

Industrial 4G LTE Cellular Router

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

User Manual

Version 1.1.8

PROSCEND[®]
Proscend Communications Inc.

Table of Contents

1	Introduction.....	6
1.1	Features.....	6
1.2	Specifications.....	7
1.3	Mechanical Dimensions.....	8
1.4	Ordering Information.....	10
2	Hardware Installation.....	10
2.1	LED Indicators.....	10
2.2	Ethernet Port.....	11
2.3	Serial Port COM1 (Console-RS232).....	12
2.4	Install the SIM Card.....	13
2.5	Reset Button.....	14
2.6	External Antenna.....	14
2.7	Connecting the Power Supply.....	14
2.8	Grounding the Router.....	15
2.9	Pin Assignments.....	15
2.10	Connecting I/O Ports.....	16
2.11	Serial Port COM2 (RS-232).....	17
2.12	Serial Port COM3 (RS-485).....	17
2.13	DIP Switch.....	18
3	Configuration via Web Browser.....	19
3.1	Access the Web Configurator.....	19
3.2	Navigate the Web Configurator.....	20
4	Status.....	21
4.1	Status > GPS.....	25
5	Configuration > System.....	25
5.1	System > Time and Date.....	26
5.2	System > COM Ports.....	29
5.3	System > Logging.....	31
5.3.1	Logging > Logging.....	31
5.3.2	Logging > Log.....	32
5.4	System > Alarm.....	33
5.4.1	Alarm > Contacts > Create and name the Group.....	34
5.4.2	Alarm > Contacts > Add User.....	36
5.4.3	Alarm > Duty Schedule.....	37
5.5	System > Ethernet.....	37
5.6	System > Modbus.....	39
5.7	System > Client List.....	39
5.8	System > LED.....	40

F	Configuration > WAN	41
F 1	WAN > Priority	41
F 2	WAN > Ethernet	42
6.2.1	WAN Ethernet Configuration	42
6.2.2	Ethernet Ping Health	45
F 3	WAN > IPv6 DNS	47
7	Configuration > LTE	48
7 1	LTE > LTE Config	48
7.1.1	LTE Configuration	48
7.1.2	LTE Ping Health	49
7 2	LTE > GPS	50
7 3	LTE > Dual SIM	52
7 4	LTE > Usage Display	57
7 5	LTE > SMS	62
7 6	LTE > Serving Cell	64
7 7	LTE > Lock PCIs	65
7.7.1	Neighbors	65
7.7.2	Locked PCIs	65
7.7.3	Saved Locked PCIs	65
7 8	LTE > Lock Bands	66
7 9	LTE > DNS	66
8	Configuration > WiFi (M301-GW)	67
8 1	WiFi > WiFi Config	67
8 2	WiFi > Client List	68
9	Configuration > LAN	69
9 1	LAN > IPv4	69
9 2	LAN > IPv6	70
9 3	LAN > VLAN	70
9 4	LAN > Subnet	74
10	IP Routing	75
10 1	IP Routing > Static Route	75
10 2	IP Routing > RIP	77
10 3	IP Routing > OSPF	79
10 4	IP Routing > BGP	82
11	Configuration > VPN	85
11 1	VPN > Open VPN	85
11.1.1	Open VPN Common Setting	85
11.1.2	Open VPN Client Setting	88
11.1.3	Open VPN Server Setting	89
11.1.4	Set up Open VPN Custom	90
11 2	VPN > IPsec	92

11.2.1	IPsec > Connections	92
11.2.2	IPsec > Authentication IDs	95
11.2.3	IPsec > X.509 Certificates	97
11.2.4	IPsec > CA Certificates	97
11.2.5	IPsec > Net-to-Net Configuration	100
11.2.6	IPsec > Hub-Spoke Topology	115
11 7	VPN > GRE	126
11 4	VPN > PPTP Server	127
11 5	VPN > L2TP	129
12	Configuration > Firewall	132
12 1	Firewall > Port Forwarding	132
12 5	Firewall > DMZ	133
12 7	Firewall > IP Filter	134
12 4	Firewall > MAC Filter	138
12 5	Firewall > URL Filter	139
12 5	Firewall > NAT	140
12 7	Firewall > IPS	141
13	Configuration > Service	142
13 1	Service > SNMP	142
13.1.1	Community	142
13.1.2	SNMP v3 User configuration	143
13.1.3	SNMP trap configuration	144
13 5	Service > TR069	145
13 7	Service > Dynamic DNS	146
13 4	Service > VRRP	148
13 5	Service > MQTT	149
13 5	Service > UPnP	151
13 7	Service > SMTP	151
13 5	Service > IP Alias	152
13 5	Service > QoS (Quality of Service)	153
13.9.1	ISP Bandwidth	153
13.9.2	QoS	154
13.9.3	Status	157
13.9.4	The case of Internet Web site access	157
13.9.5	Bandwidth divided for each IP address	161
14	Configuration > Management	162
14 1	Management > Identification	162
14 5	Management > Administration	163
14 7	Management > Contacts / On Duty	165
14.3.1	Contacts	165
14.3.2	Duty Schedule	165
14 4	Management > SSH	166
14 5	Management > Web	167

14 F	Management > Firmware	168
14 7	Management > Configuration	168
14 F	Management > Load Factory	168
14 F	Management > Restart.....	168
14 1C	Management > Schedule Reboot	169
15	Configuration > Diagnosis.....	170
15 7	Diagnosis > Ping	170
15 7	Diagnosis > Traceroute	171
1F	Configuration Applications	172
15 7	WAN Priority.....	172
15 7	LAN > IPv4/IPv6 Dual Stack.....	174
15 7	MQTT Broker	176
15 4	Virtual COM > Remote Management.....	177
15 F	Virtual COM > Remote Alarm	180
15 F	Virtual COM > Modbus RTU over TCP	181
15 7	Modbus Gateway	182
15 F	Alarm Configuration.....	182
15 F	Open VPN Configuration.....	184
16.9.1	Open VPN Server Mode	184
16.9.2	Open VPN Client Mode	185
16.9.3	Open VPN Net-to-Net.....	186
16.9.4	Open VPN 1:1 NAT.....	189
16.9.5	Open VPN with third-party server	190
16.9.6	Install Open VPN Access Server on Docker	192
16.9.7	Install Pritunl Open VPN server on Docker	197
15 1C	VRRP Topology	205
15 17	TR069 Server (GenieACS Installation).....	205
17	Test Case Example.....	215
17 7	VLAN Topology	215
17 7	MQTT Topology.....	218
17 7	Modbus Topology	224
17 4	IP Routing Topology	227
1F	Safety Notice	231
15	Wi-Fi Specifications	232

1 Introduction

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

1.1 Features

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

1.2 Specifications

Cellular Interface

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

Wi-Fi Interface (M301-GW)

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

Processor & I/O Interface

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

Physical Characteristics

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

LED Display

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

Power Supply

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

MTBF (Mean Time Between Failures)

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

Software

● Network Protocols:

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

● Routing/Firewall:

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

● VPN:

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

● Wireless Connectivity:

Two SIM for failover/ roaming over/ back up

Two SIM data usage control

Seamless multi WAN connections switch

● Others:

DDNS, QoS, Virtual COM, UPnP

● Alarm:

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

Management Software

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

Environment

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

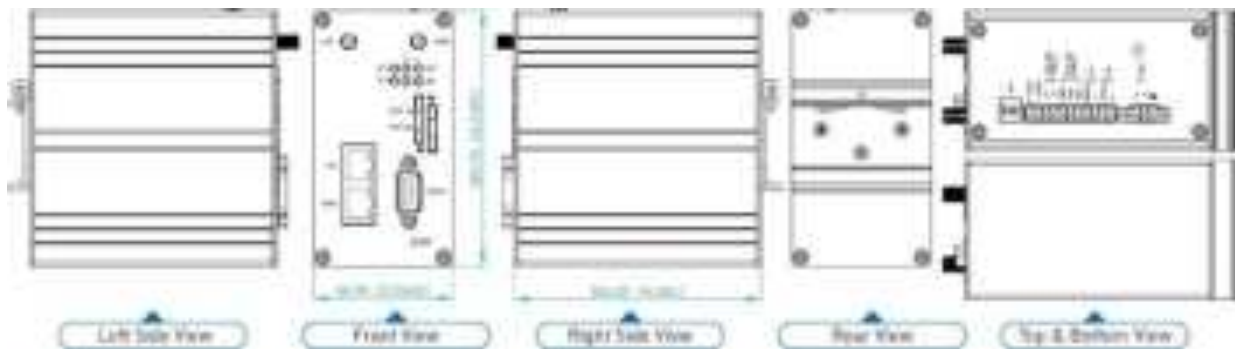
Standards and Certifications

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

1.3 Mechanical Dimensions

(1) M300 model:

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



(2) M301 model:

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



(3) M300-G model:

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



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

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



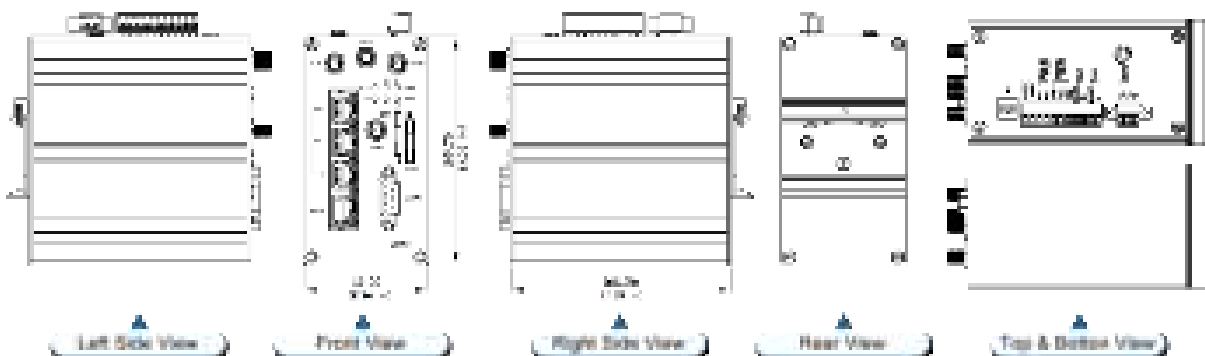
(5) M301-TPG model:

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



(6) M301-GW model:

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



1.4 Ordering Information

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

2 Hardware Installation

This chapter introduces how to install and connect the hardware.

2.1 LED Indicators

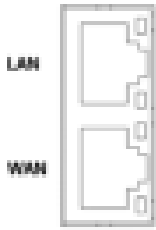


(M301-GW)

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

2.2 Ethernet Port

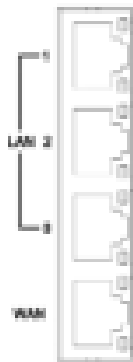
(1) 10/100 Mbps Ethernet LAN/WAN (M300/M300-G model)



The LAN and WAN interface are standard RJ45 connectors.

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

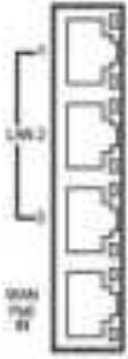
(2) 10/100 Mbps Ethernet LAN1~LAN3/WAN (M301/M301-G/M301-TG model)



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

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

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



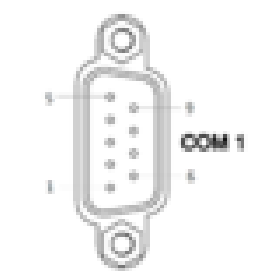
The Ethernet LAN1~3 interfaces are standard RJ45 connectors. The WAN interface is a standard RJ45 connector with IEEE 802.3at/af PoE PD.

(4) LED Indicator of Ethernet Port

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

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

2.3 Serial Port COM1 (Console-RS232)

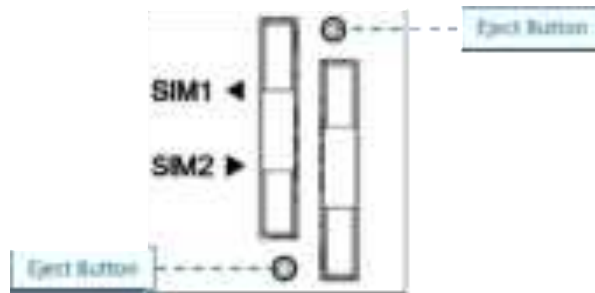


The serial port COM1 is a standard Sub-D connector.

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

2.4 Install the SIM Card

1. SIM1/SIM2 Card Drawers and Eject Buttons



2. Insert and Remove SIM1/SIM2 Card

- (1) Before inserting or removing the SIM card, ensure that the power has been turned off and the power connector has been removed from Cellular Router.
- (2) Press the button with a paper clip or suitable tool to eject the SIM card from the drawer.



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



Note:

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

2.5 Reset Button



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

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

Note:

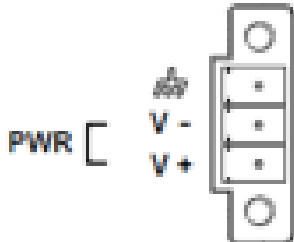
Press the Reset button and count the time around 5 seconds. The LED Indicators will be blinking to show you have activated the setting successfully.

2.6 External Antenna

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

2.7 Connecting the Power Supply

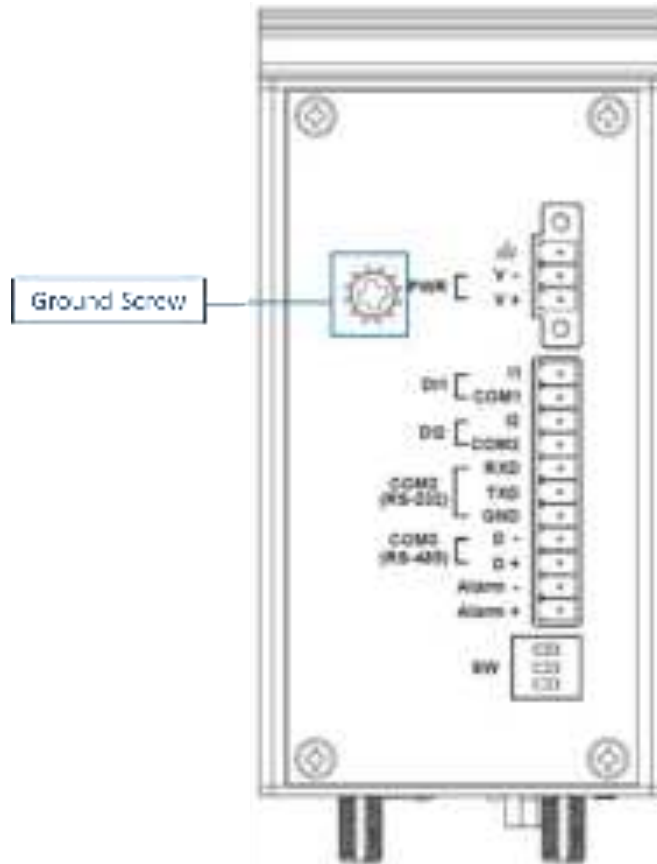
The router requires a DC power supply in the range of 10~32V DC. Please ensure all components are earthed to a common ground before connecting any wiring.



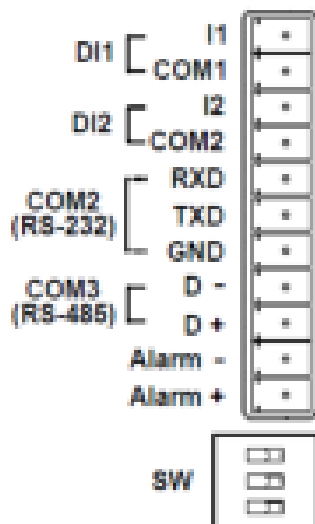
Pin	Power (10~32VDC)
	FRAME GROUND
V -	Negative
V+	Positive

2.8 Grounding the Router

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



2.9 Pin Assignments



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

2.10 Connecting I/O Ports

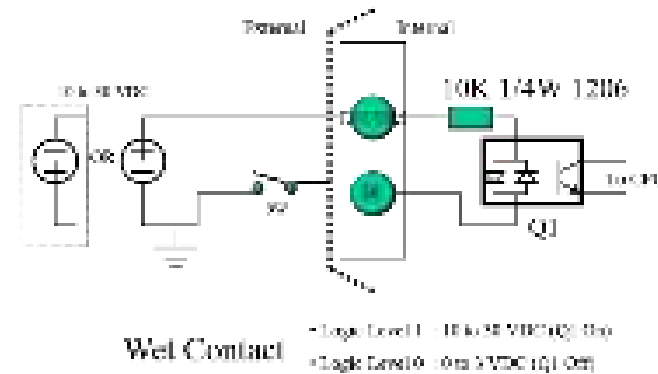
(1) Digital Input DI1 & DI2

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

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

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

Note: Q1 is a bidirectional component.

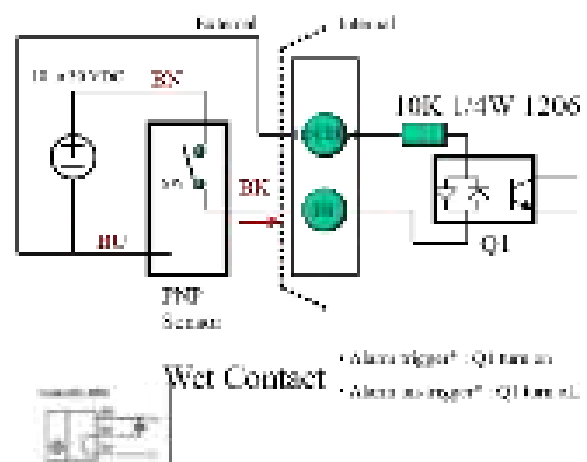
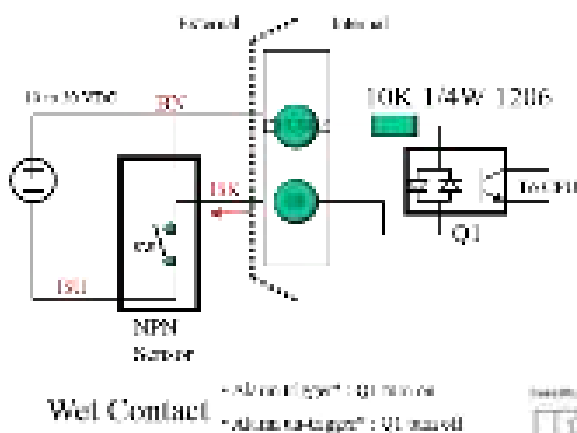


Digital Input

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

* Refer to the Alarm module for wiring connection

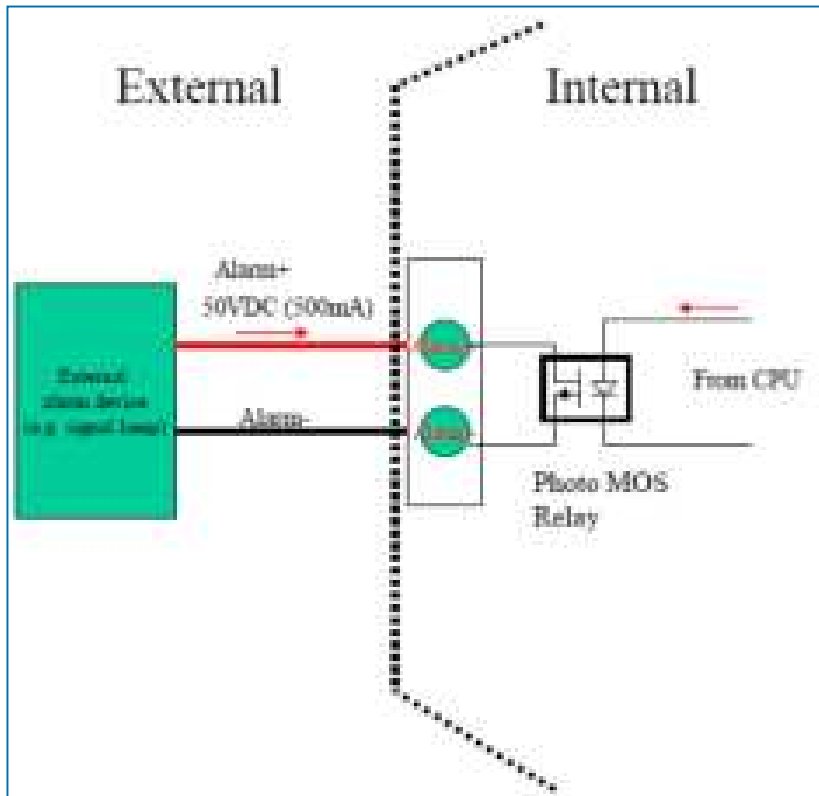
* Q1 is bidirectional



(2) Digital Output – Alarm Contacts

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

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



2.11 Serial Port COM2 (RS-232)

The serial port COM2 is a RS-232 interface.

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

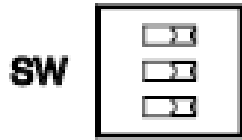
✖ Both connectors (RS-232 and RS-485) have a common ground connection.

2.12 Serial Port COM3 (RS-485)

The serial port COM3 is a RS-485 interface.

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

2.13 DIP Switch



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



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

DIP SWITCH

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

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

3 Configuration via Web Browser

3.1 Access the Web Configurator

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

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

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

Title Bar Panel > Selecting Language

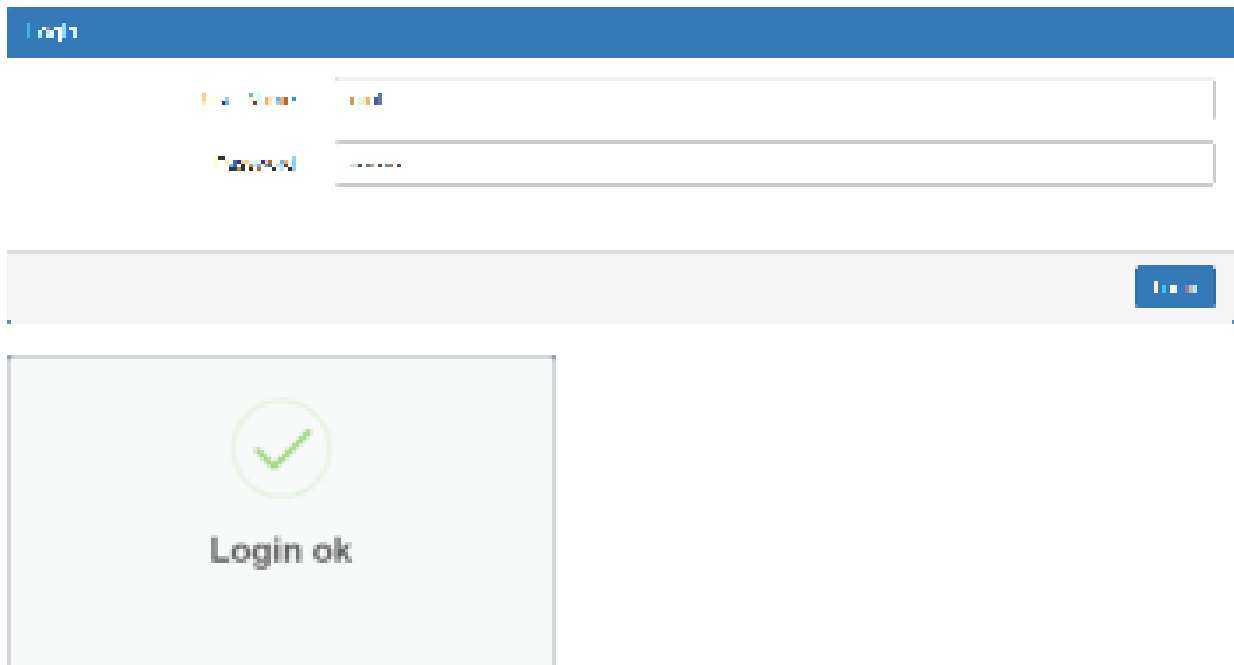
You can choose the languages, including English and Taiwan.



Logging in the Router

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

After clicking, the interface shows **Login ok**.



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

3.2 Navigate the Web Configurator

The main screen is divided into three parts as below.

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



(1) **A** : Title Bar

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



Title Bar	
Item	Description
RSSI	Show if the SIM card is inserted in the slot. If yes, RSSI (Received Signal Strength Indicator) shows the current signal strength in a wireless network and the name of telecommunication operator.
Uptime	Show the time starting turn on the router until current using.
WAN Priority	Show the three mode of WAN status, which is first to use.
SIM Slot	Show the current using of SIM Slot that inserts into SIM1 or SIM2.
Location	Show the position of router from Google Maps. Note: This function is for GPS spec.
Google Maps	Display Google Map according to location.
Language	Choose your language from the drop-down list on the upper right corner of the title bar.
Login/Logout	Click to log in or log out of the web configurator.
?	Online Manual

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

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

(3) **C** : Main Window

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

4 Status

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

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

Status	Super User	Administrator	Read Only	Guest
User name	system account (root/admin)	only Super User can modify	only Super User can modify	N/A
Password	configurable	configurable	configurable	N/A
Permission	<ul style="list-style-type: none">• Add/Delete/Modify all users' accounts except Super User.• Read/Write Configuration	Read/Write Configuration	only Read Configuration	N/A

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

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

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

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

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

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

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

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

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

4.1 Status > GPS

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



5 Configuration > System

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



5.1 System > Time and Date

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

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

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

I. Get from Time Server

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

The screenshot shows the 'Time and Date' configuration page. At the top, it displays the 'Current Time' as 'Mar 15, 2019 9:31:24 AM'. The main section is titled 'Time and Date Setup' and contains three sub-sections: 'Time and Date Setup', 'Time Zone Setup', and 'Time Server'.

- Time and Date Setup:** The 'Mode' is set to 'Get from Time Server'. The 'GPS Time' is set to 'Off'. There are six input fields for IPv4 and IPv6 servers, with the following values: IPv4 Server #1: 0.pool.ntp.org, IPv4 Server #2: pool.ntp.org, IPv4 Server #3: clock.cdn.net, IPv4 Server #4: time4.net.gn, IPv4 Server #5: 2.pool.ntp.org, and IPv4 Server #6: clock.nyu.edu.net.
- Time Zone Setup:** The 'Time Zone' is set to '(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London'. The 'Daylight Savings' is set to 'Off'. The 'Ahead of standard time' is set to '00' min. The 'Start Date' is set to '3' / '2' / '8' (Month / Year / Day) and the 'Start Time' is '2' / '0' (Hour / Minute). The 'End Date' is set to '11' / '2' / '8' (Month / Year / Day) and the 'End Time' is '2' / '0' (Hour / Minute).
- Time Server:** The 'Server Mode' is set to 'Off' and the 'Server Port' is set to '123'.

An 'Apply' button is located at the bottom right of the page.

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.

The screenshot shows a web interface for configuring time and date. At the top, it displays the current time as 'Mar-15, 2019 9:22:38 AM'. Below this, there are three main sections: 'Time and Date Setup', 'Time Zone Setup', and 'Time Server'. In the 'Time and Date Setup' section, the mode is set to 'Manual' and the date is '2019-3-15 9:29'. The 'Time Zone Setup' section has 'Time Zone' set to '(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London', 'Daylight Savings' set to 'Off', and 'Ahead of standard time' set to '60' minutes. It also includes fields for 'Start Date' (3/2/0), 'Start Time' (2:0), 'End Date' (11/3/0), and 'End Time' (2:0). The 'Time Server' section has 'Server Mode' set to 'Off' and 'Server Port' set to '123'. An 'Apply' button is located at the bottom right of the form.

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:

Daylight Savings: Off On

Ahead of standard time: mins

Start Date: / / (Month / Week / Day)

Start Time: : (Hour / Minute)

End Date: / / (Month / Week / Day)

End Time: : (Hour / Minute)

System > Time Zone Setup > Daylight Savings	
Item	Description
Daylight Saving	Turn on/off the Daylight Savings feature. Select from Off or On. The default is Off.
Ahead of standard time	The forward/backward minutes when enter/leave Daylight Savings duration. Default is 60 minus.
Start Date / Start Time	<p>Time to enter Daylight Savings duration.</p> <p>The Month range is 1~12.</p> <p>1 - Jan. 7 - Jul. 2 - Feb. 8 - Aug. 3 - Mar. 9 - Sep. 4 - Apr. 10 - Oct. 5 - May 11 - Nov. 6 - Jun. 12 - Dec.</p> <p>The Week range is 1~5.</p> <ul style="list-style-type: none"> ● 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 <p>The Day range is 0~6.</p> <p>0 - Sunday (The start day of a week) 1- Monday 2 - Tuesday 3 - Wednesday 4 - Thursday 5 - Friday 6 - Saturday</p> <p>The Hour range is 0~23. The Min range is 0~59.</p>
End Date / End Time	Time to leave Daylight Savings duration. Same with Start Date/Start Time.

IV. Time Server

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

Time Server

Server Mode Off On

Server Port




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


5.2 System > COM Ports


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

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

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

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



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

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

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

#	Mode	Host Address	Protocol	Port	
1	Server		TCP	8090	On/Off
2	Disable		TCP	0	On/Off
3	Disable		TCP	0	On/Off

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

System > COM Ports	
Item	Description
Edit Configuration	
Baud Rate	Select from the current Baud Rate.
Data	Select from 7 bit or 8 bit.
Parity	Select from the information of Parity.

Stop	Select from 1 bit or 2 bit.
Flow Control	Select from none, Xon/Xoff or hardware.
Virtual COM	
Mode	Select from Disable, Server or Client.
Protocol	Select from TCP or UDP.
Host Address	The host address is only available on client mode. Specify what the domain name or IP address (IPv4 or IPv6) to be connected.
Redirect Port	<ul style="list-style-type: none"> • Server Mode: This network package of cellular router is on this port. • Client Mode: The network package of remote device is on the remote host.

5.3 System > Logging

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

5.3.1 Logging > Logging

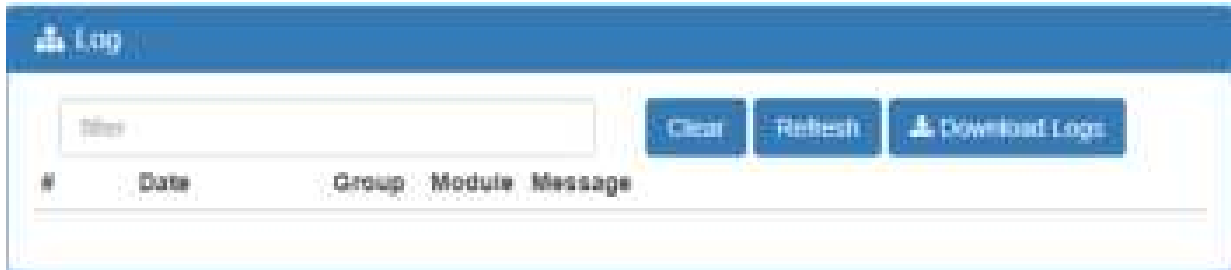
- (1) Logging section provides you to control all logging records.
- (2) Users need to select **Apply** to confirm your settings.

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

5.3.2 Logging > Log

This section displays all data status.

- (1) You can choose Filter function to quickly search for your data.
- (2) When you click **Clear**, all of the data that displays on the interface will be totally cleared without any backup.
- (3) When you click **Refresh**, the system will update and display the latest data from your cellular router.
- (4) When you click **Download Logs**, the system will download the latest data from your cellular router.



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

5.4 System > Alarm

This section allows you to configure the alarm.

Alarm configuration page showing various settings:

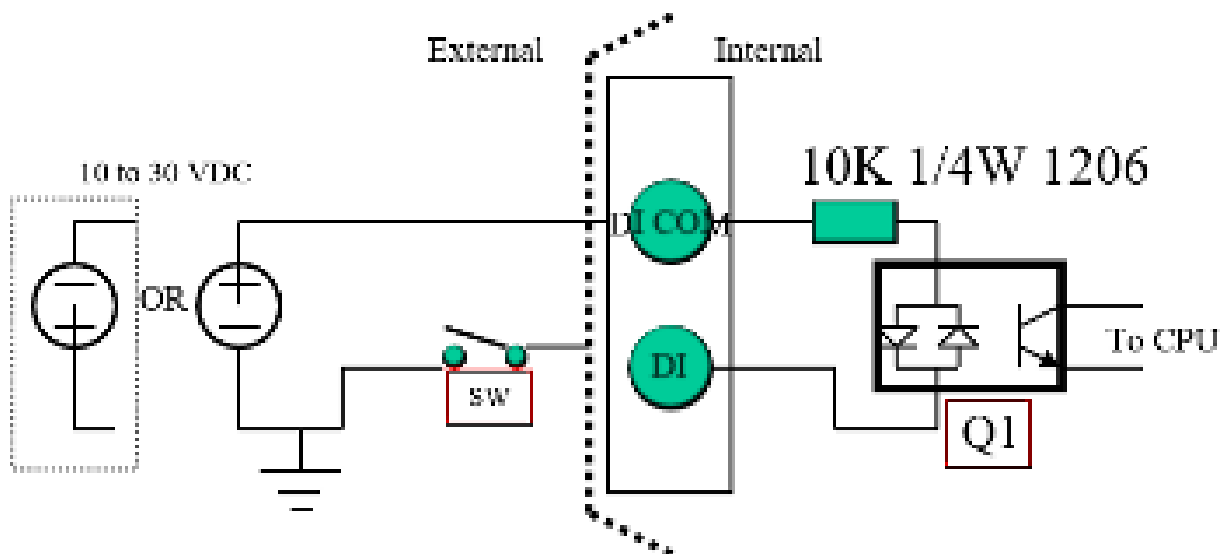
- Mode: Disable Enable
- Alarm input: SMS, DI 1, DI 2, VPN disconnect, WAN disconnect
- Alarm output: SMS, LAN disconnect, Reboot, DO, SNMP trap, E-mail
- DI 1 Trigger: High Low
- DI 2 Trigger: High Low
- DO behavior: Always Pulse
- SMS/E-mail: Limit 150 english characters

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

Apply

Note:

- (1) If you select **SMS** in Alarm input/output, you need to add the trust phone number into **Contracts/ On Duty**.
- (2) If you select **SNMP trap** in Alarm output, you need to set up SNMP trap configuration from Service SNMP.
- (3) If you select **E-Mail** in Alarm output, you need to set up SMTP configuration from Service SMTP.
- (4) If you select **TR069** in Alarm output, you need to set up TR069 configuration from Service TR069.



System > Alarm	
Item	Description
Mode	Turn on/off the Alarm configuration. Select from Disable or Enable. The default is Enable.
Alarm Input	Select from SMS, DI 1, DI 2, VPN disconnect and WAN disconnect as input to trigger alarm. <ul style="list-style-type: none"> ● SMS: It means on duty team members on Contacts / On Duty can send SMS to the phone number of using SIM card to trigger alarm. ● DI 1/2: IO to trigger alarm. ● VPN disconnect: All tunnels get disconnected then trigger alarm. ● WAN disconnect: WAN connections get disconnected then trigger alarm. ● LAN disconnect: LAN connection get disconnected then trigger alarm. ● Reboot: Reboot then trigger alarm.
Alarm Output	Select from SMS, DO, SNMP trap and E-mail as alarm output.
DI 1 / 2 Trigger	Select from High or Low. The default is High Trigger. <ul style="list-style-type: none"> ● High: SW is On to trigger. ● Low: SW is OFF to trigger.
DO behavior	<ul style="list-style-type: none"> ● Always: Pull DO high. ● Pulse: High and Low continuously. ● Pulse Time Length: Pulse time length (mini seconds).
SMS/E-mail	Write your messages and limit 150 English characters for the messages to deliver.

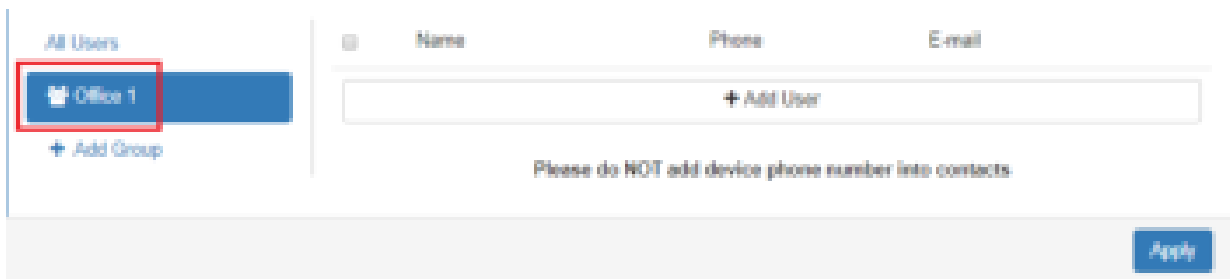
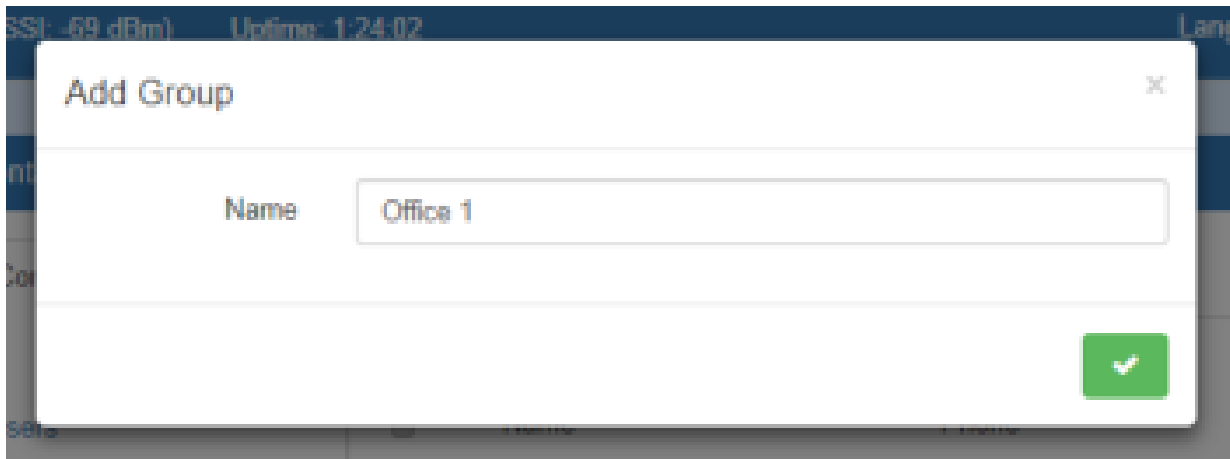
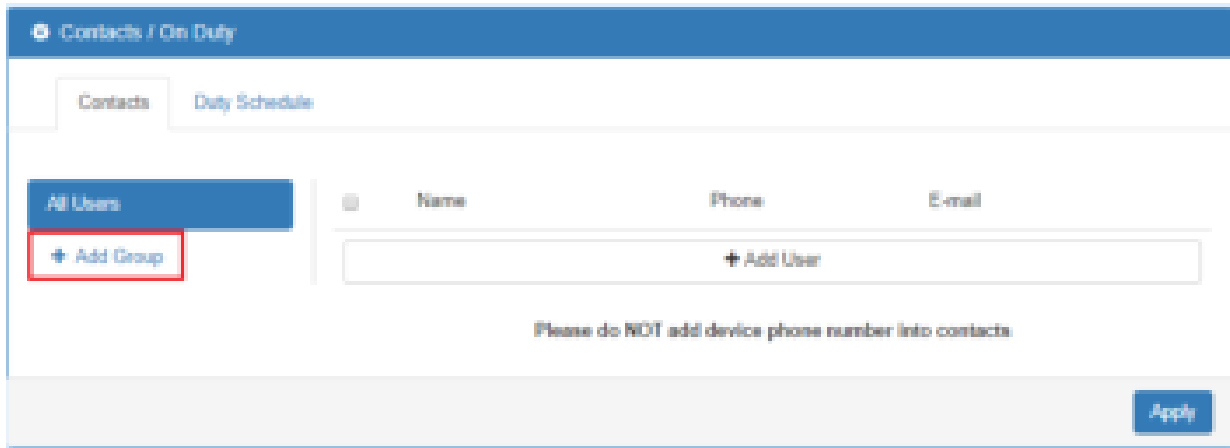
5.4.1 Alarm > Contacts > Create and name the Group

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

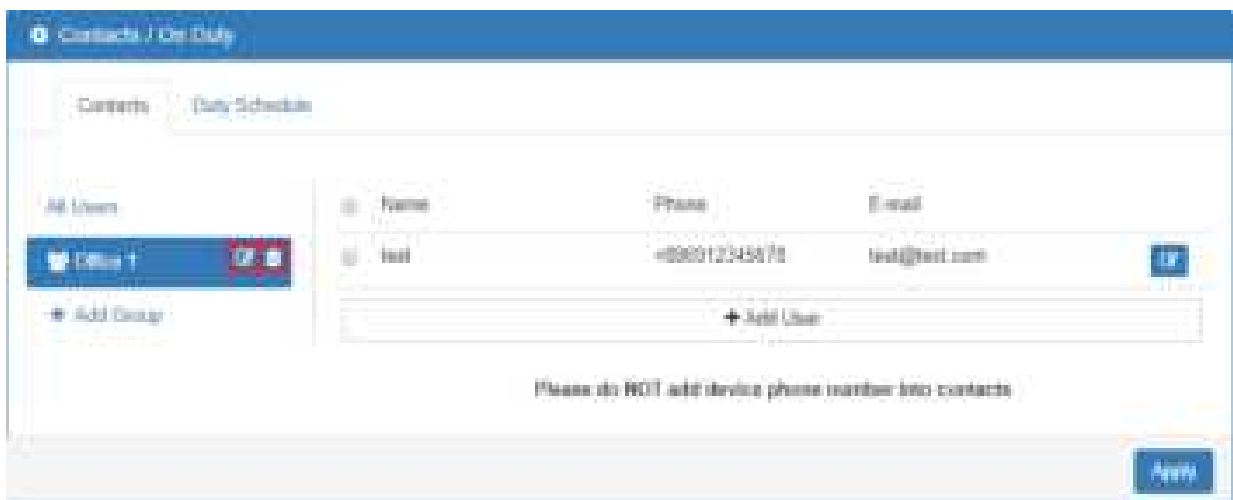
The screenshot shows the 'Alarm' configuration page. At the top, there's a blue header with 'Alarm' and a home icon. Below it, the settings are organized into sections:

- Mode:** Radio buttons for 'Disable' and 'Enable'.
- Alarm input:** Checkboxes for 'SMS', 'DI 1', 'DI 2', 'VPN disconnect', 'WAN disconnect', 'LAN disconnect', and 'Reboot'.
- Alarm output:** Checkboxes for 'SMS', 'DO', 'SNMP trap', and 'E-mail'.
- DI 1 Trigger:** Radio buttons for 'High' and 'Low'.
- DI 2 Trigger:** Radio buttons for 'High' and 'Low'.
- DO behavior:** Radio buttons for 'Always' and 'Pulse'.
- SMS/E-mail:** A text input field with a placeholder 'Limit 150 english characters'. Below it, a hint says 'Hint: for SMS/E-mail only accept trusted and on duty members', where 'trusted and on duty members' is highlighted with a red box.

An 'Apply' button is located at the bottom right of the configuration area.

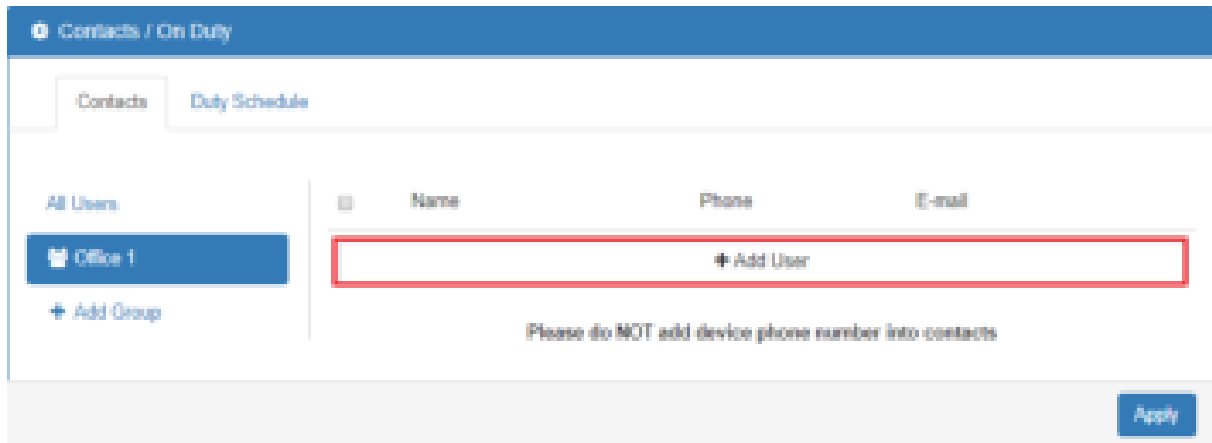



- You can click  or  button to edit or delete the group.



5.4.2 Alarm > Contacts > Add User

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





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



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



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



5.4.3 Alarm > Duty Schedule

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



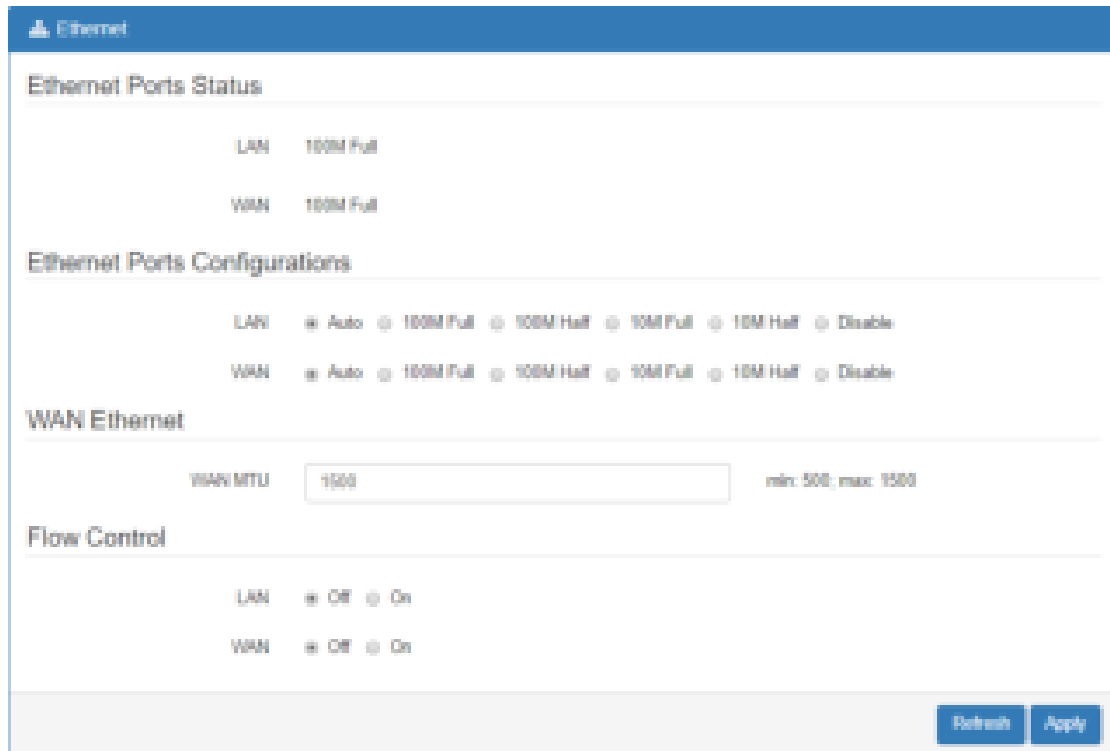
5.5 System > Ethernet

This section allows you to configure the Ethernet.

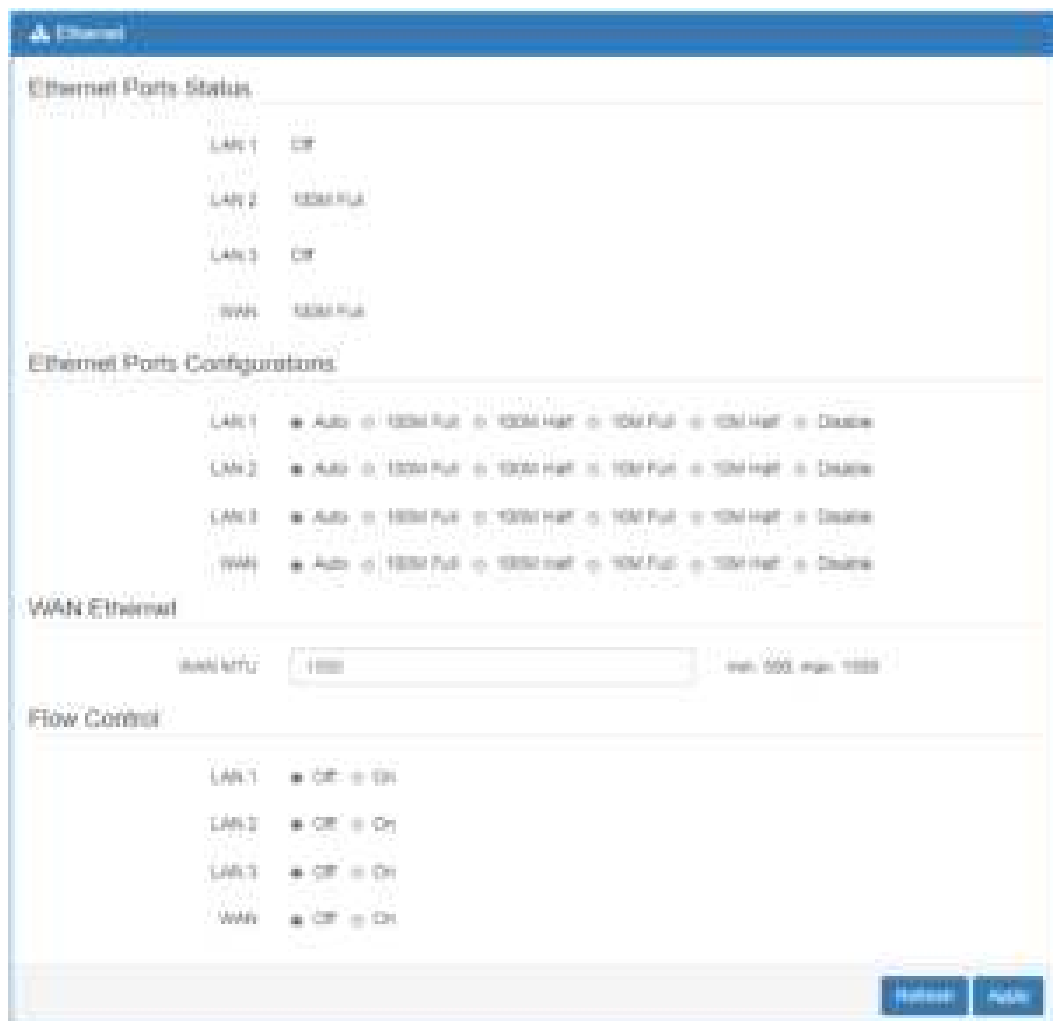
For Flow Control, it allows you to configure the Ethernet and solve unstable throughput under heavy loading. Sending 64 Bytes with bandwidth 100M bps traffic to LAN and WAN at the same time, the throughput may drop to zero at either side. When the system is very busy or buffer is exhausted, the flow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

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

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



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



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

5.6 System > Modbus

This section allows you to configure the Modbus.

