robustel | User Guide

R5020

High Speed Smart 5G Router

robustOS

Guangzhou Robustel LTD
www.robustel.com

About This Document

This document provides hardware and software information of the Robustel R5020 Router, including introduction, installation, configuration and operation.

Trademarks and Permissions

Disclaimer

Technical Support SECTRON

Tel: +420 599 509 599
Email: hotline@sectron.cz
Web: www.sectron.eu

Important Notice

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

Safety Precautions

General

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

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

Using the Router in Vehicle

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

Protecting Your Router

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

- Do not expose the router to extreme conditions such as high humidity / rain, high temperature, direct sunlight,

caustic / harsh chemicals, dust, or water.

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

Regulatory and Type Approval Information

Table 1: Directives

2011/65/EU	The European RoHS2.0 2011/65/EU Directive was issued by the European parliament and the European Council on 1 July 2011 on the restriction of the use of certain Hazardous substances in electrical and electronic equipment.
2012/19/EU	The European WEEE 2012/19/EU Directive was issued by the European parliament and the European Council on 24 July 2012 on waste electrical and electronic equipment.
2013/56/EU	The European 2013/56/EU Directive is a battery Directive which published in the EU official gazette on 10 December 2013. The button battery used in this product conforms to the standard of 2013/56/EU directive.

Table 2: Standards of the electronic industry of the People's Republic of China

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

Table 3: Toxic or Hazardous Substances or Elements with Defined Concentration Limits

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

o:
Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in RoHS2.0.
X:
Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part *might exceed* the limit requirement in RoHS2.0.
-:
Indicates that it does not contain the toxic or hazardous substance.

Document History

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

Date	Firmware Version	Document Version	Change Description
Dec. 29, 2020	3.1.1	v.1.0.0	Initial release

Contents

Chapter 1 Product Overview

1.1 Key Features

Robustel R5020 dual-SIM VPN wireless router supports WCDMA 3G network, LTE 4G network, and 5G network to provide high-speed wireless network bandwidth for devices through wireless connection, and it has dual-SIM card backup to ensure stable wireless network connection.

R5020 adopts RobustOS, the operating system developed by Robustel, which is based on Linux and applicable to most of Robustel's router devices. Besides the basic network functions and protocols, the system brings customers a more diverse, convenient and practical customized experience. Also, Robustel will provide partners and customers with SDK, allowing users to develop their own functions using C language. In addition, Robustel will also provide rich App applications running on RobustOS to meet the fragmented market demand of IoT applications.

1.2 Package Contents

Before installing your R5020 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 R5020 High Speed Smart LTE Router

- 1 x 3-pin 3.5 mm male terminal block with lock for power supply

- 1 x 2*5-pin 3.5 mm male terminal block for serial port

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

Optional Accessories (sold separately)

- LTE-5G SMA-J cellular antenna (rubber antenna)

  Rubber antenna

- RP-SMA-J WiFi antenna (stubby/magnet optional)

  Stubby antenna

  Magnet antenna

- RP-SMA-J GPS & 5G antenna

- Wall mounting kit

- 35 mm DIN rail mounting kit

- Ethernet cable

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

1.3 Specifications

Cellular Interface

- Number of antennas: 4 (ANT0, ANT1/GNSS, ANT2/GNSS, ANT3)
- Connector: SMA-K
- SIM: 2 (3.0 V & 1.8 V)
- Standards: 5G NR/LTE-FDD/LTE-TDD/WCDMA
  5G: max UL/DL = 80/445 Mbps
  LTE-FDD: max UL/DL = 100/250 Mbps
  LTE-TDD: max UL/DL = 100/250 Mbps
  WCDMA: max UL/DL = 5.76/42 Mbps

Ethernet Interface

- Number of ports: 4 x 10/100/1000 Mbps (3 x LAN + 1 x WAN)
- WAN port: Supports 802.3at PD feature (optional) on ETH0
- Magnet isolation protection: 1 KV

WiFi Interface

- Number of antennas: 2 (WiFi1 + WiFi2)
- Connector: RP-SMA-K
- Standards: 802.11a/b/g/n/ac, 2*2 MIMO, supports AP and Client modes
- Frequency bands: 2.412 - 2.472 GHz (2.4 GHz ISM band)
  5.15 - 5.825 GHz (5 GHz ISM band)
- Security: Open, WPA, WPA2, WEP
- Encryption: AES, TKIP, WEP64
- Data speed: 5G: Up to 867Mbps
  2.4G: Up to 300Mbps

GPS (Optional)

- Number of antennas: 2 (ANT1/GNSS: L5, ANT2/GNSS: L1)
- Connector: SMA-K with 50 ohms impedance
- GNSS Technology: GPS, GLONASS, Galileo, BeiDou
- Tracking sensitivity: -160 dBm
- Horizontal position accuracy: 2.5 m

Serial Interface

- Number of ports: 1 x RS232 + 1 x RS485
- Connector: 2 x 5-pin 3.5 mm female socket
- ESD protection: ±15 KV
- Baud rate: 300 bps to 115200 bps
- Parameters: 8E1, 8O1, 8N1, 8N2, 8E2, 8O2, 7E2, 7O2, 7N2, 7E1, 7O1, 7N1
- RS232: TxD, RxD, GND
- RS485: Data+ (A), Data- (B)

DI/DO

- Type: 1 x DI + 1 x DO, wet contact
- Connector: 2 x 5-pin 3.5 mm female socket
- Isolation: 3.75KVDC
- Absolute maximum VDC: “V+” + 30VDC (DI), 30VDC (DO)
- Absolute maximum ADC: 100mA

Others

- 1 x RST button (Tact Switch)
- 1 x Micro SD interface
- 1 x USB 2.0 host, Type A, 5 V/500 mA
- LED indicators - 1 x RUN, 1 x Modem, 1 x USR, 1 x RSSI, 1 x NET, 1 x WiFi
  Network port indicator (link indicator)
- Built-in: Watchdog, Timer

Power Supply and Consumption

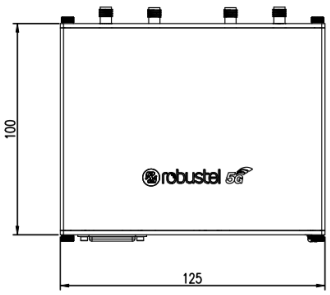
- Connector: 3-pin 3.5 mm female socket with lock
- Input voltage: 10 to 30V DC (With ignition sensing)
  9 to 36V DC (Without ignition sensing)

- Power consumption: Idle: 500 mA@12 V
  Data link: 1.5 A (peak) @12 V

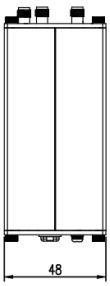
Physical Characteristics

- Ingress protection: IP30
- Operating temperature: -25 ~ +70 °C
- Storage temperature: -40 ~ +85°C
- Humidity: 5 ~ 95% RH
- Housing & Weight: Aluminum, 500 g
- Dimensions: 125 x 100 x 48 mm (device only)
- Installations: Desktop, wall mounting or 35 mm DIN rail mounting
  (Wall mounting or 35 mm DIN rail mounting sold separately)

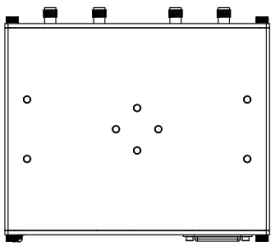
1.4 Dimensions



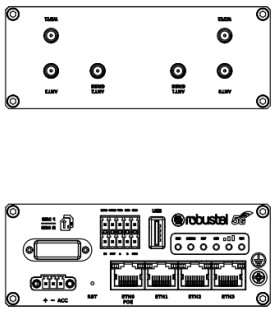
Front View



Rear View



Side View



Top&Bottom View

Chapter 2 Hardware Installation

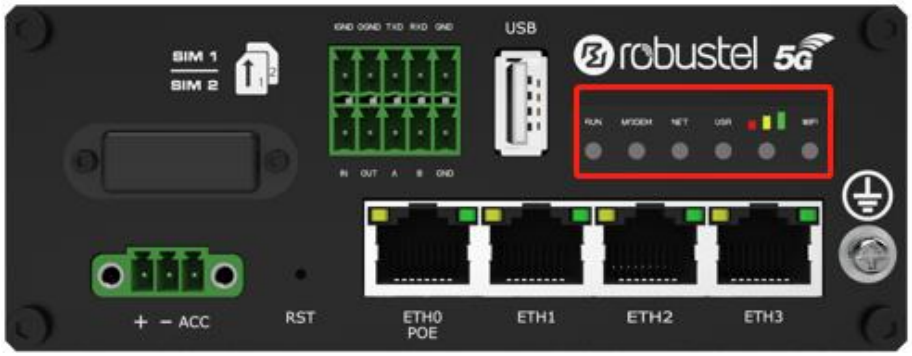
2.1 Definition of 2*5 3.5mm Interface

PIN	DI/DO	RS-232	RS-485	Direction
1	IGND	--	--	--
2	OGND	--	--	--
3	--	TXD	--	Router → Device
4	--	RXD	--	Router ← Device
5	--	GND	--	--
6	IN	--	--	--
7	OUT	--	--	--
8	--	--	A	--
9	--	--	B	--
10	--	--	GND	--

2.2 Definition of Power Interface

PIN	Power	Note
1	Positive	
2	Negative	
3	ACC	Car ignition and flameout detection

2.3 LED Indicators

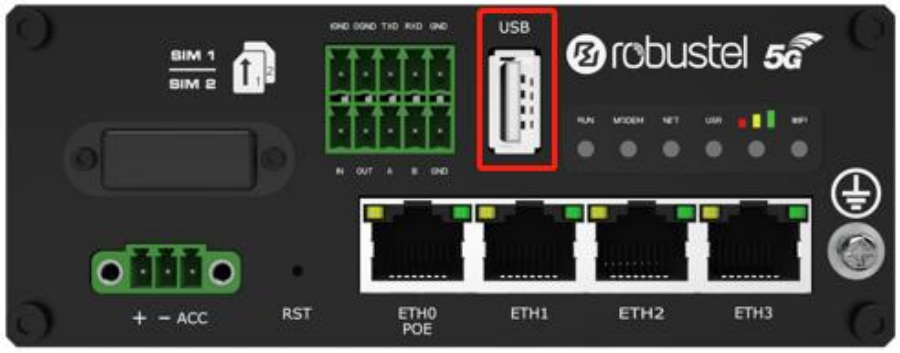


Name	Color	Status	Description
RUN	Green	On, solid	Router is powered on (System is initializing)
		On, blinking	Router starts operating
		Off	Router is powered off
MODEM	Green	On, solid	Link connection is working
		On, blinking	Data is sent and received.
		Off	Link connection is not working
NET	Green	On, solid	Connection to 4G network is established
		On, blinking	Connection to Legacy network (3G or 2G) is established
		Off	Network is not joined or joining
USR-OpenVPN	Green	On, solid	OpenVPN connection is established
		Off	OpenVPN connection is not established
USR-IPsec	Green	On, solid	IPsec connection is established
		Off	IPsec connection is not established

USR-SIM	Green	On, solid	Main SIM card is being used
		On, blinking	Backup SIM card is being used
		Off	No SIM card is being used
	Green	On, solid	Signal level: 21-30 dB (Strong signal)
	Yellow	On, solid	Signal level: 11-20 dB (Moderate signal)
	Red	On, solid	Signal level: 1-10 dB (Low signal)
	--	Off	Very Low Signal strength (0) is available or No signal
WiFi	Green	On, solid	WiFi is enabled and working properly
		Off	WiFi is disabled or not working properly

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

2.4 USB Interface



Function	Operation
Firmware upgrade	USB interface is used for batch firmware upgrading, but cannot be used for sending or receiving data from slave devices which connected to it. You can insert a USB storage device into the router's USB interface, such as a U disk or a hard disk. If there have a supported configuration file or a router firmware in this USB storage device, the router will automatically update the configuration file or the firmware. For more details, see **4.2.6 USB**.

2.5 Reset Button

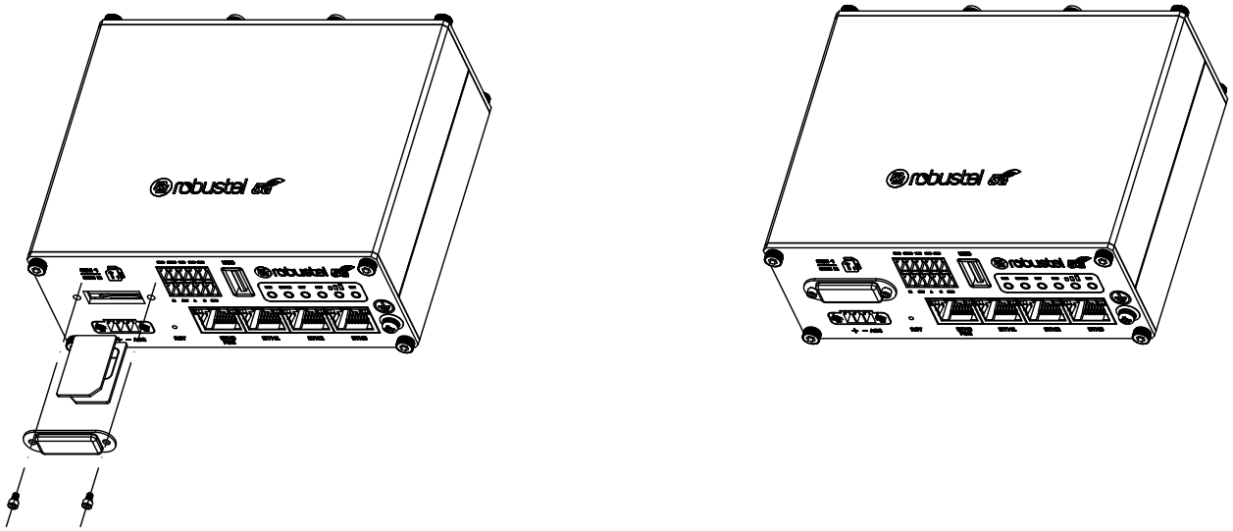
Function	Operation
Reboot	Press and hold the RST button for at least 5 seconds under the operating status.
Restore to factory default settings	Wait for 0~20 seconds after powering up the router, press and hold the RST button with a pointed stick until all six LEDs start blinking one by one, and release the button to return the router to factory defaults.

2.6 Ethernet Ports

There are four Ethernet ports on R5020, including ETH0 (POE), ETH1, ETH2, ETH3. Each has two LED indicators. The yellow one is a link indicator but the green one doesn't mean anything. For details about status, see the table below.

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

2.7 Insert or Remove SIM Card



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

- **Insert SIM card**

1. Make sure router is powered off.
2. To 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 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:

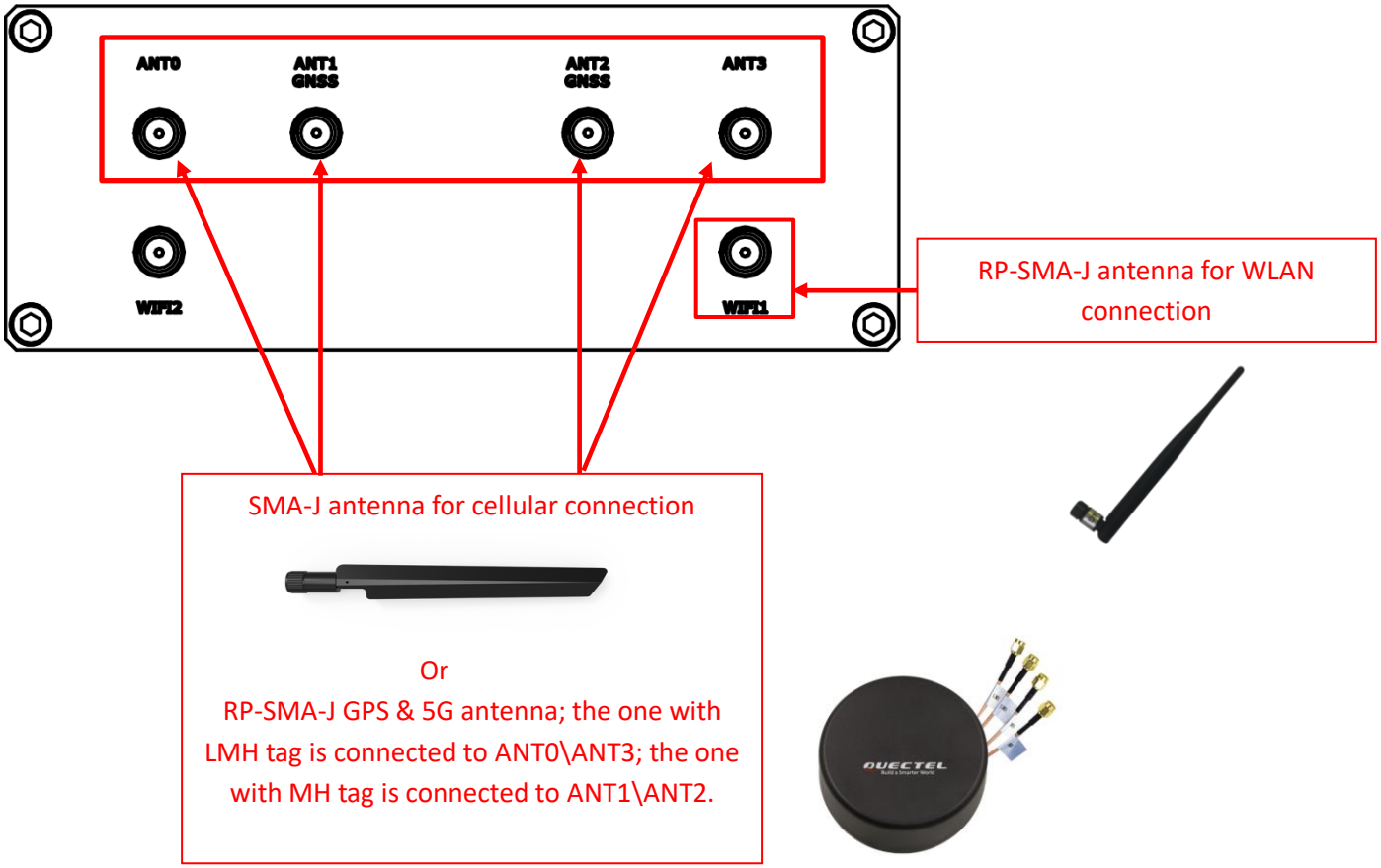
1. Use the specific card when the device is working in extreme temperature (temperature exceeding 40 °C), because the regular card for long-time working in harsh environment will be disconnected frequently.

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

2.8 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.

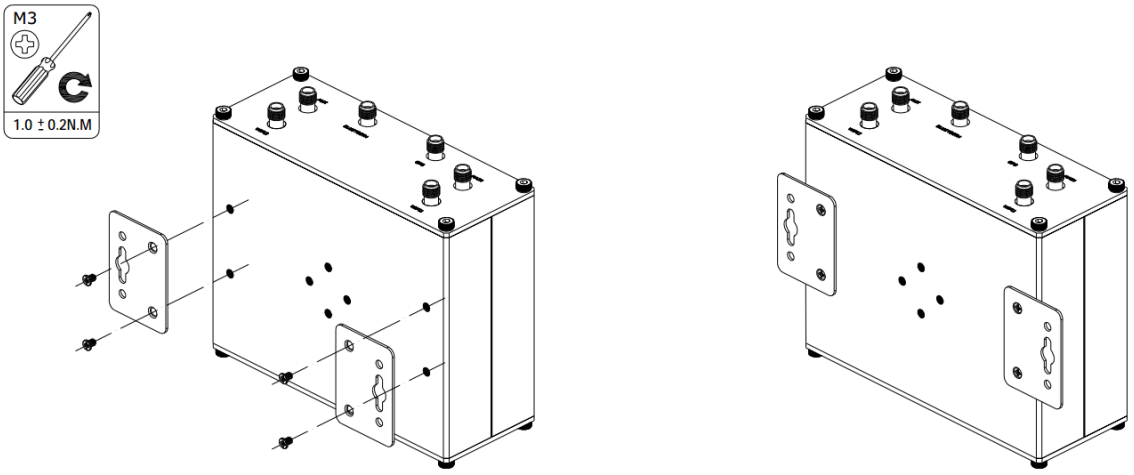


2.9 Mount the Router

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

Two methods for mounting the router

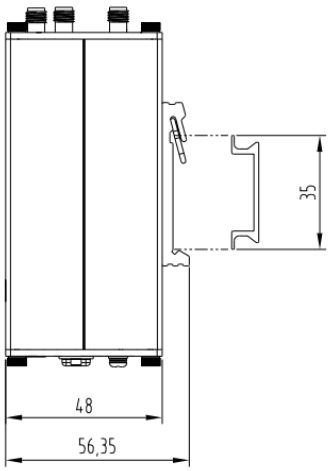
1. Wall mounting (measured in mm)

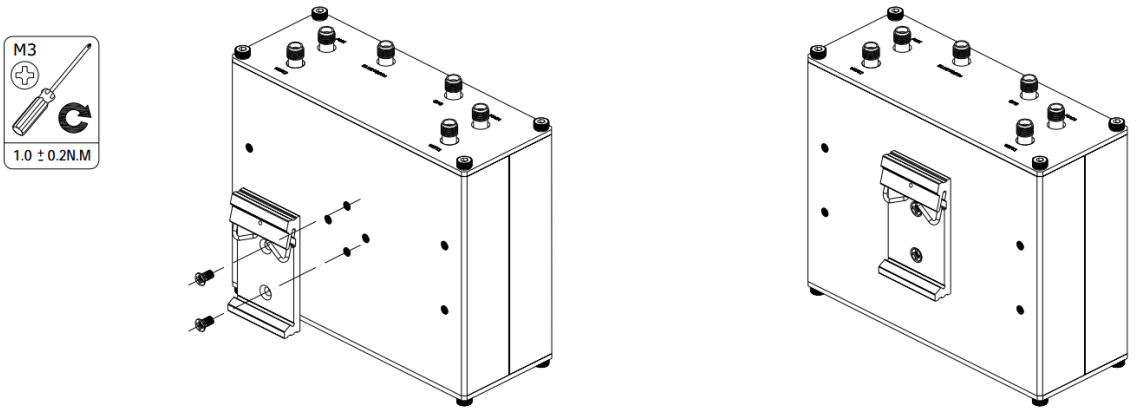


Use 4 pcs of M2.5*4 flat head Phillips screws to fix the wall mounting kit to the router, and then use 2 pcs of M3 drywall screws to mount the router associated with the wall mounting kit on the wall.

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

2. DIN rail mounting (measured in mm)
   - Option 1

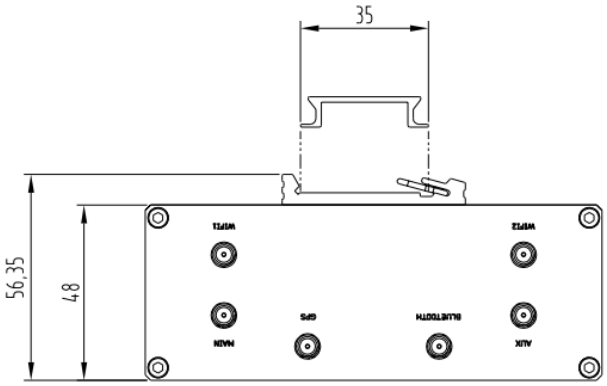


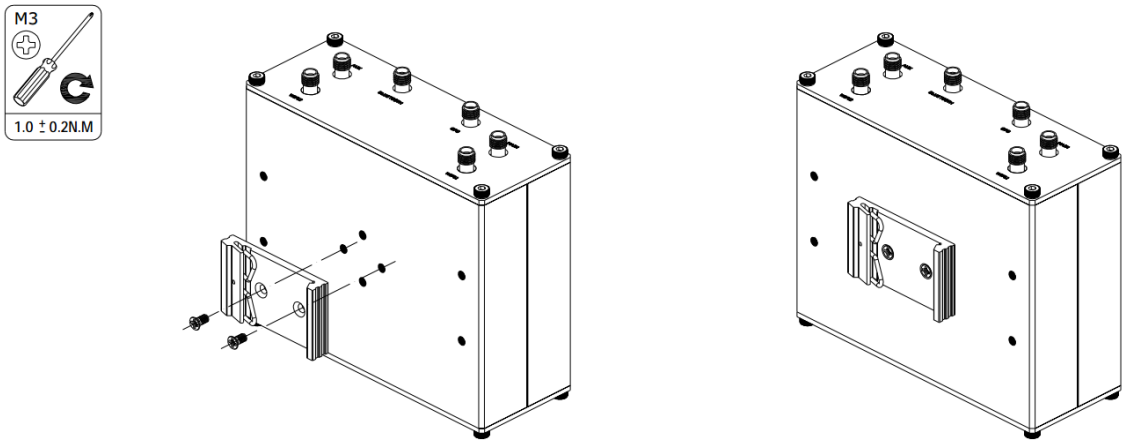


Use 2 pcs of M3*6 stainless flat head Phillips screws to fix the DIN rail to the router, and then hang the DIN rail on the mounting bracket. It is necessary to choose a standard bracket.

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

- Option 2





Use 2 pcs of M3*6 stainless flat head Phillips screws to fix the DIN rail to the router, and then hang the DIN rail on the mounting bracket. It is necessary to choose a standard bracket.

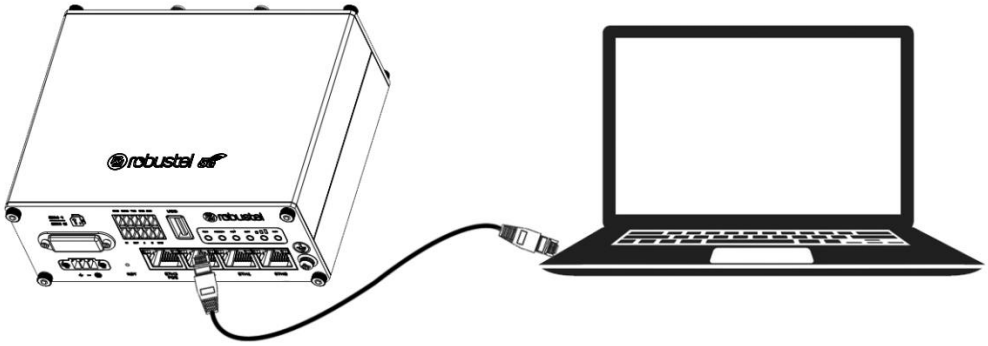
Note: Recommended torque for mounting is 1.0 N.m, and the maximum allowed is 1.2 N.m.

2.10 Ground the Router

Router grounding helps prevent the noise effect due to electromagnetic interference (EMI). Connect the router to the site ground wire by the ground screw before powering on.

Note: This product is appropriate to be mounted on a sound grounded device surface, such as a metal panel.

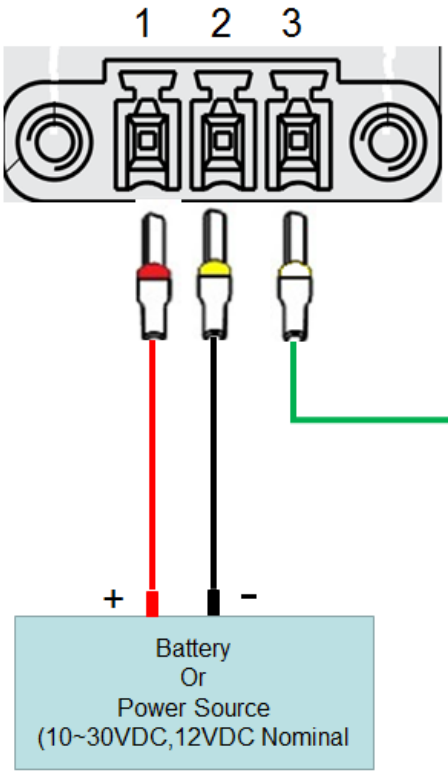
2.11 Connect the Router to a Computer



Connect an Ethernet cable to the port marked ETH1~ETH3 at the front of the R5020 Router, and connect the other end of the cable to your computer.

2.12 Power Supply

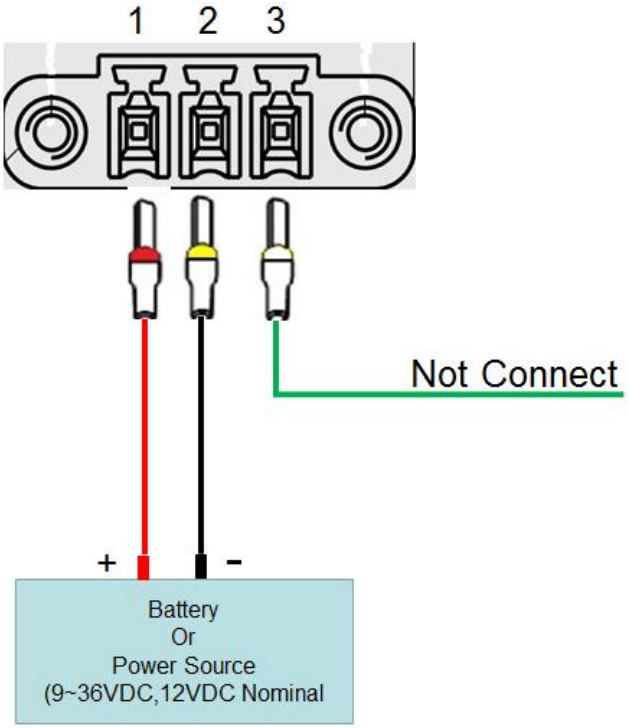
With Ignition Sensing



Note: Please connect the ACC pin of R5020 to the VCC of power supply without being floated, when you do not use the car ignition and flameout detection function.

PIN	Description	Note
1	V+	Connect adapter or battery positive (red line)
2	V-	Connect adapter or battery negative (black)
3	ACC	Car ignition and flameout detection (green line), when the car ignition and flameout detection function is not used, the ACC pin is connected to the power supply and cannot be left floating.

With POE Function

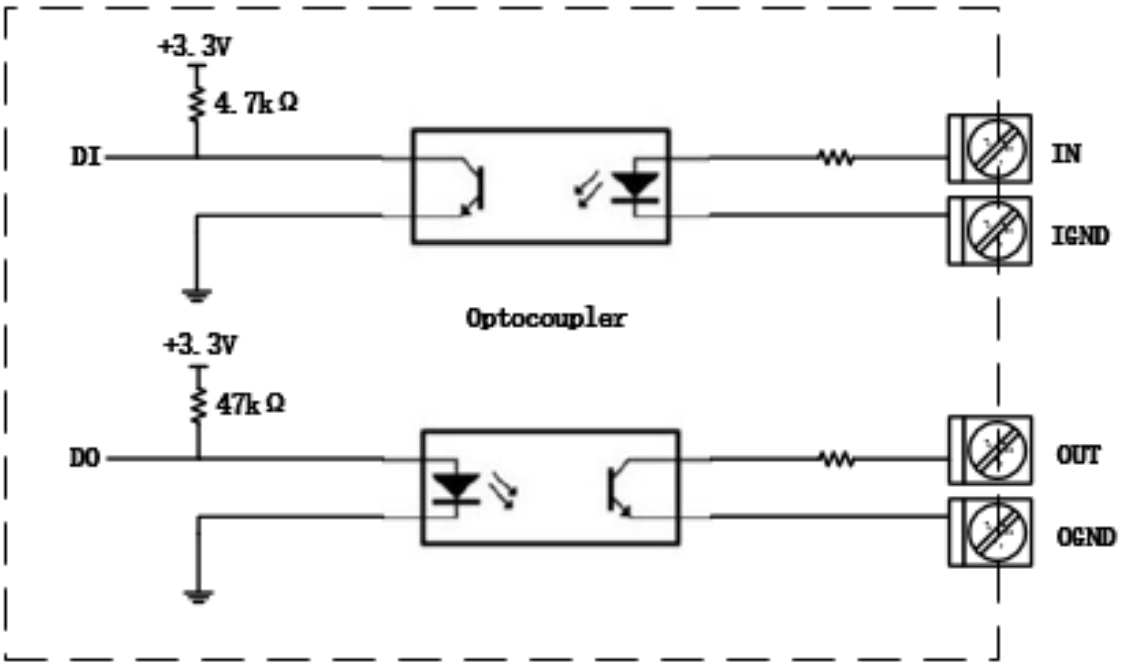


PIN	Description	Note
1	V+	Connect adapter or battery positive (red line)
2	V-	Connect adapter or battery negative (black)
3	Not connected	

Note：

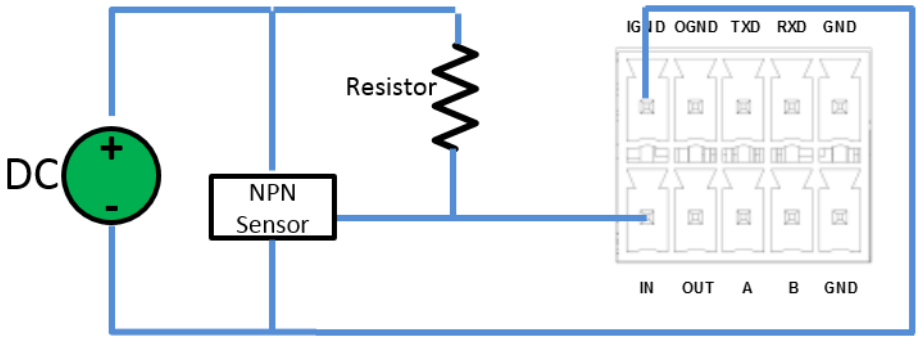
1. The Input voltage is: 10 to 30V DC(With ignition sensing)
   9 to 36V DC (Without ignition sensing)
2. The car ignition sensing function and the POE function can only be selected one by one.

2.13 DI/DO Interface



The R5020 supports 1 channel DI and 1 channel DO by default. It can support 2 channels of DI or 2 channels of DO by BOM modification. DI signal access, can be used for NPN/PNP type sensor signal or switch signal acquisition, power supply can only be accessed from IN, not reversed. DO signal output, can be used for NPN/PNP sensor control.

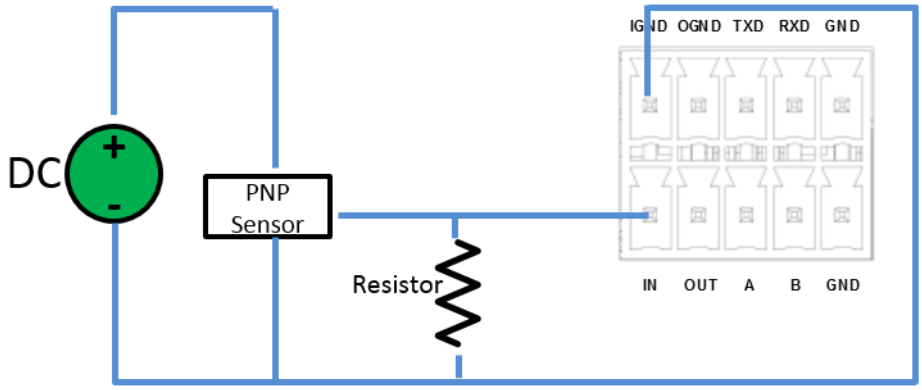
1. Application mode of DI connected with NPN sensor



IN corresponds to IN on 2*5 3.5mm interface, and IGND corresponds to IGND on 2*5 3.5mm interface. The voltage range of external power supply (DC) is 3V ~ 30V. The internal flow of the device is limited. In the normal voltage range, the external power supply does not need to be limited.

Notes: The above example NPN Sensor is a DC three-wire NPN photoelectric switch or proximity switch.

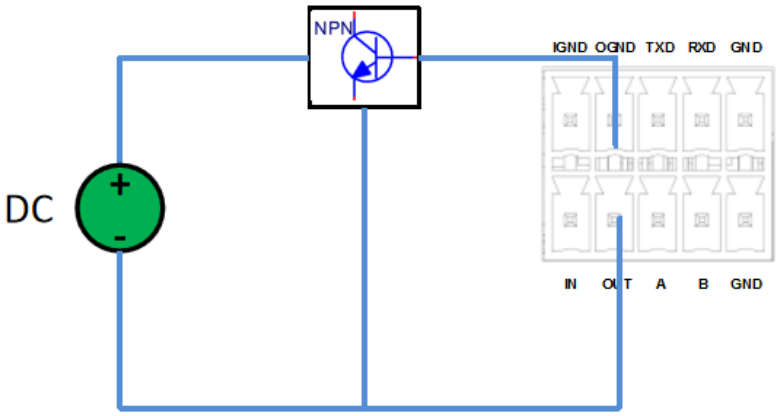
2. Application mode of DI connected with PNP sensor



IN corresponds to IN on 2*5 3.5mm interface, and IGND corresponds to IGND on 2*5 3.5mm interface. The voltage range of external power supply (DC) is 3V ~ 30V; the internal flow of the device is limited. In the normal voltage range, the external power supply does not need to be limited.

Notes: The above example PNP Sensor is a DC three-wire NPN photoelectric switch or proximity switch.

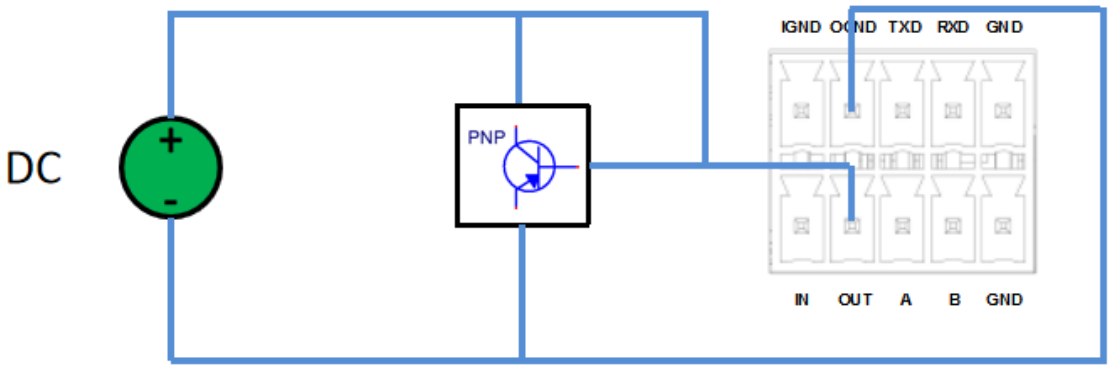
3. Application mode of DO Driven NPN Triode



OUT corresponds to OUT on 2*5 3.5mm interface, and OGND corresponds to OGND on 2*5 3.5mm interface. The maximum 2.5mA drive current can be supplied through OGND; the external power supply DC voltage range is 3V~30V.

Notes: The above illustration NPN is a common NPN triode.

4. Application mode of DO Driven PNP Triode



OUT corresponds to OUT on 2*5 3.5mm interface, and OGND corresponds to OGND on 2*5 3.5mm interface. The

external power supply DC voltage range is 3V~30V.

Notes: The above illustration PNP is a common NPN triode.

Chapter 3 Initial Configuration

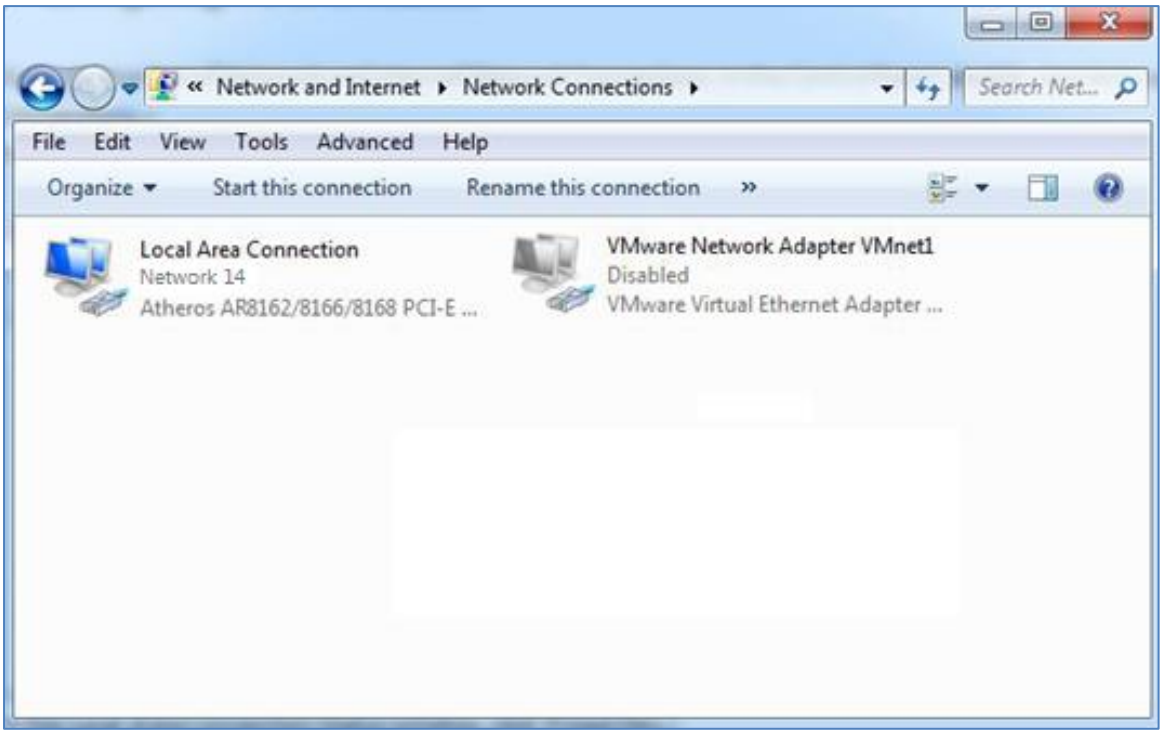
The router can be configured through your web browser that including IE 8.0 or above, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. There are various ways to connect the router, either through an external repeater/hub or connect directly to your PC. When the router is directly connected to the Ethernet port of the computer, if the router acts as a DHCP server, then the computer can get the IP directly from the router; the computer can also set a static IP in the same network segment as the router, so that the computer and the router form a small LAN. After the computer and the router have successfully established a connection, enter the default login address of the device on the computer's browser to enter the router's WEB login interface.

3.1 Configure the PC

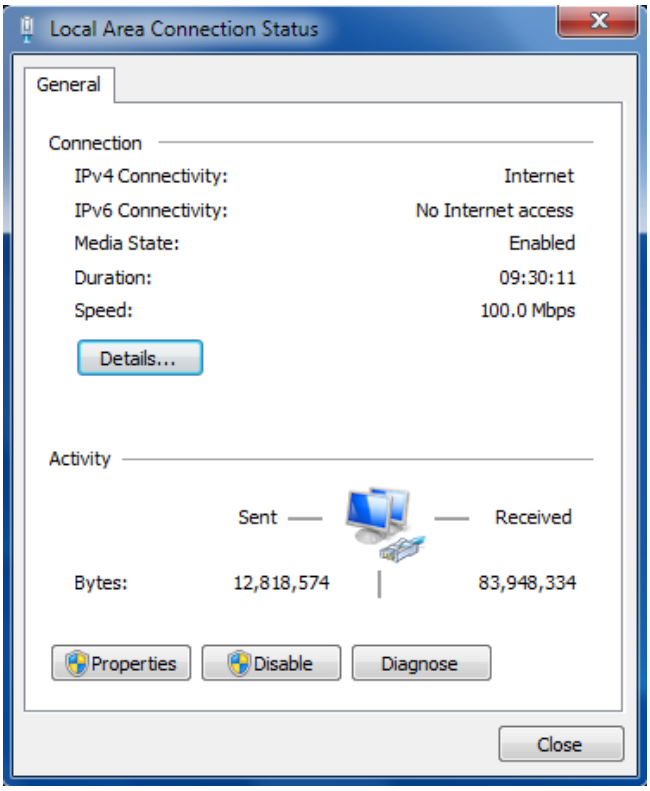
There are two methods to get IP address for the PC. One is to obtain an IP address automatically from “Local Area Connection”, and another is to configure a static IP address manually within the same subnet of the router. Please refer to the steps below.

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

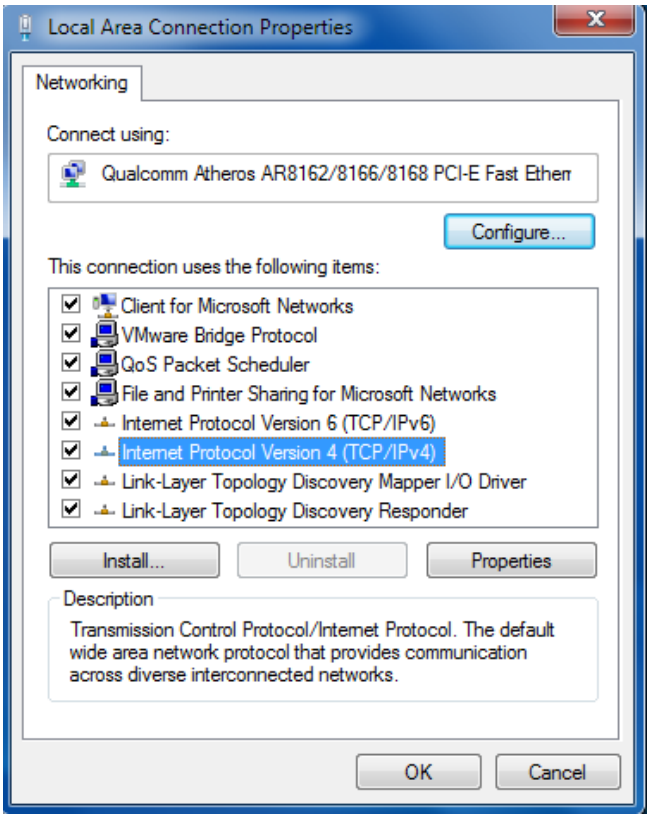
1. Click **Start > Control panel**, double-click **Network and Sharing Center**, and then double-click **Local Area Connection**.



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

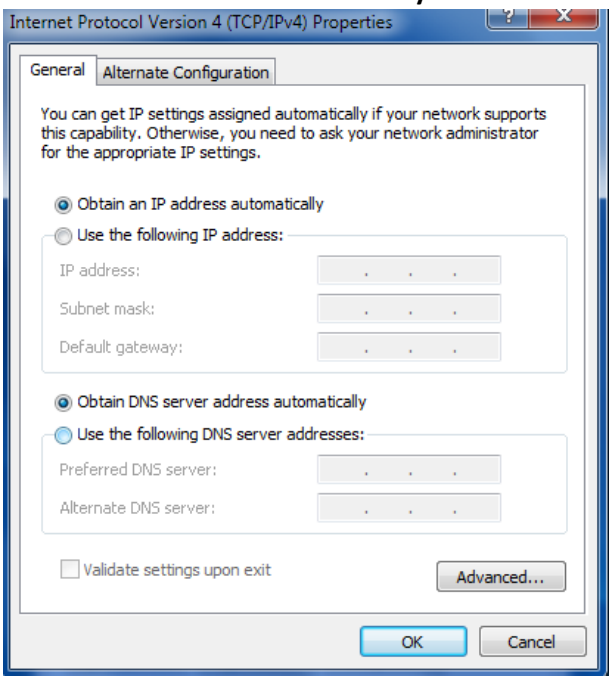


3. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



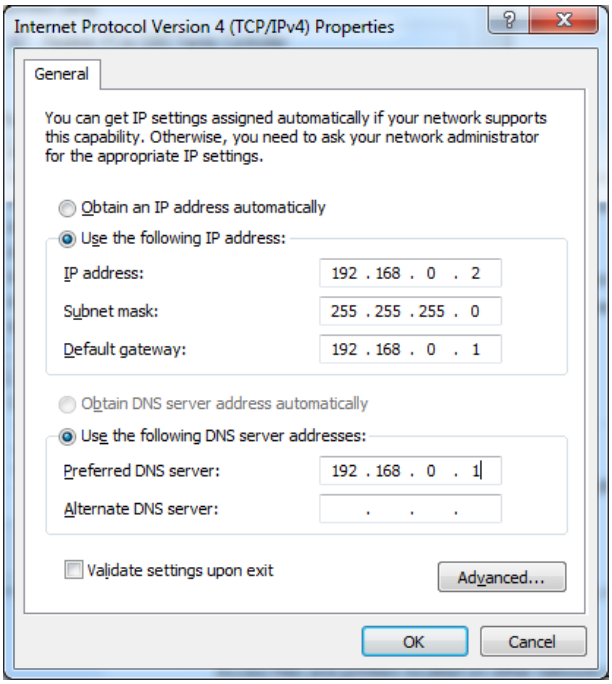
4. Two ways for configuring the IP address of PC

Obtain an IP address automatically from the DHCP server and click "Obtain an IP address automatically";



Use the following IP address:

(Configured a static IP address manually within the same subnet of the router. Click and configure "Use the following IP address.)



