

# **Industrial 4G LTE Cellular Router**

**RT-MOB-020**

**User Manual**

Version 1.1.8

# Table of Contents

<b>1</b>	<b>Introduction.....</b>	<b>6</b>
1.1	Features.....	6
1.2	Specifications.....	7
1.3	Mechanical Dimensions (RT-MOB-020) .....	8
1.4	Ordering Information .....	8
<b>2</b>	<b>Hardware Installation.....</b>	<b>8</b>
2.1	LED Indicators.....	8
2.2	Ethernet Port.....	9
2.3	Grounding the Router.....	9
2.4	Pin Assignments.....	10
2.5	Connecting the Power Supply .....	10
2.6	Connecting I/O Ports .....	10
2.7	UART (RS-232) .....	12
2.8	Install the SIM Card.....	12
2.9	Reset Button .....	13
2.10	External Antenna.....	13
<b>3</b>	<b>Configuration via Web Browser .....</b>	<b>14</b>
3.1	Access the Web Configurator .....	14
3.2	Navigate the Web Configurator .....	15
<b>4</b>	<b>Status.....</b>	<b>16</b>
4.1	Status > GPS .....	20
<b>5</b>	<b>Configuration &gt; System.....</b>	<b>20</b>
5.1	System > Time and Date .....	20
5.2	System > Logging .....	24
5.2.1	Logging > Logging .....	24
5.2.2	Logging > Log.....	25
5.3	System > Alarm .....	26
5.3.1	Alarm > Contacts > Create and name the Group .....	27
5.3.2	Alarm > Contacts > Add User .....	29
5.3.3	Alarm > Duty Schedule .....	30
5.4	System > Ethernet Ports .....	30
5.5	System > Client List .....	32
<b>6</b>	<b>Configuration &gt; WAN .....</b>	<b>32</b>
6.1	WAN > Priority.....	32
6.2	WAN > Ethernet .....	33
6.2.1	WAN Ethernet Configuration.....	33
6.2.2	Ethernet Ping Health .....	36

6.3	WAN > IPv6 DNS .....	38
<b>7</b>	<b>Configuration &gt; LTE.....</b>	<b>39</b>
7.1	LTE > LTE Config .....	40
7.1.1	LTE Configuration.....	40
7.1.2	LTE Ping Health.....	41
7.2	LTE > GPS Config.....	41
7.3	LTE > Dual APN .....	43
7.4	LTE > Usage Display.....	46
7.5	LTE > SMS.....	51
7.6	LTE > Serving Cell .....	53
7.7	LTE > DNS.....	54
<b>8</b>	<b>Configuration &gt; WiFi (RT-MOB-020).....</b>	<b>55</b>
8.1	WiFi > WiFi Config .....	55
8.2	WiFi > MAC Filter .....	56
8.3	WiFi > Client List .....	57
<b>9</b>	<b>Configuration &gt; LAN.....</b>	<b>58</b>
9.1	LAN > IPv4.....	58
9.2	LAN > IPv6.....	59
9.3	LAN > VLAN.....	59
9.4	LAN > Subnet.....	61
<b>10</b>	<b>IP Routing.....</b>	<b>62</b>
10.1	IP Routing > Static Route .....	62
10.2	IP Routing > RIP .....	65
10.3	IP Routing > OSPF.....	67
10.4	IP Routing > BGP .....	70
<b>11</b>	<b>Configuration &gt; VPN.....</b>	<b>73</b>
11.1	VPN > Open VPN.....	73
11.1.1	Open VPN Common Setting.....	74
11.1.2	Open VPN Client Setting .....	75
11.1.3	Open VPN Server Setting.....	76
11.1.4	Set up Open VPN Custom.....	78
11.2	VPN > IPsec.....	80
11.2.1	IPsec > Connections.....	80
11.2.2	IPsec > Authentication IDs.....	85
11.2.3	IPsec > X.509 Certificates .....	86
11.2.4	IPsec > CA Certificates.....	87
11.2.5	IPsec > Net-to-Net Configuration.....	89
11.3	VPN > GRE.....	104
11.4	VPN > PPTP Server.....	105
11.5	VPN > L2TP .....	107
<b>12</b>	<b>Configuration &gt; Firewall .....</b>	<b>111</b>

12.1	Firewall > Basic Rules .....	111
12.2	Firewall > Port Forwarding .....	112
12.3	Firewall > DMZ .....	113
12.4	Firewall > IP Filter .....	114
12.5	Firewall > MAC Filter .....	118
12.6	Firewall > URL Filter .....	119
12.7	Firewall > NAT .....	120
12.8	Firewall > IPS .....	121
<b>13</b>	<b>Configuration &gt; Service .....</b>	<b>122</b>
13.1	Service > SNMP .....	122
13.1.1	Community .....	122
13.1.2	SNMP v3 User Configuration .....	123
13.1.3	SNMP trap configuration .....	124
13.2	Service > TR069 .....	125
13.3	Service > Dynamic DNS .....	126
13.4	Service > VRRP .....	128
13.5	Service > MQTT .....	128
13.6	Service > UPnP .....	131
13.7	Service > SMTP .....	131
13.8	Service > IP Alias .....	132
<b>14</b>	<b>Configuration &gt; Management .....</b>	<b>133</b>
14.1	Management > Identification .....	133
14.2	Management > Administration .....	134
14.3	Management > Contacts / On Duty .....	135
14.3.1	Contacts .....	135
14.3.2	Duty Schedule .....	135
14.4	Management > SSH .....	136
14.5	Management > Firmware .....	137
14.6	Management > Configuration .....	137
14.7	Management > Load Factory .....	137
14.8	Management > Restart .....	138
<b>15</b>	<b>Configuration &gt; Diagnosis .....</b>	<b>138</b>
15.1	Diagnosis > Ping .....	138
15.2	Diagnosis > Traceroute .....	139
<b>16</b>	<b>Configuration Applications .....</b>	<b>140</b>
16.1	WAN Priority .....	140
16.2	LAN > IPv4/IPv6 Dual Stack .....	142
16.3	MQTT Broker .....	144
16.4	Alarm Configuration .....	145
16.5	Open VPN Configuration .....	147
16.5.1	Open VPN Server Mode .....	147
16.5.2	Open VPN Client Mode .....	148



16.5.3	Open VPN Net-to-Net.....	149
16.5.4	Open VPN 1:1 NAT .....	153
16.5.5	Open VPN with third-party server .....	154
16.5.6	Install Open VPN Access Server on Docker .....	156
16.5.7	Install Pritunl Open VPN server on Docker .....	162
16.6	VRRP Topology .....	170
16.7	TR069 Server (GenieACS Installation) .....	170
<b>17</b>	<b>Test Case Example.....</b>	<b>180</b>
17.1	VLAN Topology .....	180
17.2	MQTT Topology .....	183
17.3	IP Routing Topology .....	189

# 1 Introduction

**RT-MOB-020**, compact, lightweight and cost-effective **Industrial 4G LTE Cellular Routers**, are built in 2-port fast Ethernet connection as well as support 2G/3G/4G mobile networks for wired and wireless communication in harsh environments. Equipped with RS232 serial port and digital input/output interfaces, the **RT-MOB-020** is simple to configure and collect real-time data transmission quickly for Industrial IoT and machine-to-machine applications. The **RT-MOB-020** is also compliant with IEEE 802.11b/g/n Wi-Fi connectivity.

Featuring VPN Tunnels, Firewall, TR069, and SNMP Trap, **RT-MOB-020 Industrial 4G LTE Cellular Routers** enhance highly secure authentication, encryption and management to protect your data efficiently between public and private networking. Supporting -30~+70°C wide temperature operation and flexible input voltage range of 8-48VDC for diverse environments and various applications. **RT-MOB-020 Industrial 4G LTE Cellular Routers** are suitable and reliable choices for fast deployment and easy configuration to simplify your complicated solutions and fit your services for industrial networking and smart city.

## 1.1 Features

- Highly reliable and secure for mission-critical cellular communications
- Compact and lightweight design with 2-port Ethernet interfaces
- Support multi-band connectivity with FDD LTE/ TDD LTE/ WCDMA/ GSM/ LTE Cat 4
- Provide IEEE 802.11b/g/n Wi-Fi standards (RT-MOB-020 Model)
- Built-in micro SIM connector, RS232 serial port, and DI/DO interfaces
- Integrated detachable antenna against radio interference
- LED indicators for connection and data transmission status
- Industrial rated from -30 to +70°C for use in harsh environments
- IPv6/IPv4 dual stack and all applications are IPv6 ready
- Support serial communication protocols for rich connectivity
- Enhance security and encryption for authentication and transmission

## 1.2 Specifications

### Cellular Interface

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

### Wi-Fi Interface (RT-MOB-020 Model)

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

### Hardware Interface

- High Performance 550 MHz SoC with 128MByte Flash
- 1 x Micro SIM Connector (push-push type)
- 1 x LAN 10/100 Mbps Ethernet port
- 1 x WAN 10/100 Mbps Ethernet port
- WPS / RESET Button
- 1 x RS232 (TXD/RXD/GND)
- 1 x DI (Non-Isolated), 1 x DO (Non-Isolated)
- 2 x SMA connectors for detachable LTE Antenna
- 2 x RP-SMA connectors for detachable Wi-Fi Antenna (RT-MOB-020 Model)
- 1 x SMA connector for detachable GPS antenna

### Physical Characteristics

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

### LED Display

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

### Power Supply

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

### Software

- **Network Protocols:**  
IPv4, IPv6, IPv4/IPv6 dual stack, DHCP server and client, PPPoE, Static IP, SNTP, GPS sync time, DNS Proxy, VRRP, OSPF, Message Queue Telemetry Transport (MQTT Broker), BGP, Flow (Modbus master ↔ MQTT client)
- **Routing/Firewall:**  
NAT, Virtual Server, DMZ, MAC Filter, URL Filter, IP Filter, VLAN, Static Routing and RIP-1/2, IPS, Policy Route
- **VPN:**  
OpenVPN, IPSec (3DES, AES128, AES196, AES256, MD5, SHA-1, SHA256), GRE, PPTP, L2TP
- **Wireless Connectivity:**  
WAN WiFi Client
- **Others:**  
DDNS, QoS, UPnP, SMS Action, GPS Track Drawing, GPS TCP Push
- **Alarm:**  
DI, DO, SMS, VPN/WAN Disconnect, SNMP Trap, E-mail, TR069

### Management Software

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

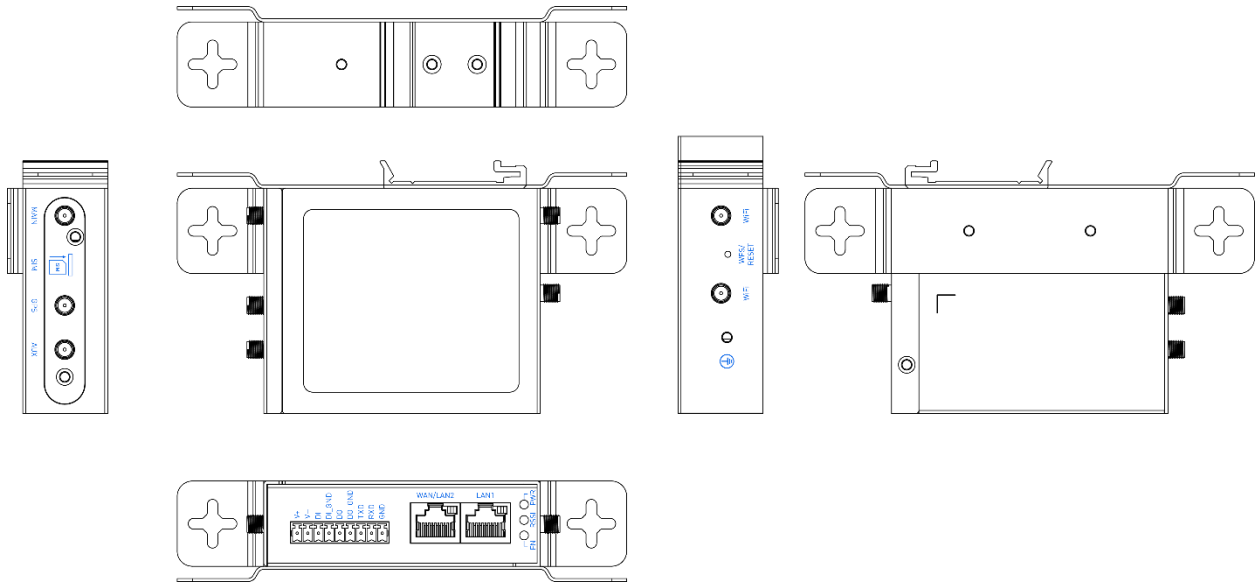
### Environment

- Operating Temperature -30 ~ +70°C
- Storage Temperature -40 ~ +85°C
- Ambient Relative Humidity 10 ~ 95% (non-condensing)
- Humidity 0 ~ 95% (non-condensing)

### Standards and Certifications

- **EMC** : CE, FCC
- **EMI** : EN 301489 , FCC Part 15B Class B
- **EMS** : EN 301489
- **Vibration** : IEC60068-2-6
- **Radio** : EN 301511, EN 301908-1, EN 301908-2, EN 301908-13, EN 300328, EN 303413, EN 62311

### 1.3 Mechanical Dimensions (RT-MOB-020)



### 1.4 Ordering Information

Model Name	Description
000000000	Compact Industrial 4G LTE Cellular Router ( 1 x WAN, 1 x LAN, 1 x RS232 , 1 x DI, 1 x DO, 1 x micro SIM Slot, GPSx1, -30 ~ +70°C )
RT-MOB-020	Compact Industrial Wi-Fi 4G LTE Cellular Router ( 1 x WAN, 1 x LAN, 1 x RS232 , 1 x DI, 1 x DO, 1 x micro SIM Slot, GPSx1, Wi-Fi, -30 ~ +70°C )

## 2 Hardware Installation

This chapter introduces how to install and connect the hardware.

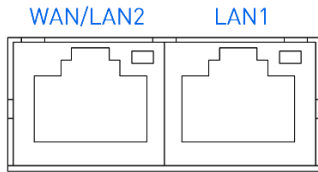
### 2.1 LED Indicators



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

## 2.2 Ethernet Port

### (1) 10/100 Mbps Ethernet LAN/WAN



The LAN and WAN interface are standard RJ45 connectors.

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

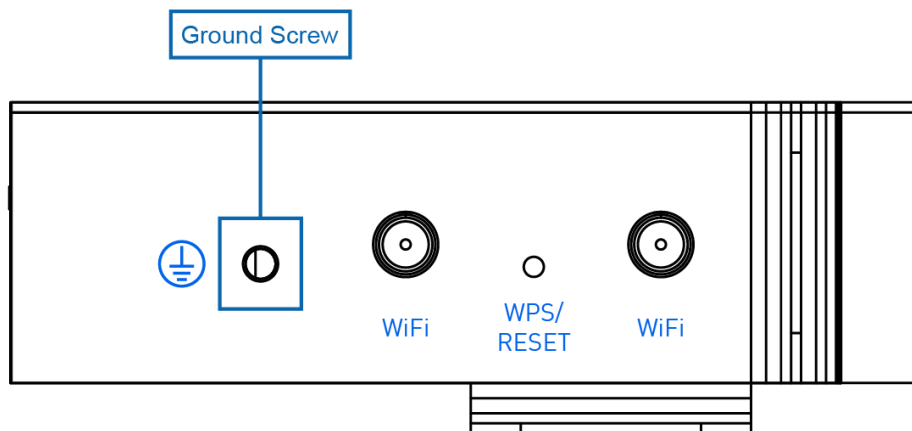
### (2) LED Indicator of Ethernet Port

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

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

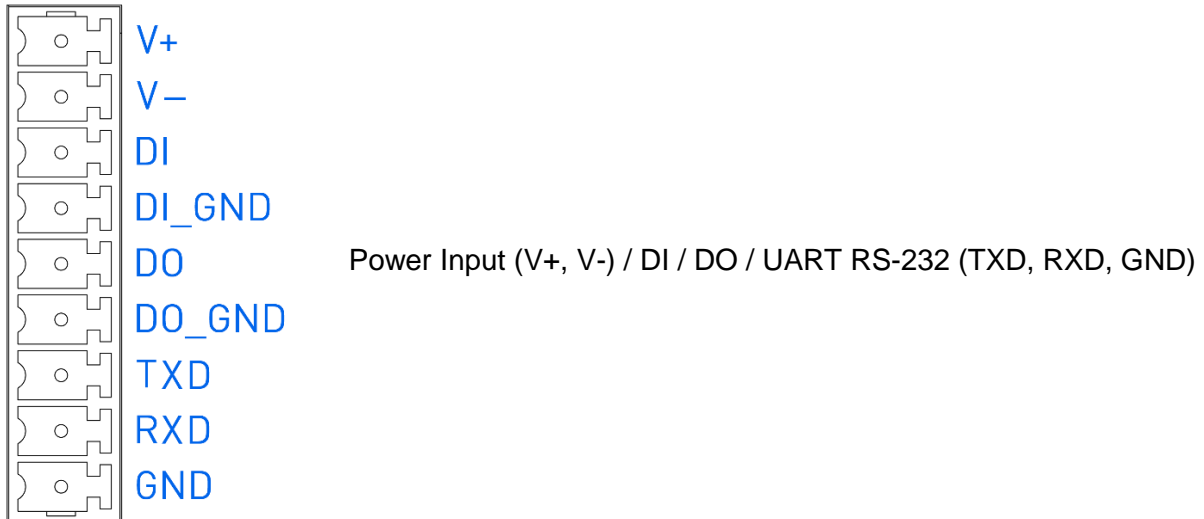
## 2.3 Grounding the Router

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



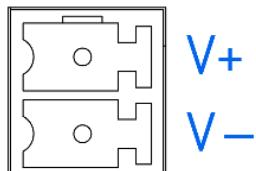
(RT-MOB-020)

## 2.4 Pin Assignments



## 2.5 Connecting the Power Supply

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



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

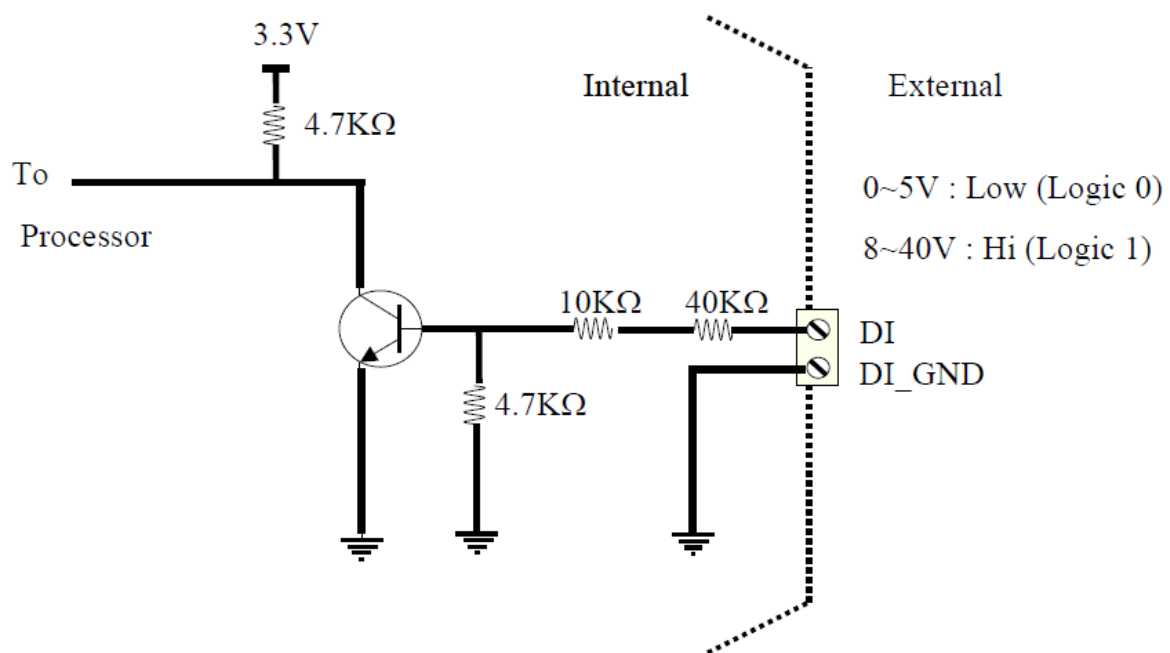
## 2.6 Connecting I/O Ports

### (1) Digital Input (DI)

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

Pin	Description
DI	Digital Input
DI_GND	

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

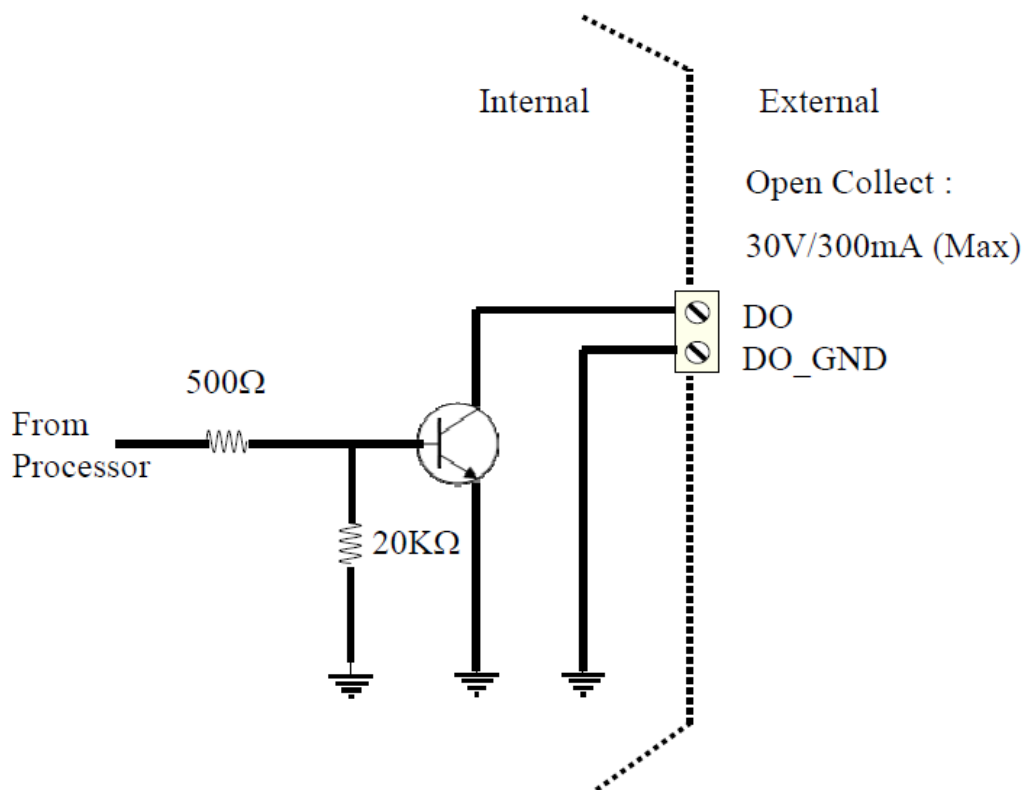


## (2) Digital Output (DO)

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

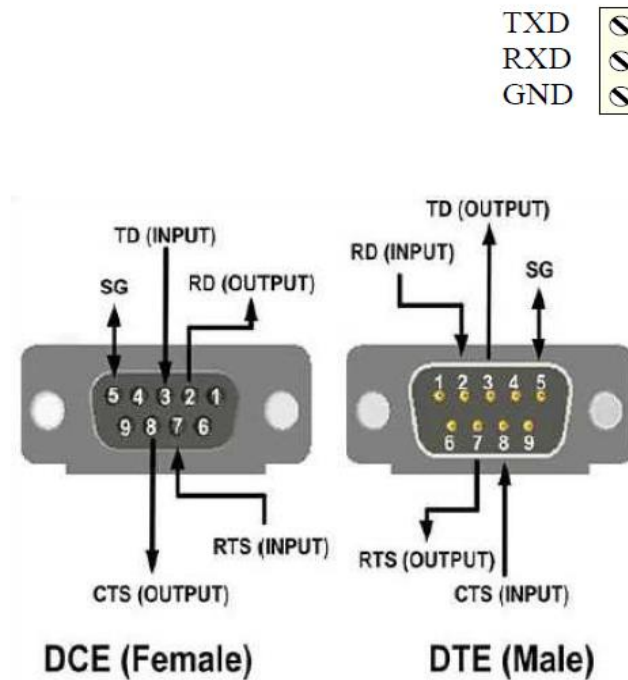
Pin	Description
DO	Digital Output
DO_GND	

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



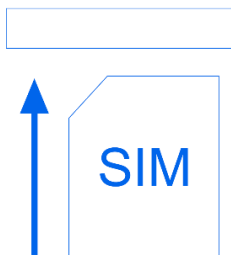
## 2.7 UART (RS-232)

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



Pin	Signal	Direction
<b>TXD</b>	Transmit Data	Output
<b>RXD</b>	Receive Data	Input
<b>GND</b>	Signal Ground	-

## 2.8 Install the SIM Card



### Insert and Remove SIM Card

- (1) Before inserting or removing the SIM card, ensure that the power has been turned off and the power connector has been removed from Cellular Router.
- (2) Insert the SIM card with right direction. Push the SIM card in to the slot, and lightly press it to lock it in the slot.
- (3) To remove the SIM card, lightly press the SIM card, and it will pop out.



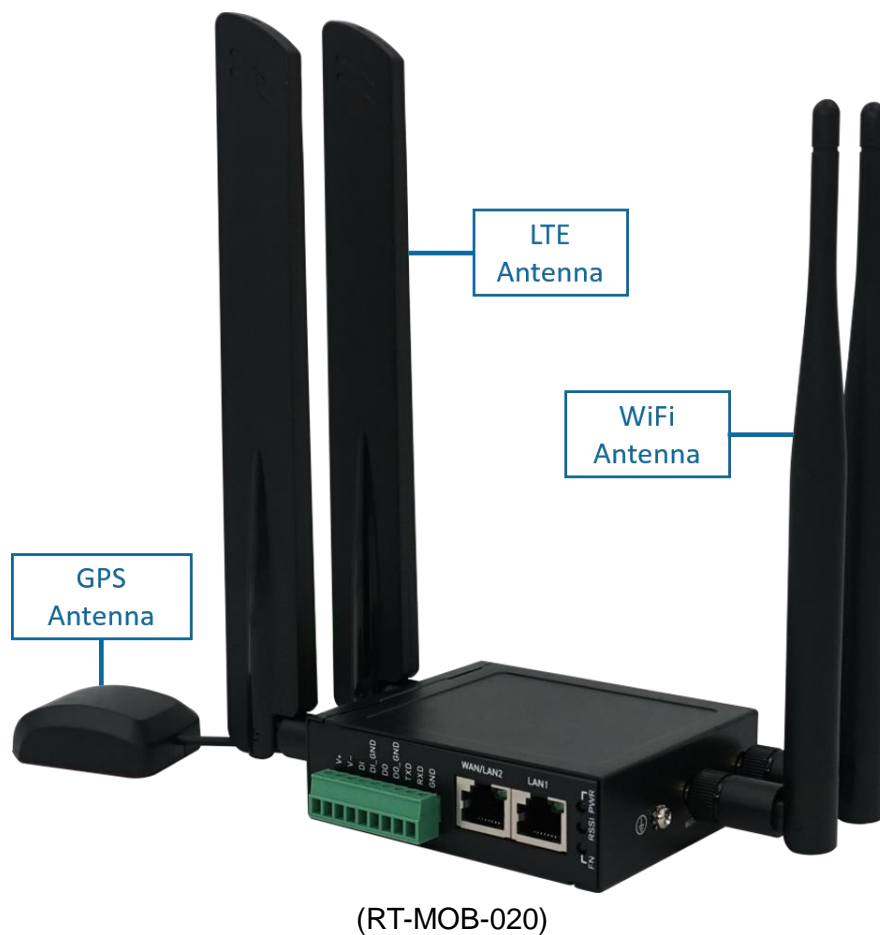
## 2.9 Reset Button



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

## 2.10 External Antenna

Each unit has three antenna connectors, MAIN, GPS, AUX (SMA). For RT-MOB-020, there will be five antenna connectors and extra two antennas for Wi-Fi (RP-SMA). Connect the antenna to MAIN when you have only one antenna. Please tighten the connecting nut properly to ensure good connection.



## 3 Configuration via Web Browser

### 3.1 Access the Web Configurator

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

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

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

#### Title Bar Panel > Selecting Language

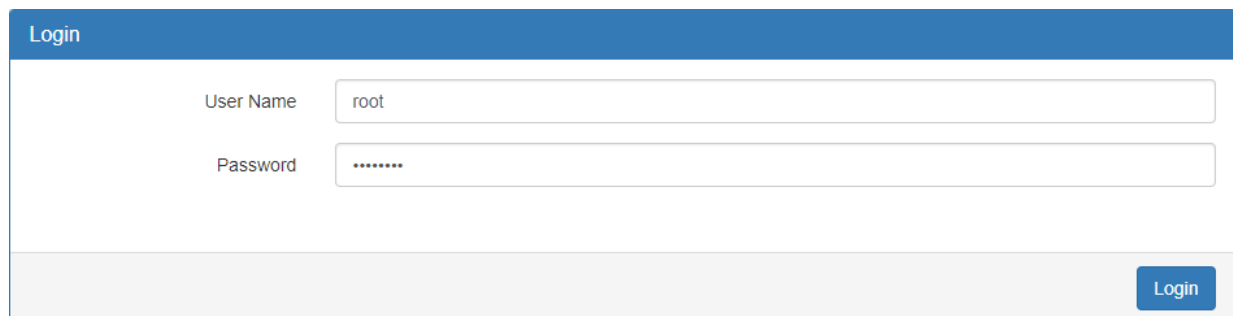
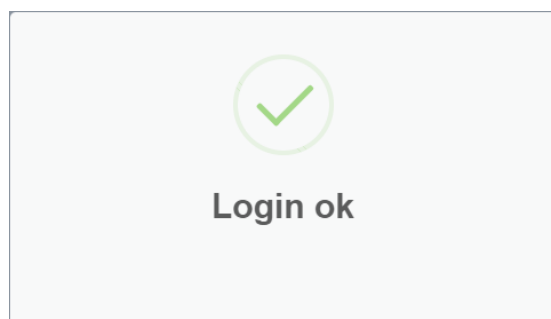
You can choose the languages, including Dutch , French ,English andTaiwan.



