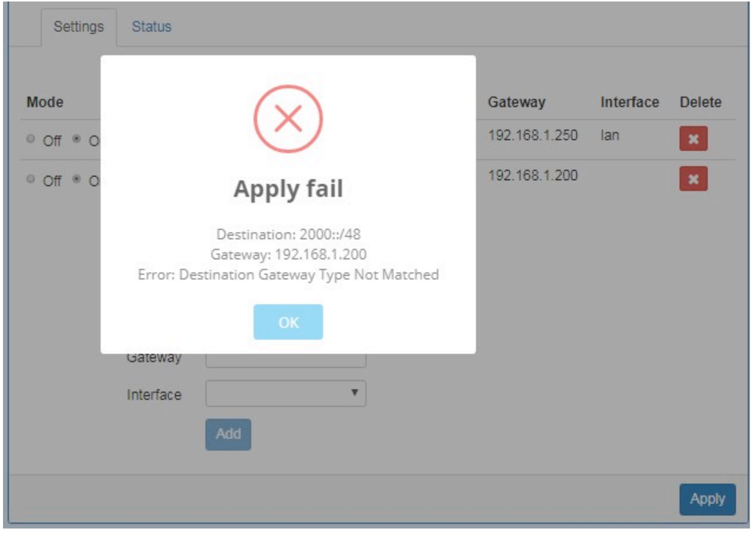
(1) Input the invalid format of destination. The interface is shown in Apply fail to notice.



Apply fail

Destination: 192.168.10.256
Error: Invalid Destination

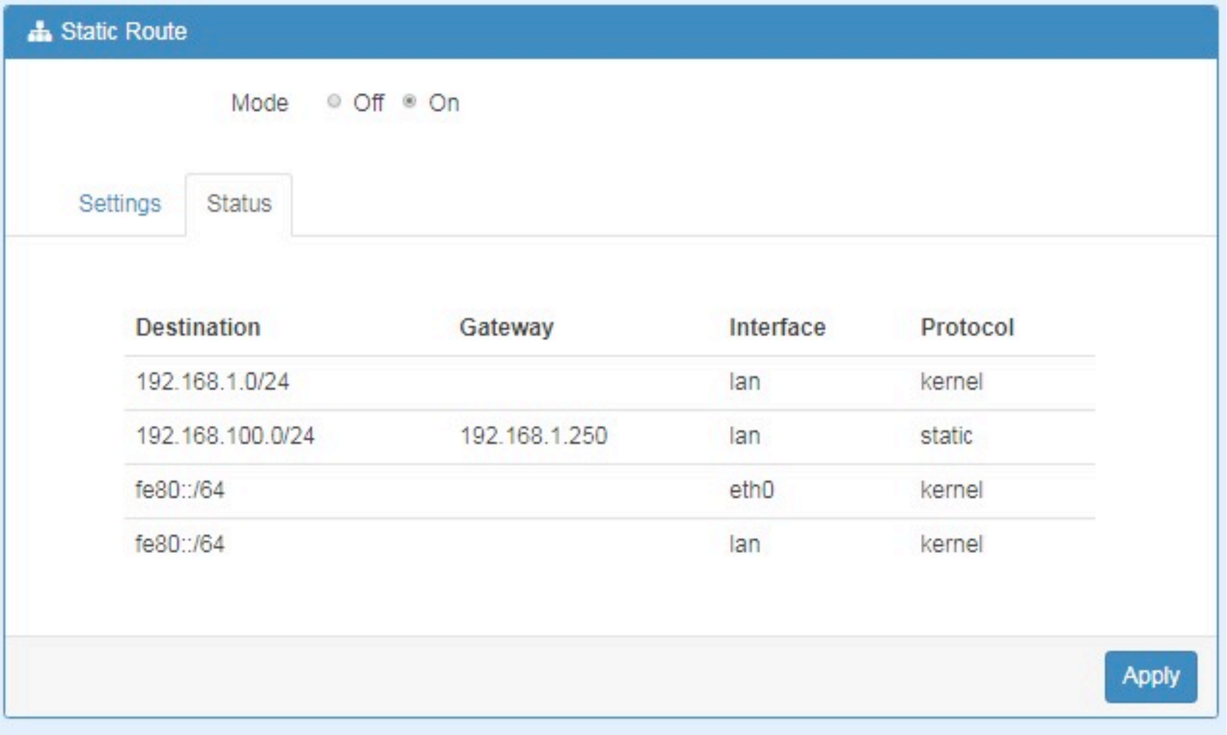
(2) Input the IP address of destination/gateway from IPv4 and IPv6 at the same time. The interface is shown in Apply fail to notice. You should select either IPv4 or IPv6 as the address of destination/gateway.



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

Settings | Status

Destination	Gateway	Interface	Protocol
192.168.1.0/24		lan	kernel
192.168.100.0/24	192.168.1.250	lan	static
fe80::/64		eth0	kernel
fe80::/64		lan	kernel

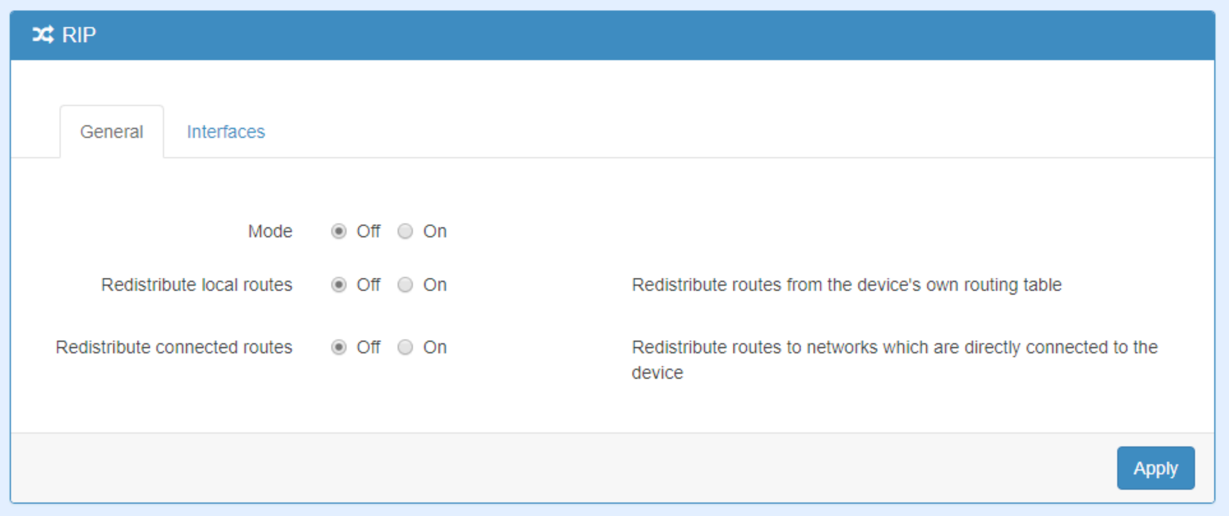
IP Routing > Static Route	
Item	**Description**
Mode	The setting is open for full network. Select from Off or On.
Status	
Destination	Show the status of destination from the setting section.
Gateway	Show the status of gateway from the setting section.
Interface	Show the status of interface from the setting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

9.2 **IP Routing > RIP**

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

Note:

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



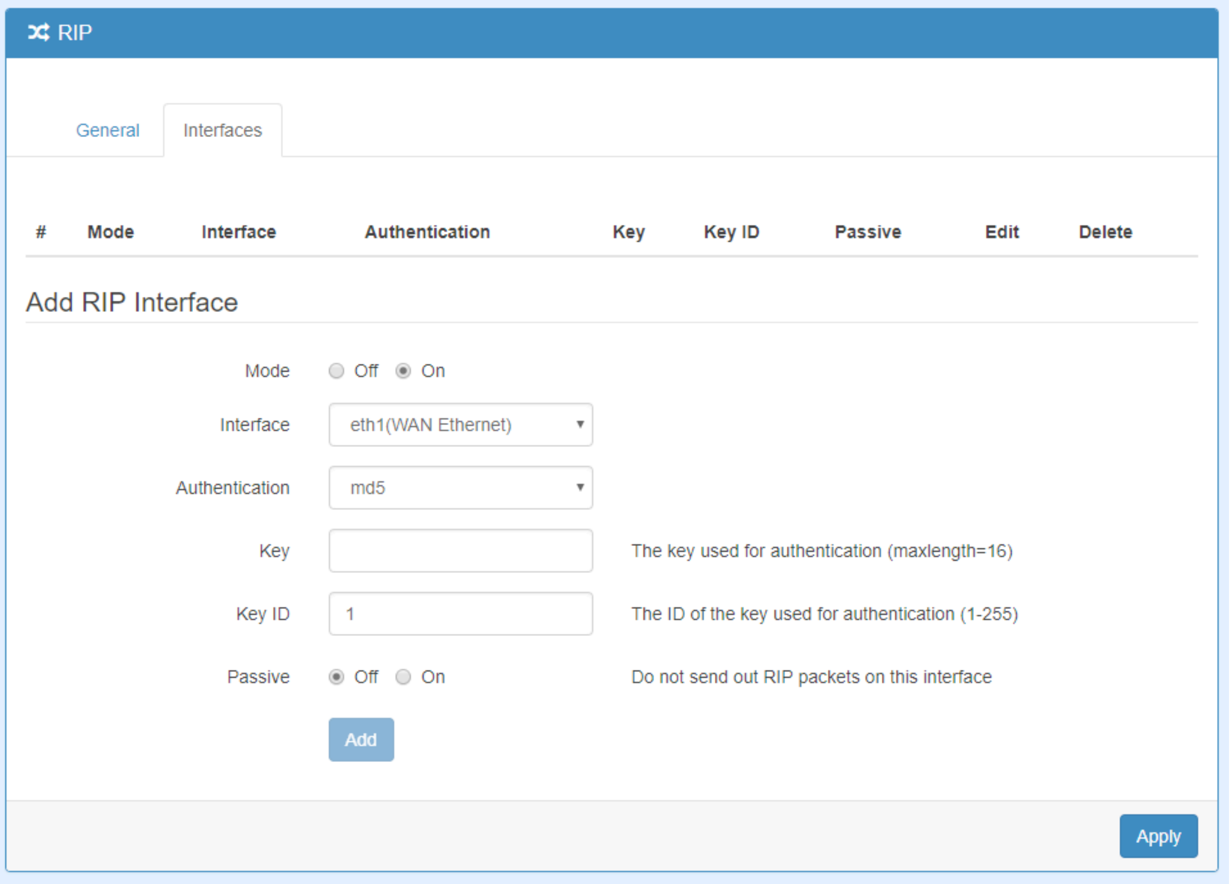
RIP

Mode ● Off ○ On

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

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

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.



RIP

#	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)

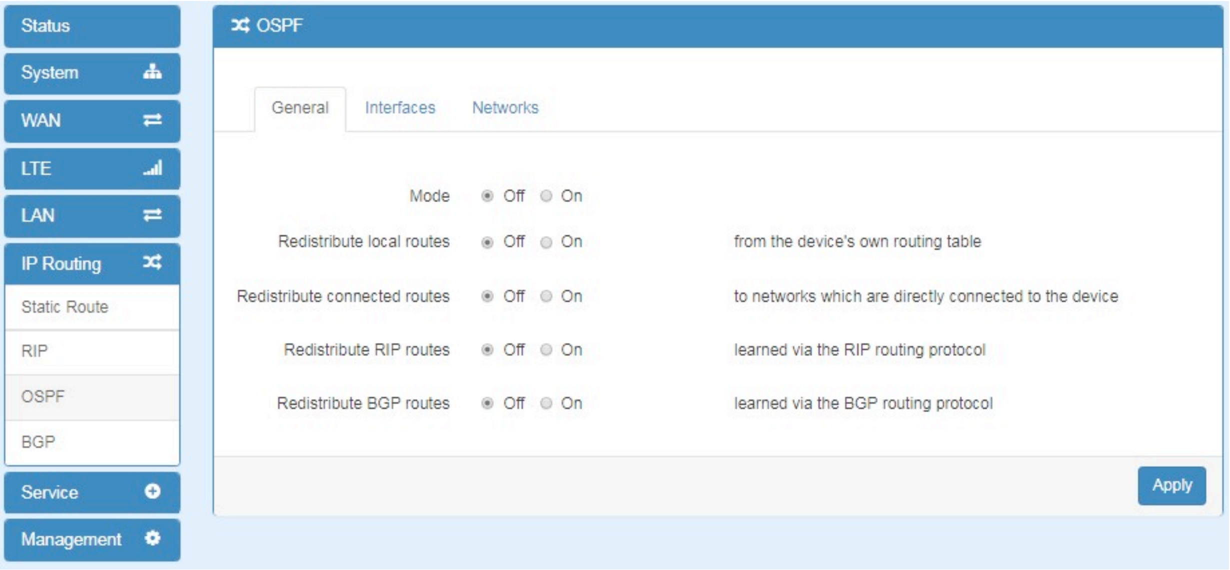
Key ID: 1 — The ID of the key used for authentication (1-255)

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.

9.3 IP Routing > OSPF

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

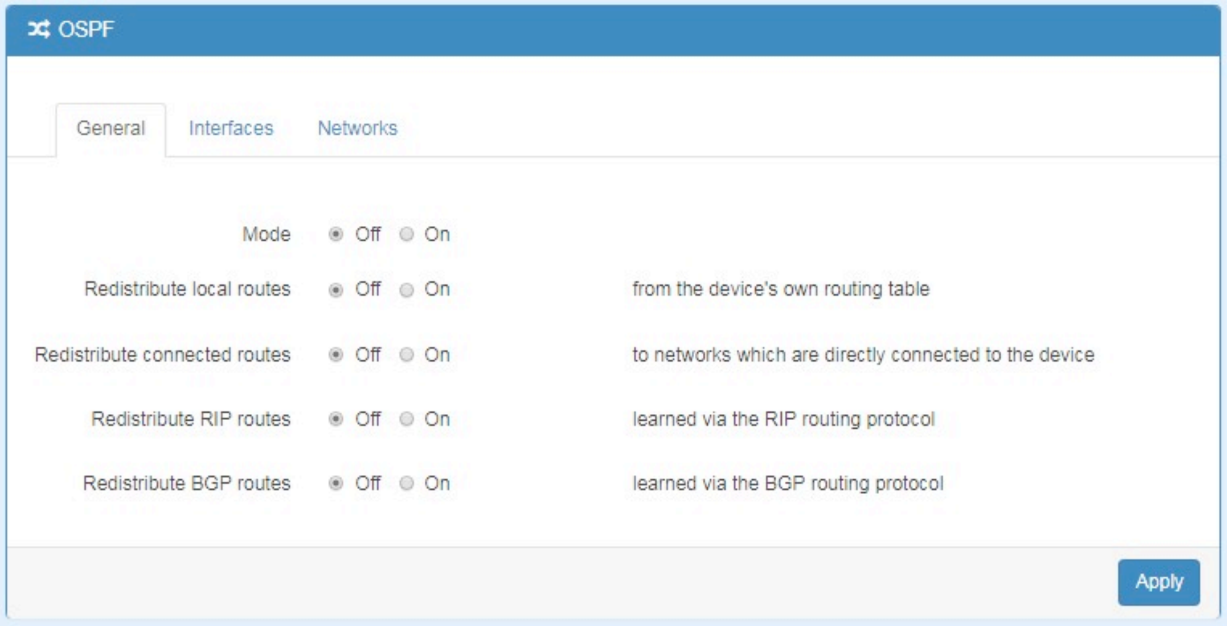
Redistribute RIP routes ● Off ○ On learned via the RIP routing protocol

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

(1) General Configuration

You can have these settings for General configuration.

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



OSPF

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.

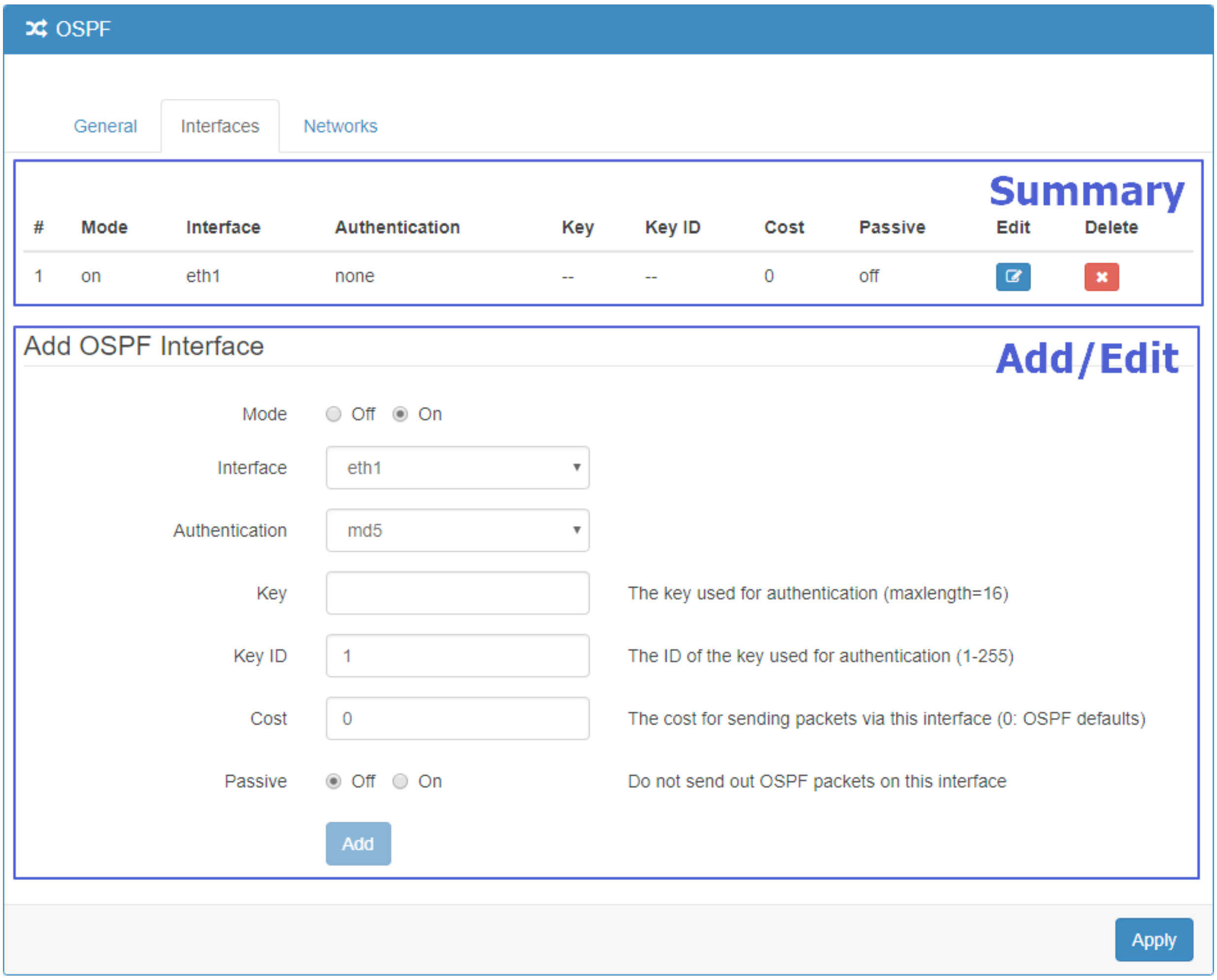
- OSPF Interfaces Summary

  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.



OSPF

General | Interfaces | Networks

Summary

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

Add OSPF Interface

Add/Edit

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

(3) Networks Configuration

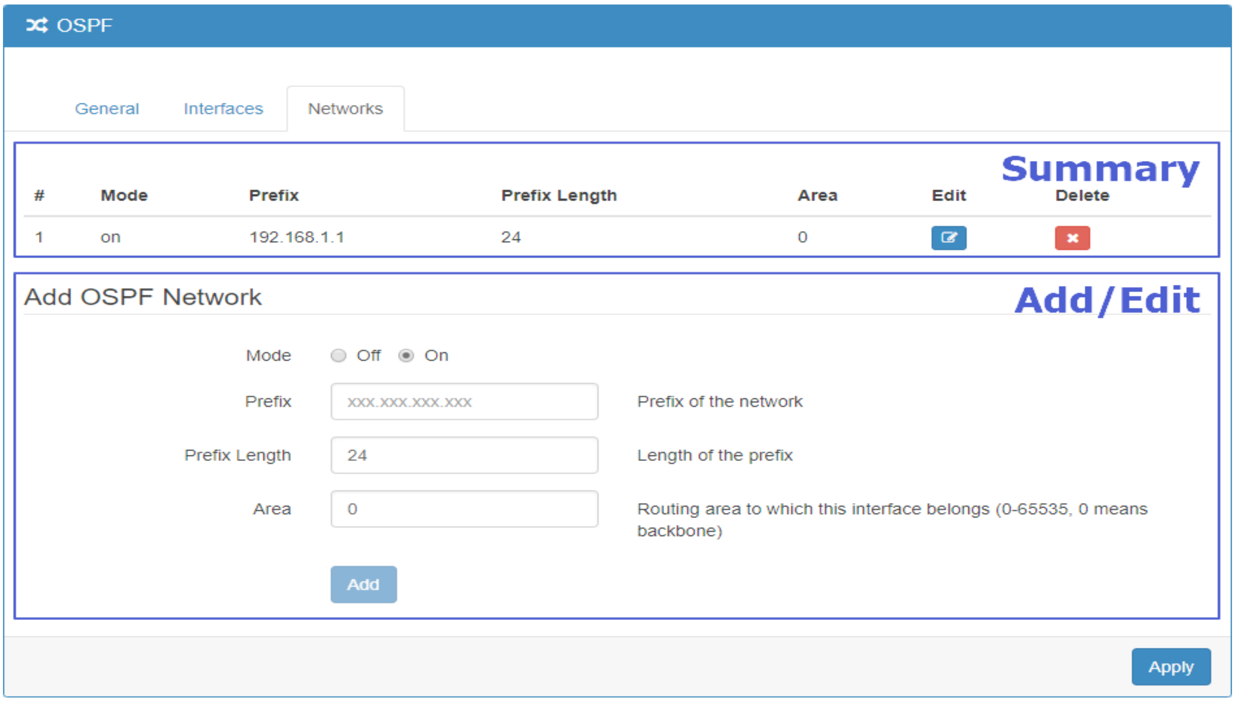
There are 2 parts for OSPF Networks configuration.

- OSPF Networks Summary

  You can edit and delete the existed OSPF networks.

- OSPF Networks Add/Edit

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



#	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

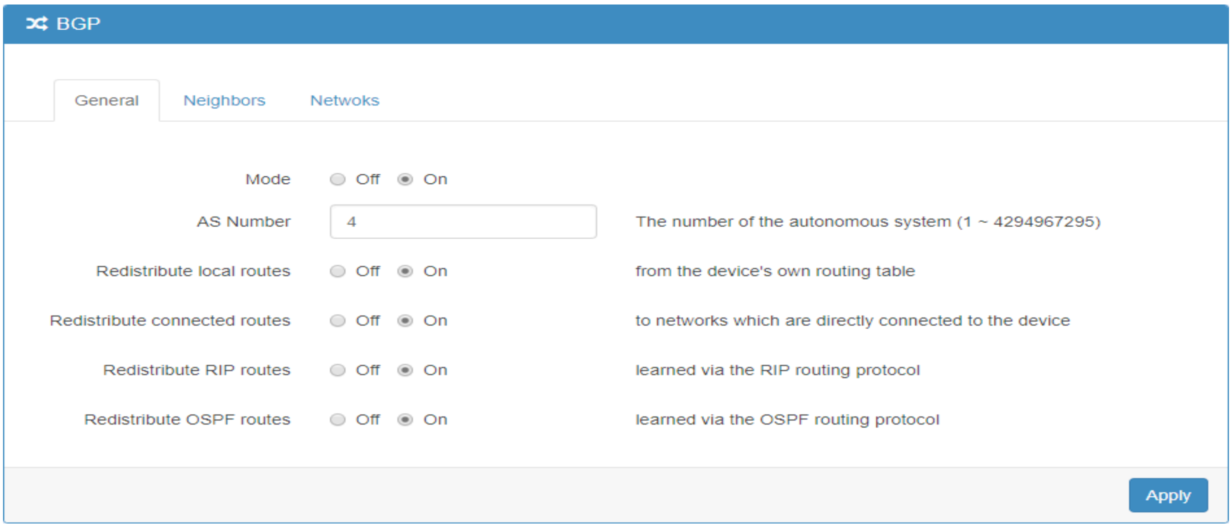
Area: 0 — Routing area to which this interface belongs (0-65535, 0 means backbone)

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

9.4 IP Routing > BGP

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

(1) General Configuration



Mode ○ Off ● On

AS Number: 4 — 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

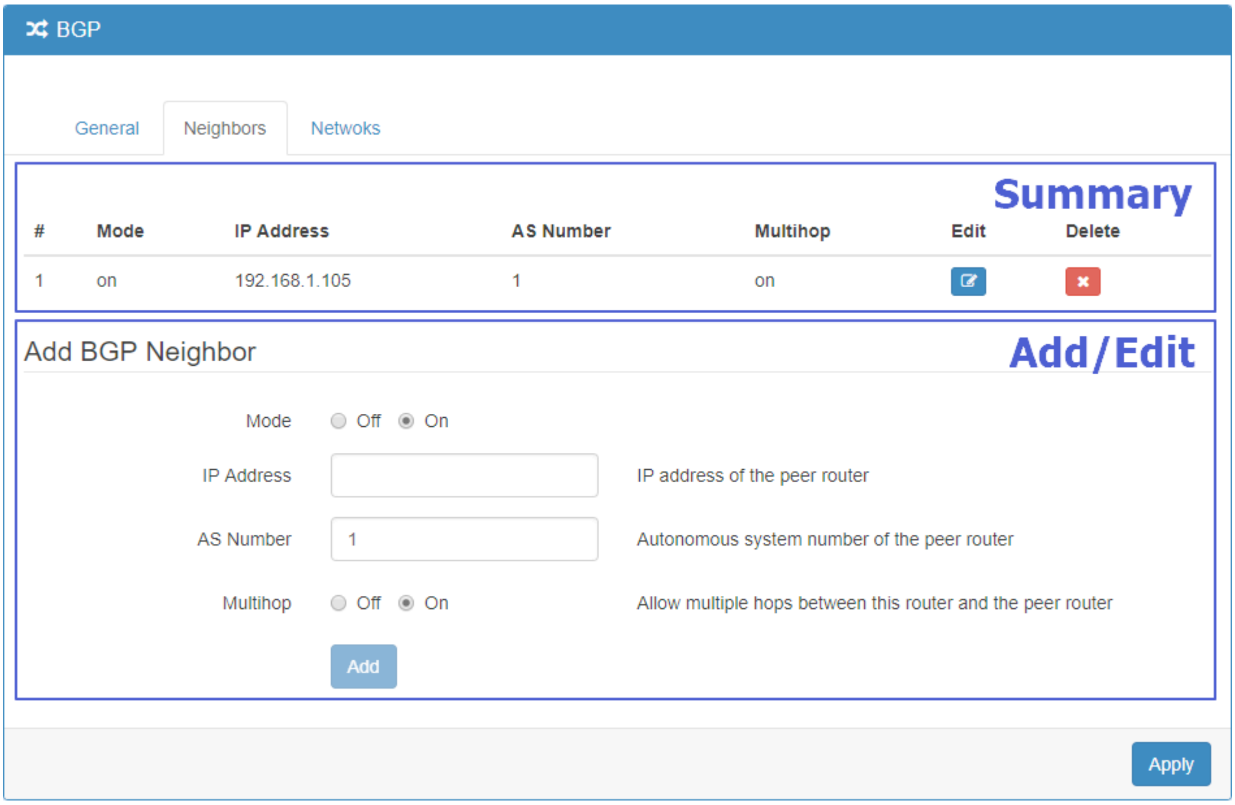
Redistribute RIP routes ○ Off ● On — learned via the RIP routing protocol

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	Edit	Delete
1	on	192.168.1.105	1	on	✎	✖

Add BGP Neighbor

Mode ○ Off ● On

IP Address [ ] IP address of the peer router

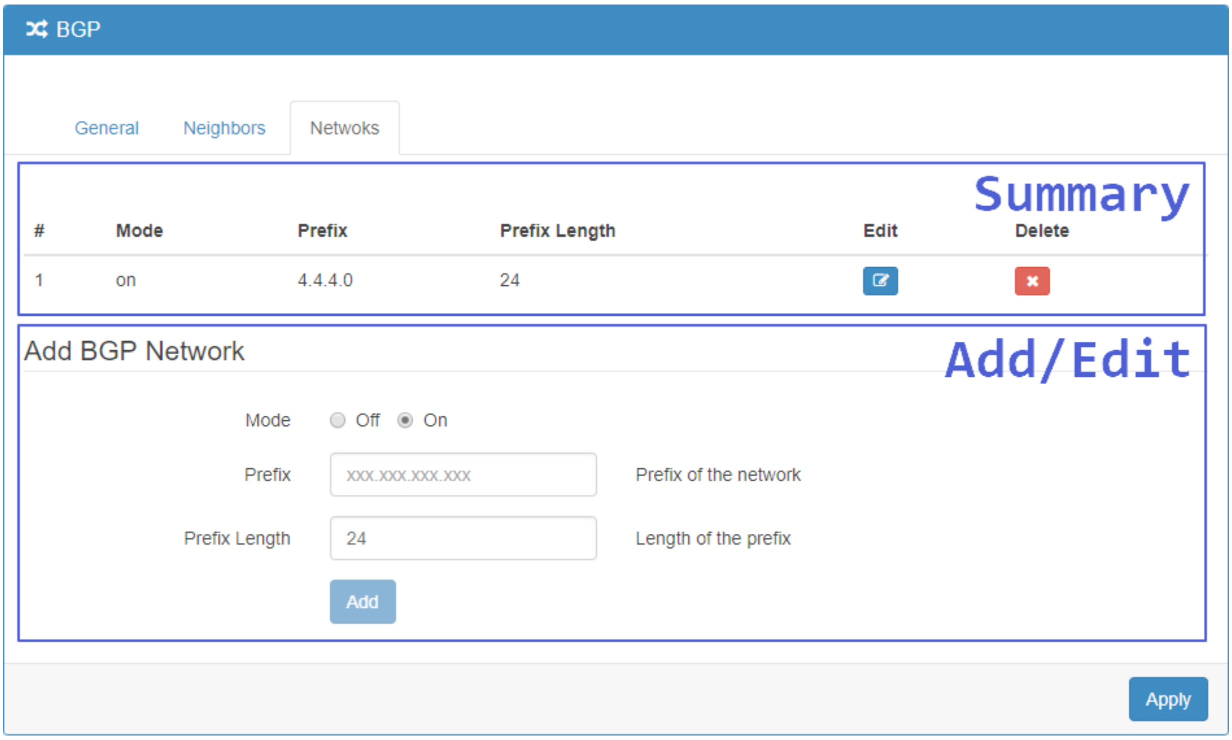
AS Number [1] Autonomous system number of the peer router

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

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

(3) Networks Configuration

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



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

Add BGP Network

Mode ○ Off ● On

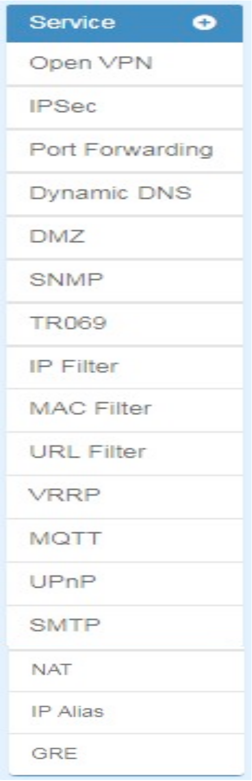
Prefix xxx.xxx.xxx.xxx Prefix of the network

Prefix Length 24 Length of the prefix

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

10 Configuration > Service

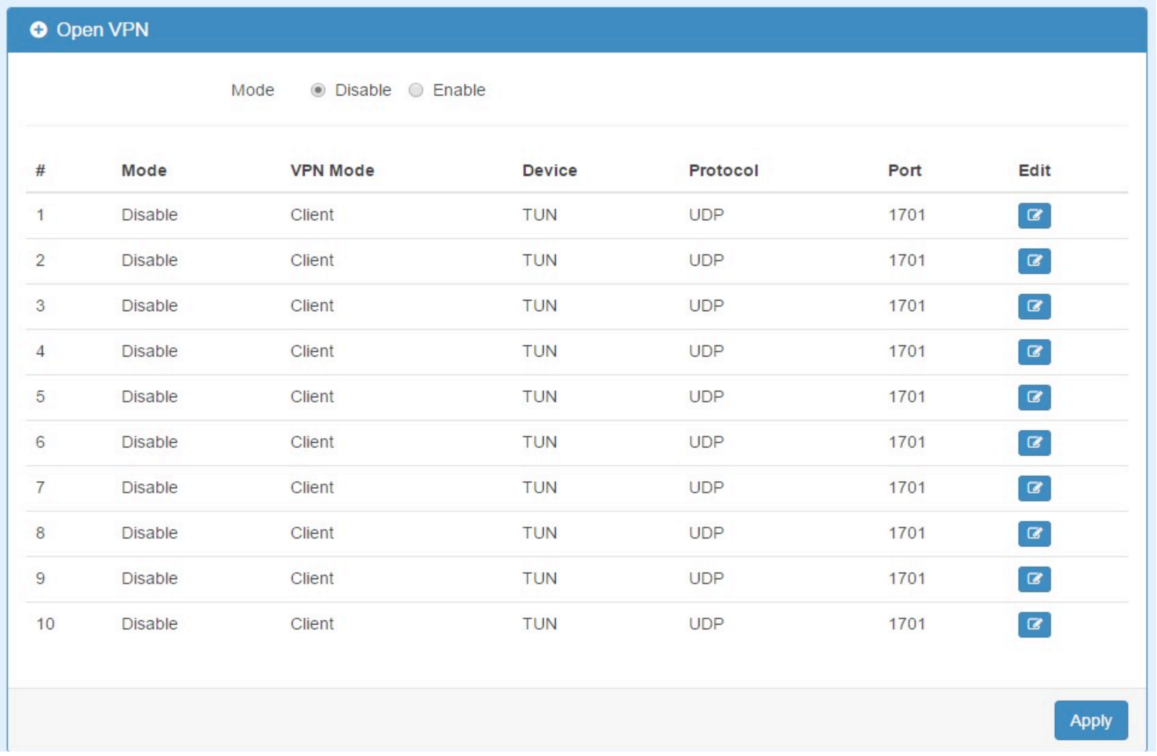
This section allows you to configure OpenVPN, IPSec, Port Forwarding, Dynamic DNS, DMZ, SNMP, IP Filter, MAC Filter, URL Filter, VRRP, MQTT, UPnP, SMTP, NAT, IP Alias and GRE.