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

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).

#	IP Address	MAC Address	Hostname	Start	End
1	192.168.1.1	20:11:35:69:00:ac	ASUS-K43-NS	2017/12/04 18:20:47	2017/12/04 18:20:47

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

Client List		
List Type	IP Address	MAC Address
1	192.168.1.19	00:FD:4D:68:21:73

System > Client List	
Item	Description
List Type	<ul style="list-style-type: none"> • DHCP Client: List all clients' information when it is via DHCP. • Online: List the information when it is online.

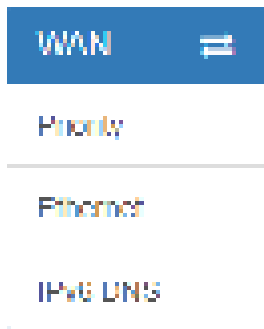
5.8 System > LED

This section allows you to set up the function led.

System > Client List	
Item	Description
Function LED	<ul style="list-style-type: none"> • Default: <ul style="list-style-type: none"> - ON: VPN connected. - Slow Blinking: WAN connected. - OFF: No WAN connection. • WiFi AP: <ul style="list-style-type: none"> - Heart Beat Blinking: WiFi clients connected and it takes precedence. - Otherwise as default behavior.

6 Configuration > WAN

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



6.1 WAN > Priority

You can set up the priority of WAN.



WAN > Priority	
Item	Description
Priority	<ul style="list-style-type: none">● ETH First: WAN Ethernet is first priority and the second priority is LTE. The default is ETH First.● LTE Only: The priority is only LTE.● ETH Only: The priority is only Ethernet.● LTE First: WAN LTE is first priority and the second priority is Ethernet.

6.2 WAN > Ethernet

6.2.1 WAN Ethernet Configuration

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

WAN Ethernet

Work As: DHCP Client PPPoE Client Static IPv4

Configuration | Ethernet Ping Health

DNS Server Configuration

IPv4 DNS Server #1: From ISP []

IPv4 DNS Server #2: From ISP []

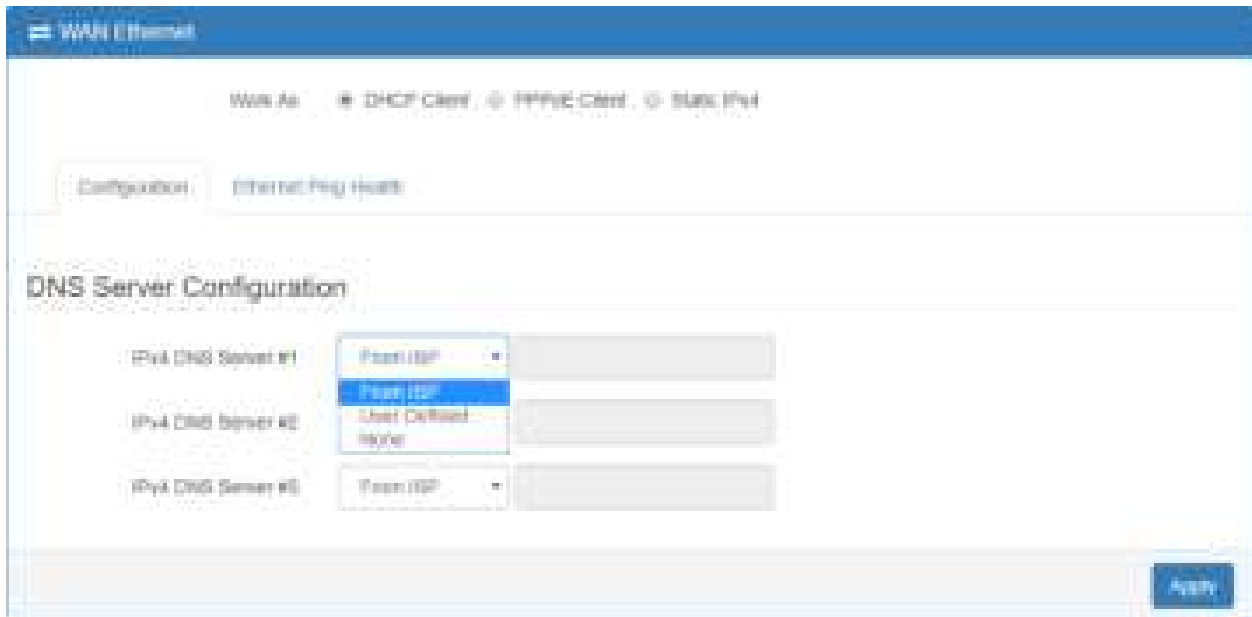
IPv4 DNS Server #3: From ISP []

Apply

WAN > Ethernet	
Item	Description
WAN Ethernet	<p>There are three options to obtain the IP of WAN Ethernet.</p> <ul style="list-style-type: none">● DHCP Client: DHCP server-assigned IP address, netmask, gateway, and DNS.● PPPoE Client: Your ISP will provide you with a username and password. This option is typically used for DSL services.● Static IPv4: User-defined IP address, netmask, and gateway address.

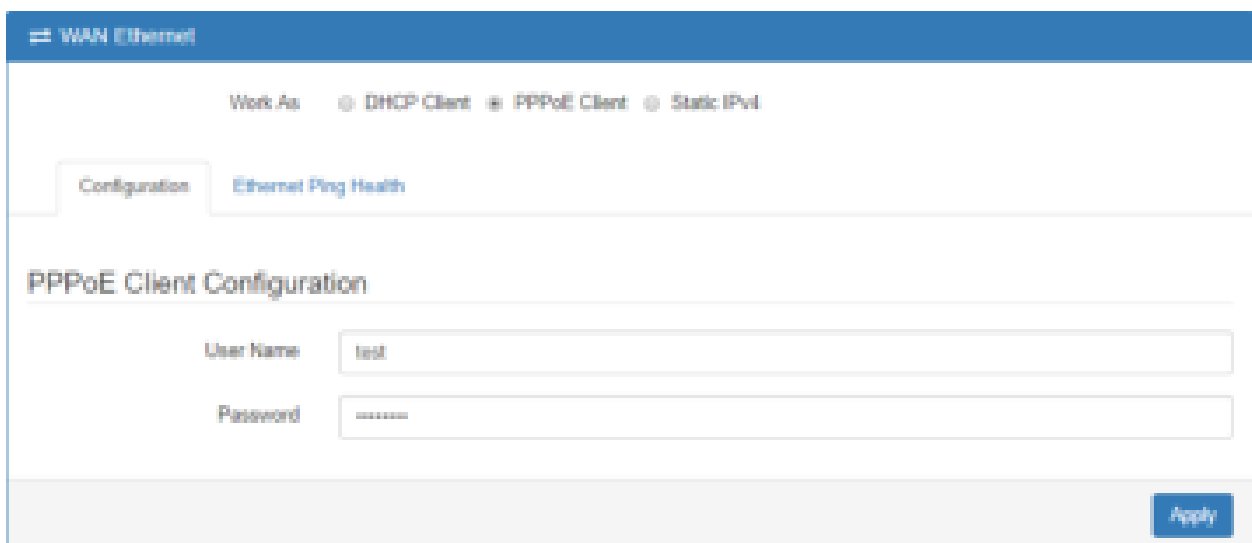
When selecting “**DHCP Client**”, you can set up DNS Server Configuration.

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



WAN > Ethernet > DHCP Client	
Item	Description
IPv4 DNS Server #1 IPv4 DNS Server #2 IPv4 DNS Server #3	<ul style="list-style-type: none"> • Each setting DNS Server has three options, including From ISP, User Defined and None. • When you select From ISP, the IPv4 DNS server IP is obtained from ISP. • When you select User Defined, the IPv4 DNS server IP is input by user.

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



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

The screenshot shows the WAN Ethernet configuration interface. At the top, there are radio buttons for 'Work As' with options: 'DHCP Client', 'PPPoE Client', and 'Static IPv4'. Below this, there are two tabs: 'Configuration' (selected) and 'Ethernet Ping Health'. The main content area is divided into two sections: 'Static IPv4 Configuration' and 'DNS Server Configuration'. In the 'Static IPv4 Configuration' section, there are three input fields: 'IP Address' (containing '0.0.0.0'), 'IP Mask' (containing '255.255.255.0'), and 'Gateway Address' (containing '0.0.0.0'). In the 'DNS Server Configuration' section, there are three empty input fields labeled 'IPv4 DNS Server #1', 'IPv4 DNS Server #2', and 'IPv4 DNS Server #3'. At the bottom right of the form, there is an 'Apply' button.

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

6.2.2 Ethernet Ping Health

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

The screenshot shows the WAN Ethernet configuration interface. At the top, there are tabs for 'Configuration' and 'Ethernet Ping Health'. Below this, the 'Ethernet Ping Health' section is active, with radio buttons for 'Disable' and 'Enable'. The 'Interval' is set to '30' seconds. There are two IPv4 Host fields with values '8.8.8.8' and '8.8.4.4', and two IPv6 Host fields with values '2001:4860:4860::888' and '2001:4860:4860::884'. A 'Hint' section explains that the system will switch to LTE if the ping fails and back to Ethernet if it succeeds. An 'Apply' button is at the bottom right.

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 Ethernet Interface when IPv6 is using as WAN connection.

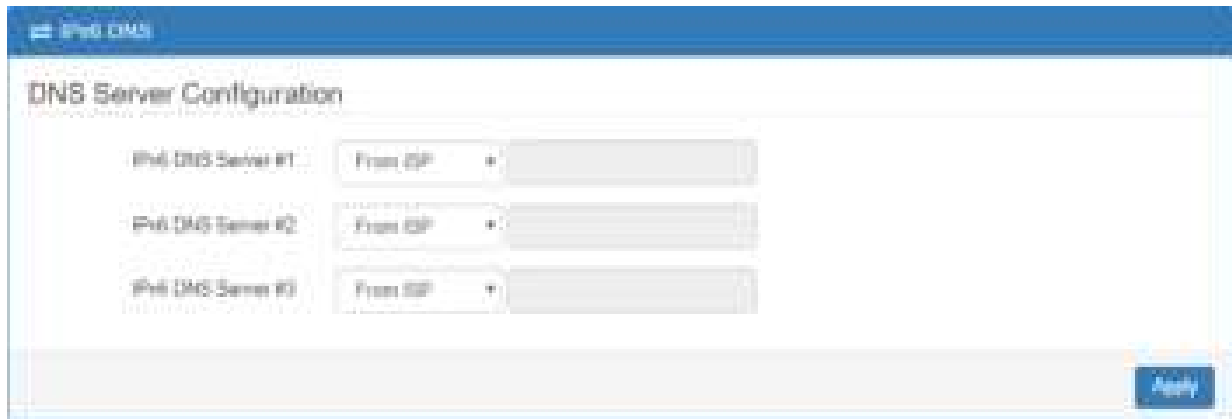
WAN LTE		
Att:	Current SIM	Backup SIM
SIM Card	SIM2	SIM1
Modem Status	Ready	Locked
Operator	Fair CellOne	ChinaNet Telecom
Modem Access	FDD LTE	FDD LTE
IMSI	46001108041467	46004090007738
Phone Number		
Band	LTE BAND 3	LTE BAND 7
Channel ID	1500	3000
IPv4 Address	10.146.85.142	
IPv4 Mask	255.255.255.255	

WAN Ethernet ✓	
Att:	Value
IPv4 Address	118.107.125.348
IPv4 Mask	255.255.255.255

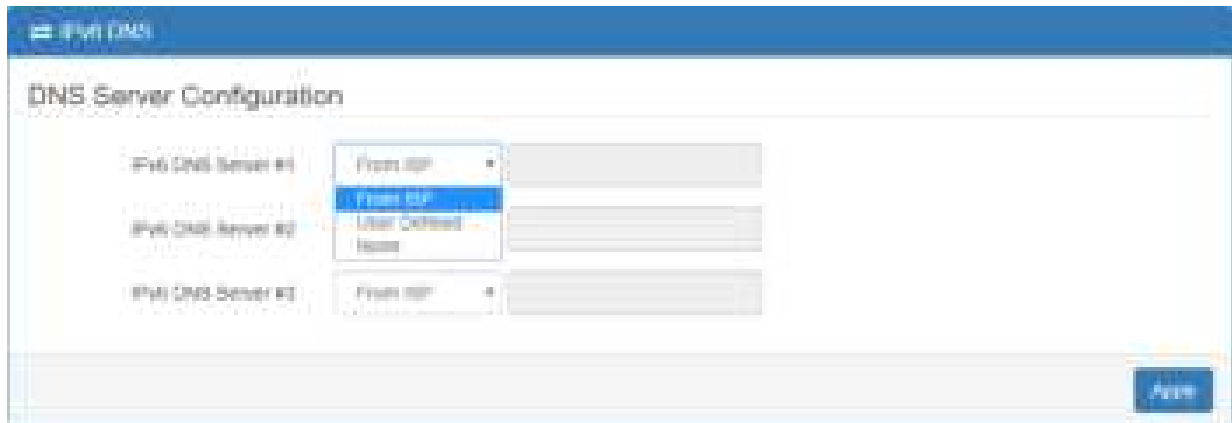
LAN Ethernet ✓	
Att:	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	2001:8011:7000:404::101

8.3 WAN > IPv6 DNS

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



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



WAN > IPv6 DNS	
Item	Description
DNS Server Configuration	
IPv6 DNS Server #1 IPv6 DNS Server #2 IPv6 DNS Server #3	<ul style="list-style-type: none"> • Each setting DNS Server has three options, including From ISP, User Defined and None. • When you select From ISP, the IPv6 DNS server IP is obtained from ISP. • When you select User Defined, the IPv6 DNS server IP is input by user.

7 Configuration > LTE

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

LTE
LTE Config
GPS
Dual SIM
Usage Display
SMS
Serving Cell
Lock PCs
Lock Bands
DNS

7.1 LTE > LTE Config

7.1.1 LTE Configuration

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

The screenshot shows the LTE Config web interface. At the top, there is a header "LTE Config" with a signal strength icon. Below the header, there are two main sections: "LTE Config" and "LTE Ping Health".

LTE Config:

- LTE Config:** A dropdown menu set to "Auto". To its right is a link: "Change this field before connecting".
- APN:** A text input field containing "cmcc". To its right is a link: "Set APN from SIM".

LTE Ping Health:

LTE Ping Health: Disabled Enabled

Interval: **Seconds**

IP Address 1:

IP Address 2:

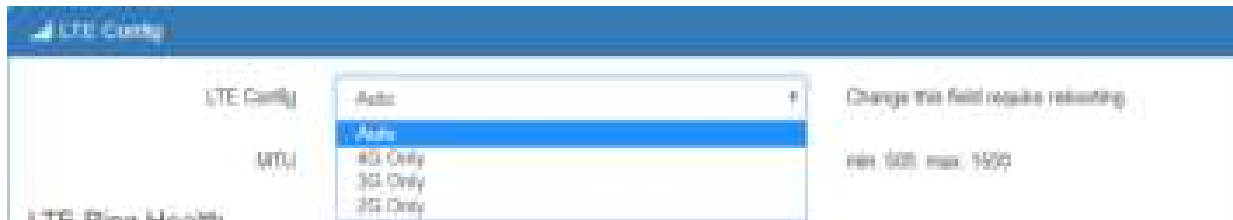
IP Address 1:

IP Address 2:

Test:

- When testing ping specified IP address to avoid the base station not find the ping server.
- In Dual SIM mode and both SIM are ready, all LTE ping test would ping into available SIM card for connection.

At the bottom right of the form, there is a blue "Apply" button.



LTE > LTE Config	
Item	Description
LTE Config	<ul style="list-style-type: none"> • Auto: Automatically connect the possible band. • 4G Only: Connect to 4G network only. • 3G Only: Connect to 3G network only. • 2G Only: Connect to 2G network only.
MTU	MTU is the Maximum Transmission Unit that can be sent over the LTE interface. It allows user to adjust the MTU size to fit into their existing network environment.

7.1.2 LTE Ping Health

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

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



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

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

7.2 LTE > GPS

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

GPS

GPS
RS232

Item	Value
Enable	off
Log on	0
IPV4V6	off
Auto on	off
Auto OFF	
IPV4V6	off

Apply

GPS

GPS
RS232

Apply Cancel Help

IPV4V6 IPV4 IPV6 IPV4 IPV6 IPV4 IPV6

Apply

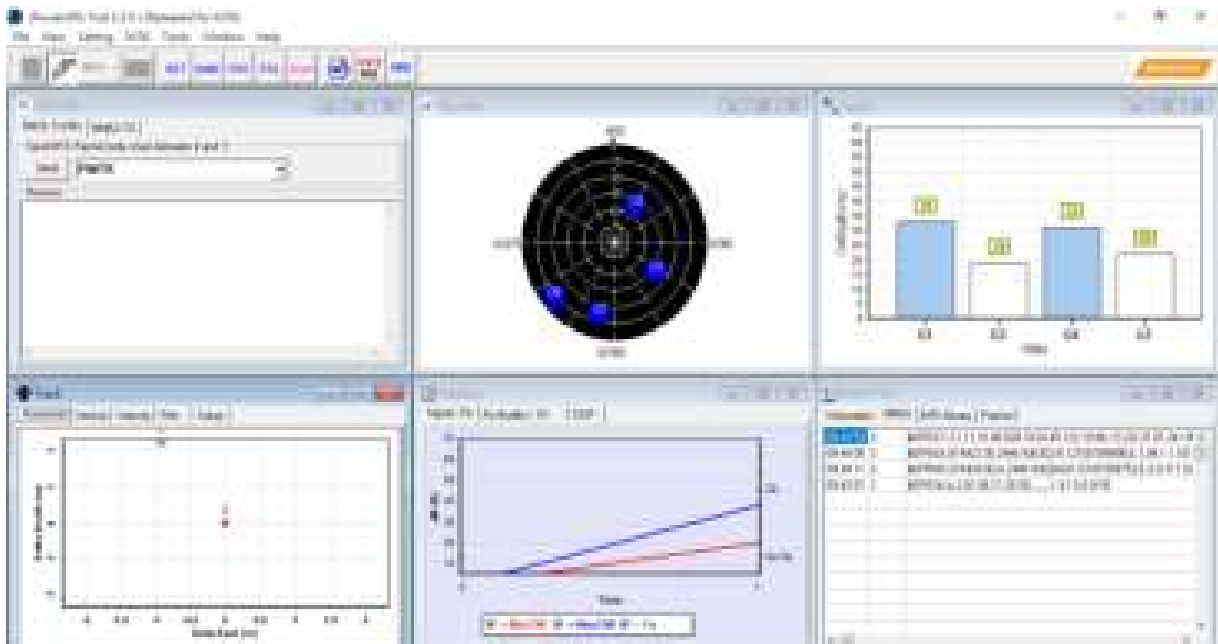
Note: You have to select **RS232** item and the interface shows the options of COM Port.

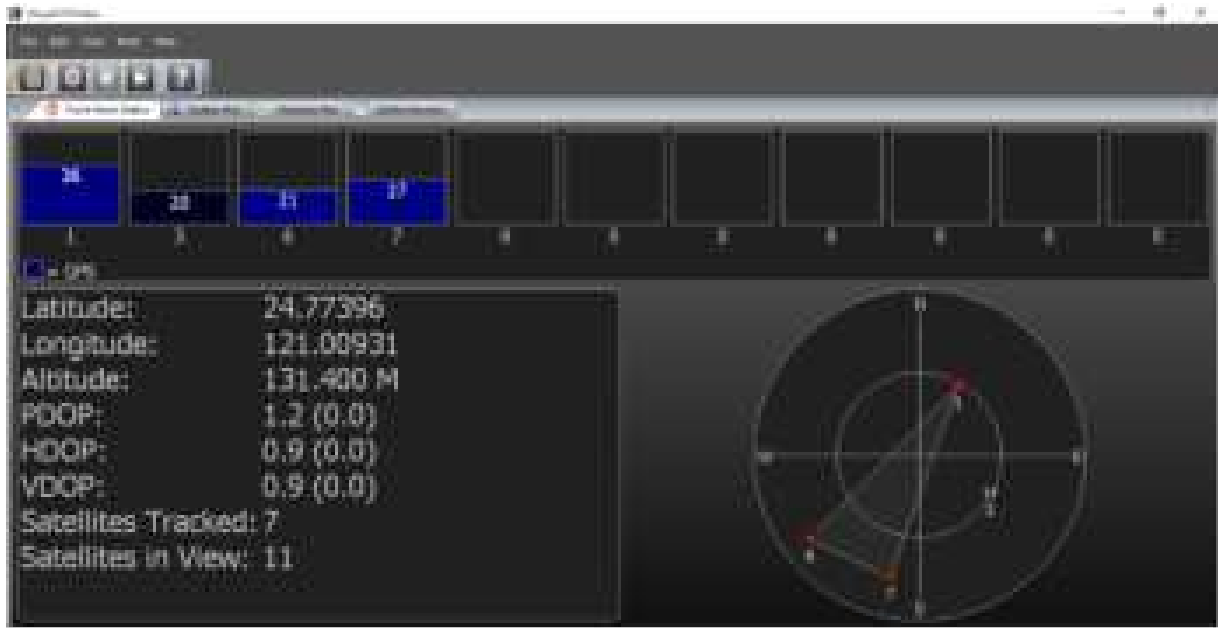


You can download software from internet and activate the GPS Configuration to display what information you need from your software.

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

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





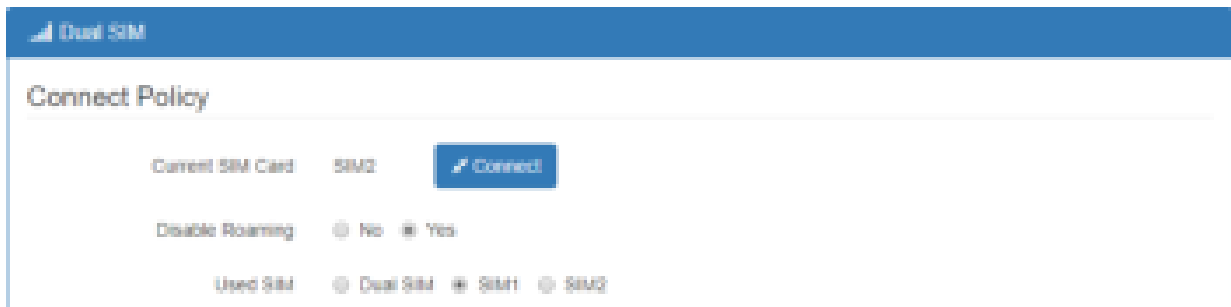
7.3 LTE > Dual SIM

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



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


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



The screenshot shows the 'Dual SIM' configuration page. At the top, it says 'Dual SIM' with a signal strength icon. Below that is the 'Connect Policy' section. It includes a 'Current SIM Card' dropdown set to 'SIM2' and a blue 'Connect' button. There are two radio button options: 'Disable Roaming' with 'No' selected and 'Yes' unselected, and 'Used SIM' with 'Dual SIM' selected, 'SIM1' unselected, and 'SIM2' unselected.

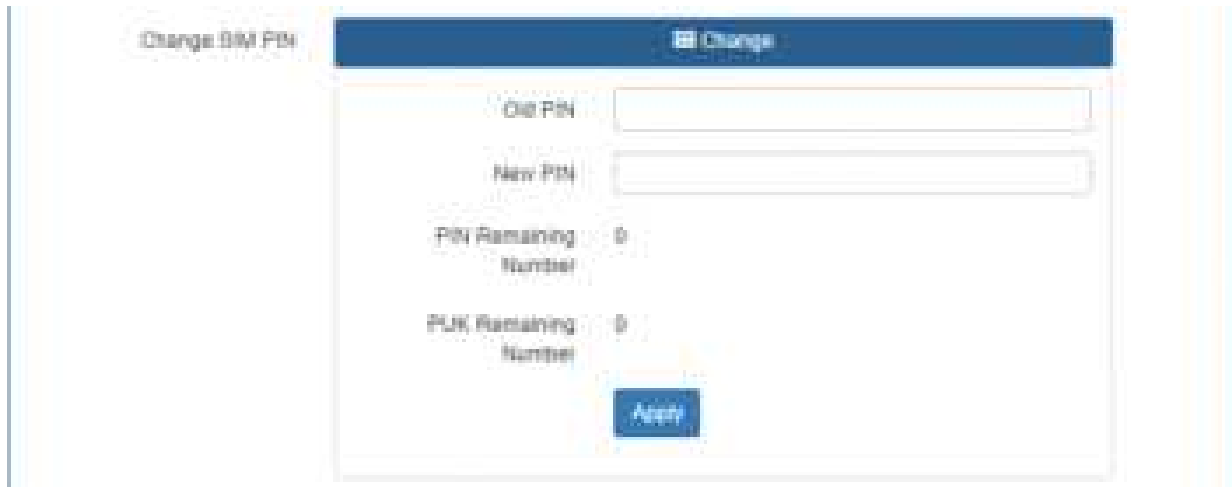
You can set up the SIM cards, SIM1 Configurations or SIM2 Configurations.

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



The screenshot shows the 'SIM1 Configuration' page. At the top, it says 'SIM1 Configuration' with a signal strength icon. Below that is the 'SIM1 Configuration' section. It includes a 'Status' dropdown set to 'Not Roaming'. There are four input fields: 'SIM PIN', 'Confirmed SIM PIN', 'SIM PUK', and 'Confirmed SIM PUK', which are highlighted with a red box. Below these are fields for 'APN', 'Username', 'Password', and 'Confirm Password'. There is a 'Auth' dropdown set to 'NONE' and a 'Change SIM PIN' button with a 'Change' sub-button. Below this is the 'Data Limitation' section, which includes a 'Always Used Data (MB)' field set to '0', a 'Mode' dropdown set to 'Default', a 'Max Data Limit (MB)' field set to '0', and several other fields for 'Monthly Limit', 'Daily Limit', 'Hourly Limit', and 'Weekly Limit'.

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



Note:

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



LTE > Dual SIM	
Item	Description
Connect Policy	
Current SIM Card	Display which SIM slot is using.
Status of SIM Card Connectivity	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● NO: Make the connection even the device is in roaming state. ● YES: No connection when the device in roaming state.
Used SIM	<ul style="list-style-type: none"> ● Dual SIM: Automatically switch SIM card when the current SIM card fail to make connection. ● SIM1: Only use SIM1 card slot. ● SIM2: Only use SIM2 card slot.
SIM Priority	<ul style="list-style-type: none"> ● Dual SIM: Automatically switch SIM card when the current SIM card fail to make connection. ● SIM1: Use SIM1 card slot as the first priority for connection. ● SIM2: Use SIM2 card slot as the first priority for connection.
Roaming Switch	Switch to another SIM when roaming is detected. System will switch SIM slot when current SIM is in roaming state and another SIM slot is in READY state.
Connect Retry Number	After timeout, the router attempts to switch another SIM Slot. The default timeout is three minutes. This option is only for Dual SIM mode.
SIM1 or SIM2 Configurations	
Status	Display the status of Dual SIM.
SIM PIN	A personal identification number (PIN) for ordinary use to protect your SIM card.
Confirmed SIM PIN	Double confirm SIM PIN.
SIM PUK	If user input the wrong SIM PIN more than 3 times, the user needs another password personal unblocking code (PUK) for PIN unlocking. Please check your operator for forgotten PUK number.
Confirmed SIM PUK	Double confirm SIM PUK.
APN	<p>The Access Point Name (APN) is the name for the settings to set up a connection to the gateway between your carrier's cellular network and the Public Internet.</p> <p>Leave it empty will search internally database automatically by SIM card for connection; however, please notice APN1 and APN2 must be manually configured different setting while concurrently use.</p>
Username	The username can be input by user or the system will search from internal database if the username is blank.

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

7.4 LTE > Usage Display

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

(1) Real-Time Usage:

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



(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.



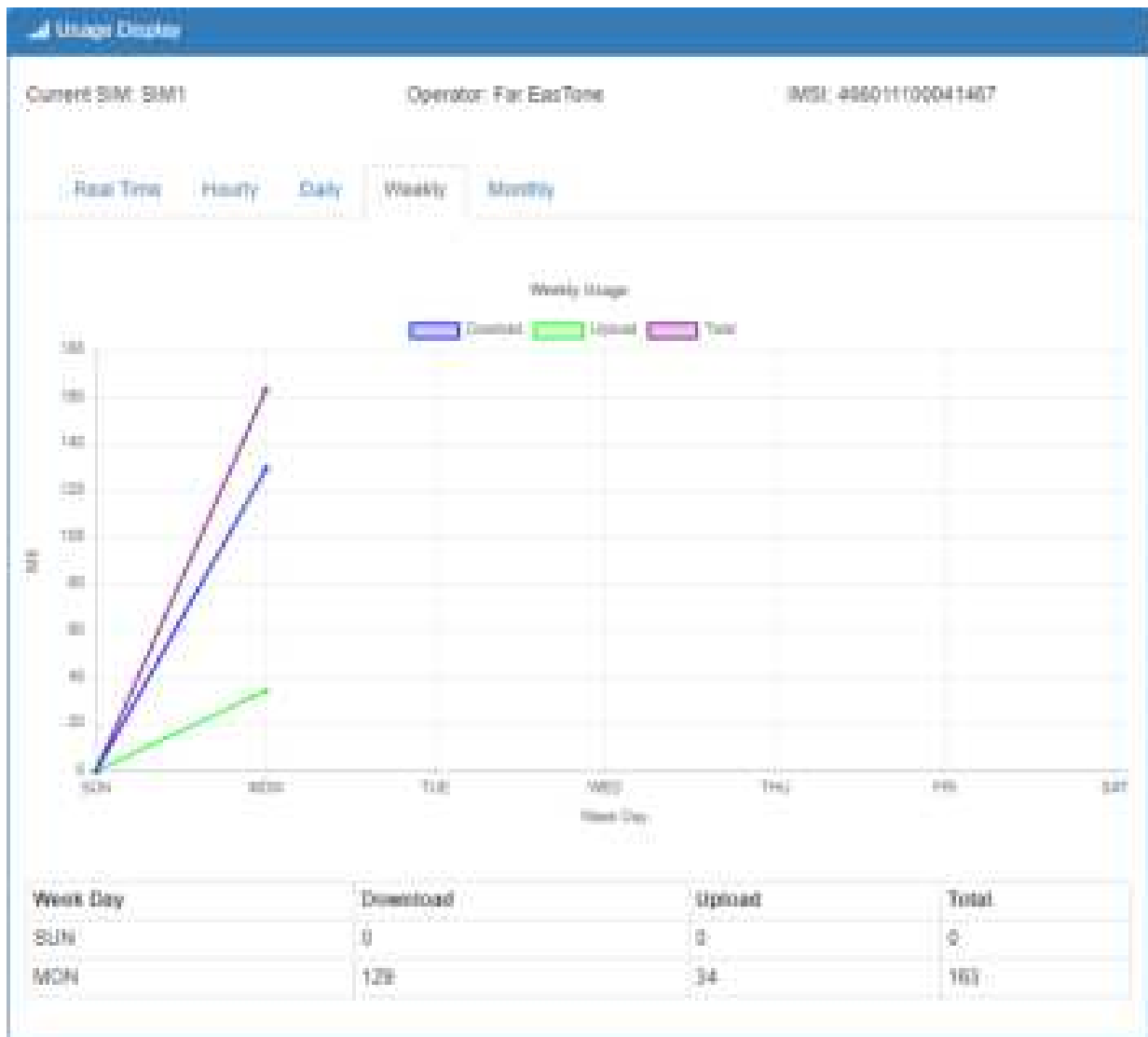
(3) Daily Usage:

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



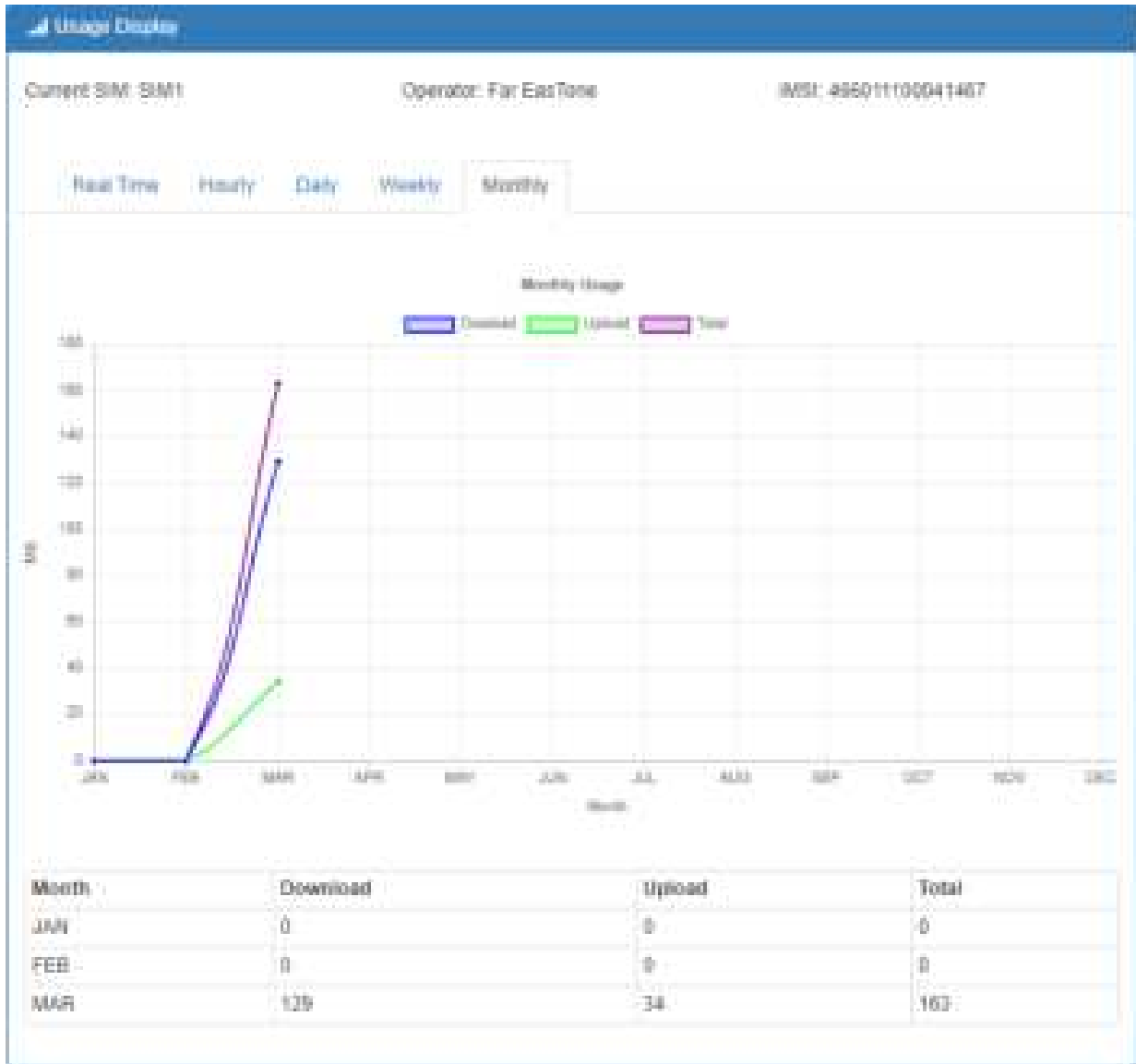
(4) Weekly Usage:

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



(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.



7.5 LTE > SMS




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

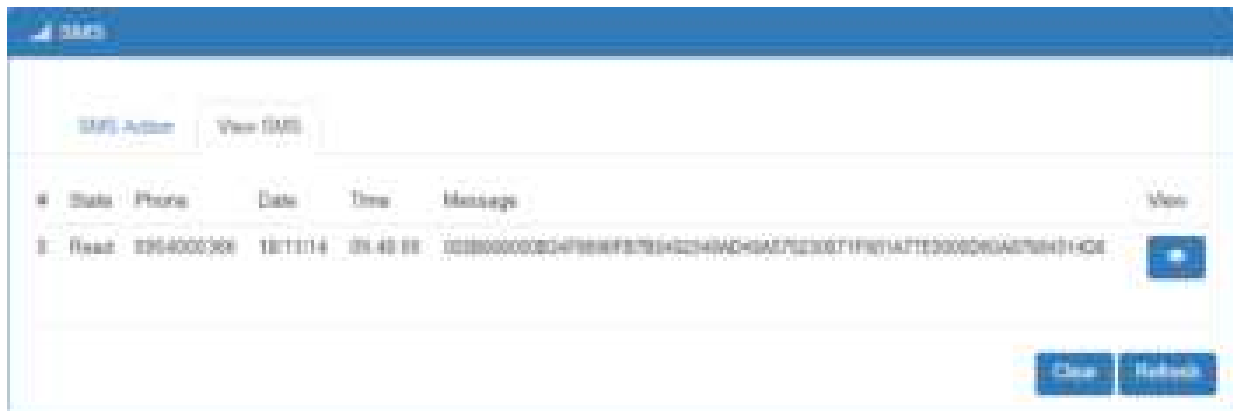
- (1) When enabling **SMS Action**, it allows trust phone number which in **Contacts/On Duty** list by sending key words SMS to trigger device setting/action/query status.

The screenshot shows the 'SMS Action' configuration page. At the top, there are tabs for 'SMS Action' and 'View SMS'. Below the tabs, there are radio buttons for 'None', 'Disable', and 'Enable', with 'Enable' selected. The main section is titled 'Actions and Keywords Setup' and contains a list of settings, each with a label and a text input field containing a keyword:

Action	Keyword
Reboot	REBOOT
Disconnect LTE	MOBILE_DISCONNECT
Connect LTE	MOBILE_CONNECT
Disable OpenVPN	MOBILE_OPENVPN_DISABLE
Enable OpenVPN	MOBILE_OPENVPN_ENABLE
Disable IPsec	MOBILE_IPSEC_DISABLE
Enable IPsec	MOBILE_IPSEC_ENABLE
Query Mobile Status	MOBILE_STATUS
Disable Alarm	MOBILE_ALARM
Enable Alarm	REENABLE_ALARM
Disable DO Alarm	MOBILE_DO_ALARM
Enable DO Alarm	REENABLE_DO_ALARM
Disable SMS Alarm	MOBILE_SMS_ALARM
Enable SMS Alarm	REENABLE_SMS_ALARM
Disable MMS Alarm	MOBILE_MMS_ALARM
Enable MMS Alarm	REENABLE_MMS_ALARM
Disable Email Alarm	MOBILE_EMAIL_ALARM
Enable Email Alarm	REENABLE_EMAIL_ALARM
DO On	MO DO
DO Off	MO DO
DO Push	MO PUSH
Restore DO Alarm	RESTORE_DO_ALARM

At the bottom of the page, there is a note: 'Note: Only accept SMS from trusted and on-duty members.' and a 'Apply' button.

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



7.6 LTE > Serving Cell

This section displays all parameters, including the following items:

Item	Value
RSRP	-115
RSRQ	-104
SINR	6
RSCP	12
ECIO	14
Cell Identity	12011412
eNB ID	120114
Cell ID	12
PCI ID	120
EARFCN	3550
UL Bandwidth	20MHz
DL Bandwidth	20MHz

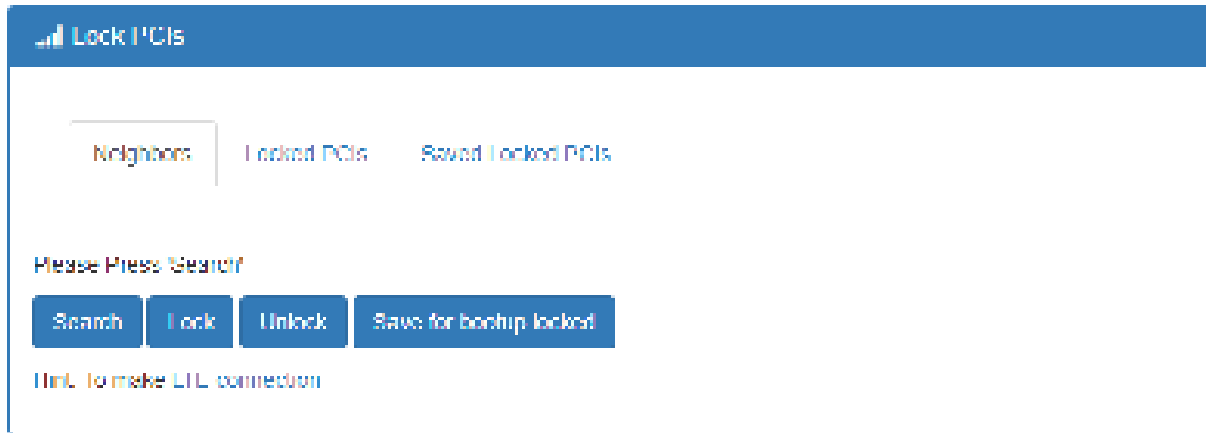
Refresh

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

7.7 LTE > Lock PCIs

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

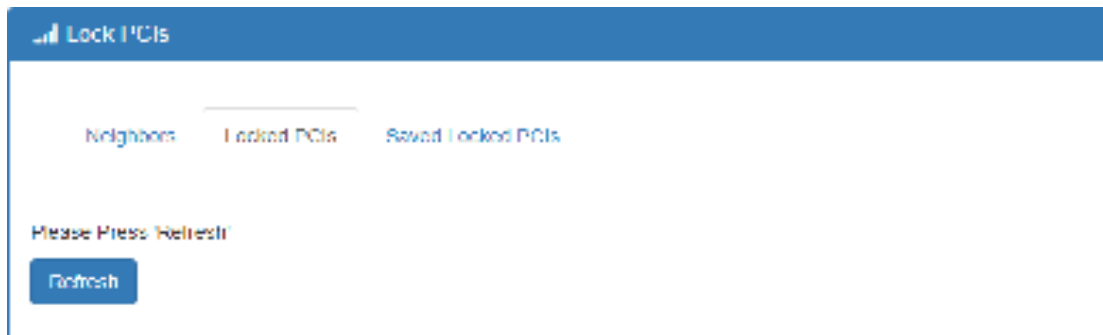
7.7.1 Neighbors



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

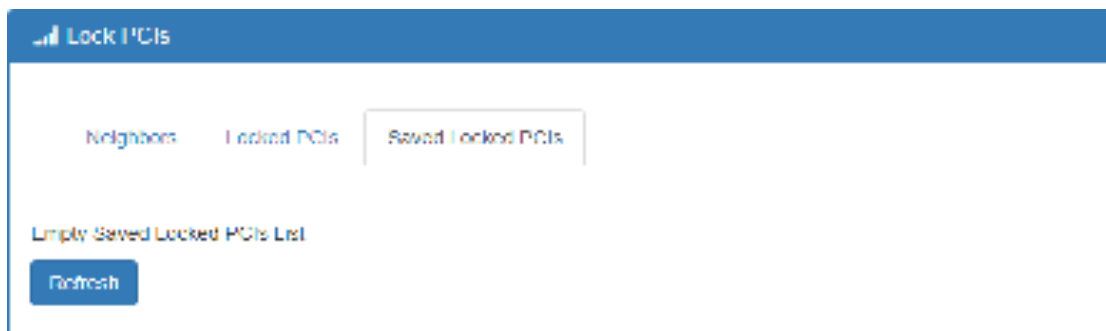
7.7.2 Locked PCIs

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



7.7.3 Saved Locked PCIs

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



7.8 LTE > Lock Bands

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

Lock LTE Bands

LTE Bands

B01 B02 B03 B04 B05 B06 B07 B08 B09

U10

U11 U12 U13 U14 U15 U16 U17 U18 U19

B20

B21 B22 B23 B24 B25 B26 B27 B28 B29

U20

U21 U22 U23 U24 U25 U26 U27 U28 U29

B40

B41 B42 B43

Hint [B3/B5] TDD-B3/B4/B10/B41; FDD-B1/B3/B5/B7/B8/B20

[Restore Default Band](#) [Apply](#)

7.9 LTE > DNS

This section allows you to setup LTE specific DNS setting.

DNS

APN1 DNS Server Configuration

IPv4 DNS Server #1

IPv4 DNS Server #2

IPv4 DNS Server #3

APN2 DNS Server Configuration

IPv4 DNS Server #1

IPv4 DNS Server #2

IPv4 DNS Server #3

[Apply](#)

LTE > DNS	
Item	Description
IPv4 DNS Server #1 IPv4 DNS Server #2 IPv4 DNS Server #3	<ol style="list-style-type: none"> 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.

8 Configuration > WiFi (M301-GW)

8.1 WiFi > WiFi Config

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

Item	Description
AP Enable	Turn on/off the Wi-Fi Network. Select from Disable or Enable. The default is Enable.
HT Mode (HT Capability)	20M: Only 20MHz Operation is Supported,40M: Both 20MHz and 40MHz Operation is Supported.
Country Code	Select Country Area for supported Channels
Name(SSID)	SSID is Wi-Fi identification. The maximum length is 32
Channel	Auto (Automatically select the best channel) or manually select channel number.

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

8.2 WiFi > Client List

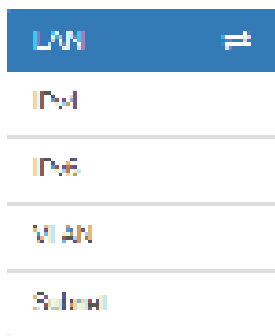
This section allows you to see all the Connected WiFi Client List.

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

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

Configuration > LAN

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



9.1 LAN > IPv4

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



LAN > IPv4	
Item	Description
LAN IPv4	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Turn on/off DHCP Server Configuration.• Enable to make router can lease IP address to DHCP clients which connect to LAN.
IP Address Pool	<ul style="list-style-type: none">• Define the beginning and the end of the pool of IP addresses which will lease to DHCP clients.
Static IP Addresses	DHCP server support static IP address assignment. The static IP address can be added by clicking the + Add Static IP Address button. Each static IP consist of mode(on/off), MAC and IP address. <ul style="list-style-type: none">• Mode: Turn on/off the static IP address• MAC: The MAC address of target host or PC• IP: The desired IP address for target host or PC

9.2 LAN > IPv6

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

The screenshot shows the 'LAN IPv6' configuration page. At the top, there's a header 'LAN IPv6'. Below it, the 'Type' section has two radio buttons: 'Delegate Prefix from WAN' (which is selected) and 'Static'. Underneath is a text input field labeled 'Static Address'. The 'DHCP Server Configuration' section has three radio buttons: 'Address Assign' (selected), 'Stateful', and 'Stateless'. At the bottom right, there is a blue 'Apply' button.

LAN > IPv6	
Item	Description
Type	<ul style="list-style-type: none">• Delegate Prefix from WAN Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.• Static Select this option to configure a fixed IPv6 address for the cellular router's LAN IPv6 address.
Static Address	You need to input the static address when you select the static type.
DHCP Server Configuration	
Address Assign	Select how you obtain an IPv6 address. <ul style="list-style-type: none">• Stateless: The cellular router uses IPv6 stateless auto configuration. RADVD (Router Advertisement Daemon) is enabled to have the cellular router send IPv6 prefix information in router advertisements periodically and in response to router solicitations.• Stateful: The cellular router uses IPv6 stateful auto configuration. The LAN IPv6 clients can obtain IPv6 addresses through DHCPv6.

