



# **Barox**

## **PD°MR°301/101°GS**

### **Industrial 4G LTE Router**

## **User Manual**

Version 1.0

**Copyright by Barox Communications Inc**

The information in this document has been checked carefully and is believed to be correct as of the date of publication. Barox Communications Inc. reserves the right to make changes in the product of specification, or both, presented in this publication at any time without notice. Barox Communications assumes no responsibility or liability arising from the specification listed herein. Barox Communications make no representations that the use of its products in the manner described in this publication will not infringe on existing or future patents, trademark, copyright, or rights of third parties. Implication or other under any patent or patent rights of Barox Communications Inc grants no license. All other trademarks and registered trademarks are the property of their respective holders.

**Revision History :**

Version	Date	Change Note
1.0	6/28/2017	Initial Release

# Table of Contents

<b>1</b>	<b>Introduction.....</b>	<b>1</b>
1.1	Features .....	1
1.2	Specifications .....	2
1.3	Mechanical Dimensions .....	2
1.4	Hardware Panel Layout.....	3
<b>2</b>	<b>Hardware Installation.....</b>	<b>7</b>
2.1	LED Indicators.....	7
2.2	Ethernet Port .....	7
2.3	Serial Port COM1 (Console) .....	9
2.4	Install the SIM Card.....	9
2.5	Reset Button .....	10
2.6	External Antenna.....	10
2.7	Connecting the Power Supply.....	10
2.8	Grounding the Router.....	11
2.9	Pin Assignments.....	11
2.10	Connecting I/O Ports.....	12
2.11	Serial Port COM2 (RS <sup>o</sup> 232) .....	13
2.12	Serial Port COM3 (RS <sup>o</sup> 485) .....	13
2.13	DIP Switch.....	14
<b>3</b>	<b>Configuration via Web Browser.....</b>	<b>15</b>
<b>4</b>	<b>Status .....</b>	<b>16</b>
4.1	Status > GPS.....	17
<b>5</b>	<b>Configuration &gt; System .....</b>	<b>18</b>
5.1	System > Time and Date.....	18
5.2	System > COM Ports .....	20
5.3	System > Logging .....	22
5.3.1	Logging > Logging .....	23
5.3.2	Logging > Log .....	23
5.4	System > Alarm .....	24
5.5	System > Ethernet Ports .....	27
5.6	System > Modbus .....	27
<b>6</b>	<b>Configuration &gt; WAN.....</b>	<b>29</b>
6.1	WAN > Priority.....	29
6.2	WAN > LTE Config .....	29
6.3	WAN > Dual SIM .....	30
6.4	WAN > Ethernet .....	34
6.5	WAN > IPv6 DNS .....	36
<b>7</b>	<b>Configuration &gt; LAN.....</b>	<b>38</b>
7.1	LAN > IPv4 .....	38
7.2	LAN > IPv6.....	39

<b>8</b>	<b>Configuration &gt; Service .....</b>	<b>41</b>
8.1	Service > Configuration OpenVPN .....	41
8.2	Service > Configuration IPSec .....	47
8.3	Service > Configuration Port Forwarding .....	50
8.4	Service > Dynamic DNS .....	52
8.5	Service > DMZ .....	54
8.6	Service > SNMP .....	54
	8.6.1 SNMP configuration .....	54
	8.6.2 SNMP v3 User configuration .....	55
	8.6.3 SNMP trap configuration .....	56
8.7	Service > IP Filter .....	58
8.8	Service > MAC Filter .....	60
8.9	Service > URL Filter .....	62
<b>9</b>	<b>Management.....</b>	<b>63</b>
9.1	Identification .....	63
9.2	Administration .....	64
9.3	Firmware .....	64
9.4	Configuration .....	64
9.5	Load Factory .....	65
9.6	Restart.....	65

# 1 Introduction

**Barox M300/M301** series 4G/LTE Router is a highly reliable and secure wireless communications gateway designed for industrial networking. It supports multi-band connectivity including FDD/TDD LTE, WCDMA and GSM for a wide range of applications and vertical machine-to-machine (M2M) markets. To enhance reliability, **M300/M301** series is equipped with dual SIM that supports failover and roaming over to ensure uninterrupted connectivity for mission-critical cellular communications.

With flexible LAN/WAN Ethernet options, **M300/M301** series allows you to customize your professional applications in diverse environments. It also provides enterprise-grade software features, such as Quality of Service (QoS) for traffic prioritization, IPSec, OpenVPN, Firewall security and etc. The device is administrated via web GUI, Telnet, SSH v2 and HTTP/HTTPS.

Built for secure and uninterrupted operation in harsh environments, **M300/M301** series supports extended operating temperature from -20 to +70°C and a flexible input voltage range of 10-32V DC. **Barox M300/M301** series is an ideal cellular communications solution for heavy industrial use.

---

## 1.1 Features

- Highly reliable and secure for mission-critical cellular communications
- Provide flexible options to configure LAN/ WAN ports
- Support multi-band connectivity with FDD LTE/ TDD LTE/ WCDMA/ GSM/ LTE Cat4
- Built-in dual SIM for network redundancy
- Integrated dual detachable antenna against radio interference
- LED indicators for connection and data transmission status
- Industrial rated from -20°C to +70°C for use in harsh environments
- IPv6/IPv4 dual stack and all applications are IPv6 ready

## 1.2 Specifications

### LTE Interface

- FDD LTE: B1/B3/B5/B7/B8/B20
- TDD LTE: B38/B40/B41
- WCDMA: B1/B5/B8
- GSM: 900/1800 MHz
- LTE Cat4

### Processor & I/O Interface

- High performance 528 MHz CPU with 512 Mbytes of DDR3 memory
- 2 x SIM Card Slots
- 1 x LAN 10/100 Mbps Ethernet port (Model: M300)
- 3 x LAN 10/100 Mbps Ethernet ports (Model: M301)
- 1 x WAN 10/100 Mbps Ethernet port
- Reset Button
- Console: 1 x RS232 (9°pin Sub°D)
- 2 x SMA connectors for detachable LTE antenna
- 1 x GPS detachable antenna (Optional)
- 1 x RS485 (D+/D°)
- 1 x RS232 (TXD/RXD)
- 2 x DI, 1 x DO (Alarm +/°)

### Physical Characteristics

- Enclosure : Metal Shell
- Housing : IP40 Protection
- Dimensions (W x H x D) : 110 x 60 x 106 mm
- Installation : DIN Rail (Default) or Wall Mount (Optional)

### LED Display

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

### Power Supply

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

### Software

#### Network Protocols:

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

#### Routing/Firewall:

NAT, Virtual Server, DMZ, MAC Filter, URL Filter, IP Filter, VLAN, Static Routing and RIP°1/2

#### VPN:

OpenVPN, IPSec (3DES, AES128, AES196, AES256, MD5, SHA°1, SHA256)

#### Wireless Connectivity:

Two SIM for failover/ roaming over/ back up  
Two SIM data usage control  
Seamless multi WAN connections switch

#### Others:

DDNS, QoS, Virtual COM, UPnP

#### Alarm:

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

### Management Software

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

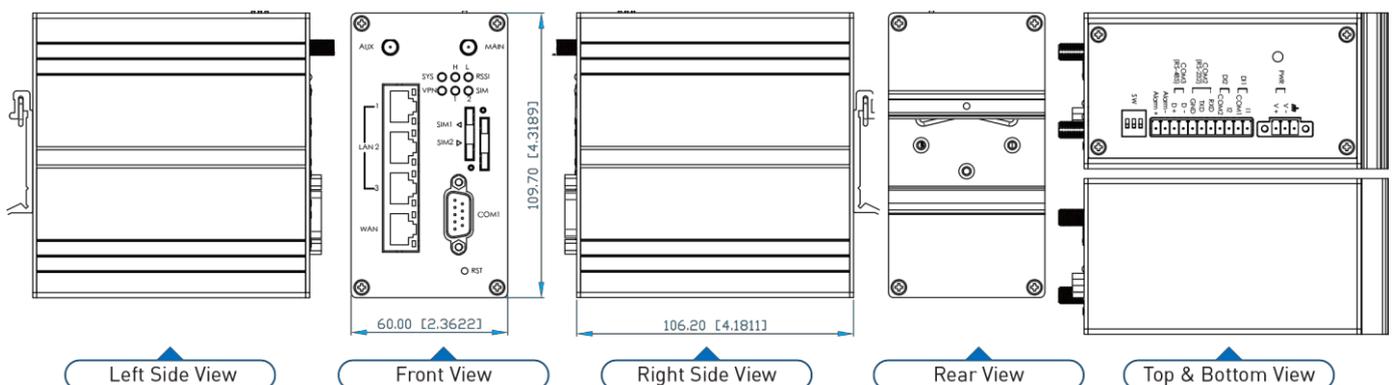
### Environment

- Operating Temperature °20 ~ +70°C
- Storage Temperature °40 ~ +85°C
- Ambient Relative Humidity 10 ~ 95% (non°condensing)
- Humidity 0 ~ 95% (non°condensing)

### Standards and Certifications

- EMC : CE, FCC
- EMI : EN 55032 Class A, FCC Part 15 Subpart B Class A
- EMS : EN 55024 / EN 61000°4°2 (ESD) Level 3 / EN 61000°4°3 (RS) Level 3 / EN 61000°4°4 (EFT) Level 4 / EN 61000°4°5 (Surge) Level 3 / EN 61000°4°6 (CS) Level 3 / EN 61000°4°8 (PFMF) Level 1 / EN 61000°4°11

## 1.3 Mechanical Dimensions



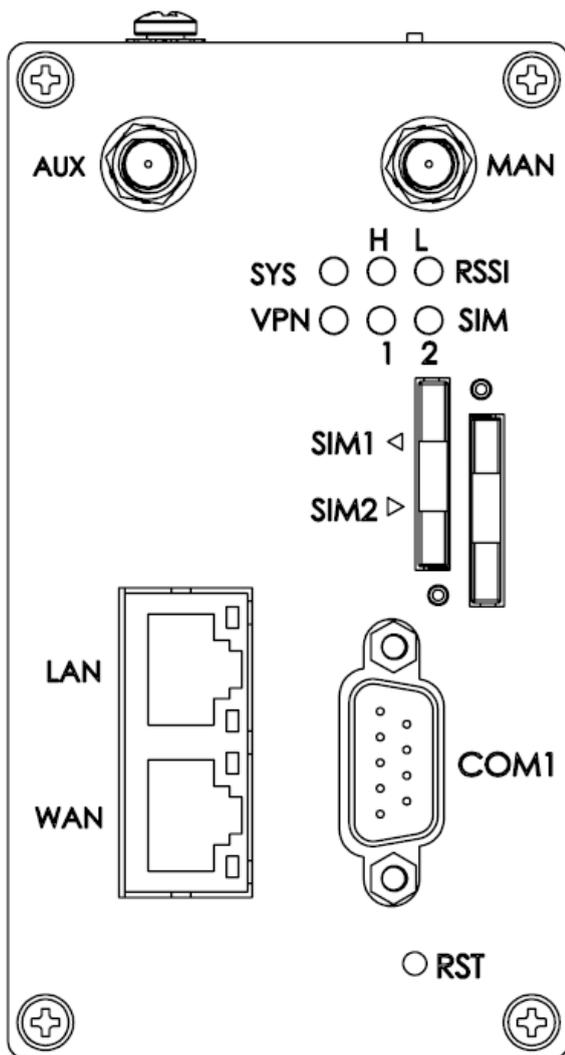
## 1.4 Hardware Panel Layout

This chapter describes the panel and interface layout of hardware. There are four models for industrial 4G LTE router series.

