# M331

# Industrial 4G LTE Dual SIM Cellular Router

## User Manual

Version 1.00

# Table of Contents

# 1 Introduction

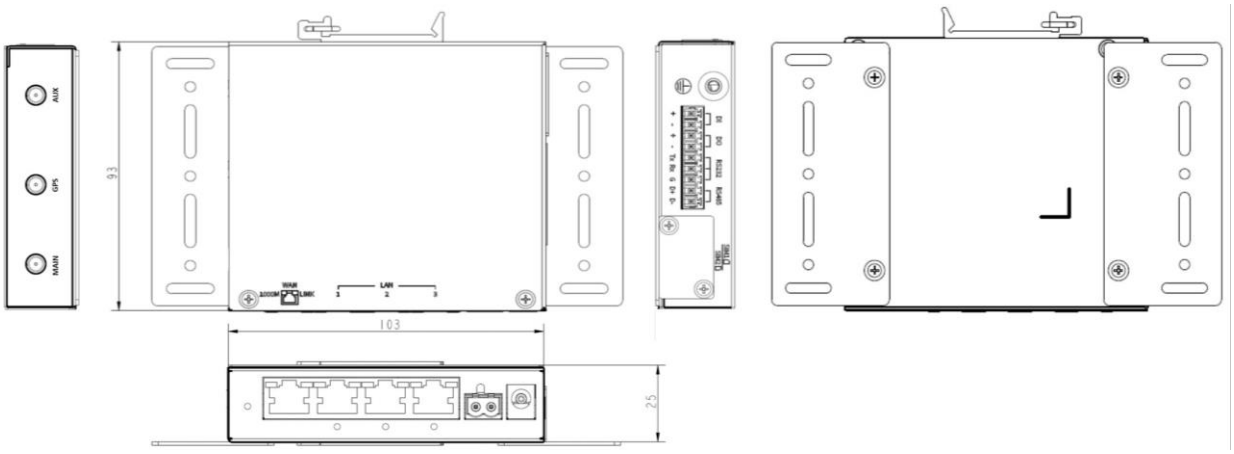
Proscend M331 Industrial 4G LTE Cellular Router comes with 3 Gigabit LAN ports, 1 Gigabit WAN port and dual SIM support to enable critical industrial applications and reliable IoT connectivity for optimal performance and network redundancy. The M331 is designed with a rugged compact enclosure for DIN-rail or wall mounting to install where tight spaces. The M331 features digital I/O, serial ports (RS-232, RS-485), DC and AC power inputs to provide flexible installation in demanding environments.

Proscend M331 is a highly secure and high-performance cellular router used in a main or backup Internet communications. To fit the deployments at scale and simplify network management, Proscend M331 can work with IoT Management System O'smart, allowing the administrator to remotely monitor, manage, and configure the M331 Cellular Router anywhere, anytime.

## 1.1 Features

- Support multi-band connectivity with FDD LTE / TDD LTE / WCDMA / GSM / LTE CAT4.
- Built-in dual Micro SIM slots, serial ports (RS-232, RS-485), and DI/DO interfaces.
- Detachable antenna design for using a wide variety of external antennas.
- LED indicators for connection and data transmission status.
- Industrial rated from -30 to +70°C for use in harsh environments.
- Support serial communication protocols for flexible connectivity.
- Enhance security and encryption for authentication and transmission.

## 1.2 Dimensions



## 1.3 Specifications

**Cellular Interface**

- 4G: FDD LTE, TDD LTE
- 3G: WCDMA
- 2G: GSM
- LTE Data Rate: CAT 4, 150Mbps (DL), 50Mbps (UL)

**Hardware Interface**

- 2 x Micro SIM slots (push-push type)
- 3 x LAN 10/100/1000 Mbps Ethernet port
- 1 x WAN 10/100/1000 Mbps Ethernet port
- 1 x RESET Button
- 1 x RS-232 (TX/RX/GND)
- 1 x RS-485 (D+/D-/GND)
- 1 x DI (Non-Isolated), 1 x DO (Non-Isolated)
- 2 x SMA connectors for detachable LTE antenna
- 1 x SMA connector for detachable GPS antenna
- 1 x DC jack for AC-DC power adapter
- 1 x DC power input

**Physical Characteristics**

- Enclosure： Metal Case
- Dimensions (W x H x D)：103 x 25 x 93 mm
- Weight：350 g
- Installation： DIN-rail / Wall mounting

**LED Display**

- 1 x Power status
- 1 x LTE Signal strength
- 1 x SIM status
- 2 x Speed and Link status (each LAN/WAN port)

**Power Supply**

- Power Consumption：7 Watts (Max)
- DC jack power Input：12 VDC
- Terminal block power input: 8 ~ 26 VDC

**Software**

- **Network Protocols**

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

- **Routing/Firewall**

  NAT, Virtual Server, DMZ, MAC Filter, URL Filter, IP Filter, Static Routing, IPS, SPI, Policy Route

- **VPN**

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

- **Others**

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

- **Alarm**

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

- **Management**

  Web GUI for remote and local management, CLI
  Syslog monitor
  SNMP
  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%HR (non-condensing)
- Humidity 0 ~ 95%HR (non-condensing)

**Standards and Certifications**

- NCC & BSMI CNS15936 & CNS15598-1

# 2 Hardware Installation

This chapter introduces how to install and connect the hardware.

## 2.1 Install the SIM Card

**STEP 1:** Before inserting or removing the SIM card, ensure that the power has been turned off, or the power connector has been removed from the M331 Cellular Router.

**STEP 2:** Using a screwdriver to remove the metal protective cover first, insert the SIM card into the card slots. The cut-off edge of the SIM card on upper SIM slot 1 (lower SIM slot 2) is to the left (right).

**STEP 3:** Push the SIM card and lightly press it to lock into the slot.

**STEP 4:** Remove the SIM card, lightly press it and it will pop out of the slot.


**NOTE:**

- Please use the industrial SIM card operating from -40°C to +105°C to ensure proper cellular router operation.

## 2.2 LED Indicators

The following table explains the LED indicators on the front panel.

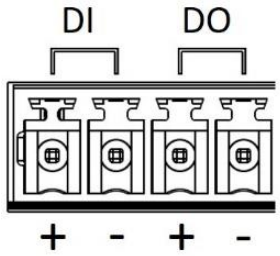
| LED | Off | On | Slow | Fast | Heartbeat |
|---|---|---|---|---|---|
| **SYS** | Power down | Power up | N/A | N/A | N/A |
| **SIM** | Not working | Connected | Connecting | Error | Reading |
| **Signal** | No signal | High signal | Medium signal | Low signal | N/A |

## 2.3 Reset Button

| Function | Operation |
|---|---|
| **Reset** | Press the button for 1 seconds. |
| **Reset to default setting** | Press the button for more than 5 seconds. |

## 2.4 Connecting I/O Ports

There are four terminals on the terminal block with two terminals used for digital input and two terminals used for digital output.



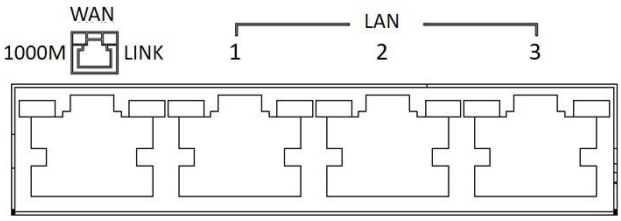

| Pin | Description |
|---|---|
| **DI +** | Digital Input |
| **DI -** | |
| **DO +** | Digital Output |
| **DO -** | |

DI: Low (+0 to +3V) / High (+8 to +40V)

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

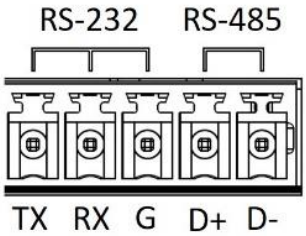
## 2.5 LED Indicators of Ethernet Port

There are two LED indicators for each of three LAN ports and one WAN port.




| LED | Blinking | On | Off |
|---|---|---|---|
| 1000M | N/A | 1000Mbps | 10/100Mbps |
| LINK | Data Transmitting | LINK UP | LINK DOWN |

## 2.6 RS-232 and RS-485 pinouts




**NOTE:** RS-232 and RS-485 share the common ground pin “G”.

**RS-232**

| Pin | Signal | Direction |
|---|---|---|
| **TX** | Transmit Data | Output |
| **RX** | Receive Data | Input |
| **G** | Signal Ground | - |

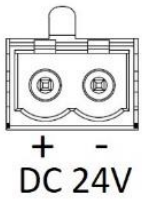
**RS-485**

| Pin | Description |
|---|---|
| **D +** | Serial Port, Data+ (A) wire |
| **D -** | Serial Port, Data- (B) wire |
| **G** | Signal Ground |

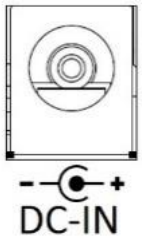
RS-485 2-wire cable (Twisted Pair)

## 2.7 Connecting the Power Supply

Powering the M331 Cellular Router is by either a terminal block or a DC jack.




One terminal block is on the front panel.
The power input voltage range is 8 ~ 26 VDC.

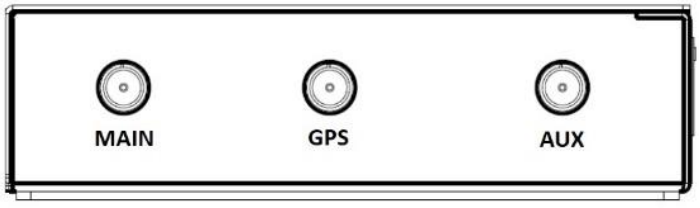



One DC Jack is on the front panel.
The power input voltage is 12 VDC.

## 2.8 Antenna Installation

Three SMA connectors placed on the left panel are for connecting to external LTE and GPS antennas.

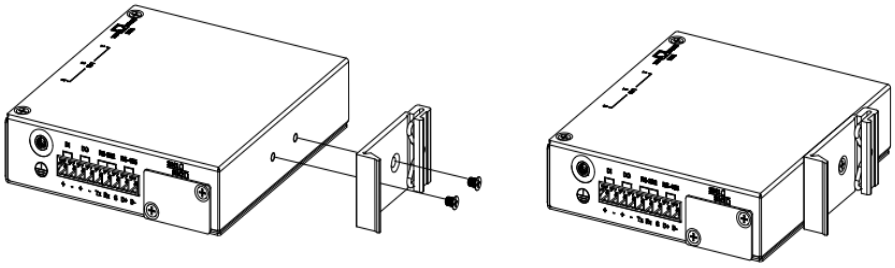
- MAIN: for LTE Transmit and Receive
- AUX: for optional LTE Receive for better downstream speed
- GPS: for GPS



## 2.9 DIN-rail Mounting

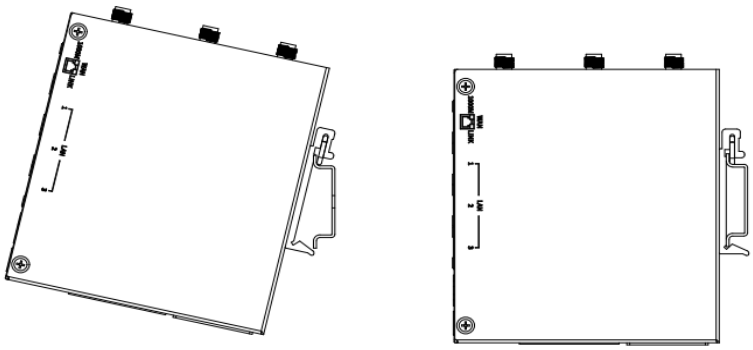
**STEP 1:** Use the screws to install the DIN-rail kit to attach at the rear side of the device.

**NOTE:** Three screw types are flat head M3 x 4 mm.



**STEP 2:** Hook the unit onto the DIN-rail.

**STEP 3:** Push the bottom of the unit towards the DIN-rail until it locks in place.



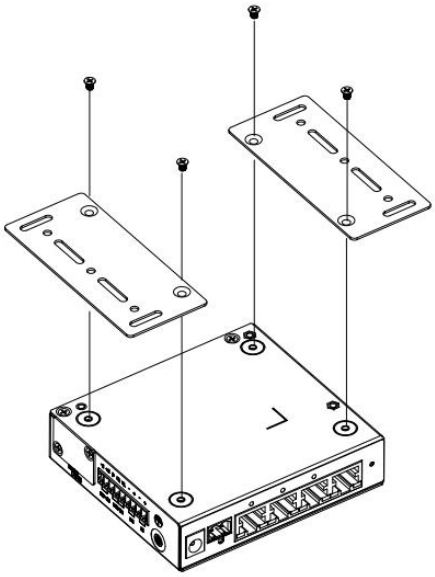
## 2.10 Wall Mounting

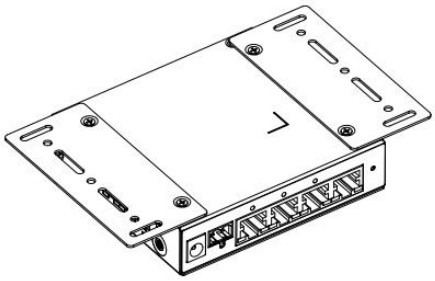
**STEP 1:** At the bottom side of the device, use two screws to install each bracket.

**NOTE:** Each screw type is flat head M3 x 6 mm.

**STEP 2:** Use the screws to attach the bracket of the device for wall mounting.

**NOTE:** These screws are not included in the package. The head of each screw is less than 7 mm in diameter, the shaft is less than 3 mm in diameter, and the length is less than 10 mm in diameter.





# 3 Configuration via Web Browser

## 3.1 Access the Web Configurator

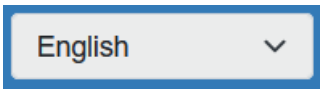
The web configuration is an HTML-based management interface for quick and easy set up of the cellular router. Monitoring of the status, configuration and administration of the router can be done via the Web interface.

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

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

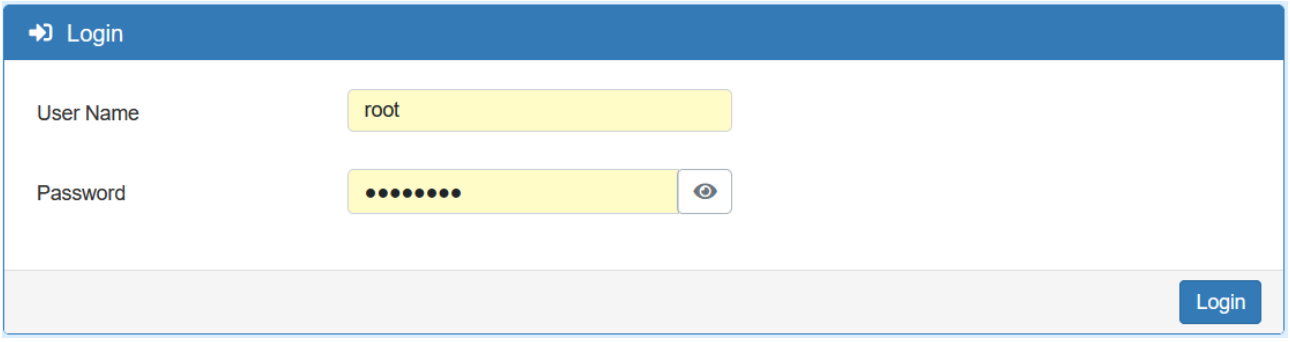
**Title Bar Panel > Selecting Language**

You can choose the different language display of web GUI.




**Logging in the Router**

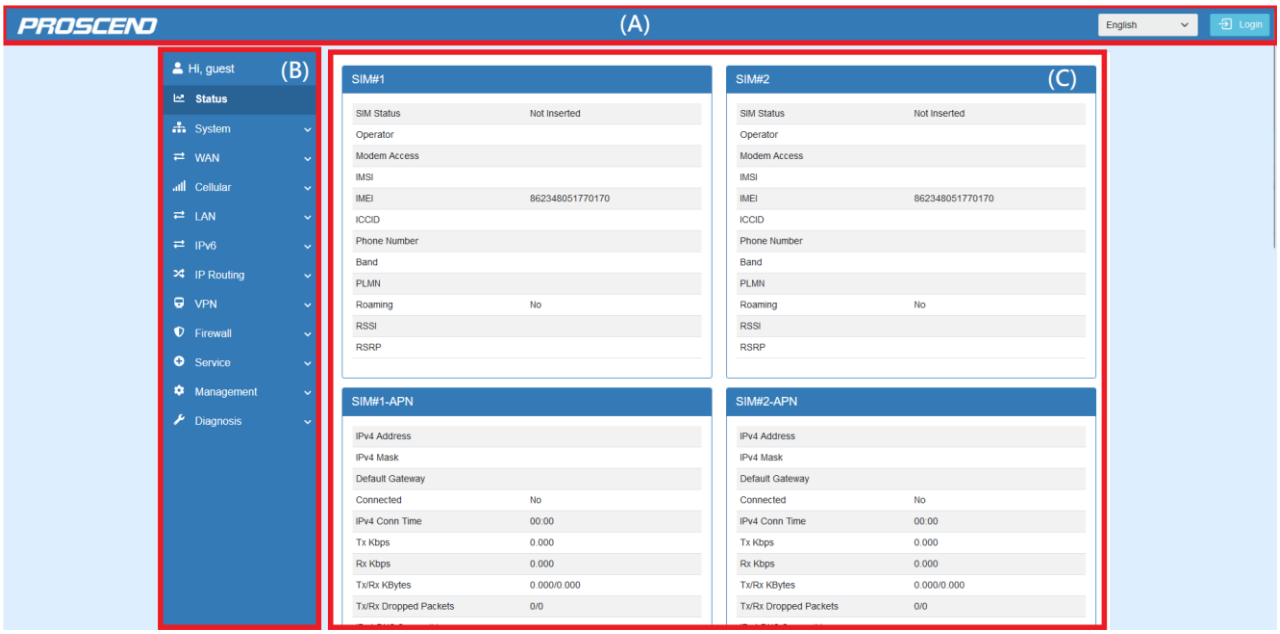
In this section, please fill in the default User Name **root** and the default Password **2wsx#EDC** and then click Login.



## 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** |
| **Language** | Choose your language from the drop-down list on the upper right corner of the title bar. |
| **Login / Logout** | Click to login or logout the web GUI. |

(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.

| Navigation Panel | |
|---|---|
| **Main Menu** | **Sub Menu** |
| **Status** | Device overall status |
| **System** | Time and Date, Logging, Alarm, Dying Gasp, COM Ports, Ethernet, Modbus, Client List |

| | |
|---|---|
| **WAN** | Connection Table, Ethernet, IPv6 DNS, Health Check |
| **Cellular** | Config, GPS, SIM Config, SIM Usage, SMS, Serving Cell, DNS |
| **LAN** | IPv4 |
| **IPv6** | IPv6 Config |
| **IP Routing** | Static Route, Policy Route |
| **VPN** | OpenVPN, IPSec, GRE, PPTP Server, L2TP |
| **Firewall** | Basic Rules, Port Forwarding, DMZ, Management IP, ACL, IP Filter, MAC Filter, URL Filter, NAT, IPS |
| **Service** | SNMP, Dynamic DNS, MQTT, UPnP, SMTP, IP Alias, QoS |
| **Management** | Identification, Administration, Contacts / On Duty, SSH, Web, Telnet, Firmware, Configuration, Load Factory, Restart, Schedule Reboot, Fail2Ban, O'smart |
| **Diagnosis** | Ping, Traceroute |

# 4 Web Menu Item > Status

This page shows overall status of device.

| Status > SIM#1 and SIM#2 | |
|---|---|
| **Item** | **Description** |
| SIM Status | The status of SIM. |
| Operator | The name of operator. |
| Modem Access | The access type between LTE module and base station. |
| IMSI | The IMSI number of the SIM card. |
| IMEI | The IMEI number of the SIM card. |
| ICCID | The ICCID number of the SIM card. |
| Phone Number | The phone number of the SIM card. |
| Band | The current connected band. |
| PLMN | The Public LAN Mobile Network ID. |
| Roaming | The status of Roaming. |
| RSSI | RSSI is measured over the entire bandwidth. |
| RSRP | RSRP is the received power of 1 RE average of power levels received across all Reference Signal symbols within the considered measurement frequency bandwidth |

| Status > SIM#1-APN/APN2 and SIM#2-APN/APN2 | |
|---|---|
| **Item** | **Description** |
| IPv4 Address | The IPv4 address that assigned by operator. |
| IPv4 Mask | The IPv4 mask that assigned by operator. |
| Default Gateway | The default gateway that assigned by operator. |
| Connected | The status of connection. “Yes” means Connected; “No” means Disconnected. |
| IPv4 Conn Time | The connection time of IPv4 network. |
| Tx Kbps | The uplink speed in Kbps. |
| Rx Kbps | The downlink speed in Kbps. |
| Tx/Rx KBytes | The accumulated TX/RX in KBytes. |
| Tx/Rx Dropped Packets | The dropped packets of Tx/Rx. |
| IPv4 DNS Server #1/#2/#3 | The DNS server address that assigned by operator. |

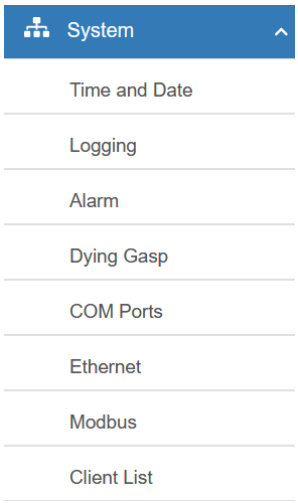
| Status > LAN Ethernet | |
|---|---|
| **Item** | **Description** |
| IPv4 Address | The IPv4 address of the M331 device. |
| IPv4 Mask | The IPv4 mask of the M331 device. |
| IPv6 Address | The IPv6 address of the M331 device. |
| IPv6 Prefix | The IPv6 Prefix of the M331 device. |
| IPv6 DNS Server #1/#2/#3 | The IPv6 DNS server address. |
| IPv6 Conn Time | The connection time of IPv6 network. |
| Tx Kbps | The speed of uplink in Kbps. |
| Rx Kbps | The speed of downlink in Kbps. |
| Tx/Rx KBytes | The accumulated TX/RX in KBytes. |
| Tx/Rx Dropped Packets | The dropped packets of Tx/Rx. |

| Status > WAN Ethernet | |
|---|---|
| **Item** | **Description** |
| IPv4 Address | The IPv4 address of the M331 device. |
| IPv4 Mask | The IPv4 mask of the M331 device. |
| IPv4 Gateway | The default gateway that assigned by operator. |
| IPv4 DNS Server #1/#2/#3 | The IPv4 DNS server address. |
| Tx Kbps | The speed of uplink in Kbps. |
| Rx Kbps | The speed of downlink in Kbps. |
| Tx/Rx KBytes | The accumulated TX/RX in KBytes. |
| Tx/Rx Dropped Packets | The dropped packets of Tx/Rx. |

| Status > Connected VPN Connections | |
|---|---|
| **Item** | **Description** |
| OpenVPN | Total connected number of OpenVPN. |
| IPSec | Total connected number of IPSec. |
| GRE | Total connected number of GRE. |
| PPTP Server | Total connected number of PPTP Server. |
| L2TP | Total connected number of L2TP. |

# 5 Web Menu Item > System

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



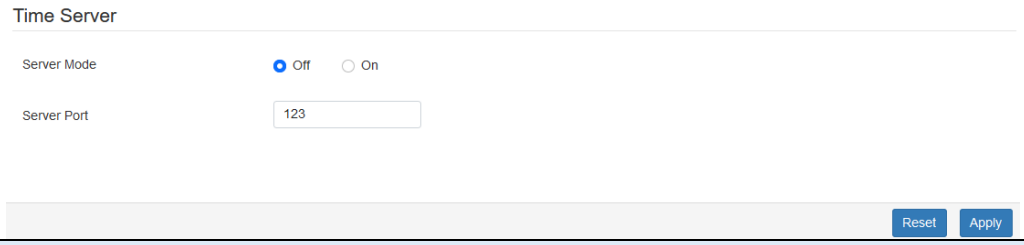

## 5.1 Time and Date

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 Local System** and **Get from Time Server**. The default mode is **Get from Time 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.

The **Time Server** feature makes M331 active as Tim Server for LAN side clients to get the time through NTP/SNTP protocol.

| System > Time and Date > Time Zone Setup | |
|---|---|
| **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 mins. |
| Start Date/Start Time | Time to enter Daylight Savings duration.<br>The Month range is 1~12;<br>1 - Jan. 2 - Feb. 3 - Mar. 4 - Apr. 5 – May 6 - Jun.<br>7 - Jul. 8 - Aug. 9 - Sep. 10 - Oct. 11 - Nov. 12 - Dec.<br>The Week range is 1~5;<br>1 - first week in month.<br>2 - second week in month<br>3 - third week in month<br>4 - fourth week in month<br>5 - fifth week in month<br>The Day range is 0~6;<br>0 - Sunday (The start day of a week)<br>1 - Monday<br>2 - Tuesday<br>3 - Wednesday<br>4 - Thursday<br>5 - Friday<br>6 - Saturday<br>The Hour range is 0~23;<br>The Min range is 0~59; |
| End Date/End Time | Time to leave Daylight Savings duration.<br>Same with Start Date/Start Time. |

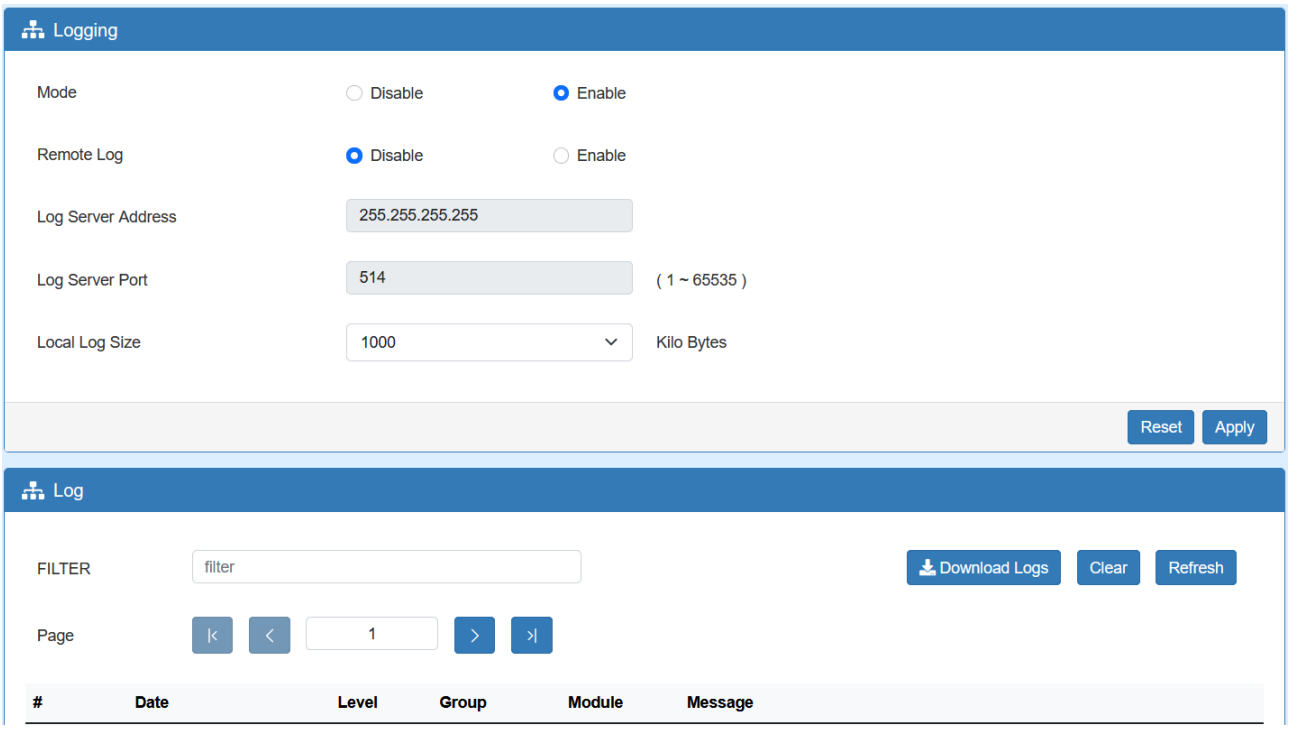



| System > Time and Date > Time Server | |
|---|---|
| **Item** | **Description** |

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

## 5.2 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.

| 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.<br>(***Note:*** This server should have installed Log software.) |
| Log Server Port | The port number of Log Server. |
| Local Log Size | Define the maximum file size of log. |

### 5.2.2 Logging > Log

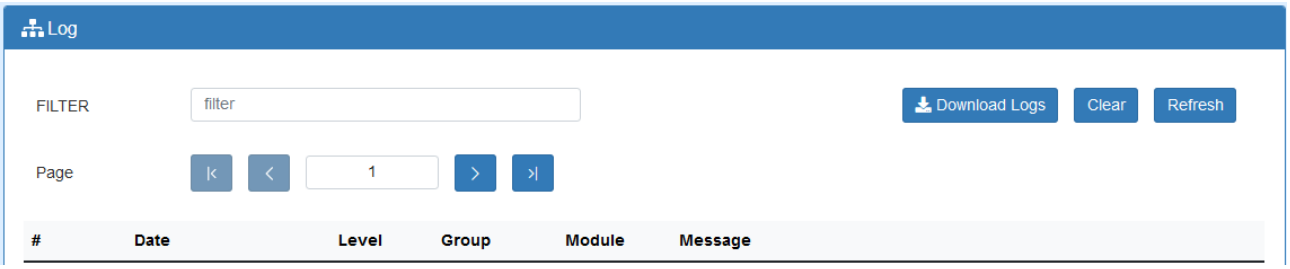
This section displays all status of router.

(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 page will be cleared totally without any backup.

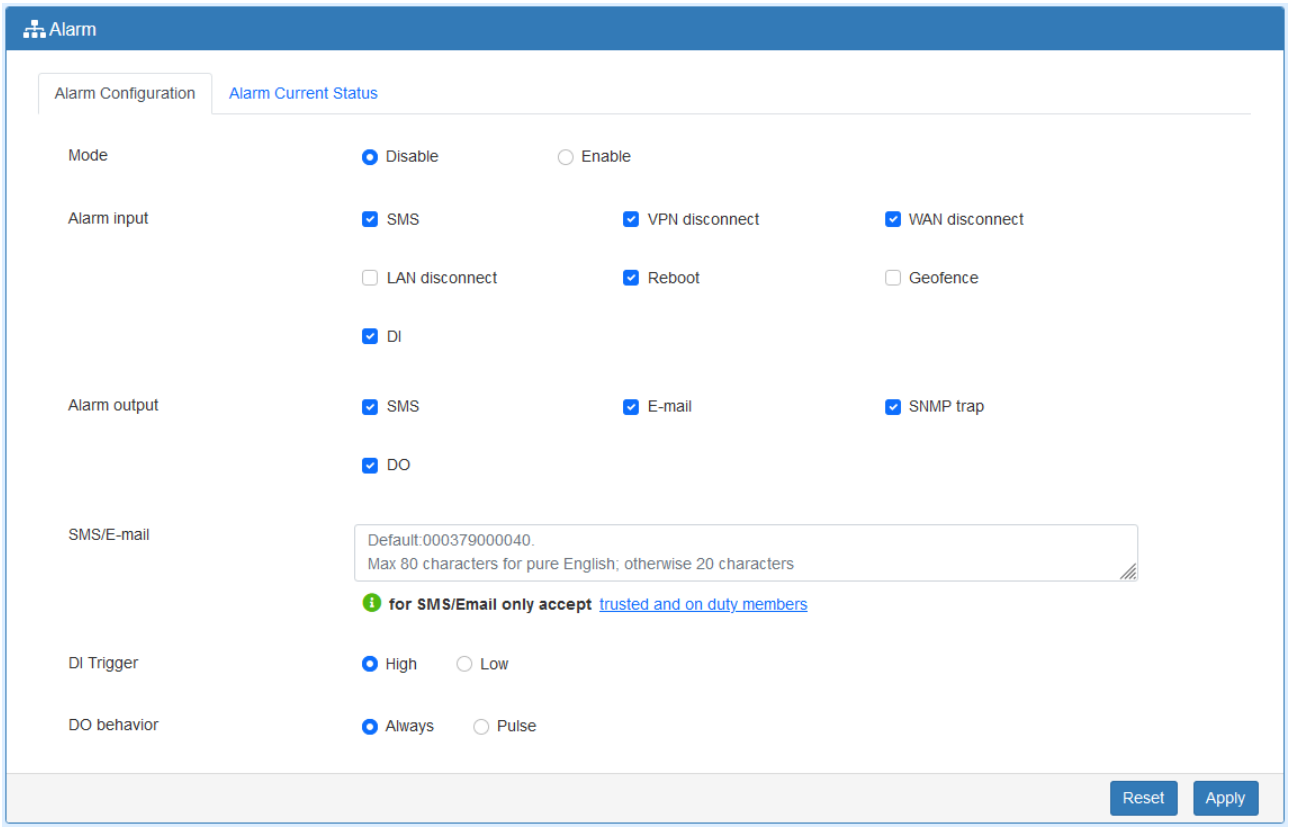
(3) When you click Refresh, the system will update and display the latest data from your cellular router.

(4) When you click Download Logs, the system will download the latest data from your cellular router.



## 5.3 Alarm

This section allows you to configure the alarm.




***Note:***

If you select SMS in Alarm input/output, you need to add the trust phone number into [Contracts/ On Duty].

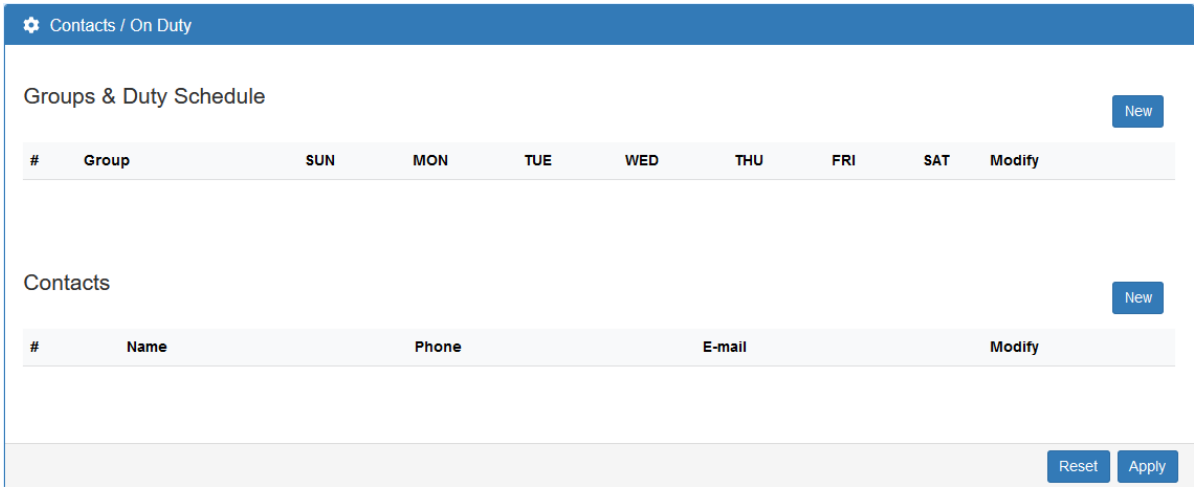
If you select SNMP trap in Alarm output, you need to set up SNMP trap configuration from Service SNMP.

