



# Industrial 4G LTE Cellular Router

## ICR111WG

## User Manual

Version 1.1

## Table of Contents

<b>1</b>	<b>Introduction.....</b>	<b>6</b>
1.1	Features.....	6
1.2	Specifications.....	7
1.3	Mechanical Dimensions .....	8
<b>2</b>	<b>Hardware Installation.....</b>	<b>8</b>
2.1	LED Indicators.....	8
2.2	Ethernet Port.....	9
2.3	Grounding the Router.....	9
2.4	Pin Assignments.....	10
2.5	Connecting the Power Supply .....	10
2.6	Connecting I/O Ports.....	10
2.7	UART (RS-232).....	12
2.8	Install the SIM Card.....	12
2.9	Reset Button .....	13
2.10	External Antenna.....	13
<b>3</b>	<b>Configuration via Web Browser .....</b>	<b>14</b>
3.1	Access the Web Configurator .....	14
3.2	Navigate the Web Configurator .....	15
<b>4</b>	<b>Status.....</b>	<b>16</b>
4.1	Status > GPS .....	19
<b>5</b>	<b>Configuration &gt; System.....</b>	<b>20</b>
5.1	System > Time and Date .....	20
5.2	System > COM Ports .....	24
5.3	System > Logging .....	26
5.3.1	Logging > Logging .....	26
5.3.2	Logging > Log .....	26
5.4	System > Alarm.....	28
5.4.1	Alarm > Contacts > Create and name the Group.....	29
5.4.2	Alarm > Contacts > Add User .....	31
5.4.3	Alarm > Duty Schedule.....	32
5.5	System > Ethernet Ports .....	32
5.6	System > Client List .....	34
<b>6</b>	<b>Configuration &gt; WAN.....</b>	<b>35</b>
6.1	WAN > Priority.....	35
6.2	WAN > Ethernet .....	36
6.2.1	WAN Ethernet Configuration .....	36
6.3	WAN > WiFi STA.....	39
6.4	WAN > IPv6 DNS .....	40
6.5	Health Check.....	40
<b>7</b>	<b>Configuration &gt; LTE.....</b>	<b>43</b>
7.1	LTE > LTE Config .....	44

7.2	LTE > GPS .....	44
7.2.1	Status.....	44
7.2.2	Config .....	45
7.3	LTE > GPS Track .....	46
7.4	LTE > APN Config.....	46
7.4.1	SIM Configuration .....	49
7.5	LTE > APN1 Usage .....	50
7.6	LTE > SMS.....	55
7.7	LTE > Serving Cell .....	57
7.8	LTE > Lock PCIs .....	58
7.9	LTE > Lock Bands.....	59
7.10	LTE > DNS .....	59
7.11	Search Operators.....	60
7.12	LTE > USSD.....	60
<b>8</b>	<b>Configuration &gt; WiFi.....</b>	<b>61</b>
8.1	WiFi > WiFi Config .....	61
8.2	WiFi > MAC Filter.....	62
8.3	WiFi > Client List.....	63
<b>9</b>	<b>Configuration &gt; LAN.....</b>	<b>64</b>
9.1	LAN > IPv4.....	64
9.2	LAN > IPv6.....	65
9.3	LAN > VLAN.....	65
9.4	LAN > Subnet.....	67
<b>10</b>	<b>IP Routing.....</b>	<b>68</b>
10.1	IP Routing > Static Route .....	68
10.2	Policy Route.....	70
10.3	IP Routing > RIP .....	72
10.4	IP Routing > OSPF.....	74
10.5	IP Routing > BGP .....	77
<b>11</b>	<b>Configuration &gt; VPN.....</b>	<b>80</b>
11.1	VPN > Open VPN.....	80
11.1.1	Open VPN Common Setting.....	80
11.1.2	Open VPN Client Setting .....	82
11.1.3	Open VPN Server Setting.....	83
11.1.4	Set up Open VPN Custom.....	85
11.2	VPN > IPsec.....	86
11.2.1	IPsec > Connections.....	87
11.2.2	IPsec > Authentication IDs.....	91
11.2.3	IPsec > X.509 Certificates .....	92
11.2.4	IPsec > CA Certificates .....	93
11.2.5	IPsec > Net-to-Net Configuration .....	95
11.3	VPN > GRE .....	110
11.4	VPN > PPTP Server.....	112

11.5	VPN > L2TP .....	113
<b>12</b>	<b>Configuration &gt; Firewall .....</b>	<b>117</b>
12.1	Firewall > Basic Rules .....	117
12.2	Firewall > Port Forwarding .....	118
12.3	Firewall > DMZ .....	119
12.4	Firewall > IP Filter .....	120
12.5	Firewall > MAC Filter .....	123
12.6	Firewall > URL Filter .....	124
12.7	Firewall > NAT .....	125
12.8	Firewall > IPS .....	126
<b>13</b>	<b>Configuration &gt; Service .....</b>	<b>127</b>
13.1	Service > SNMP .....	127
13.1.1	Community .....	127
13.1.2	SNMP v3 User Configuration .....	128
13.1.3	SNMP trap configuration .....	129
13.2	Service > TR069 .....	129
13.3	Service > Dynamic DNS .....	131
13.4	Service > VRRP .....	133
13.5	Service > MQTT .....	133
13.6	Service > UPnP .....	136
13.7	Service > SMTP .....	136
13.8	Service > IP Alias .....	137
13.9	QoS .....	137
13.9.1	QoS > ISP Bandwidth .....	138
13.9.2	QoS > QoS .....	138
13.9.3	QoS > Status .....	142
<b>14</b>	<b>Configuration &gt; Management .....</b>	<b>143</b>
14.1	Management > Identification .....	143
14.2	Management > Administration .....	144
14.3	Management > Contacts / On Duty .....	145
14.3.1	Contacts .....	146
14.3.2	Duty Schedule .....	146
14.4	Management > SSH .....	147
14.5	Management > Web .....	148
14.6	Management > Firmware .....	148
14.7	Management > Configuration .....	149
14.8	Management > Load Factory .....	149
14.9	Management > Restart .....	149
14.10	Management > Schedule Reboot .....	149
14.11	Management > Fail2Ban .....	150
14.12	Management > FOTA .....	150
<b>15</b>	<b>Configuration &gt; Diagnosis .....</b>	<b>153</b>
15.1	Diagnosis > Ping .....	153

15.2	Diagnosis > Traceroute .....	153
15.3	Diagnosis > TTY2TCP.....	154
<b>16</b>	<b>Configuration Applications .....</b>	<b>155</b>
16.1	WAN Priority.....	155
16.2	LAN > IPv4/IPv6 Dual Stack.....	157
16.3	MQTT Broker .....	159
16.4	Alarm Configuration.....	160
16.5	Open VPN Configuration.....	161
16.5.1	Open VPN Server Mode.....	162
16.5.2	Open VPN Client Mode .....	163
16.5.3	Open VPN Net-to-Net.....	164
16.5.4	Open VPN 1:1 NAT .....	167
16.5.5	Open VPN with third-party server .....	168
16.5.6	Install Open VPN Access Server on Docker .....	169
16.5.7	Install Pritunl Open VPN server on Docker .....	175
16.6	VRRP Topology .....	183
16.7	TR069 Server (GenieACS Installation).....	183
<b>17</b>	<b>Test Case Example .....</b>	<b>193</b>
17.1	VLAN Topology .....	193
17.2	MQTT Topology.....	196
17.3	IP Routing Topology .....	202

## 1 Introduction

**ICR111WG** compact, lightweight and cost-effective **Industrial 4G LTE Cellular Routers**, are built in 2-port fast Ethernet connection as well as support 2G/3G/4G mobile networks for wired and wireless communication in harsh environments. Equipped with RS232 serial port and digital input/output interfaces, the **ICR111WG** is simple to configure and collect real-time data transmission quickly for Industrial IoT and machine-to-machine applications. The **ICR111WG** is also compliant with IEEE 802.11b/g/n Wi-Fi connectivity.

Featuring VPN Tunnels, Firewall, TR069, and SNMP Trap, **ICR111WG Industrial 4G LTE Cellular Routers** enhance highly secure authentication, encryption and management to protect your data efficiently between public and private networking. Supporting -30~+70°C wide temperature operation and flexible input voltage range of 8-48VDC for diverse environments and various applications.

**ICR111WG Industrial 4G LTE Cellular Routers** are suitable and reliable choices for fast deployment and easy configuration to simplify your complicated solutions and fit your services for industrial networking and smart city.

### 1.1 Features

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

## 1.2 Specifications

### Cellular Interface

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

### Wi-Fi Interface

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

### Hardware Interface

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

### Physical Characteristics

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

### LED Display

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

### Power Supply

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

### Software

#### ● Network Protocols:

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

#### ● Routing/Firewall:

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

#### ● VPN:

OpenVPN, IPSec (3DES, AES128, AES196, AES256, MD5, SHA-1, SHA256), GRE, PPTP, L2TP

#### ● Wireless Connectivity:

WAN WiFi Client

#### ● Others:

DDNS, QoS, UPnP, SMS Action, GPS Track Drawing, GPS TCP Push

#### ● Alarm:

DI, DO, SMS, VPN/WAN Disconnect, SNMP Trap, E-mail, TR069

### Management Software

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

### Environment

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

### Standards and Certifications

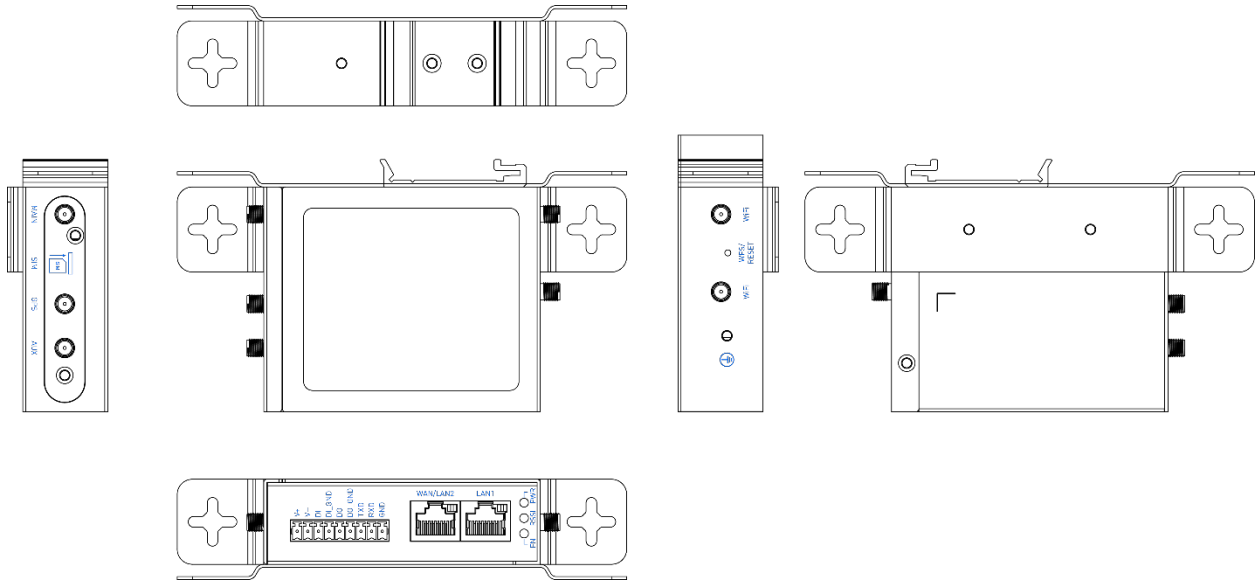
- **EMC** : CE, FCC
- **EMI** : EN 301489 , FCC Part 15B Class B
- **EMS** : EN 301489
- **Vibration** : IEC60068-2-6
- **Radio** : EN 301511, EN 301908-1, EN 301908-2, EN 301908-13, EN 300328, EN 303413, EN 62311

### Note:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.

## 1.3 Mechanical Dimensions



## 2 Hardware Installation

This chapter introduces how to install and connect the hardware.

### 2.1 LED Indicators

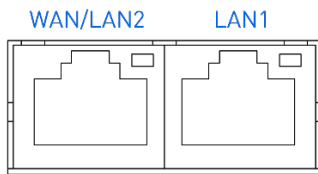


LED	FN	RSSI	PWR
ON	VPN Connected	High Signal	Power ON
Slow Blinking	Internet Connected / Reset	Medium Signal / Reset	N/A
Fast Blinking	System Booting / Reset to Default	Low Signal / Reset to Default	N/A
OFF	N/A	Error	Power OFF
Heart Beat	Wi-Fi Connected	WPS Processing	N/A



## 2.2 Ethernet Port

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



The LAN and WAN interface are standard RJ45 connectors.

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

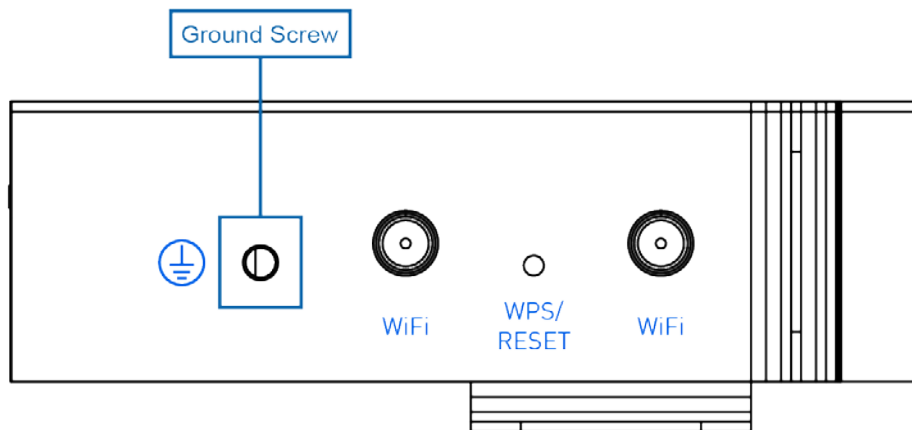
### (2) LED Indicator of Ethernet Port

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

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

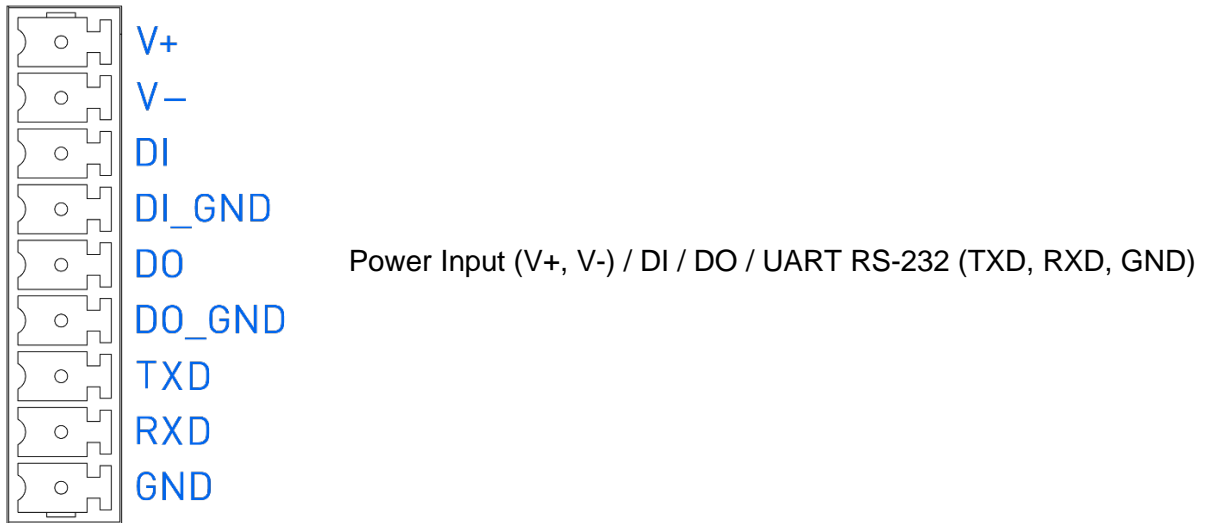
## 2.3 Grounding the Router

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



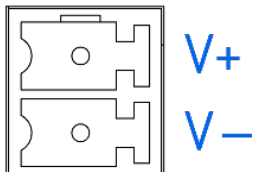
(ICR111WG)

## 2.4 Pin Assignments



## 2.5 Connecting the Power Supply

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



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

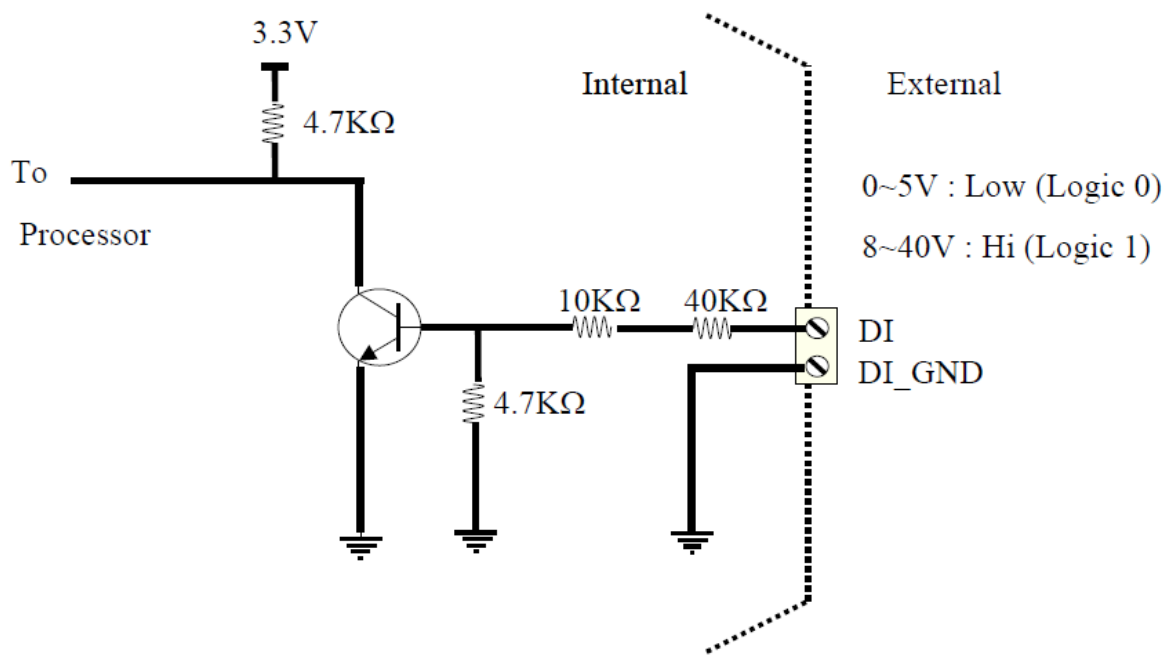
## 2.6 Connecting I/O Ports

### (1) Digital Input (DI)

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

Pin	Description
DI	Digital Input
DI_GND	

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

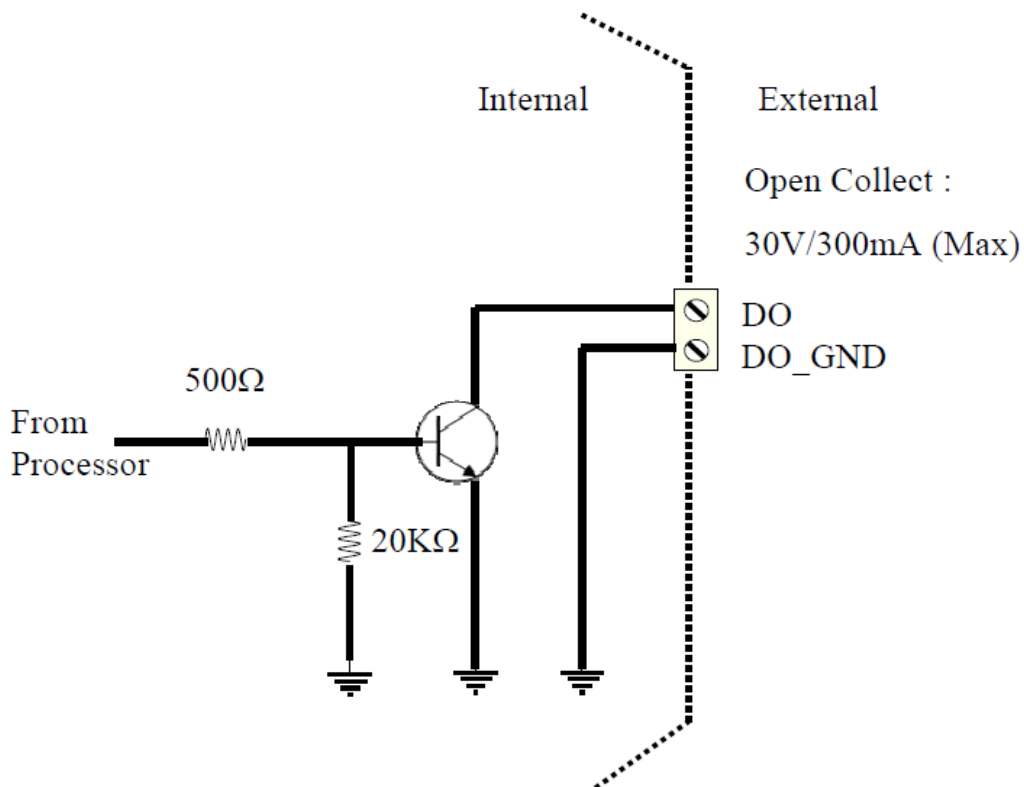


## (2) Digital Output (DO)

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

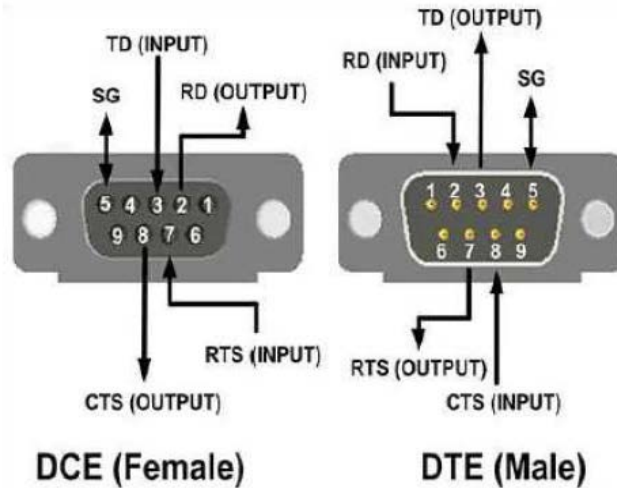
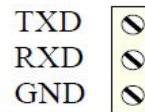
Pin	Description
DO	Digital Output
DO_GND	

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



## 2.7 UART (RS-232)

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



Pin	Signal	Direction
TXD	Transmit Data	Output
RXD	Receive Data	Input
GND	Signal Ground	-

## 2.8 Install the SIM Card



### Insert and Remove SIM Card

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

## 2.9 Reset Button

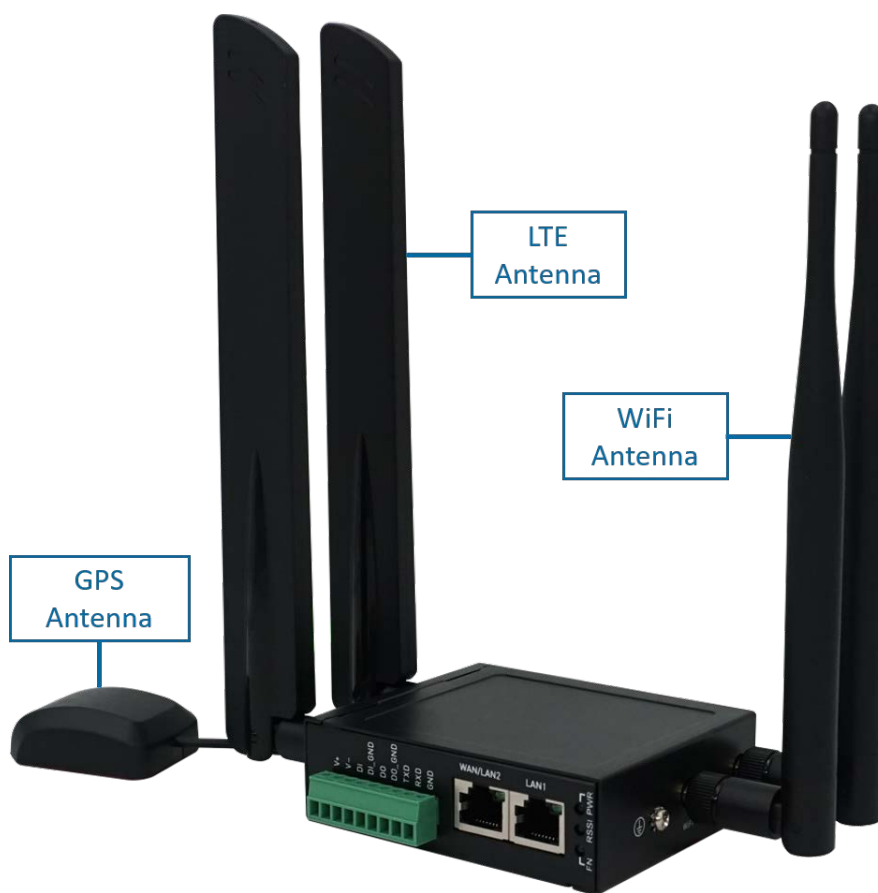


## WPS/ RESET

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

## 2.10 External Antenna

Each unit has three antenna connectors, MAIN, GPS, AUX (SMA). For ICR111WG, there will be five antenna connectors and extra two antennas for Wi-Fi (RP-SMA). Connect the antenna to MAIN when you have only one antenna. Please tighten the connecting nut properly to ensure good connection.



(ICR111WG)

## 3 Configuration via Web Browser

### 3.1 Access the Web Configurator

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

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

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

#### Title Bar Panel > Selecting Language

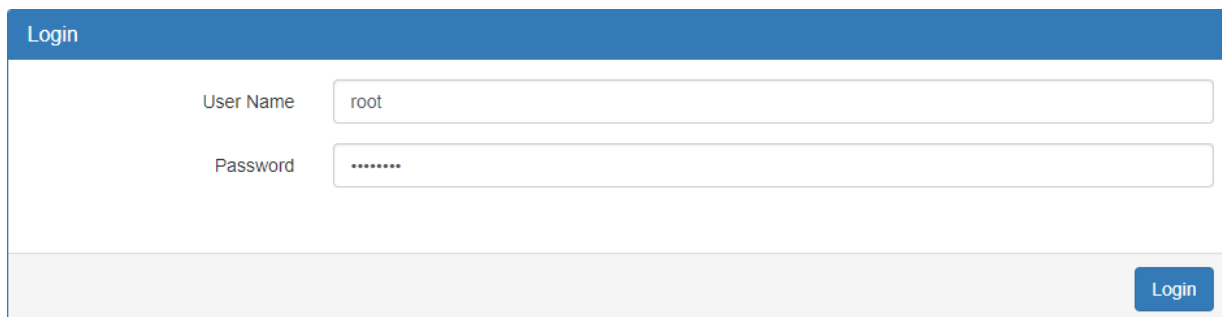
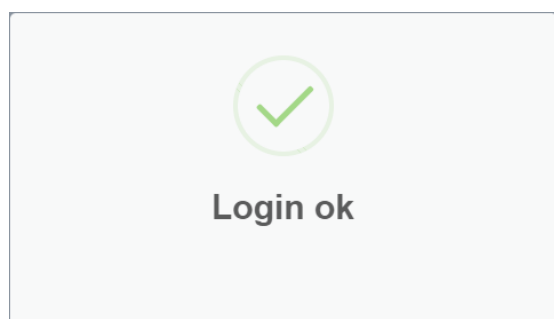
You can choose the languages, including English and Taiwan.



#### Logging in the Router

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

After clicking, the interface shows [Login ok](#).

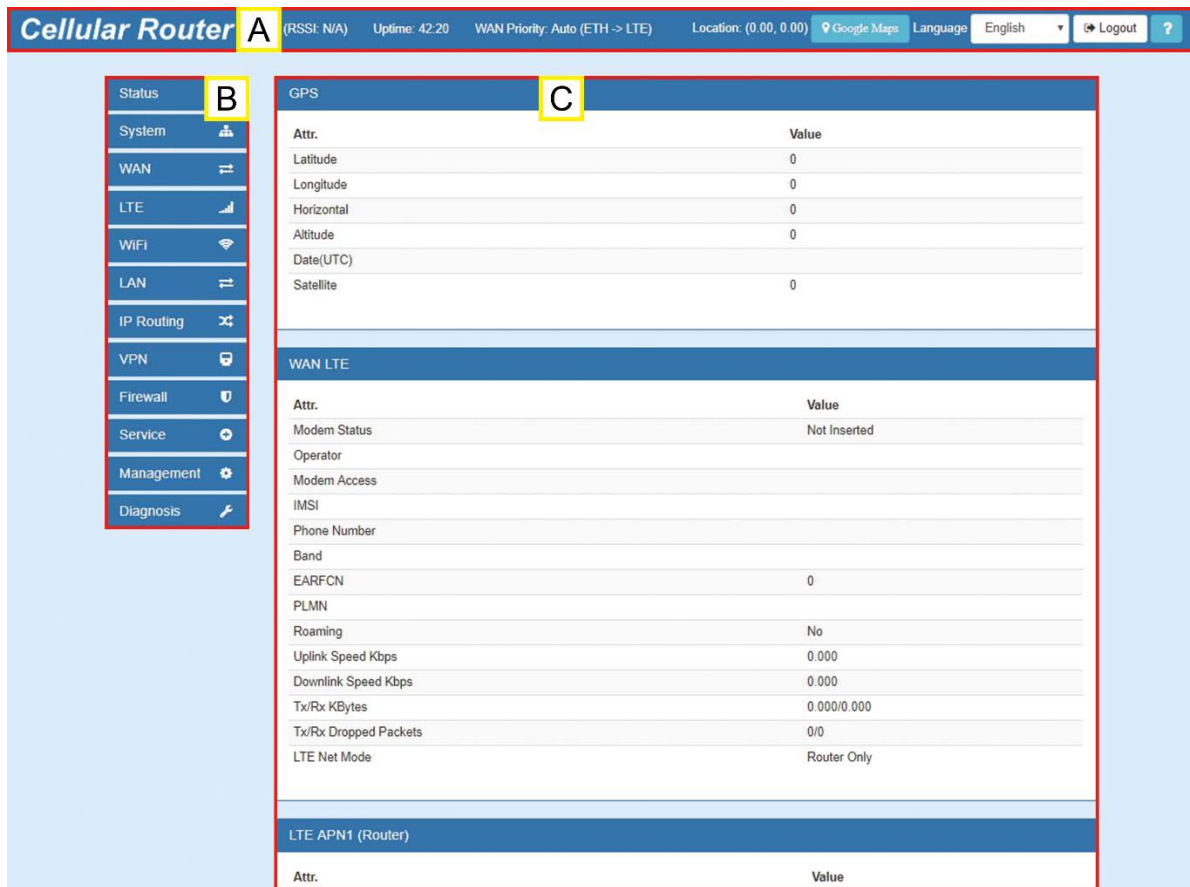
A screenshot of the router's login page. The page has a blue header with the word 'Login'. Below the header, there are two input fields: 'User Name' with the text 'root' and 'Password' with a masked password '.....'. A blue 'Login' button is located at the bottom right of the form.

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

## 3.2 Navigate the Web Configurator

The main screen is divided into three parts as below.

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



(1) **A** : Title Bar

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



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

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

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

(3) **C** : Main Window

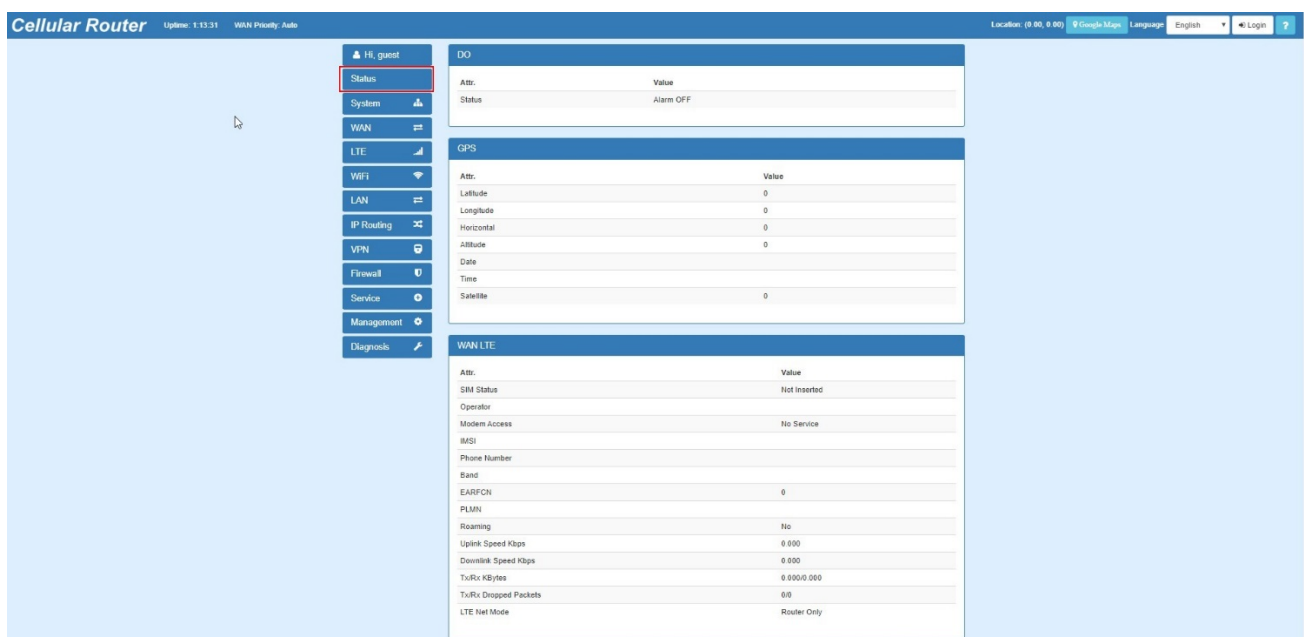
This section shows the information or setting fields from main menu and sub menu.

## 4 Status

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

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

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



The screenshot displays the Cellular Router web interface. The top navigation bar includes the title "Cellular Router", system information (Uptime: 1:13:31, WAN Priority: Auto), location (0.00, 0.00), language (English), and a login button. The left sidebar contains a menu with "Status" highlighted. The main content area shows three status sections:

- DO (Digital Out):** A table with columns "Attr." and "Value". The "Status" attribute has a value of "Alarm OFF".
- GPS:** A table with columns "Attr." and "Value". Attributes include Latitude (0), Longitude (0), Horizontal (0), Altitude (0), Date, Time, and Satellite (0).
- WAN LTE:** A table with columns "Attr." and "Value". Attributes include SIM Status (Not inserted), Operator, Modem Access (No Service), IMSI, Phone Number, Band, EARFCN (0), PLMN, Roaming (No), Uplink Speed Kbps (0.000), Downlink Speed Kbps (0.000), Tx/Rx KBytes (0.000/0.000), Tx/Rx Dropped Packets (0/0), and LTE Net Mode (Router Only).



Status > DO	
Item	Description
<b>Attribute</b>	
<b>Status</b>	<ul style="list-style-type: none"> <li>• Alarm ON: DO is configured to turn on when alarm is triggered.</li> <li>• Alarm OFF: Alarm is configured to be disabled.</li> <li>• Alarm PULSE: DO is configured to pulse when alarm is triggered.</li> <li>• Force ON: DO is turn on by remote command.</li> <li>• Force OFF: DO is turn on by remote command.</li> <li>• Force PULSE: DO is turn pulse by remote command.</li> </ul>

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>	Horizontal precision:0.5-99.9
<b>Altitude</b>	The altitude of antenna away from the sea level (unit: m), accurate to one decimal place.
<b>Date</b>	UTC date when fixing position.
<b>Time</b>	UTC time when fixing position.
<b>Satellite</b>	Number of satellites.

Status > WAN LTE	
Item	Description
<b>Attribute</b>	
<b>SIM Status</b>	<ul style="list-style-type: none"> <li>• Ready: No PIN code protection or unlock already.</li> <li>• Unlock: Unlock pin code protection.</li> <li>• Locked: Locked by pin code.</li> <li>• Error: SIM operation error.</li> <li>• Blocked: PUK needed to unlock.</li> <li>• Not Inserted: No SIM card.</li> <li>• Hardware Error: Unable to enable function.</li> <li>• Ignore: Ignore Specified SIM in dual SIM device.</li> </ul>
<b>Operator</b>	Display the name of operator.
<b>Modem Access</b>	The router to access protocol type.
<b>IMSI</b>	The IMSI number of the SIM card.
<b>Phone Number</b>	The phone number of the SIM card.
<b>Band</b>	The current connected Band.
<b>EARFCN</b>	Absolute radio-frequency channel number.
<b>PLMN</b>	Public LAN Mobile Network ID.
<b>Roaming</b>	Roaming status.
<b>Uplink Speed Kbps</b>	Uplink Speed in Kbps.
<b>Downlink Speed Kbps</b>	Downlink Speed in Kbps.
<b>Tx/Rx KBytes</b>	Accumulated TX/RX in KBytes.

<b>Tx/Rx Dropped Packets</b>	TX/RX Dropped Packets.
<b>LTE Net Mode</b>	LTE Network Mode for both APNs.

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

<b>Status &gt; WAN DNS</b>	
<b>Item</b>	<b>Description</b>
<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.

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

<b>Status &gt; WAN WiFi</b>	
<b>Item</b>	<b>Description</b>
<b>Attribute</b>	
<b>IPv4 Address</b>	WAN WiFi obtain IPv4 Address.
<b>IPv4 Mask</b>	WAN WiFi obtain IPv4 Mask.
<b>Default Gateway</b>	WAN WiFi IPv4 Default Gateway.
<b>IPv4 Conn Time</b>	WAN WiFi IPv4 Connected Time.
<b>SSID</b>	Service Set Identifier of WAN WiFi.
<b>MAC Address</b>	MAC Address of WAN WiFi.
<b>Channel</b>	The current connected Channel.

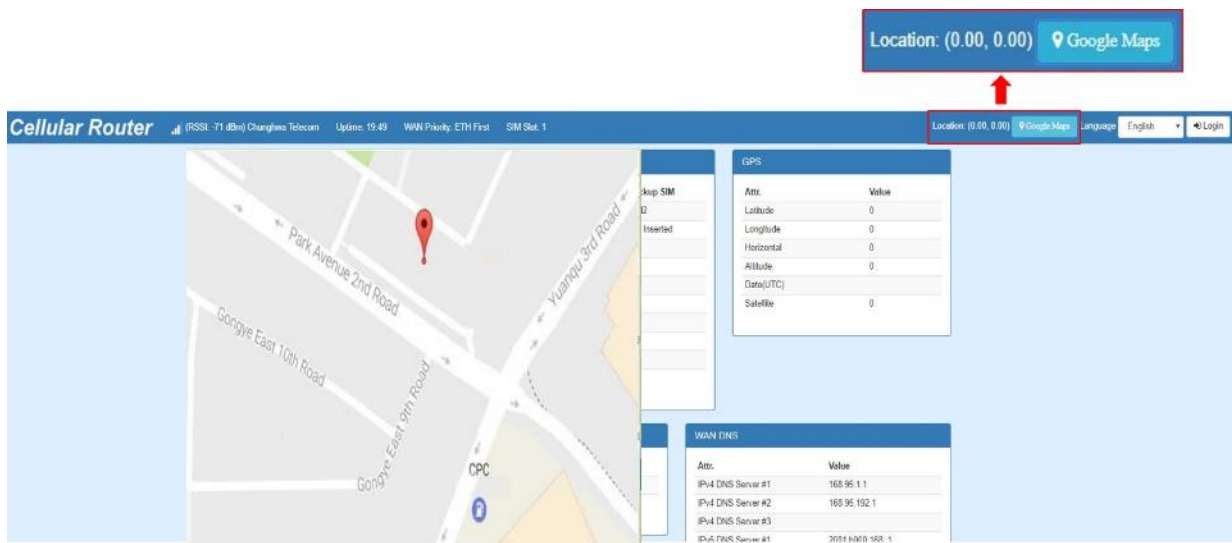
Status > LAN Ethernet	
Item	Description
<b>Attribute</b>	
IPv4 Address	LAN is assigned IPv4 Address.
IPv4 Mask	LAN is assigned IPv4 Mask.
IPv6 Address	LAN is assigned IPv6 Address.
IPv6 Conn Time	IPv6 Connected Time.
Uplink Speed Kbps	Uplink Speed in Kbps.
Downlink Speed Kbps	Downlink Speed in Kbps.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

Status > WiFi AP	
Item	Description
<b>Attribute</b>	
Connected Clients	The number of connected clients.

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

## 4.1 Status > GPS

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




The screenshot shows the Cellular Router web interface. At the top, the status bar includes 'Cellular Router', signal strength, RSSI: 71 dBm, Changhua Telecom, Uptime: 15:49, WAN Priority: ETH First, and SIM Slot: 1. On the right side of the status bar, there is a 'Location: (0.00, 0.00)' display and a 'Google Maps' button. Below the status bar, the main content area is divided into several sections. On the left, there is a map showing the current location. On the right, there are two data tables: 'GPS' and 'WAN DNS'.

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

Attr.	Value
IPv4 DNS Server #1	168.96.1.1
IPv4 DNS Server #2	168.96.192.1
IPv4 DNS Server #3	
IPv4 DNS Server #1	2011.M010.168.1

## 5 Configuration > System

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

System 
Time and Date
COM Ports
Logging
Alarm
Ethernet Ports
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 Feb 20, 2020 8:54:37 PM

### Time and Date Setup

Mode  Manual  Get from Time Server

YYYY-MM-DD HH:MM:SS 2020 - 2 - 20 20 : 48 : 7

GPS Time  Off  On

IPv4 Server #1 0.openwrt.pool.ntp.org

IPv4 Server #2 pool.ntp.org

IPv4 Server #3 clock.sjc.he.net

IPv6 Server #1 time-d.nist.gov

IPv6 Server #2 2.pool.ntp.org

IPv6 Server #3 clock.nyc.he.net

### Time Zone Setup

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

Daylight Savings  Off  On

Ahead of standard time 60 mins

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

Start Time 2 : 0 (Hour : Minute)

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

End Time 2 : 0 (Hour : Minute)

### Time Server

Server Mode  Off  On

Server Port 123

Apply

## II. Manual

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

**Time And Date**

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

### Time and Date Setup

Mode  Manual  Get from Time Server

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

### 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)

### Time Server

Server Mode  Off  On

Server Port

**Apply**

## III. Time Zone Setup

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

### Time Zone Setup

Time Zone

Daylight Savings  Off  On

Ahead of standard time  mins

Start Date  /  /  (Month / Week / Day)

Start Time  :  (Hour : Minute)

End Date  /  /  (Month / Week / Day)

End Time  :  (Hour : Minute)

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

#### IV. Time Server

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

##### Time Server

Server Mode  Off  On

Server Port

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

### 5.2 System > COM Ports

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

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

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

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



Edit COM Ports Entry #1

Baud Rate: 115200

Data: 8 bit

Parity: none

Stop: 1 bit

Flow Control: none

Is Console?