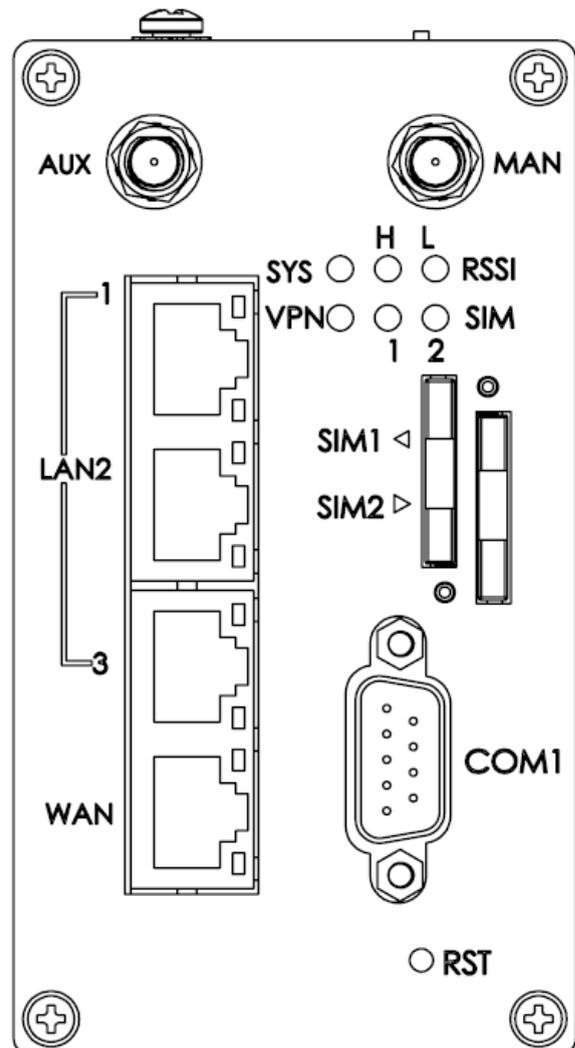
Model Name	Description
M300	Industrial 4G LTE Router (1 x WAN + 1 x LAN)
M301	Industrial 4G LTE Router (1 x WAN + 3 x LAN)
M300G	Industrial 4G LTE Router with GPS (1 x WAN + 1 x LAN + GPS)
M301G	Industrial 4G LTE Router with GPS (1 x WAN + 3 x LAN + GPS)

### [Front Panel View]

Model: **M300**

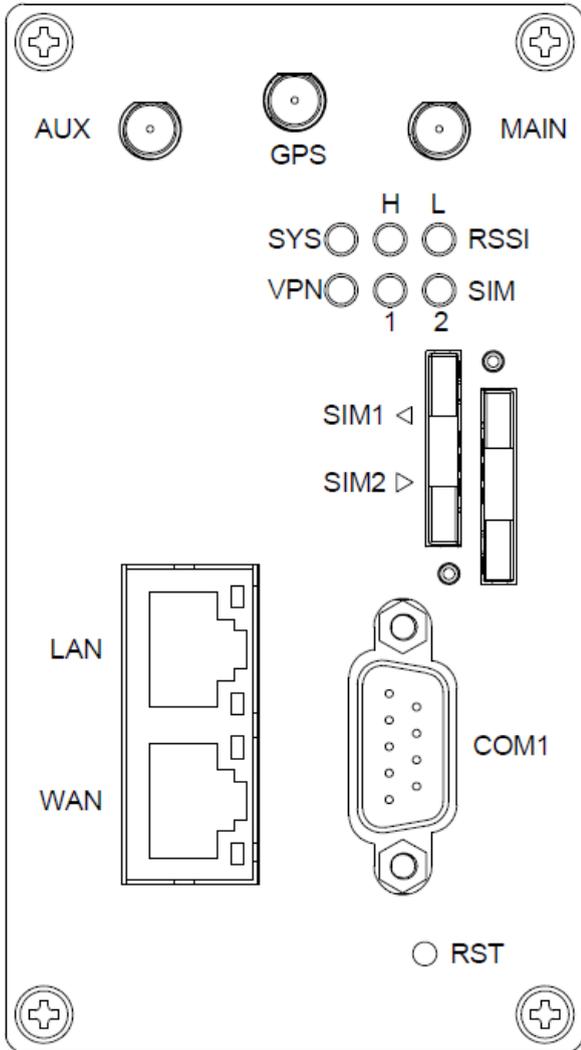


Model: **M301**

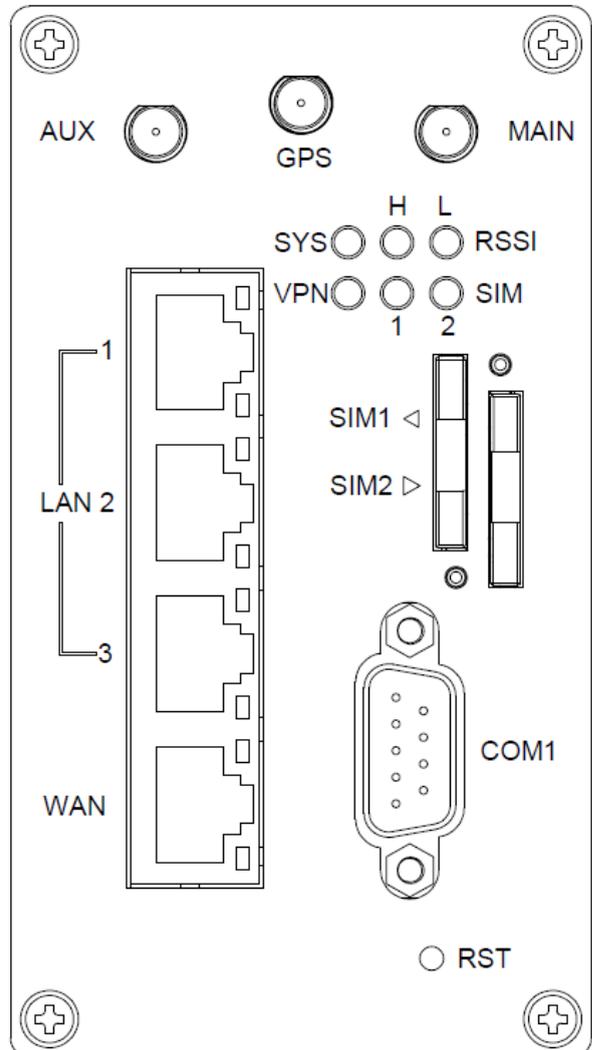


[Front Panel View]

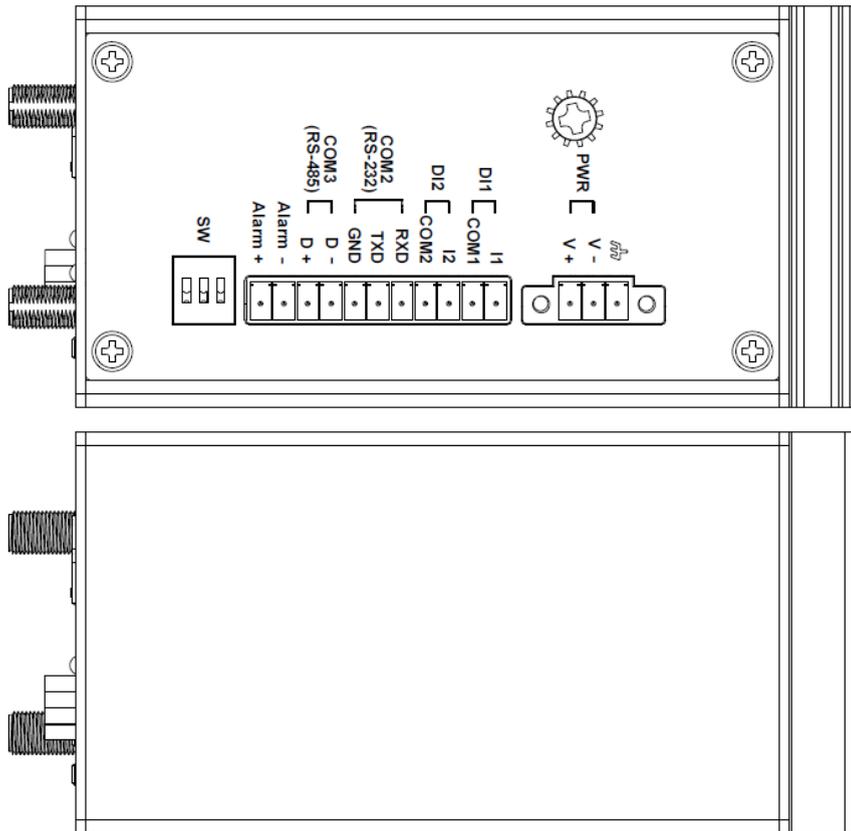
Model: **M300G**



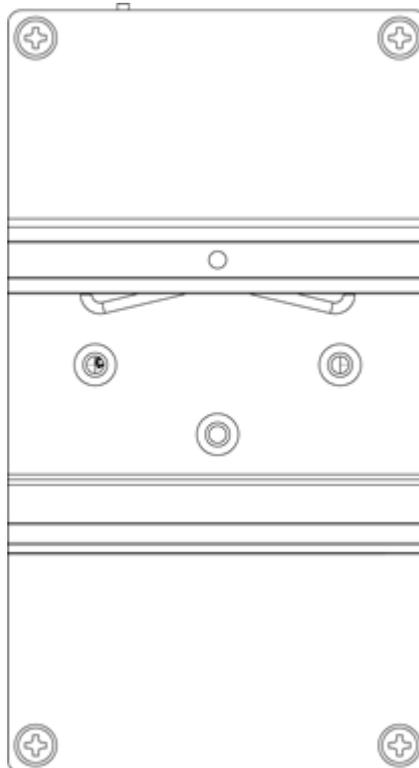
Model: **M301G**



### [Top and Bottom View]



### [Rear View]



[Left Side View]



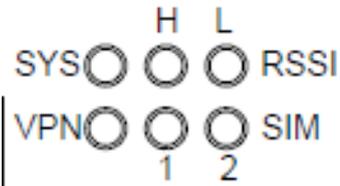
[Right Side View]



## 2 Hardware Installation

This chapter introduces how to install and connect the hardware.

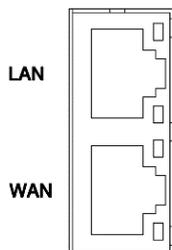
### 2.1 LED Indicators



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

### 2.2 Ethernet Port

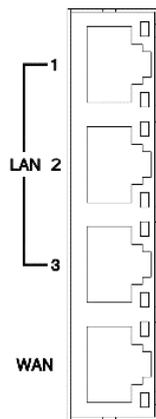
#### (1) 10/100 Mbps Ethernet WAN



The WAN interface is a standard RJ45 connector.