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

3.2 Factory Default Settings

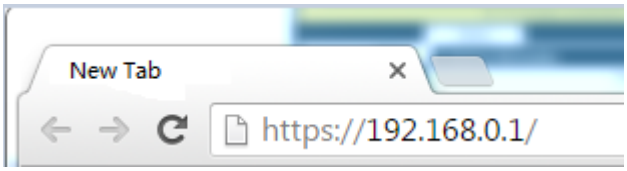
Before configuring your router, you need to know the following default settings.

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

3.3 Log in the Router

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

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

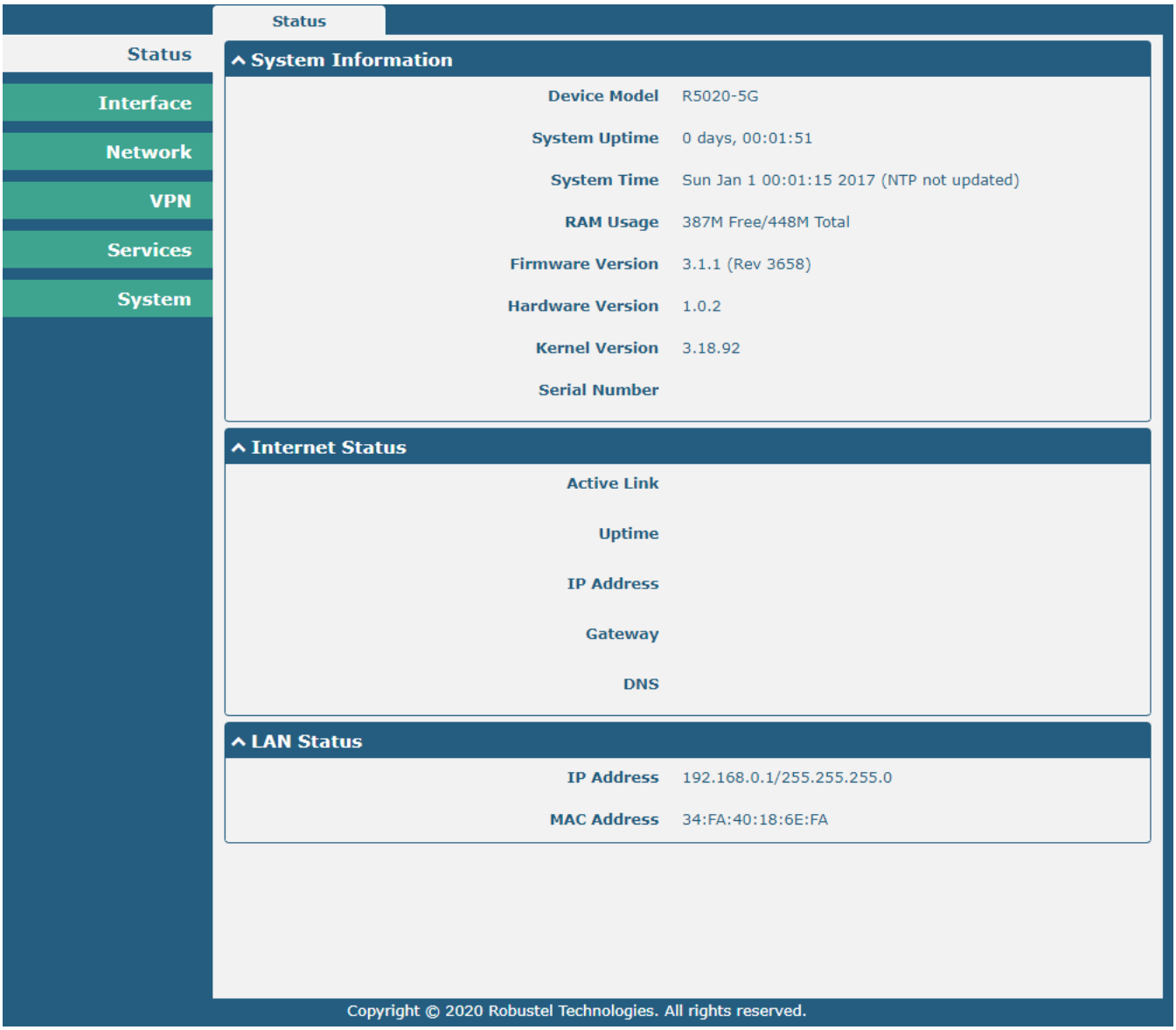


3. In the login page, enter the username and password, choose language and then click **LOGIN**. The default username and password are “admin”.

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

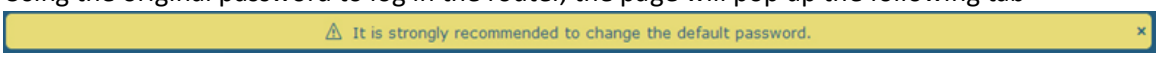
3.4 Control Panel

After logging in, the home page of the R5020 Router's web interface is displayed, for example.



In the home page, users can perform operations such as saving the configuration, restarting the router, and logging out.

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



Click the × symbol to close the popup. It is strongly recommended for security purposes that you change the default username and/or password. To change your username and/or password, see **4.6.6 User Management**.

Control Panel		
Item	**Description**	**Button**
Save & Apply	Click to save the current configuration into router's flash and apply the modification on every configuration page, to make the modification	Save & Apply

	taking effect.	
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.

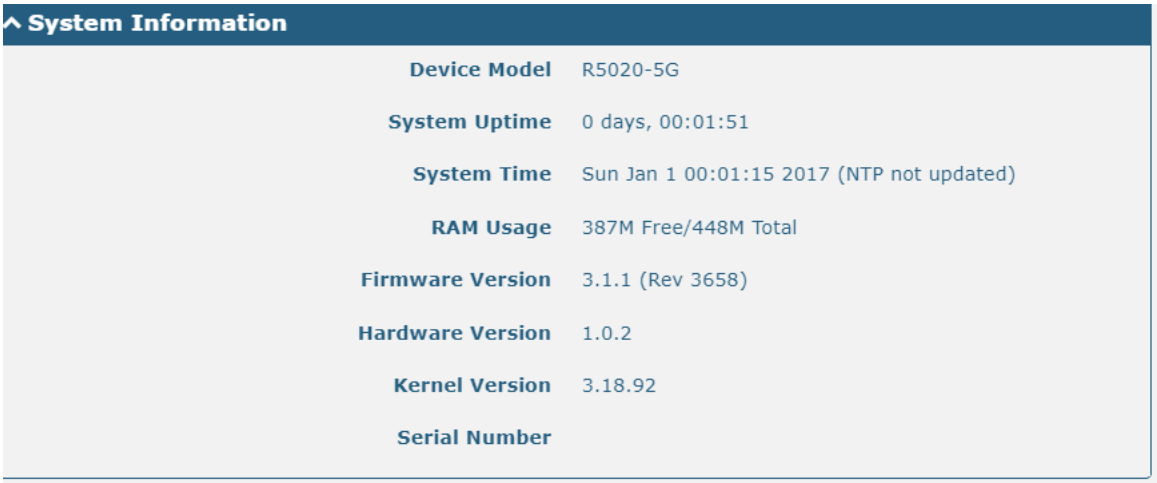
Chapter 4 Initial Configuration

4.1 Status

This page allows you to view the system information, internet status and LAN status of your router.

4.1.1 System Information

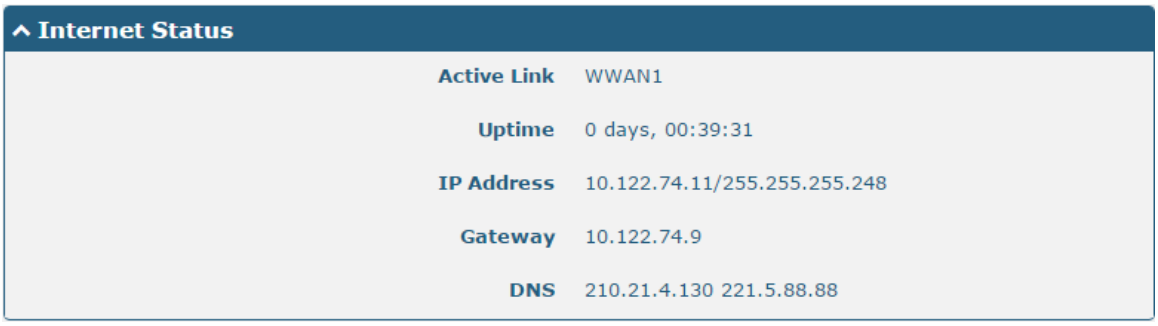
This section shows the system status information of your router.



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

4.1.2 Cellular Status

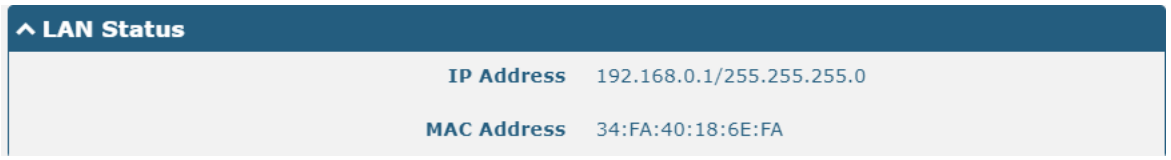
This section shows the cellular status information of the router.



Cellular Status	
Item	**Description**
Active Link	Show the current active link. WWAN1， WWAN2 or WAN.
Uptime	Show the current amount of time the link has been connected.
IP Address	Show the IP address of current link.
Router	Show the router address of the current link.
DNS	Show the current primary DNS server and secondary server.

4.1.3 Internet Status

This section shows the Internet status information of the router.

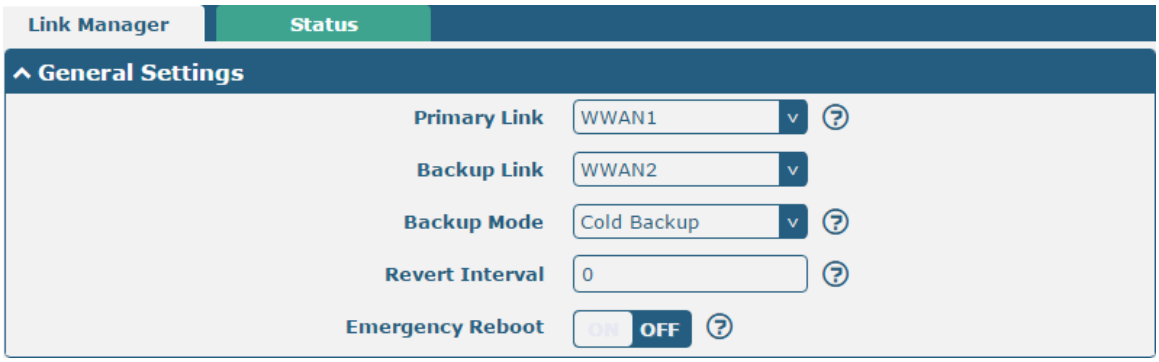


Internet Status	
Item	**Description**
IP Address	Show the IP address and the Netmask of the router.
MAC Address	Show the MAC address of the router.

4.2 Interface

4.2.1 Link Manager

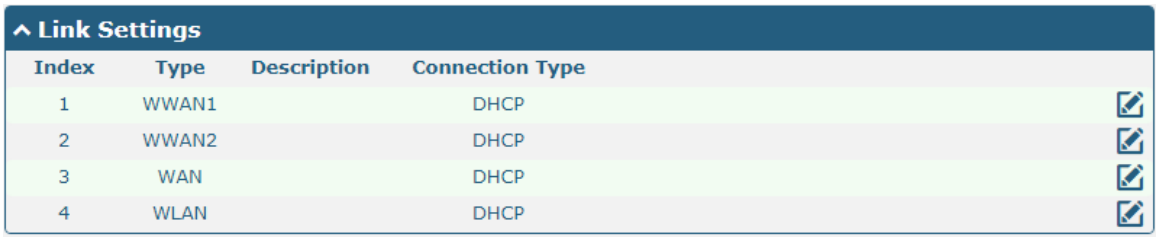
This section allows you to setup the link connection. Link management is a network link backup feature that provides backup of mobile networks and Ethernet links.



General Settings @ Link Manager		
Item	**Description**	**Default**
Primary Link	Select from “WWAN1”, “WWAN2”, “WAN” or “WLAN”. • WWAN1: Select SIM1 as the primary wireless link • WWAN2: Select SIM2 as the primary wireless link • WAN: Select WAN as the primary wired link • WLAN: Select WLAN as the primary wireless link **Note:** WLAN link is available only if enable WiFi as Client mode, please refer to **4.2.5 Interface > WiFi (Optional)**.	WWAN1
Backup Link	Select from “None”, “WWAN1”, “WWAN2”, “WAN”, “WLAN” or “None”. • WWAN1: Select SIM1 as backup wireless link • WWAN2: Select SIM2 as backup wireless link • WAN: Select WAN as the backup wired link • WLAN: Select to make WLAN as the backup wireless link **Note:** WLAN link is available only if enable WiFi as Client mode, please refer to **4.2.5 Interface > WiFi (Optional)**. • None: Do not select any backup link	WWAN2
Backup Mode	Select from “Cold Backup”, “Warm Backup” or “Load Balancing”. • Cold Backup: The inactive link is offline on standby • Warm Backup: The inactive link is online on standby **Note:** Warm backup mode is not available for dual SIM backup. • Load Balancing: Use two links simultaneously	Cold Backup
Revert Interval	Specify the number of minutes that elapses before the primary link is checked if a backup link is being used in cold backup mode. 0 means disable checking. **Note:** Revert interval is available only under the cold backup mode.	0
Emergency Reboot	Click the toggle button to enable/disable this option. Enable to reboot the whole system if no links available.	OFF

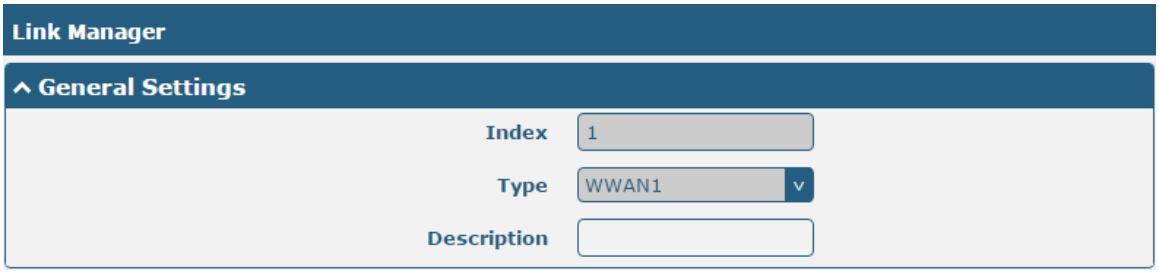
Note: Click ? for help.

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

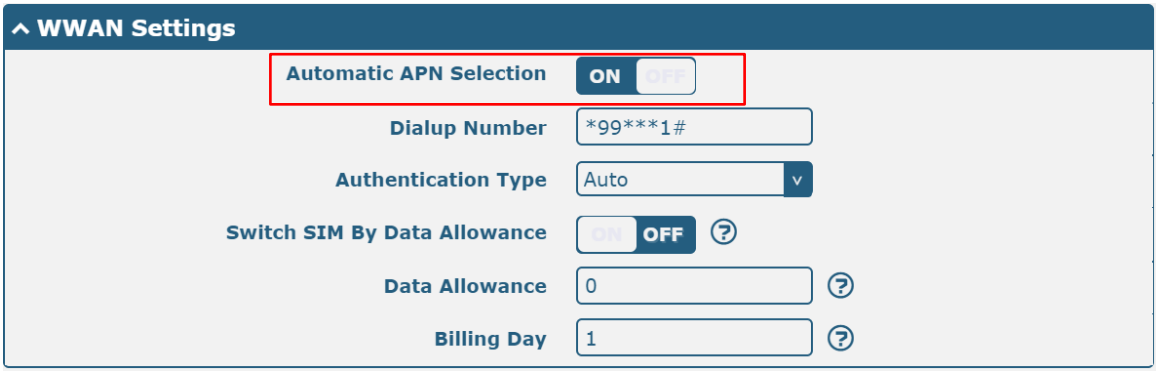


Click on the right-most of WWAN1/WWAN2 to enter the configuration window.

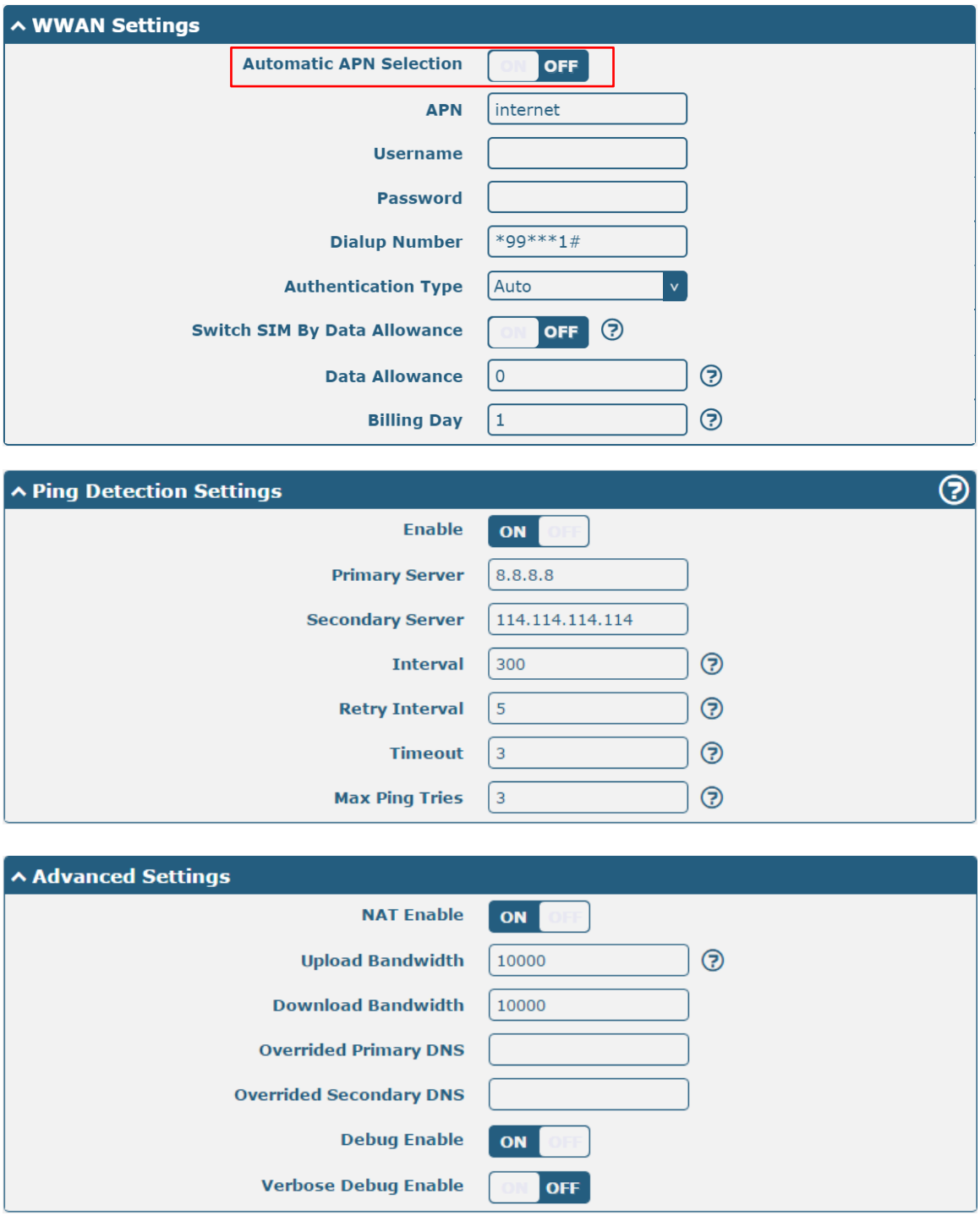
WWAN1/WWAN2



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



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



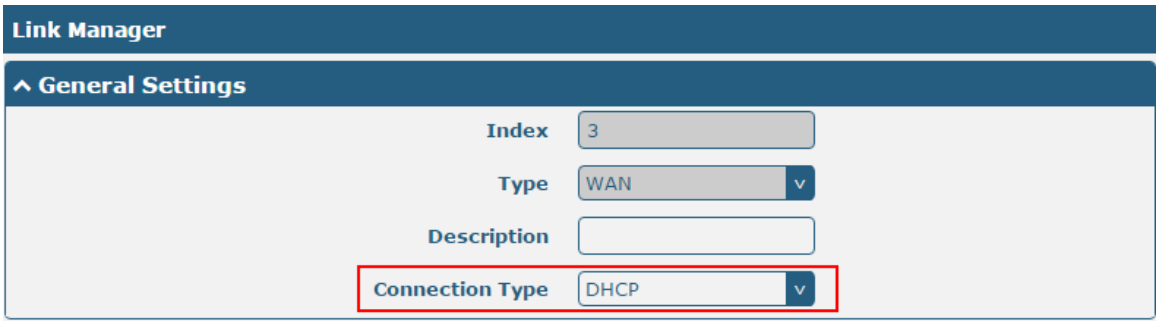
Link Settings (WWAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WWAN1
Description	Enter a description for this link.	Null
WWAN Settings		

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

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

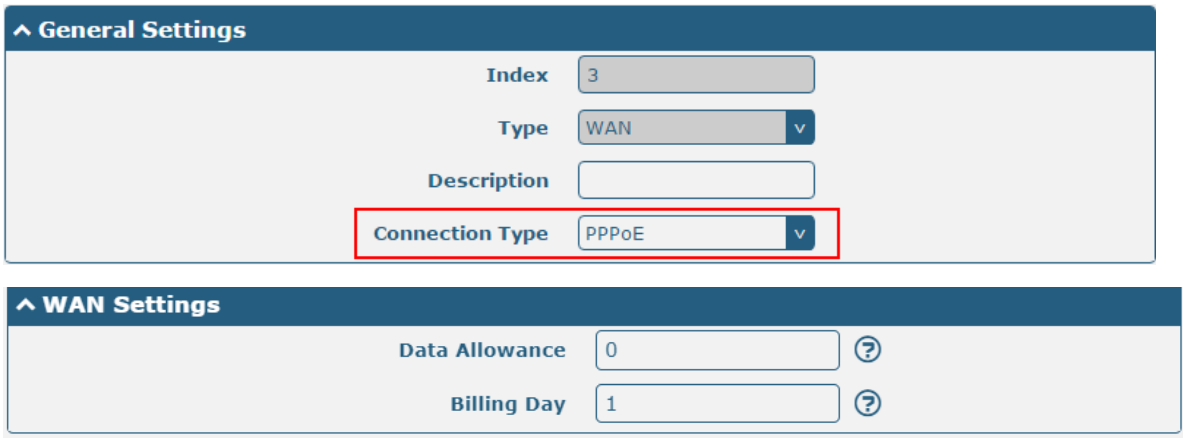
WAN

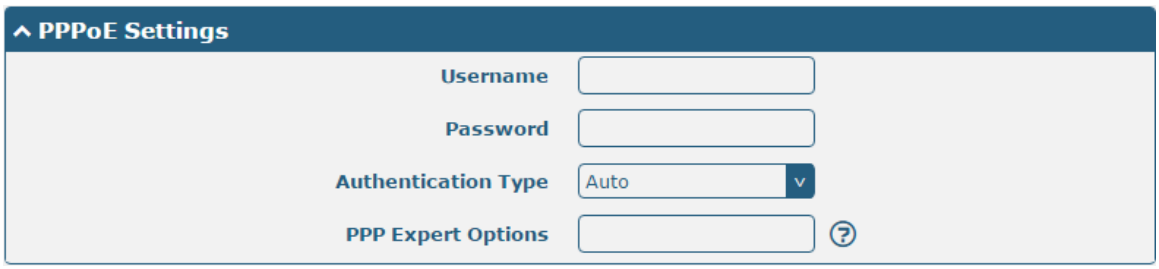
Router will obtain IP automatically from DHCP server if choosing “DHCP” as connection type. The window is displayed as below.

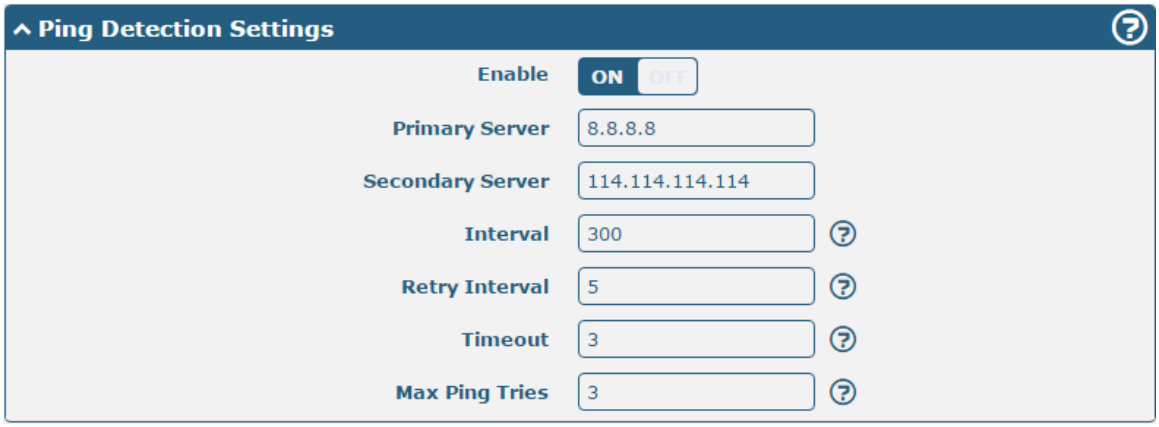


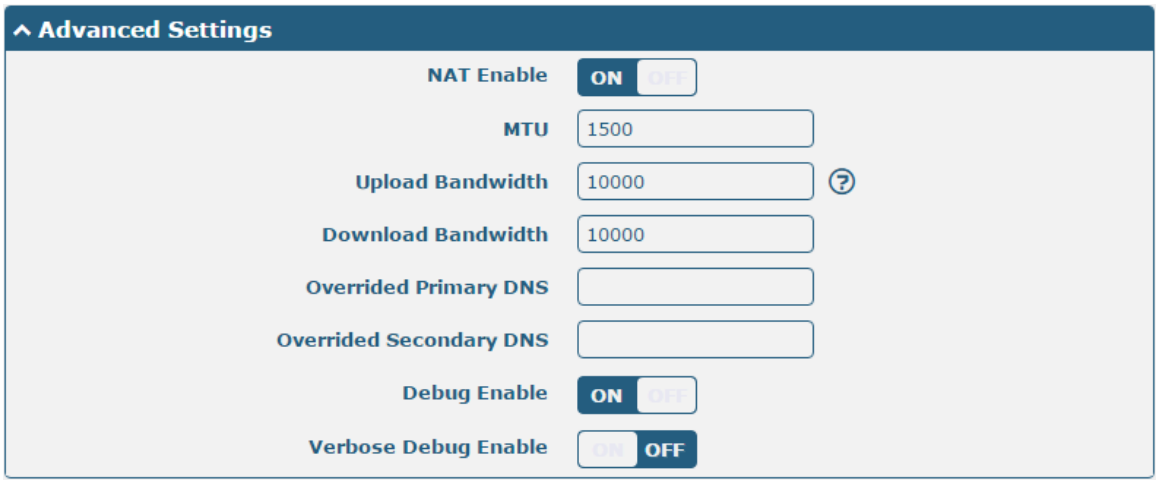
The window is displayed as below when choosing “Static” as the connection type.

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









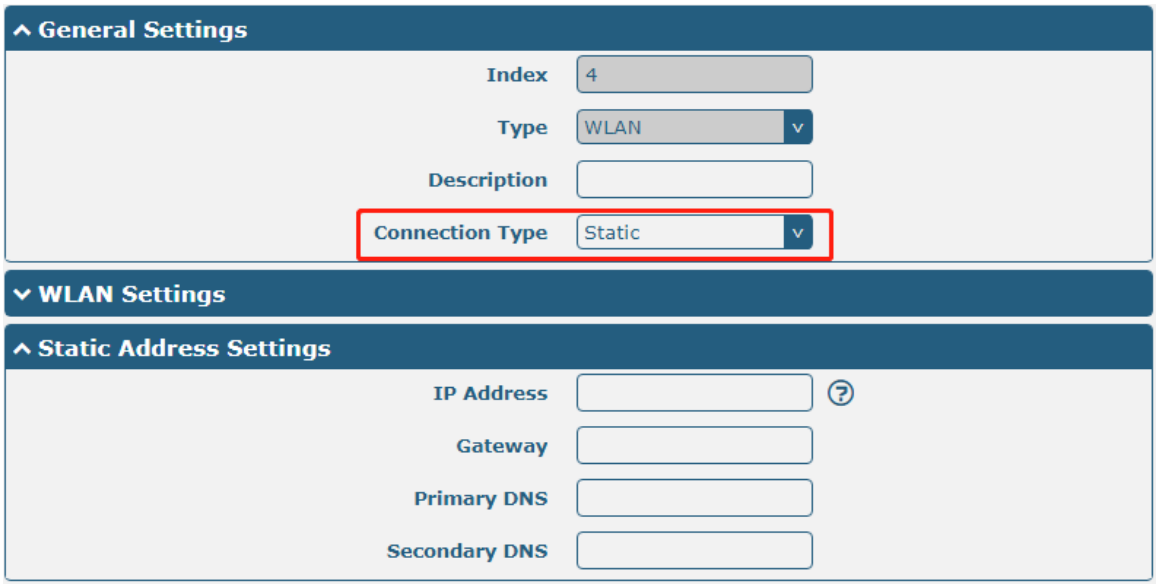
Link Settings (WAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WAN
Description	Enter a description for this link.	Null
Connection Type	Select from “DHCP”, “Static” or “PPPoE”.	DHCP
Static Address Settings		
IP Address	Set the IP address with Netmask which can access the internet. IP address with Netmask, e.g. 192.168.1.1/24	Null
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.	OFF
Billing Day	Specify the monthly billing day. The data traffic statistics will be recalculated from that day.	1
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keep-alive policy of the router.	ON
Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.114.114
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advanced Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Overrided Primary DNS	Override primary DNS will override the automatically obtained DNS.	Null
Overrided Secondary DNS	Override secondary DNS will override the automatically obtained DNS.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

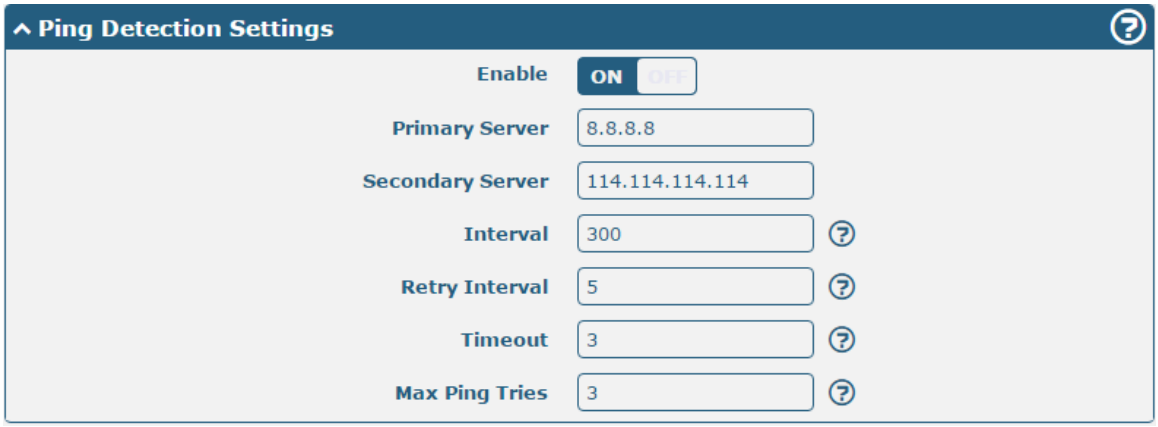
WLAN

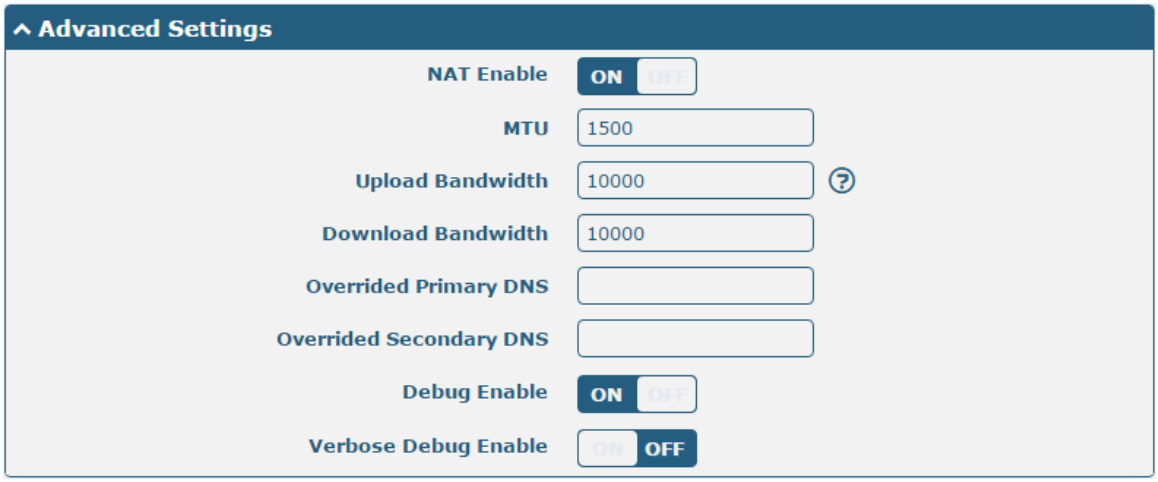
Router will obtain IP automatically from the WLAN AP if choosing “DHCP” as the connection type. The specific parameter configuration of SSID is shown as below.

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



R5020 does not support the **PPPoE** WLAN Connection Type.



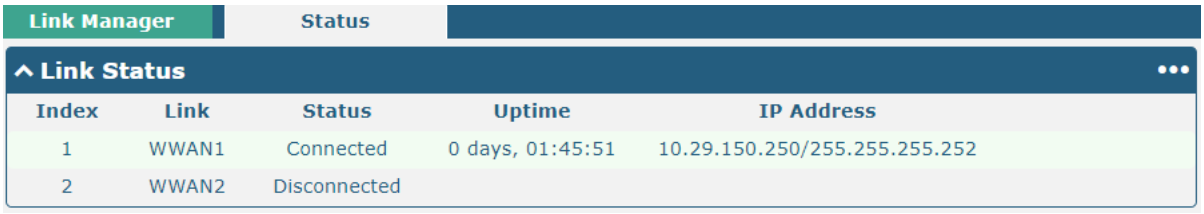


Link Settings (WLAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WLAN
Description	Enter a description for this link.	Null
Connection Type	Select from “DHCP” or “Static”.	DHCP
WLAN Settings		
SSID	Enter a 1-32 characters SSID which your router wants to connect. SSID (Service Set Identifier) is the name of your wireless network.	router
Connect to Hidden SSID	Click the toggle button to enable/disable this option. When router works as Client mode and needs to connect any access point which has hidden SSID, you need to enable this option.	OFF
Password	Enter an 8-63 characters password of the access point which your router wants to connect.	Null
Static Address Settings		
IP Address	Enter the IP address with Netmask which can access the Internet, e.g. 192.168.1.1/24	Null
Router	Enter the IP address of WiFi AP.	Null
Primary DNS	Set the primary DNS.	Null
Secondary DNS	Set the secondary DNS.	Null
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.114.114
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set the ping timeout.	3

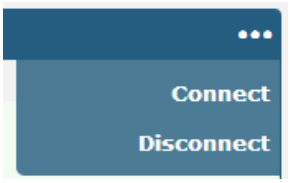
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advance Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Overrided Primary DNS	Override primary DNS will override the automatically obtained DNS.	Null
Overrided Secondary DNS	Override secondary DNS will override the automatically obtained DNS.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

Status

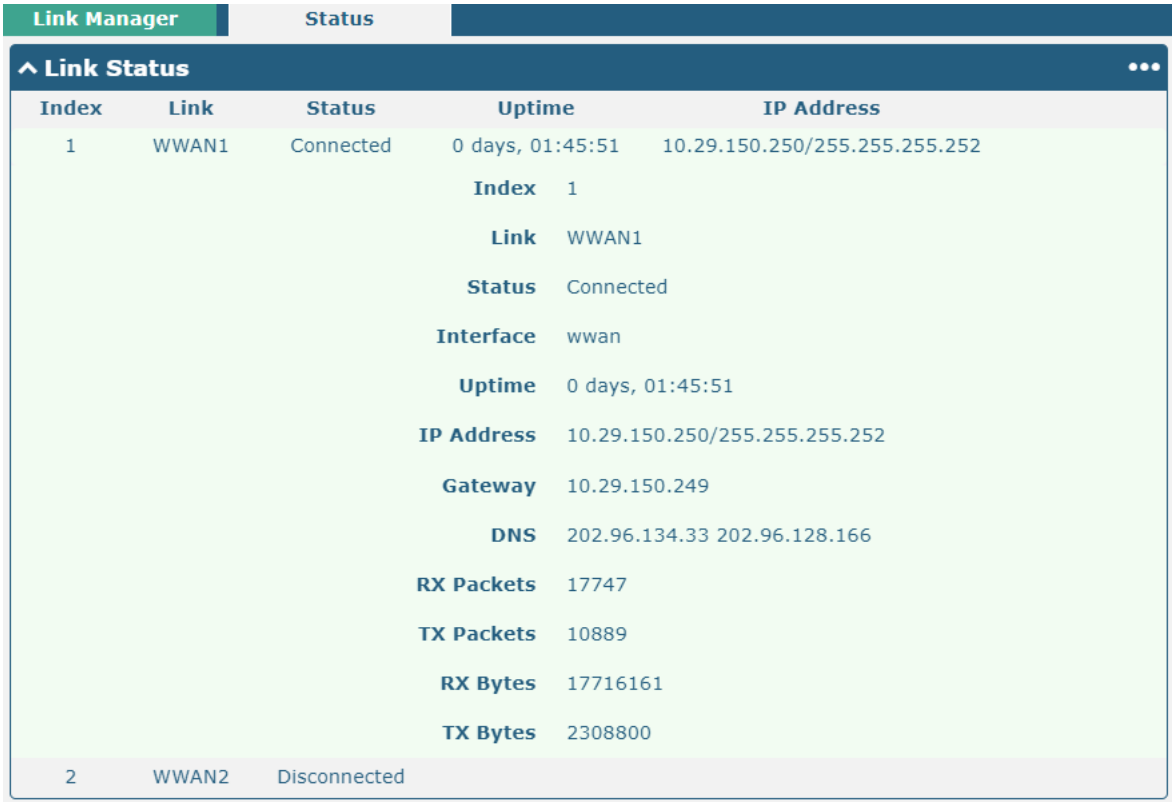
This page allows you to view the status of link connection and clear the monthly data usage statistics.



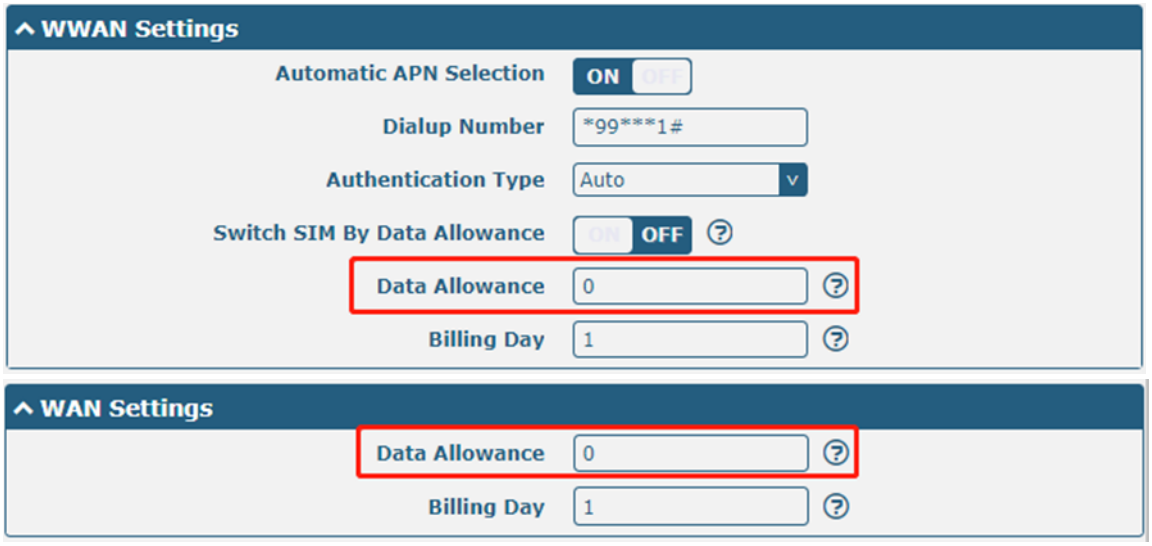
Click the right-most button ••• to select the connection status of the current link.



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



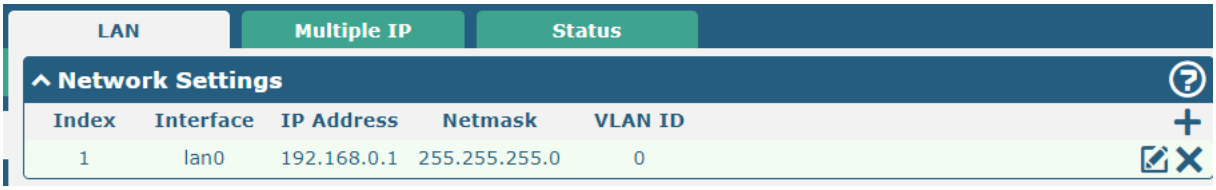
Click the **Clear** button to clear SIM1 or SIM2 monthly data traffic usage statistics. Data statistics will be displayed only if enable the Data Allowance function in **Interface > Link Manager > Link Settings > WWAN Settings > Data Allowance**.



4.2.2 LAN

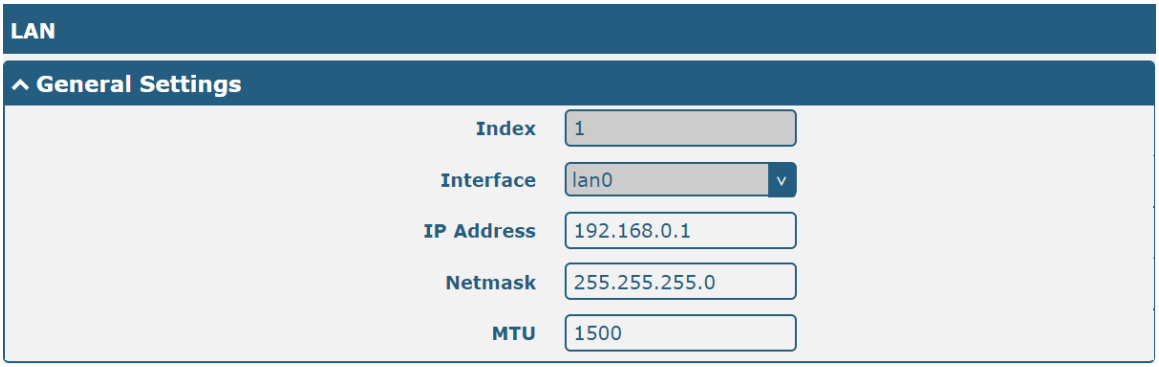
This section allows you to set the related parameters for LAN port. There are four LAN ports on R5020 Router, including ETH0, ETH1, ETH2 and ETH3. ETH0 is wan by default and is not selectable. The ETH1, ETH2 and ETH3 can freely choose from lan0, lan1 and lan2, but at least one LAN port must be assigned as lan0. The default settings of ETH0, ETH1, ETH2 and ETH3 are lan0 and their default IP are 192.168.0.1/255.255.255.0.

LAN



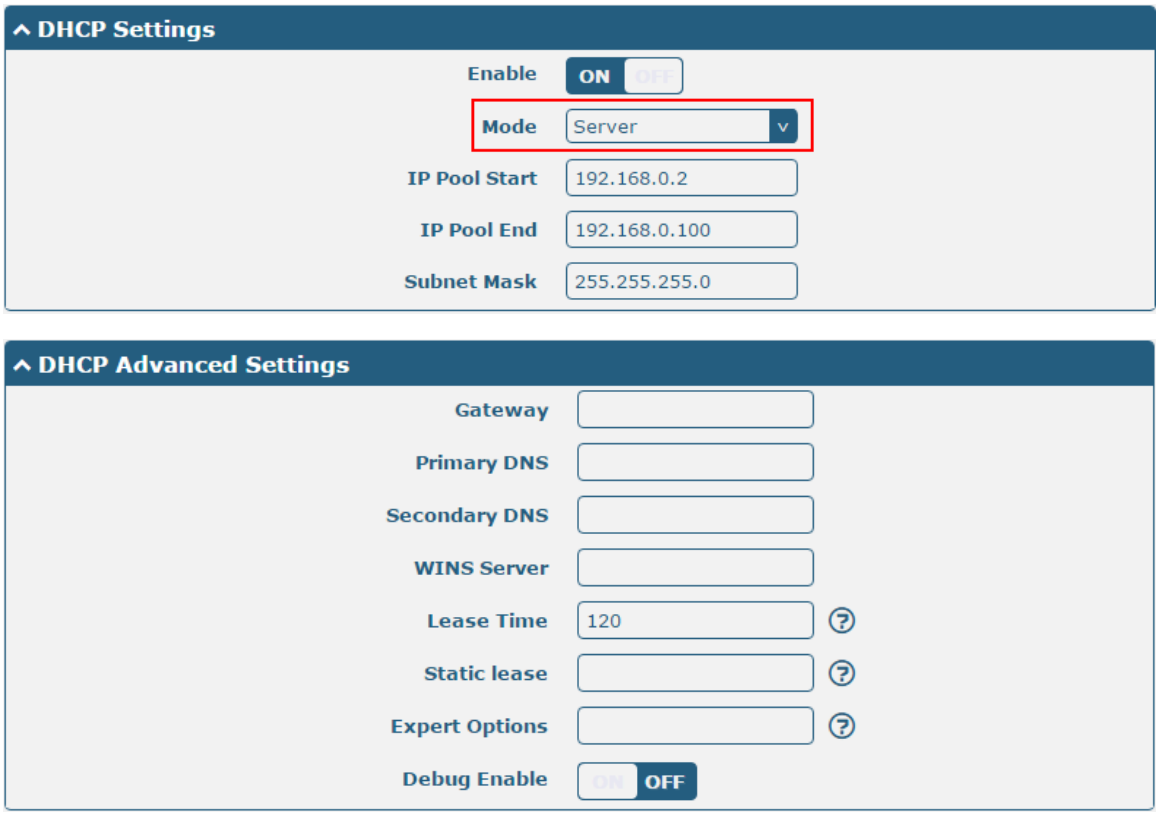
Note: Lan0 cannot be deleted.

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

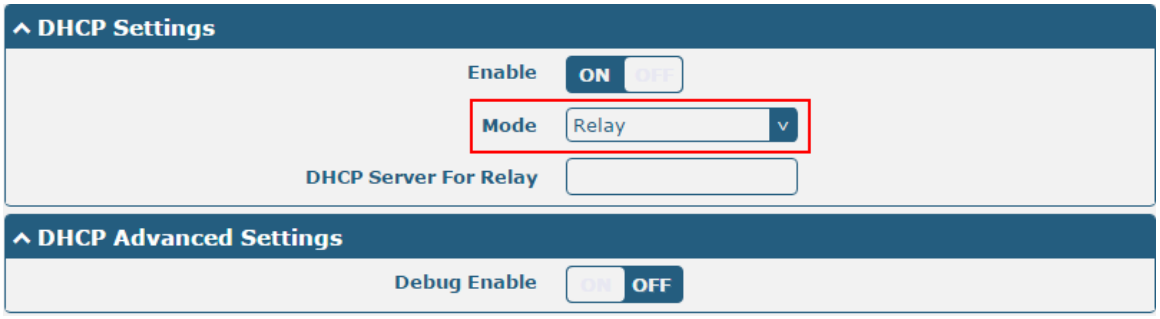


General Settings @ LAN		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Interface	Show the editing port. **Note:** Lan1 is available only if it was selected by one of ETH1~ETH3 in **Ethernet > Ports > Port Settings**.	-- lan0
IP Address	Set the IP address of the LAN port.	192.168.0.1
Netmask	Set the Netmask of the LAN port.	255.255.255.0
MTU	Enter the Maximum Transmission Unit.	1500
VLAN ID	Enter the VLAN ID corresponding to the lan interface to divide the eth interface in the same lan into the same vlan.	0

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



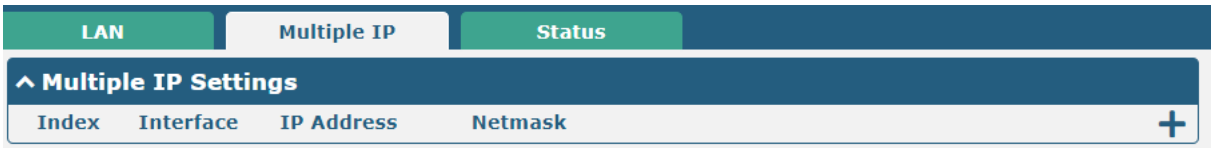
The window is displayed as below when choosing “Relay” as the mode.



