

# **TeleWell INDUSTRIAL 4G LTE Cellular Router**

SF300 / SF301  
SF300-G / SF301-G / SF301-TG  
SF301-TPG

User Manual

Version 1.1.6

# Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
1.1	Features .....	1
1.2	Specifications .....	2
1.3	Mechanical Dimensions.....	3
1.4	Ordering Information.....	4
<b>2</b>	<b>Hardware Installation .....</b>	<b>5</b>
2.1	LED Indicators .....	5
2.2	Ethernet Port .....	5
2.3	Serial Port COM1 (Console-RS232).....	7
2.4	Install the SIM Card .....	9
2.5	Reset Button.....	10
2.6	External Antenna .....	10
2.7	Connecting the Power Supply.....	10
2.8	Grounding the Router .....	11
2.9	Pin Assignments .....	11
2.10	Connecting I/O Ports .....	12
2.11	Serial Port COM2 (RS-232) .....	13
2.12	Serial Port COM3 (RS-485) .....	13
2.13	DIP Switch.....	14
<b>3</b>	<b>Configuration via Web Browser .....</b>	<b>15</b>
3.1	Access the Web Configurator .....	15
3.2	Navigate the Web Configurator.....	16
<b>4</b>	<b>Status .....</b>	<b>17</b>
4.1	Status > GPS.....	19
<b>5</b>	<b>Configuration &gt; System .....</b>	<b>20</b>
5.1	System > Time and Date .....	20
5.2	System > COM Ports.....	25
5.3	System > Logging.....	27
5.3.1	Logging > Logging.....	27
5.3.2	Logging > Log .....	28
5.4	System > Alarm .....	29
5.4.1	Alarm > Name Group.....	31
5.4.2	Alarm > Edit User .....	32
5.5	System > Ethernet.....	34
5.6	System > Modbus.....	34
5.7	System > Client List.....	35
<b>6</b>	<b>Configuration &gt; WAN .....</b>	<b>36</b>
6.1	WAN > Priority.....	36

6.2	WAN > Ethernet.....	36
6.2.1	WAN Ethernet Configuration.....	36
6.2.2	Ethernet Ping Health .....	39
6.3	WAN > IPv6 DNS .....	41
<b>7</b>	<b>Configuration &gt; LTE .....</b>	<b>42</b>
7.1	LTE > LTE Config .....	42
7.1.1	LTE Configuration.....	42
7.1.2	LTE Ping Health .....	43
7.2	LTE > GPS Config .....	44
7.3	LTE > Dual SIM .....	45
7.4	LTE > Usage Display .....	50
7.5	LTE > SMS .....	56
7.6	LTE > Engineer Info.....	57
7.7	LTE > DNS .....	58
<b>8</b>	<b>Configuration &gt; LAN .....</b>	<b>59</b>
8.1	LAN > IPv4 .....	59
8.2	LAN > IPv6 .....	60
8.3	LAN > VLAN .....	60
8.4	LAN > Subnet.....	64
<b>9</b>	<b>IP Routing .....</b>	<b>67</b>
9.1	IP Routing > Static Route .....	67
9.2	IP Routing > RIP.....	69
9.3	IP Routing > OSPF .....	72
9.4	IP Routing > BGP .....	76
<b>10</b>	<b>Configuration &gt; VPN .....</b>	<b>79</b>
10.1	VPN> OpenVPN.....	79
10.1.1	Edit OpenVPN Connection .....	80
10.1.2	Set up OpenVPN Client.....	83
10.1.3	Set up OpenVPN Server.....	84
10.1.4	Set up OpenVPN Custom.....	85
10.2	VPN > IPSec .....	87
10.2.1	IPSec > General setting.....	87
10.2.2	IPSec > Connections.....	88
10.2.3	IPSec > The setting of X.509 Certificates .....	91
10.2.4	IPSec > Net-to-Net Configuration .....	91
10.2.5	IPSec > Hub-Spoke Topology.....	97
10.3	VPN > GRE .....	99
10.4	VPN > PPTP Server .....	100
10.5	VPN > L2TP .....	102
<b>11</b>	<b>Configuration &gt; Firewall .....</b>	<b>106</b>
11.1	Firewall > Port Forwarding.....	106






11.2	Firewall > DMZ .....	108
11.3	Firewall > IP Filter .....	108
11.4	Firewall > MAC Filter .....	111
11.5	Firewall > URL Filter .....	112
11.6	Firewall > NAT .....	113
<b>12</b>	<b>Configuration &gt; Service .....</b>	<b>114</b>
12.1	Service > SNMP .....	114
12.1.1	SNMP configuration.....	114
12.1.2	SNMP v3 User configuration.....	115
12.1.3	SNMP trap configuration.....	116
12.2	Service > TR069.....	117
12.3	Service > Dynamic DNS .....	118
12.4	Service > VRRP .....	120
12.5	Service > MQTT .....	121
12.6	Service > UPnP .....	123
12.7	Service > SMTP .....	123
12.8	Service > IP Alias.....	124
<b>13</b>	<b>Configuration &gt; Management .....</b>	<b>125</b>
13.1	Management > Identification.....	125
13.2	Management > Administration .....	126
13.3	Management > SSH .....	128
13.4	Management > Firmware.....	129
13.5	Management > Configuration .....	129
13.6	Management > Load Factory .....	130
13.7	Management > Restart.....	130
<b>14</b>	<b>Configuration &gt; Diagnosis.....</b>	<b>130</b>
14.1	Diagnosis > Ping .....	130
14.2	Diagnosis > Traceroute.....	131
<b>15</b>	<b>Configuration Applications.....</b>	<b>131</b>
15.1	WAN Priority .....	131
15.2	LAN > IPv4/IPv6 Dual Stack.....	133
15.3	MQTT Broker.....	135
15.4	Virtual COM > Remote Management.....	137
15.5	Virtual COM > Remote Alarm.....	140
15.6	Virtual COM > Modbus RTU over TCP .....	141
15.7	Modbus Gateway.....	142
15.8	Alarm Configuration.....	142
15.9	OpenVPN Configuration .....	144
15.9.1	OpenVPN Server Mode.....	144
15.9.2	OpenVPN Client Mode .....	145
15.9.3	OpenVPN Net-to-Net.....	146
15.9.4	OpenVPN 1:1 NAT .....	149



15.9.5 OpenVPN with third-party server .....	151
15.9.6 Install OpenVPN Access Server on Docker .....	153
15.9.7 Install Pritunl OpenVPN server on Docker .....	159
15.10 VRRP Topology .....	167
15.11 TR069 Server (GenieACS Installation) .....	167
<b>16 Test Case Example .....</b>	<b>180</b>
16.1 VLAN Topology .....	180
16.2 MQTT Topology .....	184
16.3 Modbus Topology .....	190
16.4 IP Routing Topology.....	193

# 1 Introduction

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

Model Name	M300	M301	M300-G	M301-G M301-TG	M301-TPG
<b>Industrial 4G LTE Cellular Router (IP40/IP65/IP68)</b>					
<b>Cellular Technology</b>					
LTE Interface (2G, 3G, 4G)	GSM/WCDMA/LTE	GSM/WCDMA/LTE	GSM/WCDMA/LTE	GSM/WCDMA/LTE	GSM/WCDMA/LTE
LTE Band/Frequency	FDD LTE: B1/B3/B5/B7/B8/B20 TDD LTE: B38/B40/B41 WCDMA: B1/B5/B8 GSM: 900/1800 MHz LTE Cat4	FDD LTE: B1/B3/B5/B7/B8/B20 TDD LTE: B38/B40/B41 WCDMA: B1/B5/B8 GSM: 900/1800 MHz LTE Cat4	FDD LTE: B1/B3/B5/B7/B8/B20 TDD LTE: B38/B40/B41 WCDMA: B1/B5/B8 GSM: 900/1800 MHz LTE Cat4	FDD LTE: B1/B3/B5/B7/B8/B20 TDD LTE: B38/B40/B41 WCDMA: B1/B5/B8 GSM: 900/1800 MHz LTE Cat4	FDD LTE: B1/B3/B5/B7/B8/B20 TDD LTE: B38/B40/B41 WCDMA: B1/B5/B8 GSM: 900/1800 MHz LTE Cat4
Antenna Connector	2 x SMA (MAIN + AUX)	2 x SMA (MAIN + AUX)	3 x SMA (MAIN + AUX + GPS)	3 x SMA (MAIN + AUX + GPS)	3 x SMA (MAIN + AUX + GPS)
<b>Communication Interface</b>					
Ethernet	1 x 10/100 Mbps LAN 1 x 10/100 Mbps WAN	3 x 10/100 Mbps LANs 1 x 10/100 Mbps WAN	1 x 10/100 Mbps LAN 1 x 10/100 Mbps WAN	3 x 10/100 Mbps LANs 1 x 10/100 Mbps WAN	3 x 10/100 Mbps LANs 1 x 10/100 Mbps WAN
PoE	N/A	N/A	N/A	N/A	1 x IEEE 802.3at/af PoE P.D.
SIM Card	2	2	2	2	2
Serial	1 x RS485 (D+/D-) 1 x RS232 (TXD/RXD)	1 x RS485 (D+/D-) 1 x RS232 (TXD/RXD)	1 x RS485 (D+/D-) 1 x RS232 (TXD/RXD)	1 x RS485 (D+/D-) 1 x RS232 (TXD/RXD)	1 x RS485 (D+/D-) 1 x RS232 (TXD/RXD)
Console Port	RS232	RS232	RS232	RS232	RS232
I/O	2 x DI, 1 x DO (Alarm +/-)	2 x DI, 1 x DO (Alarm +/-)	2 x DI, 1 x DO (Alarm +/-)	2 x DI, 1 x DO (Alarm +/-)	2 x DI, 1 x DO (Alarm +/-)
GPS	N/A	N/A	1	1	1
<b>Temperature &amp; Power</b>					
Operating Temperature	-20 to +70 °C	-20 to +70 °C	-20 to +70 °C	•M301-G: -20 to +70 °C •M301-TG: -40 to +75 °C	-40 to +75 °C
Input Voltage	10~32 VDC	10~32 VDC	10~32 VDC	10~32 VDC	10~32 VDC
Power Consumption	< 7W	< 7W	< 7W	< 7W	< 7W
<b>Mechanical Construction</b>					
Dimensions (W x H x D)	60 x 110 x 106 mm	60 x 110 x 106 mm	60 x 110 x 106 mm	60 x 110 x 106 mm	60 x 110 x 106 mm
Weight	451 g (0.9943 lb)	452 g (0.9965 lb)	451 g (0.9943 lb)	452 g (0.9965 lb)	452 g (0.9965 lb)
Installation	DIN Rail (Default) Wall Mount (Optional)	DIN Rail (Default) Wall Mount (Optional)	DIN Rail (Default) Wall Mount (Optional)	DIN Rail (Default) Wall Mount (Optional)	DIN Rail (Default) Wall Mount (Optional)
Enclosure	IP40 Aluminum Case	IP40 Aluminum Case	IP40 Aluminum Case	IP40 Aluminum Case	IP40 Aluminum Case

## 1.1 Features

- Highly reliable and secure for mission-critical cellular communications
- Provide flexible options to configure LAN/ WAN ports
- Support multi-band connectivity with FDD LTE/ TDD LTE/ WCDMA/ GSM/ LTE Cat 4
- Built-in dual SIM for network redundancy
- Equipped with DI/DO and RS-232/RS-485 serial ports
- Integrated dual detachable antenna against radio interference
- LED indicators for connection and data transmission status
- A flexible input voltage range of 10-32V DC
- Industrial rated from -40°C to +75°C for use in harsh environments (SF301-TG/SF301-TPG)
- Metal Housing with IP40 Industrial grade protection
- IPv6/IPv4 dual stack and all applications are IPv6 ready
- Support various serial communication protocols for connectivity

- Enhance security and encryption for authentication and transmission

## 1.2 Specifications

### LTE Interface

- FDD LTE: B1/B3/B5/B7/B8/B20
- TDD LTE: B38/B40/B41
- WCDMA: B1/B5/B8
- GSM: 900/1800 MHz
- LTE Cat 4

### Processor & I/O Interface

- High performance 528 MHz CPU with 512 Mbytes of DDR3 memory
- 2 x SIM Card Slots
- 1 x LAN 10/100 Mbps Ethernet port (SF300/SF300-G)
- 3 x LAN 10/100 Mbps Ethernet ports (SF301/SF301-G/SF301-TG/SF301-TPG)
- 1 x WAN 10/100 Mbps Ethernet port
- 1 x WAN 10/100 Mbps Ethernet port with IEEE 802.3at/af PoE PD (SF301-TPG)
- Reset Button
- Console: 1 x RS232 (9-pin Sub-D)
- 2 x SMA connectors for detachable LTE antenna
- 1 x GPS detachable antenna (SF300-G/SF301-G/SF301-TG/SF301-TPG)
- 1 x RS485 (D+/D-)
- 1 x RS232 (TXD/RXD)
- 2 x DI, 1 x DO (Alarm +/-)

### Physical Characteristics

- Enclosure : Metal Shell, IP40 Protection
- Weight :
  - 451 g (SF300/SF300-G)
  - 452 g (SF301/SF301-G/SF301-TG/SF301-TPG)
- Dimensions (W x H x D) : 60 x 110 x 106 mm
- Installation : DIN Rail (Default) or Wall Mount (Optional)

### LED Display

- 1 x System status LED (Green)
- 1 x VPN status LED (Green)
- 1 x SIM1 status LED (Green)
- 1 x SIM2 status LED (Green)
- Ethernet status LEDs (Green for LINK/ACT, Yellow for SPEED)
- 2 x Mobile connection strength LEDs (Green)

### Power Supply

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

### MTBF (mean time between failures)

- SF300/SF300-G: 155,899 hrs (MIL-HDBK-217-FN2)
- SF301/SF301-G/SF301-TG/SF301-TPG: 148,930 hrs (MIL-HDBK-217-FN2)

### Software

- **Network Protocols:**  
IPv4, IPv6, IPv4/IPv6 dual stack, DHCP server and client, PPPoE, Static IP, SNTP, GPS sync time, DNS Proxy, Modbus, VRRP, OSPF, Message Queue Telemetry Transport (MQTT Broker), BGP
- **Routing/Firewall:**  
NAT, Virtual Server, DMZ, MAC Filter, URL Filter, IP Filter, VLAN, Static Routing and RIP-1/2
- **VPN:**  
OpenVPN, IPSec (3DES, AES128, AES196, AES256, MD5, SHA-1, SHA256), GRE, PPTP, L2TP
- **Wireless Connectivity:**  
Two SIM for failover/ roaming over/ back up  
Two SIM data usage control  
Seamless multi WAN connections switch
- **Others:**  
DDNS, QoS, Virtual COM, UPnP
- **Alarm:**  
DI, DO, SMS, VPN/WAN Disconnect, SNMP Trap, E-mail

### Management Software

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

### Environment

- Operating Temperature -20 ~ +70°C (SF300/SF301/SF300-G/SF301-G)
- Operating Temperature -40 ~ +75°C (SF301-TG/SF301-TPG)
- Storage Temperature -40 ~ +85°C
- Ambient Relative Humidity 10 ~ 95% (non-condensing)
- Humidity 0 ~ 95% (non-condensing)

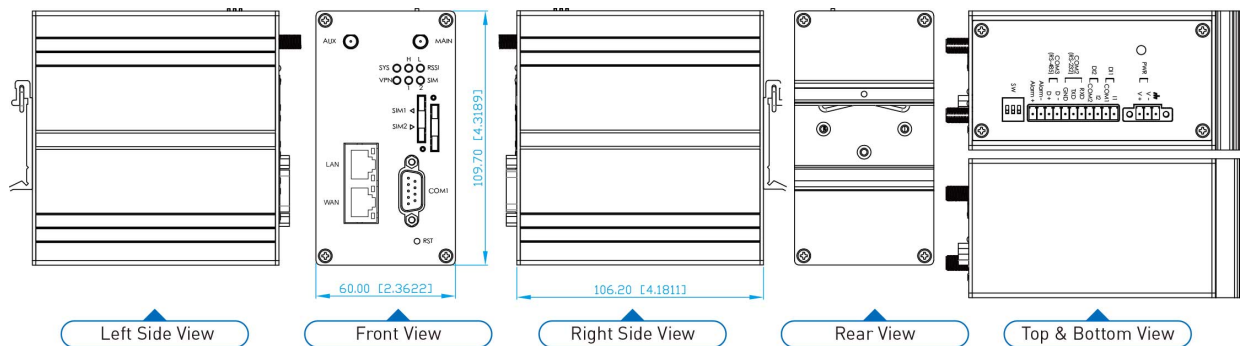
### Standards and Certifications

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

## 1.3 Mechanical Dimensions

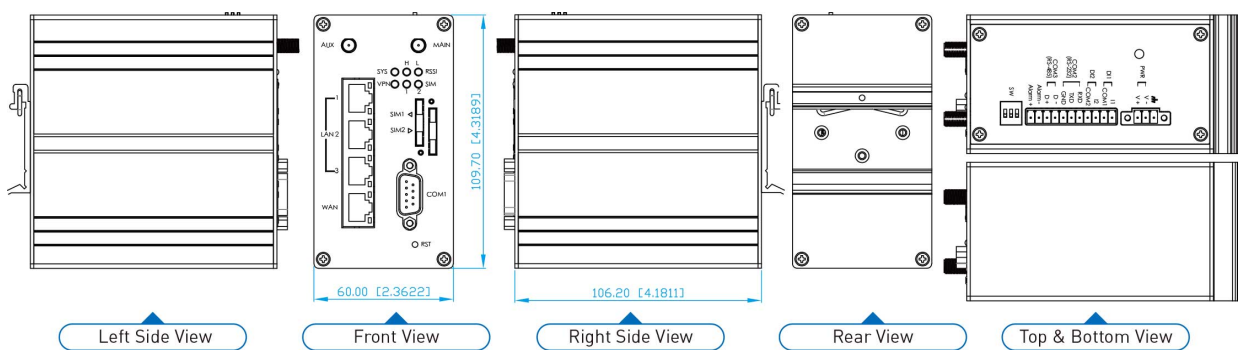
### (1) SF300 model :

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



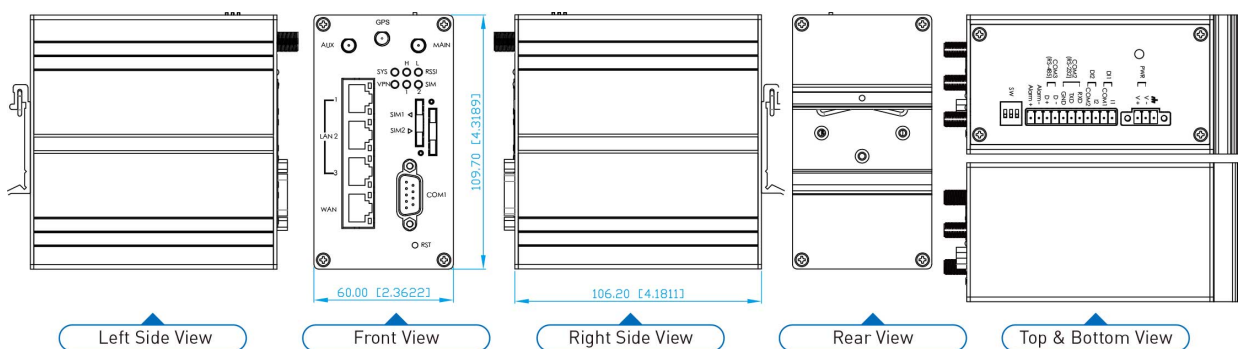
### (2) SF301 model :

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



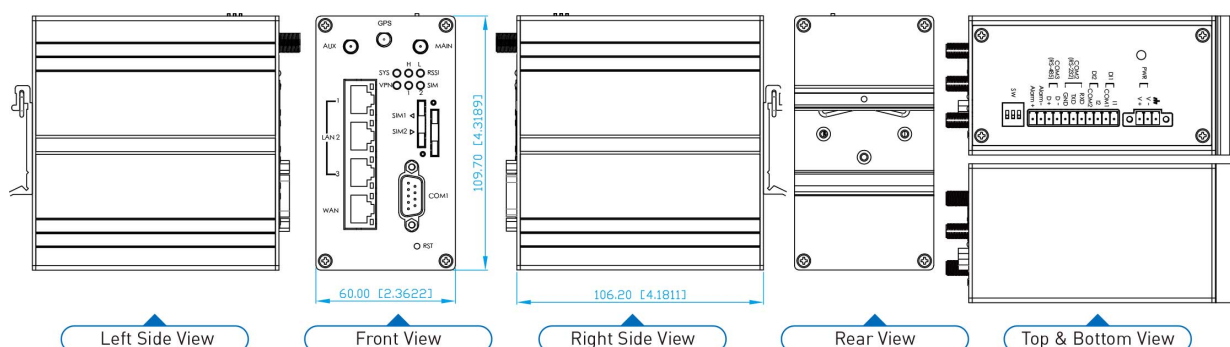
### (3) SF300-G model :

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

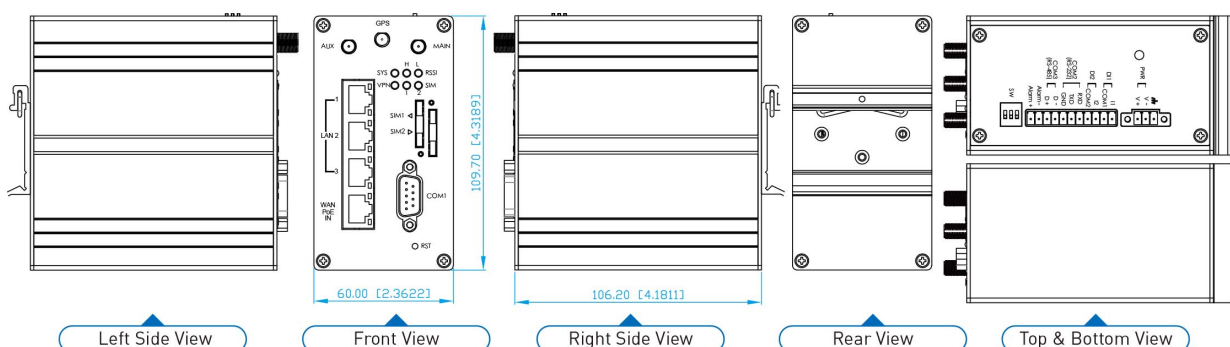


**(4) SF301-G / SF301-TG model :**

1 x WAN, 3 x LANs, 1 x GPS, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, -20 ~ +70°C (SF301-G), -40 ~ +75°C (SF301-TG)



**(5) SF301-TPG model :** 1 x WAN with IEEE 802.3at/af PoE PD, 3 x LANs, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, 1 x GPS, -40 ~ +75°C



## 1.4 Ordering Information

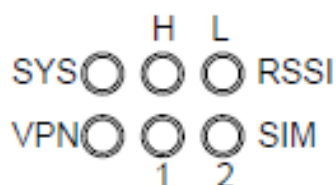
Model Name	Description
SF300	TeleWell INDUSTRIAL 4G LTE Cellular Router ( 1 x WAN, 1 x LAN, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, -20 ~ +70°C )
SF301	TeleWell INDUSTRIAL 4G LTE Cellular Router ( 1 x WAN, 3 x LANs, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, -20 ~ +70°C )
SF300-G	TeleWell INDUSTRIAL 4G LTE Cellular Router ( 1 x WAN, 1 x LAN, 1 x GPS, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, -20 ~ +70°C )
SF301-G	TeleWell INDUSTRIAL 4G LTE Cellular Router ( 1 x WAN, 3 x LANs, 1 x GPS, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, -20 ~ +70°C )
SF301-TG	TeleWell INDUSTRIAL 4G LTE Cellular Router ( 1 x WAN, 3 x LANs, 1 x GPS, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, -40 ~ +75°C )

SF301-TPG	TeleWell INDUSTRIAL 4G LTE Cellular Router ( 1 x WAN with IEEE 802.3at/af PoE PD, 3 x LANs, 2 x RS232, 1 x RS485, 2 x DI, 1 x DO, 2 x SIM Card Slots, 1 x GPS, -40 ~ +75°C )
-----------	---

## 2 Hardware Installation

This chapter introduces how to install and connect the hardware.

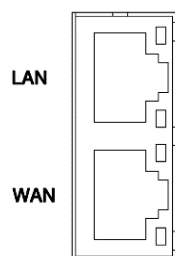
### 2.1 LED Indicators



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

### 2.2 Ethernet Port

#### (1) 10/100 Mbps Ethernet LAN/WAN (SF300/SF300-G model)

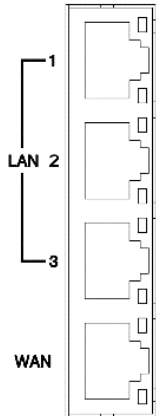


The LAN and WAN interface are standard RJ45 connectors.

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

<b>6</b>	WAN RX-	10/100 Mbps WAN, RX- Pin
<b>7</b>	N/A	N/A
<b>8</b>	N/A	N/A

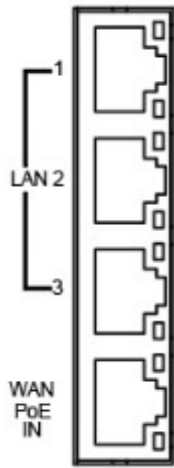
## (2) 10/100 Mbps Ethernet LAN1~LAN3/WAN (SF301/SF301-G/SF301-TG model)



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

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

## (3) 10/100 Mbps Ethernet LAN1~LAN3/WAN (SF301-TPG model)



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

#### (4) LED Indicator of Ethernet Port

Each Ethernet port has two LED indicators.

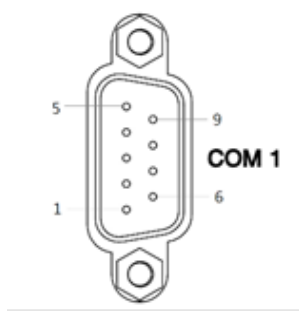
The Green LED indicates Link/ACT, and the Yellow LED indicates Speed.

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

### 2.3 Serial Port COM1 (Console-RS232)

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

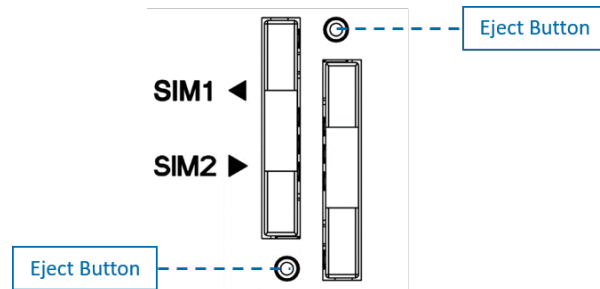




The serial port COM1 is a standard Sub-D connector.

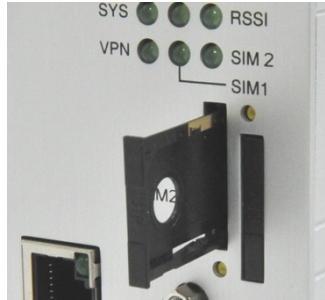
## 2.4 Install the SIM Card

### 1. SIM1/SIM2 Card Drawers and Eject Buttons

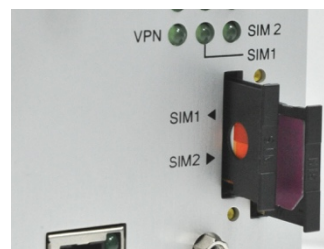


### 2. Insert and Remove SIM1/SIM2 Card

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



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



#### Note:

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

## 2.5 Reset Button



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

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

### Note:

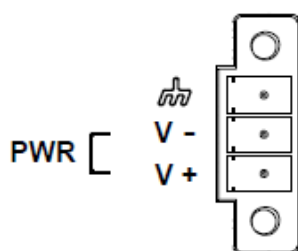
Press the Reset button and count the time around 5 seconds. The LED Indicators will be blinking to show you have activated the setting successfully.

## 2.6 External Antenna

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

## 2.7 Connecting the Power Supply

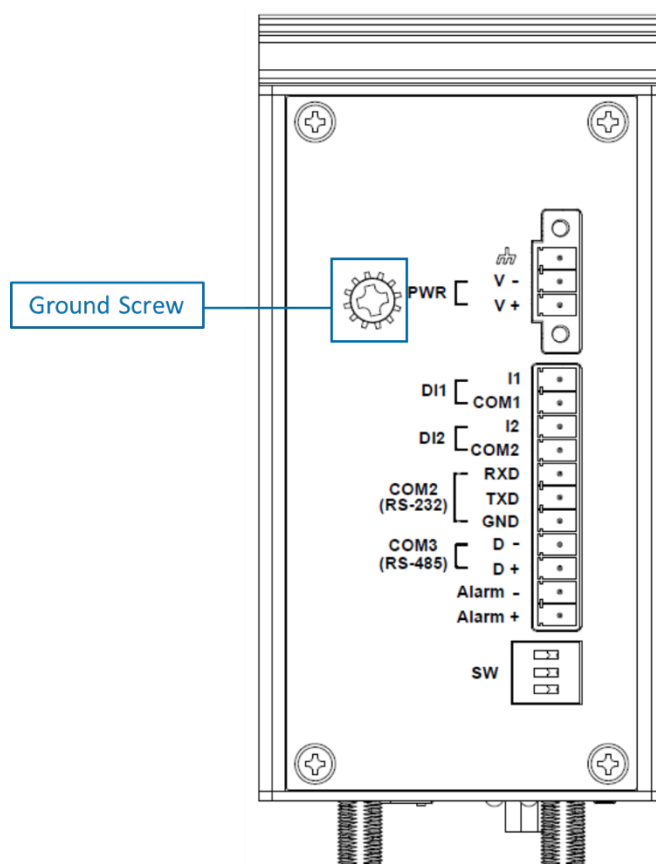
The router requires a DC power supply in the range of 10~32V DC. Please ensure all components are earthed to a common ground before connecting any wiring.