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

## (2) 10/100 Mbps Ethernet LAN1~LAN3



The Ethernet LAN1~3 interfaces are standard RJ45 connectors.

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

Each Ethernet port has two LED indicators.

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

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

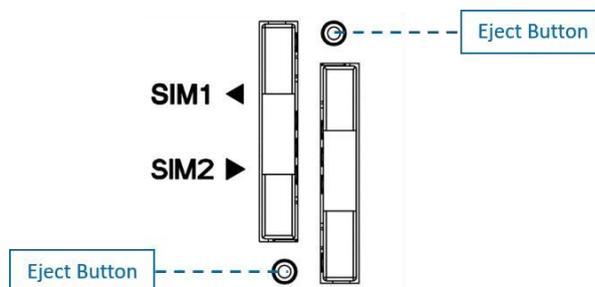
## 2.3 Serial Port COM1 (Console)

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

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

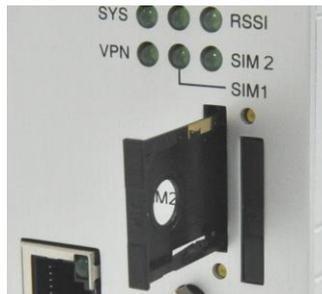
## 2.4 Install the SIM Card

### (1) SIM1/SIM2 Card Drawers and Eject Buttons



### (2) Insert and Remove SIM1/SIM2 Card

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



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



**Note:** Please make sure the direction first. When pulling into the SIM tray without putting the correct direction, the tray will be stuck inside.

## 2.5 Reset Button



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

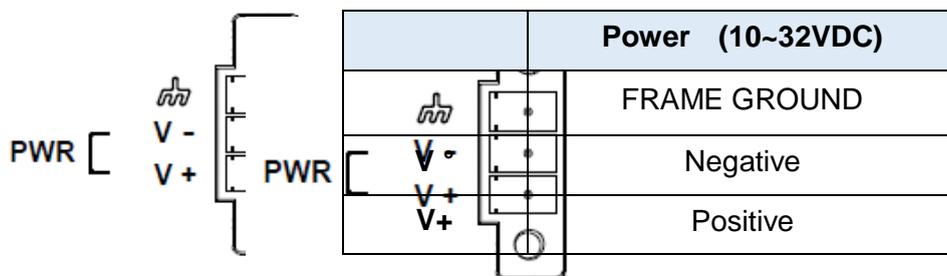
Function	Operation
Reboot	Press the button for 1 second
Restore to factory default setting	Press the button for 10 seconds

## 2.6 External Antenna

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

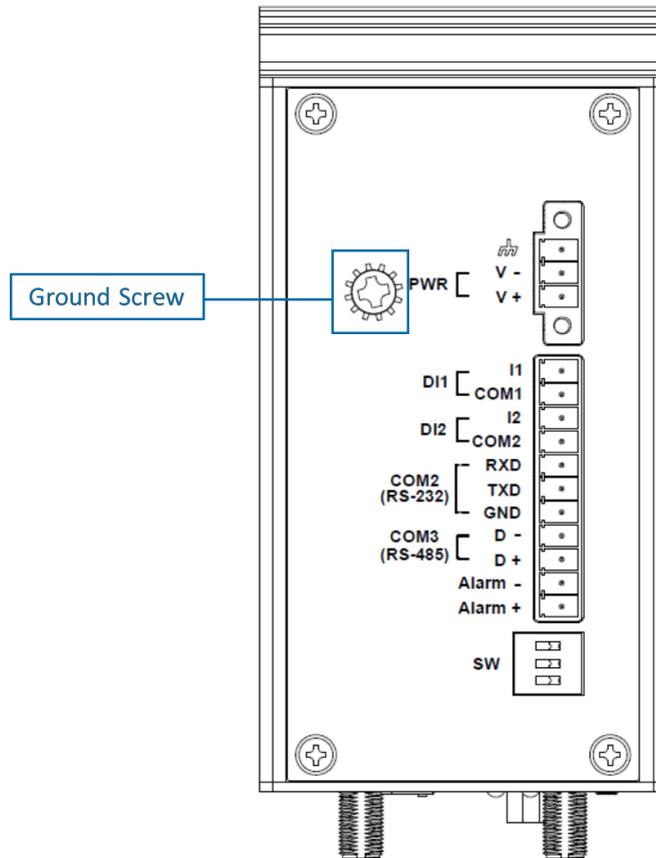
## 2.7 Connecting the Power Supply

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

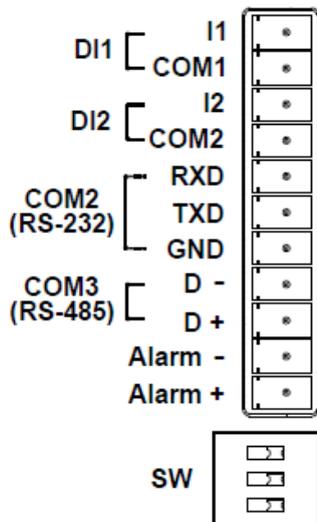


## 2.8 Grounding the Router

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



## 2.9 Pin Assignments



DI1/DI2 / Alarm Contacts / COM2 (RS<sup>o</sup>232) / COM3 (RS<sup>o</sup>485)

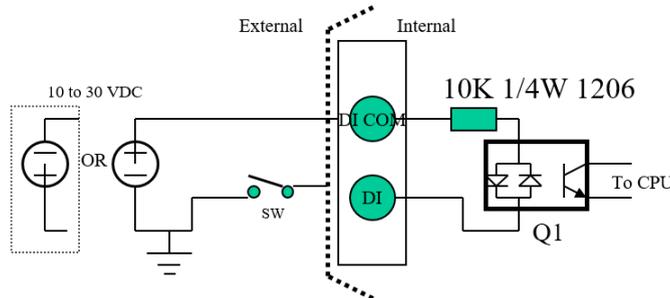
## 2.10 Connecting I/O Ports

### (1) Digital Input DI1 & DI2

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

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

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



#### Wet Contact

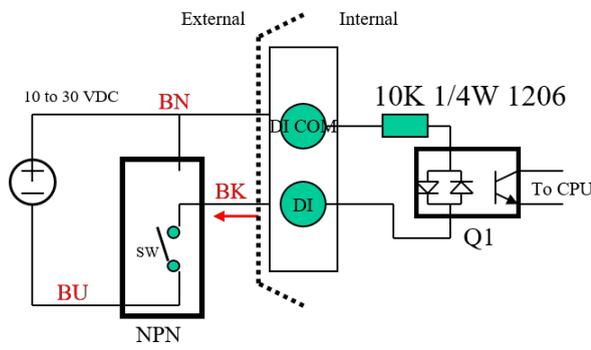
- Logic Level 1 : 10 to 30 VDC (Q1 On)
- Logic Level 0 : 0 to 3 VDC (Q1 Off)

#### Digital Input

- Wet Contact (Level from DI to DI COM)
  - Logic Level 1 : 10 to 30 VDC (Q1 on)
  - Logic Level 0 : 0 to 3 VDC (Q1 off)
- Wet Contact (Alarm trigger\*):
  - Alarm ON\* : Q1 On (SW Close)
  - Alarm Off\* : Q1 off (SW Open)

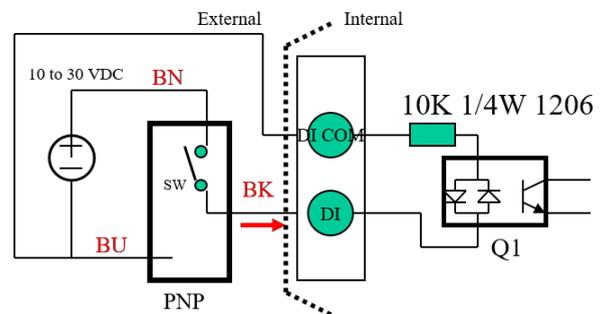
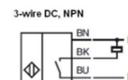
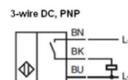
\* Refer to the Alarm function on web management

\* Q1 is bi-directional part



#### Wet Contact

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



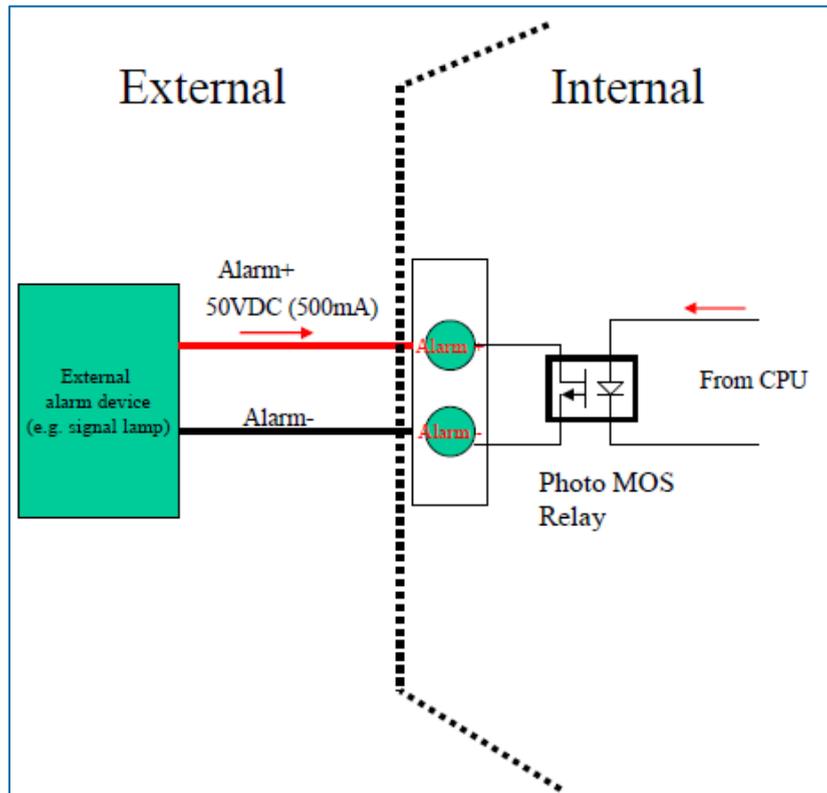
#### Wet Contact

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

### (2) Digital Output – Alarm Contacts

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

Pin	Description
Alarm °	Alarm negative signal output
Alarm +	Alarm positive signal output



## 2.11 Serial Port COM2 (RS<sup>232</sup>)

The serial port COM2 is a RS<sup>232</sup> interface.

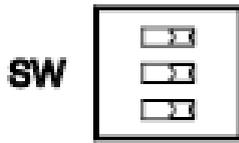
Pin	Description
<b>RXD</b>	COM2 Serial Port, RXD Signal (INPUT)
<b>TXD</b>	COM2 Serial Port, TXD Signal (OUTPUT)
<b>GND</b>	COM2 Serial Port, Signal Ground

## 2.12 Serial Port COM3 (RS<sup>485</sup>)

The serial port COM3 is a RS<sup>485</sup> interface.

