robustel | User Guide

R2011

Industrial Cellular Router

5 Eth + 2 SIM

robustOS

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

About This Document

This document provides hardware and software information of the Robustel R2011 Router, including introduction, installation, configuration and operation.

Trademarks and Permissions

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

Disclaimer

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

Technical Support

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

Important Notice

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

Safety Precautions

General

- The router generates radio frequency (RF) power. When using the router, care must be taken on safety issues related to RF interference as well as regulations of RF equipment.
- Do not use your router in aircraft, hospitals, petrol stations or in places where using cellular products is prohibited.
- Be sure that the router will not be interfering with nearby equipment. For example: pacemakers or medical equipment. The antenna of the router should be away from computers, office equipment, home appliance, etc.
- An external antenna must be connected to the router for proper operation. Only uses approved antenna with the router. Please contact authorized distributor on finding an approved antenna.
- Always keep the antenna with minimum safety distance of 20 cm or more from human body. Do not put the antenna inside metallic box, containers, etc.
- 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 local country before installing the router.
- The driver or operator of any vehicle should not operate the router while driving.
- Install the router by qualified personnel. Consult your vehicle distributor for any possible interference of electronic parts by the router.
- The router should be connected to the vehicle's supply system by using a fuse-protected terminal in the vehicle's fuse box.
- Be careful when the router is powered by the vehicle's main battery. The battery may be drained after extended period.

Protecting Your Router

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

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

Regulatory and Type Approval Information

Table 1: Directives

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

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

Name of the Part	Hazardous Substances									
	(Pb)	(Hg)	(Cd)	(Cr(VI))	(PBB)	(PBDE)	(DEHP)	(BBP)	(DBP)	(DIBP)
Metal parts	o	o	o	o	-	-	-	-	-	-
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	Descriptions
June 25, 2021		v.1.0.0	Initial release
December 25, 2021		v.1.0.1	1. Revised the company name 2. Revised *Regulatory and Type Approval Information* 3. Revised *Disclaimer*

Contents

Chapter 1 Product Overview

1.1 Key Features

The Robustel R2011 Industrial Cellular Router is a rugged, versatile 4G router with 5 Ethernet ports, dual SIM single standby capability and a range of advanced functions for mission critical IoT or M2M applications. The R2011 runs on Robustel's own Linux based Operating System, RobustOS. Developed entirely in-house, this gives way to a very high standard of technical support and high reliability. Robustel offers a Software Development Kit (SDK) to allow additional customization by using C, C++. It also provides rich Apps to meet fragmented IoT market demands such as RobustVPN, Data-Guard, Smart Reboot, and Smart Roaming.

1.2 Package Contents

Before installing your R2011 Router, verify the kit contents as following.

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

- 1 x Robustel R2011 Industrial Cellular Router

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

- 1 or 2 x SMA-J cellular antenna (external)

- 2 x RP-SMA-J Wi-Fi antenna (external)

Optional Accessories (sold separately)

- Ethernet cable

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

- DIN rail mounting kit

- Wall mounting kit

1.3 Specifications

Cellular Interface

- Number of antennas: 2 (MAIN + AUX) or 1 (MAIN)
- Connector: SMA-K, standard
- SIM: 2 mini SIMs (2FF)

Ethernet Interface

- Number of ports: 2 x 10/100 ports, 5 x LAN or 4 x LAN + 1 x WAN
- Magnet isolation protection: 1.5 KV

Wi-Fi Interface

- Number of antennas: 2 (Wi-Fi1 + Wi-Fi2)
- Connector: RP-SMA-K
- Standards: 802.11 b/g/n, 2 x 2 MIMO, supporting AP and Client modes
- Frequency bands: 2.4 GHz
- Security: WEP, WPA, WPA2
- Encryption: 68/128 AES, TKIP
- Data speed: 300 Mbps

Others

- 1 x RST button
- LED indicators: 1 x RUN, 1 x MDM, 1 x Wi-Fi, 3 x RSSI
- Built-in: Watchdog, Timer

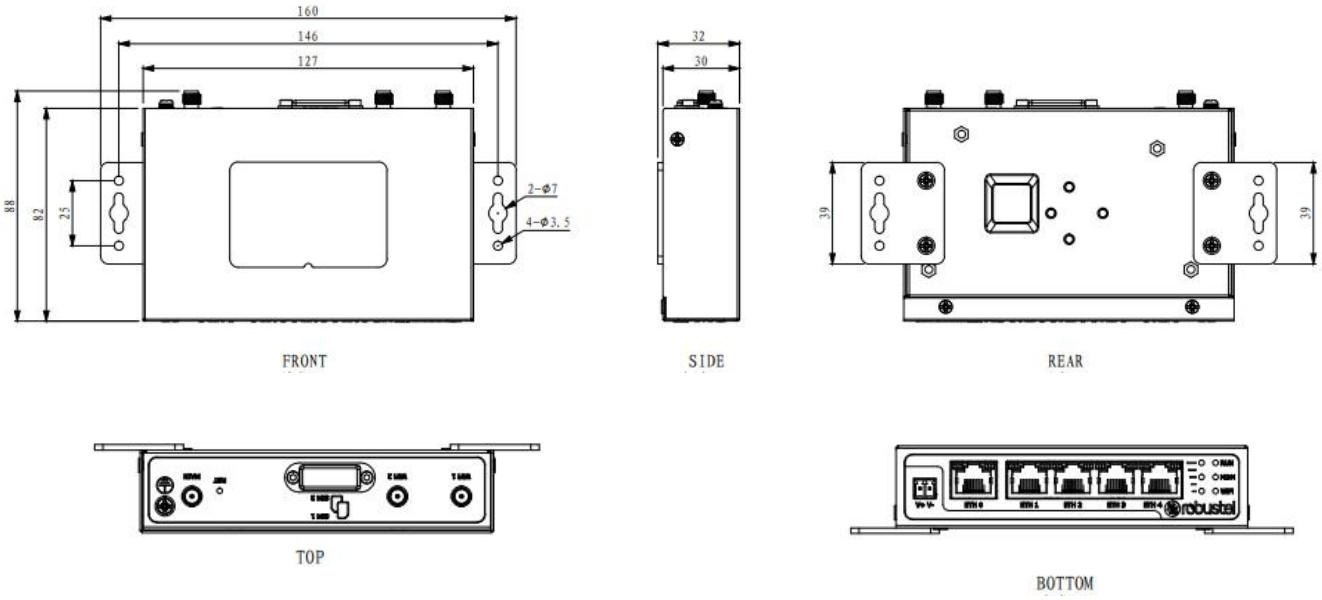
Power Supply and Consumption

- Connector: 2-pin 3.5 mm female socket
- Input voltage: 9 to 36 V DC
- Power consumption: Idle: 200 mA@12 V
  Data link: 580 mA (peak) @12 V

Physical Characteristics

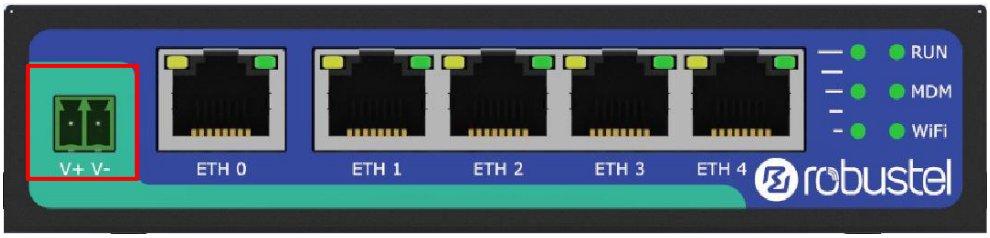
- Ingress protection: IP30
- Housing & Weight: Metal, 350 g
- Dimensions: 127 x 82 x 30 mm
- Installations: Desktop, wall mounting and DIN rail mounting (wall mounting kit and DIN rail mounting kit requires additional purchase.)
- Operation temperature: -40~+75 °C
- Storage temperature: -40~+85 °C
- Relative humidity: 5~95% RH

1.4 Dimensions



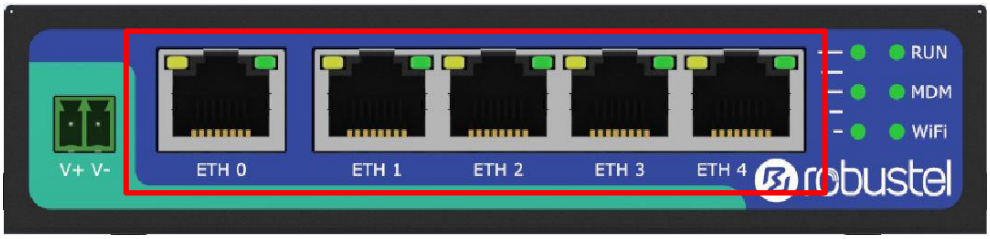
Chapter 2 Hardware Installation

2.1 PIN Assignment



PIN	Descriptions	Notes
1	V+	Positive
2	V-	Negative

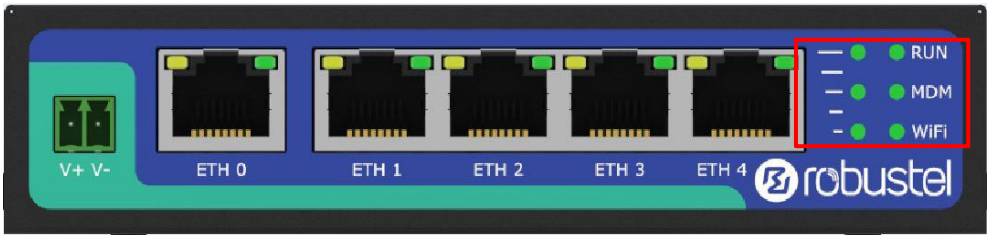
2.2 Ethernet Interface



There are five Ethernet ports on R2011 Gateway, including ETH0 (WAN/LAN) and ETH1, ETH2, ETH3, ETH4. Each has two LED indicators. The green one is a link indicator but the yellow one doesn't mean anything. For details about status, see the table below.

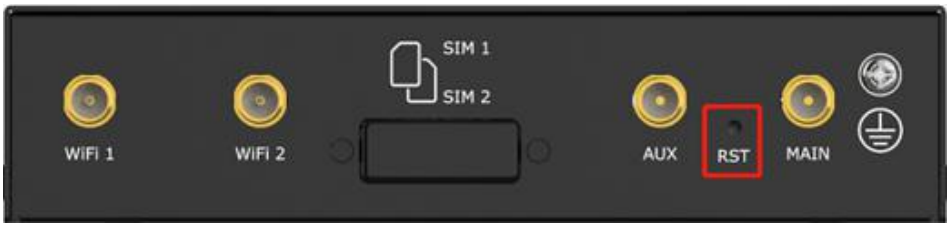
Indicator	Status	Description
Link indicator (Green)	On, solid	Connection is established
	On, blinking	Data is being transferred
	Off	Connection is not established

2.3 LED Indicators



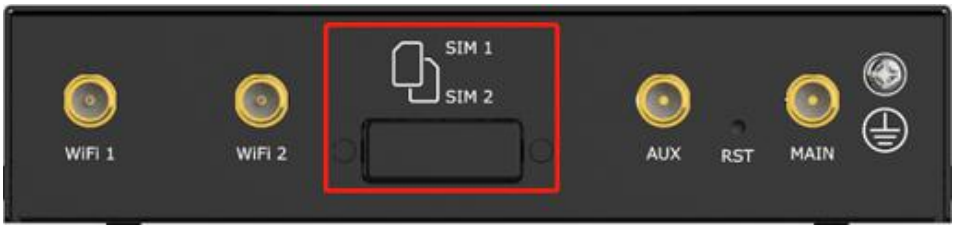
Name	Color	Status	Description
RUN	Green	On, solid	Router is powered on (System is initializing)
		On, blinking	Router starts operating
		Off	Router is powered off
MDM	Green	On, solid	Successful link connection
		On, blinking	Link connection is working
		Off	Link connection is not working
Wi-Fi	Green	On, solid	Wi-Fi is working normally
		Off	Wi-Fi is not working or abnormal
RSSI	Green	Three lights on	Cellular module: high signal (20~31 dB)
		Two lights on	Cellular module: medium signal (10~19 dB)
		One light on	Cellular module: low signal (1~9 dB)
		Off	Module initializing or no signal

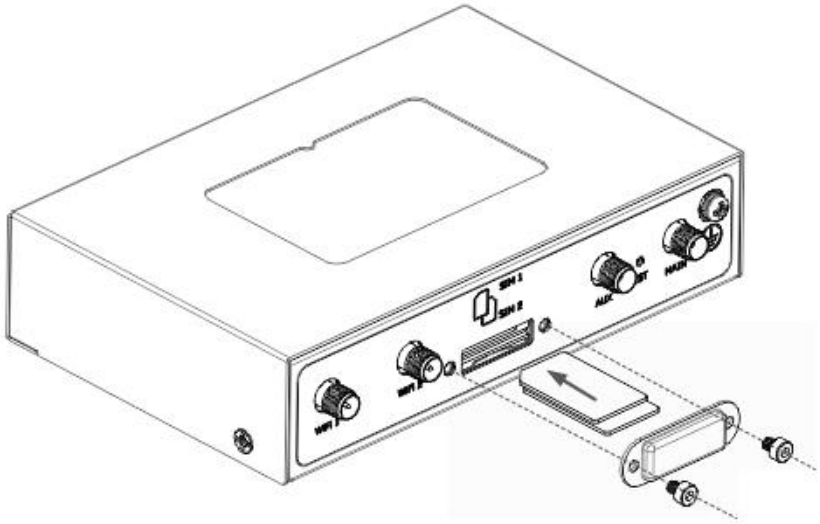
2.4 Reset Button



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 gateway, press and hold the RST button until all LEDs start blinking one by one, and release the button to return the gateway to factory defaults.

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

- **Remove SIM card**

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

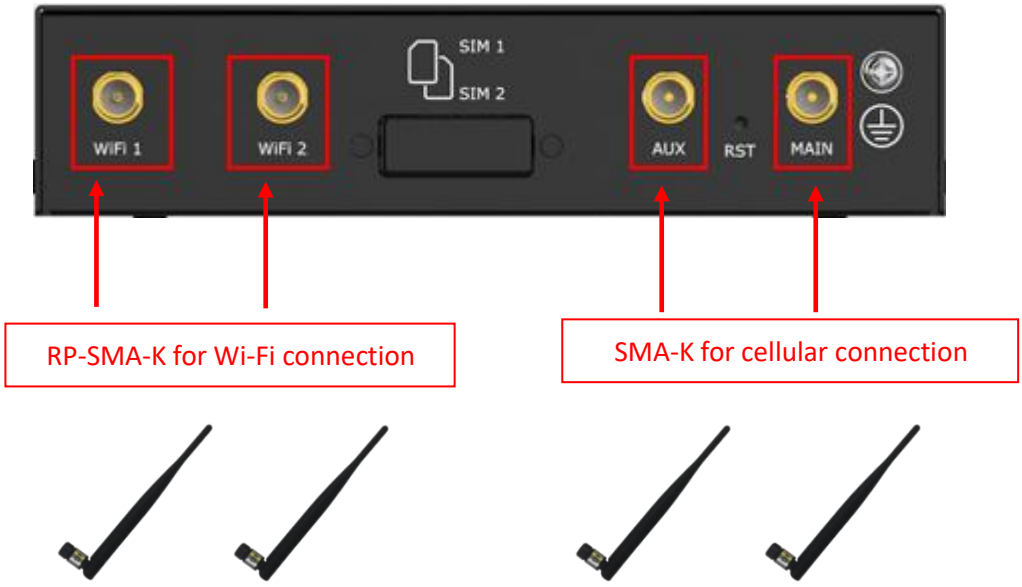
Note:

1. Use the specific M2M SIM card when the device is working in extreme temperature (temperature exceeding 40 °C), 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.

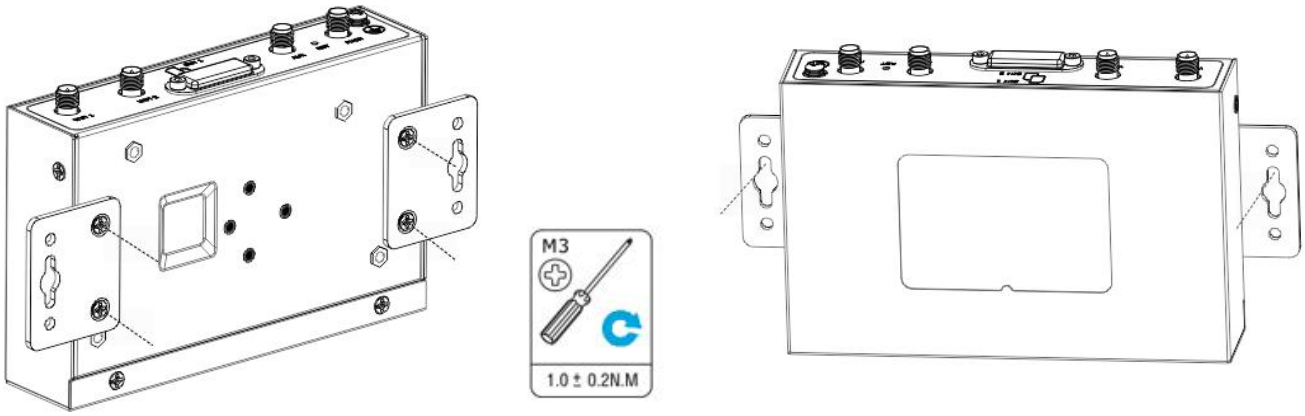


2.7 Mount the Router

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

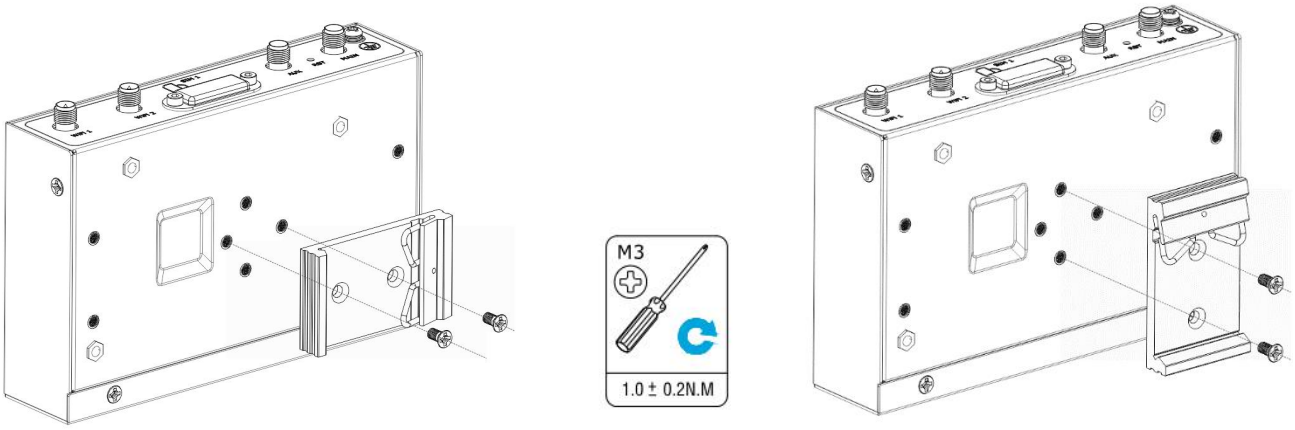
Two methods for mounting the router

- Wall mounting (measured in mm)



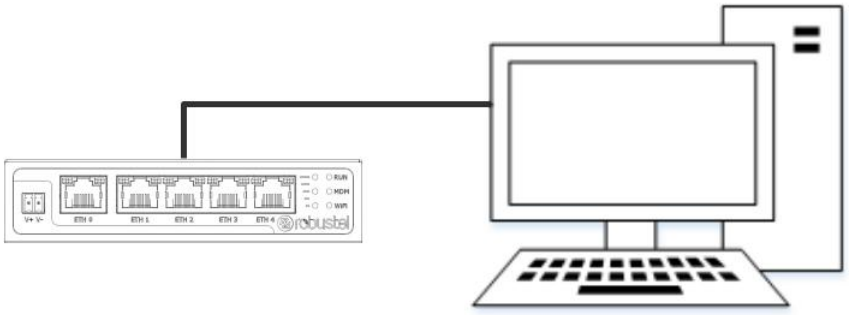
Use 4 pcs of M3 screws to fix the wall mounting kit to the router, and then use 2 pcs of M3 drywall screws to mount the router associated with the wall mounting kit on the wall.

- DIN rail mounting (measured in mm)



Use 2 pcs of M3 screws to fix the DIN rail to the router (as illustrations above shown, there are two mounting angles to choose from), and then hang the DIN rail on the mounting bracket.

2.8 Connect R2011 to a Computer

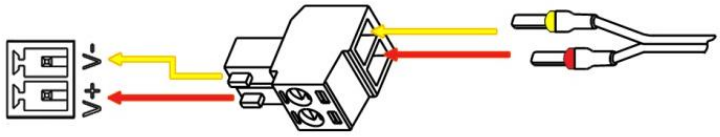


Connect the router's Ethernet port (ETH0~ETH4) to a PC with a standard Ethernet cable.

2.9 Power Supply

Power wiring diagram

Color	Descriptions
Red	+ Positive
Yellow	- Negative



The R2011 supports reverse polarity protection, but always refers to the illustration 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. The last step is to plug the power adapter into your socket.
Note: The range of power voltage is 9 to 36 V DC.

Chapter 3 Initial Configuration

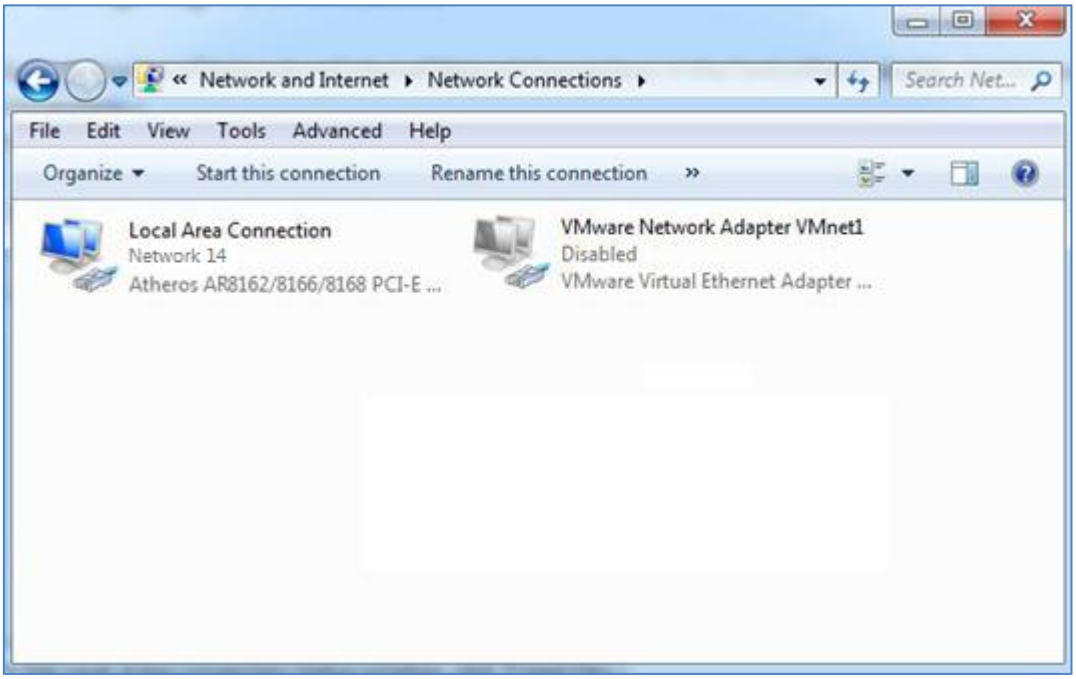
The router can be configured through your web browser that including IE 8.0 or above, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. It provides an easy and user-friendly interface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

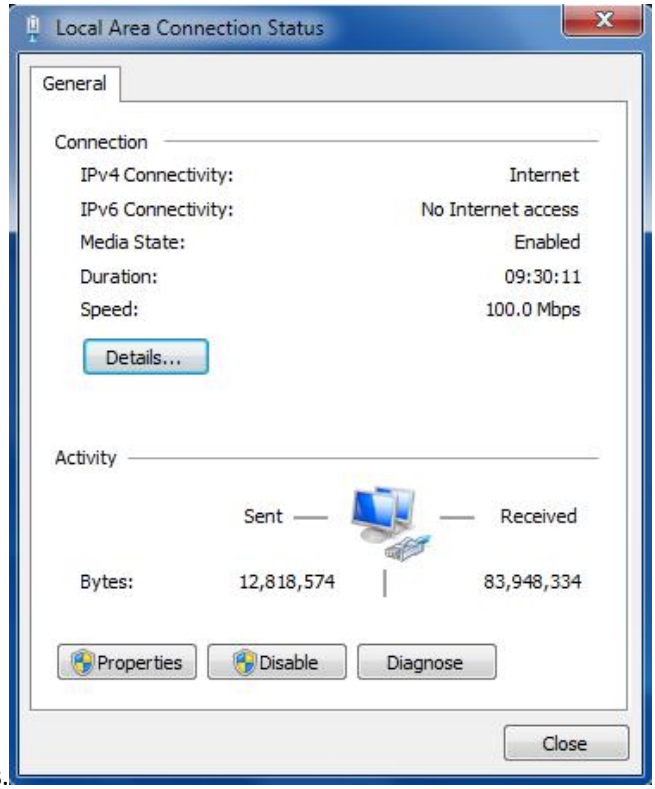
There are two methods to get IP address for the PC. One is to obtain an IP address automatically from "Local Area Connection", and another is to configure a static IP address manually within the same subnet of the router. Please refer to the steps below.

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

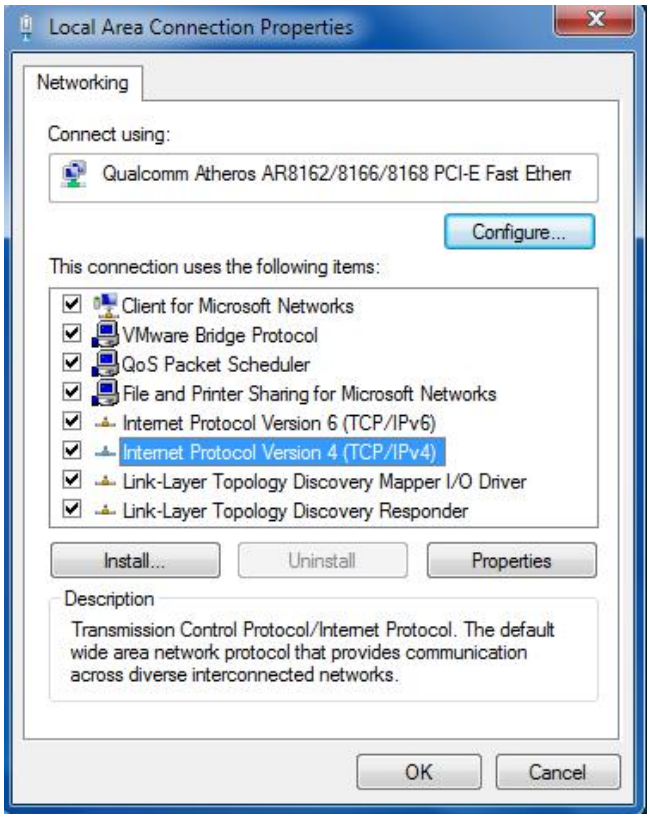
1. Click **"Start > Control panel"**, double-click **Network and Sharing Center**, and then double-click **Local Area Connection**.



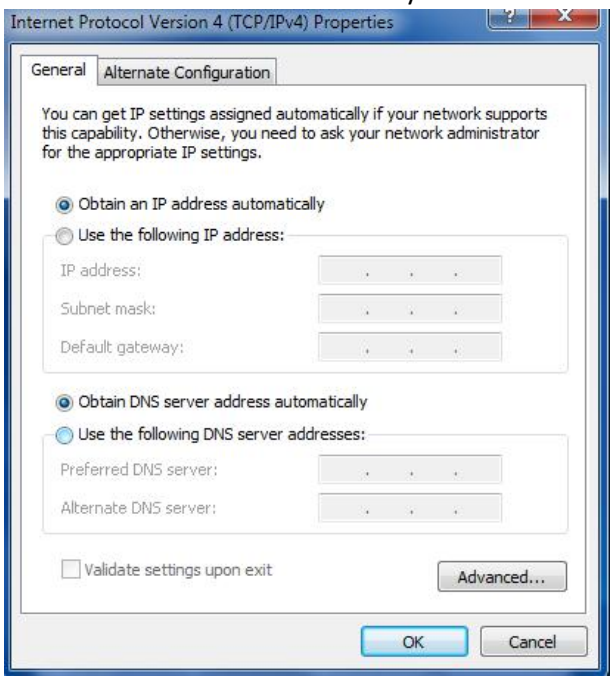
2. Click **Properties** in the window of **Local Area Connection Status**.



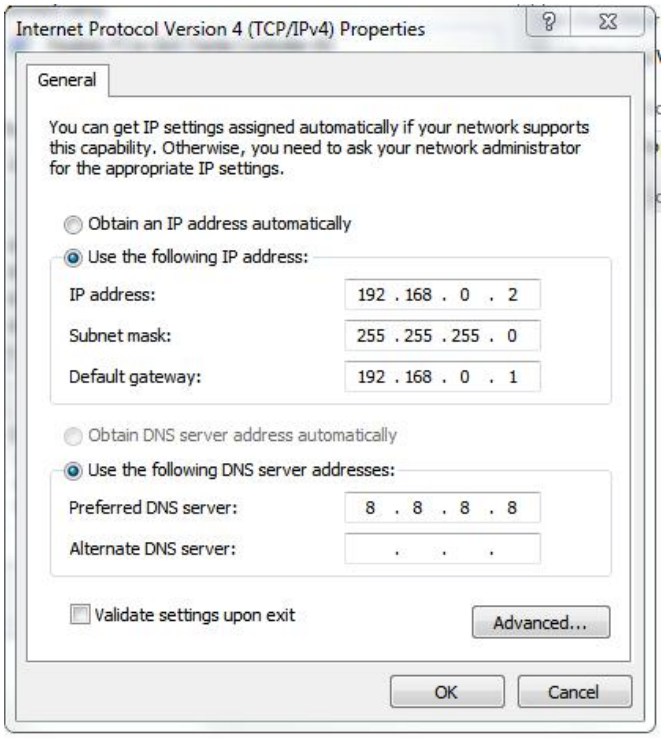
3. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



4. Two ways for configuring the IP address of PC.
   Obtain an IP address automatically from the DHCP server, click "**Obtain an IP address automatically**";



   Manually configure the PC with a static IP address on the same subnet as the router address, click and configure "**Use the following IP address**";



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

3.2 Factory Default Settings

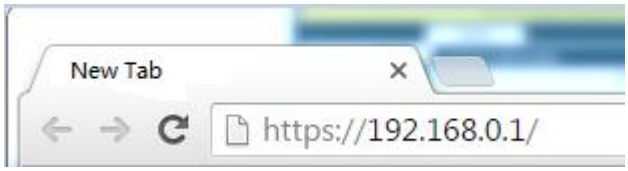
Before configuring your router, you need to know the following default settings.

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
ETH2	192.168.0.1/255.255.255.0, LAN mode
ETH3	192.168.0.1/255.255.255.0, LAN mode
ETH4	192.168.0.1/255.255.255.0, LAN mode
DHCP Server	Enabled

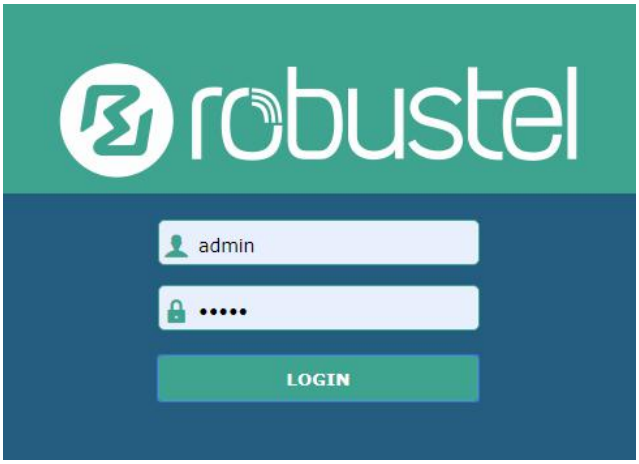
3.3 Log in the Router

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

1. On your PC, open a web browser such as Internet Explorer, Google or Firebox, etc.
2. From your web browser, type the IP address of the router into the address bar and press enter. The default IP address of the router is http://192.168.0.1/, though the actual address may vary.
   Note: If a SIM card with a public IP address is inserted in the router, enter this corresponding public IP address in the browser's address bar to access the router wirelessly.

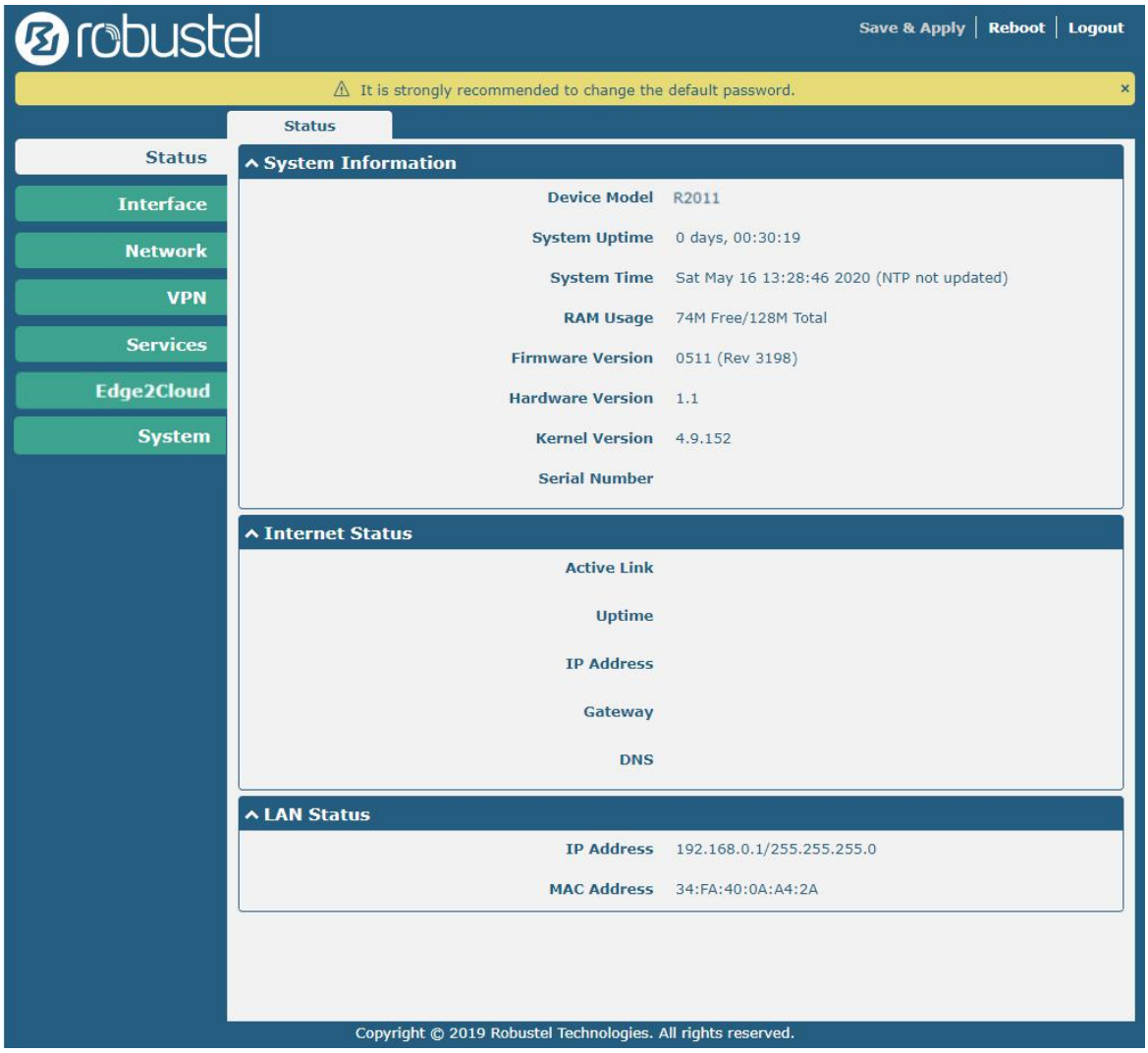


3. In the login page, enter the username and password, choose language and then click **LOGIN**. The default username and password are "admin".
   Note: If enter the wrong username or password over 6 times, the login web will be locked for 5 minutes.