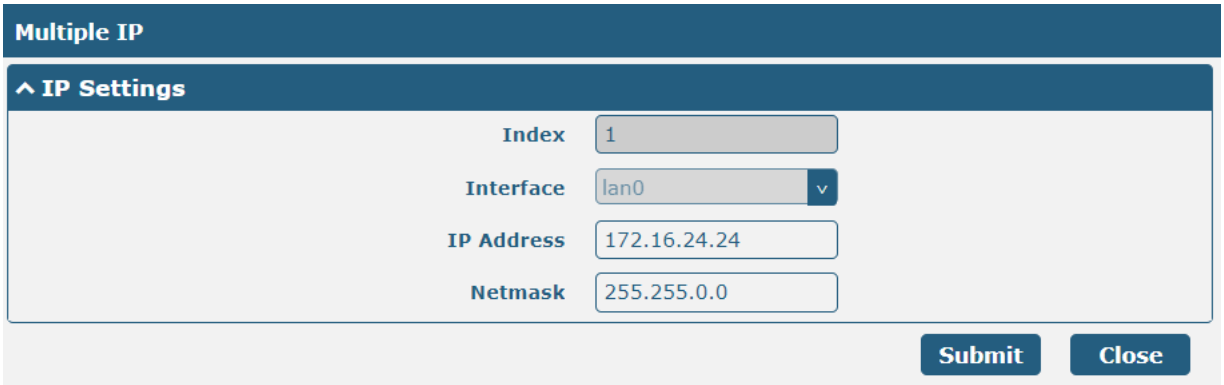
LAN		
Item	**Description**	**Default**
DHCP Settings		
Enable	Click the toggle button to enable/disable the DHCP function.	ON
Mode	Select from “Server” or “Relay”. • Server: Lease IP address to DHCP clients which have been connected to LAN port • Relay: Router can be DHCP Relay, which will provide a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

LAN		
Item	**Description**	**Default**
IP Pool End	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.0.100
Subnet Mask	Define the subnet mask of IP address obtained by DHCP clients from DHCP server.	255.255.255.0
DHCP Server for Relay	Enter the IP address of DHCP relay server.	Null
DHCP Advanced Settings		
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



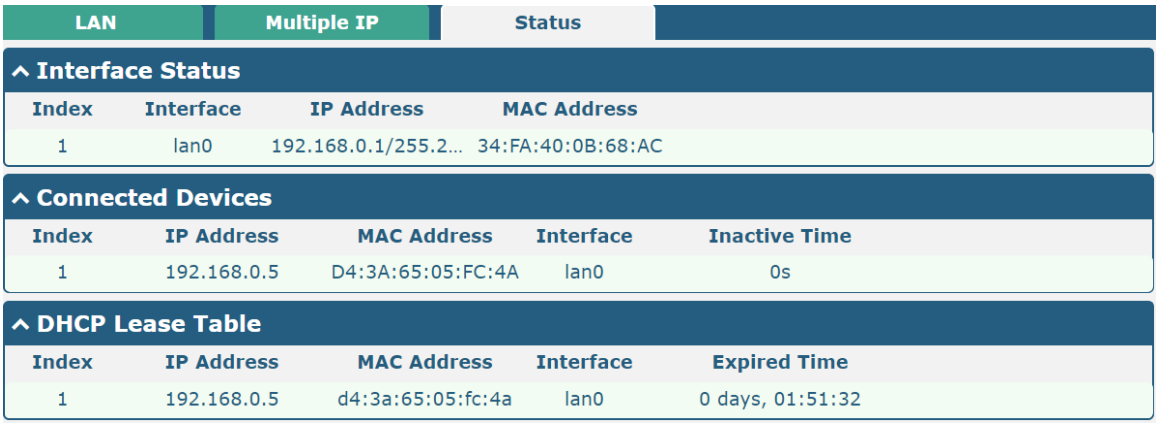
You may click ➕ to add a multiple IP to the LAN port, or click ✖ to delete the multiple IP of the LAN port. Now, click 📝 to edit the multiple IP of the LAN port.



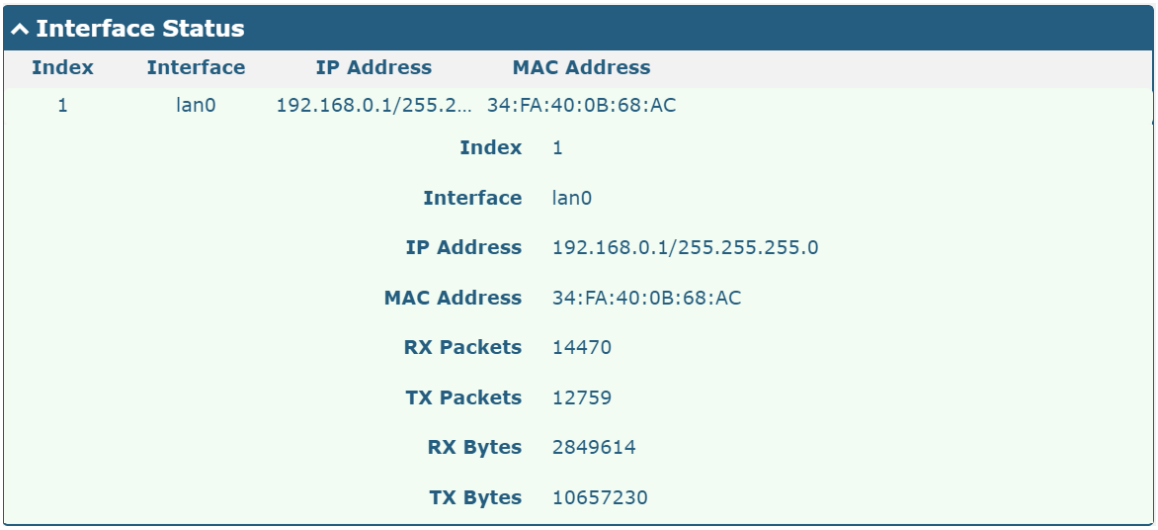
IP Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Interface	Show the editing port, read only.	--
IP Address	Set the multiple IP address of the LAN port.	Null
Netmask	Set the multiple Netmask of the LAN port.	Null

Status

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



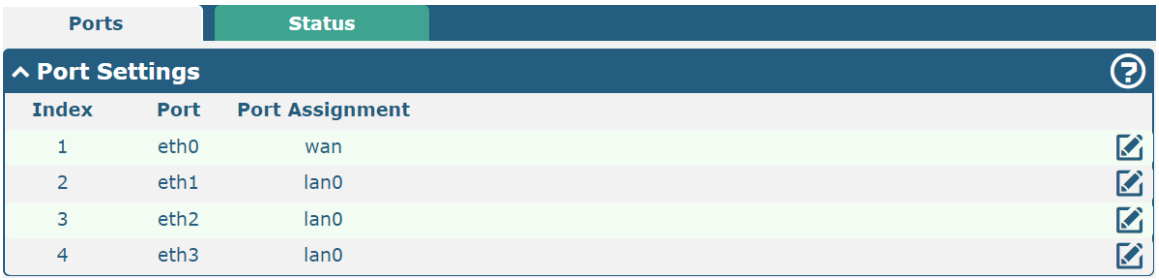
Click the row of status, the details status information will be display under the row. Please refer to the screenshot below.



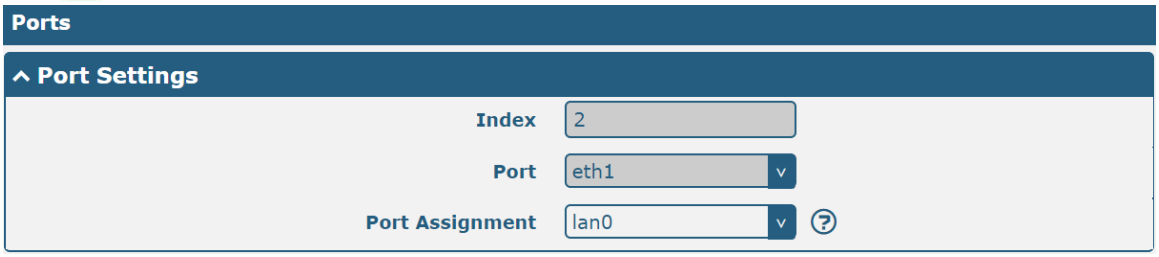
4.2.3 Ethernet

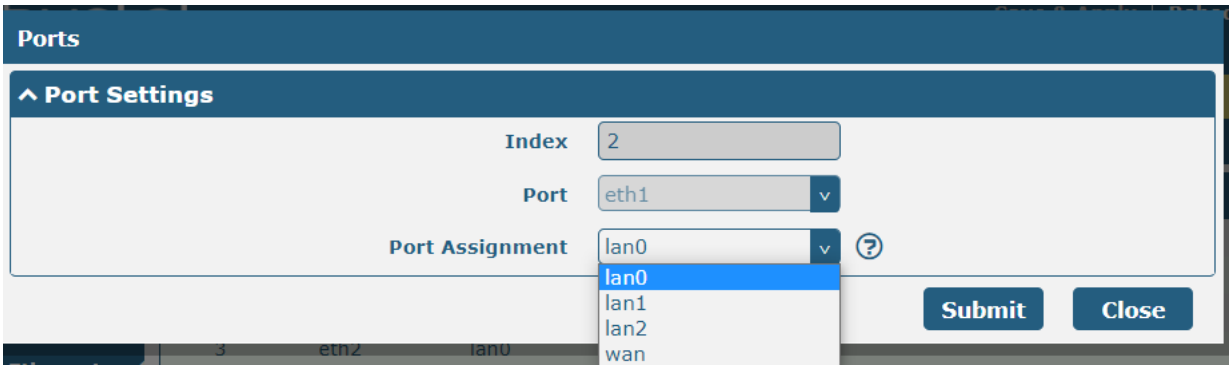
This section allows you to set the related parameters for Ethernet. There are four Ethernet ports on R5020 Router, including ETH0, ETH1, ETH2 and ETH3. The ETH0 on the router can be configured as a WAN port, while ETH1, ETH2 and ETH3 can only be configured as a LAN port. By default, ETH1, ETH2 and ETH3 are lan0, and their IP are

192.168.0.1/255.255.255.0.



Click button of eth1 to configure its parameters. Modify the network port parameters in the pop-up port window.

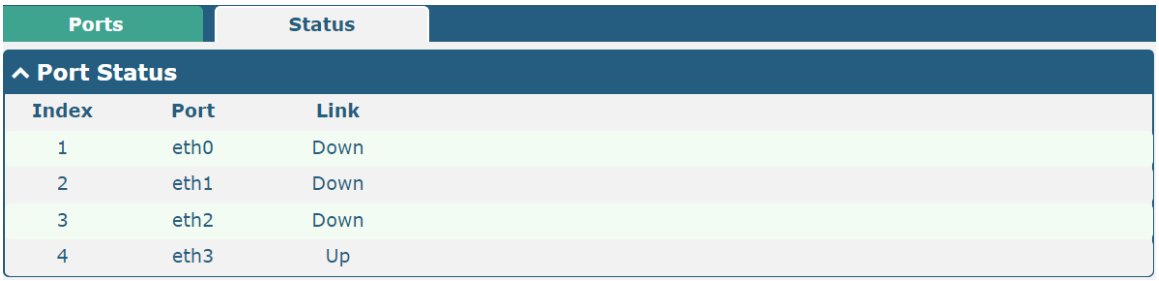




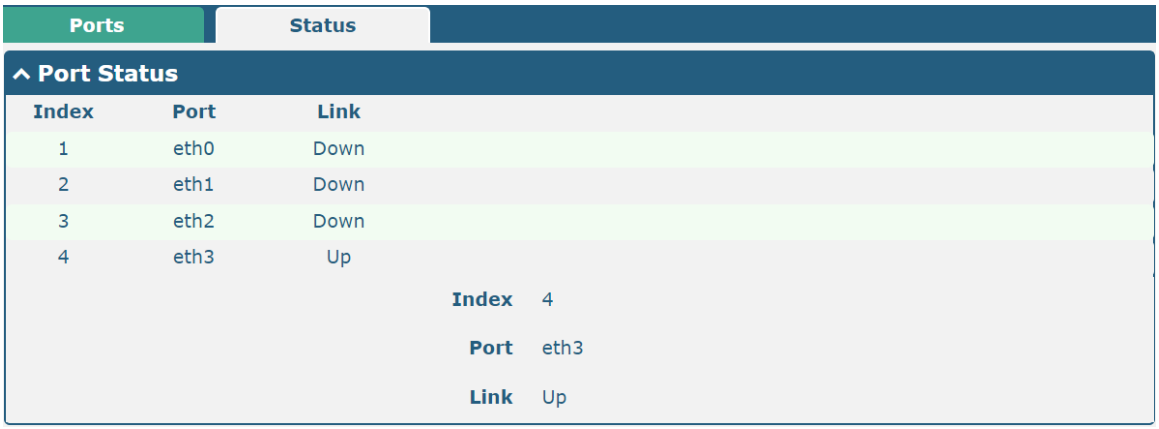
Port Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Port	Show the editing port, read only.	--
Port Assignment	Select the type of network port, WAN port or LAN port. When set it as LAN port in "Interface > LAN > LAN > Network Settings > General Setting", can select lan0 or lan1 or lan2 from the drop-down box.	Lan0

Port Settings		
Item	**Description**	**Default**
SFE Fast	Enabling SFE Fast improves the throughput of the Ethernet or cellular module, but affects the QoS function. If you need to use QoS APP, you need to turn off the SFE Fast function.	--ON

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

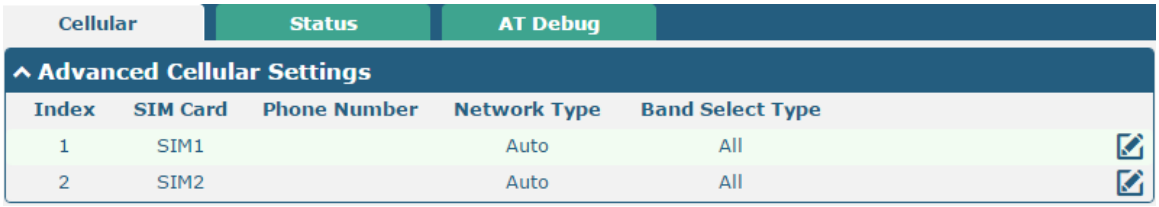


Click the row of status, the details status information will be display under the row. Please refer to the screenshot below.

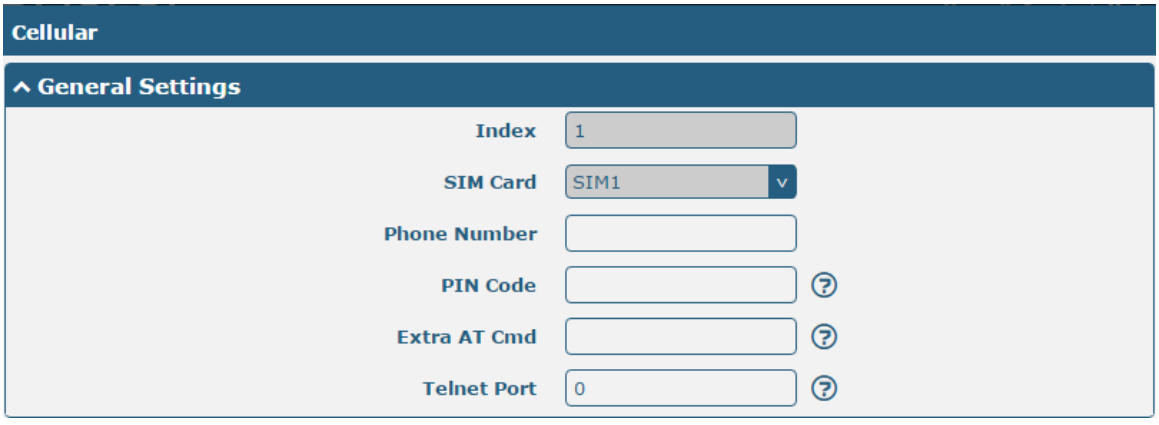


4.2.4 Cellular

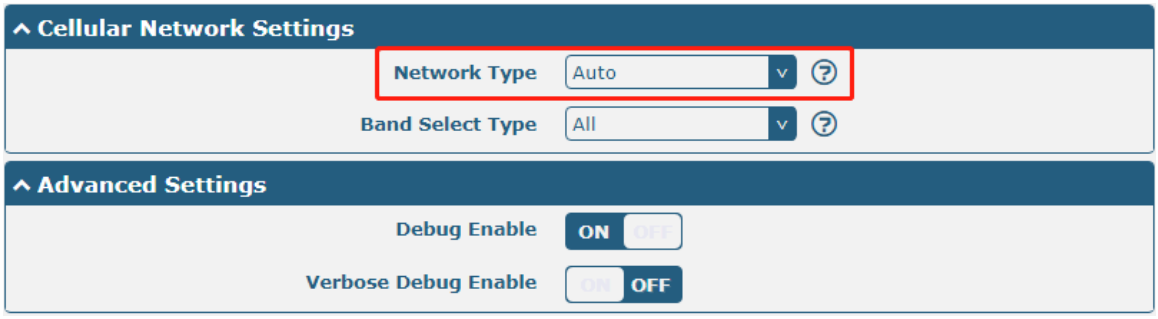
This section allows you to set the related parameters of Cellular. The R5020 Router has two SIM card slots. If insert single SIM card at the first time, SIM1 slot and SIM2 slots are available.



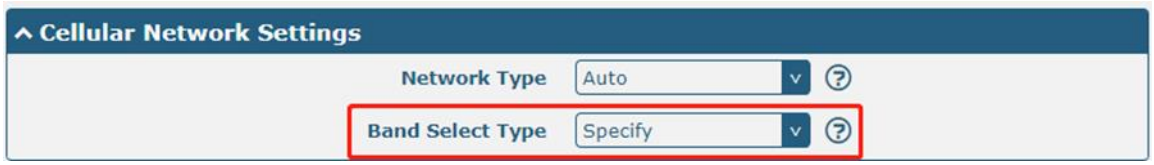
Click of SIM 1 to edit the parameters.

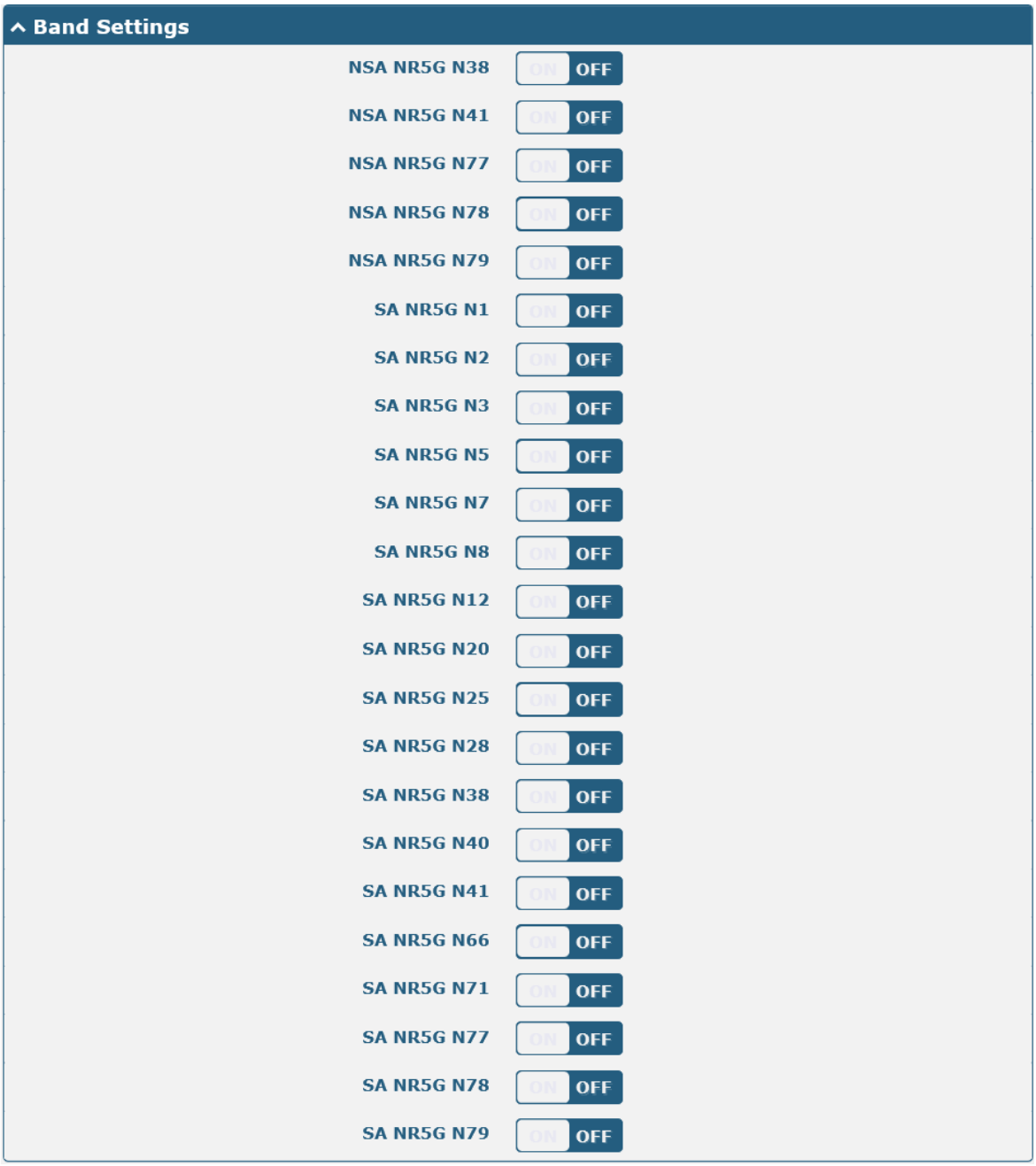


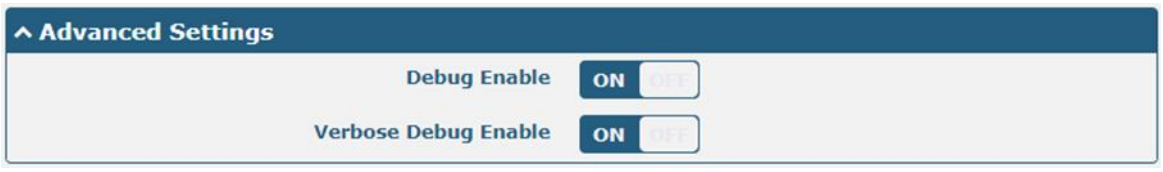
The window is displayed as below when choosing “Auto” as the network type.



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



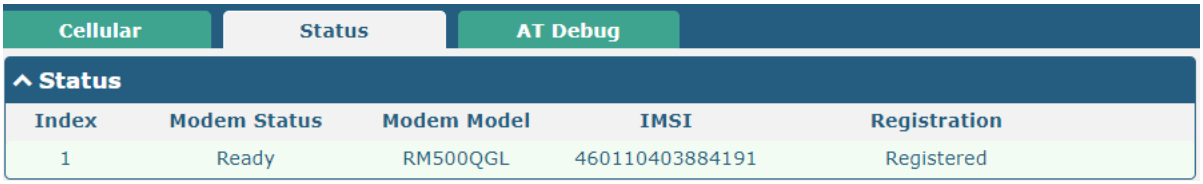




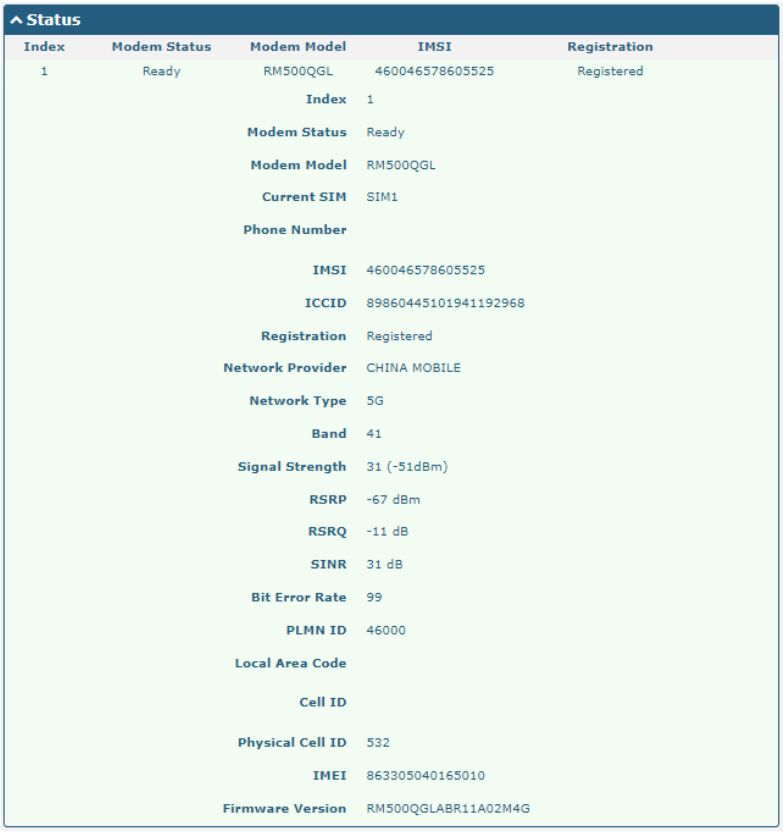
Cellular		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
SIM Card	Set the currently editing SIM card.	SIM1
Phone Number	Enter the phone number of the SIM card.	Null
PIN Code	Enter a 4-8 characters PIN code used for unlocking the SIM.	Null

Cellular		
Item	**Description**	**Default**
Extra AT Cmd	Enter the AT commands used for cellular initialization.	Null
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet.	0
Cellular Network Settings		
Network Type	Select from "Auto", "3G Only", and "4G Only". • Auto: Connect to the best signal network automatically • 3G Only: Only the 3G network is connected • 4G Only: Only the 4G network is connected	Auto
Band Select Type	Select from "All" or "Specify". You may choose certain bands if choosing "Specify".	All
Advanced Settings		
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF
Network Registration Timeout	The timeout required for the module to register to the network. 0 indicates that the default configuration is used.	0

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



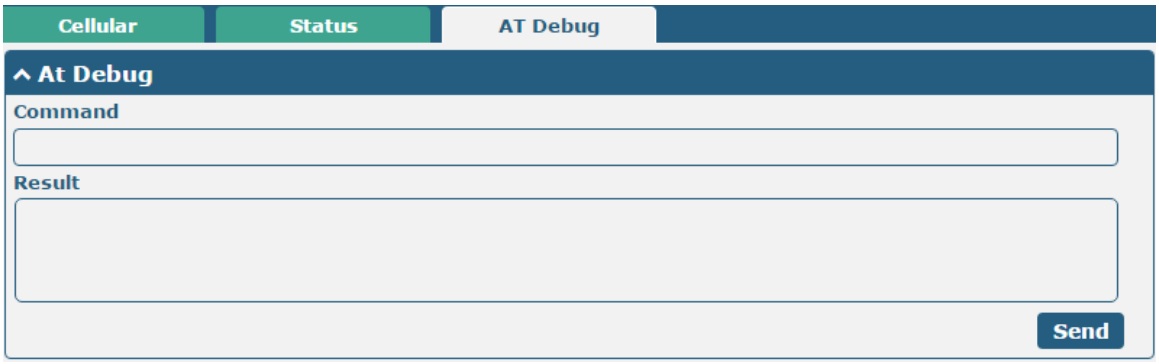
Click the row of status, the details status information will be displayed under the row.



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: SIM1 or SIM2
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/SIM2 > 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.
Band	Show the band of the current network.
Signal Strength	Show the signal strength detected by the mobile.
RSRP	Show the Reference Signal Receiving Power detected by the mobile.
RSRQ	Show the Reference Signal Received Quality detected by the mobile.
SINR	Show the Signal to Interference plus Noise Ratio detected by the mobile.
Bit Error Rate	Show the current bit error rate.
PLMN ID	Show the current PLMN ID.
Local Area Code	Show the current local area code used for identifying different area.
Cell ID	Show the current cell ID used for locating the router.

Status	
Item	**Description**
PCI	Show the current Physical Cell ID.
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.	--

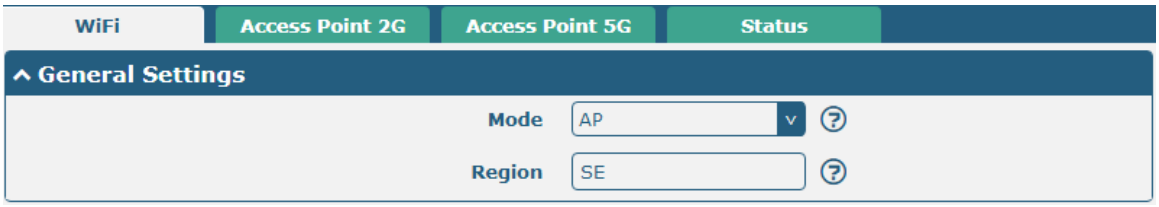
4.2.5 WiFi

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

WiFi AP

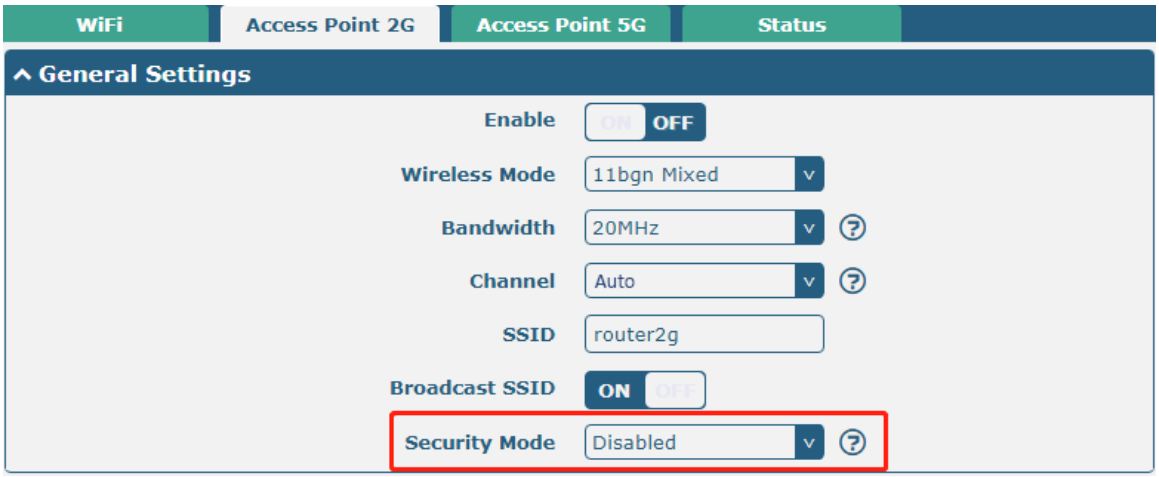
Configure Router as WiFi AP

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

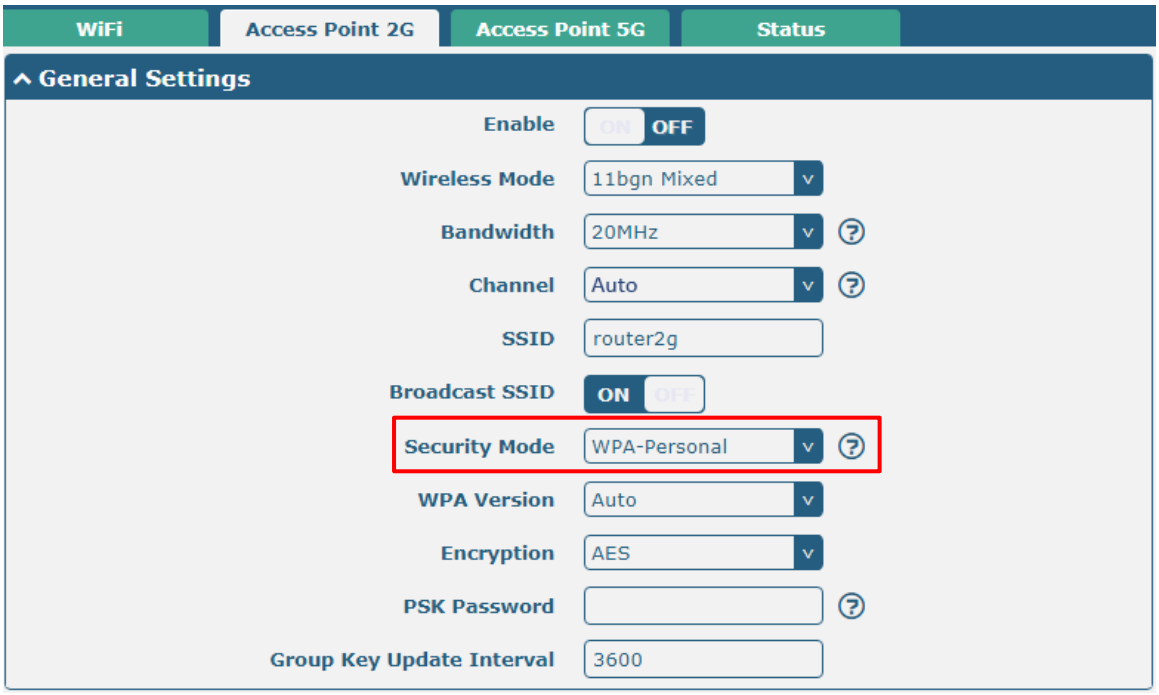


Note: Please remember to click **Save & Apply** after finish the configuration, so that the configuration can be took effect.

Click the **Access Point 2G** column to configure the parameters of WiFi AP. By default, the security mode is set as "Disabled".



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

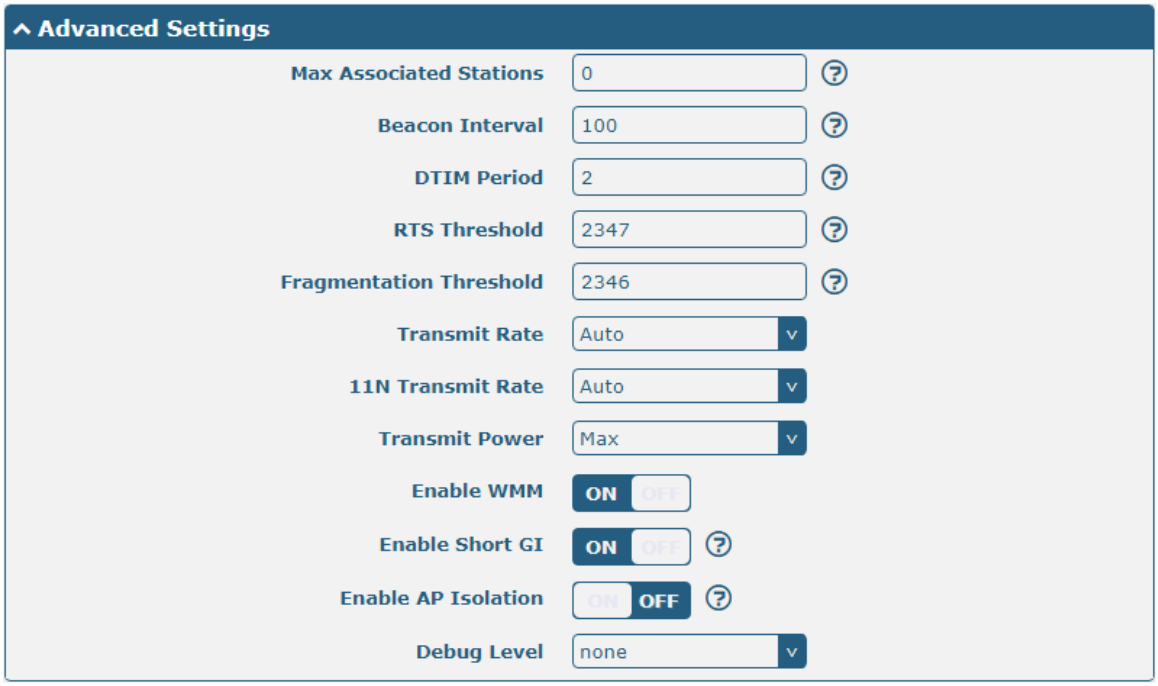


The window is displayed as below when setting “WEP” as the security mode.

General Settings @ Access Point 2G		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the WiFi access point option.	OFF
Wireless Mode	Select from “11bgn Mixed”, “11b only”, “11g only” and “11n only”. • 11bgn Mixed: mix three protocols for backward compatibility • 11b only: IEEE 802.11b, 11 Mbps~2.4GHz • 11g only: IEEE 802.11g, 54 Mbps~2.4GHz • 11n only: IEEE 802.11n, 450 Mbps	11bgn Mixed

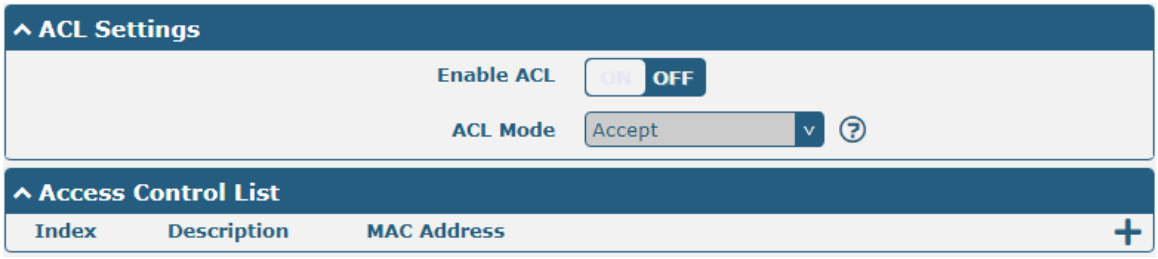
General Settings @ Access Point 2G		
Item	**Description**	**Default**
Bandwidth	Select from “20 MHz” or “40MHz”. **Note**: 40 MHz channel width provides twice the data rate available over a single 20 MHz channel;	20MHz
Channel	The channel that different bandwidth can choose is as follows. • Auto: Router will scan all frequency channels until the best one is found • The frequency of 1~13 channels of 20MHz bandwidth available 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 • The frequency of 1~13 channels of 40MHz bandwidth available 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.	router2g

General Settings @ Access Point 2G		
Item	**Description**	**Default**
Broadcast SSID	Click the toggle button to enable/disable the SSID being broadcast. When enabled, the client can scan your SSID. When disabled, the client cannot scan your SSID. If you want to connect to the router AP, you need to manually enter the SSID of router AP at WiFi client side.	ON
Security Mode	Select from "Disabled", "WPA-Personal"or "WEP". • Disabled: User can access the WiFi without password **Note**: It is strongly recommended for security purposes that you do not choose this kind of mode. • WPA-personal: WiFi access protection, only one password is provided for identity authentication • WEP: Wired Equivalent Privacy provides encryption for wireless device's data transmission	Disabled
WPA Version	Select from "Auto", "WPA" or "WPA2". • Auto: Router will choose automatically the most suitable WPA version • WPA2 is a stronger security feature than WPA	Auto
Encryption	Select from "TKIP" or "AES". • TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication • AES: AES encryption uses a wireless connection. AES can be used for CCMP WPA-PSK and WPA 802.1x authentication. AES is a stronger encryption algorithm than TKIP **Note:** The security mode will affect wireless communication rate. Different wireless modes support different encryption modes. For example, 802.11n supports neither WEP security mode nor TKIP algorithm. If they are used, the wireless communication rate will reduce to 54Mbps (802.11g mode). It is recommended to select AES in 802.11n mode.	AES
PSK Password	Enter the Pre share key password. Enter 8 to 63 characters.	Null
Group Key Update Interval	Enter the time period of group key renewal.	3600
WEP Key	Enter the WEP key. The key length should be 10 or 26 hexadecimal digits depending on which WEP key is used, 64 digits or 128 digits.	Null



Advanced Settings @ Access Point 2G		
Item	**Description**	**Default**
Max Associated Stations	Set the max number of clients allowed to access the router's AP. (Value 0 means without limitation)	0
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 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 WiFi 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.	Auto
11N Transmit Rate	Specify the transmit rate under the IEEE 802.11n mode or let is default to "Auto". Select from MCS0, MCS1, MCS2, MCS3, MCS4, MCS5, MCS6, MCS7, MCS8, MCS9, MCS10, MCS11, MCS12, MCS13, MCS14 and MCS15.	Auto
Transmit Power	Select from "Max", "High", "Medium" or "Low".	Max
Enable WMM	Click the toggle button to enable/disable the WMM option.	ON
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

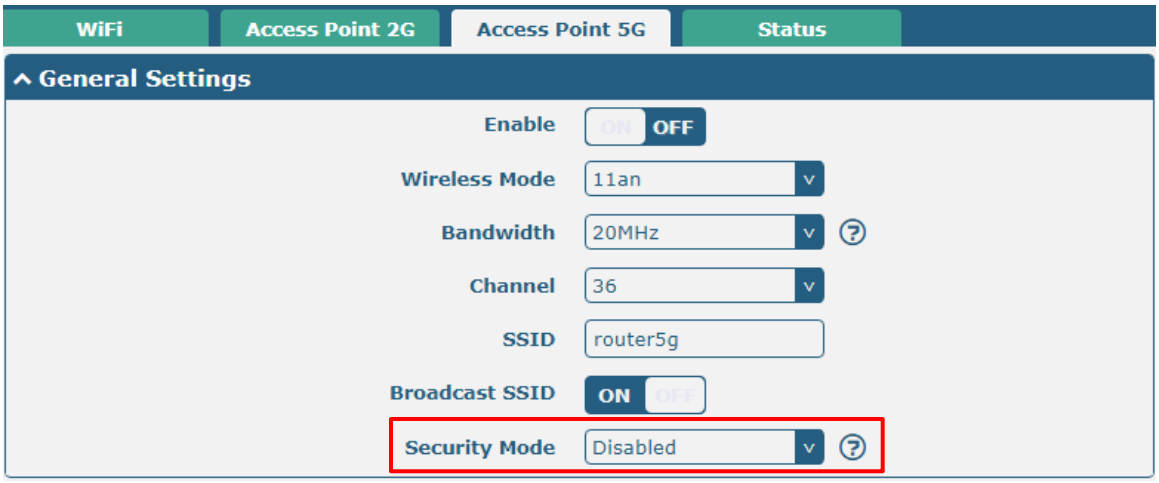
Advanced Settings @ Access Point 2G		
Item	**Description**	**Default**
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option. When enabled, the router will isolate all connected wireless devices. The wireless device cannot access the router directly via WLAN.	OFF
Debug Level	Select from “verbose”, “debug”, “info”, “notice”, “warning” or “none”.	none



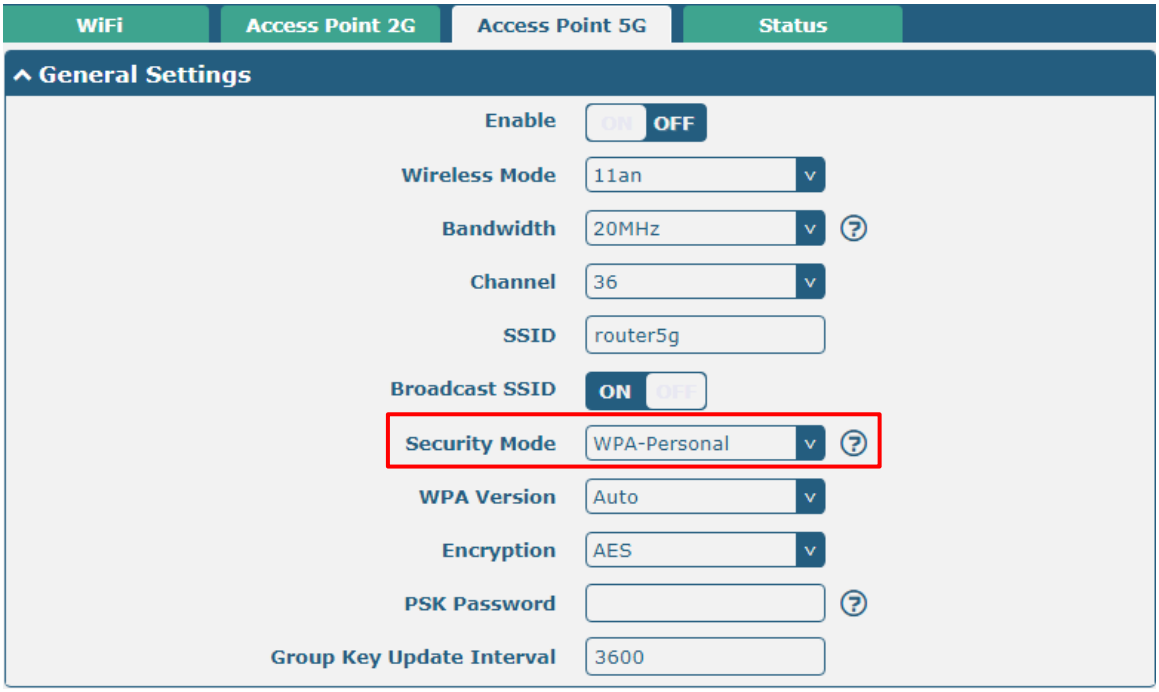
Click + to add a MAC address to the Access Control List. The maximum count for MAC address is 64.

ACL Settings @ Access Point 2G		
Item	**Description**	**Default**
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 @ Access Point 2G		
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

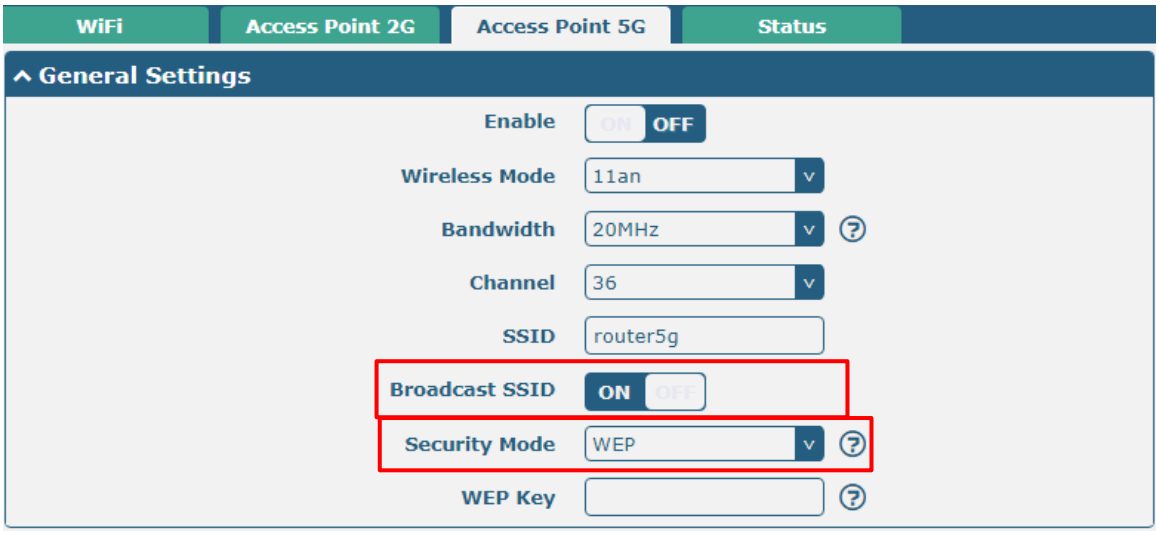
Click the **Access Point 5G** column to configure the parameters of WiFi AP. By default, the security mode is set as “Disabled”.