10.1 Service > Configuration OpenVPN

10.1.1 Edit OpenVPN Connection

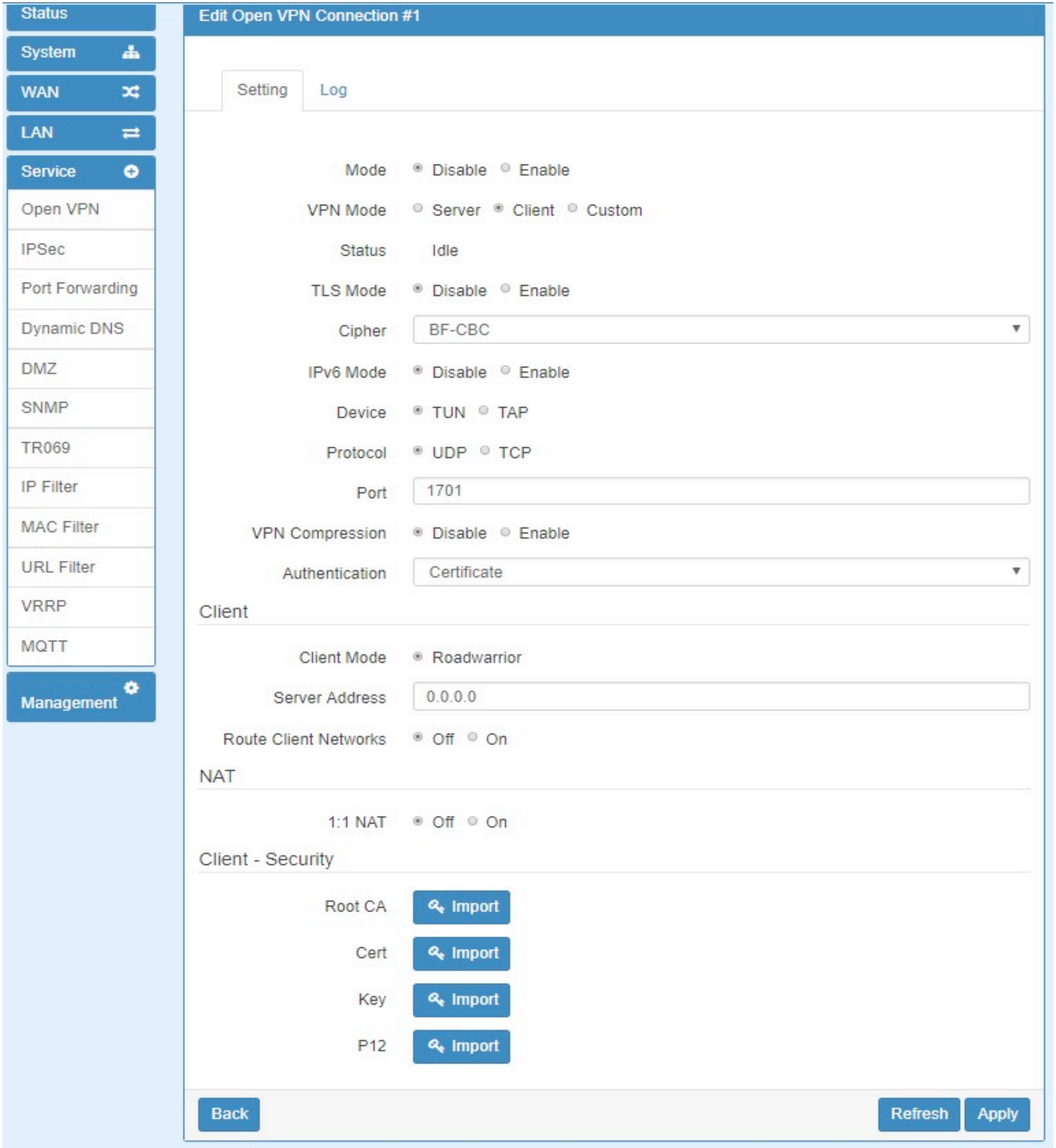
(1) This section allows you to configure the OpenVPN parameters. The default mode is Disable. Click ✎ button to edit OpenVPN Connection.



Mode ● 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 OpenVPN.



Edit Open VPN Connection #1

Mode ● Disable ○ Enable

VPN Mode ○ Server ● Client ○ Custom

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

Client

Client Mode ● Roadwarrior

Server Address 0.0.0.0

Route Client Networks ● Off ○ On

NAT

1:1 NAT ● Off ○ On

Client - Security

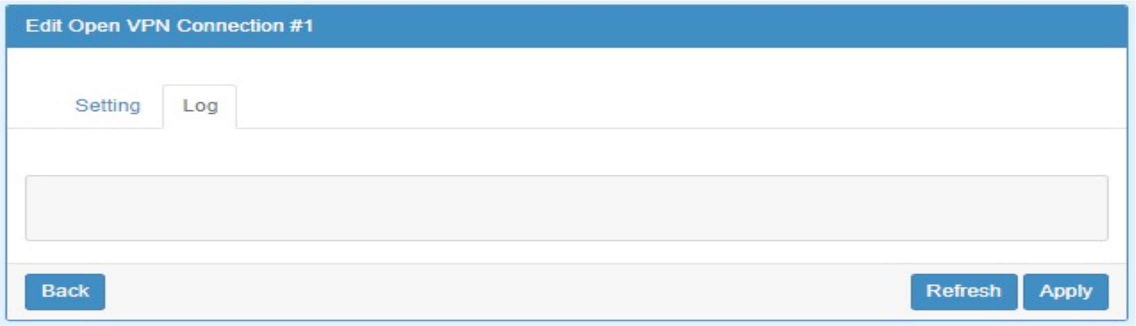
Root CA Import

Cert Import

Key Import

P12 Import

(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.

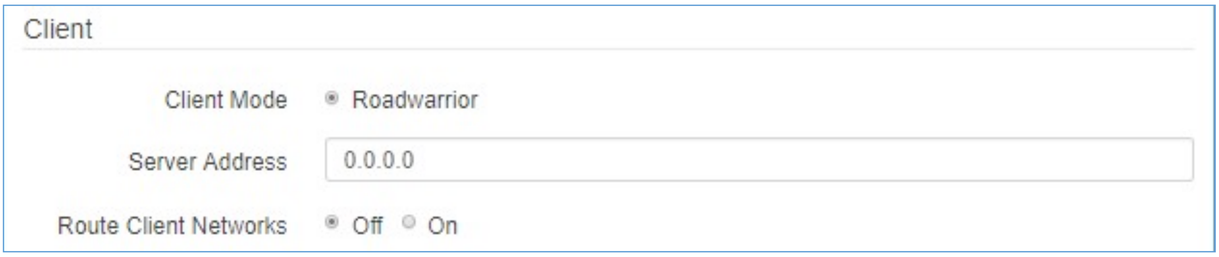


Edit Open VPN Connection #1

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

10.1.2 Set up OpenVPN Client

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

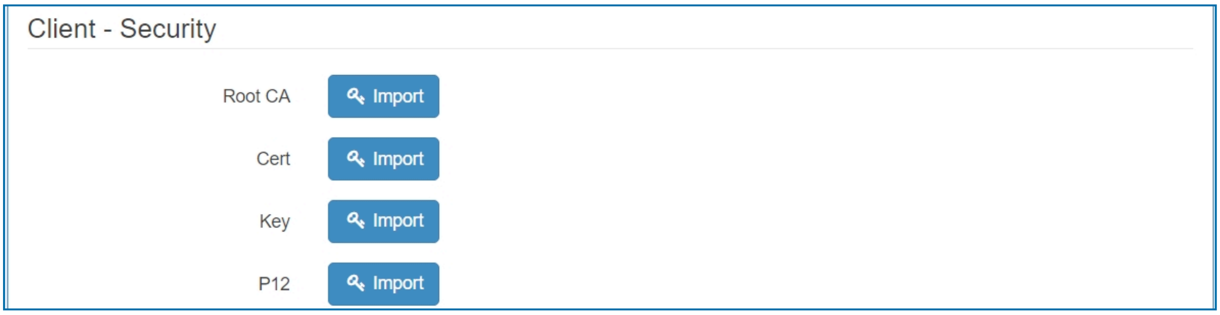


Client

Client Mode ● Roadwarrior

Server Address 0.0.0.0

Route Client Networks ● Off ○ On



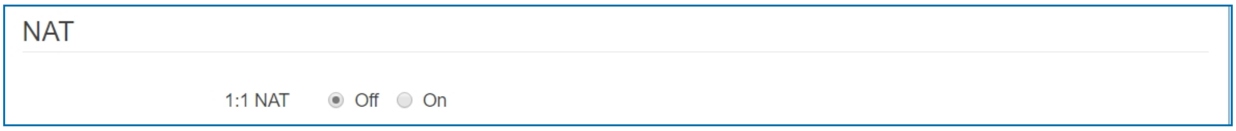
Client - Security

Root CA Import

Cert Import

Key Import

P12 Import



NAT

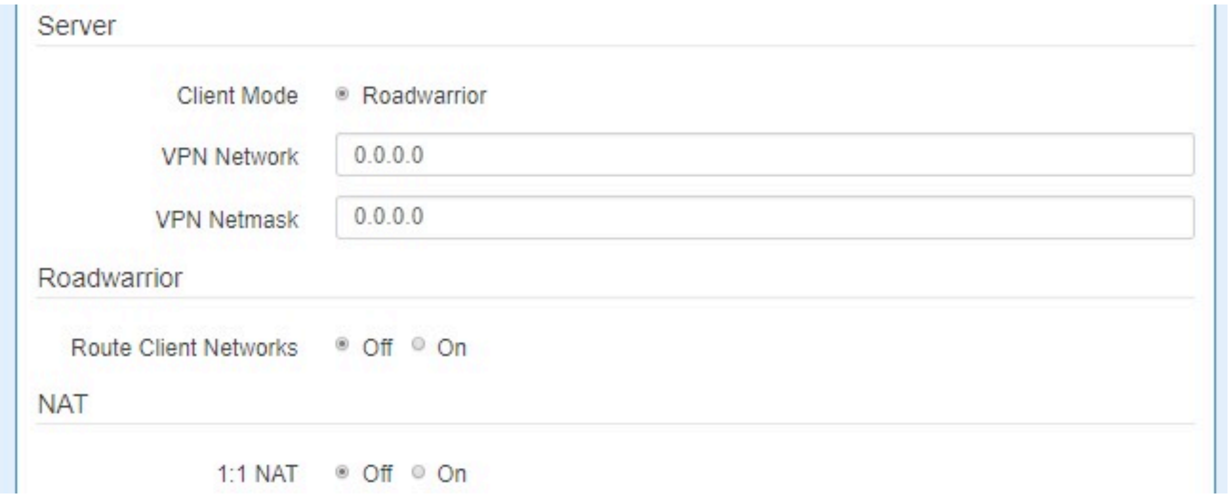
1:1 NAT ● Off ○ On

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

10.1.3 Set up OpenVPN Server

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

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



Server

Client Mode ● Roadwarrior

VPN Network 0.0.0.0

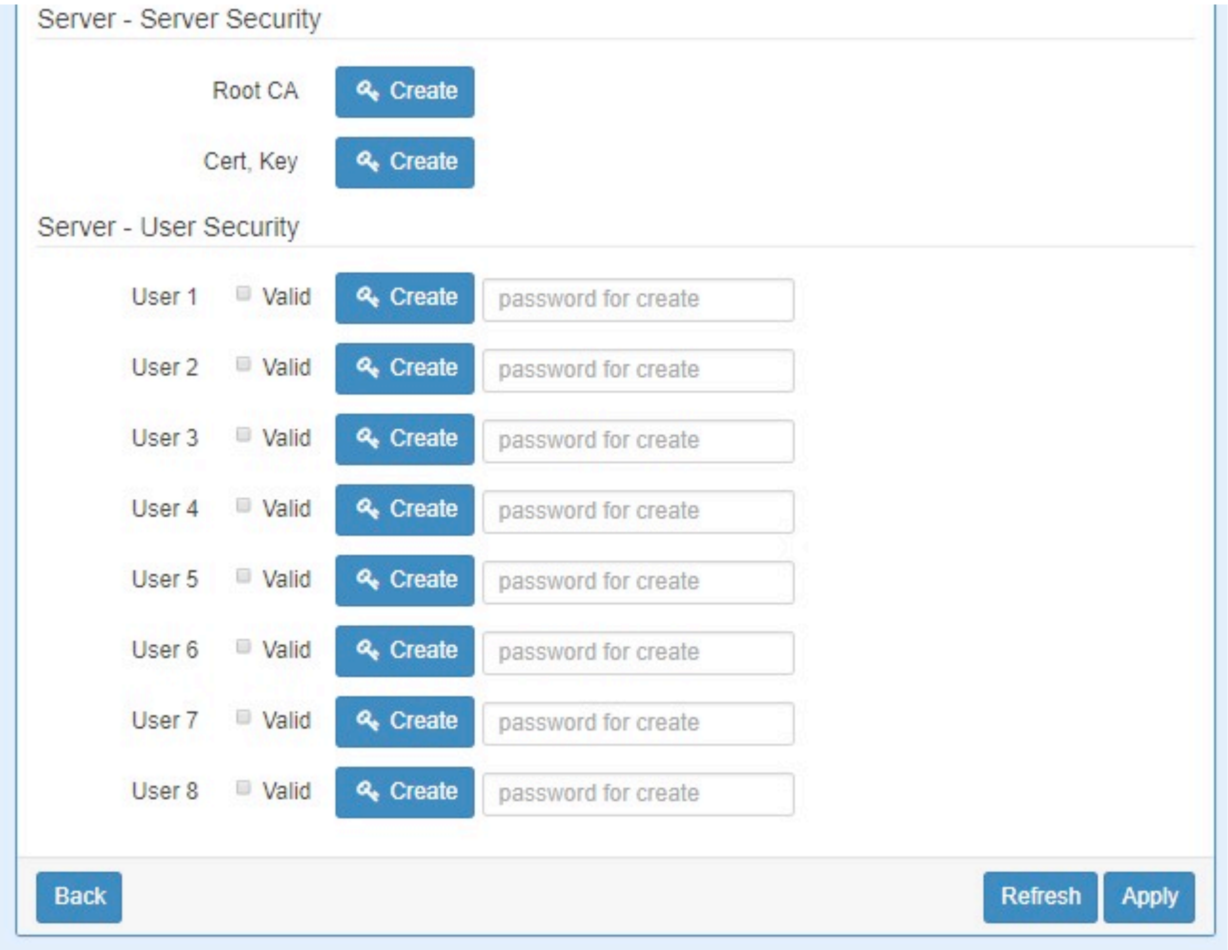
VPN Netmask 0.0.0.0

Roadwarrior

Route Client Networks ● Off ○ On

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

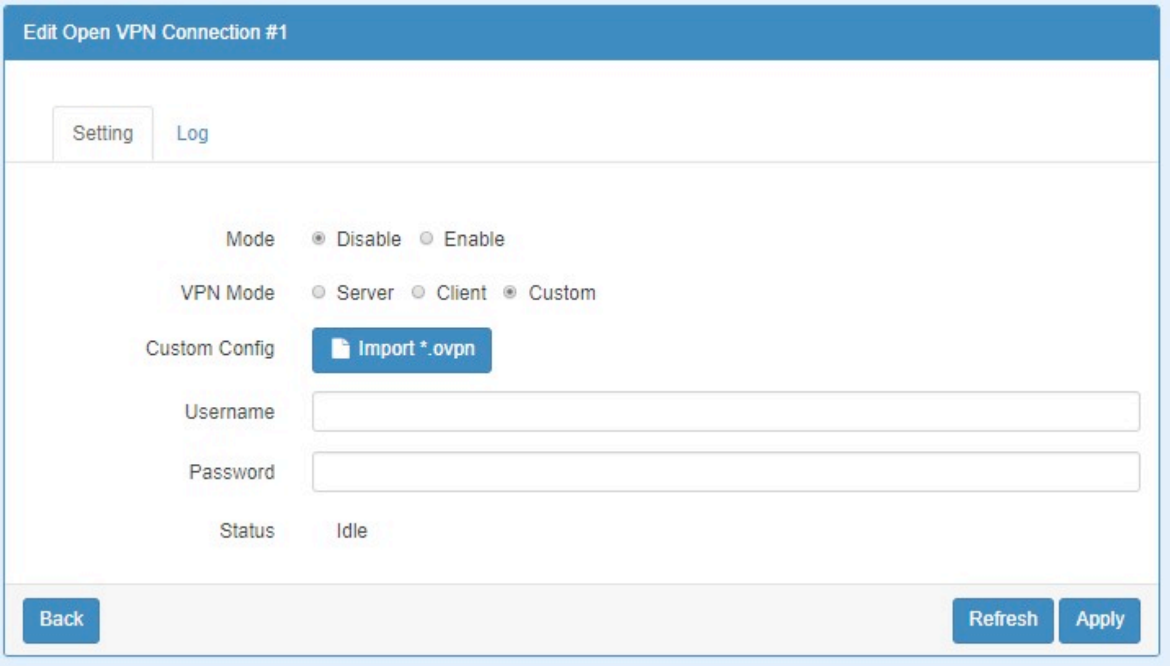
Service > OpenVPN > Server VPN Mode	
Item	**Description**
Server	
Client Mode	Only support the Roadwarrior mode.
VPN Network	The network ID for OpenVPN virtual network.
VPN Netmask	The netmask for OpenVPN virtual network.
Roadwarrior: **Route Client Networks**	Select from Off or On. The OpenVPN server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

10.1.4 Set up OpenVPN Custom

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

Note:

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

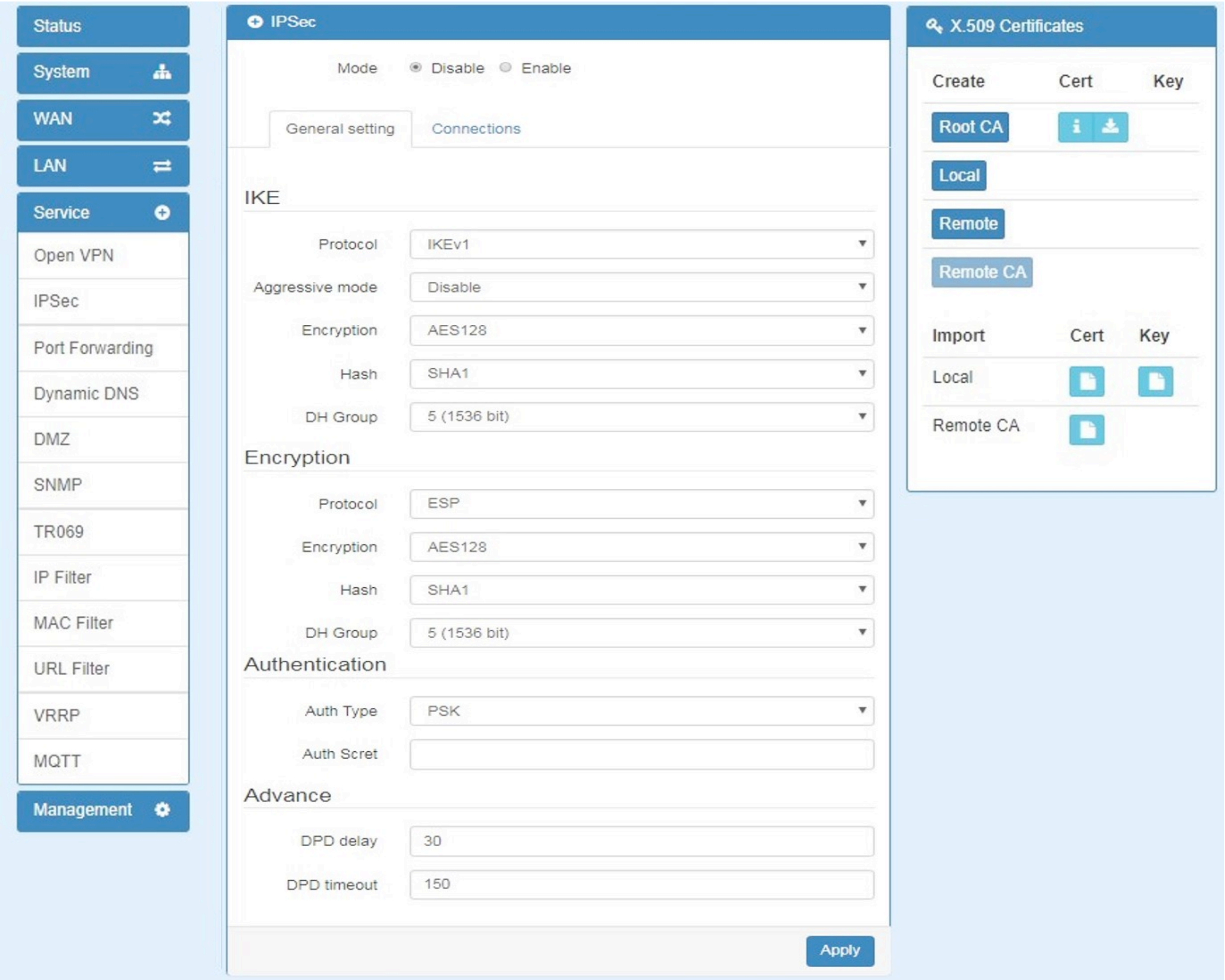
Service > OpenVPN > Custom VPN Mode	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
VPN Mode	Select from custom mode.
Custom Config	Import OpenVPN configuration.
Username	Fill in the username if the imported file has already set up the username.
Password	Fill in the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

10.2 Service > Configuration IPSec

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

10.2.1 IPSec > General setting

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



Mode ● Disable ○ Enable

IKE

Protocol	IKEv1
Aggressive mode	Disable
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)

Encryption

Protocol	ESP
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)

Authentication

Auth Type	PSK
Auth Scret	

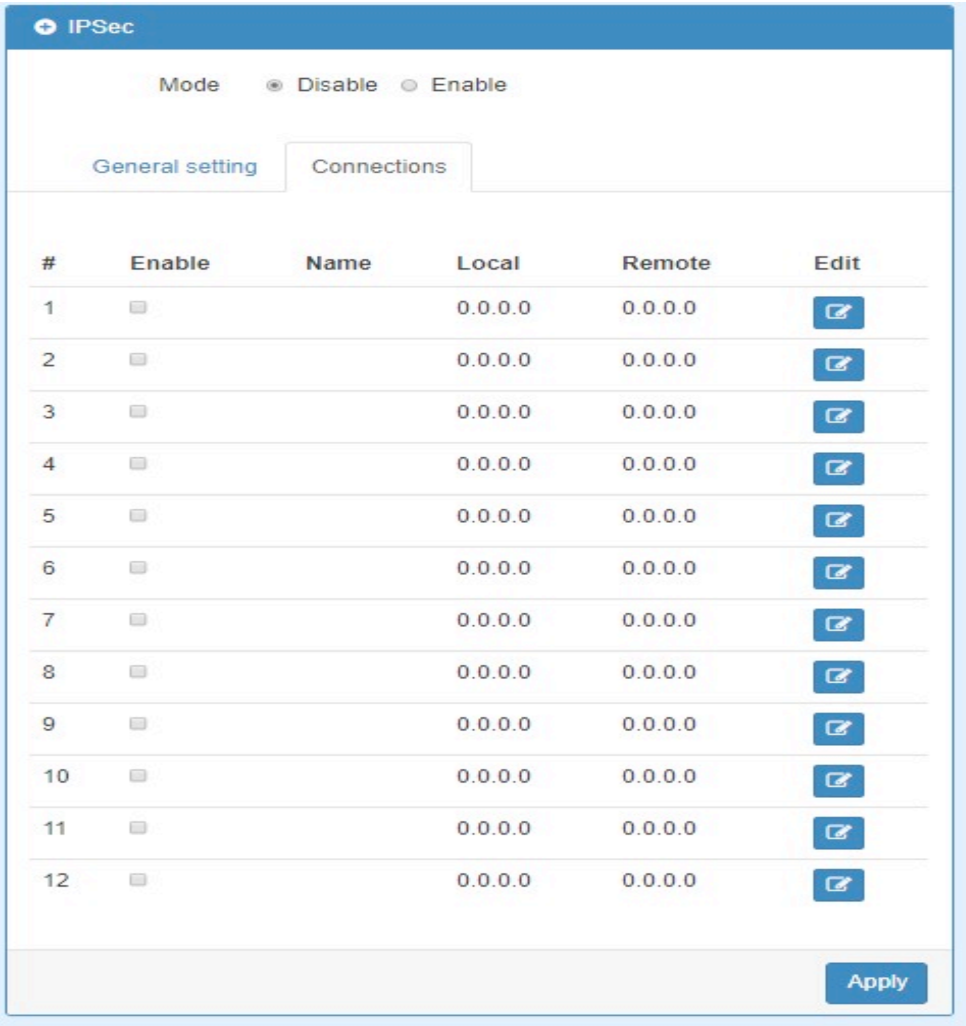
Advance

DPD delay	30
DPD timeout	150

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

10.2.2 IPSec > Connections

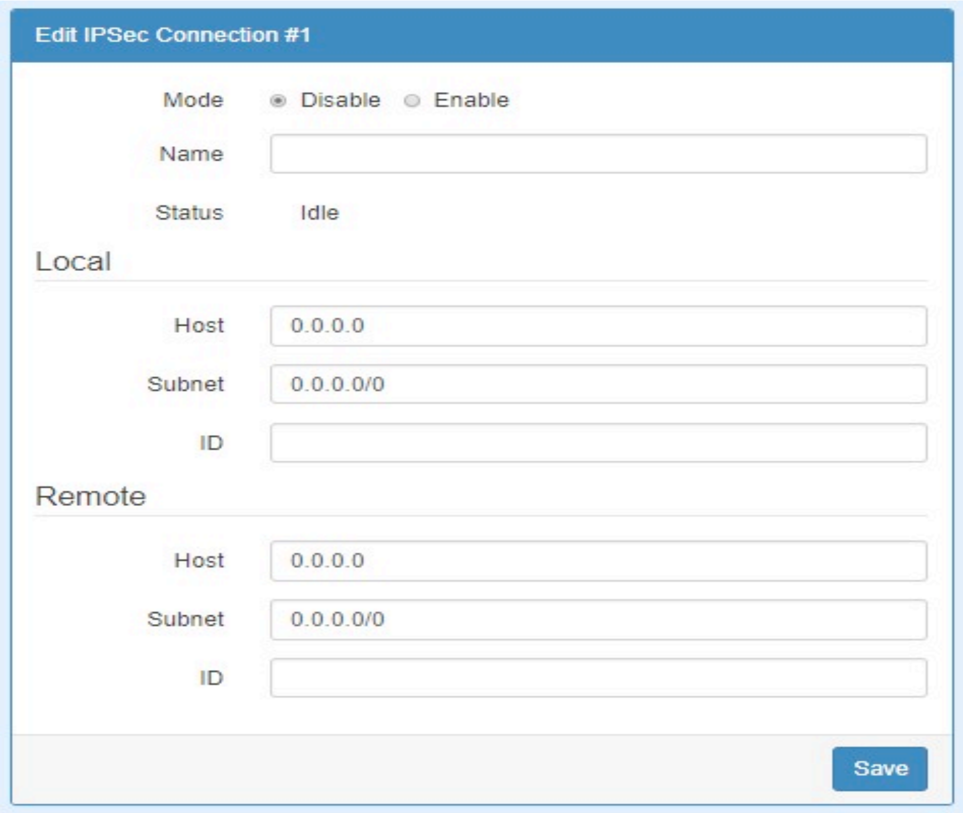
For **Connections** tab, the web UI provides the overview for each connection. Click ✎ button to edit IPSec connection and set up the local and remote side.