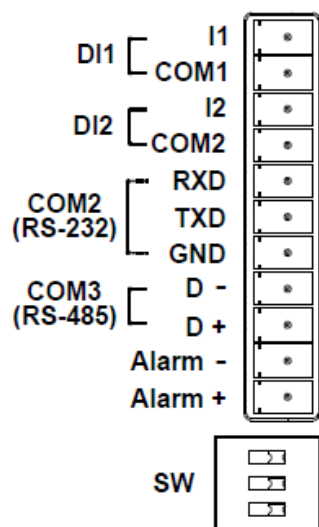
Pin	Power (10~32VDC)
	FRAME GROUND
V -	Negative
V+	Positive

## 2.8 Grounding the Router

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



## 2.9 Pin Assignments



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

## 2.10 Connecting I/O Ports

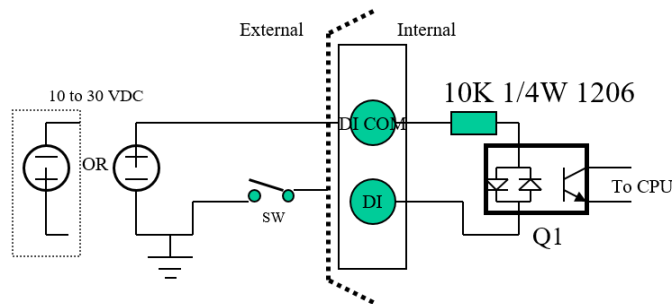
### (1) Digital Input DI1 & DI2

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

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

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

**Note:** Q1 is a bidirectional component.



Wet Contact

- Logic Level 1 : 10 to 30 VDC (Q1 On)
- Logic Level 0 : 0 to 3 VDC (Q1 Off)

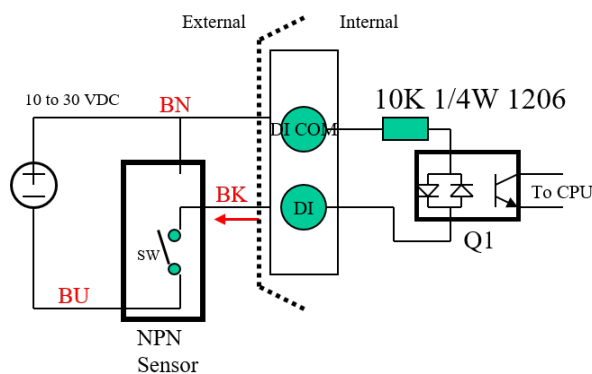
#### Digital Input

- Wet Contact (Level from DI to DI COM)
  - Logic Level 1 : 10 to 30 VDC (Q1 on)
  - Logic Level 0 : 0 to 3 VDC (Q1 off)

- Wet Contact (Alarm trigger\*):

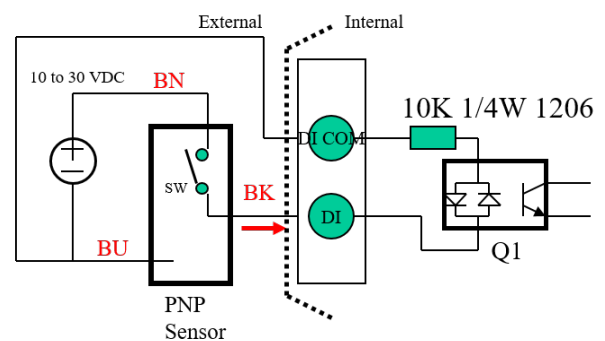
- Alarm ON\* : Q1 On (SW Close)
- Alarm Off\* : Q1 off (SW Open)

\* Refer to the Alarm function on web management  
\* Q1 is bi-directional part



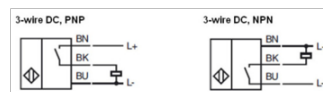
Wet Contact

- Alarm trigger\* : Q1 turn on
- Alarm un-trigger\* : Q1 turn off



Wet Contact

- Alarm trigger\* : Q1 turn on
- Alarm un-trigger\* : Q1 turn off

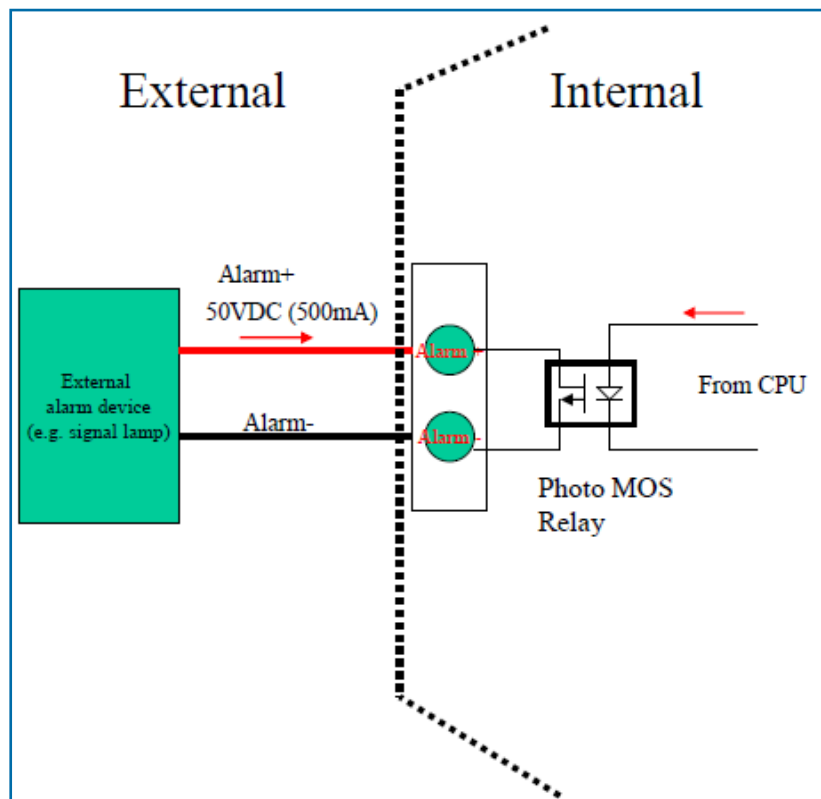


### (2) Digital Output – Alarm Contacts

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

Pin	Description
Alarm -	Alarm negative signal output

<b>Alarm +</b>	Alarm positive signal output
----------------	------------------------------



## 2.11 Serial Port COM2 (RS-232)

The serial port COM2 is a RS-232 interface.

Pin	Description
<b>RXD</b>	COM2 Serial Port, RXD Signal (INPUT)
<b>TXD</b>	COM2 Serial Port, TXD Signal (OUTPUT)
<b>GND</b>	COM2 Serial Port, Signal Ground ( ✕ )

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

## 2.12 Serial Port COM3 (RS-485)

The serial port COM3 is a RS-485 interface.

Pin	Description
<b>D -</b>	COM3 Serial Port, Data- (B) wire

<b>D +</b>	COM3 Serial Port, Data+ (A) wire
------------	----------------------------------

## 2.13 DIP Switch



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



DIP SWITCH

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

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

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

## 3 Configuration via Web Browser

### 3.1 Access the Web Configurator

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

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

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

#### Title Bar Panel > Selecting Language

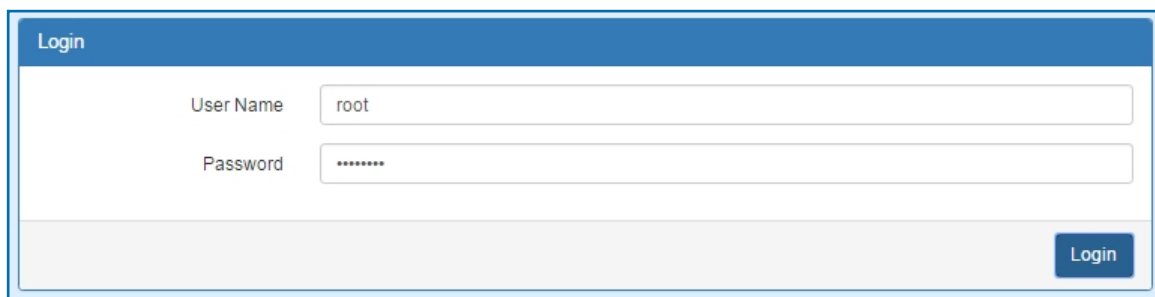
You can choose the languages, including English and Taiwan.



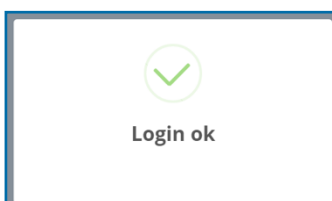
A language selection dropdown menu with the label 'Language' and the selected option 'English'.

#### 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 login form titled 'Login' with two input fields: 'User Name' containing 'root' and 'Password' containing masked characters (asterisks). A 'Login' button is located at the bottom right of the form.



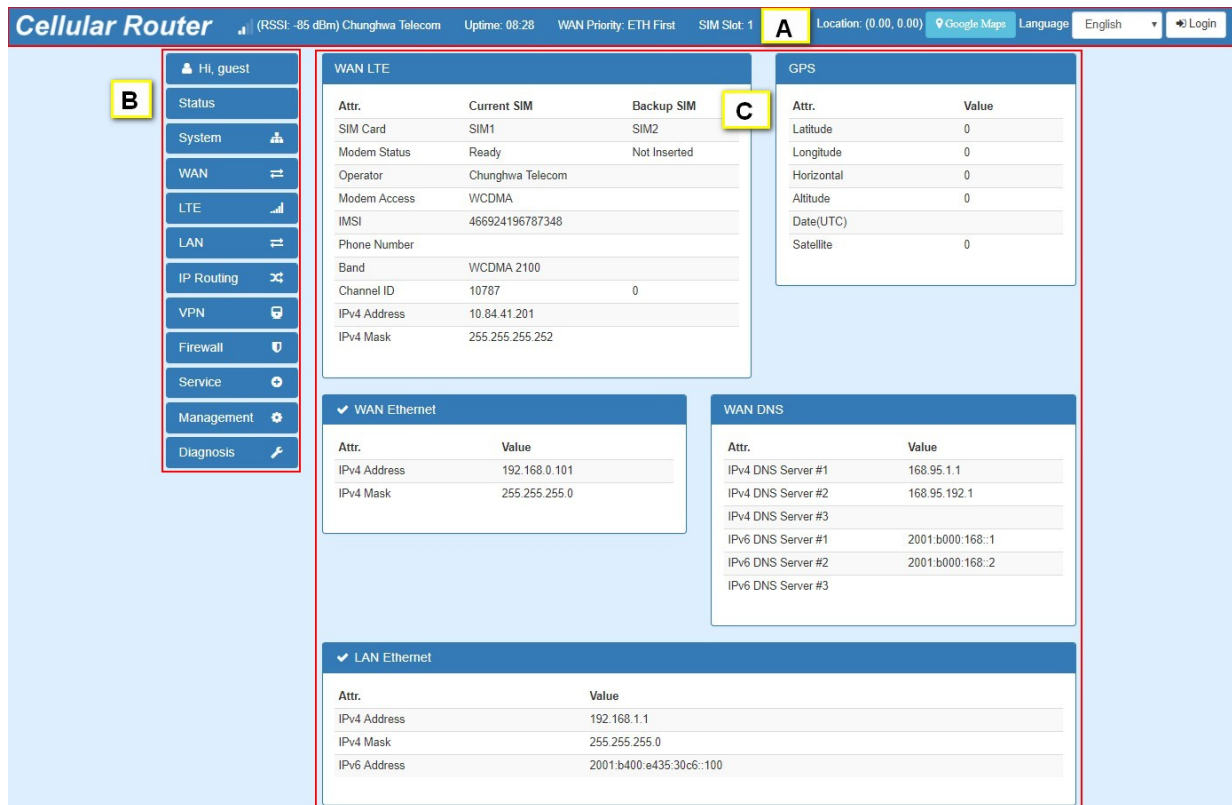
**Note:** After changing the User Name and Password, strongly recommend you to save them because another time when you login, the User Name and Password have to be used the new one you changed.



## 3.2 Navigate the Web Configurator

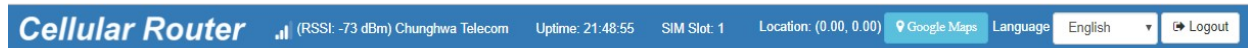
The main screen is divided into three parts as below.

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



(1) **A** : Title Bar

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



Title Bar	
Item	Description
<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>SIM Slot</b>	Show the current using of SIM Slot that inserts into SIM1 or SIM2.
<b>Language</b>	Choose your language from the drop-down list on the upper right corner of the title bar.
<b>Location</b>	Show the position of router from Google Maps. <b>Note:</b> This function is for GPS spec.
<b>Login/Logout</b>	Click to log in or log out of the web configurator.

(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 show the information or setting fields from main menu and sub menu.

## 4 Status

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

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

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

Cellular Router

(RSSI: -85 dBm) ChungHwa Telecom Uptime: 08:28 WAN Priority: ETH First SIM Slot: 1 Location: (0.00, 0.00) Google Maps Language English Login

Hi, guest

Status

System

WAN

LTE

LAN

IP Routing

VPN

Firewall

Service

Management

Diagnosis

WAN LTE

Attr.	Current SIM	Backup SIM
SIM Card	SIM1	SIM2
Modem Status	Ready	Not Inserted
Operator	Chunghwa Telecom	
Modem Access	WCDMA	
IMSI	466924196787348	
Phone Number		
Band	WCDMA 2100	
Channel ID	10787	0
IPv4 Address	10.84.41.201	
IPv4 Mask	255.255.255.252	

GPS

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

WAN Ethernet

Attr.	Value
IPv4 Address	192.168.0.101
IPv4 Mask	255.255.255.0

WAN DNS

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

LAN Ethernet

Attr.	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	2001:b400:e435:30c6::100

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

Status > WAN Ethernet	
Item	Description
<b>Attribute</b>	
<b>IPv4 Address</b>	Ethernet WAN obtain IPv4 Address.
<b>IPv4 Mask</b>	Ethernet WAN obtain IPv4 Mask.

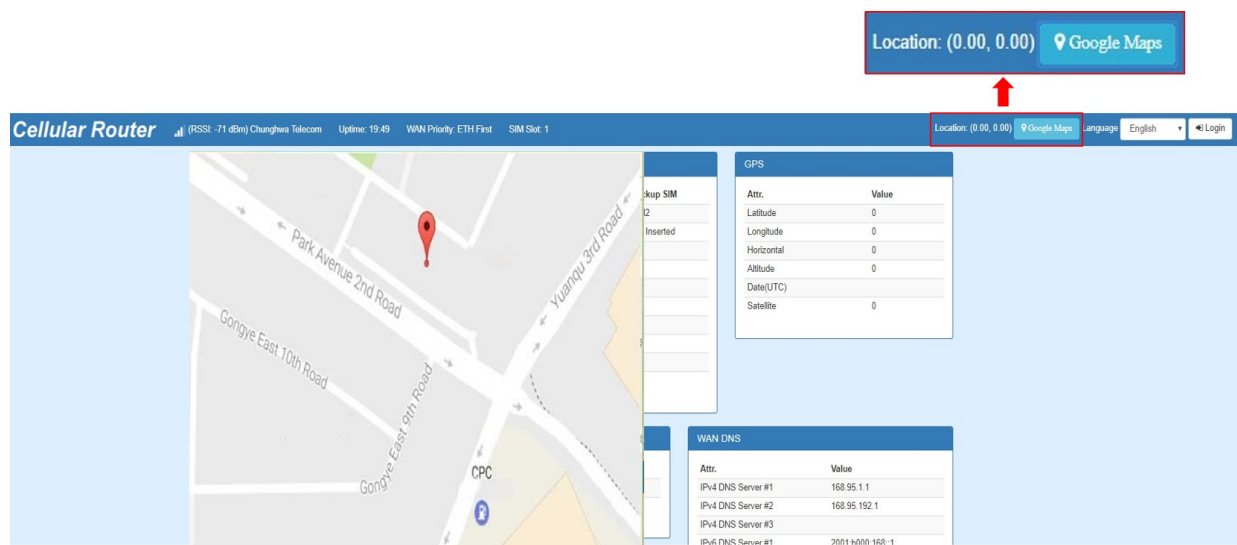
Status > WAN DNS	
Item	Description
<b>Attribute</b>	
<b>IPv4 DNS Server #1</b>	Show the address of IPv4 DNS Server #1.
<b>IPv4 DNS Server #2</b>	Show the address of IPv4 DNS Server #2.
<b>IPv4 DNS Server #3</b>	Show the address of IPv4 DNS Server #3.
<b>IPv6 DNS Server #1</b>	Show the address of IPv6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

Status > LAN Ethernet	
Item	Description
<b>Attribute</b>	
<b>IPv4 Address</b>	Ethernet LAN is assigned IPv4 Address.
<b>IPv4 Mask</b>	Ethernet LAN is assigned IPv4 Mask.
<b>IPv6 Address</b>	Ethernet LAN is assigned IPv6 Address.

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.

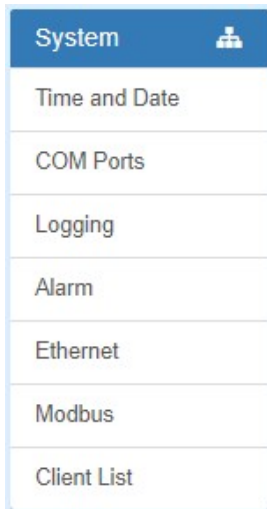
## 4.1 Status > GPS

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



## 5 Configuration > System

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



### 5.1 System > Time and Date


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

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

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

#### I. Get from Time Server

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

 Time And Date

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

Time and Date Setup

Mode    ☐ Manual    ☒ Get from Time Server

GPS Time    ☐ Off    ☒ On

IPv4 Server #1

IPv4 Server #2

IPv4 Server #3

IPv6 Server #1

IPv6 Server #2

IPv6 Server #3

Time Zone Setup

Time Zone

Daylight Savings    ☒ Off    ☐ On

Ahead of standard time        mins

Start Date     /  /     (Month / Week / Day)

Start Time     :     (Hour : Minute)


End Date     /  /     (Month / Week / Day)

End Time     :     (Hour : Minute)

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    Dec 4, 2017 10:20:54 AM

---

### Time and Date Setup

Mode    ☒ Manual    ☐ Get from Time Server

GPS Time    ☐ Off    ☒ On

YYYY-MM-DD     -  -      :  :   
 HH:MM:SS

---

### Time Zone Setup

Time Zone     ▼

Daylight Savings    ☒ Off    ☐ On

Ahead of standard time        mins

Start Date     /  /     (Month / Week / Day)

Start Time     :     (Hour : Minute)

End Date     /  /     (Month / Week / Day)

End Time     :     (Hour : Minute)

### III. Time Zone Setup

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

## Time Zone Setup

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

Daylight Savings ☐ Off ☒ On

Ahead of standard time 60 mins

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

Start Time 2 : 0 (Hour : Minute)

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

End Time 2 : 0 (Hour : Minute)

Apply



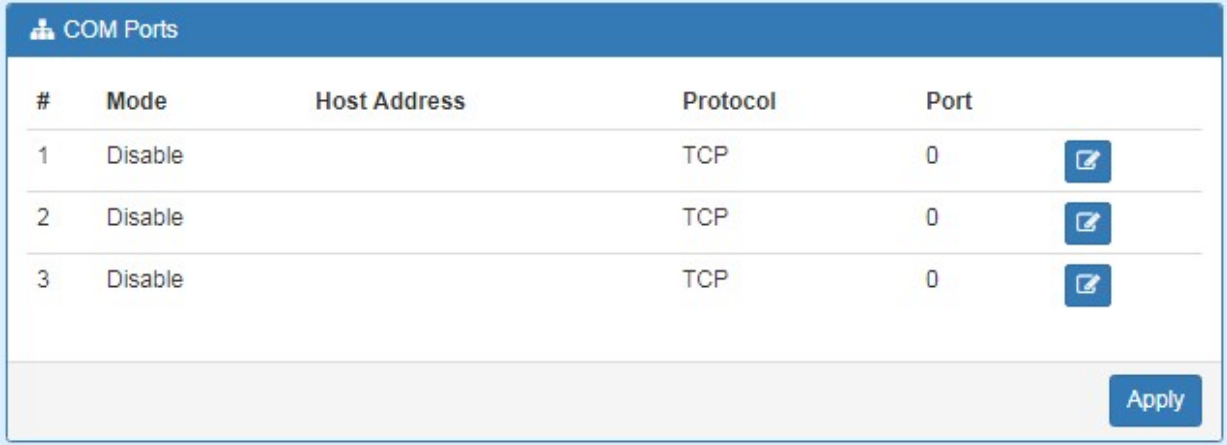
System > Time and Date->Daylight Savings	
Item	Description
<b>Daylight Saving</b>	Turn on/off the Daylight Savings feature. Select from Off or On. The default is Off.
<b>Ahead of standard time</b>	The forward/backward minutes when enter/leave Daylight Savings duration.Default is 60 mins.
<b>Start Date/Start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

## 5.2 System > COM Ports




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

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

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

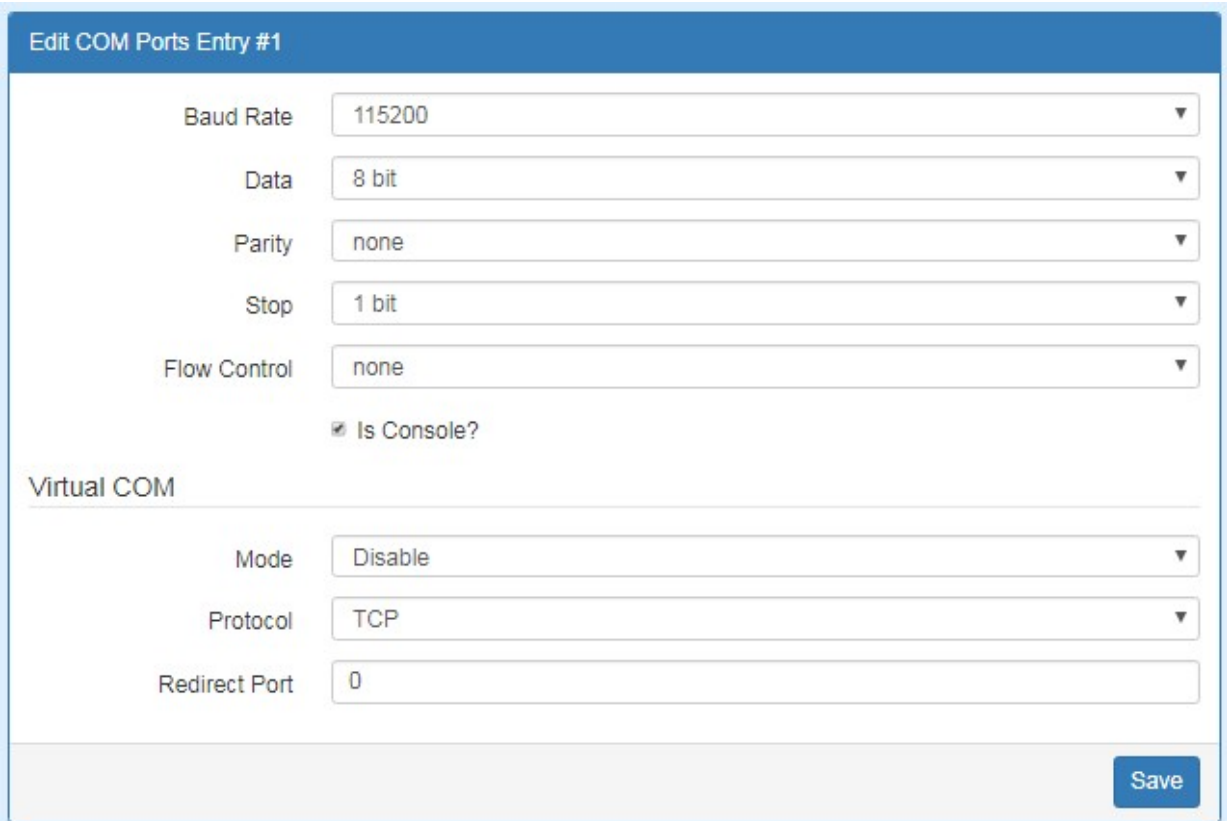


The screenshot shows a table titled "COM Ports" with the following columns: #, Mode, Host Address, Protocol, and Port. There are three rows, all with Mode set to "Disable", Protocol set to "TCP", and Port set to "0". Each row has an edit icon (a square with a pencil) to its right. At the bottom right of the table is an "Apply" button.

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

Apply

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



The screenshot shows the "Edit COM Ports Entry #1" configuration form. It has two main sections: "Serial" and "Virtual COM".

**Serial Section:**

- Baud Rate: 115200
- Data: 8 bit
- Parity: none
- Stop: 1 bit
- Flow Control: none
- ☒ Is Console?

**Virtual COM Section:**

- Mode: Disable
- Protocol: TCP
- Redirect Port: 0

At the bottom right is a "Save" button.

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

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

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

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

System > COM Ports	
Item	Description
<b>Edit Configuration</b>	
<b>Baud Rate</b>	Select from the current Baud Rate.
<b>Data</b>	Select from 7 bit or 8 bit.
<b>Parity</b>	Select from the information of Parity.
<b>Stop</b>	Select from 1 bit or 2 bit.
<b>Flow Control</b>	Select from none, Xon/Xoff or hardware.
<b>Virtual COM</b>	
<b>Mode</b>	Select from Disable, Server or Client.
<b>Protocol</b>	Select from TCP or UDP.
<b>Host Address</b>	The host address is only available on client mode. Specify what the domain name or IP address (IPv4 or IPv6) to be connected.
<b>Redirect Port</b>	<ul style="list-style-type: none"> <li>Server Mode: This network package of cellular router is on this port.</li> <li>Client Mode: The network package of remote device is on the remote host.</li> </ul>

## 5.3 System > Logging

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

**Logging**

Mode ☐ Disable ☒ Enable

Remote Log ☒ Disable ☐ Enable

Log Server Address: 255.255.255.255

Apply

**Log**

filter [ ] Clear Refresh Download Logs

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

### 5.3.1 Logging > Logging

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

**Logging**

Mode ☐ Disable ☒ Enable

Remote Log ☒ Disable ☐ Enable

Log Server Address: 255.255.255.255

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.)

### 5.3.2 Logging > Log

This section displays all data status.

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

The screenshot shows a web interface for logging. At the top, there's a blue header with a user icon and the word 'Log'. Below this, there's a search bar labeled 'filter'. To the right of the search bar are three buttons: 'Clear', 'Refresh', and 'Download Logs' (which has a download icon). Below these elements is a table with five columns: '#', 'Date', 'Group', 'Module', and 'Message'.

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

## 5.4 System > Alarm

This section allows you to configure the alarm.

Alarm

Mode ☒ Disable ☐ Enable

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

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

DI 1 Trigger ☒ High ☐ Low

DI 2 Trigger ☒ High ☐ Low

DO behavior ☒ Always ☐ Pulse

Groups

SMS/E-mail

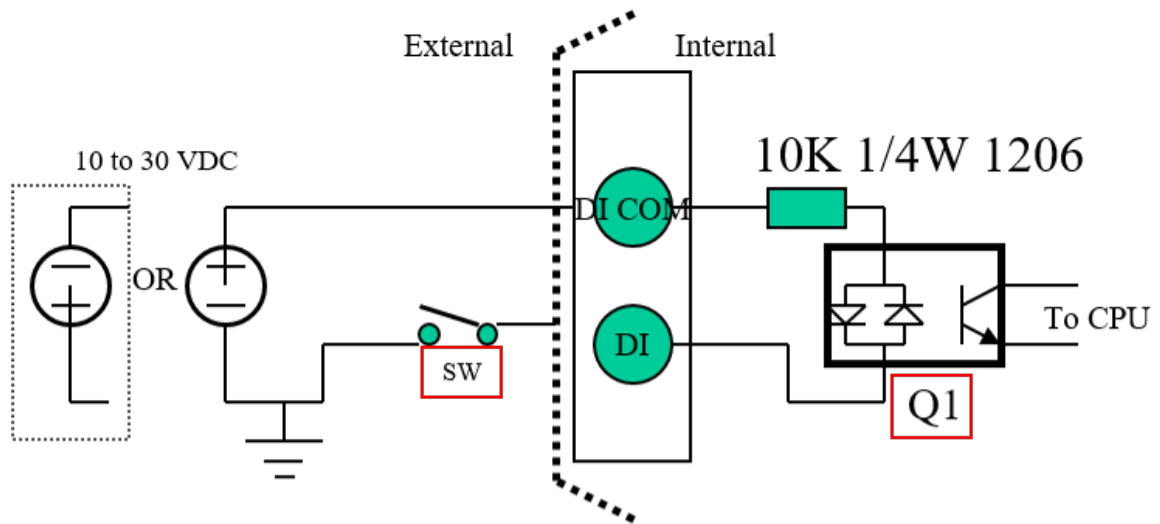
Group

Name	SUN	MON	TUE	WED	THU	FRI	SAT
Office1		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply

### Note:

- (1) If you select **SNMP trap** in Alarm output, you need to set up SNMP trap configuration from Service SNMP.
- (2) DI trigger "High" means High Trigger. (SW is On to trigger;SW is OFF in Normal state.)
- (3) DI trigger "Low" means Low Trigger. (SW is OFF to trigger;SW is ON in Normal state.)

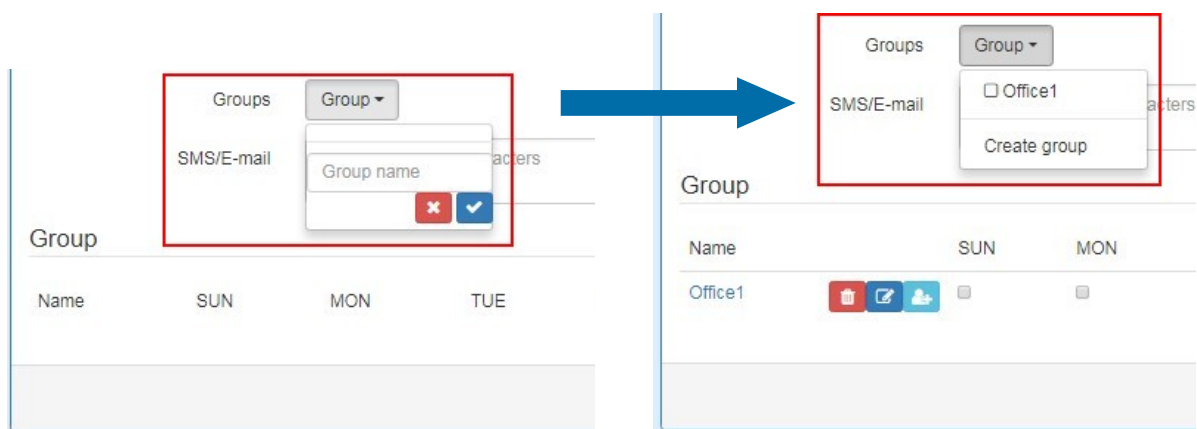


System > Alarm	
Item	Description
Mode	Turn on/off the Alarm configuration. Select from Disable or Enable. The default is Enable.
Alarm Input	Select from SMS, DI 1, DI 2, VPN disconnect and WAN disconnect as input to trigger alarm. <ul style="list-style-type: none"> <li>• <b>SMS:</b> It means team members on selected week day can send SMS to the phone number of using SIM card to trigger alarm.</li> <li>• <b>DI 1/2:</b> IO high 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> </ul>
Alarm Output	Select from SMS, DO, SNMP trap and E-mail as alarm output.
DI 1 Trigger	Select from High or Low. The default is High Trigger. <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>
DI 2 Trigger	Select from High or Low. The default is High Trigger.
DO behavior	<ul style="list-style-type: none"> <li>• <b>Always:</b> Pull DO high.</li> <li>• <b>Pulse:</b> High and Low continuously.</li> </ul>
Groups	Create your contact phone book for each group and edit your information for each user.
SMS/E-mail	Write your messages and the messages limit 150 English characters to deliver.

#### 5.4.1 Alarm > Name Group

##### (1) How to create your group

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





Groups Group ▾

SMS/E-mail acters

Group

Name

Office1

✖ ✎ 👤

	SUN	MON	TUE	WED	THU	FRI	SAT
Office1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply

## 5.4.2 Alarm > Edit User


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

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

Group

Name	SUN	MON	TUE	WED	THU	FRI	SAT
Office1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply

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

**User** ✕

Name

Phone

E-mail




Groups 👤 ▾

☒ Office1

✓


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


Group

Name	SUN	MON	TUE	WED	THU	FRI	SAT
Office1	  	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>


[Apply](#)


↓


User 

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

[Back](#) [Apply](#)

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


User 

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

[Back](#) [Apply](#)

## 5.5 System > Ethernet

This section allows you to configure the Ethernet.

 Ethernet

### Ethernet Ports Status

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

### Ethernet Ports Configurations

LAN 1	<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
LAN 2	<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
LAN 3	<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  min: 500; max: 1500


Refresh Apply

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

## 5.6 System > Modbus

This section allows you to configure the Modbus.

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

 Modbus

Mode ☐ Disable ☒ Enable

Port

Apply

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

## 5.7 System > Client List

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

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

Client List					
List Type		<input checked="" type="checkbox"/> DHCP Client	<input type="checkbox"/> Online		
#	IP Address	MAC Address	Hostname	Start	End
1	192.168.1.2	20:cf:30:69:b9:ac	ASUS-K42-NB	2017/12/04 10:20:47	2017/12/04 15:20:47

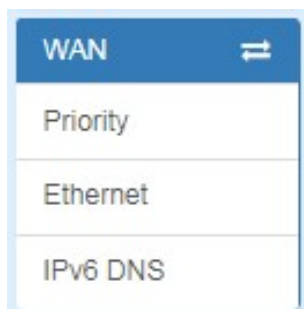
For **Online** type, the information shows IP address and MAC address when the client is online.

Client List		
List Type		<input type="checkbox"/> DHCP Client <input checked="" type="checkbox"/> Online
#	IP Address	MAC Address
1	192.168.1.2	20:cf:30:69:b9:ac

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.



### 6.1 WAN > Priority

You can set up the priority of WAN.



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

Status

System

WAN

Priority

Ethernet

IPv6 DNS

LTE

LAN

IP Routing

Service

Management

WAN Ethernet

Work As

☒ DHCP Client
 ☐ PPPoE Client
 ☐ Static IPv4

Configuration

Ethernet Ping Health

DNS Server Configuration

IPv4 DNS Server #1

From ISP

IPv4 DNS Server #2

From ISP

IPv4 DNS Server #3

From ISP

Apply

WAN > Ethernet	
Item	Description
WAN Ethernet	<p>There are three options to obtain the IP of WAN Ethernet.</p> <ul style="list-style-type: none"> <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

From ISP

IPv4 DNS Server #2

IPv4 DNS Server #3

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. Under 'Work As', 'PPPoE Client' is selected. The 'Configuration' tab is active, showing fields for 'User Name' (filled with 'test') and 'Password' (filled with asterisks). An 'Apply' button is at the bottom right.

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. Under 'Work As', 'Static IPv4' is selected. The 'Configuration' tab is active, showing fields for 'IP Address' (0.0.0.0), 'IP Mask' (255.255.255.0), and 'Gateway Address' (0.0.0.0). Below these is a 'DNS Server Configuration' section with three empty fields for 'IPv4 DNS Server #1', '#2', and '#3'. An 'Apply' button is at the bottom right.

