robustel | User Guide

R1511

Industrial Cellular VPN Router

robustOS

Guangzhou Robustel LTD
www.robustel.com

About This Document

This document provides hardware and software information of the Robustel Industrial Cellular VPN Router R1511, including introduction, installation, configuration and operation.

Copyright©2020 Guangzhou Robustel LTD
All rights reserved.

Trademarks and Permissions

robustel robustOS are trademark of Guangzhou Robustel 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 use of this document.

Technical Support

Tel: +86-20-29019902
Fax: +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.
- 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.
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: Standards of the electronic industry of the People's Republic of China

SJ/T 11363-2006	The electronic industry standard of the People's Republic of China SJ/T 11363-2006 "Requirements for Concentration Limits for Certain Toxic and Hazardous Substances in Electronic Information Products" issued by the ministry of information industry of the People's Republic of China on November 6, 2006, stipulates the maximum allowable concentration of toxic and hazardous substances in electronic information products. Please see **Table 3** for an overview of toxic or hazardous substances or elements that might be contained in product parts in concentrations above the limits defined by SJ/T 11363-2006.
SJ/T 11364-2014	The electronic industry standard of the People's Republic of China SJ/T 11364-2014 "Labeling Requirements for Restricted Use of Hazardous Substances in Electronic and Electrical Products" issued by the ministry of Industry and information technology of the People's Republic of China on July 9, 2014, stipulates the Labeling requirements of hazardous substances in electronic and electrical products, environmental protection use time limit and whether it can be recycled. This standard is applicable to electronic and electrical products sold within the territory of the People's Republic of China, and can also be used for reference in the logistics process of electronic and electrical products. The orange logo below is used for Robustel products: Indicates its warning attribute, that is, some hazardous substances are contained in the product. The "10" in the middle of the legend refers to the environment-friendly Use Period (EFUP) * of electronic information product, which is 10 years. It can be used safely during the environment-friendly Use Period. After the environmental protection period of use, it should enter the recycling system. *The term of environmental protection use of electronic information products refers to the term during which the toxic and hazardous substances or elements contained in electronic information products will not be leaked or mutated and cause serious pollution to the environment or serious damage to people and property under normal conditions of use.

Table 3: 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	–	–	–	–	–	–
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.
–:
Indicates that it does not contain the toxic or hazardous substance.

Document History

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

Date	Firmware Version	Document Version	Change Description
Aug. 28, 2020	3.1.5	v.1.0.0	Initial release

Contents

Contents **8**
Chapter 1 Product Overview **10**
1.1 Introduction 10
1.2 Package Contents 10
1.3 Specifications 12
1.4 Dimensions 13
Chapter 2 Hardware Installation **14**
2.1 Pin Description 14
2.2 LED Indicators 14
2.3 Reset Button 16
2.4 Ethernet Ports 16
2.5 Insert or Remove SIM Card 17
2.6 Attach External Antenna (SMA Type) 18
2.7 Mount the Router 18
2.8 Connect the Router to a Computer 21
2.9 Power Supply 21
Chapter 3 Initial Configuration **22**
3.1 Configure the PC 22
3.2 Factory Default Settings 25
3.3 Log in the Router 25
3.4 Control Panel 26
Chapter 4 Router Configuration **28**
4.1 Status 28
4.1.1 System Information 28
4.1.2 Internet Status 29
4.1.3 LAN Status 29
4.2 Interface 30
4.2.1 Link Manager 30
4.2.2 LAN 39
4.2.3 Ethernet 43
4.2.4 Cellular 44
4.2.5 WiFi 49
4.2.6 Serial port 58
4.3 Network 63
4.3.1 Route 63
4.3.2 Firewall 65
4.3.3 IP Passthrough 71
4.4 VPN 71
4.4.1 IPsec 71
4.4.2 OpenVPN 80
4.4.3 GRE 94
4.5 Services 95

4.5.1 Syslog 95
4.5.2 Event 97
4.5.3 NTP 100
4.5.4 SMS 101
4.5.5 Email 102
4.5.6 DDNS 103
4.5.7 SSH 104
4.5.8 Web Server 105
4.5.9 Advanced 106
4.6 System 107
4.6.1 Debug 107
4.6.2 Update 109
4.6.3 App Center 109
4.6.4 Tools 111
4.6.5 Profile 113
4.6.6 User Management 115
Chapter 5 Configuration Examples 117
5.1 Cellular 117
5.1.1 Cellular Dial-Up 117
5.1.2 SMS Remote Control 119
5.2 VPN Configuration Example 121
5.2.1 IPsec VPN 121
5.2.2 OpenVPN 125
5.2.3 GRE VPN 127
Chapter 6 Introductions for CLI 130
6.1 What Is CLI 130
6.2 How to Configure the CLI 132
6.3 Commands Reference 132
6.4 Quick Start with Configuration ExampleS 133
Glossary 139

Chapter 1 Product Overview

1.1 Introduction

Robustel R1511 industrial-grade cellular VPN wireless router provides high-speed wireless network bandwidth for devices through wireless connection to ensure a stable connection to the wireless network.

Robustel's routers are based on the "RobustOS" operating system. With 5 years of mature and innovative functions, RobustOS provides customers with a very professional product with an easy-to-navigate graphical user interface and essential IoT applications and connection stability. The router occupies a very small space and is very useful for space-constrained applications, such as ticket vending machines, vending machines, hidden surveillance and digital signage applications.

1.2 Package Contents

Before installing your R1511 Router, verify the kit contents as following.

Note: Accessories are subject to the actual order. If you have any questions, please contact your sales representative.

- 1 x Robustel R1511 Industrial Cellular VPN Router

- 1 x 2-pin 3.5 mm male terminal block for power supply

- 1 x 3-pin 3.5 mm male terminal block for 232/485

- 3G/4G SMA-J cellular antenna (Two as standard)

Stubby antenna

- RP- SMA-J WIFI antenna
  Stubby antenna

- Ethernet cable

- 1 x SIM Card Sticker

Optional Accessories (sold separately)

- AC/DC power adapter (12V DC, 1 A; EU/US/UK/AU plug optional)

- Wall mounting kit

- 35 mm DIN rail mounting kit

1.3 Specifications

Cellular Interface

- Number of antennas: 2
- Connector: SMA-K
- SIM: 1* (3 V & 1.8 V) Standard SIM or eSIM

Ethernet Interface

- Number of ports: 2 x 10/100 Mbps, 2 x LAN or 1 x LAN + 1 x WAN
- Magnet isolation protection: 1.5 KV

WiFi Interface

- Number of antennas: 1 (external antenna)
- Connector: RP-SMA-K (external antenna)
- Standards: 802.11b/g/n, supports AP and Client modes
- Frequency bands: 2.4 GHz
- Security: WEP, WPA, WPA2
- Encryption: 64/128 AES, TKIP
- Data speed: 2*2 MIMO, 300 Mbps

Serial port

- Type: 1 x RS232 or 1 x RS485
- Connector: 3-pin 3.5 mm female socket

Others

- 1 x Reset button (RST button)
- LED indicators - 1 x RUN, 1 x MDM, 1 x USR, 1 x RSSI, 1 x WiFi
- Built-in: Watchdog, Timer

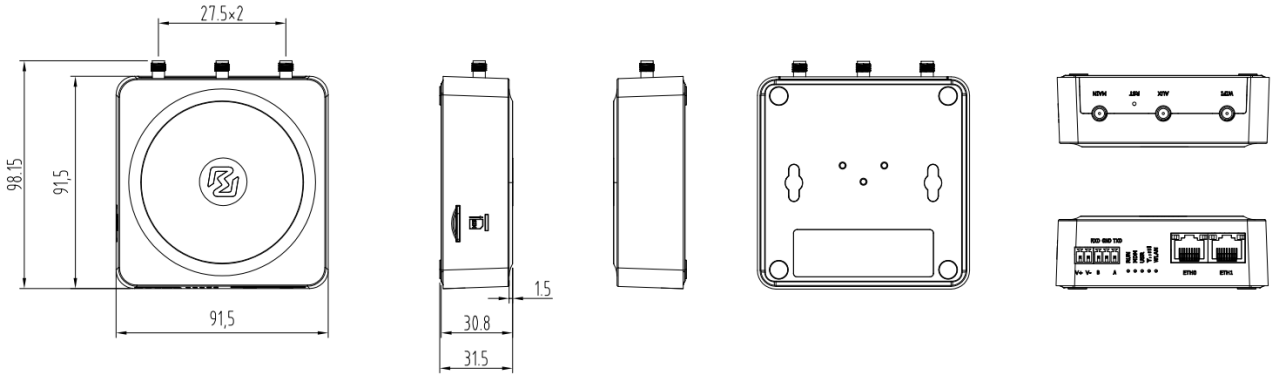
Power Supply and Consumption

- Connector: 2-pin 3.5 mm female socket
- Input voltage: 9 to 36V DC
- Power consumption: Idle: 100 mA@12 V;
  Data link: 500 mA (peak) @12 V

Physical Characteristics

- Ingress protection: IP30
- Housing & Weight: Plastic, 150 g
- Dimensions: 91.5 x 91.5 x 31.5mm
- Installations: Desktop, wall mounting or DIN rail mounting (Wall mounting and Din rail mounting installation requires additional installation accessories)
- Operating Temperature: -25 to +70 °C
- Storage Temperature: -40 to +85 °C
- Relative Humidity: 5 to 95% RH

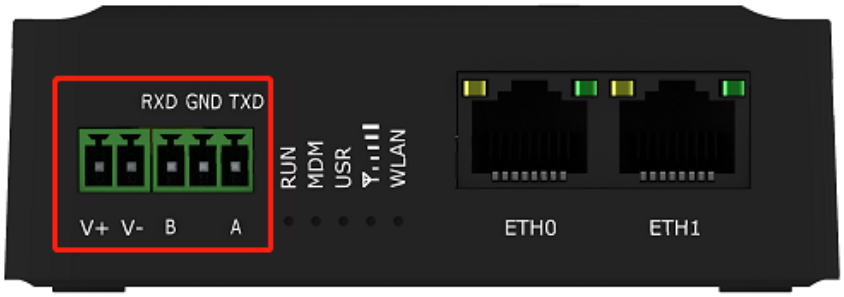
1.4 Dimensions



Front View Left View Right View Side View Top&Bottom View

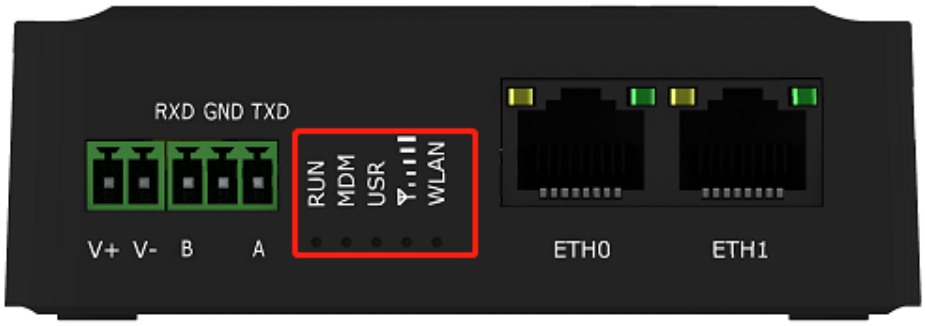
Chapter 2 Hardware Installation

2.1 Pin Description



PIN	Power	232/485	Note
1	V+	--	VCC
2	V-	--	VSS
3	--	RXD/B	RS232 data receiving/RS485_B, please refer to specific model for specific definition
4	--	GND	Signal ground
5	--	TXD/A	RS232 data transmission/RS485_A, please refer to specific model for specific definition

2.2 LED Indicators



Name	Color	Status	Description
RUN	Green	On, solid	Router is powered on (System is initializing)
		On, blinking	Router starts operating
		Off	Router is powered off
MDM	Green	On, solid	Link connection is working
		On, blinking	Data is sent and received.
		Off	Link connection is not working

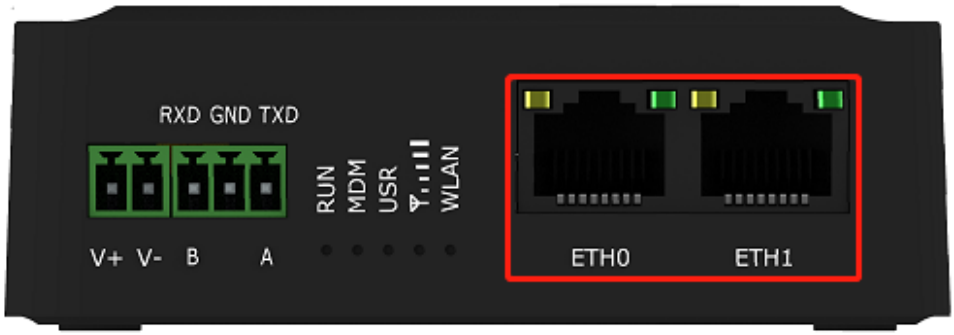
USR	USR-OpenVPN	Green	On, solid	OpenVPN connection is established
			Off	OpenVPN connection is not established
	USR-IPsec	Green	On, solid	IPsec connection is established
			Off	IPsec connection is not established
RSSI		Green	On, solid	Signal level: Wireless module : 21-31 dB (High Signal strength)
		Green	On, blinking	Signal level: Wireless module : 11-20 dB (Medium Signal strength)
		Green	Off	Signal level: Wireless module : 1-10 dB (Low Signal strength)
WLAN		Green	On, solid	WiFi is enabled and working properly
		Green	Off	WiFi is disabled or not working properly

Note: click Services > Advanced > system > System Settings > Custom LED light type to set the display type of USR LED.

2.3 Reset Button

Function	Operation
Reboot	Press and hold the RST button for 2 to 7 seconds under the operating status.
Restore to factory default settings	Wait for 0~20 seconds after powering up the router, press and hold the RST button until four LEDs(RUN, MDM, USR, RSSI) start blinking one by one, and release the button to return the router to factory defaults.

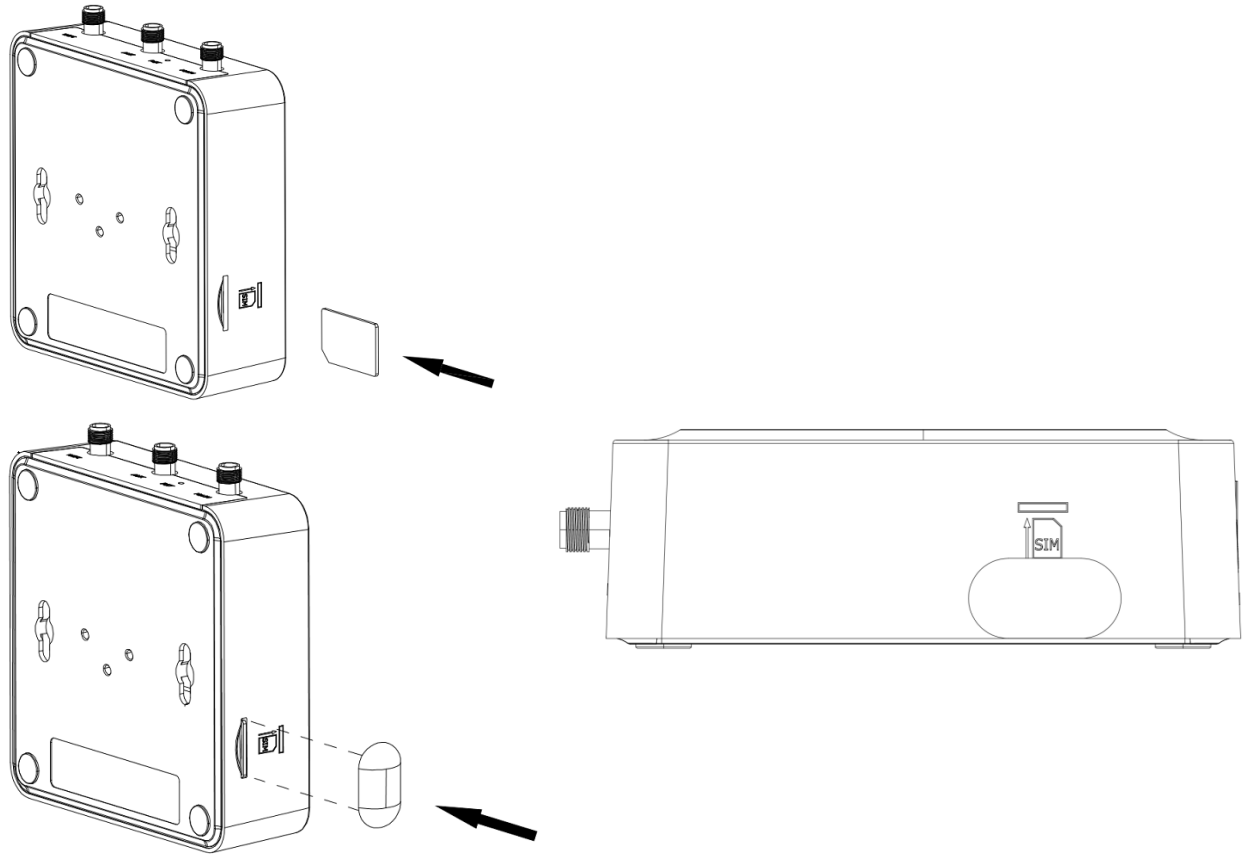
2.4 Ethernet Ports



There are two Ethernet ports on R1511, including ETH0 (WAN/LAN), and ETH1. Each has two LED indicators. The green one is a link indicator but the yellow one doesn't mean anything(always off). For details about status, see the table below.

Indicator	Status	Description
Link indicator (Green)	On, solid	Connection is established
	On, blinking	Data is being transferred
	Off	Connection is not established

2.5 Insert or Remove SIM Card



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

- **Insert SIM card**

1. Make sure router is powered off.
2. To insert SIM card, press the card with finger until you hear a click.
3. After the SIM card is inserted, attach the SIM card sticker to the card slot.

- **Remove SIM card**

1. Make sure router is powered off.
2. Tear the SIM card sticker from the slot.
3. To remove SIM card, press the card with finger until it pops out and then take out the card.

Note:

1. Use the specific M2M SIM card when the device is working in extreme temperature, because the regular card for

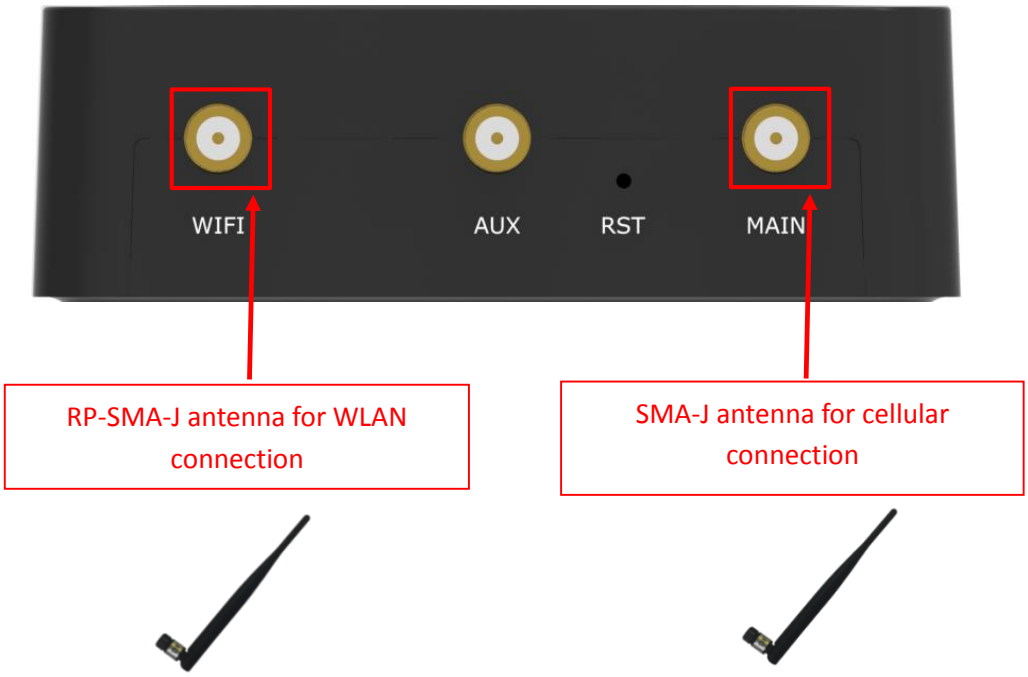
long-time working in harsh environment will be disconnected frequently.

2. Do not touch the metal of the card surface in case information in the card will lose or be destroyed.
3. Do not bend or scratch the card.
4. Keep the card away from electricity and magnetism.
5. Make sure router is powered off before inserting or removing the card.

2.6 Attach External Antenna (SMA Type)

Attach an external SMA antenna to the router's antenna 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.

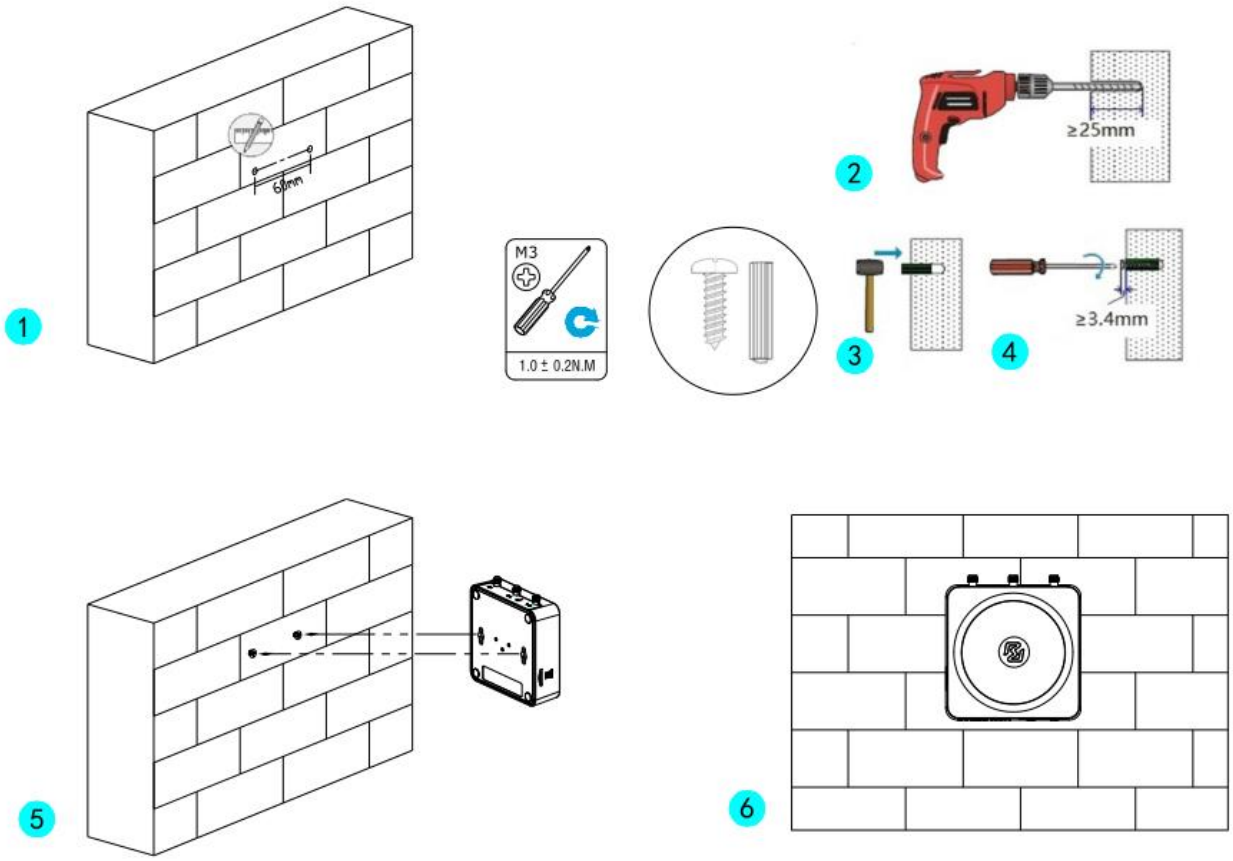


2.7 Mount the Router

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

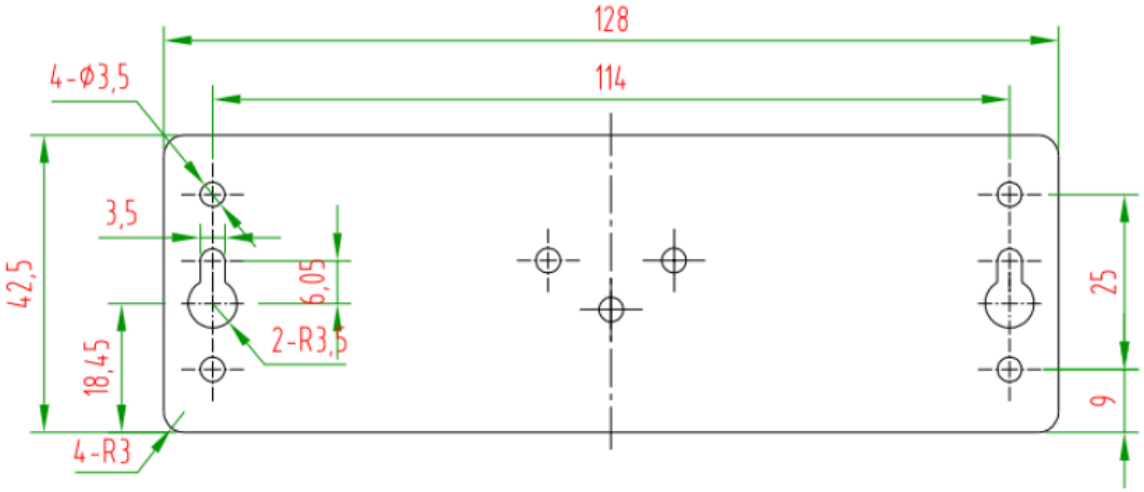
Two methods for mounting the router

1. Wall mounting (measured in mm)
   - Option 1

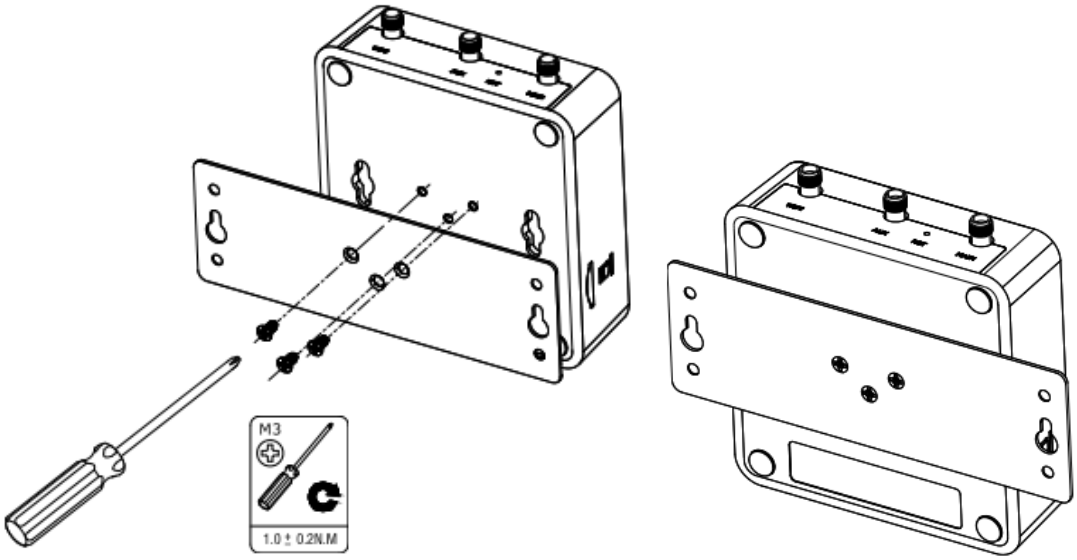


First, drill holes on the wall, the distance between the two holes is 60mm, then knock the expansion pipe into the wall with a rubber hammer, align the screw with the expansion pipe, insert the screw and reserve the corresponding length, and finally fix the product on the wall.

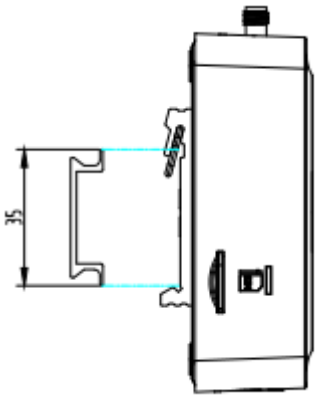
- Option 2
  Size of Wall mounted kit:



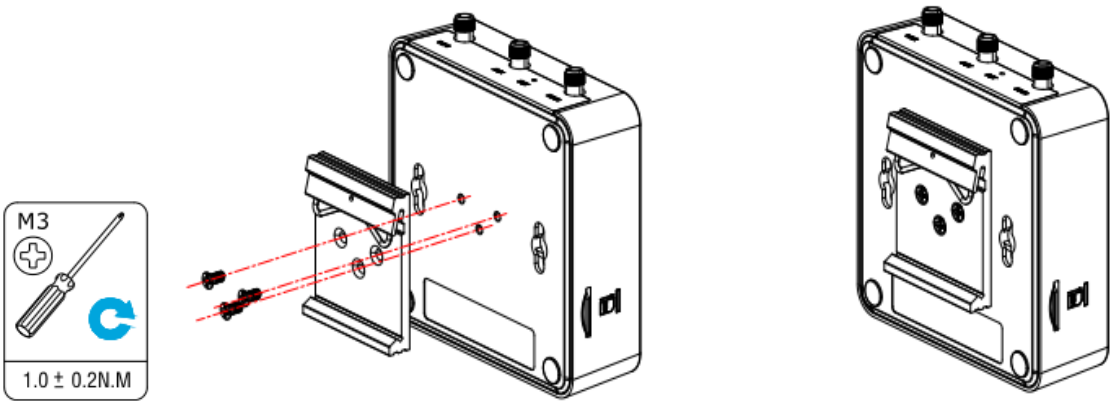
Use 3 pcs of M3 screws to mount the router on the wall mounting kit, and then use 2 pcs of M3 screws to mount the wall mounting kit on the wall.



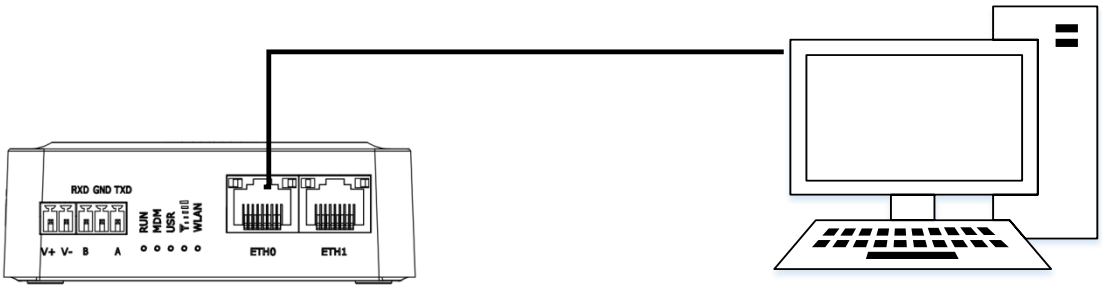
2. DIN rail mounting (measured in mm)



Use 3 pcs of M3 screws to mount the router on the DIN rail, and then hang the DIN rail on the holder. You need to choose a standard holder.

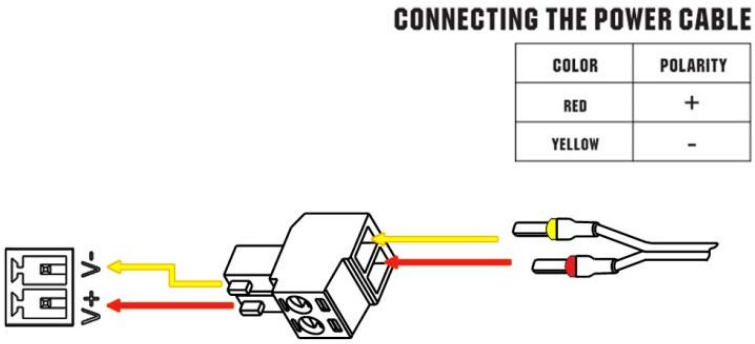


2.8 Connect the Router to a Computer



Connect a standard Ethernet cable to the port marked ETH0~ETH1 at the front of the R1511 Router, and connect the other end of the cable to your computer.

2.9 Power Supply



R1511 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 36V DC.

Chapter 3 Initial Configuration

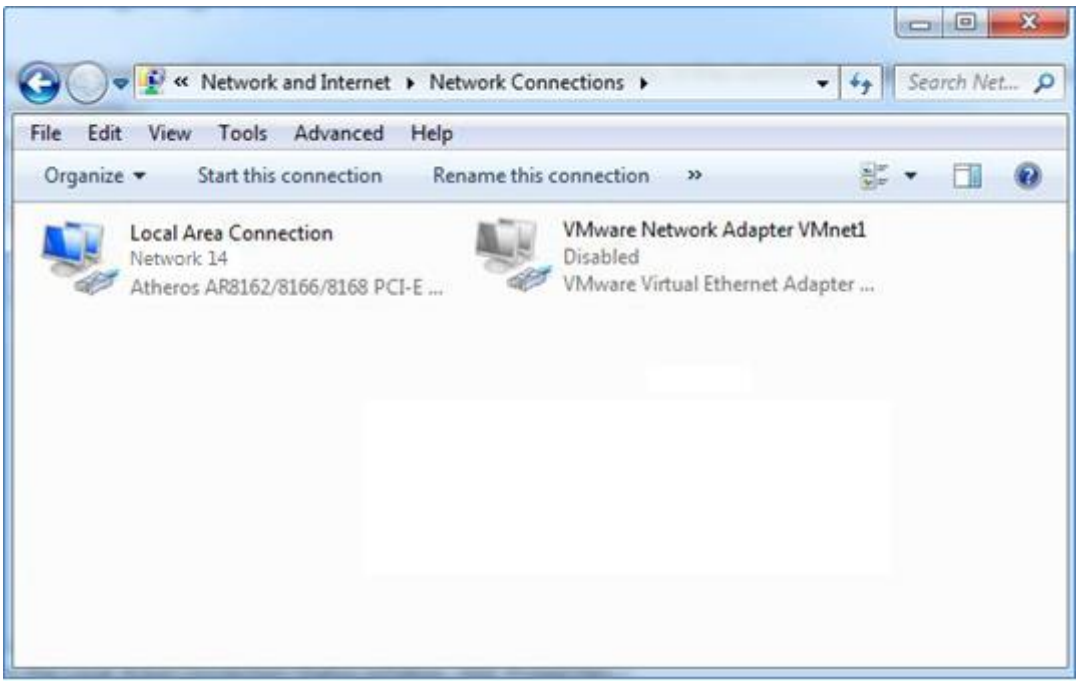
The router can be configured through your web browser that including IE 8.0 or above, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. It provides an easy and user-friendly interface 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

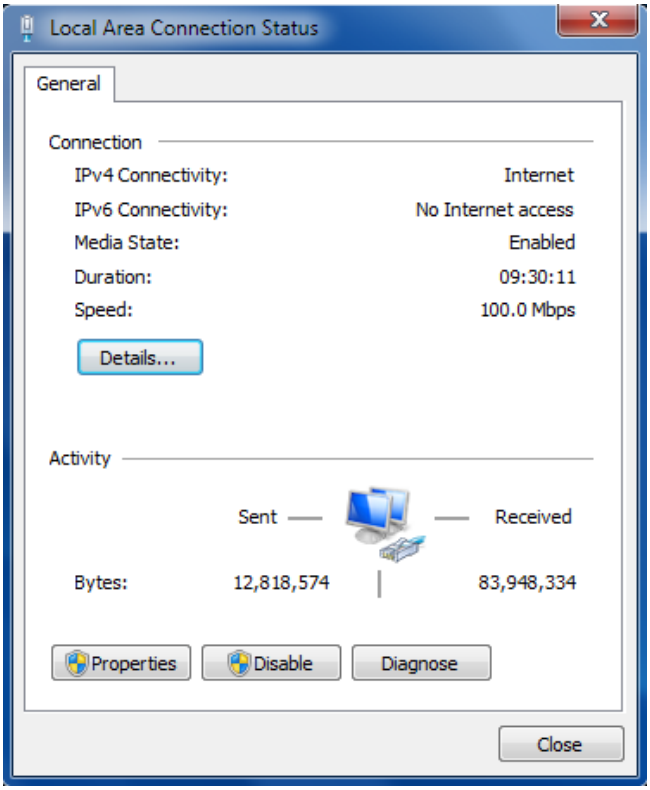
There are two methods to get IP address for the PC. One is to obtain an IP address automatically from “Local Area Connection”, and another is to configure a static IP address manually within the same subnet of the router. Please refer to the steps below.

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

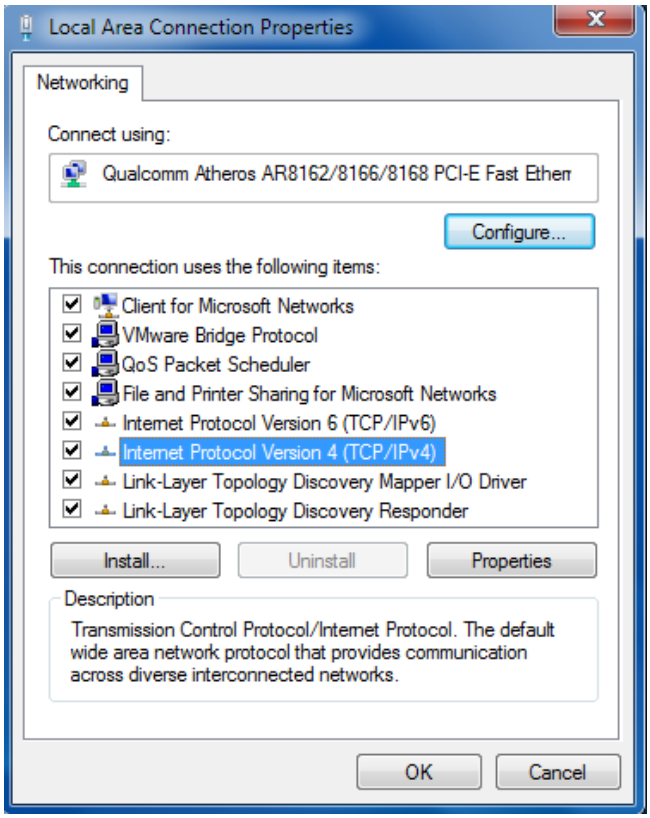
1. Click **Start > Control Panel**, double-click **Network and Internet**, and then double-click **Network Connections.**



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

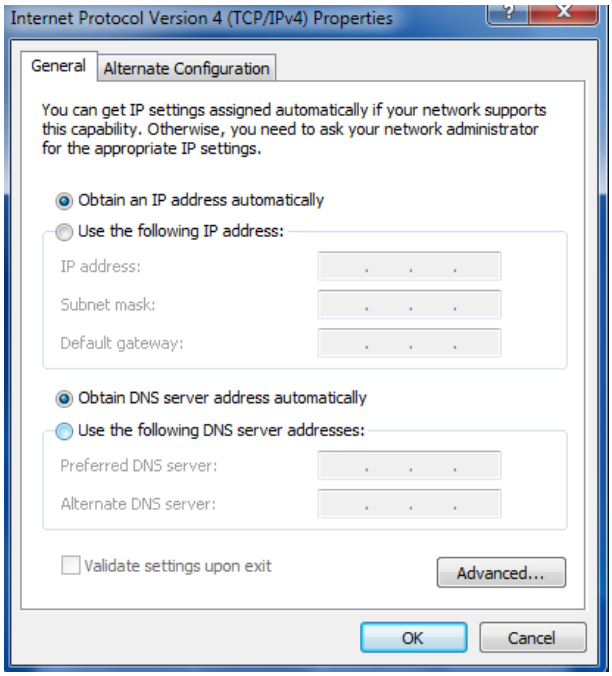


3. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



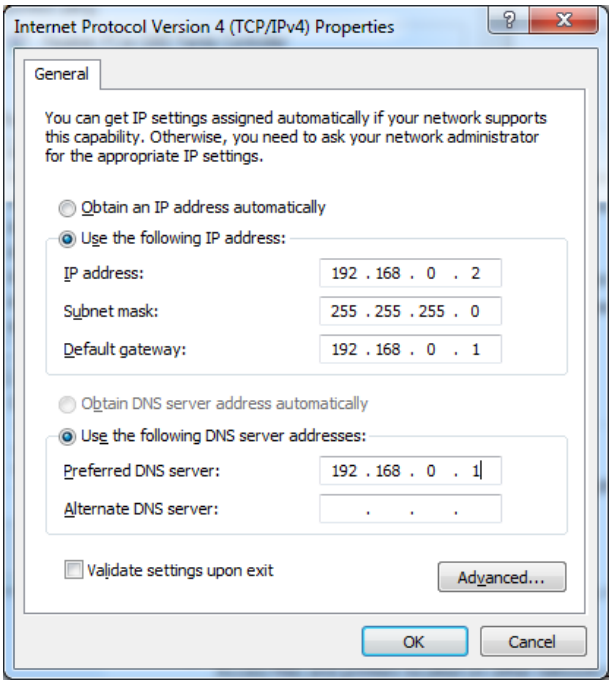
4. Two ways for configuring the IP address of PC

   Obtain an IP address from the DHCP server automatically; Click **"Obtain an IP address automatically ";**



Use the following IP address:

(Configured a static IP address manually within the same subnet of the router, click and configure "**Use the following IP address**"



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

3.2 Factory Default Settings

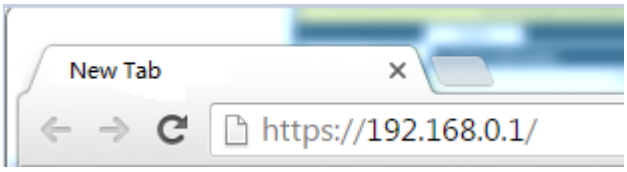
Before configuring your router, you need to know the following default settings.

