



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

1	Introduction.....	1
1.1	Features	1
1.2	Specifications	2
1.3	Mechanical Dimensions	2
1.4	Hardware Panel Layout.....	3
2	Hardware Installation.....	7
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°232)	13
2.12	Serial Port COM3 (RS°485)	13
2.13	DIP Switch.....	14
3	Configuration via Web Browser.....	15
4	Status	16
4.1	Status > GPS.....	17
5	Configuration > System	18
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
6	Configuration > WAN.....	29
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
7	Configuration > LAN.....	38
7.1	LAN > IPv4	38
7.2	LAN > IPv6.....	39

8	Configuration > Service	41
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
9	Management.....	63
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

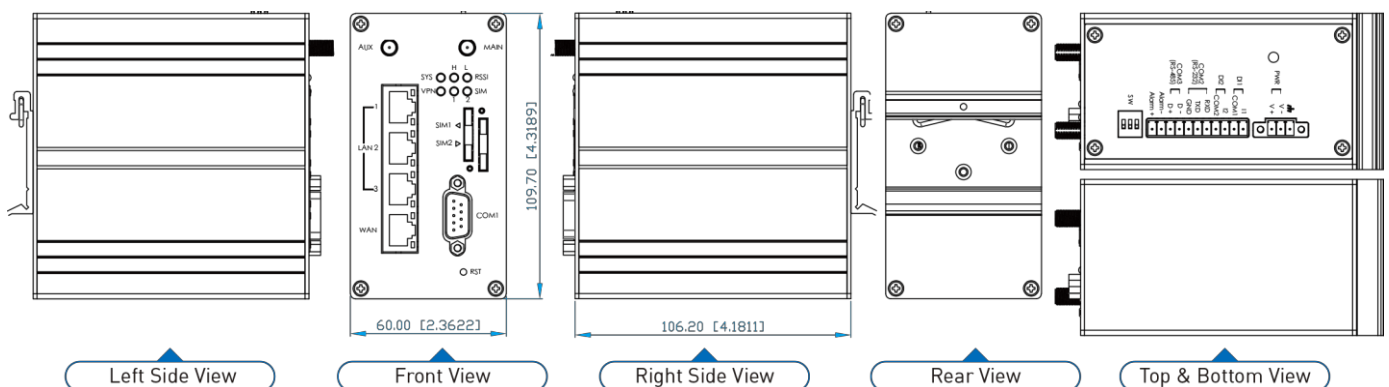
Environment

- 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



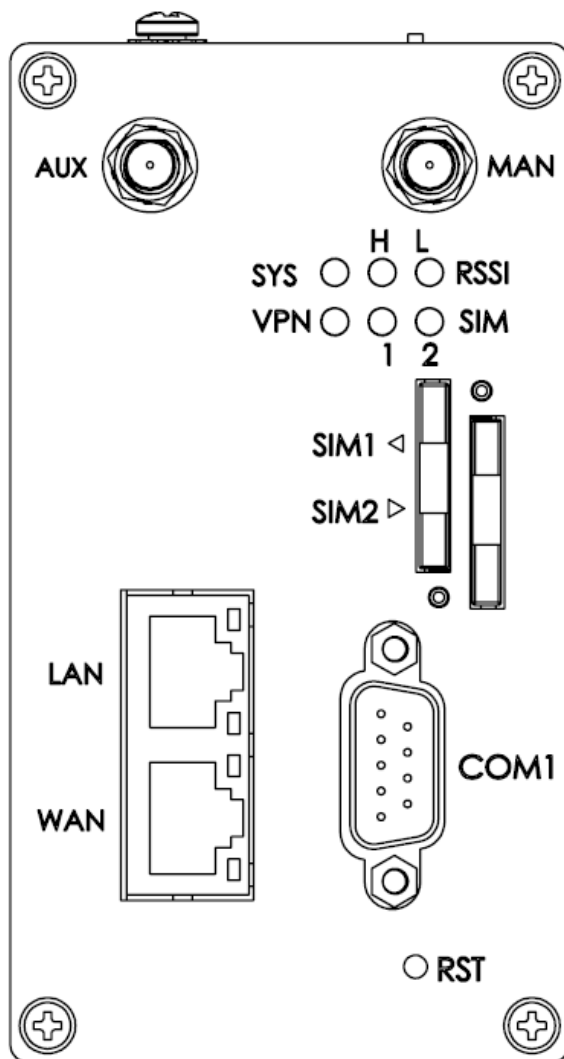
1.4 Hardware Panel Layout

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

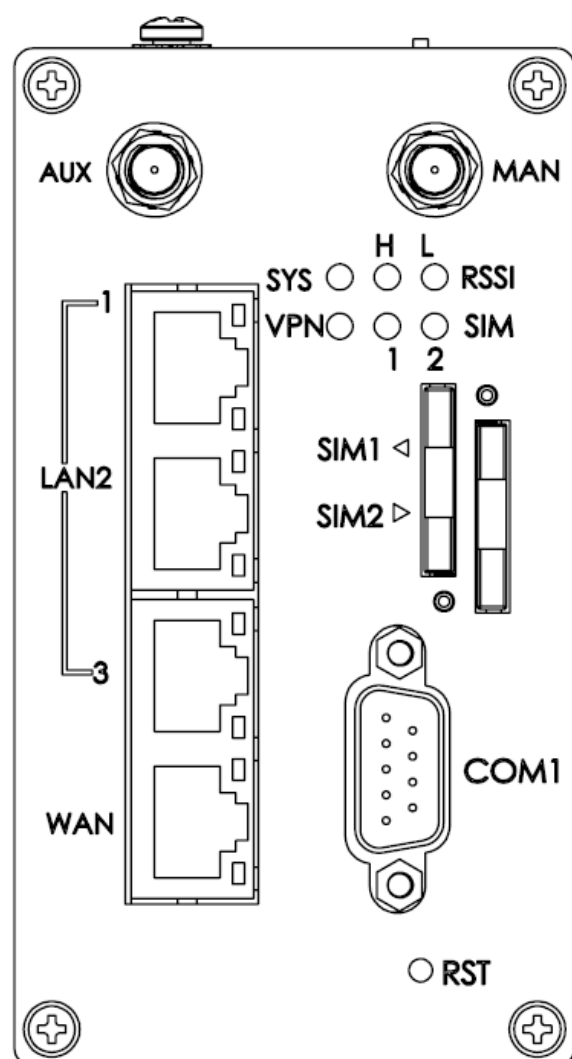
Model Name	Description
M300	Industrial 4G LTE Router (1 x WAN + 1 x LAN)
M301	Industrial 4G LTE Router (1 x WAN + 3 x LAN)
M300G	Industrial 4G LTE Router with GPS (1 x WAN + 1 x LAN + GPS)
M301G	Industrial 4G LTE Router with GPS (1 x WAN + 3 x LAN + GPS)

[Front Panel View]