If you select E-Mail in Alarm output, you need to set up SMTP configuration from Service SMTP.

| System > Alarm | |
|---|---|
| **Item** | **Description** |
| Mode | Turn on/off the Alarm configuration. Select from Disable or Enable. The default is Disable. |
| Alarm Input | ● **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.<br>● **VPN disconnect:** All tunnels get disconnected then trigger alarm.<br>● **WAN disconnect:** All WAN connections get disconnected then trigger alarm.<br>● **LAN disconnect:** All LAN connections get disconnected then trigger alarm.<br>● **Reboot:** Reboot then trigger alarm.<br>● **Geofence:** When moving device is touching the virtual perimeter then trigger alarm.<br>● **DI:** When device gets DI input then trigger alarm. |
| Alarm Output | Select from SMS, E-mail, SNMP trap and DO as alarm output. |
| SMS / E-mail | Write your messages and the messages limit 80 pure English characters or 20 characters for other languages to deliver. |
| DI Trigger | Set High or Low to trigger DI. |
| Do behavior | Set DO output behavior, always ON or pulse. |

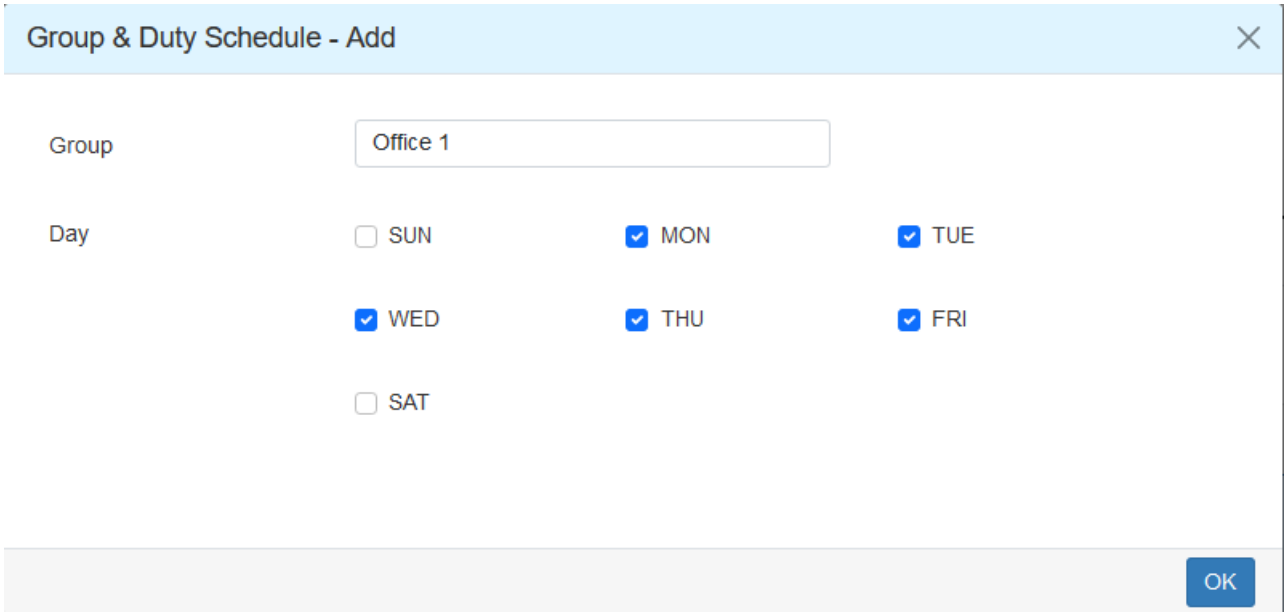
### 5.3.1 Alarm > Group > Create the Group

- Click **trusted and on duty members** to add trusted user who can send SMS message or receive the mail from device.

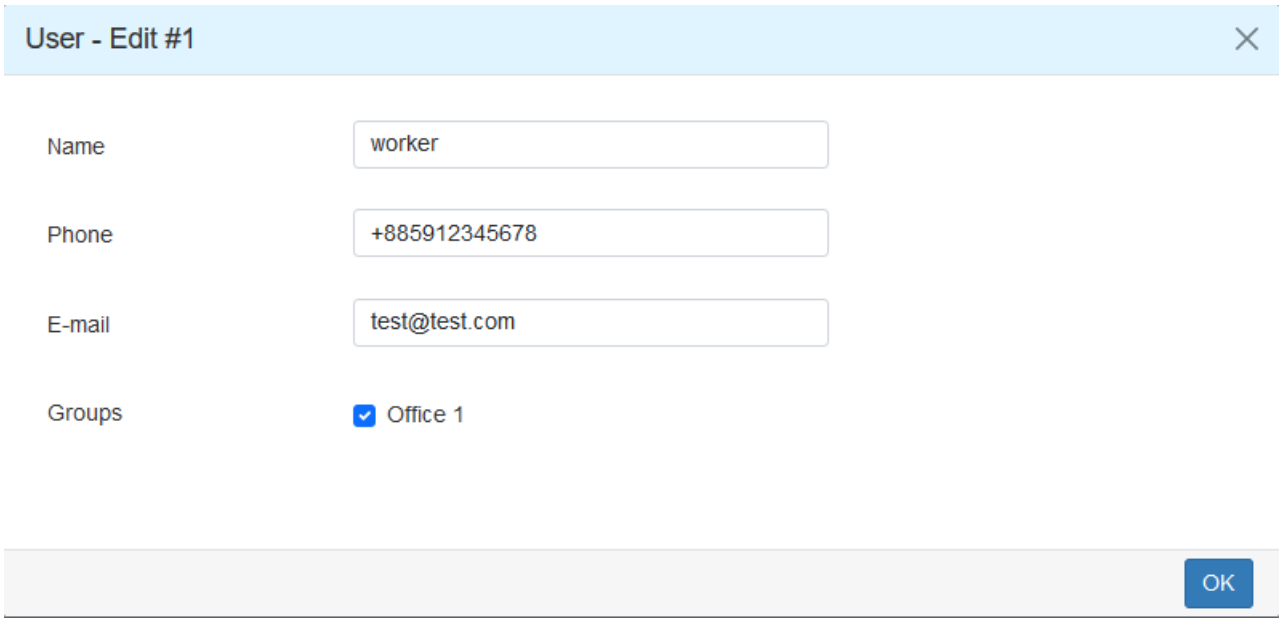

Firstly, we need to create the group and assign the duty day.

The settings below mean the user who only takes effect from Monday to Friday every week in-group “Office 1”.

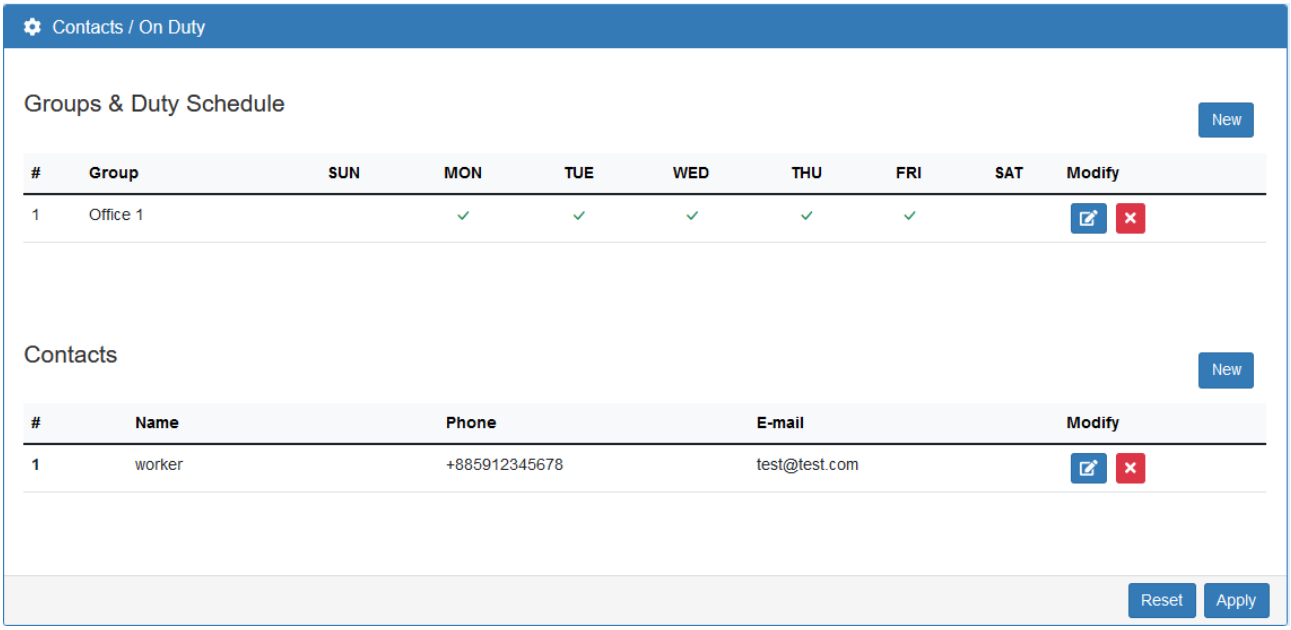



### 5.3.2 Alarm > Contacts > Add User

Once the group created, we need to create the new user and assign to the group we created. Device only accepts the phone number that specify here.




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.




## 5.4 Dying Gasp

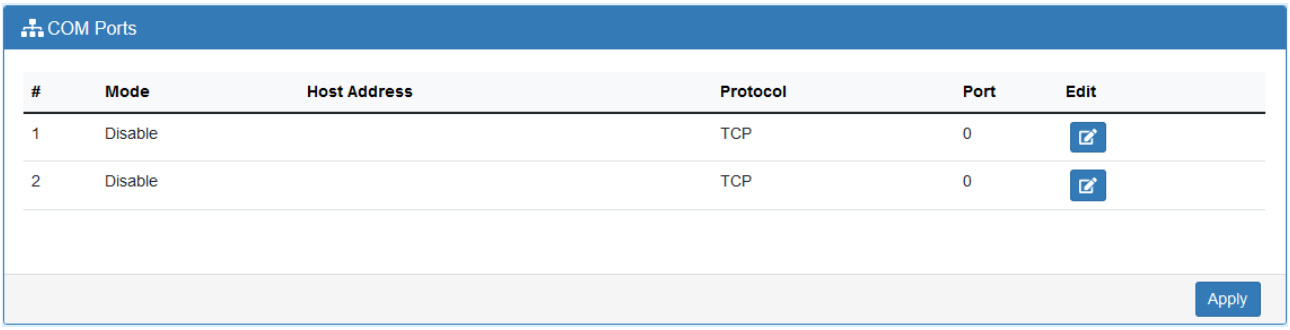
This section allows user to enable dying gasp for sending power lost message to O'smart IOT management system. Default is disable.


**Note:** This function is only valid when the alarm DI input is not checked and the device must connect with the dying gasp hardware box.

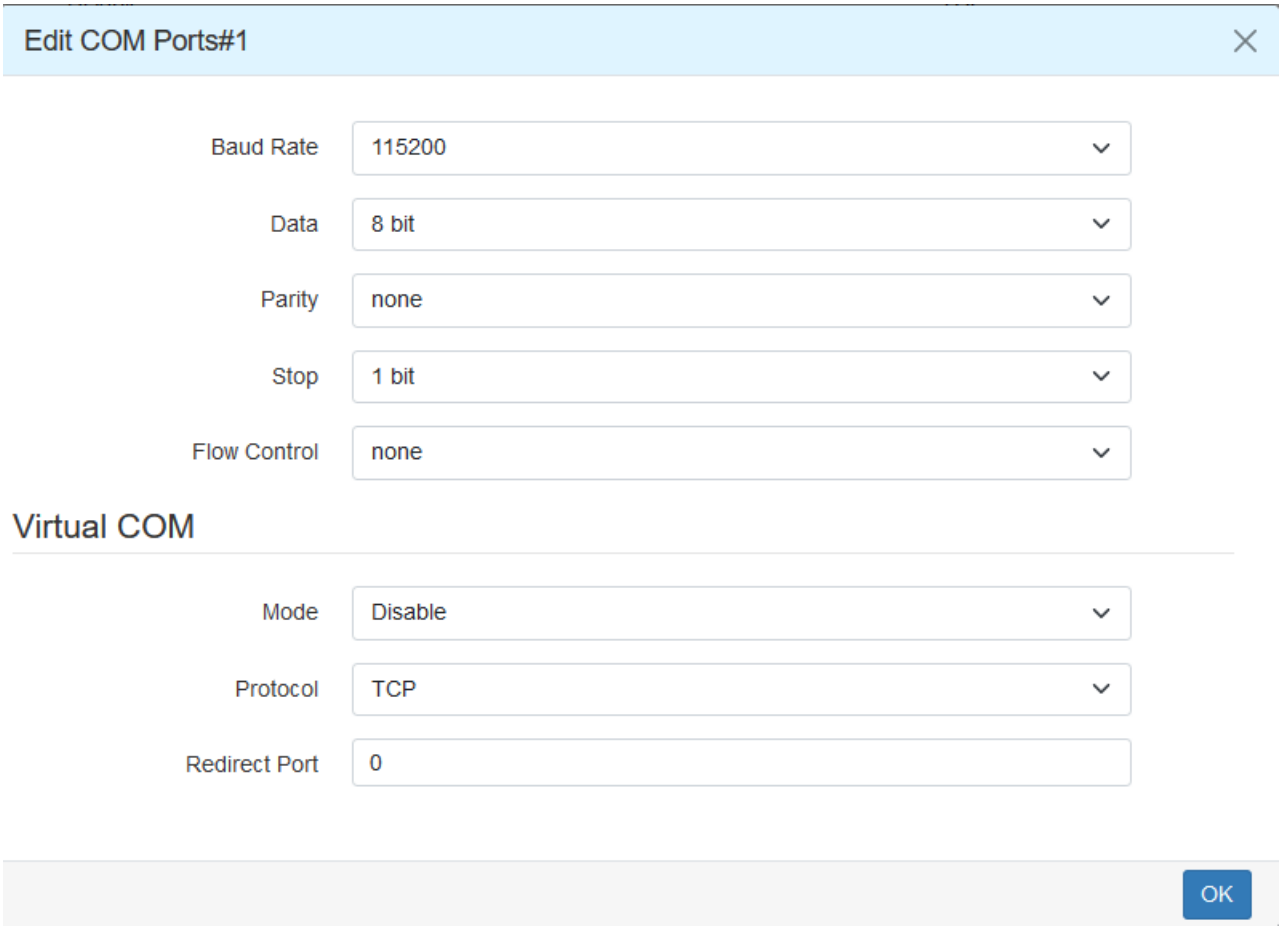
## 5.5 COM Ports

This section allows user to configure the COM port settings and remotely manage the device through the virtual COM setting. For the remote management, the managed device should connect to the cellular router by serial interface.

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




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



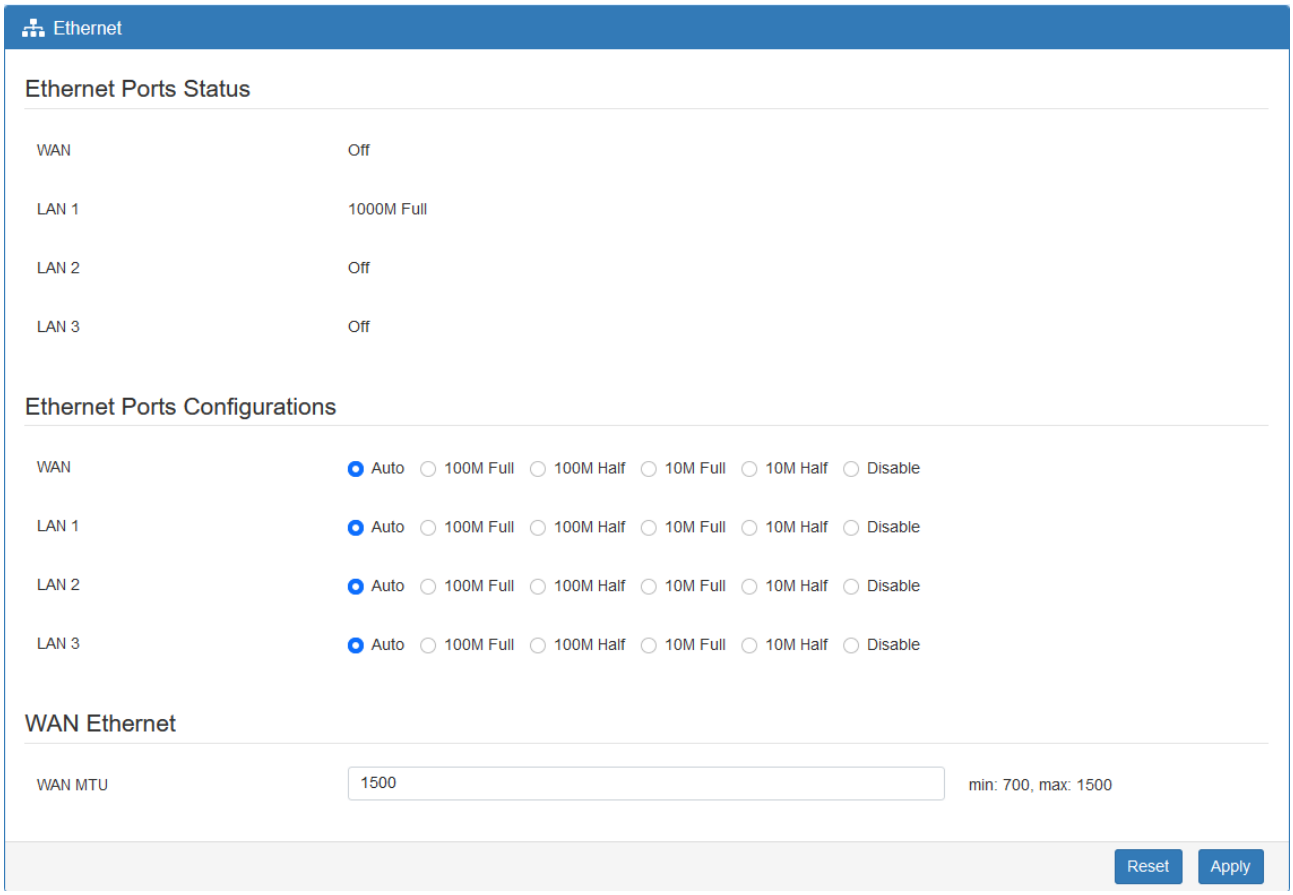

(3) The interface shows the setting information and click Apply to configure.

| System > COM Ports | |
|---|---|
| **Item** | **Description** |
| **Edit Configuration** | |
| **Baud Rate** | Select from the current Baud Rate. |
| **Data** | Select from 7 bit or 8 bit. |

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

## 5.6 Ethernet

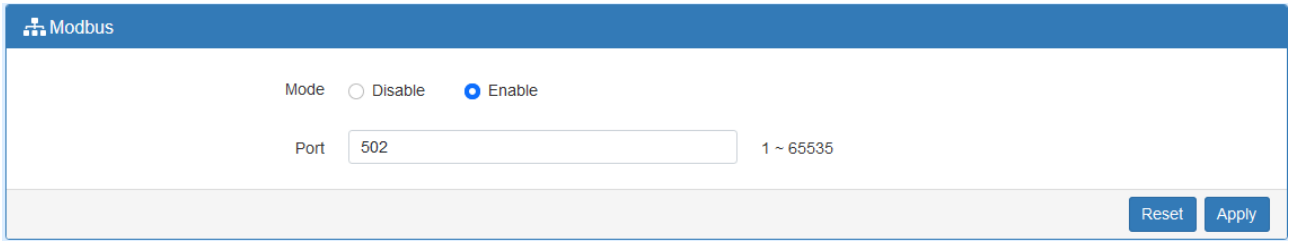
This section allows you to configure the Ethernet switch port.




| **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 | Allow user to configure the MTU size of Ethernet WAN port. |

## 5.7 Modbus

This section allows you to configure the Modbus.

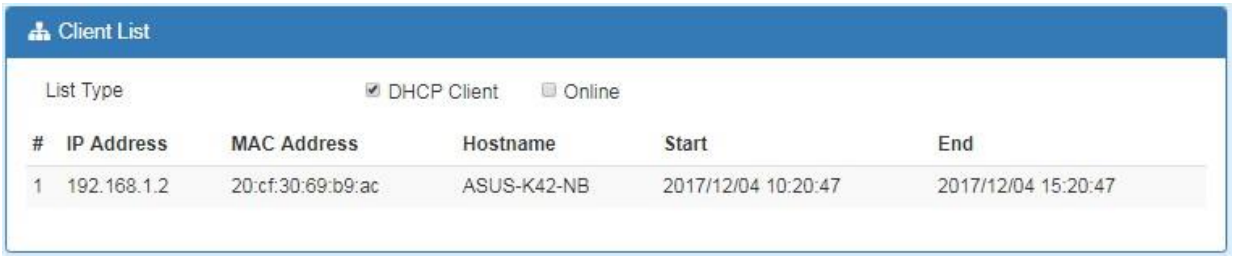



| System > Modbus | |
|---|---|
| **Item** | **Description** |
| **Mode** | Select from Disable or Enable. |
| **Port** | The listening port of Modbus TCP. |

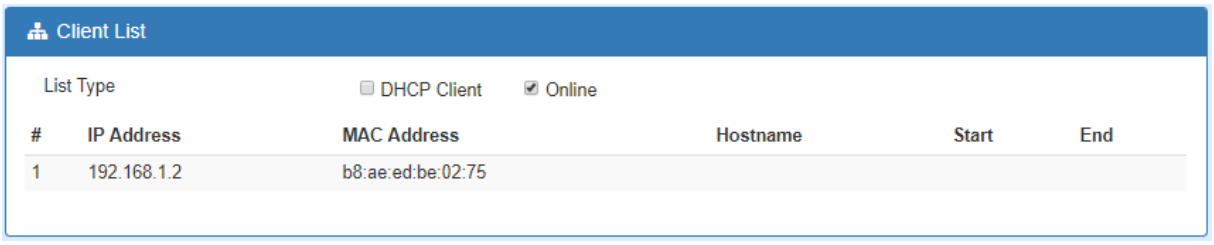
## 5.8 Client List

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

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



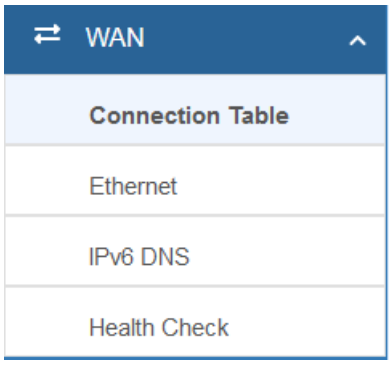

For **Online** type, the information shows IP address and MAC address when the client is online.




| System > Client List | |
|---|---|
| **Item** | **Description** |
| List Type | ● **DHCP Client:** List all clients' information when it is via DHCP.<br>● **Online:** List the information when it is online. |

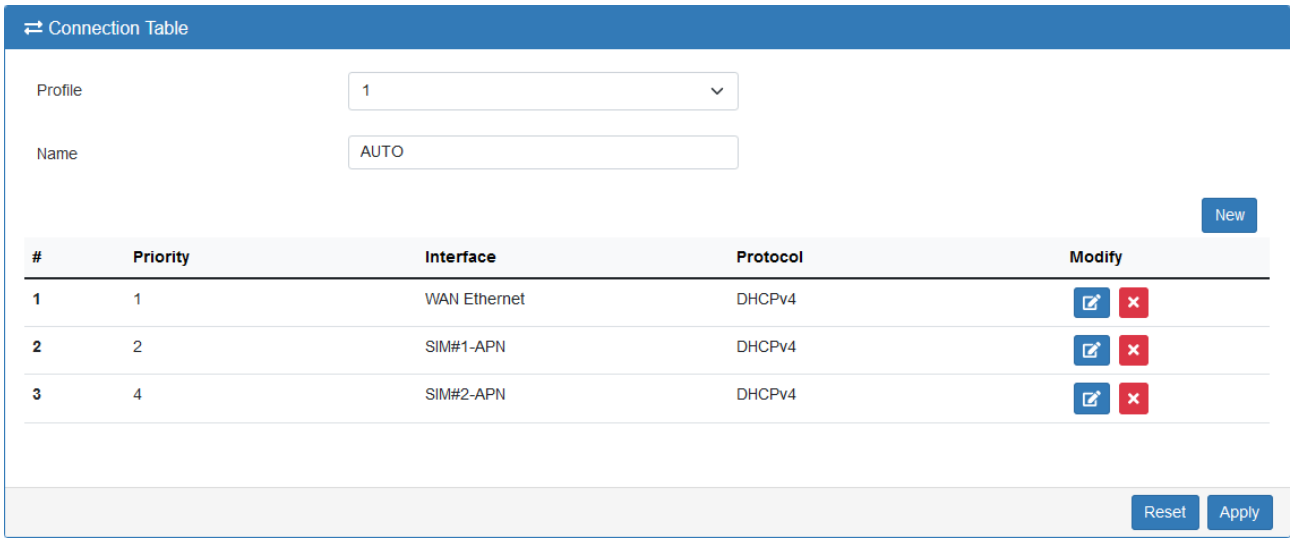
# 6 Web Menu Item > WAN

This section allows you to configure WAN, including Connection Table, IPv6 DNS, and Health Check.




## 6.1 Connection Table

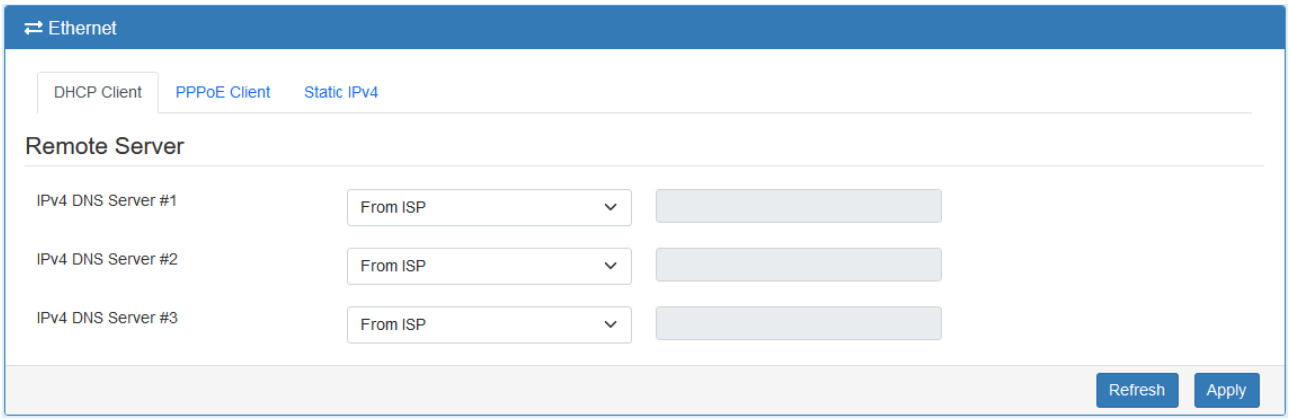
This section allows to configure the priority for Ethernet WAN and each APN of SIM slot.




| WAN > Connection Table | |
|---|---|
| **Item** | **Description** |
| Profile | Profile number. There are 3 profiles allow to set in advance. |
| Name | Name for profile |
| Priority | Interface priority for fail over operation. Only the highest priority interface is working. The other one is standby interface. |

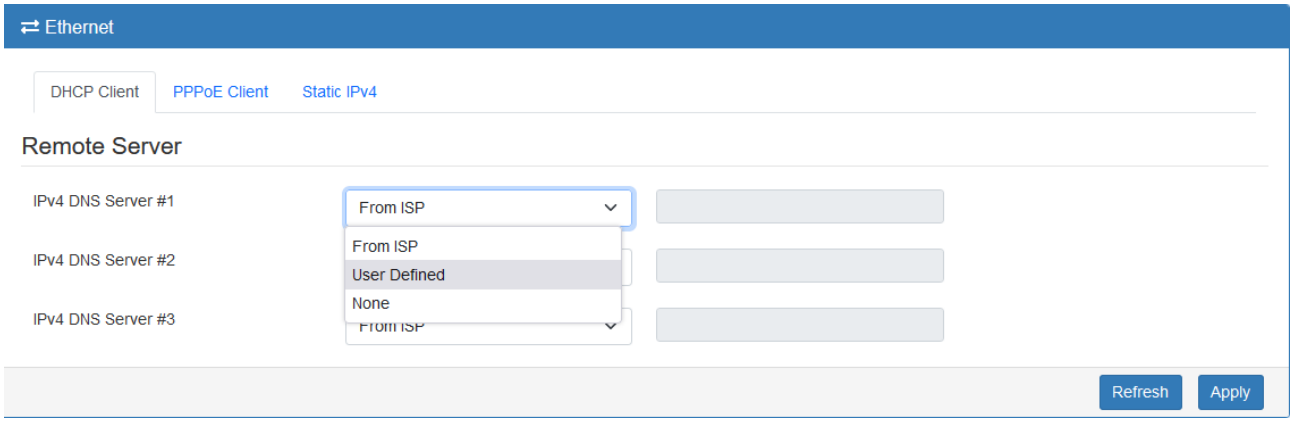
## 6.2 Ethernet

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




| WAN > Ethernet | |
|---|---|
| **Item** | **Description** |
| **WAN Ethernet** | • **DHCP Client:** DHCP server-assigned IP address, netmask, gateway, and DNS.<br>• **PPPoE Client:** Your ISP will provide you with a username and password. This option is typically used for DSL services.<br>• **Static IPv4:** User-defined IP address, netmask, and gateway address. |

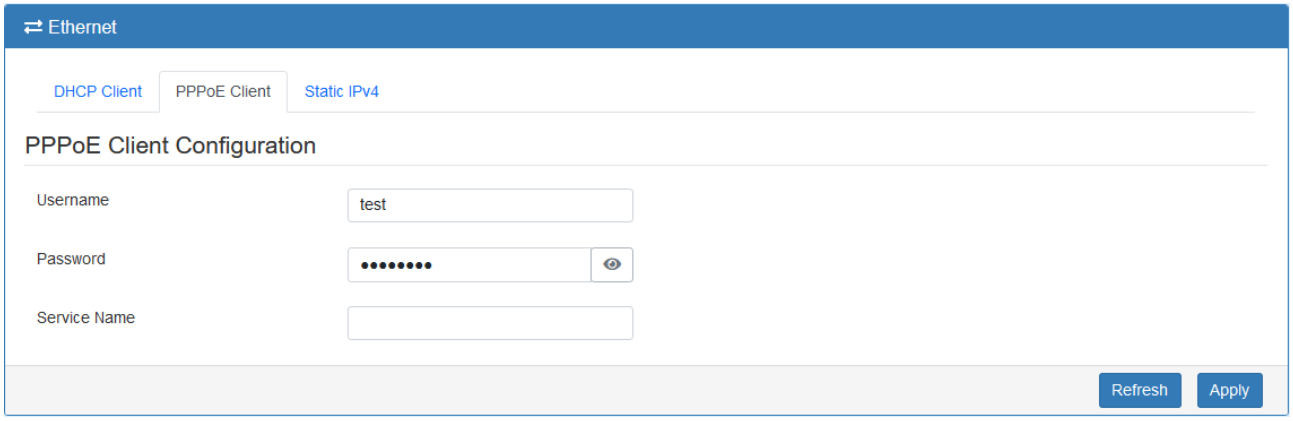
When selecting “DHCP Client”, you can set up DNS Server Configuration.
For IPv4 DNS Server, it provides three options to set up and each option has provided with “From ISP”, “User Defined” and “None” to configure.



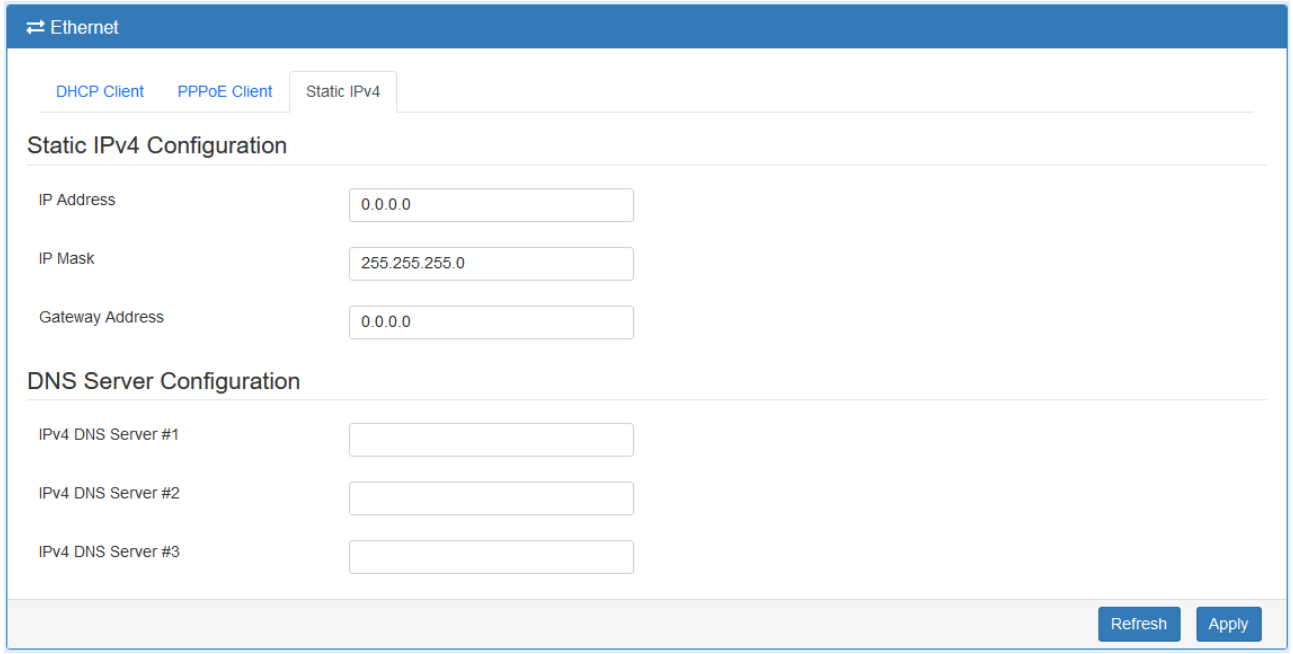

| WAN > Ethernet > DHCP Client | |
|---|---|
| **Item** | **Description** |
| **IPv4 DNS Server #1**<br>**IPv4 DNS Server #2** | • Each setting DNS Server has three options, including From ISP, User Defined and None.<br>• When you select From ISP, the IPv4 DNS server IP will be assigned by ISP. |

| | |
|---|---|
| **IPv4 DNS Server #3** | • When you select User Defined, user inputs the IPv4 DNS server IP manually. |

When you select PPPoE Client, the interface shows the item of configuration to fill in your User Name and Password. Service name is an option setting.




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

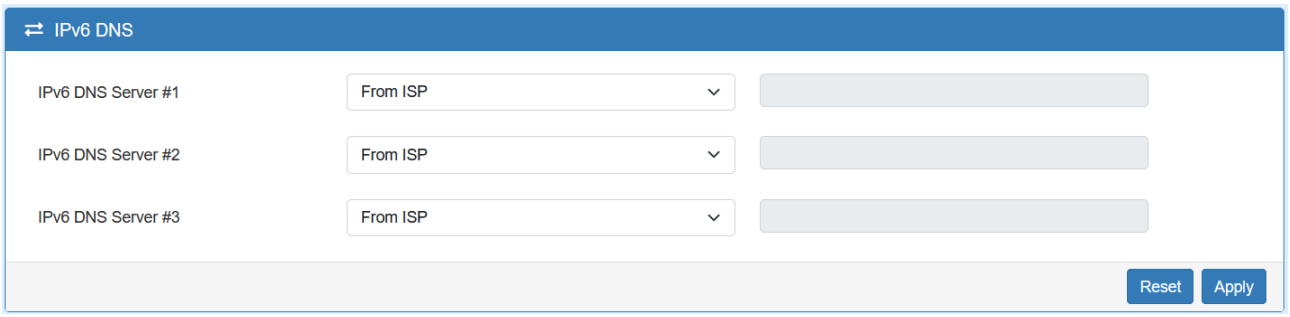



| **WAN > Ethernet > Static IPv4** | |
|---|---|
| **Item** | **Description** |
| **Static IPv4 Configuration** | |
| **IP Address** | Fill in the IP Address. |
| **IP Mask** | Fill in the IP Mask. |
| **Gateway Address** | Fill in Gateway Address. |
| **DNS Server Configuration** | |
| **IPv4 DNS Server #1~3** | User can enter the IPv4 DNS server IP manually. |

## 6.3 IPv6 DNS

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

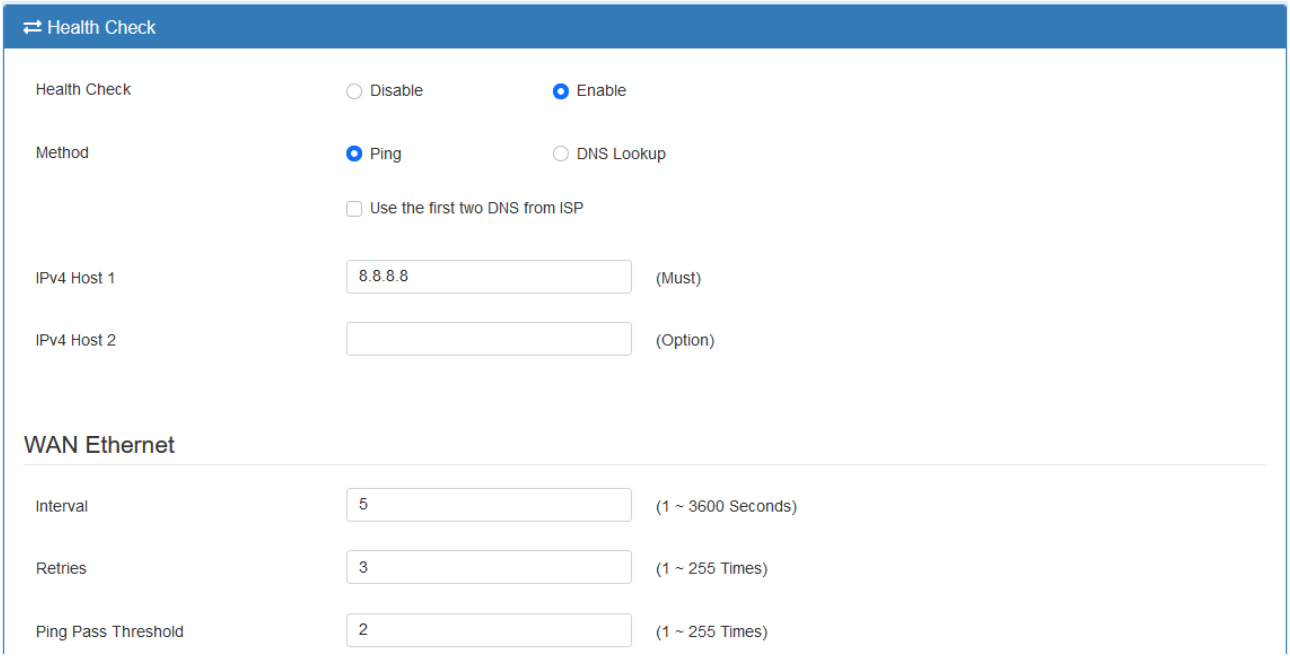
For IPv6 DNS Server, it provides three options to set up and each option has provided with “From ISP”, “User Defined” and “None” to configure.




| WAN > IPv6 DNS | |
|---|---|
| **Item** | **Description** |
| IPv6 DNS Server #1<br>IPv6 DNS Server #2<br>IPv6 DNS Server #3 | Each setting DNS Server has three options, including From ISP, User Defined and None.<br>When you select From ISP, the IPv6 DNS server IP will assign by ISP.<br>When you select User Defined, the IPv6 DNS server IP is enter by user self. |

## 6.4 Health Check

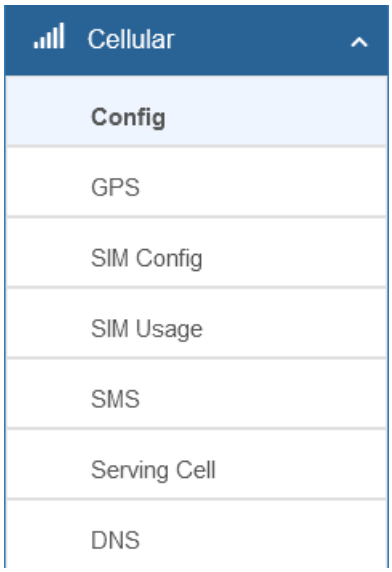
This section allows user to configure the WAN healthy check for failover function between different APN of SIM slot and Ethernet WAN.




| **WAN > Health Check** | |
|---|---|
| **Item** | **Description** |
| Health Check | • Select from Disable or Enable. The default is Enable.<br>• When Disable is chosen, the connection will NOT be treated as down of IP routing error. |
| Method | This setting specifies the health check method for the WAN connection. This Value can be PING, DNS Lookup. The default is Ping.<br>DNS Lookup: Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result. |
| Use the first two DNS from ISP | • If this setting is checked, the first two DNS from ISP will be DNS lookup targets for checking a connection health.<br>• If this setting is not checked, Host 1 must be filled, while a value for Host 2 is optional. |
| IPv4 Host 1 | Input the address of IPv4 Host 1. |
| IPv4 Host 2 | Input the address of IPv4 Host 2. This field is optional. |
| Interval | Set the interval time to ping WAN Ethernet. The interval is from 1 to 60 seconds. |
| Retries | Retry time for the check. |
| Ping Pass Threshold | The threshold value of successful check to think WAN interface is OK. |

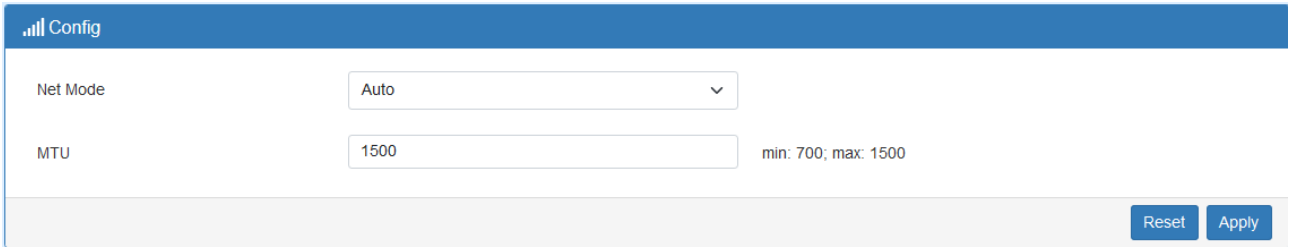
# 7 Configuration > Cellular

This section allows you to configure the LTE Config, GPS, APN, APN1/2 Usage, SMS, Serving Cell, and DNS.