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

### 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

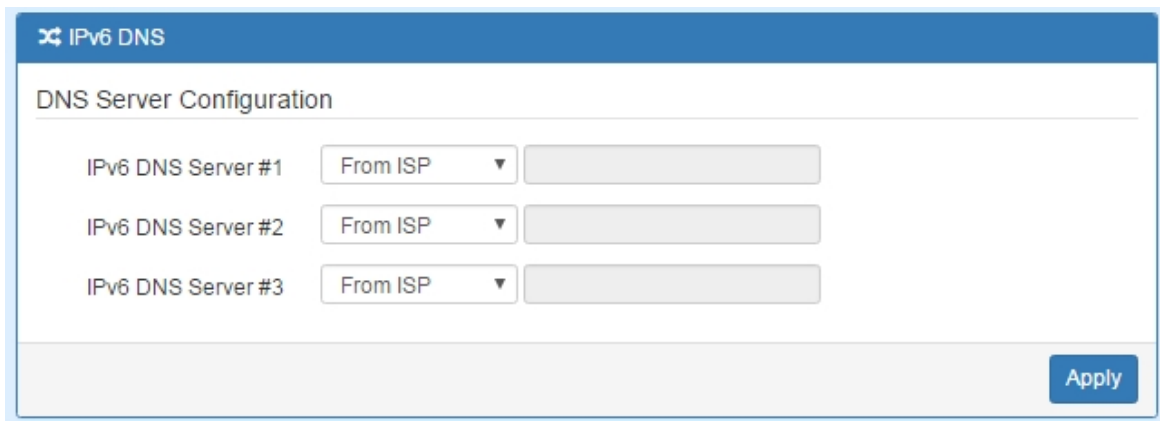
Attr.	Value
IPv4 Address	118.167.125.240
IPv4 Mask	255.255.255.255

✓ LAN Ethernet

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

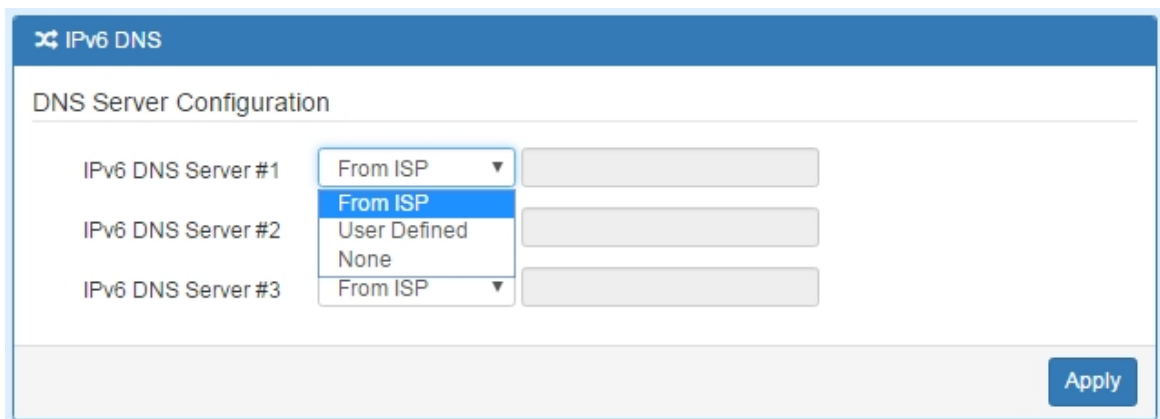
## 6.3 WAN > IPv6 DNS

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



The screenshot shows the 'IPv6 DNS' configuration page. At the top is a blue header with a router icon and the text 'IPv6 DNS'. Below the header is a section titled 'DNS Server Configuration'. It contains three rows, each for a DNS server. Each row has a label (IPv6 DNS Server #1, #2, #3), a dropdown menu currently set to 'From ISP', and an empty text input field for the IP address. At the bottom right of the configuration area is a blue 'Apply' button.

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.




This screenshot is similar to the previous one, but the dropdown menu for 'IPv6 DNS Server #1' is open. It shows three options: 'From ISP' (which is highlighted in blue), 'User Defined', and 'None'. The other two dropdown menus remain set to 'From ISP'.

WAN > IPv6 DNS	
Item	Description
DNS Server Configuration	
IPv6 DNS Server #1 IPv6 DNS Server #2 IPv6 DNS Server #3	<ul style="list-style-type: none"><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 SIM, Usage Display, SMS, Engineer Info, and DNS.

LTE 
LTE Config
GPS Config
Dual SIM
Usage Display
SMS
Engineer Info
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

Lock LTE Band

Default Band

▼

Lock GSM/WCDMA Band

Default Band

▼

MTU

1500

min: 500; max: 1500

LTE Ping Health

LTE Ping Health

☐ Disable ☒ Enable

Interval

60

Seconds

IPv4 Host 1

www.google.com

IPv4 Host 2

www.yahoo.com

IPv6 Host 1

ipv6.google.com

IPv6 Host 2

www.ipv6.hinet.net

Hint

LTE ping health: Enable

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

Apply

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

The screenshot shows the 'LTE Config' section of a web interface. It features a dropdown menu labeled 'LTE Config' with the following options: 'Auto' (selected), '4G Only', '3G Only', and '2G Only'. To the right of the dropdown, a text label reads 'Change this field require rebooting'. Below the dropdown, there are labels for 'Lock LTE Band' and 'Lock GSM/WCDMA Band', each followed by a dropdown menu.

LTE > LTE Config	
Item	Description
<b>LTE Config</b>	<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>
<b>Lock LTE Band</b>	Configure specified LTE Band to lock.
<b>Lock GSM/WCDMA Band</b>	Configure specified GSM/WCDMA Band to lock.
<b>MTU</b>	MTU is the Maximum Transmission Unit that can be sent over the LTE interface. It allows user to adjust the MTU size to fit into their existing network environment.

### 7.1.2 LTE Ping Health

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

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

The screenshot displays the 'LTE Ping Health' configuration page. At the top, there are radio buttons for 'Disable' and 'Enable' (selected). Below this is an 'Interval' field set to '60' with the unit 'Seconds'. There are four input fields for hosts: 'IPv4 Host 1' (www.google.com), 'IPv4 Host 2' (www.yahoo.com), 'IPv6 Host 1' (ipv6.google.com), and 'IPv6 Host 2' (www.ipv6.hinet.net). A 'Hint' section at the bottom provides additional information: 'LTE ping health: Enable', followed by two bullet points explaining that it prevents the base station from kicking out the idle device and that it will switch SIM slots in 'Dual SIM' mode if a ping fails. An 'Apply' button is located at the bottom right.

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

## 7.2 LTE > GPS Config

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

GPS Config

Report To ☐ RS232 ☐ LOG

NMEA Type ☒ GSV ☒ GGA ☒ RMC ☒ GSA

Apply

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

GPS Config

Report To ☒ RS232 ☐ LOG

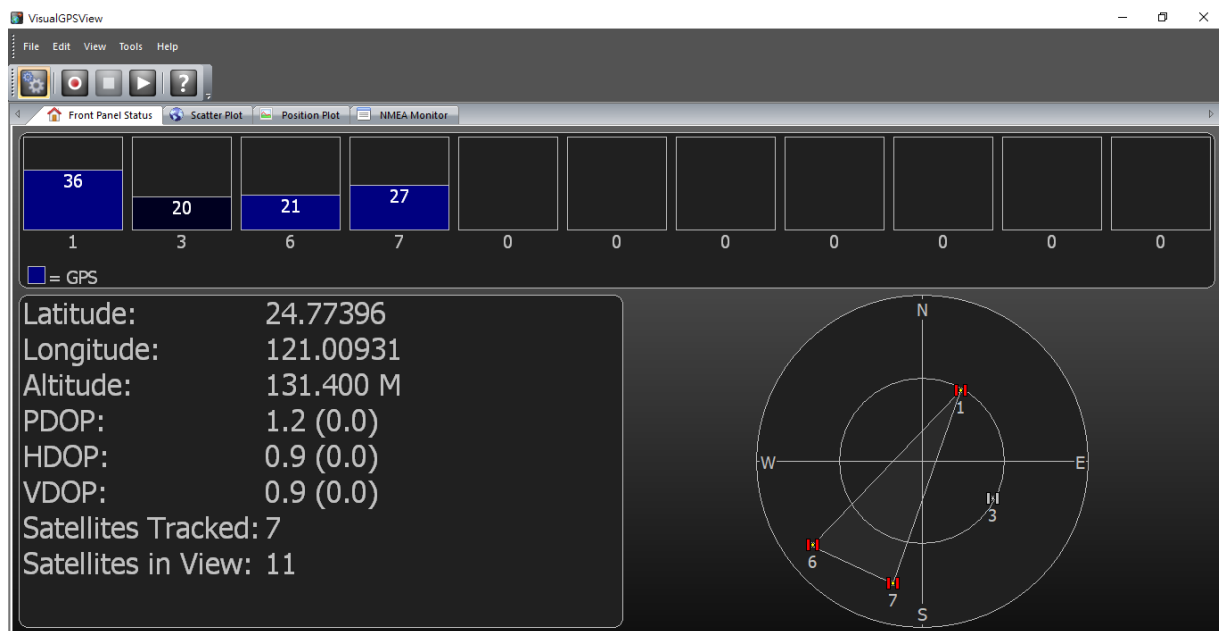
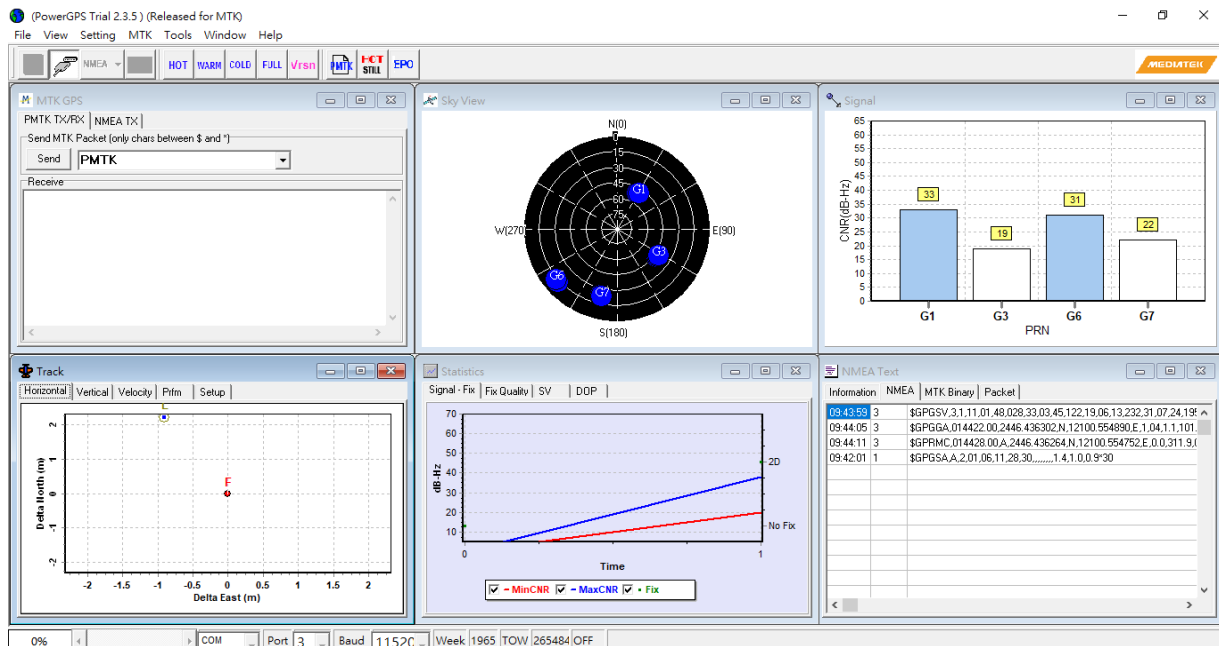
COM Port ☒ COM 1 ☐ COM 2

NMEA Type ☒ GSV ☒ GGA ☒ RMC ☒ GSA

Apply

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

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



## 7.3 LTE > Dual SIM

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

**Dual SIM**

**Connect Policy**

Current SIM Card: SIM1 [Disconnect](#)

Disable Roaming: ☐ No ☒ Yes

Used SIM: ☒ Dual SIM ☐ SIM1 ☐ SIM2

SIM Priority: ☐ Auto ☒ SIM1 ☐ SIM2

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

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

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

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

**Dual SIM**

**Connect Policy**

Current SIM Card: SIM1 [Disconnect](#)

Disable Roaming: ☐ No ☒ Yes

Used SIM: ☐ Dual SIM ☒ SIM1 ☐ SIM2

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

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

## Connect Policy

Current SIM Card SIM1

 DisconnectDisable Roaming ☐ No ☒ YesUsed SIM ☒ Dual SIM ☐ SIM1 ☐ SIM2SIM Priority ☐ Auto ☒ SIM1 ☐ SIM2Roaming Switch ☒ Switch to another SIM when roaming is detected

Connect Retry Number 3

(1 ~ 100) \* 60 seconds

✓ SIM1 Configurations

SIM2 Configurations

Status Ready

SIM PIN

Confirmed SIM PIN

SIM PUK

Confirmed SIM PUK

APN

Username


Password

Confirm Password

Auth

NONE

Change SIM PIN

 Change

## Data Limitation

Already Used Data (MB) 0

Mode ☒ Disable ☐ Enable

Max Data Limitation (MB)

0

Monthly Reset

Date: 31

▼

Hours: 23

Minutes: 0

Seconds: 0

Now Time

Date: 29

Hours: 8

Minutes: 1

Seconds: 54

Apply



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

Change SIM PIN

Change

Old PIN

New PIN

PIN Remaining Number

0

PUK Remaining Number

0

Apply

**Note:**

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

Dual SIM

Connect Policy

Current SIM Card

SIM1

Disconnect

Disable Roaming

☐ Disable
 ☒ Enable

Used SIM

☐ Dual SIM
 ☒ SIM1
 ☐ SIM2

☒ SIM1 Configurations
 ☐ SIM2 Configurations

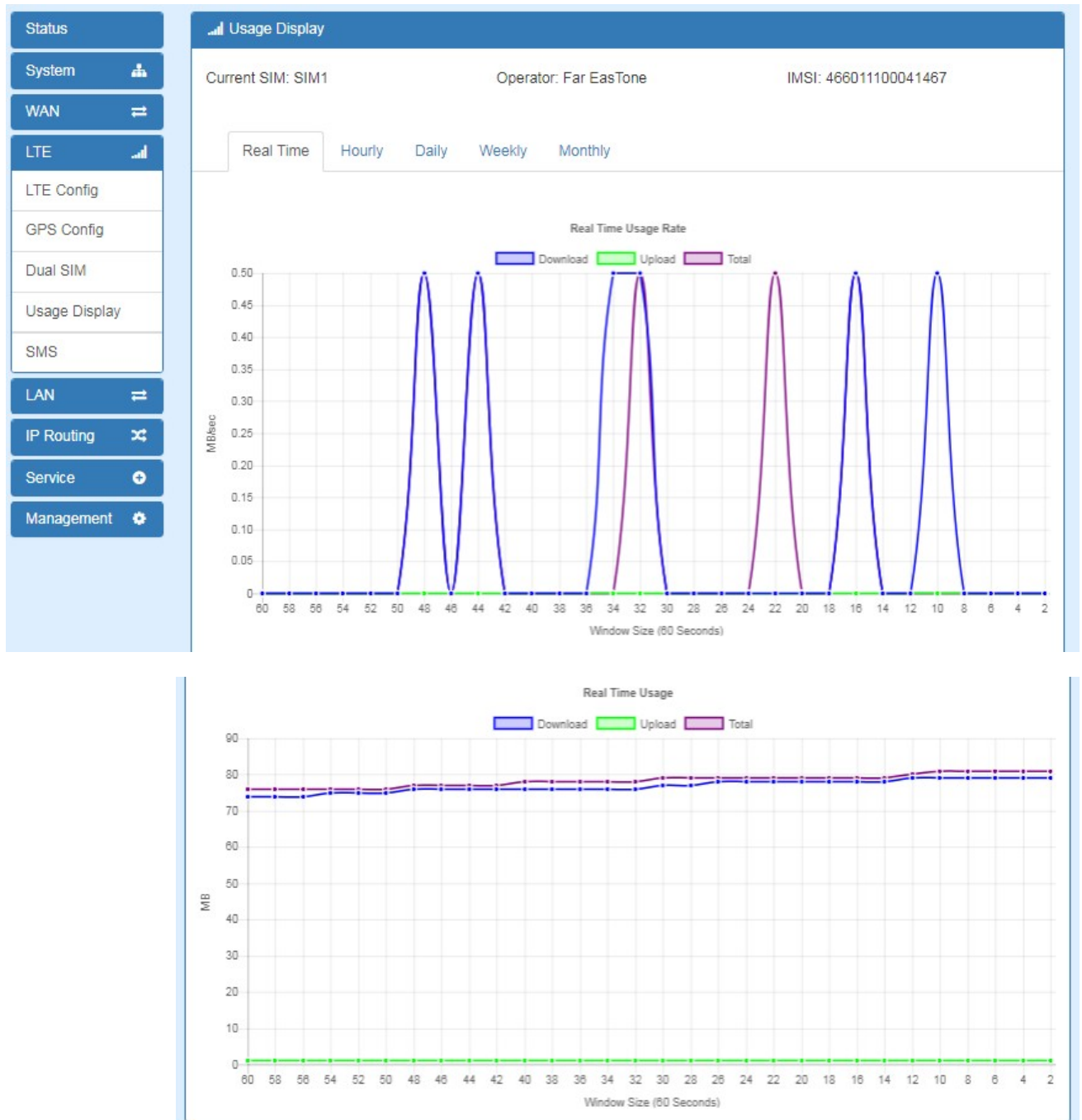
Status

Ready

LTE > Dual SIM	
Item	Description
<b>Connect Policy</b>	
Current SIM Card	Display which SIM slot is using.
Status of SIM Card Connectivity	<ul style="list-style-type: none"> <li>• <b>Connect:</b> After manually disconnect, user can only click <b>Connect</b> button to get connection or reboot the device to make it automatically connect.</li> <li>• <b>Disconnect:</b> If there is one SIM slot get 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>Disable:</b> SIM gets connection even it is in roaming state.</li> <li>• <b>Enable:</b> SIM would not get connection when in roaming state.</li> </ul>
Used SIM	Three options to show SIM Card's used status, including Dual SIM, SIM1 and SIM2.
SIM Priority	Three options to set the priority for SIM Card, including Auto, SIM1 and SIM2. To set up the first link SIM slot from Dual SIM mode with two SIM cards.
Roaming Switch	Switch to another SIM when roaming is detected. System will switch SIM slot when current SIM is in roaming state and another SIM slot is in READY state.
Connect Retry Number	After timeout, the router attempts to switch another SIM Slot. The default timeout is three minutes. This option is only for Dual SIM mode.
<b>SIM1 Configurations or SIM2 Configurations</b>	
Status	Display the status of Dual SIM.
SIM PIN	Configure PIN code to unlock SIM PIN.
Confirmed SIM PIN	Confirm PIN code.
SIM PUK	Fill in PUK to unlock SIM Card after typing more than 3 times.
Confirmed SIM PUK	Confirm SIM PUK.
APN	APN can be input by user or the system will search from internal database if APN is blank.
Username	The username can be input by user or the system will search from internal database if the username is blank.
Password	The password can be input by user or the system will search from internal database if the password is blank.
Confirm Password	Fill in your changed password.
Auth	Configure Authentication mode with three modes, including NONE, PAP, and CHAP. <ul style="list-style-type: none"> <li>• <b>Username:</b> If Auth is not NONE. Most server require username and password.</li> <li>• <b>Password:</b> If Auth is not NONE. Most server require username and password.</li> </ul>
Change SIM PIN	Change your old SIM PIN code into new SIM PIN code.
<b>Data Limitation</b>	
Mode	Turn on/off the Data Limitation to disable or enable.
Already Used Data (MB)	Display current used throughput since last reset.
Max Data Limitation (MB)	Configure max throughput.
Monthly Reset	Set up the reset time during the month.
Now Time	Show the current time of system.

## 7.4 LTE > Usage Display

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



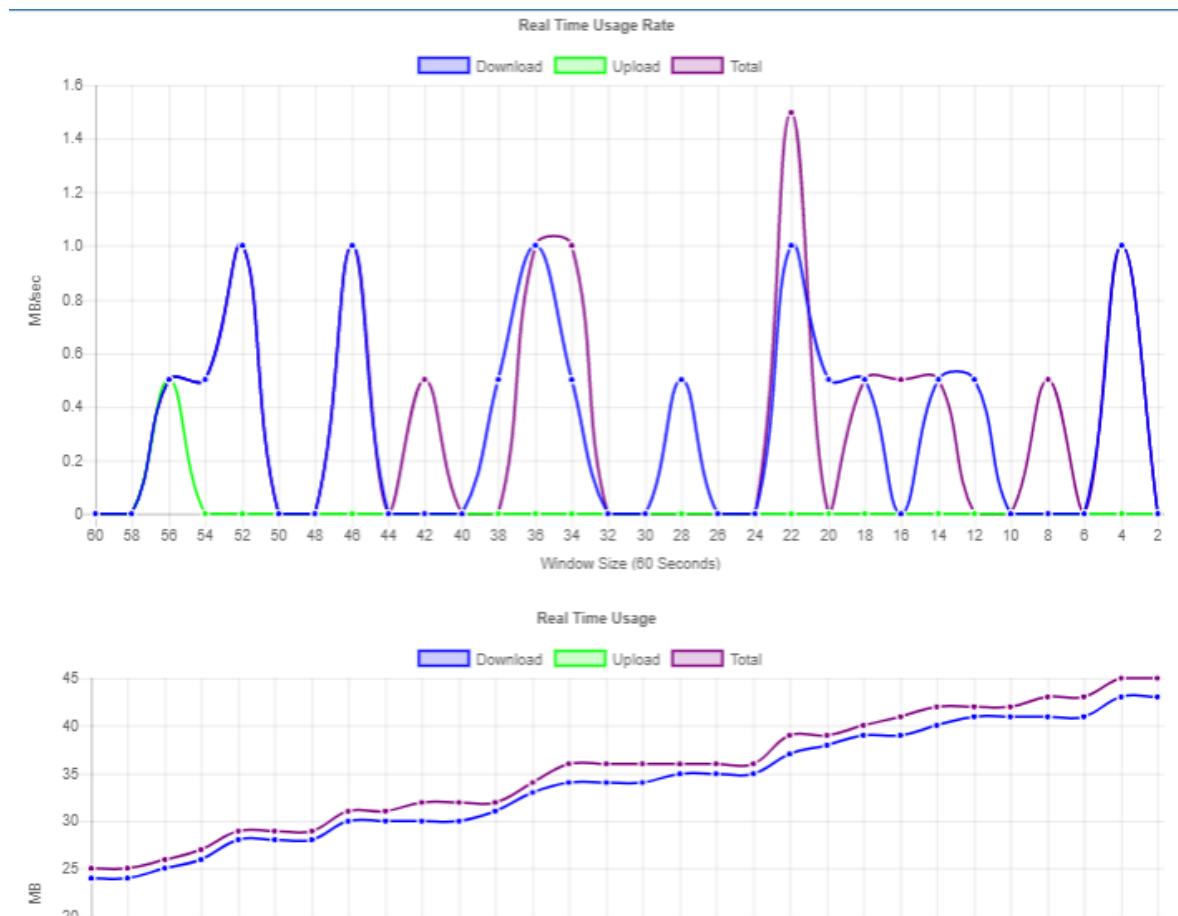
## (1) Real-Time Usage:

- **Real-Time Usage Rate:**

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

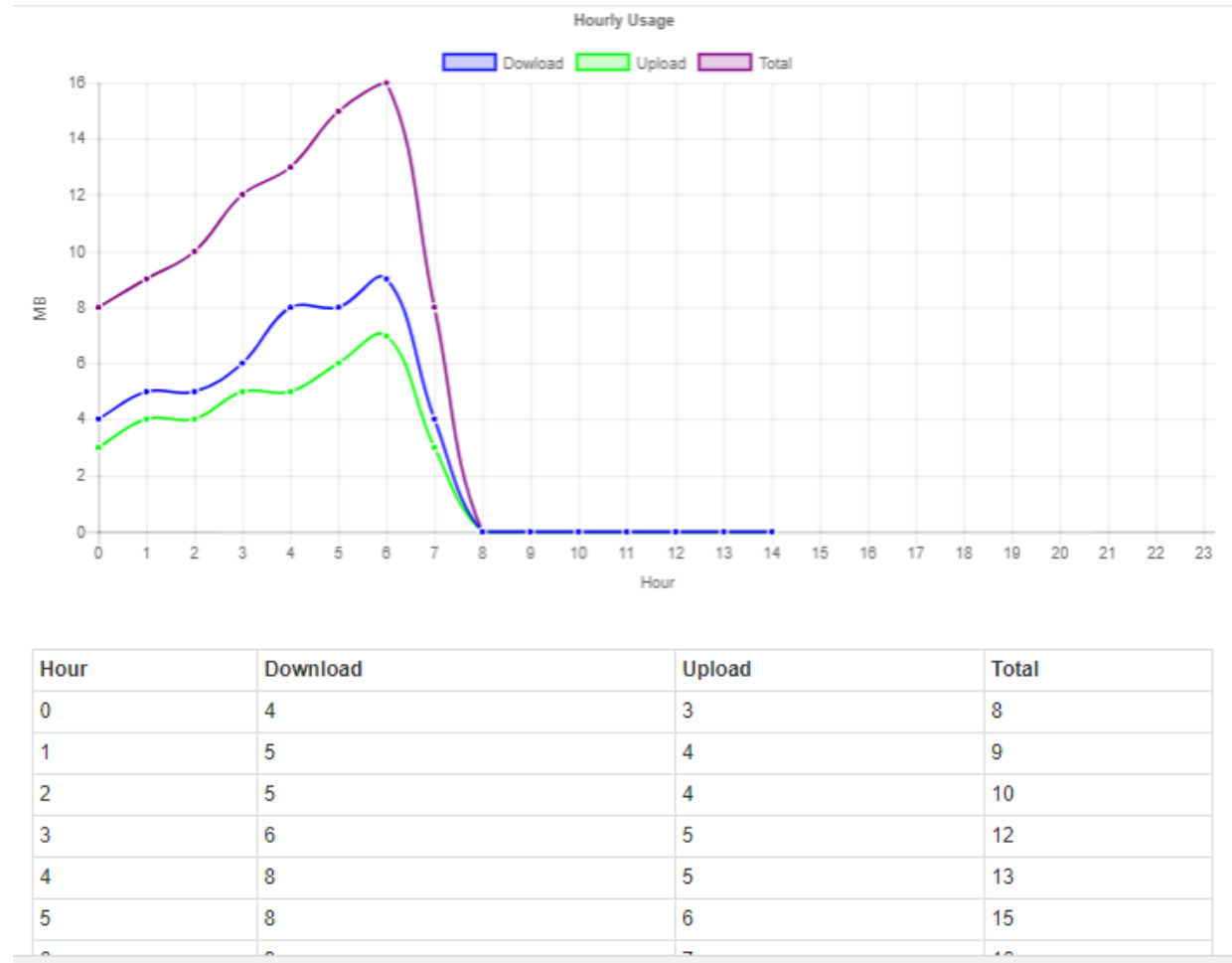
- **Real-Time Usage:**

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



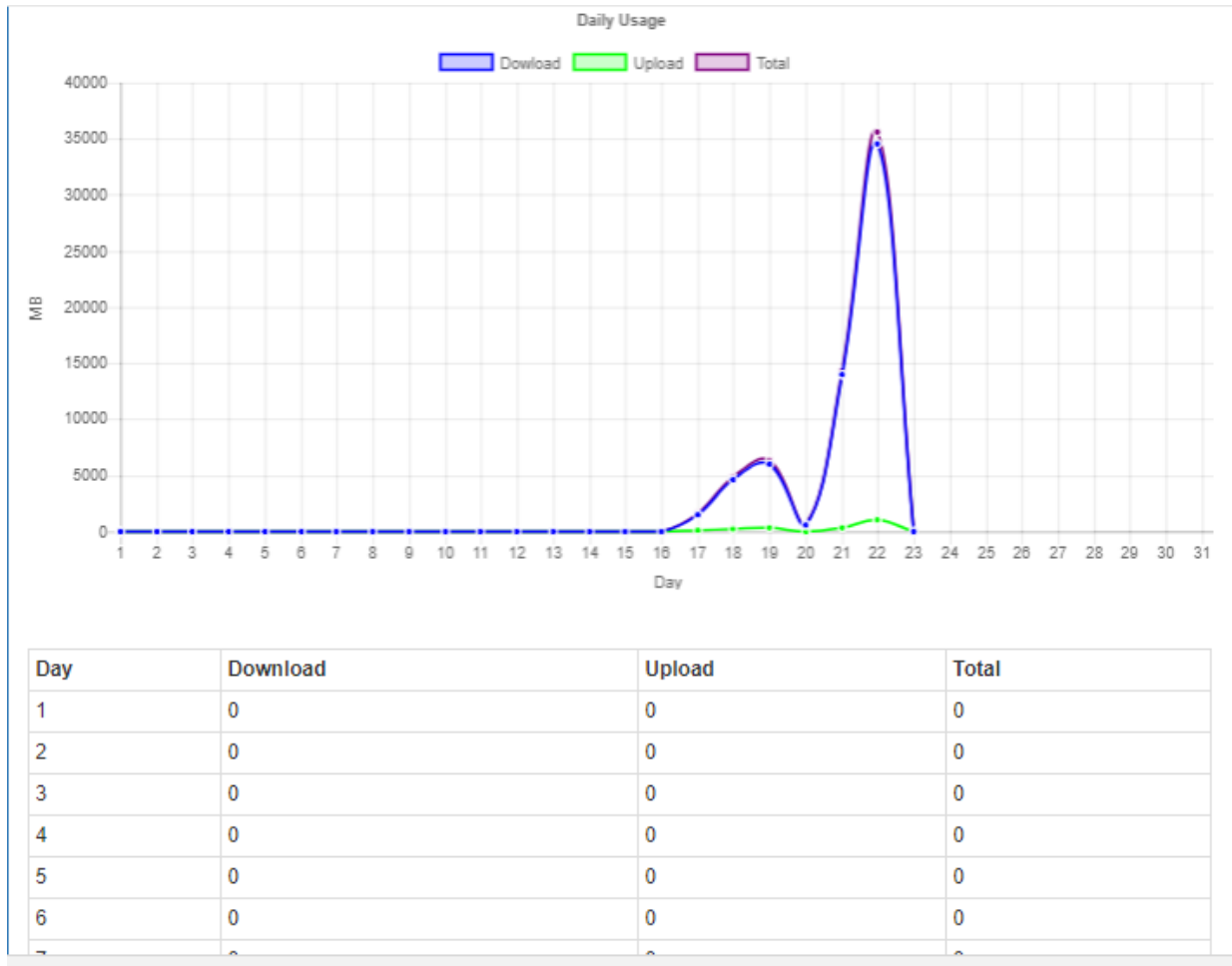
## (2) Hourly Usage:

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



### (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.



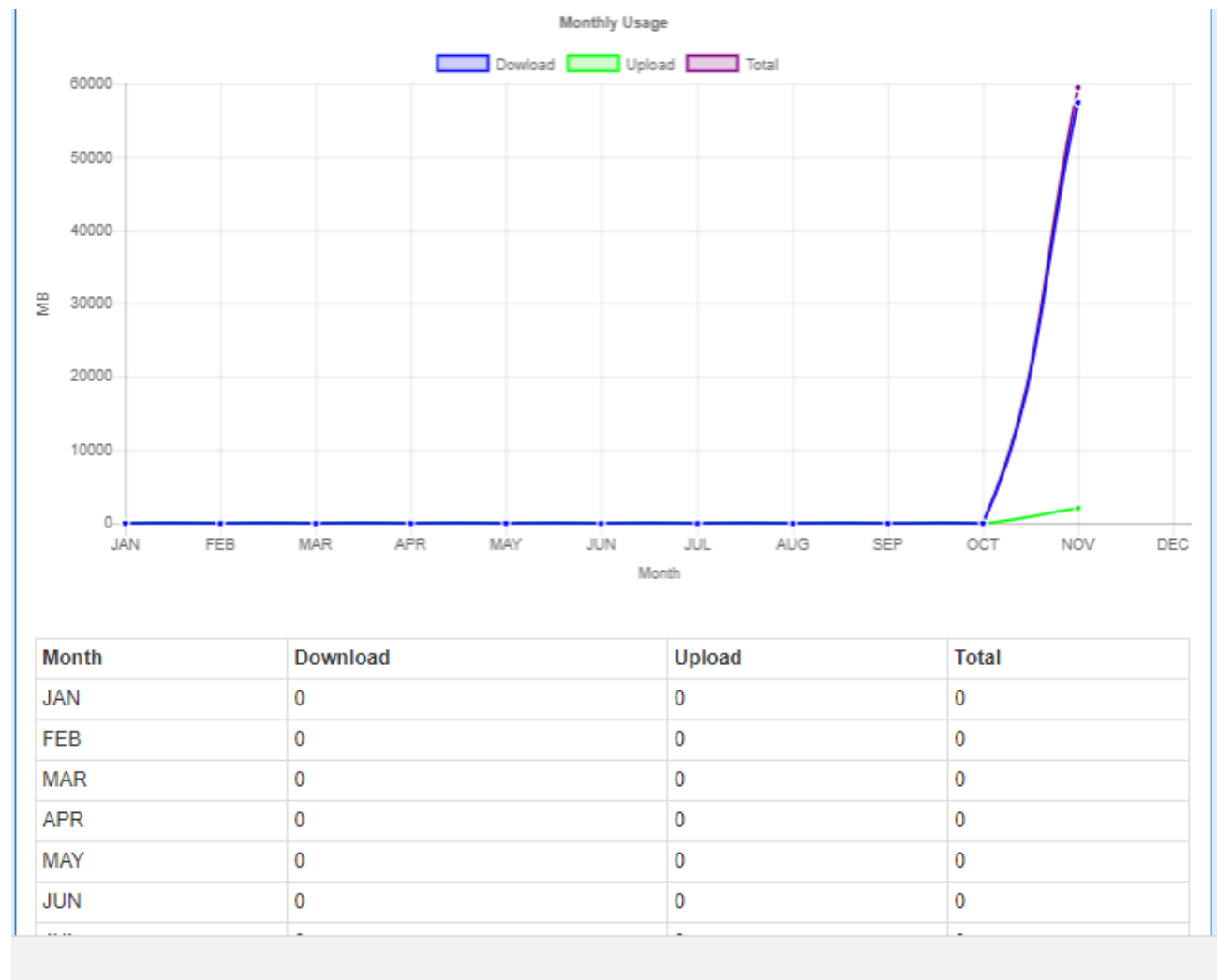
#### (4) Weekly Usage:

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 you by sending key words SMS to trigger device setting/action/query status.