Model: **M300**

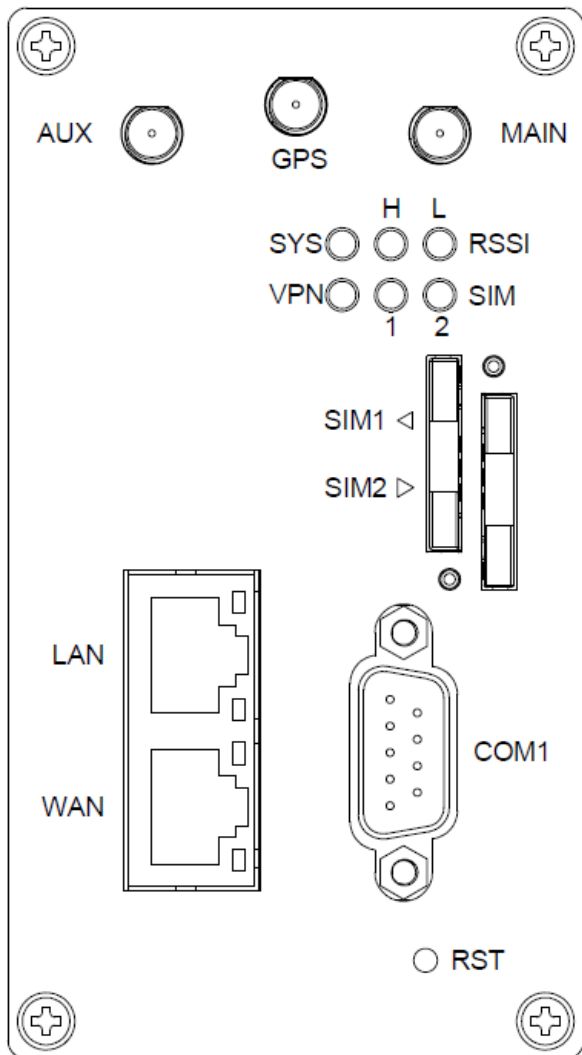


Model: **M301**

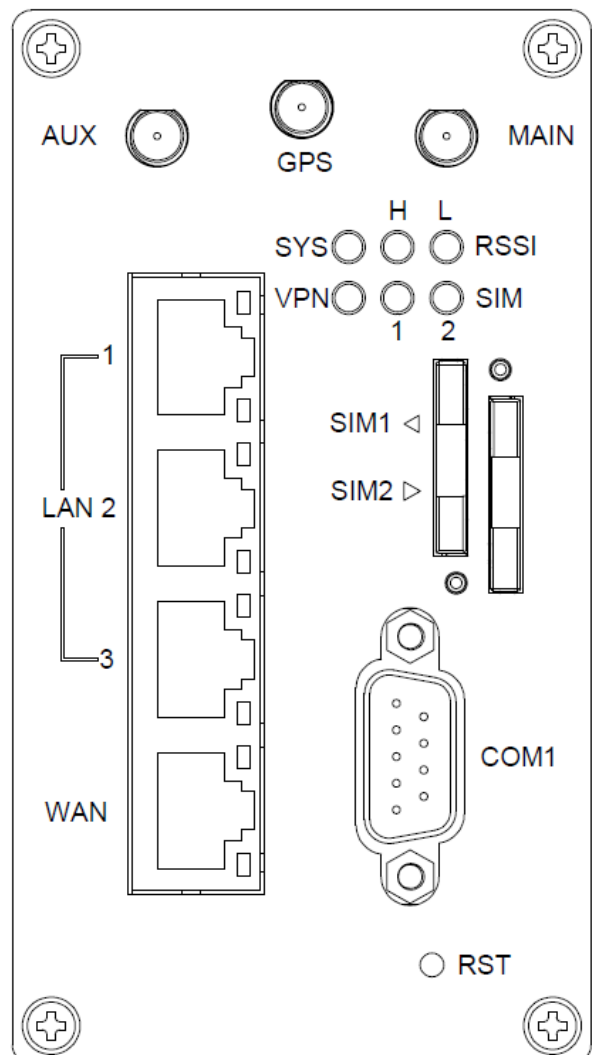


[Front Panel View]

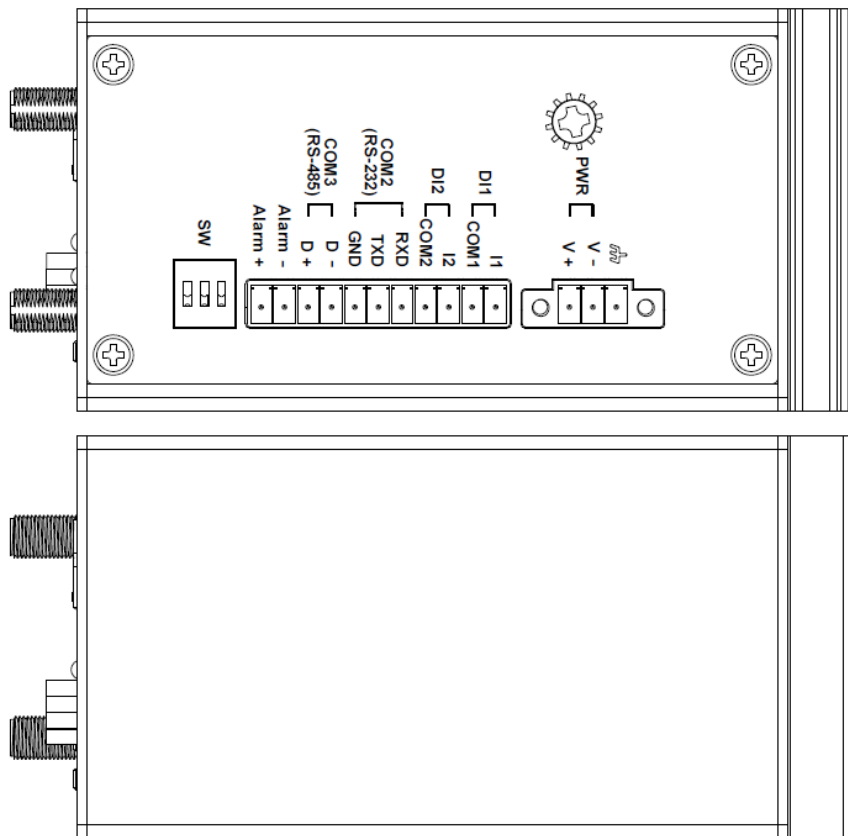
Model: **M300G**



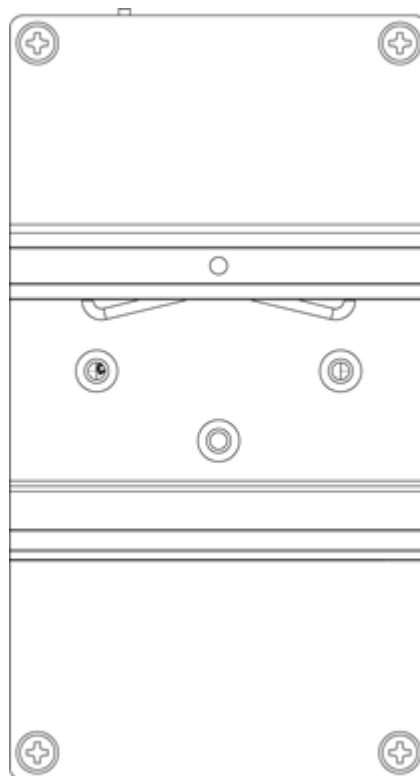
Model: **M301G**



[Top and Bottom View]



[Rear View]



[Left Side View]



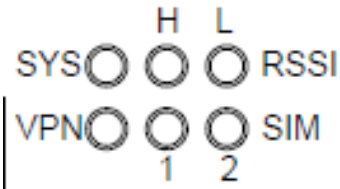
[Right Side View]



2 Hardware Installation

This chapter introduces how to install and connect the hardware.

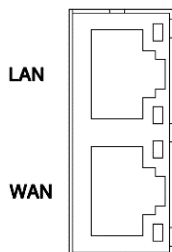
2.1 LED Indicators



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

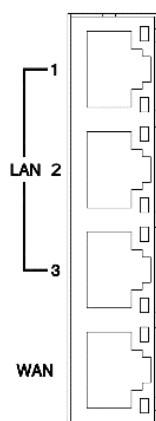
(1) 10/100 Mbps Ethernet WAN



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

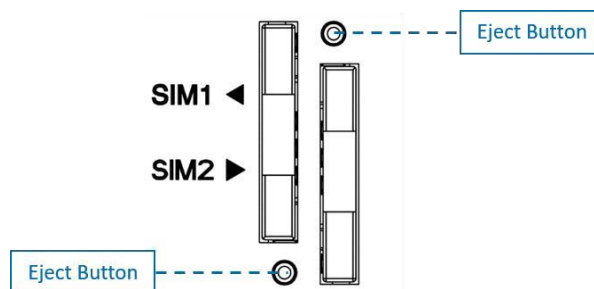
2.3 Serial Port COM1 (Console)

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.