#### 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.

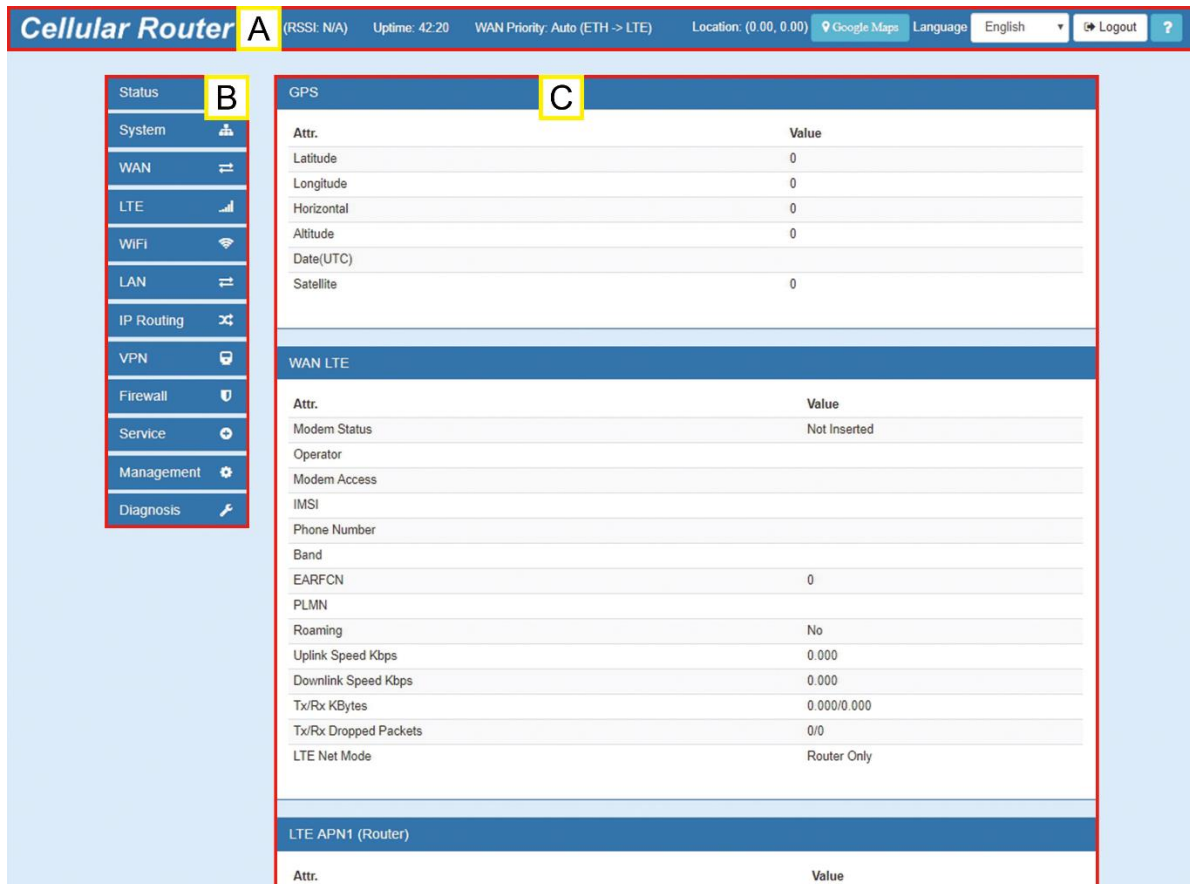
A screenshot of the router's login page. It has a blue header with the word 'Login'. Below the header, there are two input fields: 'User Name' containing the text 'root' and 'Password' containing seven dots. At the bottom right of the form area is a blue button labeled 'Login'.

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

## 3.2 Navigate the Web Configurator

The main screen is divided into three parts as below.

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



(1) **A** : Title Bar

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



Title Bar	
Item	Description
<b>RSSI</b>	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.
<b>Uptime</b>	Show the time starting turn on the router until current using.
<b>WAN Priority</b>	Show the three mode of WAN status, which is first to use.
<b>Location</b>	Show the position of router from Google Maps. <b>Note:</b> This function is for GPS spec.
<b>Google Maps</b>	Display Google Map according to location.
<b>Language</b>	Choose your language from the drop-down list on the upper right corner of the title bar.
<b>Login/Logout</b>	Click to log in or log out of the web configurator.
<b>?</b>	Online Manual

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

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

(3) **C** : Main Window

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

## 4 Status

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

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

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

Cellular Router

(RSSI: N/A)
Uptime: 1:42:30
WAN Priority: Auto (ETH -> LTE)
Location: (0.00, 0.00)
Google Maps
Language: English
Logout
?

Status

System

WAN

LTE

WiFi

LAN

IP Routing

VPN

Firewall

Service

Management

Diagnosis

GPS

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

WAN LTE

Attr.	Value
Modem Status	Not Inserted
Operator	
Modem Access	
IMSI	
Phone Number	
Band	
EARFCN	0
PLMN	
Roaming	No
Uplink Speed Kbps	0.000
Downlink Speed Kbps	0.000
Tx/Rx KBytes	0.000/0.000
Tx/Rx Dropped Packets	0/0
LTE Net Mode	Router Only

LTE APN1 (Router)

Attr.	Value
IPv4 Address	
IPv4 Mask	
Default Gateway	
Connected	No
IPv4 Conn Time	00:00
Uplink Speed Kbps	0.000
Downlink Speed Kbps	0.000
Tx/Rx KBytes	0.000/0.000
Tx/Rx Dropped Packets	0/0

LTE APN1 DNS

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

WAN Ethernet

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

LAN Ethernet

Attr.	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	
IPv6 Conn Time	00:00
Uplink Speed Kbps	31.000
Downlink Speed Kbps	5.000
Tx/Rx KBytes	5650.000/1774.000
Tx/Rx Dropped Packets	0/0

Connected VPN Connections

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

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

Status > WAN LTE	
Item	Description
<b>Attribute</b>	
<b>Modem Status</b>	The status of LTE.
<b>Operator</b>	Display the name of operator.
<b>Modem Access</b>	The router to access protocol type.
<b>IMSI</b>	The IMSI number of the SIM card.
<b>Phone Number</b>	The phone number of the SIM card.
<b>Band</b>	The current connected Band.
<b>EARFCN</b>	Absolute radio-frequency channel number.
<b>PLMN</b>	Public LAN Mobile Network ID.
<b>Roaming</b>	Roaming status.
<b>Uplink Speed Kbps</b>	Uplink Speed in Kbps.
<b>Downlink Speed Kbps</b>	Downlink Speed in Kbps.
<b>Tx/Rx KBytes</b>	Accumulated TX/RX in KBytes.
<b>Tx/Rx Droppes Packets</b>	TX/RX Dropped Packets.
<b>LTE Net Mode</b>	LTE Network Mode for both APNs.

Status > LTE APN1 / LTE APN2	
Item	Description
<b>Attribute</b>	
<b>IPv4 Address</b>	Ethernet WAN obtain IPv4 Address.
<b>IPv4 Mask</b>	Ethernet WAN obtain IPv4 Mask.
<b>Default Gateway</b>	Ethernet WAN IPv4 Default Gateway.
<b>Connected</b>	Yes: Connected; No: Disconnected.
<b>IPv4 Conn Time</b>	Ethernet WAN IPv4 Connected Time.
<b>Uplink Speed Kbps</b>	Uplink Speed in Kbps.
<b>Downlink Speed Kbps</b>	Downlink Speed in Kbps.
<b>Tx/Rx KBytes</b>	Accumulated TX/RX in KBytes.
<b>Tx/Rx Droppes Packets</b>	TX/RX Dropped Packets.

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

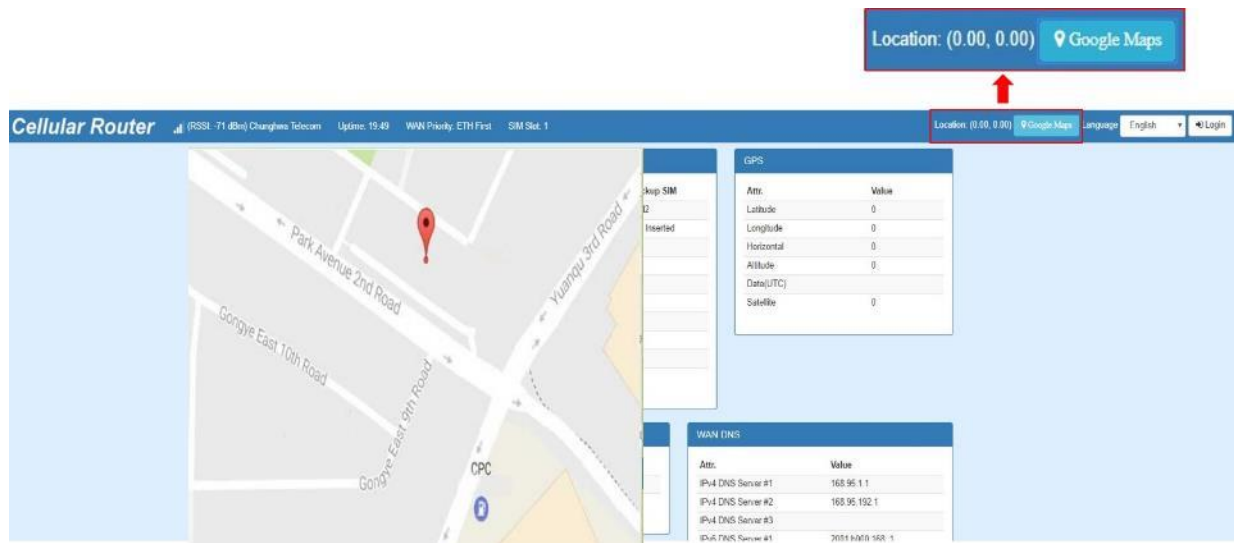
Status > WAN Ethernet	
Item	Description
<b>Attribute</b>	
IPv4 Address	Ethernet WAN obtain IPv4 Address.
IPv4 Mask	Ethernet WAN obtain IPv4 Mask.
Default Gateway	Ethernet WAN IPv4 Default Gateway.
IPv6 Conn Time	Ethernet WAN IPv4 Connected Time.

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

Status > GPS	
Item	Description
<b>Attribute</b>	
Open VPN	Open VPN connected number
IPSec	IPSec connected number
GRE	GRE connected number
PPTP Server	PPTP server connected number
L2TP	L2TP connected number

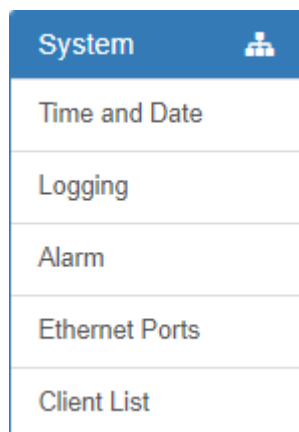
## 4.1 Status > GPS

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, Logging, Alarm, Ethernet Ports, and Client List.



### 5.1 System > Time and Date

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


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

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



## I. Get from Time Server

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

 Time And Date

Current Time Mar 15, 2019 9:21:24 AM

### Time and Date Setup

Mode

☐ Manual ☒ Get from Time Server

GPS Time

☐ Off ☒ On

IPv4 Server #1

0.openwrt.pool.ntp.org

IPv4 Server #2

pool.ntp.org

IPv4 Server #3

clock.sjc.he.net

IPv6 Server #1

time-d.nist.gov

IPv6 Server #2

2.pool.ntp.org

IPv6 Server #3

clock.nyc.he.net

### Time Zone Setup

Time Zone

(GMT) Greenwich Mean Time : Dublin Edinburgh, Lisbon, London ▼

Daylight Savings

☒ Off ☐ On

Ahead of standard time

60 mins

Start Date

3 / 2 / 0 (Month / Week / Day)

Start Time

2 : 0 (Hour : Minute)

End Date

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

End Time

2 : 0 (Hour : Minute)

### Time Server

Server Mode

☒ Off ☐ On


Server Port

123

Apply

## II. Manual

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

 Time And Date

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

Time and Date Setup

Mode ☒ Manual ☐ Get from Time Server

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

Time Zone Setup

Time Zone (GMT) Greenwich Mean Time : Dublin Edinburgh, Lisbon, London ▼

Daylight Savings ☒ Off ☐ On

Ahead of standard time 60 mins

Start Date 3 / 2 / 0 (Month / Week / Day)

Start Time 2 : 0 (Hour : Minute)

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

End Time 2 : 0 (Hour : Minute)

Time Server

Server Mode ☒ Off ☐ On

Server Port 123

Apply

## III. Time Zone Setup

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

## Time Zone Setup

Time Zone (GMT) Greenwich Mean Time : Dublin Edinburgh, Lisbon, London ▼

Daylight Savings ☐ Off ☒ On

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

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

### 5.2.1 Logging > Logging

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

 **Logging**

Mode ☐ Disable ☒ Enable

Remote Log ☒ Disable ☐ Enable

Log Server Address


**Apply**

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. ( <b>Note:</b> This server should have installed Log software.)

## 5.2.2 Logging > Log

This section displays all data status.

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

 Log

**Clear** **Refresh** **Download Logs**

#	Date	Level	Group	Module	Message
---	------	-------	-------	--------	---------

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

## 5.3 System > Alarm

This section allows you to configure the alarm.

### Note:

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

System > Alarm	
Item	Description
<b>Mode</b>	Turn on/off the Alarm configuration. Select from Disable or Enable. The default is Enable.
<b>Alarm Input</b>	Select from SMS, DI 1, DI 2, VPN disconnect and WAN disconnect as input to trigger alarm. <ul style="list-style-type: none"> <li>• <b>SMS:</b> It means on duty team members on Contacts / On Duty can send SMS to the phone number of using SIM card to trigger alarm.</li> <li>• <b>DI:</b> IO to trigger alarm.</li> <li>• <b>VPN disconnect:</b> All tunnels get disconnected then trigger alarm.</li> <li>• <b>WAN disconnect:</b> WAN connections get disconnected then trigger alarm.</li> <li>• <b>LAN disconnect:</b> LAN connection get disconnected then trigger alarm.</li> <li>• <b>Reboot:</b> Reboot then trigger alarm.</li> </ul>
<b>Alarm Output</b>	Select from SMS, DO, SNMP trap and E-mail as alarm output.
<b>DI 1 / 2</b>	Select from High or Low. The default is High Trigger.

<b>Trigger</b>	<ul style="list-style-type: none"> <li>• <b>High:</b> SW is On to trigger.</li> <li>• <b>Low:</b> SW is OFF to trigger.</li> </ul>
<b>DO behavior</b>	<ul style="list-style-type: none"> <li>• <b>Always:</b> Pull DO high.</li> <li>• <b>Pulse:</b> High and Low continuously.</li> <li>• <b>Pulse Time Length:</b> Pulse time length (mini seconds).</li> </ul>
<b>SMS/E-mail</b>	Write your messages and limit 150 English characters for the messages to deliver.

### 5.3.1 Alarm > Contacts > Create and name the Group

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

Alarm

Mode

☒ Disable
☐ Enable

Alarm input

☒ SMS
☒ DI
☒ VPN disconnect
☒ WAN disconnect

☒ LAN disconnect
☒ Reboot

Alarm output

☒ SMS
☒ DO
☒ SNMP trap
☒ E-mail

☒ TR069

DI 1 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

Contacts / On Duty

Contacts

Duty Schedule

All Users

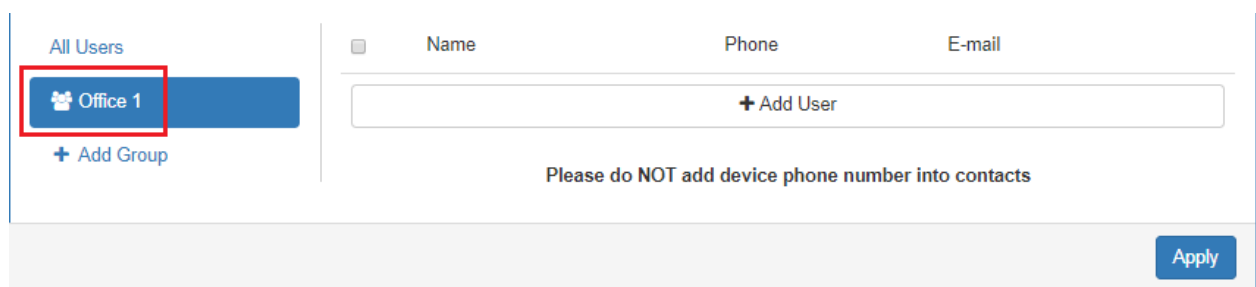
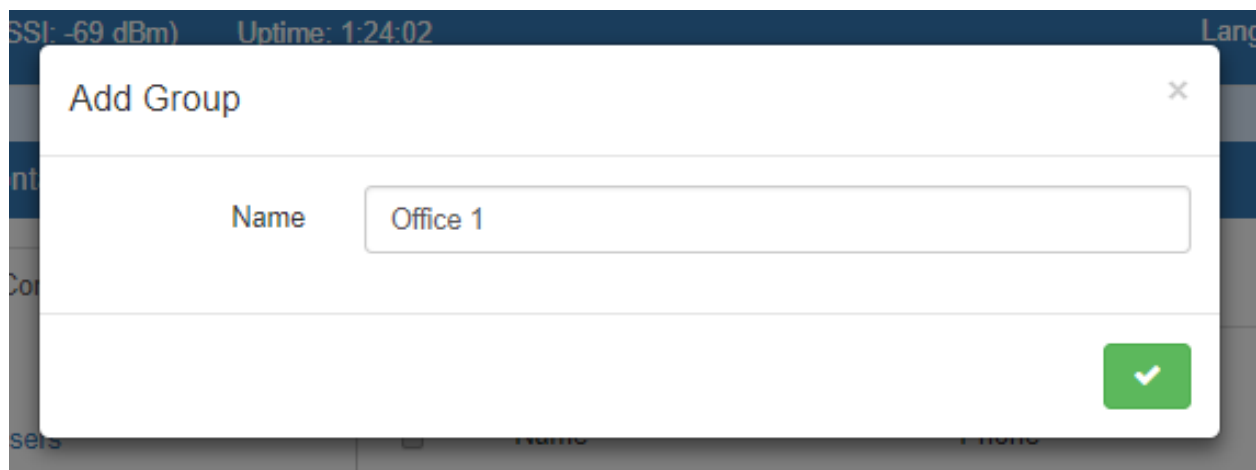
+ Add Group



☐ Name
Phone
E-mail

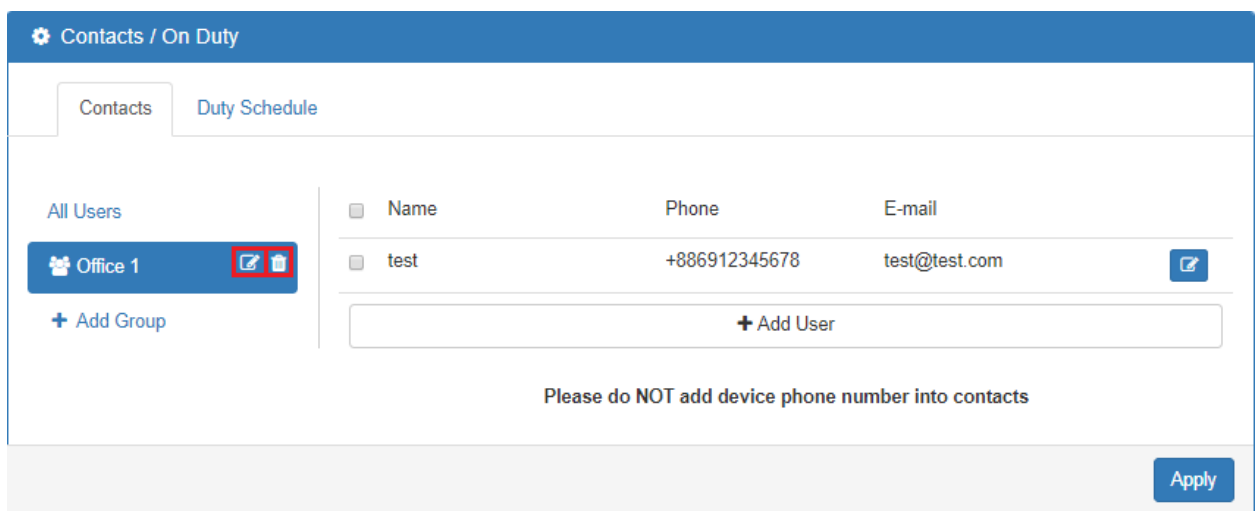
+ Add User

Please do NOT add device phone number into contacts

Apply



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





### 5.3.2 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.

Contacts / On Duty

Contacts Duty Schedule

All Users


Office 1

+ Add Group

Name	Phone	E-mail
+ Add User		

Please do NOT add device phone number into contacts

Apply

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

Add User


Name test

Phone +886912345678

E-mail test@test.com

Groups Office 1

Please do NOT add device phone number into contacts



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


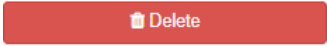
All Users

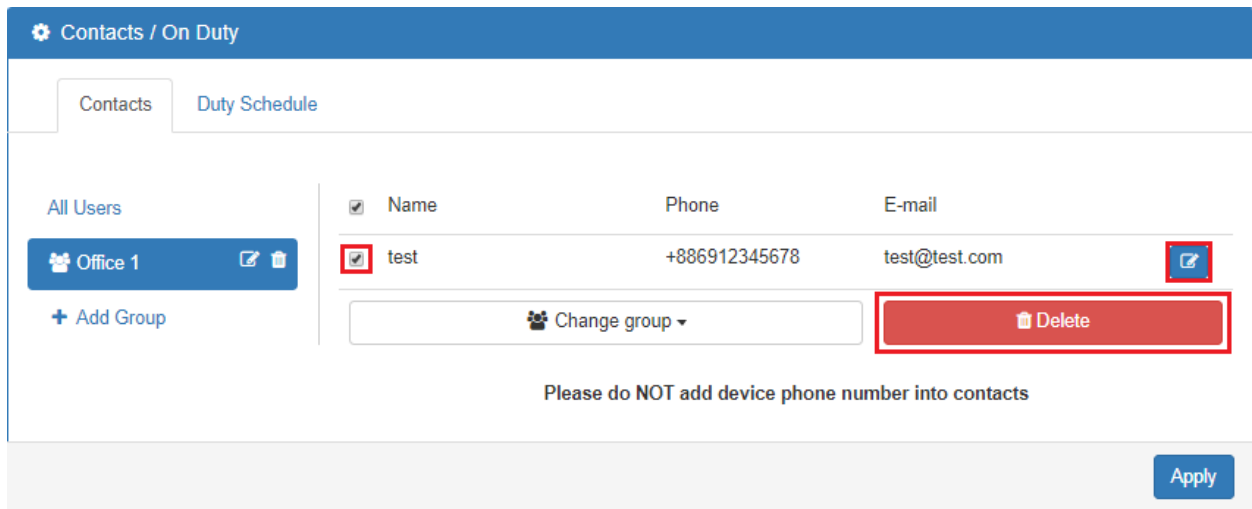
Office 1

+ Add Group

Name	Phone	E-mail
test	+886912345678	test@test.com
+ Add User		

Please do NOT add device phone number into contacts

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




Contacts / On Duty

Contacts Duty Schedule

All Users

Office 1

+ Add Group

<input checked="" type="checkbox"/>	Name	Phone	E-mail	
<input checked="" type="checkbox"/>	test	+886912345678	test@test.com	

Change group

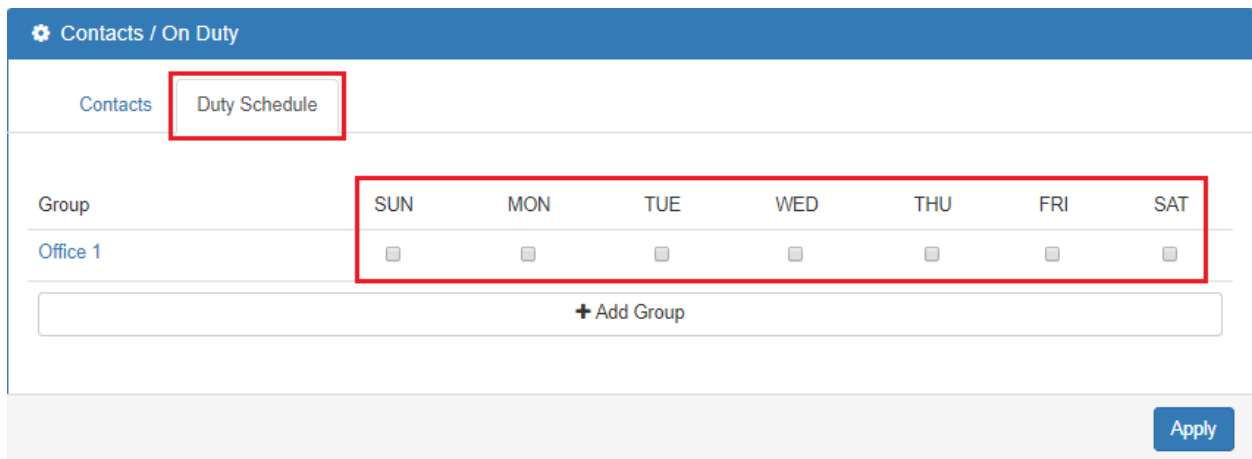
Delete

Please do NOT add device phone number into contacts

Apply

### 5.3.3 Alarm > Duty Schedule

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



Contacts / On Duty

Contacts Duty Schedule

Group	SUN	MON	TUE	WED	THU	FRI	SAT
Office 1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

+ Add Group

Apply

## 5.4 System > Ethernet Ports

This section allows you to configure the Ethernet.

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

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

Ethernet

### Ethernet Ports Status

LAN	100M Full
WAN	Off

### Ethernet Ports Configurations

LAN	<input checked="" type="radio"/> Auto <input type="radio"/> 100M Full <input type="radio"/> 100M Half <input type="radio"/> 10M Full <input type="radio"/> 10M Half <input type="radio"/> Disable
WAN	<input checked="" type="radio"/> Auto <input type="radio"/> 100M Full <input type="radio"/> 100M Half <input type="radio"/> 10M Full <input type="radio"/> 10M Half <input type="radio"/> Disable

### WAN Ethernet

WAN MTU	<input type="text" value="1500"/> <span>min: 500; max: 1500</span>
---------	--

### Flow Control

LAN	<input type="radio"/> Off <input checked="" type="radio"/> On
-----	---

### WAN/LAN2 Port Function

	<input checked="" type="radio"/> Auto <input type="radio"/> WAN <input type="radio"/> LAN2
Hint	For Auto mode, it decided by WAN Priority setting

Refresh

Apply

System > Ethernet Ports	
Item	Description
<b>Ethernet Ports Status</b>	Show the connectivity status of LAN and WAN.
<b>Ethernet Ports Configurations</b>	Select from Auto, 100M Full, 100M Half, 10M Full, 10M Half and Disable.
<b>WAN Ethernet</b>	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.
<b>Flow Control</b>	Allow users to control the traffic ingress from Ethernet LAN or WAN.
<b>WAN/LAN2 Port Function</b>	Allow users to setup the WAN/LAN2 Port function as Auto, LAN, or WAN.

## 5.5 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.

Client List					
List Type		<input type="checkbox"/> DHCP Client	<input type="checkbox"/> Online		
#	IP Address	MAC Address	Hostname	Start	End
1	192.168.1.19	00:e0:4c:68:21:73			

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

## 6 Configuration > WAN

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

WAN
Priority
Ethernet
IPv6 DNS

### 6.1 WAN > Priority

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

Priority	
WAN Priority	<div>Auto (ETH -&gt; LTE)</div>
Hint	<div>Auto (ETH -&gt; LTE)</div> <div>LTE Only</div> <div>ETH Only</div>
<div>Apply</div>	

Priority

WAN Priority

LTE Only

LTE Net Mode

Bridge + Router

Bridge Only

Router Only

Dual Router

Hint

Ethernet WAN as LAN2 when WAN/LAN2 Port Function is Auto

Apply

WAN > Priority	
Item	Description
Priority	<ul style="list-style-type: none"> <li>• <b>Auto (ETH -&gt; LTE):</b> WAN Ethernet is first priority and the second priority is LTE.</li> <li>• <b>LTE Only:</b> The priority is only LTE.</li> <li>• <b>ETH Only:</b> The priority is only WAN Ethernet.</li> </ul>
LTE Net Mode (The priority is LTE Only)	<ul style="list-style-type: none"> <li>• <b>Bridge + Router:</b> APN1 act as bridge for internet access. APN2 act as router for management from WAN site which like TR069, ssh...</li> <li>• <b>Bridge Only:</b> APN1 act as bridge for internet access.</li> <li>• <b>Router Only:</b> APN1 act as router for internet access.</li> <li>• <b>Router + Router:</b> APN1 act as router for internet access. APN2 act as router for management from WAN site which like TR069, ssh...</li> </ul>

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

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

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

WAN Ethernet

Work As

☒ DHCP Client
☐ PPPoE Client
☐ Static IPv4

Configuration

Ethernet Ping Health

DNS Server Configuration

IPv4 DNS Server #1

From ISP

From ISP

User Defined

None

IPv4 DNS Server #2

From ISP

From ISP

User Defined

None

IPv4 DNS Server #3

From ISP

From ISP

User Defined

None

Apply

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

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

The screenshot shows the 'WAN Ethernet' configuration page. At the top, there's a header 'WAN Ethernet' with a double-headed arrow icon. Below it, the 'Work As' section has three radio buttons: 'DHCP Client', 'PPPoE Client' (which is selected), and 'Static IPv4'. There are two tabs: 'Configuration' (active) and 'Ethernet Ping Health'. The main section is titled 'PPPoE Client Configuration'. It contains two input fields: 'User Name' with the value 'test' and 'Password' with masked characters '\*\*\*\*\*'. At the bottom right, there is an 'Apply' button.

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 page with 'Static IPv4' selected. The 'Work As' section now has 'Static IPv4' selected. The 'Configuration' tab is active. The main section is titled 'Static IPv4 Configuration'. It contains three input fields: 'IP Address' with '0.0.0.0', 'IP Mask' with '255.255.255.0', and 'Gateway Address' with '0.0.0.0'. Below this is a section titled 'DNS Server Configuration' with three input fields for 'IPv4 DNS Server #1', 'IPv4 DNS Server #2', and 'IPv4 DNS Server #3', all of which are currently empty. At the bottom right, there is an 'Apply' button.

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

## 6.2.2 Ethernet Ping Health

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

WAN Ethernet

Work As
☐ DHCP Client
☐ PPPoE Client
☒ Static IPv4

Configuration
Ethernet Ping Health

Ethernet Ping Health
☐ Disable
☒ Enable

Interval
(1 ~ 60 Seconds)

IPv4 Host 1

IPv4 Host 2

IPv6 Host 1

IPv6 Host 2

Hint

Wan Priority: Auto  
Ethernet ping health: Enable

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

Apply



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

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

✓ WAN Ethernet

Attr.	Value
IPv4 Address	118.167.125.240
IPv4 Mask	255.255.255.255

✓ LAN Ethernet

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

## 6.3 WAN > IPv6 DNS

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

IPv6 DNS

### APN1 DNS Server Configuration

IPv6 DNS Server #1	From ISP ▼	
IPv6 DNS Server #2	From ISP ▼	
IPv6 DNS Server #3	From ISP ▼	

### APN2 DNS Server Configuration

IPv6 DNS Server #1	From ISP ▼	
IPv6 DNS Server #2	From ISP ▼	
IPv6 DNS Server #3	From ISP ▼	

Apply

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.