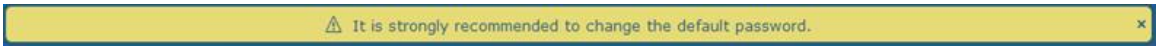
3.4 Control Panel

After logging in, the home page of the R2011 Router's web interface is displayed, for example.



From the homepage, users can perform operations such as saving the configuration, restarting the router, and logging out.

Using the original user name 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 × button to close the popup. To change your username and/or password, see **4.6.6 System > User Management**.

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

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

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

Chapter 4 Router Configuration

4.1 Status

4.1.1 System Information

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

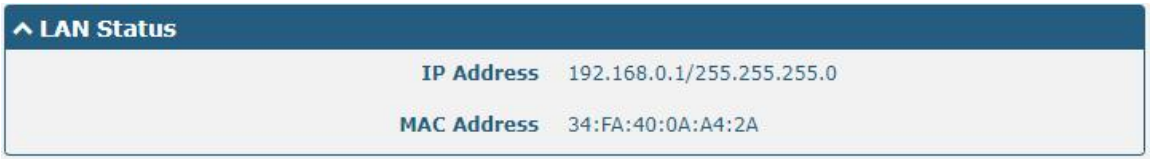
4.1.2 Internet Status

This page shows the router's Internet status information.

Internet Status	
Item	**Description**
Uptime	Show the current amount of time the link has been connected.
Active Link	Show the currently online link: WWAN1, WWAN2, or WAN.
IP Address	Show the address of current link.
Router	Show the router address of the current link.
DNS	Show the current DNS server.

4.1.3 LAN Status

This page shows the routers' LAN status

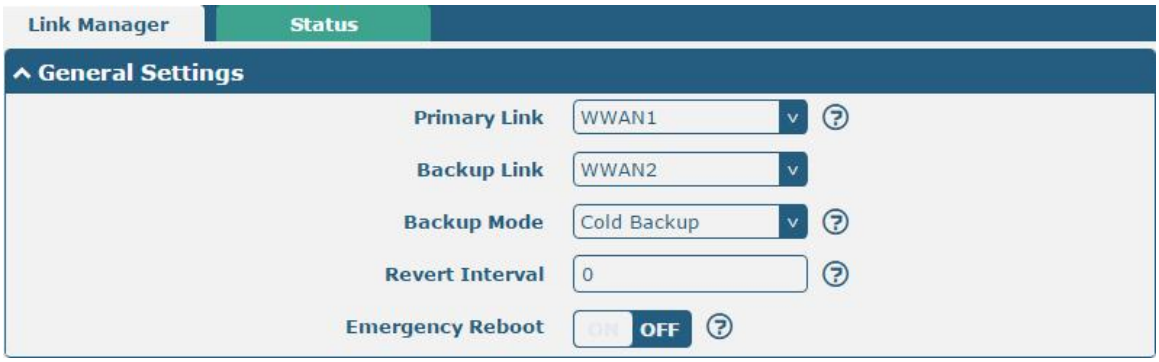


LAN Status	
Item	**Description**
IP Address	Show the IP address and the Netmask of the router.
MAC Address	Show the MAC address of the router.

4.2 Interface

4.2.1 Link Manager

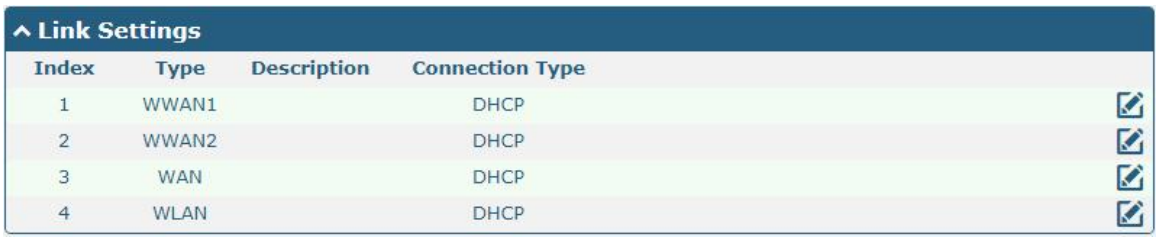
Users can manage link connections in this section. Link Manager is a link backup feature that provides mobile network and Ethernet link backup.



General Settings @ Link Manager		
Item	**Description**	**Default**
Primary Link	Select from “WWAN1”, “WWAN2”, “WAN” or “WLAN”. • WWAN1: Select to make SIM1 as the primary wireless link • WWAN2: Select to make SIM2 as the primary wireless link • WAN: Select to make WAN Ethernet port as the primary wired link • WLAN: Select to make WLAN as the primary wireless link **Note:** WLAN link is available only if enable Wi-Fi as Client mode, please refer to **4.2.5 Wi-Fi**.	WWAN1
Backup Link	Select from “WWAN1”, “WWAN2”, “WAN”, “WLAN” or “None”. • WWAN1: Select to make SIM1 as backup wireless link • WWAN2: Select to make SIM2 as backup wireless link • WAN: Select to make WAN Ethernet port as the primary wired link • WLAN: Select to make WLAN as the primary wireless link **Note:** WLAN link is available only if enable Wi-Fi as Client mode, please refer to **4.2.5 Wi-Fi**. • 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 • 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.

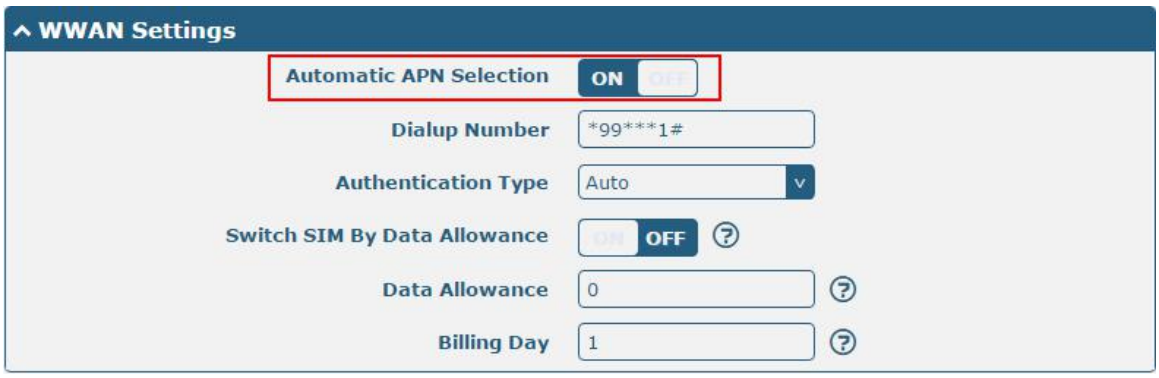
Link Settings allows you to configure the parameters of link connection, including WWAN1/WWAN2, WAN and WLAN. It is recommended to enable Ping detection to keep the router always online. The Ping detection increases the reliability and also saves the data traffic.



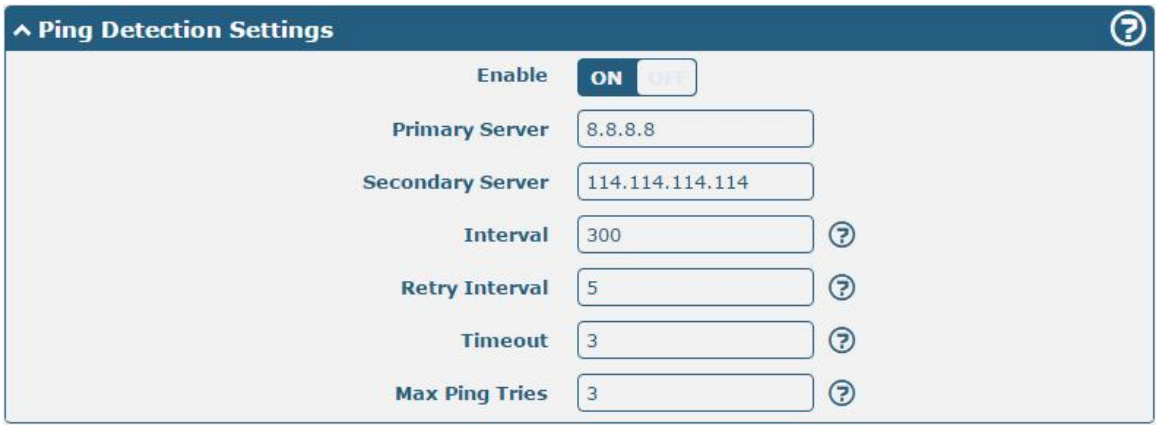
Click on the right-most of WWAN1/WWAN2 to enter the configuration window.

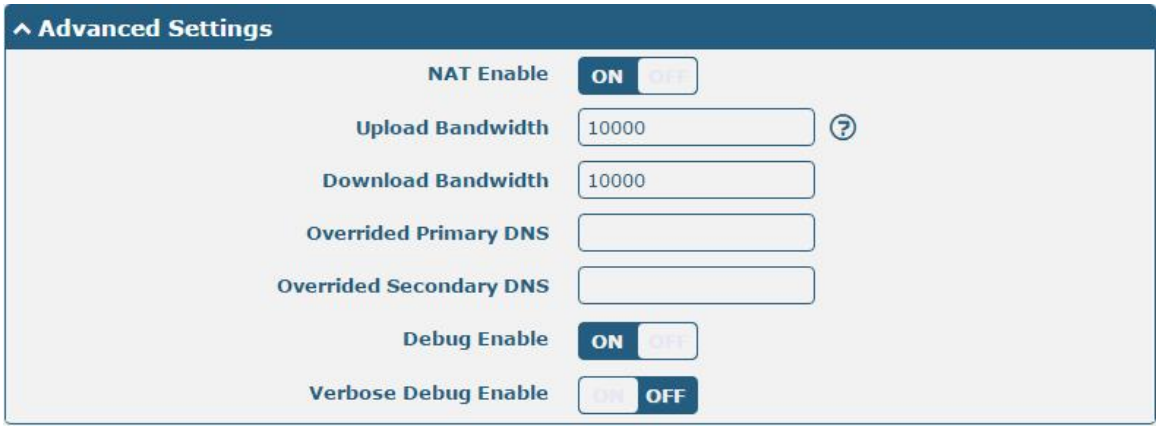
WWAN1/WWAN2

The window is displayed as below when enabling the "**Automatic APN Selection**" option



The window is displayed as below when disabling the "**Automatic APN Selection**" option.





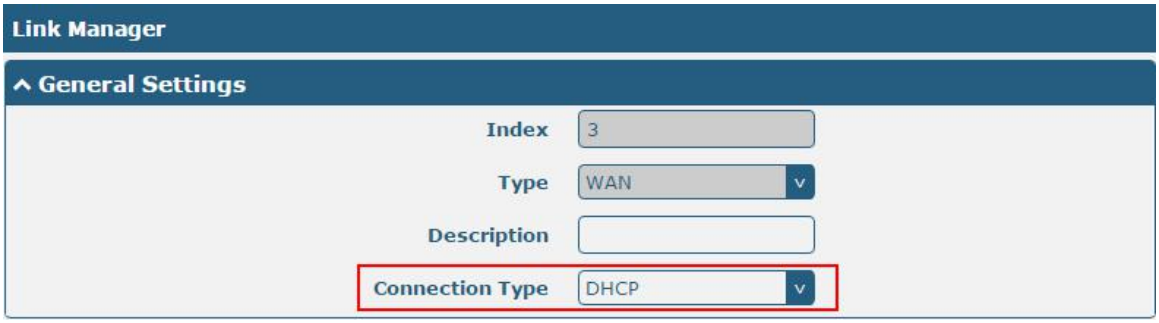
Link Settings (WWAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WWAN1
Description	Enter a description for this link.	Null

Link Settings (WWAN)		
Item	**Description**	**Default**
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
PPP Preferred	The PPP dial-up method is preferred.	OFF
Switch SIM By Data Allowance	Click the toggle button to enable/disable this option. After enabling, it will switch to another SIM when the data limit reached. **Note**: Only used for dual-SIM backup.	OFF
Data Allowance	Set the monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will be displayed in **Interface > Link Manager > Status > WWAN Data Usage Statistics**. 0 means disable data traffic record.	0
Billing Day	Specify the monthly billing day. The data traffic statistics will be recalculated from that day.	1
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
Primary Server	Router will ping this primary address/domain name to check that if the current IPv4 connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check that if the current IPv4 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
Specify Primary DNS	Defines the primary IPv4 DNS server used by the link.	Null
Specify Secondary DNS	Defines the secondary IPv4 DNS server used by the link.	Null

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

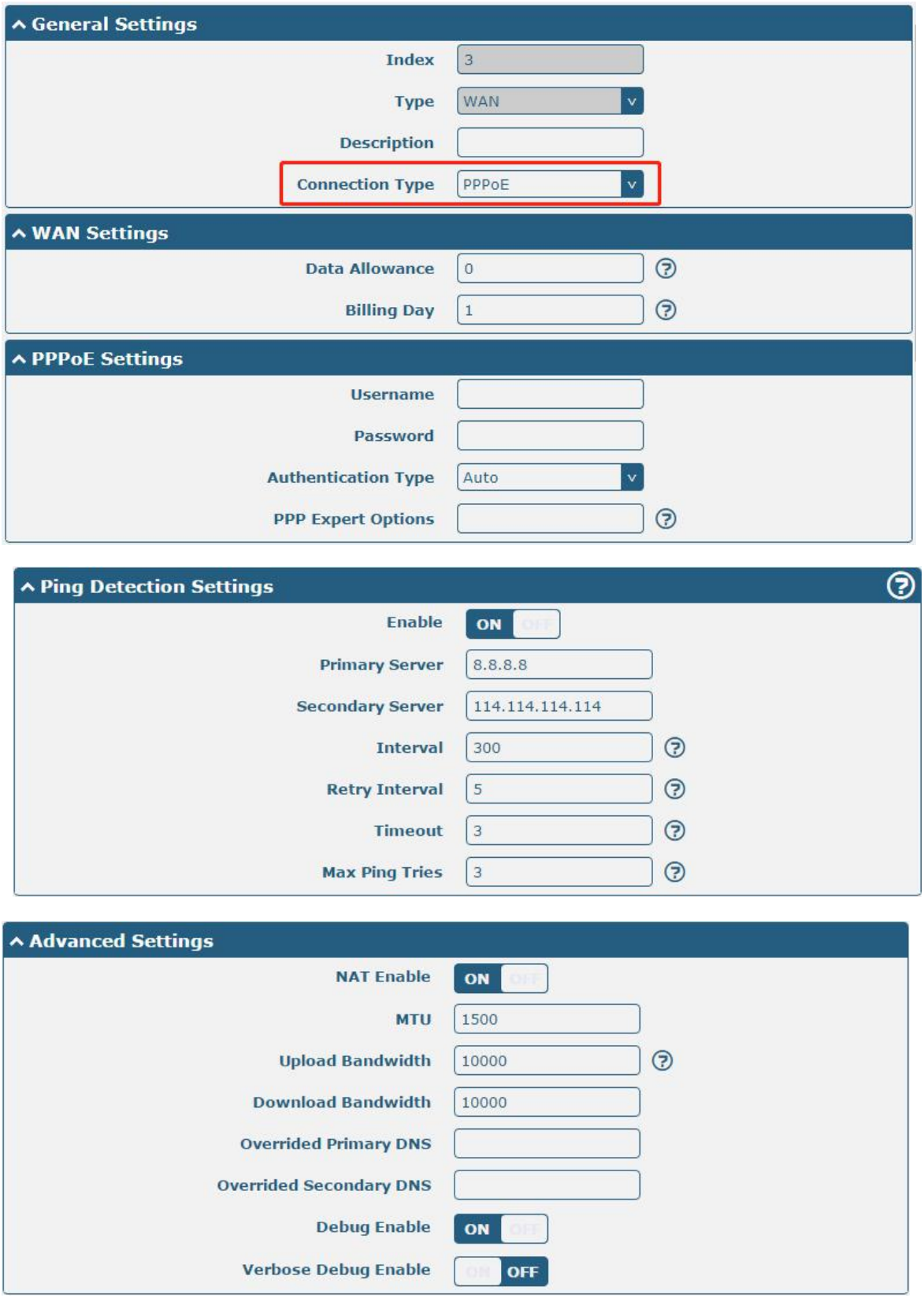
WAN

Router will obtain IP automatically from DHCP server if choosing **"DHCP"**.



The window is displayed as below when choosing "**Static**" as the **connection type**.

The window is displayed as below when choosing "**PPPoE**" as the **connection type**.

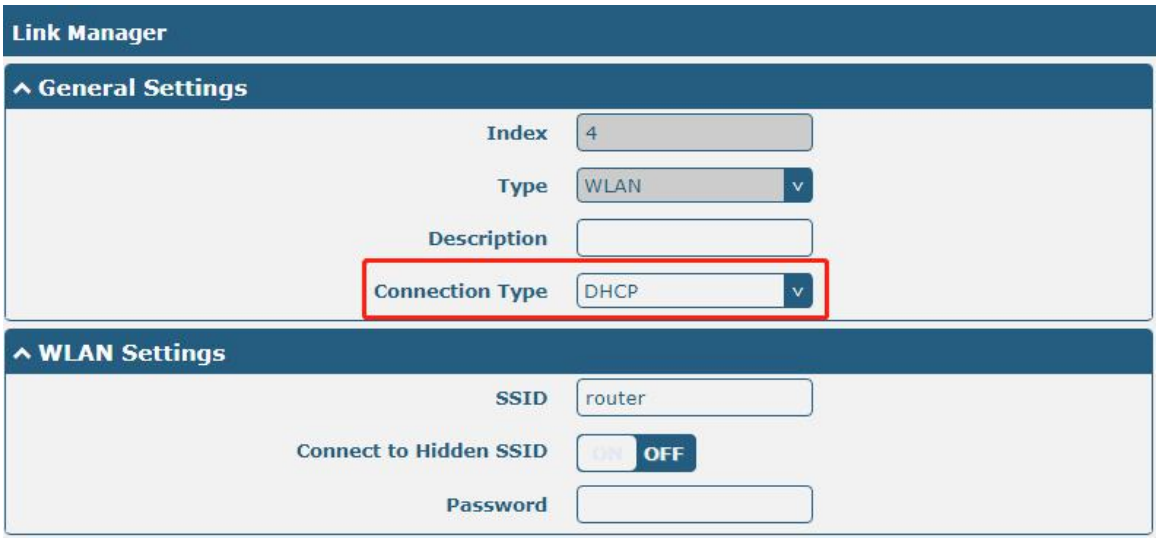


Link Settings (WAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WAN
Description	Enter a description for this link.	Null
Connection Type	Select from “DHCP”, “Static” or “PPPoE”.	DHCP
Static Address Settings		
IP Address	Set the IP address with Netmask which can access the Internet. IP address with Netmask, e.g. 192.168.1.1/24	Null
Router	Set the router 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
WAN Settings		
Data Allowance	Set the monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will be displayed in **Interface > Link Manager > Status > WWAN Data Usage Statistics**. 0 means disable data traffic record.	0
Billing Day	Specify the monthly billing day. The data traffic statistics will be recalculated from that day.	1
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.114.114
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advanced Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500

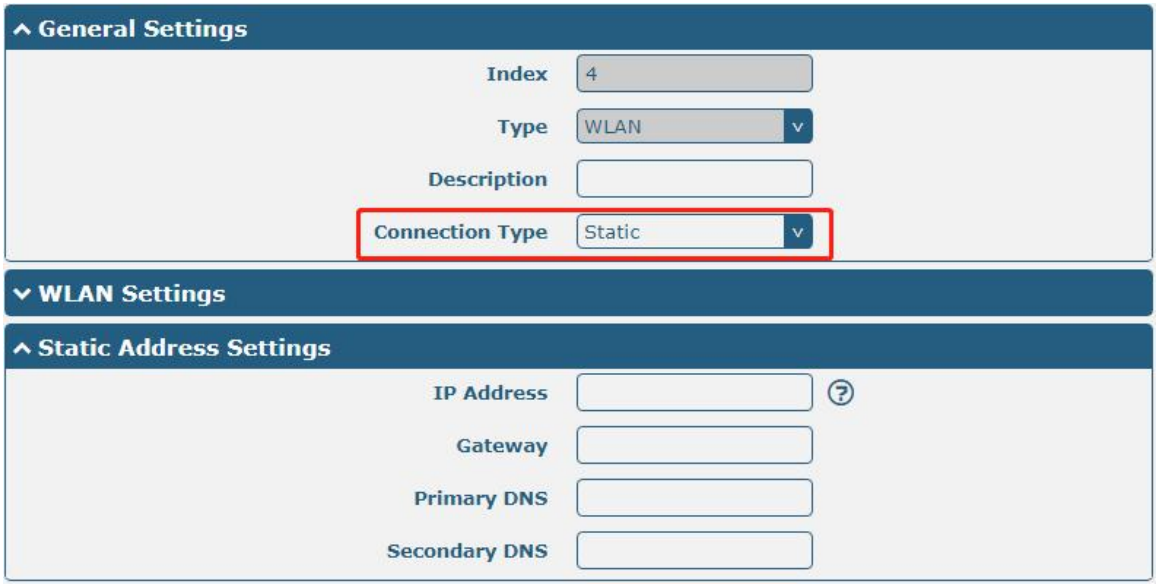
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Specify Primary DNS	Defines the primary IPv4 DNS server used by the link.	Null
Specify Secondary DNS	Defines the secondary IPv4 DNS server for the link.	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

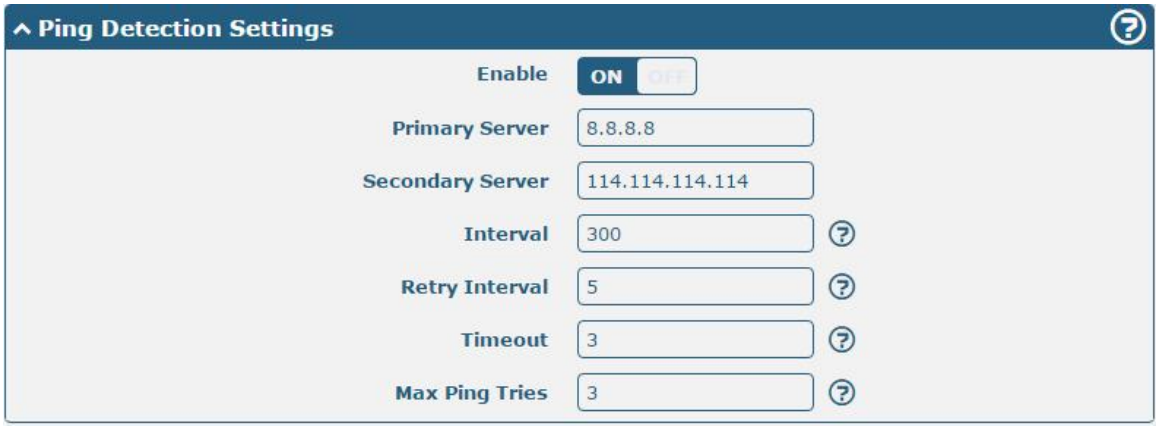
Router will obtain IP automatically from the WLAN AP if choosing “DHCP” as the connection type. The specific parameter configuration of SSID is shown as below.

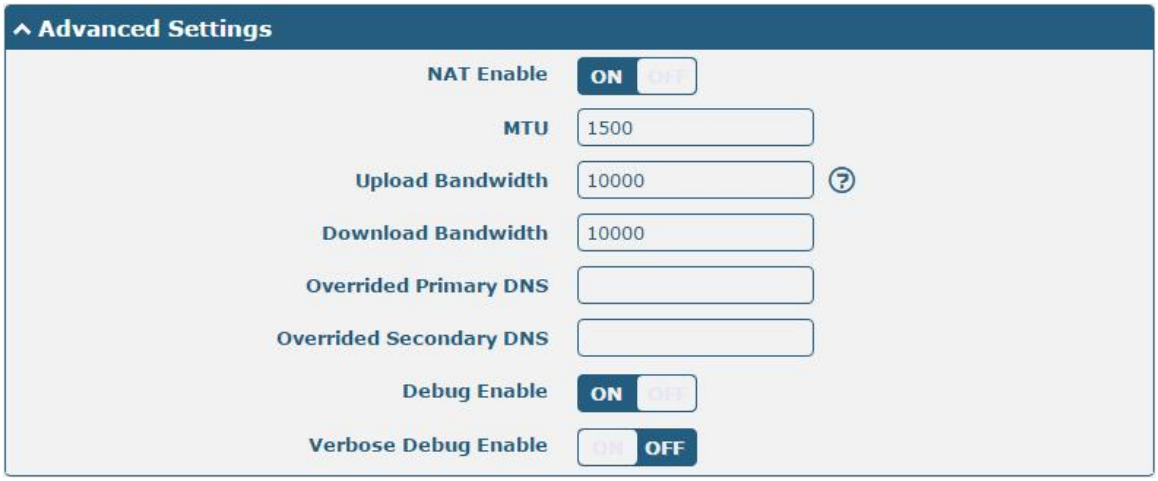


The window is displayed as below when choosing “Static” as the connection type.



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



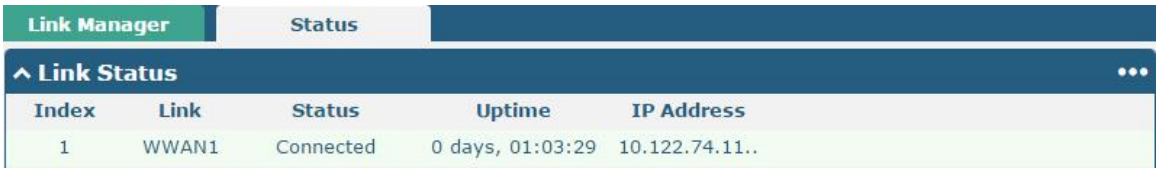


Link Settings (WLAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WLAN
Description	Enter a description for this link.	Null
Connection Type	Select from “DHCP” or “Static”.	DHCP

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
Router	Enter the IP address of Wi-Fi 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
Specify Primary DNS	Defines the primary DNS server used by the link.	Null
Specify Secondary DNS	Defines the secondary DNS server for the link.	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

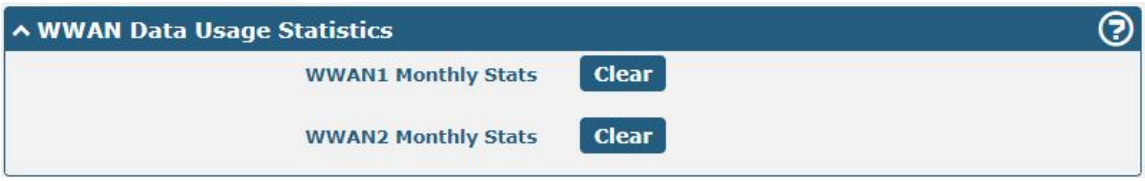
Status

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

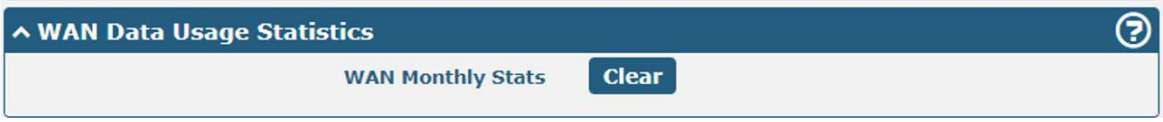


Click the right-most button ••• to select the connection status of the current link.

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**.

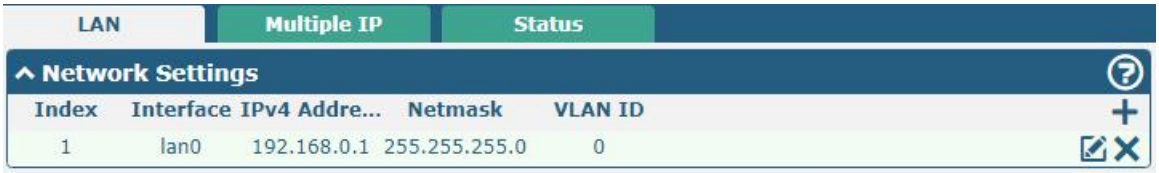


Click the Clear button to clear WAN monthly data traffic usage statistics. Data statistics will be displayed only if enable the Data Allowance function in **Interface > Link Manager > Link Settings > WAN Settings > Data Allowance**.

4.2.2 LAN

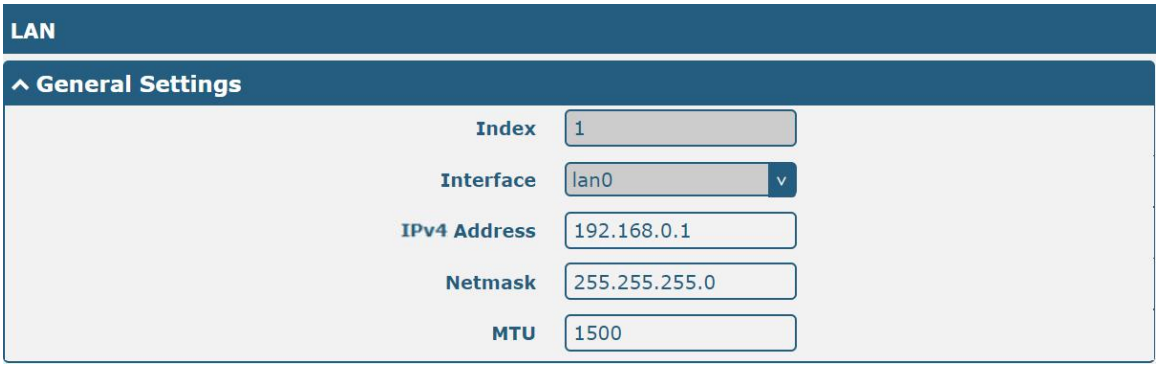
This section allows you to set the related parameters for LAN port. There are two LAN ports on R2011 Router, including ETH0 and ETH1. The ETH0 and ETH1 can freely choose from lan0 and lan1, but at least one LAN port must be assigned as lan0. The default settings of ETH0 and ETH1 are lan0 and their default IP are 192.168.0.1/255.255.255.0.

LAN



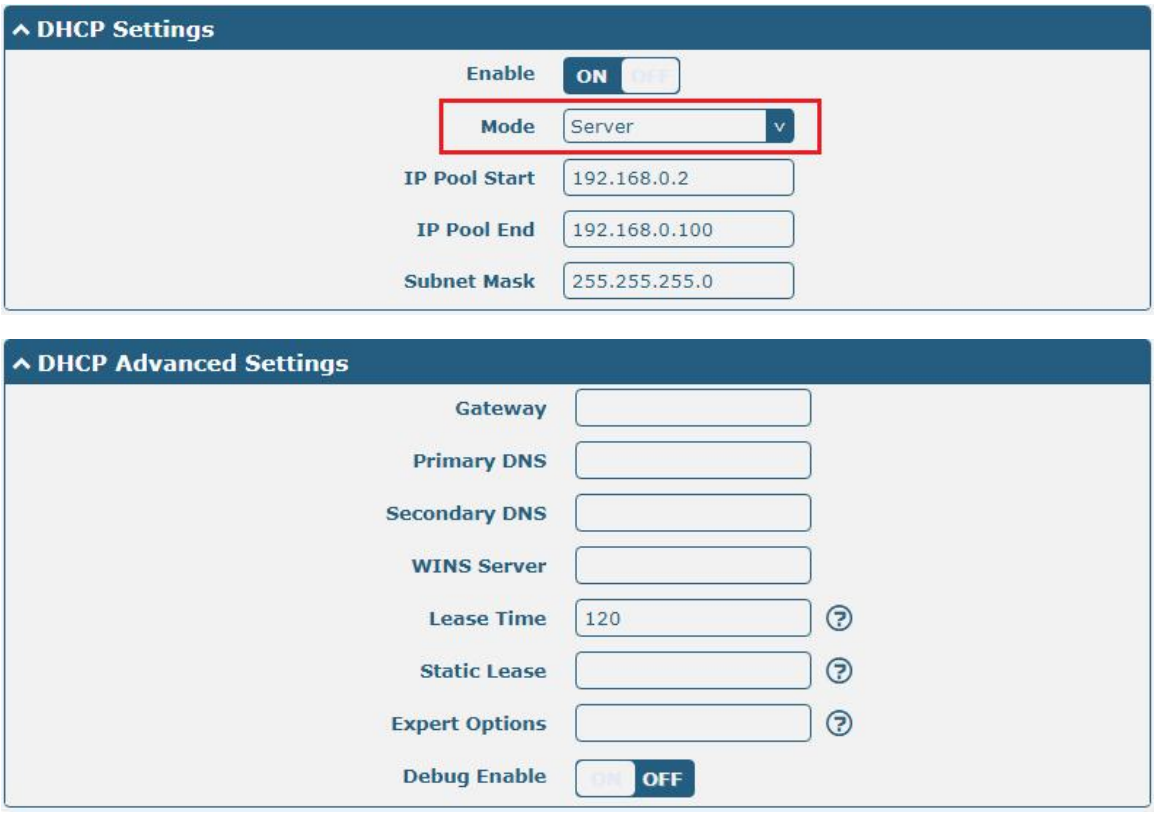
Note: Lan0 cannot be deleted.

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.