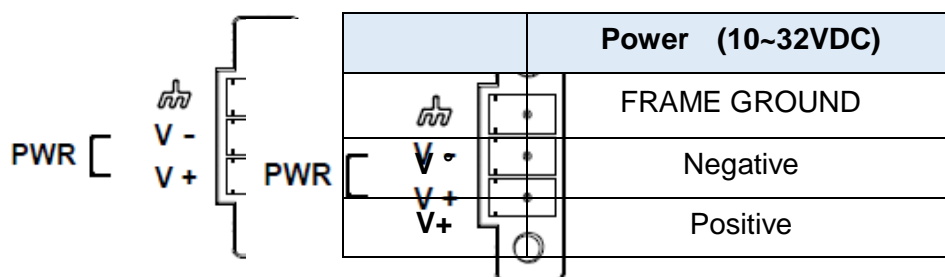
Function	Operation
Reboot	Press the button for 1 second
Restore to factory default setting	Press the button for 10 seconds

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.

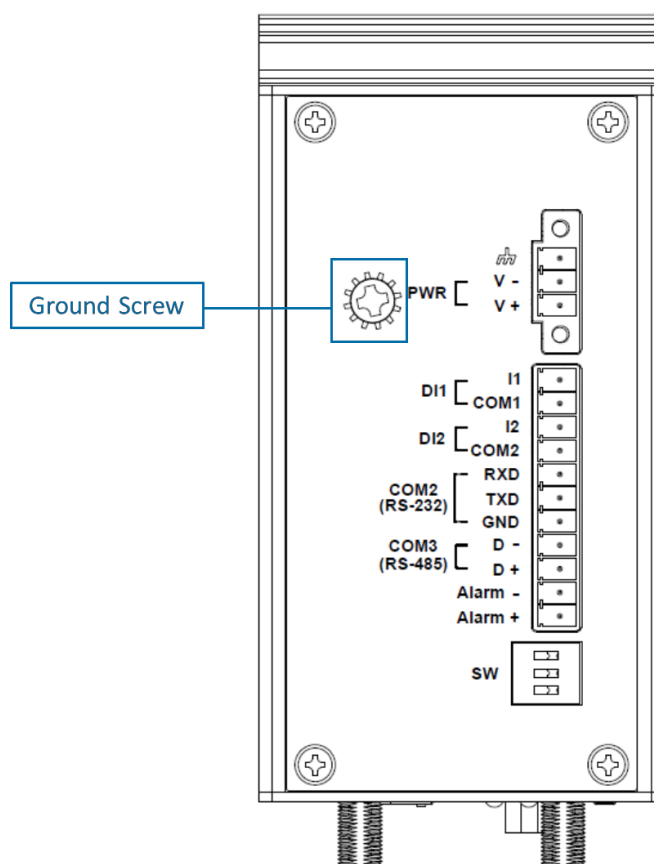
2.7 Connecting the Power Supply

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.

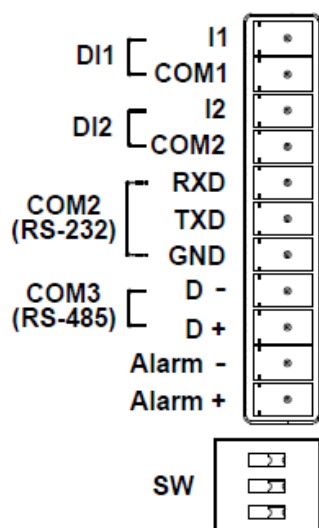


2.8 Grounding the Router

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°232) / COM3 (RS°485)

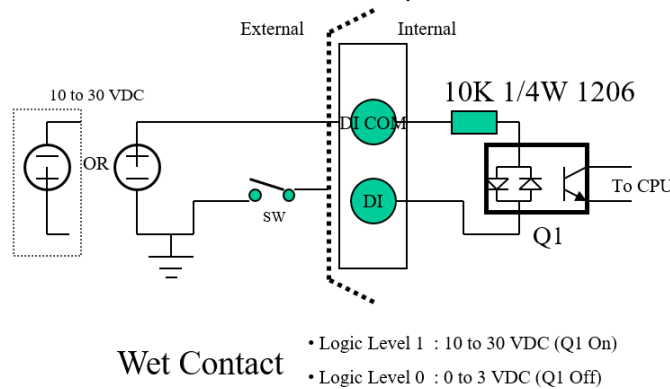
2.10 Connecting I/O Ports

(1) Digital Input DI1 & DI2

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

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

Note: Q1 is a bidirectional component.



Digital Input

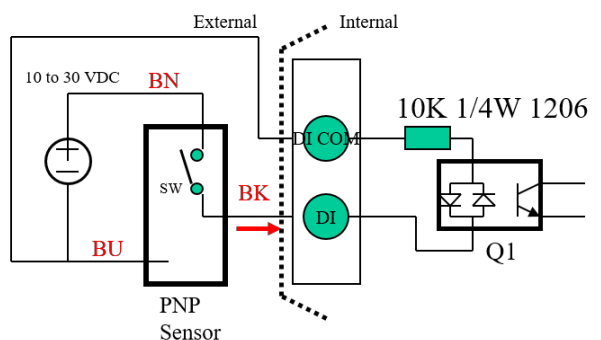
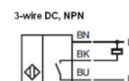
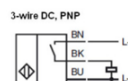
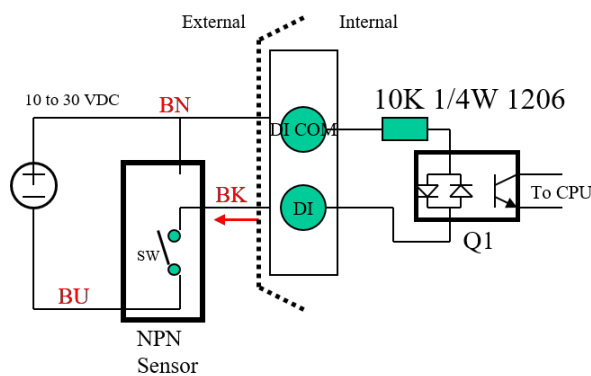
- Wet Contact (Level from DI to DI COM)
 - Logic Level 1 : 10 to 30 VDC (Q1 on)
 - Logic Level 0 : 0 to 3 VDC (Q1 off)

- Wet Contact (Alarm trigger*):