Item	Description
Username	admin
Password	admin
ETH0	WAN mode or 192.168.0.1/255.255.255.0, LAN mode
ETH1	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.

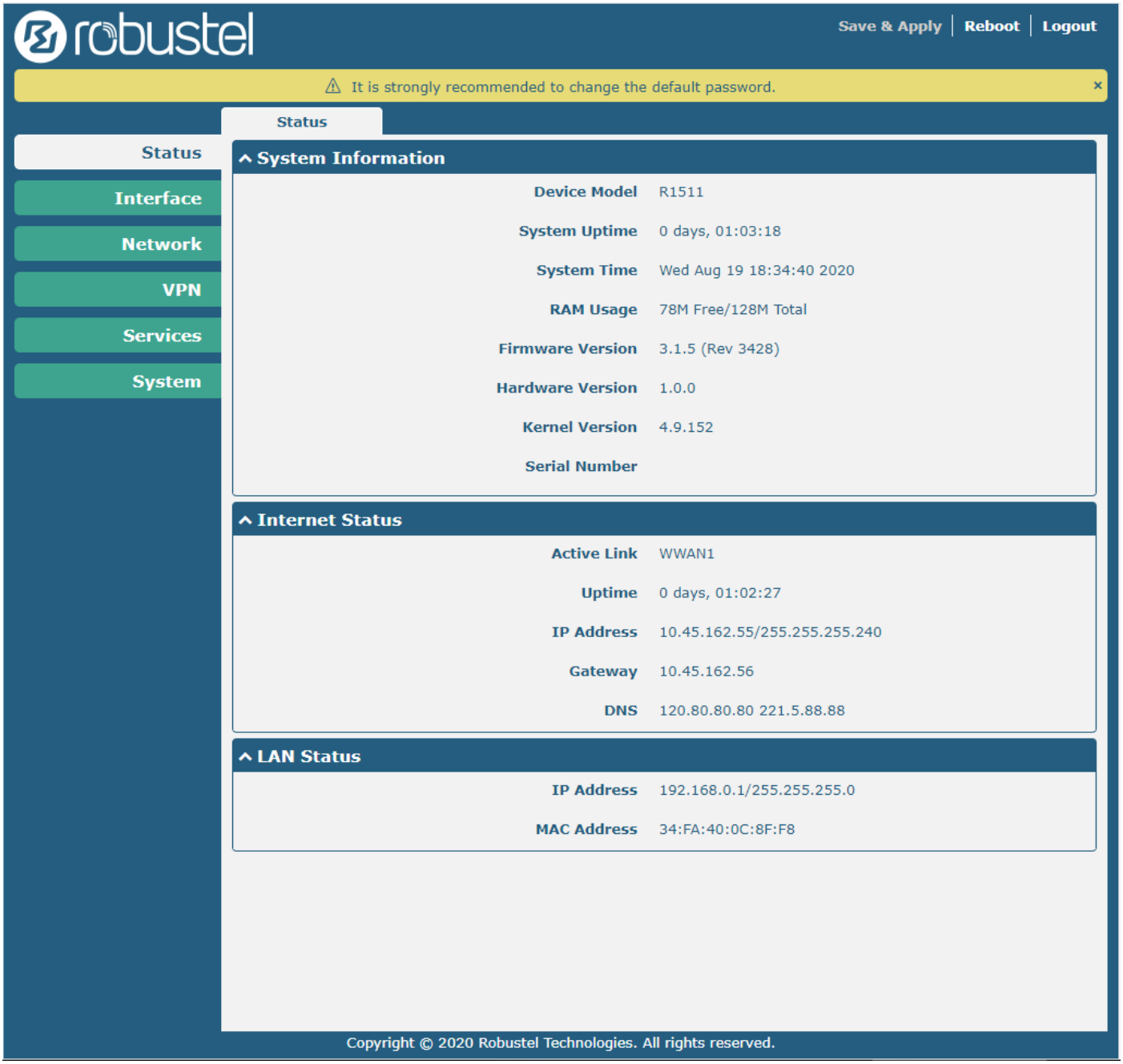
1. On your PC, open a web browser such as Internet Explorer and Google, etc.
2. From your web browser, type the IP address of the router into the address bar and press enter. The default IP address of the router is http://192.168.0.1/, though the actual address may vary.



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.

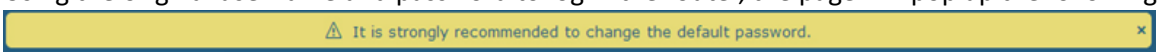
3.4 Control Panel

After logging in, the home page of the R1511 Router's web interface is displayed, for example.



In the home page, the user can save the configuration, restart the router, log out, and so on.

Using the original username and 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. Click the × to close the popup. To change your username and/or password, see **4.6.6 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.	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:

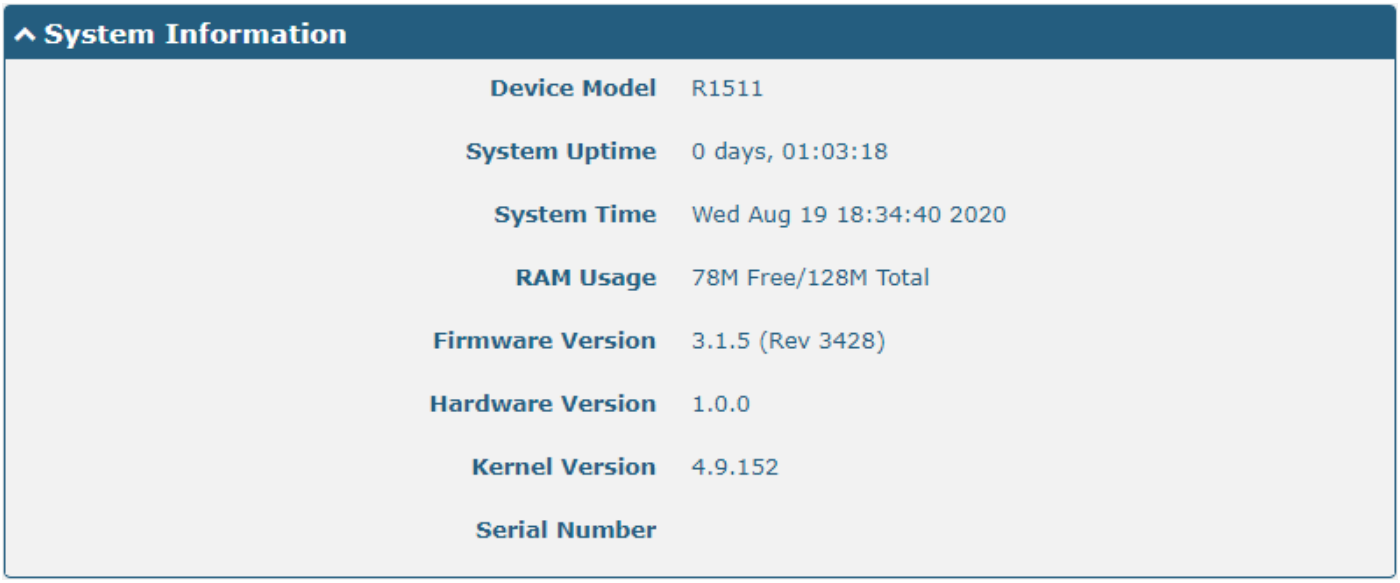
1. Modify in one page;
2. Click Submit under this page;
3. Modify in another page;
4. Click Submit under this page;
5. Complete all modification;
6. Click Save & Apply.

Chapter 4 Router Configuration

4.1 Status

4.1.1 System Information

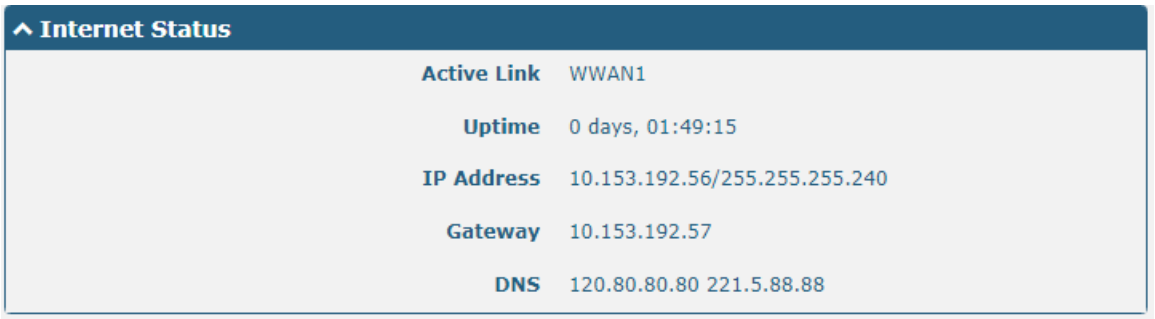
This section allows you to view the System Information of your Router.



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, from which you can get information such as the router's time of delivery.

4.1.2 Internet Status

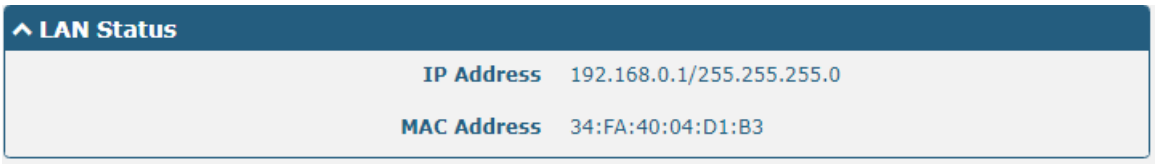
This section shows the Internet status information of your Router.



Internet Status	
Item	**Description**
Active Link	Show the current active link. WWAN1 or WAN。
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.

4.1.3 LAN Status

This section shows the router's LAN status information.

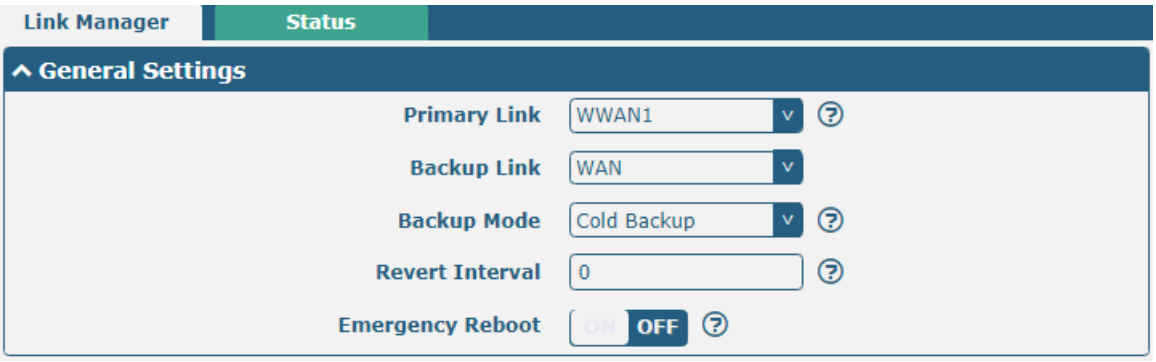


LAN Status	
Item	**Description**
IP Address	Show the IP address and the Netmask of the router.
MAC Address	Show the MAC address of the router.

4.2 Interface

4.2.1 Link Manager

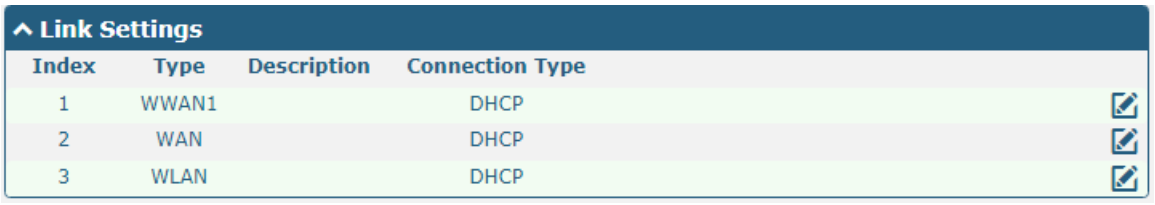
This section allows you to setup the connection of Link Manager. Link manager is a network link backup function that provides mobile network and Ethernet link backups.



General Settings @ Link Manager		
Item	**Description**	**Default**
Primary Link	Select from "WWAN1", "WAN" or "WLAN". • WWAN1: Select to make SIM1 as the primary wireless link • WAN: Select to make WAN as the primary wired 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 **4.2.5 WiFi (Optional)**.	WWAN1
Backup Link	Select from "WWAN1", "WAN", "WLAN" or "None". • WWAN1: Select to make SIM1 as backup wireless link • WAN: Select to make WAN as the backup wired link • WLAN: Select to make WLAN as the backup wireless link **Note:** WLAN link is available only if enable WiFi as Client mode, please refer to **4.2.5 WiFi (Optional)**. • None: Do not select any backup link	None
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 **Note:** Warm backup mode is not available for dual SIM backup. • Load Balancing: Use two links simultaneously	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

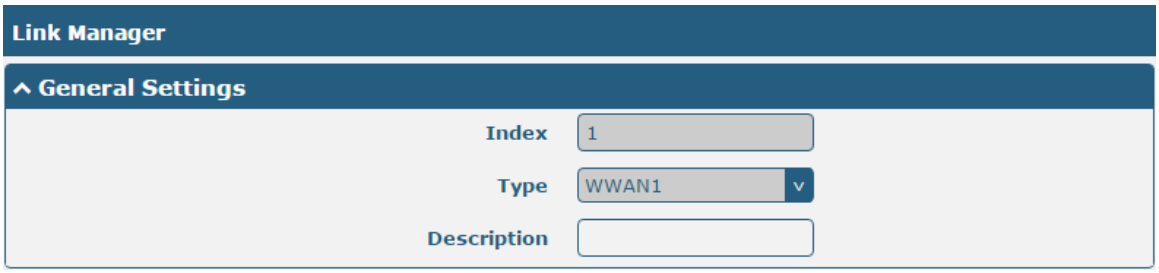
Note: Click ? for help.

Link Settings allows you to configure the parameters of link connection, including WWAN1, 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.

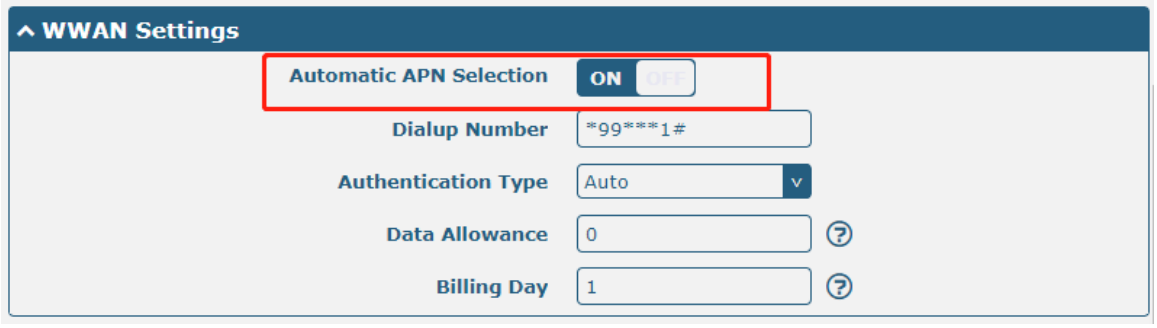


Click on the right-most of WWAN1/WAN/WLAN to enter the configuration window.

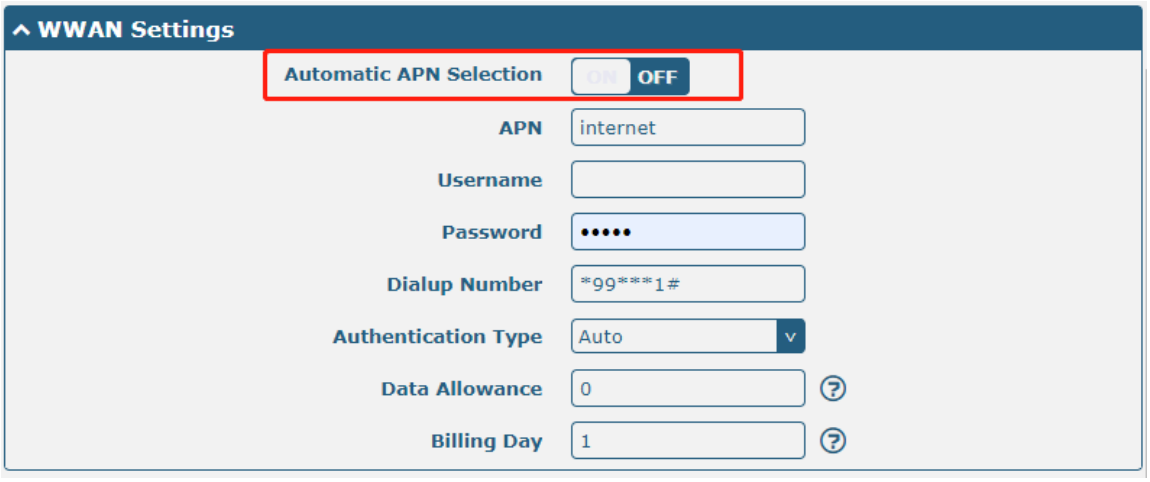
WWAN1

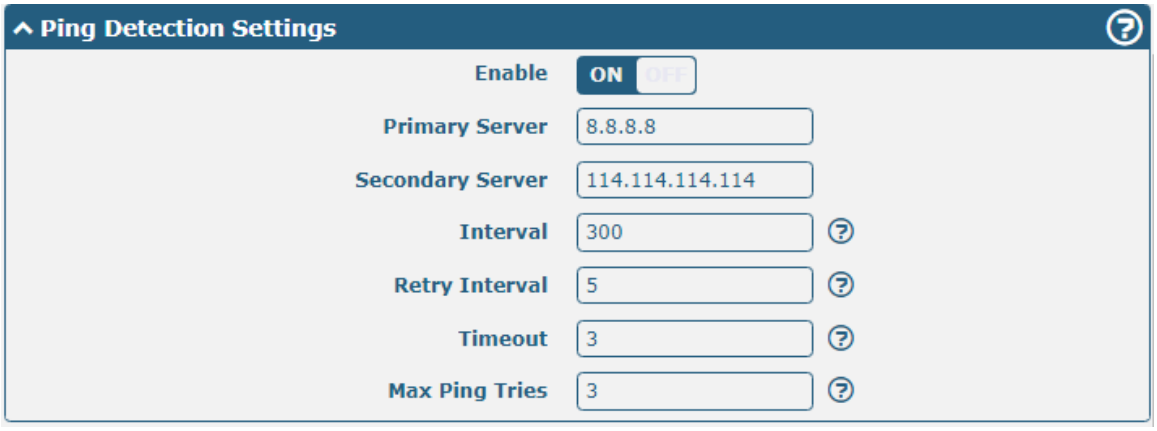


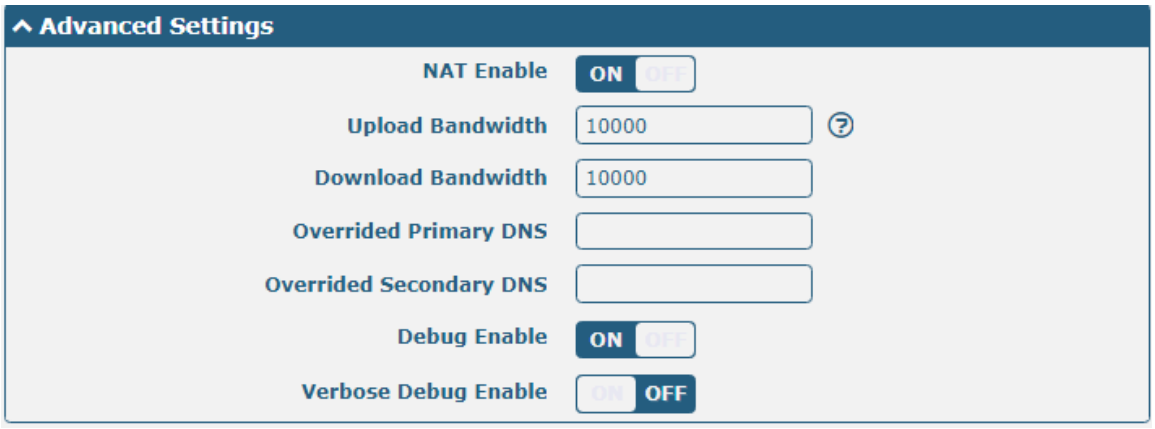
The window is displayed as below when enabling the “Automatic APN Selection” option.



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





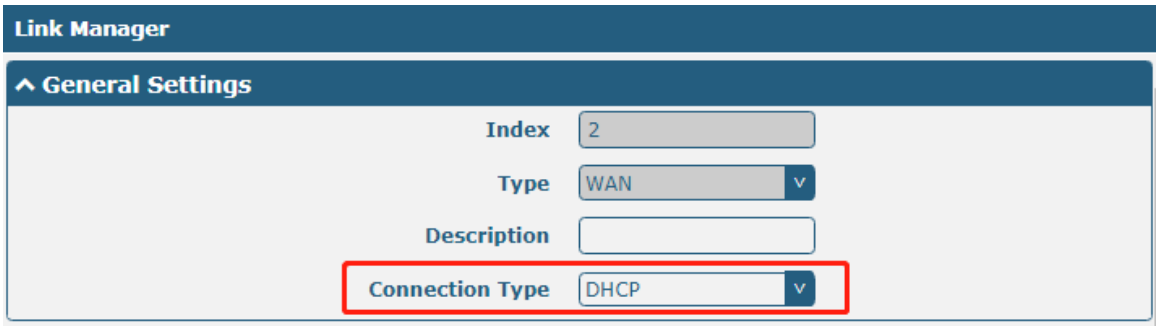


Link Settings (WWAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WWAN1
Description	Enter a description for this link. It can be null.	Null
WWAN Settings		
Automatic APN Selection	Click the toggle button to enable/disable 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
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

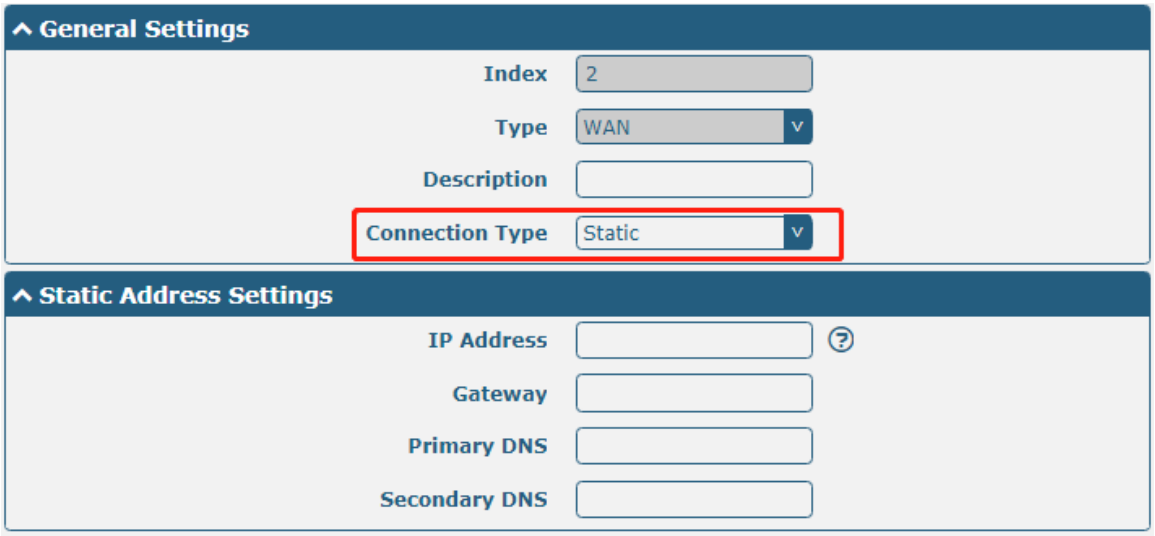
Link Settings (WWAN)		
Item	**Description**	**Default**
Billing Day	Specify the monthly billing day. The data traffic statistics will be recalculated from that day.	1
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keep-alive policy of the router.	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
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

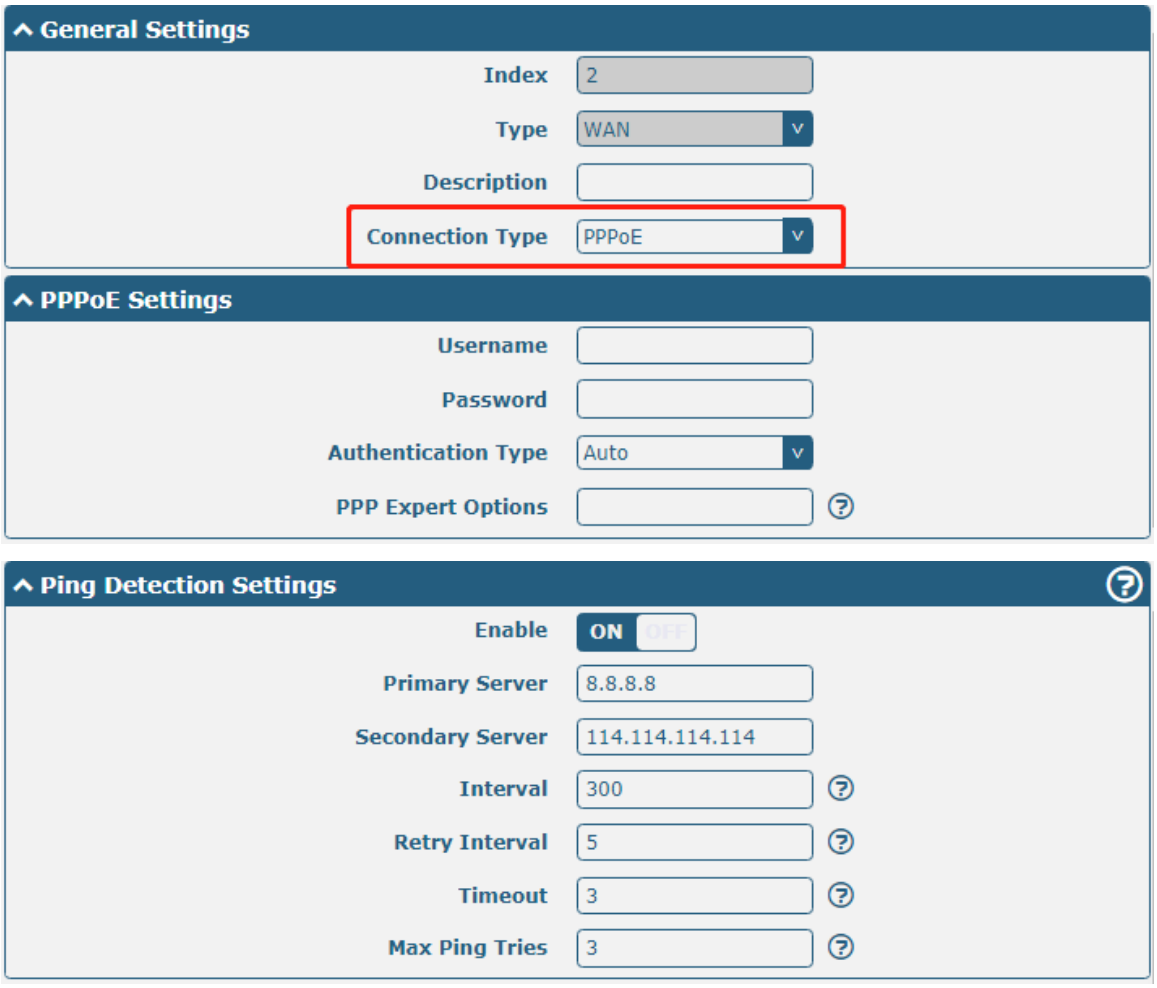
Router will obtain IP automatically from DHCP server if choosing “DHCP” as connection type. The window is displayed as below.

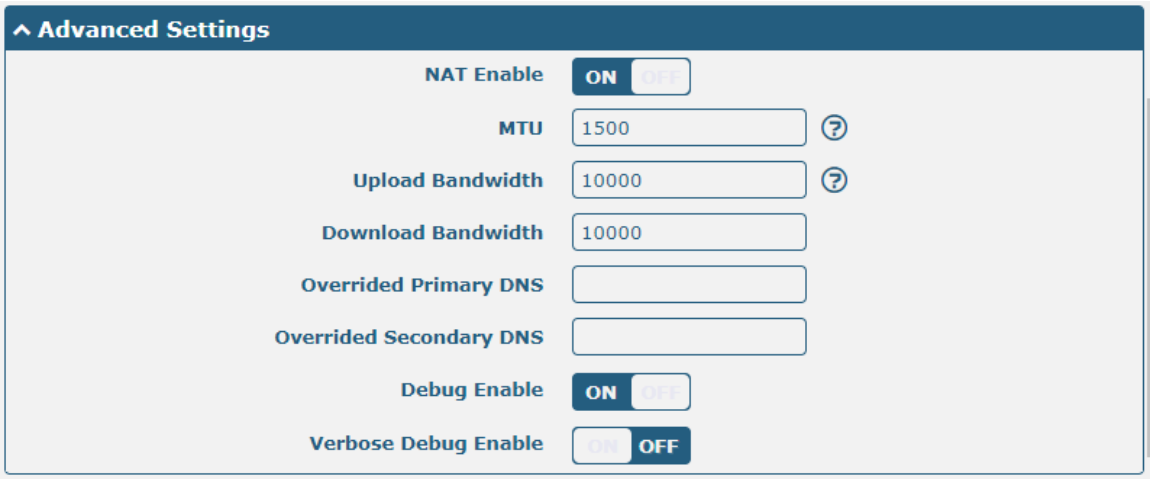


The window is displayed as below when choosing “Static” as the connection type.



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





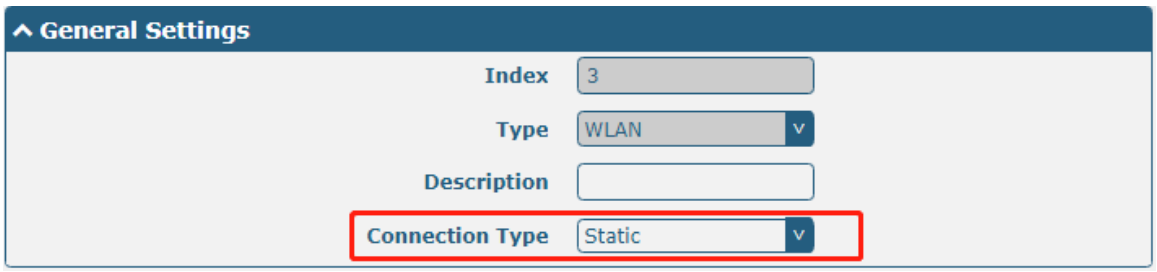
Link Settings (WAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WAN
Description	Enter a description for this link. It can be null.	Null
Connection Type	Select from “DHCP”, “Static” or “PPPoE”.	DHCP
Static Address Settings		
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 keep-alive 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	3

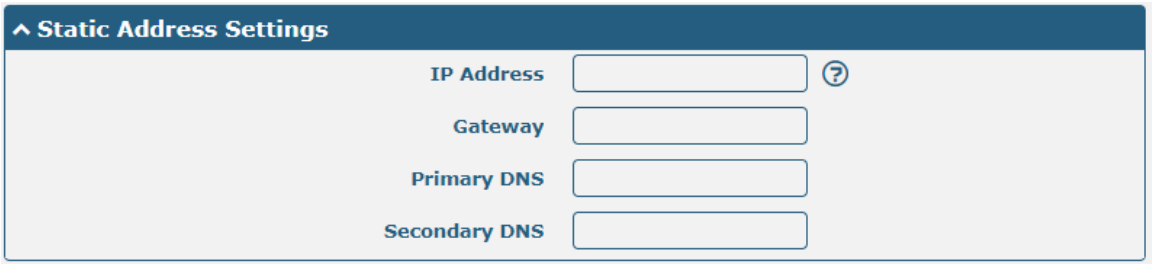
	the max continuous ping tries reached.	
Advanced Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	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

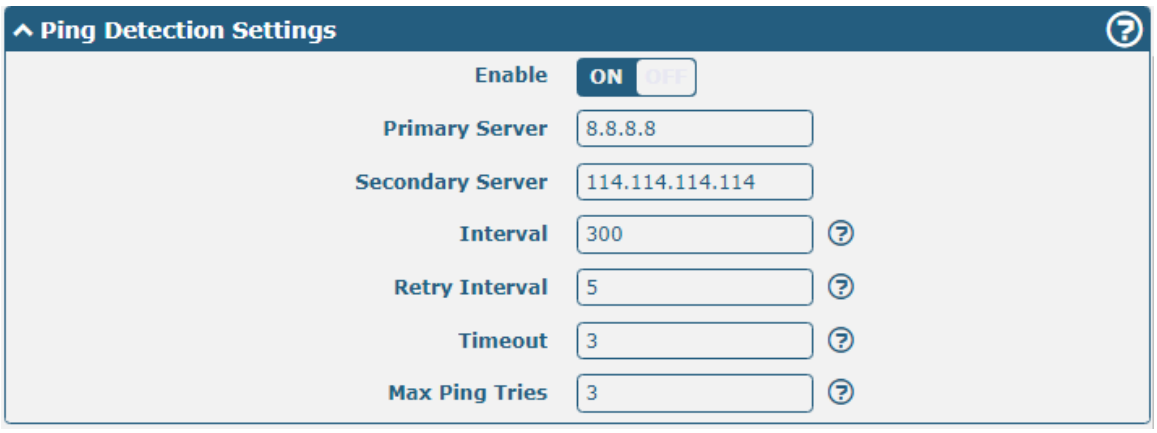
WLAN

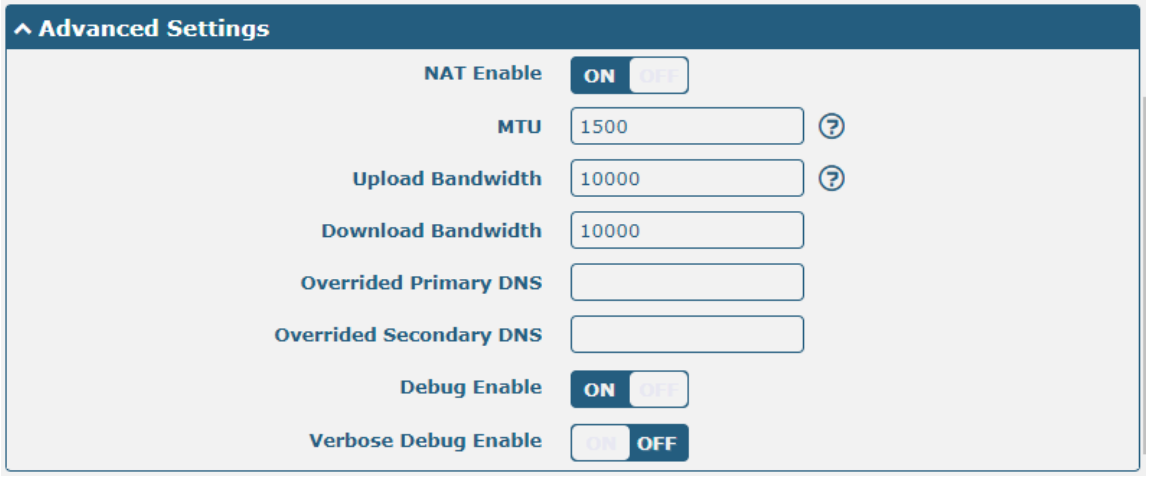
Router will obtain IP automatically from the WLAN AP if choosing “DHCP” as the connection type. The specific parameter configuration of SSID is shown as below.

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







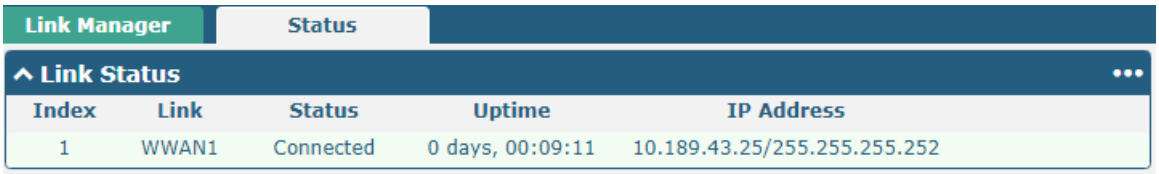


Link Settings (WLAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WLAN
Description	Enter a description for this link. It can be null.	Null
Connection Type	Select from “DHCP” or “Static”.	DHCP
WLAN Settings		
SSID	Enter 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

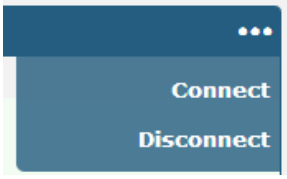
Static Address Settings		
IP Address	Enter the IP address with Netmask which can access the Internet, e.g. 192.168.1.1/24	Null
Gateway	Enter the IP address of WiFi AP.	Null
Primary DNS	Set the primary DNS.	Null
Secondary DNS	Set the secondary DNS.	Null
Ping Detection Settings		
Enable	Click the toggle 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

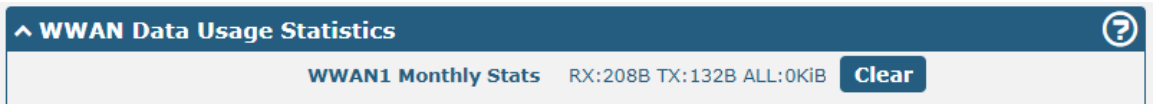
This page allows you to view the status of link connection and clear the monthly data usage statistics.



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 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**.

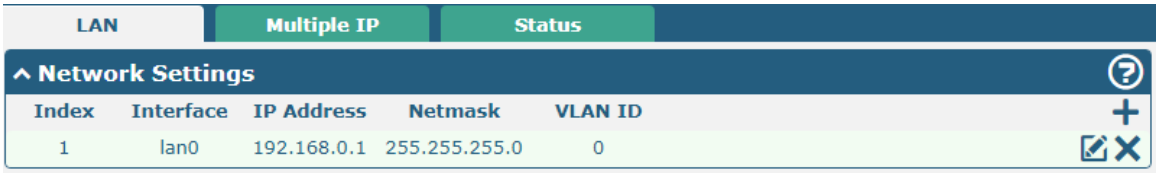
4.2.2 LAN

This section allows you to set the related parameters for LAN port. There are two LAN ports on R1511 Router, including ETH0, and ETH1. Wan is assigned as ETH0. The ETH0 and ETH1 can freely choose from lan0 and lan1, but at least one LAN port must be assigned as lan0. The default settings of ETH0 and ETH1 are lan0 and their default IP are 192.168.0.1/255.255.255.0.

LAN

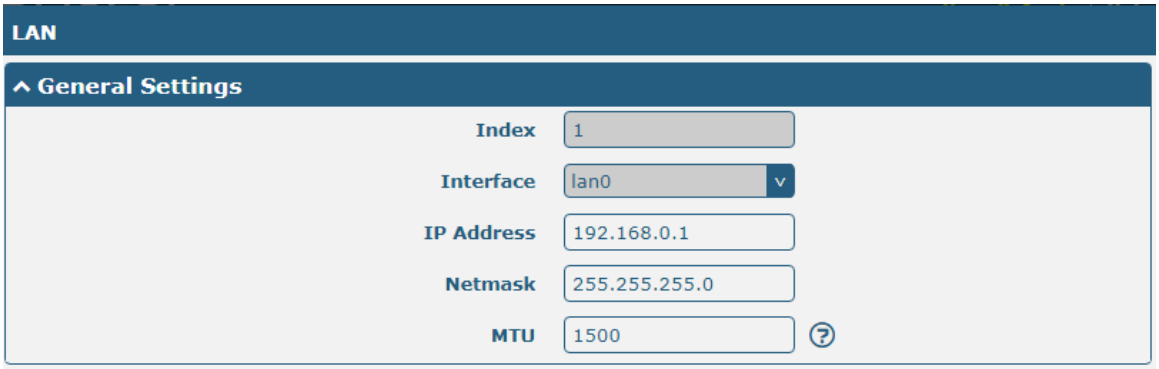
By default, there is a LAN port (lan0) in the list. To begin adding a new LAN port (lan1), please configure ETH1, ETH2

or ETH3 as lan1 first in **Ethernet > Ports > Port Settings**. Otherwise, the operation will be prompted as “List is full”.