Pin	Description
<b>D<sup>°</sup></b>	COM3 Serial Port, Data <sup>°</sup> (B) wire
<b>D<sup>+</sup></b>	COM3 Serial Port, Data <sup>+</sup> (A) wire

## 2.13 DIP Switch



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



DIP SWITCH

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

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

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

## 3 Configuration via Web Browser

### Access the Web Interface

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

After properly connecting the hardware of Mobile 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 Mobile Router are 192.168.1.1 and 255.255.255.0. Because the mobile router acts as DHCP server in your network, the mobile router will automatically assign IP address for PC or NB in the network.

### Control Panel > Selecting Language

You can choose the languages, including English and Taiwan.



Language English ▾

### Logging in the Router

In this section, please fill in the default User Name **root** and the default Password **2wsx#EDC** and then click Login. For the system security, suggest changing them after configuration. After clicking, the interface shows Login ok.

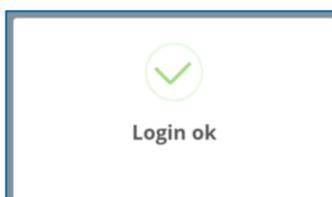


Login

User Name root

Password \*\*\*\*\*

Login



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

## 4 Status

When you enter the web browser in the beginning, the interface displays the status of router to make you know about Cellular Attribute, Dual SIM information, the current connectivity of Ethernet WAN and Ethernet LAN.

The screenshot shows the 'Mobile Router' web interface. The top navigation bar includes 'System Uptime: 5:26:50' and 'WAN Priority: ETH Only'. The left sidebar has a 'Status' button highlighted. The main content area is divided into three sections:

- Status:** A table showing cellular attributes for Current SIM and Backup SIM.
 

Attr.	Current SIM	Backup SIM
SIM Card	SIM1	SIM2
Modem Status	Ready	Not Inserted
Operator	TW Mobile	
Modem Access	FDD LTE	
IMSI	466977101068370	
Phone Number		
Band	LTE BAND 3	
Channel ID	1250	0
IPv4 Address		
IPv4 Mask		
- Ethernet WAN:** A table showing WAN interface attributes.
 

Attr.	Value
IPv4 Address	
IPv4 Mask	
- Ethernet LAN:** A table showing LAN interface attributes.
 

Attr.	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	

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

Ethernet WAN	
Attr.	Value
IPv4 Address	
IPv4 Mask	

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

Ethernet LAN	
Attr.	Value
IPv4 Address	192.168.1.1
IPv4 Mask	255.255.255.0
IPv6 Address	

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

## 4.1 Status > GPS

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

The screenshot shows the 'Mobile Router' web interface. At the top, the status bar includes 'Chunghwa Telecom', 'System Uptime: 06:49', 'WAN Priority: Auto', and a location field displaying 'Location: (24.77, 121.01)'. Below the status bar, there are navigation tabs for 'Status' and 'System'. The 'Status' tab is active, showing a table with columns for 'Attr.', 'Current SIM', and 'Backup SIM'. The 'Current SIM' section shows 'SIM1' as 'Ready' and 'Chunghwa Telecom' with 'FDD LTE' and '466924290355496'. The 'Backup SIM' section shows 'SIM2' as 'Not Inserted'. Below the SIM information, there is a table for 'LTE BAND 7' with values '3050', '10.162.241.68', and '255.255.255.255'. On the left side, a map displays the current location with a red pin and the address 'No. 36, Gongye East 4th Road, East District'. The map shows surrounding roads like 'Park Avenue 2nd Road', 'Gongye East 10th Road', 'Gongye East 9th Road', and 'Yuanqu 3rd Road'. At the bottom right, there is a small 'Ethernet LAN' status table showing 'IPv4 Address' as '192.168.1.1'.

## 5 Configuration > System

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



System	
Item	Description
<b>Time and Date</b>	Configure the time and date of router and NTP server.
<b>COM Ports</b>	Configure the COM Ports.
<b>Logging</b>	Configure the Logging.
<b>Alarm</b>	Configure the Alarm.
<b>Ethernet Ports</b>	Configure the Ethernet Ports.
<b>Modbus</b>	Configure the Modbus.

### 5.1 System > Time and Date

This section allows you to set up the time and date of router and NTP server.

There are two modes, including **Get from Time Server** and **Manual**.

The default mode is Get from Time Server.

#### I. Get from Time Server

Set up the time servers of IPv4 and IPv6.

Select your local time zone.

Click Apply to keep your configuration settings.

**Time And Date**

Current Time Jan 12, 2017 8:01:58 AM

### Time and Date Setup

Mode  Manual  Get from Time Server

IPv4 Server #1

IPv4 Server #2

IPv4 Server #3

IPv6 Server #1

IPv6 Server #2

IPv6 Server #3

### Time Zone Setup

Time Zone

**Apply**

## II. Manual

Set up the information of time and date, including year, month, date, and hour, minute, and second.

Set up your local time zone.

Click Apply to submit your configuration changes.

**Time And Date**

Current Time Jan 12, 2017 8:02:53 AM

### Time and Date Setup

Mode  Manual  Get from Time Server

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

### Time Zone Setup

Time Zone

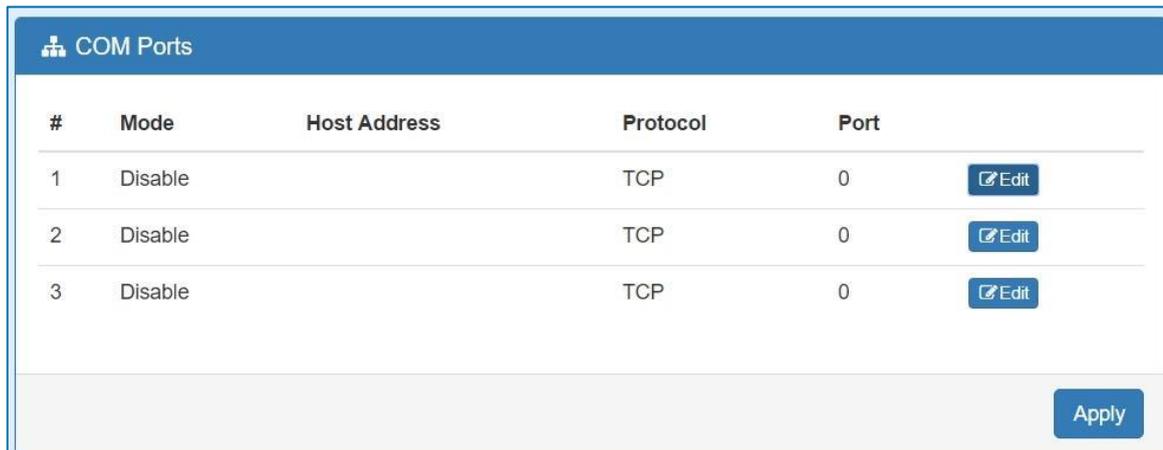
**Apply**

## 5.2 System > COM Ports

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

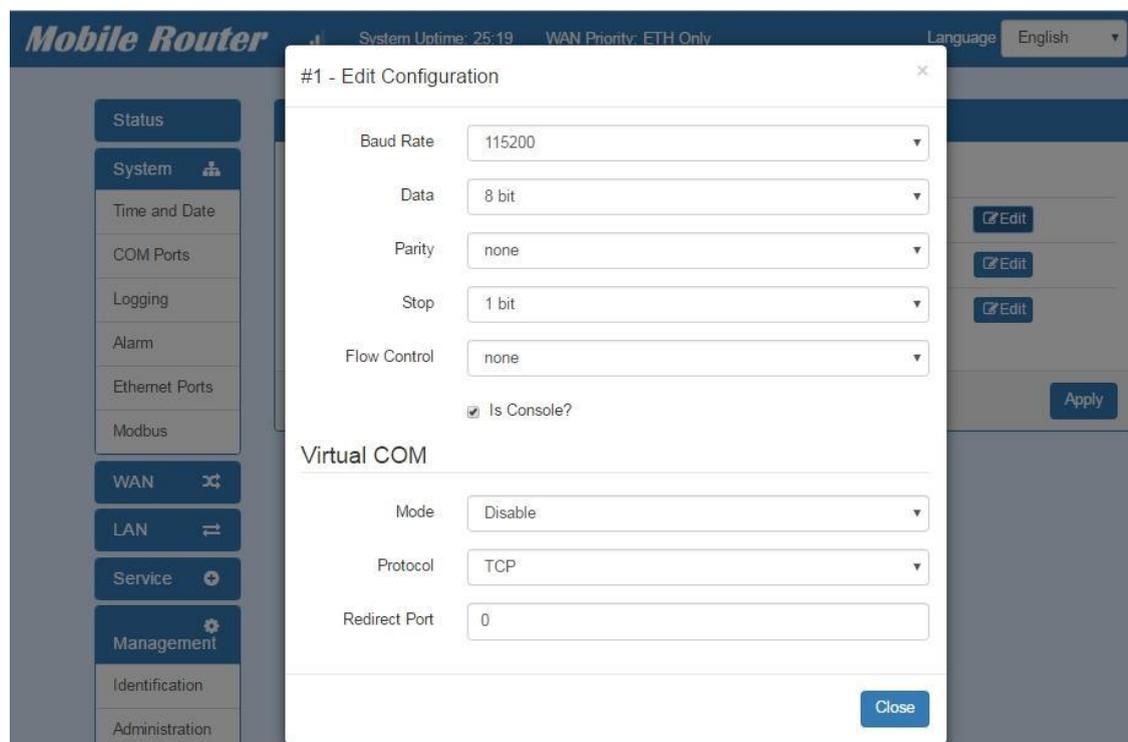
**Note:** The COM 1 and COM 2 are RS232 interface, and the COM 3 is RS485 interface.

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



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

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



**#1 - Edit Configuration**

Baud Rate: 115200

Data: 8 bit

Parity: none

Stop: 1 bit

Flow Control: none

Is Console?

**Virtual COM**

Mode: Disable

Protocol: TCP

Redirect Port: 0

Close

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

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

#1 - Edit Configuration

Baud Rate: 115200

Data: 8 bit

Parity: none

Stop: 1 bit

Flow Control: none

Is Console?

Virtual COM

Mode: Disable

Protocol: TCP

Redirect Port: 0

Close

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

#	Mode	Host Address	Protocol	Port	
1	Server		TCP	6000	<a href="#">Edit</a>
2	Disable		TCP	0	<a href="#">Edit</a>
3	Disable		TCP	0	<a href="#">Edit</a>

Apply

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

### 5.3 System > Logging

This section allows Mobile Router to record the data and display the status of data.

