robustel | User Guide

R3000 Quad

Industrial Cellular VPN Router with 4 Ethernet Ports

4 Eth + 1 RS232/1 RS485 + 1 USB Host

robustOS

Guangzhou Robustel Co., Ltd.
www.robustel.com

About This Document

This document provides hardware and software information of the Robustel R3000 Quad Router, including introduction, installation, configuration and operation.

Trademarks and Permissions


are trademarks of Guangzhou Robustel Co., Ltd.. All other trademarks and trade names mentioned in this document are the property of their respective owners.

Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner. The contents of this document are subject to change without notice due to continued progress in methodology, design and manufacturing. Robustel shall have no liability for any error or damage of any kind resulting from the inappropriate use of this document.

Technical Support

Tel: +86-20-82321505
Email: support@robustel.com
Web: www.robustel.com

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the router is used in a normal manner with a well-constructed network, the router should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Robustel accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the router, or for failure of the router to transmit or receive such data.

Safety Precautions

General

- The router generates radio frequency (RF) power. When using the router, care must be taken on safety issues related to RF interference as well as regulations of RF equipment.
- Do not use your router in aircraft, hospitals, petrol stations or in places where using cellular products is prohibited.
- Be sure that the router will not be interfering with nearby equipment. For example: pacemakers or medical equipment. The antenna of the router should be away from computers, office equipment, home appliance, etc.
- An external antenna must be connected to the router for proper operation. Only uses approved antenna with the router. Please contact authorized distributor on finding an approved antenna.
- Always keep the antenna with minimum safety distance of 20 cm or more from human body. Do not put the antenna inside metallic box, containers, etc.
- When used, the device needs a suitable environment.
    1. If indoors, it needs to be provided an indoor enclosure.
    2. If outdoors, it needs to be provided a rain proof enclosure.
- RF exposure statements
    1. For mobile devices without co-location (the transmitting antenna is installed or located more than 20cm away from the body of user and nearby person)
- FCC RF Radiation Exposure Statement
    1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
    2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and human body.

***Note**: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open.* Router *may be used at this time.*

Using the Router in Vehicle

- Check for any regulation or law authorizing the use of cellular devices in vehicle in your country before installing the router.
- The driver or operator of any vehicle should not operate the router while driving.
- Install the router by qualified personnel. Consult your vehicle distributor for any possible interference of electronic parts by the router.
- The router should be connected to the vehicle's supply system by using a fuse-protected terminal in the vehicle's fuse box.
- Be careful when the router is powered by the vehicle's main battery. The battery may be drained after extended period.

Protecting Your Router

To ensure error-free usage, please install and operate your router with care. Do remember the following:

- Do not expose the router to extreme conditions such as high humidity / rain, high temperature, direct sunlight, caustic / harsh chemicals, dust, or water.
- Do not try to disassemble or modify the router. There is no user serviceable part inside and the warranty would be void.
- Do not drop, hit or shake the router. Do not use the router under extreme vibrating conditions.
- Do not pull the antenna or power supply cable. Attach/detach by holding the connector.
- Connect the router only according to the instruction manual. Failure to do it will void the warranty.
- In case of problem, please contact authorized distributor.

Regulatory and Type Approval Information

Table 1: Directives

2011/65/EU	The European RoHS2.0 2011/65/EU Directive was issued by the European parliament and the European Council on 1 July 2011 on the restriction of the use of certain Hazardous substances in electrical and electronic equipment.
	On June 4, 2015, the Official Journal of the European Union published the RoHS2.0 Amendment Directive (EU) In 2015/863, four phthalates (DEHP, BBP, DBP, DIBP) were officially included in the list of restricted substances in Appendix II of RoHS 2.0 (2011/65/EU). From July 22, 2019, all electronic and electrical products exported to Europe (except medical and monitoring equipment) must meet this restriction; from July 22, 2021, medical equipment and monitoring equipment will also be included in the scope of control.
2012/19/EU	The European WEEE 2012/19/EU Directive was issued by the European parliament and the European Council on 24 July 2012 on waste electrical and electronic equipment.
2013/56/EU	The European 2013/56/EU Directive is a battery Directive which published in the EU official gazette on 10 December 2013. The button battery used in this product conforms to the standard of 2013/56/EU directive.

Table 2: Toxic or Hazardous Substances or Elements with Defined Concentration Limits

Name of the Part	Hazardous Substances									
	(Pb)	(Hg)	(Cd)	(Cr(VI))	(PBB)	(PBDE)	(DEHP)	(BBP)	(DBP)	(DIBP)
Metal parts	o	o	o	o	o	o	o	o	o	o
Circuit modules	o	o	o	o	o	o	o	o	o	o
Cables and cable assemblies	o	o	o	o	o	o	o	o	o	o
Plastic and polymeric parts	o	o	o	o	o	o	o	o	o	o

o:
Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in RoHS2.0.
X:
Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part *might exceed* the limit requirement in RoHS2.0.

Document History

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Date	Firmware Version	Doc Version	Change Description
28 May, 2017	3.0.0	v.3.0.0	Initial release
14 Sept., 2017	3.0.0	v.3.0.1	Updated the certificate and ordering information
29 Jun., 2018	3.0.0	v.3.0.2	Revised the company name
29 Jan., 2019	3.0.0	v.3.0.4	Revised the certifications Revised the Frequency bands of Wifi
22 Jul., 2019	3.0.0	v.3.0.5	• Revised the description of enclosure • Revised the Regulatory and Type Approval Information
26 Nov., 2019	3.0.0	v.3.0.6	• Revised the description of Update firmware via tftp
25 Dec., 2021	3.0.0	v.3.0.7	• Revised the company name • Revised *Regulatory and Type Approval Information* • Revised *Disclaimer*

Contents

Chapter 1 Product Overview 9
1.1 Key Features 9
1.2 Package Contents 10
1.3 Specifications 12
1.4 Dimensions 14
1.5 Ordering Information 14
1.6 Warning 14
Chapter 2 Hardware Installation 16
2.1 LED Indicators 16
2.2 PIN Assignment 17
2.3 USB Interface 18
2.4 Reset Button 19
2.5 Ethernet Port 20
2.6 Insert or Remove SIM Card/Micro SD Card 21
2.7 Attach External Antenna (SMA Type) 22
2.8 Mount the Router 22
2.9 Connect the Router to a Computer 23
2.10 Power Supply 24
Chapter 3 Initial Configuration 25
3.1 Configure the PC 25
3.2 Factory Default Settings 28
3.3 Log in the Router 28
3.4 Control Panel 29
3.5 Status 30
3.6 Interface > Link Manager 32
3.7 Interface > LAN 42
3.8 Interface > Ethernet 47
3.9 Interface > Cellular 48
3.10 Interface > WiFi 52
3.11 Interface > USB 59
3.12 Interface > Serial Port 59
3.13 Network > Route 64
3.14 Network > Firewall 65
3.15 Network > IP Passthrough 69
3.16 VPN > IPsec 69
3.17 VPN > OpenVPN 77
3.18 VPN > GRE 85
3.19 Services > Syslog 86
3.20 Services > Event 87
3.21 Services > NTP 91
3.22 Services > SMS 92
3.23 Services > Email 93
3.24 Services > DDNS 94
3.25 Services > SSH 95

3.26 Services > GPS 96
3.27 Services > Web Server 99
3.28 Services > Advanced 100
3.29 System > Debug 101
3.30 System > Update 102
3.31 System > APP Center 103
3.32 System > Tools 104
3.33 System > Profile 106
3.34 System > User Management 108
Chapter 4 Configuration Examples 110
4.1 Cellular 110
4.1.1 Cellular Dial-Up 110
4.1.2 SMS Remote Control 112
4.2 Network 114
4.2.1 IPsec VPN 114
4.2.2 OpenVPN 117
4.2.3 GRE VPN 120
Chapter 5 Introductions for CLI 122
5.1 What Is CLI 122
5.2 How to Configure the CLI 123
5.3 Commands Reference 129
Glossary 130

Chapter 1 Product Overview

1.1 Key Features

The Robustel Industrial Cellular VPN Router with 4 Ethernet Ports (R3000 Quad) is a rugged cellular router offering state-of-the-art mobile connectivity for machine to machine (M2M) applications. R3000 Quad is a powerful router developed from RobustOS, a Robustel self-developed and Linux-based operating system which is designed to be used in Robustel hardware routers. The RobustOS includes basic networking features and protocols providing customers with a very good user experience. Meanwhile, Robustel offers a Software Development Kit (SDK) for partners and customers to allow additional customization by using C, C++. It also provides rich APPs to meet fragmented IoT market demands.

- The feature *Link Manager* supporting WWAN1, WWAN2, Ethernet WAN, WLAN WAN link backup and ICMP detection
- The option *Backup Mode* supporting cold, warm and load balancing
- Wi-Fi mode supporting AP and Client (2.4 GHz/5 GHz), also supporting Captive Portal
- Dual SIM redundancy for persistent 2G/3G/4G cellular network connections
- RobustOS + SDK + App
- IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN
- Supporting Modbus RTU to TCP
- Supporting Modbus Master
- Supporting TCP Client/Server, UDP and virtual serial port
- Supporting DHCP server
- Supporting 802.1Q VLAN Trunk protocol
- Supporting IP Pass-through
- Supporting RobustVPN (a Cloud VPN Portal providing easy and secure remote access for PLC and machines)
- Management and maintenance via Web/CLI/USB/RobustLink Cloud
- Alarm via SMS/Email/SNMP trap/RobustLink
- Auto reboot via SMS/Timing
- Desktop and easy wall or DIN rail mounting options

1.2 Package Contents

Before installing your R3000 Quad Router, verify the kit contents as following.

Note: The following pictures are for illustration purposes only, not based on their actual sizes.

- 1 x Robustel GoRugged R3000 Quad Industrial Cellular VPN Router with 4 Ethernet Ports

- 1 x 3-pin pluggable terminal block with lock for power supply

- 1 x7-pin pluggable terminal block with lock for serial and console port

- 1 x *Quick Start Guide* with download link of other documents or tools

*If any of the above items is missing or damaged, please contact your Robustel sales representative.

Optional accessories (sold separately):

- 3G/4G SMA cellular antenna (stubby/magnet optional)

Stubby antenna Magnet antenna

- Wall mounting kit

- 35 mm DIN rail mounting kit

- Ethernet cable

- AC/DC power adapter (12V DC, 1.5 A; EU/US/UK/AU plug optional)

1.3 Specifications

Cellular Interface

- Number of ports: 2 (MAIN + AUX)
- Connector: SMA, female
- SIM: 2 (3.0 V & 1.8 V)
- Standards: GSM/GPRS/EDGE/WCDMA/HSDPA/HSUPA/HSPA+/DC-HSPA+/TD-SCDMA/CDMA(CDMA 1X/EVDO)/FDD LTE/TDD LTE
  GSM: max DL/UL = 9.6/2.7 Kbps
  GPRS: max DL/UL = 86 Kbps
  EDGE: max DL/UL = 236.8 Kbps
  WCDMA/TD-SCDMA: max DL/UL = 2.8 Mbps/384 Kbps
  EVDO: max DL/UL = 5.4 Mbps/14.7 Kbps
  HSPA+: max DL/UL = 21/5.76 Mbps, fallback to 2G
  DC-HSPA+: max DL/UL = 42/5.76 Mbps, fallback to 2G
  FDD LTE: max DL/UL = 100/50 Mbps, fallback to 2G/3G
  TDD LTE: max DL/UL = 100/50 Mbps, fallback to 2G/3G

Ethernet Interface

- Number of ports: 4 x 10/100 ports(4 x LAN or 3 x LAN + 1 WAN)
- Magnet isolation protection: 1.5 KV

Wi-Fi Interface

- Number of ports: 1
- Connector: RP-SMA, male
- Standards: 802.11a/b/g/n, supporting AP and Client mode
- Frequency bands: 2.4 GHz
  5 GHz
- Security: Open, WPA, WEP
- Encryption: AES, TKIP, WEP64
- Data speed: Up to 150 Mbps

GPS/GLONASS Interface (Optional)

- Number of ports: 1
- Connector: SMA, female, with 50 ohms impedance
- Tracking sensitivity: GPS: greater than -148 dBm
  GLONASS: greater than -140 dBm
- Horizontal position accuracy: GPS: 2.5 m
  GLONASS: 4.0 m
- Protocol: NMEA-0183 V2.3

Serial Interface (Software selectable)

- Number of ports: 1 x RS-232 or 1 x RS-485
- Connector: 7-pin pluggable terminal block with lock, female
- Baud rate: 300 bps to 230400 bps

- Parameters: 8E1, 8O1, 8N1, 8N2, 7E2, 7O2, 7N2, 7E1
- RS-232: TxD, RxD, RTS, CTS, GND
- RS-485: Data+ (A), Data- (B)

Others

- Reset button : 1 x RST
- Expansion: 1 x USB 2.0 host up to 480 Mbps
- SD: 1 x Micro SD interface
- CLI: 1 x CLI interface
- LED indicators: 1 x RUN, 1 x PPP, 1 x USR, 1 x RSSI, 1 x NET, 1 x SIM
- Built-in: RTC, Watchdog, Timer

Software (Basic features of RobustOS)

- Network protocols: PPP, PPPoE, TCP, UDP, DHCP, ICMP, NAT, HTTP, HTTPs, DNS, ARP, NTP, SMTP, Telnet, VLAN, SSH2, DDNS, etc.
- VPN tunnel: IPsec, OpenVPN, GRE
- Firewall: DMZ, anti-DoS, Filtering (IP/Domain name/MAC address), Port Mapping, Access Control
- Management: Web, CLI, SMS
- Serial port: Transparent, TCP Client/Server, UDP, Modbus RTU Gateway

App Center

- Available apps for RobustOS: L2TP, PPTP, DMVPN, RobustVPN, VRRP, QoS, SNMP, Language, RobustLink
  *Request on demand. For more APPs please visit www.robustel.com.

Power Supply and Consumption

- Connector: 5 mm terminal block with lock
- Input voltage: 9~60V DC
- Power consumption: Idle: 100 mA@12 V
  Data link: 400 mA (peak) @12 V

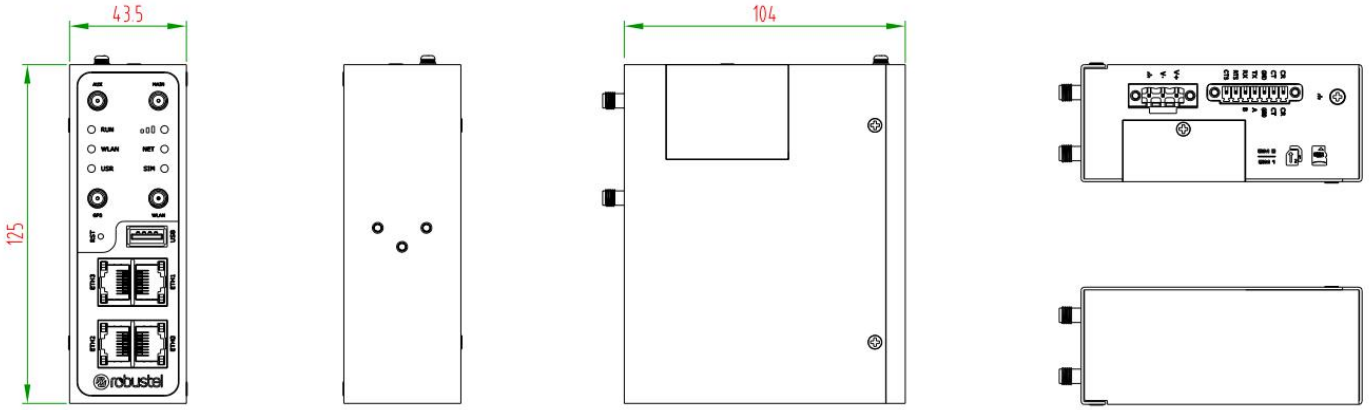
Physical Characteristics

- Ingress protection: IP30
- Housing & Weight: Metal, 500 g
- Dimensions: 125 x 104 x 43.5 mm
- Installations: Desktop or wall mounting or 35 mm DIN rail mounting

Approvals

- Regulatory: RCM, CE, EAC
- Application: IEC 60945 (Maritime Navigation and Radiocommunication Equipment and Systems)
- Environmental: RoHS2.0, WEEE
- EMI: EN 55032: 2012/AC: 2013 (CE & RE) Class B
- EMS: IEC 61000-4-2 (ESD)connect Level2; Air Level 3
  IEC 61000-4-3 (RS) Level 2
  IEC 61000-4-4 (EFT) Level 2
  IEC 61000-4-5 (Surge) Level 3
  IEC 61000-4-6 (CS) Level 2

1.4 Dimensions



Front View | Rear View | Side View | Top&Bottom View

1.5 Ordering Information

Model	R3000-Q3PB	R3000-Q4LB	R3000-QLB
Router Type	HSPA+ Router	LTE Router	Wireline Router
Air Interface	GSM/GPRS/EDGE/HSDPA/HSUPA/HSPA+	GSM/GPRS/EDGE/WCDMA/HSDPA/HSUPA/HSPA+/DC-HSPA+/TD-SCDMA/CDMA (CDMA 1X/EVDO)/FDD LTE/TDD LTE	--
Frequency Bands 4G*	--	AU: B1/B3/B5/B7/B8/B28, B40 EU: B1/B3/B7/B8/B20/B28/B31, B38/B40 US: B2/B4/B5/B13/B17/B25, B41 JP: B1/B3/B8/B9/B18/B19/B21/B28, B41 CN: B1/B3, B38/B39/B40/B41	--
3G	B1/B2/B4(AWS)/B5/B8/B19	WCDMA/HSDPA/HSUPA/HSPA+/DC-HSPA+: B1/B2/B5/B6/B8/B9/B19 TD-SCDMA: B34/B39 CDMA (CDMA 1X/EVDO): R0/A BC0/BC1/BC10	--
2G	850/900/1800/1900 MHz	850/900/1800/1900 MHz	--
Operating Environment	-40 to +75 °C 5 to 95% RH	-40 to +75 °C 5 to 95% RH	-40 to +75 °C 5 to 95% RH

*For more information about 4G frequency bands in different countries, please contact your Robustel sales representative.

1.6 Warning

WARNING – EXPLOSION HAZAD. DO NOT REMOVE OR REPLACE WHILE CIRCUIT IS LIVE UNLESS THE AREA IS FREE OF

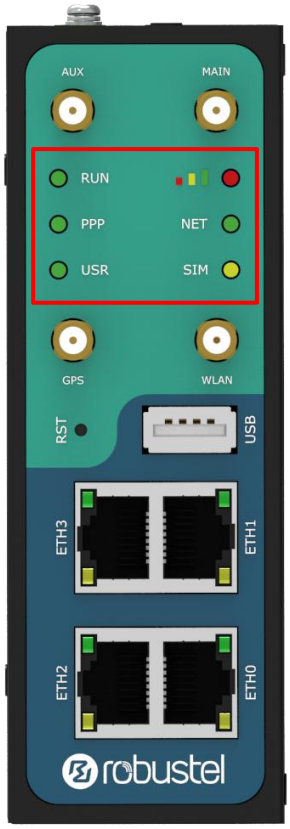
IGNITIBLE CONCENTRATIONS.

AVERTISSEMENT — RISQUE D ' EXPLOSION. NE PAS RETIRER OU REMPLACER LORSQUE LE CIRCUIT EST SOUS TENSION, À MOINS QUE LE MILIEU SOIT LIBRE DE SUBSTANCES INFLAMMABLES CONCENTRÉES.

Chapter 2 Hardware Installation

2.1 LED Indicators

The R3000 Quad has been designed to be placed on a desktop. Below is the front view of the R3000 Quad.

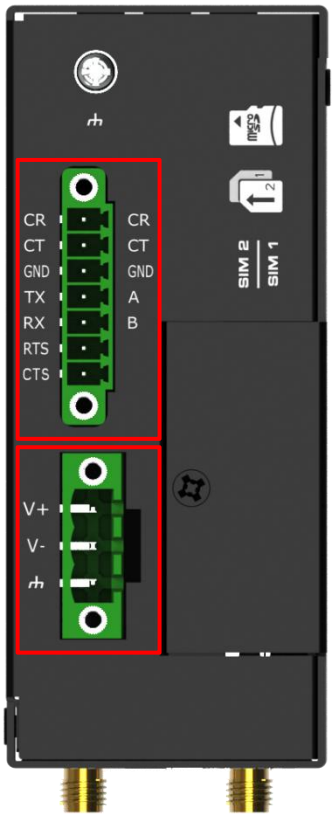


Name	Color	Status	Description
RUN	Green	On, fast blinking (250 mSec blink time)	Router is powered on (System is initializing)
		On, blinking (500 mSec blink time)	Router starts operating
		Off	Router is powered off
PPP	Green	On, solid	Link connection is working
		Off	Link connection is not working
USR-OpenVPN	Green	On, solid	OpenVPN connection is established
		Off	OpenVPN connection is not established
USR-IPsec	Green	On, solid	IPsec connection is established
		Off	IPsec connection is not established
USR-WiFi	Green	On, solid	WiFi is enabled and working properly
		Off	WiFi is disabled or not working properly

	Green	On, solid	High Signal strength (21-31) is available
	Yellow	On, solid	Medium Signal strength (11-20) is available
	Red	On, solid	Low Signal strength (1-10) is available
	/	Off	No signal
NET	Green	On, solid	Connection to 4G network is established
	Yellow	On, solid	Connection to 3G network is established
	Red	On, solid	Connection to 2G network is established
	/	Off	Connection to network is not established or establishing
SIM	Green	On, blinking	Backup card is being used
		Off	Main card is being used

Note: You can choose the display type of USR LED. For more details, please refer to **3.28 Service > Advanced**.

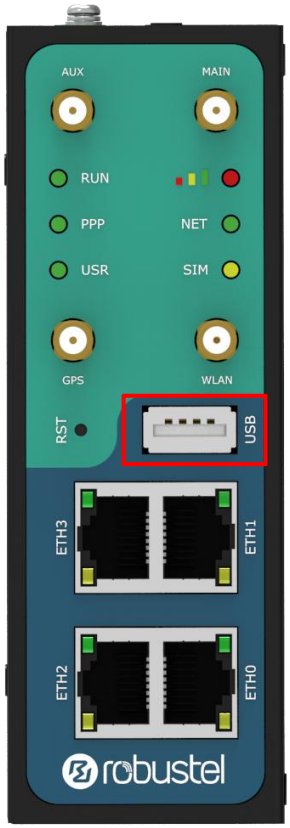
2.2 PIN Assignment



PIN	Debug	RS-232	RS-485	Direction
1	CR	--	--	Router ← Device
2	CT	--	--	Router → Device
3	GND	GND	GND	--
4	--	TXD	Data+(A)	Router → Device
5	--	RXD	Data+(B)	Router ← Device
6	--	RTS	--	Router → Device
7	--	CTS	--	Router ← Device

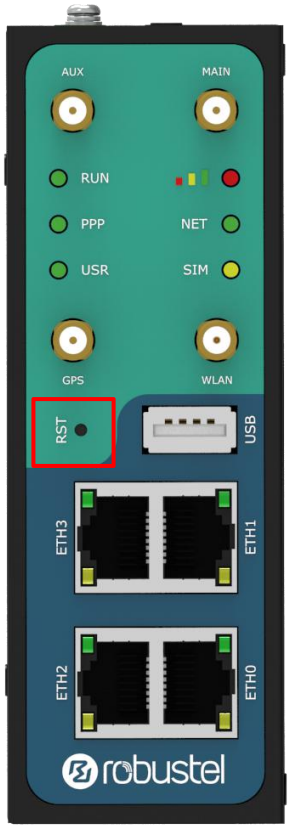
PIN	Polarity
8	Positive
9	Negative
10	GND

2.3 USB Interface



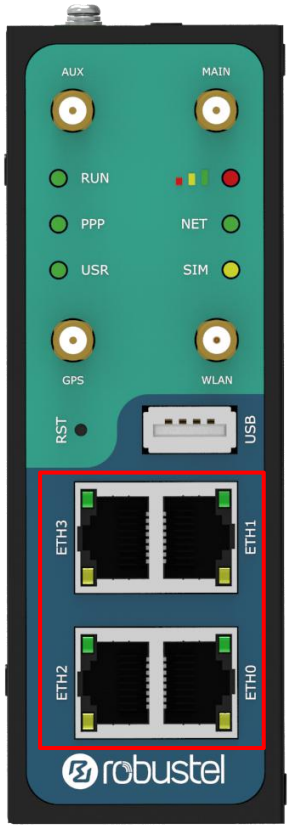
Function	Operation
Firmware upgrade	USB interface is used for batch firmware upgrading, but cannot be used for sending or receiving data from slave devices which connected to it. You can insert a USB storage device into the router's USB interface, such as a U disk or a hard disk. If there have a supported configuration file or a router firmware in this USB storage device, the router will automatically update the configuration file or the firmware. For more details, see **3.11 Interface > USB**.

2.4 Reset Button



Function	Operation
Reboot	Press and hold the RST button for 5 seconds under the operating status.
Restore to factory default settings	Wait for 5 seconds after powering up the router, press and hold the RST button until all six LEDs start blinking one by one, and release the button to return the router to factory defaults.

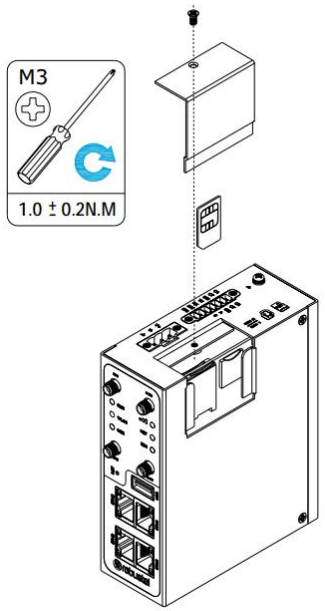
2.5 Ethernet Port



R3000 Quad Router has four Ethernet port with two LED indicators. The yellow one is link indicator and the green one is speed indicator. For details about status, see the table below.

Indicator	Status	Description
Link indicator	On, solid	Connection is established
	On, blinking	Data is being transferred
	Off	Connection is not established
Speed indicator	On, solid	100 Mbps mode
	Off	10 Mbps mode

2.6 Insert or Remove SIM Card/Micro SD Card



Insert or remove the SIM card and SD card as shown in the following steps.

- **Insert SIM card/Micro SD card**

1. Make sure router is powered off.
2. To remove slot cover, loosen the screws associated with the cover by using a screwdriver and then find the SIM card slot/Micro SD card slot.
3. To insert SIM card/Micro SD card, press the card with finger until you hear a click and then tighten the screws associated with the cover by using a screwdriver.
4. To put back the cover and tighten the screws associated with the cover by using a screwdriver.

- **Remove SIM card/Micro SD card**

1. Make sure router is powered off.
2. To remove slot cover, loosen the screws associated with the cover by using a screwdriver and then find the SIM card slot/Micro SD card slot.
3. To remove SIM card/Micro SD card, press the card with finger until it pops out and then take out the card.
4. To put back the cover and tighten the screws associated with the cover by using a screwdriver.

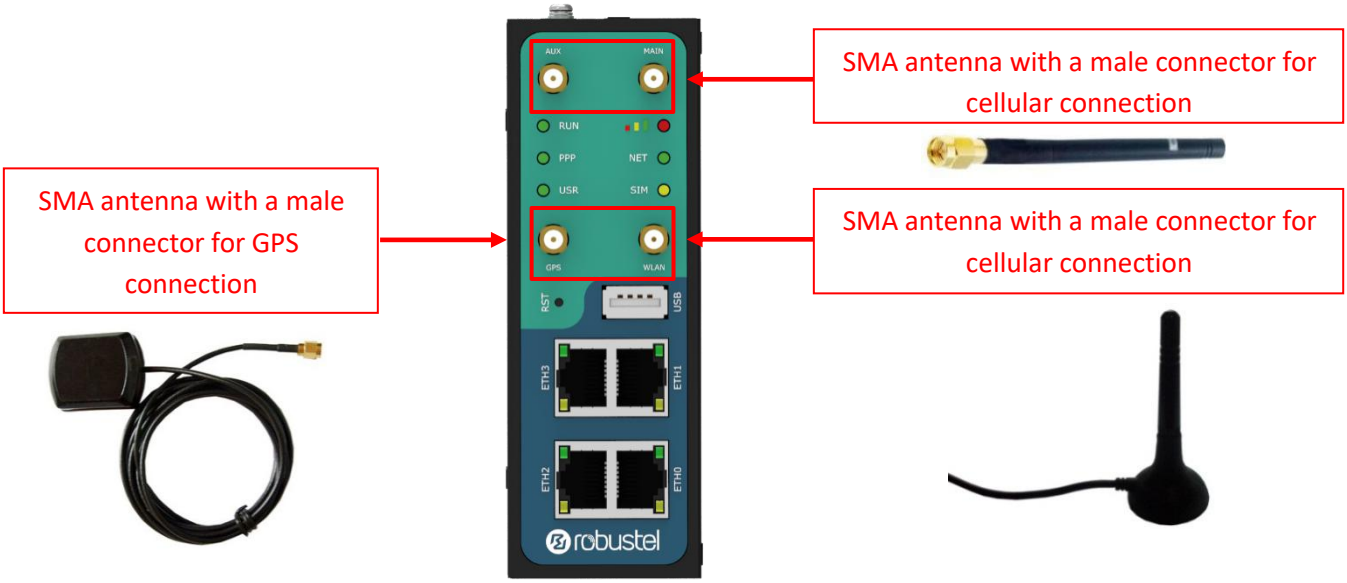
Note:

1. Recommended torque for inserting is 1.0 N.m, and the maximum allowed is 1.2 N.m.
2. Use the specific card when the device is working in extreme temperature (temperature exceeding 40℃), because the regular card for long-time working in harsh environment will be disconnected frequently.
3. Do not forget to twist the cover tightly to avoid being stolen.
4. Do not touch the metal of the card surface in case information in the card will lose or be destroyed.
5. Do not bend or scratch the card.
6. Keep the card away from electricity and magnetism.
7. Make sure router is powered off before inserting or removing the card.

2.7 Attach External Antenna (SMA Type)

Attach an external SMA antenna to the router's connector and twist tightly. Make sure the antenna is within the correct frequency range provided by the ISP and with 50 Ohm impedance.

Note: Recommended torque for tightening is 0.35 N.m.



2.8 Mount the Router

The router can be placed on a desktop or mounted to a wall or a 35 mm DIN rail.

Note:

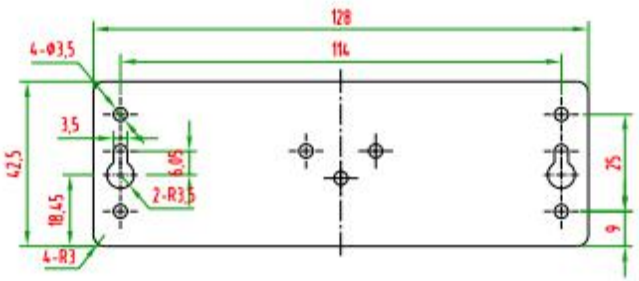
When used, the device needs a suitable environment.

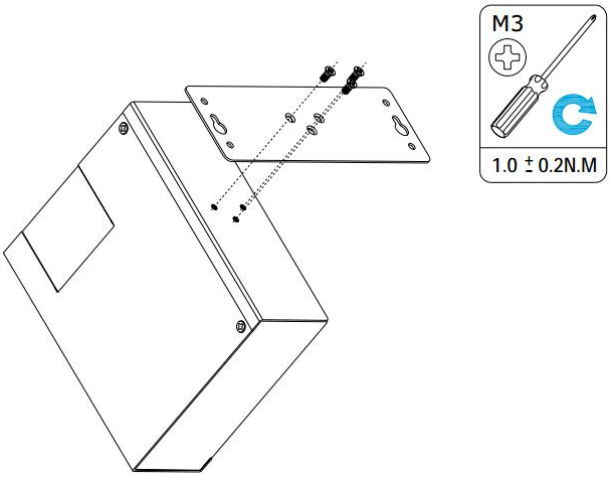
1. If indoors, it needs to be provided an indoor enclosure.
2. If outdoors, it needs to be provided a rain proof enclosure.

Two methods for mounting the router

1. Wall mounting

   Wall mounting kit size (measured in mm)



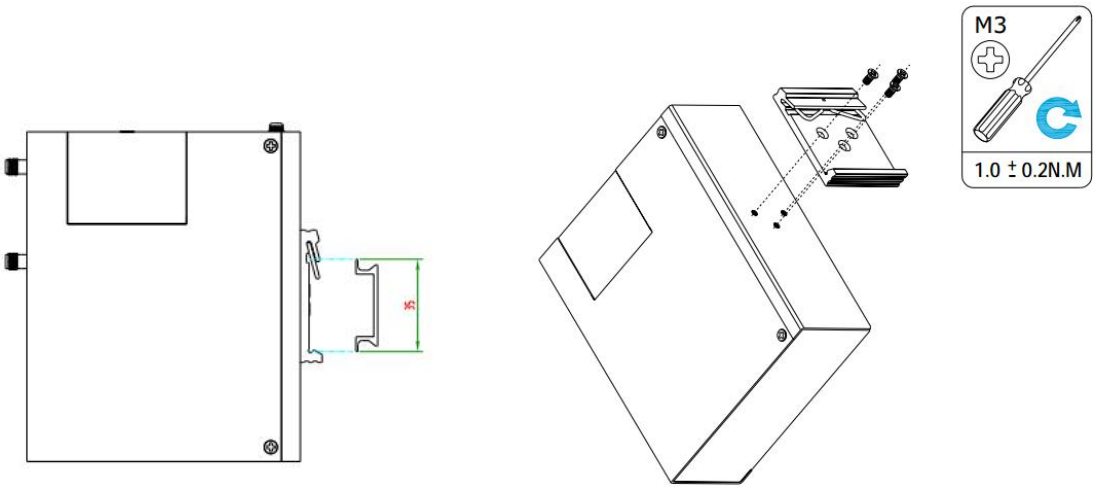


Use 3 pcs of M3*4 flat head Phillips screws to fix the wall mounting kit to the router, and then use 2 pcs of M3 drywall screws to mount the router associated with the wall mounting kit on the wall.

Note: Recommended torque for mounting is 1.0 N.m, and the maximum allowed is 1.2 N.m.

2. DIN rail mounting

DIN rail size (measured in mm)

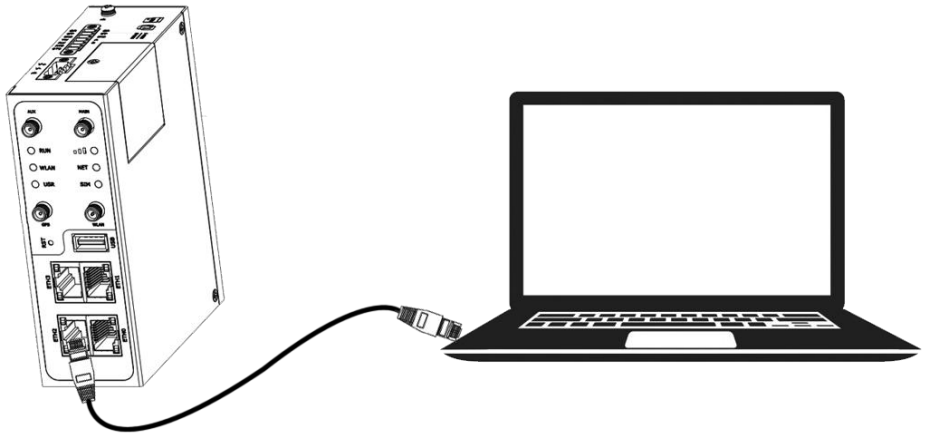


Use 3 pcs of M3*6 flat head Phillips screws to fix the DIN rail to the router, and then hang the DIN rail on the mounting bracket. It is necessary to choose a standard bracket.

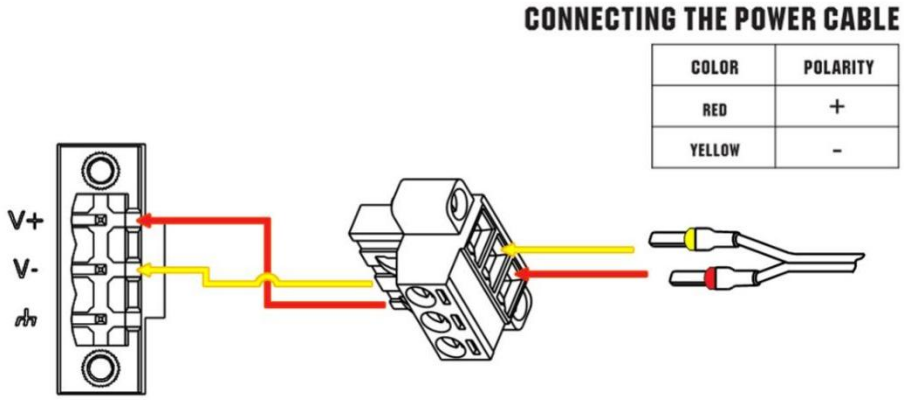
Note: Recommended torque for mounting is 1.0 N.m, and the maximum allowed is 1.2 N.m.