## 7.1 Config

This page allows to setup cellular net mode and MTU size.



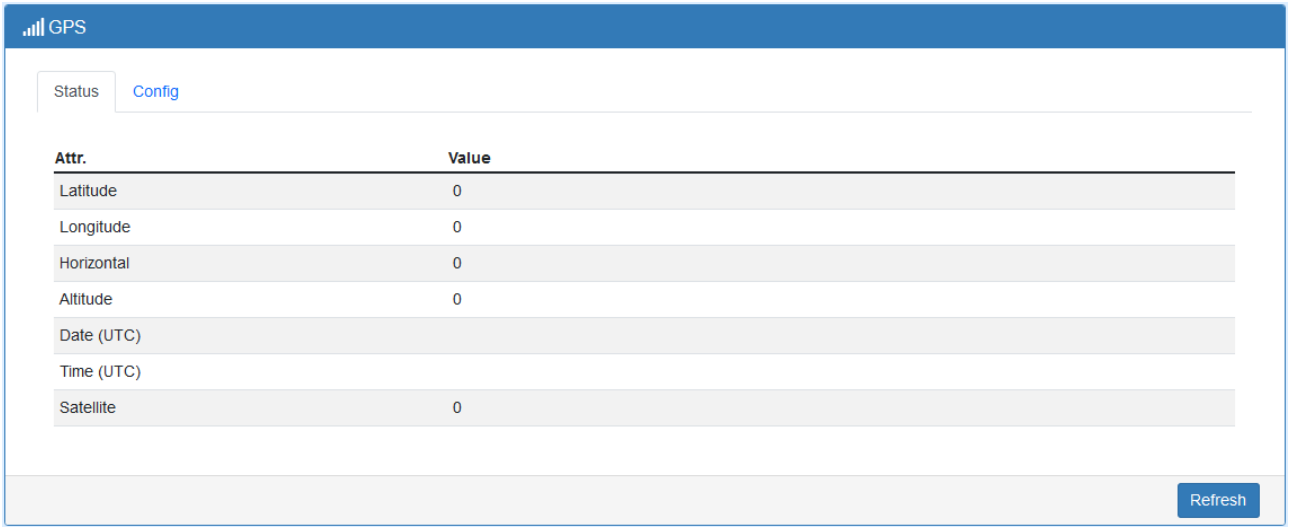

| Cellular > Config | |
|---|---|
| **Item** | **Description** |
| Net Mode | Auto: Automatically connect the possible band.<br>4G Only: Connect to 4G network only.<br>3G Only: Connect to 3G network only.<br>2G Only: Connect to 2G network only. |
| MTU | MTU is the Maximum Transmission Unit that can send over the cellular interface. It allows user to adjust the MTU size to fit into their existing network environment. |

## 7.2 GPS

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

## Status

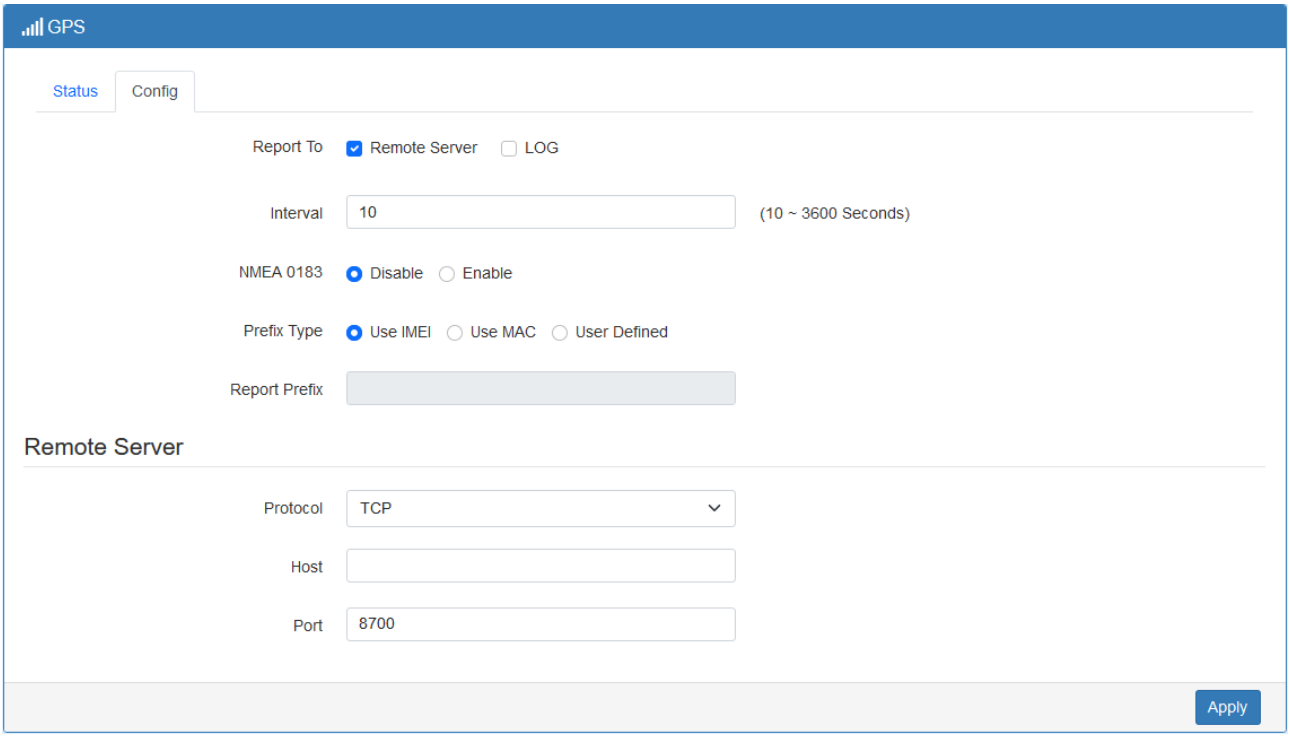
In the status tab, it shows the current location of device.




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

## Config

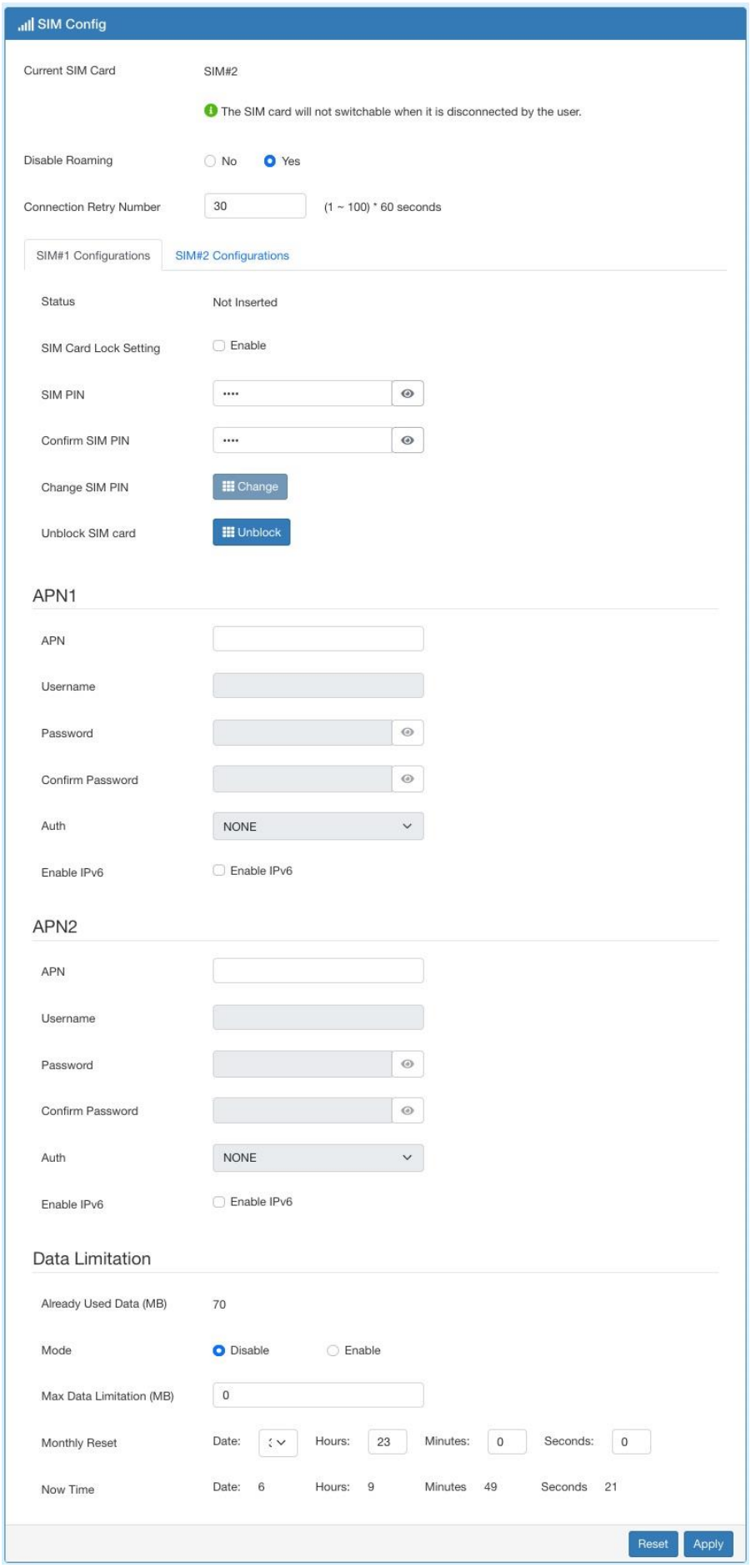
This section allows you to set up GPS configuration and send out GPS location to TCP Server or display in log.




| LTE > GPS > Config | |
|---|---|
| **Item** | **Description** |
| **Report to** | Select from Remote Server or LOG sever |
| **Internal** | Query GPS interval. |
| **NMEA 0183** | Report in NMEA 0183 format. If enabled, no further prefix is allowed |
| **Prefix Type** | If NMEA0183 is disabled, you can add prefix to identify the device |
| **Protocol** | Report GPS message via TCP or UDP |
| **Host** | Host IPv4 address |
| **Port** | Host port number (Default 8700) |

## 7.3 SIM Config

This section allows user to setup configuration for the SIM card.


SIM Config
Current SIM Card
SIM#2
The SIM card will not switchable when it is disconnected by the user.
Disable Roaming
No
Yes
Connection Retry Number
30
(1 ~ 100) * 60 seconds
SIM#1 Configurations
SIM#2 Configurations
Status
Not Inserted
SIM Card Lock Setting
Enable
SIM PIN
Confirm SIM PIN
Change SIM PIN
Change
Unblock SIM card
Unblock
APN1
APN
Username
Password
Confirm Password
Auth
NONE
Enable IPv6
Enable IPv6
APN2
APN
Username
Password
Confirm Password
Auth
NONE
Enable IPv6
Enable IPv6
Data Limitation
Already Used Data (MB)
70
Mode
Disable
Enable
Max Data Limitation (MB)
0
Monthly Reset
Date:
Hours:
23
Minutes:
0
Seconds:
0
Now Time
Date: 6
Hours: 9
Minutes 49
Seconds 21
Reset
Apply

| Cellular > SIM Config | |
|---|---|
| **Item** | **Description** |
| Current SIM Card | It shows the current used SIM card.<br>● **Disconnect:** When getting connection, the Disconnect button appear. After manually click Disconnect, the system would not automatically get connection until next reboot.<br>● **Connect:** After manually disconnect, it will show Connect button. Click to get connection or reboot the device to make it automatically connect. |
| Disable Roaming | ● **No:** Enable the roaming function.<br>● **Yes:** Disable the roaming function. |
| Connection Retry Number | The number of attempts to connect to the network. The interval between each attempt is 60 seconds. |
| **SIM#1 & SIM#2 Configurations** | |
| Status | Display the status of SIM Card. |
| SIM Card Lock Setting | ● Enable to display SIM PIN setting.<br>● Disable to hide SIM PIN setting. |
| SIM PIN | A password personal identification number (PIN) for ordinary use to protect your SIM card. |
| Confirm SIM PIN | Double confirm SIM PIN password. |
| 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). |
| Unblock SIM card | 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. |
| **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. |
| Username | Username for authentication. The username can be input by user or the system will search from internal database if the APN setting is empty. |
| Password | Password for authentication. 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 | Select the authentication method (None/PAP/CHAP). |
| Enable IPv6 | If IPv6 is not selected, then only pure IPv4 connection. |
| **Data Limitation** | |
| Already Used Data (MB) | Display current used Data since last reset. |

| | |
|---|---|
| Mode | Turn on/off the Data Limitation to disable or enable. |
| Max Data Limitation (MB) | Configure maximum Data Limitation. |
| Monthly Reset | Set up the reset time during the month. |
| Now Time | Show the current time of system. |

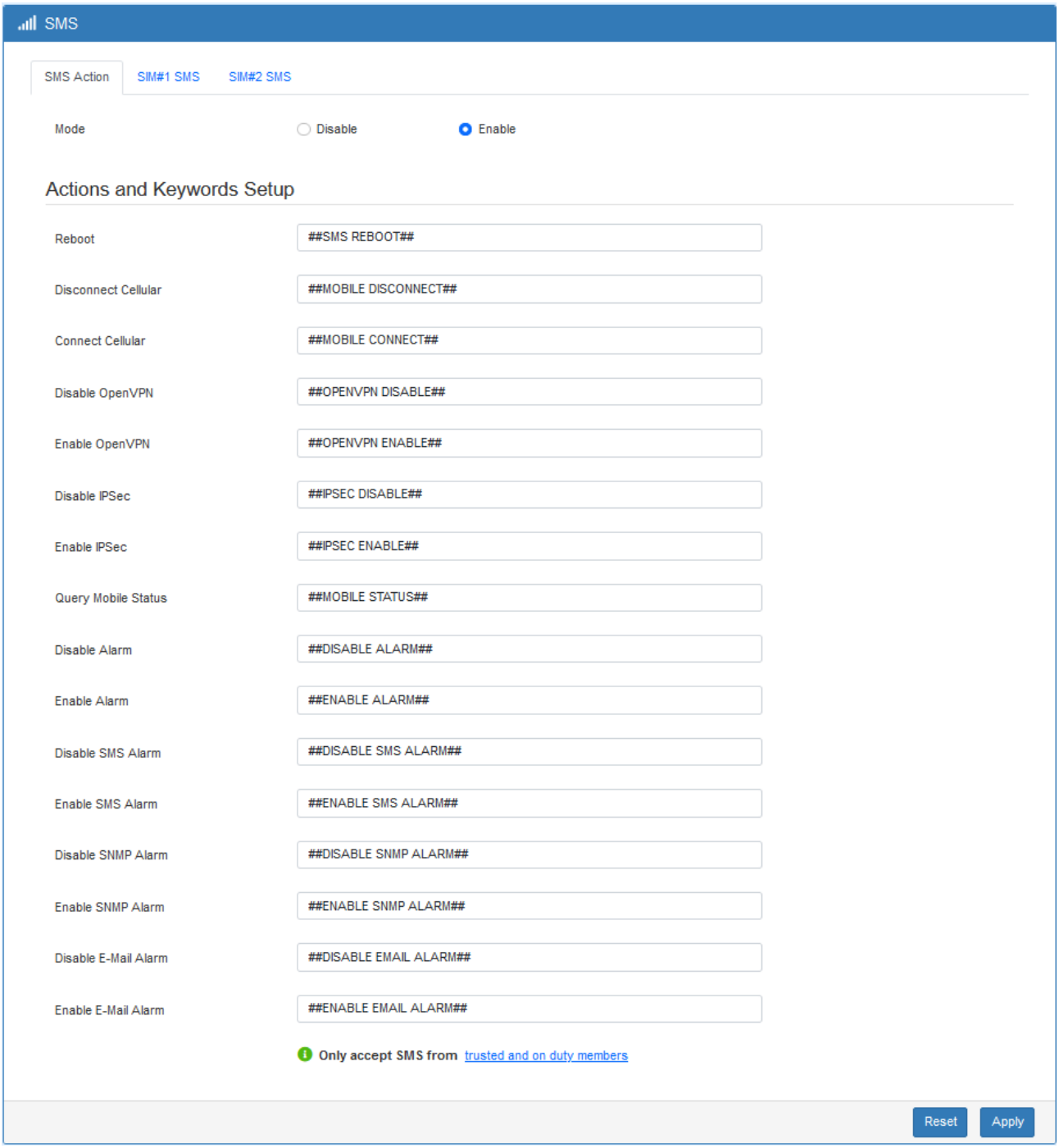
## 7.4 SIM Usage

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

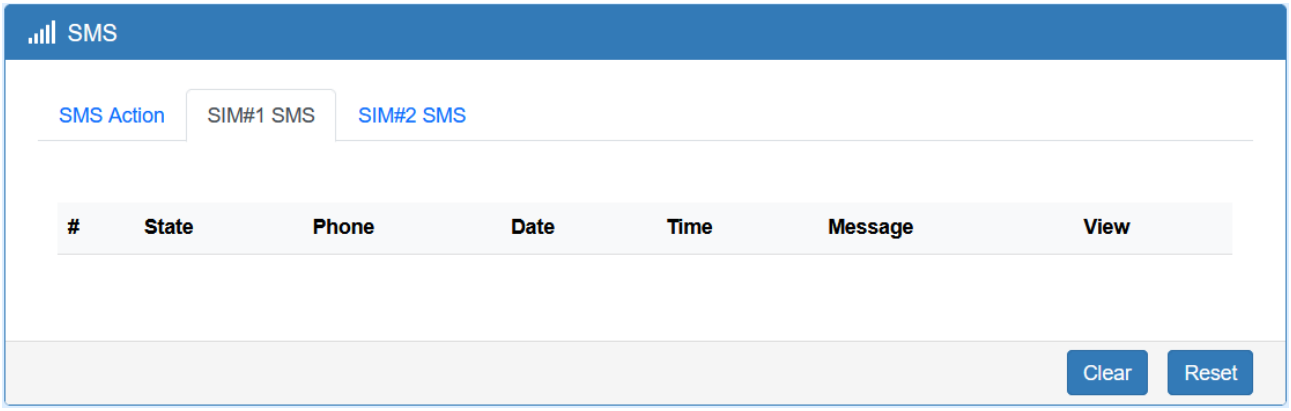
## 7.5 SMS

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

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



**(2)** **SIM#1 and SIM#2 SMS** allows you to review the information of SMS that you have received, including the state, phone, date and time. You can click  button to view the whole message, click Refresh button to reload the messages, or click Clear button to remove all read messages.

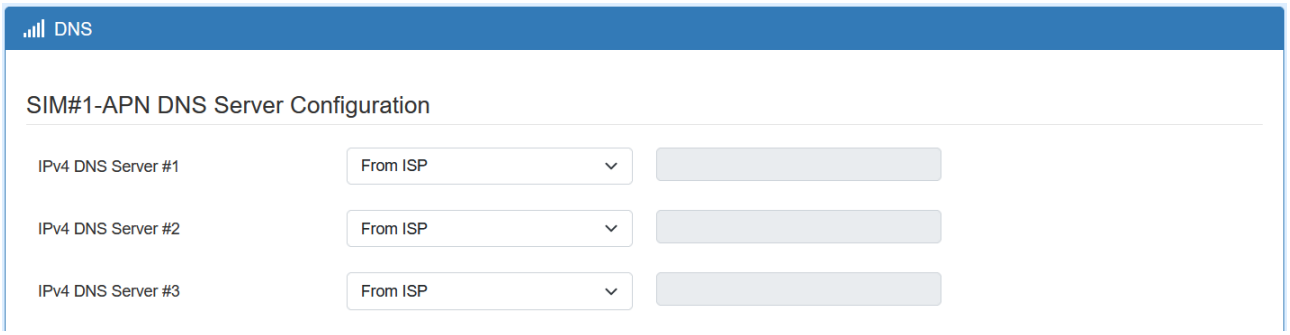



## 7.6 Serving Cell

This section displays the information of Serving Cell, including the following items.

## 7.7 DNS

This section allows you to set specific DNS server setting.



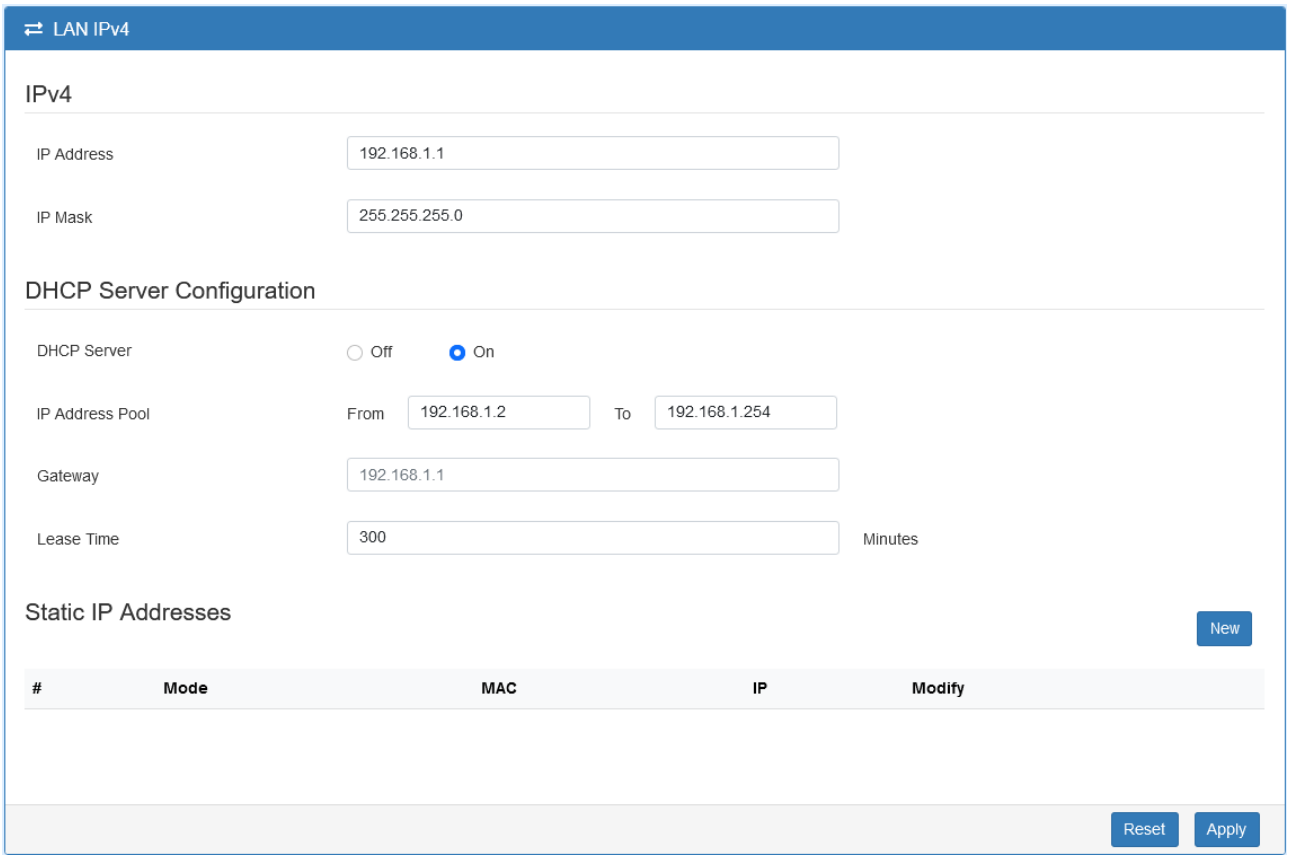

| Cellular > DNS | |
|---|---|
| **Item** | **Description** |
| IPv4 DNS Server #1<br>IPv4 DNS Server #2<br>IPv4 DNS Server #3 | There are three options, including From ISP, User Defined and None.<br>When you select From ISP, the IPv4 DNS server IP will assign from ISP.<br>When you select User Defined, the IPv4 DNS server IP is enter by user self. |

# 8 Web Menu Item > LAN

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


## 8.1 IPv4

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



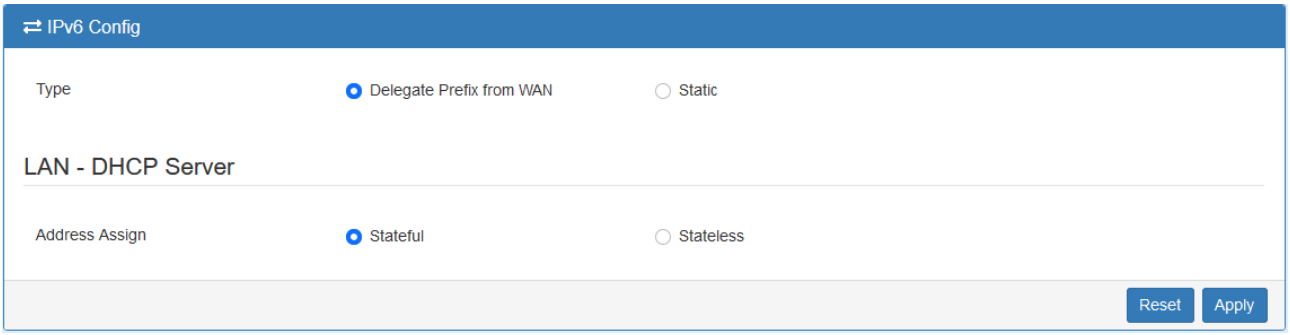
| LAN > IPv4 | |
|---|---|
| **Item** | **Description** |
| LAN IPv4 | IP Address:192.168.1.1<br>IP Mask:255.255.255.0<br>Both of them are default, you can change them according to your local IP Address and IP Mask. |
| DHCP Server Configuration | Turn on/off DHCP Server Configuration.<br>Enable to make 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. |
| Gateway | Define the gateway IP address that will assign to DHCP clients. |
| Lease Time | Define the lease time for DHCP clients. |
| Static IP Addresses | DHCP server support static IP address assignment.<br>The static IP address can add by clicking the **New** button.<br>Each static IP consist of mode (on/off), MAC and IP address.<br>Mode: Turn on/off the static IP address.<br>MAC: The MAC address of target host or PC.<br>IP: The desired IP address for target host or PC. |

# 9 Web Menu Item > IPv6

This section allows you to configure the LAN IPv6.


## 9.1 IPv6 Config

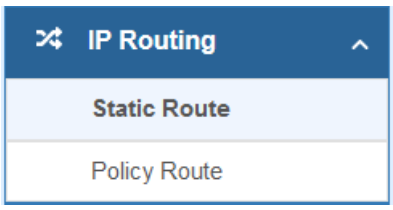
Select your type of IPv6, which shows **Delegate Prefix from WAN** or **Static,** and then set up DHCP Server Configuration.




| **LAN > IPv6** | |
|---|---|
| **Item** | **Description** |
| Type | ● **Delegate Prefix from WAN**<br>Select this option to obtain an IPv6 network prefix automatically from the service provider or an uplink router.<br>● **Static**<br>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.<br>● **Stateful**: The cellular router uses IPv6 stateful auto configuration. The LAN IPv6 clients can obtain IPv6 addresses through DHCPv6.<br>● **Stateless:** The cellular router uses IPv6 stateless auto configuration. RADVD (Router Advertisement Daemon) is enable to have the cellular router send IPv6 prefix information in router advertisements periodically and in response to router solicitations. |

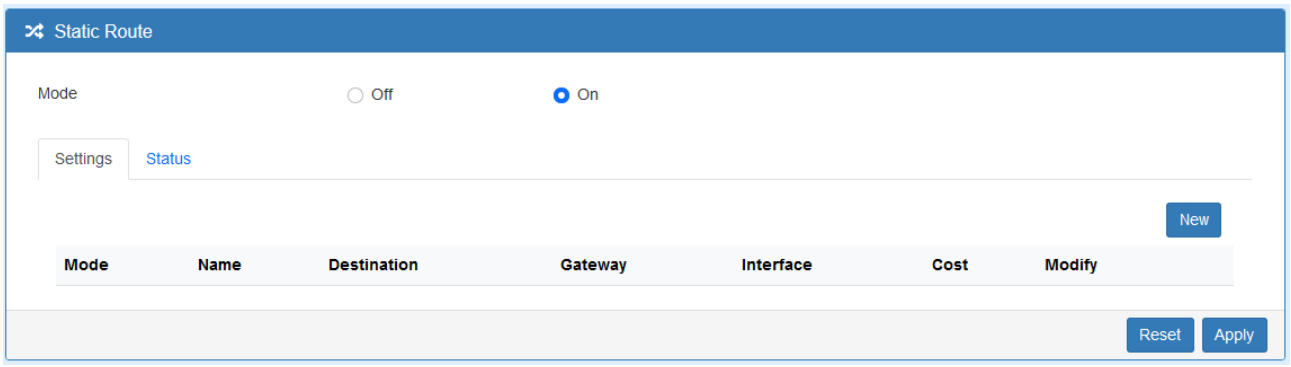
# 10 Web Menu Item > IP Routing

This section allows you to configure the Static Route and Policy Route.

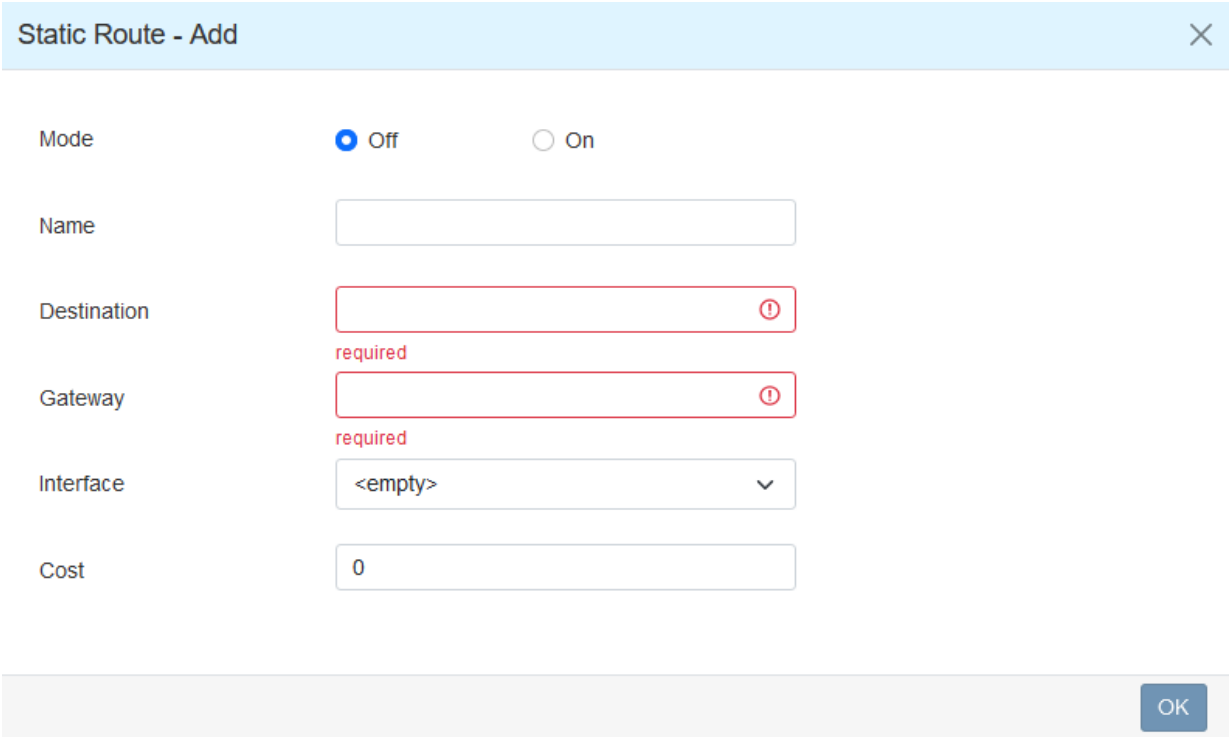



## 10.1 Static Route

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.




Click the **New** button to add the static route.