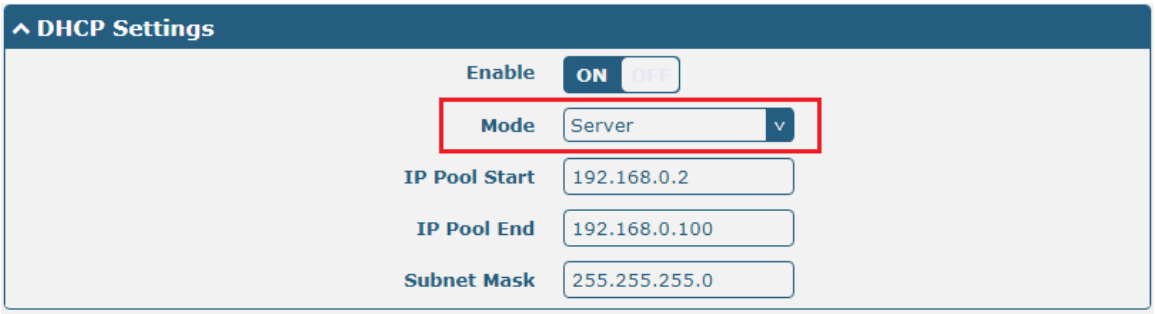
Note: Lan0 cannot be deleted.

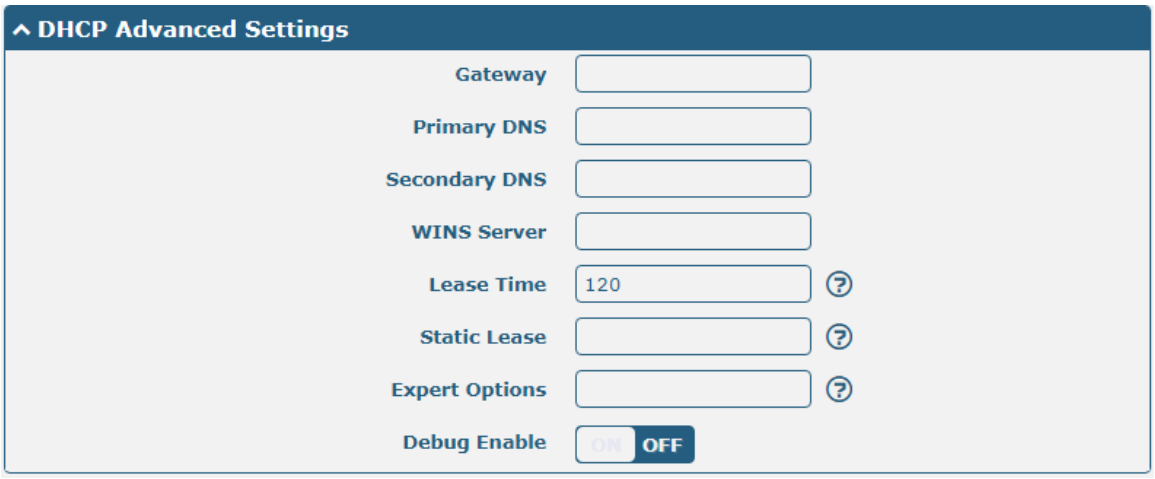
You may click + to add a new LAN port, or click ✕ to delete the current LAN port. Now, click to edit the configuration of the LAN port.



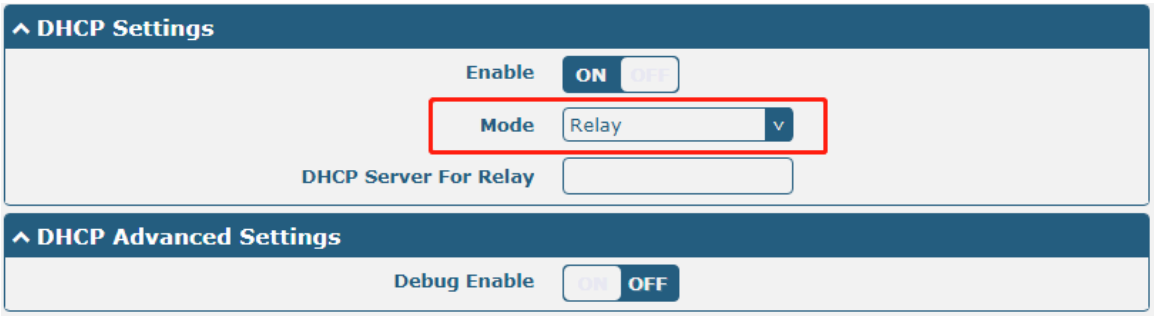
General Settings @ LAN		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Interface	Show the editing port. **Note:** Lan1 is available only if it was selected by one of ETH0~ETH1 in **Ethernet > Ports > Port Settings**.	--
IP Address	Set the IP address of the LAN port.	192.168.0.1
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.





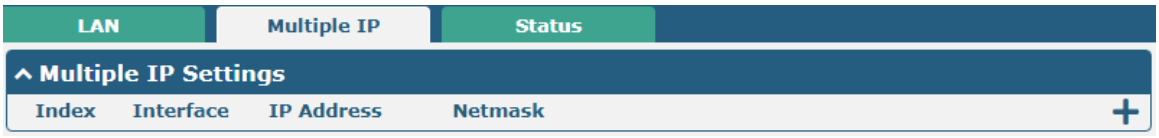
The window is displayed as below when choosing “Relay” as the mode.



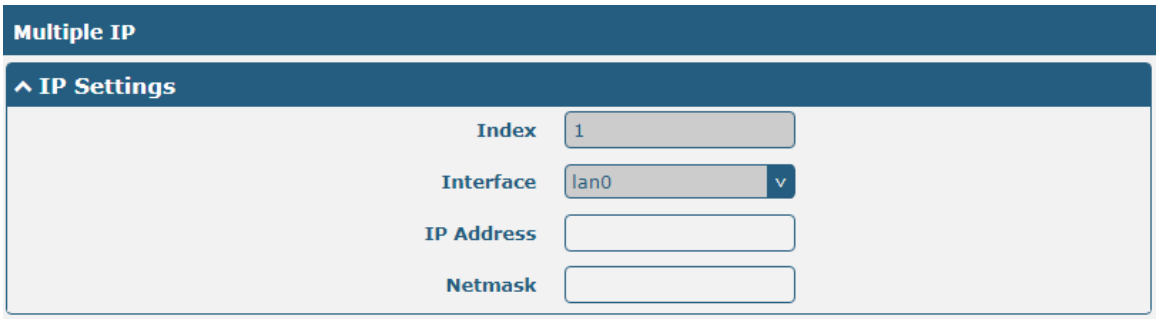
LAN		
Item	**Description**	**Default**
DHCP Settings		
Enable	Click the toggle button to enable/disable the DHCP function.	ON
Mode	Select the mode of DHCP from “Server” or “Relay”. • Server: Lease IP address to DHCP clients which have been connected to LAN port • Relay: Router can be DHCP Relay, which will provide a relay tunnel to solve problem that DHCP Client and DHCP Server is 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

LAN		
Item	**Description**	**Default**
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



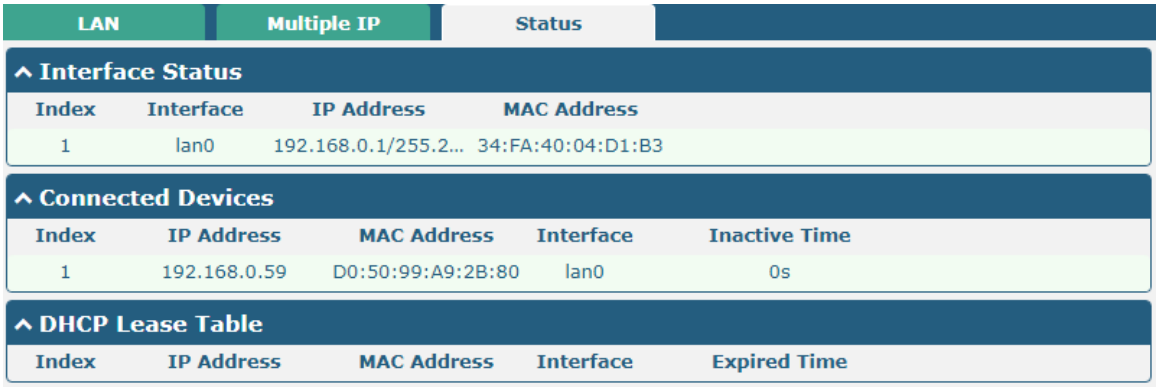
You may click + to add a multiple IP to the LAN port, or click ✕ to delete the multiple IP of the LAN port. Now, click to edit the multiple IP of the LAN port.



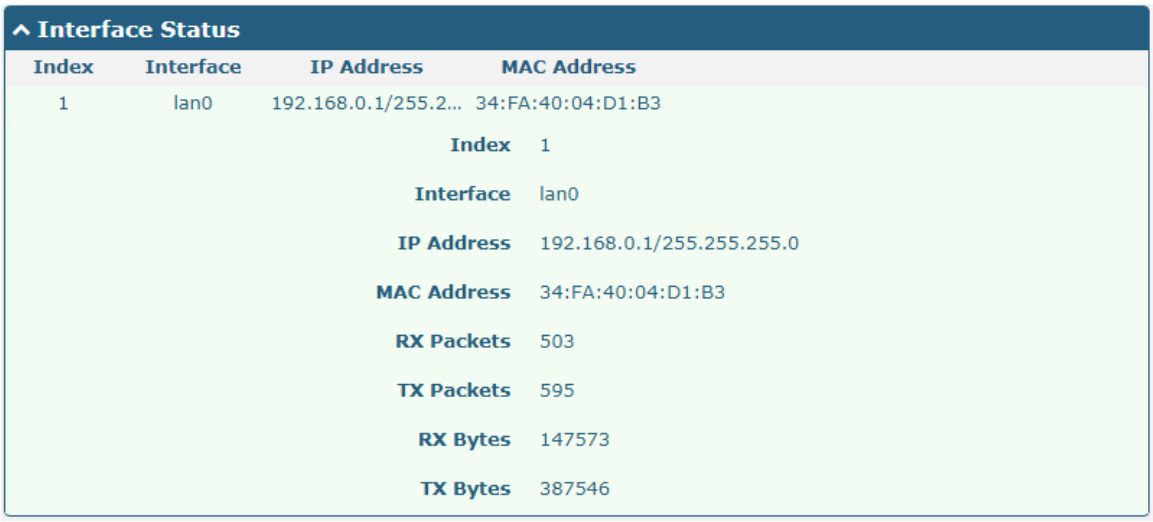
IP Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Interface	Show the editing port, read only.	--
IP Address	Set the multiple IP address of the LAN port.	Null
Netmask	Set the multiple Netmask of the LAN port.	Null

Status

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

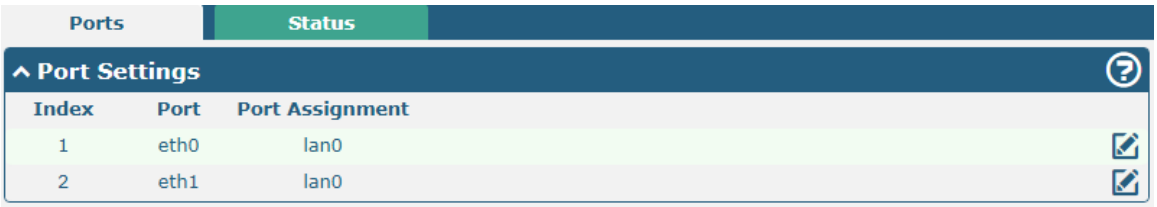


Click the row of status, the details status information will be display under the row. Please refer to the screenshot below.

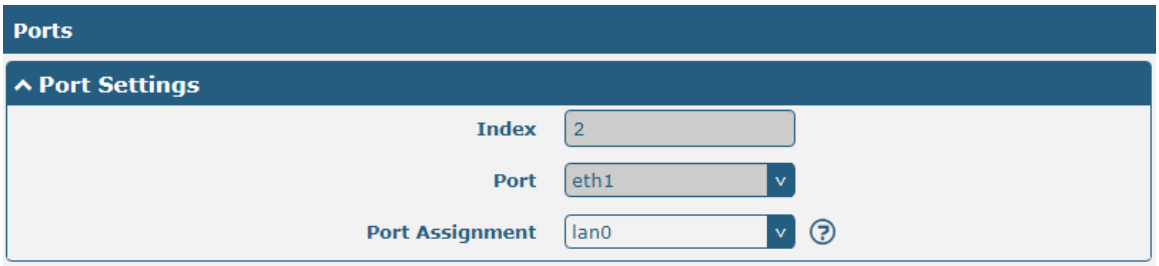


4.2.3 Ethernet

This section allows you to set the related parameters for Ethernet. There are two Ethernet ports on R1511 Router, including ETH0 and ETH1. ETH0 can be configured as the WAN port for the router to access the outer network or the LAN port for the lower end devices to connect with the router. ETH1 can only be configured as a LAN port for the lower device to connect to the router. By default, ETH0 and ETH1 are lan0, and their IP are 192.168.0.1/255.255.255.0.

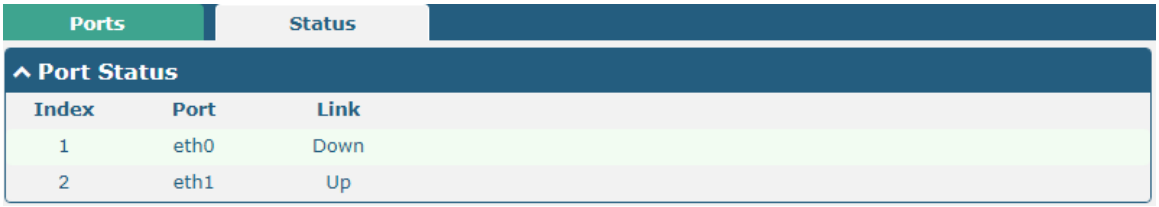


Click the button on the right-most of eth1 to change the port parameters in the port window that pops up.

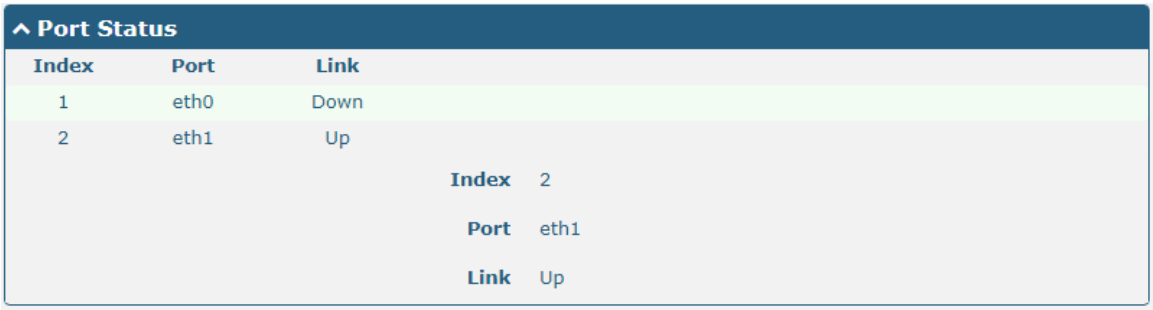


Port Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Port	Show the editing port, read only.	--
Port Assignment	Choose the Ethernet port's type, as a WAN port or a LAN port. When setting the port as a LAN port in **Interface > LAN > LAN > Network Settings > General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

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

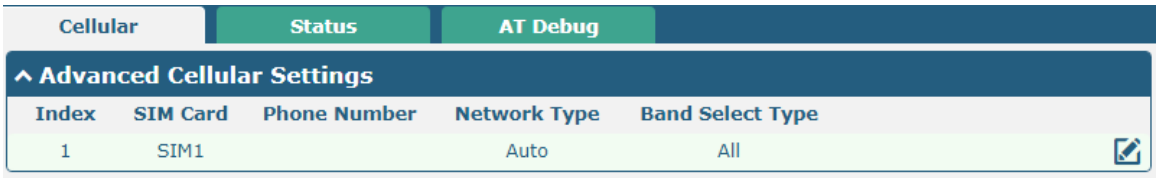


Click the row of status, the details status information will be display under the row. Please refer to the screenshot below.

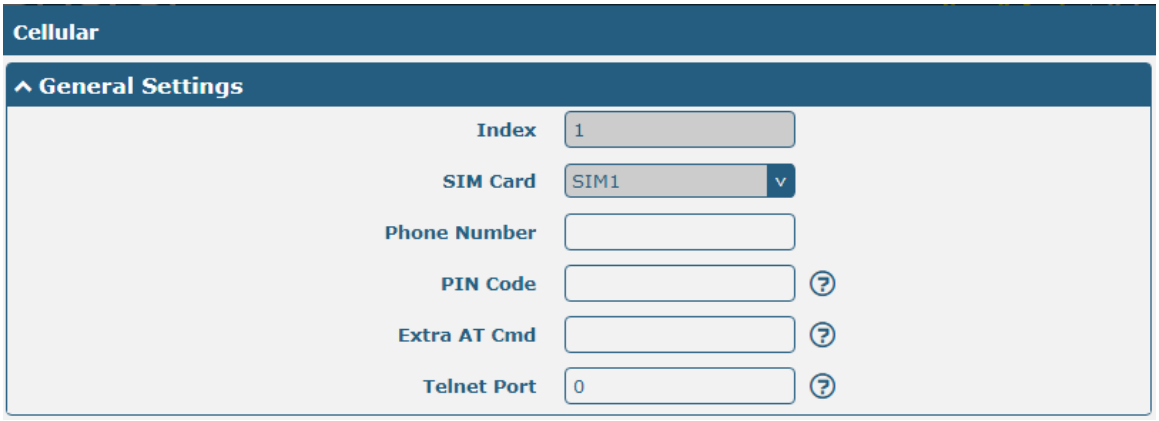


4.2.4 Cellular

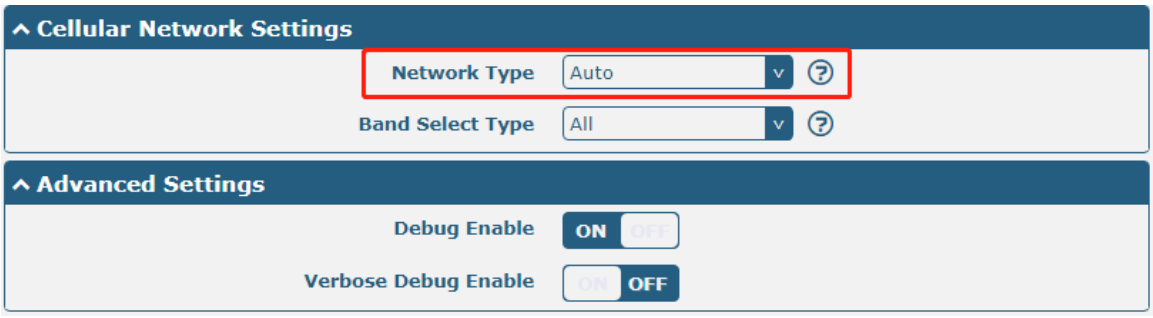
This section allows you to set the related parameters of Cellular. The R1511 Router has one SIM card slot.



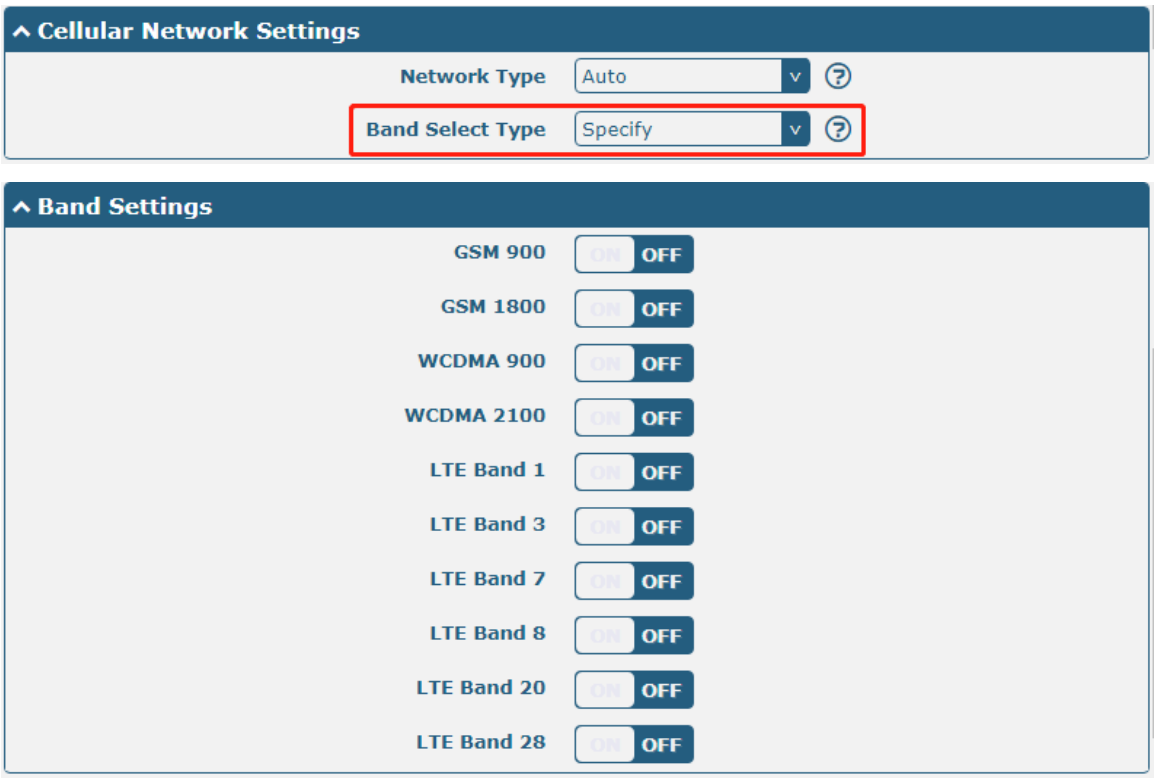
Click the right most button of SIM 1 to edit the parameters.



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

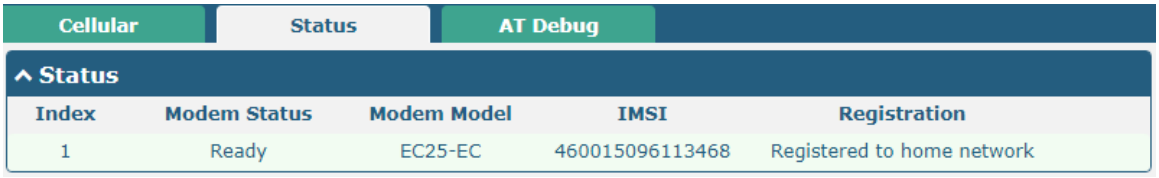


The window is displayed as below when choosing “Specify” as the band select type.



Cellular		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
SIM Card	Set 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”, “2G Only”, “2G First”, “3G Only”, “3G First”, “4G Only”, “4G First”. • Auto: Connect to the best signal network automatically • 2G Only: Only the 2G network is connected • 2G First: Connect to the 2G Network preferentially • 3G Only: Only the 3G network is connected • 3G First: Connect to the 3G Network preferentially • 4G Only: Only the 4G network is connected • 4G First: Connect to the 4G Network preferentially	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.

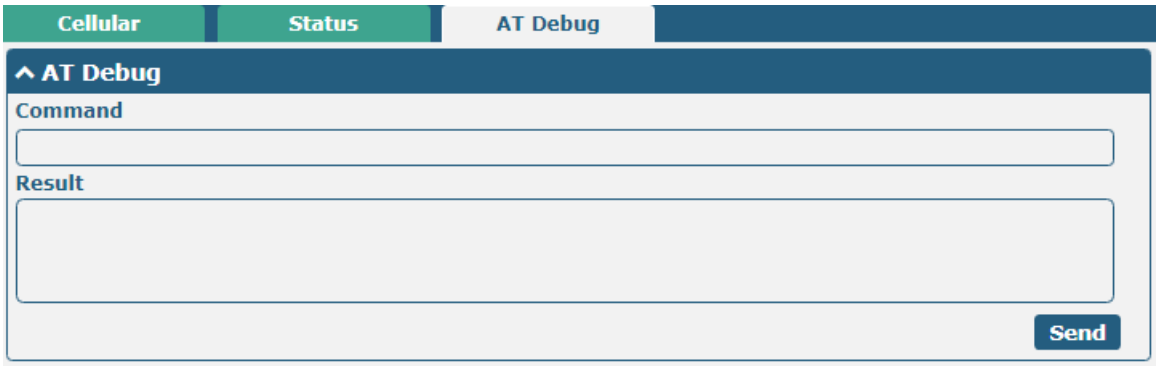


Click the row of status, the details status information will be displayed under the row.

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. **Note:** This option will be displayed if enter manually in **Cellular > Advanced Cellular Settings > SIM1 > General Settings > Phone Number**.
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.
Community ID	Show the current Community ID used for locating the router.

Status	
Item	**Description**
IMEI	Show the IMEI (International Mobile Equipment Identity) number of the radio module.
Firmware Version	Show the current firmware version of the radio module.

Click the "AT Debug" to detect the AT command.



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.	--

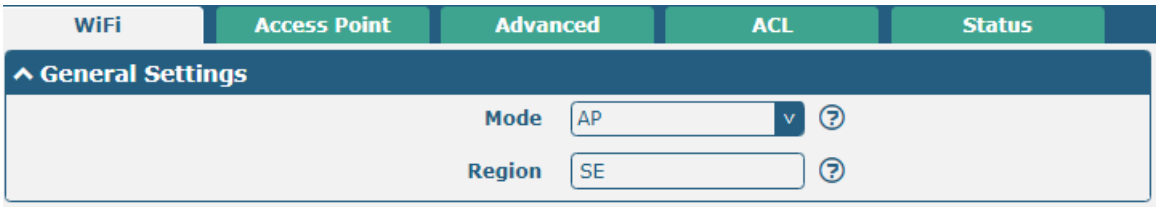
4.2.5 WiFi

This section allows you to configure the parameters of WiFi AP and WiFi Clinet. Router supports either WiFi AP mode or Client mode, and defaults as AP.

WiFi AP

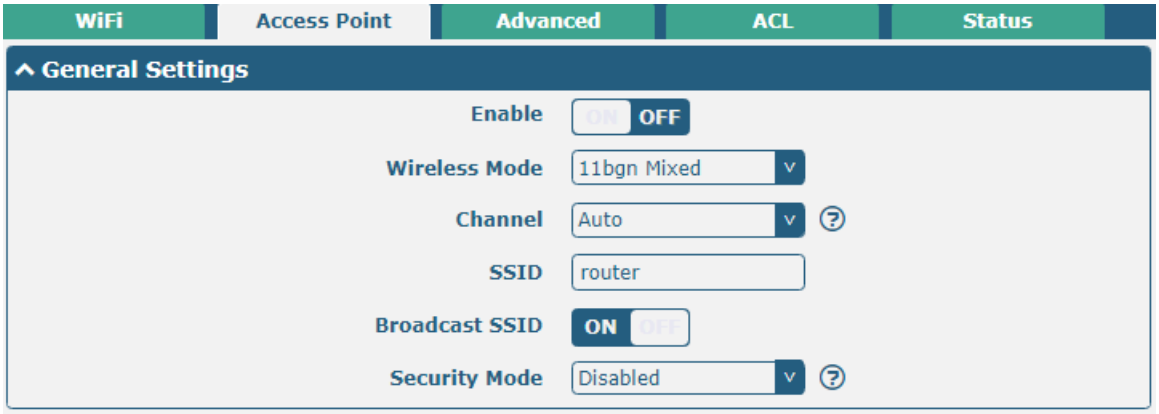
Configure Router as WiFi AP

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



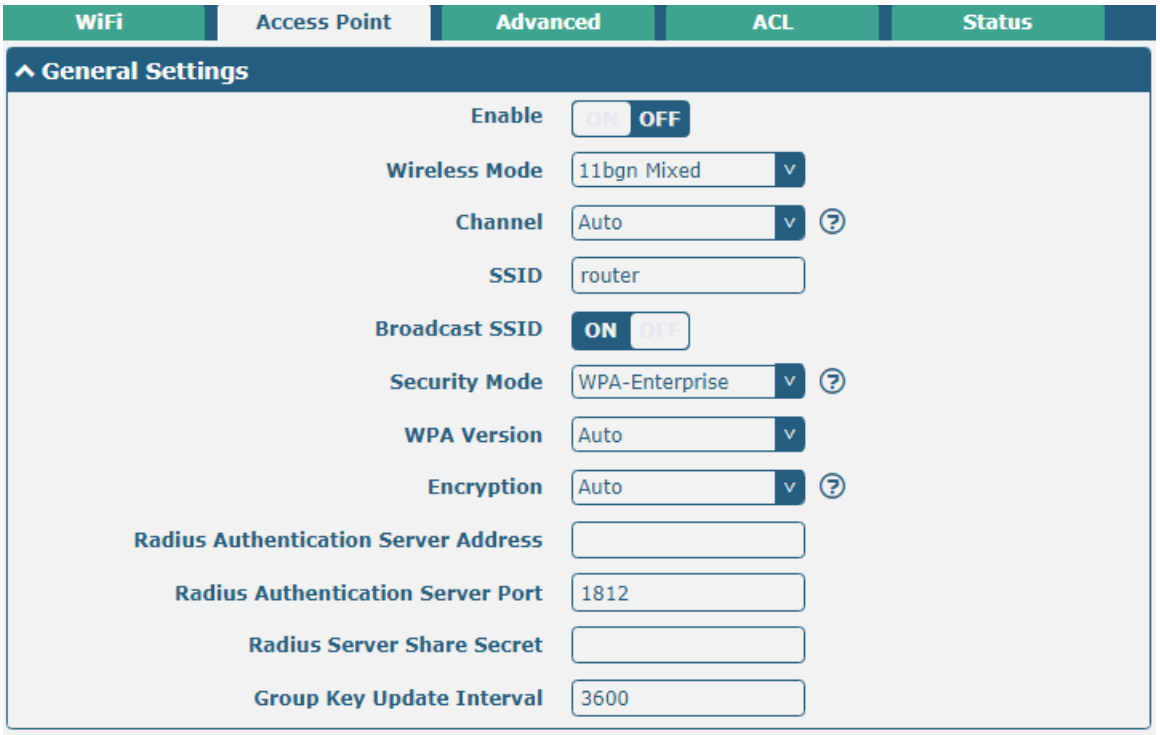
Note: Please remember to click **Save & Apply** after finish the configuration, so that the configuration can be took effect.

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

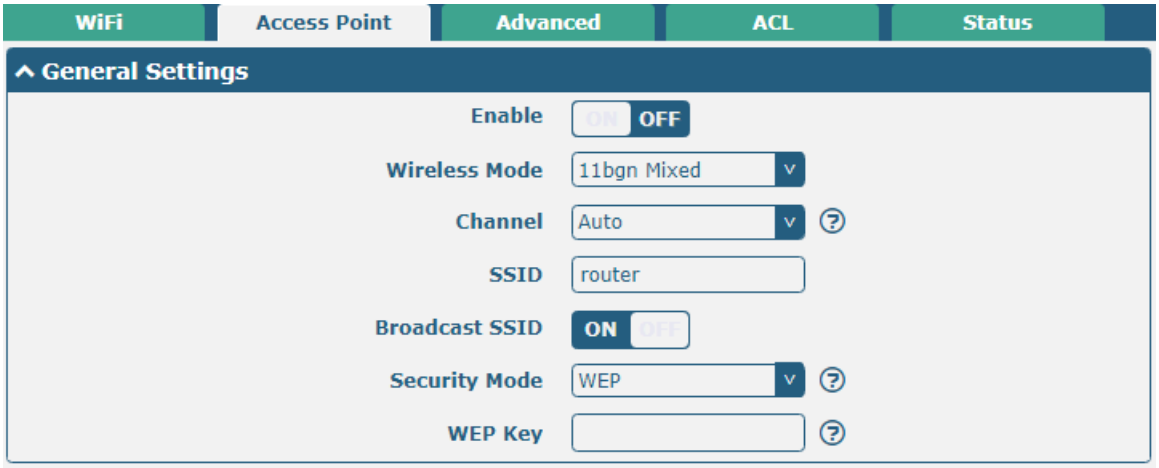


The window is displayed as below when setting “WPA-Personal” as the security mode.

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



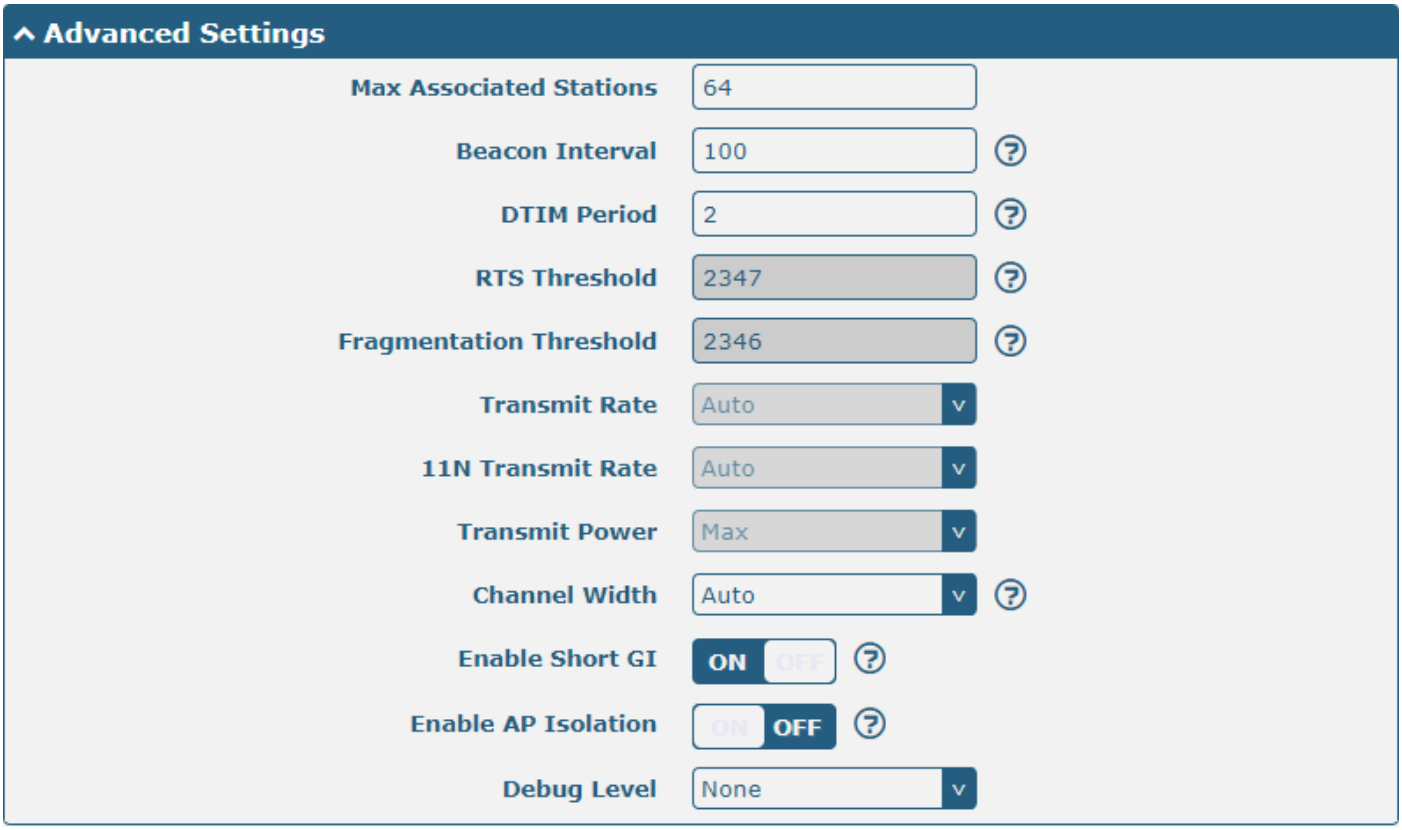
The window is displayed as below when setting “WEP” as the security mode.



General Settings @ Access Point		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the WiFi access point option.	OFF
Wireless Mode	Select from “11bgn Mixed mode”, “11b only”, “11g only” and “11n only”. • 11bgn Mixed mode: mix three protocols for backward compatibility • 11b only: IEEE 802.11b, 11 Mbps~2.4GHz • 11g only: IEEE 802.11g, 54 Mbps~2.4GHz • 11n only: IEEE 802.11n, 300 Mbps	11bgn Mixed mode
Channel	The channel that different bandwidth can choose is as follows. • Auto: Router will scan all frequency channels until the best one is found • 1~13 channel 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

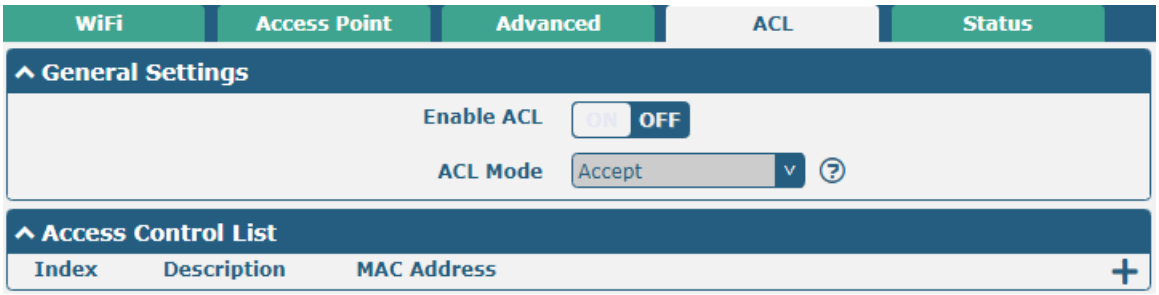
General Settings @ Access Point		
Item	**Description**	**Default**
SSID	Enter the Service Set Identifier, the name of your wireless network. The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other. Enter 1 to 32 characters.	router
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-Personal”, “WPA-Enterprise”, 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-personal: WiFi access protection, only one password is provided for identity authentication • WPA- enterprise: Using RADIUS service for Wi Fi security network protection • 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 “TKIP” or “AES”. • TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication • 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 **Note:** The security mode will affect wireless communication rate. Different wireless modes support different encryption modes. For example, 802.11n supports neither WEP security mode nor TKIP algorithm. If they are used, the wireless communication rate will reduce to 54Mbps (802.11g mode). It is recommended to select AES in 802.11n mode.	Auto

General Settings @ Access Point		
Item	**Description**	**Default**
PSK Password	Enter the Pre share key password. Enter 8 to 63 characters.	Null
Group Key Update Interval	Enter the time period of group key renewal.	3600
Radius Authentication Server Address	Address used by RADIUS Server	Null
Radius Authentication Server port	Port used by RADIUS Server	1812
Radius Authentication Server Share Key	A trust connection is established between RADIUS client and RADIUS server, and the interaction of authentication message is ensured by shared key	Null
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



Advanced Settings @ Access Point		
Item	**Description**	**Default**
Max Associated Stations	Set the max number of clients allowed to access the router's AP.	64
Beacon Interval	Set the interval of time in which the router AP broadcasts a beacon which is used for wireless network authentication.	100
DTIM Period	Set the delivery traffic indication message period and the router AP will multicast the data according to this period.	2
RTS/CTS Threshold	Set the threshold of "request to send", which is the request to send a threshold. When the threshold set as 2347, the router AP will not send detection signal before sending data. And when the threshold set as 0, the router AP will send detection signal before sending data.	2347
Fragmentation Threshold	Set the fragmentation threshold of a WiFi AP. It is recommended that you use the default value 2346.	2346
Transmit Rate	Specify the data transfer rate or default to automatic.	Auto
11N Transmit Rate	Specifiy the data transfer rate in IEEE 802.11n WiFi mode or default to automatic.	Auto
Transmit Power	Select the transmit power level. Select from "Max", "High", "Medium" or "Low".	Max
Channel width	Optional channel width is "Auto", "20MHz" or "40MHz". Note: The 40MHz channel bandwidth provides an available data transfer rate that is more than twice that of a single 20MHz channel.	Auto
Enable Short GI	Click the toggle button to enable/disable the Short Guard Interval option. Short GI is a blank time between two symbols, providing a long buffer time for signal delay. Using the Short GI would increase	ON

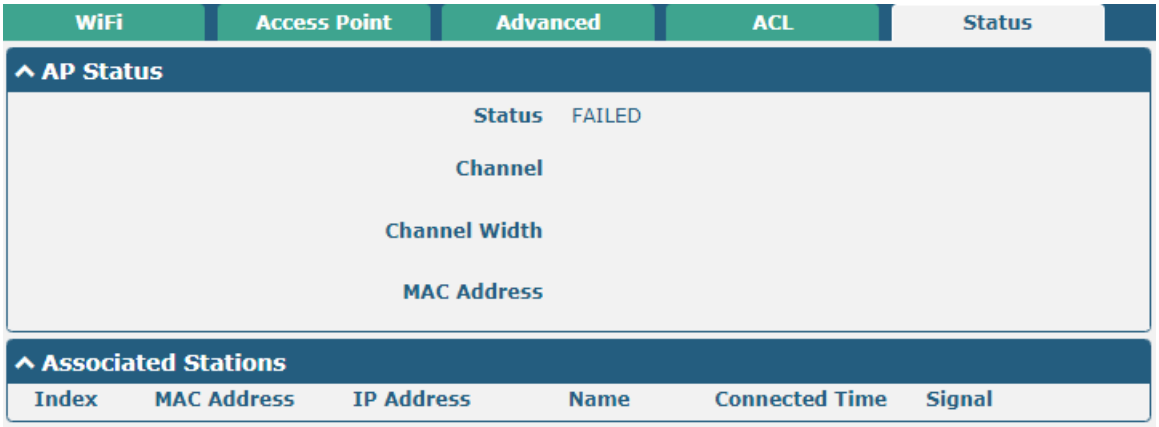
Advanced Settings @ Access Point		
Item	**Description**	**Default**
	11% in data rates, but also result in higher packet error rates.	
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option. When enabled, the router will isolate all connected wireless devices. The wireless device cannot access the router directly via WLAN.	OFF
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 Settings @ Access Point		
Item	**Description**	**Default**
Enable ACL	Click the toggle button to enable/disable this option.	OFF
ACL Mode	Select 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
Access Control List @ Access Point		
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.