IPSec

Mode ● Disable ○ Enable

#	Enable	Name	Local	Remote	Edit
1	□		0.0.0.0	0.0.0.0	✎
2	□		0.0.0.0	0.0.0.0	✎
3	□		0.0.0.0	0.0.0.0	✎
4	□		0.0.0.0	0.0.0.0	✎
5	□		0.0.0.0	0.0.0.0	✎
6	□		0.0.0.0	0.0.0.0	✎
7	□		0.0.0.0	0.0.0.0	✎
8	□		0.0.0.0	0.0.0.0	✎
9	□		0.0.0.0	0.0.0.0	✎
10	□		0.0.0.0	0.0.0.0	✎
11	□		0.0.0.0	0.0.0.0	✎
12	□		0.0.0.0	0.0.0.0	✎



Edit IPSec Connection #1

Mode ● Disable ○ Enable

Name

Status Idle

Local

Host 0.0.0.0

Subnet 0.0.0.0/0

ID

Remote

Host 0.0.0.0

Subnet 0.0.0.0/0

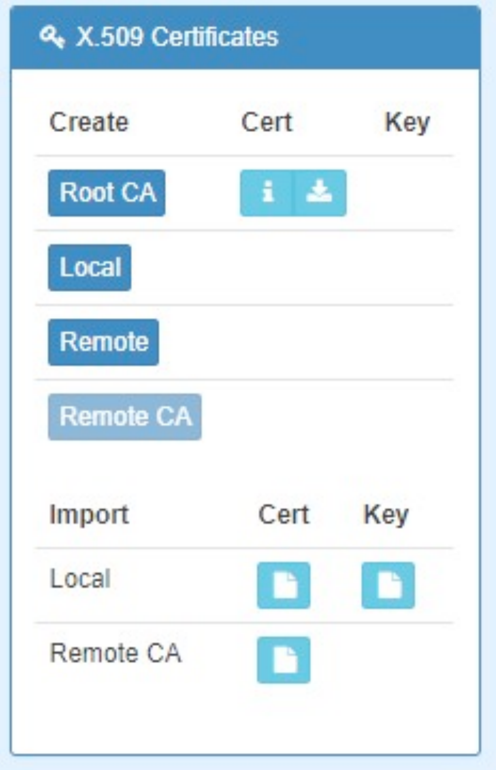
ID

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

10.2.3 IPSec > The setting of X.509 Certificates

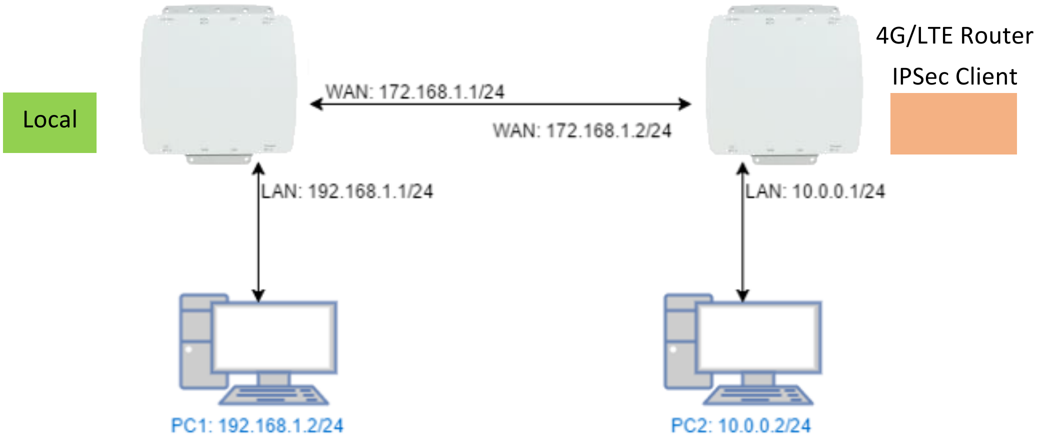
The interface shows the setting items of X.509 Certificates.

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



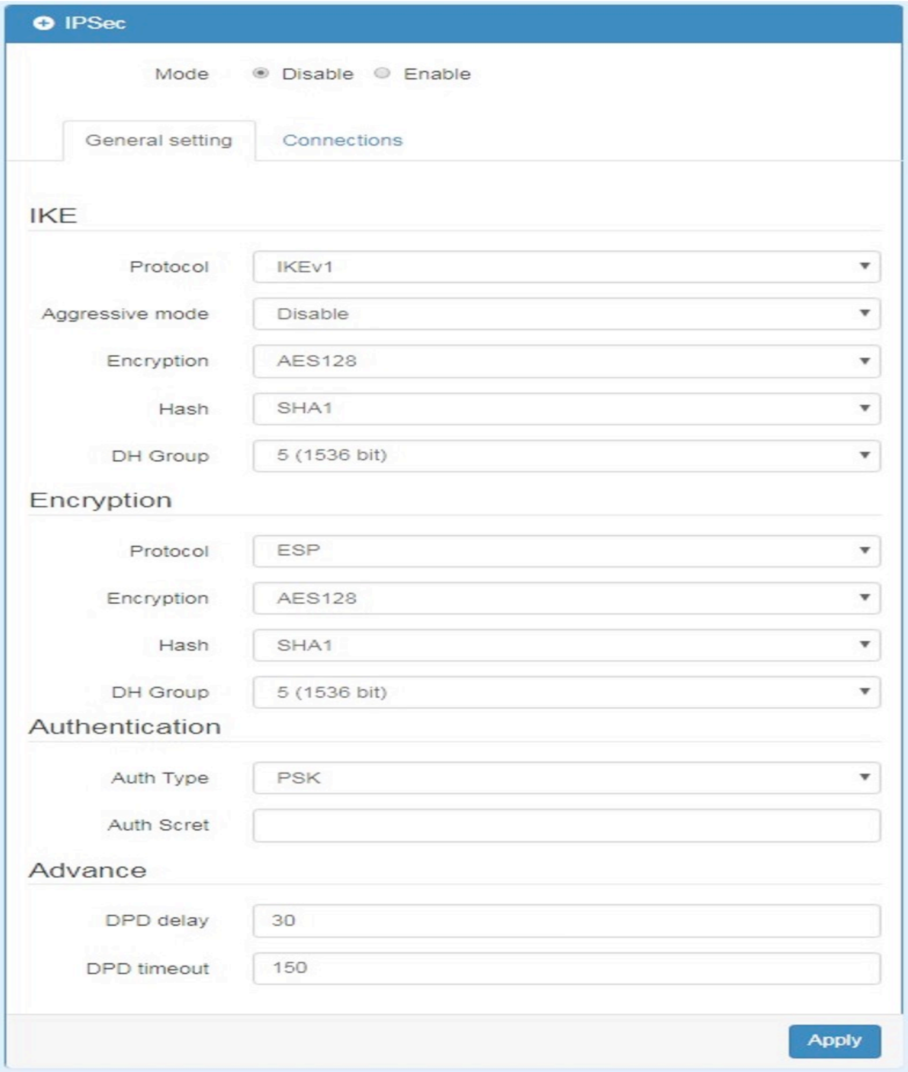
10.2.4 IPSec > Net-to-Net Configuration

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



General setting

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



Mode ● Disable ○ Enable

IKE

Protocol	IKEv1
Aggressive mode	Disable
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)

Encryption

Protocol	ESP
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)

Authentication

Auth Type	PSK
Auth Scret	

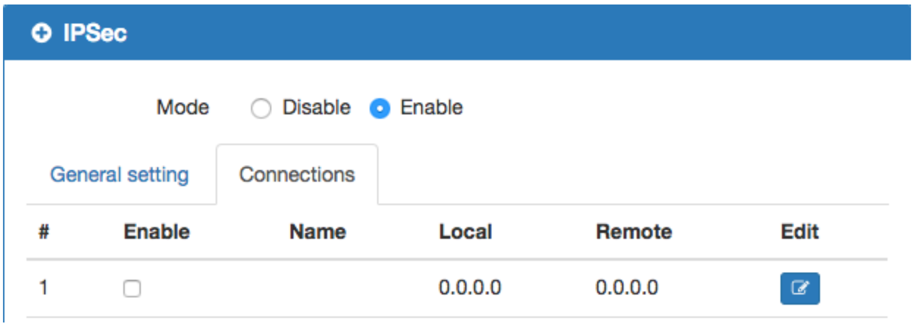
Advance

DPD delay	30
DPD timeout	150

Connections Setting

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

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



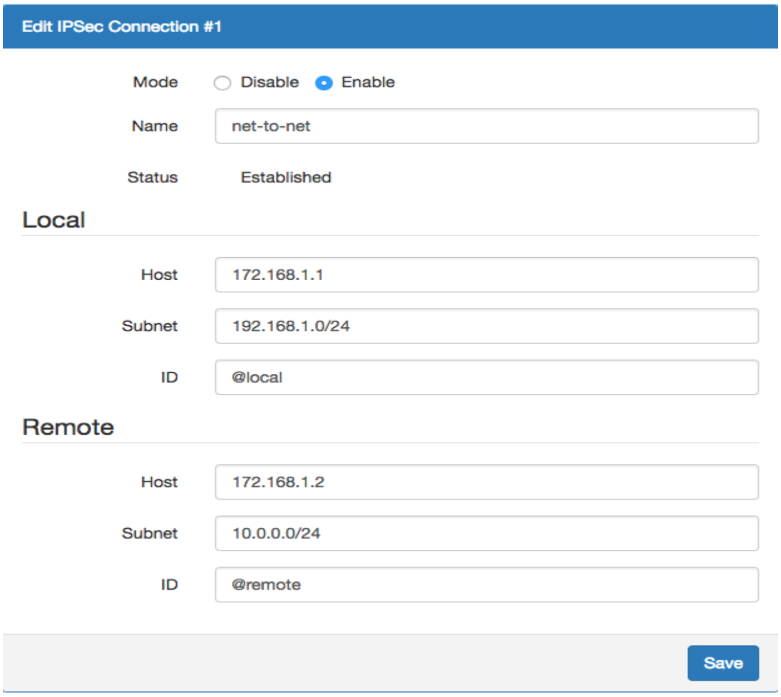
Mode ○ Disable ● Enable

#	Enable	Name	Local	Remote	Edit
1	□		0.0.0.0	0.0.0.0	

- Local Side

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

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



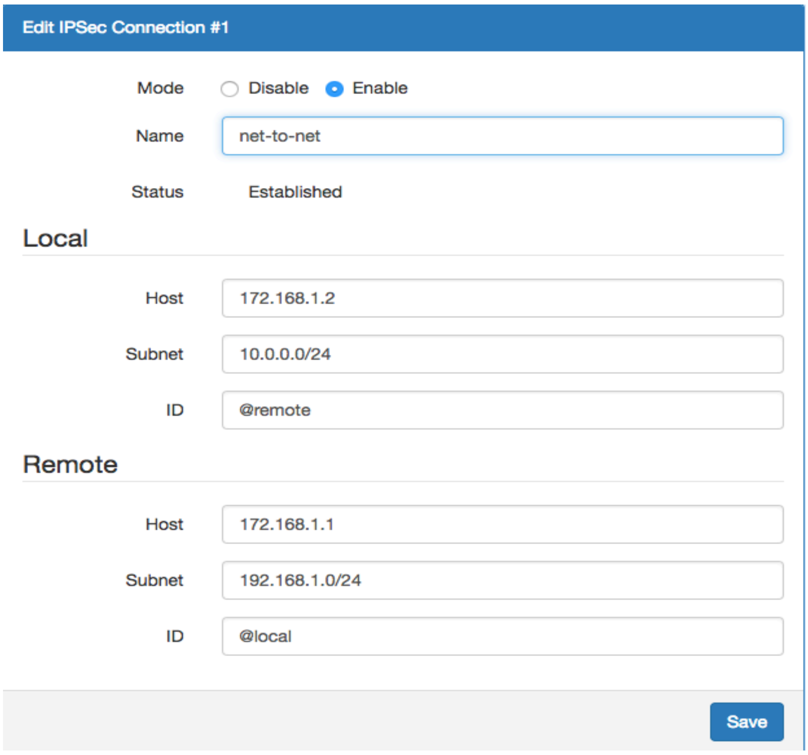
Mode ○ Disable ● Enable
Name: net-to-net
Status: Established

Local
Host: 172.168.1.1
Subnet: 192.168.1.0/24
ID: @local

Remote
Host: 172.168.1.2
Subnet: 10.0.0.0/24
ID: @remote

- Remote Side

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



Edit IPSec Connection #1

Mode ○ Disable ● Enable

Name: net-to-net

Status: Established

Local

Host: 172.168.1.2

Subnet: 10.0.0.0/24

ID: @remote

Remote

Host: 172.168.1.1

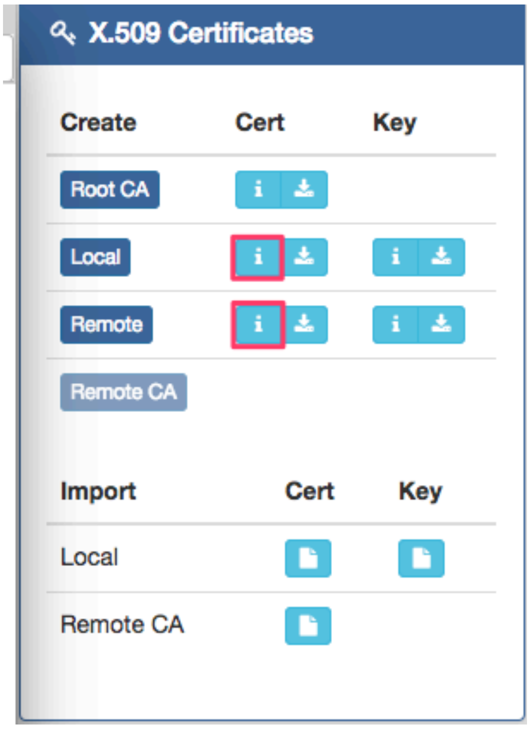
Subnet: 192.168.1.0/24

ID: @local

Net-to-Net (Pre-shared key)

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

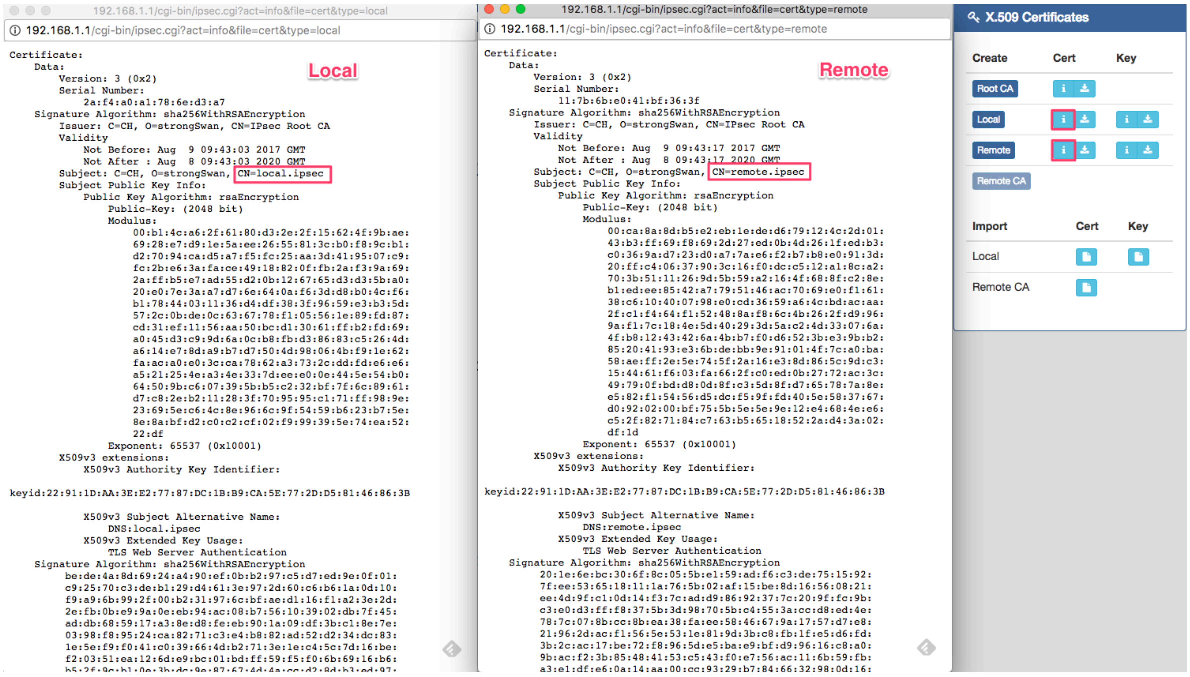
For the Cellular router IPSec certificate generation, it generates the local and remote side certificates with **@local.ipsec** and **@remote.ipsec**. (The certificate information can be queried by i the information button.)



X.509 Certificates

Create	Cert	Key
Root CA	i ⬇	
Local	i ⬇	i ⬇
Remote	i ⬇	i ⬇
Remote CA		

Import	Cert	Key
Local	🗎	🗎
Remote CA	🗎	



192.168.1.1/cgi-bin/ipsec.cgi?act=info&file=cert&type=local

Local

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2a:f4:a0:a1:78:6e:d3:a7
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CH, O=strongSwan, CN=IPsec Root CA
        Validity
            Not Before: Aug  9 09:43:03 2017 GMT
            Not After : Aug  8 09:43:03 2020 GMT
        Subject: C=CH, O=strongSwan, CN=local.ipsec
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b1:4c:a6:2f:61:80:d3:2e:2f:15:62:4f:9b:ae:
                    69:28:e7:d9:1e:5a:ee:26:55:81:3c:b0:f8:9c:b1:
                    d2:70:94:ca:d5:a7:f5:fc:25:aa:3d:41:95:07:c9:
                    fc:2b:e6:3a:fa:ce:49:18:82:0f:fb:2a:f3:9a:69:
                    2a:ff:b5:e7:ad:55:d2:0b:12:67:65:d3:d3:5b:a0:
                    20:e0:7e:3a:a7:d7:6e:64:0a:f6:3d:d8:b0:4c:f6:
                    b1:78:44:03:11:36:d4:df:38:3f:96:59:e3:b3:5d:
                    57:2c:0b:de:0c:63:67:78:f1:05:56:1e:89:fd:87:
                    cd:31:ef:11:56:aa:50:bc:d1:30:61:ff:b2:fd:69:
                    a0:45:d3:c9:9d:6a:0c:b8:fb:d3:86:83:c5:26:4d:
                    a6:14:e7:8d:a9:b7:d7:50:4d:98:06:4b:f9:1e:62:
                    fa:ac:a0:e0:3c:ca:78:62:a3:73:2c:dd:fd:e6:e6:
                    a5:21:25:4e:a3:4e:33:7d:ee:e0:0e:44:5e:54:b0:
                    64:50:9b:c6:07:39:5b:b5:c2:32:bf:7f:6c:89:61:
                    d7:c8:2e:b2:11:28:3f:70:95:95:c1:71:ff:98:9e:
                    23:69:5e:c6:4c:8e:96:6c:9f:54:59:b6:23:b7:5e:
                    8e:8a:bf:d2:c0:c2:cf:02:f9:99:39:5e:74:ea:52:
                    22:df
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:

keyid:22:91:1D:AA:3E:E2:77:87:DC:1B:B9:CA:5E:77:2D:D5:81:46:86:3B

            X509v3 Subject Alternative Name:
                DNS:local.ipsec
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
    Signature Algorithm: sha256WithRSAEncryption
         be:de:4a:8d:69:24:a4:90:ef:0b:b2:97:c5:d7:ed:9e:0f:01:
         c9:25:70:c3:de:b1:29:d4:61:3e:97:2d:60:c6:b6:1a:0d:10:
         f9:a9:6b:99:2f:00:b2:31:97:6c:bf:ae:d1:16:f1:a2:3e:2d:
         2e:fb:0b:e9:9a:0e:eb:94:ac:08:b7:56:10:39:02:db:7f:45:
         ad:db:68:59:17:a3:8e:d8:fe:eb:90:1a:09:df:3b:c1:8e:7e:
         03:98:f8:95:24:ca:82:71:c3:e4:b8:82:ad:52:d2:34:dc:83:
         1e:5e:f9:f0:41:c0:39:66:4d:b2:71:3e:1e:c4:5c:7d:16:be:
         f2:03:51:ea:12:6d:e9:bc:01:bd:ff:59:f5:f0:6b:69:16:b6:
         b5:2f:9c:b1:0e:3b:dc:9e:87:67:4d:4a:cc:d2:8d:b3:ed:97:
```

192.168.1.1/cgi-bin/ipsec.cgi?act=info&file=cert&type=remote

Remote

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            11:7b:6b:e0:41:bf:36:3f
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CH, O=strongSwan, CN=IPsec Root CA
        Validity
            Not Before: Aug  9 09:43:17 2017 GMT
            Not After : Aug  8 09:43:17 2020 GMT
        Subject: C=CH, O=strongSwan, CN=remote.ipsec
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ca:8a:8d:b5:e2:eb:1e:de:d6:79:12:4c:2d:01:
                    43:b3:ff:69:f8:69:2d:27:ed:0b:4d:26:1f:ed:b3:
                    c0:36:9a:d7:23:d0:a7:7a:e6:f2:b7:b8:e0:91:3d:
                    20:ff:c4:06:37:90:3c:16:f0:dc:c5:12:a1:8c:a2:
                    70:3b:51:11:26:9d:5b:59:a2:16:4f:68:8f:c2:8e:
                    b1:ed:ee:85:42:a7:79:51:46:ac:70:69:e0:f1:61:
                    38:c6:10:40:07:98:e0:cd:36:59:a6:4c:bd:ac:aa:
                    2f:c1:f4:64:f1:52:48:8a:f8:6c:4b:26:2f:d9:96:
                    9a:f1:7c:18:4e:5d:40:29:3d:5a:c2:4d:33:07:6a:
                    4f:b8:12:43:42:6a:4b:b7:f0:d6:52:3b:e3:9b:b2:
                    85:20:41:93:e3:6b:de:bb:9e:91:01:4f:7c:a0:ba:
                    58:ae:ff:2e:5e:74:5f:2a:16:e3:8d:86:5c:9d:c3:
                    15:44:61:f6:03:fa:66:2f:c0:ed:0b:27:72:ac:3c:
                    49:79:0f:bd:d8:0d:8f:c3:5d:8f:d7:65:78:7a:8e:
                    e5:82:f1:54:56:d5:dc:f5:9f:fd:40:5e:58:37:67:
                    d0:92:02:00:bf:75:5b:5e:5e:9e:12:e4:68:4e:e6:
                    c5:2f:82:71:84:c7:63:b5:65:18:52:2a:d4:3a:02:
                    df:1d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:

keyid:22:91:1D:AA:3E:E2:77:87:DC:1B:B9:CA:5E:77:2D:D5:81:46:86:3B

            X509v3 Subject Alternative Name:
                DNS:remote.ipsec
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
    Signature Algorithm: sha256WithRSAEncryption
         20:1e:6e:bc:30:6f:8c:05:5b:e1:59:ad:f6:c3:de:75:15:92:
         7f:ee:53:65:18:11:1a:76:5b:02:af:15:be:8d:16:56:08:21:
         ee:4d:9f:c1:0d:14:f3:7c:ad:d9:86:92:37:7c:20:9f:fc:9b:
         c3:e0:d3:ff:f8:37:5b:3d:98:70:5b:c4:55:3a:cc:d8:ed:4e:
         78:7c:07:8b:cc:8b:ea:38:fa:ee:58:46:67:9a:17:57:d7:e8:
         21:96:2d:ac:f1:56:5e:53:1e:81:9d:3b:c8:fb:1f:e5:d6:fd:
         3b:2c:ac:17:be:72:f8:96:5d:e5:ba:e9:bf:d9:96:16:c8:a0:
         9b:ac:f2:3b:85:48:41:53:c5:43:f0:e7:56:ac:11:6b:59:fb:
         a3:e1:df:e6:0a:14:aa:00:cc:93:29:b7:84:66:32:98:0d:16:
```

Import Certificate

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

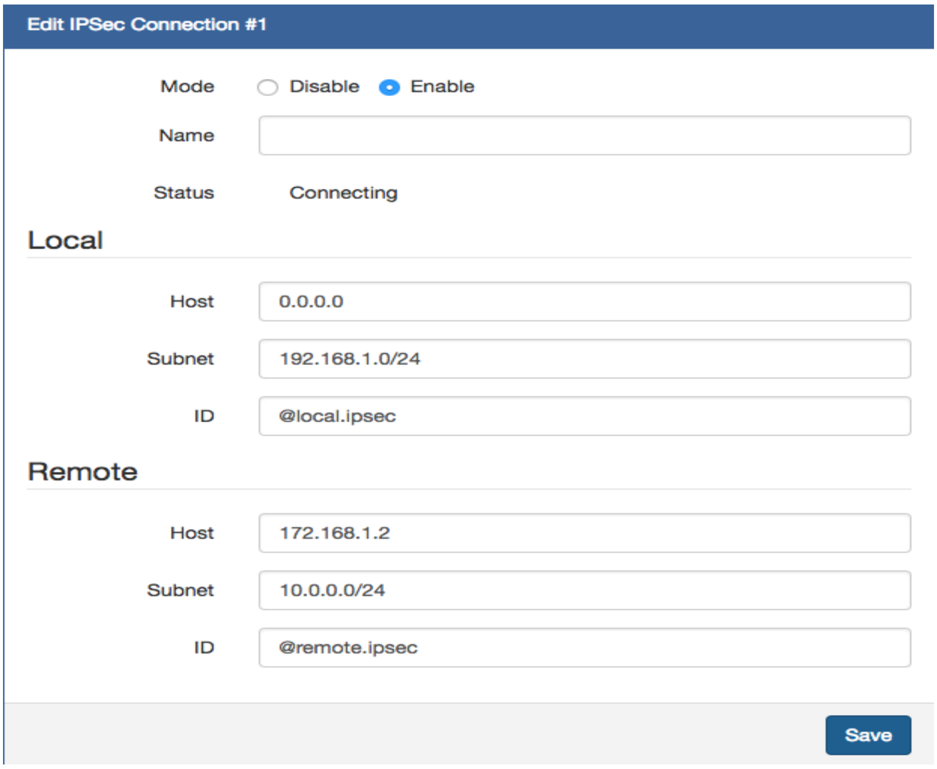
The mapping is as below:

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

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

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

Local Side



Edit IPSec Connection #1

Mode ○ Disable ● Enable

Name

Status Connecting

Local

Host 0.0.0.0

Subnet 192.168.1.0/24

ID @local.ipsec

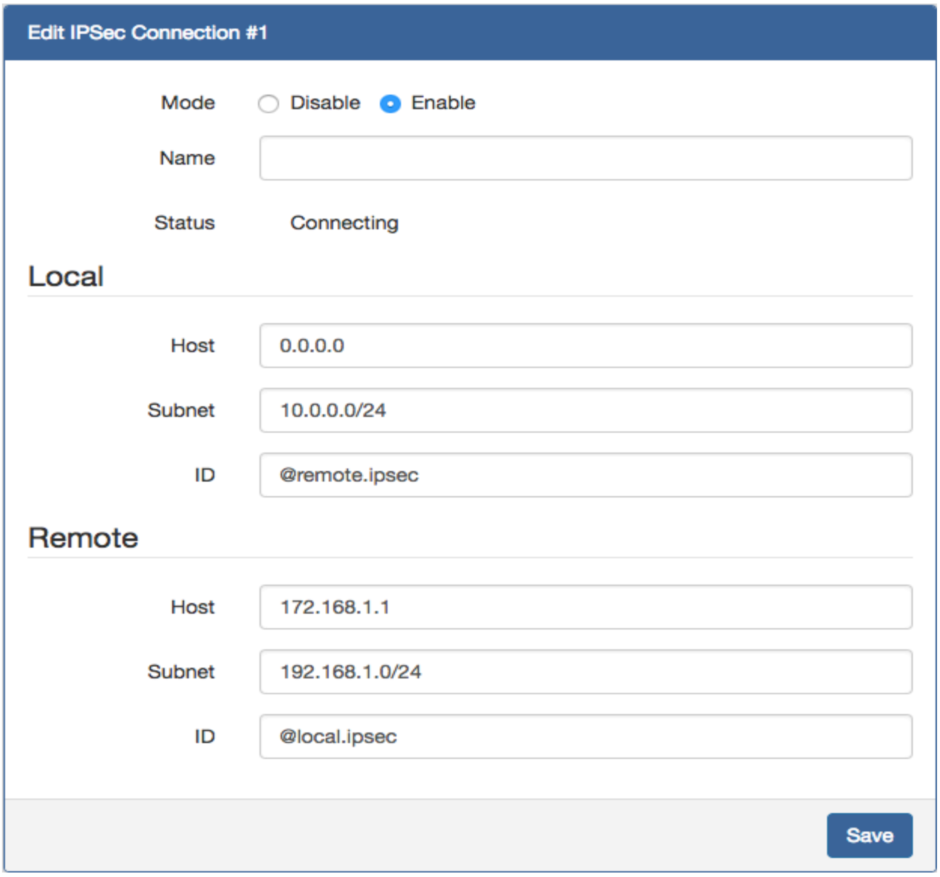
Remote

Host 172.168.1.2

Subnet 10.0.0.0/24

ID @remote.ipsec

Remote Side



Edit IPSec Connection #1

Mode ○ Disable ● Enable

Name

Status Connecting

Local

Host 0.0.0.0

Subnet 10.0.0.0/24

ID @remote.ipsec

Remote

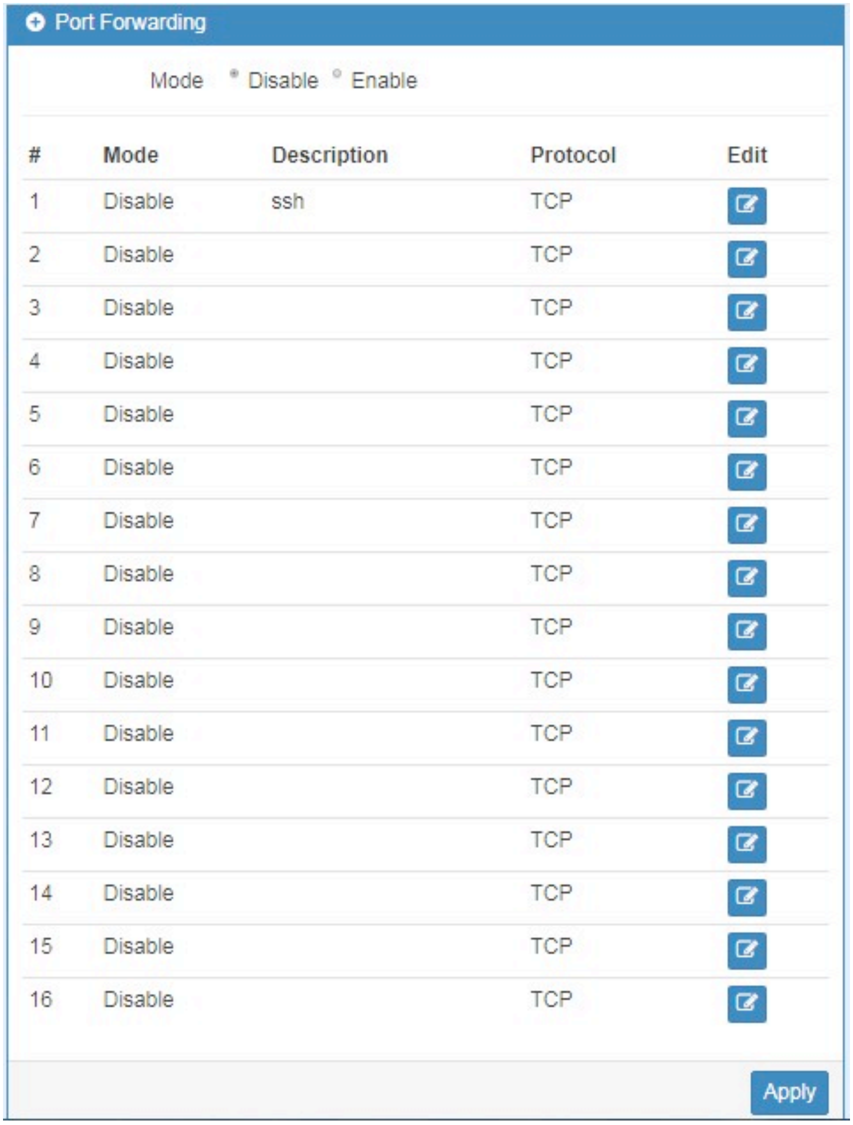
Host 172.168.1.1

Subnet 192.168.1.0/24

ID @local.ipsec

10.3 Service > Configuration Port Forwarding

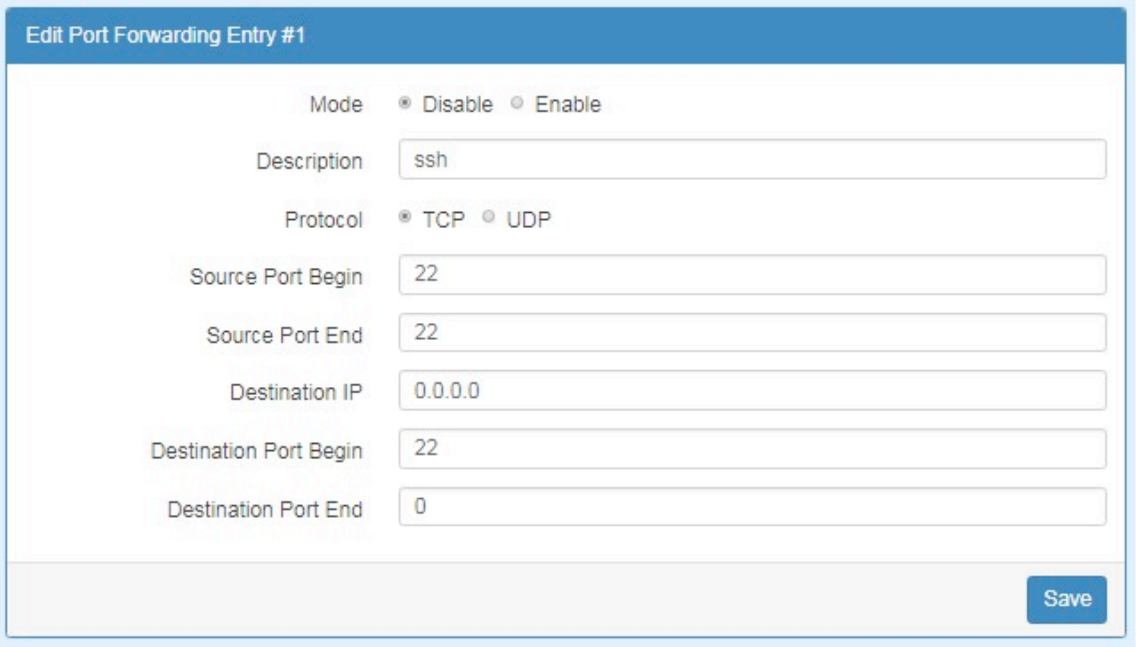
This section allows you to set up Port Forwarding and click ✎ edit button to configure.