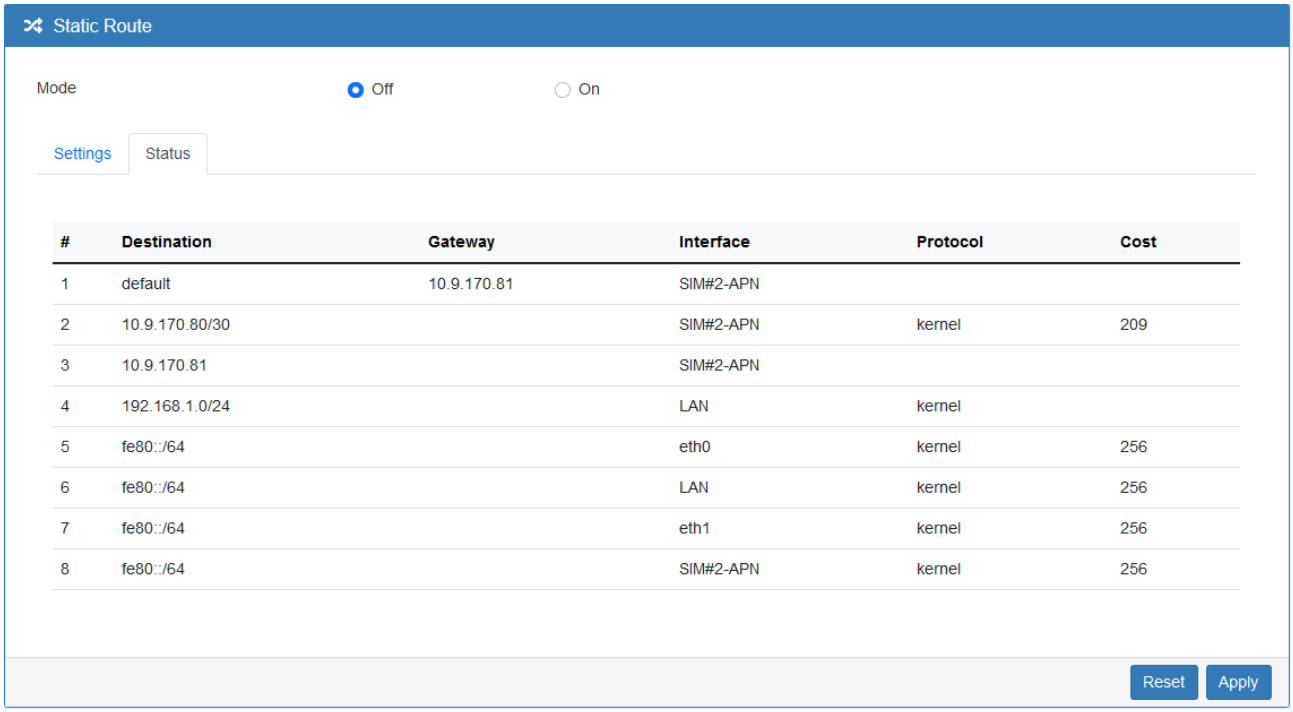


| IP Routing > Static Route | |
|---|---|
| **Item** | **Description** |
| Mode | The setting is to enable or disable the static route for full network. |
| **Settings** | |
| Mode | The setting is for the specific network. Select Off or On. |
| Name | Set up each name for your running host or network. |
| 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. |
| Cost | Cost is a policy for router to commit router, to determine the optimal route.<br>Enter one number greater than or equal to 0. |

***Note:***

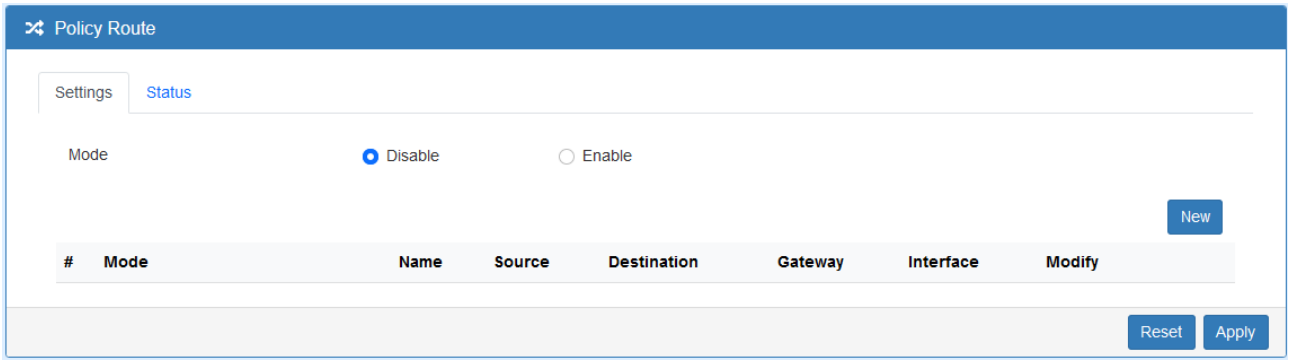
- The destination field is required to fill in. The format of destination is IPv4 or IPv6.
- The address of gateway or the type of interface can chose one or both to fill in the field.

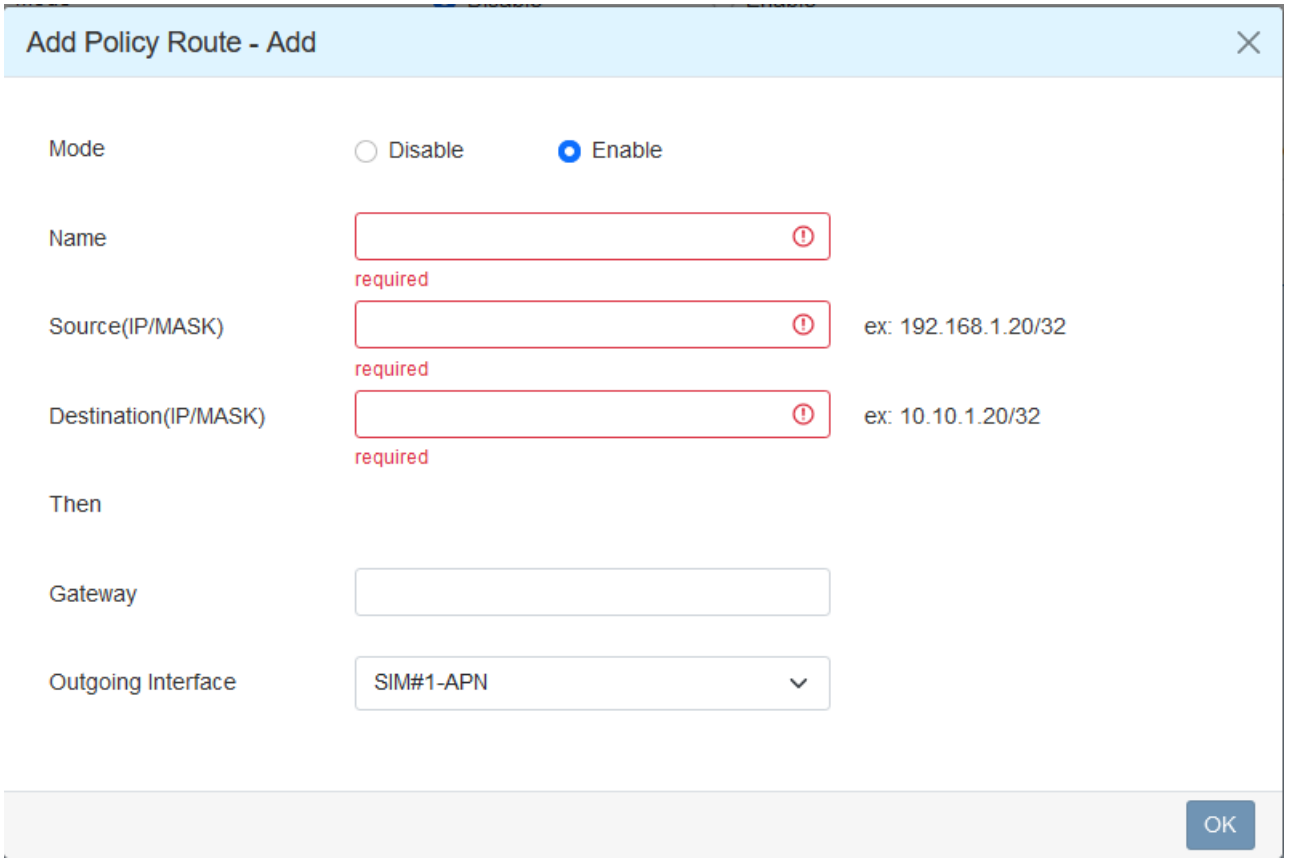
The status tab shows the information from the settings of static route.



## 10.2 Policy Route

This section allows user to setup the policy route and check the status of policy route settings. Policy routing works on the activated interfaces only, but disabled on deactivated interfaces automatically.

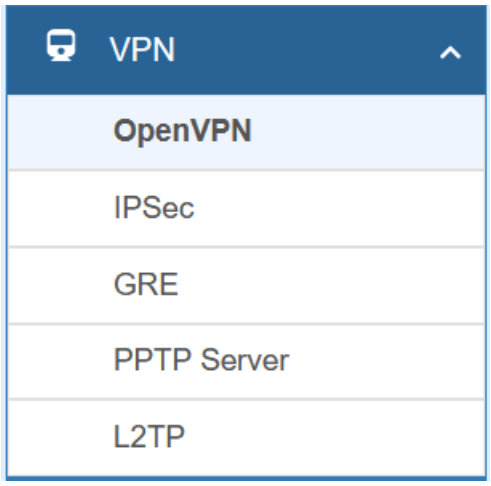


| IP Routing > Policy Route | |
|---|---|
| **Item** | **Description** |
| Mode | Enable or disable the policy route function. |
| **Settings** | |
| Mode | Enable or disable the selected policy route entry. |
| Name | Set up each name for your running host or network. |
| Source(IP/MASK) | Fill in the source of a specific IP/MASK from network. |
| Destination(IP/MASK) | Fill in the destination of a specific IP/MASK from network. |
| Gateway | Fill in the gateway address of your router. |
| Outgoing Interface | Select the outgoing interface. |

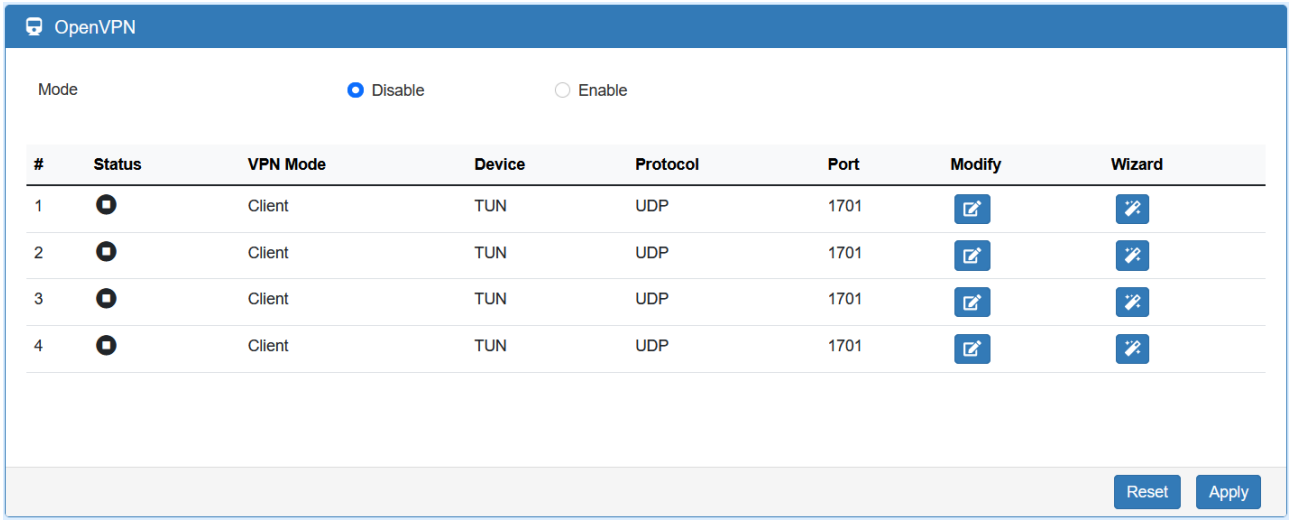
# 11 Web Menu Item > VPN

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




## 11.1 OpenVPN

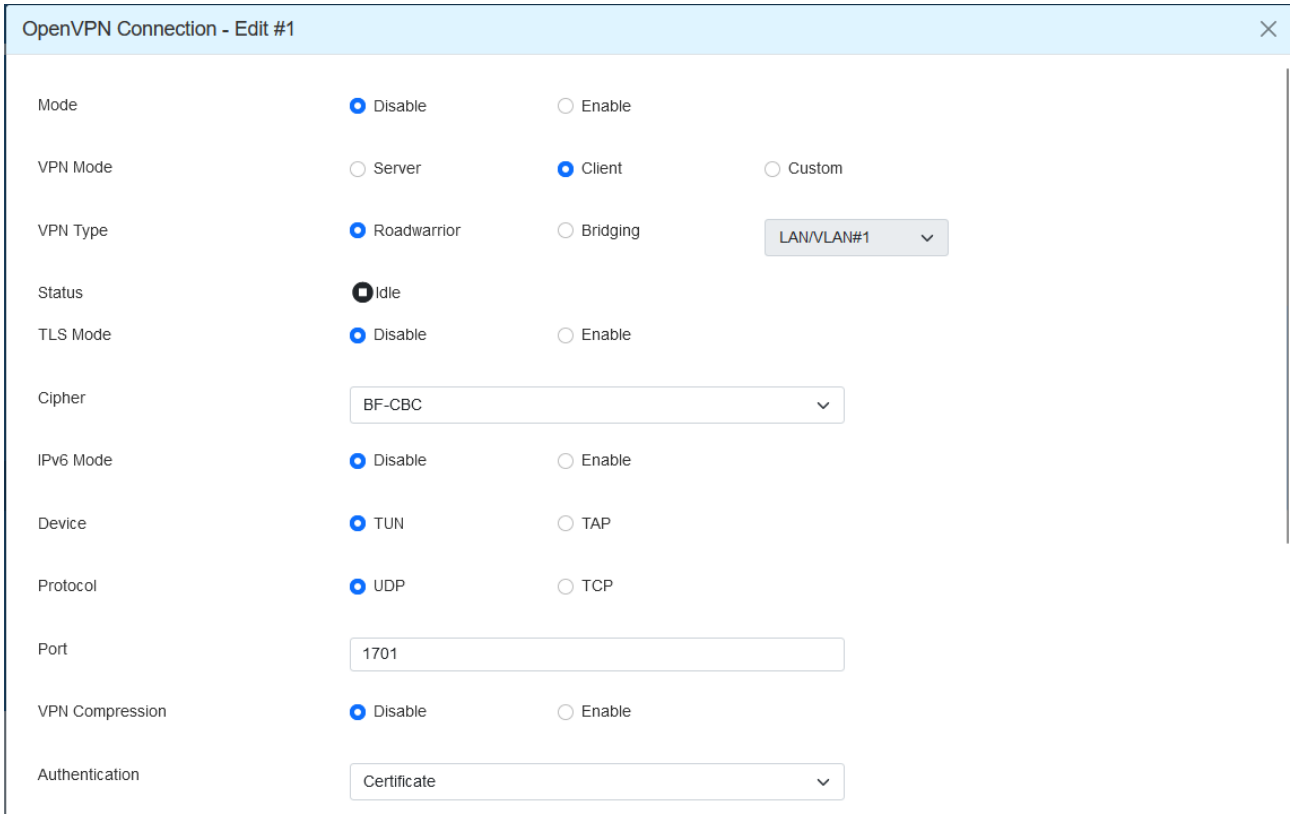
This section allows you to set up the connection of OpenVPN. The default mode is Disable. From **Log** tab, the interface will show the status of connection to make you follow the situation whenever it is successful or fail connection.



### 11.1.1 OpenVPN Common Setting

(1) Click  button to edit OpenVPN Connection.

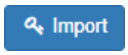
(2) From **Setting** tab, you can set up the connection of OpenVPN.



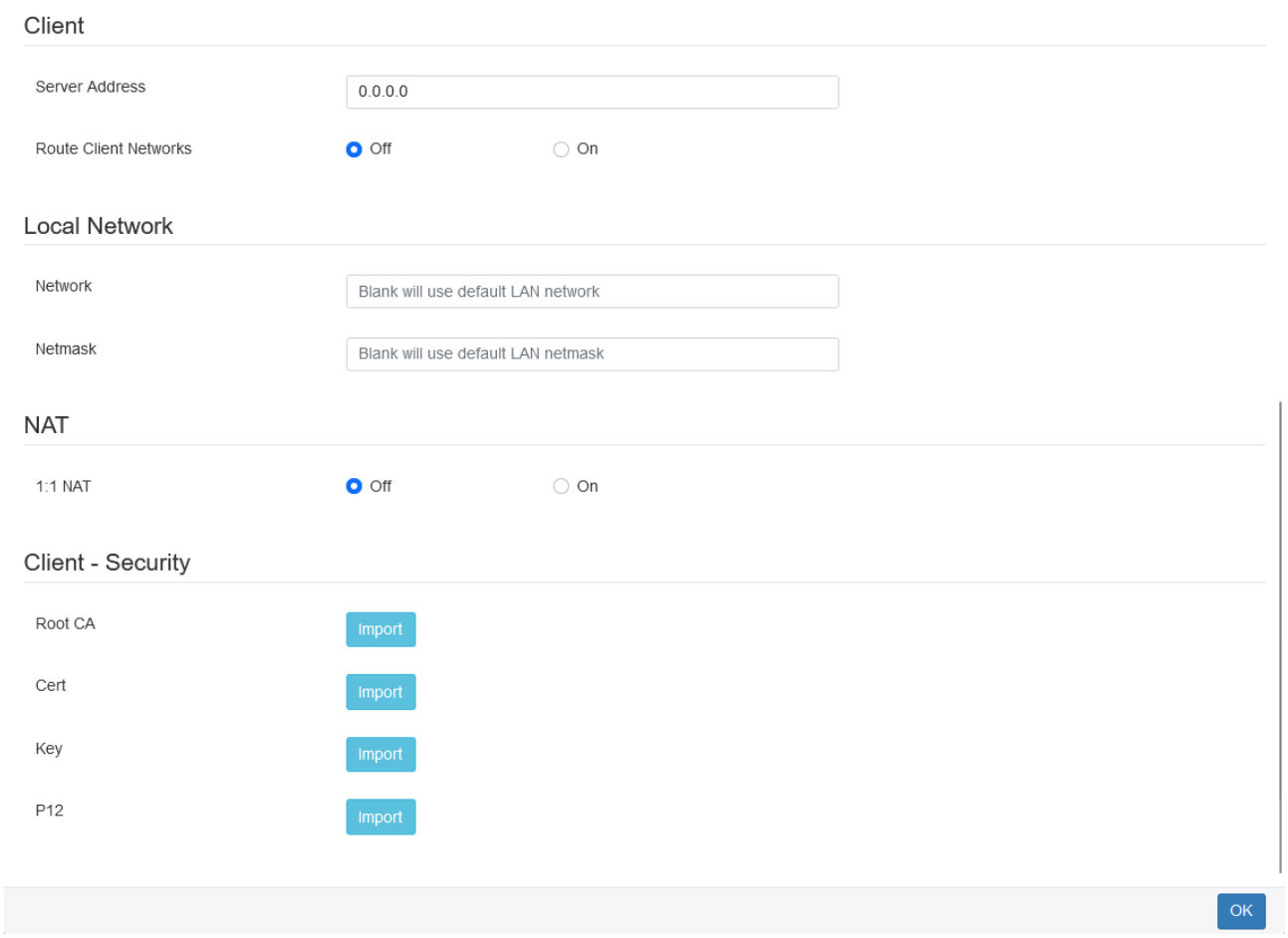
| VPN > OpenVPN > Setting | |
|---|---|
| **Item** | **Description** |
| Mode | Turn on/off OpenVPN to select Disable or Enable. |
| VPN Mode | Server: Tick to enable OpenVPN server tunnel.<br>Client: Tick to enable OpenVPN client tunnel. The default is Client.<br>Custom: This option allows user to use the .ovpn configuration file to set up VPN tunnel quickly with third-party server or use the OpenVPN advanced options to be compatible with other servers. |
| VPN Type | Roadwarrior (default)<br>Bridging: Bridging the VPN tunnel and LAN/VLAN |
| Status | Display the status of OpenVPN. |
| TLS Mode | Select from Disable or Enable for data security. The default is Disable. |
| Cipher | The OpenVPN 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 that depends on the application. The default is UDP. |
| Port | Enter the listening port of remote side OpenVPN 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.<br>The pkcs#12 option is only available on the VPN client mode. |

### 11.1.2 OpenVPN Client Setting

Select option "**Client**" from VPN Mode, and this section allows you configure the **OpenVPN client** and authentication files.

The files can import by clicking 

button and the file should download from OpenVPN server.

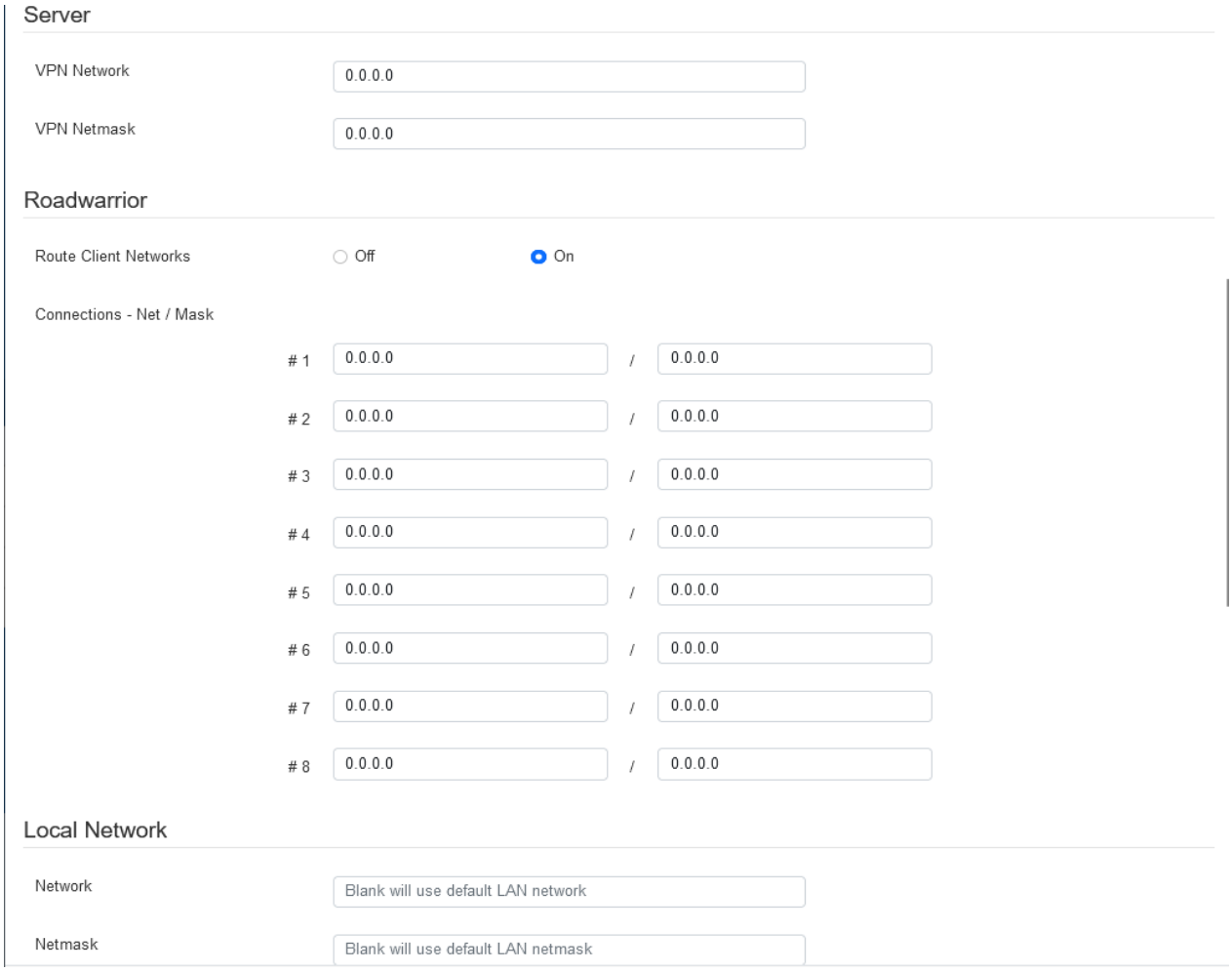


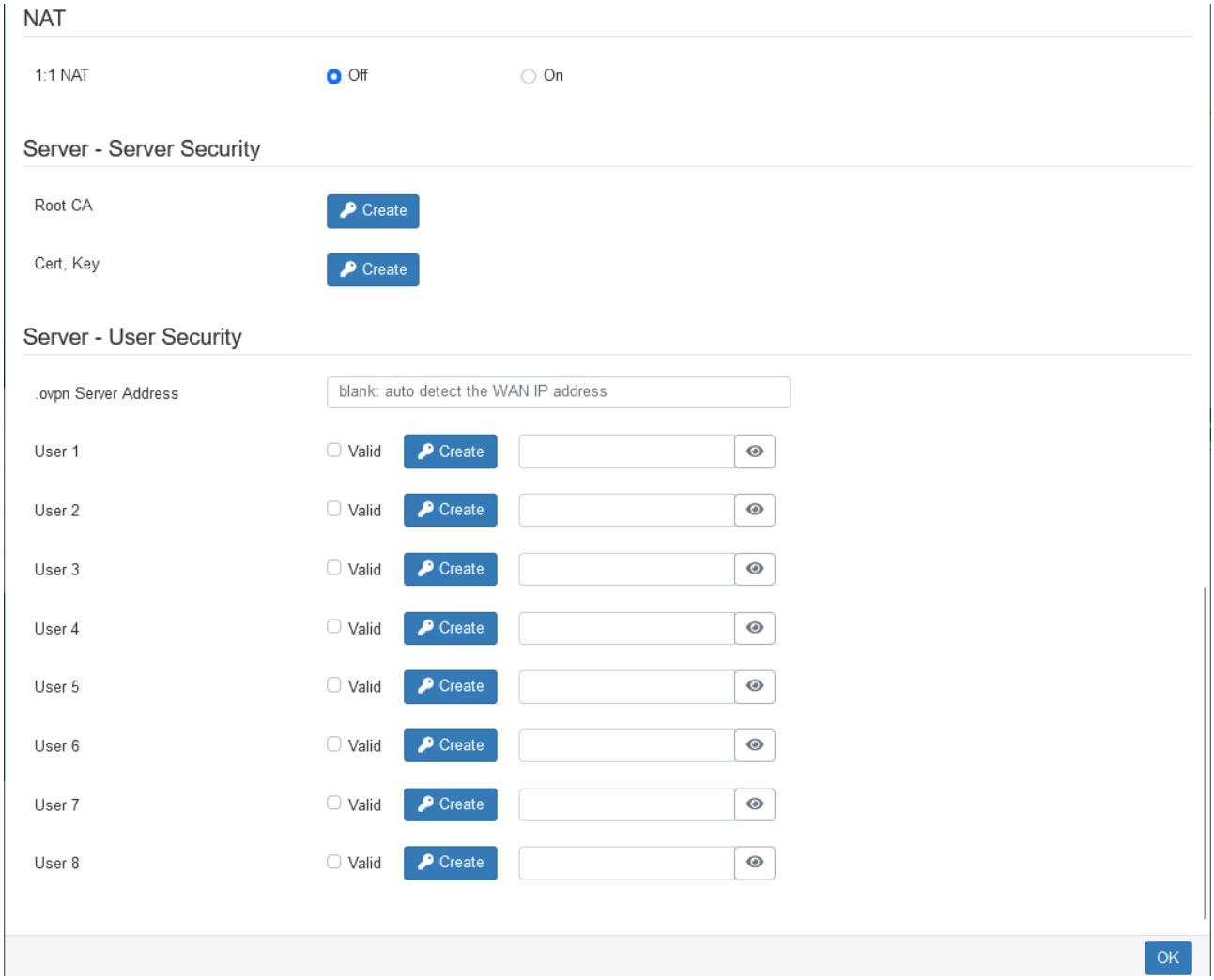

| VPN > OpenVPN > Client VPN Mode | |
|---|---|
| **Item** | **Description** |
| **Client** | |
| Server Address | Fill in WAN IP of OpenVPN server. |
| Route Client Networks | This setting needs to match the server side. When enabled, the cellular router will auto apply the properly routing rules. |
| **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 OpenVPN. This item must be enabled when the router under NAT environment.<br>When two routers' LAN Subnet are same and create OpenVPN tunnels, this function should turn on. |
| **Client-Security** | |
| Root CA | The Certificate Authority file of OpenVPN server, which can download |

| | |
|---|---|
| | from OpenVPN server. |
| Cert | The certification file is for OpenVPN client, which can download from OpenVPN server. |
| Key | The private key file is for OpenVPN client, which can download from OpenVPN server. |
| P12 | The PKCS#12 file is for OpenVPN client, which can download from OpenVPN server. |

### 11.1.3 OpenVPN Server Setting

Select option "**Server"** from VPN Mode, and this section allows you to configure the **server settings of VPN Mode**.



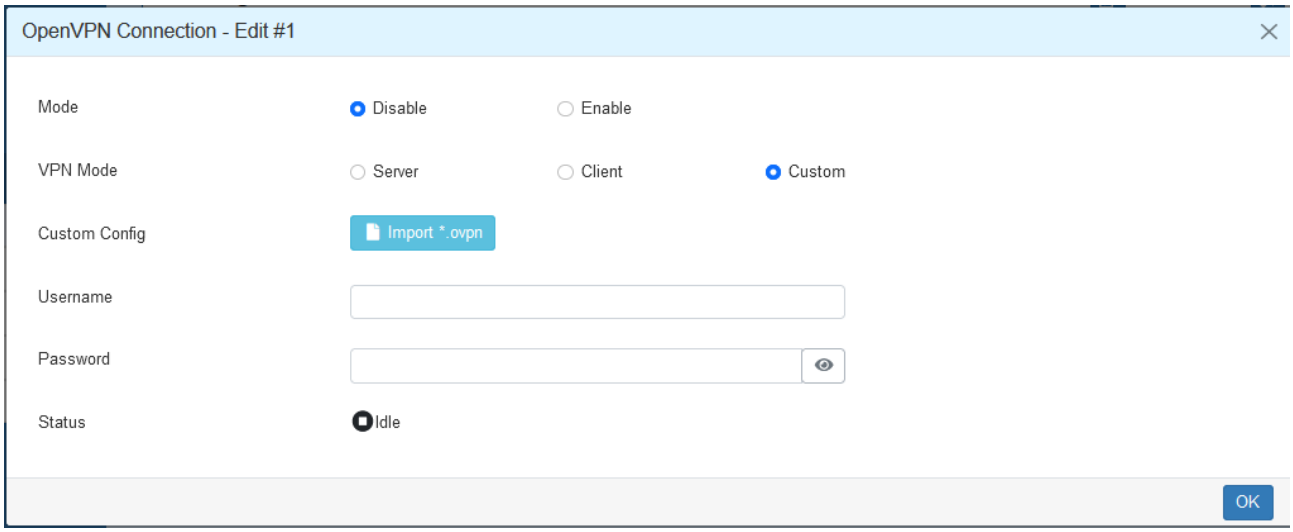



| **VPN > OpenVPN > Server VPN Mode** | |
|---|---|
| **Item** | **Description** |
| **Server** | |
| VPN Network | The network ID for OpenVPN virtual network. |
| VPN Netmask | The netmask for OpenVPN virtual network. |
| Roadwarrior:<br>Route Client Networks | The OpenVPN server will route the client traffic or not. User should fill in the client IP and netmask when this option is enable. |
| **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 OpenVPN. This item must be enabled |

| | |
|---|---|
| | when router under NAT environment.<br>The default is Off. |
| **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 OpenVPN Custom

This section helps you use the .ovpn configuration file to set up OpenVPN tunnel quickly with third-party server or use the OpenVPN advance options to be compatible with other servers.

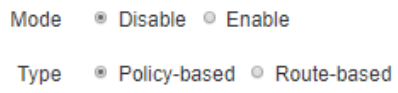



| **VPN > OpenVPN > Custom VPN Mode** | |
|---|---|
| **Item** | **Description** |
| Mode | Enable or disable the selected OpenVPN connection. |
| VPN Mode | Select the custom mode. |
| Custom Config | Import OpenVPN configuration with “.ovpn” file. |
| Username | Fill in the username if the imported file has already set up the username. |
| Password | Fill in the password if the imported file has already set up the password. |
| Status | Display the connection status of OpenVPN, such as IP address and the connected time. |

## 11.2 IPSec

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

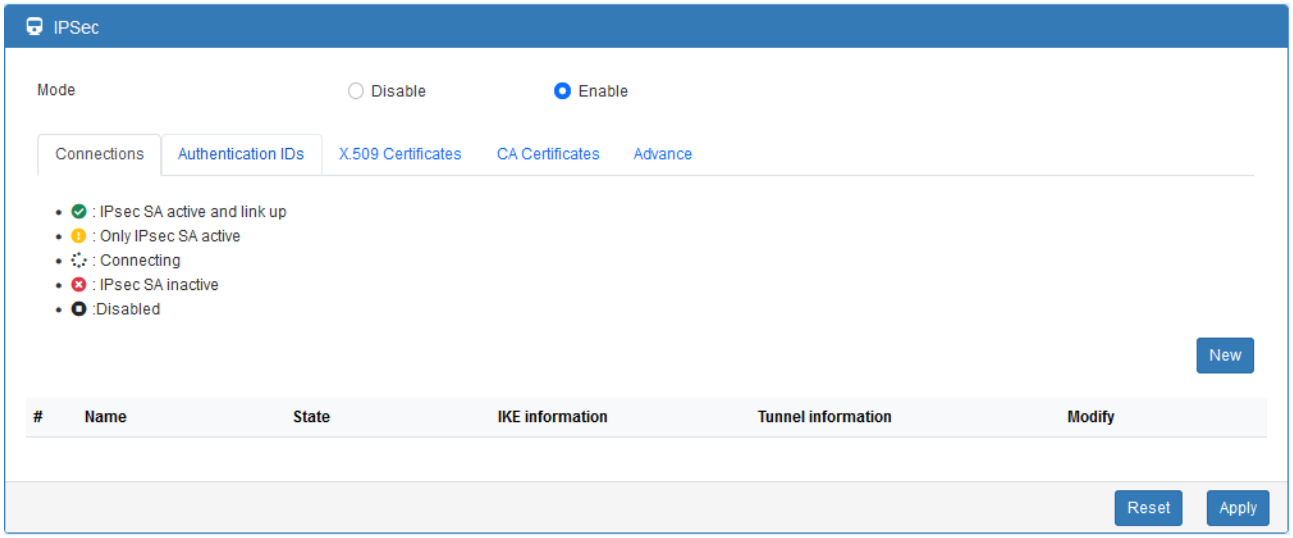
For the IPsec connection which be authenticated by **pre-shared key**, it only need to setup the **Connections** and **Authentication IDs.** For the IPsec connection which be authenticated by **RSA or TLS**, the settings must cover the four parts.