2.9 Connect the Router to a Computer

Connect an Ethernet cable to any port marked ETH0~ETH3 at the bottom of the router, and connect the other end of the cable to your computer.



2.10 Power Supply



R3000 Quad router supports reverse polarity protection, but always refers to the figure above to connect the power adapter correctly. There are two cables associated with the power adapter. Following to the color of the head, connect the cable marked red to the positive pole through a terminal block, and connect the yellow one to the negative in the same way.

Note: The range of power voltage is 9 to 60V DC.

Chapter 3 Initial Configuration

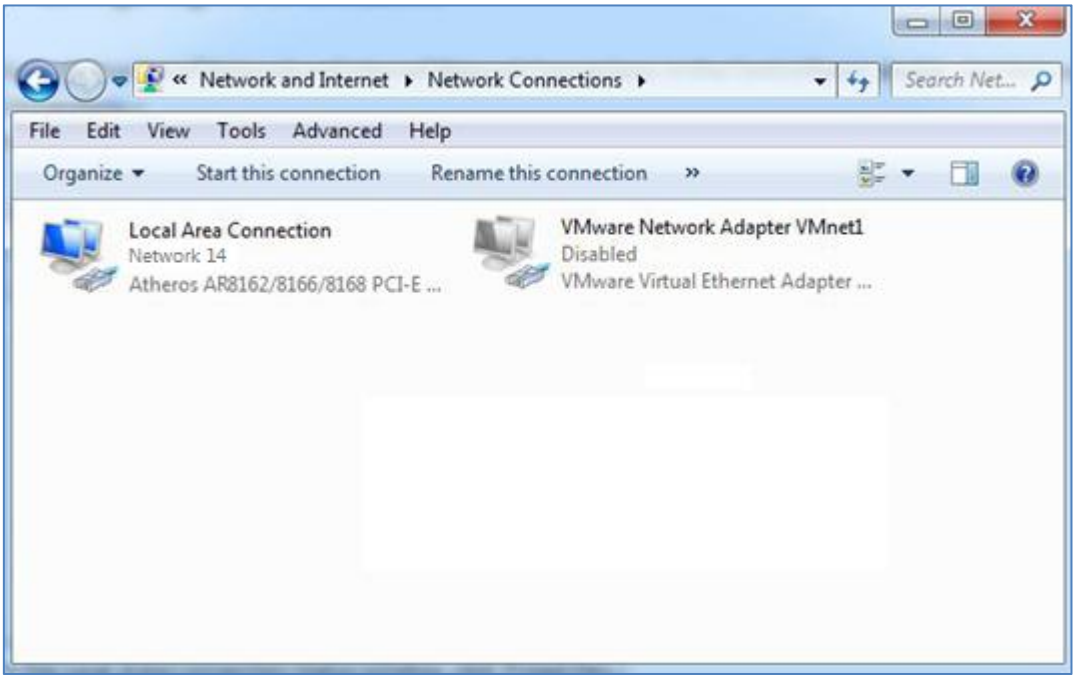
The router can be configured through your web browser that including IE 8.0 or above, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. It provides an easy and user-friendly interface for configuration. There are various ways to connect the router, either through an external repeater/hub or connect directly to your PC. However, make sure that your PC has an Ethernet interface properly installed prior to connecting the router. You must configure your PC to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. If you encounter any problems accessing the router web interface, it is advisable to uninstall your firewall program on your PC, as this tends to cause problems accessing the IP address of the router.

3.1 Configure the PC

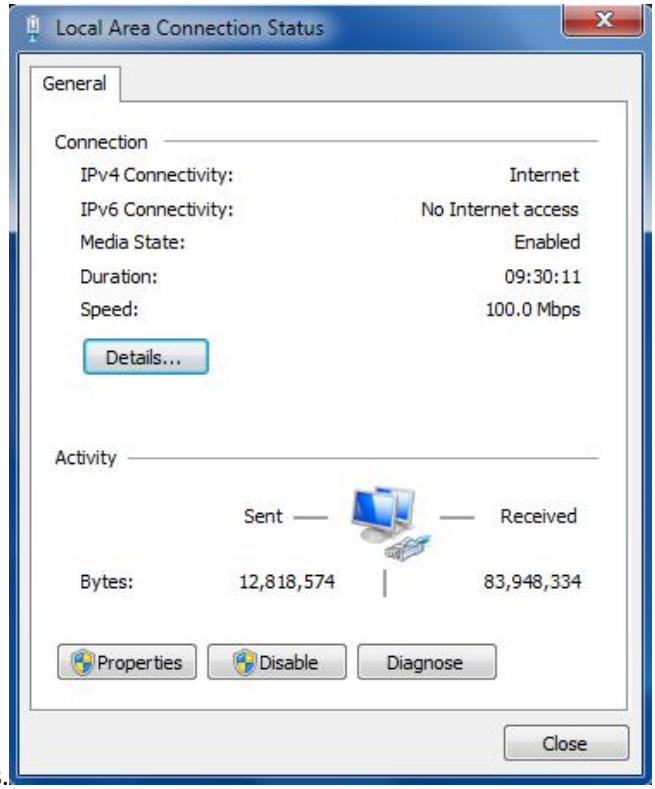
There are two methods to get IP address for the PC, one is to obtain an IP address automatically from "Local Area Connection", and another is to configure a static IP address manually within the same subnet of the router. Please refer to the steps below.

Here take **Windows 7** as example, and the configuration for windows system is similar.

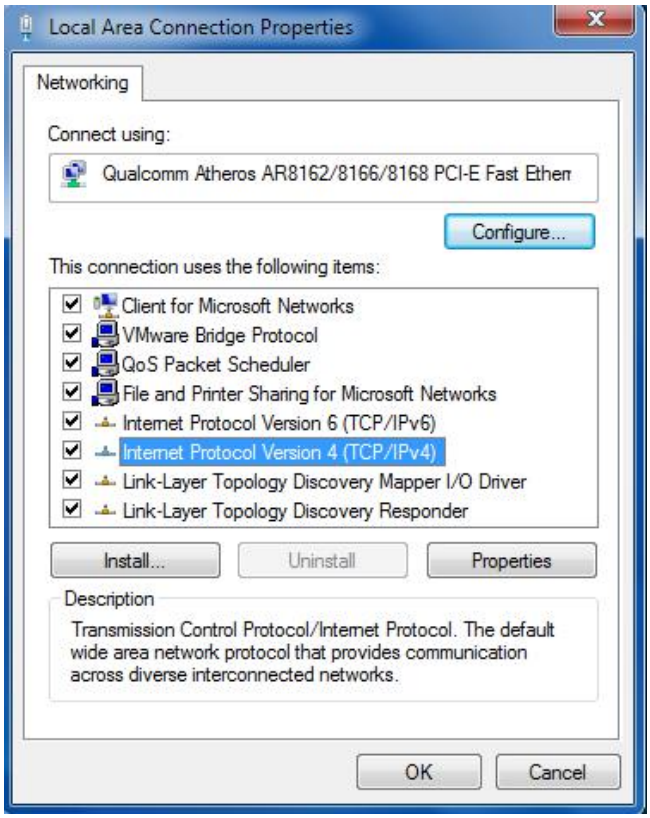
1. Click **Start > Control panel**, double-click **Network and Sharing Center**, and then double-click **Local Area Connection**.



2. Click **Properties** in the window of **Local Area Connection Status**.

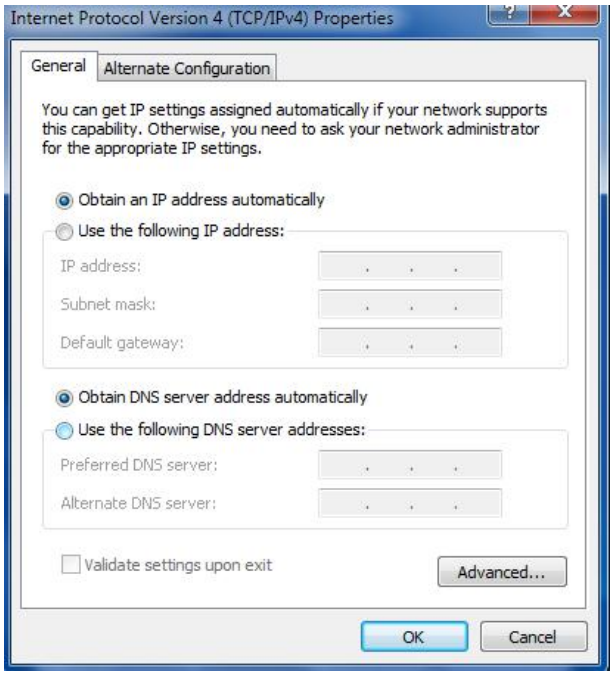


3. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



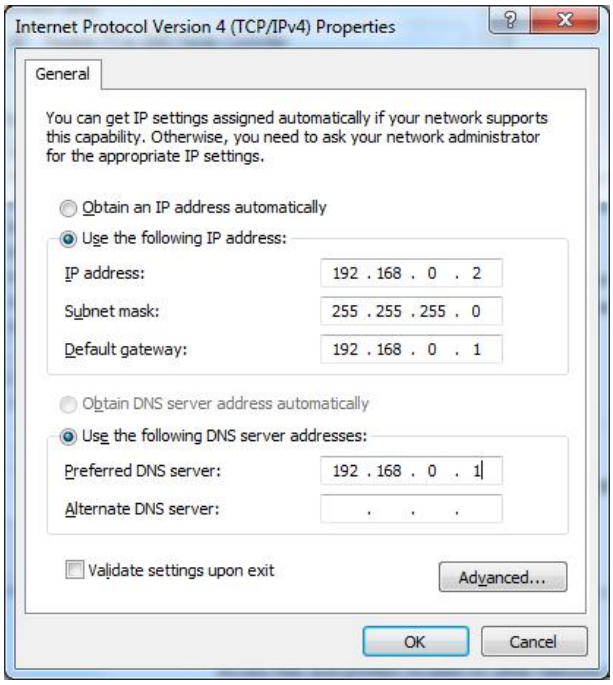
4. Two ways for configuring the IP address of PC.

Obtain an IP address automatically:



Use the following IP address:

(Configured a static IP address manually within the same subnet of the router)



5. Click **OK** to finish the configuration.

3.2 Factory Default Settings

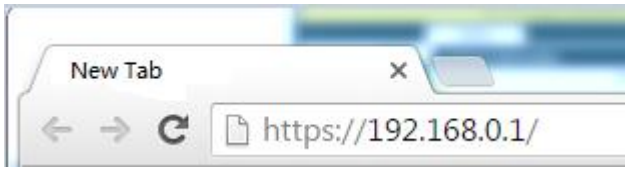
Before configuring your router, you need to know the following default settings.

Item	Description
Username	admin
Password	admin
ETH0	192.168.0.1/255.255.255.0, LAN mode
ETH1	192.168.0.1/255.255.255.0, LAN mode
ETH2	192.168.0.1/255.255.255.0, LAN mode
ETH3	192.168.0.1/255.255.255.0, LAN mode
DHCP Server	Enabled

3.3 Log in the Router

To log in to the management page and view the configuration status of your router, please follow the steps below.

1. On your PC, open a web browser such as Internet Explorer, Google and Firebox, etc.
2. From your web browser, type the IP address of the router into the address bar and press enter. The default IP address of the router is 192.168.0.1, though the actual address may vary.

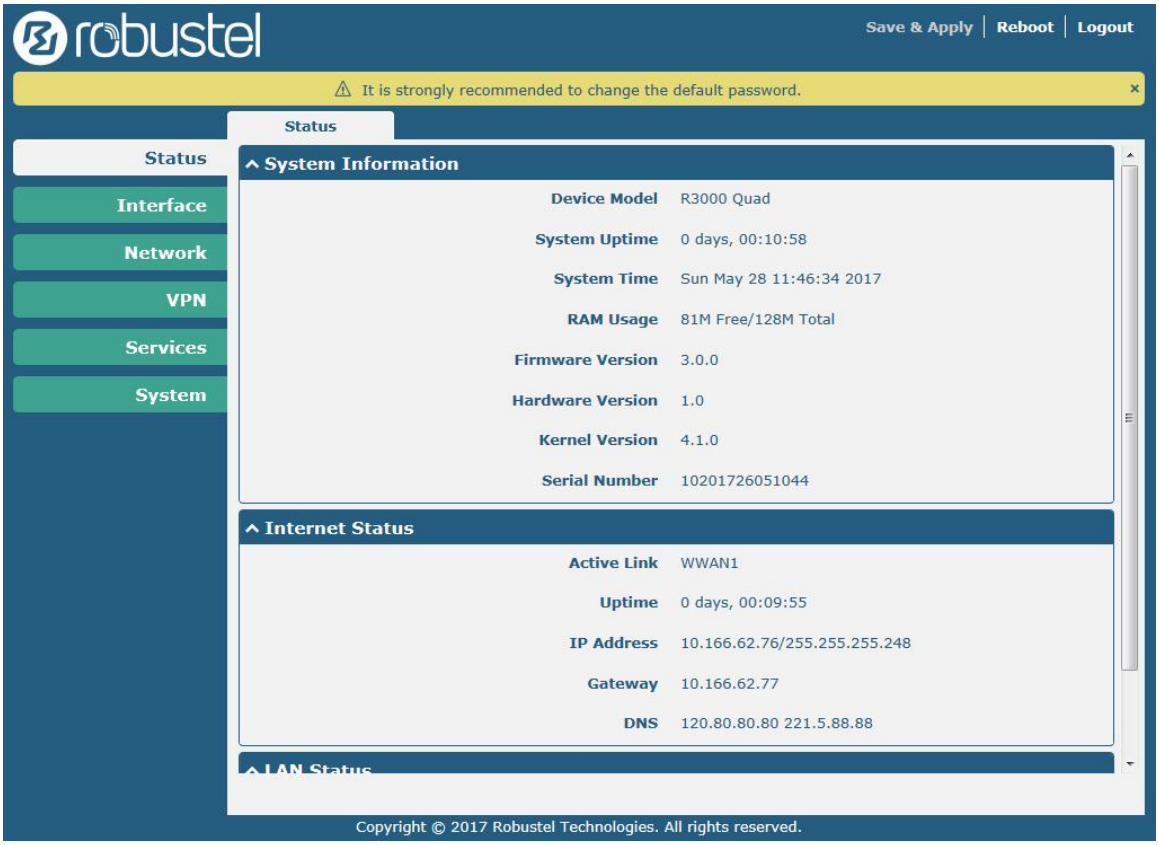


3. In the login page, enter the username and password, choose language and then click **LOGIN**. The default username and password are “admin”.

   Note: If enter the wrong username or password over six times, the login web will be locked for 5 minutes.

3.4 Control Panel

After logging in, the home page of the R3000 Quad Router's web interface is displayed, for example.



Using the original password to log in the router, the page will pop up the following tab

It is strongly recommended for security purposes that you change the default username and/or password. To change your username and/or password, see **3.34 System > User Management**.

Control Panel		
Item	**Description**	**Button**
Save & Apply	Click to save the current configuration into router's flash and apply the modification on every configuration page, to make the modification taking effect.	Save & Apply
Reboot	Click to reboot the router. If the Reboot button is yellow, it means that some completed configurations will take effect only after reboot.	Reboot
Logout	Click to log the current user out safely. After logging out, it will switch to login page. Shut down web page directly without logout, the next one can login web on this browser without a password before timeout.	Logout
Submit	Click to save the modification on current configuration page.	Submit
Cancel	Click to cancel the modification on current configuration page.	Cancel

Note: The steps of how to modify configuration are as bellow:

1. Modify in one page;
2. Click **Submit** under this page;
3. Modify in another page;
4. Click **Submit** under this page;
5. Complete all modification;
6. Click **Save & Apply**.

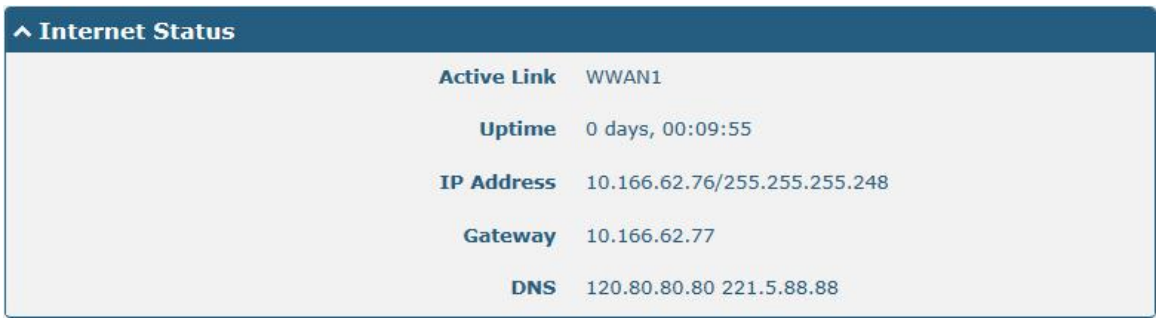
3.5 Status

This page allows you to view the System Information, Internet Status and LAN Status of your router.

System Information

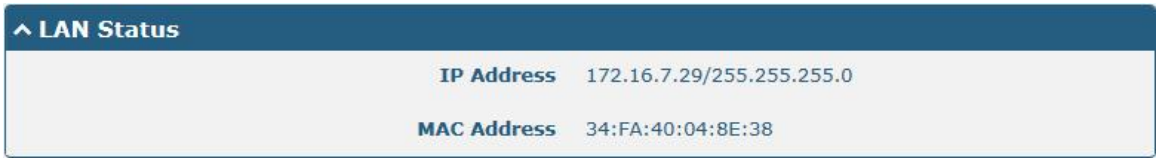
System Information	
Item	**Description**
Device Model	Show the model name of your device.
System Uptime	Show the current amount of time the router has been connected.
System Time	Show the current system time.
RAM Usage	Show the free memory and the total memory.
Firmware Version	Show the firmware version running on the router.
Hardware Version	Show the current hardware version.
Kernel Version	Show the current kernel version.
Serial Number	Show the serial number of your device.

Internet Status



Internet Status	
Item	**Description**
Active Link	Show the current active link.
Uptime	Show the current amount of time the link has been connected.
IP Address	Show the IP address of current link.
Gateway	Show the gateway address of the current link.
DNS	Show the current primary DNS server and secondary server.

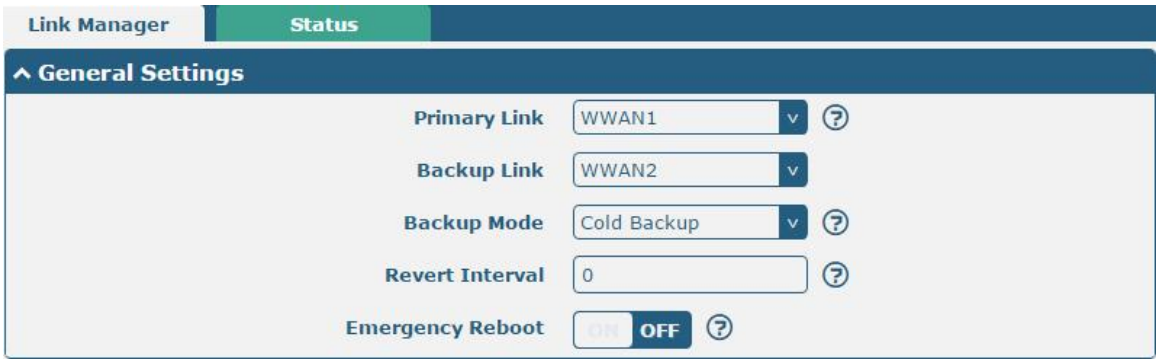
LAN Status



LAN Status	
Item	**Description**
IP Address	Show the IP address and the Netmask of the router.
MAC Address	Show the MAC address of the router.

3.6 Interface > Link Manager

This section allows you to setup the link connection.



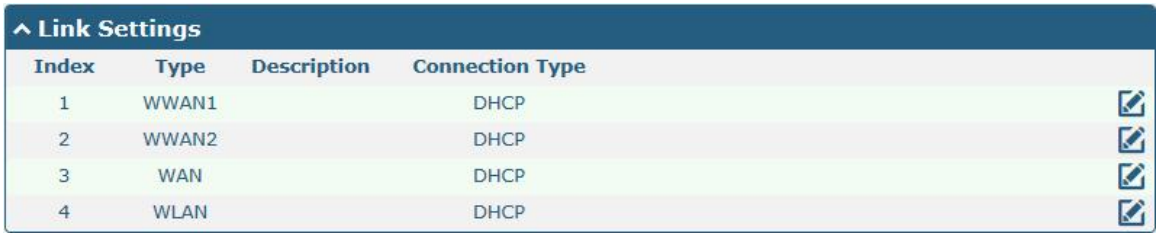
General Settings @ Link Manager		
Item	**Description**	**Default**
Primary Link	Select from "WWAN1", "WWAN2", "WAN" or "WLAN". • WWAN1: Select to make SIM1 as the primary wireless link • WWAN2: Select to make SIM2 as the primary wireless link • WAN: Select to make WAN as the primary wire link • WLAN: Select to make WLAN as the primary wireless link **Note:** WLAN link is available only if enable WiFi as Client mode, please refer to **3.10 Interface > WiFi**.	WWAN1
Backup Link	Select from "None", "WWAN1", "WWAN2", "WAN" or "WLAN". • None: Do not select any backup link • WWAN1: Select to make SIM1 as backup wireless link • WWAN2: Select to make SIM2 as backup wireless link • WAN: Select to make WAN as the primary wire link • WLAN: Select to make WLAN as the primary wireless link **Note:** WLAN link is available only if enable WiFi as Client mode, please refer to **3.10 Interface > WiFi**.	WWAN2
Backup Mode	Select from "Cold Backup", "Warm Backup" or "Load Balancing". • Cold Backup: The inactive link is offline on standby • Warm Backup: The inactive link is online on standby • Load Balancing: Use two links simultaneously **Note**: R3000 Quad do not support warm backup and load balancing in the situation of two WWAN links.	Cold Backup
Revert Interval	Specify the number of minutes that elapses before the primary link is checked if a backup link is being used in cold backup mode. 0 means disable checking. **Note:** Revert interval is available only under the cold backup mode.	0
Emergency Reboot	Click the toggle button to enable/disable this option. Enable to reboot the whole system if no links available.	OFF

Note: Click for help.

Link Settings allows you to configure the parameters of link connection, including WWAN1/WWAN2, WAN and

WLAN.

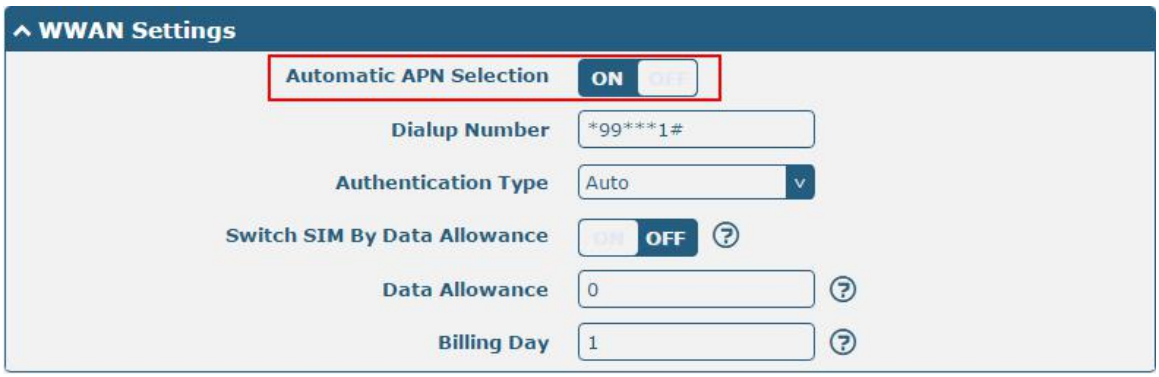
It is recommended to enable Ping detection to keep the router always online. The Ping detection increases the reliability and also costs the data traffic.



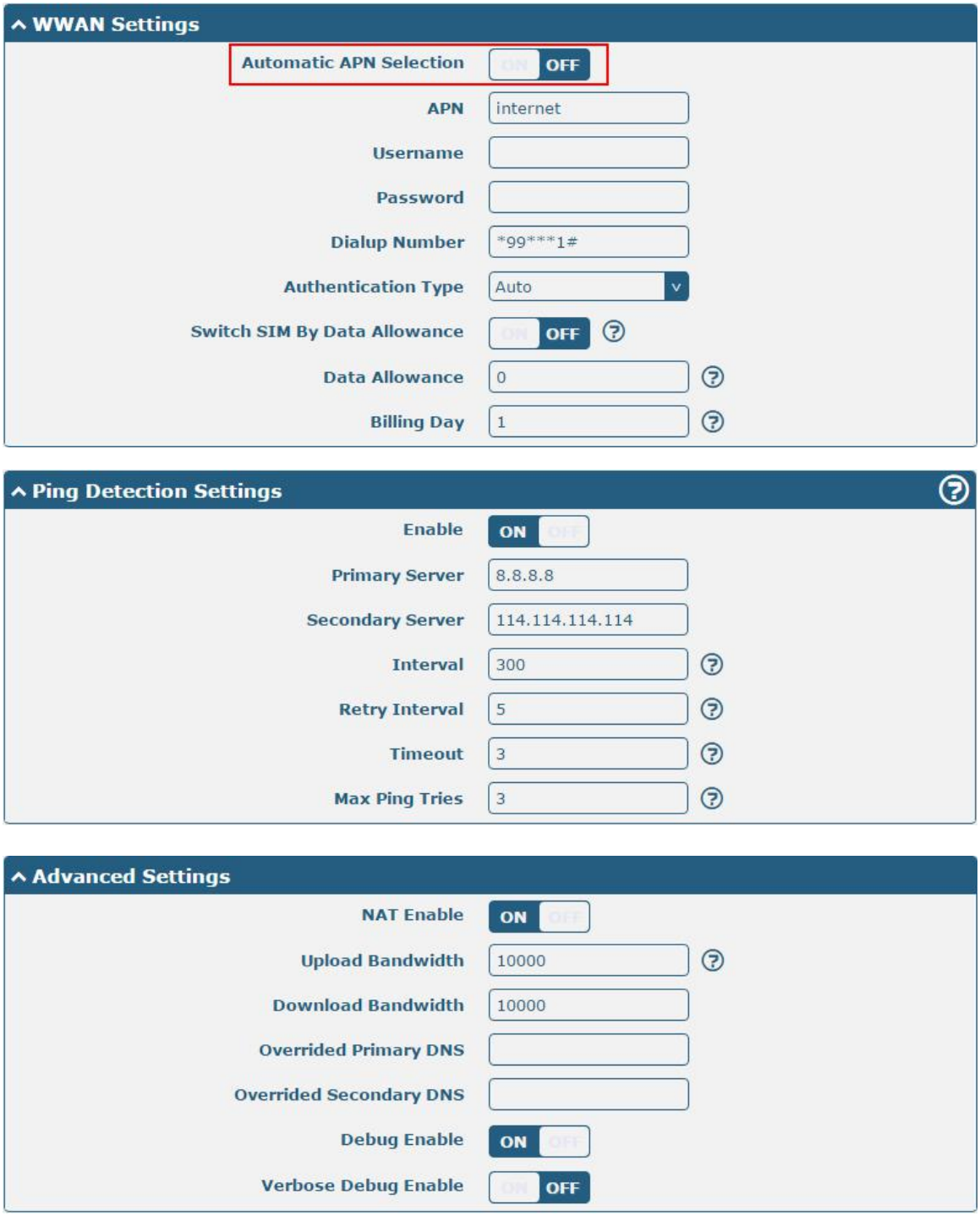
Click on the right-most of WWAN1/WWAN2 to enter the configuration window.

WWAN1/WWAN2

The window is displayed as below when enabling the “Automatic APN Selection” option.



The window is displayed as below when disabling the “Automatic APN Selection” option.



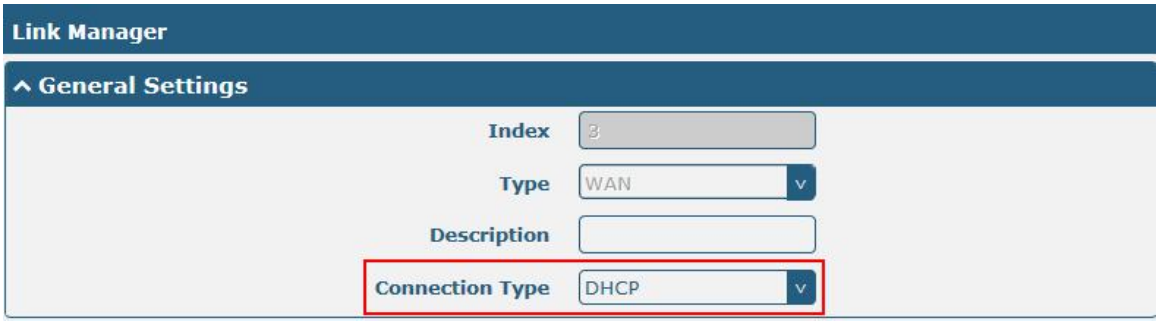
Link Settings (WWAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WWAN1
Description	Enter a description for this link.	Null
WWAN Settings		

Link Settings (WWAN)		
Item	**Description**	**Default**
Automatic APN Selection	Click the toggle button to enable/disable the "Automatic APN Selection" option. After enabling, the device will recognize the access point name automatically. Alternatively, you can disable this option and manually add the access point name.	ON
APN	Enter the Access Point Name for cellular dial-up connection, provided by local ISP.	internet
Username	Enter the username for cellular dial-up connection, provided by local ISP.	Null
Password	Enter the password for cellular dial-up connection, provided by local ISP.	Null
Dialup Number	Enter the dialup number for cellular dial-up connection, provided by local ISP.	*99***1#
Authentication Type	Select from "Auto", "PAP" or "CHAP" as the local ISP required.	Auto
Switch SIM By Data Allowance	Click the toggle button to enable/disable this option. After enabling, it will switch to another SIM when the data limit reached. **Note**: Only used for dual SIM backup.	OFF
Data Allowance	Set the monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will be displayed in **Interface > Link Manager > Status > WWAN Data Usage Statistics**. 0 means disable data traffic record.	0
Billing Day	Specify the monthly billing day. The data traffic statistics will be recalculated from that day.	1
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.114.114
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advanced Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
Upload Bandwidth	Set the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Set the download bandwidth used for QoS, measured in kbps.	10000
Overrided Primary DNS	Override primary DNS will override the automatically obtained DNS.	Null
Overrided Secondary DNS	Override secondary DNS will override the automatically obtained DNS.	Null

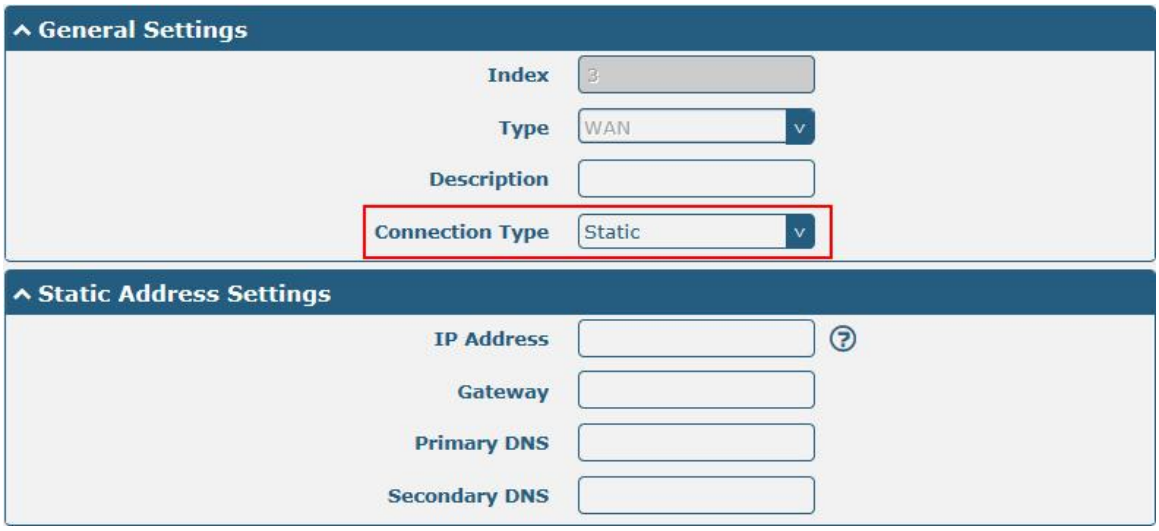
Link Settings (WWAN)		
Item	**Description**	**Default**
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

WAN

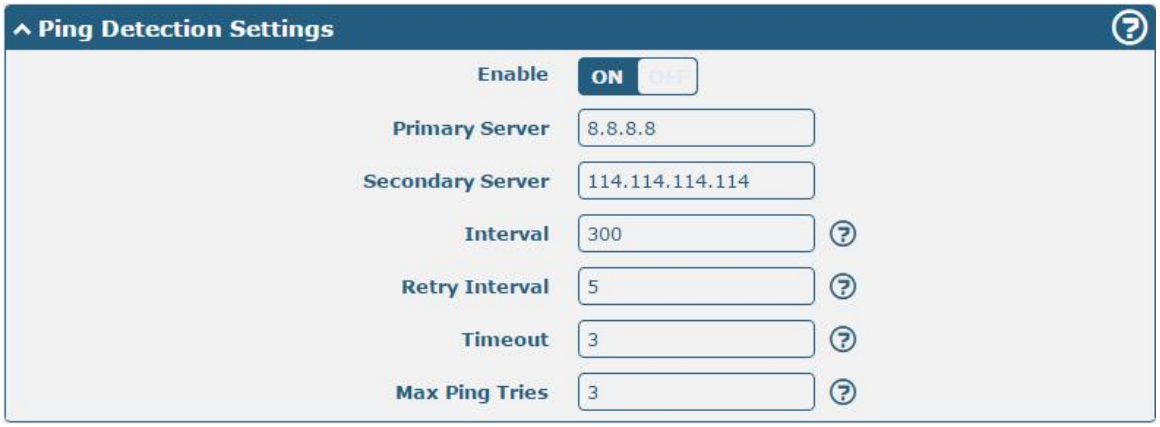
Router will obtain IP automatically from DHCP server if choosing “DHCP” as connection type. The window is displayed as below.

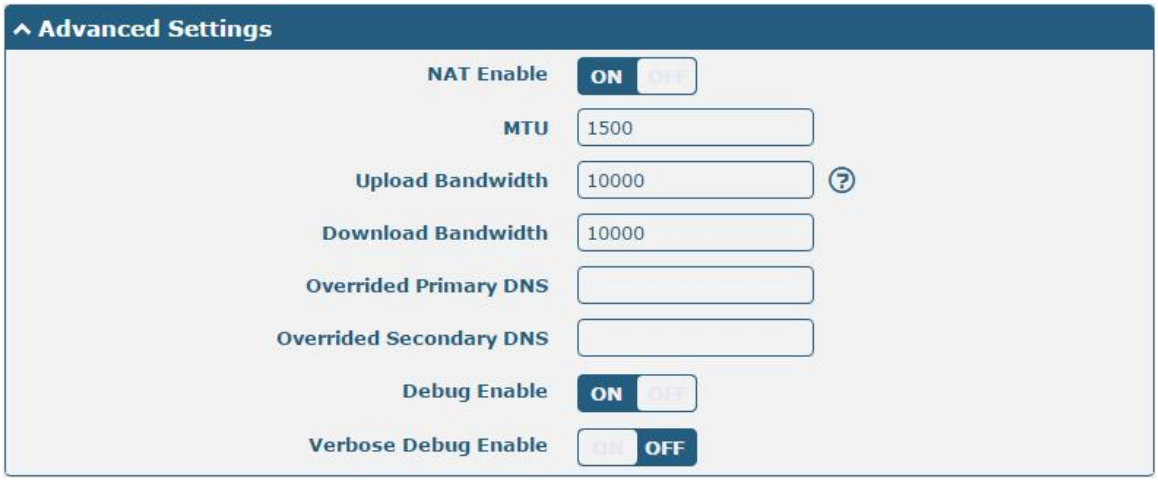


The window is displayed as below when choosing “Static” as the connection type.



The window is displayed as below when choosing “PPPoE” as the connection type.