Virtual COM

Mode: Disable

Protocol: TCP

Redirect Port: 0

Save

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

#	Mode	Host Address	Protocol	Port	
1	Server		TCP	6000	<input checked="" type="checkbox"/>

Apply

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

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</li> </ul>

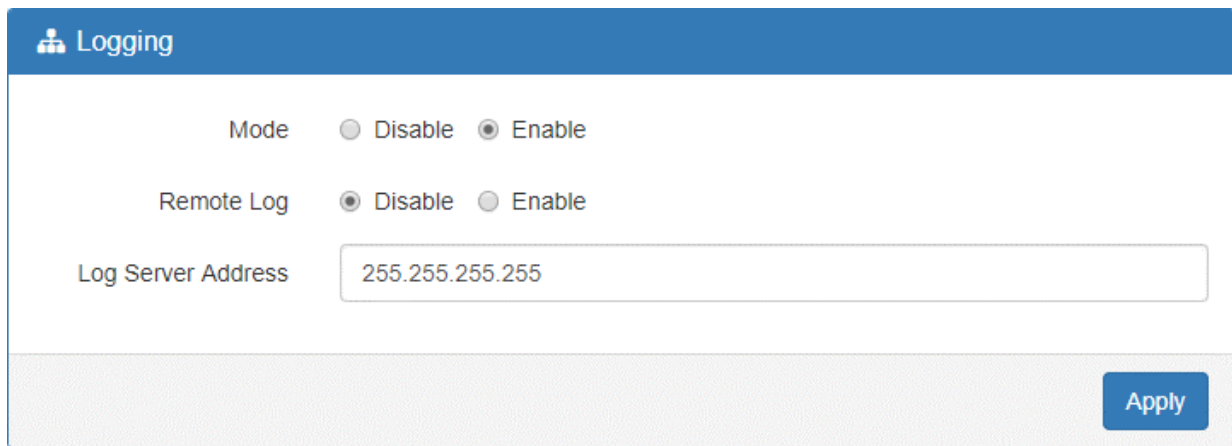
	<p>this port.</p> <ul style="list-style-type: none"> <li>Client Mode: The network package of remote device is on the remote host.</li> </ul>
--	--

### 5.3 System > Logging

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

#### 5.3.1 Logging > Logging

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




System > Logging > Logging	
Item	Description
<b>Mode</b>	Turn on/off the logging configuration. Select from Disable or Enable. The default is Enable.
<b>Remote Log</b>	The logging messages send to remote log or not. Select from Disable or Enable. The default is Disable.
<b>Log Server Address</b>	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.

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

 Log

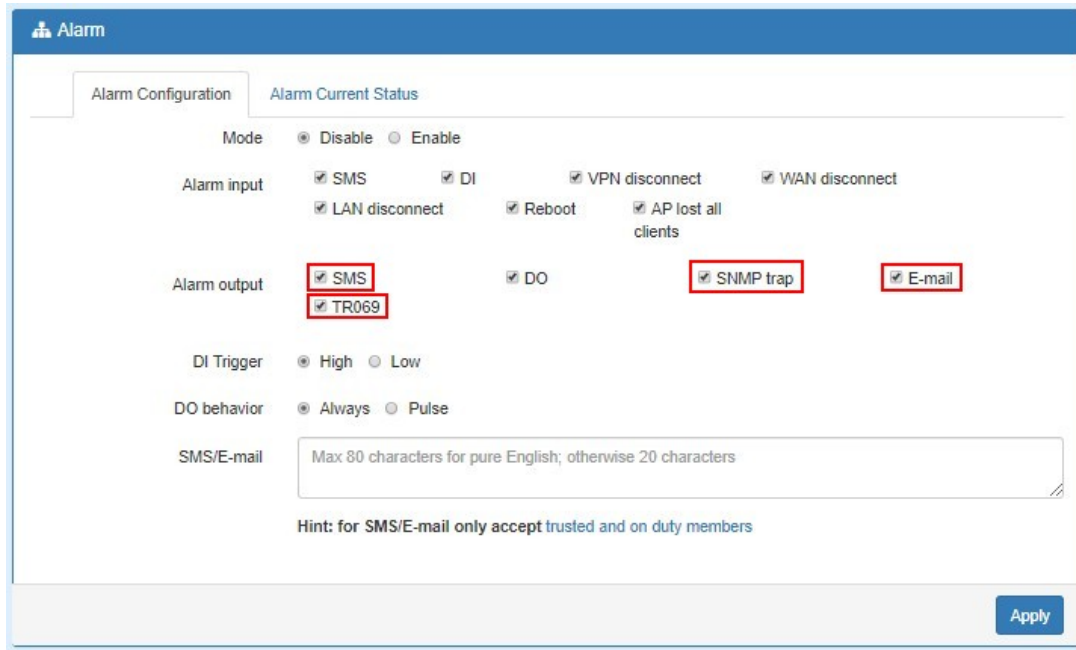
[Clear](#) [Refresh](#) [Download Logs](#)

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

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

## 5.4 System > Alarm

This section allows you to configure the alarm.



**Note:**

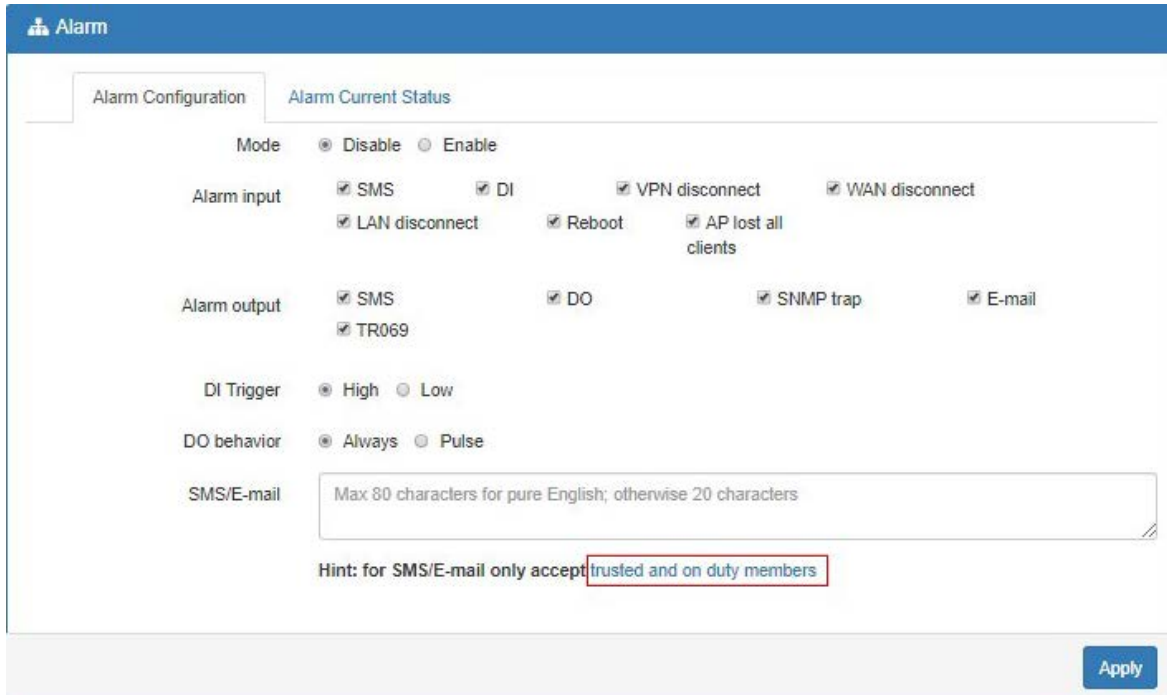
- (1) If you select **SMS** in Alarm input/output, you need to add the trust phone number into Contracts/ On Duty.
- (2) If you select **SNMP trap** in Alarm output, you need to set up SNMP trap configuration from Service SNMP.
- (3) If you select **E-Mail** in Alarm output, you need to set up SMTP configuration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

System > Alarm	
Item	Description
<b>Mode</b>	Turn on/off the Alarm configuration. Select from Disable or Enable. The default is Enable.
<b>Alarm Input</b>	<ul style="list-style-type: none"> <li>● <b>SMS:</b> It means on duty team members on Contacts / On Duty can send SMS to the phone number of using SIM card to trigger alarm.</li> <li>● <b>DI:</b> IO to trigger alarm.</li> <li>● <b>VPN disconnect:</b> All tunnels get disconnected then trigger alarm.</li> <li>● <b>WAN disconnect:</b> WAN connections get disconnected then trigger alarm.</li> <li>● <b>LAN disconnect:</b> LAN connection get disconnected then trigger alarm.</li> <li>● <b>Reboot:</b> Reboot then trigger alarm.</li> </ul>
<b>Alarm Output</b>	Select from SMS, DO, SNMP trap, E-mail and TR069 as alarm output.
<b>DI Trigger</b>	Select from High or Low. The default is High Trigger.
<b>DO behavior</b>	<ul style="list-style-type: none"> <li>● <b>Always:</b> Pull DO high.</li> <li>● <b>Pulse:</b> High and Low continuously.</li> <li>● <b>Pulse Time Length:</b> Pulse time length (unit: mini seconds).</li> </ul>

<b>SMS/E-mail</b>	Write your messages and the messages limit 80 pure English characters or 20 characters for other languages to deliver.
-------------------	--

**5.4.1 Alarm > Contacts > Create and name the Group**

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



**Alarm**

Alarm Configuration | Alarm Current Status

Mode:  Disable  Enable

Alarm input:  SMS  DI  VPN disconnect  WAN disconnect  
 LAN disconnect  Reboot  AP lost all clients

Alarm output:  SMS  DO  SNMP trap  E-mail  
 TR069

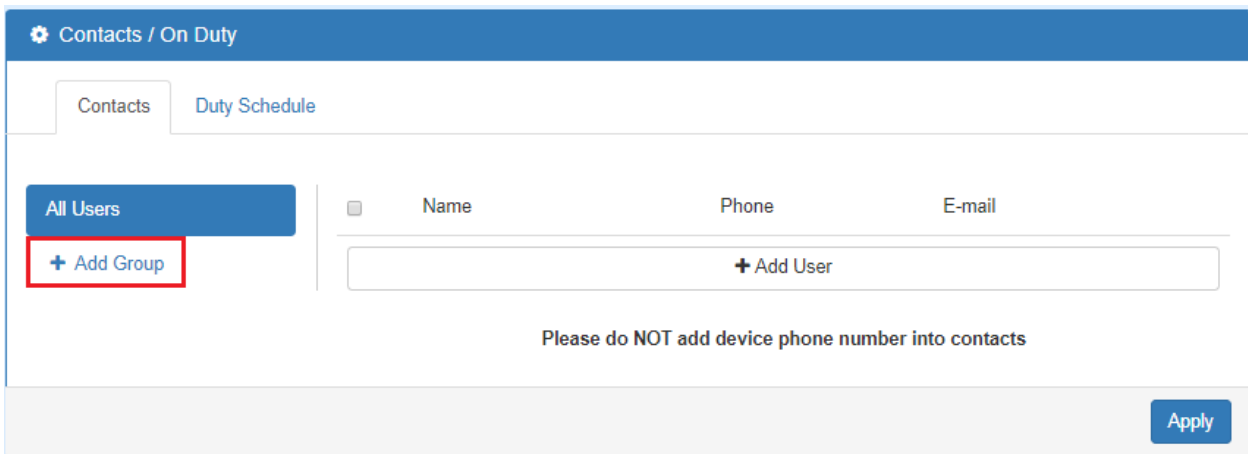
DI Trigger:  High  Low

DO behavior:  Always  Pulse

SMS/E-mail:

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

**Apply**



**Contacts / On Duty**

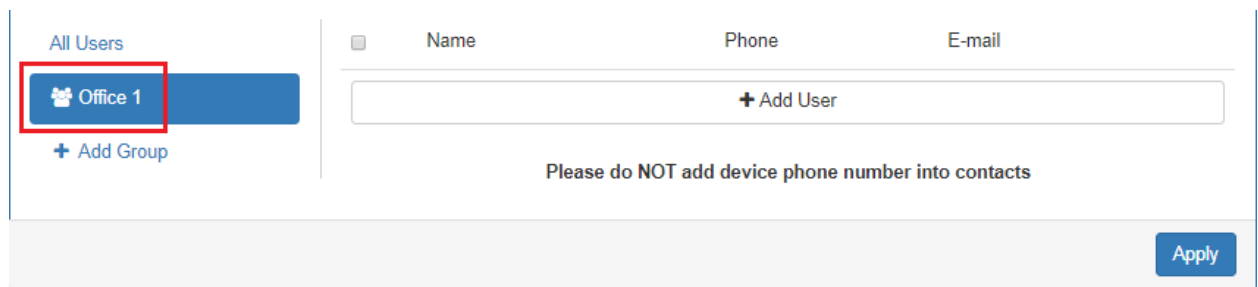
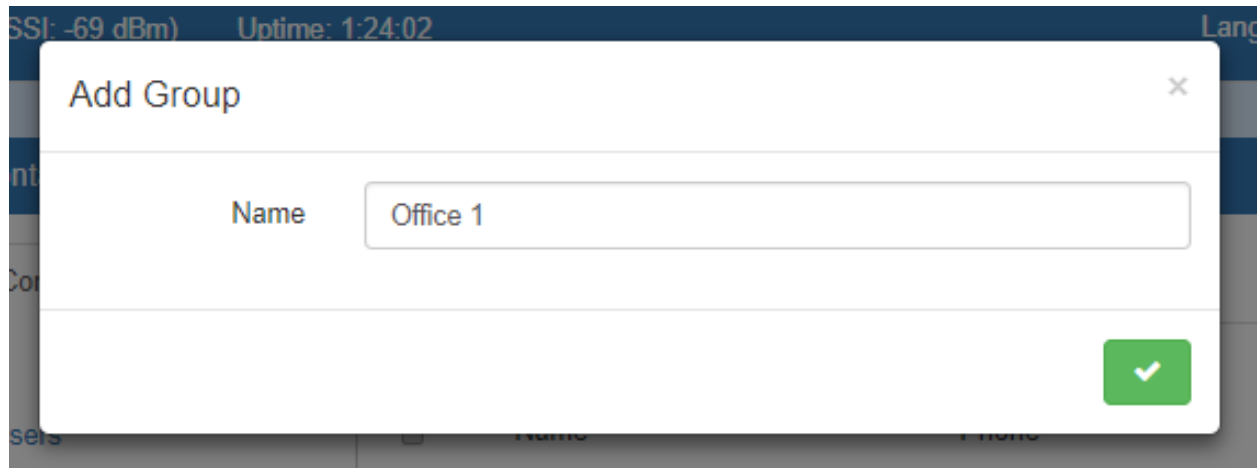
Contacts | Duty Schedule

All Users + Add Group

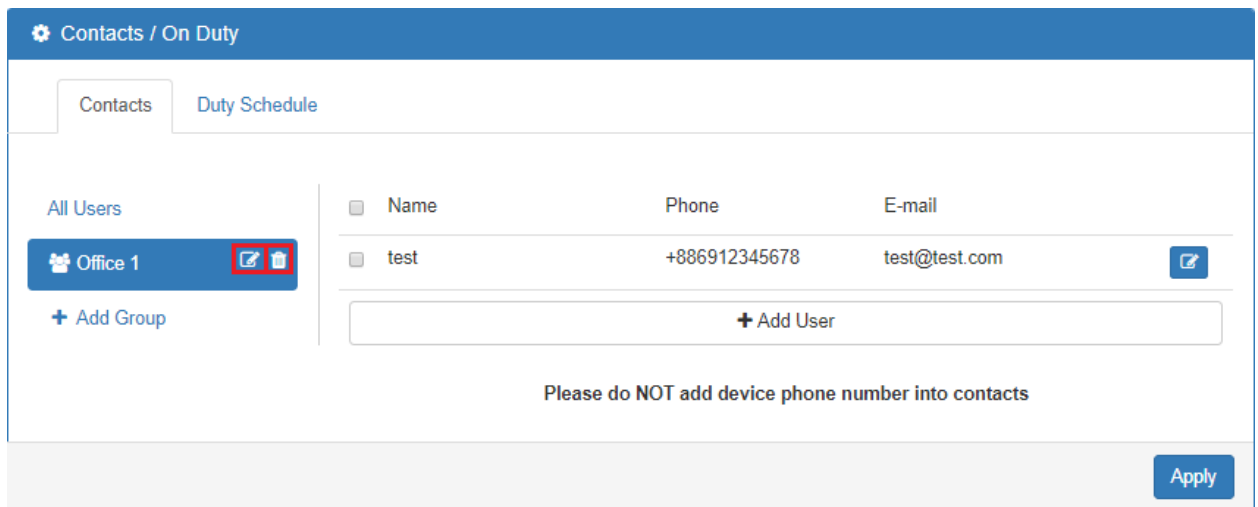
Name	Phone	E-mail
<span style="border: 1px solid gray; padding: 5px;">+ Add User</span>		

Please do NOT add device phone number into contacts

**Apply**

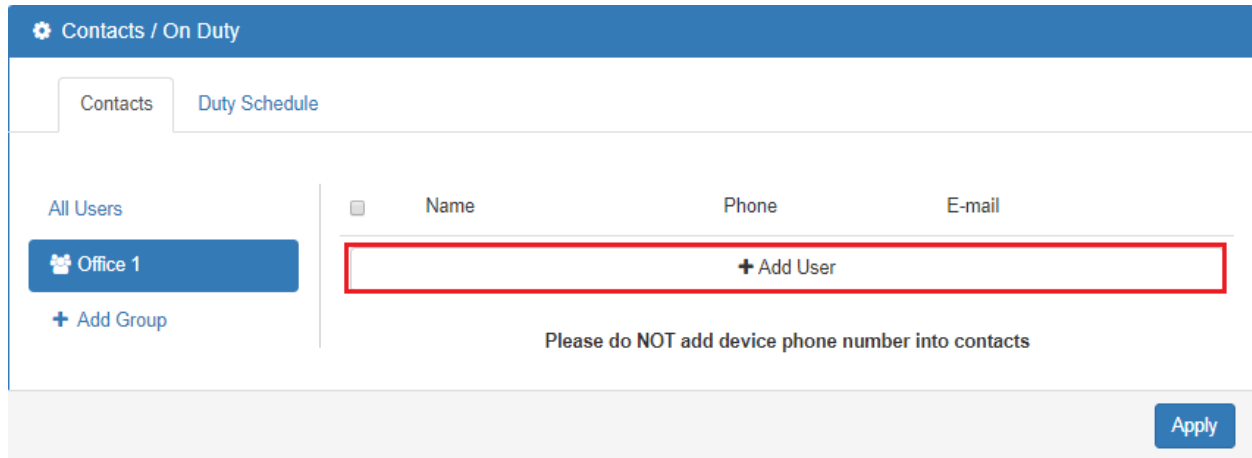



- You can click  or  button to edit or delete the group.

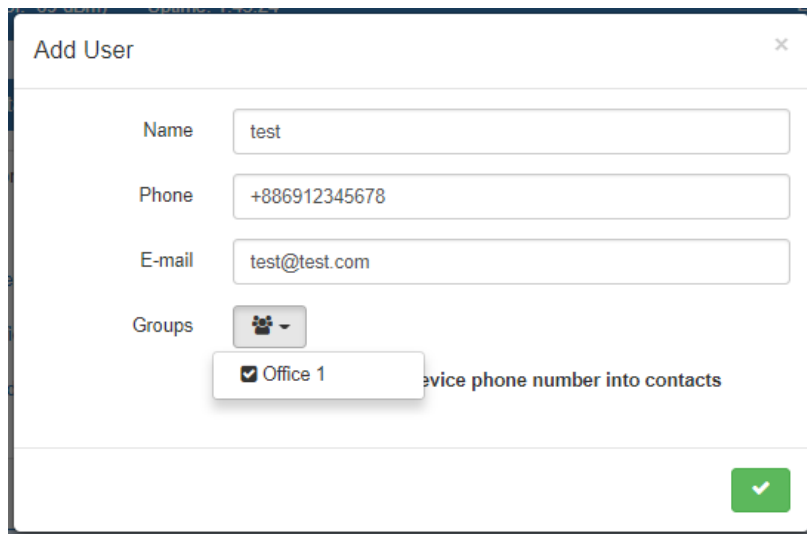


## 5.4.2 Alarm > Contacts > Add User

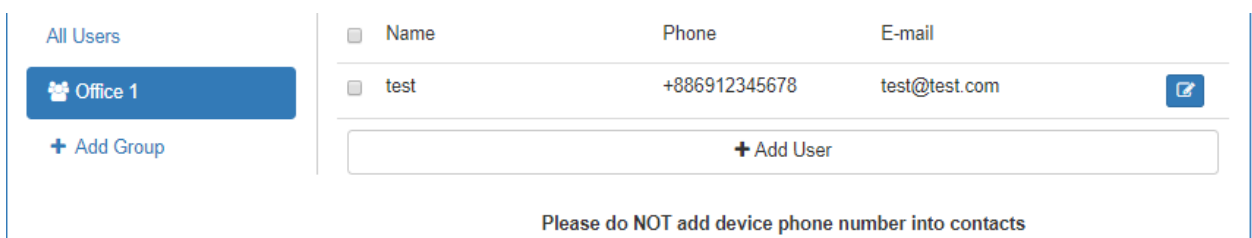
- Select your naming group and click **+ Add User** button to add your user's information, including Name, Phone and E-mail.


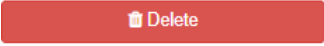


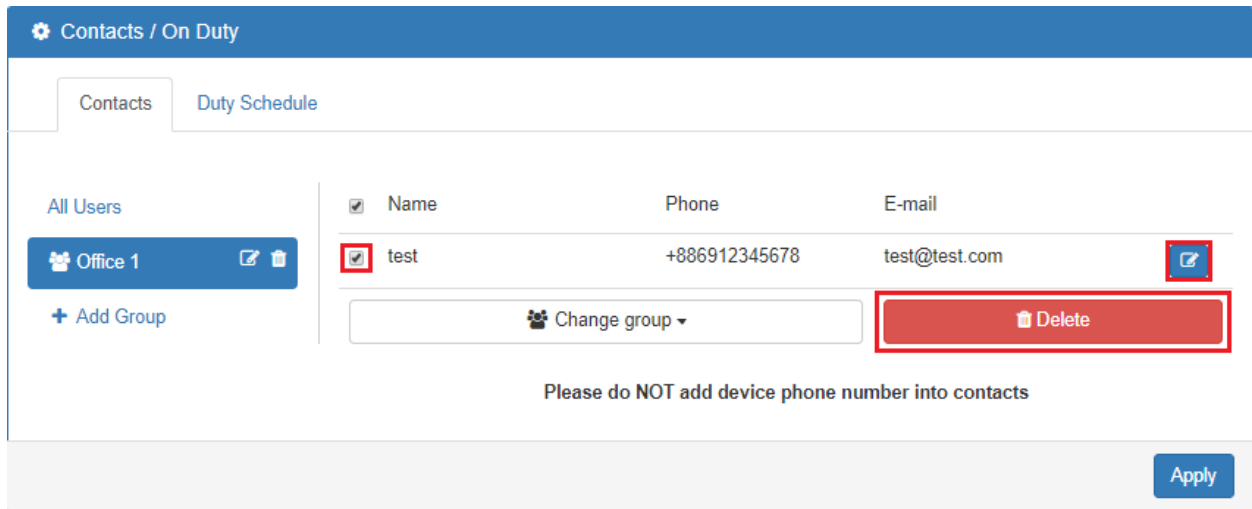
- After filling in your information for each row, chose your naming group and click  to submit your settings.



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



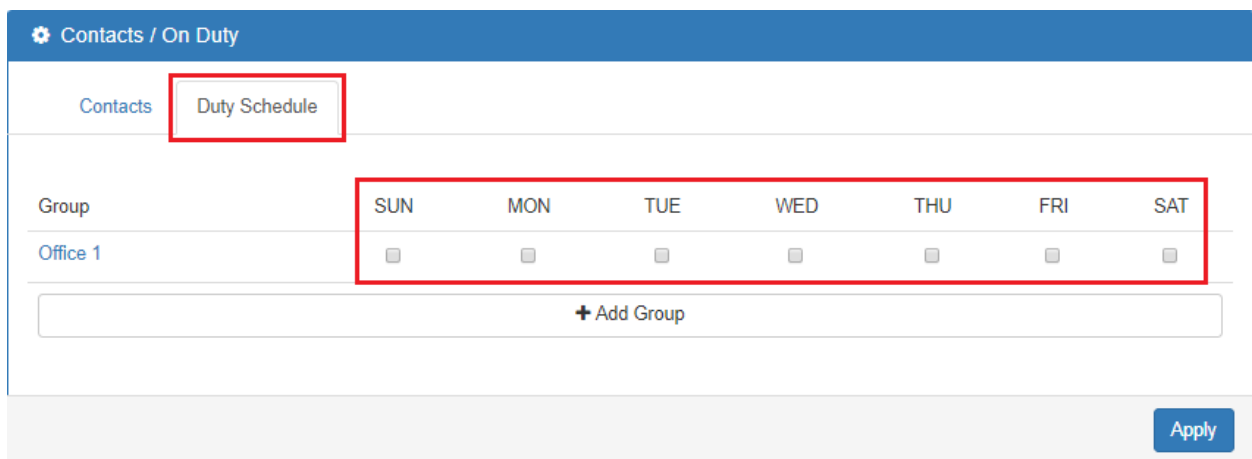
- You can click  button to edit the user's information or click the check box and  to delete the user.



The screenshot shows the 'Contacts / On Duty' interface. On the left, there are tabs for 'Contacts' and 'Duty Schedule', and a list of groups including 'Office 1'. The main area displays a table of users with columns for Name, Phone, and E-mail. The user 'test' is selected, and a 'Delete' button is highlighted with a red box. Below the table, there is a 'Change group' dropdown and an 'Apply' button at the bottom right.

### 5.4.3 Alarm > Duty Schedule

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



The screenshot shows the 'Duty Schedule' interface. The 'Duty Schedule' tab is selected and highlighted with a red box. Below it, there is a grid for selecting days of the week (SUN, MON, TUE, WED, THU, FRI, SAT) for the group 'Office 1'. Each day has a checkbox, and the entire grid is highlighted with a red box. There is an 'Add Group' button below the grid and an 'Apply' button at the bottom right.

## 5.5 System > Ethernet Ports

This section allows you to configure the Ethernet.

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

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



🏠 Ethernet

---

### Ethernet Ports Status

LAN  100M Full

WAN  Off

---

### Ethernet Ports Configurations

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

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

---

### WAN Ethernet

WAN MTU  min: 500; max: 1500

---

### Flow Control

LAN  Off  On

---

### WAN/LAN2 Port Function

Auto  WAN  LAN2

Hint For Auto mode, it decided by WAN Priority setting

Refresh
Apply

System > Ethernet Ports	
Item	Description
<b>Ethernet Ports Status</b>	Show the connectivity status of LAN and WAN.
<b>Ethernet Ports Configurations</b>	Select from Auto, 100M Full, 100M Half, 10M Full, 10M Half and Disable.
<b>WAN Ethernet</b>	MTU is the Maximum Transmission Unit that can be sent over the WAN Ethernet interface. It allows users to adjust the MTU size to fit into their existing network environment.
<b>Flow Control</b>	Allow users to control the traffic ingress from Ethernet LAN or WAN.
<b>WAN/LAN2 Port Function</b>	Allow users to setup the WAN/LAN2 Port function as Auto, LAN, or WAN.

## 5.6 System > Client List

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

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

System > Client List	
Item	Description
<b>List Type</b>	<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>

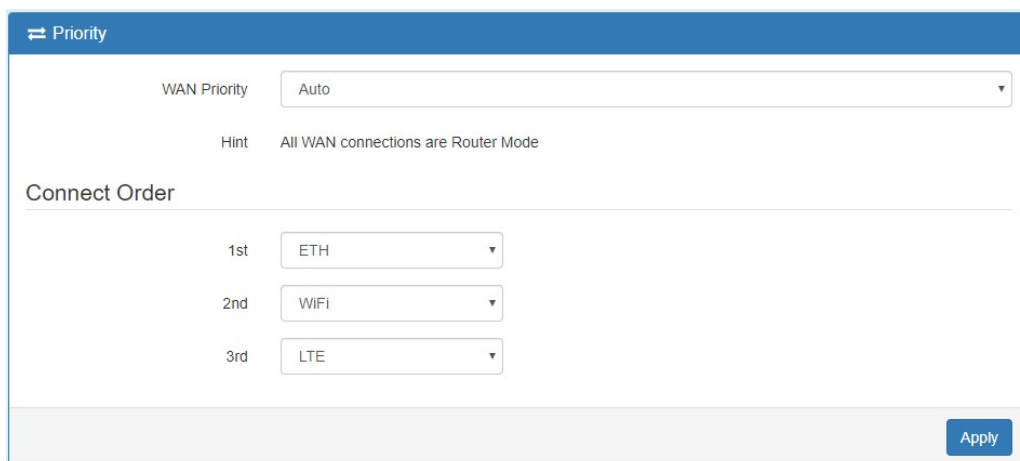
## 6 Configuration > WAN

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. The default is Auto.



WAN > Priority	
Item	Description
<b>Priority</b>	<ul style="list-style-type: none"> <li>● <b>Auto:</b> Please specify the connection order.</li> <li>● <b>LTE Only:</b> Only use LTE connection.</li> <li>● <b>ETH Only:</b> Only use WAN Ethernet connection.</li> <li>● <b>WiFi Only:</b> Only use WAN WiFi connection.</li> </ul>
<b>Connect Order</b>	<ul style="list-style-type: none"> <li>● <b>1st:</b> The first priority of wan interface for connection.</li> <li>● <b>2nd:</b> The second priority of wan interface for connection.</li> <li>● <b>3rd:</b> The 3rd priority of wan interface for connection.</li> </ul>
<b>LTE Net Mode</b>	The priority is <b>LTE Only</b> . <ul style="list-style-type: none"> <li>● <b>Bridge Only:</b> APN1 acts as bridge for internet access.</li> <li>● <b>Router Only:</b> APN1 acts as router for internet access.</li> </ul>
<b>WiFi Mode</b>	The priority is <b>WiFi Only</b> . <ul style="list-style-type: none"> <li>● <b>Bridge Only:</b> WiFi station acts as bridge for internet access.</li> <li>● <b>Router Only:</b> WiFi station acts as router for internet access.</li> </ul>

## 6.2 WAN > Ethernet

### 6.2.1 WAN Ethernet Configuration

This section provides three options to obtain the IP of WAN Ethernet. The options include **DHCP Client**, **PPPoE Client** and **Static IPv4**. The default is DHCP Client.

☰ WAN Ethernet

Work As  DHCP Client  PPPoE Client  Static IPv4

#### DNS Server Configuration

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

Apply

WAN > Ethernet	
Item	Description
<b>WAN Ethernet</b>	<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

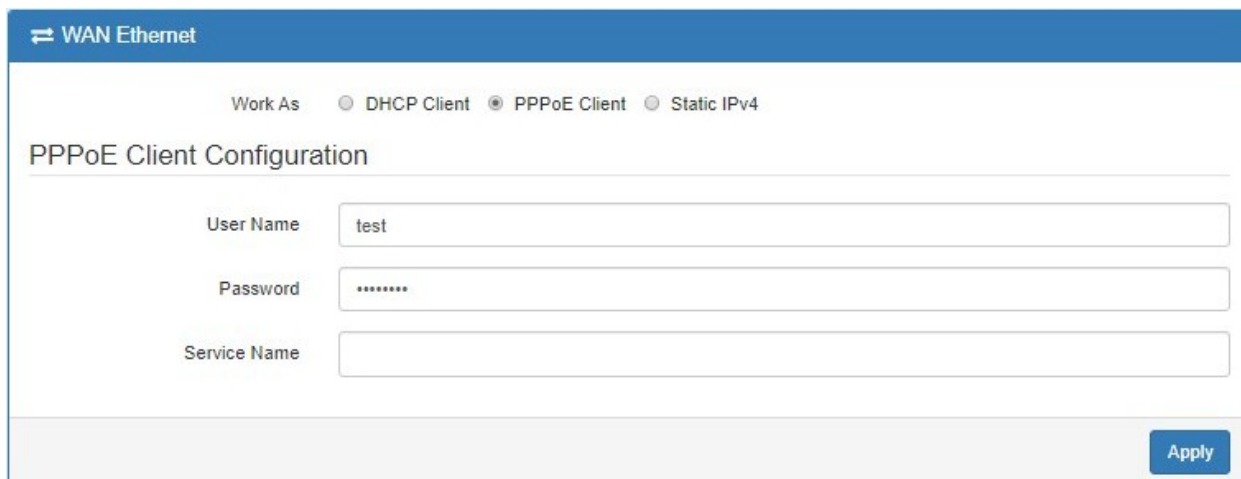
#### DNS Server Configuration

IPv4 DNS Server #1	From ISP ▼	<input type="text"/>
IPv4 DNS Server #2	<div style="border: 1px solid #ccc; padding: 2px;"> <span style="background-color: #0056b3; color: white; padding: 2px;">From ISP</span>              User Defined              None           </div>	<input type="text"/>
IPv4 DNS Server #3	From ISP ▼	<input type="text"/>

Apply

<b>WAN &gt; Ethernet &gt; DHCP Client</b>	
<b>Item</b>	<b>Description</b>
<b>IPv4 DNS Server #1 IPv4 DNS Server #2 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. Service name is an option setting.



WAN Ethernet

Work As  DHCP Client  PPPoE Client  Static IPv4

PPPoE Client Configuration

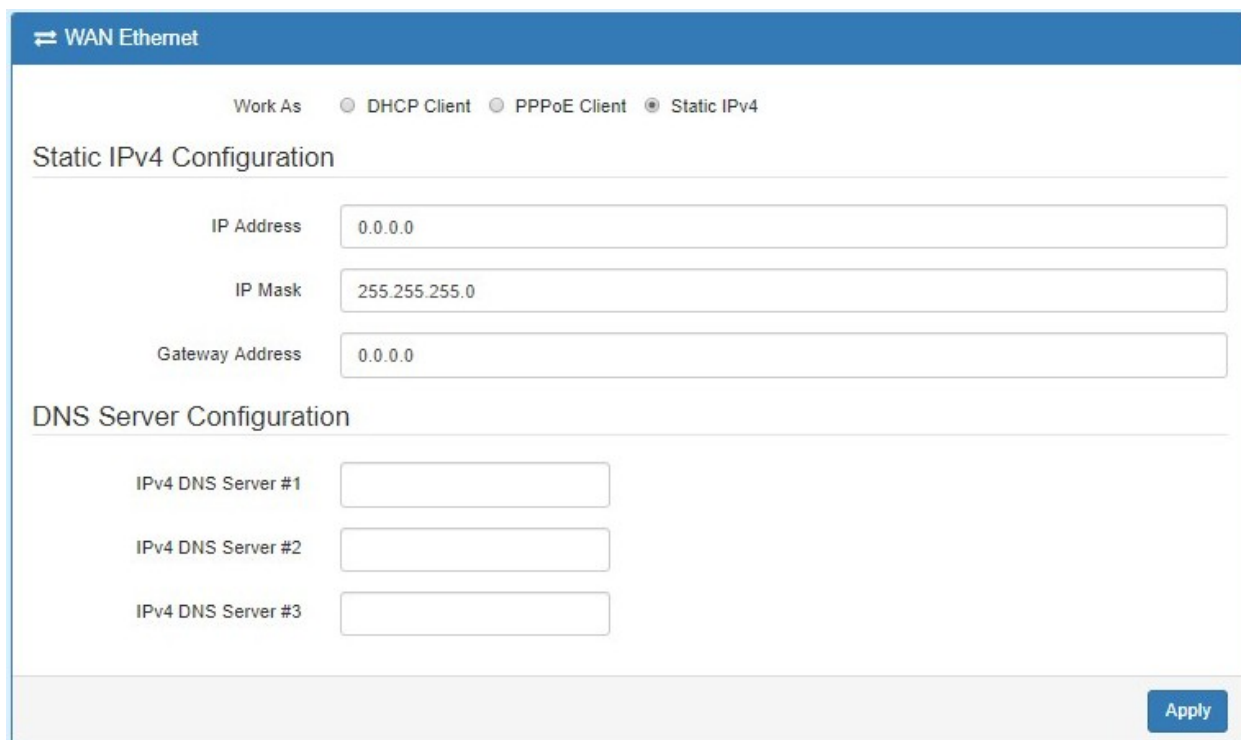
User Name

Password

Service Name

Apply

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



WAN Ethernet

Work As  DHCP Client  PPPoE Client  Static IPv4

Static IPv4 Configuration

IP Address

IP Mask

Gateway Address

DNS Server Configuration

IPv4 DNS Server #1

IPv4 DNS Server #2

IPv4 DNS Server #3

Apply

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

## 6.3 WAN > WiFi STA

Station (STA) mode is used to connect to a Wi-Fi network established by an access point.

☰
WiFi STA

STA Mode  Disable  Enable

Hint WiFi STA would stop the WiFi AP function.

Country Code

Tx Power  (1~100)%

---

Scan table

Enable the STA Mode to get the scan table

Manage Known WiFi Networks

Empty Known WiFi Networks

Apply

WAN > WiFi STA	
Item	Description
<b>STA Mode</b>	Disable or Enable this feature.
<b>Tx Power</b>	The TX power setting specifies the strength of the signal.
<b>Scan Table</b>	
<b>Scan</b>	List AP information that can be scanned.
<b>Connect</b>	Connect to your chosen Wireless Access Point.
<b>Manage Known WiFi Networks</b>	
<b>Connect</b>	Connect to your chosen Wireless Access Point.
<b>Delete</b>	Delete your choice of Wireless Access Point.

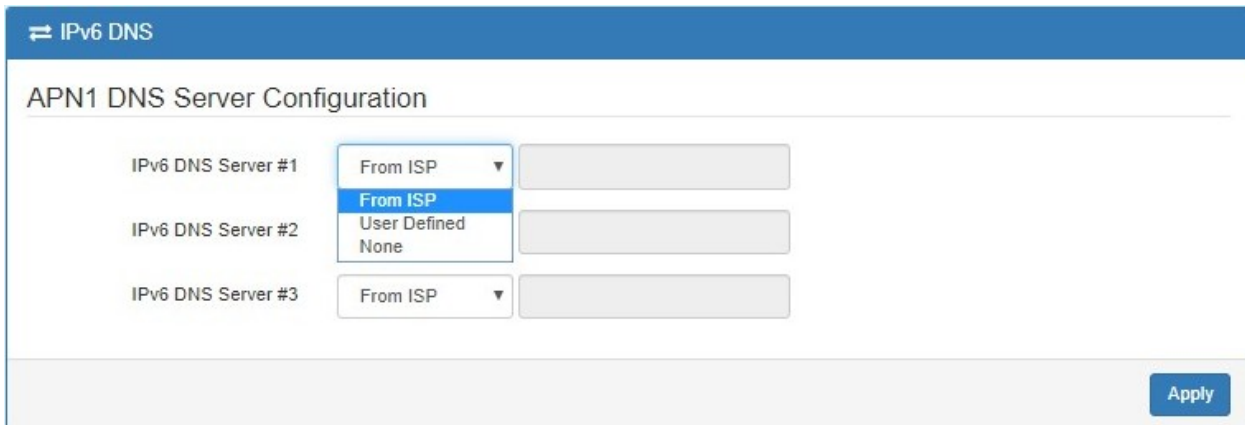
## 6.4 WAN > IPv6 DNS

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



The screenshot shows the 'IPv6 DNS' configuration page for 'APN1 DNS Server Configuration'. It features three rows, each for an IPv6 DNS Server (#1, #2, and #3). Each row has a dropdown menu currently set to 'From ISP' and an adjacent empty text input field. An 'Apply' button is located at the bottom right of the configuration area.

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, showing three options: 'From ISP' (highlighted in blue), 'User Defined', and 'None'. The other two servers remain set to 'From ISP'.

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

## 6.5 Health Check

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 WAN “Health Check” and the system would switch to LTE connection and switch back whenever Ethernet is able to access internet again.



⇌
WAN Health Check

Health Check  Disable  Enable

Method  Ping  DNS Lookup

Use the first two DNS from ISP

Interval  (1 ~ 60 Seconds)

IPv4 Host 1  (Must)

IPv4 Host 2  (Option)

Hint Wan Priority: Auto  
Health Check: Enable

- WAN connection would fail over to next priority connection and change back whenever health check PASS.