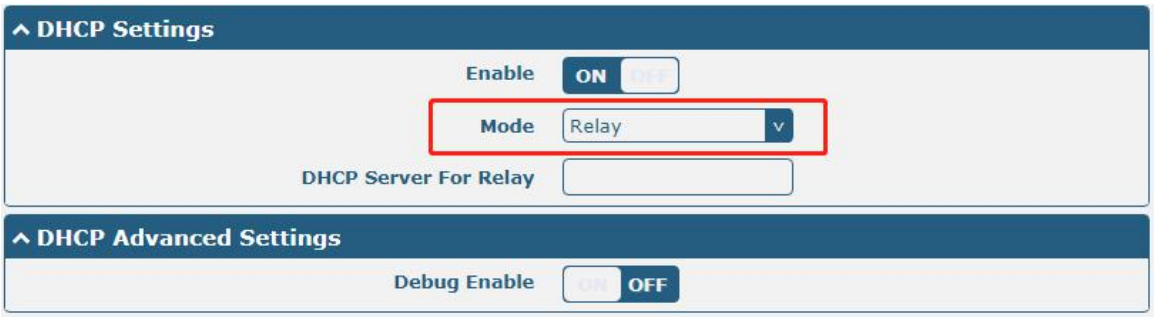


General Settings @ LAN		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Interface	Show the editing port. Lan1 is available only if it was selected by one of ETH0~ETH1 in **Ethernet > Ports > Port Settings**.	--
IPv4 Address	Set the IP address of the LAN port.	192.168.0.1
Netmask	Set the Netmask of the LAN port.	255.255.255.0
MTU	Enter the Maximum Transmission Unit.	1500

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



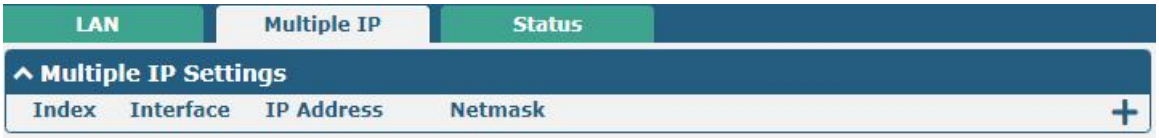
The window is displayed as below when choosing “Relay” as the mode.



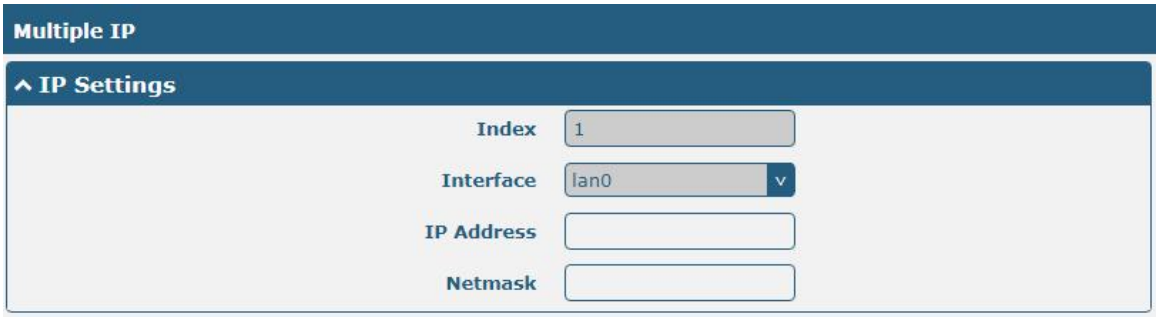
LAN		
Item	**Description**	**Default**
DHCP Settings		
Enable	Click the toggle button to enable/disable the DHCP function.	ON
Mode	Select from “Server” or “Relay”. • Server: Lease IP address to DHCP clients which have been connected to LAN port • Relay: Router can be a DHCP Relay, which will provide a relay tunnel to solve the problem that DHCP Client and DHCP Server are not in a same subnet	Server
IPv4 Pool Start	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.0.2

LAN		
Item	**Description**	**Default**
IPv4 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		
Router	Define the router assigned by the DHCP server to the clients, which must be on the same network segment with DHCP address pool.	Null
Primary DNS	Define the primary DNS server assigned by the DHCP server to the clients.	Null
Secondary DNS	Define the secondary DNS server assigned by the DHCP server to the clients.	Null
WINS Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever.	Null
Lease Time	Set the lease time which the client can use the IP address obtained from DHCP server, measured in seconds.	120
Static lease	Bind a lease to correspond an IP address via a MAC address. format: mac,ip;mac,ip;..., e.g. FF:ED:CB:A0:98:01,192.168.0.200	Null
Expert Options	Enter some other options of DHCP server in this field. format: config-desc;config-desc, e.g. log-dhcp;quiet-dhcp	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for DHCP information output.	OFF

Multiple IP



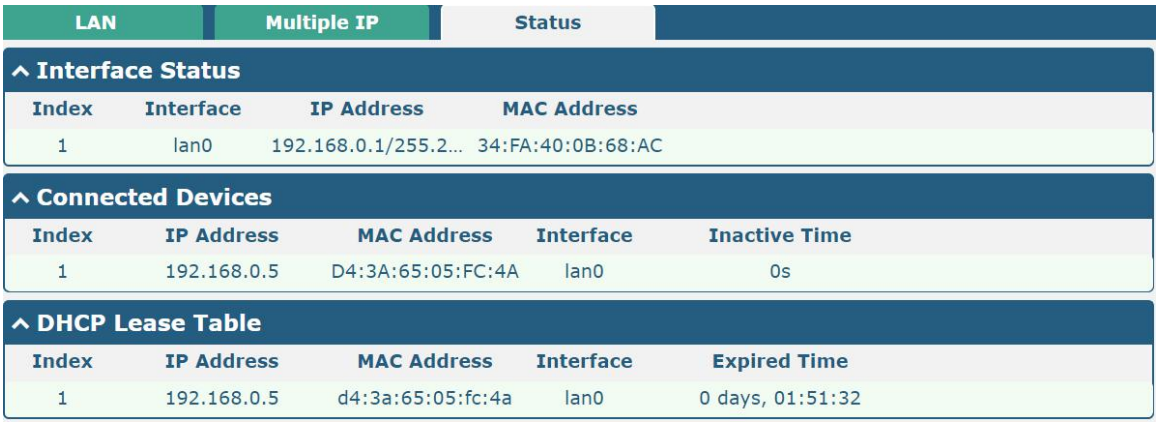
You may click + to add a multiple IP to the LAN port, or click ✕ to delete the multiple IP of the LAN port. Now, click to edit the multiple IP of the LAN port.



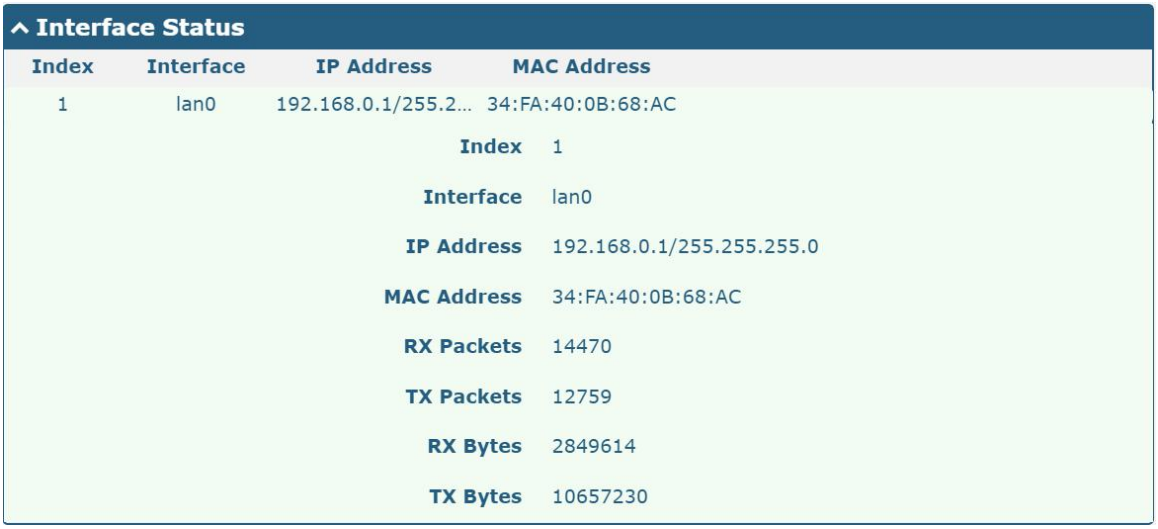
IP Settings		
Item	**Description**	**Default**
Index	Display the index list.	--
Interface	Show the editing port.	--
IP Address	Set the multiple IP address of the LAN port.	Null
Netmask	Set the multiple Netmask of the LAN port.	Null

Status

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

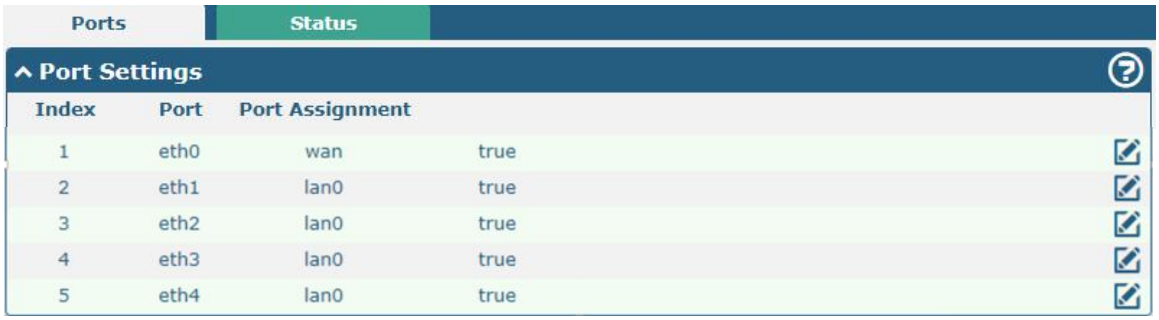


Click the row of status, the details status information will be displayed under the row.

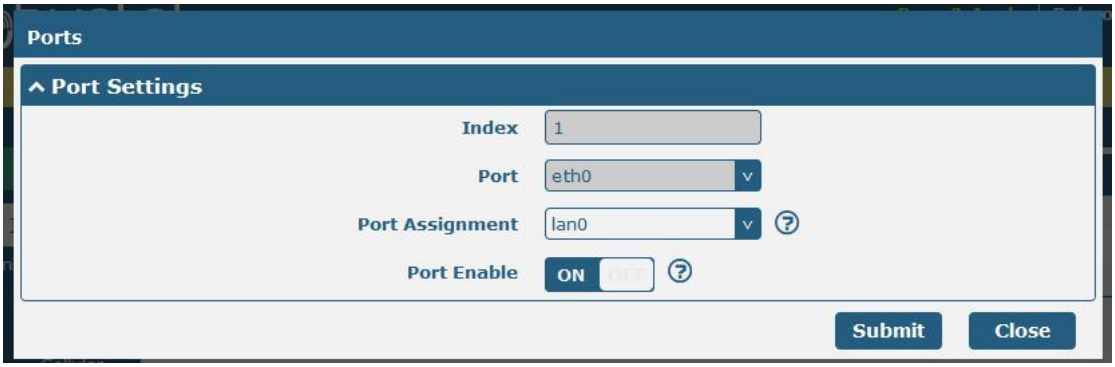


4.2.3 Ethernet

This section allows you to set the related parameters for Ethernet. There are five Ethernet ports on R2011 Router, including ETH0 and ETH1, ETH2, ETH3, and ETH4. The ETH0 on the router can be configured as either a WAN port or LAN port, also can be assigned as a PoE port, while ETH1 can only be configured as a LAN port. The default settings of ETH0, ETH1, ETH2, ETH3, and ETH4 are lan0 and their default IP are 192.168.0.1/255.255.255.0.

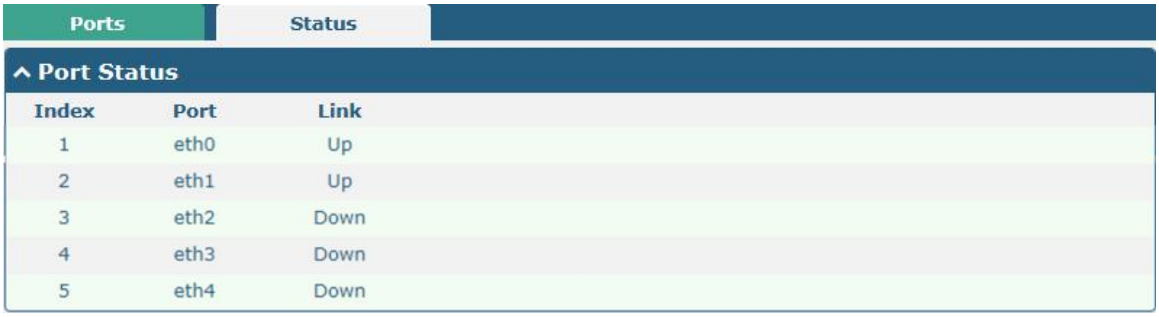


Click button of eth0 to configure its parameters, and modify the port assignment parameters of eth0 in the pop-up window.



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 LAN port. When setting the port as a LAN port, you can click the drop-down list to select from "lan0" or "lan1".	lan0
Port Enable	eth0: When the WAN switch to LAN, this function needs to reboot to take effect. eth1: Enable or disable the port	true

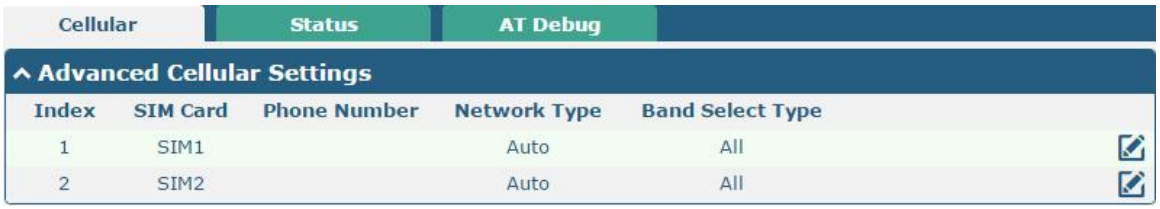
This page allows you to view the status of Ethernet port.



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

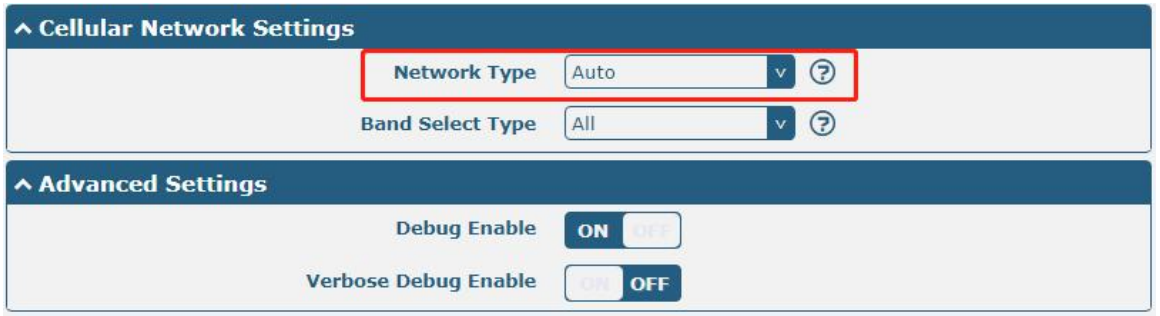
4.2.4 Cellular

This section allows you to set the related parameters of Cellular. The R2011 has 2 SIM card slots.

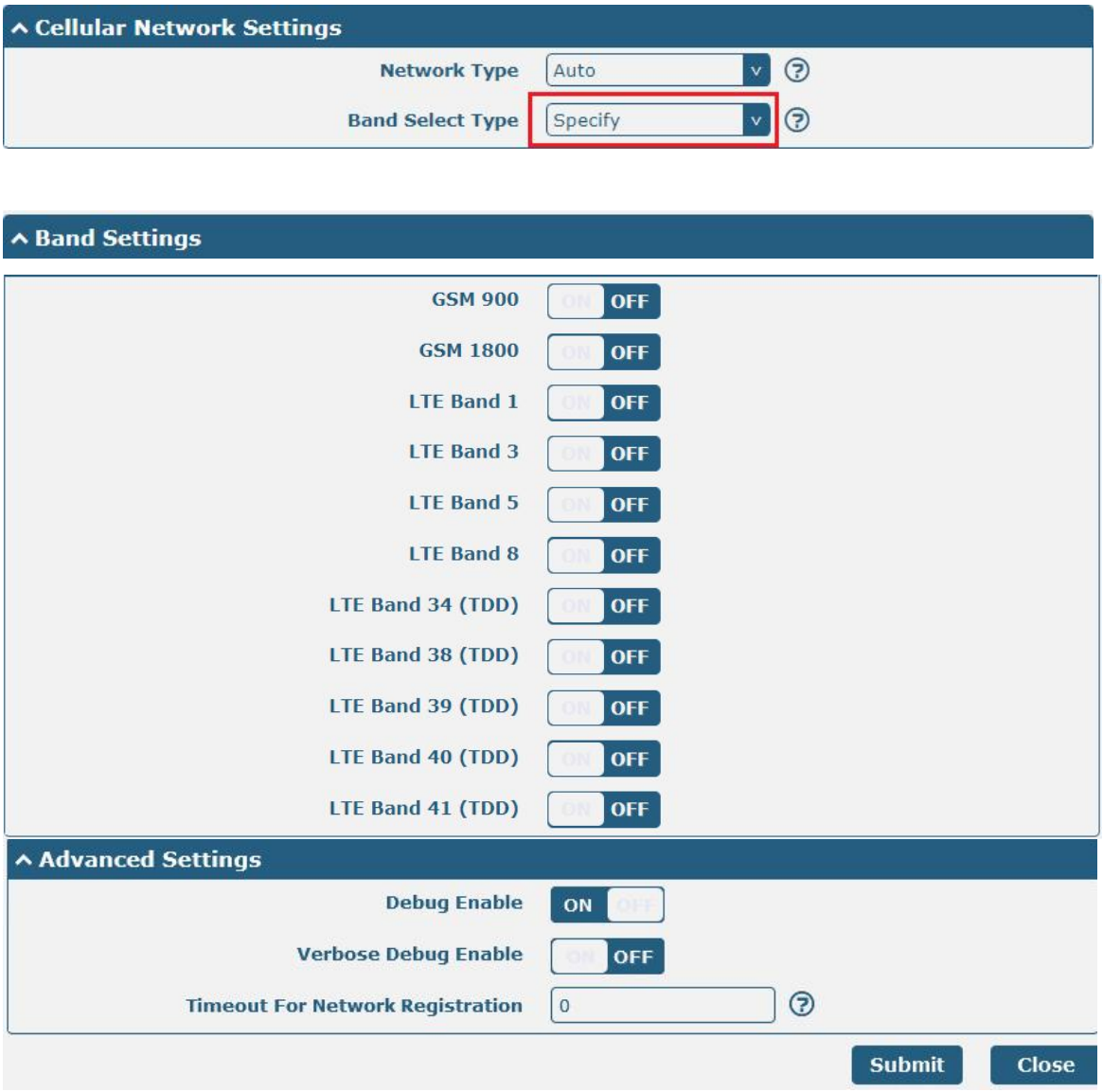


Click on the right-most of SIM 1 to edit the parameters.

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



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

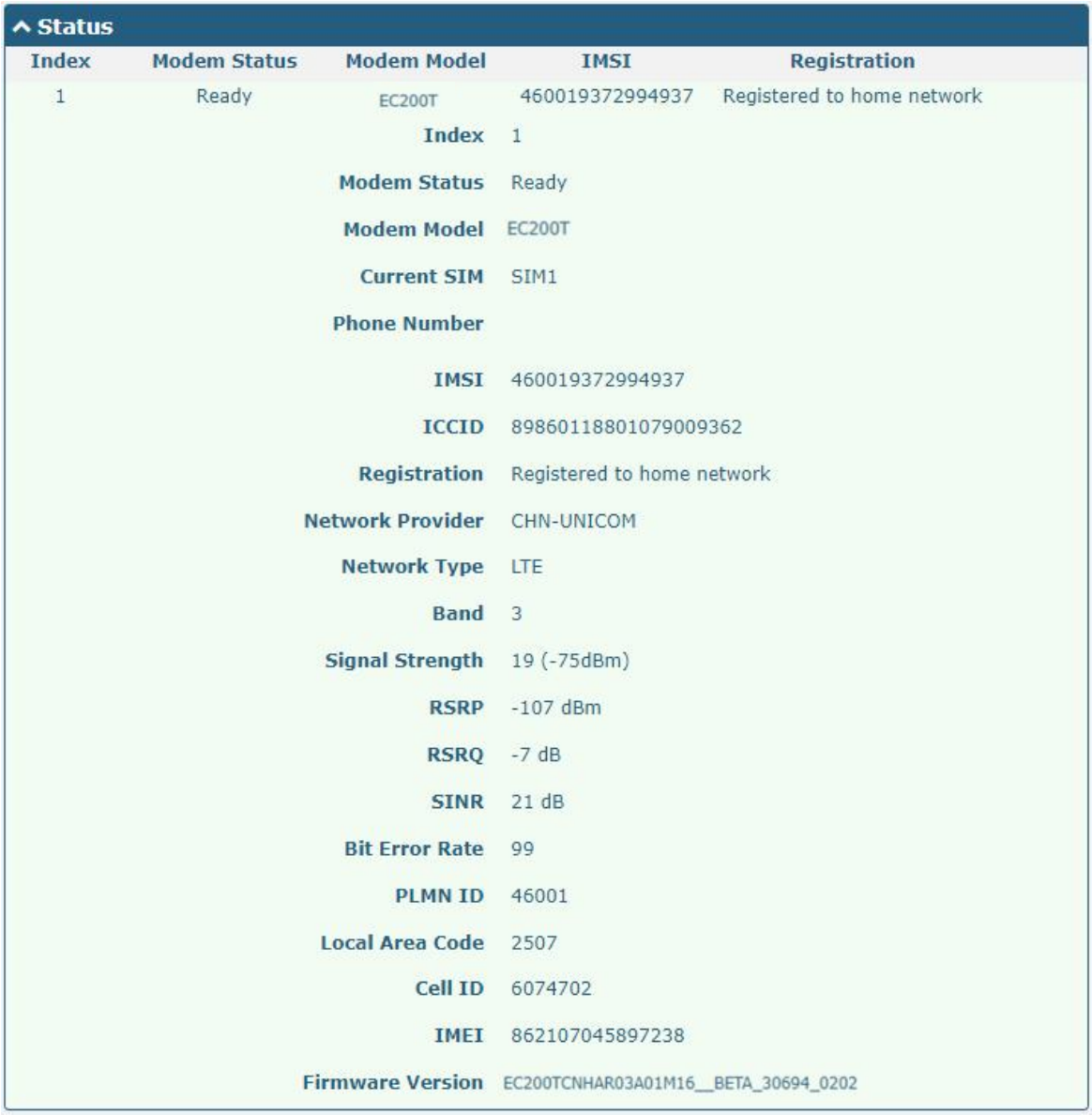


Cellular		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
SIM Card	Show the currently editing SIM card.	SIM1
Phone Number	Enter the phone number of the SIM card.	Null
PIN Code	Enter a 4-8 characters PIN code used for unlocking the SIM.	Null
Extra AT Cmd	Enter the AT commands used for cellular initialization.	Null
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet.	0
Cellular Network Settings		

Cellular		
Item	**Description**	**Default**
Network Type	Select the cellular network type, which is the network access order. 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
Timeout For Network Registration	The timeout required for the module to register to the network. Unit: seconds. 0 means the default setting is used.	0

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

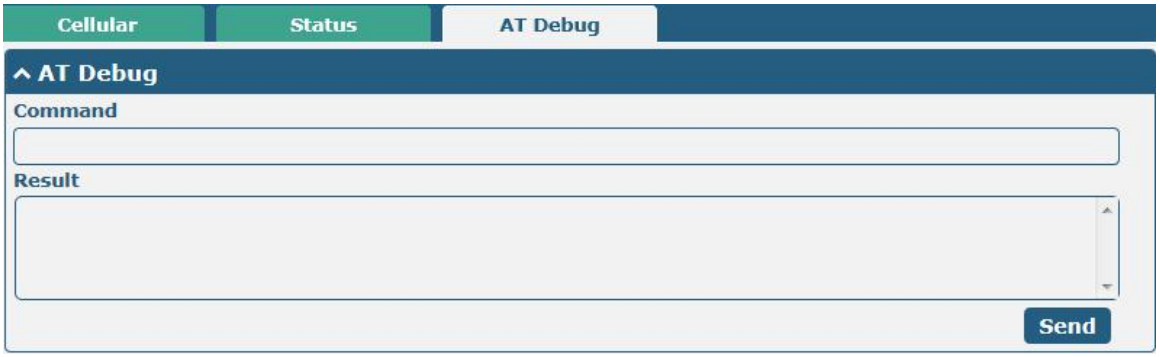
Click the row of status, the details status information will be displayed under the row.



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.

Status	
Item	**Description**
Signal Strength	Show the signal strength detected by the mobile.
RSRP	Show the current RSRP when you register to the 4G network.
RSRQ	Show the current RSRQ when you register to the 4G network.
SINR	Show the current SINR when you register to the 4G network.
Bit Error Rate	Show the current bit error rate.
PLMN ID	Show the current PLMN ID.
Local Area Code	Show the current local area code used for identifying different area.
Cell ID	Show the current cell ID used for locating the router.
IMEI	Show the IMEI (International Mobile Equipment Identity) number of the radio module.
Firmware Version	Show the current firmware version of the radio module.

This page allows you to check the AT Debug.



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

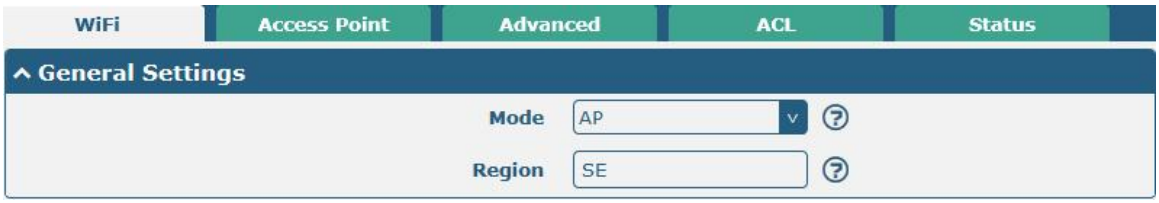
4.2.5 Wi-Fi

This section allows you to configure the parameters of two Wi-Fi modes. Router supports both Wi-Fi AP or Client modes, and default as AP.

Wi-Fi AP

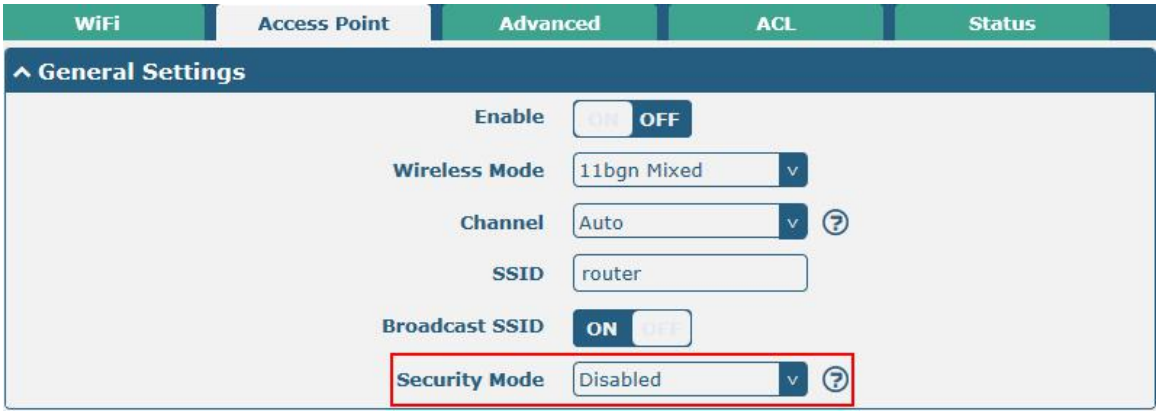
Configure Router as Wi-Fi AP

Click **"Interface > Wi-Fi > Wi-Fi"**, select "AP" as the mode and click "Submit".



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

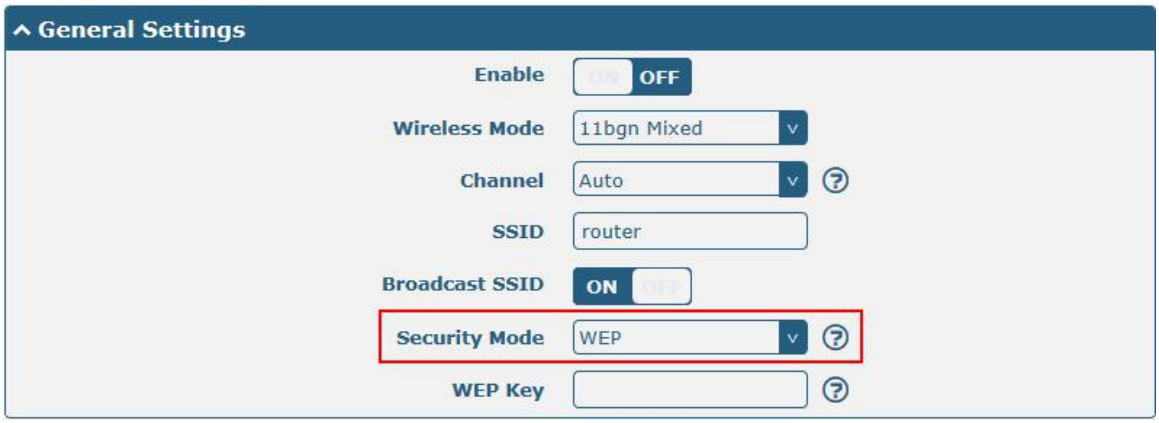
Click the Access Point column to configure the parameters of Wi-Fi AP. By default, the security mode is set as "Disabled".



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.

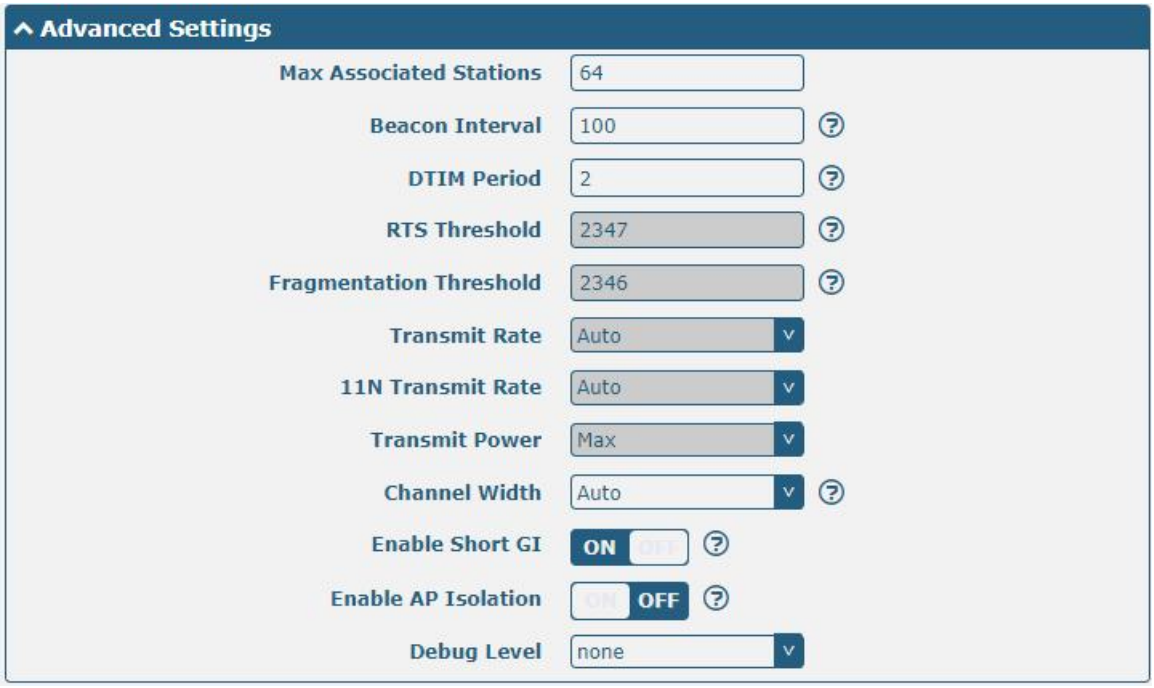
The window is displayed as below when setting “WEP” as the security mode.