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

* Refer to the Alarm function on web management

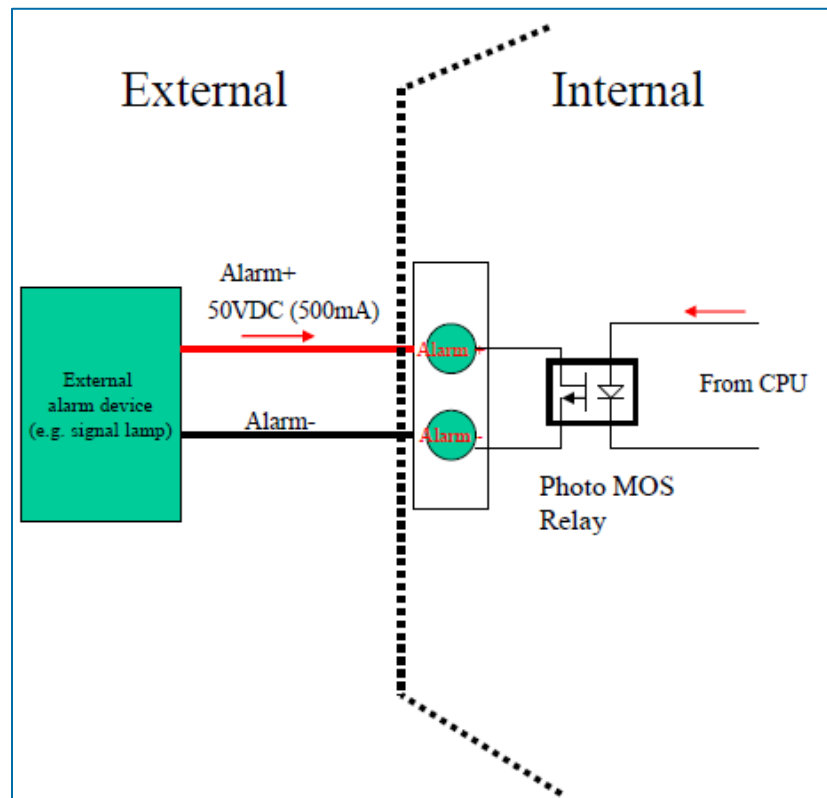
* Q1 is bi-directional part



(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 (RS²³²)

The serial port COM2 is a RS²³² interface.

Pin	Description
RXD	COM2 Serial Port, RXD Signal (INPUT)
TXD	COM2 Serial Port, TXD Signal (OUTPUT)
GND	COM2 Serial Port, Signal Ground

2.12 Serial Port COM3 (RS⁴⁸⁵)

The serial port COM3 is a RS⁴⁸⁵ interface.

Pin	Description
D °	COM3 Serial Port, Data° (B) wire
D +	COM3 Serial Port, Data+ (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^obased 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^omask 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.



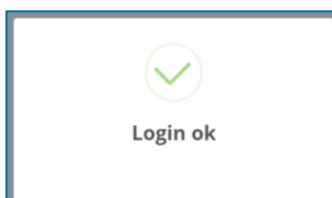
A language selection dropdown menu. The label 'Language' is on the left, and a box contains the word 'English' followed by a downward-pointing arrow.

Logging in the Router

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



A login form with a blue header bar labeled 'Login'. Below the header, there are two input fields: 'User Name' with the text 'root' and 'Password' with masked characters '*****'. A blue 'Login' button is located at the bottom right of the form.



Note: After changing the User Name and Password, strongly recommend you to save them because another time when you 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 header includes 'System Uptime: 5:26:50' and 'WAN Priority: ETH Only'. The sidebar on the left has buttons for 'Status', 'System', 'WAN', 'LAN', 'Service', and 'Management'. The 'Status' page is active, showing a table of cellular attributes and two sections for Ethernet WAN and Ethernet LAN.

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	
Attr.	Value
IPv4 Address	
IPv4 Mask	

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

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

Ethernet WAN	
Attr.	Value
IPv4 Address	
IPv4 Mask	

Status > Ethernet WAN	
Item	Description
Attribute	
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
Attribute	
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.

Mobile Router | Chungwa Telecom | System Uptime: 06:49 | WAN Priority: Auto | Location: (24.77, 121.01) | Language: English | Login

Status | **System**

Status

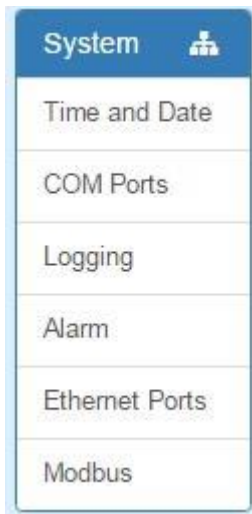
Attr.	Value
Current SIM	Backup SIM
SIM1	SIM2
Ready	Not Inserted
Chunghwa Telecom	
FDD LTE	
466924290355496	
LTE BAND 7	
3050	0
10.162.241.68	
255.255.255.255	

Ethernet LAN

Attr.	Value
IPv4 Address	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
Time and Date	Configure the time and date of router and NTP server.
COM Ports	Configure the COM Ports.
Logging	Configure the Logging.
Alarm	Configure the Alarm.
Ethernet Ports	Configure the Ethernet Ports.
Modbus	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 time.nist.gov

IPv4 Server #2 pool.ntp.org

IPv4 Server #3 ntp.eu.sixxs.net

IPv6 Server #1 time-d.nist.gov

IPv6 Server #2 2.pool.ntp.org

IPv6 Server #3 ntp.eu.sixxs.net

Time Zone Setup

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

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

2017

-

1

-

12

8

:

1

:

38

Time Zone Setup

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





Apply

5.2 System > COM Ports

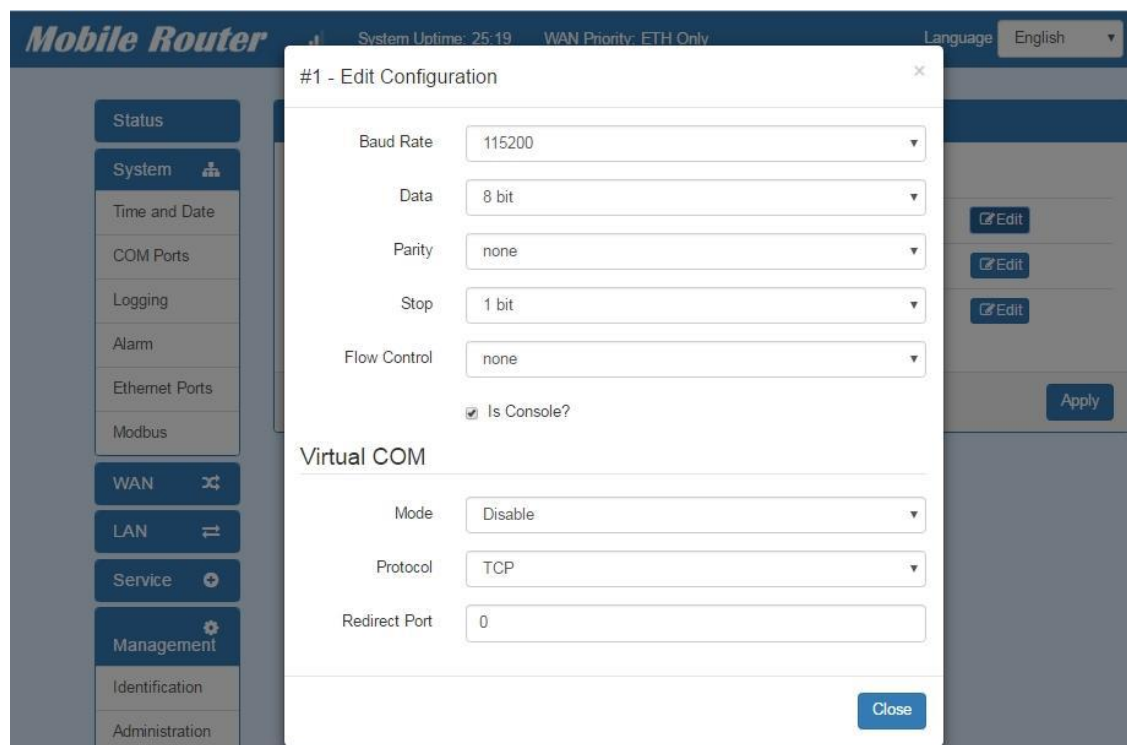
This section provides you to configure the COM port settings and remotely manage the device through the virtual COM setting. For the remote management, the managed device should be connected to the mobile router by serial interface either RS232 or RS485.