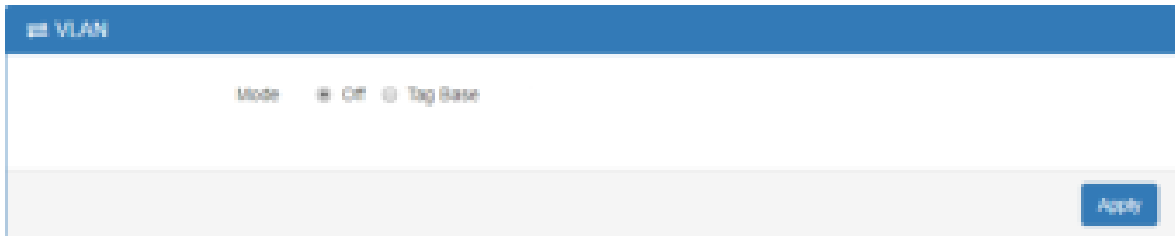
9.3 LAN > VLAN

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

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

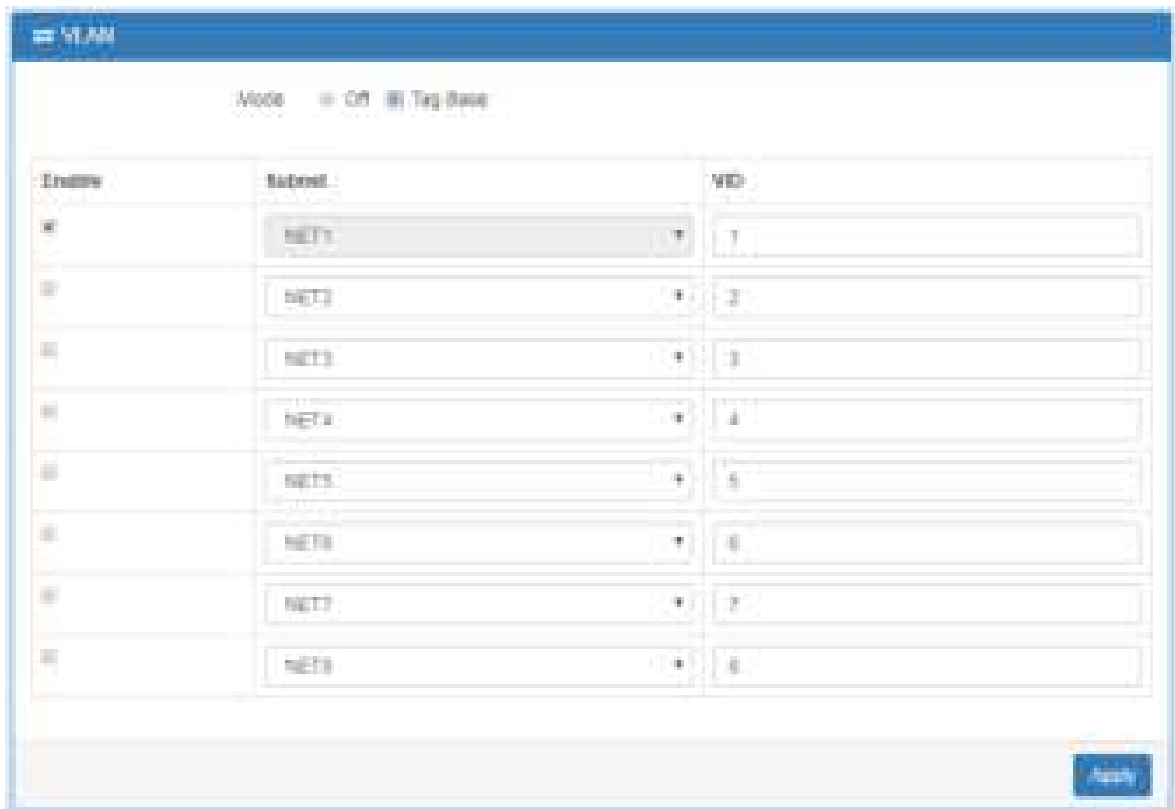
- Type 1:

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



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

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



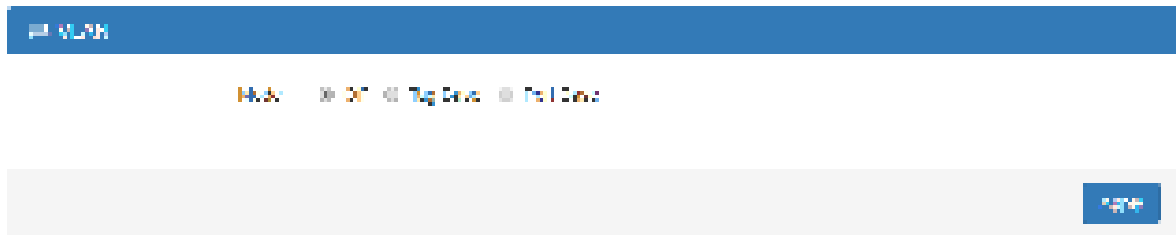
Furthermore, the **Subnet** provides DHCP Server function to allow the third party for the same VLAN to get IP address and IP mask. Therefore, you do not need to configure manually.

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

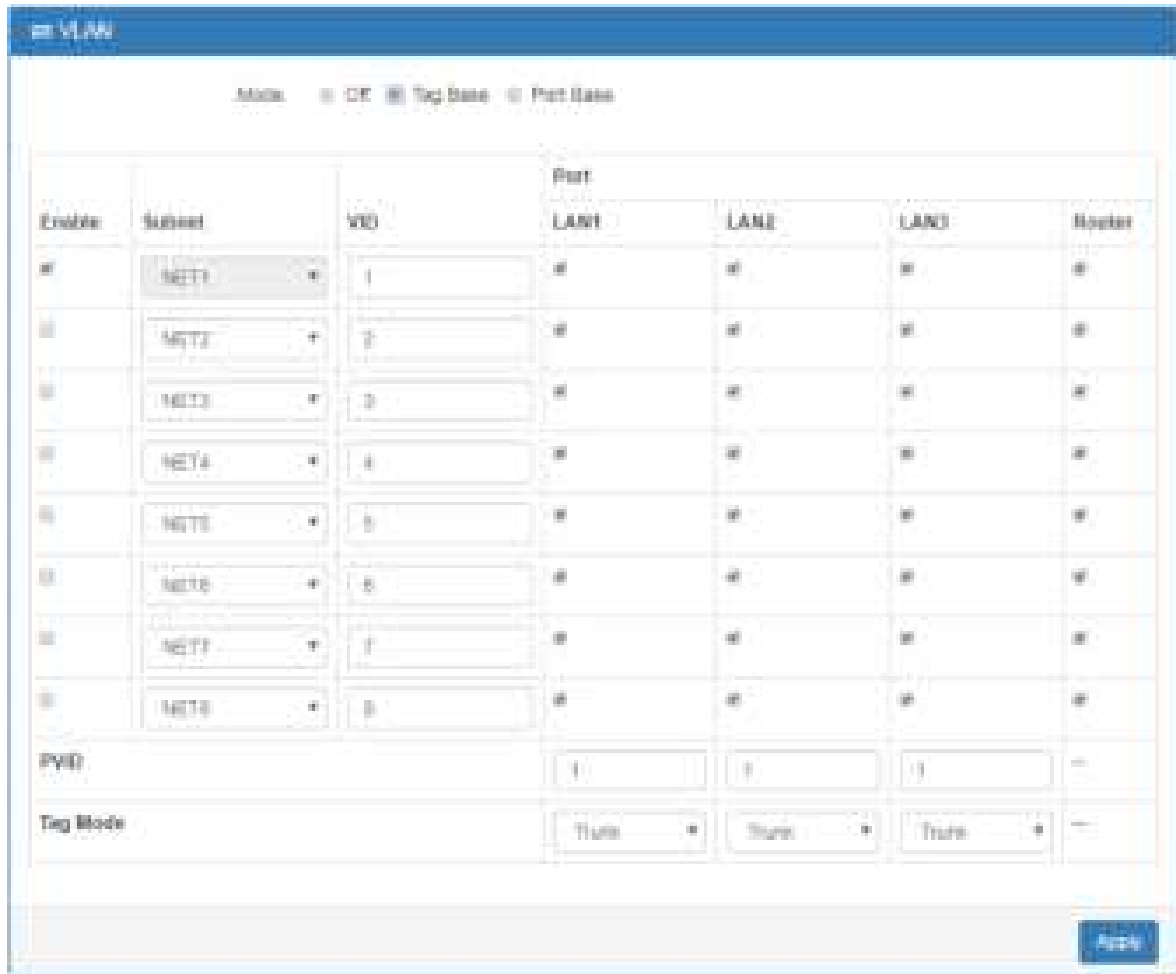
LAN > VLAN (1-port LANs)	
Item	Description
Mode	The VLAN mode is Off or Tag Base (802.1p VLAN).
Enable	The assigned row of setting is enabled.
Subnet	The subnet provides IP address and IP mask for the router.
VID	The VLAN ID range is from 1 to 4094.

- Type 2:

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



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



The **VLAN Isolation** function allows administrator to separate the different Subnet (VLAN). When it is on, the different Subnet (VLAN) user cannot communication each other.

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

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

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

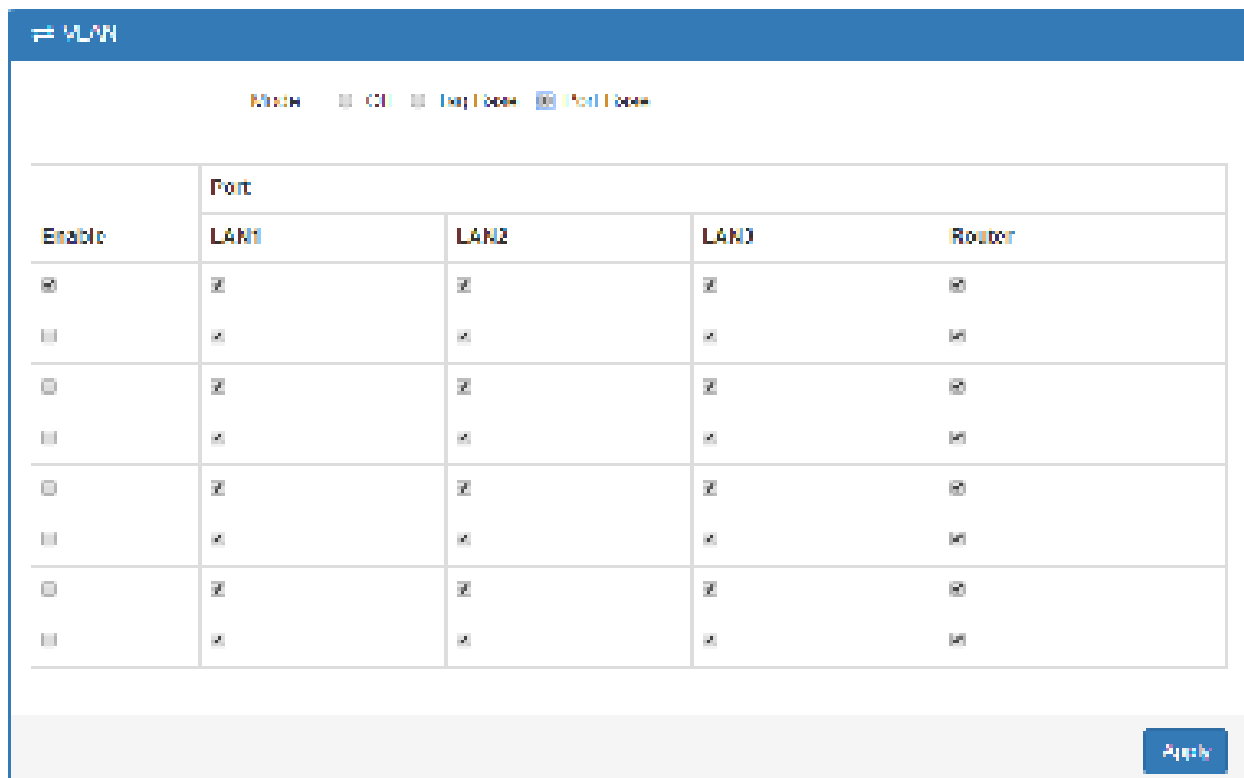
There are three ports for **Tag Base Mode**, including LAN1, LAN2 and LAN3. And one **Router port**

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

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

LAN > VLAN (3-port LANs) > Tag Base	
Item	Description
Mode	The VLAN mode is Off or Tag Base (802.1p VLAN).
VLAN Isolation	The VLAN Isolation is Off or On.
Enable	The assigned row of settings is enabled.
Subnet	Sets the IP address, IP mask and DHCP server.
VID	The VLAN ID range is from 1 to 4094.
Port	The port is shown to assign the port to a VLAN which the device is connected from LAN 1, LAN2, LAN3 and Router.
PVID	<ul style="list-style-type: none"> The PVID range from 1 to 4094 Sets the default VLAN ID for untagged devices connected to the port.
Tag Mode	<ul style="list-style-type: none"> The Trunk port setting is connected to another 802.1p VLAN aware switch or device. The Access port setting is connected to a single untagged device.

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



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

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

9.4 LAN > Subnet

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

Subnet

Name	IP Address	IP Mask	Off
M-17	192.168.2.1	255.255.255.0	<input type="checkbox"/>
M-18	192.168.2.1	255.255.255.0	<input type="checkbox"/>
M-12	192.168.2.1	255.255.255.0	<input type="checkbox"/>
M-13	192.168.2.1	255.255.255.0	<input type="checkbox"/>
M-16	192.168.2.1	255.255.255.0	<input type="checkbox"/>
M-14	192.168.2.1	255.255.255.0	<input type="checkbox"/>
M-15	192.168.2.1	255.255.255.0	<input type="checkbox"/>

Add Subnet

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

Subnet

IP Address:

IP Mask:

DHCP Server Configuration

DHCP Server Configuration:

IP Address Pool: From To

10 IP Routing

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

IP Routing	☒
Static Route	
RIP	
OSPF	
BGP	

10.1 IP Routing > Static Route

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

The screenshot shows the 'Static Route' configuration page. At the top, there are tabs for 'Settings' and 'Status'. Below this is a table with the following columns: Mode, Name, Destination, Gateway, Interface, and Delete. The table contains one entry with Mode set to 'Off', Name as an empty field, Destination as '192.168.100.0/24', Gateway as '192.168.1.255', and a red delete button. Below the table is a form for adding a new static route. The form has a 'Mode' dropdown set to 'Off', a 'Name' text field, a 'Destination' text field, a 'Gateway' text field, and an 'Interface' dropdown menu. A 'Submit' button is located at the bottom of the form. At the bottom right of the page, there is an 'Apply' button.

IP Routing > Static Route > Settings

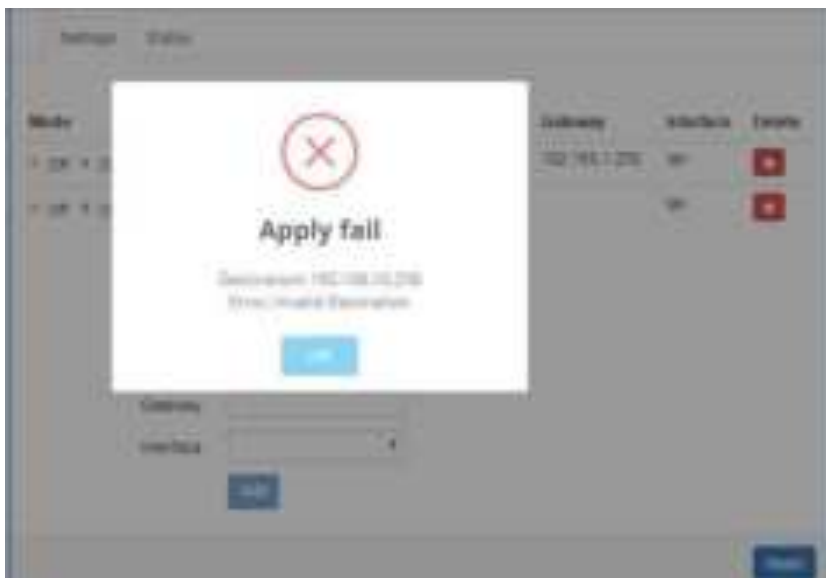
Item	Description
Mode	The setting is for full network. Select from Off or On.
Settings	
Mode	The setting is for the specific network. Select from Off or On.

Name	Set up each name for your running host or network.
Destination	Fill in the destination of a specific subnet or IP from network.
Gateway	Fill in the gateway address of your router.
Interface	Select the interface from LAN or Ethernet.

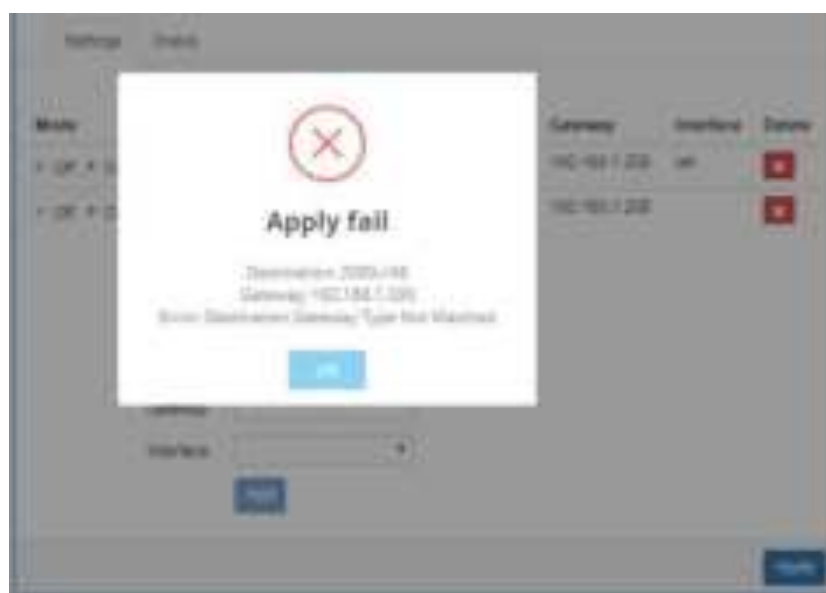
Note:

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

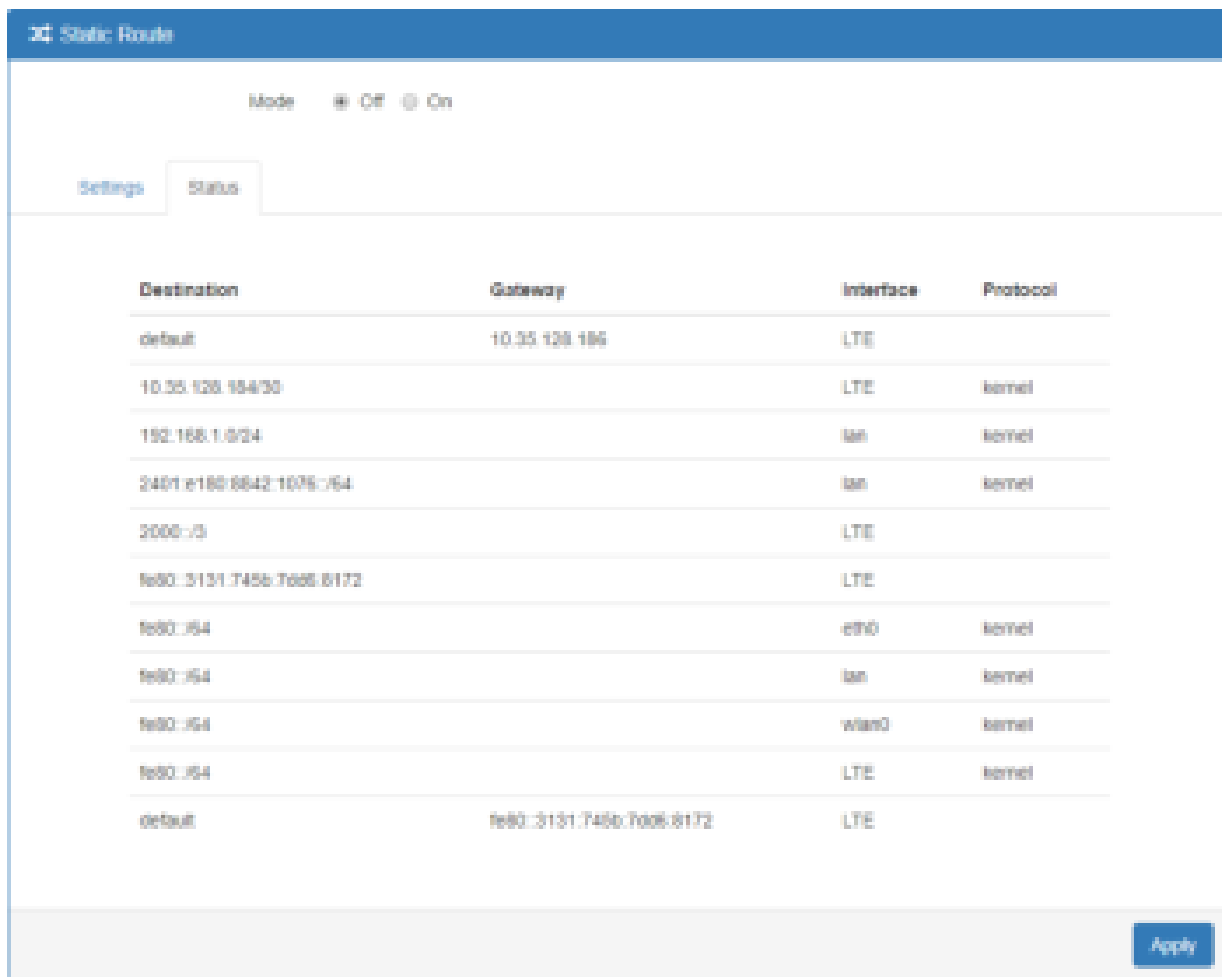
(1) Input the invalid format of destination. The interface is shown in **Apply fail** to notice.



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



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



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

10.2 IP Routing > RIP

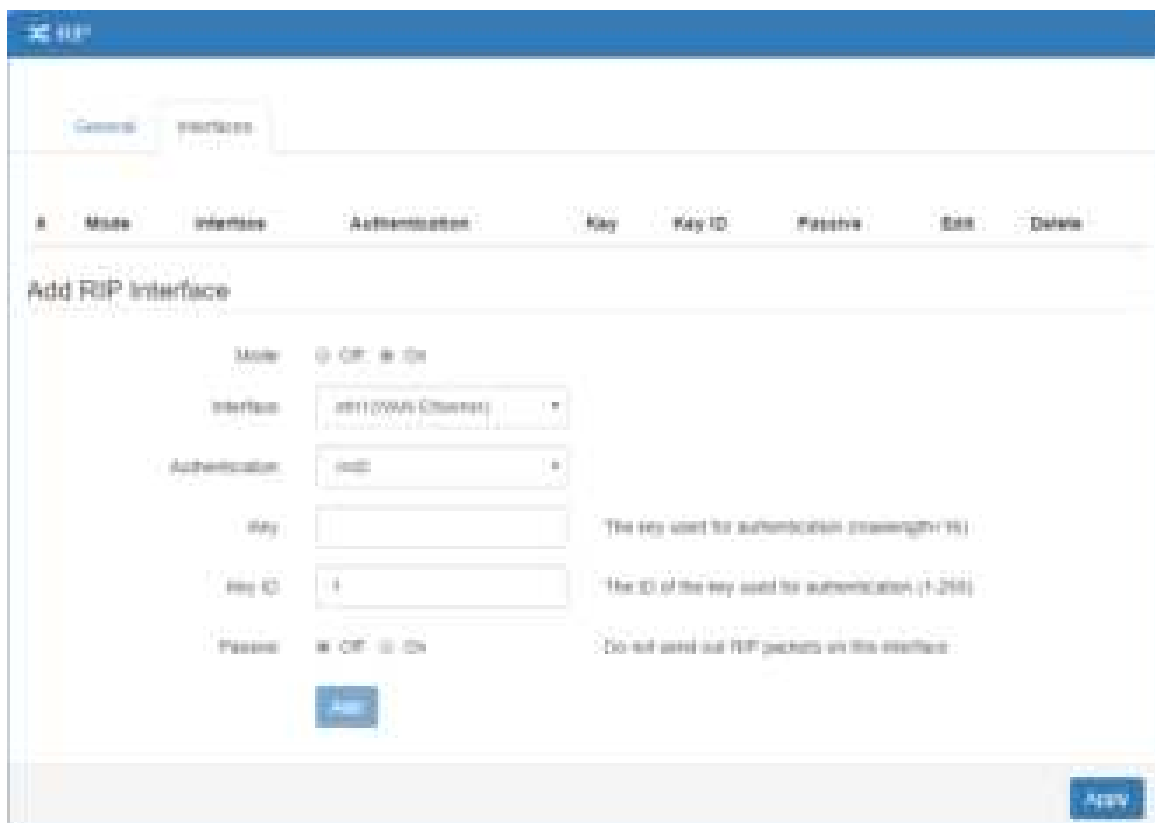
This section allows you to configure RIP and select the mode from Disable or Enable. The default is Disable.

Note:

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



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



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

10.3 IP Routing > OSPF

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

(1) General Configuration

IP Routing > OSPF > General	
Item	Description
General	
Mode	<ul style="list-style-type: none"> Off: OSPF function is off. On: OSPF function is on.
Redistribute local routes	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Off: Not redistribute connected routes to networks which are directly connected to the device.

	<ul style="list-style-type: none"> ● On: Redistribute connected routes to networks which are directly connected to the device.
Redistribute RIP routes	<ul style="list-style-type: none"> ● Off: Not redistribute RIP routes learned via the RIP routing protocol. ● On: Redistribute RIP routes learned via the RIP routing protocol.
Redistribute BGP routes	<ul style="list-style-type: none"> ● 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.

The screenshot displays the OSPF configuration page. At the top, there are tabs for 'General', 'Interfaces', and 'Networks'. Below the tabs is a 'Summary' table with columns: #, Name, Interface, Authentication, Key, Key ID, Cost, Passive, Edit, and Delete. The table contains one entry with #1, Name 'ospf', Interface 'eth1', Authentication 'null', Key '-', Key ID '-', Cost '0', and Passive 'off'. Below the table is the 'Add/Edit' form for an OSPF interface. The form includes fields for Name (radio buttons for Off/On), Interface (dropdown menu), Authentication (dropdown menu), Key (text input), Key ID (text input), Cost (text input), and Passive (radio buttons for Off/On). Each input field has a corresponding tooltip explaining its function. For example, the Key field tooltip says 'The key used for authentication (maxlength 16)'. The Key ID tooltip says 'The ID of the key used for authentication (1-255)'. The Cost tooltip says 'The cost for sending packets via the interface (0-OSPF default)'. The Passive tooltip says 'Do not send out OSPF packets on this interface'. There is an 'Add' button at the bottom of the form.

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

(3) Networks Configuration

There are 2 parts for OSPF Networks configuration.

- OSPF Networks Summary

You can edit and delete the existed OSPF networks.

- OSPF Networks Add/Edit

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

The screenshot displays the OSPF Networks configuration page. At the top, there are tabs for 'General', 'Interfaces', and 'Networks'. Below the tabs is a 'Summary' table:

ID	Mode	Prefix	Prefix Length	Area	Edit	Delete
1	On	192.168.1.1	24	0		

Below the summary table is the 'Add/Edit' form for an OSPF Network. It includes the following fields:

- Mode:** Radio buttons for 'Off' and 'On'.
- Prefix:** Text input field containing '192.168.1.1'.
- Prefix Length:** Text input field containing '24'.
- Area:** Text input field containing '0'.

At the bottom right of the form is an 'Apply' button.

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

10.4 IP Routing > BGP

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

(1) General Configuration

The screenshot shows the BGP General Configuration page. It includes the following settings:

- Mode:** Radio buttons for Off and On.
- AS Number:** Input field containing '1'. Description: The number of the autonomous system (1 ~ 4294967295).
- Redistribute local routes:** Radio buttons for Off and On. Description: from the device's own routing table.
- Redistribute connected routes:** Radio buttons for Off and On. Description: to networks which are directly connected to the device.
- Redistribute RIP routes:** Radio buttons for Off and On. Description: learned via the RIP routing protocol.
- Redistribute OSPF routes:** Radio buttons for Off and On. Description: learned via the OSPF routing protocol.

An 'Apply' button is located at the bottom right of the configuration area.

IP Routing > BGP > General	
Item	Description
General	
Mode	<ul style="list-style-type: none"> ● Off: BGP function is off. ● On: BGP function is on.
AS Number	The number of the autonomous system (1 ~ 4294967295)
Redistribute local routes	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● Off: Not redistribute RIP routes learned via the RIP routing protocol. ● On: Redistribute RIP routes learned via the RIP routing protocol.
Redistribute OSPF routes	<ul style="list-style-type: none"> ● Off: Not redistribute OSPF routes learned via the OSPF routing protocol. ● On: Redistribute OSPF routes learned via the OSPF routing protocol.

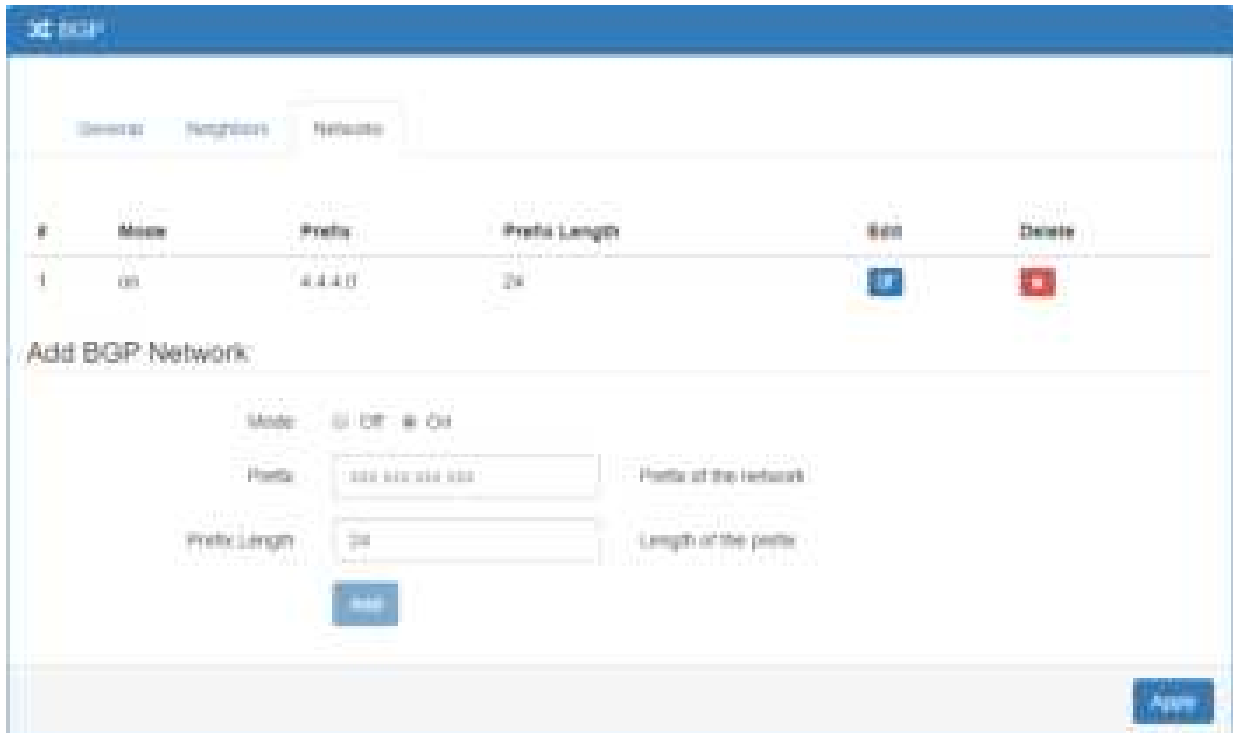
(2) Neighbor Configuration

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

IP Routing > BGP > Neighbors	
Item	Description
Mode	Select from Off or On to enable the neighbor setting.
IP Address	Set IP address of the peer router.
AS Number	Autonomous system number of the peer router.
Multihop	Allow multiple hops between this router and the peer router.
Update Source Mode	Whether to specify the source address to this neighbor.
Update Source Address	The source address to this neighbor.

(3) Networks Configuration


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



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

11 Configuration > VPN

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

VPN 

Open VPN

IPSec


GRE


PPTP Server




L2TP











11.1 VPN > Open VPN


11.1.1 Open VPN Common Setting

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

Open VPN 

Mode  Detail  Add 

ID	Mode	VPN Mode	Enabled	Protocol	Port	PSK	edit
1	ENABLE	COMF	ON	UDP	1194		
2	ENABLE	COMF	ON	UDP	1194		
3	ENABLE	COMF	ON	UDP	1194		
4	ENABLE	COMF	ON	UDP	1194		
5	ENABLE	COMF	ON	UDP	1194		
6	ENABLE	COMF	ON	UDP	1194		
7	ENABLE	COMF	ON	UDP	1194		
8	ENABLE	COMF	ON	UDP	1194		
9	ENABLE	COMF	ON	UDP	1194		
10	ENABLE	COMF	ON	UDP	1194		



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

The screenshot shows the 'Edit Open VPN Connection #1' interface with the 'Setting' tab selected. The configuration options are as follows:

- Mode:** Disable Enable
- VPN Mode:** Server Client Custom
- VPN Type:** Roadwarrior Bridging
- Status:** Idle
- TLS Mode:** Disable Enable
- Cipher:** BF-CBC
- IPV6 Mode:** Disable Enable
- Device:** TUN TAP
- Protocol:** UDP TCP
- Port:** 1191
- VPN Compression:** Disable Enable
- Authentication:** Certificate

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

The screenshot shows the 'Edit Open VPN Connection #1' interface with the 'Log' tab selected. The log area is currently empty, and there are 'Back' and 'Refresh' buttons at the bottom right.

VPN > Open VPN > Setting	
Item	Description
Mode	Turn on/off Open VPN to select Disable or Enable.
VPN Mode	<ul style="list-style-type: none"> • Server: Tick to enable Open VPN server tunnel. • Client: Tick to enable Open VPN client tunnel. The default is Client. • Custom: This option allows user to use the .ovpn configuration file to quickly set up VPN tunnel with third-party server or use the Open VPN advanced options to be compatible with other servers.

VPN Type	<ul style="list-style-type: none"> • Roadwarrior (default) • Bridging: Bridging the VPN tunnel and LAN/VLAN
Status	Display the status of Open VPN.
TLS Mode	Select from Disable or Enable for data security. The default is Disable.
Cipher	The Open VPN format of data transmission.
IPv6 Mode	Select from Disable or Enable. The default is Disable.
Device	Select from TUN or TAP. The default is TUN.
Protocol	Select from UDP or TCP Client which depends on the application. The default is UDP.
Port	Enter the listening port of remote side Open VPN server.
VPN Compression	Select Disable or Enable to compress the data stream. The default is Disable.
Authentication	<ul style="list-style-type: none"> • Select from two different kinds of authentication ways: Certificate or pkcs#12 Certificate. • The pkcs#12 option is only available on the VPN client mode.

11.1.2 Open VPN Client Setting

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

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

VPN > Open VPN > Client VPN Mode	
Item	Description
Client	
Server Address	Fill in WAN IP of Open VPN server.
Route Client Networks	Select from Off or On. This setting needs to match the server side. When enabled, the cellular router will auto apply the properly routing rules.
NAT	
1:1 NAT	<ul style="list-style-type: none"> • Tick to enable NAT Traversal for Open VPN. This item must be enabled when the router under NAT environment. • Select from Off or On. • When two routers' LAN Subnet are same and create Open VPN tunnels, this function should be turned on.
Client-Security	
Root CA	The Certificate Authority file of Open VPN server could be downloaded from Open VPN server.
Cert	The certification file is for Open VPN client, which could be downloaded from Open VPN server.
Key	The private key file is for Open VPN client, which could be downloaded from Open VPN server.
P12	The PKCS#12 file is for Open VPN client, which could be downloaded from Open VPN server.

11.1.3 Open VPN Server Setting

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

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

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

The screenshot shows the configuration interface for an Open VPN Server. It is organized into several sections:

- Server:** Contains two input fields for "VPN Password" and "VPN Username", both currently set to "0000".
- RoadWarrior:** Features a "Route Client Networks" toggle set to "On". Below it is a "Connections (IP / MASK)" table with 8 rows, each containing two input fields for IP and Mask, all set to "0.0.0.0".
- NAT:** Includes a "NAT" toggle set to "Off".
- Server - Server Security:** Contains two buttons: "Add CA" and "Get Key".
- Server - User Security:** Lists 8 users (User 1 to User 8). Each user entry includes a "Yes" status, a "Add" button, and an "Assigned to users" field.





At the bottom of the page, there are three buttons: "Save", "Cancel", and "Apply".

VPN > Open VPN > Server VPN Mode	
Item	Description
Server	
VPN Network	The network ID for Open VPN virtual network.
VPN Netmask	The netmask for Open VPN virtual network.
Roadwarrior: Route Client Networks	Select from Off or On. The Open VPN server will route the client traffic or not. User should fill in the client IP and netmask when this option is enabled.
NAT	
1:1 NAT	<ul style="list-style-type: none"> • Tick to enable NAT Traversal for Open VPN. This item must be enabled when router under NAT environment. • Select from Off or On. The default is Off. • When two routers' LAN Subnet are same and create Open VPN tunnels, this function is turned on.
Server- Server Security	
Root CA	Create Root CA key.
Cert, Key and DH	Create Cert, Key and DH key.
Server- User Security	
User 1 - User 8	According to your requirement, you can create different kinds of user security key from User 1 to User 8.

11.1.4 Set up Open VPN Custom

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

Note:

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

Edit Open VPN Connection #1

Setting Log

Mode Disable Enable

VPN Mode Server Client Custom

Custom Config

Username

Password

Status Idle

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

11.2 VPN > IPsec

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

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

Mode Disable Enable

Type Policy based Route based

VPN > IPsec > General setting	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
Type	Select from Policy-based or Route-based. The default is Policy-based. <ul style="list-style-type: none"> ● Policy-based: transmit traffic that meet the IPsec phase 2 local/remote subnet. ● Route-based: transmit traffic that match routing table.

11.2.1 IPsec > Connections

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

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

The screenshot displays the IPsec configuration page. At the top, there are radio buttons for 'Mode' (Disable, Enable) and 'Type' (Policy-based, Route-based). Below this are four tabs: 'Connections', 'Authentication IDs', 'X.509 Certificates', and 'CA Certificates'. The 'Connections' tab is active, showing a legend of connection states: IPsec SA active and link up (green), Only IPsec SA active (orange), Connecting (yellow), IPsec SA inactive (red), and Disabled (grey). To the right of the legend are three buttons: 'Phase 1' (blue), 'Phase 2' (green), and 'Advanced' (grey). Below the legend is a table with columns for Name, State, IKE information, and Tunnel information. One connection is listed with Name '1' and State 'On'. At the bottom of the table are buttons for 'Phase 1', 'Phase 2', and 'Advanced'. Below the table is a '+ Add Connection' button. At the very bottom right is an 'Apply' button.

(1) IPsec Phase 1 Setting

Configure IPsec Phase 1

Mode	<input type="text" value="Disable"/>
Name	<input type="text" value=""/>
Protocol	<input type="text" value="IKEv1"/>
Aggressive mode	<input type="text" value="Disable"/>
Auth Type	<input type="text" value="PSK"/>
Encryption	<input type="text" value="AES128"/>
Hash	<input type="text" value="SHA1"/>
DH Group	<input type="text" value="1(768 bit)"/>
Lifetime	<input type="text" value="30 minutes"/>
Local ID	<input type="text" value="192.168.1.100"/>
Remote ID	<input type="text" value=""/>
Remote IP	<input type="text" value="192.168.1.100"/>

OK
Cancel

VPN > IPsec > Connections > Phrase 1 setting	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
Name	Short name or description.
Protocol	Select from IKEv1 or IKEv2. The default is IKEv1.
Aggressive mode	Select from Disable or Enable. The default is Disable. When this option be enabled, the connection will be running on IKEv1 Aggressive mode. (Note: This option only work on IKEv1.)
Auth Type	Select from PSK (default), RSA, EAP-TLS. (Note: The EAP-TLS is for IKEv2 only.)
Encryption	The encryption algorithm. Select from AES128 (default), AES192, AES256 or 3DES.
Hash	The integrity algorithm. Select from MD5, SHA1 (default) or SHA256.
DH Group	The Diffie Hellman Group. Select from 1(768 bit), 2(1024 bit), 5(1536 bit) (default), 14(2048 bit), 15(3072 bit), 16(4096 bit), 17(6144 bit) or 18(8192 bit).
Lifetime	The length of the keying channel of a connection. Select from 30 minutes, 1 hour, 2 hours, 3 hours, 6 hours, 12 hours or 24 hours.

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

(2)IPsec Phase 2 Setting

Configure IPsec Phase 2

Protocol	<input type="text" value="ESP"/>
Encryption	<input type="text" value="AES128"/>
Hash	<input type="text" value="SHA1"/>
Diffie Hellman	<input type="text" value="5(1536 bit)"/>
Lifetime	<input type="text" value="3 hours"/>
Local Subnet	<input type="text"/>
Remote Subnet	<input type="text"/>
Priority	<input type="text" value="40"/>

Back
Save

VPN > IPsec > Connections > Phrase 2 setting	
Item	Description
Protocol	Only support ESP.
Encryption	The encryption algorithm. Select from AES128 (default), AES192, AES256 or 3DES.
Hash	The integrity algorithm. Select from MD5, SHA1 (default) or SHA256.
DH Group	The Diffie Hellman Group. Select from 1(768 bit), 2(1024 bit), 5(1536 bit) (default), 14(2048 bit), 15(3072 bit), 16(4096 bit), 17(6144 bit) or 18(8192 bit).
Lifetime	The length of a particular instance of a connection. Select from 30 minutes, 1 hour, 2 hours, 3 hours, 6 hours, 12 hours or 24 hours.
Local Subnet	The private subnet behind the router. The available formats are A.B.C.D, A.B.C.D/M, A.B::C.D or A.B::C.D/M If this value is blank, the connection will set it as the "Local Host" of Phase 1 setting.

	<p>Note:</p> <p>(1) This option only work on Policy-based IPsec VPN type.</p> <p>(2) This option will be setup as 0.0.0.0/0 automatically on IPsec Route-based VPN.</p> <p>(3) This option will be omitted when the service option is L2TP. (For host-to-host connection only)</p>
Remote Subnet	<p>The private subnet behind the peer gateway. The available formats are A.B.C.D, A.B.C.D/M, A.B::C.D or A.B::C.D/M If this value is blank, the connection will set it as the `Remote Host` of Phase 1 setting.</p> <p>Note:</p> <p>(1) This option only work on Policy-based IPsec VPN type.</p> <p>(2) This option will be setup as 0.0.0.0/0 automatically on IPsec Route-based VPN.</p> <p>(3) This option will be omitted when the service option is L2TP. (for host-to-host connection only)</p>
Service	<p>Restrict the VPN traffic to the particular protocol only. Select from the Any, TCP, UDP or L2TP.</p>

(3) IPsec Advance Setting

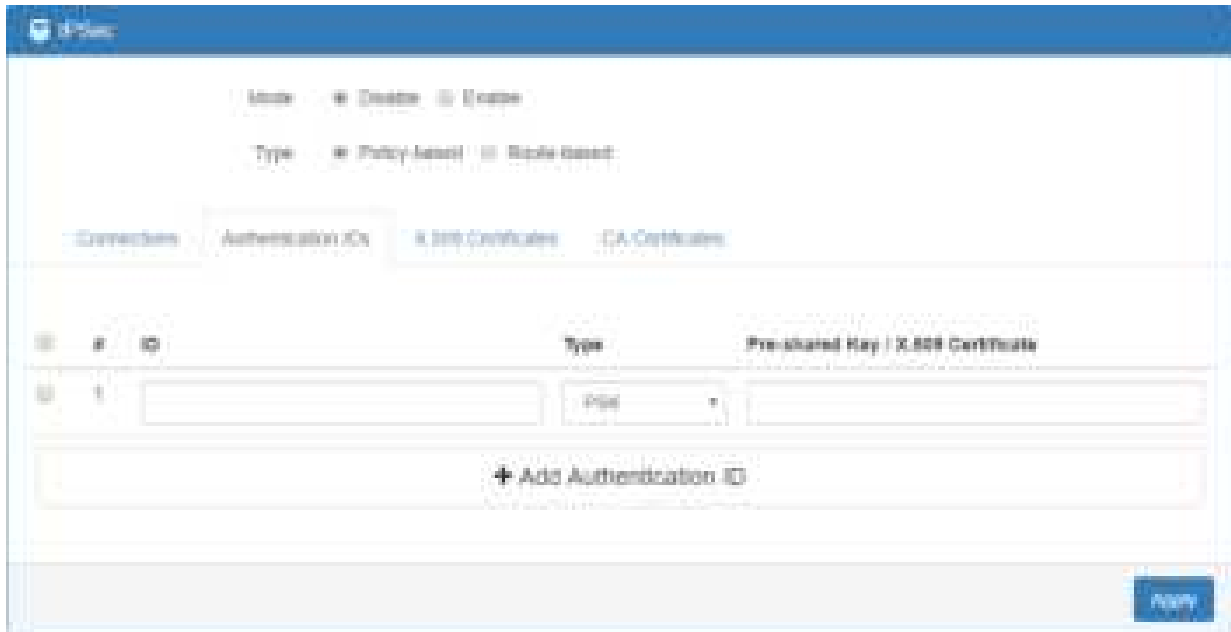
VPN > IPsec > Connections > Advance Setting	
Item	Description
DPD interval	The period time interval to detect dead peers. The default is 30 seconds.
DPD retry	The max number of retry of dead peer detection. The default is 5 times.

11.2.2 IPsec > Authentication IDs

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

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

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



VPN > IPsec > Authentication IDs	
Item	Description
ID	The identification for authentication. It only work on PSK type.
Type	Select from PSK or RSA. The default is PSK. <ul style="list-style-type: none"> ● PSK: Use the pre-shared key to authenticate the connection. ● RSA: Use the certificate to authenticate the connection.
Pre-shared Key / X.509 Certificate	The X.509 certificate for authentication. The certificate could be generated or imported by X.509 Certificates section.

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

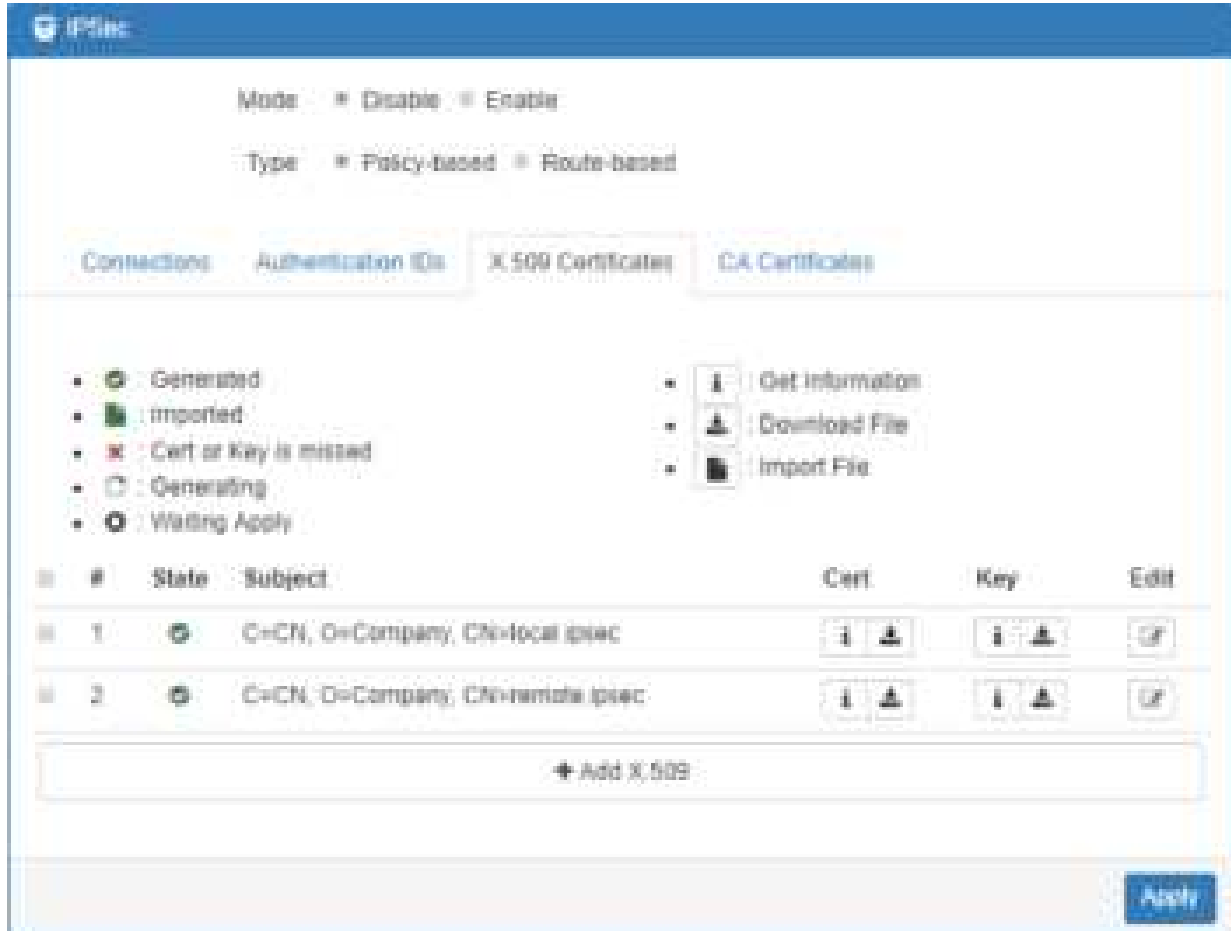
VPN > IPsec > Authentication IDs				
#	ID	Type	Pre-shared Key / X.509 Certificate	Comment
1		PSK	password	The default password for the PSK connections.
2	remote.IPsec	PSK	2wsx#EDC	The password only for the PSK connection with remote.IPsec ID. Normally, this case will be used to authenticate peer gateway.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

11.2.3 IPsec > X.509 Certificates

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

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

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

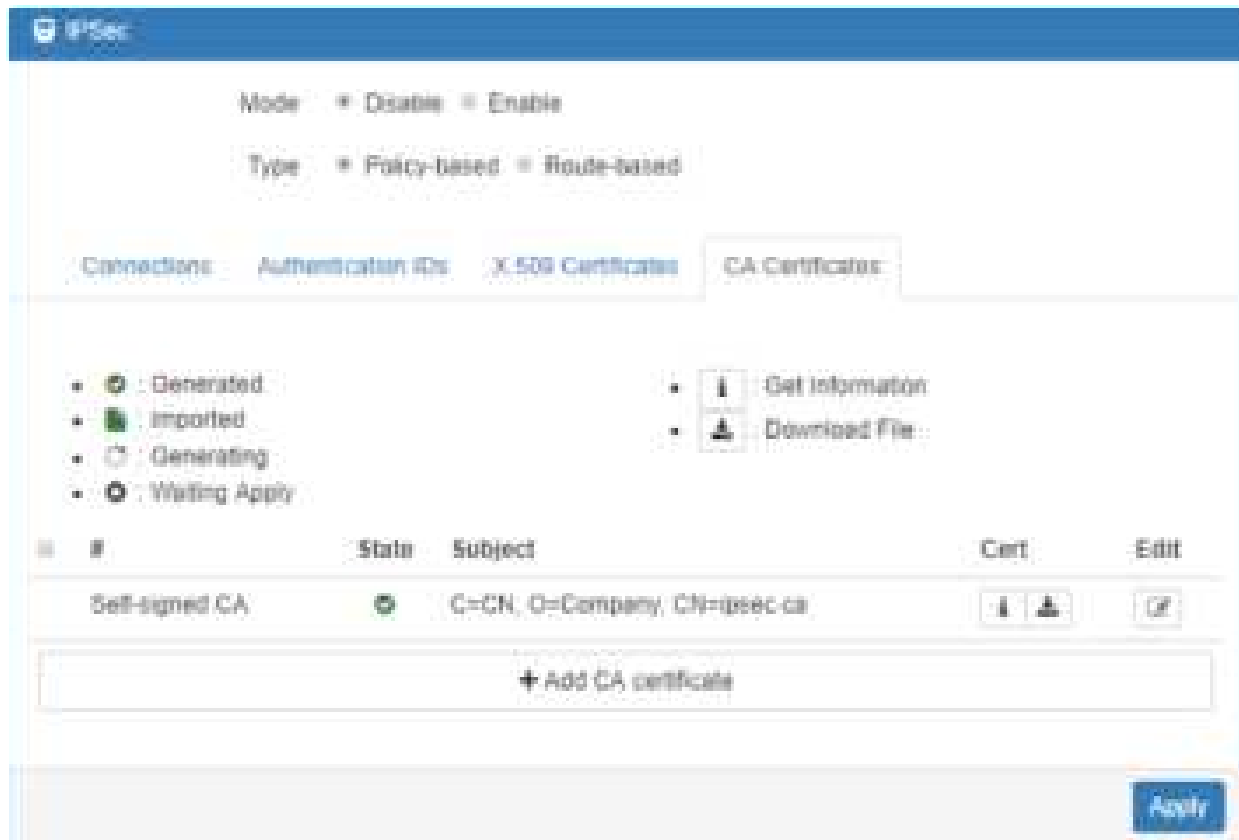


11.2.4 IPsec > CA Certificates

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

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


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



Certificate Generation

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

To generate the self-signed CA certificate:

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

To generate the X.509 certificate:

1. Make sure the self-signed CA certificate generated.
2. Navigate to [X.509 Certificates](#) tab.
3. Add the new X.509 certificate by [+ Add X.509](#) button. (If it's not existed.)
4. Click the Edit button to navigate the **Certificate Setting** page.
5. Fill up the informations of the X.509 certificate.
6. Click the [Generate Certificate](#) button and [Save](#).
7. Click the [Apply](#) button to apply the changes.