The screenshot displays the 'Logging' configuration interface. On the left is a navigation menu with options: Status, System, Time and Date, COM Ports, Logging, Alarm, Ethernet Ports, Modbus, WAN, LAN, Service, and Management. The main content area is titled 'Logging' and includes the following settings:

- Mode:  Disable  Enable
- Remote Log:  Disable  Enable
- Log Server Address:

An 'Apply' button is located at the bottom right of the configuration section. Below this is the 'Log' section, which features a 'filter' input field and a table of log entries:

#	Date	Group	Module	Message
1	2017-05-31 05:06:48	WAN	DHCP	DHCP client timeout.

'Clear' and 'Refresh' buttons are positioned at the bottom right of the log table.

### 5.3.1 Logging > Logging

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

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



### 5.3.2 Logging > Log

This section displays all data status.

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



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

## 5.4 System > Alarm

This section allows you to configure the alarm.

**Alarm**

Mode  Disable  Enable

Alarm input  SMS  DI 1  DI 2  VPN disconnect  WAN disconnect

Alarm output  SMS  DO  **SNMP trap**

DO behavior  Always  Pulse

Groups

SMS

Group

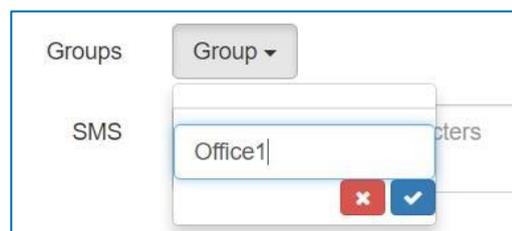
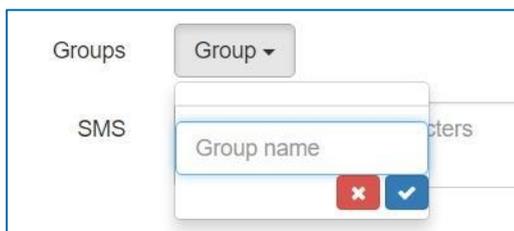
Name	SUN	MON	TUE	WED	THU	FRI	SAT

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

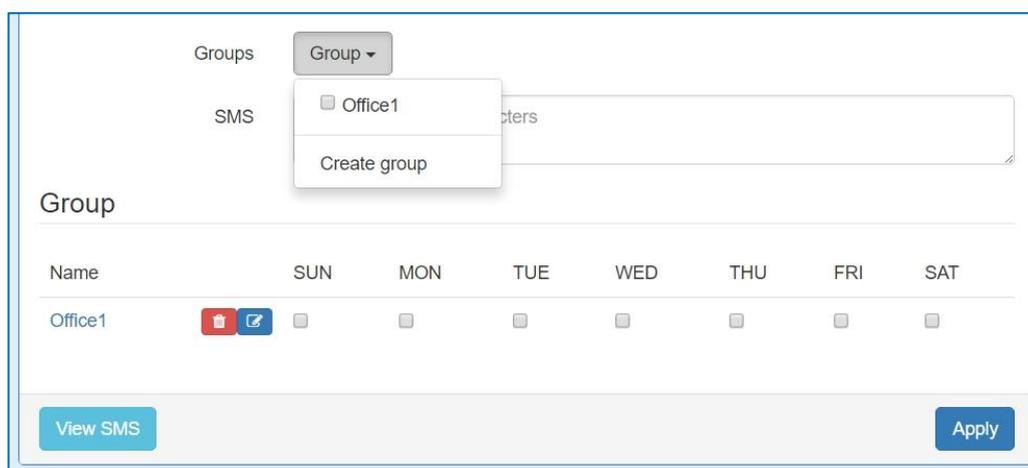
System > Alarm	
Item	Description
<b>Mode</b>	Turn on/off the Alarm configuration. Select Disable or Enable. The default is Enable.
<b>Alarm Input</b>	Select from SMS, DI 1, DI 2, VPN disconnect and WAN disconnect as input to trigger alarm. <input type="checkbox"/> <b>SMS:</b> It means team members on selected week day can send SMS to the phone number of using SIM card to trigger alarm. <input type="checkbox"/> <b>DI 1/2:</b> IO high to trigger alarm. <input type="checkbox"/> <b>VPN disconnect:</b> All tunnels get disconnected then trigger alarm. <input type="checkbox"/> <b>WAN disconnect:</b> All WAN connections get disconnected then trigger alarm.
<b>Alarm Output</b>	Select from SMS, DO and SNMP trap as alarm output.
<b>DO behavior</b>	<input type="checkbox"/> <b>Always:</b> Pull DO high. <input type="checkbox"/> <b>Pulse:</b> High and Low continuously.
<b>Groups</b>	Create your groups and edit your information of groups.
<b>SMS</b>	Write your messages and the messages limit 150 English characters.
<b>View SMS</b>	Click <a href="#">View SMS</a> to show the messages.
<b>Apply</b>	Click <a href="#">Apply</a> to submit your settings.

### (1) How to create your group

Name a group

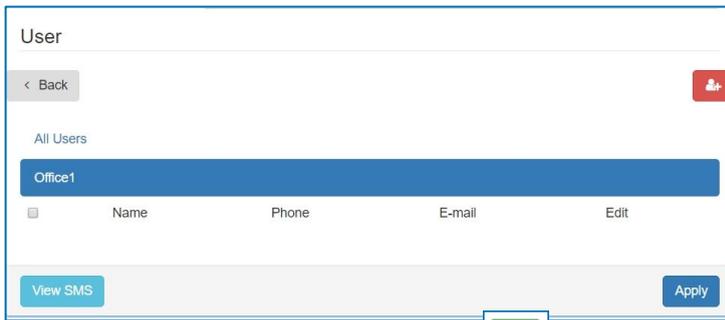


Show your group name from the list of group.



## (2) How to edit your group

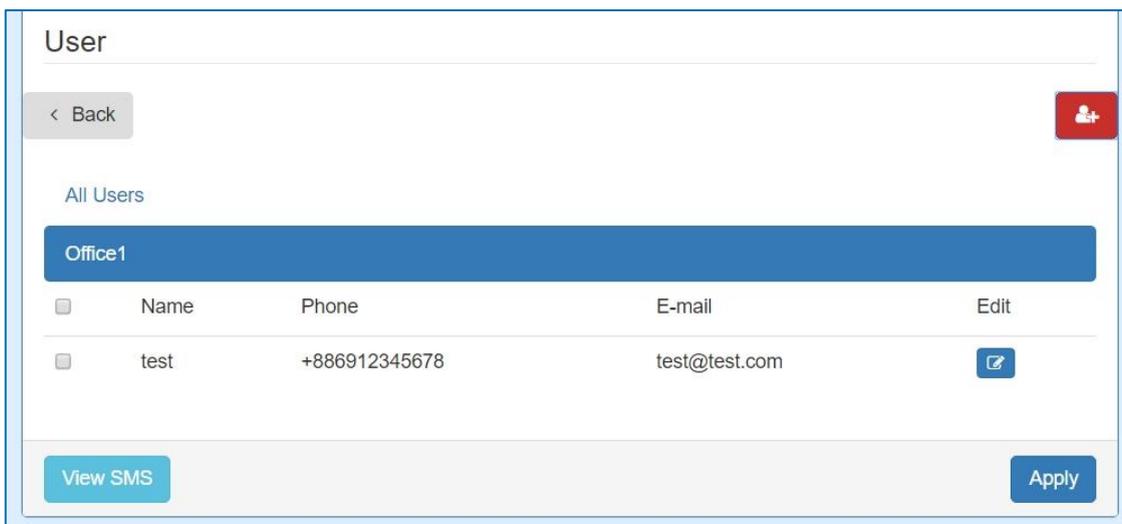
☐ Select your group and click  to edit your group information, including Name, Phone and E-mail.



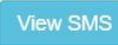
☐ After filling in your information, click  to submit your settings.



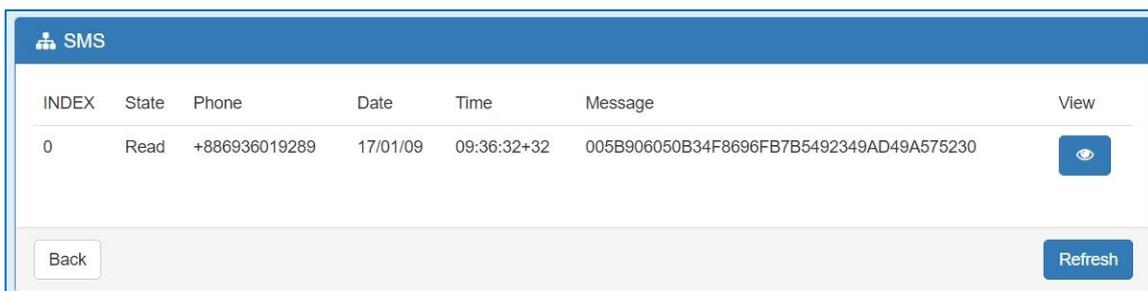
☐ After submitting your setting, the interface shows the information that you edited.

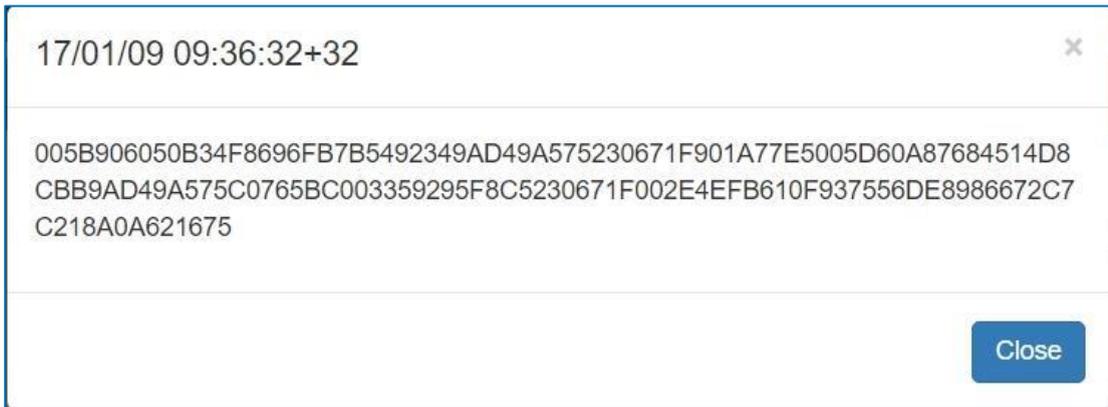


## (3) How to View SMS

☐ Click  to view the information, including the state, phone and date and time.