The screenshot shows the 'SMS' configuration page with the 'SMS Action' tab selected. The 'Mode' is set to 'Enable'. The 'Actions and Keywords Setup' section contains a list of actions and their corresponding keywords, each with a text input field. The actions and keywords are:

Action	Keyword
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##

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

- (2) For **View SMS**, this section allows you to review the information of SMS that you have

received, including the state, phone and date and time. You can click  **view button** to review all messages.

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

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

005B906050B34F8696FB7B5492349AD49A575230671F901A77E5005D60A87684514D8CBB9AD49A575C0765BC003359295F8C5230671F002E4EFB610F937556DE8986672C7C218A0A621675

Close

## 7.6 LTE > Engineer Info

This section displays Engineer Information. RSRP, RSRQ, and SINR are for LTE connection. RSCP is for WCDMA connection.

Engineer Info	
Connect Mode	LTE
RSRP	-105
RSRQ	-10
SINR	13
RSCP	

## 7.7 LTE > DNS

This section allows you to setup LTE specific DNS setting.

 DNS

**DNS Server Configuration**

IPv4 DNS Server #1

From ISP

IPv4 DNS Server #2

From ISP

IPv4 DNS Server #3

From ISP

Apply

WAN > Ethernet > DHCP Client	
Item	Description
IPv4 DNS Server #1 IPv4 DNS Server #2 IPv4 DNS Server #3	<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>

## 8 Configuration > LAN

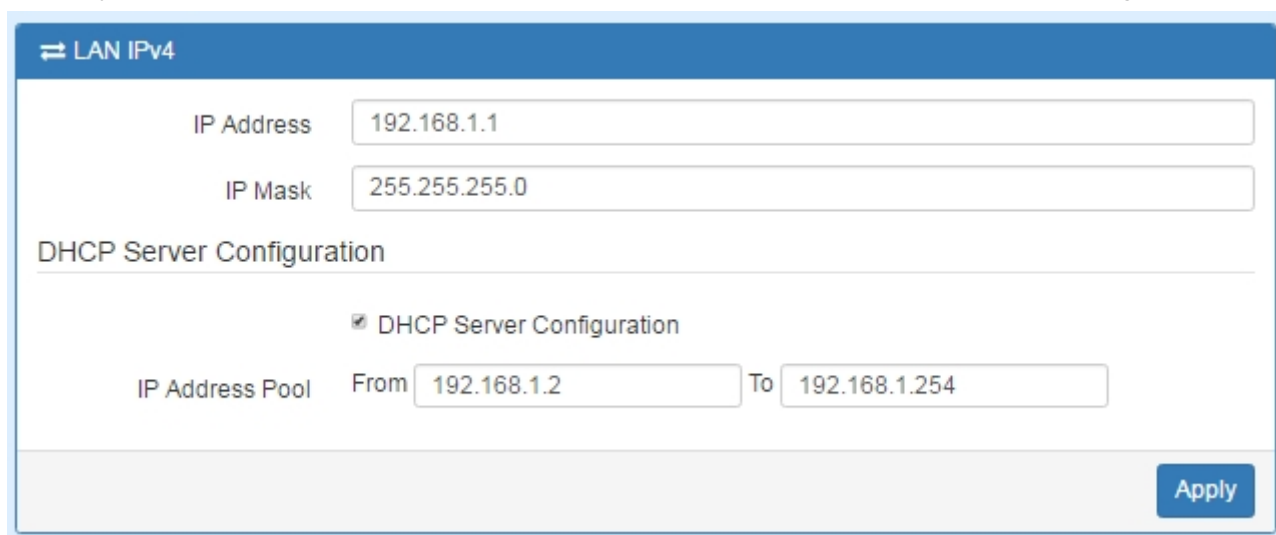
This section allows you to configure LAN IPv4, LAN IPv6, VLAN and Subnet.



The screenshot shows a vertical menu with a blue header labeled 'LAN' and a double arrow icon. Below the header are four white buttons with blue borders: 'IPv4', 'IPv6', 'VLAN', and 'Subnet'.

### 8.1 LAN > IPv4

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



The screenshot shows the 'LAN IPv4' configuration page. It has a blue header with a double arrow icon and the text 'LAN IPv4'. Below the header, there are two input fields: 'IP Address' with the value '192.168.1.1' and 'IP Mask' with the value '255.255.255.0'. Below these fields is a section titled 'DHCP Server Configuration'. Inside this section, there is a checkbox labeled 'DHCP Server Configuration' which is checked. Below the checkbox, there is an 'IP Address Pool' section with 'From' and 'To' input fields. The 'From' field has the value '192.168.1.2' and the 'To' field has the value '192.168.1.254'. At the bottom right of the page, there is a blue 'Apply' button.

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>• Turn on/off DHCP Server Configuration.</li><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>

## 8.2 LAN > IPv6

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

LAN > IPv6	
Item	Description
<b>LAN IPv6</b>	<ul style="list-style-type: none"> <li>This section provides two types, including <b>Delegate Prefix from WAN</b> and <b>Static</b>.</li> <li><b>Static Address:</b> You need to input the static address when you select the static type.</li> </ul>
<b>Delegate Prefix from WAN</b>	<ul style="list-style-type: none"> <li>Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.</li> </ul>
<b>Static</b>	<ul style="list-style-type: none"> <li>Select this option to configure a fixed IPv6 address for the cellular router's LAN IPv6 address.</li> </ul>
<b>Address Assign Setup</b>	Select how you obtain an IPv6 address: <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. DHCPv6 clients.</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>

## 8.3 LAN > VLAN

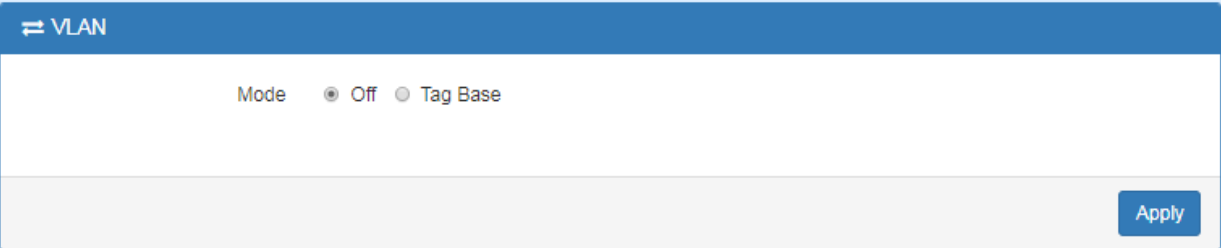
This section allows you to set up VLAN that provides a network segmentation system to distinguish the LAN clients and separate them into different LAN subnet for enhancing security and controlling traffic.

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

- Type 1:

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

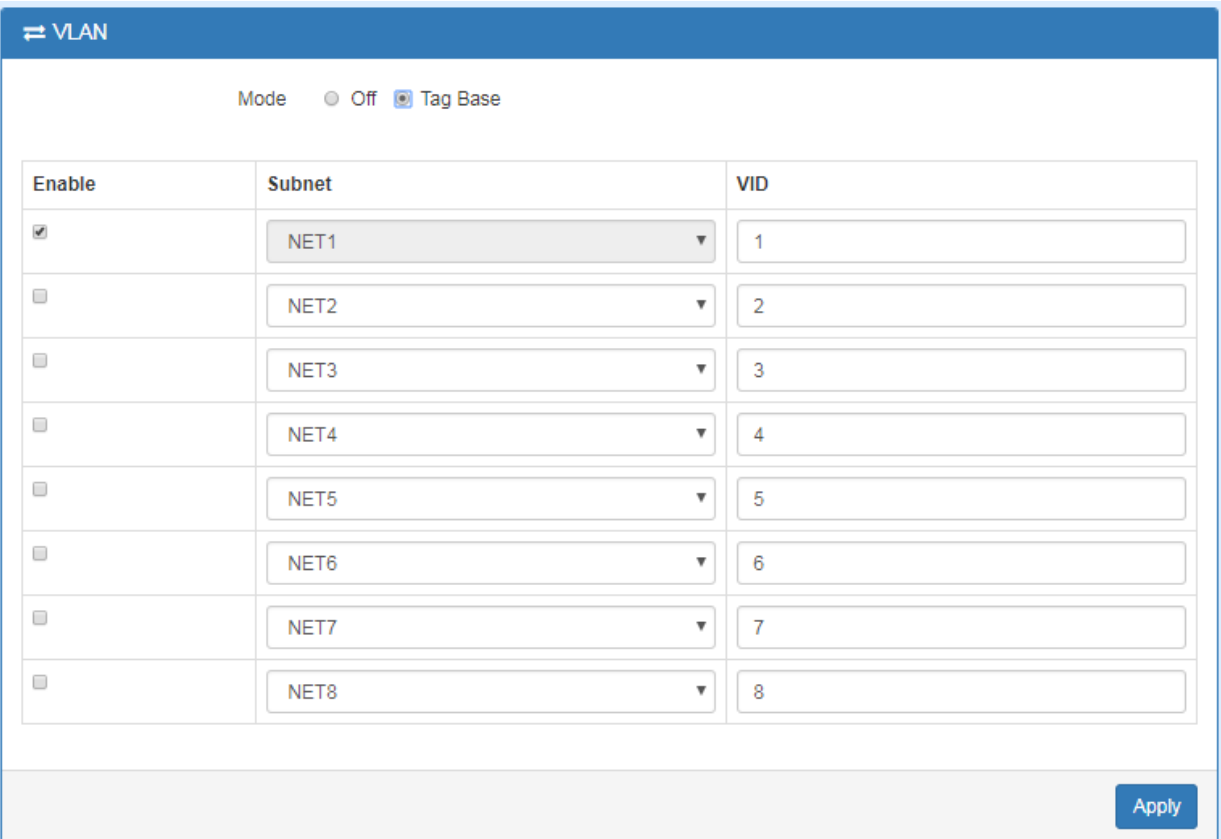
**Mode** allows you to select **Off** or **Tag Base (802.1p)**.



The image shows a 'VLAN' configuration window. At the top, there is a blue header with a double arrow icon and the text 'VLAN'. Below the header, the 'Mode' is set to 'Off' with a selected radio button. The 'Tag Base' option is also visible but not selected. At the bottom right, there is an 'Apply' button.

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

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



The image shows a 'VLAN' configuration window with 'Mode' set to 'Tag Base'. Below the mode selection, there is a table with three columns: 'Enable', 'Subnet', and 'VID'. The table contains eight rows, each with a checkbox, a subnet dropdown menu, and a VID input field. The first row has the checkbox checked and the subnet set to 'NET1'. The other rows have the checkbox unchecked and subnets from 'NET2' to 'NET8'. The VID field for each row contains a number from 1 to 8. An 'Apply' button is located at the bottom right.

Enable	Subnet	VID
<input checked="" type="checkbox"/>	NET1	1
<input type="checkbox"/>	NET2	2
<input type="checkbox"/>	NET3	3
<input type="checkbox"/>	NET4	4
<input type="checkbox"/>	NET5	5
<input type="checkbox"/>	NET6	6
<input type="checkbox"/>	NET7	7
<input type="checkbox"/>	NET8	8

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

LAN > VLAN (1-port LANs)	
Item	Description
<b>Mode</b>	<ul style="list-style-type: none"> <li>The VLAN mode is Off or Tag Base (802.1p VLAN).</li> </ul>
<b>Enable</b>	<ul style="list-style-type: none"> <li>The assigned row of setting are enabled.</li> </ul>
<b>Subnet</b>	<ul style="list-style-type: none"> <li>The subnet provides IP address and IP mask for the router.</li> </ul>
<b>VID</b>	<ul style="list-style-type: none"> <li>The VLAN ID range is from 1 to 4094.</li> </ul>

- Type 2:

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

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

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

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

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

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

VLAN

Mode

☐ Off
 ☒ Tag Base
 ☐ Port Base

Enable	Subnet	VID	Port			
			LAN1	LAN2	LAN3	Router
<input checked="" type="checkbox"/>	NET1	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	NET2	2	<input checked="" type="checkbox"/>	<input checked="" 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			1	1	1	--
Tag Mode			Trunk	Trunk	Trunk	--

Apply

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



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

VLAN

Mode
☐ Off
☐ Tag Base
☒ Port Base

Enable	Port	LAN1	LAN2	LAN3	Router
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Apply

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

## 8.4 LAN > Subnet

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

Status

System

WAN

LTE

LAN

IPv4

IPv6

VLAN

Subnet

IP Routing

Service

Management

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 with LAN->IPv4 setting and follows with Tag Base Mode of VLAN to enable the function.

Subnet

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

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

Apply

### 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

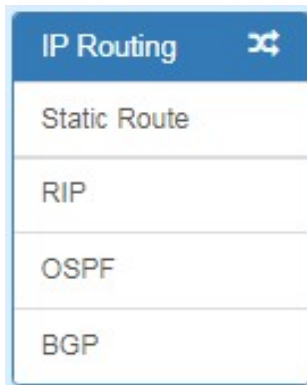
To

192.168.2.254

Save

## 9 IP Routing

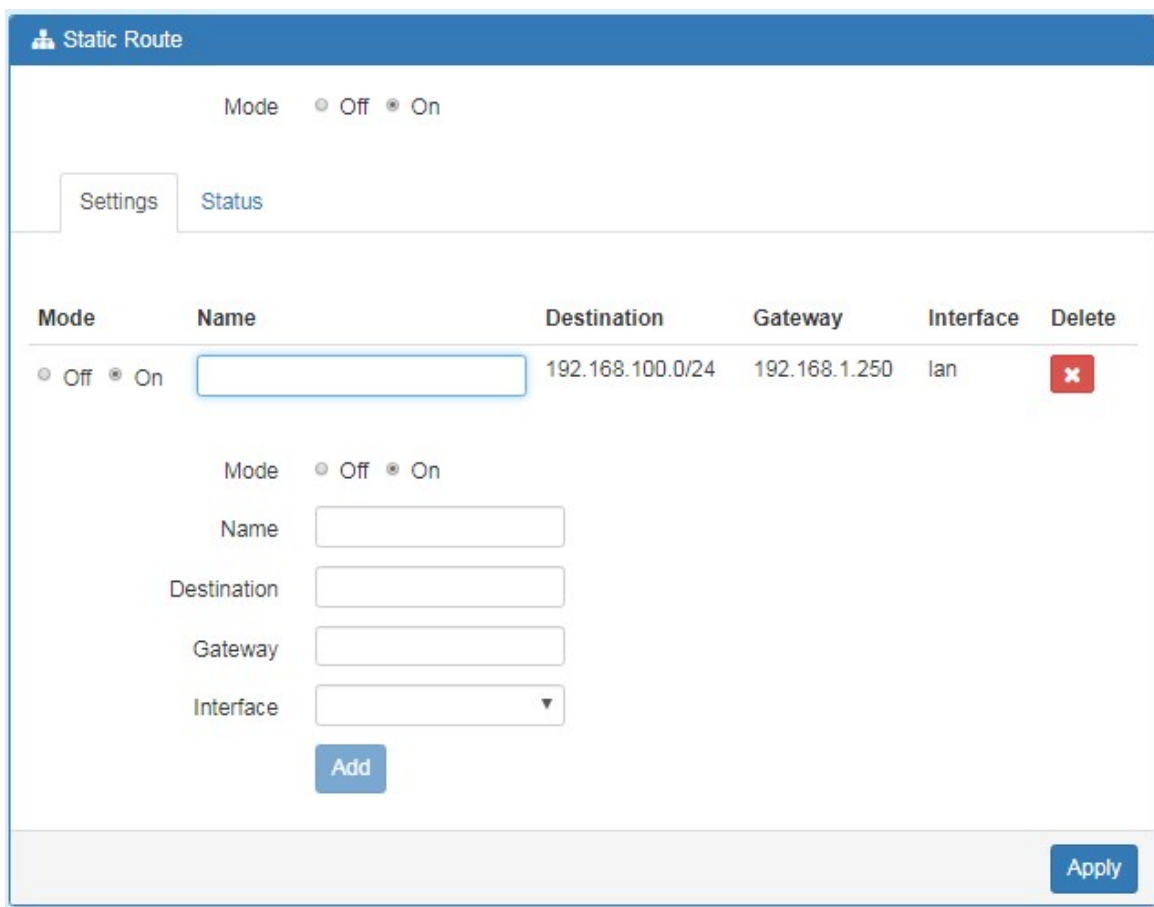
This section allows you to configure the Static Route, RIP, OSPF, and BGP.



A vertical menu titled "IP Routing" with a gear icon. It contains four options: "Static Route", "RIP", "OSPF", and "BGP".

### 9.1 IP Routing > Static Route

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

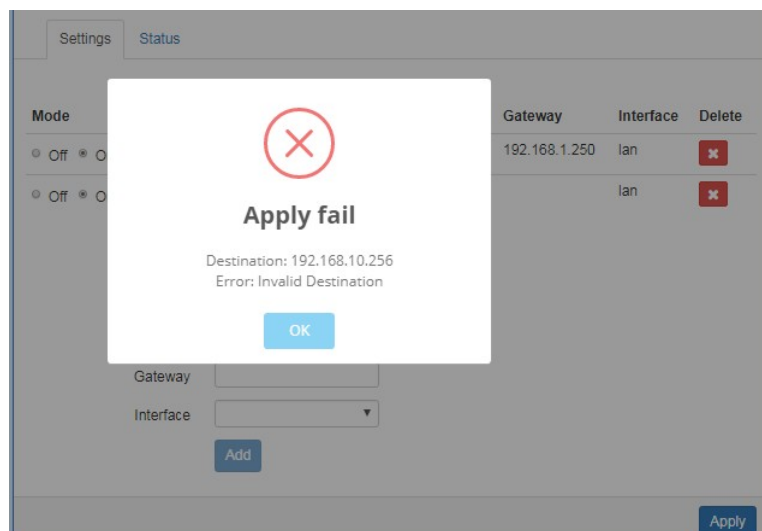


The "Static Route" configuration interface. At the top, there is a "Mode" section with radio buttons for "Off" and "On". Below this are two tabs: "Settings" and "Status". The "Settings" tab is active, showing a table with columns: "Mode", "Name", "Destination", "Gateway", "Interface", and "Delete". The table has one row with "Off" selected for Mode, an empty "Name" field, "192.168.100.0/24" for Destination, "192.168.1.250" for Gateway, "lan" for Interface, and a red "X" icon for Delete. Below the table, there is another "Mode" section with "Off" and "On" radio buttons. Below that are input fields for "Name", "Destination", "Gateway", and "Interface" (a dropdown menu). An "Add" button is at the bottom left of the form, and an "Apply" button is at the bottom right.

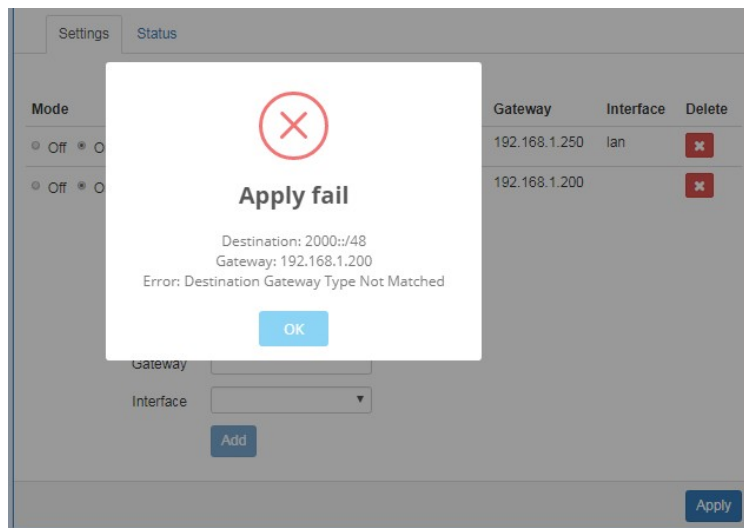
IP Routing > Static Route	
Item	Description
Mode	The setting is for full network. Select from Off or On.
Settings	
Mode	The setting is for the specific network. Select from Off or On.
Name	Set up each name for your running host or network.
Destination	Fill in the destination of a specific subnet or IP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

**Note:**

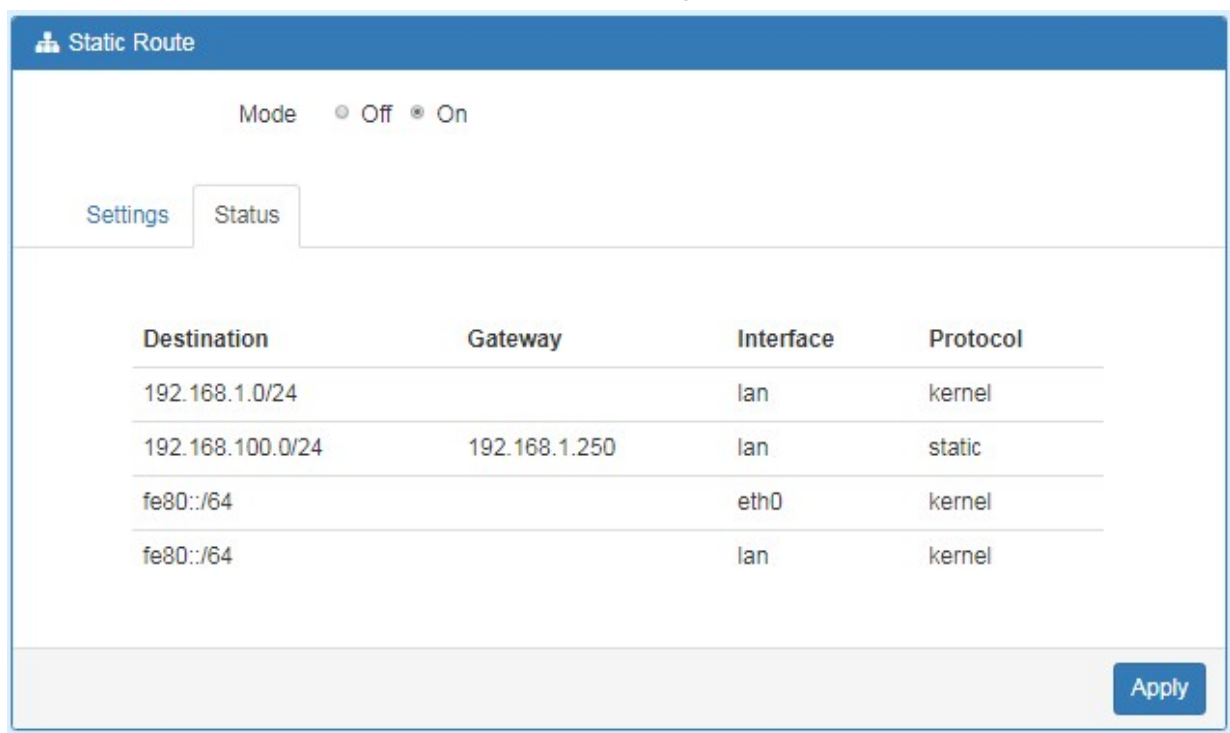
- The destination field is required to fill in. The format of destination is IPv4 or IPv6.
- The address of gateway or the type of interface can be chosen one or both to fill in the field.
- There are two fail situations when you fill in the incorrect type for the field.  
 (1) Input the invalid format of destination. The interface is shown in **Apply fail** to notice.



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



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



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

## 9.2 IP Routing > RIP

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

**Note:**

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

RIP

General

Interfaces

Mode

☒ Off
 ☐ On

Redistribute local routes

☒ Off
 ☐ On

Redistribute routes from the device's own routing table

Redistribute connected routes

☒ Off
 ☐ On

Redistribute routes to networks which are directly connected to the device

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.

RIP

General

Interfaces

#	Mode	Interface	Authentication	Key	Key ID	Passive	Edit	Delete					
Add RIP Interface													
	Mode	<input type="radio"/> Off <input checked="" type="radio"/> On											
	Interface	eth1(WAN Ethernet) ▼											
	Authentication	md5 ▼											
	Key			The key used for authentication (maxlength=16)									
	Key ID	1		The ID of the key used for authentication (1-255)									
	Passive	<input checked="" type="radio"/> Off <input type="radio"/> On											
		Do not send out RIP packets on this interface											
		Add											

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.

## 9.3 IP Routing > OSPF

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

The screenshot displays the OSPF configuration page with a left-hand navigation menu and a main configuration area. The navigation menu includes Status, System, WAN, LTE, LAN, IP Routing (selected), Static Route, RIP, OSPF, BGP, Service, and Management. The main area is titled 'OSPF' and has three tabs: General, Interfaces, and Networks. The 'General' tab is active, showing several settings with radio button options for 'Off' and 'On':

- Mode:** Radio buttons for Off and On.
- Redistribute local routes:** Radio buttons for Off and On, with a note 'from the device's own routing table'.
- Redistribute connected routes:** Radio buttons for Off and On, with a note 'to networks which are directly connected to the device'.
- Redistribute RIP routes:** Radio buttons for Off and On, with a note 'learned via the RIP routing protocol'.
- Redistribute BGP routes:** Radio buttons for Off and On, with a note 'learned via the BGP routing protocol'.

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

### (1) General Configuration

You can have these settings for General configuration.

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

OSPF

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>General</b>	
<b>Mode</b>	<ul style="list-style-type: none"> <li>Off: OSPF function is off.</li> <li>On: OSPF function is on.</li> </ul>
<b>Redistribute local routes</b>	<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>
<b>Redistribute connected routes</b>	<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>
<b>Redistribute RIP routes</b>	<ul style="list-style-type: none"> <li>Off: Not redistribute RIP routes learned via the RIP routing protocol.</li> <li>On: Redistribute RIP routes learned via the RIP routing protocol.</li> </ul>
<b>Redistribute BGP routes</b>	<ul style="list-style-type: none"> <li>Off: Not redistribute BGP routes learned via the RIP routing protocol.</li> <li>On: Redistribute BGP routes learned via the RIP routing protocol.</li> </ul>

## (2) Interfaces Configuration

There are 2 parts for OSPF Interfaces configuration.

- OSPF Interfaces Summary

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

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

- Add/Edit OSPF Interface

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

OSPF

General

Interfaces

Networks

Summary

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

Add OSPF Interface

Add/Edit

Mode

☐ Off
☒ On

Interface

eth1

Authentication

md5

Key

The key used for authentication (maxlength=16)

Key ID

1

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

Cost

0

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

Passive

☒ Off
☐ On

Do not send out OSPF packets on this interface

Add

Apply

IP Routing > OSPF > 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 OSPF 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>Cost</b>	The cost for sending packets via this interface (0: OSPF defaults).
<b>Passive</b>	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

Mode

☐ Off ☒ On

Prefix

Prefix of the network

Prefix Length

Length of the prefix

Area

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

Add

Summary

Add/Edit


Apply

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

## 9.4 IP Routing > BGP

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

### (1) General Configuration

 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

Redistribute RIP routes

☐ Off ☒ On

learned via the RIP routing protocol

Redistribute OSPF routes

☐ Off ☒ On

learned via the OSPF routing protocol

Apply

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

Summary

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

Add BGP Neighbor

Add/Edit

Mode

☐ Off
 ☒ On

IP Address

IP address of the peer router

AS Number

1

Autonomous system number of the peer router

Multihop

☐ Off
 ☒ On

Allow multiple hops between this router and the peer router

Add

Apply

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

### (3) Networks Configuration

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

BGP

General

Neighbors

Networks

Summary

#	Mode	Prefix	Prefix Length	Edit	Delete
1	on	4.4.4.0	24		

Add BGP Network

Add/Edit

Mode

☐ Off
☒ On

Prefix

xxx.xxx.xxx.xxx

Prefix of the network

Prefix Length

24

Length of the prefix

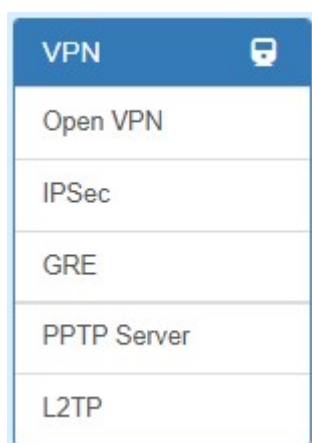
Add

Apply

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

## 10 Configuration > VPN


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




### 10.1 VPN> OpenVPN













### 10.1.1 Edit OpenVPN Connection

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

 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

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

Edit Open VPN Connection #1

Setting

Log

Mode

☒ Disable
☐ Enable

VPN Mode

☐ Server
☒ Client
☐ Custom

Status

Idle

TLS Mode

☒ Disable
☐ Enable

Cipher

BF-CBC

IPv6 Mode

☒ Disable
☐ Enable

Device

☒ TUN
☐ TAP

Protocol

☒ UDP
☐ TCP

Port

1701

VPN Compression

☒ Disable
☐ Enable

Authentication

Certificate

Client

Client Mode

☒ Roadwarrior

Server Address

0.0.0.0

Route Client Networks

☒ Off
☐ On

NAT

1:1 NAT

☒ Off
☐ On

Client - Security

Root CA

Import

Cert

Import

Key

Import

P12

Import

Back

Refresh

Apply

(3) From **Log** tab, the interface will be shown the status of connection to make you follow the

suitation whenever is successful or fail connection.

Edit Open VPN Connection #1

Setting

Log

Back

Refresh

Apply

VPN > OpenVPN	
Item	Description
<b>Mode</b>	Turn on/off OpenVPN to select Disable or Enable.
<b>VPN Mode</b>	<ul style="list-style-type: none"> <li>• Server: Tick to enable OpenVPN server tunnel.</li> <li>• Client: Tick to enable OpenVPN client tunnel. The default is Client.</li> <li>• Custom: This option allows user to use the .ovpn configuration file to quickly set up VPN tunnel with third-party server or use the OpenVPN advanced options to be compatible with other servers.</li> </ul>
<b>Status</b>	Display the status of OpenVPN.
<b>TLS Mode</b>	Select from Disable or Enable for data security. The default is Disable.
<b>Cipher</b>	The OpenVPN format of data transmission.
<b>IPv6 Mode</b>	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 OpenVPN 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>

### 10.1.2 Set up OpenVPN Client

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

Client

Client Mode

☒ Roadwarrior

Server Address

0.0.0.0

Route Client Networks

☒ Off
☐ On

NAT

1:1 NAT

☒ Off
☐ On

Client - Security

Root CA

Import

Cert

Import

Key

Import

P12

Import

VPN > OpenVPN > Client VPN Mode	
Item	Description
<b>Client</b>	
<b>Client Mode</b>	Only support the Roadwarrior mode.
<b>Server Address</b>	Fill in WAN IP of OpenVPN 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>NAT</b>	
<b>1:1 NAT</b>	<ul style="list-style-type: none"> <li>• Tick to enable NAT Traversal for OpenVPN. 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 OpenVPN tunnels, this function should be turned on.</li> </ul>
<b>Client-Security</b>	
<b>Root CA</b>	The Certificate Authority file of OpenVPN server could be downloaded from OpenVPN server.
<b>Cert</b>	The certification file is for OpenVPN client, which could be downloaded from OpenVPN server.
<b>Key</b>	The private key file is for OpenVPN client, which could be downloaded from OpenVPN server.
<b>P12</b>	The PKCS#12 file is for OpenVPN client, which could be downloaded from OpenVPN server.