IPv6 DNS

### APN1 DNS Server Configuration

IPv6 DNS Server #1	From ISP ▼	
IPv6 DNS Server #2	From ISP ▼	
IPv6 DNS Server #3	From ISP ▼	

### APN2 DNS Server Configuration


IPv6 DNS Server #1	From ISP ▼	
IPv6 DNS Server #2	From ISP ▼	
IPv6 DNS Server #3	From ISP ▼	

Apply

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

## 7 Configuration > LTE

This section allows you to configure LTE Config, GPS Config, Dual APN, APN Usage, SMS, Serving Cell, and DNS.

LTE 
LTE Config
GPS Config
Dual APN
APN1 Usage
APN2 Usage
SMS
Serving Cell
DNS

## 7.1 LTE > LTE Config

### 7.1.1 LTE Configuration

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

LTE Config

LTE Config

Auto

▼

Change this field require rebooting

MTU

1500

min: 500; max: 1500

LTE Ping Health

LTE Ping Health

☐ Disable ☒ Enable

Interval

60

Seconds

IPv4 Host 1

8.8.8.8

IPv4 Host 2

8.8.4.4

IPv6 Host 1

2001:4860:4860::8888

IPv6 Host 2

2001:4860:4860::8844

Hint

LTE ping health: Enable

- Then system ping specified IP address to avoid the base station kick out the idle device.

Apply

LTE Config

LTE Config

Auto

▼

Change this field require rebooting

MTU

4G Only  
3G Only  
2G Only

min: 500; max: 1500

LTE Ping Health

LTE > LTE Config	
Item	Description
LTE Config	<ul style="list-style-type: none"><li><b>Auto:</b> Automatically connect the possible band.</li><li><b>4G Only:</b> Connect to 4G network only.</li><li><b>3G Only:</b> Connect to 3G network only.</li><li><b>2G Only:</b> Connect to 2G network only.</li></ul>
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.

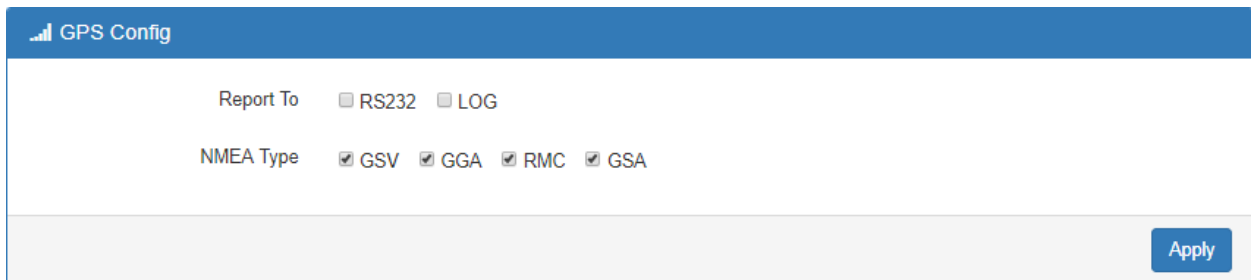
### 7.1.2 LTE Ping Health

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

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

## 7.2 LTE > GPS Config

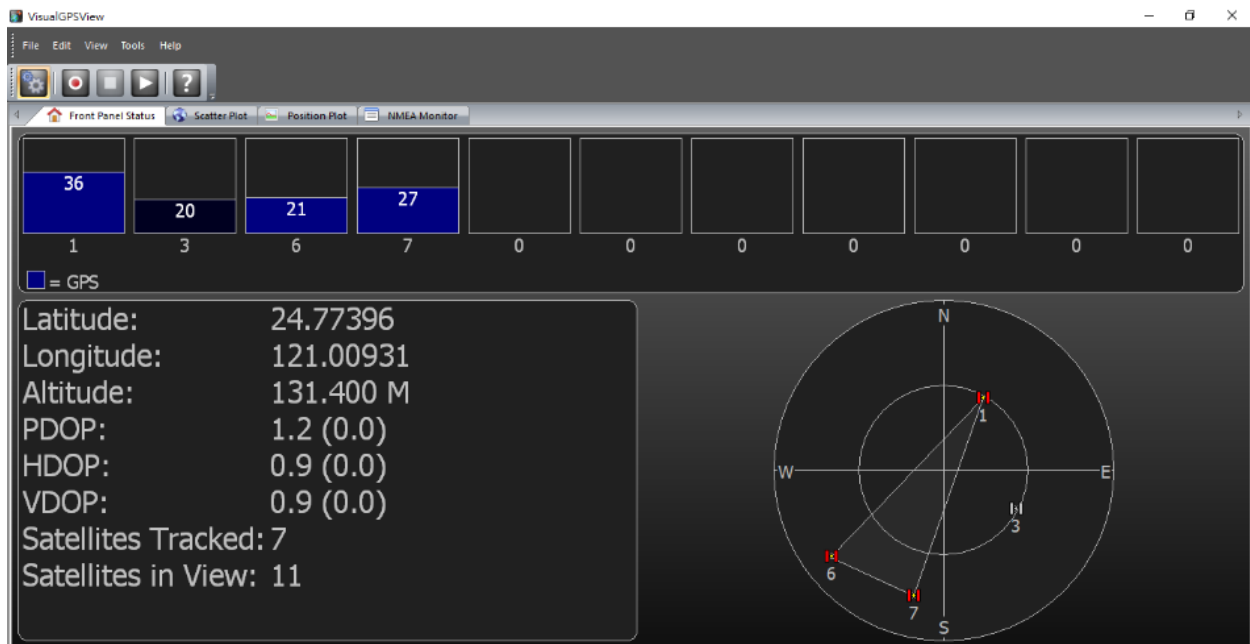
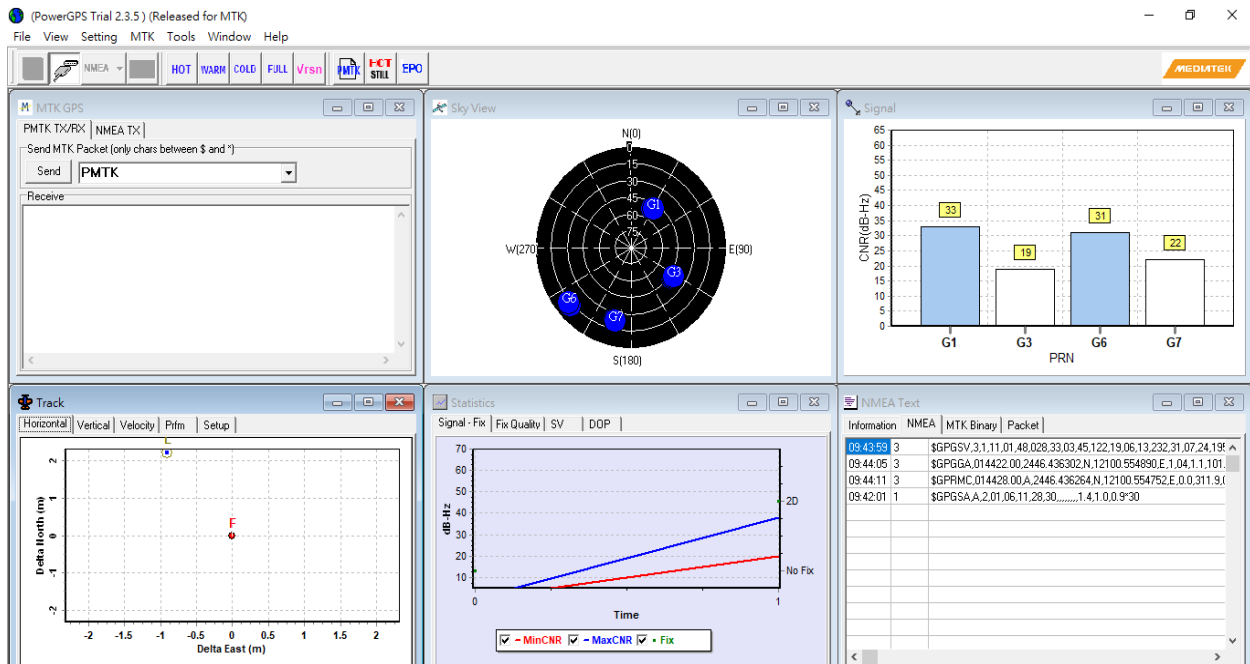
This section allows you to set up GPS Configuration and connect RS232 from the used router to have more detailed information for your specific purpose.

The image shows a screenshot of the 'GPS Config' interface. At the top, there is a blue header bar with the text 'GPS Config' and a signal strength icon. Below the header, the interface is divided into two sections. The first section is labeled 'Report To' and contains two checkboxes: 'RS232' and 'LOG'. The second section is labeled 'NMEA Type' and contains four checkboxes: 'GSV', 'GGA', 'RMC', and 'GSA'. All four checkboxes in the 'NMEA Type' section are checked. At the bottom right of the interface, there is a blue button labeled 'Apply'.

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

LTE > GPS Config	
Item	Description
<b>Report to</b>	Select from RS232 and LOG.
<b>NMEA Type</b>	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 APN

This section allows you to understand the status of connectivity for Dual APN.

Dual APN

Connect Policy

Connect Action

Disable Roaming ☐ No ☒ Yes

SIM Configuration APN1 APN2

Status Not Inserted

☒ SIM PIN Enable

SIM PIN

Confirmed SIM PIN

SIM PUK

Confirmed SIM PUK

Change SIM PIN

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

**Change**

Old PIN

New PIN

PIN Remaining Number

0

PUK Remaining Number

0

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

LTE > Dual SIM	
Item	Description
<b>Connect Policy</b>	
Connect Action	<ul style="list-style-type: none"> <li>● <b>Connect</b>: After manually disconnect, it will show <b>Connect</b> button. Click to get connection or reboot the device to make it automatically connect.</li> <li>● <b>Disconnect</b>: When getting connection, the <b>Disconnect</b> button appear. After manually click Disconnect, the system would not automatically get connection until next reboot.</li> </ul>
Disable Roaming	<ul style="list-style-type: none"> <li>● <b>NO</b>: Make the connection even the device is in roaming state.</li> <li>● <b>YES</b>: No connection when the device in roaming state.</li> </ul>
<b>SIM Configurations</b>	
Status	Display the status of SIM Card.
SIM PIN Enable	<ul style="list-style-type: none"> <li>● Enable to display SIM PIN setting.</li> <li>● Disable to hide SIM PIN setting.</li> </ul>
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.
Change SIM PIN	When you change the SIN PIN, please aware not to exceed the retry number (PIN remaining number and PUN remaining number).
Old PIN	Please input the current SIM PIN.
New PIN	Please input the newly update SIM PIN.



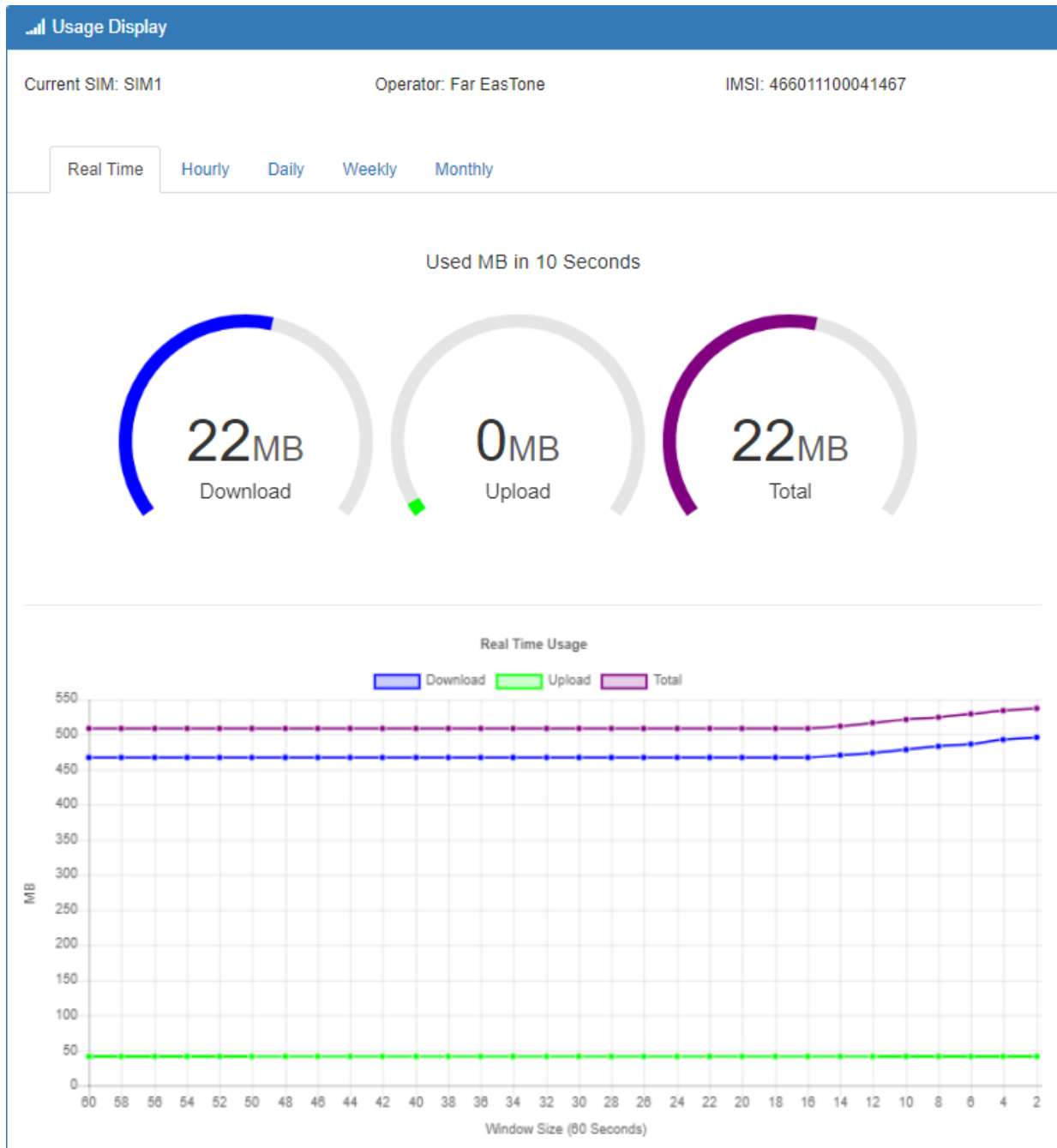
PIN remaining number	Display the allowed remaining PIN retry number.
PUK remaining number	Display the allowed remaining PUK retry number.
<b>APN1 / APN2</b>	
APN	The Access Point Name (APN) is the name of the setting that set up a connection to the gateway between your carrier's cellular network and the public Internet. Leaving it empty will search internally database automatically by SIM card for connection. However, please notice APN1 and APN2 must be manually configured different setting while concurrently use.
Username	The username can be input by user or the system will search from internal database if the APN setting is empty.
Password	The password can be input by user or the system will search from internal database if the APN setting is empty.
Confirm Password	Double confirm password.
Auth (None/PAP/CHAP)	If Auth mode is not None, most servers require username and password above.

## 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.



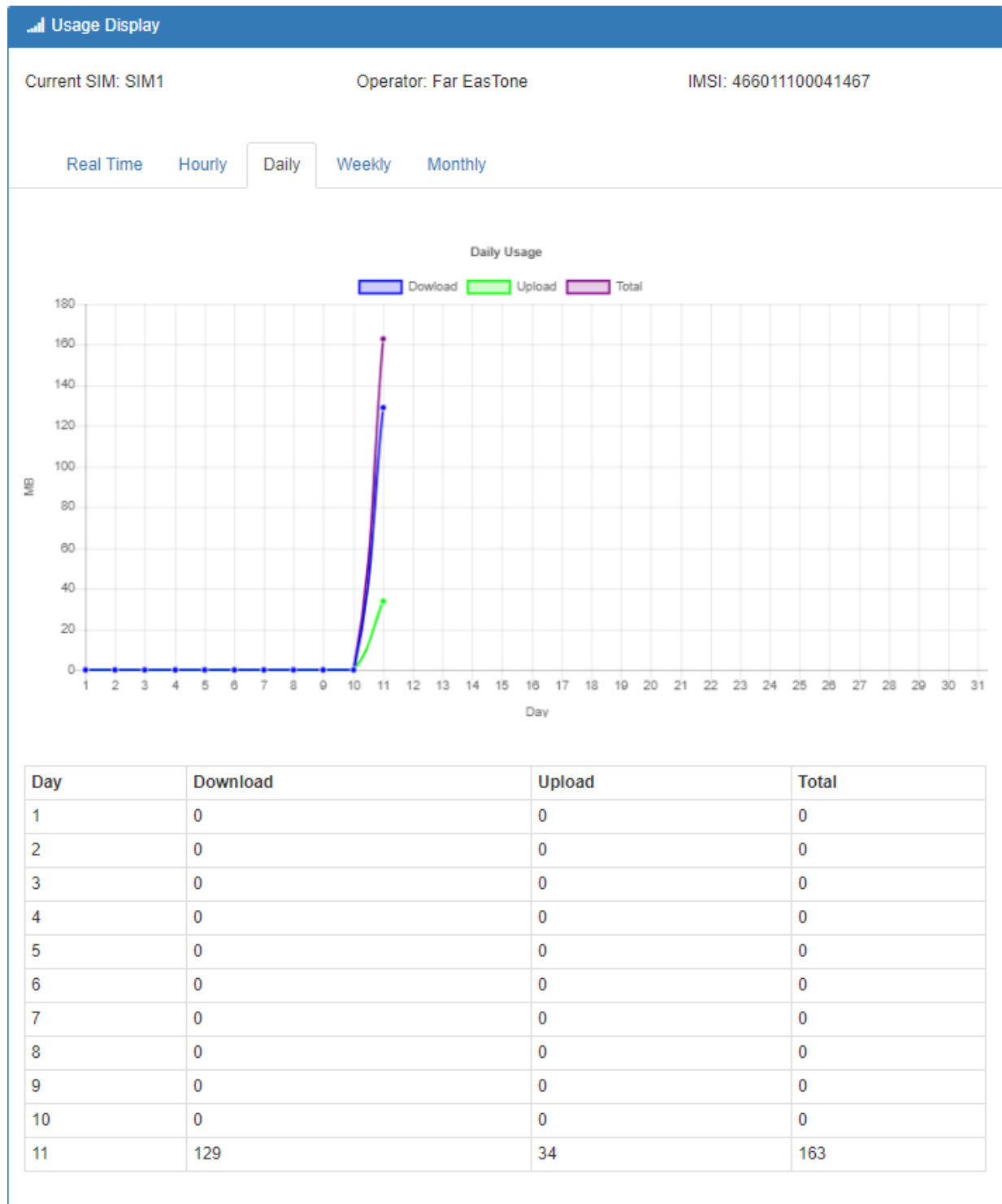
## (2) Hourly Usage:

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



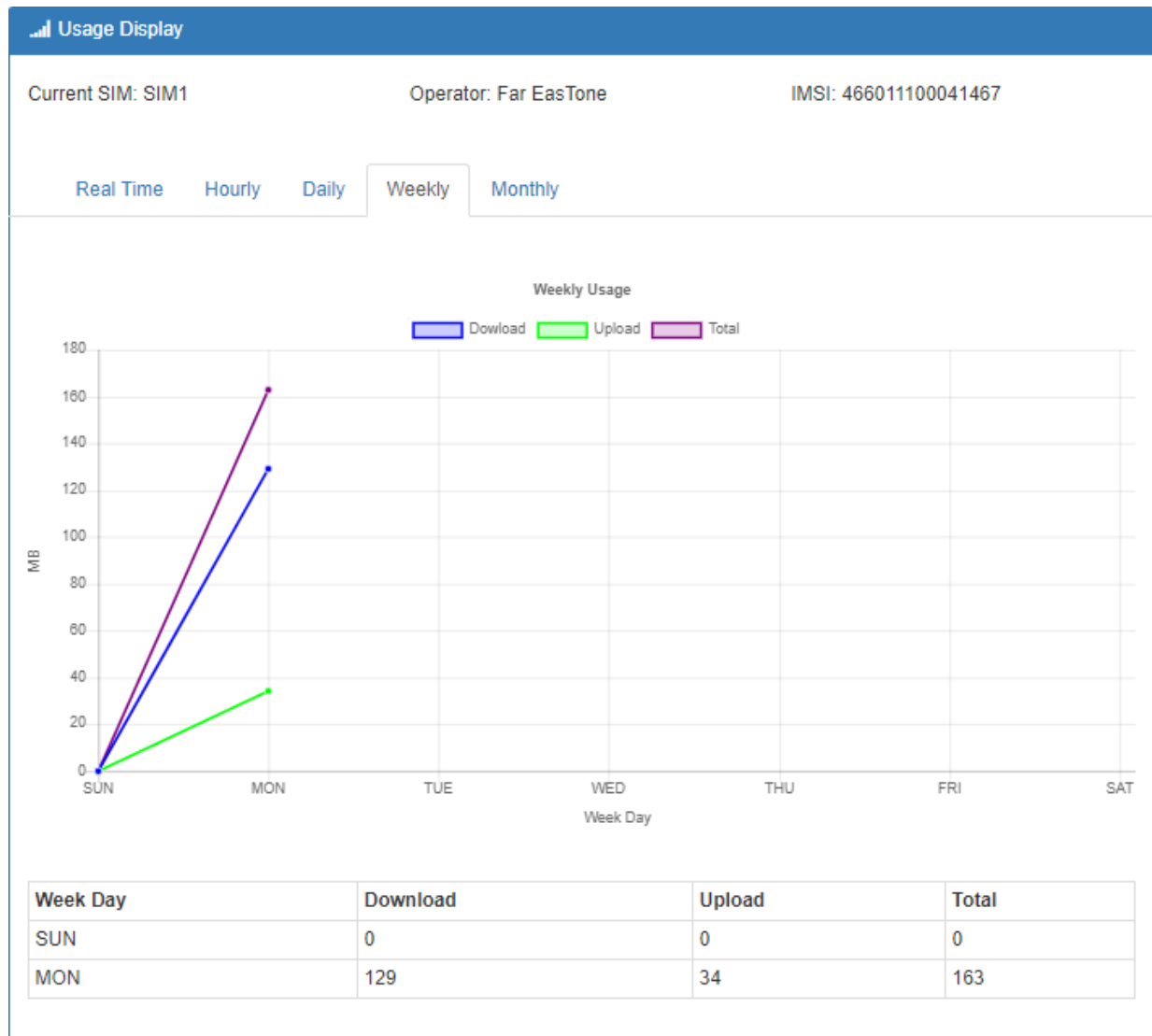
### (3) Daily Usage:

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



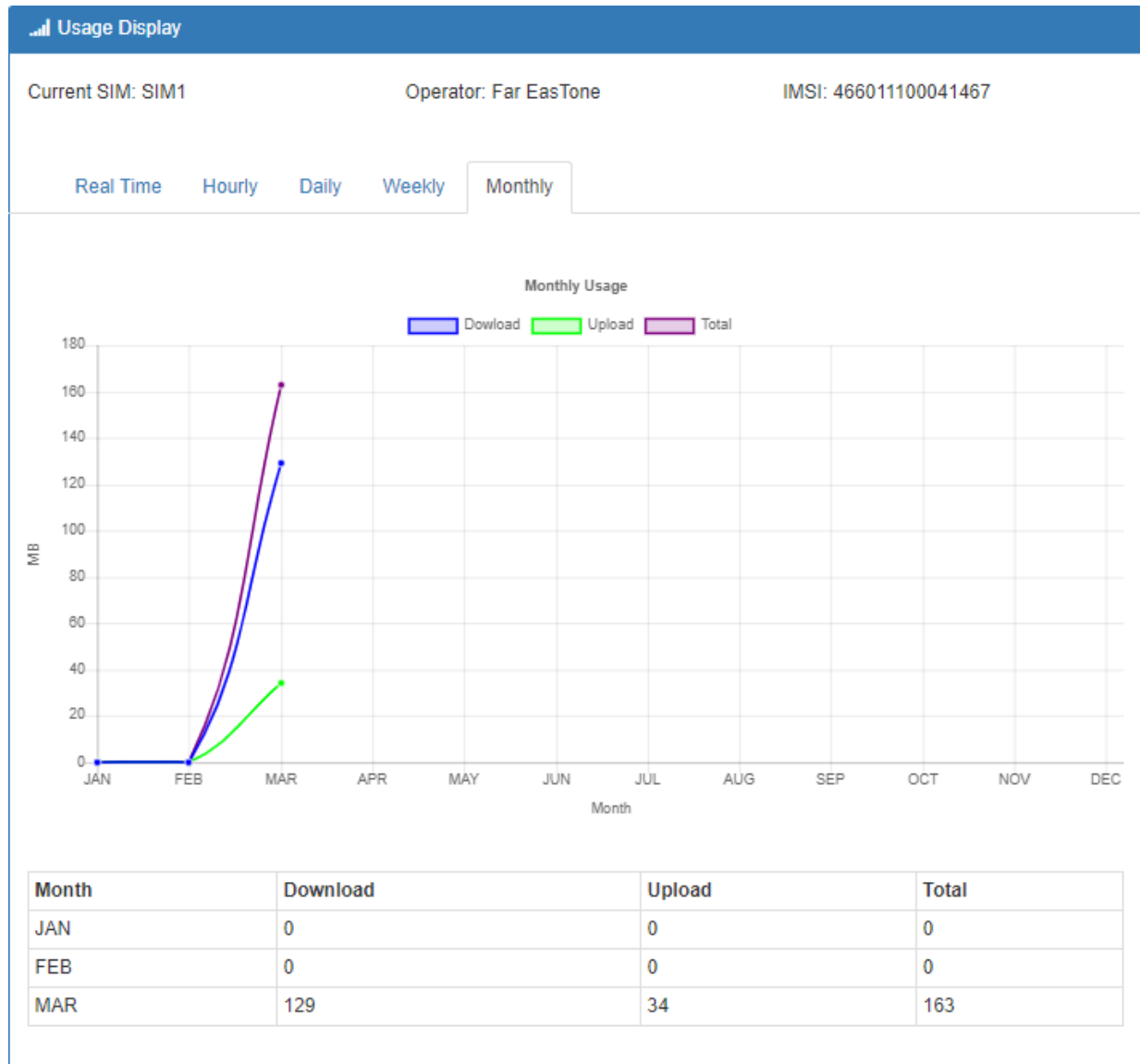
#### (4) Weekly Usage:

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.

SMS

SMS Action

View SMS



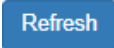
Mode ☐ Disable ☒ Enable

Actions and Keywords Setup

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

Hint: Only accept SMS from trusted and on duty members


Apply

(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.

SMS

SMS Action

View SMS

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

Clear

Refresh

18/11/14 09:48:00

005B906050B34F8696FB7B5492349AD49A575230671F901A77E5005D60A87684514D8  
CBB9AD49A575C0765BC003359295F8C5230671F002E4EFB610F937556DE8986672C7  
C218A0A621675

Close



## 7.6 LTE > Serving Cell


This section displays all parameters, including the following items:

Serving Cell	
Attr.	Value
Rate	LTE
RSRP	-104
RSRQ	-9
SINR	12
RSCP	
ECIO	0
Cell Identity	220147-13
eNB ID	220147
Cell ID	13
PCI ID	237
EARFCN	3250
UL Bandwidth	20MHz
DL Bandwidth	20MHz
RSSI	0 dBm
Refresh	

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

## 7.7 LTE > DNS

This section allows you to setup LTE specific DNS setting.

 DNS

### APN1 DNS Server Configuration

IPv4 DNS Server #1	<div>From ISP ▼</div>	<input type="text"/>
IPv4 DNS Server #2	<div>From ISP User Defined None</div>	<input type="text"/>
IPv4 DNS Server #3	<div>From ISP ▼</div>	<input type="text"/>

### APN2 DNS Server Configuration


IPv4 DNS Server #1	<div>From ISP ▼</div>	<input type="text"/>
IPv4 DNS Server #2	<div>From ISP ▼</div>	<input type="text"/>
IPv4 DNS Server #3	<div>From ISP ▼</div>	<input type="text"/>

Apply

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

## 8 Configuration > WiFi (RT-MOB-020)

This section allows you to set up the WiFi configuration.

**WiFi** 


WiFi Config

MAC Filter

Client List

### 8.1 WiFi > WiFi Config

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

 Config

**WiFi Network**

AP Enable

☐ Disable ☒ Enable

AP Isolate

☒ Off ☐ On

HT Mode

☒ 20M ☐ 40M

Country Code

TW - Taiwan

Channel

Auto

Name(SSID)

M330-W-44d1fa72d797

Hidden SSID

☒ Off ☐ On

Security Option

WPA2-PSK(AES)

Passphrase

\*\*\*\*\*

(8~63 characters)

Key Update

0

(0 no update or 30~86400 seconds)

Apply

WiFi > Config	
Item	Description
AP Enable	Turn on/off the Wi-Fi Network. Select from Disable or Enable. The default is Enable.
AP Isolate	AP isolation is a technique for preventing mobile devices connected to an AP from communicating directly with each other.
HT Mode (HT Capability)	20M: Only 20MHz Operation is Supported,40M: Both 20MHz and 40MHz Operation is Supported.
Country Code	Select Country Area for supported Channels

WiFi > Config	
Item	Description
<b>Name(SSID)</b>	SSID is Wi-Fi identification. The maximum length is 32
<b>Hidden SSID</b>	SSID hiding is the process of hiding the network name from being publicly broadcast.
<b>Channel</b>	Auto (Automatically select the best channel) or manually select channel number.
<b>Security Option</b>	None / WPA2-PSK(AES).
<b>Passphrase</b>	The legal length is 8 ~ 63. The string should belong to [0-9 A-F a-f].
<b>Key Update</b>	0 means no update or 30~86400 seconds update period.

## 8.2 WiFi > MAC Filter

This section allows you to set up MAC Filter.