Mode ● Disable ○ Enable

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

.

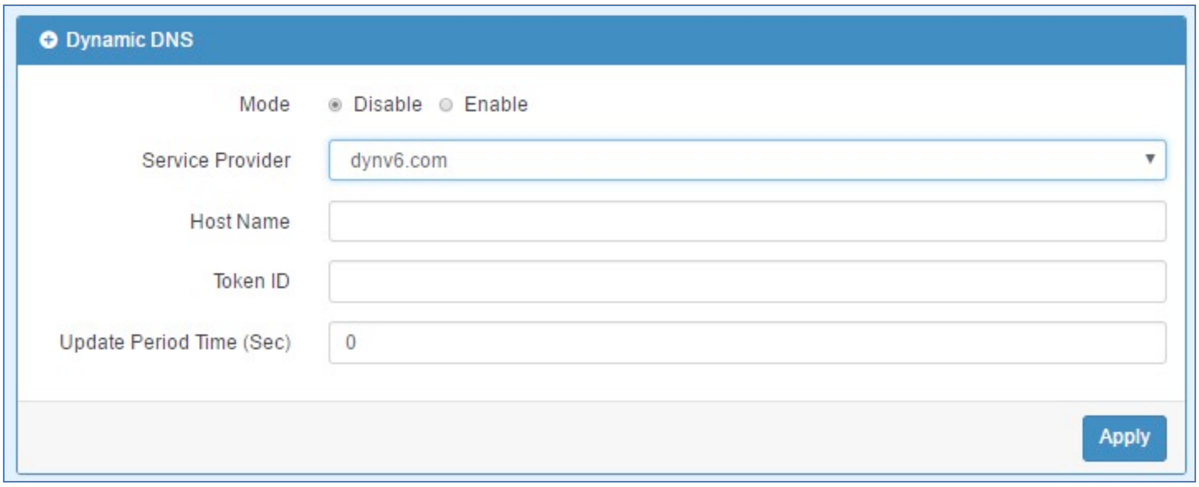


Mode	● Disable ○ Enable
Description	ssh
Protocol	● TCP ○ UDP
Source Port Begin	22
Source Port End	22
Destination IP	0.0.0.0
Destination Port Begin	22
Destination Port End	0

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

10.4 Service > Dynamic DNS

This section allows you to set up Dynamic DNS.



Dynamic DNS

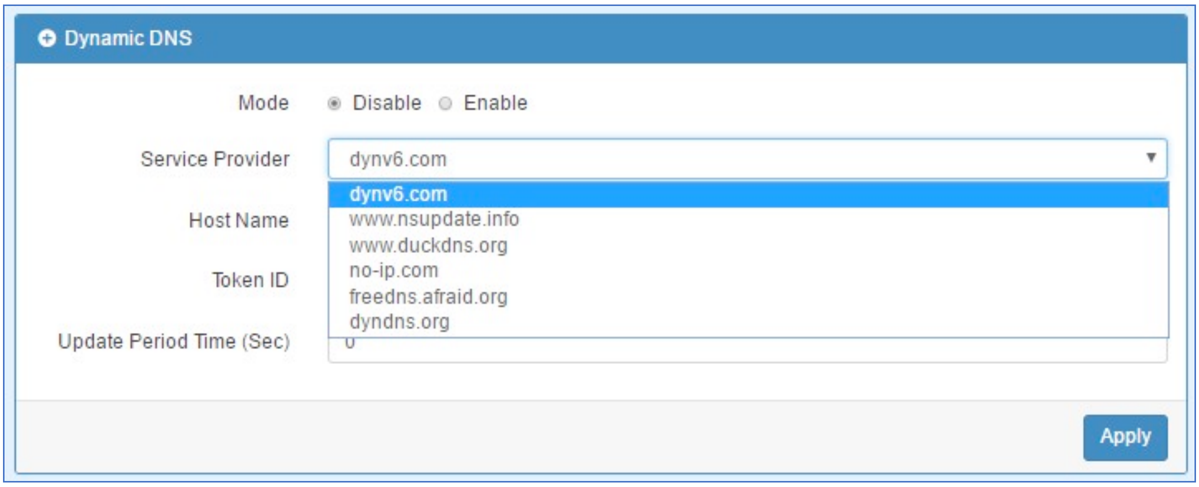
Mode ● Disable ○ Enable

Service Provider: dynv6.com

Host Name:

Token ID:

Update Period Time (Sec): 0



Dynamic DNS

Mode ● Disable ○ Enable

Service Provider: dynv6.com

Host Name:

Token ID:

Update Period Time (Sec): 0

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

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

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

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

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

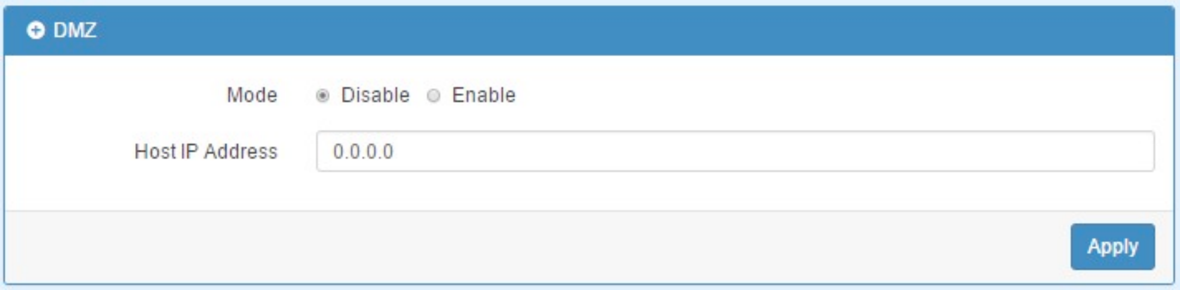
Service Provider	no-ip.com
Host Name	Register hostname, e.g. tester.hopto.org
Username	Register username.
Password	Register password.

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

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

10.5 Service > DMZ

This section allows you to set the DMZ configuration.



DMZ

Mode ● Disable ○ Enable

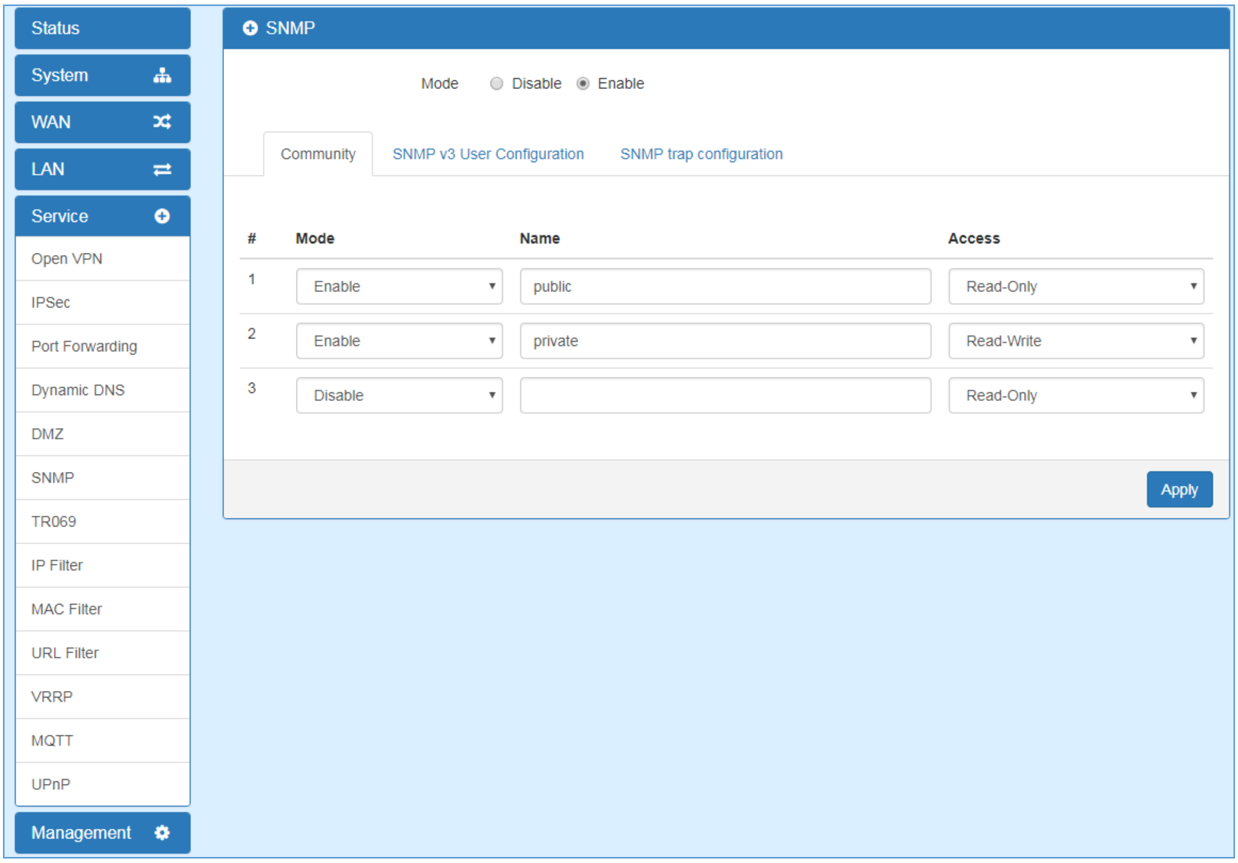
Host IP Address 0.0.0.0

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

10.6 Service > SNMP

10.6.1 SNMP configuration

This section allows you to set the SNMP configuration.



SNMP

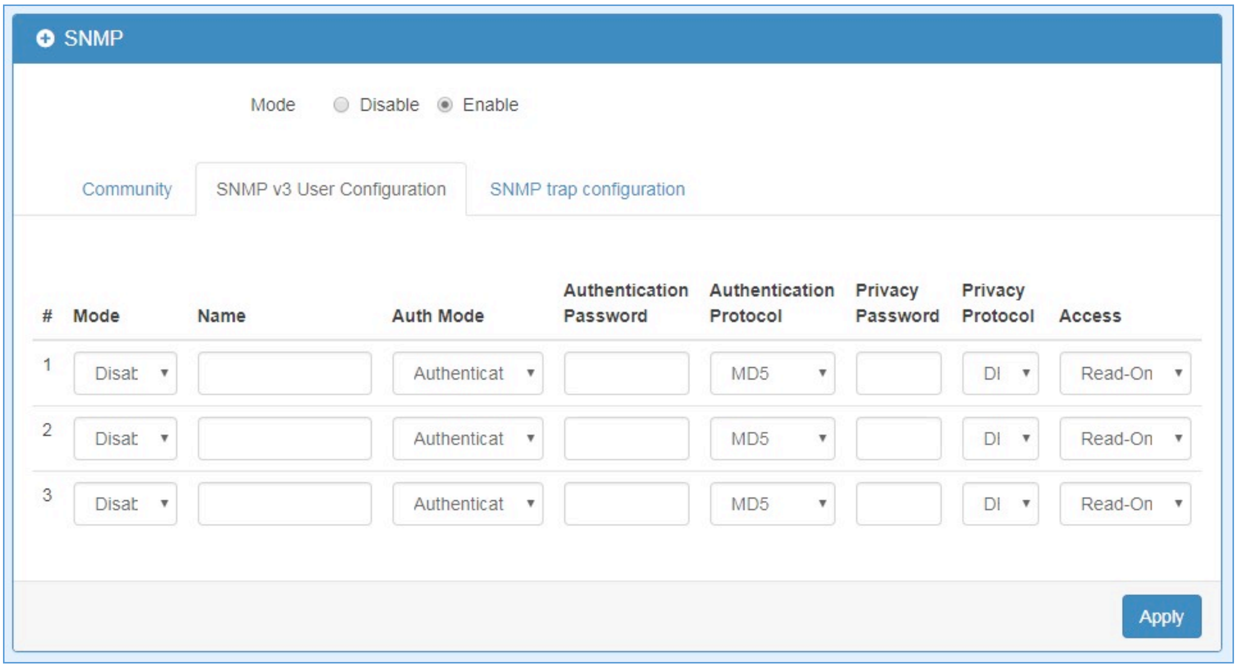
Mode ○ Disable ● Enable

#	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.

10.6.2 SNMP v3 User configuration

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



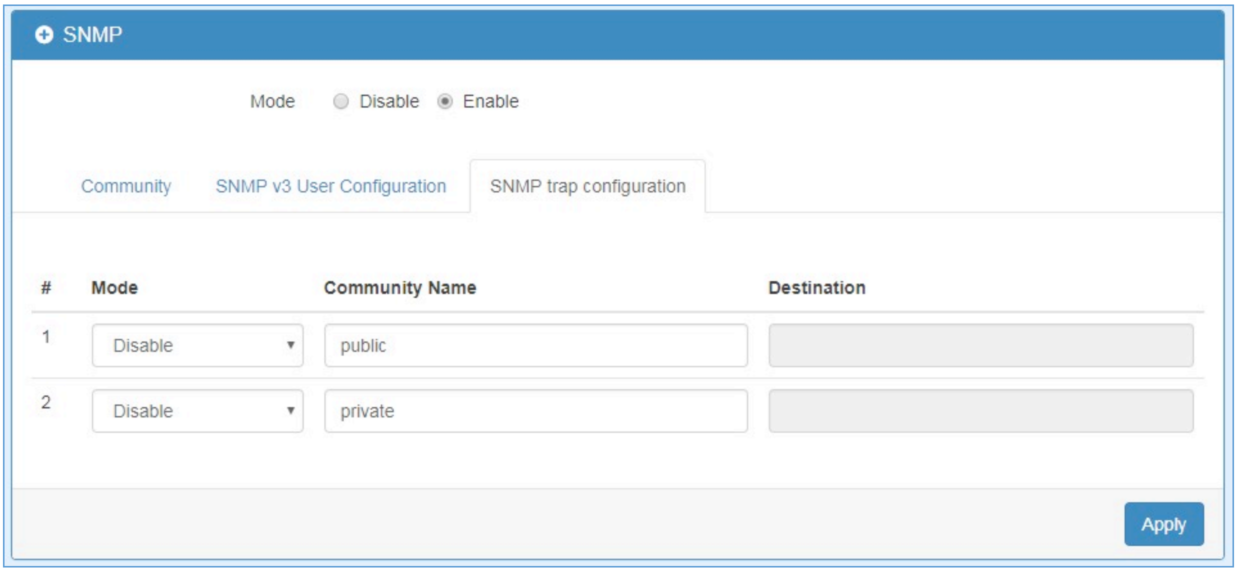
Mode ○ Disable ● Enable

#	Mode	Name	Auth Mode	Authentication Password	Authentication Protocol	Privacy Password	Privacy Protocol	Access
1	Disat		Authenticat		MD5		DI	Read-On
2	Disat		Authenticat		MD5		DI	Read-On
3	Disat		Authenticat		MD5		DI	Read-On

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

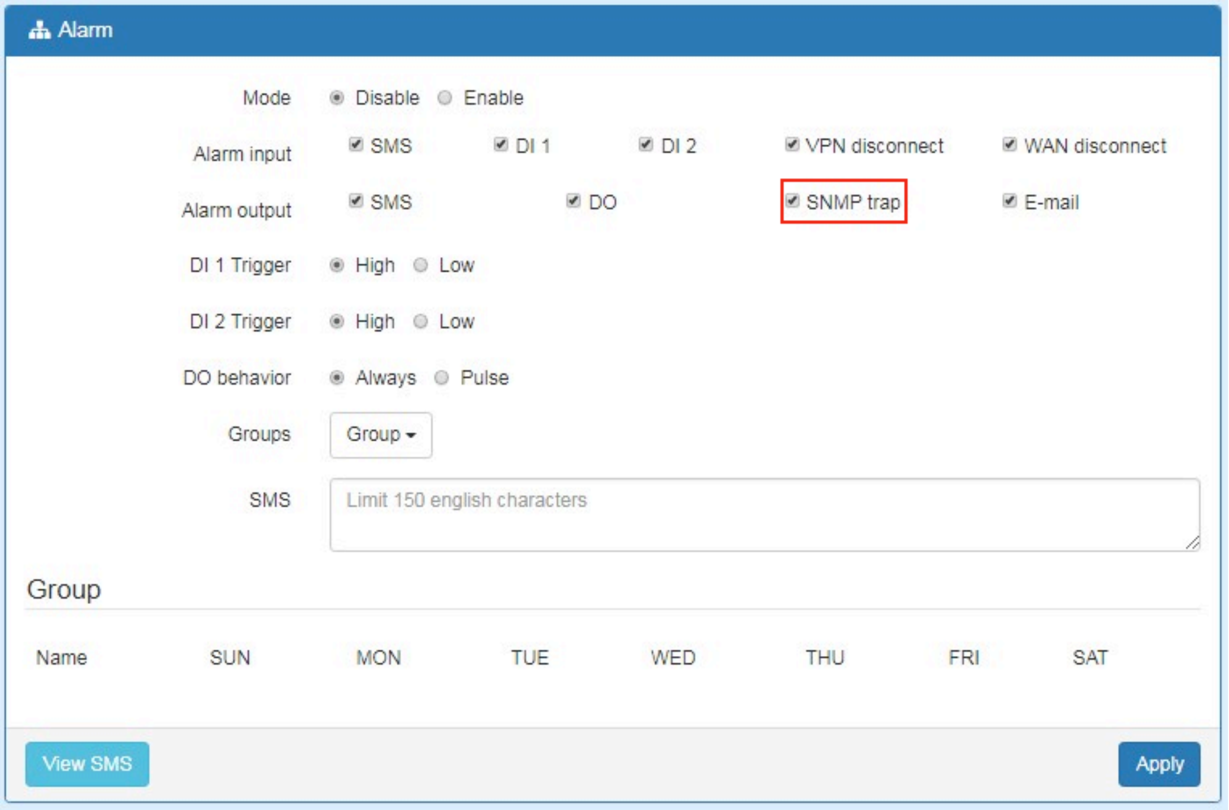
10.6.3 SNMP trap configuration

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



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

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

DI 1 Trigger ● High ○ Low

DI 2 Trigger ● High ○ Low

DO behavior ● Always ○ Pulse

Groups Group

SMS Limit 150 english characters

Group

Name	SUN	MON	TUE	WED	THU	FRI	SAT

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

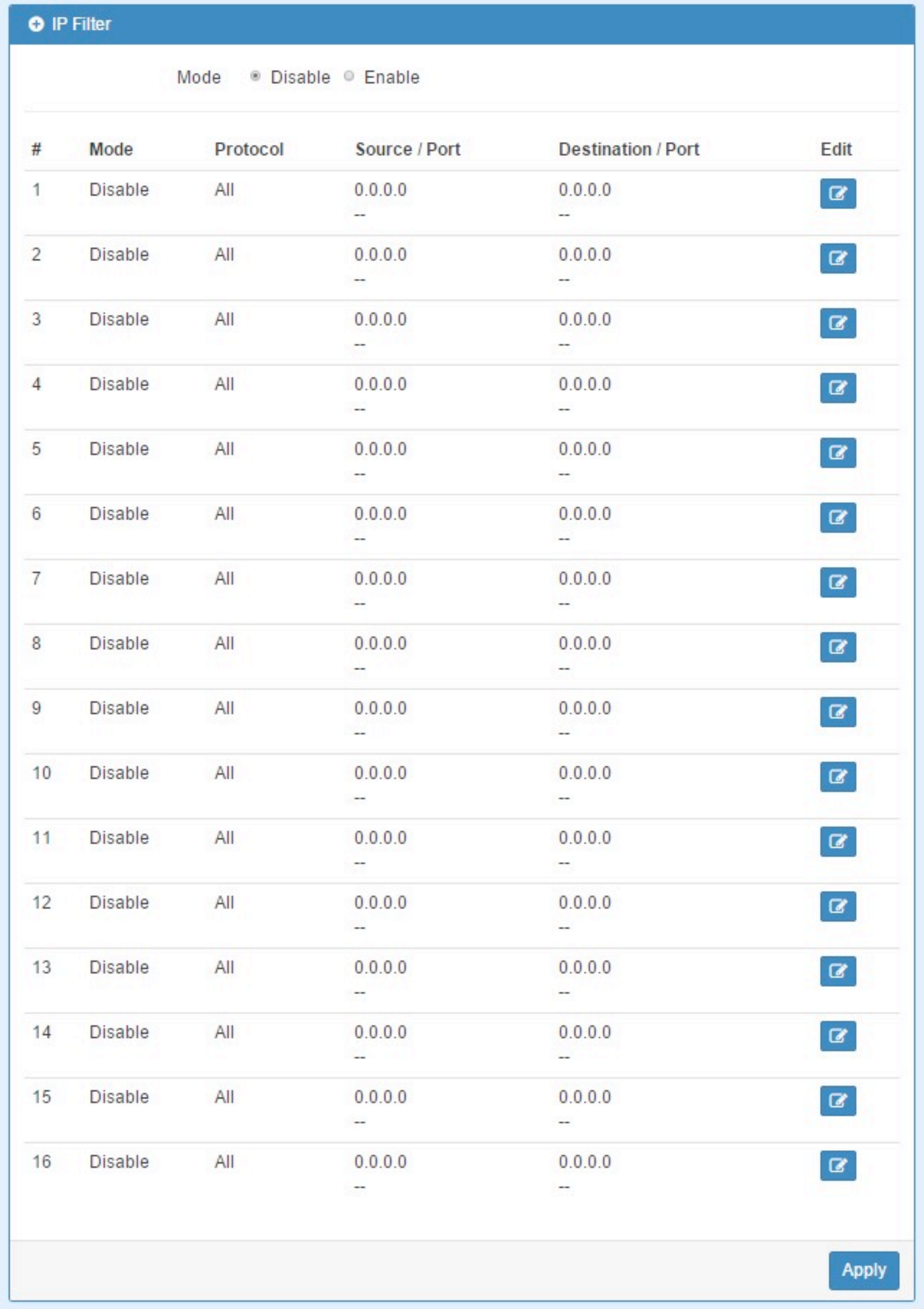
10.7 Service > TR069

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

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

10.8 Service > IP Filter

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

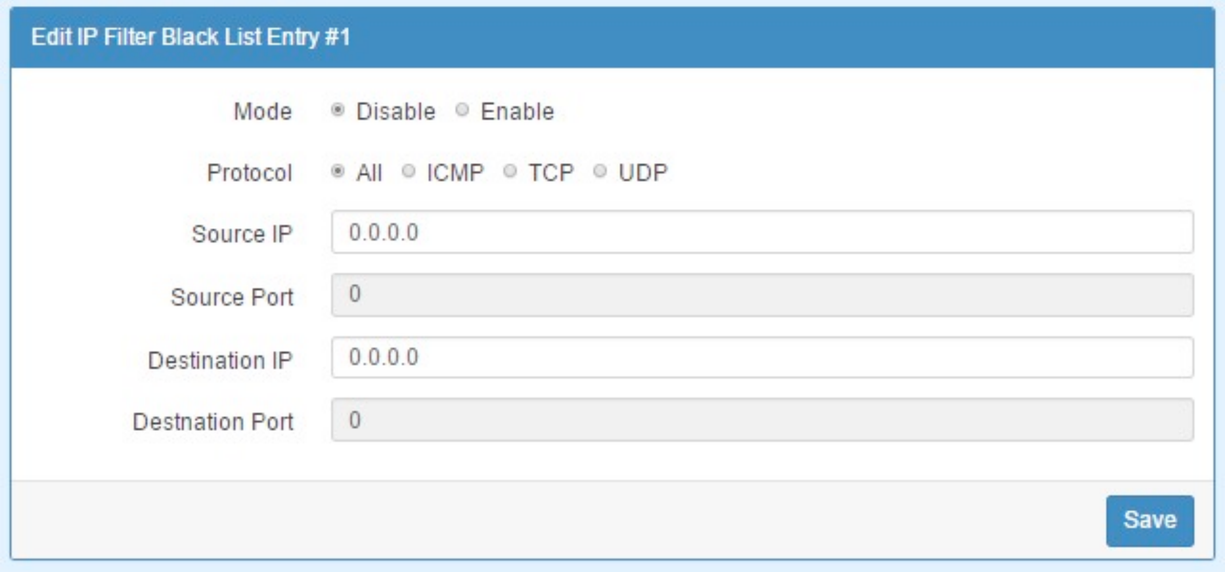


IP Filter

Mode ● Disable ○ Enable

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

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



Edit IP Filter Black List Entry #1

Mode ● Disable ○ Enable

Protocol ● All ○ ICMP ○ TCP ○ UDP

Source IP 0.0.0.0

Source Port 0

Destination IP 0.0.0.0

Destnation Port 0

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

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

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

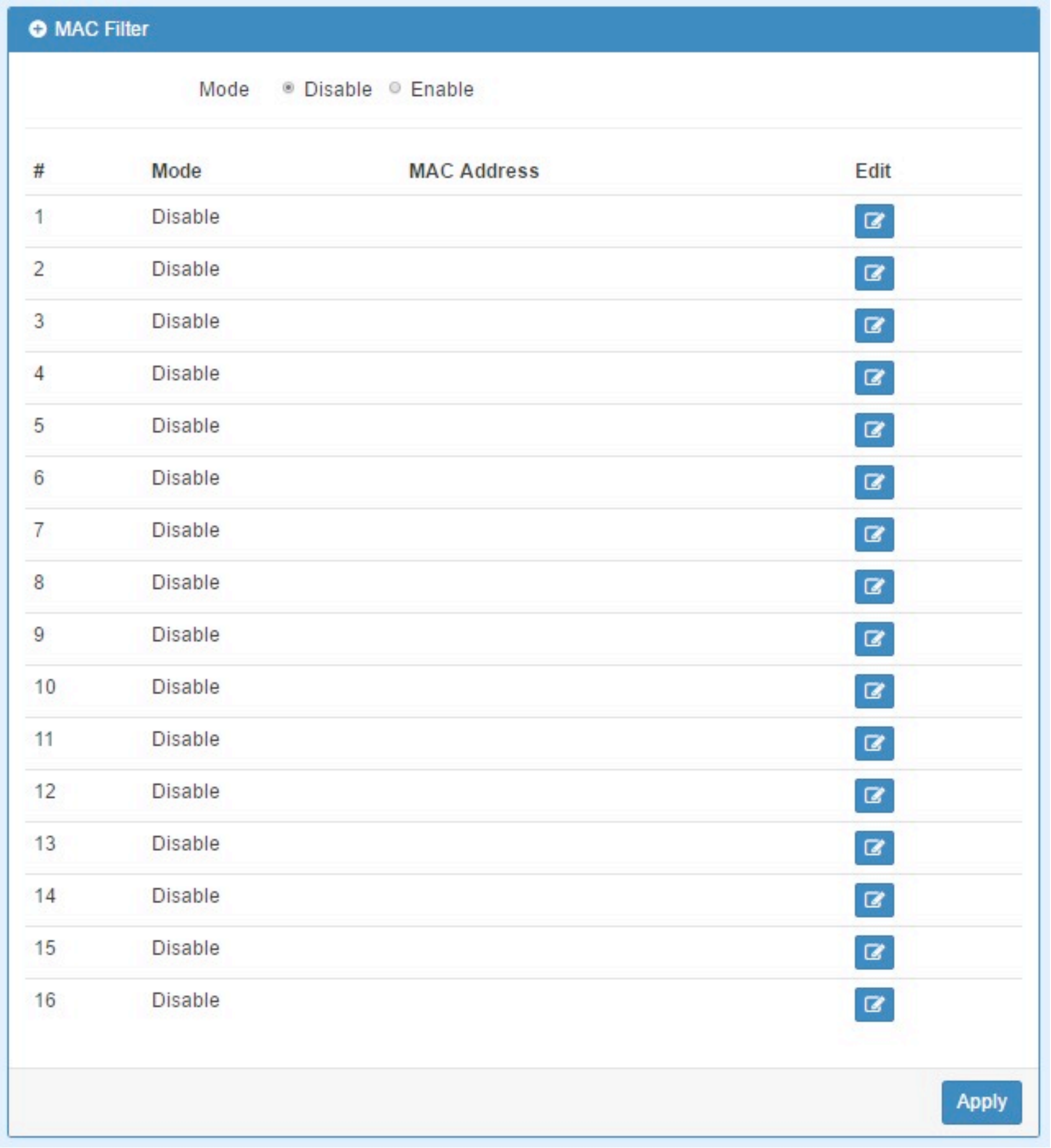
Service > Edit IP Filter > Source IP			
IP Format	**Single IP**	**IP with Mask**	**Ranged IP**
IPv4	192.168.0.123	192.168.1.0/24 192.168.1.0/255.255.255.0	192.168.1.1-192.168.1.123
IPv6	2607:f0d0:1002:51::4	2607:f0d0:1002:51::0/64	2607:f0d0:1002:51::4- 2607:f0d0:1002:51::aaaa
Note: Setting up a range of IP, please use **–** hyphen symbol to mark your ranged IP.			