Certificate Setting

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

Configure CA Certificate

Country Name (C)	<input type="text"/>
State (ST)	<input type="text"/>
Location (L)	<input type="text"/>
Organization Name (O)	<input type="text"/>
Organization Unit Name (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
E-mail	<input type="text"/>
<input type="button" value="Generate Certificate"/>	

Certificate Importing

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

To import the CA certificate:

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

To import the X.509 certificate:

1. Navigate to [X.509 Certificates](#) tab.

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

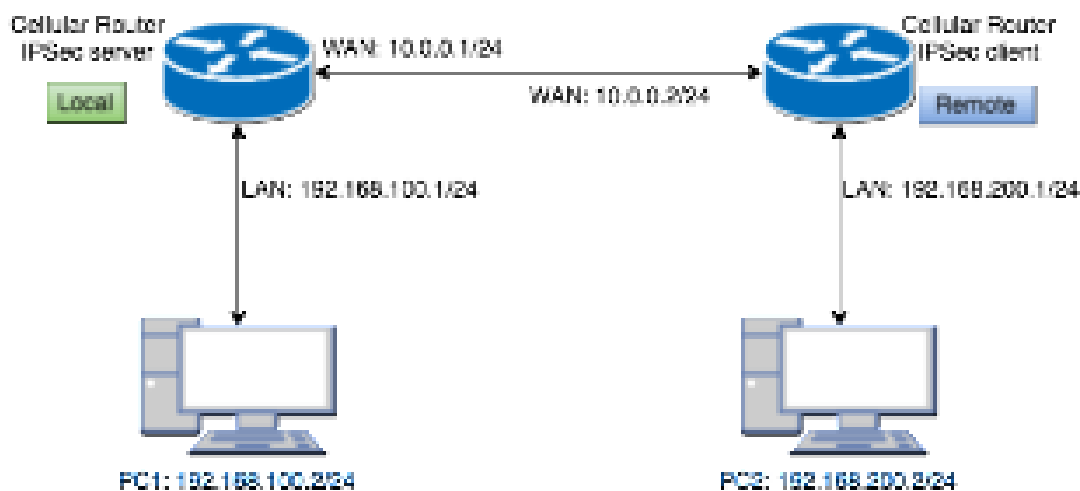
How to download the certificate

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

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

11.2.5 IPsec > Net-to-Net Configuration

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



- **Pre-shared Key authentication**

Configure Net-to-Net VPN Server

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

5. Navigate to the [Connections](#) tab.

6. Add IPsec connection

(1) Edit the phase 1 setting

(2) Change **Mode** from Disable to **Enable**.

(3) Save the changes.

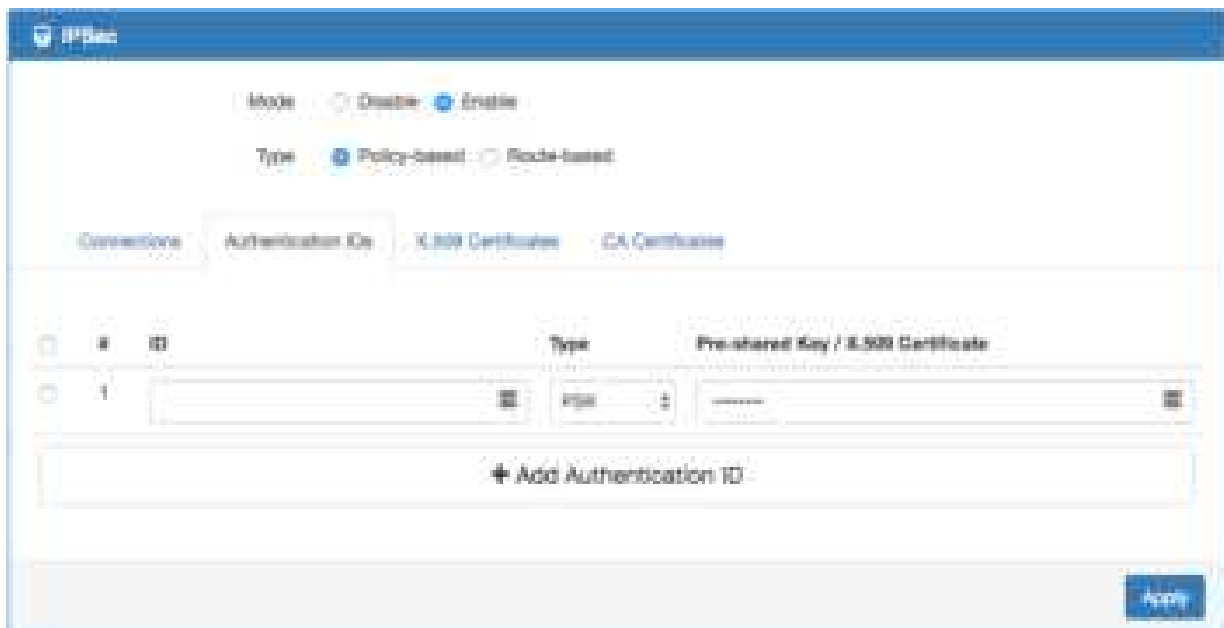
(4) Edit the phase 2 setting

(5) Fill up the **Local Subnet** and **Remote Subnet**.

- e.g. Local Subnet: 192.168.100.0/24, Remote Subnet: 192.168.200.0/24

(6) Save the changes

7. Apply the changes



Connection #1 Phase 1

Mode Disable Enable

Name:

Protocol: IKEv1

Aggressive mode: Disable

Auth Type: PSK

Encryption: AES128

Hash: SHA1

DH Group: 0 (1024 bit)

Lifetime: 1 hour

Local Host:

Local ID: empty (allow any)

Remote Host:

Remote ID: empty (allow any)

Connection #1 Phase 2

Protocol: ESP

Encryption: AES128

Hash: SHA1

DH Group: 0 (1024 bit)

Lifetime: 1 hour

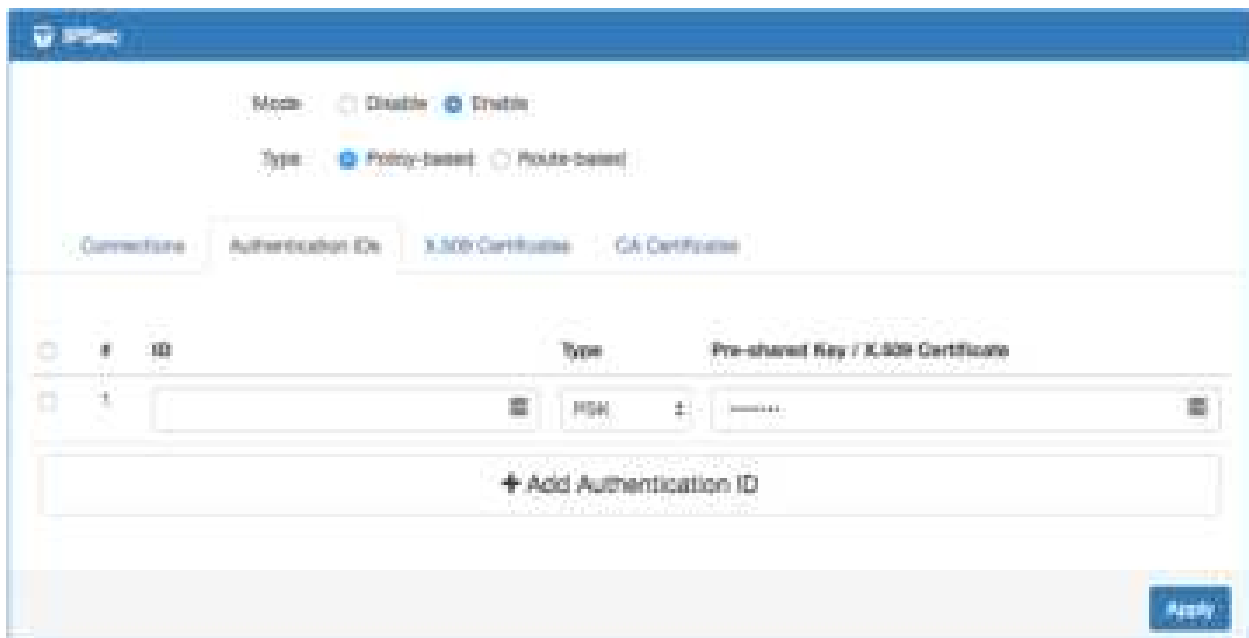
Local Subnet: 192.168.100.0/24

Remote Subnet: 192.168.200.0/24

Service: Any

Configure Net-to-Net VPN Client

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



Connection #1 Phase 1

Mode Dynamic Static

Name

Protocol

Aggressive mode

Auth Type

Encryption

Hash

DH Group

Lifetime

Local Host

Local ID

Remote Host

Remote ID

Connection #1 Phase 2

Protocol

Encryption

Hash

DH Group

Lifetime

Local Subnet

Remote Subnet

Service

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

- Server



- Client



- **RSA authentication - Server**

Prepare the self-signed CA certificate

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

Configure X.509 Certificate:

Country Name (C)	<input type="text"/>
State (ST)	<input type="text"/>
Locality (L)	<input type="text"/>
Organization Name (O)	<input type="text"/>
Organization Unit Name (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Private Key (PK)	<input type="text"/>
<input type="button" value="Generate Certificate"/>	

Prepare the X.509 certificates

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

3.500 Certificate

Country Name (C)

State (ST)

Common Name (CN)

Organization Name (O)

Organization Unit Name (OU)

Common Name (CN)

Serial

Generate Certificate

Back

Save

3.510 Certificate

Country Name (C)

State (ST)

Common Name (CN)

Organization Name (O)

Organization Unit Name (OU)

Common Name (CN)

Serial

Generate Certificate

Back

Save

IPSec

Mode: Disable Enable

Type: Policy-based Route-based

Connections Authentication Da X.509 Certificates CA Certificates

- Generated
- Imported
- Cert or Key is missing
- Generating
- Waiting Apply

- Get Information
- Download File
- Import File

#	State	Subject	Cert	Key	Edit
1	Generated	C=CN, O=Company, DN=local.psec			IP
2	Generated	C=CN, O=Company, DN=remote.psec			IP

+ Add X.509

Apply

IPSec

Mode: Disable Enable

Type: Policy-based Route-based

Connections Authentication Da X.509 Certificates CA Certificates

- Generated
- Imported
- Cert or Key is missing
- Generating
- Waiting Apply

- Get Information
- Download File
- Import File

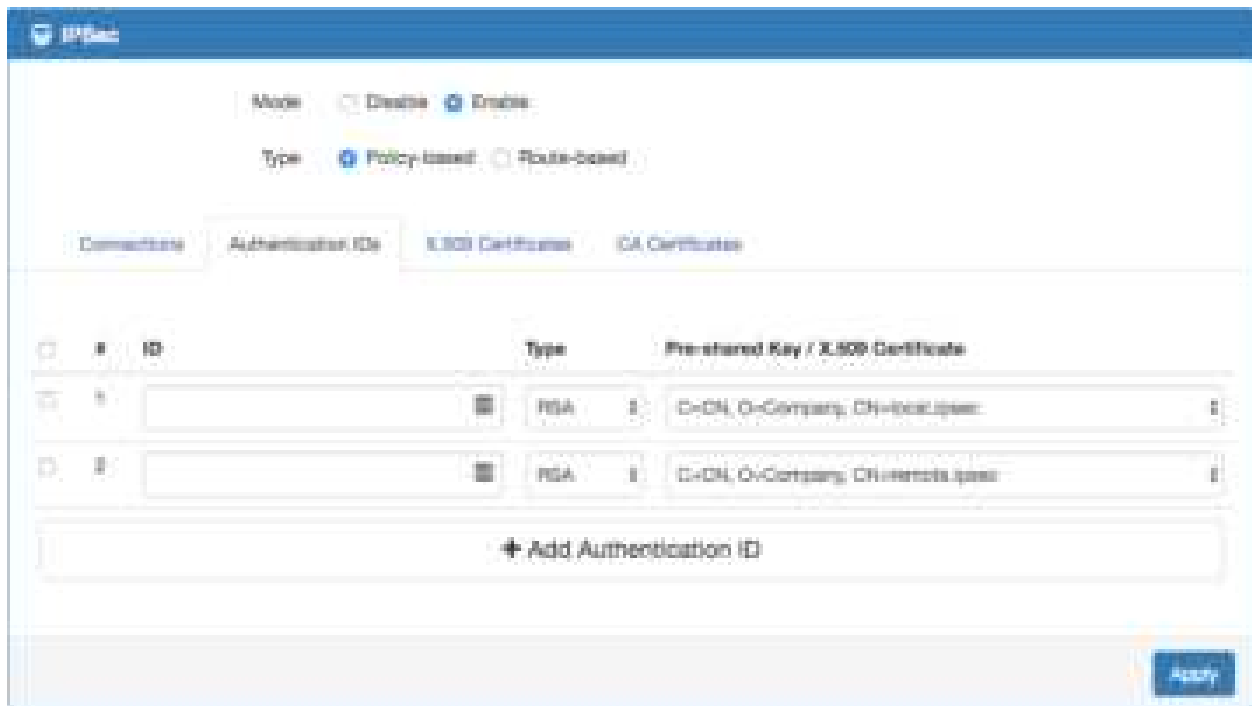
#	State	Subject	Cert	Key	Edit
1	Generated	C=CN, O=Company, CN=local.psec	Get Information Download File	Get Information Download File	IP
2	Generated	C=CN, O=Company, CN=remote.psec	Get Information Download File	Get Information Download File	IP

+ Add X.509

Apply

Prepare the authentication IDs

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



Setup the connection on VPN server

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

Connection #1 Phase 1

Mode	<input type="checkbox"/> Disable <input checked="" type="checkbox"/> Enable
Name	<input type="text"/>
Protocol	IPsec
Aggressive mode	Disable
Auth Type	PSA
Encryption	AES128
Hash	SHA1
Diff Group	1 (1024 bit)
Lifetime	1 hour
Local Host	<input type="text"/>
Local ID	0x1 local (peer) (PSA)
Remote Host	<input type="text"/>
Remote ID	remote (show any)

Connection #1 Phase 2

IPsec ID	1001
Display	AES128
Hash	SHA1
Diff Group	1 (1024 bit)
Lifetime	1 hour
Local ID	0x1 local (peer)
Remote ID	remote (show any)
Curve	Agp

● RSA authentication – Client

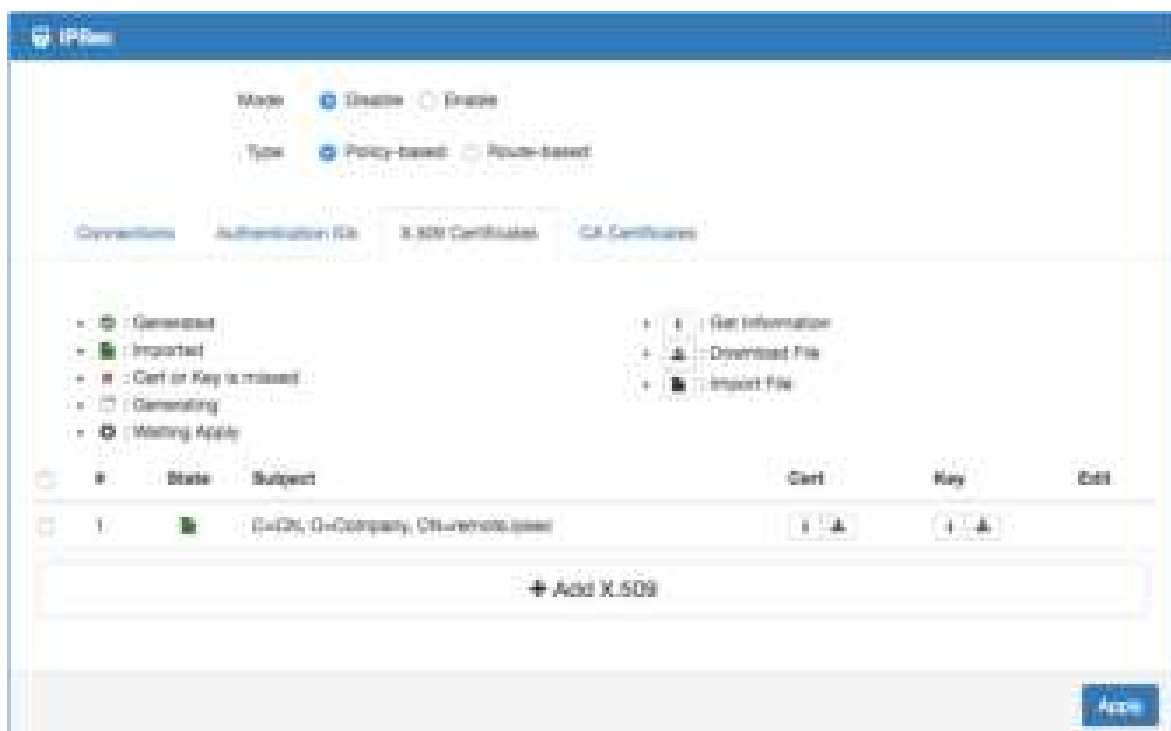
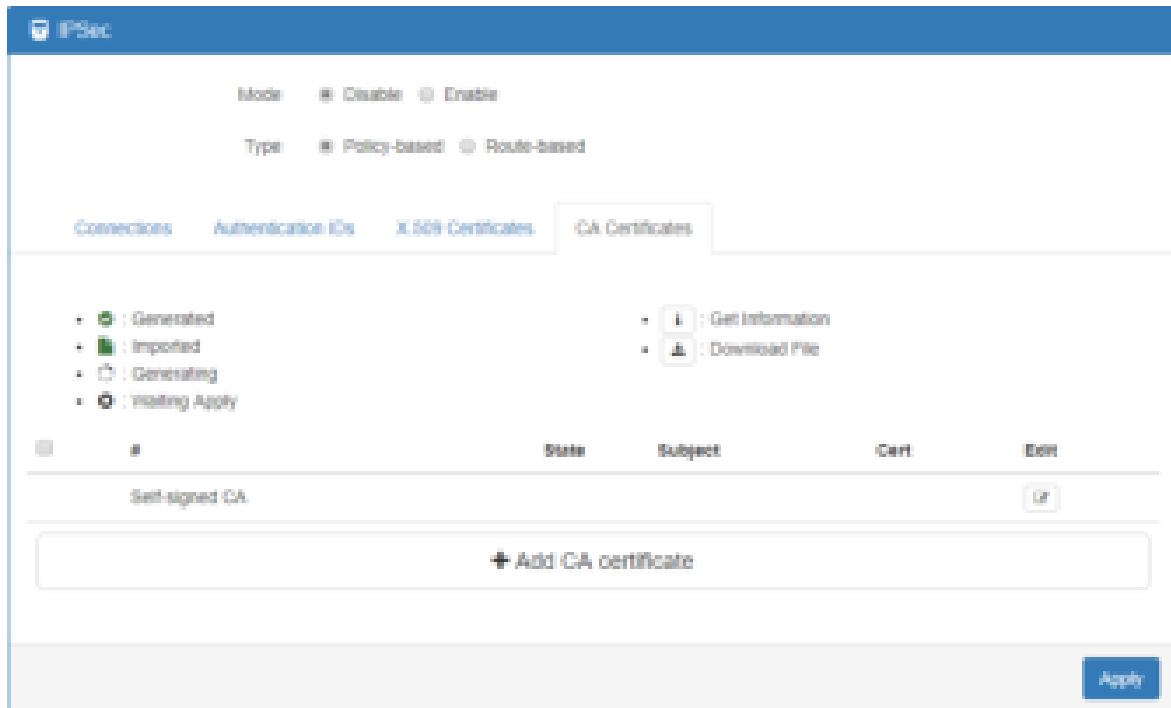
Prerequisite for VPN Client with RSA authentication

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

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

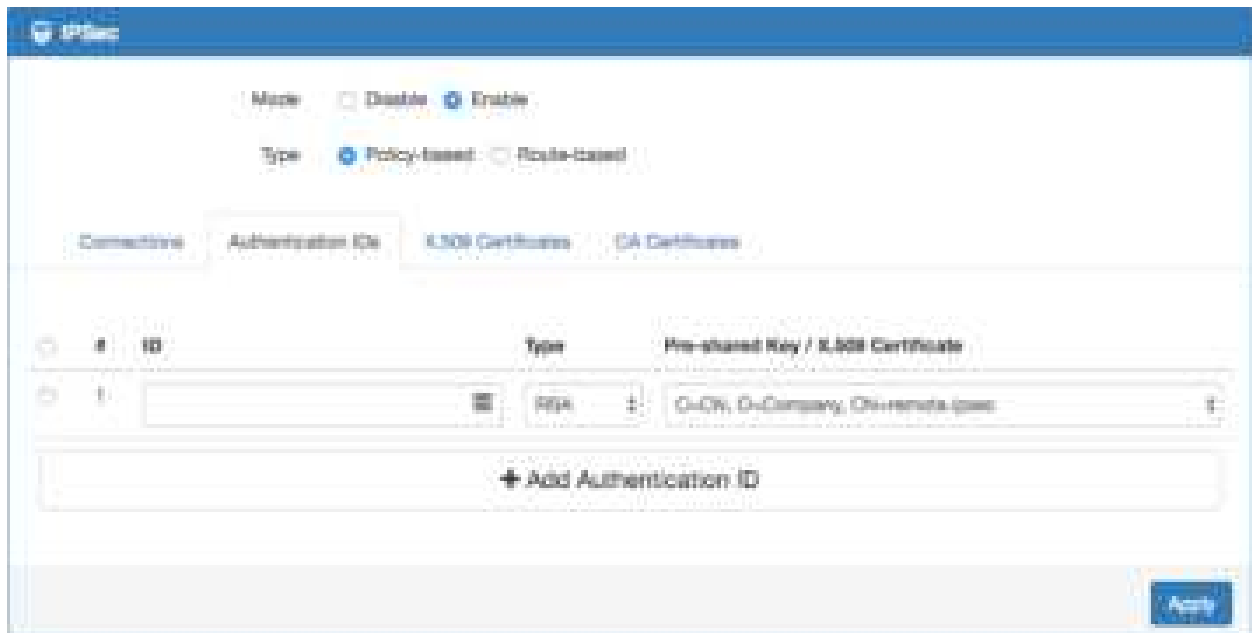
Import the CA certificate and the X.509 certificate

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



Setup the connection on VPN client

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



Connection #1 Phase 1

Mode: Disable Enable

Name:

Protocol: IKEv1

Aggressive mode: Disable

Auth Type: RSA

Encryption: AES128

Hash: SHA3

DH Group: 8 (2048 bit)

Lifetime: 3 hours

Local Host:

Local ID: CA1 (remote peer ID)

Remote Host: 10.0.0.1

Remote ID: (empty - allow any)

Connection #1 Phase 2

Proposal: #1

Encryption: AES128

Hash: SHA3

DH Group: 8 (2048 bit)

Lifetime: 3 hours

Local ID: 10.10.10.1/24

Remote ID: 10.10.10.1/24

Diffie: Any

● IPsec Net-to-Net with RSA authentication result

• Server

Connections | Authentication CA | IKE Certificates | CA Certificates

- IPsec SA active and link up
- Only IPsec SA active
- Connecting
- IPsec SA inactive
- Disabled
- Edit Phase 1
- Edit Phase 2
- Edit IPsec Advance setting

#	Name	State	IKE information	Tunnel information
1	rsa	IPsec SA active and link up	IKEv1 : 10.0.0.1 (local-peer) ... 10.0.0.3 (remote-peer)	192.168.100.0/24 ... 192.168.200.0/24

+ Add Connection

• Client

Connections | Authentication CA | IKE Certificates | CA Certificates

- IPsec SA active and link up
- Only IPsec SA active
- Connecting
- IPsec SA inactive
- Disabled
- Edit Phase 1
- Edit Phase 2
- Edit IPsec Advance setting

#	Name	State	IKE information	Tunnel information
1	rsa	IPsec SA active and link up	IKEv1 : 10.0.0.2 (remote-peer) ... 10.0.0.1 (local-peer)	192.168.200.0/24 ... 192.168.100.0/24

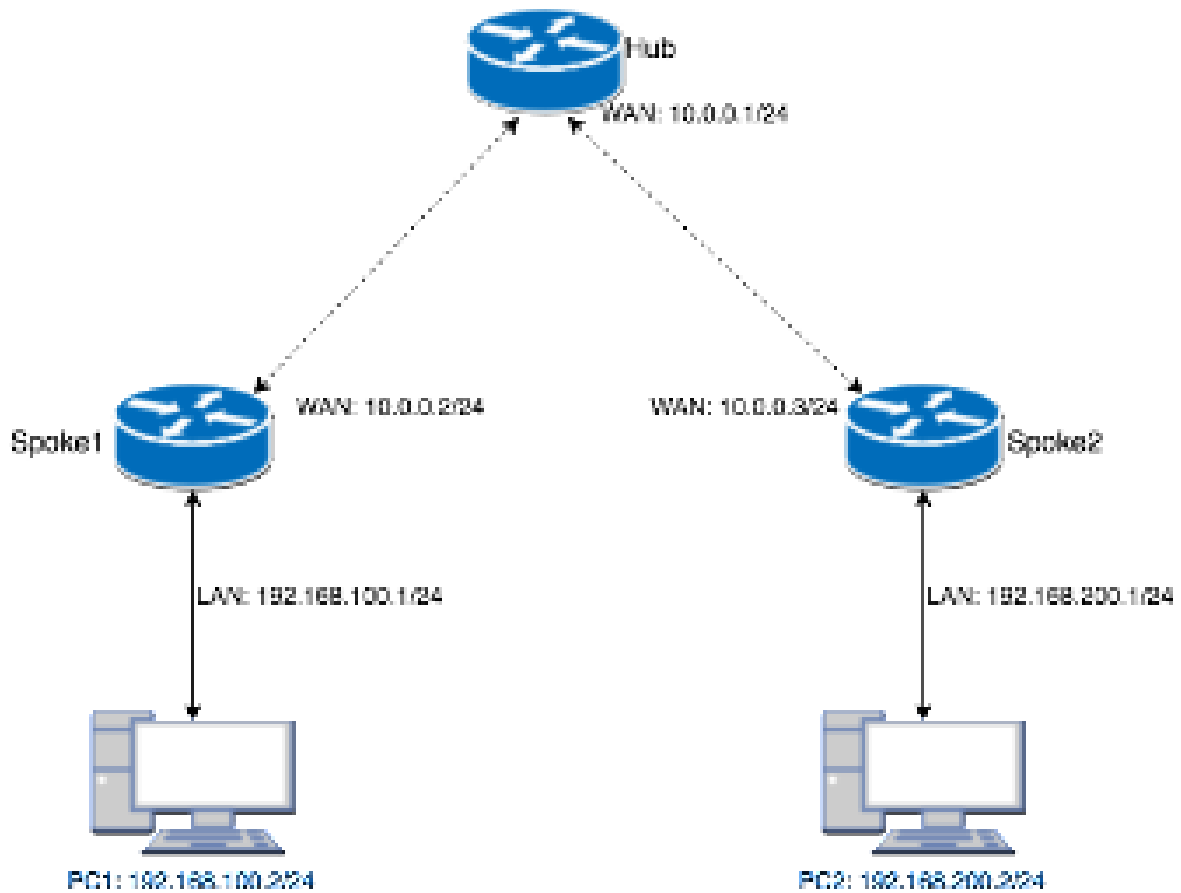
+ Add Connection

11.2.6 IPsec > Hub-Spoke Topology

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

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

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



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

- **Hub configuration**

Hub IPsec configuration

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

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

IPSec

Mode Disable Enable

Type Policy-based Route-based

Connections Authentication IDs X.509 Certificates CA Certificates

ID	Type	Pre-shared Key / X.509 Certificate
1	PSK	*****
2	PSK	*****
3	PSK	*****

[+ Add Authentication ID](#)

[Apply](#)

Connection #1 Phase 1

Mode Disable Enable

Name

Protocol

Aggressive mode

Auth-Type

Encryption

Hash

DH Group

Lifetime

Local Host

Local ID

Remote Host

Remote ID

[Back](#) [Save](#)

Connection #1 Phase 1

Protocol	ESP
Encryption	AES128
Hash	SHA1
DPV Group	5 (128Kbps)
Lifetime	1 hour
Service	Any

Back Next

Connection #1 Phase 2

Mode Disable Enable

Name

Protocol	IPSec
Aggressive mode	Disable
Auth type	PSK
Encryption	AES128
Hash	SHA1
DPV Group	5 (128Kbps)
Lifetime	8 hours
Local Host	
Local ID	company@192.168.1.1
Remote Host	
Remote ID	192.168.1.1@192.168.1.1

Back Next

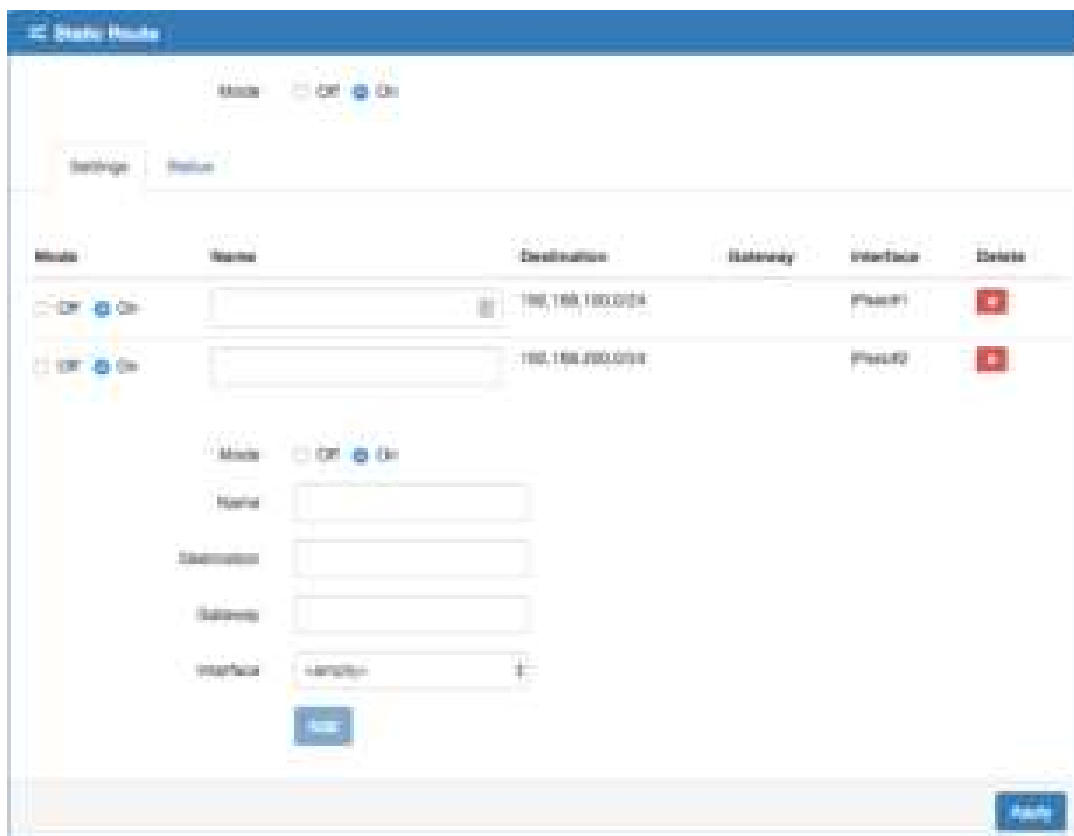
Connection #1 Phase 3

Protocol	ESP
Encryption	AES128
Hash	SHA1
DPV Group	5 (128Kbps)
Lifetime	8 hours
Service	Any

Back Next

• Hub Static Route configuration

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



• Spoke 1 configuration

Spoke 1 IPsec configuration

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

The screenshot shows the IPsec configuration interface. At the top, there are radio buttons for Mode (Disable, Enable) and Type (Policy-based, Route-based). Below this are tabs for Connections, Authentication IDs, IKE Certificates, and CA Certificates. The Authentication IDs tab is active, showing a table with columns for ID, Type, and Pre-shared Key / IKE Certificate. There are two entries: one with ID '1' and another with ID 'spoke1'. Below the table is a button to '+ Add Authentication ID'. At the bottom right, there is an 'Apply' button.

ID	Type	Pre-shared Key / IKE Certificate
1	PSK	defaultpsk
spoke1	PSK	testspoke1

Mode	<input type="radio"/> Profile 1 <input checked="" type="radio"/> Profile 2 <input type="radio"/> Profile 3
Name	<input type="text"/>
Protocol	<input type="text" value="TCP"/>
Application	<input type="text" value="HTTP"/>
URL type	<input type="text" value="URL"/>
Endpoint	<input type="text" value="HTTP/1.1"/>
URI	<input type="text" value="/*"/>
URI type	<input type="text" value="URI (HTTP)"/>
URI filter	<input type="text" value="/*"/>
IP filter	<input type="text"/>
Port filter	<input type="text" value="HTTP (80)"/>
Timeout	<input type="text" value="10.00"/>
Header	<input type="text" value="Accept: */*"/>

Spoke 1 Static Route configuration

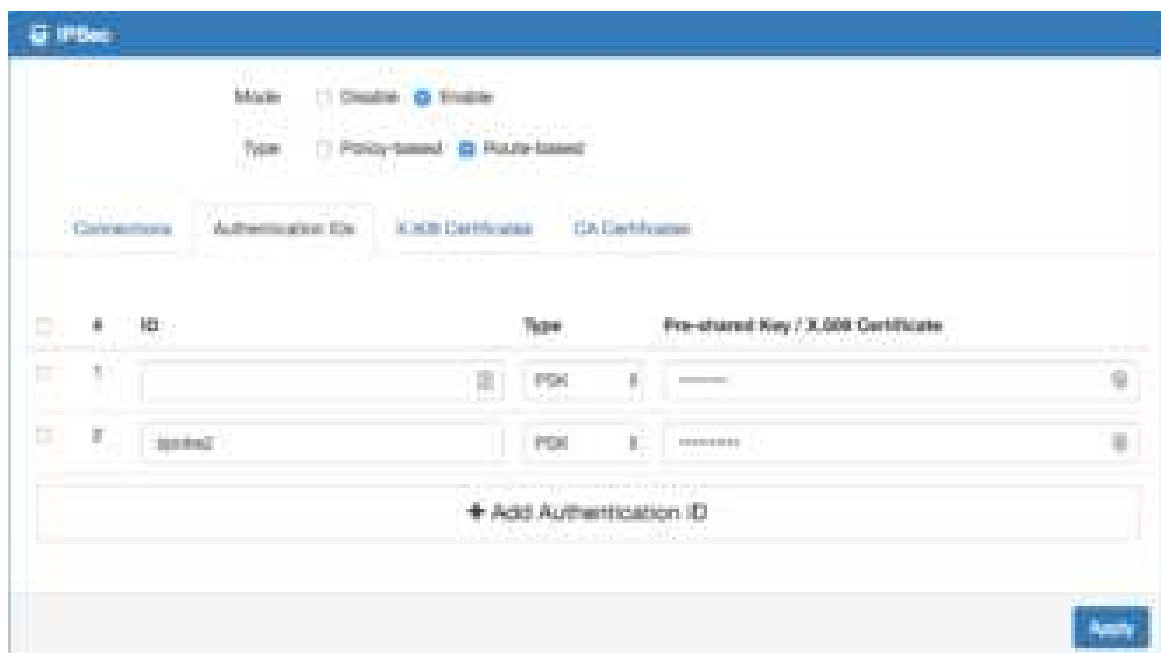
1. Navigate to the **IP Routing > Static Route** page
2. Add the static route for IPsec connection
 - **Mode:** On
 - **Destination:** 192.168.200.0/24
 - **Interface:** Select the IPsec interface by connection number
 - e.g. If your IPsec connection is **#1** then the interface should be **IPsec#1**.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

The screenshot displays the 'Static Route' configuration page. At the top, there is a 'Mode' toggle set to 'On'. Below this, there are two tabs: 'Settings' and 'Table'. The 'Table' tab is active, showing a table with the following columns: Mode, Name, Destination, Gateway, Interface, and Delete. A single row is visible in the table with the following values: Mode (On), Name (empty), Destination (192.168.200.0/24), Gateway (empty), Interface (IPsec#1), and Delete (a red square icon). Below the table, there is a form for adding a new static route. The form includes a 'Mode' toggle set to 'On', and input fields for 'Name', 'Destination', 'Gateway', and 'Interface'. The 'Interface' field is currently set to '<empty>'. An 'Add' button is located below the form.

- **Spoke 2 configuration**

Spoke 2 IPsec configuration

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



Connection #1 Phase 1

Mode Disable Enable

Name

Protocol

Aggressive mode

Auth Type

Encryption

Hash

Diff Group

Lifetime

Local Host

Local ID

Remote Host

Remote ID

Back

Next

Spoke 2 Static Route configuration

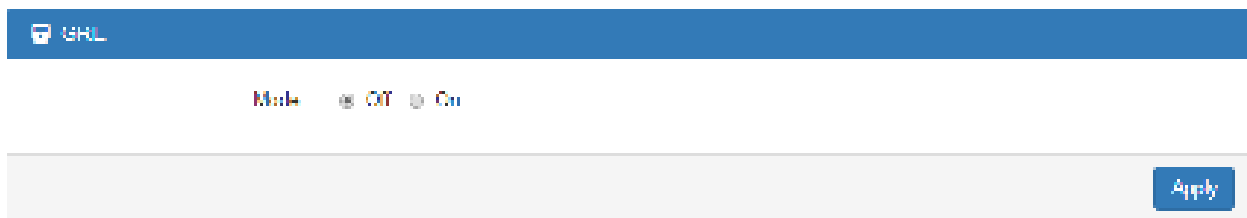
1. Naviagte to the [IP Routing > Static Route](#) page
2. Add the static route for IPsec connection
 - Mode: On
 - Destination: 192.168.100.0/24
 - Interface: Select the IPsec interface by connection number
 - e.g. If your IPsec connection is #1 then the interface should be IPsec#1.
3. Apply the changes

The screenshot displays the 'Static Route' configuration page. At the top, there is a 'Mode' selector set to 'On'. Below this are 'Settings' and 'Status' tabs. A table lists existing static routes with columns: Mode, Name, Destination, Gateway, Interface, and Delete. One route is shown with Destination '192.168.100.0/24' and Interface 'IPsec#1'. Below the table is a form to add a new route, with fields for Mode (On/Off), Name, Destination, Gateway, and Interface (IPsec#1). A blue 'Apply' button is at the bottom right of the form.

11.3 VPN > GRE

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

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



The screenshot shows the GRE configuration interface. At the top, there is a blue header with a shield icon and the text 'GRE'. Below the header, the 'Mode' is set to 'Off', with radio buttons for 'Off' and 'On'. There are four input fields for 'Local Address', 'Remote Address', 'Tunnel Device Address', and 'Tunnel Device Address Prefix', all of which are currently empty. An 'Apply' button is located in the bottom right corner of the configuration area.

The GRE Mode is on.



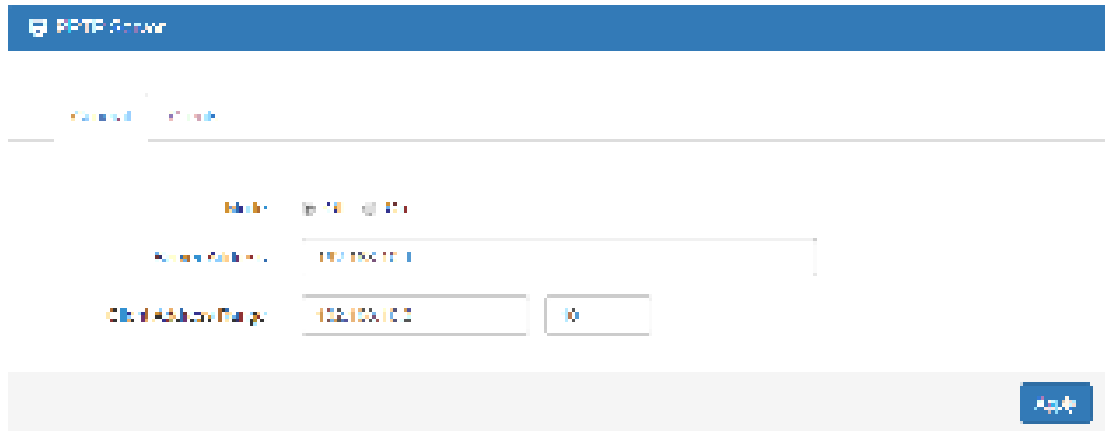
The screenshot shows the GRE configuration interface with the 'Mode' set to 'On'. The 'Local Address' is set to '192.168.1.8', the 'Remote Address' is set to '192.168.1.9', the 'Tunnel Device Address' is set to '10.1.1.8', and the 'Tunnel Device Address Prefix' is set to '8'. An 'Apply' button is located in the bottom right corner of the configuration area.

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

11.4 VPN > PPTP Server

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

(1) General Configuration



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



(2) Clients Configuration

There are two parts for Clients configuration.

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

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

General Clients

#	Mode	Username	Password	Edit	Summary Delete
1	on	client	client		

Add PPTPD Client

Add/Edit

Mode Off On

Username

Password

Add

Apply

11.5 VPN > L2TP

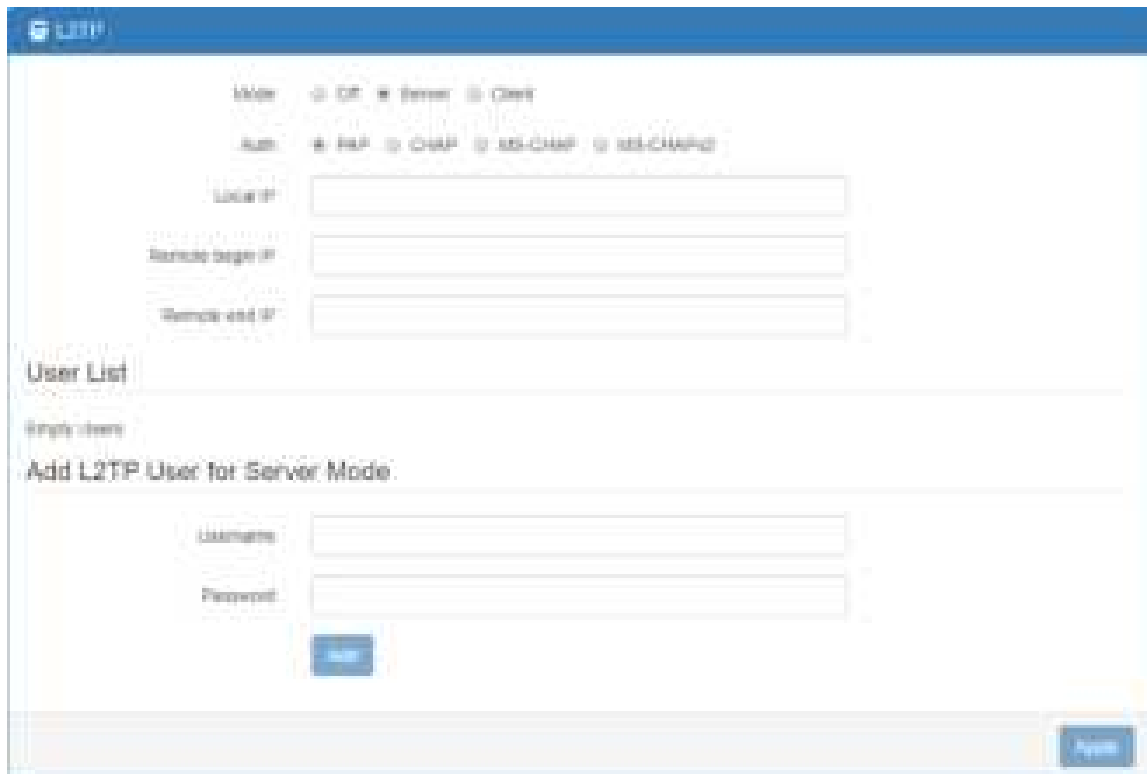
This section allows you to set up L2TP and provides three modes for configuration, including Off, Server, and Client Mode.