WiFi Network MAC Filter

Mode

☒ Disable
 ☐ Enable

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

Apply

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

Edit MAC Filter Entry #1

Mode

☒ Disable ☐ Enable


MAC Address

Save

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

### 8.3 WiFi > Client List

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

 Client List

WiFi Client List

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

Refresh

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

## 9 Configuration > LAN

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

LAN	⇌
IPv4	
IPv6	
VLAN	
Subnet	

### 9.1 LAN > IPv4

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

⇌ LAN IPv4	
IP Address	192.168.1.1
IP Mask	255.255.255.0
DHCP Server Configuration	
<input checked="" type="checkbox"/> DHCP Server Configuration	
IP Address Pool	From 192.168.1.2 To 192.168.1.254
Apply	

LAN > IPv4	
Item	Description
LAN IPv4	<ul style="list-style-type: none"><li>IP Address:192.168.1.1</li><li>IP Mask:255.255.255.0</li></ul> 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"><li>Enable to make router can lease IP address to DHCP clients which connect to LAN.</li></ul>
IP Address Pool	<ul style="list-style-type: none"><li>Define the beginning and the end of the pool of IP addresses which will lease to DHCP clients.</li></ul>

## 9.2 LAN > IPv6

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

LAN IPv6

Type

☒ Delegate Prefix from WAN ☐ Static

Static Address

DHCP Server Configuration

Address Assign

☒ Stateful ☐ Stateless

Apply

LAN > IPv6	
Item	Description
Type	<ul style="list-style-type: none"><li>• <b>Delegate Prefix from WAN</b> Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.</li><li>• <b>Static</b> Select this option to configure a fixed IPv6 address for the cellular router's LAN IPv6 address.</li></ul>
Static Address	You need to input the static address when you select the static type.
DHCP Server Configuration	
Address Assign	<p>Select how you obtain an IPv6 address.</p> <ul style="list-style-type: none"><li>• <b>Stateless:</b> 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.</li><li>• <b>Stateful:</b> The cellular router uses IPv6 stateful auto configuration. The LAN IPv6 clients can obtain IPv6 addresses through DHCPv6.</li></ul>

## 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.

VLAN

Mode

☒ Off ☐ Tag Base

VLAN Isolation

☐ Off ☒ On

Apply

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.

VLAN

Mode

☐ Off
 ☒ Tag Base

VLAN Isolation

☐ Off
 ☒ On

Enable	Subnet	VID	Name
<input checked="" type="checkbox"/>	NET1	1	Ian(Full Feature LAN)
<input type="checkbox"/>	NET2	2	Ian.2(LAN)
<input type="checkbox"/>	NET3	3	Ian.3(LAN)
<input type="checkbox"/>	NET4	4	Ian.4(LAN)
<input type="checkbox"/>	NET5	5	Ian.5(LAN)
<input type="checkbox"/>	NET6	6	Ian.6(LAN)
<input type="checkbox"/>	NET7	7	Ian.7(LAN)
<input type="checkbox"/>	NET8	8	Ian.8(LAN)

Apply

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
<b>Mode</b>	The VLAN mode is Off or Tag Base (802.1p VLAN).
<b>VLAN Isolation</b>	The VLAN Isolation is Off or On.
<b>Enable</b>	The assigned row of setting is enabled.
<b>Subnet</b>	The subnet provides IP address and IP mask for the router.
<b>VID</b>	The VLAN ID range is from 1 to 4094.
<b>Name</b>	The Interface name and LAN feature.



## 9.4 LAN > Subnet

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

 Subnet

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

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

Apply

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

Edit Subnet NET2

IP Address

192.168.2.1

IP Mask

255.255.255.0

DHCP Server Configuration

☒ DHCP Server Configuration

IP Address Pool

From

192.168.2.2

To

192.168.2.254

Save

## 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.

**Static Route**

Mode ☒ Off ☐ On

Settings

Status

Mode	Name	Destination	Gateway	Interface	Delete
<input type="radio"/> Off <input checked="" type="radio"/> On	<input type="text"/>	192.168.100.0/24	192.168.1.250		

Mode ☐ Off ☒ On

Name

Destination

Gateway

Interface

Add

Apply

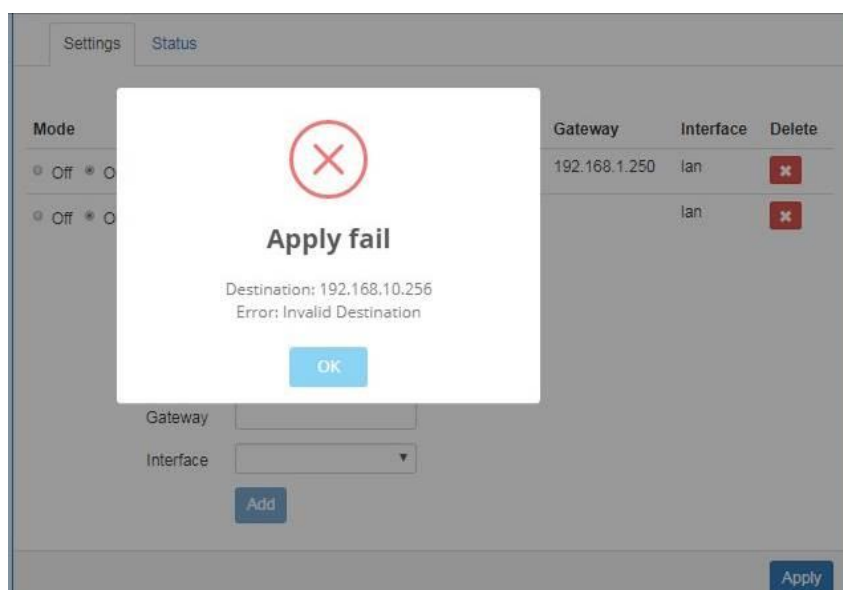
IP Routing > Static Route > Settings	
Item	Description
Mode	The setting is for full network. Select from Off or On.
Settings	
Mode	The setting is for the specific network. Select from Off or On.

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

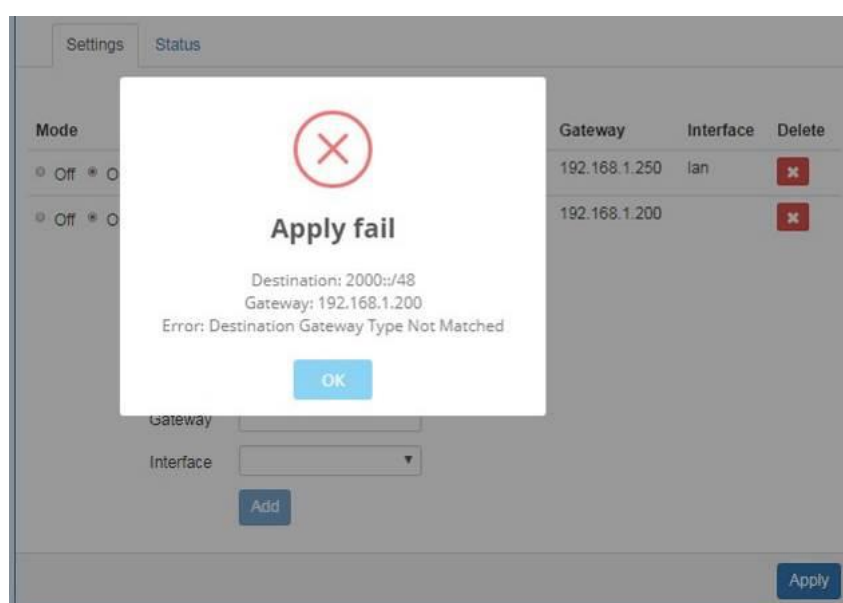
**Note:**

- 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.

 Static Route

Mode
 ☒ Off
 ☐ On

Settings
 Status

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

Apply


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.

 RIP

General

Interfaces

Mode

☒ Off ☐ On

Redistribute local routes

☒ Off ☐ On

from the device's own routing table

Redistribute connected routes

☒ Off ☐ On

to networks which are directly connected to the device

Redistribute OSPF routes

☒ Off ☐ On

learned via the OSPF routing protocol

Redistribute BGP routes

☒ Off ☐ On

learned via the BGP routing protocol

Apply

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

✕ RIP

General
Interfaces

#	Mode	Interface	Authentication	Key	Key ID	Passive	Edit	Delete
<h3>Add RIP Interface</h3> <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 45%;"> <p>Mode <input type="radio"/> Off <input checked="" type="radio"/> On</p> <p>Interface <span style="border: 1px solid #ccc; padding: 2px 10px;">eth1(WAN Ethernet) ▼</span></p> <p>Authentication <span style="border: 1px solid #ccc; padding: 2px 10px;">md5 ▼</span></p> <p>Key <span style="border: 1px solid #ccc; padding: 2px 10px;"></span></p> <p>Key ID <span style="border: 1px solid #ccc; padding: 2px 10px;">1</span></p> <p>Passive <input checked="" type="radio"/> Off <input type="radio"/> On</p> </div> <div style="width: 50%;"> <p>The key used for authentication (maxlength=16)</p> <p>The ID of the key used for authentication (1-255)</p> <p>Do not send out RIP packets on this interface</p> </div> </div> <div style="text-align: center; margin-top: 10px;"> <span style="background-color: #0056b3; color: white; padding: 5px 15px; border: 1px solid #0056b3;">Add</span> </div>								


Apply

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

 OSPF

General

Interfaces

Networks

Mode

☒ Off ☐ On

Redistribute local routes

☒ Off ☐ On

from the device's own routing table

Redistribute connected routes

☒ Off ☐ On

to networks which are directly connected to the device

Redistribute RIP routes

☒ Off ☐ On

learned via the RIP routing protocol

Redistribute BGP routes

☒ Off ☐ On

learned via the BGP routing protocol

Apply

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

## (2) Interfaces Configuration

There are 2 parts for OSPF Interfaces configuration.

- OSPF Interfaces Summary

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

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

- Add/Edit OSPF Interface

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

OSPF

General

Interfaces

Networks

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

Add OSPF Interface

Add/Edit

Mode

☐ Off
☒ On

Interface

eth1

Authentication

md5

Key

The key used for authentication (maxlength=16)

Key ID

1

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

Cost

0

The cost for sending packets via this interface (0: OSPF defaults)

Passive

☒ Off
☐ On

Do not send out OSPF packets on this interface

Add

Apply

IP Routing > OSPF > Interfaces	
Item	Description
Mode	Select from <b>Off</b> or <b>On</b> to use or not to use the OSPF function in the interface.
Interface	Select from <b>eth1 (WAN Ethernet)</b> or <b>LAN</b> .
Authentication	Select from <b>none</b> or <b>md5</b> to approve authentication. <b>Note:</b> Please offer <b>Key</b> and <b>Key ID</b> when you select <b>md5</b> 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 <b>Off</b> or <b>On</b> 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.

OSPF

General

Interfaces

Networks

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

Add OSPF Network

Add/Edit

Mode

☐ Off
 ☒ On

Prefix

xxx.xxx.xxx.xxx

Prefix of the network

Prefix Length

24

Length of the prefix

Area

0

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

Add


Apply

IP Routing > OSPF > Networks	
Item	Description
<b>Mode</b>	Select from <b>Off</b> or <b>On</b> to enable the network setting.
<b>Prefix</b>	Set Prefix of the network
<b>Prefix Length</b>	Set Length of the prefix
<b>Area</b>	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

 BGP

General

Neighbors

Networks

Mode

☒ Off ☐ On

AS Number

The number of the autonomous system (1 ~ 4294967295)

Redistribute local routes

☒ Off ☐ On

from the device's own routing table

Redistribute connected routes

☒ Off ☐ On

to networks which are directly connected to the device

Apply

IP Routing > BGP > General	
Item	Description
General	
Mode	<ul style="list-style-type: none"><li>Off: BGP function is off.</li><li>On: BGP function is on.</li></ul>
AS Number	The number of the autonomous system (1 ~ 4294967295)
Redistribute local routes	<ul style="list-style-type: none"><li>Off: Not redistribute local routes from the device's own routing table.</li><li>On: Redistribute local routes from the device's own routing table.</li></ul>
Redistribute connected routes	<ul style="list-style-type: none"><li>Off: Not redistribute connected routes to networks which are directly connected to the device.</li><li>On: Redistribute connected routes to networks which are directly connected to the device.</li></ul>

## (2) Neighbor Configuration

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

BGP

General

Neighbors

Networks

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

Add BGP Neighbor

Mode

☐ Off ☒ On

IP Address

IP address of the peer router

AS Number

Autonomous system number of the peer router

Multihop

☐ Off ☒ On

Allow multiple hops between this router and the peer router

Update Source Mode

☒ Off ☐ On

Whether to specify the source address to this neighbor

Update Source Address

The source address to this neighbor

Add

Apply

IP Routing > BGP > Neighbors	
Item	Description
Mode	Select from <b>Off</b> or <b>On</b> 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.

BGP

General

Neighbors

Networks

#	Mode	Prefix	Prefix Length	Edit	Delete
1	on	4.4.4.0	24		

Add BGP Network

Mode

☐ Off ☒ On

Prefix

Prefix of the network

Prefix Length

Length of the prefix


Add

Apply

IP Routing > BGP > Networks	
Item	Description
Mode	Select from <b>Off</b> or <b>On</b> 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

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


 Open VPN

Mode ☒ Disable ☐ Enable

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

Apply

### 11.1.1 Open VPN Common Setting

- (1) Click  button to edit Open VPN Connection.
- (2) From **Setting** tab, you can set up the connection of Open VPN.

Edit Open VPN Connection #1

Setting

Log

Mode

☒ Disable ☐ Enable

VPN Mode

☐ Server ☒ Client ☐ Custom

VPN Type

☒ Roadwarrior ☐ Bridging

Status

Idle

TLS Mode

☒ Disable ☐ Enable

Cipher

BF-CBC

IPv6 Mode

☒ Disable ☐ Enable

Device

☒ TUN ☐ TAP

Protocol

☒ UDP ☐ TCP

Port

1701

VPN Compression

☒ Disable ☐ Enable

Authentication


Certificate

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"><li>● <b>Server:</b> Tick to enable Open VPN server tunnel.</li><li>● <b>Client:</b> Tick to enable Open VPN client tunnel. The default is Client.</li><li>● <b>Custom:</b> 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.</li></ul>
VPN Type	<ul style="list-style-type: none"><li>● Roadwarrior (<b>default</b>)</li><li>● <b>Bridging:</b> Bridging the VPN tunnel and LAN/VLAN</li></ul>
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.

<b>Device</b>	Select from TUN or TAP. The default is TUN.
<b>Protocol</b>	Select from UDP or TCP Client which depends on the application. The default is UDP.
<b>Port</b>	Enter the listening port of remote side Open VPN server.
<b>VPN Compression</b>	Select Disable or Enable to compress the data stream. The default is Disable.
<b>Authentication</b>	<ul style="list-style-type: none"> <li>Select from two different kinds of authentication ways: Certificate or pkcs#12 Certificate.</li> <li>The pkcs#12 option is only available on the VPN client mode.</li> </ul>

### 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  button and the file should be downloaded from Open VPN server.

Client

Server Address

Route Client Networks

☒ Off ☐ On

Local Network

Network

Netmask


NAT

1:1 NAT


☒ Off ☐ On

Client - Security


Root CA




Cert



Key



P12



Back

Refresh

Apply

VPN > Open VPN > Client VPN Mode	
Item	Description
<b>Client</b>	
<b>Server Address</b>	Fill in WAN IP of Open VPN server.
<b>Route Client Networks</b>	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.
<b>Local Network</b>	
<b>Network</b>	The local network exported by OpenVPN. When keeping this option blank, the OpenVPN will export the LAN network automatically.
<b>Netmask</b>	The local netmask exported by OpenVPN. When keeping this option blank, the OpenVPN will export the LAN netmask automatically.
<b>NAT</b>	
<b>1:1 NAT</b>	<ul style="list-style-type: none"> <li>• Tick to enable NAT Traversal for Open VPN. This item must be enabled when the router under NAT environment.</li> <li>• Select from Off or On.</li> <li>• When two routers' LAN Subnet are same and create Open VPN tunnels, this function should be turned on.</li> </ul>
<b>Client-Security</b>	
<b>Root CA</b>	The Certificate Authority file of Open VPN server could be downloaded from Open VPN server.
<b>Cert</b>	The certification file is for Open VPN client, which could be downloaded from Open VPN server.
<b>Key</b>	The private key file is for Open VPN client, which could be downloaded from Open VPN server.
<b>P12</b>	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 ☐ 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.



## Roadwarrior

Route Client Networks ☐ Off ☒ On

Connections - Net / Mask

#1	<input type="text" value="0.0.0.0"/>	/	<input type="text" value="0.0.0.0"/>
#2	<input type="text" value="0.0.0.0"/>	/	<input type="text" value="0.0.0.0"/>
#3	<input type="text" value="0.0.0.0"/>	/	<input type="text" value="0.0.0.0"/>
#4	<input type="text" value="0.0.0.0"/>	/	<input type="text" value="0.0.0.0"/>
#5	<input type="text" value="0.0.0.0"/>	/	<input type="text" value="0.0.0.0"/>
#6	<input type="text" value="0.0.0.0"/>	/	<input type="text" value="0.0.0.0"/>
#7	<input type="text" value="0.0.0.0"/>	/	<input type="text" value="0.0.0.0"/>
#8	<input type="text" value="0.0.0.0"/>	/	<input type="text" value="0.0.0.0"/>



## Local Network

Network	<input type="text" value="Blank will use default LAN network"/>
Netmask	<input type="text" value="Blank will use default LAN netmask"/>









## NAT

1:1 NAT ☒ Off ☐ On

## Server - Server Security

Root CA	 Create
Cert, Key	 Create

## Server - User Security

ovpn Server Address	<input type="text" value="blank: auto detect the WAN IP address"/>		
User 1	<input type="checkbox"/> Valid	 Create	<input type="text" value="password for create"/>
User 2	<input type="checkbox"/> Valid	 Create	<input type="text" value="password for create"/>
User 3	<input type="checkbox"/> Valid	 Create	<input type="text" value="password for create"/>
User 4	<input type="checkbox"/> Valid	 Create	<input type="text" value="password for create"/>
User 5	<input type="checkbox"/> Valid	 Create	<input type="text" value="password for create"/>
User 6	<input type="checkbox"/> Valid	 Create	<input type="text" value="password for create"/>
User 7	<input type="checkbox"/> Valid	 Create	<input type="text" value="password for create"/>
User 8	<input type="checkbox"/> Valid	 Create	<input type="text" value="password for create"/>

Back

Refresh






Apply

VPN > Open VPN > Server VPN Mode	
Item	Description
<b>Server</b>	
<b>VPN Network</b>	The network ID for Open VPN virtual network.
<b>VPN Netmask</b>	The netmask for Open VPN virtual network.
<b>Roadwarrior: Route Client Networks</b>	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.
<b>Local Network</b>	
<b>Network</b>	The local network exported by OpenVPN. When keeping this option blank, the OpenVPN will export the LAN network automatically.
<b>Netmask</b>	The local netmask exported by OpenVPN. When keeping this option blank, the OpenVPN will export the LAN netmask automatically.
<b>NAT</b>	
<b>1:1 NAT</b>	<ul style="list-style-type: none"> <li>• Tick to enable NAT Traversal for Open VPN. This item must be enabled when router under NAT environment.</li> <li>• Select from Off or On. The default is Off.</li> <li>• When two routers' LAN Subnet are same and create Open VPN tunnels, this function is turned on.</li> </ul>
<b>Server- Server Security</b>	
<b>Root CA</b>	Create Root CA key.
<b>Cert, Key and DH</b>	Create Cert, Key and DH key.
<b>Server- User Security</b>	
<b>User 1 - User 8</b>	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

Import \*.ovpn

Username

Password

Status

Idle

Back

Refresh

Apply

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.

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

Mode   ☒ Disable   ☐ Enable

Type   ☒ Policy-based   ☐ Route-based

### 11.2.1 IPsec > Connections

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

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

IPSec

Mode

☒ Disable
 ☐ Enable

Connections

Authentication IDs

X.509 Certificates

CA Certificates

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

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

#	Name	State	IKE information	Tunnel information
1			Phase 1	Phase 2

+ Add Connection

Apply

## (1) IPsec Phase 1 Setting

Connection #1 Phase 1

Mode

☒ Disable
 ☐ Enable

Name

Protocol

IKEv1

Aggressive mode

Disable

Auth Type

PSK

Encryption

AES128

Hash

SHA1

DH Group

5 (1536 bit)

Lifetime

3 hours

Local Host

Local ID

<empty> (allow any)

Remote Host

Remote ID

<empty> (allow any)

Back

Save

VPN > IPsec > Connections > Phrase 1 setting	
Item	Description
<b>Mode</b>	Select from Disable or Enable. The default is Disable.
<b>Name</b>	Short name or description.
<b>Protocol</b>	Select from IKEv1 or IKEv2. The default is IKEv1.
<b>Aggressive mode</b>	Select from Disable or Enable. The default is Disable. When this option be enabled, the connection will be running on IKEv1 Aggressive mode. ( <b>Note:</b> This option only work on IKEv1.)
<b>Auth Type</b>	Select from PSK (default), RSA, EAP-TLS. ( <b>Note:</b> The EAP-TLS is for IKEv2 only.)
<b>Encryption</b>	The encryption algorithm. Select from AES128 (default), AES192, AES256 or 3DES.
<b>Hash</b>	The integrity algorithm. Select from MD5, SHA1 (default) or SHA256.
<b>DH Group</b>	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).
<b>Lifetime</b>	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.

<b>Local Host</b>	The IP address of the router's public network interface. If this value is blank, the connection will automatically detect the correct IP address.
<b>Local ID</b>	The identification for authentication on local peer. Select from the created authentication IDs or empty.
<b>Remote Host</b>	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.
<b>Remote ID</b>	The identification for authentication on remote peer. Select from the created authentication IDs or empty.

## (2) IPsec Phase 2 Setting

Connection #1 Phase 2

Protocol

ESP

Encryption

AES128

Hash

SHA1

DH Group

5 (1536 bit)

Lifetime

3 hours

Local Subnet

Remote Subnet

Service

Any

Back

Save

VPN > IPsec > Connections > Phrase 2 setting	
Item	Description
<b>Protocol</b>	Only support ESP.
<b>Encryption</b>	The encryption algorithm. Select from AES128 (default), AES192, AES256 or 3DES.
<b>Hash</b>	The integrity algorithm. Select from MD5, SHA1 (default) or SHA256.
<b>DH Group</b>	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).
<b>Lifetime</b>	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.
<b>Local Subnet</b>	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.

	<b>Note:</b> This option only work on Policy-based IPsec VPN type.
<b>Remote Subnet</b>	<p>The private subnet behind the peer gateway.</p> <p>The available formats are A.B.C.D, A.B.C.D/M, A.B::C.D or A.B::C.D/M</p> <p>If this value is blank, the connection will set it as the “Remote Host” of Phase 1 setting.</p> <p><b>Note:</b> This option only work on Policy-based IPsec VPN type.</p>
<b>Service</b>	<p>Restrict the VPN traffic to the particular protocol only.</p> <p>Select from the Any, TCP, UDP or L2TP.</p>

### (3) IPsec Advance Setting

Connection #1 Advance

DPD interval (s)

DPD retry

Back

Save

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



## 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.

IPSec

Mode ☒ Disable ☐ Enable

Connections Authentication IDs X.509 Certificates CA Certificates

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

+ Add Authentication ID

Apply

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"><li>● PSK: Use the pre-shared key to authenticate the connection.</li><li>● RSA: Use the certificate to authenticate the connection.</li></ul>
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 <b>remote.IPsec</b> ID. Normally, this case will be used to authenticate peer gateway.
3	local.ipsec	PSK		The identification for the connection. Normally, this case will be used to announce the ID of the router.

4	test	RSA	<b>created X.509</b>	The ID field will be omitted, and use the common name(CN) of X.509 as the ID field.
---	------	-----	----------------------	---

### 11.2.3 IPsec > X.509 Certificates

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

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

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

IPSec

Mode

☒ Disable
 ☐ Enable

Connections

Authentication IDs

X.509 Certificates

CA Certificates

- : Generated
- : Imported
- : Cert or Key is missed
- : Generating
- : Waiting Apply

- : Get Information
- : Download File
- : Import File

<input type="checkbox"/>	#	State	Subject	Cert	Key	Edit
<input type="checkbox"/>	1		C=CN, O=Company, CN=local.ipsec			
<input type="checkbox"/>	2		C=CN, O=Company, CN=remote.ipsec			

+ Add X.509

Apply

## 11.2.4 IPsec > CA Certificates

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

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

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

IPSec

Mode ☒ Disable ☐ Enable

Connections Authentication IDs X.509 Certificates CA Certificates

- : Generated
- : Imported
- : Generating
- : Waiting Apply

- : Get Information
- : Download File

#	State	Subject	Cert	Edit
Self-signed CA		C=CN, O=Company, CN=ipsec.ca		

+ Add CA certificate

Apply

### Certificate Generation

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

To generate the self-signed CA certificate:

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

To generate the X.509 certificate:

1. Make sure the self-signed CA certificate generated.
2. Navigate to [X.509 Certificates](#) tab.

3. Add the new X.509 certificate by [+ Add X.509](#) button. (If it's not existed.)
4. Click the Edit button to navigate the **Certificate Setting** page.
5. Fill up the information of the X.509 certificate.
6. Click the [Generate Certificate](#) button and [Save](#).
7. Click the [Apply](#) button to apply the changes.

### Certificate Setting

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

Self-signed CA Certificate

Country Name (C)

State (ST)


Location, e.g. city (L)

Organization Name (O)

Organization Unit Name (OU)

Common Name (CN)

E-mail

 Generate Certificate

Back
Save

### Certificate Importing

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

To import the CA certificate:

1. Navigate to [CA Certificates](#) tab.
2. Click the [+ Add CA certificate](#) button.
3. Select the CA certificate file from browser window.

4. When the file be selected and everything all right, the newly CA certificate will show the CA certificate list with **Imported** state.

To import the X.509 certificate:

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

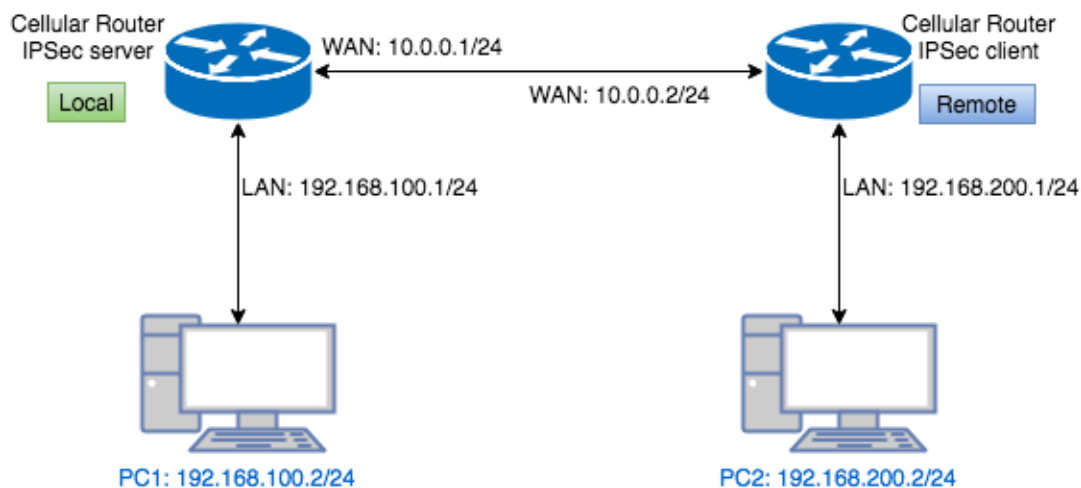
### Download the certificate

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

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

## 11.2.5 IPsec > Net-to-Net Configuration

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



### ● Pre-shared Key authentication

#### Configure Net-to-Net VPN Server

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

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

The screenshot displays the IPsec configuration interface. At the top, there's a blue header with the IPsec icon and label. Below it, the 'Mode' is set to 'Enable' (radio button selected) and 'Type' is set to 'Policy-based' (radio button selected). A tabbed interface shows 'Connections' as the active tab, with other tabs being 'Authentication IDs', 'X.509 Certificates', and 'CA Certificates'. Below the tabs, there's a table with columns: '#', 'ID', 'Type', and 'Pre-shared Key / X.509 Certificate'. The first row shows a checkbox, the number '1', an empty ID field, a dropdown menu set to 'PSK', and a masked pre-shared key field. Below the table is a button labeled '+ Add Authentication ID'. At the bottom right, there is an 'Apply' button.

#	ID	Type	Pre-shared Key / X.509 Certificate
<input type="checkbox"/>	1	PSK	.....

+ Add Authentication ID

Apply

### Connection #1 Phase 1

Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Name	<input type="text"/>
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="5 (1536 bit)"/>
Lifetime	<input type="text" value="3 hours"/>
Local Host	<input type="text"/>
Local ID	<input type="text" value="&lt;empty&gt; (allow any)"/>
Remote Host	<input type="text"/>
Remote ID	<input type="text" value="&lt;empty&gt; (allow any)"/>

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

### Connection #1 Phase 2

Protocol	<input type="text" value="ESP"/>
Encryption	<input type="text" value="AES128"/>
Hash	<input type="text" value="SHA1"/>
DH Group	<input type="text" value="5 (1536 bit)"/>
Lifetime	<input type="text" value="2 hours"/>
Local Subnet	<input type="text" value="192.168.100.0/24"/>
Remote Subnet	<input type="text" value="192.168.200.0/24"/>
Service	<input type="text" value="Any"/>

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

## Configure Net-to-Net VPN Client

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

The screenshot shows the IPsec configuration interface. At the top, there's a blue header with the IPsec icon and label. Below it, the 'Mode' is set to 'Enable' (radio button selected) and 'Type' is set to 'Policy-based' (radio button selected). There are four tabs: 'Connections', 'Authentication IDs' (active), 'X.509 Certificates', and 'CA Certificates'. Below the tabs is a table with columns: '#', 'ID', 'Type', and 'Pre-shared Key / X.509 Certificate'. There is one row with '# 1', an empty 'ID' field, 'PSK' in the 'Type' dropdown, and a masked 'Pre-shared Key' field. Below the table is a button labeled '+ Add Authentication ID'. At the bottom right is an 'Apply' button.