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

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

10.9 Service > MAC Filter

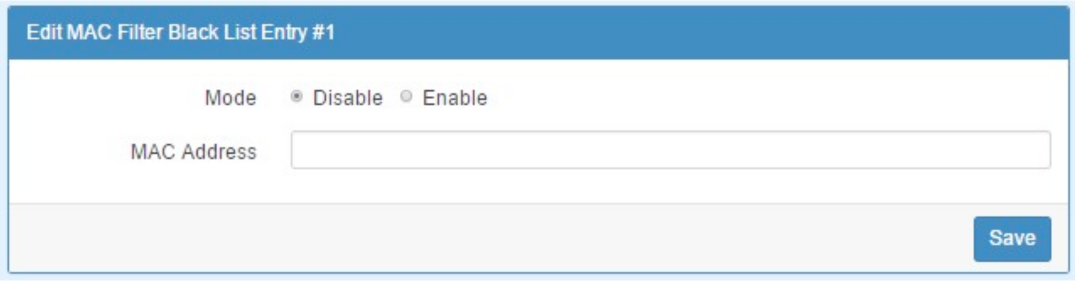
This section allows you to set up MAC Filter. After clicking ✎ button, you can edit your MAC address.



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

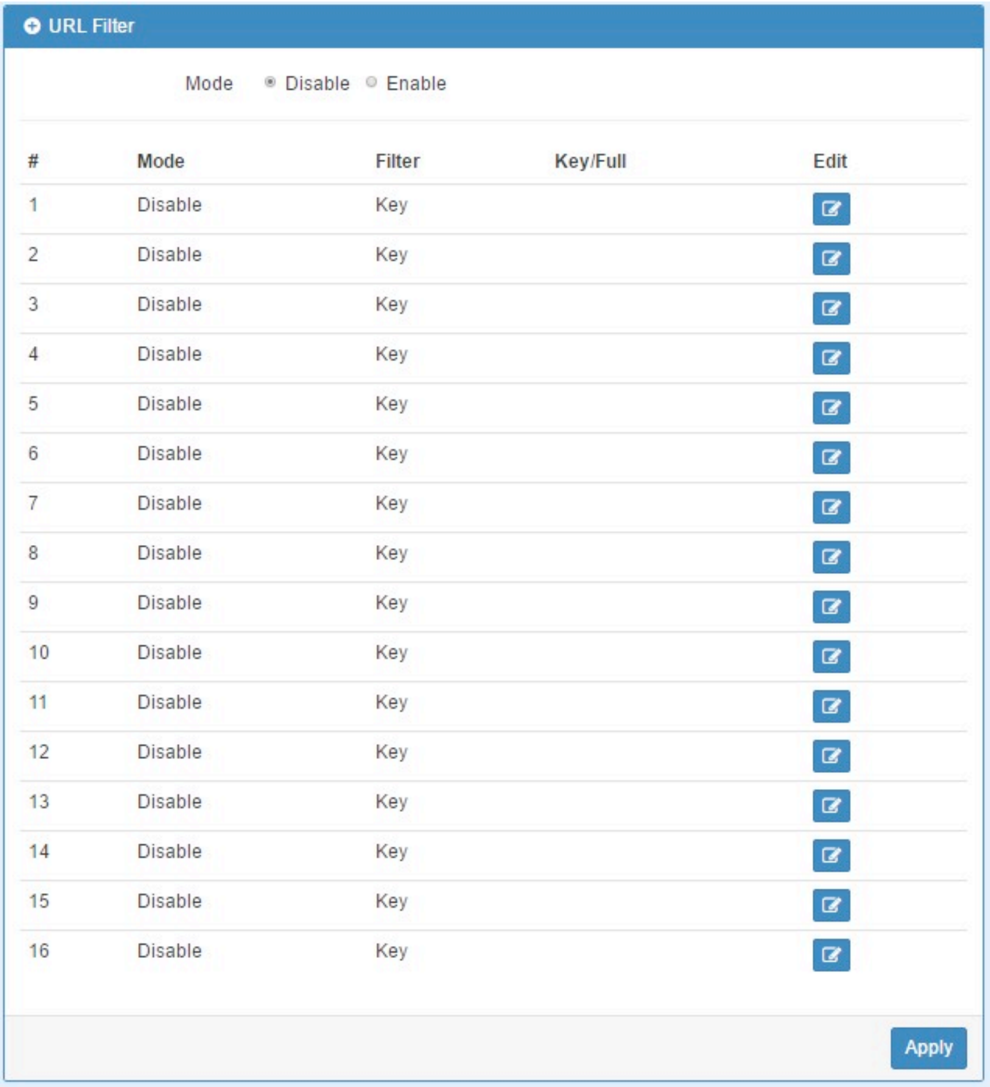
MAC Address

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).

10.10 Service > URL Filter

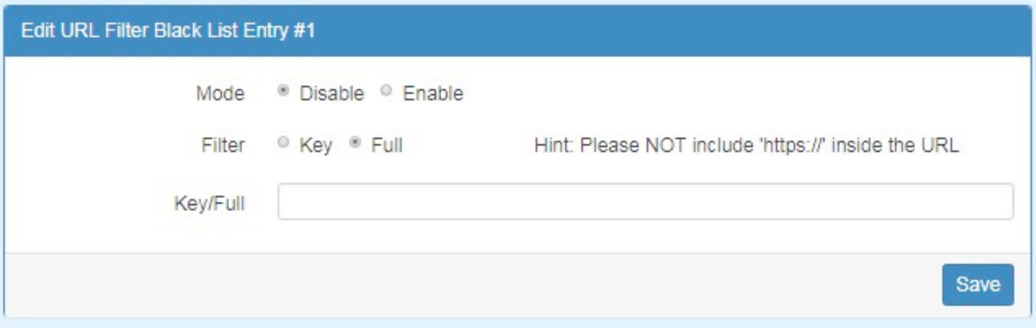
This section allows you to set up URL Filter. After clicking ✎ button, you can edit the type of filter and information.



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		✎



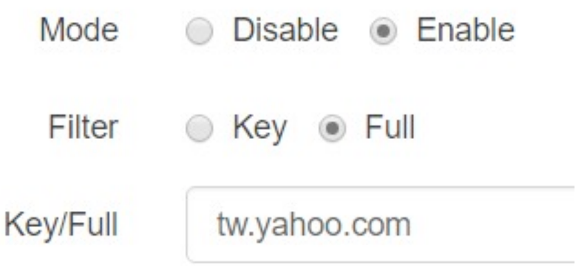
Edit URL Filter Black List Entry #1

Mode ● Disable ○ Enable

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

Key/Full

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



Mode ○ Disable ● Enable

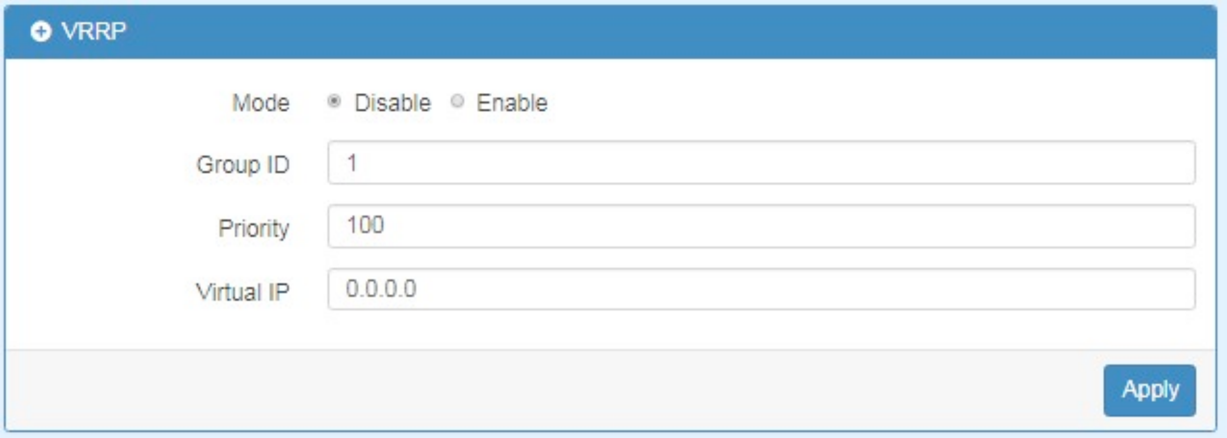
Filter ○ Key ● Full

Key/Full tw.yahoo.com

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

10.11 Service > VRRP

This section allows you to configure VRRP.



VRRP

Mode ● Disable ○ Enable

Group ID 1

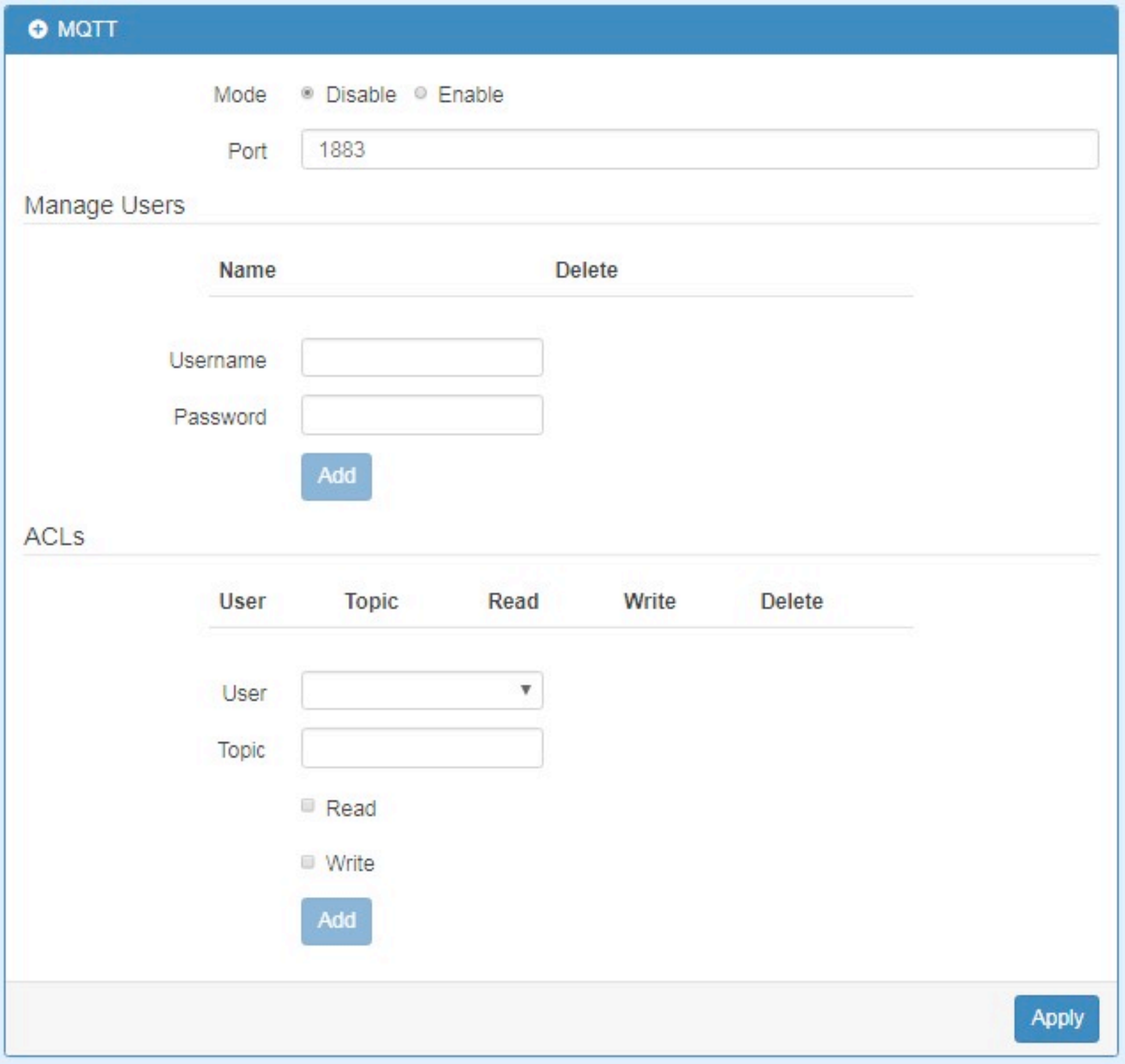
Priority 100

Virtual IP 0.0.0.0

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

10.12 Service > MQTT

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



MQTT

Mode ● Disable ○ Enable

Port 1883

Manage Users

Name	Delete

Username

Password

Add

ACLs

User	Topic	Read	Write	Delete

User

Topic

□ Read

□ Write

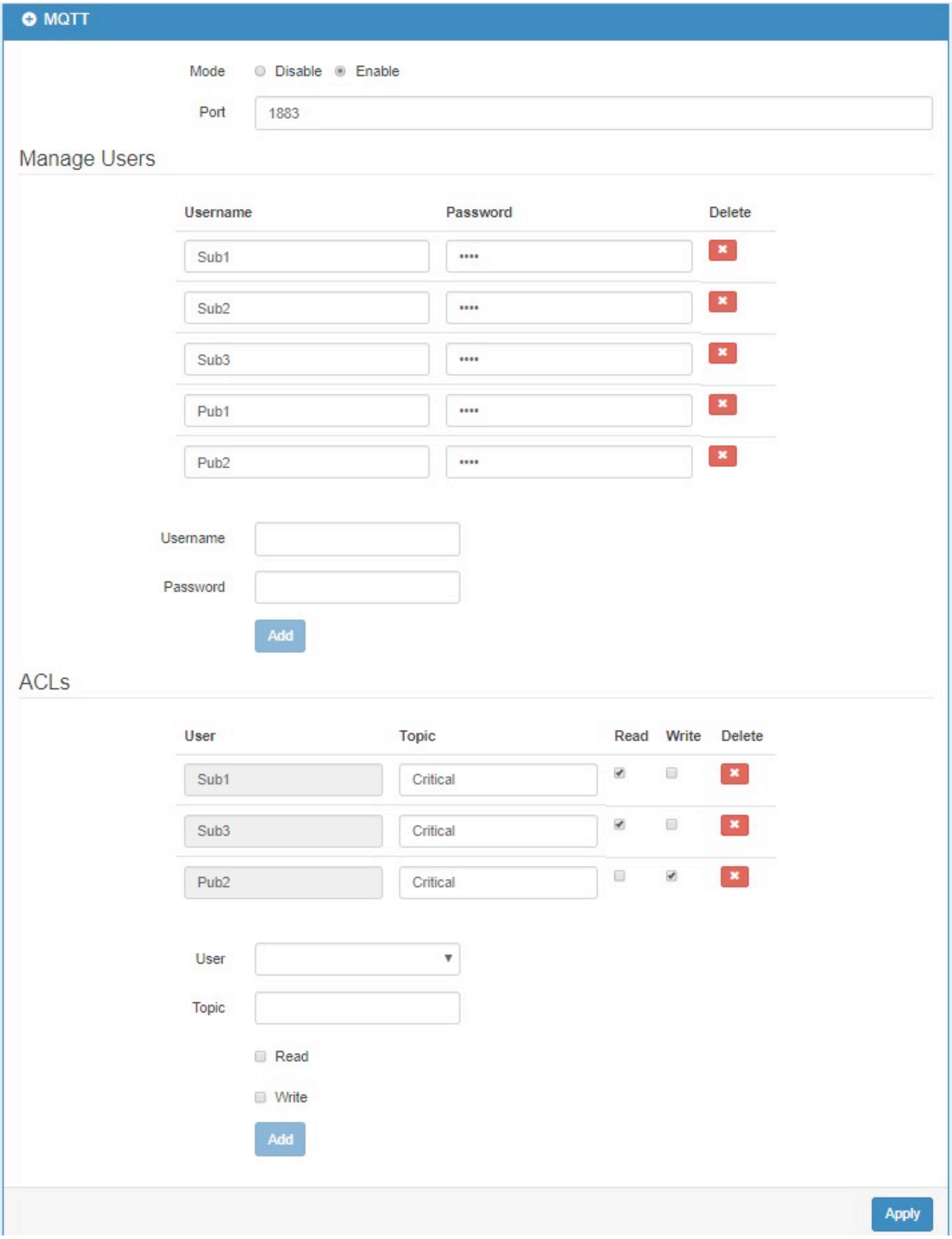
Add

Apply

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.

For example, the interface is shown as below:

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



Mode ○ Disable ● Enable

Port 1883

Manage Users

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

Username

Password

ACLs

User	Topic	Read	Write	Delete
Sub1	Critical	☑	□	✖
Sub3	Critical	☑	□	✖
Pub2	Critical	□	☑	✖

User

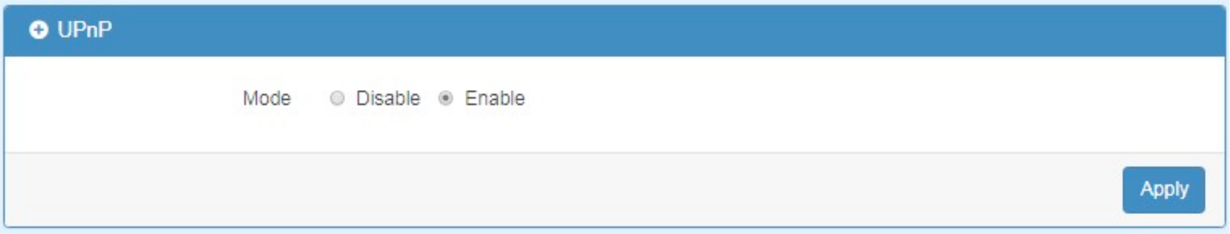
Topic

□ Read

□ Write

10.13 Service > UPnP

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



UPnP

Mode ○ Disable ● Enable

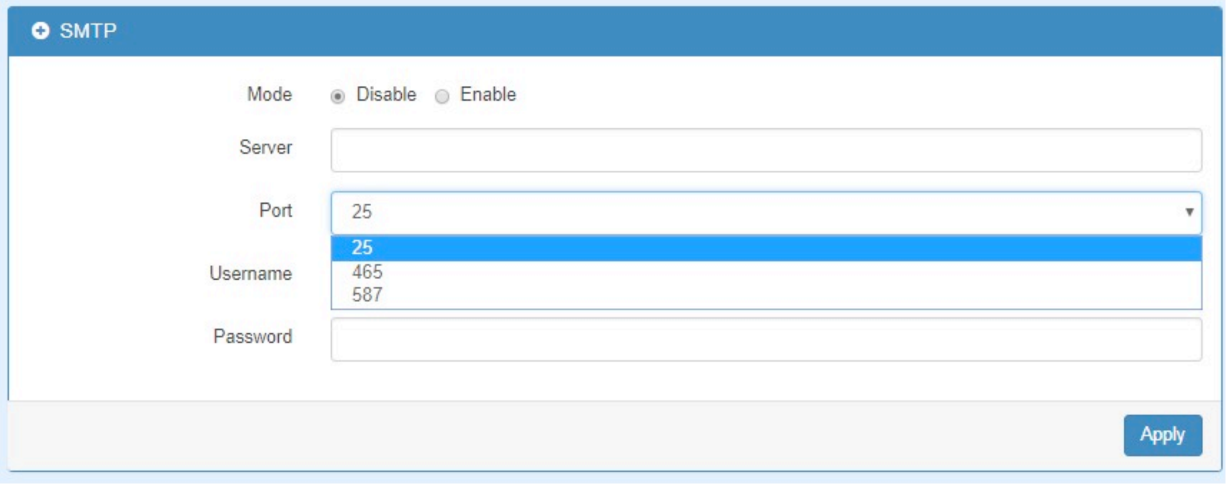
Note:

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.

10.14 Service > SMTP

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



SMTP

Mode ● Disable ○ Enable

Server

Port 25

25
465
587

Username

Password

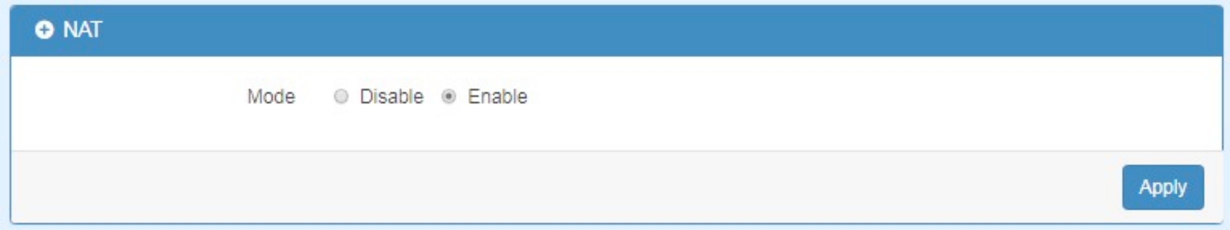
Service > SMTP	
Item	**Description**
Mode	Select from Disable or Enable. The default is Disable.
Server	The email will be sent through the server.
Port	There are three ports for SMTP communication between mail servers. ● **Port 25**：Use TCP port 25 without encryption. ● **Port 465**：SMTP connections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

10.15 Service > NAT

This section allows you to set NAT configuration.

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

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



NAT

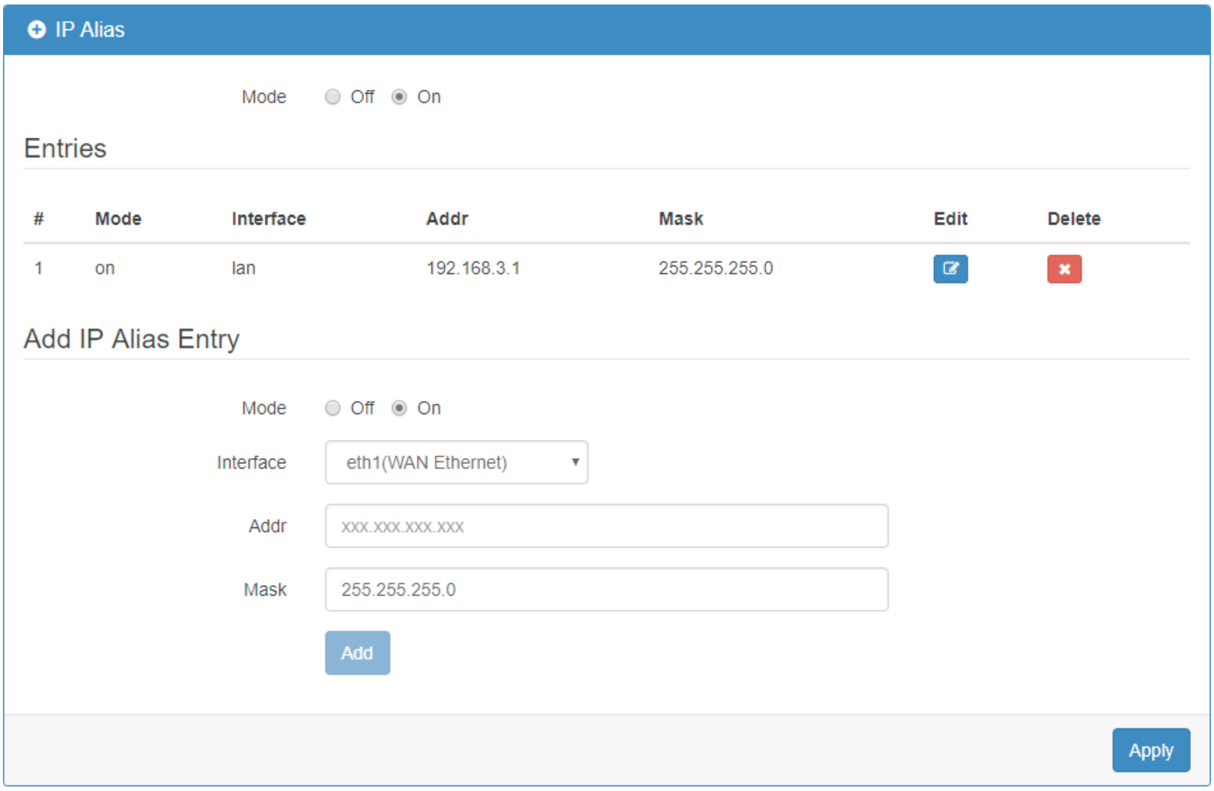
Mode ○ Disable ● Enable

10.16 Service > IP Alias

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

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

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



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

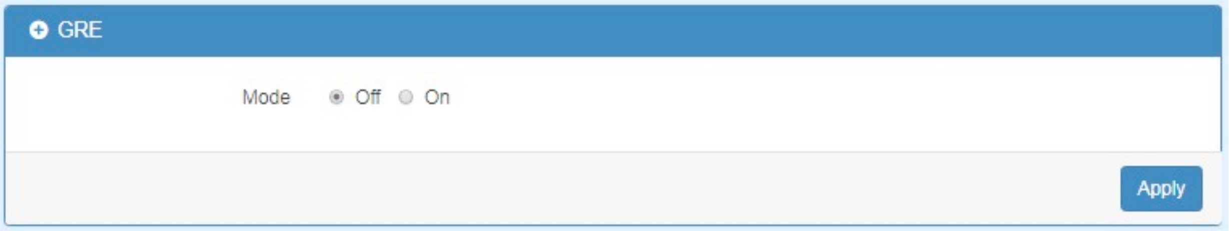
Mask: 255.255.255.0

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.

10.17 Service > GRE

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

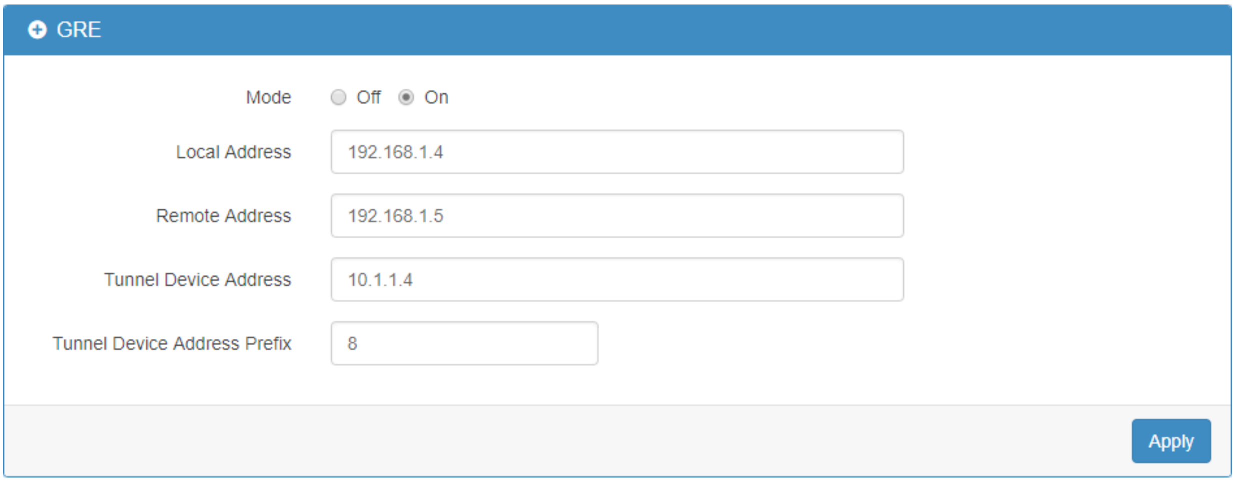
Generic Routing Encapsulation (GRE) is one of the available tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel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



GRE

Mode ● Off ○ On

The GRE Mode is on.



GRE

Mode ○ Off ● On

Local Address: 192.168.1.4

Remote Address: 192.168.1.5

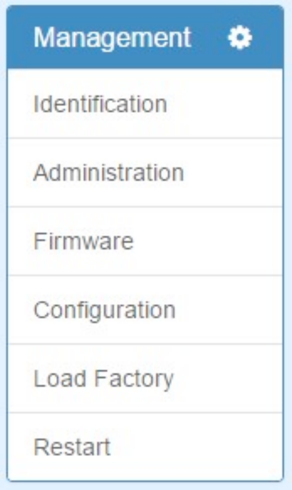
Tunnel Device Address: 10.1.1.4

Tunnel Device Address Prefix: 8

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

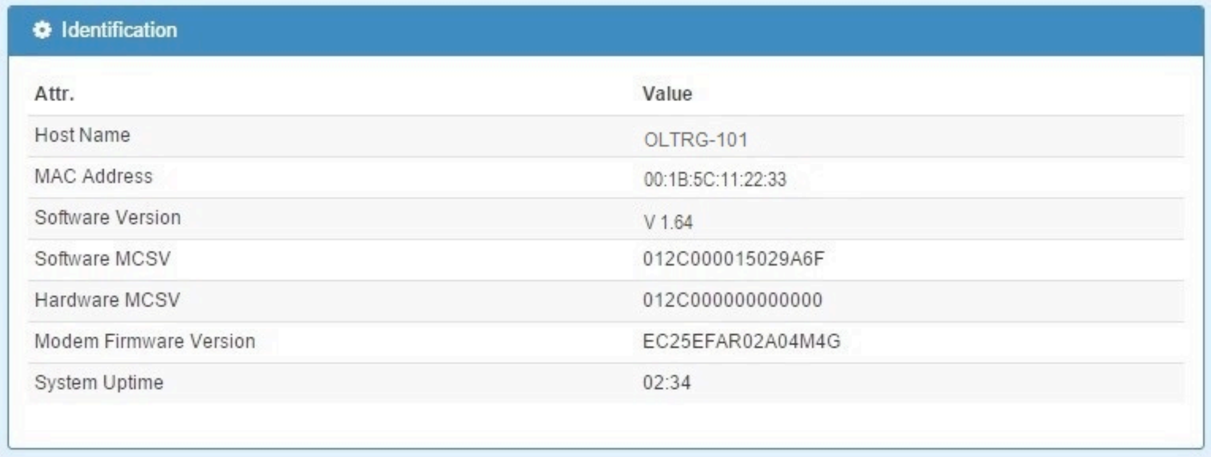
11 Management

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



11.1 Identification

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

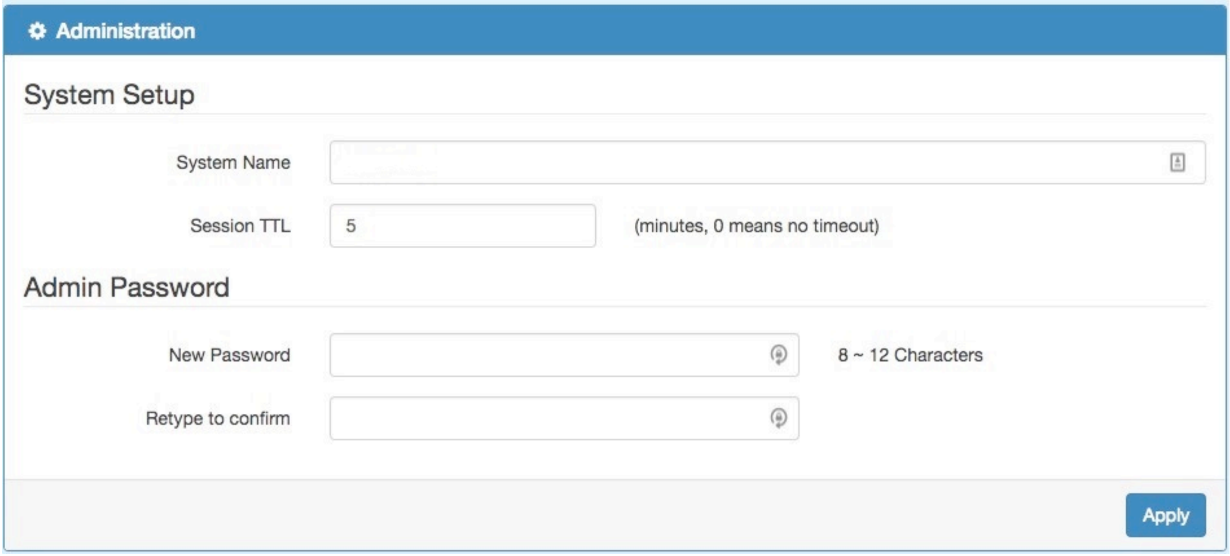


Attr.	Value
Host Name	OLTRG-101
MAC Address	00:1B:5C:11:22:33
Software Version	V 1.64
Software MCSV	012C000015029A6F
Hardware MCSV	012C000000000000
Modem Firmware Version	EC25EFAR02A04M4G
System Uptime	02:34

Management > Identification	
Item	**Description**
Host Name	Show the host name of cellular router.
MAC Address	Show the MAC address.
Software Version	Show the current software version.
Software MCSV	Show the current software MCSV.
Hardware MCSV	Show the current hardware MCSV.
Modem Firmware Version	Show the current firmware version.
System Uptime	Show the current system uptime.