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.

COM Ports					
#	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.



The screenshot shows the 'Mobile Router' configuration interface. On the left is a sidebar with navigation options: Status, System, Time and Date, COM Ports, Logging, Alarm, Ethernet Ports, Modbus, WAN, LAN, Service, Management, Identification, and Administration. The 'COM Ports' section is active. The main area displays a table with three rows, each representing a COM port (1, 2, and 3). All ports are currently set to 'Disable' mode, 'TCP' protocol, and port '0'. Each row has an 'Edit' button. A dialog box titled '#1 - Edit Configuration' is open, showing settings for COM port 1. The settings are: Baud Rate (115200), Data (8 bit), Parity (none), Stop (1 bit), Flow Control (none), and a checked 'Is Console?' checkbox. Below these is the 'Virtual COM' section with settings: Mode (Disable), Protocol (TCP), and Redirect Port (0). The dialog box has a 'Close' button at the bottom right.

- (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.

COM Ports					
#	Mode	Host Address	Protocol	Port	
1	Server		TCP	6000	Edit
2	Disable		TCP	0	Edit
3	Disable		TCP	0	Edit
					Apply

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	<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.

Status

System

Time and Date

COM Ports

Logging

Alarm

Ethernet Ports

Modbus

WAN

LAN

Service

Management

Logging

Mode ☐ Disable ☒ Enable

Remote Log ☒ Disable ☐ Enable

Log Server Address

Apply

Log

filter

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

Clear Refresh

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



The screenshot shows the 'Log' interface. At the top, there is a 'filter' input field. Below it is a table with the following columns: '#', 'Date', 'Group', 'Module', and 'Message'. There is one entry in the table: '# 1', 'Date 2017-05-31 05:06:48', 'Group WAN', 'Module DHCP', and 'Message DHCP client timeout.'. At the bottom right of the table, there are two buttons: 'Clear' and 'Refresh'.

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.



The screenshot shows the 'Logging' configuration interface. It has a blue header with a 'Logging' title. Below the header, there are two rows of radio button settings. The first row is 'Mode' with 'Disable' and 'Enable' options, where 'Enable' is selected. The second row is 'Remote Log' with 'Disable' and 'Enable' options, where 'Disable' is selected. Below these, there is a 'Log Server Address' label and a text input field containing '255.255.255.255'. At the bottom right, there is an 'Apply' button.

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

5.4 System > Alarm

This section allows you to configure the alarm.

Alarm

Mode ☒ Disable ☐ Enable

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

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

(1) How to create your group

☐ Name a group

Groups Group ▾

SMS characters

Group name

✕ ✓

Groups Group ▾

SMS characters

Office1

✕ ✓

☐ Show your group name from the list of group.

Groups Group ▾

SMS characters

Office1


✕ ✓

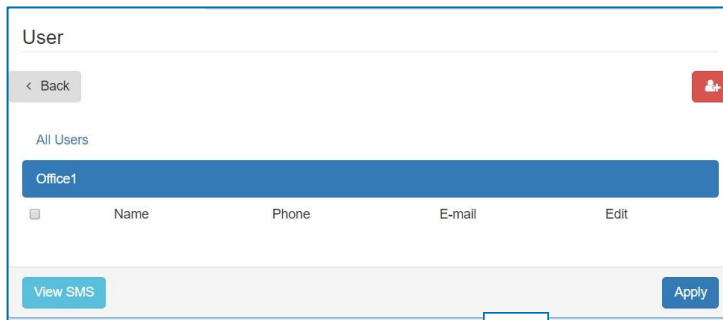
Group

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


View SMS
Apply

(2) How to edit your group

□ Select your group and click  to edit your group information, including Name, Phone and E°mail.



User


< Back 

All Users

Office1

<input type="checkbox"/>	Name	Phone	E-mail	Edit
--------------------------	------	-------	--------	------

View SMS Apply

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



User

Name: test

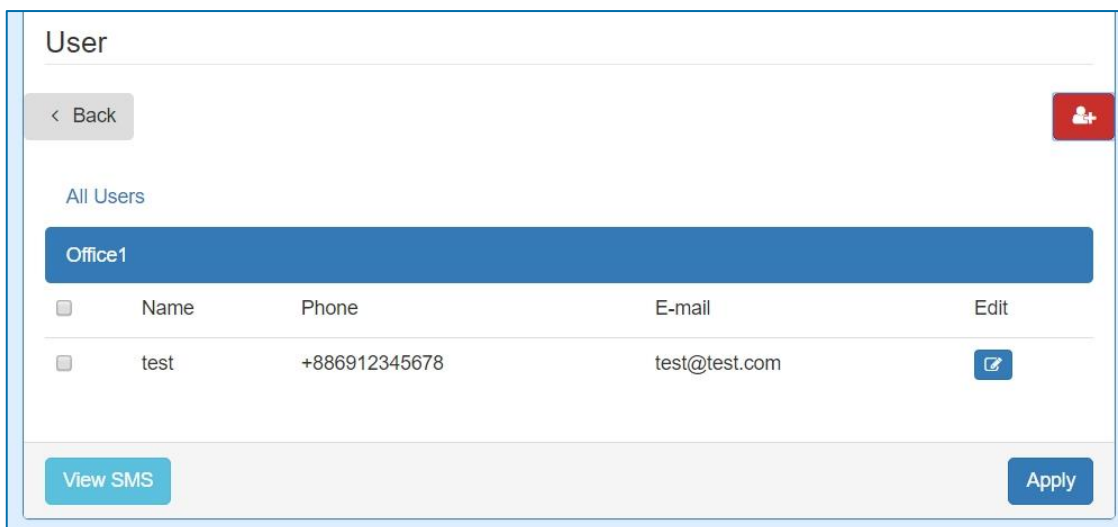
Phone: +886912345678

E-mail: test@test.com


Groups: 



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




User

< Back 


All Users


Office1

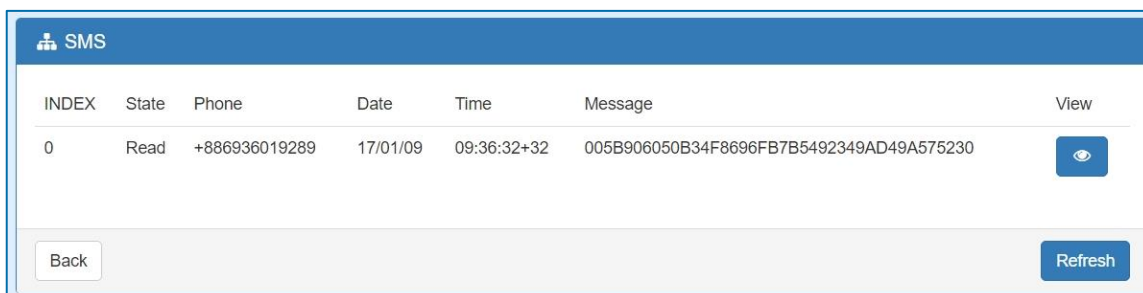
<input type="checkbox"/>	Name	Phone	E-mail	Edit
<input type="checkbox"/>	test	+886912345678	test@test.com	


View SMS Apply

(3) How to View SMS

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

□ Click  to review your all messages.



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

Back Refresh


17/01/09 09:36:32+32 ✕

005B906050B34F8696FB7B5492349AD49A575230671F901A77E5005D60A87684514D8
CBB9AD49A575C0765BC003359295F8C5230671F002E4EFB610F937556DE8986672C7
C218A0A621675

Close

5.5 System > Ethernet Ports

This section allows you to configure the Ethernet Ports.