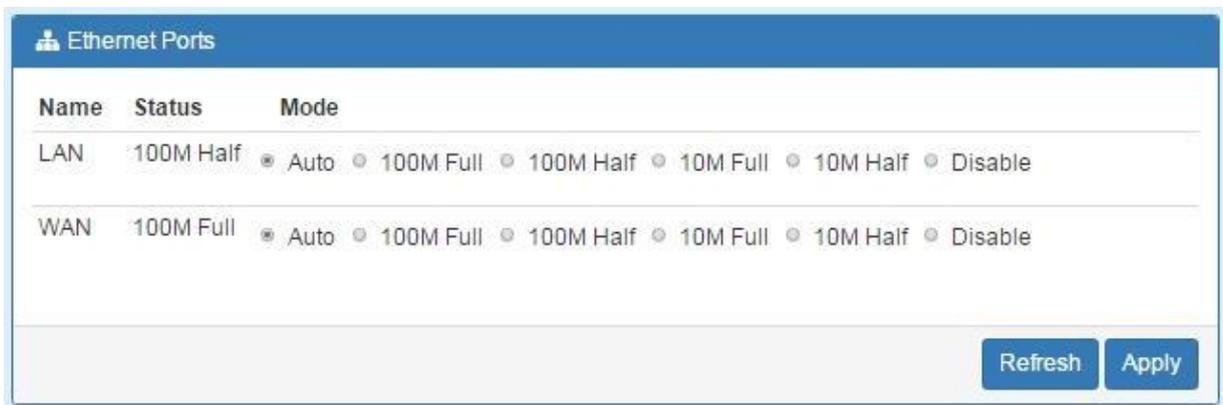
☐ Click  to review your all messages.





## 5.5 System > Ethernet Ports

This section allows you to configure the Ethernet Ports.



System > Ethernet Ports	
Item	Description
<b>Name</b>	Show the name of LAN and WAN.
<b>Status</b>	Show the connectivity status of LAN and WAN.
<b>Mode</b>	Select from Auto, 100M Full, 100M Half, 10M Full, 10M Half and Disable.

## 5.6 System > Modbus

This section allows you to configure the Modbus.

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

🏠
Modbus

Mode    Disable    Enable

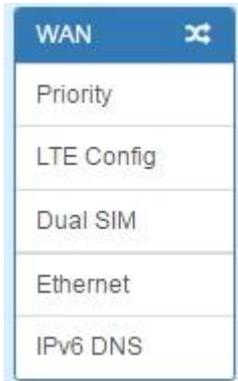
Port

Apply

<b>System &gt; Modbus</b>	
<b>Item</b>	<b>Description</b>
<b>Mode</b>	Select from Disable or Enable.
<b>Port</b>	The listening port of Modbus TCP.

## 6 Configuration > WAN

This section allows you to configure WAN, including Priority, LTE Config, Dual SIM, Ethernet and DNS.



### 6.1 WAN > Priority

You can set up the priority of WAN.



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

### 6.2 WAN > LTE Config

You can set up the LTE Configuration, including Auto, 4G Only or 3G Only.



System > LTE Config	
Item	Description
Auto	Automatically connect the possible band.
4G Only	Connect to 4G network only.
3G Only	Connect to 3G network only.

---

### 6.3 WAN > Dual SIM

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

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

☒
Dual SIM

	SIM1	SIM2
Status	Ready	Not Inserted
SIM PIN	<input type="password" value="****"/>	<input type="password"/>
Confirmed SIM PIN	<input type="password" value="****"/>	<input type="password"/>
SIM PUK	<input type="password"/>	<input type="password"/>
Confirmed SIM PUK	<input type="password"/>	<input type="password"/>
APN	<input type="text"/>	<input type="text"/>
Username	<input type="text"/>	<input type="text"/>
Password	<input type="password"/>	<input type="password"/>
Confirm Password	<input type="password"/>	<input type="password"/>
Change SIM PIN	<input type="button" value="Change"/>	<input type="button" value="Change"/>

#### Data Limitation

	SIM1	SIM2
Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Max Data Limitation (MB)	<input type="text" value="0"/>	<input type="text" value="0"/>
Already Used Data (MB)	<input type="text" value="1"/>	<input type="text" value="0"/>
Pay Date	<input type="text" value="31"/>	<input type="text" value="31"/>

#### Connect Policy

Current SIM Card: SIM1

Disable Roaming:  Disable  Enable

Switch to another SIM when roaming is detected:

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

Change SIM PIN

Change

Change

Old PIN

New PIN

PIN  
Remaining  
Number

3

PUK  
Remaining  
Number

10

Apply

WAN > Dual SIM	
Item	Description
<b>Dual SIM</b>	
Status	Display the status of Dual SIM.
SIM PIN	Configure PIN code to unlock SIM PIN.
Confirmed SIM PIN	Confirm PIN code.
SIM PUK	Fill in PUK to unlock SIM Card after typing more than 3 times.
Confirmed SIM PUK	Confirm SIM PUK.
APN	APN can be input by user or the system will search from internal database if APN is blank.
Username	The username can be input by user or the system will search from internal database if the username is blank.
Password	The password can be input by user or the system will search from internal database if the password is blank.
Confirm Password	Fill in your changed password.
Change SIM PIN	Change your old SIM PIN code into new SIM PIN code.
<b>Data Limitation</b>	
Mode	Turn on/off the Data Limitation to disable or enable.
Max Data Limitation (MB)	Configure max throughput.
Already Used Data (MB)	Display current used throughput.
Pay Date	Clean already used data after Pay Date.
<b>Connect Policy</b>	
Current SIM Card	Display which SIM slot is using.
Status of SIM Card Connectivity	<p><input type="checkbox"/> <b>Connect:</b> If there is one SIM slot get connection, the Disconnect button appear. After manually click Disconnect, the system would not automatically get connection until next reboot.</p> <p><input type="checkbox"/> <b>Connect:</b> After manually disconnect, user can only click Connect button to get connection or reboot the device to make it automatically connect.</p>
Disable Roaming	<p><input type="checkbox"/> <b>Disable:</b> SIM gets connection even it roaming state.</p> <p><input type="checkbox"/> <b>Enable:</b> SIM would not get connection when in roaming state.</p>
Switch to another SIM when roaming is detected.	System will switch SIM slot when current SIM is in roaming state and another SIM slot is in READY state.

## 6.4 WAN > Ethernet

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

The screenshot shows the 'WAN Ethernet' configuration page. At the top, there are three radio buttons for 'Work As': 'DHCP Client' (selected), 'PPPoE Client', and 'Static IPv4'. Below this is the 'DNS Server Configuration' section, which contains three rows for 'IPv4 DNS Server #1', '#2', and '#3'. Each row has a dropdown menu currently set to 'From ISP' and an adjacent text input field. An 'Apply' button is located in the bottom right corner.

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

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

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

This screenshot is similar to the previous one, but the dropdown menu for 'IPv4 DNS Server #1' is open, showing three options: 'From ISP' (highlighted in blue), 'User Defined', and 'None'. The other two dropdown menus remain set to 'From ISP'. The 'Apply' button is still visible in the bottom right corner.

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

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

The screenshot shows the 'WAN Ethernet' configuration page. At the top, there are radio buttons for 'Work As': DHCP Client, PPPoE Client (selected), and Static IPv4. Below this is the 'PPPoE Client Configuration' section with two input fields: 'User Name' containing 'test' and 'Password' containing '\*\*\*\*\*'. An 'Apply' button is located at the bottom right.

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

The screenshot shows the 'WAN Ethernet' configuration page with 'Static IPv4' selected. The 'Static IPv4 Configuration' section includes three input fields: 'IP Address' (192.168.2.1), 'IP Mask' (255.255.255.0), and 'Gateway Address' (192.168.2.2). Below this is the 'DNS Server Configuration' section with three empty input fields for 'IPv4 DNS Server #1', 'IPv4 DNS Server #2', and 'IPv4 DNS Server #3'. An 'Apply' button is at the bottom right.

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

## 6.5 WAN > IPv6 DNS

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

The screenshot shows the 'IPv6 DNS' configuration window. Under the 'DNS Server Configuration' section, there are three rows for 'IPv6 DNS Server #1', '#2', and '#3'. Each row has a dropdown menu currently set to 'From ISP' and an adjacent empty text input field. An 'Apply' button is located in the bottom right corner of the configuration area.

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

This screenshot is similar to the previous one, but the dropdown menu for 'IPv6 DNS Server #2' is open, displaying three options: 'From ISP' (which is highlighted in blue), 'User Defined', and 'None'. The other two server entries remain unchanged with 'From ISP' selected. The 'Apply' button is still visible in the bottom right.

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

## 7 Configuration > LAN

This section allows you to configure LAN IPv4 and LAN IPv6.

LAN	⇌
IPv4	
IPv6	

Status	⇌ LAN IPv4
System	IP Address <input type="text" value="192.168.1.1"/>
WAN	IP Mask <input type="text" value="255.255.255.0"/>
LAN	DHCP Server Configuration
IPv4	<input checked="" type="checkbox"/> DHCP Server Configuration
IPv6	IP Address Pool From <input type="text" value="192.168.1.2"/> To <input type="text" value="192.168.1.254"/>
Service	<input type="button" value="Apply"/>
Management	

### 7.1 LAN > IPv4

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

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

LAN > IPv4	
Item	Description
<b>LAN IPv4</b>	<input type="checkbox"/> IP Address:192.168.1.1 <input type="checkbox"/> IP Mask:255.255.255.0 Both of them are default, you can change them according to your local IP Address and IP Mask.
<b>DHCP Server Configuration</b>	<input type="checkbox"/> Turn on/off DHCP Server Configuration. <input type="checkbox"/> Enable to make router can lease IP address to DHCP clients which connect to LAN.
<b>IP Address Pool</b>	<input type="checkbox"/> Define the beginning and the end of the pool of IP addresses which will lease to DHCP clients.

## 7.2 LAN > IPv6

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

☰
LAN IPv6

Type     Delegate Prefix from WAN     Static

Static Address   

---

DHCP Server Configuration

Address Assign     Stateful     Stateless

LAN > IPv6	
Item	Description
<b>LAN IPv6</b>	<ul style="list-style-type: none"> <li><input type="checkbox"/> This section provides two types, including <b>Delegate Prefix from WAN</b> and <b>Static</b>.</li> <li><input type="checkbox"/> <b>Static Address:</b> You need to input the static address when you select the static type.</li> </ul>
<b>Delegate Prefix from WAN</b>	<input type="checkbox"/> Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
<b>Static</b>	<input type="checkbox"/> Select this option to configure a fixed IPv6 address for the mobile router's LAN IPv6 address.
<b>Address Assign Setup</b>	<p>Select how you want to obtain an IPv6 address:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <b>Stateless:</b> The mobile router uses IPv6 stateless auto configuration. RADVD (Router Advertisement Daemon) is enabled to have the mobile router send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 clients.</li> <li><input type="checkbox"/> <b>Stateful:</b> The mobile router uses IPv6 stateful auto configuration. The LAN IPv6 clients can obtain IPv6 addresses through DHCPv6.</li> </ul>

## 8 Configuration > Service

This section allows you to configure OpenVPN, IPSec, Port Forwarding, Dynamic DNS, DMZ, SNMP, IP Filter, MAC Filter and URL Filter.



### 8.1 Service > Configuration OpenVPN

(1) This section allows you to configure the OpenVPN parameters. The default mode is Disable.

The OpenVPN configuration page shows a "Mode" section with radio buttons for "Disable" (selected) and "Enable". Below is a table with 10 rows, each representing a VPN configuration. The columns are: #, Mode, VPN Mode, Device, Protocol, Port, and Edit. All entries are currently set to "Disable", "Client", "TUN", "UDP", and "1701". An "Apply" button is located at the bottom right.

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

(2) Click  to edit OpenVPN Connection.