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




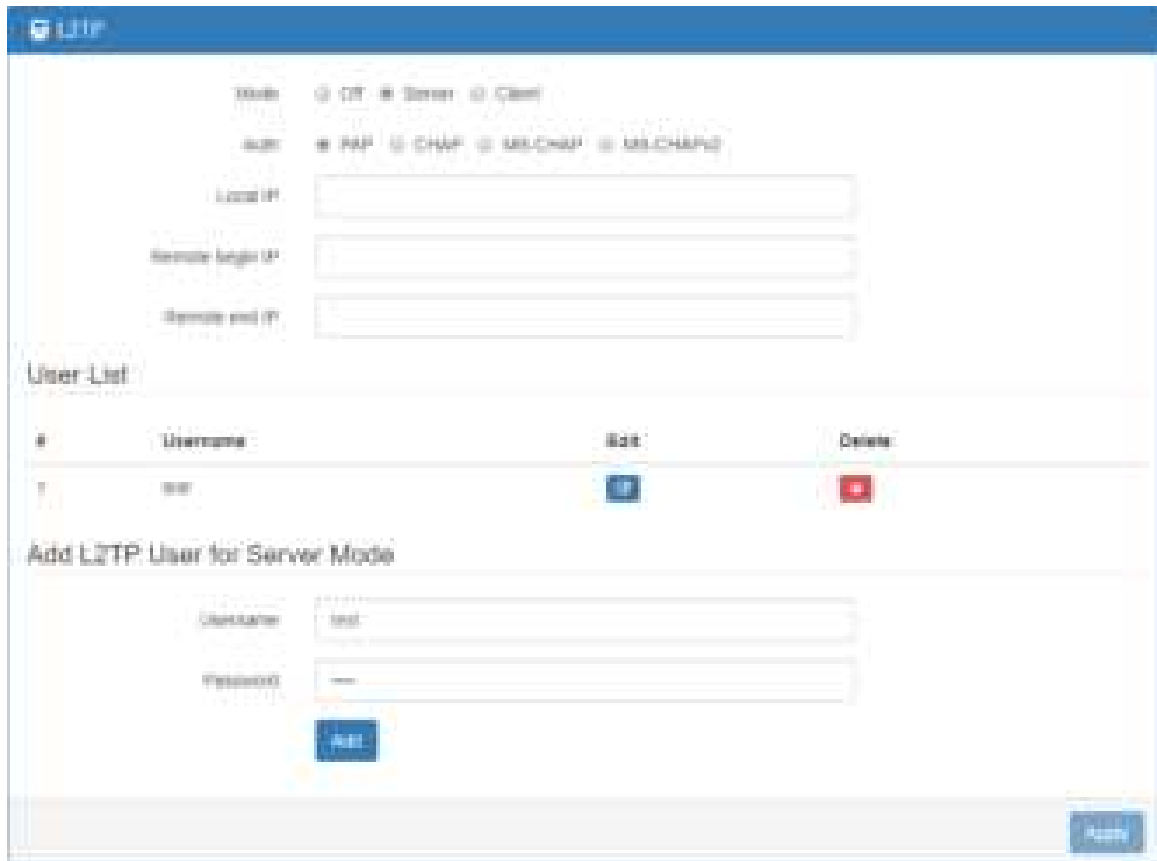
(2) **Server Mode:**

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





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

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

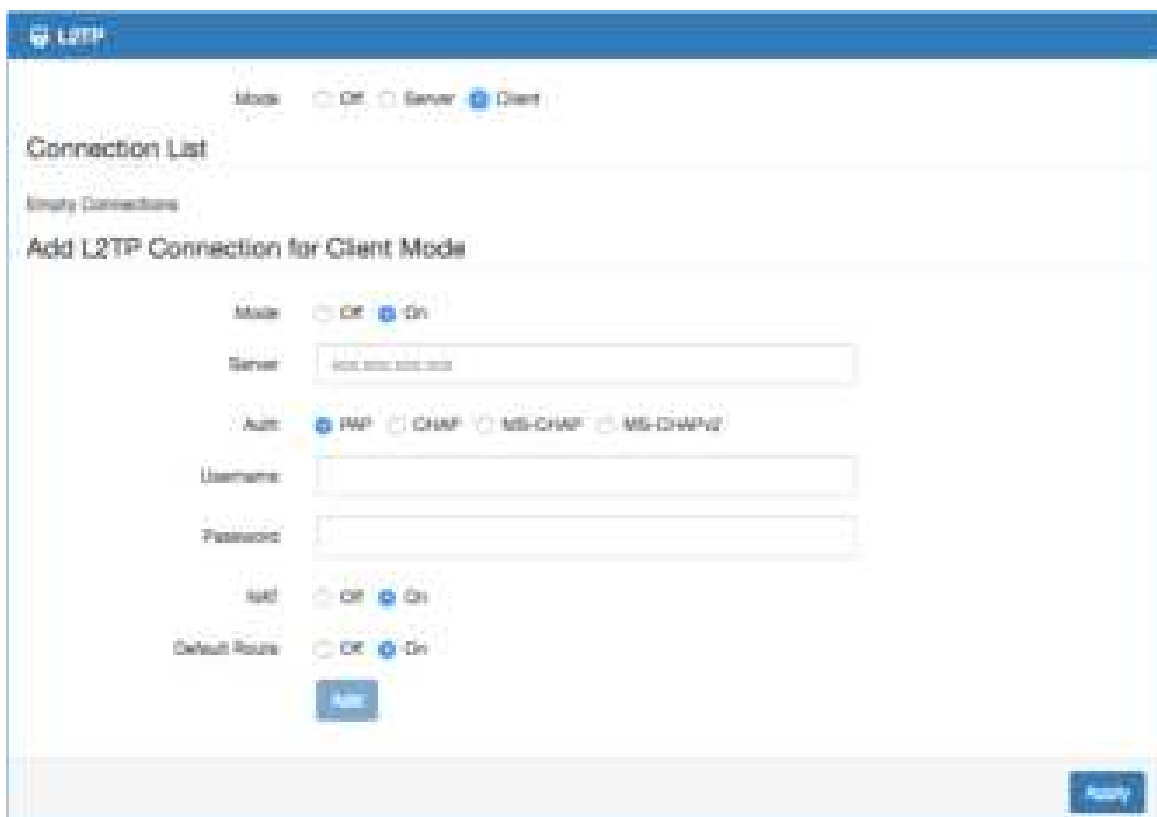


The screenshot shows the L2TP configuration page in Server Mode. At the top, there are radio buttons for Mode: Off, Server, and Client. Below this, there are radio buttons for Auth: PAP, CHAP, MS-CHAP, and MS-CHAPv2. There are three input fields for Local IP, Remote Login IP, and Remote End IP. A 'User List' table is shown with one entry: # 1, Username test, with Edit and Delete buttons. Below the table is the 'Add L2TP User for Server Mode' section with fields for Username (test) and Password (123), and an Add button.

#	Username	Edit	Delete
1	test		


(3) Client Mode:

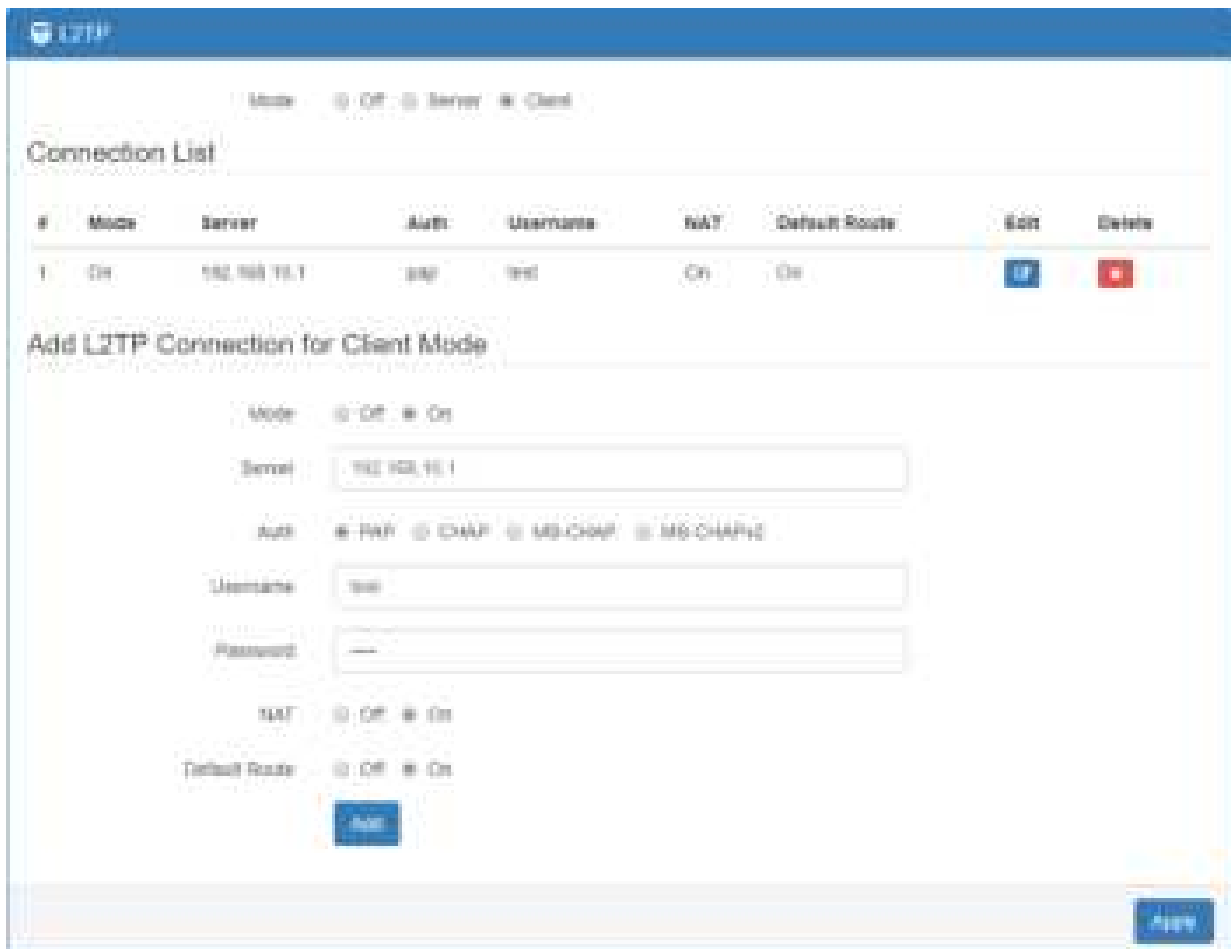
Choose the Client mode and the interface will be changed as below.





The screenshot shows the L2TP configuration page in Client Mode. At the top, there are radio buttons for Mode: Off, Server, and Client. Below this, there are radio buttons for Auth: PAP, CHAP, MS-CHAP, and MS-CHAPv2. There are several input fields: Server (192.168.1.100), Username, and Password. There are also radio buttons for Add and Default Route, both set to On.

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

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



The screenshot displays the L2TP configuration page. At the top, there are tabs for 'Mode', 'Server', and 'Client'. The 'Client' tab is selected. Below the tabs is a 'Connection List' table:

#	Mode	Server	Auth	Username	NAT	Default Route	Edit	Delete
1	On	192.168.16.1	pap	l2tp	On	On		

Below the table is the 'Add L2TP Connection for Client Mode' form:


- Mode: Off On
- Server:
- Auth: PAP CHAP MS-CHAP MS-CHAPv2
- Username:
- Password:
- NAT: Off On
- Default Route: Off On
-

At the bottom right of the form area, there is an button.

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














12 Configuration > Firewall


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

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

12.1 Firewall > Port Forwarding

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

Port Forwarding 				
ID	Mode	Destination	Port	Act
1	10.1.1.1	10.1.1.1	100	
2	10.1.1.1	10.1.1.1	100	
3	10.1.1.1	10.1.1.1	100	
4	10.1.1.1	10.1.1.1	100	
5	10.1.1.1	10.1.1.1	100	
6	10.1.1.1	10.1.1.1	100	
7	10.1.1.1	10.1.1.1	100	
8	10.1.1.1	10.1.1.1	100	
9	10.1.1.1	10.1.1.1	100	
10	10.1.1.1	10.1.1.1	100	
11	10.1.1.1	10.1.1.1	100	
12	10.1.1.1	10.1.1.1	100	



Mode Enable Disable

Description:

Protocol: TCP UDP

Source Port Begin:

Source Port End:

Destination IP:

Destination Port Begin:

Destination Port End:

Save

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

12.2 Firewall > DMZ

This section allows you to set the DMZ configuration.


Mode Enable Disable

Host IP Address:

Save

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

















12.3 Firewall > IP Filter


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

IP Filter

Mode: Disable Enable

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

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



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

IP Filter

Mode: Disable Enable

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

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

Service Ports:
Note: You can prepend the service character in front of port number for non default setting. The default setting is WAN side, protocol is TCP, and the direction is Output.
 Note: The Service character include 'L' for LAN side, 'A' for LAN plus WAN, 'U' for UDP, 'C' for ICMP, and 'P' for all protocols; 'I' for Input.

- For example: U53 means allow device make a outgoing connection(default) to remote DNS(UDP) server on WAN side(default)
- For example: LH43 means allow PC make a (incoming connection to WebUI(default TCP) of Router on LAN(L) side

#	Mode	Protocol	Source / Port	Destination / Port	Edit
1	Disable	All	0.0.0.0 --	0.0.0.0 --	Edit
2	Disable	All	0.0.0.0 --	0.0.0.0 --	Edit
3	Disable	All	0.0.0.0 --	0.0.0.0 --	Edit
4	Disable	All	0.0.0.0 --	0.0.0.0 --	Edit
5	Disable	All	0.0.0.0 --	0.0.0.0 --	Edit
6	Disable	All	0.0.0.0 --	0.0.0.0 --	Edit


Management IP Address:

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

Service Ports:

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

Edit Black/White List

- (1) Click  button to edit Black/White list.
- (2) The default is **Disable** mode as the following interface (Black/White).

EDIT The Black List Page#1

Mode: Enable Disable

Protocol: All ICMP TCP UDP

Access IP:
Range:
- 192.168.1.1/24
- 10.0.0.0/24
- 192.168.0.0/16
- 192.168.1.1/24
- 202.106.0.0/24
- 10.168.1.1/24
- 192.168.1.1/24

Access IP:
Range:
- 10.0
- 104.570

Access IP:

Access IP:

EDIT The White List Page#1

Mode: Enable Disable

Protocol: All ICMP TCP UDP

Access IP:
Range:
- 192.168.1.1/24
- 10.0.0.0/24
- 192.168.0.0/16
- 192.168.1.1/24
- 202.106.0.0/24
- 10.168.1.1/24
- 192.168.1.1/24

Access IP:
Range:
- 10.0
- 104.570

Access IP:

Access IP:

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

- (3) When selecting Enable Mode, the protocol is TCP. The source IP has IPv4 and IPv6 setting formats.
- (4) For Source IP, there are three types to input your source IP that depends on your requirement, including single IP, IP with Mask or giving a range of IP. The following table provides some examples.

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

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

















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

12.4 Firewall > MAC Filter

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

MAC Filter

Mode | Enable | Disable

#	Mode	MAC Address	Edit
1	Enable	00:00:00:00:00:00	
2	Enable	00:00:00:00:00:00	
3	Enable	00:00:00:00:00:00	
4	Enable	00:00:00:00:00:00	
5	Enable	00:00:00:00:00:00	
6	Enable	00:00:00:00:00:00	
7	Enable	00:00:00:00:00:00	
8	Enable	00:00:00:00:00:00	
9	Enable	00:00:00:00:00:00	
10	Enable	00:00:00:00:00:00	
11	Enable	00:00:00:00:00:00	
12	Enable	00:00:00:00:00:00	
13	Enable	00:00:00:00:00:00	
14	Enable	00:00:00:00:00:00	
15	Enable	00:00:00:00:00:00	
16	Enable	00:00:00:00:00:00	

Apply

Fill MAC Filter Description

Mode | Enable | Disable


MAC Address

Apply

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

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

12.5 Firewall > URL Filter

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

URL Filter

Menu Filter Add

ID	Name	Filter	Key Path	Port
1	10.0.0.0	0%		10
2	10.0.0.0	0%		10
3	10.0.0.0	0%		10
4	10.0.0.0	0%		10
5	10.0.0.0	0%		10
6	10.0.0.0	0%		10
7	10.0.0.0	0%		10
8	10.0.0.0	0%		10
9	10.0.0.0	0%		10
10	10.0.0.0	0%		10
11	10.0.0.0	0%		10
12	10.0.0.0	0%		10
13	10.0.0.0	0%		10
14	10.0.0.0	0%		10
15	10.0.0.0	0%		10
16	10.0.0.0	0%		10

Save

URL Filter (This Device Only)

Menu Filter Add

Filter Key Path

Keywords

Save

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

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

12.6 Firewall > NAT

This section allows you to set NAT configuration.

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

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

12.7 Firewall > IPS

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

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

IPS (Intrusion Prevention System)

Mode: On Off

Per IP Address


Total allow incoming connection number:

Max incoming connection retry number: seconds

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

13 Configuration > Service

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

Service: 

SNMP

TR069

Dynamic DNS

VRRP

MQTT

UPnP

SMTP

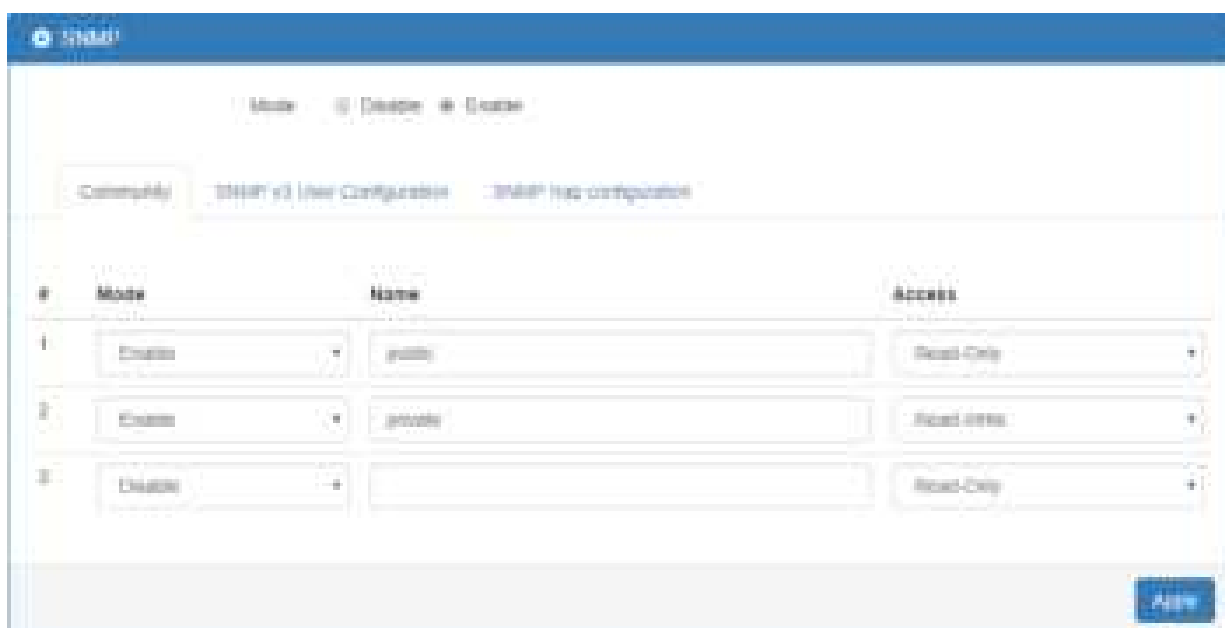
IP Alias

VoS

13.1 Service > SNMP

13.1.1 Community

This section allows you to set the SNMP configuration.



#	Mode	Name	Access
1	Create	public	Read-Only
2	Create	private	Read-Only
3	Create		Read-Only

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

13.1.2 SNMP v3 User configuration

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

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

13.1.3 SNMP trap configuration

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

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

13.2 Service > TR069

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

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

13.3 Service > Dynamic DNS

This section allows you to set up Dynamic DNS.

Dynamic DNS

Mode: Disable Enable

Service Provider:

Host Name:

Token ID:

Host Secret ID:

IP Address Selection: Internet IP WAN IP

Dynamic DNS

Mode: Disable Enable

Service Provider:

Host Name:

Token ID:

Update Period Time (Sec):

IP Address Selection: Internet IP WAN IP

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

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

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

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

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

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

Service provider	freedns.afraid.org
Host Name	Register hostname, e.g. tester.mo00.com
Username	Register username.
Password	Register password.

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

13.4 Service > VRRP

This section allows you to configure VRRP.

Mode: Disable Enable

Group ID:

Priority:

Virtual IP:

Apply

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	<ul style="list-style-type: none">• Each router in the same VRRP group must have the same virtual IP address. The default is 0.0.0.0.• This virtual IP address must belong to the same address range as the real IP address of the interface.

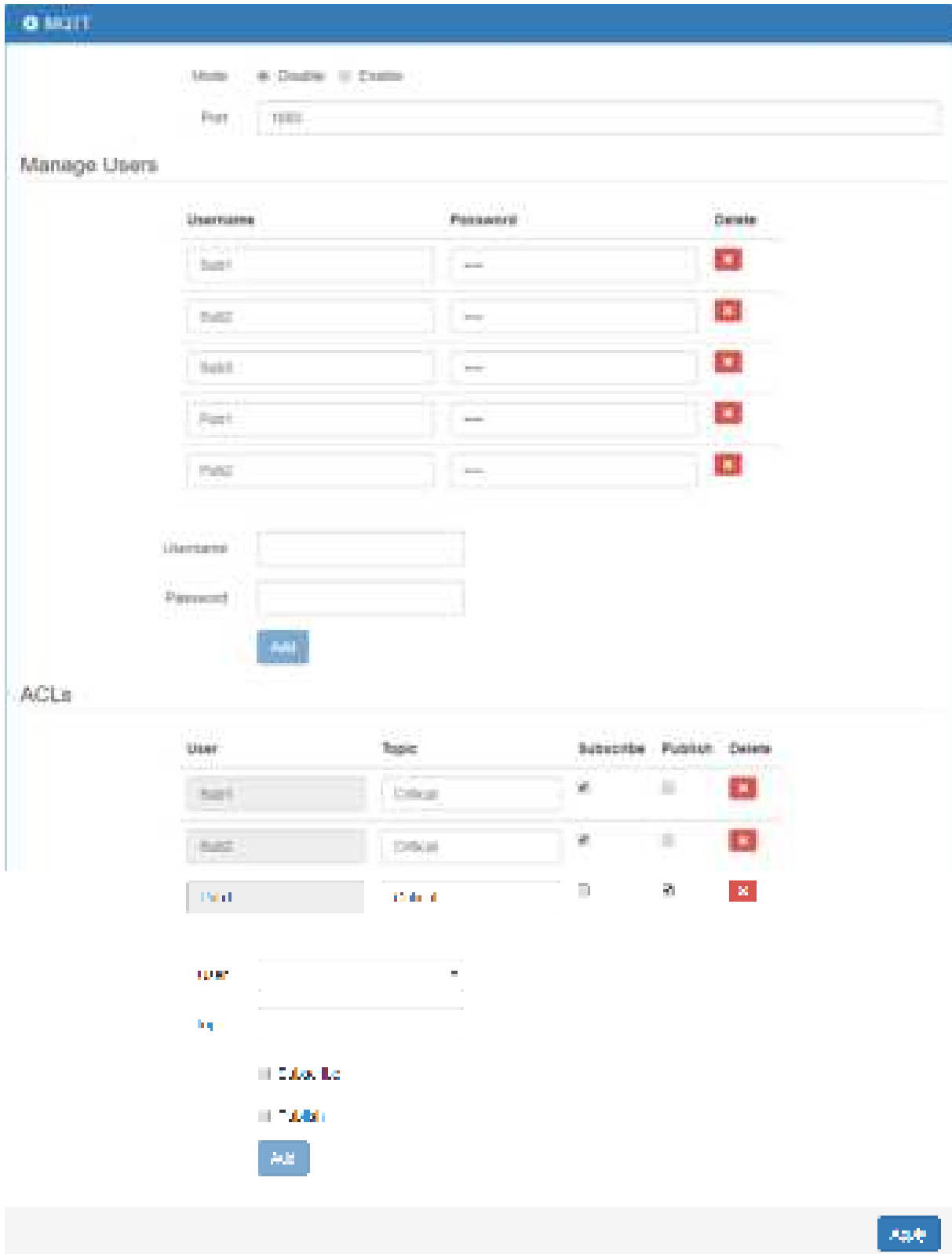
13.5 Service > MQTT

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

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

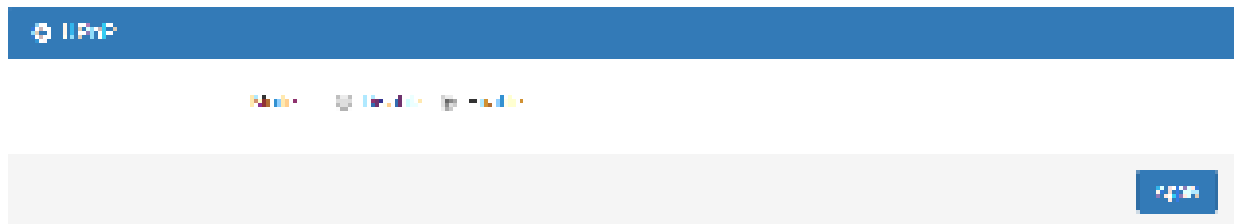
Take for example, the interface is shown as below.

The **Manage Users** section will show all users that you create. Moreover, each user can use the delete button to delete it. For the **ACLs** control, user can specify what topic should be limited. In this case, we set up the publisher **pub1** to write the critical topic. Additionally, we also allow the subscribers **sub1** and **sub2** to read the critical topic. Thus, only the sub1 and sub2 can receive it when **pub1** sending the message.



13.6 Service > UPnP

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



Note:

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

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

13.7 Service > SMTP

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

Service > SMTP	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
Server	The email will be sent through the server.
Port	There are three ports for SMTP communication between mail servers. <ul style="list-style-type: none">● Port 25 : Use TCP port 25 without encryption.● Port 465 : SMTP connections secured by SSL.● Port 587 : SMTP connections secured by TLS.
Username / Password	Fill in your username and password as the same your server.

13.1 Service > IP Alias

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

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

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

The screenshot shows the 'IP Alias' configuration page. At the top, there is a 'Mode' selector set to 'Off'. Below this is a table titled 'Entries' with the following data:

ID	Mode	Interface	Addr	Mask	Edit	Delete
1	on	eth1	192.168.3.1	255.255.255.0	[Edit]	[Delete]

Below the table is the 'Add IP Alias Entry' form. It includes a 'Mode' selector (set to 'Off'), an 'Interface' dropdown menu (set to 'eth1 (WAN Ethernet)'), an 'Addr' text input field (containing '192.168.3.100'), and a 'Mask' text input field (containing '255.255.255.0'). An 'Add' button is located at the bottom of the form.

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	<ul style="list-style-type: none"> ● Mode: select from Off or On to use or not use this entry. ● Interface: the interface you want to provide the additional address. ● Addr: the IP address. ● Mask: the network mask.

13.9 Service > QoS (Quality of Service)

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

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

13.9.1 ISP Bandwidth


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



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

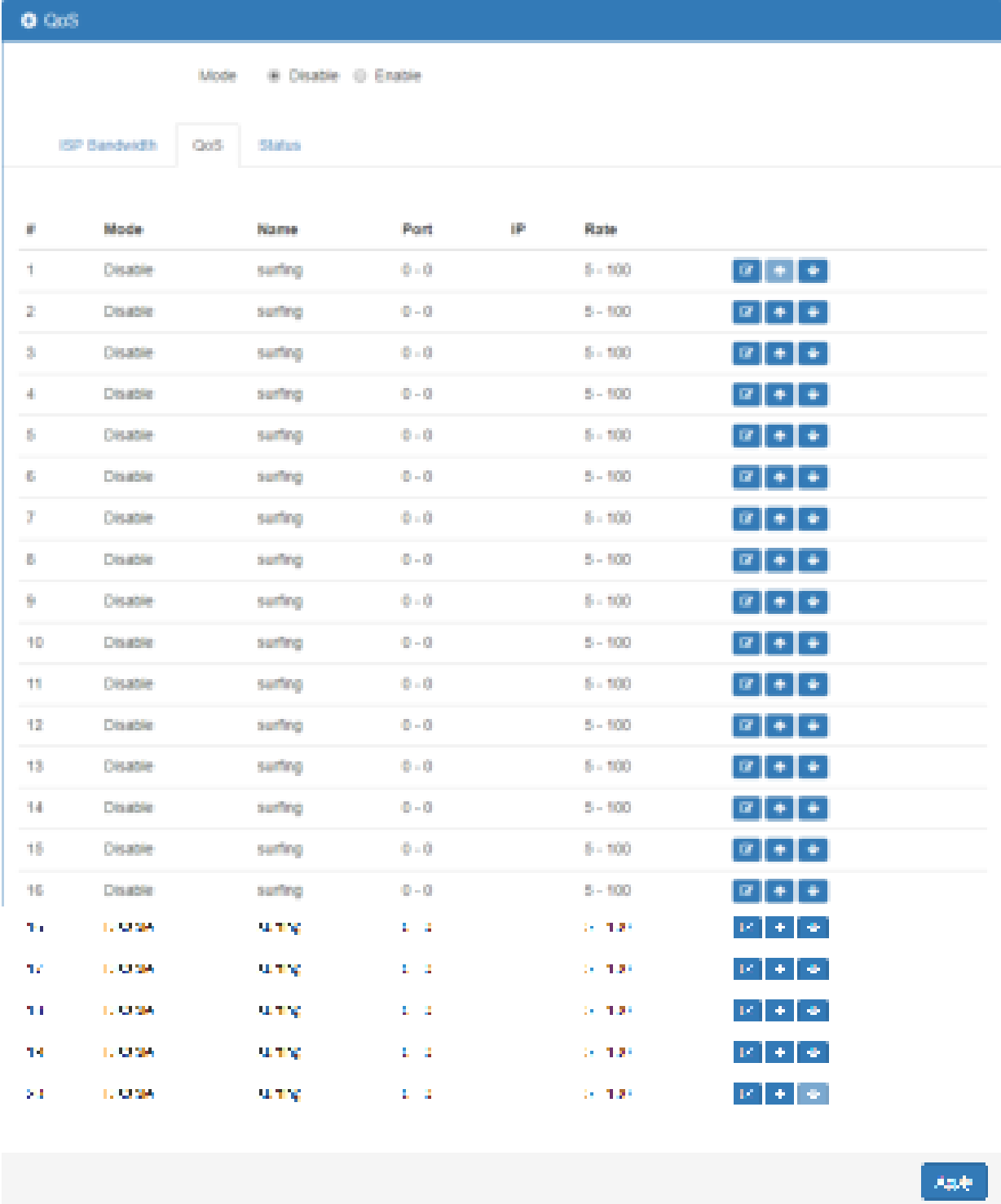
The screenshot displays the QoS configuration page. At the top, there are radio buttons for 'Mode', 'Disable', and 'Enable'. Below this, there are tabs for 'ISP Bandwidth', 'QoS', and 'Status'. The main content area is divided into two sections: 'WAN ETHERNET' and 'LTE'. Each section contains two rows of input fields: 'Upstream' and 'Downstream'. For 'WAN ETHERNET', both 'Upstream' and 'Downstream' are set to '1000' with a unit of 'Kbps'. Similarly, for 'LTE', both 'Upstream' and 'Downstream' are set to '1000' with a unit of 'Kbps'. A 'Save' button is located at the bottom right of the configuration area.

13.9.2 QoS

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

 **button** allows you to edit QoS Entry and configure QoS settings.
































































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



QoS

Mode Disable Enable

ISP Bandwidth QoS Status

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

Save

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

1. Classify traffic by following items:

Service > QoS > Edit QoS Entry	
Item	Description
Mode	Select from Disable or Enable QoS.
Name	The setting can be edited or deleted the existed entries.
Interface	The interface of QoS entry is either WAN Ethernet or LTE and both options.
Direction	<ul style="list-style-type: none"> When selecting Upstream for LAN to WAN traffic, the Port Begin/End is for public server. When selecting Downstream for WAN to LAN traffic, the Port Begin/End is for public server. When selecting Upstream (LAN server) for WAN to LAN traffic, the Port Begin/End is for LAN server. When selecting Downstream (LAN server) for LAN to WAN traffic, the Port Begin/End is for LAN server. Downstream (LAN server) is for LAN to WAN traffic, and the Port Begin/End is for LAN server.
IPv4v6 Address	<p>Choose four types to set address format, including All, Single, Subnet, and Range.</p> <ul style="list-style-type: none"> All is for none. Single is for single IP address. Subnet is for IP address with subnet mask bit. Range is for the specified range between two IP addresses. <p>Hint: When [RANGE] is selected, compare the difference from left to right octet and find out different octet for setting the specified range of IP address. All other parts after different octet would be ignored.</p>
Protocol	<ul style="list-style-type: none"> All is for none. UDP is for User Datagram Protocol. TCP is for Transmission.
Port Begin/Port End	the TCP/UDP service port
VLAN follow vid of	<ul style="list-style-type: none"> NONE NET1 - NET8 <p>Note: For NET1 to NET8, make sure the related subnet is enabled at VLAN→Tag Base. The VLAN ID, vid, will be the VID field of the related Subnet at VLAN→Tag Base.</p>
COS (Class of Service or 802.1q)	NONE or 0~7. It is class of service for VLAN.

2. Assign bandwidth by following items:

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

3. Assign group IP bandwidth by following items:

Bandwidth divided for each IP Address: When this feature is selected, the bandwidth assigned by Min Rate / Max Rate will be divided by the number of IP addresses. The available IP type is Subnet and Range. User needs to calculate the Min Rate and Max Rate for those IP addresses.

The subnet mask bit in IP Type Subnet is octet boundary and the number of IP addresses is also one octet, 256, from subnet mask bit to subnet mask plus eight bit.

The screenshot shows the 'Edit QoS Entry #1' configuration page. At the top, there are 'Apply', 'Disable', and 'Enable' buttons. The configuration fields are as follows:

- Name:** jcting
- Interface:** WAN ETHERNET
- Direction:** Upstream
- IP Address:** All (with a note: 'Example: 192.168.1.0/24')
- Port Range:** 0 (with a note: 'When [RANGE] is selected, the most left different octet would be the specified range. All other parts after the most left different octet would be ignored.') (with a note: 'When [RANGE] is selected, the most left different octet would be the specified range. All other parts after the most left different octet would be ignored.') (with a note: 'When [RANGE] is selected, the most left different octet would be the specified range. All other parts after the most left different octet would be ignored.'))
- Protocol:** All
- Port Range:** 0
- Port End:** 0
- IP Address below yd of:** NONE
- Class of Service:** NONE
- Min Rate:** 0 (with a note: 'Kbps')
- Max Rate:** 0 (with a note: 'Kbps')

At the bottom, there is a checked checkbox labeled 'Bandwidth divided for each IP Address' and a 'Save' button.

13.9.3 Status

1. Refresher Setting select the showed content of bandwidth usage by following items:
 - **Refresh rate:** how long the browser will update the showed content once.
 - **Direct:** show Upstream or Downstream.
 - **Show detail bandwidth for each IP address:** show the group IP bandwidth usage.
 - **Apply Refresh Setting button:** press this button to take above new setting effect.
2. Data part is the content of bandwidth usage.

QoS

Mode Disable Enable

ISP Bandwidth QoS Status

Refresher Setting

Update every secs

Direction Upstream Downstream

Show detail of bandwidth for each IP Address

Data

Please enable this function first

13.9.4 The case of Internet Web site access

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

Mode: Disable Enable

Edit QoS Entry #1

Mode: Disable Enable

Name:

Interface: WAN ETHERNET LTE

Direction: Upstream Downstream Upstream(LAN Server) Downstream(LAN Server)

(Policy) Address:

Example (wrong)

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

Protocol: All TCP UDP

Port Begin:

Port End:

VLAN follow list of:

Class of Service:

Min Rate: Kbits

Max Rate: Kbits

Bandwidth divided for each IP Address

- Step 3: Set QoS Entry #2

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

The screenshot shows the 'Edit QoS Entry #2' configuration page. At the top, there is a 'Mode' section with radio buttons for 'Disable' and 'Enable', where 'Enable' is selected. Below this is the title 'Edit QoS Entry #2'. The main configuration area includes:

- 'Name': 'Internet Browse US' (text input)
- 'Interface': 'WIREETHERNET' and 'LTE' (radio buttons, with 'LTE' selected)
- 'Direction': 'Upstream', 'Downstream', 'Upstream(LAN Server)', and 'Downstream(LAN Server)' (radio buttons, with 'Upstream' selected)
- 'IP Policy Address': A dropdown menu showing 'all' and an adjacent empty text input field.
- 'How IP Policy Address': A note stating: 'When [NONE] is selected, the most left different octet would be the specified range. All other parts after the most left different octet would be ignored.' Below this is a 'Protocol' section with radio buttons for 'All', 'TCP', and 'UDP', where 'All' is selected.
- 'Port Begin': '443' (text input)
- 'Port End': '443' (text input)
- 'VLAN follow out of': 'NONE' (dropdown menu)
- 'Class of Service': 'NONE' (dropdown menu)
- 'Min Rate': '100' (text input) with a 'Kbps' label.
- 'Max Rate': '100' (text input) with a 'Kbps' label.
- A checkbox at the bottom: 'Bandwidth divided to each IP Address' (unchecked).

 A blue 'Save' button is located in the bottom left corner of the configuration area.

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

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

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

- Step 8: Check Status Downstream.

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

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

The screenshot shows the QoS Status page with the following settings and data:

- Mode: Disable Enable
- ISP Bandwidth | QoS | Status
- Refresher Setting:
 - Update every: secs
 - Direction: Upstream Downstream
 - Show detail of bandwidth for each IP Address
 - Apply Refresh Setting
- Data Table:

#	Name	Send Bytes	Send Packets	Dropped Packets	Bandwidth(kbits/s)	Percentage(%)
1	Internet Browse US	57956	399	0	60.56	9.06
2	Total	57956	399	0	60.56	9.06

The screenshot shows the QoS Status page with the following settings and data:

- Mode: Disable Enable
- ISP Bandwidth | QoS | Status
- Refresher Setting:
 - Update every: secs
 - Direction: Upstream Downstream
 - Show detail of bandwidth for each IP Address
 - Apply Refresh Setting
- Data Table:

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

13.9.5 Bandwidth divided for each IP address

The screenshot shows the configuration page for a QoS entry. The 'Name' field is set to 'Ten'. The 'Interface' is 'WAN ETHERNET'. The 'Direction' is 'Upstream'. The 'IP Address' is set to a range of '192.168.1.2-192.168.1.11'. Below this, a note explains that when a range is selected, the most left different octet is used for calculation. The 'Protocol' is set to 'All'. The 'Port Begin' and 'Port End' fields are both set to '0'. The 'VLAN Identifier' and 'Class of Service' are both set to 'NONE'. The 'Min Rate' is set to '100' kbit/s and the 'Max Rate' is set to '200' kbit/s. At the bottom, the checkbox 'Bandwidth divided for each IP Address' is checked.

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

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


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

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

The Min rate will be divided by two, $100/2=50$ kbit/s for IP address 192.168.2.0 and 192.168.1.0. The Max rate is same with configuration for both IP addresses, 192.168.1.0 and 192.168.2.0, since we don't want to waste the bandwidth when there is just one IP address in using. For example, if only 192.168.1.0 have traffic to send/receive, then it can use all of the 200 kbit/s.

14 Configuration > Management

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

Management 
Identification
Administration
Contacts / On Duty
SSH
Web
Firmware
Configuration
Reset Factory
Reboot
Schedule Reboot

14.1 Management > Identification

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

Attr.	Value
Active Image Partition	b
Model Name	M001 6W
LAN Ethernet MAC Address	18:0E:10:00:18:00
WAN Ethernet MAC Address	18:0E:10:00:18:02
Bootloader Version	1.0
Software Version	V1.05
Serial Number	
Software MCSN	016000001762L9L2
Hardware MCSN	01600002002L9L0
Modem Firmware Version	LU25L17A02/06M4G
IMSI	861107030524950
Uptime	4:30:02

Management > Identification	
Item	Description
Model Name	Show the model name of cellular router.
LAN Ethernet MAC Address	Show the LAN Ethernet MAC address.
WAN Ethernet MAC Address	Show the WAN Ethernet MAC address.
Bootloader Version	Show the bootloader version currently running on the device.
Software Version	Show the software version currently running on the device
Serial Number	Show the product serial number.
Software MCSV	Show the software MCSV of the running firmware
Hardware MCSV	Show the current hardware MCSV of the device.
Modem Firmware Version	Show the modem firmware version of the device
IMEI	Show the IMEI (International Mobile Equipment Identity number).
Uptime	Show the current system uptime.

14.2 Management > Administration

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

The screenshot shows a web interface for system configuration. Under 'System Setup', there is a 'Model Name' field with the value 'Cellular Router' and a 'Session TTL' field with the value '5' and a unit '(minutes, 0 means no limit)'. Below this is the 'Super User' section with 'New Password' and 'Retype to confirm' fields.

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

User Level Status	Super User	Administrator	Read Only	Guest
User name	System Account (root / admin)	only Super User can modify	only Super User can modify	N/A
Password	configurable	configurable	configurable	N/A
Permission	(1) Add/Delete/Modify all users' accounts except Super User. (2) Read/Write Configuration	Read / Write Configuration	only Read Configuration	N/A

System Setup

Model Name: Cellular Router
Session TTL: 0 (minutes, 0 means no timeout)

Super User

New Password:
Retype to confirm:

User #1

Name:
User Level:
New Password:
Retype to confirm:

User #2

Name:
User Level:
New Password:
Retype to confirm:

User #3

Name:
User Level:
New Password:
Retype to confirm:

14.3 Management > Contacts / On Duty

This section allows you to create the groups, add the users. For more detailed instruction, please navigate to [System > Alarm](#).

14.3.1 Contacts

Name	Phone	E-mail
Test	+800912345678	test@test.com

+ Add Group: Please fill out group name.

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

14.3.2 Duty Schedule

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

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

14.4 Management > SSH

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

SSH

Mode Disable Enable

Server Port

Access Control Allow All Allow specified IPv4v6 Address below

IPv4v6 Address Set

#	IP Address
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>
8	<input type="text"/>
9	<input type="text"/>
10	<input type="text"/>

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

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

Apply

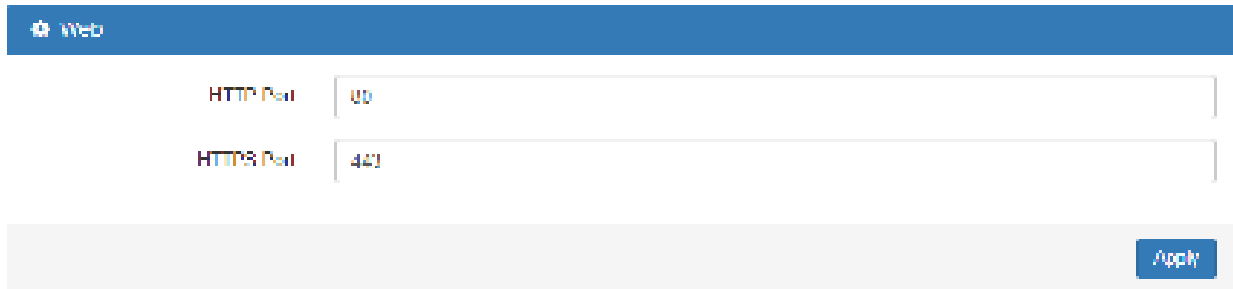
Management > SSH	
Item	Description
Mode	Select from Disable or Enable SSH function.
Server Port	The port number is where SSH server works on.
Access Control	<ul style="list-style-type: none"> Allow All: Any client who own the IPv4v6 Address can reach system is able to connect system. Allow specified IPv4v6 Address below: Only those configured IPv4v6 Address client are allowed to connect system.

14.5 Management > Web

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

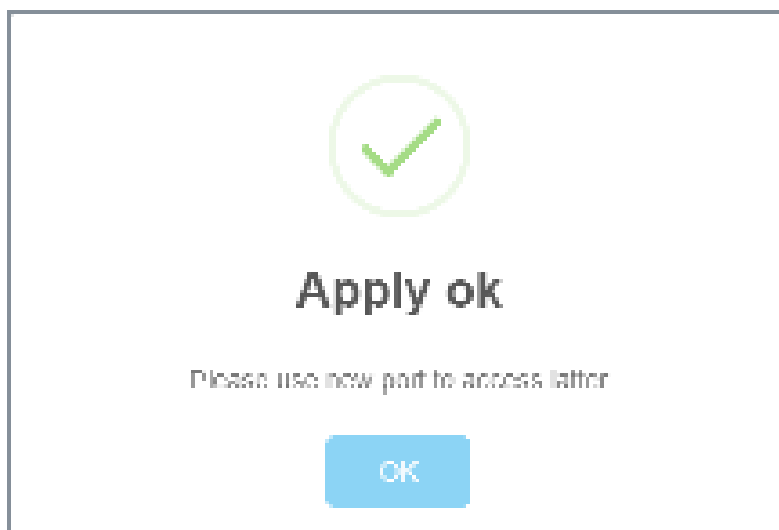
We need a way to reply immediately and apply the configuration latter. By using fork, we can make parent process reply immediately and the child process execute the configuration.

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





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

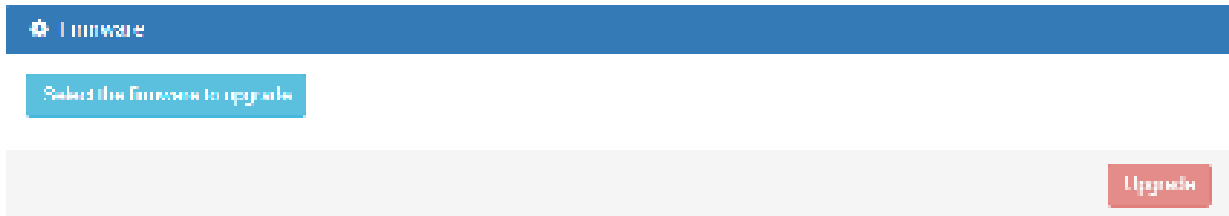
After pressing **Apply** button, the device will apply immediately and give you some hints “Please use new port to access latter”. For example, set the HTTP Port as 3000.



14.6 Management > Firmware

This section provides you to upgrade the firmware of router.

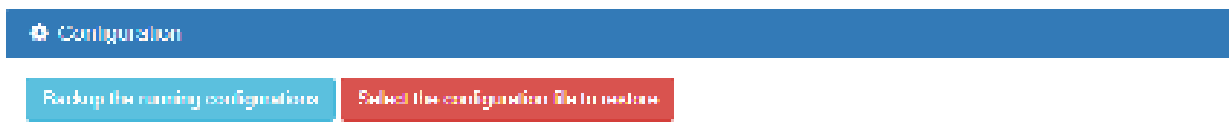
- (1) Click  button to choose your current firmware version in your PC.
- (2) Select  button to update.
- (3) After upgrading successfully, please reboot the router.



14.7 Management > Configuration


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

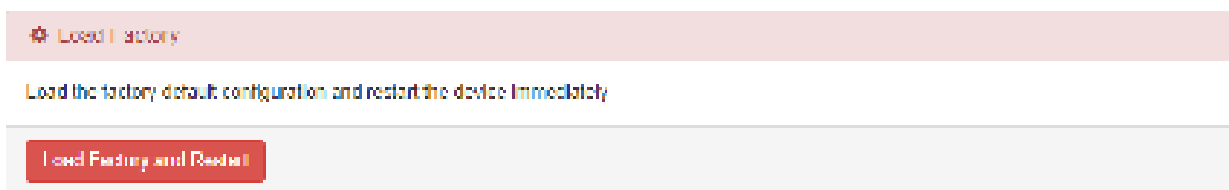
- (1) Click  button to export your current configurations.



- (2) Click  button to import the configuration file.

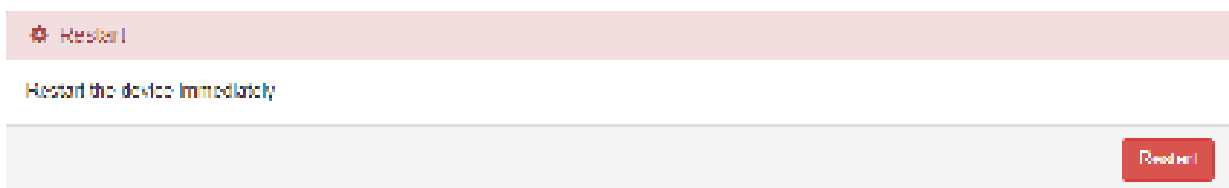
14.8 Management > Load Factory

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



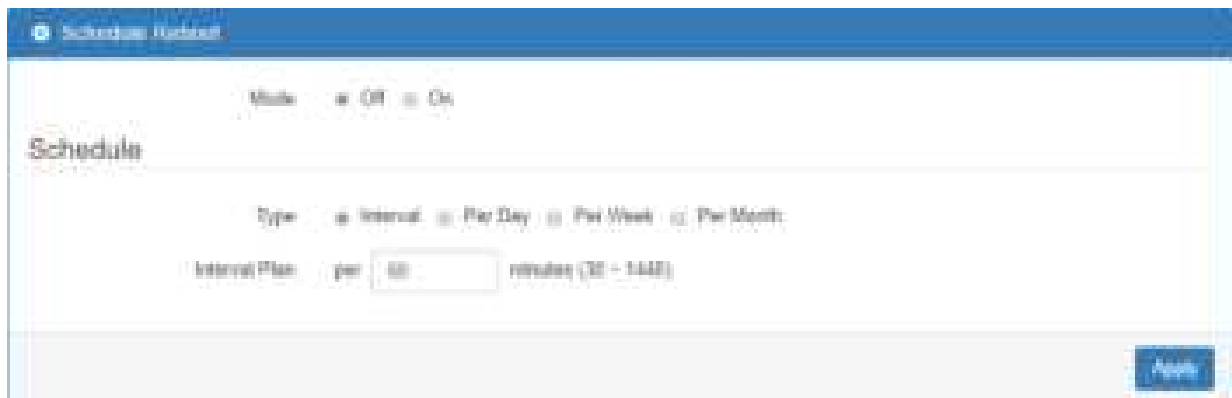
14.9 Management > Restart

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



14.1C Management > Schedule Reboot

The setting allows you to schedule the reboot time regularly.



● Schedule Type – Interval



● Schedule Type - Per Day



● Schedule Type - Per Week



● Schedule Type - Per Month



15 Configuration > Diagnosis

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

Diagnosis



Ping

Traceroute

15.1 Diagnosis > Ping

Please assign the Host you want to ping.

Ping

Host

Ping

The result of the ping is as below.

Ping

Host

0.0.0.0

```
PING 0.0.0.0 (0.0.0.0): 56 data bytes  
ping_xxx: Network is unreachable
```

Ping

15.2 Diagnosis > Traceroute

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

Traceroute

Host

Traceroute

The result of the traceroute is as below.