 Ethernet Ports

Name	Status	Mode
LAN	100M Half	<input checked="" type="radio"/> Auto <input type="radio"/> 100M Full <input type="radio"/> 100M Half <input type="radio"/> 10M Full <input type="radio"/> 10M Half <input type="radio"/> Disable
WAN	100M Full	<input checked="" type="radio"/> Auto <input type="radio"/> 100M Full <input type="radio"/> 100M Half <input type="radio"/> 10M Full <input type="radio"/> 10M Half <input type="radio"/> Disable


Refresh Apply

System > Ethernet Ports	
Item	Description
Name	Show the name of LAN and WAN.
Status	Show the connectivity status of LAN and WAN.
Mode	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

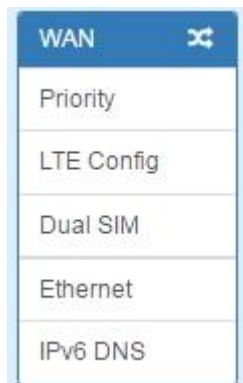
Mode ☐ Disable ☒ Enable

Port

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

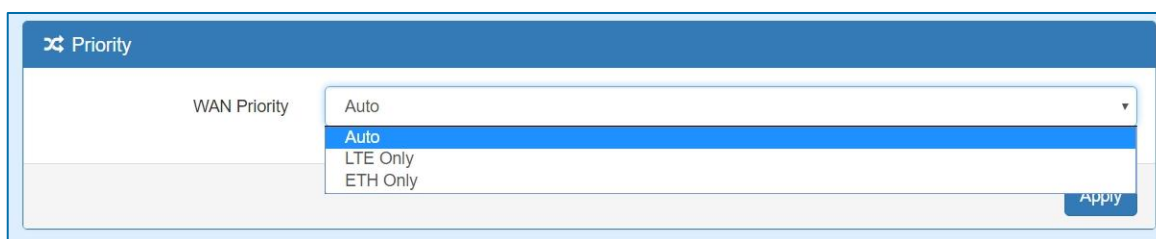
6 Configuration > WAN

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
Priority	<ul style="list-style-type: none">□Auto: WAN Ethernet is first priority and second priority is LTE. The default is Auto.□LTE Only: The priority is only LTE.□ETH Only: The priority is only Ethernet.

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"/>	<input type="password"/>
Confirmed SIM PIN	<input type="password"/>	<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 <input type="button" value="Disconnect"/>
Disable Roaming	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Switch to another SIM when roaming is detected	<input type="checkbox"/>

Apply

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

Change SIM PIN

 Change

 Change

Old PIN

New PIN

PIN
Remaining
Number

3

PUK
Remaining
Number

10

Apply

WAN > Dual SIM	
Item	Description
Dual SIM	
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.
Data Limitation	
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.
Connect Policy	
Current SIM Card	Display which SIM slot is using.
Status of SIM Card Connectivity	<p><input type="checkbox"/> Connect: 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"/> Connect: 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"/> Disable: SIM gets connection even it roaming state.</p> <p><input type="checkbox"/> Enable: 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's a header 'WAN Ethernet' with a router icon. Below it, the 'Work As' section has three radio buttons: 'DHCP Client' (selected), 'PPPoE Client', and 'Static IPv4'. Underneath is the 'DNS Server Configuration' section with three rows for 'IPv4 DNS Server #1', '#2', and '#3'. Each row has a dropdown menu set to 'From ISP' and an adjacent text input field. An 'Apply' button is located at the bottom right.

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

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

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

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. It contains two input fields: 'User Name' with the value 'test' and 'Password' with masked characters '*****'. An 'Apply' button is located at the bottom right of the configuration area.

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, which has 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
Static IPv4 Configuration	
IP Address	Fill in the IP Address.
IP Mask	Fill in the IP Mask.
Gateway Address	Fill in Gateway Address.
DNS Server Configuration	
IPv4 DNS Server #1	The IPv4 DNS server IP is input by user.
IPv4 DNS Server #2	
IPv4 DNS Server #3	

6.5 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 at the bottom right of the configuration area.

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

This screenshot shows the same 'IPv6 DNS' configuration window, but the dropdown menu for 'IPv6 DNS Server #2' is open. It displays three options: 'From ISP' (which is highlighted in blue), 'User Defined', and 'None'. The other two dropdowns remain set to 'From ISP'. The 'Apply' button is still visible at the bottom right.

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

7 Configuration > LAN

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



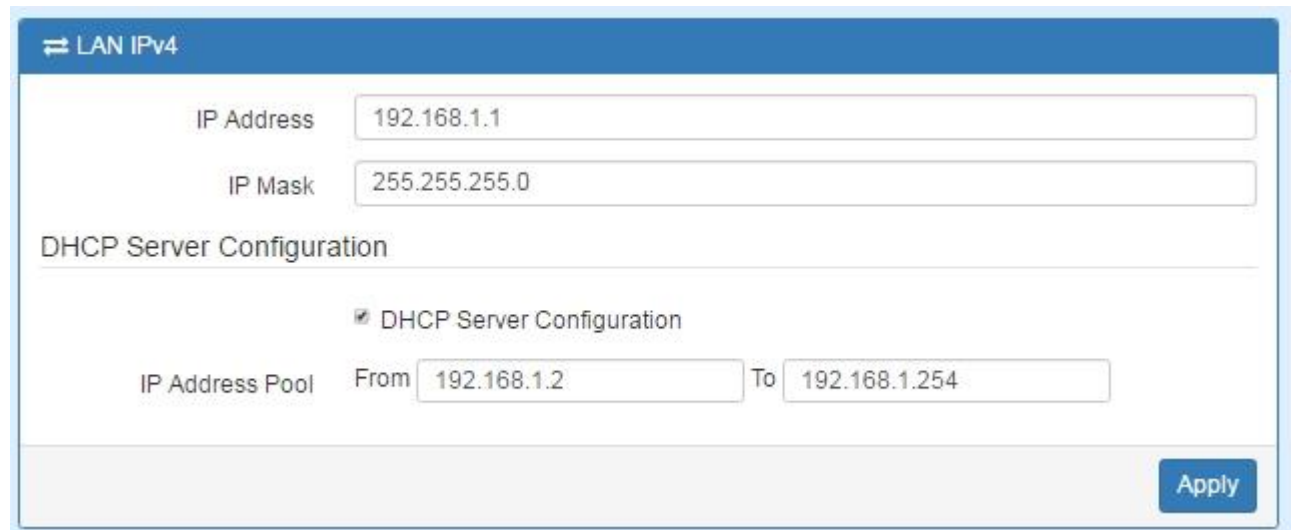
A vertical menu with a blue header 'LAN' and a double-headed arrow icon. Below the header are two white buttons: 'IPv4' and 'IPv6'.



The LAN IPv4 configuration page. On the left is a sidebar with buttons: Status, System, WAN, LAN (selected), IPv4, IPv6, Service, and Management. The main area has a blue header 'LAN IPv4'. It contains fields for 'IP Address' (192.168.1.1) and 'IP Mask' (255.255.255.0). Below is a section 'DHCP Server Configuration' with a checked checkbox 'DHCP Server Configuration'. Underneath are fields for 'IP Address Pool' with 'From' (192.168.1.2) and 'To' (192.168.1.254). An 'Apply' button is at the bottom right.

7.1 LAN > IPv4

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



A detailed view of the LAN IPv4 configuration page. It shows the same fields as the previous image: 'IP Address' (192.168.1.1), 'IP Mask' (255.255.255.0), 'DHCP Server Configuration' (checked), and 'IP Address Pool' (From 192.168.1.2 to 192.168.1.254). An 'Apply' button is at the bottom right.