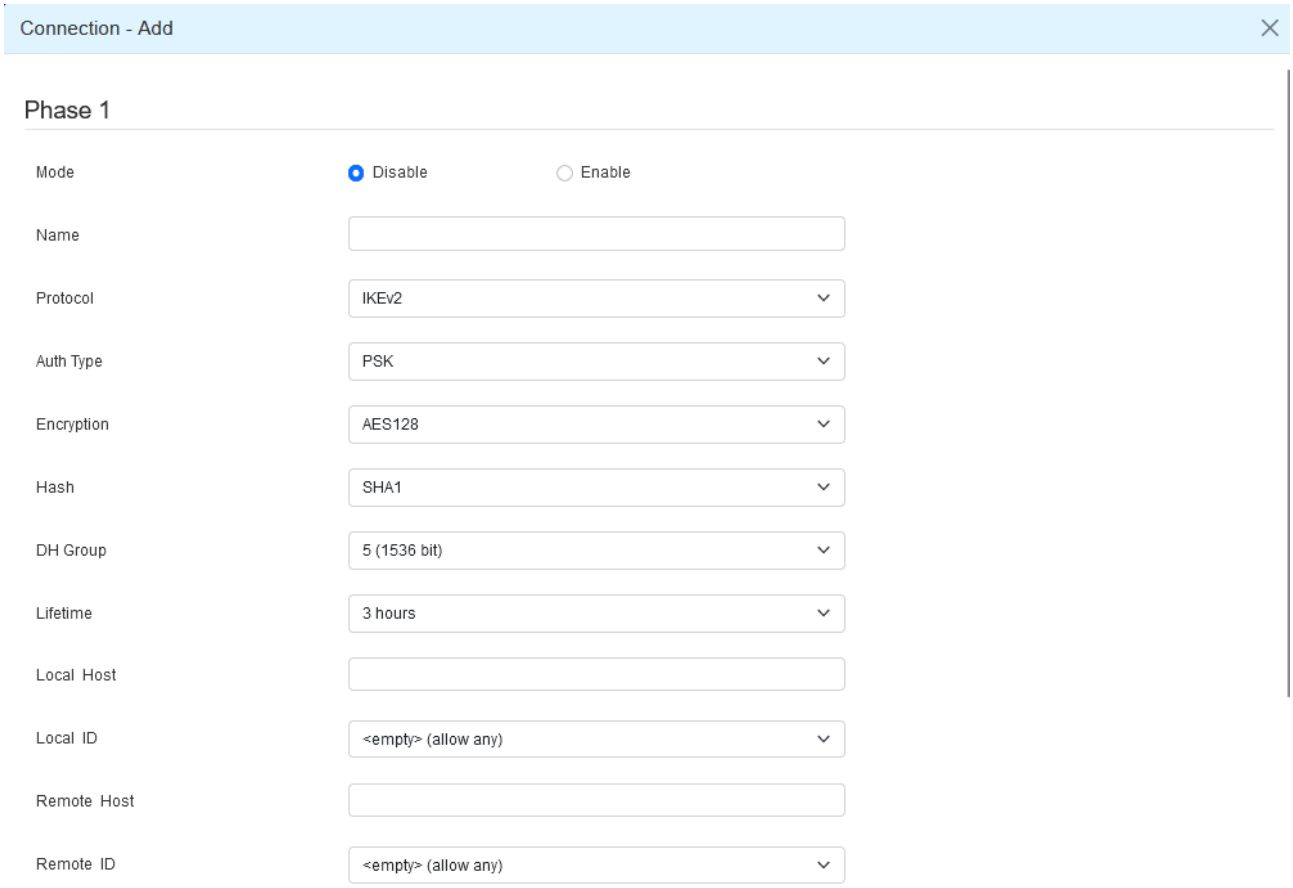

| VPN > IPsec > General setting | |
|---|---|
| **Item** | **Description** |
| Mode | Select from Disable or Enable. The default is Disable. |

### 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 clicking **New** button.



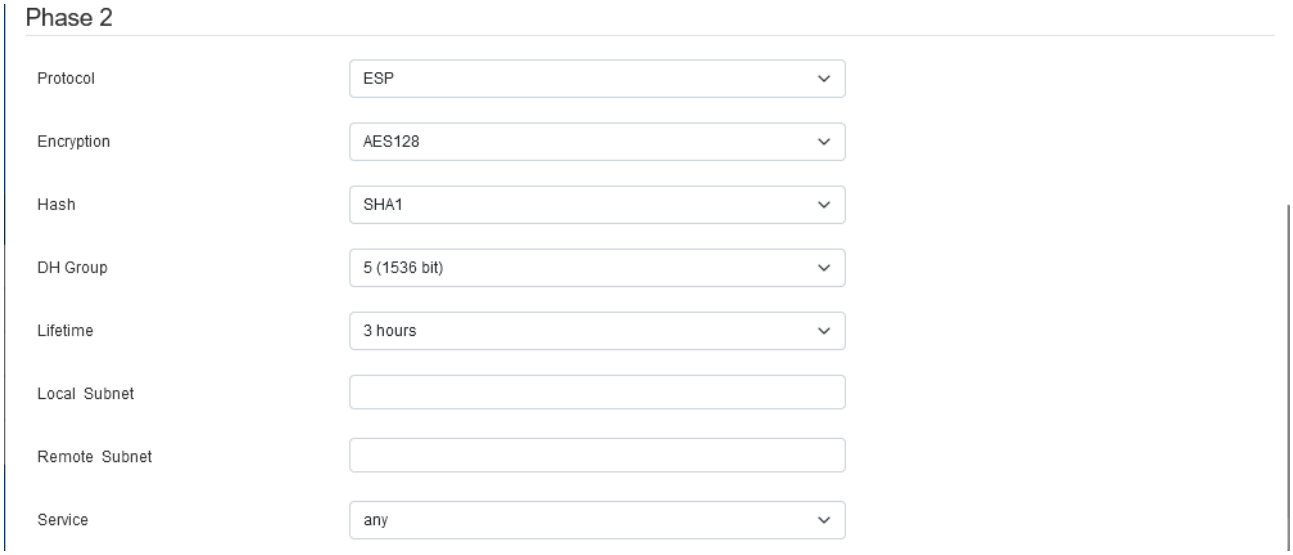

**(1) IPsec Phase 1 Setting**




| **VPN > IPsec > Connections > Phrase 1 setting** | |
|---|---|
| **Item** | **Description** |
| Mode | Enable or disable the selected IPSec connection. |
| Name | Short name or description. |
| Protocol | Select from IKEv1 or IKEv2. The default is IKEv1. |
| Auth Type | Select from PSK (default), RSA, EAP-TLS.<br>(Note: The EAP-TLS is for IKEv2 only.) |
| Encryption | The encryption algorithm.<br>Select from AES128 (default), AES192, AES256 or 3DES. |
| Hash | The integrity algorithm.<br>Select from MD5, SHA1 (default) or SHA256. |
| DH Group | The Diffie Hellman Group.<br>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.<br>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.<br>If this value is blank, the connection will automatically detect the correct IP address. |

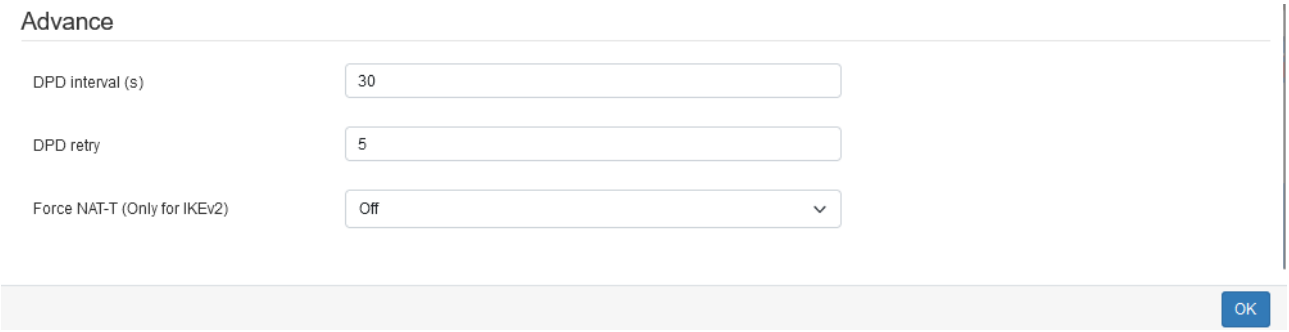
| | |
|---|---|
| Local ID | The identification for authentication on local peer.<br>Select from the created authentication IDs or empty. |
| Remote Host | The IP address of the peer gateway's public network interface.<br>If this value is blank, the connection will act the server role to wait the incoming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

### (2) IPsec Phase 2 Setting




| VPN > IPsec > Connections > Phrase 2 setting | |
|---|---|
| **Item** | **Description** |
| Protocol | ESP supported only. |
| Encryption | The encryption algorithm.<br>Select from AES128 (default), AES192, AES256 or 3DES. |
| Hash | The integrity algorithm.<br>Select from MD5, SHA1 (default) or SHA256. |
| DH Group | The Diffie Hellman Group.<br>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.<br>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.<br>The available formats are A.B.C.D, A.B.C.D/M, A.B::C.D or A.B::C.D/M<br>If this value is blank, the connection will set it as the “Local Host” of Phase 1 setting.<br>*Note:* This option only work on Policy-based IPsec VPN type. |
| Remote Subnet | The private subnet behind the peer gateway.<br>The available formats are A.B.C.D, A.B.C.D/M, A.B::C.D or A.B::C.D/M<br>If this value is blank, the connection will set it as the “Remote Host” of Phase 1 setting.<br>*Note:* This option only work on Policy-based IPsec VPN type. |
| Service | Restrict the VPN traffic to the particular protocol only.<br>Select from the Any, TCP, UDP or L2TP. |

### (3) IPsec Advance Setting

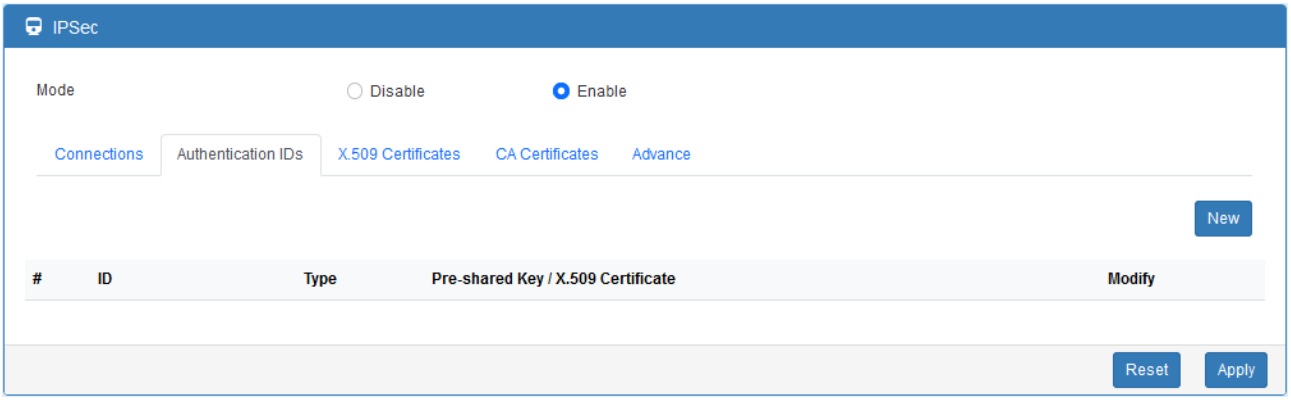


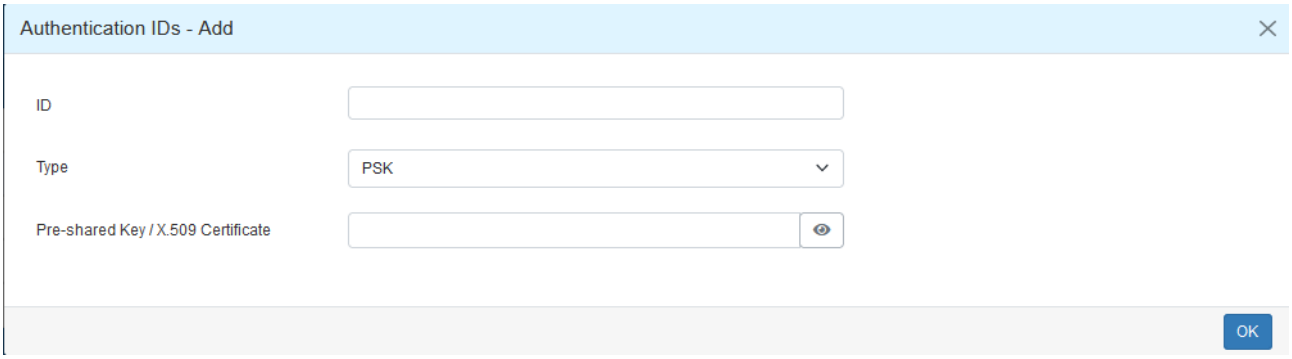

| VPN > IPsec > Connections > Advance Setting | |
|---|---|
| **Item** | **Description** |
| DPD interval | The period time interval to detect dead peers.<br>The default is 30 seconds. |
| DPD retry | The max number of retry of dead peer detection.<br>The default is 5 times. |
| Force NAT-T (Only for IKEv2) | Enable or disable the NAT-T for selected IPSec connection. |

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 clicking the **New** button.




| **VPN > IPsec > Authentication IDs** | |
|---|---|
| **Item** | **Description** |
| ID | The identification for authentication. It works with PSK type only. |
| Type | Select from PSK or RSA. The default is PSK.<br>PSK: Use the pre-shared key to authenticate the connection.<br>RSA: Use the certificate to authenticate the connection. |
| Pre-shared Key / X.509 Certificate | The X.509 certificate for authentication.<br>The certificate is generate or import by X.509 Certificates section. |

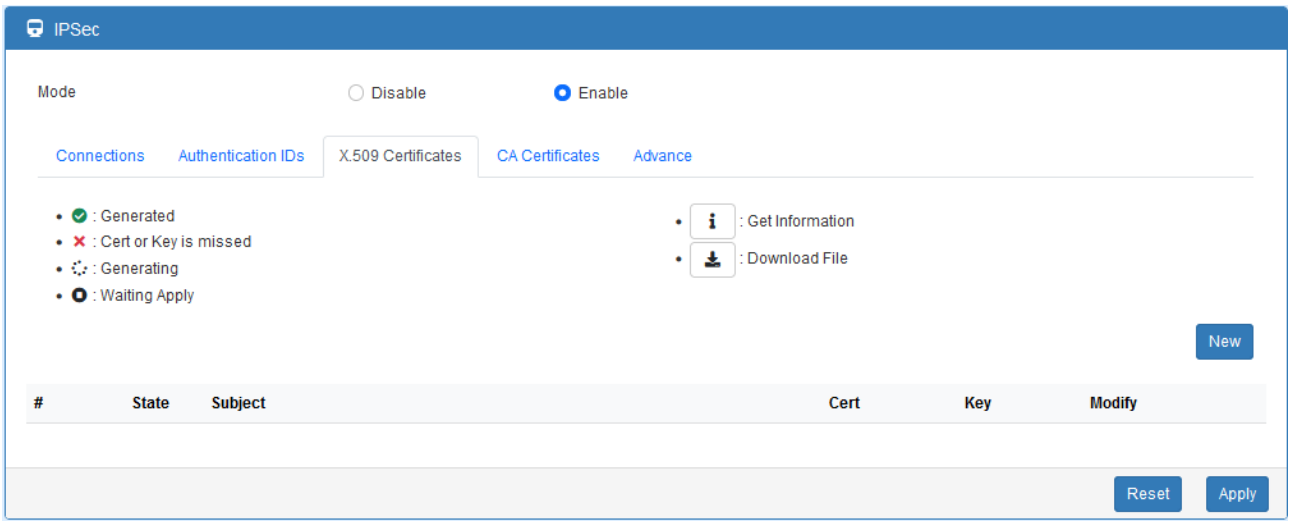
According to the above options, there are some combinations to authenticate the IPsec connection.

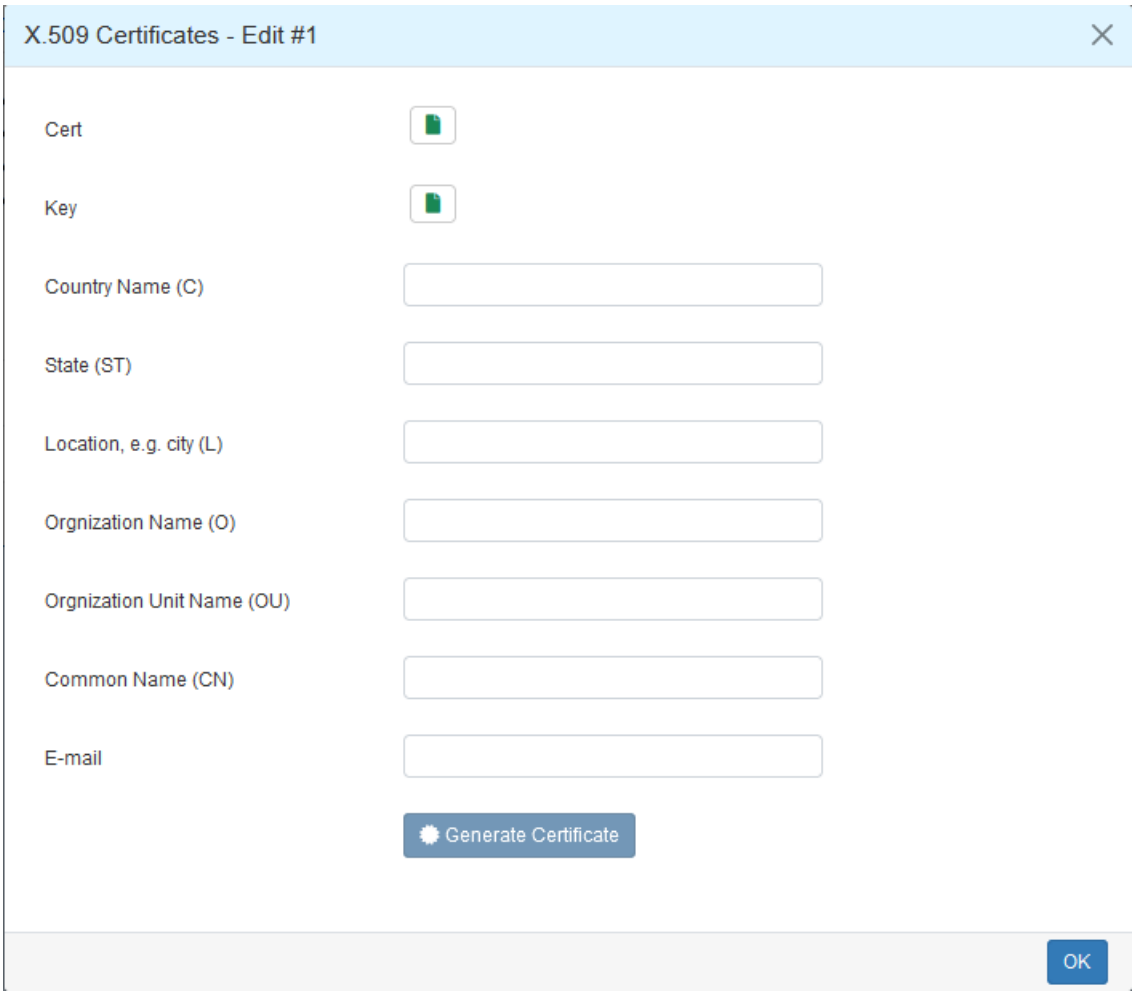
| VPN > IPsec > Authentication IDs | | | | |
|---|---|---|---|---|
| **#** | **ID** | **Type** | **Pre-shared Key / X.509 Certificate** | **Comment** |
| 1 | | PSK | password | The default password for the PSK connections. |
| 2 | remote.ipsec | PSK | 2wsx#EDC | The password only for the PSK connection with remote.IPsec ID.<br>Normally, this case is use to authenticate peer gateway. |
| 3 | local.ipsec | PSK | | The identification for the connection.<br>Normally, this case is use 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. |

### 11.2.2 IPsec > X.509 Certificates

This section provides the certificates setting which is use by IPsec authentication ID.

Each certificate will show the **State** and **Subject** information.



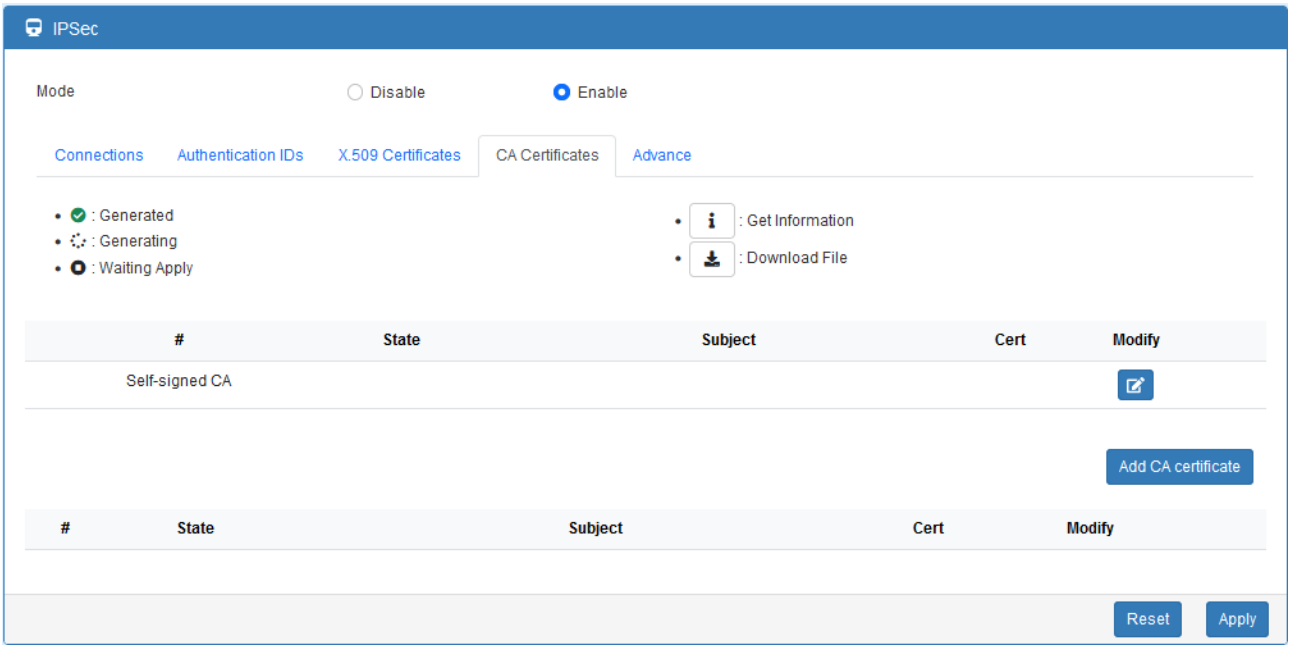



### 11.2.3 IPsec > CA Certificates

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 import in 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.

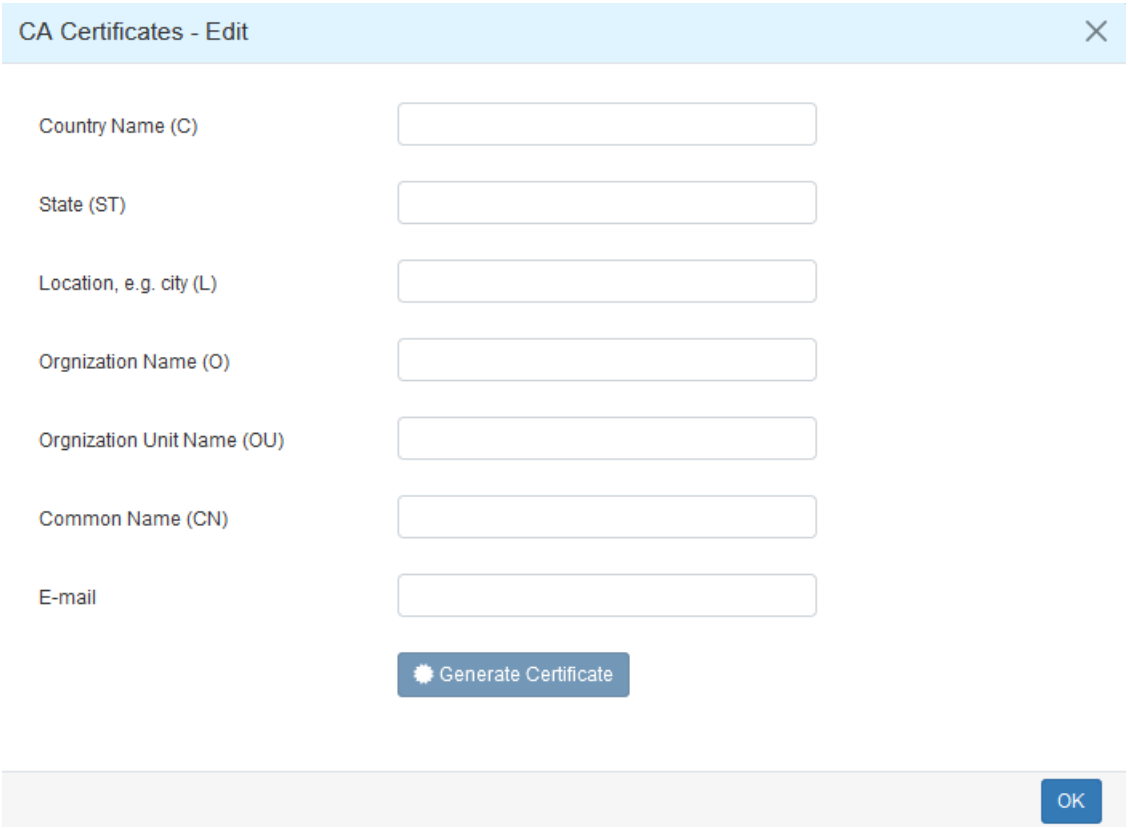
To generate the self-signed CA certificate:

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 OK
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 New 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 OK.
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<br>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<br>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<br>This option is required for certificate generation. |
| E-mail | The maintainer's E-mail. |

**Certificate Importing**

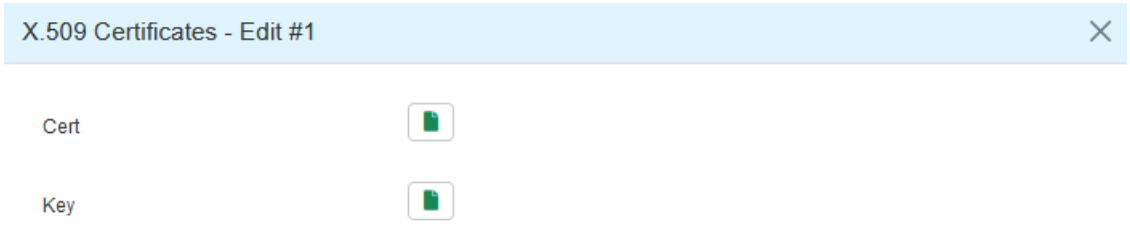
Same as the **Certificate Generation**, the router supports the CA and X.509 certificate importing.

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 authenticate 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.

## 11.3 GRE

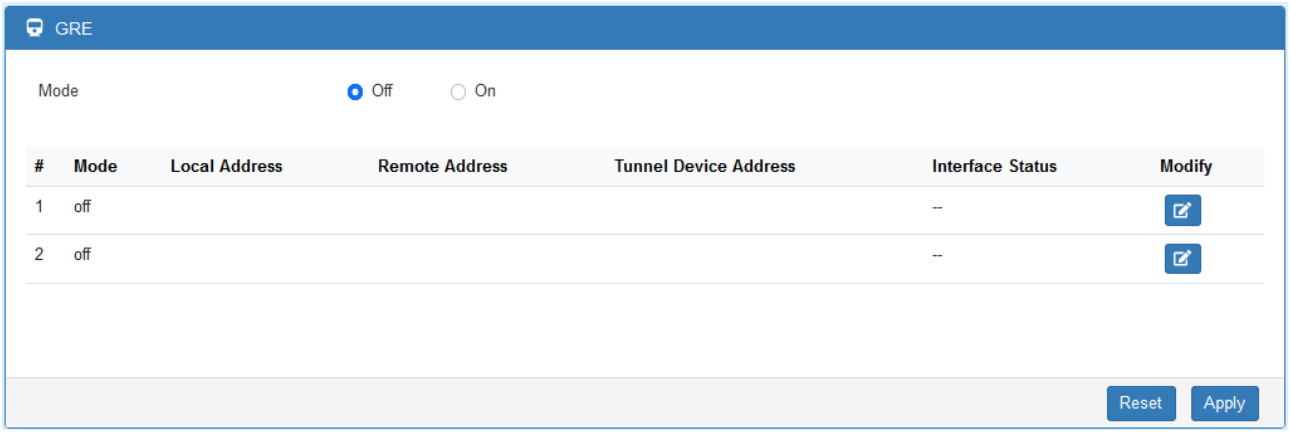
This section allows you to set **GRE configuration**. The default mode is off.

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

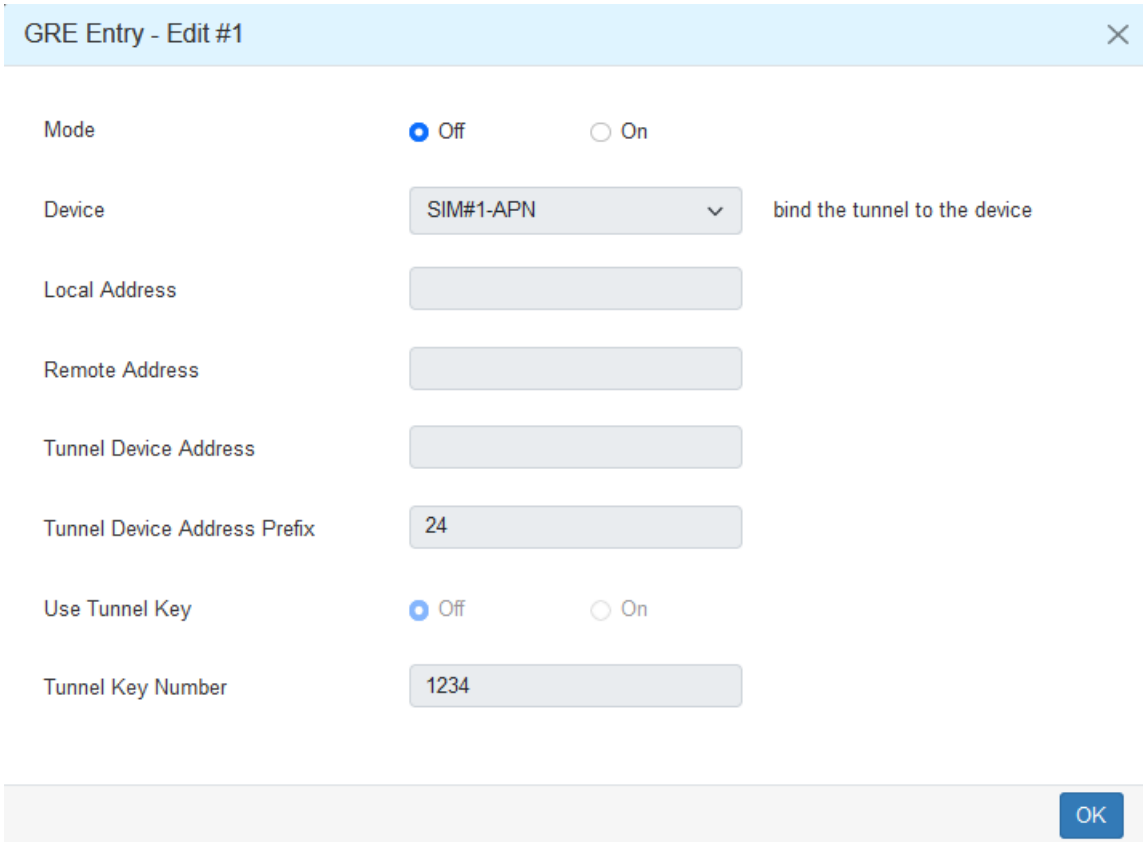
- GRE Tunnel interface comes up as soon as it is configured.
- Local endpoint does not bring the interface down if the remote endpoint is unreachable.
- No way to determine problems in the intervening network.
- Keepalives are used to solve this issue.

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

There are two entries for user to configure, please press Edit  button.



Setup the GRE connection by clicking Edit button.

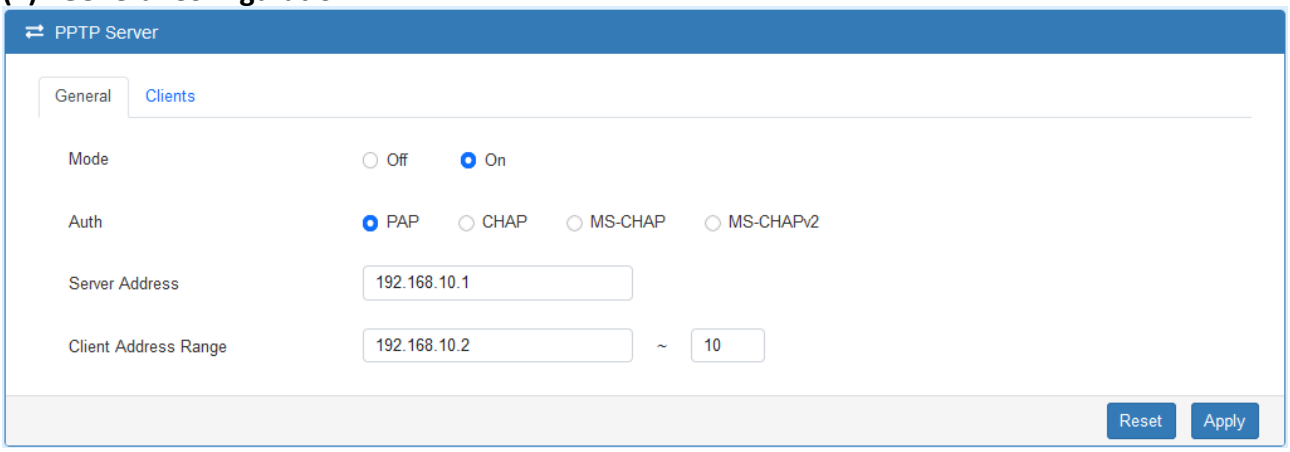



| **VPN > GRE** | |
|---|---|
| **Item** | **Description** |
| Mode | Enable or disable the selected GRE connection. |
| Device | Select the interface that GRE should be applied |
| Local Address | Set local address of the GRE tunnel. |
| Remote Address | Set remote address of the GRE tunnel. |
| Tunnel Device Address | Set IP address of this GRE tunnel device. |
| Tunnel Device Address Prefix | Set Prefix of the Tunnel Device Address. |
| Use Tunnel Key | Whether to use the key for identifying an individual traffic flow within a tunnel. |
| Tunnel Key Number | The number of the tunnel key; default is '1234'. |

## 11.4 PPTP Server

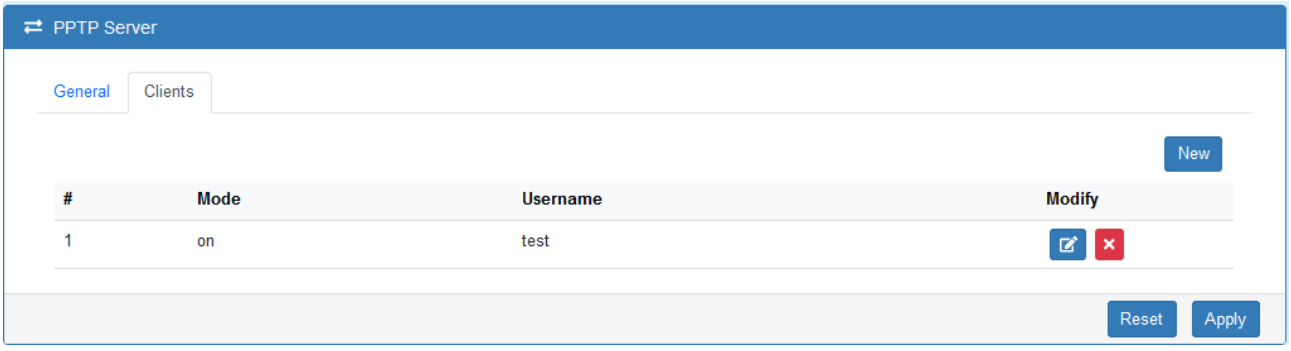
This section provides 2 sub configurations, including General Configuration and Clients Configuration.

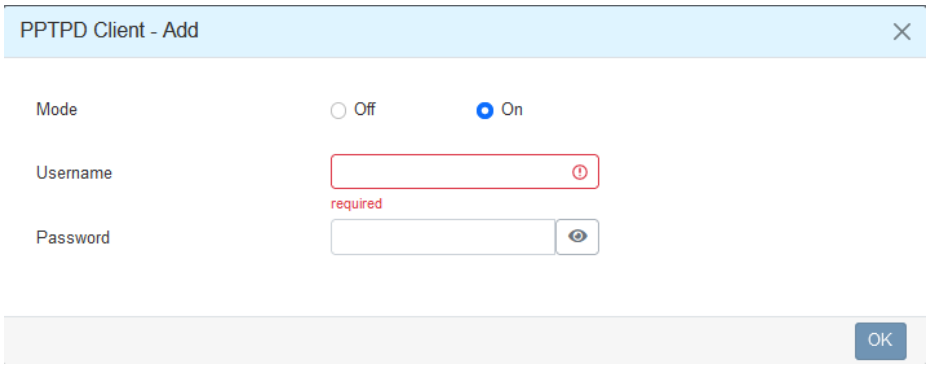
### (1) General Configuration




| VPN > PPTP Server > General | |
|---|---|
| **Item** | **Description** |
| Mode | Enable or disable the PPTP Server function. |
| Auth | Select the authentication type. |
| Server Address | This IP address is use as tunnel IP at server site. |
| Client Address Range | A list of IP addresses to assign to remote PPTP clients. |

### (2) Clients Configuration



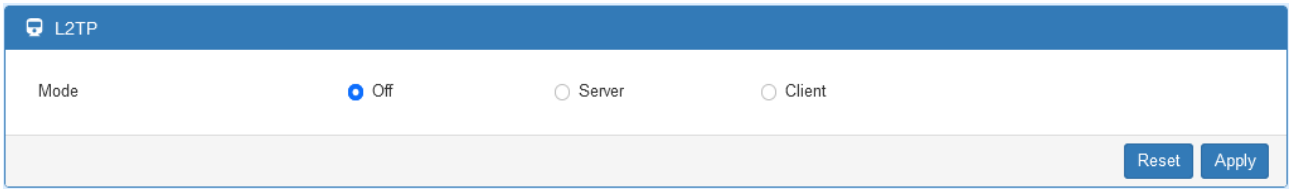



| VPN > PPTP Server > Clients | |
|---|---|
| **Item** | **Description** |
| Mode | Enable or disable the selected account. |
| Username | The username of this client. |
| Password | The password of this client. |

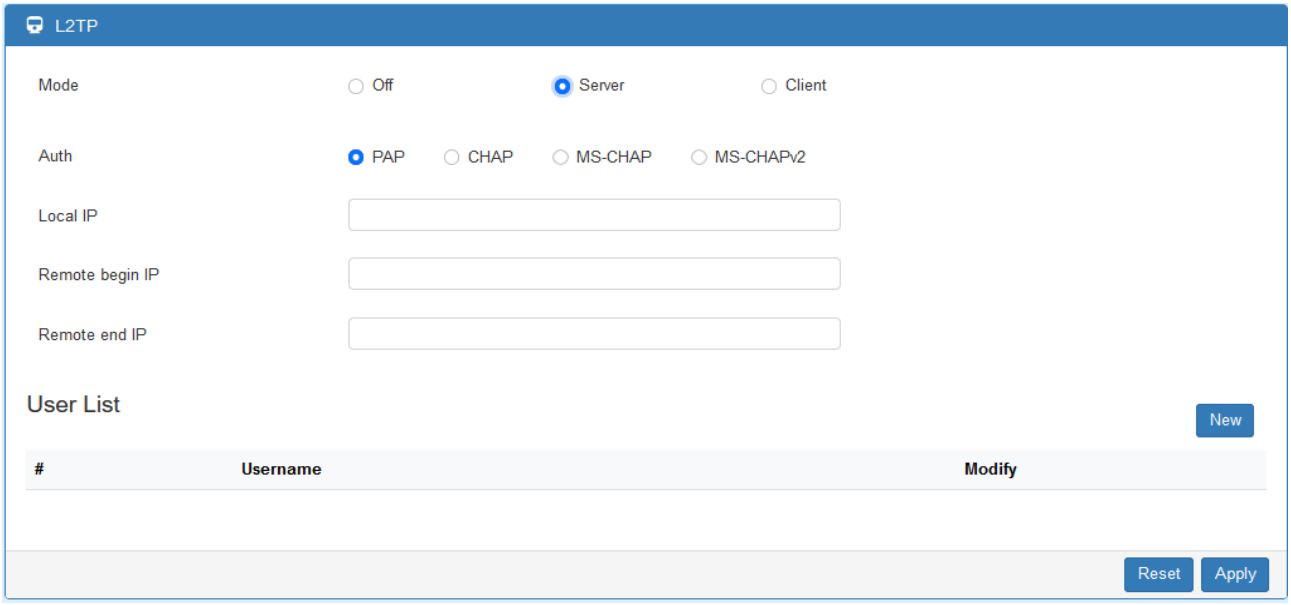
## 11.5 L2TP

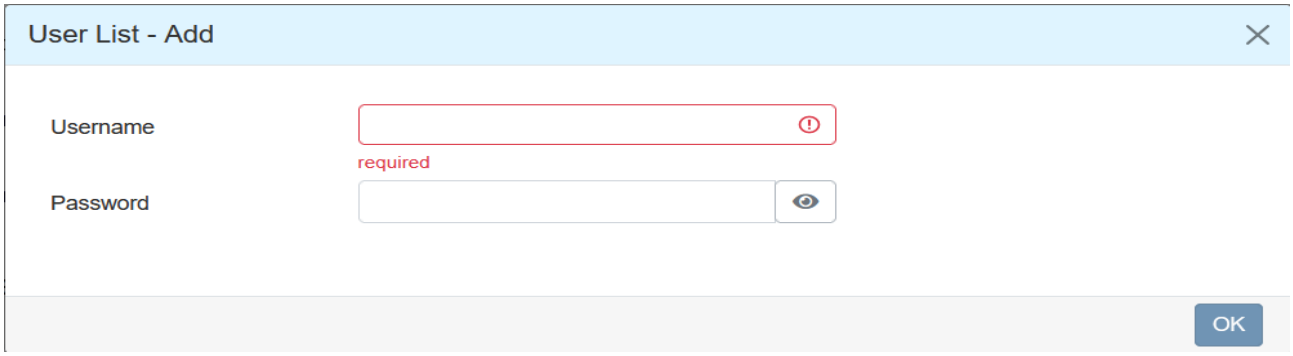
This section allows you to set up L2TP and provides three modes for configuration, including Off, Server, and Client Mode.