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



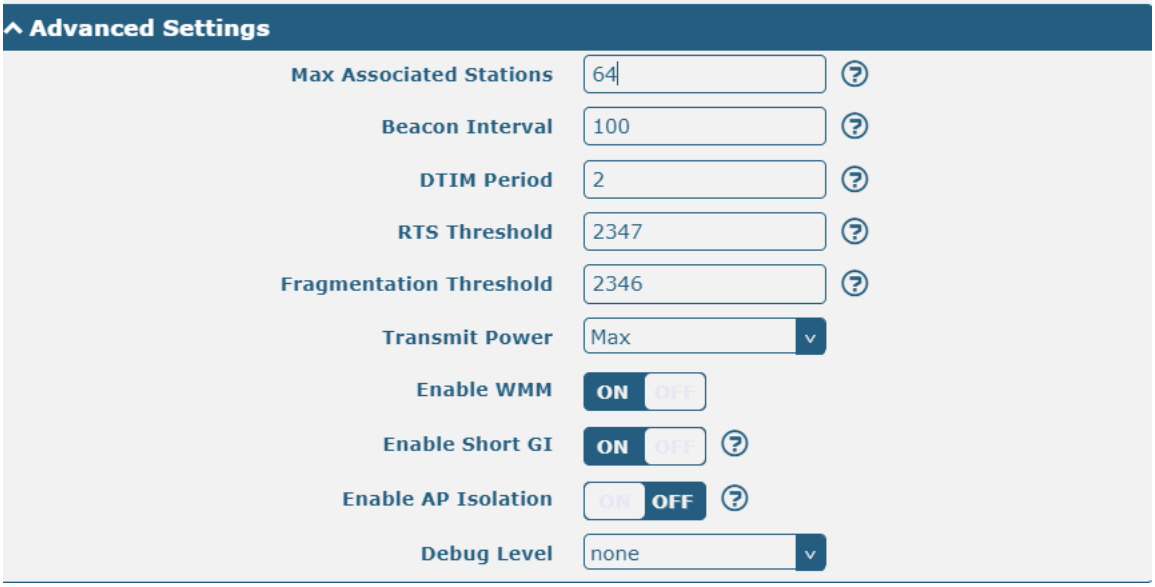
The window is displayed as below when setting "WEP" as the security mode.



General Settings @ Access Point 5G		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the WiFi access point option.	OFF
Wireless Mode	Select from “11an”, or “11/a/an/ac”. • 11an : Compatible IEEE 802.11a, 54 Mbps and IEEE 802.11n, 300Mbps • 11n/a/an/ac: Compatible IEEE 802.11a, 54 Mbps, IEEE802.11n 300 Mbps and 802.11ac, 867 Mbps	11an
Bandwidth	Select from “20MHz”, “40MHz” or “80MHz”. **Note**: 40 MHz channel width provides twice the data rate available over a single 20 MHz channel; the data transfer rate of 80MHz bandwidth is 4 times greater than that of a single 20Mhz bandwidth.	20MHz
Channel	The optional channels for bandwidths are as below. • The frequency of 36~165 channels of 20MHz bandwidth available channels: 36–5180 MHz 40–5200 MHz 44–5220 MHz 48–5240 MHz 149–5745 MHz 153–5765 MHz 157–5785 MHz 161–5805 MHz 165–5825 MHz • The frequency of 36~165 channels of 40MHz bandwidth available channels: 36–5180 MHz 40–5200 MHz 44–5220 MHz 48–5240 MHz 149–5745 MHz 153–5765 MHz 157–5785 MHz 161–5805 MHz 165–5825 MHz • The frequency of 36~165 channels of 80MHz bandwidth available channels: 36–5180 MHz 40–5200 MHz 44–5220 MHz 48–5240 MHz 149–5745 MHz 153–5765 MHz	36

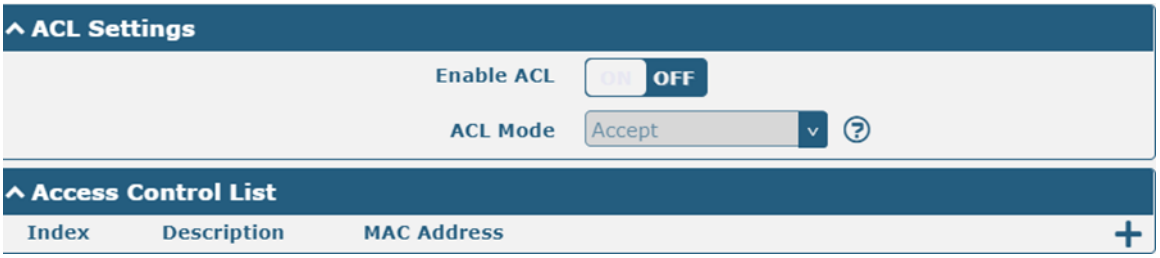
General Settings @ Access Point 5G		
Item	**Description**	**Default**
	157–5785 MHz 161–5805 MHz 165–5825 MHz **Note:** All available channels of 5GHz WiFi in different bandwidths are listed above. Web parameters should be configured due to the different available channels in different countries and areas.	
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.	router5g
Broadcast SSID	Click the toggle button to enable/disable the SSID being broadcast. When enabled, the client can scan your SSID. When disabled, the client cannot scan your SSID. If you want to connect to the router AP, you need to manually enter the SSID of router AP at WiFi client side.	ON
Security Mode	Select from “Disabled”, “WPA-Personal”, or “WEP”. • Disabled: User can access the WiFi without password **Note**: It is strongly recommended for security purposes that you do not choose this kind of mode. • WPA-personal: WiFi access protection, only one password is provided for identity authentication • 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 5G		
Item	**Description**	**Default**
Encryption	Select from "TKIP" or "AES". • TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication • AES: AES encryption uses a wireless connection. AES can be used for CCMP WPA-PSK and WPA 802.1x authentication. AES is a stronger encryption algorithm than TKIP **Note:** The security mode will affect wireless communication rate. Different wireless modes support different encryption modes. For example, 802.11n supports neither WEP security mode nor TKIP algorithm. If they are used, the wireless communication rate will reduce to 54Mbps (802.11g mode). It is recommended to select AES in 802.11n mode.	AES
PSK Password	Enter the Pre share key password. Enter 8 to 63 characters.	Null
Group Key Update Interval	Enter the time period of group key renewal.	3600
WEP Key	Enter the WEP key. The key length should be 10 or 26 hexadecimal digits depending on which WEP key is used, 64 digits or 128 digits.	Null



Advanced Settings @ Access Point 5G		
Item	**Description**	**Default**
Max Associated Stations	Set the max number of clients allowed to access the router's AP. (Value 0 means without limitation)	0

Advanced Settings @ Access Point 5G		
Item	**Description**	**Default**
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 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 WiFi AP. It is recommended that you use the default value 2346.	2346
Transmit Power	Select from "Max", "High", "Medium" or "Low".	Max
Enable WMM	Click the toggle button to enable/disable the WMM option.	ON
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. When enabled, the router will isolate all connected wireless devices. The wireless device cannot access the router directly via WLAN.	OFF
Debug Level	Select from "verbose", "debug", "info", "notice", "warning" or "none".	none

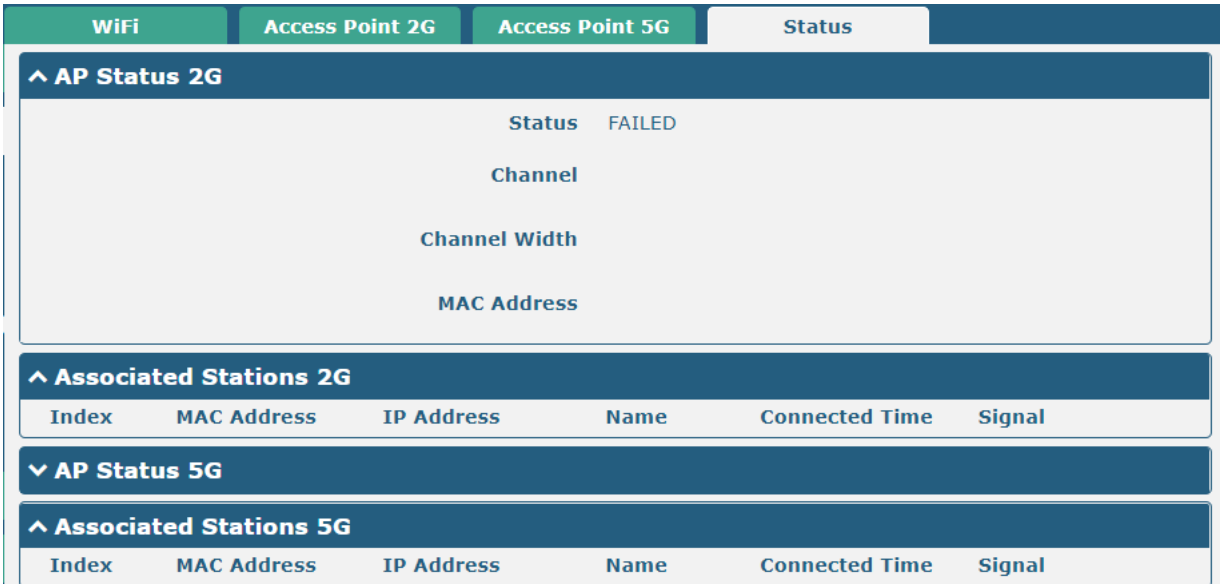


Click + to add a MAC address to the Access Control List. The maximum count for MAC address is 64.

ACL Settings @ Access Point 5G		
Item	**Description**	**Default**
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	Accept

ACL Settings @ Access Point 5G		
Item	**Description**	**Default**
	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.	
Access Control List @ Access Point 5G		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this access control list.	Null
MAC Address	Add a MAC address here.	Null

This section allows you to view the status of AP.



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

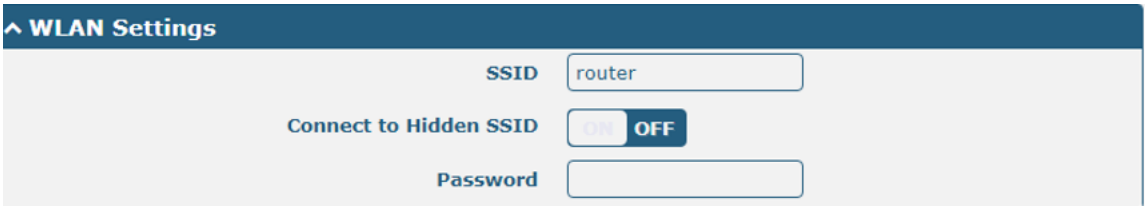
WiFi Client

Configure Router as WiFi Client

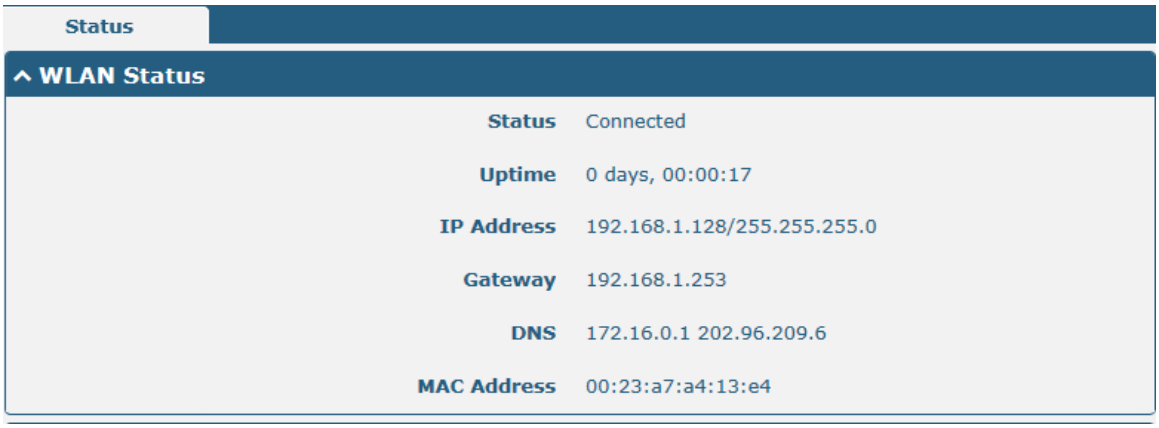
Click **Interface > WiFi > WiFi**, select "Client" as the mode and regarding the AP type to choose the related Client Band then click "Submit".

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

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

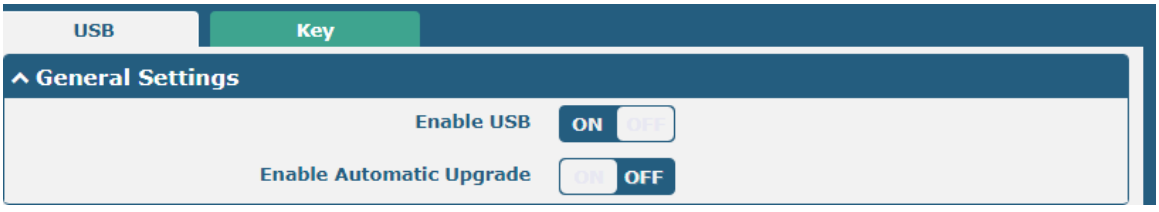


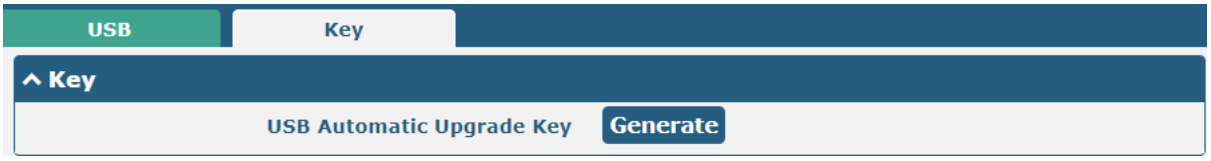
Click **Interface > WLAN** to configure the parameters of WiFi Client after setting the mode as Client. Please remember to click **Save & Apply > Reboot** after finish the configuration, so that the configuration can be took effect.



4.2.6 USB

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





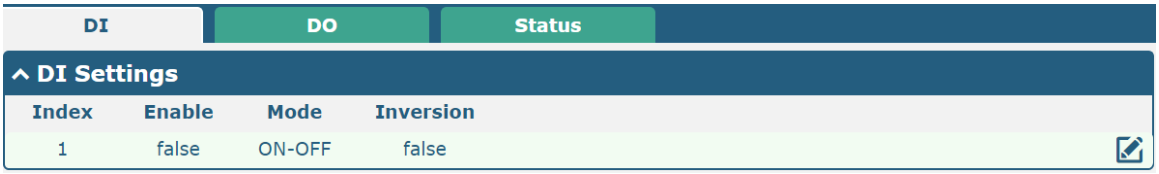
General Settings @ USB		
Item	**Description**	**Default**
Enable USB	Click the toggle button to enable/disable the USB option.	ON
Enable Automatic Upgrade	Click the toggle button to enable/disable this option. Enable to automatically update the firmware of the router when inserting a USB storage device with a router firmware.	OFF
Key		
Item	**Description**	**Default**
USB Automatic Update Key	Click Generate to generate a key, and click Download to download the key.	--

Note: In the process of USB auto upgrade, when using the USB auto-upgrade function, when the running light appears, it means the upgrade is in progress. When the running light stops and the USER light is on, it means the upgrade is complete. After upgrading, the device will not restart automatically. If there is no running light effect, it means that there is an abnormality and it does not enter into the automatic upgrade process

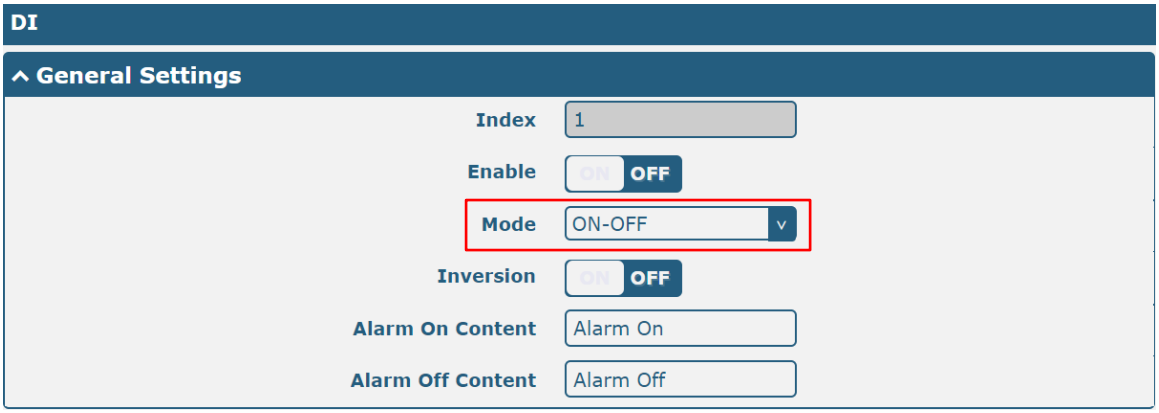
4.2.7 DI/DO

This section allows you to set the DI/DO parameters. Digital Input and Digital Output are the specific interfaces for R5020. The DI interface can be used for triggering alarm, while the DO can be used for controlling the slave device so as to realize real-time monitoring.

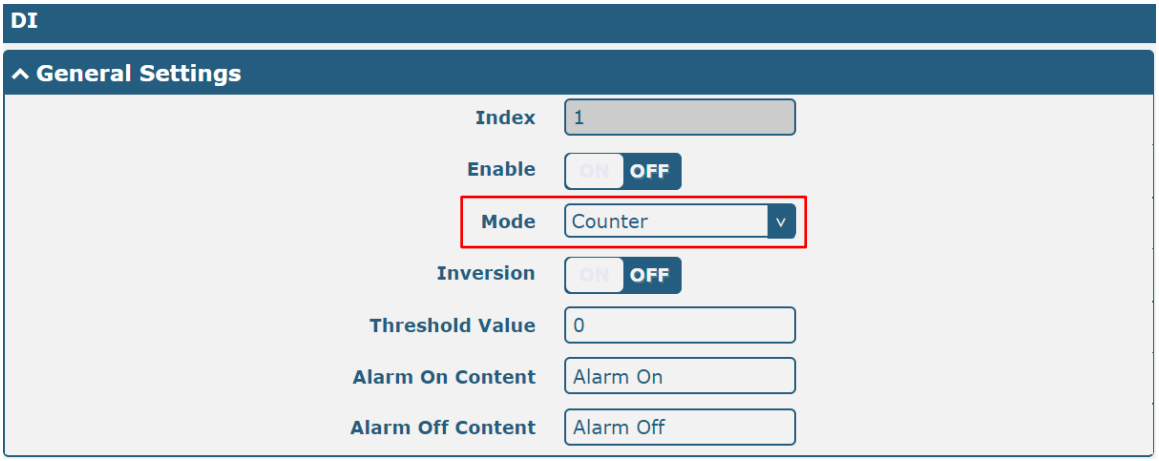
DI



Click the right-most button of index 1 as below. The default mode is “ON-OFF”.



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

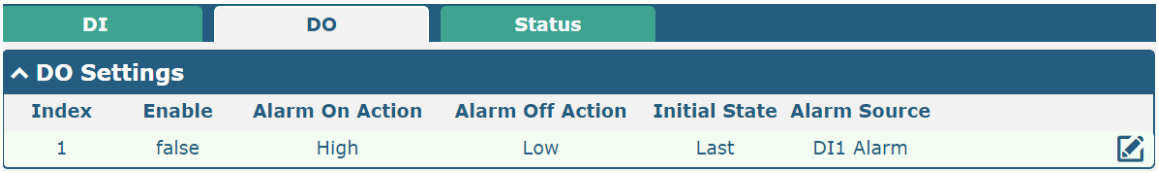


General Settings @ DI		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this DI.	OFF
Mode	Select from “ON-OFF” or “Counter”. • ON-OFF: DI interface support ON and OFF mode (high or low level electrical) trigger DI alarm. The mode default to ON, and OFF mode is available only when enabling the inversion feature ON—Under this mode, DI alarm status will be triggered to ON when DI interface open from GND or input a high level electrical (logic 1), on the contrary DI alarm status will be trigged to OFF when DI interface connect to GND or input a low level electrical (logic 0) OFF—Under this mode, DI alarm status will be triggered to ON when DI interface connect to GND or input a low level electrical (logic 0), on the contrary DI alarm status will be trigged to OFF when DI interface open from GND or input a high level electrical (logic 1) • Counter: Event counter mode	ON-OFF
Inversion	Click the toggle button to enable/disable this option. Enable to set DI mode as OFF mode.	OFF
Threshold Value	Set the threshold vale. It will trigger alarm when event counter reaches this	0

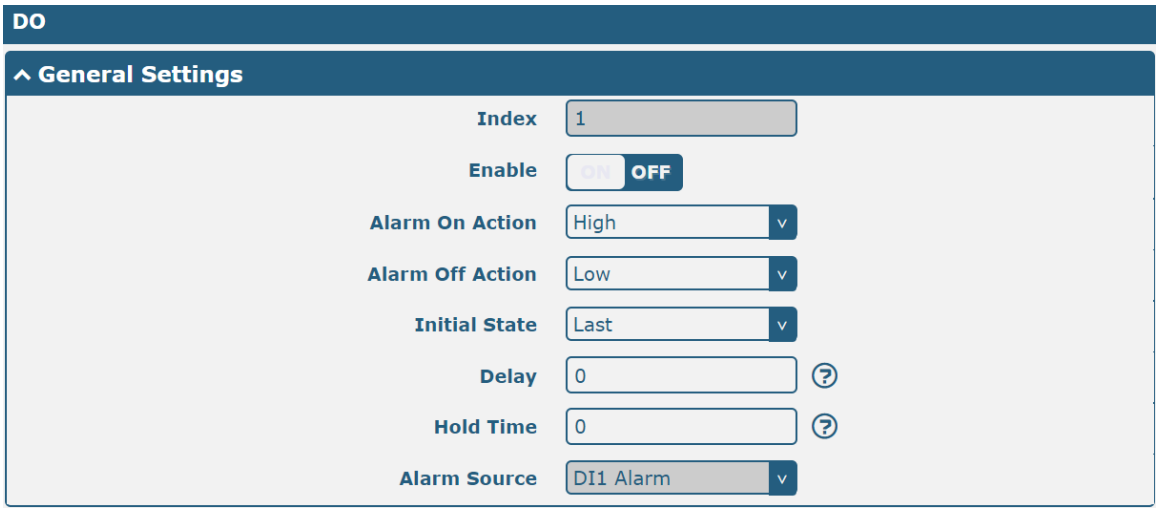
General Settings @ DI		
Item	**Description**	**Default**
	figure. After triggering alarm, DI will keep counting but not trigger alarm again. Enter 0 to 65535 digits. (0=will not trigger alarm) **Note**: This option is only available when DI under the "Counter" mode.	
Alarm On Content	Show the content when alarm on.	Alarm On
Alarm Off Content	Show the content when alarm off.	Alarm Off

Note: It defaults as high alarm, while turns to low alarm after enabling the "Inversion" button.

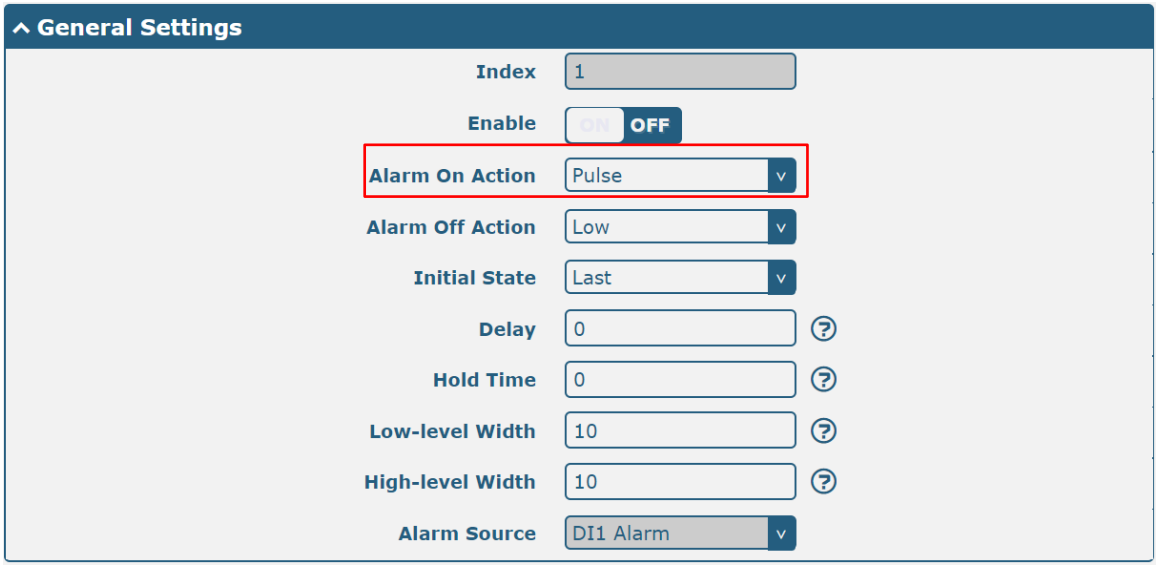
DO



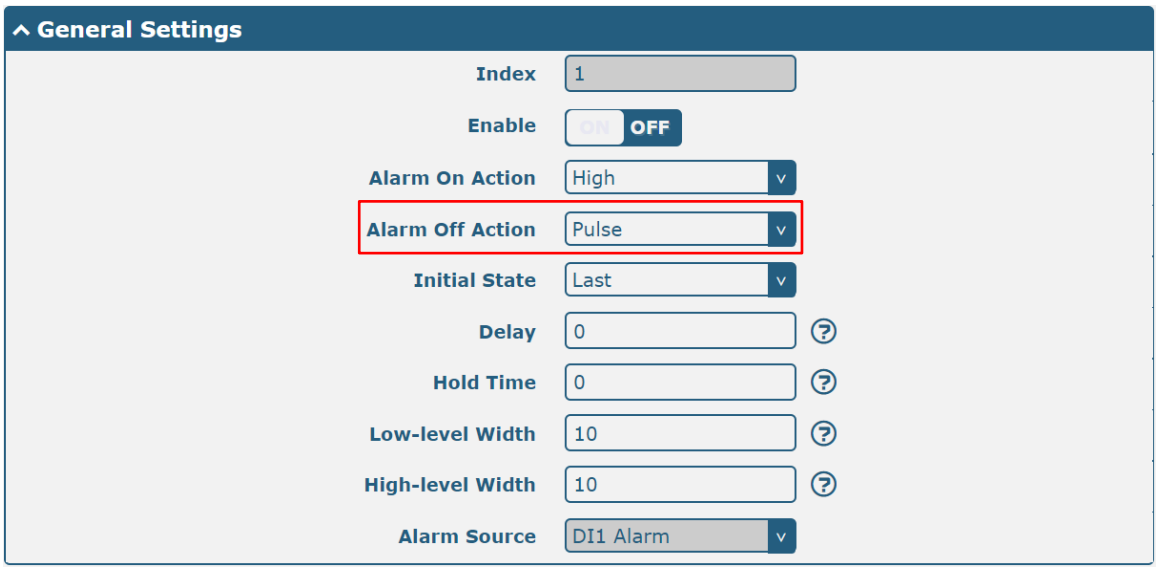
Click to enter the DO configuration window.



The window is displayed as below when choosing “Pulse” as the alarm on action.



The window is displayed as below when choosing “Pulse” as the alarm off action.

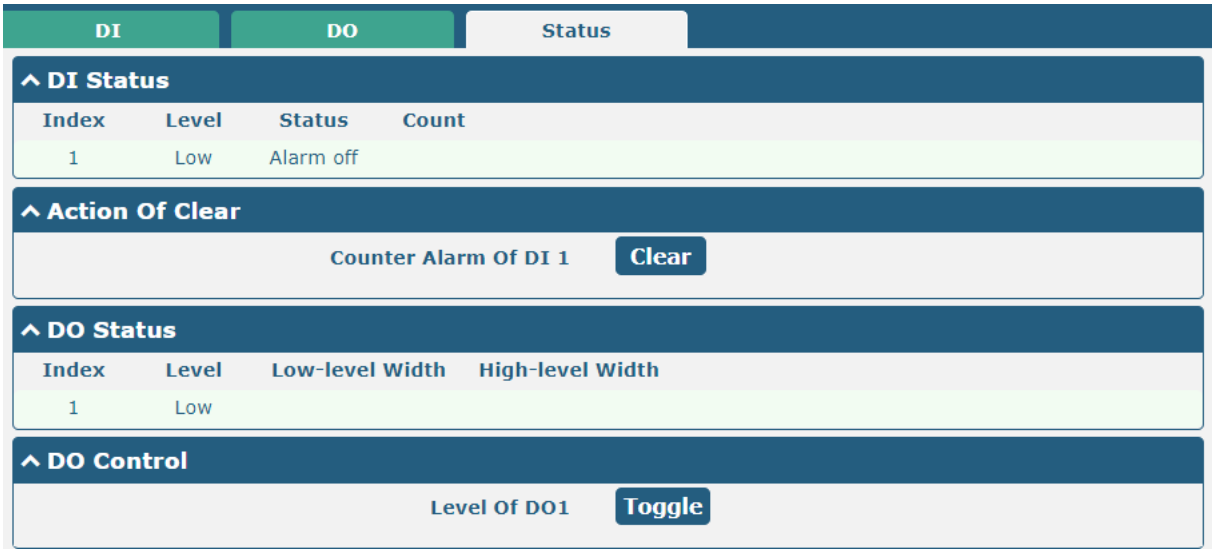


General Settings @ DO		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this DO.	OFF
Alarm On Action	Digital Output initiates when there is an alarm. Selected from “High”, “Low” or “Pulse”. • High: a high electrical level output • Low: a low electrical level output • Pulse: Generates a square wave as specified in the pulse mode parameters when triggered	High

General Settings @ DO		
Item	**Description**	**Default**
Alarm Off Action	Digital Output initiates when alarm removed. Selected from “High”, “Low” or “Pulse”. • High: a high electrical level output • Low: a low electrical level output • Pulse: Generates a square wave as specified in the pulse mode parameters when triggered	Low
Initial State	Specify the Digital Output status when powered on. Selected from “Last”, “High” or “Low”. • Last: DO’s status will consist with the status of last power off • High: DO interface is in high electrical level • Low: DO interface is in low electrical level	Last
Delay	Set the delay time for DO alarm start-up. The first pulse will be generated after a “Delay”. Enter from 0 to 300000ms. (0=generate pulse without delay)	0
Hold Time	Set the hold time of DO status (Alarm On Action/Alarm Off Action). When the action time reach this specified time, DO will stop the action. Enter from 0 to 3000 seconds. (0=keep on until the next action)	0
Low-level Width	Set the low-level width. It is available when enabling Pulse as “Alarm On Action/Alarm Off Action”. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low level widths are specified here. Enter from 1 to 3000 ms.	1000
High-level Width	Set the high-level width. It is available when enabling Pulse as “Alarm On Action/Alarm Off Action”. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The high level widths are specified here. Enter from 1 to 3000 ms.	1000
Alarm Source	Digital Output initiates according to different alarm source. Selected only “DI1 Alarm”. DI1 Alarm: Digital Output triggers the related action when there is alarm from Digital Input.	DI1

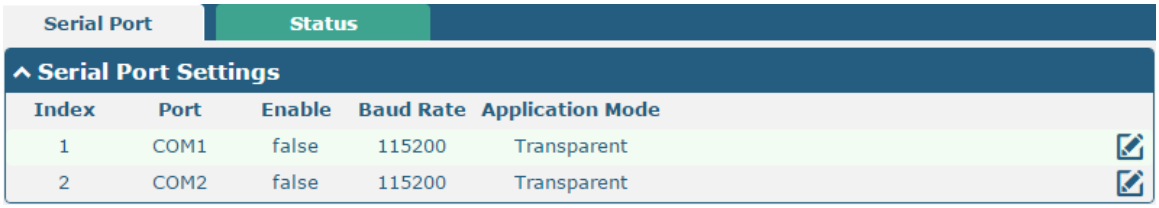
Status

This window allows you to view the status of DO and DI interface. It also can clear the counter alarm of DI in here. Click Clear button to clear DI1 or DI2 monthly usage statistics info for counter alarm.

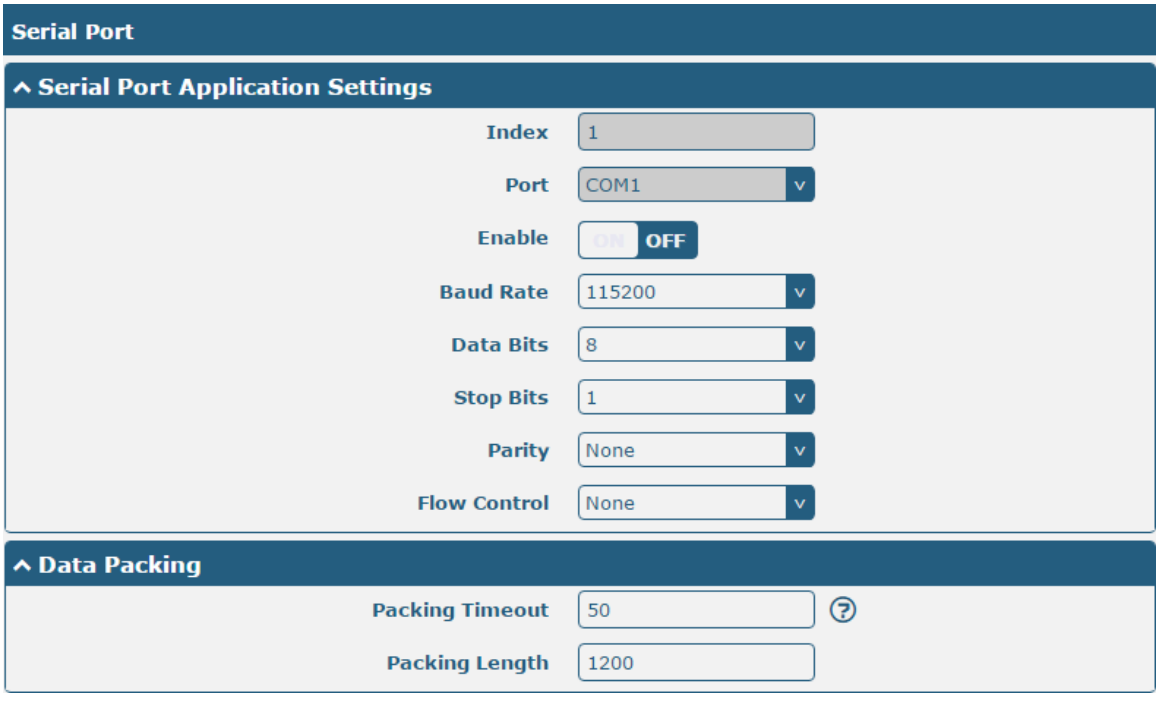


4.2.8 Serial Port

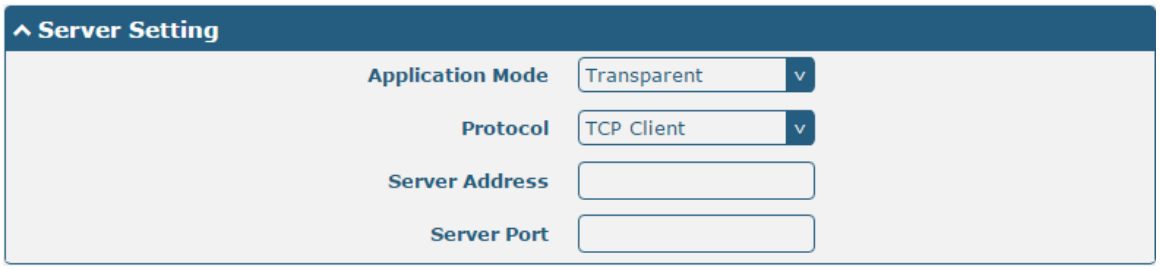
This section allows you to set the serial port parameters. R5020 Router supports one COM1 and one COM2, also can be configured as either two COM1 or two COM2. Serial port provides a way to transfer serial data to IP data, or vice versa, and transmit these data via wired or wireless network to achieve data transparent transmission.



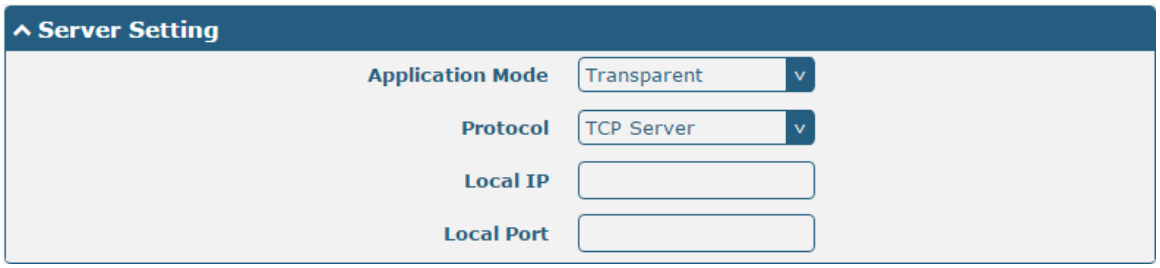
Click the edit button of COM1.



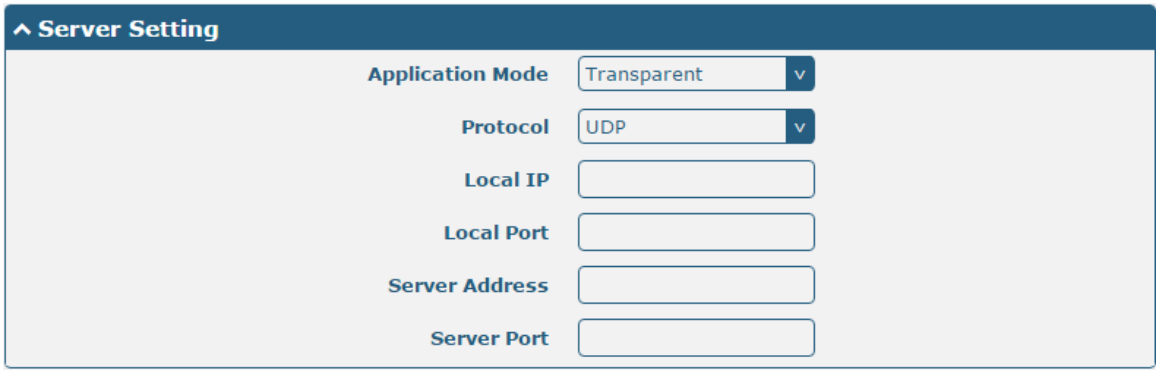
The window is displayed as below when choosing “Transparent” as the application mode and “TCP Client” as the protocol.



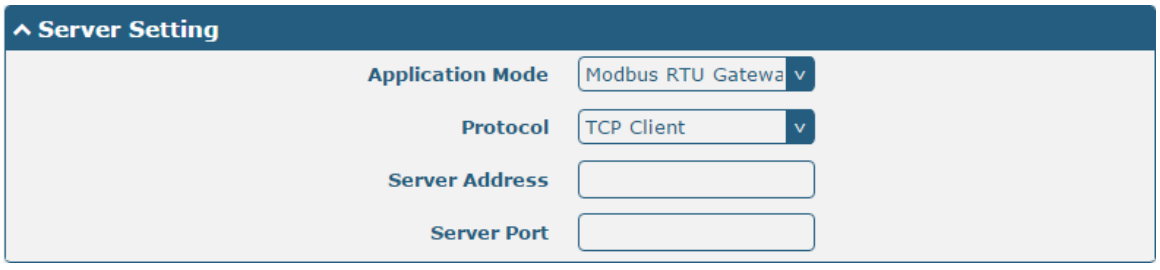
The window is displayed as below when choosing “Transparent” as the application mode and “TCP Server” as the protocol.



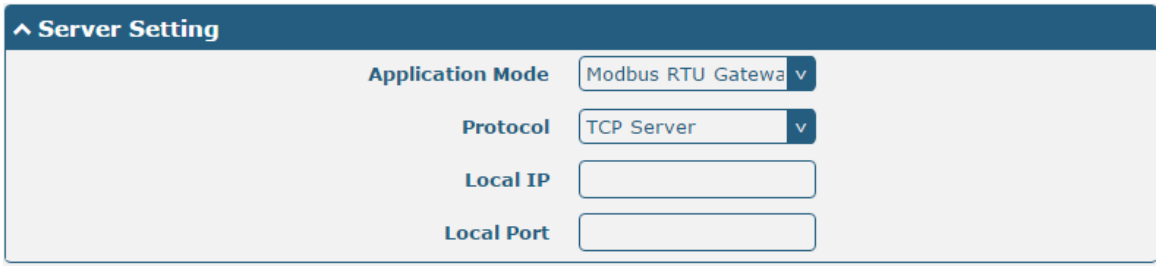
The window is displayed as below when choosing “Transparent” as the application mode and “UDP” as the protocol.



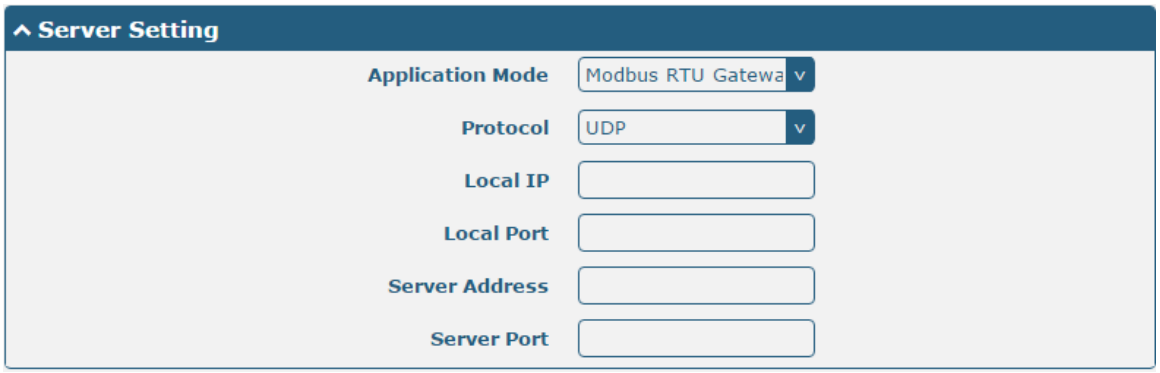
The window is displayed as below when choosing “Modbus RTU Router” as the application mode and “TCP Client” as the protocol.



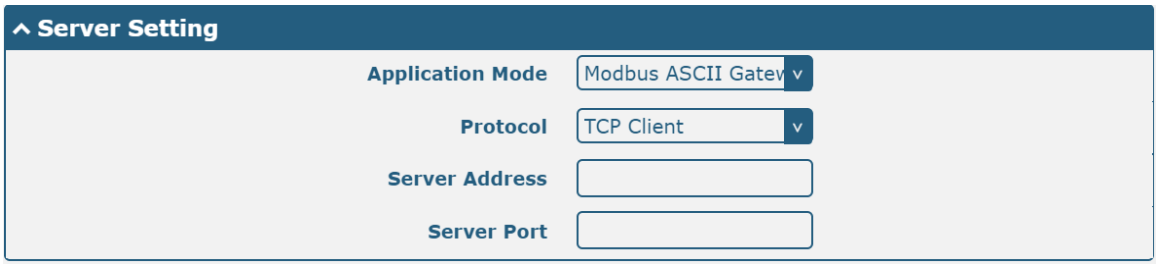
The window is displayed as below when choosing “Modbus RTU Router” as the application mode and “TCP Server” as the protocol.



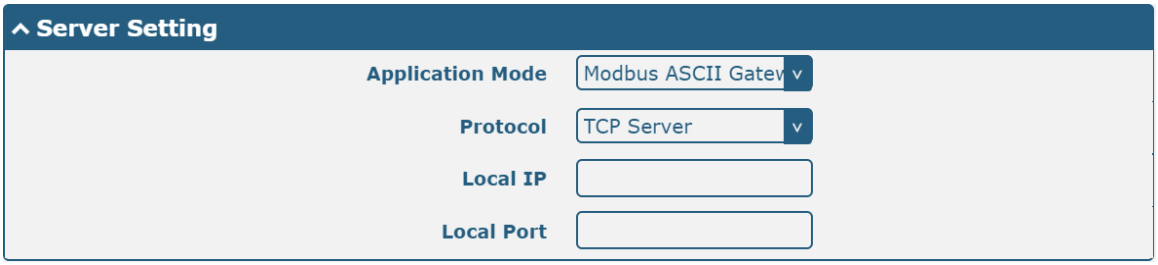
The window is displayed as below when choosing “Modbus RTU Router” as the application mode and “UDP” as the protocol.



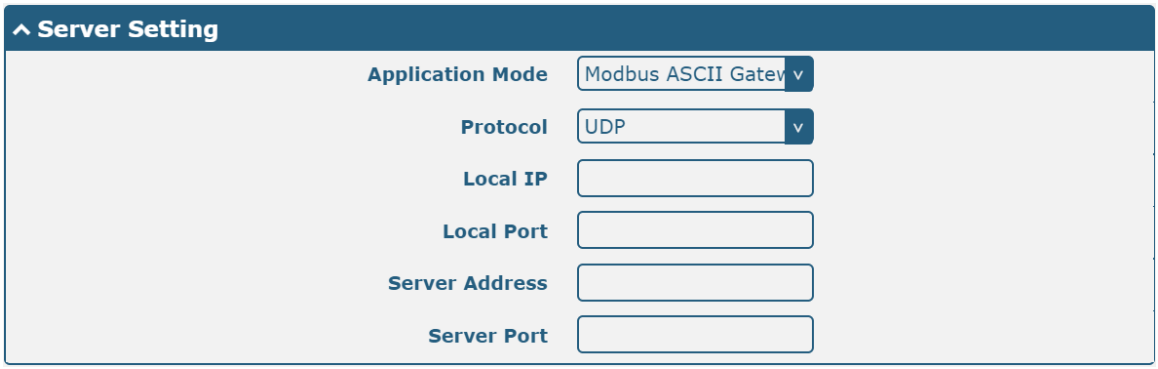
The window is displayed as below when choosing “Modbus ASCII Router” as the application mode and “TCP Client” as the protocol.



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



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

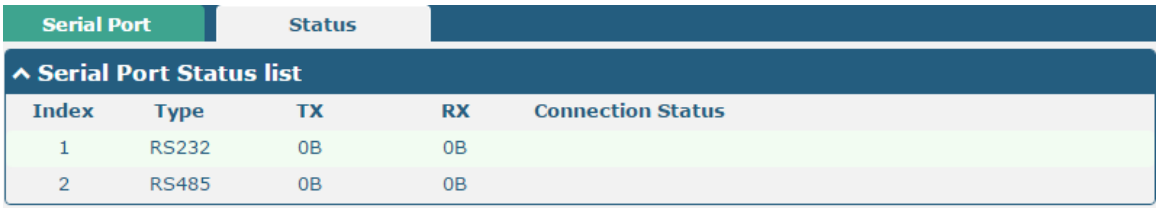


Serial Port		
Item	**Description**	**Default**
Serial Port Application Settings		
Index	Indicate the ordinal of the list.	--
Port	Show the current serial’s name, read only.	COM1--
Enable	Click the toggle button to enable/disable this serial port. When the status is OFF, the serial port is not available.	OFF
Baud Rate	Select from “300”, “600”, “1200”, “2400”, “4800”, “9600”, “19200”, “38400”, “57600” , “115200” or “230400”.	115200
Data Bits	Select from “7” or “8”.	8
Stop Bits	Select from “1” or “2”.	1
Parity	Select from “None”, “Odd” or “Even”.	None
Flow control	Select from “None”, “Software” or “Hardware”.	None
Data Packing		
Packing Timeout	Set the packing timeout. The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field. **Note**: Data will also be sent as specified by the packet length even when data is not reaching the interval timeout in the field.	50
Packing Length	Set the packet length. The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When a packet length between 1 and 3000 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.	1200

Server Settings		
Item	**Description**	**Default**
Application Mode	Select from “Transparent”, “Modbus RTU Router” or “Modbus ASCII Router”. • Transparent: Router will transmit the serial data transparently • Modbus RTU Router: Router will translate the Modbus RTU data to Modbus TCP data and sent out, and vice versa	Transparent

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

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

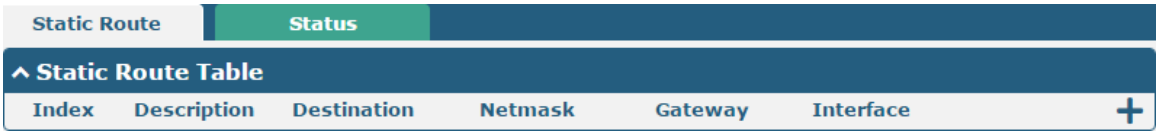


4.3 Network

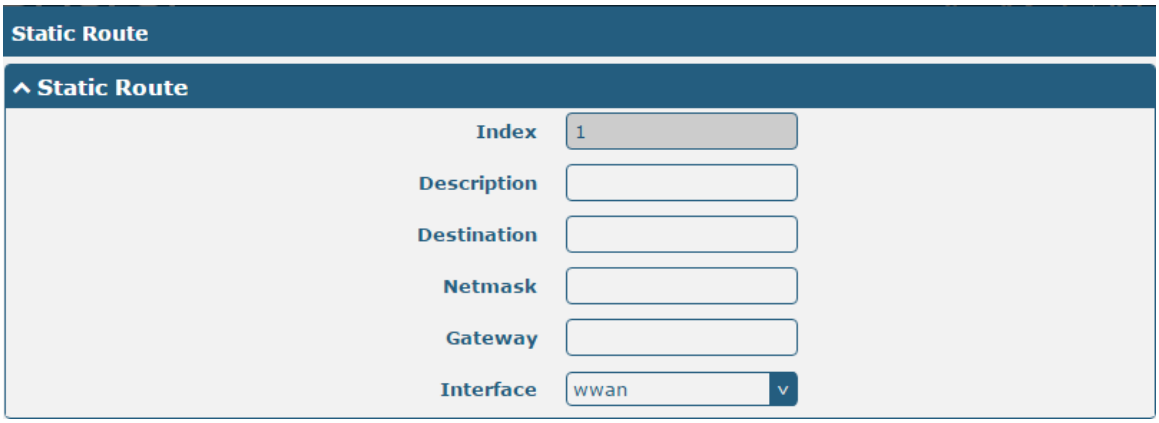
4.3.1 Route

This section allows you to set the static route. Static routes, based on the destination address, can add up to 20 static routes to the router.