11.2 Administration

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



Administration

System Setup

System Name

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

Admin Password

New Password — 8 ~ 12 Characters

Retype to confirm

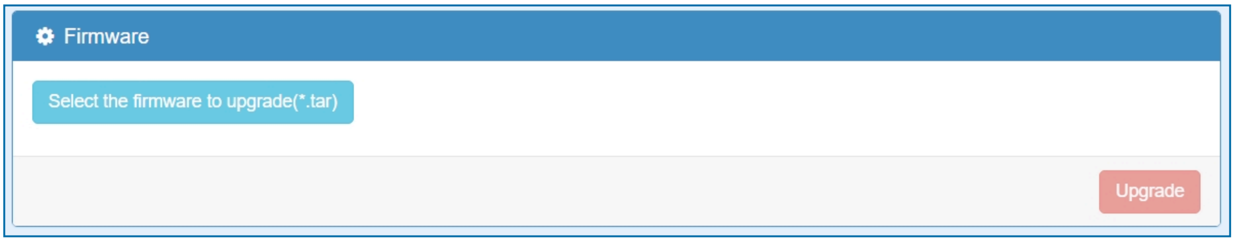
11.3 Firmware

This section provides you to upgrade the firmware of router.

(1) Click Select the firmware to upgrade button to choose your current firmware version in your PC.

(2) Select Upgrade button to update.

(3) After upgrading successfully, the router will reboot automatically.



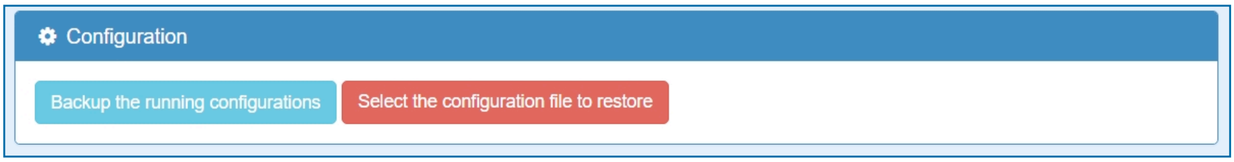
Firmware

11.4 Configuration

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

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

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

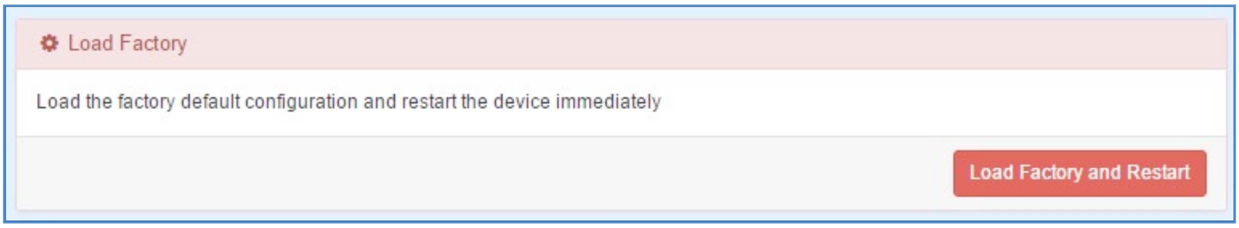


Configuration

Backup the running configurations
Select the configuration file to restore

11.5 Load Factory

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

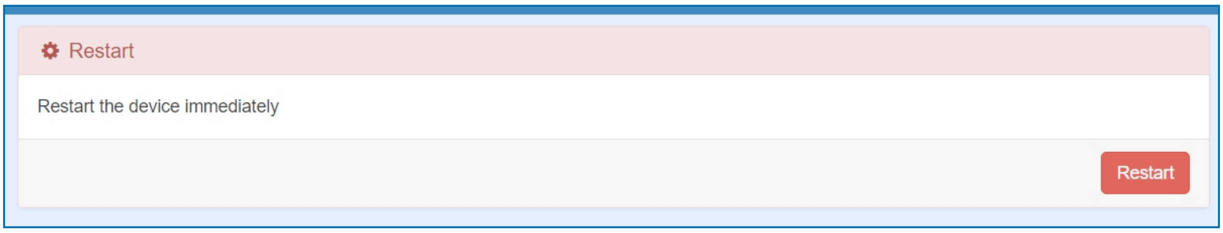


Load Factory

Load the factory default configuration and restart the device immediately

11.6 Restart

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



Restart

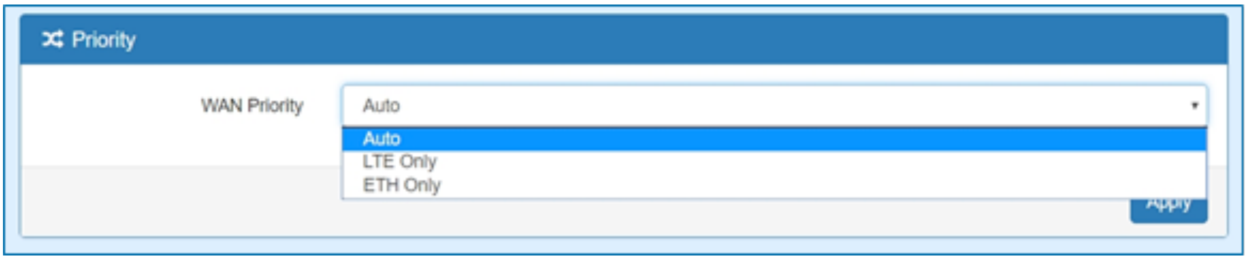
Restart the device immediately

12 Configuration Applications

This section explains specific examples how to configure your applications.

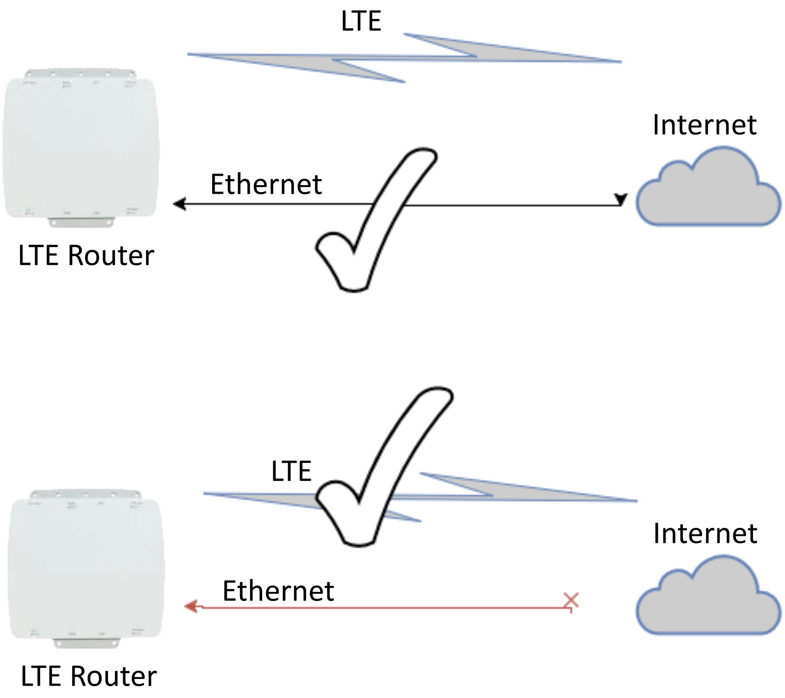
12.1 WAN Priority

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



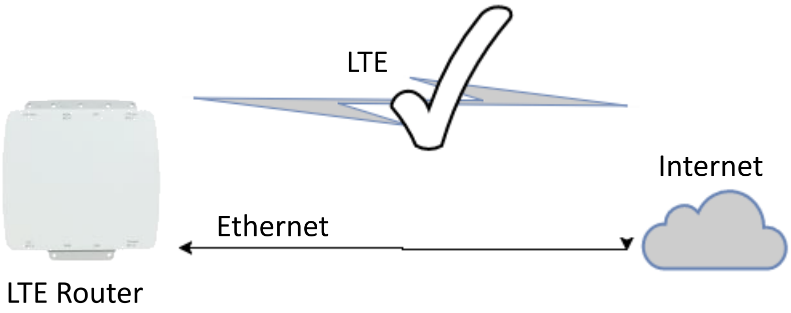
(1) WAN Priority > Auto:

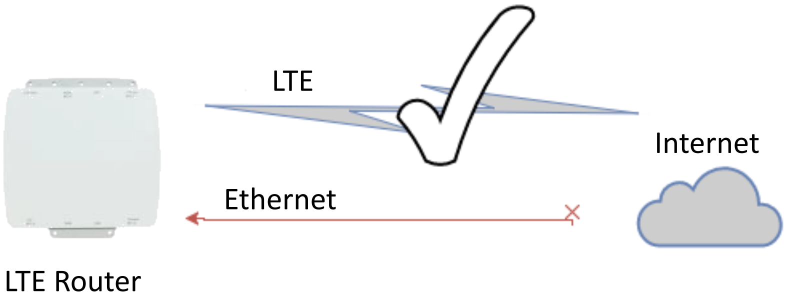
In case both Ethernet and LTE can access Internet, the router would route network packages through Ethernet. The reason is Ethernet that is low price and stable.
However, in case Ethernet is unplug or not able to access Internet (check by ping), the router would route network packages through LTE network.



(2) WAN Priority > LTE Only:

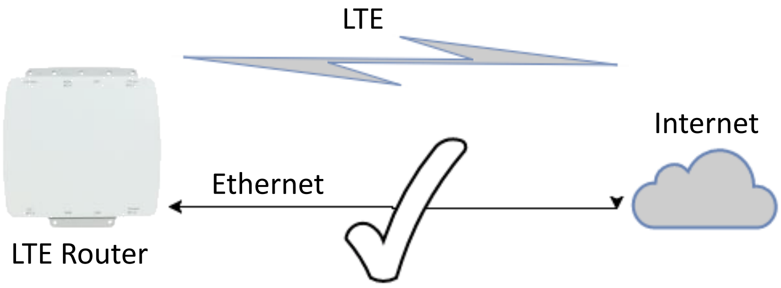
In this mode, the router only routes network packages through LTE.

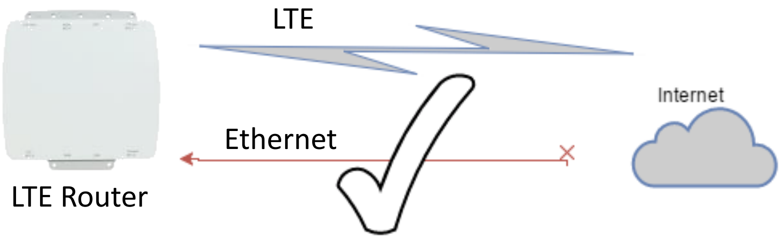




(3) WAN Priority > ETH Only:

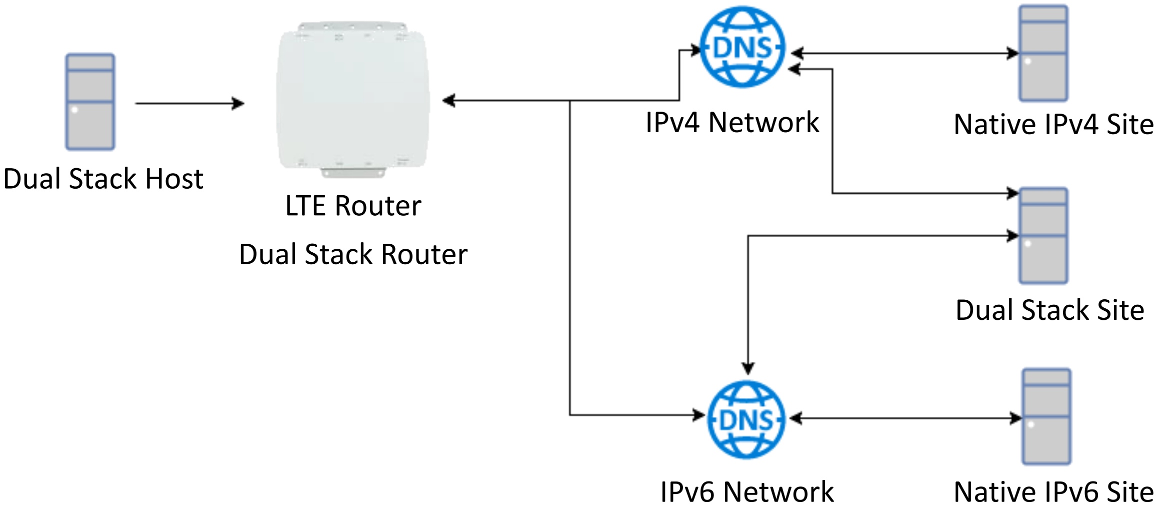
In this mode, the router only routes network packages through Ethernet.



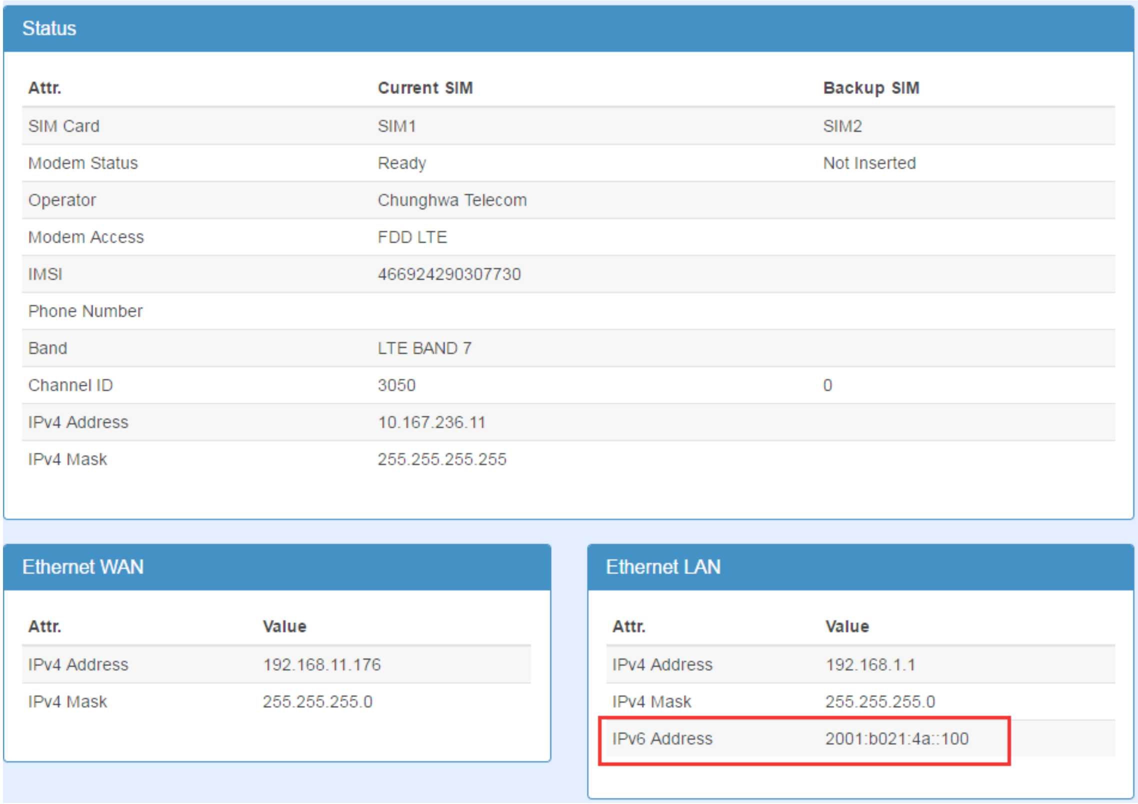


12.2 LAN > IPv4/IPv6 Dual Stack

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



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



Status

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

Ethernet WAN

Attr.	Value
IPv4 Address	192.168.11.176
IPv4 Mask	255.255.255.0

Ethernet LAN

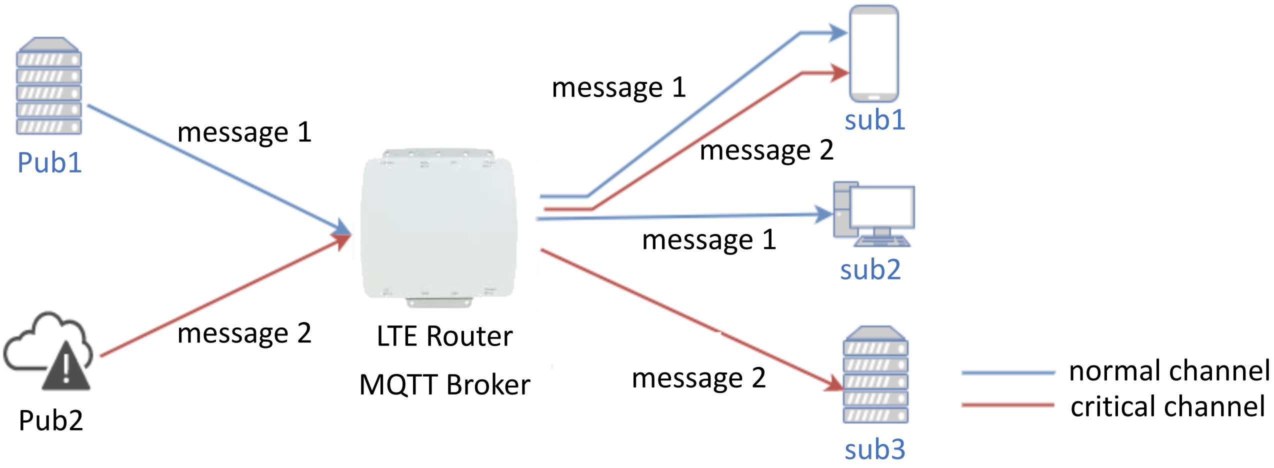
Attr.	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	2001:b021:4a::100

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

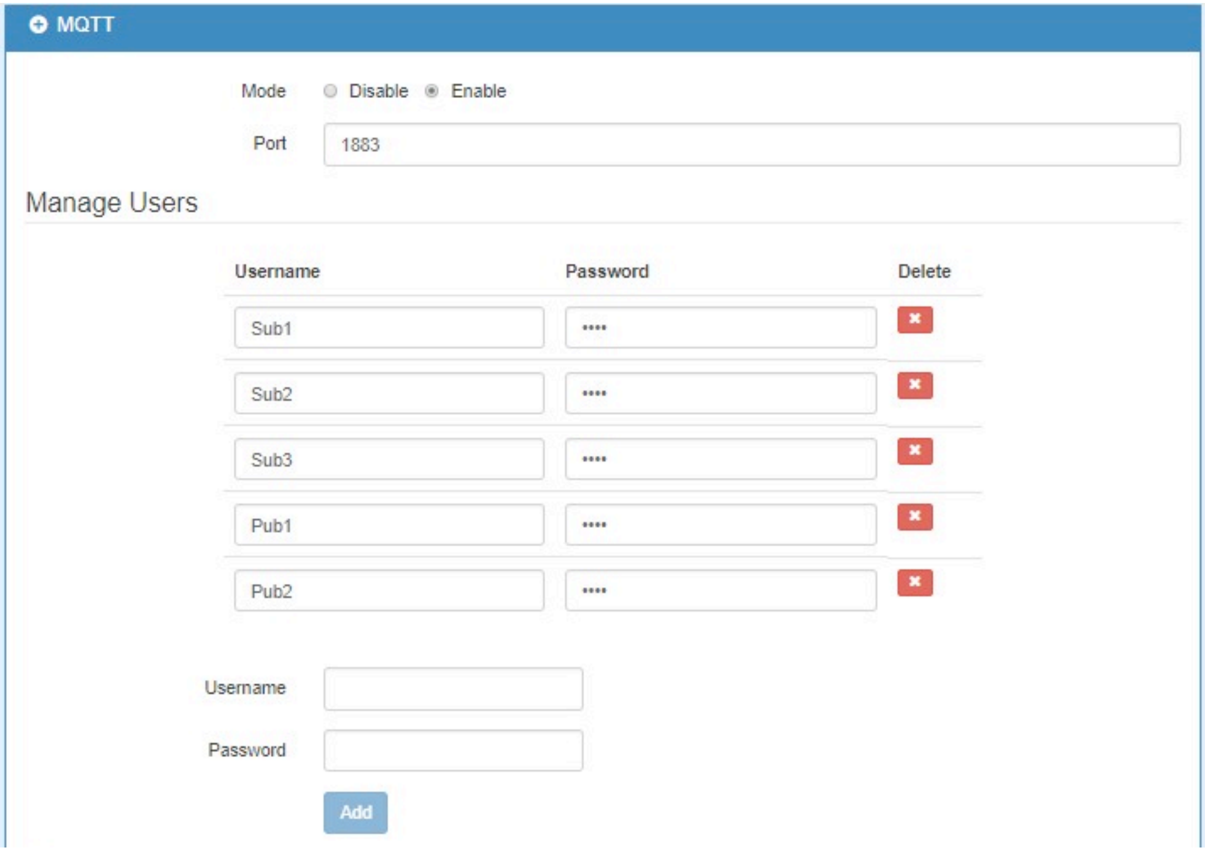
12.3 MQTT Broker

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

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



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



Mode ○ Disable ● Enable

Port 1883

Manage Users

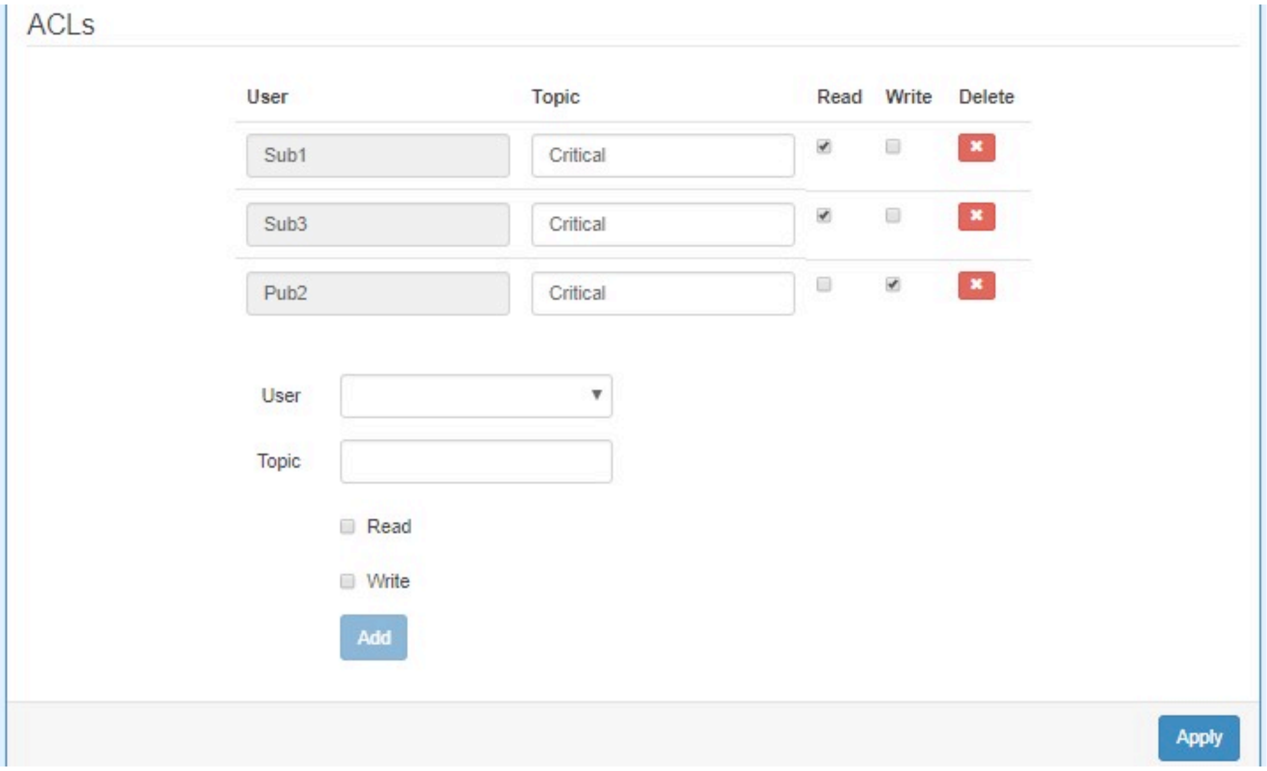
Username	Password	Delete
Sub1	••••	✖
Sub2	••••	✖
Sub3	••••	✖
Pub1	••••	✖
Pub2	••••	✖

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 **pub1** to write the critical topic.
Additionally, we also the subscribers **sub1** and **sub3** can read the critical topic.
Thus, when **pub1** is sending the message only the **sub1**, the **sub3** can receive it.



ACLs

User	Topic	Read	Write	Delete
Sub1	Critical	☑	□	☒
Sub3	Critical	☑	□	☒
Pub2	Critical	□	☑	☒

User

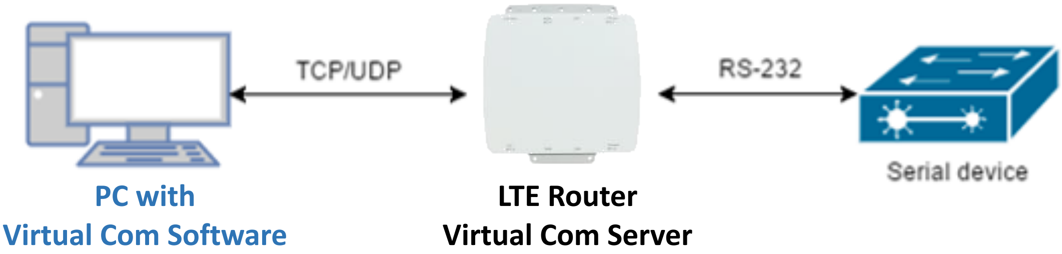
Topic

□ Read

□ Write

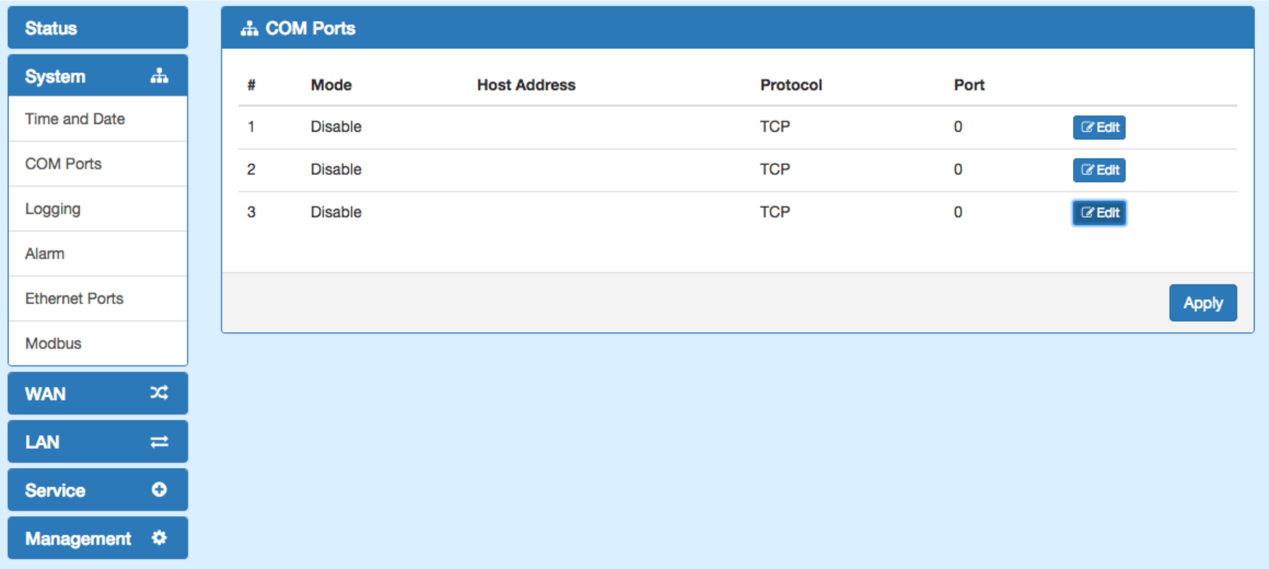
12.4 Virtual COM > Remote Management

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



- **How to set up**

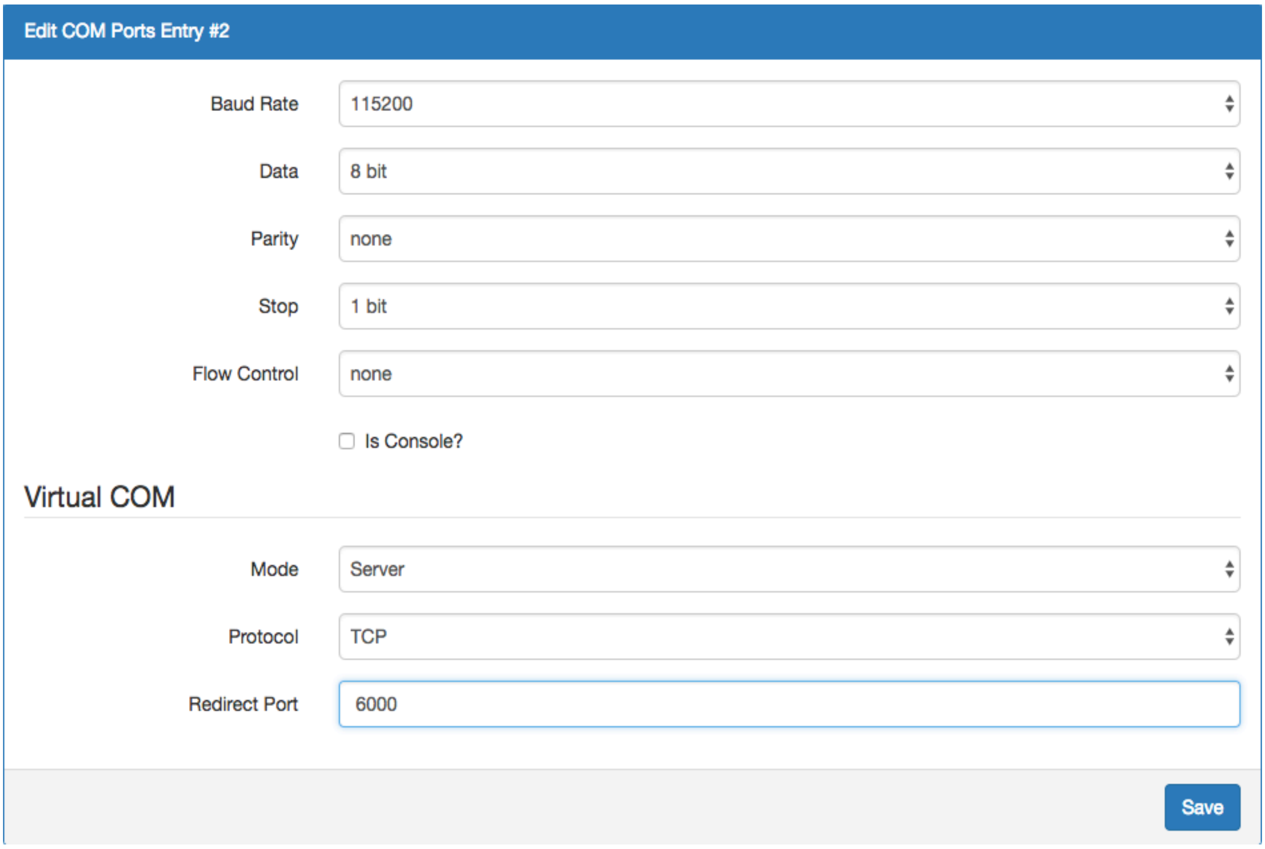
The router provides RS-232 (COM1, COM2) and RS-458 (COM3). You can choose one serial port to connect the device. For example, if you use COM2 to connect the serial device, you need to adjust the setting like baud rate, date bits to fit the device. You can use the web UI to set up the serial settings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



COM Ports

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

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.