Traceroute

Host

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 0 0.0.0.0 0.000 100% connect: Network unreachable
```

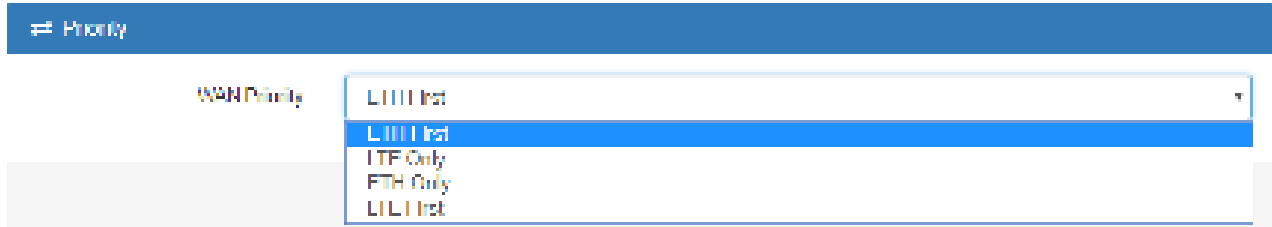
Traceroute

16 Configuration Applications

This section explains specific examples how to configure your applications.

16.1 WAN Priority

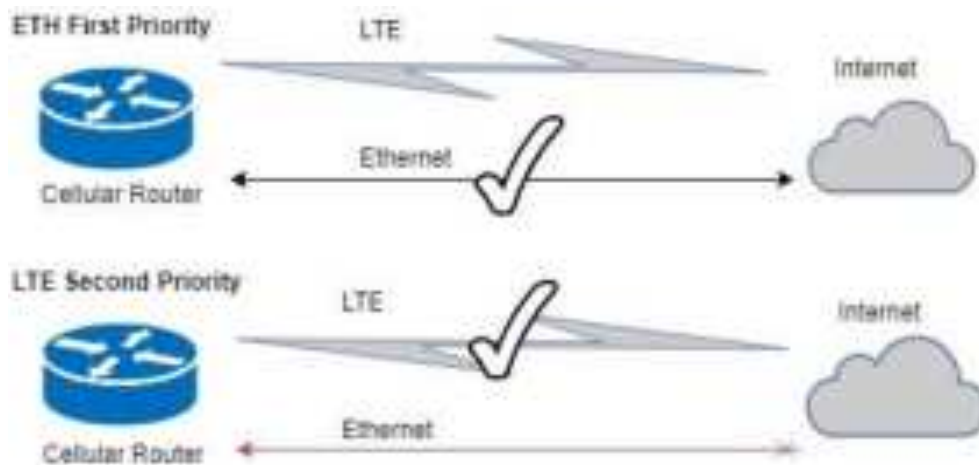
You can select from ETH First, LTE Only, ETH Only or LTE First.



(1) WAN Priority > ETH First:

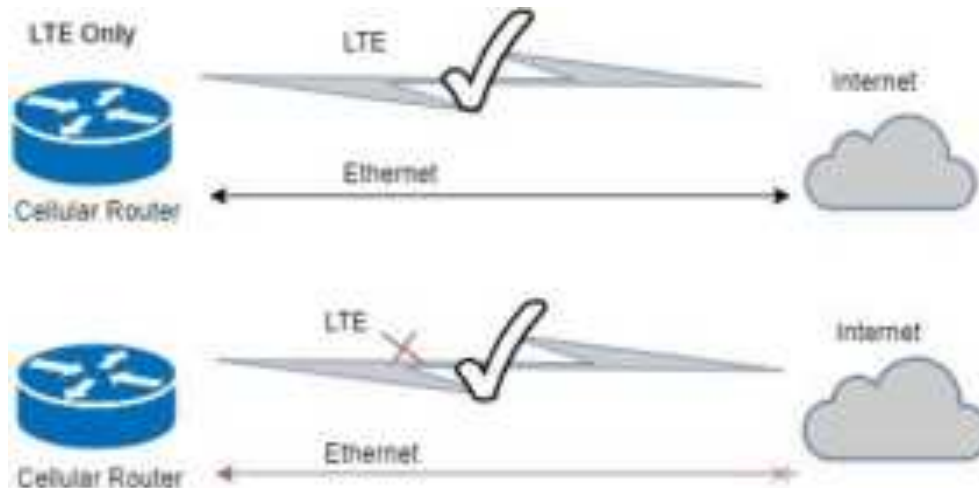
In case both Ethernet and LTE can access Internet, the router would route network packages through Ethernet. The reason is Ethernet that is low price and stable.

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



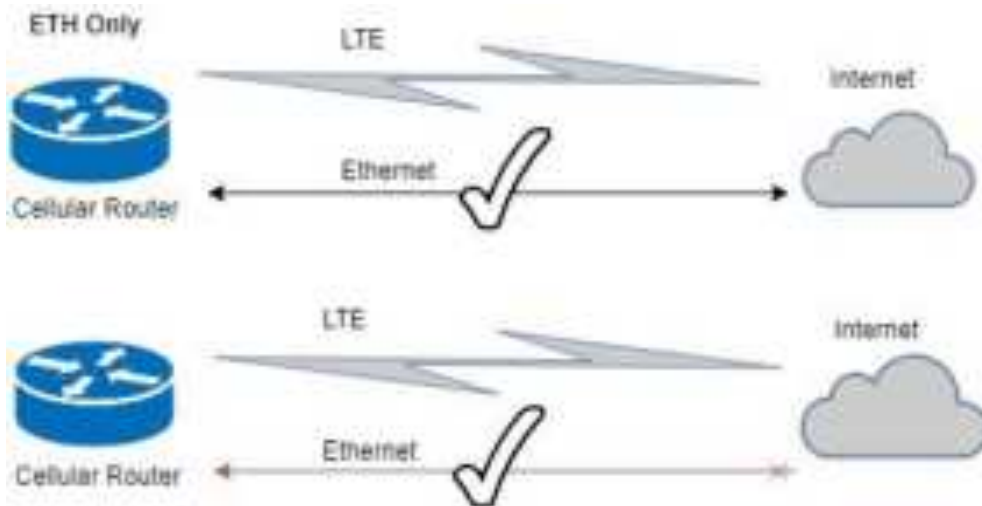
(2) WAN Priority > LTE Only:

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



(3) WAN Priority > ETH Only:

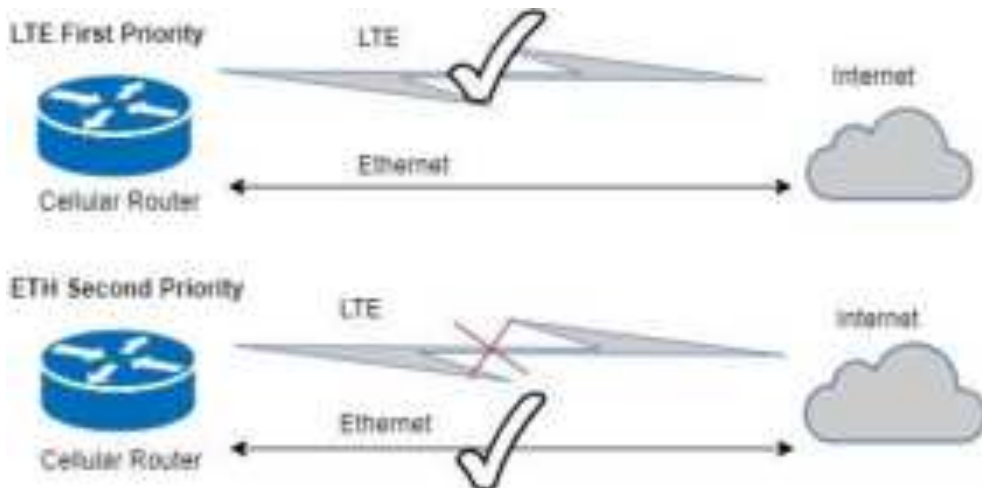
In this mode, the router only routes network packages through Ethernet.



(4) WAN Priority > LTE First:

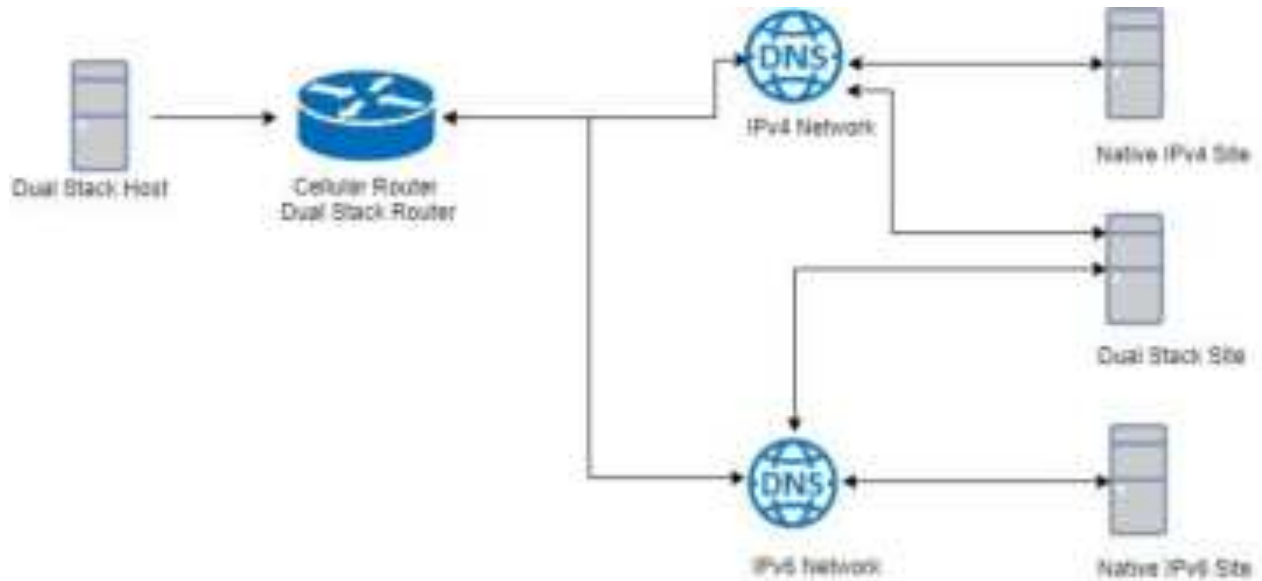
In case both Ethernet and LTE can access Internet, the router would route network packages through LTE.

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



16.2 LAN > IPv4/IPv6 Dual Stack

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



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

Status		
Att:	Current SIM	Backup SIM
SIM Card	SIM1	SIM2
Insert Status	Ready	Not inserted
Operator	China Mobile Telecom	
Insert Access	FDD LTE	
MNO	454634290007750	
Phone Number		
Band	LTE BAND 7	
Channel ID	3000	0
IPv4 Address	10.107.200.11	
IPv4 Mask	255.255.255.255	

Ethernet WAN	
Att:	Value
IPv4 Address	102.100.11.176
IPv4 Mask	255.255.255.0

Ethernet LAN	
Att:	Value
IPv4 Address	102.100.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	2001:0021:0001:100

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

```
Command Prompt (1)
C:\>ipconfig /all

Windows IP Configuration

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

Ethernet adapter Blue:

Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GBE Family Controller #2
Physical Address. . . . . : 00-E0-4C-68-00-FD
Dhcp Enabled. . . . . : Yes
IPv6 Address . . . . . : 2001:b400:a335:a5ca::101(Preferred)
Lease Obtained. . . . . : Thursday, March 15, 2018 1:15:00 PM
Lease Expires . . . . . : Thursday, March 15, 2018 1:17:06 PM
Link-local IPv6 Address . . . . . : fe80::8c61ae319:2e70:1140%15(Preferred)
IPv4 Address. . . . . : 192.168.1.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, March 15, 2018 11:23:20 AM
Lease Expires . . . . . : Thursday, March 15, 2018 6:14:00 PM
Default Gateway . . . . . : fe80::c2e:43ff:fe0d:4743%15
                               192.168.1.1
Dhcp Server . . . . . : 192.168.1.1
Dhcpv6 IAID . . . . . : 620814412
Dhcpv6 Client DUID. . . . . : 00-01-00-01-18-04-03-75-08-50-E6-C3-63-E0

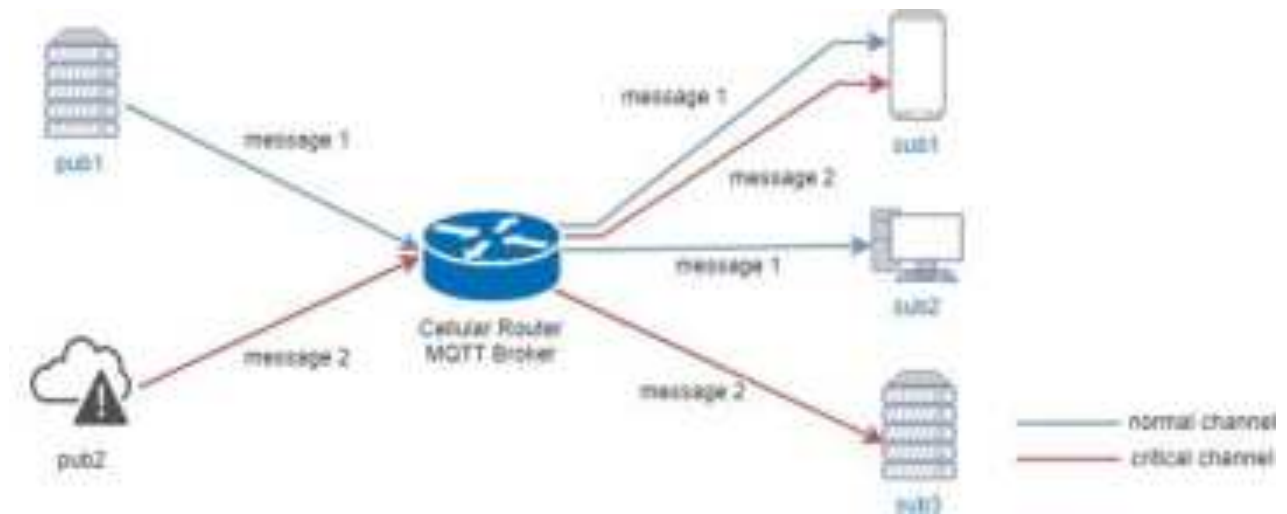
DNS Servers . . . . . : fe80::c2e:43ff:fe0d:4743%15
                               192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

C:\>
```

16.3 MQTT Broker

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

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



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

The screenshot shows the MQTT web interface. At the top, there is a 'Mode' selector with 'Disable' selected and 'Enable' as an option. Below it is a 'Port' input field with the value '1883'. The main section is titled 'Manage Users' and contains a table of existing users:

Username	Password	Delete
Sub1	---	[Delete]
Sub2	---	[Delete]
Sub3	---	[Delete]
Pub1	---	[Delete]
Pub2	---	[Delete]

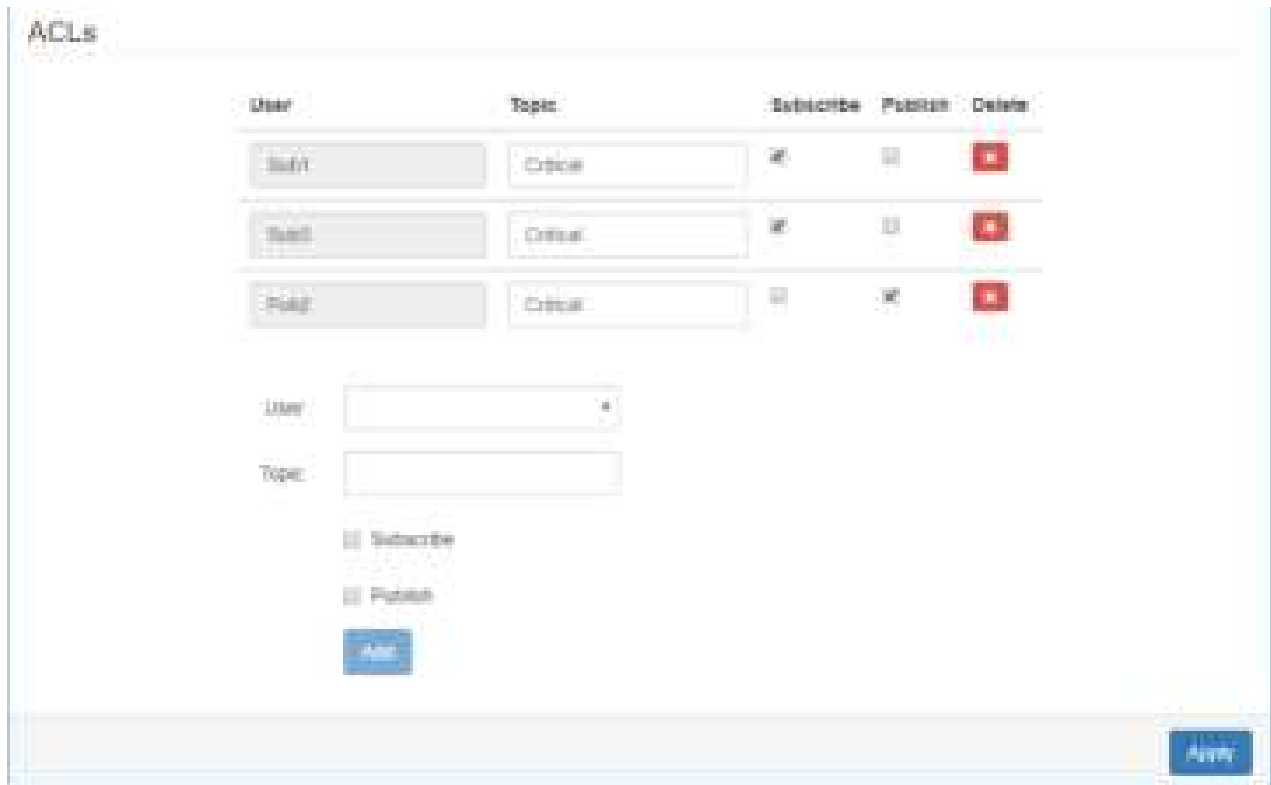
Below the table, there are input fields for 'Username' and 'Password', and a 'Add' button.

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

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

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

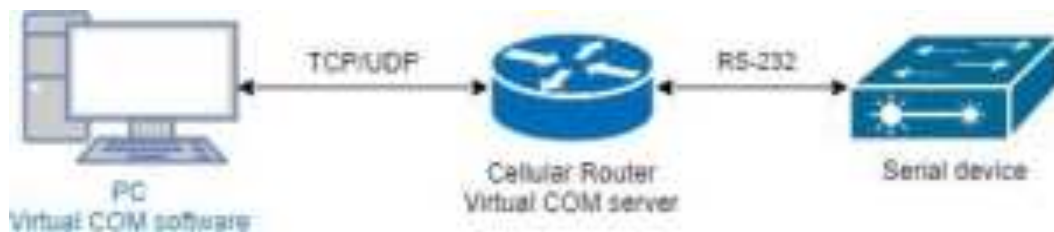
Thus, when **pub2** is sending the message only the **sub1**, the **sub3** can receive it.



16.4 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. USB-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, data 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	Server	192.168.1.1	TCP	6000	Edit
2	Server	192.168.1.1	TCP	6000	Edit
3	Server	192.168.1.1	TCP	6000	Edit

[Close](#)

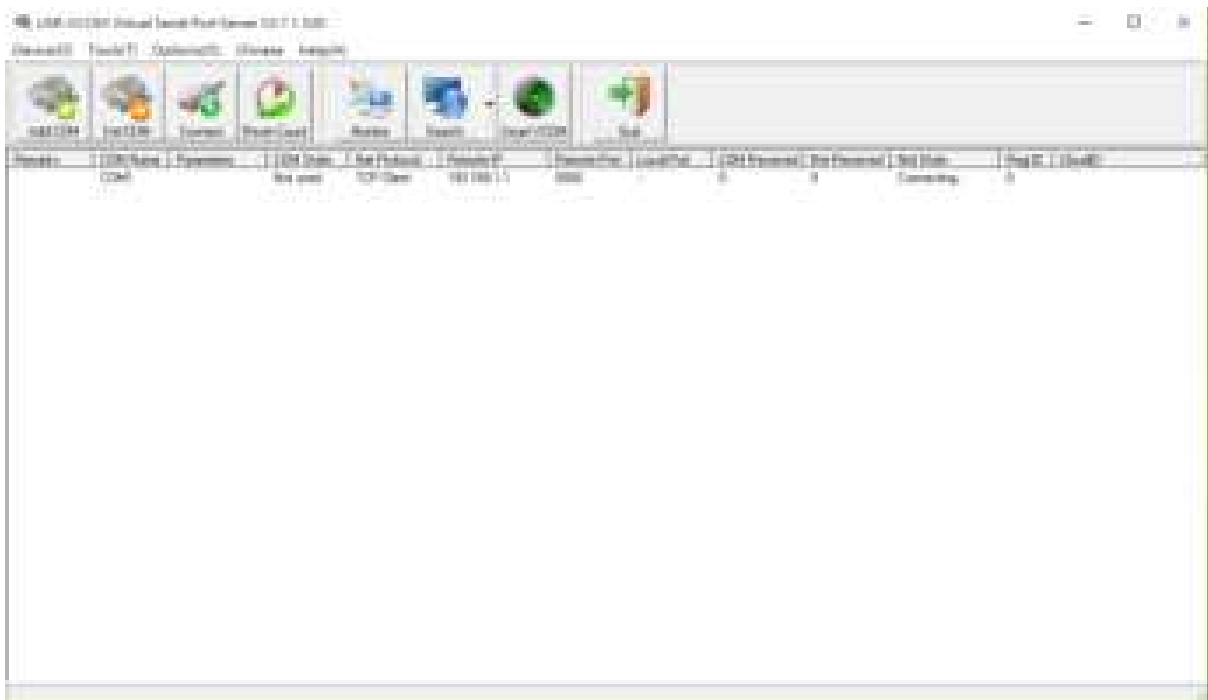
You can click the **Edit** button to configure COM2 setting. The configuration UI shows the following picture.

The screenshot shows a configuration page for COM ports. It is divided into two main sections: 'Serial COM' and 'Virtual COM'.
 In the 'Serial COM' section, there are several dropdown menus: 'Baud Rate' is set to 115200, 'Data' to 8 bit, 'Parity' to none, 'Stop' to 1 bit, and 'Flow Control' to none. Below these is a checkbox for 'Inconsistent' which is checked.
 In the 'Virtual COM' section, there are three dropdown menus: 'Mode' is set to Server, 'Protocol' is set to TCP, and 'Redirect Port' is set to 6000.
 At the bottom right of the form, there is a blue 'Save' button.

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.



16.5 Virtual COM > Remote Alarm



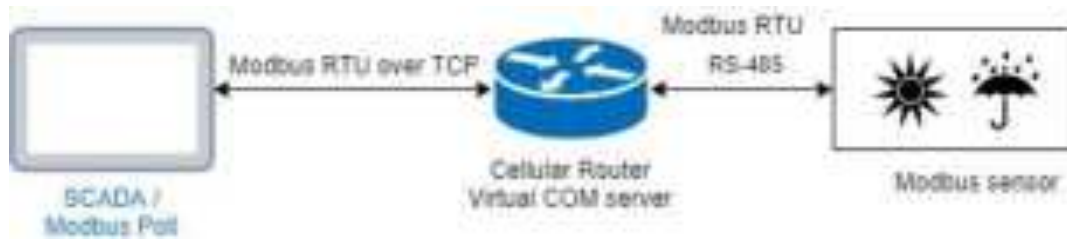
When the router connected with the alarm device, the alarming data from the device can be forwarded by the router to the warning center. Same as the remote management, the serial settings of connected COM port need to be configured properly. And the virtual should be opened and run as **Client** mode.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

The web UI of router shows the below picture.

Virtual COM Ports Config	
Baud Rate	115200
Data	8 bit
Parity	none
Stop	1 bit
Flow Control	none
Use Console?	<input type="checkbox"/>
Virtual COM	
Mode	Client
Host Address	192.168.1.2
Protocol	TCP
Remote Port	8080
<input type="button" value="Save"/>	

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

16.6 Virtual COM > Modbus RTU over TCP



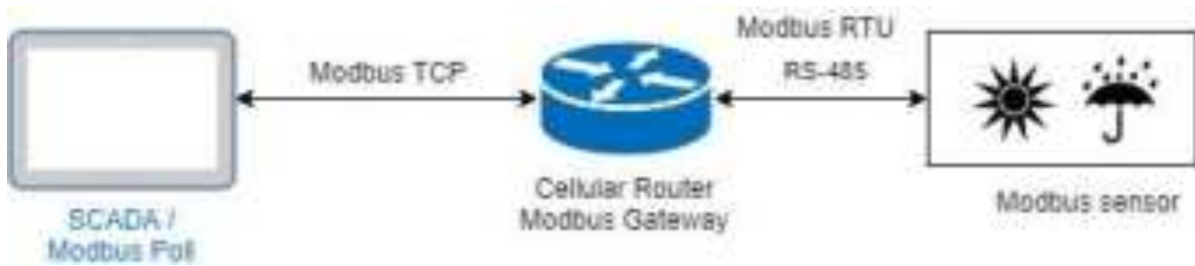
For the industrial products, the Modbus protocol is the most popular industrial control protocol.

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

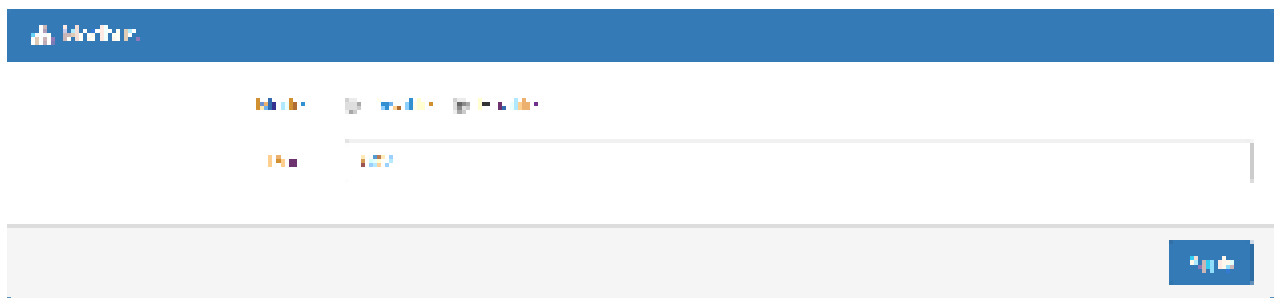
Edit COM Ports Entry #0	
Baud Rate	9600
Data	8 bit
Parity	none
Stop	1 bit
Flow Control	none
<input type="checkbox"/> In Control?	
Virtual COM	
Mode	Server
Protocol	TCP
Redirect Port	8001
<input type="button" value="Save"/>	

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

16.7 Modbus Gateway



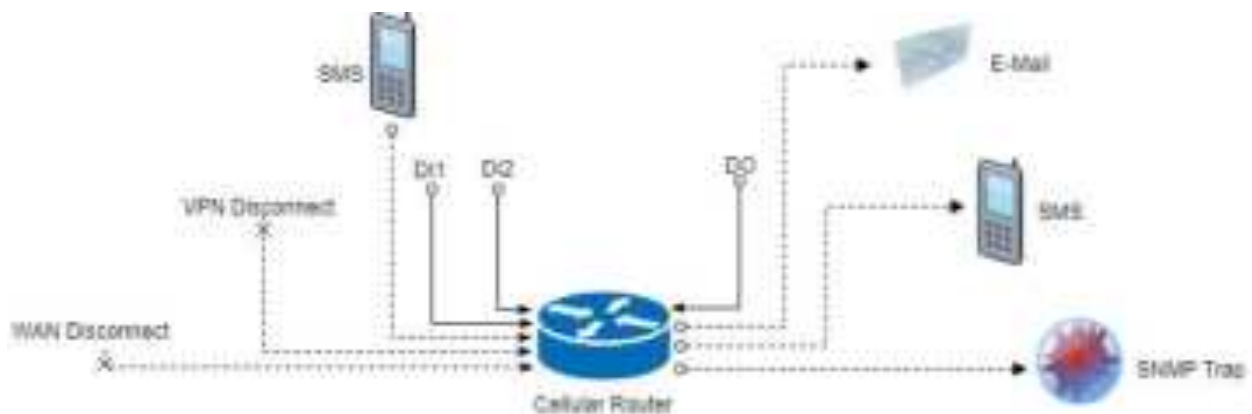
The Modbus gateway feature of router could convert the Modbus TCP to the Modbus RTU protocol and send it to the connected RS-485 device. This feature depends on the COM3 setting, you need to configure the serial setting in the **System -> COM ports** web UI and set up this feature in the **System ->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



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

16.8 Alarm Configuration

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



(1) Alarm Input:

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

(2) Alarm Output:

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

The screenshot shows the 'Alarm' configuration page. At the top, there is a 'Mode' section with radio buttons for 'Disable' and 'Enable'. Below this are several sections for configuring alarm inputs and outputs. The 'Alarm input' section includes checkboxes for 'SMS', 'DI 1', 'DI 2', 'VPN disconnect', 'WAN disconnect', 'LAN disconnect', and 'Reboot'. The 'Alarm output' section includes checkboxes for 'SMS', 'DO', 'SNMP trap', and 'E-mail'. There are also sections for 'DI 1 Trigger' and 'DI 2 Trigger' with radio buttons for 'High' and 'Low', and a 'DO behavior' section with radio buttons for 'Always' and 'Pulse'. A text input field for 'SMS/E-mail' is present with a placeholder 'Limit 100 english characters'. A hint below the field reads 'Hint: for SMS/E-mail only accept trusted and on duty members'. An 'Apply' button is located at the bottom right.

The screenshot shows the 'SNMP' configuration page. At the top, there is a 'Mode' section with radio buttons for 'Disable' and 'Enable'. Below this are three tabs: 'Community', 'SNMP v1 User Configuration', and 'SNMP trap Configuration'. The 'SNMP trap Configuration' tab is active. It contains a table with the following columns: '#', 'Mode', 'Community name', and 'Destination'. There are two rows in the table, both with 'Disable' in the 'Mode' column and 'public' in the 'Community name' column. The 'Destination' column is empty. An 'Apply' button is located at the bottom right.

#	Mode	Community name	Destination
1	Disable	public	
2	Disable	public	

16.9 Open VPN Configuration

Generic setup

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

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

16.9.1 Open VPN Server Mode

Open VPN server certificate generation

Server - Server Security

Root CA	<input type="button" value="Create"/>
Cert, Key	<input type="button" value="Create"/>

Server - User Security

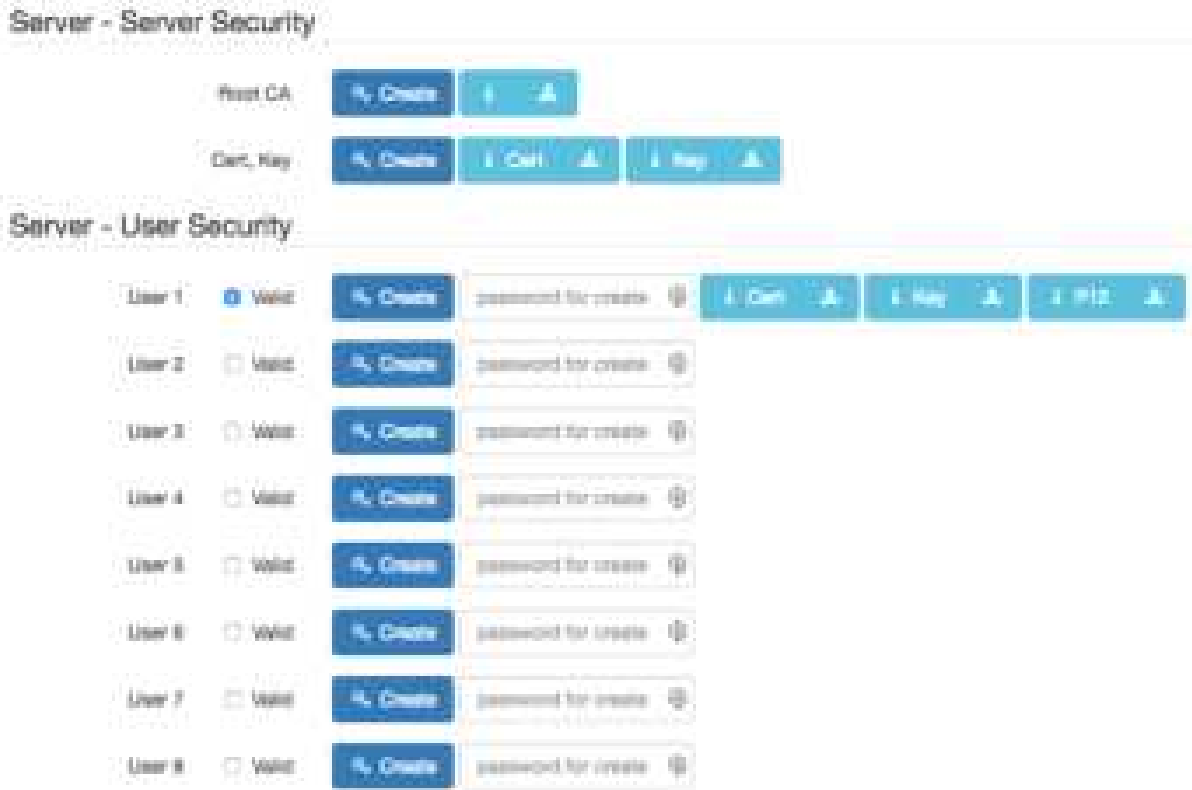
User 1	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="password" value="password for create"/>
User 2	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="password" value="password for create"/>
User 3	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="password" value="password for create"/>
User 4	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="password" value="password for create"/>
User 5	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="password" value="password for create"/>
User 6	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="password" value="password for create"/>
User 7	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="password" value="password for create"/>
User 8	<input type="checkbox"/> Valid	<input type="button" value="Create"/>	<input type="password" value="password for create"/>

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

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

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

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



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

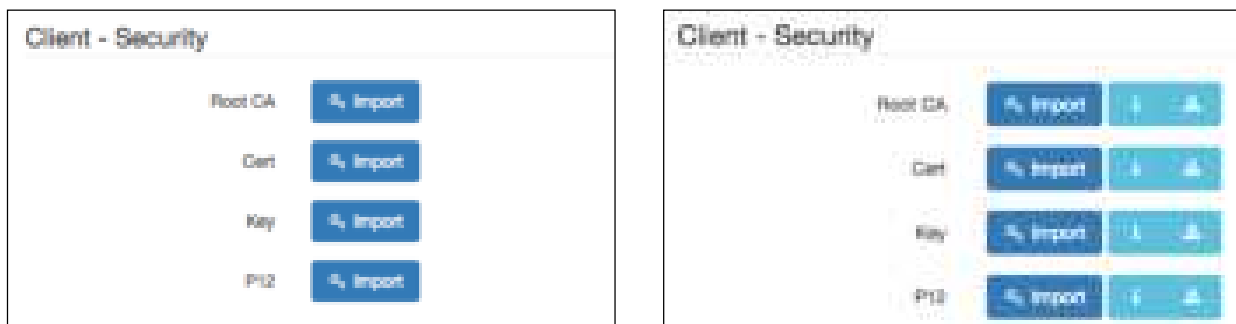
16.9.2 Open VPN Client Mode

Open VPN client certificate import

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

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

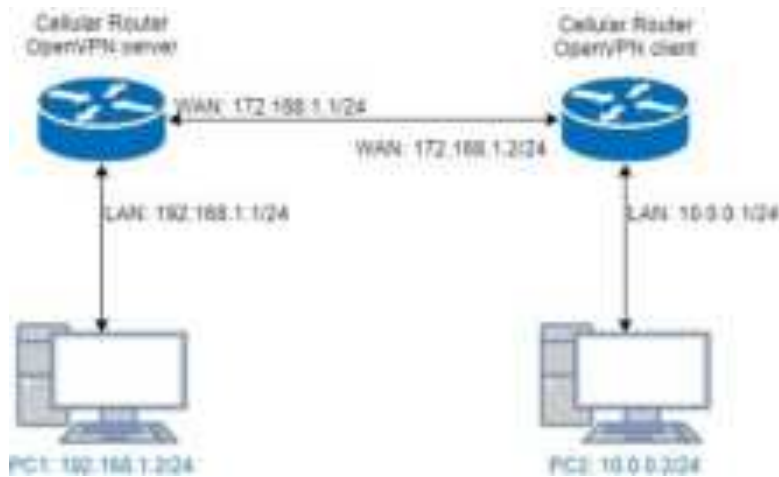
When the files are imported, the web UI is as shown in the right-bottom picture.



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

16.9.3 Open VPN Net-to-Net

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



(1) Open VPN server configuration

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

The screenshot shows the configuration page for an OpenVPN server. The settings are as follows:

- Mode: Server
- VPN mode: Server
- TLS mode: Disable
- TLS protocol version: 1.2
- Cipher: BF CBC
- Status: Running
- Device: TUN
- Protocol: UDP
- Port: 1194
- VPN Compressor: Disable
- Authentication: Certificate
- Server section:
 - Client mode: Roadwarrior
 - VPN network: 192.168.20.0
 - VPN netmask: 255.255.255.0
- Roadwarrior section:
 - Route Client Networks: On
 - Connection - nat / Mask: 10.0.0.0 / 255.255.255.0

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

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

When PC1 and PC2 communicate each other, the Route Client Networks should be enabled.

And add the LAN information of Open VPN client side, in this case the **#1** route will be **10.0.0.0** and **255.255.255.0**

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

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

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

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



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

(2) Open VPN client configuration

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

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

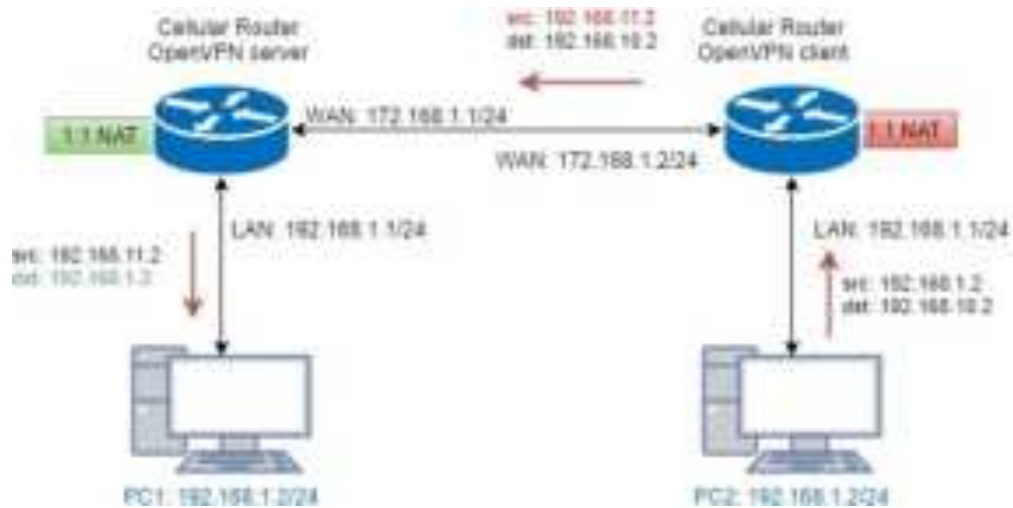
This option requires the P12 file which generated from Generic Setup Open VPN server part.

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

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

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

16.9.4 Open VPN 1:1 NAT



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

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

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

Roadwarrior

Route Client Networks: Off On

Connections: Nat / Mode

#1	192.168.1.0	255.255.255.0
#2	0.0.0.0	0.0.0.0
#3	0.0.0.0	0.0.0.0
#4	0.0.0.0	0.0.0.0
#5	0.0.0.0	0.0.0.0
#6	0.0.0.0	0.0.0.0
#7	0.0.0.0	0.0.0.0
#8	0.0.0.0	0.0.0.0

NAT

1:1 NAT: Off On

Network: 192.168.10.0

Netmask: 255.255.255.0

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

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

Client

Client Mode: Router/Client

Server Address:

PROCID Password:

Route Client Networks: Off On

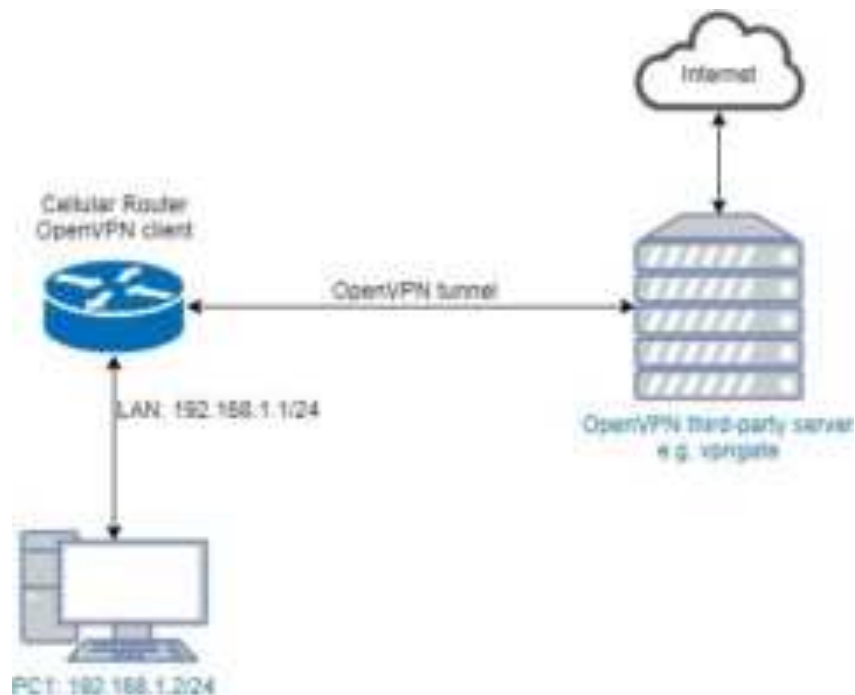
NAT

1:1 NAT: Off On

Network:

Netmask:

16.9.5 Open VPN with third-party server



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

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

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

Firstly, download the ovpn configuration files from [vpngate.net](http://www.vpngate.net).

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



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

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



16.9.6 Install Open VPN Access Server on Docker

Open VPN Access Server on Docker installation

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

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

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

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

Quick Installation

■ Prerequisites

- Ubuntu 16.04
- curl or wget should be installed

Install via curl

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

Install via wget

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

Install Docker on Ubuntu 16.04 64bit

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

Set up the repository

```
sudo apt-get remove docker docker-engine docker.io
```

```
sudo apt-get update
```

```
sudo apt-get install \
```

```
    apt-transport-https \
```

```
    ca-certificates \
```

```
    curl \
```

```
    software-properties-common
```

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
```

```
sudo add-apt-repository \
```

```
    "deb [arch=amd64] https://download.docker.com/linux/ubuntu \
```

```
    $(lsb_release -cs) \
```

```
    stable"
```


Install Docker CE

```
sudo apt-get update
```

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

Install Open VPN Access Server by docker image

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

```
sudo mkdir -p /Open_VPN-as
```

```
sudo docker create --name=Open_VPN-as \
```

```
    -v /Open_VPN-as:/config \
```

```
    -e TZ="Asia/Taipei" \
```

```
    -e INTERFACE=enp3s0 \
```

```
    --net=host --privileged linuxserver/Open_VPN-as
```

```
sudo docker start Open_VPN-as
```

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

Setup Open VPN Access Server for Cellular Router

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

The default administrator username and password is admin/password.

Login page:



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



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



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

User Permissions

Search By Username/Group (use * for wildcard)

Username	Group	More Settings	Admin	Allow Auto-Login	Deny Access	Delete
admin	No Default Group	<input type="button" value="More"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
New Username: test	No Default Group	<input type="button" value="More"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Local Password: test **4.**

Select IP Addressing: Use Dynamic Use Static

Access Control: Use NAT Use routing

Select addressing method:

Allow Access To these networks:

Allow Access From:

Allow Access From: **5.** all other VPN clients

VPN Gateway: No Yes

DMZ settings: No Yes

Configure DMZ IP address: No Yes

Require user permissions record for VPN access

6.

User Permissions Changed

User 'test' added.

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

7.

Setup Cellular Router Open VPN client



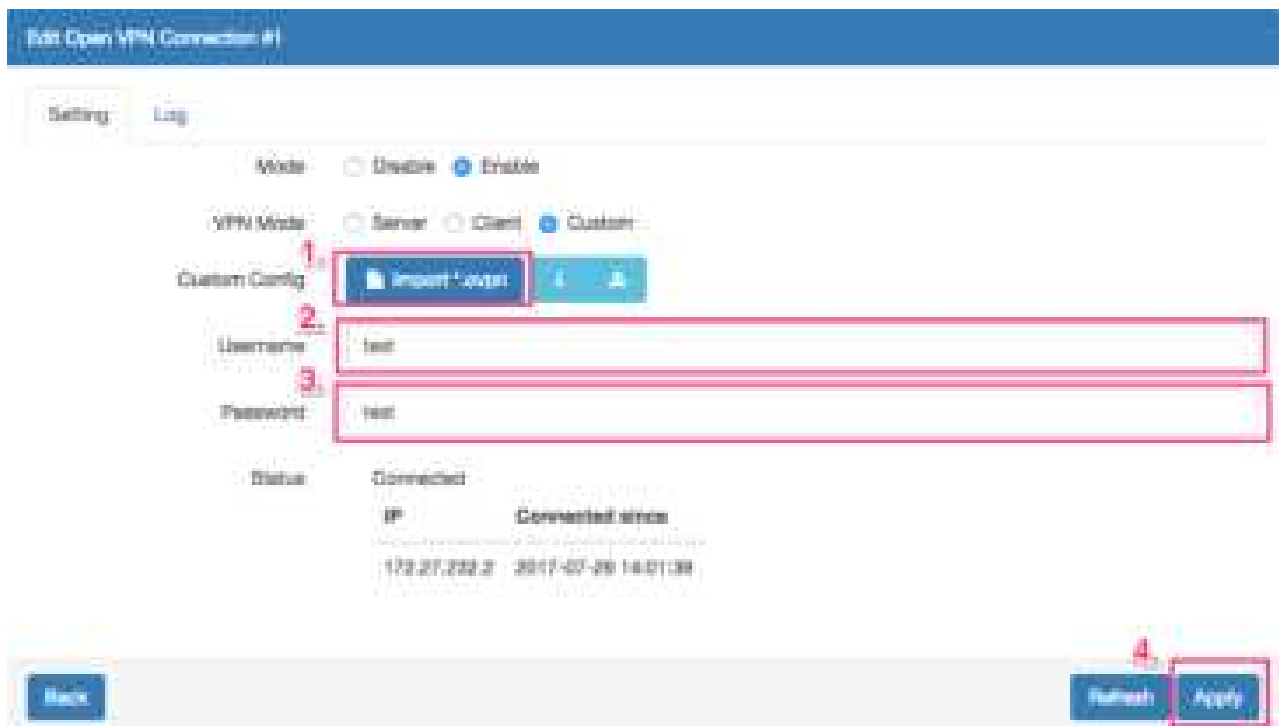
The image shows the OpenVPN login interface. At the top is the OpenVPN logo. Below it are two input fields: 'Username' with the text 'test' and 'Password' with four asterisks. At the bottom right, there are two buttons: 'Login' and 'Go'. The 'Login' button is highlighted with a red box.

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

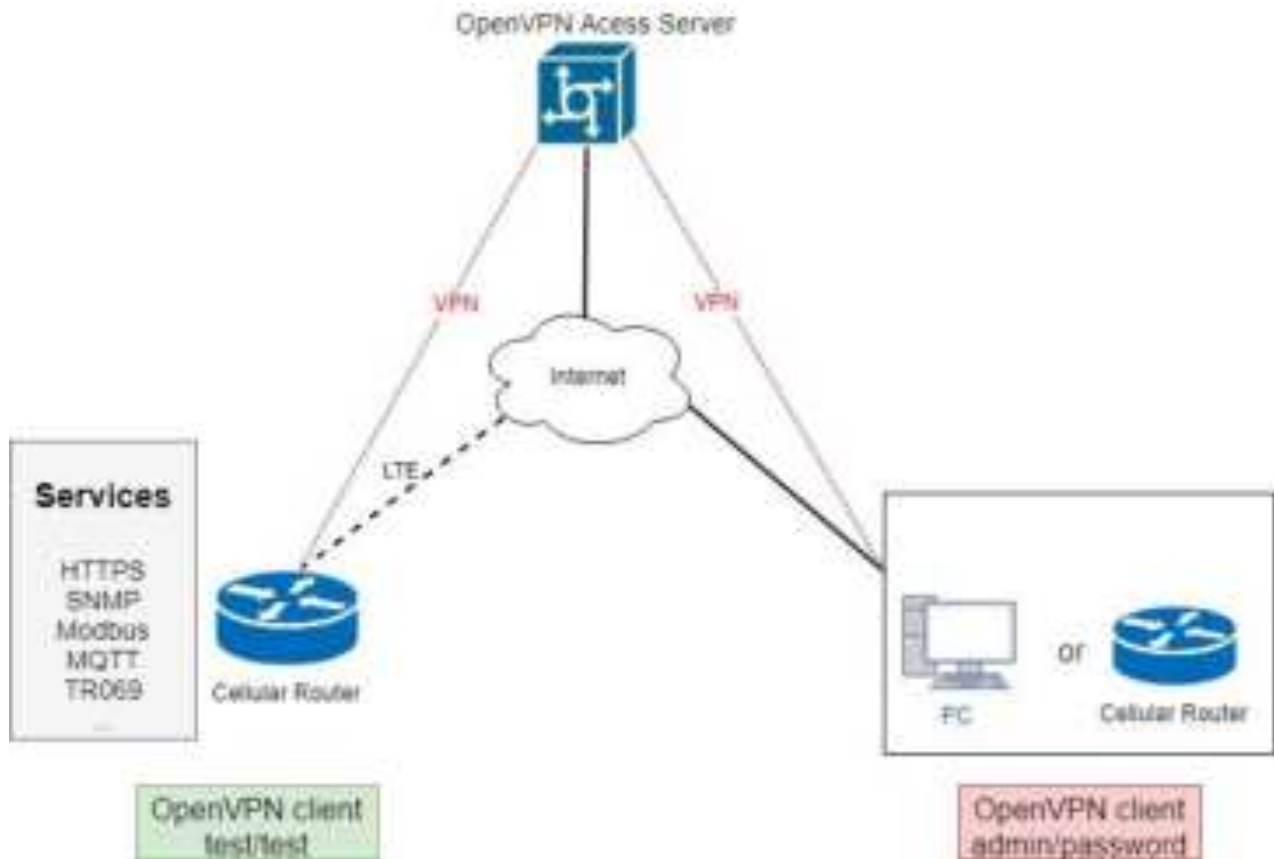
Please make sure to change the type from Connect to Login.