Click **Network > Routing > Static Routing** to enter the static routing table, which allows users to manually add, delete or modify static routing rules.

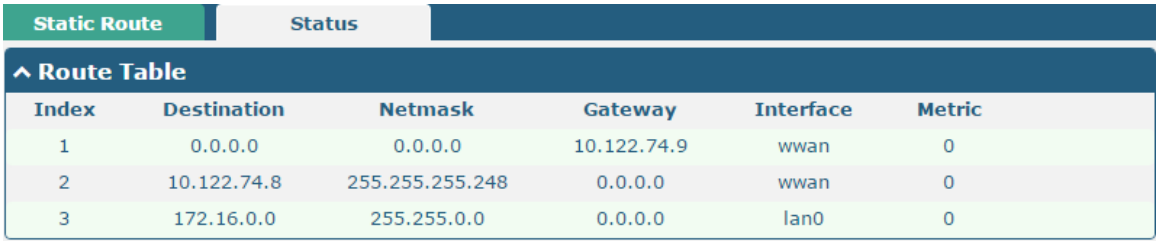


Click + to add static route. The maximum count is 20.



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

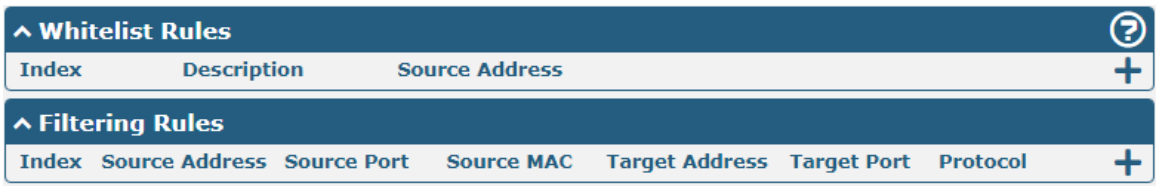
This window allows you to view the status of route.



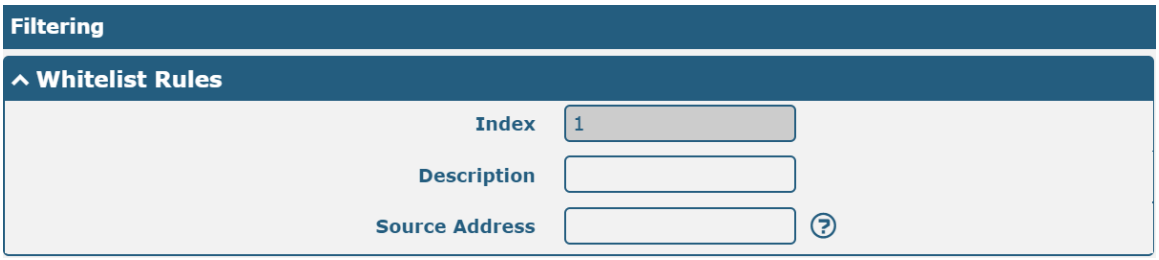
4.3.2 Firewall

This section is used to set firewall parameters, including setting access control and adding filtering rules. Filtering rules allow users to customize to accept or discard specified access sources and filter their IP addresses or MAC addresses.

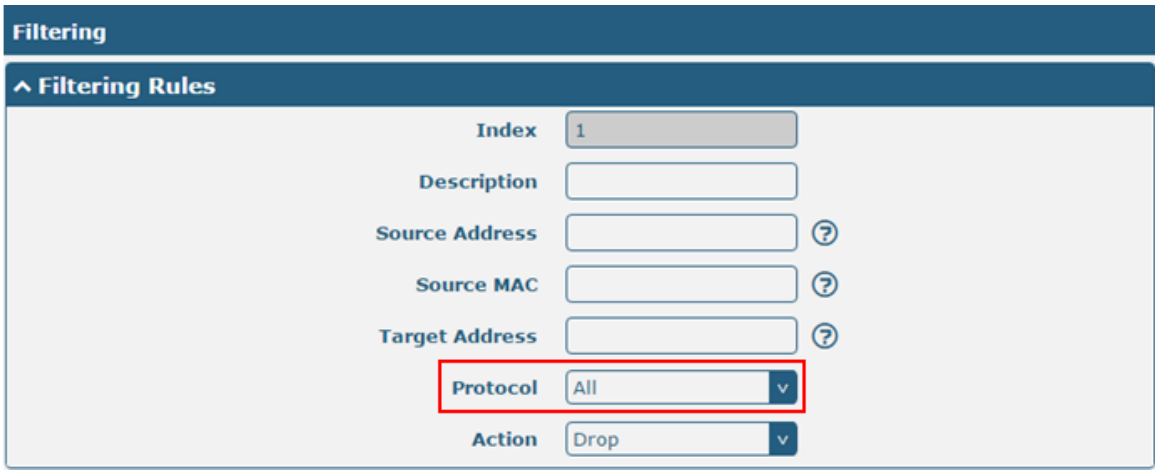
Click **Network > Firewall > Filtering** to display the following.



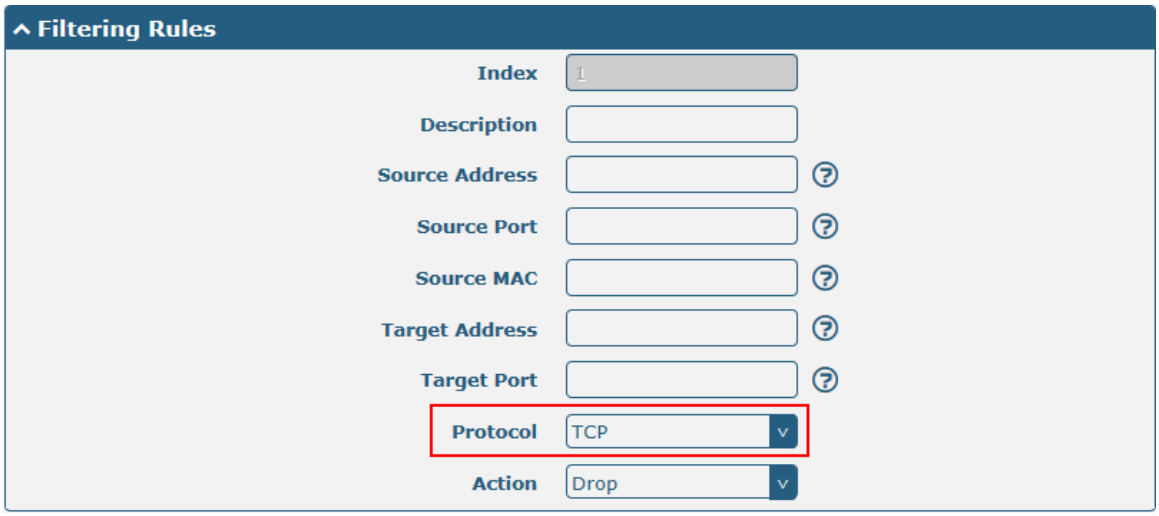
Click + to add whitelist rules. The maximum count is 50.



Click + to add filtering rules. The maximum count is 50. The window is displayed as below when defaulting "All" or choosing "ICMP" as the protocol. Here take "All" as an example.



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



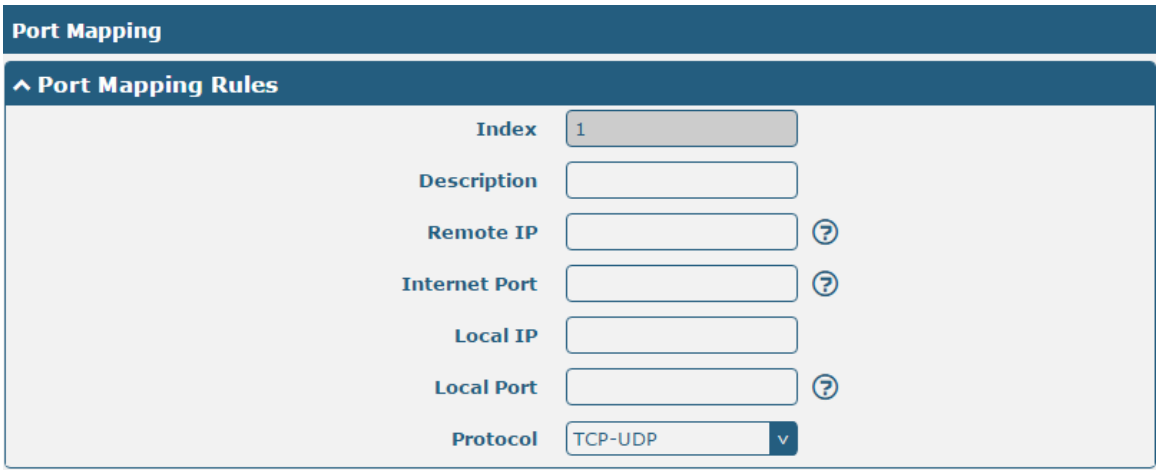
Filtering		
Item	**Description**	**Default**
General Settings		
Enable Filtering	Click the toggle button to enable/disable the filtering option.	ON
Default Filtering Policy	Select from "Accept" or "Drop". Cannot be changed when filtering rules table is not empty. • Accept: Router will accept all the connecting requests except the hosts which fit the drop filter list • Drop: Router will drop all the connecting requests except the hosts which fit the accept filter list	Accept
Access Control Settings		
Enable Remote SSH Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via SSH.	OFF

Filtering		
Item	**Description**	**Default**
Enable Local SSH Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via SSH.	ON
Enable Remote Telnet Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via Telnet.	OFF
Enable Local Telnet Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via Telnet.	ON
Enable Remote HTTP Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via HTTP.	OFF
Enable Local HTTP Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via HTTP.	ON
Enable Remote HTTPS Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via HTTPS.	ON
Enable Remote Ping Respond	Click the toggle button to enable/disable this option. When enabled, the router will reply to the Ping requests from other hosts on the Internet.	ON
Enable DOS Defending	Click the toggle button to enable/disable this option. When enabled, the router will defend the DOS. Dos attack is an attempt to make a machine or network resource unavailable to its intended users.	ON
Enable Console	Click the toggle button to enable/disable this option. When enabled, the user can access the router via Console.	ON
Enable the vpn_nat traversal	Click the toggle button to enable/disable this option. When enabled, the router automatically modifies the IP address of the VPN header received by WAN/WWAN to the IP address of the device under LAN port and sends it out.	OFF
Whitelist Rules		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this whitelist rule.	Null
Source Address	Defines if access is allowed from one or a range of IP addresses which are defined by Source IP Address, or every IP addresses.	Null
Filtering Rules		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this filtering rule.	Null
Source Address	Defines if access is allowed from one or a range of IP addresses which are defined by Source IP Address, or every IP addresses.	Null
Source Port	Specify an access originator and enter its source port.	Null
Source MAC	Enter the MAC address of the defined source IP address.	Null
Target Address	Defines if access is allowed to one or a range of IP addresses which are defined by Target IP Address, or every IP addresses.	Null
Target Port	Enter the target port which the access originator wants to access.	Null
Protocol	Select from “All”, “TCP”, “UDP”, “ICMP” or “TCP-UDP”. **Note**: It is recommended that you choose “All” if you don’t know which protocol of your application to use.	All

Filtering		
Item	**Description**	**Default**
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 routers, and all data received from certain ports of the public network is forwarded to a certain port of an IP in the intranet. Click **Network > Firewall > Port Mapping** to display as follows:

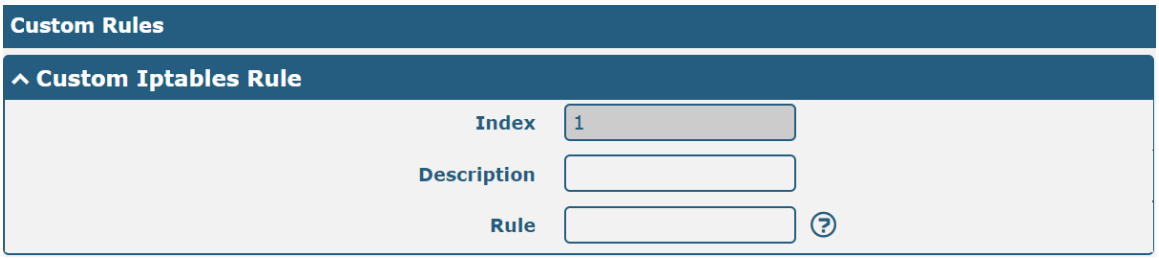
Click + to add port mapping rules. The maximum rule count is 50.



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

"Custom Rules" is user-defined rules. Click "**Network > Firewall > Custom Rules**" to display the following.

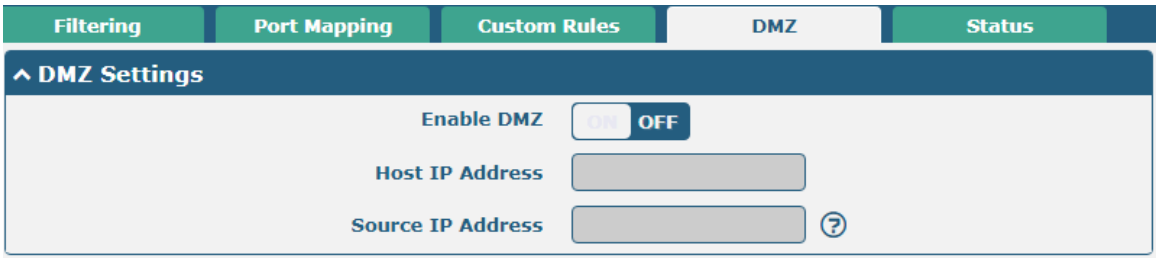
Click + to add custom rules. The maximum rule count is 50.



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

DMZ (Demilitarized Zone), namely the isolation zone, also known as the demilitarized zone. It is a buffer between a non-security system and a security system in order to solve the problem that the access users of the external network cannot access the internal network server after installing the firewall. The DMZ host is an intranet host that has open access to all ports except those occupied and forwarded.

Click "**Network > Firewall > DMZ**" to display as follows:



DMZ Settings		
Item	**Description**	**Default**
Enable DMZ	Click the toggle button to enable/disable DMZ. DMZ host is a host on the internal network that has all ports exposed, except those ports otherwise forwarded.	OFF
Host IP Address	Enter the IP address of the DMZ host on your internal network.	Null
Source IP Address	Set the address which can talk to the DMZ host. 0.0.0.0 means for any addresses.	Null

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

Filtering | Port Mapping | Custom Rules | DMZ | Status

Chain Input

Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	DROP	tcp	wwan	*	0.0.0.0/0	0.0.0.0/0
2	0	DROP	tcp	wwan	*	0.0.0.0/0	0.0.0.0/0
3	0	DROP	tcp	wwan	*	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	52	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	0	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

Chain Forward

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

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 Pass-through option.

IP Passthrough

General Settings

Enable ON OFF

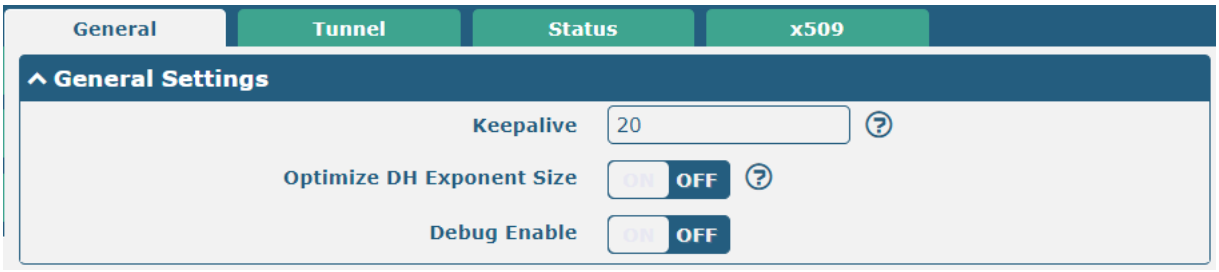
If router enables the IP Pass-through, the terminal device (such as PC) will enable the DHCP Client mode and connect to LAN port of the router; and after the router dial up successfully, the PC will automatically obtain the IP address and DNS server address which assigned by ISP. To use this feature, the primary link needs to be set to WWAN and the backup link needs to be set to None.

4.4 VPN

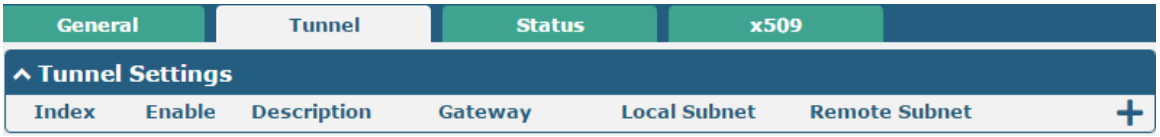
4.4.1 IPsec

IPsec (Internet Protocol Security) is a protocol built on the Internet Protocol layer that enables two hosts to communicate in a secure manner. IPsec is the direction of secure networking and provides proactive protection against attacks on private networks and the Internet through end-to-end security.

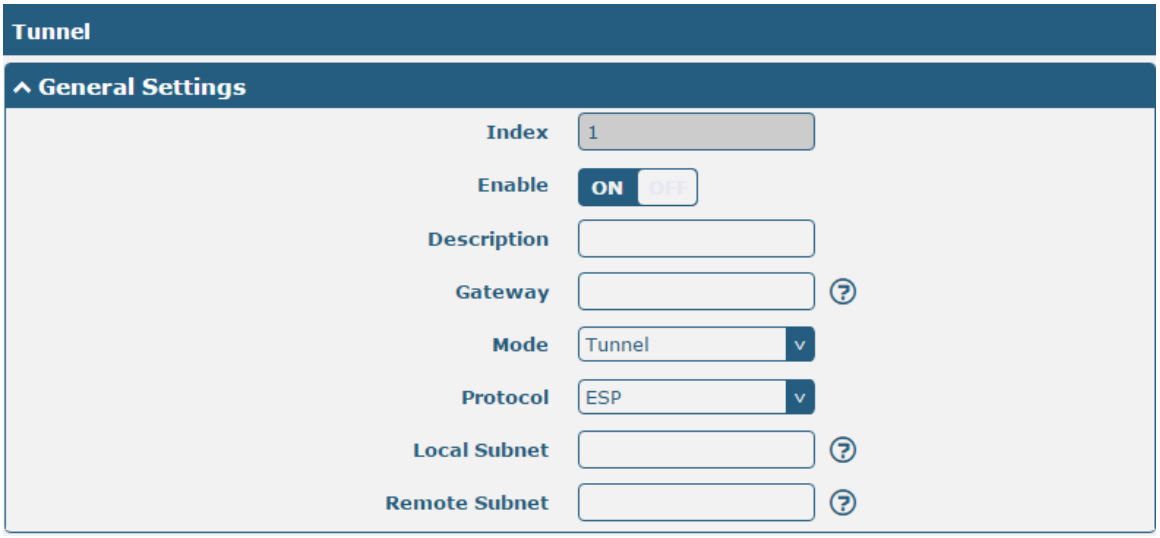
Click **Virtual Private Network > IPsec > General** to set IPsec parameters



General Settings @ General		
Item	**Description**	**Default**
Keepalive	Set the keepalive time, measured in seconds. The router will send packets to NAT server every keepalive time to avoid record remove from the NAT list.	20
Optimize DH Exponent Size	Click the toggle button to enable/disable this option. When enabled, it reduces the time to generate the key	OFF
Debug Enable	Click the toggle button to enable/disable this option. Enable for IPsec VPN information output to the debug port.	OFF



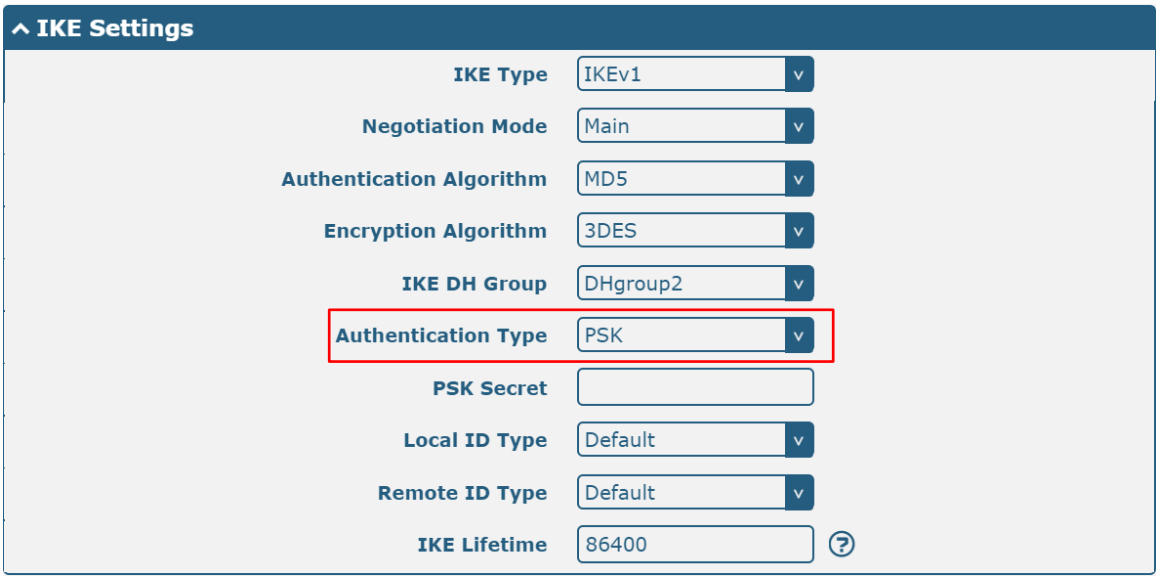
Click + to add tunnel settings. The maximum count is 6.



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 of remote side IPsec VPN server. 0.0.0.0 represents for any address.	Null

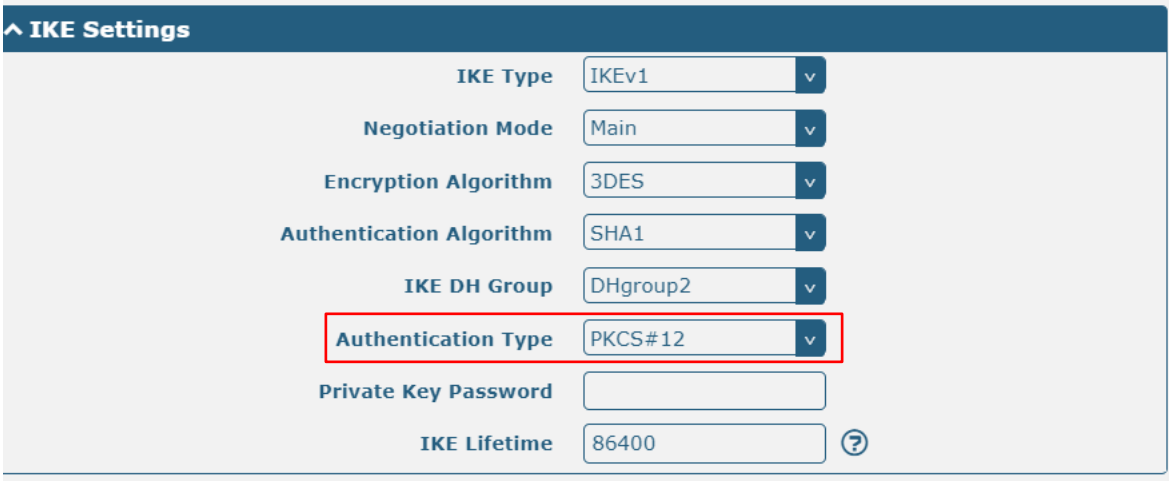
Mode	Select from “Tunnel” and “Transport”. • Tunnel: Commonly used between routers, or at an end-station to a router, the router acting as a proxy for the hosts behind it • Transport: Used between end-stations or between an end-station and a router, if the router is being treated as a host-for example, 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 the link to build IPsec.	Unbound

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



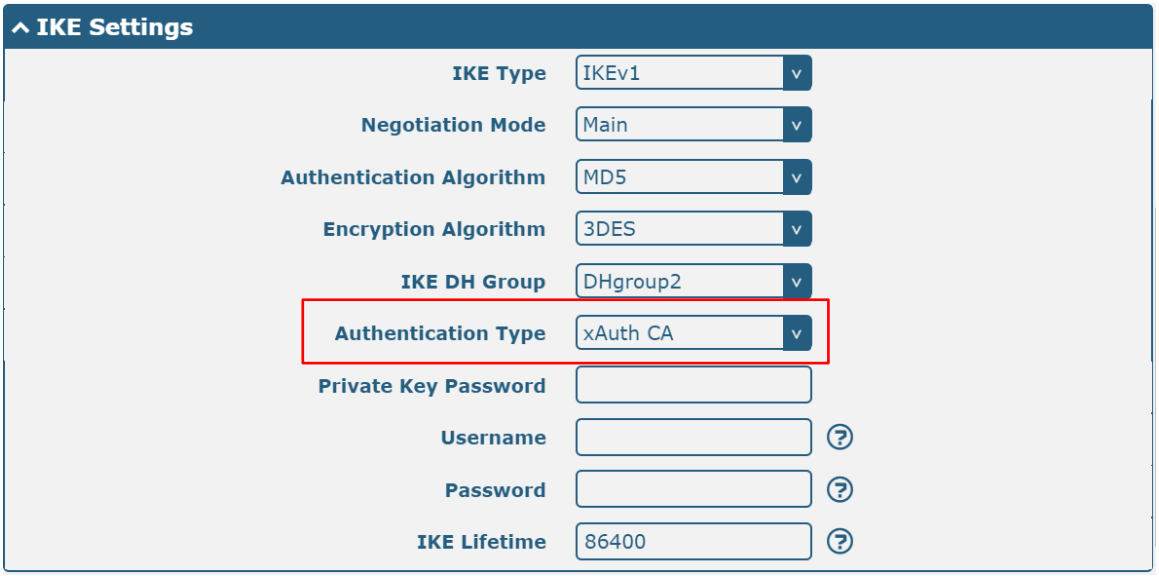
The window is displayed as below when choosing “CA” as the authentication type.

The window is displayed as below when choosing “PCKS#12” as the authentication type.



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

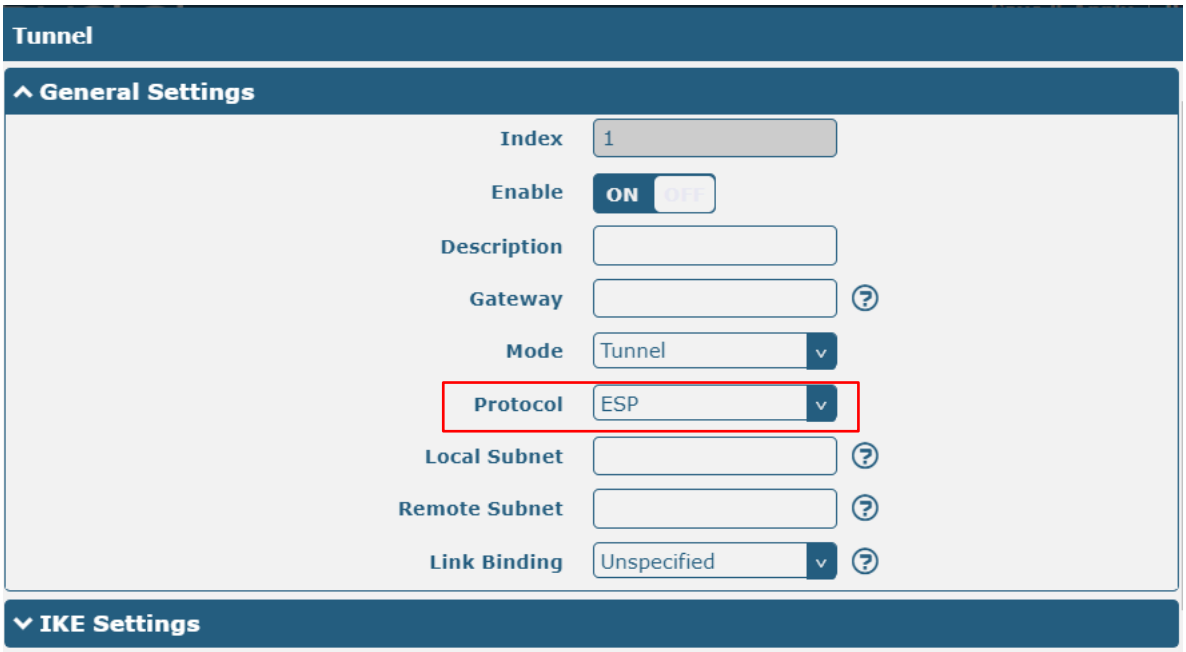
The window is displayed as below when choosing “xAuth CA” as the authentication type.

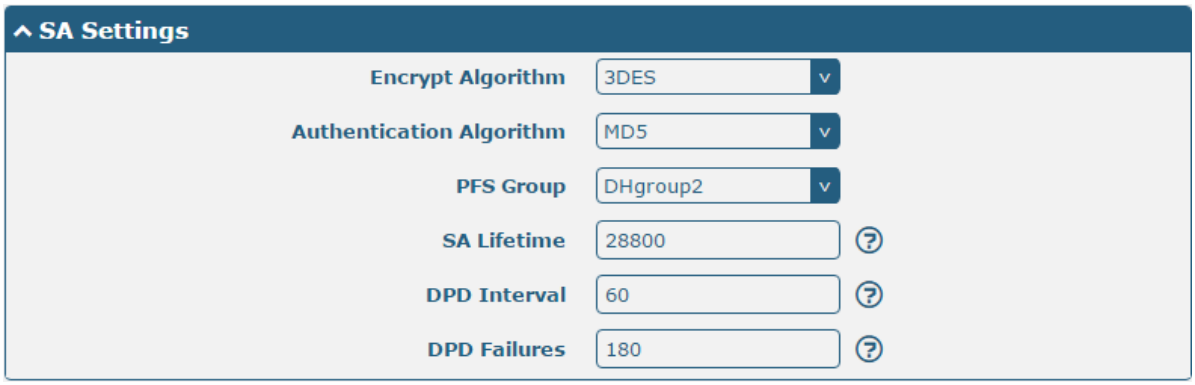


IKE Settings		
Item	**Description**	**Default**
IKE Type	Select from “IKEv1” and “IKEv2”.	IKEv1
Negotiation Mode	Select from “Main” and “Aggressive” for the IKE negotiation mode in phase 1. If the IP address of one end of an IPsec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. 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.	MD5
Encrypt Algorithm	Select from “3DES”, “AES128”, “AES192”and “AES256”to be used in IKE negotiation. • 3DES: Use 168-bit 3DES encryption algorithm in CBC mode • AES128: Use 128-bit AES encryption algorithm in CBC mode • AES128: Use 192-bit AES encryption algorithm in CBC mode • AES256: Use 256-bit AES encryption algorithm in CBC mode	3DES
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”, “xAuth PSK” and “xAuth CA” to be used in IKE negotiation. • PSK: Pre-shared Key • CA: Certification 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: Uses an IP address as the ID in IKE negotiation • FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security router, e.g., test.robustel.com	Default

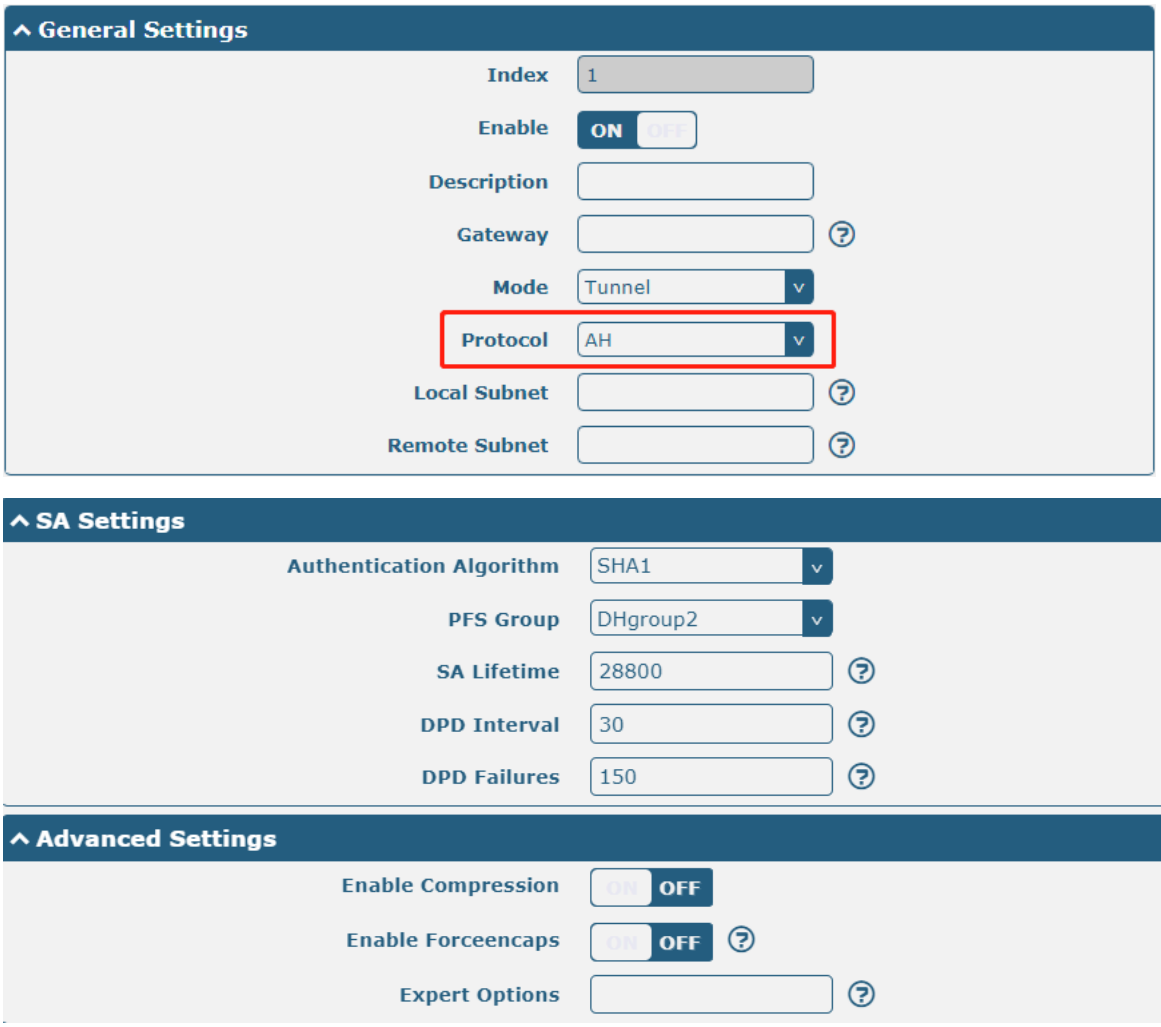
IKE Settings		
Item	**Description**	**Default**
	• User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security router, e.g., test@robustel.com	
Remote ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. • Default: Uses an IP address as the ID in IKE negotiation • FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security router, e.g., test.robustel.com • User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security router, e.g., test@robustel.com	Default
IKE Lifetime	Set the lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as the new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.	86400
Private Key Password	Enter the private key under the "CA" and "xAuth CA" authentication types.	Null
Username	Enter the username used for the "xAuth PSK" and "xAuth CA" authentication types.	Null
Password	Enter the password used for the "xAuth PSK" and "xAuth CA" authentication types.	Null

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





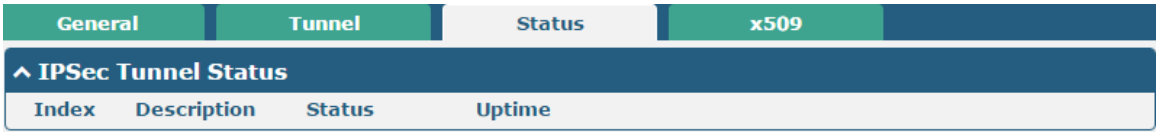
If choose AH as protocol, the window of SA Settings is displayed as below.



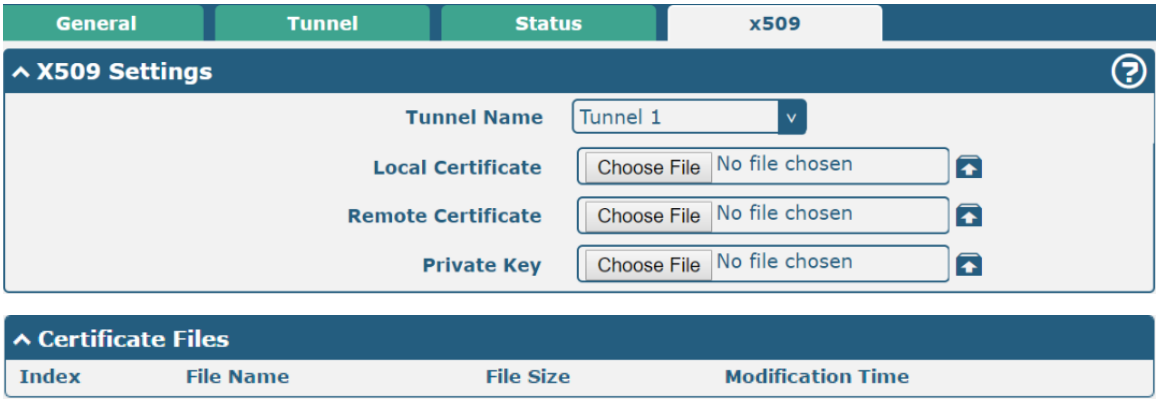
SA Settings		
Item	**Description**	**Default**
Encrypt Algorithm	Select from “3DES”, “AES128”, “AES192”or “AES256” when you select “ESP” in “Protocol”. Higher security means more complex implementation and lower speed. DES is enough to meet general requirements. Use 3DES when high confidentiality and security are required.	3DES
Authentication Algorithm	Select from “MD5”, “SHA1”, “SHA2 256” or “SHA2 512” to be used in SA negotiation.	MD5

SA Settings		
Item	**Description**	**Default**
PFS Group	Select from “PFS (N/A)”, “DHgroup1”, “DHgroup2”, “DHgroup5”, “DHgroup14”, “DHgroup15”, “DHgroup16”, “DHgroup17” or “DHgroup18” to be used in SA negotiation.	DHgroup2
SA Lifetime	Set the IPsec SA lifetime. When negotiating to set up IPsec SAs, IKE uses the smaller one between the lifetime set locally and the lifetime proposed by the peer.	28800
DPD Interval	Set the interval after which DPD is triggered if no IPsec protected packets is received from the peer. DPD is a Dead peer detection. DPD irregularly detects dead IKE peers. When the local end sends an IPsec packet, DPD checks the time the last IPsec packet was received from the peer. If the time exceeds the DPD interval, it sends a DPD hello to the peer. If the local end receives no DPD acknowledgment within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgment after having made the maximum number of retransmission attempts, it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.	30
DPD Failures	Set the timeout of DPD (Dead Peer Detection) packets.	150
Advanced Settings		
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the inner headers of IP packets.	OFF
Enable Forceencaps	Click the toggle button to enable/disable this option. When enabled, UDP encapsulation of esp packets is forced even if NAT conditions are not detected. This helps 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.



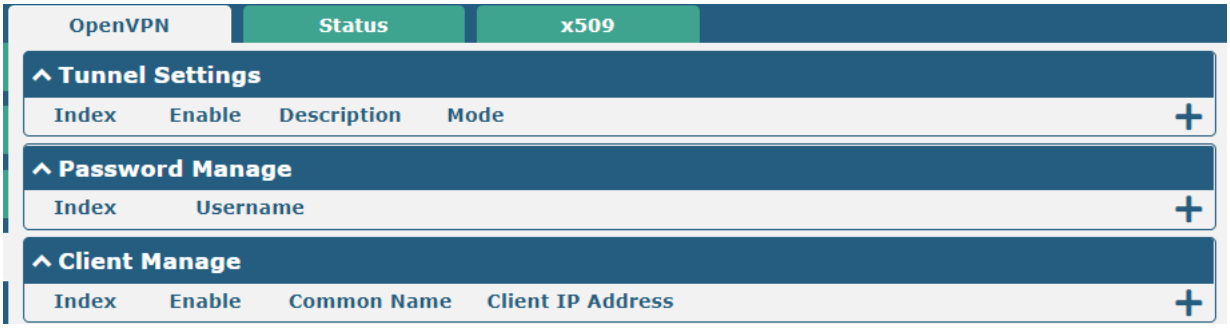
User can upload the X509 certificates for the IPsec tunnel in this section.



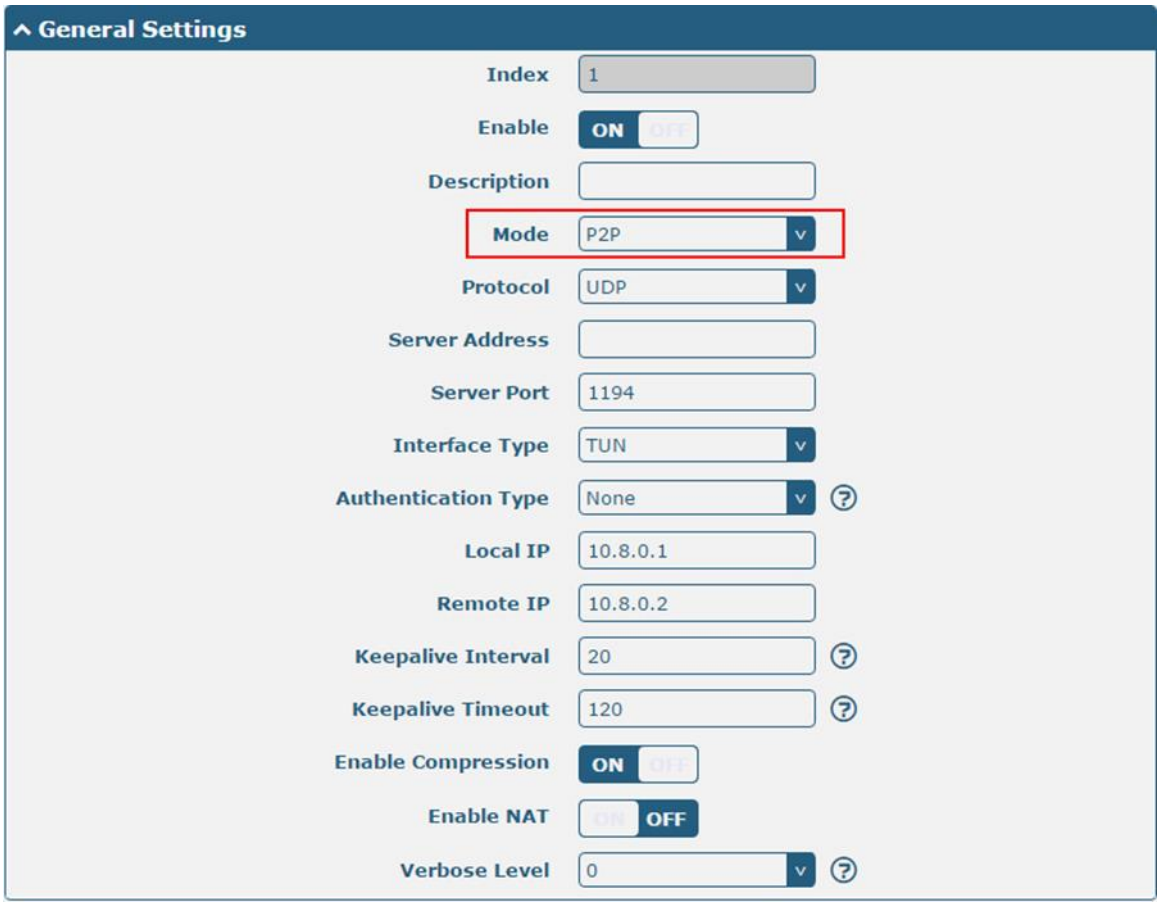
x509		
Item	**Description**	**Default**
X509 Settings		
Tunnel Name	Choose a valid tunnel from “tunnel 1”, “tunnel 2”, “tunnel 3”, “tunnel 4”, “tunnel 5” and “tunnel 6”.	Tunnel 1
Local Certificate	Click on “Choose File” to locate the certificate file from local computer, and then import this file into your router.	--
Remote Certificate	Click on “Choose File” to locate the certificate file from remote computer, and then import this file into your router.	--
Private Key	Click on “Choose File” to locate the private key file from local computer, and then import this file into your router.	--
CA certificate	Click on “Choose File” to locate the private key file from local computer, and then import CA certificate into your router.	--
PKCS#12 Certificate	Click on “Choose File” to locate the private key file from local computer, and then import PKCS#12 certificate into your router.	--
Certificate Files		
Index	Indicate the ordinal of the list.	--
Filename	Show the imported certificate’s name.	Null
File Size	Show the size of the certificate file.	Null
Modification Time	Show the timestamp of that the last time to modify the certificate file.	Null

4.4.2 OpenVPN

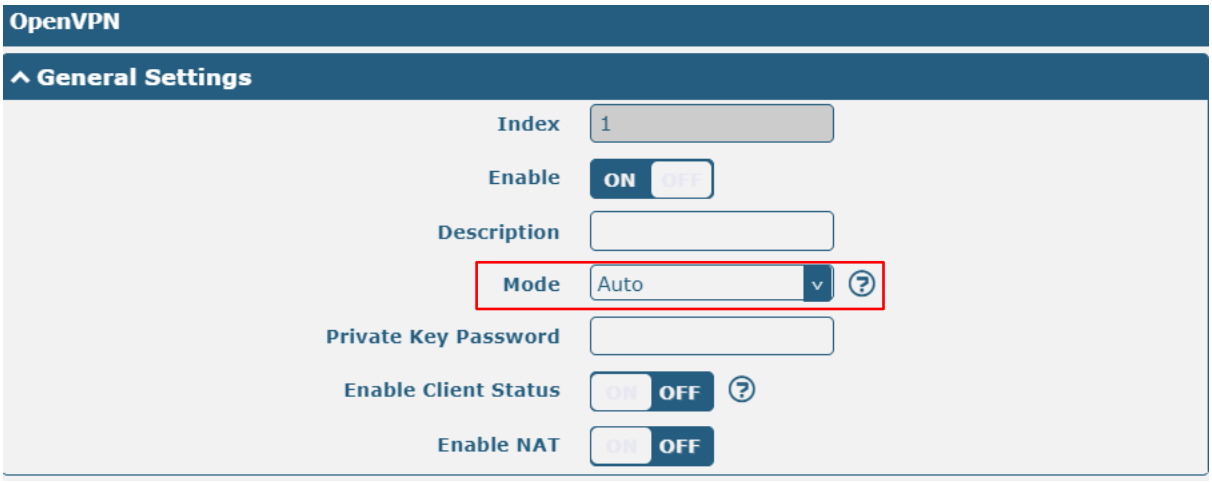
This section allows you to set the OpenVPN and the related parameters. OpenVPN, an open source SSL-based VPN system. The OpenVPN feature can support both point-to-point and point-to-multipoint (client-side) VPN channels. Click "**VPN > OpenVPN > OpenVPN**" to display the following.