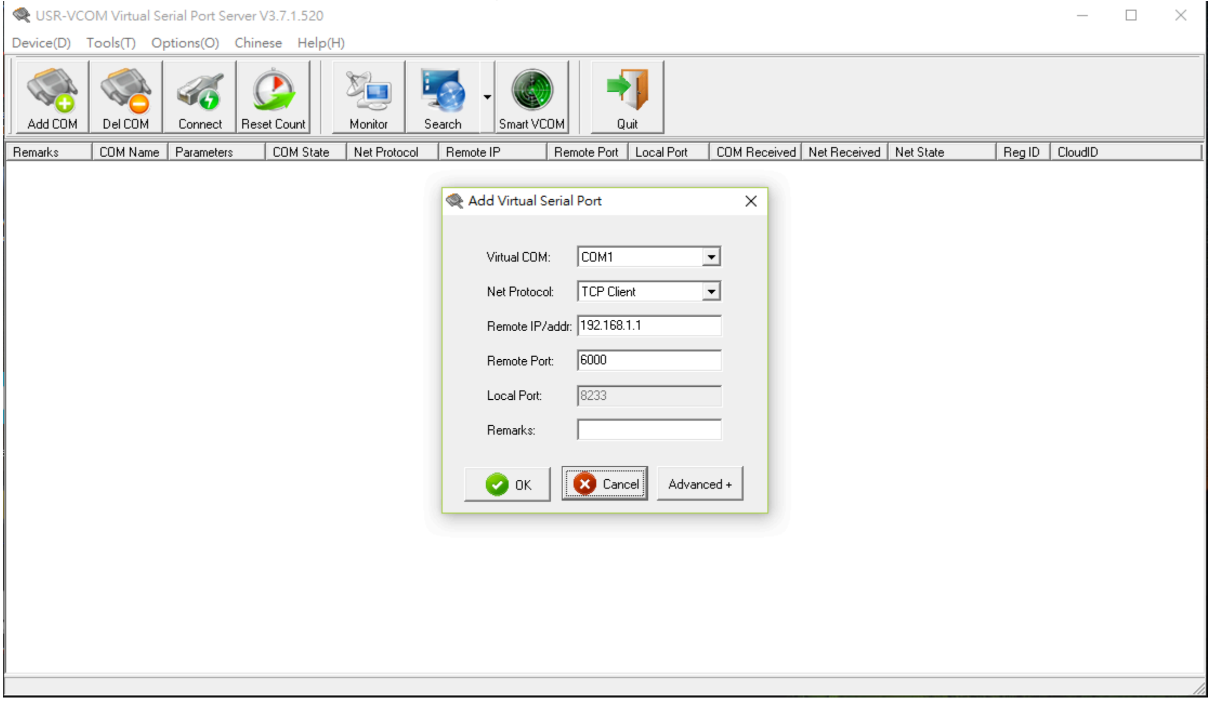
(1) For the serial setting, you need to change the setting like baud rate to fit the connected device.

(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.



Add Virtual Serial Port

Virtual COM: COM1

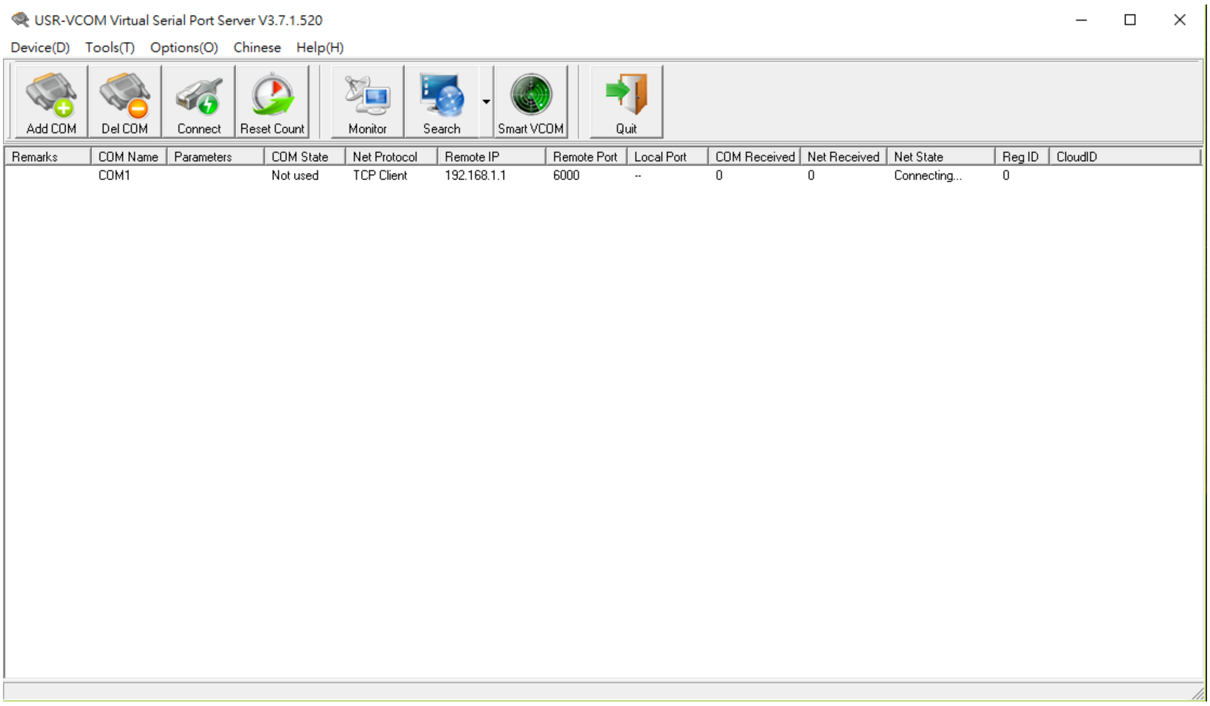
Net Protocol: TCP Client

Remote IP/addr: 192.168.1.1

Remote Port: 6000

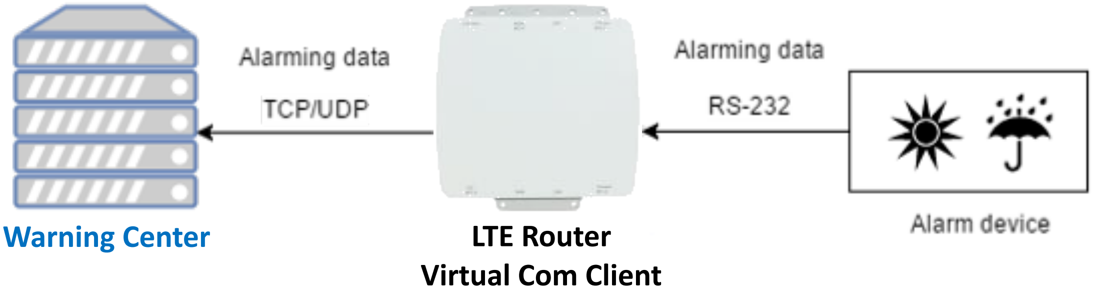
Local Port: 8233

Remarks:

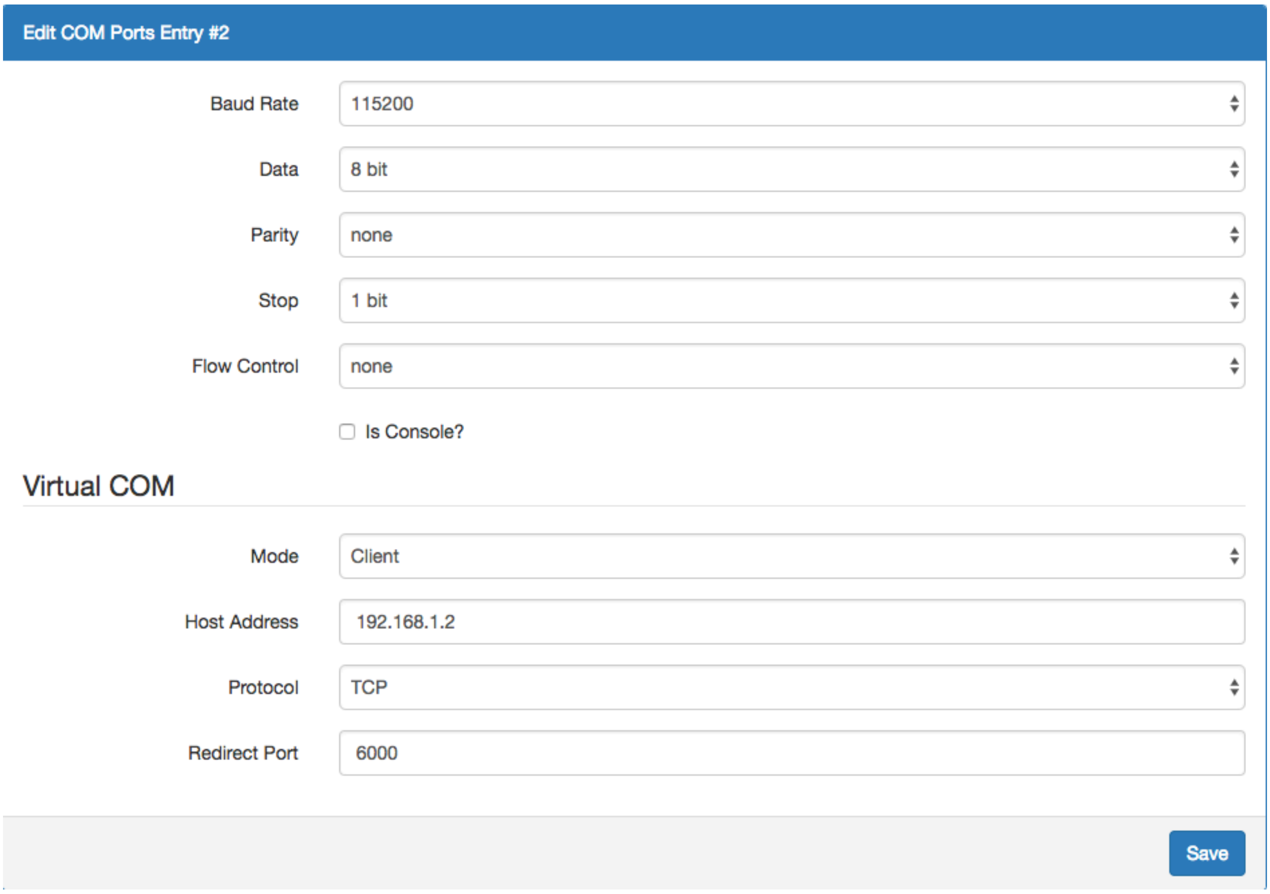

USR-VCOM Virtual Serial Port Server V3.7.1.520
Device(D) Tools(T) Options(O) Chinese Help(H)
Add COM
Del COM
Connect
Reset Count
Monitor
Search
Smart VCOM
Quit

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	

12.5 Virtual COM > Remote Alarm



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



Edit COM Ports Entry #2

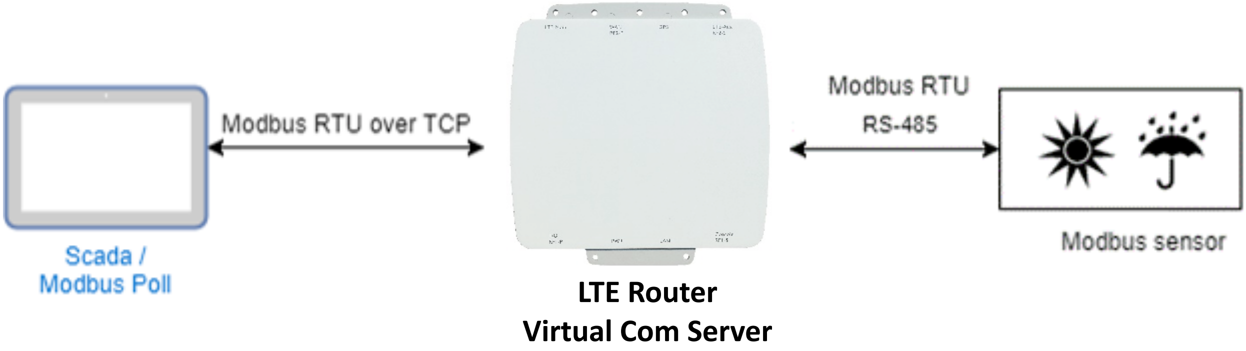
Baud Rate	115200
Data	8 bit
Parity	none
Stop	1 bit
Flow Control	none
	□ Is Console?

Virtual COM

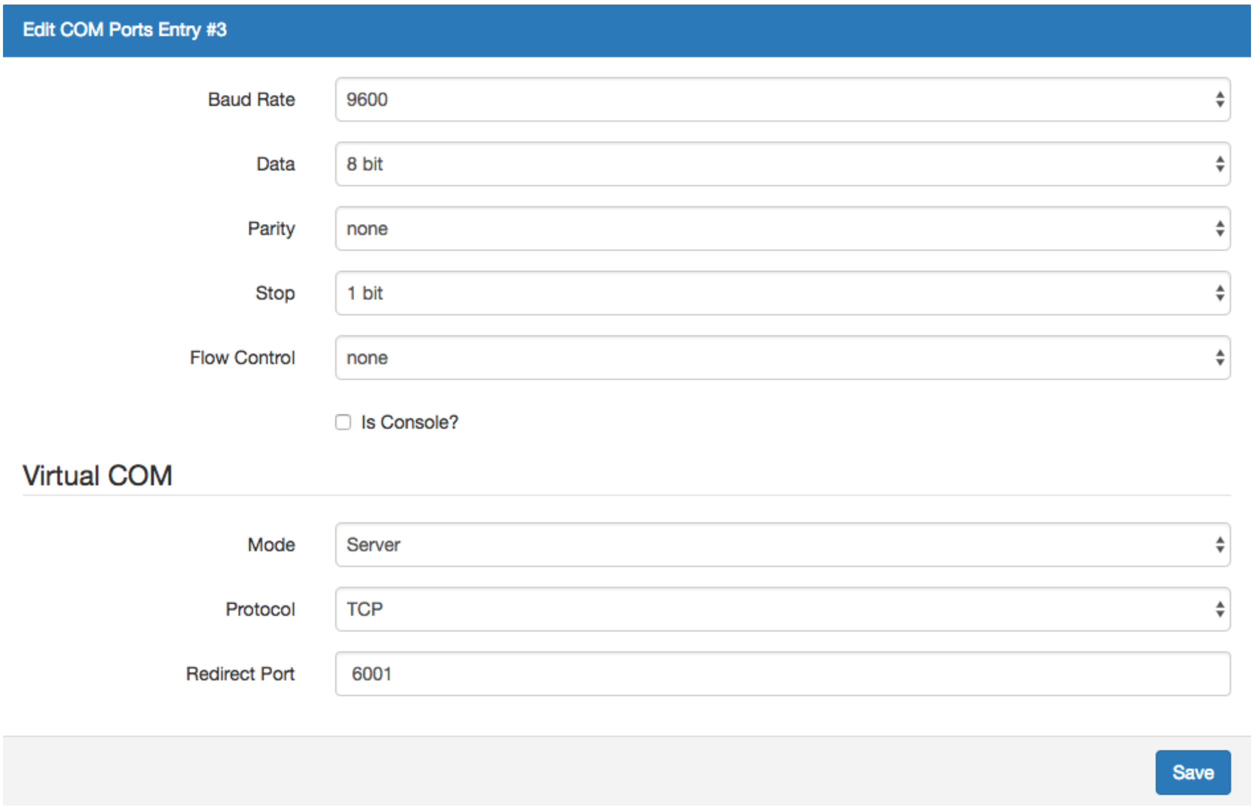
Mode	Client
Host Address	192.168.1.2
Protocol	TCP
Redirect Port	6000

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

12.6 Virtual COM > Modbus RTU over TCP



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



Edit COM Ports Entry #3

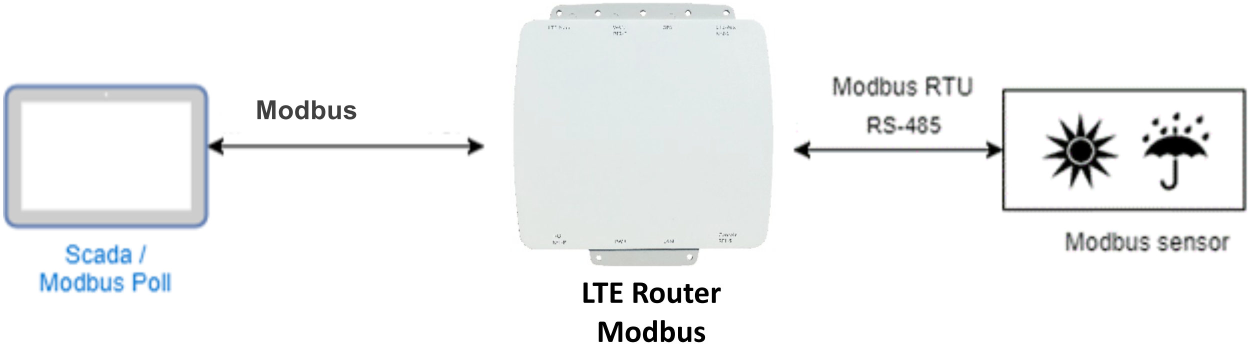
Baud Rate	9600
Data	8 bit
Parity	none
Stop	1 bit
Flow Control	none
	□ Is Console?

Virtual COM

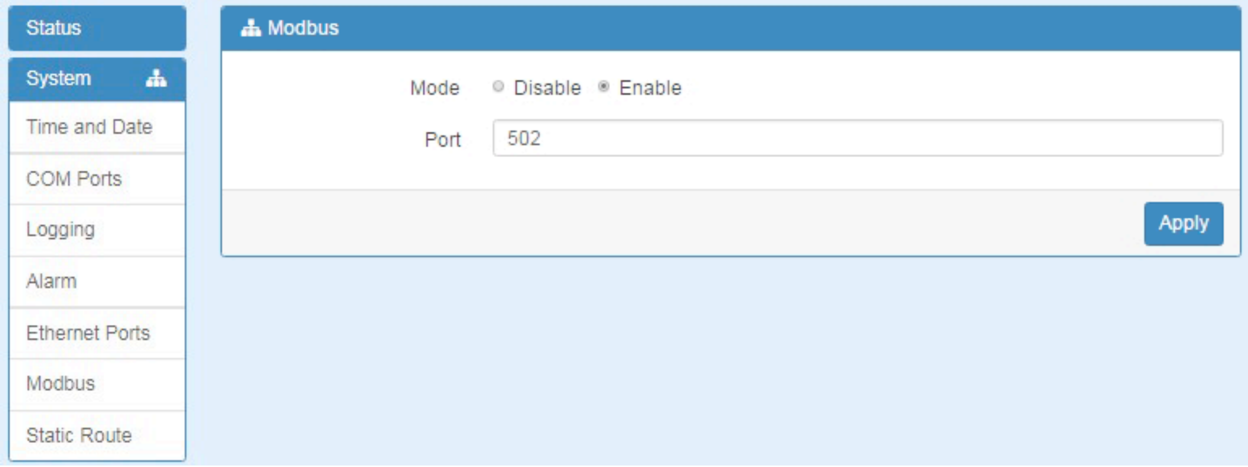
Mode	Server
Protocol	TCP
Redirect Port	6001

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

12.7 Modbus Gateway



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



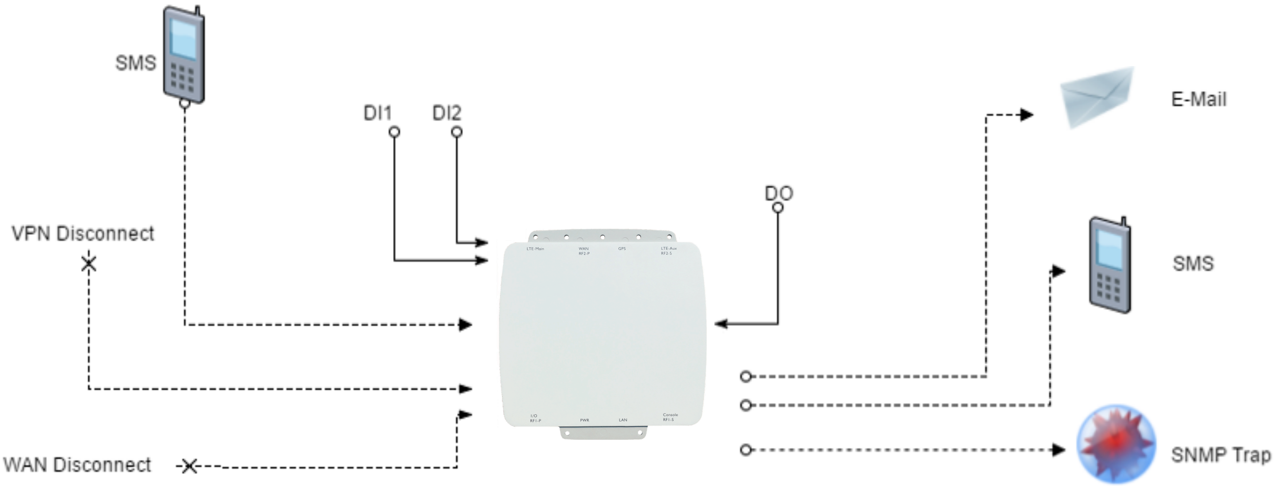
Mode ○ Disable ● Enable

Port 502

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

12.8 Alarm Configuration

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

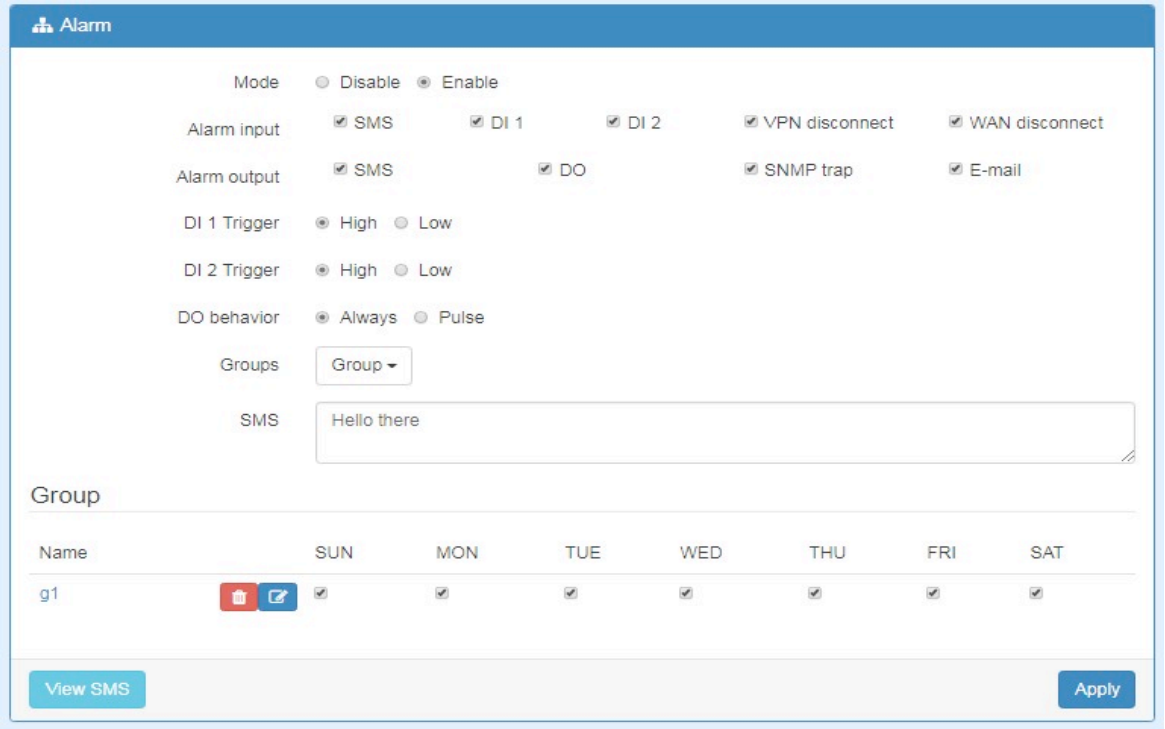


(1) Alarm Input:

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

(2) Alarm Output:

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



Alarm

Mode ○ Disable ● Enable

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

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

DI 1 Trigger ● High ○ Low

DI 2 Trigger ● High ○ Low

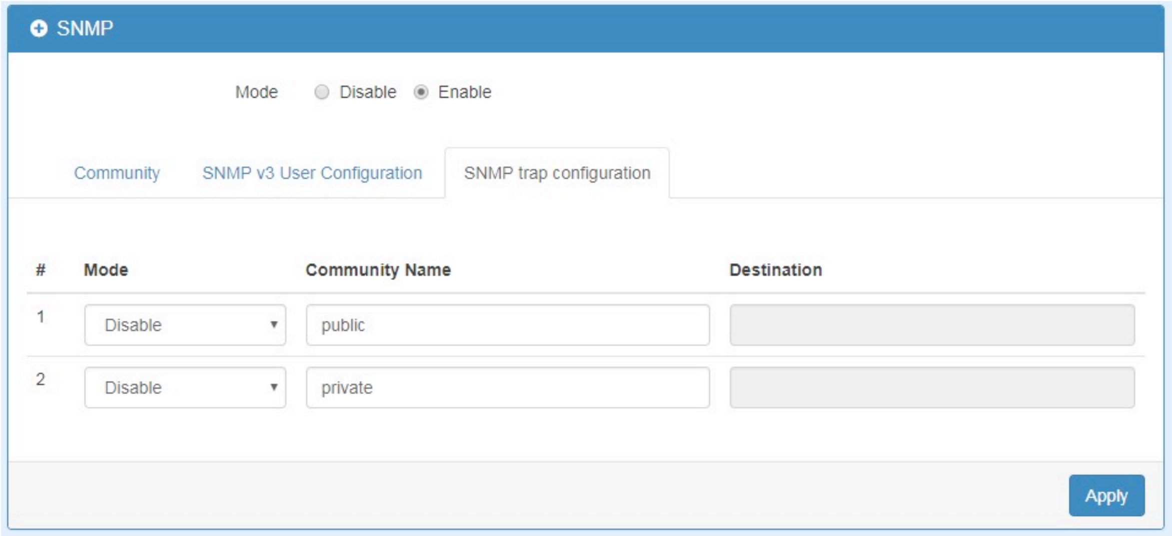
DO behavior ● Always ○ Pulse

Groups: Group ▾

SMS: Hello there

Group

Name	SUN	MON	TUE	WED	THU	FRI	SAT
g1	☑	☑	☑	☑	☑	☑	☑



SNMP

Mode ○ Disable ● Enable

#	Mode	Community Name	Destination
1	Disable	public	
2	Disable	private	

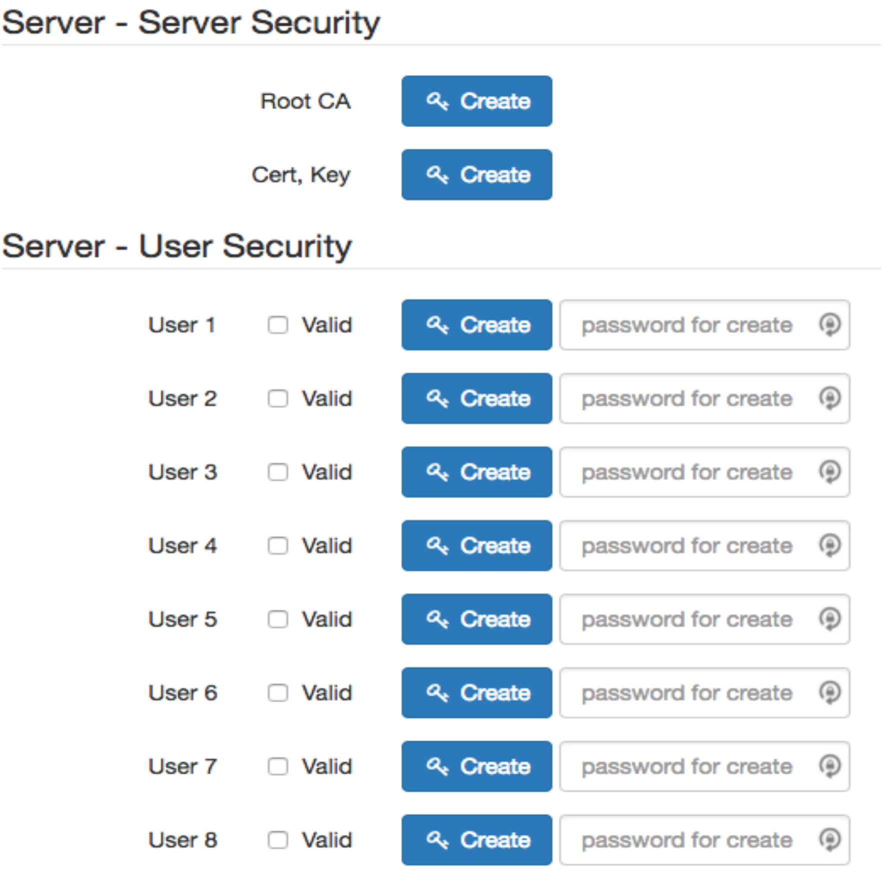
12.9 OpenVPN Configuration

Generic setup

For OpenVPN configuration, use the certificate to authenticate the VPN connection.
Thus, you need to generate the required files for OpenVPN server or import the required file to OpenVPN client.