### 10.1.3 Set up OpenVPN Server

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

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

Server

Client Mode

☒ Roadwarrior

VPN Network

0.0.0.0

VPN Netmask

0.0.0.0

Roadwarrior

Route Client Networks

☒ Off ☐ On


NAT

1:1 NAT


☒ Off ☐ On

Server - Server Security

Root CA

 Create


Cert, Key

 Create

Server - User Security

User 1


☐ Valid

 Create

password for create

User 2


☐ Valid

 Create

password for create

User 3


☐ Valid

 Create

password for create

User 4


☐ Valid

 Create

password for create

User 5


☐ Valid

 Create

password for create

User 6


☐ Valid

 Create

password for create

User 7


☐ Valid

 Create

password for create

User 8

☐ Valid

 Create

password for create

Back

Refresh





Apply

VPN > OpenVPN > Server VPN Mode	
Item	Description
<b>Server</b>	
<b>Client Mode</b>	Only support the Roadwarrior mode.
<b>VPN Network</b>	The network ID for OpenVPN virtual network.
<b>VPN Netmask</b>	The netmask for OpenVPN virtual network.
<b>Roadwarrior: Route Client Networks</b>	Select from Off or On. The OpenVPN server will route the client traffic or not. User should fill in the client IP and netmask when this option is enabled.
<b>NAT</b>	
<b>1:1 NAT</b>	<ul style="list-style-type: none"> <li>• Tick to enable NAT Traversal for OpenVPN. 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 OpenVPN 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.

#### 10.1.4 Set up OpenVPN Custom

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

**Note:**

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

Edit Open VPN Connection #1

Setting

Log

Mode

☒ Disable
☐ Enable

VPN Mode

☐ Server
☐ Client
☒ Custom

Custom Config

Import \*.ovpn

Username

Password

Status

Idle

Back

Refresh

Apply

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

## 10.2 VPN > IPSec

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

### 10.2.1 IPSec > General setting

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

The screenshot displays the 'IPSec' configuration page, specifically the 'General setting' tab. The interface includes a left sidebar with navigation options: Status, System, WAN, LAN, Service, and Management. The main content area is divided into three sections: IKE, Encryption, and Authentication. The IKE section has a 'Mode' toggle set to 'Disable' and a 'General setting' tab. The IKE configuration includes dropdown menus for Protocol (IKEv1), Aggressive mode (Disable), Encryption (AES128), Hash (SHA1), and DH Group (5 (1536 bit)). The Encryption section includes dropdown menus for Protocol (ESP), Encryption (AES128), Hash (SHA1), and DH Group (5 (1536 bit)). The Authentication section includes a dropdown for Auth Type (PSK) and a text field for Auth Secret. The Advance section includes input fields for DPD delay (30) and DPD timeout (150). An 'Apply' button is located at the bottom right of the main content area. On the right side of the interface, there is a panel titled 'X.509 Certificates' with tabs for 'Create', 'Cert', and 'Key'. The 'Create' tab shows buttons for 'Root CA', 'Local', 'Remote', and 'Remote CA'. The 'Cert' and 'Key' tabs show buttons for 'Import', 'Local', and 'Remote CA'.

Mode	General setting	Connections
Disable		
Enable		

### IKE

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

### Encryption

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

### Authentication

Auth Type	Auth Secret
PSK	

### Advance

DPD delay	DPD timeout
30	150

Apply

### X.509 Certificates


Create	Cert	Key
Root CA		
Local		
Remote		
Remote CA		

Import	Cert	Key
Local		
Remote CA		



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

### 10.2.2 IPSec > Connections













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

## + IPsec

Mode ☒ Disable ☐ Enable

General setting

Connections

#	Enable	Name	Local	Remote	Edit
1	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
2	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
3	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
4	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
5	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
6	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
7	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
8	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
9	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
10	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
11	<input type="checkbox"/>		0.0.0.0	0.0.0.0	
12	<input type="checkbox"/>		0.0.0.0	0.0.0.0	

Apply

**Edit IPSec Connection #1**

**Mode**    ☒ Disable    ☐ Enable

**Name**   

**Status**    Idle

---

**Local**

**Host**   

**Subnet**   

**ID**   

---

**Remote**

**Host**   

**Subnet**   


**ID**   

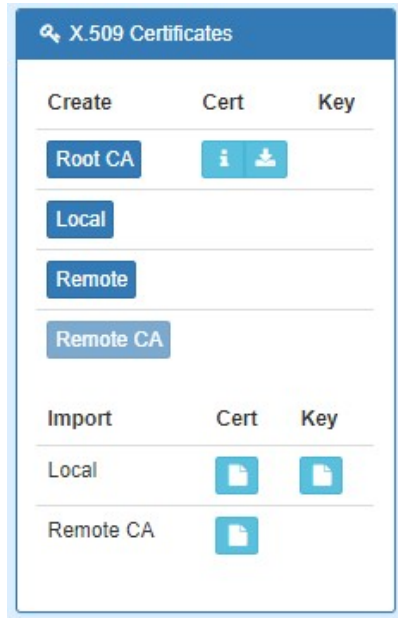
Save

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

### 10.2.3 IPsec > The setting of X.509 Certificates

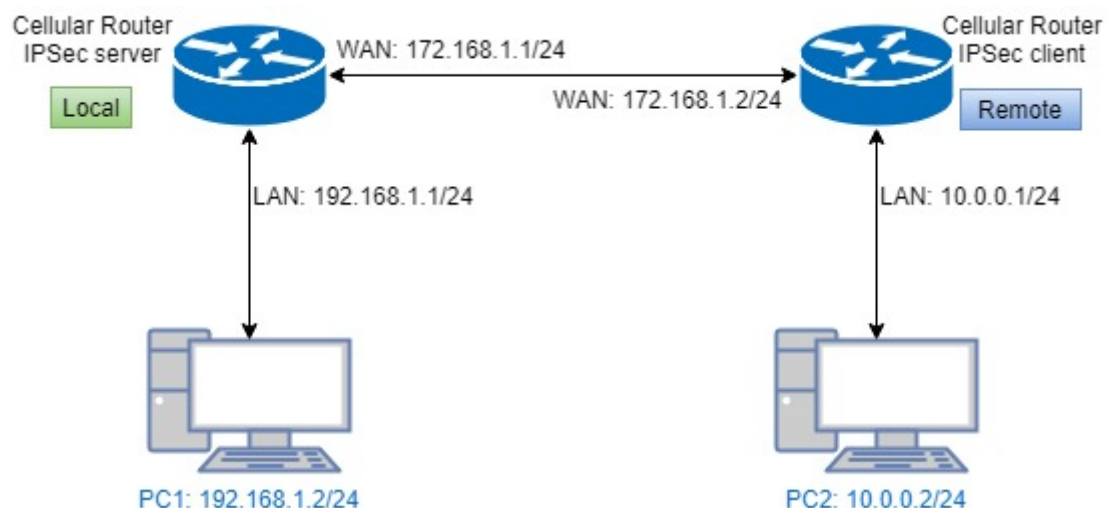
The interface shows the setting items of X.509 Certificates.

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



### 10.2.4 IPsec > Net-to-Net Configuration

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



#### General setting

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



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

IPSec

Mode

Disable

Enable

General setting

Connections

#	Enable	Name	Local	Remote	Edit
1	<input type="checkbox"/>		0.0.0.0	0.0.0.0	

- Local Side

First, fill up the local Host and Subnet fields by the network information of IPSec server.

And, use the network information of IPSec client to fill up the remote setting.

Then, specify the ID for the both sides.

In this case, the IDs for the local and remote side are named as @local and @remote respectively.

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

Edit IPSec Connection #1

Mode

Disable

Enable

Name

net-to-net

Status

Established

Local

Host

172.168.1.1

Subnet

192.168.1.0/24

ID

@local

Remote

Host

172.168.1.2

Subnet

10.0.0.0/24

ID

@remote

Save

- Remote Side

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

Edit IPSec Connection #1

Mode

☐ Disable ☒ Enable

Name

net-to-net

Status

Established

Local

Host

172.168.1.2

Subnet

10.0.0.0/24

ID

@remote

Remote

Host

172.168.1.1

Subnet

192.168.1.0/24


ID

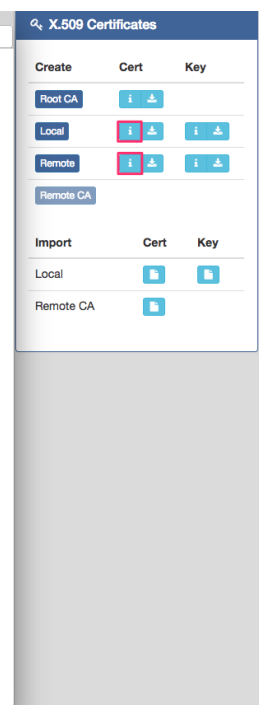
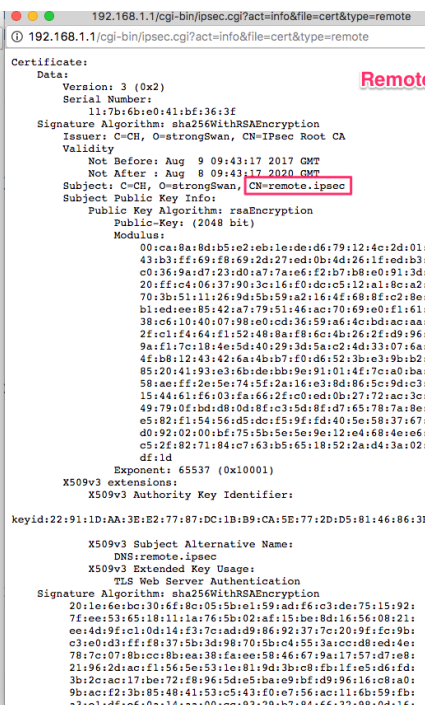
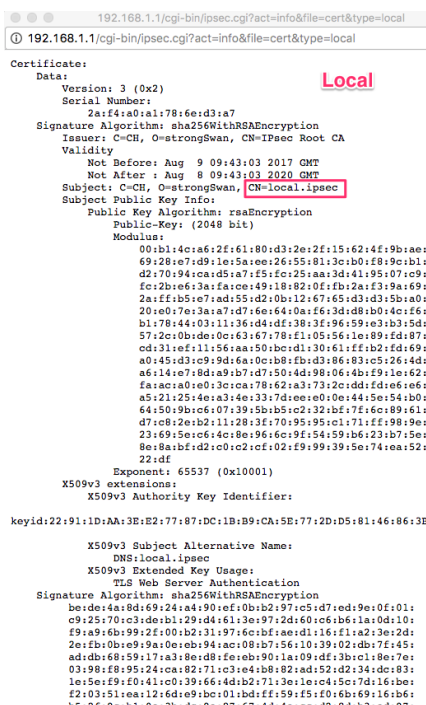
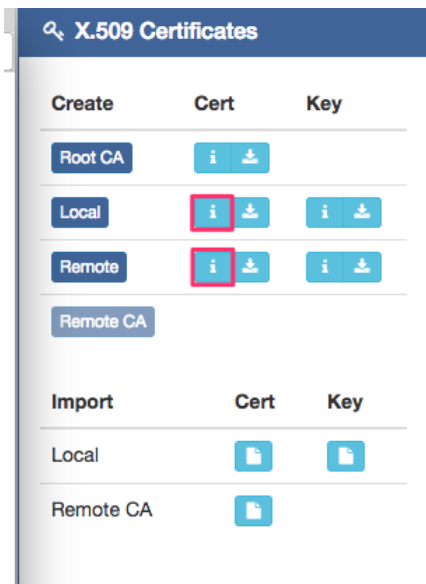
@local

Save

### Net-to-Net (Pre-shared key)

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

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



## Import Certificate

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

The mapping is as below:

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

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



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

## Local Side

Edit IPSec Connection #1

Mode ☐ Disable ☒ Enable

Name

Status Connecting

### Local

Host

Subnet

ID

### Remote

Host

Subnet

ID

Save

## Remote Side

Edit IPSec Connection #1

Mode

☐ Disable ☒ Enable

Name

Status

Connecting

Local

Host

0.0.0.0

Subnet

10.0.0.0/24

ID

@remote.ipsec

Remote

Host

172.168.1.1

Subnet

192.168.1.0/24

ID

@local.ipsec

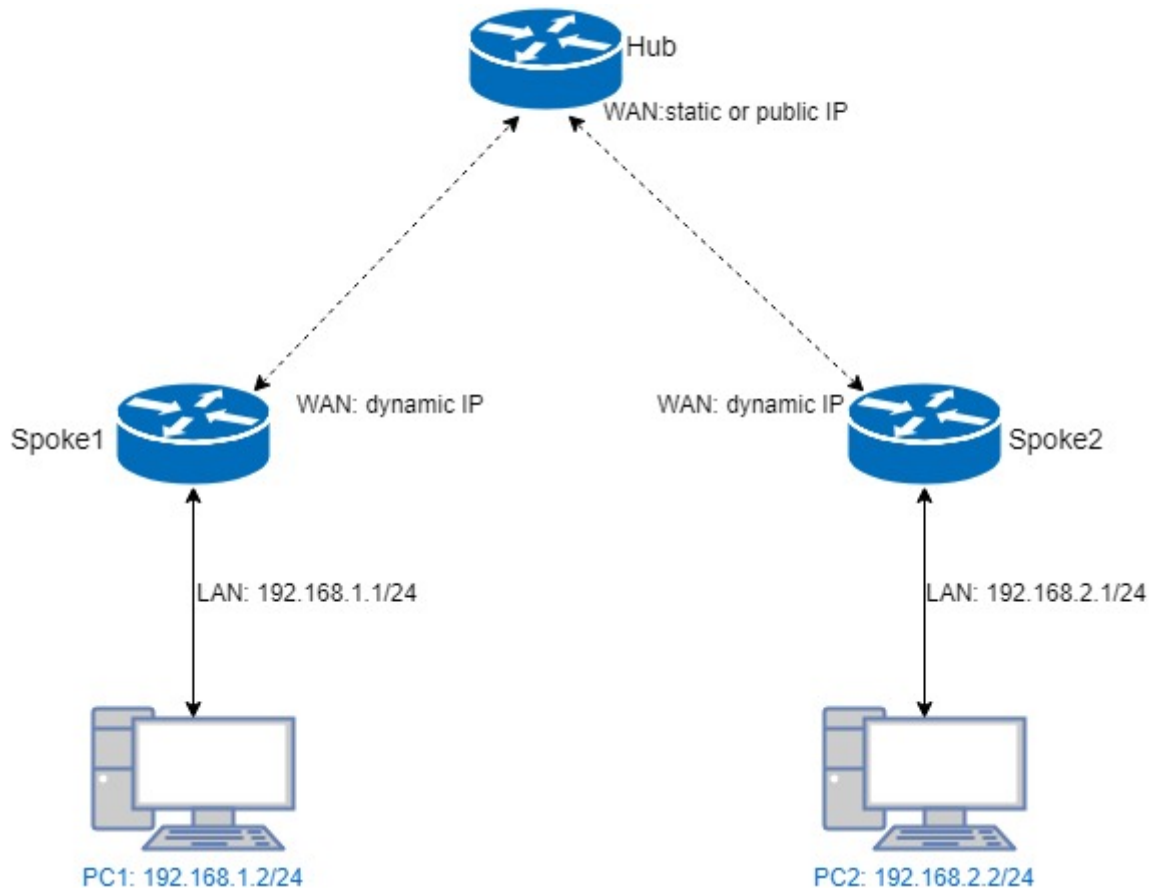
Save

### 10.2.5 IPSec > Hub-Spoke Topology

This section explains how to sets Hub-Spoke Topology. Connect two (or more) gateways to a central one.

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

For example, we use three gateways to setup this topology. It should like the following figure.



After some configuration setup, the PC1 and PC2 could communicate each other through the Hub gateway.

**Note:**

- (1) This example should be running under the pre-shared key authentication.
- (2) This example will cause the cellular router internet traffic loss (Only handle IPSec VPN traffic)

- **Hub configuration**

In this example, we have two spoke on the topology. Thus, the Hub needs to setup two IPSec connections for each spoke.

The settings should be like the following table.

Attribute	Hub's conn 1	Hub's conn 2
Local host		
Local subnet	0.0.0.0/0	0.0.0.0/0
Local id		
Remote host		
Remote subnet	192.168.1.0/24	192.168.2.0/24
Remote id		

- **Spoke configuration**

In this example, the spoke gateways only need to setup one IPSec connection.

The setting needs to correspond the hub gateway settings, it should be like the following table.

Attribute	Hub's conn 1	Hub's conn 2
Local host		
Local subnet	192.168.1.0/24	192.168.2.0/24
Local id		
Remote host	Hub's WAN IP	Hub's WAN IP
Remote subnet	0.0.0.0/0	0.0.0.0/0
Remote id		

**Note:** The Remote subnet **0.0.0.0/0**, it will make the all traffic into the IPSec VPN tunnel.

## 10.3 VPN > GRE

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

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

+ GRE

Mode

☐ Off
☒ On

Apply

The GRE Mode is on.

+ GRE

Mode

☐ Off
☒ On

Local Address

192.168.1.4

Remote Address

192.168.1.5

Tunnel Device Address

10.1.1.4

Tunnel Device Address Prefix

8

Apply

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.

## 10.4 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	
Item	Description
<b>Mode</b>	Select from Off or On to enable PPTP Server.
<b>Server Address</b>	IP addresses to be used at the local end of the tunneled PPP links between the server and the client.
<b>Client Address Range</b>	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
<b>Mode</b>	Select from Off or On to set the client setting.
<b>Username</b>	The username of this client.
<b>Password</b>	The password of this client.

PPTP Server

General
Clients

#	Mode	Username	Password	Edit	Summary Delete
1	on	client	client		

Add PPTPD Client
Add/Edit

Mode
☐ Off
☒ On

Username

Password

Add

Apply

## 10.5 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.

**Tip:** To manage the L2TP clients under server mode, there are two steps to create the L2TP client. First, Fill in the Username and Password. Second, Click the Add button.

User List

Empty Users

Add L2TP User for Server Mode

Username

test

Password

test

Add



## User List


#	Username	Password	Edit	Delete
1	test	test		

## Edit L2TP User #1 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

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

**Tip 1:** There are two steps to manage the L2TP connection under client mode, First, Fill in the required parameters. Second, Click the Add button to create the L2TP connection.

#### 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

#### Connection List

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

**Tip 2:** There are two steps to update the L2TP connection. First, Click the Edit button. Second, Update the parameters.

## Connection List

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

## Edit L2TP Connection #1 for Client Mode

Mode ☐ Off ☒ On

Server

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

Username

Password

NAT ☐ Off ☒ On

Default Route ☐ Off ☒ On

# 11 Configuration > Firewall

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



















## 11.1 Firewall > Port Forwarding

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

Port Forwarding

Mode
☒ Disable
☐ Enable

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

## 11.2 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.

## 11.3 Firewall > IP Filter

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

+

IP Filter

Mode

☒ Disable
 ☐ Enable

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

Apply

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

Edit IP Filter Black List Entry #1

Mode    ☒ Disable   ☐ Enable

Protocol   ☒ All   ☐ ICMP   ☐ TCP   ☐ UDP

Source IP   

Source Port  

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.

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

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

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.			

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

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

















## 11.4 Firewall > MAC Filter

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

MAC Filter

Mode

☒ Disable
 ☐ Enable

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

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).

## 11.5 Firewall > URL Filter

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

URL Filter

Mode ☒ Disable ☐ Enable

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

Apply

Edit URL Filter Black List Entry #1

Mode ☒ Disable ☐ Enable

Filter ☐ Key ☒ Full

Hint: Please NOT include 'https://' inside the URL

Key/Full

Save

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

Mode    ☐ Disable    ☒ Enable

Filter    ☐ Key    ☒ Full

Key/Full   


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.

## 11.6 Firewall > NAT

This section allows you to set NAT configuration.

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

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

 NAT

Mode    ☐ Disable    ☒ Enable

Apply

## 12 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

### 12.1 Service > SNMP

#### 12.1.1 SNMP configuration

This section allows you to set the SNMP configuration.

**SNMP**

Mode

☐ Disable

☒ Enable

Community

SNMP v3 User Configuration

SNMP trap configuration

#	Mode	Name	Access
1	<div>Enable</div>	<div>public</div>	<div>Read-Only</div>
2	<div>Enable</div>	<div>private</div>	<div>Read-Write</div>
3	<div>Disable</div>	<div></div>	<div>Read-Only</div>

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.

### 12.1.2 SNMP v3 User configuration

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

Mode ☐ Disable ☒ Enable

Community SNMP v3 User Configuration SNMP trap configuration

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

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.

### 12.1.3 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 1
 ☒ DI 2
 ☒ VPN disconnect
 ☒ WAN disconnect

Alarm output

☒ SMS
 ☒ DO
 

SNMP trap

☒ E-mail

DI 1 Trigger

☒ High
 ☐ Low

DI 2 Trigger

☒ High
 ☐ Low

DO behavior

☒ Always
 ☐ Pulse

Groups

Group

SMS

Limit 150 english characters

Group

Name	SUN	MON	TUE	WED	THU	FRI	SAT

View SMS

Apply

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

## 12.2 Service > TR069

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

Service > TR069	
Item	Description
<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 connecting.
<b>Connection Request Password</b>	Fill in the connection request password to authenticate the ACS if the ACS attempts to communicate with the CPE connecting.

## 12.3 Service > Dynamic DNS

This section allows you to set up Dynamic DNS.

The image displays two screenshots of the 'Dynamic DNS' configuration page. Both screenshots show the 'Dynamic DNS' title and a 'Mode' section with 'Disable' and 'Enable' radio buttons. The 'Service Provider' is set to 'dynv6.com'. The 'Host Name', 'Token ID', and 'Update Period Time (Sec)' fields are present. In the top screenshot, 'Host Name' is empty. In the bottom screenshot, 'Host Name' is expanded to show a list of suggestions: 'dynv6.com', 'www.nsupdate.info', 'www.duckdns.org', 'no-ip.com', 'freedns.afraid.org', and 'dyndns.org'. An 'Apply' button is located at the bottom right of each form.

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

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

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

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

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

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

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

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



## 12.4 Service > VRRP

This section allows you to configure VRRP.

+

 VRRP

Mode

☒ Disable ☐ Enable

Group ID

1

Priority

100

Virtual IP

0.0.0.0

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>

## 12.5 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

Name

Delete

Username

Password

Add

ACLs

User

Topic

Read

Write

Delete

User

Topic

☐ Read

☐ Write

Add

Apply

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

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 ACL control, user can specify what topic should be limited. In this case, we set up the publisher **pub1** to write the critical topic. Additionally, we also allow the subscribers **sub1** and **sub3** to read the critical topic. Thus, only the sub1 and sub3 can receive it when **pub1** sending the message.

MQTT

Mode

☐ Disable ☒ Enable

Port

1883

Manage Users

Username	Password	Delete
Sub1	....	<input checked="" type="checkbox"/>
Sub2	....	<input checked="" type="checkbox"/>
Sub3	....	<input checked="" type="checkbox"/>
Pub1	....	<input checked="" type="checkbox"/>
Pub2	....	<input checked="" type="checkbox"/>

Username

Password

Add

ACLs

User	Topic	Read	Write	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

☐ Read

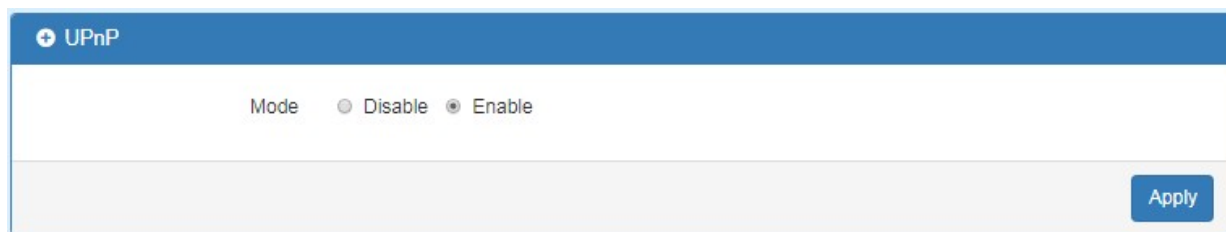
☐ Write

Add

Apply

## 12.6 Service > UPnP

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



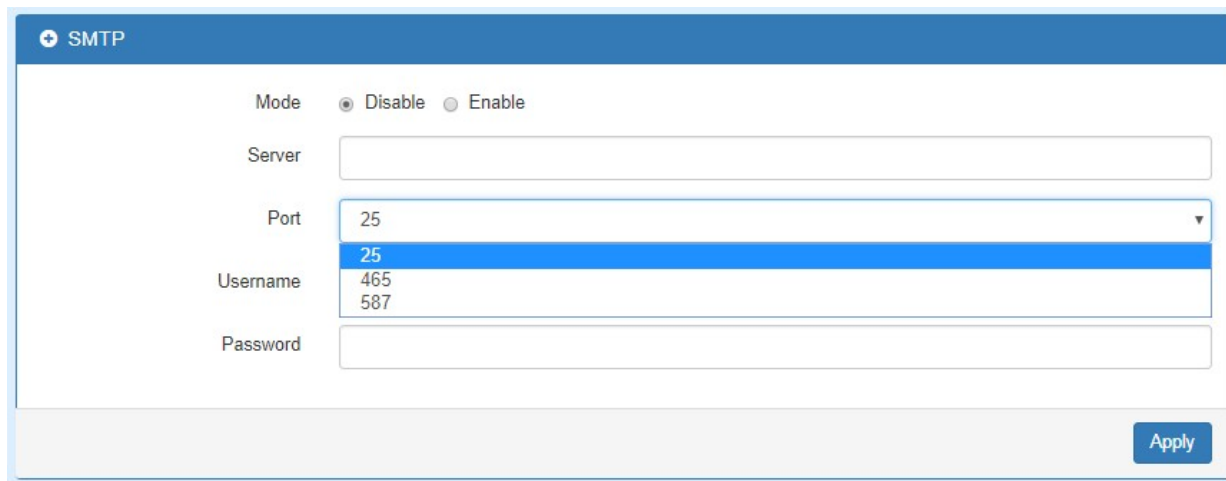
### Note:

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

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

## 12.7 Service > SMTP

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



Service > SMTP	
Item	Description
Mode	Select from Disable or Enable. The default is Disable.
Server	The email will be sent through the server.
Port	There are three ports for SMTP communication between mail servers. <ul style="list-style-type: none"><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.

## 12.8 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 have multiple connections to a network, each serving a different purpose.

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

IP Alias

Mode ☐ Off ☒ On

Entries

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

Add IP Alias Entry

Mode ☐ Off ☒ On

Interface 

eth1(WAN Ethernet) ▾

Addr 

xxx.xxx.xxx.xxx

Mask 

255.255.255.0

Add

Apply

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

## 13 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.



### 13.1 Management > Identification

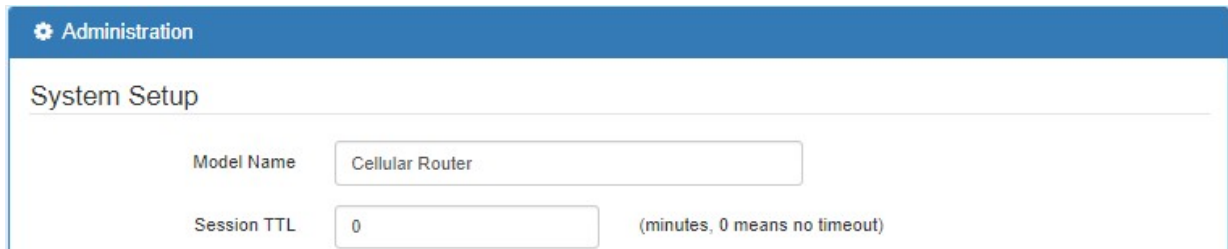
This section allows you to confirm the profile of router, current software, firmware version and system uptime.

Identification	
Attr.	Value
Model Name	Cellular Router
MAC Address	CA:97:37:B3:68:1A
Software Version	V1.68
Software MCSV	013600001682C133
Hardware MCSV	013600001682C132
Modem Firmware Version	EC25EFAR02A04M4G
IMEI	861107030239025
Uptime	1:11:34

Management > Identification	
Item	Description
<b>Model Name</b>	Show the host name of cellular router.
<b>MAC Address</b>	Show the MAC address.
<b>Software Version</b>	Show the current software version.
<b>Software MCSV</b>	Show the current software MCSV.
<b>Hardware MCSV</b>	Show the current hardware MCSV.
<b>Modem Firmware Version</b>	Show the current firmware version.
<b>IMEI</b>	Show the IMEI (International Mobile Equipment Identity number).
<b>Uptime</b>	Show the current system uptime.

## 13.2 Management > Administration

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



Administration

System Setup

Model Name: Cellular Router

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

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

## System Setup

Model Name

Session TTL  (minutes, 0 means no timeout)

## Super User

New Password  8 ~ 12 Characters

Retype to confirm

## User #1

Name

User Level

New Password  8 ~ 12 Characters

Retype to confirm

## User #2

Name

User Level

New Password  8 ~ 12 Characters

Retype to confirm

## User #3

Name

User Level

New Password  8 ~ 12 Characters

Retype to confirm

Apply



### 13.3 Management > SSH

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

SSH

Mode

☐ Disable ☒ Enable

Server Port

Access Control

☒ Allow All ☐ Allow specified IPv4v6 Address below

Apply

Management > SSH	
Item	Description
Mode	Select from Disable or Enable SSH function.
Server Port	The port number is where SSH server works on.
Access Control	<ul style="list-style-type: none"><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>

SSH

Mode
☐ Disable
☒ Enable

Server Port

Access Control
☐ Allow All
☒ Allow specified IPv4v6 Address below

IPv4v6 Address Set

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

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

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

Apply

## 13.4 Management > Firmware

This section provides you to upgrade the firmware of router.

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

Firmware

Select the firmware to upgrade(\*.tar)

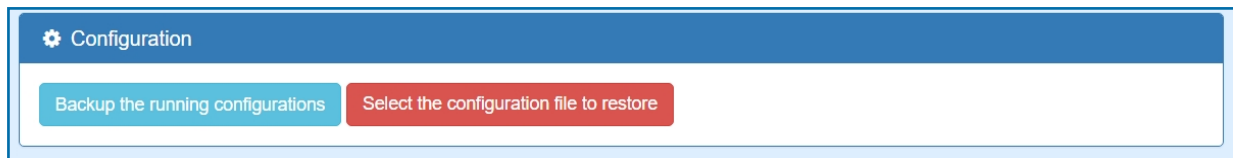
Upgrade

## 13.5 Management > Configuration

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

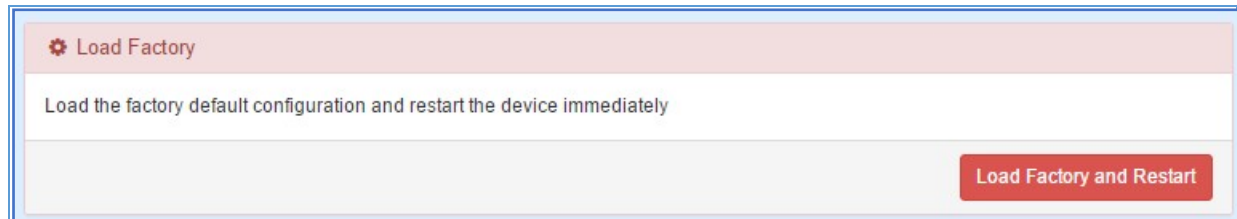
- (1) Click **Backup the running configurations** button to export your current configurations.

