

Industrial 4G LTE Cellular Router

M330 / M330-W

User Manual

Version 1.1.8

Table of Contents

1	Introduction.....	6
1.1	Features.....	6
1.2	Specifications.....	7
1.3	Mechanical Dimensions (M330-W).....	8
1.4	Ordering Information	8
2	Hardware Installation.....	8
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
3	Configuration via Web Browser.....	14
3.1	Access the Web Configurator	14
3.2	Navigate the Web Configurator	15
4	Status.....	16
4.1	Status > GPS	20
5	Configuration > System.....	20
5.1	System > Time and Date	20
5.2	System > Logging	24
5.2.1	Logging > Logging.....	24
5.2.2	Logging > Log.....	25
5.3	System > Alarm.....	26
5.3.1	Alarm > Contacts > Create and name the Group.....	27
5.3.2	Alarm > Contacts > Add User	29
5.3.3	Alarm > Duty Schedule.....	30
5.4	System > Ethernet Ports	30
5.5	System > Client List	32
6	Configuration > WAN	32
6.1	WAN > Priority.....	32
6.2	WAN > Ethernet	33
6.2.1	WAN Ethernet Configuration.....	33
6.2.2	Ethernet Ping Health	36
6.3	WAN > IPv6 DNS	38

7	Configuration > LTE	39
7.1	LTE > LTE Config	40
7.1.1	LTE Configuration	40
7.1.2	LTE Ping Health	41
7.2	LTE > GPS Config	41
7.3	LTE > Dual APN	43
7.4	LTE > Usage Display	46
7.5	LTE > SMS	51
7.6	LTE > Serving Cell	53
7.7	LTE > DNS	54
8	Configuration > WiFi (M330-W)	55
8.1	WiFi > WiFi Config	55
8.2	WiFi > MAC Filter	56
8.3	WiFi > Client List	57
9	Configuration > LAN	58
9.1	LAN > IPv4	58
9.2	LAN > IPv6	59
9.3	LAN > VLAN	59
9.4	LAN > Subnet	61
10	IP Routing	62
10.1	IP Routing > Static Route	62
10.2	IP Routing > RIP	65
10.3	IP Routing > OSPF	67
10.4	IP Routing > BGP	70
11	Configuration > VPN	73
11.1	VPN > Open VPN	73
11.1.1	Open VPN Common Setting	74
11.1.2	Open VPN Client Setting	75
11.1.3	Open VPN Server Setting	76
11.1.4	Set up Open VPN Custom	78
11.2	VPN > IPsec	80
11.2.1	IPsec > Connections	80
11.2.2	IPsec > Authentication IDs	84
11.2.3	IPsec > X.509 Certificates	85
11.2.4	IPsec > CA Certificates	86
11.2.5	IPsec > Net-to-Net Configuration	88
11.3	VPN > GRE	103
11.4	VPN > PPTP Server	104
11.5	VPN > L2TP	106
12	Configuration > Firewall	110
12.1	Firewall > Basic Rules	110

12.2	Firewall > Port Forwarding	111
12.3	Firewall > DMZ	112
12.4	Firewall > IP Filter	113
12.5	Firewall > MAC Filter	117
12.6	Firewall > URL Filter	118
12.7	Firewall > NAT	119
12.8	Firewall > IPS	120
13	Configuration > Service	121
13.1	Service > SNMP	121
13.1.1	Community	121
13.1.2	SNMP v3 User Configuration	122
13.1.3	SNMP trap configuration	123
13.2	Service > TR069	124
13.3	Service > Dynamic DNS	125
13.4	Service > VRRP	127
13.5	Service > MQTT	127
13.6	Service > UPnP	130
13.7	Service > SMTP	130
13.8	Service > IP Alias	131
14	Configuration > Management	132
14.1	Management > Identification	132
14.2	Management > Administration	133
14.3	Management > Contacts / On Duty	134
14.3.1	Contacts	134
14.3.2	Duty Schedule	134
14.4	Management > SSH	135
14.5	Management > Firmware	136
14.6	Management > Configuration	136
14.7	Management > Load Factory	136
14.8	Management > Restart	137
15	Configuration > Diagnosis	137
15.1	Diagnosis > Ping	137
15.2	Diagnosis > Traceroute	138
16	Configuration Applications	139
16.1	WAN Priority	139
16.2	LAN > IPv4/IPv6 Dual Stack	141
16.3	MQTT Broker	143
16.4	Alarm Configuration	144
16.5	Open VPN Configuration	146
16.5.1	Open VPN Server Mode	146
16.5.2	Open VPN Client Mode	147
16.5.3	Open VPN Net-to-Net	148

16.5.4	Open VPN 1:1 NAT	151
16.5.5	Open VPN with third-party server	152
16.5.6	Install Open VPN Access Server on Docker	154
16.5.7	Install Pritunl Open VPN server on Docker	159
16.6	VRRP Topology	167
16.7	TR069 Server (GenieACS Installation)	167
17	Test Case Example.....	177
17.1	VLAN Topology	177
17.2	MQTT Topology	180
17.3	IP Routing Topology	186

1 Introduction

M330 and M330-W, 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 **M330** and **M330-W** are simple to configure and collect real-time data transmission quickly for Industrial IoT and machine-to-machine applications. The **M330-W** is also compliant with IEEE 802.11b/g/n Wi-Fi connectivity.

Featuring VPN Tunnels, Firewall, TR069, and SNMP Trap, **M330 and M330-W 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.

M330 and M330-W 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 (M330-W Model)
- Built-in micro SIM connector, RS232 serial port, and DI/DO interfaces
- Integrated detachable antenna against radio interference
- LED indicators for connection and data transmission status
- Industrial rated from -30 to +70°C for use in harsh environments
- IPv6/IPv4 dual stack and all applications are IPv6 ready
- Support serial communication protocols for rich connectivity
- Enhance security and encryption for authentication and transmission

1.2 Specifications

Cellular Interface

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

Wi-Fi Interface (M330-W Model)

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

Hardware Interface

- High Performance 550 MHz SoC with 128MByte Flash
- 1 x Micro SIM Connector (push-push type)
- 1 x LAN 10/100 Mbps Ethernet port
- 1 x WAN 10/100 Mbps Ethernet port
- WPS / RESET Button
- 1 x RS232 (TXD/RXD/GND)
- 1 x DI (Non-Isolated), 1 x DO (Non-Isolated)
- 2 x SMA connectors for detachable LTE Antenna
- 2 x RP-SMA connectors for detachable Wi-Fi Antenna (M330-W Model)
- 1 x SMA connector for detachable GPS antenna

Physical Characteristics

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

LED Display

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

Power Supply

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

Software

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

Management Software

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

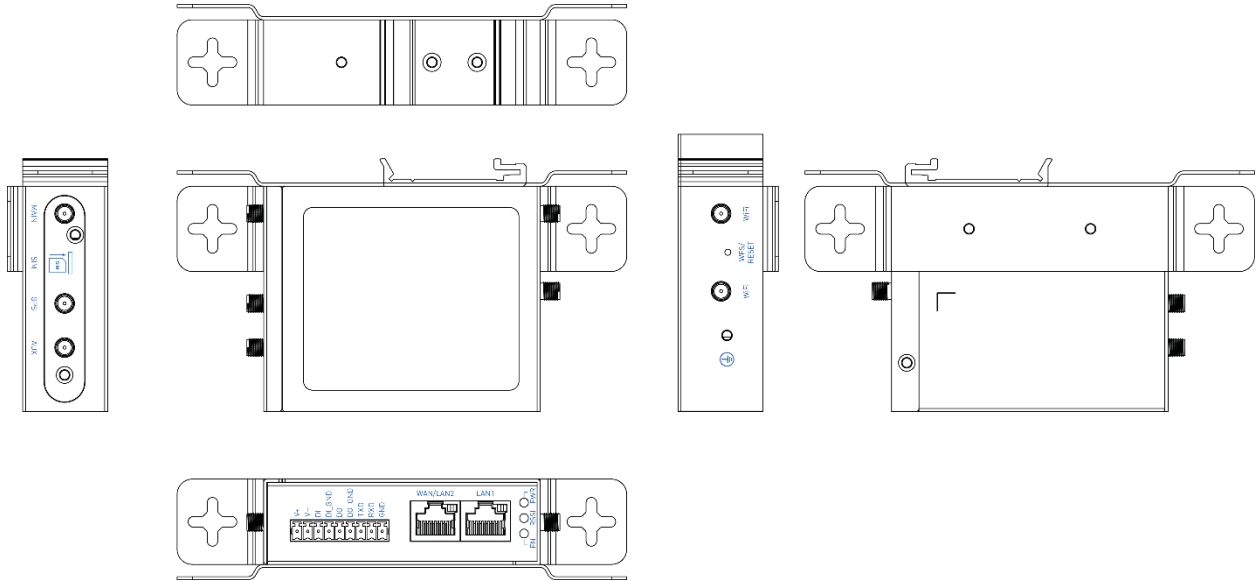
Environment

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

Standards and Certifications

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

1.3 Mechanical Dimensions (M330-W)



1.4 Ordering Information

Model Name	Description
M330	Compact Industrial 4G LTE Cellular Router (1 x WAN, 1 x LAN, 1 x RS232 , 1 x DI, 1 x DO, 1 x micro SIM Slot, GPSx1, -30 ~ +70°C)
M330-W	Compact Industrial Wi-Fi 4G LTE Cellular Router (1 x WAN, 1 x LAN, 1 x RS232 , 1 x DI, 1 x DO, 1 x micro SIM Slot, GPSx1, Wi-Fi, -30 ~ +70°C)

2 Hardware Installation

This chapter introduces how to install and connect the hardware.

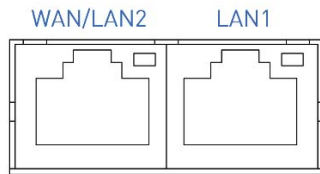
2.1 LED Indicators



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

2.2 Ethernet Port

(1) 10/100 Mbps Ethernet LAN/WAN



The LAN and WAN interface are standard RJ45 connectors.

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

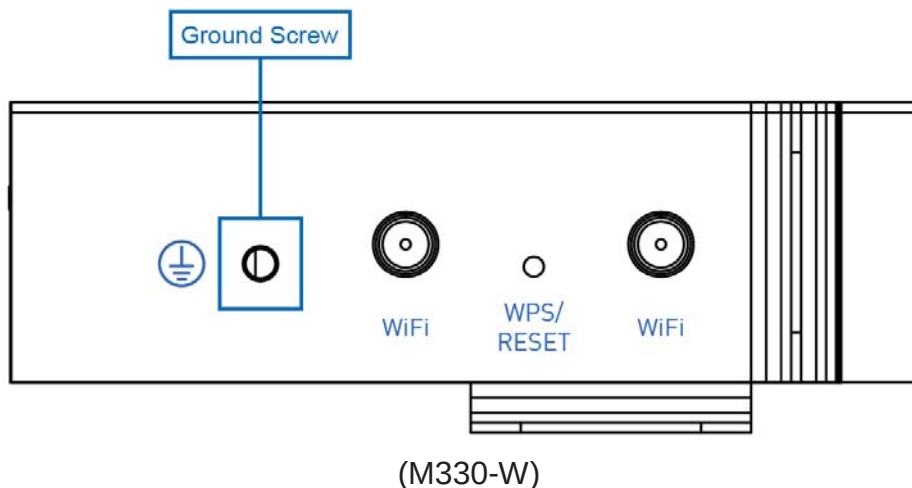
(2) LED Indicator of Ethernet Port

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

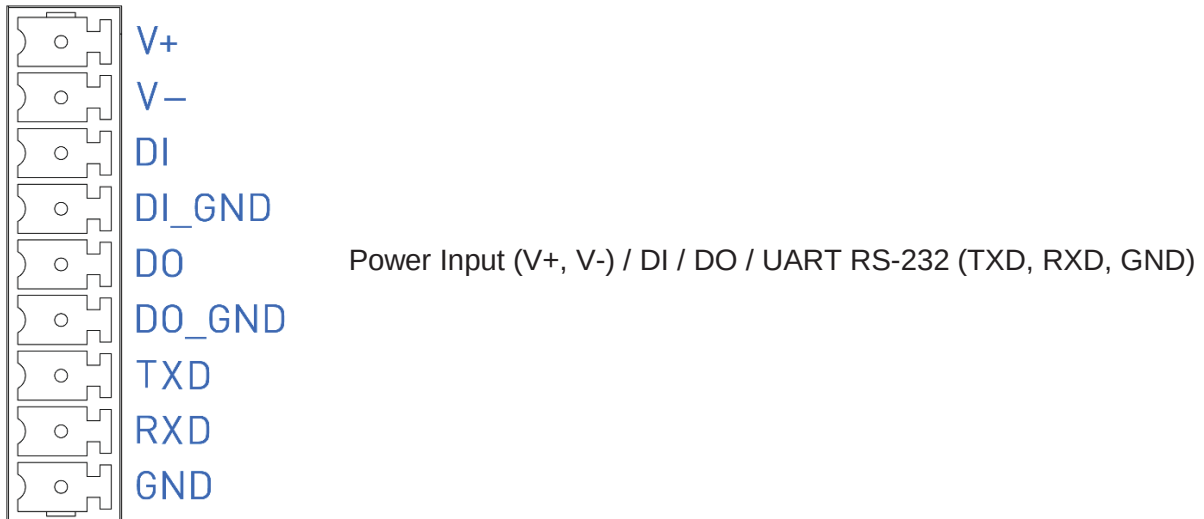
LED	Status	Description
Green (Link/ACT)	Off	Connection is down.
	Blink	Data is being transmitted.
	On	Connection is up.