### Edit Open VPN Connection #1

Mode  Disable  Enable

VPN Mode  Server  Client  Custom

TLS Mode  Disable  Enable

TLS minimal version  none  1.0  1.1  1.2

Cipher

Status

Device  TUN  TAP

Protocol  UDP  TCP

Port

VPN Compression  Disable  Enable

Authentication

#### Client

Client Mode  Roadwarrior

Server Address

Route Client Networks  Off  On

#### NAT

1:1 NAT  Off  On

#### Client - Security

Root CA

Cert

Key

P12

Service > OpenVPN	
Item	Description
<b>Mode</b>	Turn on/off OpenVPN to select Disable or Enable.
<b>VPN Mode</b>	<input type="checkbox"/> Server: Tick to enable OpenVPN server tunnel. <input type="checkbox"/> Client: Tick to enable OpenVPN client tunnel. The default is Client. <input type="checkbox"/> Custom: This option allows user to use the .ovpn configuration file to quickly set up VPN tunnel with third°party server or use the OpenVPN advance options to be compatible with other servers.
<b>TLS Mode</b>	Select from Disable or Enable for data security. The default is Disable.
<b>TLS minimal version</b>	Select from none, 1.0, 1.1 or 1.2. The default is none.
<b>Cipher</b>	The OpenVPN format of data transmission.
<b>Status</b>	Display the status of OpenVPN.
<b>Device</b>	Select from TUN or TAP. The default is TUN.
<b>Protocol</b>	Select from UDP or TCP Client which depends on the application. The default is UDP.
<b>Port</b>	Enter the listening port of remote side OpenVPN server.
<b>VPN Compression</b>	Select Disable or Enable to compress the data stream. The default is Disable.
<b>Authentication</b>	<input type="checkbox"/> Select from two different kinds of authentication ways: Certificate or pkcs#12 Certificate. <input type="checkbox"/> The pkcs#12 option is only available on the VPN client mode.

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

Client

Client Mode  Roadwarrior

Server Address

Route Client Networks  Off  On

NAT

1:1 NAT  Off  On

Client - Security

Root CA

Cert

Key

P12

Service > OpenVPN	
Item	Description
<b>Client</b>	
<b>Client Mode</b>	Only support the Roadwarrior mode.
<b>Server Address</b>	Fill in WAN IP of OpenVPN server.
<b>Route Client Networks</b>	Select from Off or On. This setting needs to match the server side. When enabled, the mobile router will auto apply the properly routing rules.
<b>NAT</b>	
<b>1:1 NAT</b>	<input type="checkbox"/> Tick to enable NAT Traversal for OpenVPN. This item must be enabled when router under NAT environment. <input type="checkbox"/> Select from Off or On. <input type="checkbox"/> When two routers' LAN Subnet are same and create OpenVPN tunnels, this function should be turned on.
<b>Client°Security</b>	
<b>Root CA</b>	The Certificate Authority file of OpenVPN server could be downloaded from OpenVPN server.
<b>Cert</b>	The certification file is for OpenVPN client, which could be downloaded from OpenVPN server.
<b>Key</b>	The private key file is for OpenVPN client, which could be downloaded from OpenVPN server.
<b>P12</b>	The PKCS#12 file is for OpenVPN client, which could be downloaded from OpenVPN server.

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

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

Edit Open VPN Connection #1

Mode  Disable  Enable

VPN Mode  Server  Client  Custom

TLS Mode  Disable  Enable

TLS minimal version  none  1.0  1.1  1.2

Cipher

Status

Device  TUN  TAP

Protocol  UDP  TCP

Port

VPN Compression  Disable  Enable

Authentication

## Server

Client Mode  Roadwarrior

VPN Network

VPN Netmask

## Server - Server Security

Root CA

Cert, Key

## Server - User Security

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

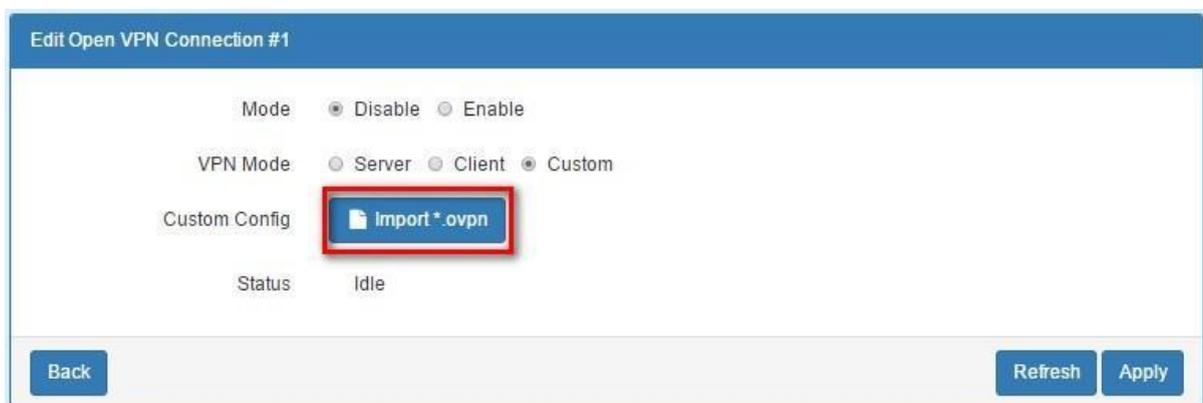
Service > OpenVPN > Server VPN Mode	
Item	Description
<b>Server</b>	
<b>Client Mode</b>	Only support the Roadwarrior mode.
<b>VPN Network</b>	The network ID for OpenVPN virtual network.
<b>VPN Netmask</b>	The netmask for OpenVPN virtual network.
<b>Roadwarrior: Route Client Networks</b>	Select from Off or On. The OpenVPN server will route the client traffic or not. User should fill in the client IP and netmask when this option is enabled.
<b>NAT</b>	
<b>1:1 NAT</b>	<input type="checkbox"/> Tick to enable NAT Traversal for OpenVPN. This item must be enabled when router under NAT environment. <input type="checkbox"/> Select from Off or On. The default is Off. <input type="checkbox"/> When two routers' LAN Subnet are same and create OpenVPN tunnels, this function is turned on.
<b>Server° Server Security</b>	
<b>Root CA</b>	Create Root CA key.
<b>Cert, Key and DH</b>	Create Cert, Key and DH key.
<b>Server° User Security</b>	
<b>User 1 ° User 8</b>	According to your requirement, you can create different kinds of user security key from User 1 to User 8.

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

**Note:**

When clicking the **Import** button, you can import third°party OpenVPN configuration that find out from Internet and save the document into your server or PC. After importing the file, the interface will show   button to click  for displaying the information and to click  for downloading the file.

For third°party OpenVPN configuration, suggest from <http://www.vpngate.net/en/>



**Edit Open VPN Connection #1**

Mode  Disable  Enable

VPN Mode  Server  Client  Custom

Custom Config

Status Idle

Service > OpenVPN > Custom VPN Mode	
Item	Description
<b>Mode</b>	Select from Disable or Enable. The default is Disable.
<b>VPN Mode</b>	Select from custom mode.
<b>Custom Config</b>	Import OpenVPN configuration.
<b>Status</b>	Display the status of OpenVPN.

## 8.2 Service > Configuration IPSec

☐ This section allows you to set up IPSec Tunnel. Click  button to edit IPSec connection.

**IPSec**

Mode  Disable  Enable

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

**Security of Connection #1**

Create Cert Key

□ The interface shows the setting items of Edit IPsec Connection and Security of Connection.

The image shows two side-by-side configuration panels. The left panel, titled "Edit IPsec Connection #1", contains the following settings:

- Mode:  Disable  Enable
- Name:
- IKE section:
  - Protocol:
  - Encryption:
  - Hash:
  - DH Group:
- Encryption section:
  - Protocol:
  - Encryption:
  - Hash:
  - DH Group:
- Local section:
  - Host:
  - Subnet:
- Remote section:
  - Host:
  - Subnet:
  - Auth Type:
  - Auth Scret:
- Save button at the bottom right.

The right panel, titled "Security of Connection #1", contains the following settings:

- Buttons for "Create", "Cert", and "Key".
- Buttons for "Root CA", "Server", "User 0", "User 1", "User 2", and "User 3".

□ Set up IKE.

The image shows a close-up of the IKE configuration section from the previous screenshot. It includes the following settings:

- Protocol:
- Encryption:
- Hash:
- DH Group:

□ Set up Encryption.

### Encryption

Protocol	esp
Encryption	aes128
Hash	sha1
DH Group	modp1536

□ Set up Local.

### Local

Host	0.0.0.0
Subnet	0.0.0.0/0

□ Set up Remote. After you configure all setting, click Save.

🔗 You need to create the IPsec Security Keys by clicking Create button, including Root CA, Server and User Keys/Certs for User 0 to User 3. E.g. To create server file, click the Server button. To create user 0 file, click the User 0 button.

🔗 For the IPsec connection, the client should setup properly Root CA, server cert, user key and user cert files. The files could be downloaded by clicking Download button after the file generated.

### Security of Connection #1

Create	Cert	Key
Root CA	 	
Server		
User 0		
User 1		
User 2		
User 3		

Service > IPSec	
Item	Description
<b>Mode</b>	Select from Disable or Enable. The default is Disable.
<b>Name</b>	Fill in the name of IPSec Tunnel.
<b>IKE</b>	
<b>Protocol</b>	Select from ikev1 or ikev2.
<b>Encryption</b>	Select from aes128 (default), aes192, aes256 or 3des.
<b>Hash</b>	Select from sha1 (default), md5 or sha256.
<b>DH Group</b>	Select from modp1536 (default)、 modp768、 modp1024、 modp2048、 modp3072、 modp4096、 modp6144 or modp8192.
<b>Encryption</b>	
<b>Protocol</b>	Select from esp or aes128.
<b>Encryption</b>	Select from aes128 (default), aes192, aes256 or 3des.
<b>Hash</b>	Select from sha1 (default), md5 or sha256.
<b>DH Group</b>	Select from modp1536 (default), modp768, modp1024, modp2048, modp3072, modp4096, modp6144 or modp8192.
<b>Local</b>	
<b>Host</b>	Fill in the WAN IP of mobile router.
<b>Subnet</b>	Fill in the subnet for the LAN of mobile router.
<b>Remote</b>	
<b>Host</b>	Fill in the granted remote IP. If no limitation, keep blank.
<b>Subnet</b>	Fill in the granted remote subnet. If no limitation, keep blank.
<b>Auth Type</b>	Select from psk or rsa.
<b>Auth Scret</b>	The password is for psk authentication type.