Link Settings (WAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WAN
Description	Enter a description for this link.	Null
Connection Type	Select from “DHCP”, “Static” or “PPPoE”.	DHCP
Static Address Settings		
IP Address	Set the IP address with Netmask which can access the Internet. IP address with Netmask, e.g. 192.168.1.1/24	Null
Gateway	Set the gateway of the IP address in WAN port.	Null
Primary DNS	Set the primary DNS.	Null
Secondary DNS	Set the secondary DNS.	Null
PPPoE Settings		

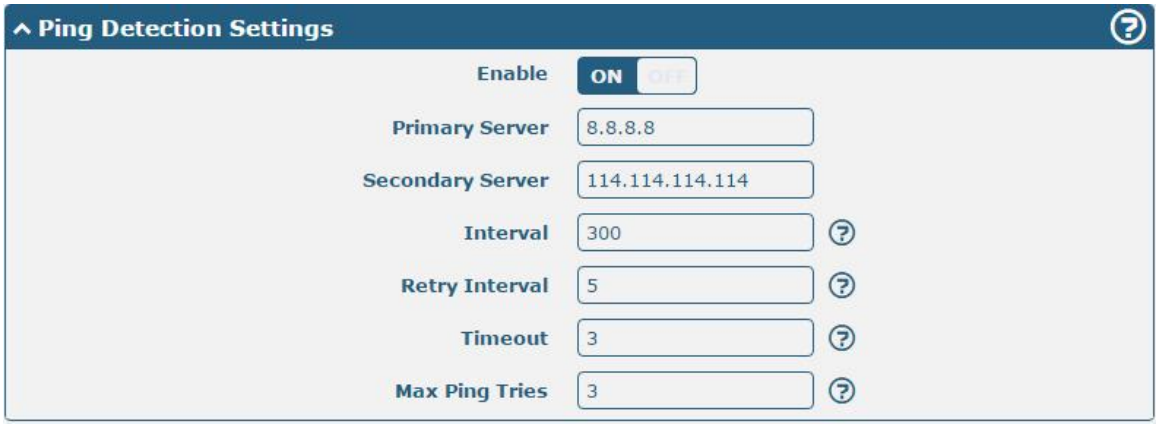
Username	Enter the username provided by your Internet Service Provider.	Null
Password	Enter the password provided by your Internet Service Provider.	Null
Authentication Type	Select from “Auto”, “PAP” or “CHAP” as the local ISP required.	Auto
PPP Expert Options	Enter the PPP Expert options used for PPPoE dialup. You can enter some other PPP dial strings in this field. Each string can be separated by a semicolon.	Null
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.114.114
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advanced Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Overrided Primary DNS	Override primary DNS will override the automatically obtained DNS.	Null
Overrided Secondary DNS	Override secondary DNS will override the automatically obtained DNS.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

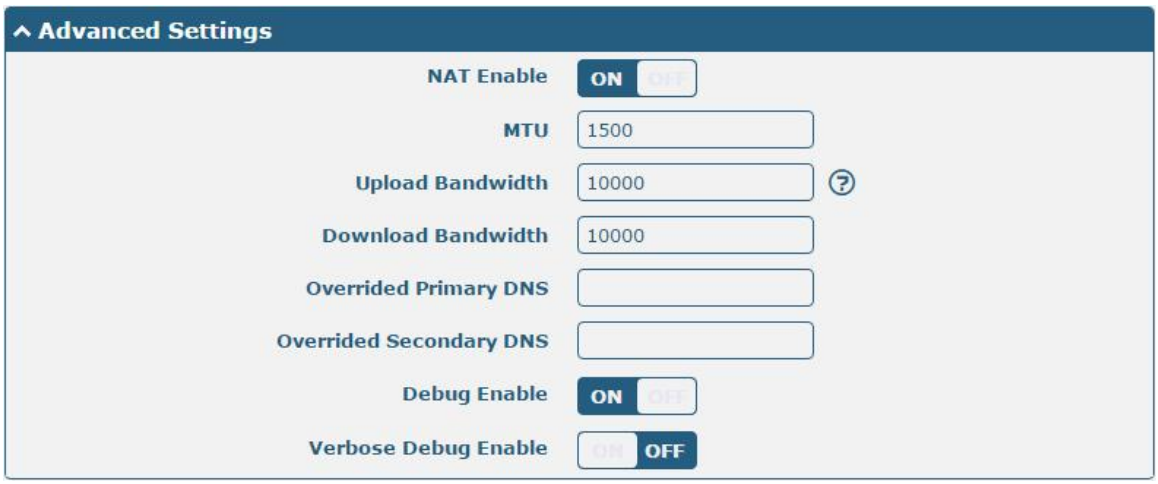
WLAN

Router will obtain IP automatically from the WLAN AP if choosing “DHCP” as the connection type. The specific parameter configuration of SSID is shown as below.

The window is displayed as below when choosing “Static” as the connection type.

R3000 Quad Router does not support the **PPPoE** WLAN Connection Type.





Link Settings (WLAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WLAN
Description	Enter a description for this link.	Null
Connection Type	Select from “DHCP” or “Static”.	DHCP
WLAN Settings		
SSID	Enter a 1-32 characters SSID which your router wants to connect. SSID (Service Set Identifier) is the name of your wireless network.	router
Connect to Hidden SSID	Click the toggle button to enable/disable this option. When router works as Client mode and needs to connect any access point which has hidden SSID, you need to enable this option.	OFF
Password	Enter an 8-63 characters password of the access point which your router wants to connect.	Null
Static Address Settings		
IP Address	Enter the IP address with Netmask which can access the Internet, e.g. 192.168.1.1/24	Null
Gateway	Enter the IP address of WiFi AP.	Null
Primary DNS	Set the primary DNS.	Null
Secondary DNS	Set the secondary DNS.	Null

Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.114.114
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advance Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Overrided Primary DNS	Override primary DNS will override the automatically obtained DNS.	Null
Overrided Secondary DNS	Override secondary DNS will override the automatically obtained DNS.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

Status

This page allows you to view the status of link connection and clear the monthly data usage statistics.

Click the right-most button ••• to select the connection status of the current link.

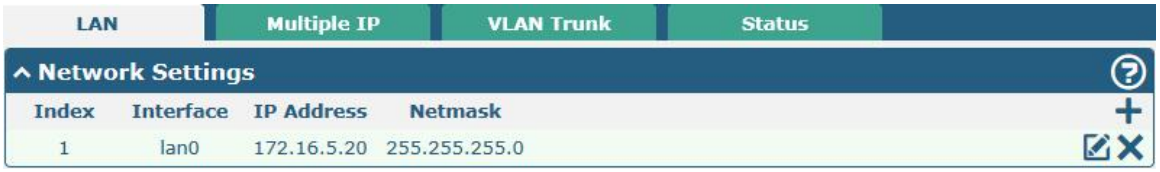
Click the row of the link, and it will show the details information of the current link connection under the row.

Click the **Clear** button to clear SIM1 or SIM2 monthly data traffic usage statistics. Data statistics will be displayed only if enable the Data Allowance function in **Interface > Link Manager > Link Settings > WWAN Settings > Data Allowance**.

3.7 Interface > LAN

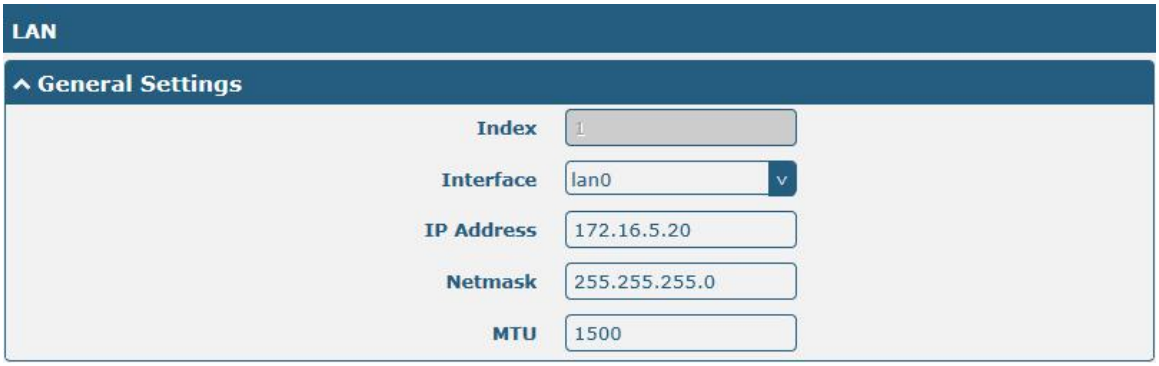
This section allows you to set the related parameters for LAN port. There are four LAN ports on R3000 Quad Router, including ETH0~ETH3. The ETH0~ETH3 can freely choose from lan0~lan3, but at least one LAN port must be assigned as lan0. The default settings of ETH0~ETH3 are lan0 and their default IP are 192.168.0.1/255.255.255.0.

LAN



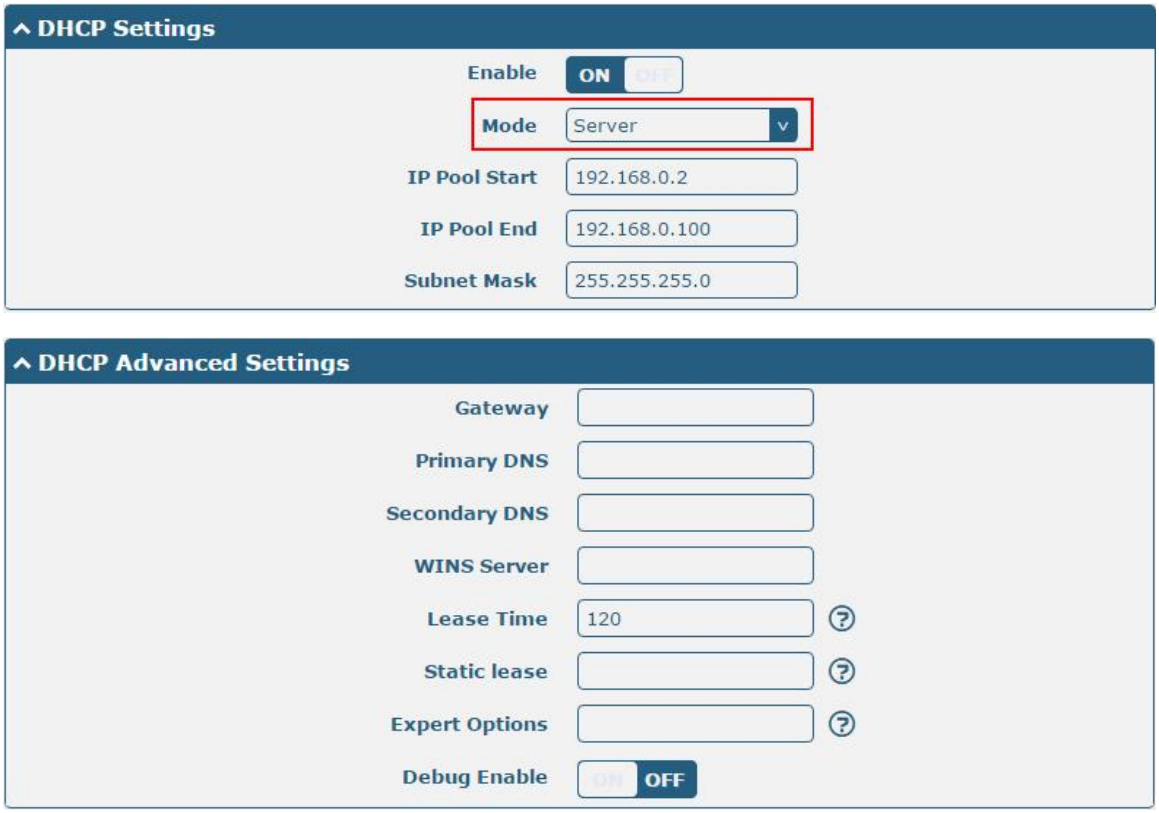
Note: Lan0 cannot be deleted.

You may click to edit the configuration of the LAN port, or click to delete the current LAN port. Now, click to add a new LAN port.



General Settings @ LAN		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Interface	Show the editing port. Lan1 is available only if it was selected by one of ETH0~ETH3 in **Ethernet > Ports > Port Settings**, and so on.	lan0
IP Address	Set the IP address of the LAN port.	192.168.0.1
Netmask	Set the Netmask of the LAN port.	255.255.255.0
MTU	Enter the Maximum Transmission Unit.	1500

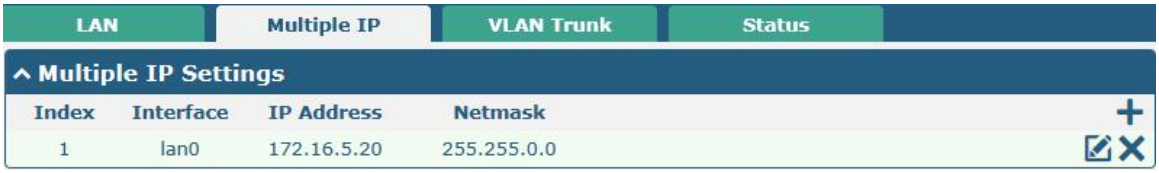
The window is displayed as below when choosing “Server” as the mode.



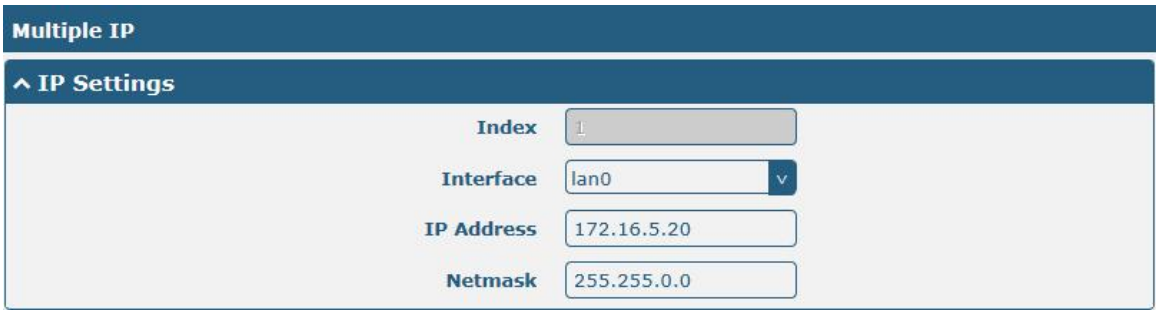
The window is displayed as below when choosing “Relay” as the mode.

LAN		
Item	**Description**	**Default**
DHCP Settings		
Enable	Click the toggle button to enable/disable the DHCP function.	ON
Mode	Select from "Server" or "Relay". • Server: Lease IP address to DHCP clients which have been connected to LAN port • Relay: Router can be a DHCP Relay, which will provide a relay tunnel to solve the problem that DHCP Client and DHCP Server are not in a same subnet	Server
IP Pool Start	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.0.2
IP Pool End	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.0.100
Subnet Mask	Define the subnet mask of IP address obtained by DHCP clients from DHCP server.	255.255.255.0
DHCP Server for Relay	Enter the IP address of DHCP relay server.	Null
DHCP Advanced Settings		
Gateway	Define the gateway assigned by the DHCP server to the clients, which must be on the same network segment with DHCP address pool.	Null
Primary DNS	Define the primary DNS server assigned by the DHCP server to the clients.	Null
Secondary DNS	Define the secondary DNS server assigned by the DHCP server to the clients.	Null
WINS Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever.	Null
Lease Time	Set the lease time which the client can use the IP address obtained from DHCP server, measured in seconds.	120
Static lease	Bind a lease to correspond an IP address via a MAC address. format: mac,ip;mac,ip;..., e.g. FF:ED:CB:A0:98:01,192.168.0.200	Null
Expert Options	Enter some other options of DHCP server in this field. format: config-desc;config-desc, e.g. log-dhcp;quiet-dhcp	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for DHCP information output.	OFF

Multiple IP

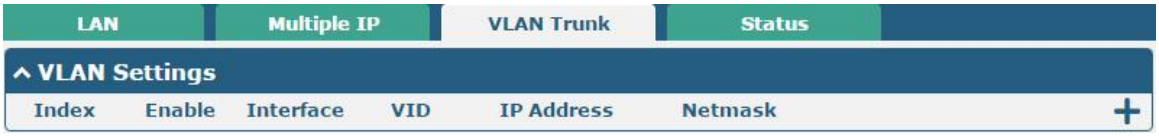


You may click + to add a multiple IP to the LAN port, or click ✕ to delete the multiple IP of the LAN port. Now, click to edit the multiple IP of the LAN port.

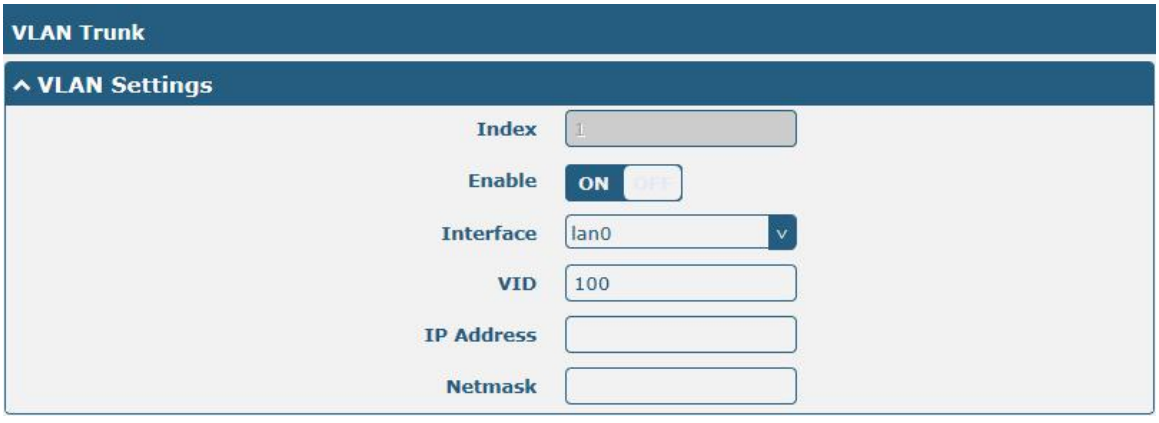


IP Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Interface	Show the editing port.	--
IP Address	Set the multiple IP address of the LAN port.	Null
Netmask	Set the multiple Netmask of the LAN port.	Null

VLAN Trunk



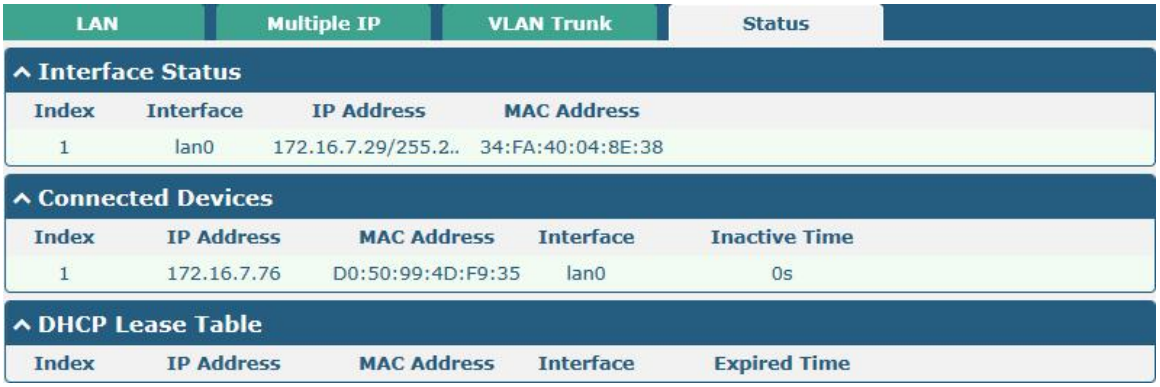
Click + to add a VLAN. The maximum count is 8.



VLAN Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this VLAN. Enable to make router can encapsulate and de-encapsulate the VLAN tag.	ON
Interface	Choose the interface which wants to enable VLAN trunk function. Select from "lan0", "lan1", "lan2" or "lan3" depends on your ETH0~ETH3's corresponding LAN port.	lan0
VID	Set the tag ID of VLAN and digits from 1 to 4094.	100
IP Address	Set the IP address of VLAN port.	Null
Netmask	Set the Netmask of VLAN port.	Null

Status

This section allows you to view the status of LAN connection.



Click the row of status, the details status information will be display under the row. Please refer to the screenshot below.

3.8 Interface > Ethernet

This section allows you to set the related parameters for Ethernet. There are four Ethernet ports on R3000 Quad Router, including ETH0~ETH3. The ETH0 on the router can be configured as either a WAN or a LAN port, while ETH1~ETH3 can only be configured as LAN ports. The ETH0~ETH3 can freely choose from lan0~lan3, but at least one LAN port must be assigned as lan0. The default settings of ETH0~ETH3 are lan0 and their default IP are 192.168.0.1/255.255.255.0.

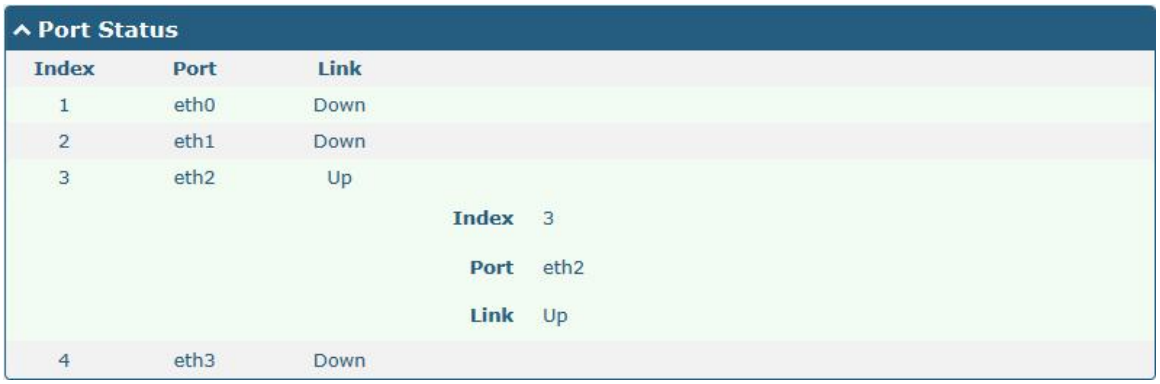
Click button of eth0 to configure its parameters.

Port Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Port	Show the editing port, read only.	--
Port Assignment	Choose the Ethernet port's type, as a WAN port or a LAN port. When setting the port as a LAN port in **Interface > LAN > LAN > Network Settings > General Settings**, you can click the drop-down list to select from "lan0", "lan1", "lan2" or "lan3".	lan0

This column allows you to view the status of Ethernet port.

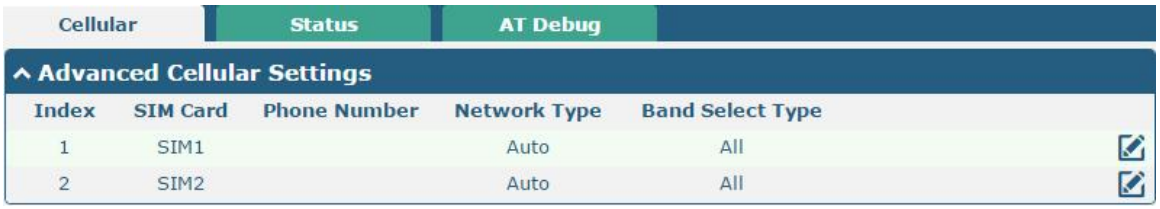
Click the row of status, the details status information will be display under the row. Please refer to the screenshot

below.

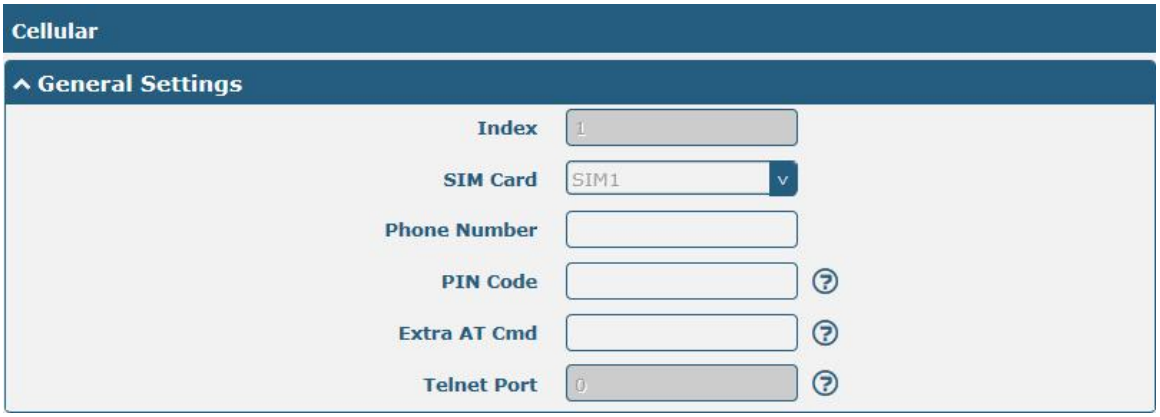


3.9 Interface > Cellular

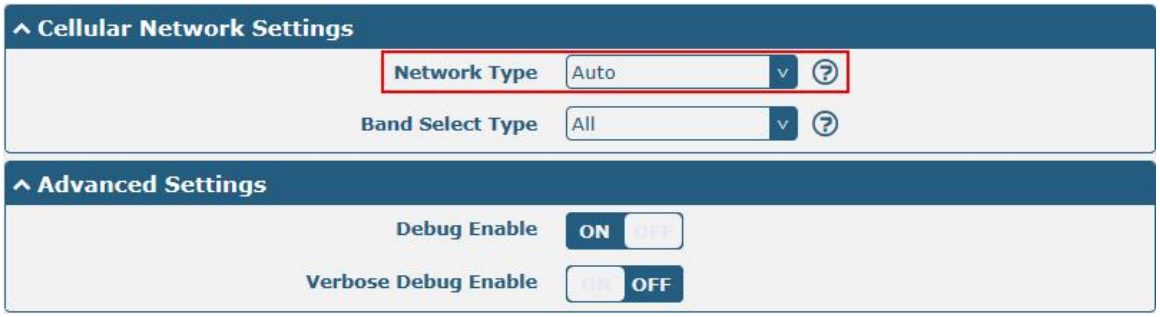
This section allows you to set the related parameters of Cellular. The R3000 Quad Router has two SIM card slots, but do not support two SIM cards online simultaneously due to its single-module design. If insert single SIM card at the first time, SIM1 slot and SIM2 slots are available.



Click of SIM 1 to edit the parameters.



The window is displayed as below when choosing “Auto” as the network type.



The window is displayed as below when choosing “Specify” as the band select type.

Cellular		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
SIM Card	Show the currently editing SIM card.	SIM1
Phone Number	Enter the phone number of the SIM card.	Null
PIN Code	Enter a 4-8 characters PIN code used for unlocking the SIM.	Null
Extra AT Cmd	Enter the AT commands used for cellular initialization.	Null
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet.	0
Cellular Network Settings		
Network Type	Select from "Auto", "3G Only" and "4G Only". • Auto: Connect to the best signal network automatically • 3G Only: Only the 3G network is connected • 4G Only: Only the 4G network is connected	Auto
Band Select Type	Select from "All" or "Specify". You may choose certain bands if choosing "Specify".	All
Advanced Settings		
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

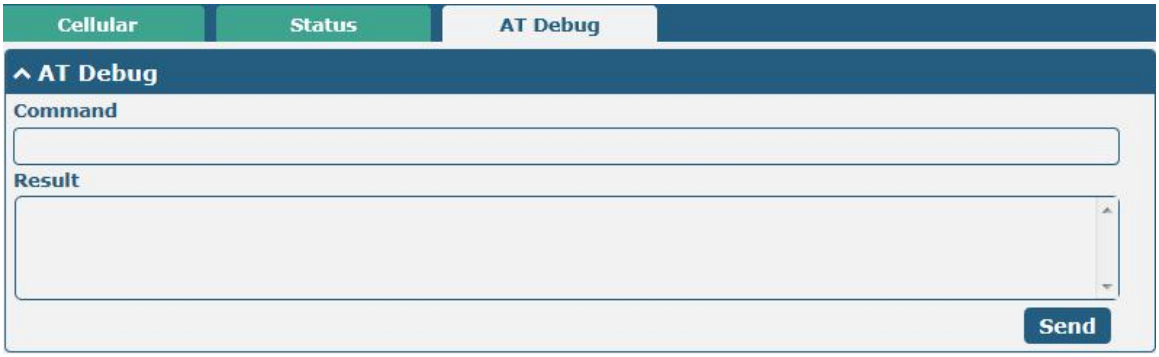
This section allows you to view the status of the cellular connection.

Click the row of status, the details status information will be displayed under the row.

Status	
Item	**Description**
Index	Indicate the ordinal of the list.
Modem Status	Show the status of the radio module.
Modem Model	Show the model of the radio module.
Current SIM	Show the SIM card that your router is using.
Phone Number	Show the phone number of the current SIM.
IMSI	Show the IMSI number of the current SIM.
ICCID	Show the ICCID number of the current SIM.
Registration	Show the current network status.
Network Provider	Show the name of Network Provider.
Network Type	Show the current network service type, e.g. GPRS.
Signal Strength	Show the signal strength detected by the mobile.
Bit Error Rate	Show the current bit error rate.
PLMN ID	Show the current PLMN ID.
Local Area Code	Show the current local area code used for identifying different area.
Cell ID	Show the current cell ID used for locating the router.
IMEI	Show the IMEI (International Mobile Equipment Identity) number of the radio module.

Status	
Item	**Description**
Firmware Version	Show the current firmware version of the radio module.

This page allows you to check the AT Debug.



AT Debug		
Item	**Description**	**Default**
Command	Enter the AT command that you want to send to cellular module in this text box.	Null
Result	Show the AT command responded by cellular module in this text box.	Null
Send	Click the button to send AT command.	--

3.10 Interface > WiFi

This section allows you to configure the parameters of two Wi-Fi modes. Router supports either WiFi AP mode or Client mode, and default as AP mode.
Note: Need to reboot to make configuration take effect if switching the AP and Client mode.

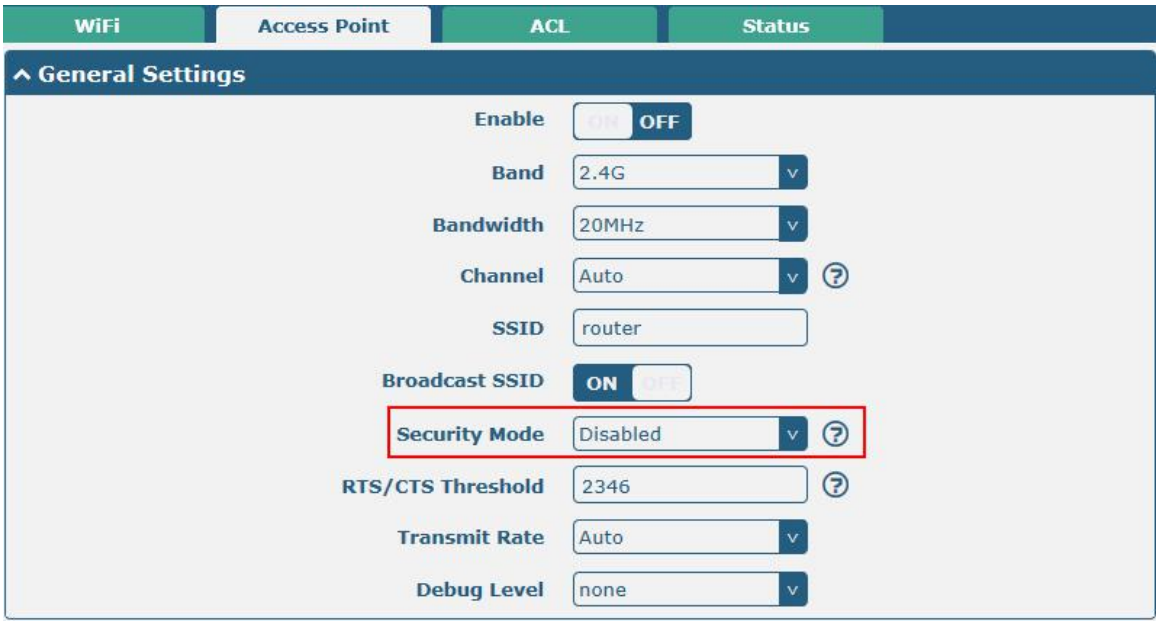
WiFi AP

Configure Router as WiFi AP

Click **Interface > WiFi > WiFi**, select "AP" as the mode and click "Submit".

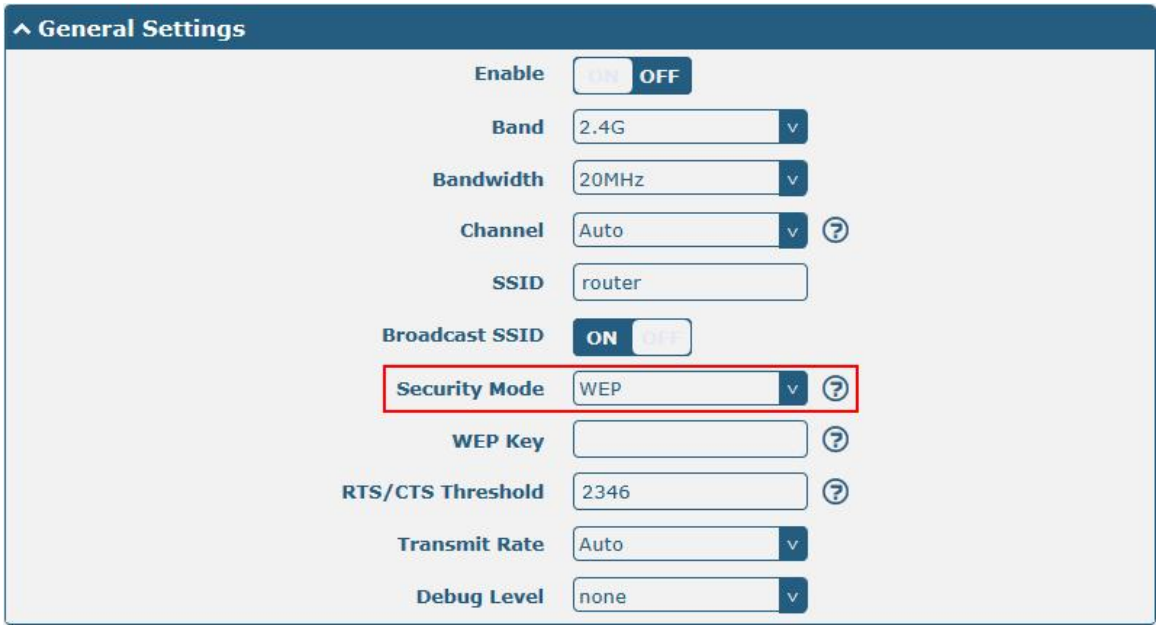
Note: Please remember to click **Save & Apply > Reboot** after finish the configuration, so that the configuration can be took effect.

Click the **Access Point** column to configure the parameters of WiFi AP. By default, the security mode is set as "Disabled".



The window is displayed as below when setting “WPA” as the security mode.

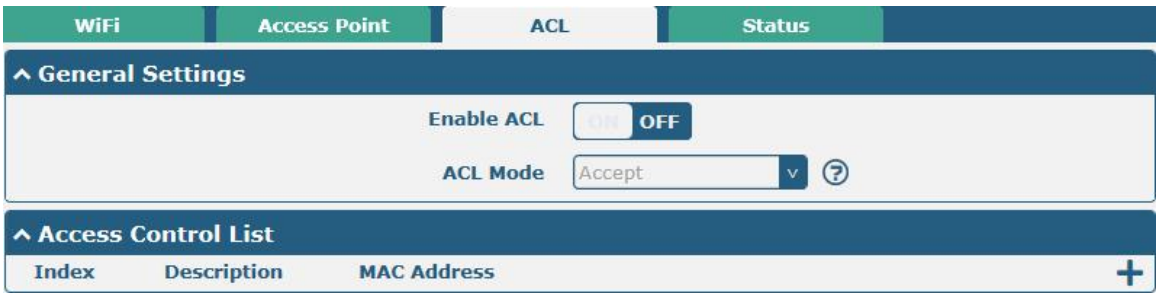
The window is displayed as below when setting “WEP” as the security mode.