2.3 Grounding the Router

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

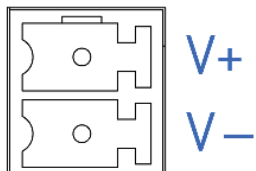


2.4 Pin Assignments



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

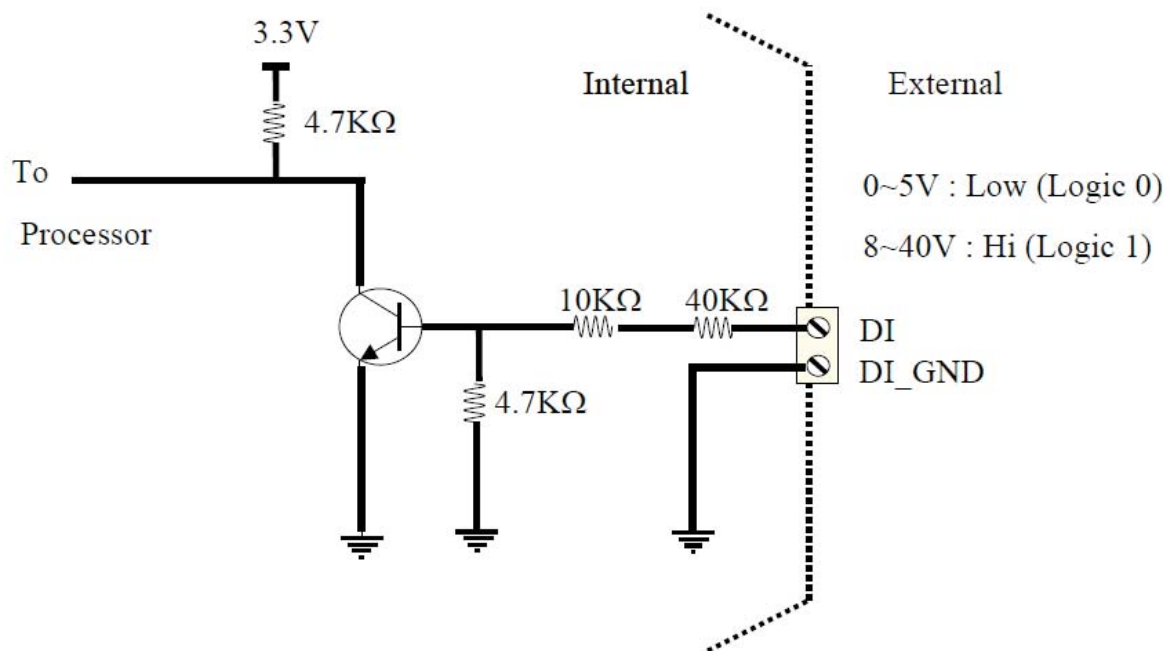
2.6 Connecting I/O Ports

(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)

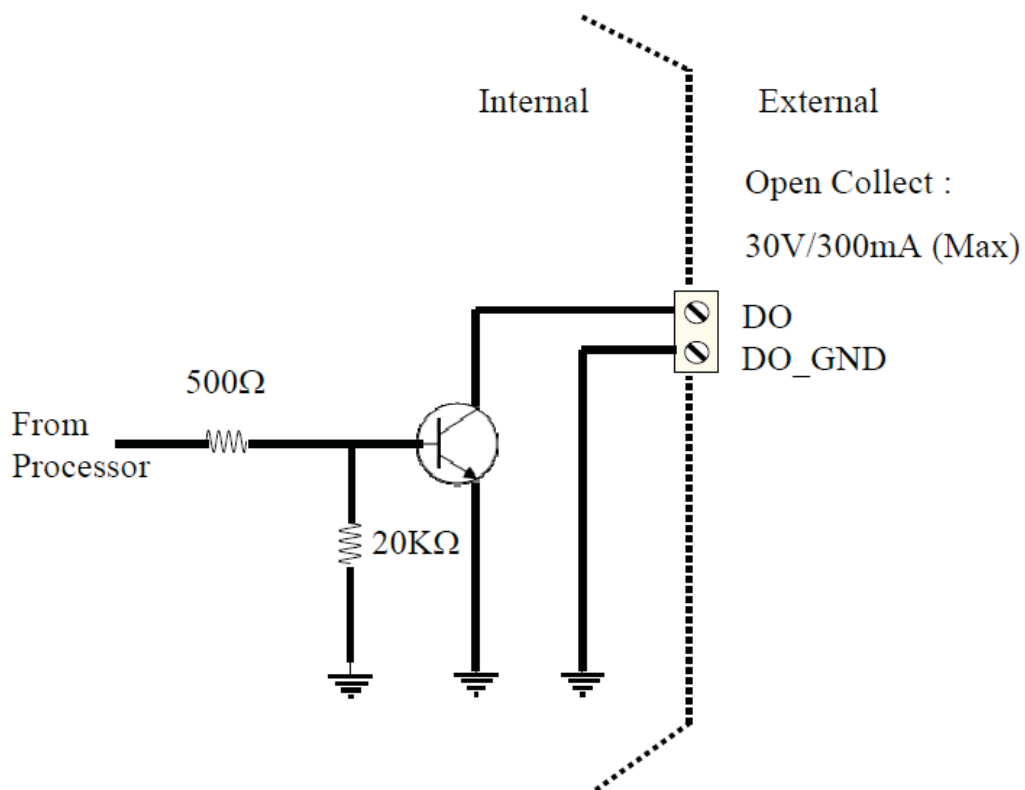


(2) Digital Output (DO)

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

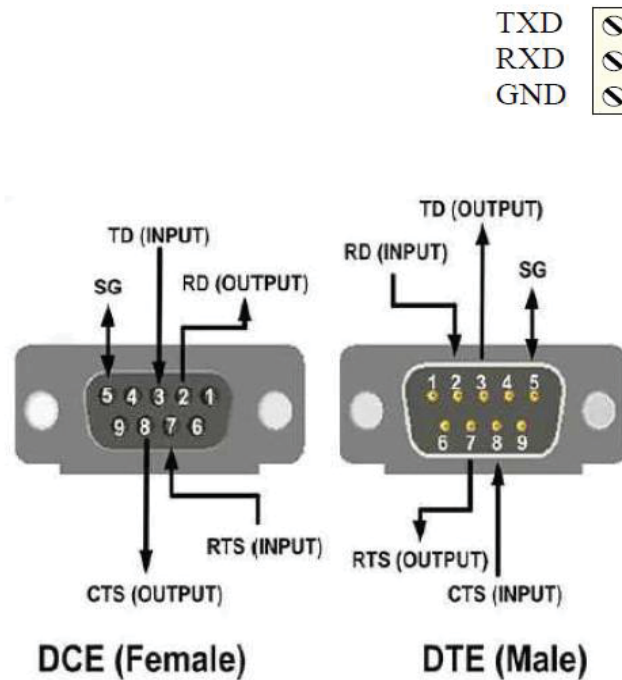
Pin	Description
DO	Digital Output
DO_GND	

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



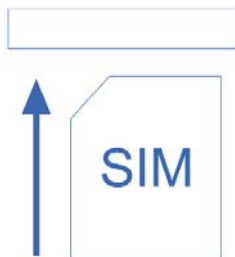
2.7 UART (RS-232)

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

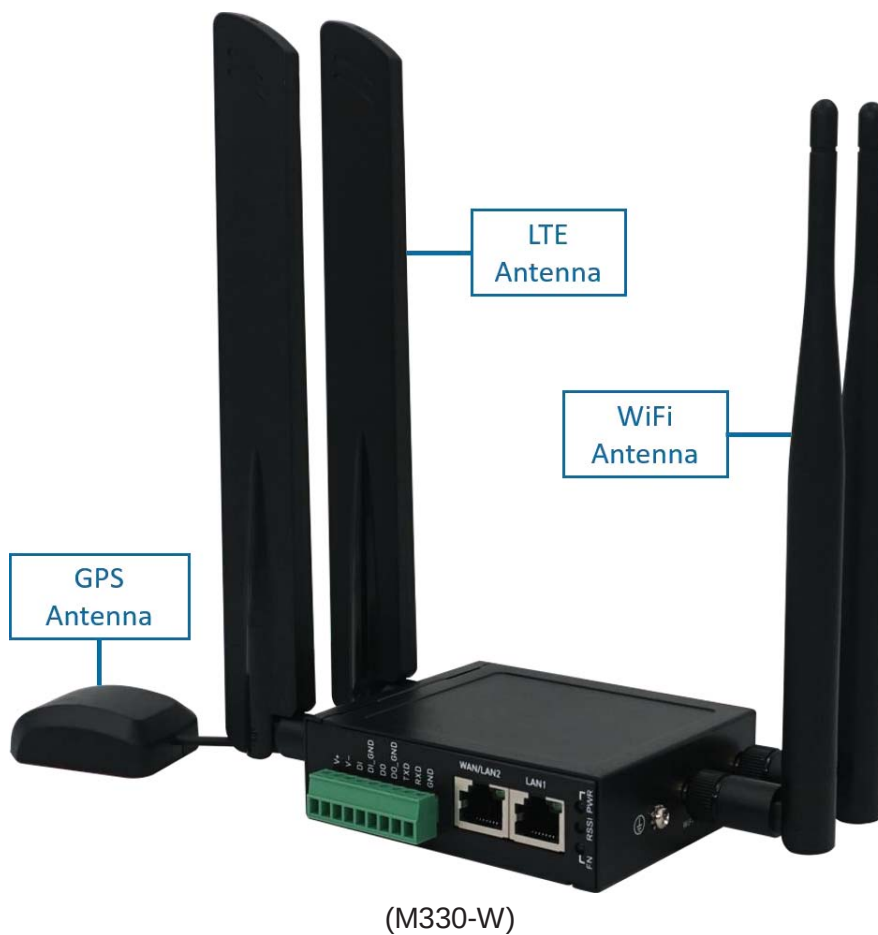


WPS/ RESET

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

2.10 External Antenna

Each unit has three antenna connectors, MAIN, GPS, AUX (SMA). For M330-W, there will be five antenna connectors and extra two antennas for Wi-Fi (RP-SMA). Connect the antenna to MAIN when you have only one antenna. Please tighten the connecting nut properly to ensure good connection.



3 Configuration via Web Browser

3.1 Access the Web Configurator

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

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

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

Title Bar Panel > Selecting Language

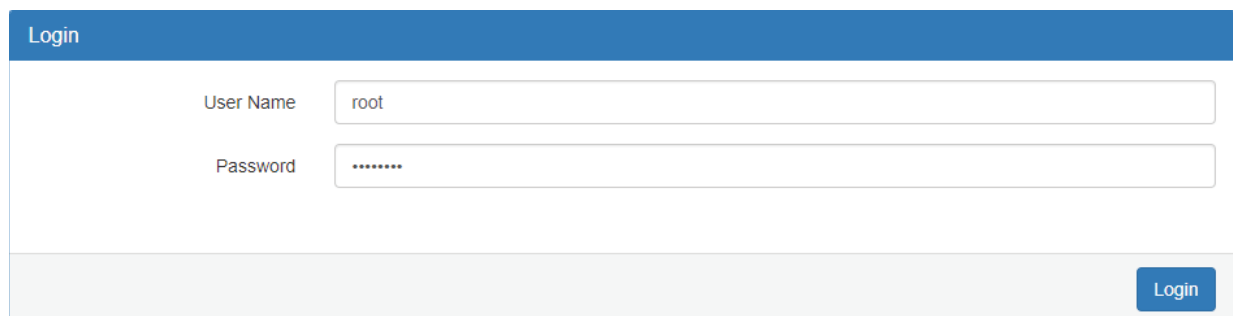
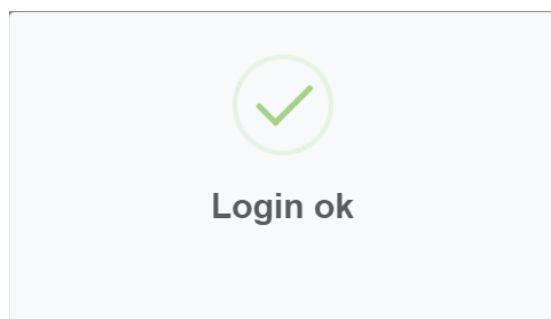
You can choose the languages, including English and Taiwan.