LAN > IPv6	
Item	Description
LAN IPv6	<p><input type="checkbox"/> This section provides two types, including Delegate Prefix from WAN and Static.</p> <p><input type="checkbox"/> Static Address: You need to input the static address when you select the static type.</p>
Delegate Prefix from WAN	<p><input type="checkbox"/> Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.</p>
Static	<p><input type="checkbox"/> Select this option to configure a fixed IPv6 address for the mobile router's LAN IPv6 address.</p>
Address Assign Setup	<p>Select how you want to obtain an IPv6 address:</p> <p><input type="checkbox"/> Stateless: 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.</p> <p><input type="checkbox"/> Stateful: The mobile router uses IPv6 stateful auto configuration. The LAN IPv6 clients can obtain IPv6 addresses through DHCPv6.</p>

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 screenshot shows the 'Open VPN' configuration page. At the top, there is a 'Mode' section with radio buttons for 'Disable' (selected) and 'Enable'. Below this is a table with 7 columns: #, Mode, VPN Mode, Device, Protocol, Port, and Edit. The table contains 10 rows, all with 'Disable' in the Mode column, 'Client' in the VPN Mode column, 'TUN' in the Device column, 'UDP' in the Protocol column, and '1701' in the Port column. Each row has an 'Edit' icon in the last column. At the bottom right, there is an 'Apply' button.

#	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

BF-CBC

Status

Idle

Device

☒ TUN ☐ TAP

Protocol

☒ UDP ☐ TCP

Port

1701

VPN Compression

☒ Disable ☐ Enable

Authentication

Certificate

Client

Client Mode

☒ Roadwarrior

Server Address

0.0.0.0

Route Client Networks

☒ Off ☐ On


NAT

1:1 NAT


☒ Off ☐ On

Client - Security


Root CA

 Import


Cert

 Import

Key

 Import

P12

 Import

Back

Refresh

Apply

Service > OpenVPN	
Item	Description
Mode	Turn on/off OpenVPN to select Disable or Enable.
VPN Mode	<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.
TLS Mode	Select from Disable or Enable for data security. The default is Disable.
TLS minimal version	Select from none, 1.0, 1.1 or 1.2. The default is none.
Cipher	The OpenVPN format of data transmission.
Status	Display the status of OpenVPN.
Device	Select from TUN or TAP. The default is TUN.
Protocol	Select from UDP or TCP Client which depends on the application. The default is UDP.
Port	Enter the listening port of remote side OpenVPN server.
VPN Compression	Select Disable or Enable to compress the data stream. The default is Disable.
Authentication	<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
Client	
Client Mode	Only support the Roadwarrior mode.
Server Address	Fill in WAN IP of OpenVPN server.
Route Client Networks	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.
NAT	
1:1 NAT	<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.
Client°Security	
Root CA	The Certificate Authority file of OpenVPN server could be downloaded from OpenVPN server.
Cert	The certification file is for OpenVPN client, which could be downloaded from OpenVPN server.
Key	The private key file is for OpenVPN client, which could be downloaded from OpenVPN server.
P12	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

BF-CBC

Status

Idle

Device

☒ TUN
☐ TAP

Protocol

☒ UDP
☐ TCP

Port

1701

VPN Compression

☒ Disable
☐ Enable

Authentication

Certificate

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
Server	
Client Mode	Only support the Roadwarrior mode.
VPN Network	The network ID for OpenVPN virtual network.
VPN Netmask	The netmask for OpenVPN virtual network.
Roadwarrior: Route Client Networks	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.
NAT	
1:1 NAT	<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.
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.

- (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.

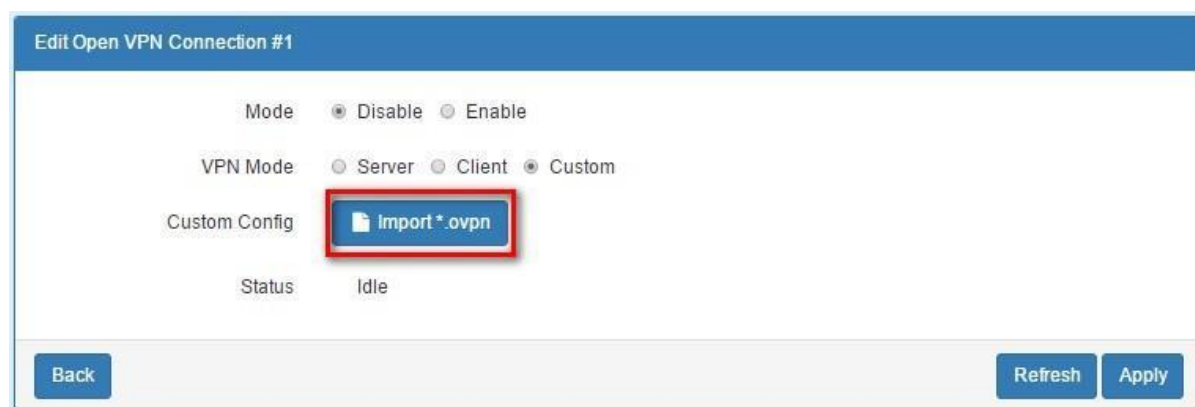
Note:

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
Mode	Select from Disable or Enable. The default is Disable.
VPN Mode	Select from custom mode.
Custom Config	Import OpenVPN configuration.
Status	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 checked="" type="button" value="u"/>
2	<input type="checkbox"/>		0.0.0.0	0.0.0.0	<input checked="" type="button" value="i"/>	<input checked="" type="button" value="u"/>
3	<input type="checkbox"/>		0.0.0.0	0.0.0.0	<input checked="" type="button" value="i"/>	<input checked="" type="button" value="u"/>
4	<input type="checkbox"/>		0.0.0.0	0.0.0.0	<input checked="" type="button" value="i"/>	<input checked="" type="button" value="u"/>
5	<input type="checkbox"/>		0.0.0.0	0.0.0.0	<input checked="" type="button" value="i"/>	<input checked="" type="button" value="u"/>
6	<input type="checkbox"/>		0.0.0.0	0.0.0.0	<input checked="" type="button" value="i"/>	<input checked="" type="button" value="u"/>
7	<input type="checkbox"/>		0.0.0.0	0.0.0.0	<input checked="" type="button" value="i"/>	<input checked="" type="button" value="u"/>
8	<input type="checkbox"/>		0.0.0.0	0.0.0.0	<input checked="" type="button" value="i"/>	<input checked="" type="button" value="u"/>
9	<input type="checkbox"/>		0.0.0.0	0.0.0.0	<input checked="" type="button" value="i"/>	<input checked="" type="button" value="u"/>
10	<input type="checkbox"/>		0.0.0.0	0.0.0.0	<input checked="" type="button" value="i"/>	<input checked="" type="button" value="u"/>
11	<input type="checkbox"/>		0.0.0.0	0.0.0.0	<input checked="" type="button" value="i"/>	<input checked="" type="button" value="u"/>
12	<input type="checkbox"/>		0.0.0.0	0.0.0.0	<input checked="" type="button" value="i"/>	<input checked="" 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.

Edit IPsec Connection #1

Mode

☒ Disable ☐ Enable

Name

IKE

Protocol

ikev1

Encryption

aes128

Hash

sha1

DH Group

modp1536

Encryption

Protocol

esp

Encryption

aes128

Hash

sha1

DH Group

modp1536

Local

Host

0.0.0.0

Subnet

0.0.0.0/0

Remote

Host

0.0.0.0

Subnet

0.0.0.0/0

Auth Type

psk

Auth Scret

Save

Security of Connection #1

Create

Cert

Key

Root CA

i

u

Server

User 0

User 1

User 2

User 3

□ Set up IKE.