General Settings @ Access Point		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the WiFi access point option.	OFF
Band	Select from “2.4G” or “5G”.	2.4G
Bandwidth	Select from “20MHz”, “40MHz”. 40 MHz channel width provides twice the data rate available over a single 20 MHz channel.	20MHz
Channel	Select the frequency channel, including “Auto”, “1”, “2”…… “13”. • Auto: Router will scan all frequency channels until the best one is found • 1~13 Router will be fixed to work with this channel Following are the frequency of 1~13 channel: 1: 2412 MHz 2: 2417 MHz 3: 2422 MHz 4: 2427 MHz 5: 2432 MHz 6: 2437 MHz 7: 2442 MHz 8: 2447 MHz 9: 2452 MHz 10: 2457 MHz 11: 2462 MHz 12: 2467 MHz 13: 2472 MHz	Auto

General Settings @ Access Point		
Item	**Description**	**Default**
SSID	Enter the Service Set Identifier, the name of your wireless network. The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other. Enter 1 to 32 characters.	router
Broadcast SSID	Click the toggle button to enable/disable the SSID being broadcast. When enabled, the client can scan your SSID. When disabled, the client cannot scan your SSID. If you want to connect to the router AP, you need to manually enter the SSID of router AP at WiFi client side.	ON
Security Mode	Select from "Disabled", "WPA" or "WEP". • Disabled: User can access the WiFi without password **Note**: It is strongly recommended for security purposes that you do not choose this kind of mode. • WPA: Include WPA and WPA2. Personal versions of WPA (Wi-Fi Protected Access), also known as WPA/WPA-PSK (Pre-Shared Key), provide a simple way of encrypting a wireless connection for high confidentiality. • WEP: Wired Equivalent Privacy provides encryption for wireless device's data transmission	Disabled
WPA Version	Select from "Auto", "WPA" or "WPA2". • Auto: Router will choose automatically the most suitable WPA version • WPA2 is a stronger security feature than WPA	Auto
Encryption	Select from "Auto", "TKIP" or "AES". • Auto: Router will choose automatically the most suitable encryption • TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication **Note**: It's not recommended to use TKIP encryption in 802.11n mode. • AES: AES encryption uses a wireless connection. AES can be used for CCMP WPA-PSK and WPA 802.1x authentication. AES is a stronger encryption algorithm than TKIP	Auto
PSK Password	Enter the Pre share key password. When router works as AP mode, enter Master key to generate keys for encryption. A PSK Password is used as a basis for encryption methods (or cipher types) in a WLAN connection. The PSK Password should be complicated and as long as possible. For security reasons, this PSK Password should only be disclosed to users who need it, and it should be changed regularly. Enter 8 to 63 characters.	Null
Group Key Update Interval	Enter the time period of group key renewal.	3600

General Settings @ Access Point		
Item	**Description**	**Default**
WEP Key	Enter the WEP key. The key length should be 10 or 26 hexadecimal digits depending on which WEP key is used, 64 digits or 128 digits.	Null
RTS/CTS Threshold	Specify the RTS (request to send) threshold or CTS (clear to send) threshold and digits from 256 to 2346. The router AP will never send the signal before sending out data if setting the RTS threshold as 2347, and the router AP will send the signal once it sending out data if setting the RTS threshold as 0.	2346
Transmit Rat	Set the transmit rate. You can choose Auto or specify a Transmit Rate, including 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps, MCS0, MCS1, MCS2, MCS3, MCS4, MCS5, MCS6 and MCS7.	Auto
Debug Level	Select from “verbose”, “debug”, “info”, “notice”, “warning” or “none”.	none

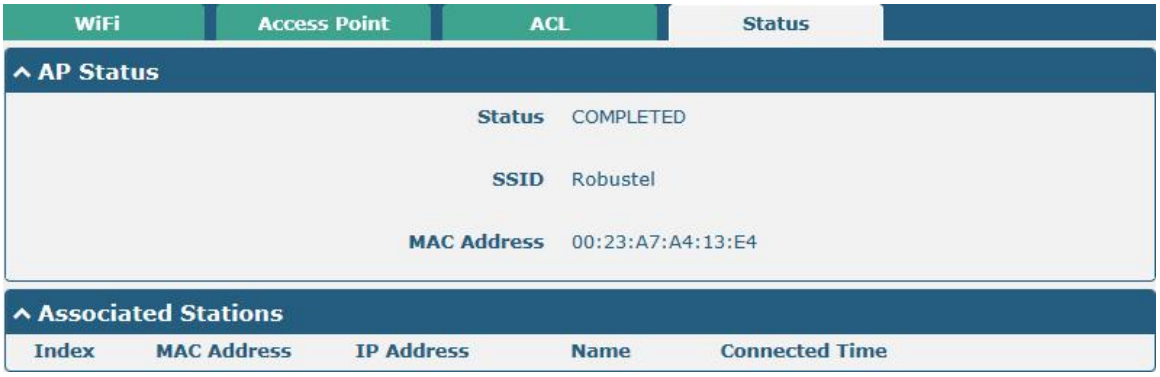


Click + to add a MAC address to the Access Control List. The maximum count for MAC address is 64.

ACL		
Item	**Description**	**Default**
General Settings		
Enable ACL	Click the toggle button to enable/disable this option.	OFF
ACL Mode	Select from “Accept” or “Deny”. • Accept: Only the packets fitting the entities of the “Access Control List” can be allowed • Deny: All the packets fitting the entities of the “Access Control List” will be denied **Note**: Router can only allow or deny devices which are included in “Access Control List” at one time.	Accept

ACL		
Item	**Description**	**Default**
Access Control List		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this access control list.	Null
MAC Address	Add a MAC address here.	Null

This section allows you to view the status of AP.



WiFi Client

Configure Router as WiFi client

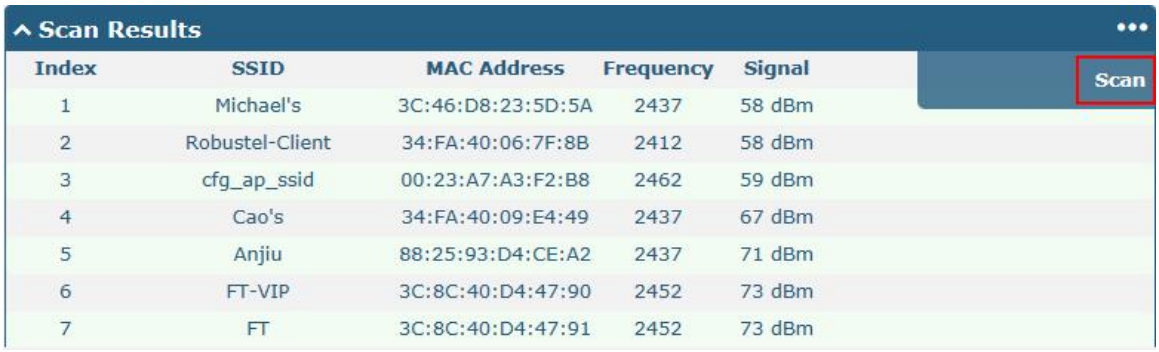
Click **Interface > WiFi > WiFi**, select "Client" as the mode and click "Submit".

And then a "WLAN" column will appear under the Interface list.

Click **Interface > Link Manager > Link Settings**, and click the edit button of WLAN, then configure its related parameters.

Click **Interface > WLAN** to configure the parameters of WiFi Client after setting the mode as Client. Please remember to click **Save & Apply > Reboot** after finish the configuration, so that the configuration can be took effect.

This window allows you to scan for all available SSIDs in your area and connect to one of those shown on the "Scan Results" list.



3.11 Interface > USB

This section allows you to set the USB parameters. The USB interface of the router can be used for firmware upgrade and configuration upgrade.

General Settings @ USB		
Item	**Description**	**Default**
Enable USB	Click the toggle button to enable/disable the USB option.	ON
Enable Automatic Firmware Updating	Click the toggle button to enable/disable this option. Enable to update automatically the router's firmware when inserting a USB storage device with a router's firmware.	ON

Router has the key for USB automatic update. User can generate the key in this page.

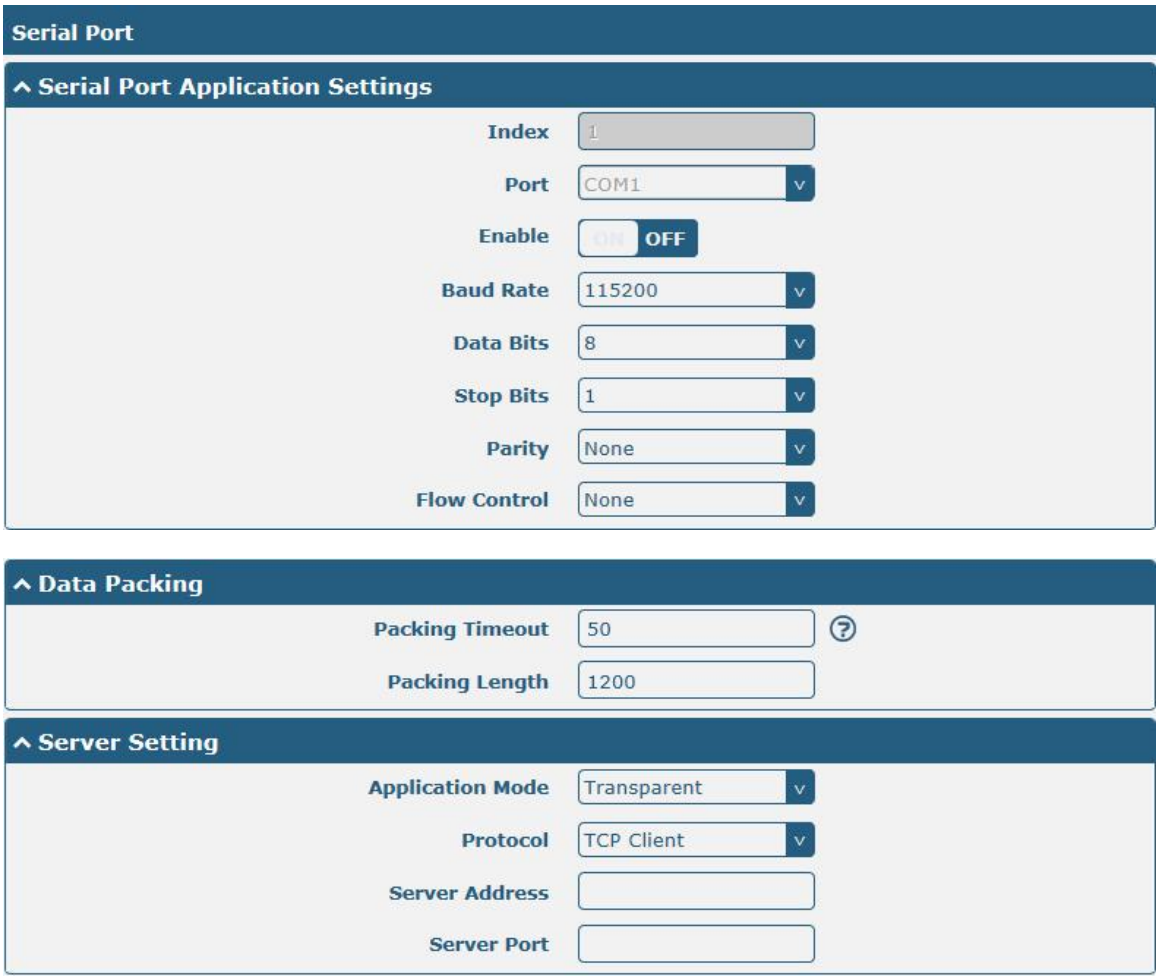
Key		
Item	**Description**	**Default**
USB Automatic Update Key	Click Generate to generate a key, and click Download to download the key.	--

3.12 Interface > Serial Port

This section allows you to set the serial port parameters. R3000 Quad Router supports one RS-232 or one RS-485

across a 7-pin terminal block with lock. Serial port provides a way to transfer serial data to IP data, or vice versa, and transmit these data via wired or wireless network to achieve data transparent transmission.

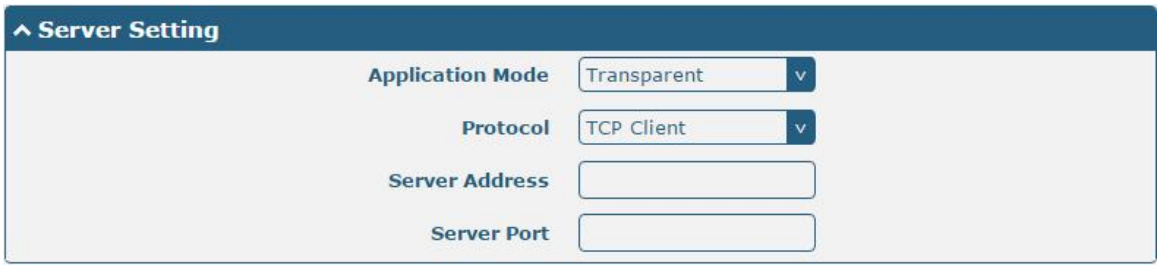
Click the edit button of COM1.



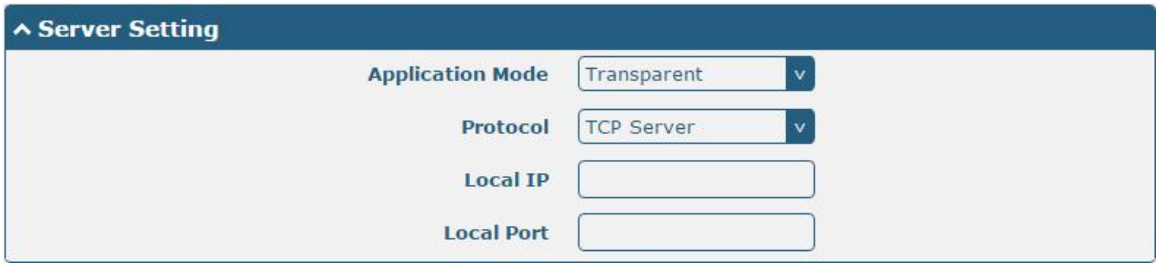
Serial Port		
Item	**Description**	**Default**
Serial Port Application Settings		
Index	Indicate the ordinal of the list.	--
Port	Show the current serial's name, read only.	COM1
Enable	Click the toggle button to enable/disable this serial port. When the status is OFF, the serial port is not available.	OFF
Baud Rate	Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400", "57600" , "115200" or "230400".	115200
Data Bits	Select from "7" or "8".	8
Stop Bits	Select from "1" or "2".	1
Parity	Select from "None", "Odd" or "Even".	None

Flow control	Select from “None”, “Software” or “Hardware”.	None
Data Packing		
Packing Timeout	Set the packing timeout. The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field. **Note**: Data will also be sent as specified by the packet length even when data is not reaching the interval timeout in the field.	50
Packing Length	Set the packet length. The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When a packet length between 1 and 3000 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.	1200

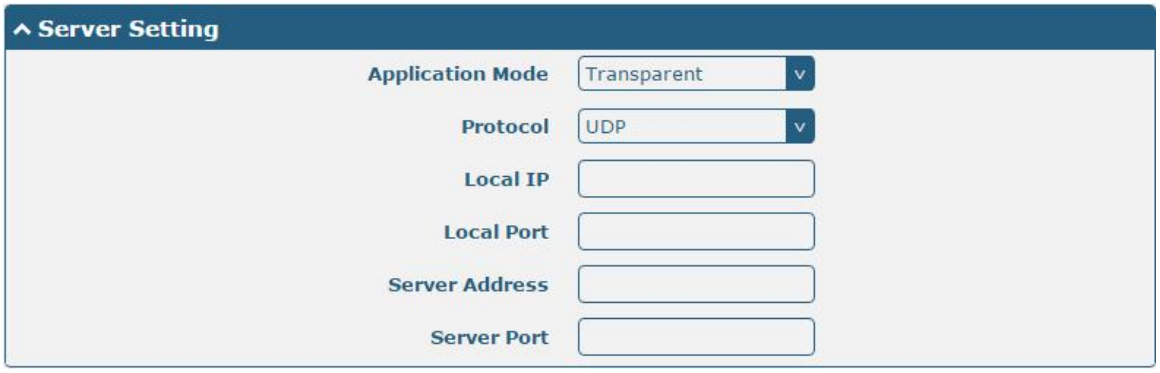
- The window is displayed as below when choosing “Transparent” as the application mode and “TCP Client” as the protocol.



The window is displayed as below when choosing “Transparent” as the application mode and “TCP Server” as the protocol.

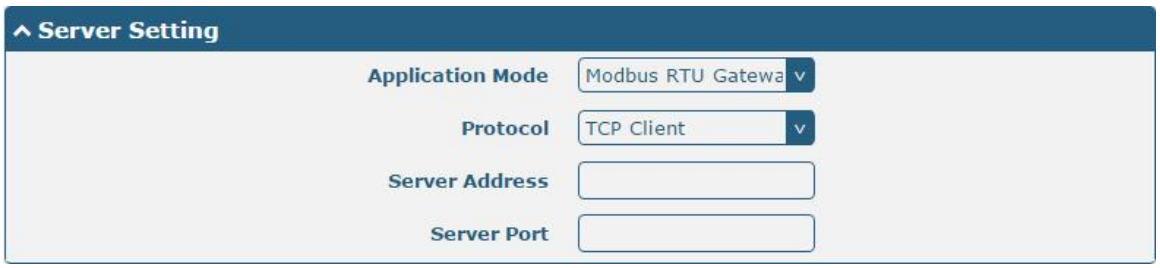


The window is displayed as below when choosing “Transparent” as the application mode and “UDP” as the protocol.

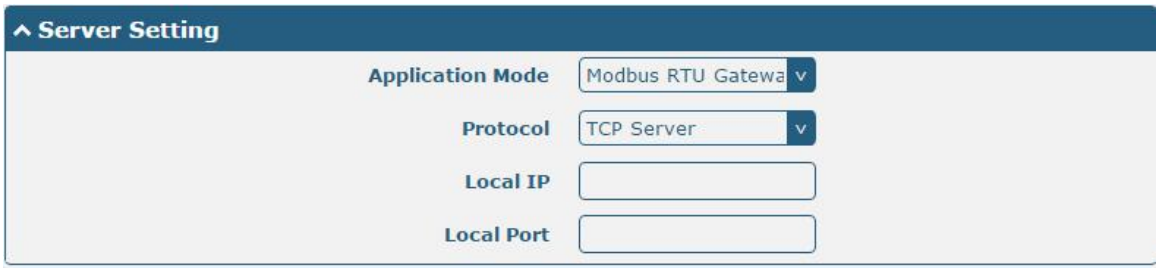


The window is displayed as below when choosing “Transparent” as the application mode and “Robustlink” as the protocol.

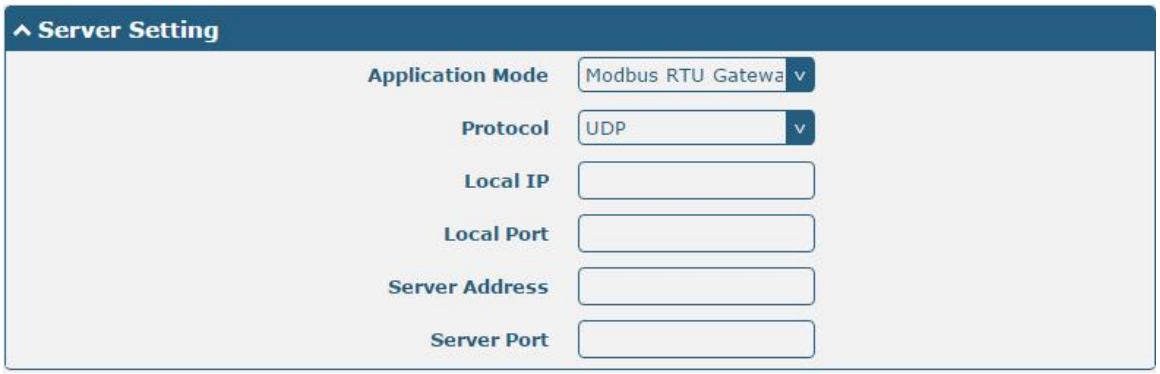
- The window is displayed as below when choosing “Modbus RTU Gateway” as the application mode and “TCP Client” as the protocol.



The window is displayed as below when choosing “Modbus RTU Gateway” as the application mode and “TCP Server” as the protocol.



The window is displayed as below when choosing “Modbus RTU Gateway” as the application mode and “UDP” as the protocol.



The window is displayed as below when choosing “Modbus RTU Gateway” as the application mode and “Robustlink” as the protocol.

Server Settings		
Item	**Description**	**Default**

Server Settings		
Item	**Description**	**Default**
Application Mode	Select from “Transparent” or “Modbus RTU Gateway”. • Transparent: Router will transmit the serial data transparently • Modbus RTU Gateway: Router will translate the Modbus RTU data to Modbus TCP data and sent out, and vice versa	Transparent
Protocol	Select from “TCP Client”, “TCP Server”, “UDP” or “Robustlink”. • TCP Client: Router works as TCP client, initiate TCP connection to TCP server. Server address supports both IP and domain name • TCP Server: Router works as TCP server, listening for connection request from TCP client • UDP: Router works as UDP client • Robustlink: Router will automatically upload the serial data to Robustlink platform under the Robustlink protocol. Robustlink is a management platform from Robustel. This function only available when Router is connects to Robustlink	TCP Client
Server Address	Enter the address of server which will receive the data sent from router’s serial port. IP address or domain name will be available.	Null
Server Port	Enter the specified port of server which is used for receiving the serial data.	Null
Local IP @ Transparent	Enter router’s LAN IP which will forward to the internet port of router.	Null
Local Port @ Transparent	Enter the port of router’s LAN IP.	Null
Local IP @ Modbus	Enter the local IP of under Modbus mode.	Null
Local Port @ Modbus	Enter the local port of under Modbus mode.	Null

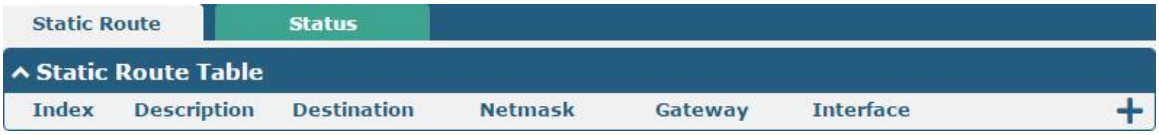
Click the “Status” column to view the type which the current serial port corresponds. The default setting of serial port is RS-485, changed by software. Software selectable refers to change the serial port to RS-232 or RS-485 through an importing APP.

Note: To change your serial type, please contact your Robustel sales representative.

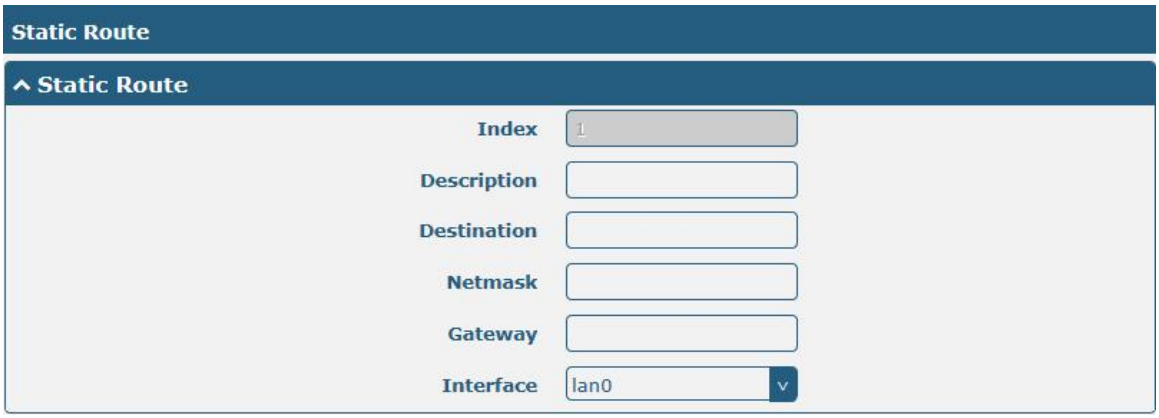
3.13 Network > Route

This section allows you to set the static route. Static route is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing traffic. Route Information Protocol (RIP) is widely used in small network with stable use rate. Open Shortest Path First (OSPF) is made router within a single autonomous system and used in large network.

Static Route



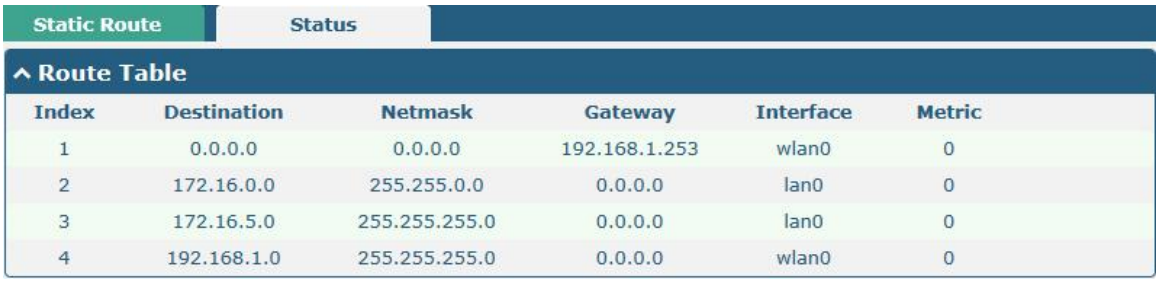
Click + to add static routes. The maximum count is 20.



Static Route		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this static route.	Null
Destination	Enter the IP address of destination host or destination network.	Null
Netmask	Enter the Netmask of destination host or destination network.	Null
Gateway	Define the gateway of the destination.	Null
Interface	Choose the corresponding port of the link that you want to configure.	wwan

Status

This window allows you to view the status of route.

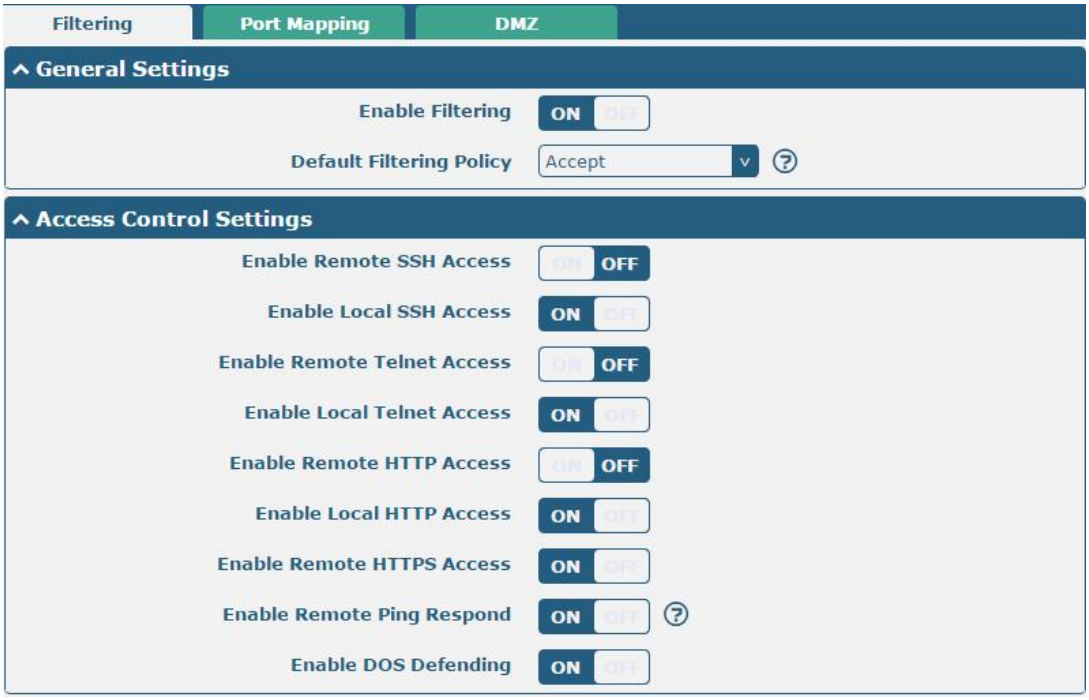


3.14 Network > Firewall

This section allows you to set the firewall and its related parameters, including Filtering, Port Mapping and DMZ.

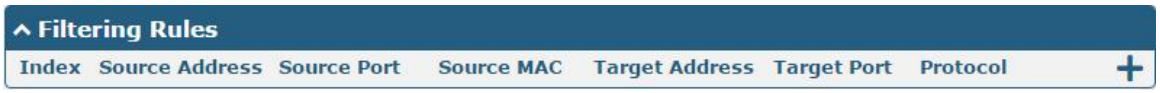
Filtering

The filtering rules can be used to either accept or block certain users or ports from accessing your router.

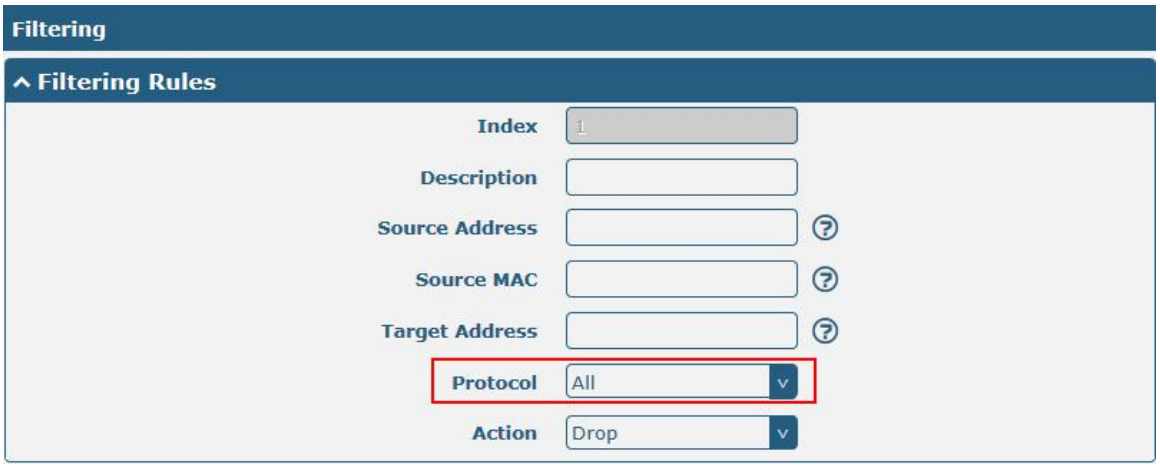


Filtering		
Item	**Description**	**Default**
General Settings		
Enable Filtering	Click the toggle button to enable/disable the filtering option.	ON
Default Filtering Policy	Select from “Accept” or “Drop”. Cannot be changed when filtering rules table is not empty. • Accept: Router will accept all the connecting requests except the hosts which fit the drop filter list • Drop: Router will drop all the connecting requests except the hosts which fit the accept filter list	Accept

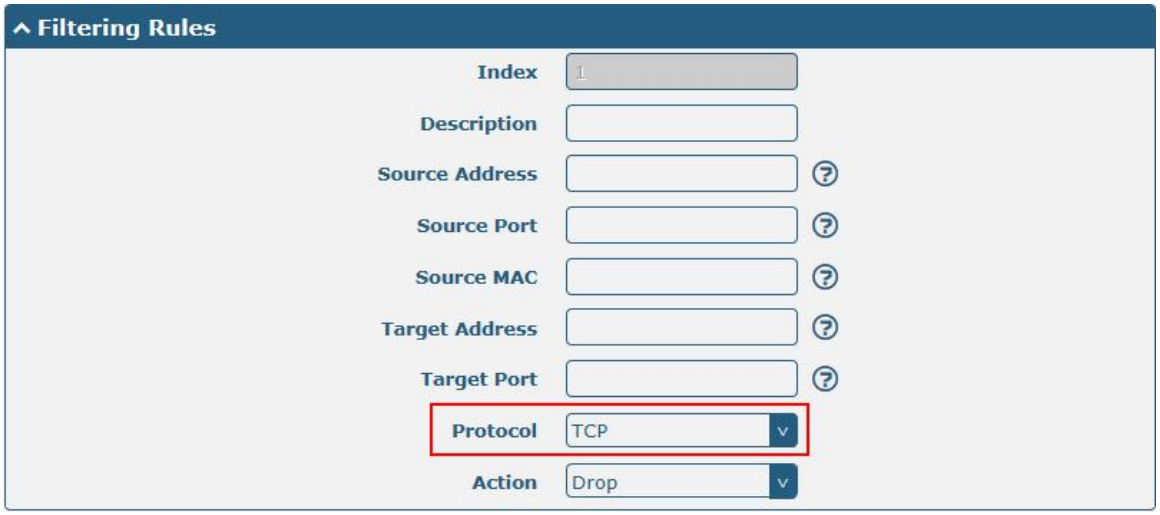
Filtering		
Item	**Description**	**Default**
Access Control Settings		
Enable Remote SSH Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via SSH.	OFF
Enable Local SSH Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via SSH.	ON
Enable Remote Telnet Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via Telnet.	OFF
Enable Local Telnet Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via Telnet.	ON
Enable Remote HTTP Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via HTTP.	OFF
Enable Local HTTP Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via HTTP.	ON
Enable Remote HTTPS Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via HTTPS.	ON
Enable Remote Ping Respond	Click the toggle button to enable/disable this option. When enabled, the router will reply to the Ping requests from other hosts on the Internet.	ON
Enable DOS Defending	Click the toggle button to enable/disable this option. When enabled, the router will defend the DOS. Dos attack is an attempt to make a machine or network resource unavailable to its intended users.	ON



Click + to add a filtering rule. The maximum count is 20. The window is displayed as below when defaulting "All" or choosing "ICMP" as the protocol. Here take "All" as an example.



The window is displayed as below when choosing "TCP", "UDP" or "TCP-UDP" as the protocol. Here take "TCP" as an example.

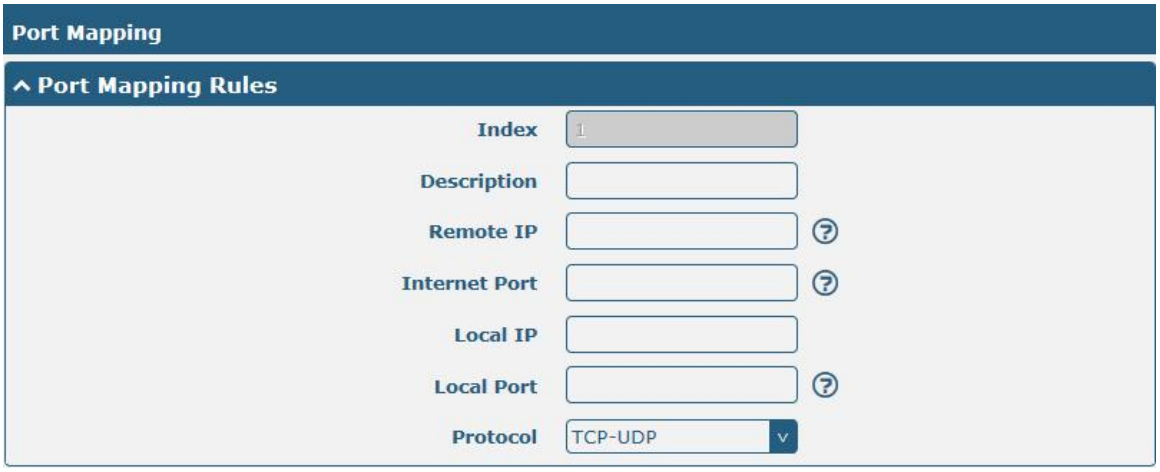


Filtering Rules		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this filtering rule.	Null
Source Address	Specify an access originator and enter its source address.	Null
Source Port	Specify an access originator and enter its source port.	Null
Source MAC	Specify an access originator and enter its source MAC address.	Null
Target Address	Enter the target address which the access originator wants to access.	Null
Target Port	Enter the target port which the access originator wants to access.	Null

Filtering Rules		
Item	**Description**	**Default**
Protocol	Select from “All”, “TCP”, “UDP”, “ICMP” or “TCP-UDP”. **Note**: It is recommended that you choose “All” if you don’t know which protocol of your application to use.	All
Action	Select from “Accept” or “Drop”.	Drop

Port Mapping

Click + to add port mapping rules. The maximum rule count is 40.



Port Mapping Rules		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this port mapping.	Null
Remote IP	Specify the host or network which can access the local IP address. Empty means unlimited, e.g. 10.10.10.10/255.255.255.255 or 192.168.1.0/24	Null
Internet Port	Enter the internet port of router which can be accessed by other hosts from internet.	Null
Local IP	Enter router’s LAN IP which will forward to the internet port of router.	Null
Local Port	Enter the port of router’s LAN IP.	Null
Protocol	Select from “TCP”, “UDP” or “TCP-UDP” as your application required.	TCP-UDP

DMZ

DMZ host is a host on the internal network that has all ports exposed, except those ports otherwise forwarded.