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.

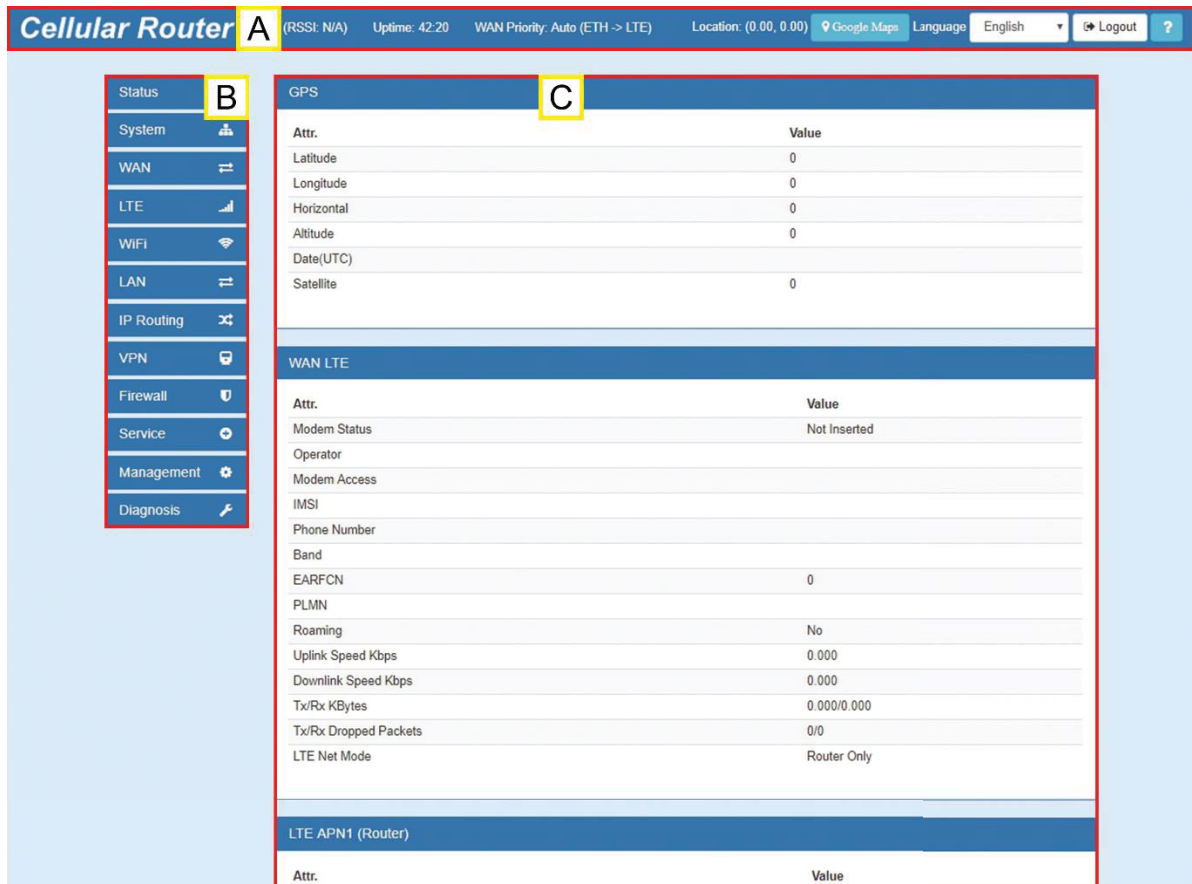
A screenshot of the router's login page. It has a blue header with the word 'Login'. Below the header, there are two input fields: 'User Name' containing the text 'root' and 'Password' containing seven dots. A blue 'Login' button is located at the bottom right of the form area.

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

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

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

(3) **C** : Main Window

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

4 Status

When you enter the web browser in the beginning and have not log in, the first item of main menu shows your status that you are a guest. This status only can view status page without any permission to log in. The interface of main window displays the status of router to show about information, including Cellular Attribute, 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	● Add/Delete/Modify all users' accounts except Super User. ● Read/Write Configuration	Read/Write Configuration	only Read Configuration	N/A

Cellular Router

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

Status

System

WAN

LTE

WiFi

LAN

IP Routing

VPN

Firewall

Service

Management

Diagnosis

GPS

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

WAN LTE

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

LTE APN1 (Router)

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

LTE APN1 DNS

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

WAN Ethernet

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

LAN Ethernet

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

Connected VPN Connections

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

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

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

Status > LTE APN1 / LTE APN2	
Item	Description
Attribute	
IPv4 Address	Ethernet WAN obtain IPv4 Address.
IPv4 Mask	Ethernet WAN obtain IPv4 Mask.
Default Gateway	Ethernet WAN IPv4 Default Gateway.
Connected	Yes: Connected; No: Disconnected.
IPv4 Conn Time	Ethernet WAN IPv4 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 Droppes Packets	TX/RX Dropped Packets.

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

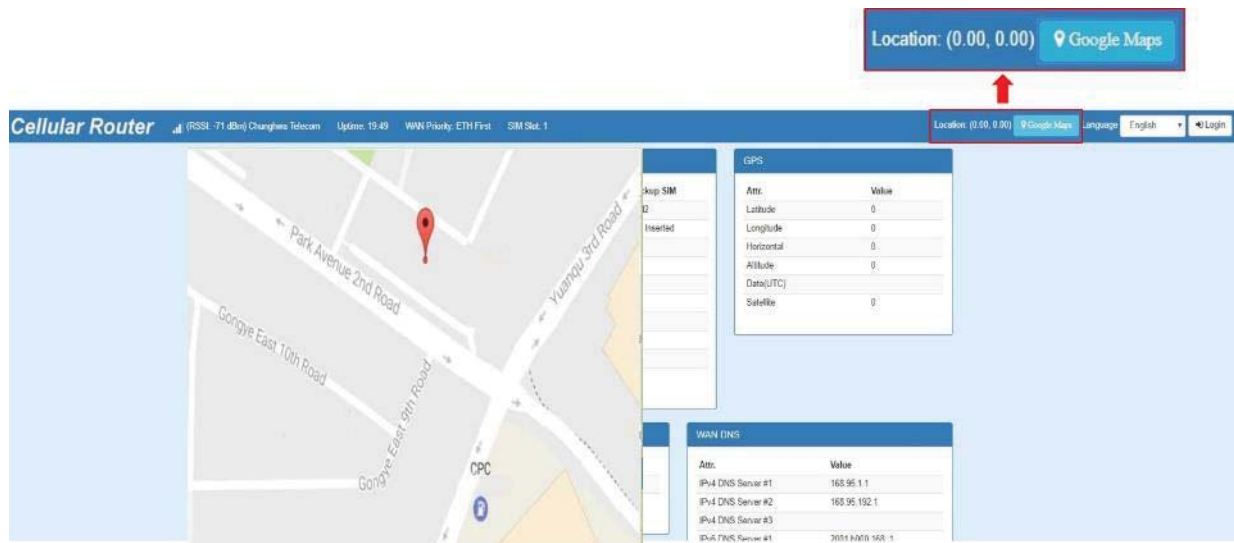
Status > WAN Ethernet	
Item	Description
Attribute	
IPv4 Address	Ethernet WAN obtain IPv4 Address.
IPv4 Mask	Ethernet WAN obtain IPv4 Mask.
Default Gateway	Ethernet WAN IPv4 Default Gateway.
IPv6 Conn Time	Ethernet WAN IPv4 Connected Time.

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

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

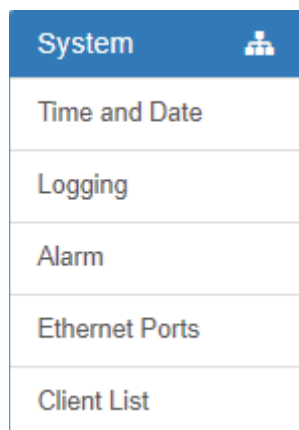
4.1 Status > GPS

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



5 Configuration > System

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



5.1 System > Time and Date

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

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

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

I. Get from Time Server

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

 Time And Date

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

Time and Date Setup

Mode

☐ Manual ☒ Get from Time Server

GPS Time

☐ Off ☒ On

IPv4 Server #1

0.openwrt.pool.ntp.org

IPv4 Server #2

pool.ntp.org

IPv4 Server #3

clock.sjc.he.net

IPv6 Server #1

time-d.nist.gov

IPv6 Server #2

2.pool.ntp.org

IPv6 Server #3

clock.nyc.he.net

Time Zone Setup

Time Zone

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

Daylight Savings

☒ Off ☐ On

Ahead of standard time

60

mins

Start Date

3 / 2 / 0

(Month / Week / Day)

Start Time

2 : 0

(Hour : Minute)

End Date

11 / 2 / 0

(Month / Week / Day)

End Time

2 : 0

(Hour : Minute)

Time Server

Server Mode

☒ Off ☐ On

Server Port

123

Apply

II. Manual

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

 Time And Date

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

Time and Date Setup

Mode ☒ Manual ☐ Get from Time Server

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

Time Zone Setup

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

Daylight Savings ☒ Off ☐ On

Ahead of standard time 60 mins

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

Start Time 2 : 0 (Hour : Minute)

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

End Time 2 : 0 (Hour : Minute)

Time Server

Server Mode ☒ Off ☐ On

Server Port 123

Apply

III. Time Zone Setup

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

Time Zone Setup

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

Daylight Savings ☐ Off ☒ On

Ahead of standard time 60 mins

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

Start Time 2 : 0 (Hour : Minute)

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

End Time 2 : 0 (Hour : Minute)

System > Time 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	Time to enter Daylight Savings duration. The Month range is 1~12. <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> The Week range is 1~5. ● 1 - first week in month. ● 2 - second week in month ● 3 - third week in month ● 4 - fourth week in month ● 5- fifth week in month The Day range is 0~6. 0 - Sunday (The start day of a week) 1- Monday 2 - Tuesday 3 - Wednesday 4 - Thursday 5 - Friday 6 - Saturday The Hour range is 0~23. The Min range is 0~59.	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 > Logging

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

5.2.1 Logging > Logging

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

 Logging

Mode

☐ Disable ☒ Enable

Remote Log

☒ Disable ☐ Enable

Log Server Address

Apply

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

5.2.2 Logging > Log

This section displays all data status.

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

 Log

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

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

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

5.3 System > Alarm

This section allows you to configure the alarm.

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

Note:

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

System > Alarm	
Item	Description
Mode	Turn on/off the Alarm configuration. Select from Disable or Enable. The default is Enable.
Alarm Input	Select from SMS, DI 1, DI 2, VPN disconnect and WAN disconnect as input to trigger alarm. • SMS: It means on duty team members on Contacts / On Duty can send SMS to the phone number of using SIM card to trigger alarm. • DI: IO to trigger alarm. • VPN disconnect: All tunnels get disconnected then trigger alarm. • WAN disconnect: WAN connections get disconnected then trigger alarm. • LAN disconnect: LAN connection get disconnected then trigger alarm. • Reboot: Reboot then trigger alarm.
Alarm Output	Select from SMS, DO, SNMP trap and E-mail as alarm output.
DI 1 / 2 Trigger	Select from High or Low. The default is High Trigger.

	• High: SW is On to trigger. • Low: SW is OFF to trigger.
DO behavior	• Always: Pull DO high. • Pulse: High and Low continuously. • Pulse Time Length: Pulse time length (mini seconds).
SMS/E-mail	Write your messages and limit 150 English characters for the messages to deliver.