**(1) General Mode:** The default mode is Off as shown as below.




**(2) Server Mode:**

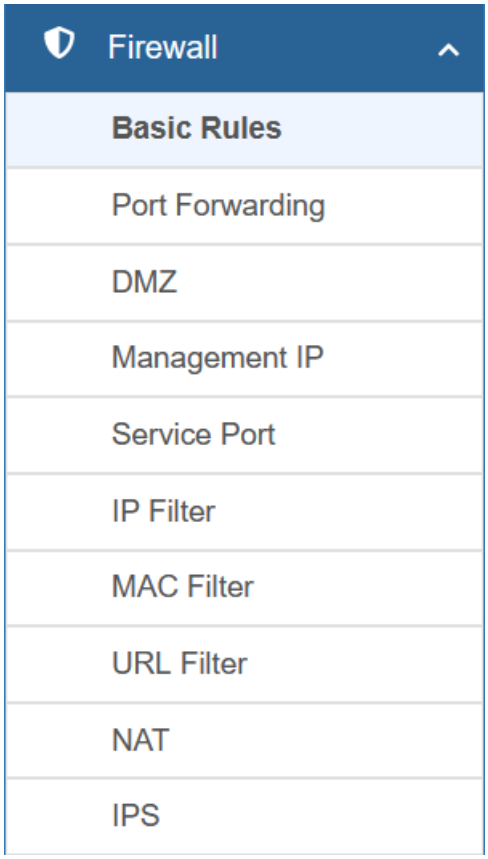



| VPN> L2TP > Server Mode | |
|---|---|
| **Item** | **Description** |
| Mode | Select from Off or On to set the client setting. |
| Auth | The authentication method for L2TP connection. Available options: PAP, CHAP, MS-CHAP, MS-CHAPv2 |
| Local IP | The virtual IP for L2TP server. |
| Remote begin IP | The begin address of L2TP client's IP pool. |
| Remote end IP | The end address of L2TP client's IP pool. |
| New | Create a new user account for connecting with server. |
| Username | The username for L2TP client. |
| Password | The password for L2TP client. |

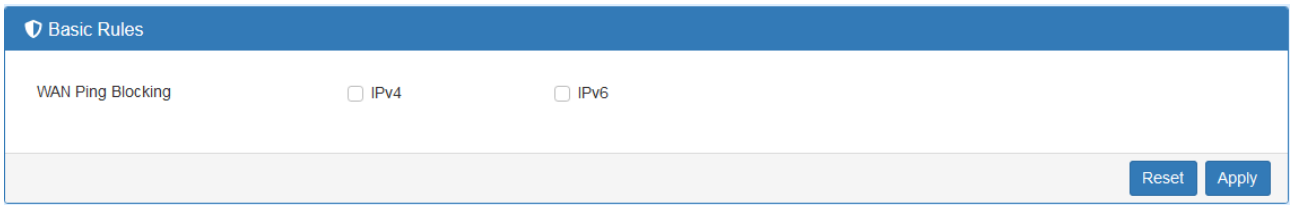
# 12 Web Menu Item > Firewall

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




## 12.1 Basic Rules

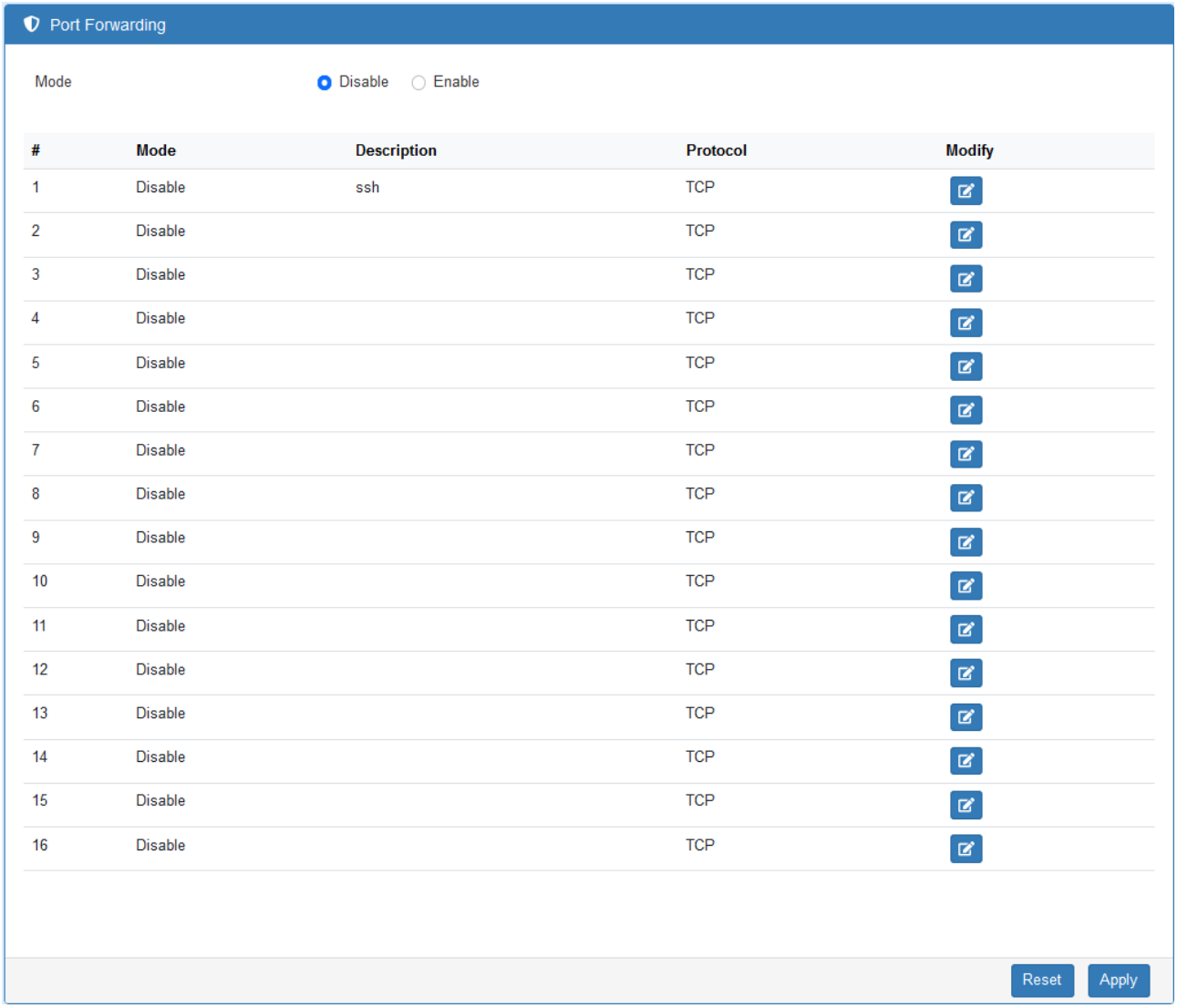
This section allows you to set the Basic Rules configuration.

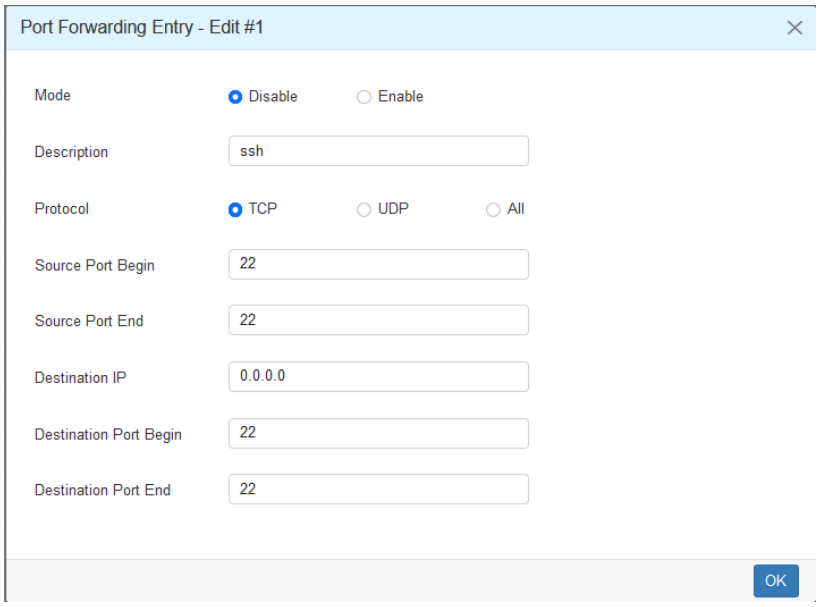



| Firewall > Basic Rules | |
|---|---|
| **Item** | **Description** |
| WAN Ping Blocking | Check IPv4 or IPv6 for blocking |

## 12.2 Port Forwarding

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

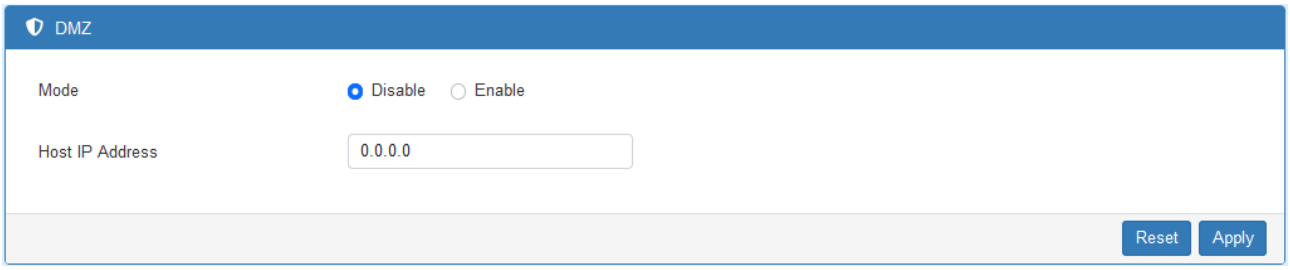


| Firewall > Port Forwarding | |
|---|---|
| **Item** | **Description** |
| Mode | Enable or disable the selected port forwarding entry. |
| Description | Descript the name of Port Forwarding. |
| Protocol | Select from UDP or TCP Client, which depends on the application. |
| Source Port Begin | Fill in the beginning of source port. |
| Source Port End | Fill in the end of source port. |
| Destination IP | Fill in the current private destination IP. |
| Destination Port Begin | Fill in the beginning of private destination port. |
| Destination Port End | Fill in the end of private destination port. |

## 12.3 DMZ

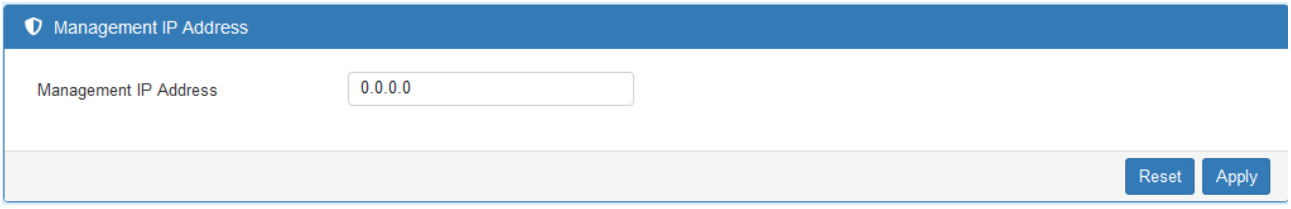
This section allows you to set the DMZ configuration.




| Firewall > DMZ | |
|---|---|
| **Item** | **Description** |
| Mode | Enable or disable the DMZ function. |
| Host IP Address | Fill in your Host IP Address. |

## 12.4 Management IP

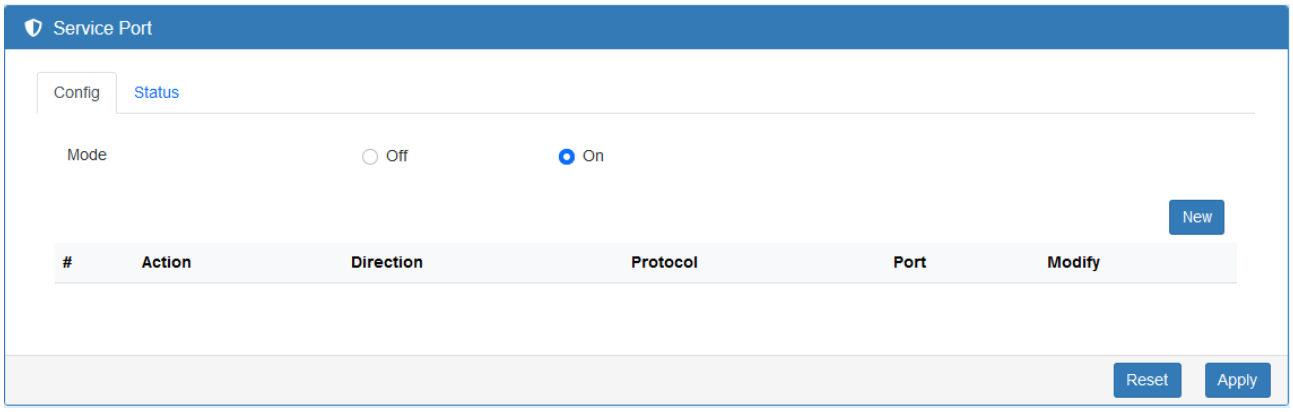
This section allows user to setup a management IP that is able to access the device from LAN or WAN side. This IP has higher management permissions than firewall settings.

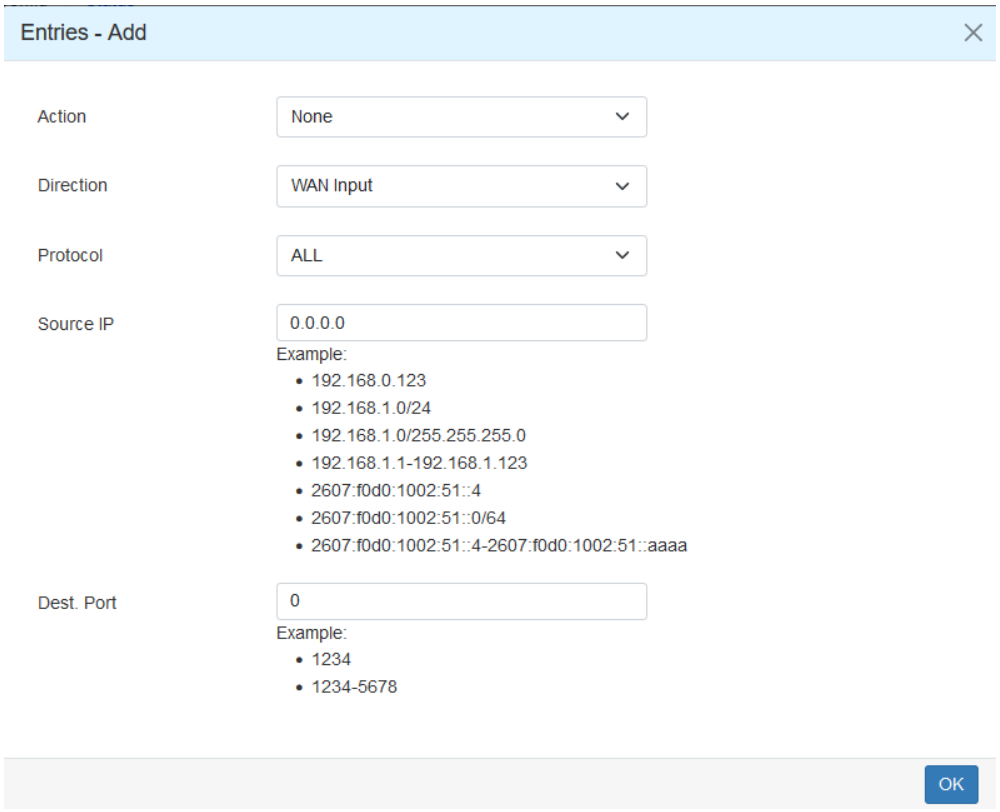


| Firewall > Management IP | |
|---|---|
| **Item** | **Description** |
| Management IP Address | Fill in your management IP Address. |

## 12.5 ACL

This section allows managing access to the router's own services.

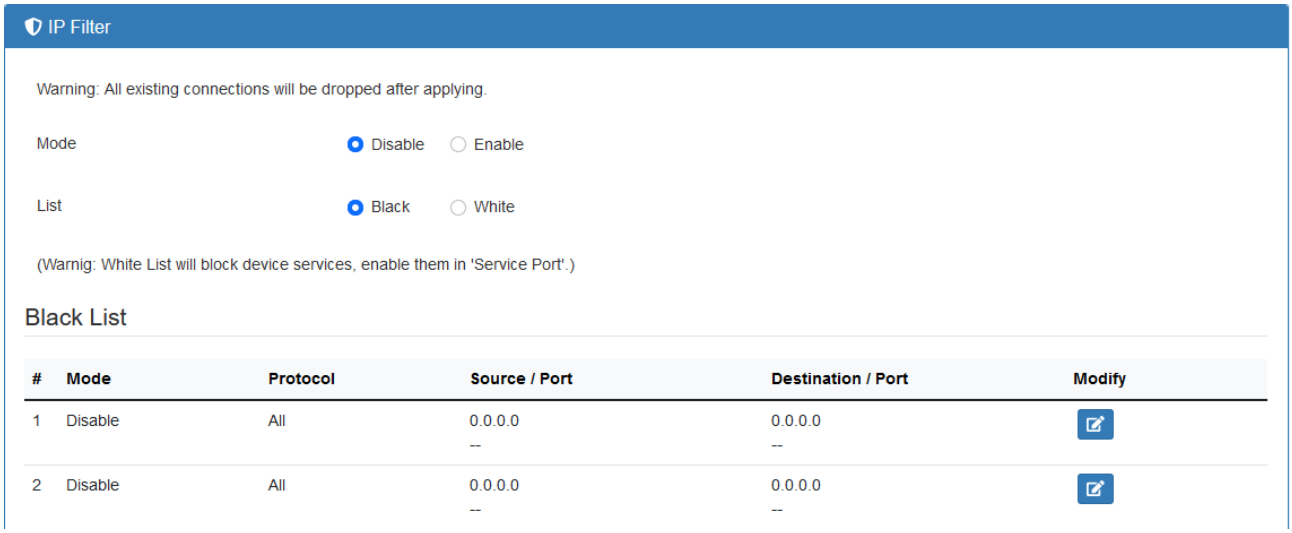


| Firewall > Service Port | |
|---|---|
| **Item** | **Description** |
| Mode | Enable or disable the service port function. |
| Action | Select the action for selected entry. |
| Direction | Select the direction of traffic for selected entry. |
| Protocol | Select the protocol type. |
| Source IP | Enter the source IP, 0.0.0.0 means any. |
| Dest. Port | Enter the service port number. |

## 12.6 IP Filter

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



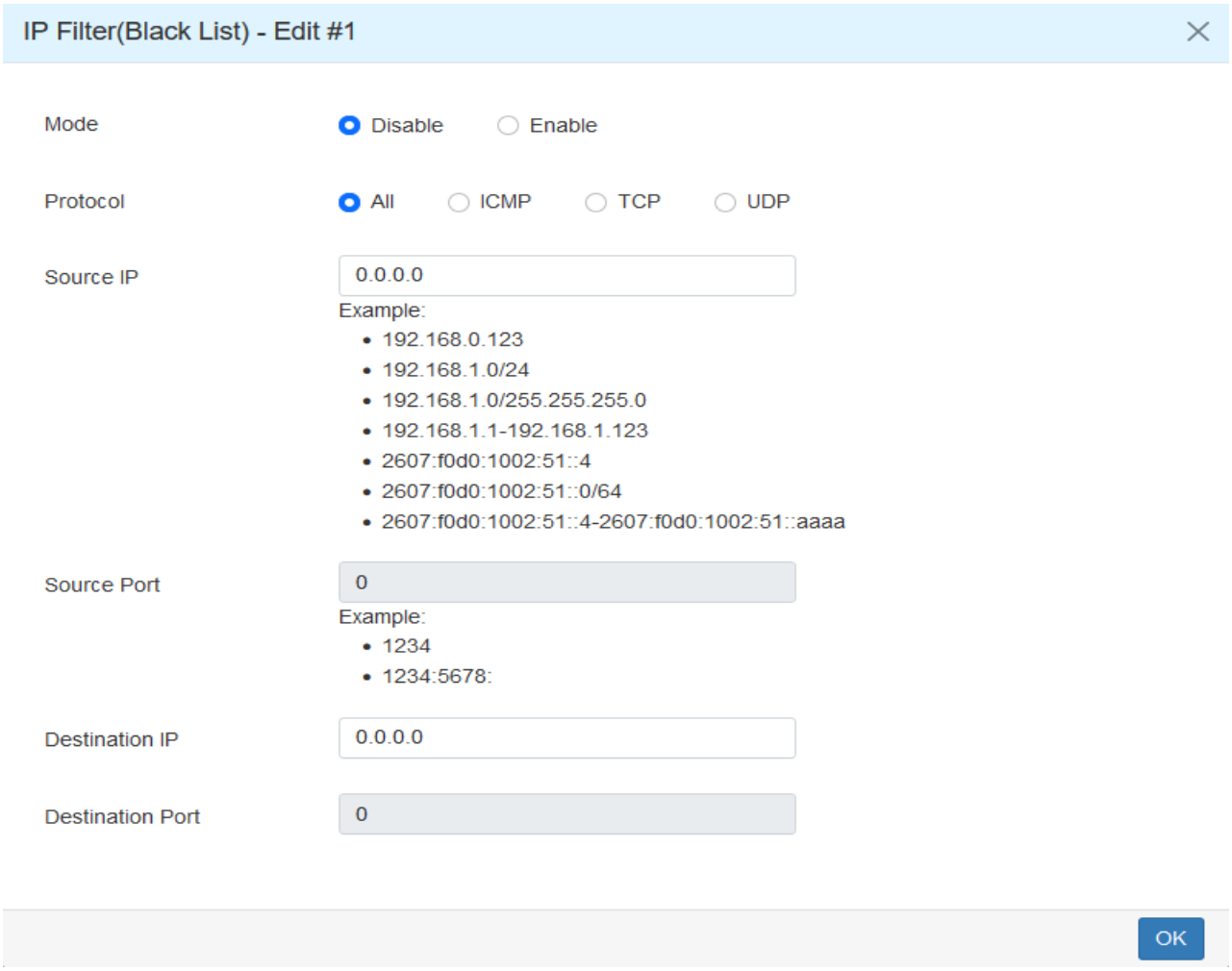

**Black List:** When Black List selected, all specified IP address/port are blocked.

**White List:** When White List selected, all specified IP address/port are accepted.

**Edit Black/White List**

(1) Click  button to edit Black/White list.

(2) The default is **Disable** mode as the following interface (Black/White).




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

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

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

| **Firewall > Edit IP Filter > Source IP** | | | |
|---|---|---|---|
| **IP Format** | **Single IP** | **IP with Mask** | **Ranged IP** |

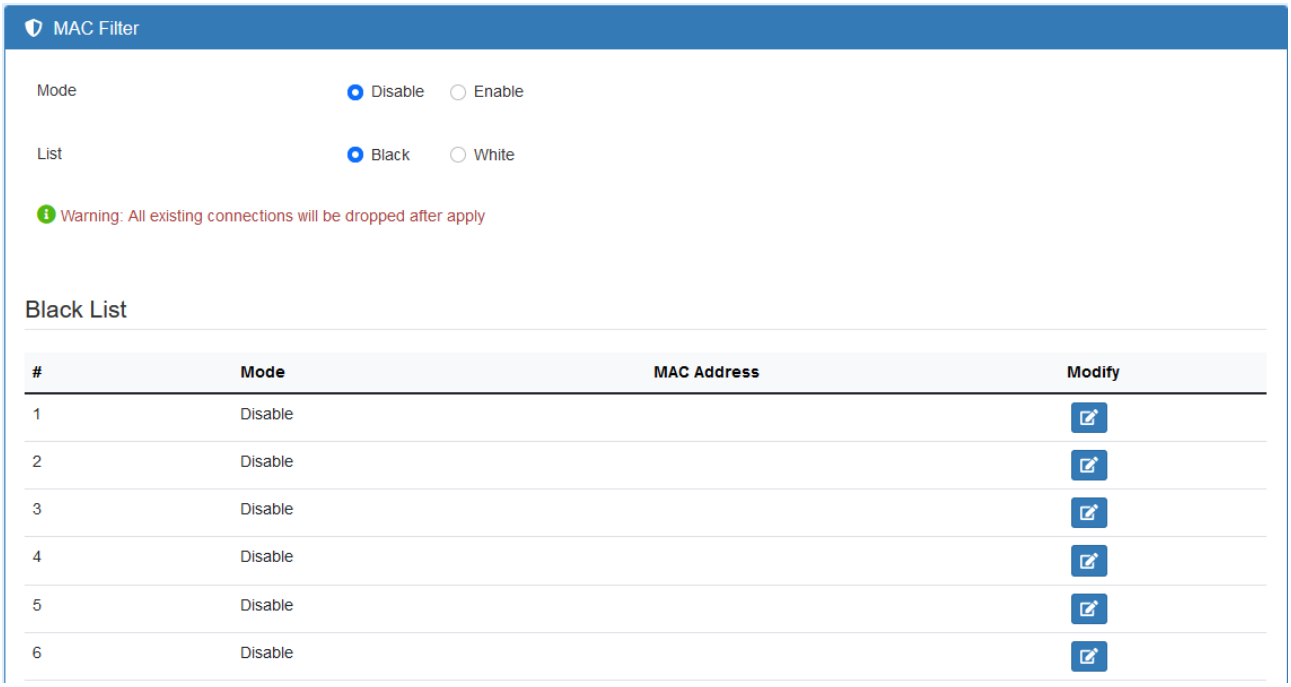
| | | | |
|---|---|---|---|
| IPv4 | 192.168.0.123 | 192.168.1.0/24<br>192.168.1.0/255.255.255. | 192.168.1.1-192.168.1.123 |
| IPv6 | 2607:f0d0:1002:51::4 | 2607:f0d0:1002:51::0/64 | 2607:f0d0:1002:51::4-<br>2607:f0d0:1002:51::aaaa |
| *Note:* Setting up a range of IP, please use – hyphen symbol to mark your ranged IP. | | | |

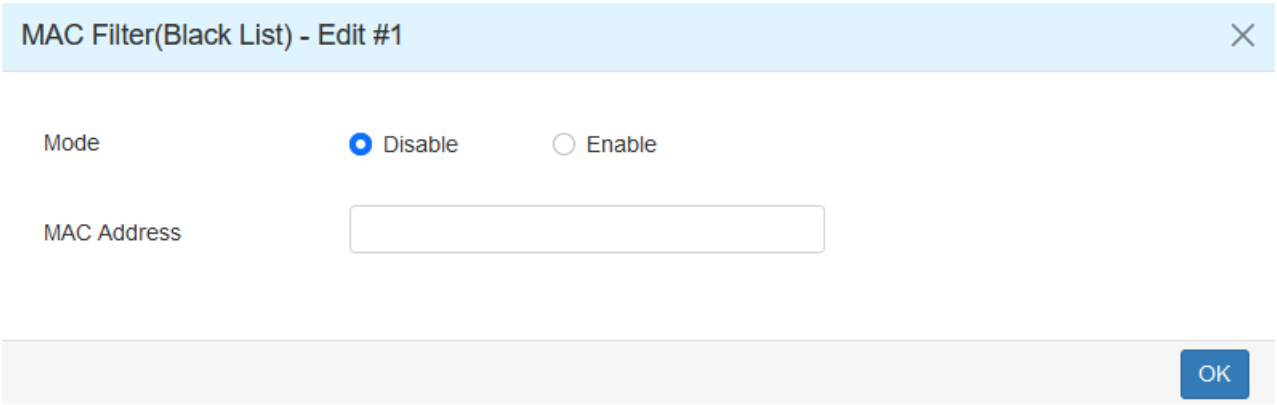
(5) For Source Port, there are two types to input your source port that depends on your requirement, including single port (e.g.1234) or giving a range of ports (e.g.1234:5678).

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

## 12.7 MAC Filter

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



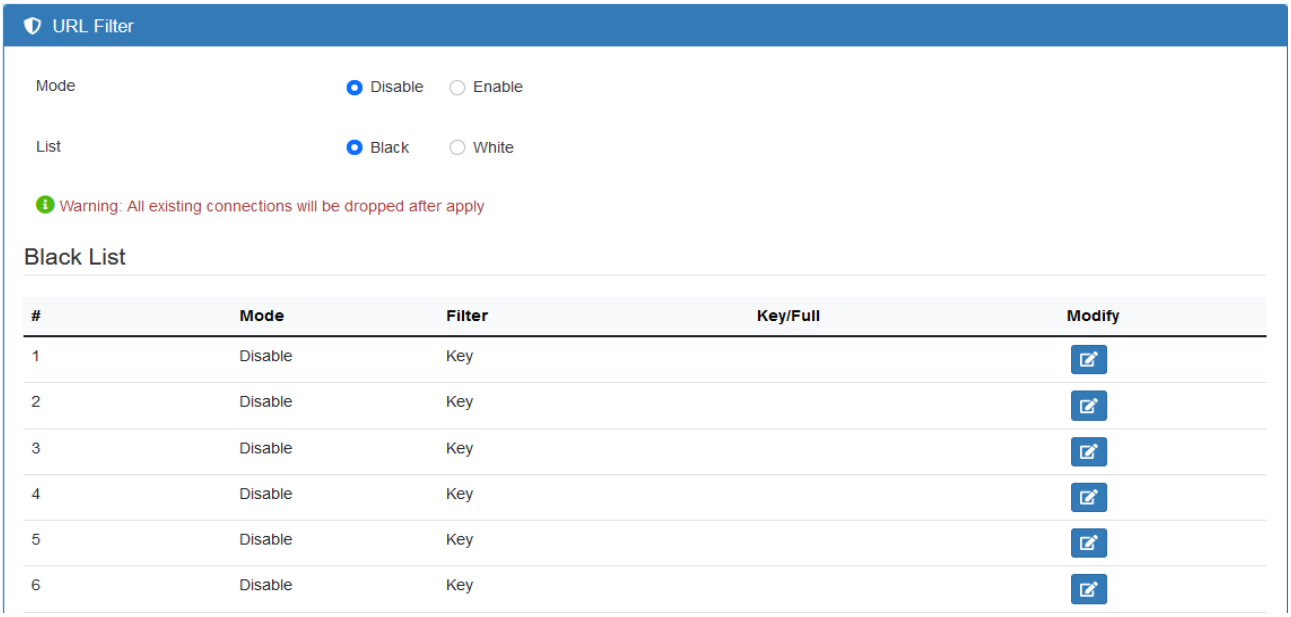



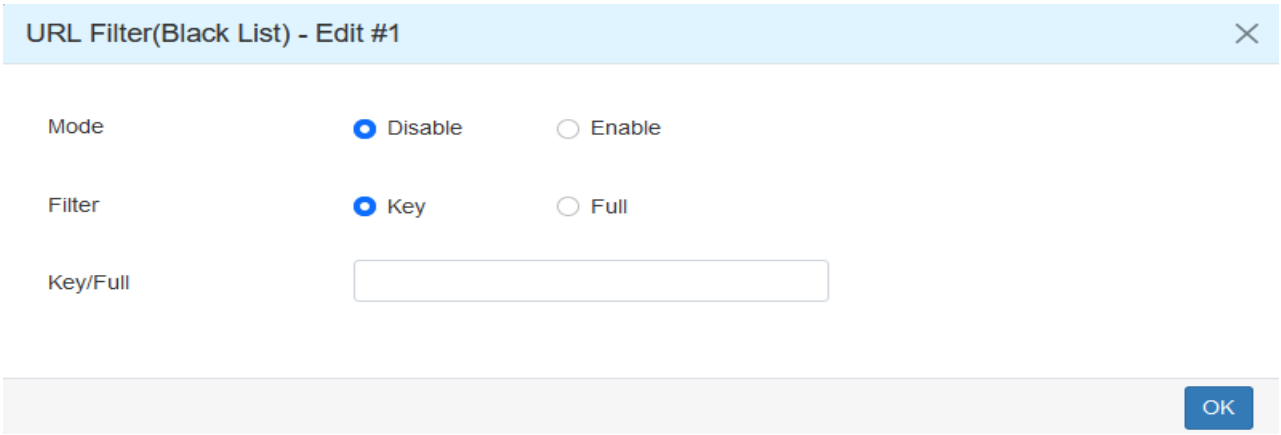

| Service > MAC Filter | |
|---|---|
| **Item** | **Description** |
| Mode | Select from Disable or Enable. The default is Disable. |
| MAC Address | Fill in your MAC address. |

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

## 12.8 URL Filter

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




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

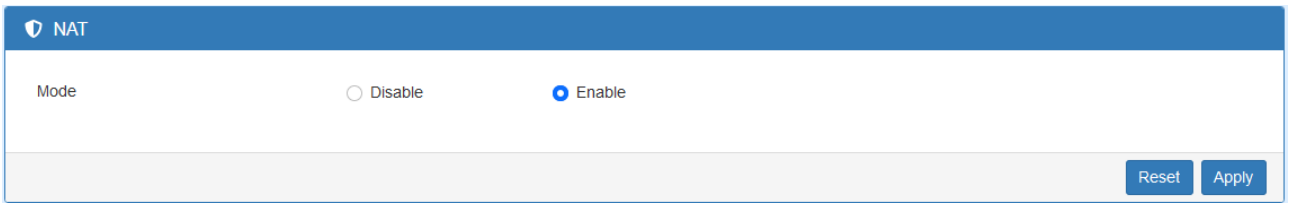
| **Firewall > URL Filter** | |
|---|---|
| **Item** | **Description** |
| Mode | Select from Disable or Enable. The default is Disable. |
| Filter | Select from Key or Full. The default is Key. |
| Key / Full | Fill in your Key / Full information. |

## 12.9 NAT

This section allows you to set NAT configuration.