12.9.1 OpenVPN Server Mode

OpenVPN server certificate generation



Server - Server Security

Root CA	Create
Cert, Key	Create

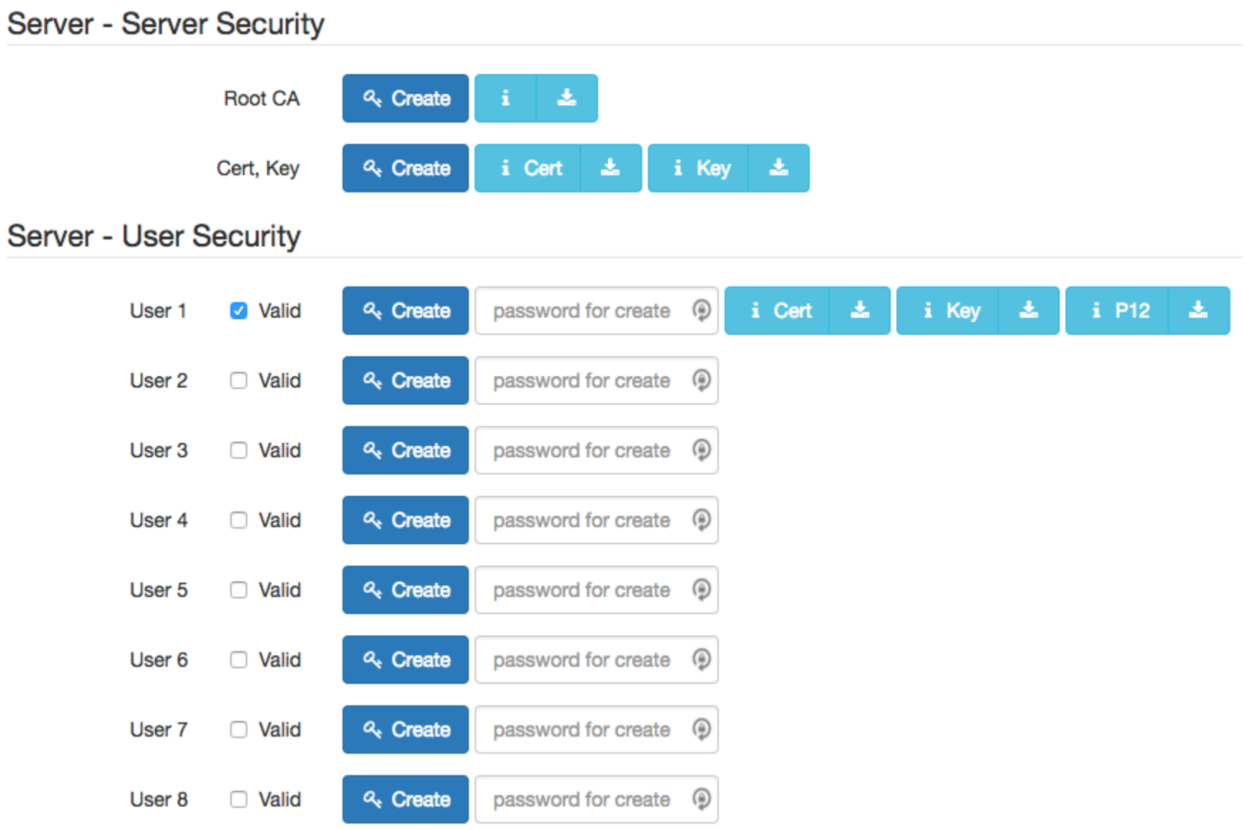
Server - User Security

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

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

To generate the OpenVPN client files, you need to type the password to create it.
The password will be used in the OpenVPN client when the client use **PKCS#12** to authenticate the VPN connection. After the generation, the web UI shows the below picture.

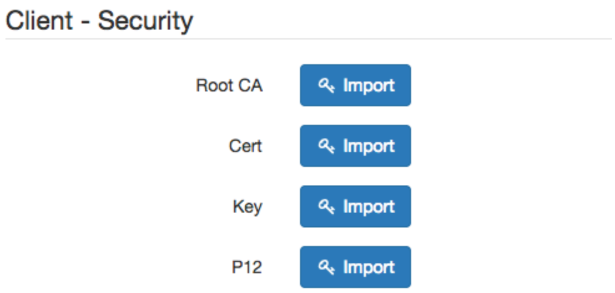


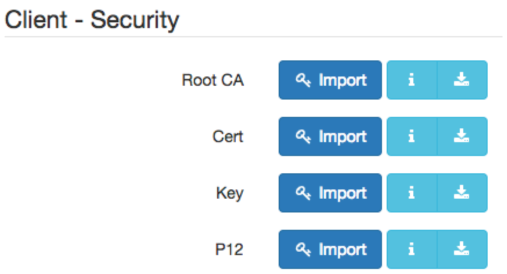
And you can click the info button to show the detail for each files, or click the download button to download the file to PC.

12.9.2 OpenVPN Client Mode

OpenVPN client certificate import

For the OpenVPN client mode, the OpenVPN web UI provides the buttons to import the required files.The OpenVPN client can use the **Root CA**, **User Key** and **User Cert** files from OpenVPN server to authenticate the VPN tunnel. Or just only use the **PKCS#12 (P12)** file from OpenVPN server to authenticate it.
Note: The PKCS#12 files will contain the Root CA, User Key and User Cert.
When the files are imported, the web UI is as shown in the right-bottom picture.

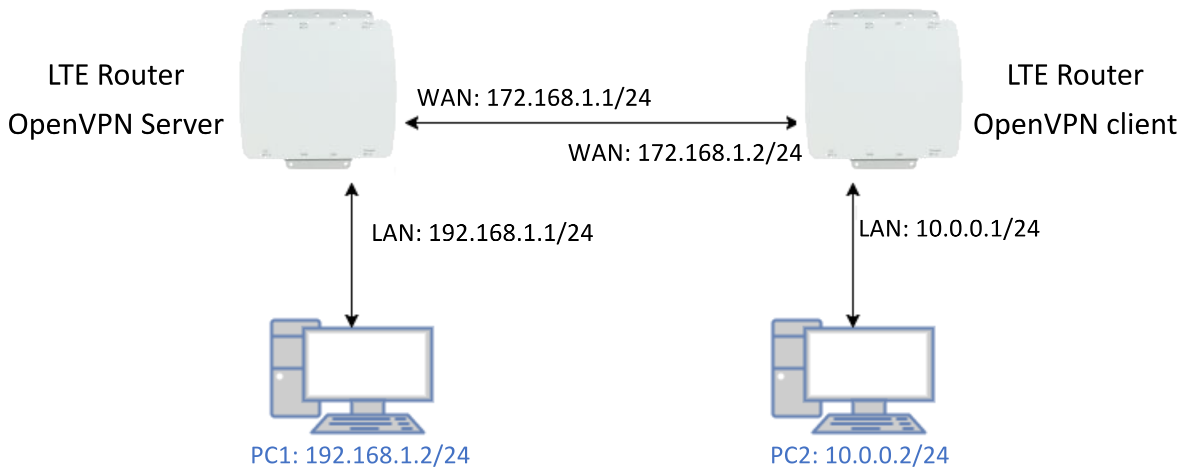




Same as OpenVPN server part, you can use the info/download buttons to get the information of file or download the file to PC.

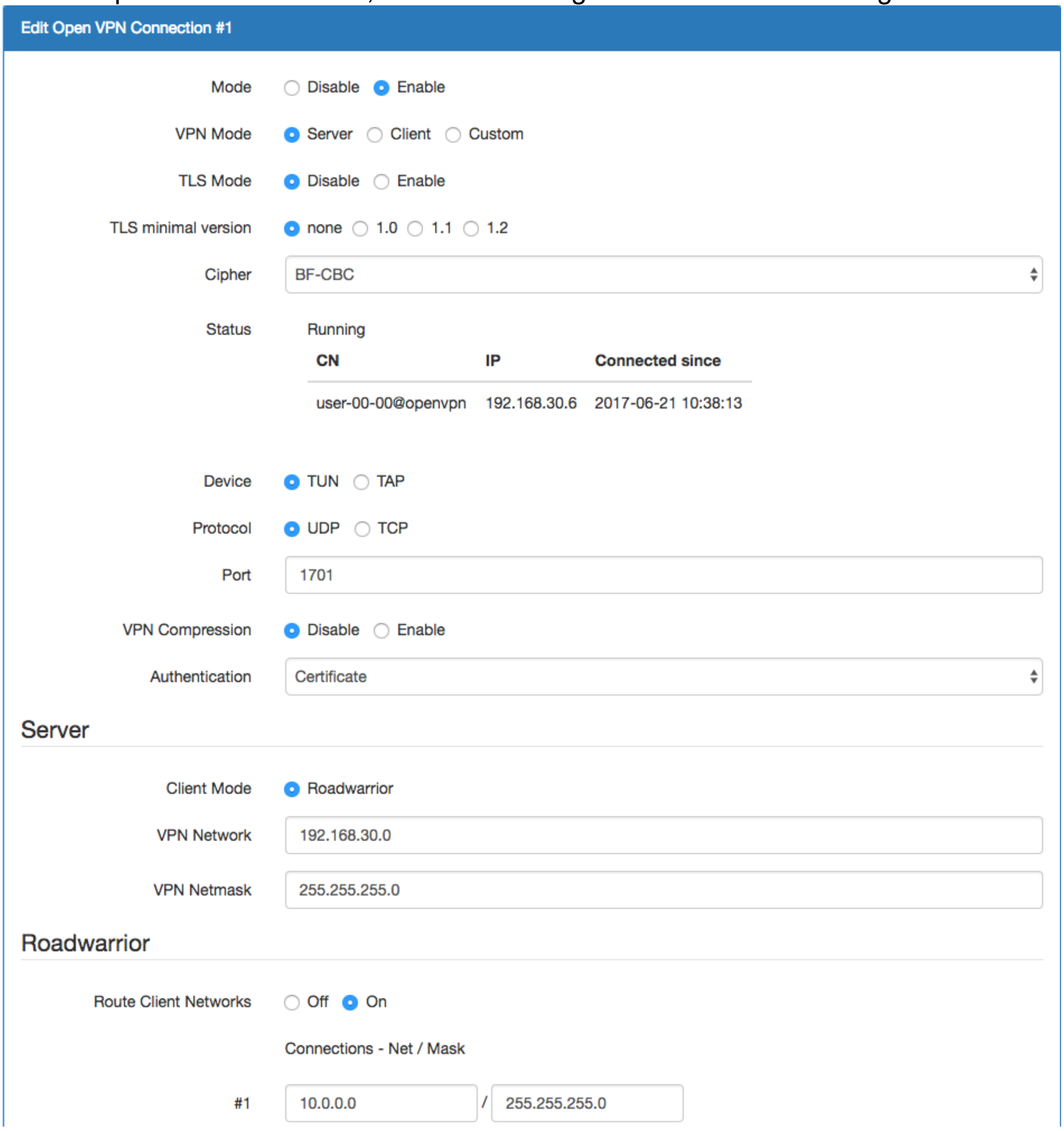
12.9.3 OpenVPN Net-to-Net

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



(1) OpenVPN server configuration

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



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

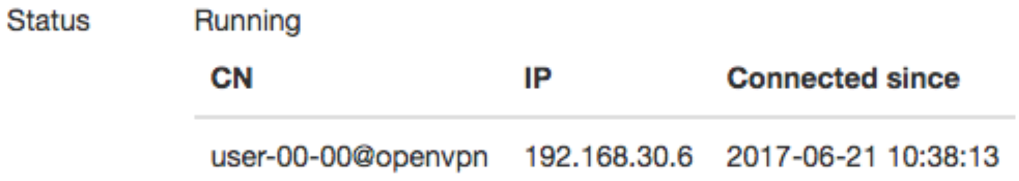
Client Mode	● Roadwarrior
VPN Network	192.168.30.0
VPN Netmask	255.255.255.0

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 OpenVPN client side, in this case the **#1** route will be **10.0.0.0** and **255.255.255.0**

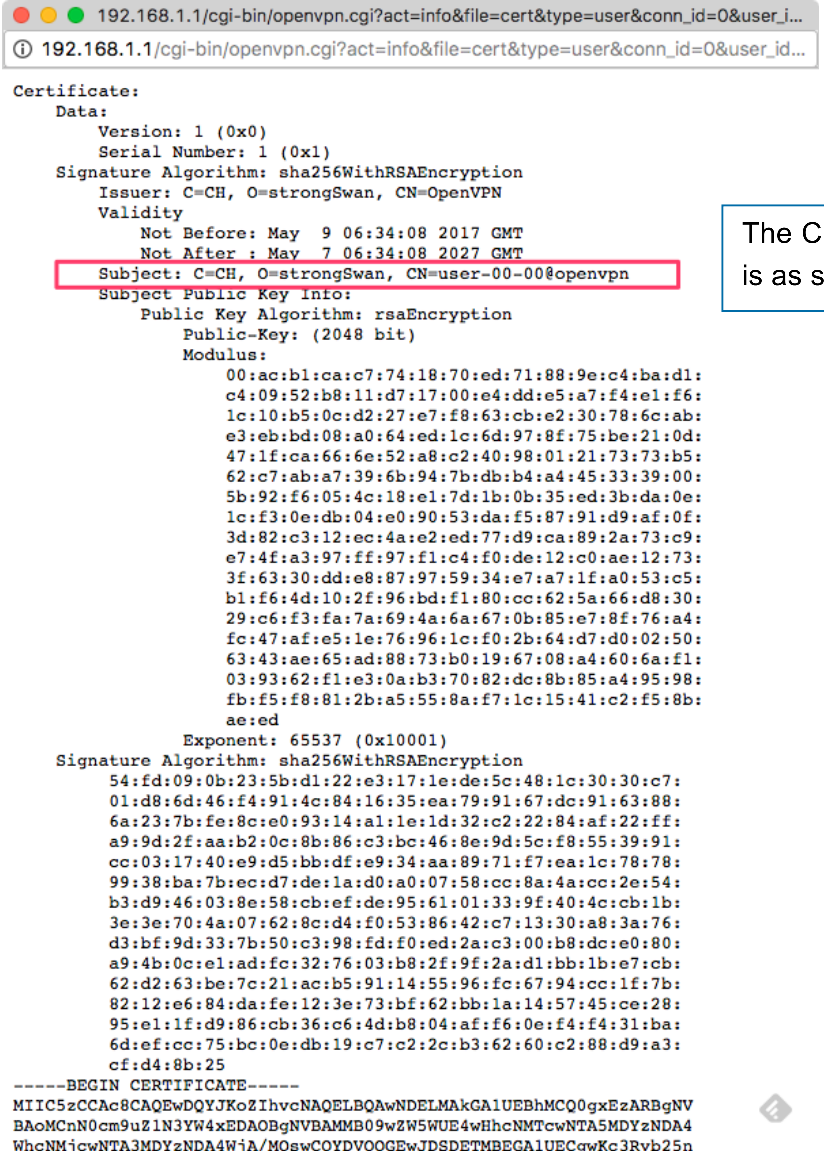
Note: The **#1** route means the routing information for **User 1**.
If all settings set up properly, the web UI will show the **Apply OK** and the OpenVPN server status should be **Running**. When OpenVPN Client mode is connected, the status will show the information which client is connected, IP address and connected time.



Status Running

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

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



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

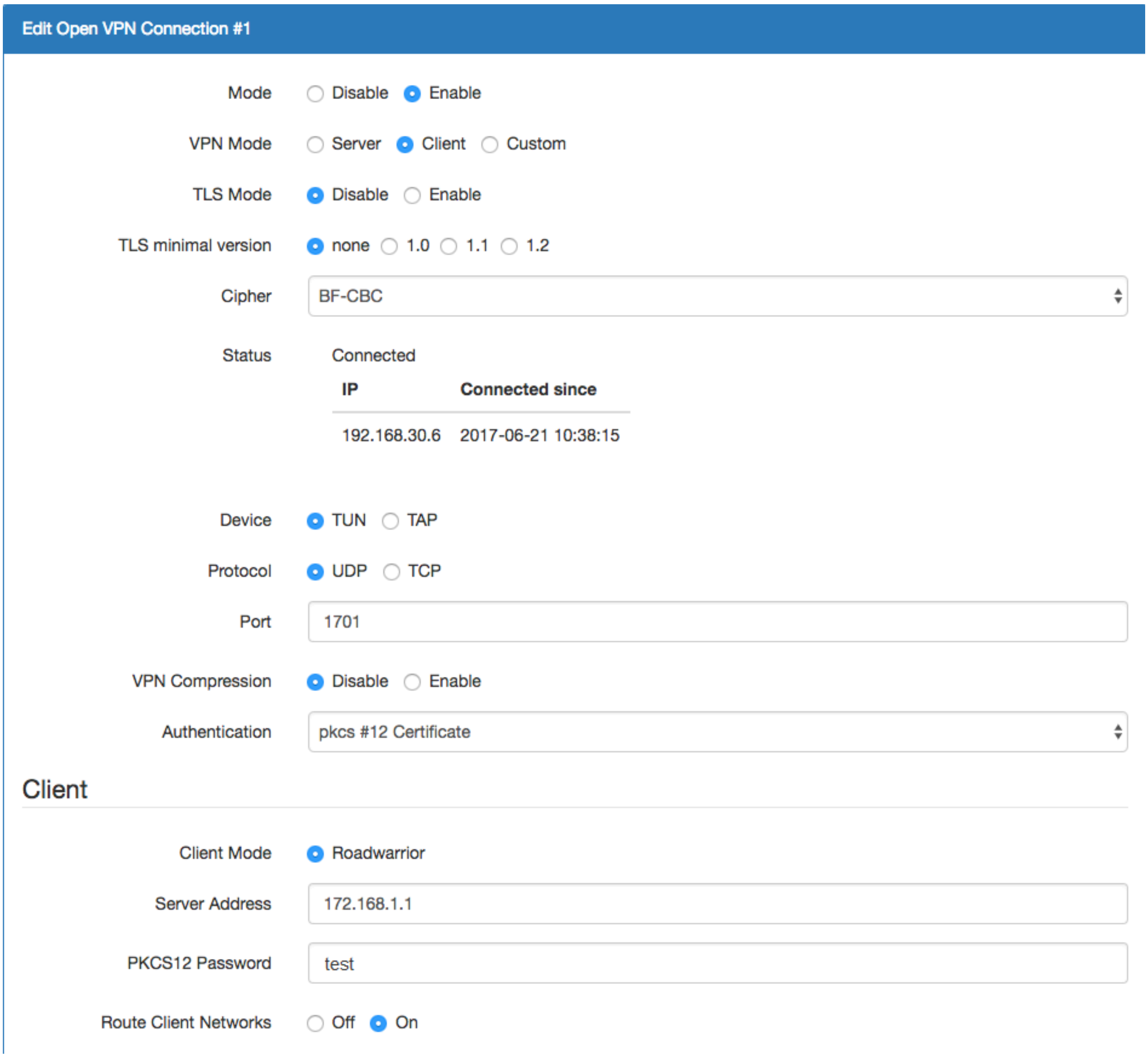
192.168.1.1/cgi-bin/openvpn.cgi?act=info&file=cert&type=user&conn_id=0&user_id...

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

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

(2) OpenVPN client configuration

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



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 test

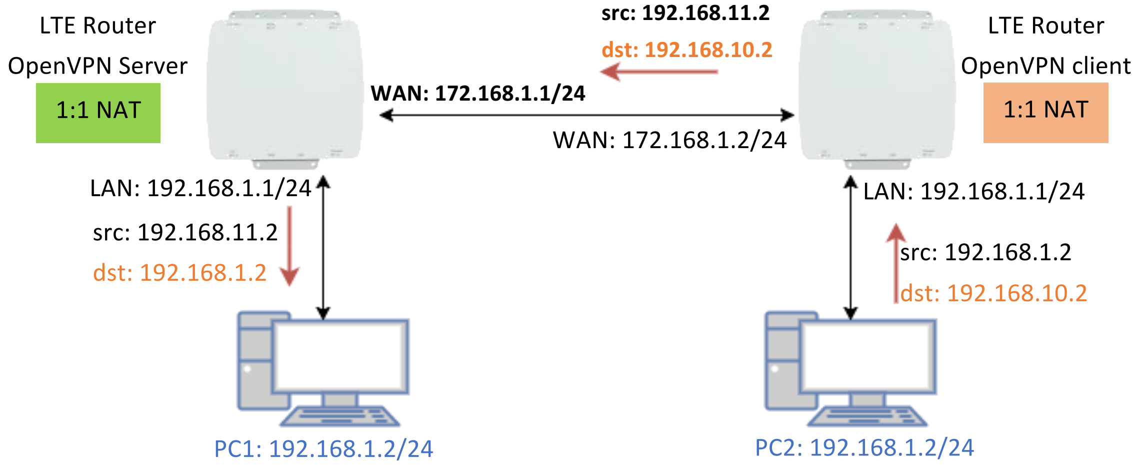
Route Client Networks ○ Off ● On

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

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

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

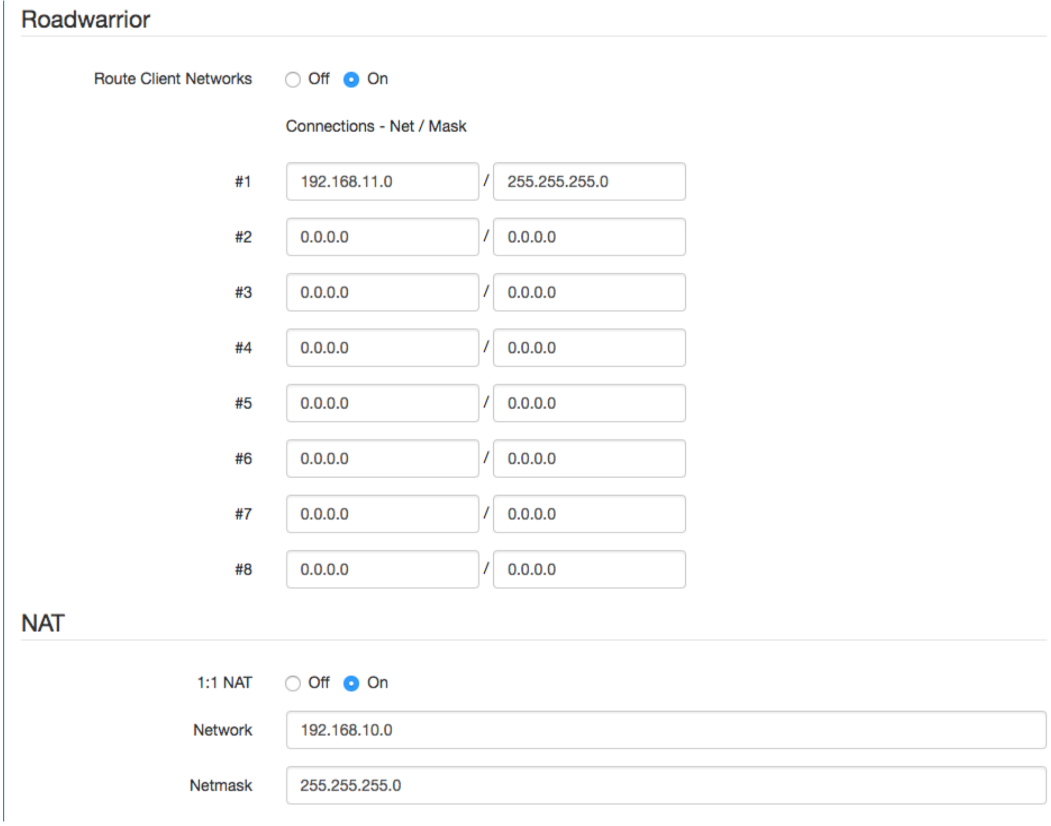
12.9.4 OpenVPN 1:1 NAT



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

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

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



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

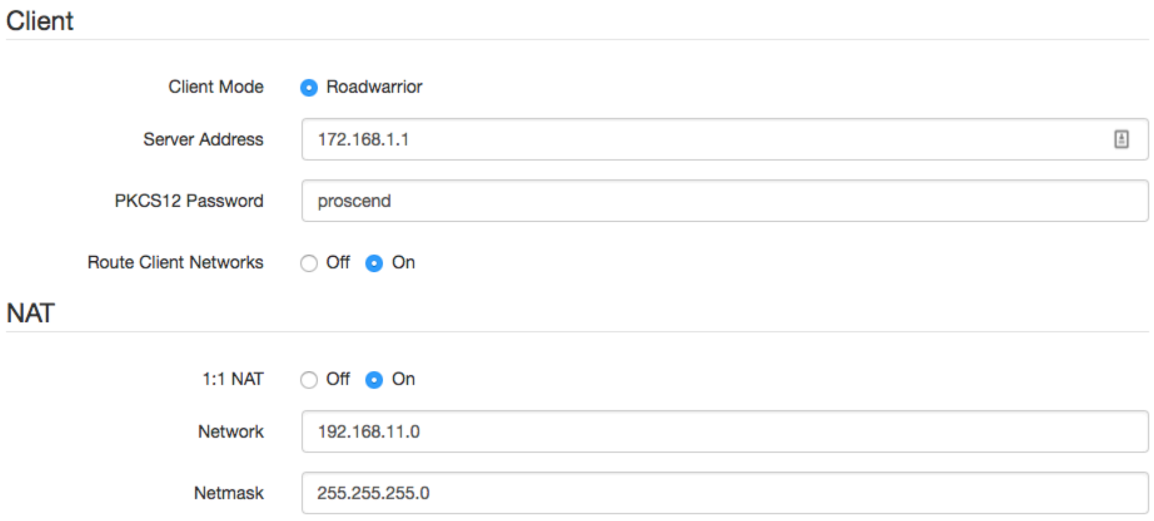
NAT

1:1 NAT ○ Off ● On

Network: 192.168.10.0

Netmask: 255.255.255.0

For the OpenVPN client side, same as server side but we fill up the Network as **192.168.11.0**. The setting will make router convert the OpenVPN client side LAN network from **192.168.1.0/24** to **192.168.11.0/24** when the VPN traffic is coming.



Client

Client Mode ● Roadwarrior

Server Address 172.168.1.1

PKCS12 Password proscend

Route Client Networks ○ Off ● On

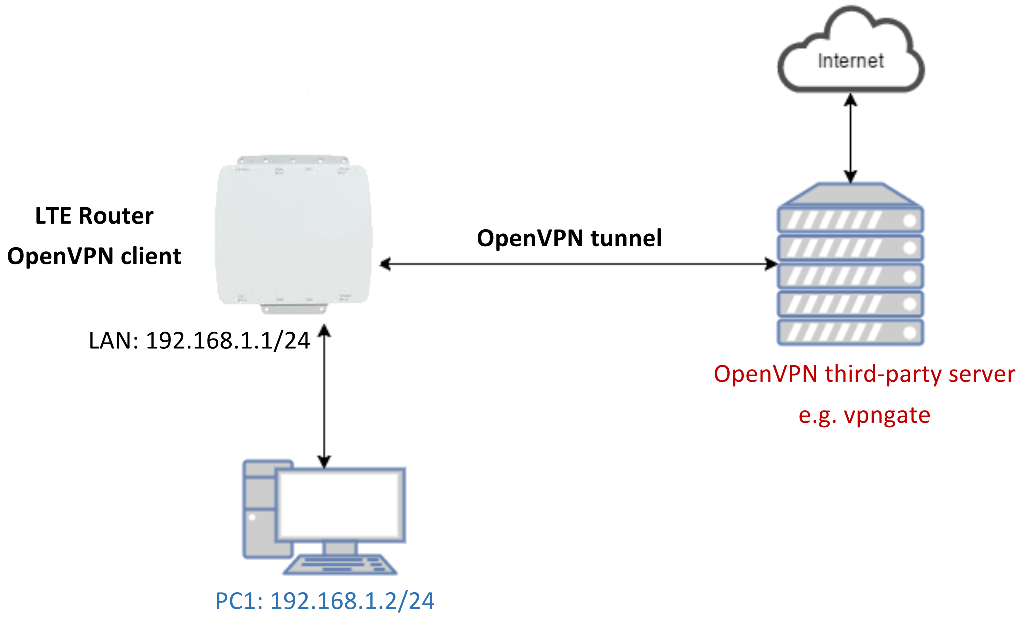
NAT

1:1 NAT ○ Off ● On

Network 192.168.11.0

Netmask 255.255.255.0

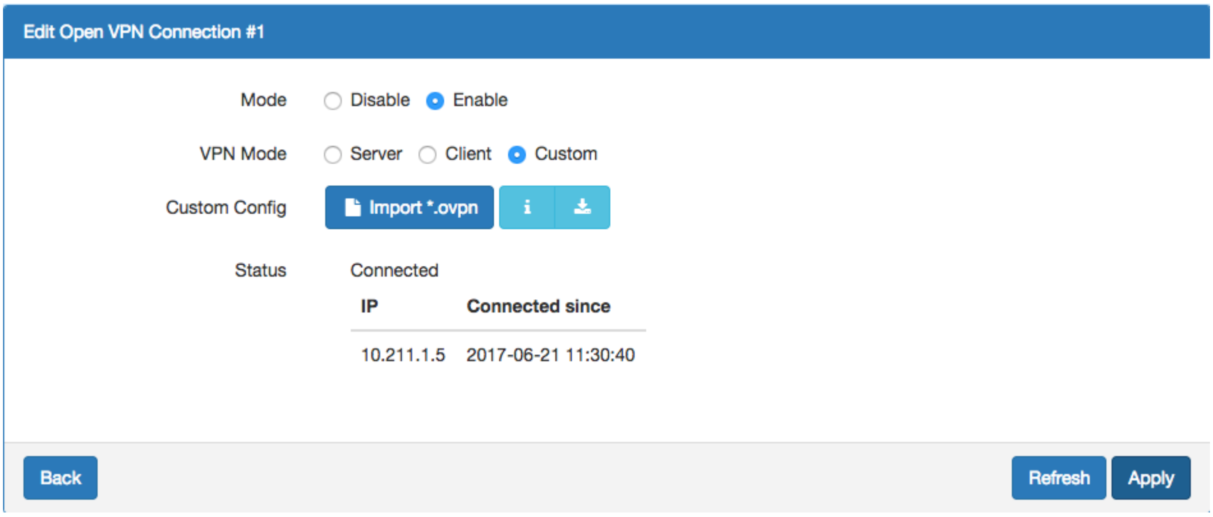
12.9.5 OpenVPN with third-party server



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

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

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



Edit Open VPN Connection #1

Mode ○ Disable ● Enable

VPN Mode ○ Server ○ Client ● Custom

Custom Config

Status Connected

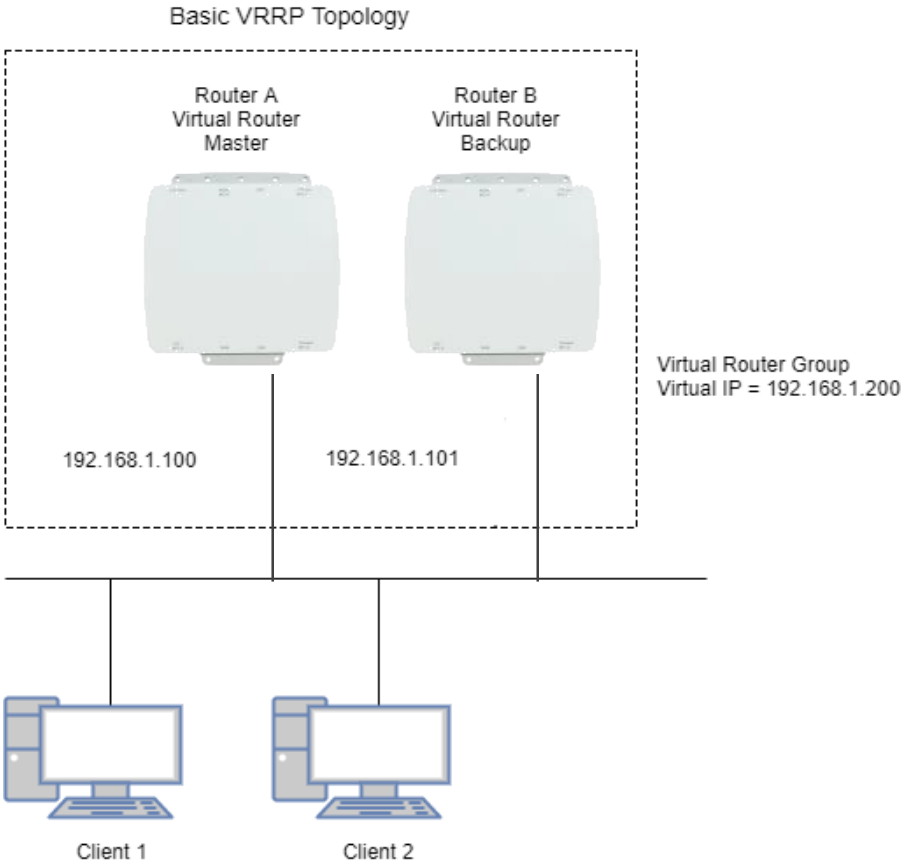
IP	Connected since
10.211.1.5	2017-06-21 11:30:40

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

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

12.10 VRRP Topology

Basic VRRP Topology



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