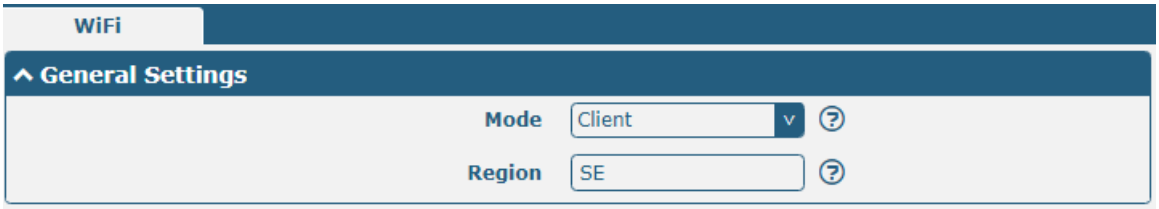


Note: WiFi is off by default. Follow the steps below to enable it and configure the router as WiFi client.

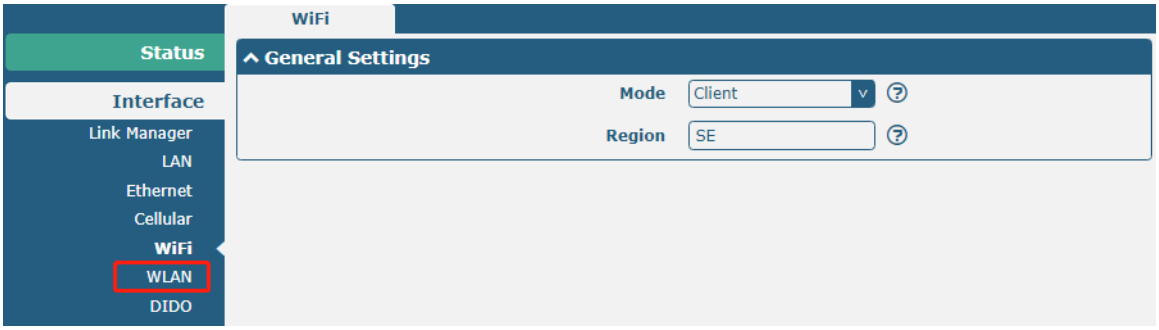
WiFi Client

Configure Router as WiFi Client

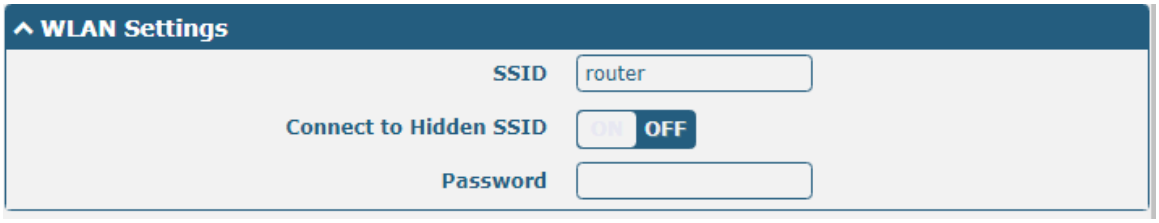
Click **Interface > WiFi > WiFi**, select "Client" as the mode and regarding the AP type to choose the related Client Band then click "Submit".



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.

Status

WLAN Status

Status	Connected
Uptime	0 days, 00:00:06
IP Address	192.168.50.72/255.255.255.0
Gateway	192.168.50.1
DNS	192.168.50.1
MAC Address	34:fa:40:09:09:cc

Link Status

Signal	-67 dBm
Noise	9999 dBm
Width	20 MHz
TX Bitrate	57.8 MBit/s MCS 11 short GI
TX	1442 bytes (11 packets)
RX	39177 bytes (214 packets)

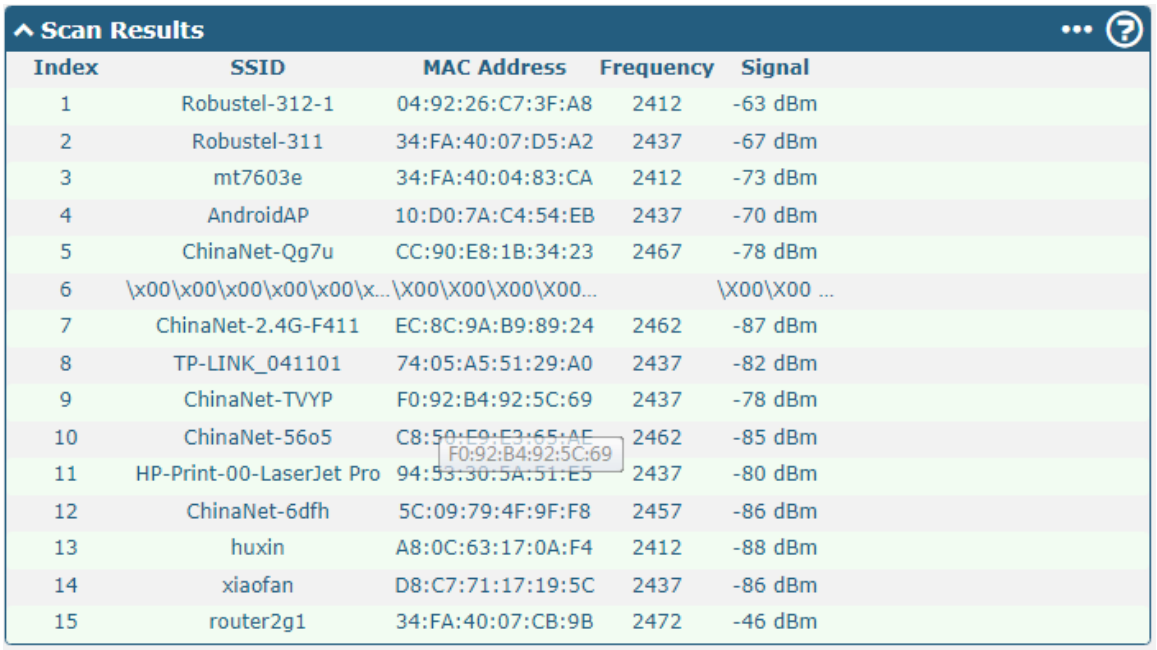
WPA Status

WPA State	COMPLETED
Frequency	2412
BSSID	04:92:26:c7:3f:a8
SSID	Robustel-312-1
Mode	station
Key Management	WPA2-PSK
Pairwise Cipher	CCMP
Group Cipher	CCMP

This window allows you to scan for all available SSIDs in your area. Please click ••• and “Scan Results” list to refresh the surrounding SSID.

Scan Results •••

Index	SSID	MAC Address	Frequency	Signal



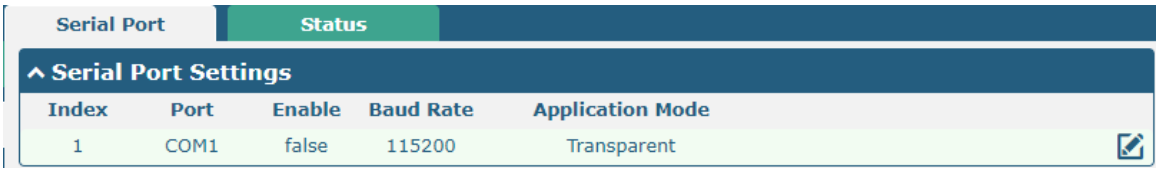
Scan Results

Index	SSID	MAC Address	Frequency	Signal
1	Robustel-312-1	04:92:26:C7:3F:A8	2412	-63 dBm
2	Robustel-311	34:FA:40:07:D5:A2	2437	-67 dBm
3	mt7603e	34:FA:40:04:83:CA	2412	-73 dBm
4	AndroidAP	10:D0:7A:C4:54:EB	2437	-70 dBm
5	ChinaNet-Qg7u	CC:90:E8:1B:34:23	2467	-78 dBm
6	\x00\x00\x00\x00\x00\x...	\X00\X00\X00\X00...		\X00\X00 ...
7	ChinaNet-2.4G-F411	EC:8C:9A:B9:89:24	2462	-87 dBm
8	TP-LINK_041101	74:05:A5:51:29:A0	2437	-82 dBm
9	ChinaNet-TVYP	F0:92:B4:92:5C:69	2437	-78 dBm
10	ChinaNet-56o5	C8:50:E9:E3:65:AE	2462	-85 dBm
11	HP-Print-00-LaserJet Pro	94:53:30:5A:51:E5	2437	-80 dBm
12	ChinaNet-6dfh	5C:09:79:4F:9F:F8	2457	-86 dBm
13	huxin	A8:0C:63:17:0A:F4	2412	-88 dBm
14	xiaofan	D8:C7:71:17:19:5C	2437	-86 dBm
15	router2g1	34:FA:40:07:CB:9B	2472	-46 dBm

F0:92:B4:92:5C:69

4.2.6 Serial port

This section allows you to set the parameters of serial port. The R1511 router supports COM1, which can convert serial port data into IP data or convert IP data into serial port data, and then transmit the data through a wired or wireless network, thereby achieving the function of transparent data transmission.

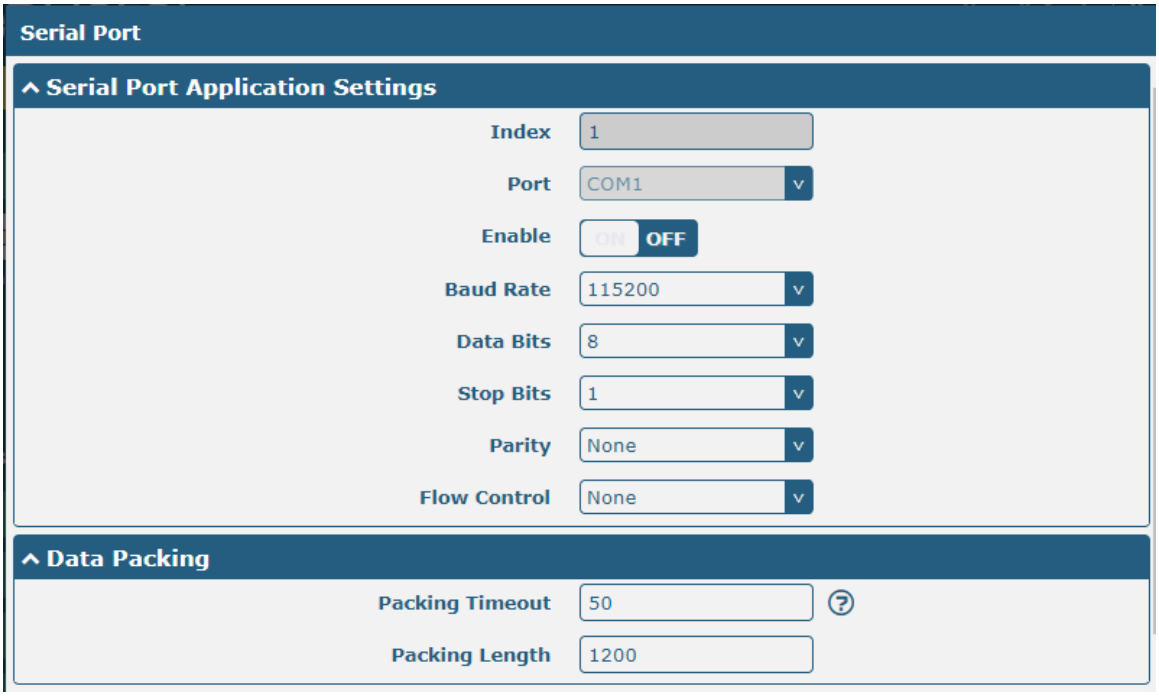


Serial Port | Status

Serial Port Settings

Index	Port	Enable	Baud Rate	Application Mode
1	COM1	false	115200	Transparent

Click the right-most button of serial port as below. The window is displayed as below.



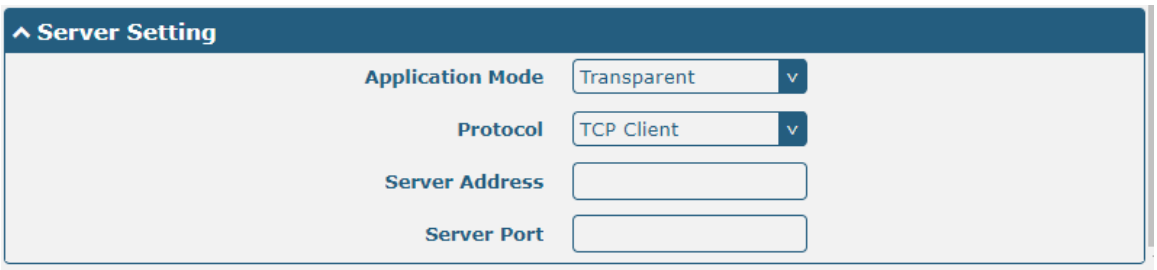
Serial Port

Serial Port Application Settings

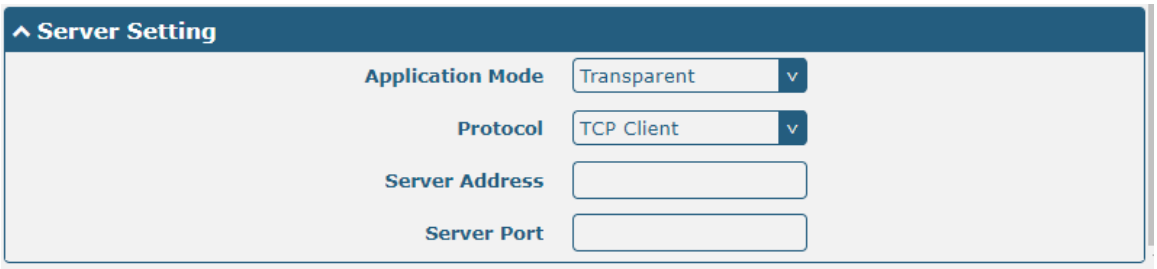
Index	1
Port	COM1
Enable	ON OFF
Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None

Data Packing

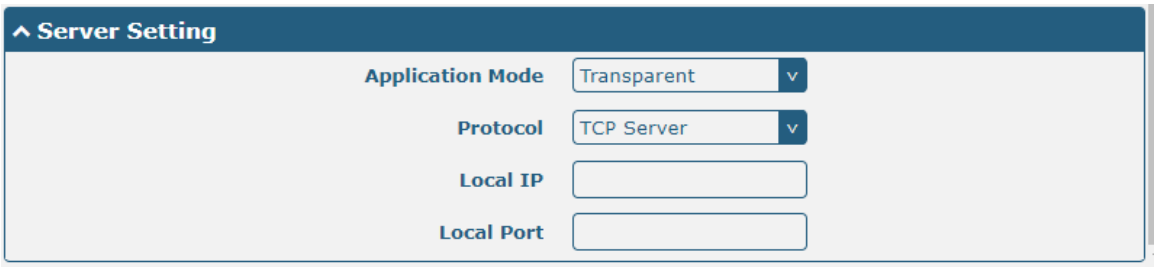
Packing Timeout	50
Packing Length	1200



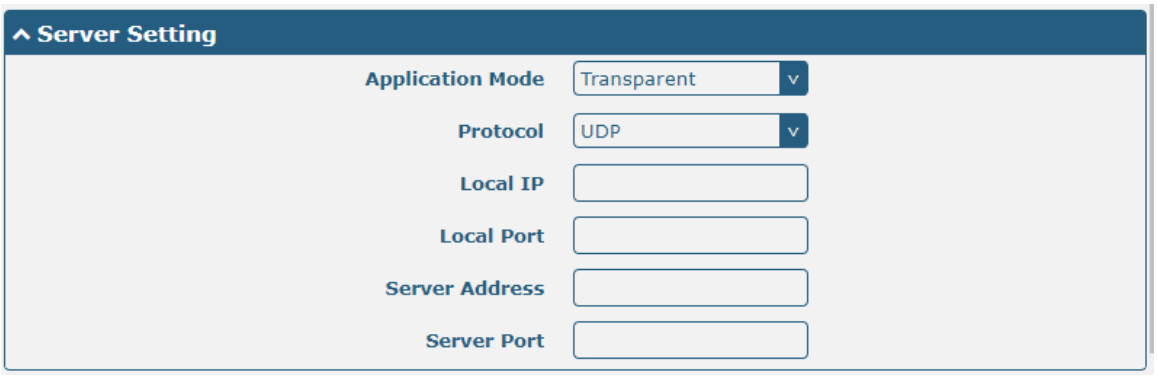
- In the "Server Settings" column, when you select "Transparent Transmission" as the application mode and "TCP Client" as the protocol, the window is as follows:



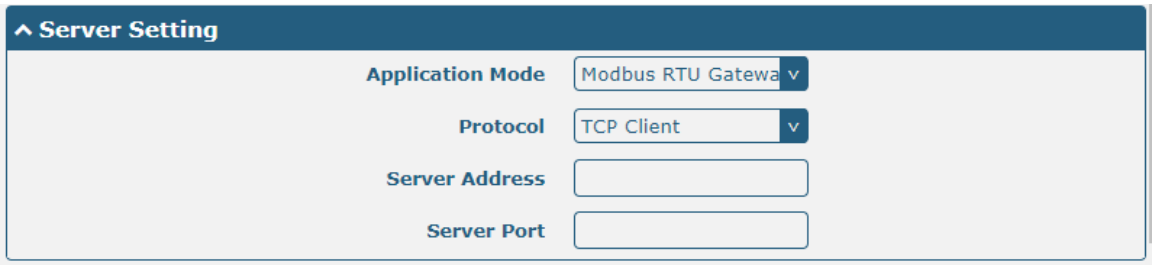
When selecting "Transparent Transmission" as the application mode and "TCP Server" as the protocol, the window is as follows:



When selecting "Transparent Transmission" as the application mode and "UDP" as the protocol, the window is as follows:

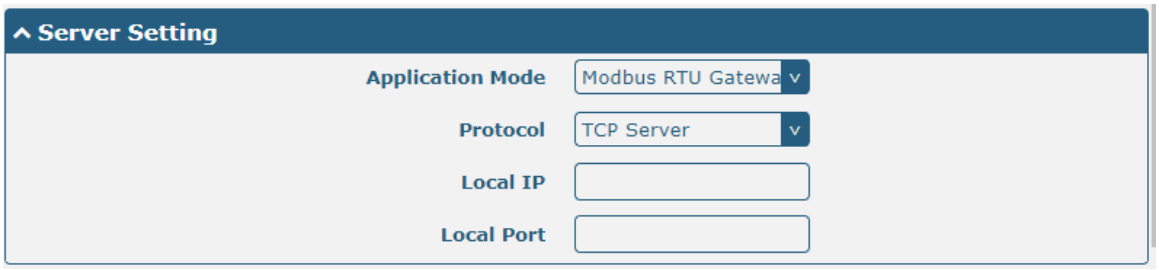


- When selecting "ModBus RTU Gateway" as the application mode and "TCP Client" as the protocol, the window is as follows:

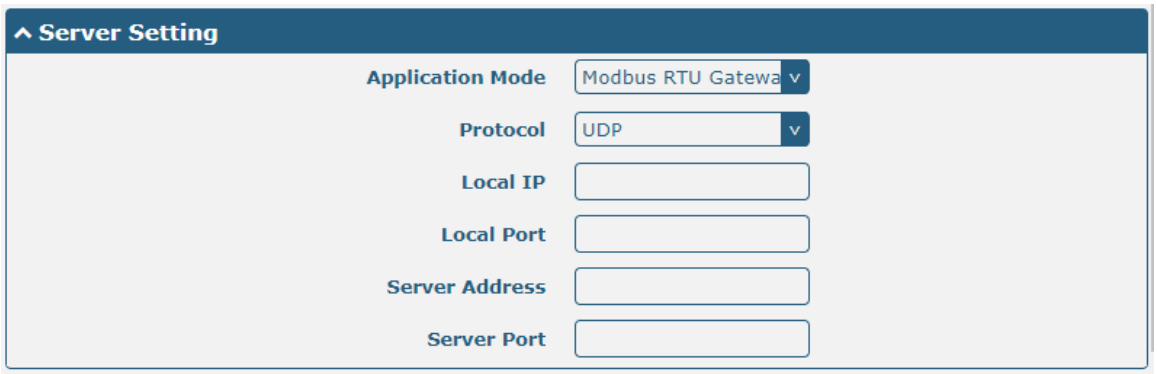


When selecting "ModBus RTU Gateway" as the application mode and "TCP Server" as the protocol, the window

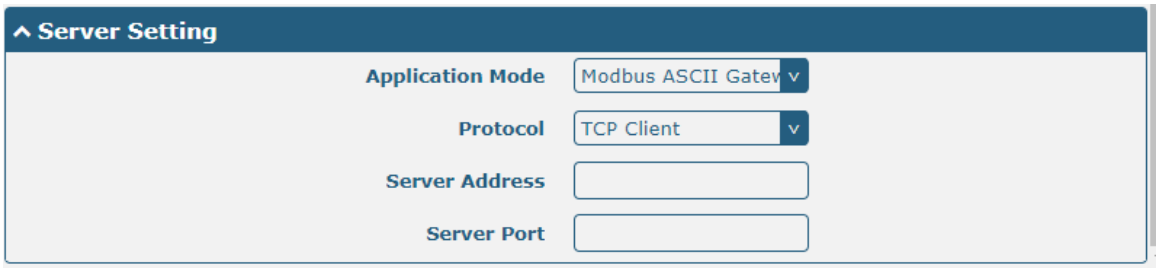
is as follows:



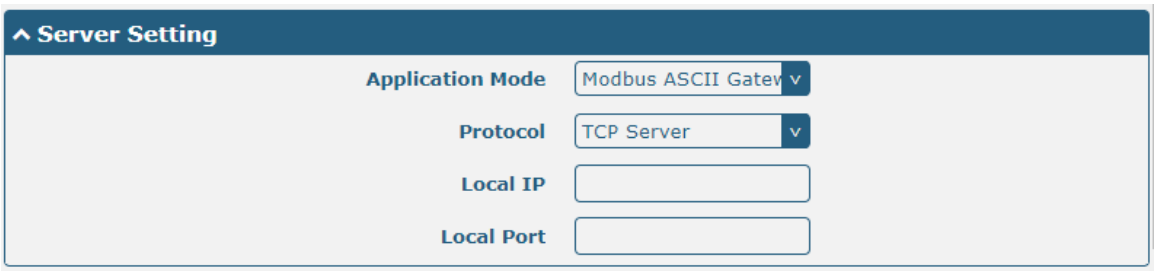
When selecting "ModBus RTU Gateway" as the application mode and "UDP" as the protocol, the window is as follows:



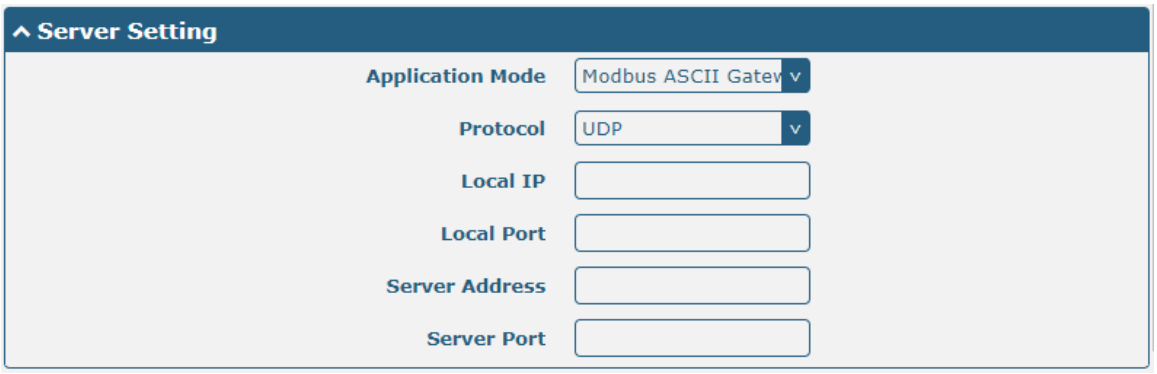
- When selecting "ModBus ASCII Gateway" as the application mode and "TCP Client" as the protocol, the window is as follows:



When selecting "ModBus ASCII Gateway" as the application mode and "TCP Server" as the protocol, the window is as follows:



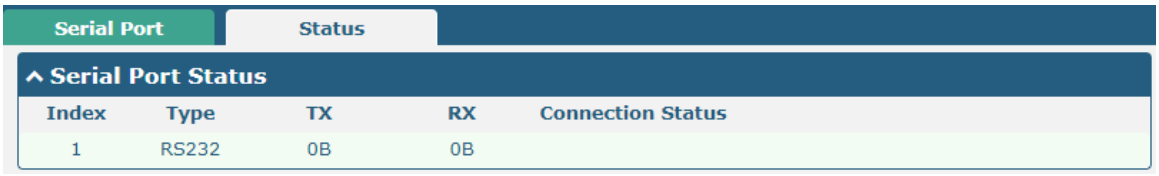
When selecting "ModBus ASCII Gateway" as the application mode and "UDP" as the protocol, the window is as follows:



General Settings @ Serial Port		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
port	Indicate the name of the current serial port and cannot be edited.	COM1
Enable	Click the toggle button to enable/disable this port.	OFF
Baud rate	Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400", "57600" and "115200".	115200
Data bit	Select from "7" and "8".	8
Stop bit	Select from "1" and "2".	1
Check Digit	Select from "None", "Odd Parity" and "Even Parity".	No
Flow Control	Select from "None", "Hardware" and "Software".	No
Data packing		
Packing timeout	Set the packaging timeout period. The serial port arranges the data in the buffer, and when the interval timeout period is reached, it will send the data to the mobile WAN/Ethernet WAN. The unit is milliseconds. Note: Even if the interval timeout period is not reached, the data will be sent when it is the same as the specified packet length or the set delimiter.	50
Packed data length	Set the length of the packed data. The packet length setting refers to the maximum amount of data that the serial buffer allows to accumulate before sending. When the packet length is set to 0, the maximum amount of data is not specified; when the specified interval timeout time is reached, when the set delimiter is detected or the buffer is full, the data in the buffer will be sent out; when the packet When the length is specified as between 1 and 3000 bytes, the data in the buffer will be sent out when it reaches the specified length. Note: Even if the preset packet length is not reached, the data will be sent out when the specified interval timeout time or the set delimiter is reached.	1200
Server settings		
Application mode	Select from "Transparent Transmission", "ModBus RTU Gateway", and "ModBus ASCII Gateway". • Transparent transmission: The router will transparently transmit serial data that is not encapsulated with any protocol • ModBus RTU gateway: the router converts ModBus RTU data into ModBus TCP data, and vice versa	Transparent Transmission

General Settings @ Serial Port		
Item	**Description**	**Default**
	• ModBus ASCII gateway: the router converts ModBus ASCII data into ModBus TCP data, and vice versa	
Protocol	Select from "TCP Client", "TCP Server", and "UDP". • TCP client: The router acts as a TCP client and initiates a TCP connection to the TCP server. The server address can be either an IP address or a domain name • TCP server: The router acts as a TCP server and listens to connection requests from TCP clients • UDP: The router acts as a UDP client	TCP Client
Server address	Enter the address of the opposite server.	Null
Server port	Enter the port of the opposite server.	Null
Local IP@Transparent Transmission	Enter the IP address of the router.	Null
Local port @ transparent transmission	Enter the local port of TCP or UDP.	Null
Local IP@ModBus gateway	Enter the IP address of the router.	Null
Local port@ ModBus gateway	Enter the local port of ModBus.	Null

Click the "Status" column to view the current serial port type.

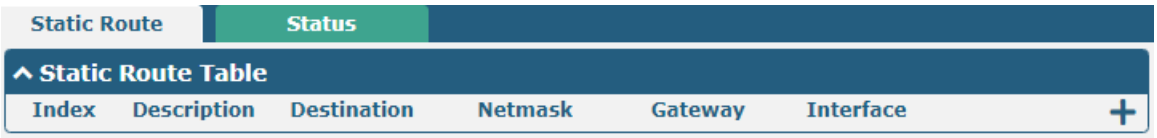


4.3 Network

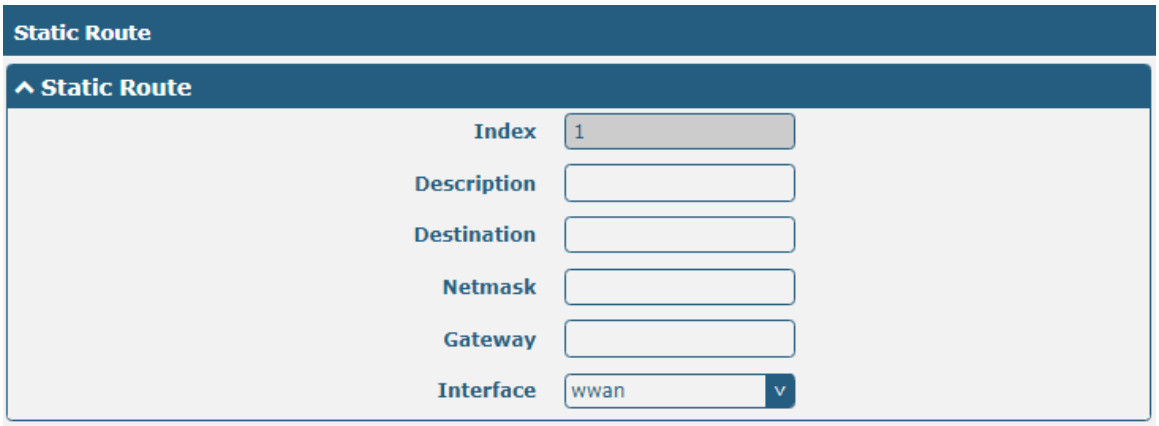
4.3.1 Route

This section allows you to set the static route. Up to 20 static routes can be added to the router. 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.
Click network > route > static route to enter the static route table, which allows users to manually add, remove, or modify static route rules.

Static Route



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



Static Route		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this 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.

Static Route | Status

Route Table

Index	Destination	Netmask	Gateway	Interface	Metric
1	0.0.0.0	0.0.0.0	10.189.43.26	wwan	0
2	10.189.43.24	255.255.255.252	0.0.0.0	wwan	0
3	192.168.0.0	255.255.255.0	0.0.0.0	lan0	0

4.3.2 Firewall

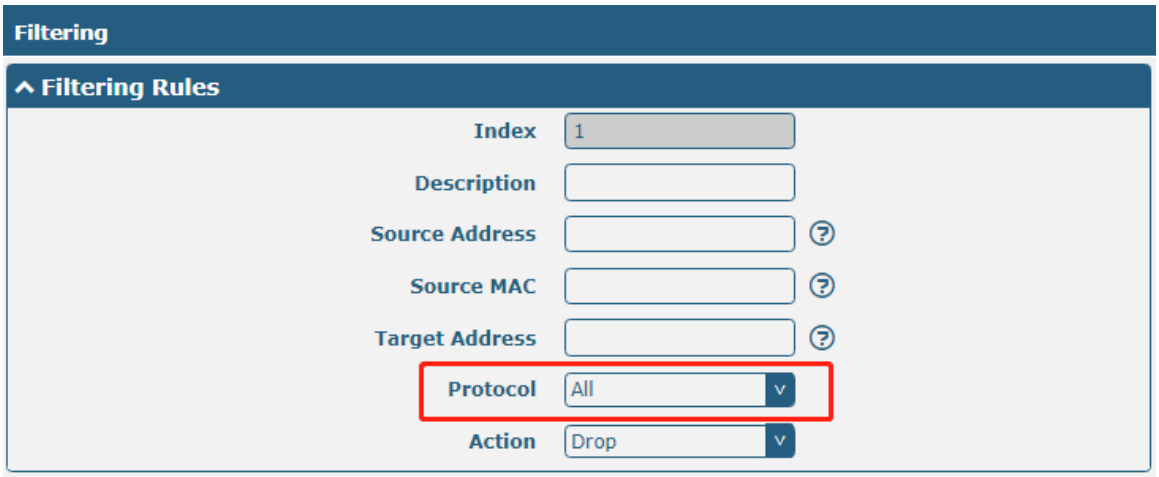
This section allows you to set the firewall and its related parameters, including Filtering, Port Mapping, Custom Rules, DMZ and Status. Filtering rules allow users to custom accept or discard a specified access source, filtering its IP address or MAC address.
Click "> firewall > filter" to display as follows:

Filtering

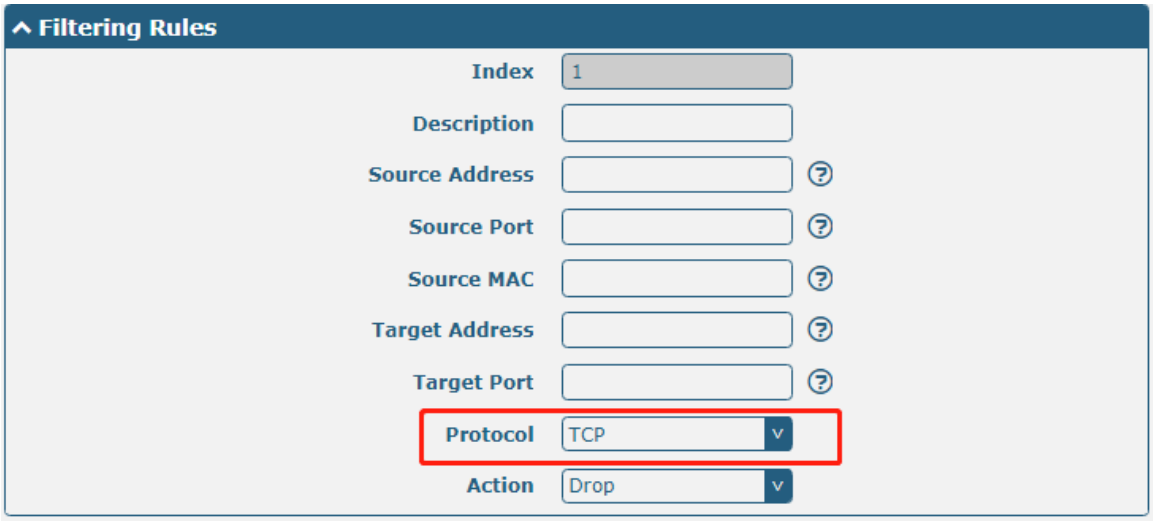
The filtering rules can be used to either accept or block certain users or ports from accessing your router.

Click + to add whitelist rules. The maximum count is 5.

Click + to add filtering rules. The maximum count is 50. 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		
Item	**Description**	**Default**
General Settings		
Enable Filtering	Click the toggle button to enable/disable the filtering option.	ON

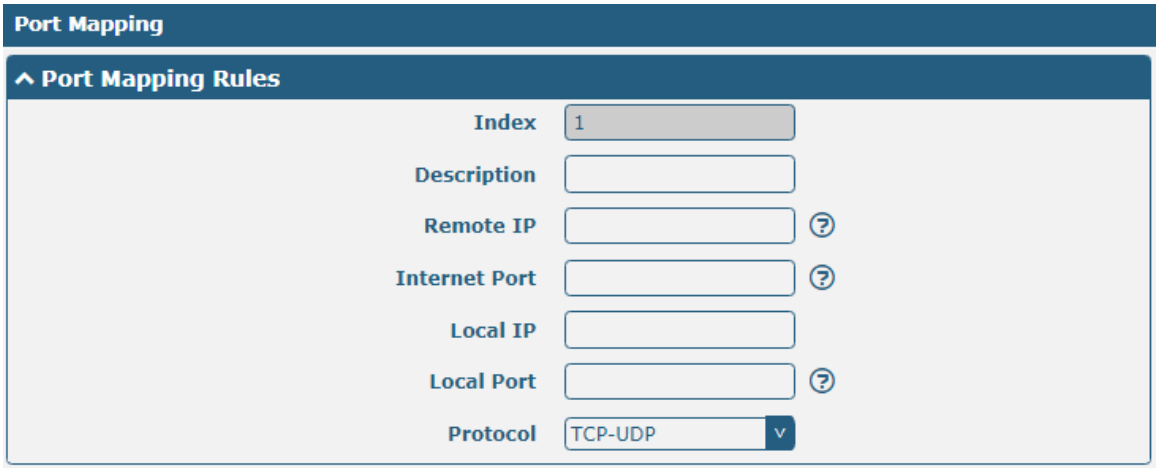
Filtering		
Item	**Description**	**Default**
Default Filtering Policy	Select from "Accept" or "Drop". Cannot be changed when filtering rules table is not empty. • Accept: Router will accept all the connecting requests except the hosts which fit the drop filter list • Drop: Router will drop all the connecting requests except the hosts which fit the accept filter list	Accept
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
Enable debug	Click the toggle button to enable/disable this option.	ON
Enable VPN NAT traversal	Click the toggle button to enable/disable this option. When enabled, enable NAT traversal for the GRE/L2TP/PPTP VPN package.	OFF
White list		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this filtering rule.	Null
Source Address	Defines if access is allowed from one or a range of IP addresses which are defined by Source IP Address, or every IP addresses.	Null
Filtering rule		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this filtering rule.	Null
Source Port	Specify an access originator and enter its source port.	Null
Source MAC	Enter the MAC address of the defined source IP address.	Null
Target Address	Defines if access is allowed to one or a range of IP addresses which are defined by Target IP Address, or every IP addresses.	Null
Target Port	Enter the target port which the access originator wants to access.	Null

Filtering		
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”. • Accept: When Default Filtering Policy is drop, router will drop all the connecting requests except the hosts which fit this accept filtering list • Drop: When Default Filtering Policy is accept, router will accept all the connecting requests except the hosts which fit this drop filtering list	Drop

Port Mapping

Port mapping is defined manually in the router, and the data received from some ports in the public network are all forwarded to a port of an IP in the internal network. Click "network > firewall > port map" to display as follows:

Click + to add port mapping rules. The maximum rule count is 50.



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 to the local IP address. Empty means unlimited. e.g. 10.10.10.10/255.255.255.255 or 192.168.1.0/24	Null

Port Mapping Rules		
Item	**Description**	**Default**
Internet Port	Set 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

Custom Rules

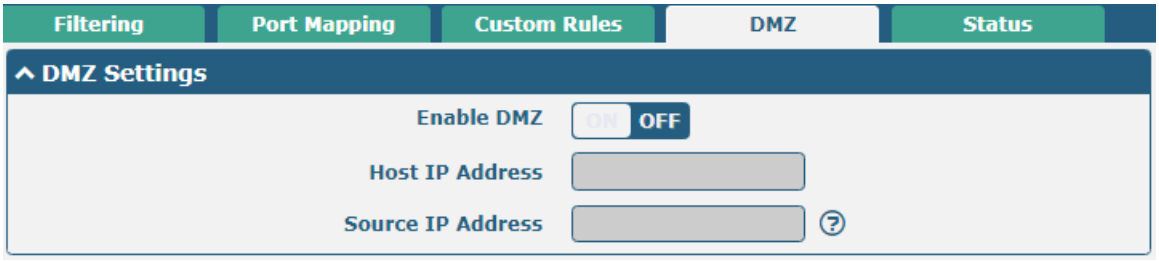
"Custom Rules" meets customer's demand for personal filtering of IP package, filter data usage of a website for example. Users can add any iptables rules which meet the iptables rule format standard in this list.

Click + to add custom rules.