Apply

WAN > Health Check	
Item	Description
<b>Health Check</b>	<ul style="list-style-type: none"> <li>Select from Disable or Enable. The default is Enable.</li> <li>When Disable is chosen, the connection will NOT be treated as down of IP routing error.</li> </ul>
<b>Method</b>	<p>This setting specifies the health check method for the WAN connection. This Value can be PING, DNS Lookup. The default is Ping.</p> <p>DNS Lookup: Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result.</p>
<b>Use the first two DNS from ISP</b>	<ul style="list-style-type: none"> <li>If this setting is checked, the first two DNS from ISP will be DNS lookup targets for checking a connection health.</li> <li>If this setting is not checked, Host 1 must be filled, while a value for Host 2 is optional.</li> </ul>
<b>Interval</b>	The interval is from 1 to 60 seconds.
<b>IPv4 Host 1</b>	Input the address of IPv4 Host 1. Host1 must be filled.
<b>IPv4 Host 2</b>	Input the address of IPv4 Host 2. Host2 is optional.
<b>LTE Keep Alive</b>	Enable LTE Keep Alive to continue to send health check packages to avoid no network traffic cause operation kick out the connection.
<b>LTE Keep Interval</b>	LTE Keep Alive interval is from 1 to 60 seconds.
<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.	Value
SIM Status	Ready
Operator	Chunghwa Telecom
Modem Access	FDD LTE
IMSI	466924202684767
Phone Number	
Band	LTE BAND 3
EARFCN	1750
PLMN	46692
Roaming	No
Uplink Speed Kbps	0.000
Downlink Speed Kbps	0.000
Tx/Rx KBytes	35.000/31.000
Tx/Rx Dropped Packets	0/0
LTE Net Mode	Router Only

### ✓ WAN Ethernet

Attr.	Value
IPv4 Address	192.168.0.164
IPv4 Mask	255.255.255.0
Default Gateway	192.168.0.250
IPv4 Conn Time	15:59

### LAN Ethernet

Attr.	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	2001:b400:e331:614c::1
IPv6 Conn Time	15:50
Uplink Speed Kbps	0.000
Downlink Speed Kbps	0.000
Tx/Rx KBytes	262.000/0.000
Tx/Rx Dropped Packets	0/0

## 7 Configuration > LTE

This section allows you to configure LTE Config, GPS, GPS Track, APN Config, APN1 Usage, SMS, Serving Cell, Lock PCIs, Lock Bands, DNS, Search Operators, and USSD.

LTE 
LTE Config
GPS
GPS Track 
APN Config
APN1 Usage
SMS
Serving Cell
Lock PCIs
Lock Bands
DNS
Search Operators
USSD

## 7.1 LTE > LTE Config

You can set up the LTE Configuration.

LTE Config

LTE Config

Change this field require rebooting

MTU

min: 700; max: 1500

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>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.

## 7.2 LTE > GPS

This section allows you to get GPS status and set the GPS configuration to report the location.

### 7.2.1 Status

In the status tab, it shows the current device location.

GPS

Status
Config

Attr.	Value
Latitude	0
Longitude	0
Horizontal	0
Altitude	0
Date	
Time	
Satellite	0

LTE > GPS > Status	
Item	Description
Latitude	Latitude
Longitude	Longitude
Horizontal	Horizontal precision:0.5-99.9
Altitude	The altitude of antenna away from the sea level(unit: m), accurate to one decimal place
Date	UTC date when fixing position
Time	UTC time when fixing position
Satellite	Number of satellites

## 7.2.2 Config

This section allows you to set up GPS configuration and send out GPS location to TCP Server or display in log.

📶 GPS

Status
Config

Report To  TCP Server  LOG

TCP Server

---

Interval  (10 ~ 3600 Seconds)

IPv4 Address

IPv4 Address Port

IPv6 Address

IPv6 Address Port

Report Prefix  Default: IMEI

Apply

LTE > GPS > Config	
Item	Description
Report to	Select from TCP Server and LOG.
Internal	Query GPS interval.
IPv4 Address	GPS IPv4 TCP Server Address.
IPv4 Address Port	GPS IPv4 TCP Server Port.
IPv6 Address	GPS IPv6 TCP Server Address.
IPv6 Address Port	GPS IPv6 TCP Server Port.
Report Prefix	Identification for GPS Track.

## 7.3 LTE > GPS Track

This section allows you to see the GPS Track.

📶 GPS Track

- Number of satellites: 0
- Last Positioning Date: --
- Last Positioning Time: --
- Latitude: --
- Longitude: --

## 7.4 LTE > APN Config

This section allows you to set APN Configuration. It includes Connect Policy, Recover APN1, SIM Configuration, APN1 and Data Limitation.

📶 APN Config

**Connect Policy**

Connect Action 🔌 Disconnect

Disable Roaming  No  Yes

---

**Recover APN1**

Recover APN1  No  Yes

When APN1 continuous link down for  times (3 ~ 15)

Reboot

Recover to default APN

Recover to previous working APN

---

**SIM Configuration**    **APN1**

---

Status Ready

SIM PIN Enable

SIM PIN

Confirmed SIM PIN

SIM PUK

Confirmed SIM PUK

Change SIM PIN 🔑 Change

Old PIN

New PIN

PIN Remaining Number 0

PUK Remaining Number 0

Apply

SIM Configuration
APN1

APN

Username

Password

Confirm Password

Auth NONE

Enable IPv6

Data Limitation

Already Used Data (MB) 14956

Mode  Disable  Enable

Max Data Limitation (MB)

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

Now Time Date: 26 Hours: 7 Minutes: 54 Seconds: 3

Apply

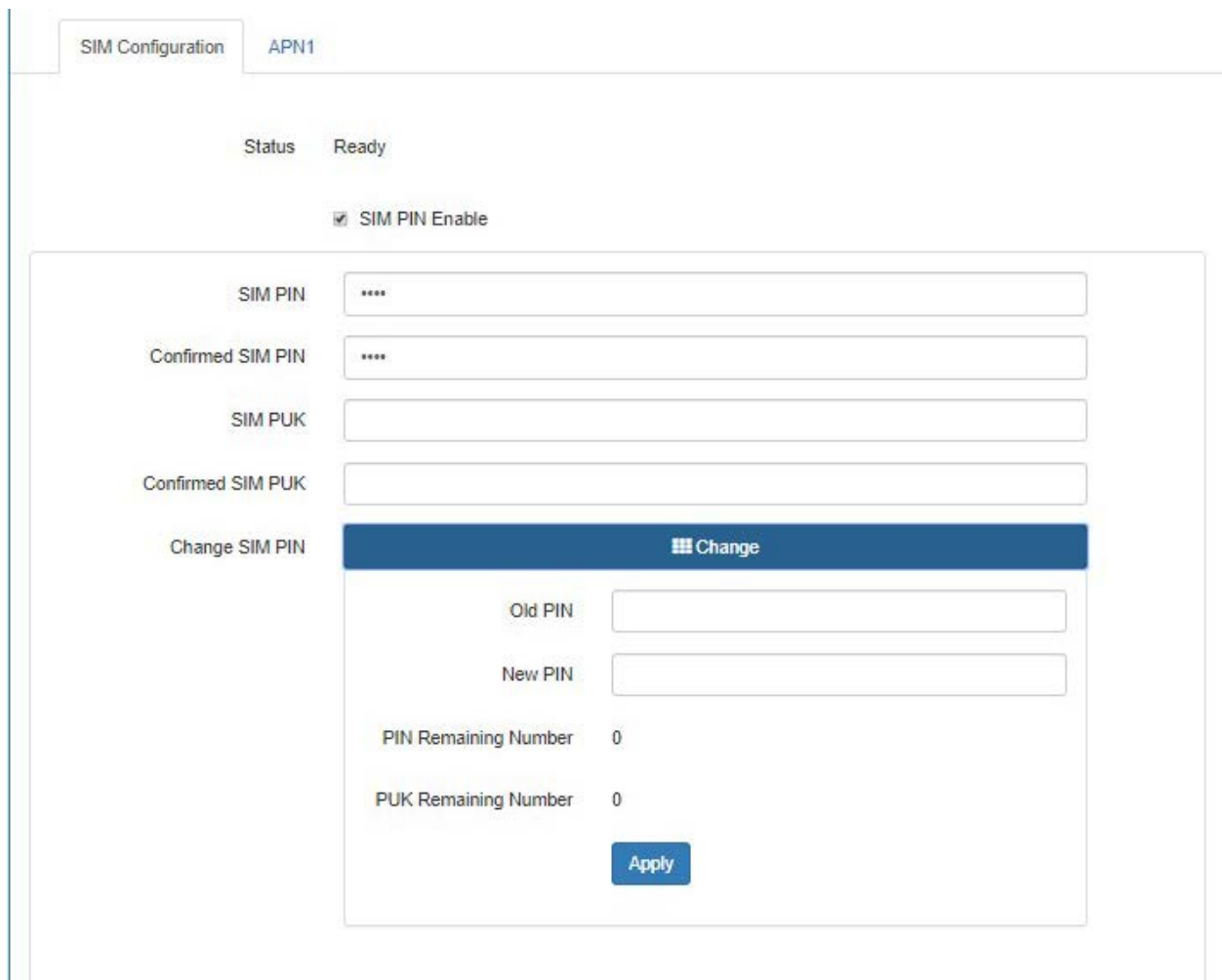
LTE > APN Config	
Item	Description
<b>Connect Policy</b>	
<b>Connect Action</b>	<ul style="list-style-type: none"> <li>● <b>Disconnect:</b> When getting connection, the <span style="border: 1px solid black; padding: 2px;">Disconnect</span> button appear. After manually click Disconnect, the system would not automatically get connection until next reboot.</li> <li>● <b>Connect:</b> After manually disconnect, it will show <span style="border: 1px solid black; padding: 2px;">Connect</span> button. Click to get connection or reboot the device to make it automatically connect.</li> </ul>
<b>Disable Roaming</b>	<ul style="list-style-type: none"> <li>● <b>No:</b> Make connection even the device is in roaming state.</li> <li>● <b>Yes:</b> No connection when the device in roaming state.</li> </ul>
<b>Recover APN1</b>	
<b>Recover APN1</b>	<ul style="list-style-type: none"> <li>● <b>No:</b> Not to recover when APN1 is continuous link down.</li> <li>● <b>Yes:</b> Recover APN1 by using specified method.</li> </ul>
<b>When APN1 continuous link down for xx times.</b>	<p>When link down number reach the specified number then the system will proceed recover action.</p> <ul style="list-style-type: none"> <li>● <b>Reboot:</b> Reboot the system.</li> <li>● <b>Recover to default APN:</b> Replace active APN by using factory default APN.</li> <li>● <b>Recover to previous working APN:</b> Replace active APN by using previous working APN.</li> </ul>
<b>SIM Configurations</b>	
<b>Status</b>	Display the status of SIM Card.
<b>SIM PIN Enable</b>	<ul style="list-style-type: none"> <li>● Enable to display SIM PIN setting.</li> <li>● Disable to hide SIM PIN setting.</li> </ul>
<b>SIM PIN</b>	A password personal identification number (PIN) for ordinary use to

	protect your SIM card.
<b>Confirmed SIM PIN</b>	Double confirm SIM PIN password.
<b>SIM PUK</b>	If user input the wrong SIM PIN more than 3 times, the user needs another password personal unblocking code (PUK) for PIN unlocking. Please check your operator for forgotten PUK number.
<b>Confirmed SIM PUK</b>	Double confirm SIM PUK.
<b>Change SIM PIN</b>	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).
<b>Old PIN</b>	Please input the current SIM PIN code.
<b>New PIN</b>	Please input the newly update SIM PIN.
<b>PIN remaining number</b>	Display the allowed remaining PIN retry number.
<b>PUK remaining number</b>	Display the allowed remaining PUK retry number.
<b>APN1</b>	
<b>APN</b>	The Access Point Name (APN) is the name of the setting that set up a connection to the gateway between your carrier's cellular network and the public Internet. Leaving it empty will search internally database automatically by SIM card for connection.
<b>Username</b>	Username for authentication. The username can be input by user or the system will search from internal database if the APN setting is empty.
<b>Password</b>	Password for authentication. The password can be input by user or the system will search from internal database if the APN setting is empty.
<b>Confirm Password</b>	Double confirm password.
<b>Auth: (None/PAP/CHAP)</b>	If Auth mode is not None, most servers require username and password above.
<b>Enable IPv6</b>	If IPv6 is not selected, then only pure IPv4 connection.
<b>Data Limitation</b>	
<b>Mode</b>	Turn on/off the Data Limitation to disable or enable.
<b>Already Used Data (MB)</b>	Display current used Data since last reset.
<b>Max Data Limitation (MB)</b>	Configure maximum Data Limitation.
<b>Monthly Reset</b>	Set up the reset time during the month.
<b>Now Time</b>	Show the current time of system.



### 7.4.1 SIM Configuration

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



The screenshot shows a web interface for SIM configuration. At the top, there are two tabs: "SIM Configuration" (selected) and "APN1". Below the tabs, the status is "Ready". There is a checkbox labeled "SIM PIN Enable" which is checked. The main configuration area contains several input fields: "SIM PIN" (masked with four asterisks), "Confirmed SIM PIN" (masked with four asterisks), "SIM PUK", and "Confirmed SIM PUK". Below these fields is a "Change SIM PIN" section. This section has a blue "Change" button. Underneath the button are two input fields: "Old PIN" and "New PIN". At the bottom of this section, there are two rows of text: "PIN Remaining Number 0" and "PUK Remaining Number 0". A blue "Apply" button is located at the bottom of the "Change SIM PIN" section.

## 7.5 LTE > APN1 Usage

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

### (1) Real-Time Usage:

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



## (2) Hourly Usage:

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



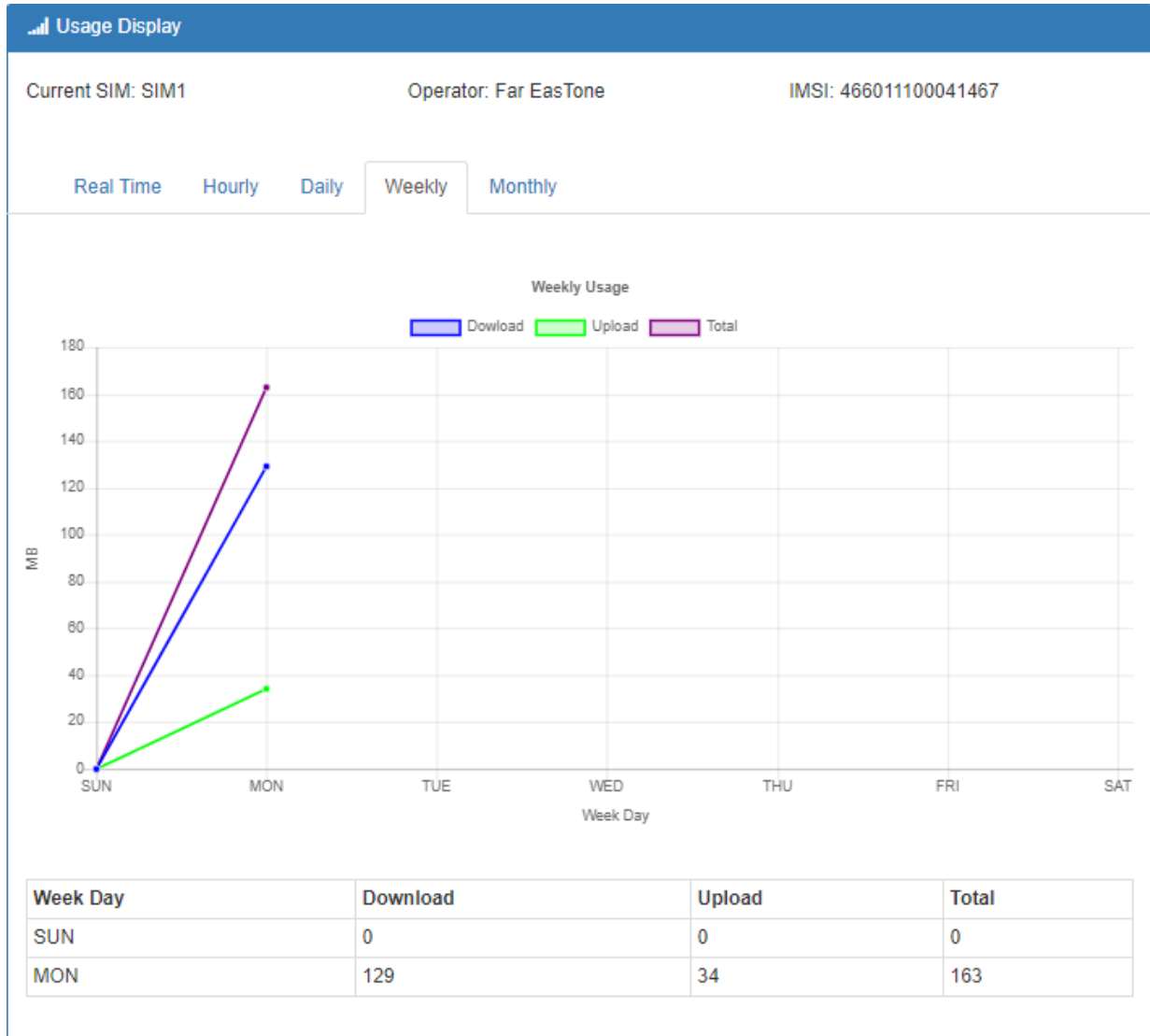
### (3) Daily Usage:

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



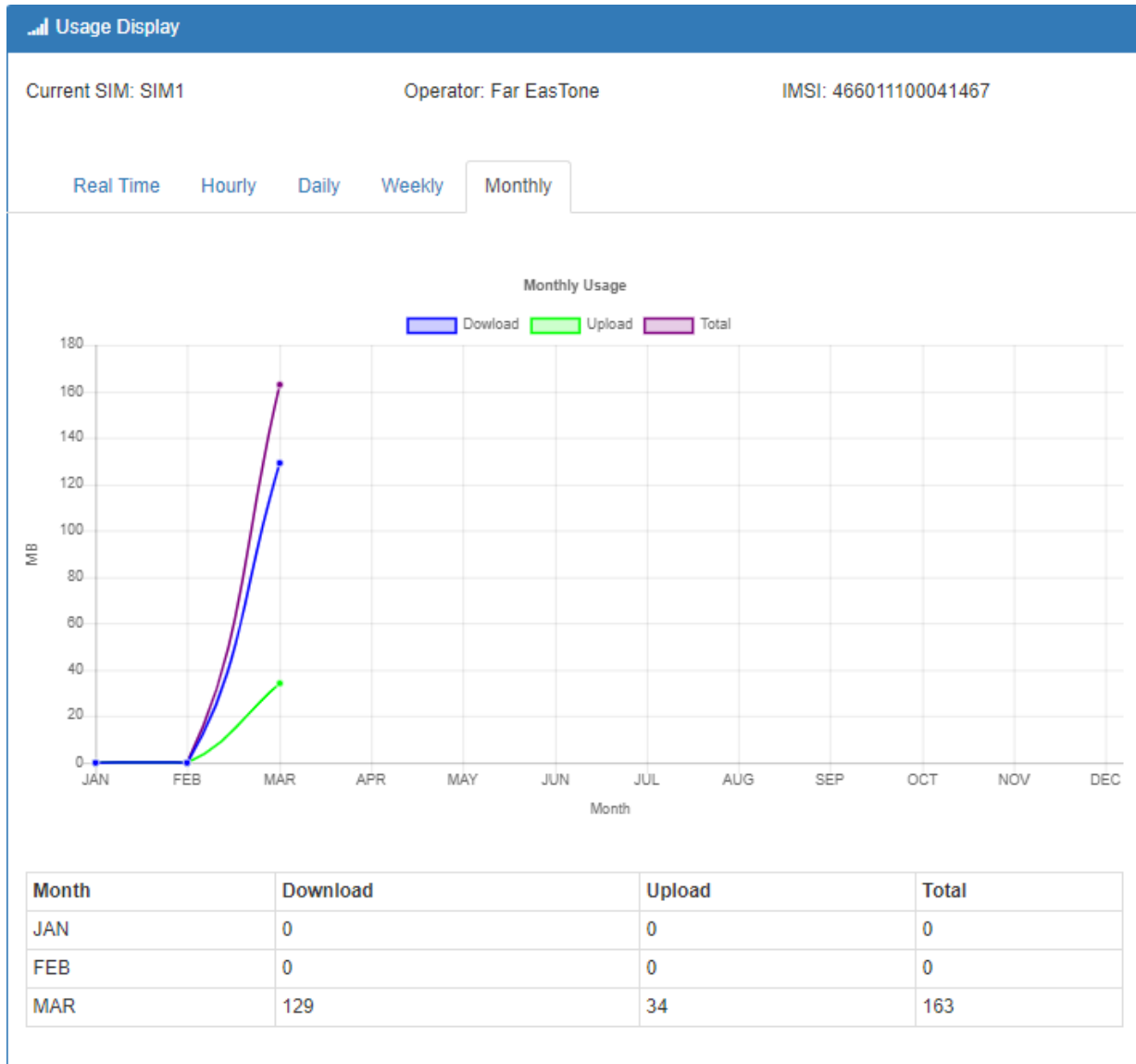
#### (4) Weekly Usage:

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



### (5) Monthly Usage:

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



## 7.6 LTE > SMS

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

- (1) When enabling **SMS Action**, it allows trust phone number which in **trusted and on duty members** list by sending key words SMS to trigger device setting/action/query status.

SMS




SMS Action
View SMS

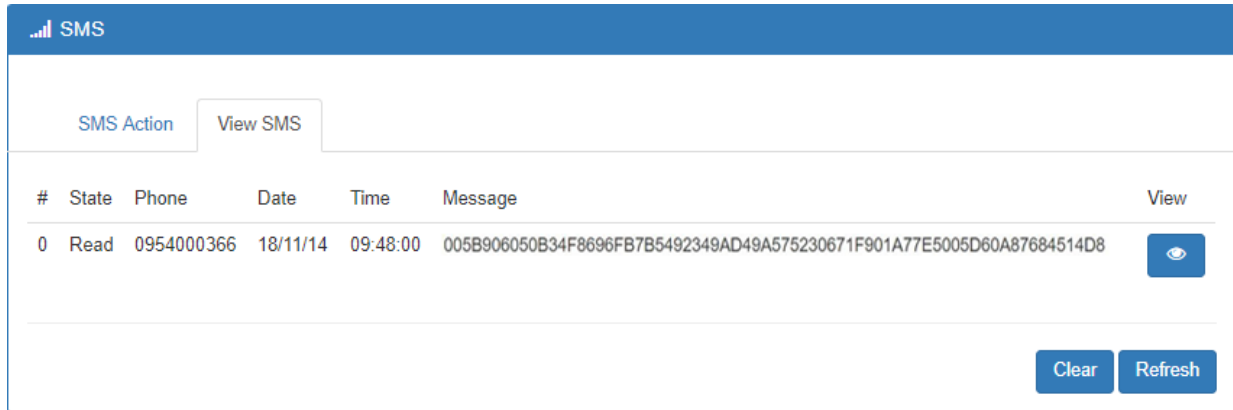
Mode  Disable  Enable

**Actions and Keywords Setup**


Reboot	<input type="text" value="##SMS REBOOT##"/>
Disconnect LTE	<input type="text" value="##MOBILE DISCONNECT##"/>
Connect LTE	<input type="text" value="##MOBILE CONNECT##"/>
Disable OpenVPN	<input type="text" value="##OPENVPN DISABLE##"/>
Enable OpenVPN	<input type="text" value="##OPENVPN ENABLE##"/>
Disable IPsec	<input type="text" value="##IPSEC DISABLE##"/>
Enable IPsec	<input type="text" value="##IPSEC ENABLE##"/>
Query Mobile Status	<input type="text" value="##MOBILE STATUS##"/>
Disable Alarm	<input type="text" value="##DISABLE ALARM##"/>
Enable Alarm	<input type="text" value="##ENABLE ALARM##"/>
Disable DO Alarm	<input type="text" value="##DISABLE DO ALARM##"/>
Enable DO Alarm	<input type="text" value="##ENABLE DO ALARM##"/>
Disable SMS Alarm	<input type="text" value="##DISABLE SMS ALARM##"/>
Enable SMS Alarm	<input type="text" value="##ENABLE SMS ALARM##"/>
Disable SNMP Alarm	<input type="text" value="##DISABLE SNMP ALARM##"/>
Enable SNMP Alarm	<input type="text" value="##ENABLE SNMP ALARM##"/>
Disable E-Mail Alarm	<input type="text" value="##DISABLE EMAIL ALARM##"/>
Enable E-Mail Alarm	<input type="text" value="##ENABLE EMAIL ALARM##"/>
DO On	<input type="text" value="##DO ON##"/>
DO Off	<input type="text" value="##DO OFF##"/>
DO Pulse	<input type="text" value="##DO PULSE##"/>
Restore DO Alarm	<input type="text" value="##RESTORE DO ALARM##"/>

Hint: Only accept SMS from trusted and on duty members

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



The screenshot shows a web interface for managing SMS. At the top, there is a blue header with a signal strength icon and the text "SMS". Below the header, there are two tabs: "SMS Action" and "View SMS", with "View SMS" being the active tab. The main content area contains a table with the following columns: "#", "State", "Phone", "Date", "Time", "Message", and "View". A single row of data is visible, representing a read message from phone number 0954000366 on 18/11/14 at 09:48:00. The message content is a long alphanumeric string. To the right of the message is a blue "View" button with an eye icon. At the bottom right of the interface, there are two buttons: "Clear" and "Refresh".

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



The screenshot shows a modal window displaying the details of a message. At the top, the date and time "18/11/14 09:48:00" are shown next to a close button (X). Below this, the full alphanumeric message content is displayed. At the bottom right of the modal, there is a "Close" button.

18/11/14 09:48:00

005B906050B34F8696FB7B5492349AD49A575230671F901A77E5005D60A87684514D8  
CBB9AD49A575C0765BC003359295F8C5230671F002E4EFB610F937556DE8986672C7  
C218A0A621675

Close



## 7.7 LTE > Serving Cell

This section displays all parameters, including the following items:

📶 Serving Cell	
Attr.	Value
Rate	LTE
RSRP	-84
RSRQ	-10
SINR	7
RSCP	
ECIO	0
Cell Identity	318565-31
eNB ID	318565
Cell ID	31
PCI ID	95
EARFCN	3650
UL Bandwidth	10MHz
DL Bandwidth	10MHz
RSSI	-57 dBm
State	NOCONN
Band	LTE BAND 8

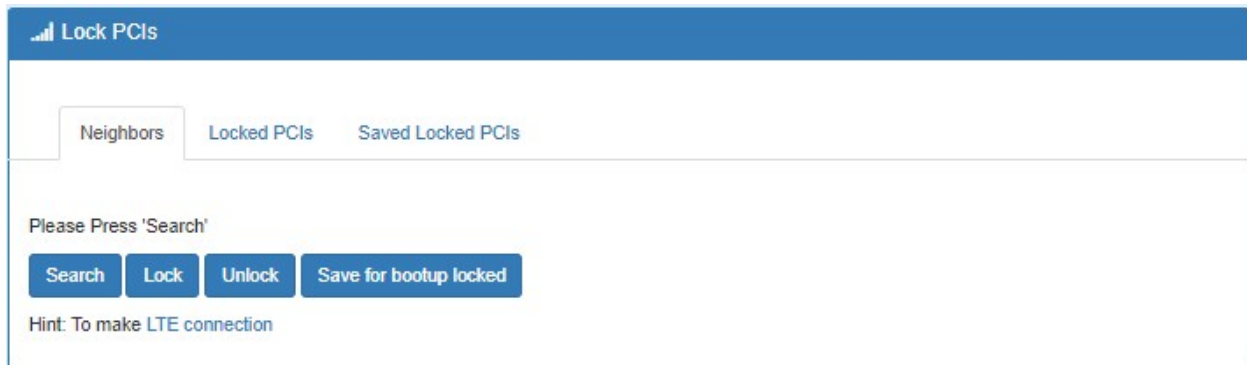
[Refresh](#)

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

## 7.8 LTE > Lock PCIs

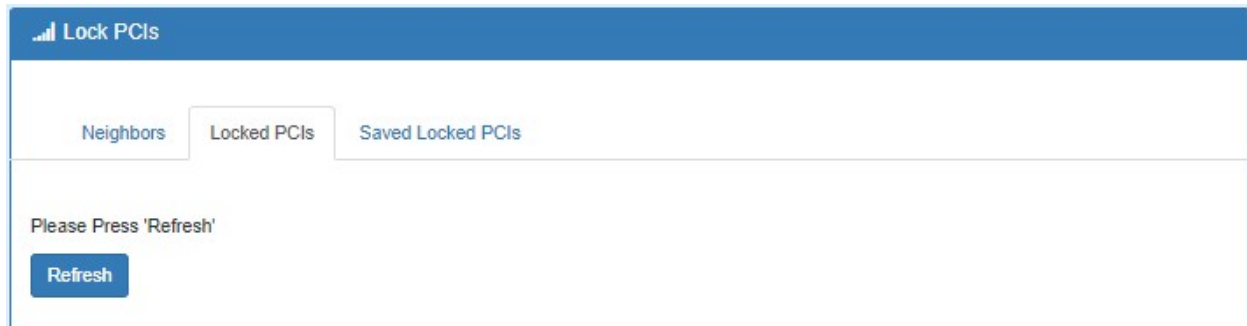
This section allows you to set Lock PCIs. It includes Neighbors, Locked PCIs, Saved Locked PCIs.

### (1) Neighbors

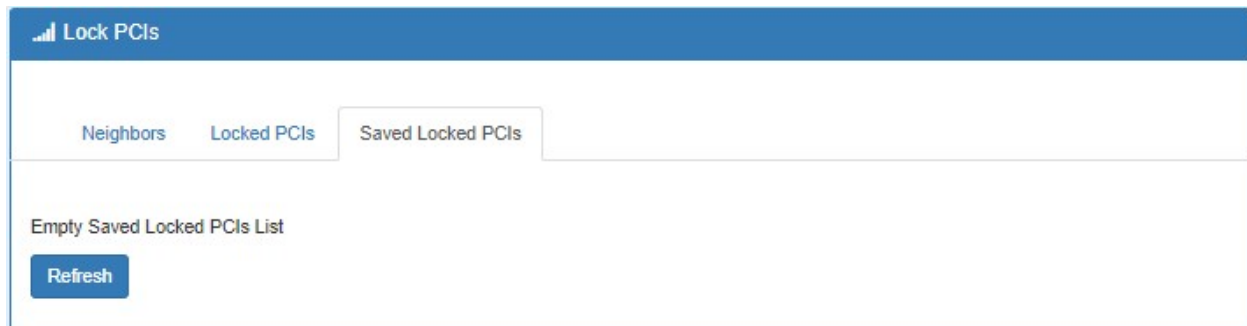


LTE > Lock PCIs > Neighbors	
Item	Description
<b>Search</b>	Search Neighbors from the Air for further action.
<b>Lock</b>	Select multiple PCI (Physical Cell ID) from Neighbor List to lock.
<b>Unlock</b>	Unlock all.
<b>Save for bootup locked</b>	Save selected lock PCIs for next boot up.

### (2) Locked PCIs: Click **Refresh** button to display all locked PCI (Physical Cell ID) information.



### (3) Saved Locked PCIs: Click **Refresh** button to display all saved locked PCI (Physical Cell ID) information.



## 7.9 LTE > Lock Bands

Please check Hint for module support bands and then select your desired multiple bands to lock for use. It allows you to restore your default bands.

📶 Lock LTE Bands

LTE Bands

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

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

Restore Default Band
Apply

## 7.10 LTE > DNS

This section allows you to set LTE specific DNS setting.

📶 DNS

APN1 DNS Server Configuration

---

IPv4 DNS Server #1 From ISP ▼

IPv4 DNS Server #2 From ISP ▼

IPv4 DNS Server #3 From ISP ▼

Apply

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

## 7.11 Search Operators

This section is to search the operators and get the status.

Search Operators			
State	Operator	PLMN	Act
Current	Chunghwa Telecom	46692	E-UTRAN
Available	Chunghwa Telecom	46692	UTRAN
Available	Far EasTone	46601	E-UTRAN
Forbidden	TWNAPT	46605	GSM
Forbidden	T Star	46689	UTRAN
Forbidden	TW Mobile	46697	UTRAN
Available	Far EasTone	46601	UTRAN
Forbidden	T Star	46689	E-UTRAN
Forbidden	TW Mobile	46697	E-UTRAN

LTE > Search Operators	
Item	Description
STATE	<ul style="list-style-type: none"> <li>• Current: Current connection.</li> <li>• Available: Possible connection.</li> <li>• Forbidden: Forbidden connection.</li> </ul>
OPERATOR	Operator Name.
PLMN	Public Land Mobile Network ID.
ACT	3GPP Technology.

## 7.12 LTE > USSD

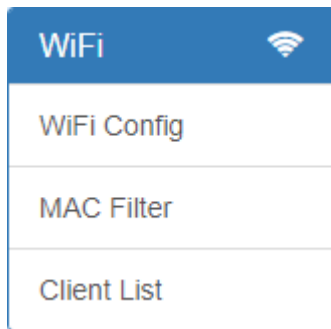
This section is to send USSD and get the response from the operator.

USSD	
USSD Input	<input type="text"/> <input type="button" value="Send"/>
Hint	Maximum Response Time: 120 seconds, determined by network.
Responded	<input type="text"/>

LTE > USSD	
Item	Description
USSD Input	Input the USSD you want to send.
Responded	The response from operator according your USSD.

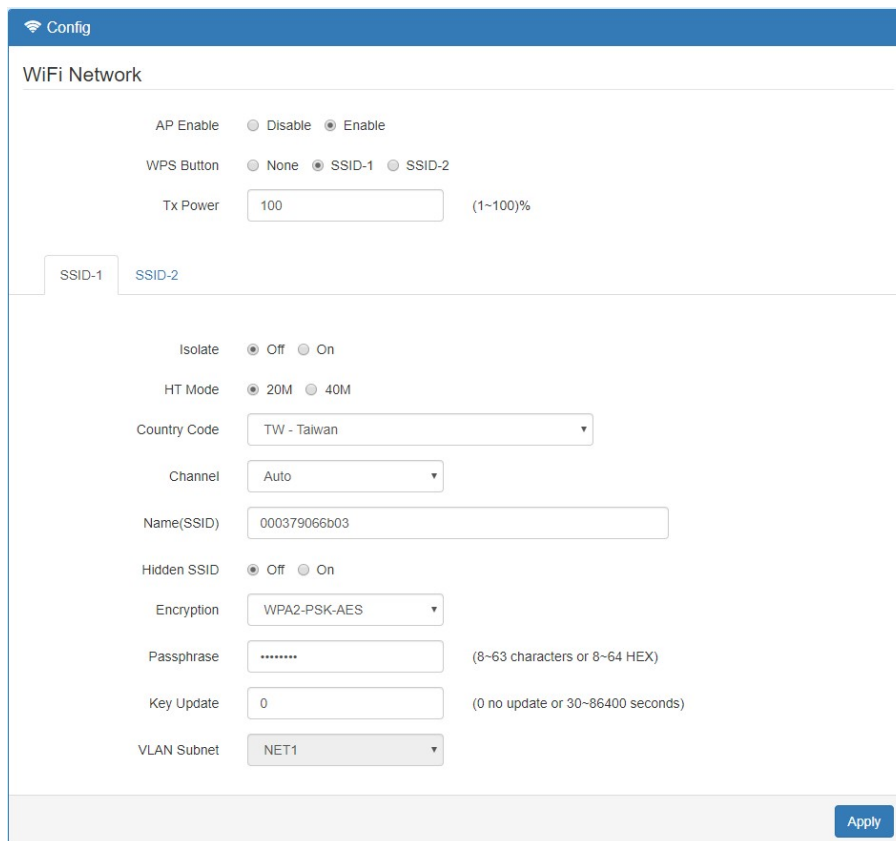
## 8 Configuration > WiFi

This section allows you to configure WiFi and it is used for ICR111WG model.



### 8.1 WiFi > WiFi Config

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

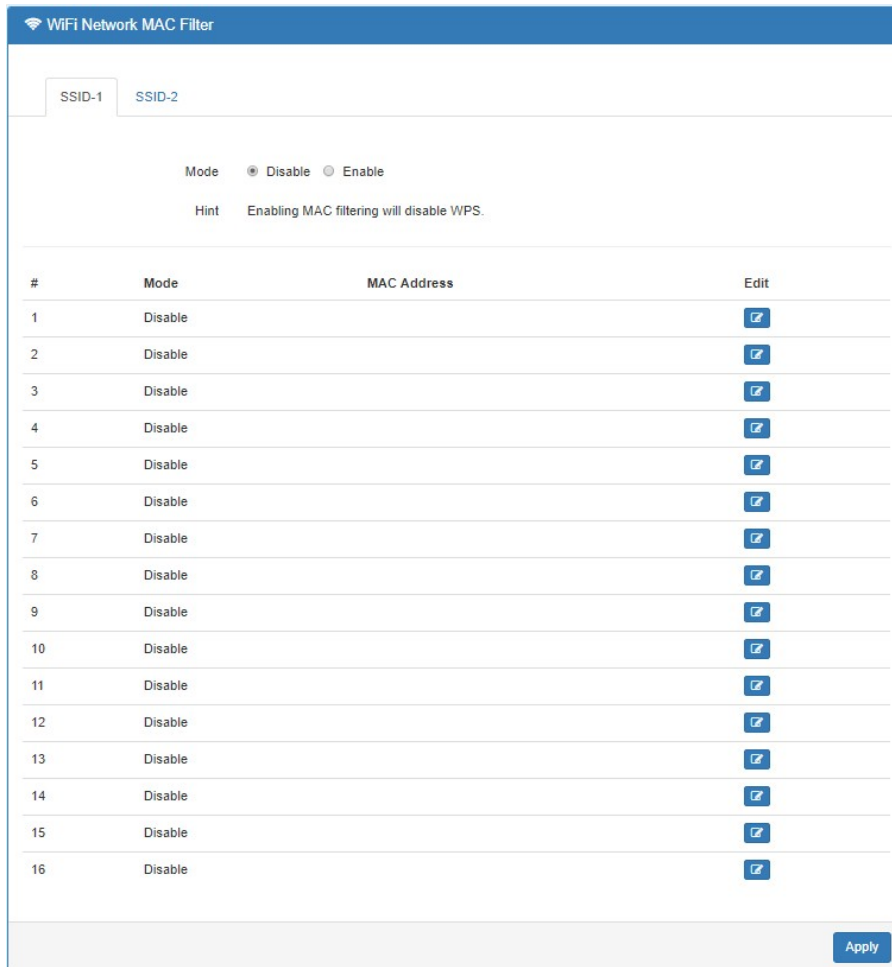


WiFi > Config	
Item	Description
<b>AP Enable</b>	Turn on/off the Wi-Fi Network. Select from Disable or Enable. The default is Enable.
<b>WPS Button</b>	Hardware button for WPS. Select the SSID you want to bind.
<b>Tx Power</b>	The TX power setting specifies the strength of the signal.
<b>Enable</b>	Turn on/off the SSID Network. Select from Disable or Enable.
<b>Isolate</b>	Isolation is a technique for preventing mobile devices connected to

WiFi > Config	
Item	Description
	an AP from communicating directly with each other.
<b>HT Mode (HT Capability)</b>	<ul style="list-style-type: none"> <li>• 20M: Only 20MHz Operation is supported.</li> <li>• 40M: Both 20MHz and 40MHz Operation is supported.</li> </ul>
<b>Country Code</b>	Select Country Area for supported Channels
<b>Channel</b>	Auto (Automatically select the best channel) or manually select channel number.
<b>Name(SSID)</b>	SSID is Wi-Fi identification. The maximum length is 32.
<b>Hidden SSID</b>	SSID hiding is the process of hiding the network name from being publicly broadcast.
<b>Encryption</b>	None or WPA2-PSK-AES.
<b>Passphrase</b>	Strings with a legal length of 8 to 63 or a length of 64 should belong to [0-9 A-F a-f].
<b>Key Update</b>	0 means no update or 30~86400 seconds update period.
<b>VLAN Subnet</b>	Select the VLAN Subnet you want to bind.

## 8.2 WiFi > MAC Filter

This section allows you to set up MAC Filter.



WiFi Network MAC Filter

SSID-1 SSID-2

Mode  Disable  Enable

Hint Enabling MAC filtering will disable WPS.

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

Apply

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

**Edit MAC Filter Entry #1 for SSID-1**

Mode  Disable  Enable

MAC Address

**Save**

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

### 8.3 WiFi > Client List

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

**Client List**

WiFi Client List

SSID-1 SSID-2

MAC Address	IP Address	Connected Time
E0:05:C5:7B:7A:C3	192.168.1.200	9

**Refresh**

**Client List**

WiFi Client List

SSID-1 SSID-2

MAC Address	IP Address	Connected Time
E0:05:C5:7B:7A:C3	192.168.1.200	0

**Refresh**

WiFi > Client List	
Item	Description
<b>MAC Address</b>	MAC Address
<b>IP Address</b>	Client IP Address
<b>Connected Time</b>	Connected Time in Seconds.

## 9 Configuration > LAN

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

LAN	⇌
IPv4	
IPv6	
VLAN	
Subnet	

### 9.1 LAN > IPv4

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

⇌ LAN IPv4

IP Address

IP Mask

**DHCP Server Configuration**

DHCP Server  On

IP Address Pool From  To

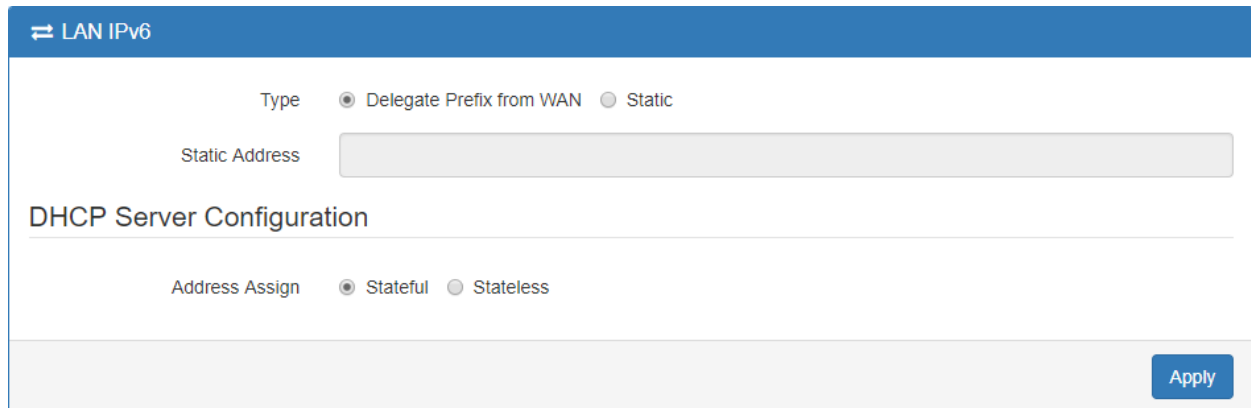
Static IP Addresses

LAN > IPv4	
Item	Description
<b>LAN IPv4</b>	<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.
<b>DHCP Server Configuration</b>	<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>
<b>IP Address Pool</b>	<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>
<b>Static IP Addresses</b>	DHCP server support static IP address assignment. The static IP address can be added by clicking the <b>+Add Static IP Address button</b> . Each static IP consist of mode (on/off), MAC and IP address. <ul style="list-style-type: none"> <li>Mode: Turn on/off the static IP address.</li> <li>MAC: The MAC address of target host or PC.</li> <li>IP: The desired IP address for target host or PC.</li> </ul>



## 9.2 LAN > IPv6

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



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

## 9.3 LAN > VLAN

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



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

The **VLAN Isolation** function allows administrator to separate the different Subnet (VLAN). When

it is **on**, the different Subnet (VLAN) user cannot communication each other.