5.3.1 Alarm > Contacts > Create and name the Group

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

Alarm

Mode ☒ Disable ☐ Enable

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

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

DI 1 Trigger ☒ High ☐ Low

DO behavior ☒ Always ☐ Pulse

SMS/E-mail

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

Apply

Contacts / On Duty

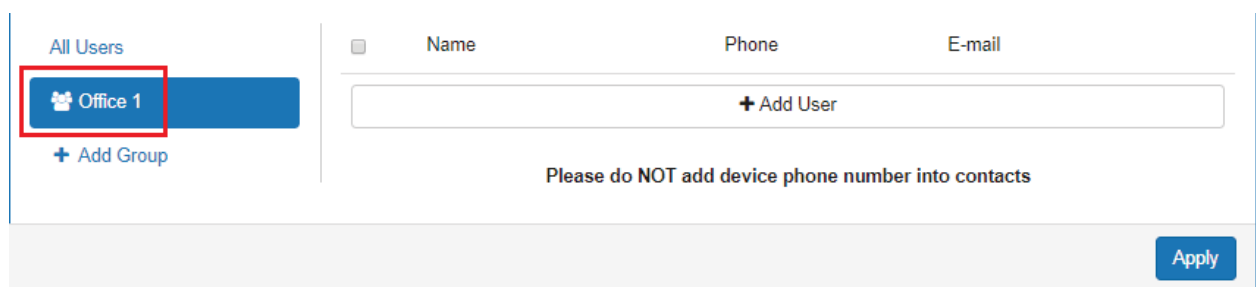
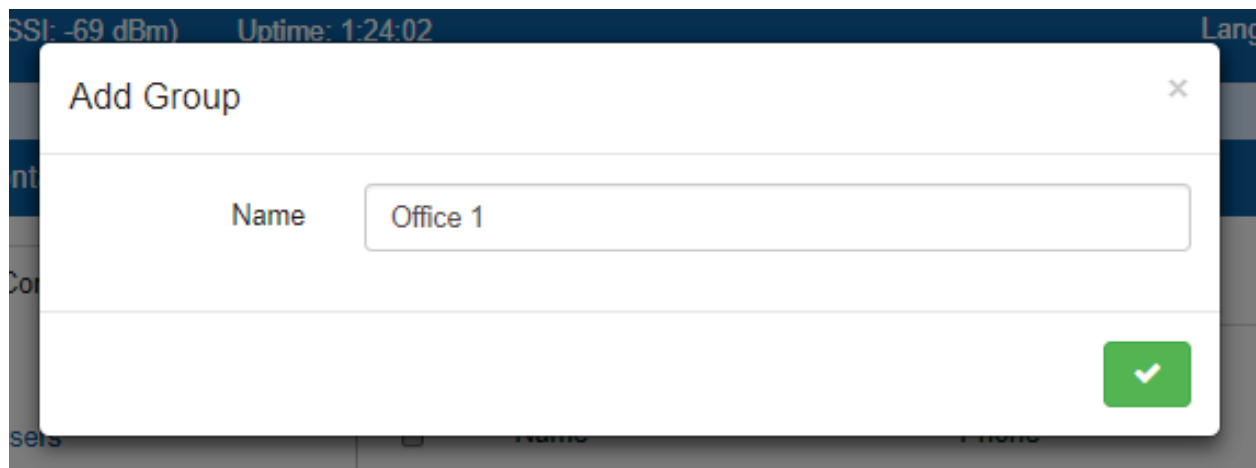
Contacts Duty Schedule

All Users **+ Add Group**

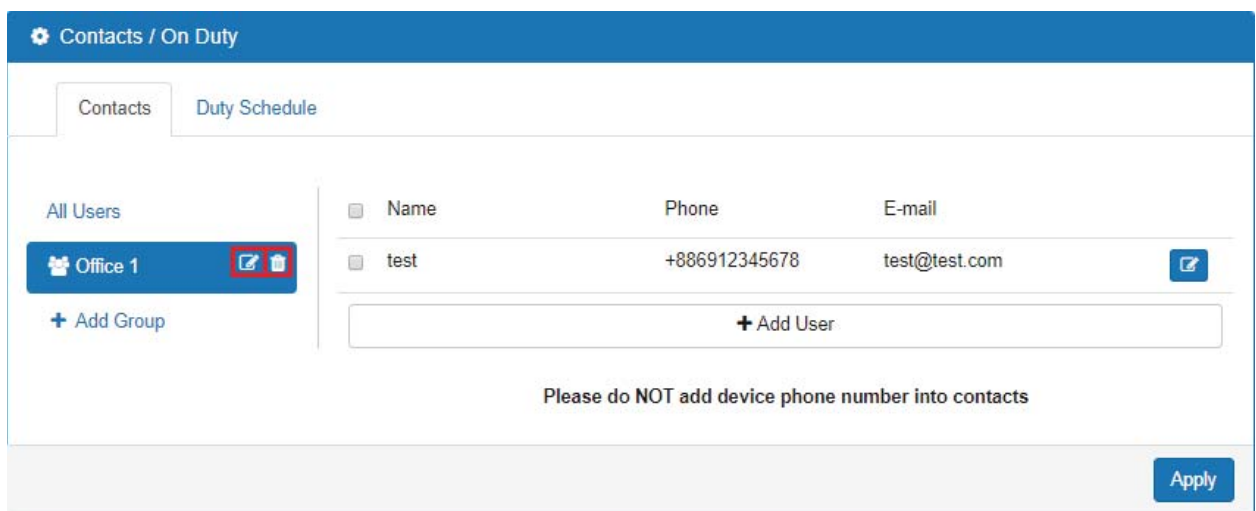
Name	Phone	E-mail
+ Add User		

Please do NOT add device phone number into contacts

Apply



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



5.3.2 Alarm > Contacts > Add User

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

Contacts / On Duty

Contacts Duty Schedule

All Users

Office 1

+ Add Group

Name	Phone	E-mail
+ Add User		

Please do NOT add device phone number into contacts

Apply

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

Add User

Name test

Phone +886912345678

E-mail test@test.com

Groups

Office 1

Please do NOT add device phone number into contacts



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

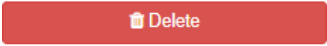
All Users

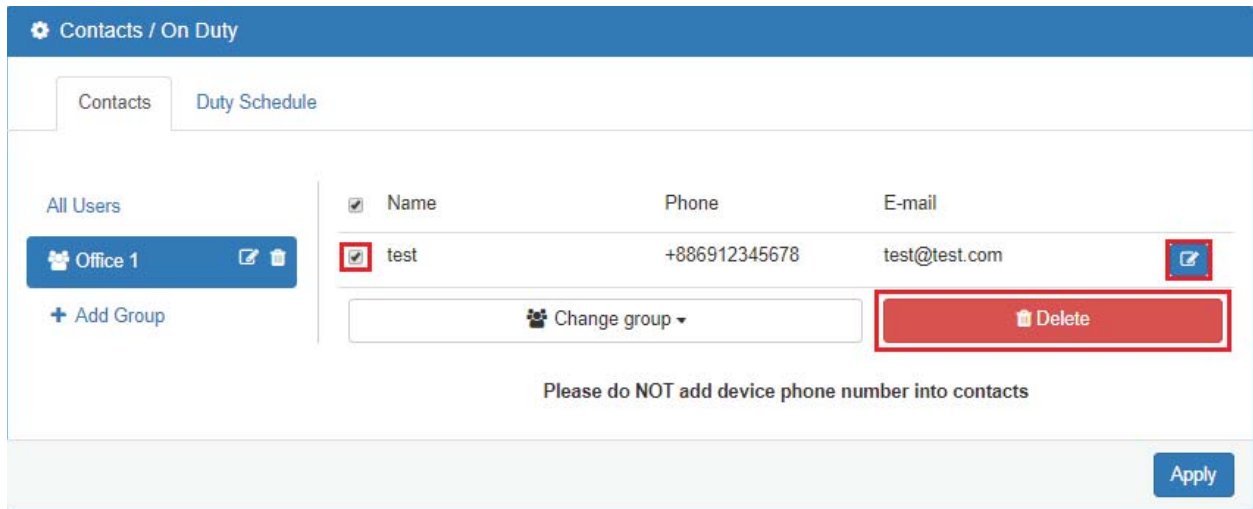
Office 1

+ Add Group

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

Please do NOT add device phone number into contacts

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



Contacts / On Duty

Contacts Duty Schedule

All Users

Office 1

+ Add Group

☒	Name	Phone	E-mail	
☒	test	+886912345678	test@test.com	

Change group

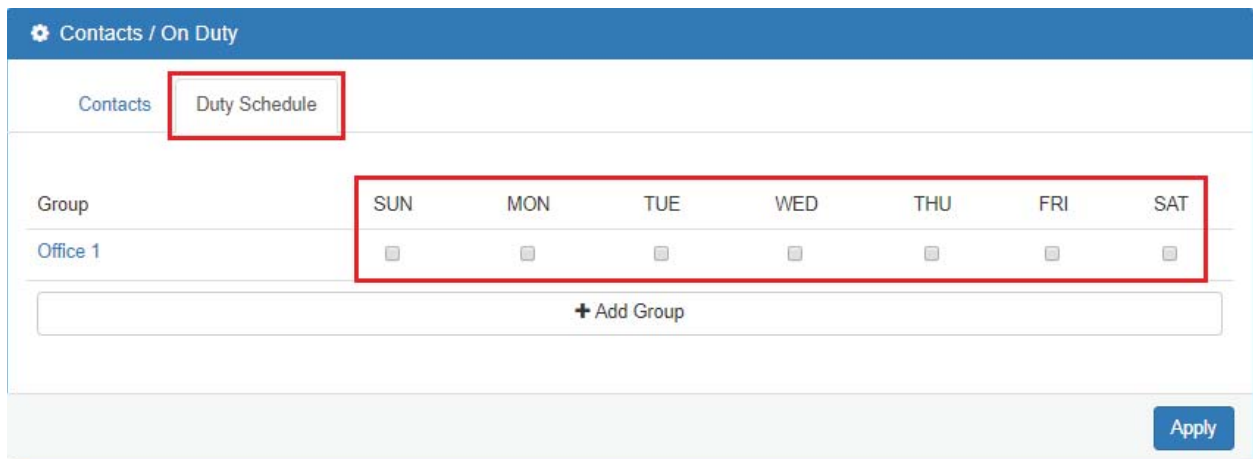
Delete

Please do NOT add device phone number into contacts

Apply

5.3.3 Alarm > Duty Schedule

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



Contacts / On Duty

Contacts Duty Schedule

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

+ Add Group

Apply

5.4 System > Ethernet Ports

This section allows you to configure the Ethernet.

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

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

Ethernet

Ethernet Ports Status

LAN

100M Full

WAN

Off

Ethernet Ports Configurations

LAN

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

5.5 System > Client List

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

Client List					
List Type		☐ DHCP Client	☐ Online		
#	IP Address	MAC Address	Hostname	Start	End
1	192.168.1.19	00:e0:4c:68:21:73			

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

6 Configuration > WAN

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

WAN
Priority
Ethernet
IPv6 DNS

6.1 WAN > Priority

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

Priority	
WAN Priority	Auto (ETH -> LTE)
Hint	Auto (ETH -> LTE) LTE Only ETH Only
Apply	

Priority

WAN Priority

LTE Only

LTE Net Mode

Bridge + Router

Bridge Only

☒ Router Only

Dual Router

Hint

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

Apply

WAN > Priority	
Item	Description
Priority	Auto (ETH -> LTE): WAN Ethernet is first priority and the second priority is LTE. LTE Only: The priority is only LTE. ETH Only: The priority is only WAN Ethernet.
LTE Net Mode (The priority is LTE Only)	Bridge + Router: APN1 act as bridge for internet access. APN2 act as router for management from WAN site which like TR069, ssh... Bridge Only: APN1 act as bridge for internet access. Router Only: APN1 act as router for internet access. Router + Router: APN1 act as router for internet access. APN2 act as router for management from WAN site which like TR069, ssh...

6.2 WAN > Ethernet

6.2.1 WAN Ethernet Configuration

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

WAN Ethernet

Work As

☒ DHCP Client

☐ PPPoE Client

☐ Static IPv4

Configuration

Ethernet Ping Health

DNS Server Configuration

IPv4 DNS Server #1

From ISP

IPv4 DNS Server #2

From ISP

IPv4 DNS Server #3

From ISP

Apply

WAN > Ethernet	
Item	Description
WAN Ethernet	There are three options to obtain the IP of WAN Ethernet. ● DHCP Client: DHCP server-assigned IP address, netmask, gateway, and DNS. ● PPPoE Client: Your ISP will provide you with a username and password. This option is typically used for DSL services. ● Static IPv4: User-defined IP address, netmask, and gateway address.

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

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

WAN Ethernet

Work As
☒ DHCP Client
☐ PPPoE Client
☐ Static IPv4

Configuration
Ethernet Ping Health

DNS Server Configuration

IPv4 DNS Server #1

From ISP
From ISP
User Defined
None

IPv4 DNS Server #2

From ISP
From ISP
User Defined
None

IPv4 DNS Server #3

From ISP
From ISP
User Defined
None

Apply

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

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

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

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

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

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

6.2.2 Ethernet Ping Health

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

WAN Ethernet

Work As
☐ DHCP Client
☐ PPPoE Client
☒ Static IPv4

Configuration
Ethernet Ping Health

Ethernet Ping Health
☐ Disable
☒ Enable

Interval
(1 ~ 60 Seconds)

IPv4 Host 1

IPv4 Host 2

IPv6 Host 1

IPv6 Host 2

Hint

Wan Priority: Auto
Ethernet ping health: Enable

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

Apply

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

In addition, you can check which WAN is actually using from “**Status**” page. The interface will be shown **check mark** (✓ symbol) on the connection title. For IPv6 address, the status will be displayed on LAN Ethernet Interface when IPv6 is using as WAN connection.