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



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



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

16.9.7 Install Pritunl Open VPN server on Docker

Pritunl Open VPN server on Docker installation

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

Quick Installation

■ Prerequisites

- Ubuntu 16.04
- curl or wget should be installed

■ Install via curl

```
sh -c "$(curl -fsSL https://bit.ly/2lpJN1X)"
```

■ Install via wget

```
sh -c "$(wget https://bit.ly/2lpJN1X -O -)"
```

Install Docker on Ubuntu 16.04 64bit

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

Set up the repository

```
sudo apt-get remove docker docker-engine docker.io
```

```
sudo apt-get update
sudo apt-get install \
    apt-transport-https \
    ca-certificates \
    curl \
    software-properties-common
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
sudo add-apt-repository \
    "deb [arch=amd64] https://download.docker.com/linux/ubuntu \
    $(lsb_release -cs) \
    stable"
```

Install Docker CE

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

Install Docker compose

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

Install Pritunl Open VPN Server by docker compose

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

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

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

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

- "443:443/tcp"

volumes:

mongo:

pritunl:

(3) Run the command `docker-compose up -d` to start the server

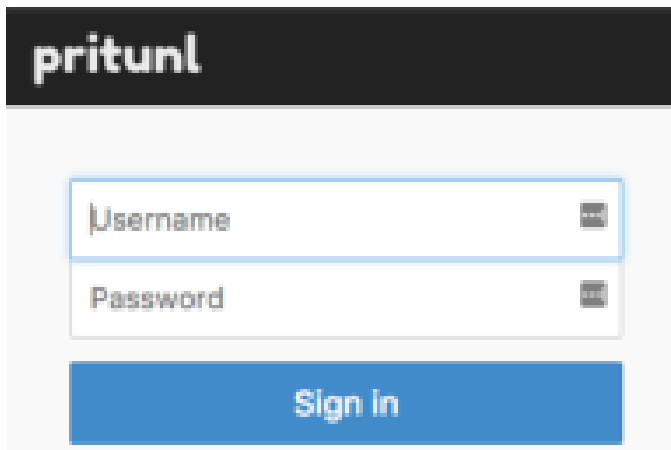
(4) Check the Pritunl Open VPN Server by visiting `https://<server_ip_or_domain>`

Setup Pritunl Open VPN Server for Cellular Router

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

The default username/password is pritunl/pritunl.

Login Page:



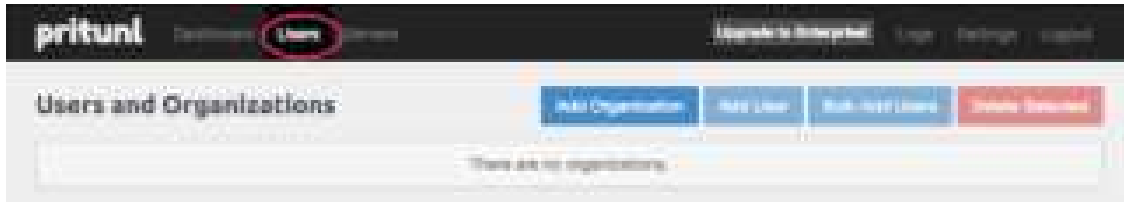
After logged, the server will ask you to do the initial setup. You can change the username and the password setting in this page.

Initial Setup:



Open VPN user setup

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



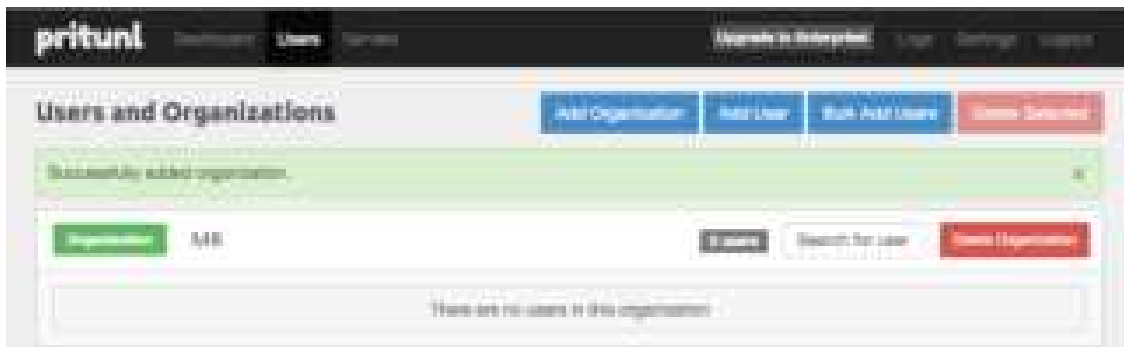
Add the organization by click the Add Organization button.

Add Organization

Name Name of organization

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

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



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

Add User

Name

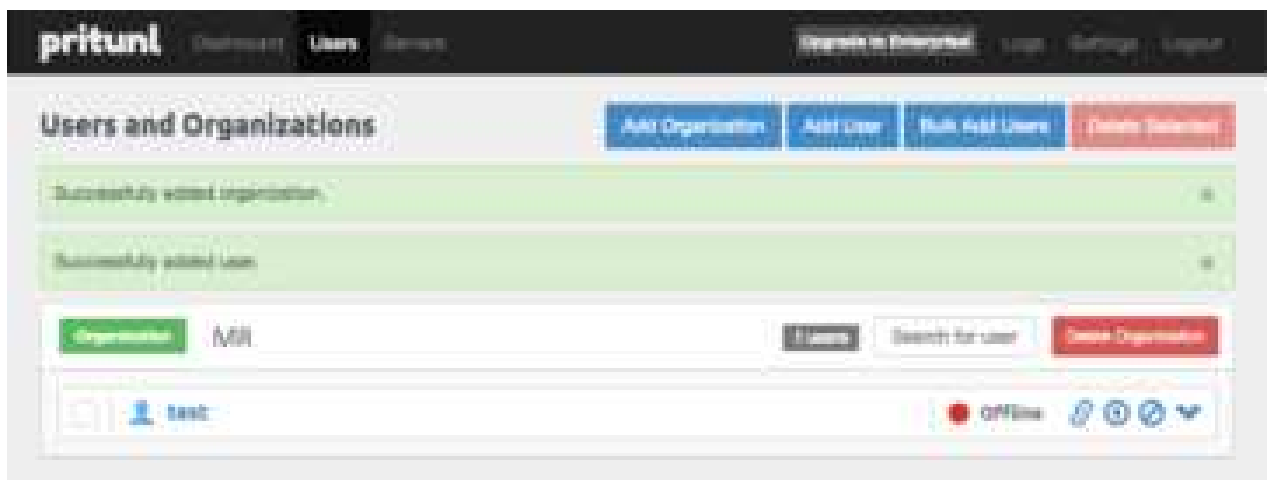
Select an organization

Email (optional)

Pin

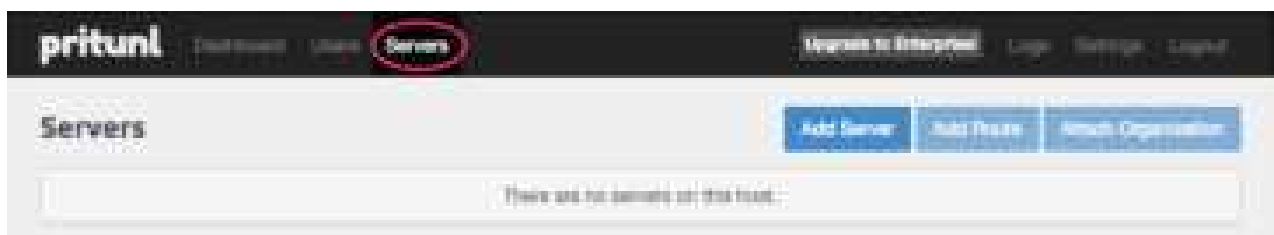
Note: In this Open VPN server, the PIN must contain only digits.

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



Open VPN server setup

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

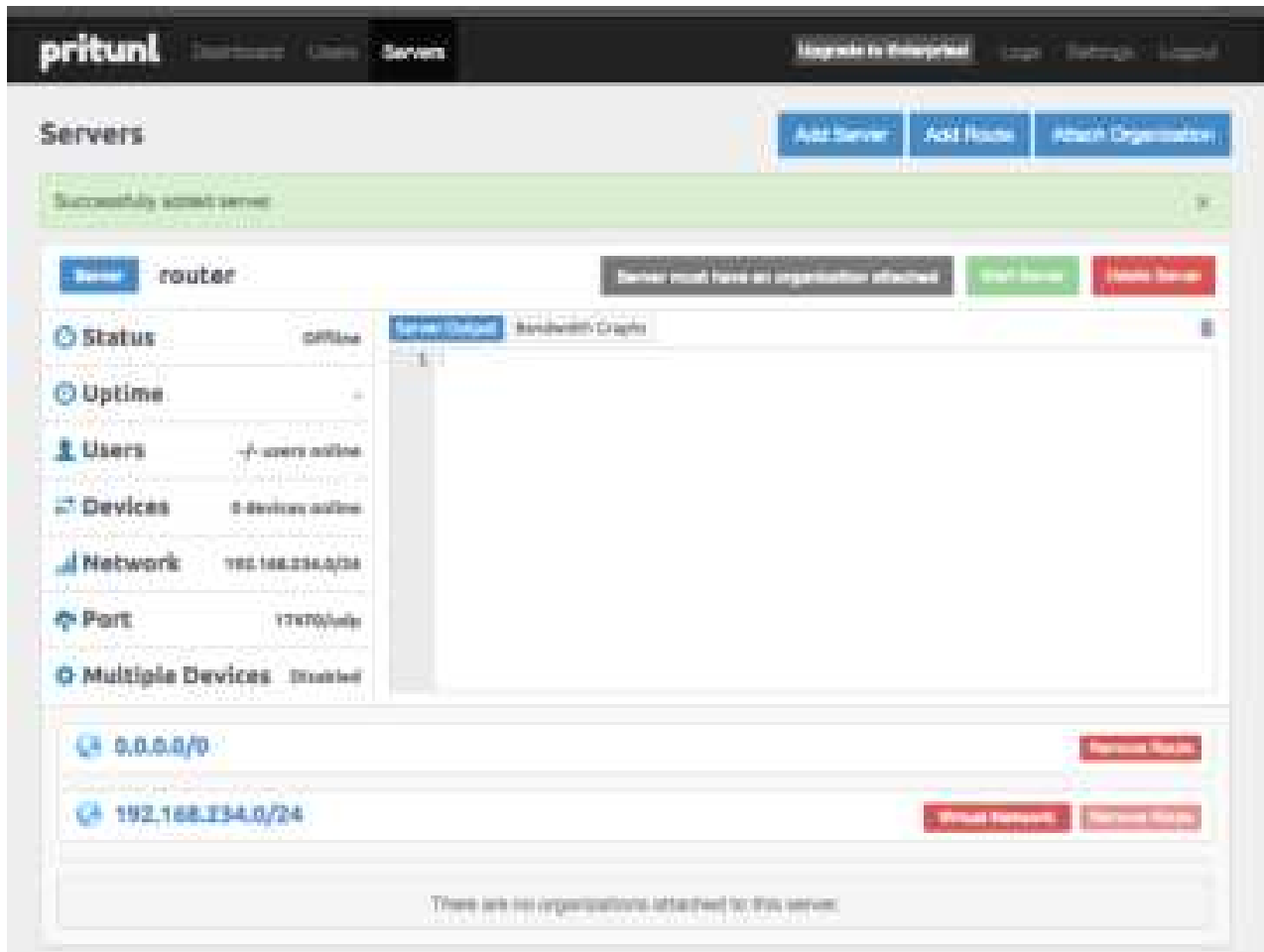


And click the Add Server button to create the Open VPN server.

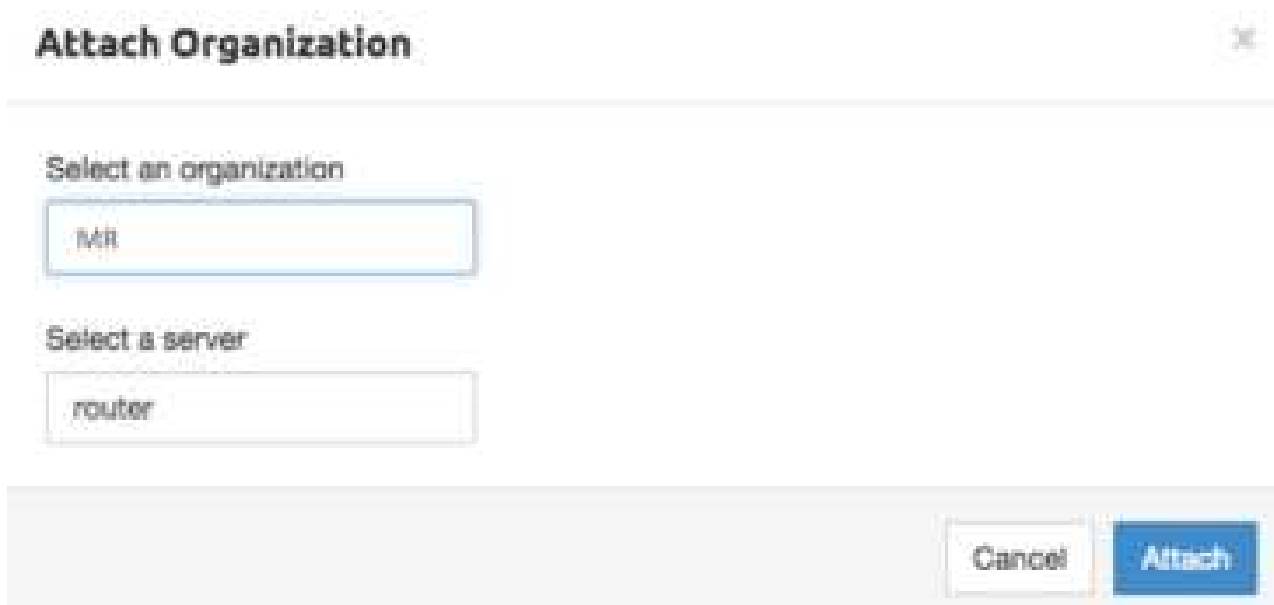


Note: Please click the Advanced tab and make sure the Inter-Client Communication be checked

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



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

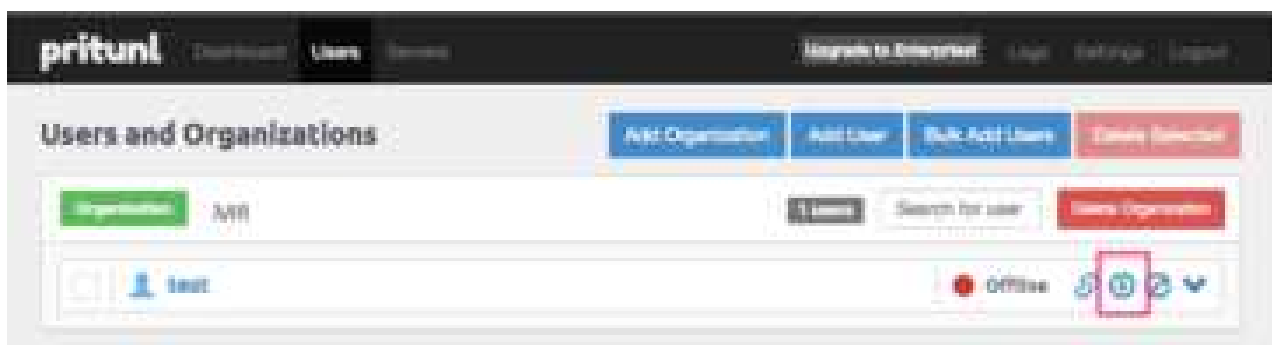


Start the Open VPN server by click Start Server button.



Cellular Router setup

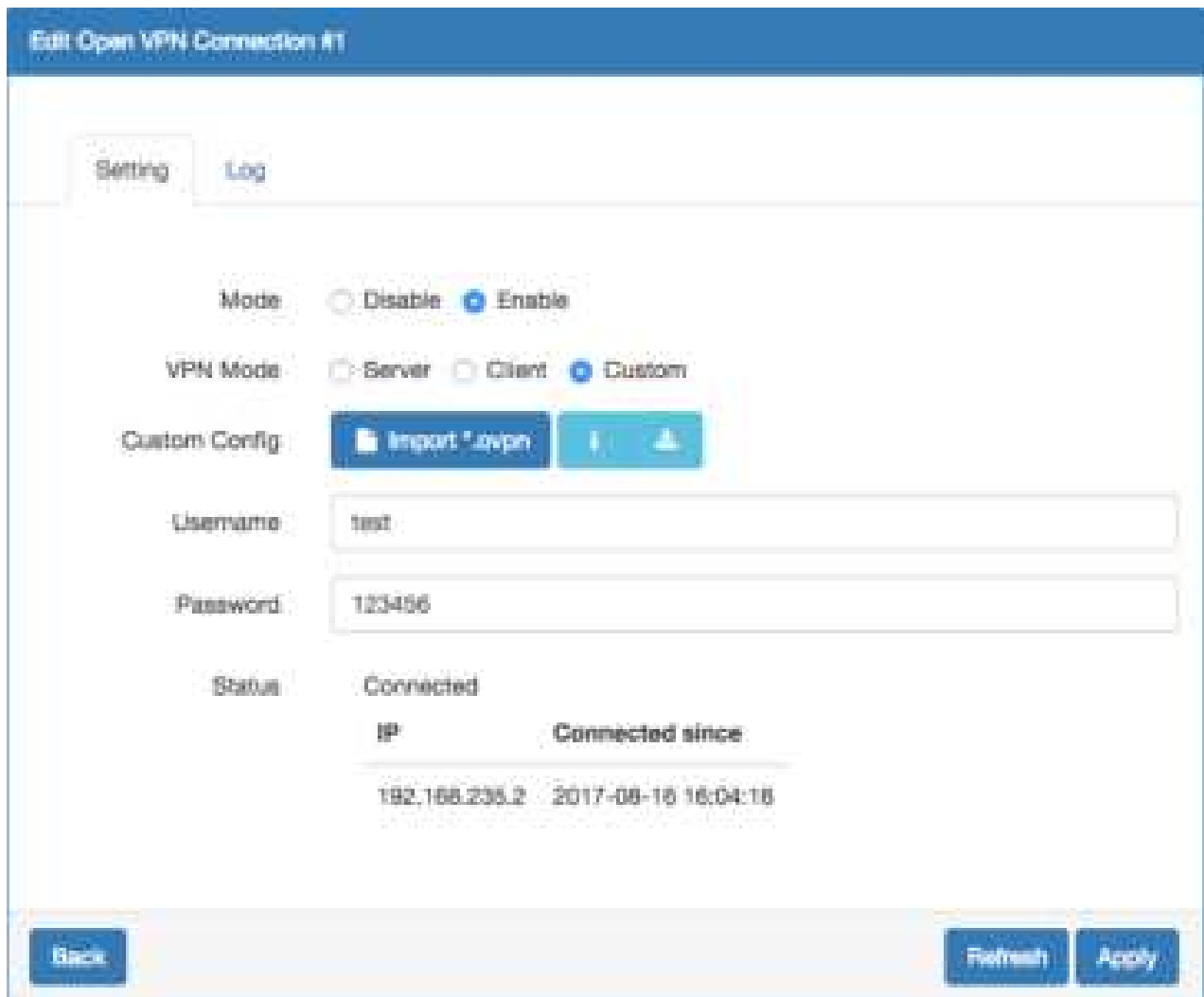
First, please navigate to the Users page and download the user configuration file and extract it.



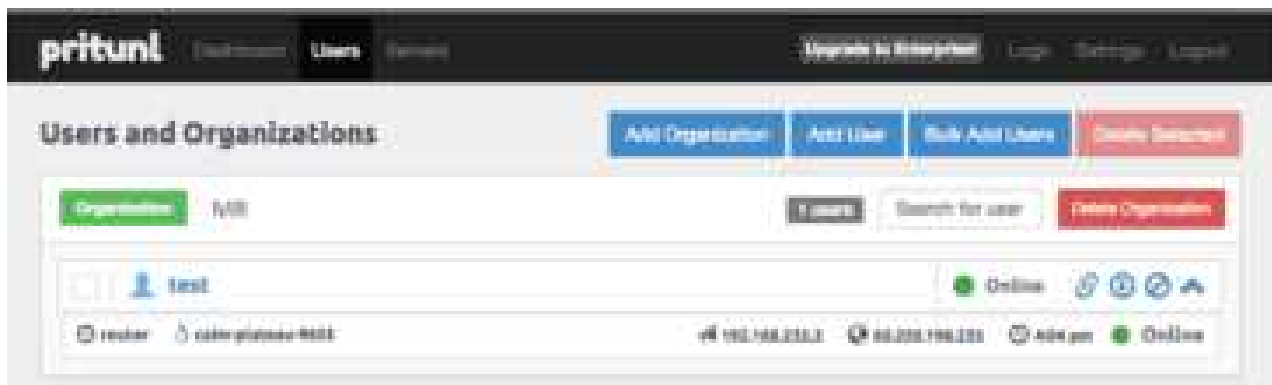
Note: In this document, you should get the MR_test_router.ovpn file.

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

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

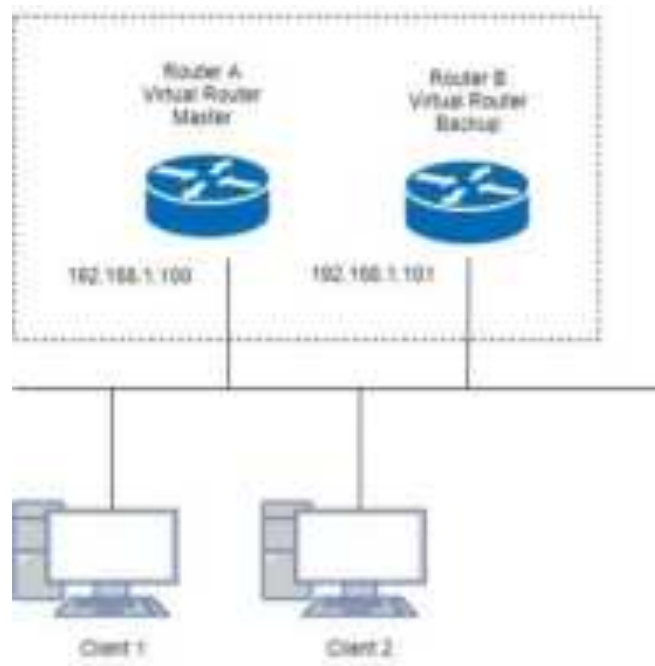


When the Cellular Router Open VPN connected, the Prituni Open VPN server also update the user status.



16.10 VRRP Topology

Basic VRRP Topology



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

16.11 TR069 Server (GenieACS Installation)

Server OS: Ubuntu 14.04 on Virtualbox

Installation:

- 1) Login ubuntu
- 2) Change to root by 'su -' and enter your root password.
- 3) Install required package as below command:
>apt install gcc openssl-devel zlib-devel readline-devel sqlite-devel
- 4) Make a directory for application installation
>mkdir /opt
- 5) Install yaml
cd /opt
wget <http://pyyaml.org/download/libyaml/yaml-0.1.7.tar.gz>
tar xvzf yaml-0.1.7.tar.gz
cd yaml-0.1.7
./configure
make && make install
- 6) Install ruby
cd /opt
wget <http://cache.ruby-lang.org/pub/ruby/2.4/ruby-2.4.1.tar.gz>
tar xvzf uby-2.4.1.tar.gz
cd ruby-2.4.1

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

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

7) Install node.js

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

8) Install redis

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

9) Install mongodb

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

10) Install genieACS

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

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

Original configuration:

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

New configuration example.:

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

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

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

Original configuration:

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

New configuration example:

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

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

11) Install genieACS-Gui

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

```
gem install json  
bundle update
```

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

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

GenieACS startup script:

```
#!/bin/sh
```

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

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

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

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

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

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

GenieACS stop:

Ctrl-C

Usage:

1) Device Configuration

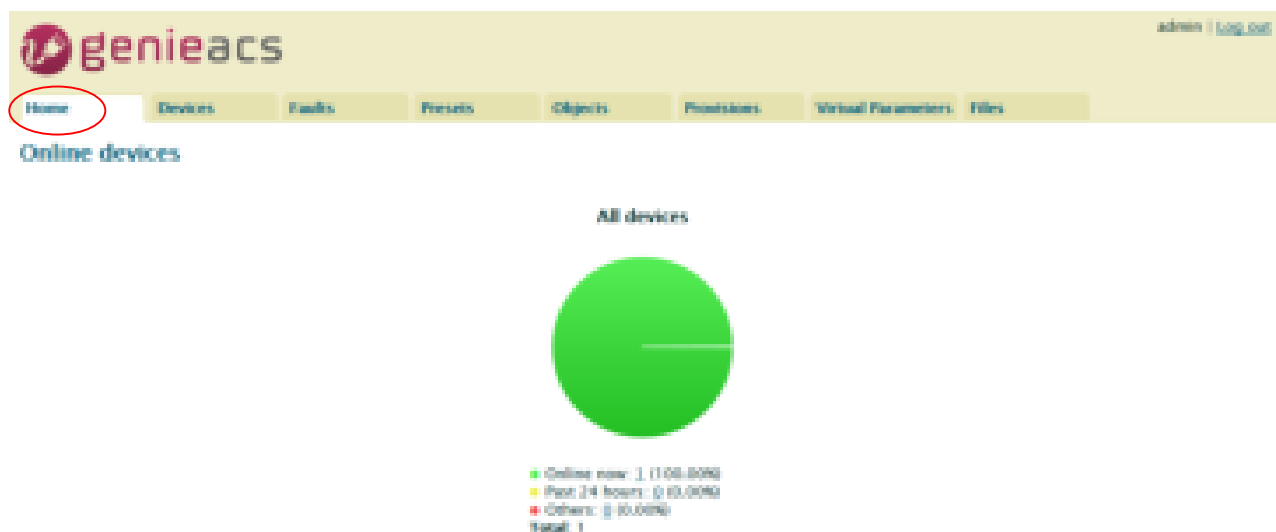
Fill in the ACS URL field as http://GenieACS server IP:**7547**

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

2) GenieACS Operation

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

Press Home tab to refresh Online devices status.



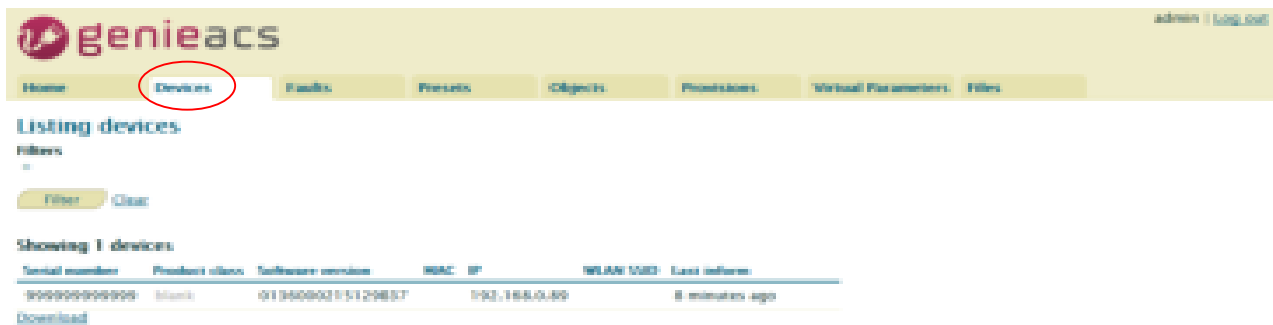
2.1) Login

Username and Password are admin/admin.



3) Device information

Press Devices tab

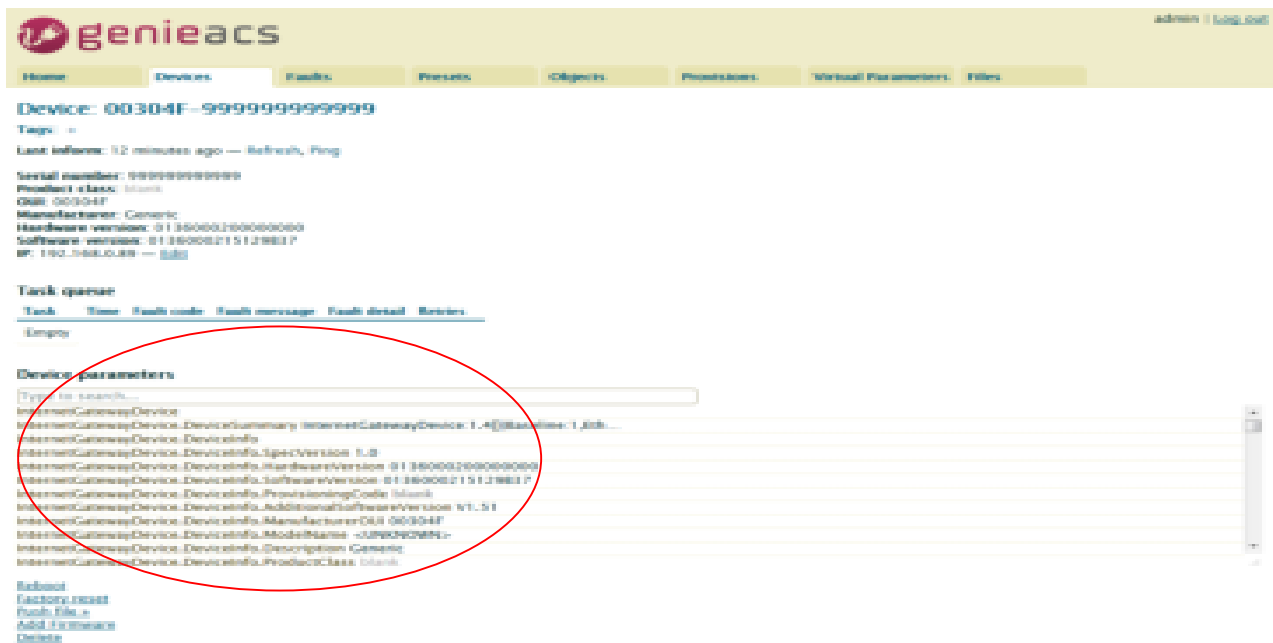


Move mouse to line end of your device, the [Show](#) link show up.

Showing 1 devices

Serial number	Product class	Software version	MAC	IP	WLAN SSID	Last inform
000000000000	blank	0136000215129837	192.168.0.89			8 minutes ago

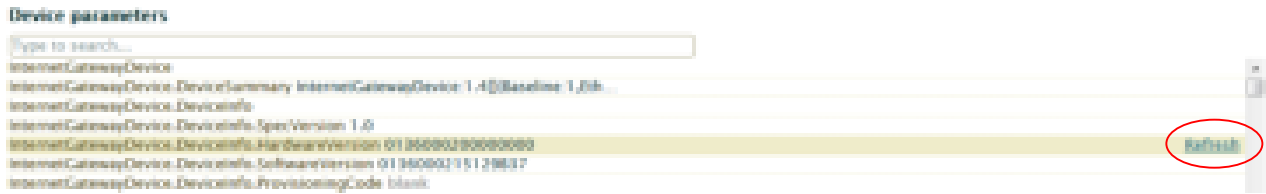
Press [Show](#) link, the device information shows up.



4) Access parameters

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

For Readable parameter

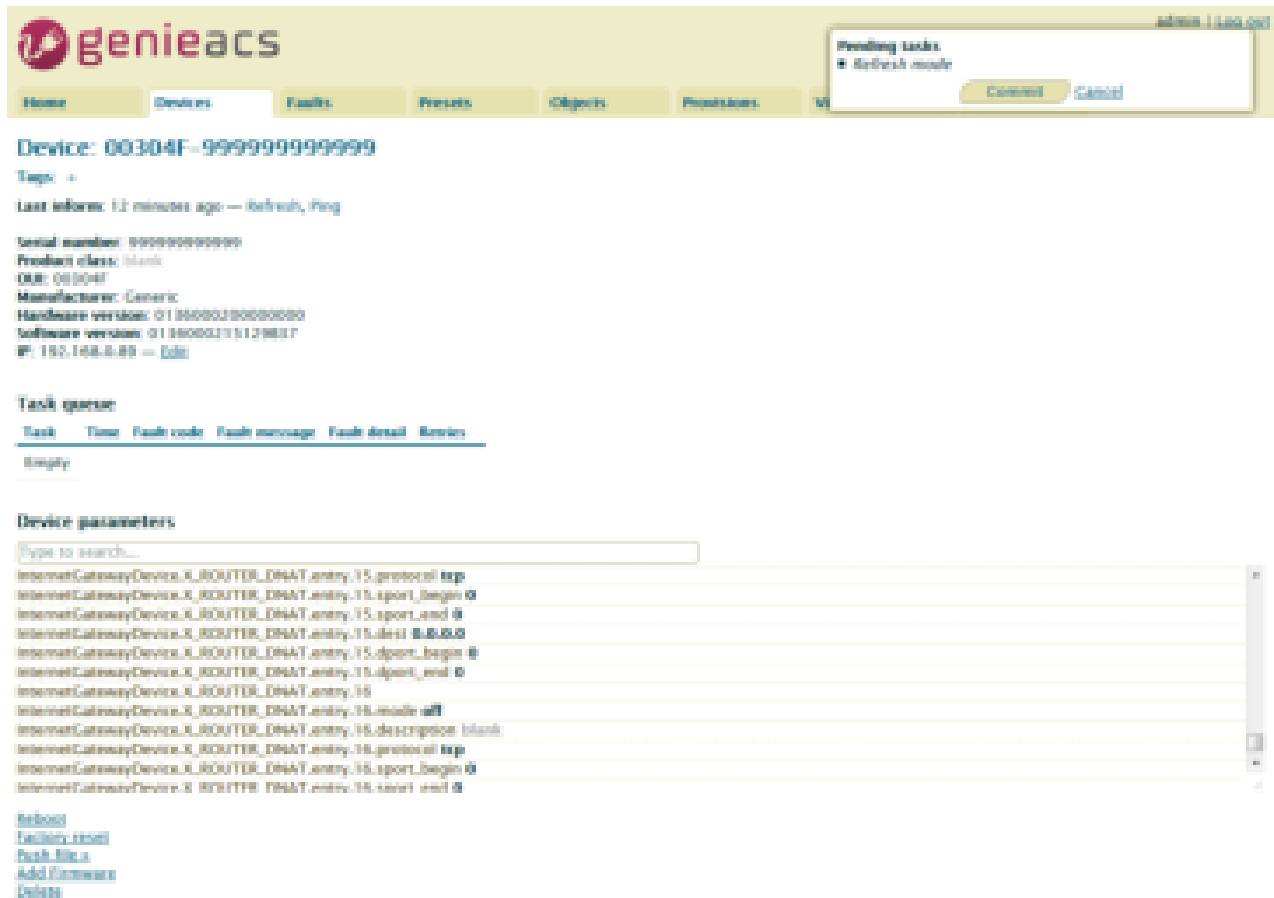


For Readable and Writable parameter



4.1) Get parameter value

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



Press Commit to get this parameter value.

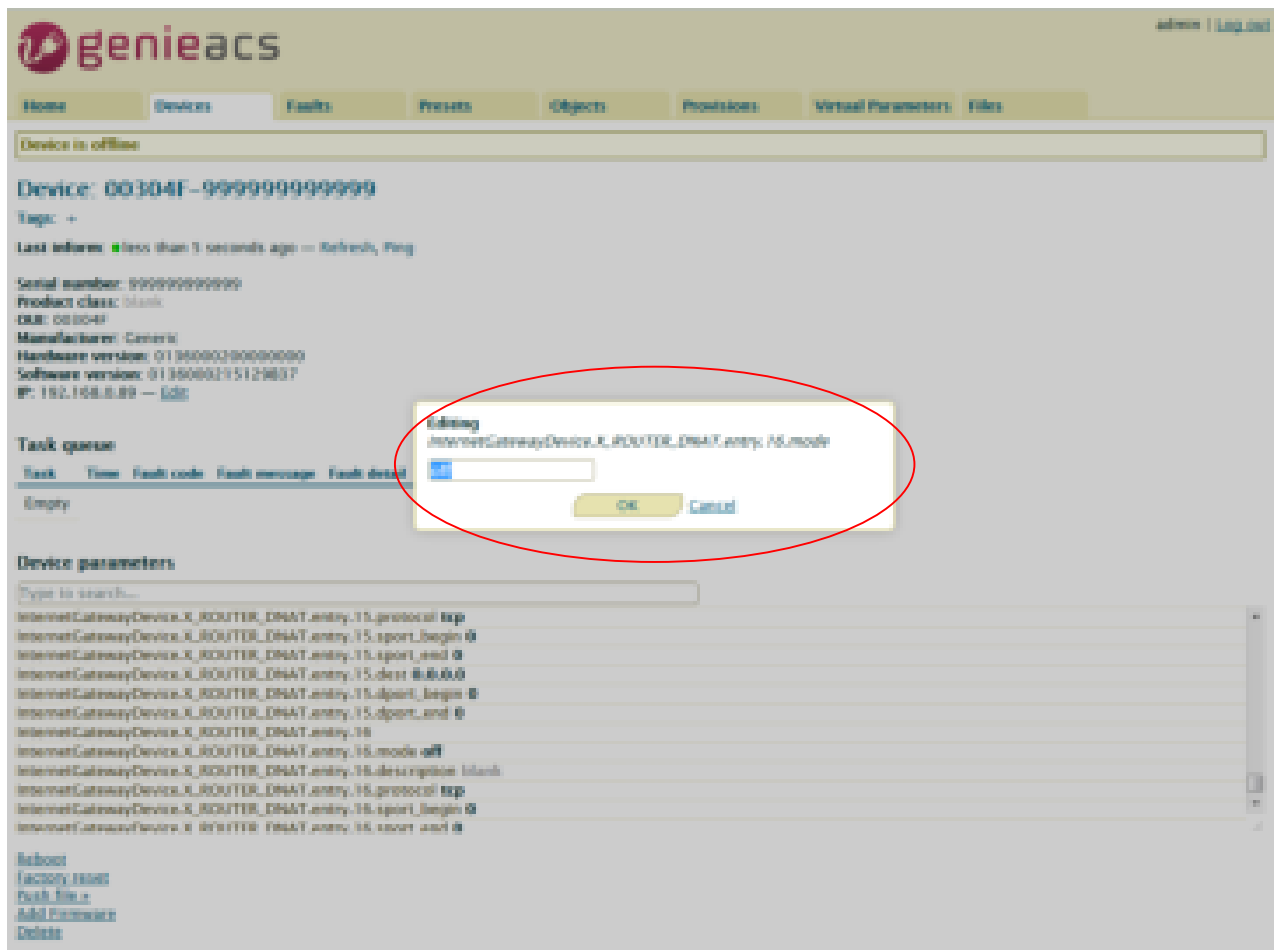
Note: If the GenieACS can reach the device, the parameter value will be updated immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.

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

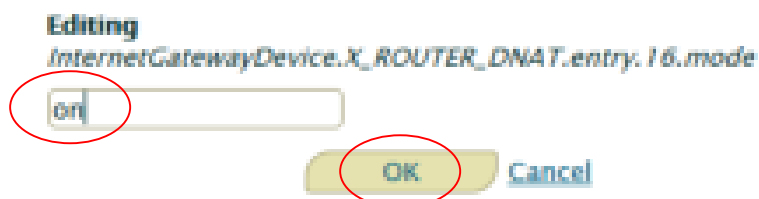
Note: To update partial tree, refresh the parent node of the partial tree.

4.2) Set parameter value

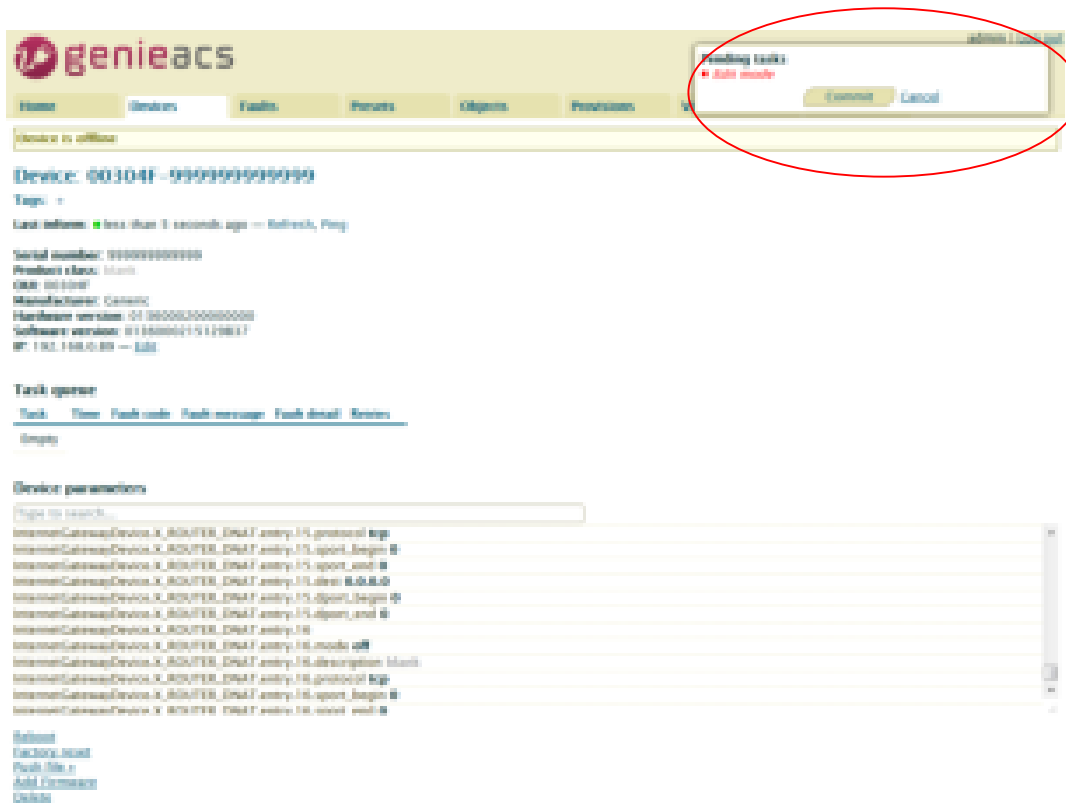
Press on the **Edit** link, editing window will pop up to ask you to change the value of this parameter.



Input new value and press OK.



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



Press Commit to set this parameter value.

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

5) Reboot device

Press on [Reboot](#) link.



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



Press Commit to reboot device.

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

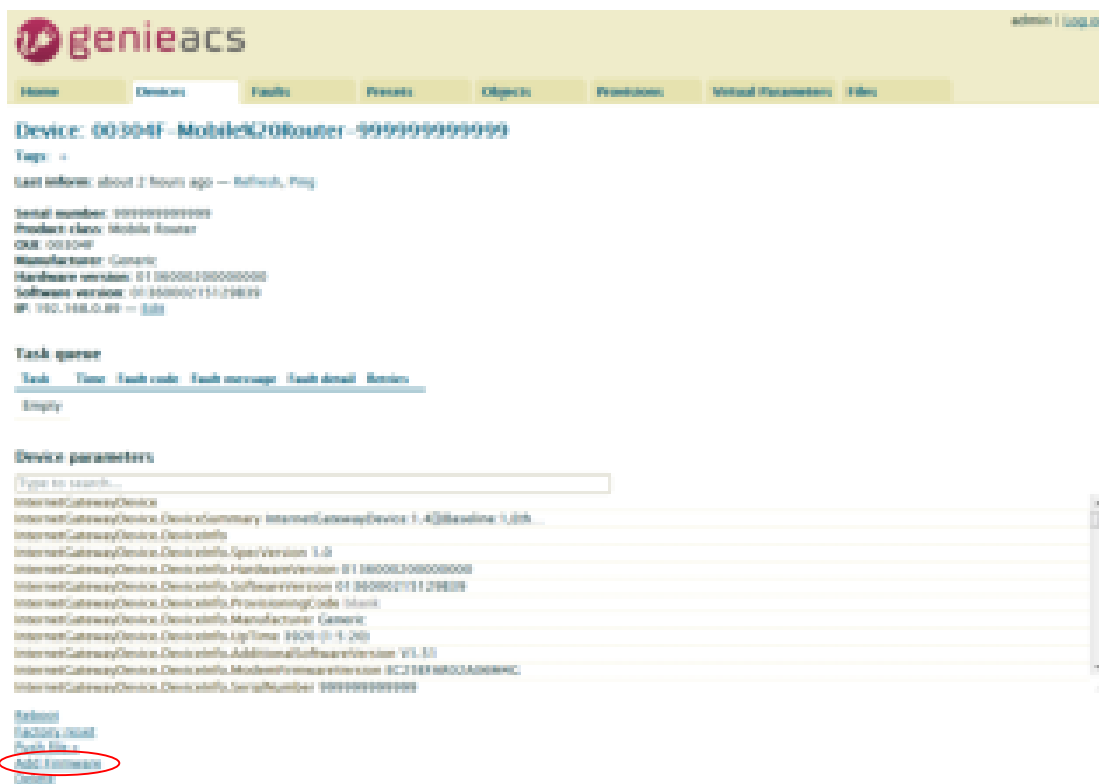
6) Reset to default

Similar to Reboot device except pressing on [Factory reset](#) link.

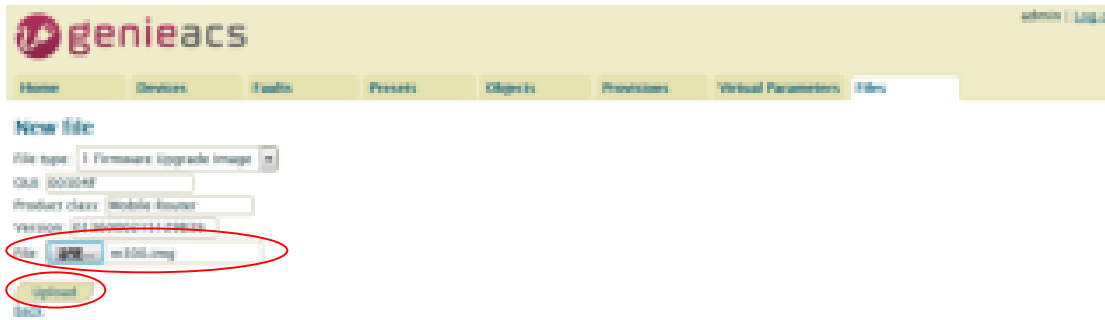
7) Firmware Upgrade

7.1) Upload Firmware

Press [Add Firmware](#) link



The link will redirect to Files tab

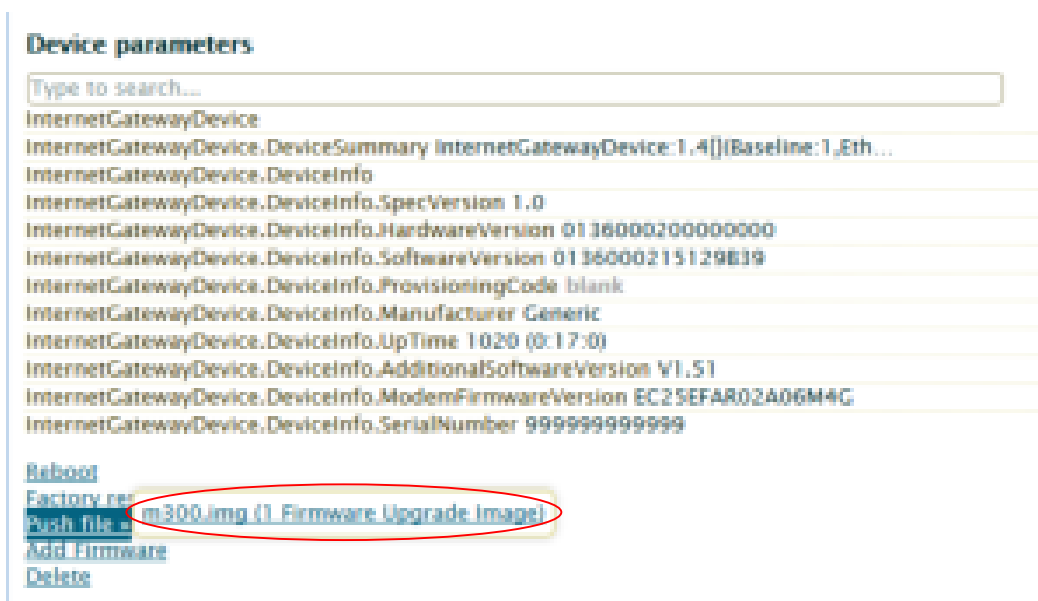


Press File: browse button, select the firmware, and then press Upload button. The firmware will be added to listing files as below.

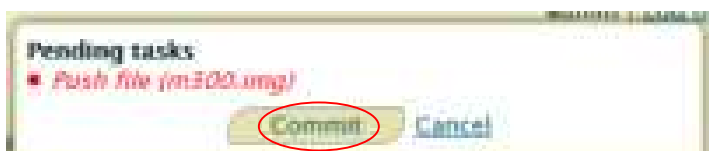


7.2) Upgrade

Move mouse to the [Push file>>](#) link, the upgrade firmware name will pop up as below picture.