≡
VLAN

Mode  Off  Tag Base

VLAN Isolation  Off  On

Enable	Subnet	VID	Port		
			LAN	LAN2	Router
<input checked="" type="checkbox"/>	NET1 ▼	1	<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 type="checkbox"/>	NET3 ▼	3	<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 type="checkbox"/>	NET5 ▼	5	<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 type="checkbox"/>	NET7 ▼	7	<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"/>
PVID			1	1	1
Tag Mode			Trunk ▼	Trunk ▼	Trunk ▼

Apply

For each row, the settings can be enabled or disabled by checkbox and select the **Subnet** and the **VLAN ID (VID)**. The **Subnet** sets up the IP address and IP mask for the router, so this router can communicate with the third party by this IP address and IP mask on this VLAN.

**(Note:** The NET1 can't remove it and fixes in the first 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 window will show the Subnet window from the LAN catalogue.)

There are two ports for Tag Base Mode, including LAN and LAN2. And one Router port which is a gate allows those ports to access internet or the router. The PVID and Tag Mode are for LAN and LAN2 ports. The PVID provides the untagged devices to communicate with third-party devices.

**(Note:** The untagged devices mean not to support 802.1p VLANs.)

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

LAN > VLAN (1-port LANs)	
Item	Description
<b>Mode</b>	The VLAN mode is Off or Tag Base (802.1p VLAN).
<b>VLAN Isolation</b>	The VLAN Isolation is Off or On.
<b>Enable</b>	The assigned row of settings are enabled.
<b>Subnet</b>	Set up 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, LAN2 and Router.
<b>PVID</b>	<ul style="list-style-type: none"> <li>The PVID range from 1 to 4094.</li> <li>Set up 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 Trunk port setting is connected to another 802.1p VLAN aware switch or device.</li> <li>The Access port setting is connected to a single untagged device.</li> </ul>

## 9.4 LAN > Subnet

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

⇌ Subnet

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

Note: Subnet **NET1** is the default IPv4 LAN, go [IPv4](#) for configuration.

Apply

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

Edit Subnet NET2

IP Address

IP Mask

**DHCP Server Configuration**

DHCP Server Configuration

IP Address Pool From  To

Save


## 10 IP Routing

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

<b>IP Routing</b> 
Static Route
Policy Route
RIP
OSPF
BGP

### 10.1 IP Routing > Static Route

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

 Static Route

Mode  Off  On

Settings Status

Mode	Name	Destination	Gateway	Interface	Delete
<input type="radio"/> Off <input checked="" type="radio"/> On	<input type="text"/>	192.168.100.0/24	192.168.1.250		<span style="color: red; font-weight: bold;">✕</span>

Mode  Off  On

Name

Destination

Gateway

Interface

Add

Apply

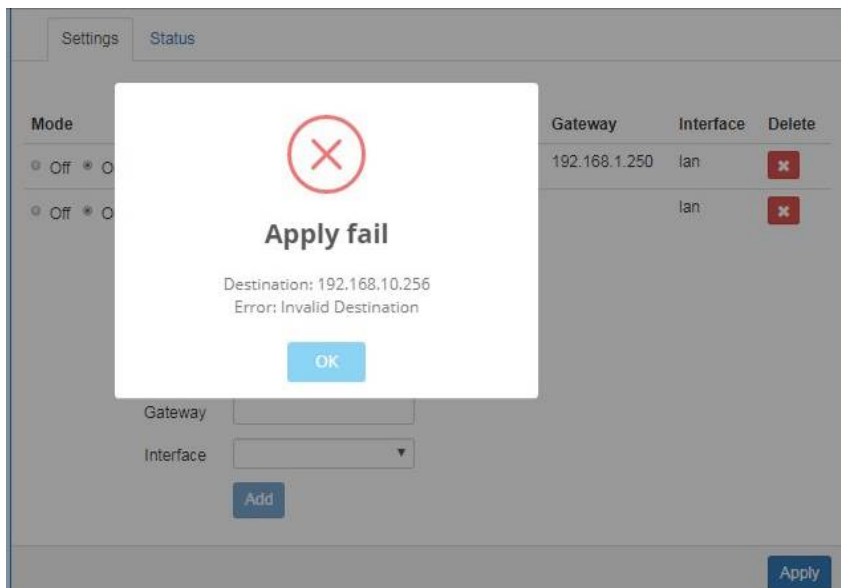
IP Routing > Static Route > Settings	
Item	Description
<b>Mode</b>	The setting is for full network. Select from Off or On.
<b>Settings</b>	
<b>Mode</b>	The setting is for the specific network. Select from Off or On.
<b>Name</b>	Set up each name for your running host or network.

<b>Destination</b>	Fill in the destination of a specific subnet or IP from network.
<b>Gateway</b>	Fill in the gateway address of your router.
<b>Interface</b>	Select the interface from LAN or Ethernet.

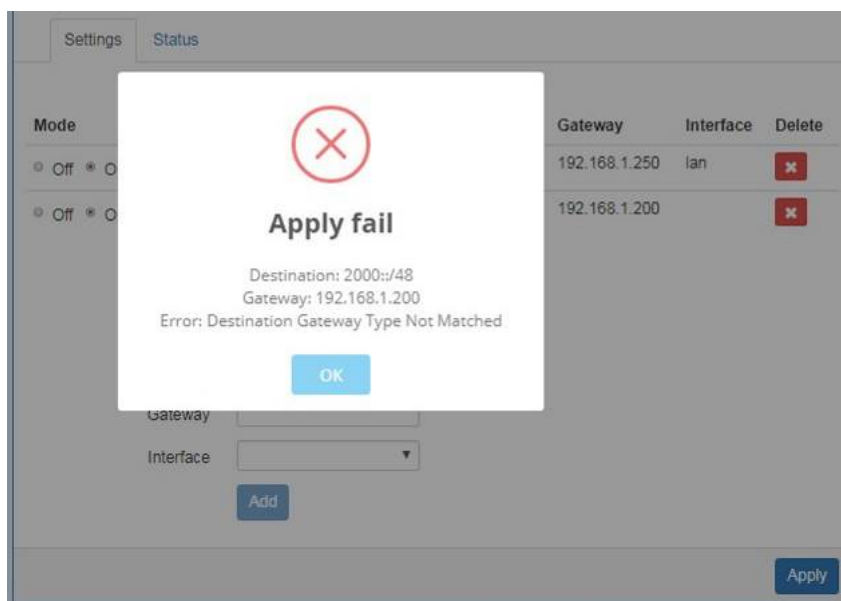
**Note:**

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

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



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



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

**Static Route**

Mode  Off  On

Settings
Status

Destination	Gateway	Interface	Protocol
default	192.168.0.250	WAN Ethernet	
192.168.0.0/24		WAN Ethernet	kernel
192.168.1.0/24		LAN	kernel
2001:b400:e230:cdf::/64		LAN	kernel
2000::/3		LTE APN1	
fe80::656e:8268:78a2:d130		LTE APN1	
fe80::/64		WAN Ethernet	kernel
fe80::/64		ath01	kernel
fe80::/64		LAN	kernel
fe80::/64		LTE APN1	kernel
default	fe80::656e:8268:78a2:d130	LTE APN1	

Apply

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

## 10.2 Policy Route

This section allows you to set up the settings and get the status for Policy Route.

**Note:** Policy Route is only enabled on active interfaces, but it is disabled on deactivated interfaces automatically.

Policy Route

Settings
Status

Mode  Disable  Enable

#	Mode	Name	Source	Destination	Gateway	Interface	Delete
Add Policy Route							
<p>Mode <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p>Name <input style="width: 150px;" type="text"/></p> <p>Source(IP/MASK) <input style="width: 150px;" type="text"/> ex: 192.168.1.20/32</p> <p>Destination(IP/MASK) <input style="width: 150px;" type="text"/> ex: 10.10.1.20/32</p> <p>Then</p> <p>Gateway <input style="width: 150px;" type="text"/></p> <p>Outgoing Interface <input style="width: 150px;" type="text" value="&lt;empty&gt;"/></p> <p style="text-align: center;"><input type="button" value="Add"/></p>							

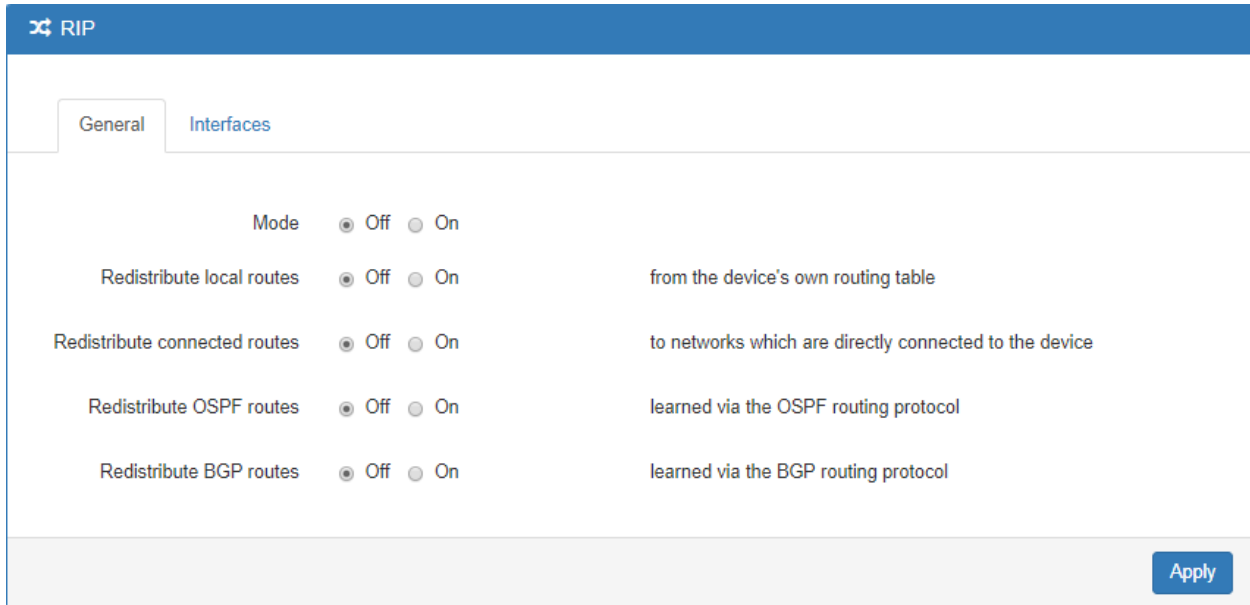
IP Routing > Policy Route	
Item	Description
<b>Mode</b>	The setting is for full network. Select from Disable or Enable.
<b>Settings</b>	
<b>Mode</b>	The setting is for the specific network. Select from Disable or Enable.
<b>Name</b>	Set up each name for your running host or network.
<b>Source(IP/MASK)</b>	Fill in the source of a specific IP/MASK from network.
<b>Destination (IP/MASK)</b>	Fill in the destination of a specific IP/MASK from network.
<b>Gateway</b>	Fill in the gateway address of your router.
<b>Outgoing Interface</b>	Select the interface from LAN or Ethernet.

## 10.3 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.



The screenshot shows the configuration page for RIP. It has two tabs: 'General' (selected) and 'Interfaces'. Under the 'General' tab, there are five rows of configuration options, each with a radio button for 'Off' and 'On':

- Mode:**  Off  On
- Redistribute local routes:**  Off  On. Description: from the device's own routing table
- Redistribute connected routes:**  Off  On. Description: to networks which are directly connected to the device
- Redistribute OSPF routes:**  Off  On. Description: learned via the OSPF routing protocol
- Redistribute BGP routes:**  Off  On. Description: learned via the BGP routing protocol

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

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



⌘ RIP

General
Interfaces

#	Mode	Interface	Authentication	Key	Key ID	Passive	Edit	Delete
<div style="border-bottom: 1px solid #ccc; margin-bottom: 10px;"> <p>Add RIP Interface</p> <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 45%;"> <p>Mode <input type="radio"/> Off <input checked="" type="radio"/> On</p> <p>Interface <input type="text" value="eth1(WAN Ethernet)"/></p> <p>Authentication <input type="text" value="md5"/></p> <p>Key <input type="text"/></p> <p>Key ID <input type="text" value="1"/></p> <p>Passive <input checked="" type="radio"/> Off <input type="radio"/> On</p> <p style="text-align: center;"><input type="button" value="Add"/></p> </div> <div style="width: 50%; font-size: small;"> <p>The key used for authentication (maxlength=16)</p> <p>The ID of the key used for authentication (1-255)</p> <p>Do not send out RIP packets on this interface</p> </div> </div> </div>								

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

## 10.4 IP Routing > OSPF

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

### (1) General Configuration

✕ OSPF

General

Interfaces

Networks

	Mode	<input checked="" type="radio"/> Off <input type="radio"/> On	
Redistribute local routes	<input checked="" type="radio"/> Off <input type="radio"/> On		from the device's own routing table
Redistribute connected routes	<input checked="" type="radio"/> Off <input type="radio"/> On		to networks which are directly connected to the device
Redistribute RIP routes	<input checked="" type="radio"/> Off <input type="radio"/> On		learned via the RIP routing protocol
Redistribute BGP routes	<input checked="" type="radio"/> Off <input type="radio"/> On		learned via the BGP routing protocol

Apply

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

## (2) Interfaces Configuration

There are 2 parts for OSPF Interfaces configuration.

- OSPF Interfaces Summary  
Click **Edit** button to edit the existed interface.  
Click **Delete** button to delete the existed interface.
- Add/Edit OSPF Interface

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

OSPF

General
Interfaces
Networks

								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

Authentication

Key  The key used for authentication (maxlength=16)

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

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

Passive  Off  On Do not send out OSPF packets on this interface

IP Routing > OSPF > Interfaces	
Item	Description
<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
Add/Edit

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)

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

## 10.5 IP Routing > BGP

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

### (1) General Configuration

⌘ BGP

General

Neighbors

Networks

Mode  Off  On

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

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

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

Apply

IP Routing > BGP > General	
Item	Description
<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>

## (2) Neighbor Configuration

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

✕ BGP

General

Neighbors

Networks

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

### Add BGP Neighbor

Mode  Off  On

IP Address

AS Number

Multihop  Off  On

Update Source Mode  Off  On

Update Source Address

Add

IP address of the peer router

Autonomous system number of the peer router

Allow multiple hops between this router and the peer router

Whether to specify the source address to this neighbor

The source address to this neighbor

Apply

IP Routing > BGP > Neighbors	
Item	Description
<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.
<b>Update Source Mode</b>	Whether to specify the source address to this neighbor.
<b>Update Source Address</b>	The source address to this neighbor.

### (3) Networks Configuration

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

✕ BGP

General

Neighbors

Networks

#	Mode	Prefix	Prefix Length	Edit	Delete
1	on	4.4.4.0	24		

Add BGP Network

Mode  Off  On


Prefix  Prefix of the network

Prefix Length  Length of the prefix

IP Routing > BGP > Networks	
Item	Description
<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














## 11 Configuration > VPN

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


VPN 
Open VPN
IPSec
GRE
PPTP Server
L2TP

### 11.1 VPN > Open VPN

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

OpenVPN 							
Mode <input checked="" type="radio"/> Disable <input type="radio"/> Enable							
#	Status	VPN Mode	Device	Protocol	Port	Edit	Wizard
1		Client	TUN	UDP	1701		
2		Client	TUN	UDP	1701		
3		Client	TUN	UDP	1701		
4		Client	TUN	UDP	1701		

#### 11.1.1 Open VPN Common Setting

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



Setting
Log

Mode  Disable  Enable

VPN Mode  Server  Client  Custom

VPN Type  Roadwarrior  Bridging

Status Idle

TLS Mode  Disable  Enable

Cipher

IPv6 Mode  Disable  Enable

Device  TUN  TAP

Protocol  UDP  TCP

Port

VPN Compression  Disable  Enable

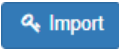
Authentication

VPN > Open VPN > Setting	
Item	Description
<b>Mode</b>	Turn on/off Open VPN to select Disable or Enable.
<b>VPN Mode</b>	<ul style="list-style-type: none"> <li>● <b>Server:</b> Tick to enable Open VPN server tunnel.</li> <li>● <b>Client:</b> Tick to enable Open VPN client tunnel. The default is Client.</li> <li>● <b>Custom:</b> This option allows user to use the .ovpn configuration file to quickly set up VPN tunnel with third-party server or use the Open VPN advanced options to be compatible with other servers.</li> </ul>
<b>VPN Type</b>	<ul style="list-style-type: none"> <li>● <b>Roadwarrior (default)</b></li> <li>● <b>Bridging:</b> Bridging the VPN tunnel and LAN/VLAN</li> </ul>
<b>Status</b>	Display the status of Open VPN.
<b>TLS Mode</b>	Select from Disable or Enable for data security. The default is Disable.
<b>Cipher</b>	The Open VPN 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 Open VPN server.
<b>VPN Compression</b>	Select Disable or Enable to compress the data stream. The default is Disable.
<b>Authentication</b>	<ul style="list-style-type: none"> <li>● Select from two different kinds of authentication ways: Certificate or pkcs#12 Certificate.</li> </ul>

- The pkcs#12 option is only available on the VPN client mode.

### 11.1.2 Open VPN Client Setting

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

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

#### Client

Server Address

Route Client Networks  Off  On

#### Local Network


Network


Netmask

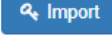
#### NAT

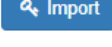
1:1 NAT  Off  On




#### Client - Security

Root CA 

Cert 

Key 

P12 

VPN > Open VPN > Client VPN Mode	
Item	Description
<b>Client</b>	
<b>Server Address</b>	Fill in WAN IP of Open VPN server.
<b>Route Client Networks</b>	Select from Off or On. This setting needs to match the server side. When enabled, the cellular router will auto apply the properly routing rules.
<b>Local Network</b>	
<b>Network</b>	The local network exported by OpenVPN. When keeping this option blank, the OpenVPN will export the LAN network automatically.
<b>Netmask</b>	The local netmask exported by OpenVPN. When keeping this option blank, the OpenVPN will export the LAN netmask automatically.
<b>NAT</b>	

<b>1:1 NAT</b>	<ul style="list-style-type: none"> <li>• Tick to enable NAT Traversal for Open VPN. This item must be enabled when the router under NAT environment.</li> <li>• Select from Off or On.</li> <li>• When two routers' LAN Subnet are same and create Open VPN tunnels, this function should be turned on.</li> </ul>
<b>Client-Security</b>	
<b>Root CA</b>	The Certificate Authority file of Open VPN server could be downloaded from Open VPN server.
<b>Cert</b>	The certification file is for Open VPN client, which could be downloaded from Open VPN server.
<b>Key</b>	The private key file is for Open VPN client, which could be downloaded from Open VPN server.
<b>P12</b>	The PKCS#12 file is for Open VPN client, which could be downloaded from Open VPN server.

### 11.1.3 Open VPN Server Setting

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

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

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

**Roadwarrior**

---

Route Client Networks  Off  On

Connections - Net / Mask

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

**Local Network**

---

Network

Netmask

## NAT

1:1 NAT  Off  On

### Server - Server Security

Root CA [Create](#)

Cert, Key [Create](#)

### Server - User Security

OpenVPN Server Address

User 1  Valid [Create](#)

User 2  Valid [Create](#)

User 3  Valid [Create](#)

User 4  Valid [Create](#)

User 5  Valid [Create](#)

User 6  Valid [Create](#)

User 7  Valid [Create](#)

User 8  Valid [Create](#)

[Back](#)

[Refresh](#)

[Apply](#)

## VPN > Open VPN > Server VPN Mode


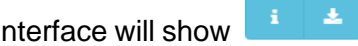


Item	Description
<b>Server</b>	
<b>VPN Network</b>	The network ID for Open VPN virtual network.
<b>VPN Netmask</b>	The netmask for Open VPN virtual network.
<b>Roadwarrior: Route Client Networks</b>	Select from Off or On. The Open VPN server will route the client traffic or not. User should fill in the client IP and netmask when this option is enabled.
<b>Local Network</b>	
<b>Network</b>	The local network exported by OpenVPN. When keeping this option blank, the OpenVPN will export the LAN network automatically.
<b>Netmask</b>	The local netmask exported by OpenVPN. When keeping this option blank, the OpenVPN will export the LAN netmask automatically.
<b>NAT</b>	
<b>1:1 NAT</b>	<ul style="list-style-type: none"> <li>• Tick to enable NAT Traversal for Open VPN. This item must be enabled when router under NAT environment.</li> <li>• Select from Off or On. The default is Off.</li> <li>• When two routers' LAN Subnet are same and create Open VPN tunnels, this function is turned on.</li> </ul>
<b>Server- Server Security</b>	
<b>Root CA</b>	Create Root CA key.

<b>Cert, Key and DH</b>	Create Cert, Key and DH key.
<b>Server- User Security</b>	
<b>User 1 - User 8</b>	According to your requirement, you can create different kinds of user security key from User 1 to User 8.

#### 11.1.4 Set up Open VPN Custom

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

**Note:**

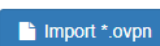


- When clicking the  button, you can import third-party Open VPN configuration that find out from Internet and save the document into your server or PC.
- After importing the file, the interface will show  button. Click  for displaying the information and  for downloading the file.
- For third-party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

Edit Open VPN Connection #1

Setting
Log

Mode  Disable  Enable

VPN Mode  Server  Client  Custom

Custom Config   

Username

Password

Status Idle

Back
Refresh
Apply

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

## 11.2 VPN > IPsec

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

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

Mode  Disable  Enable

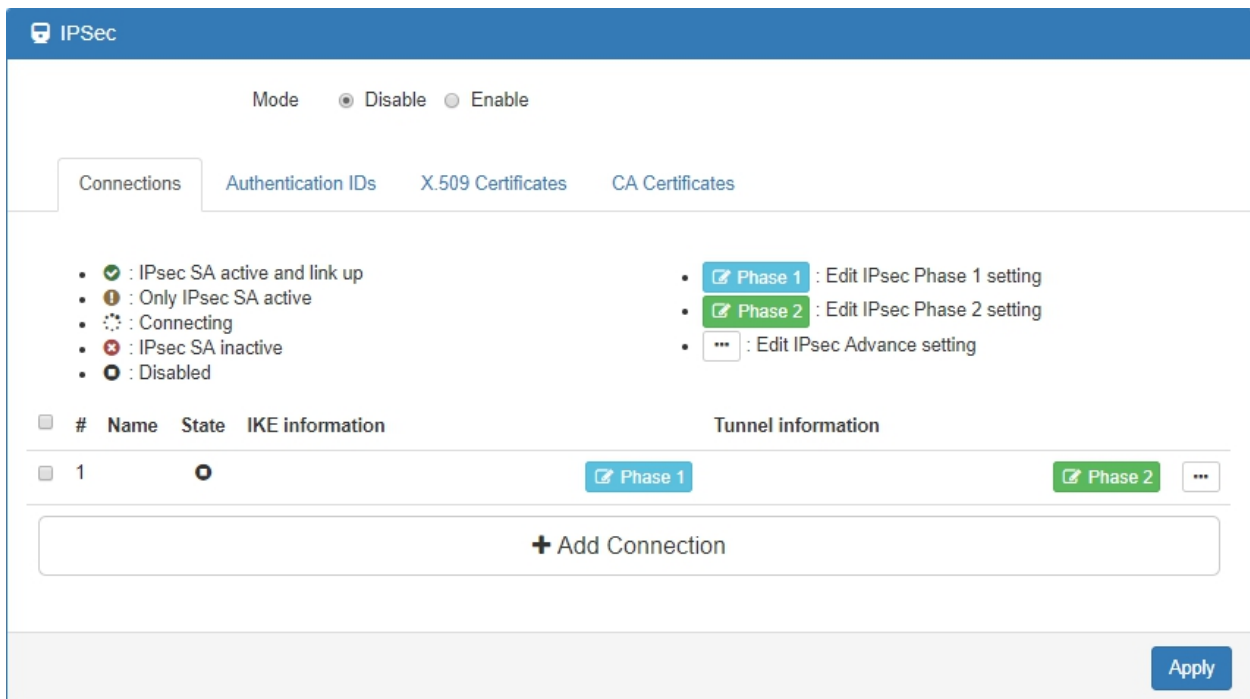
Type  Policy-based  Route-based

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

## 11.2.1 IPsec > Connections

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






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




IPSec

Mode  Disable  Enable

Connections Authentication IDs X.509 Certificates CA Certificates

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

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

#	Name	State	IKE information	Tunnel information
1				<b>Phase 1</b> <b>Phase 2</b> <b>...</b>

**+ Add Connection**

Apply

## (1) IPsec Phase 1 Setting

Connection #1 Phase 1

Mode  Disable  Enable

Name

Protocol

Aggressive mode

Auth Type

Encryption

Hash

DH Group

Lifetime

Local Host

Local ID

Remote Host

Remote ID

Back
Save

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



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

## (2) IPsec Phase 2 Setting

Connection #1 Phase 2

Protocol	<input type="text" value="ESP"/>
Encryption	<input type="text" value="AES128"/>
Hash	<input type="text" value="SHA1"/>
DH Group	<input type="text" value="5 (1536 bit)"/>
Lifetime	<input type="text" value="3 hours"/>
Local Subnet	<input type="text"/>
Remote Subnet	<input type="text"/>
Service	<input type="text" value="Any"/>

Back
Save

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

	<p>If this value is blank, the connection will set it as the “Remote Host” of Phase 1 setting.</p> <p><b>Note:</b> This option only work on Policy-based IPsec VPN type.</p>
<b>Service</b>	<p>Restrict the VPN traffic to the particular protocol only.</p> <p>Select from the Any, TCP, UDP or L2TP.</p>

### (3) IPsec Advance Setting

Connection #1 Advance

DPD interval (s)

DPD retry

Back
Save

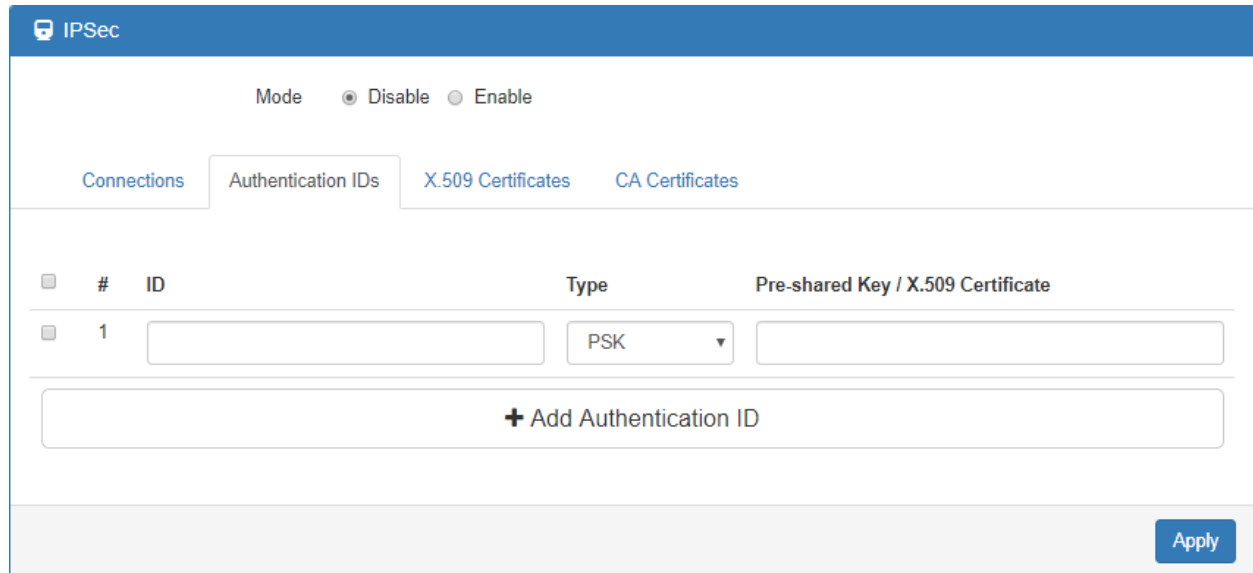
VPN > IPsec > Connections > Advance Setting	
Item	Description
<b>DPD interval</b>	The period time interval to detect dead peers. The default is 30 seconds.
<b>DPD retry</b>	The max number of retry of dead peer detection. The default is 5 times.

## 11.2.2 IPsec > Authentication IDs

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

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

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



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

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

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

### 11.2.3 IPsec > X.509 Certificates

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

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

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

IPSec

Mode    Disable    Enable

Connections
Authentication IDs
X.509 Certificates
CA Certificates

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

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

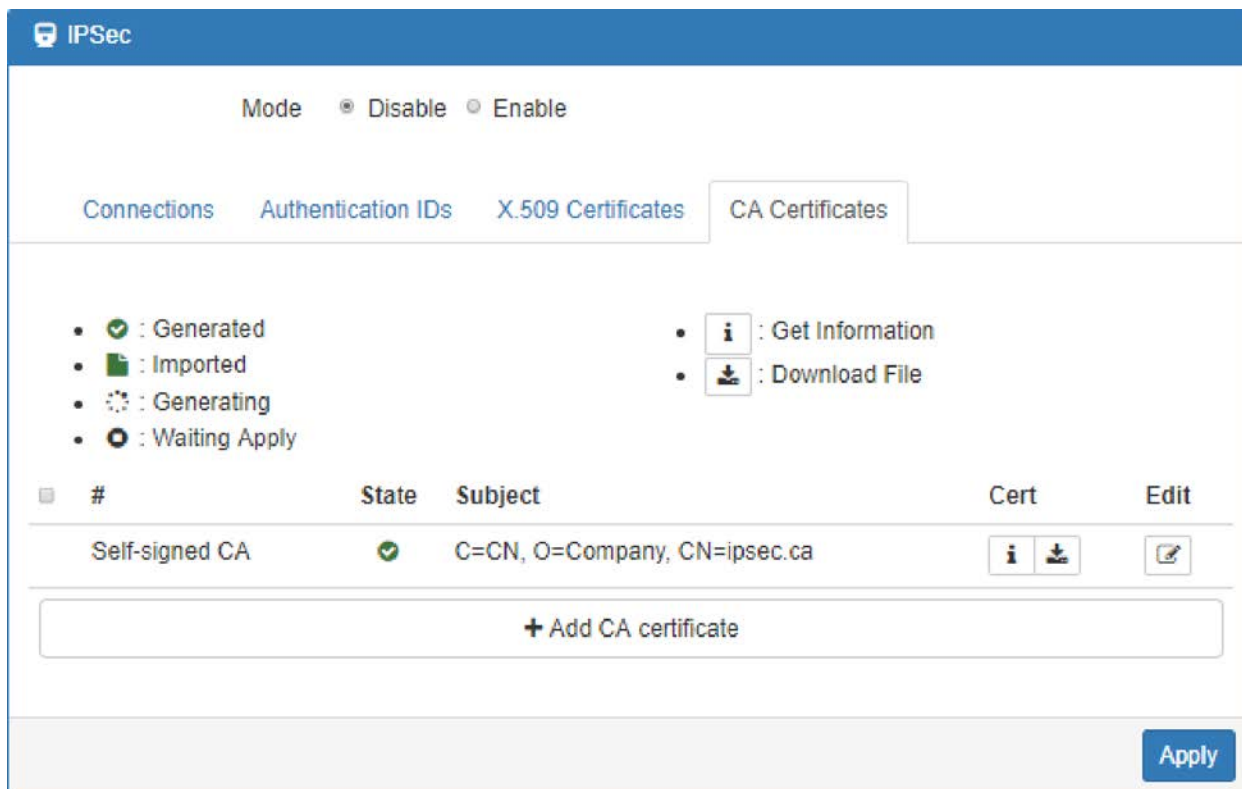
#	State	Subject	Cert	Key	Edit
1		C=CN, O=Company, CN=local.ipsec			
2		C=CN, O=Company, CN=remote.ipsec			

## 11.2.4 IPsec > CA Certificates

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

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

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



IPSec

Mode  Disable  Enable

Connections Authentication IDs X.509 Certificates CA Certificates

- : Generated
- : Imported
- : Generating
- : Waiting Apply
- : Get Information
- : Download File

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

[+ Add CA certificate](#)

[Apply](#)

### Certificate Generation

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

To generate the self-signed CA certificate:

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

To generate the X.509 certificate:

1. Make sure the self-signed CA certificate generated.
2. Navigate to [X.509 Certificates](#) tab.
3. Add the new X.509 certificate by [+ Add X.509](#) button. (If it's not existed.)

4. Click the Edit button to navigate the **Certificate Setting** page.
5. Fill up the information of the X.509 certificate.
6. Click the **Generate Certificate** button and **Save**.
7. Click the **Apply** button to apply the changes.

### Certificate Setting

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

Self-signed CA Certificate

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

### Certificate Importing

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

To import the CA certificate:

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

To import the X.509 certificate:

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

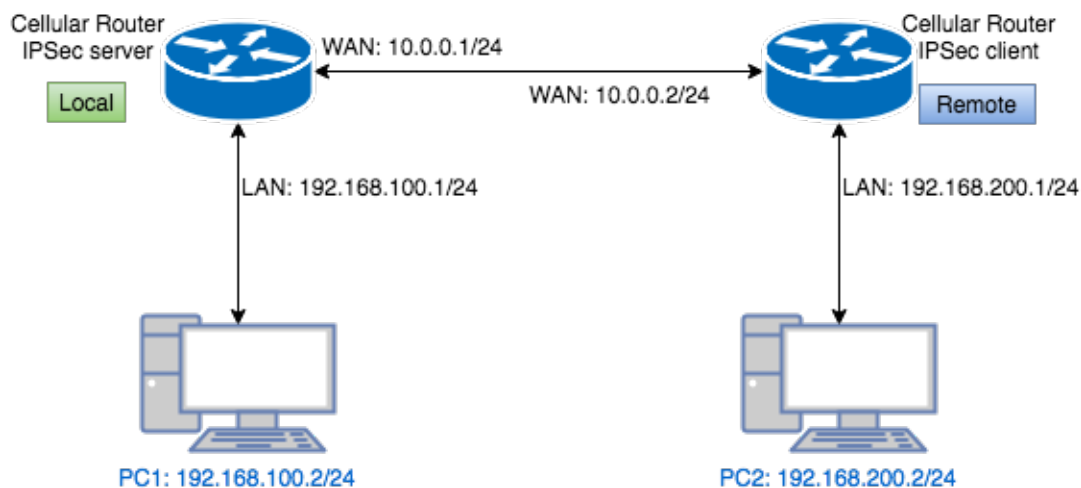
### Download the certificate

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

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

### 11.2.5 IPsec > Net-to-Net Configuration

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



- **Pre-shared Key authentication**

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

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

## 6. Add IPsec connection

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

## 7. Apply the changes

### IPSec

Mode  Disable  Enable

Type  Policy-based  Route-based

Connections Authentication IDs X.509 Certificates CA Certificates

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

[+ Add Authentication ID](#)

[Apply](#)



## Connection #1 Phase 1

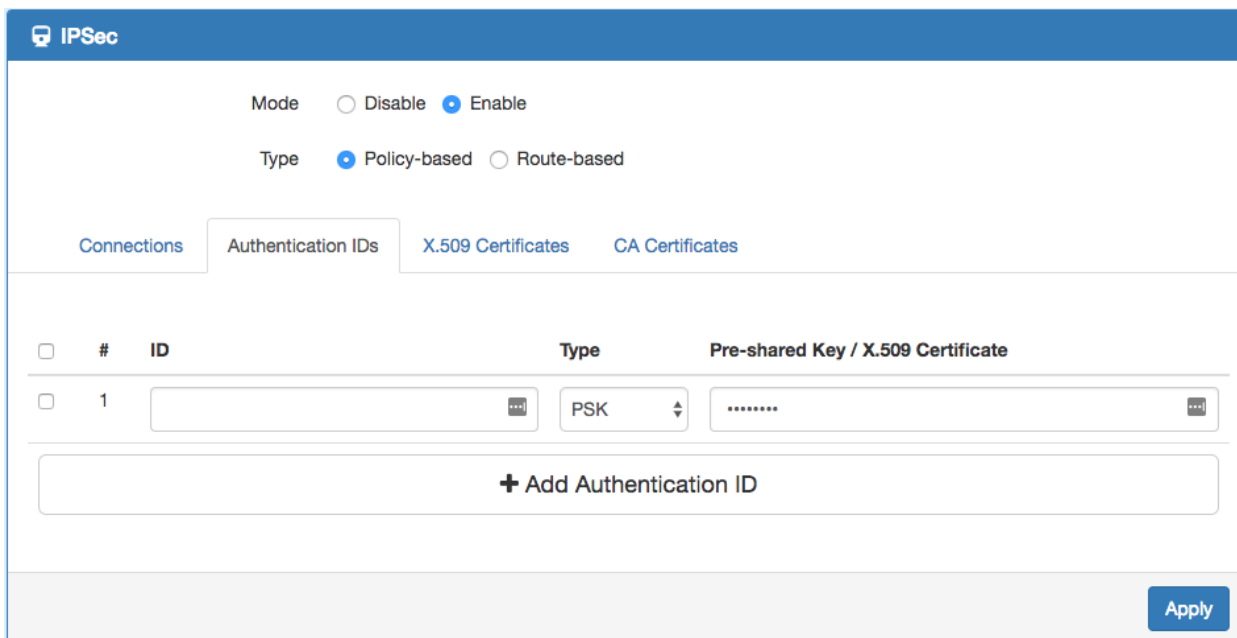
Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Name	<input type="text"/>
Protocol	IKEv1
Aggressive mode	Disable
Auth Type	PSK
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	3 hours
Local Host	<input type="text"/>
Local ID	<empty> (allow any)
Remote Host	<input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

## Connection #1 Phase 2

Protocol	ESP
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	2 hours
Local Subnet	192.168.100.0/24
Remote Subnet	192.168.200.0/24
Service	Any

## Configure Net-to-Net VPN Client

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



The screenshot shows the IPsec configuration interface. At the top, there is a blue header with the IPsec icon and the text "IPSec". Below the header, there are two radio buttons for "Mode": "Disable" (unselected) and "Enable" (selected). There are also two radio buttons for "Type": "Policy-based" (selected) and "Route-based" (unselected). Below these are four tabs: "Connections", "Authentication IDs" (selected), "X.509 Certificates", and "CA Certificates". The main area contains a table with columns: "#", "ID", "Type", and "Pre-shared Key / X.509 Certificate". There is one row with "# 1", an empty "ID" field, "PSK" in the "Type" dropdown, and a masked "Pre-shared Key" field. Below the table is a button labeled "+ Add Authentication ID". At the bottom right, there is a blue "Apply" button.