General Settings @ Access Point		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Wi-Fi access point option.	OFF
Wireless Mode	Select from “11bgn Mixed”, “11b Only”, “11g Only” or “11n Only”. • 11bgn Mixed: Mix three agreements, for backward compatibility • 11b only: IEEE 802.11b，11Mbit/s~2.4GHz • 11g only: IEEE 802.11g，54Mbit/s~2.4GHz • 11n only: IEEE 802.11n，300Mbps~600Mbps	11bgn Mixed

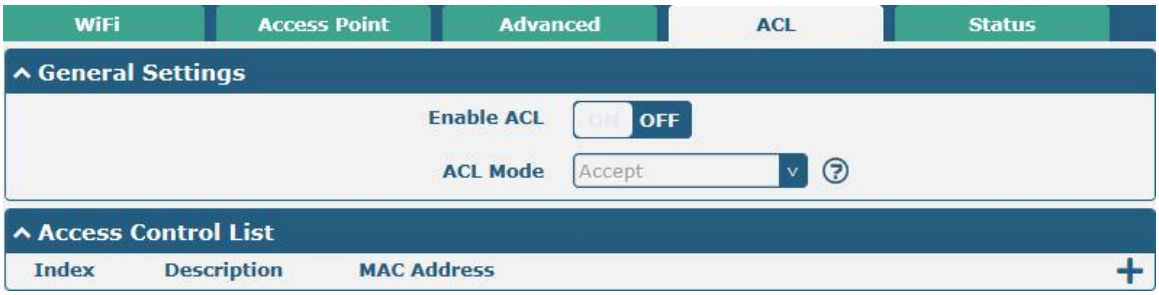
General Settings @ Access Point		
Item	**Description**	**Default**
Channel	Select the frequency channel, including “Auto”, “1”, “2”…… “13”. • Auto: Router will scan all frequency channels until the best one is found • 1~13 Router will be fixed to work with this channel Following are the frequency of 1~13 channel: 1–2412 MHz 2–2417 MHz 3–2422 MHz 4–2427 MHz 5–2432 MHz 6–2437 MHz 7–2442 MHz 8–2447 MHz 9–2452 MHz 10–2457 MHz 11–2462 MHz 12–2467 MHz 13–2472 MHz	Auto
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 Wi-Fi client side.	ON
Security Mode	Select from “Disabled”, “WPA-Personal”, “WPA-Enterprise” or “WEP”. • Disabled: User can access the Wi-Fi without password **Note**: It is strongly recommended for security purposes that you do not choose this kind of mode. • WPA-Personal: Wi-Fi Protected Access only provides one password used for Identity Authentication • WPA-Enterprise: Provides an authentication interface for EAP which can be authenticated via Radius Authentication Server or other Extended Authentication • 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

General Settings @ Access Point		
Item	**Description**	**Default**
Encryption	Select from “Auto”, “TKIP” or “AES”. • Auto: Router will choose automatically the most suitable encryption • TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication **Note**: It's not recommended to use TKIP encryption in 802.11n mode. • AES: AES encryption uses a wireless connection. AES can be used for CCMP WPA-PSK and WPA 802.1x authentication. AES is a stronger encryption algorithm than TKIP	Auto
PSK Password	Enter the Pre share key password. When router works as AP mode, enter Master key to generate keys for encryption. A PSK Password is used as a basis for encryption methods (or cipher types) in a WLAN connection. The PSK Password should be complicated and as long as possible. For security reasons, this PSK Password should only be disclosed to users who need it, and it should be changed regularly. Enter 8 to 63 characters.	Null
Group Key Update Interval	Enter the interval of group key update.	3600
Radius Authentication Server Address	Enter the address of radius authentication server.	Null
Radius Authentication Server Port	Enter the port of radius authentication server.	1812
Radius Server Share Secret	Enter the shared secret of radius authentication server.	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		
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 "request to send" 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 Wi-Fi AP. It is recommended that you use the default value 2346.	2346
Transmit Rate	Set the transmit rate. You can choose Auto or specify a Transmit Rate, including 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, and 54Mbps, MCS0, MCS1, MCS2, MCS3, MCS4, MCS5, MCS6 and MCS7.	Auto
11N Transmit Rate	Specify the transmit rate under the IEEE 802.11n mode or let is default to "Auto".	Auto
Transmit Power	Select from "Max", "High", "Medium" or "Low".	Max
Channel Width	Select from "Auto", "20MHz" or "40MHz". **Note**: 40 MHz channel width provides higher available data rate, twice as many as 20 MHz channel width.	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 11% in data rates, but also result in higher packet error rates.	ON
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option.	OFF

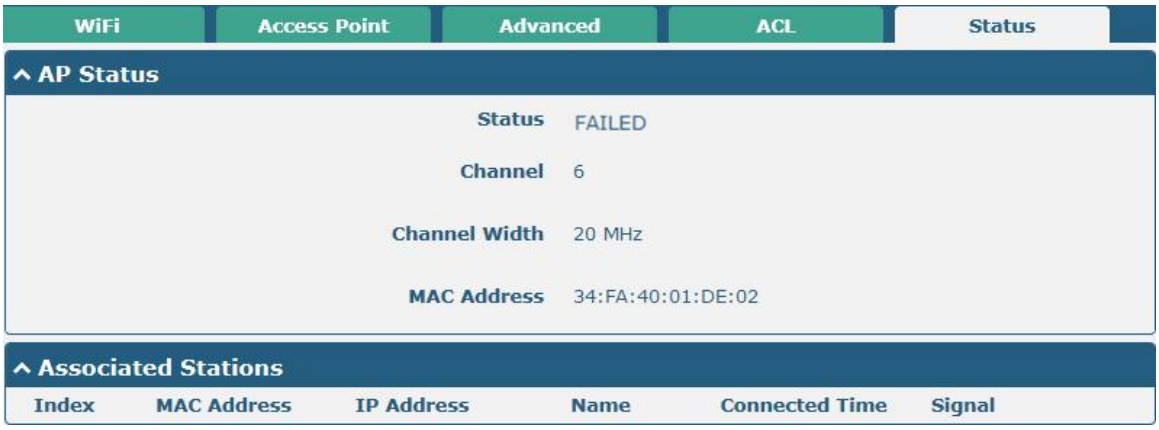
Advanced Settings		
Item	**Description**	**Default**
	When enabled, the router will isolate all connected wireless devices. The wireless device cannot access the router directly via WLAN.	
Debug Level	Select from “verbose”, “debug”, “info”, “notice”, “warning” or “none”.	none



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

ACL		
Item	**Description**	**Default**
General Settings		
Enable ACL	Click the toggle button to enable/disable this option.	OFF
ACL Mode	Select from “Accept” or “Deny”. • Accept: Only the packets fitting the entities of the “Access Control List” can be allowed • Deny: All the packets fitting the entities of the “Access Control List” will be denied **Note**: Router can only allow or deny devices which are included in “Access Control List” at one time.	Accept
Access Control List		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this access control list.	Null
MAC Address	Add a MAC address here.	Null

This section allows you to view the status of AP.

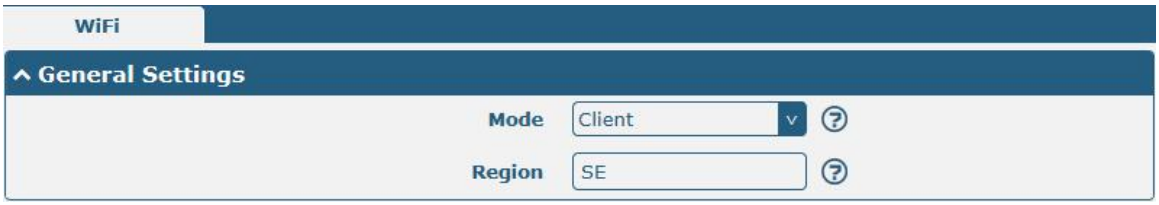


Note: Wi-Fi function is disabled by factory default, if you need to use it, please enable Wi-Fi according to the following steps, and configure the device as Wi-Fi client.

Wi-Fi Client

Configure Router as Wi-Fi Client

Click **"Interface > Wi-Fi > Wi-Fi"**, select "Client" as the mode and click "Submit".

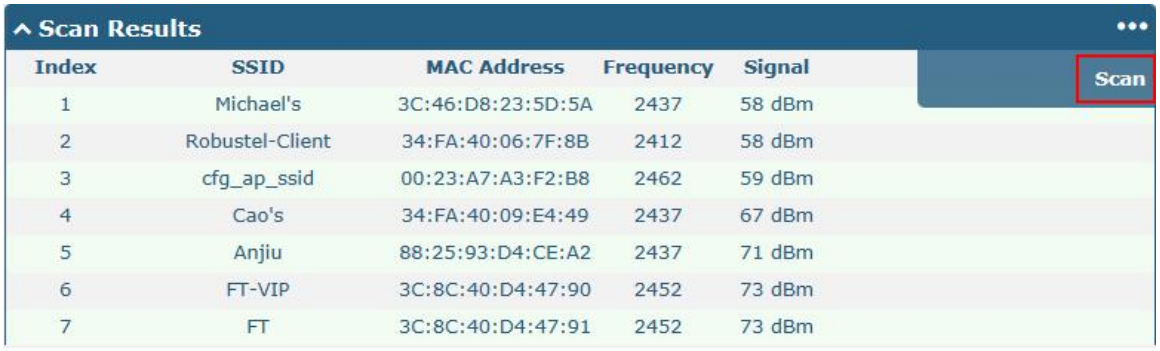


And then a "WLAN" column will appear under the Interface list.

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

Click "**Interface > WLAN"** to configure the parameters of Wi-Fi Client after setting the mode as Client.

This window allows you to scan for all available SSIDs in your area. Please click ••• and then click "Scan" to refresh the surrounding SSID.



Index	SSID	MAC Address	Frequency	Signal
1	Michael's	3C:46:D8:23:5D:5A	2437	58 dBm
2	Robustel-Client	34:FA:40:06:7F:8B	2412	58 dBm
3	cfg_ap_ssid	00:23:A7:A3:F2:B8	2462	59 dBm
4	Cao's	34:FA:40:09:E4:49	2437	67 dBm
5	Anjiu	88:25:93:D4:CE:A2	2437	71 dBm
6	FT-VIP	3C:8C:40:D4:47:90	2452	73 dBm
7	FT	3C:8C:40:D4:47:91	2452	73 dBm

4.3 Network

4.3.1 Route

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

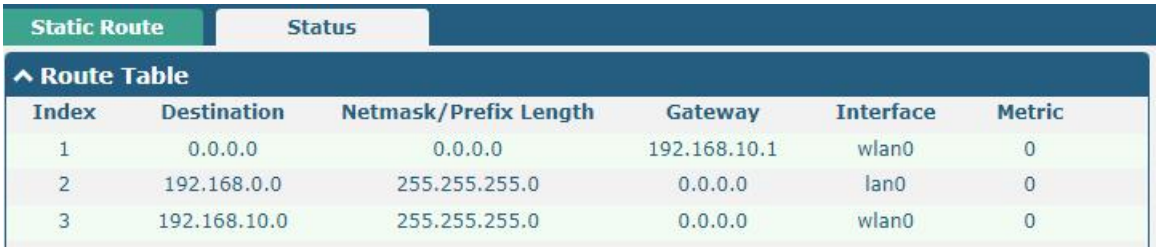
Static Route

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

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

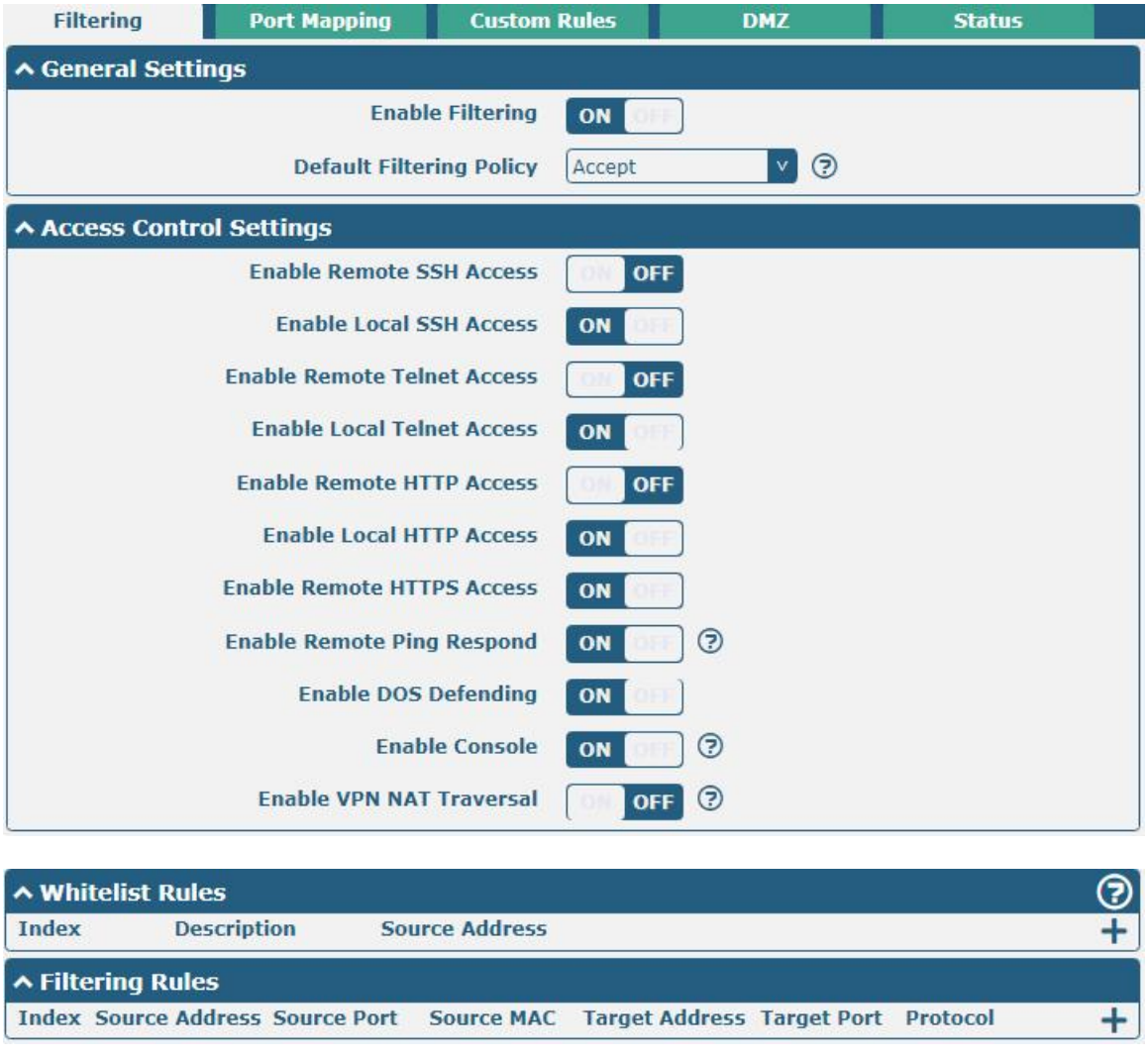
Status

This window allows you to view the status of route.



4.3.2 Firewall

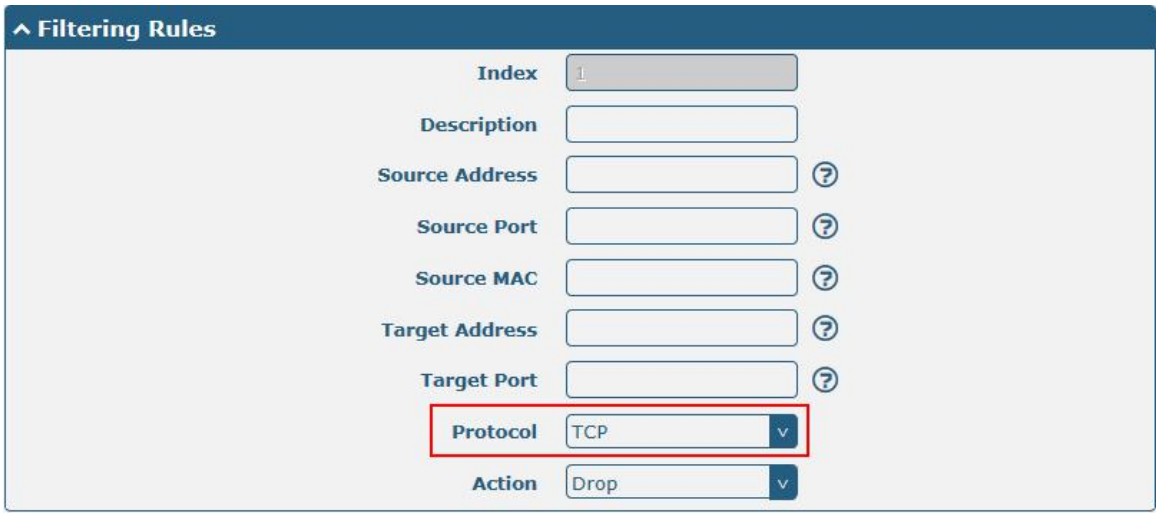
This section allows you to set the firewall and its related parameters, including Filtering, Port Mapping and DMZ. The filtering rules can be used to either accept or block certain users or ports from accessing your router. Click "**Network> Firewall> Filter"**. The following information is displayed:



Click + to add the whitelist rules.

Click + to add a filtering rule. 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.

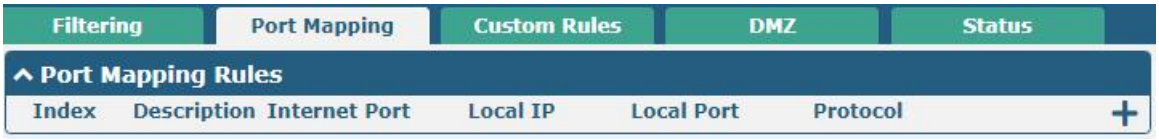


Filtering		
Item	**Description**	**Default**
General Settings		
Enable Filtering	Click the toggle button to enable/disable the filtering option.	ON

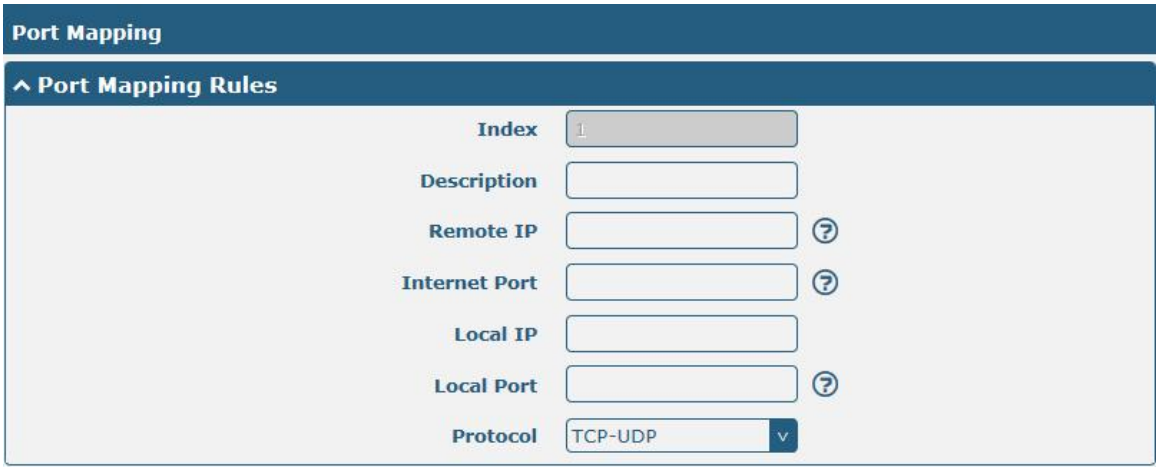
Filtering		
Item	**Description**	**Default**
Default Filtering Policy	Select from “Accept” or “Drop”. • Accept: Router will accept all the connecting requests except the hosts which fit the drop filter list • Drop: Router will drop all the connecting requests except the hosts which fit the accept filter 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.	OFF
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 port	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 GRE / L2TP / PPTP VPN packets.	OFF
Whitelist Rules		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this whitelist rule.	Null
Source Address	Specify an access originator and enter its source address.	Null
Filtering Rules		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this filtering rule.	Null
Source Address	Specify an access originator and enter its source address.	Null
Source Port	Specify an access originator and enter its source port.	Null
Source MAC	Specify an access originator and enter its source MAC address.	Null
Target Address	Enter the target address which the access originator wants to access.	Null
Target Port	Enter the target port which the access originator wants to access.	Null

Filtering		
Item	**Description**	**Default**
Protocol	Select from “All”, “TCP”, “UDP”, “ICMP”, “ICMPv6” 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 is defined manually in the router, and all data received from certain ports on the public network is forwarded to a certain port on a certain IP in the internal network. Click “**Network> Firewall> Port Mapping”** to display the following:



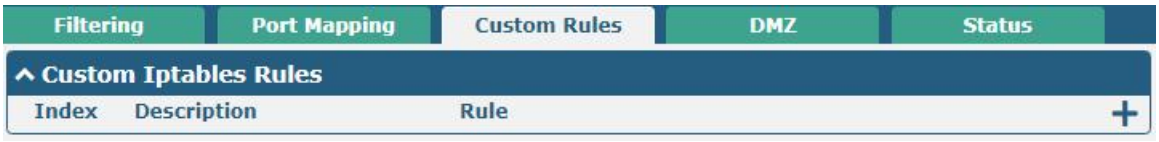
Click + to add port mapping rules. The maximum rule count is 50.



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 the local IP address. Empty means unlimited, e.g. 10.10.10.10/255.255.255.255 or 192.168.1.0/24	Null
Internet Port	Enter the internet port of router which can be accessed by other hosts from internet.	Null
Local IP	Enter router’s LAN IP which will forward to the internet port of router.	Null
Local Port	Enter the port of router’s LAN IP.	Null

Port Mapping Rules		
Item	**Description**	**Default**
Protocol	Select from “TCP”, “UDP” or “TCP-UDP” as your application required.	TCP-UDP

Custom rules, that is, rules that you define yourself. Click “**Network> Firewall> Custom Rule”** to display the following:



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 Firewall Rules.	Null
Rule	Enter custom rules.	Null

DMZ (Demilitarized Zone), also known as the demilitarized zone. It is a buffer between a non-secure system and a secure system that is set up to solve the problem that users who access the external network cannot access the internal network server after the firewall is installed. A DMZ host is an intranet host where all ports are open to the specified address except the ports that are occupied and forwarded.

Click “**Network> Firewall> DMZ”**. The following information is displayed:

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. Null means for any addresses.	Null

NAT setting, i.e. custom NAT rules. Click "**Network > Firewall > NAT**" to display the following.

Click + to add custom rules.

NAT Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description of this NAT rule.	Null
Source Address	Enter the source address in the format x.x.x.x, x.x.x.x/xx, x.x.x.x-x.x.x.x, or null to indicate any address.	Null
Out	Select the output interface. Selecting unspecified means any output interface.	unspecified
Target Address	Enter the target address in the format x.x.x.x, x.x.x.x/xx, x.x.x.x-x.x.x.x.	Null
NAT IP	Enter the NAT address in the format x.x.x.x.	Null

Click **Status** to view the device's firewall status.

Filtering | Port Mapping | Custom Rules | NAT | Status

Chain Input

Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	DROP	tcp	wlan0	*	0.0.0.0/0	0.0.0.0/0
2	0	DROP	tcp	wlan0	*	0.0.0.0/0	0.0.0.0/0
3	0	DROP	tcp	wlan0	*	0.0.0.0/0	0.0.0.0/0
4	0	REJECT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
5	6	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
6	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
7	5	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
8	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
9	0	ACCEPT	icmp	*	*	0.0.0.0/0	0.0.0.0/0
10	0	DROP	icmp	*	*	0.0.0.0/0	0.0.0.0/0
11	0	DROP	tcp	wlan0	*	::/0	::/0
12	0	DROP	tcp	wlan0	*	::/0	::/0
13	0	DROP	tcp	wlan0	*	::/0	::/0
14	0	REJECT	tcp	*	*	::/0	::/0
15	0	ACCEPT	tcp	*	*	::/0	::/0
16	0	DROP	tcp	*	*	::/0	::/0
17	0	ACCEPT	tcp	*	*	::/0	::/0
18	0	DROP	tcp	*	*	::/0	::/0
19	0	ACCEPT	icmpv6	*	*	::/0	::/0
20	0	DROP	icmpv6	*	*	::/0	::/0

Chain Forward

Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	TCPMSS	tcp	*	*	0.0.0.0/0	0.0.0.0/0
2	0	TCPMSS	tcp	*	*	::/0	::/0

Chain Output

Index	Packets	Target	Protocol	In	Out	Source	Destination

4.3.3 IP Passthrough

Click "**Network > IP Passthrough > IP Passthrough"** to enable or disable the IP Passthrough option.

If router enables the IP Passthrough, 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.

Note: The IP Passthrough function can only assign one network provider address.

4.4 VPN

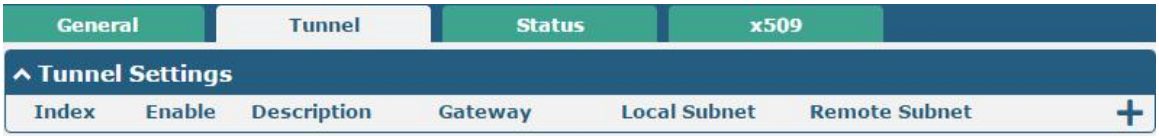
4.4.1 IPsec

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 "**Virtual Private Network> 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 information output to the debug port.	OFF



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
Router	Enter the address or domain name of remote side IPsec VPN server.0.0.0.0 represents 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. 192.168.1.0/24	Null
Remote Subnet	Enter the remote subnet’s address with mask protected by IPsec, e.g. 10.8.0.0/24	Null
Link binding	Select from WWAN1, WWAN2, 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.

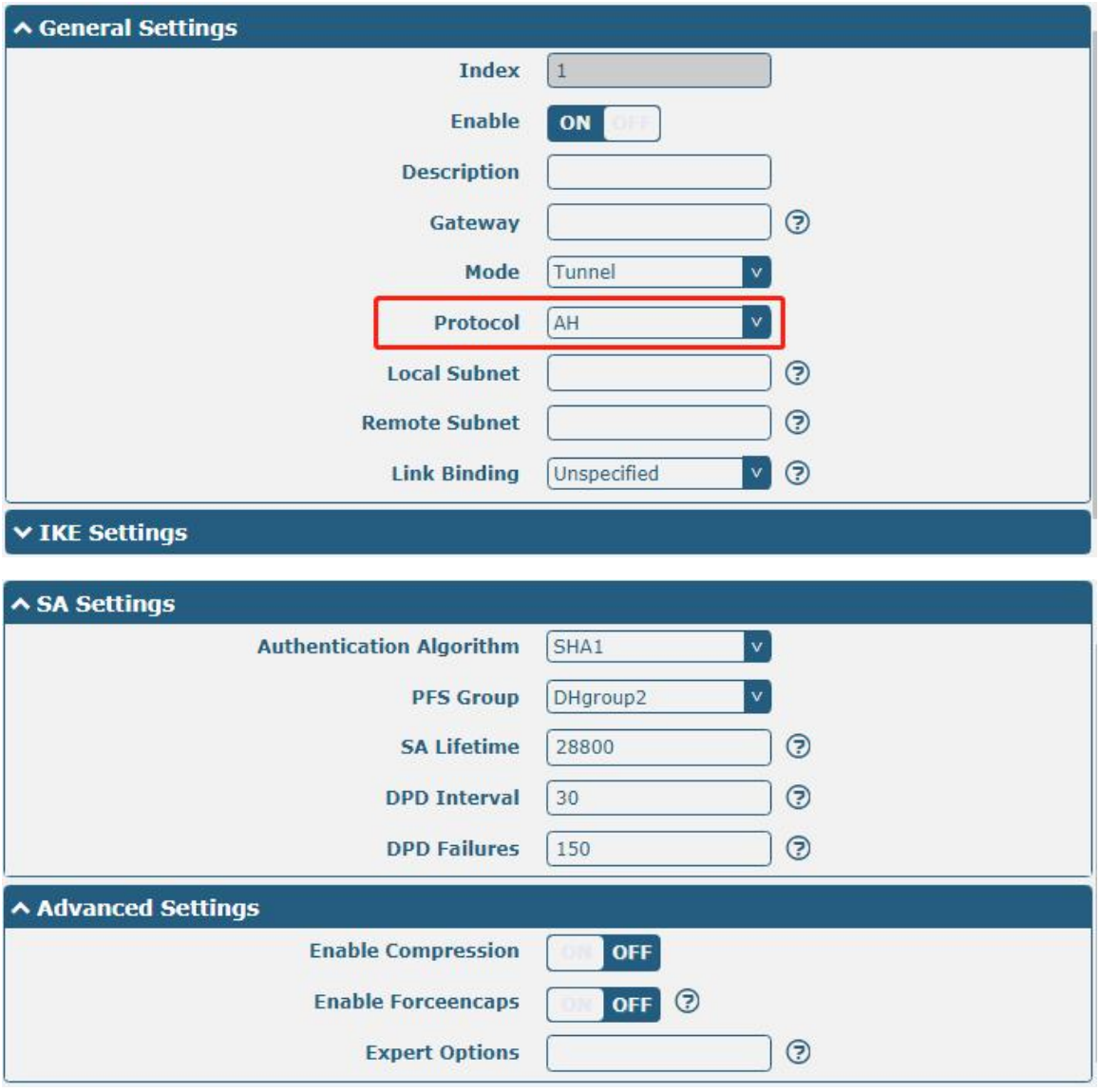
The window is displayed as below when choosing “xAuth CA” as the authentication type.

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
Authentication Algorithm	Select from “MD5”, “SHA1”, “SHA2 256” or “SHA2 512” to be used in IKE negotiation.	SHA1
Encrypt Algorithm	Select from “3DES”, “AES128”, “AES192” and “AES256”to be used in IKE	3DES

IKE Settings		
Item	**Description**	**Default**
	negotiation. • 3DES: Use 168-bit 3DES encryption algorithm in CBC mode • AES128: Use 128-bit AES encryption algorithm in CBC mode • AES256: Use 256-bit AES encryption algorithm in CBC mode	
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 Certificate Authority • xAuth: Extended Authentication to AAA server	PSK
PSK Secret	Enter the pre-shared key.	Null
Local ID Type	Select from “Default”, “FQDN” and “User FQDN” for IKE negotiation. • Default: Use an IP address as the ID in IKE negotiation • FQDN: Use an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security router, e.g., test.robustel.com. • User FQDN: Use a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign “@” for the local security router, e.g., test@robustel.com.	Default
Remote ID Type	Select from “Default”, “FQDN” and “User FQDN” for IKE negotiation. • Default: Use an IP address as the ID in IKE negotiation • FQDN: Use an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security router, e.g., test.robustel.com. • User FQDN: Use a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign “@” for the local security 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

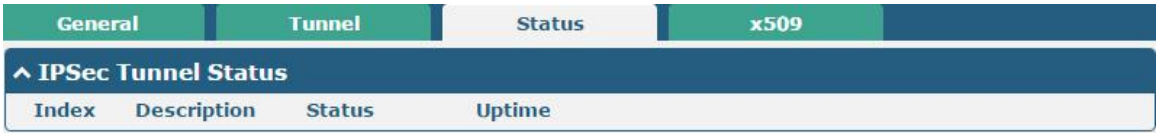
If click "**VPN > IPsec > Tunnel > General Settings**", and choose **ESP** as protocol. The specific parameter configuration is shown as below.

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

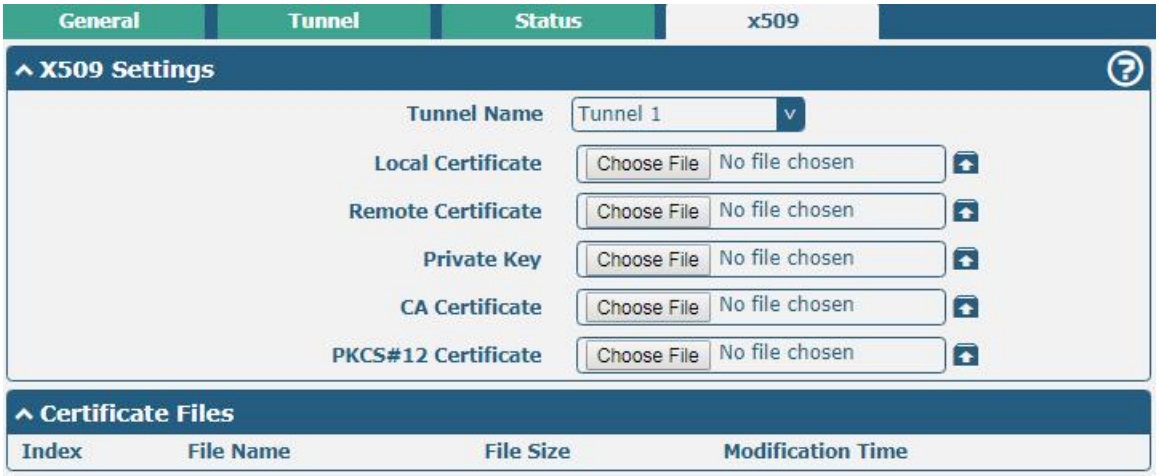


SA Settings		
Item	**Description**	**Default**
Encrypt Algorithm	Select from “3DES”, “AES128” or “AES256” when you select “ESP” in “Protocol”. Higher security means more complex implementation and lower speed. DES is enough to meet general requirements. Use 3DES when high confidentiality and security 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 “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 set up IPsec SAs, IKE uses the smaller one between the lifetime set locally and the lifetime proposed by the peer.	28800
DPD Interval	Set the interval after which DPD is triggered if no IPsec protected packets is received from the peer. DPD is Dead peer detection. DPD irregularly detects dead IKE peers. When the local end sends an IPsec packet, DPD checks the time the last IPsec packet was received from the peer. If the time exceeds the DPD interval, it sends a DPD hello to the peer. If the local end receives no DPD acknowledgment within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgment after having made the maximum number of retransmission attempts, it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.	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 toggle button to enable / disable this option. After it is enabled, even if no NAT condition is detected, the UDP encapsulation of esp packets is forced. This may help overcome restrictive firewalls.	OFF
Expert Options	Add more PPP configuration options here, format: config-desc;config-desc, e.g. protostack=netkey;plutodebug=none	Null

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



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

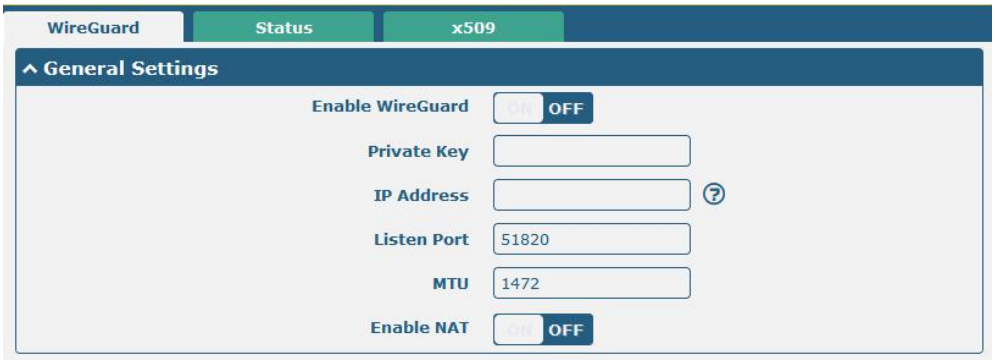


x509		
Item	**Description**	**Default**
X509 Settings		
Tunnel Name	Choose a valid tunnel.	Tunnel 1
Local Certificate	Click on "Choose File" to locate the certificate file from your PC, and then import this file into your router.	--
Peer Certificate	Select the peer certificate to import to the router.	--
Private Key	Select the correct private key file to import into the router.	--
Root Certificate	Select the root certificate file to import into the router.	--
PKCS#12 Certificate	Select the PKCS#12 certificate file to import into the route	--
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

4.4.2 WireGuard

This section is used to set the parameters of WireGuard VPN, an open source SSL-based VPN system. The router's WireGuard feature can support both point-to-point and point-to-multipoint VPN channels.

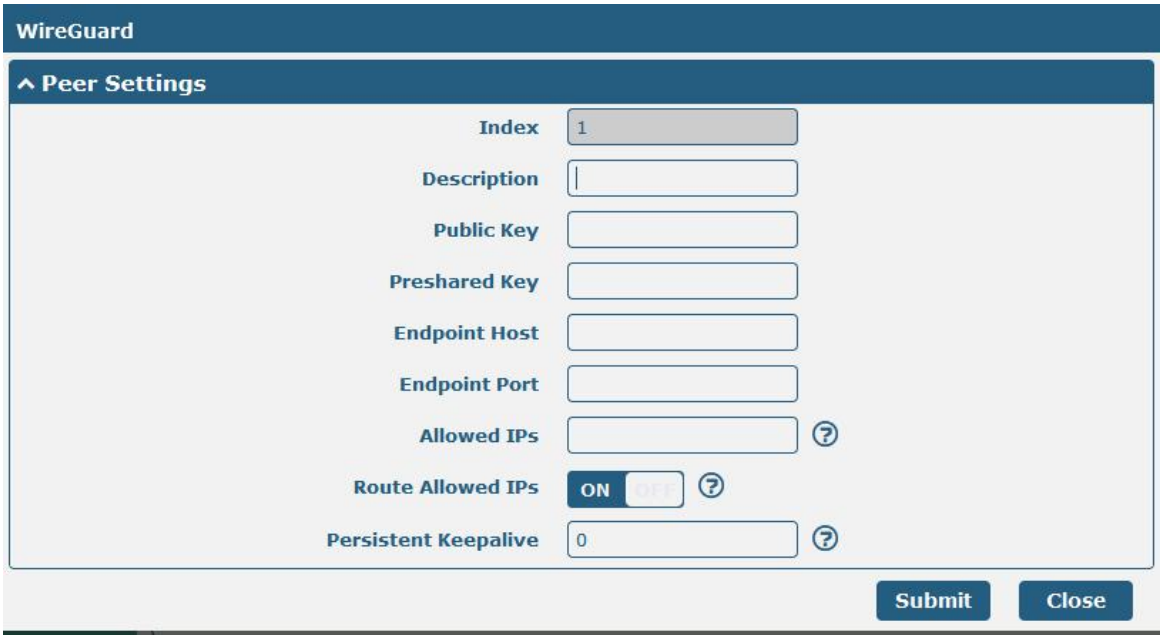
Click "**Virtual Private Network** > **WireGuard** > **WireGuard"** to set the WireGuard parameters.