DMZ Settings		
Item	**Description**	**Default**
Enable DMZ	Click the toggle button to enable/disable DMZ.	OFF
Host IP Address	Enter the IP address of the DMZ host on your internal network.	Null
Source IP Address	Set the address which can talk to the DMZ host. Null means for any addresses.	Null

3.15 Network > IP Passthrough

Click **Network > IP Passthrough > IP Passthrough** to enable or disable the IP Pass-through option.

If router enables the IP Pass-through, the terminal device (such as PC) will enable the DHCP Client mode and connect to LAN port of the router; and after the router dial up successfully, the PC will automatically obtain the IP address and DNS server address which assigned by ISP.

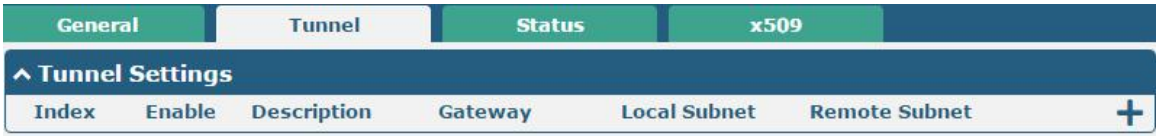
3.16 VPN > IPsec

This section allows you to set the IPsec and the related parameters. Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session.

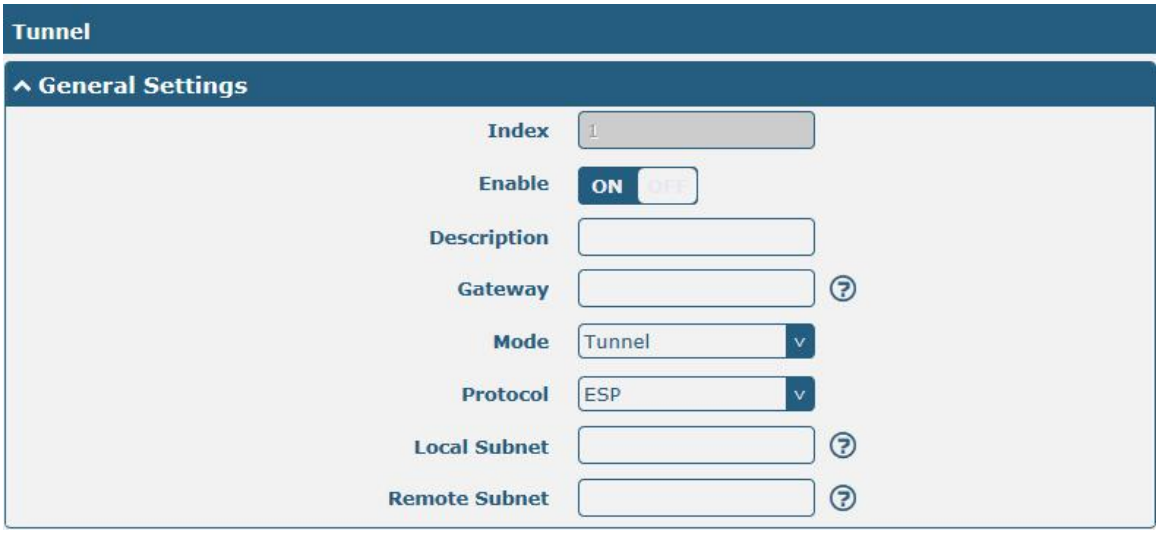
General

General Settings @ General		
Item	**Description**	**Default**
Enable NAT Traversal	Click the toggle button to enable/disable the NAT Traversal function. This option must be enabled when router under NAT environment.	ON
Keepalive	Set the keepalive time, measured in seconds. The router will send packets to NAT server every keepalive time to avoid record remove from the NAT list.	60
Debug Enable	Click the toggle button to enable/disable this option. Enable for IPsec VPN information output to the debug port.	OFF

Tunnel



Click + to add tunnel settings. The maximum count is 3.

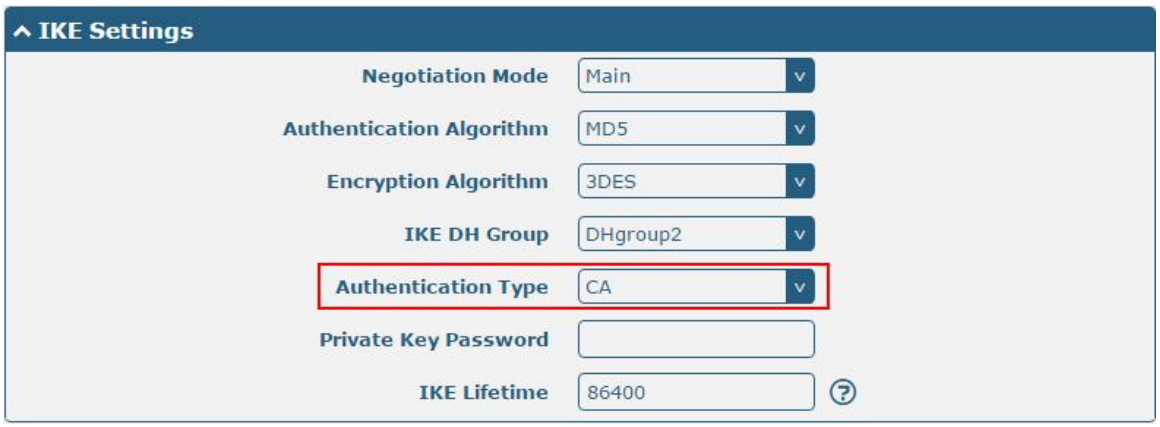


General Settings @ Tunnel		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this IPsec tunnel.	ON
Description	Enter a description for this IPsec tunnel.	Null
Gateway	Enter the address of remote IPsec VPN server. 0.0.0.0 represents for any address.	Null
Mode	Select from “Tunnel” and “Transport”. • Tunnel: Commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it • Transport: Used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host-for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual	Tunnel

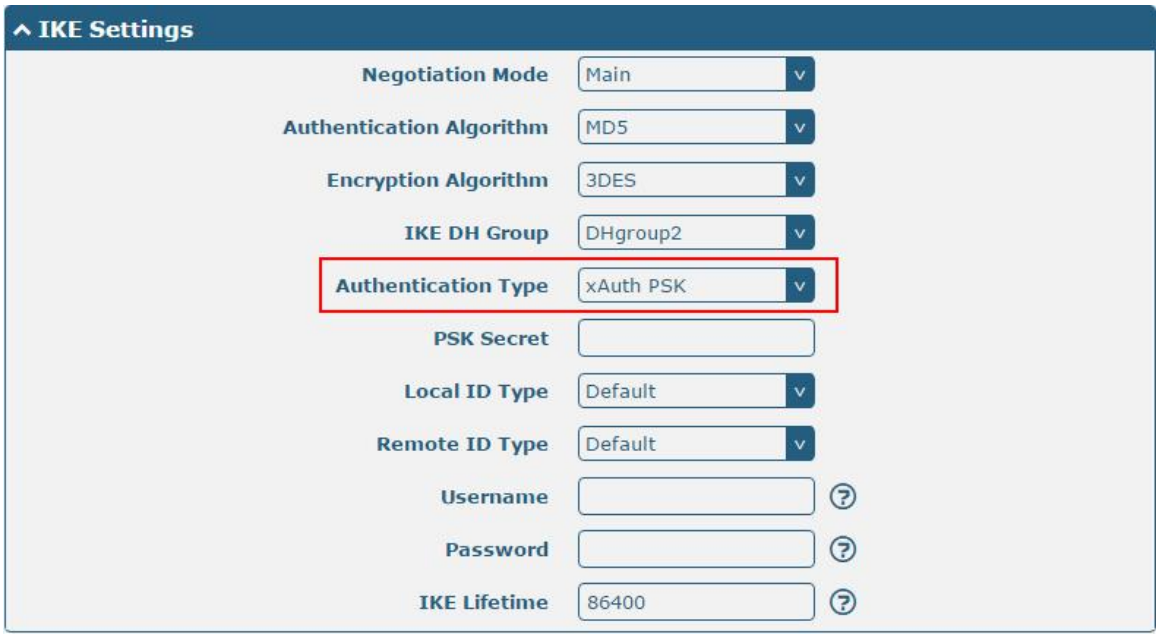
	destination	
Protocol	Select the security protocols from “ESP” and “AH”. • ESP: Use the ESP protocol • AH: Use the AH protocol	ESP
Local Subnet	Enter the local subnet’s address with mask protected by IPsec, e.g. 192.168.1.0/24	Null
Remote Subnet	Enter the remote subnet’s address with mask protected by IPsec, e.g. 10.8.0.0/24	Null

The window is displayed as below when choosing “PSK” as the authentication type.

The window is displayed as below when choosing “CA” as the authentication type.



The window is displayed as below when choosing “xAuth PSK” as the authentication type.

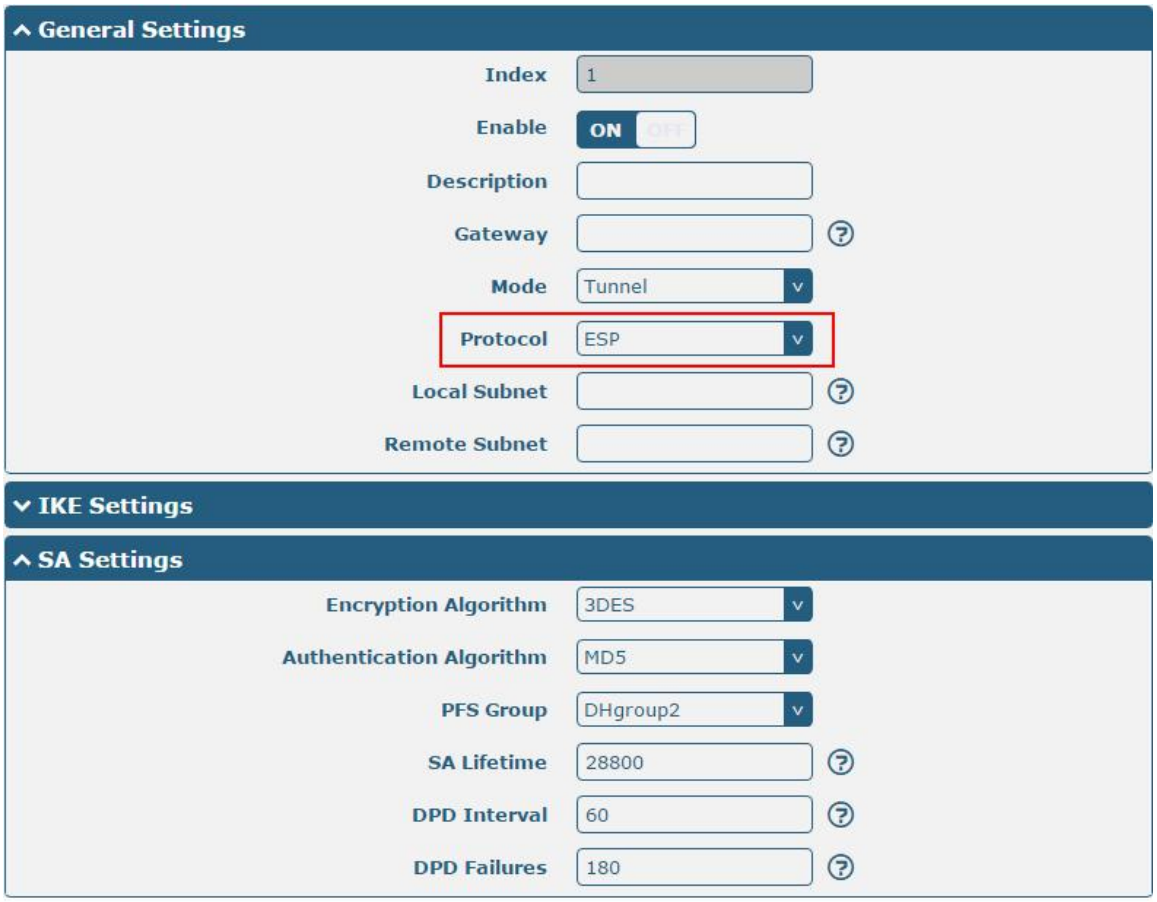


The window is displayed as below when choosing “xAuth CA” as the authentication type.

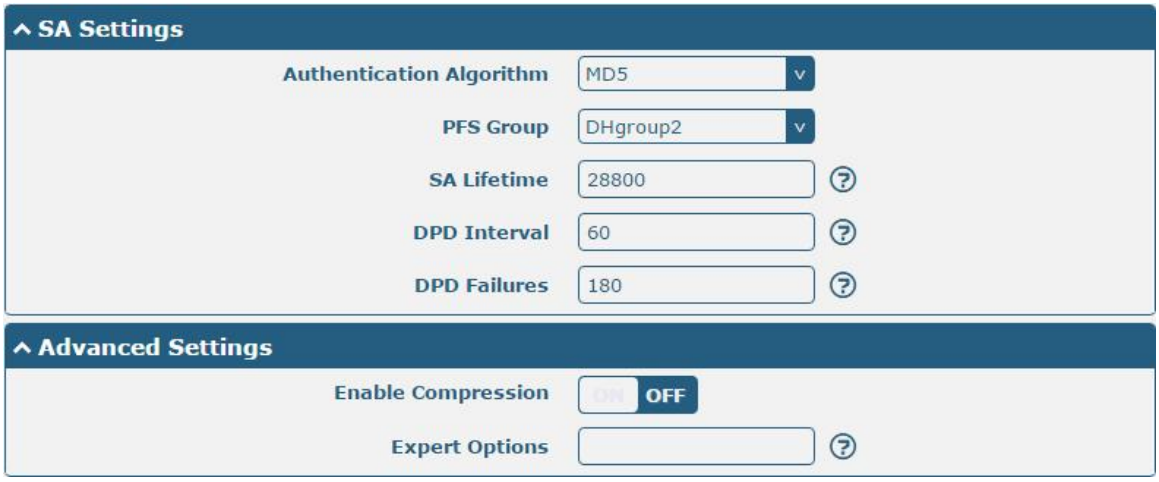
IKE Settings		
Item	**Description**	**Default**
Negotiation Mode	Select from “Main” and “Aggressive” for the IKE negotiation mode in phase 1. If the IP address of one end of an IPsec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main
Authentication Algorithm	Select from “MD5”, “SHA1”, “SHA2 256” or “SHA2 512” to be used in IKE negotiation.	MD5
Encrypt Algorithm	Select from “3DES”, “AES128” and “AES256”to be used in IKE negotiation. • 3DES: Use 168-bit 3DES encryption algorithm in CBC mode • AES128: Use 128-bit AES encryption algorithm in CBC mode • AES256: Use 256-bit AES encryption algorithm in CBC mode	3DES
IKE DH Group	Select from “DHgroup2”, “DHgroup5”, “DHgroup14”, “DHgroup15”,	DHgroup2

IKE Settings		
Item	**Description**	**Default**
	"DHgroup16", "DHgroup17" or "DHgroup18" to be used in key negotiation phase 1.	
Authentication Type	Select from "PSK", "CA", "xAuth PSK" and "xAuth CA" to be used in IKE negotiation. • PSK: Pre-shared Key • CA: x509 Certificate Authority • xAuth: Extended Authentication to AAA server	PSK
PSK Secret	Enter the pre-shared key.	Null
Local ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. • Default: Use an IP address as the ID in IKE negotiation • FQDN: Use an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com. • User FQDN: Use a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security gateway, e.g., test@robustel.com.	Default
Remote ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. • Default: Use an IP address as the ID in IKE negotiation • FQDN: Use an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com. • User FQDN: Use a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security gateway, e.g., test@robustel.com.	Default
IKE Lifetime	Set the lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as the new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.	86400
Private Key Password	Enter the private key under the "CA" and "xAuth CA" authentication types.	Null
Username	Enter the username used for the "xAuth PSK" and "xAuth CA" authentication types.	Null
Password	Enter the password used for the "xAuth PSK" and "xAuth CA" authentication types.	Null

If click **VPN > IPsec > Tunnel > General Settings**, and choose **ESP** as protocol. The specific parameter configuration is shown as below.



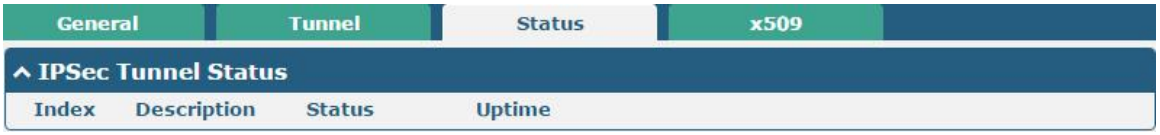
If choose **AH** as protocol, the window of SA Settings is displayed as below.



SA Settings		
Item	**Description**	**Default**
Encrypt Algorithm	Select from “3DES”, “AES128” or “AES256” when you select “ESP” in “Protocol”. Higher security means more complex implementation and lower speed. DES is enough to meet general requirements. Use 3DES when high confidentiality and security are required.	3DES
Authentication Algorithm	Select from “MD5”, “SHA1”, “SHA2 256” or “SHA2 512” to be used in SA negotiation.	MD5
PFS Group	Select from “DHgroup2”, “DHgroup5”, “DHgroup14”, “DHgroup15”, “DHgroup16”, “DHgroup17” or “DHgroup18” to be used in SA negotiation.	DHgroup2
SA Lifetime	Set the IPsec SA lifetime. When negotiating set up IPsec SAs, IKE uses the smaller one between the lifetime set locally and the lifetime proposed by the peer.	28800
DPD Interval	Set the interval after which DPD is triggered if no IPsec protected packets is received from the peer. DPD is Dead peer detection. DPD irregularly detects dead IKE peers. When the local end sends an IPsec packet, DPD checks the time the last IPsec packet was received from the peer. If the time exceeds the DPD interval, it sends a DPD hello to the peer. If the local end receives no DPD acknowledgment within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgment after having made the maximum number of retransmission attempts, it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.	60
DPD Failures	Set the timeout of DPD (Dead Peer Detection) packets.	180
Advanced Settings		
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the inner headers of IP packets.	OFF
Expert Options	Add more PPP configuration options here, format: config-desc;config-desc, e.g. protostack=netkey;plutodebug=none	Null

Status

This section allows you to view the status of the IPsec tunnel.



x509

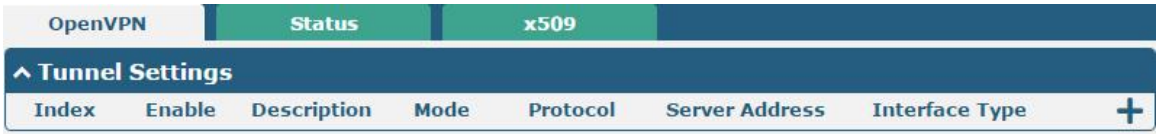
User can upload the X509 certificates for the IPsec tunnel in this section.

x509		
Item	**Description**	**Default**
X509 Settings		
Tunnel Name	Choose a valid tunnel.	Tunnel 1
Certificate Files	Click on "Choose File" to locate the certificate file from your computer, and then import this file into your router. The correct file format is displayed as follows: @ca.crt @remote.crt @local.crt @private.key @crl.pem	Null
Certificate Files		
Index	Indicate the ordinal of the list.	--
Filename	Show the imported certificate's name.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

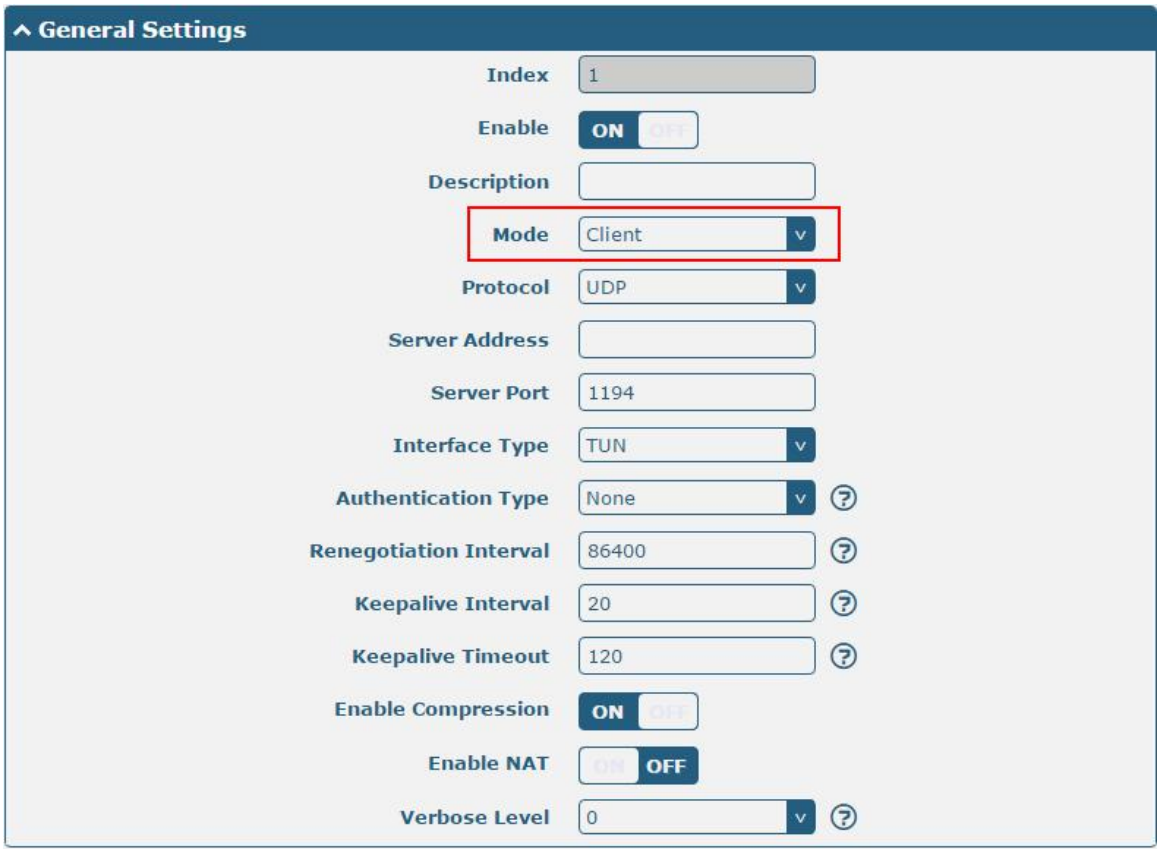
3.17 VPN > OpenVPN

This section allows you to set the OpenVPN and the related parameters. OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. Router supports point-to-point and point-to-points connections.

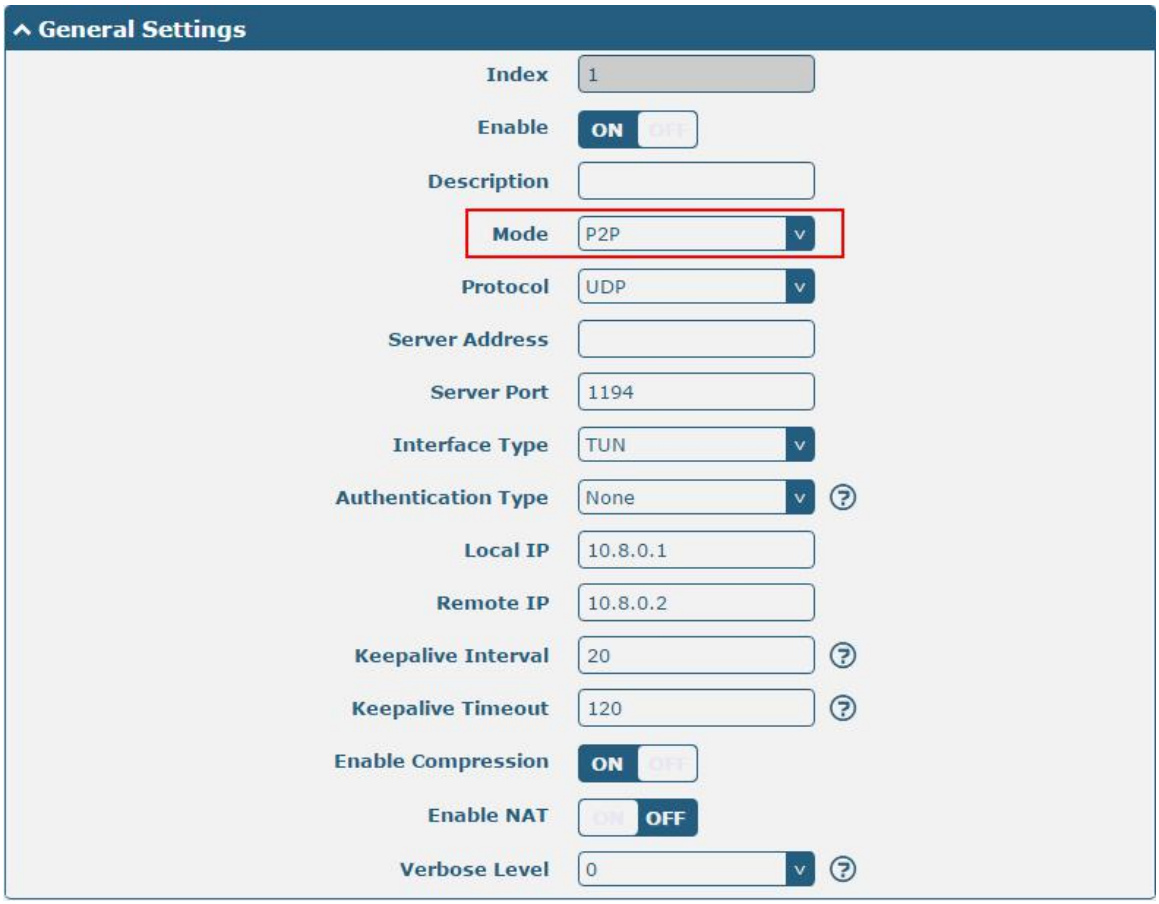
OpenVPN



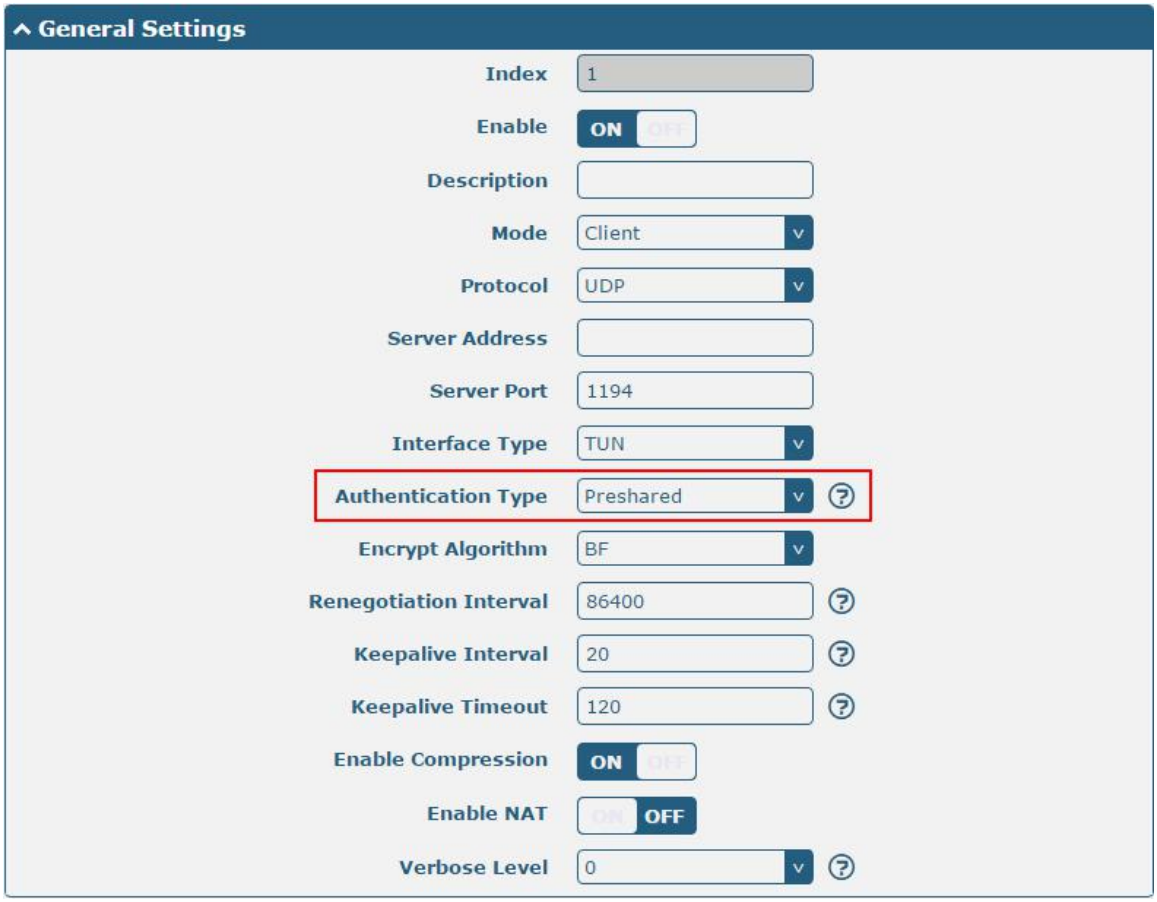
Click + to add tunnel settings. The maximum count is 3. The window is displayed as below when choosing "None" as the authentication type. By default, the mode is "Client".



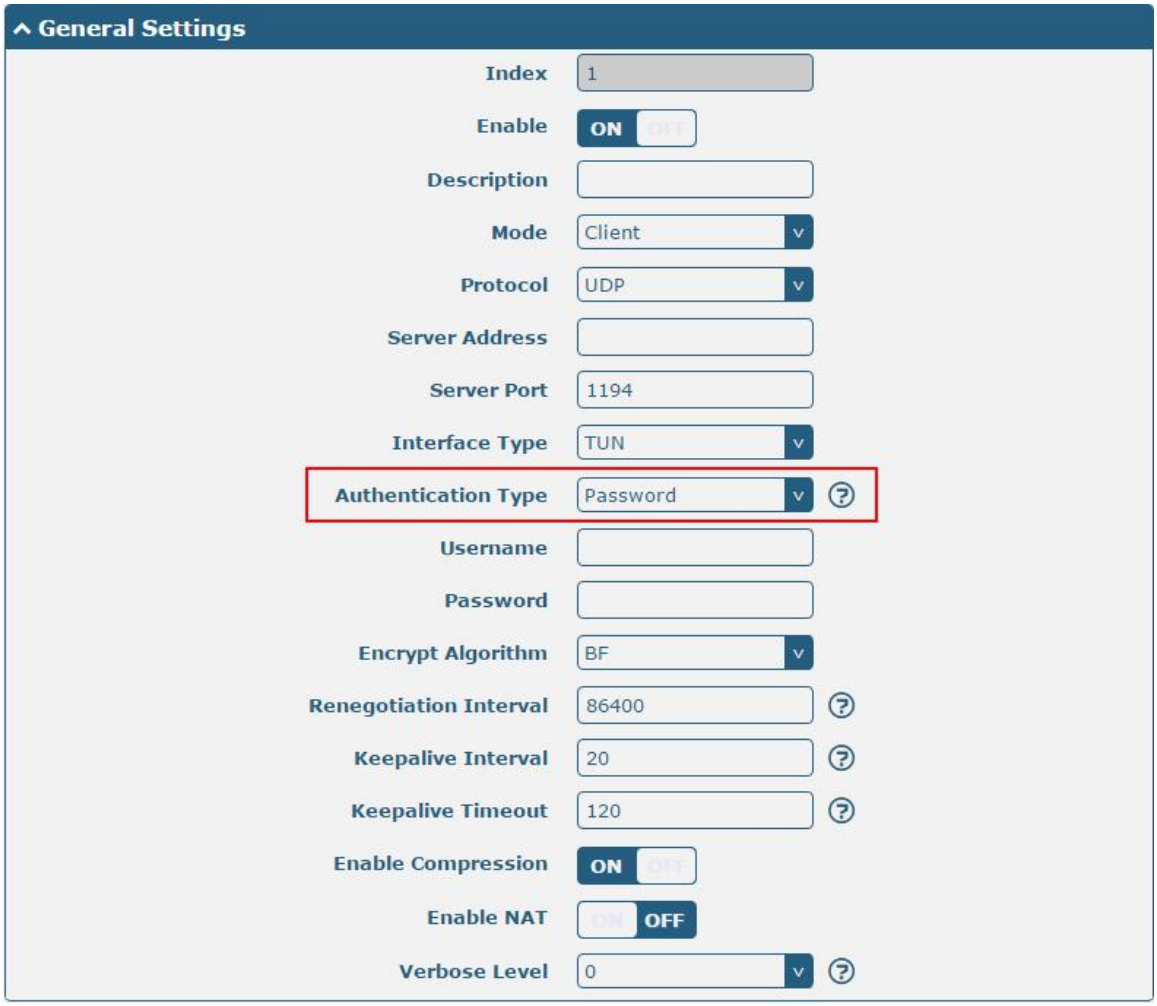
The window is displayed as below when choosing “P2P” as the mode.



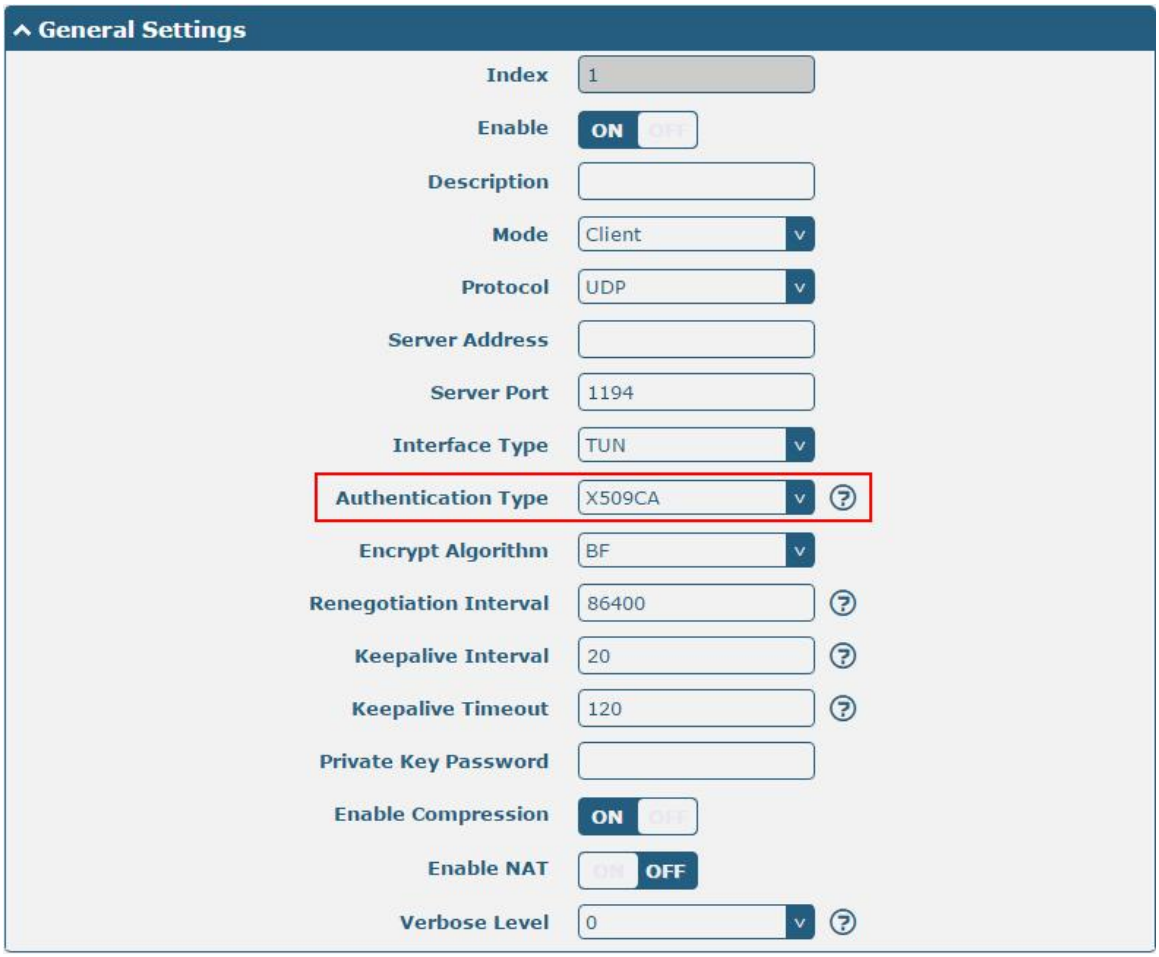
The window is displayed as below when choosing “Preshared” as the authentication type.