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



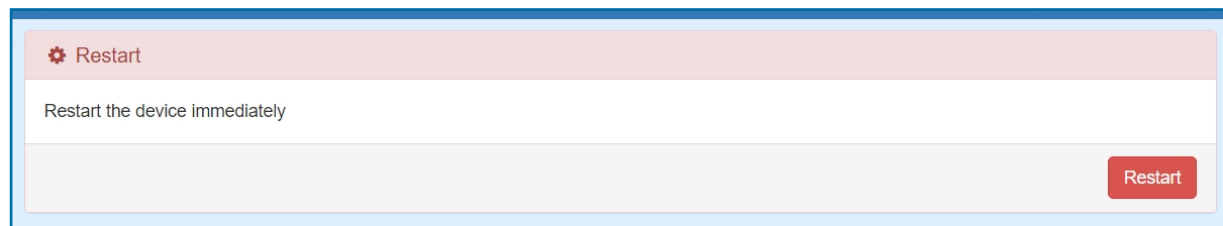
## 13.6 Management > Load Factory

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



## 13.7 Management > Restart

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



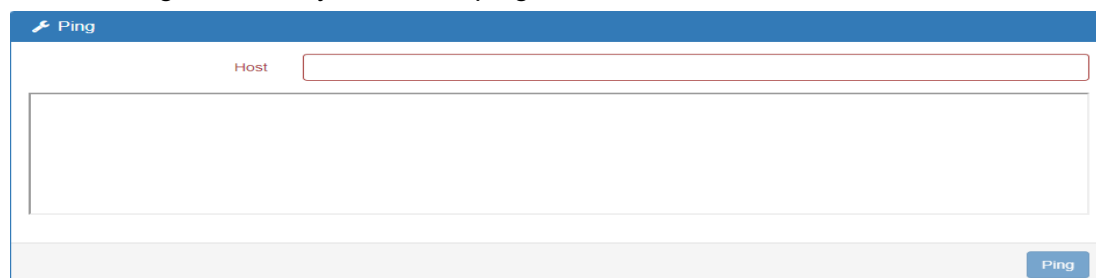
# 14 Configuration > Diagnosis

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



## 14.1 Diagnosis > Ping

Please assign the Host you want to ping.



The result of the ping is as below.

**Ping**

Host: 8.8.8.8

```

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=56 time=745.328 ms
64 bytes from 8.8.8.8: seq=1 ttl=56 time=343.289 ms
64 bytes from 8.8.8.8: seq=2 ttl=56 time=341.637 ms
64 bytes from 8.8.8.8: seq=3 ttl=56 time=341.180 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
  
```

Ping

## 14.2 Diagnosis > Traceroute

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

**Traceroute**

Host:

Traceroute

The result of the traceroute is as below.

**Traceroute**

Host: 8.8.8.8

```

traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 38 byte packets
1 ***
2 10.158.65.5 (10.158.65.5) 204.175 ms 37.861 ms 41.625 ms
3 10.158.67.7 (10.158.67.7) 39.770 ms 34.422 ms 39.602 ms
4 10.158.67.17 (10.158.67.17) 39.639 ms 38.743 ms 10.158.67.18 (10.158.67.18) 39.397 ms
5 tchn-3301.hinet.net (210.65.126.186) 41.858 ms 38.494 ms tchn-3302.hinet.net (210.65.126.190) 39.745 ms
6 tchn-3011.hinet.net (220.128.16.234) 42.402 ms 42.652 ms 39.585 ms
  
```

Traceroute

## 15 Configuration Applications

This section explains specific examples how to configure your applications.

### 15.1 WAN Priority

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

**Priority**

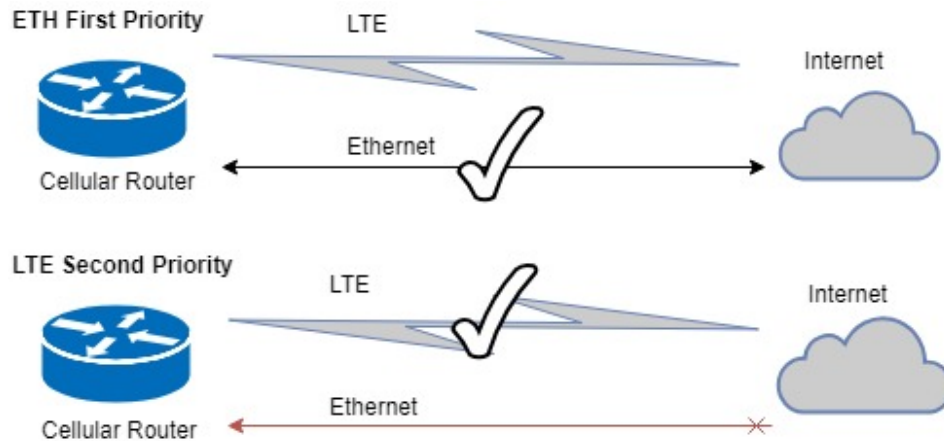
WAN Priority: ETH First

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

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

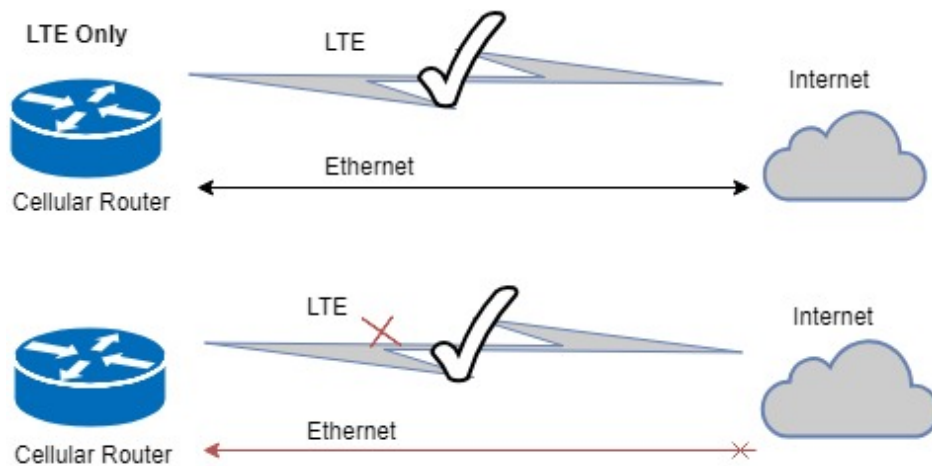
In case both Ethernet and LTE can access Internet, the router would route network packages through Ethernet. The reason is Ethernet that is low price and stable.

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



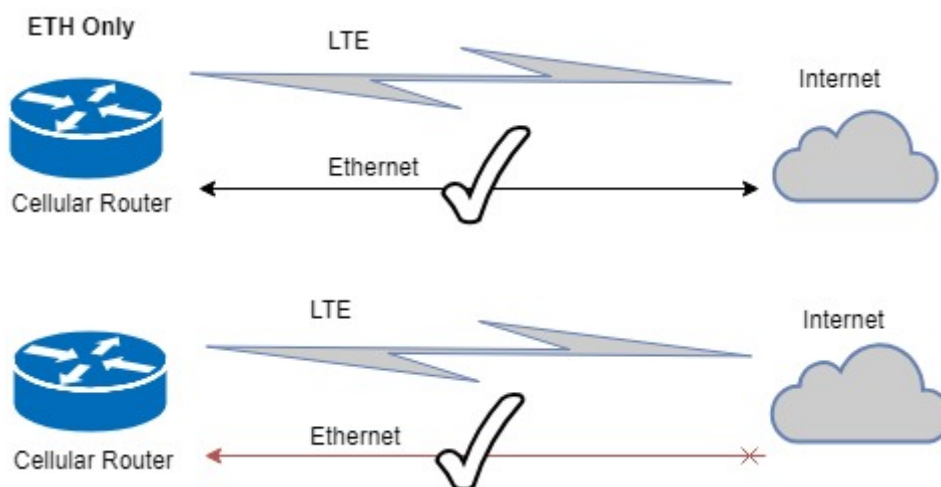
## (2) WAN Priority > LTE Only:

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



## (3) WAN Priority > ETH Only:

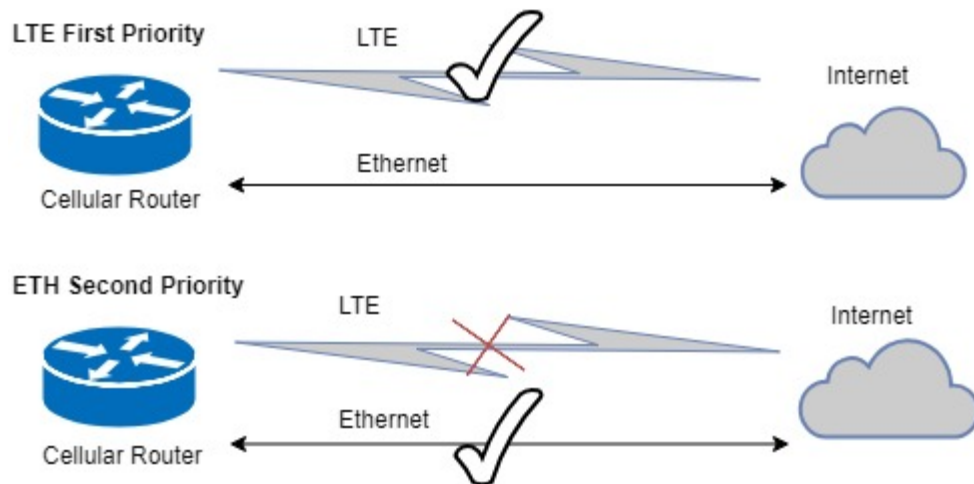
In this mode, the router only routes network packages through Ethernet.



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

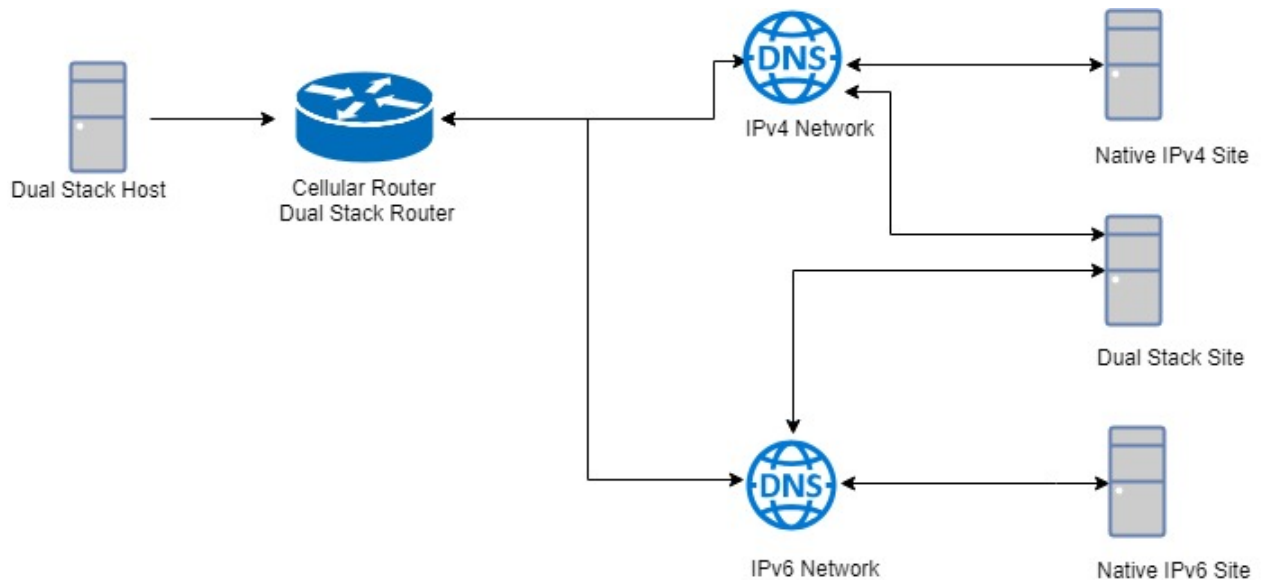
In case both Ethernet and LTE can access Internet, the router would route network packages through LTE.

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



## 15.2 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
IPv6 Address. . . . . : 2001:b400:e335:e5ca::101(Preferred)
Lease Expires . . . . . : Thursday, March 15, 2018 1:15:07 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

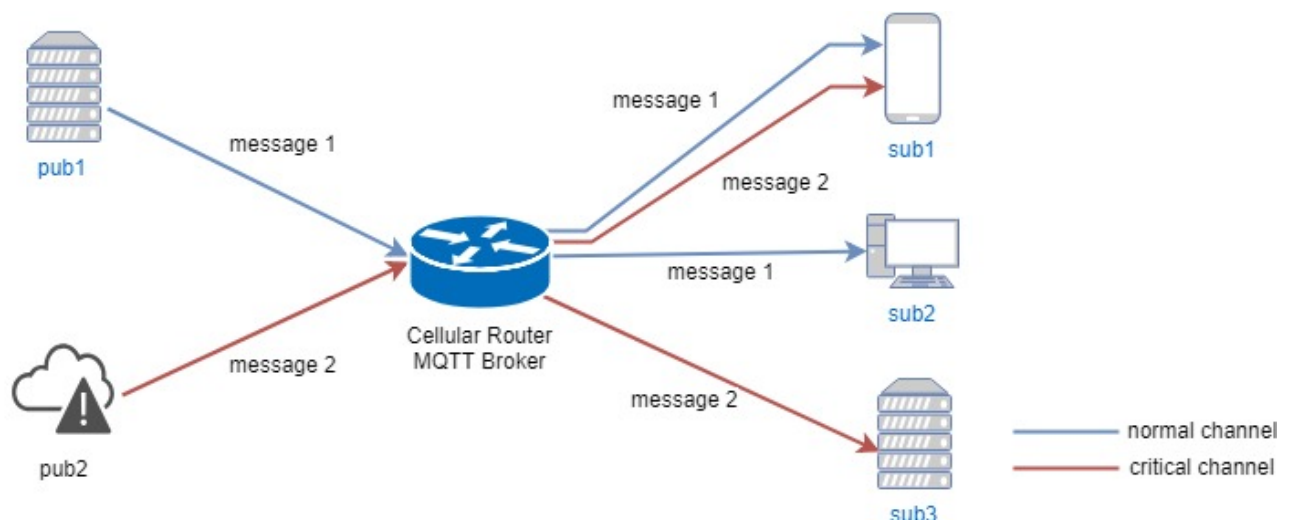
DNS Servers . . . . . : fe80::c2e:43ff:fe0d:4743%15
                          192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

C:\>
```

## 15.3 MQTT Broker

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

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



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



MQTT

Mode

☐ Disable ☒ Enable

Port

1883

Manage Users

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

Username

Password

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

## ACLs

User	Topic	Read	Write	Delete
Sub1	Critical	<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"/>

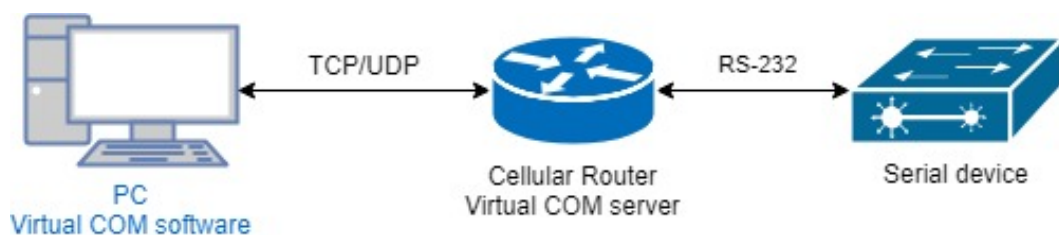
User:

Topic:

☐ Read
   
☐ Write

## 15.4 Virtual COM > Remote Management

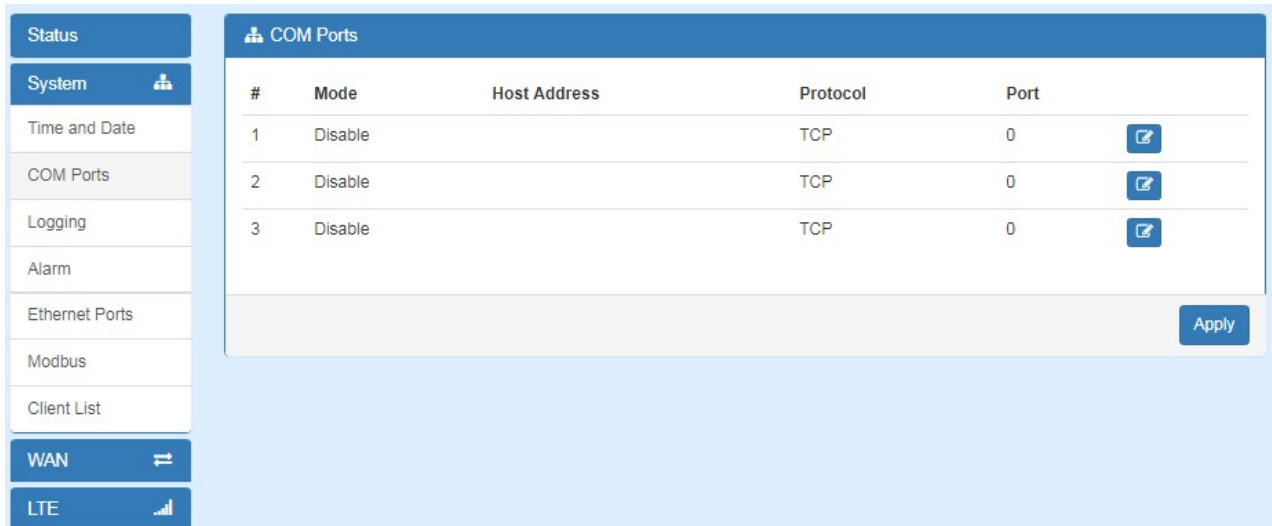
You can access the remote serial device (e.g. Console) by the Virtual COM server feature. When you set up the above environment, use the Virtual COM software (e.g. USB-VCOM) to simulate the COM device. After the simulation, the user can use the terminal tool (e.g. putty, tera term) to access the remote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



### • How to set up

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

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



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

**Edit COM Ports Entry #2**

Baud Rate: 115200

Data: 8 bit

Parity: none

Stop: 1 bit

Flow Control: none

☐ Is Console?

**Virtual COM**

Mode: Server

Protocol: TCP

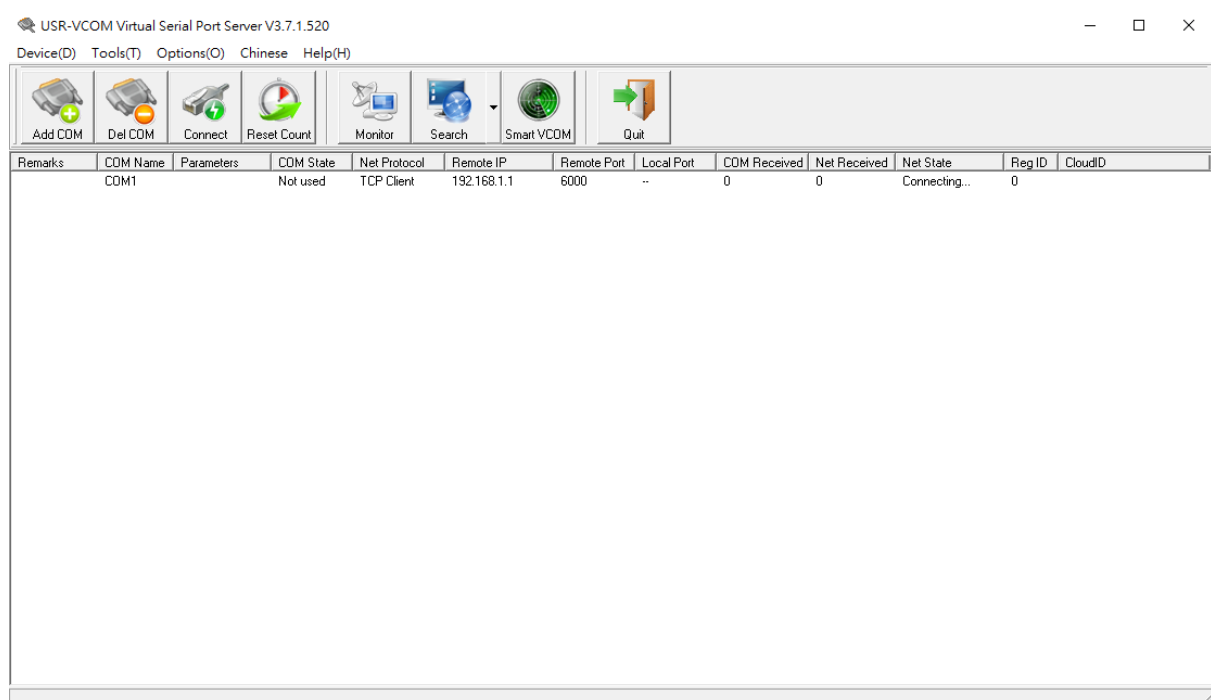
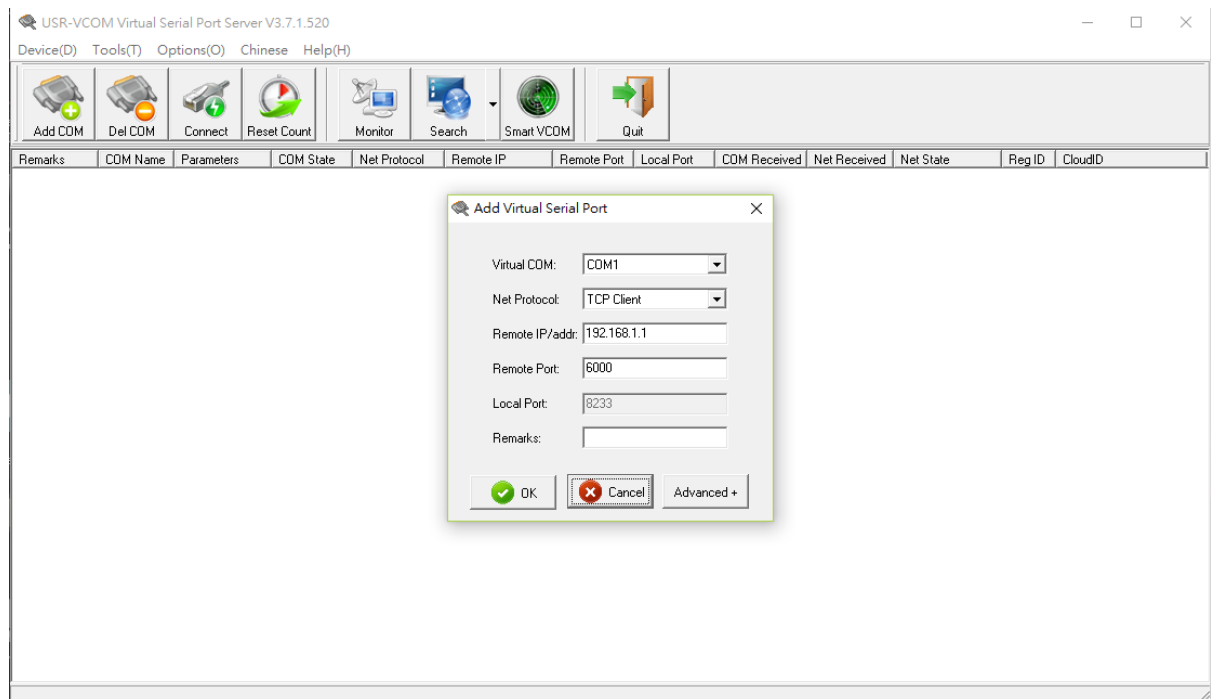
Redirect Port: 6000

Save

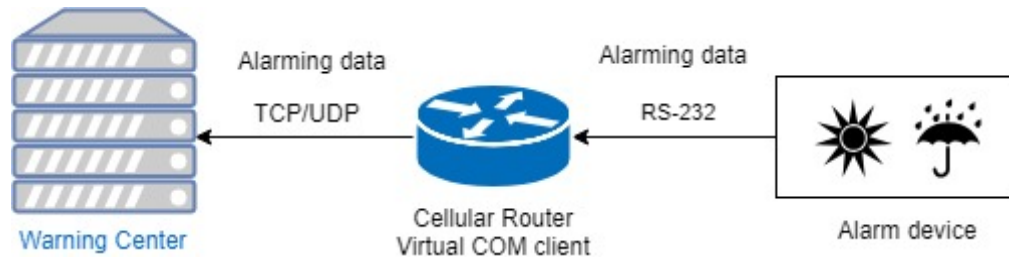
The configuration UI provides the serial setting and the Virtual COM setting.

- (1) For the serial setting, you need to change the setting like baud rate to fit the connected device.
- (2) For the Virtual COM, you need to change the mode to **Server** and specify the **Protocol**, **Port** to reach the remote management feature. (**Note:** In this case, we use the **TCP** and port **6000** to be the Virtual COM server settings.)
- (3) Click the **Close** and the **Apply** button. If all settings are correct, the web UI will display **Apply OK**.
- (4) Then you can open the Virtual COM software on PC. (**Note:** In this case, we use the **USR-VCOM** to be the Virtual COM software.)

- (5) And set up the virtual serial port by **192.168.1.1** (The default is LAN IP), **TCP client** and **Remote Port 6000** as the following picture.



## 15.5 Virtual COM > Remote Alarm



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

**Edit COM Ports Entry #2**

Baud Rate

115200

Data

8 bit

Parity

none

Stop

1 bit

Flow Control

none

☐ Is Console?

**Virtual COM**

Mode

Client

Host Address

192.168.1.2

Protocol

TCP

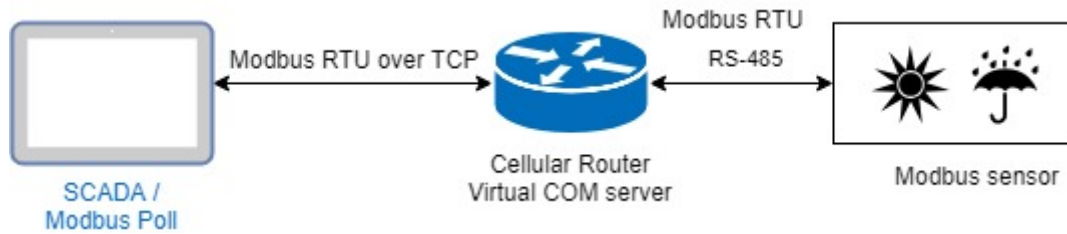
Redirect Port

6000

Save

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

## 15.6 Virtual COM > Modbus RTU over TCP



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

### Edit COM Ports Entry #3

Baud Rate	9600
Data	8 bit
Parity	none
Stop	1 bit
Flow Control	none
<input type="checkbox"/> Is Console?	

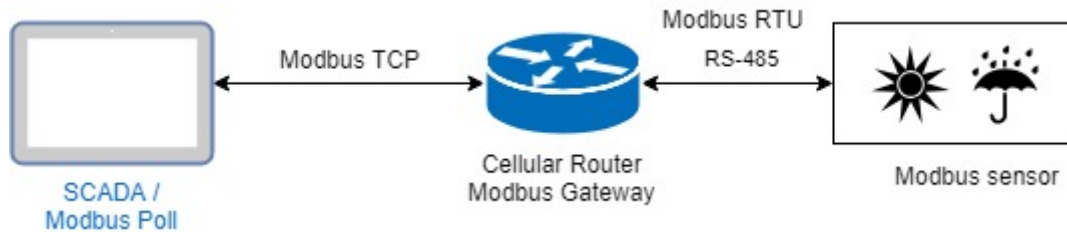
### Virtual COM

Mode	Server
Protocol	TCP
Redirect Port	6001

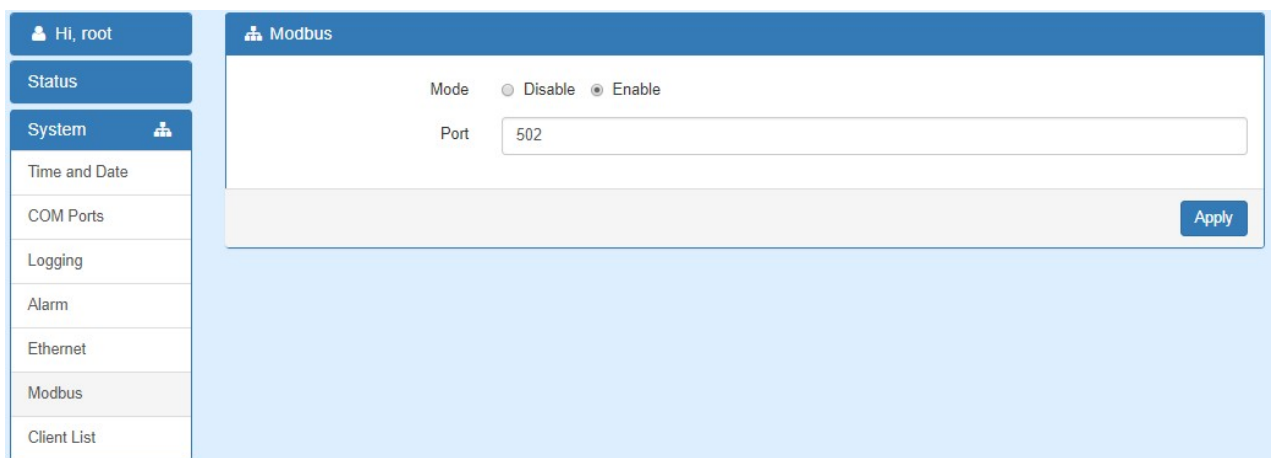
Save

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

## 15.7 Modbus Gateway



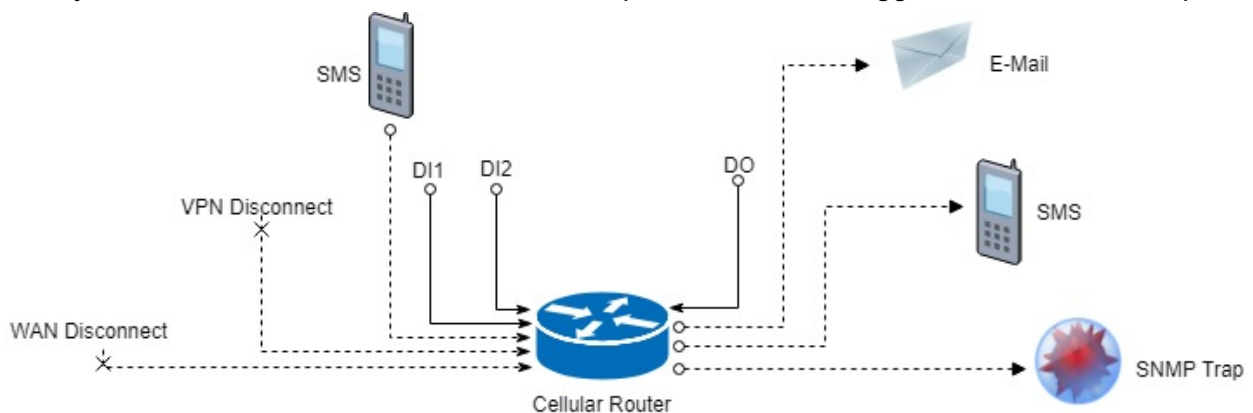
The Modbus gateway feature of router could convert the Modbus TCP to the Modbus RTU protocol and send it to the connected RS-485 device. This feature depends on the COM3 setting, you need to configure the serial setting in the **System -> COM ports** web UI and set up this feature in the **System ->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



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

## 15.8 Alarm Configuration

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



### (1) Alarm Input:

- The alarm would be triggered when DI1/DI2 show(s) high signal.

- The user's phone number is in device contact phone book can send a SMS to device SIM card to trigger alarm.
- VPN / WAN disconnect would trigger alarm no matter which interface is currently using.

## (2) Alarm Output:

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

Alarm

Mode ☒ Disable ☐ Enable

Alarm input

☒ SMS
☒ DI 1
☒ DI 2
☒ VPN disconnect
☒ WAN disconnect

☒ LAN disconnect
☒ Reboot

Alarm output

☒ SMS
☒ DO
☒ SNMP trap
☒ E-mail

DI 1 Trigger

☒ High ☐ Low

DI 2 Trigger

☒ High ☐ Low

DO behavior

☒ Always ☐ Pulse

Groups

Group ▼

SMS/E-mail

Limit 150 english characters

Group

Name	SUN	MON	TUE	WED	THU	FRI	SAT
g1				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Apply

SNMP

Mode ☐ Disable ☒ Enable

Community

SNMP v3 User Configuration

SNMP trap configuration

#	Mode	Community Name	Destination
1	Disable ▼	public	
2	Disable ▼	private	

Apply



## 15.9 OpenVPN Configuration

### Generic setup

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

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

### 15.9.1 OpenVPN Server Mode

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

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























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

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

### Server - Server Security

Root CA	 Create	 
Cert, Key	 Create	 Cert   Key 

### Server - User Security

User 1	<input checked="" type="checkbox"/> Valid	 Create	password for create 	 Cert 	 Key 	 P12 
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 			

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.

## 15.9.2 OpenVPN Client Mode





### OpenVPN client certificate import

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












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

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

Client - Security

Root CA	 Import
Cert	 Import
Key	 Import
P12	 Import

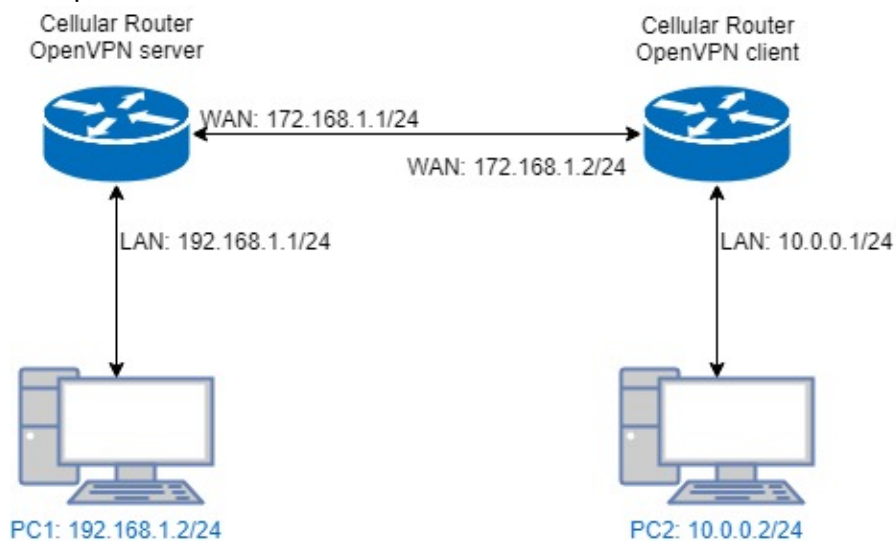
Client - Security

Root CA	 Import	 
Cert	 Import	 
Key	 Import	 
P12	 Import	 

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

### 15.9.3 OpenVPN Net-to-Net

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



#### (1) OpenVPN server configuration

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

Edit Open VPN Connection #1

Mode
☐ Disable
☒ Enable

VPN Mode
☒ Server
☐ Client
☐ Custom

TLS Mode
☒ Disable
☐ Enable

TLS minimal version
☒ none
☐ 1.0
☐ 1.1
☐ 1.2

Cipher

BF-CBC

Status
Running

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

Device
☒ TUN
☐ TAP

Protocol
☒ UDP
☐ TCP

Port

1701

VPN Compression
☒ Disable
☐ Enable

Authentication

Certificate

Server

Client Mode
☒ Roadwarrior

VPN Network

192.168.30.0

VPN Netmask

255.255.255.0

Roadwarrior

Route Client Networks
☐ Off
☒ On

Connections - Net / Mask

#1

10.0.0.0

/

255.255.255.0

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

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

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

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

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

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

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

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

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

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-----

MIIC5zCCAc8CAQEWdQYJKoZIhvcNAQELBQAwNDELMAkGA1UEBhMCQ0gxARBgNV  
BAoMCnN0cm9uZlN3YW4xEDAOBgNVBAMMB09wZW5WUE4wHhcNMTCwNTA5MDYzNDA4  
WhcNMicwNTA3MDYzNDA4WjA/MOswCOYDVOOGEwJDSDETMBECA1UECwKc3Rvb25n

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

## (2) OpenVPN client configuration

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

Edit Open VPN Connection #1

Mode
☐ Disable
☒ Enable

VPN Mode
☐ Server
☒ Client
☐ Custom

TLS Mode
☒ Disable
☐ Enable

TLS minimal version
☒ none
☐ 1.0
☐ 1.1
☐ 1.2

Cipher
BF-CBC

Status
Connected

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

Device
☒ TUN
☐ TAP

Protocol
☒ UDP
☐ TCP

Port
1701

VPN Compression
☒ Disable
☐ Enable

Authentication
pkcs #12 Certificate

Client

Client Mode
☒ Roadwarrior

Server Address
172.168.1.1

PKCS12 Password
1234567

Route Client Networks
☐ Off
☒ On

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

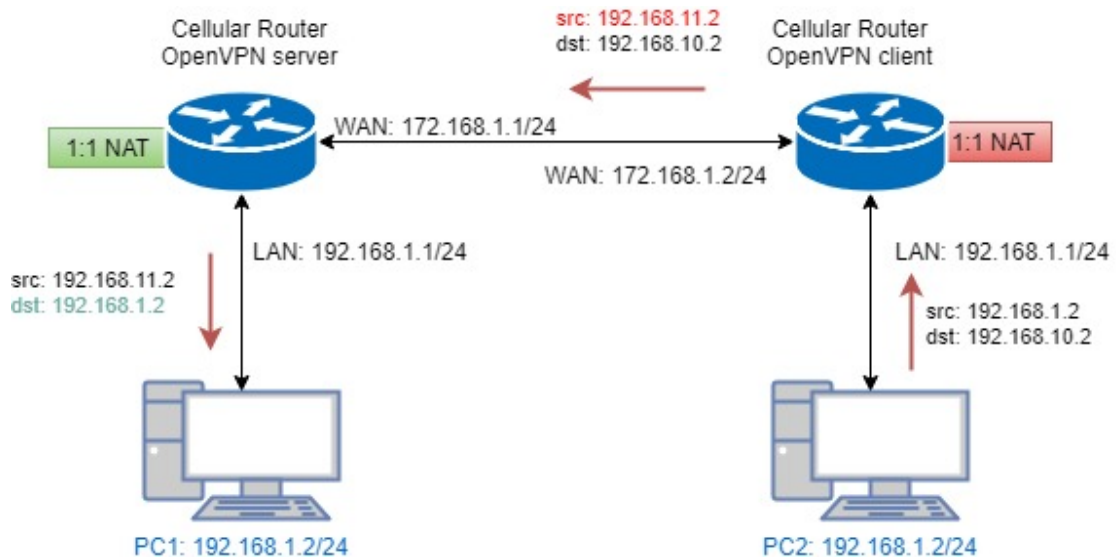
This option require the P12 file which generated from Generic Setup OpenVPN server part.

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

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

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

#### 15.9.4 OpenVPN 1:1 NAT



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

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

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

#### Roadwarrior

Route Client Networks ☐ Off ☒ On

Connections - Net / Mask

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

#### NAT

1:1 NAT ☐ Off ☒ On

Network 192.168.10.0

Netmask 255.255.255.0

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

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

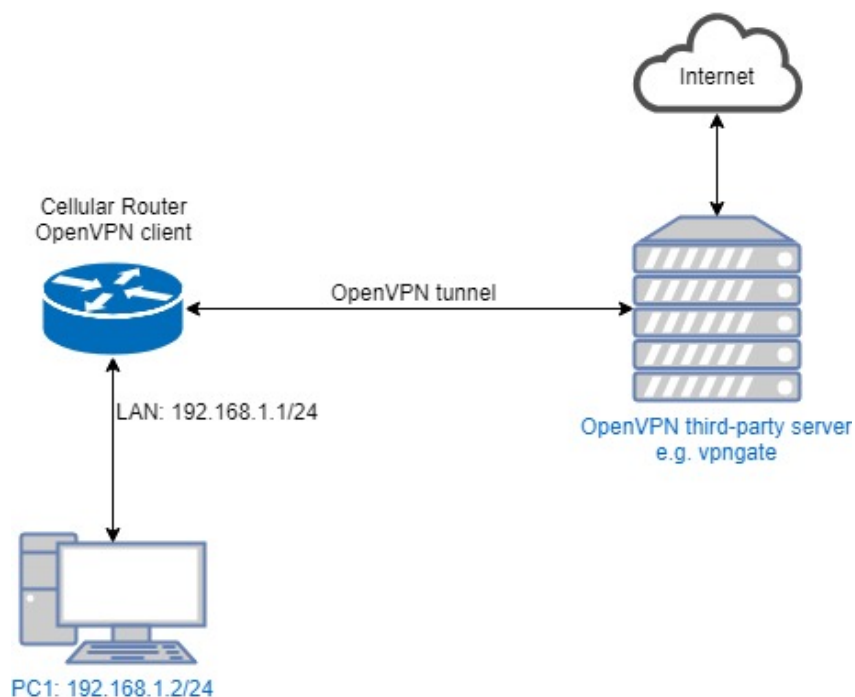
#### Client

Client Mode	<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"/>

### 15.9.5 OpenVPN with third-party server



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

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



For example, use the Japan OpenVPN server which provided by <http://www.vpngate.net/en/> . Firstly, download the .ovpn configuration files from vpngate.net. Additionally, use the OpenVPN custom import button to import it. The result is as the below figure. If the .ovpn configuration file is correct, the web UI will show **Apply OK**.

Edit Open VPN Connection #1

Mode

☐ Disable
☒ Enable

VPN Mode

☐ Server
☐ Client
☒ Custom

Custom Config

Import \*.ovpn

Status

Connected

IP

Connected since

10.211.1.5

2017-06-21 11:30:40

Back

Refresh

Apply

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

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

**VPN Gate**  
An academic experiment  
Public VPN relay servers  
Hosted by volunteers

Firewall Out of order by unknown reason  
Bypass FW  
Liberty!!

VPN Gate Client Domestic internet  
Target servers Overseas internet

[www.vpngate.net](http://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.  
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 \(Refreshed in real time\)](#)

### OpenVPN Access Server on Docker installation

OpenVPN Access Server is a full featured secure network tunneling VPN software solution that integrates OpenVPN server capabilities, enterprise management capabilities, simplified OpenVPN Connect UI, and OpenVPN Client software packages that accommodate Windows, MAC, Linux, Android, and iOS environments. OpenVPN 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 OpenVPN 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 OpenVPN Access Server by docker image

Reference: <https://hub.docker.com/r/linuxserver/openvpn-as/>