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

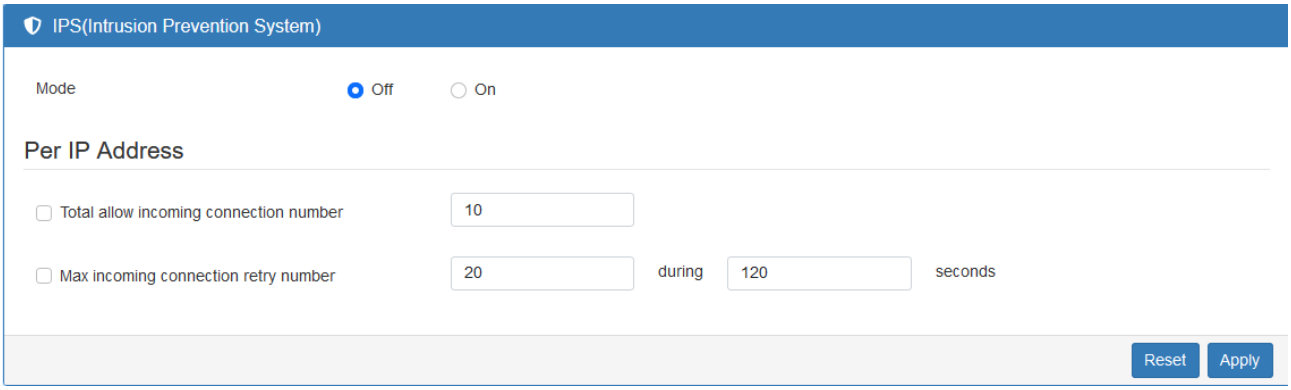
When NAT mode is **Disable**, the router will send the source LAN private IP address for outgoing packets and allow to receive the destination LAN private IP address for incoming packets.




## 12.10 IPS

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

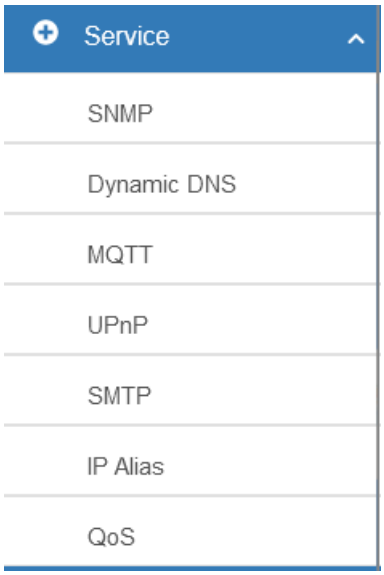
The system allows user to limit the max incoming connection number from WAN per source IP address to prevent system resource exhausted. Also, the system allows to limit the max incoming connection retry number during a specific time period from WAN per source IP address to prevent too many unexpected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



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

# 13 Web Menu Item > Service

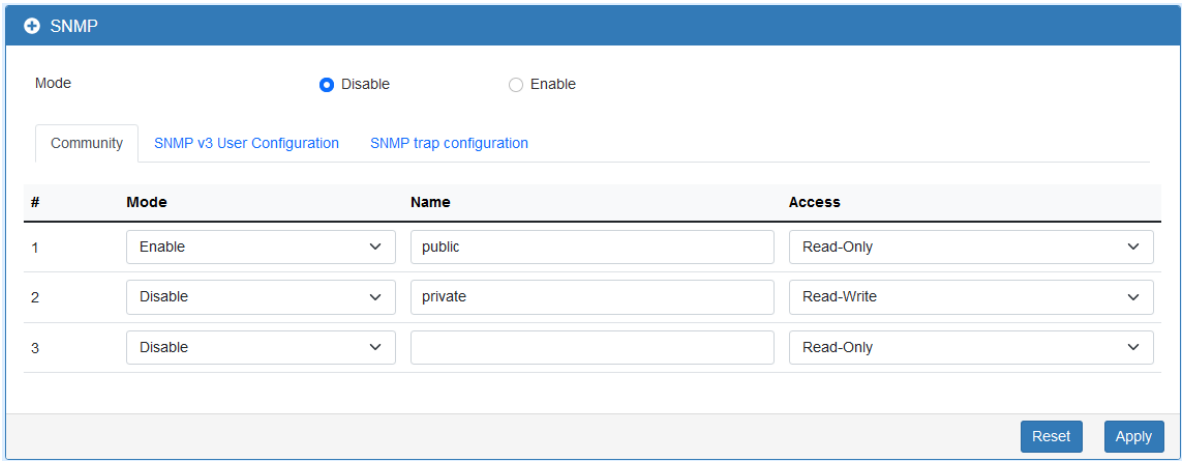
This section allows you to configure SNMP, Dynamic DNS, VRRP, SMTP, IP Alias, and QoS.




## 13.1 SNMP

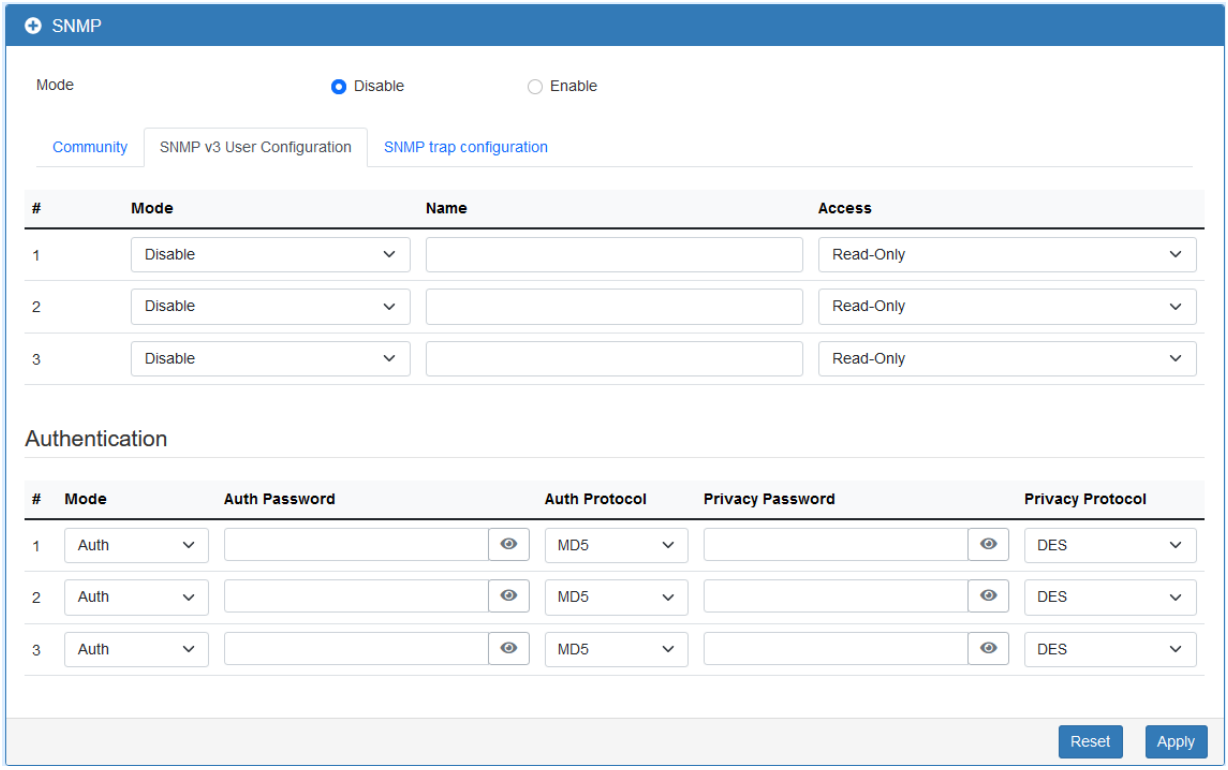
This section allows user to configure the SNMP function.

### 13.1.1 Community




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

### 13.1.2 SNMP v3 User Configuration

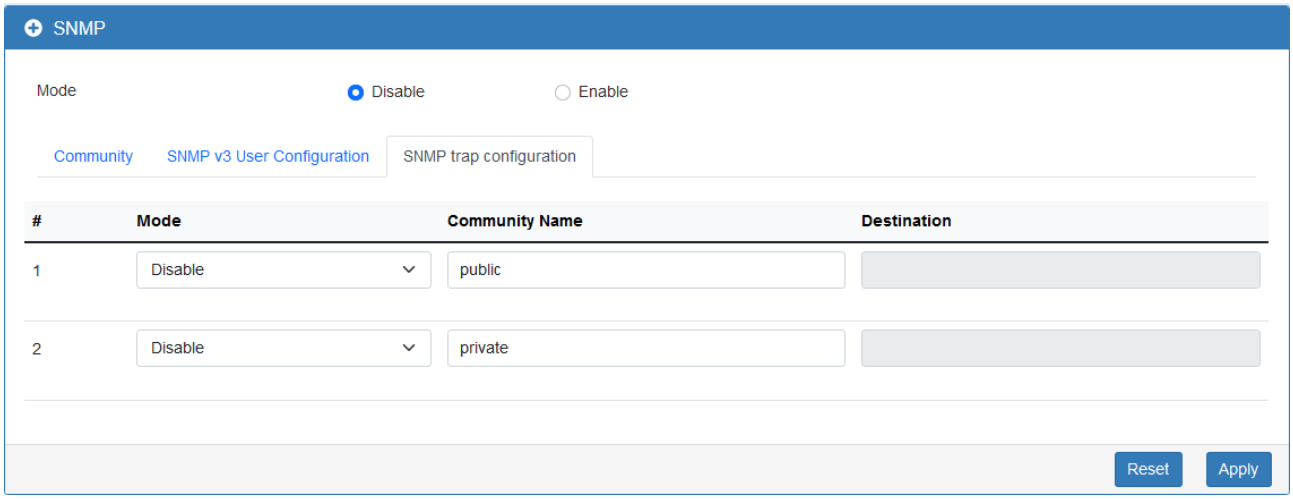


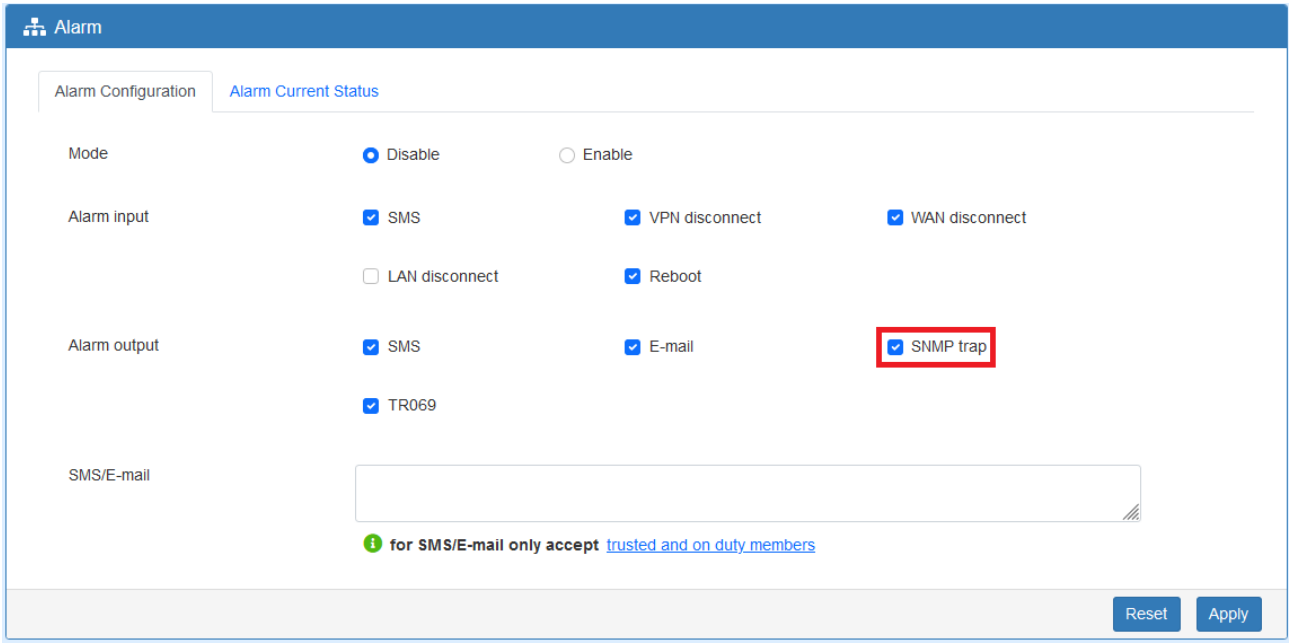

For SNMP v3 User Configuration, you need to register authentication and allow a receiver that confirm the packet was not modified in transit. There are three options to set up SNMP v3 Configuration.

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

### 13.1.3 SNMP trap configuration

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

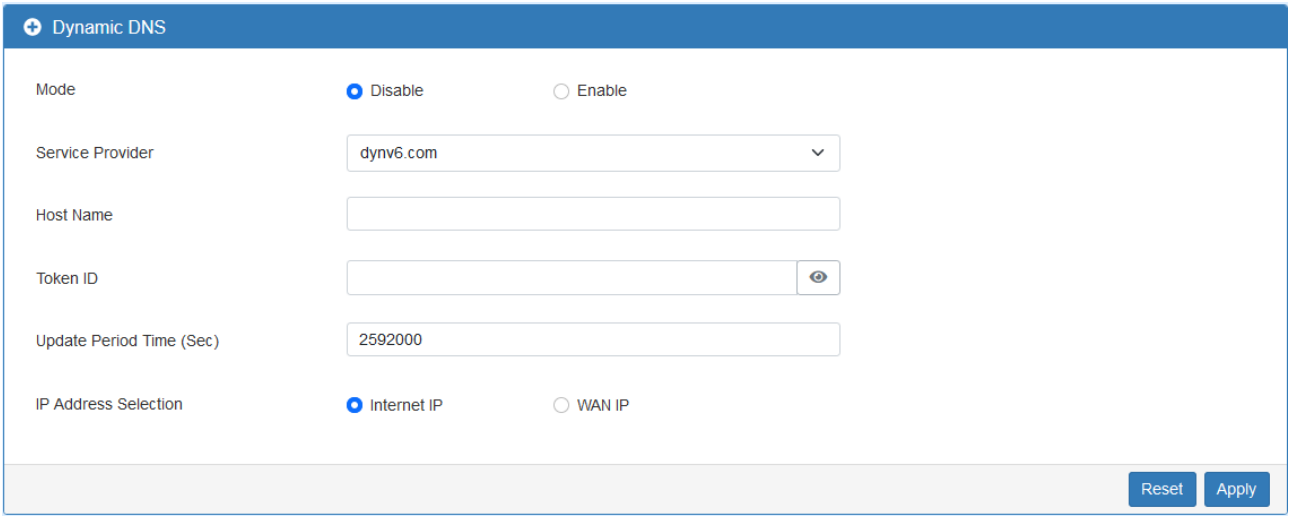



| Service > SNMP > SNMP trap configuration | |
|---|---|
| **Item** | **Description** |
| Mode | Select from Disable or Enable. The default is Disable. |
| Community Name | Fill in your community name. |
| Destination | The destination (domain name/IP) of remote SNMP trap server. |

## 13.2 Dynamic DNS

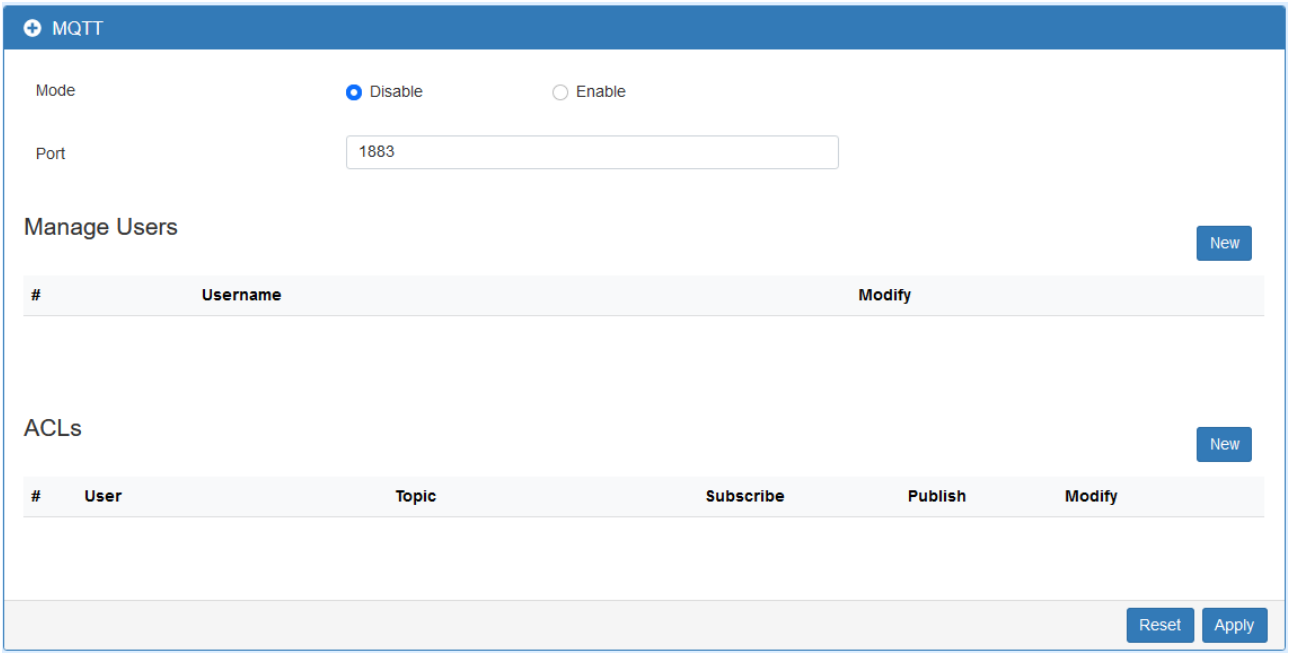
This section allows you to set up Dynamic DNS.




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

## 13.3 MQTT

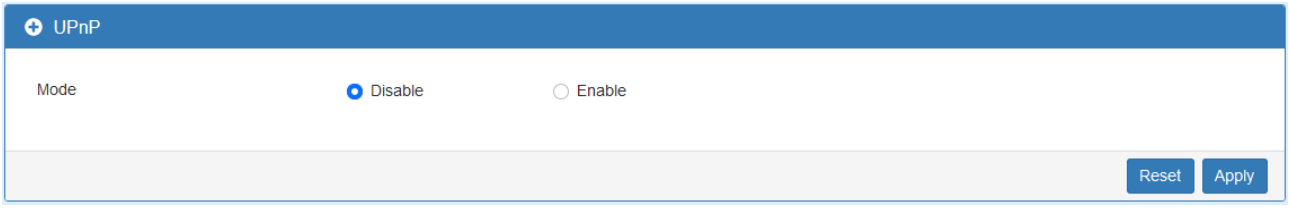
This section allows user to configure the MQTT. It allows the MQTT client to send the message within specific topic or channel. By default, the router does not allow anonymous to read/write the MQTT topic or channel. Thus, you need to create the account with username and password for MQTT client on the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




| Service > MQTT | |
|---|---|
| **Item** | **Description** |
| Mode | Select from Disable or Enable. The default is Disable. |
| Port | Fill in the port number of MQTT application. |
| Manage Users | Enter the priority value from 1 to 254. The larger value has higher priority. The default is 100. |
| Username | Fill in the username of manage user. |
| Password | Fill in the password of manage user. |
| ACLs | Allow to specify what topic should be limited. |
| User | Select the users and identify their authority to read or write the MQTT topic/channel. |
| Topic | Name the topic of MQTT message. |

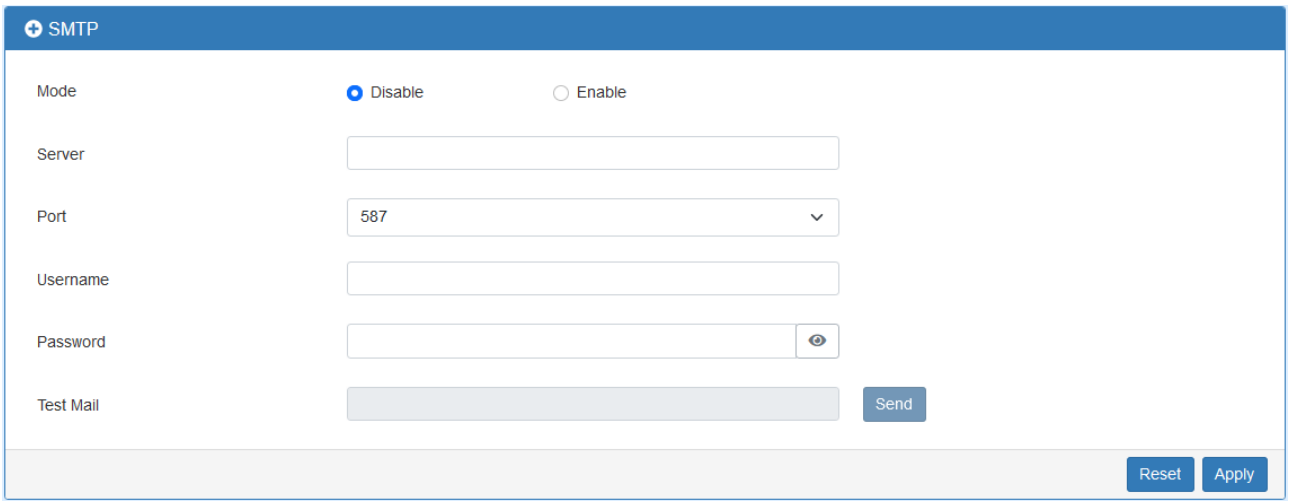
## 13.4 UPnP

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




## 13.5 SMTP

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

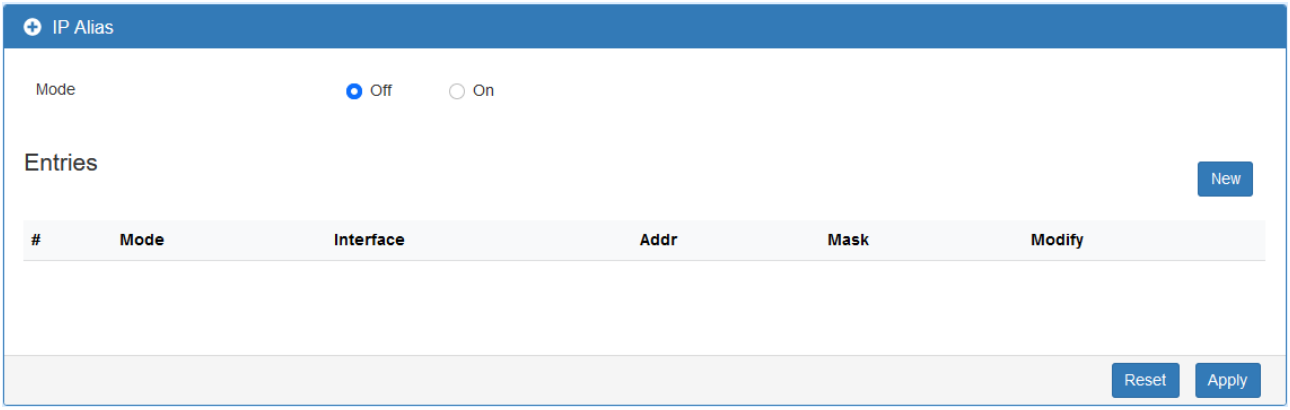


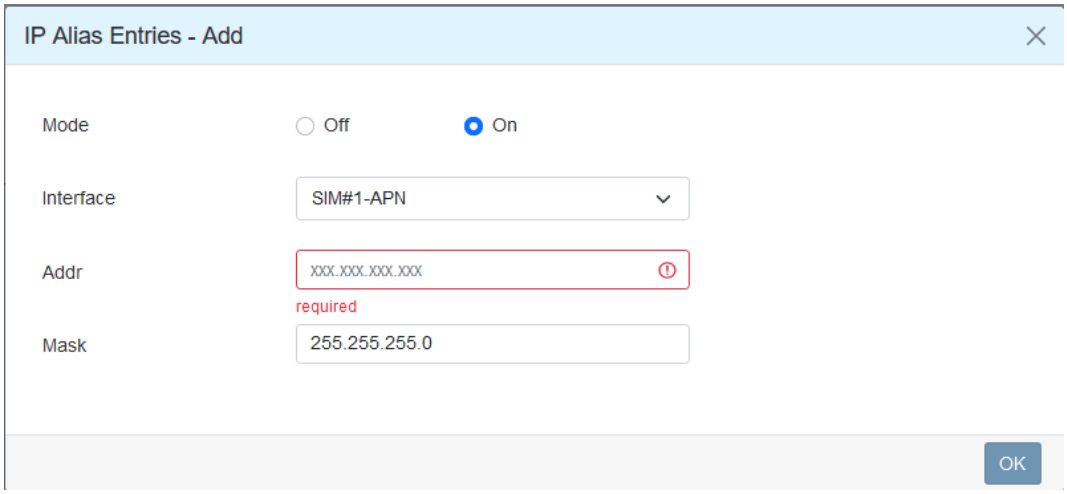

| **Service > SMTP** | |
|---|---|
| **Item** | **Description** |
| Mode | Select from Disable or Enable. The default is Disable. |
| Server | Enter the domain or IP address of the SMTP server. |
| Port | There are three ports for SMTP communication between mail servers.<br>Port 25：Use TCP port 25 without encryption.<br>Port 465：SMTP connections secured by SSL.<br>Port 587：SMTP connections secured by TLS. |
| Username / Password | Fill in your username and password as the same your server. |
| Test Mail | Enter the mail address for sending test mail. |

## 13.6 IP Alias

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

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




| **Service > IP Alias** | |
|---|---|
| **Item** | **Description** |
| Mode | Select from Off or On to enable the IP Alias. |
| Entries | View / Modify / Delete the existing entries. |
| New / Edit IP Alias Entry | Mode: select from Off or On to use or not use this entry.<br>Interface: the interface you want to provide the additional address.<br>IP Address: Enter the IP address.<br>IP Mask: Enter the network mask. |

## 13.7 QoS

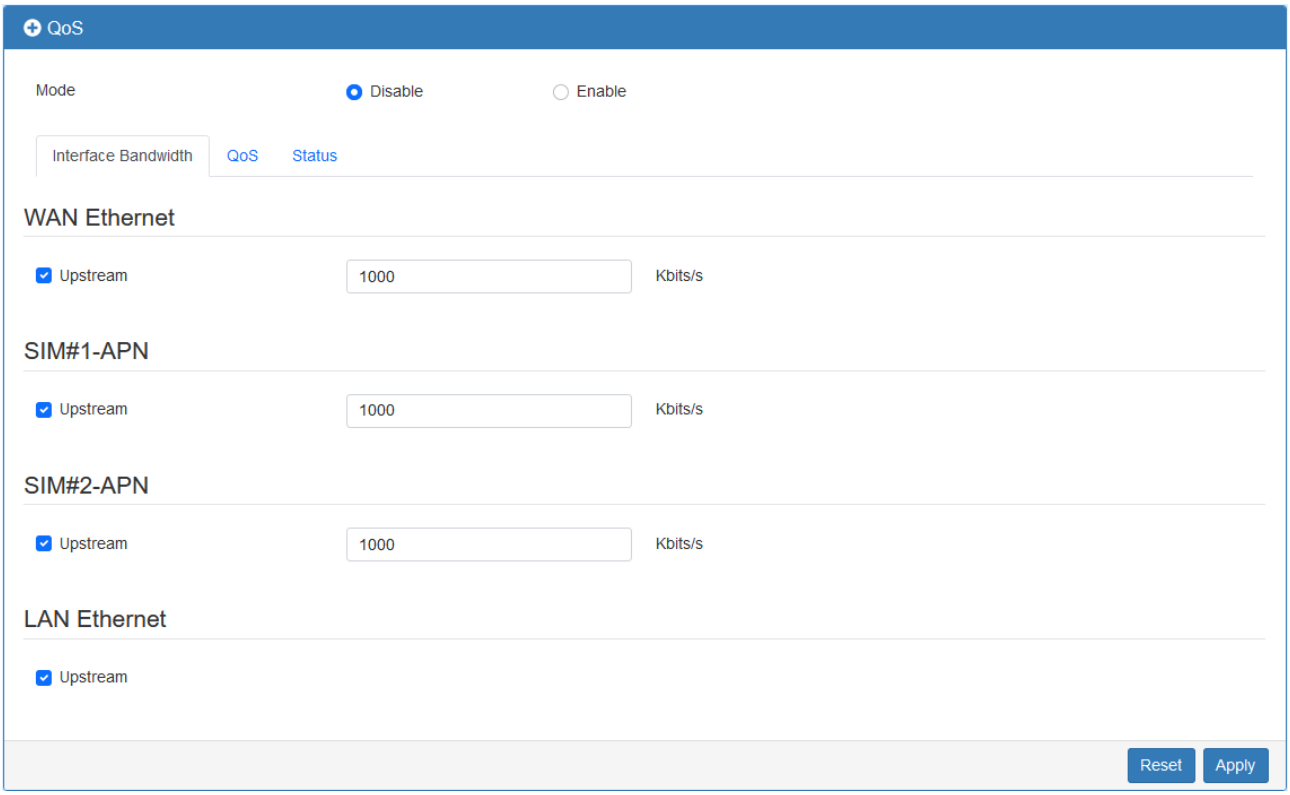
QoS (Quality of Service) refers to a network ability to achieve maximum bandwidth and allow minimum bandwidth. It guarantees the minimum and limit the maximum bandwidth class of traffic. The QoS configuration has three parts, including ISP bandwidth, QoS, and Status.

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

### 13.7.1 QoS > Interface Bandwidth

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

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



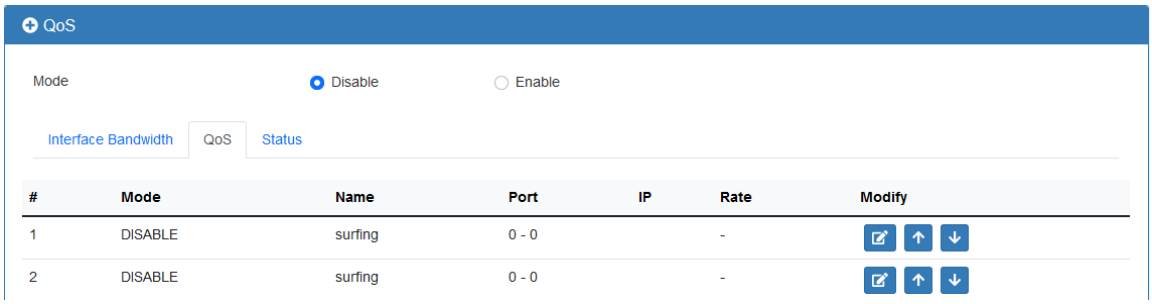

### 13.7.2 QoS > QoS

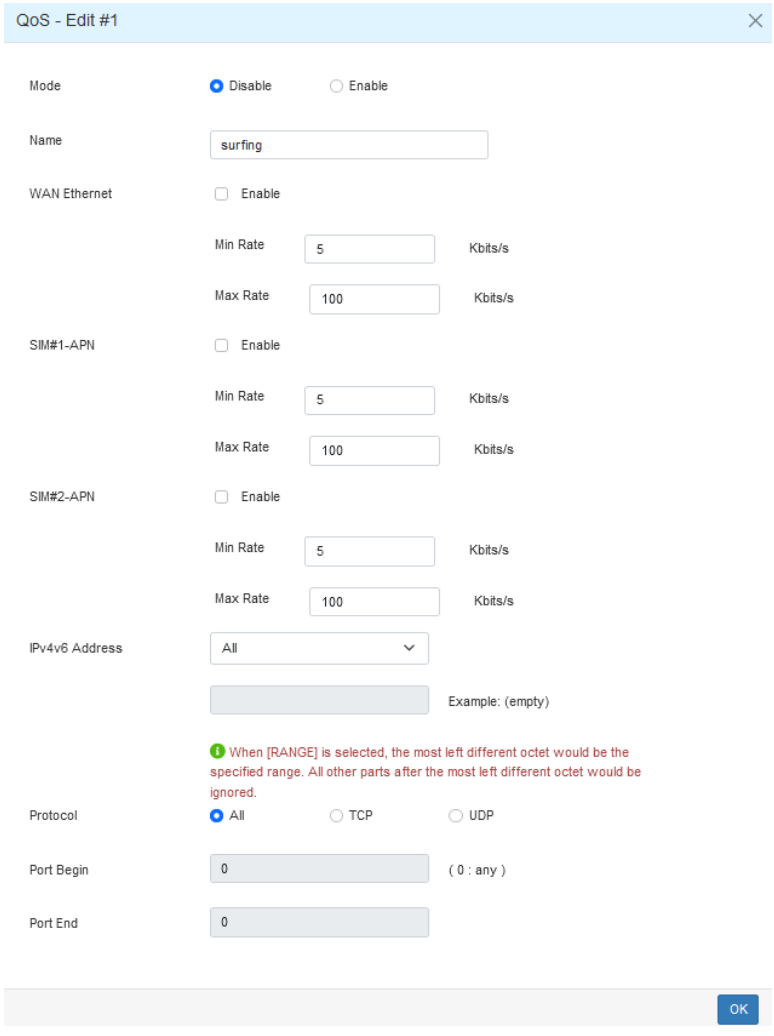
You can select QoS tab to show an overall view for QoS configuration.

At right side of window, there are three buttons.

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

The QoS entry configuration page has two parts for assigning bandwidth, and bandwidth of group IP address.




| **Service > IP Alias** | |
|---|---|
| **Item** | **Description** |
| Mode | Select from Disable or Enable QoS. |
| Name | The setting can be edited or deleted the existed entries. |

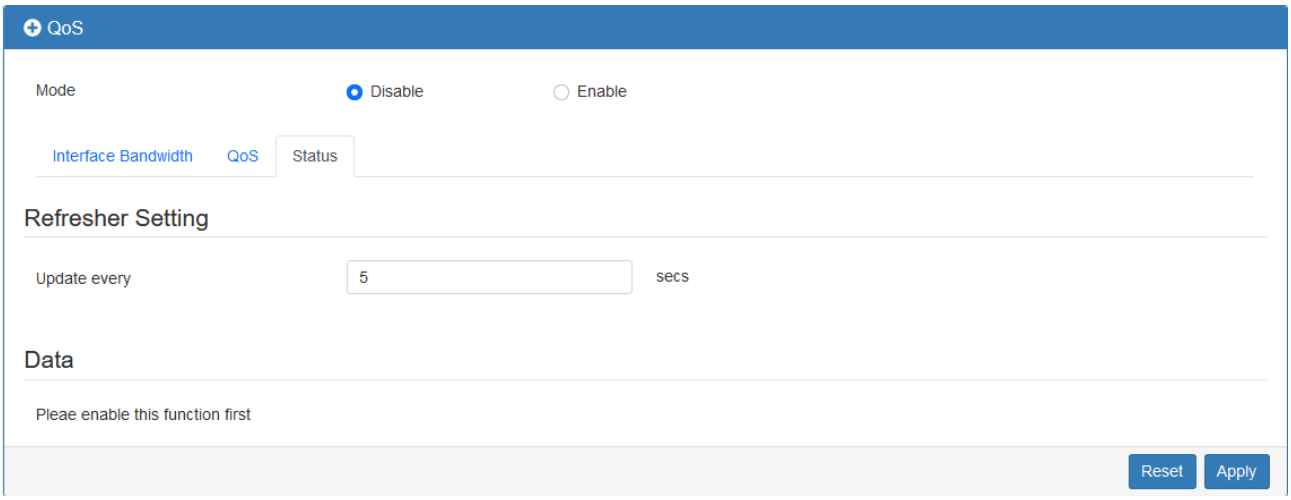
| | |
|---|---|
| Interface/Min rate(Result)/Max rate | Min Rate: This value guarantees the minimum bandwidth.<br>Max Rate: It is the maximum limited bandwidth. |
| IPv4v6 Address | Choose four types to set address format, including All, Single, Subnet, and Range. |
| Protocol | Select the protocol type of traffic. |
| Port Begin/Port End | Specify the port range of traffic. |

### 13.7.3 QoS > Status

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

- Refresh rate: how long the browser will update the showed content once with selected interface.
- Show detail bandwidth for each IP address: show the group IP bandwidth usage.
- Apply Refresh Setting button: press this button to take effect with above new settings.

Data part is the content of bandwidth usage.