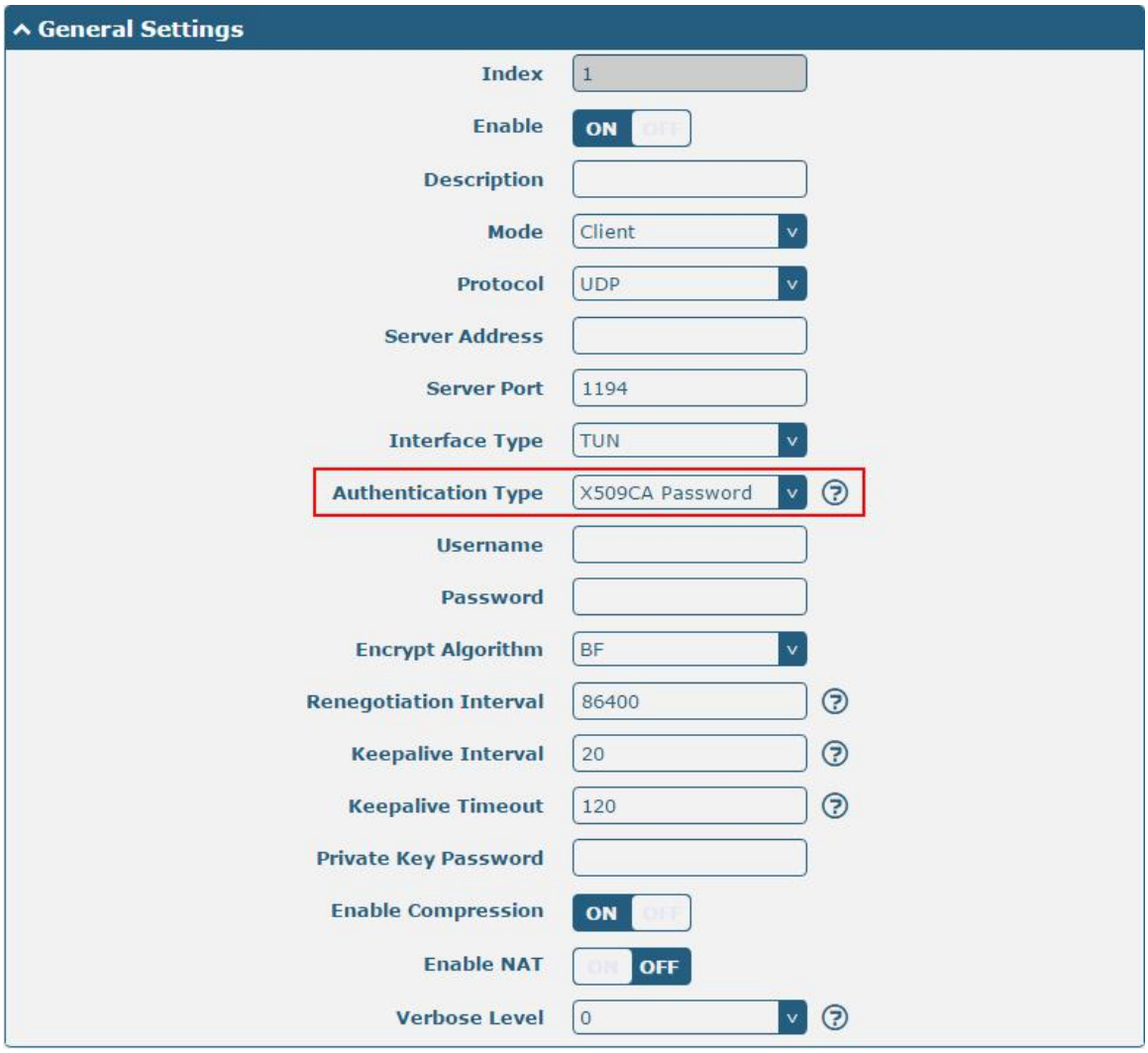
The window is displayed as below when choosing “Password” as the authentication type.



The window is displayed as below when choosing “X509CA” as the authentication type.



The window is displayed as below when choosing “X509CA Password” as the authentication type.



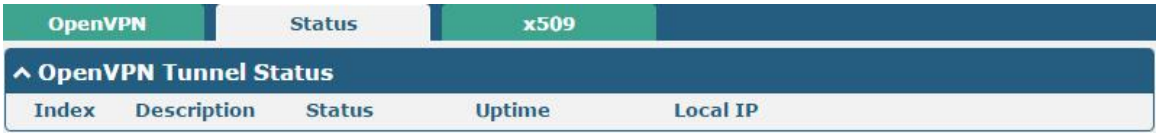
General Settings @ OpenVPN		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this OpenVPN tunnel.	ON
Description	Enter a description for this OpenVPN tunnel.	Null
Mode	Select from “P2P” or “Client”.	Client
Protocol	Select from “UDP”, “TCP-Client” or “TCP-Server”.	UDP
Server Address	Enter the end-to-end IP address or the domain of the remote OpenVPN server.	Null
Server Port	Enter the end-to-end listener port or the listening port of the OpenVPN server.	1194
Interface Type	Select from “TUN” or “TAP” which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.	TUN

General Settings @ OpenVPN		
Item	**Description**	**Default**
Authentication Type	Select from “None”, “Preshared”, “Password”, “X509CA” and “X509CA Password”. “None” and “Preshared” authentication type are only working with p2p mode.	None
Username	Enter the username used for “Password” or “X509CA Password” authentication type.	Null
Password	Enter the password used for “Password” or “X509CA Password” authentication type.	Null
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
Encrypt Algorithm	Select from “BF”, “DES”, “DES-EDE3”, “AES128”, "AES192” and “AES256”. • BF: Use 128-bit BF encryption algorithm in CBC mode • DES: Use 64-bit DES encryption algorithm in CBC mode • DES-EDE3: Use 192-bit 3DES encryption algorithm in CBC mode • AES128: Use 128-bit AES encryption algorithm in CBC mode • AES192: Use 192-bit AES encryption algorithm in CBC mode • AES256: Use 256-bit AES encryption algorithm in CBC mode	BF
Renegotiation Interval	Set the renegotiation interval. If connection failed, OpenVPN will renegotiate when the renegotiation interval reached.	86400
Keepalive Interval	Set keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Set the keepalive timeout. Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120
Private Key Password	Enter the private key password under the “X509CA” and “X509CA Password” authentication type.	Null
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the data stream of the header.	ON
Enable NAT	Click the toggle button to enable/disable the NAT option. When enabled, the source IP address of host behind router will be disguised before accessing the remote OpenVPN client.	OFF
Verbose Level	Select the level of the output log and values from 0 to 11. • 0: No output except fatal errors • 1~4: Normal usage range • 5: Output R and W characters to the console for each packet read and write • 6~11: Debug info range	0

Advanced Settings @ OpenVPN		
Item	**Description**	**Default**
Enable HMAC Firewall	Click the toggle button to enable/disable this option. Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.	OFF
Enable PKCS#12	Click the toggle button to enable/disable the PKCS#12 certificate. It is an exchange of digital certificate encryption standard, used to describe personal identity information.	OFF
Enable nsCertType	Click the toggle button to enable/disable nsCertType. Require that peer certificate was signed with an explicit nsCertType designation of "server".	OFF
Expert Options	Enter some other options of OpenVPN in this field. Each expression can be separated by a ';'.	Null

Status

This section allows you to view the status of the OpenVPN tunnel.



x509

User can upload the X509 certificates for the OpenVPN in this section.

x509		
Item	**Description**	**Default**
X509 Settings		
Tunnel Name	Choose a valid tunnel.	Tunnel 1
Certificate Files	Click on "Choose File" to locate the certificate file from your computer, and	Null

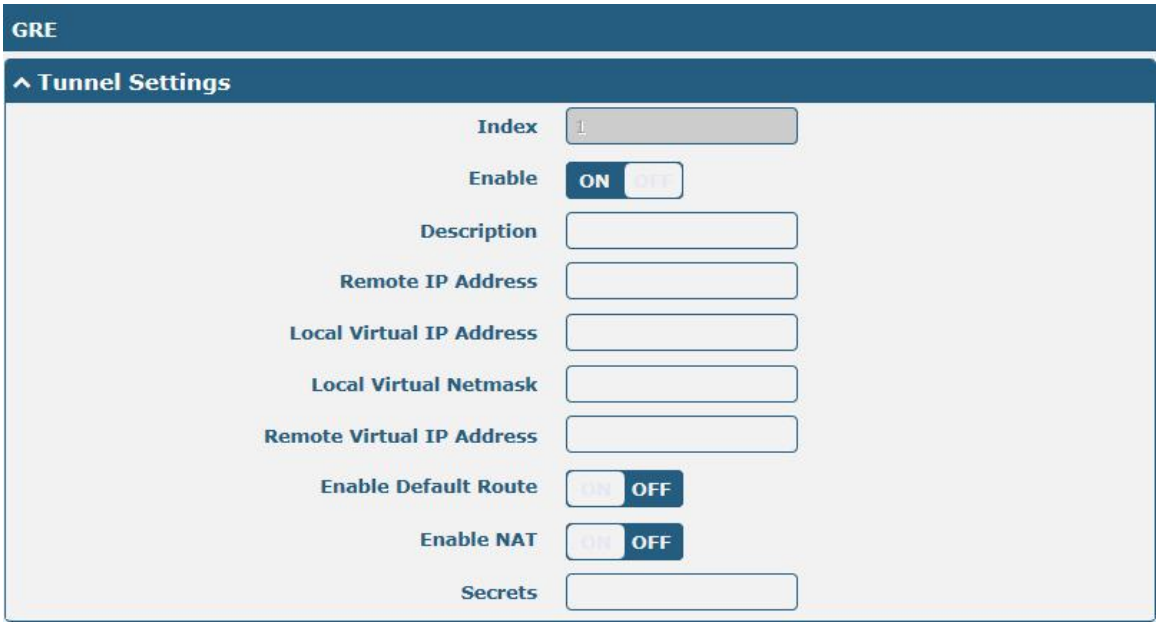
	then import this file into your router. The correct file format is displayed as follows: @ca.crt @remote.crt @local.crt @private.key @crl.pem @client.p12	
Certificate Files		
Index	Indicate the ordinal of the list.	--
Filename	Show the imported certificate's name.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

3.18 VPN > GRE

This section allows you to set the GRE and the related parameters. Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network.

GRE

Click + to add tunnel settings. The maximum count is 3.



Tunnel Settings @ GRE

Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this GRE tunnel.	ON
Description	Enter a description for this GRE tunnel.	Null
Remote IP Address	Set the remote real IP address of the GRE tunnel.	Null
Local Virtual IP Address	Set the local virtual IP address of the GRE tunnel.	Null
Local Virtual Netmask	Set the local virtual Netmask of the GRE tunnel.	Null
Remote Virtual IP Address	Set the remote virtual IP Address of the GRE tunnel.	Null
Enable Default Route	Click the toggle button to enable/disable this option. When enabled, all the traffics of the router will go through the GRE VPN.	OFF
Enable NAT	Click the toggle button to enable/disable this option. This option must be enabled when router under NAT environment.	OFF
Secrets	Set the key of the GRE tunnel.	Null

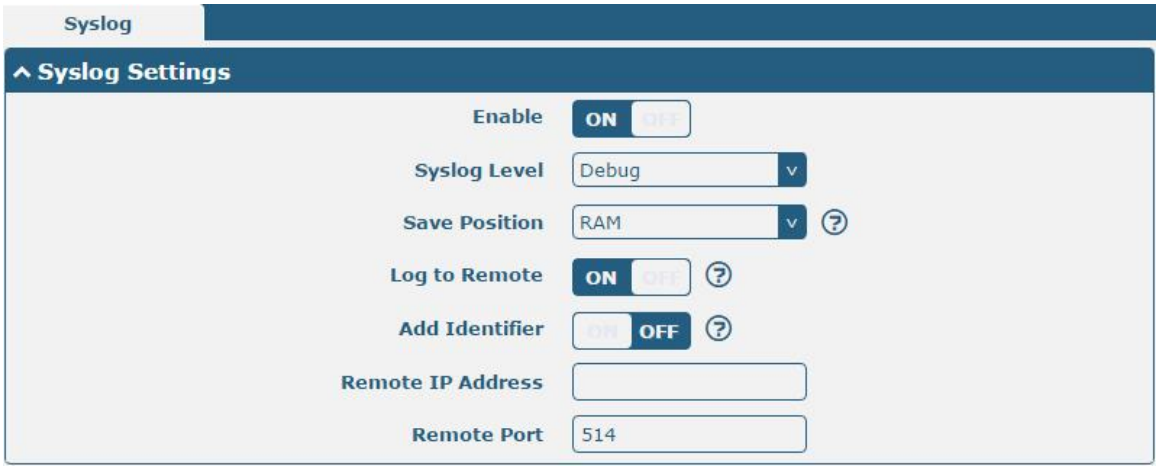
Status

This section allows you to view the status of GRE tunnel.

3.19 Services > Syslog

This section allows you to set the syslog parameters. The system log of the router can be saved in the local, also supports to be sent to remote log server and specified application debugging. By default, the “Log to Remote” option is disabled.

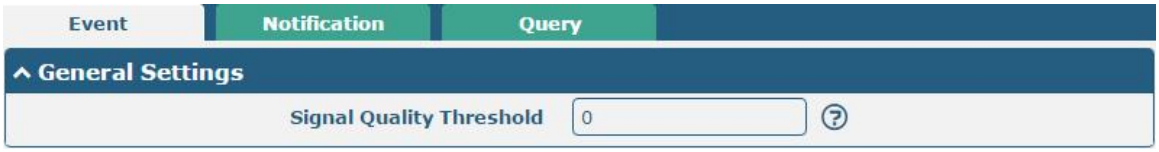
The window is displayed as below when enabling the “Log to Remote” option.



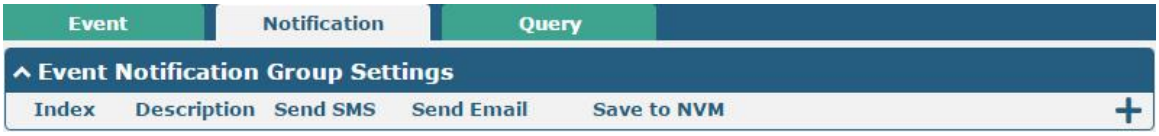
Syslog Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Syslog settings option.	OFF
Syslog Level	Select from “Debug”, “Info”, “Notice”, “Warning” or “Error”, which from low to high. The lower level will output more syslog in details.	Debug
Save Position	Select the save position from “RAM”, “NVM” or “Console”. Choose “RAM”. The data will be cleared after reboot. **Note**: It's not recommended that you save syslog to NVM (Non-Volatile Memory) for a long time.	RAM
Log to Remote	Click the toggle button to enable/disable this option. Enable to allow router sending syslog to the remote syslog server. You need to enter the IP and Port of the syslog server.	OFF
Add Identifier	Click the toggle button to enable/disable this option. When enabled, you can add serial number to syslog message which used for loading Syslog to RobustLink.	OFF
Remote IP Address	Enter the IP address of syslog server when enabling the “Log to Remote” option.	Null
Remote Port	Enter the port of syslog server when enabling the “Log to Remote” option.	514

3.20 Services > Event

This section allows you to set the event parameters. Event feature provides an ability to send alerts by SMS or Email when certain system events occur.



General Settings @ Event		
Item	**Description**	**Default**
Signal Quality Threshold	Set the threshold for signal quality. Router will generate a log event when the actual threshold is less than the specified threshold. 0 means disable this option.	0


Event
Notification
Query
Event Notification Group Settings
Index
Description
Send SMS
Send Email
Save to NVM

Click + button to add an Event parameters.

General Settings @ Notification		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this group.	Null
Sent SMS	Click the toggle button to enable/disable this option. When enabled, the router will send notification to the specified phone numbers via SMS if event occurs. Set the related phone number in “3.23 Services > Email”, and use ‘;’to separate each number.	OFF
Phone Number	Enter the phone numbers used for receiving event notification. Use a semicolon (;) to separate each number.	Null
Send Email	Click the toggle button to enable/disable this option. When enabled, the router will send notification to the specified email box via Email if event occurs. Set the related email address in “3.23 Services > Email”.	OFF
Email Address	Enter the email addresses used for receiving event notification. Use a space to separate each address.	Null
Save to NVM	Click the toggle button to enable/disable this option. Enable to save event to nonvolatile memory.	OFF

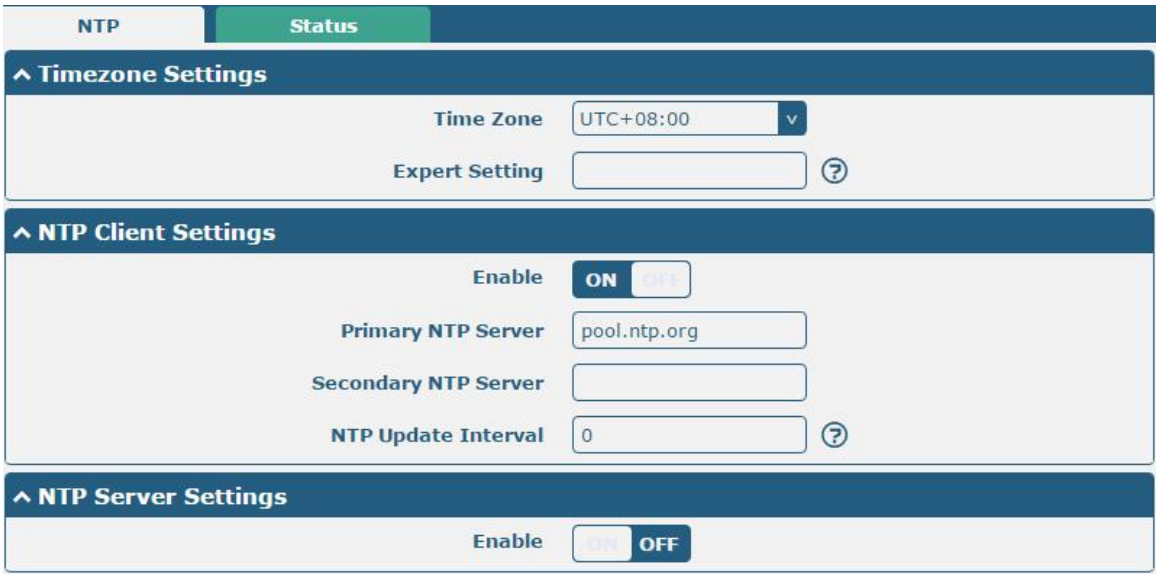
In the following window you can query various types of events record. Click **Refresh** to query filtered events while click **Clear** to clear the event records in the window.

Event Details

Item	Description	Default
Save Position	Select the events' save position from "RAM" or "NVM". • RAM: Random-access memory • NVM: Non-Volatile Memory	RAM
Filter Message	Enter the filtering message based on the keywords set by users. Click the "Refresh" button, the filtered event will be displayed in the follow box. Use "&" to separate more than one filter message, such as message1&message2.	Null

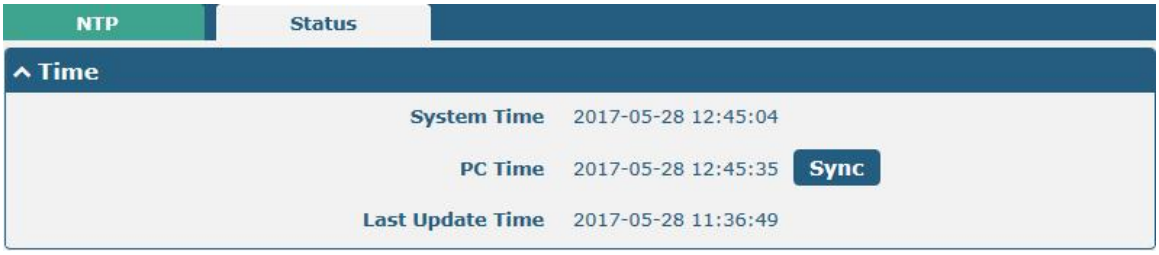
3.21 Services > NTP

This section allows you to set the related NTP (Network Time Protocol) parameters, including Time zone, NTP Client and NTP Server.



NTP		
Item	**Description**	**Default**
Timezone Settings		
Time Zone	Click the drop down list to select the time zone you are in.	UTC +08:00
Expert Setting	Specify the time zone with Daylight Saving Time in TZ environment variable format. The Time Zone option will be ignored in this case.	Null
NTP Client Settings		
Enable	Click the toggle button to enable/disable this option. Enable to synchronize time with the NTP server.	ON
Primary NTP Server	Enter primary NTP Server's IP address or domain name.	pool.ntp.org
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.	Null
NTP Update interval	Enter the interval (minutes) synchronizing the NTP client time with the NTP server's. Minutes wait for next update, and 0 means update only once.	0
NTP Server Settings		
Enable	Click the toggle button to enable/disable the NTP server option.	OFF

This window allows you to view the current time of router and also synchronize the router time. Click Sync button to synchronize the router time with the PC's.



3.22 Services > SMS

This section allows you to set SMS parameters. Router supports SMS management, and user can control and configure their routers by sending SMS. For more details about SMS control, refer to **4.1.2 SMS Remote Control**.

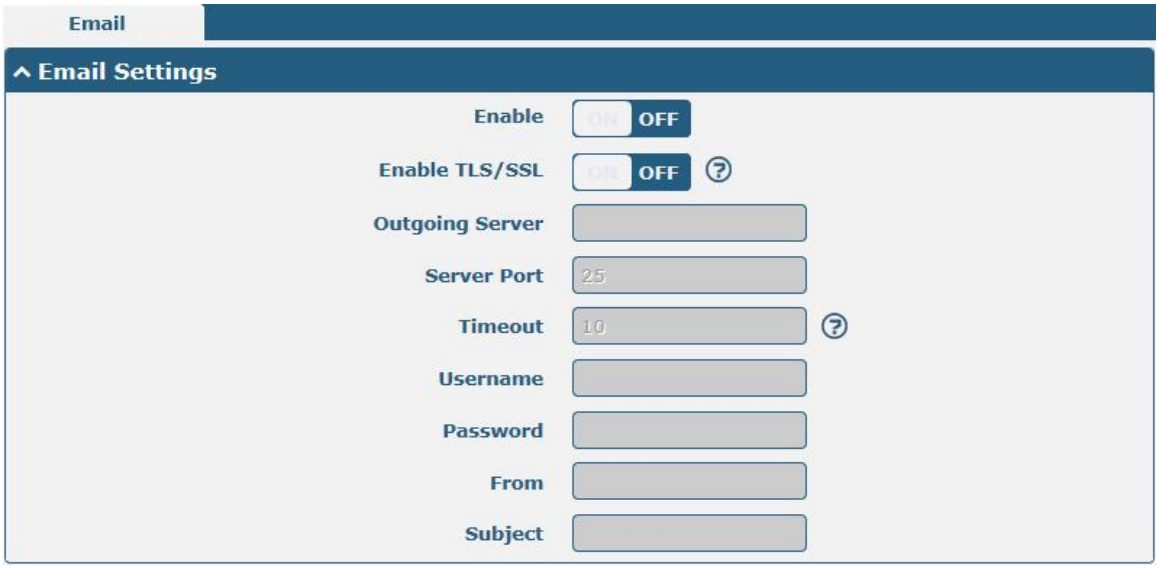
SMS Management Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the SMS Management option. **Note**: If this option is disabled, the SMS configuration is invalid.	ON
Authentication Type	Select Authentication Type from "Password", "Phonenum" or "Both". • Password: Use the same username and password as WEB manager for authentication. For example, the format of the SMS should be "username: password; cmd1; cmd2; …" **Note:** Set the WEB manager password in **System > User Management** section. • Phonenum: Use the Phone number for authentication, and user should set the Phone Number that is allowed for SMS management. The format of the SMS should be "cmd1; cmd2; …" • Both: Use both the "Password" and "Phonenum" for authentication. User should set the Phone Number that is allowed for SMS management. The format of the SMS should be "username: password; cmd1; cmd2; …"	Password
Phone Number	Set the phone number used for SMS management, and use '; 'to separate each number.	Null

User can test the current SMS service whether it is available in this section.

SMS Testing		
Item	**Description**	**Default**
Phone Number	Enter the specified phone number which can receive the SMS from router.	Null
Message	Enter the message that router will send it to the specified phone number.	Null
Result	The result of the SMS test will be displayed in the result box.	Null
Send	Click the button to send the test message.	--

3.23 Services > Email

Email function supports to send the event notifications to the specified recipient by ways of email.

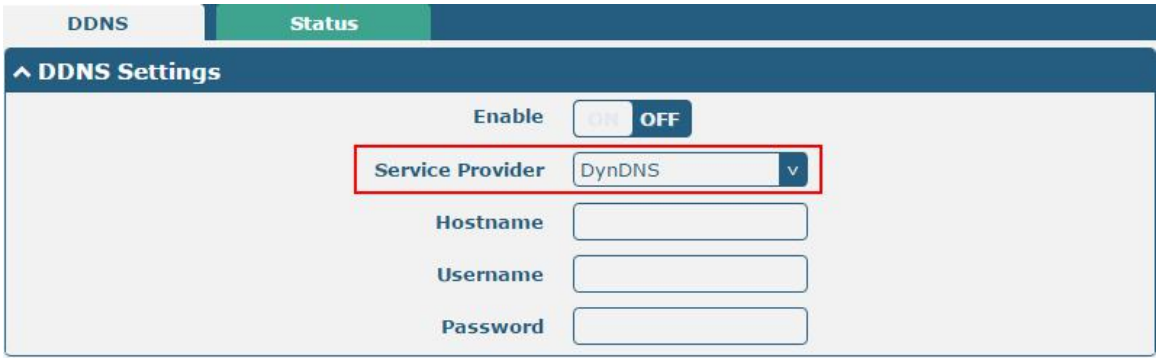


Email Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Email option.	OFF
Enable TLS/SSL	Click the toggle button to enable/disable the TLS/SSL option.	OFF
Outgoing server	Enter the SMTP server IP Address or domain name.	Null

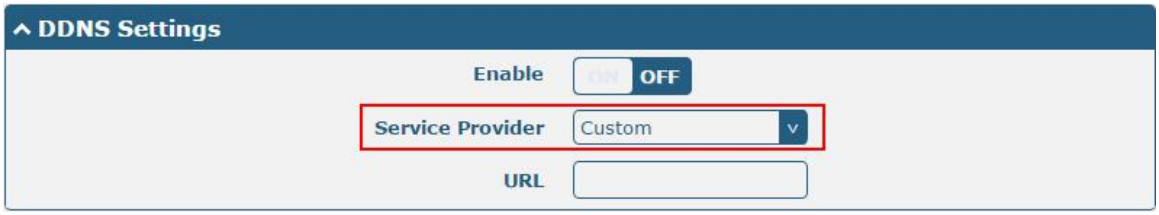
Email Settings		
Item	**Description**	**Default**
Server port	Enter the SMTP server port.	25
Timeout	Set the max time for sending email to SMTP server. When the server doesn't receive the email over this time, it will try to resend.	10
Username	Enter the username which has been registered from SMTP server.	Null
Password	Enter the password of the username above.	Null
From	Enter the source address of the email.	Null
Subject	Enter the subject of this email.	Null

3.24 Services > DDNS

This section allows you to set the DDNS parameters. The Dynamic DNS function allows you to alias a dynamic IP address to a static domain name, allows you whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP. The service provider defaults to "DynDNS", as shown below.



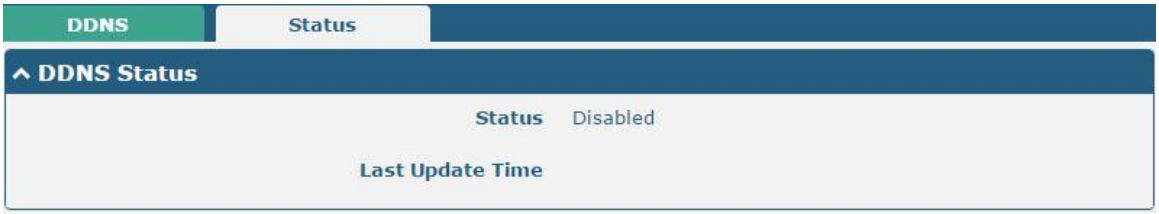
When "Custom" service provider chosen, the window is displayed as below.



DDNS Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the DDNS option.	OFF
Service Provider	Select the DDNS service from "DynDNS", "NO-IP", "3322" or "Custom". **Note:** the DDNS service only can be used after registered by Corresponding service provider.	DynDNS
Hostname	Enter the hostname provided by the DDNS server.	Null

Username	Enter the username provided by the DDNS server.	Null
Password	Enter the password provided by the DDNS server.	Null
URL	Enter the URL customized by user.	Null

Click “Status” bar to view the status of the DDNS.



DDNS Status	
Item	**Description**
Status	Display the current status of the DDNS.
Last Update Time	Display the date and time for the DDNS was last updated successfully.

3.25 Services > SSH

Router supports SSH password access and secret-key access.

SSH Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable this option. When enabled, you can access the router via SSH.	ON
Port	Set the port of the SSH access.	22
Disable Password Logins	Click the toggle button to enable/disable this option. When enabled, you cannot use username and password to access the router via SSH. In this case, only the key can be used for login.	OFF

Import Authorized Keys	
Item	**Description**

Authorized Keys	Click on “Choose File” to locate an authorized key from your computer, and then click “Import” to import this key into your router. **Note**: This option is valid when enabling the password logins option.

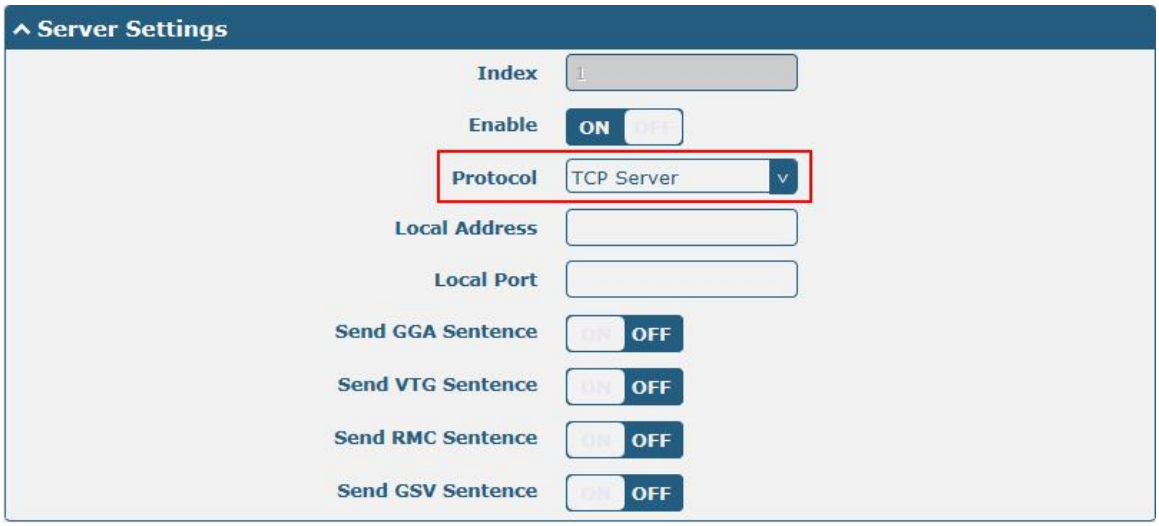
3.26 Services > GPS

This section allows you to set the GPS setting parameters.

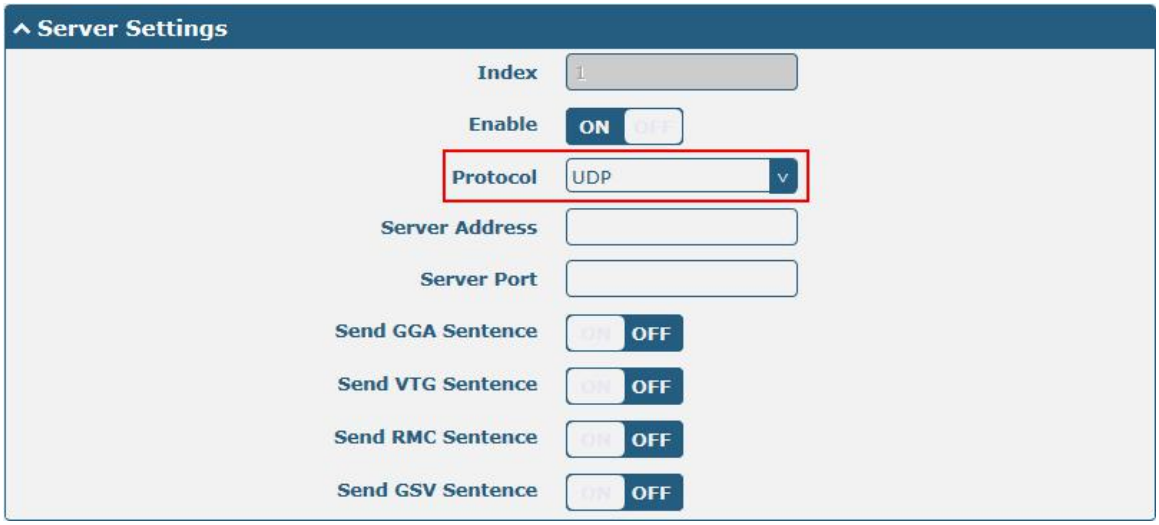
General Settings @ GPS		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the GPS option.	ON

The window is displayed as below when choosing “TCP Client” as the protocol.

The window is displayed as below when choosing “TCP Server” as the protocol.



The window is displayed as below when choosing “UDP” as the protocol.

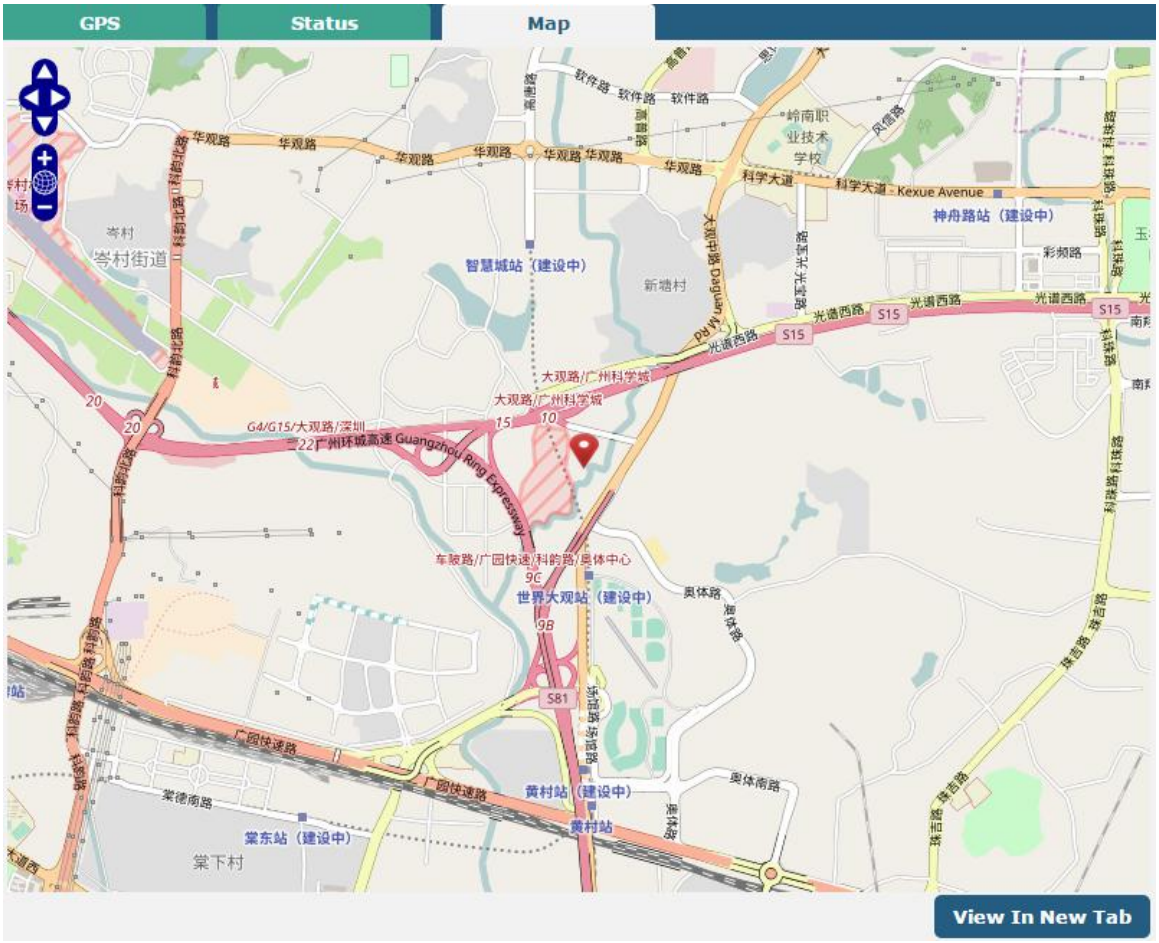


Server Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable the GPS server settings.	ON
Protocol	Select from “TCP Client”, “TCP Server” or “UDP”.	TCP Client
Server Address @TCP Client	Set the address of the TCP Client.	Null
Server Port @TCP Client	Set the port of the remote TCP Server.	Null
Local Address	Set the local address when the router set as a TCP Server.	Null
Local Port	Set the local port when the router set as a TCP Server.	Null
Server Address @ UDP	Set the address of the TCP Server.	Null
Server Port @ UDP	Set the port of the remote TCP Server.	Null
Send GGA Sentence	Send GGA information in NMEA format.	OFF

Server Settings		
Item	**Description**	**Default**
Send VTG Sentence	Send VTG information in NMEA format.	OFF
Send RMC Sentence	Send RMC information in NMEA format.	OFF
Send GSV Sentence	Send GSV information in NMEA format.	OFF

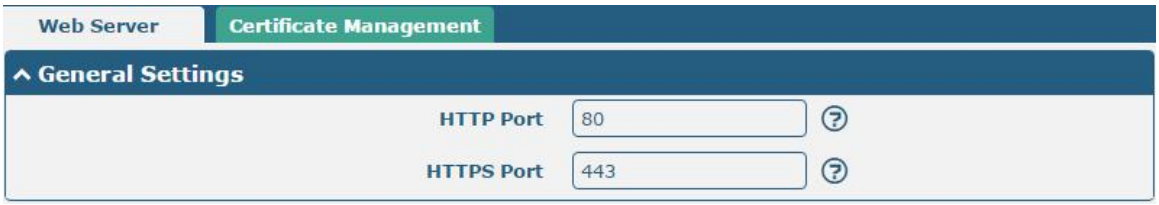
GPS Status	
Item	**Description**
Status	Show the GPS Status. GPS status includes “NO Fix”, “2D Fix” and “3D Fix”.
UTC Time	Show the UTC of satellites, which is world unified time, not local time.
Latitude	Show the latitude status of router.
Longitude	Show the longitude status of router.
Altitude	Show the altitude status of router.
Speed	Show the horizontal speed of router.