```
sudo mkdir -p /openvpn-as
```

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

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

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

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

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

```
sudo docker start openvpn-as
```

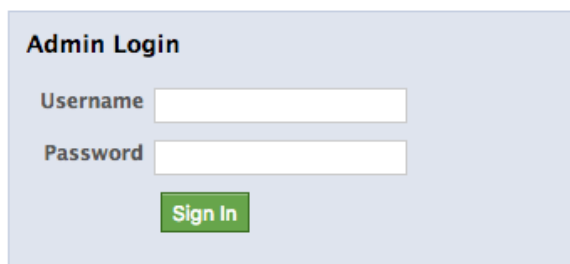
Check the OpenVPN Access Server by visiting [https://<server\\_ip\\_or\\_domain>:943](https://<server_ip_or_domain>:943)

### **Setup OpenVPN 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'. Below the 'Password' field is a green button with the text 'Sign In' in white.

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

OPENVPN™

Access Server

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

Fallover

User Management

User Permissions

Group Permissions

Revoke Certificates

Authentication

1. 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.)

**OPENVPN™**

Access Server

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: <input type="text" value="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 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"/>	
New Username: <input type="text" value="test"/>	No Default Group	Hide	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Local Password:  (No Password Set)

4.

Select IP Addressing :

☒ Use Dynamic
 ☐ Use Static

Access Control

Select addressing method:

☒ Use NAT
 ☐ Use routing

Allow Access To these Networks:

List subnets in network/nbits form

☐ all server-side private subnets
 

5. ☒ all other VPN clients

Allow Access From:

5.

☒ all other VPN clients

VPN Gateway

Configure VPN Gateway:

☒ No
 ☐ Yes

DMZ settings

Configure DMZ IP address:

☒ No
 ☐ Yes

☐ Require user permissions record for VPN access

6. 

Save Settings

### User Permissions Changed

User 'test' added.

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

7.

Update Running Server

### Setup Cellular Router OpenVPN client



Username

test

Password

....

Login

Go

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.



Connect

Logout

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

- [OpenVPN Connect for Windows](#)
- [OpenVPN Connect for Mac OS X](#)
- [OpenVPN Connect for Android](#)
- [OpenVPN Connect for iOS](#)
- [OpenVPN for Linux](#)

Connection profiles can be downloaded for:

- [Yourself \(user-locked profile\)](#)

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

**Edit Open VPN Connection #1**

Setting

Log

Mode

☐ Disable ☒ Enable

VPN Mode

☐ Server ☐ Client ☒ Custom

Custom Config

1.

2. Username

test

3. Password

test

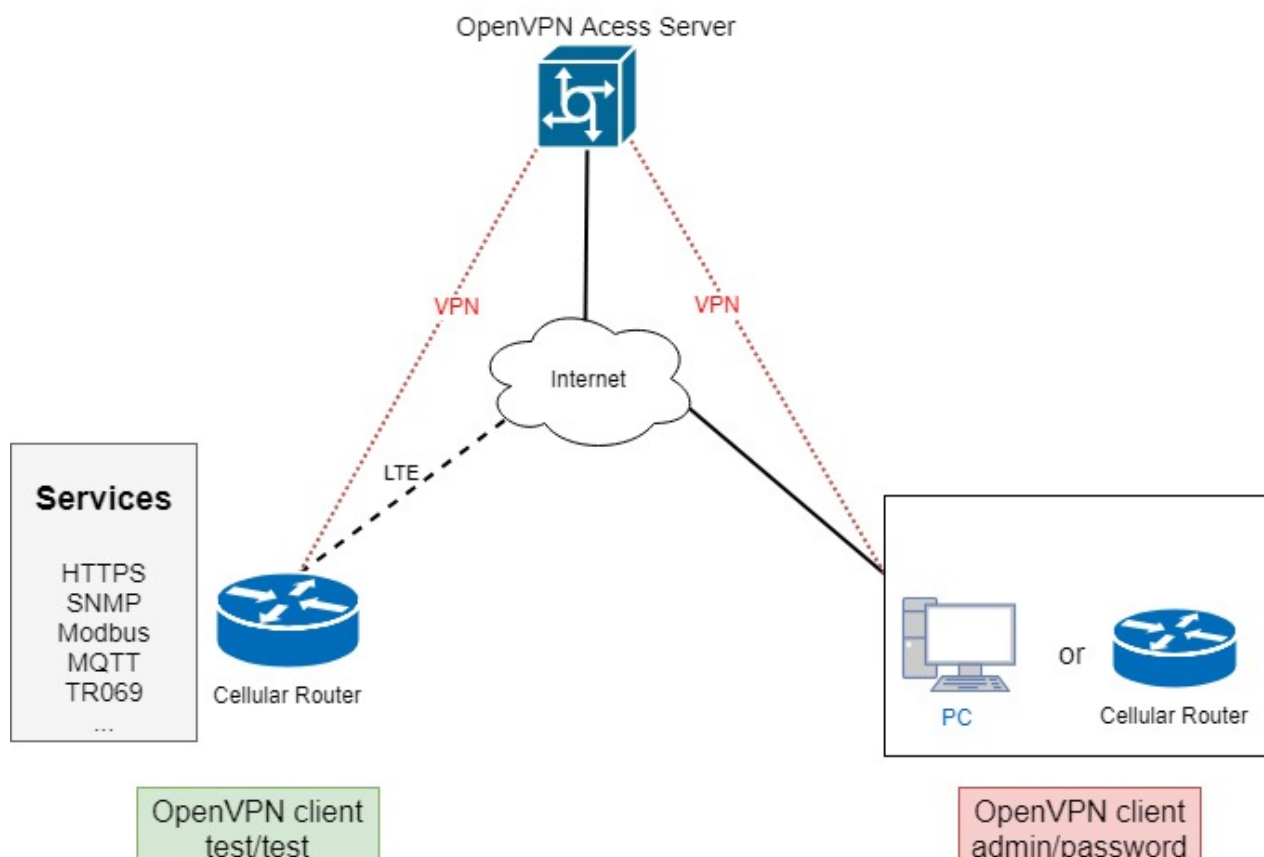
Status

Connected

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

4.

Upload the .ovpn configuration to Cellular Router OpenVPN 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.

## 15.9.7 Install Pritunl OpenVPN server on Docker

### Pritunl OpenVPN server on Docker installation

Pritunl is a distributed enterprise vpn server built using the OpenVPN 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 OpenVPN 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

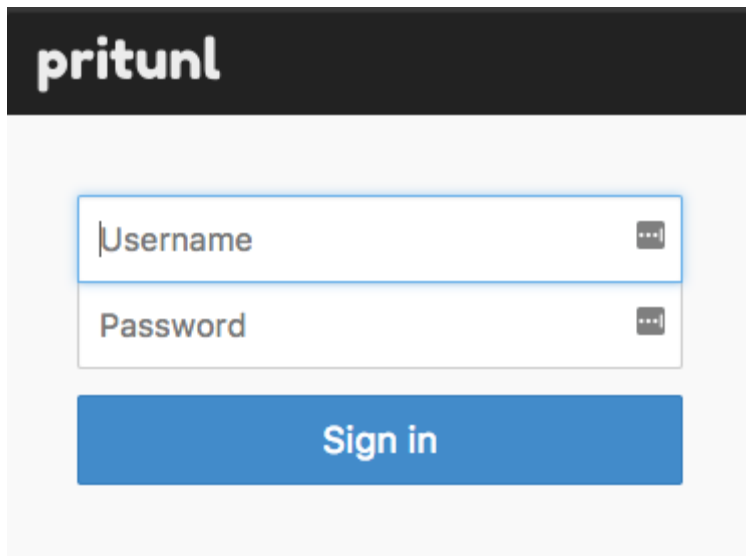
(4) Check the Pritunl OpenVPN Server by visiting `https://<server_ip_or_domain>`

### Setup Pritunl OpenVPN Server for Cellular Router

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

The default username/password is pritunl/pritunl.

Login Page:

The image shows the Pritunl login page. At the top, there is a black header with the 'pritunl' logo in white. Below the header, the page has a light gray background. In the center, there is a white login form with a blue border. The form contains two input fields: 'Username' and 'Password'. Each field has a small icon on the right side, likely for toggling password visibility. Below the input fields is a blue button with the text 'Sign in' in white.

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

### Initial Setup:

## Initial Setup



Username

prituul

New Password

Enter password

Public Address

60.250.198.239

Public IPv6 Address

Enter public address

Web Console Port

443

Lets Encrypt Domain

mrdrd.ddns.net

Setup Later

Save

### OpenVPN user setup

Please navigate to the User page to setup the OpenVPN user account.

Add the organization by click the Add Organization button.

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

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

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

### Users and Organizations

Add Organization Add User Bulk Add Users Delete Selected

Successfully added organization. ✕

Organization	MR	0 users	Search for user	Delete Organization
There are no users in this organization				

Then add the OpenVPN user by click the Add User button.

### Add User ✕

Name

Select an organization

Email (optional)

Pin

Cancel Add

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

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

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

### Users and Organizations

Add Organization Add User Bulk Add Users Delete Selected

Successfully added organization. ×

Successfully added user. ×

Organization MR 1 users Search for user Delete Organization

☐ test Offline

## OpenVPN server setup

Please navigate to the Server page to setup the OpenVPN server.

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

### Servers

Add Server Add Route Attach Organization

There are no servers on this host.

And click the Add Server button to create the OpenVPN server.

### Add Server

Advanced ×

Name **Name of VPN server**

DNS Server

Port Protocol

Virtual Network  
 **253 Users**

☐ Enable IPv6 ☐ Enable Two-Step Authentication

Cancel Add

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

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

The screenshot shows the Pritunl web interface. At the top, there's a navigation bar with 'pritudl' logo, 'Dashboard', 'Users', 'Servers' (active), 'Upgrade to Enterprise!', 'Logs', 'Settings', and 'Logout'. Below the navigation bar, the 'Servers' page is displayed. A green notification bar at the top says 'Successfully added server.' with a close button. The main content area shows a server named 'router' with a status of 'Offline'. To the right of the server name are buttons: 'Add Server', 'Add Route', and 'Attach Organization'. Below the server name, there's a message: 'Server must have an organization attached'. To the right of this message are 'Start Server' and 'Delete Server' buttons. The server details are listed on the left: Status (Offline), Uptime (-), Users (-/- users online), Devices (0 devices online), Network (192.168.234.0/24), Port (17470/udp), and Multiple Devices (Disabled). On the right, there's a 'Server Output' tab and a 'Bandwidth Graphs' tab. Below these, there's a list of routes: '0.0.0.0/0' with a 'Remove Route' button, and '192.168.234.0/24' with a 'Virtual Network' button and a 'Remove Route' button. At the bottom, a message says 'There are no organizations attached to this server.'

And click Attach Organization button to setup the OpenVPN server.

The screenshot shows the 'Attach Organization' dialog box. It has a title bar with 'Attach Organization' and a close button. The main content area has two sections: 'Select an organization' with a dropdown menu showing 'MR', and 'Select a server' with a dropdown menu showing 'router'. At the bottom right, there are two buttons: 'Cancel' and 'Attach'.

Start the OpenVPN server by click Start Server button.

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

## Servers

Add Server Add Route Attach Organization

Successfully added server. ×

Successfully attached organization. ×

**Server** router **Start Server** Delete Server

**Status** Offline **Server Output** Bandwidth Graphs

**Uptime** -

**Users** 0/1 users online

**Devices** 0 devices online

**Network** 192.168.234.0/24

**Port** 17470/udp

**Multiple Devices** Disabled

0.0.0.0/0 Remove Route

192.168.234.0/24 Virtual Network Remove Route

MR Detach Organization

### Cellular Router setup


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

**pritul** 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 Offline 

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

And visit the Cellular Router OpenVPN custom page then import the .ovpn file.  
Fill up the username/password which be setup in OpenVPN 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	Connected since
192.168.235.2	2017-08-16 16:04:16

Back

Refresh

Apply

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

pritu
Dashboard
Users
Servers
Upgrade to Enterprise!
Logs
Settings
Logout

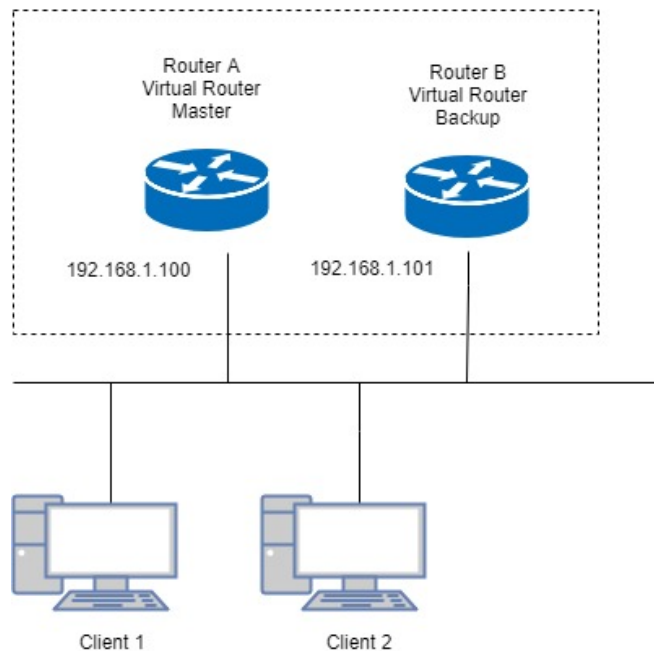
Users and Organizations
Add Organization
Add User
Bulk Add Users
Delete Selected

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

## 15.10 VRRP Topology

### Basic VRRP Topology



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

## 15.11 TR069 Server (GenieACS Installation)

Server OS: Ubuntu 14.04 on Virtualbox

### Installation:

- 1) Login ubuntu
- 2) Change to root by 'su -' and enter your root password.
- 3) Install required package as below command:  
`>apt install gcc openssl-devel zlib-devel readline-devel sqlite-devel`
- 4) Make a directory for application installation  
`>mkdir /opt`
- 5) Install yaml  
`cd /opt`  
`wget http://pyyaml.org/download/libyaml/yaml-0.1.7.tar.gz`  
`tar 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 xvzf uby-2.4.1.tar.gz
cd ruby-2.4.1
./configure
make && make install
ruby -v
ruby 2.4.1p111 (2017-03-22 revision 58053) [i686-linux]
```

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

#### 7) Install node.js

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

#### 8) Install redis

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

#### 9) Install mongodb

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

#### 10) Install genieACS

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

```
npm run configure
npm run compile
```

### **Modify FS\_HOSTNAME field in genieacs/config/config.json for device retrieve firmware file**

Original configuration:

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

New configuration example.:

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

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

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

Original configuration:

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

New configuration example:

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

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

### 11) Install genieACS-Gui

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

```
gem install json
bundle update
```

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

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

```
cp graphs-sample.json.erb graphs.json.erb
```

### **GenieACS startup script:**

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

```
GENIE_PATH=/opt/genieacs/bin
```

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

```
echo "start mongod."
```

```
pidof mongod
```

```
if [ $? != 0 ]; then
```

```
/opt/mongodb-linux-i686-3.3.3/bin/mongod --dbpath /data/db --journal --storageEngine=mmapv1
```

```
--fork --syslog
```

```
fi
```

```
echo "start North Bound/RESTful Interface service."
```

```
$GENIE_PATH/genieacs-nbi &
```

```
echo "start ACS/CWMP service."
```

```
$GENIE_PATH/genieacs-cwmp &
```

```
echo "start HTTP/File streaming service."
```

```
$GENIE_PATH/genieacs-fs &
```

```
echo "start GenieACS/WebUI."
```

```
cd $GENIE_GUI_PATH
```

```
rails server -b 0.0.0.0
```

### **GenieACS stop:**

Ctrl-C

### **Usage:**

#### 1) Device Configuration

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

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

+

TR069

Mode

☐ Disable
☒ Enable

ACS URL

http://192.168.0.105:7547

ACS Username

cpe

ACS Password

cpe

Periodic Inform

☐ Disable
☒ Enable

Periodic Inform Interval(Sec)

1800

Connection Request Username

tr069

Connection Request Password

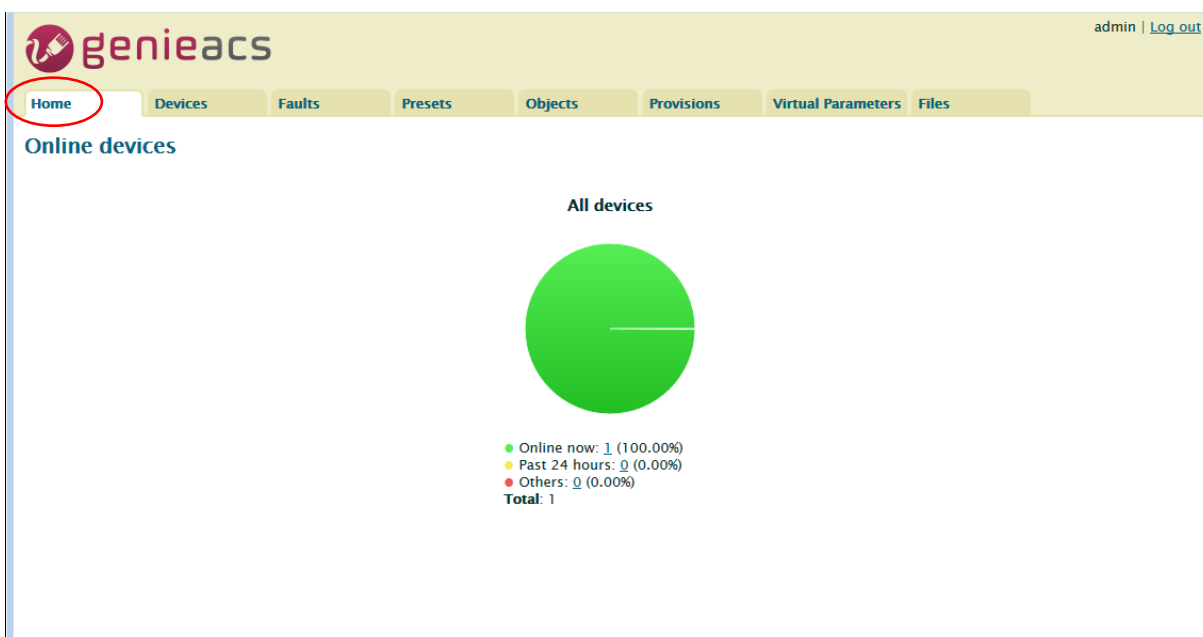
tr069

Apply

## 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.

genieacs [Log in](#)

Home

**Log in**

Username

Password

[Log in](#)

### 3) Device information

Press Devices tab

genieacs admin | [Log out](#)

Home **Devices** Faults Presets Objects Provisions Virtual Parameters Files

**Listing devices**

Filters  
+

[Filter](#) [Clear](#)

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

[Download](#)

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	<a href="#">Show</a>

[Download](#)

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

genieacs admin | Log out

Home Devices **Faults** Presets Objects Provisions Virtual Parameters Files

Device: 00304F-999999999999

Tags: +

Last inform: 12 minutes ago — Refresh, Ping

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

Task queue

Task	Time	Fault code	Fault message	Fault detail	Retries
Empty					

Device parameters

Type to search...

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

Reboot  
 Factory reset  
 Push file »  
 Add Firmware  
 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 [Refresh](#)
- InternetGatewayDevice.DeviceInfo.SoftwareVersion 0136000215129837
- InternetGatewayDevice.DeviceInfo.ProvisioningCode blank

##### For Readable and Writable parameter

- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.15.dport\_begin 0
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.15.dport\_end 0
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.16
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.16.mode off [Edit](#) [Refresh](#)
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.16.description blank
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.16.protocol tcp
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.16.sport\_begin 0

#### 4.1) Get parameter value

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

genieacs admin | Log out

Home Devices Faults Presets Objects Provisions Vi

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: 0136000215129837  
IP: 192.168.0.89 — Edit

Task queue

Task	Time	Fault code	Fault message	Fault detail	Retries
Empty					

Device parameters

Type to search...

- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.15.protocol tcp
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.15.sport\_begin 0
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.15.sport\_end 0
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.15.dest 0.0.0.0
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.15.dport\_begin 0
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.15.dport\_end 0
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.16
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.16.mode off
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.16.description blank
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.16.protocol tcp
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.16.sport\_begin 0
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.16.sport\_end 0

Reboot  
Factory reset  
Push file >  
Add Firmware  
Delete

Press Commit to get this parameter value.

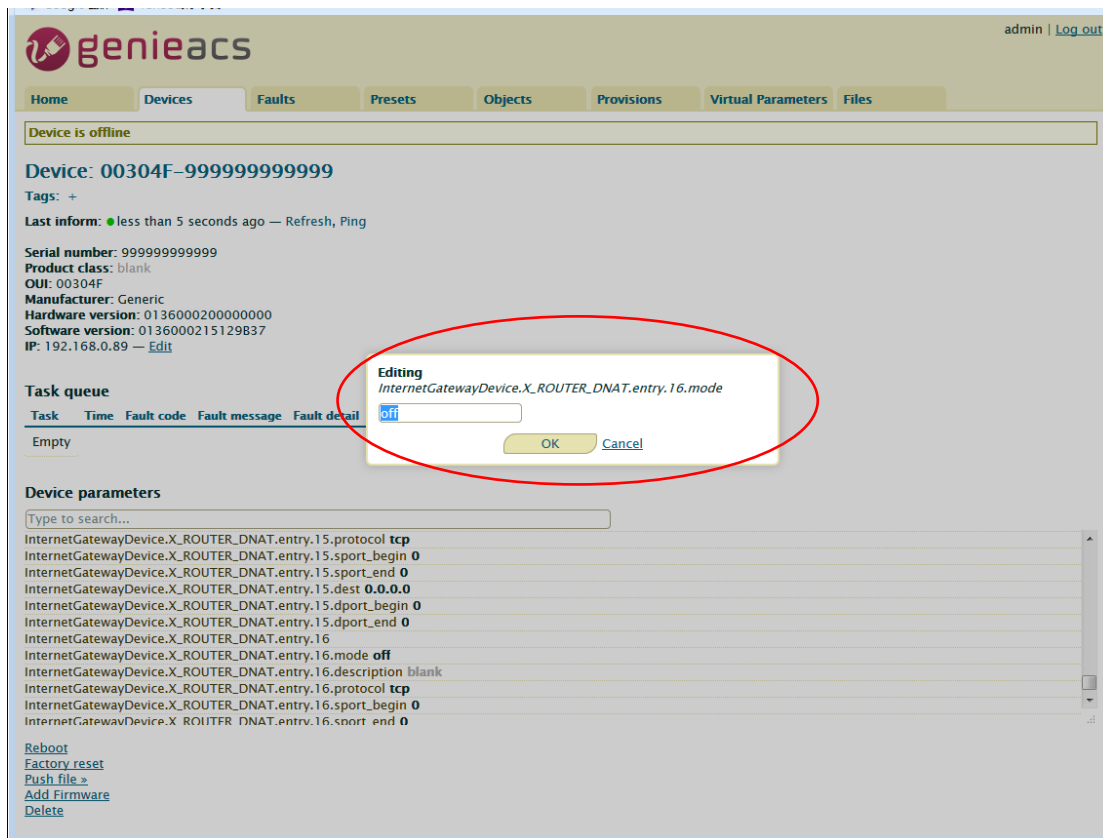
**Note:** If the GenieACS can reach the device, the parameter value will be updated immediately. Otherwise, this request will be queued on Task queue list until next time device connect to GenieACS.