Custom firewall Rules		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this custom rule.	Null
Rule	Specify one custom rule.	Null

DMZ

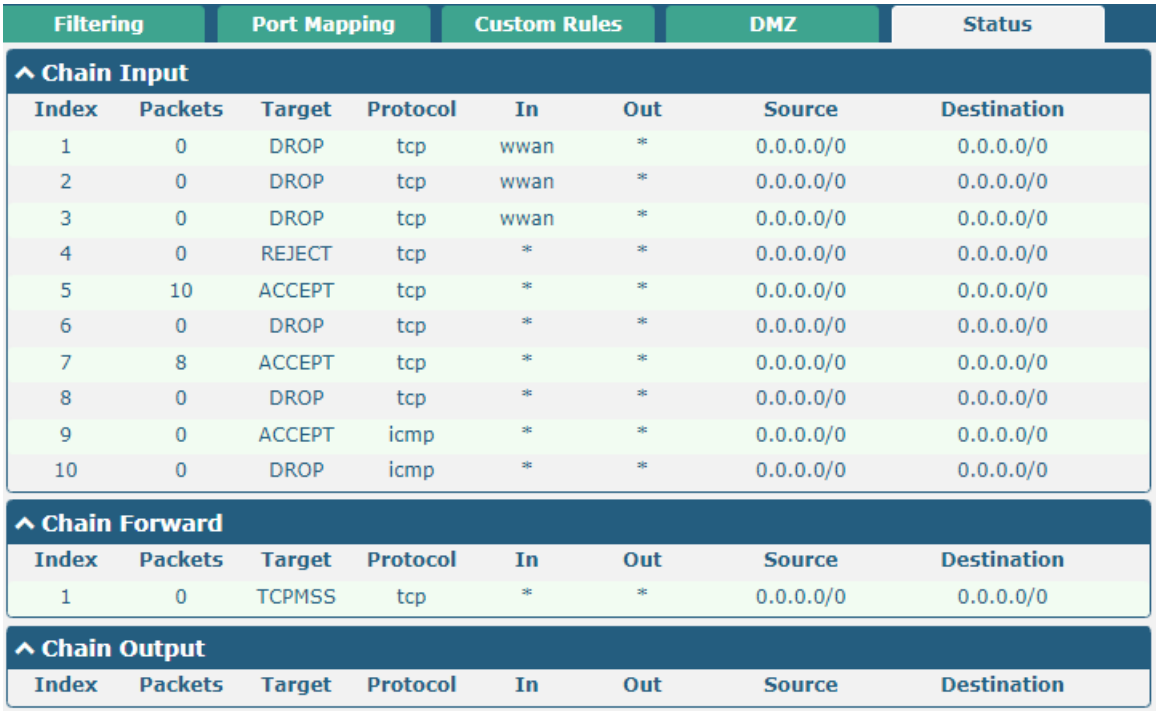
The DMZ, also known as the Demilitarized Zone, is being transformed into a large swath of land. It is to solve the problem that the access user of the external network cannot access the internal network server after installing the firewall, and set up a buffer between the non-secure system and the secure system. A DMZ host is an Intranet host that has open access to all ports except the occupied and forwarded ports to the specified address.
Click "> firewall > DMZ" to display the following:



DMZ Settings		
Item	**Description**	**Default**
Enable DMZ	Click the toggle button to enable/disable DMZ. DMZ host is a host on the internal network that has all ports exposed, except those ports otherwise forwarded.	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. 0.0.0.0 means for any addresses.	Null

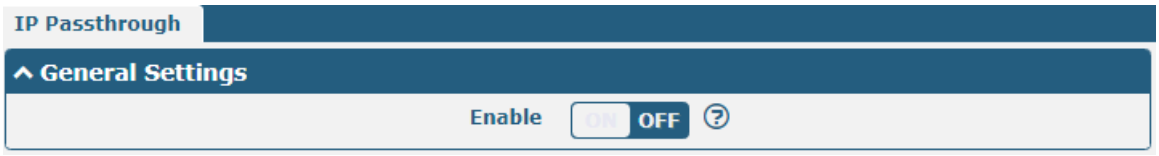
Status

This window allows you to view the status of chain input, chain forward and chain output.



4.3.3 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.

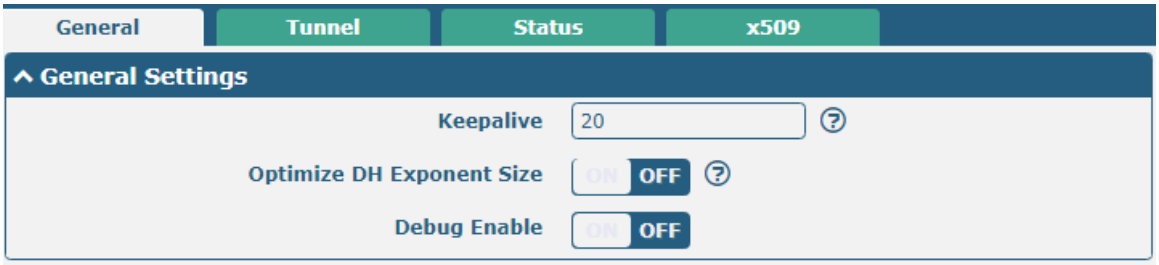
4.4 VPN

4.4.1 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.

Click **VPN > IPsec > general** to set IPsec parameters.

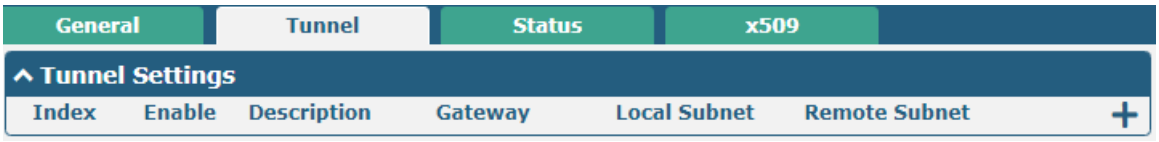
General



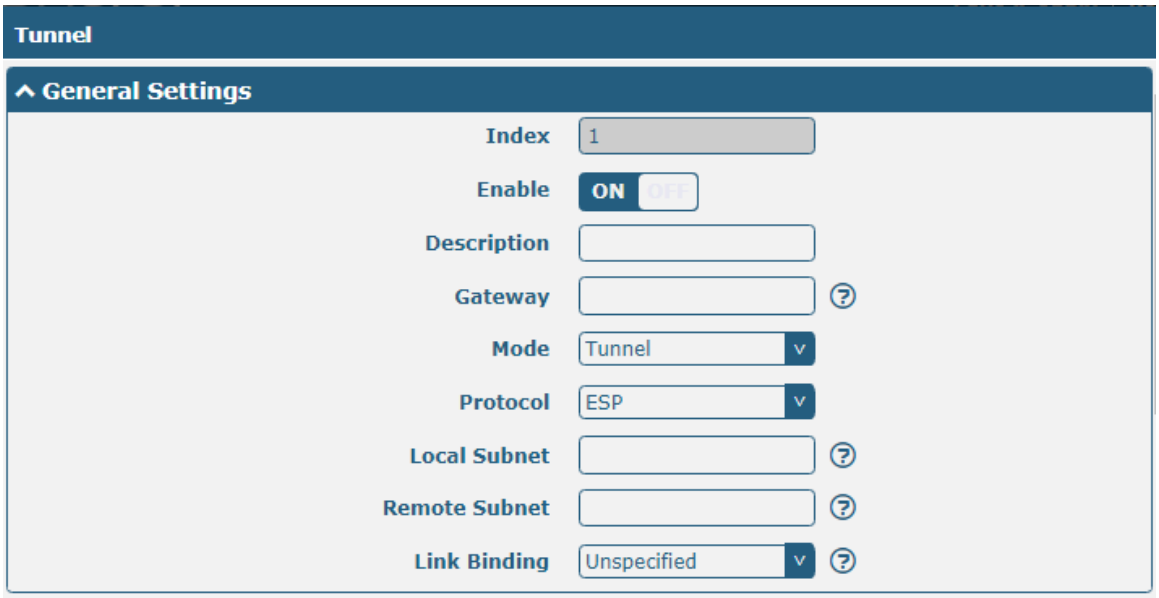
General Settings @ General		
Item	**Description**	**Default**
Keepalive	Set the time to live in seconds. The router sends keep-alive packets to the NAT (Network Address Translation) server at regular intervals to prevent the records on the NAT table from disappearing.	20
Optimize DH Exponent size	Click the toggle button to enable/disable this option. When enabled, when using dhgroup17 or dhgroup18, it helps to shorten the time to generate the dh key.	OFF
Debug Enable	Click the toggle button to enable/disable this option. Enable for IPsec VPN	OFF

	information output to the debug port.	

Tunnel



Click + to add tunnel settings. The maximum count is 6.



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 side IPsec VPN server. 0.0.0.0 means for any address.	Null
Mode	Select from “Tunnel” and “Transport”. • Tunnel: Commonly used between routers, or at an end-station to a router, the router acting as a proxy for the hosts behind it • Transport: Used between end-stations or between an end-station and a router, if the router 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 destination	Tunnel
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.	Null

	192.168.1.0/24	
Remote Subnet	Enter the remote subnet's address with mask protected by IPsec, e.g. 10.8.0.0/24	Null
Link Binding	Select from"WWAN1", "WAN", or "WLAN".	Not bound

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 "PKCS#12" as the authentication type.

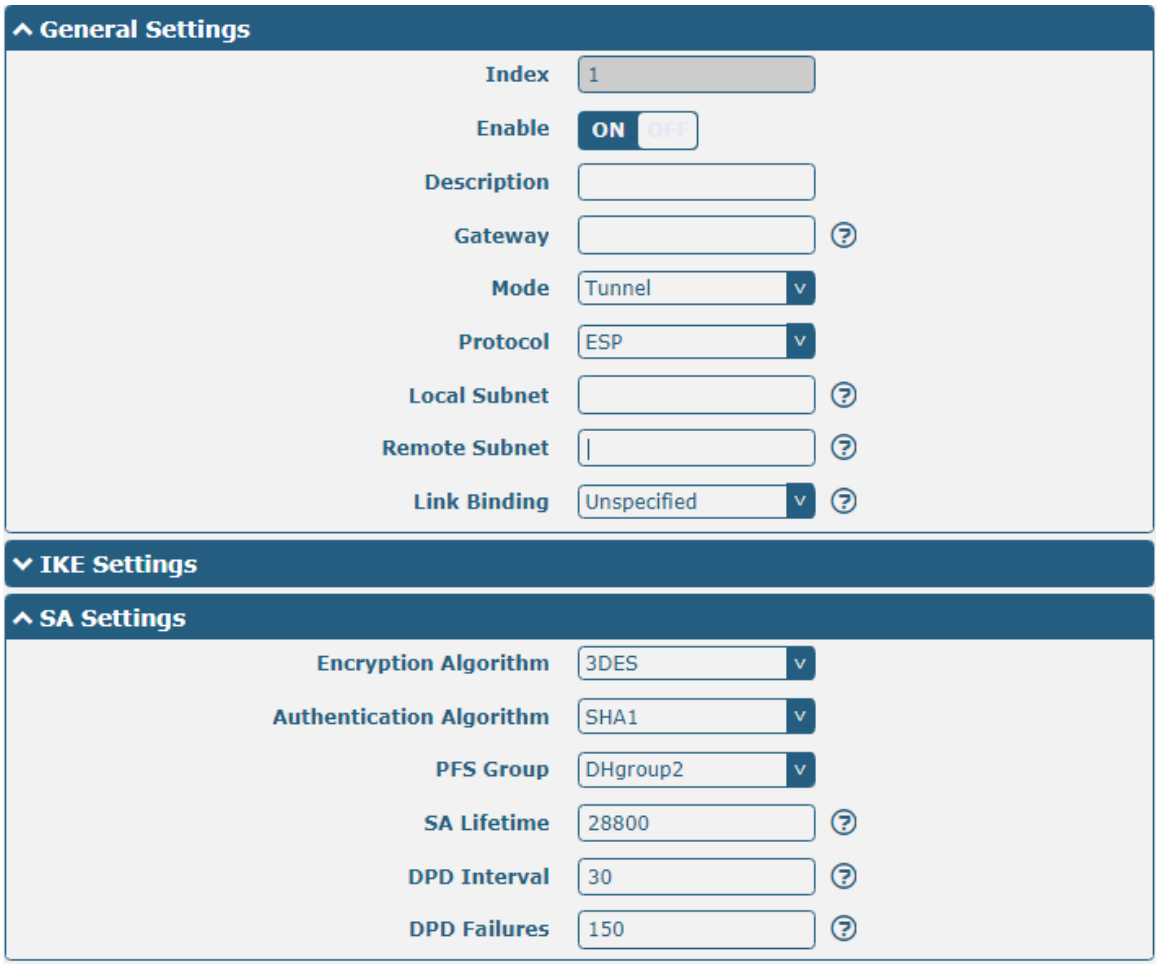
The window is displayed as below when choosing “xAuth PSK” as the authentication type.

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

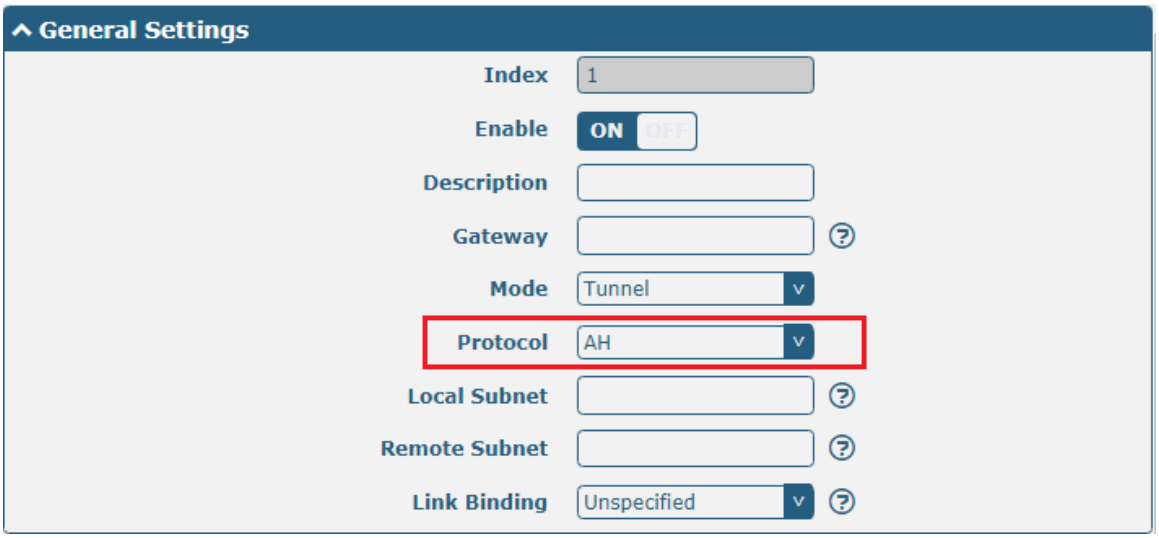
IKE Settings		
Item	**Description**	**Default**
IKE Type	Select from “IKEv1” and “IKEv2”.	IKEv1
Negotiation Mode	Select from “Main” and “Aggressive” for the IKE negotiation mode in phase 1. If the IP address of one end of an IPsec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main Mode
Encryption Algorithm	Select from “3DES”, “AES128”, “AES192”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 • AES192: Use 192-bit AES encryption algorithm in CBC mode • AES256: Use 256-bit AES encryption algorithm in CBC mode	3DES
Authentication Algorithm	Select from “MD5”, “SHA1”, “SHA2 256” or “SHA2 512” to be used in IKE negotiation.	SHA1
IKE DH Group	Select from “DHgroup1”,“DHgroup2”, “DHgroup5”, “DHgroup14”, “DHgroup15”, “DHgroup16”, “DHgroup17” or “DHgroup18” to be used in key negotiation phase 1.	DHgroup2
Authentication Type	Select from “PSK”, “CA”, “PKCS#12”, “xAuth PSK” and “xAuth CA” to be used in IKE negotiation. • PSK: Pre-shared Key • CA: x509 Certification Authority • xAuth: Extended Authentication to AAA server • PKCS#12: Exchange digital certificate authentication	PSK
PSK Secret	Enter the pre-shared key.	Null
Local ID Type	Select from “Default”, “FQDN” and “User FQDN” for IKE negotiation. • Default: Uses an IP address as the ID in IKE negotiation • FQDN: Uses 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	Default

IKE Settings		
Item	**Description**	**Default**
	router, e.g., test.robustel.com • User FQDN: Uses 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 router, e.g., test@robustel.com	
Remote ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. • Default: Uses an IP address as the ID in IKE negotiation • FQDN: Uses 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 router, e.g., test.robustel.com • User FQDN: Uses 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 router, 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.

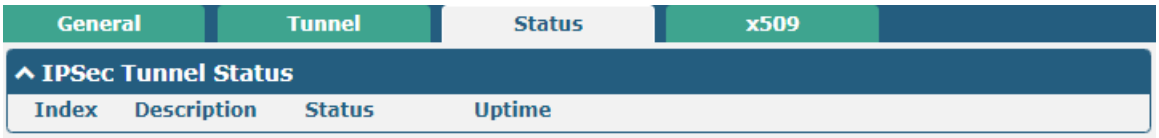


SA Settings		
Item	**Description**	**Default**
Encrypt Algorithm	Select from “3DES”, “AES128”, “AES192”or “AES256” when you select “ESP” in “Protocol”. Higher security means more complex implementation and lower speed. DES is enough to meet general requirements. Use 3DES when high confidentiality and security are required.	3DES
Authentication Algorithm	Select from “MD5”, “SHA1”, “SHA2 256” or “SHA2 512” to be used in SA negotiation.	SHA1
PFS Group	Select from “PFS (N/A)”, “DHgroup1”, “DHgroup2”, “DHgroup5”, “DHgroup14”, “DHgroup15”, “DHgroup16”, “DHgroup17” or “DHgroup18” to be used in SA negotiation.	DHgroup2
SA Lifetime	Set the IPsec SA lifetime. When negotiating to 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 a 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.	30
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
Enable Forced Encapsulation	Click the switch button to enable/disable this option. When enabled, UDP encapsulation of esp packets is enforced even if NAT conditions are not	OFF

SA Settings		
Item	**Description**	**Default**
	detected. This may help overcome restrictive firewalls.	
Expert Options	Add more PPP configuration options here, format: config-desc;config-desc, e.g. protostack=netkey;plutodebug=none	null

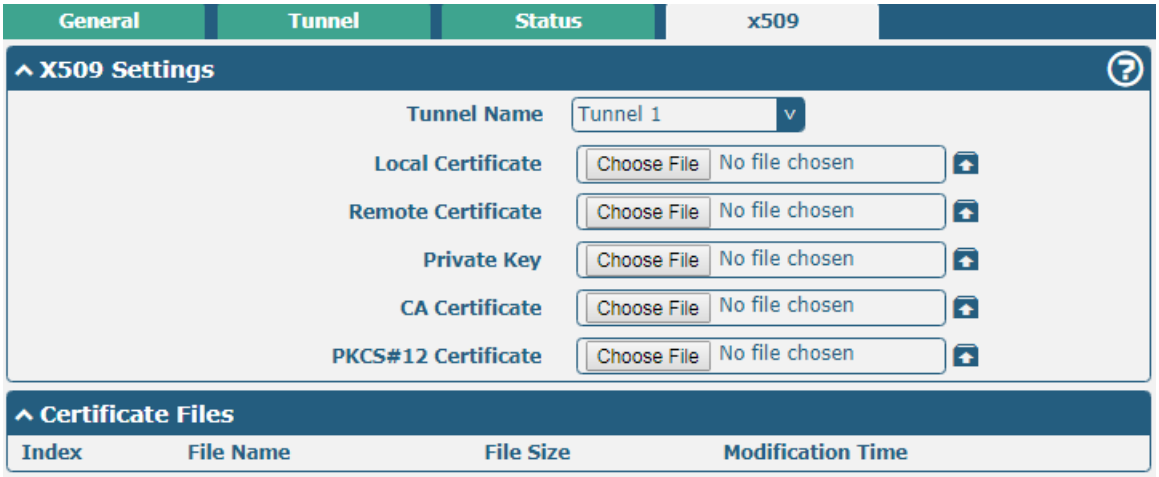
Status

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



x509

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



x509		
Item	**Description**	**Default**
X509 Settings		
Tunnel Name	Choose a valid tunnel. Choose from tunnel 1, tunnel 2, tunnel 3, tunnel 4, tunnel 5, and tunnel 6.	Tunnel 1
Local Certificate	Click on “Choose File” to locate the certificate file from local computer, and then import this file into your router.	--
Remote Certificate	Click on “Choose File” to locate the certificate file from remote computer, and then import this file into your router.	--
Private Key	Click on “Choose File” to locate the private key file.	--
CA certificate	Select the root certificate file to import into the router.	--
PKCS # 12	Select the PKCS#12 certificate file to import into the router.	--

x509		
Item	**Description**	**Default**
X509 Settings		
certificate		
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
Modification Time	Show the timestamp of that the last time to modify the certificate file.	Null

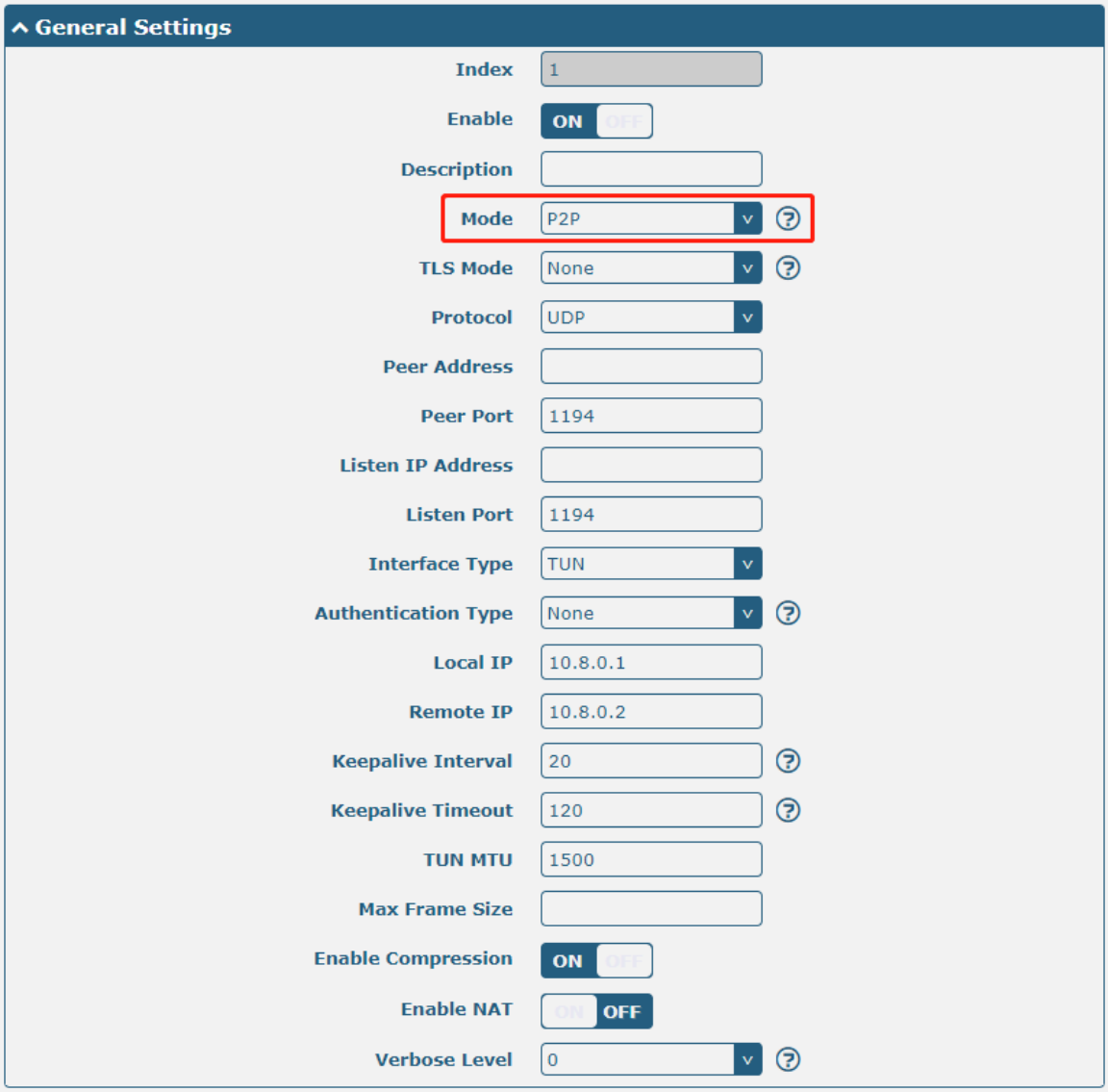
4.4.2 OpenVPN

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.

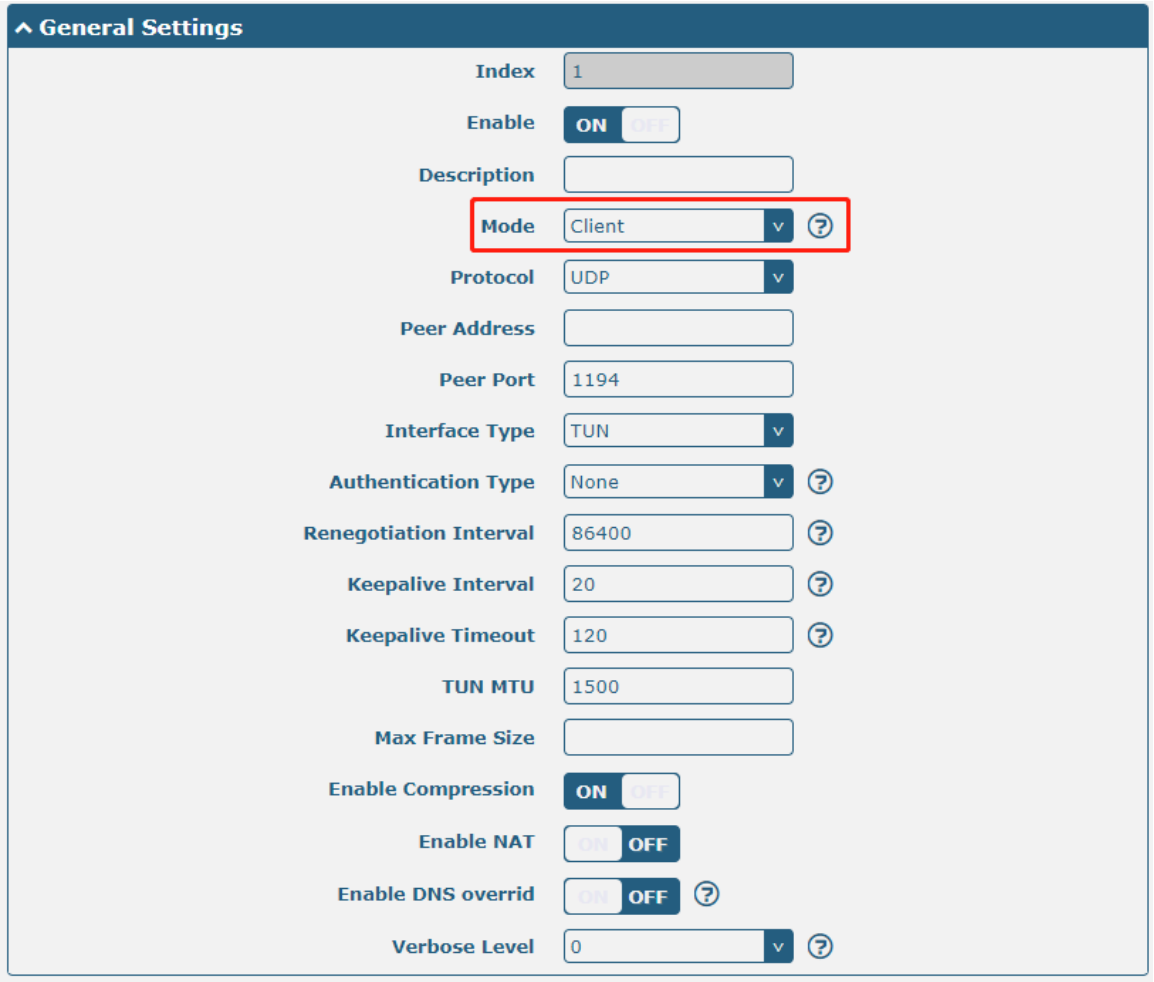
Click "**VPN > OpenVPN > OpenVPN**" to display as follows:

OpenVPN

Click + to add tunnel settings. The maximum count is 6. By default, the mode is "P2P". The window is displayed as below when choosing "P2P" as the mode.

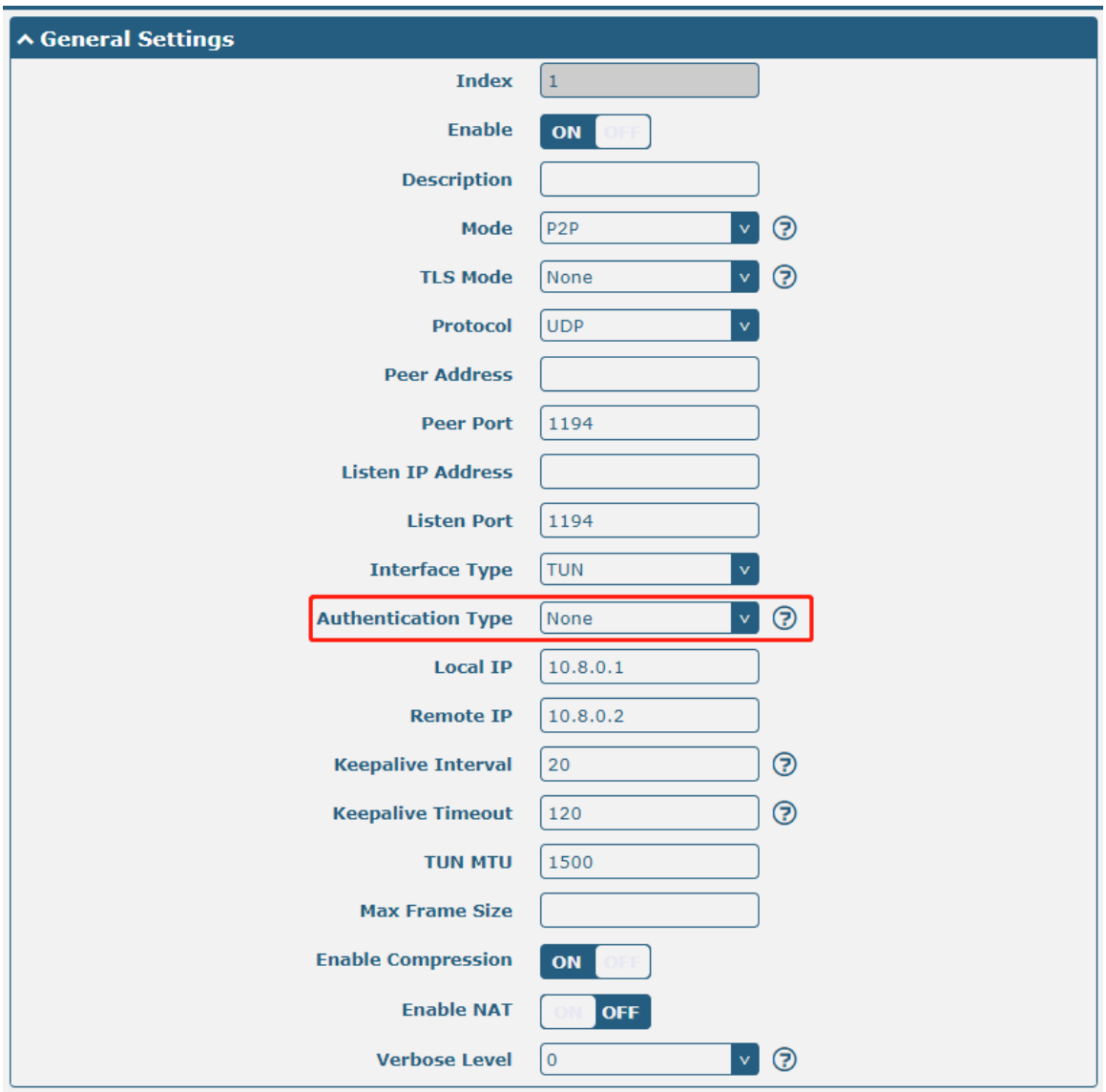

General Settings
Index
1
Enable
ON
OFF
Description
Mode
P2P
TLS Mode
None
Protocol
UDP
Peer Address
Peer Port
1194
Listen IP Address
Listen Port
1194
Interface Type
TUN
Authentication Type
None
Local IP
10.8.0.1
Remote IP
10.8.0.2
Keepalive Interval
20
Keepalive Timeout
120
TUN MTU
1500
Max Frame Size
Enable Compression
ON
OFF
Enable NAT
ON
OFF
Verbose Level
0

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



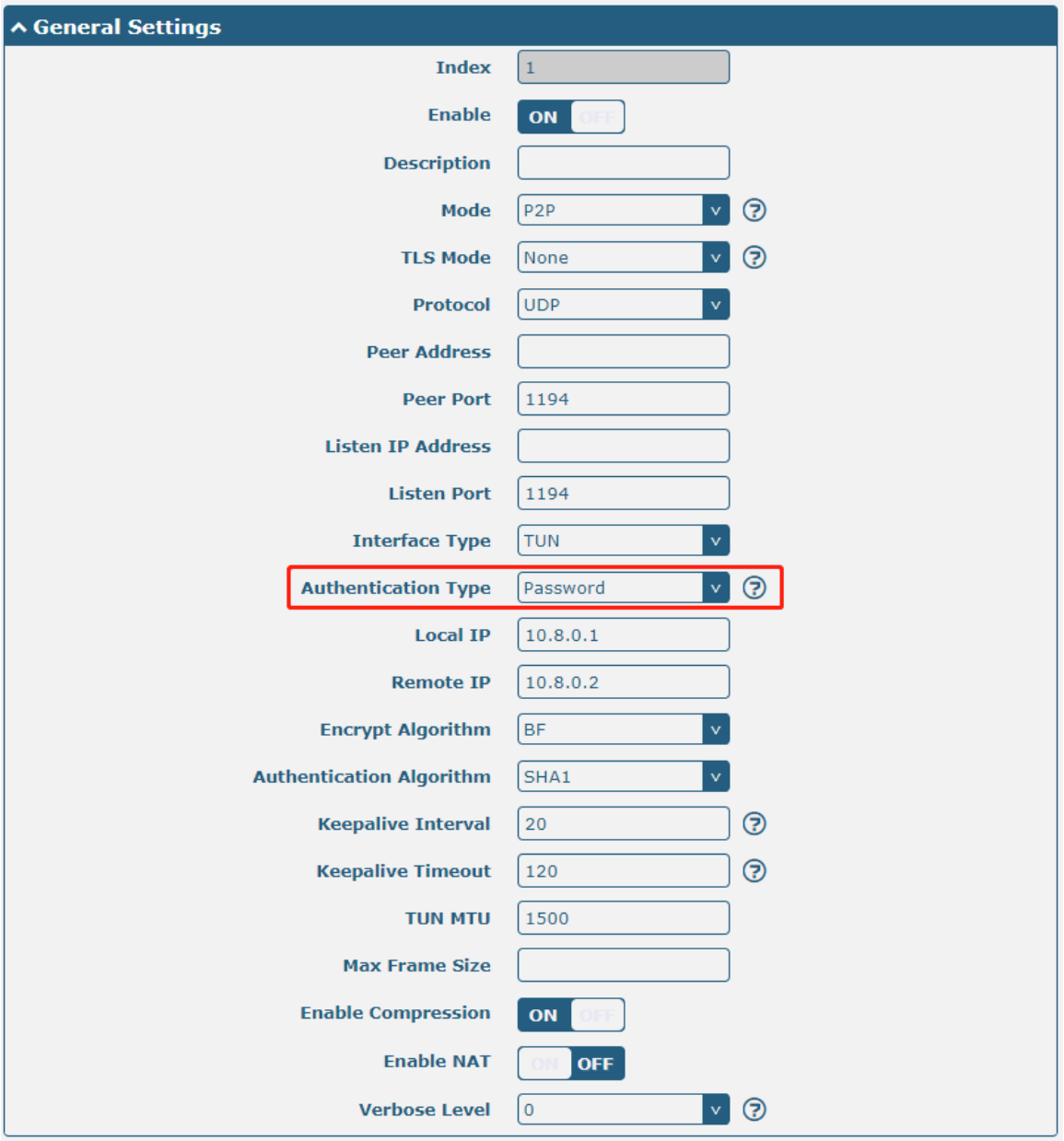
The window is displayed as below when choosing “Server” as the mode.

The window is displayed as below when choosing “None” as the authentication type.

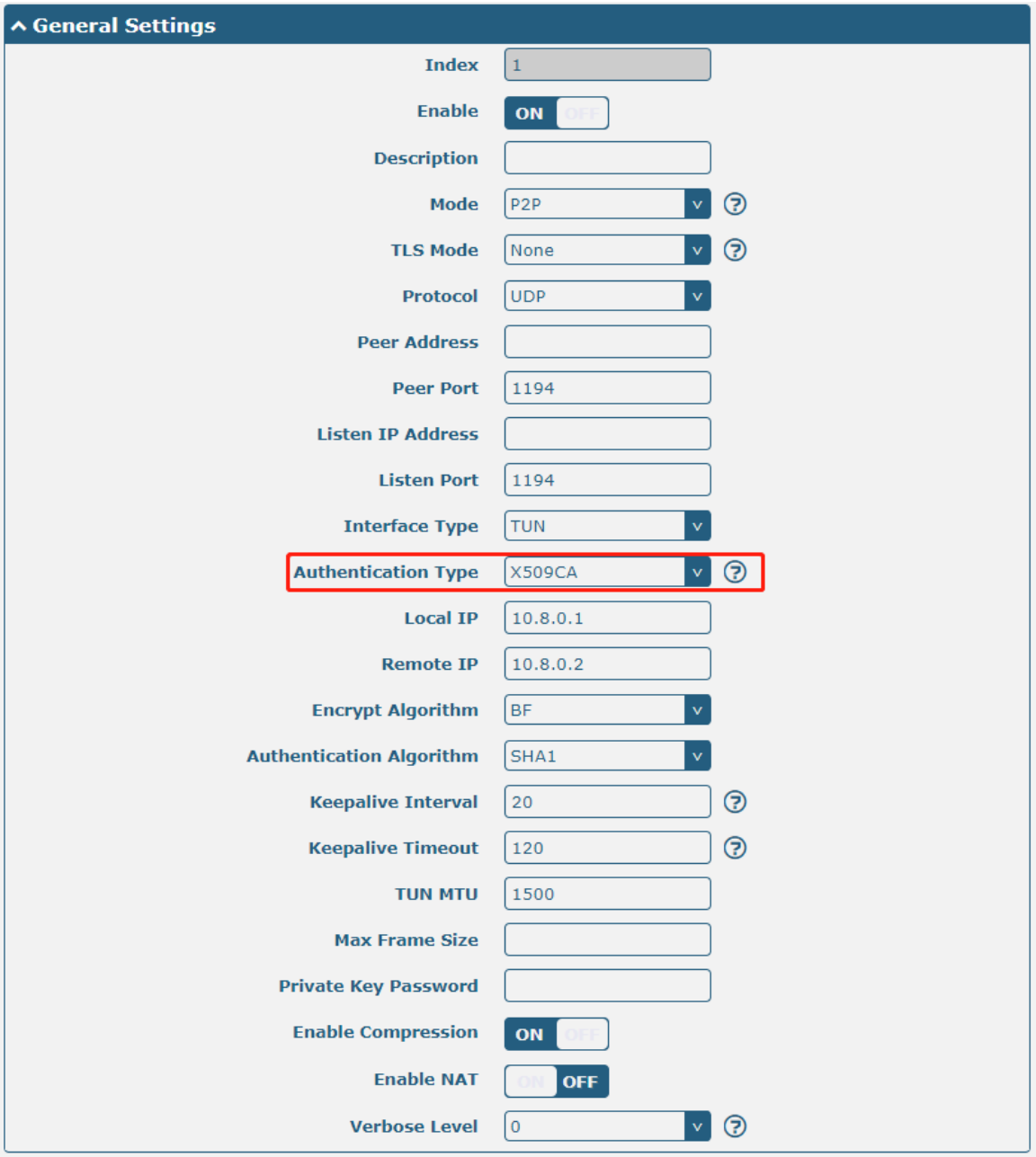


The window is displayed as below when choosing “Preshared” as the authentication type.