### Connection #1 Phase 1

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

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

### Connection #1 Phase 2

Protocol	ESP
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	2 hours
Local Subnet	192.168.200.0/24
Remote Subnet	192.168.100.0/24
Service	Any

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

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

### • Server

Connections

[Authentication IDs](#)
[X.509 Certificates](#)
[CA Certificates](#)

- ✔ : IPsec SA active and link up
- ! : Only IPsec SA active
- ⋮ : Connecting
- ✘ : IPsec SA inactive
- ● : Disabled

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

	#	Name	State	IKE information	Tunnel information
<input type="checkbox"/>	1	psk	✔	IKEv1 : 10.0.0.1 [10.0.0.1] ... 10.0.0.2 [10.0.0.2]	<span style="background-color: #007bff; color: white; padding: 2px 5px;">✎ Phase 1</span> 192.168.100.0/24 ... 192.168.200.0/24 <span style="background-color: #28a745; color: white; padding: 2px 5px;">✎ Phase 2</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">⋮</span>

+ Add Connection

### • Client

Connections

[Authentication IDs](#)
[X.509 Certificates](#)
[CA Certificates](#)

- ✔ : IPsec SA active and link up
- ! : Only IPsec SA active
- ⋮ : Connecting
- ✘ : IPsec SA inactive
- ● : Disabled

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

	#	Name	State	IKE information	Tunnel information
<input type="checkbox"/>	1	psk	✔	IKEv1 : 10.0.0.2 [10.0.0.2] ... 10.0.0.1 [10.0.0.1]	<span style="background-color: #007bff; color: white; padding: 2px 5px;">✎ Phase 1</span> 192.168.200.0/24 ... 192.168.100.0/24 <span style="background-color: #28a745; color: white; padding: 2px 5px;">✎ Phase 2</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">⋮</span>

+ Add Connection

### • RSA authentication - Server

#### Prepare the self-signed CA certificate

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

5. Waiting for the **State** of self-signed CA become generated
6. Refresh the page

Self-signed CA Certificate

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

### Prepare the X.509 certificates

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

## 7. Waiting for the **State** of X.509 Certificate become generated

### X.509 Certificate #1

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

### X.509 Certificate #2

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

**IPSec**

Mode  Disable  Enable

Type  Policy-based  Route-based

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

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

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

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

+ Add X.509

**Apply**

**IPSec**

Mode  Disable  Enable

Type  Policy-based  Route-based

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

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

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

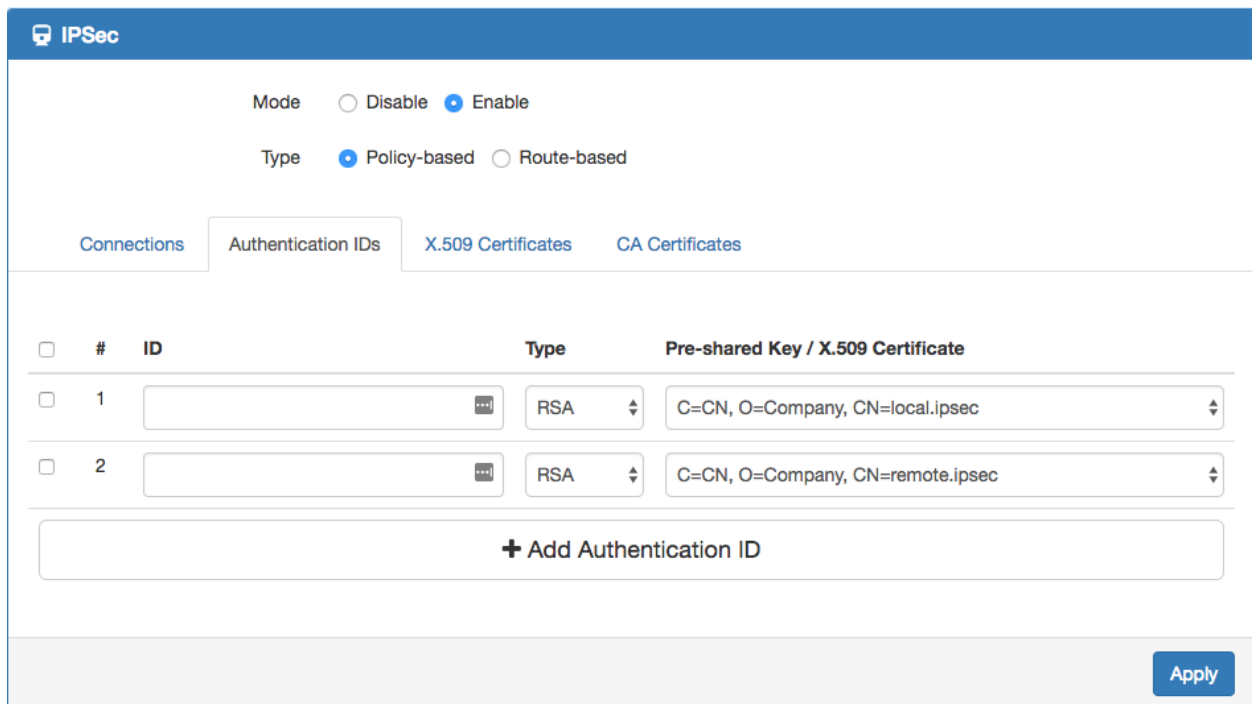
<input type="checkbox"/>	#	State	Subject	Cert	Key	Edit
<input type="checkbox"/>	1		C=CN, O=Company, CN=local.ipsec			
<input type="checkbox"/>	2		C=CN, O=Company, CN=remote.ipsec			

+ Add X.509

**Apply**

### Prepare the authentication IDs

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



### Setup the connection on VPN server

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



#### 4. Apply the changes

Connection #1 Phase 1

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

Connection #1 Phase 2

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

• **RSA authentication – Client**

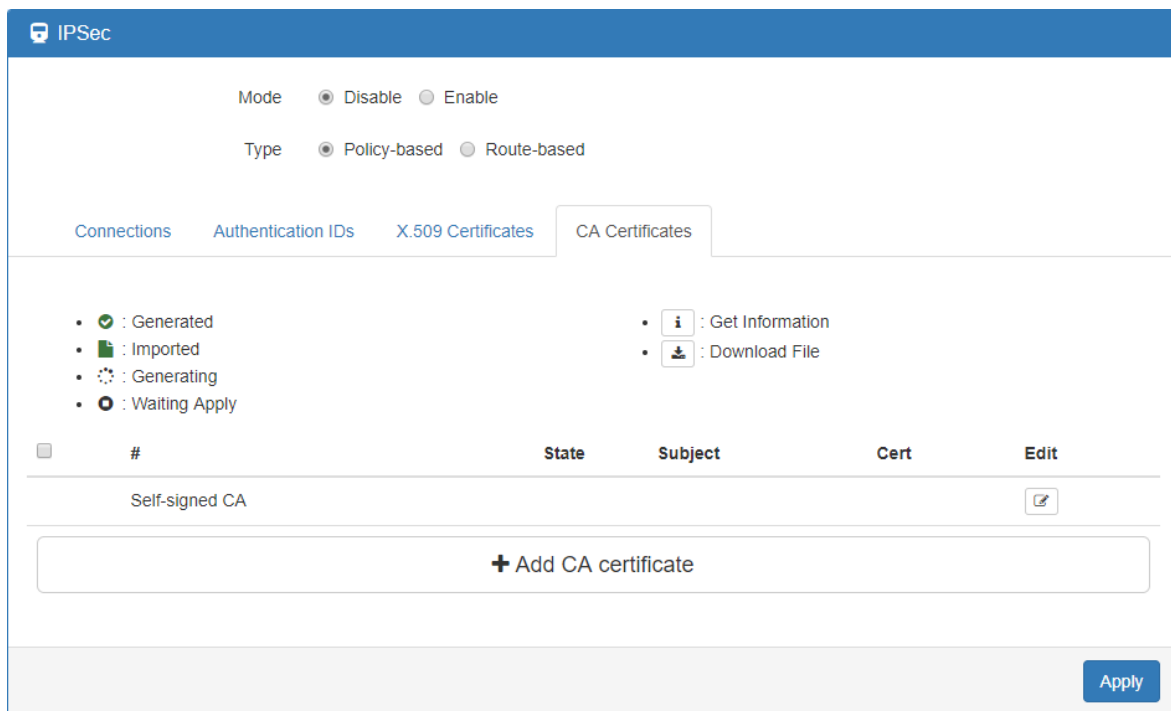
**Prerequisite for VPN Client with RSA authentication**

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

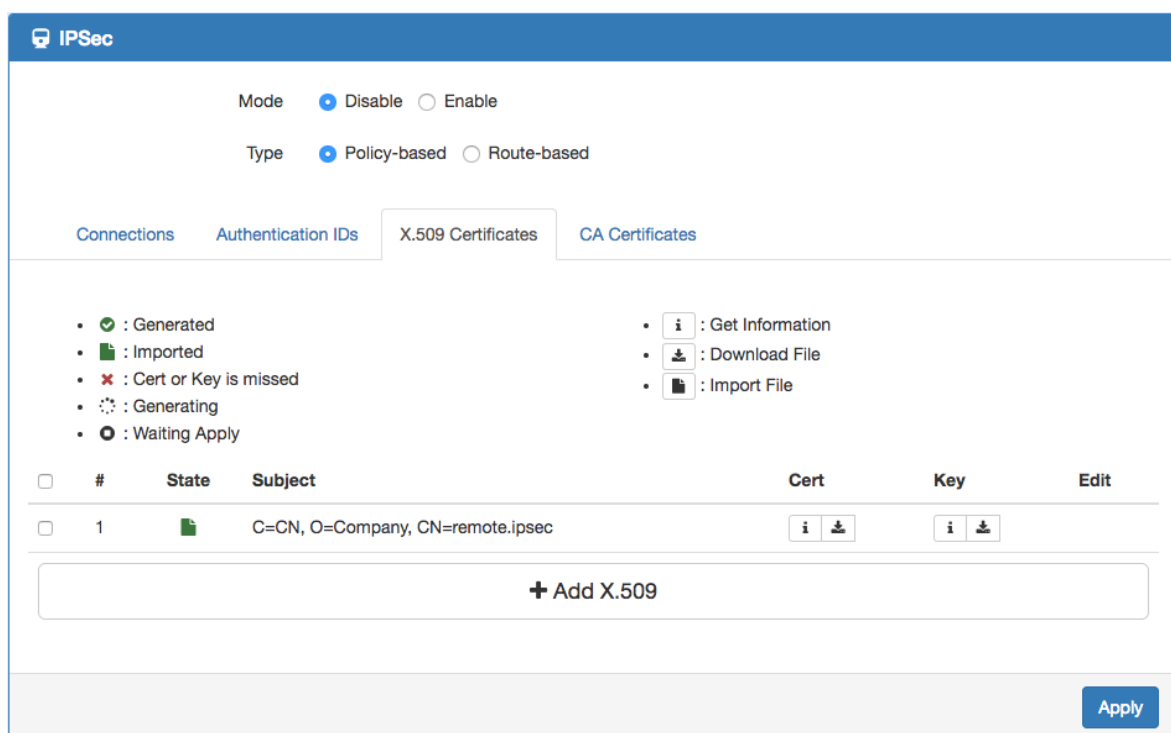
These files could be downloaded from VPN server. The detail could reference “ How to download the certificate section ” of user manual.

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

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



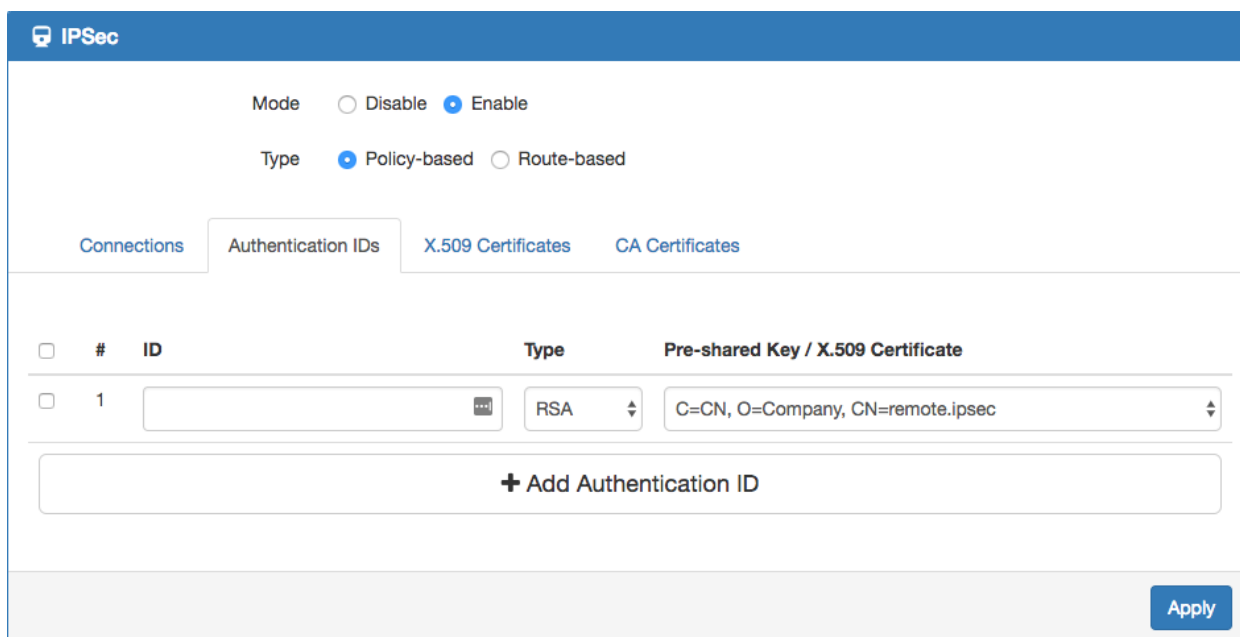
The screenshot shows the IPsec configuration interface with the 'CA Certificates' tab selected. The 'Mode' is set to 'Disable' and 'Type' is 'Policy-based'. A legend indicates: Generated (green check), Imported (green document), Generating (dotted circle), Waiting Apply (black circle), Get Information (i icon), and Download File (download icon). A table lists one entry: 'Self-signed CA' with an 'Edit' icon. Below the table is a '+ Add CA certificate' button and an 'Apply' button at the bottom right.



The screenshot shows the IPsec configuration interface with the 'X.509 Certificates' tab selected. The 'Mode' is set to 'Disable' and 'Type' is 'Policy-based'. A legend indicates: Generated (green check), Imported (green document), Cert or Key is missed (red x), Generating (dotted circle), Waiting Apply (black circle), Get Information (i icon), Download File (download icon), and Import File (import icon). A table lists one entry: '1' with state 'Imported' and subject 'C=CN, O=Company, CN=remote.ipsec', with 'Get Information' and 'Download File' icons for both Cert and Key columns. Below the table is a '+ Add X.509' button and an 'Apply' button at the bottom right.

## Setup the connection on VPN client

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



The screenshot shows the IPsec configuration interface. At the top, there are radio buttons for Mode (Disable, Enable) and Type (Policy-based, Route-based). Below this are four tabs: Connections, Authentication IDs (selected), X.509 Certificates, and CA Certificates. A table lists authentication IDs with columns for #, ID, Type, and Pre-shared Key / X.509 Certificate. The first row shows ID 1 with a blank ID field, Type RSA, and Pre-shared Key / X.509 Certificate C=CN, O=Company, CN=remote.ipsec. Below the table is a button to add a new authentication ID. An Apply button is located at the bottom right.

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

### Connection #1 Phase 1

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

### Connection #1 Phase 2

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

• IPsec Net-to-Net with RSA authentication result

• Server

Connections   Authentication IDs   X.509 Certificates   CA Certificates

- ✔ : IPsec SA active and link up
- ⚠ : Only IPsec SA active
- 🔄 : Connecting
- ✖ : IPsec SA inactive
- ⏻ : Disabled

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

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

+ Add Connection

• Client

Connections   Authentication IDs   X.509 Certificates   CA Certificates

- ✔ : IPsec SA active and link up
- ⚠ : Only IPsec SA active
- 🔄 : Connecting
- ✖ : IPsec SA inactive
- ⏻ : Disabled

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

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

+ Add Connection

## 11.3 VPN > GRE

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

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



- GRE Tunnel interface comes up as soon as it is configured.
- Local endpoint does not bring the interface down if the remote endpoint is unreachable.
- No way to determine problems in the intervening network.
- Keepalives are used to solve this issue.

The GRE Tunnel Keepalive feature provides the capability of configuring keepalive packets to be sent over IP-encapsulated GRE tunnels. You can specify the rate at which keepalives will be sent and the number of times that a device will continue to send keepalive packets without a response before the interface becomes inactive. GRE keepalive packets may be sent from both sides of a tunnel or from just one side.

There are 2 entry for user to configure, please press Edit  button.

**GRE**

Mode  Off  On

#	Mode	Local Address	Remote Address	Tunnel Device Address	Interface Status	Edit
1	off				--	
2	off				--	

[Apply](#)

While clicking Edit button, it shows Off or On mode. Please select On to display setting items.

**Edit GRE Entry #1**

Mode  Off  On

[Save](#)

The GRE Mode is On.

Edit GRE Entry #1

Mode  Off  On

Device WAN Ethernet ▼ bind the tunnel to the device

Local Address

Remote Address

Tunnel Device Address

Tunnel Device Address Prefix 24

Use Tunnel Key  Off  On

Keepalive Period 10 (0 ~ 32767); 0: keepalive not set

Keepalive Retries 3 (1 ~ 255)

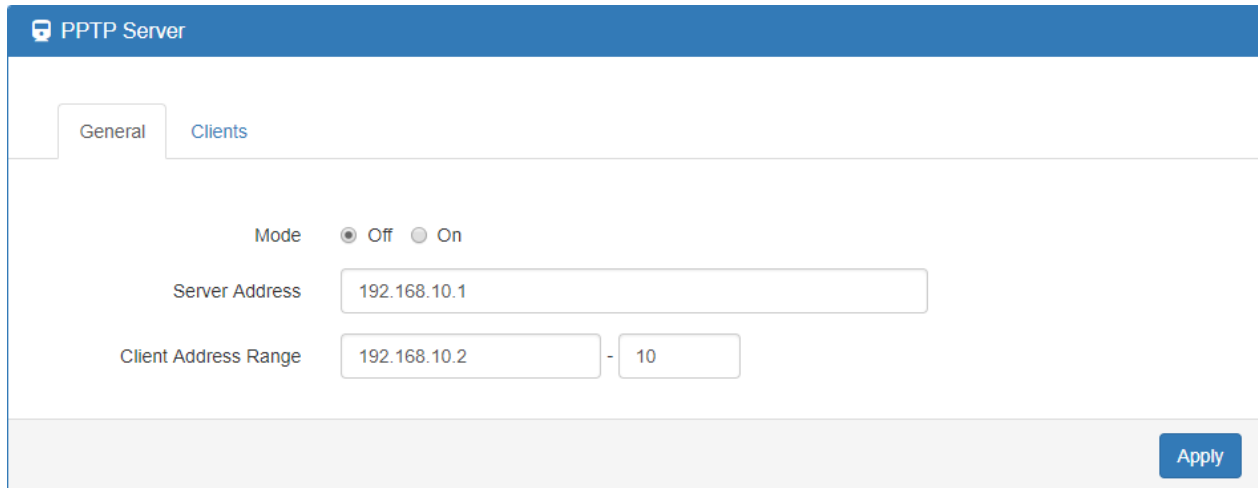
Save

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.
<b>Use Tunnel Key</b>	Whether to use the key for identifying an individual traffic flow within a tunnel.
<b>Tunnel Key Number</b>	The number of the tunnel key; default is '1234'.
<b>Keepalive Period</b>	(0 ~ 32767); 0: keepalive not set.
<b>Keepalive Retries</b>	1 ~ 255.

## 11.4 VPN > PPTP Server

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

### (1) General Configuration



The screenshot shows the 'PPTP Server' configuration page with the 'General' tab selected. It includes a 'Mode' section with radio buttons for 'Off' and 'On'. Below that is a 'Server Address' text input field containing '192.168.10.1'. The 'Client Address Range' is configured with a text input '192.168.10.2' followed by a range indicator '-' and a separate text input '10'. An 'Apply' button is located at the bottom right.

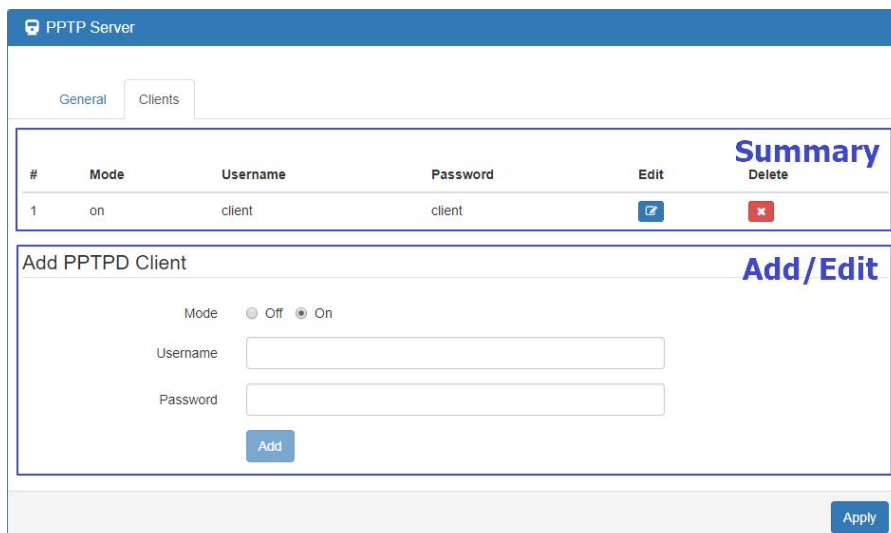
VPN > PPTP Server > General	
Item	Description
<b>Mode</b>	Select from Off or On to enable PPTP Server.
<b>Server Address</b>	IP addresses to be used at the local end of the tunneled PPP links between the server and the client.
<b>Client Address Range</b>	A list of IP addresses to assign to remote PPTP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



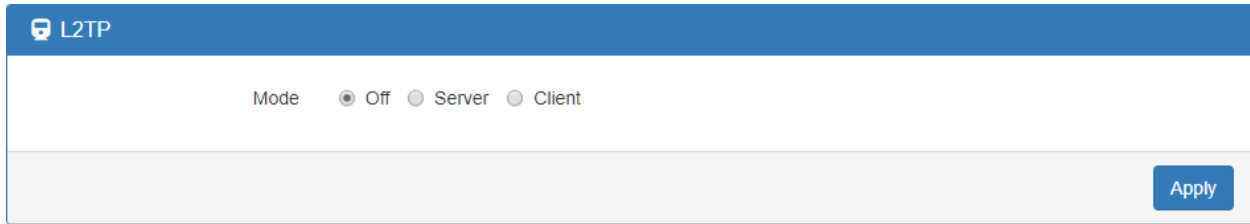
The screenshot shows the 'PPTP Server' configuration page with the 'Clients' tab selected. It features a 'Summary' table with columns for '#', 'Mode', 'Username', 'Password', 'Edit', and 'Delete'. The first row shows a client with mode 'on', username 'client', and password 'client'. Below the table is an 'Add PPTPD Client' section with radio buttons for 'Off' and 'On', and text input fields for 'Username' and 'Password'. An 'Add' button is at the bottom of this section, and an 'Apply' button is at the bottom right of the entire page.



## 11.5 VPN > L2TP

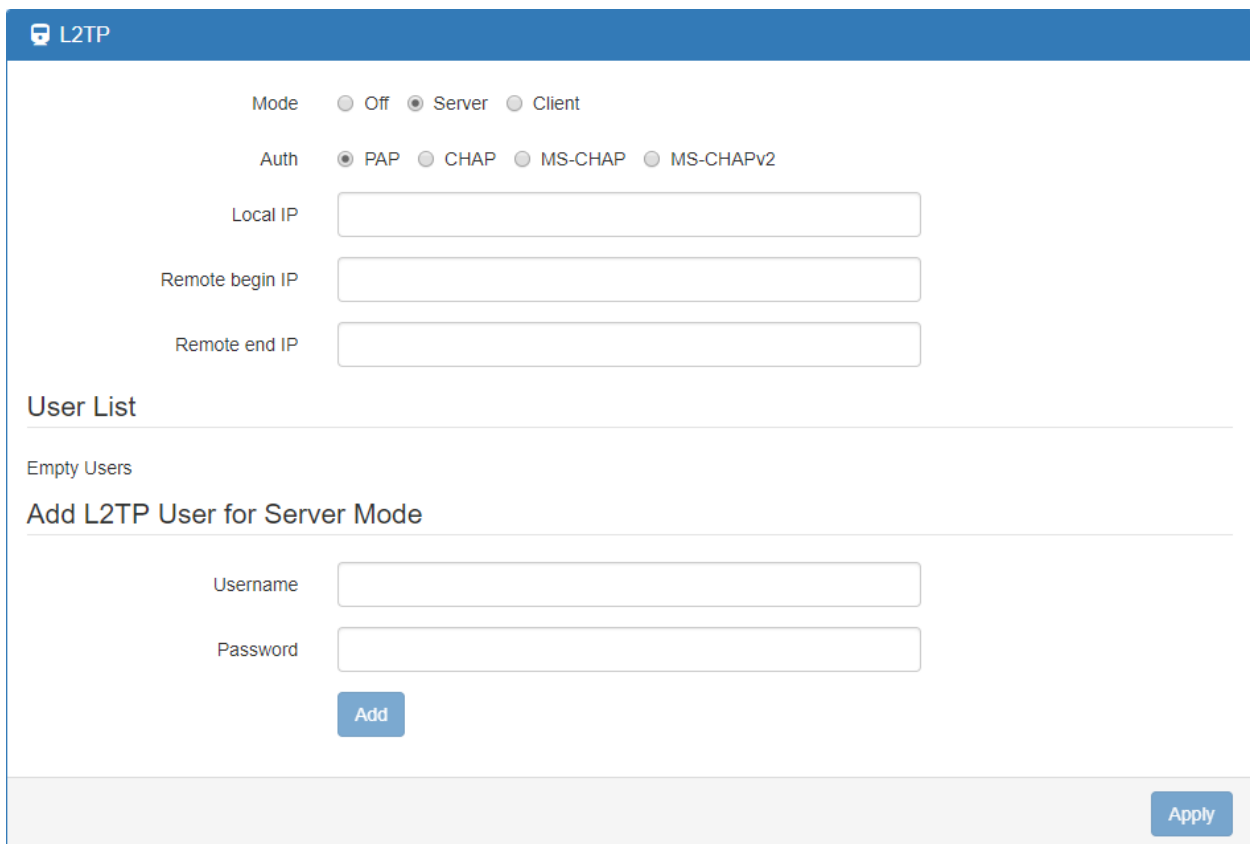
This section allows you to set up L2TP and provides three modes for configuration, including Off, Server, and Client Mode.

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



(2) **Server Mode:**

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



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

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

### L2TP

Mode  Off  Server  Client



Auth  PAP  CHAP  MS-CHAP  MS-CHAPv2

Local IP

Remote begin IP

Remote end IP

#### User List

#	Username	Edit	Delete
1	test		

#### Add L2TP User for Server Mode

Username

Password

**Add**

**Apply**

### (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.

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

L2TP

Mode  Off  Server  Client

### Connection List

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

### Add L2TP Connection for Client Mode

Mode  Off  On

Server

Auth  PAP  CHAP  MS-CHAP  MS-CHAPv2

Username

Password


NAT  Off  On

Default Route  Off  On

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


## 12 Configuration > Firewall

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

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

### 12.1 Firewall > Basic Rules

This section allows you to set the Basic Rules configuration.

 Basic Rules

WAN Ping Blocking  IPv4  IPv6















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

## 12.2 Firewall > Port Forwarding

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

**Port Forwarding**

Mode  Disable  Enable

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

Apply

**Edit Port Forwarding Entry #1**

Mode  Disable  Enable

Description

Protocol  TCP  UDP

Source Port Begin

Source Port End

Destination IP

Destination Port Begin

Destination Port End

Save

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

## 12.3 Firewall > DMZ

This section allows you to set the DMZ configuration.


🛡️ DMZ

Mode  Disable  Enable

Host IP Address

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

## 12.4 Firewall > IP Filter

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

















**IP Filter**

Warning: All existing connections will be dropped after apply

Mode  Disable  Enable

List  Black  White

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

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



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

IP Filter

Warning: All existing connections will be dropped after apply

Mode  Disable  Enable

List  Black  White

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

Management IP Address

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

Service Ports

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

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

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


### Management IP Address:

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

### Service Ports:

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

## Edit Black/White List

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

Edit IP Filter Black List Entry #1

**Black List Setting**

Mode  Disable  Enable

Protocol  All  ICMP  TCP  UDP

Source IP   
Example:

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

Source Port   
Example:

- 1234
- 1234:5678:

Destination IP

Destination Port

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.

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

**Note:** Setting up a range of IP, please use – hyphen symbol to mark your ranged IP.

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

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

## 12.5 Firewall > MAC Filter

















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

**MAC Filter**

Warning: All existing connections will be dropped after apply

Mode  Disable  Enable

List  Black  White

#	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
<b>Mode</b>	Select from Disable or Enable. The default is Disable.
<b>MAC Address</b>	Fill in your MAC address.

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

















## 12.6 Firewall > URL Filter

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

**URL Filter**

Warning: All existing connections will be dropped after apply

Mode  Disable  Enable

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

Apply

**Edit URL Filter Black List Entry #1**

Mode  Disable  Enable

Filter  Key  Full

Key/Full

Hint **About the 'Full' filter:**

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

Save

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


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

## 12.7 Firewall > NAT

This section allows you to set NAT configuration.

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

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

 NAT

Mode  Disable  Enable

## 12.8 Firewall > IPS

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

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

🛡️
IPS(Intrusion Prevention System)

Mode     Off     On

---

Per IP Address

Total allow incoming connection number

Max incoming connection retry number     during  seconds

Apply

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

## 13 Configuration > Service

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

Service <span style="float: right;">+</span>
SNMP
TR069
Dynamic DNS
VRRP
MQTT
UPnP
SMTP
IP Alias
QoS

### 13.1 Service > SNMP

This section allows you to set the SNMP configuration.

#### 13.1.1 Community

+
SNMP

Mode  Disable  Enable

Community
SNMP v3 User Configuration
SNMP trap configuration

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

Apply

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

### 13.1.2 SNMP v3 User Configuration

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

+
SNMP

Mode  Disable  Enable

Community
SNMP v3 User Configuration
SNMP trap configuration

#	Mode	Name	Access
1	Disable ▼	<input type="text"/>	Read-Only ▼
2	Disable ▼	<input type="text"/>	Read-Only ▼
3	Disable ▼	<input type="text"/>	Read-Only ▼

Authentication

#	Mode	Auth Password	Auth Protocol	Privacy Password	Privacy Protocol
1	Auth ▼	<input type="text"/>	MD5 ▼	<input type="text"/>	DES ▼
2	Auth ▼	<input type="text"/>	MD5 ▼	<input type="text"/>	DES ▼
3	Auth ▼	<input type="text"/>	MD5 ▼	<input type="text"/>	DES ▼

Apply

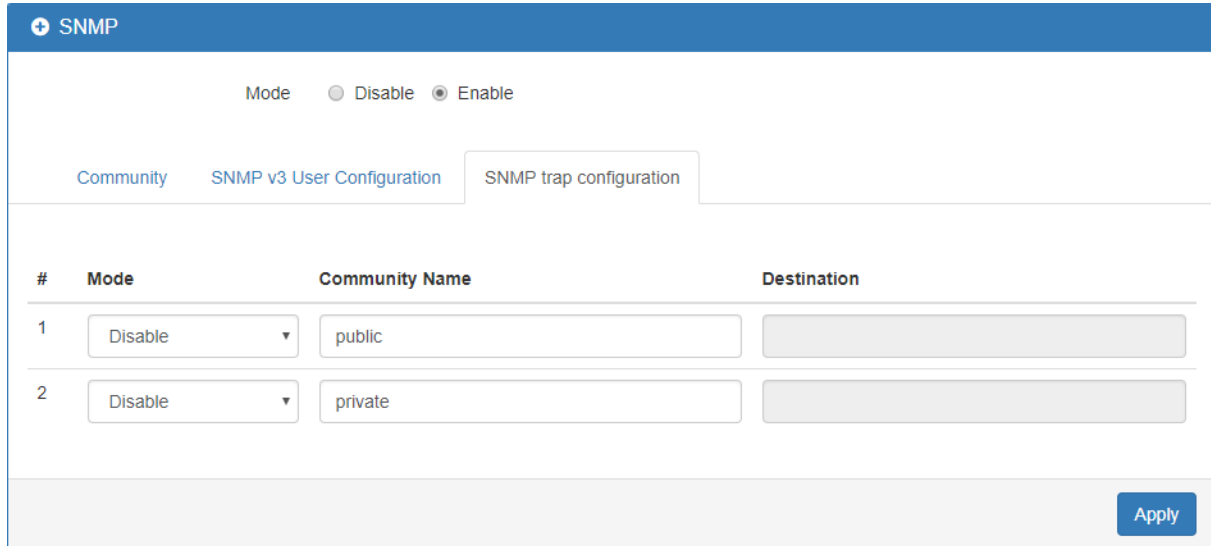
Service > SNMP > SNMP v3 User configuration	
Item	Description
<b>Mode</b>	Select from Disable or Enable to configure SNMP. The default is Disable.
<b>Name</b>	Fill in your name.
<b>Auth Mode</b>	Select from Authentication or Privacy.
<b>Authentication Password</b>	Fill in your authentication password.
<b>Authentication Protocol</b>	Select from MD5 or SHA.
<b>Privacy Password</b>	Fill in your privacy password.



<b>Privacy Protocol</b>	Select from DES or AES.
<b>Access</b>	Select from Read-Only or Read-Write.

### 13.1.3 SNMP trap configuration

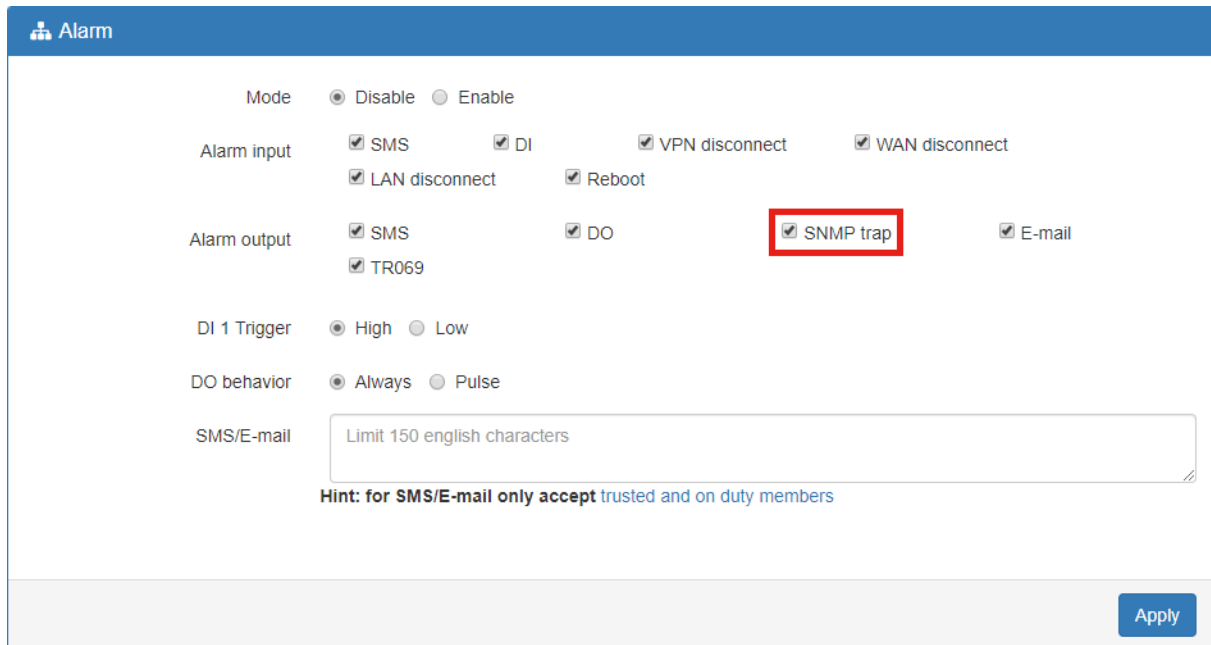
This section allows you to set up the SNMP trap configuration when you select the **SNMP trap** function from Alarm output of system for your router. With SNMP trap setting, you can know the status of remote device.



The screenshot shows the 'SNMP' configuration page. At the top, there is a 'Mode' section with radio buttons for 'Disable' and 'Enable', where 'Enable' is selected. Below this are three tabs: 'Community', 'SNMP v3 User Configuration', and 'SNMP trap configuration', with the third tab being active. A table below lists two entries:

#	Mode	Community Name	Destination
1	Disable	public	
2	Disable	private	

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



The screenshot shows the 'Alarm' configuration page. At the top, there is a 'Mode' section with radio buttons for 'Disable' and 'Enable', where 'Disable' is selected. Below this are several sections for configuring alarm inputs and outputs:

- Alarm input:** Includes checkboxes for SMS, DI, VPN disconnect, WAN disconnect, LAN disconnect, and Reboot.
- Alarm output:** Includes checkboxes for SMS, DO, **SNMP trap** (highlighted with a red box), and E-mail.
- DI 1 Trigger:** Includes radio buttons for High and Low.
- DO behavior:** Includes radio buttons for Always and Pulse.
- SMS/E-mail:** Includes a text input field with the placeholder 'Limit 150 english characters'.

A hint at the bottom states: 'Hint: for SMS/E-mail only accept trusted and on duty members'. An 'Apply' button is located at the bottom right.

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

### 13.2 Service > TR069

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

+ TR069

Mode  Disable  Enable

ACS URL

ACS Username

ACS Password

Periodic Inform  Disable  Enable

Periodic Inform Interval(Sec)

Connection Request Username

Connection Request Password

Connection Request Port

Apply

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

## 13.3 Service > Dynamic DNS

This section allows you to set up Dynamic DNS.

+ Dynamic DNS

Mode  Disable  Enable

Service Provider

Host Name

Token ID

Update Period Time (Sec)

IP Address Selection  Internet IP  WAN IP

+ Dynamic DNS

Mode  Disable  Enable

Service Provider

Host Name

Token ID

Update Period Time (Sec)

IP Address Selection  Internet IP  WAN IP

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

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

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

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

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

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

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

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

## 13.4 Service > VRRP

This section allows you to configure VRRP.

+ VRRP

Mode  Disable  Enable

Group ID

Priority

Virtual IP

Apply

Service > VRRP	
Item	Description
<b>Mode</b>	Select from Disable or Enable. The default is Disable.
<b>Group ID</b>	Specify which VRRP group of this router belong to (1-255). The default is 1.
<b>Priority</b>	Enter the priority value from 1 to 254. The larger value has higher priority. The default is 100.
<b>Virtual IP</b>	<ul style="list-style-type: none"> <li>Each router in the same VRRP group must have the same virtual IP address. The default is 0.0.0.0.</li> <li>This virtual IP address must belong to the same address range as the real IP address of the interface.</li> </ul>

## 13.5 Service > MQTT

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

MQTT

Mode  Disable  Enable

Port

### Manage Users

Username	Password	Delete
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

### ACLs

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

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

Take for example, the interface is shown as below.

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

Mode  Disable  EnablePort 

## Manage Users

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

Username Password 

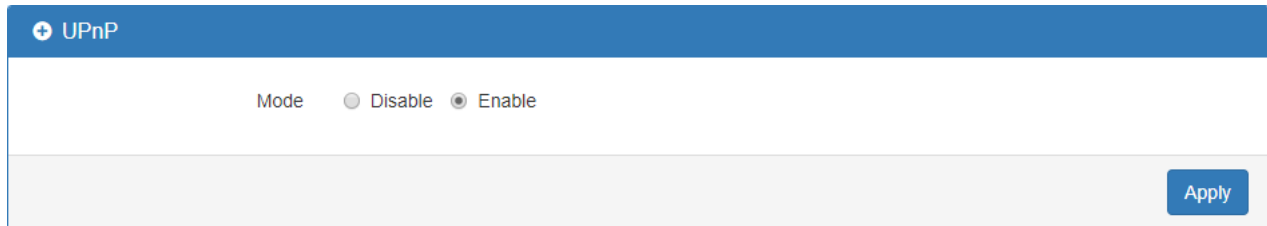
## ACLs

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

User Topic  Subscribe Publish

## 13.6 Service > UPnP

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



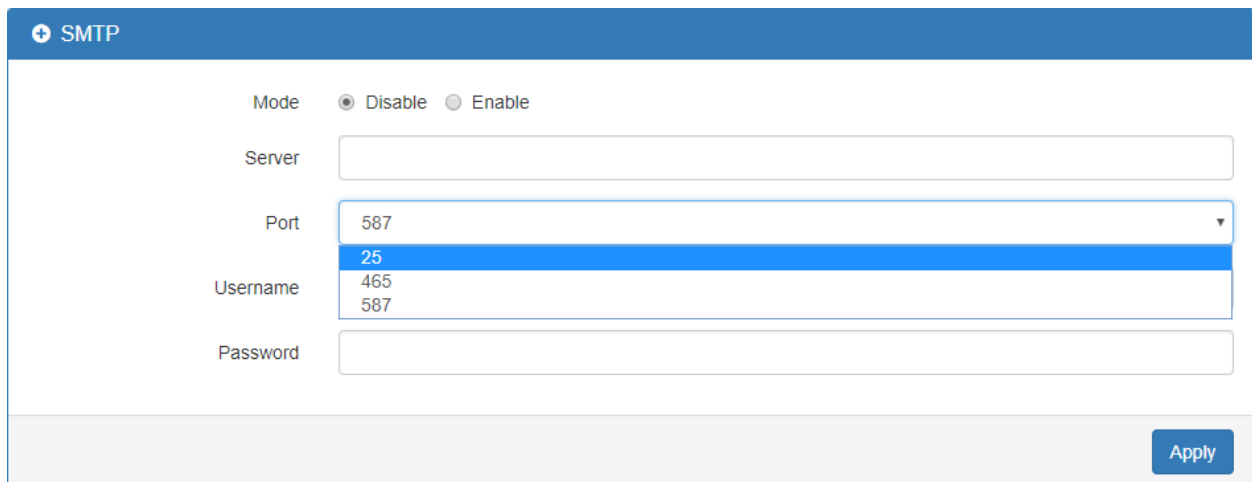
**Note:**

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

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

## 13.7 Service > SMTP

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



Service > SMTP	
Item	Description
<b>Mode</b>	Select from Disable or Enable. The default is Disable.
<b>Server</b>	The email will be sent through the server.
<b>Port</b>	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>
<b>Username / Password</b>	Fill in your username and password as the same your server.



## 13.8 Service > IP Alias

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

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

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

+ IP Alias

Mode  Off  On

Entries

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

Add IP Alias Entry

Mode  Off  On

Interface

Addr

Mask

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

## 13.9 QoS

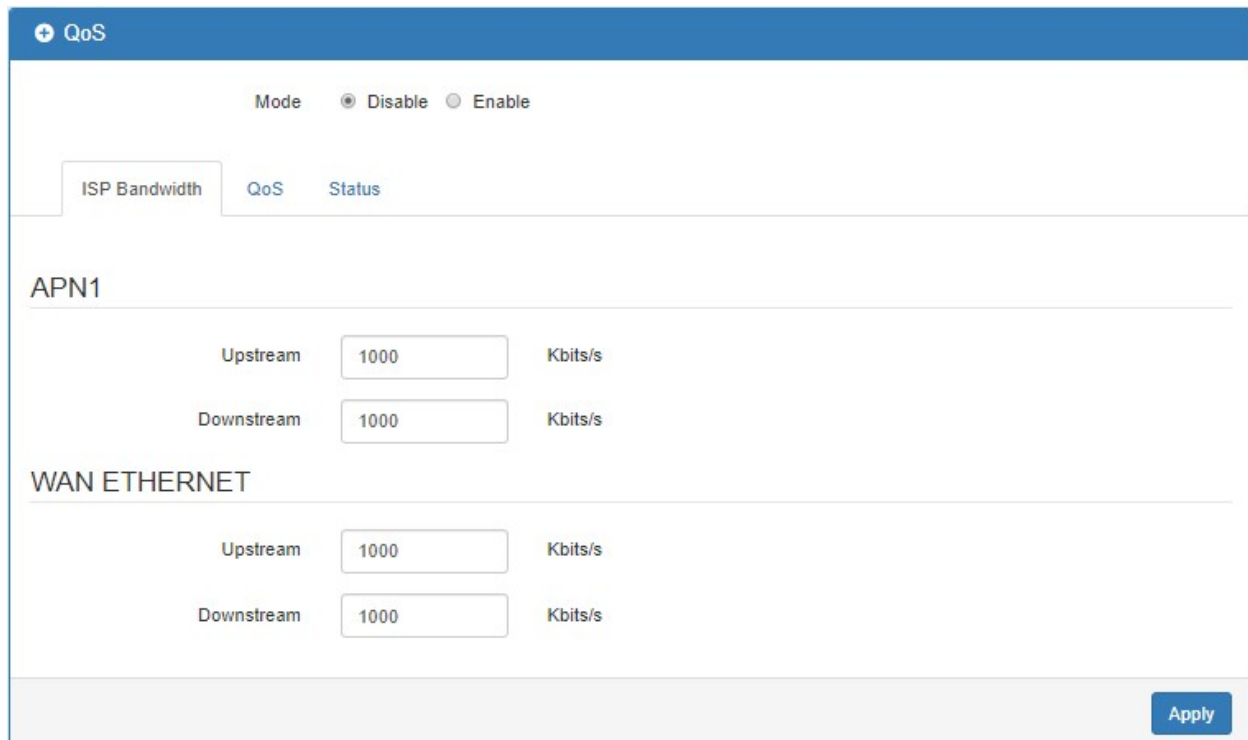
QoS (Quality of Service) refers to a network ability to achieve maximum bandwidth and allow minimum bandwidth. It guarantees the minimum and limit the maximum bandwidth for certain class of traffic. The QoS configuration has three parts, including ISP bandwidth, QoS, and Status.