WireGuard@General Settings		
Item	**Descriptions**	**Default**
Enable WireGuard	Enable or disable WireGuard	OFF
Private Key	Enter the local private key. It can be generated automatically or imported manually via X509 settings, but cannot be empty.	Null
IP Address	Enter the IP address of the virtual interface. It cannot be empty.	Null
Listen Port	Enter the virtual interface listen port. It cannot be empty.	51820
MTU	Enter the virtual interface slice size.	1472
Enable NAT	Enable/disable the NAT feature. When enabled, the IP address will be converted to the interface virtual IP address.	ON

Note: click for help.

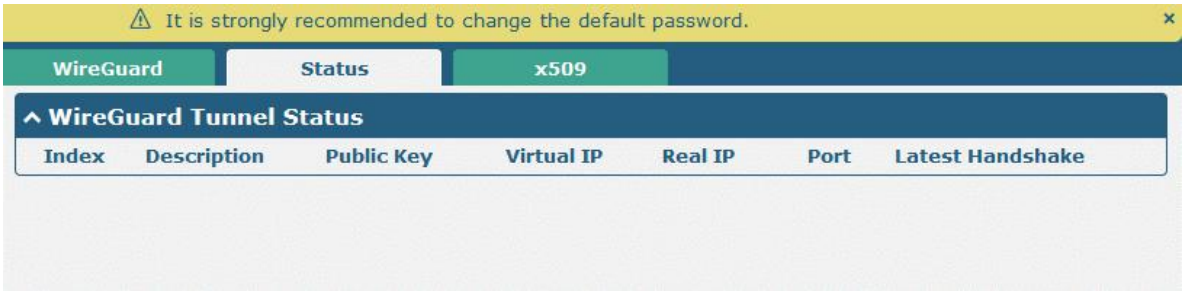
Click to add peer setting. The maximum count is 20.



WireGuard@Peer Settings		
Item	**Descriptions**	**Default**
Peer Settings		
Index	Display the index	--
Description	Enter peer descriptions. Can be empty.	Null
Public Key	Enter public key and it cannot be empty.	Null

WireGuard@Peer Settings		
Item	**Descriptions**	**Default**
Preshared Key	Enter preshared key and it cannot be empty.	Null
Endpoint Host	Enter the peer IP address. A null value will not initiate a connection request.	Null
Endpoint Port	Enter the peer port. A null value will not initiate a connection request.	Null
Allowed IPs	Enter the allowed IP address, which cannot be empty.	Null
Route Allowed IPs	Enable/disable the feature. When enabled, routes will be created for the networks allowed for this peer. If the allowed network is 0.0.0.0/0, this peer will be set as the default route.	ON
Persistent Keepalive	Enter the interval of sending Persistent Keepalive messages, in seconds. 0 means disabling the feature.	0

The status bar allows to view WireGuard's connection status. Click on one of the rows and details of its link connection will be displayed below the current row.



This section is used to generate or import private and public keys.

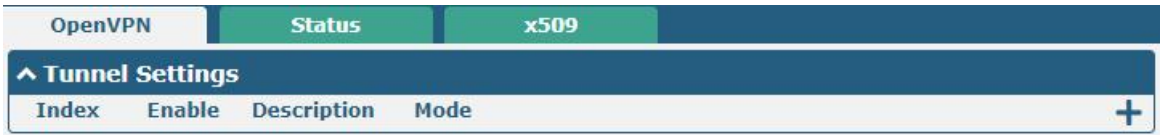
x509		
Item	**Descriptions**	**Default**
X509 Settings		
Private Key	Click **Generate** to generate private key; click **Import** to import the private key.	--
Private Key	Click **Import** to import the private key from the PC to the router.	--

x509		
Item	**Descriptions**	**Default**
Public Key	Click Import to generate public key.	--

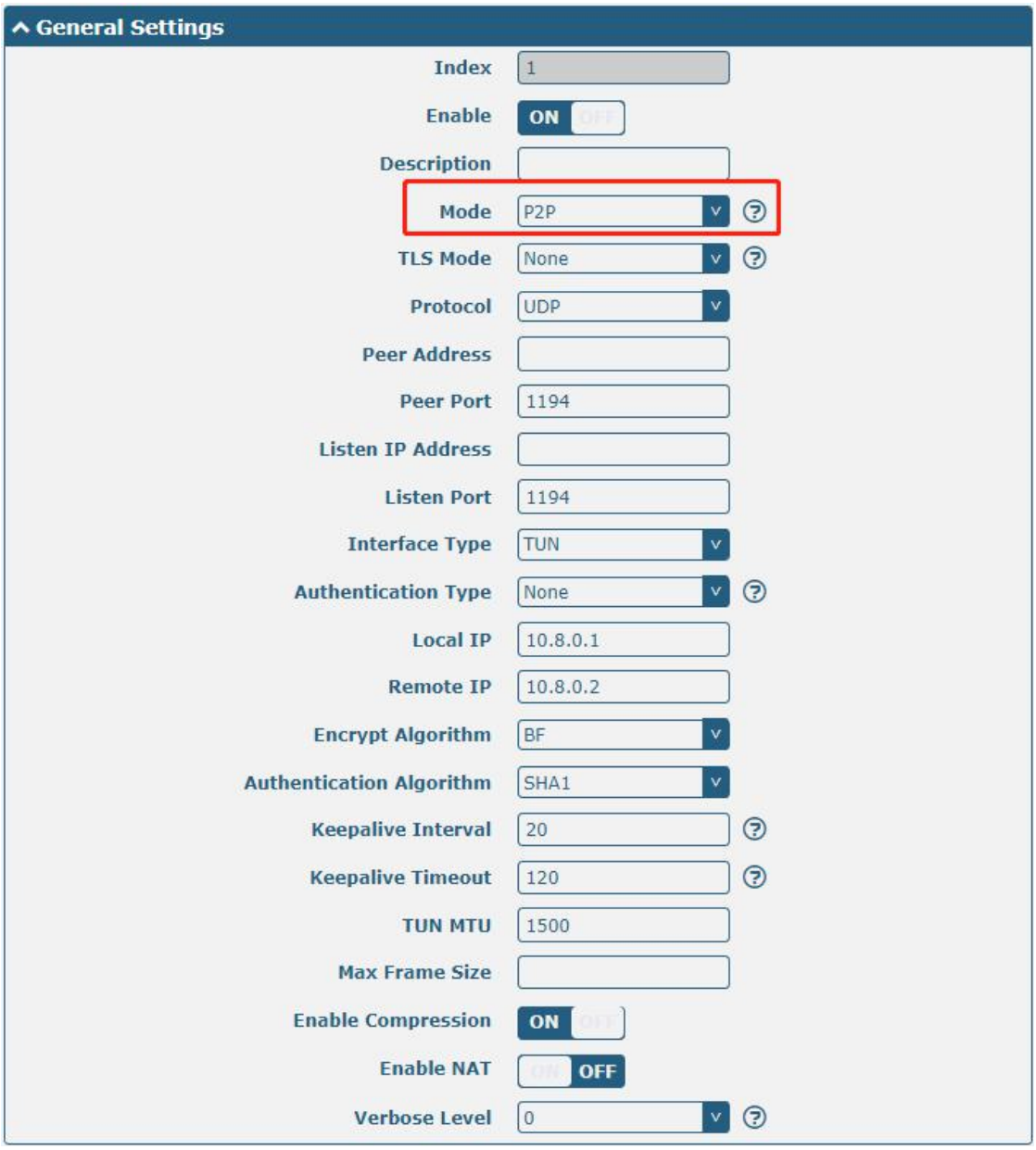
4.4.3 OpenVPN

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.

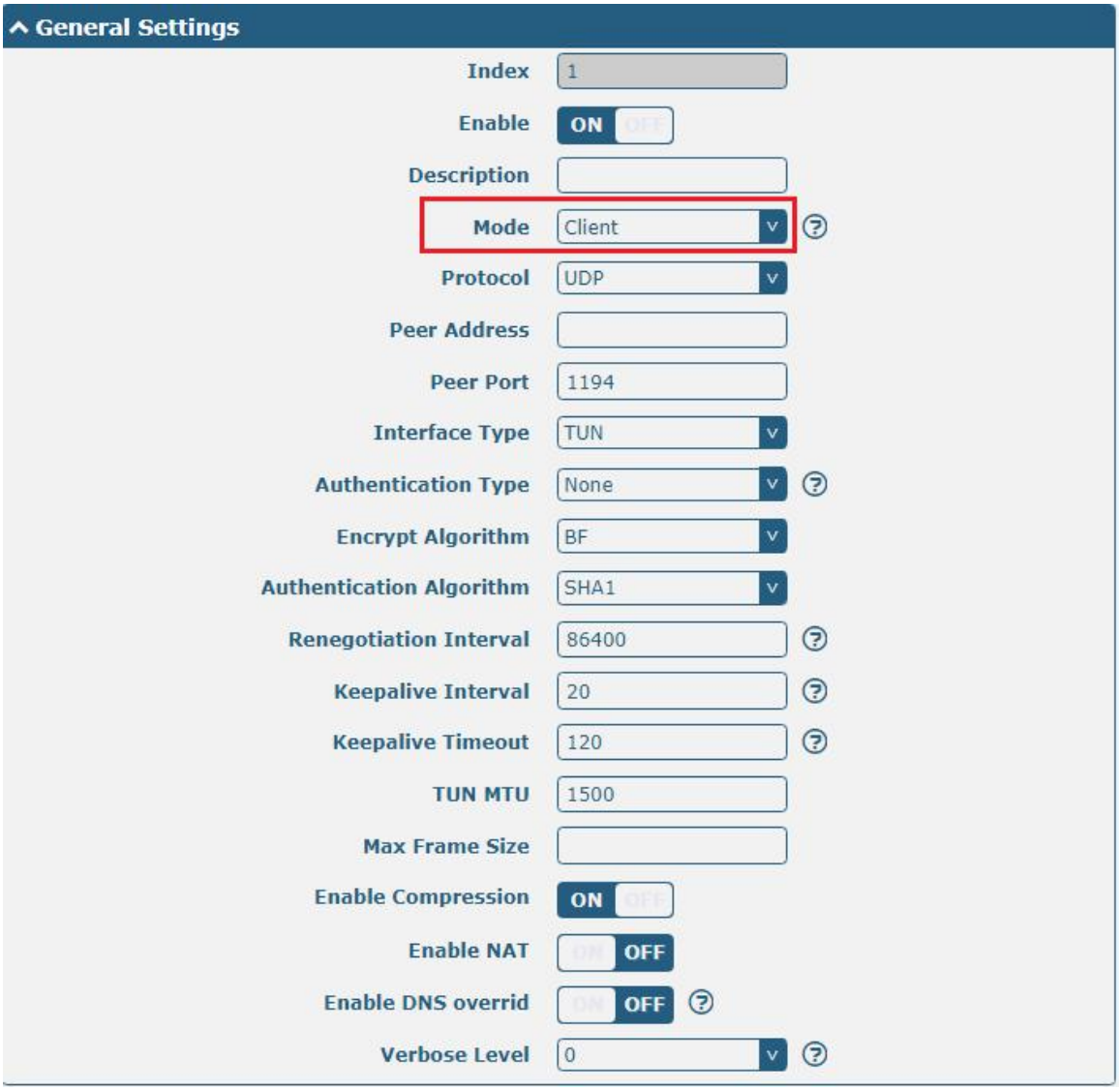
Click "**Virtual Private Network> OpenVPN> OpenVPN"**. The following information is displayed:



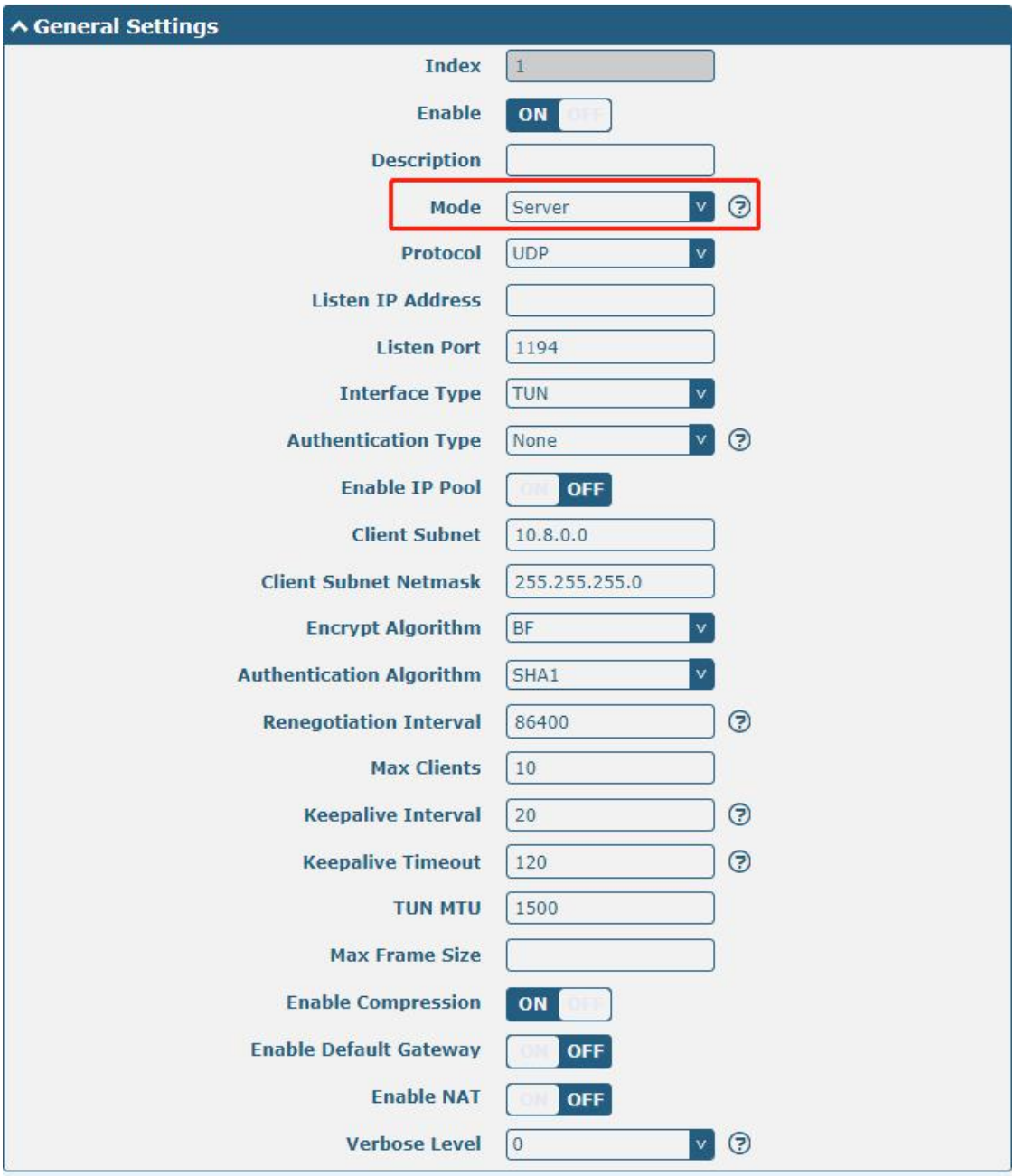
Click + to add tunnel settings. The maximum count is 6. By default, the mode is “P2P”.



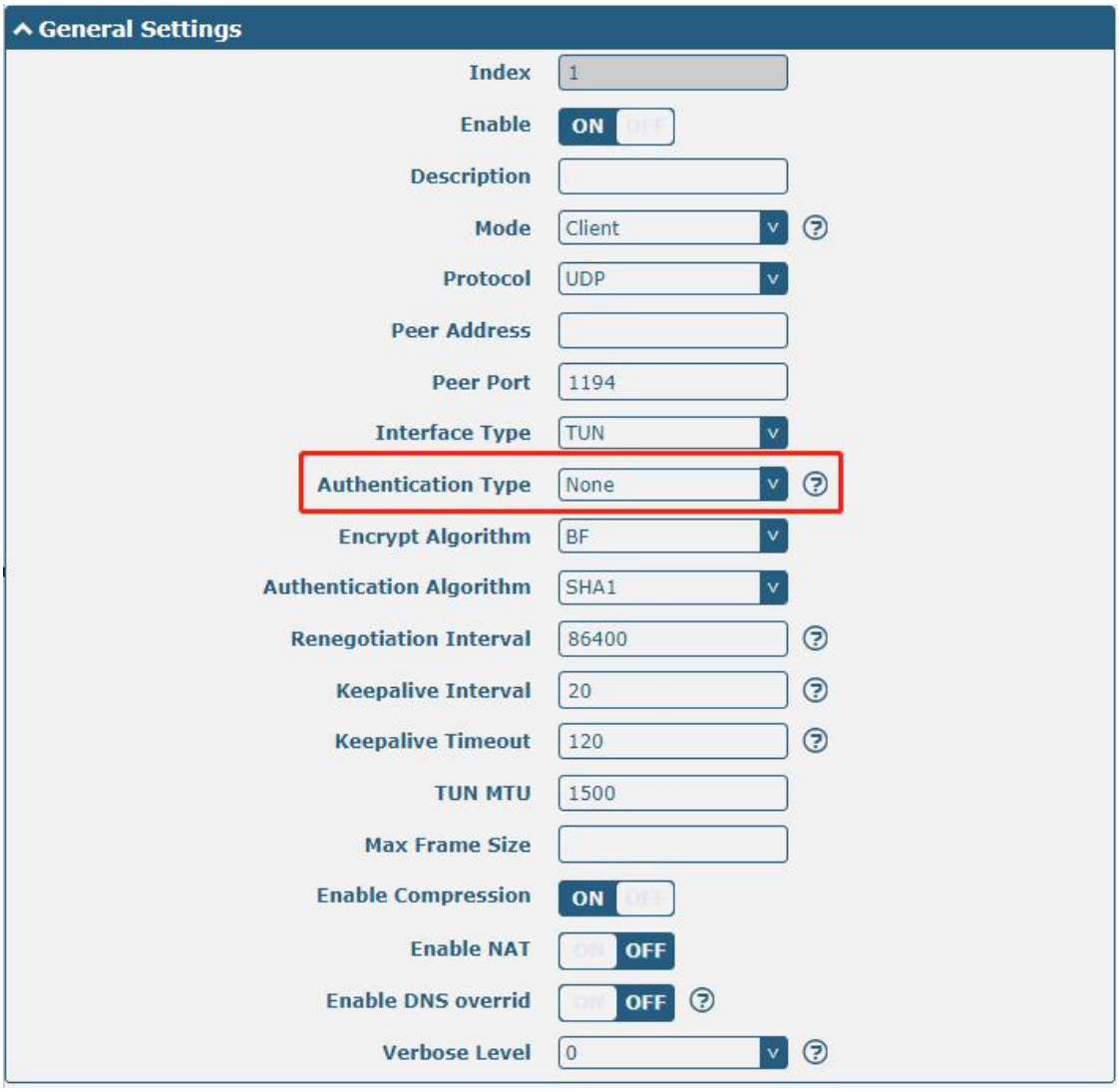
The window is displayed as below when choosing “Client” as the mode.



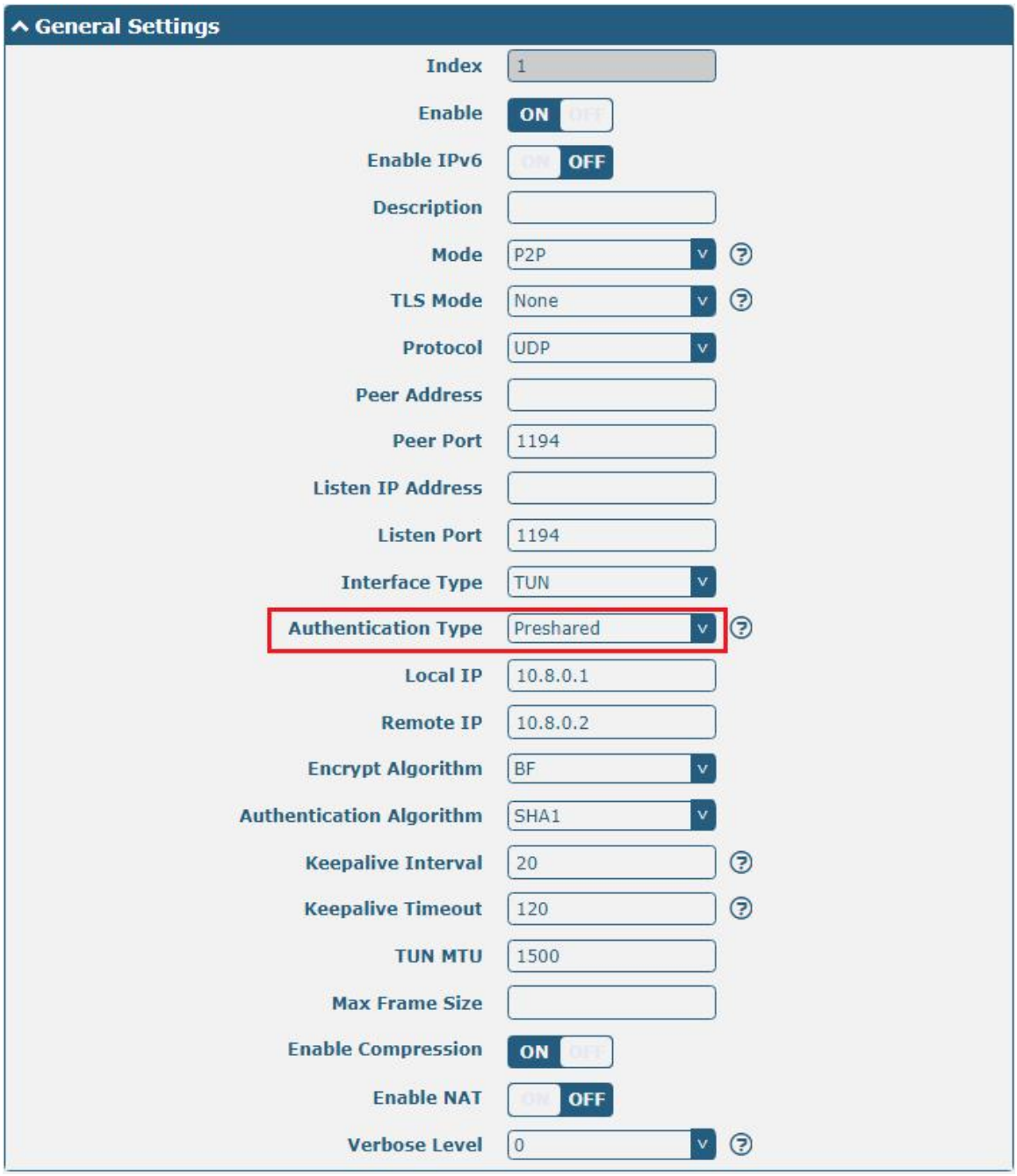
The window is displayed as below when choosing “Server” as the mode.



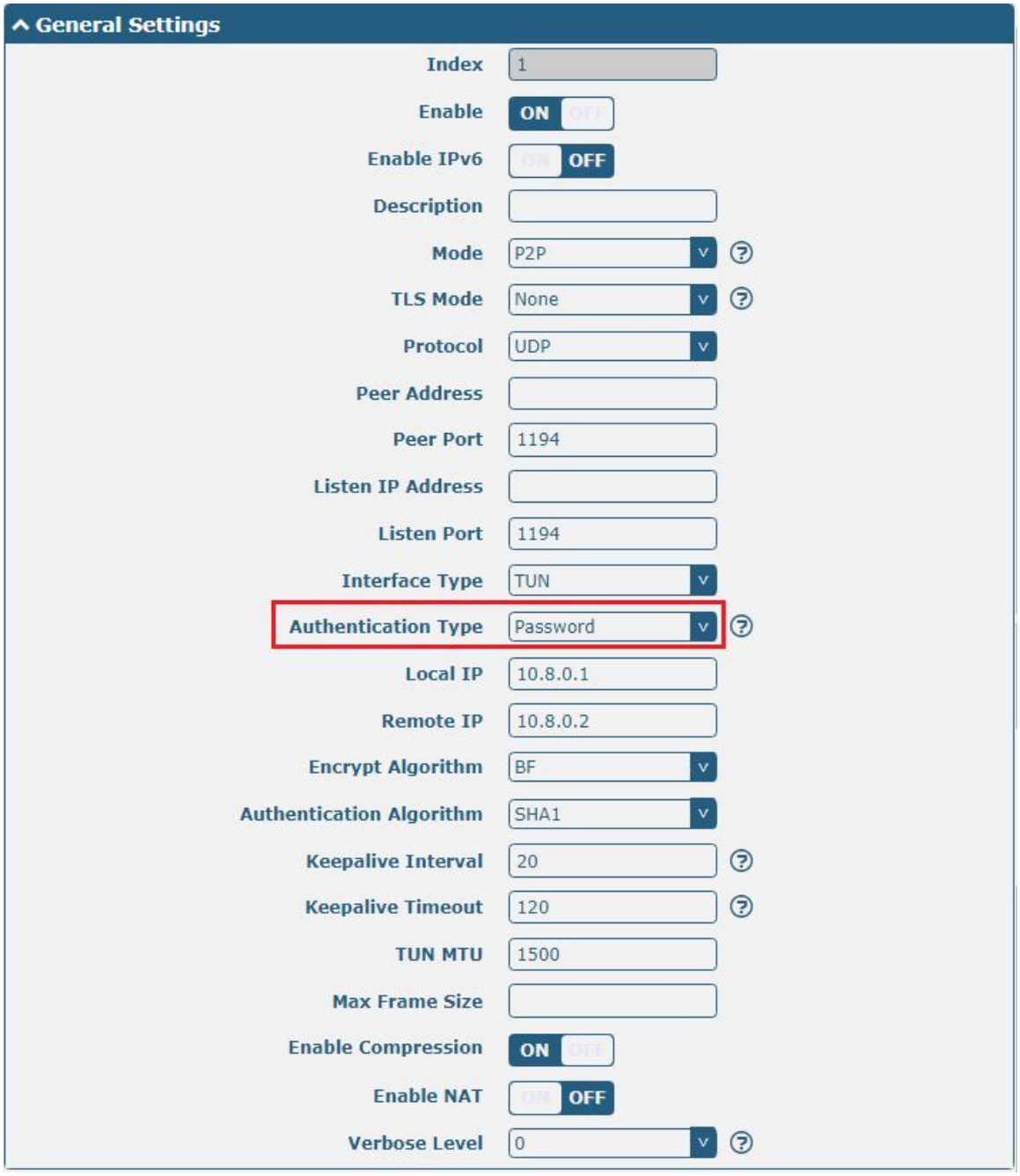
The window is displayed as below when choosing “None” as the authentication type.



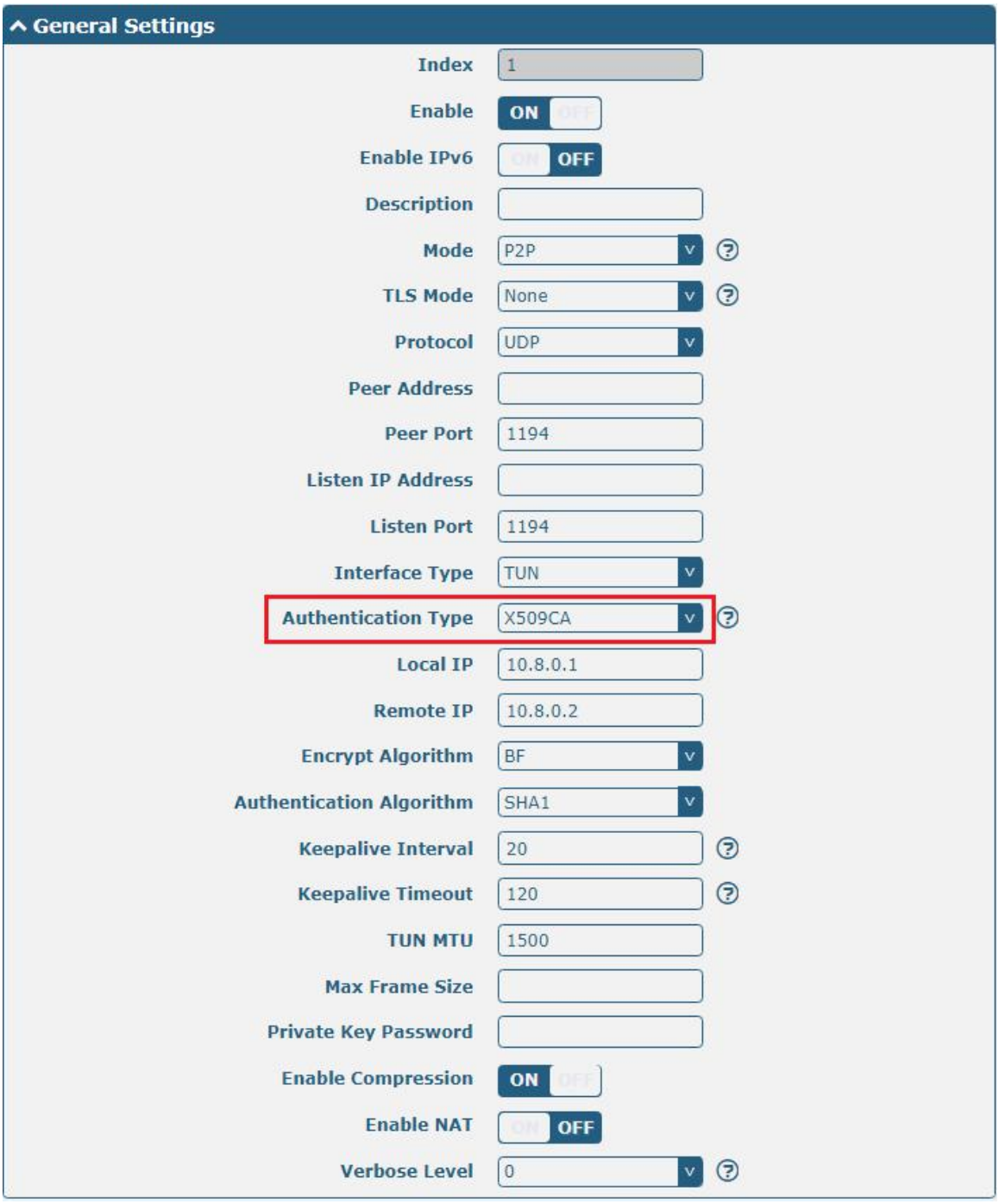
The window is displayed as below when choosing “Preshared” as the authentication type.



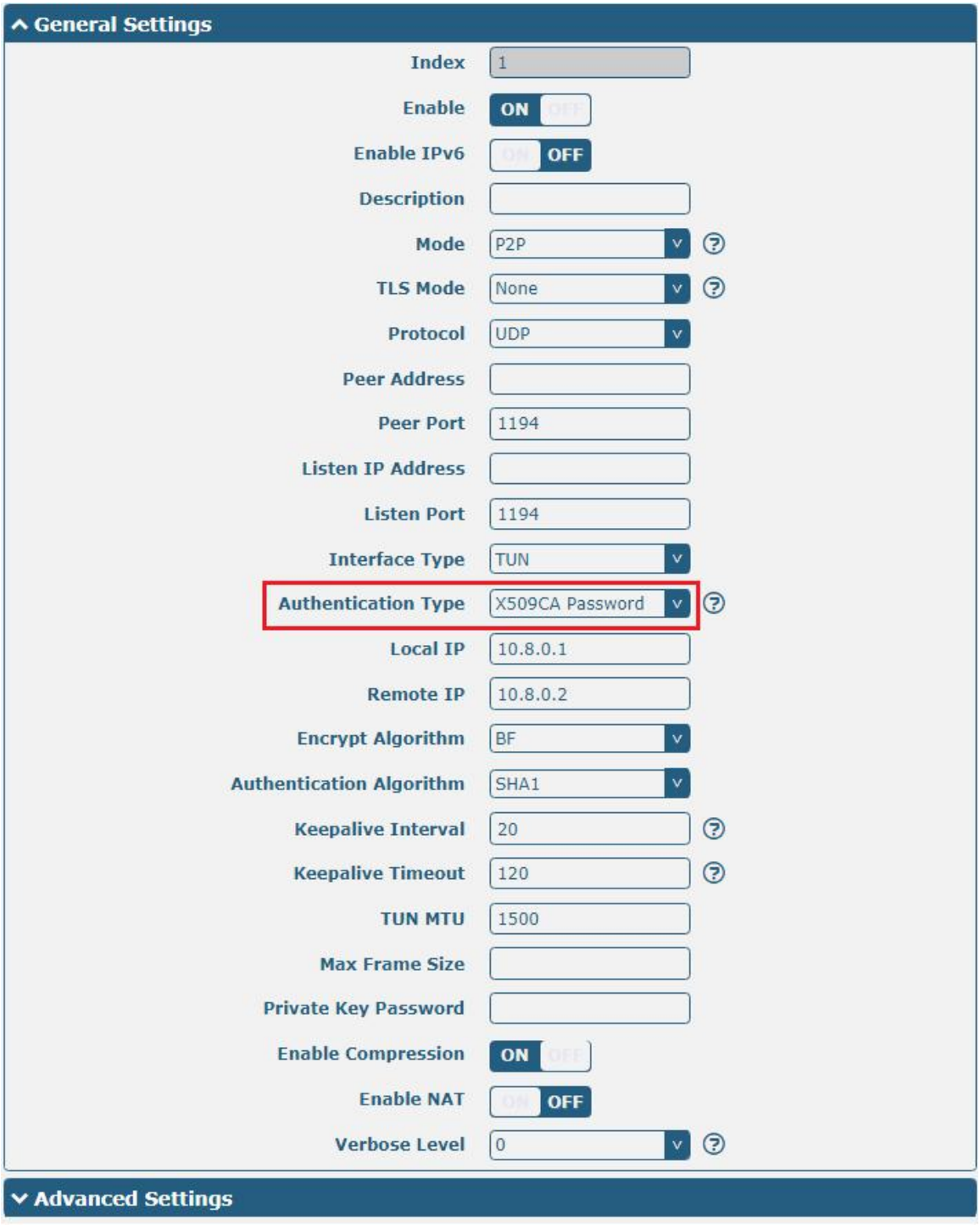
The window is displayed as below when choosing “Password” as the authentication type.