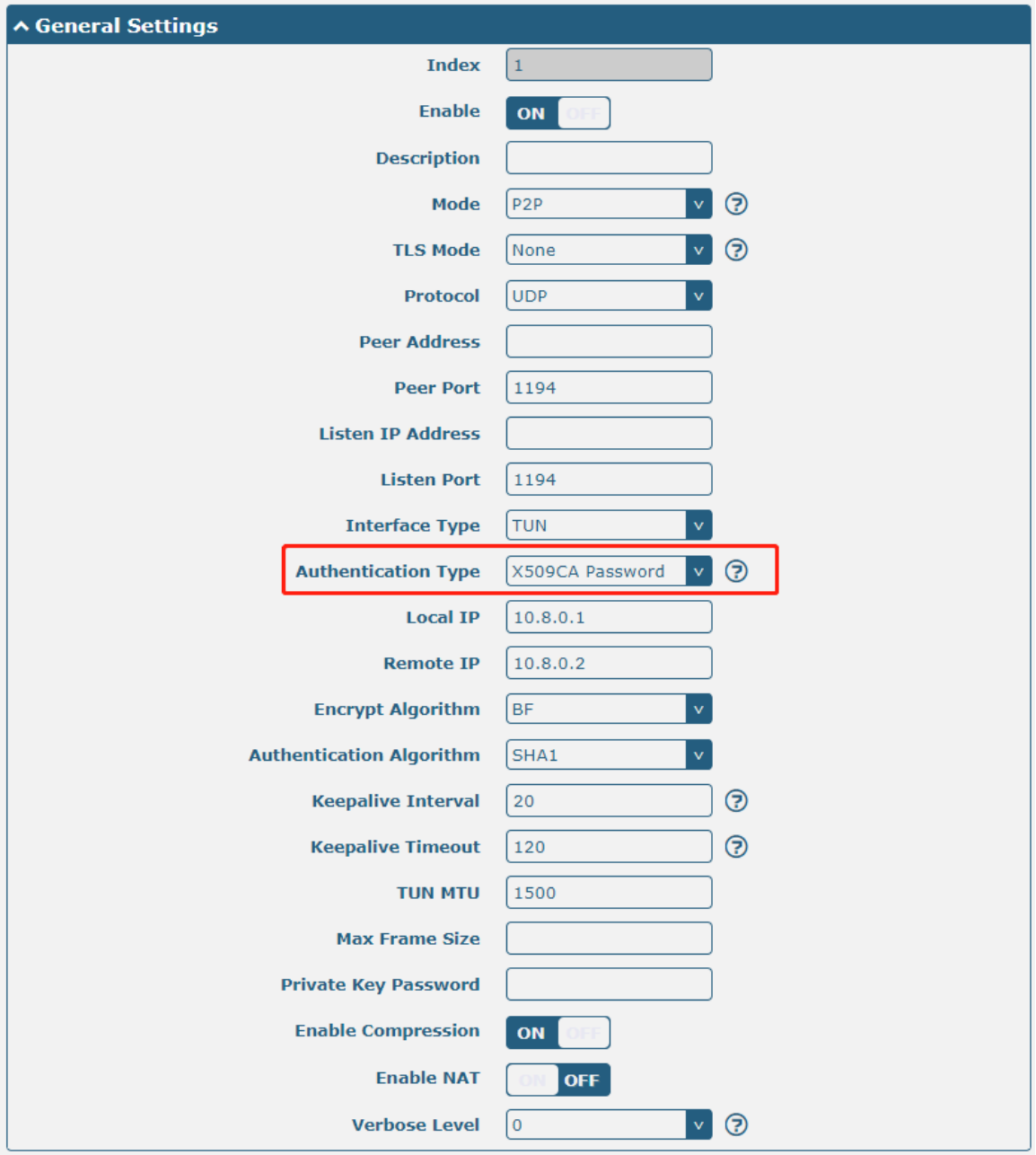
The window is displayed as below when choosing “Password” as the authentication type.



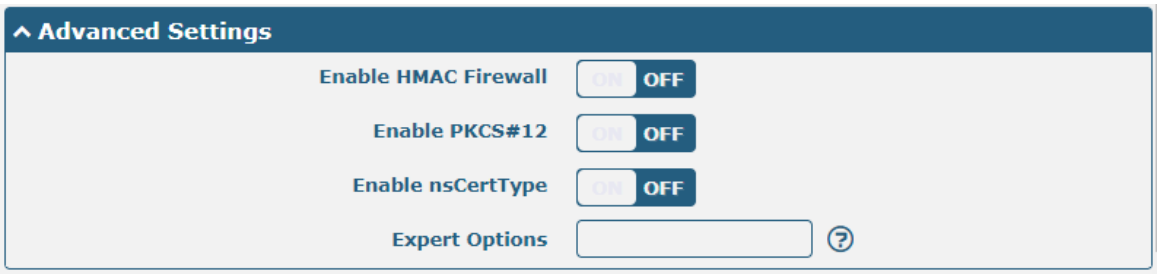
The window is displayed as below when choosing “X509CA” as the authentication type.



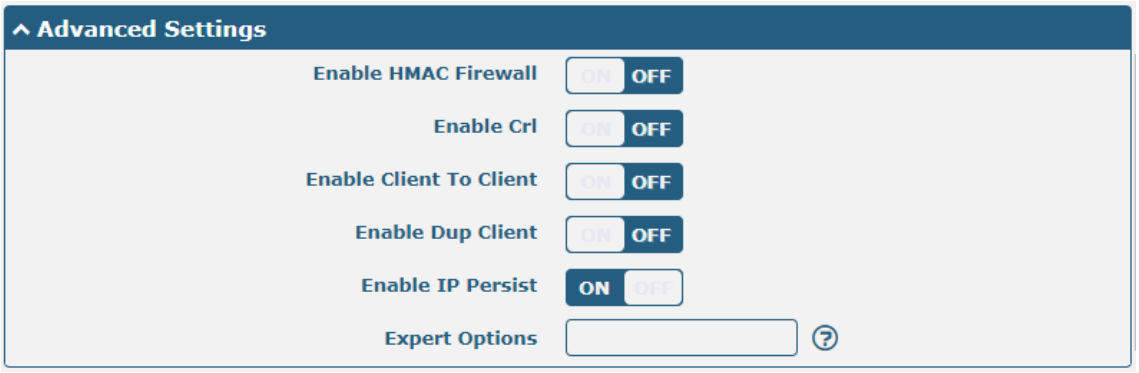
The window is displayed as below when choosing “X509CA Password” as the authentication type.



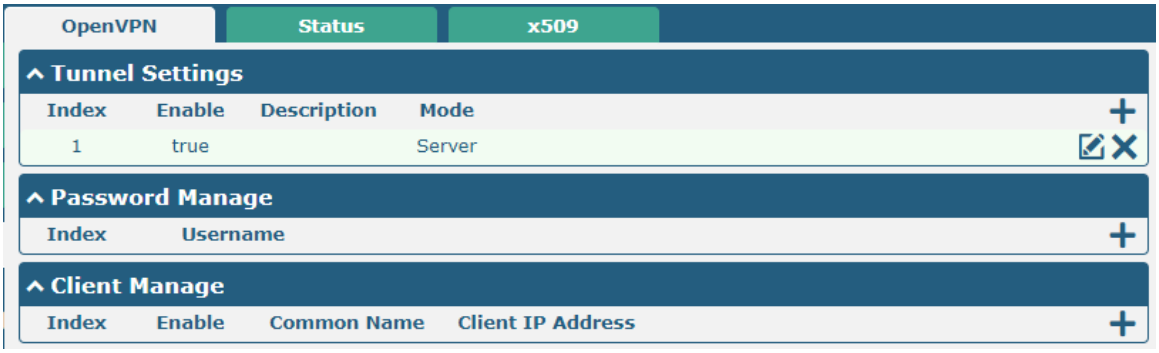
When "mode" selects "Client", the window displays as follows:



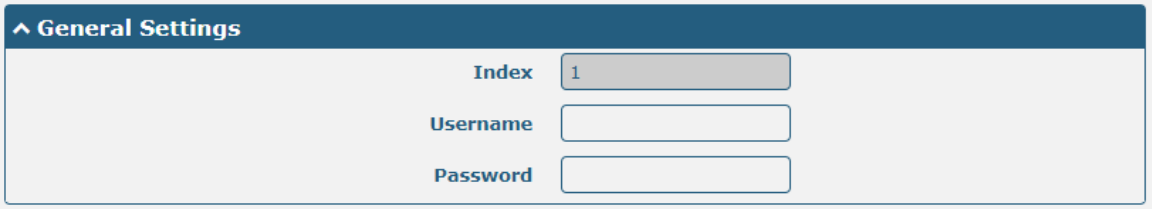
When "mode" is selected "Server", the window displays as follows:



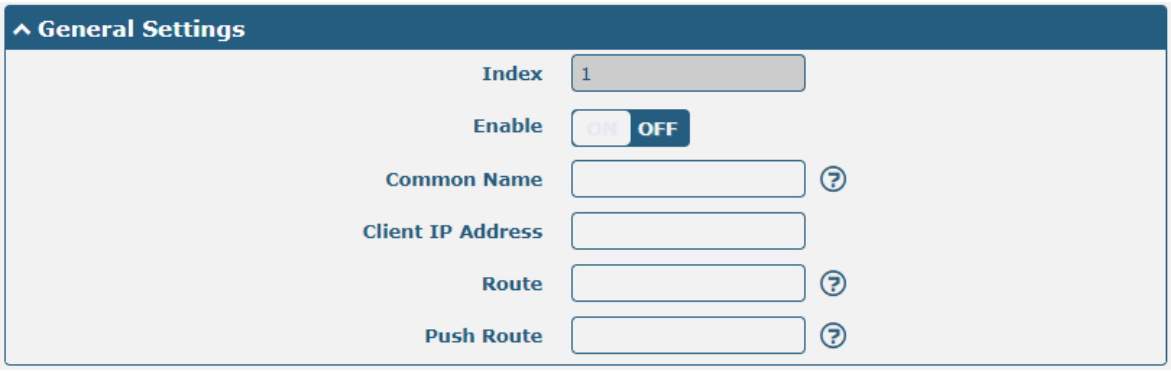
When "mode" selects "Server" and "authentication mode" selects "X509 certificate and password", the window of **"VPN > OpenVPN > OpenVPN"**



Click user password management + to add a user name and password, as shown below.



Click client administration + to client information, as shown below.



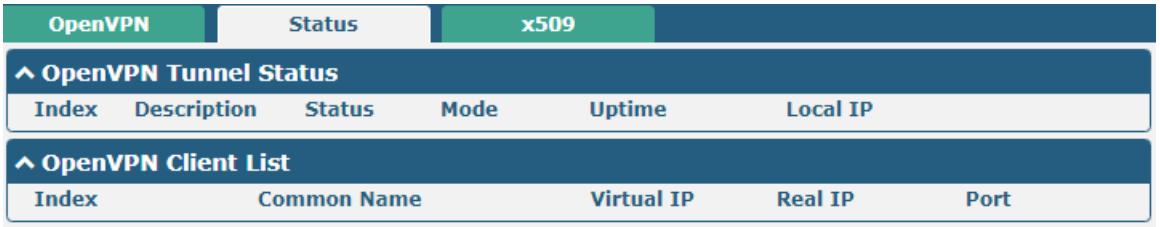
General Settings @ OpenVPN		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this OpenVPN tunnel.	ON
Description	Enter a description for this OpenVPN tunnel.	Null
Mode	Select from “P2P” or “Client”.	P2P
TLS Mode	Select from “None”, “Client” or “server”.	None
Protocol	Select from “UDP”, “TCP-Client” or “TCP-Server”.	UDP
Peer Address	Enter the end-to-end IP address or the domain of the remote OpenVPN server.	Null
Peer Port	Enter the end-to-end listener port or the listener port of the OpenVPN server.	1194
Listen Address	Enter the Listen address	Null
Listen Port	Enter the Listen port	1194
Interface Type	Select from “TUN”, “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
Authentication Type	Select from “None”, “Preshared”, “Password”, “X509CA” and “X509CA Password”. **Note**: “None” and “Preshared” authentication type are only working with P2P mode.	None
Enable IP address pool	Click the toggle button to enable/disable the IP address pool allocation function.	OFF
Initial address	Define the IP address pool start to assign addresses to OpenVPN clients.	10.8.0.5
End address	Defines the end of the IP address pool that assigns addresses to OpenVPN clients.	10.8.0.254
Client network	Enter the IP of Client network.	10.8.0.0
Client network mask	Enter the Client network mask.	255.255.255.0
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
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
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

General Settings @ OpenVPN		
Item	**Description**	**Default**
Max number of clients	Set the maximum number of clients allowed to access the OpenVPN server.	10
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
MTU	Set the maximum transmission unit.	1500
Data fragmentation	Set the maximum frame length.	Null
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 default gateway	Click the toggle button to enable/disable the default gateway function. After being enabled, the local tunnel address is pushed as the default gateway of the peer device.	OFF
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
Receive DNS push	Click the toggle button to enable/disable receiving DNS push. After being enabled, it is allowed to receive DNS information pushed by the peer.	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		
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
Enable Crl	Click the toggle button to enable/disable the Crl. Once enabled, the client certificate can be revoked.	OFF
Enable client to client	Click the toggle button to enable/disable this option. When enabled, clients can communicate with each other.	OFF

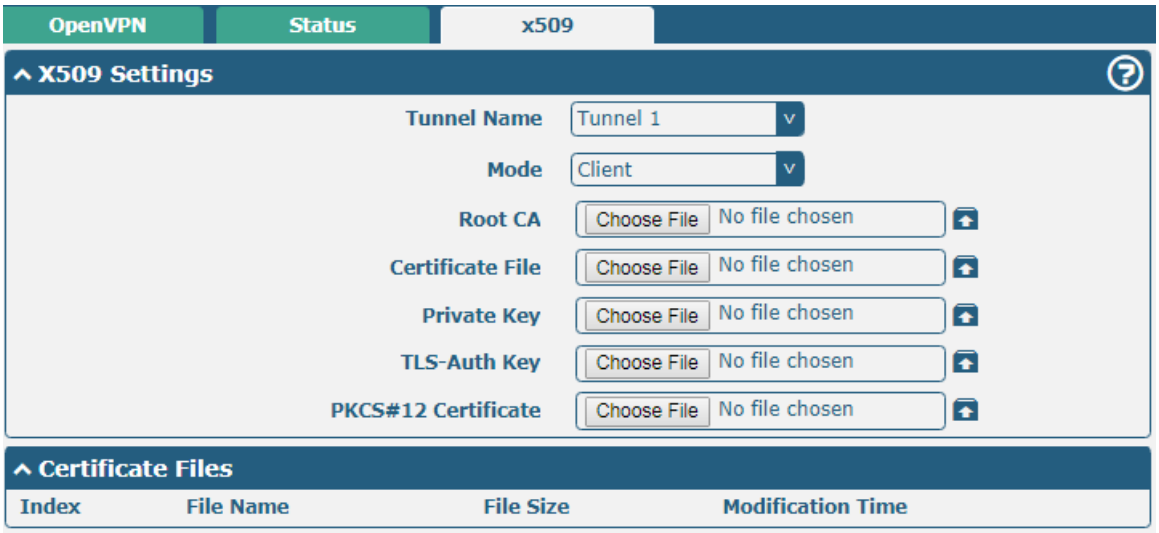
General Settings @ OpenVPN		
Item	**Description**	**Default**
Enable Dup Client	Click the toggle button to enable/disable the Dup Client. After being enabled, the tunnel IPs obtained by multiple clients are different, and the tunnel IP of the client is interconnected with the tunnel IP of the server.	OFF
Enable IP address retention	Click the toggle button to enable/disable this option. When enabled, the IP in the address pool is automatically obtained.	ON
Expert Options	Enter some other options of OpenVPN in this field. Each expression can be separated by a ';'.	Null
Advanced Settings @User password management		
Username	Enter the username for Custom tunnel connection username.	Null
Password	Enter the password for Custom tunnel connection password.	Null
General Settings @ Client management		
Enable	Click the toggle button to enable/disable this option. After being enabled, the Client IP address can be managed.	OFF
Common Name	Click the toggle button to set the certificate name.	Null
Client IP address	Click the toggle button to set a fixed allocation client virtual IP.	Null
Router	Set the Client terminal network.	Null
Push the router	Set the Sever terminal network.	Null

Status

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



This section is used to import certificates such as CA.



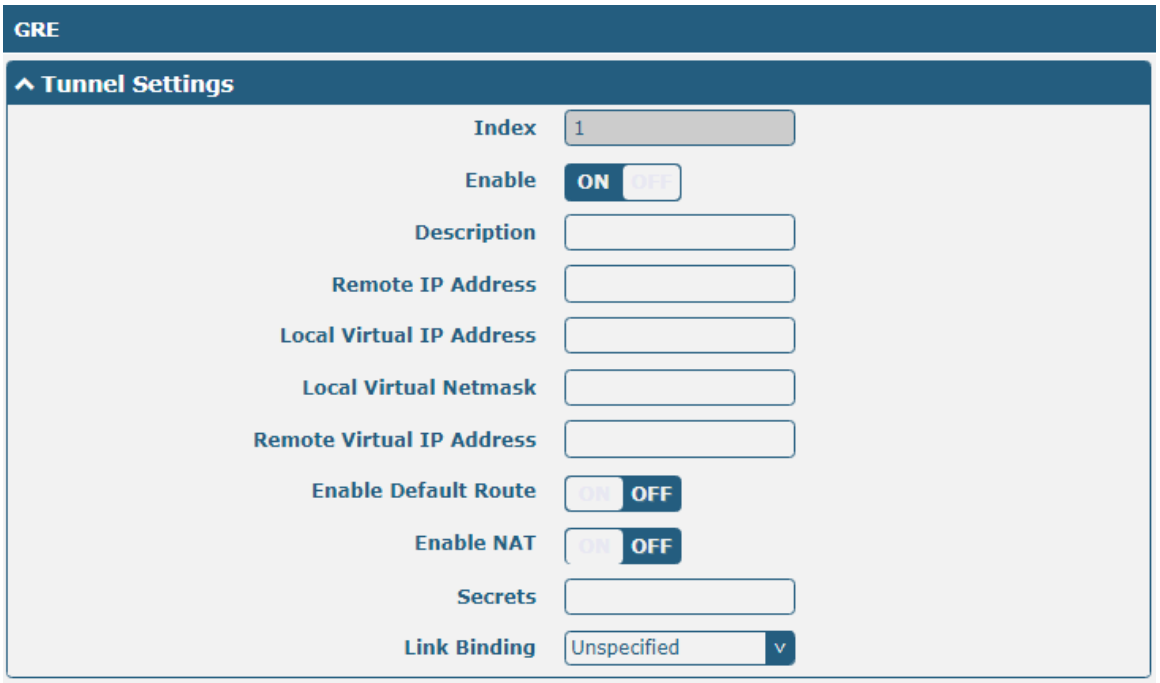
x509		
Item	**Description**	**Default**
X509 Settings		
Tunnel Name	Choose a valid tunnel. Select from Tunnel 1, Tunnel 2, Tunnel 3, Tunnel 4, Tunnel 5 and Tunnel 6.	Tunnel 1
Tunnel Mode	Select from"P2P mode", "client mode" or "server mode"	Client mode
Root CA	Click on “Choose File” to locate the root ca file, and then import this file into your router.	--
Certificate File	Click on “Choose File” to locate the certificate file, and then import this file into your router.	--
Private Key	Click on “Choose File” to locate the private key file, and then import this file into your router.	--
TLS-Auth Key	Click on “Choose File” to locate the tls-auth key file, and then import this file into your router.	--
PKCS#12 Certificate	Click on “Choose File” to locate the pkcs#12 certificate file ,and then import this file into your router.	--
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

4.4.3 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 6.

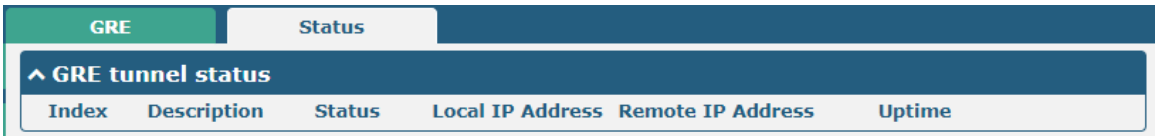


Tunnel Settings @ GRE		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this GRE tunnel.	ON
Description	Enter a description for this GRE tunnel.	Null
Remote IP Address	Set the remote real IP address of the GRE tunnel.	Null
Local 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
Link binding	Select from "WWAN1", "WAN", or "WLAN".	Unspecified

Status

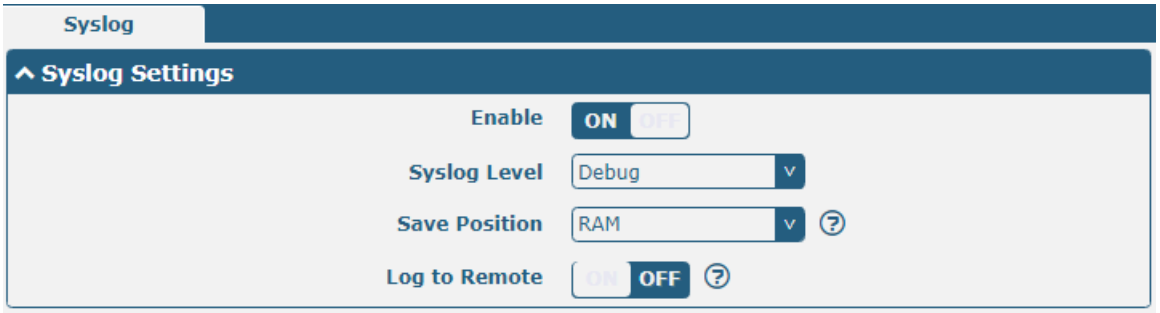
This section allows you to view the GRE tunnel status.



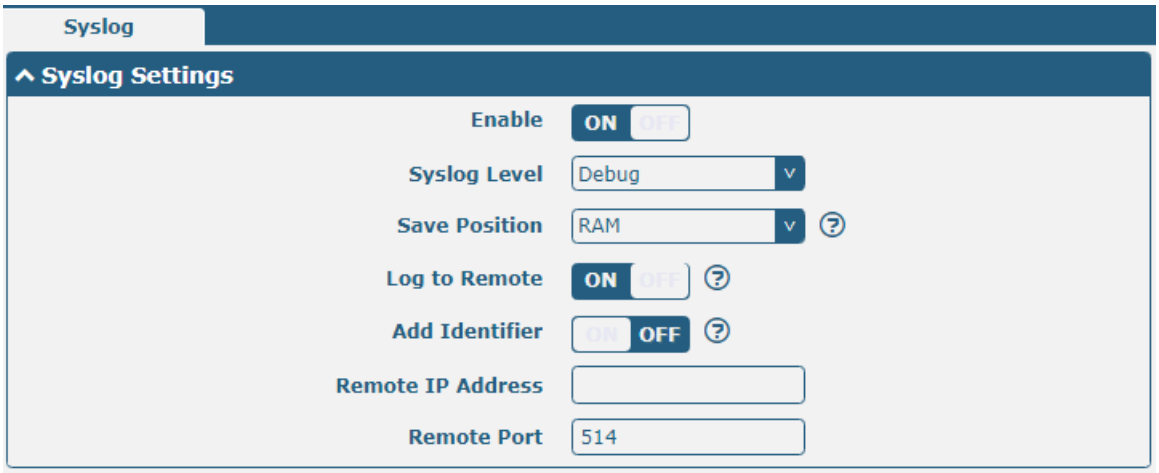
4.5 Services

4.5.1 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.



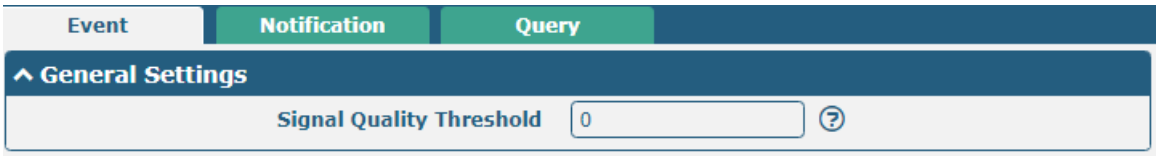
The window is displayed as below when enabling the “Log to Remote” option.



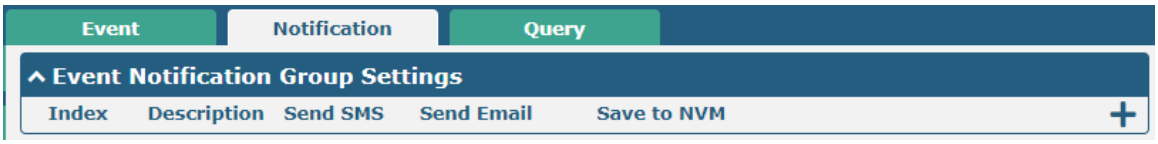
Syslog Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Syslog settings option.	ON
Syslog Level	Select from “Debug”, “Info”, “Notice”, “Warning” or “Error”, which from low to high. The lower level will output more syslog in detail.	Debug
Save Position	Select the save position from “RAM” or “NVM. Choose “RAM”, the data will be cleared after reboot. **Note**: It's not recommended that saving 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

4.5.2 Event

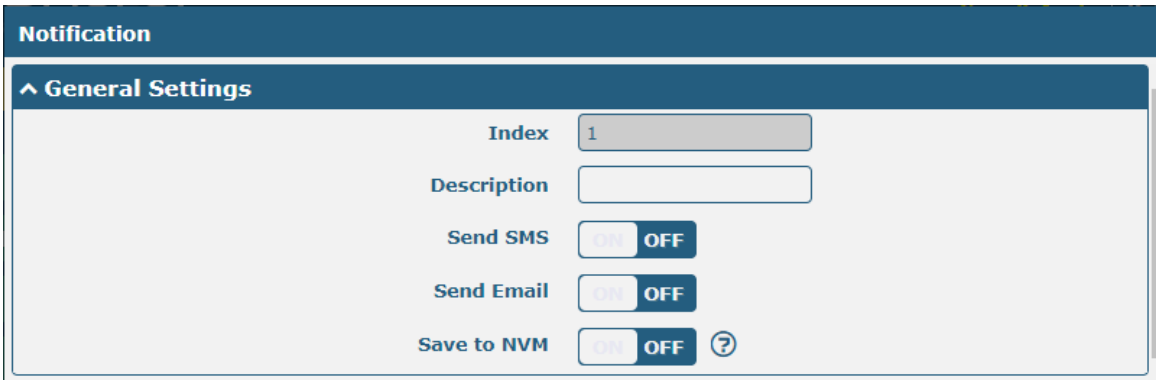
This section allows you to set the event parameters. Event feature provides an ability to send alerts by SNMP and RobustLink when certain system events occur.

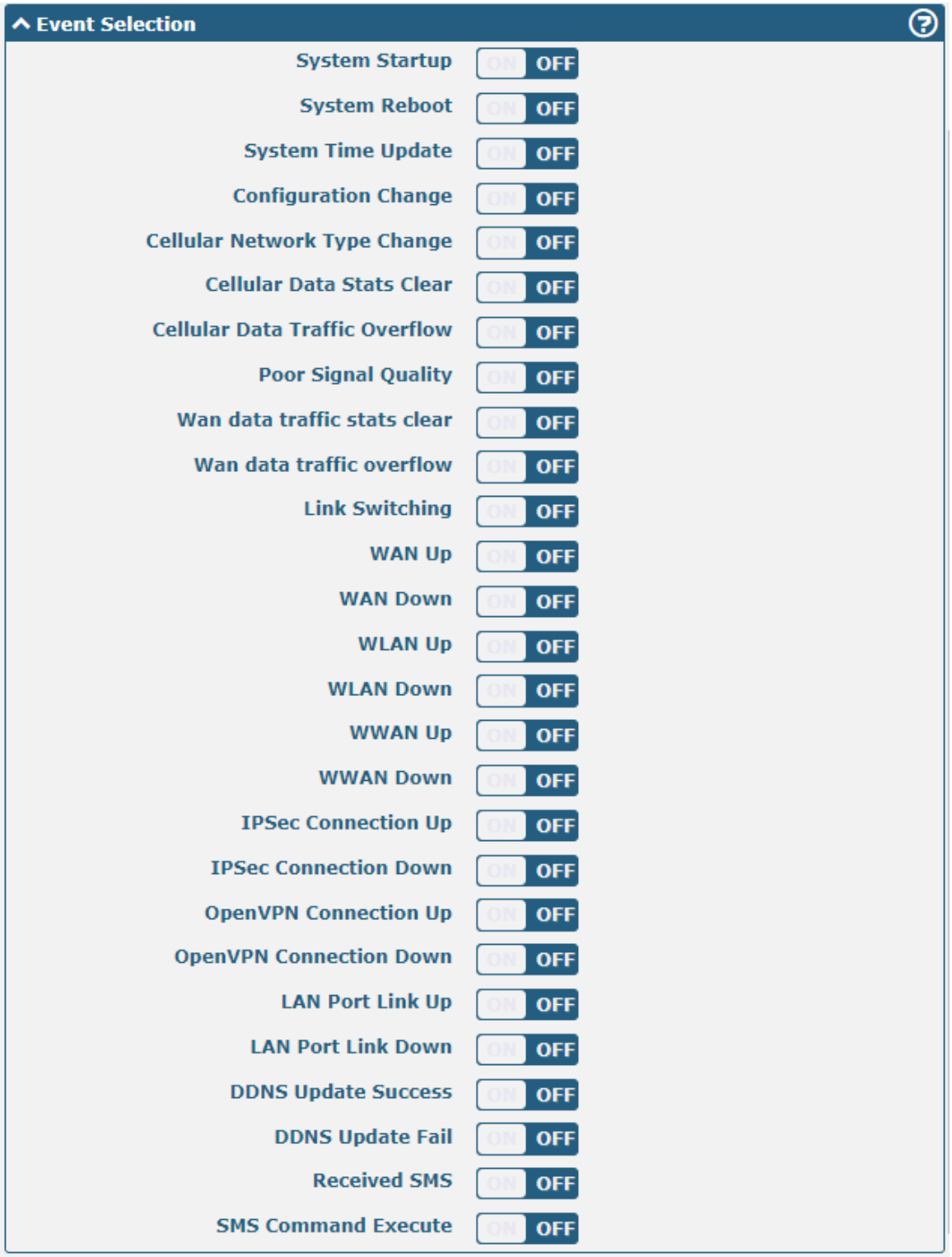


General Settings @ Event		
Item	**Description**	**Default**
Signal Quality Threshold	Set the threshold for signal quality. Router will generate a log event when the actual threshold is less than the specified threshold. 0 means disable this option.	0



Click + button to add an Event parameters.

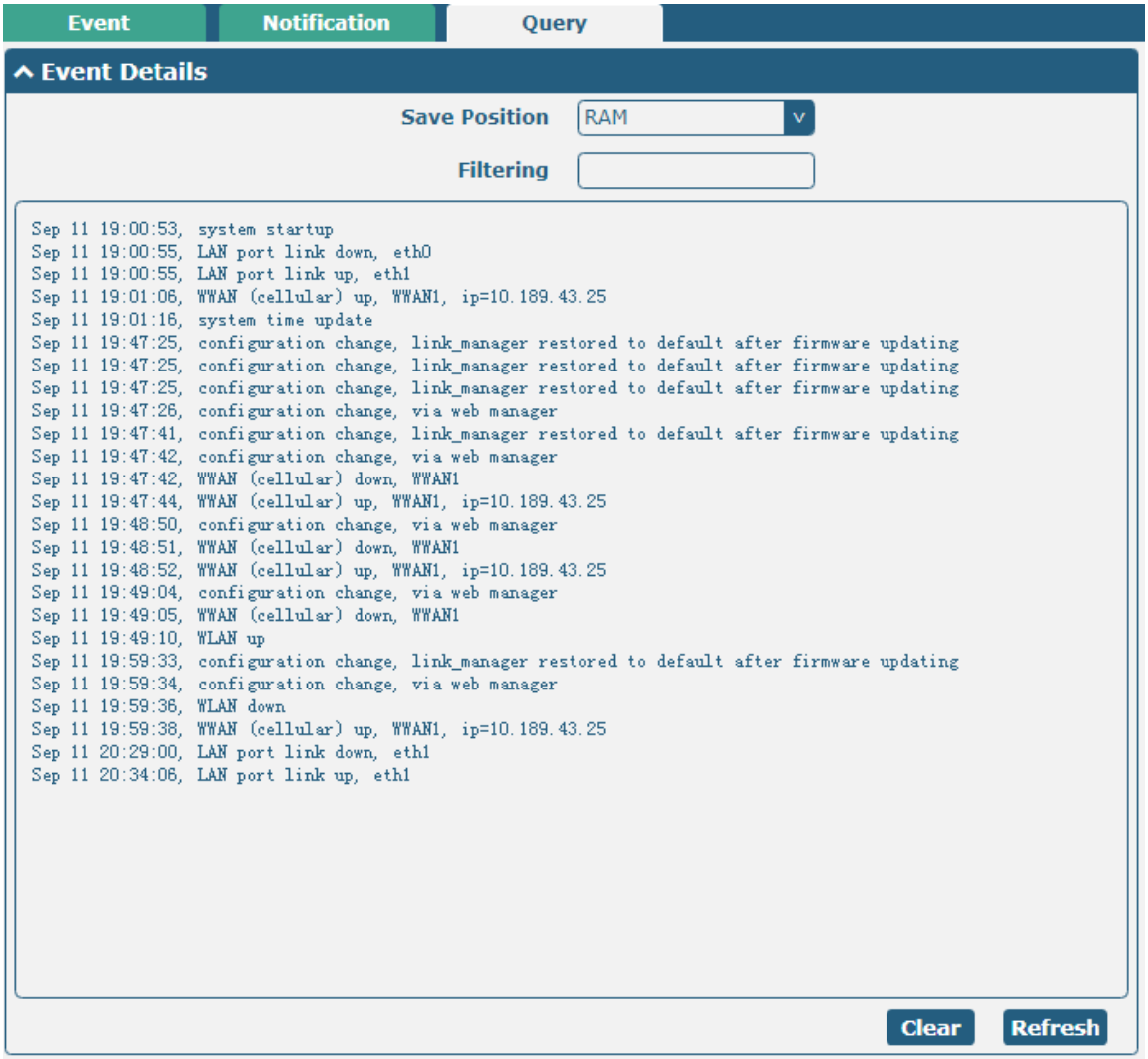




General Settings @ Notification		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this group.	Null
Sent SMS	Click the toggle button to enable/disable this option. When enabled, the router will send notification to the specified phone numbers via SMS if event occurs.	OFF
Send Email	Click the toggle button to enable/disable this option. When enabled, the router will	OFF

	send notification to the specified email box via Email if event occurs.	
Email Addresses	Enter the email addresses used for receiving event notification. Use a space to separate each address.	OFF
Save to NVM	Click the toggle button to enable/disable this option. Enable to save event to nonvolatile memory.	OFF

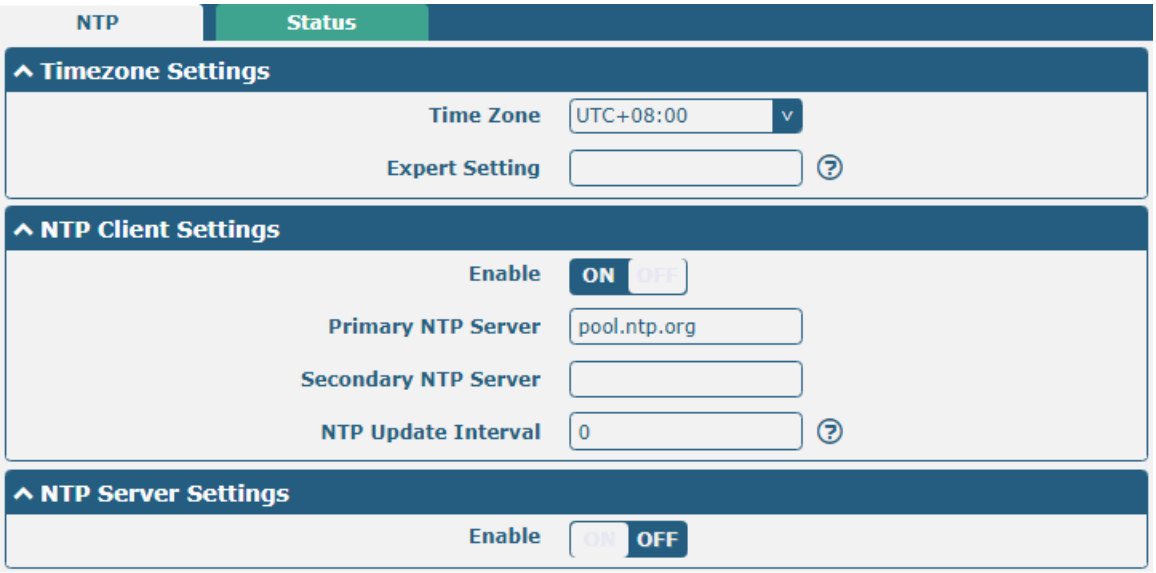
In the following window you can query various types of events record. Click **Refresh** to query filtered events while click **Clear** to clear the event records in the window.



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	Event will be filtered according to the Filter Message that the user set. 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

4.5.3 NTP

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

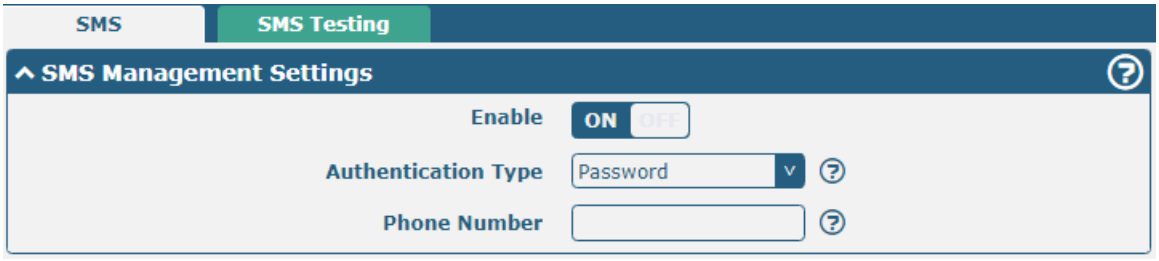


NTP		
Item	**Description**	**Default**
Timezone Settings		
Time Zone	Click the drop down list to select the time zone you are in. e.g., China: UTC+08:00.	UTC +08:00
Expert Setting	Specify the time zone with Daylight Saving Time in TZ environment variable format. The Time Zone option will be ignored in 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) which NTP client synchronize the time from NTP server. Minutes wait for next update, and 0 means update only once.	0
NTP Server Settings		
Enable	Click the toggle button to enable the NTP server option. When enabled, the NTP client can synchronize with the router in time.	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 PC's.

4.5.4 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 **5.2.2 SMS Remote Control**.



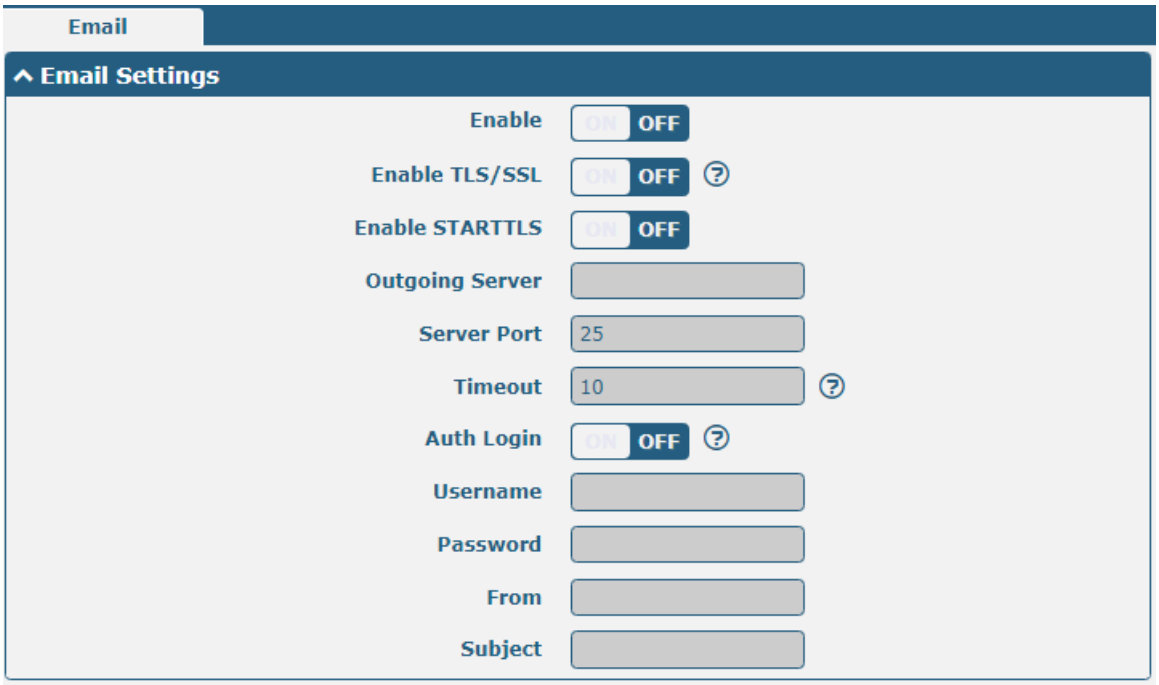
SMS Management Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the SMS Management option. **Note**: If this option is disabled, the SMS configuration is invalid.	ON
Authentication Type	Select Authentication Type from “Password”, “Phone num” or “Both”. • Password: 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 authenticating, 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. **Note**: It can be null when choose “Password” as the authentication type.	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.	--

4.5.5 Email

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

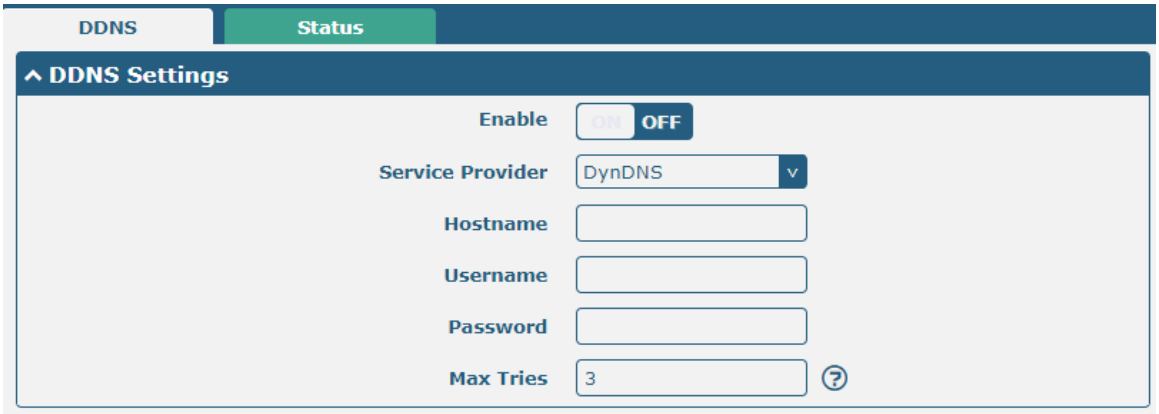


Email Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Email option.	OFF
Enable TLS/SSL	Click the toggle button to enable/disable the TLS/SSL option.	OFF
Enable STARTTLS	Click the toggle button to enable/disable STARTTLS encryption.	OFF
Outgoing server	Enter the SMTP server IP Address or domain name.	Null
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
Auth Login	If the mail server supports AUTH login, you must enable this button and set the username and password.	OFF
Username	Enter the username which has been registered from SMTP server.	OFF
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

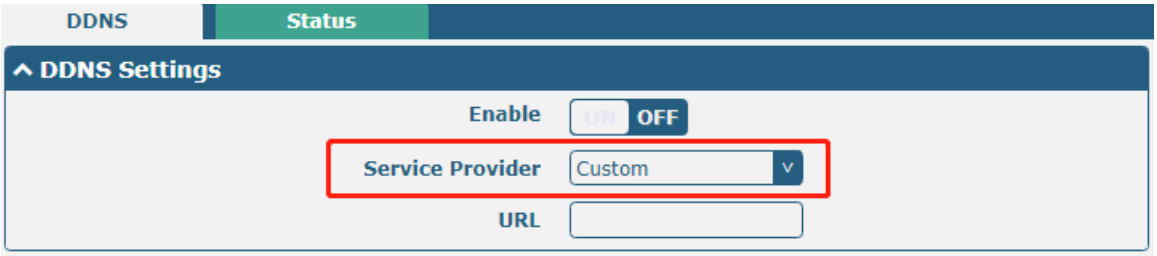
4.5.6 DDNS

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.