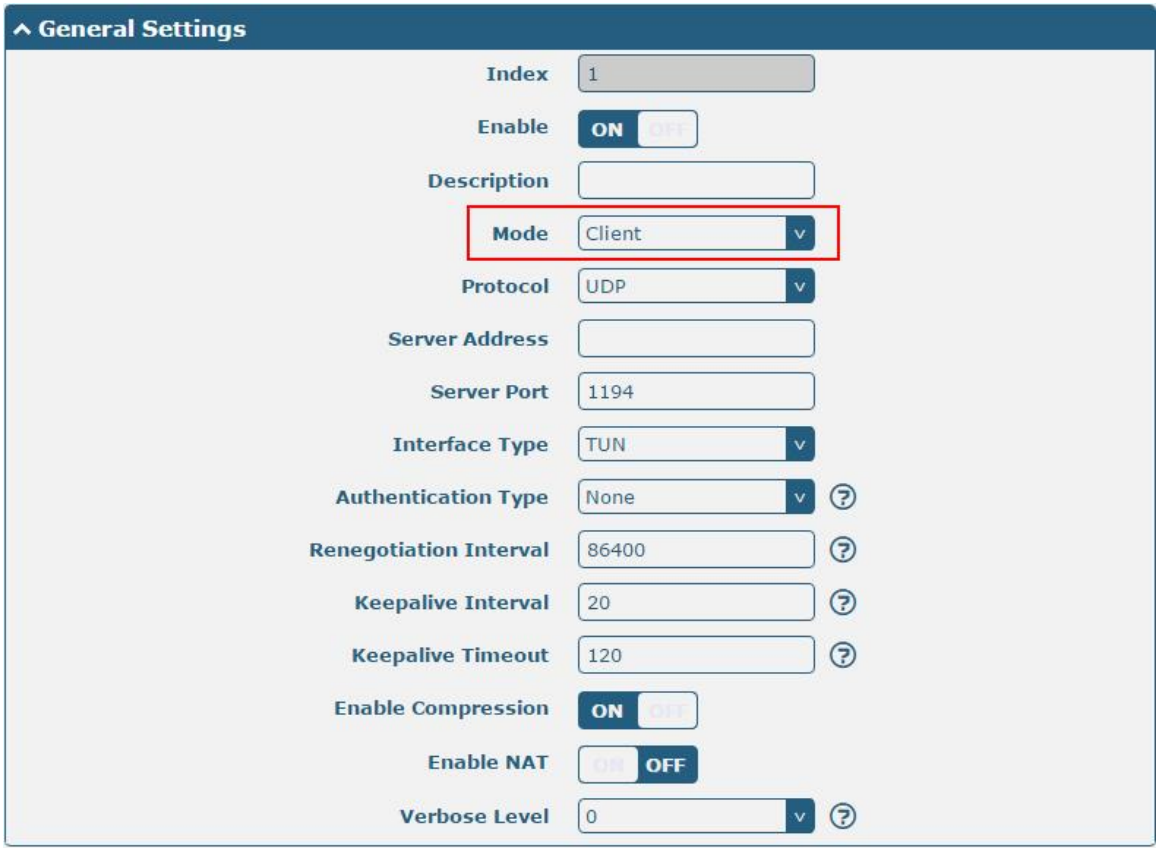
Click to add tunnel settings. The maximum count is 5. The window is displayed as below when choosing “P2P” as the mode.



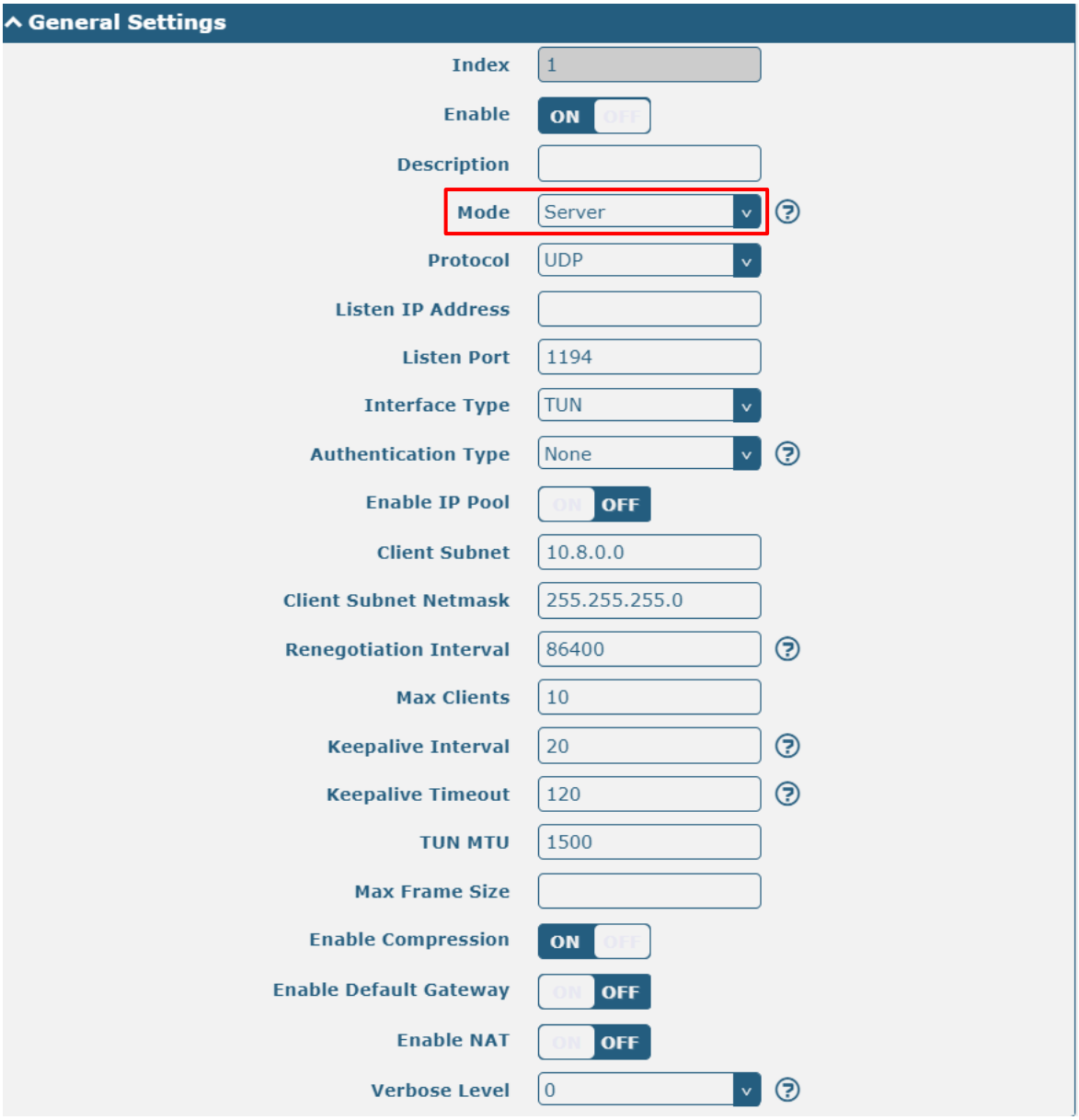
The window is displayed as below when choosing “Auto” as the mode.



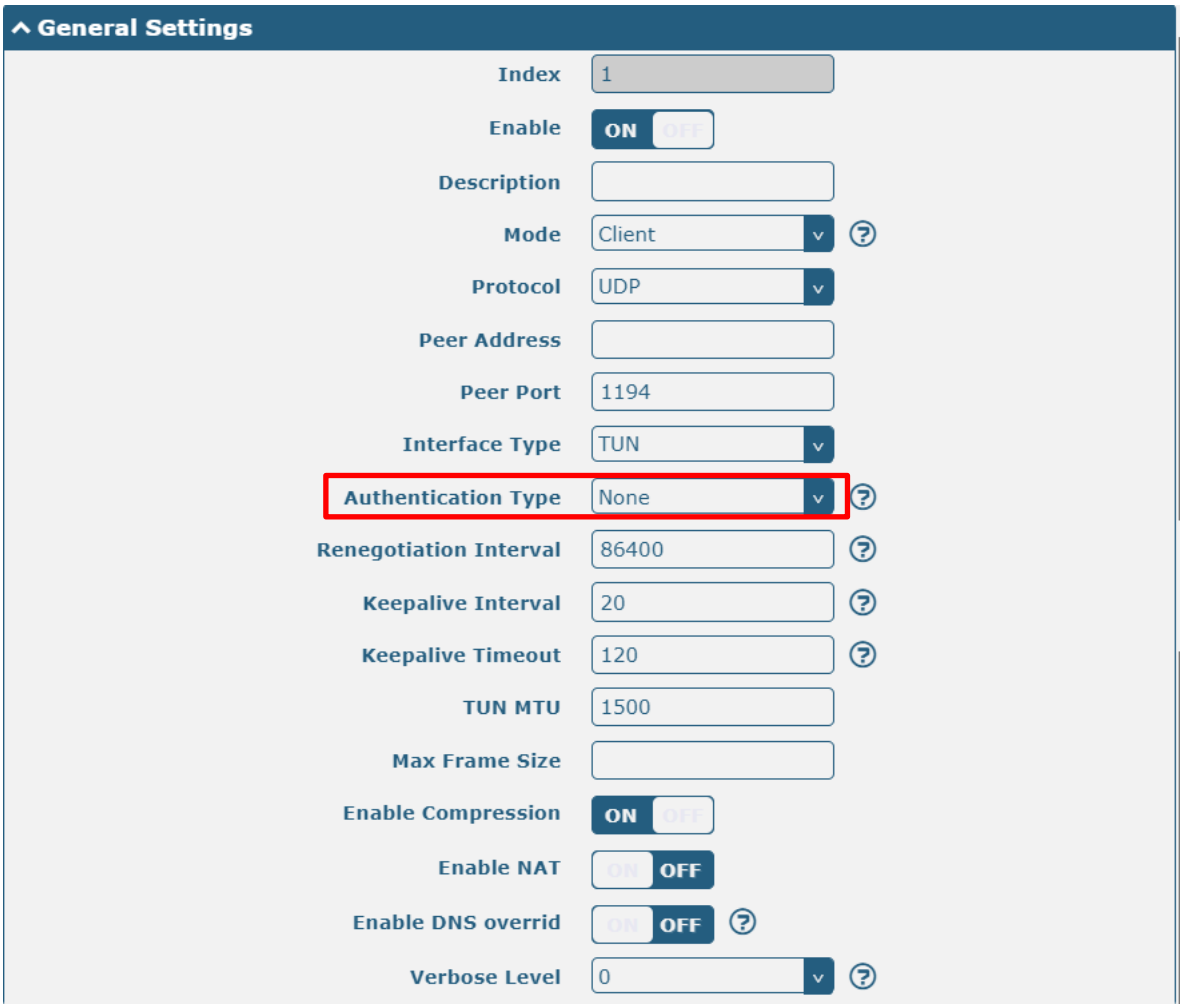
The window is displayed as below when choosing “Client” as the mode.



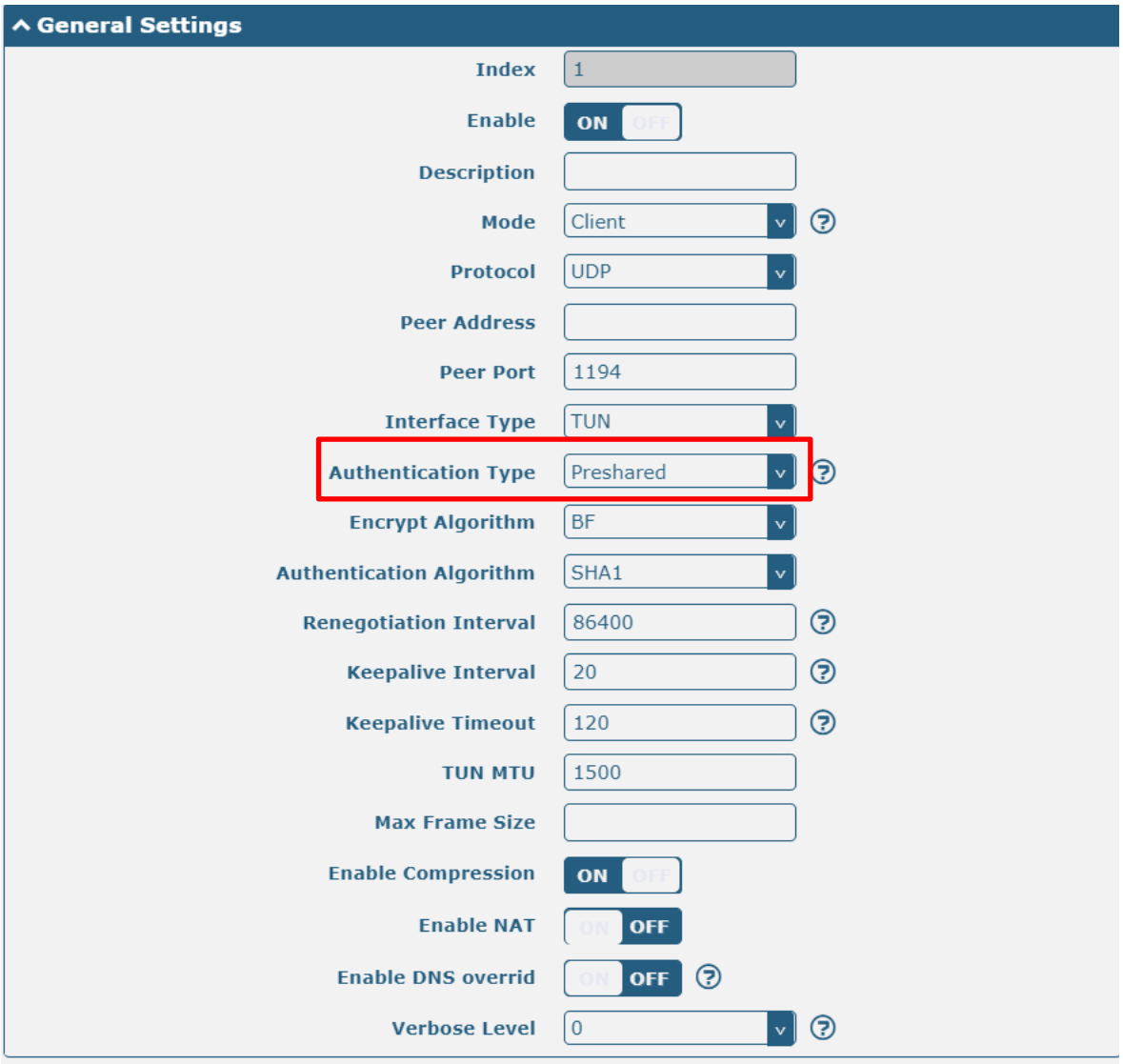
The window is displayed as below when choosing “Server” as the mode.



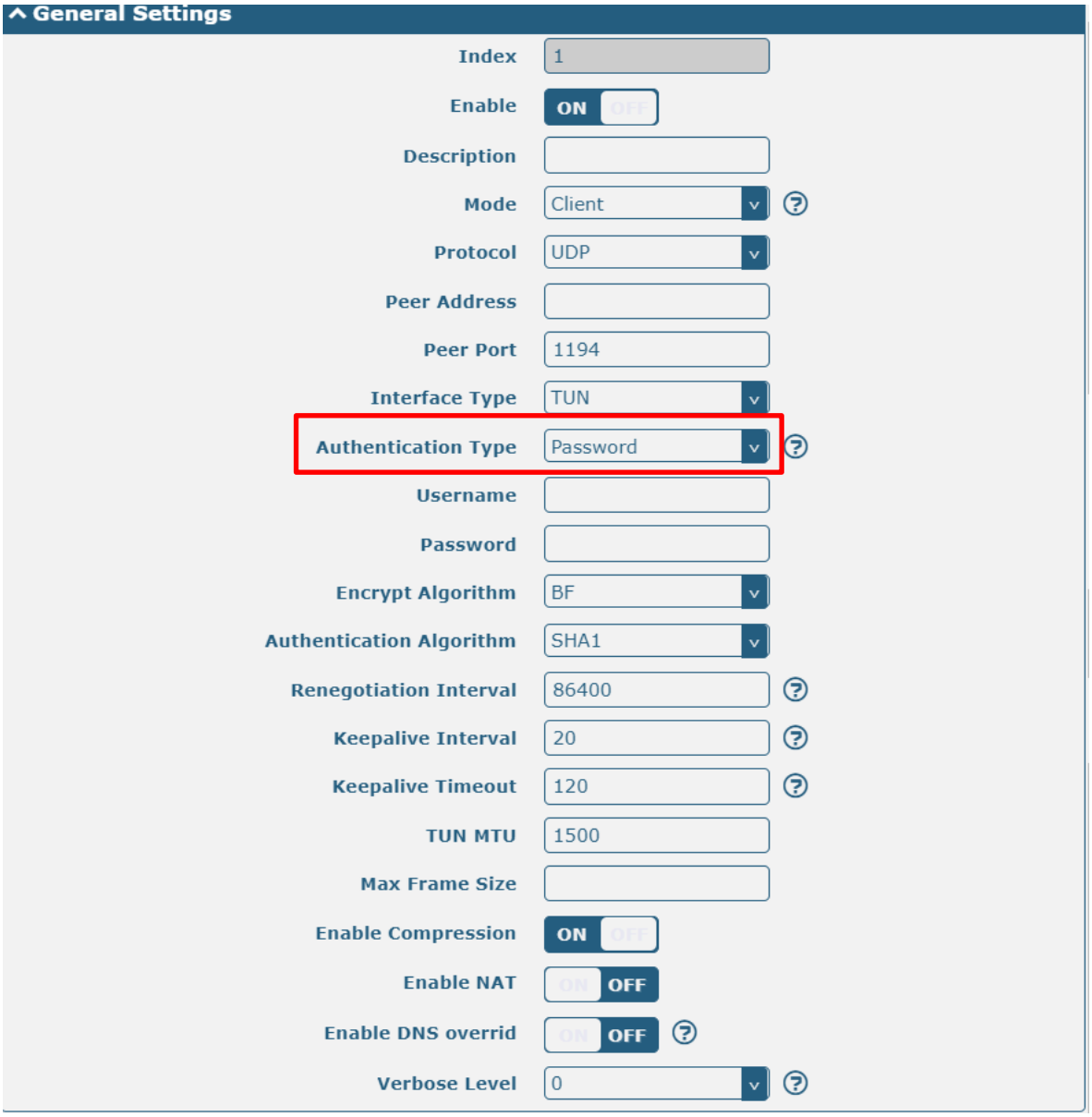
The window displays as follows when "None" is selected as the authentication type.



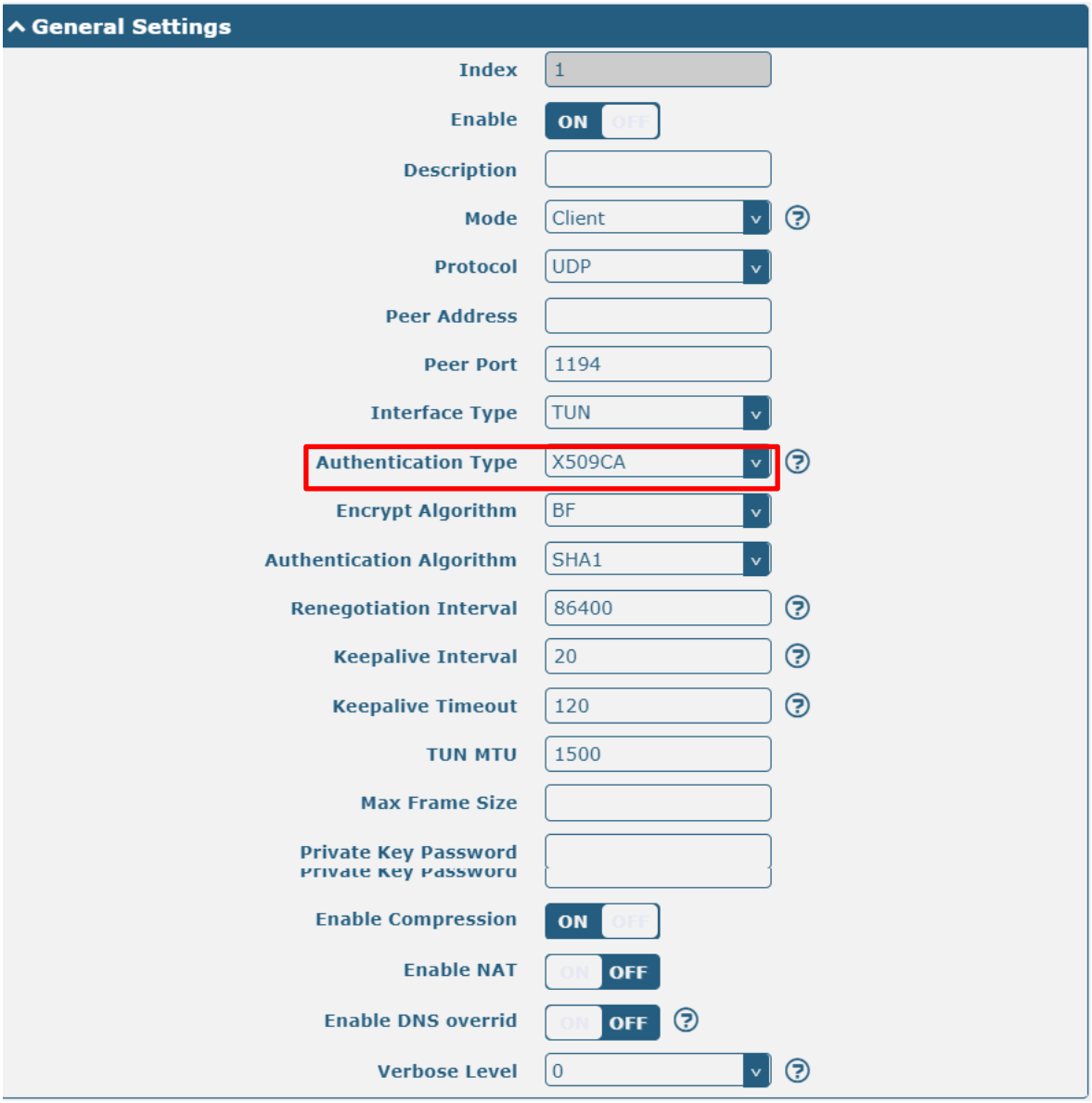
The window displays as follows when "Preshared" is selected as the authentication type.



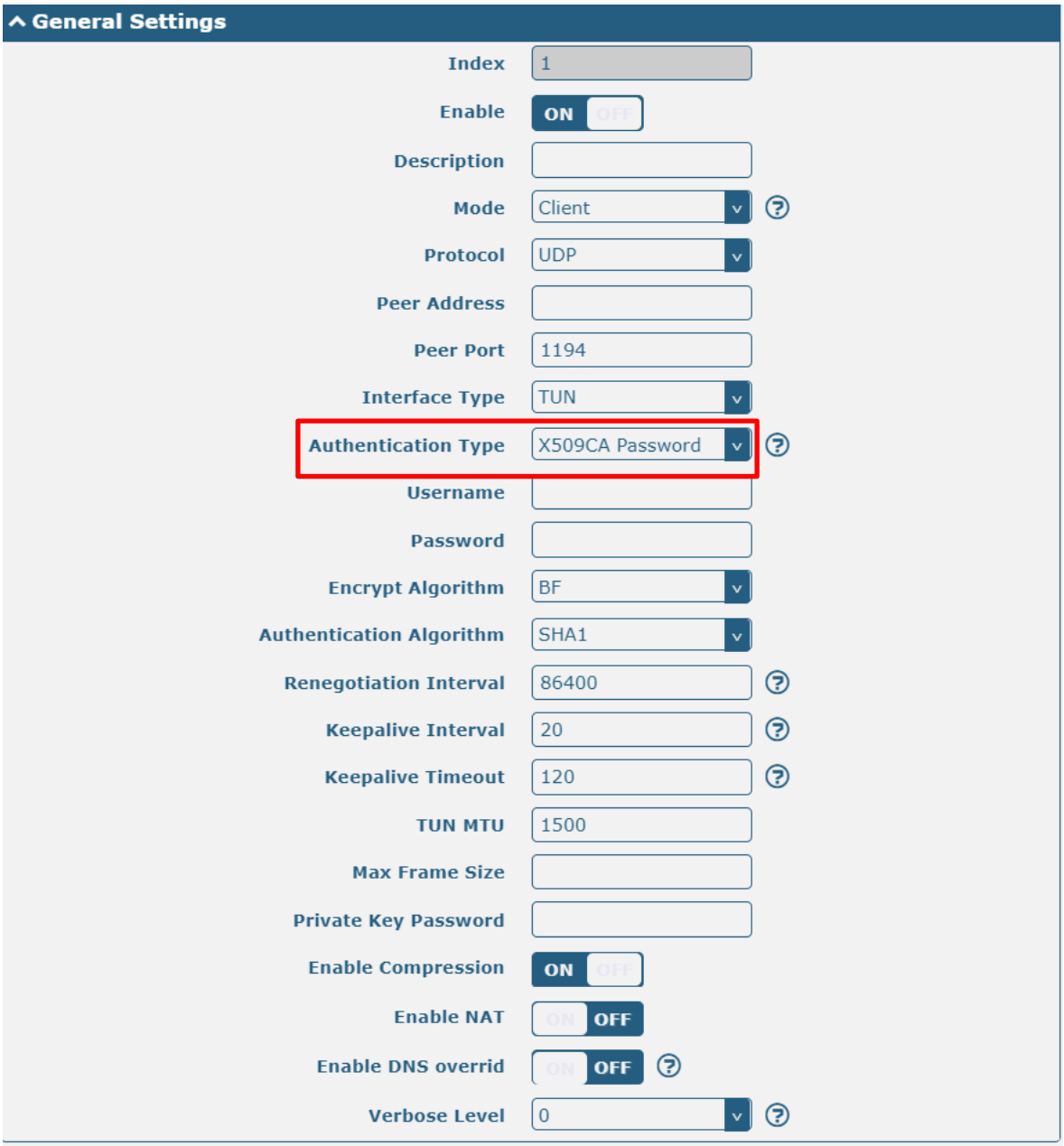
The window displays as follows when "Password" is selected as the authentication type.



The window displays as follows when "X509CA" is selected as the authentication type.



The window displays as follows when "X509CA Pssword" is selected as the authentication type.



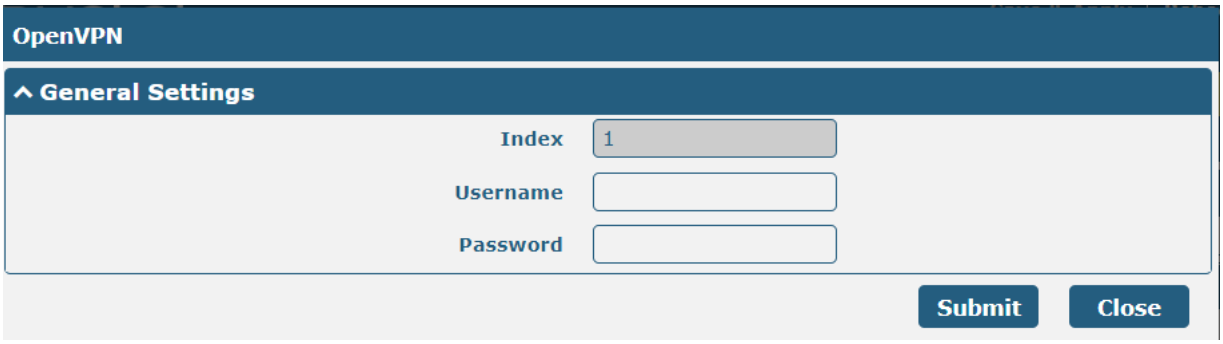
General Settings @ OpenVPN		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this OpenVPN tunnel.	ON
Description	Enter a description for this OpenVPN tunnel.	Null
Mode	Select from “P2P” or “Client”.	Client
Protocol	Select from “UDP”, “TCP-Client” or “TCP-Server”.	UDP
Server Address	Enter the end-to-end IP address or the domain of the remote OpenVPN server.	Null
Server Port	Enter the end-to-end listener port or the listener port of the OpenVPN server.	1194
Listen IP Address	Enter the IP address or domain name of this end.	Null

General Settings @ OpenVPN		
Item	**Description**	**Default**
Listen Port	Enter the listening port of this end.	1194
Interface Type	Select from “TUN”, “TAP” which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.	TUN
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
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 Pool	Click the toggle button to enable/disable this option. When enabled, the client will get the virtual IP from the address pool.	OFF
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
Client Subnet	The client virtual IP network address.	10.8.0.0
Client Subnet Netmask	The client virtual IP network address mask.	255.255.255.0
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
Authentication Algorithm	Choose from "MD5", "SHA1", "SHA256" and "SHA512".	SHA1
Max Clients	Set the maximum number of client connections in server mode.	10
Renegotiation Interval	Set the renegotiation interval. If connection failed, OpenVPN will renegotiate when the renegotiation interval reached.	86400
Keepalive Interval	Set keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Set the keepalive timeout. Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120
TUN MTU	Set the MTU of tunnel.	1500
Max Frame Size	Set the slice size of the data to be transferred in the tunnel.	Null
Private Key Password	Enter the private key password under the “X509CA” and “X509CA Password” authentication type.	Null
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the data stream of the header.	ON

General Settings @ OpenVPN		
Item	**Description**	**Default**
Enable DNS overrid	Click the toggle button to enable/disable this option. When enabled, the DNS pushed by the server will be received as the local DNS server.	OFF
Enable Default Gateway	Click the toggle button to enable/disable this option. When enabled, the gateway pushed by the server will be received as the local gateway.	ON
Enable Client Status	Click the toggle button to enable/disable this option. Used to display information about the status of connected clients when the server is enabled.	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

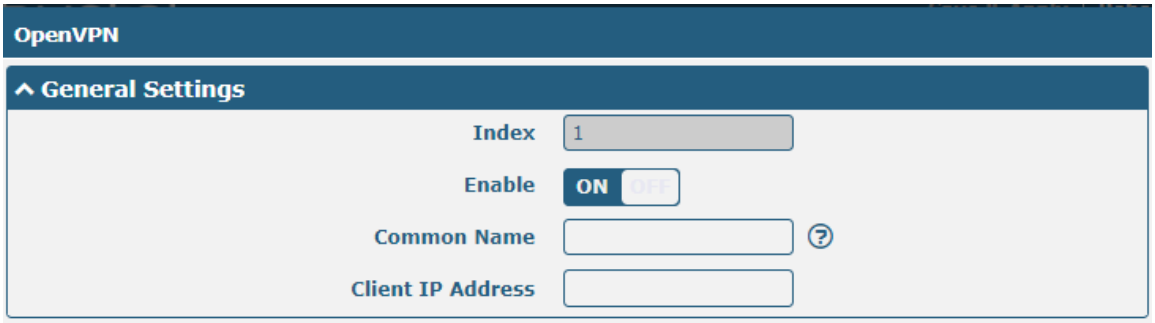
Advanced Settings @ OpenVPN		
Item	**Description**	**Default**
Enable HMAC Firewall	Click the toggle button to enable/disable this option. Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.	OFF
Enable PKCS#12	Click the toggle button to enable/disable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

Click Password Manage + to add user names and passwords, up to 20. The following is displayed.



Password Manage		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Username	In server mode, configure the username of the client.	Null
Password	In server mode, configure the password corresponding to the user name of the client.	Null

Click Password Manage + to add user names and passwords, up to 20. The following is displayed.



OpenVPN		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this option.	ON
Common Name	Specify the client's common name.	Null
Client IP address	Specifies the client's virtual IP address.	Null

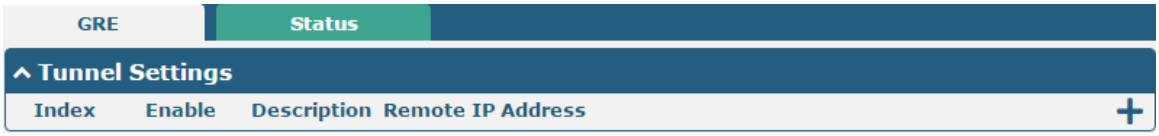
This section allows you to view the status of the OpenVPN tunnel.

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

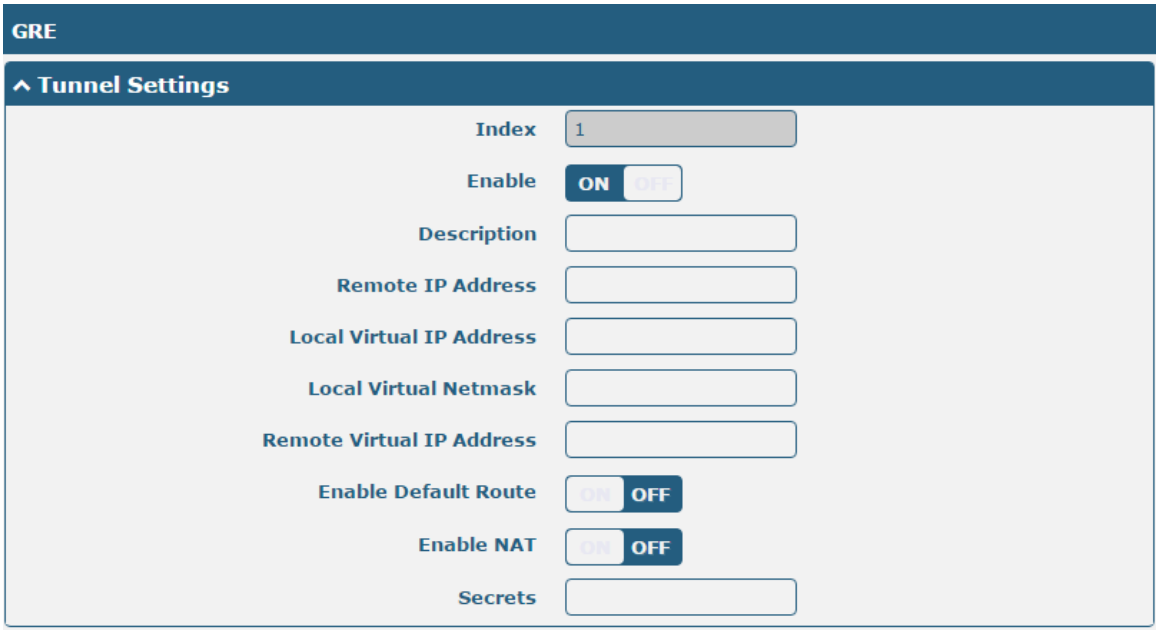
x509		
Item	**Description**	**Default**
X509 Settings		
Tunnel Name	Choose a valid tunnel.	Tunnel 1
Mode	Set for the selected tunnel.	Client
Root CA	Click on “Choose File” to locate the root ca file, and then import this file into your router.	Null
Certificate File	Click on “Choose File” to locate the certificate file, and then import this file into your router.	
Private Key	Click on “Choose File” to locate the private key file, and then import this file into your router.	
TLS-Auth Key	Click on “Choose File” to locate the tls-auth key file, and then import this file into your router.	
PKCS#12 Certificate	Click on “Choose File” to locate the pkcs#12 certificate file, and then import this file into your router.	
Certificate Files		
Index	Indicate the ordinal of the list.	--
File Name	Show the imported certificate’s name.	Null
File Size	Show the size of the certificate file.	Null
Modification Time	Show the timestamp of that the last time to modify the certificate file.	Null

4.4.3 GRE

This section allows you to set the GRE and the related parameters. GRE (Generic Routing Encapsulation) specifies how one network protocol can be used to encapsulate another. There are two main uses of the GRE protocol: intra-enterprise protocol encapsulation and private address encapsulation.

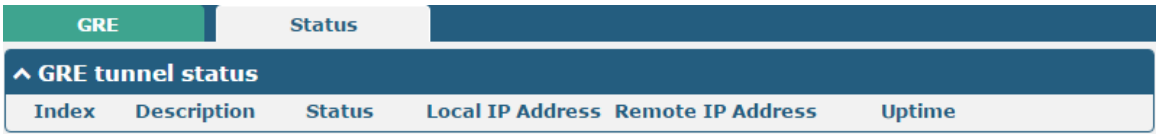


Click + to add tunnel settings. The maximum count is 5.



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.	Disable
Secrets	Set the key of the GRE tunnel.	Null

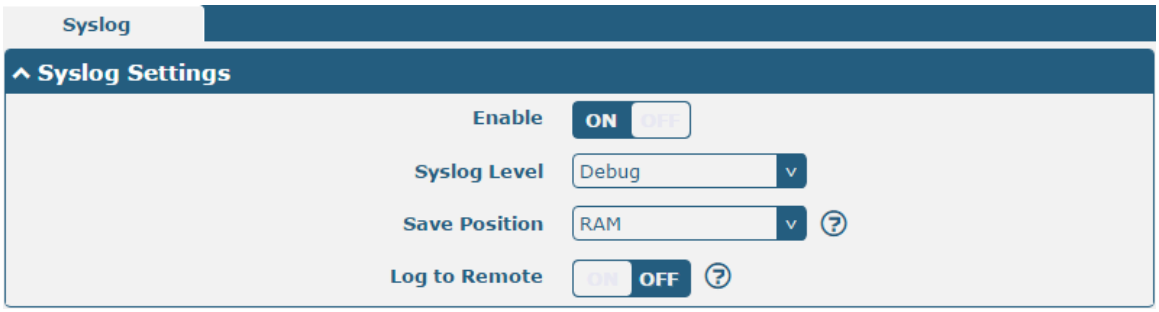
This section allows you to view the status of GRE tunnel.



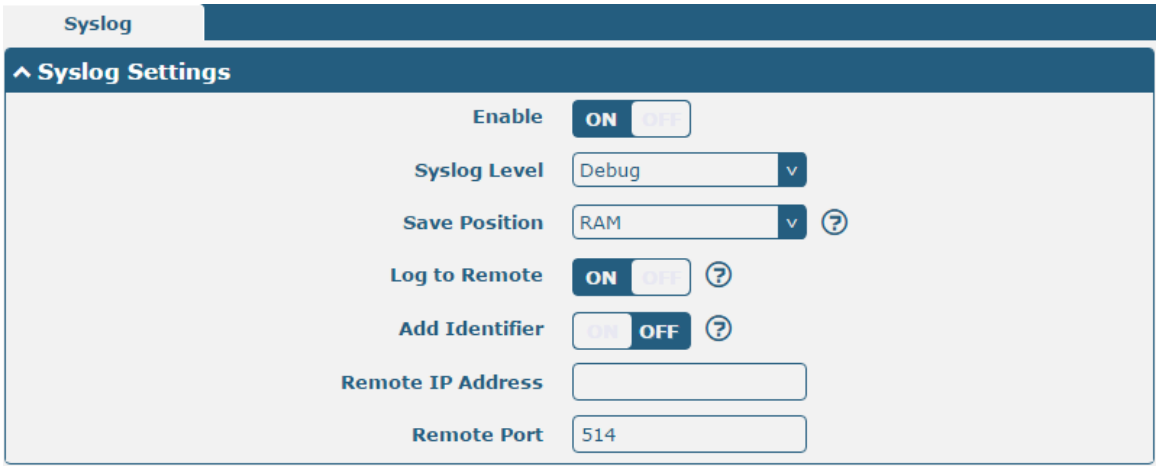
4.5 Services

4.5.1 Syslog

This section allows you to set the syslog parameters. And its "Log to Remote" is disabled by default. The system log can be saved locally, and sending the system log to the remote log server is supported, as well as the debugging of specified applications.



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



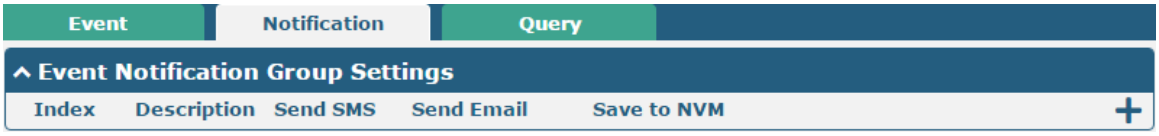
Syslog Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Syslog settings option.	OFF
Syslog Level	Select from “Debug”, “Info”, “Notice”, “Warning” or “Error”, which from low to high. The lower level will output more syslog in detail.	Debug
Save Position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

Remote IP Address	Enter the IP address of syslog server when enabling the “Log to Remote” option.	Null
Remote Port	Enter the port of syslog server when enabling the “Log to Remote” option.	514

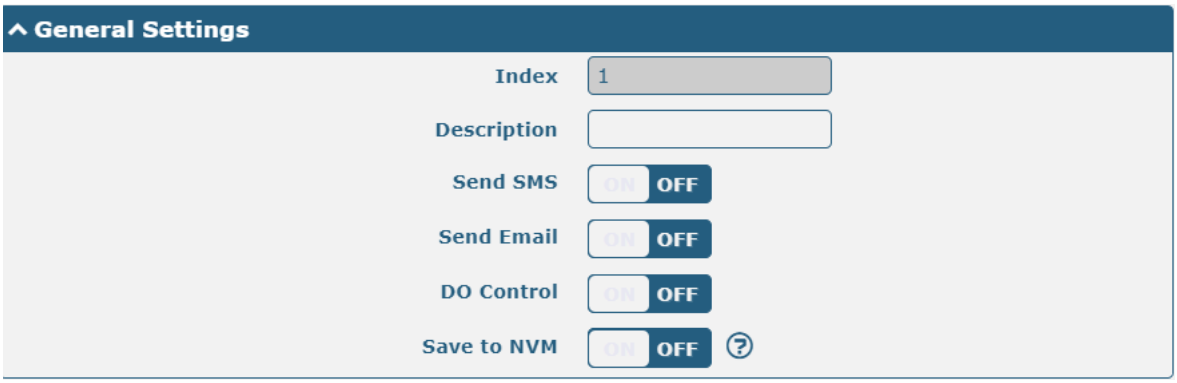
4.5.2 Event

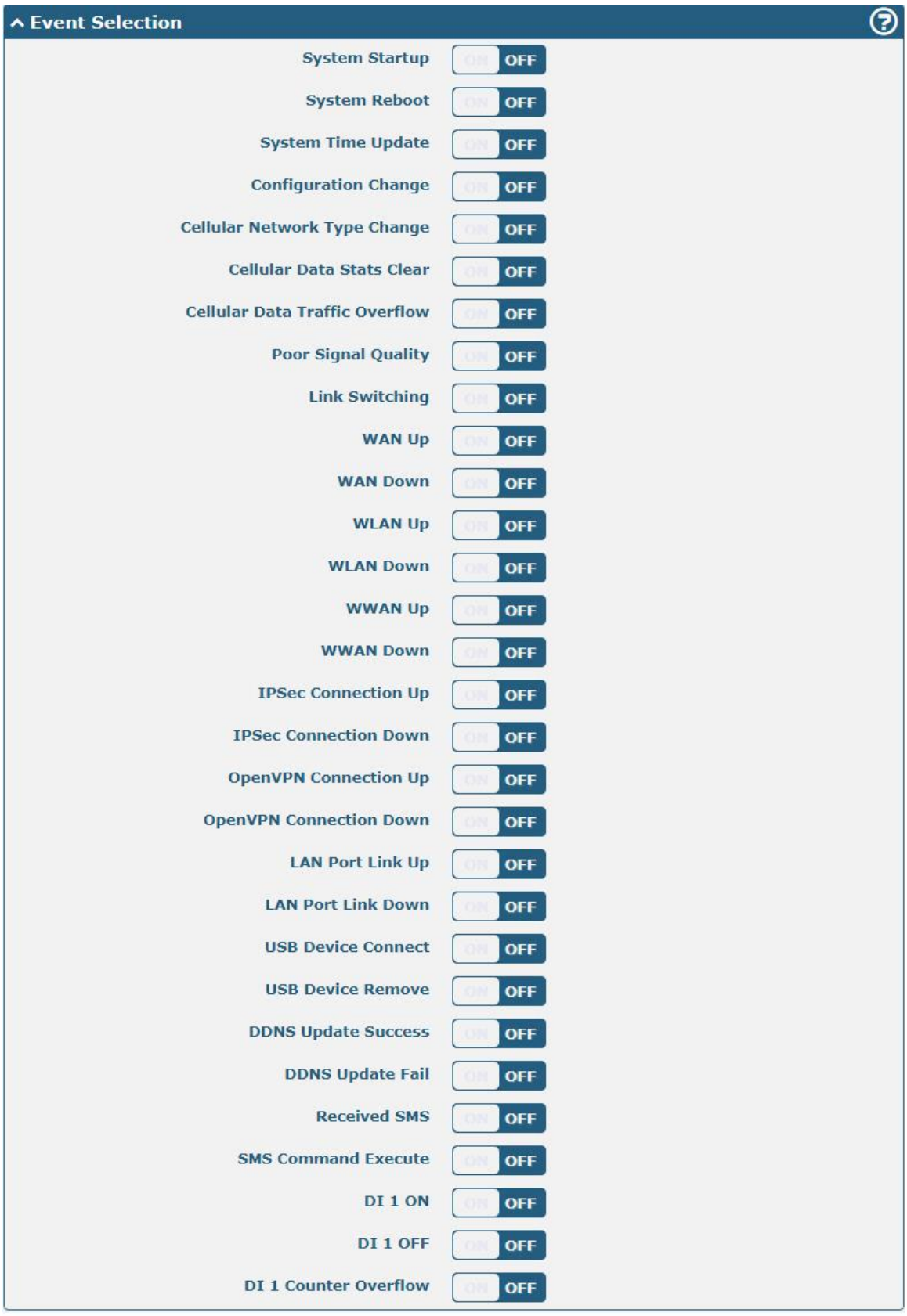
This section allows you to set the router events. It can be configured to send event alerts via SMS or report router event occurrences via SNMP-TRAP and RCMS.

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 event parameters.

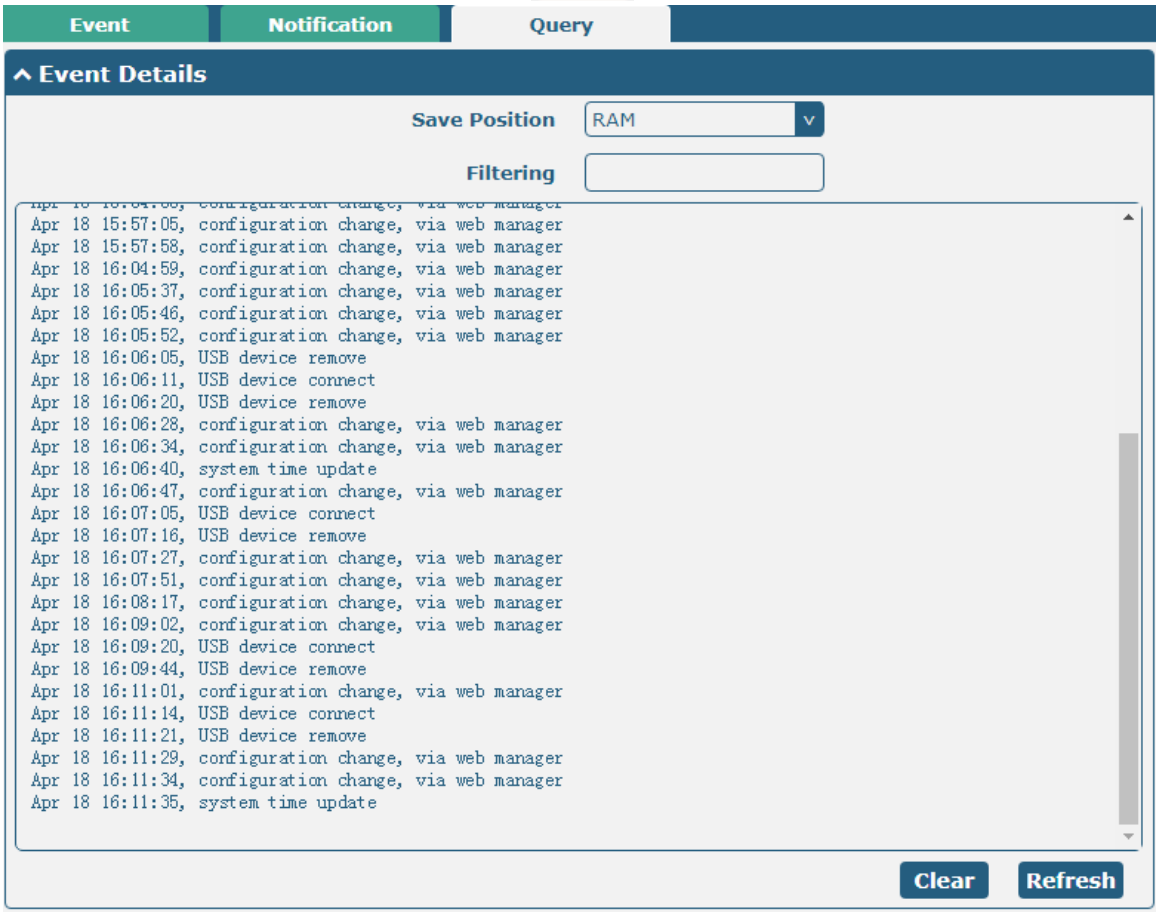




General Settings @ Notification		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--

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. The specified phone number is set in "4.5.4 SMS".	OFF
Phone Number	Enter the phone numbers used for receiving event notification. Use a semicolon (;) to separate each number.	Null
Send Email	Click the toggle button to enable/disable this option. When enabled, the router will send notification to the specified email box via Email if event occurs. Set the related email address in “4.5.5 Services > Email”.	OFF
Email Addresses	Enter the email addresses used for receiving event notification. Use a space to separate each address.	Null
DO Control	Click the toggle button to enable/disable this option. When enabled, the DO output is triggered.	OFF
Save to NVM	Click the toggle button to enable/disable this option. Enable to save event to nonvolatile memory.	OFF

In the "Query" column, you can query the occurrence records of various events. Select the storage location, enter keywords in the filter item to filter events, and use the separator "&" to separate two or more keywords. Click **Refresh** to query filtered events while click **Clear** to clear the event records in the window.