IKE

Protocol

ikev1

Encryption

aes128

Hash

sha1

DH Group

modp1536

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

8.3 Service > Configuration Port Forwarding

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

+

Port Forwarding

Mode

☒ Disable
 ☐ Enable

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

Apply

Edit Configuration #1

×

Mode

☒ Disable
 ☐ Enable

Description

ssh

Protocol

☒ TCP
 ☐ UDP

Source Port Begin

22

Source Port End

22

Destination IP

0.0.0.0

Destination Port

22

Close

Service > Port Forwarding	
Item	Description
Mode	Turn on/off Port Forwarding to select Disable or Enable. The default is Disable.
Description	Describe 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	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

dynv6.com

Host Name

Token ID

Update Period Time (Sec)

0

Apply

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

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

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

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

Service Provider	www.duckdns.org
Host Name	Register hostname, e.g. tester.duckdns.org
Token ID	The token ID, e.g. 12345678°de49°4e97°a33c°98b159ae2b

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
Mode	Select from Disable or Enable to configure SNMP. 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.

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
Mode	Select from Disable or Enable to configure SNMP. The default is Disable.
Community Name	Fill in your community name.
Destination	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 web interface titled "Edit IP Filter Black List Entry #1". It contains several configuration fields:

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

Service > 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.

- (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
IPv4	192.168.0.123	192.168.1.0/24 192.168.1.0/255.255.255.	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° 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

TCP

Source IP

192.168.0.0/24

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

3:123

Ex.
1234
1234:5678

Destination IP


192.168.0.0-192.168.0.100

Destination Port

9000

Apply

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
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 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
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.

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

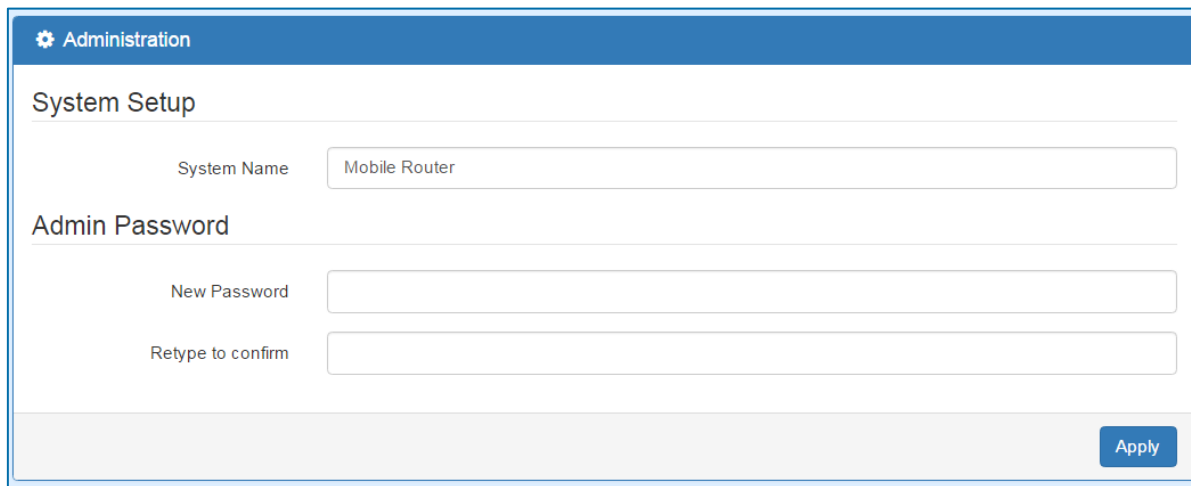
This section allows you to confirm the profile of router, current software, firmware version and system uptime.

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

9.2 Administration

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

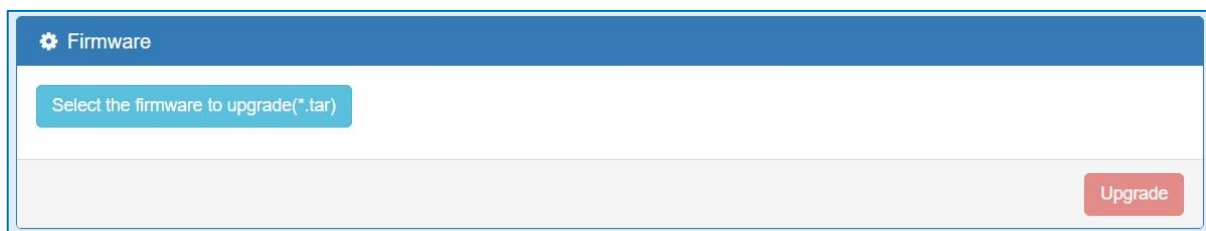


The screenshot shows the 'Administration' section of a web interface. It has a blue header bar with a gear icon and the word 'Administration'. Below the header, the 'System Setup' section contains a 'System Name' label and a text input field with 'Mobile Router' entered. The 'Admin Password' section has two labels, 'New Password' and 'Retype to confirm', each followed by an empty text input field. At the bottom right of the form is a blue 'Apply' button.

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.

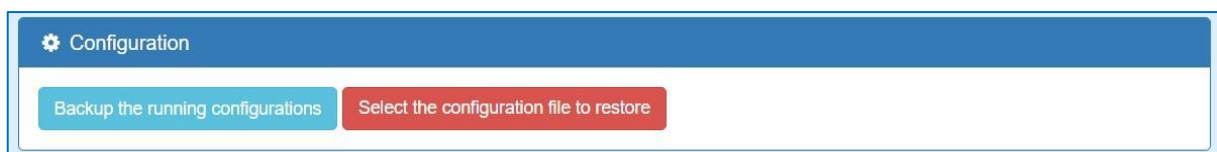


The screenshot shows the 'Firmware' section of a web interface. It has a blue header bar with a gear icon and the word 'Firmware'. Below the header, there is a light blue button labeled 'Select the firmware to upgrade(*.tar)'. At the bottom right of the section is a red 'Upgrade' button.

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 of a web interface. It has a blue header bar with a gear icon and the word 'Configuration'. Below the header, there are two buttons: a light blue button labeled 'Backup the running configurations' and a red button labeled 'Select the configuration file to restore'.

9.5 Load Factory

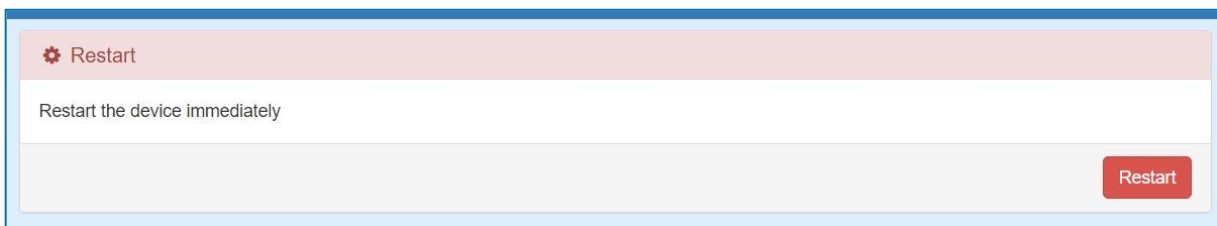
This section supports you to load the factory default configuration and restart the device immediately. You can click the Load Factory and Restart button.



The screenshot shows a web interface for the 'Load Factory' function. It features a red header bar with a gear icon and the text 'Load Factory'. Below the header is a white text area containing the instruction 'Load the factory default configuration and restart the device immediately'. At the bottom right of the interface is a red button labeled 'Load Factory and Restart'.

9.6 Restart

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



The screenshot shows a web interface for the 'Restart' function. It features a red header bar with a gear icon and the text 'Restart'. Below the header is a white text area containing the instruction 'Restart the device immediately'. At the bottom right of the interface is a red button labeled 'Restart'.