Click “Map” column to view the current location of the router.



3.27 Services > Web Server

This section allows you to modify the parameters of Web Server.



General Settings @ Web Server		
Item	**Description**	**Default**
HTTP Port	Enter the HTTP port number you want to change in router’s Web Server. On a Web server, port 80 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTP Port number except 80, only adding that port number then you can login router’s Web Server.	80
HTTPS Port	Enter the HTTPS port number you want to change in router’s Web Server. On a Web server, port 443 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTPS Port	443

	number except 443, only adding that port number then you can login router's Web Server. **Note**: HTTPS is more secure than HTTP. In many cases, clients may be exchanging confidential information with a server, which needs to be secured in order to prevent unauthorized access. For this reason, HTTP was developed by Netscape corporation to allow authorization and secured transactions.	

This section allows you to import the certificate file into the route.

Import Certificate		
Item	**Description**	**Default**
Import Type	Select from "CA" and "Private Key". • CA: a digital certificate issued by CA center • Private Key: a private key file	CA
HTTPS Certificate	Click on "Choose File" to locate the certificate file from your computer, and then click "Import" to import this file into your router.	--

3.28 Services > Advanced

This section allows you to set the Advanced and parameters.

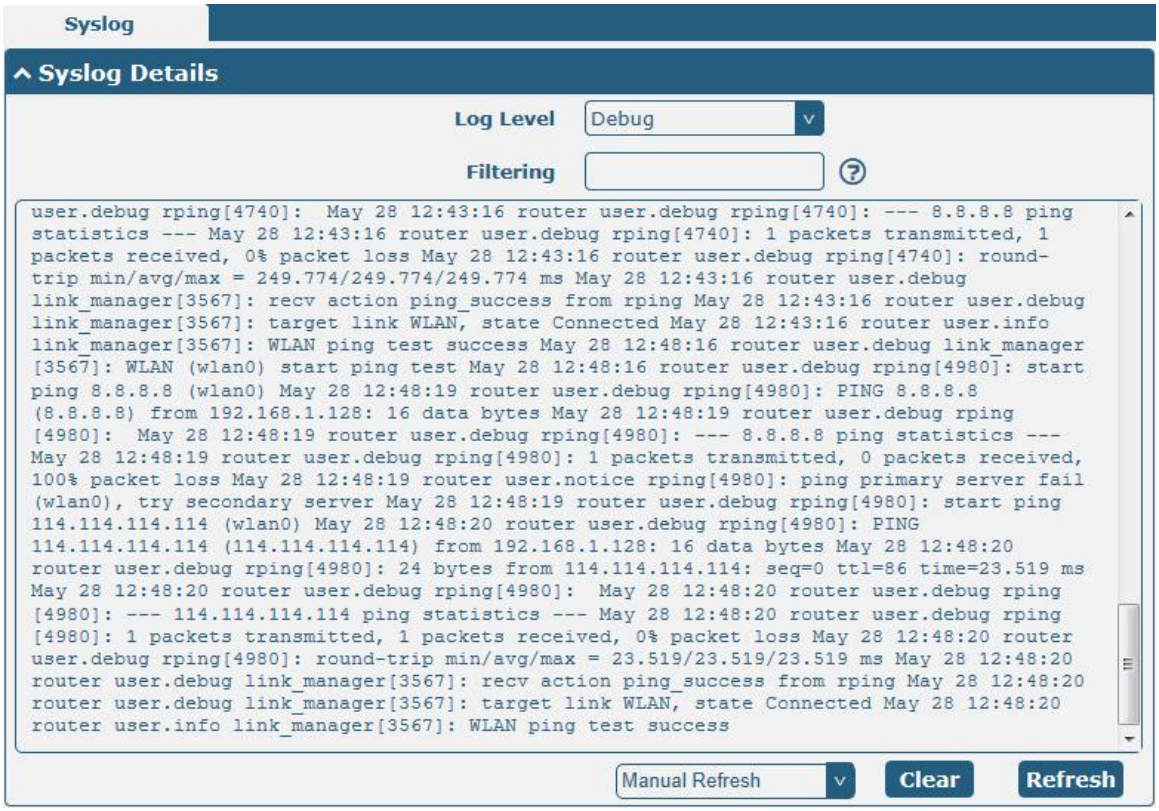
System Settings		
Item	**Description**	**Default**
Device Name	Set the device name to distinguish different devices you have installed; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	router
User LED Type	Specify the display type of your USR LED. Select from "None", "OpenVPN", "IPSec" or "WiFi".	None

	• None: Meaningless indication, and the LED is off • OpenVPN: USR indicator showing the OpenVPN status • IPSec: USR indicator showing the IPsec status • WiFi: USR indicator showing the WiFi status **Note**: For more details about USR indicator, see "2.1 LED Indicators".	

Periodic Reboot Settings		
Item	**Description**	**Default**
Periodic Reboot	Set the reboot period of the router. 0 means disable.	0
Daily Reboot Time	Set the daily reboot time of the router. You should follow the format as HH: MM, in 24h time frame, otherwise the data will be invalid. Leave it empty means disable.	Null

3.29 System > Debug

This section allows you to check and download the syslog details.



Syslog		
Item	**Description**	**Default**
Syslog Details		
Log Level	Select from "Debug", "Info", "Notice", "Warn", "Error" which from low to high. The lower level will output more syslog in detail.	Debug
Filtering	Enter the filtering message based on the keywords. Use "&" to separate more than one filter message, such as "keyword1&keyword2".	Null
Refresh	Select from "Manual Refresh", "5 Seconds", "10 Seconds", "20 Seconds" or "30 Seconds". You can select these intervals to refresh the log information displayed in the follow box. If selecting "manual refresh", you should click the refresh button to refresh the syslog.	Manual Refresh
Clear	Click the button to clear the syslog.	--
Refresh	Click the button to refresh the syslog.	--
Syslog Files		
Syslog Files List	It can show at most 5 syslog files in the list, the files' name range from message0 to message 4. And the newest syslog file will be placed on the top of the list.	--
System Diagnosing Data		
Generate	Click to generate the syslog diagnosing file.	--
Download	Click to download system diagnosing file.	--

3.30 System > Update

This section allows you to upgrade the firmware of your router. Click **System > Update > System Update**, and click on "Choose File" to locate the firmware file to be used for the upgrade. Once the latest firmware has been chosen, click "Update" to start the upgrade process. The upgrade process may take several minutes. Do not turn off your Router during the firmware upgrade process.

Note: To access the latest firmware file, please contact your technical support engineer.

System Update

Item	Description	Default
System Update	Click Choose File button to select the correct firmware in your PC, and then click Update button to update. After updating successfully, you need to click "save and apply", and then reboot the router to take effect.	Null

3.31 System > APP Center

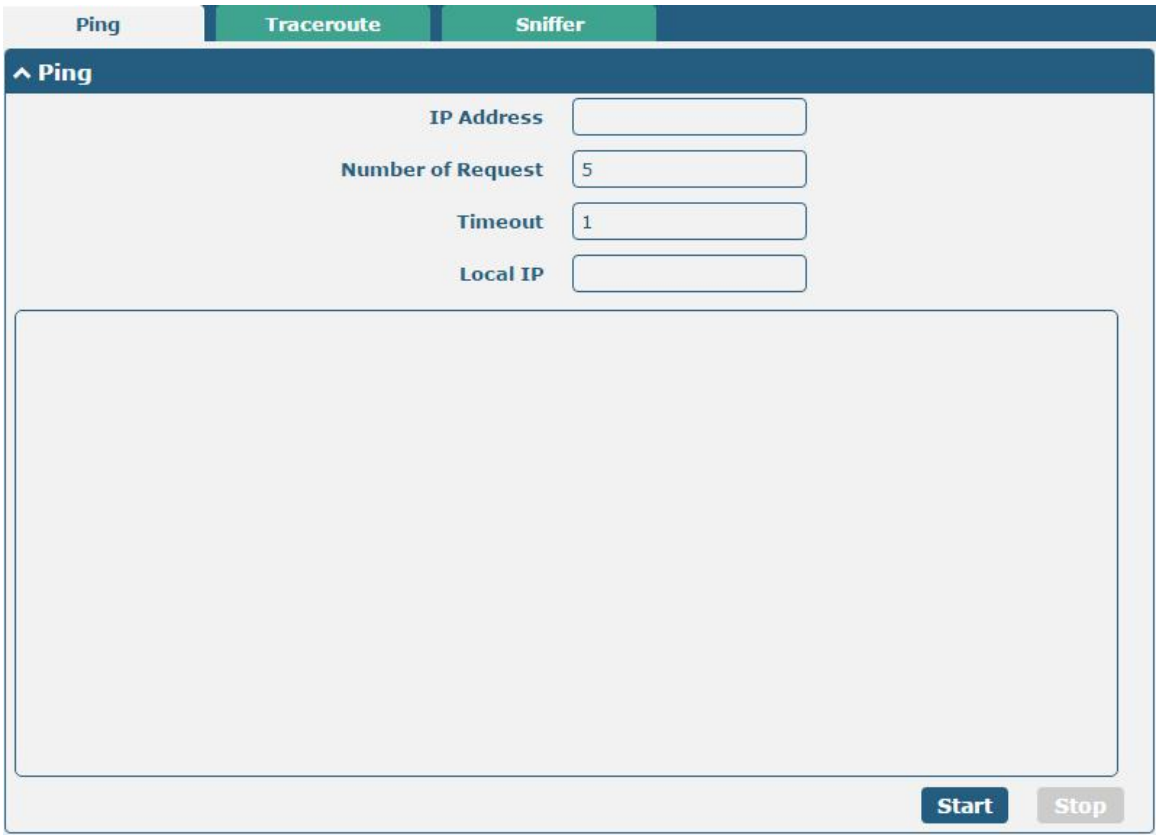
This section allows you to add some required or customized applications to the router. Import and install your applications to the APP Center, and reboot the device according to the system prompts. Each installed application will be displayed under the "Services" menu, while other applications related to VPN will be displayed under the "VPN" menu.

Note: After importing the applications to the router, the page display may have a slight delay due to the browser cache. It is recommended that you clear the browser cache first and log in the router again.

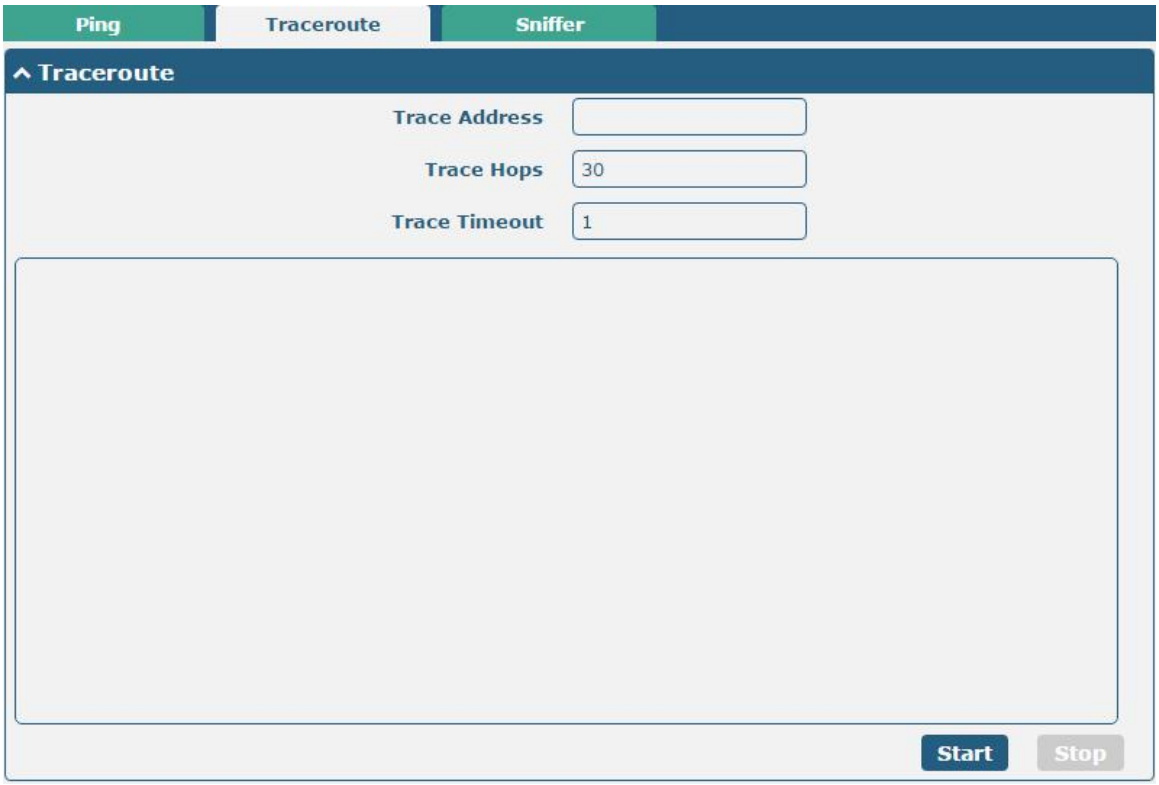
App Center		
Item	**Description**	**Default**
App Install		
File	Click on "Choose File" to locate the App file from your computer, and then click Install to import this file into your router. **Note**: File format should be *xxx.rpk*, e.g. *R3000 Quad-robustlink-1.0.0.rpk*.	--
Installed Apps		
Index	Indicate the ordinal of the list.	--
Name	Show the name of the App.	Null
Version	Show the version of the App.	Null
Status	Show the status of the App.	Null
Description	Show the description for this App.	Null

3.32 System > Tools

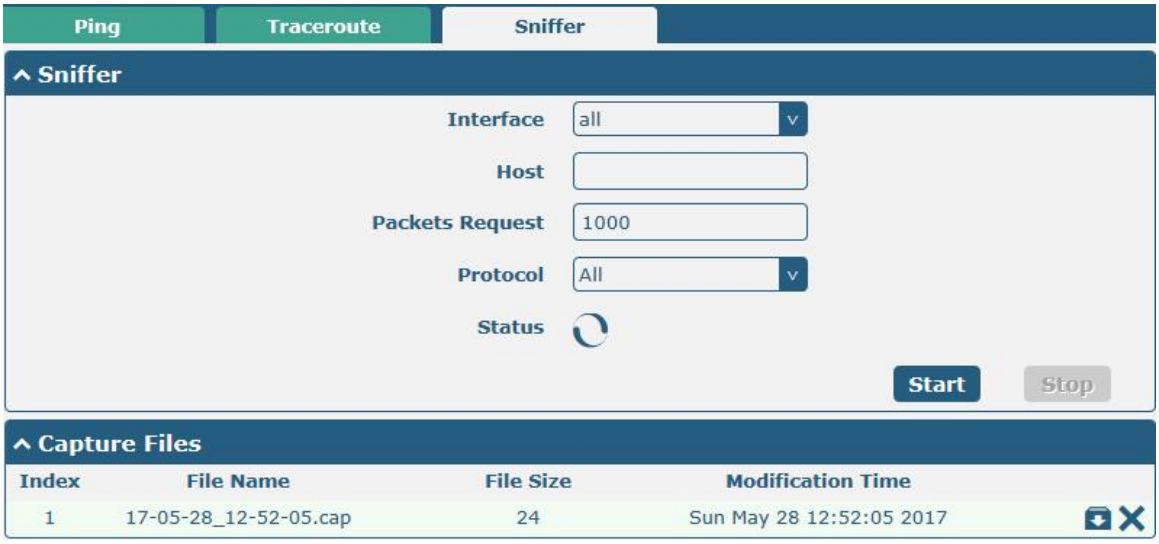
This section provides users three tools: Ping, Traceroute and Sniffer.



Ping		
Item	**Description**	**Default**
IP address	Enter the ping's destination IP address or destination domain.	Null
Number of Requests	Specify the number of ping requests.	5
Timeout	Specify the timeout of ping requests.	1
Local IP	Specify the local IP from cellular WAN, Ethernet WAN or Ethernet LAN. Null stands for selecting local IP address from these three automatically.	Null
Start	Click this button to start ping request, and the log will be displayed in the follow box.	Null
Stop	Click this button to stop ping request.	--



Traceroute		
Item	**Description**	**Default**
Trace Address	Enter the trace's destination IP address or destination domain.	Null
Trace Hops	Specify the max trace hops. Router will stop tracing if the trace hops has met max value no matter the destination has been reached or not.	30
Trace Timeout	Specify the timeout of Traceroute request.	1
Start	Click this button to start Traceroute request, and the log will be displayed in the follow box.	--
Stop	Click this button to stop Traceroute request.	--

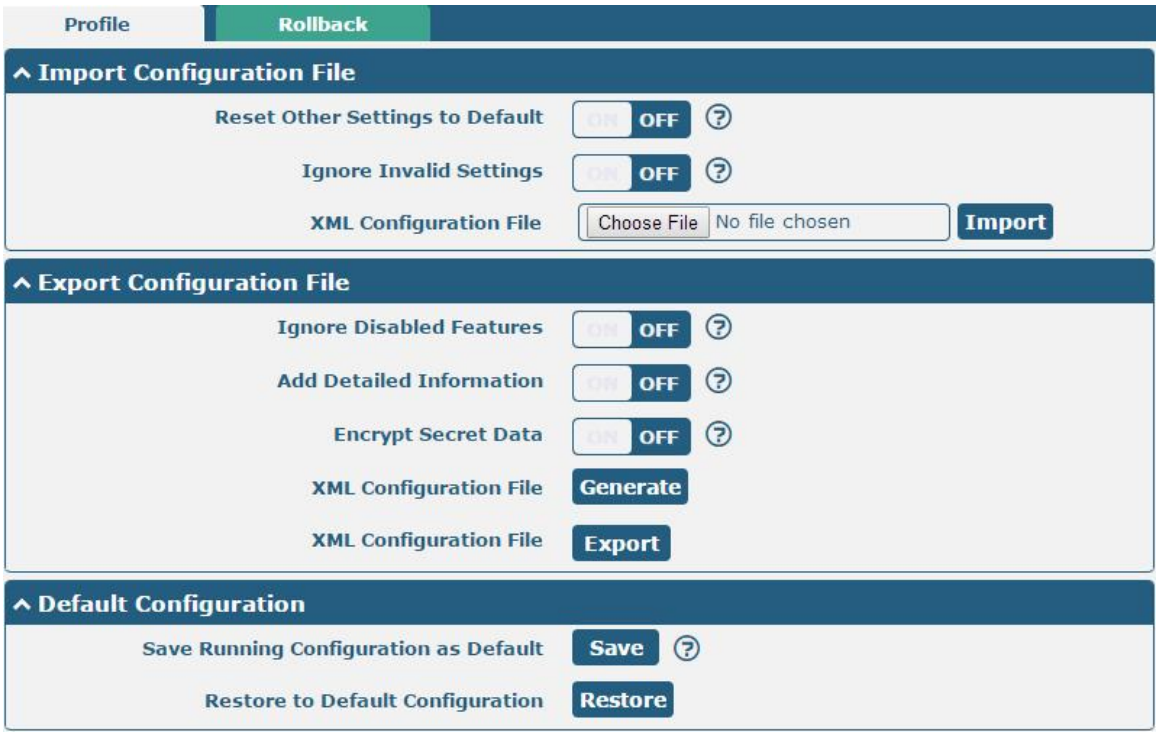


Sniffer

Item	Description	Default
Interface	Choose the interface according to your Ethernet configuration.	All
Host	Filter the packet that contain the specify IP address.	Null
Packets Request	Set the packet number that the router can sniffer at a time.	1000
Protocol	Select from “All”, “IP”, “TCP”, “UDP” and “ARP”.	All
Port	Set the port number for TCP or UDP that is used in sniffer.	Null
Status	Show the current status of sniffer.	Null
Start	Click this button to start the sniffer.	--
Stop	Click this button to stop the sniffer. Once you click this button, a new log file will be displayed in the following List.	--
Capture Files	Every times of sniffer log will be saved automatically as a new file. You can find the file from this Sniffer Traffic Data List and click to download the log, click to delete the log file. It can cache a maximum of 5 files.	Null

3.33 System > Profile

This section allows you to import or export the configuration file, and restore the router to factory default setting.



Profile		
Item	**Description**	**Default**
Import Configuration File		
Reset Other Settings to Default	Click the toggle button as “ON” to return other parameters to default settings.	OFF
Ignore Invalid Settings	Click the toggle button as “OFF” to ignore invalid settings.	OFF
XML Configuration File	Click on Choose File to locate the XML configuration file from your	--

	computer, and then click **Import** to import this file into your router.	
Export Configuration File		
Ignore Disabled Features	Click the toggle button as "OFF" to ignore the disabled features.	OFF
Add Detailed Information	Click the toggle button as "On" to add detailed information.	OFF
Encrypt Secret Data	Click the toggle button as "ON" to encrypt the secret data.	OFF
XML Configuration File	Click **Generate** button to generate the XML configuration file, and click **Export** to export the XML configuration file.	--
Default Configuration		
Save Running Configuration as Default	Click this button to save the current running parameters as default configuration.	--
Restore to Default Configuration	Click this button to restore the factory defaults.	--

Rollback		
Item	**Description**	**Default**
Configuration Rollback		
Save as a Rollbackable Archive	Create a save point manually. Additionally, the system will create a save point every day automatically if configuration changes.	--
Configuration Archive Files		
Configuration Archive Files	View the related information about configuration archive files, including name, size and modification time.	--

3.34 System > User Management

This section allows you to change your username and password, and create or manage user accounts. One router has only one super user who has the highest authority to modify, add and manage other common users.

Note: Your new password must be more than 5 character and less than 32 characters and may contain numbers, upper and lowercase letters, and standard symbols.

Super User Settings		
Item	**Description**	**Default**
Old Username	Enter the old username of your router. The default is “admin”.	Null
New Username	Enter a new username you want to create; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	Null
Old Password	Enter the old password of your router. The default is “admin”.	Null
New Password	Enter a new password you want to create; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	Null
Confirm Password	Enter the new password again to confirm.	Null

Click + button to add a new common user. The maximum rule count is 5.

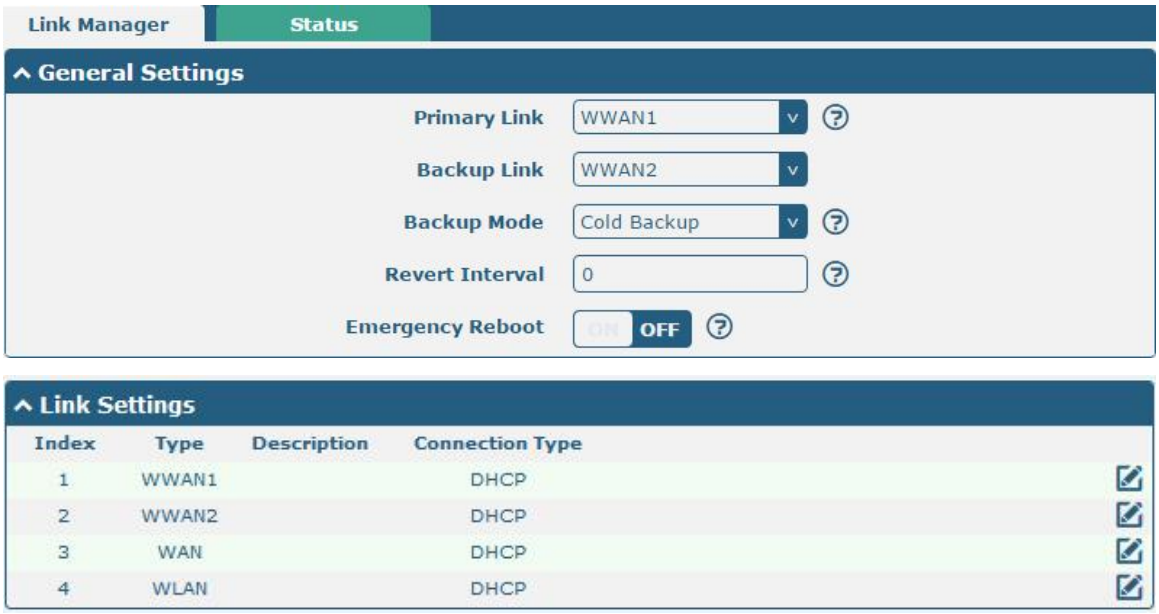
Common User Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Role	Select from “Visitor” and “Editor”. • Visitor: Users only can view the configuration of router under this level • Editor: Users can view and set the configuration of router under this level	Visitor
Username	Set the Username; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	Null
Password	Set the password which at least contains 5 characters; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	Null

Chapter 4 Configuration Examples

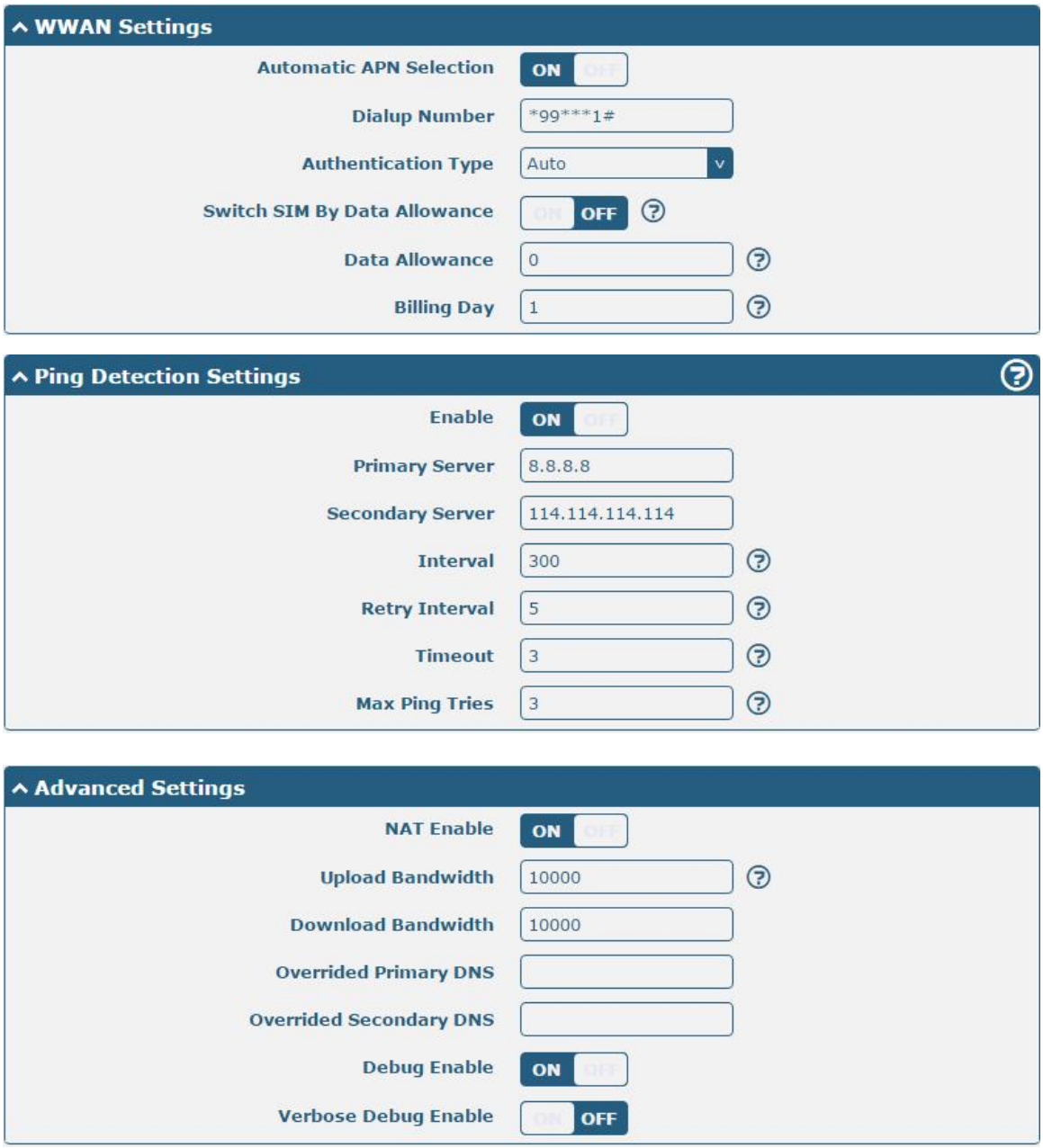
4.1 Cellular

4.1.1 Cellular Dial-Up

This section shows you how to configure the primary and backup SIM card for Cellular Dial-up. Connect the router correctly and insert two SIM, then open the configuration page. Under the homepage menu, click **Interface > Link Manager > Link Manager > General Settings**, choose “WWAN1” as the primary link, “WWAN2” as the backup link and “Cold Backup” as the backup mode.

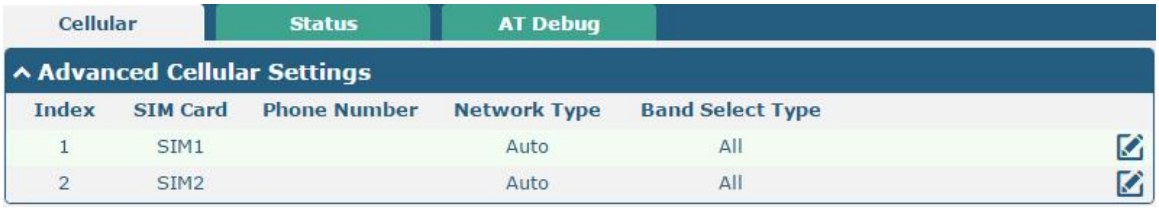


Click the edit button of WWAN1 to set its parameters according to the current ISP.

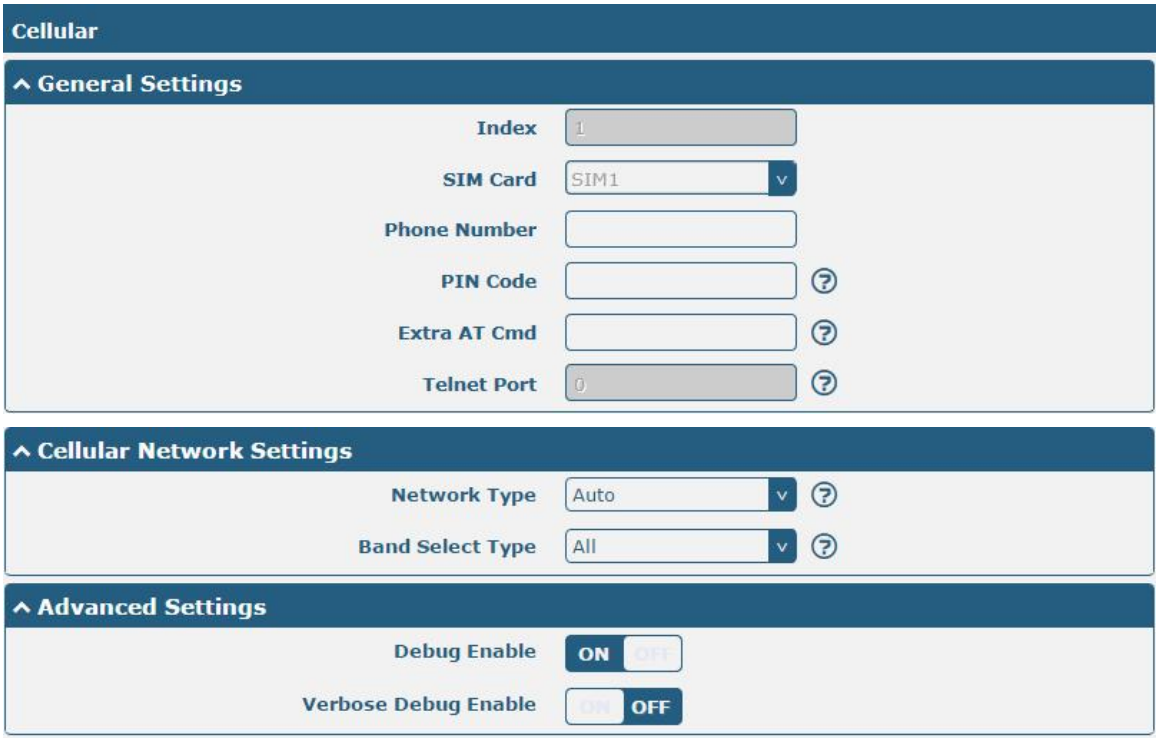


When finished, click **Submit > Save & Apply** for the configuration to take effect.

The window is displayed below by clicking **Interface > Cellular > Advanced Cellular Settings**.



Click the edit button of SIM1 to set its parameters according to your application request.



When finished, click **Submit > Save & Apply** for the configuration to take effect.

4.1.2 SMS Remote Control

R3000 Quad supports remote control via SMS. You can use following commands to get the status of the router, and set all the parameters of the router. There are three authentication types for SMS control. You can select from "Password", "Phonenum" or "Both".

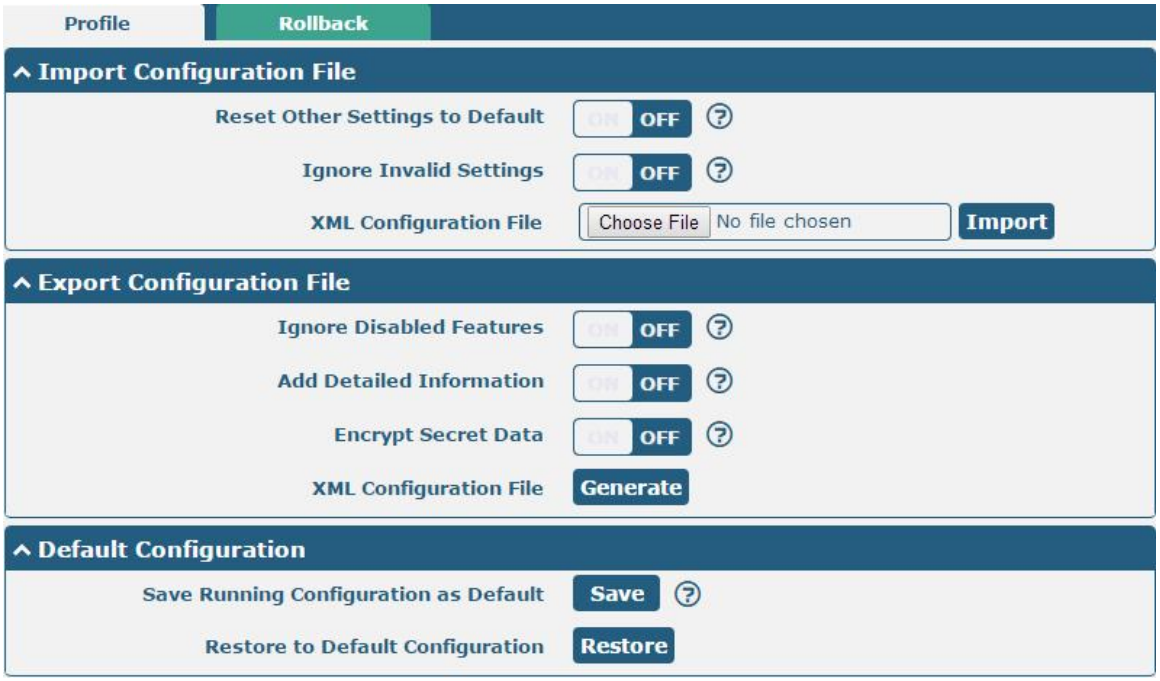
An SMS command has the following structure:

1. Password mode—Username: Password;cmd1;cmd2;cmd3; …cmdn (available for every phone number).
2. Phonenum mode--cmd1; cmd2; cmd3; … cmdn (available when the SMS was sent from the phone number which had been added in router's phone group).
3. Both mode-- Username: Password;cmd1;cmd2;cmd3; …cmdn (available when the SMS was sent from the phone number which had been added in router's phone group).