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

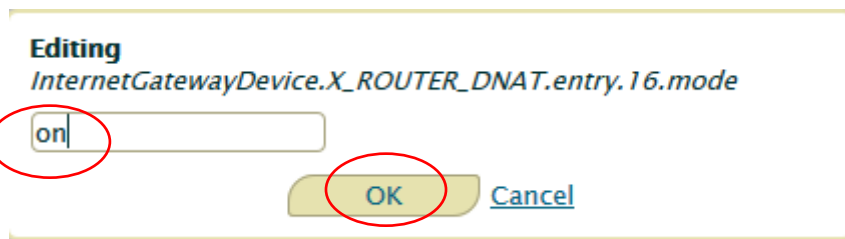
**Note:** To update partial tree, refresh the parent node of the partial tree.

#### 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.

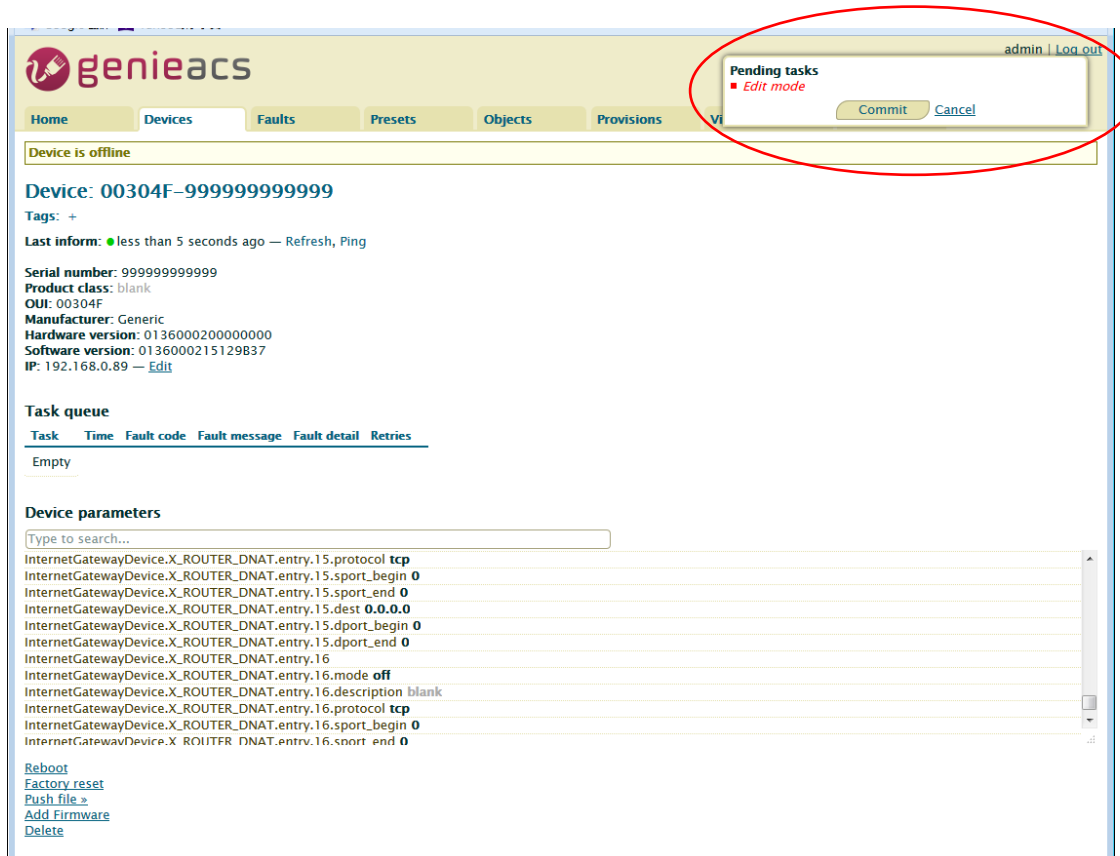


Input new value and press OK.



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





Press Commit to set this parameter value.

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

## 5) Reboot device

Press on [Reboot](#) link.

genieacs admin | [Log out](#)

Home Devices **Faults** Presets Objects Provisions Virtual Parameters Files

**Device:** 00304F-Mobile%20Router-99999999999

Tags: +

Last inform: about 2 hours ago — Refresh, Ping

Serial number: 99999999999  
 Product class: Mobile Router  
 OUI: 00304F  
 Manufacturer: Generic  
 Hardware version: 0136000200000000  
 Software version: 0136000215129839  
 IP: 192.168.0.89 — [Edit](#)

**Task queue**

Task	Time	Fault code	Fault message	Fault detail	Retries
Empty					

**Device parameters**

Type to search...

- InternetGatewayDevice
- InternetGatewayDevice.DeviceSummary InternetGatewayDevice:1.4[]@Baseline:1,Eth...
- InternetGatewayDevice.DeviceInfo
- InternetGatewayDevice.DeviceInfo.SpecVersion 1.0
- InternetGatewayDevice.DeviceInfo.HardwareVersion 0136000200000000
- InternetGatewayDevice.DeviceInfo.SoftwareVersion 0136000215129839
- InternetGatewayDevice.DeviceInfo.ProvisioningCode blank
- InternetGatewayDevice.DeviceInfo.Manufacturer Generic
- InternetGatewayDevice.DeviceInfo.UpTime 3920 (1:5:20)
- InternetGatewayDevice.DeviceInfo.AdditionalSoftwareVersion V1.51
- InternetGatewayDevice.DeviceInfo.ModemFirmwareVersion EC25EFAR02A06M4G
- InternetGatewayDevice.DeviceInfo.SerialNumber 99999999999

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

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

admin | [Log out](#)

**Pending tasks**

- Reboot

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

Provisions Vi

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

admin | [Log out](#)

Home Devices **Faults** Presets Objects Provisions Virtual Parameters Files

**Device: 00304F-Mobile%20Router-99999999999**

Tags: +

Last inform: about 2 hours ago — Refresh, Ping

Serial number: 99999999999  
 Product class: Mobile Router  
 OUI: 00304F  
 Manufacturer: Generic  
 Hardware version: 0136000200000000  
 Software version: 0136000215129839  
 IP: 192.168.0.89 — [Edit](#)

**Task queue**

Task	Time	Fault code	Fault message	Fault detail	Retries
Empty					

**Device parameters**

Type to search...

InternetGatewayDevice  
 InternetGatewayDevice.DeviceSummary InternetGatewayDevice:1.4[] (Baseline: 1, Eth...  
 InternetGatewayDevice.DeviceInfo  
 InternetGatewayDevice.DeviceInfo.SpecVersion 1.0  
 InternetGatewayDevice.DeviceInfo.HardwareVersion 0136000200000000  
 InternetGatewayDevice.DeviceInfo.SoftwareVersion 0136000215129839  
 InternetGatewayDevice.DeviceInfo.ProvisioningCode blank  
 InternetGatewayDevice.DeviceInfo.Manufacturer Generic  
 InternetGatewayDevice.DeviceInfo.UpTime 3920 (1:5:20)  
 InternetGatewayDevice.DeviceInfo.AdditionalSoftwareVersion V1.51  
 InternetGatewayDevice.DeviceInfo.ModemFirmwareVersion EC25EFAR02A06M4G  
 InternetGatewayDevice.DeviceInfo.SerialNumber 99999999999

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

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: 0136000215129839

File: [Browse...](#) m300.img

[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	0136000215129839

[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](#)

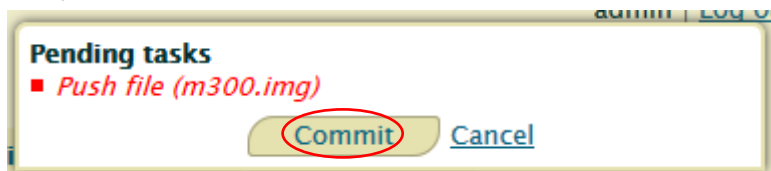
[Factory reset](#)

[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.

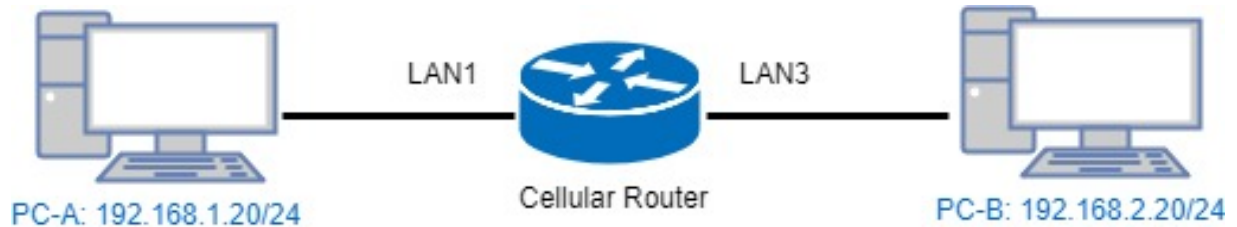


Press Commit, then firmware upgrade started.

**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.

## 16 Test Case Example

### 16.1 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

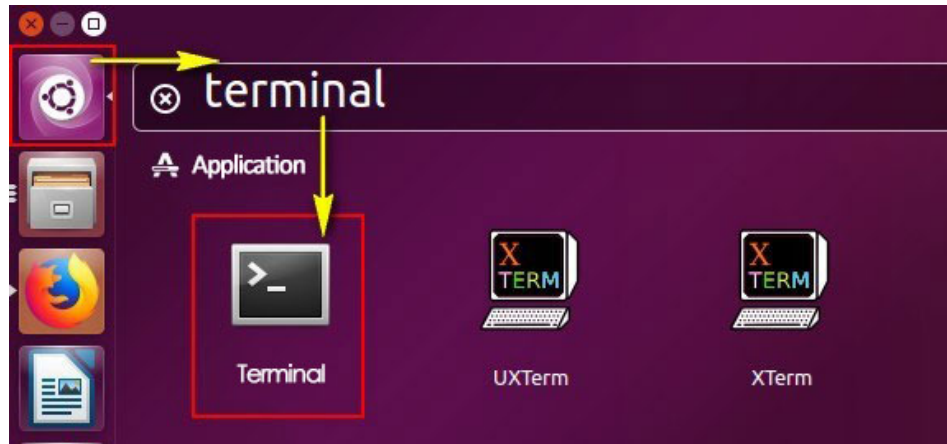
Mode
Off
Tag Base
Port Base

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	--

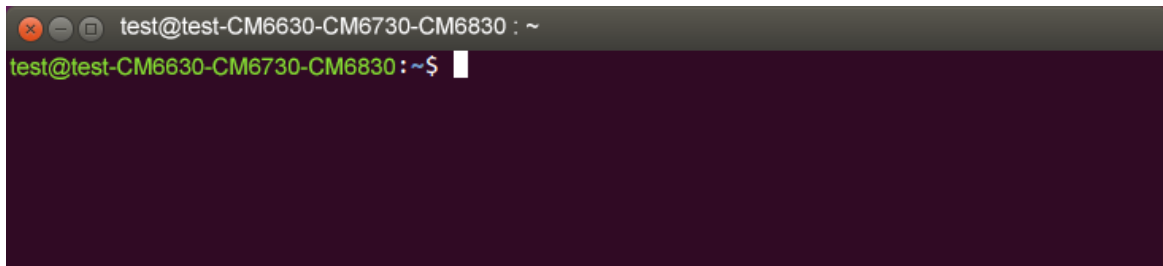
Apply

**Note:**

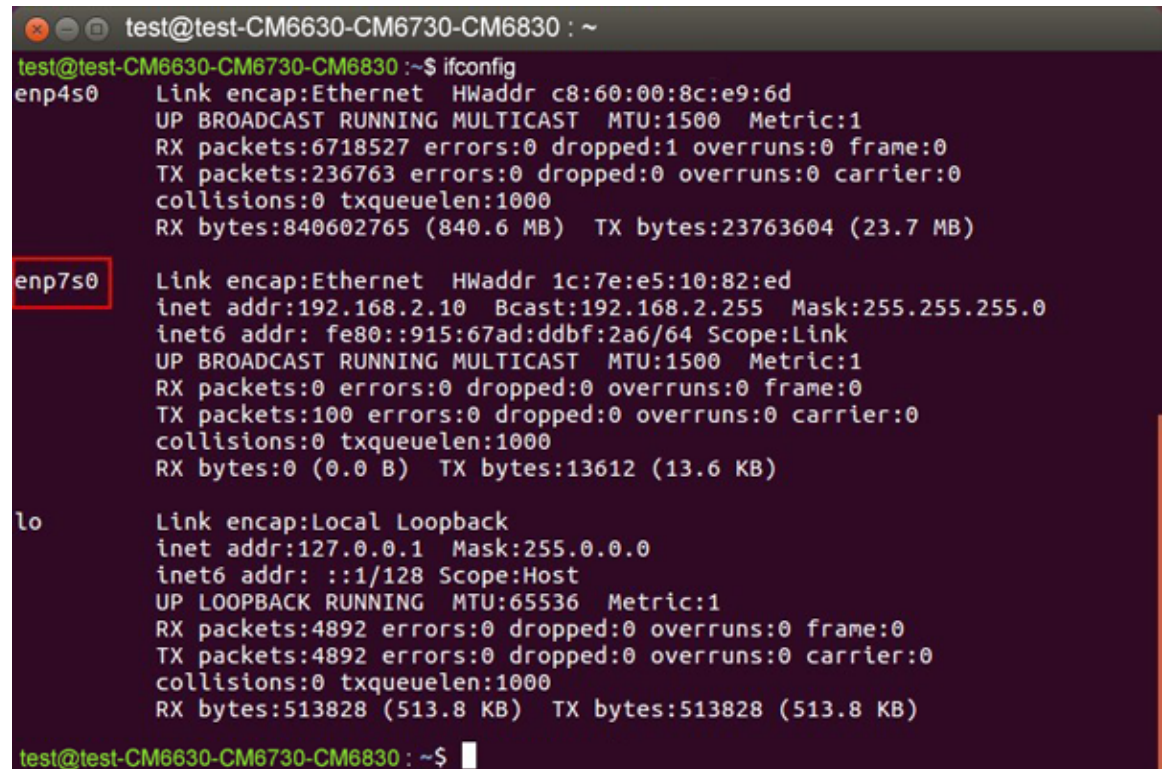
- Different PCs have different interface of network cards, like PC-A network card is eth1.10 for example 1 and PC-B network card is eth1.20 for example 2.
- How to find out the terminal and the interface of network cards based on different PCs.
  - From the following picture, you can click *the finding 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)**

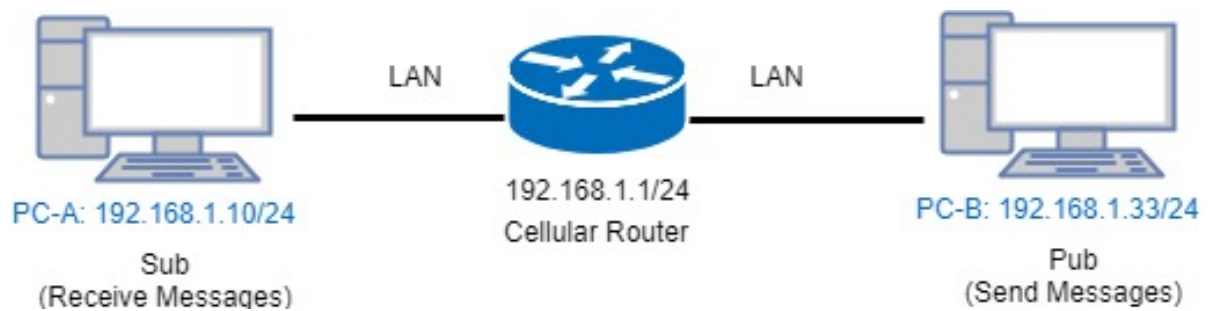
For PC-B, add default gateway and LAN's MAC to ARP

- 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.



## 16.2 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 libwscodec3 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

Manage Users

	Username	Password	Delete
	<input type="text" value="test"/>	<input type="password" value="...."/>	<input type="button" value="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	Read	Write	Delete
User	test			
Topic	abc			
		<input checked="" type="checkbox"/> Read	<input type="checkbox"/> Write	

Add

## ACLs

User	Topic	Read	Write	Delete
test	abc	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

User:

Topic:

☐ Read

☒ Write

## ACLs

User	Topic	Read	Write	Delete
test	abc	<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:

☐ Read

☐ Write

### Note:

- For Receive message command format:  
Mosquitto\_sub -h <SF300 IP> -t <Topic> -u <username> -P <password>
- For Send message command format:  
Mosquitto\_pub -h <SF300 IP> -t <Topic> -u <username> -P <password> -m <message>

- Step3: There are two test MQTT examples.

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

For PC-B, command "mosquitto\_sub -h 192.168.1.1 -t abc -u test2 -P test2".

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

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

Windows IP Configuration

Ethernet adapter Blue:

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

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

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

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

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

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

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

Windows IP Configuration

Ethernet adapter Blue:

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

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

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

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

```
test@test: ~  
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.

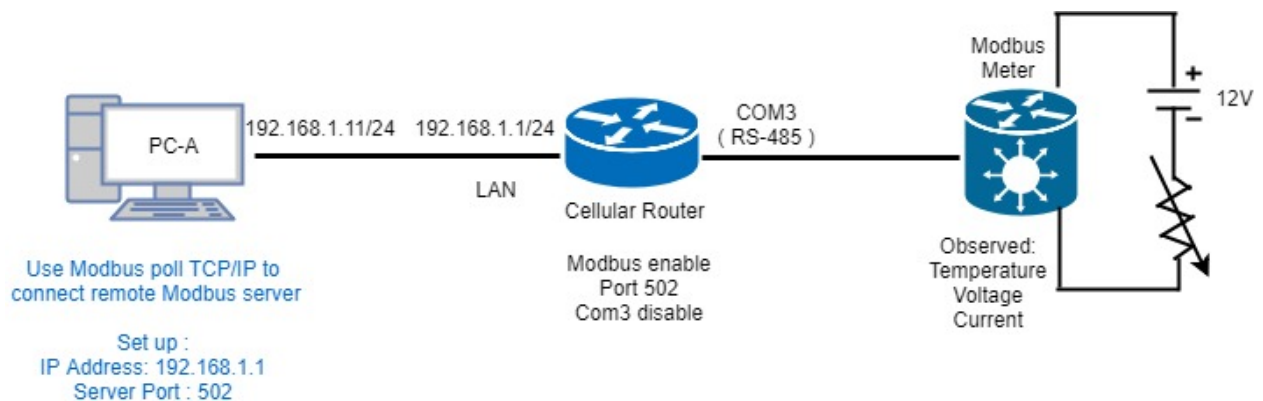
```
Command Prompt (1)  
C:\Program Files (x86)\mosquitto>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Blue:  
  
    Connection-specific DNS Suffix  . :  
    IPv6 Address. . . . . : 2001:b400:e335:e5ca::101  
    Link-local IPv6 Address . . . . . : fe80::8c61:e319:2e70:1140%15  
    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
```



## 16.3 Modbus Topology

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



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

### Modbus

Mode ☐ Disable ☒ Enable

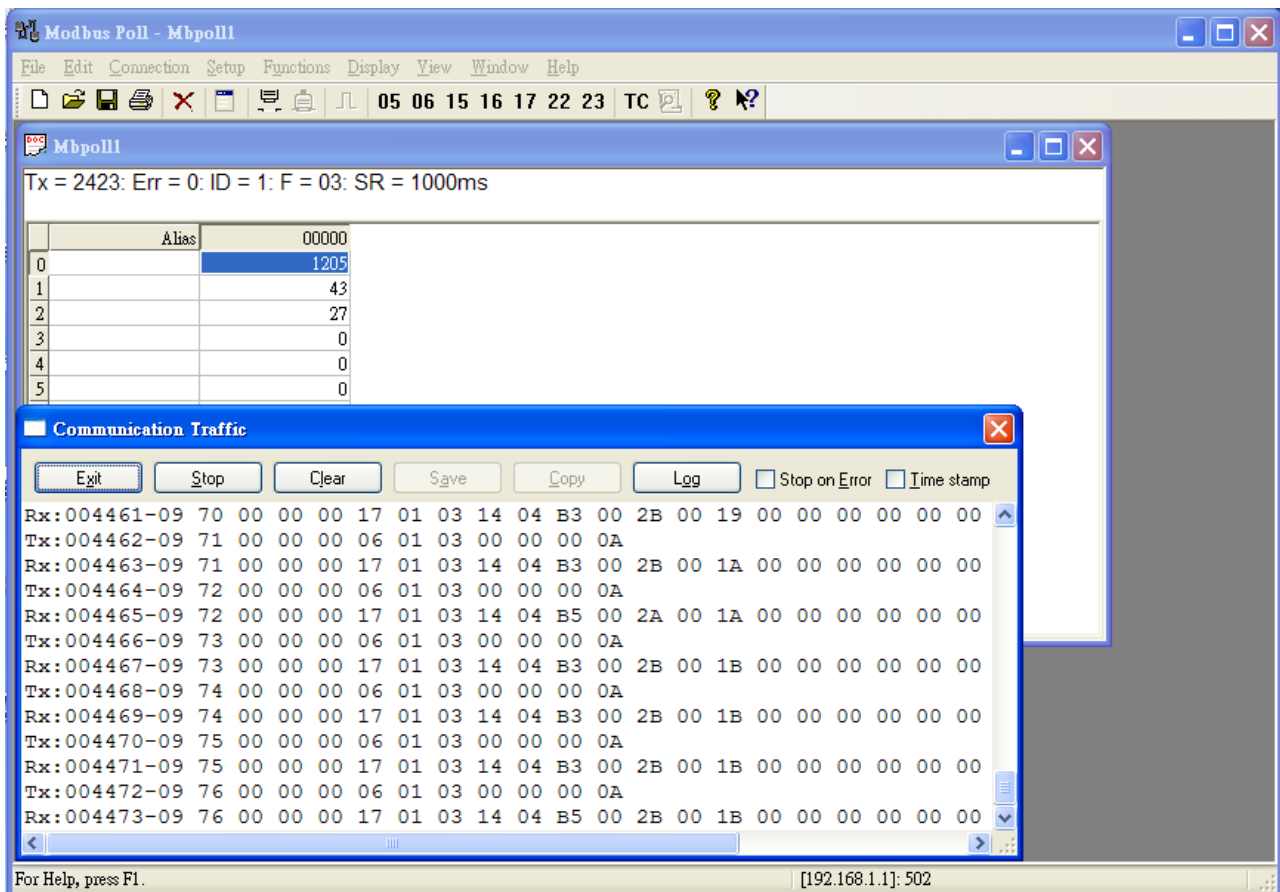
Port

Apply

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

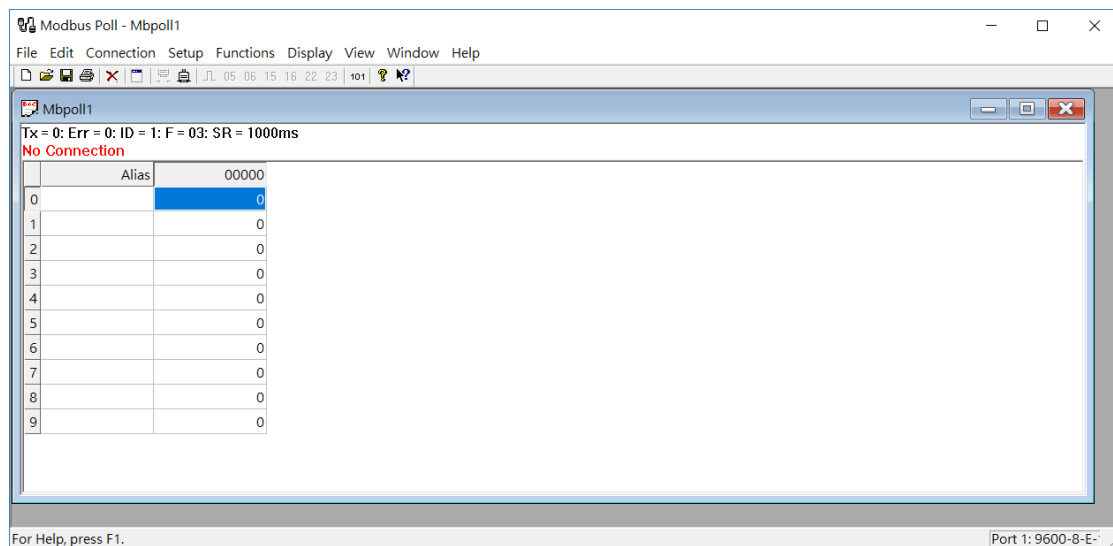
COM Ports				
#	Mode	Host Address	Protocol	Port
1	Disable		TCP	0
2	Disable		TCP	0
3	Disable		TCP	0

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



### Note 1:

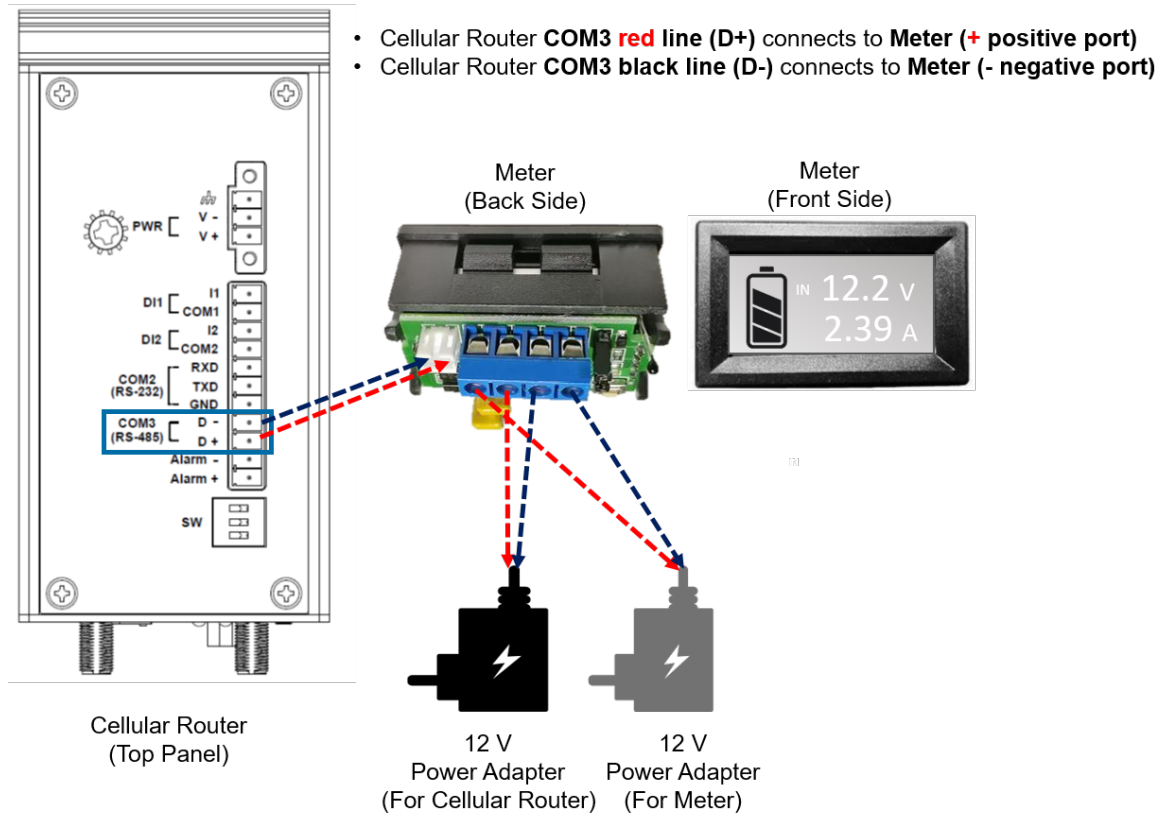
- There is a reference for Modbus poll software to download and install on PC.  
<http://www.tucows.com/preview/502459/Modbus-Poll>



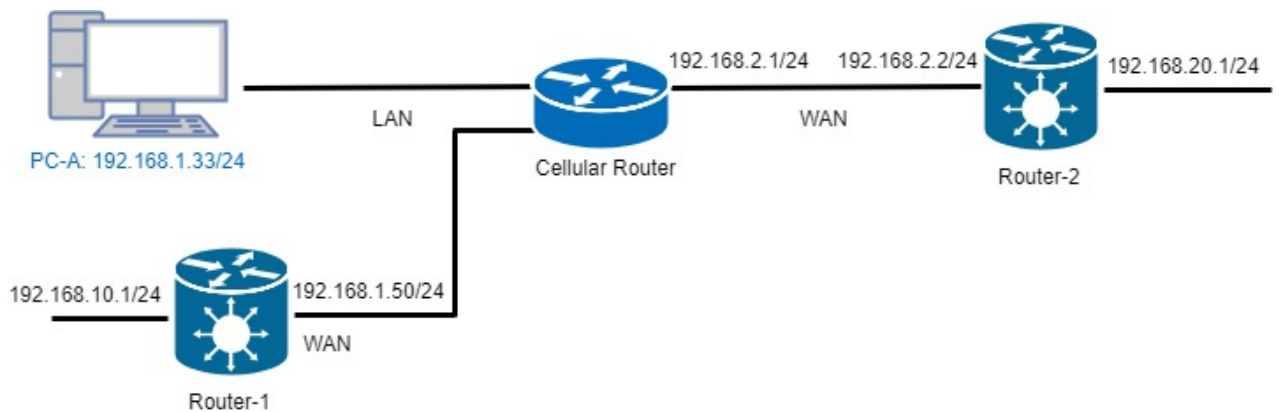


**Note 2:**

- You can purchase a meter of DC voltage and current supporting Modbus protocol with RS-485 serial for test and connection to COM Port 3.
- The following picture shows how connect the ports and the lines between a cellular router and a meter.



## 16.4 IP Routing Topology



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

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

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

### • LAN configuration:

The screenshot shows the LAN IPv4 configuration interface. The left sidebar contains navigation options: Status, System, WAN, LTE, LAN (selected), IPv4, IPv6, VLAN, Subnet, and IP Routing. The main content area is titled "LAN IPv4" and includes fields for IP Address (192.168.1.1) and IP Mask (255.255.255.0). Below these is the "DHCP Server Configuration" section, which has a checkbox for "DHCP Server Configuration" (checked) and a field for "IP Address Pool" (From 192.168.1.2 To 192.168.1.254). An "Apply" button is located at the bottom right.

### • WAN configuration:

The screenshot shows the WAN Ethernet configuration interface. The left sidebar contains navigation options: Status, System, WAN (selected), Priority, Ethernet, IPv6 DNS, LTE, LAN, and IP Routing. The main content area is titled "WAN Ethernet" and includes a "Work As" section with radio buttons for DHCP Client, PPPoE Client, and Static IPv4 (selected). Below this is the "Configuration" tab, which shows the "Static IPv4 Configuration" section. This section includes fields for IP Address (192.168.2.1), IP Mask (255.255.255.0), and Gateway Address (192.168.2.2). An "Ethernet Ping Health" tab is also visible.

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	lan side	192.168.10.1	192.168.1.50	lan	

Add

Apply

Static Route

Mode ☐ Off ☒ On

Settings Status

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

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

```

Command Prompt (1)

Ethernet adapter Blue:

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

C:\tools>ping 192.168.1.50

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

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

C:\tools>ping 192.168.10.1

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

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

C:\tools>

```

### Example 2: Add IP Routing on WAN interface

- Step1: The cellular router for Static Route configuration  
The Mode is on at the settings section and add the routing.
- Step2: Router-2 configuration is as below.
  - (1) Login to the Router-2 web site, and then "NAT disable".
  - (2) Configure LAN IP: 192.168.20.1
  - (3) Configure WAN IP: 192.168.2.2

Static Route

Mode

☐ Off
☒ On

Settings

Status

Mode	Name	Destination	Gateway	Interface	Delete
<input type="radio"/> Off <input checked="" type="radio"/> On	<input type="text" value="wan side"/>	192.168.20.1	192.168.2.2	eth1	<input checked="" type="button" value="x"/>

- 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>

```