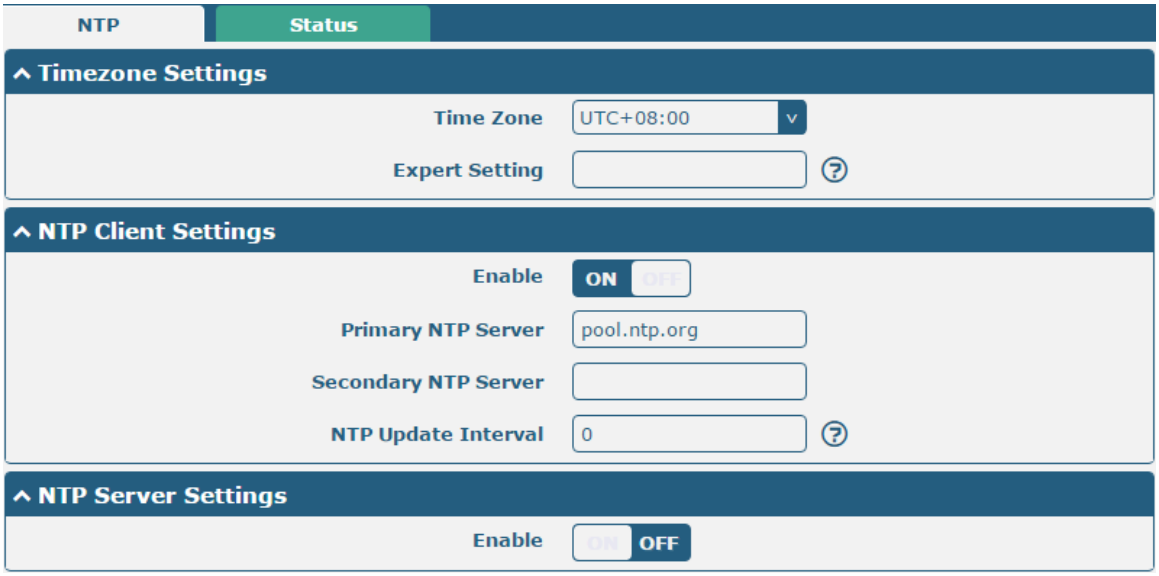


Event Details		
Item	**Description**	**Default**
Save Position	Select the events’ save position from “RAM” or “NVM”.	RAM

	• RAM: Random-access memory • NVM: Non-Volatile Memory	
Filter Message	Event will be filtered according to the Filter Message that the user set. Click the "Refresh" button, the filtered event will be displayed in the follow box. Use "&" to separate more than one filter message, such as message1&message2.	Null

4.5.3 NTP

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

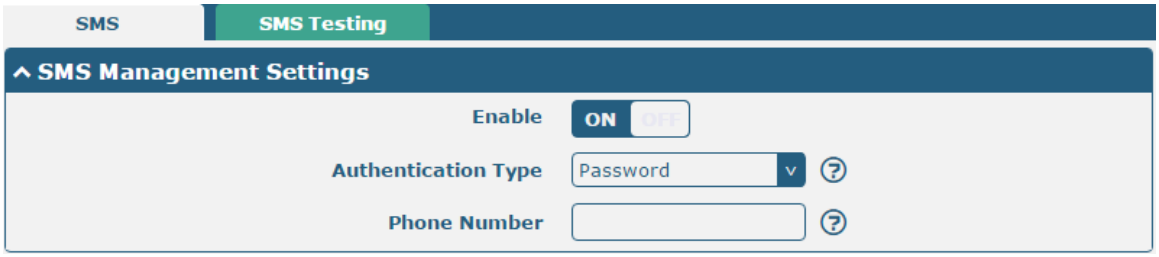


NTP		
Item	**Description**	**Default**
Timezone Settings		
Time Zone	Click the drop down list to select the time zone you are in.	UTC +08:00
Expert Setting	Specify the time zone with Daylight Saving Time in TZ environment variable format. The Time Zone option will be ignored in this case. Not support setting special characters, such as" ~ ".	Null
NTP Client Settings		
Enable	Click the toggle button to enable/disable this option. Enable to synchronize time with the NTP server.	ON
Primary NTP Server	Enter primary NTP Server's IP address or domain name.	pool.ntp.org
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.	Null
NTP Update interval	Enter the interval (minutes) which NTP client synchronize the time from NTP server. Minutes wait for next update, and 0 means update only once.	0
NTP Server Settings		
Enable	Click the toggle button to enable the NTP server option.	OFF

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

4.5.4 SMS

This section allows you to set SMS parameters. Router supports SMS management, and user can control and configure their routers by sending SMS. For more details about SMS control, refer to **5.1.2 SMS Remote Control**.



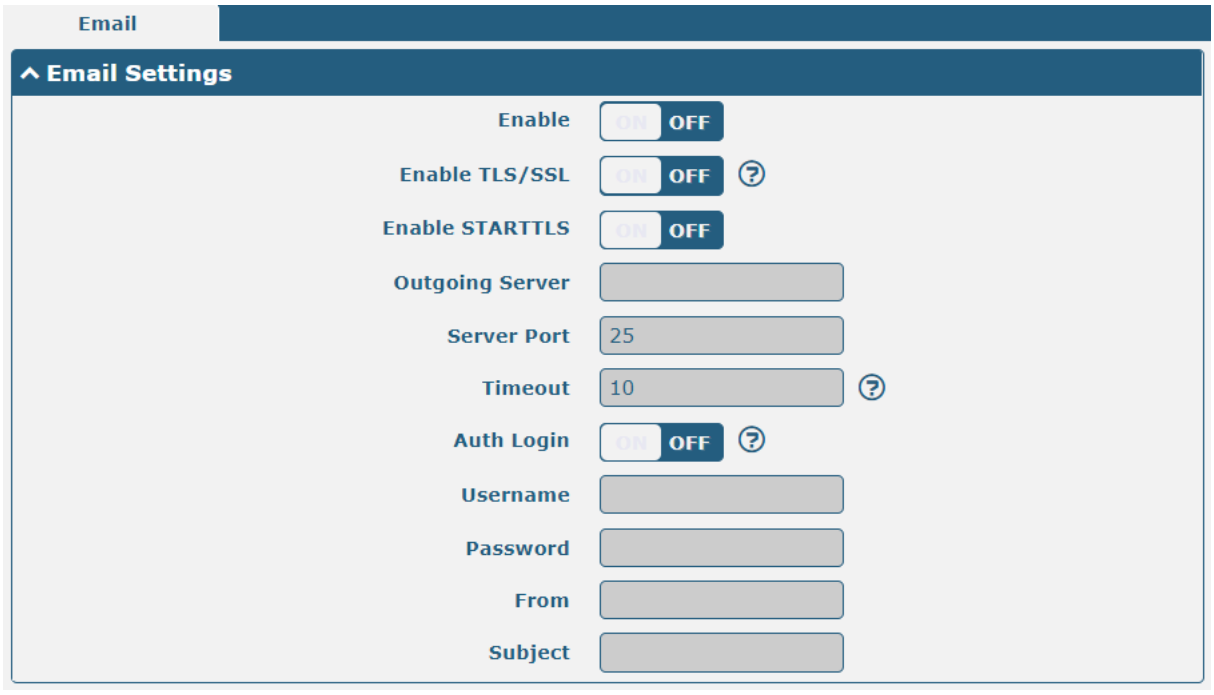
SMS Management Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the SMS Management option. **Note**: If this option is disabled, the SMS configuration is invalid.	ON
Authentication Type	Select Authentication Type from "Password", "Phonenum" or "Both". • Password: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

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

SMS Testing		
Item	**Description**	**Default**
Phone Number	Enter the specified phone number which can receive the SMS from router.	Null
Message	Enter the message that router will send it to the specified phone number.	Null
Result	The result of the SMS test will be displayed in the result box. For example, if the SMS is sent successfully, this result box will show "OK".	
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.

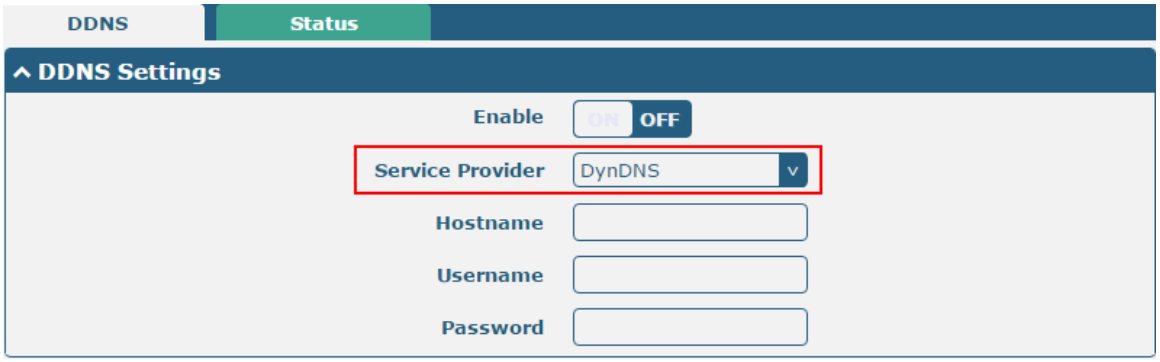


Email Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Email option.	OFF
Enable TLS/SSL	Click the toggle button to enable/disable the TLS/SSL option.	OFF
Enable STARTTLS	Click the toggle button to enable/disable the STARTTLS option.	OFF
Outgoing server	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	Use username and password to authenticate.	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

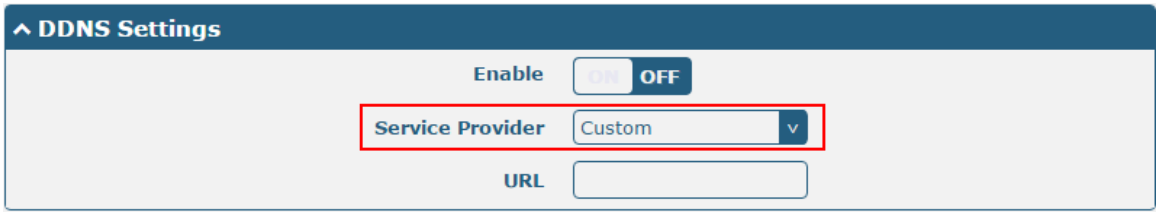
4.5.6 DDNS

DDNS, full name Dynamic Domain Name Server, allows a dynamic IP address to be mapped to a fixed domain name resolution service, each time a user connects to the network the client program will transmit the dynamic IP address of the host to the server program located on the service provider's host through messaging. The server program is responsible for providing DNS services and implementing dynamic domain name resolution, i.e. DDNS service allows you to assign a fixed domain name to the host's dynamic WAN IP, and other users can access your host directly through this fixed domain name, instead of through the dynamic WAN IP address. The router's dynamic WAN IP address is assigned directly by the ISP.

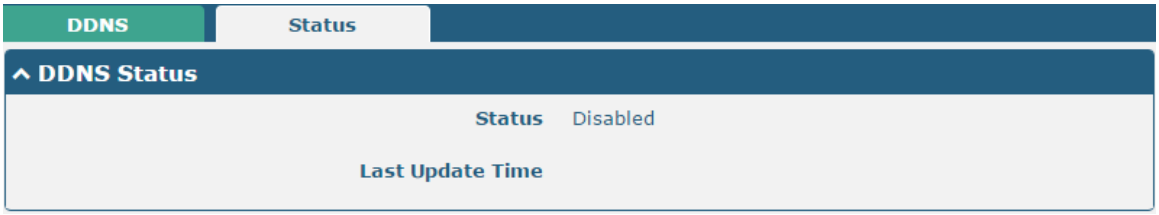
Click "**Services > DDNS"** to set the parameters for DDNS, the default service provider is "DynDNS".



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



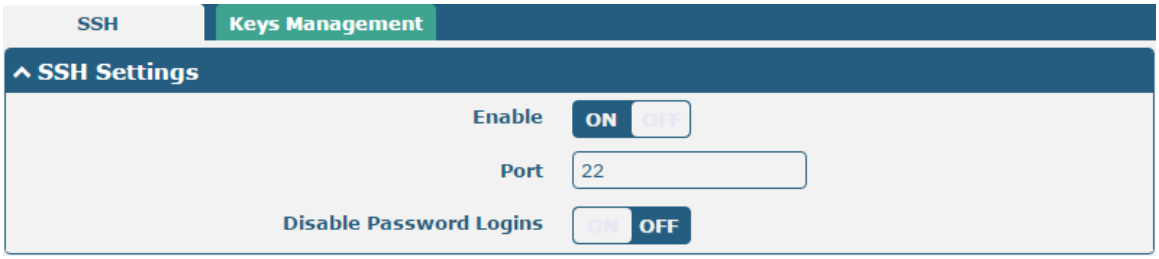
DDNS Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the DDNS option.	OFF
Service Provider	Select the DDNS service from “DynDNS”, “NO-IP”, “3322” or “Custom”. **Note:** the DDNS service only can be used after registered by Corresponding service provider.	DynDNS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



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.



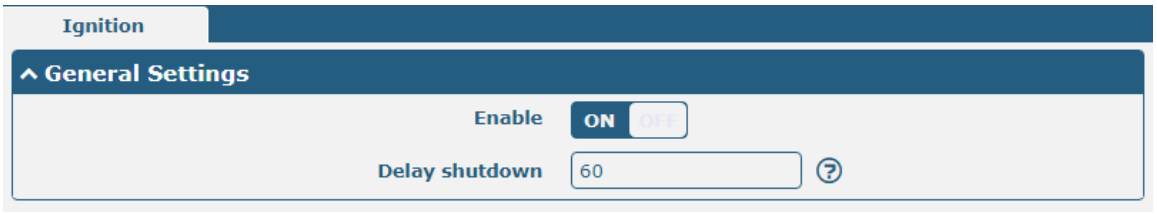
SSH Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable this option. When enabled, you can access the router via SSH.	ON
Port	Set the port of the SSH access.	22
Disable Password Logins	Click the toggle button to enable/disable this option. When enabled, you	OFF

	cannot use username and password to access the router via SSH. In this case, only the key can be used for login.	

Import Authorized Keys	
Item	**Description**
Authorized Keys	This is valid when disabling password login is enabled. Importing a correct public key from your computer to the router will allow users to SSH directly to the router without a password.

4.5.8 Ignition

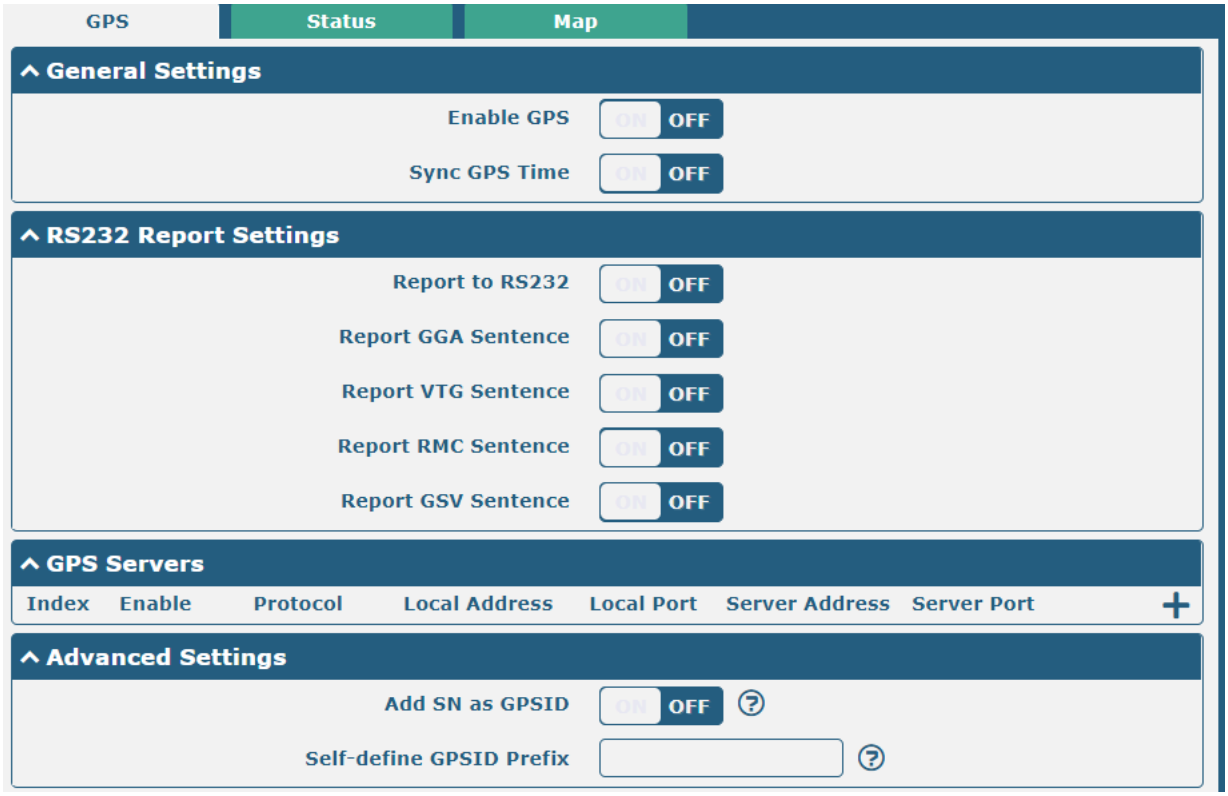
This section is used to configure the parameters of Ignition. Ignition is an application for the in-car ignition sensing. Ignition and POE function can only choose one or the other.



General Settings		
Item	**Description**	**Default**
Waiting time	Enter the time in seconds you want to delay power down. The timeout for delayed power down is 60 seconds to 3600 seconds.	60

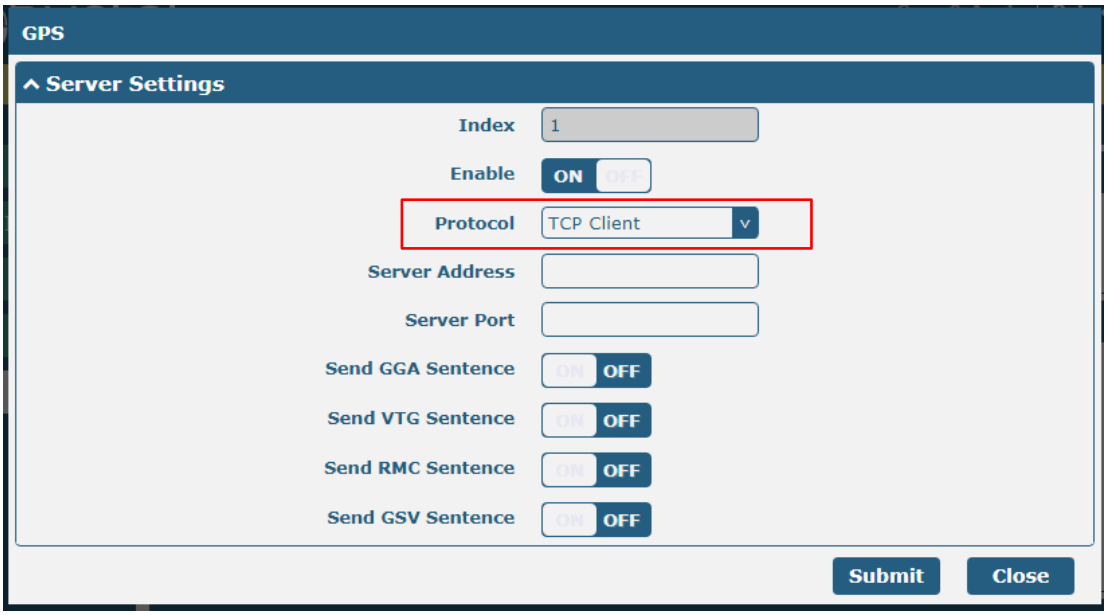
4.5.9 GPS

This section is used to configure the parameters of GPS. The GPS function can locate and obtain the location information and report it to the designated server. The R5020 does not have a separate GPS module and the location data comes from the cellular module.

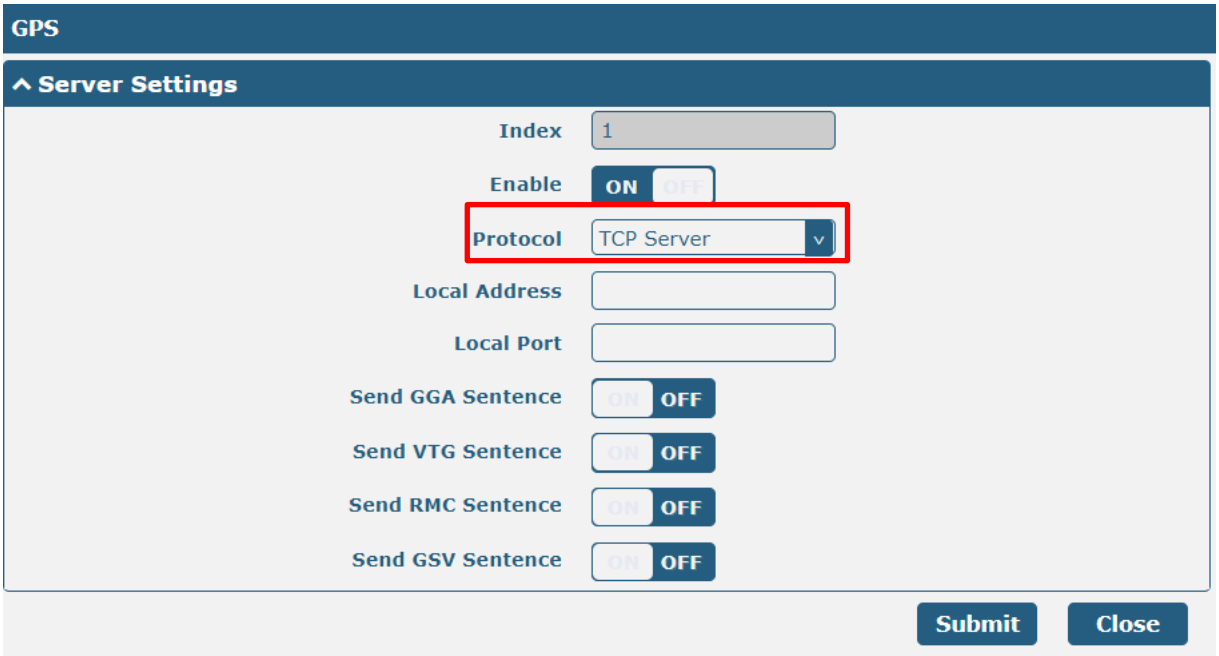


GPS		
Item	**Description**	**Default**
General Settings		
Enable	Click the toggle button to ON to enable GPS.	OFF
Synchronized GPS Time	Click the toggle button to ON to synchronize GPS time.	OFF
RS232 Report Data Settings		
Reporting data through RS232	Reporting GPS Information by RS232.	OFF
Reporting GGA Information	Reporting GGA Information.	OFF
Reporting VTG Information	Reporting VTG Information.	OFF
Reporting RMC Information	Reporting RMC Information.	OFF
Reporting GSV Information	Reporting GSV Information.	OFF

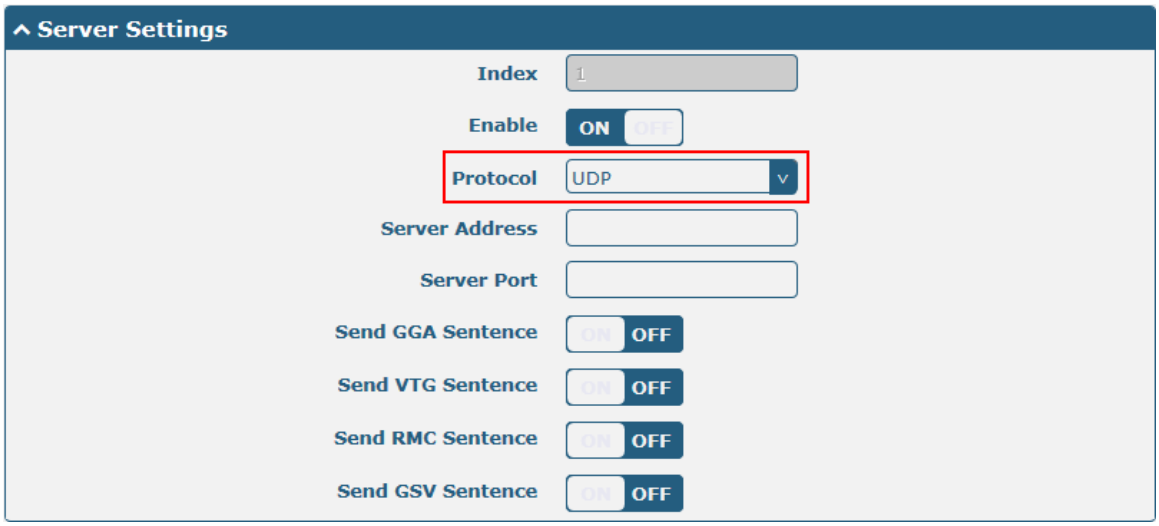
Click the Add button in the GPS server window, and the protocol defaults to "TCP Client" as follows:



When selecting "TCP Server" as the protocol, the window appears as follows:

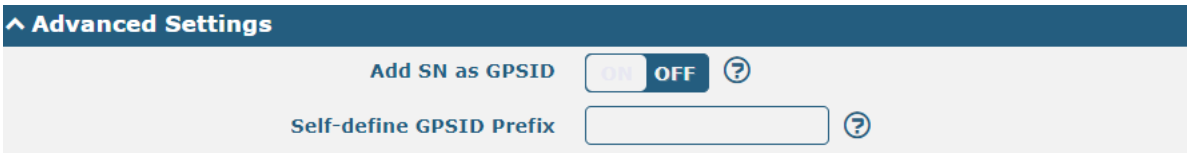


When selecting "UDP" as the protocol, the window appears as follows:



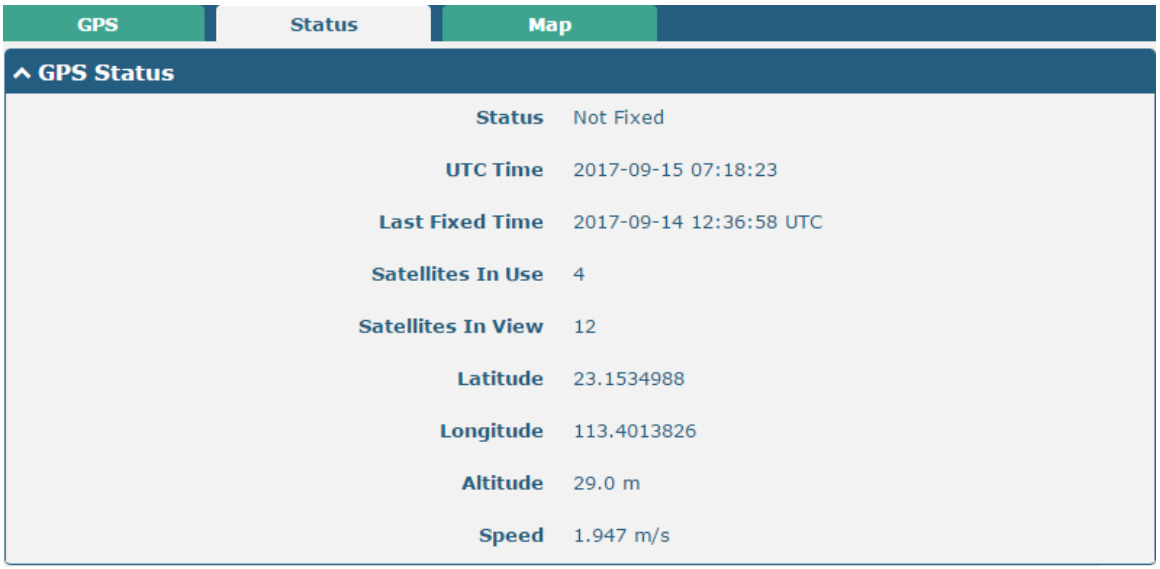
GPS Data Forwarding Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to "ON" to enable the GPS data forwarding settings.	ON
Protocol	Select "TCP client", "TCP server" or "UDP" as the protocol. • TCP Client: When the router acts as a TCP client, it starts up with the TCP server (GPS server). The address of the server supports both IP and domain name. • TCP server: The router acts as a TCP server (GPS server) and listens for connection requests from TCP clients. • UDP： Router as a UDP client.	TCP Client
Server address @TCP client	Set the address of the TCP server.	Null
Server port @TCP client	Set the port of the remote TCP server	Null
Local address	Set the local address of the router as a TCP server.	Null
Local port	Set the local port of the router as a TCP server.	Null
Server address @UDP	Set the address of the TCP server	Null
Server port @UDP	Set the port of the remote TCP server.	Null
Send GGA information	Send GGA information in NMEA format	OFF
Send VTG information	Send VTG information in NMEA format	OFF
Send RMC information	Send RMC information in NMEA format	OFF

GPS Data Forwarding Settings		
Item	**Description**	**Default**
Send GSV information	Send GSV information in NMEA format	OFF



Advanced Settings		
Item	**Description**	**Default**
Add SN as GPSID	Click the toggle button to enable/disable this option. When enabled, the SN is appended to the NMEA message as a GPSID before transmission.	OFF
Self-define GPSID Prefix	Customize the GPSID prefix with a 4-capital letter prefix.	Null

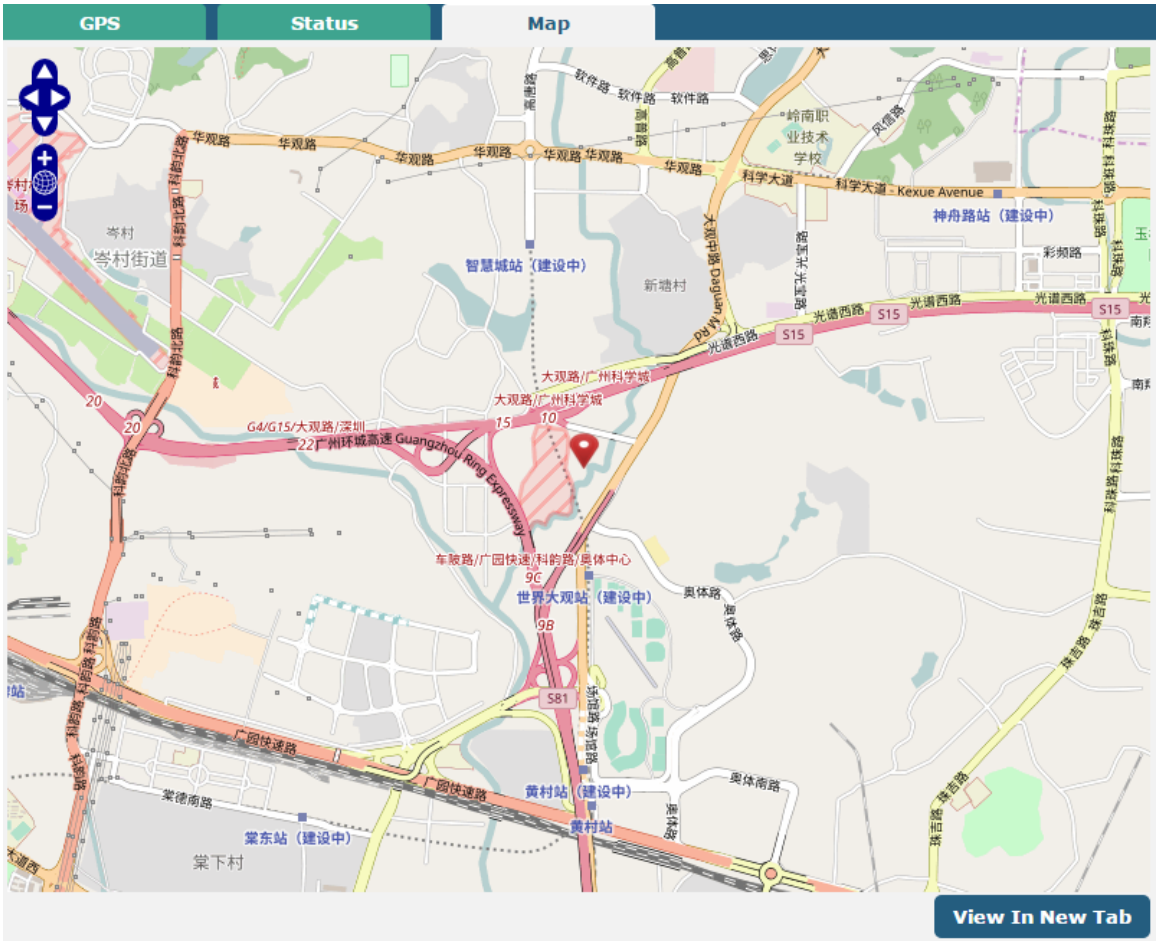
Click the Status bar to view the current GPS status;



GPS Status	
Item	**Description**
Status	Shows the current GPS status of the router.
UTC	Shows the UTC of satellite. **Note:** UTC is the world's unified time, not local time.
Final positioning time	The time of the last successful positioning.
Number of satellites used	Number of satellites used

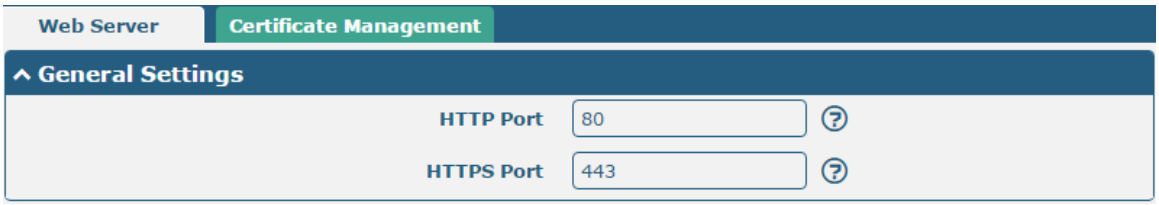
GPS Status	
Item	**Description**
Number of visible satellites	Number of visible satellites
Latitude	Shows the Latitude information of the router.
Longitude	Shows the longitude information of the router.
Height	Shows the height information of the router.
Speed	Shows the speed information of the router.

Click the Map bar to view the current geolocation.



4.5.10 Web Server

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



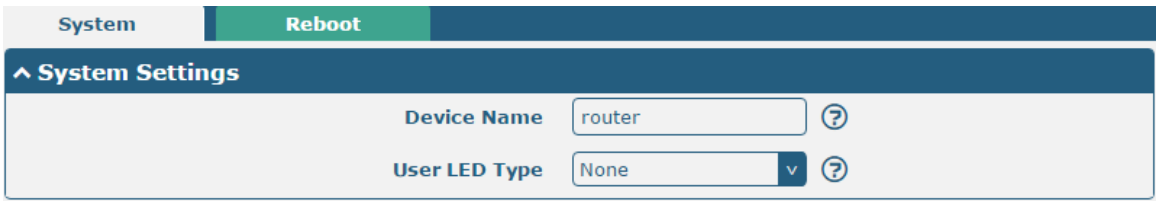
General Settings @ Web Server		
Item	**Description**	**Default**
HTTP Port	Enter the HTTP port number you want to change in router's Web Server. On a Web server, port 80 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTP Port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

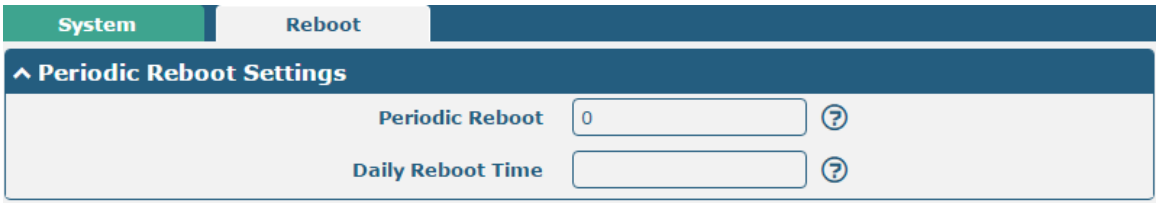
Import Certificate		
Item	**Description**	**Default**
Import Type	Select from "CA" and "Private Key". • CA: a digital certificate issued by CA center • Private Key: a private key file	CA
HTTPS Certificate	Click on "Choose File" to locate the certificate file from your computer, and then click "Import"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

4.5.11 Advanced

Router advanced settings including system settings and reboot.



System Settings		
Item	**Description**	**Default**
Device Name	Set the device name to distinguish different devices you have installed; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	router
User LED Type	Specify the display type of your USR LED. Select from “None”, “OpenVPN” or “IPsec”. • None: Meaningless indication, and the LED is off • SIM:show the sim status. • OpenVPN: USR indicator showing the OpenVPN status • IPsec: USR indicator showing the IPsec status **Note**: For more details about USR indicator, see “2.2 LED Indicators”.	None

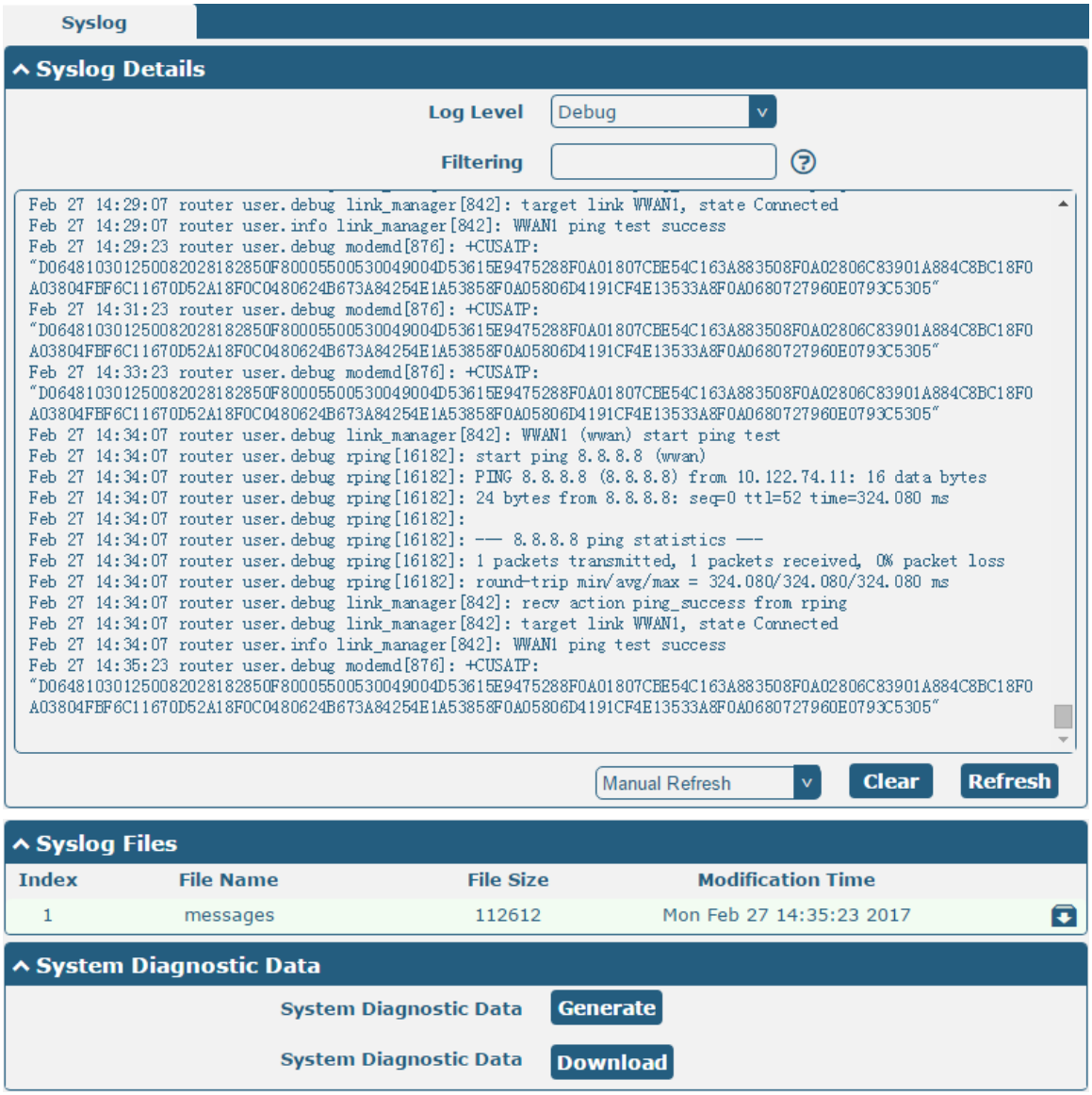


Reboot		
Item	**Description**	**Default**
Periodic Reboot	Set the reboot period of the router. 0 means disable.	0
Daily Reboot Time	Set the daily reboot time of the router, you should follow the format as HH: MM, in 24h time frame, otherwise the data will be invalid. Leave it empty means disable.	Null

4.6 System

4.6.1 Debug

This section is used to view and generate the system operation logs and diagnostic data. Click **Service > System Log > System Log Settings** to open the system log.



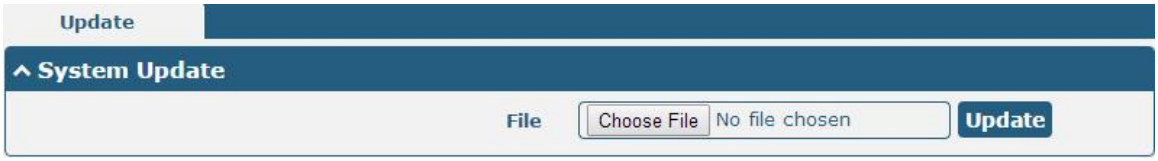
Syslog	
Item	**Description**
Syslog Details	
Log Level	Select from “Debug”, “Info”, “Notice”, “Warn”, “Error” which from low to high. The lower level will output more syslog in detail.
Filtering	Enter the filtering message based on the keywords. Use “&” to separate more than one filter message, such as “keyword1&keyword2”.
Refresh	Select from “Manual Refresh”, “5 Seconds”, “10 Seconds”, “20 Seconds” or “30 Seconds”. You can select these intervals to refresh the log information displayed in the follow box. If selecting “manual refresh”, you should click the refresh button to refresh the syslog.
Clear	Click the button to clear the syslog.
Refresh	Click the button to refresh the syslog.
Syslog Files	
Syslog Files	Only when logging is enabled in "Service > System Log > Enable” files will be displayed in this list. The logs are generated in one file of 200k size, and up to 6 system log files can be displayed. 5 files with the file name of messages0~messages4 are old logs, and the latest

	system log file messages will be on top.
System Diagnosing Data	
Generate	Click to generate the syslog diagnosing file.
Download	Click to download system diagnosing file.

4.6.2 Update

This section is used to upgrade the router system to import and update the firmware file to implement the system update. Import a firmware file from your computer to your router and click Update to start the upgrade process. And follow the system prompts to reboot the device to complete the firmware update.

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

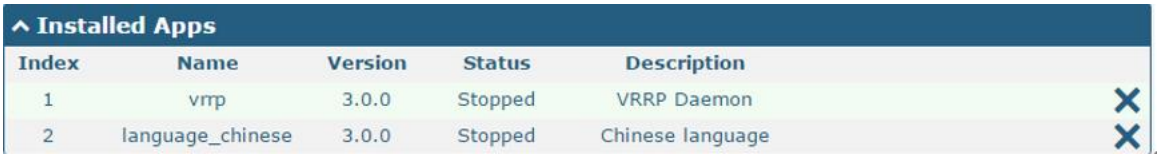


4.6.3 App Center

The router supports App import. You can import and install the app directly in this application, and reboot the device according to the system prompt. After successful installation, the app will be displayed in the "Services" column, while other VPN apps will be displayed in the "VPN" column after installation.

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 shown in the following list, click ✕ to uninstall the app.