SMS command Explanation:

1. User name and Password: Use the same username and password as WEB manager for authentication.
2. cmd1, cmd2, cmd3 to Cmdn, the command format is the same as the CLI command, more details about CLI cmd please refer to **Chapter 5 Introductions for CLI**.

   Note: Download the configure XML file from the configured web browser. The format of SMS control command can refer to the data of the XML file.
   Go to **System > Profile > Export Configuration File**, click **Generate** to generate the XML file and click **Export** to export the XML file.



XML command:

```
<lan >
<network max_entry_num="2" >
<id > 1</id >
<interface > lan0</interface >
<ip > 172.16.7.29</ip >
<netmask > 255.255.0.0</netmask >
<mtu > 1500</mtu >
```

SMS cmd:

set lan network 1 interface lan0
set lan network 1 ip 172.16.7.29
set lan network 1 netmask 255.255.0.0
set lan network 1 mtu 1500

3. The semicolon character (';') is used to separate more than one commands packed in a single SMS.
4. E.g.

admin:admin;status system

In this command, username is "admin", password is "admin", and the function of the command is to get the system status.

SMS received:

hardware_version = 1.0
firmware_version = "3.0.0"
kernel_version = 4.1.0
device_model = R3000 Quad
serial_number = 10201726051044
system_uptime = "0 days, 00:10:58"
system_time = "Sun May 28 11:46:34 2017"

admin:admin;reboot

In this command, username is “admin”, password is “admin”, and the command is to reboot the Router.

SMS received:

OK

admin:admin;set firewall remote_ssh_access false;set firewall remote_telnet_access false

In this command, username is “admin”, password is “admin”, and the command is to disable the remote_ssh and remote_telnet access.

SMS received:

OK

OK

admin:admin; set lan network 1 interface lan0;set lan network 1 ip 172.16.99.11;set lan network 1 netmask 255.255.0.0;set lan network 1 mtu 1500

In this command, username is “admin”, password is “admin”, and the commands is to configure the LAN parameter.

SMS received:

OK

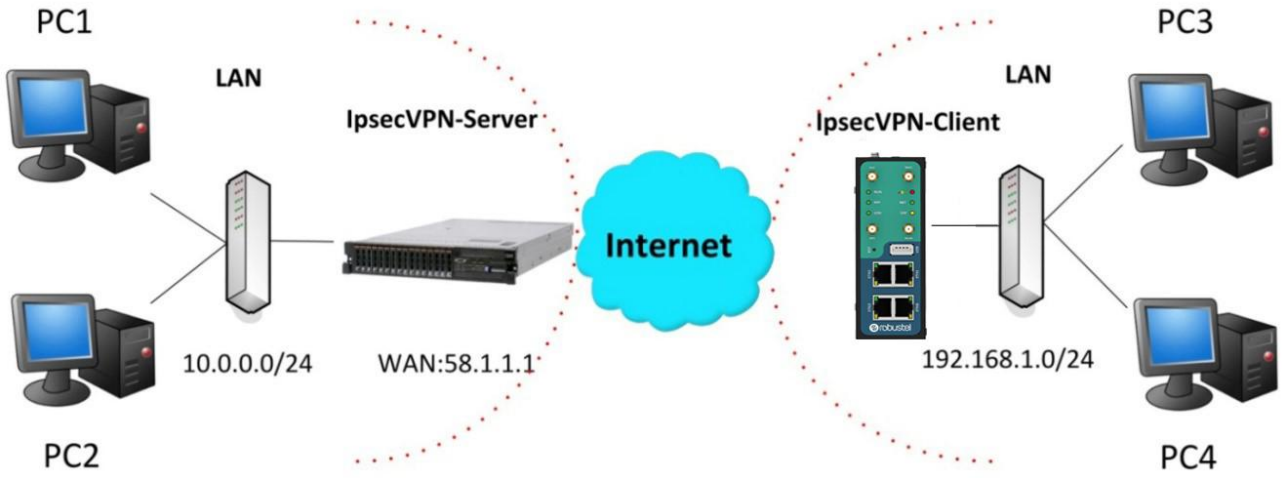
OK

OK

OK

4.2 Network

4.2.1 IPsec VPN



The configuration of server and client is as follows.

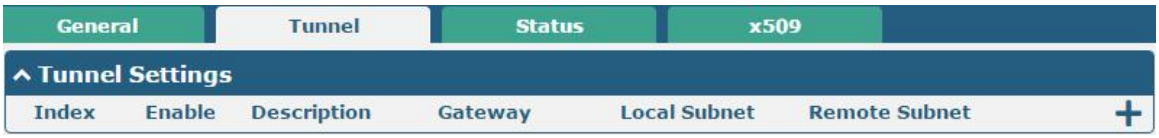
IPsec VPN_Server:

Cisco 2811:

```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp ?
  client  Set client configuration policy
  enable  Enable ISAKMP
  key     Set pre-shared key for remote peer
  policy  Set policy for an ISAKMP protection suite
Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0


Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association parameters
  transform-set         Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac


Router(config)#ip access-list extended vpn
Router(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#exit

Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1
Router(config-crypto-map)#exit


Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#cr
Router(config-if)#crypto map cry-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

IPsec VPN_Client:

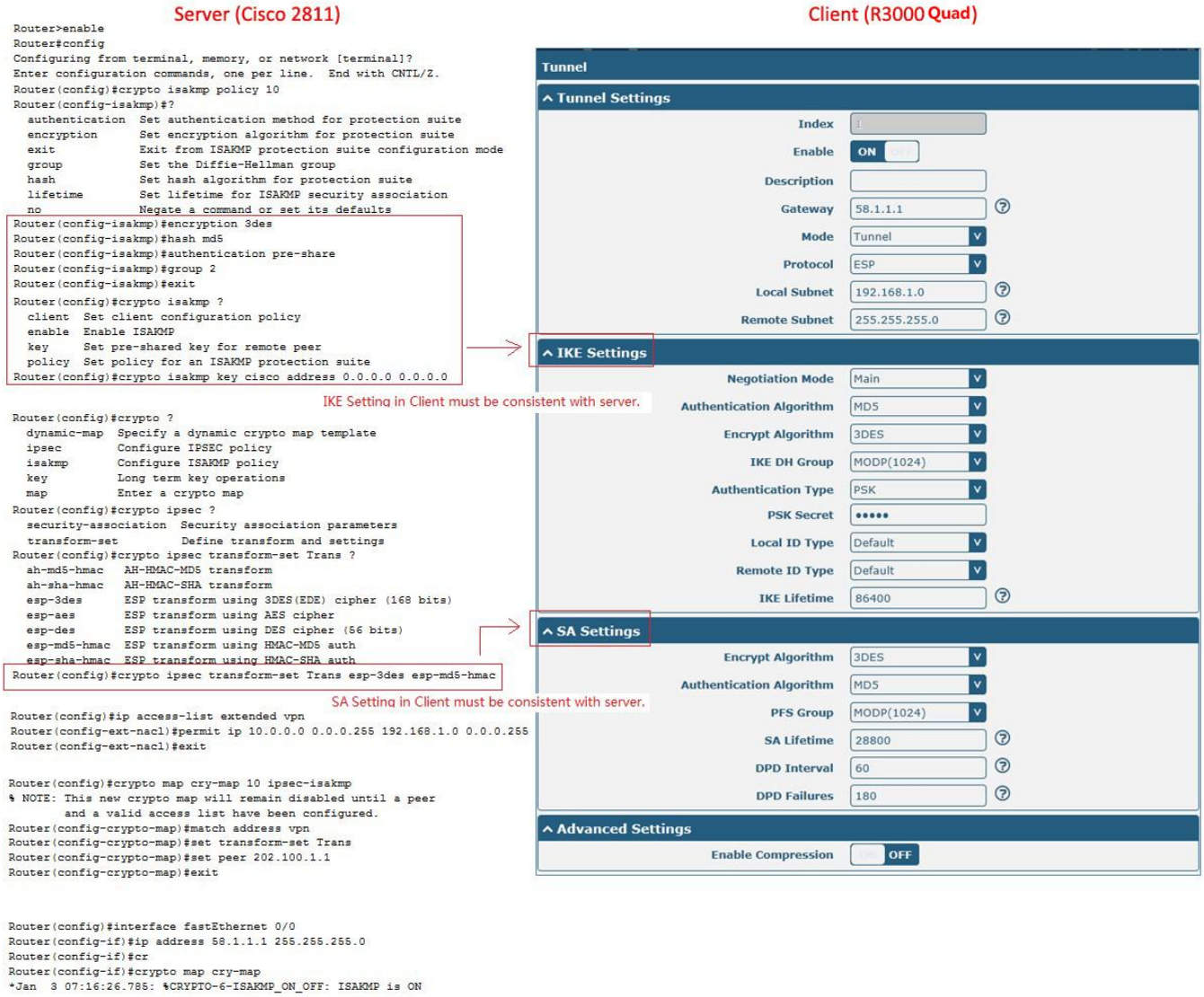
The window is displayed as below by clicking **VPN > IPsec > Tunnel**.



Click + button and set the parameters of IPsec Client as below.

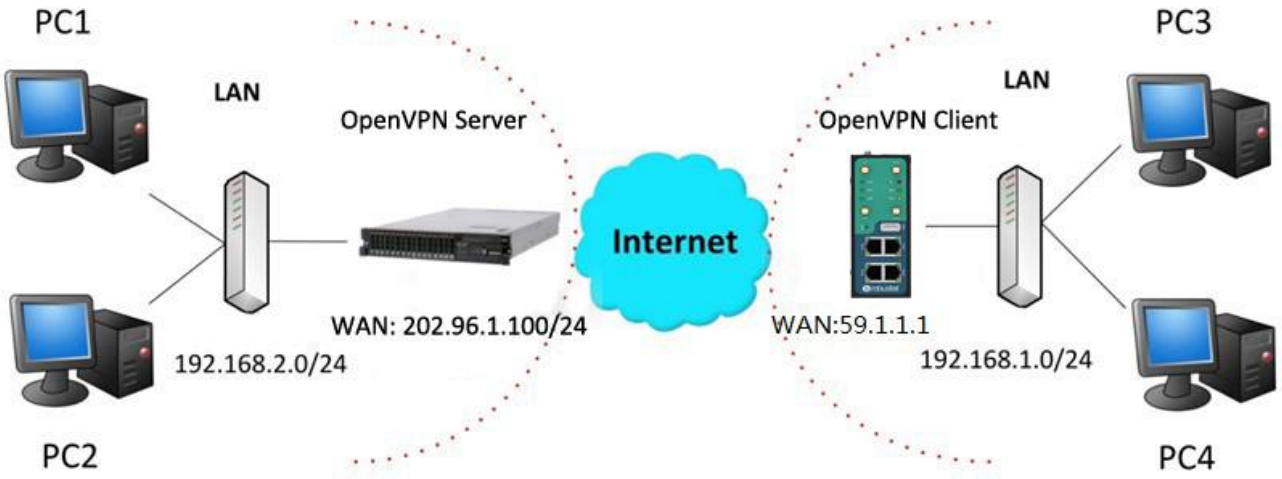
When finished, click **Submit > Save & Apply** for the configuration to take effect.

The comparison between server and client is as below.



4.2.2 OpenVPN

OpenVPN supports two modes, including Client and P2P. Here takes Client as an example.



OpenVPN_Server:

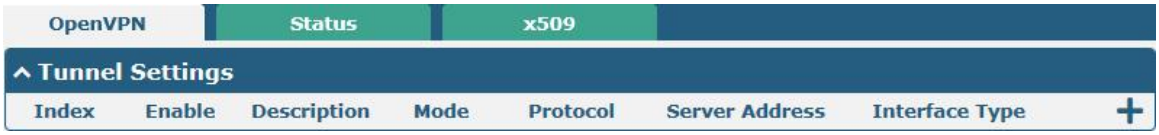
Generate relevant OpenVPN certificate on the server side firstly, and refer to the following commands to configuration the Server:

```
local 202.96.1.100
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert Server01.crt
key Server01.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.3.0 255.255.255.0"
client-config-dir ccd
route 192.168.1.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

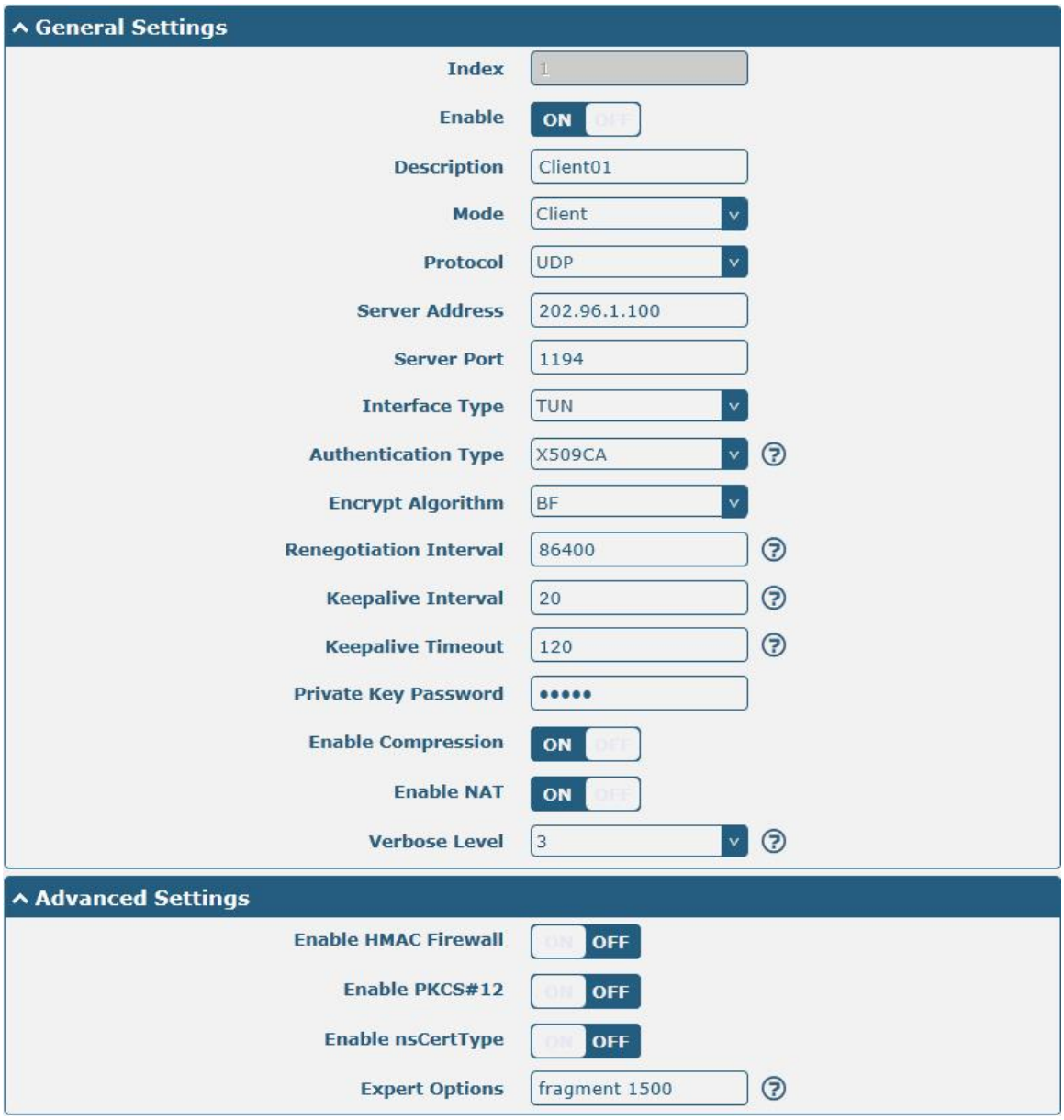
Note: For more configuration details, please contact your technical support engineer.

OpenVPN_Client:

Click **VPN > OpenVPN > OpenVPN** as below.

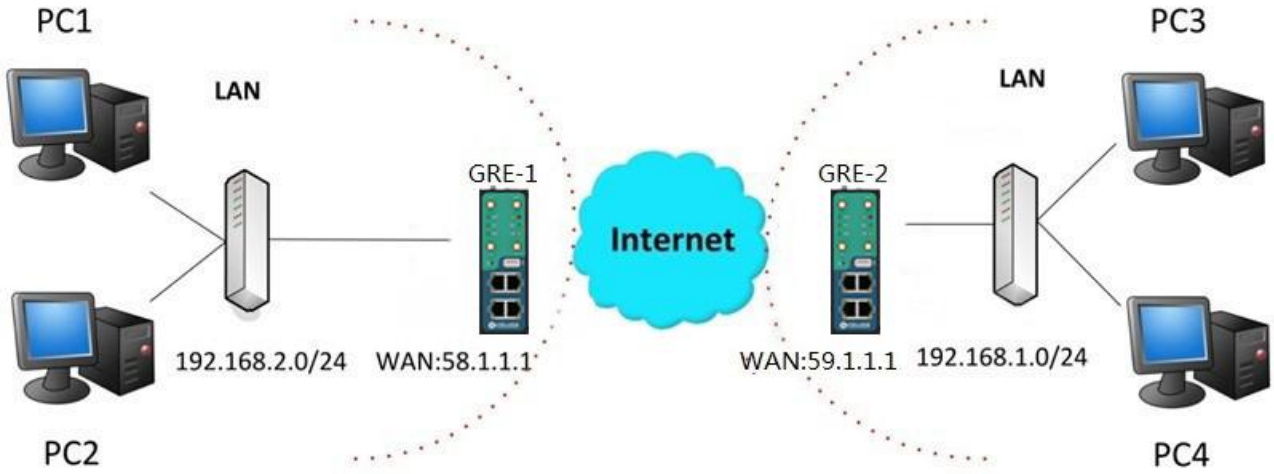


Click + to configure the Client01 as below.



When finished, click **Submit > Save & Apply** for the configuration to take effect.

4.2.3 GRE VPN

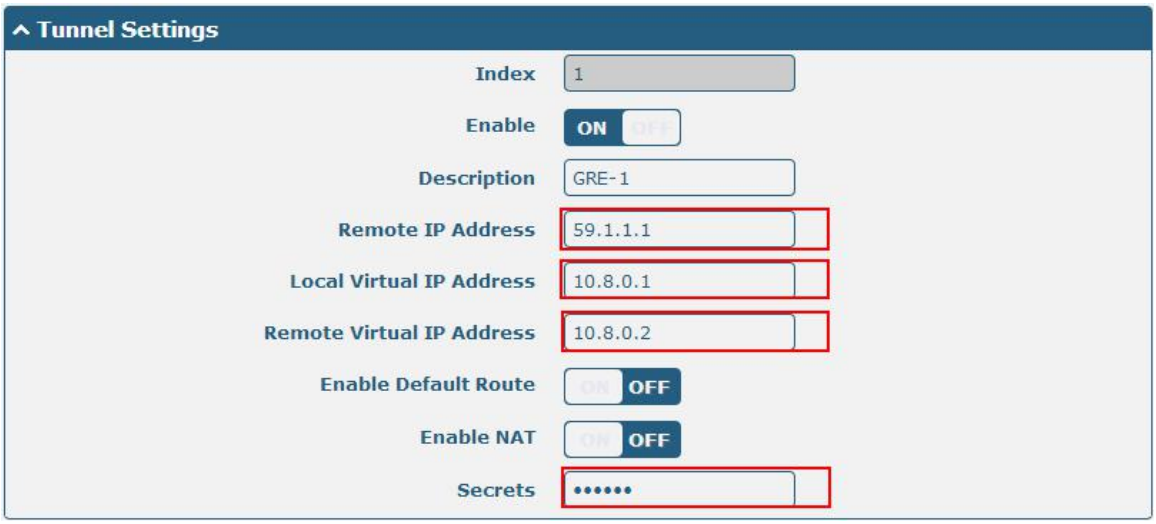


The configuration of two points is as follows.

The window is displayed as below by clicking **VPN > GRE > GRE**.

GRE-1：

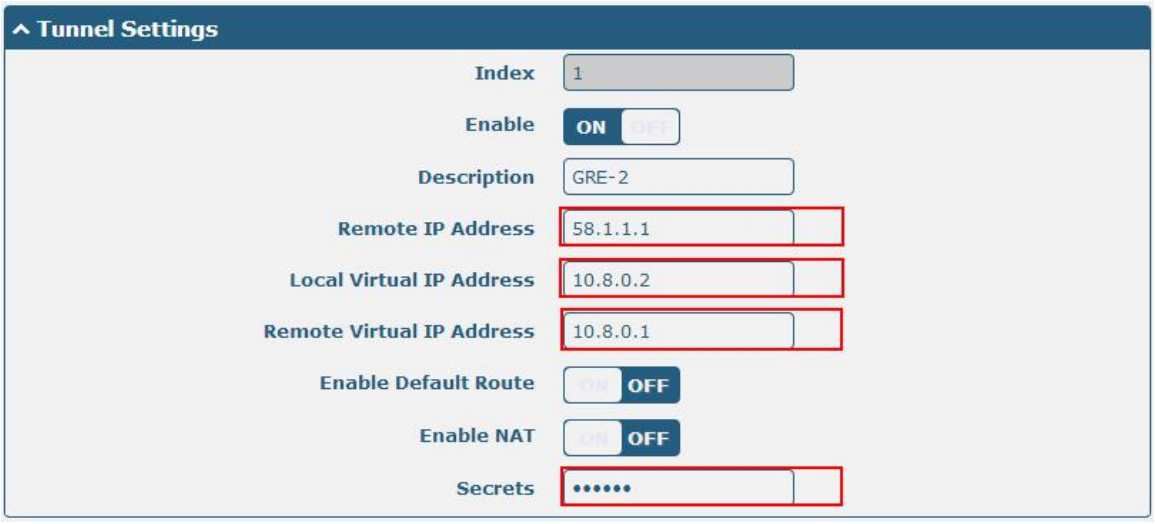
Click + button and set the parameters of GRE-1 as below.



When finished, click **Submit > Save & Apply** for the configuration to take effect.

GRE-2:

Click + button and set the parameters of GRE-1 as below.

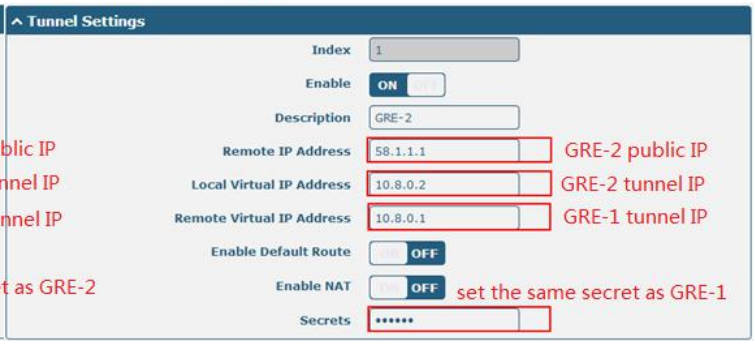


When finished, click **Submit > Save & Apply** for the configuration to take effect.

The comparison between GRE-1 and GRE-2 is as below.

GRE-1

GRE-2



Chapter 5 Introductions for CLI

5.1 What Is CLI

Command-line interface (CLI) is a software interface providing another way to set the parameters of equipment from the SSH or through a telnet network connection.

Route login:

Router login: admin

Password: admin

#

CLI commands:

? (***Note***: the '?' won't display on the page.)

!	Comments
add	Add a list entry of configuration
clear	Clear statistics
config	Configuration operation
debug	Output debug information to the console
del	Delete a list entry of configuration
exit	Exit from the CLI
help	Display an overview of the CLI syntax
ping	Send messages to network hosts
reboot	Halt and perform a cold restart
route	Static route modify dynamically, this setting will not be saved
set	Set system configuration
show	Show system configuration
status	Show running system information
tftpupdate	Update firmware using tftp
traceroute	Print the route packets trace to network host
urlupdate	Update firmware using http or ftp
ver	Show version of firmware

5.2 How to Configure the CLI

Following is a table about the description of help and the error should be encountered in the configuring program.

Commands /tips	Description
?	Typing a question mark “?” will show you the help information.
Ctrl+c	Press these two keys at the same time, except its “copy” function but also can be used for “break” out of the setting program.
Syntax error: The command is not completed	Command is not completed.
Tick space key+ Tab key	It can help you finish you command. Example: # config (tick enter key) Syntax error: The command is not completed # config (tick space key+ Tab key) commit save_and_apply loaddefault
# config save_and_apply / #config commit	When your setting finished, you should enter those commands to make your setting take effect on the device. **Note:** Commit and save_and_apply plays the same role.

Quick Start with Configuration Examples

The best and quickest way to master CLI is firstly to view all features from the webpage and then read all CLI commands at a time, finally learn to configure it with some reference examples.

Example 1: Show current version

```
# status system
hardware_version = 1.0
firmware_version = "3.0.0"
kernel_version = 4.1.0
device_model = R3000 Quad
serial_number = 10201726051044
system_uptime = "0 days, 00:10:58"
system_time = "Sun May 28 11:46:34 2017"
```

Example 2: Update firmware via tftp

```
# tftpupdate (space+?)
  firmware  New firmware
# tftpupdate firmware (space+?)
  String  Firmware name
# tftpupdate firmware filename R3000 Quad-firmware-sysupgrade-unknown.bin host 192.168.100.99 //enter a new firmware name
Downloading
```

```
R3000 Quad-firmware-s 100% |*******************************|    5018k    0:00:00 ETA
Flashing
Checking 100%
Decrypting 100%
Flashing 100%
Verifying 100%
Verfify Success
upgrade success                                    //update success
# config save_and_apply
OK                                          // save and apply current configuration, make you configuration effect
```

Example 3: Set link-manager

```
# set
# set
   at_over_telnet          AT Over Telnet
   cellular                Cellular
   ddns                    Dynamic DNS
   ethernet                Ethernet
   event                   Event Management
   firewall                Firewall
   gre                     GRE
   ipsec                   IPsec
   lan                     Local Area Network
   link_manager            Link Manager
   ntp                     NTP
   openvpn                 OpenVPN
   reboot                  Automatic Reboot
   RobustLink              RobustLink
   route                   Route
   sms                     SMS
   snmp                    SNMP agent
   ssh                     SSH
   syslog                  Syslog
   system                  System
   user_management         User Management
   vrrp                    VRRP
   web_server              Web Server
# set link_manager
   primary_link            Primary Link
   backup_link             Backup Link
   backup_mode             Backup Mode
   emergency_reboot        Emergency Reboot
   link                    Link Settings
# set link_manager primary_link (space+?)
Enum    Primary Link (wwan1/wwan2/wan)
```

```
# set link_manager primary_link wwan1                    //select “wwan1” as primary_link
OK                                                       //setting succeed
# set link_manager link 1
   type                 Type
   desc                 Description
   connection_type      Connection Type
   wwan                 WWAN Settings
   static_addr          Static Address Settings
   pppoe                PPPoE Settings
   ping                 Ping Settings
   mtu                  MTU
   dns1_overrided       Overrided Primary DNS
   dns2_overrided       Overrided Secondary DNS
# set link_manager link 1 type wwan1
OK
# set link_manager link 1 wwan
   auto_apn                     Automatic APN Selection
   apn                          APN
   username                     Username
   password                     Password
   dialup_number                Dialup Number
   auth_type                    Authentication Type
   aggressive_reset             Aggressive Reset
   switch_by_data_allowance     Switch SIM By Data Allowance
   data_allowance               Data Allowance
   billing_day                  Billing Day
# set link_manager link 1 wwan switch_by_data_allowance true
OK
#
# set link_manager link 1 wwan data_allowance 100        //open cellular switch_by_data_traffic
OK                                                       //setting succeed
# set link_manager link 1 wwan billing_day 1             //setting specifies the day of month for billing
OK                                                       // setting succeed
…
# config save_and_apply
OK                                  // save and apply current configuration, make you configuration effect
```

Example 4: Set LAN IP address

```
# show lan all
network {
    id = 1
    interface = lan0
    ip = 192.168.0.1
    netmask = 255.255.255.0
    mtu = 1500
```

```
        dhcp {
                enable = true
                mode = server
                relay_server = ""
                pool_start = 192.168.0.2
                pool_end = 192.168.0.100
                netmask = 255.255.255.0
                gateway = ""
                primary_dns = ""
                secondary_dns = ""
                wins_server = ""
                lease_time = 120
                expert_options = ""
                debug_enable = false
        }
}
multi_ip {
        id = 1
        interface = lan0
        ip = 172.16.7.29
        netmask = 255.255.0.0
}
#
# set lan
   network          Network Settings
   multi_ip         Multiple IP Address Settings
   vlan             VLAN
# set lan network 1(space+?)
   interface        Interface
   ip               IP Address
   netmask          Netmask
   mtu              MTU
   dhcp             DHCP Settings
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.99.22                    //set IP address for lan
OK                                                     //setting succeed
# set lan network 1 netmask 255.255.0.0
OK
#
…
# config save_and_apply
OK                                          // save and apply current configuration, make you configuration effect
```

Example 5: CLI for setting Cellular

```
# show cellular all
```

```
sim {
        id = 1
        card = sim1
        phone_number = ""
        extra_at_cmd = ""
        network_type = auto
        band_select_type = all
        band_gsm_850 = false
        band_gsm_900 = false
        band_gsm_1800 = false
        band_gsm_1900 = false
        band_wcdma_850 = false
        band_wcdma_900 = false
        band_wcdma_1900 = false
        band_wcdma_2100 = false
        band_lte_800 = false
        band_lte_850 = false
        band_lte_900 = false
        band_lte_1800 = false
        band_lte_1900 = false
        band_lte_2100 = false
        band_lte_2600 = false
        band_lte_1700 = false
        band_lte_700 = false
        band_tdd_lte_2600 = false
        band_tdd_lte_1900 = false
        band_tdd_lte_2300 = false
        band_tdd_lte_2500 = false
}
sim {
        id = 2
        card = sim2
        phone_number = ""
        extra_at_cmd = ""
        network_type = auto
        band_select_type = all
        band_gsm_850 = false
        band_gsm_900 = false
        band_gsm_1800 = false
        band_gsm_1900 = false
        band_wcdma_850 = false
        band_wcdma_900 = false
        band_wcdma_1900 = false
        band_wcdma_2100 = false
        band_lte_800 = false
        band_lte_850 = false
```

```
        band_lte_900 = false
        band_lte_1800 = false
        band_lte_1900 = false
        band_lte_2100 = false
        band_lte_2600 = false
        band_lte_1700 = false
        band_lte_700 = false
        band_tdd_lte_2600 = false
        band_tdd_lte_1900 = false
        band_tdd_lte_2300 = false
        band_tdd_lte_2500 = false
}
# set(space+?)
at_over_telnet      cellular            ddns            dhcp            dns
event               firewall            ipsec           lan             link_manager
ntp                 openvpn             reboot          route           serial_port
sms                 snmp                syslog          system          user_management
vrrp
# set cellular(space+?)
   sim    SIM Settings
# set cellular sim(space+?)
   Integer    Index (1..2)

# set cellular sim 1(space+?)
   card                    SIM Card
   phone_number            Phone Number
   extra_at_cmd            Extra AT Cmd
   network_type            Network Type
   band_select_type        Band Select Type
   band_gsm_850            GSM 850
   band_gsm_900            GSM 900
   band_gsm_1800           GSM 1800
   band_gsm_1900           GSM 1900
   band_wcdma_850          WCDMA 850
   band_wcdma_900          WCDMA 900
   band_wcdma_1900         WCDMA 1900
   band_wcdma_2100         WCDMA 2100
   band_lte_800            LTE 800 (band 20)
   band_lte_850            LTE 850 (band 5)
   band_lte_900            LTE 900 (band 8)
   band_lte_1800           LTE 1800 (band 3)
   band_lte_1900           LTE 1900 (band 2)
   band_lte_2100           LTE 2100 (band 1)
   band_lte_2600           LTE 2600 (band 7)
   band_lte_1700           LTE 1700 (band 4)
   band_lte_700            LTE 700 (band 17)
```

```
    band_tdd_lte_2600    TDD LTE 2600 (band 38)
    band_tdd_lte_1900    TDD LTE 1900 (band 39)
    band_tdd_lte_2300    TDD LTE 2300 (band 40)
    band_tdd_lte_2500    TDD LTE 2500 (band 41)
# set cellular sim 1 phone_number 18620435279
OK
…
# config save_and_apply
OK                                    // save and apply current configuration, make you configuration effect
```

5.3 Commands Reference

Commands	Syntax	Description
Debug	Debug *parameters*	Turn on or turn off debug function
Show	Show *parameters*	Show current configuration of each function , if we need to see all please using “show running ”
Set	Set *parameters*	All the function parameters are set by commands set and add, the difference is that set is for the single parameter and add is for the list parameter
Add	Add *parameters*	

Note: Download the config.XML file from the configured web browser. The command format can refer to the config.XML file format.

Glossary

Abbr.	Description
AC	Alternating Current
APN	Access Point Name
ASCII	American Standard Code for Information Interchange
CE	Conformité Européene (European Conformity)
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface for batch scripting
CSD	Circuit Switched Data
CTS	Clear to Send
dB	Decibel
dBi	Decibel Relative to an Isotropic radiator
DC	Direct Current
DCD	Data Carrier Detect
DCE	Data Communication Equipment (typically modems)
DCS 1800	Digital Cellular System, also referred to as PCN
DI	Digital Input
DO	Digital Output
DSR	Data Set Ready
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-frequency
DTR	Data Terminal Ready
EDGE	Enhanced Data rates for Global Evolution of GSM and IS-136
EMC	Electromagnetic Compatibility
EMI	Electro-Magnetic Interference
ESD	Electrostatic Discharges
ETSI	European Telecommunications Standards Institute
EVDO	Evolution-Data Optimized
FDD LTE	Frequency Division Duplexing Long Term Evolution
GND	Ground
GPRS	General Packet Radio Service
GRE	generic route encapsulation
GSM	Global System for Mobile Communications
HSPA	High Speed Packet Access
ID	identification data
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
kbps	kbits per second
L2TP	Layer 2 Tunneling Protocol

Abbr.	Description
LAN	local area network
LED	Light Emitting Diode
M2M	Machine to Machine
MAX	Maximum
Min	Minimum
MO	Mobile Originated
MS	Mobile Station
MT	Mobile Terminated
OpenVPN	Open Virtual Private Network
PAP	Password Authentication Protocol
PC	Personal Computer
PCN	Personal Communications Network, also referred to as DCS 1800
PCS	Personal Communication System, also referred to as GSM 1900
PDU	Protocol Data Unit
PIN	Personal Identity Number
PLCs	Program Logic Control System
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
PSU	Power Supply Unit
PUK	Personal Unblocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTC	Real Time Clock
RTS	Request to Send
RTU	Remote Terminal Unit
Rx	Receive Direction
SDK	Software Development Kit
SIM	subscriber identification module
SMA antenna	Stubby antenna or Magnet antenna
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TE	Terminal Equipment, also referred to as DTE
Tx	Transmit Direction
UART	Universal Asynchronous Receiver-transmitter
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
USSD	Unstructured Supplementary Service Data
VDC	Volts Direct current
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSWR	Voltage Stationary Wave Ratio

Abbr.	Description
WAN	Wide Area Network

Guangzhou Robustel Co., Ltd.
Add: 501, Building 2, No. 63, Yong'an Avenue,
Huangpu District, Guangzhou, China 510660
Tel: 86-20-82321505
Email: support@robustel.com
Web: www.robustel.com