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

+ Add Authentication ID

Apply



### Connection #1 Phase 1

Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Name	<input type="text"/>
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="5 (1536 bit)"/>
Lifetime	<input type="text" value="3 hours"/>
Local Host	<input type="text"/>
Local ID	<input type="text" value="&lt;empty&gt; (allow any)"/>
Remote Host	<input type="text" value="10.0.0.1"/>
Remote ID	<input type="text" value="&lt;empty&gt; (allow any)"/>

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

### Connection #1 Phase 2

Protocol	<input type="text" value="ESP"/>
Encryption	<input type="text" value="AES128"/>
Hash	<input type="text" value="SHA1"/>
DH Group	<input type="text" value="5 (1536 bit)"/>
Lifetime	<input type="text" value="2 hours"/>
Local Subnet	<input type="text" value="192.168.200.0/24"/>
Remote Subnet	<input type="text" value="192.168.100.0/24"/>
Service	<input type="text" value="Any"/>

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

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

- Server

Connections

Authentication IDs

X.509 Certificates

CA Certificates

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

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

<input type="checkbox"/>	#	Name	State	IKE information	Tunnel information
<input type="checkbox"/>	1	psk		IKEv1 : 10.0.0.1 [10.0.0.1] ... 10.0.0.2 [10.0.0.2]	<b>Phase 1</b> 192.168.100.0/24 ... 192.168.200.0/24 <b>Phase 2</b>

+ Add Connection

- Client

Connections

Authentication IDs

X.509 Certificates

CA Certificates

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

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

<input type="checkbox"/>	#	Name	State	IKE information	Tunnel information
<input type="checkbox"/>	1	psk		IKEv1 : 10.0.0.2 [10.0.0.2] ... 10.0.0.1 [10.0.0.1]	<b>Phase 1</b> 192.168.200.0/24 ... 192.168.100.0/24 <b>Phase 2</b>

+ Add Connection

- **RSA authentication - Server**

### Prepare the self-signed CA certificate

1. Navigate to the [CA Certificates](#) tab.
2. Edit the self-signed CA. (Skip it if the self-signed CA is generated.)
  - (1) Fill the information of the self-signed CA
  - (2) **Country Name**: CN
  - (3) **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

Self-signed CA Certificate

Country Name (C)

State (ST)


Location, e.g. city (L)

Organization Name (O)

Organization Unit Name (OU)

Common Name (CN)

E-mail

 Generate Certificate

Back

Save

### 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

X.509 Certificate #1

Country Name (C)

State (ST)

Location, e.g. city (L)

Organization Name (O)

Organization Unit Name (OU)

Common Name (CN)

E-mail

Generate Certificate

Back

Save

X.509 Certificate #2

Country Name (C)

State (ST)

Location, e.g. city (L)

Organization Name (O)

Organization Unit Name (OU)

Common Name (CN)

E-mail

Generate Certificate

Back

Save

IPSec

Mode
☐ Disable
☒ Enable

Type
☒ Policy-based
☐ Route-based

Connections
Authentication IDs
X.509 Certificates
CA Certificates

- : Generated
- : Imported
- : Cert or Key is missed
- : Generating
- : Waiting Apply

- : Get Information
- : Download File
- : Import File

<input type="checkbox"/>	#	State	Subject	Cert	Key	Edit
<input type="checkbox"/>	1		C=CN, O=Company, CN=local.ipsec			
<input type="checkbox"/>	2		C=CN, O=Company, CN=remote.ipsec			

+ Add X.509

Apply

IPSec

Mode
☐ Disable
☒ Enable

Type
☒ Policy-based
☐ Route-based

Connections
Authentication IDs
X.509 Certificates
CA Certificates

- : Generated
- : Imported
- : Cert or Key is missed
- : Generating
- : Waiting Apply

- : Get Information
- : Download File
- : Import File

<input type="checkbox"/>	#	State	Subject	Cert	Key	Edit
<input type="checkbox"/>	1		C=CN, O=Company, CN=local.ipsec			
<input type="checkbox"/>	2		C=CN, O=Company, CN=remote.ipsec			

+ Add X.509

Apply

## Prepare the authentication IDs

1. Navigate to the [Authentication IDs](#) tab.
2. Add 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

The screenshot shows the IPsec configuration interface. At the top, there's a header 'IPSec'. Below it, there are two radio buttons for 'Mode': 'Disable' and 'Enable' (selected). There are also two radio buttons for 'Type': 'Policy-based' (selected) and 'Route-based'. Below these are four tabs: 'Connections', 'Authentication IDs' (selected), 'X.509 Certificates', and 'CA Certificates'. The 'Authentication IDs' tab contains a table with two rows. Each row has a checkbox, a '#' column, an 'ID' column, a 'Type' column, and a 'Pre-shared Key / X.509 Certificate' column. Row 1 has ID 1, Type RSA, and Certificate C=CN, O=Company, CN=local.ipsec. Row 2 has ID 2, Type RSA, and Certificate C=CN, O=Company, CN=remote.ipsec. Below the table is a button '+ Add Authentication ID'. At the bottom right is an 'Apply' button.

	#	ID	Type	Pre-shared Key / X.509 Certificate
<input type="checkbox"/>	1		RSA	C=CN, O=Company, CN=local.ipsec
<input type="checkbox"/>	2		RSA	C=CN, O=Company, CN=remote.ipsec

[+ Add Authentication ID](#)

[Apply](#)

## Setup the connection on VPN server

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

#### 4. Apply the changes

**Connection #1 Phase 1**

Mode

☐ Disable ☒ Enable

Name

Protocol

IKEv1

Aggressive mode

Disable

Auth Type

RSA

Encryption

AES128

Hash

SHA1

DH Group

5 (1536 bit)

Lifetime

3 hours

Local Host

Local ID

ID#1: local.ipsec (RSA)

Remote Host

Remote ID

<empty> (allow any)

Back

Save

**Connection #1 Phase 2**

Protocol

ESP

Encryption

AES128

Hash

SHA1

DH Group

5 (1536 bit)

Lifetime

3 hours

Local Subnet

192.168.100.0/24

Remote Subnet

192.168.200.0/24

Service

Any

Back

Save

## ● RSA authentication – Client

### Prerequisite for VPN Client with RSA authentication

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

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

### Import the CA certificate and the X.509 certificate

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

IPSec

Mode

☒ Disable ☐ Enable

Type

☒ Policy-based ☐ Route-based

Connections

Authentication IDs

X.509 Certificates

CA Certificates

• : Generated

• : Imported

• : Generating

• : Waiting Apply

• : Get Information

• : Download File

#	State	Subject	Cert	Edit
		Self-signed CA		

+ Add CA certificate

Apply

IPSec

Mode

☒ Disable ☐ Enable

Type

☒ Policy-based ☐ Route-based

Connections

Authentication IDs

X.509 Certificates

CA Certificates

• : Generated

• : Imported

• : Cert or Key is missed

• : Generating

• : Waiting Apply

• : Get Information

• : Download File

• : Import File

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

+ Add X.509

Apply

4G LTE COMPACT INDUSTRIAL CELLULAR ROUTER\_RT-MOB-020 - UM V1.1.8

100



## 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

The screenshot displays the IPsec configuration interface. At the top, there's a header bar with the IPsec icon and label. Below it, the 'Mode' is set to 'Enable' (radio button selected) and 'Type' is set to 'Policy-based' (radio button selected). The 'Connections' tab is active, showing a table of authentication IDs. The table has columns for '#', 'ID', 'Type', and 'Pre-shared Key / X.509 Certificate'. There is one entry with ID '1', Type 'RSA', and Pre-shared Key 'C=CN, O=Company, CN=remote.ipsec'. Below the table is a button to '+ Add Authentication ID'. At the bottom right, there is an 'Apply' button.

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

+ Add Authentication ID

Apply

### Connection #1 Phase 1

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

Back

Save

### Connection #1 Phase 2

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

Back

Save

## ● IPsec Net-to-Net with RSA authentication result

### • Server

Connections
Authentication IDs
X.509 Certificates
CA Certificates

- ✓ : IPsec SA active and link up
- ! : Only IPsec SA active
- ⋮ : Connecting
- ✖ : IPsec SA inactive
- ⦿ : Disabled

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

<input type="checkbox"/>	#	Name	State	IKE information	Tunnel information
<input type="checkbox"/>	1	rsa	✓	IKEv1 : 10.0.0.1 [local.ipsec] ... 10.0.0.2 [remote.ipsec]	Phase 1 192.168.100.0/24 ... 192.168.200.0/24  Phase 2

+ Add Connection

### • Client

Connections
Authentication IDs
X.509 Certificates
CA Certificates

- ✓ : IPsec SA active and link up
- ! : Only IPsec SA active
- ⋮ : Connecting
- ✖ : IPsec SA inactive
- ⦿ : Disabled

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

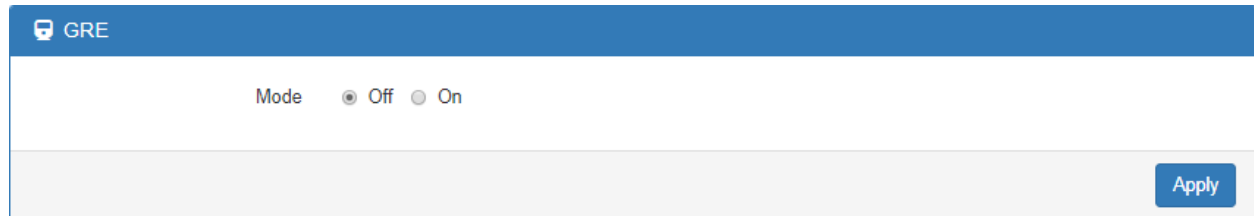
<input type="checkbox"/>	#	Name	State	IKE information	Tunnel information
<input type="checkbox"/>	1	rsa	✓	IKEv1 : 10.0.0.2 [remote.ipsec] ... 10.0.0.1 [local.ipsec]	Phase 1 192.168.200.0/24 ... 192.168.100.0/24  Phase 2

+ Add Connection

## 11.3 VPN > GRE

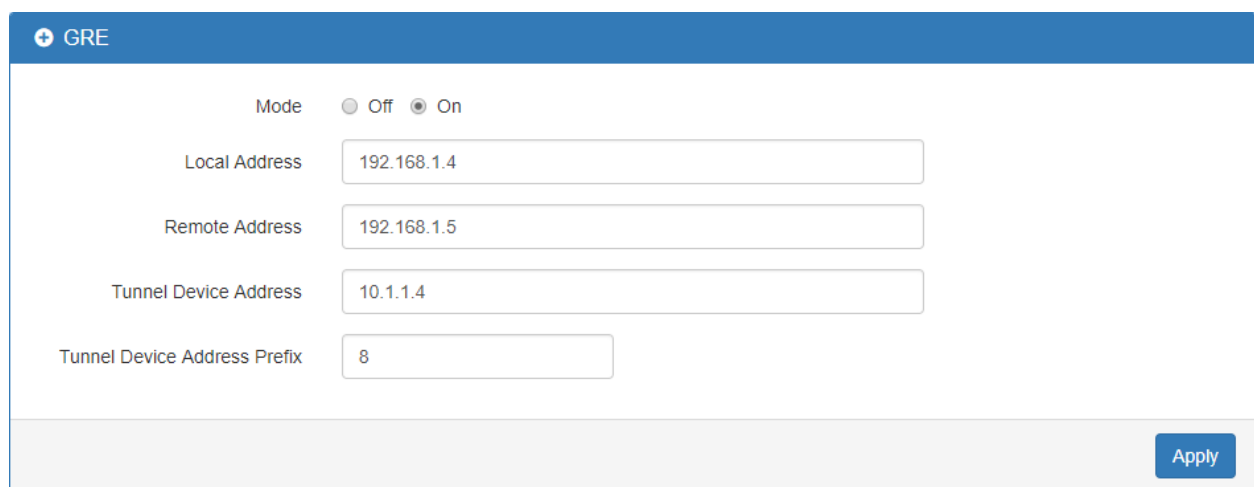
This section allows you to set **GRE configuration**. The default mode is off.

**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 a radio button. There is an 'Apply' button in the bottom right corner.

The GRE Mode is on.




The screenshot shows the GRE configuration interface with 'Mode' set to 'On'. The 'Local Address' is 192.168.1.4, 'Remote Address' is 192.168.1.5, 'Tunnel Device Address' is 10.1.1.4, and 'Tunnel Device Address Prefix' is 8. There is an 'Apply' button in the bottom right corner.

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

 PPTP Server

General

Clients

Mode

☒ Off ☐ On

Server Address

192.168.10.1

Client Address Range

192.168.10.2

-

10

Apply

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

### (2) Clients Configuration

There are two parts for Clients configuration.

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

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

PPTP Server

General

Clients

#	Mode	Username	Password	Edit	Summary Delete
1	on	client	client		

Add PPTPD Client

Mode

☐ Off ☒ On

Username

Password

Add

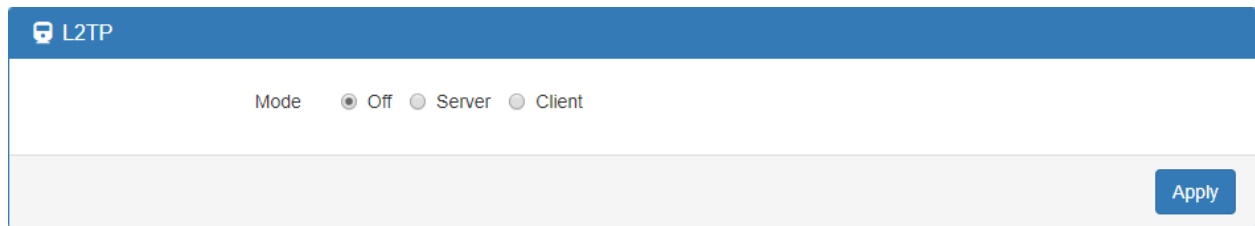
Add/Edit

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.



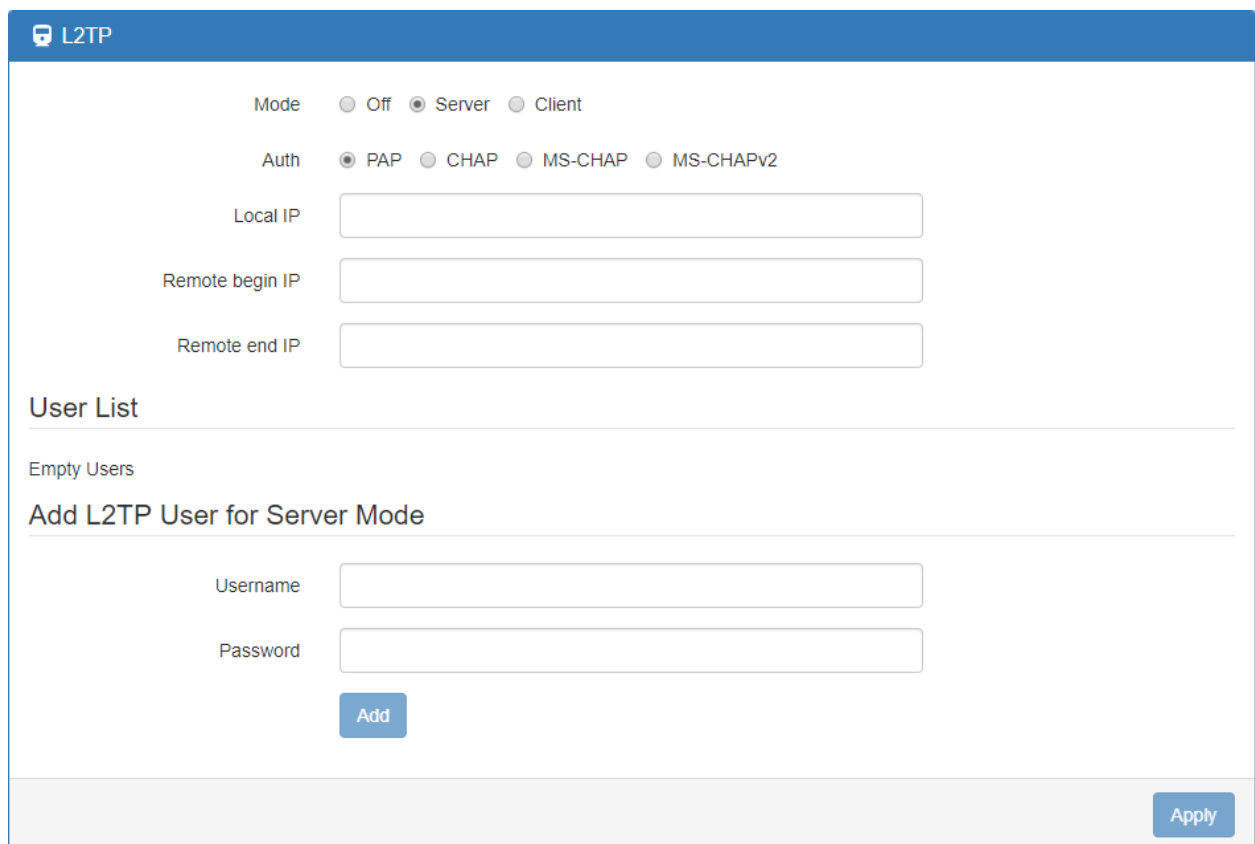
L2TP

Mode ☒ Off ☐ Server ☐ Client

Apply

**(2) Server Mode:**

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



L2TP

Mode ☐ Off ☒ Server ☐ Client

Auth ☒ PAP ☐ CHAP ☐ MS-CHAP ☐ MS-CHAPv2

Local IP

Remote begin IP

Remote end IP

User List

Empty Users

Add L2TP User for Server Mode

Username

Password


Add


Apply

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.

 L2TP

Mode ☐ Off ☒ Server ☐ Client



Auth ☒ PAP ☐ CHAP ☐ MS-CHAP ☐ MS-CHAPv2

Local IP

Remote begin IP

Remote end IP


User List


#	Username	Edit	Delete
1	test		

Add L2TP User for Server Mode

Username

Password







### (3) Client Mode:

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

L2TP

Mode ☐ Off ☐ Server ☒ Client

Connection List

Empty Connections

Add L2TP Connection for Client Mode

Mode ☐ Off ☒ On

Server

Auth ☒ PAP ☐ CHAP ☐ MS-CHAP ☐ MS-CHAPv2

Username

Password

NAT ☐ Off ☒ On

Default Route ☐ Off ☒ On

Add

Apply

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

Fill in the required parameters and click the 

Add



 button to create the L2TP connection and manage the L2TP connection under client mode.

L2TP

Mode

☐ Off
 ☐ Server
 ☒ Client

Connection List

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

Add L2TP Connection for Client Mode

Mode

☐ Off
 ☒ On

Server

Auth

☒ PAP
 ☐ CHAP
 ☐ MS-CHAP
 ☐ MS-CHAPv2

Username

Password

NAT


☐ Off
 ☒ On

Default Route

☐ Off
 ☒ On


Add

Apply

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


## 12 Configuration > Firewall

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

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

### 12.1 Firewall > Basic Rules

This section allows you to set the Basic Rules configuration.

Basic Rules 	
WAN Ping Blocking <input type="checkbox"/> IPv4 <input type="checkbox"/> IPv6	
<div>Apply</div>	















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

## 12.2 Firewall > Port Forwarding

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

Port Forwarding

Mode ☒ Disable ☐ Enable

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

Apply

Edit Port Forwarding Entry #1

Mode ☒ Disable ☐ Enable

Description

Protocol ☒ TCP ☐ UDP

Source Port Begin

Source Port End

Destination IP

Destination Port Begin

Destination Port End

Save

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

## 12.3 Firewall > DMZ

This section allows you to set the DMZ configuration.

DMZ

Mode

☒ Disable
 ☐ Enable


Host IP Address


0.0.0.0

Apply

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

## 12.4 Firewall > IP Filter

















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

 IP Filter

Mode ☒ Disable ☐ Enable

List ☒ Black ☐ White

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

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

Apply

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

IP Filter

Mode

☒ Disable
 ☐ Enable

List

☐ Black
 ☒ White

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

Management IP Address

0.0.0.0

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

Service Ports

U53,C00

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

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

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

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


### Management IP Address:

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

### Service Ports:

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

## Edit Black/White List

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

Edit IP Filter Black List Entry #1

Black List Setting

Mode

☒ Disable ☐ Enable

Protocol

☒ All ☐ ICMP ☐ TCP ☐ UDP

Source IP

Example:

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

Source Port

Example:

- 1234
- 1234:5678:

Destination IP

Destination Port

Save

Edit IP Filter White List Entry #1

White List Setting

Mode

☒ Disable ☐ Enable

Protocol

☒ All ☐ ICMP ☐ TCP ☐ UDP

Source IP

Example:

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

Source Port

Example:

- 1234
- 1234:5678:

Destination IP

Destination Port

Save



Firewall > IP Filter	
Item	Description
<b>Mode</b>	Select from Disable or Enable. The default is Disable.
<b>Protocol</b>	Select from All, ICMP, TCP or UDP.
<b>Source IP</b>	Fill in your source IP address.
<b>Source Port</b>	Fill in your source port.
<b>Destination IP</b>	Fill in your destination IP address.
<b>Destination Port</b>	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
<b>IPv4</b>	192.168.0.123	192.168.1.0/24 192.168.1.0/255.255.255.	192.168.1.1-192.168.1.123
<b>IPv6</b>	2607:f0d0:1002:51::4	2607:f0d0:1002:51::0/64	2607:f0d0:1002:51::4- 2607:f0d0:1002:51::aaaa
<b>Note:</b> Setting up a range of IP, please use – hyphen symbol to mark your ranged IP.			

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

















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

## 12.5 Firewall > MAC Filter

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

MAC Filter

Mode ☒ Disable ☐ Enable

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

Apply

Edit MAC Filter Black List Entry #1

Mode ☒ Disable ☐ Enable


MAC Address

Save

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

















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

## 12.6 Firewall > URL Filter

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

URL Filter

Mode ☒ Disable ☐ Enable

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

Apply

Edit URL Filter Black List Entry #1

Mode ☐ Disable ☒ Enable

Filter ☐ Key ☒ Full

Key/Full

Hint About the 'Full' filter:

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

Save

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


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

## 12.7 Firewall > NAT

This section allows you to set NAT configuration.

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

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

 NAT

Mode ☐ Disable ☒ Enable

Apply

## 12.8 Firewall > IPS

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

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

IPS(Intrusion Prevention System)

Mode ☒ Off ☐ On

Per IP Address

☐ Total allow incoming connection number

10

☐ Max incoming connection retry number

20

during

120


seconds

Apply

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

### 13.1 Service > SNMP

This section allows you to set the SNMP configuration.

#### 13.1.1 Community

 SNMP

Mode ☐ Disable ☒ Enable

Community SNMP v3 User Configuration SNMP trap configuration

#	Mode	Name	Access
1	<input type="text" value="Enable"/>	<input type="text" value="public"/>	<input type="text" value="Read-Only"/>
2	<input type="text" value="Enable"/>	<input type="text" value="private"/>	<input type="text" value="Read-Write"/>
3	<input type="text" value="Disable"/>	<input type="text"/>	<input type="text" value="Read-Only"/>

Apply

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

### 13.1.2 SNMP v3 User Configuration

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

+ SNMP

Mode
☐ Disable
☒ Enable

Community
SNMP v3 User Configuration
SNMP trap configuration

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

Authentication

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

Apply

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

<b>Authentication Protocol</b>	Select from MD5 or SHA.
<b>Privacy Password</b>	Fill in your privacy password.
<b>Privacy Protocol</b>	Select from DES or AES.
<b>Access</b>	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.

SNMP

Mode

☐ Disable
☒ Enable

Community

SNMP v3 User Configuration

SNMP trap configuration

#	Mode	Community Name	Destination
1	Disable	public	
2	Disable	private	

Apply

Alarm

Mode

☒ Disable
☐ Enable

Alarm input

☒ SMS
☒ DI
☒ VPN disconnect
☒ WAN disconnect

☒ LAN disconnect
☒ Reboot

Alarm output

☒ SMS
☒ DO
☒ **SNMP trap**
☒ E-mail

☒ TR069

DI 1 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

Service > SNMP > SNMP trap configuration	
Item	Description
<b>Mode</b>	Select from Disable or Enable. The default is Disable.
<b>Community Name</b>	Fill in your community name.
<b>Destination</b>	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.

+

 TR069

Mode

☒ Disable ☐ Enable

ACS URL

http://192.168.1.100:8080/acs

ACS Username

cpe

ACS Password

...

Periodic Inform

☒ Disable ☐ Enable

Periodic Inform Interval(Sec)

1800

Connection Request Username

tr069

Connection Request Password

.....

Connection Request Port

7547

Apply

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

## 13.3 Service > Dynamic DNS

This section allows you to set up Dynamic DNS.

Dynamic DNS

Mode

☒ Disable ☐ Enable

Service Provider

dynv6.com

Host Name

Token ID

Update Period Time (Sec)

2592000

IP Address Selection

☒ Internet IP ☐ WAN IP

Apply

Dynamic DNS

Mode

☒ Disable ☐ Enable

Service Provider

dynv6.com

Host Name

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

Token ID

Update Period Time (Sec)

2592000

IP Address Selection

☒ Internet IP ☐ WAN IP

Apply

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.

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

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

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

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

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

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

## 13.4 Service > VRRP

This section allows you to configure VRRP.

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"><li>Each router in the same VRRP group must have the same virtual IP address. The default is 0.0.0.0.</li><li>This virtual IP address must belong to the same address range as the real IP address of the interface.</li></ul>

## 13.5 Service > MQTT

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

MQTT

Mode

☒ Disable
 ☐ Enable

Port

1883

Manage Users

Username

Password

Delete

Username

Password

Add

ACLs

User

Topic

Subscribe

Publish

Delete

User

Topic

☐ Subscribe
   
☐ Publish

Add

Apply

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

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.

Mode ☒ Disable ☐ Enable

Port 1883

## Manage Users

Username	Password	Delete
Sub1	....	
Sub2	....	
Sub3	....	
Pub1	....	
Pub2	....	

Username Password 

## ACLs

User	Topic	Subscribe	Publish	Delete
Sub1	Critical	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Sub2	Critical	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Pub1	Critical	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

User Topic ☐ Subscribe☐ Publish

## 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.

UPnP

Mode ☐ Disable ☒ Enable

Apply

### 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.

SMTP

Mode ☒ Disable ☐ Enable

Server

Port 

58725465587

Username

Password

Apply

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"><li>● <b>Port 25</b> : Use TCP port 25 without encryption.</li><li>● <b>Port 465</b> : SMTP connections secured by SSL.</li><li>● <b>Port 587</b> : SMTP connections secured by TLS.</li></ul>
Username / Password	Fill in your username and password as the same your server.

## 13.8 Service > IP Alias

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

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

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



IP Alias

Mode

Off

On

Entries

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

Add IP Alias Entry

Mode

Off

On

Interface

eth1(WAN Ethernet) ▼

Addr

xxx.xxx.xxx.xxx

Mask

255.255.255.0

Add


Apply

Service > IP Alias	
Item	Description
<b>Mode</b>	Select from Off or On to enable the IP Alias.
<b>Entries</b>	The setting can be edited or deleted the existed entries.
<b>Add / Edit IP Alias Entry</b>	<ul style="list-style-type: none"> <li>● <b>Mode:</b> select from Off or On to use or not use this entry.</li> <li>● <b>Interface:</b> the interface you want to provide the additional address.</li> <li>● <b>Addr:</b> the IP address.</li> <li>● <b>Mask:</b> the network mask.</li> </ul>




## 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
Firmware
Configuration
Load Factory
Restart

### 14.1 Management > Identification

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

 Identification		
Attr.	Value	
Active Image Partition	a	
Model Name	M330-W	
LAN Ethernet MAC Address	00:03:79:06:2F:BD	
WAN Ethernet MAC Address	00:03:79:06:2F:BE	
Software Version	3.3.8	
Firmware Version	V0.02	
Hardware Version		
Software MCSV	014B00000022E82C	
Hardware MCSV	014B000000000000	
Serial Number	BL9U43VZ0005	
Modem Firmware Version	EC25EFAR06A03M4G	
IMEI	866758043832480	
Uptime	6:42:38	

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

## 14.2 Management > Administration

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

Administration

System Setup

Model Name

M330-W

Session TTL

0

(minutes, 0 means no timeout)

Admin Password

New Password

Retype to confirm

Apply

## 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

**Contacts / On Duty**

Contacts | Duty Schedule

All Users

Office 1

+ Add Group

<input type="checkbox"/>	Name	Phone	E-mail	
<input type="checkbox"/>	Test	+886912345678	test@test.com	

+ Add User

Please do NOT add device phone number into contacts

Apply

**+ Add Group:** Please fill out group name.

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

### 14.3.2 Duty Schedule

**Contacts / On Duty**

Contacts | Duty Schedule

Group	SUN	MON	TUE	WED	THU	FRI	SAT
Office 1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>


+ Add Group

Apply

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


LAN Server Port

WAN Server Port

Access Control

☒ Allow All ☐ Allow specified IPv4v6 Address below

Apply

 SSH

Mode

☐ Disable ☒ Enable

LAN Server Port

WAN 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.
LAN Server Port	The LAN side TCP port number listened by SSH server.
WAN Server Port	The WAN side TCP port number listened by SSH server.
Access Control	<ul style="list-style-type: none"> <li>● <b>Allow All:</b> Any client who own the IPv4v6 Address can reach system is able to connect system.</li> <li>● <b>Allow specified IPv4v6 Address below:</b> Only those configured IPv4v6 Address client are allowed to connect system.</li> </ul>

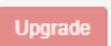
## 14.5 Management > Firmware

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.

 Firmware





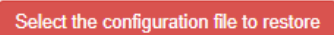


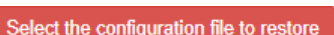
## 14.6 Management > Configuration

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

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


 Configuration

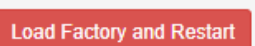
- (2) Click  button to import the configuration file.

## 14.7 Management > Load Factory

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


 Load Factory

Load the factory default configuration and restart the device immediately




## 14.8 Management > Restart

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


 **Restart**

Restart the device immediately



## 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**


Use Interface As Source ☒ No ☐ Yes

Use Interface 

APN2 ▼

 (LTE Net Mode: NA )


Host



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

## 15.2 Diagnosis > Traceroute

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

 Traceroute

Use Interface As Source ☒ No ☐ Yes

Use Interface 


APN2 ▼

 ( LTE Net Mode: NA )

Host

Traceroute

The result of the traceroute is as below.

 Traceroute

Use Interface As Source ☒ No ☐ Yes

Use Interface 

APN2 ▼

 ( LTE Net Mode: NA )

Host 

8.8.8.8

Traceroute

tracert to 8.8.8.8 (8.8.8.8), 30 hops max, 38 byte packets  
1tracert: sendto: Network is unreachable

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

## 16 Configuration Applications

This section explains specific examples how to configure your applications.