WAN LTE

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

✓ WAN Ethernet

Attr.	Value
IPv4 Address	118.167.125.240
IPv4 Mask	255.255.255.255

✓ LAN Ethernet

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

6.3 WAN > IPv6 DNS

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

 IPv6 DNS

APN1 DNS Server Configuration

IPv6 DNS Server #1

From ISP ▼

IPv6 DNS Server #2

From ISP ▼

IPv6 DNS Server #3

From ISP ▼

APN2 DNS Server Configuration

IPv6 DNS Server #1

From ISP ▼

IPv6 DNS Server #2

From ISP ▼

IPv6 DNS Server #3

From ISP ▼

Apply

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

 IPv6 DNS

APN1 DNS Server Configuration

IPv6 DNS Server #1

From ISP ▼

IPv6 DNS Server #2

From ISP
User Defined
None

IPv6 DNS Server #3

From ISP ▼

APN2 DNS Server Configuration

IPv6 DNS Server #1

From ISP ▼

IPv6 DNS Server #2

From ISP ▼

IPv6 DNS Server #3

From ISP ▼

Apply

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

7 Configuration > LTE

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

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

7.1 LTE > LTE Config

7.1.1 LTE Configuration

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

LTE Config

LTE Config

Auto

▼

Change this field require rebooting

MTU

1500

min: 500; max: 1500

LTE Ping Health

LTE Ping Health

☐ Disable ☒ Enable

Interval

60

Seconds

IPv4 Host 1

8.8.8.8

IPv4 Host 2

8.8.4.4

IPv6 Host 1

2001:4860:4860::8888

IPv6 Host 2

2001:4860:4860::8844

Hint

LTE ping health: Enable

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

Apply

LTE Config

LTE Config

Auto

▼

Change this field require rebooting

MTU

4G Only
3G Only
2G Only

min: 500; max: 1500

LTE Ping Health

LTE > LTE Config	
Item	Description
LTE Config	Auto: Automatically connect the possible band. 4G Only: Connect to 4G network only. 3G Only: Connect to 3G network only. 2G Only: Connect to 2G network only.
MTU	MTU is the Maximum Transmission Unit that can be sent over the LTE interface. It allows user to adjust the MTU size to fit into their existing network environment.

7.1.2 LTE Ping Health

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

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

7.2 LTE > GPS Config

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

 GPS Config

Report To

☐ RS232 ☐ LOG

NMEA Type

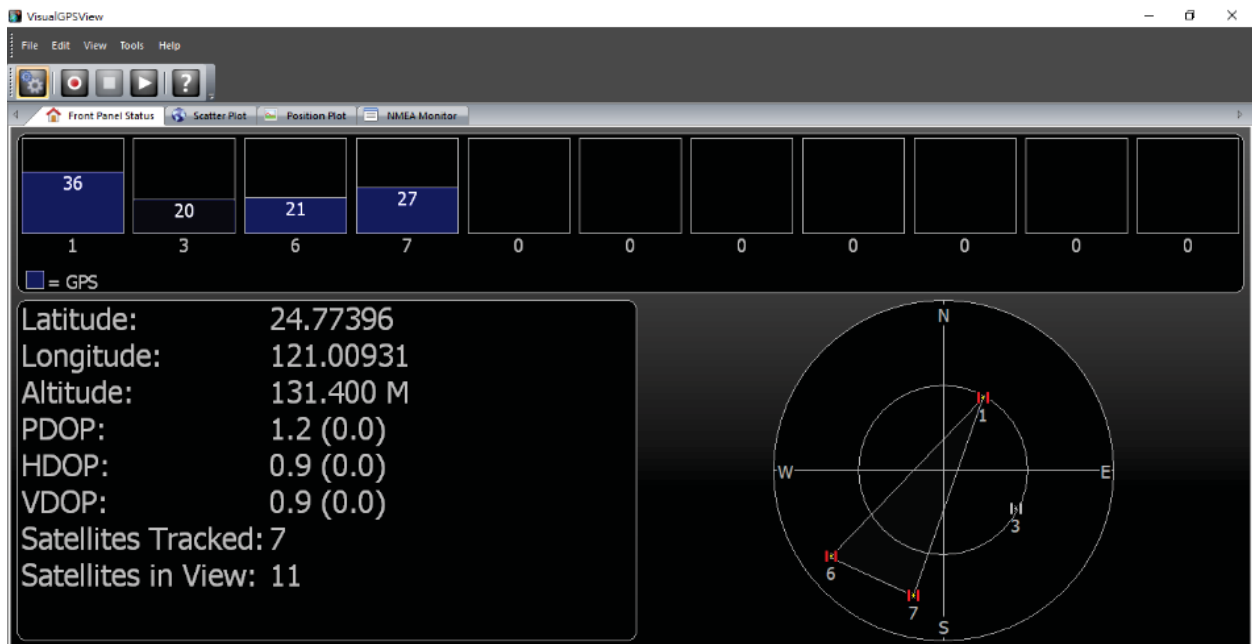
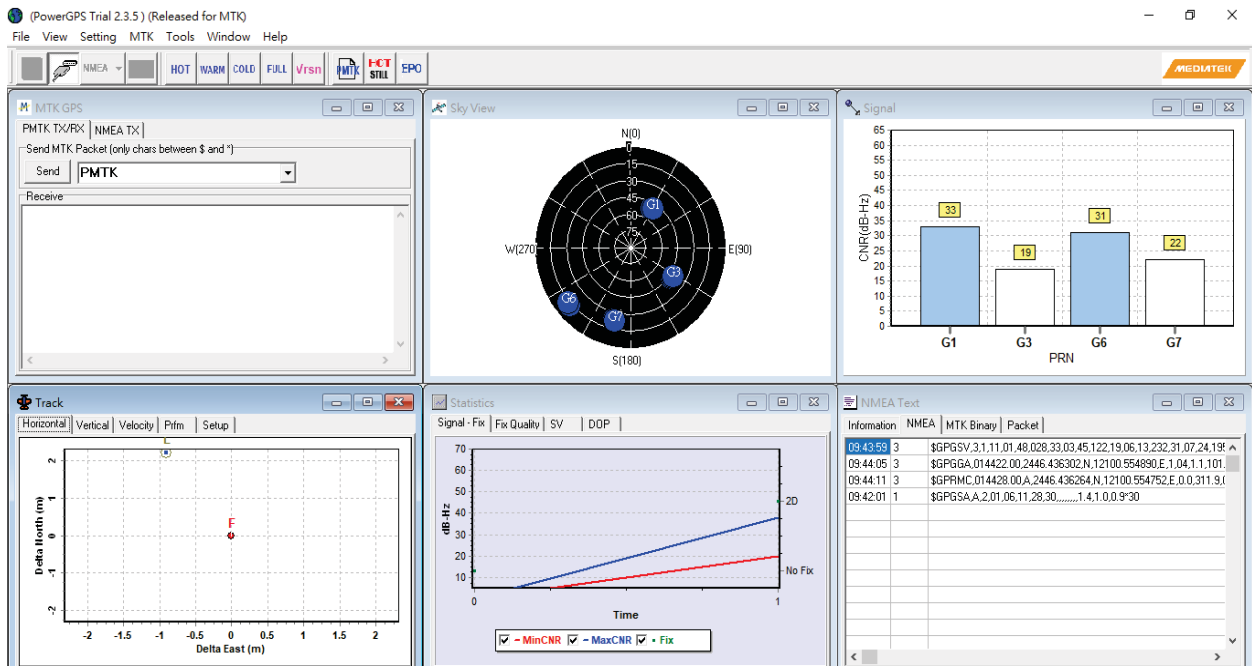
☒ GSV ☒ GGA ☒ RMC ☒ GSA

Apply

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

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

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



7.3 LTE > Dual APN

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

Dual APN

Connect Policy

Connect Action

Connect

Disable Roaming

☐ No ☒ Yes

SIM Configuration

APN1

APN2

Status

Not Inserted

☒ SIM PIN Enable

SIM PIN

Confirmed SIM PIN

SIM PUK

Confirmed SIM PUK

Change SIM PIN

Change

Apply

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

Change

Old PIN

New PIN

PIN Remaining Number

0

PUK Remaining Number

0

Apply

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

LTE > Dual SIM	
Item	Description
Connect Policy	
Connect Action	● Connect: After manually disconnect, it will show Connect button. Click to get connection or reboot the device to make it automatically connect. ● Disconnect: When getting connection, the Disconnect button appear. After manually click Disconnect, the system would not automatically get connection until next reboot.
Disable Roaming	● NO: Make the connection even the device is in roaming state. ● YES: No connection when the device in roaming state.
SIM Configurations	
Status	Display the status of SIM Card.
SIM PIN Enable	● Enable to display SIM PIN setting. ● Disable to hide SIM PIN setting.
SIM PIN	A personal identification number (PIN) for ordinary use to protect your SIM card.
Confirmed SIM PIN	Double confirm SIM PIN.
SIM PUK	If user input the wrong SIM PIN more than 3 times, the user needs another password personal unblocking code (PUK) for PIN unlocking. Please check your operator for forgotten PUK number.
Confirmed SIM PUK	Double confirm SIM PUK.
Change SIM PIN	When you change the SIN PIN, please aware not to exceed the retry number (PIN remaining number and PUN remaining number).
Old PIN	Please input the current SIM PIN.
New PIN	Please input the newly update SIM PIN.

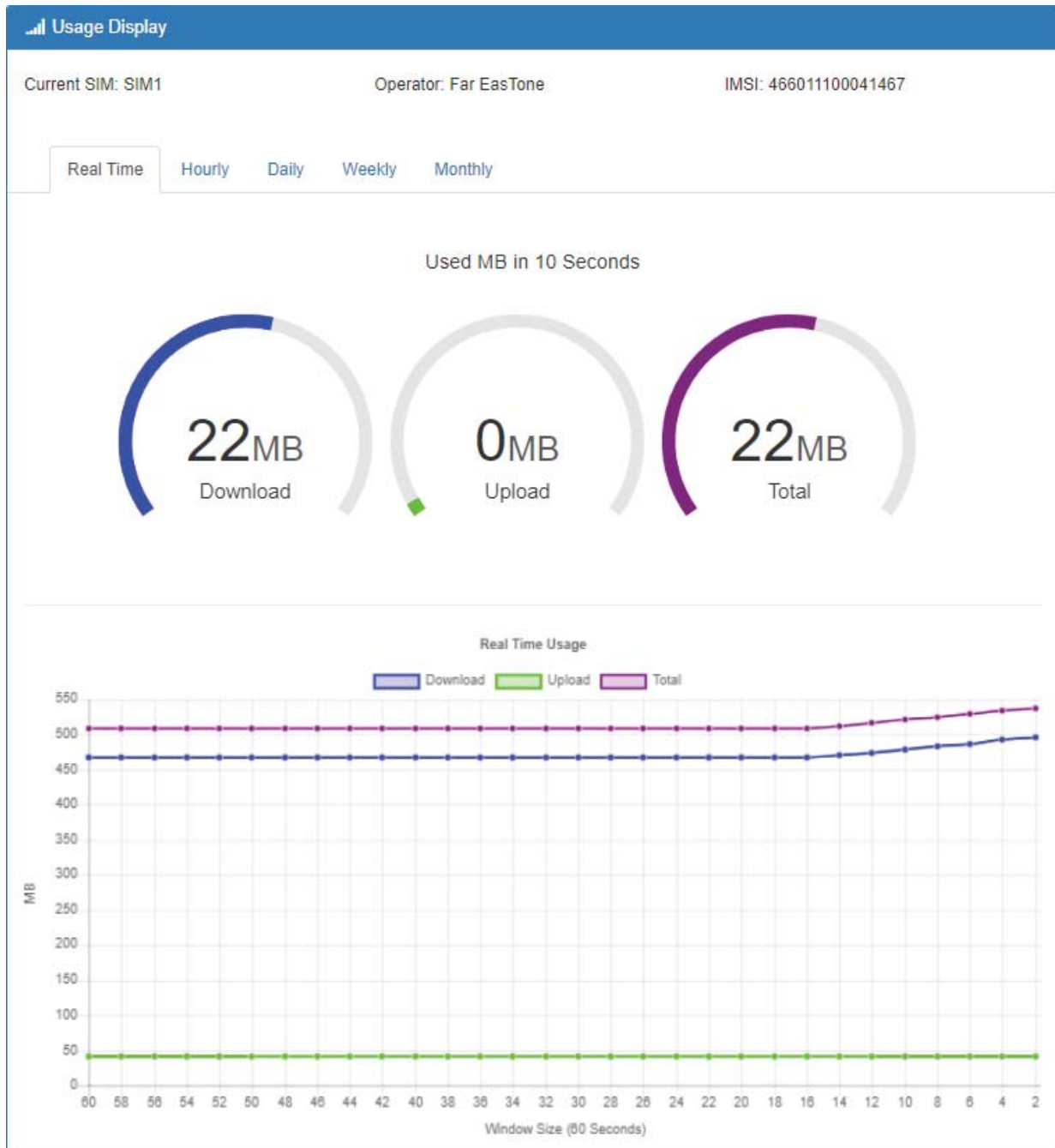
PIN remaining number	Display the allowed remaining PIN retry number.
PUK remaining number	Display the allowed remaining PUK retry number.
APN1 / APN2	
APN	The Access Point Name (APN) is the name of the setting that set up a connection to the gateway between your carrier's cellular network and the public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