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

### 13.9.1 QoS > ISP Bandwidth

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

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



The screenshot displays the QoS configuration page. At the top, there is a 'Mode' section with radio buttons for 'Disable' (selected) and 'Enable'. Below this are three tabs: 'ISP Bandwidth' (active), 'QoS', and 'Status'. The main content area is divided into two sections: 'APN1' and 'WAN ETHERNET'. Each section has two rows of input fields: 'Upstream' and 'Downstream', both set to '1000' Kbits/s. An 'Apply' button is located at the bottom right of the configuration area.

### 13.9.2 QoS > QoS

You can select QoS tab to show an overall view for QoS configuration.

At right side of window, there are three buttons.

- Edit button: It allows you to edit QoS Entry and configure QoS settings.
- Up/Down arrow button: It allows you to adjust priority of the QoS entry. The first QoS entry is the highest priority.





























































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

Mode  Disable  Enable

ISP Bandwidth

QoS

Status

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

Apply

+ QoS

Mode  Disable  Enable

---

### Edit QoS Entry #1

Mode  Disable  Enable

Name

Interface  APN1  WAN ETHERNET

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

IPv4v6 Address

Example: (empty)

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

Protocol  All  TCP  UDP

Port Begin

Port End

VLAN follow vid of

Class of Service

Min Rate  Kbits/s

Max Rate  Kbits/s

Bandwidth divided for each IP Address

Service > IP Alias	
Item	Description
<b>Mode</b>	Select from Disable or Enable QoS.
<b>Name</b>	The setting can be edited or deleted the existed entries.
<b>Interface</b>	The interface of QoS entry is either WAN Ethernet or LTE and both options.
<b>Direction</b>	<ul style="list-style-type: none"> <li>When selecting Upstream for LAN to WAN traffic, the Port Begin/End is for public server.</li> <li>When selecting Downstream for WAN to LAN traffic, the Port Begin/End is for public server.</li> <li>When selecting Upstream (LAN server) for WAN to LAN traffic, the Port Begin/End is for LAN server.</li> </ul>

	<ul style="list-style-type: none"> <li>• When selecting Downstream (LAN server) for LAN to WAN traffic, the Port Begin/End is for LAN server.</li> <li>• Downstream (LAN server) is for LAN to WAN traffic, and the Port Begin/End is for LAN server.</li> </ul>
<b>IPv4v6 Address</b>	<p>Choose four types to set address format, including All, Single, Subnet, and Range.</p> <ul style="list-style-type: none"> <li>• All is for none.</li> <li>• Single is for single IP address.</li> <li>• Subnet is for IP address with subnet mask bit.</li> <li>• Range is for the specified range between two IP addresses.</li> </ul> <p>Hint: When [RANGE] is selected, compare the difference from left to right octet and find out different octet for setting the specified range of IP address. All other parts after different octet would be ignored.</p>
<b>Protocol</b>	<ul style="list-style-type: none"> <li>• All is for none.</li> <li>• UDP is for User Datagram Protocol.</li> <li>• TCP is for Transmission Control Protocol.</li> </ul>
<b>Port Begin/Port End</b>	the TCP/UDP service port
<b>VLAN follow vid of</b>	<ul style="list-style-type: none"> <li>• NONE.</li> <li>• NET1 - NET8.</li> </ul> <p>Note: For NET1 to NET8, make sure the related subnet is enabled at VLAN-&gt;Tag Base. The VLAN ID, vid, will be the VID field of the related Subnet at VLAN-&gt;Tag Base.</p>
<b>COS (Class of Service or 802.1q)</b>	NONE or 0~7. It is class of service for VLAN.
<b>Min Rate/Max Rate</b>	The unit is kilobits per second. Min Rate guarantee the minimum bandwidth and Max Rate is the limit bandwidth.
<b>Bandwidth divided for each IP Address</b>	When this feature is selected, the bandwidth assigned by Min Rate/Max Rate will be divided by the number of IP addresses. The available IP type is Subnet and Range. User needs to calculate the Min Rate and Max Rate for those IP addresses. The subnet mask bit in IP Type Subnet is octet boundary and the number of IP addresses is one octet too, 256, from subnet mask bit to subnet mask plus eight bit.

**Note:** To guarantee minimum bandwidth for assigning each IP, you should select **Bandwidth divided for each IP Address**.

**Refresher Setting** select the showed content of bandwidth usage by following items:

- Refresh rate: how long the browser will update the showed content once.
- Direct: show Upstream or Downstream.
- Show detail bandwidth for each IP address: show the group IP bandwidth usage.
- Apply Refresh Setting button: press this button to take above new setting effect.

Data part is the content of bandwidth usage.

**QoS**

Mode  Disable  Enable

ISP Bandwidth QoS **Status**

---

### Refresher Setting

Update every  secs

Interface  APN1  WAN ETHERNET

Direction  Upstream  Downstream

Show detail of bandwidth for each IP Address

**Apply Refresh Setting**

---

### Data

Please enable this function first


## 14 Configuration > Management

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

Management 
Identification
Administration
Contacts / On Duty
SSH
Web
Firmware
Configuration
Load Factory
Restart
Schedule Reboot
Fail2Ban
FOTA

### 14.1 Management > Identification

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

Identification 	
Attr.	Value
Active Image Partition	a
Model Name	Cellular Router
LAN Ethernet MAC Address	00-03:79-06:6B-01
WAN Ethernet MAC Address	00-03:79-06:6B-02
WiFi AP MAC Address	00-03:79-06:6B-03
Bootloader Version	1.01
Software Version	V1.00
Software MCSV	014B000010030E22
Hardware MCSV	014B000010030E20
Dual Image A MCSV	014B000010030E22
Dual Image B MCSV	014B000010030E20
Serial Number	BL7VB3WE0077
Modem Firmware Version	EC25EFAR06A03M4G
IMEI	866758043841978
Uptime	4 Day 4:55:42
Fota check time	
Fota Software Version	
Fota next check time	

Management > Identification	
Item	Description
<b>Active Image Partition</b>	Show the active image partition: a or b
<b>Model Name</b>	The model name of cellular router.
<b>LAN Ethernet MAC Address</b>	The LAN Ethernet MAC address.
<b>WAN Ethernet MAC Address</b>	The WAN Ethernet MAC address.
<b>WiFi AP MAC Address</b>	The WiFi AP MAC address.
<b>Bootloader Version</b>	The bootloader version of the device.
<b>Software Version</b>	The software version currently running on the device.
<b>Software MCSV</b>	Show the software MCSV of the running firmware
<b>Hardware MCSV</b>	Show the current hardware MCSV of the device.
<b>Dual Image A MCSV</b>	Show the Dual Image A MCSV.
<b>Dual Image B MCSV</b>	Show the Dual Image B MCSV.
<b>Serial Number</b>	Show the product serial number.
<b>Modem Firmware Version</b>	Show the modem firmware version of the device
<b>IMEI</b>	Show the IMEI (International Mobile Equipment Identity number).
<b>Uptime</b>	Show the current system uptime.
<b>FOTA check time</b>	Show the FOTA check time.
<b>FOTA Software Version</b>	Show the FOTA software version.
<b>FOTA next check time</b>	Show the FOTA next check time.

## 14.2 Management > Administration

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

For different users' authority, you can set up each level and password from this section.

(1) Super User can set User 1, 2 and 3 and give them different level authority:

- Level Administrator – can see and can apply each function except super user's password.
- Level Read Only – only can see the current configuration of each function.

(2) Non-super user can only edit his/her password.



Administration

### System Setup

Model Name

Session TTL  (minutes, 0 means no timeout)

### Super User

New Password

Retype to confirm

### User #1

Name

User Level

New Password

Retype to confirm

### User #2

Name

User Level

New Password

Retype to confirm

### User #3

Name

User Level

New Password

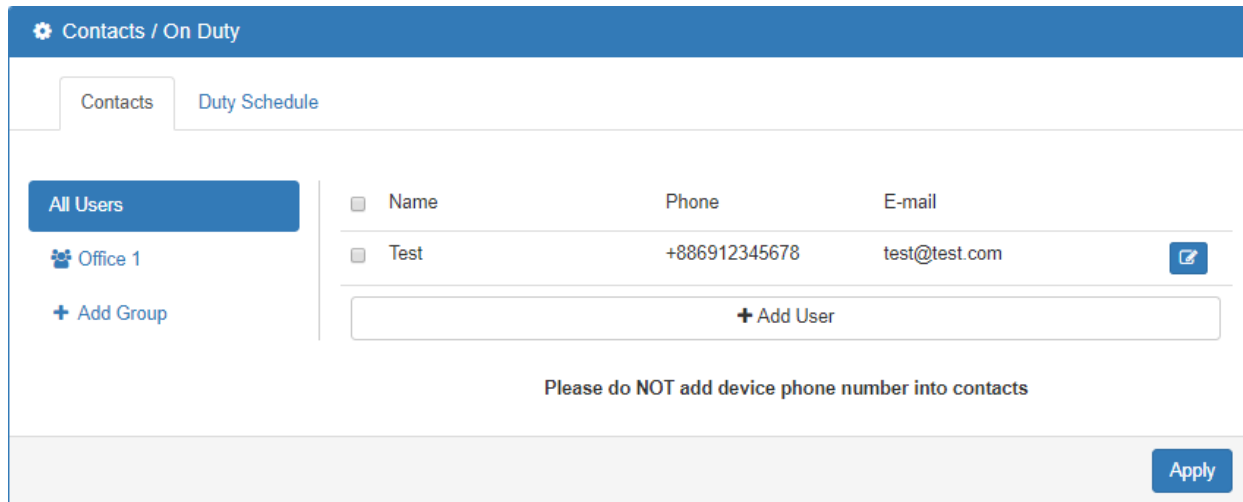
Retype to confirm

## 14.3 Management > Contacts / On Duty

There are two pages, **Contacts** and **Duty Schedule**. **Contacts** allows you to create the groups, and add the users. **Duty Schedule** is to select the duty date for specified groups. The on duty group members can receive alarm, perform SMS actions and input SMS alarm.

### 14.3.1 Contacts

You can create the groups, and add the users by Contacts.



Contacts / On Duty

Contacts Duty Schedule

All Users

Office 1

+ Add Group

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

+ Add User

Please do NOT add device phone number into contacts

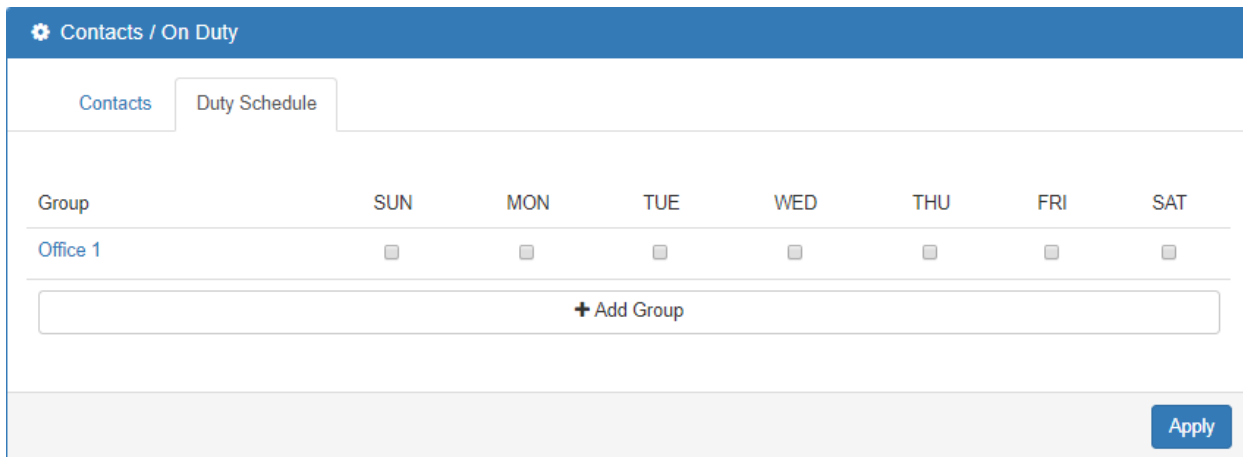
Apply

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

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

### 14.3.2 Duty Schedule

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



Contacts / On Duty

Contacts Duty Schedule

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

+ Add Group

Apply

## 14.4 Management > SSH

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

⚙️ SSH

Mode  Disable  Enable

LAN Server Port

WAN Server Port

Access Control  Allow All  Allow specified IPv4v6 Address below

Apply

⚙️ SSH

Mode  Disable  Enable

LAN Server Port

WAN Server Port

Access Control  Allow All  Allow specified IPv4v6 Address below

**IPv4v6 Address Set**

#	IP Address
1	<input style="width: 90%;" type="text"/>
2	<input style="width: 90%;" type="text"/>
3	<input style="width: 90%;" type="text"/>
4	<input style="width: 90%;" type="text"/>
5	<input style="width: 90%;" type="text"/>
6	<input style="width: 90%;" type="text"/>
7	<input style="width: 90%;" type="text"/>
8	<input style="width: 90%;" type="text"/>
9	<input style="width: 90%;" type="text"/>
10	<input style="width: 90%;" type="text"/>

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

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

Apply

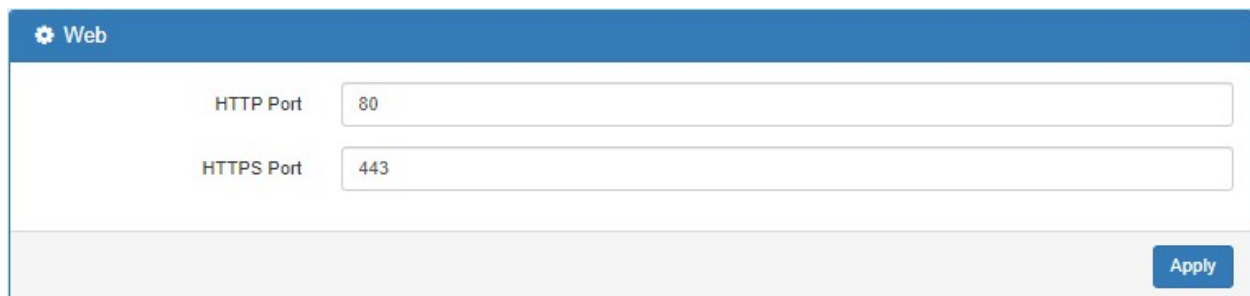
Management > SSH	
Item	Description
Mode	Select from Disable or Enable SSH function.
LAN Server Port	The LAN side TCP port number listened by SSH server.
WAN Server Port	The WAN side TCP port number listened by SSH server.
Access Control	<ul style="list-style-type: none"> <li>● <b>Allow All:</b> Any client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

## 14.5 Management > Web

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

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

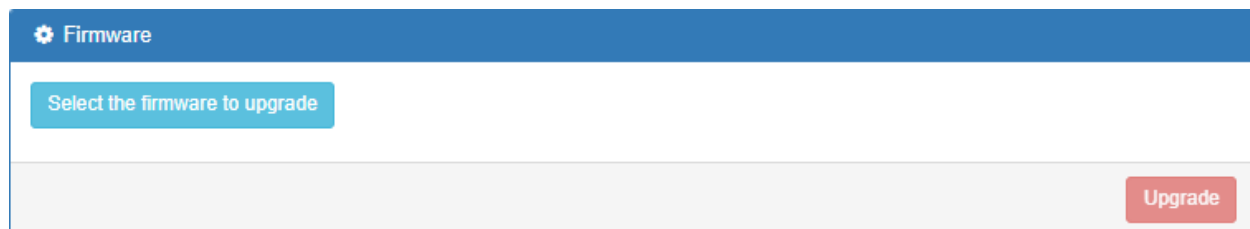
Management > Web	
Item	Description
HTTP Port	The TCP port listened by HTTP daemon.
HTTPS Port	The TCP port listened by HTTPS daemon.



## 14.6 Management > Firmware

This section provides you to upgrade the firmware of router.

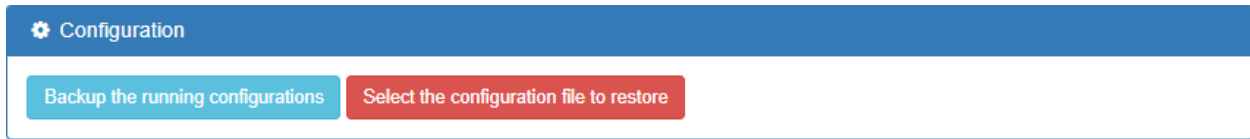
- (1) Click **Select the firmware to upgrade** button to choose your current firmware version in your PC.
- (2) Select **Upgrade** button to update.
- (3) After upgrading successfully, please reboot the router.



## 14.7 Management > Configuration

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

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

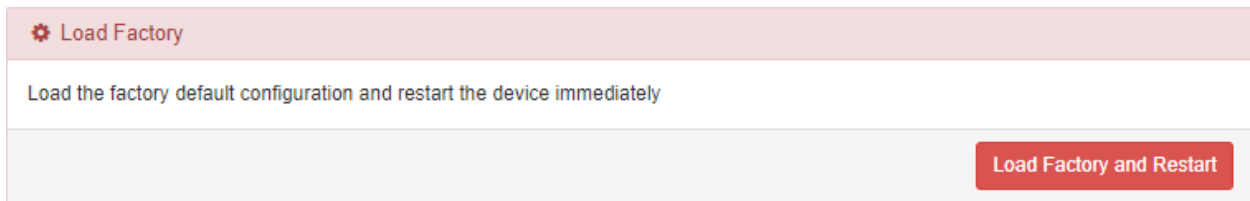


The screenshot shows a blue header with a gear icon and the text "Configuration". Below the header, there are two buttons: a blue button labeled "Backup the running configurations" and a red button labeled "Select the configuration file to restore".

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

## 14.8 Management > Load Factory

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



The screenshot shows a light red header with a gear icon and the text "Load Factory". Below the header, there is a text description: "Load the factory default configuration and restart the device immediately". At the bottom right, there is a red button labeled "Load Factory and Restart".

## 14.9 Management > Restart

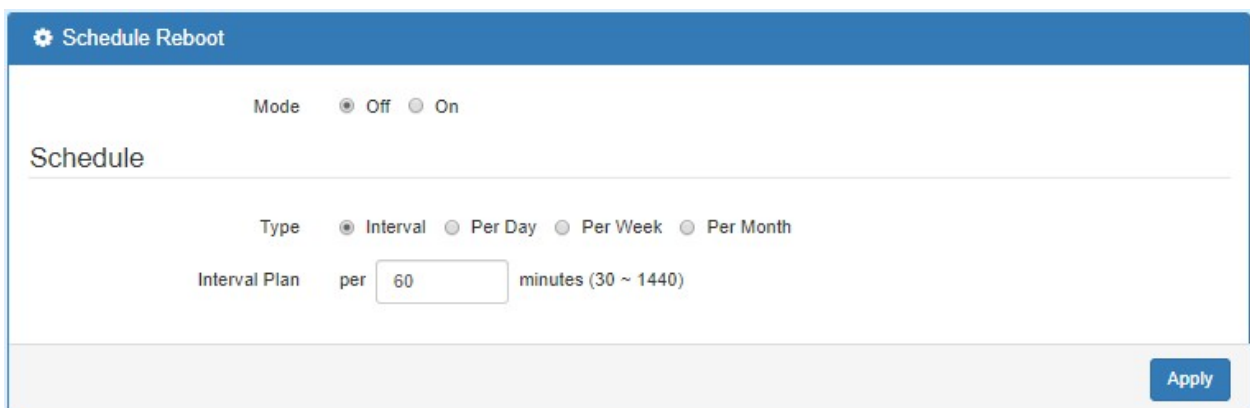
This section allows you to click **Restart** button and the router will restart immediately.



The screenshot shows a light red header with a gear icon and the text "Restart". Below the header, there is a text description: "Restart the device immediately". At the bottom right, there is a red button labeled "Restart".

## 14.10 Management > Schedule Reboot

The setting allows you to schedule the reboot time regularly.




The screenshot shows a blue header with a gear icon and the text "Schedule Reboot". Below the header, there is a "Mode" section with radio buttons for "Off" (selected) and "On". Below that is a "Schedule" section with a "Type" section containing radio buttons for "Interval" (selected), "Per Day", "Per Week", and "Per Month". Under "Interval", there is an "Interval Plan" section with a text input field containing "60" and the text "minutes (30 ~ 1440)". At the bottom right, there is a blue button labeled "Apply".

Management > Schedule Reboot	
Item	Description
<b>Mode</b>	Select the mode from Off or On. The default is Off.
<b>Type</b>	Schedule types include Interval, Per Day, Per Week, and Per Month.
<b>Interval Plan</b>	Input the interval minutes which you want to plan.

## 14.11 Management > Fail2Ban

Fail2Ban is an intrusion prevention feature that protects the device from brute-force login attacks.



Management > Fail2Ban	
Item	Description
<b>Mode</b>	Select from Disable or Enable. The default is Enable.
<b>Retry</b>	The limit for maximum login retries/Attempts.
<b>Ban Time(s)</b>	The banned time(s) for user or IP when it exceeded the retry limit.

## 14.12 Management > FOTA

This section allows you to set up the Firmware Over-the-Air.

### Firmware Over the Air

- Enable
- Check only the new firmware version (not upgrade)
- Update backup partition image

Server URL

Hint ex:(ftp or http)://user:password@host:port/path

### Schedule

- Auto  Custom

Automatic

- Every day  Every week

Custom

**Immediately**

<input type="checkbox"/> Sun	<input type="text" value="00:00"/> ▾ - <input type="text" value="01:00"/> ▾
<input type="checkbox"/> Mon	<input type="text" value="00:00"/> ▾ - <input type="text" value="01:00"/> ▾
<input type="checkbox"/> Tue	<input type="text" value="00:00"/> ▾ - <input type="text" value="01:00"/> ▾
<input type="checkbox"/> Wed	<input type="text" value="00:00"/> ▾ - <input type="text" value="01:00"/> ▾
<input type="checkbox"/> Thu	<input type="text" value="00:00"/> ▾ - <input type="text" value="01:00"/> ▾
<input type="checkbox"/> Fri	<input type="text" value="00:00"/> ▾ - <input type="text" value="01:00"/> ▾
<input type="checkbox"/> Sat	<input type="text" value="00:00"/> ▾ - <input type="text" value="01:00"/> ▾

### Status

Attr.	Value
Update information server	
Firmware download server	
Fota check time	
Fota software version	
Result	
Fota next check time	

**Apply**

<b>Management &gt; FOTA</b>	
<b>Item</b>	<b>Description</b>
<b>Firmware Over the Air</b>	
<b>Enable</b>	Enable or disable the FOTA function, which is Enabled by default.
<b>Check only the new firmware version (not upgrade)</b>	Only check, not download firmware from the server.
<b>Update backup partition image</b>	upgrade image to backup partition, sync two partition
<b>Server URL</b>	Enter custom server URL.
<b>Schedule</b>	
You can choose Auto or Custom, which is Auto by default.	
<b>Auto</b>	There are two options for automatic, every day or every week.
<b>Custom</b>	You can choose the time or execute it immediately
<b>Status</b>	Show the status information after running. Update information server, Firmware download server, FOTA check time, FOTA software version, Result, FOTA next check time.



## 15 Configuration > Diagnosis

This section allows you to diagnose Ping, Traceroute, and TTY2TCP.

Diagnosis
🔧

Ping

Traceroute

TTY2TCP

### 15.1 Diagnosis > Ping

Please assign the Host you want to ping.

🔧 Ping

Host

Ping

Diagnosis > Ping	
Item	Description
<b>Host</b>	The host name or the host IP address

### 15.2 Diagnosis > Traceroute

Please assign the Host you want to traceroute.

🔧 Traceroute

Host

Traceroute

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

## 15.3 Diagnosis > TTY2TCP

TTY2TCP

Port number

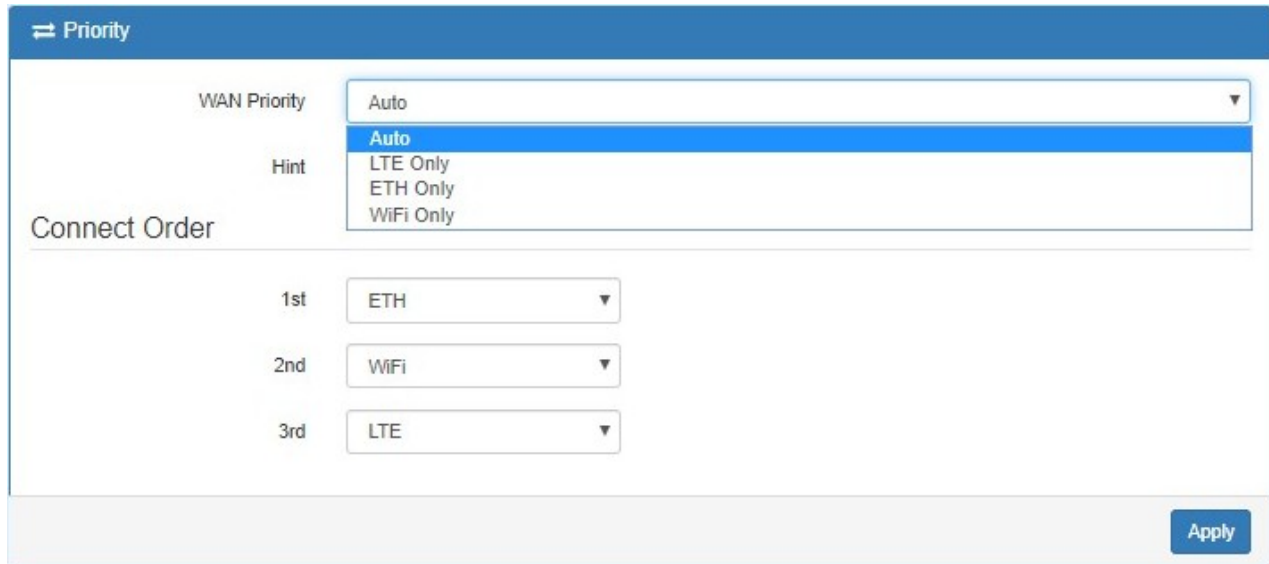
Diagnosis > TTY2TCP	
Item	Description
Port number	the port number to issue TTY2TCP
Start	start TTY2TCP
Stop	stop TTY2TCP

## 16 Configuration Applications

This section explains specific examples how to configure your applications.

### 16.1 WAN Priority

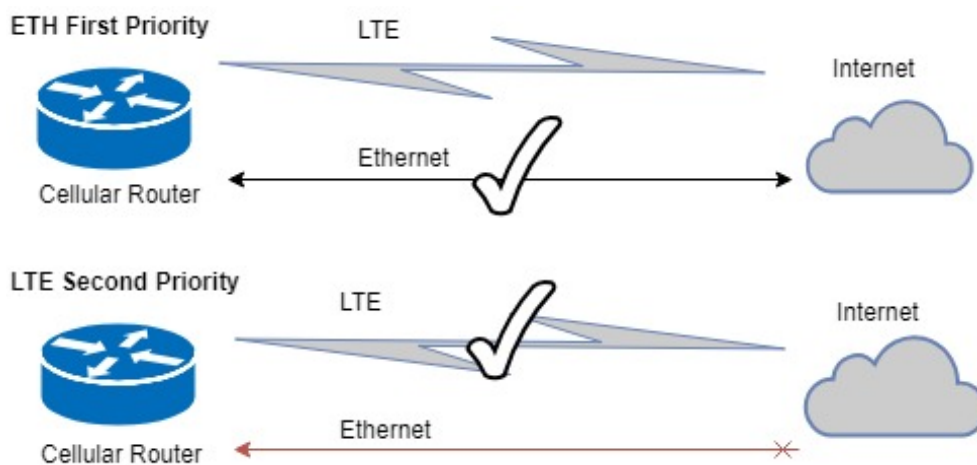
You can select from Auto, LTE Only, ETH Only or WiFi Only. Moreover, you can configure Connect Order to set up the priority.



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

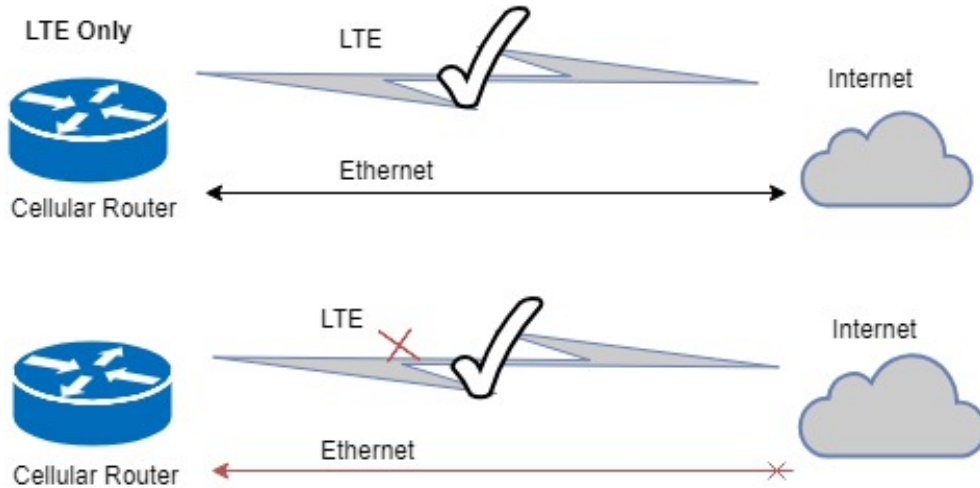
In case both Ethernet and LTE can access Internet, the router would route network packages through Ethernet. The reason is Ethernet that is low price and stable.

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



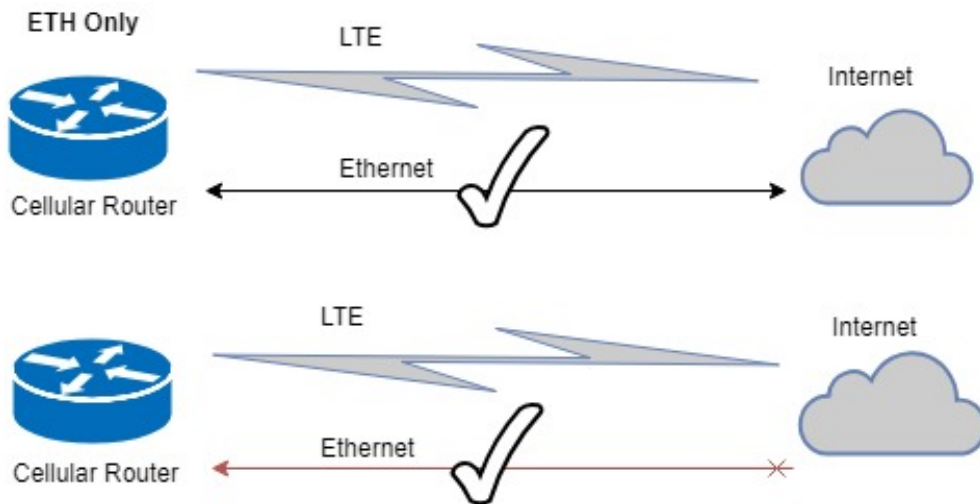
#### (2) WAN Priority > LTE Only:

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



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

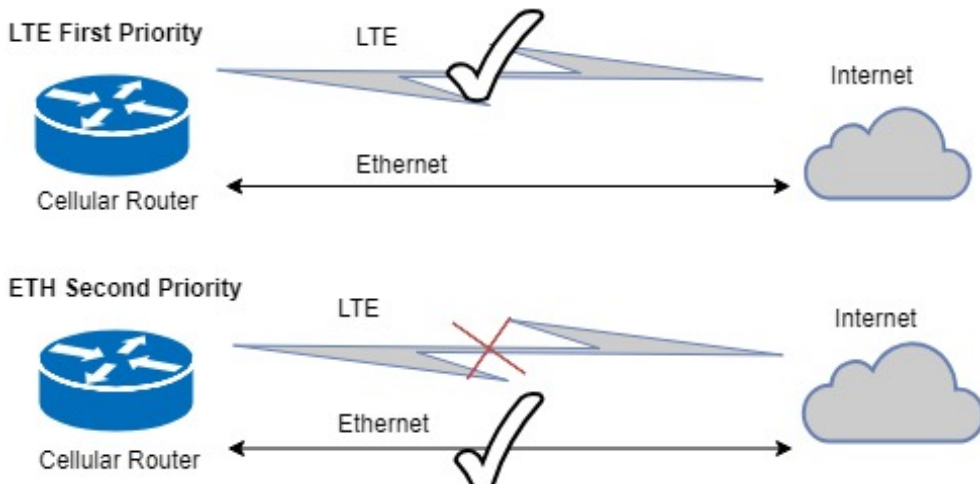
In this mode, the router only routes network packages through Ethernet.



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

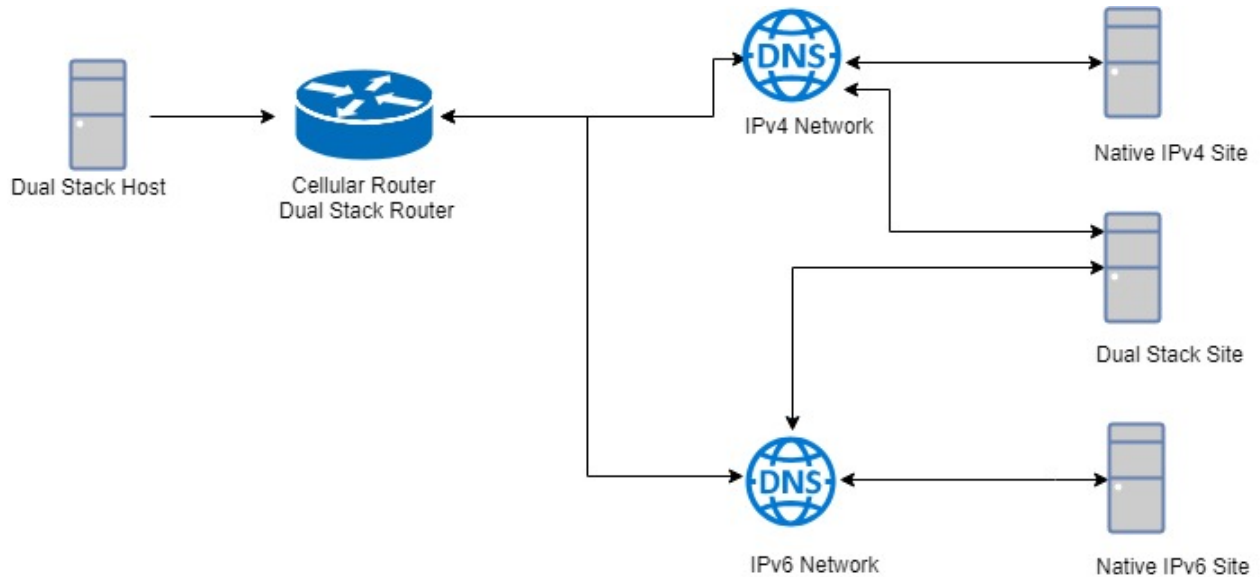
In case both Ethernet and LTE can access Internet, the router would route network packages through LTE.

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



## 16.2 LAN > IPv4/IPv6 Dual Stack

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



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

LAN Ethernet	
Attr.	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	2001:b400:e230:cdfc::1
IPv6 Conn Time	5 Day 3:38:09
Uplink Speed Kbps	0.000
Downlink Speed Kbps	0.000
Tx/Rx KBytes	84411.000/0.000
Tx/Rx Dropped Packets	0/0

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

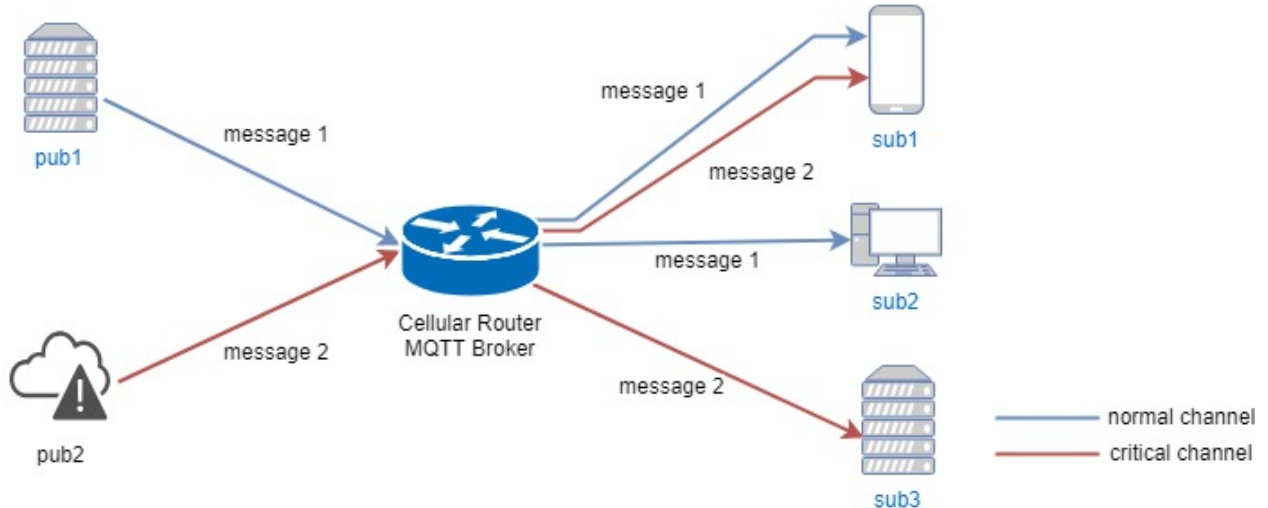
DNS Servers . . . . . : fe80::c2e:43ff:fe0d:4743%15
                            192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

C:\>
```

## 16.3 MQTT Broker

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

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



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

+ MQTT

Mode  Disable  Enable

Port

### Manage Users

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

Username

Password

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

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

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

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

ACLs

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

User

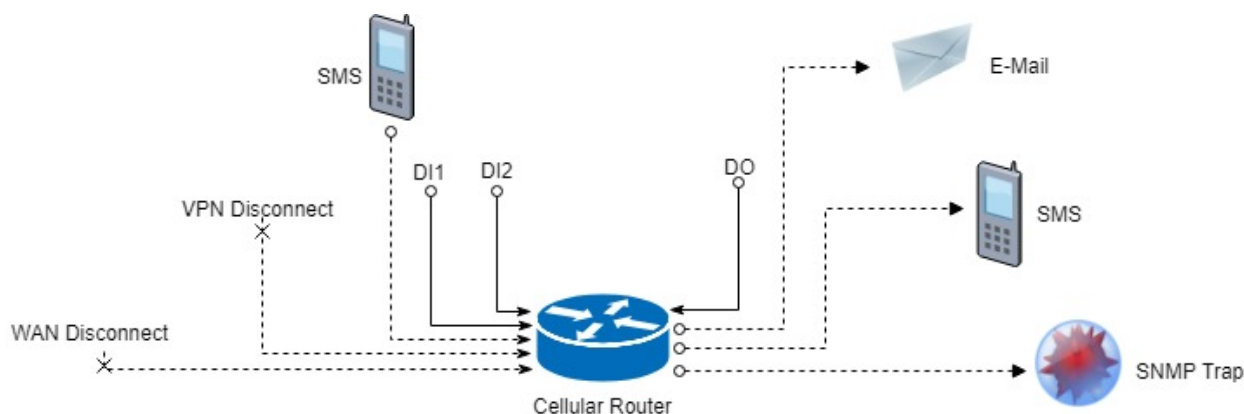
Topic

Subscribe

Publish

## 16.4 Alarm Configuration

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



### (1) Alarm Input:

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

### (2) Alarm Output:

- In case of SMS is selected then only user's phone number is in selected group and on selected working day would receive alarm SMS.



- In case of DO is selected, please make sure your DO is connected to your alarm device.
- In case of SNMP trap is selected, please make sure you enable SNMP trap (**Service -> SNMP**) and fill our server IP.

**Alarm**

Mode  Disable  Enable

Alarm input  SMS  DI  VPN disconnect  WAN disconnect  
 LAN disconnect  Reboot

Alarm output  SMS  DO  SNMP trap  E-mail  
 TR069

DI 1 Trigger  High  Low

DO behavior  Always  Pulse

SMS/E-mail

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

Apply

**SNMP**

Mode  Disable  Enable

Community    SNMP v3 User Configuration    **SNMP trap configuration**

#	Mode	Community Name	Destination
1	<input type="text" value="Disable"/>	<input type="text" value="public"/>	<input type="text"/>
2	<input type="text" value="Disable"/>	<input type="text" value="private"/>	<input type="text"/>

Apply

## 16.5 Open VPN Configuration

### Generic setup

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

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

**Open VPN server certificate generation****Server - Server Security**

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

**Server - User Security**









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

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























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

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

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

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.

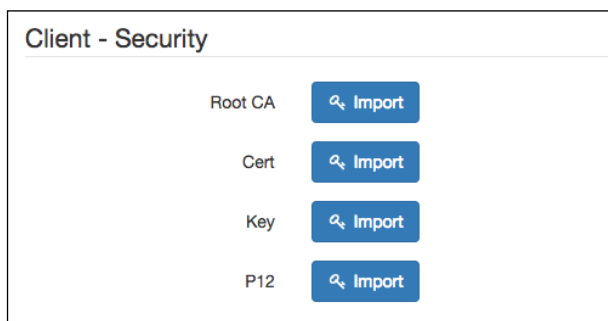
### 16.5.2 Open VPN Client Mode

#### Open VPN client certificate import

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

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

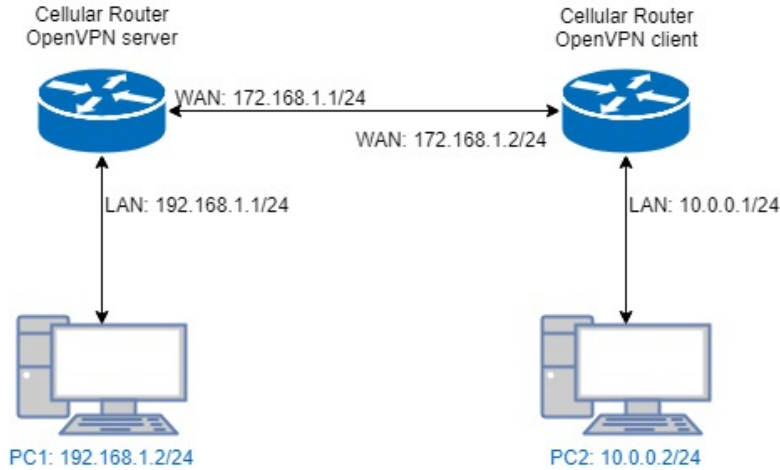
When the files are imported, the web UI is as shown in the right-bottom picture.



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

### 16.5.3 Open VPN Net-to-Net

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



#### (1) Open VPN server configuration

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

Edit Open VPN Connection #1

Mode  Disable  Enable

VPN Mode  Server  Client  Custom

TLS Mode  Disable  Enable

TLS minimal version  none  1.0  1.1  1.2

Cipher

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

VPN Compression  Disable  Enable

Authentication

---

**Server**

Client Mode  Roadwarrior

VPN Network

VPN Netmask

---

**Roadwarrior**

Route Client Networks  Off  On

Connections - Net / Mask

#1  /

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

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

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

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

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

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

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

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