### 16.1 WAN Priority

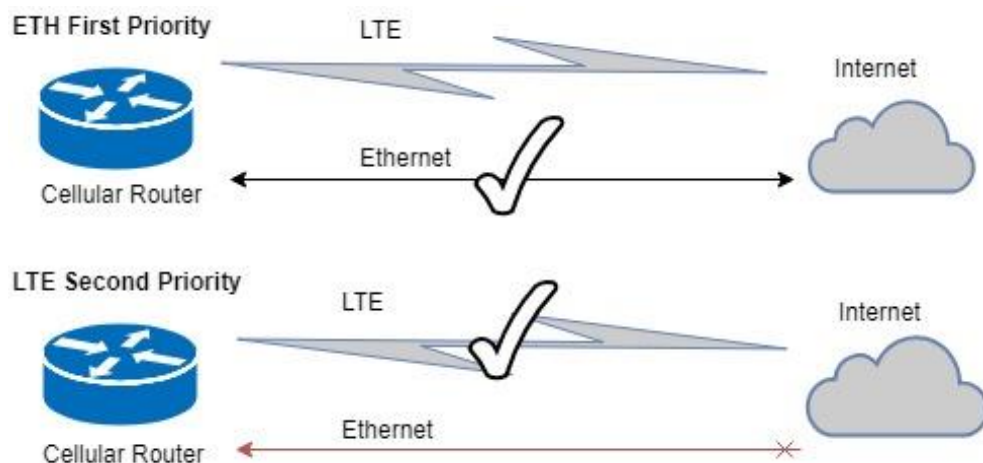
You can select from ETH First, LTE Only, ETH Only or LTE First.

Priority	
WAN Priority	<div>ETH First</div> <div>ETH First</div> <div>LTE Only</div> <div>ETH Only</div> <div>LTE First</div>

#### (1) WAN Priority > ETH First:

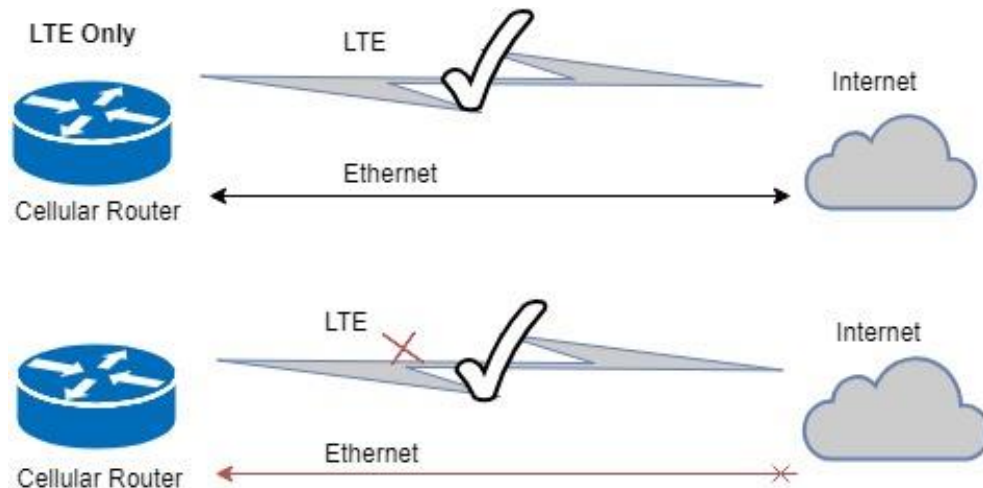
In case both Ethernet and LTE can access Internet, the router would route network packages through Ethernet. The reason is Ethernet that is low price and stable.

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:

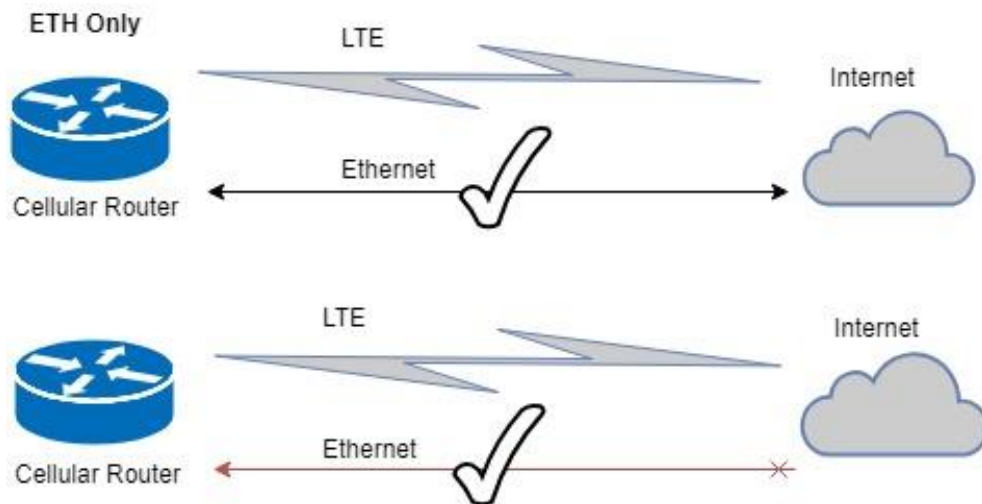
In this mode, the router only routes network packages through LTE.





### (3) WAN Priority > ETH Only:

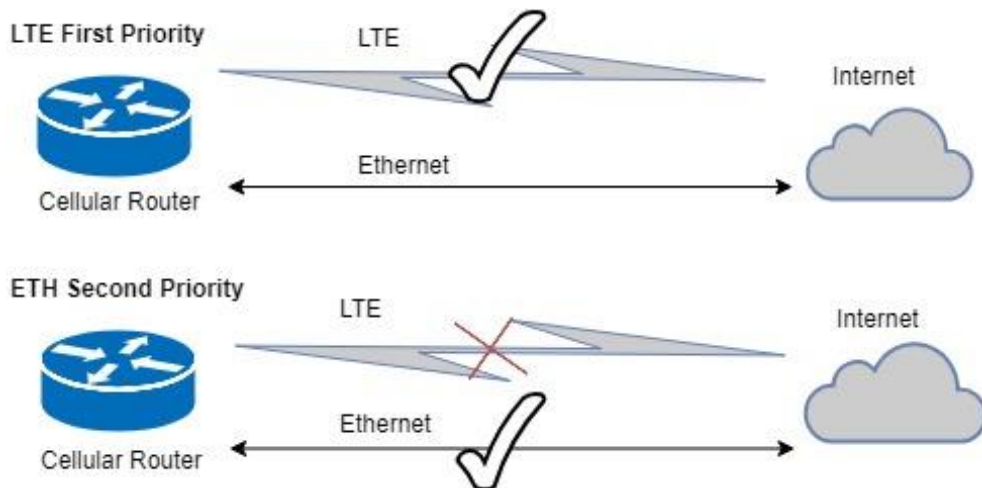
In this mode, the router only routes network packages through Ethernet.



### (4) WAN Priority > LTE First:

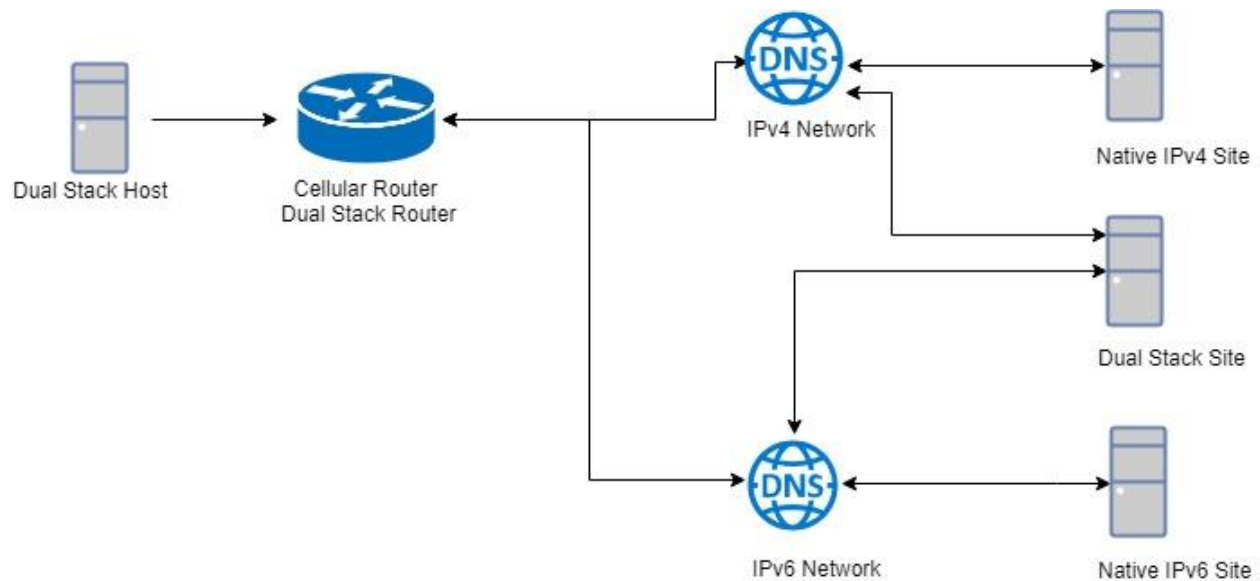
In case both Ethernet and LTE can access Internet, the router would route network packages through LTE.

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



## 16.2 LAN > IPv4/IPv6 Dual Stack

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



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

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

Ethernet WAN	
Attr.	Value
IPv4 Address	192.168.11.176
IPv4 Mask	255.255.255.0

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

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

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

Windows IP Configuration

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

Ethernet adapter Blue:

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

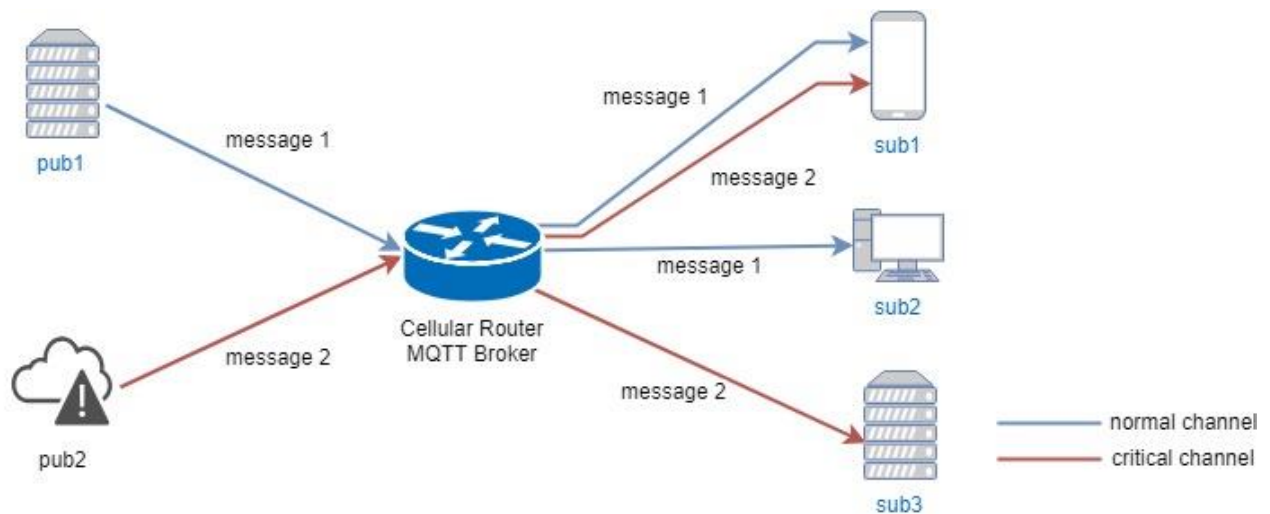
DNS Servers . . . . . : fe80::c2e:43ff:fe0d:4743%15
                             192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

C:\>
```

## 16.3 MQTT Broker

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

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



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

MQTT

Mode

☐ Disable ☒ Enable

Port

1883

Manage Users

Username	Password	Delete
Sub1	....	<input type="button" value="x"/>
Sub2	....	<input type="button" value="x"/>
Sub3	....	<input type="button" value="x"/>
Pub1	....	<input type="button" value="x"/>
Pub2	....	<input type="button" value="x"/>

Username

Password

Add

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

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

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

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

ACLs

User	Topic	Subscribe	Publish	Delete
Sub1	Critical	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Sub3	Critical	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Pub2	Critical	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

User

Topic

☐ Subscribe

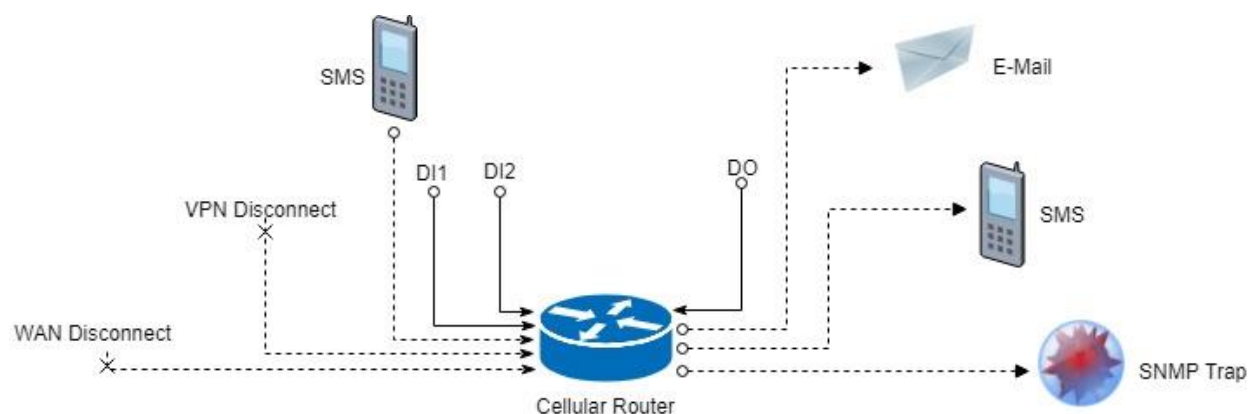
☐ Publish

Add

Apply

## 16.4 Alarm Configuration

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




### (1) Alarm Input:

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

## (2) Alarm Output:

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

 Alarm

Mode ☒ Disable ☐ Enable

Alarm input ☒ SMS ☒ DI ☒ VPN disconnect ☒ WAN disconnect  
☒ LAN disconnect ☒ Reboot

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

DI 1 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

 SNMP

Mode ☐ Disable ☒ Enable

Community SNMP v3 User Configuration SNMP trap configuration

#	Mode	Community Name	Destination
1	Disable	public	
2	Disable	private	

Apply

## 16.5 Open VPN Configuration

### Generic setup



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

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

















### 16.5.1 Open VPN Server Mode

#### Open VPN server certificate generation

##### Server - Server Security

Root CA	 Create
Cert, Key	 Create

##### Server - User Security

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

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

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

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

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

## Server - Server Security

Root CA	<a href="#">🔍 Create</a>	<a href="#">i</a>	<a href="#">📄</a>		
Cert, Key	<a href="#">🔍 Create</a>	<a href="#">i Cert</a>	<a href="#">📄</a>	<a href="#">i Key</a>	<a href="#">📄</a>

## Server - User Security

User 1	<input checked="" type="checkbox"/> Valid	<a href="#">🔍 Create</a>	<input type="text" value="password for create"/>	<a href="#">🔍 Cert</a>	<a href="#">📄</a>	<a href="#">i Key</a>	<a href="#">📄</a>	<a href="#">i P12</a>	<a href="#">📄</a>
User 2	<input type="checkbox"/> Valid	<a href="#">🔍 Create</a>	<input type="text" value="password for create"/>						
User 3	<input type="checkbox"/> Valid	<a href="#">🔍 Create</a>	<input type="text" value="password for create"/>						
User 4	<input type="checkbox"/> Valid	<a href="#">🔍 Create</a>	<input type="text" value="password for create"/>						
User 5	<input type="checkbox"/> Valid	<a href="#">🔍 Create</a>	<input type="text" value="password for create"/>						
User 6	<input type="checkbox"/> Valid	<a href="#">🔍 Create</a>	<input type="text" value="password for create"/>						
User 7	<input type="checkbox"/> Valid	<a href="#">🔍 Create</a>	<input type="text" value="password for create"/>						
User 8	<input type="checkbox"/> Valid	<a href="#">🔍 Create</a>	<input type="text" value="password for create"/>						

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

### 16.5.2 Open VPN Client Mode

#### Open VPN client certificate import

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

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

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

Client - Security	
Root CA	<a href="#">🔍 Import</a>
Cert	<a href="#">🔍 Import</a>
Key	<a href="#">🔍 Import</a>
P12	<a href="#">🔍 Import</a>

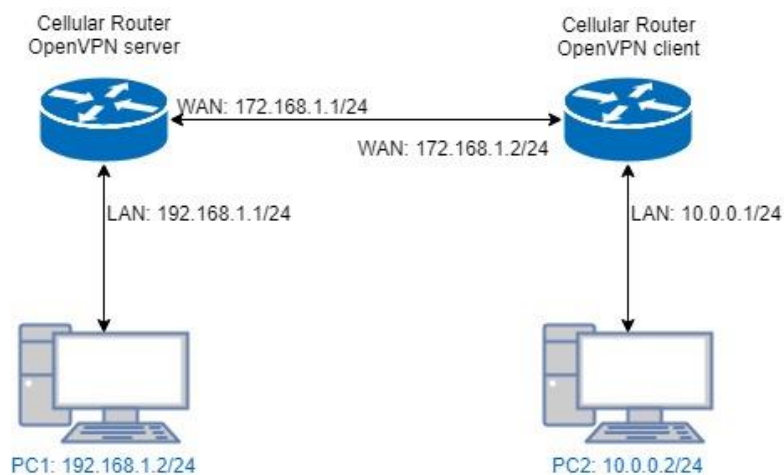
Client - Security			
Root CA	<a href="#">🔍 Import</a>	<a href="#">i</a>	<a href="#">📄</a>
Cert	<a href="#">🔍 Import</a>	<a href="#">i</a>	<a href="#">📄</a>
Key	<a href="#">🔍 Import</a>	<a href="#">i</a>	<a href="#">📄</a>
P12	<a href="#">🔍 Import</a>	<a href="#">i</a>	<a href="#">📄</a>

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



### 16.5.3 Open VPN Net-to-Net

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



#### (1) Open VPN server configuration

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

Edit Open VPN Connection #1

Mode ☐ Disable ☒ Enable

VPN Mode ☒ Server ☐ Client ☐ Custom

TLS Mode ☒ Disable ☐ Enable

TLS minimal version ☒ none ☐ 1.0 ☐ 1.1 ☐ 1.2

Cipher BF-CBC

Status Running

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

Device ☒ TUN ☐ TAP

Protocol ☒ UDP ☐ TCP

Port 1701

VPN Compression ☒ Disable ☐ Enable

Authentication Certificate

**Server**

Client Mode ☒ Roadwarrior

VPN Network 192.168.30.0

VPN Netmask 255.255.255.0

**Roadwarrior**

Route Client Networks ☐ Off ☒ On

Connections - Net / Mask

#1	10.0.0.0	/ 255.255.255.0
----	----------	-----------------

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

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

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

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

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

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

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

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

192.168.1.1/cgi-bin/openvpn.cgi?act=info&file=cert&type=user&conn\_id=0&user\_id...

Certificate:

```
Data:
  Version: 1 (0x0)
  Serial Number: 1 (0x1)
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C=CH, O=strongSwan, CN=OpenVPN
  Validity
    Not Before: May  9 06:34:08 2017 GMT
    Not After : May  7 06:34:08 2027 GMT
  Subject: C=CH, O=strongSwan, CN=user-00-00@openvpn
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:ac:b1:ca:c7:74:18:70:ed:71:88:9e:c4:ba:d1:
      c4:09:52:b8:11:d7:17:00:e4:dd:e5:a7:f4:e1:f6:
      1c:10:b5:0c:d2:27:e7:f8:63:cb:e2:30:78:6c:ab:
      e3:eb:bd:08:a0:64:ed:1c:6d:97:8f:75:be:21:0d:
      47:1f:ca:66:6e:52:a8:c2:40:98:01:21:73:73:b5:
      62:c7:ab:a7:39:6b:94:7b:db:b4:a4:45:33:39:00:
      5b:92:f6:05:4c:18:e1:7d:1b:0b:35:ed:3b:da:0e:
      1c:f3:0e:db:04:e0:90:53:da:f5:87:91:d9:af:0f:
      3d:82:c3:12:ec:4a:e2:ed:77:d9:ca:89:2a:73:c9:
      e7:4f:a3:97:ff:97:f1:c4:f0:de:12:c0:ae:12:73:
      3f:63:30:dd:e8:87:97:59:34:e7:a7:1f:a0:53:c5:
      b1:f6:4d:10:2f:96:bd:f1:80:cc:62:5a:66:d8:30:
      29:c6:f3:fa:7a:69:4a:6a:67:0b:85:e7:8f:76:a4:
      fc:47:af:e5:1e:76:96:1c:f0:2b:64:d7:d0:02:50:
      63:43:ae:65:ad:88:73:b0:19:67:08:a4:60:6a:f1:
      03:93:62:f1:e3:0a:b3:70:82:dc:8b:85:a4:95:98:
      fb:f5:f8:81:2b:a5:55:8a:f7:1c:15:41:c2:f5:8b:
      ae:ed
    Exponent: 65537 (0x10001)
  Signature Algorithm: sha256WithRSAEncryption
  54:fd:09:0b:23:5b:d1:22:e3:17:1e:de:5c:48:1c:30:30:c7:
  01:d8:6d:46:f4:91:4c:84:16:35:ea:79:91:67:dc:91:63:88:
  6a:23:7b:fe:8c:e0:93:14:a1:1e:1d:32:c2:22:84:af:22:ff:
  a9:9d:2f:aa:b2:0c:8b:86:c3:bc:46:8e:9d:5c:f8:55:39:91:
  cc:03:17:40:e9:d5:bb:df:e9:34:aa:89:71:f7:ea:1c:78:78:
  99:38:ba:7b:ec:d7:de:1a:d0:a0:07:58:cc:8a:4a:cc:2e:54:
  b3:d9:46:03:8e:58:cb:ef:de:95:61:01:33:9f:40:4c:cb:1b:
  3e:3e:70:4a:07:62:8c:d4:f0:53:86:42:c7:13:30:a8:3a:76:
  d3:bf:9d:33:7b:50:c3:98:fd:f0:ed:2a:c3:00:b8:dc:e0:80:
  a9:4b:0c:e1:ad:fc:32:76:03:b8:2f:9f:2a:d1:bb:1b:e7:cb:
  62:d2:63:be:7c:21:ac:b5:91:14:55:96:fc:67:94:cc:1f:7b:
  82:12:e6:84:da:fe:12:3e:73:bf:62:bb:1a:14:57:45:ce:28:
  95:e1:1f:d9:86:cb:36:c6:4d:b8:04:af:f6:0e:f4:f4:31:ba:
  6d:ef:cc:75:bc:0e:db:19:c7:c2:2c:b3:62:60:c2:88:d9:a3:
  cf:d4:8b:25
-----BEGIN CERTIFICATE-----
MIIC5zCCAc8CAQEDQYJKoZIhvcNAQELBQAwNDELMAkGA1UEBhMCQ0gxARBgNV
BAoMCnN0cm9uZ1N3YW4xEDAOBgNVBAMMB09wZW5WUE4wHhcNMTcwNTA5MDYzNDA4
WWhcNMicwNTA3MDYzNDA4WjA/MOswCOYDVOOGEwJDSDETMBEGA1UECwwKc3Rvb25n
```

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

## (2) Open VPN client configuration

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

Edit Open VPN Connection #1

Mode
☐ Disable
☒ Enable

VPN Mode
☐ Server
☒ Client
☐ Custom

TLS Mode
☒ Disable
☐ Enable

TLS minimal version
☒ none
☐ 1.0
☐ 1.1
☐ 1.2

Cipher
BF-CBC

Status
Connected

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

Device
☒ TUN
☐ TAP

Protocol
☒ UDP
☐ TCP

Port
1701

VPN Compression
☒ Disable
☐ Enable

Authentication
pkcs #12 Certificate

Client

Client Mode
☒ Roadwarrior

Server Address
172.168.1.1

PKCS12 Password
1234567

Route Client Networks
☐ Off
☒ On

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

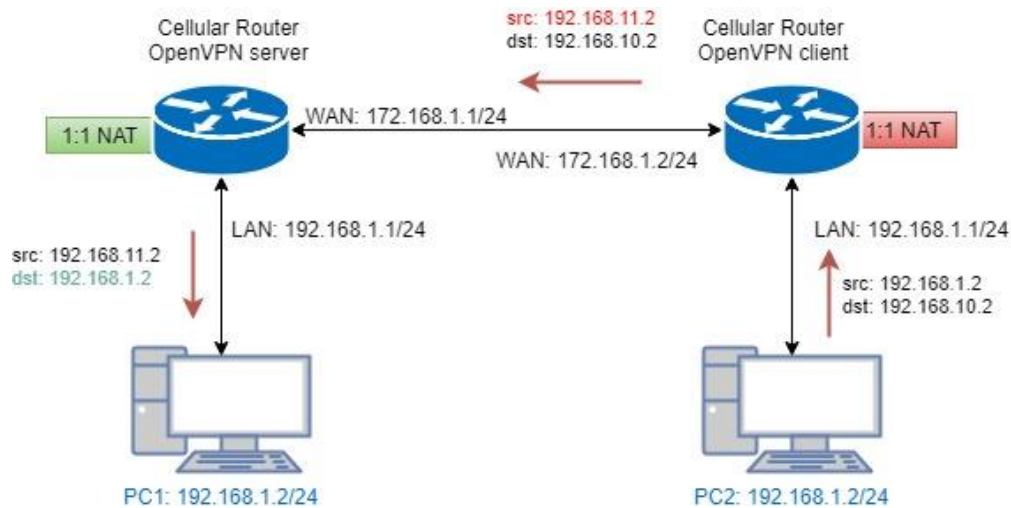
This option requires the P12 file which generated from Generic Setup Open VPN server part.

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

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

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

## 16.5.4 Open VPN 1:1 NAT



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

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

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

### Roadwarrior

Route Client Networks ☐ Off ☒ On

Connections - Net / Mask

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

### NAT

1:1 NAT ☐ Off ☒ On

Network 192.168.10.0

Netmask 255.255.255.0

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

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

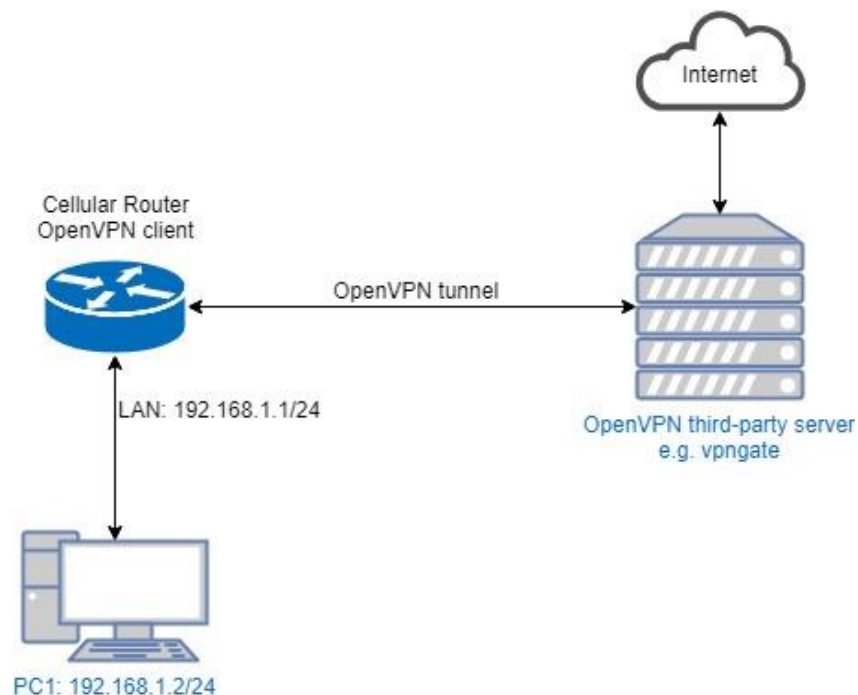
#### Client

Client Mode	<input checked="" type="radio"/> Roadwarrior
Server Address	<input type="text" value="172.168.1.1"/>
PKCS12 Password	<input type="text" value="proscend"/>
Route Client Networks	<input type="radio"/> Off <input checked="" type="radio"/> On

#### NAT

1:1 NAT	<input type="radio"/> Off <input checked="" type="radio"/> On
Network	<input type="text" value="192.168.11.0"/>
Netmask	<input type="text" value="255.255.255.0"/>

### 16.5.5 Open VPN with third-party server



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

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

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

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

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

Edit Open VPN Connection #1

Mode

☐ Disable ☒ Enable

VPN Mode

☐ Server ☐ Client ☒ Custom

Custom Config

Import \*.ovpn

i

⬇

Status

Connected

IP

Connected since

10.211.1.5

2017-06-21 11:30:40

Back

Refresh

Apply

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.

Follow @vpngate

VPN Gate

An academic experiment

Public VPN relay servers

Hosted by volunteers

Liberty!!

VPN Gate Client

Domestic Internet

VPN

Target servers

Oversea Internet

YouTube

twitter

www.vpngate.net

An academic experiment  
@ Graduate School of  
University of Tsukuba, Japan  
[www.tsukuba.ac.jp/english/](http://www.tsukuba.ac.jp/english/)

Free Access to World Knowledge Beyond Government's Firewall.

Your IP: FL1-119-240-145-93.stm.mesh.ad.jp (119.240.145.93)

Your country: Japan

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

🔧

Welcome to VPN Gate. (Launched on March 8, 2013.)

- You can get through your government's firewall to browse restricted websites. (e.g. YouTube.)

- You can disguise your IP address to hide your identity while surfing the Internet.

- You can protect yourself by utilizing the strong encryption while using public Wi-Fi. More Details...

Supports Windows, Mac, iPhone, iPad and Android.

SoftEther VPN

Supports OpenVPN, L2TP/IPsec and SSL-VPN.

www.softether.org

An open-source VPN software development project since March 8.

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

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

VPN Session ID	Start time (UTC)	VPN source country	VPN destination country	Destination VPN server	VPN protocol
VPN-3897814392	2018/03/07 1:31:13 (0 mins ago)	Ukraine	Canada	184.146.x.x	OpenVPN
VPN-3897814391	2018/03/07 1:30:31 (0 mins ago)	France	Croatia (LOCAL Name: Hrvatska)	93.143.x.x	OpenVPN
VPN-3897814390	2018/03/07 1:29:53 (1 mins ago)	United Kingdom	Japan	58.183.x.x	OpenVPN
VPN-3897814389	2018/03/07 1:29:40 (1 mins ago)	France	Venezuela	190.75.x.x	OpenVPN
VPN-3897814388	2018/03/07 1:29:36 (1 mins ago)	France	Venezuela	190.75.x.x	OpenVPN

Recent VPN activity status worldwide (3,185 entries)

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

Rank	Country	Traffic	# Connections
1	Korea Republic of	23,065,257.5 GB	118,005,960
2	China	10,001,271.4 GB	539,459,030
3	United States	9,442,248.6 GB	230,129,948
4	Taiwan	7,964,893.1 GB	306,587,109
5	Japan	6,644,702.7 GB	104,583,401

Top countries with most users (Refreshed in real time)

4G LTE COMPACT INDUSTRIAL CELLULAR ROUTER\_RT-MOB-020 - UM V1.1.8

155



## 16.5.6 Install Open VPN Access Server on Docker

### Open VPN Access Server on Docker installation

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

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

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

The detail please look <https://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/](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
```

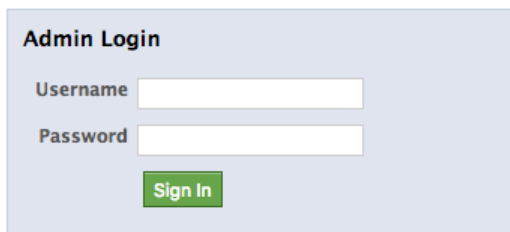
Check the Open VPN Access Server by visiting [https://<server\\_ip\\_or\\_domain>:943](https://<server_ip_or_domain>:943)

## Setup Open VPN Access Server for Cellular Router

The admin page is [https://<server\\_ip\\_or\\_domain>:943/admin](https://<server_ip_or_domain>:943/admin)

The default administrator username and password is admin/password.