7.4 LTE > Usage Display

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

(1) Real-Time Usage:

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



(2) Hourly Usage:

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



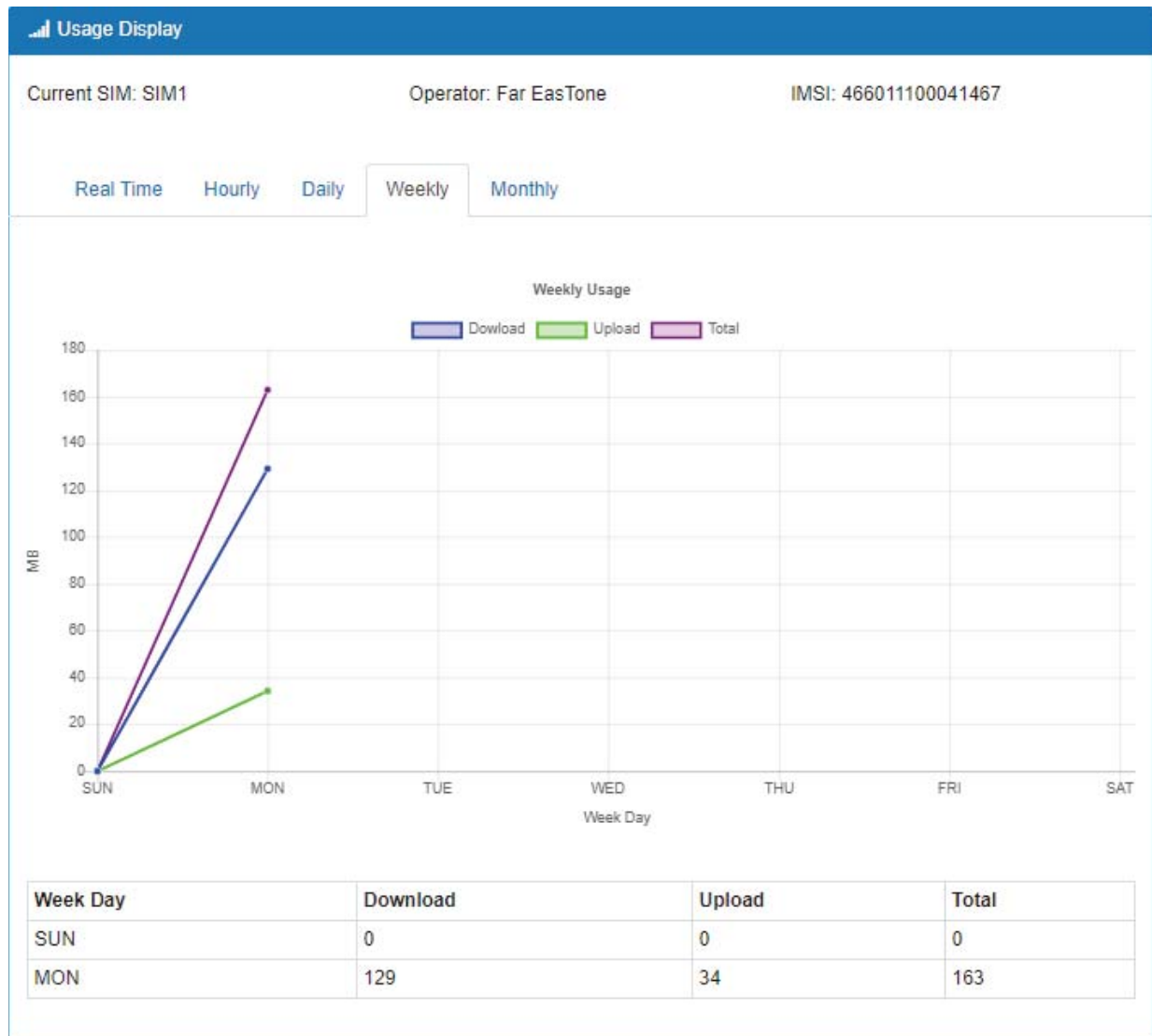
(3) Daily Usage:

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



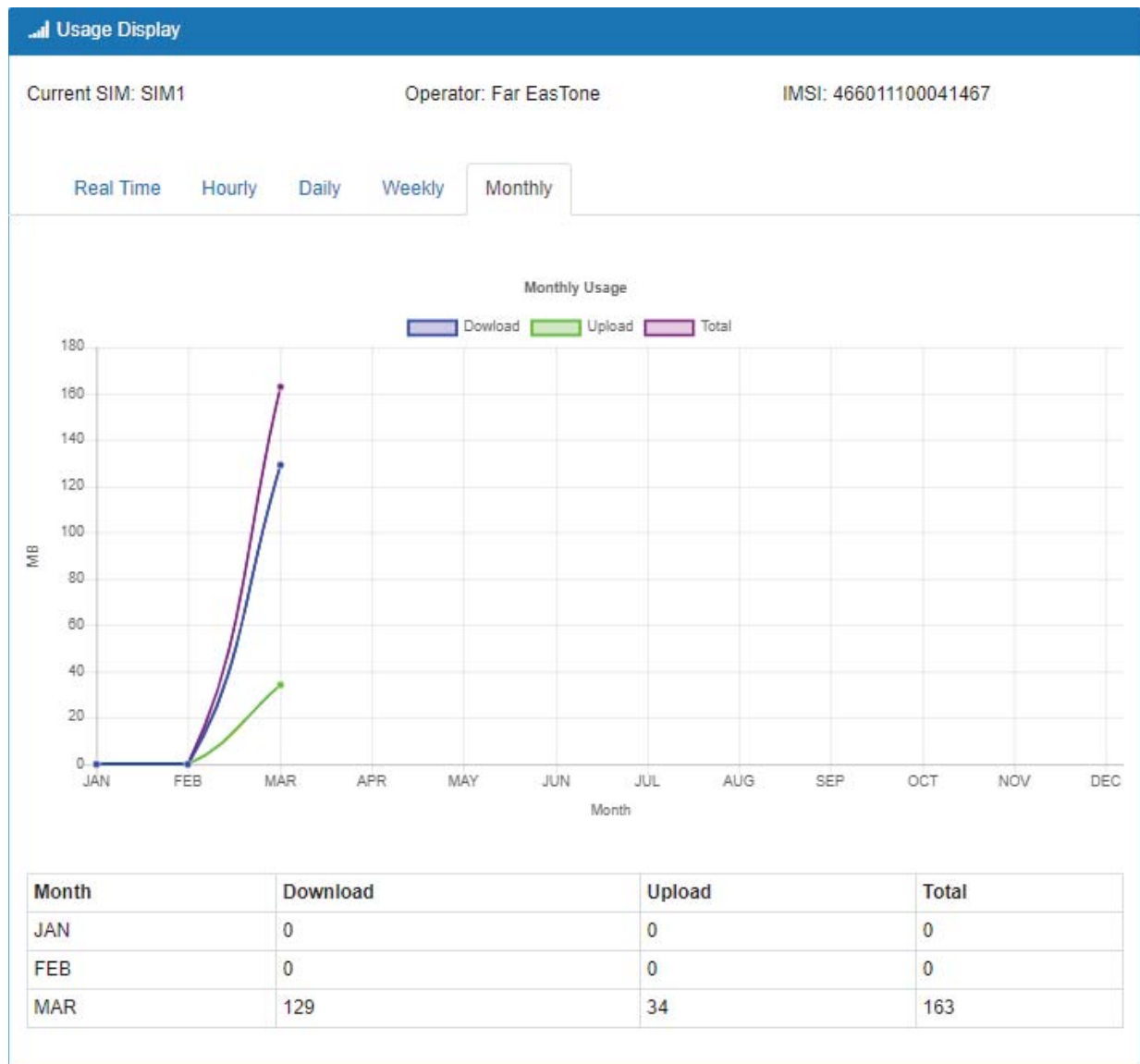
(4) Weekly Usage:

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



(5) Monthly Usage:

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



7.5 LTE > SMS

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

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

SMS

SMS Action

View SMS

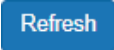
Mode ☐ Disable ☒ Enable

Actions and Keywords Setup

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

Hint: Only accept SMS from trusted and on duty members

Apply

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

SMS

SMS Action

View SMS

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

Clear

Refresh

18/11/14 09:48:00 

005B906050B34F8696FB7B5492349AD49A575230671F901A77E5005D60A87684514D8
CBB9AD49A575C0765BC003359295F8C5230671F002E4EFB610F937556DE8986672C7
C218A0A621675

Close

7.6 LTE > Serving Cell

This section displays all parameters, including the following items:

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

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

7.7 LTE > DNS

This section allows you to setup LTE specific DNS setting.

 DNS

APN1 DNS Server Configuration

IPv4 DNS Server #1

From ISP ▼

IPv4 DNS Server #2

From ISP
User Defined
None

IPv4 DNS Server #3

From ISP ▼

APN2 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
IPv4 DNS Server #1 IPv4 DNS Server #2 IPv4 DNS Server #3	- Each setting DNS Server has three options, including From ISP, User Defined and None. - When you select From ISP, the IPv4 DNS server IP is obtained from ISP. - When you select User Defined, the IPv4 DNS server IP is input by user.

8 Configuration > WiFi (M330-W)

This section allows you to set up the WiFi configuration.

WiFi 

WiFi Config

MAC Filter

Client List

8.1 WiFi > WiFi Config

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

 Config

WiFi Network

AP Enable

☐ Disable ☒ Enable

AP Isolate

☒ Off ☐ On

HT Mode

☒ 20M ☐ 40M

Country Code

TW - Taiwan

Channel

Auto

Name(SSID)

M330-W-44d1fa72d797

Hidden SSID

☒ Off ☐ On

Security Option

WPA2-PSK(AES)

Passphrase

.....

(8~63 characters)

Key Update

0

(0 no update or 30~86400 seconds)

Apply

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

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

8.2 WiFi > MAC Filter

This section allows you to set up MAC Filter.

WiFi Network MAC Filter

Mode

☒ Disable
 ☐ Enable

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

Apply

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

Edit MAC Filter Entry #1

Mode

☒ Disable ☐ Enable

MAC Address

Save

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

8.3 WiFi > Client List

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

 Client List

WiFi Client List

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

Refresh

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

9 Configuration > LAN

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

LAN	⇌
IPv4	
IPv6	
VLAN	
Subnet	

9.1 LAN > IPv4

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

⇌ LAN IPv4	
IP Address	192.168.1.1
IP Mask	255.255.255.0
DHCP Server Configuration	
☒ DHCP Server Configuration	
IP Address Pool	From 192.168.1.2 To 192.168.1.254
Apply	

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

9.2 LAN > IPv6

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

LAN IPv6

Type ☒ Delegate Prefix from WAN ☐ Static

Static Address

DHCP Server Configuration

Address Assign ☒ Stateful ☐ Stateless

Apply

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

9.3 LAN > VLAN

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

VLAN

Mode ☒ Off ☐ Tag Base

VLAN Isolation ☐ Off ☒ On

Apply

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

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

VLAN

Mode

☐ Off
 ☒ Tag Base

VLAN Isolation

☐ Off
 ☒ On

Enable	Subnet	VID	Name
☒	NET1	1	lan(Full Feature LAN)
☐	NET2	2	lan.2(LAN)
☐	NET3	3	lan.3(LAN)
☐	NET4	4	lan.4(LAN)
☐	NET5	5	lan.5(LAN)
☐	NET6	6	lan.6(LAN)
☐	NET7	7	lan.7(LAN)
☐	NET8	8	lan.8(LAN)

Apply

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

(**Note:** The NET1 can't remove it and fixes in the first row.)