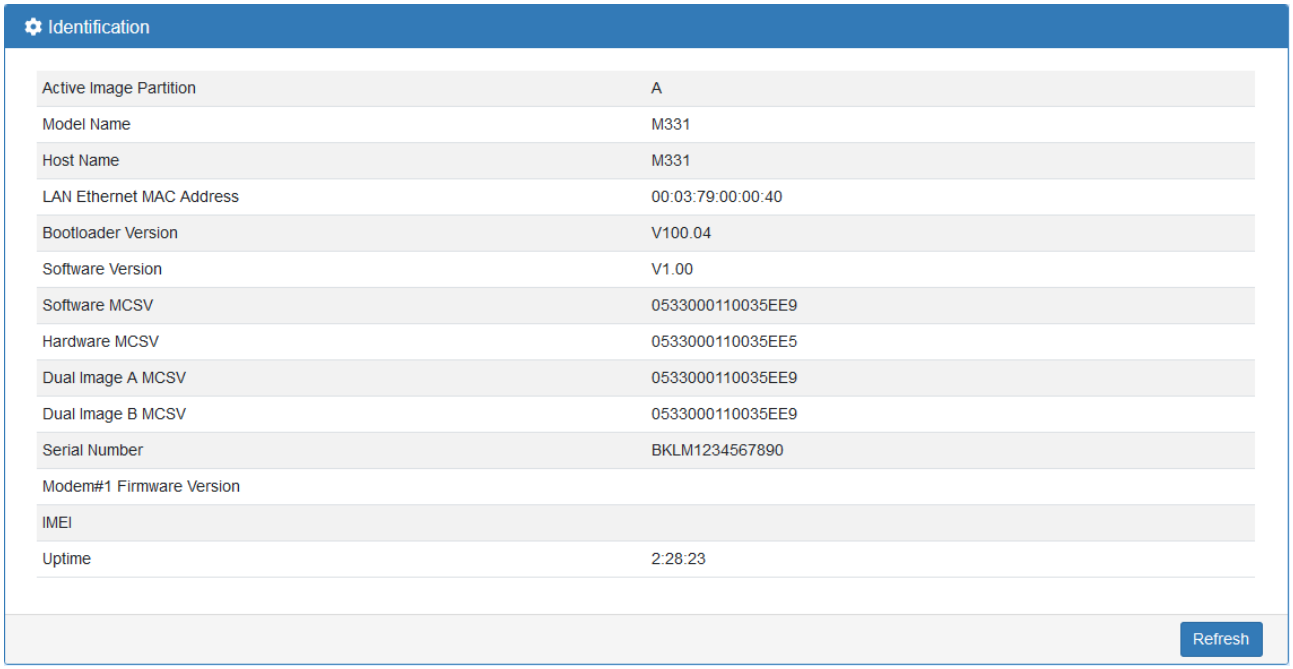


# 14 Web Menu Item > Management

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


## 14.1 Identification

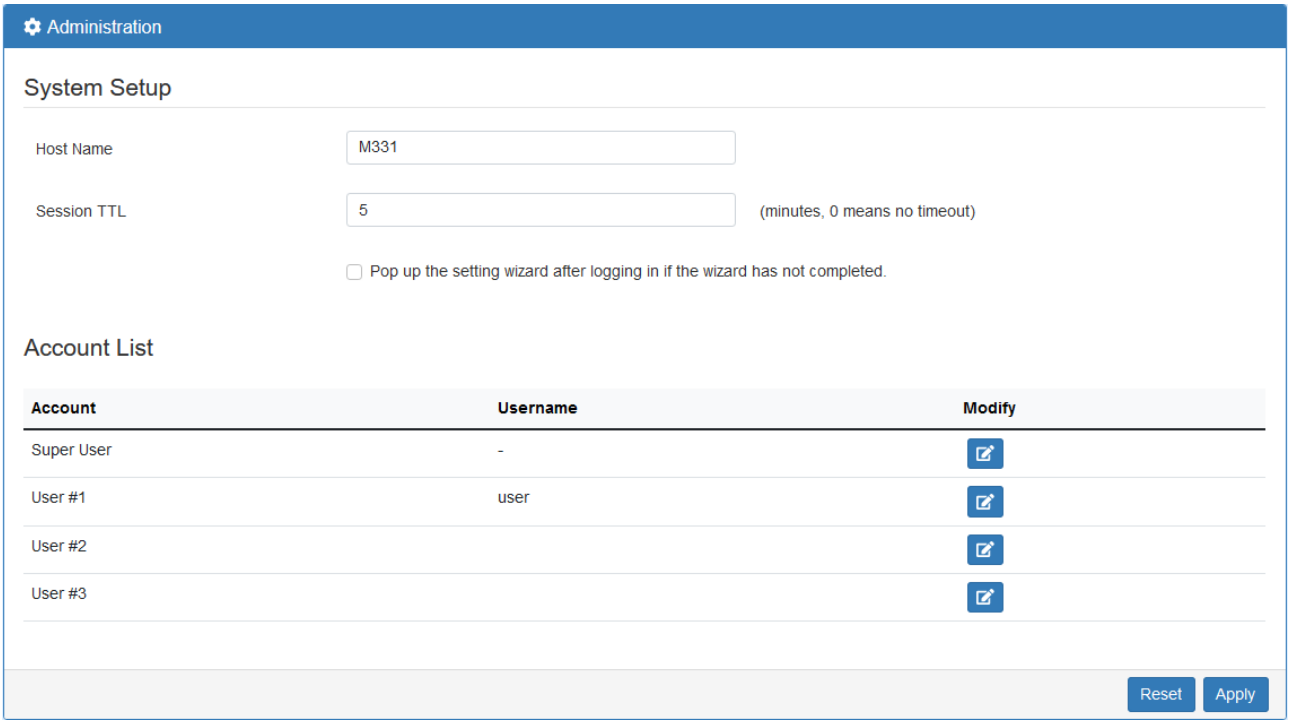
This section allows you to confirm the profile of router, current software, firmware version and system uptime.




| **Management > Identification** | |
|---|---|
| **Item** | **Description** |
| Active Image Partition | Show the active image partition: A or B |
| Model Name | Show the model name of the cellular router. |
| Host Name | Show the host name of the cellular router. |
| LAN Ethernet MAC Address | Show the MAC address of LAN interface. |
| Bootloader Version | The bootloader version of the device. |
| Software Version | Show the software version currently running on the device. |
| Software MCSV | Show the software MCSV of the running firmware. |
| Hardware MCSV | Show the hardware MCSV of the device. |
| Dual Image A MCSV | Show the Dual Image A MCSV. |
| Dual Image B MCSV | Show the Dual Image B MCSV. |
| Serial Number | Show the product serial number. |
| Modem#1 Firmware Version | Show the modem firmware version of the device. |
| IMEI | Show the International Mobile Equipment Identity number. |
| Uptime | Show the current system uptime. |

## 14.2 Administration

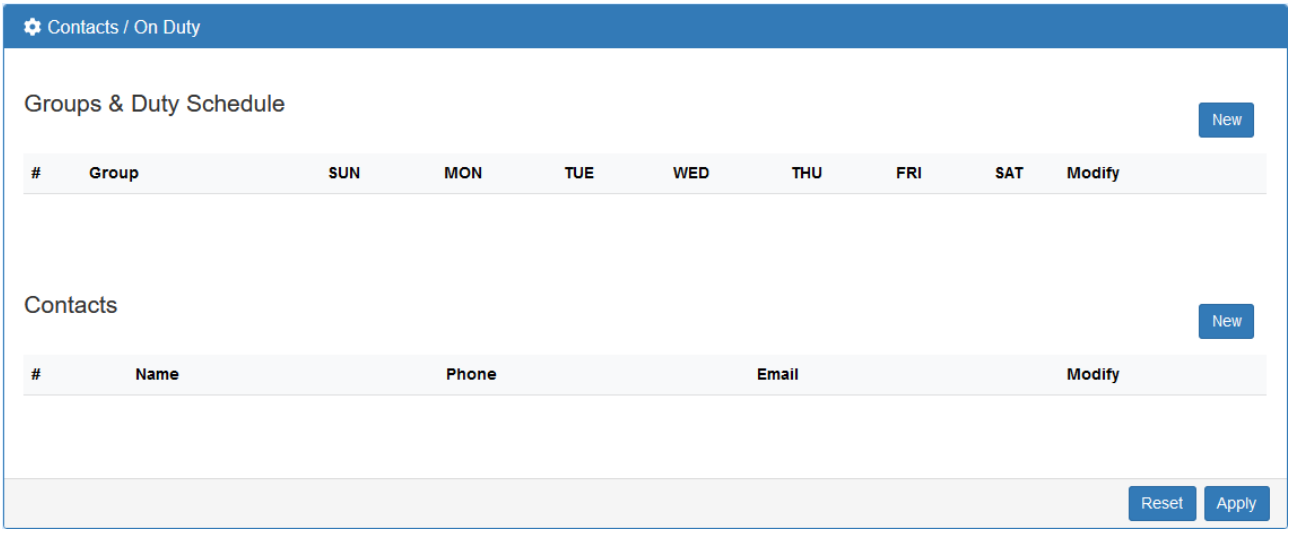
This section allows you to set up the name of system and change your new password. For the Session TTL, you can set up what duration of time will be logout. If you do not need to have this timeout limitation, you can fill in “0” (Zero).




| Management > Administration | |
|---|---|
| **Item** | **Description** |
| **System Setup** | |
| Host Name | Enter the device’s host name. |
| Session TTL | Minutes (0 means no timeout). |
| **Admin Password** | |
| New Password | Type the password you want to change. |
| Retype to confirm | Retype the password you want to change. |

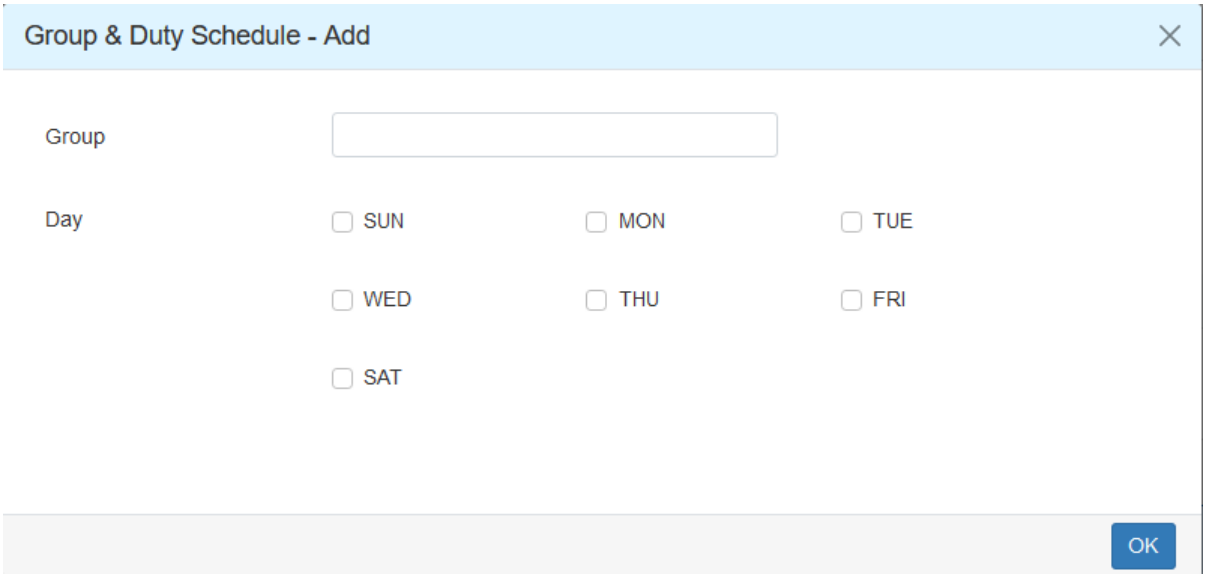
## 14.3 Contacts / On Duty

This section allows you to create groups, and add users. For more detailed instruction, please navigate to System > Alarm.



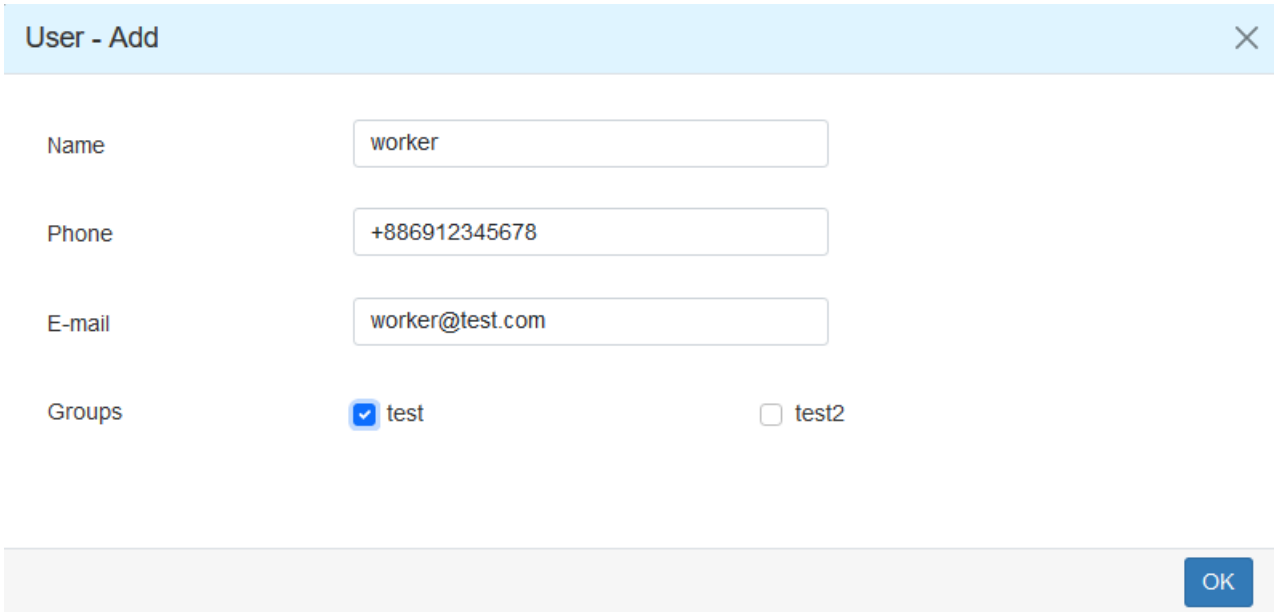

### 14.3.1 Group

Click the **New** button to create a new group. Then enter the name for the group and select the day that should be applied.




### 14.3.2 Contacts

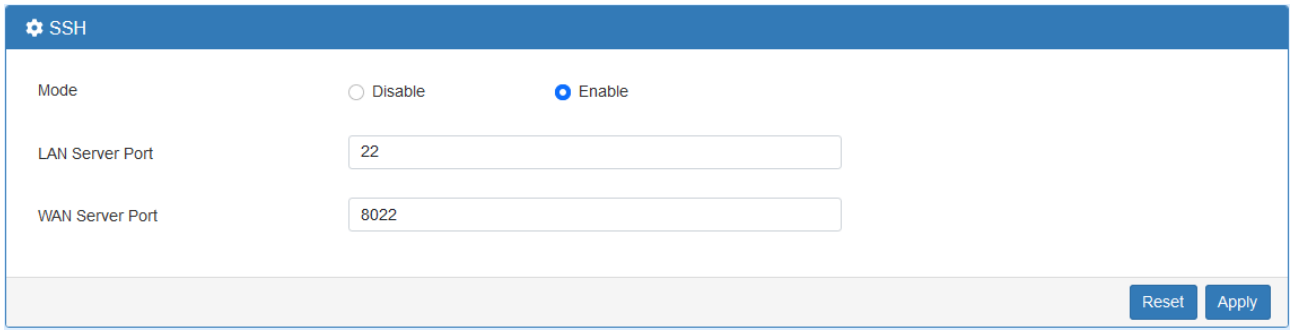
Click the **New** button to create a new user. Enter the user's information and select the group which created by above step.




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

## 14.4 SSH

Secure Shell (SSH) allows user to configure system via a secure channel.

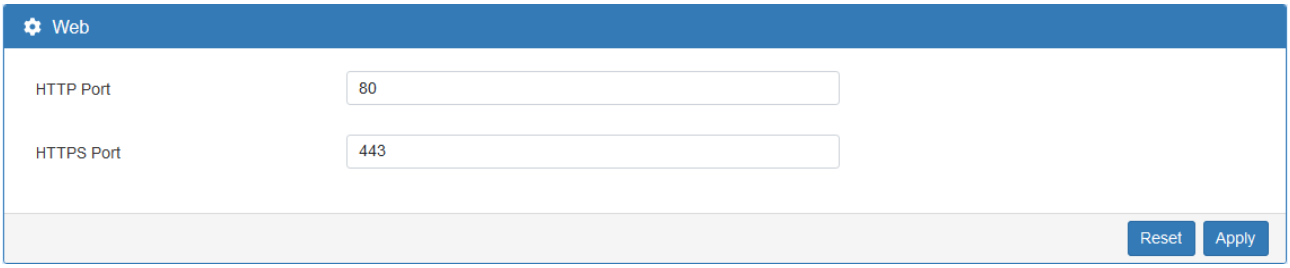



| **Management > SSH** | |
|---|---|
| **Item** | **Description** |
| Mode | Select from Disable or Enable SSH function. |
| LAN Server Port | The listen port on LAN interface. |
| WAN Server Port | The listen port on WAN interface. |

## 14.5 Web

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

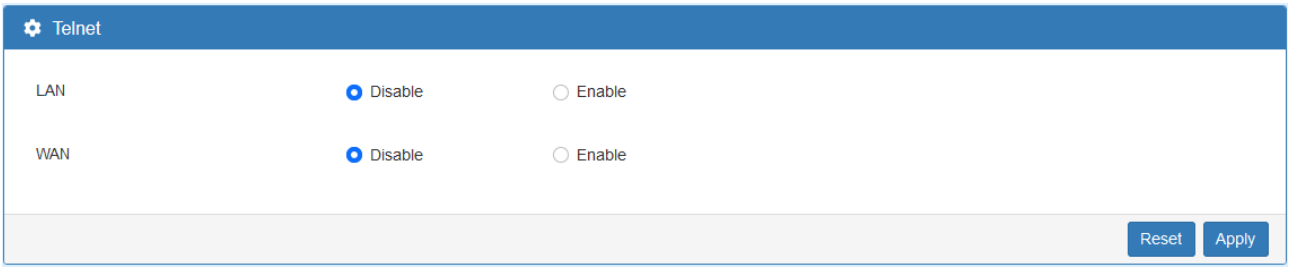
After pressing Apply button, the device will apply immediately and give you some hints "Please use new port to access latter". For example, port 3000.




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

## 14.6 Telnet

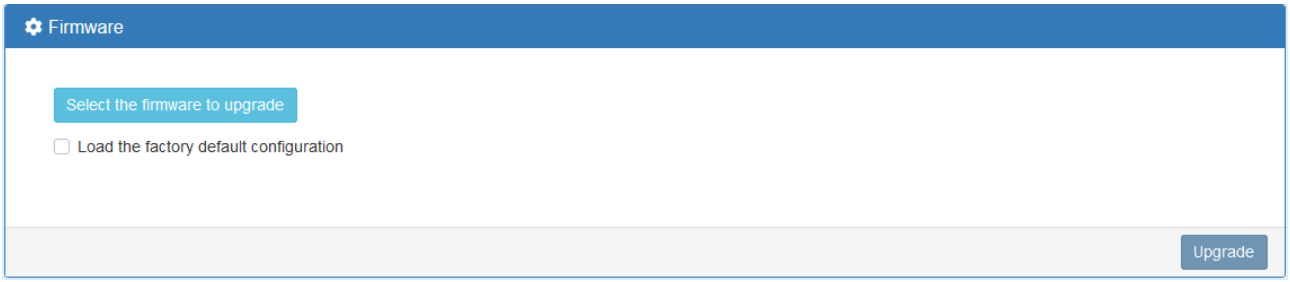
This section allows user to choose whether offer the telnet via LAN/WAN. Default is disale.




| Management > Telnet | |
|---|---|
| **Item** | **Description** |
| LAN | Whether or not offer the telnet service. |
| WAN | Whether or not offer the telnet service. |

## 14.7 Firmware

This section provides you to upgrade the firmware of the device.



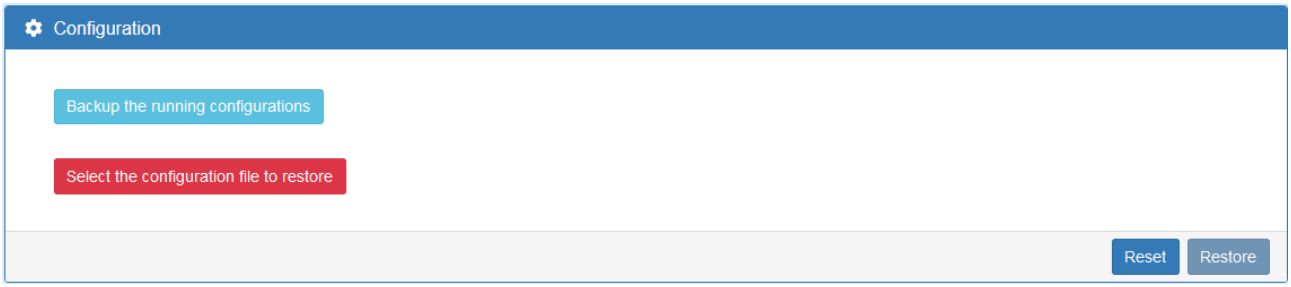

(1) Click Select the firmware to upgrade button to choose your current firmware version in your PC.

(2) Select Upgrade button to update.

(3) After upgrading successfully, the device will reboot automatically. The configuration will reset to factory default after upgrading when “Load the factory default configuration” checked.

## 14.8 Configuration

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

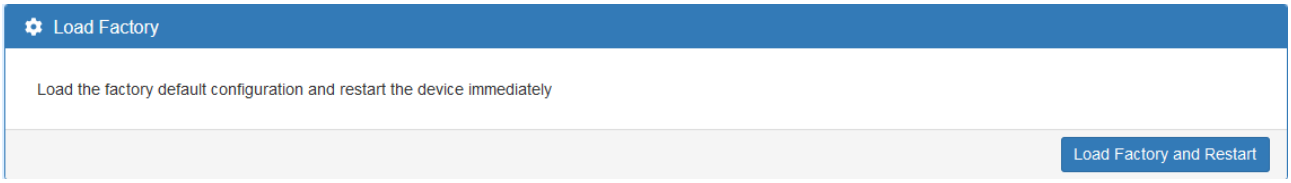



(1) Click Backup the running configurations button to export your current configurations.

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

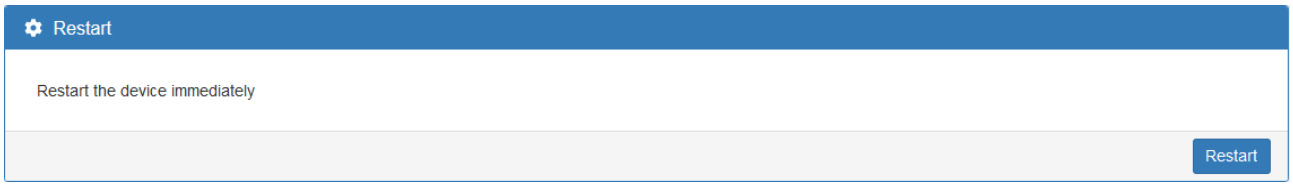
## 14.9 Load Factory

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



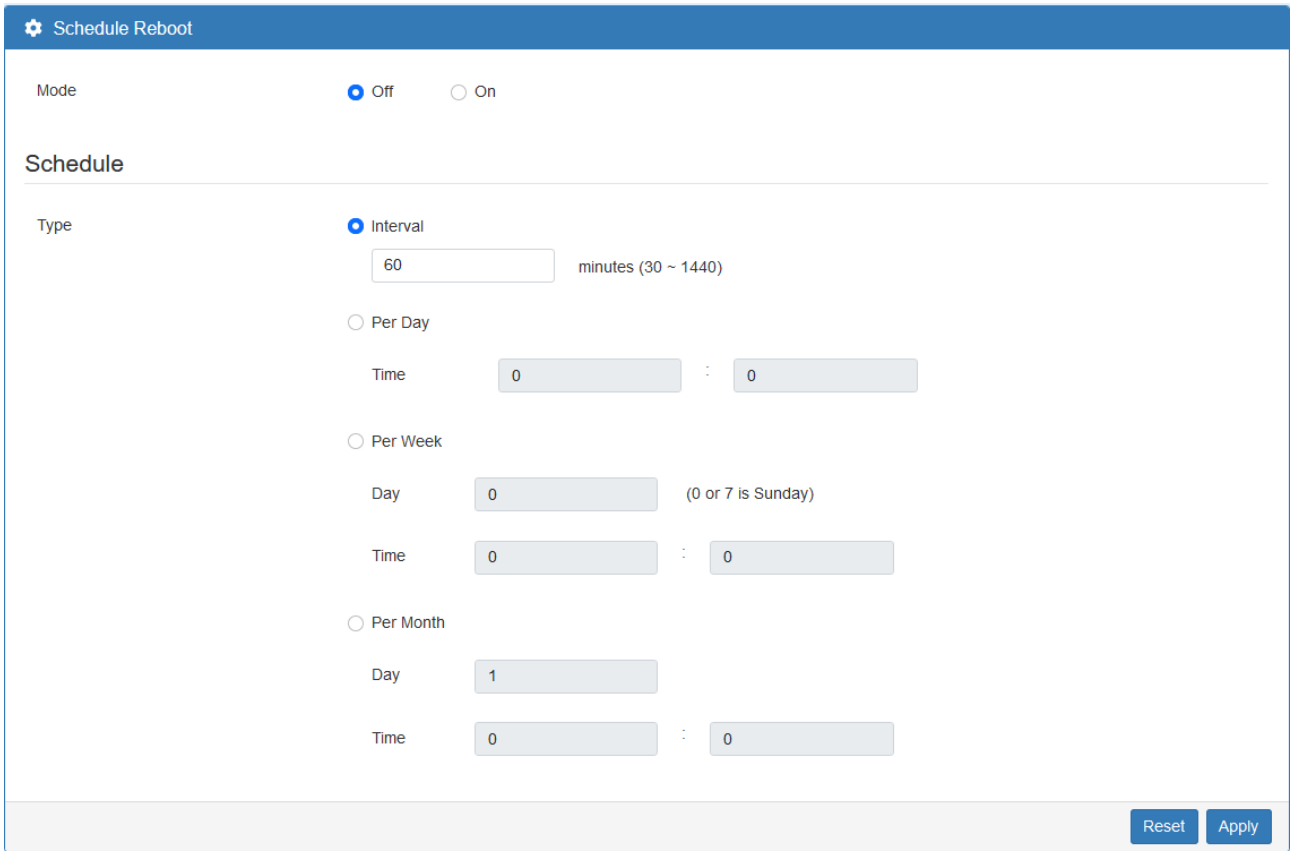

## 14.10 Restart

This section allows you to click Restart button to restart immediately.



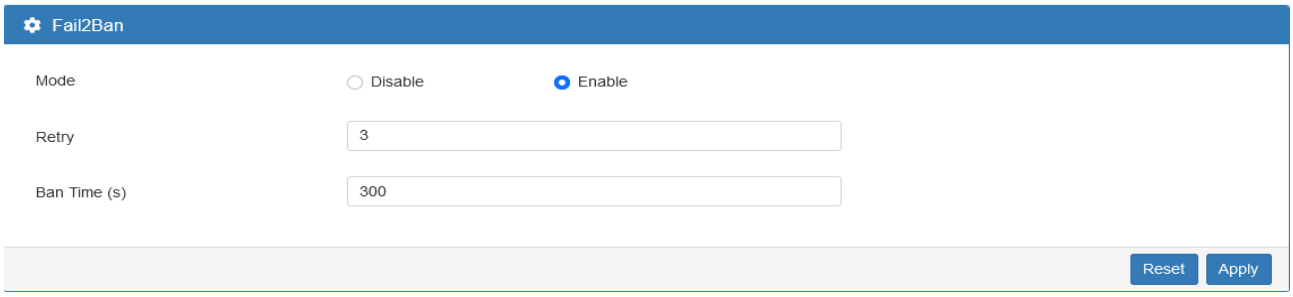

## 14.11 Schedule Reboot

The setting allows you to schedule the reboot time regularly.



## 14.12 Fail2Ban

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




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

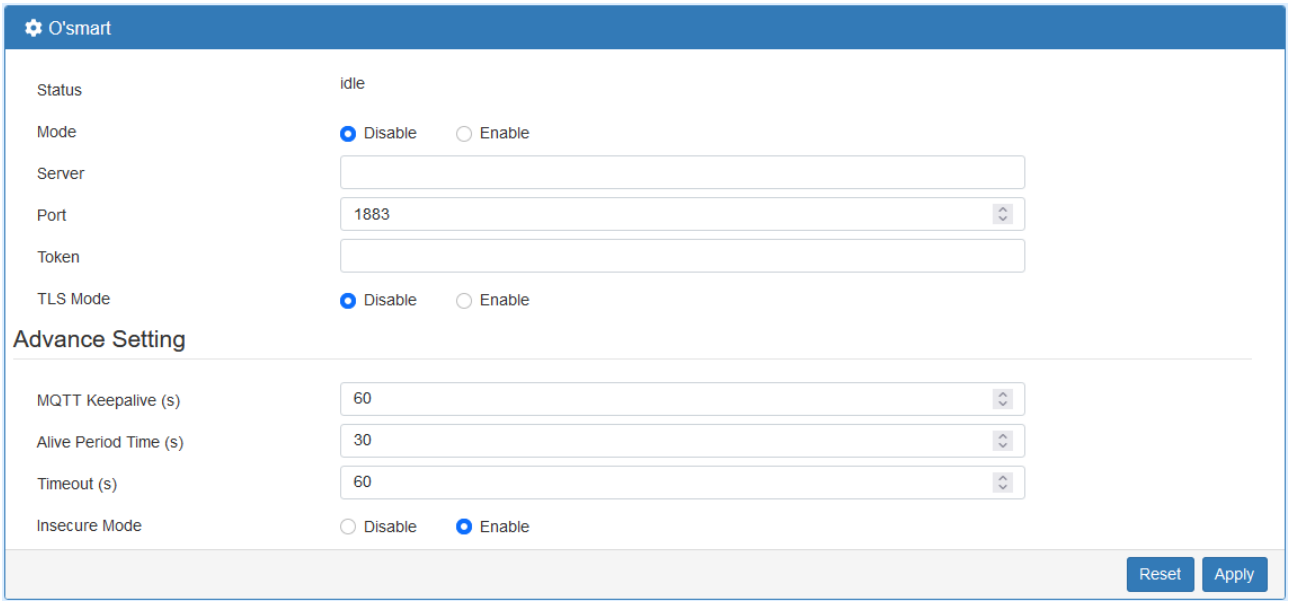
***Note:*** There is an example to explain how to configure. E.g. Assume the retry is 3 and the ban time is 300 seconds. If a specified IP has 3 login failures within 5 minutes then it will be banned 300 seconds. Moreover, if it keeps to attempt a login and still fail then the banned time will be extended automatically.

| Time | The count of login failure | The banned time (s) |
|---|---|---|
| 2019/1/1 12:00:00 | 0 | 0 |
| 2019/1/1 12:00:01 | 1 | 0 |
| 2019/1/1 12:00:03 | 3 | 300 |
| 2019/1/1 12:00:10 | 4 | 300 |
| 2019/1/1 12:00:30 | 6 | 600 |

## 14.13 O’smart

This section allows you to set up the connection with O’smart IoT management system.

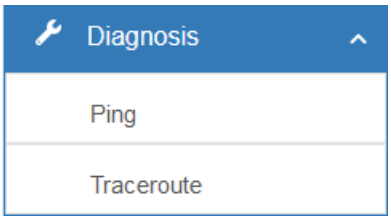
About the O’smart setting, please contact with reseller.




| **Management > O’smart** | |
|---|---|
| **Item** | **Description** |
| Status | The status between device and O’smart server. |
| Mode | Enable or disable the connection with O’smart server. |
| Server | Enter the O’smart server IP address or domain name. |
| Port | Enter the listen port of O’smart server. |
| Token | Enter the token that generated by O’smart server. |
| TLS Mode | Enable or disable the secure connection with O’smart server. |
| **Advance Setting** | |
| MQTT Keep alive | |
| Alive Period Time | |
| Timeout | |
| Insecure Mode | |

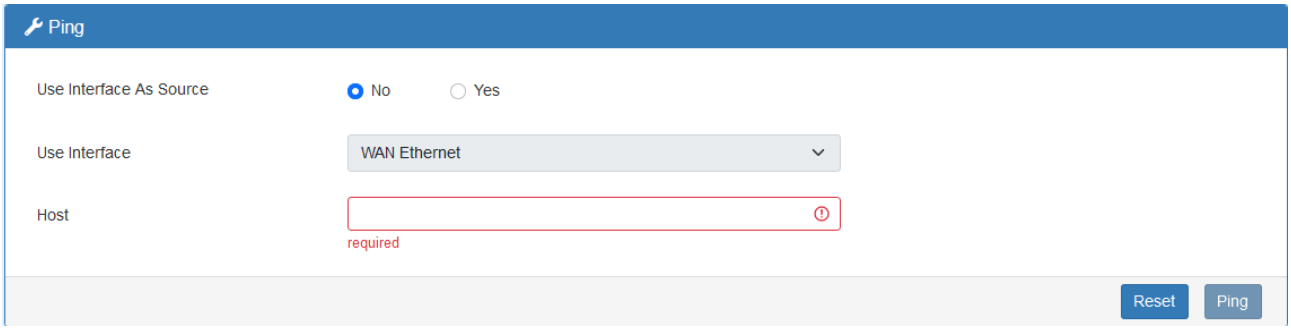
# 15 Web Menu Item > Diagnosis

This section allows you to diagnose Ping and Traceroute.




## 15.1 Ping

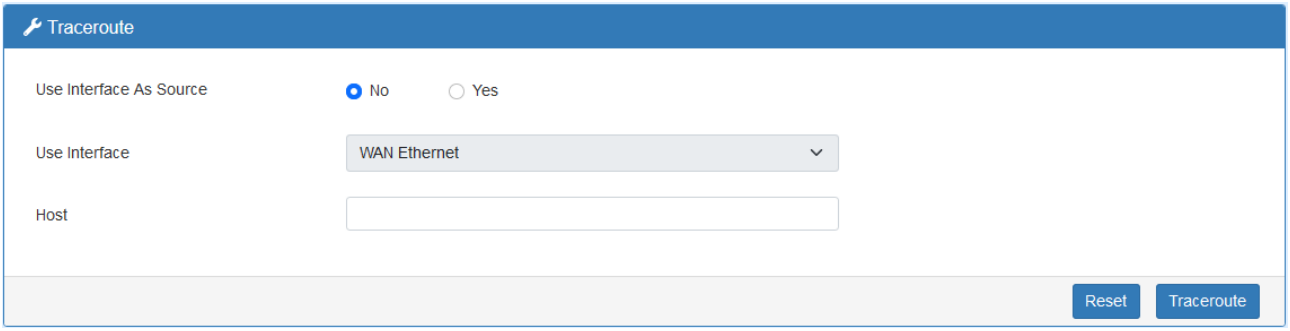
Please assign the Host that you want to ping.




| Diagnosis > Ping | |
|---|---|
| **Item** | **Description** |
| Use Interface as Source | When set to Yes, it will use the selected interface as source IP. |
| Use Interface | Specify the IP address of selected interface as source IP. |
| Host | The host name or the host IP address |

## 15.2 Traceroute

Please assign the Host you want to traceroute.



| Diagnosis > Traceroute | |
|---|---|
| **Item** | **Description** |
| Use Interface as Source | When set to Yes, it will use the selected interface as source IP. |
| Use Interface | Specify the IP address of selected interface as source IP. |
| Host | The host name or the host IP address |

# 16 Troubleshooting Guide

## 16.1 Troubleshooting Information

If you encounter any issue, please refer to the following troubleshooting guide table first for solutions to common problems:

If you cannot find your issue listed here, please refer to the User Manual document for more information that may help you solve your problem.

| Problem Type Table | | |
|---|---|---|
| No. | Problem Type | Description |
| 1 | The Cellular Router No power. | Unit has no power. |
| 2 | The Cellular Router Access Issue. | Cannot access the Web management page. |
| 3 | No internet (From the Cellular Router). | No Internet from your LTE network. |

### 16.2.1 The Cellular Router “No Power” Problem

#Problem 1: Unit has no power.

For the possible solotion, please try the following:

a. Unplug and replug your power adapter from the power source.

b. Disconnect and Connect the Ethernet cable from the Ethernet port of Cellular Router.

If the above didn’t solve your “No power” issue, please contact your support engineer for further advanced troubleshooting. (This could involve a possible software or hardware problem that needs to be identified and solved.)

### 16.2.2 The Cellular Router “Access Issue” Problem

#Problem 2: Cannot access the Web Management page.

For the possible solotion, please try the following:

a. Check that your PC Ethernet card is enabled and configured to get the IP/DNS address automatically.

b. Disconnect and connect the Ethernet cable from the Ethernet port of Cellular Router.

c. Ping the LAN IP (default IP is 192.168.1.1). The ping should PASS.

d. If ping is OK, please try to access the Web Management page again.

If the above didn’t solve your Access Issue then please contact your MIS or anyone that build your network infrastructure to fix the ping fail problem.

If your network infrastructure is confirmed to be OK (hardware works normally and is configured correctly), please contact your support engineer for further advanced troubleshooting. (This could involve a possible software or hardware problem that needs to be identified and solved.)

### 16.2.3 No Internet (from the Cellular Router) Problem

#Problem 3: No Internet from LTE network of Cellular Router.

The problem might be on the physical contact of the SIM card.

- For the possible solution 1, please try the following:

a. Remove your SIM card.

b. Please re-insert it again (Cheking that the SIM card is in the correct orentation).

c. Reboot the Cellular Router by turning Off/On the power source.

d. Wait for at least 3 minues and check again if you receive internet correctly.

If the above didn't solve your "No internet" issue then please continue to solution2 bellow.

- For the possible solution 2, please try the following:

a. Access the Web management page (default url is http://192.168.1.1/).

b. Check that the LTE configuration is OK by going to the "Cellular -> SIM Config" web page.

c. If you change any configuration, please wait for 2 minues after apply and check again the internet.

If the above didn't solve your "No internet" issue then please check that your SIM card is active and with traffic enabled (by contacting your SIM card provider or by trying that SIM card in another device).

If you are still experiencing the "No internet issue" then please contact your support engineer for further advanced trublesooting (This could involve a posible Software or Hardware problem that needs to be identified and solved).