Click **Service > DDNS** to set the parameters related to DDNS. The service provider defaults to DynDNS.

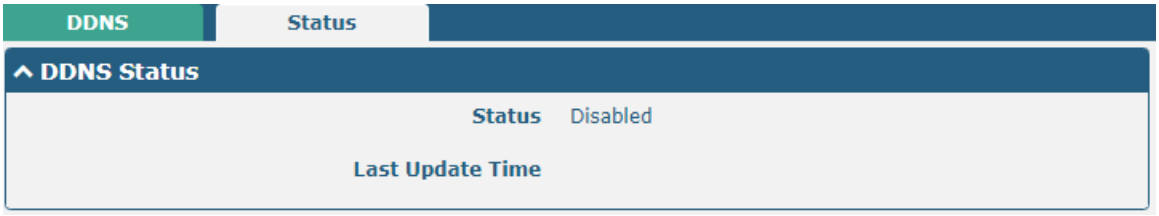


When service provider chose "Custom", the window is displayed as below.



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
Max Tries	Enter max tries	3

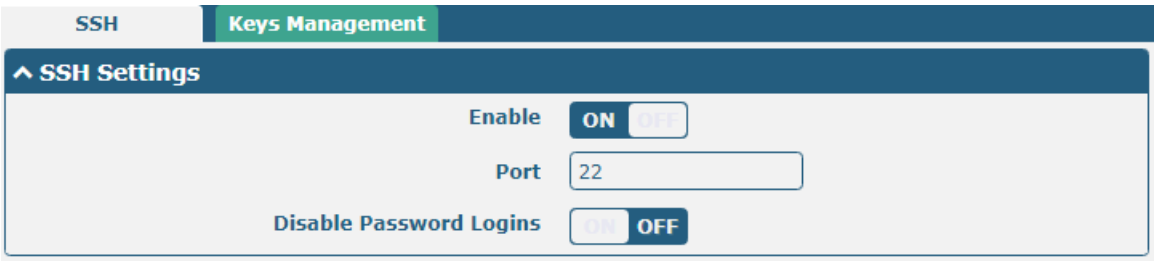
Click “Status” bar to view the status of the DDNS.



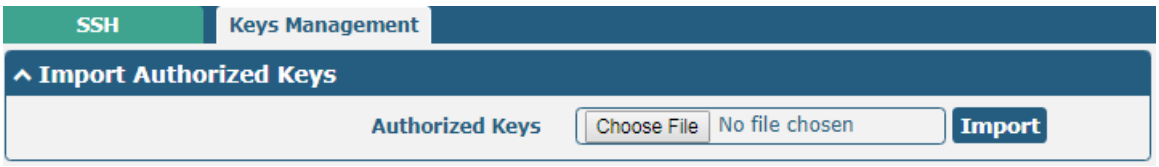
DDNS Status	
Item	**Description**
Status	Display the current status of the DDNS.
Last Update Time	Display the date and time for the DDNS was last updated successfully.

4.5.7 SSH

Router supports SSH password access and secret-key access.



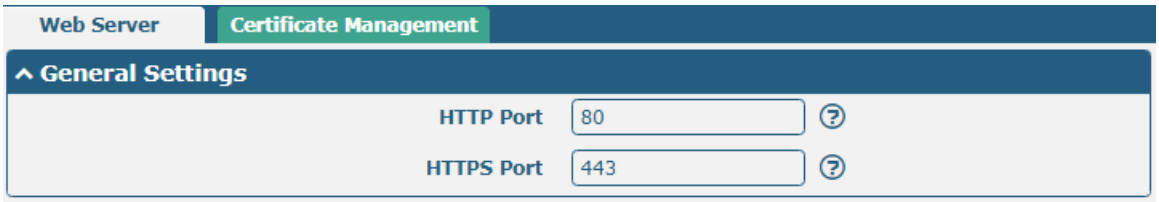
SSH Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable this option. When enabled, you can access the router via SSH.	ON
Port	Set the port of the SSH access.	22
Disable Password Logins	Click the toggle button to enable/disable this option. When enabled, you cannot 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.

4.5.8 Web Server

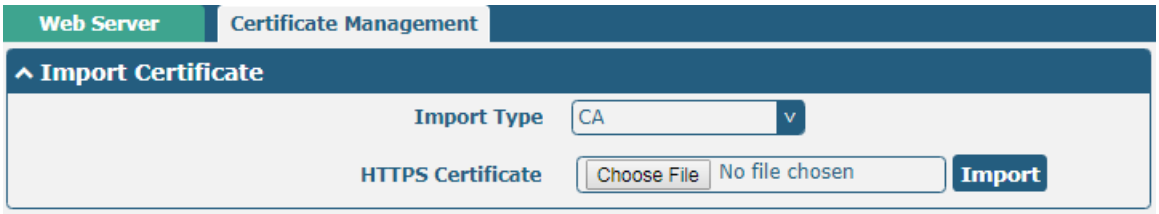
This section allows you to modify the parameters of Web Server.



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 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	443

	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.	

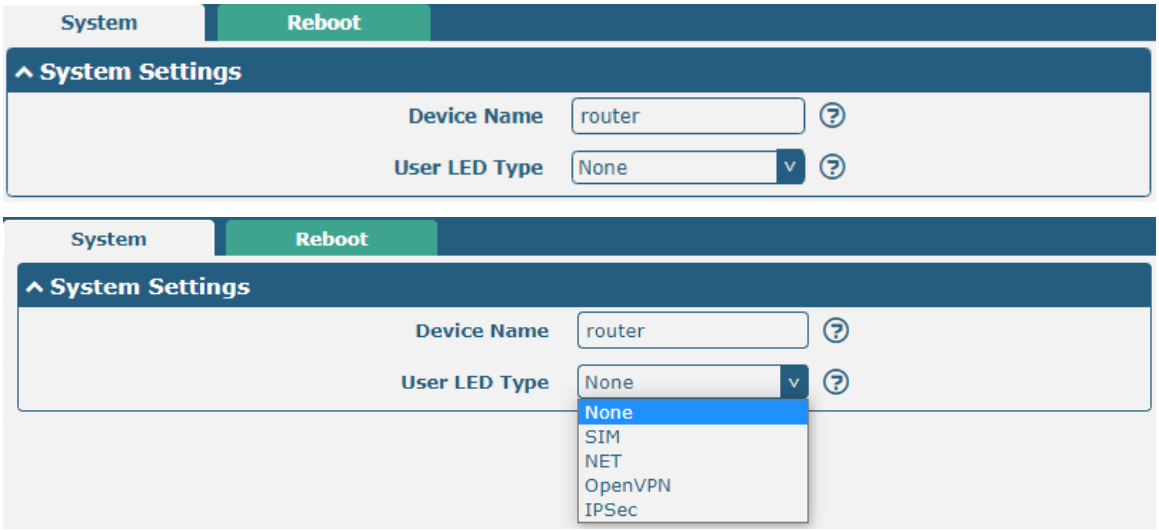
This section allows you to import the certificate file into the router.



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.	--

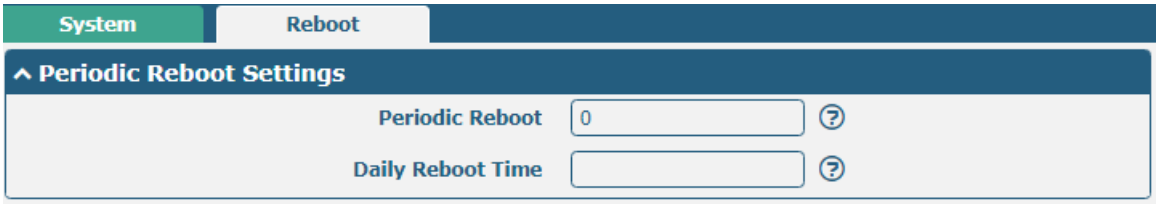
4.5.9 Advanced

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", "SIM", "NET",	None

	"OpenVPN" or "IPsec". • None: Meaningless indication, and the LED is off • SIM: show the sim status. • NET: After selecting this type, the USR indicator of the gateway shows the status of NET • OpenVPN: USR indicator showing the OpenVPN status • IPsec: USR indicator showing the IPsec status **Note**: For more details about USR indicator, see "2.2 LED Indicators".	

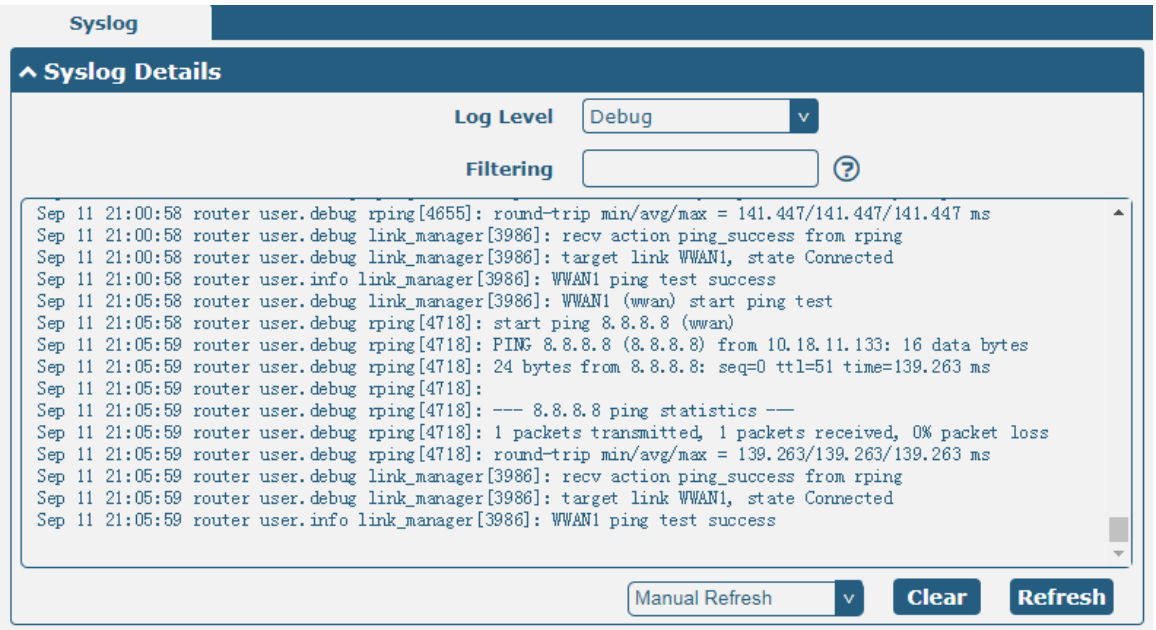


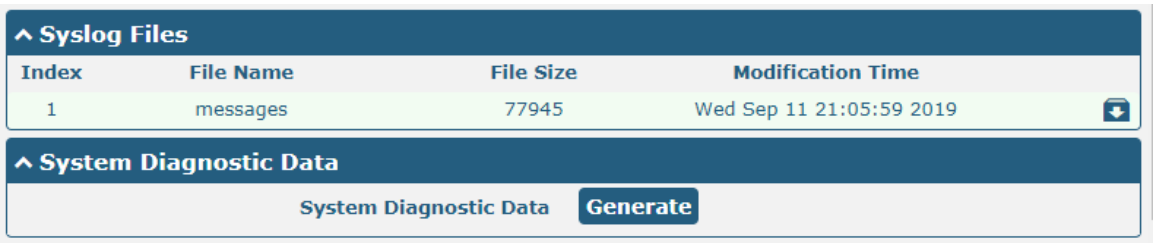
Reboot		
Item	**Description**	**Default**
Periodic Reboot	Set the reboot period of the router. 0 means disable.	0
Daily Reboot Time	Set the daily reboot time of the router, you should follow the format as HH: MM, in 24h time frame, otherwise the data will be invalid. Leave it empty means disable.	Null

4.6 System

4.6.1 Debug

This section allows you to check and download the syslog details. Click Service > System Log > System Log Settings to open the system log.



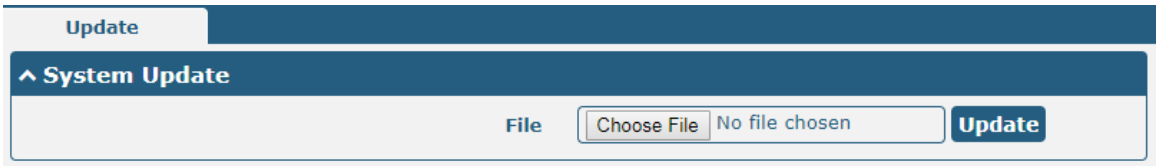


Syslog	
Item	**Description**
Syslog Details	
Log Level	Select from “Debug”, “Info”, “Notice”, “Warn”, “Error” which from low to high. The lower level will output more syslog in detail.
Filtering	Enter the filtering message based on the keywords. Use “&” to separate more than one filter message, such as “keyword1&keyword2”.
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.
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.

4.6.2 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.

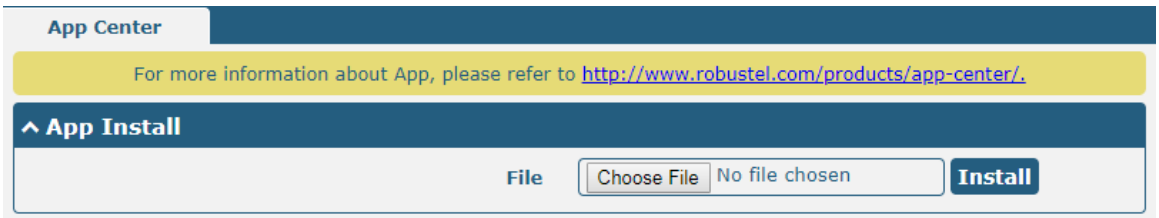
Note: To access the latest firmware file, please contact your technical support engineer.



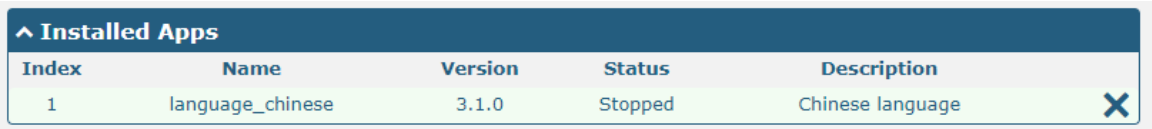
4.6.3 App Center

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.



Successfully installed apps will be displayed in the following list, click ✕ to uninstall the app.

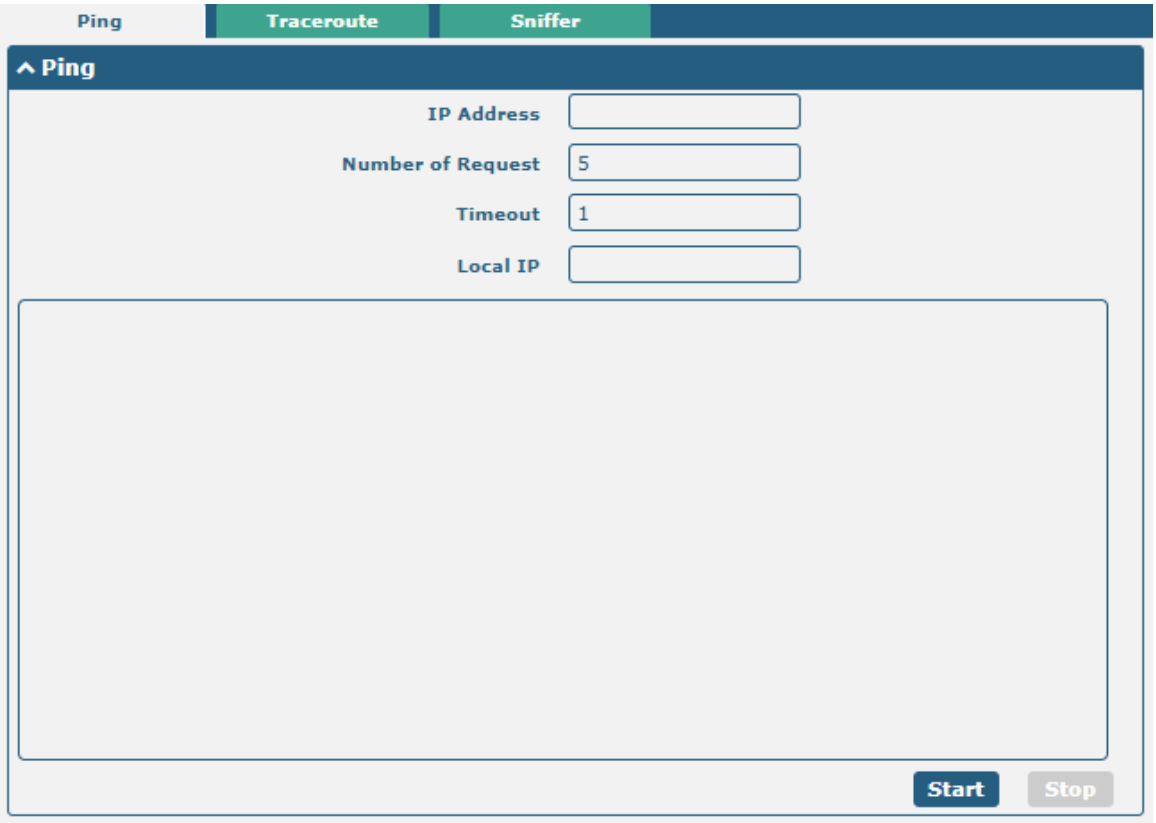


App Center		
Item	**Description**	**Default**
App Install		
File	Click on "Choose File" to locate the App file from your computer, and then click **Install** to import this file into your router. **Note**: File format should be *xxx.rpk*, e.g. *R1511-robustlink-1.0.0.rpk*.	--
Installed Apps		
Index	Indicate 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

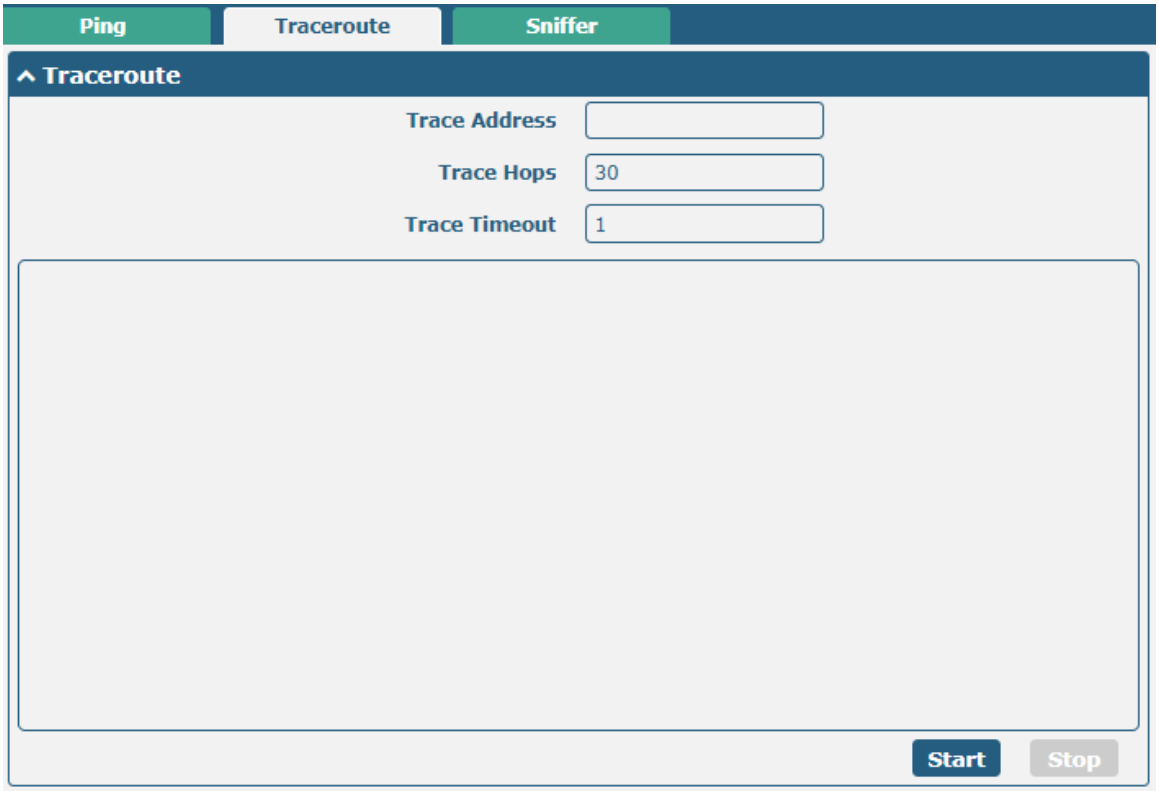
App Center		
Item	**Description**	**Default**
App Install		
Description	Show the description for this App.	Null

4.6.4 Tools

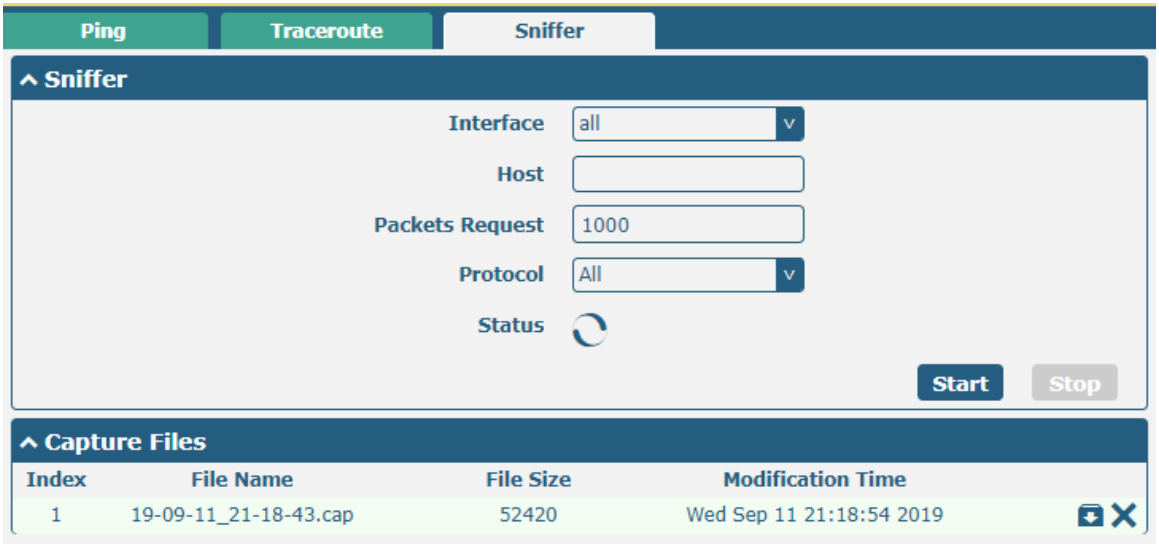
This section provides users three tools: Ping, Traceroute and Sniffer. The Ping tool is used to detect the network connectivity of the router.



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 request.	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.	--
Stop	Click this button to stop ping request.	--



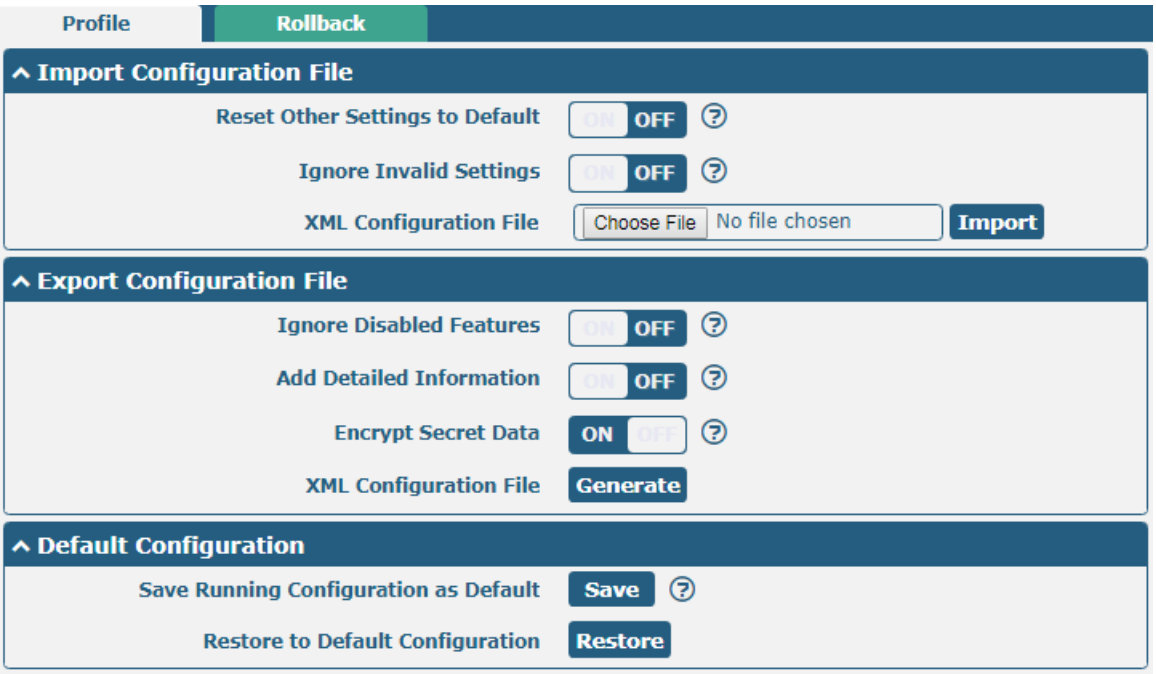
Traceroute		
Item	**Description**	**Default**
Trace Address	Enter the trace's destination IP address or destination domain.	Null
Trace Hops	Specify the max trace hops. Router will stop tracing if the trace hops has met max value no matter the destination has been reached or not.	30
Trace Timeout	Specify 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
Status	Show the current status of sniffer.	--
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.	--

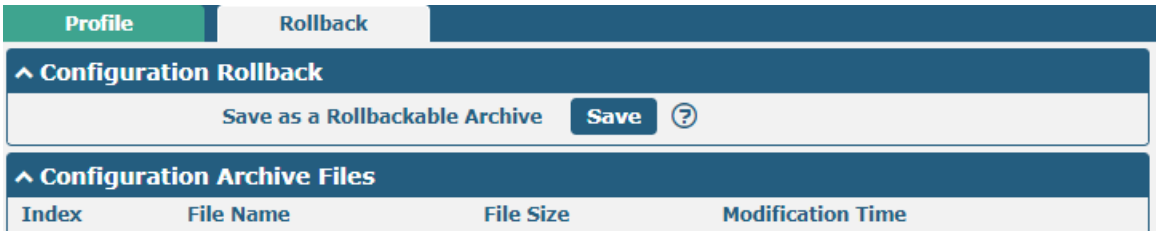
4.6.5 Profile

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 “ON” to ignore invalid settings.	ON

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 "ON" 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.	ON
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.	--

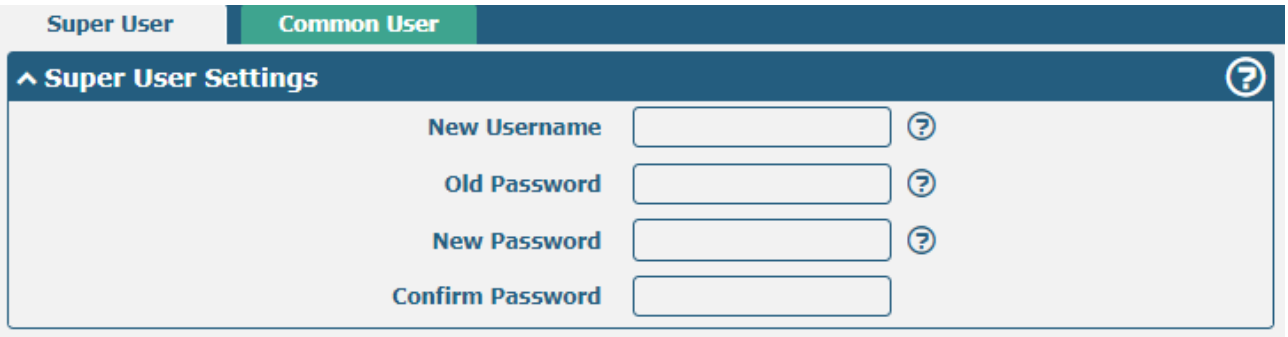


Rollback		
Item	**Description**	**Default**
Configuration Rollback		
Save as a Rollbackable Archive	Create a save point manually. Additionally, the system will create a save point every day automatically if configuration changes.	--
Configuration Archive Files		
Configuration Archive Files	View the related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

4.6.6 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**
New Username	Enter a new username you want to create,If you do not want to change username, leave it blank. 5-32 characters, valid characters: a-z, A-Z, 0-9, @, #, $, ., *, !, -	Null
Old Password	Enter the old password of your router. The default is “admin”, 5-32 characters, valid characters: a-z, A-Z, 0-9, @, #, $, ., *, !, -	Null
New Password	Enter a new password you want to create, 5-32 characters, valid characters: a-z, A-Z, 0-9, @, #, $, ., *, !, -	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.

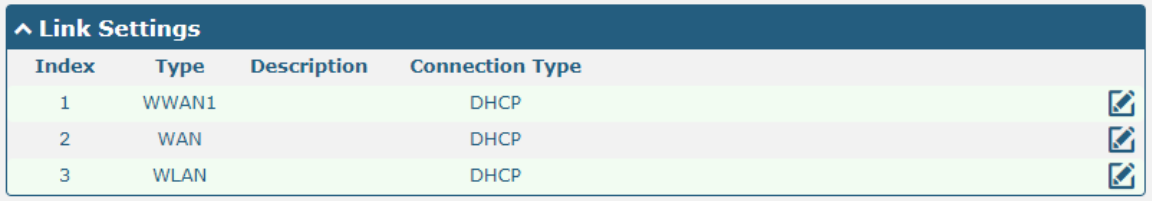
Common User Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Role	Select from “Visitor” and “Editor”. • Visitor: Users only can view the configuration of router under this level • Editor: Users can view and set the configuration of router under this level	Visitor
Username	Set the Username, 5-32 characters, valid characters: a-z, A-Z, 0-9, @, #, $, ., *, !, -	Null
Password	Set the password, 5-32 characters, valid characters: a-z, A-Z, 0-9, @, #, $, ., *, !, -	Null

Chapter 5 Configuration Examples

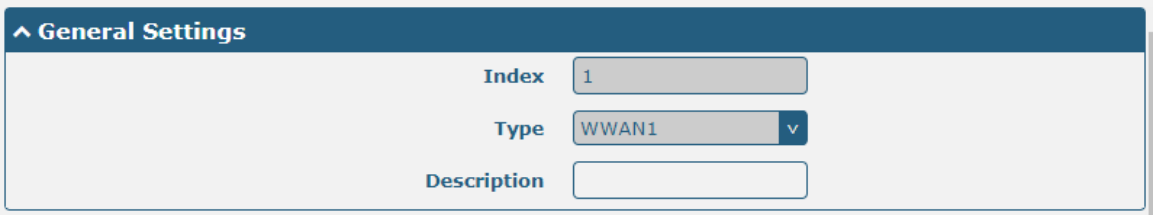
5.1 Cellular

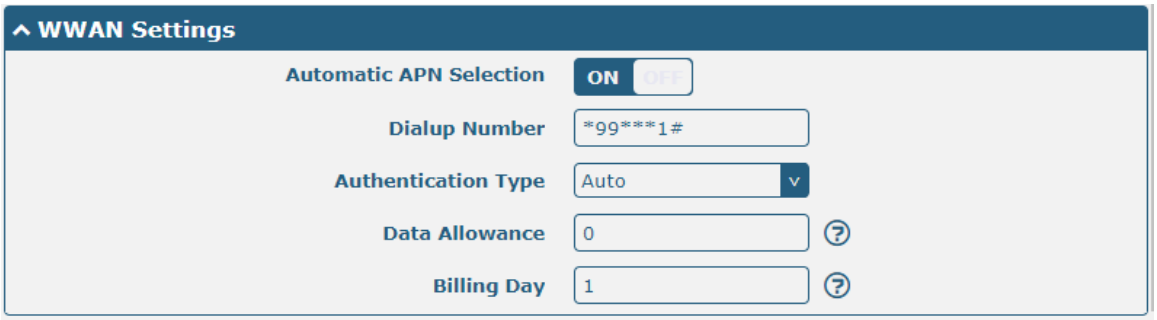
5.1.1 Cellular Dial-Up

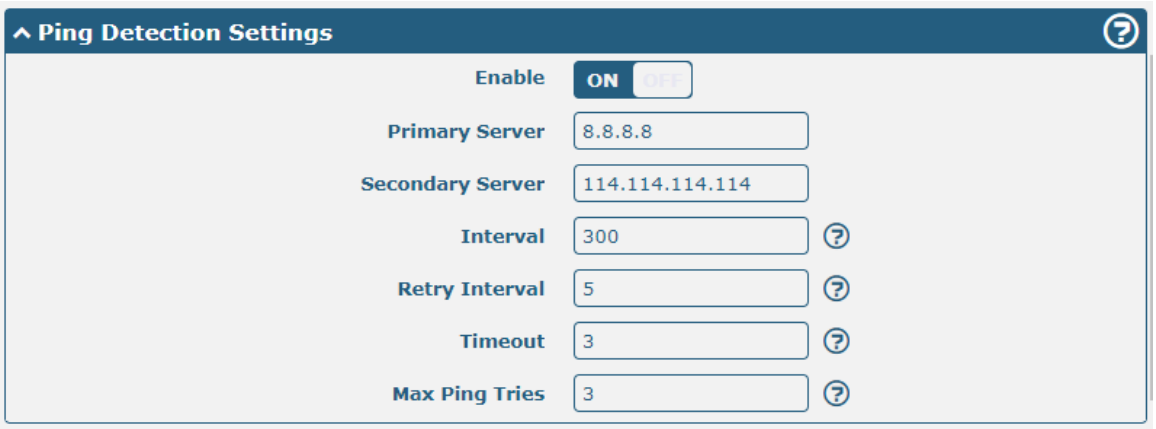
This section shows you how to configure the primary and backup SIM card for Cellular Dial-up. Connect the router correctly and insert two SIM, then open the configuration page. Under the homepage menu, click **Interface > Link Manager > Link Manager > General Settings**, choose “WWAN1” as the primary link and “None” as the backup link, then click “Submit”.

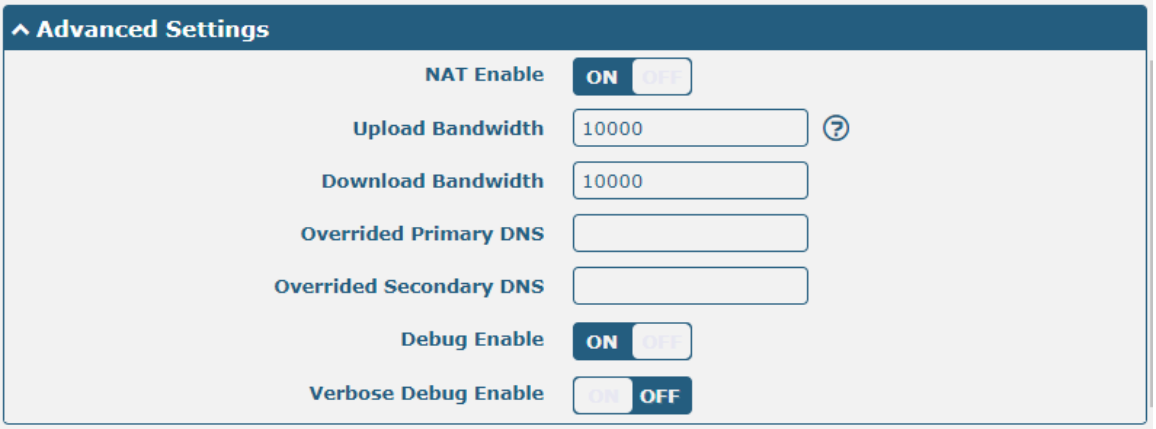


Click the right most of edit button of WWAN1 to set its parameters according to the current ISP.



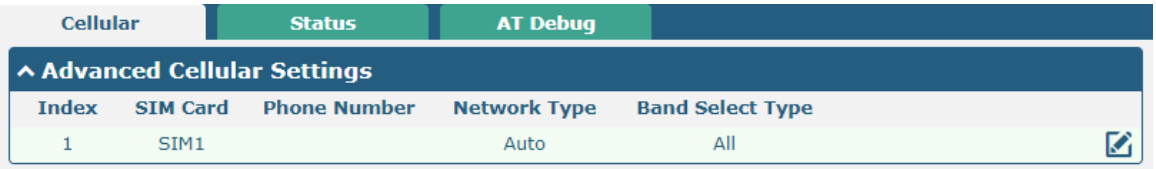




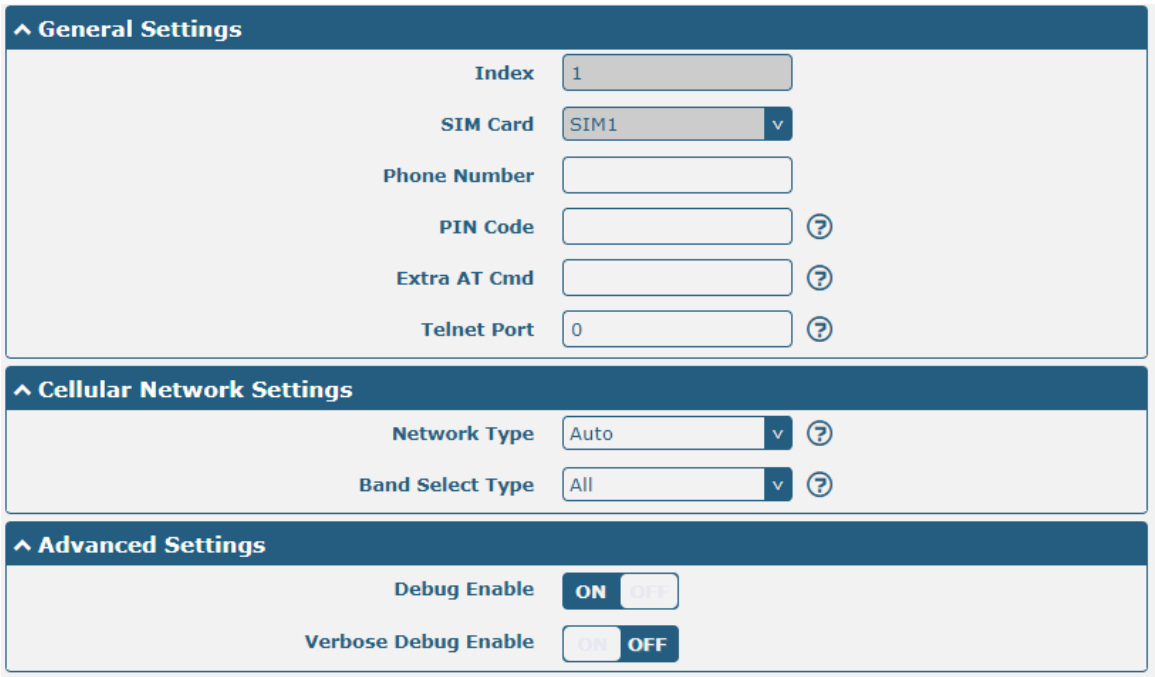


When finished, click **Submit > Save & Apply** for the configuration to take effect.

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



Click the right most of 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.