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

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

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

9.4 LAN > Subnet

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

Subnet			
Name	IP Address	IP Mask	Edit
NET2	192.168.2.1	255.255.255.0	
NET3	192.168.3.1	255.255.255.0	
NET4	192.168.4.1	255.255.255.0	
NET5	192.168.5.1	255.255.255.0	
NET6	192.168.6.1	255.255.255.0	
NET7	192.168.7.1	255.255.255.0	
NET8	192.168.8.1	255.255.255.0	
Note: Subnet NET1 is the default IPv4 LAN, go IPv4 for configuration.			
			Apply

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

Edit Subnet NET2	
IP Address	192.168.2.1
IP Mask	255.255.255.0
DHCP Server Configuration	
☒ DHCP Server Configuration	
IP Address Pool	From 192.168.2.2 To 192.168.2.254
Save	

10 IP Routing

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

IP Routing

Static Route

RIP

OSPF

BGP

10.1 IP Routing > Static Route

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

Static Route

Mode ☒ Off ☐ On

Settings

Status

Mode	Name	Destination	Gateway	Interface	Delete
☐ Off ☒ On		192.168.100.0/24	192.168.1.250		

Mode ☐ Off ☒ On

Name

Destination

Gateway

Interface

Add

Apply

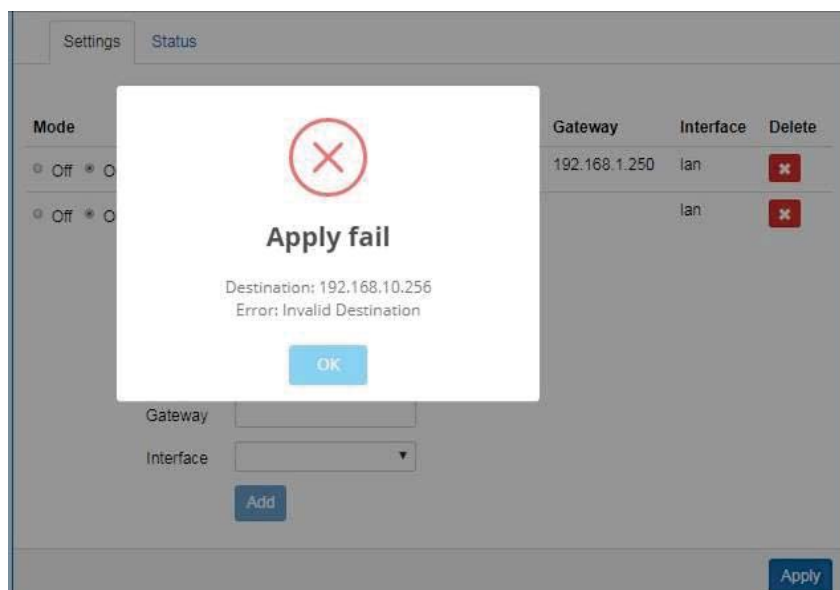
IP Routing > Static Route > Settings	
Item	Description
Mode	The setting is for full network. Select from Off or On.
Settings	
Mode	The setting is for the specific network. Select from Off or On.

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

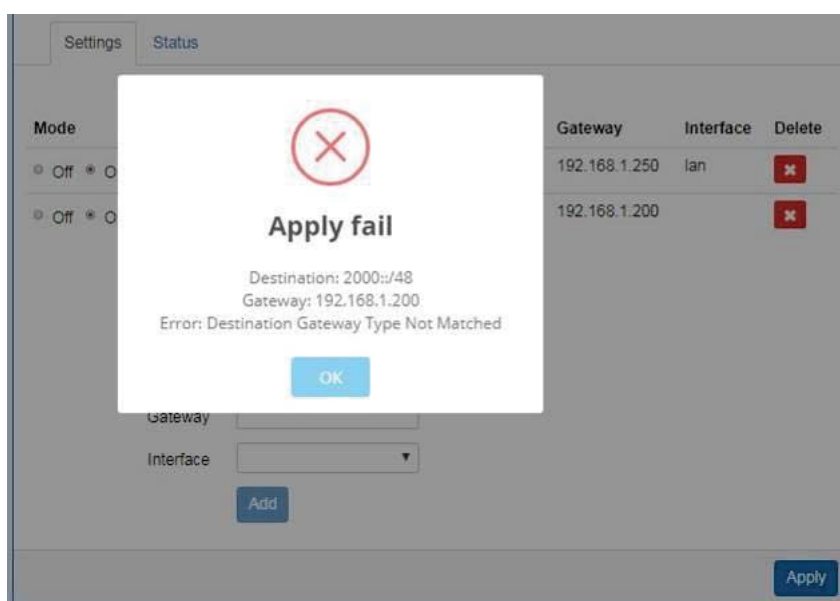
Note:

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

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



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



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

 Static Route

Mode ☒ Off ☐ On

Settings Status

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

Apply

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

10.2 IP Routing > RIP

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

Note:

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

 RIP

General

Interfaces

Mode

☒ Off ☐ On

Redistribute local routes

☒ Off ☐ On

from the device's own routing table

Redistribute connected routes

☒ Off ☐ On

to networks which are directly connected to the device

Redistribute OSPF routes

☒ Off ☐ On

learned via the OSPF routing protocol

Redistribute BGP routes

☒ Off ☐ On

learned via the BGP routing protocol

Apply

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

RIP

General
Interfaces

#	Mode	Interface	Authentication	Key	Key ID	Passive	Edit	Delete
Add RIP Interface								
Mode ☐ Off ☒ On Interface eth1(WAN Ethernet) Authentication md5 Key The key used for authentication (maxlength=16) Key ID 1 The ID of the key used for authentication (1-255) Passive ☒ Off ☐ On Do not send out RIP packets on this interface Add								

Apply

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

10.3 IP Routing > OSPF

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

(1) General Configuration

 OSPF

General

Interfaces

Networks

Mode

☒ Off ☐ On

Redistribute local routes

☒ Off ☐ On

from the device's own routing table

Redistribute connected routes

☒ Off ☐ On

to networks which are directly connected to the device

Redistribute RIP routes

☒ Off ☐ On

learned via the RIP routing protocol

Redistribute BGP routes

☒ Off ☐ On

learned via the BGP routing protocol

Apply

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

(2) Interfaces Configuration

There are 2 parts for OSPF Interfaces configuration.

- OSPF Interfaces Summary

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

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

- Add/Edit OSPF Interface

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

OSPF

General

Interfaces

Networks

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

Add OSPF Interface

Add/Edit

Mode

☐ Off ☒ On

Interface

eth1

Authentication

md5

Key

The key used for authentication (maxlength=16)

Key ID

1

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

Cost

0

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

Passive

☒ Off ☐ On

Do not send out OSPF packets on this interface

Add

Apply

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

(3) Networks Configuration

There are 2 parts for OSPF Networks configuration.

- OSPF Networks Summary

You can edit and delete the existed OSPF networks.

- OSPF Networks Add/Edit

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

OSPF

General

Interfaces

Networks

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

Add OSPF Network

Mode

☐ Off ☒ On

Prefix

Prefix of the network

Prefix Length

Length of the prefix

Area

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

Add

Add/Edit

Apply

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

10.4 IP Routing > BGP

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

(1) General Configuration

 BGP

General

Neighbors

Networks

Mode

☒ Off ☐ On

AS Number

The number of the autonomous system (1 ~ 4294967295)

Redistribute local routes

☒ Off ☐ On

from the device's own routing table

Redistribute connected routes

☒ Off ☐ On

to networks which are directly connected to the device

Apply

IP Routing > BGP > General	
Item	Description
General	
Mode	- Off: BGP function is off. - On: BGP function is on.
AS Number	The number of the autonomous system (1 ~ 4294967295)
Redistribute local routes	- Off: Not redistribute local routes from the device's own routing table. - On: Redistribute local routes from the device's own routing table.
Redistribute connected routes	- Off: Not redistribute connected routes to networks which are directly connected to the device. - On: Redistribute connected routes to networks which are directly connected to the device.

(2) Neighbor Configuration

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

BGP

General

Neighbors

Networks

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

Add BGP Neighbor

Mode

☐ Off ☒ On

IP Address

IP address of the peer router

AS Number

Autonomous system number of the peer router

Multihop

☐ Off ☒ On

Allow multiple hops between this router and the peer router

Update Source Mode

☒ Off ☐ On

Whether to specify the source address to this neighbor

Update Source Address

The source address to this neighbor

Add

Apply

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

(3) Networks Configuration

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

BGP

General

Neighbors

Networks

#	Mode	Prefix	Prefix Length	Edit	Delete
1	on	4.4.4.0	24		

Add BGP Network

Mode

☐ Off ☒ On

Prefix

Prefix of the network

Prefix Length

Length of the prefix

Add

Apply

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

11 Configuration > VPN

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

VPN 
Open VPN
IPSec
GRE
PPTP Server
L2TP

11.1 VPN > Open VPN

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

 Open VPN

Mode ☒ Disable ☐ Enable

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

Apply

11.1.1 Open VPN Common Setting

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

Edit Open VPN Connection #1

Setting

Log

Mode

☒ Disable ☐ Enable

VPN Mode

☐ Server ☒ Client ☐ Custom

VPN Type

☒ Roadwarrior ☐ Bridging

Status

Idle

TLS Mode

☒ Disable ☐ Enable

Cipher

BF-CBC

IPv6 Mode

☒ Disable ☐ Enable

Device

☒ TUN ☐ TAP

Protocol

☒ UDP ☐ TCP

Port

1701

VPN Compression

☒ Disable ☐ Enable

Authentication

Certificate

VPN > Open VPN > Setting	
Item	Description
Mode	Turn on/off Open VPN to select Disable or Enable.
VPN Mode	● Server: Tick to enable Open VPN server tunnel. ● Client: Tick to enable Open VPN client tunnel. The default is Client. ● Custom: This option allows user to use the .ovpn configuration file to quickly set up VPN tunnel with third-party server or use the Open VPN advanced options to be compatible with other servers.
VPN Type	● Roadwarrior (default) ● Bridging: Bridging the VPN tunnel and LAN/VLAN
Status	Display the status of Open VPN.
TLS Mode	Select from Disable or Enable for data security. The default is Disable.
Cipher	The Open VPN format of data transmission.
IPv6 Mode	Select from Disable or Enable. The default is Disable.
Device	Select from TUN or TAP. The default is TUN.

Protocol	Select from UDP or TCP Client which depends on the application. The default is UDP.
Port	Enter the listening port of remote side Open VPN server.
VPN Compression	Select Disable or Enable to compress the data stream. The default is Disable.
Authentication	- Select from two different kinds of authentication ways: Certificate or pkcs#12 Certificate. - The pkcs#12 option is only available on the VPN client mode.

11.1.2 Open VPN Client Setting

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

The files could be imported by clicking  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

Import

Cert

Import

Key

Import

P12

Import

Back

Refresh

Apply

VPN > Open VPN > Client VPN Mode	
Item	Description
Client	
Server Address	Fill in WAN IP of Open VPN server.
Route Client Networks	Select from Off or On. This setting needs to match the server side. When enabled, the cellular router will auto apply the properly

	routing rules.
Local Network	
Network	The local network exported by OpenVPN. When keeping this option blank, the OpenVPN will export the LAN network automatically.
Netmask	The local netmask exported by OpenVPN. When keeping this option blank, the OpenVPN will export the LAN netmask automatically.
NAT	
1:1 NAT	• Tick to enable NAT Traversal for Open VPN. This item must be enabled when the router under NAT environment. • Select from Off or On. • When two routers' LAN Subnet are same and create Open VPN tunnels, this function should be turned on.
Client-Security	
Root CA	The Certificate Authority file of Open VPN server could be downloaded from Open VPN server.
Cert	The certification file is for Open VPN client, which could be downloaded from Open VPN server.
Key	The private key file is for Open VPN client, which could be downloaded from Open VPN server.
P12	The PKCS#12 file is for Open VPN client, which could be downloaded from Open VPN server.

11.1.3 Open VPN Server Setting

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

Note: When selecting the ☐ 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	0.0.0.0	/	0.0.0.0
#2	0.0.0.0	/	0.0.0.0
#3	0.0.0.0	/	0.0.0.0
#4	0.0.0.0	/	0.0.0.0
#5	0.0.0.0	/	0.0.0.0
#6	0.0.0.0	/	0.0.0.0
#7	0.0.0.0	/	0.0.0.0
#8	0.0.0.0	/	0.0.0.0

Local Network

Network	Blank will use default LAN network
Netmask	Blank will use default LAN netmask

NAT

1:1 NAT ☒ Off ☐ On

Server - Server Security

Root CA	 Create
Cert, Key	 Create

Server - User Security

ovpn Server Address	blank: auto detect the WAN IP address		
User 1	☐ Valid	 Create	password for create
User 2	☐ Valid	 Create	password for create
User 3	☐ Valid	 Create	password for create
User 4	☐ Valid	 Create	password for create
User 5	☐ Valid	 Create	password for create
User 6	☐ Valid	 Create	password for create
User 7	☐ Valid	 Create	password for create
User 8	☐ Valid	 Create	password for create

Back

Refresh

Apply

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

11.1.4 Set up Open VPN Custom

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

Note:

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

Edit Open VPN Connection #1

Setting

Log

Mode

☒ Disable
☐ Enable

VPN Mode

☐ Server
☐ Client
☒ Custom

Custom Config

Import *.ovpn

i

Username

Password

Status

Idle

Back

Refresh

Apply

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

11.2 VPN > IPsec

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

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

Mode ☒ Disable ☐ Enable

Type ☒ Policy-based ☐ Route-based

VPN > IPsec > General setting	
Item	Description
Mode	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		⏻		Phase 1 Phase 2 ...