Login page:

The image shows a screenshot of the OpenVPN Admin Login page. It has a light blue background. At the top, it says 'Admin Login'. Below that, there are two input fields: 'Username' and 'Password'. At the bottom, there is a green 'Sign In' button.

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

Logout

Help

Status

Status Overview

Current Users

Log Reports

Configuration

License

SSL Settings

Server Network Settings

VPN Mode

VPN Settings

Advanced VPN

Web Server

Client Settings

Failover

User Management

User Permissions

Group Permissions

Revoke Certificates

Authentication

General

PAM

RADIUS

LDAP

Tools

Profiles

Connectivity Test

Documentation

Support

Settings Changed

LOCAL selected for user authentication.

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

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

3. Update Running Server

User Authentication

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

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

Authenticate users using:

2. Local

PAM

RADIUS

LDAP

Save Settings

At a glance

Server Status: on

More

License: 2 devices

Info

Current Users: 0

List

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.)

Logout

Help

Status

Status Overview

Current Users

Log Reports

Configuration

License

SSL Settings

Server Network Settings

VPN Mode

VPN Settings

Advanced VPN

Web Server

Client Settings

Failover

User Management

1. User Permissions

Group Permissions

Revoke Certificates

User Permissions

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

No Default Group

Search/Refresh

Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
admin	No Default Group	Show	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2. New Username: test	No Default Group	3. Show	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

☐ Require user permissions record for VPN access

Save Settings

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

## User Permissions

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

 No Default Group 

Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
admin	No Default Group	Show	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>New Username:</b>						
test	No Default Group	Hide	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Local Password:</b>						
		4.	<input type="password"/> (No Password Set)			
<b>Select IP Addressing :</b>						
			<input checked="" type="radio"/> Use Dynamic <input type="radio"/> Use Static			
<b>Access Control</b>						
<b>Select addressing method:</b>						
			<input checked="" type="radio"/> Use NAT <input type="radio"/> Use routing			
<b>Allow Access To these Networks:</b>						
			<input type="text"/>			
List subnets in <i>network/nbits</i> form						
<input type="checkbox"/> all server-side private subnets						
<b>Allow Access From:</b>		5.	<input checked="" type="checkbox"/> all other VPN clients			
<b>VPN Gateway</b>						
<b>Configure VPN Gateway:</b>			<input checked="" type="radio"/> No <input type="radio"/> Yes			
<b>DMZ settings</b>						
<b>Configure DMZ IP address:</b>			<input checked="" type="radio"/> No <input type="radio"/> 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.

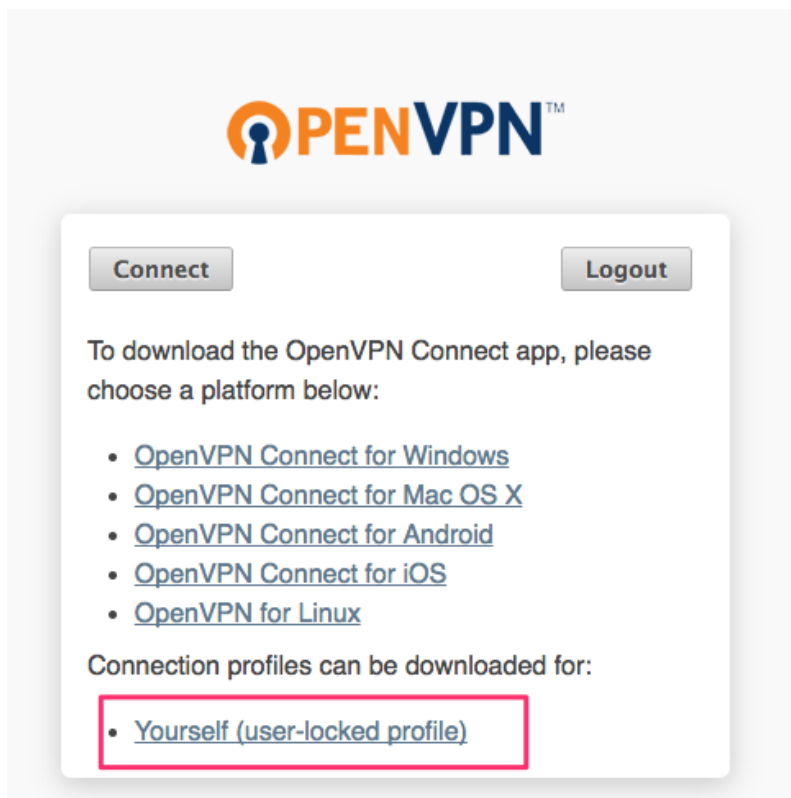
7.

## Setup Cellular Router Open VPN client

The image shows the OpenVPN login interface. At the top is the OpenVPN logo. Below it is a form with two input fields: 'Username' containing the text 'test' and 'Password' containing four dots. To the right of the password field is a dropdown menu currently set to 'Login', which is highlighted with a red rectangle. Next to the dropdown is a blue 'Go' button.

Use the user test/test to login [https://<server\\_ip\\_or\\_domain>:943](https://<server_ip_or_domain>:943)

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

The image shows the OpenVPN interface after a successful login. At the top is the OpenVPN logo. Below it are two buttons: 'Connect' and 'Logout'. The 'Logout' button is highlighted with a red rectangle. Below the buttons, there is a section titled 'To download the OpenVPN Connect app, please choose a platform below:' followed by a list of links: 'OpenVPN Connect for Windows', 'OpenVPN Connect for Mac OS X', 'OpenVPN Connect for Android', 'OpenVPN Connect for iOS', and 'OpenVPN for Linux'. Below this list is another section titled 'Connection profiles can be downloaded for:' followed by a list with one item: 'Yourself (user-locked profile)', which is highlighted with a red rectangle.

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

Edit Open VPN Connection #1

Setting

Log

Mode
☐ Disable
☒ Enable

VPN Mode
☐ Server
☐ Client
☒ Custom

Custom Config

1.
Import \*.ovpn
i

2.
Username
test

3.
Password
test

Status
Connected

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

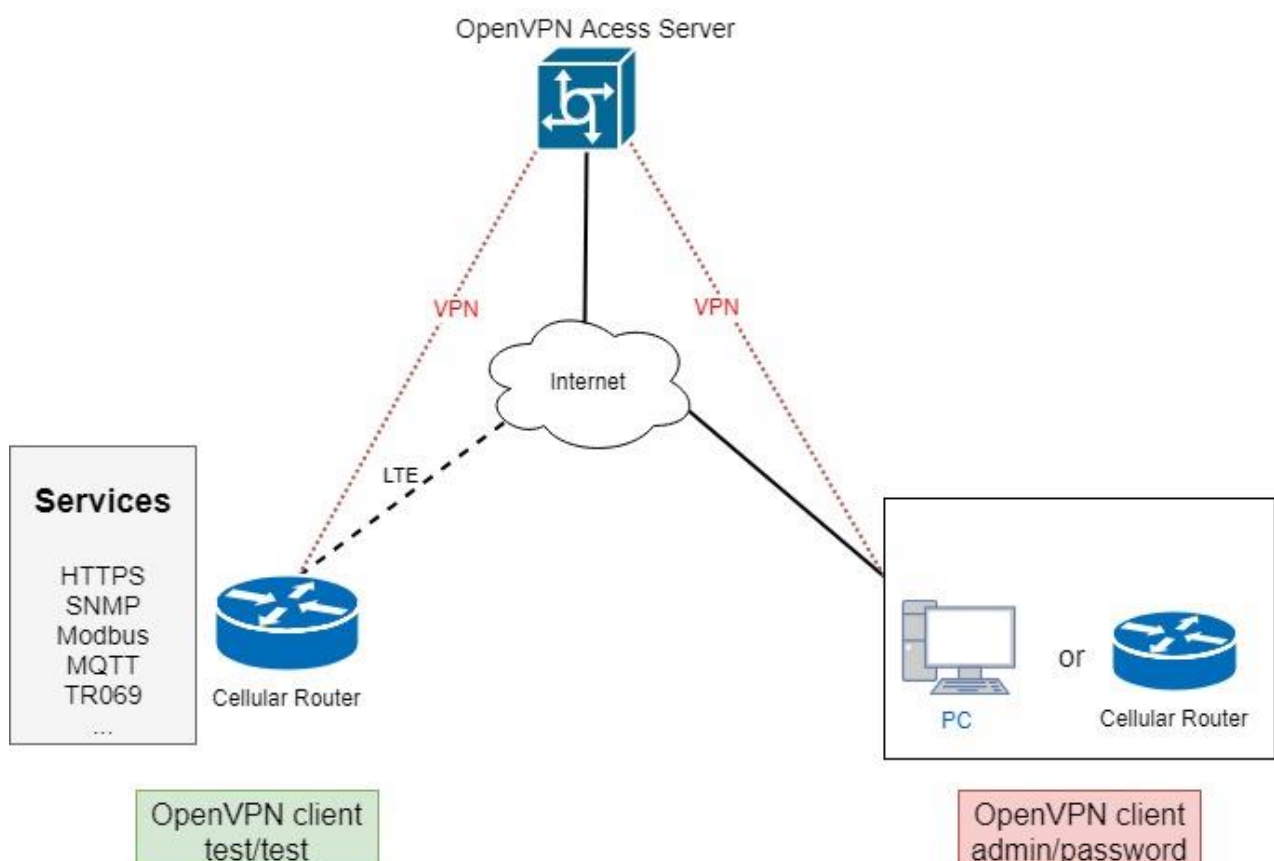
Back

4.

Refresh

Apply

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



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

## 16.5.7 Install Pritunl Open VPN server on Docker

### Pritunl Open VPN server on Docker installation

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

#### Quick Installation

##### ■ Prerequisites

- Ubuntu 16.04
- curl or wget should be installed

##### ■ Install via curl

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

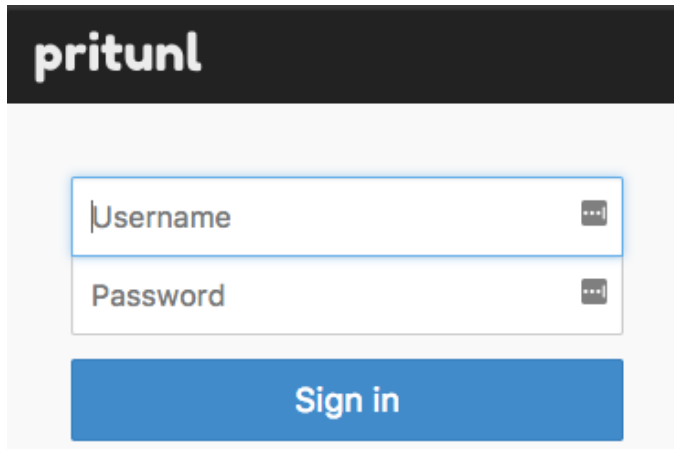
(4) Check the Pritunl Open VPN Server by visiting `https://<server_ip_or_domain>`

## 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.

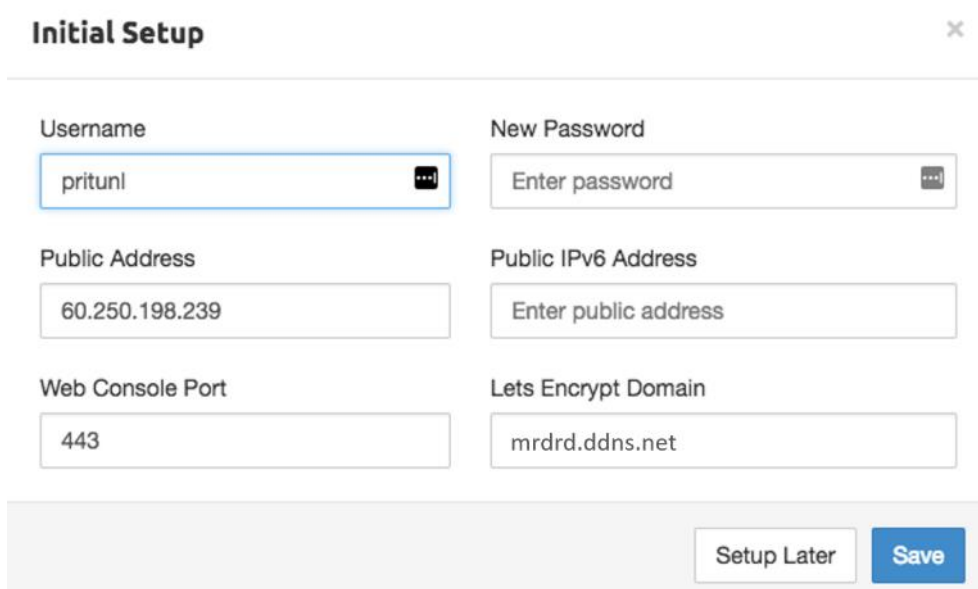
Login Page:



The login form features the 'pritunl' logo at the top. Below it are two input fields: 'Username' and 'Password', each with a toggle icon on the right. A blue 'Sign in' button is positioned at the bottom of the form.

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

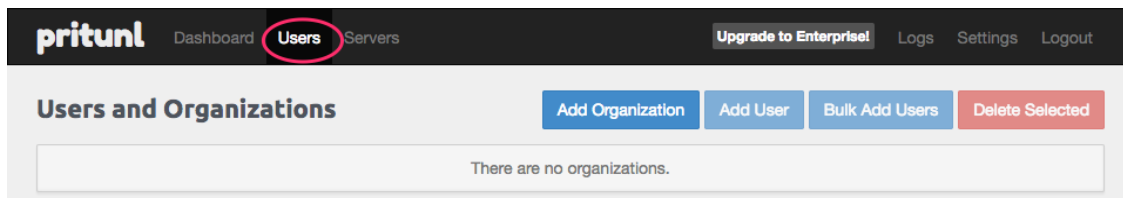
### Initial Setup:



The 'Initial Setup' page has a title bar with a close button. It contains six input fields arranged in two columns: 'Username' (pre-filled with 'pritunl'), 'New Password' (placeholder 'Enter password'), 'Public Address' (pre-filled with '60.250.198.239'), 'Public IPv6 Address' (placeholder 'Enter public address'), 'Web Console Port' (pre-filled with '443'), and 'Lets Encrypt Domain' (pre-filled with 'mrdrd.ddns.net'). At the bottom right are 'Setup Later' and 'Save' buttons.

### Open VPN user setup

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



The 'Users and Organizations' page shows a navigation bar with 'Dashboard', 'Users' (highlighted with a red circle), and 'Servers'. It also includes links for 'Upgrade to Enterprise!', 'Logs', 'Settings', and 'Logout'. Below the navigation bar are buttons for 'Add Organization', 'Add User', 'Bulk Add Users', and 'Delete Selected'. A message box states 'There are no organizations.'

Add the organization by click the Add Organization button.



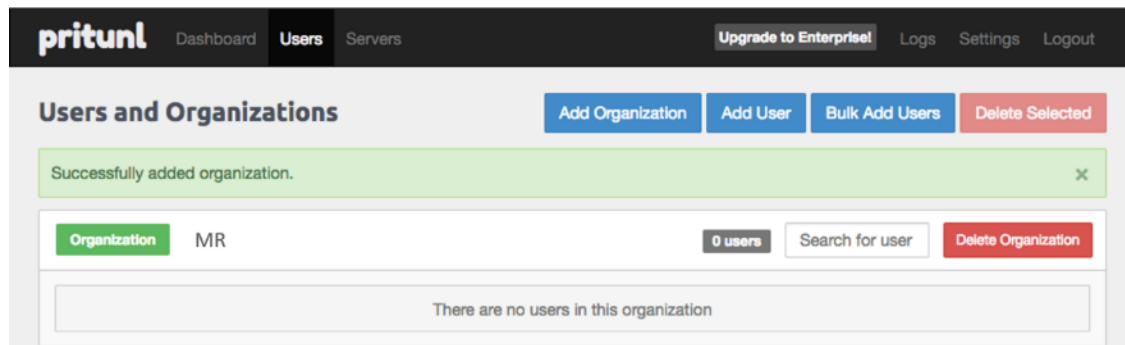
## Add Organization



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

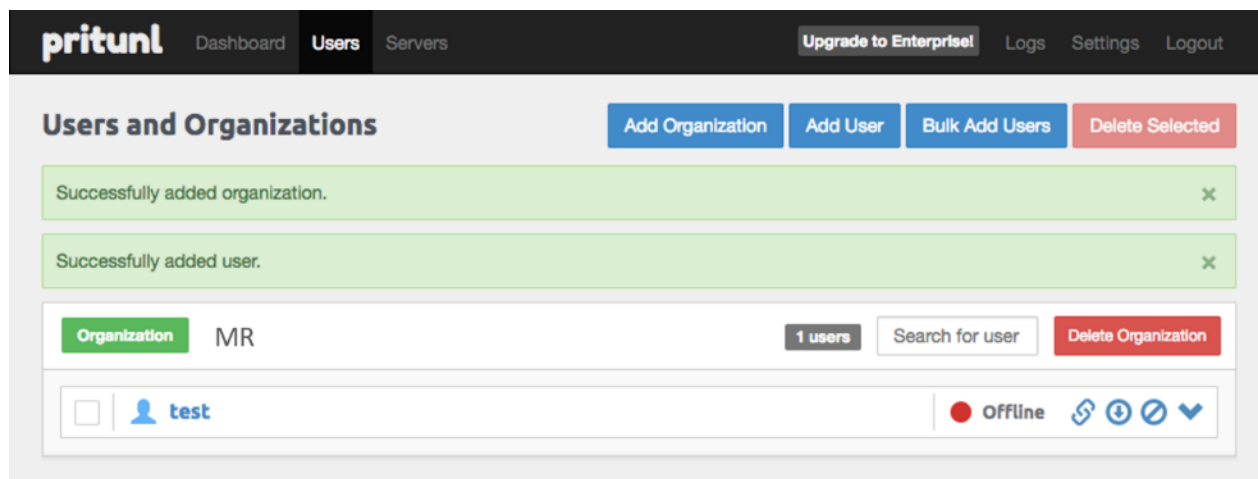
Select an organization

Email (optional)

Pin

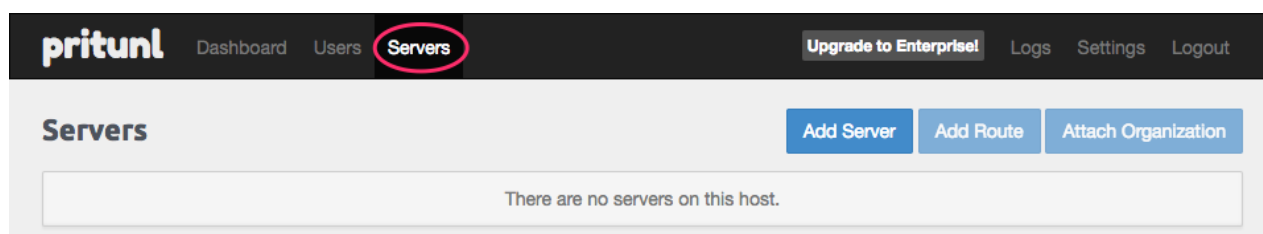
**Note:** In this Open VPN server, the PIN must contain only digits.

**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.

### Add Server

Advanced

Name

Name of VPN server

Port

Protocol

☐ Enable IPv6

DNS Server

Virtual Network

253 Users

☐ Enable Two-Step Authentication

Cancel

Add

**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.

**pritudl** Dashboard Users **Servers** Upgrade to Enterprise! Logs Settings Logout

## Servers

Add Server Add Route Attach Organization

Successfully added server. ✕

**Server** router **Server must have an organization attached** Start Server Delete Server

<p><b>Status</b> Offline</p> <p><b>Uptime</b> -</p> <p><b>Users</b> -/- users online</p> <p><b>Devices</b> 0 devices online</p> <p><b>Network</b> 192.168.234.0/24</p> <p><b>Port</b> 17470/udp</p> <p><b>Multiple Devices</b> Disabled</p>	<p>Server Output Bandwidth Graphs</p> <p>1</p>
---	--

0.0.0.0/0 Remove Route

192.168.234.0/24 Virtual Network Remove Route

There are no organizations attached to this server.

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

## Attach Organization ✕

Select an organization

MR

Select a server

router

Cancel Attach

Start the Open VPN server by click Start Server button.

The screenshot shows the Pritunl web interface with the 'Servers' tab selected. At the top, there are navigation links: Dashboard, Users, Servers, Upgrade to Enterprise!, Logs, Settings, and Logout. Below the navigation bar, the 'Servers' section has buttons for 'Add Server', 'Add Route', and 'Attach Organization'. Two green success messages are displayed: 'Successfully added server.' and 'Successfully attached organization.'.

The main content area shows a server named 'router' with a status of 'Offline'. To the right of the server name are two buttons: 'Start Server' (highlighted with a red circle) and 'Delete Server'. Below the server name, there is a 'Server Output' tab and a 'Bandwidth Graphs' tab. The 'Server Output' tab shows a list of output lines, with the first line being '1'.

Below the server output, there are three rows of configuration options:

- 0.0.0.0/0 with a 'Remove Route' button.
- 192.168.234.0/24 with 'Virtual Network' and 'Remove Route' buttons.
- MR with a 'Detach Organization' button.

## Cellular Router setup

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

The screenshot shows the Pritunl web interface with the 'Users' tab selected. The 'Users and Organizations' section has buttons for 'Add Organization', 'Add User', 'Bulk Add Users', and 'Delete Selected'. Below these buttons, there is a search bar and a 'Delete Organization' button.

The main content area shows a user named 'test' with a status of 'Offline'. To the right of the user name are four buttons: a red circle, a blue circle, a blue circle with a plus sign (highlighted with a red circle), and a blue circle with a minus sign.

**Note:** In this document, you should get the MR\_test\_router.ovpn file.

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

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

Edit Open VPN Connection #1

Setting

Log

Mode

☐ Disable
☒ Enable

VPN Mode

☐ Server
☐ Client
☒ Custom

Custom Config

Import \*.ovpn

i

Username

test

Password

123456

Status

Connected

IP

192.168.235.2

Connected since

2017-08-16 16:04:16

Back

Refresh

Apply

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

pritu
Dashboard
Users
Servers
Upgrade to Enterprise!
Logs
Settings
Logout

Users and Organizations

Add Organization
Add User
Bulk Add Users
Delete Selected

Organization

MR

1 users

Search for user

Delete Organization

☐

test

Online

router
calm-plateau-9655

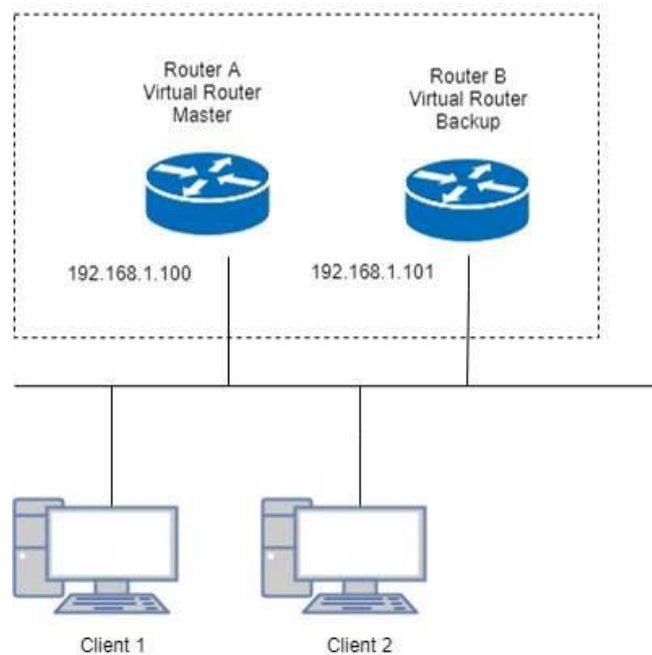
192.168.235.2
60.250.198.235
4:04 pm
Online

4G LTE COMPACT INDUSTRIAL CELLULAR ROUTER\_RT-MOB-020 - UM V1.1.8

169

## 16.6 VRRP Topology

### Basic VRRP Topology



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

## 16.7 TR069 Server (GenieACS Installation)

Server OS: Ubuntu 14.04 on Virtualbox

### Installation:

- 1) Login ubuntu
- 2) Change to root by 'su -' and enter your root password.
- 3) Install required package as below command:  
`>apt install gcc openssl-devel zlib-devel readline-devel sqlite-devel`
- 4) Make a directory for application installation  
`>mkdir /opt`
- 5) Install yaml  
`cd /opt`  
`wget http://pyyaml.org/download/libyaml/yaml-0.1.7.tar.gz`  
`tar xvfz 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 xvfz 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

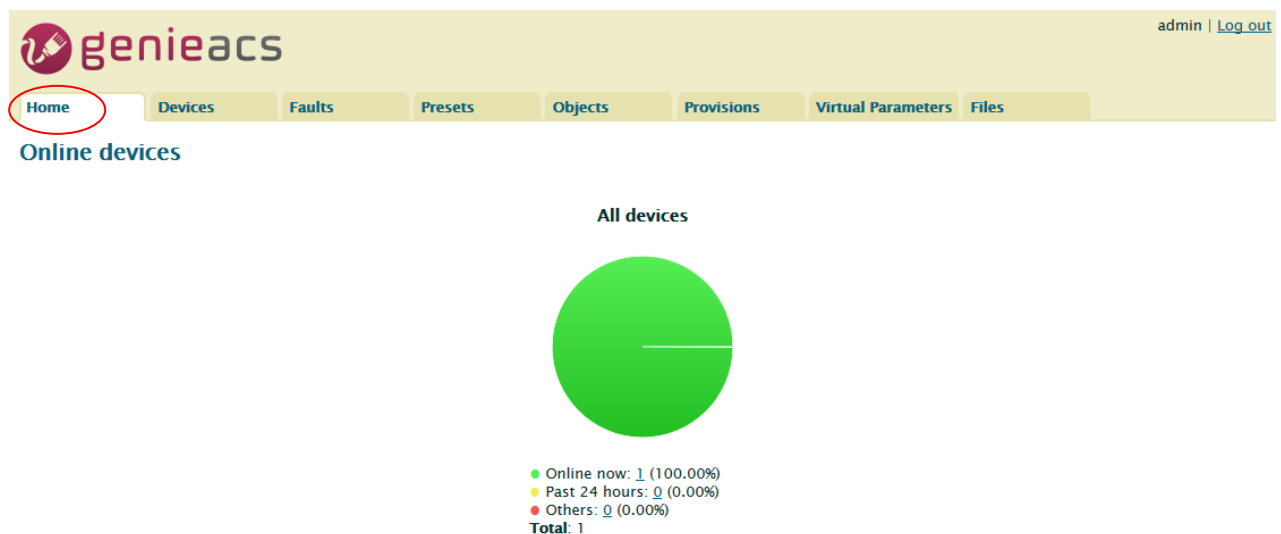
Fill in the ACS URL field as http://GenieACS server IP:**7547**

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

### 2) GenieACS Operation

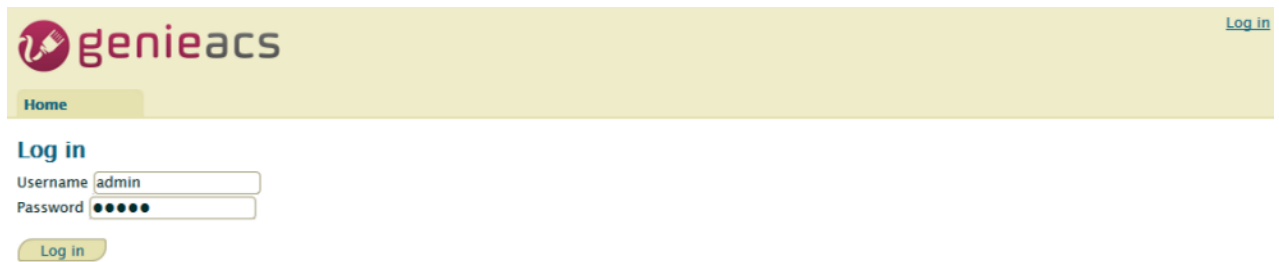
Input http://GenieACS server IP:**3000** on browser url bar and Enter.

Press Home tab to refresh Online devices status.



## 2.1) Login

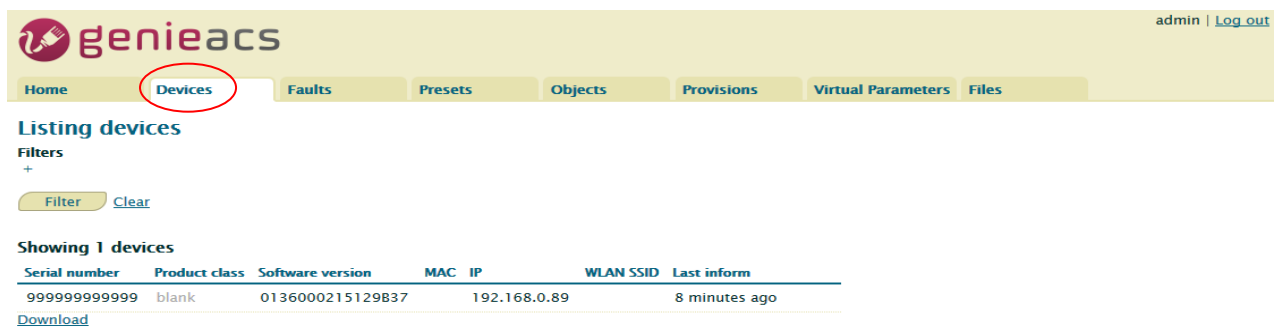
Username and Password are admin/admin.



The login page features the Genieacs logo at the top left and a 'Log in' link at the top right. Below the logo is a 'Home' button. The main section is titled 'Log in' and contains two input fields: 'Username' with the value 'admin' and 'Password' with masked characters. A 'Log in' button is positioned below the password field.