5.1.2 SMS Remote Control

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

An SMS command has the following structure:

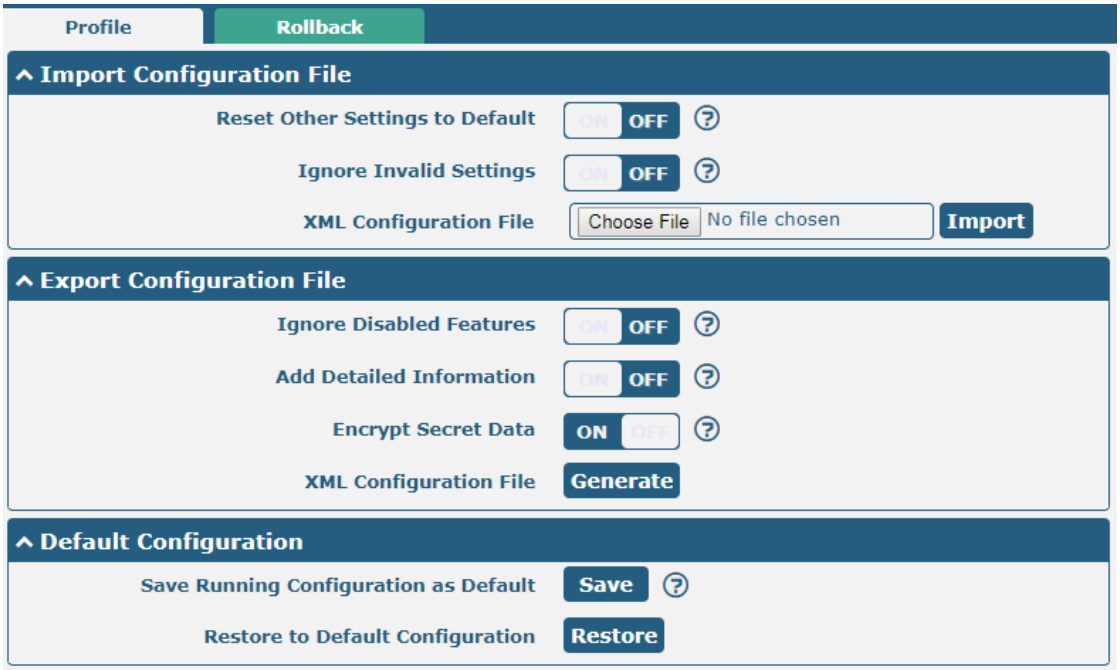
1. Password mode—**Username:Password;cmd1;cmd2;cmd3;…cmdn** (available for every phone number).
2. Phonenum mode--**cmd1;cmd2;cmd3;… cmdn** (available when the SMS was sent from the phone number which had been added in R1511’s phone group).
3. Both mode—**Username:Password;cmd1;cmd2;cmd3;…cmdn** (available when the SMS was sent from the phone number).

Note: All command symbols must be entered in the English input half angle mode.

SMS command Explanation:

1. Password: The SMS control password defaults to the login password of the super user or the login password of the ordinary user who has read and write permissions.
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 6 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**, Select export type as "complete", 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>172.16.24.24</ip>
<netmask>255.255.0.0</netmask>
<mtu>1500</mtu>
```

SMS cmd:

set lan network 1 interface lan0
set lan network 1 ip 172.16.24.24
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 command packed in a single SMS.
4. E.g.

Password mode—admin:admin;status system

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

SMS received:

firmware_version = 3.1.5
firmware_version_full = "3.1.5 (Rev 3428)"
hardware_version = 1.0
kernel_version = 4.9.152
device_model = R1511
serial_number = ""
uptime = "0 days, 00:25:13"
system_time = "Thu Aug 20 09:42:11 2020"

ram_usage = "76M Free/128M Total"

admin:admin;reboot

In this command, username is “admin”, password is “admin”, and the command is to reboot the R1511 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 172.16.24.24;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

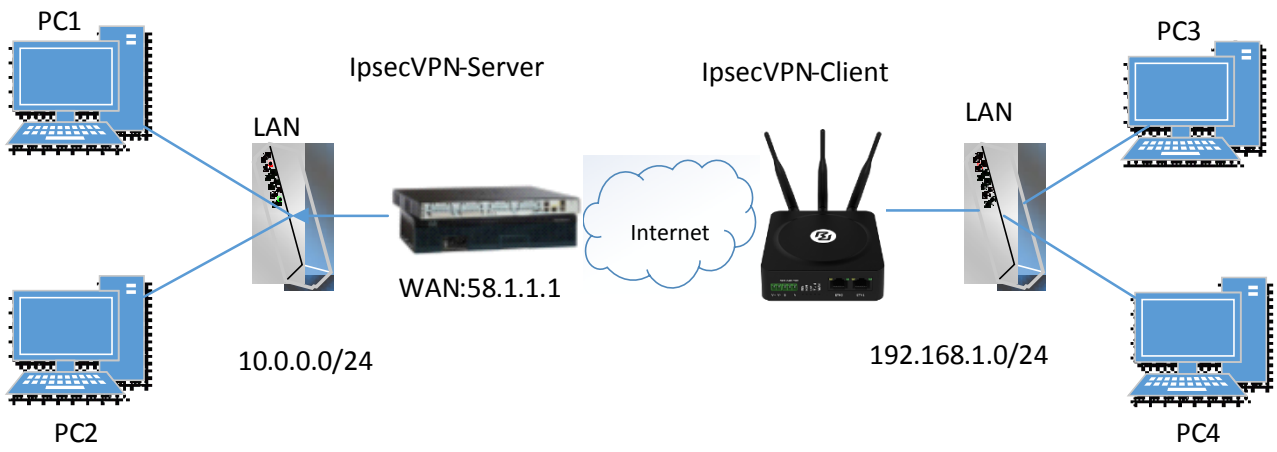
OK

OK

5.2 VPN Configuration Example

5.2.1 IPsec VPN

IPSec VPN sample topology (configuration of Ike and SA parameters of server and client must be consistent):



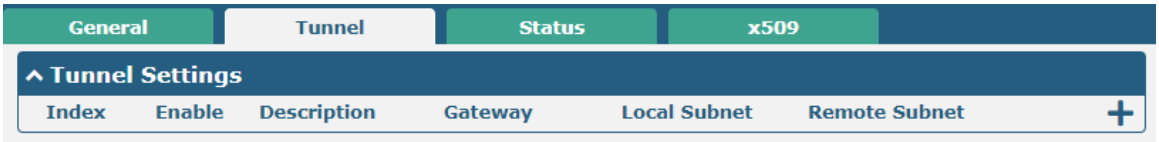
IPsec VPN_Server:

Cisco 2811:

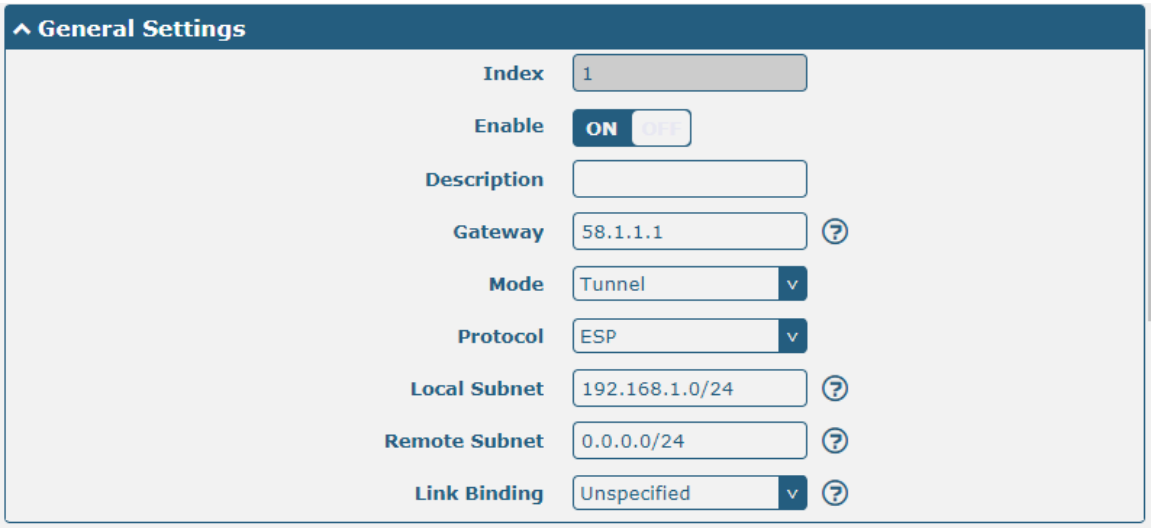
```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set 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
```

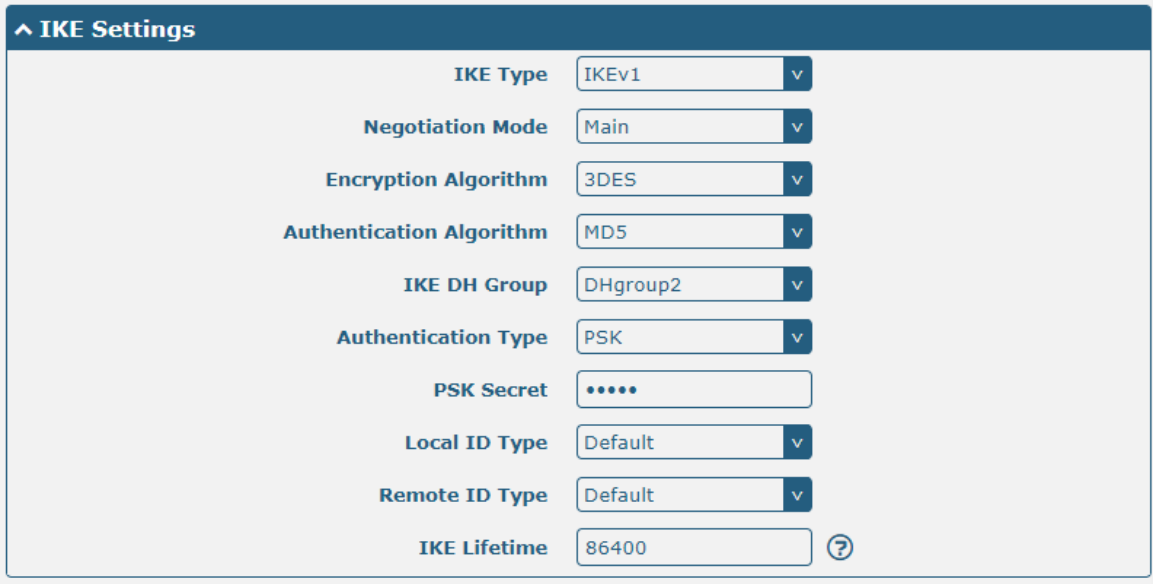
IPsec VPN_Client:

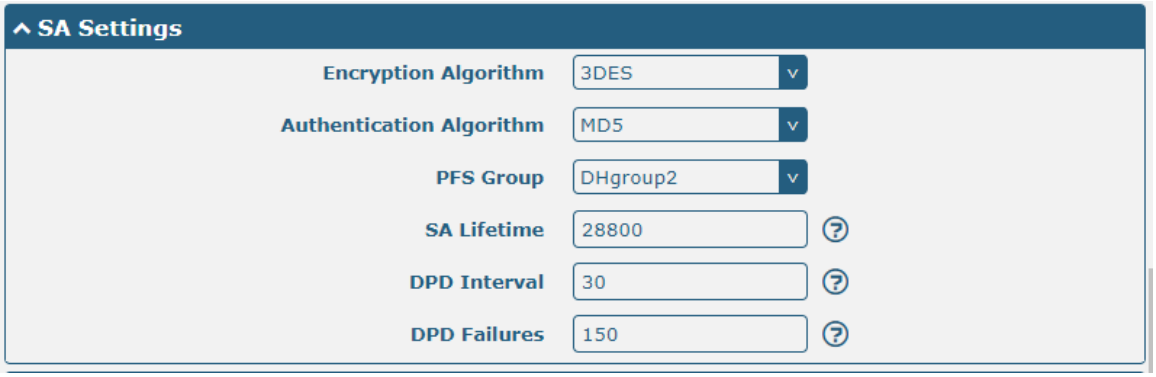
The window is displayed as below by clicking **VPN > IPsec > Tunnel**.

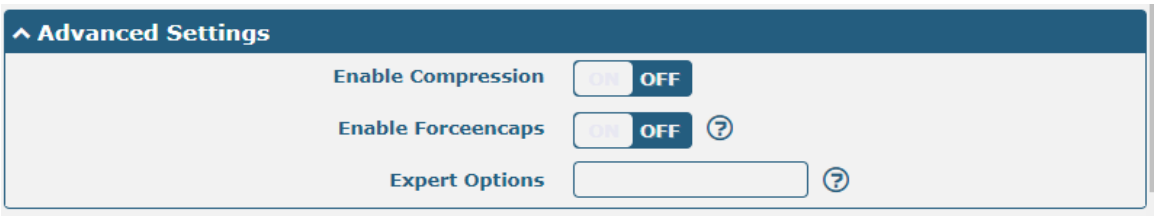


Click + button and set the parameters of IPsec Client as below.



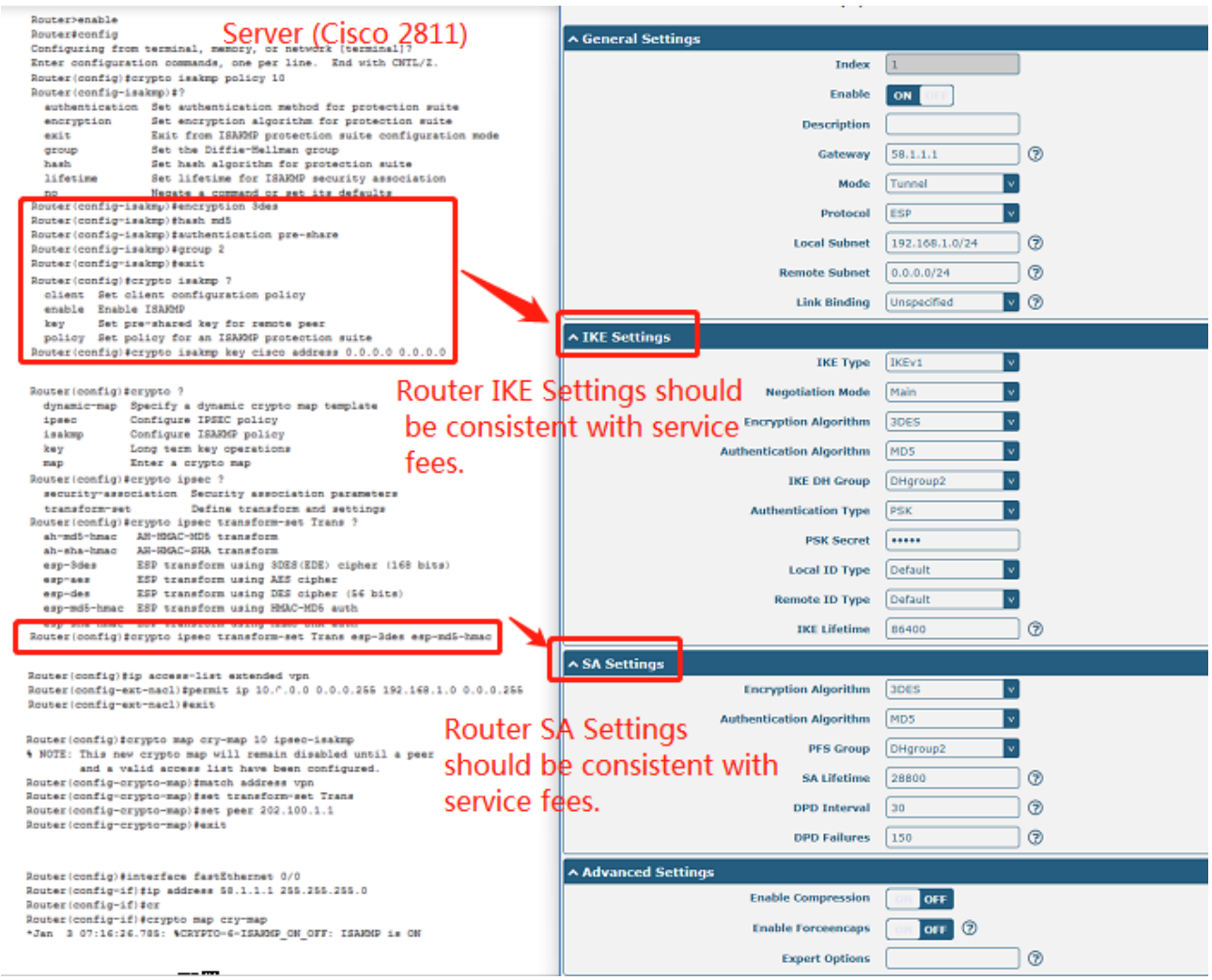






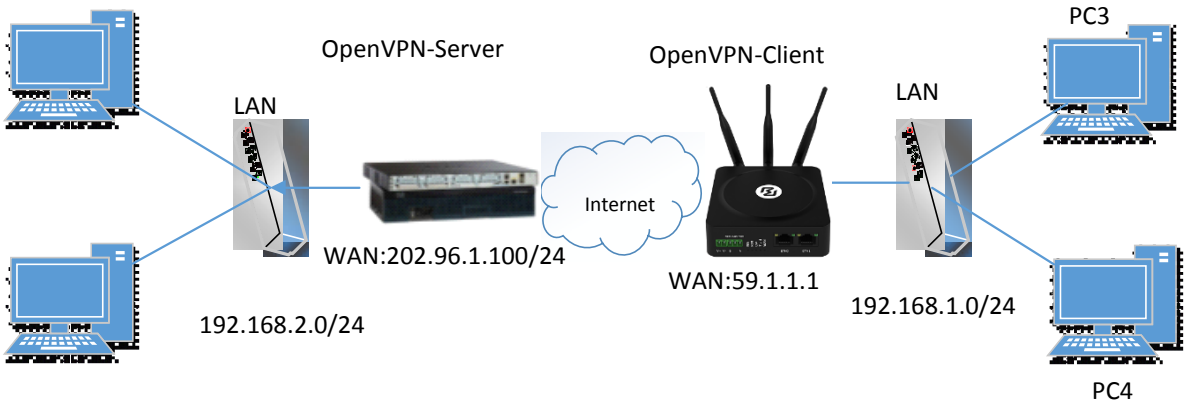
When finished, click **Submit > Save & Apply** for the configuration to take effect.

The comparison between IPec Server and Client is as below.



5.2.2 OpenVPN

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



The configuration of two points is as follows.

OpenVPN_Server:

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

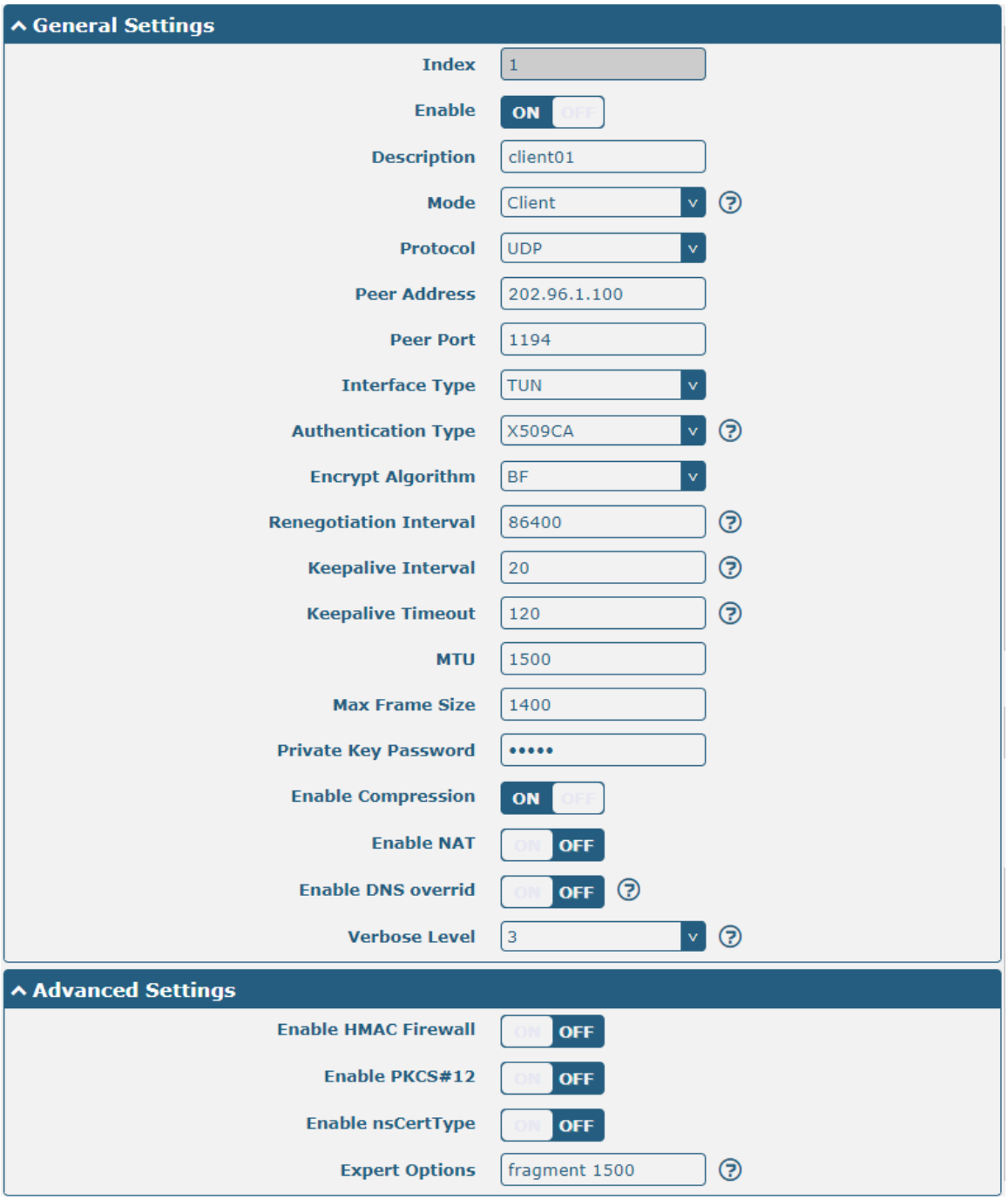
```
local 202.96.1.100
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert Server01.crt
key Server01.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.3.0 255.255.255.0"
client-config-dir ccd
route 192.168.1.0 255.255.255.0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

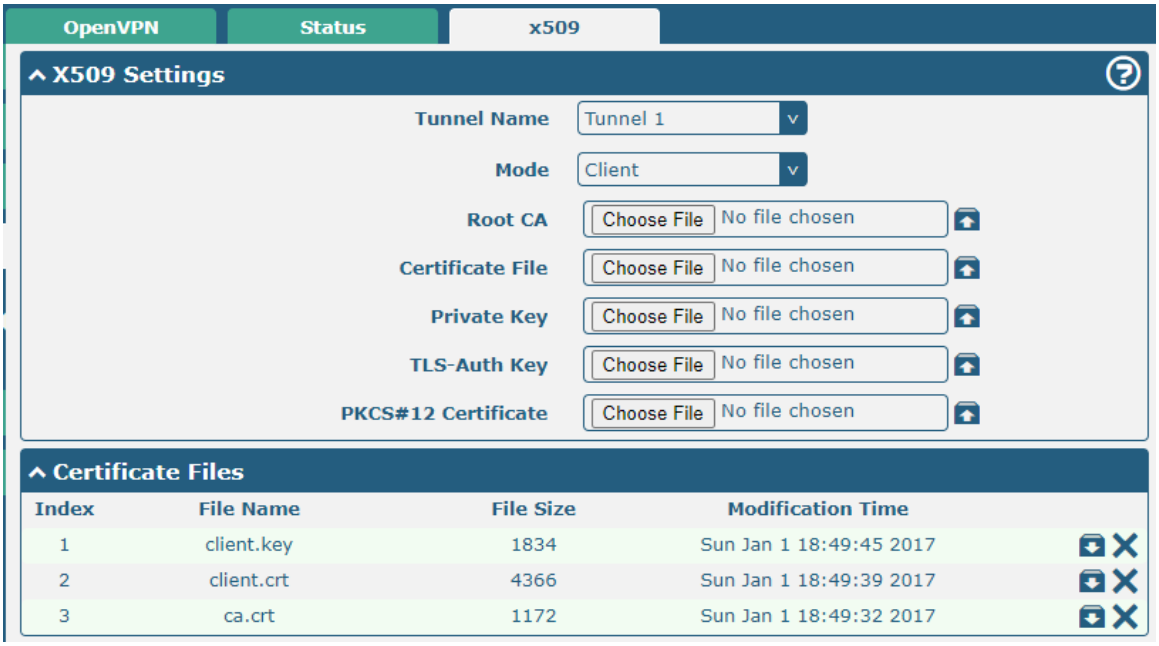
Note: For more configuration details, please contact your technical support engineer.

OpenVPN_Client:

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

Click + to configure the Client01 as below.

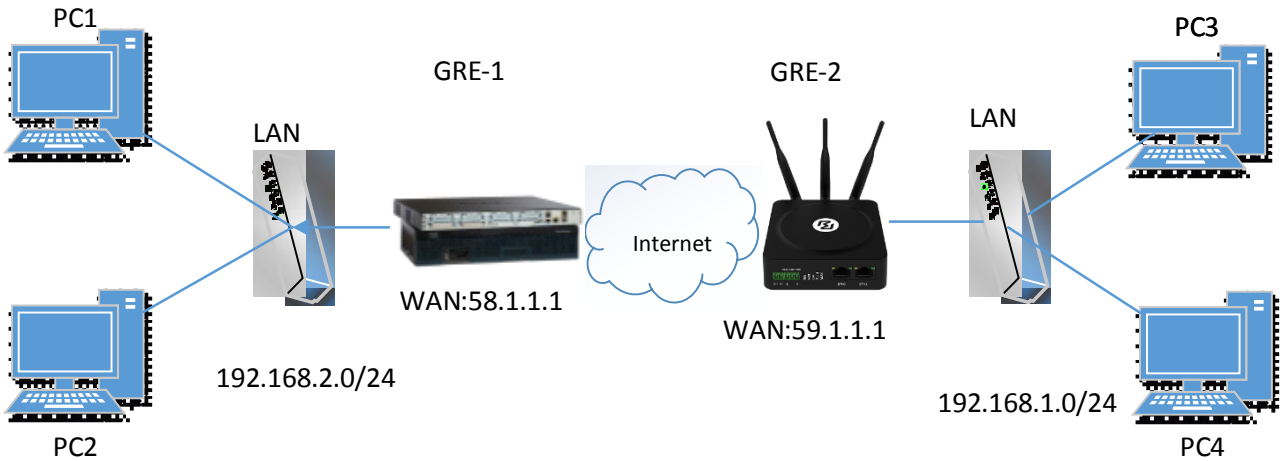




When finished, click **Submit > Save & Apply** for the configuration to take effect.

5.2.3 GRE VPN

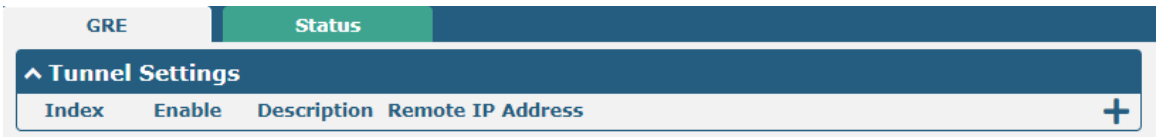
GRE VPN example topology:



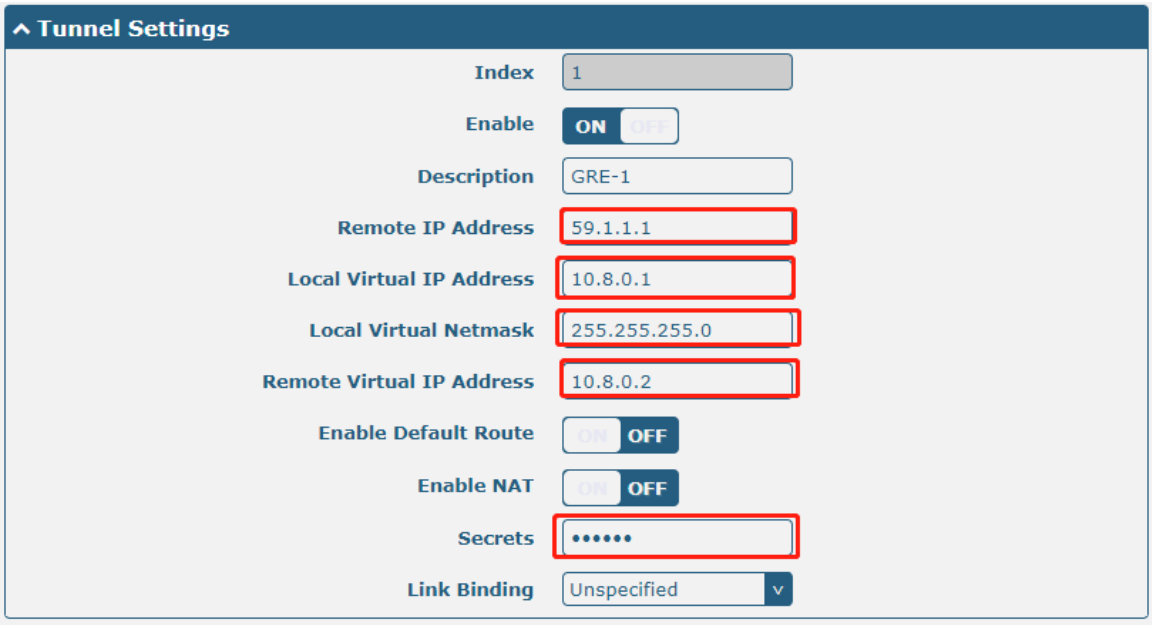
The configuration of two points is as follows.

GRE-1:

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



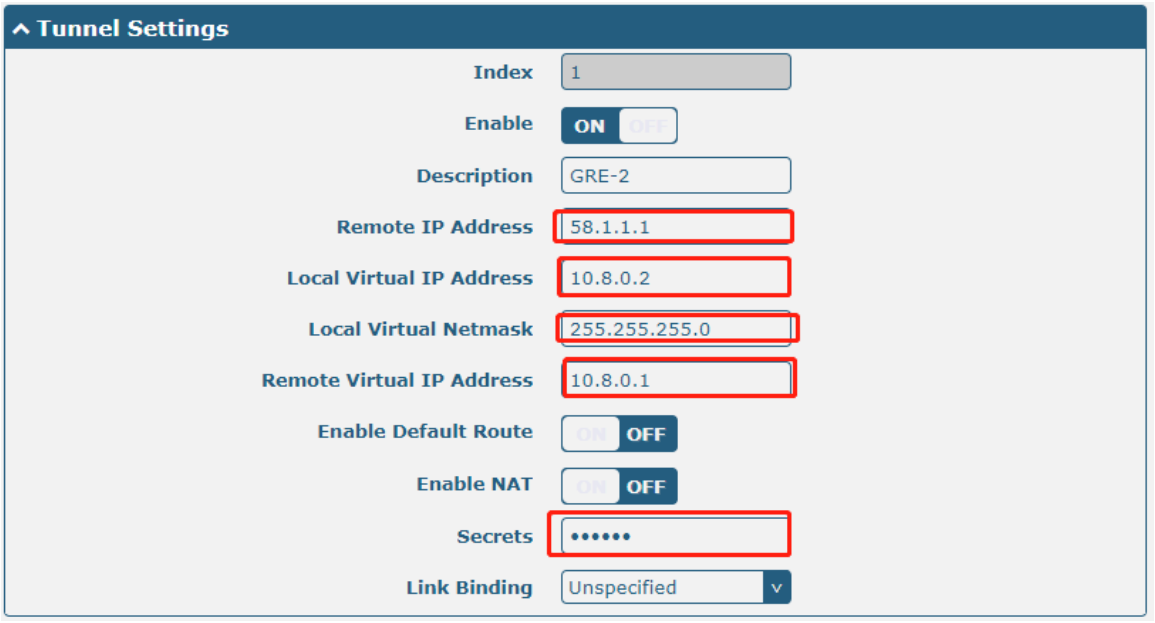
Click + button and set the parameters of GRE-1 as below.



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

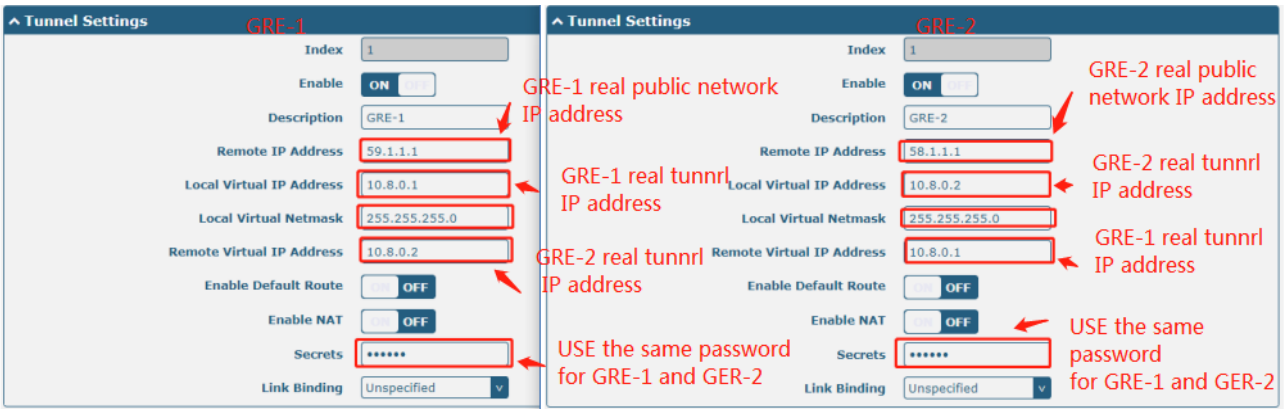
GRE-2:

Click + button and set the parameters of GRE-2 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.



Chapter 6 Introductions for CLI

6.1 What Is CLI

The Command Line Interface (CLI) is a set of software interfaces that provide another way to configure device parameters. Users can connect to the router through SSH or telnet to configure CLI commands. After establishing a Telnet or SSH connection with the router, enter the login account and password (default admin/admin) to enter the router's configuration mode, as shown below.

```
router login: admin
Password:
#
  !               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
  ovpn_cert_get   Download OpenVPN certificate file via http or ftp
  ping            Send messages to network hosts
  reboot          Halt and perform a cold restart
  set             Set system configuration
  show            Show system configuration
  status          Show running system information
  tftpupdate      Update firmware or configuration file using tftp
  traceroute      Print the route packets trace to network host
  trigger         Trigger action
  urlupdate       Update firmware via http or ftp
  ver             Show version of firmware

#
```

Router login:

Router login: admin

Password: admin

#

CLI commands:

?

!	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

6.2 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. Example: # config（Tick '?'） config Configuration operation # config（Tick the space key+'?'） commit Save the configuration changes and take effect changed configuration save_and_apply Save the configuration changes and take effect changed configuration loaddefault Restore Factory Configuration
Ctrl+c	Tick 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 your currently incomplete commands. 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.

6.3 Commands Reference

Commands	Syntax	Description
Debug	Debug *parameters*	enable on or disenable the debug function
Show	Show *parameters*	Show current configuration of each function
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: More detail about CLI command, please refer to "Command Line Interface Guide".

6.4 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
firmware_version = 3.1.5
firmware_version_full = "3.1.5 (Rev 3428)"
hardware_version = 1.0
kernel_version = 4.9.152
device_model = R1511
serial_number = “”
uptime = "0 days, 00:45:43"
system_time = "Thu Aug 20 09:42:11 2020"
ram_usage = "78M Free/128M Total
```

Example 2: Update firmware via tftp

```
# tftpupdate （space+?）
  firmware    New firmware
   config       New configuration file
# tftpupdate firmware （space+?）
  filename    New file
# tftpupdate firmware filename R1511-firmware-sysupgrade-unknown.ruf host 192.168.100.99 // enter a new firmware name
Downloading
Download success.
Upgrading
Upgrade success.            //update success
# reboot                    //make you configuration effect after reboot
Rebooting...
OK
```

Example 3: Set link-manager

```
# set
# set (space+?)
   cellular                Cellular
   ddns                    DDNS
   dido                    DIDO
   email                   Email
```

```
   ethernet              Ethernet
   event                 Event Management
   firewall              Firewall
   gre                   GRE
   ip_passthrough        IP Passthrough
   ipsec                 IPSec
   lan                   Local Area Network
   link_manager          Link Manager
   ntp                   NTP
   openvpn               OpenVPN
   reboot                Automatic Reboot
   route                 Route
   serial_port           Serial
   sms                   SMS
   ssh                   SSH
   syslog                Syslog
   system                System
   user_management       User Management
   web_server            Web Server
   wifi                  WiFi AP

# set link_manager（space+?）
   primary_link          Primary Link
   backup_link           Backup Link
   backup_mode           BackSup Mode
   revert_interval       Revert Interval
   emergency_reboot      Emergency Reboot
   link                  Link Settings
# set link_manager primary_link（space+?）
Enum    Primary Link  （wwan1/wan/wlan）
 # set link_manager primary_link wwan1                    //select “wwan1” as primary link
OK                                                        //setting succeed
#set link_manager link 1（space+?）
   type                  Type
   desc                  Description
   connection_type       Connection Type
   wwan                  WWAN Settings
   static_addr           Static Address Settings
   pppoe                 PPPoE Settings
   ping                  Ping Settings
   nat_enable            NAT Enable
   mtu                   MTU
   weight                Weight
   upload_bandwidth      Upload Bandwidth
   download_bandwidth    Download Bandwidth
   dns1_overrided        Overrided Primary DNS
```

```
   dns2_overrided              Overrided Secondary DNS
   debug_enable                Debug Enable
   verbose_debug_enable        Verbose Debug Enable
# set link_manager link 1 type wwan1
OK
# set link_manager link 1 wwan（space+?）
   auto_apn                    Automatic APN Selection
   apn                         APN
   username                    Username
   password                    Password
   dialup_number               Dialup Number
   auth_type                   Authentication Type
   data_allowance              Data Allowance
   billing_day                 Billing Day
# 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 Ethernet

```
# set Ethernet port_setting 2 port_assignment lan0          //Set Table 2 (eth1) to lan0
OK
# config save_and_apply          //save and apply current configuration, make you configuration effect
OK
```

Example 5: 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
            static_lease = ""
            expert_options = ""
            debug_enable = false
        }
        vlan_id = 0
}
#
# set lan（space+?）
    network          Network Settings
    multi_ip     Multiple IP Address Settings
# set lan network 1(space+?)
    interface    Interface
    ip           IP Address
    netmask      Netmask
    mtu          MTU
    dhcp         DHCP Settings
    Vlan_id       VLAN ID
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.24.24                    // 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 6: CLI for setting Cellular

```
# show cellular all
sim {
        id = 1
        card = sim1
        phone_number = ""
        pin_code = ""
        extra_at_cmd = ""
        telnet_port = 0
```

```
        network_type = auto
        band_select_type = all
        band_settings {
                gsm_850 = false
                gsm_900 = false
                gsm_1800 = false
                gsm_1900 = false
                wcdma_800 = false
                wcdma_850 = false
                wcdma_900 = false
                wcdma_1900 = false
                wcdma_2100 = false
                wcdma_1700 = false
                wcdma_band19 = false
                lte_band1 = false
                lte_band2 = false
                lte_band3 = false
                lte_band4 = false
                lte_band5 = false
                lte_band7 = false
                lte_band8 = false
                lte_band13 = false
                lte_band17 = false
                lte_band18 = false
                lte_band19 = false
                lte_band20 = false
                lte_band21 = false
                lte_band25 = false
                lte_band28 = false
                lte_band31 = false
                lte_band38 = false
                lte_band39 = false
                lte_band40 = false
                lte_band41 = false
        }
        telit_band_settings {
                gsm_band = 900_and_1800
                wcdma_band = 1900
        }
        debug_enable = true
        verbose_debug_enable = false
}
# set(space+space)
cellular        ddns            dido            email           ethernet
event           firewall        gre             ip_passthrough  ipsec
l2tp            lan             link_manager    ntp             openvpn
```

```
pptp            reboot          route           serial_port     sms
ssh             syslog          system          user_management web_server      wifi
# set cellular(space+?)
  sim    SIM Settings
# set cellular sim(space+?)
  Integer    Index (1..1)

# set cellular sim 1(space+?)
   card                    SIM Card
   phone_number            Phone Number
   pin_code                PIN Code
   extra_at_cmd            Extra AT Cmd
   telnet_port             Telnet Port
   network_type            Network Type
   band_select_type        Band Select Type
   band_settings           Band Settings
   telit_band_settings     Band Settings
   debug_enable            Debug Enable
   verbose_debug_enable    Verbose Debug Enable
# set cellular sim 1 phone_number 18620435279
OK
…
# config save_and_apply
OK                                          //save and apply current configuration, make you configuration eff
```

Glossary

Abbr.	Description
AC	Alternating Current
APN	Access Point Name of GPRS Service Provider Network
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
EDGE	Enhanced Data rates for Global Evolution of GSM and IS-136
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 Identification
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
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 LTD
Address: 3rd Floor, Building F, Kehui Park, No.95 Daguan Road, Guangzhou, China 510660
Tel: 86-20-29019902
Email: info@robustel.com