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



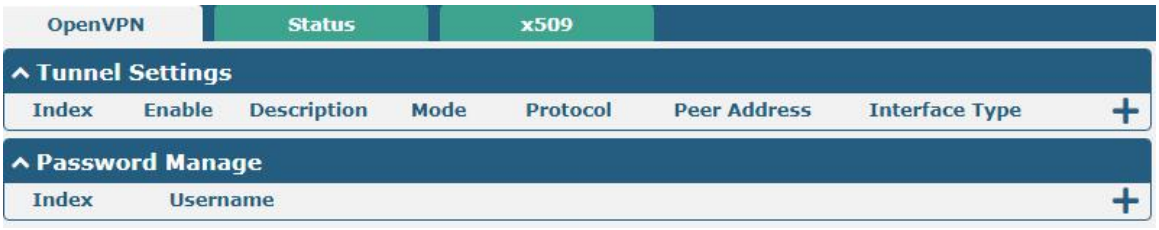
The window is displayed as below when choosing “X509CA Password” as the authentication type.



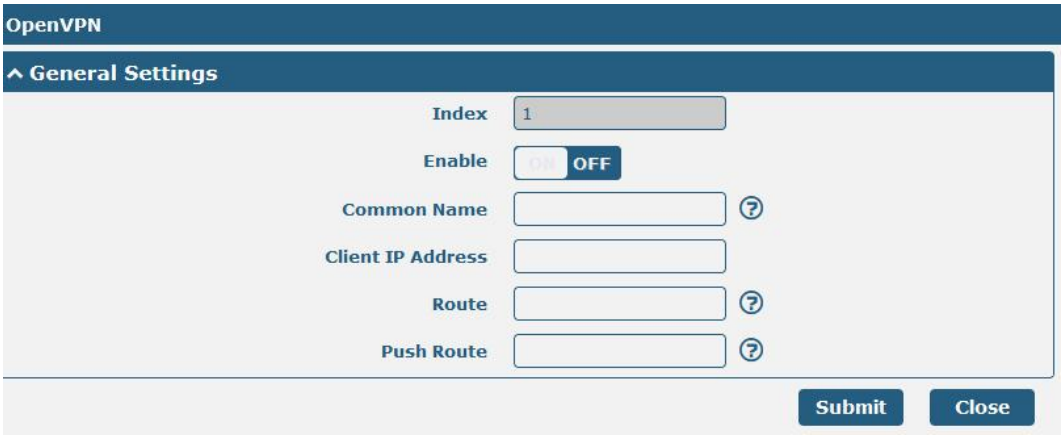
The window is displayed as below when choosing “Client” as the mode.

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

The window of "**Virtual Private Network> OpenVPN> OpenVPN**" is displayed as below when choosing “Server” as the mode and choosing “X509CA Password” as the authentication type.



Click Client Management + to add 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” or “Server”.	P2P
TLS Mode	Select from “None”, “Client” or “Server”.	None
Protocol	Select from “UDP”, “TCP-Client” or “TCP-Server”.	UDP
Server Address	Enter the end-to-end IP address or the domain of the remote OpenVPN server.	Null
Server Port	Enter the end-to-end listener port or the listening port of the OpenVPN server.	1194

General Settings @ OpenVPN		
Item	**Description**	**Default**
Listening Address	Local server address.	Null
Listening Port	Local server port.	1194
Interface Type	Select from "TUN" or "TAP" which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.	TUN
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
Starting Address	Defines the beginning of an IP address pool that assigns addresses to OpenVPN clients.	10.8.0.5
End Address	Defines the end of the IP address pool for assigning addresses to OpenVPN clients.	10.8.0.254
Client Network	Enter the client network IP.	10.8.0.0
Client Netmask	Enter the client netmask.	255.255.255.0
Username	Enter the username used for "Password" or "X509CA Password" authentication type.	Null
Password	Enter the password used for "Password" or "X509CA Password" authentication type.	Null
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
Encrypt Algorithm	Select from "BF", "DES", "DES-EDE3", "AES128", "AES192" and "AES256". • BF: Use 128-bit BF encryption algorithm in CBC mode • DES: Use 64-bit DES encryption algorithm in CBC mode • DES-EDE3: Use 192-bit 3DES encryption algorithm in CBC mode • AES128: Use 128-bit AES encryption algorithm in CBC mode • AES192: Use 192-bit AES encryption algorithm in CBC mode • AES256: Use 256-bit AES encryption algorithm in CBC mode	BF
Renegotiation Interval	Set the renegotiation interval. If connection failed, OpenVPN will renegotiate when the renegotiation interval reached.	86400
Maximum 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

General Settings @ OpenVPN		
Item	**Description**	**Default**
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 Router	Standalone switch button to enable / disable the default router function. After enabling, push the local tunnel address as the default router of the peer device.	OFF
Receive DNS Push	Standalone switch button to enable / disable receiving DNS push function. After enabling, it is allowed to receive DNS information pushed by the peer.	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
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 option. When enabled, client certificates can be revoked.	OFF
Enable Client to Client	Click the toggle button to enable / disable the option. When enabled, clients can communicate with each other.	OFF
Enable Dup Client	Click the toggle button to enable / disable the option. After being enabled, the tunnel IPs obtained by multiple clients are different, and the tunnel IP of the client and the tunnel IP of the server are interoperable.	OFF
Enable IP Address Hold	Click the toggle button to enable / disable the option. When enabled, the IP in the address pool is obtained automatically.	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	Custom tunnel connection username.	Null

General Settings @ OpenVPN		
Item	**Description**	**Default**
Password	Custom tunnel connection password.	Null
Client Management		
Enable	Click the toggle button to enable / disable this option. When enabled, the client IP address can be managed.	OFF
Common Name	Set the certificate name.	Null
Client IP Address	Set a fixed client virtual IP.	Null
Route	Set client-side subnet.	Null
Push Route	Set server-side subnet.	Null

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

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

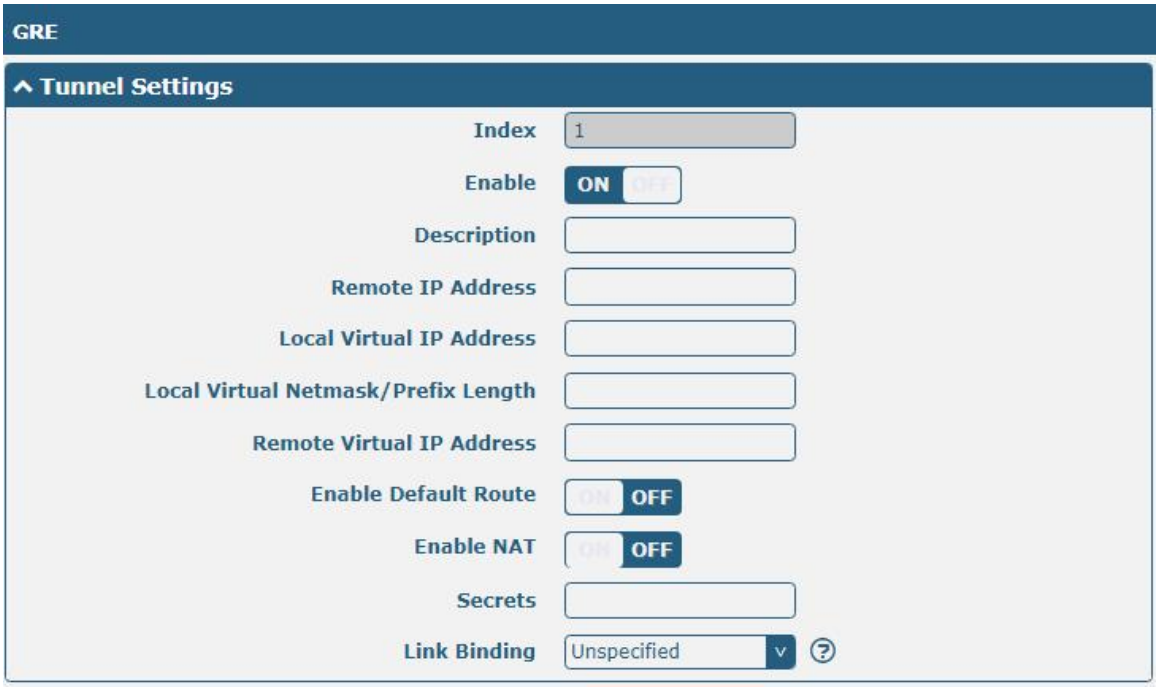
x509		
Item	**Description**	**Default**
X509 Settings		
Tunnel Name	Choose a valid tunnel. Select from "Tunnel 1", "Tunnel 2", "Tunnel 3", "Tunnel 4", "Tunnel 5"or "Tunnel 6".	Tunnel 1
Tunnel mode	Select "P2P Mode", "Client Mode" or "Server Mode".	Client mode
Root certificate	Select the root certificate file to import into the router.	--
Certificate Files	Click on “Choose File” to locate the certificate file from your PC, and then import this file into your router.	--
Private Key	Select the private key file to import into the router.	--

TLS-Auth Key	Select the TLS-Auth key file to import into the router.	--
PKCS # 12 Certificate	Select the PKCS # 12 certificate file to import into the 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

4.4.4 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. There are two main uses of the GRE protocol: enterprise internal protocol encapsulation and private address encapsulation.

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", "WWAN2", "WAN", or "WLAN".	Not bound

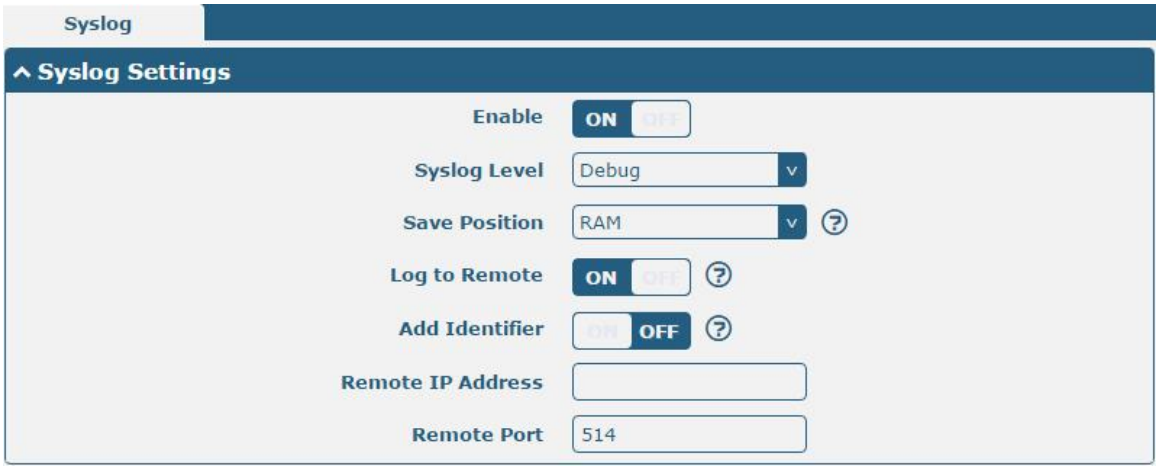
This section allows you to view the status of GRE tunnel.

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.

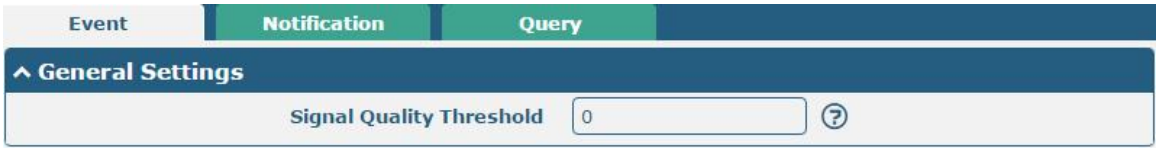
The window is displayed as below when enabling the “Log to Remote” option.



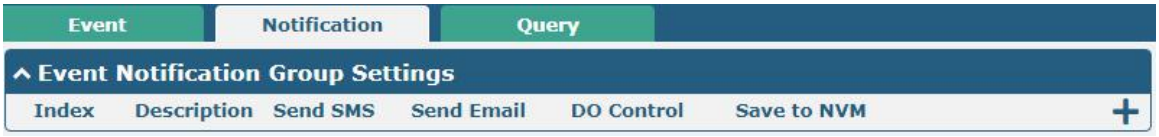
Syslog Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Syslog settings option.	ON
Syslog Level	Select from “Debug”, “Info”, “Notice”, “Warning” or “Error”, which from low to high. The lower level will output more syslog in details.	Debug
Save Position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

4.5.2 Event

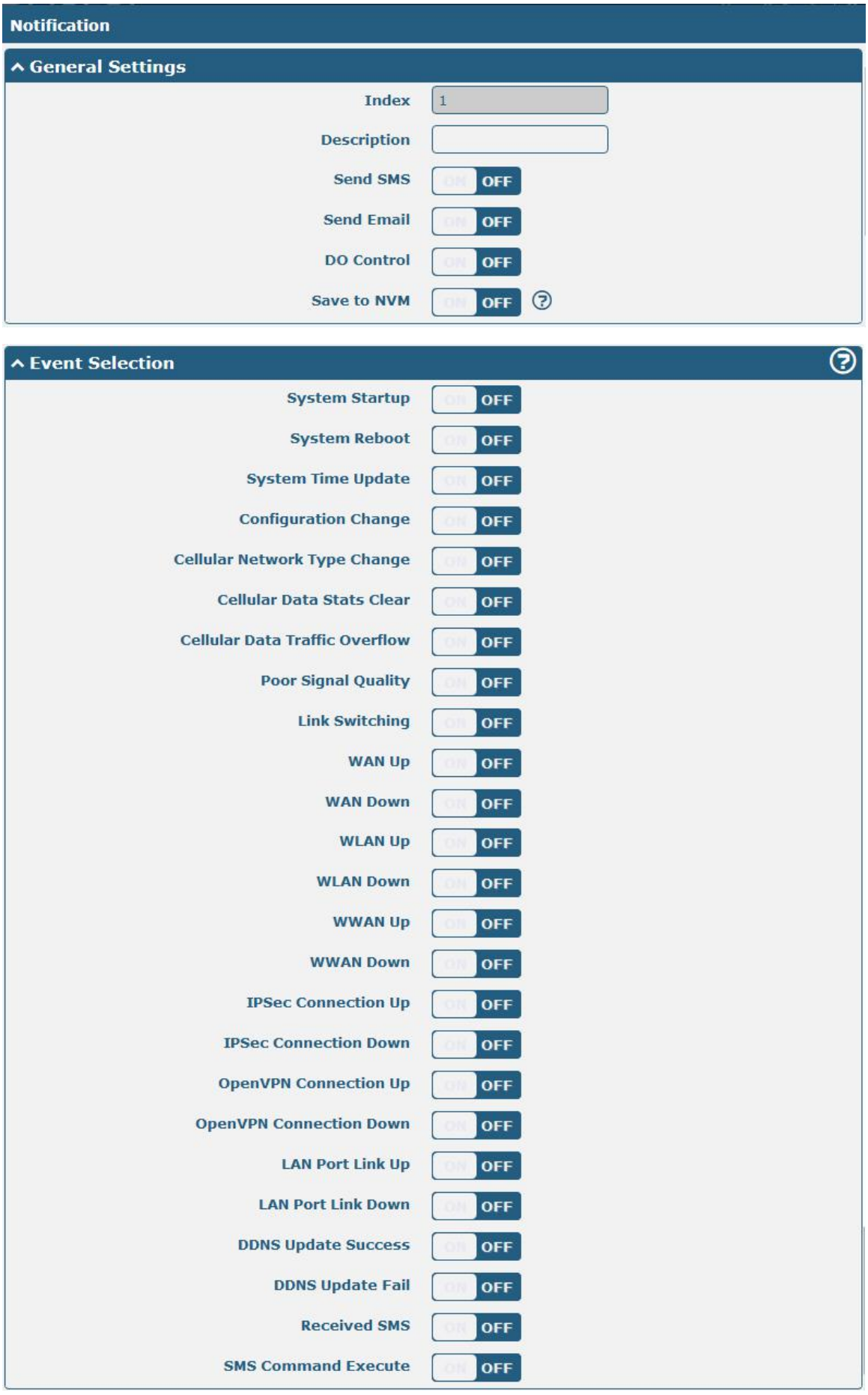
This section allows you to set the event parameters. Event feature provides an ability to send alerts by SMS or Email when certain system events occur.



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

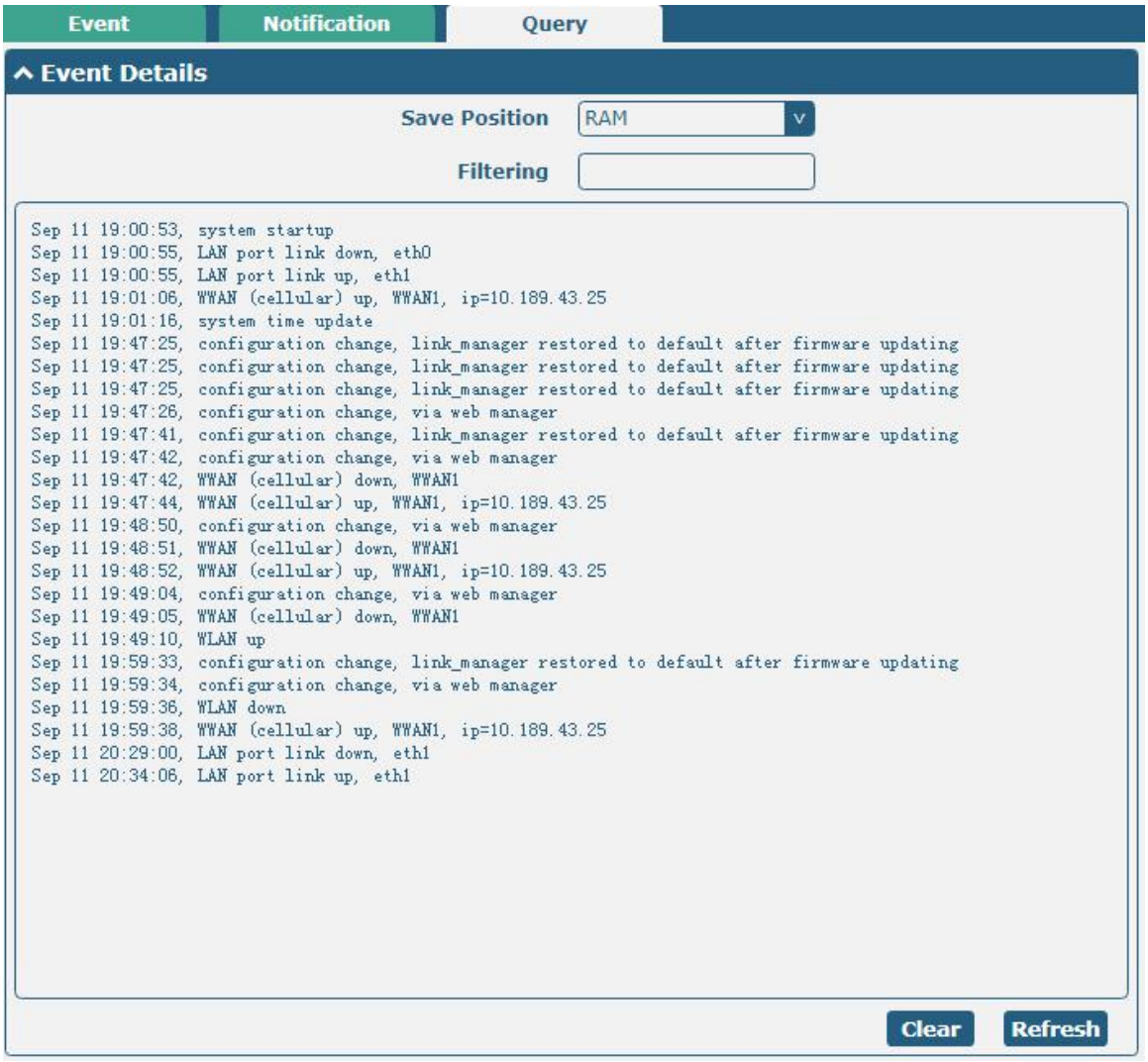


Click + button to add an Event parameters.



General Settings @ Notification		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this group.	Null
Sent SMS	Click the toggle button to enable/disable this option. When enabled, the router will send notification to the specified phone numbers via SMS if event occurs. Set the related phone number in "3.21 Services > Email", and use ';'to separate each number.	OFF
Send Email	Click the toggle button to enable/disable this option. When enabled, the router will send notification to the specified email box via Email if event occurs. Set the related email address in "3.21 Services > Email".	OFF
DO Control	Click the toggle button to enable / disable this option. After it is turned on, the event router will send it to the corresponding DO in the form of Low / High level.	OFF
Save to NVM	Click the toggle button to enable/disable this option. Enable to save event to nonvolatile memory.	OFF

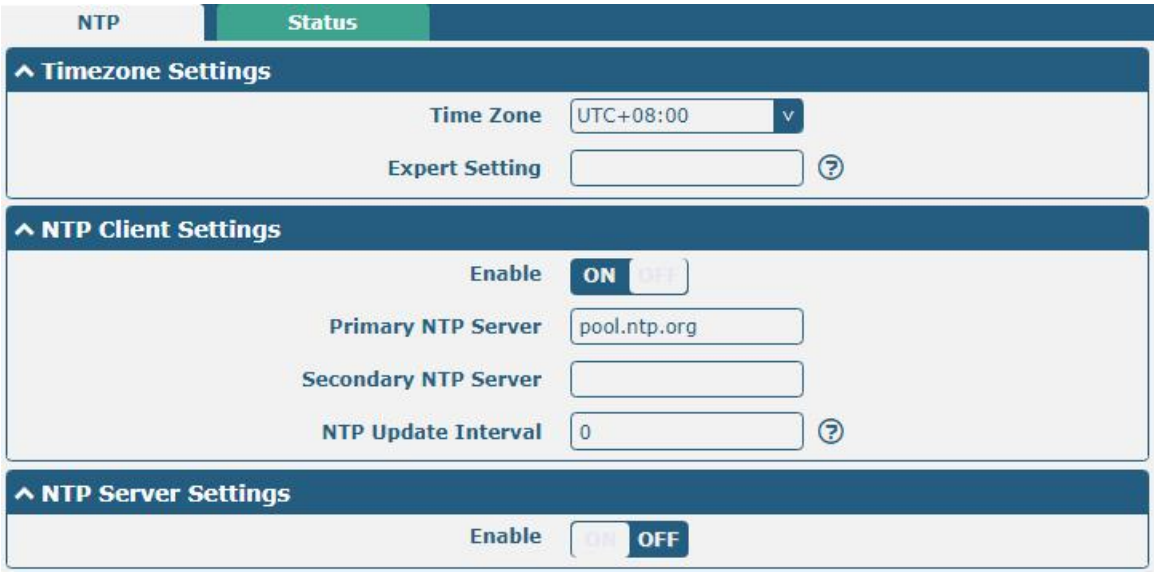
In the following window you can query various types of events record. Click **Refresh** to query filtered events while click **Clear** to clear the event records in the window.



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	Enter the filtering message based on the keywords set by users. Click the "Refresh" button, the filtered event will be displayed in the follow box. Use "&" to separate more than one filter message, such as message1&message2.	Null

4.5.3 NTP

This section allows you to set the related NTP (Network Time Protocol) parameters.



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

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

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**.

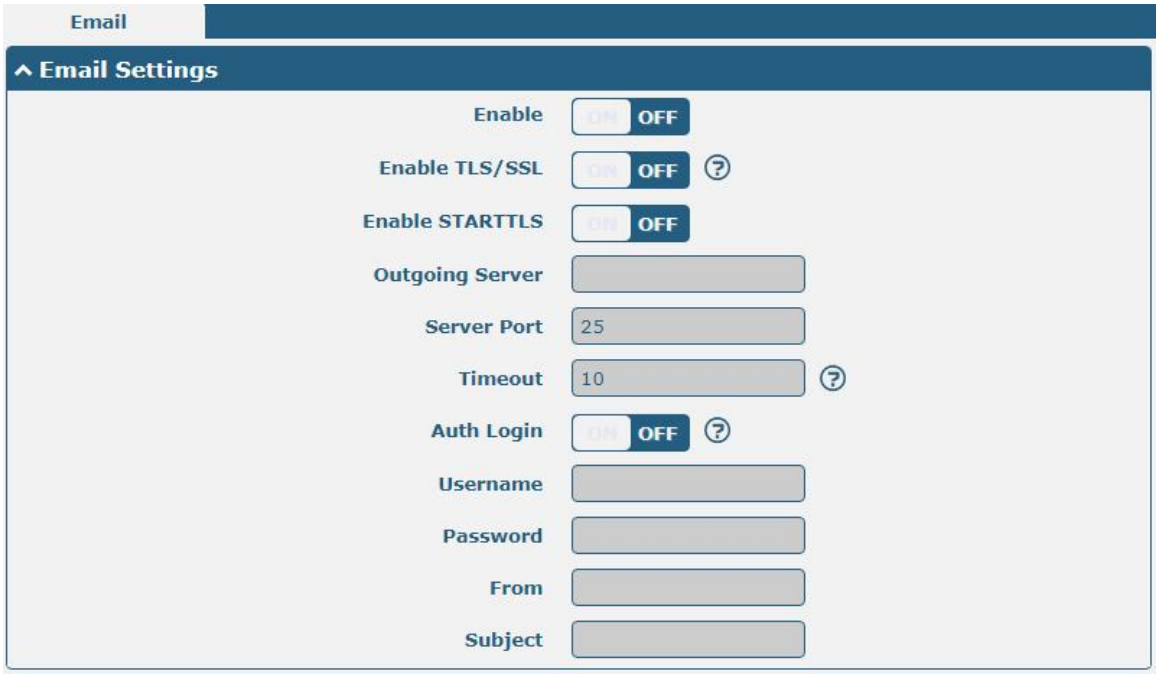
SMS Management Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the SMS Management option. **Note**: If this option is disabled, the SMS configuration is invalid.	ON
Authentication Type	Select Authentication Type from "Password", "Phonenum" or "Both". • Password: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

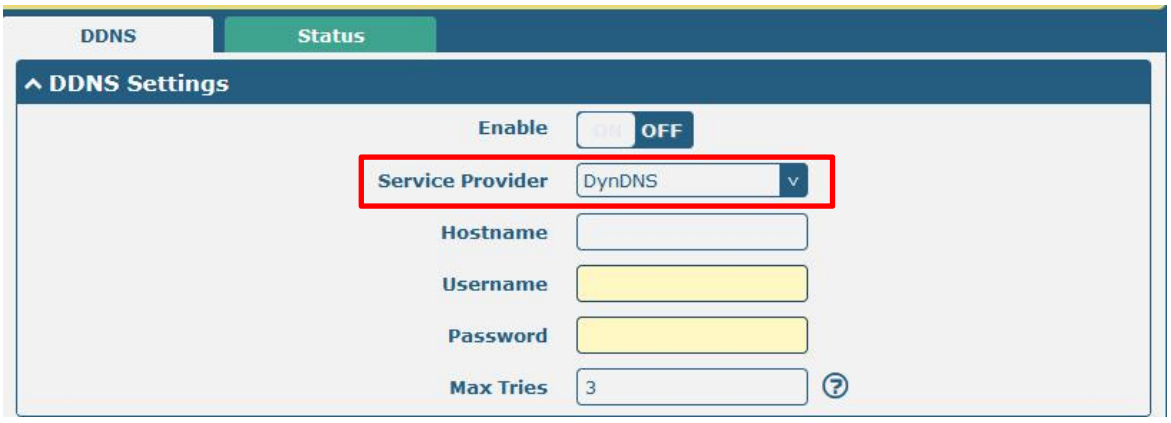
Email function supports to send the event notifications to the specified recipient by ways of email.



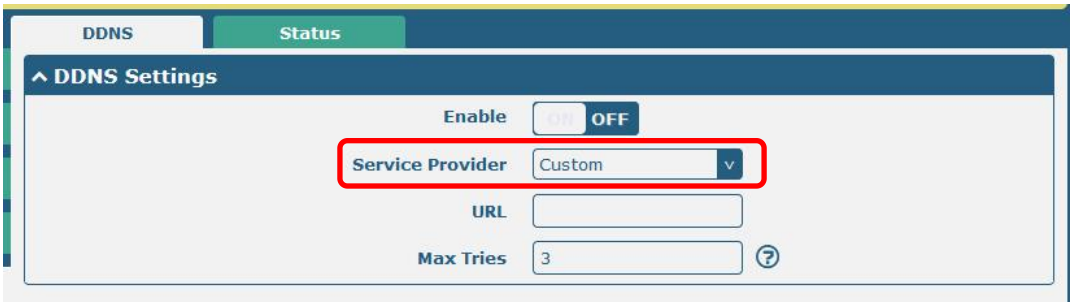
Email Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Email option.	OFF
Enable TLS/SSL	Click the toggle button to enable/disable the TLS/SSL option.	OFF
Enable STARTTLS	Click the toggle button to enable / disable STARTTLS encryption.	OFF
Outgoing server	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 a username and password.	OFF
Username	Enter the username which has been registered from SMTP server.	Null
Password	Enter the password of the username above.	Null
From	Enter the source address of the email.	Null
Subject	Enter the subject of this email.	Null

4.5.6 DDNS

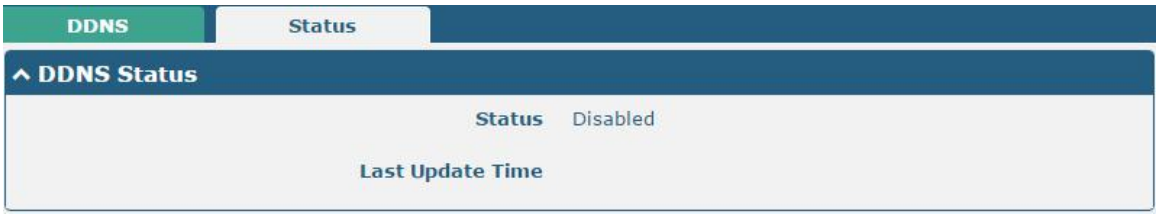
This section allows you to set the DDNS parameters. The Dynamic DNS function allows you to alias a dynamic IP address to a static domain name, allows you whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your connection, so that 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.



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



DDNS Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the DDNS option.	OFF
Service Provider	Select the DDNS service from “DynDNS”, “NO-IP”, “3322” or “Custom”. **Note:** The DDNS service only can be used after registered by Corresponding service provider.	DynDNS
Hostname	Enter the hostname provided by the DDNS server.	Null
Username	Enter the username provided by the DDNS server.	Null
Password	Enter the password provided by the DDNS server.	Null
URL	Enter the URL customized by user.	Null
Max tries	Enter the maximum tries times	3



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

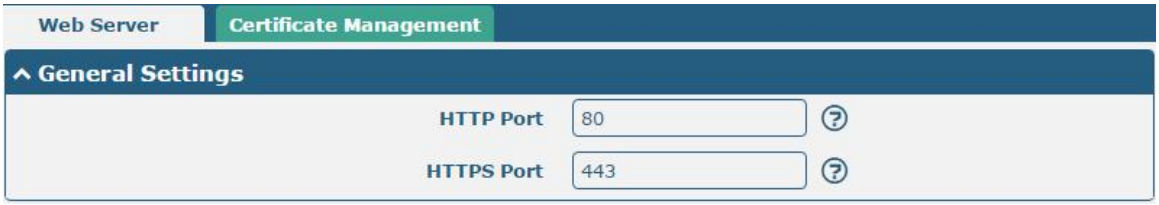
Router supports SSH password access and secret-key access.

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 PC, and then click “Import” to import this key into your router. **Note**: This option is valid when enabling the password logins option.

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 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.	443

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 PC, and then click "Import" to import this file into your router.	--

4.5.9 Advanced

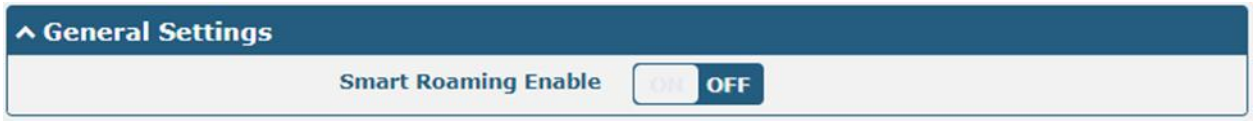
This section allows you to set the Advanced and parameters.

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

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

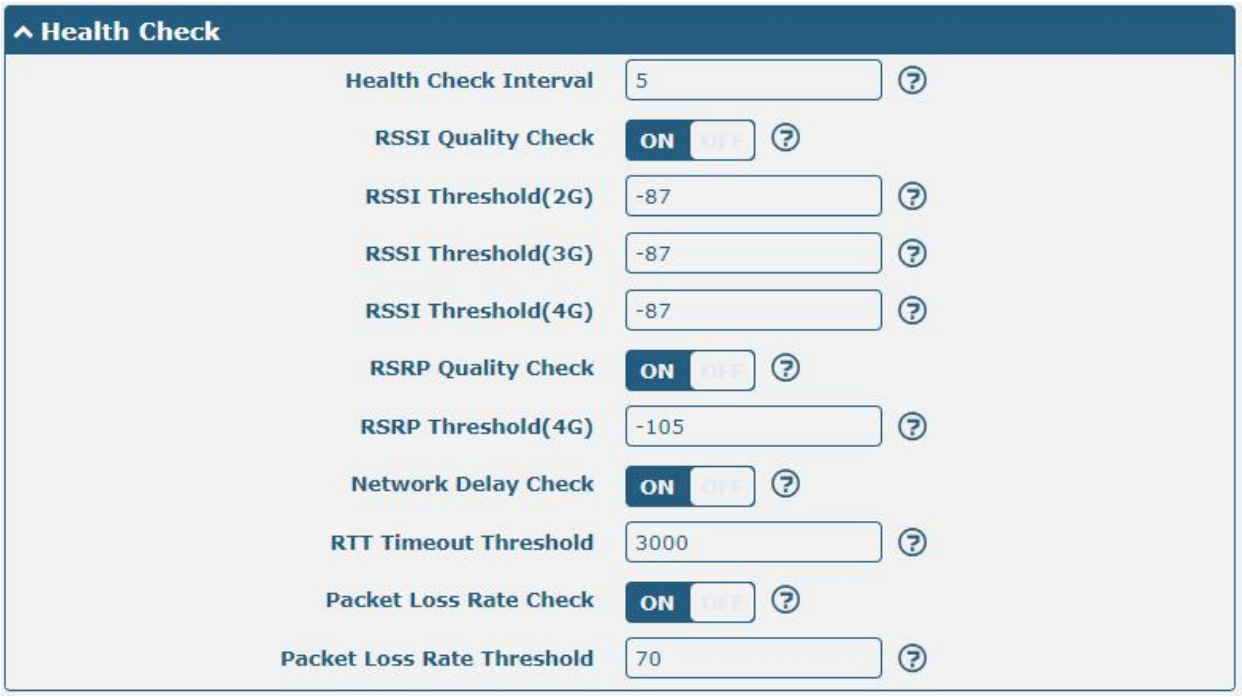
4.5.10 Smart Roaming

Smarting roaming includes general settings, health check, PING settings and advanced settings.