## 3) Device information

Press Devices tab



The 'Devices' page shows a navigation bar with tabs: Home, Devices (highlighted), Faults, Presets, Objects, Provisions, Virtual Parameters, and Files. Below the navigation bar is a 'Listing devices' section with a 'Filters' dropdown and 'Filter' and 'Clear' buttons. A table titled 'Showing 1 devices' displays the following data:

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

A 'Download' link is located below the table.

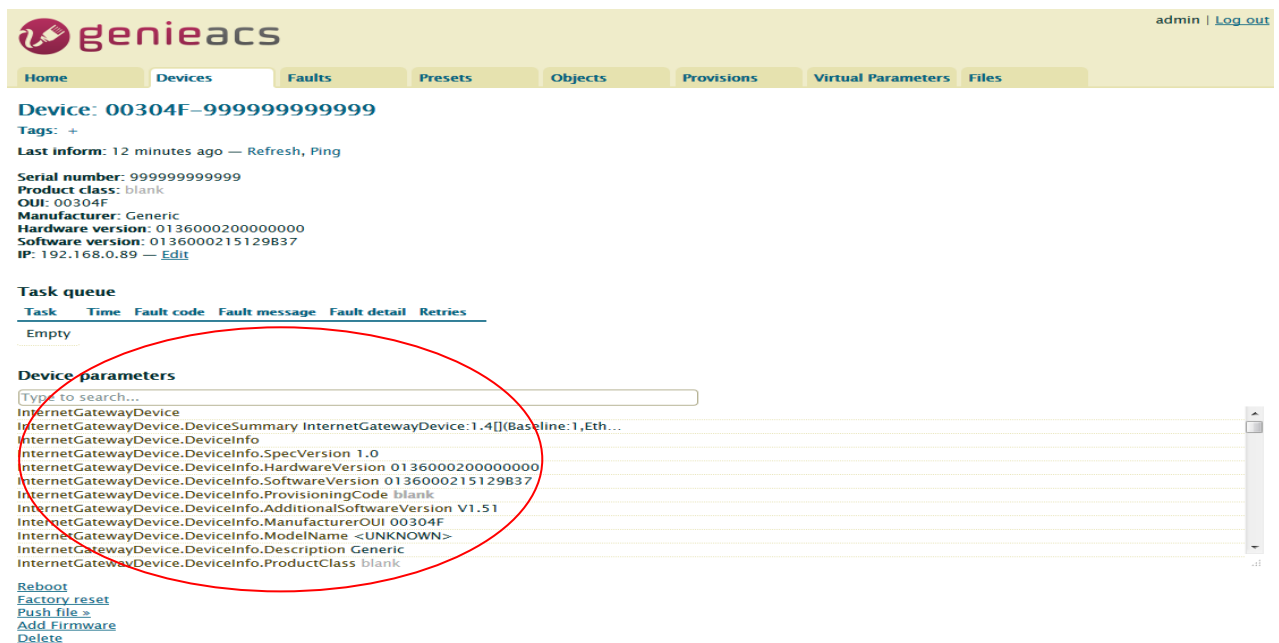
Move mouse to line end of your device, the [Show](#) link show up.

### Showing 1 devices

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

Download

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



The 'Device: 00304F-999999999999' page displays detailed information about the selected device. It includes a 'Tags' section, a 'Last inform' timestamp, and a list of device parameters such as Serial number, Product class, OUI, Manufacturer, Hardware version, Software version, and IP. A 'Task queue' table is also present, showing an empty state. The 'Device parameters' section is highlighted with a red circle, showing a list of parameters and their values. At the bottom, there are links for 'Reboot', 'Factory reset', 'Push file', 'Add Firmware', and 'Delete'.

#### 4) Access parameters

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

*For Readable parameter*

##### Device parameters

Type to search...
InternetGatewayDevice
InternetGatewayDevice.DeviceSummary InternetGatewayDevice:1.4[] (Baseline: 1, Eth...
InternetGatewayDevice.DeviceInfo
InternetGatewayDevice.DeviceInfo.SpecVersion 1.0
InternetGatewayDevice.DeviceInfo.HardwareVersion 0136000200000000
InternetGatewayDevice.DeviceInfo.SoftwareVersion 0136000215129B37
InternetGatewayDevice.DeviceInfo.ProvisioningCode blank

[Refresh](#)


*For Readable and Writable parameter*

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

[Edit](#) [Refresh](#)

#### 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.

admin | [Log out](#)

[Home](#) [Devices](#) [Faults](#) [Presets](#) [Objects](#) [Provisions](#) [V...](#)

Pending tasks  
■ Refresh mode  
[Commit](#) [Cancel](#)

**Device: 00304F-999999999999**  
**Tags:** +  
**Last inform:** 12 minutes ago — [Refresh](#), [Ping](#)  
**Serial number:** 999999999999  
**Product class:** blank  
**OUI:** 00304F  
**Manufacturer:** Generic  
**Hardware version:** 0136000200000000  
**Software version:** 0136000215129B37  
**IP:** 192.168.0.89 — [Edit](#)

**Task queue**

Task	Time	Fault code	Fault message	Fault detail	Retries
Empty					

**Device parameters**

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

[Reboot](#)  
[Factory reset](#)  
[Push file »](#)  
[Add Firmware](#)  
[Delete](#)

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.

The screenshot shows the GenieACS web interface. At the top, there's a navigation bar with links: Home, Devices, Faults, Presets, Objects, Provisions, Virtual Parameters, and Files. Below this, a status bar indicates 'Device is offline'. The main content area displays details for a device with ID '00304F-999999999999'. It lists various attributes like Serial number, Product class, OUI, Manufacturer, Hardware version, Software version, and IP. A 'Task queue' section is visible, showing a table with columns for Task, Time, Fault code, Fault message, and Fault detail. Below this, the 'Device parameters' section is shown, with a search bar and a list of parameters. One parameter, 'InternetGatewayDevice.X\_ROUTER\_DNAT.entry.16.mode', is highlighted. An 'Editing' dialog box is open, showing the current value 'off' and buttons for 'OK' and 'Cancel'. The dialog box is circled in red.

Input new value and press OK.

This is a close-up of the 'Editing' dialog box from the previous screenshot. The title is 'Editing InternetGatewayDevice.X\_ROUTER\_DNAT.entry.16.mode'. The input field contains the text 'on'. The 'OK' button is circled in red, along with the input field.

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

The screenshot shows the GenieACS web interface. At the top right, a 'Pending tasks' modal is open, containing a red square icon, the text 'Edit mode', and 'Commit' and 'Cancel' buttons. The modal is circled in red. Below the modal, the page shows 'Device is offline'. The device details for '00304F-999999999999' are listed, including serial number, product class, OUI, manufacturer, hardware and software versions, and IP address. A 'Task queue' section shows an empty table. The 'Device parameters' section has a search bar and a list of parameters for 'InternetGatewayDevice.X\_ROUTER\_DNAT.entry.15'. At the bottom, there are links for 'Reboot', 'Factory reset', 'Push file', 'Add Firmware', and 'Delete'.

Press Commit to set this parameter value.

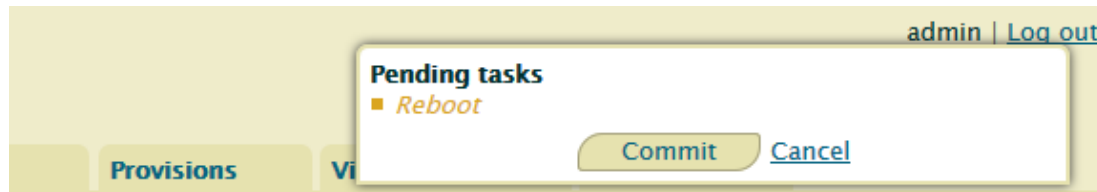
**Note:** If the GenieACS can reach the device, the parameter value will be set immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.

## 5) Reboot device

Press on **Reboot** link.

The screenshot shows the GenieACS web interface for a device named '00304F-Mobile%20Router-999999999999'. The device details are listed, including serial number, product class, OUI, manufacturer, hardware and software versions, and IP address. The 'Task queue' section shows an empty table. The 'Device parameters' section has a search bar and a list of parameters for 'InternetGatewayDevice'. At the bottom, there are links for 'Reboot', 'Factory reset', 'Push file', 'Add Firmware', and 'Delete'. The 'Reboot' link is circled in red.

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.

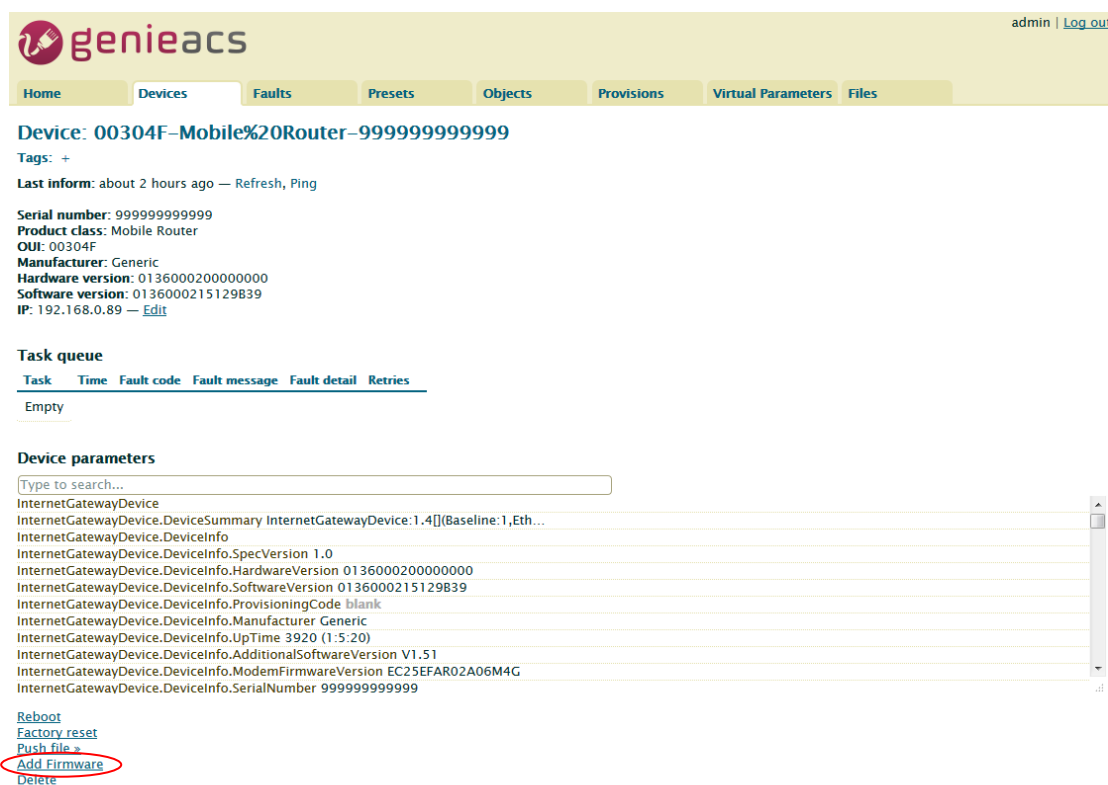
## 6) Reset to default

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

admin | [Log out](#)

Home Devices Faults Presets Objects Provisions Virtual Parameters Files

### New file

File type: 1 Firmware Upgrade Image

OUI: 00304F

Product class: Mobile Router

Version: 0136000215129B39

File:  [浏览...](#)

[Upload](#) [Back](#)

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

admin | [Log out](#)

Home Devices Faults Presets Objects Provisions Virtual Parameters Files

### Listing files

Showing 1 files

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

[New File](#)

## 7.2) Upgrade

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

### Device parameters

Type to search...

InternetGatewayDevice

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

InternetGatewayDevice.DeviceInfo

InternetGatewayDevice.DeviceInfo.SpecVersion 1.0

InternetGatewayDevice.DeviceInfo.HardwareVersion 0136000200000000

InternetGatewayDevice.DeviceInfo.SoftwareVersion 0136000215129B39

InternetGatewayDevice.DeviceInfo.ProvisioningCode blank

InternetGatewayDevice.DeviceInfo.Manufacturer Generic

InternetGatewayDevice.DeviceInfo.UpTime 1020 (0:17:0)

InternetGatewayDevice.DeviceInfo.AdditionalSoftwareVersion V1.51

InternetGatewayDevice.DeviceInfo.ModemFirmwareVersion EC25EFAR02A06M4G

InternetGatewayDevice.DeviceInfo.SerialNumber 999999999999

[Reboot](#)

[Factory reset](#)

[Push file >>](#) **m300.img (1 Firmware Upgrade Image)**

[Add Firmware](#)

[Delete](#)

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

### Pending tasks

■ Push file (m300.img)

[Commit](#) [Cancel](#)

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.

VLAN

Mode

☐ Off ☒ Tag Base ☐ Port Base

VLAN Isolation

☒ Off ☐ On

Enable	Subnet	VID	Port			
			LAN1	LAN2	LAN3	Router
<input checked="" type="checkbox"/>	NET1	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	NET2	20	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	NET3	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	NET4	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	NET5	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	NET6	6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	NET7	7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	NET8	8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PVID			10	10	20	--
Tag Mode			Access	Access	Trunk	--

Apply

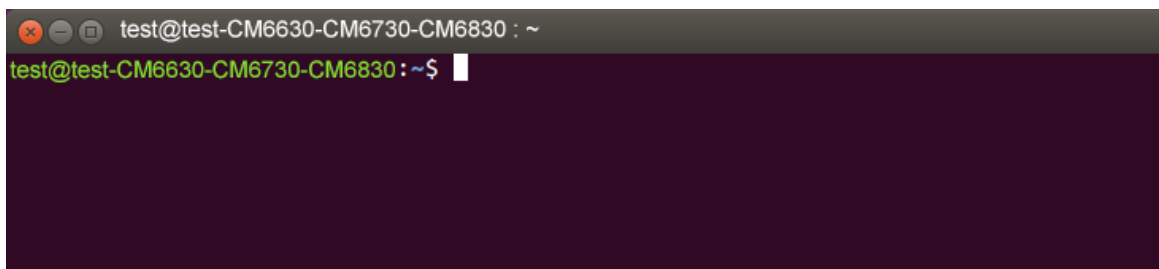


### Note:

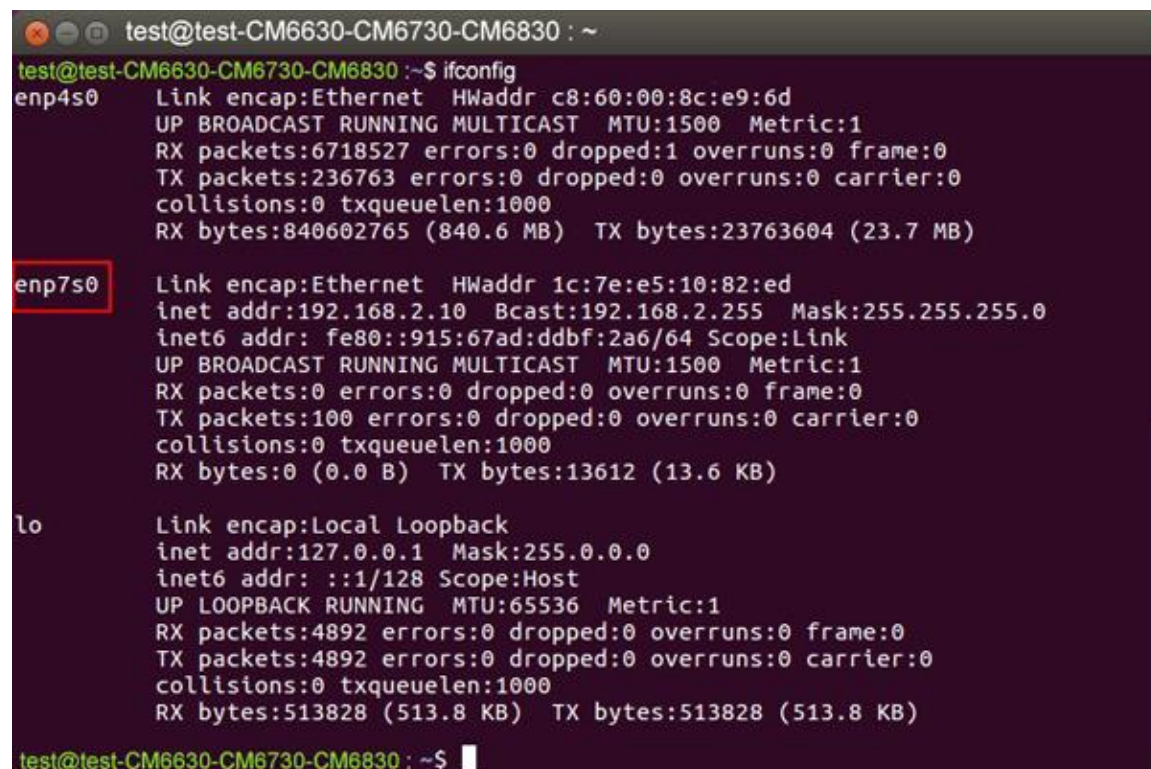
- Different PCs have different interface of network cards, like PC-A network card is eth1.10 for example 1 and PC-B network card is eth1.20 for example 2.
- How to find out the terminal and the interface of network cards based on different PCs.
  - From the following picture, you can click *the finding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



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



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



There are two examples to explain how configure VLAN settings.

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

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

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

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

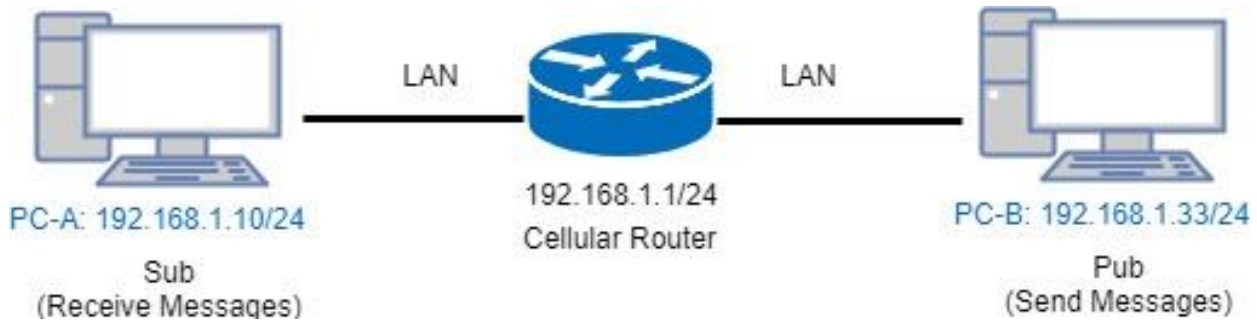
#### **Example 2: PC-A ping PC-B (Trunk to Access)**

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

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

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

## 17.2 MQTT Topology



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

Expect Result:

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

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

There is a process to explain the steps and result.

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

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

```
test@test: ~  
test@test:~$ sudo apt-get install mosquitto-clients  
sudo: unable to resolve host test  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  geoip-database-extra javascript-common libjs-openlayers libnghttp2-14  
  libnl-route-3-200 libqgsttools-p1 libqt5multimedia5-plugins  
  libqt5multimediawidgets5 libsmi2ldbl libssh-gcrypt-4 libwireshark-data  
  libwiretap6 libwscodec5 libwsutil7 linux-headers-4.10.0-28  
  linux-headers-4.10.0-28-generic linux-headers-4.10.0-42  
  linux-headers-4.10.0-42-generic linux-headers-4.13.0-26  
  linux-headers-4.13.0-26-generic linux-image-4.10.0-28-generic  
  linux-image-4.10.0-42-generic linux-image-4.13.0-26-generic  
  linux-image-extra-4.10.0-28-generic linux-image-extra-4.10.0-42-generic  
  linux-image-extra-4.13.0-26-generic  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
  libc-ares2 libmosquitto1  
The following NEW packages will be installed:  
  libc-ares2 libmosquitto1 mosquitto-clients  
0 upgraded, 3 newly installed, 0 to remove and 119 not upgraded.  
Need to get 65.3 kB/96.4 kB of archives.  
After this operation, 330 kB of additional disk space will be used.  
Do you want to continue? [Y/n] Y
```

```

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

```

- Step2: Configure MQTT for the Cellular Router

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

MQTT

Mode

☐ Disable
 ☒ Enable

Port

1883

Manage Users

	Username	Password	Delete
Username	test		
Password		....	
			Add



MQTT

Mode

☐ Disable
 ☒ Enable

Port

1883

Manage Users

Username	Password	Delete
test	....	

Username

test2

Password

.....

Add

MQTT

Mode

☐ Disable
 ☒ Enable

Port

1883

Manage Users

Username	Password	Delete
test	....	
test2	.....	

Username

Password

Add

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

## ACLs

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

## ACLs

User	Topic	Subscribe	Publish	Delete
test	acb	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
test2	abc	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User				
Topic				
		<input type="checkbox"/> Subscribe		
		<input type="checkbox"/> Publish		
<button>Add</button>				

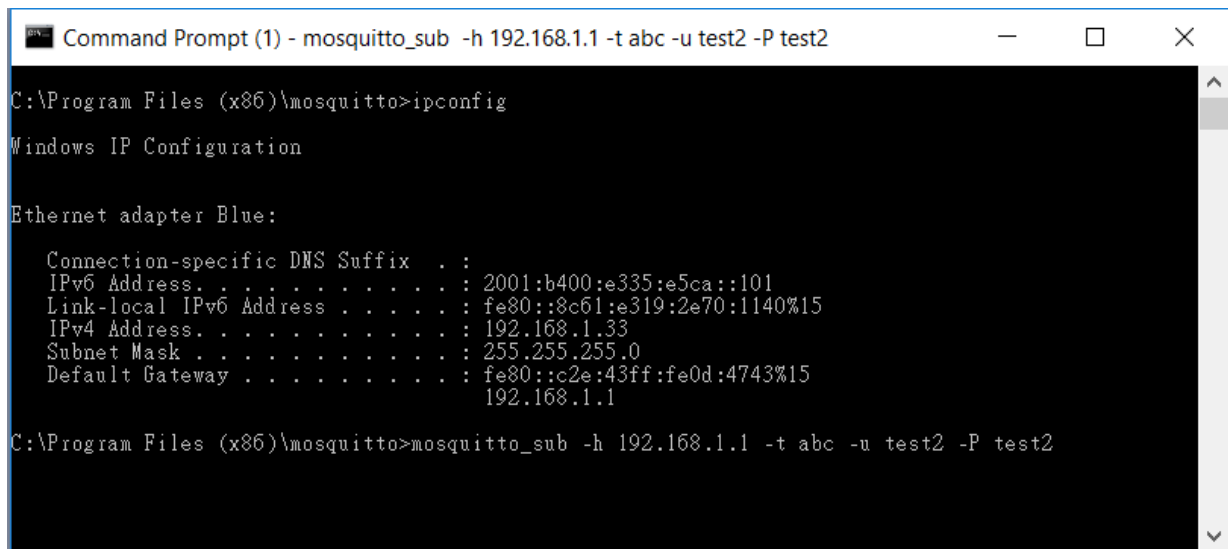
### Note:

- 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".



```

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

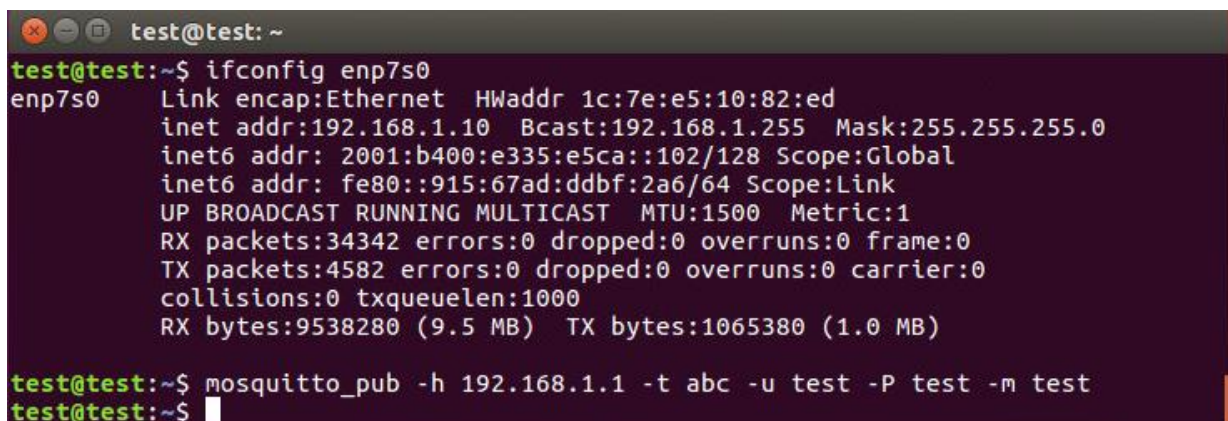
Windows IP Configuration

Ethernet adapter Blue:

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

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

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



```

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

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



```

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

Windows IP Configuration

Ethernet adapter Blue:

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

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

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

For PC-A, command "mosquitto\_sub -h 192.168.1.1 -t abc -u test -P test"

```
test@test: ~  
test@test:~$ ifconfig enp7s0  
enp7s0    Link encap:Ethernet  HWaddr 1c:7e:e5:10:82:ed  
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: 2001:b400:e335:e5ca::102/128 Scope:Global  
          inet6 addr: fe80::915:67ad:ddbf:2a6/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:50690 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:4831 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:10908302 (10.9 MB)  TX bytes:1150596 (1.1 MB)  
  
test@test:~$ mosquitto_sub -h 192.168.1.1 -t abc -u test -P test
```

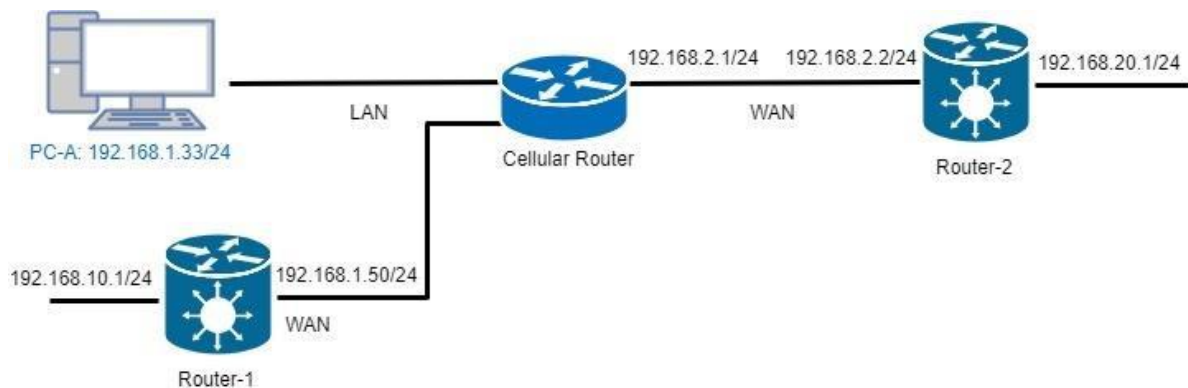
For PC-B, command "mosquitto\_pub -h 192.168.1.1 -t abc -u test2 -P test2 -m test" and confirm the message on PC-A. It will receive test message on PC-A.

```
Command Prompt (1)  
C:\Program Files (x86)\mosquitto>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Blue:  
  
    Connection-specific DNS Suffix  . :  
    IPv6 Address. . . . . : 2001:b400:e335:e5ca::101  
    Link-local IPv6 Address . . . . . : fe80::8c61:e319:2e70:1140%15  
    IPv4 Address. . . . . : 192.168.1.33  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : fe80::c2e:43ff:fe0d:4743%15  
                                192.168.1.1  
  
C:\Program Files (x86)\mosquitto>mosquitto_pub -h 192.168.1.1 -t abc -u test2 -P test2 -m test  
C:\Program Files (x86)\mosquitto>
```

```
test@test: ~  
enp7s0    Link encap:Ethernet  HWaddr 1c:7e:e5:10:82:ed  
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: 2001:b400:e335:e5ca::102/128 Scope:Global  
          inet6 addr: fe80::915:67ad:ddbf:2a6/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:50690 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:4831 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:10908302 (10.9 MB)  TX bytes:1150596 (1.1 MB)  
  
test@test:~$ mosquitto_sub -h 192.168.1.1 -t abc -u test -P test  
test
```



## 17.3 IP Routing Topology



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

- (1) PC-A sends ICMP packet to Router-1 LAN and WAN IP and they should have response.
- (2) PC-A sends ICMP packet to Router-2 LAN and WAN IP and they should have response.

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

- LAN configuration:

LAN IPv4

IP Address

192.168.1.1

IP Mask

255.255.255.0

DHCP Server Configuration

☒ DHCP Server Configuration

IP Address Pool

From

192.168.1.2

To

192.168.1.254

Apply

- WAN configuration:

WAN Ethernet

Work As

☐ DHCP Client

☐ PPPoE Client

☒ Static IPv4

Configuration

Ethernet Ping Health

Static IPv4 Configuration

IP Address

0.0.0.0

IP Mask

255.255.255.0

Gateway Address

0.0.0.0

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

### Example 1: Add IP Routing on LAN interface

- Step 1: The cellular router for Static Route configuration  
The Mode is on at the settings section and add the routing.
- Step 2: Router-1 configuration is as below.
  - (1) Login to the Router-1 web site, and then "NAT disable".
  - (2) Configure LAN IP: 192.168.10.1
  - (3) Configure WAN IP: 192.168.1.50

Static Route

Mode ☐ Off ☒ On

Settings

Status

Mode	Name	Destination	Gateway	Interface	Delete
<input type="radio"/> Off <input checked="" type="radio"/> On	<input type="text" value="lan side"/>	<input type="text" value="192.168.10.1"/>	<input type="text" value="192.168.1.50"/>	<input type="text" value="&lt;empty&gt;"/>	

Add

Apply

Static Route

Mode ☐ Off ☒ On

Settings

Status

Mode	Name	Destination	Gateway	Interface	Delete
<input type="radio"/> Off <input checked="" type="radio"/> On	<input type="text" value="lan side"/>	192.168.10.1	192.168.1.50		<input checked="" type="checkbox"/>

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



Static Route

Mode    ☐ Off    ☒ On

Settings

Status

Mode	Name	Destination	Gateway	Interface	Delete
<input type="radio"/> Off <input checked="" type="radio"/> On	<input type="text" value="wan side"/>	192.168.20.1	192.168.2.2	WAN Ethernet	

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

Command Prompt (1)

```

Ethernet adapter Blue:

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

C:\tools>ping 192.168.2.2

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

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

C:\tools>ping 192.168.20.1

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

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

C:\tools>

```