```

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

Certificate:
Data:
  Version: 1 (0x0)
  Serial Number: 1 (0x1)
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C=CH, O=strongSwan, CN=OpenVPN
  Validity
    Not Before: May  9 06:34:08 2017 GMT
    Not After : May  7 06:34:08 2027 GMT
  Subject: C=CH, O=strongSwan, CN=user-00-00@openvpn
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:ac:b1:ca:c7:74:18:70:ed:71:88:9e:c4:ba:d1:
      c4:09:52:b8:11:d7:17:00:e4:dd:e5:a7:f4:e1:f6:
      1c:10:b5:0c:d2:27:e7:f8:63:cb:e2:30:78:6c:ab:
      e3:eb:bd:08: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: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-----
MIIC5zCCAc8CAQEwDQYJKoZIhvcNAQELBQAwNDELMAkGA1UEBhMCQ0gxZARBgNV
BAoMCnN0cm9uZ1N3YW4xEDAOBgNVBAMMB09wZW5WUE4wHhcNMTcwNTA5MDYzNDA4
WWhcNMicwNTA5MDYzNDA4WjA/MoswCOYDV0OGEwJDSDETBGALUECawKc3Rvb25n

```

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

## (2) Open VPN client configuration

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

Edit Open VPN Connection #1

Mode  Disable  Enable

VPN Mode  Server  Client  Custom

TLS Mode  Disable  Enable

TLS minimal version  none  1.0  1.1  1.2

Cipher

Status **Connected**

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

Device  TUN  TAP

Protocol  UDP  TCP

Port

VPN Compression  Disable  Enable

Authentication

---

**Client**

Client Mode  Roadwarrior

Server Address

PKCS12 Password

Route Client Networks  Off  On

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

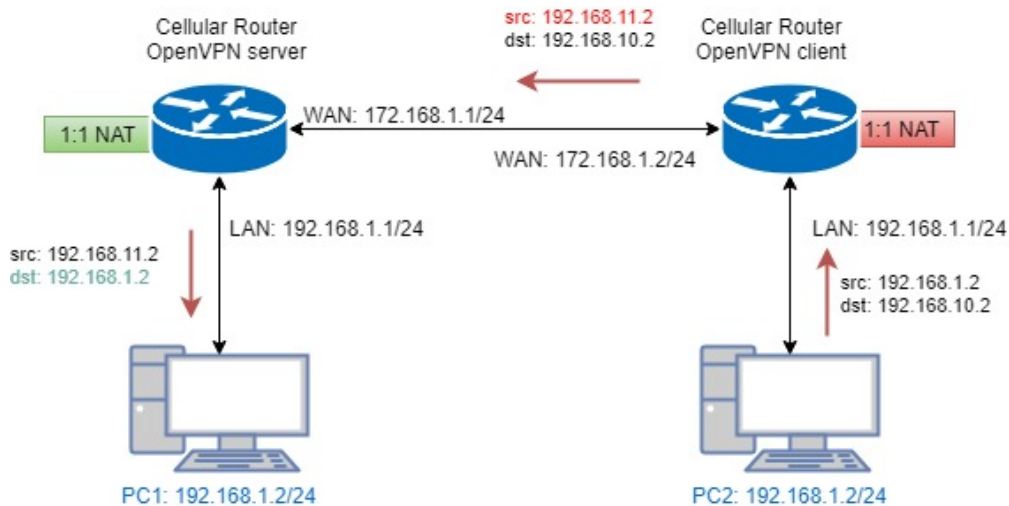
This option requires the P12 file which generated from Generic Setup Open VPN server part.

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

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

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

## 16.5.4 Open VPN 1:1 NAT



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

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

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

### Roadwarrior

Route Client Networks  Off  On

Connections - Net / Mask

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

### NAT

1:1 NAT  Off  On

Network

Netmask

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

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

### Client

Client Mode  Roadwarrior

Server Address

PKCS12 Password

Route Client Networks  Off  On

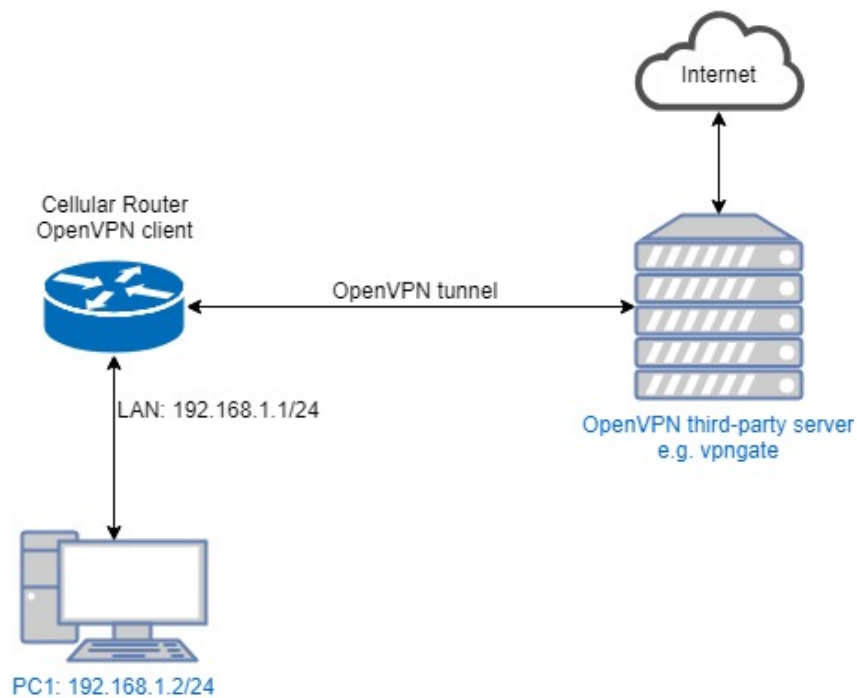
### NAT

1:1 NAT  Off  On

Network

Netmask

### 16.5.5 Open VPN with third-party server



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

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

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

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



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

Edit Open VPN Connection #1

Mode  Disable  Enable

VPN Mode  Server  Client  Custom

Custom Config Import \*.ovpn i ↓

Status **Connected**


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

Back
Refresh
Apply

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

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

Follow @vpngate



**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 \(Refreshed in real time\)](#)

## 16.5.6 Install Open VPN Access Server on Docker

### Open VPN Access Server on Docker installation

Open VPN Access Server is a full featured secure network tunneling VPN software solution that integrates Open VPN server capabilities, enterprise management capabilities, simplified Open VPN Connect UI, and Open VPN Client software packages that accommodate Windows, MAC,



Linux, Android, and iOS environments. Open VPN Access Server supports a wide range of configurations, including secure and granular remote access to internal network and/ or private cloud network resources and applications with fine-grained access control.

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

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

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

## Quick Installation

### ■ Prerequisites

- Ubuntu 16.04
- curl or wget should be installed

### Install via curl

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

### Install via wget

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

### Install Docker on Ubuntu 16.04 64bit

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

Set up the repository

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

```
sudo apt-get update
```

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

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

```
    ca-certificates \
```

```
    curl \
```

```
    software-properties-common
```

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

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

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

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

```
    stable"
```

### Install Docker CE

```
sudo apt-get update
```

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

Install Open VPN Access Server by docker image

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



```
sudo mkdir -p /Open VPN-as
```

```
sudo docker create --name=Open VPN-as \  
-v /Open VPN-as:/config \  
-e TZ="Asia/Taipei" \  
-e INTERFACE=enp3s0 \  
--net=host --privileged linuxserver/Open VPN-as
```

```
sudo docker start Open VPN-as
```

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

### Setup Open VPN Access Server for Cellular Router

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

The default administrator username and password is admin/password.

Login page:



OpenVPN Technologies, Inc.

A screenshot of the OpenVPN Admin Login page. It features a light blue background with the text 'Admin Login' at the top. Below this, there are two input fields: 'Username' and 'Password'. A green 'Sign In' button is positioned below the password field.

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

**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.)

**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**

- 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	<a href="#">No Default Group</a>	<a href="#">Show</a>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2. <input type="text" value="New Username: test"/>	<a href="#">No Default Group</a>	3. <a href="#">Show</a>	<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"/>	
<p>New Username: <input type="text" value="test"/></p> <p>Local Password: 4. <input type="password" value="....."/> (No Password Set)</p> <p>Select IP Addressing : <input checked="" type="radio"/> Use Dynamic <input type="radio"/> Use Static</p> <p><b>Access Control</b></p> <p>Select addressing method: <input checked="" type="radio"/> Use NAT <input type="radio"/> Use routing</p> <p>Allow Access To these Networks:</p> <div style="border: 1px solid #ccc; height: 30px; width: 100%;"></div> <p>List subnets in <i>network/nbits</i> form</p> <p>Allow Access From: <input type="checkbox"/> all server-side private subnets</p> <p>Allow Access From: 5. <input checked="" type="checkbox"/> all other VPN clients</p> <p><b>VPN Gateway</b></p> <p>Configure VPN Gateway: <input checked="" type="radio"/> No <input type="radio"/> Yes</p> <p><b>DMZ settings</b></p> <p>Configure DMZ IP address: <input checked="" type="radio"/> No <input type="radio"/> Yes</p>						

Require user permissions record for VPN access

6.

### User Permissions Changed

User 'test' added.

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

7.

## Setup Cellular Router Open VPN client



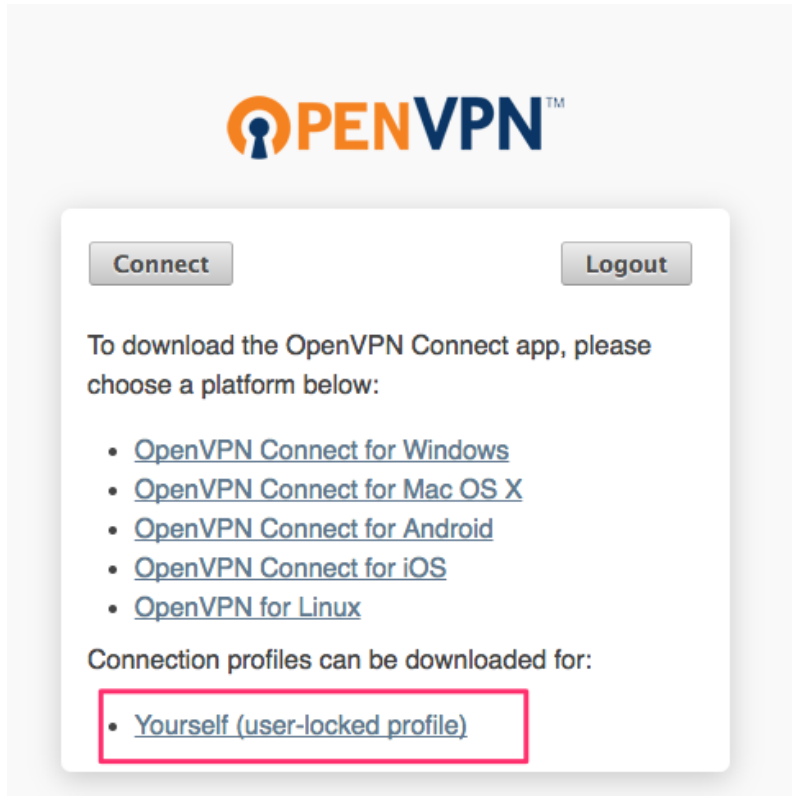


Username:

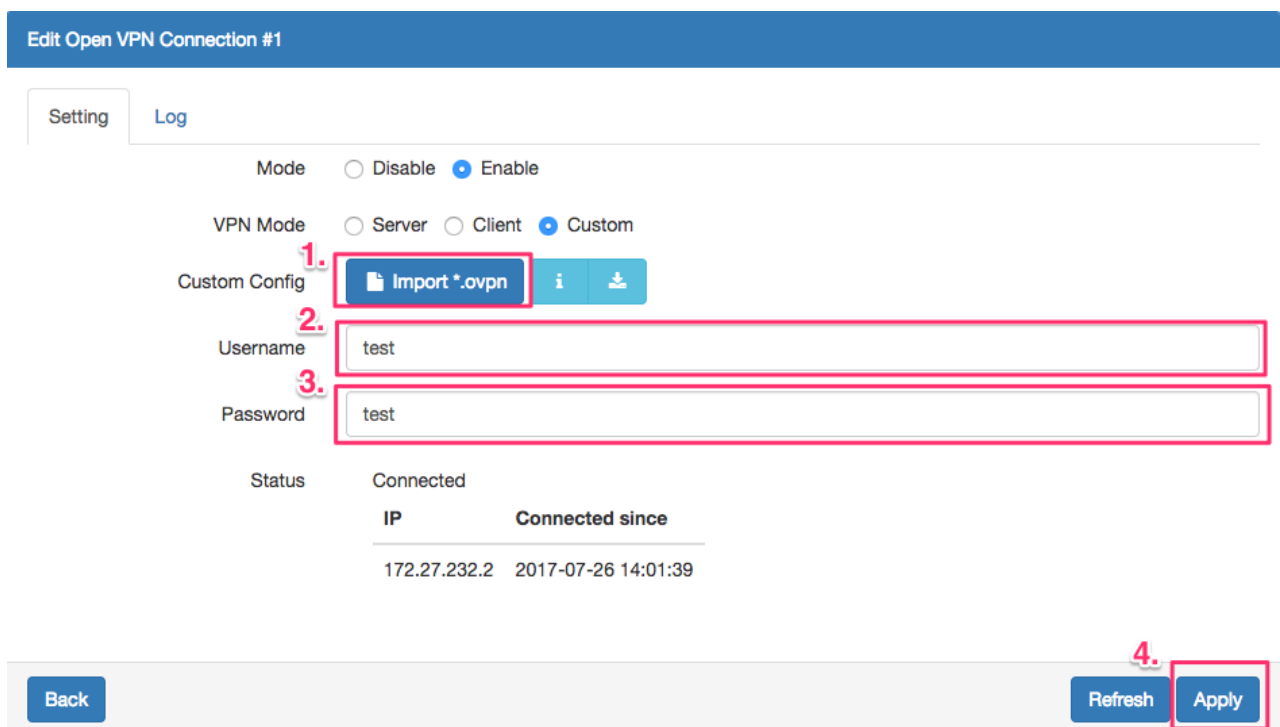
Password:

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

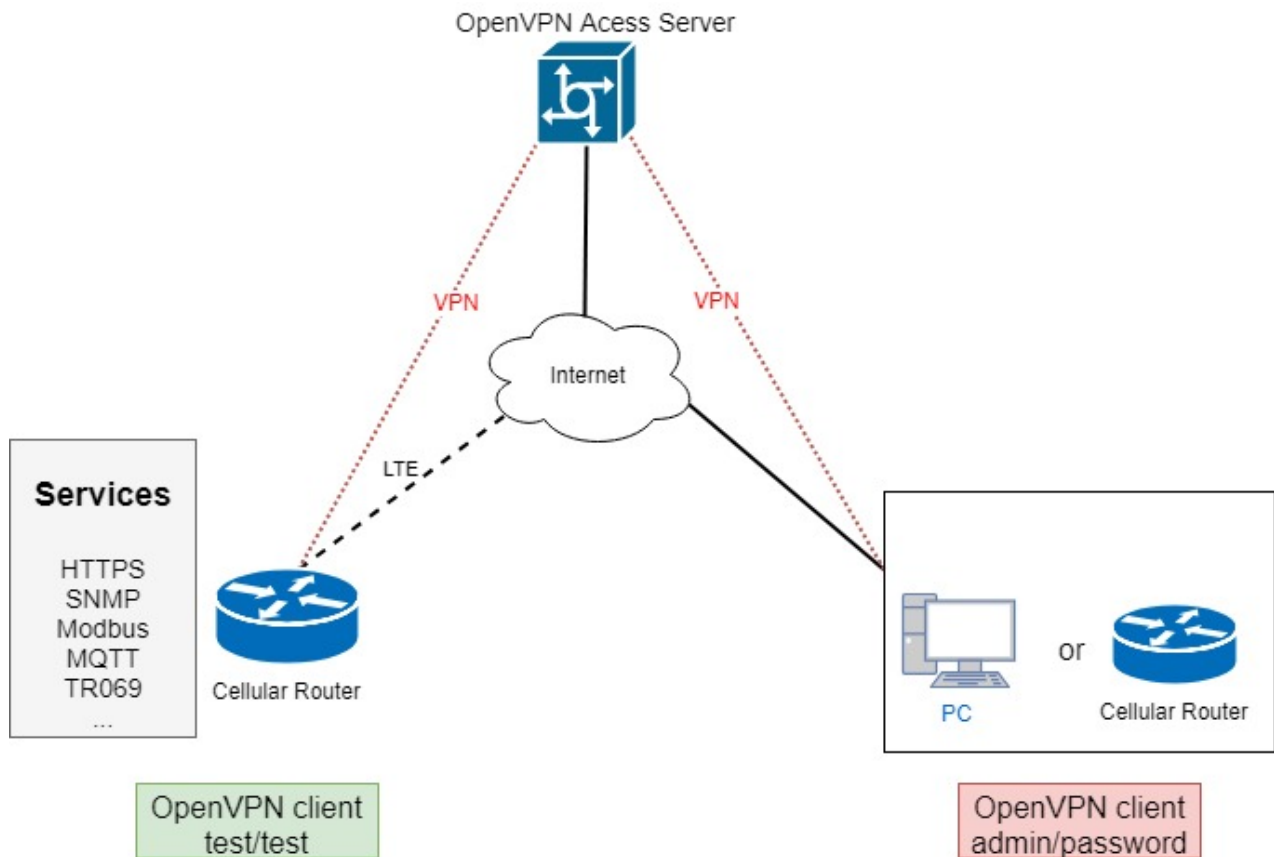
Please make sure to change the type from Connect to Login.



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



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



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

### 16.5.7 Install Pritunl Open VPN server on Docker

#### Pritunl Open VPN server on Docker installation

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

#### Quick Installation

##### ■ Prerequisites

- Ubuntu 16.04
- curl or wget should be installed

##### ■ Install via curl

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

##### ■ Install via wget

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

#### Install Docker on Ubuntu 16.04 64bit

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

#### Set up the repository

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

```
sudo apt-get update
```

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

### **Install Docker CE**

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

### **Install Docker compose**

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

### **Install Pritunl Open VPN Server by docker compose**

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

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

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

```
version: '2'  
services:  
    pritunl:  
        image: jippi/pritunl  
        volumes:  
            - pritunl:/var/lib/pritunl  
            - mongo:/var/lib/mongodb  
        privileged: true  
        network_mode: "host"  
        ports:  
            - "1194:1194/tcp"  
            - "1194:1194/udp"  
            - "80:80/tcp"  
            - "443:443/tcp"
```

```
volumes:
```



mongo:

pritunl:

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

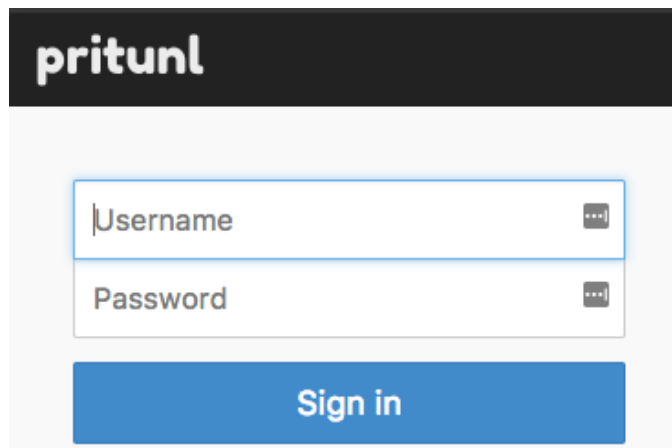
(4) Check the Pritunl Open VPN Server by visiting `https://<server_ip_or_domain>`

### Setup Pritunl Open VPN Server for Cellular Router

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

The default username/password is pritunl/pritunl.

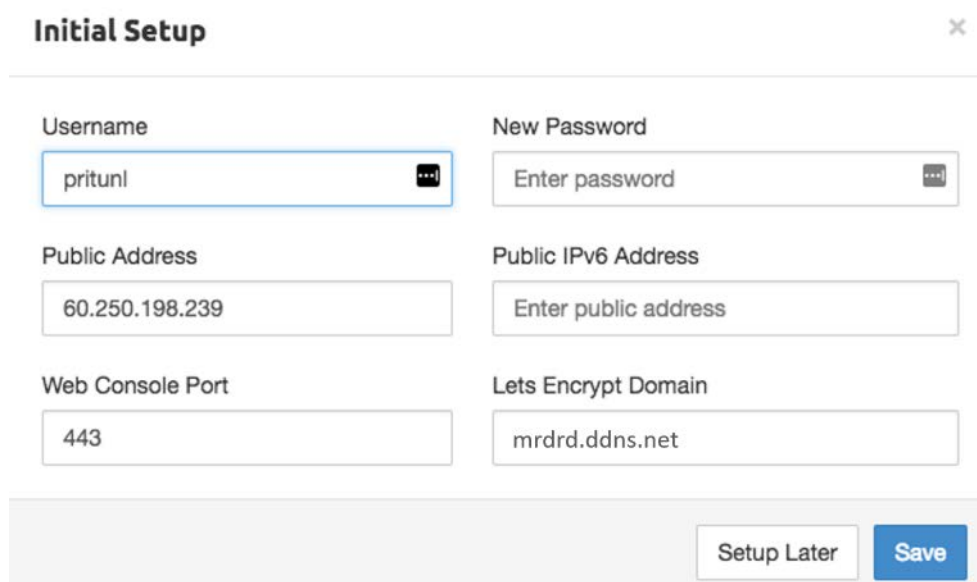
Login Page:



The login page features the Pritunl logo at the top left. Below it are two input fields: 'Username' and 'Password', each with a toggle icon on the right. A blue 'Sign in' button is positioned below the password field.

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

### Initial Setup:



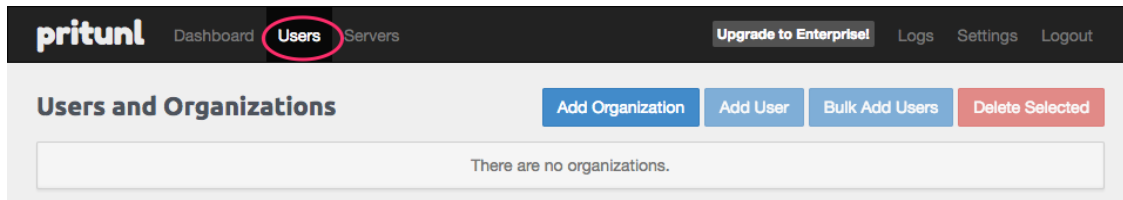
The 'Initial Setup' dialog box contains several configuration fields:

Username	New Password
pritunl	Enter password
Public Address	Public IPv6 Address
60.250.198.239	Enter public address
Web Console Port	Lets Encrypt Domain
443	mrdrd.ddns.net

At the bottom right, there are two buttons: 'Setup Later' and 'Save'.

### Open VPN user setup

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



Add the organization by click the Add Organization button.

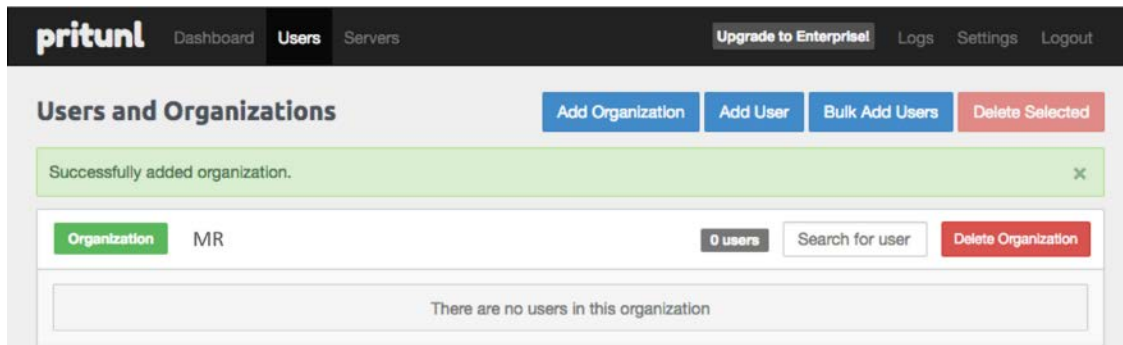
### Add Organization ✕

Name **Name of organization**

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

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



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

### Add User ✕

Name

Select an organization

Email (optional)

Pin

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

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

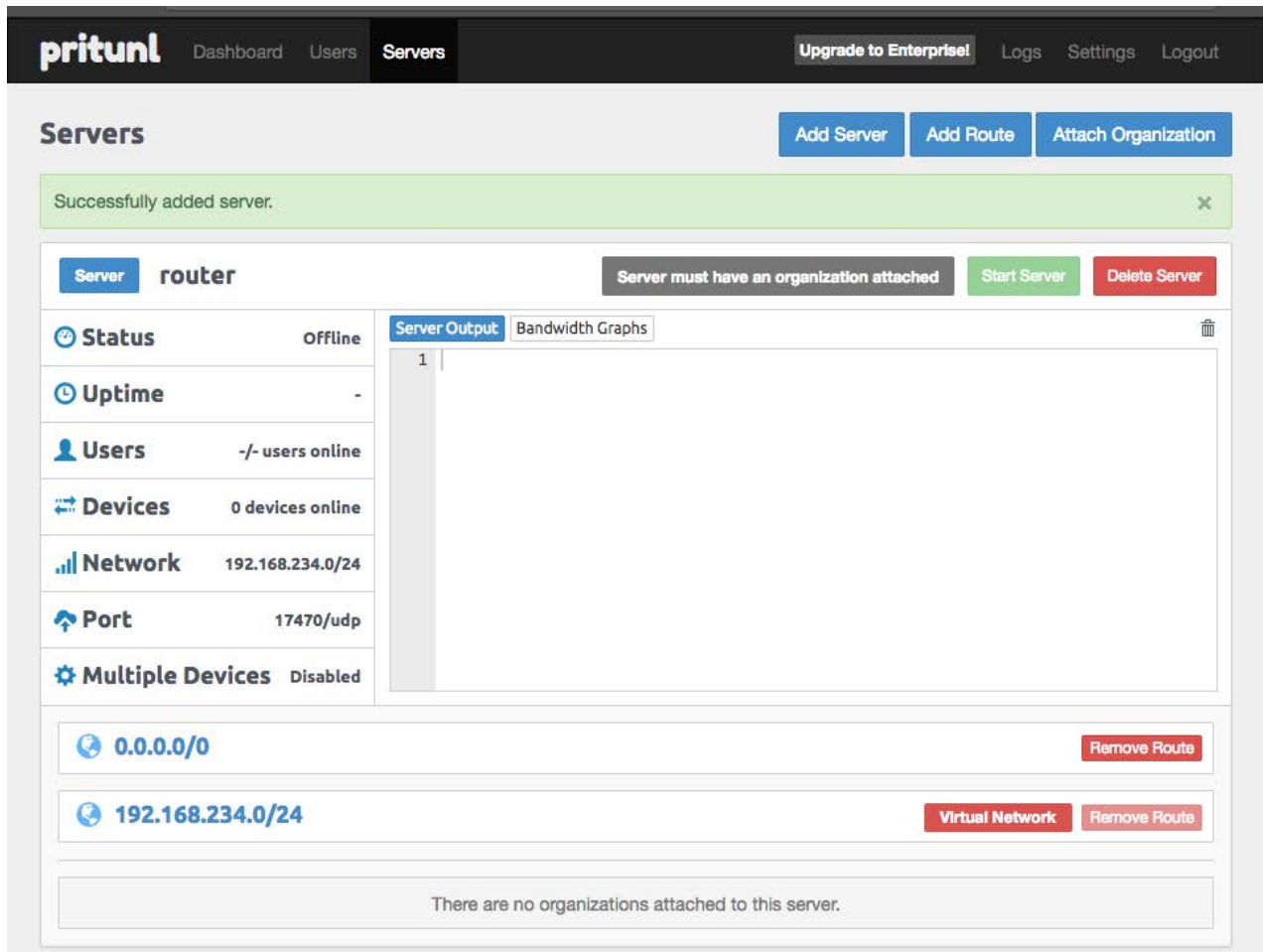
### Open VPN server setup

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

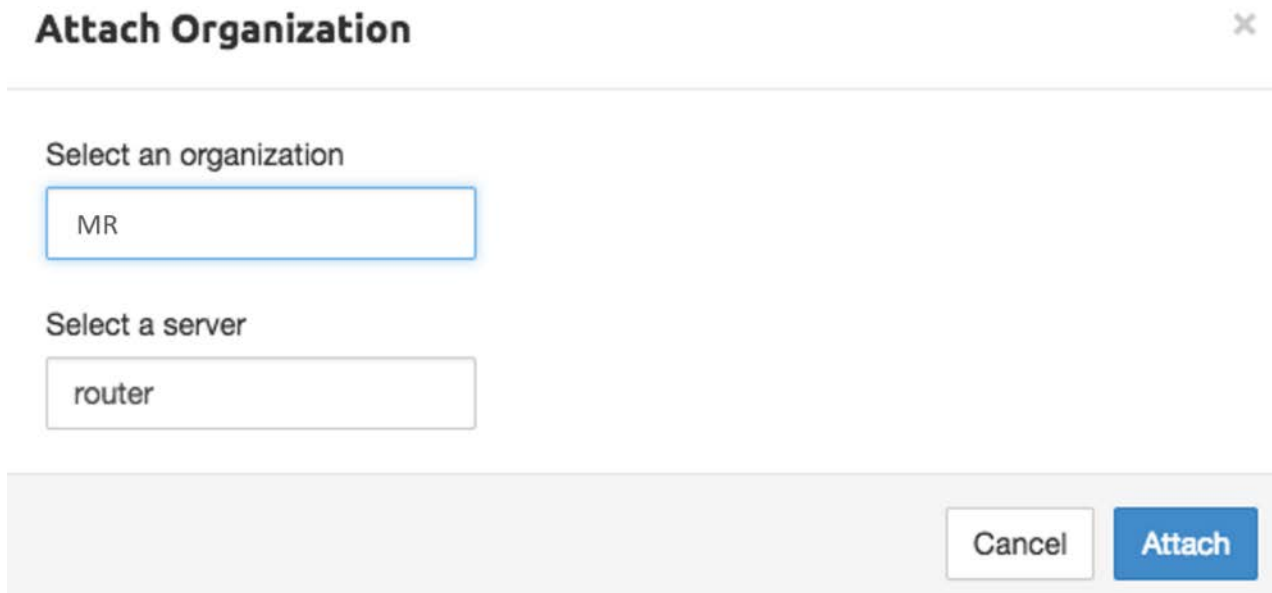
And click the Add Server button to create the Open VPN server.

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

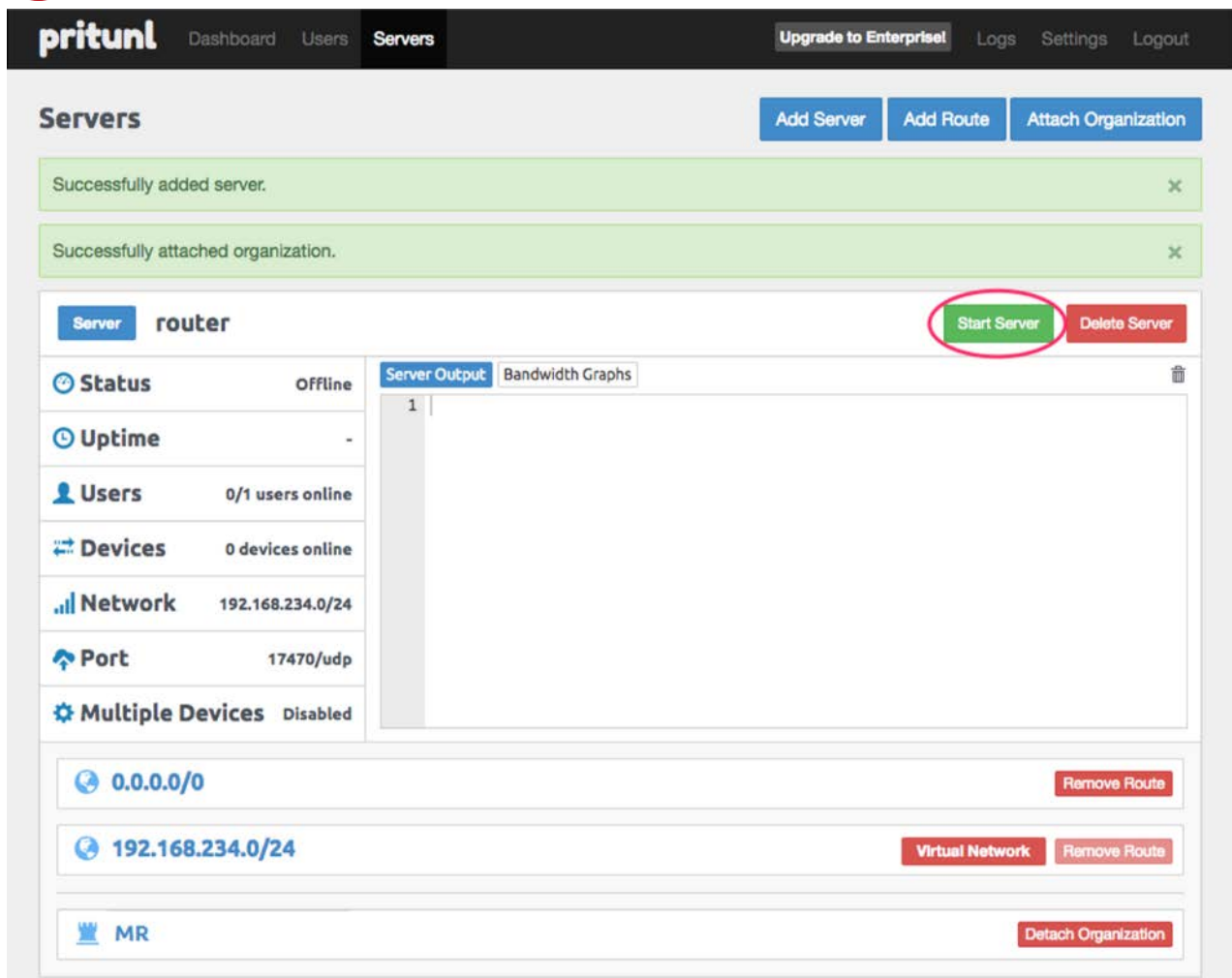
When the Open VPN server created, the Servers page should like the following figure.



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



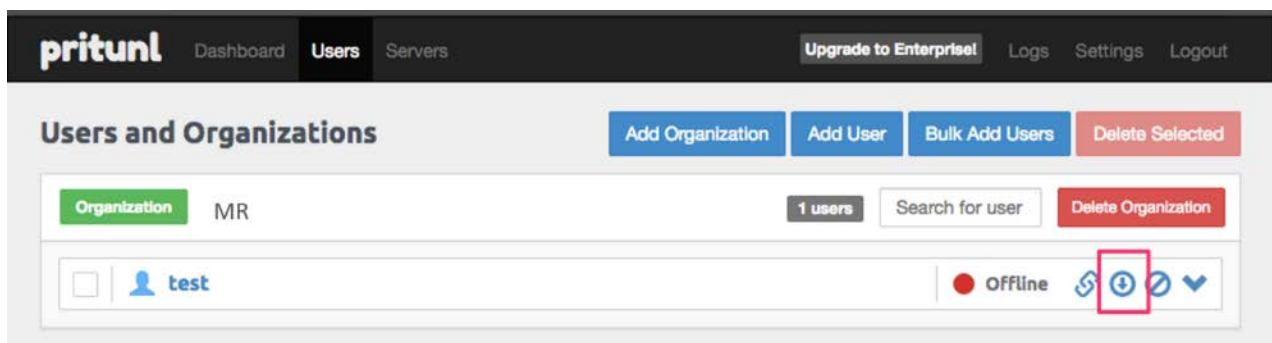
Start the Open VPN server by click Start Server button.



The screenshot shows the 'Servers' page in the Pritunl interface. At the top, there are navigation tabs for 'Dashboard', 'Users', and 'Servers', along with an 'Upgrade to Enterprise!' button and links for 'Logs', 'Settings', and 'Logout'. Below the navigation, there are three buttons: 'Add Server', 'Add Route', and 'Attach Organization'. Two green notification boxes indicate 'Successfully added server.' and 'Successfully attached organization.'. The main content area shows a server named 'router' with a status of 'Offline'. A red circle highlights the 'Start Server' button. To the right of the 'Start Server' button is a 'Delete Server' button. Below the server details, there are three route entries: '0.0.0.0/0' with a 'Remove Route' button, '192.168.234.0/24' with 'Virtual Network' and 'Remove Route' buttons, and 'MR' with a 'Detach Organization' button.

## Cellular Router setup

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



The screenshot shows the 'Users and Organizations' page in the Pritunl interface. At the top, there are navigation tabs for 'Dashboard', 'Users', and 'Servers', along with an 'Upgrade to Enterprise!' button and links for 'Logs', 'Settings', and 'Logout'. Below the navigation, there are four buttons: 'Add Organization', 'Add User', 'Bulk Add Users', and 'Delete Selected'. The main content area shows an organization named 'MR' with '1 users'. Below the organization details, there is a user named 'test' with a status of 'Offline'. A red circle highlights the 'Start' button (represented by a power icon) next to the user's status.

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

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

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

**Edit Open VPN Connection #1**

Setting | Log

Mode  Disable  Enable

VPN Mode  Server  Client  Custom

Custom Config

Username

Password

Status **Connected**

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

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

**pritunl** Dashboard **Users** Servers  Logs Settings Logout

**Users and Organizations**

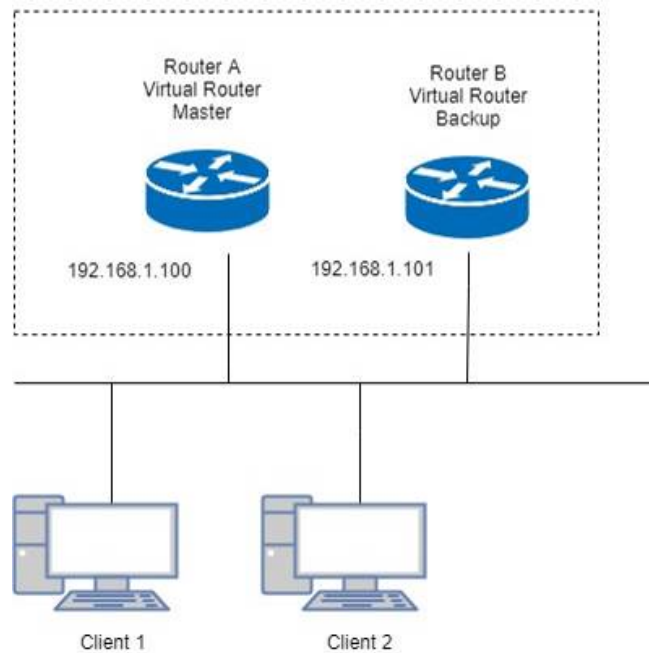
**Organization** MR 1 users

**test** Online

192.168.235.2 60.250.198.235 4:04 pm Online

## 16.6 VRRP Topology

### Basic VRRP Topology



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

## 16.7 TR069 Server (GenieACS Installation)

Server OS: Ubuntu 14.04 on Virtualbox

### Installation:

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



```
make && make install
```

```
ruby -v
```

```
ruby 2.4.1p111 (2017-03-22 revision 58053) [i686-linux]
```

```
cd /opt
```

```
gem install rails --no-ri --no-rdoc
```

```
gem install bundle --no-ri --no-rdoc
```

7) Install node.js

```
cd /opt
```

```
wget http://nodejs.org/dist/v8.2.1/node-v8.2.1.tar.gz
```

```
tar zxvf node-v8.2.1.tar.gz
```

```
cd node-v8.2.1
```

```
./configure
```

```
make && make install
```

```
node -v
```

```
v8.2.1
```

8) Install redis

```
cd /opt
```

```
wget http://download.redis.io/releases/redis-4.0.1.tar.gz
```

```
tar zxvf redis-4.0.1.tar.gz
```

```
cd redis-4.0.1
```

```
make
```

```
make test
```

```
All tests passed without errors!
```

```
make install
```

```
#Start redis server
```

```
redis-server
```

9) Install mongodb

```
cd /opt
```

```
wget https://fastdl.mongodb.org/linux/mongodb-linux-i686-3.3.3.tgz
```

```
tar zxvf mongodb-linux-i686-3.3.3.tgz
```

```
cd mongodb-linux-i686-3.3.3
```

```
mkdir -p /data/db
```

10) Install genieACS

```
cd /opt
```

```
git clone https://github.com/zaidka/genieacs.git
```

```
cd genieacs
```

```
npm install
```

```
npm run configure
```

```
npm run compile
```



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

Original configuration:

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

New configuration example.:

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

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

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

Original configuration:

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

New configuration example:

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

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

#### 11) Install genieACS-Gui