+ Add Connection

Apply

(1) IPsec Phase 1 Setting

Connection #1 Phase 1

Mode

☒ Disable
 ☐ Enable

Name

Protocol

IKEv1

Aggressive mode

Disable

Auth Type

PSK

Encryption

AES128

Hash

SHA1

DH Group

5 (1536 bit)

Lifetime

3 hours

Local Host

Local ID

<empty> (allow any)

Remote Host

Remote ID

<empty> (allow any)

Back

Save

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

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

(2) IPsec Phase 2 Setting

Connection #1 Phase 2

Protocol

ESP

Encryption

AES128

Hash

SHA1

DH Group

5 (1536 bit)

Lifetime

3 hours

Local Subnet

Remote Subnet

Service

Any

Back

Save

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

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

(3) IPsec Advance Setting

Connection #1 Advance

DPD interval (s)

DPD retry

Back

Save

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

11.2.2 IPsec > Authentication IDs

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

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

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

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

+ Add Authentication ID

Apply

VPN > IPsec > Authentication IDs	
Item	Description
ID	The identification for authentication. It only work on PSK type.
Type	Select from PSK or RSA. The default is PSK. ● PSK: Use the pre-shared key to authenticate the connection. ● RSA: Use the certificate to authenticate the connection.
Pre-shared Key / X.509 Certificate	The X.509 certificate for authentication. The certificate could be generated or imported by X.509 Certificates section.

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

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

11.2.3 IPsec > X.509 Certificates

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

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

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

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			

+ Add X.509

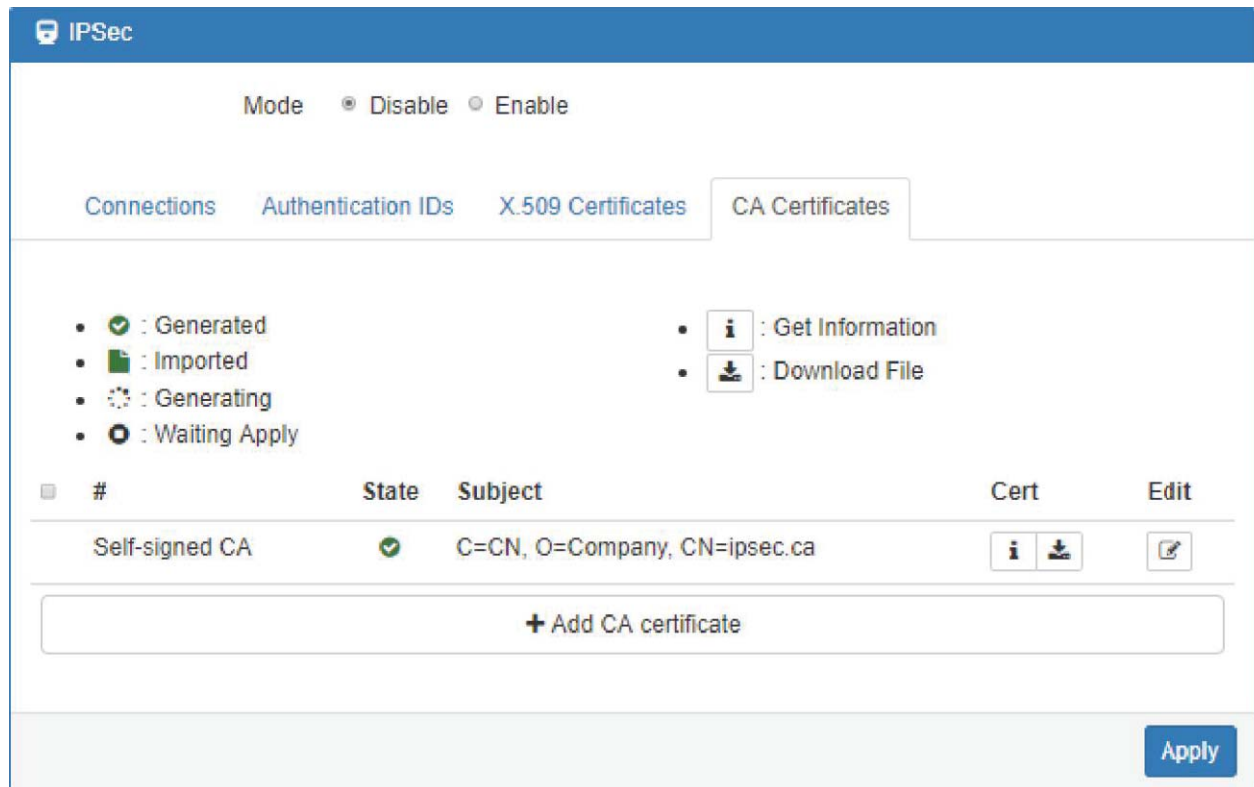
Apply

11.2.4 IPsec > CA Certificates

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

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

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



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

Self-signed CA Certificate

Country Name (C)

State (ST)

Location, e.g. city (L)

Organization Name (O)

Organization Unit Name (OU)

Common Name (CN)

E-mail

 Generate Certificate

Back
Save

Certificate Importing

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

To import the CA certificate:

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

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

To import the X.509 certificate:

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

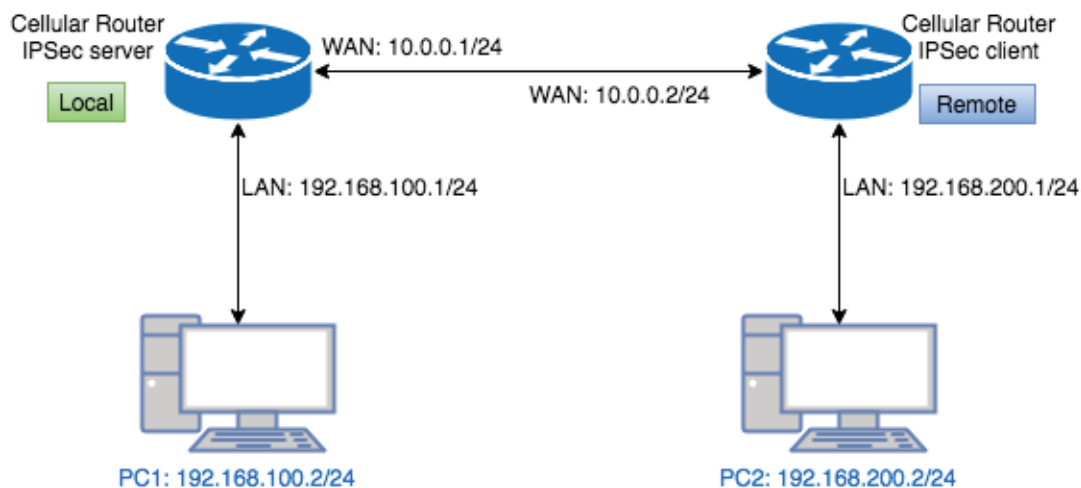
Download the certificate

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

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

11.2.5 IPsec > Net-to-Net Configuration

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



● Pre-shared Key authentication

Configure Net-to-Net VPN Server

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

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

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

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

+ Add Authentication ID

Apply

Connection #1 Phase 1

Mode	☐ Disable ☒ Enable
Name	
Protocol	IKEv1
Aggressive mode	Disable
Auth Type	PSK
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	3 hours
Local Host	
Local ID	<empty> (allow any)
Remote Host	
Remote ID	<empty> (allow any)

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

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

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

Configure Net-to-Net VPN Client

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

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

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

+ Add Authentication ID

Apply

Connection #1 Phase 1

Mode	☐ Disable ☒ Enable
Name	
Protocol	IKEv1
Aggressive mode	Disable
Auth Type	PSK
Encryption	AES128
Hash	SHA1
DH Group	5 (1536 bit)
Lifetime	3 hours
Local Host	
Local ID	<empty> (allow any)
Remote Host	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
☐	1	psk		IKEv1 : 10.0.0.1 [10.0.0.1] ... 10.0.0.2 [10.0.0.2]	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	psk		IKEv1 : 10.0.0.2 [10.0.0.2] ... 10.0.0.1 [10.0.0.1]	Phase 1 192.168.200.0/24 ... 192.168.100.0/24 Phase 2

+ Add Connection

- RSA authentication - Server

Prepare the self-signed CA certificate

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

6. Refresh the page

Self-signed CA Certificate

Country Name (C)

State (ST)

Location, e.g. city (L)

Organization Name (O)

Organization Unit Name (OU)

Common Name (CN)

E-mail

 Generate Certificate

Back

Save

Prepare the X.509 certificates

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

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

X.509 Certificate #1

Country Name (C)

State (ST)

Location, e.g. city (L)

Organization Name (O)

Organization Unit Name (OU)

Common Name (CN)

E-mail

 Generate Certificate

Back

Save

X.509 Certificate #2

Country Name (C)

State (ST)

Location, e.g. city (L)

Organization Name (O)

Organization Unit Name (OU)

Common Name (CN)

E-mail

 Generate Certificate

Back

Save

Mode
☐ Disable
☒ Enable

Type
☒ Policy-based
☐ Route-based

Connections
Authentication IDs
X.509 Certificates
CA Certificates

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

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

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

+ Add X.509

Apply

Mode
☐ Disable
☒ Enable

Type
☒ Policy-based
☐ Route-based

Connections
Authentication IDs
X.509 Certificates
CA Certificates

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

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

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

+ Add X.509

Apply

Prepare the authentication IDs

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

The screenshot shows the IPsec configuration interface. At the top, there's a blue header with the IPsec icon and label. Below it, there are two radio buttons for 'Mode' (Disable and Enable, with Enable selected) and two radio buttons for 'Type' (Policy-based and Route-based, with Policy-based selected). Below these are four tabs: 'Connections', 'Authentication IDs' (which is active), 'X.509 Certificates', and 'CA Certificates'. The 'Authentication IDs' tab contains a table with two columns: '# ID' and 'Type'. There are two rows in the table. The first row has ID '1' and Type 'RSA'. The second row has ID '2' and Type 'RSA'. To the right of the table is a column for 'Pre-shared Key / X.509 Certificate'. Below the table is a button labeled '+ Add Authentication ID'. At the bottom right is an 'Apply' button.

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

+ Add Authentication ID

Apply

Setup the connection on VPN server

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

4. Apply the changes

Connection #1 Phase 1

Mode

☐ Disable ☒ Enable

Name

Protocol

IKEv1

Aggressive mode

Disable

Auth Type

RSA

Encryption

AES128

Hash

SHA1

DH Group

5 (1536 bit)

Lifetime

3 hours

Local Host

Local ID

ID#1: local.ipsec (RSA)

Remote Host

Remote ID

<empty> (allow any)

Back

Save

Connection #1 Phase 2

Protocol

ESP

Encryption

AES128

Hash

SHA1

DH Group

5 (1536 bit)

Lifetime

3 hours

Local Subnet

192.168.100.0/24

Remote Subnet

192.168.200.0/24

Service

Any

Back

Save

● RSA authentication – Client

Prerequisite for VPN Client with RSA authentication

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

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

Import the CA certificate and the X.509 certificate

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

IPSec

Mode ☒ Disable ☐ Enable

Type ☒ Policy-based ☐ Route-based

Connections Authentication IDs X.509 Certificates CA Certificates

• : Generated

• : Imported

• : Generating

• : Waiting Apply

• : Get Information

• : Download File

#	State	Subject	Cert	Edit
		Self-signed CA		

+ Add CA certificate

Apply

IPSec

Mode ☒ Disable ☐ Enable

Type ☒ Policy-based ☐ Route-based

Connections Authentication IDs X.509 Certificates CA Certificates

• : Generated

• : Imported

• : Cert or Key is missed

• : Generating

• : Waiting Apply

• : Get Information

• : Download File

• : Import File

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

+ Add X.509

Apply

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's a blue header with the IPsec icon and label. Below it, the 'Mode' is set to 'Enable' (radio button selected) and 'Type' is set to 'Policy-based' (radio button selected). There are four tabs: 'Connections', 'Authentication IDs' (active), 'X.509 Certificates', and 'CA Certificates'. The 'Authentication IDs' tab contains a table with columns: '#', 'ID', 'Type', and 'Pre-shared Key / X.509 Certificate'. There is one entry with ID '1', an empty ID field, 'RSA' type, and the certificate 'C=CN, O=Company, CN=remote.ipsec'. Below the table is a button '+ Add Authentication ID'. At the bottom right is an 'Apply' button.

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

+ Add Authentication ID

Apply