General Setting

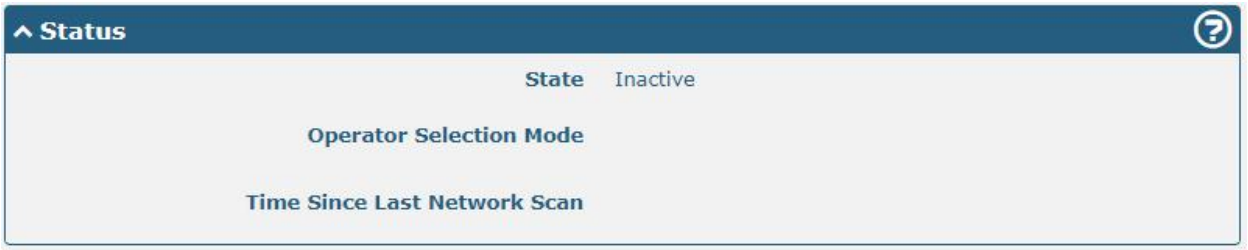
Item	Descriptions	Default
Smart Roaming Enable	Enable Smart Roaming	OFF



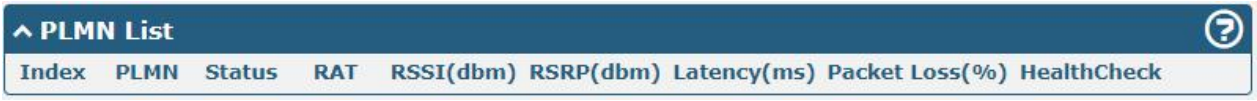
Health Check		
Item	**Descriptions**	**Default**
Health Check Interval	The health check interval for the current connection in minutes. If the health check fails, Smart Roaming will try to switch to another carrier network. Be careful not to set all check conditions to theoretically unattainable values.	5 Minutes
RSSI Quality Check	To enable/disable the "RSSI Quality Check" feature.	ON
RSSI Threshold (2G)	Signal strength threshold for 2G networks.	-87 dBm
RSSI Threshold (3G)	Signal strength threshold for 3G networks.	-87 dBm
RSSI Threshold (4G)	Signal strength threshold for 4G networks.	-87 dBm
RSRP Quality Check	To enable/disable the "RSRP Quality Check" feature.	OFF
RSRP Threshold (4G)	The reference signal received power threshold for 4G networks.	-105 dBm
Network Delay Check	To enable/disable the “Network Delay Check " feature.	ON
RTT Timeout Threshold	The reference signal received power threshold for 4G networks.	3000 ms
Packet Loss Rate Check	To enable/disable the “Packet Loss Rate Check" feature.	ON
Packet Loss Rate Threshold	Packet loss rate threshold value.	70 %

PING Settings		
Item	**Descriptions**	**Default**
Primary Server	The router pings the primary address/domain name to detect if the current connection is always alive.	8.8.8.8
Secondary Server	The router pings the secondary address/domain name to detect if the current connection is always alive.	114.114.114.114
Ping Timeout	Set the Ping timeout.	5 seconds
Ping Tries	The number of ping attempts per health check. Each ping attempt sends 3 ping messages by default, so the total number of ping messages sent per health check is (3 * number of ping attempts).	3 times

Advanced Settings		
Item	**Descriptions**	**Default**
Use Degraded Network	To enable/disable the "Use degraded network" feature. A degraded network is defined as a network that can be connected, but the network quality does not meet the health check thresholds.	OFF
Periodic Restart	Set the period of rebooting "Smart Roaming" function in hours. 0 means no periodic reboot is enabled. Restarting "Smart Roaming" will re-find the available carrier network and reset the current status, because it takes a long time to search the available provider network, the reboot may take 3 to 5 minutes.	0
Daily Restart Time	Set the time point to restart "Smart Roaming" every day in the format of HH:MM (24-hour system). When this item is empty, it means disable the timer reboot.	Null



Status	
Item	**Descriptions**
Status	Display the current status of "Smart Roaming". It includes Scanning, Connecting, Connected and Inactive status, which indicate that the network is searching for available network, connecting network, network is connected and the function is not started respectively.
Operator Selection Mode	Displays how the carrier network is currently selected. These include Automatic and Manual, which refer to automatic selection according to standard specifications and software selection based on network quality, respectively, and the software will cycle through the two methods.
Time Since Last Network Scan	Displays the time elapsed since the last search for available networks. A "Smart Roaming" reboot will refresh this time.



PLMN List	
Item	**Descriptions**
Index	PLMN list index
PLMN	PLMN = MCC + MNC, that is, a combination of mobile country code and mobile network code.
Status	The current network status, including Current, Visible, Forbidden, and Unknown, indicates the current use of this network, the available network, the forbidden network, and the unknown network, respectively.
RAT (dbm)	Current wireless access technologies, including 2G/3G/4G.
RSSI (dbm)	Current signal quality for 3G and 4G networks.
RSRP (dbm)	Current reference signal reception power for 4G networks.
Latency	Current network latency.
Packet Loss (%)	Current network packet loss rate.
Health Check	The current health check status, including Pending, Good, Degraded, and Failed, indicates that the current network has not yet been health checked; the network quality is good; the network is degraded; and the network quality is poor (including disconnected or does not meet the health check threshold), respectively.

4.6 Edge2Cloud

4.6.1 Edge2Cloud

Edge2Cloud (E2C) is a series of software collections running in the ROS operating system embedded in the Robustel Smart Router device, which can provide various functions of the IoT router at the hardware and software levels and solve the problem of data interfacing between traditional industrial device and the cloud platform.

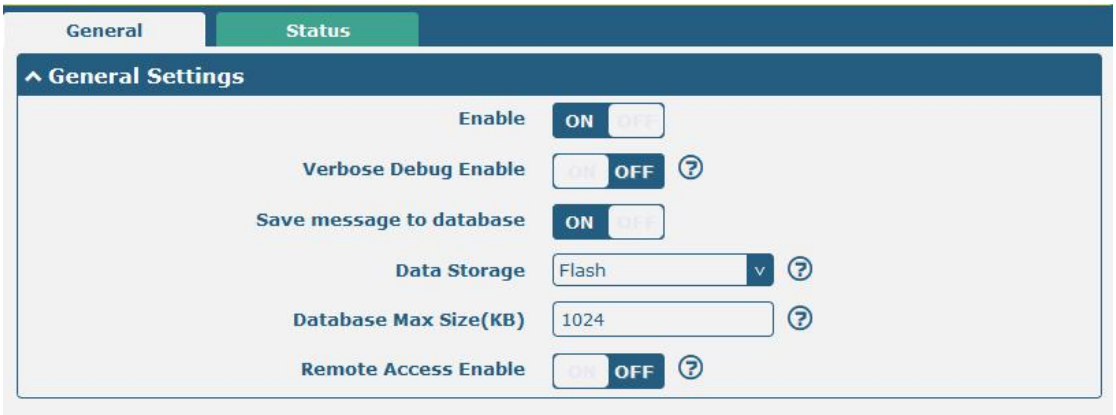
There are three types of E2C: Southbound APP, Northbound APP and Broker.

Southbound APP	Broker	Northbound APP
• Collect data according to the configuration and protocol (Modbus, OPCUA, ELA, S7 PLC etc.) • Encapsulate the collected data into JSON object • Send the JSON string as QPID body to broker APP the message address is the public address of northbound APP • Get the control instruction message from E2C_Broker at its own address, and send the response to E2C_Broker after processing the message.	• Receive and send AMQP message • Store the unconsumed message into the database for message persistence. • Database storage size configuration • Provide remote debugging service. Can inspect the message content from northbound and southbound directions	• Log in the corresponding cloud platform according to UCI configuration and keep online • Receive JSON data from broker APP, and adjust the format to match the cloud platform's requirements. Northbound interface doesnt care about the data type and content. • Subscribe to corresponding topics in the cloud, forward the control command from cloud platform to broker APP and vice-versa.

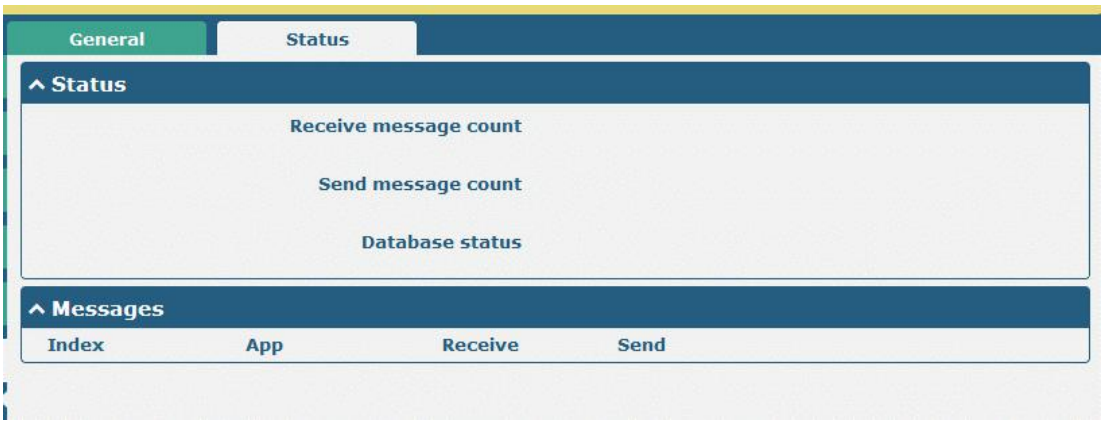
The latest ROS firmware has integrated E2C Broker, users can use the full functionality of Edeg2Cloud by choosing to install the corresponding Southbound APP and Northbound APP according to their needs.

4.6.2 E2C Broker

This section is used to set E2C Broker parameters and view the operational status of E2C Broker. Click "**Edge2Cloud > E2C Broker**" to display the following.



E2C Broker Settings		
Item	**Descriptions**	**Default**
General Settings		
Enable	Enable or disable E2C Broker	OFF
Verbose Debug Enable	Enable or disable more detailed verbose debug	OFF
Save message to database	Whether the messages received by Broker are saved to the database.	ON
Data Storage	Database file storage area, optional: RAM, FLASH, SD-Card and USB-Storage.	FLASH
Database Max Size (kB)	The maximum size of the database file, in KB.	1024
Remote Access Enable	Whether to support sending and receiving messages through the web interface.	OFF

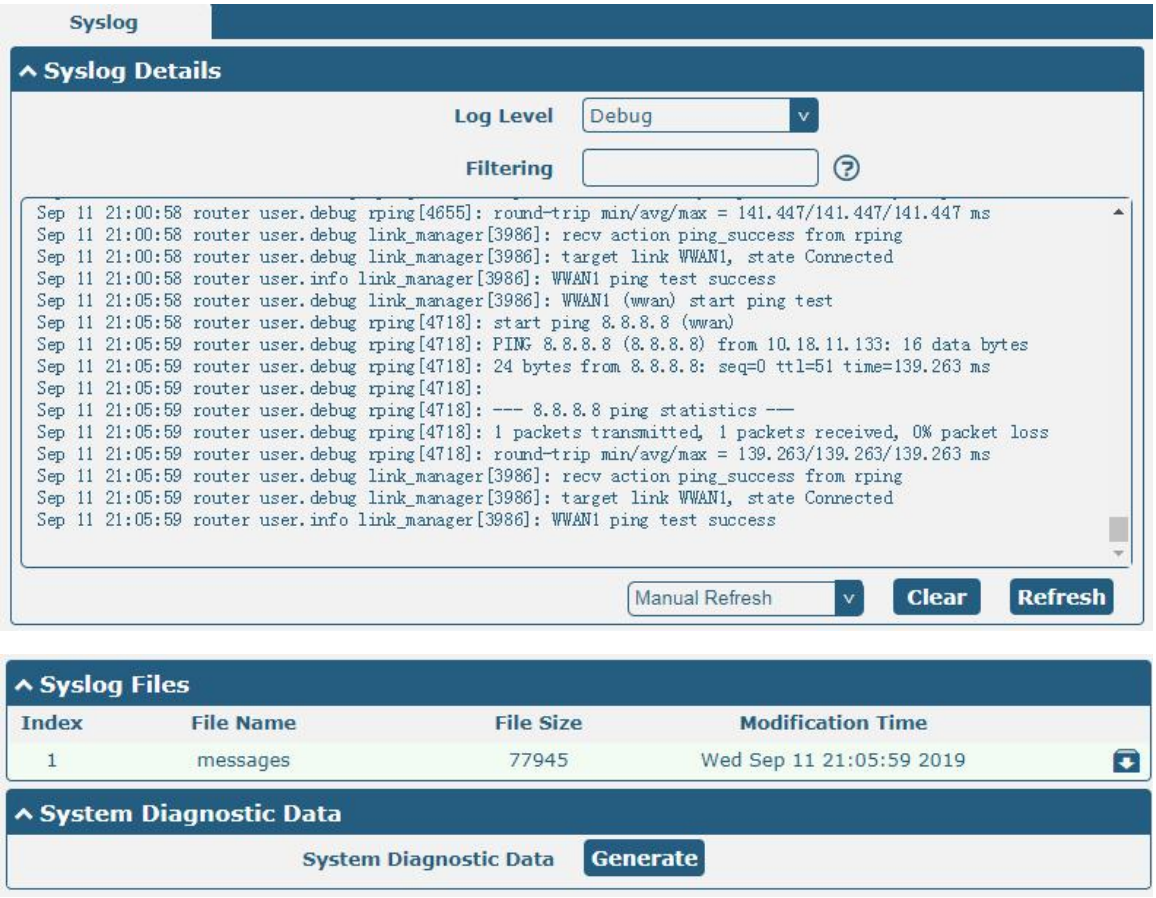


E2C Broker Status	
Item	**Descriptions**
Status	
Receive message count	The number of MQ messages received by Broker.
Send message count	Debugging of MQ messages sent by Broker.
Database status	Available means that the database is available and Space exceed means that the database capacity has reached the set maximum.
Messages	
App	Edge2Cloud southbound and northbound app name.
Receive	The number of messages received from the application.
Send	The number of messages sent to the reapplication.

4.7 System

4.7.1 Debug

This section allows you to check and download the syslog details. Click "**Service > Syslog > Syslog Settings**" to enable the syslog.



Syslog		
Item	**Description**	**Default**
Syslog Details		
Log Level	Select from "Debug", "Info", "Notice", "Warn", "Error" which from low to high. The lower level will output more syslog in detail.	Debug
Filtering	Enter the filtering message based on the keywords. Use "&" to separate more than one filter message, such as "keyword1&keyword2".	Null
Refresh	Select from "Manual Refresh", "5 Seconds", "10 Seconds", "20 Seconds" or "30 Seconds". You can select these intervals to refresh the log information displayed in the follow box. If selecting "manual refresh", you should click the refresh button to refresh the syslog.	Manual Refresh
Clear	Click the button to clear the syslog.	--
Refresh	Click the button to refresh the syslog.	--
Syslog Files		

Syslog Files List	It can show at most 5 syslog files in the list, the files' name range from message0 to message 4. And the newest syslog file will be placed on the top of the list.	--
System Diagnosing Data		
Generate	Click to generate the syslog diagnosing file.	--

4.7.2 Update

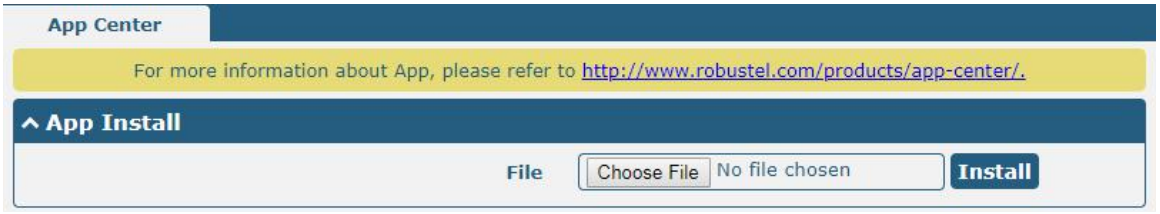
This section allows you to upgrade the router system and implement system update by importing and updating firmware files. Import a firmware file from the PC to the router, click Update and restart the device as prompted to complete the firmware update.

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

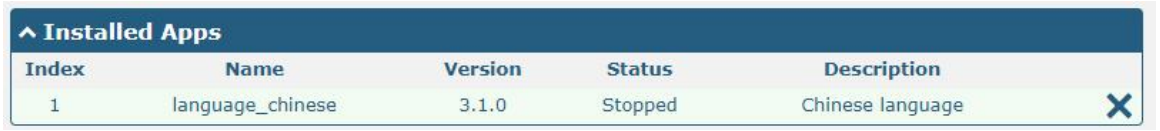
4.7.3 App Center

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.



The successfully installed app will be displayed in the following list. Click ✕ to uninstall the app.

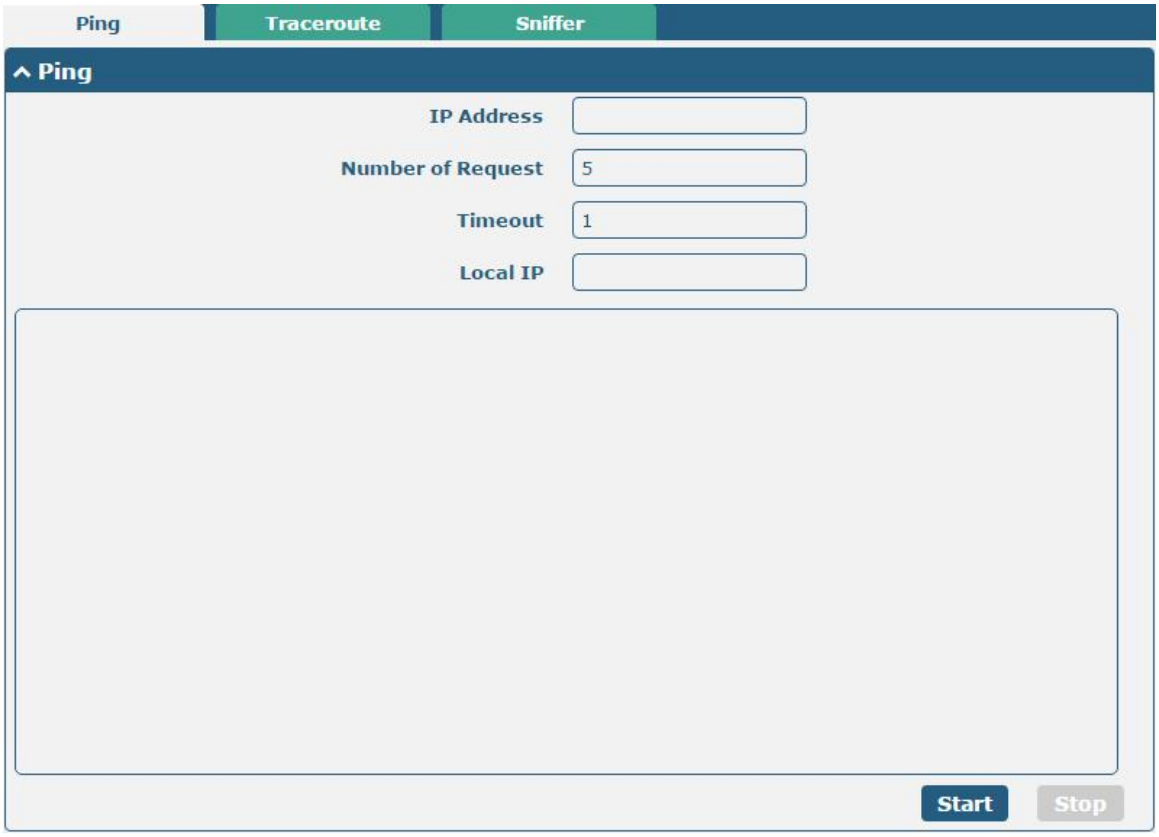


App Center		
Item	**Description**	**Default**
App Install		
File	Click on "Choose File" to locate the App file from your PC, and then click Install to import this file into your router. **Note**: File format should be *xxx.rpk*, e.g. *R2011-robustlink-1.0.0.rpk*.	--
Installed Apps		
Index	Indicate the ordinal of the list.	--
Name	Show the name of the App.	Null

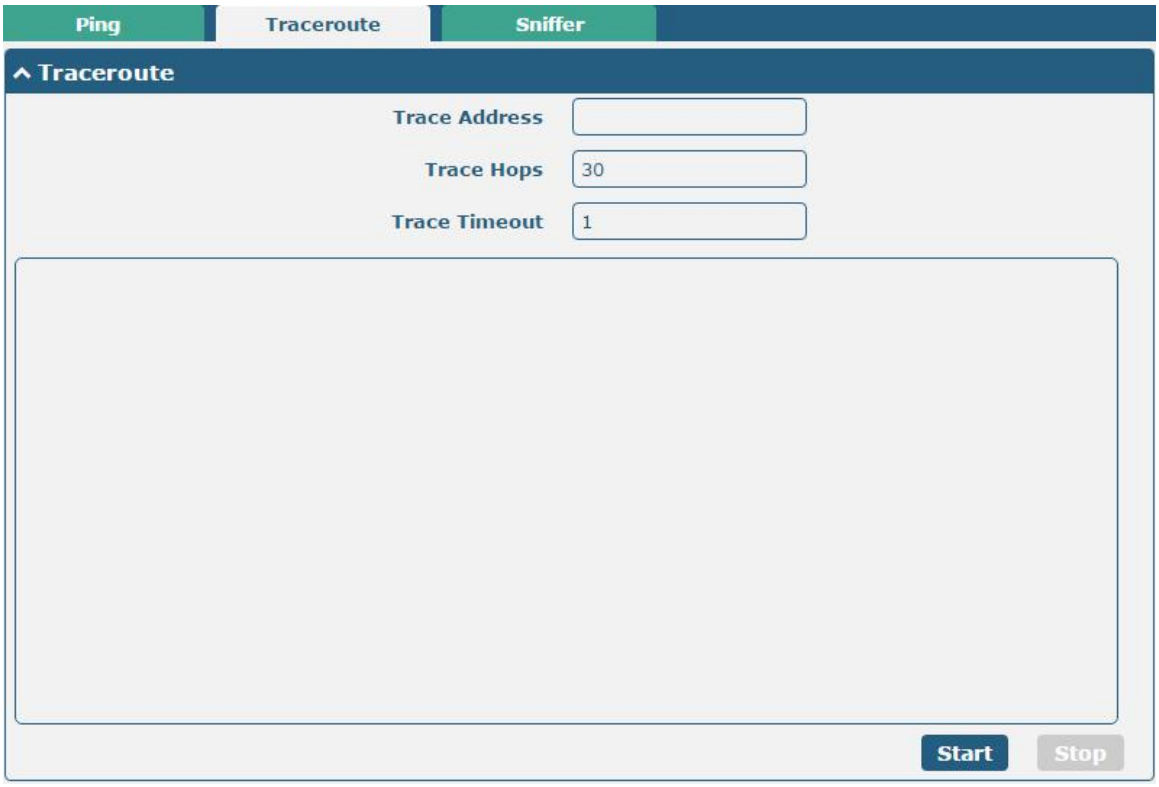
App Center		
Item	**Description**	**Default**
Version	Show the version of the App.	Null
Status	Show the status of the App.	Null
Description	Show the description for this App.	Null

4.7.4 Tools

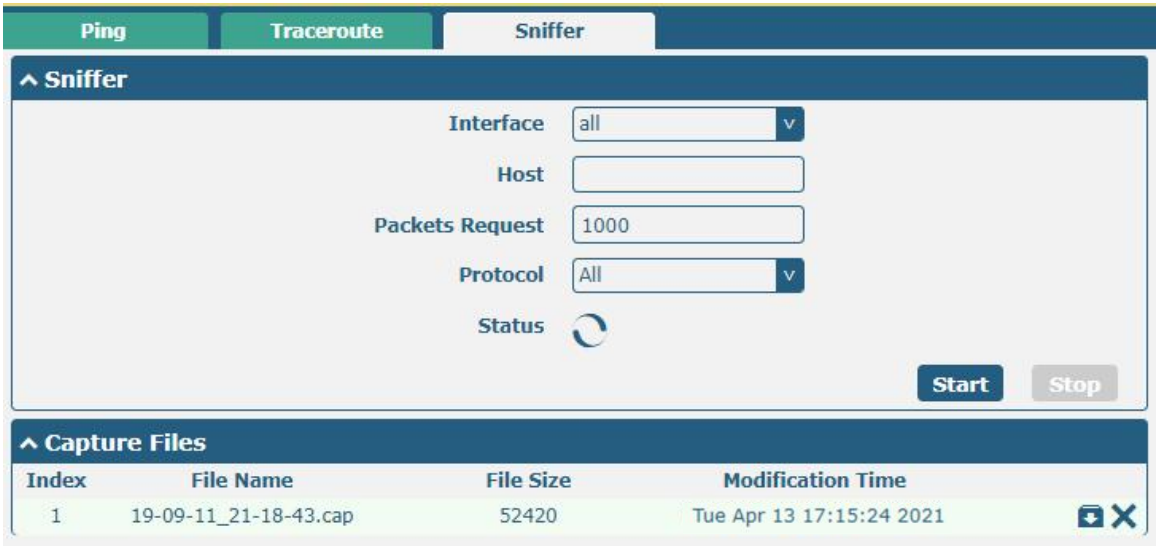
This section provides users three tools: Ping, Traceroute and Sniffer. The Ping is used to check the network connectivity.



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



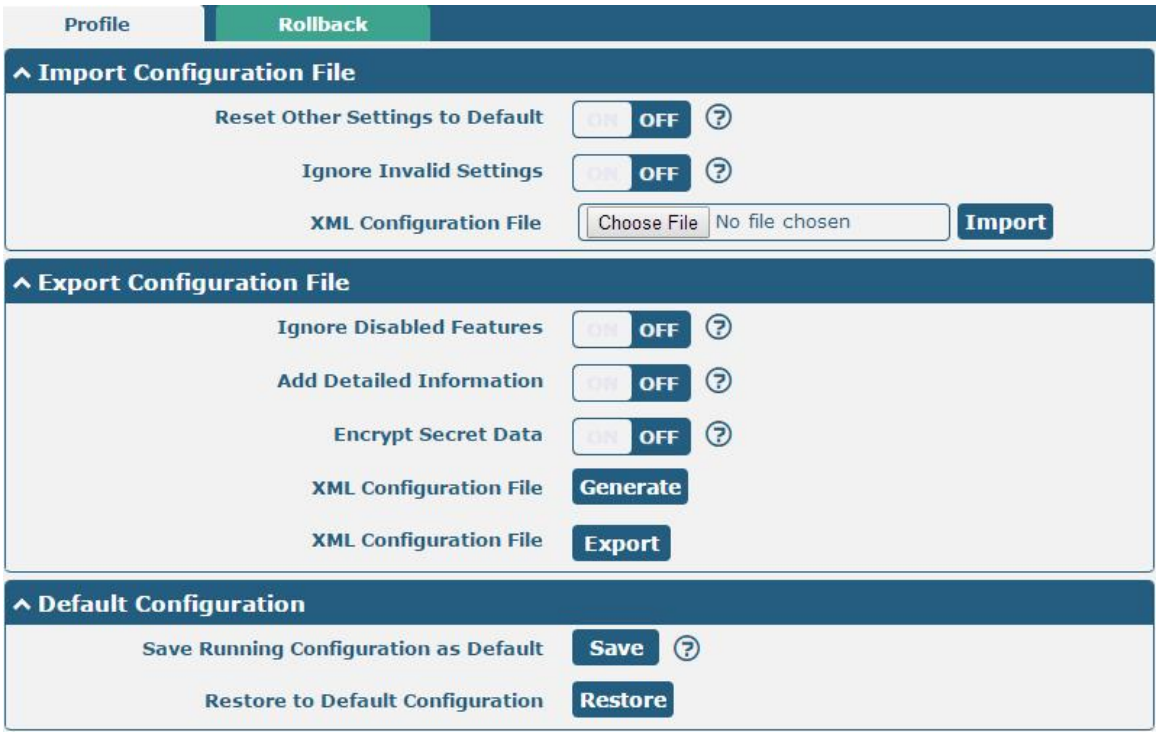
Traceroute		
Item	**Description**	**Default**
Trace Address	Enter the trace's destination IP address or destination domain.	Null
Trace Hops	Specify the max trace hops. Router will stop tracing if the trace hops has met max value no matter the destination has been reached or not.	30
Trace Timeout	Specify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

4.7.5 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 “OFF” to ignore invalid settings.	ON
XML Configuration File	Click on Choose File to locate the XML configuration file from your PC, and then click Import to import this file into your router.	--

Export Configuration File		
Ignore Disabled Features	Click the toggle button as "OFF" to ignore the disabled features.	OFF
Add Detailed Information	Click the toggle button as "On" to add detailed information.	OFF
Encrypt Secret Data	Click the toggle button as "ON" to encrypt the secret data.	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 Save button to save the current running parameters as default configuration.	--
Restore to Default Configuration	Click Restore 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.	--

4.7.6 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.

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

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

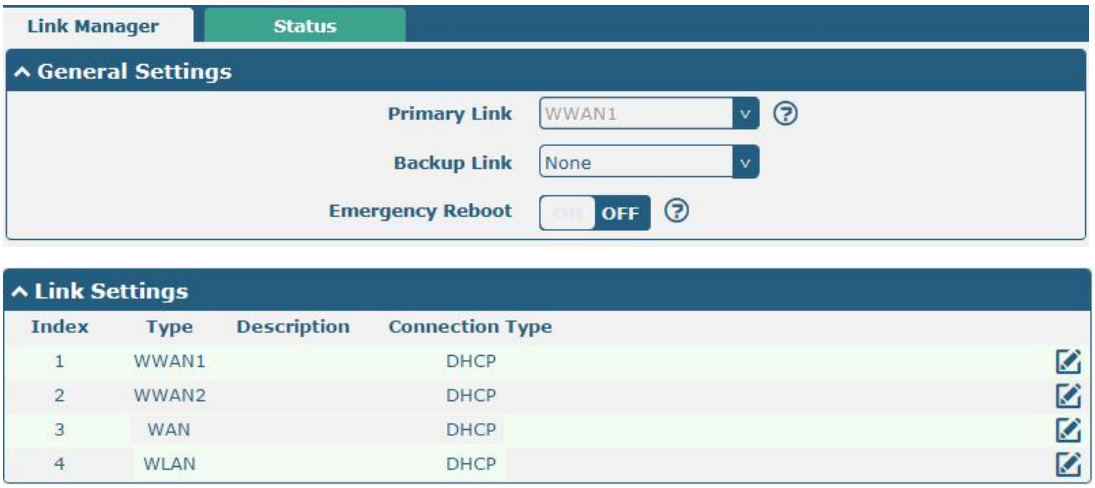
Common User Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Role	Select from “Visitor” and “Editor”. • Visitor: Users only can view the configuration of router under this level • Editor: Users can view and set the configuration of router under this level	Visitor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

5 Configuration Examples

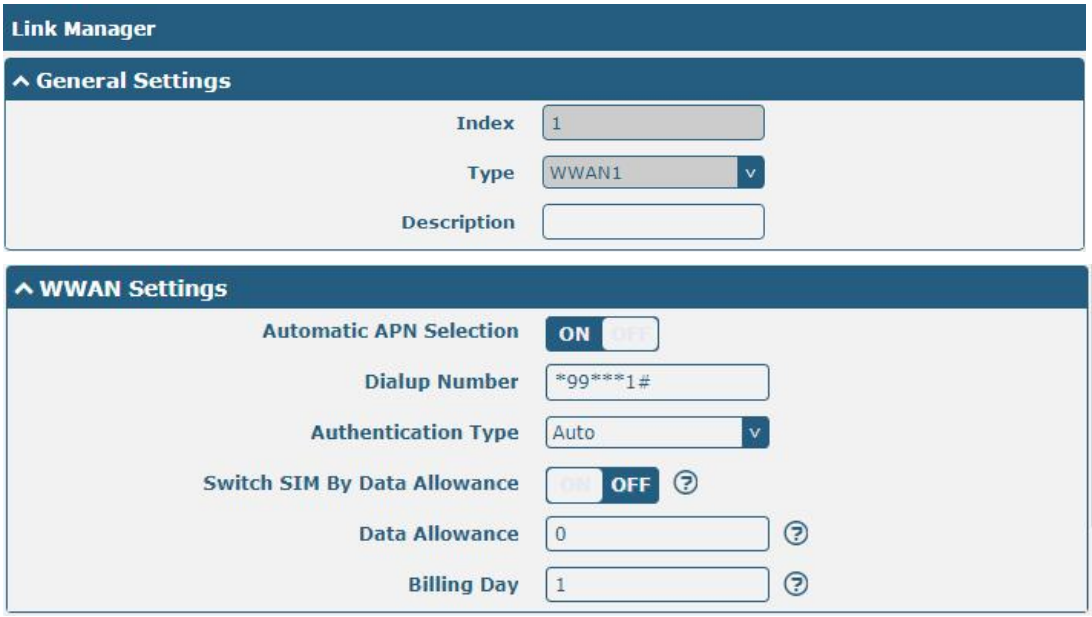
5.1 Cellular

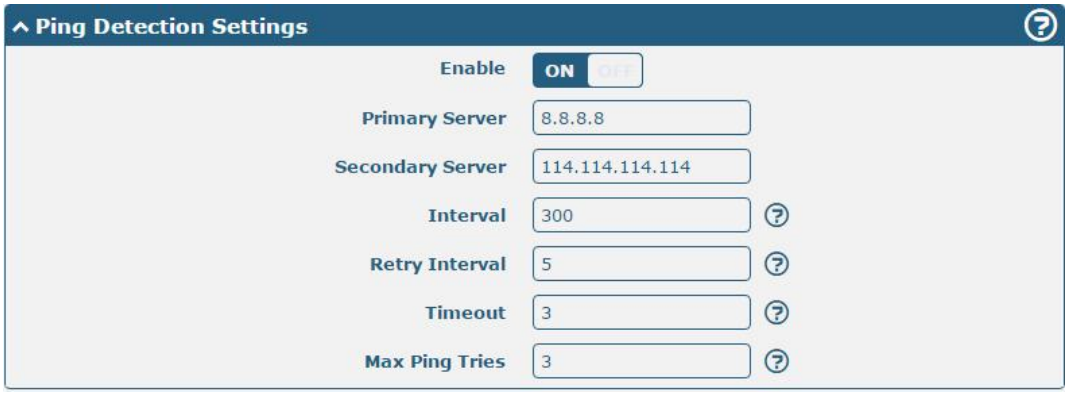
5.1.1 Cellular Dial-Up

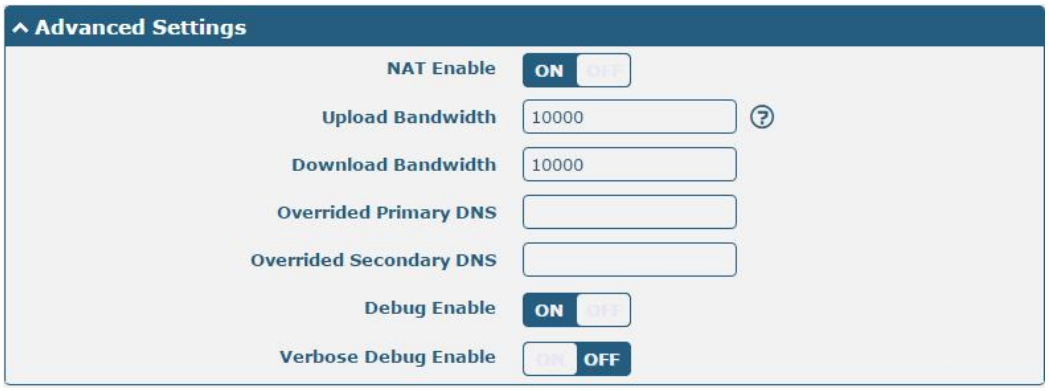
This section shows you how to configure the primary and backup SIM card for Cellular Dial-up. Connect the router correctly and insert two SIM, then open the configuration page. Under the homepage menu, click "**Interface > Link Manager > Link Manager > General Settings"**, choose "WWAN1" as the primary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



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

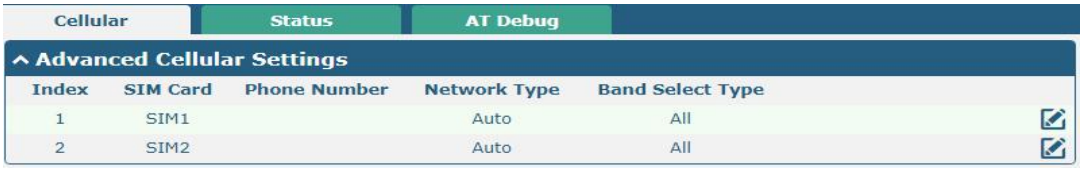




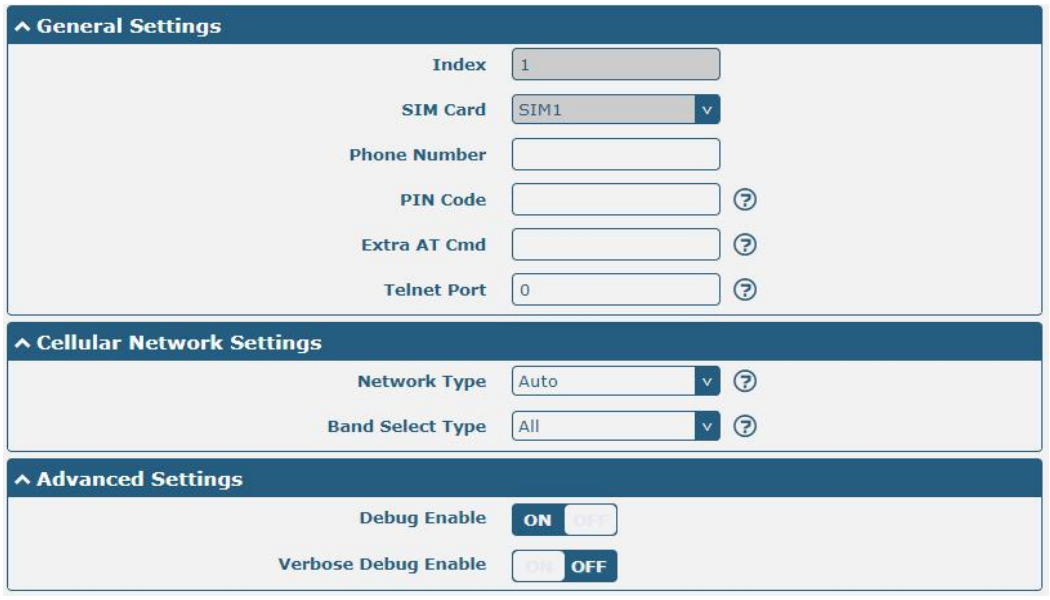


When finished, click "**Submit > Save & Apply"** for the configuration to take effect.