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



Press Commit, then firmware upgrade started.

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

17 Test Case Example

17.1 VLAN Topology



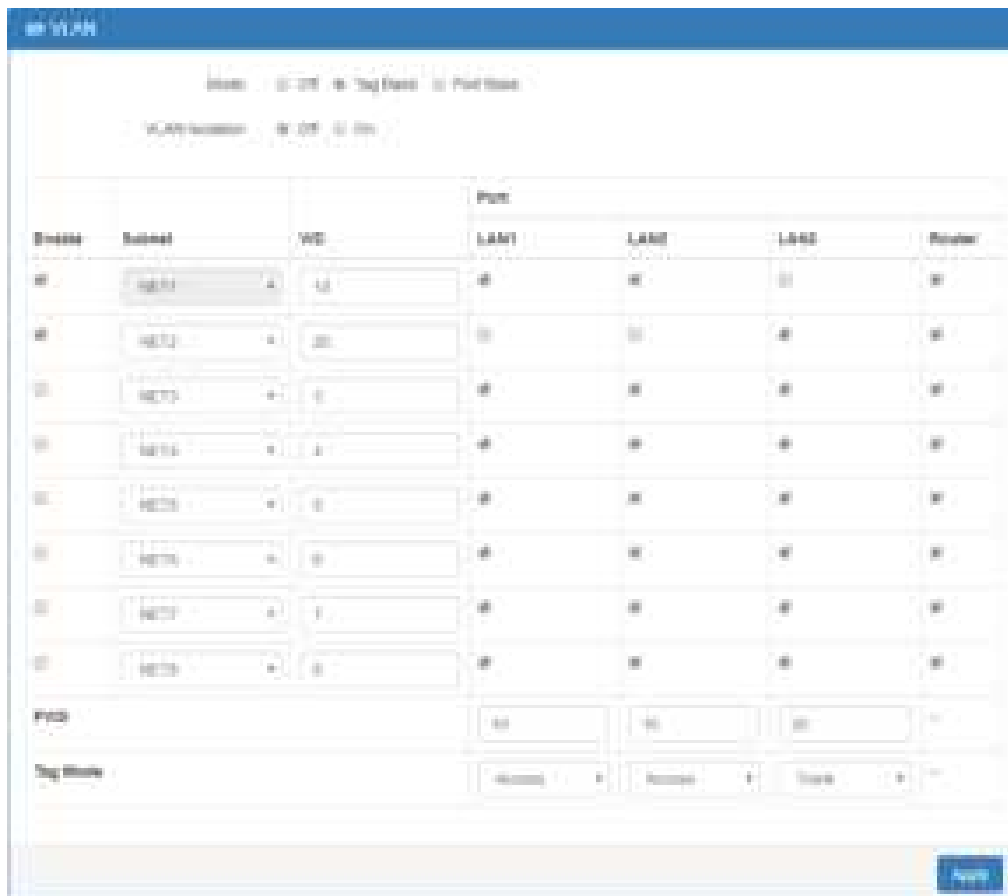
This VLAN Topology for **3-port LANs** shows different PCs how to configure VLAN settings with different LAN ports and has two results for this configuration.

- (1) PC-A sends ICMP packet to PC-B IP (192.168.2.20) and captures traffic on PC-B. Thus, PC-B will receive Tag20 traffic.
- (2) PC-B sends ICMP packet to PC-A IP (192.168.1.20) and captures traffic on PC-A. Thus, PC-A will receive untag traffic.

Note:

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

The following interface shows VLAN settings for the cellular router.

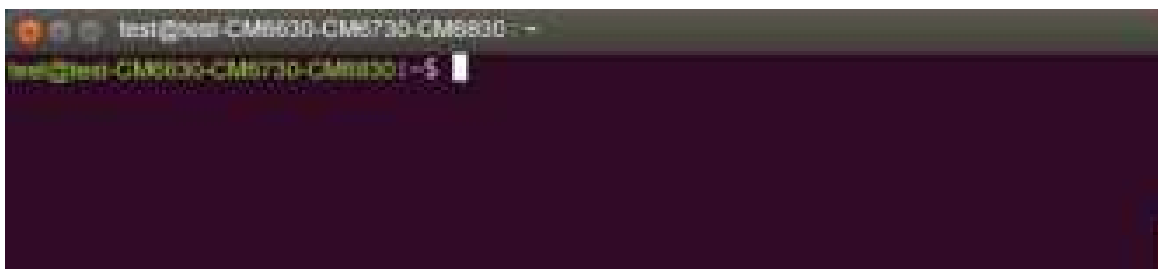


Note:

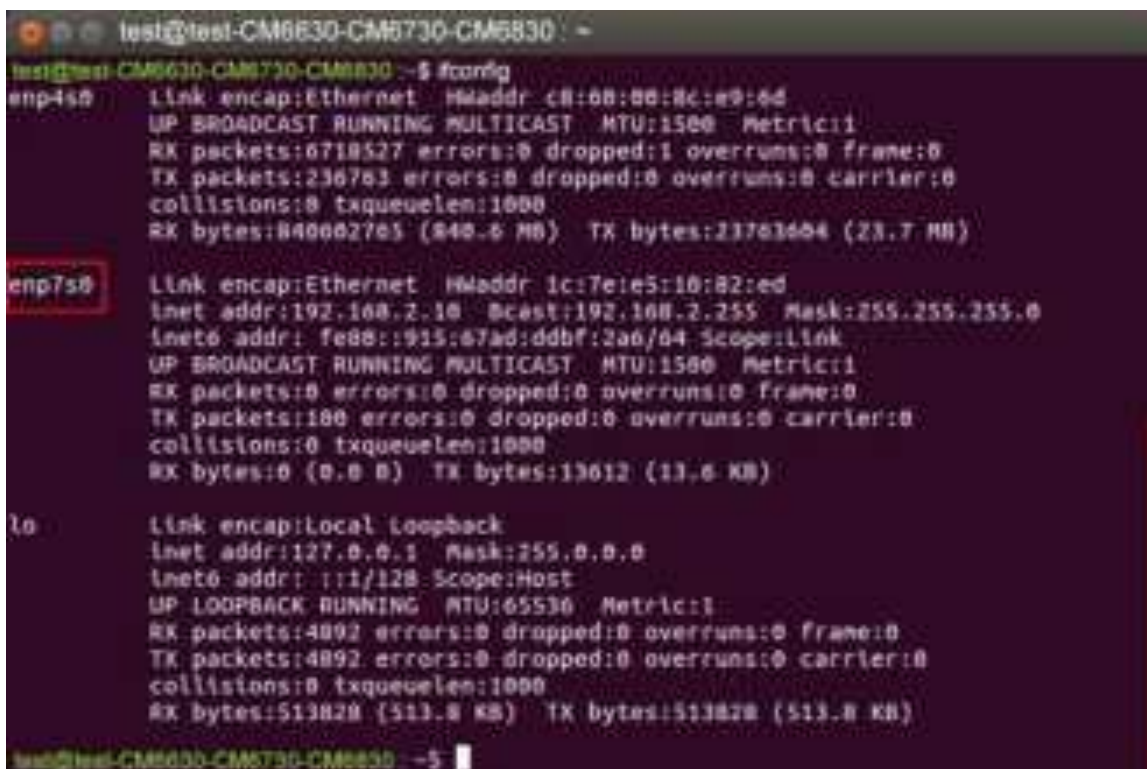
- Different PCs have different interface of network cards, like PC-A network card is eth1.10 for example 1 and PC-B network card is eth1.20 for example 2.
- How to find out the terminal and the interface of network cards based on different PCs.
 - From the following picture, you can click *the finding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



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



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



There are two examples to explain how configure VLAN settings.

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

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

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

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

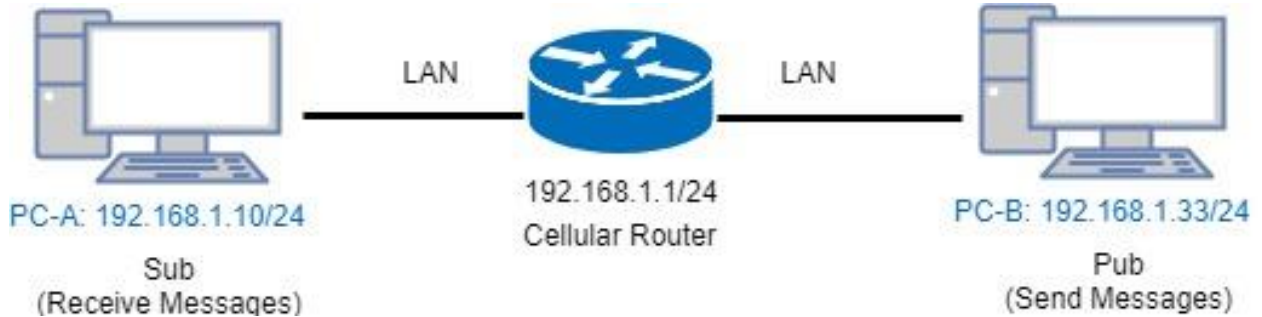
Example 2: PC-A ping PC-B (Trunk to Access)

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

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

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

17.2 MQTT Topology



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

Expect Result:

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

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

There is a process to explain the steps and result.

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

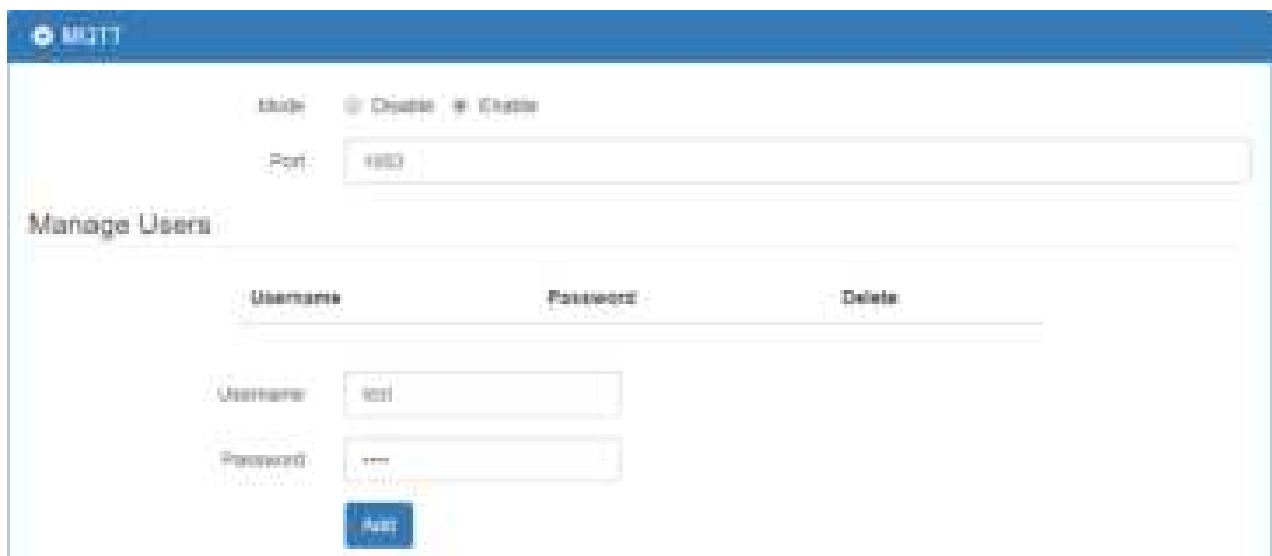
If your OS system is Ubuntu, you should install as below steps:

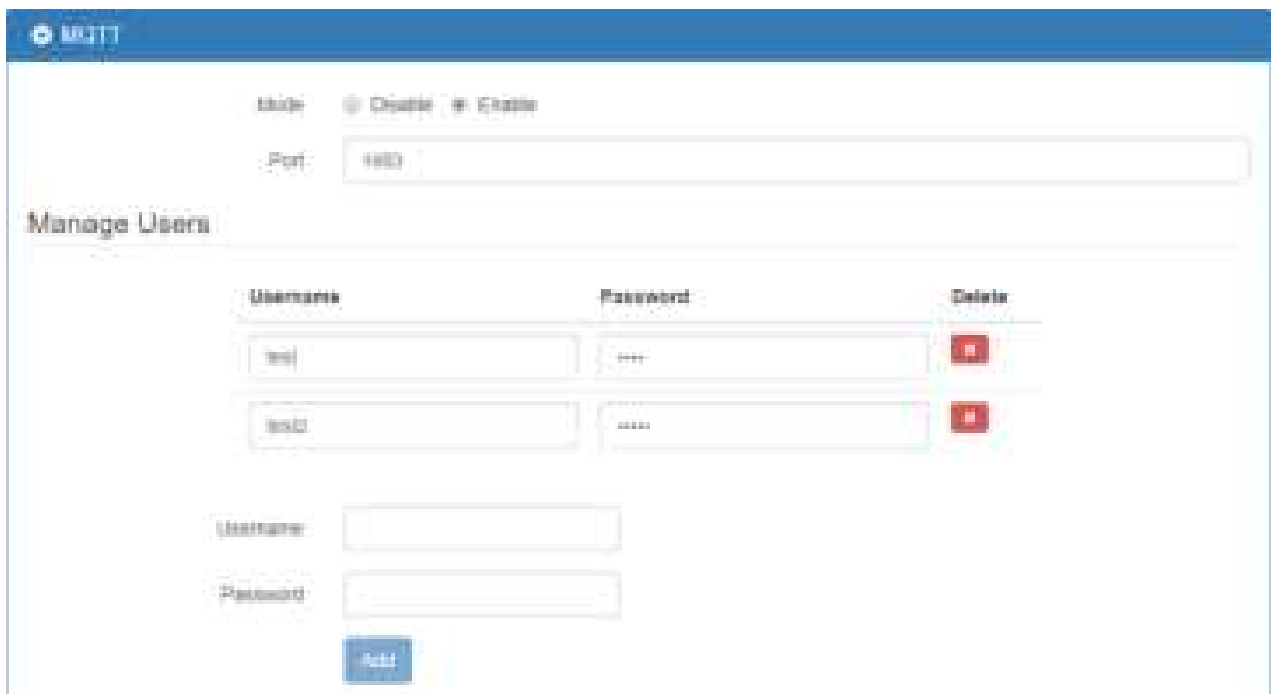
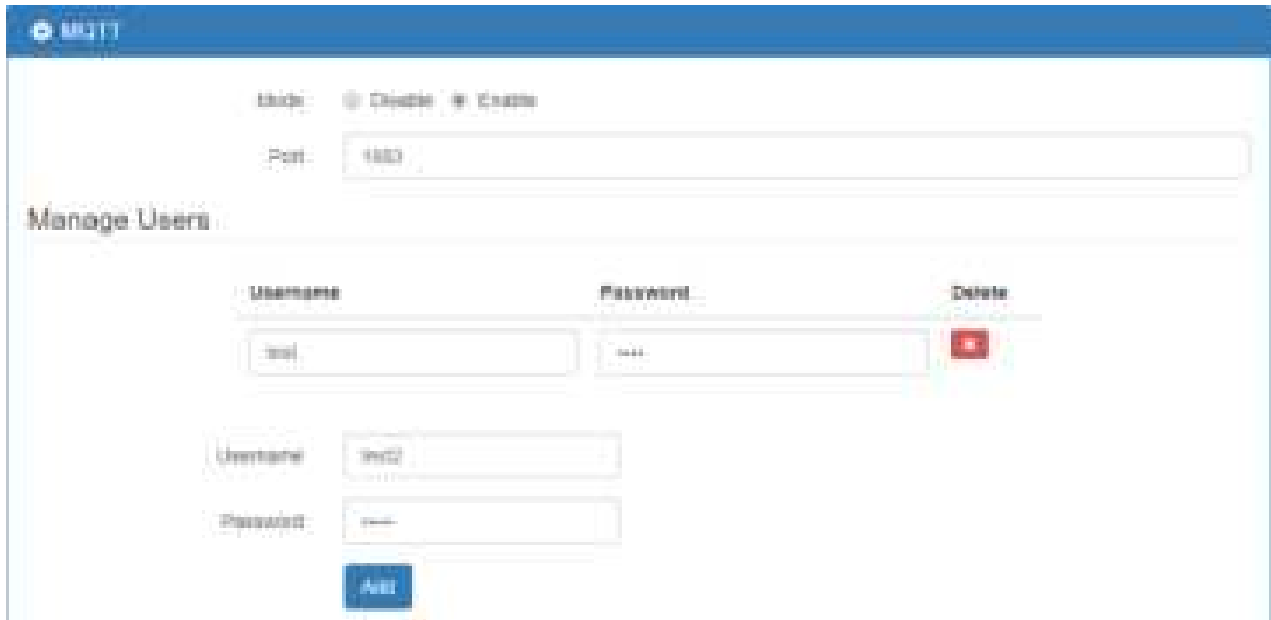
```
test@test:~$ sudo apt-get install mosquitto-clients
sudo: unable to resolve host test
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  geopip-database-extra javascript-common libjs-openlayers libnghttp2-14
  libnl-route-3-200 libqsttools-pi libqt5multimedia5-plugins
  libqt5multimediacore5 libqt5multimediacore5-gstreamer5 libssh-gcrypt-4 libwire shark-data
  libwiretap6 libwscodec1 libwsutil7 linux-headers-4.10.0-28
  linux-headers-4.10.0-28-generic linux-headers-4.10.0-42
  linux-headers-4.10.0-42-generic linux-headers-4.13.0-26
  linux-headers-4.13.0-26-generic linux-image-4.10.0-28-generic
  linux-image-4.10.0-42-generic linux-image-4.13.0-26-generic
  linux-image-extra-4.10.0-28-generic linux-image-extra-4.10.0-42-generic
  linux-image-extra-4.13.0-26-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libc-ares2 libmosquitto1
The following NEW packages will be installed:
  libc-ares2 libmosquitto1 mosquitto-clients
0 upgraded, 3 newly installed, 0 to remove and 119 not upgraded.
Need to get 65.3 kB/96.4 kB of archives.
After this operation, 330 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

```
test@test: ~
After this operation, 338 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://tw.archive.ubuntu.com/ubuntu xenial-updates/main amd64 libc-ares2 amd64 1.10.0-3ubuntu0.2 [14.1 kB]
Get:2 http://tw.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 libmosquitto1 amd64 1.4.8-1ubuntu0.16.04.2 [31.3 kB]
Fetched 65.3 kB in 0s (201 kB/s)
Selecting previously unselected package libc-ares2:amd64.
(Reading database ... 319300 files and directories currently installed.)
Preparing to unpack .../libc-ares2_1.10.0-3ubuntu0.2_amd64.deb ...
Unpacking libc-ares2:amd64 (1.10.0-3ubuntu0.2) ...
Selecting previously unselected package libmosquitto1:amd64.
Preparing to unpack .../libmosquitto1_1.4.8-1ubuntu0.16.04.2_amd64.deb ...
Unpacking libmosquitto1:amd64 (1.4.8-1ubuntu0.16.04.2) ...
Selecting previously unselected package mosquitto-clients.
Preparing to unpack .../mosquitto-clients_1.4.8-1ubuntu0.16.04.2_amd64.deb ...
Unpacking mosquitto-clients (1.4.8-1ubuntu0.16.04.2) ...
Processing triggers for libc-bin (2.23-8ubuntu10) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up libc-ares2:amd64 (1.10.0-3ubuntu0.2) ...
Setting up libmosquitto1:amd64 (1.4.8-1ubuntu0.16.04.2) ...
Setting up mosquitto-clients (1.4.8-1ubuntu0.16.04.2) ...
Processing triggers for libc-bin (2.23-8ubuntu10) ...
test@test:~$
```

- Step2: Configure MQTT for the Cellular Router

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





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

ACLs

User	Topic	Subscribe	Publish	Delete
User	<input type="text" value="test"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Topic	<input type="text" value="act"/>	<input checked="" type="checkbox"/> Subscribe	<input type="checkbox"/> Publish	<input type="checkbox"/>
<input type="button" value="Add"/>				

ACLs

User	Topic	Subscribe	Publish	Delete
<input type="text" value="test"/>	<input type="text" value="act"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="X"/>
<input type="text" value="test2"/>	<input type="text" value="abc"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="X"/>
User	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Topic	<input type="text"/>	<input type="checkbox"/> Subscribe	<input type="checkbox"/> Publish	<input type="checkbox"/>
<input type="button" value="Add"/>				

Note:

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

- Step3: There are two test MQTT examples.

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

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

```

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

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

Windows IP Configuration

Ethernet adapter Blue:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:b400:a335:e5ca:101
    Link-local IPv6 Address . . . . . : fe80::8c61:e319:2e70:1140%15
    IPv4 Address. . . . . : 192.168.1.33
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::c2e:43ff:fe0d:4743%15
                                192.168.1.1

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

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

```

test@test: ~
test@test:~$ ifconfig enp7s0
enp7s0  Link encap:Ethernet  HWaddr 1c:7e:e5:18:82:ed
        inet addr:192.168.1.18  Bcast:192.168.1.255  Mask:255.255.255.0
        inet6 addr: 2001:b400:a335:e5ca::102/128  Scope:Global
        inet6 addr: fe80::915:67ad:ddb7:3a6/64  Scope:link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:34342  errors:0  dropped:0  overruns:0  frame:0
        TX packets:4582  errors:0  dropped:0  overruns:0  carrier:0
        collisions:0  txqueuelen:1000
        RX bytes:9538280 (9.5 MB)  TX bytes:1665380 (1.6 MB)

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

```

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

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

Windows IP Configuration

Ethernet adapter Blue:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:b400:a335:e5ca:101
    Link-local IPv6 Address . . . . . : fe80::8c61:e319:2e70:1140%15
    IPv4 Address. . . . . : 192.168.1.33
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::c2e:43ff:fe0d:4743%15
                                192.168.1.1

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

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

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

```
test@test:~$ ifconfig enp7s0
enp7s0:  Link encap:Ethernet  HWaddr 1c:7e:e5:10:82:ed
         inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
         inet6 addr: 2001:b400:e335:e5ca::102/128  Scope:Global
         inet6 addr: fe80::915:67ad:ddbf:2a6/64  Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:58690  errors:0  dropped:0  overruns:0  frame:0
         TX packets:4831  errors:0  dropped:0  overruns:0  carrier:0
         collisions:0  txqueuelen:1000
         RX bytes:16908302 (16.9 MB)  TX bytes:1150596 (1.1 MB)

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

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

```
Command Prompt (1)
C:\Program Files (x86)\mosquitto>ipconfig

Windows IP Configuration

Ethernet adapter Blues:

   Connection-specific DNS Suffix  . : 
   IPv6 Address. . . . . : 2001:b400:e335:e5ca::101
   Link-local IPv6 Address . . . . . : fe80::18c61e319:2e70:1140%15
   IPv4 Address. . . . . : 192.168.1.33
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : fe80::c2e43ff:fe0d:4743%15
                               192.168.1.1

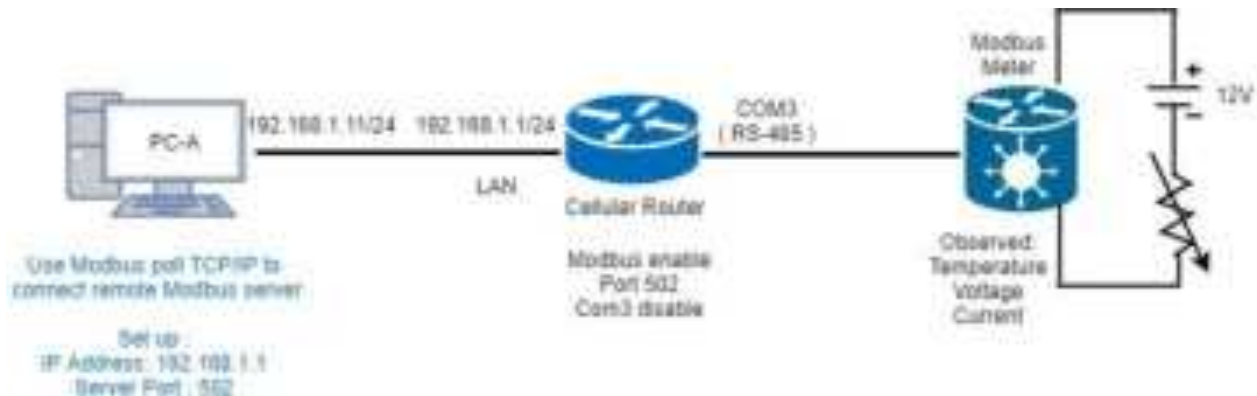
C:\Program Files (x86)\mosquitto>mosquitto_pub -h 192.168.1.1 -t abc -u test2 -P test2 -m test
C:\Program Files (x86)\mosquitto>
```

```
test@test:~$ ifconfig enp7s0
enp7s0:  Link encap:Ethernet  HWaddr 1c:7e:e5:10:82:ed
         inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
         inet6 addr: 2001:b400:e335:e5ca::102/128  Scope:Global
         inet6 addr: fe80::915:67ad:ddbf:2a6/64  Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:58690  errors:0  dropped:0  overruns:0  frame:0
         TX packets:4831  errors:0  dropped:0  overruns:0  carrier:0
         collisions:0  txqueuelen:1000
         RX bytes:16908302 (16.9 MB)  TX bytes:1150596 (1.1 MB)

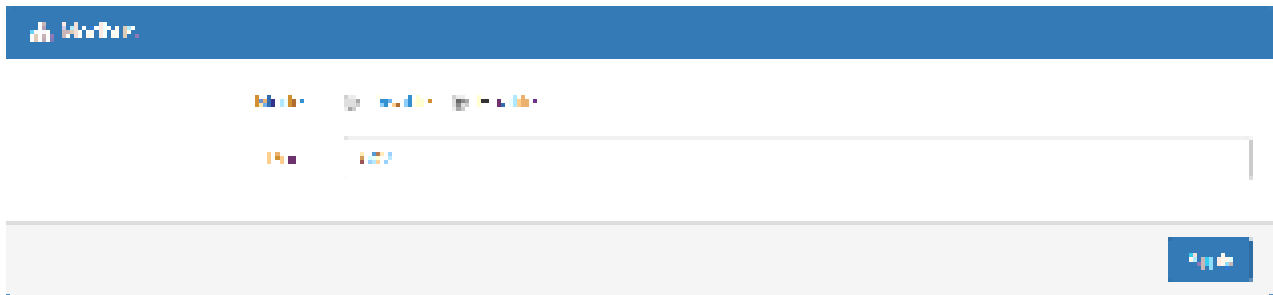
test@test:~$ mosquitto_sub -h 192.168.1.1 -t abc -u test -P test
test
```

17.3 Modbus Topology

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



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

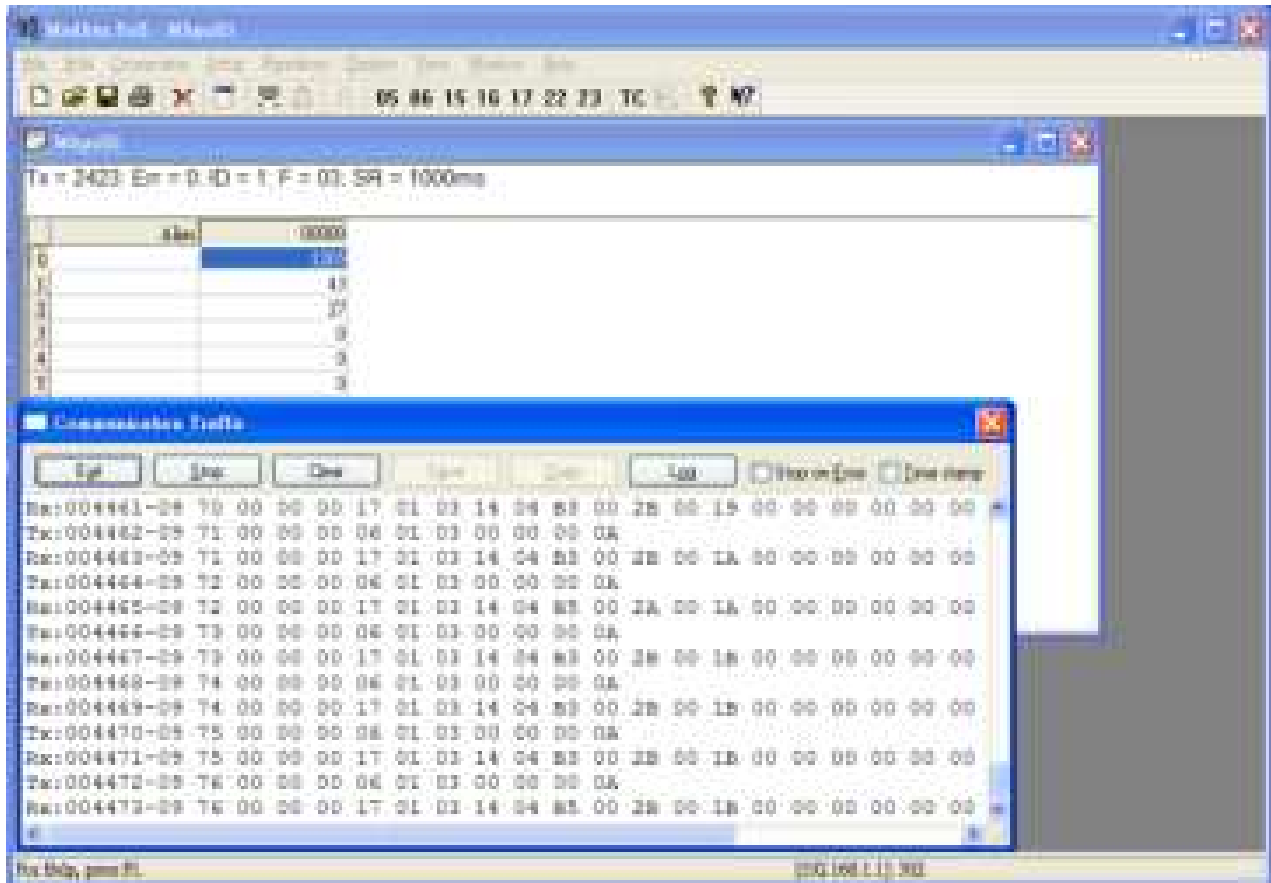


Please confirm the interface of COM Port 3 that the mode is Disable.

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

Apply

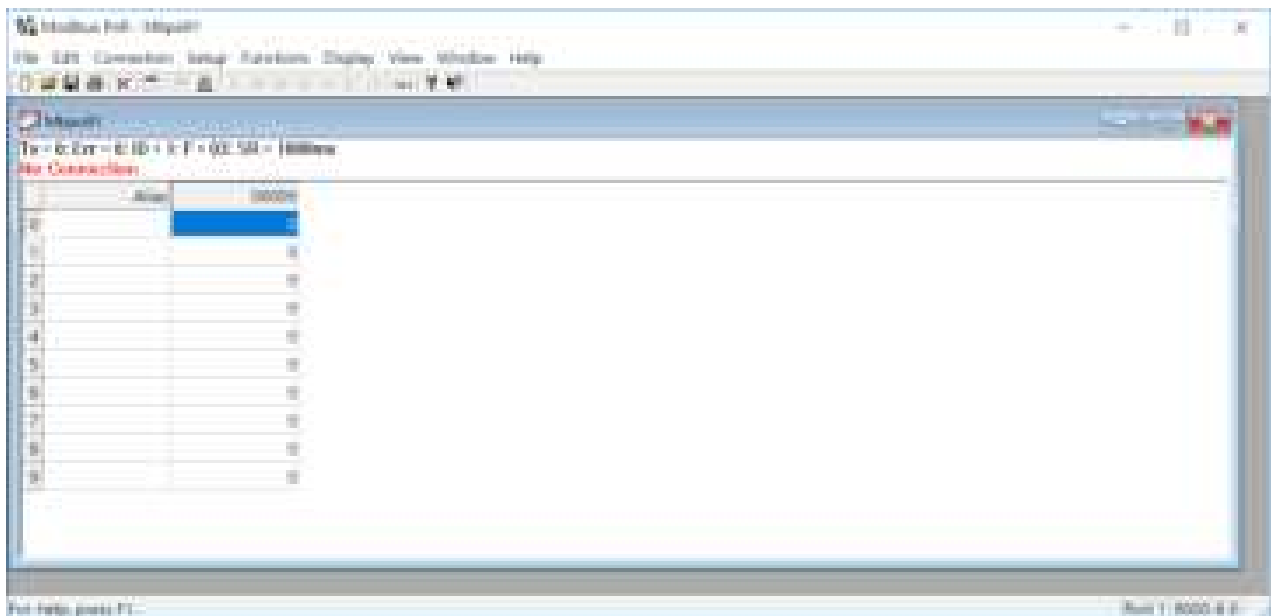
Next, you can connect a meter of DC voltage and current for supporting Modbus protocol with RS-485 serial to COM Port 3 from the cellular router and know the information about temperature, voltage and current.



Note 1:

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

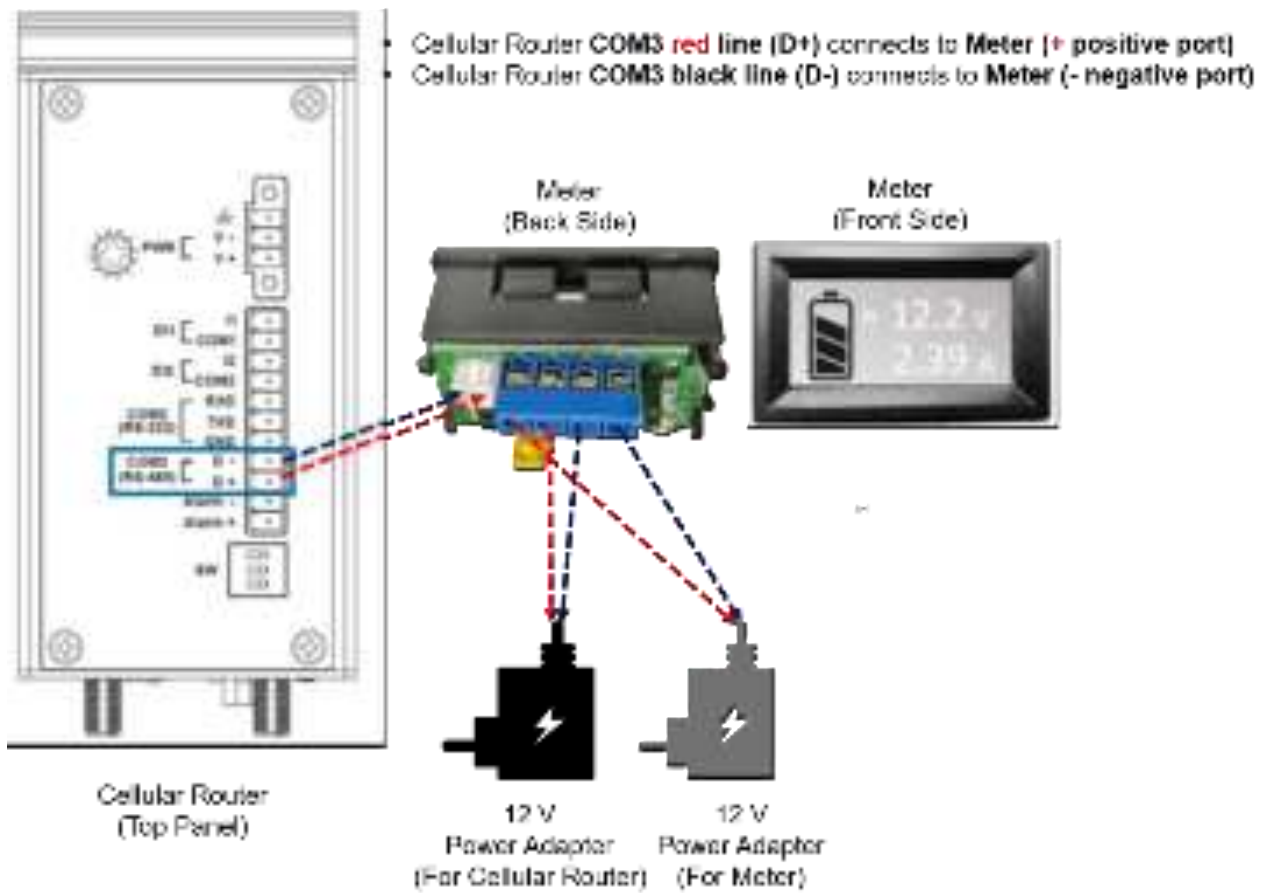
<http://www.tucows.com/preview/502459/Modbus-Poll>



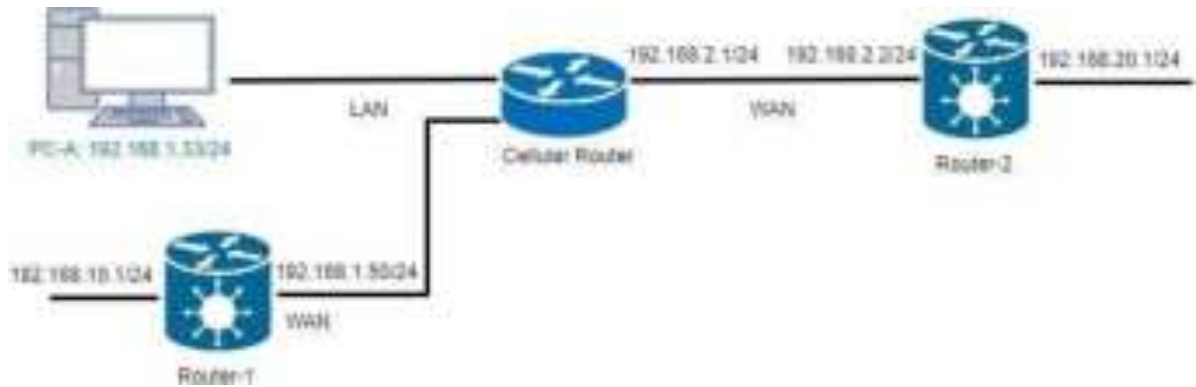
Note 2:

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

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



17.4 IP Routing Topology



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

- (1) PC-A sends ICMP packet to Router-1 LAN and WAN IP and they should have response.
- (2) PC-A sends ICMP packet to Router-2 LAN and WAN IP and they should have response.

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

- LAN configuration:

The screenshot shows the 'LAN IPv4' configuration page. The 'IP Address' field is set to 192.168.1.1 and the 'IP Mask' field is set to 255.255.255.0. The 'DHCP Server Configuration' section has the 'DHCP Server' toggle set to 'On'. The 'IP Address Pool' is configured with 'From' 192.168.1.2 and 'To' 192.168.1.254. There is an 'Add Static IP Address' button and a 'Apply' button at the bottom right.

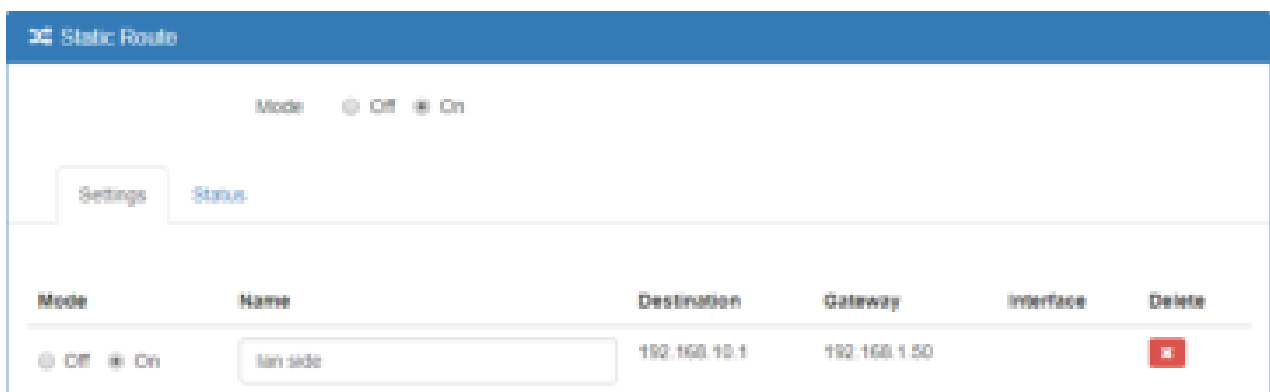
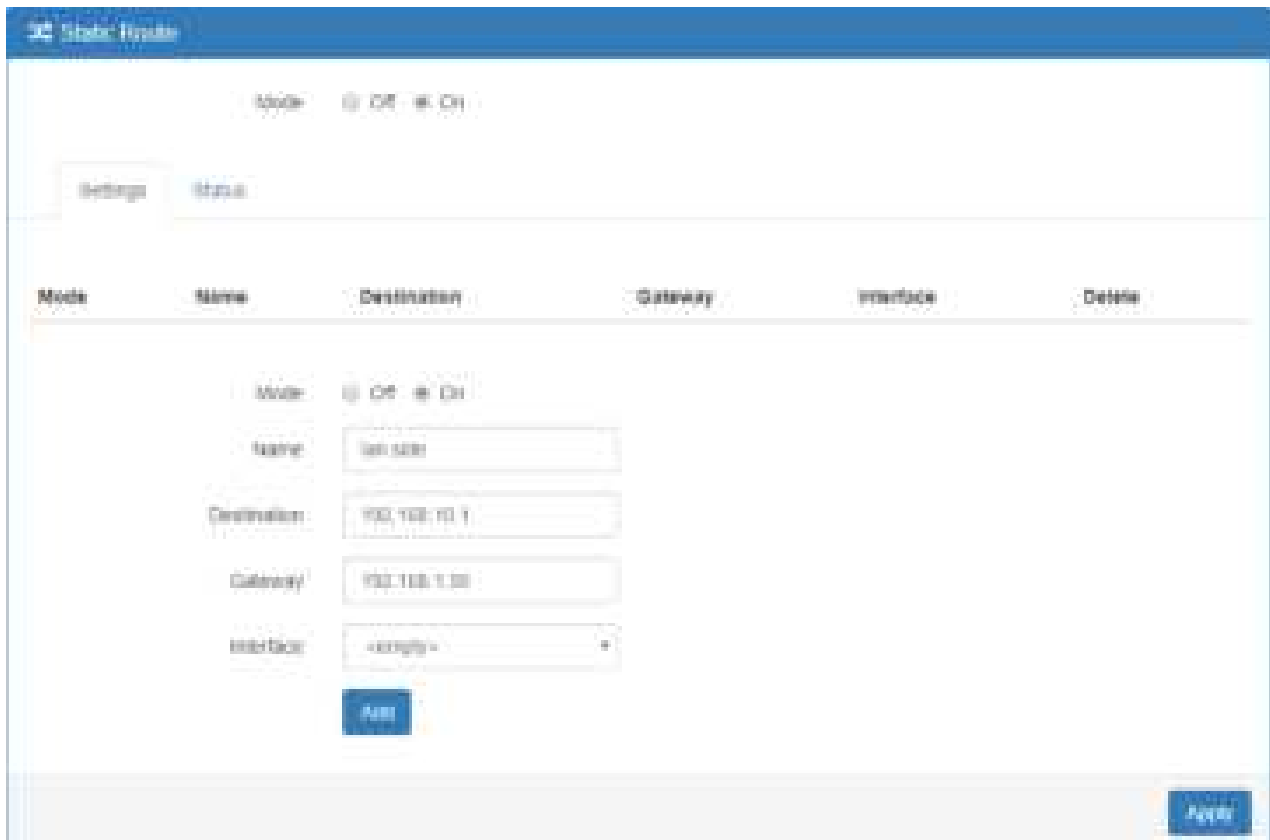
- WAN configuration:

The screenshot shows the 'WAN Ethernet' configuration page. The 'Work As' section has 'Static IPv4' selected. The 'Configuration' tab is active. The 'Static IPv4 Configuration' section has the 'IP Address' field set to 0.0.0.0, the 'IP Mask' field set to 255.255.255.0, and the 'Gateway Address' field set to 0.0.0.0. There is an 'Ethernet Ping Health' link and a 'Apply' button at the bottom right.

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

Example 1: Add IP Routing on LAN interface

- Step 1: The cellular router for Static Route configuration
The Mode is on at the settings section and add the routing.
- Step 2: Router-1 configuration is as below.
 - (1) Login to the Router-1 web site, and then "NAT disable".
 - (2) Configure LAN IP: 192.168.10.1
 - (3) Configure WAN IP: 192.168.1.50



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

```

Command Prompt (1)
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : 
IPv6 Address. . . . . : 2001:b400:e333::5ca:1901
Link-local IPv6 Address . . . . . : fe80::8c81:e333::2a7d:1b407e15
IPv4 Address. . . . . : 192.168.1.11
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::8c81:e333::2a7d:1b407e15
192.168.1.1

C:\msdostools>ping 192.168.1.50

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

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

C:\msdostools>ping 192.168.10.1

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

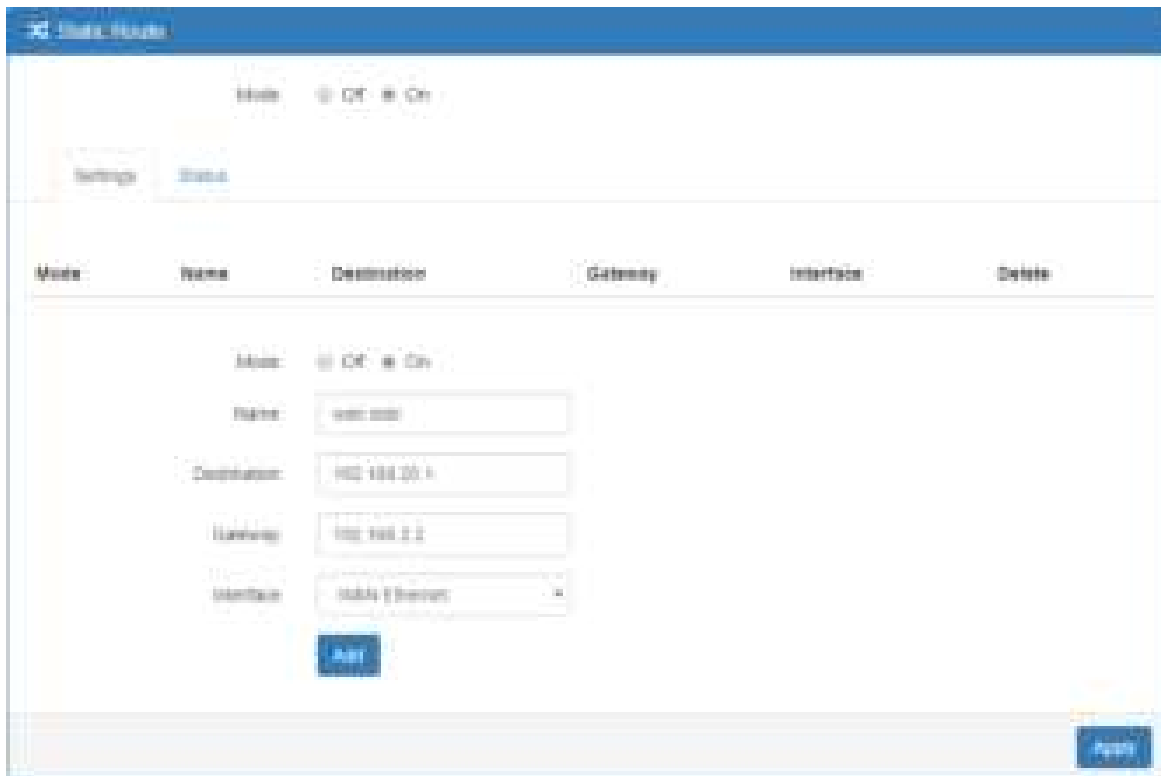
Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\msdostools>

```

Example 2: Add IP Routing on WAN interface

- Step1: The cellular router for Static Route configuration
The Mode is on at the settings section and add the routing.
- Step2: Router-2 configuration is as below.
 - (1) Login to the Router-2 web site, and then "NAT disable".
 - (2) Configure LAN IP: 192.168.20.1
 - (3) Configure WAN IP: 192.168.2.2





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

```

Command Prompt (1)
Ethernet adapter Blue:
    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:b400:e335:e5ca::101
    Link-local IPv6 Address . . . . . : fe80::8c61:e319:2e70:1140%15
    IPv4 Address. . . . . : 192.168.1.33
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::c2e:43ff:fe0d:4743%15
                               192.168.1.1

C:\tools>ping 192.168.2.2

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

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

C:\tools>ping 192.168.20.1

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

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

C:\tools>

```

13 Safety Notice

* 第十二條

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率加大功率或變更原設計之特性及功能。

* 第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電通信。

低功率射頻電機忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

* 減少電磁波影響，請妥適使用。

* 本器材須經專業工程人員安裝及設定，始得設置使用，且得直接販售給一般消費者。

* FCC 15.19:

THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES. OPERATIONS IS SUBJECT TO THE FOLLOWING TWO CONDITIONS: (1) THIS DEVICE MAY NOT CAUSE HARMFUL INTERFERENCE AND (2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED, INCLUDING INTERFEERENCE THAT MAY CAUSE UNDESIRE OPERATION (15.19)

* FCC 15.21:

The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

* FCC 15.105:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

* RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

19 Wi-Fi Specifications

Standards

- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

Modulations

- 802.11b: CCK/QPSK, BPSK
- 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
- 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM

Channels

- 11 Channels (US, Canada)
- 13 Channels (Europe, Japan)

Data Rates

- 6 / 9 / 11 / 12 / 18 / 24 / 36 / 48 / 54 Mbps in 802.11g mode
- 1 / 2 / 5.5 / 11 Mbps in 802.11b mode

Frequency Range

- 2.4GHz to 2.483GHz

Wi-Fi Antenna Type

- One (1) detachable reverse SMA Antenna

Antenna Gain in dBi

- 2.0 (Max)