```
git clone https://github.com/zaidka/genieacs-gui  
cd genieacs-gui  
bundle  
  
gem install json  
bundle update  
  
rm -f db/*.sqlite3  
rake db:create  
RAILS_ENV=development rake db:migrate  
  
cd /opt  
cd genieacs-gui/config  
cp index_parameters-sample.yml index_parameters.yml  
cp parameter_renderers-sample.yml parameter_renderers.yml  
cp parameters_edit-sample.yml parameters_edit.yml  
cp roles-sample.yml roles.yml  
cp summary_parameters-sample.yml summary_parameters.yml  
cp users-sample.yml users.yml  
cp graphs-sample.json.erb graphs.json.erb
```

**GenieACS startup script:**

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

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

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

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

```
pidof mongod
```

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

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

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

```
fi
```

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

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

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

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

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

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

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

```
cd $GENIE_GUI_PATH
```

```
rails server -b 0.0.0.0
```

**GenieACS stop:**

Ctrl-C

**Usage:**

## 1) Device Configuration

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

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

## 2) GenieACS Operation

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

Press Home tab to refresh Online devices status.



The screenshot shows the GenieACS web interface. At the top left is the GenieACS logo. At the top right, there is a user name 'admin' and a 'Log out' link. Below the header is a navigation menu with tabs: Home (circled in red), Devices, Faults, Presets, Objects, Provisions, Virtual Parameters, and Files. Below the navigation menu, the text 'Online devices' is displayed.

**All devices**

● Online now: 1 (100.00%)  
● Past 24 hours: 0 (0.00%)  
● Others: 0 (0.00%)  
**Total: 1**

## 2.1) Login

Username and Password are admin/admin.



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

## 3) Device information

Press Devices tab



The 'Devices' page shows a navigation bar with 'Home', 'Devices', 'Faults', 'Presets', 'Objects', 'Provisions', 'Virtual Parameters', and 'Files'. The 'Devices' tab is selected. Below the navigation bar is a 'Listing devices' section with a 'Filters' dropdown and 'Filter' and 'Clear' buttons. A table displays one device:

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

A 'Download' link is located below the table.

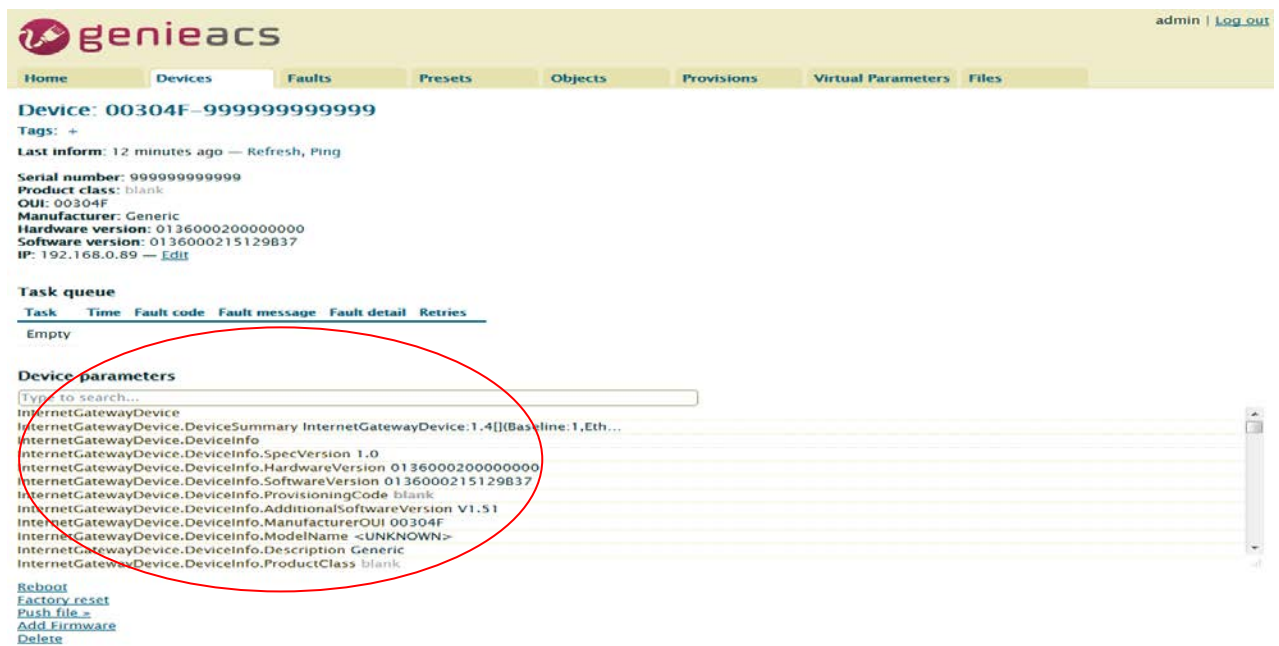
Move mouse to line end of your device, the [Show](#) link show up.

### Showing 1 devices

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

A 'Download' link is located below the table. A 'Show' link is visible at the end of the last information column.

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



The device details page shows the 'Devices' tab selected. The device ID is '00304F-999999999999'. Below this are 'Tags' and 'Last inform' (12 minutes ago). The main section lists device details:

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

Below the details is a 'Task queue' table with columns: Task, Time, Fault code, Fault message, Fault detail, Retries. The queue is empty. The 'Device parameters' section contains a search box and a list of parameters, including 'InternetGatewayDevice.DeviceInfo.SpecVersion 1.0' and 'InternetGatewayDevice.DeviceInfo.HardwareVersion 0136000200000000'. A 'Reboot' button is located at the bottom of the parameters section.

## 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...

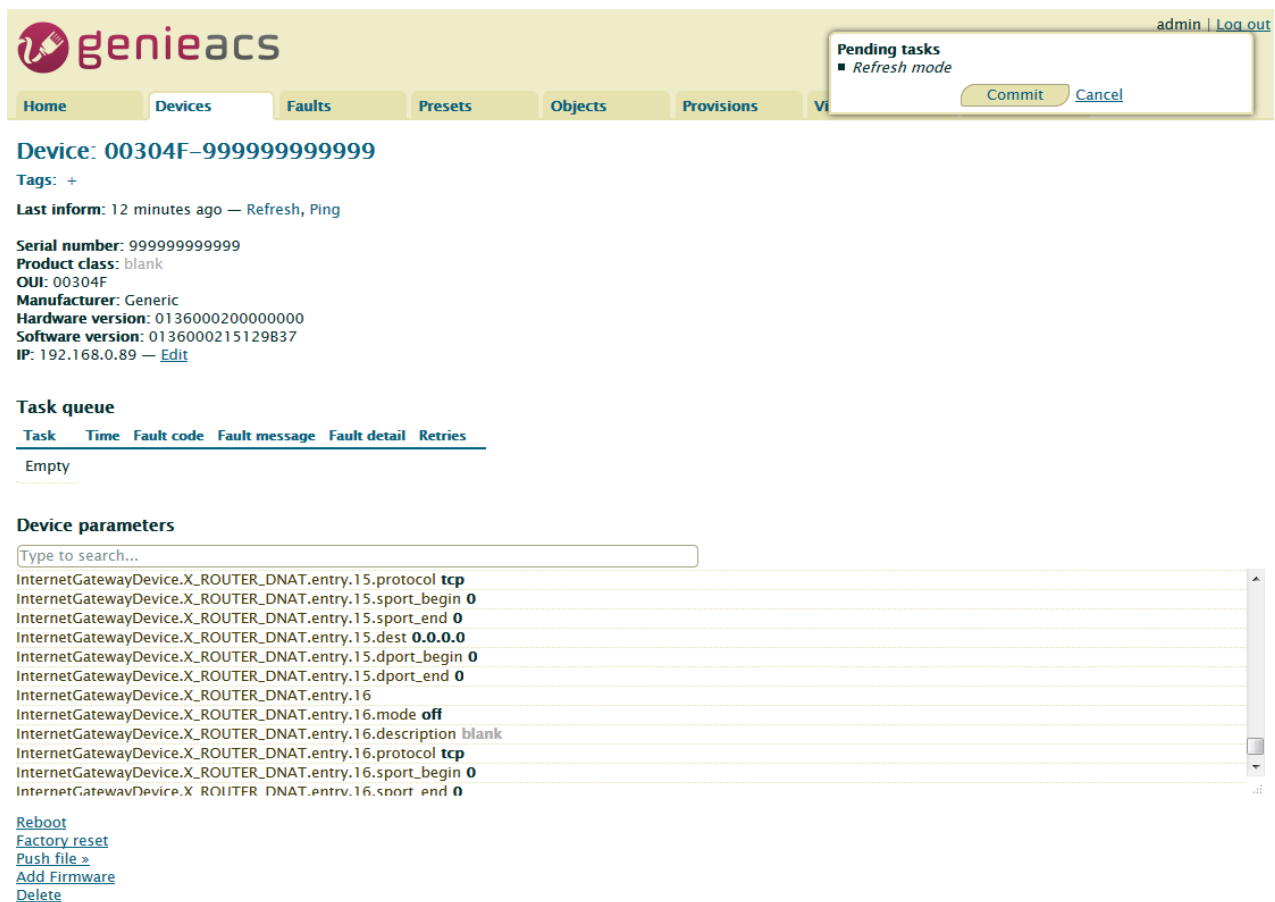
- InternetGatewayDevice
- InternetGatewayDevice.DeviceSummary InternetGatewayDevice:1.4[(Baseline:1,Eth...
- InternetGatewayDevice.DeviceInfo
- InternetGatewayDevice.DeviceInfo.SpecVersion 1.0
- InternetGatewayDevice.DeviceInfo.HardwareVersion 0136000200000000 [Refresh](#)
- InternetGatewayDevice.DeviceInfo.SoftwareVersion 0136000215129B37
- InternetGatewayDevice.DeviceInfo.ProvisioningCode blank

### For Readable and Writable parameter

- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.15.dest 0.0.0.0
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.15.dport\_begin 0
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.15.dport\_end 0
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.16
- InternetGatewayDevice.X\_ROUTER\_DNAT.entry.16.mode **off** [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.



The screenshot shows the GenieACS interface for a device with ID 00304F-999999999999. A 'Pending tasks' window is open in the top right corner, displaying 'Refresh mode' with 'Commit' and 'Cancel' buttons. The device details include: Serial number: 999999999999, Product class: blank, OUI: 00304F, Manufacturer: Generic, Hardware version: 0136000200000000, Software version: 0136000215129B37, and IP: 192.168.0.89. Below the details is a 'Task queue' table which is currently empty. At the bottom, the 'Device parameters' list is visible, showing various X\_ROUTER\_DNAT entries with a 'Refresh' link at the end of the entry for mode 'off'.

Press Commit to get this parameter value.

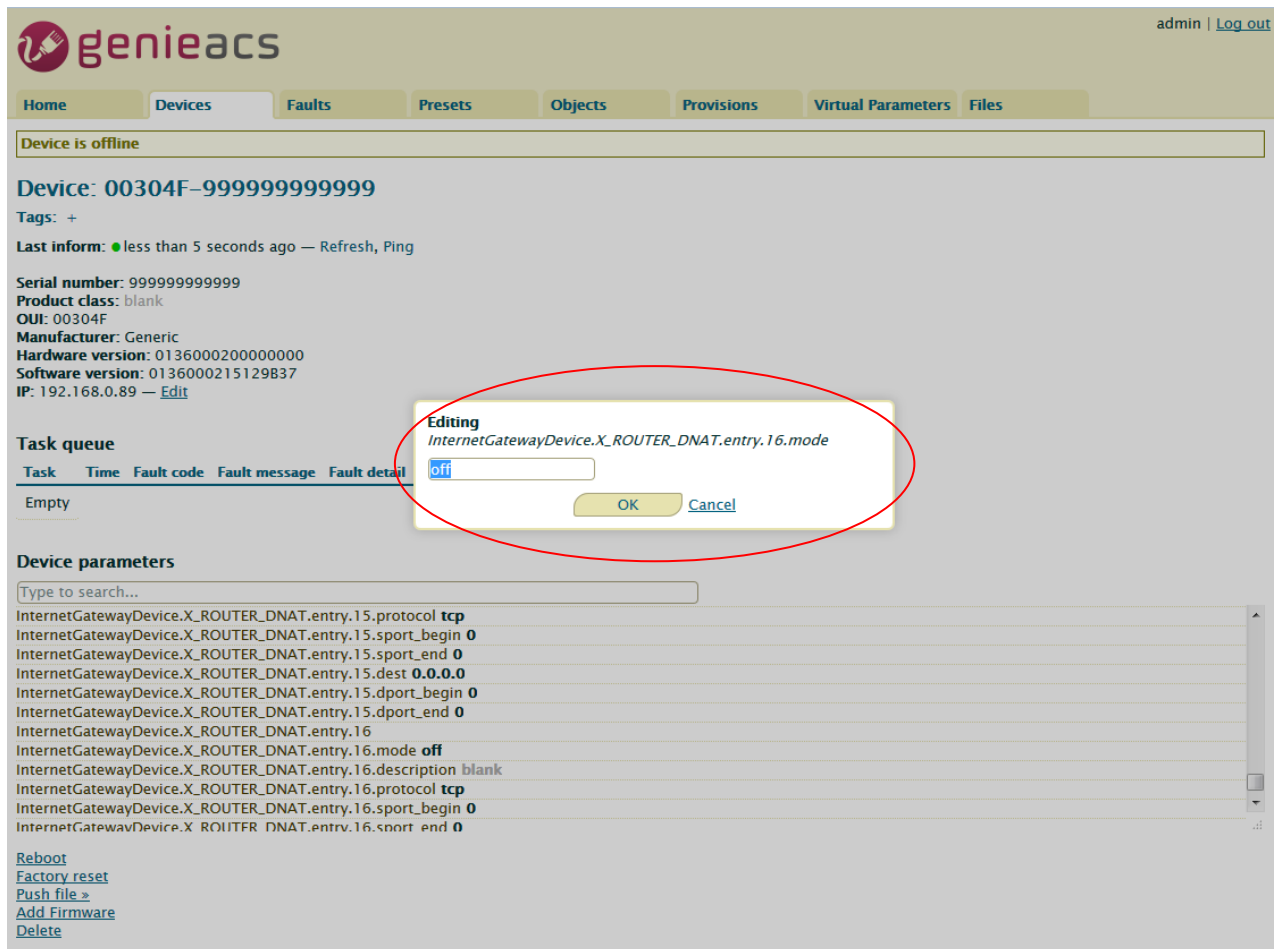
**Note:** If the GenieACS can reach the device, the parameter value will be updated immediately. Otherwise, this request will be queued on Task queue list until next time device connect to

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

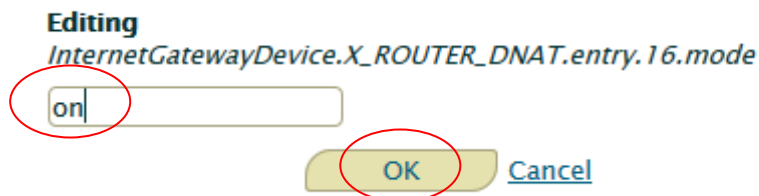
**Note:** To update partial tree, refresh the parent node of the partial tree.

#### 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.

admin | [Log out](#)

**Pending tasks**

- Edit mode

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

Device is offline

Device: 00304F-999999999999

Tags: +

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

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

**Task queue**

Task	Time	Fault code	Fault message	Fault detail	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 set this parameter value.

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

5) Reboot device

Press on [Reboot](#) link.

Device: 00304F-Mobile%20Router-999999999999

Tags: +

Last inform: about 2 hours ago — Refresh, Ping

Serial number: 999999999999  
 Product class: Mobile Router  
 OUI: 00304F  
 Manufacturer: Generic  
 Hardware version: 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	999999999999

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

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



Press Commit to reboot device.

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

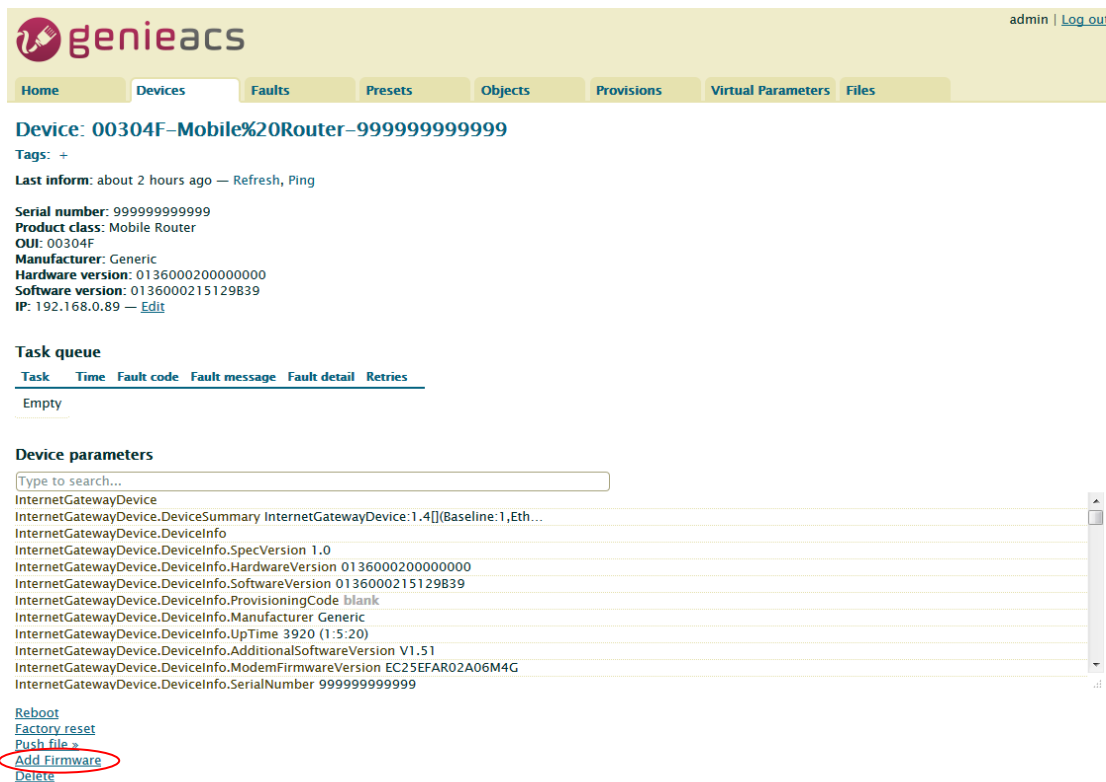
## 6) Reset to default

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

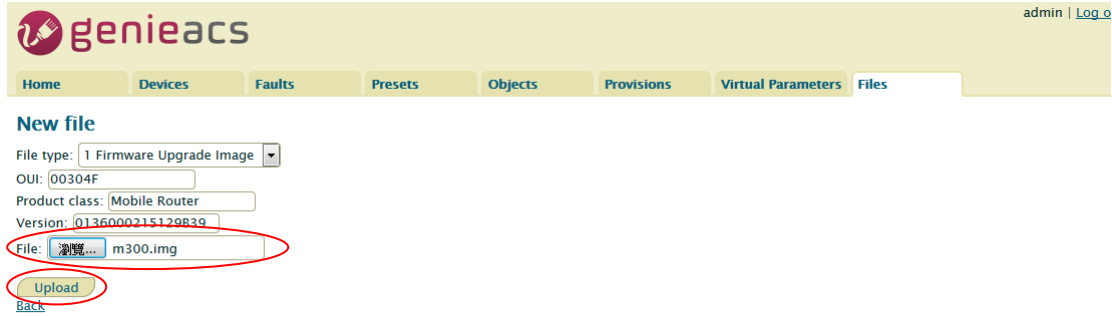
## 7) Firmware Upgrade

### 7.1) Upload Firmware

Press [Add Firmware](#) link



The link will redirect to Files tab

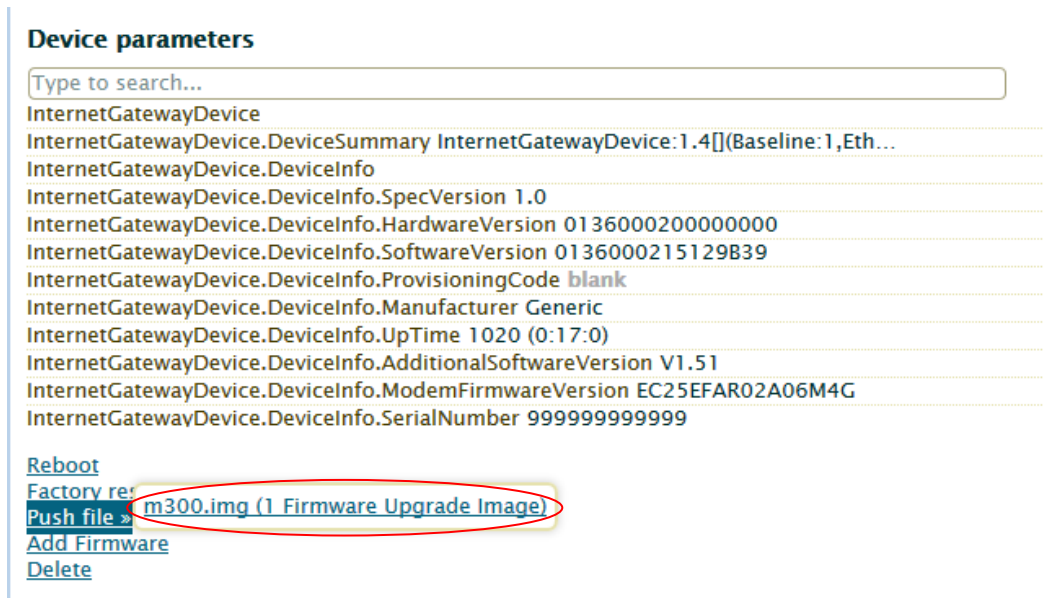


Press File: browse button, select the firmware, and then press Upload button.  
The firmware will be added to listing files as below.

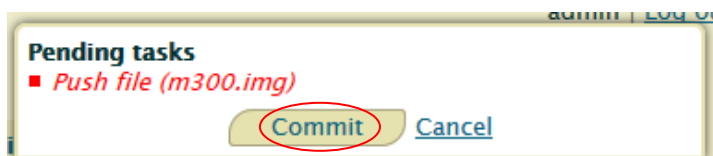


## 7.2) Upgrade

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



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



Press Commit, then firmware upgrade started.

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



## 17.1 VLAN Topology



This VLAN Topology for **2-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

VLAN Isolation  Off  On

Enable	Subnet	VID	Port		
			LAN	LAN2	Router
<input checked="" type="checkbox"/>	NET1	1	<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 type="checkbox"/>	NET3	3	<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 type="checkbox"/>	NET5	5	<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 type="checkbox"/>	NET7	7	<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"/>
PVID			1	1	1
Tag Mode			Trunk	Trunk	Trunk

## Note:

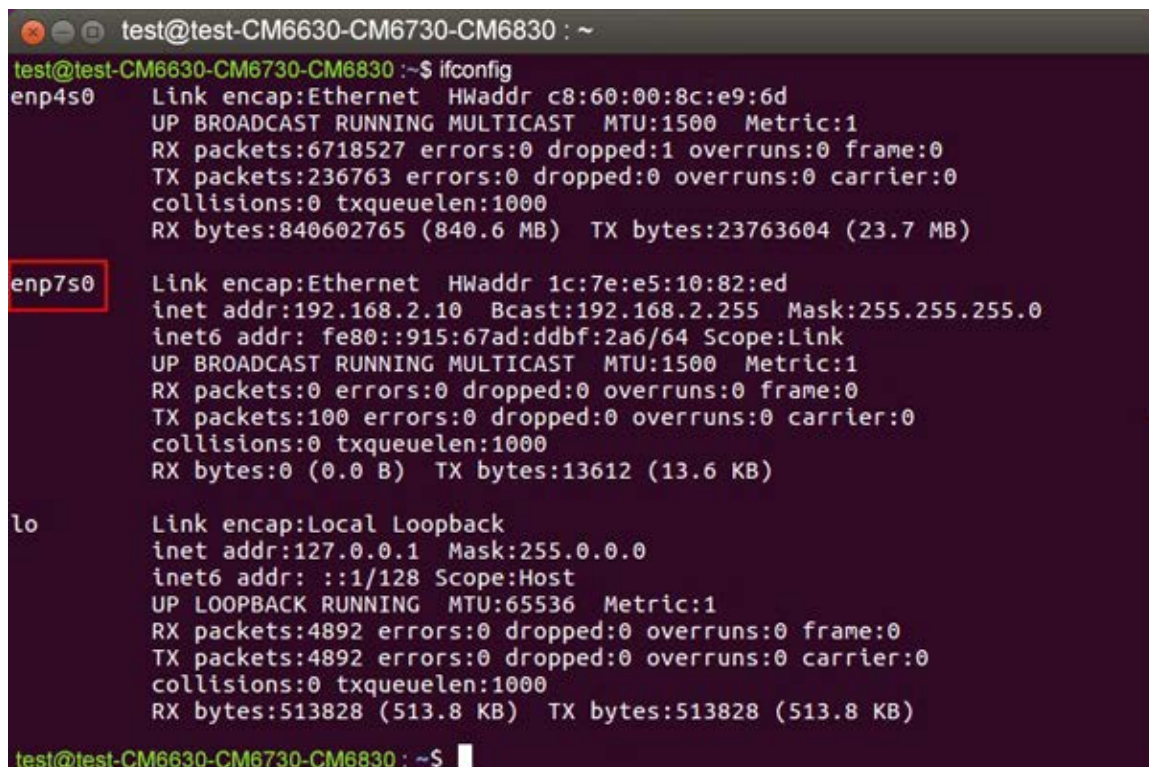
- Different PCs have different interface of network cards, like PC-A network card is eth1.10 for example 1 and PC-B network card is eth1.20 for example 2.
- How to find out the terminal and the interface of network cards based on different PCs.
  - From the following picture, you can click *the finding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



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



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



There are two examples to explain how configure VLAN settings.

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

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

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

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

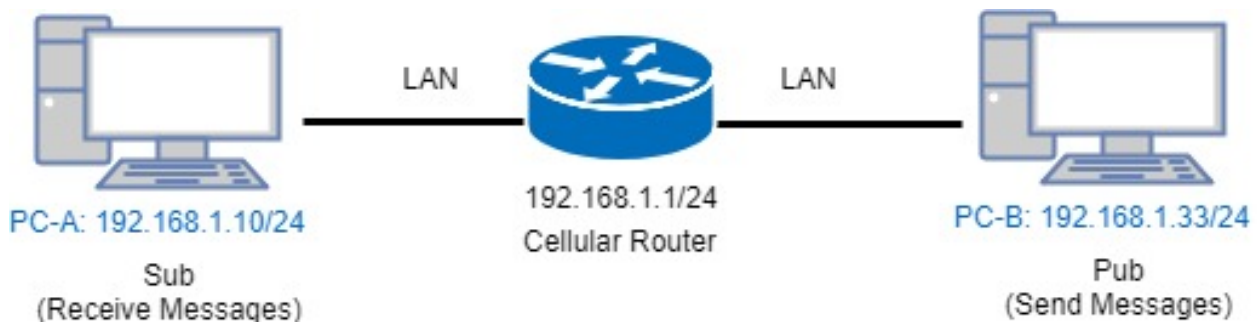
**Example 2: PC-A ping PC-B (Trunk to Access)**

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

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

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

## 17.2 MQTT Topology



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

Expect Result:

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

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

There is a process to explain the steps and result.

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

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

```

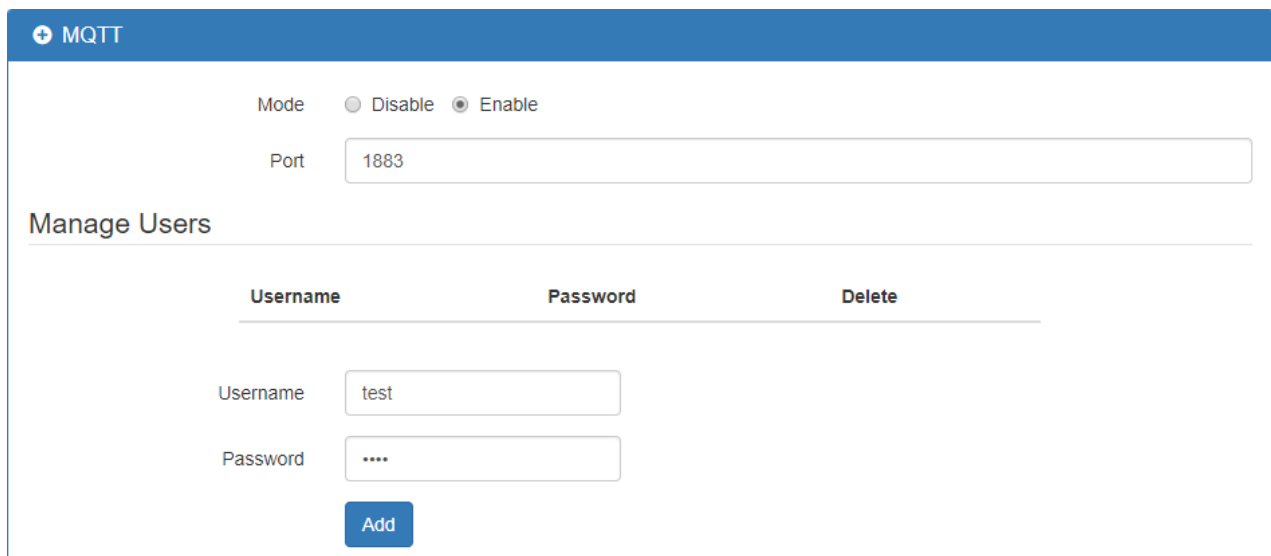
test@test: ~
test@test:~$ sudo apt-get install mosquitto-clients
sudo: unable to resolve host test
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  geopip-database-extra javascript-common libjs-openlayers libnghttp2-14
  libnl-route-3-200 libqgsttools-p1 libqt5multimedia5-plugins
  libqt5multimediamultimedia5 libsmi2ldbl libssh-gcrypt-4 libwireshark-data
  libwiretap6 libwscodexs1 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 amd64 1.10.0-3ubuntu0.2 [34.1 kB]
Get:2 http://tw.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 libmosquitto1 amd64 1.4.8-1ubuntu0.16.04.2 [31.3 kB]
Fetched 65.3 kB in 0s (201 kB/s)
Selecting previously unselected package libc-ares2:amd64.
(Reading database ... 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.



The image shows a web interface for MQTT configuration. At the top, there is a blue header with a plus icon and the text "MQTT". Below the header, there are two radio buttons for "Mode": "Disable" and "Enable", with "Enable" selected. A "Port" input field contains the value "1883". Below this is a section titled "Manage Users" with a horizontal line separator. Underneath, there are three columns: "Username", "Password", and "Delete". The "Username" field contains "test", and the "Password" field contains four dots. A blue "Add" button is positioned below the password field.

**+ MQTT**

Mode  Disable  Enable

Port

---

**Manage Users**

Username	Password	Delete
<input type="text" value="test"/>	<input type="password" value="...."/>	<input checked="" type="checkbox"/>

Username

Password

**+ MQTT**

Mode  Disable  Enable

Port

---

**Manage Users**

Username	Password	Delete
<input type="text" value="test"/>	<input type="password" value="...."/>	<input checked="" type="checkbox"/>
<input type="text" value="test2"/>	<input type="password" value="....."/>	<input checked="" type="checkbox"/>

Username

Password

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

## ACLs

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

## ACLs

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

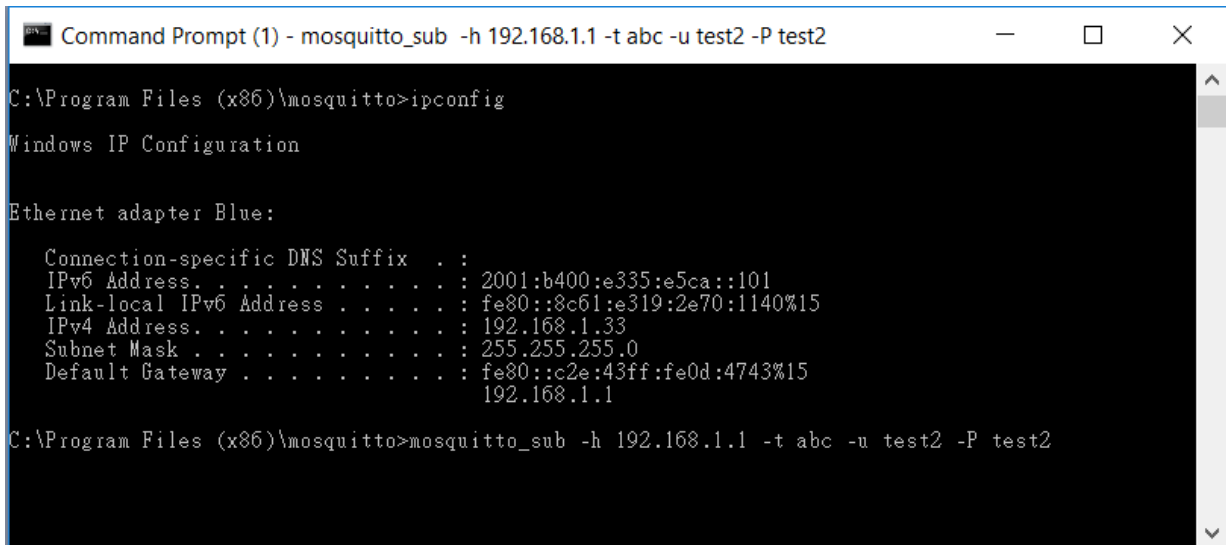
### Note:

- For Receive message command format:  
Mosquitto\_sub -h <M300 IP> -t <Topic> -u <username> -P <password>
- For Send message command format:  
Mosquitto\_pub -h <M300 IP> -t <Topic> -u <username> -P <password> -m <message>

- Step3: There are two test MQTT examples.

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

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



```

Command Prompt (1) - mosquitto_sub -h 192.168.1.1 -t abc -u test2 -P test2
C:\Program Files (x86)\mosquitto>ipconfig

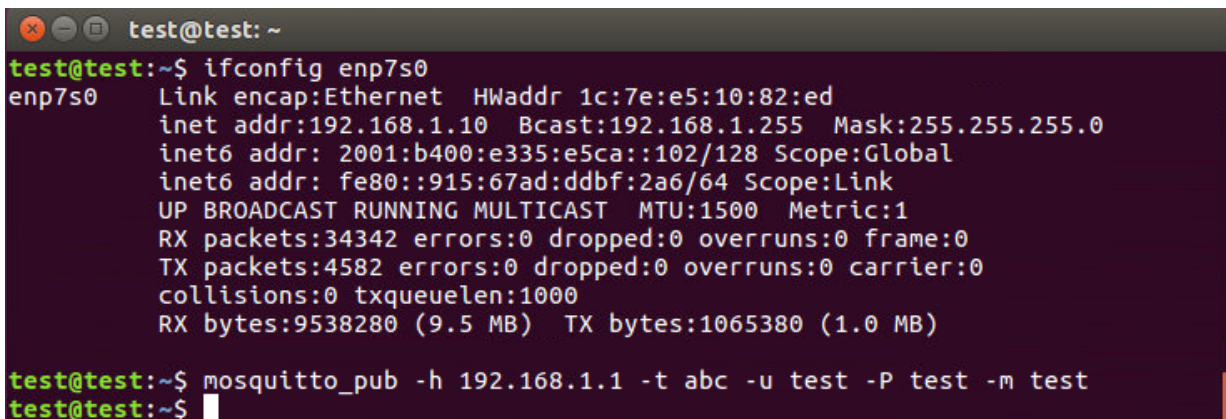
Windows IP Configuration

Ethernet adapter Blue:

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

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

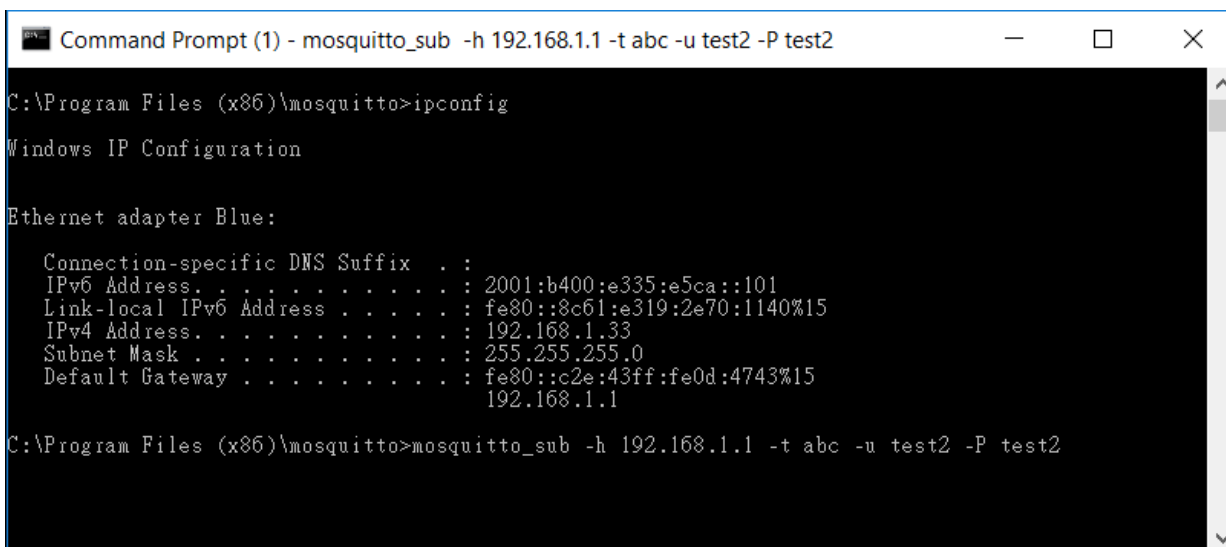
For PC-A, command "mosquitto\_pub -h 192.168.1.1 -t abc -u test -P test -m test" and confirm the message on PC-B. It won't receive any message on PC-B.



```

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

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



```

Command Prompt (1) - mosquitto_sub -h 192.168.1.1 -t abc -u test2 -P test2
C:\Program Files (x86)\mosquitto>ipconfig

Windows IP Configuration

Ethernet adapter Blue:

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

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

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

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



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

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

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

```
Command Prompt (1)
C:\Program Files (x86)\mosquitto>ipconfig

Windows IP Configuration

Ethernet adapter Blue:

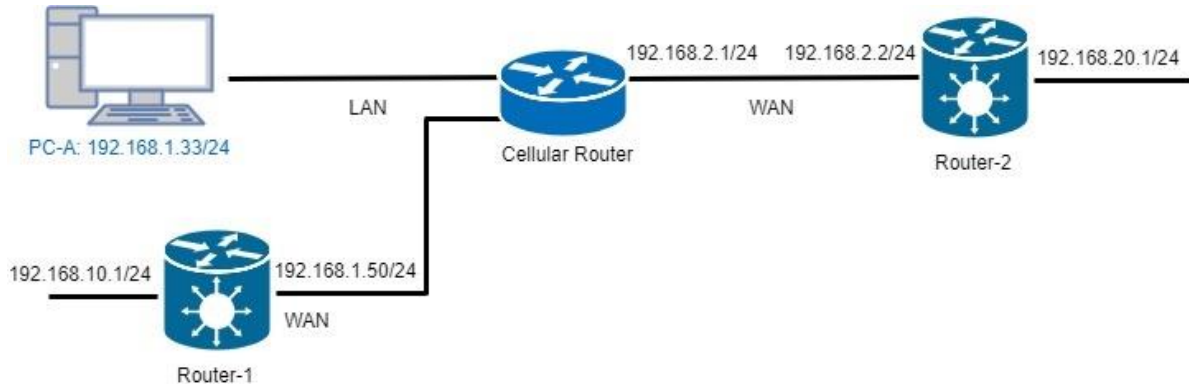
    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:b400:e335:e5ca::101
    Link-local IPv6 Address . . . . . : fe80::8c61:e319:2e70:1140%15
    IPv4 Address. . . . . : 192.168.1.33
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::c2e:43ff:fe0d:4743%15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

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

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

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

## 17.3 IP Routing Topology



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

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

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

- LAN configuration:

⇌ LAN IPv4

IP Address

IP Mask

### DHCP Server Configuration

DHCP Server Configuration

IP Address Pool From  To

Apply

- WAN configuration:

⇌ WAN Ethernet

Work As  DHCP Client  PPPoE Client  Static IPv4

Configuration Ethernet Ping Health

### Static IPv4 Configuration

IP Address

IP Mask

Gateway Address

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
Mode <input type="radio"/> Off <input checked="" type="radio"/> On  Name <input style="width: 150px;" type="text" value="lan side"/>  Destination <input style="width: 150px;" type="text" value="192.168.10.1"/>  Gateway <input style="width: 150px;" type="text" value="192.168.1.50"/>  Interface <input style="width: 150px;" type="text" value="&lt;empty&gt;"/>					

**Static Route**

Mode  Off  On

Settings
Status

Mode	Name	Destination	Gateway	Interface	Delete
<input type="radio"/> Off <input checked="" type="radio"/> On	<input style="width: 150px;" type="text" value="lan side"/>	192.168.10.1	192.168.1.50		<input style="background-color: red; color: white; padding: 2px 5px; border: none;" type="button" value="x"/>

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

```

Command Prompt (1)

Ethernet adapter Blue:

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

C:\tools>ping 192.168.1.50

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

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

C:\tools>ping 192.168.10.1

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

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

C:\tools>

```

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

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

✕
Static Route

Mode  Off  On

Settings


Status

Mode	Name	Destination	Gateway	Interface	Delete
Mode <input type="radio"/> Off <input checked="" type="radio"/> On	Name <input style="width: 150px;" type="text" value="wan side"/>	Destination <input style="width: 150px;" type="text" value="192.168.20.1"/>	Gateway <input style="width: 150px;" type="text" value="192.168.2.2"/>	Interface <input style="width: 150px;" type="text" value="WAN Ethernet"/>	<input type="button" value="Add"/>

Static Route

Mode  Off  On

Settings Status

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

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

```
Command Prompt (1)
Ethernet adapter Blue:

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

C:\tools>ping 192.168.2.2

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

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

C:\tools>ping 192.168.20.1

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

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

C:\tools>
```