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



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



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

5.1.2 SMS Remote Control

R2011 supports remote control via SMS. You can use following commands to get the status of the router, and set all the parameters of the router.

SMS command have the following structures:

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

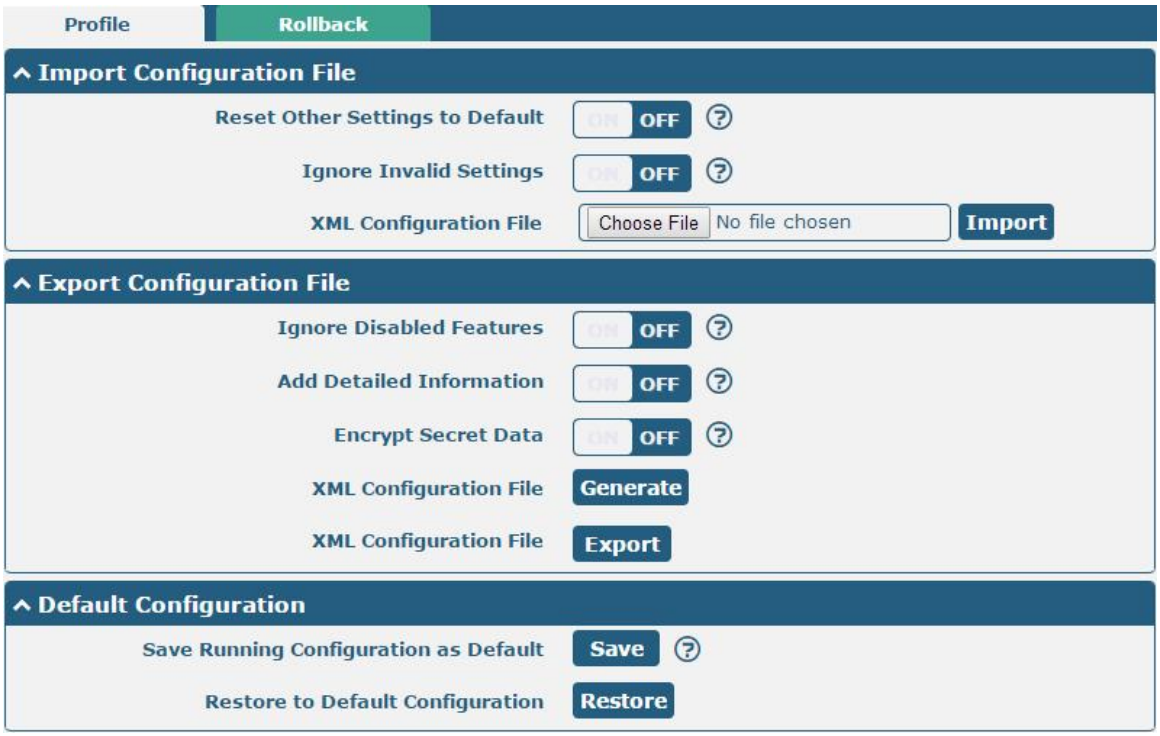
Note: All command symbols must be entered in the half-angle mode of the English input method.

SMS command Explanation:

1. Username and Password: Use the same username and password as WEB manager for authentication.
2. **cmd1, cmd2, cmd3 to cmdn**, the command format is the same as the CLI command, more details about CLI cmd please refer to **6.1 Introductions for CLI**.

   Note: Download the configure XML file from the configured web browser. The format of SMS control command can refer to the data of the XML file.

   Go to "**System > Profile > Export Configuration File"**, click **Generate** to generate the XML file and click **Export** to export the XML file.



XML command:

```
<lan>
<network max_entry_num="5">
<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 commands packed in a single SMS.
4. E.g.

admin:admin;status system

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

SMS received:

hardware_version = 1.0

firmware_version = beta210618

firmware_version_full = "beta210618 (Rev 4250)"

kernel_version = 4.9.152

device_model = R2011

serial_number = ""

uptime = "0 days, 01:25:16"

system_time = "Tue Apr 21 17:09:04 2021"

ram_usage = "77M Free/128M Total"

admin:admin;reboot

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

SMS received:

OK

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

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

SMS received:

OK

OK

admin:admin;set lan network 1 interface lan0;set lan network 1 ip 172.16.24.24;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

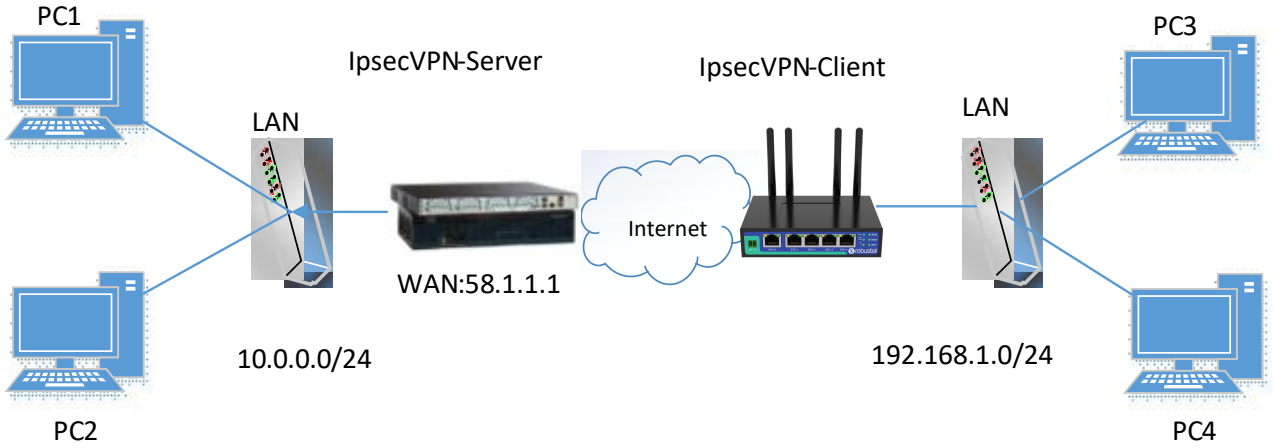
OK

OK

5.2 VPN Configuration Examples

5.2.1 IPsec VPN

IPsec VPN topology (server-side and client-side IKE and SA parameters must be configured the same).



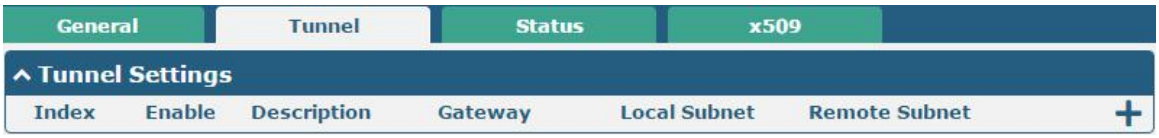
IPsecVPN_Server:

Cisco 2811:

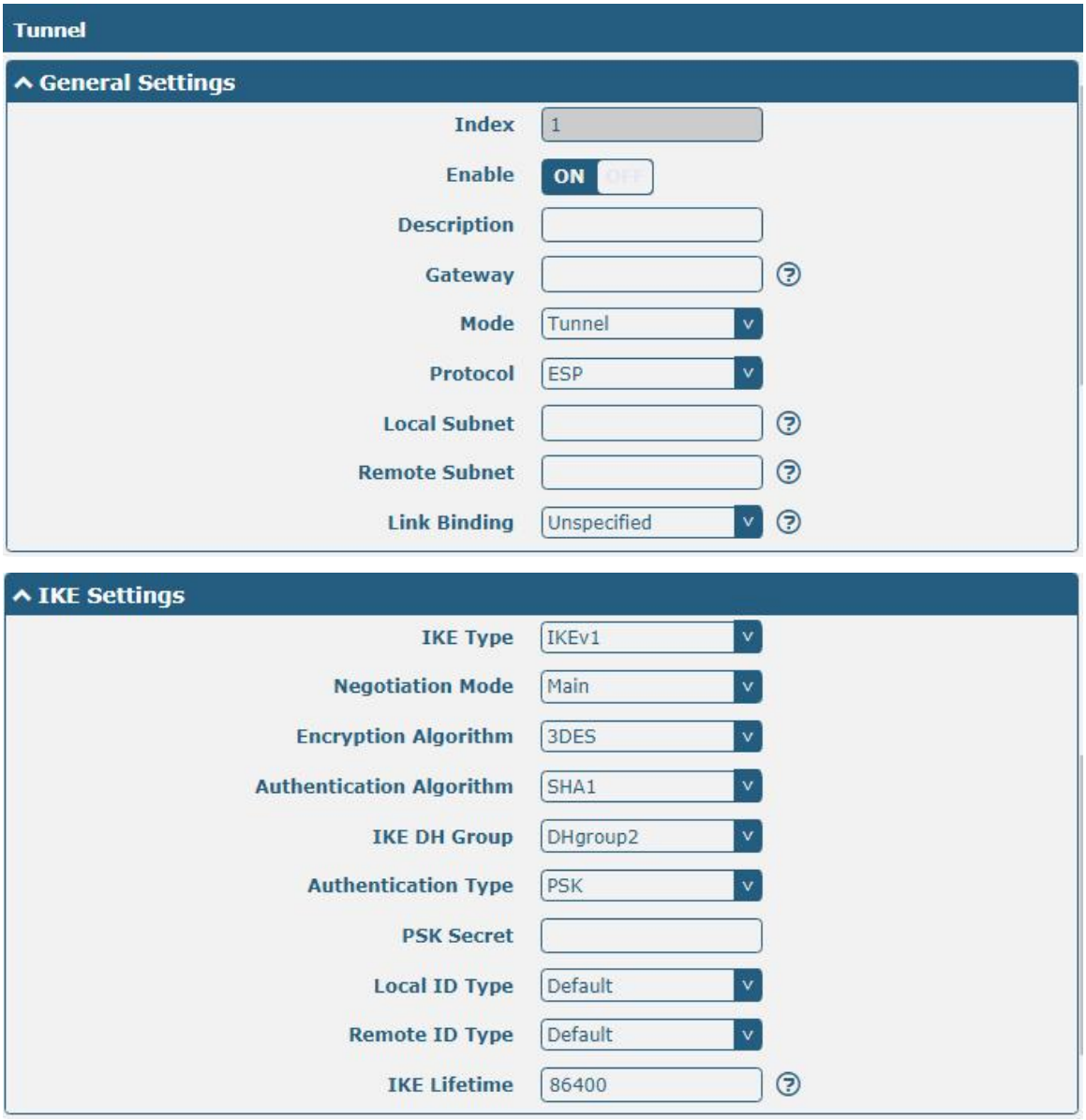
```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set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


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


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


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


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

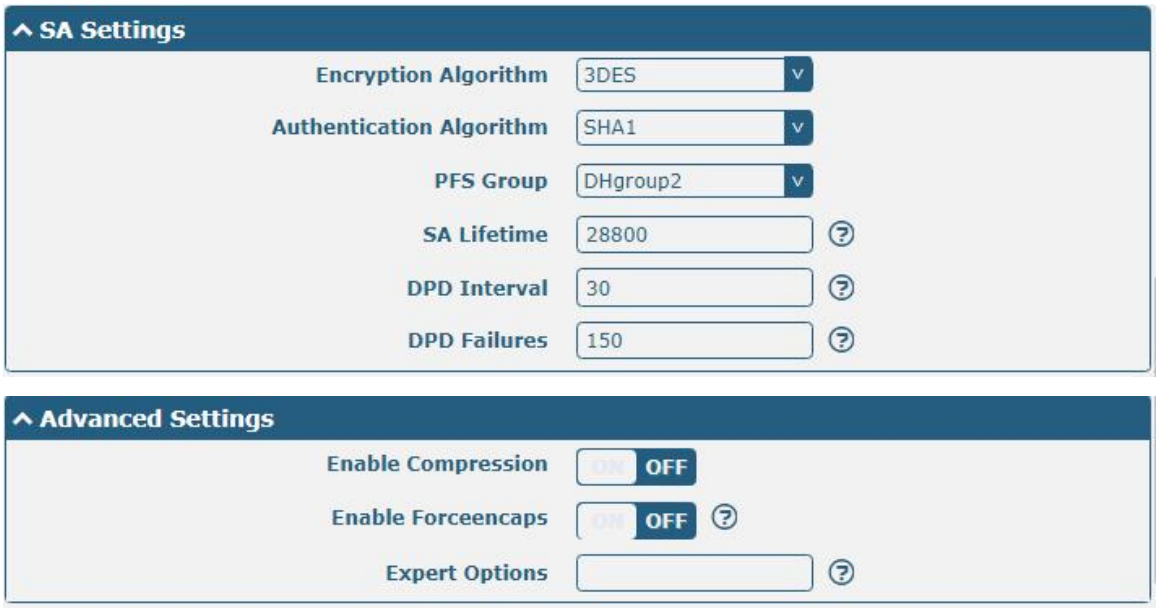
IPsec VPN_Client:

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



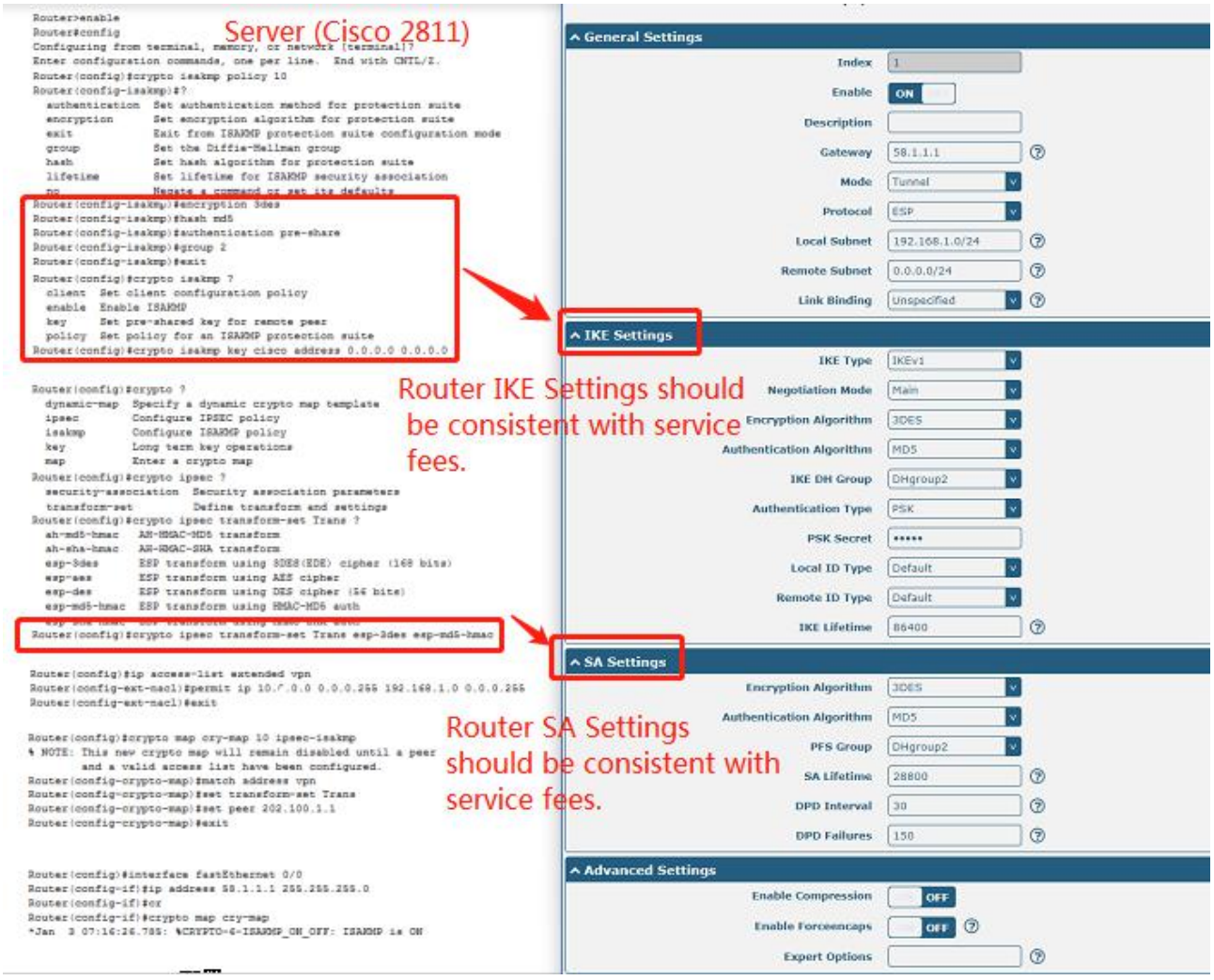
Click + button and set the parameters of IPsec Client as below.





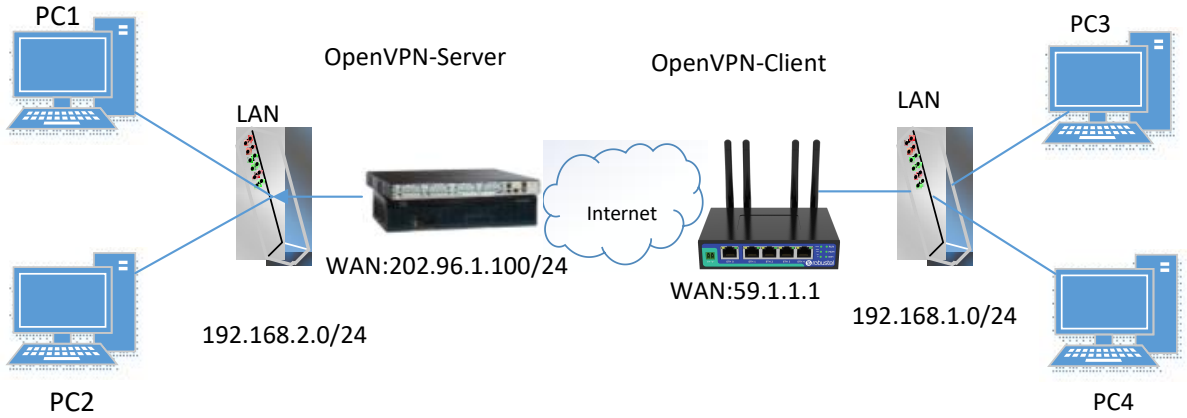
When finished, click "**Submit > Save & Apply"** for the configuration to take effect.

The comparison between server and client is as below.



5.2.2 OpenVPN

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



OpenVPN_Server:

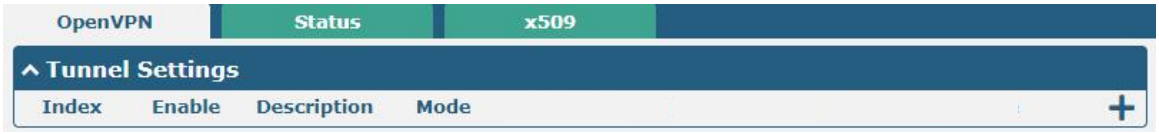
Generate relevant OpenVPN certificate on the server side firstly, and refer to the following commands to configuration the Server:

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

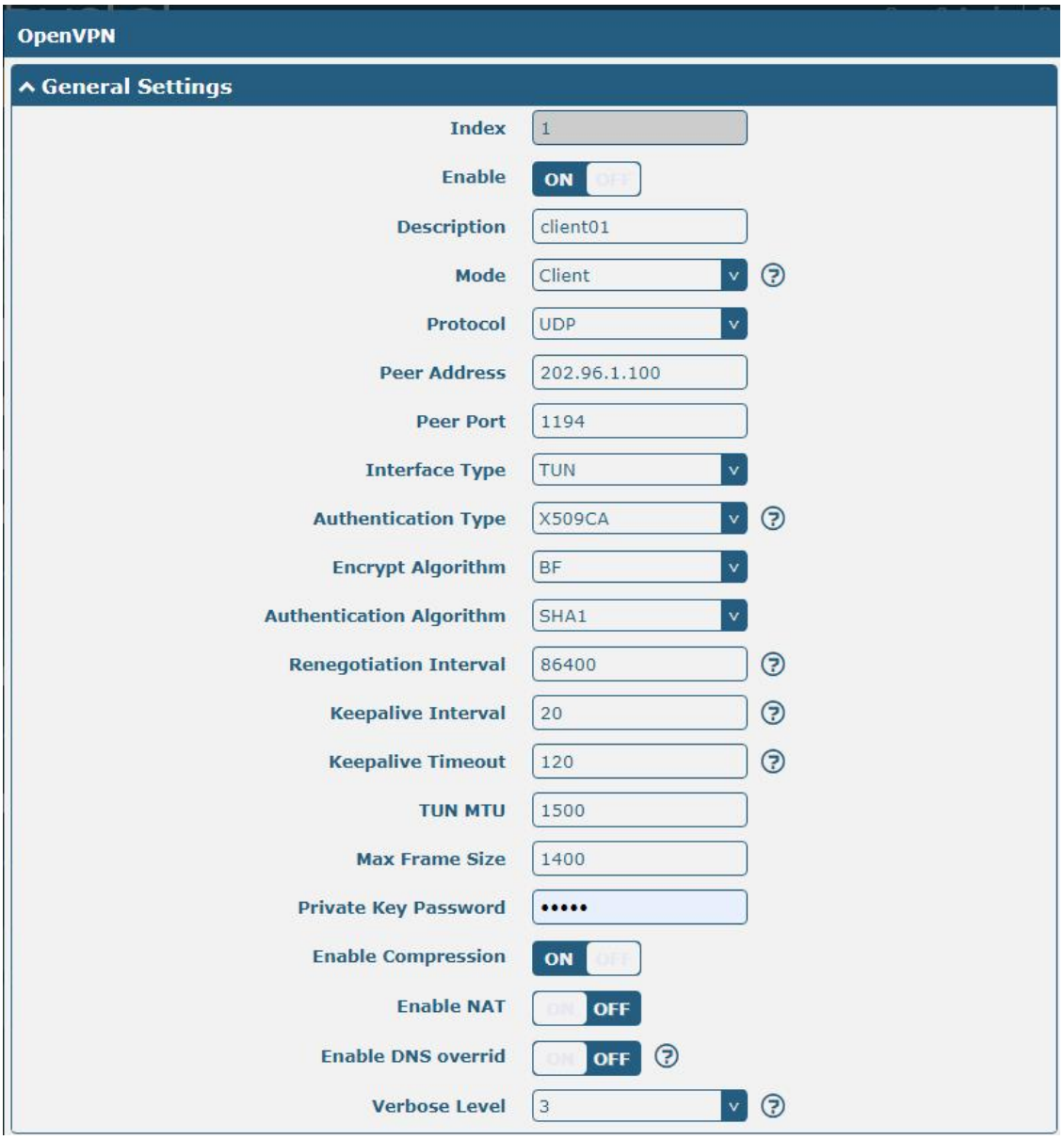
Note: For more configuration details, please contact your technical support engineer.

OpenVPN_Client:

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



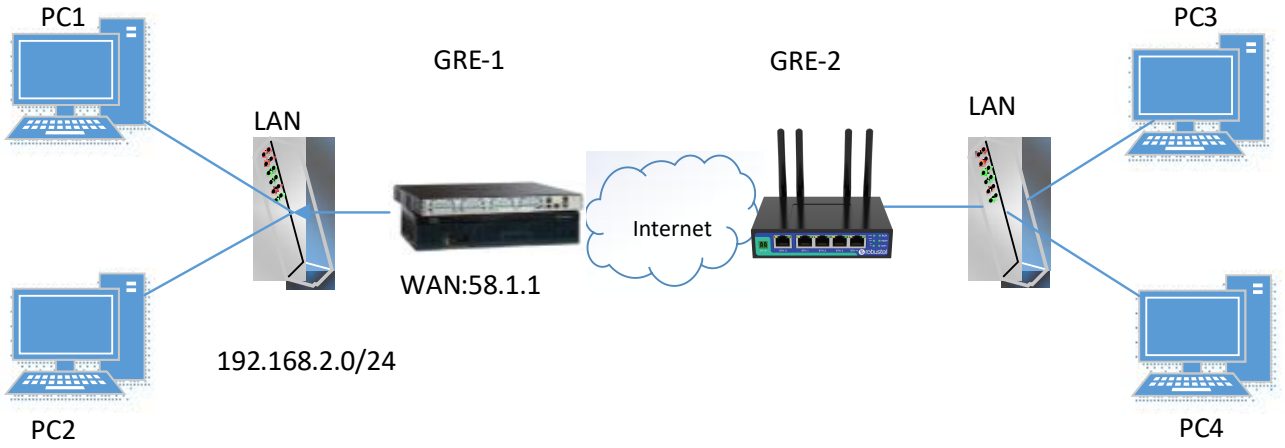
Click + to configure the Client01 as below.



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

5.2.3 GRE VPN

GRE VPN topology



GRE-1：

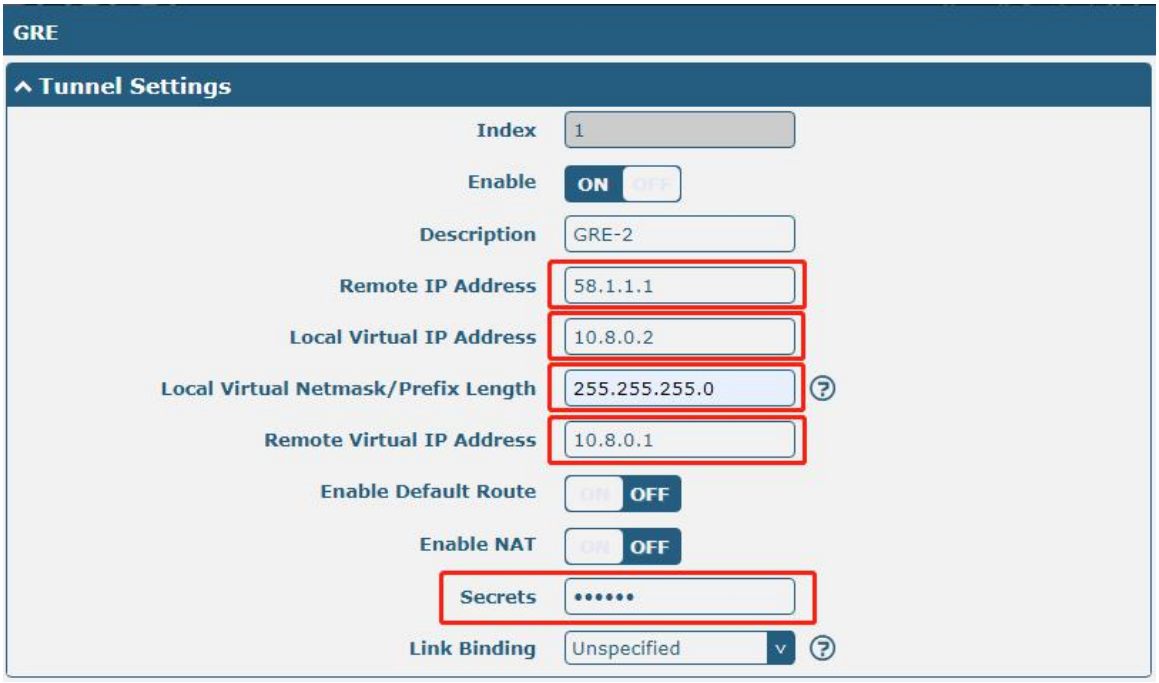
The window is displayed as below by clicking "**VPN > GRE > GRE"**.

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

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

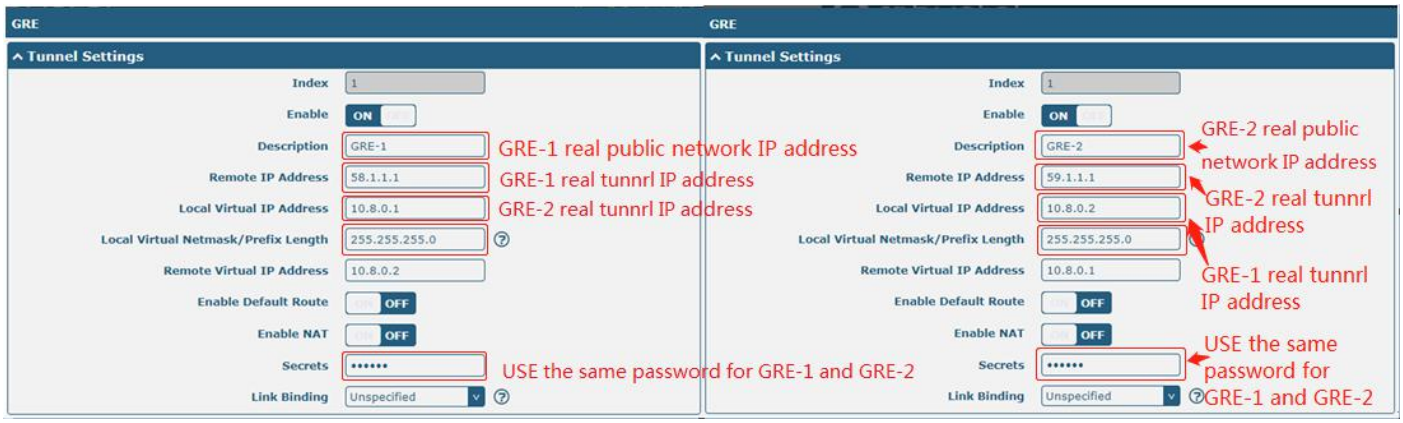
GRE-2:

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.



6 Introductions for CLI

6.1 What Is CLI

Command-line interface (CLI) is a software interface providing another way to set the parameters of equipment from the SSH or through a telnet network connection. After establishing a Telnet or SSH connection with the router, enter the login account and password (default admin/admin) to enter the configuration mode of the router, as shown below.

Route 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
  do                Set the level state of the do
  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
```

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. eg. # config（Press '?'） config Configuration operation # config（Press spacebar +'?'） 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	Press these two keys at the same time, except its "copy" function but also can be used for "break" out of the setting program.
Syntax error: The command is not completed	Command is not completed.
Tick space key+ Tab key	It can help you finish you command. Example: # config (tick enter key) Syntax error: The command is not completed # config (tick space key+ Tab key) commit save_and_apply loaddefault
#config commit # config save_and_apply	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*	Turn on or turn off debug function
Show	Show *parameters*	Show current configuration of each function , if we need to see all please using "show running "
Set	Set *parameters*	All the function parameters are set by commands set and add, the difference is that set is for the single parameter and add is for the list parameter
Add	Add *parameters*	

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

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
hardware_version = 1.0
firmware_version = beta210618
firmware_version_full = "beta210618 (Rev 4250)"
kernel_version = 4.9.152
device_model = R2011
serial_number = ""
uptime = "0 days, 01:25:16"
system_time = "Tue Apr 15 17:09:04 2021"
ram_usage = "77M 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 R2011-firmware-sysupgrade-unknown.ruf host 192.168.100.99 //enter a new
firmware name
Downloading
Download success.
Upgrading
Upgrade success.              //Update succeed
# reboot                      //Take effect after rebooting
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

# 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）
# 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          //enable 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                                    //setting succeed
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
        router = ""
```

```
            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
# 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 effect
```

Glossary

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

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

Abbr.	Description
WAN	Wide Area Network

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