### 8.3 Service > Configuration Port Forwarding

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

**Port Forwarding**

Mode  Disable  Enable

#	Mode	Description	Protocol	
1	Disable	ssh	TCP	<a href="#">Edit</a>
2	Disable		TCP	<a href="#">Edit</a>
3	Disable		TCP	<a href="#">Edit</a>
4	Disable		TCP	<a href="#">Edit</a>
5	Disable		TCP	<a href="#">Edit</a>
6	Disable		TCP	<a href="#">Edit</a>
7	Disable		TCP	<a href="#">Edit</a>
8	Disable		TCP	<a href="#">Edit</a>
9	Disable		TCP	<a href="#">Edit</a>
10	Disable		TCP	<a href="#">Edit</a>
11	Disable		TCP	<a href="#">Edit</a>
12	Disable		TCP	<a href="#">Edit</a>
13	Disable		TCP	<a href="#">Edit</a>
14	Disable		TCP	<a href="#">Edit</a>
15	Disable		TCP	<a href="#">Edit</a>
16	Disable		TCP	<a href="#">Edit</a>

[Apply](#)

**Edit Configuration #1** ✕

Mode  Disable  Enable

Description

Protocol  TCP  UDP

Source Port Begin

Source Port End

Destination IP

Destination Port

[Close](#)

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

## 8.4 Service > Dynamic DNS

This section allows you to set up Dynamic DNS.

+
Dynamic DNS

Mode  Disable  Enable

Service Provider

Host Name

Token ID

Update Period Time (Sec)

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

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

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

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

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

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

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

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

## 8.5 Service > DMZ

This section allows you to set the DMZ configuration.

**DMZ**

Mode  Disable  Enable

Host IP Address

**Apply**

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

## 8.6 Service > SNMP

### 8.6.1 SNMP configuration

This section allows you to set the SNMP configuration.

**SNMP**

Mode  Disable  Enable

Community

# 1

Mode  Disable  Enable

Name

Access  Read-Only  Read-Write

# 2

Mode  Disable  Enable

Name

Access  Read-Only  Read-Write

# 3

Mode  Disable  Enable

Name

Access  Read-Only  Read-Write

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.

### 8.6.2 SNMP v3 User configuration

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

#### SNMP v3 User Configuration

# 1

Mode  Disable  Enable

Name

Auth Mode  Authentication  Privacy

Authentication Password

Authentication Protocol  MD5  SHA

Privacy Password

Privacy Protocol  DES  AES

Access  Read-Only  Read-Write

# 2

Mode  Disable  Enable

Name

Auth Mode  Authentication  Privacy

Authentication Password

Authentication Protocol  MD5  SHA

Privacy Password

Privacy Protocol  DES  AES

Access  Read-Only  Read-Write

# 3

Mode  Disable  Enable

Name

Auth Mode  Authentication  Privacy

Authentication Password

Authentication Protocol  MD5  SHA

Privacy Password

Privacy Protocol  DES  AES

Access  Read-Only  Read-Write

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

### 8.6.3 SNMP trap configuration

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

### SNMP trap configuration

# 1

Mode  Disable  Enable

Community Name

Destination

# 2

Mode  Disable  Enable

Community Name

Destination

[Apply](#)

### Alarm

Mode  Disable  Enable

Alarm input  SMS  DI 1  DI 2  VPN disconnect  WAN disconnect

Alarm output  SMS  DO  **SNMP trap**

DO behavior  Always  Pulse

Groups

SMS

Group

Name	SUN	MON	TUE	WED	THU	FRI	SAT

[View SMS](#) [Apply](#)

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

## 8.7 Service > IP Filter

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

**IP Filter**

Mode  Disable  Enable

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

**Apply**

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

The screenshot shows a configuration window titled "Edit IP Filter Black List Entry #1". It contains several fields and radio buttons:

- Mode:** Radio buttons for "Disable" (selected) and "Enable".
- Protocol:** Radio buttons for "All" (selected), "ICMP", "TCP", and "UDP".
- Source IP:** Text input field containing "0.0.0.0".
- Source Port:** Text input field containing "0".
- Destination IP:** Text input field containing "0.0.0.0".
- Destination Port:** Text input field containing "0".
- Save:** A blue button at the bottom right.

Service > IP Filter	
Item	Description
<b>Mode</b>	Select from Disable or Enable. The default is Disable.
<b>Protocol</b>	Select from All, ICMP, TCP or UDP.
<b>Source IP</b>	Fill in your source IP address.
<b>Source Port</b>	Fill in your source port.
<b>Destination IP</b>	Fill in your destination IP address.
<b>Destination Port</b>	Fill in your destination port.

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

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

Service > Edit IP Filter > Source IP			
IP Format	Single IP	IP with Mask	Ranged IP
<b>IPv4</b>	192.168.0.123	192.168.1.0/24 192.168.1.0/255.255.255.	192.168.1.1°192.168.1.123
<b>IPv6</b>	2607:f0d0:1002:51::4	2607:f0d0:1002:51::0/64	2607:f0d0:1002:51::4° 2607:f0d0:1002:51::aaaa

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

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

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

### Edit IP Filter #1

White List Setting

Mode  Enable  Disable

Protocol

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

Source Port   
Ex.  
1234  
1234:5678

Destination IP

Destination Port

---

## 8.8 Service > MAC Filter

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

**MAC Filter**

Mode  Disable  Enable

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

**Apply**

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

Mode  Disable  Enable

MAC Address

**Save**

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

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

## 8.9 Service > URL Filter

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

+ URL Filter

Mode  Disable  Enable

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

Apply

Edit MAC Filter Black List Entry #1

Mode  Disable  Enable

Filter  Key  Full

Key/Full

Save

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

## 9 Management

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



### 9.1 Identification

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



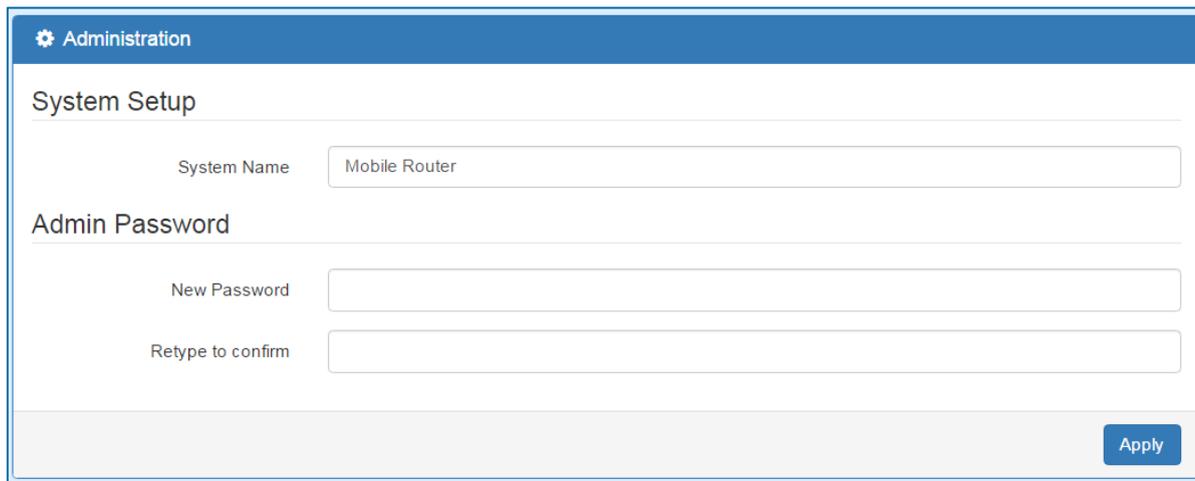
Attr.	Value
Host Name	Mobile Router
MAC Address	CE:CD:16:4B:D7:1D
Software Version	V1.50
Software MCSV	012C000015029A6F
Hardware MCSV	012C000000000000
Modem Firmware Version	EC25EFAR02A04M4G
System Uptime	02:34

Management > Identification	
Item	Description
<b>Host Name</b>	Show the host name of mobile router.
<b>MAC Address</b>	Show the MAC address.
<b>Software Version</b>	Show the current software version.
<b>Software MCSV</b>	Show the current software MCSV.
<b>Hardware MCSV</b>	Show the current hardware MCSV.
<b>Modem Firmware Version</b>	Show the current firmware version.
<b>System Uptime</b>	Show the current system uptime.

---

## 9.2 Administration

This section allows you to set up the name of system and change your new password.



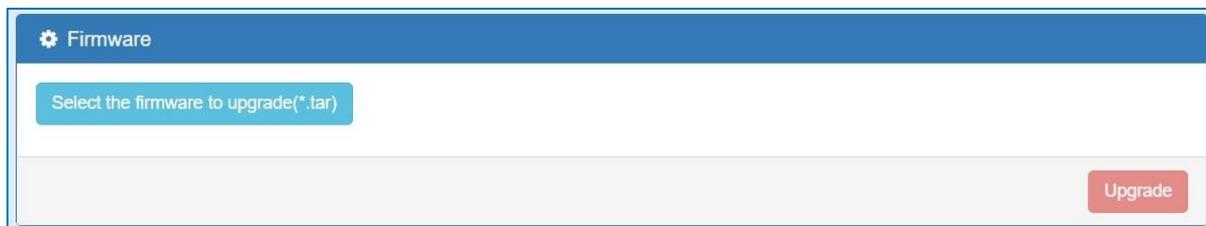
The screenshot shows the 'Administration' section with a 'System Setup' sub-section. It contains two input fields: 'System Name' with the value 'Mobile Router' and 'Admin Password' with two sub-fields for 'New Password' and 'Retype to confirm'. An 'Apply' button is located at the bottom right.

---

## 9.3 Firmware

This section provides you to upgrade the firmware of router.

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



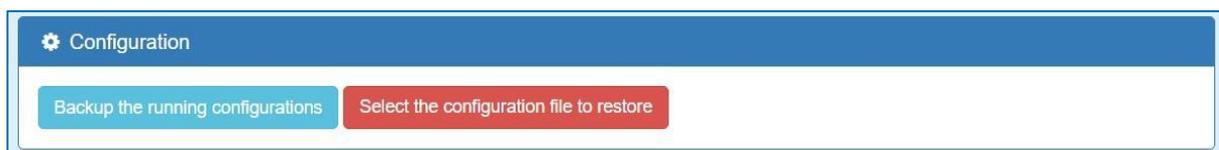
The screenshot shows the 'Firmware' section with a button labeled 'Select the firmware to upgrade(\*.tar)' and an 'Upgrade' button at the bottom right.

---

## 9.4 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.

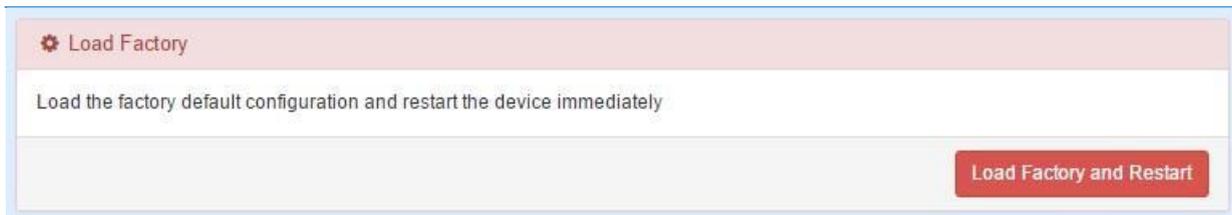


The screenshot shows the 'Configuration' section with two buttons: 'Backup the running configurations' and 'Select the configuration file to restore'.

---

## 9.5 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.



---

## 9.6 Restart

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