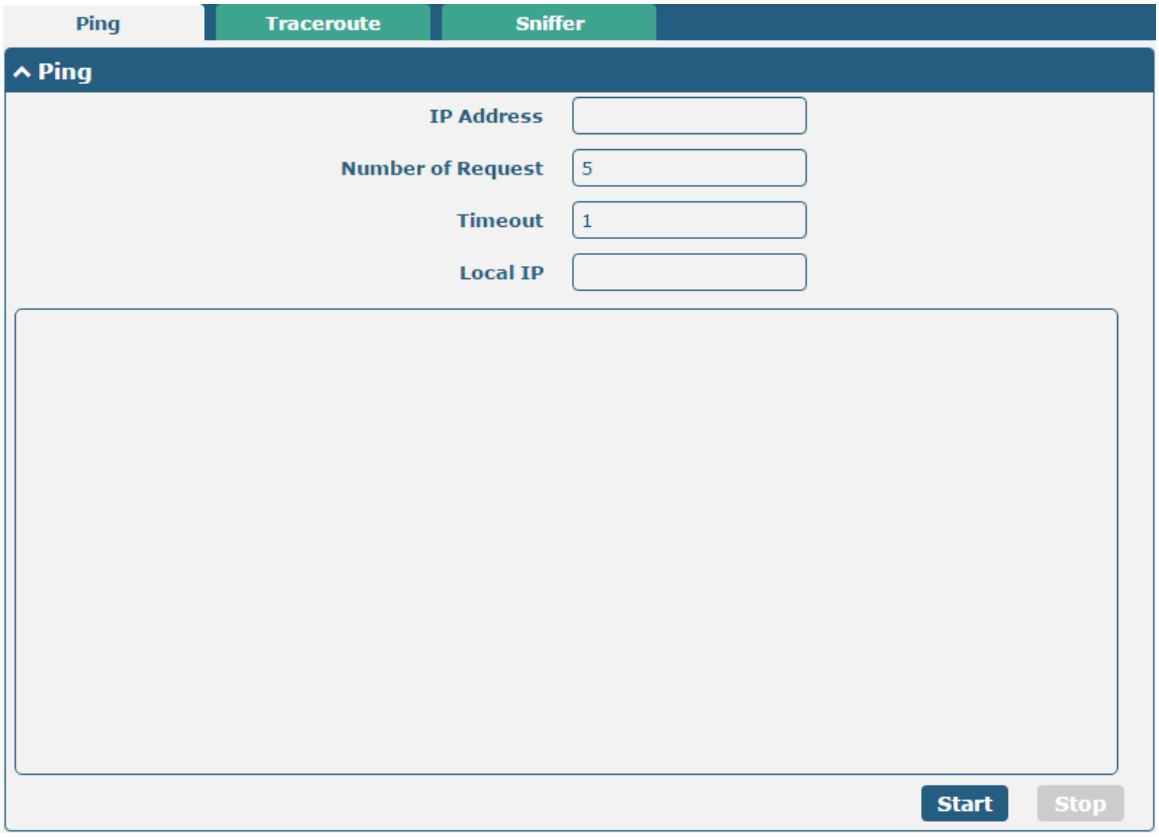


App Center		
Item	**Description**	**Default**
App Install		
File	Click on “Choose File” to locate the App file from your computer, and then click Install to import this file into your router. **Note**: File format should be *xxx.rpk*, e.g. *R5020-robustlink-1.0.0.rpk*.	--

App Center		
Item	**Description**	**Default**
App Install		
Installed Apps		
Index	Indicate the ordinal of the list.	--
Name	Show the name of the App.	Null
Version	Show the version of the App.	Null
Status	Show the status of the App.	Null
Description	Show the description for this App.	Null

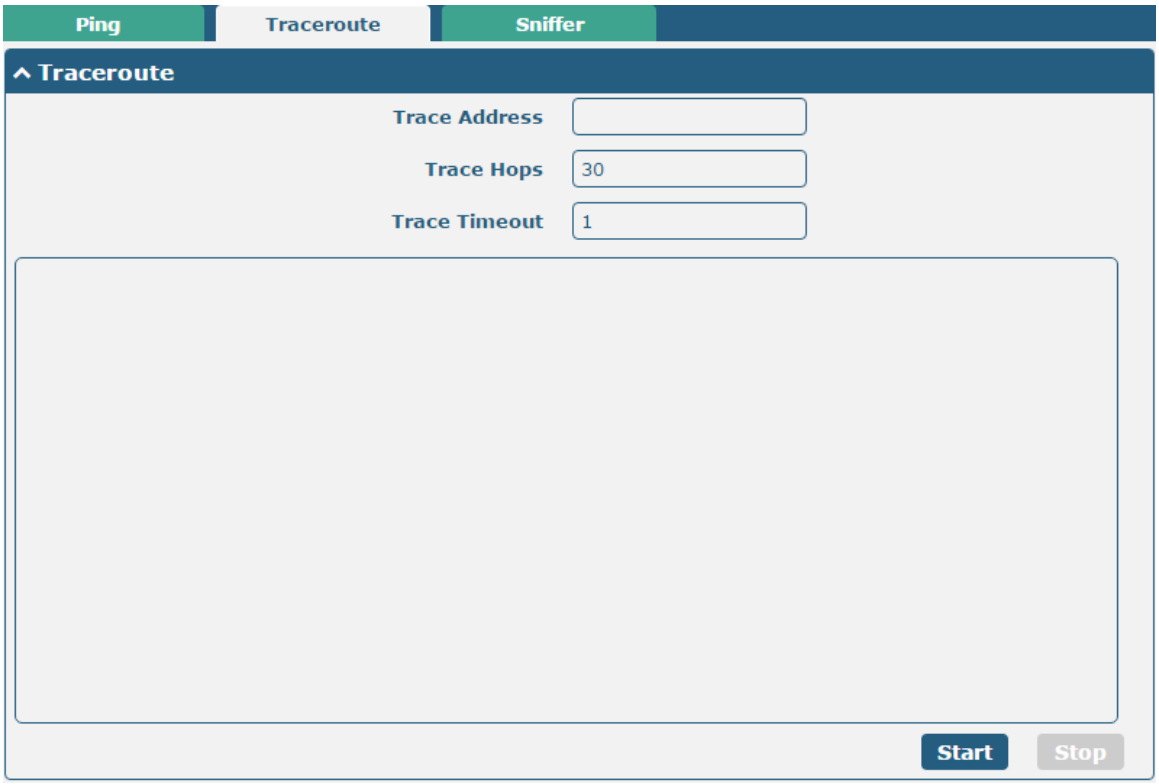
4.6.4 Tools

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

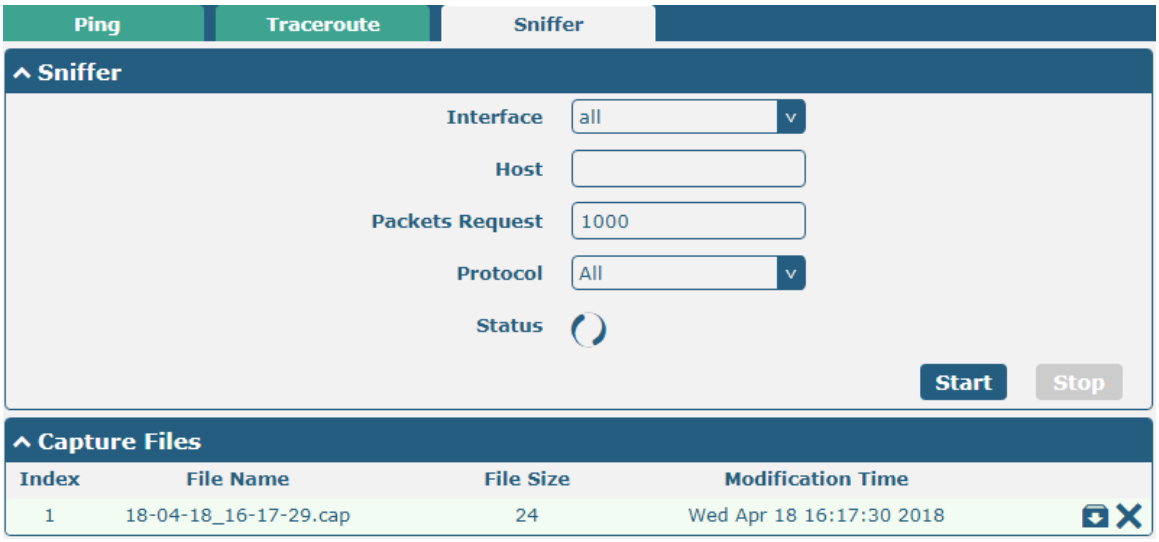


Ping		
Item	**Description**	**Default**
IP address	Enter the ping's destination IP address or destination domain.	Null
Number of Requests	Specify the number of ping requests.	5
Timeout	Specify the timeout of ping request.	1
Local IP	Specify the local IP from cellular WAN, Ethernet WAN or Ethernet LAN. Null stands for selecting local IP address from these three automatically.	Null

Start	Click this button to start ping request, and the log will be displayed in the follow box.	--
Stop	Click this button to stop ping request.	--



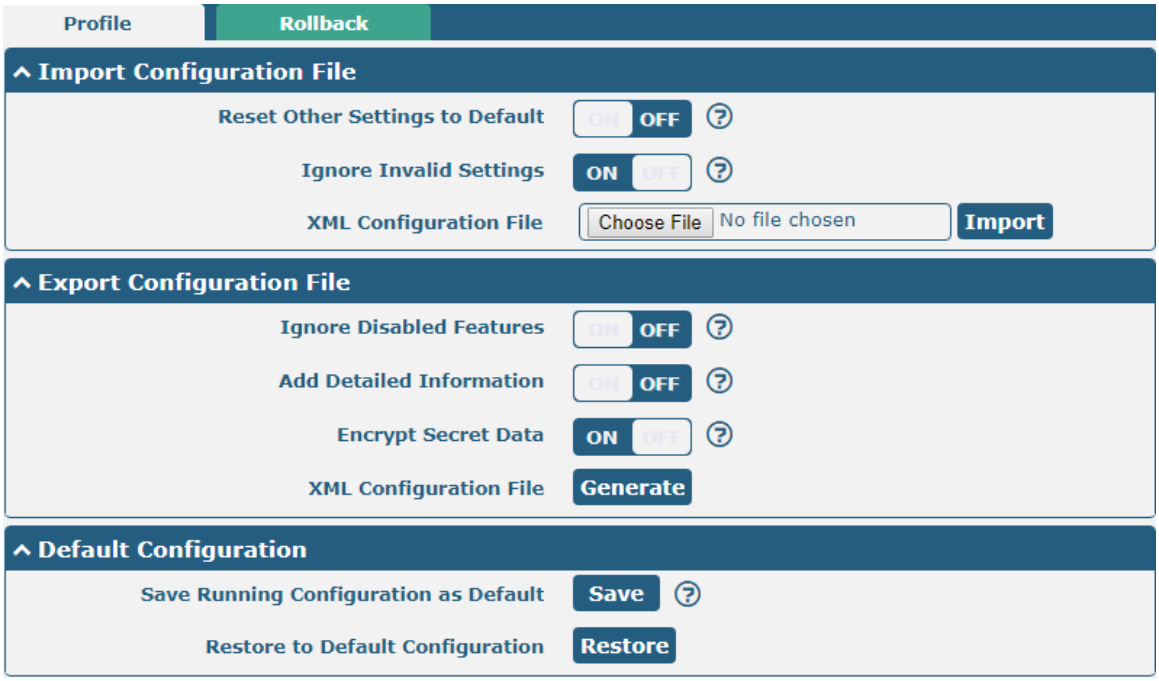
Traceroute		
Item	**Description**	**Default**
Trace Address	Enter the trace's destination IP address or destination domain.	Null
Trace Hops	Specify the max trace hops. Router will stop tracing if the trace hops has met max value no matter the destination has been reached or not.	30
Trace Timeout	Specify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



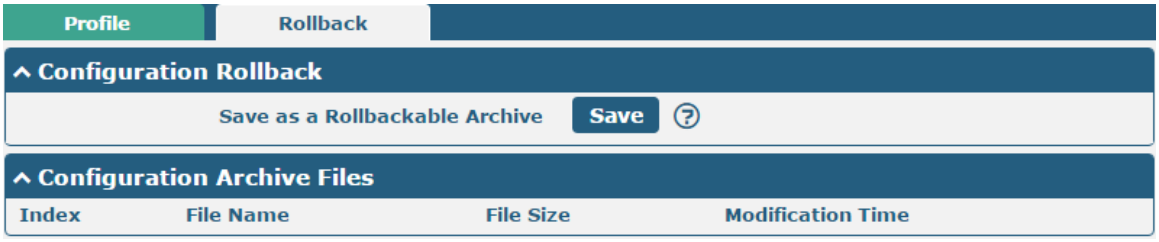
Sniffer		
Item	**Description**	**Default**
Interface	Choose the interface according to your Ethernet configuration.	All
Host	Filter the packet that contain the specify IP address.	Null
Packets Request	Set the packet number that the router can sniffer at a time.	1000
Protocol	Select from “All”, “IP”,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

4.6.5 Profile

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



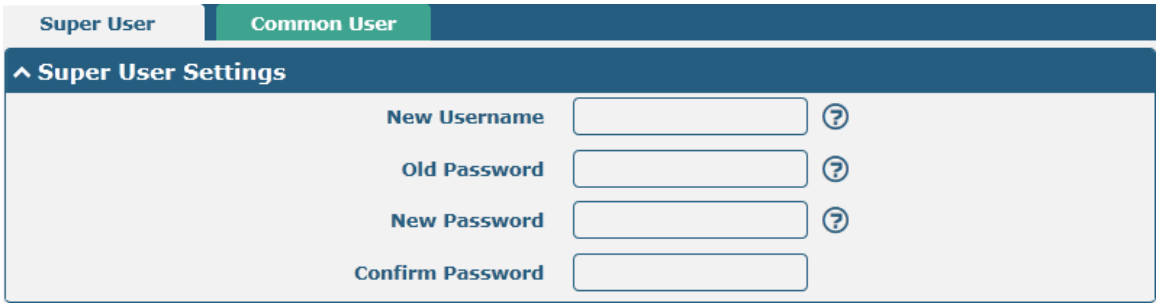
Profile		
Item	**Description**	**Default**
Import Configuration File		
Reset Other Settings to Default	Click the toggle button as “ON” to return other parameters to default settings.	OFF
Ignore Invalid Settings	Click the toggle button as “ON” to ignore invalid settings.	OFF
XML Configuration File	Click on Choose File to locate the XML configuration file from your computer, and then click Import to import this file into your router.	--
Export Configuration File		
Ignore Disabled Features	Click the toggle button as “ON” to ignore the disabled features.	OFF
Add Detailed Information	Click the toggle button as “ON” to add detailed information.	OFF
Encrypt Secret Data	Click the toggle button as “ON” to encrypt the secret data.	ON
XML Configuration File	Click Generate button to generate the XML configuration file, and click Export to export the XML configuration file.	--
Default Configuration		
Save Running Configuration as Default	Click 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.	--

4.6.6 User Management

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



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

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

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

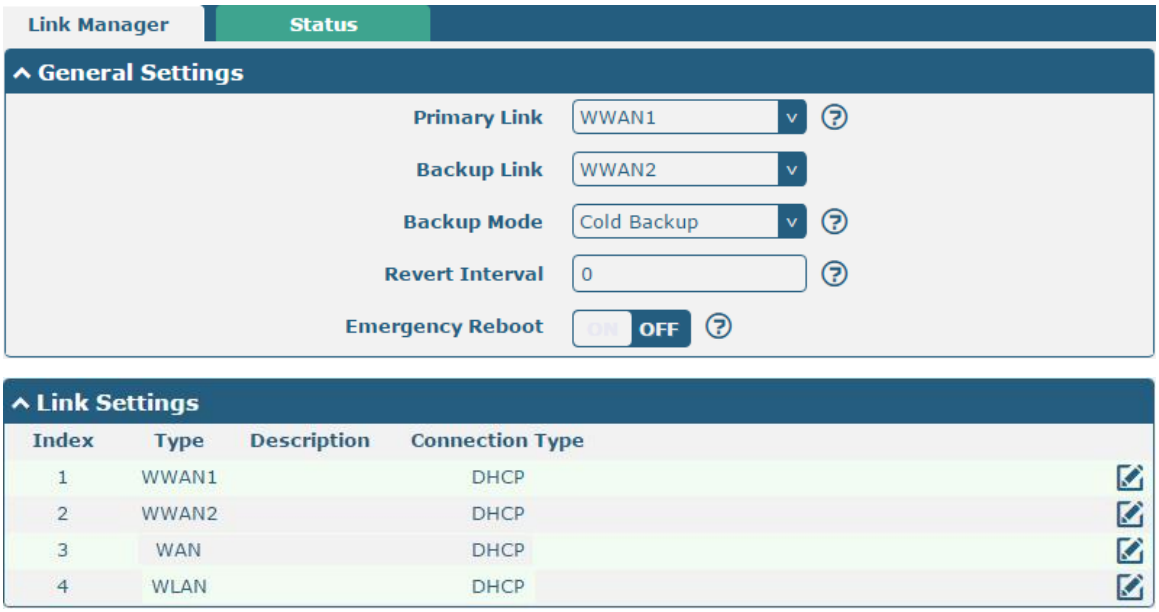
Chapter 5 Configuration Examples

5.1 Cellular

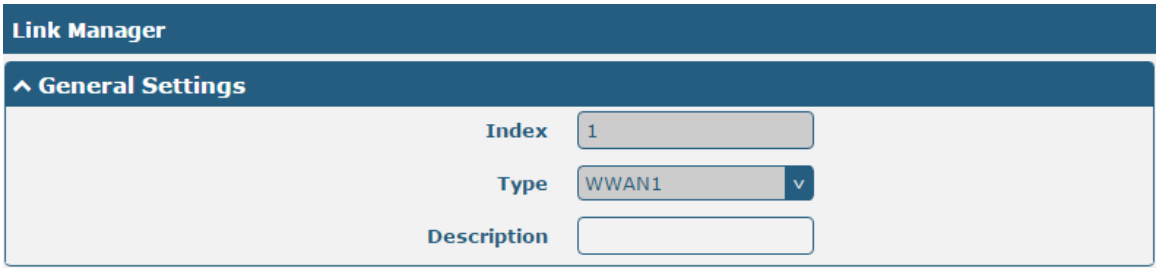
5.1.1 Cellular Dial-Up

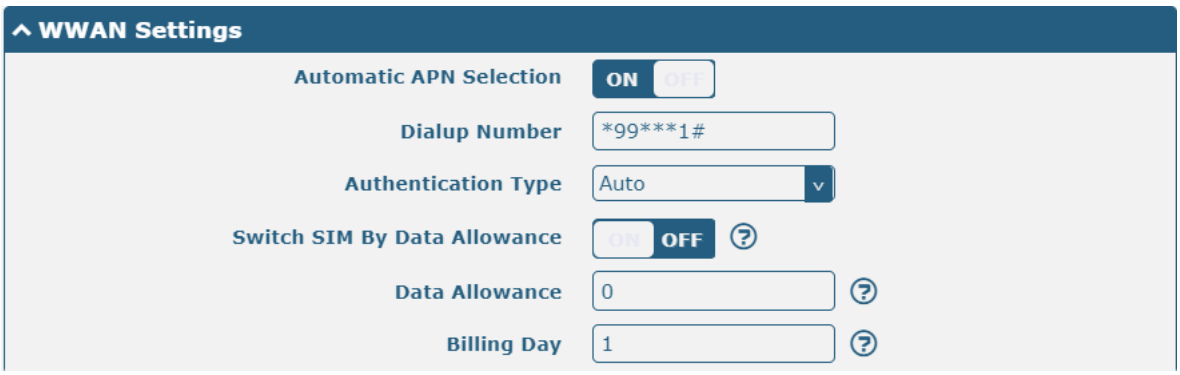
This section shows you how to configure the primary and backup SIM card for Cellular Dial-up. Connect the router correctly and insert two SIM, then open the configuration page. Under the homepage menu, click **Interface > Link Manager > Link Manager > General Settings**, choose "WWAN1" as the primary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

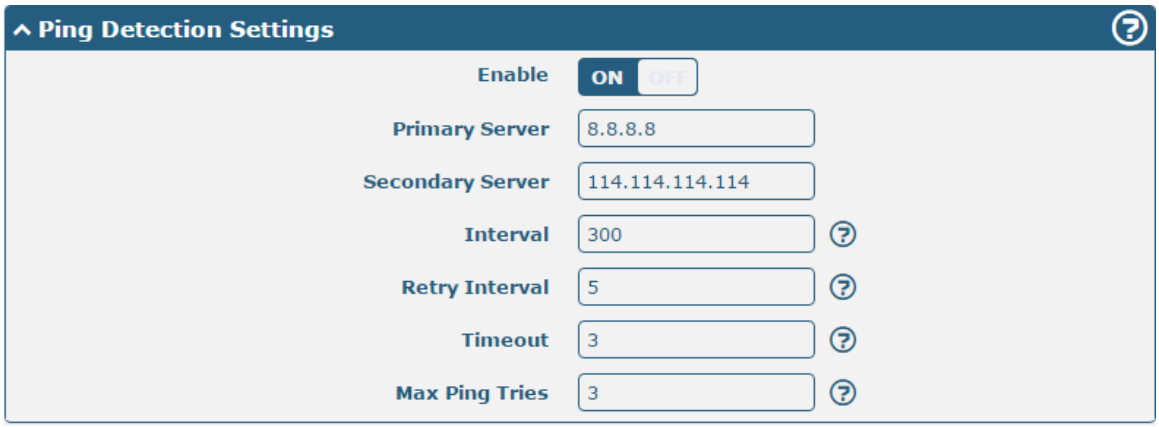
Note: All data will be transferred via WWAN1 when choose WWAN1 as the primary link and set backup mode as cold backup. At the same time, WWAN2 is always offline as a backup link. All data transmission will be switched to WWAN2 when the WWAN1 is disconnected.

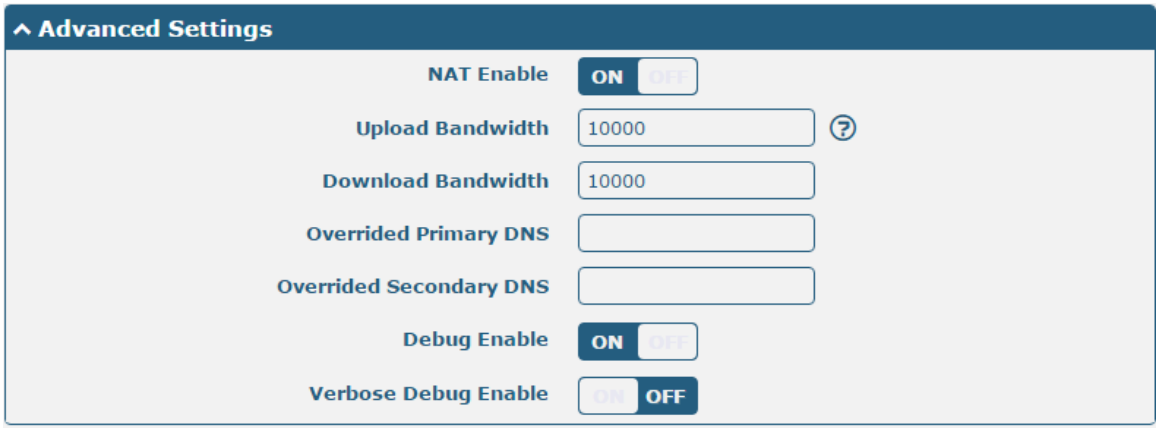


Click the edit button of WWAN1 to set its parameters according to the current ISP.



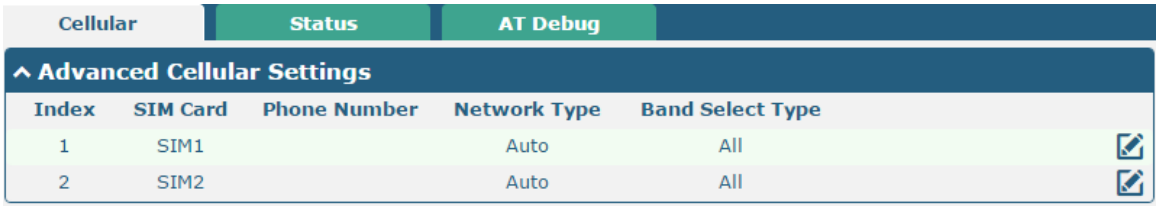




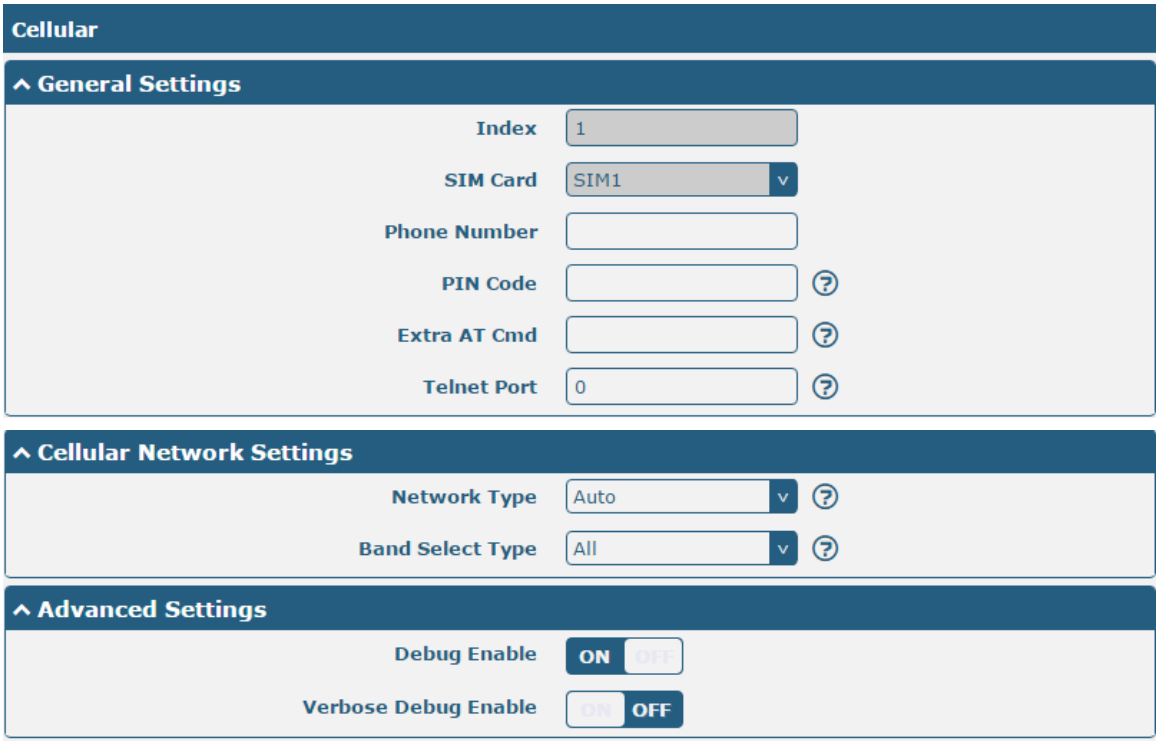


When finished, click **Submit > Save & Apply** for the configuration to take effect.

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



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



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

5.1.2 SMS Remote Control

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

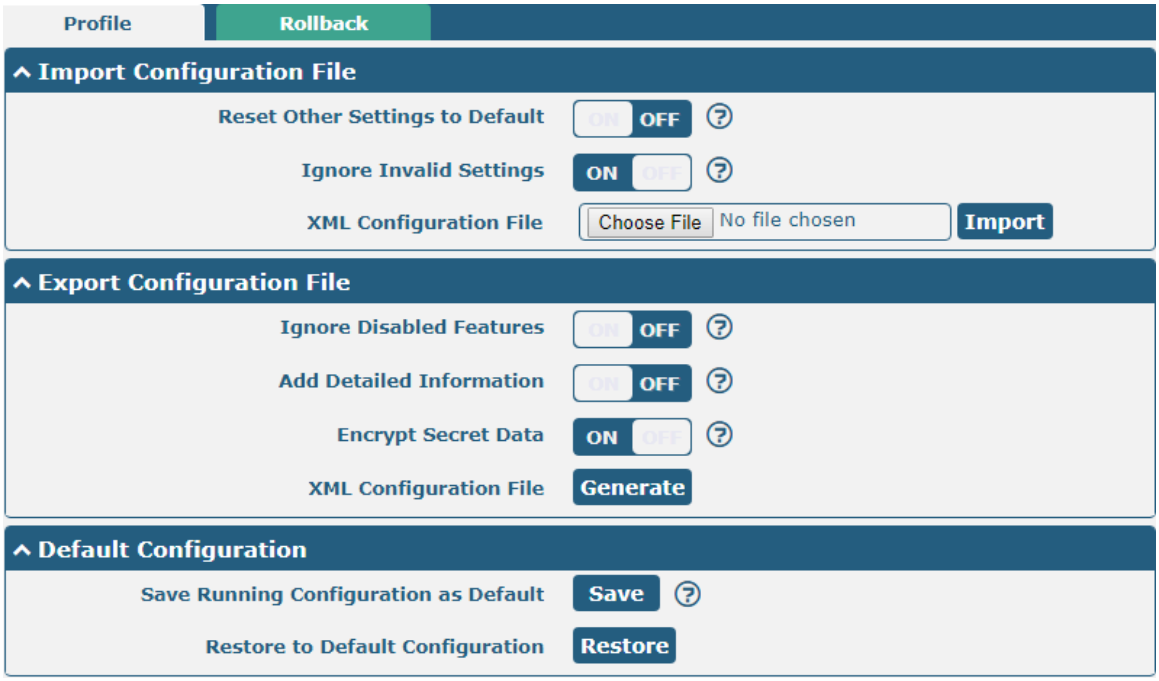
An SMS command has the following structure:

1. Password mode—**Username: Password; cmd1; cmd2; cmd3; …cmdn (**available for every phone number).
2. Phonenum mode-- **Password; cmd1; cmd2; cmd3; … cmdn** (available when the SMS was sent from the phone number which had been added in R5020'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 R5020's phone group).
   Note: All command symbols must be entered in the half-angle mode of the English input method.

SMS command Explanation:

1. User name and Password: use the same username and password as WEB manager for authentication.
2. cmd1, cmd2, cmd3 to Cmdn, the command format is the same as the CLI command, more details about CLI cmd please refer to **Chapter 6 Introductions for CLI**.

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



XML command:

<lan>

<network max_entry_num="2">

<id>1</id>

<interface>lan0</interface>

<ip>172.16.24.24</ip>

<netmask>255.255.0.0</netmask>

<mtu>1500</mtu>

SMS cmd:

set lan network 1 interface lan0

set lan network 1 ip 172.16.24.24

set lan network 1 netmask 255.255.0.0

set lan network 1 mtu 1500

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

admin:admin;status system

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

SMS received:

hardware_version = 1.1

firmware_version = 3.1.0

firmware_version_full = "3.1.0 (Rev 3527)"

kernel_version = 4.9.152

device_model = R5020

serial_number = ""

uptime = "0 days, 00:02:55"

system_time = "Thu May 14 05:51:56 2020 (NTP not updated)"

ram_usage = "389M Free/448M Total"
admin:admin;reBoot
In this command, username is “admin”, password is “admin”, and the command is to reBoot the R5020 Router.
SMS received:
OK

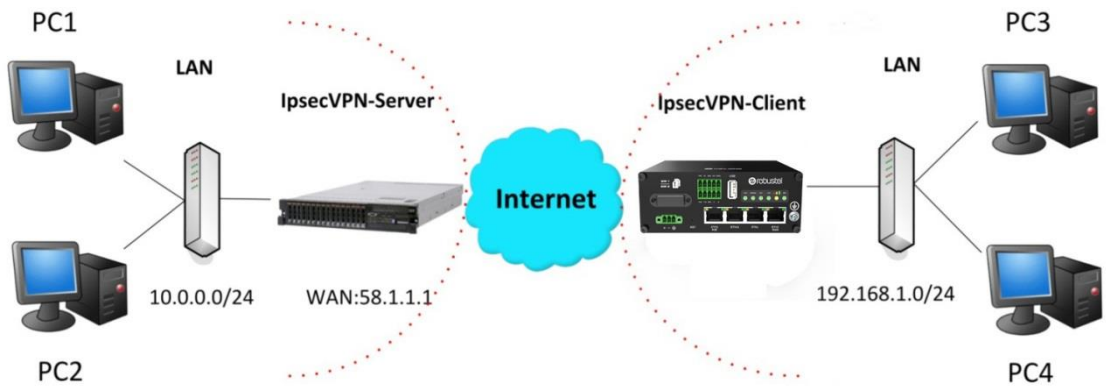
admin:admin;set firewall remote_ssh_access false;set firewall remote_telnet_access false
In this command, username is “admin”, password is “admin”, and the command is to disaBle the remote_ssh and remote_telnet access.
SMS received:
OK
OK

admin:admin; set lan network 1 interface lan0;set lan network 1 ip 172.16.24.24;set lan network 1 netmask 255.255.0.0;set lan network 1 mtu 1500
In this command, username is “admin”, password is “admin”, and the commands is to configure the LAN parameter.
SMS received:
OK
OK
OK
OK

5.2 VPN Configuration Example

5.2.1 IPsec VPN

IPsec VPN example topology (the IKE and SA parameters must be configured on the server and client):



The configuration of server and client is as follows.

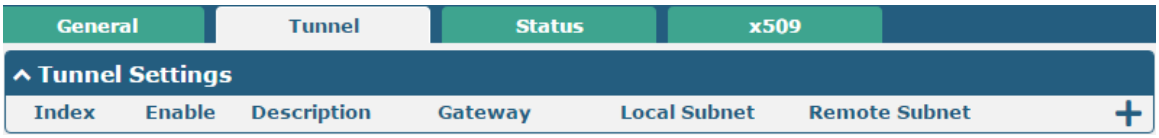
IPsec VPN_Server:

Cisco 2811:

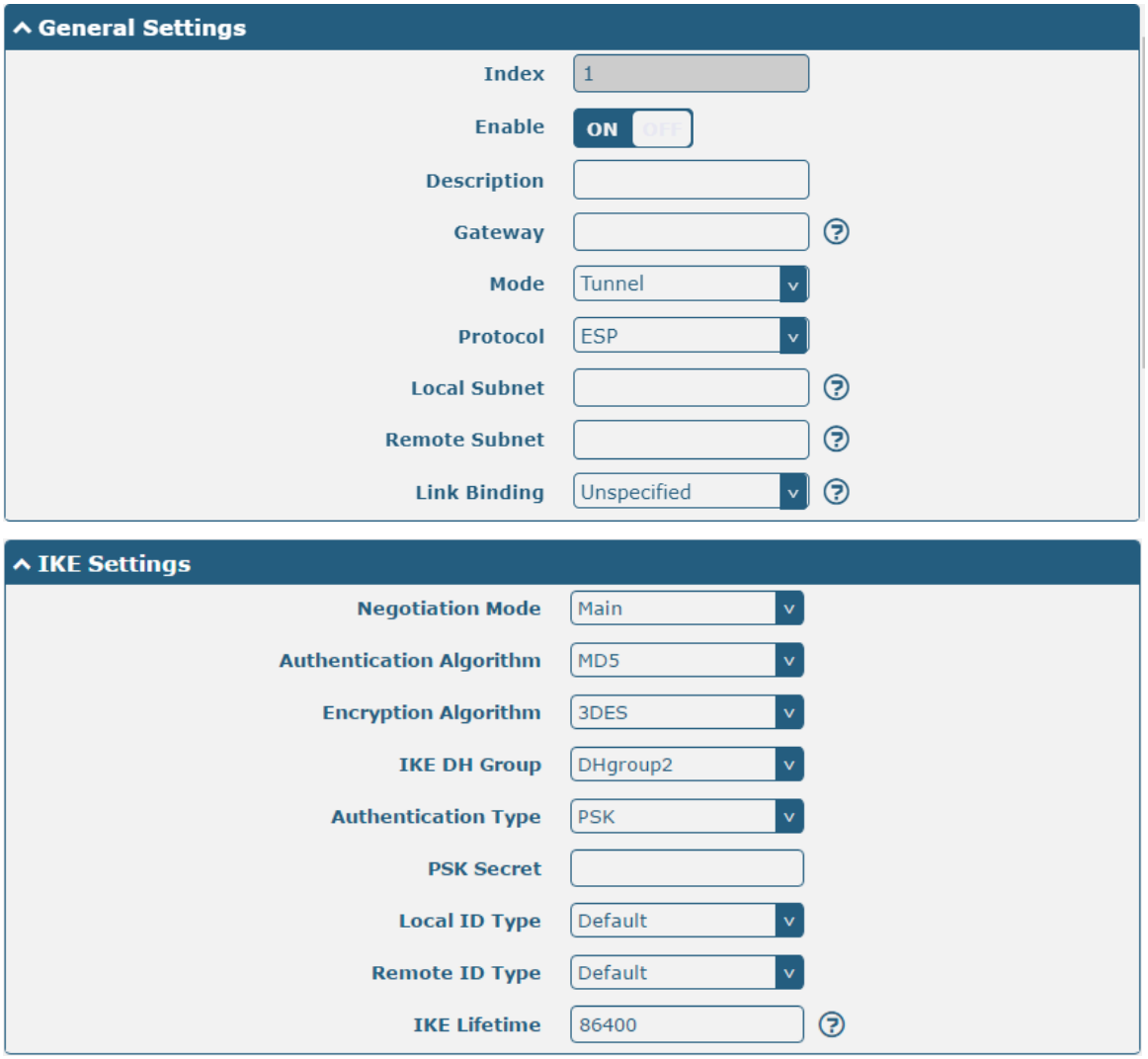
```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set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


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


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


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



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

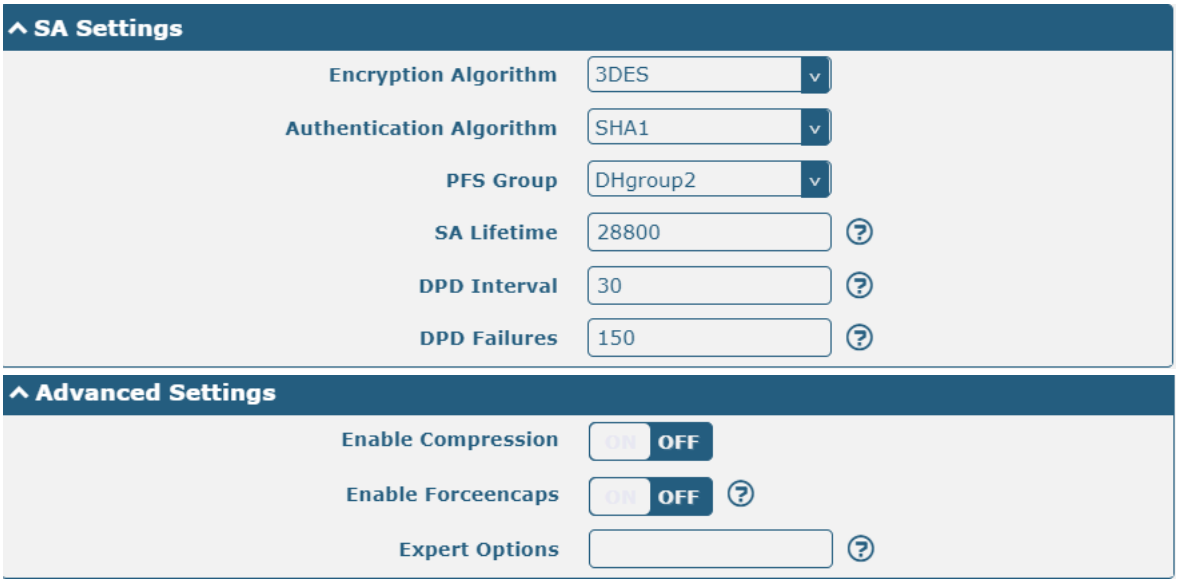
IPsec VPN Client

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



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





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

The comparison between server and client is as below.

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
```

IKE Setting in Client must be consistent with server.

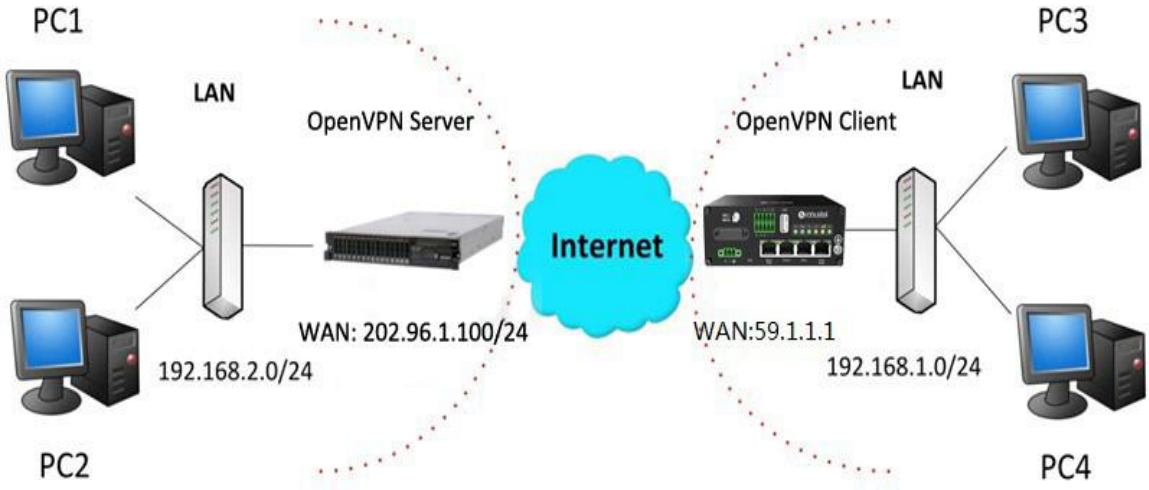
```
Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association 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
```

SA Setting in Client must be consistent with server.

```
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
```

5.2.2 OpenVPN

OpenVPN supports both client and P2P (peer-to-peer) modes. Here, the client is used as an example. The sample topology is shown below:



OpenVPN_Server:

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

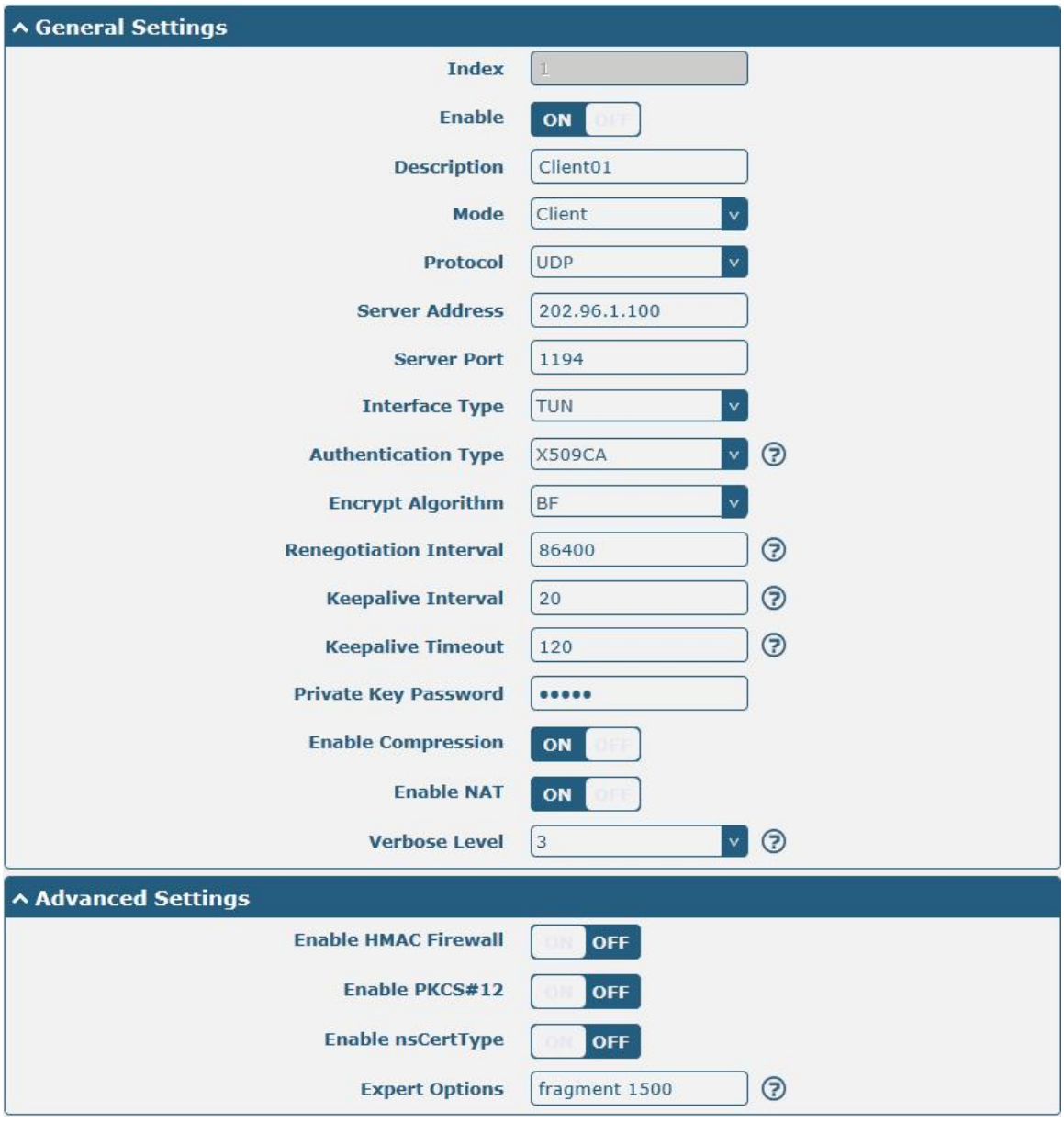
```
local 202.96.1.100
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert Server01.crt
key Server01.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.3.0 255.255.255.0"
client-config-dir ccd
route 192.168.1.0 255.255.255.0
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.

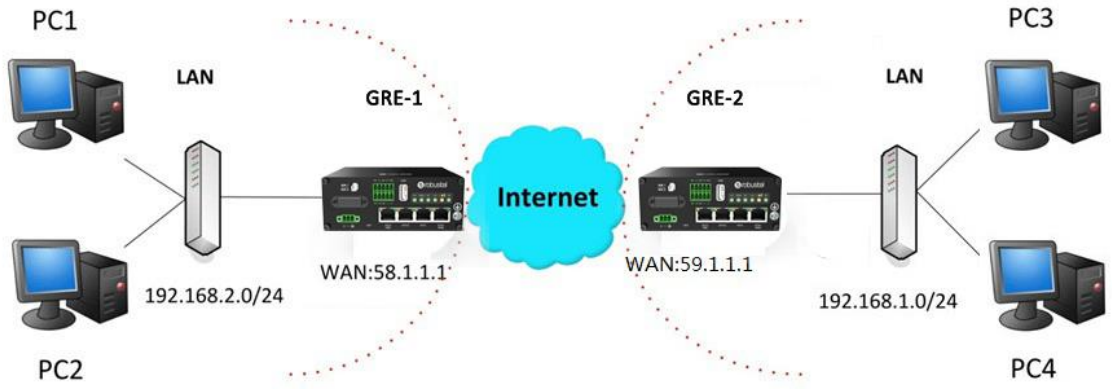
Click + to configure the Client01 as below.



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

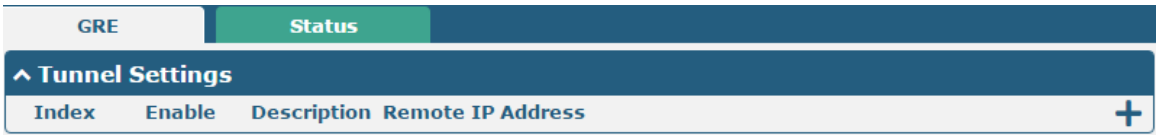
5.2.3 GRE VPN

The configuration of two points is as follows.

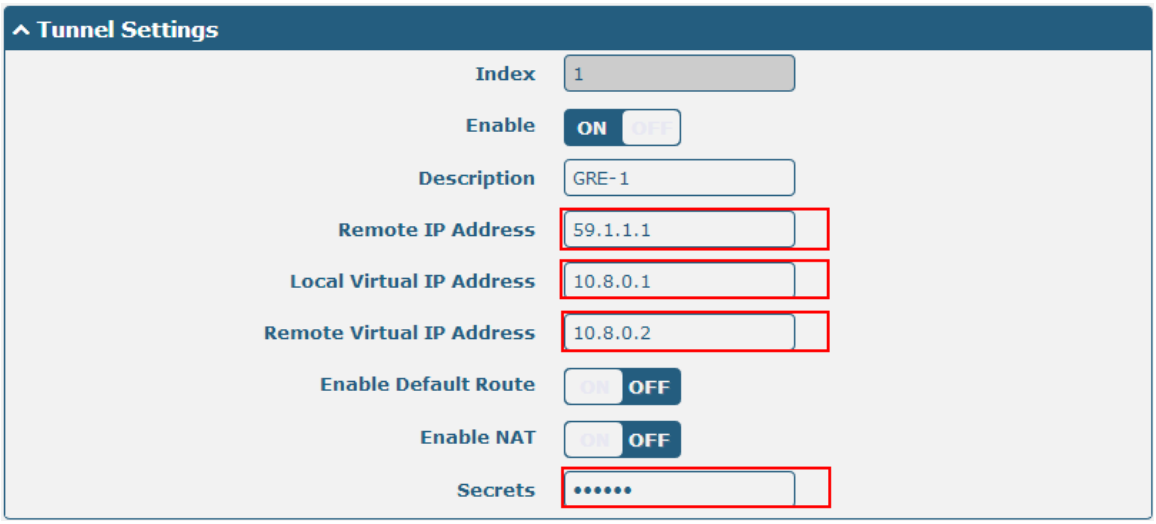


GRE-1:

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



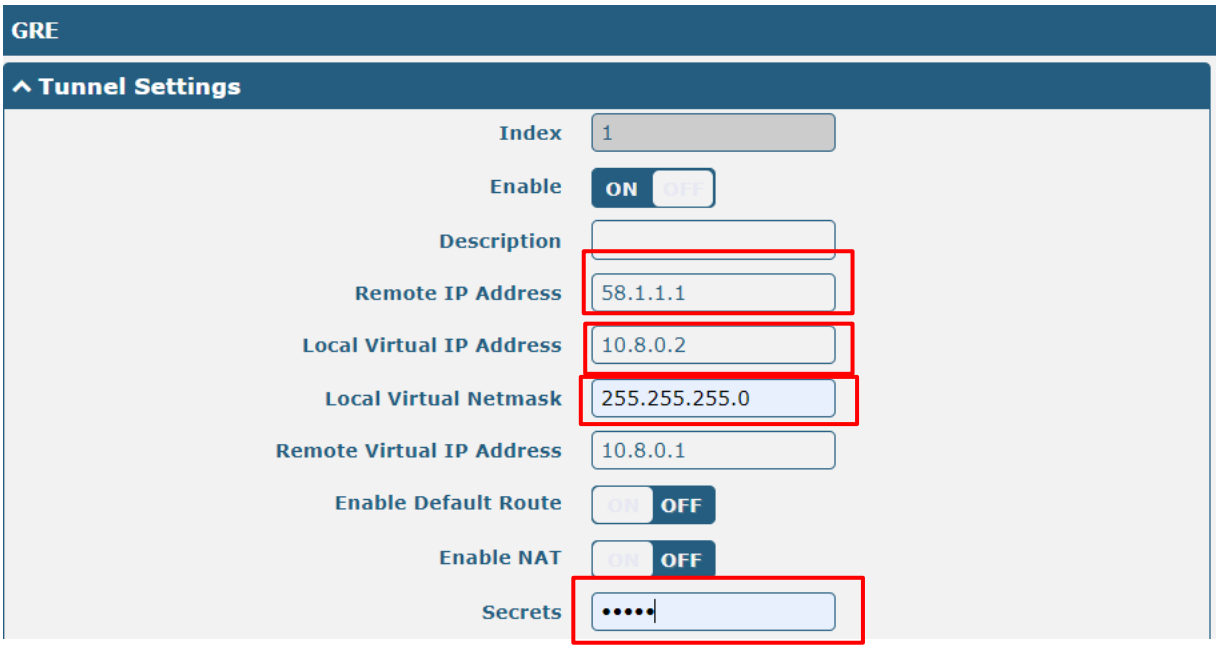
Click + button and set the parameters of GRE-1 as below.



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

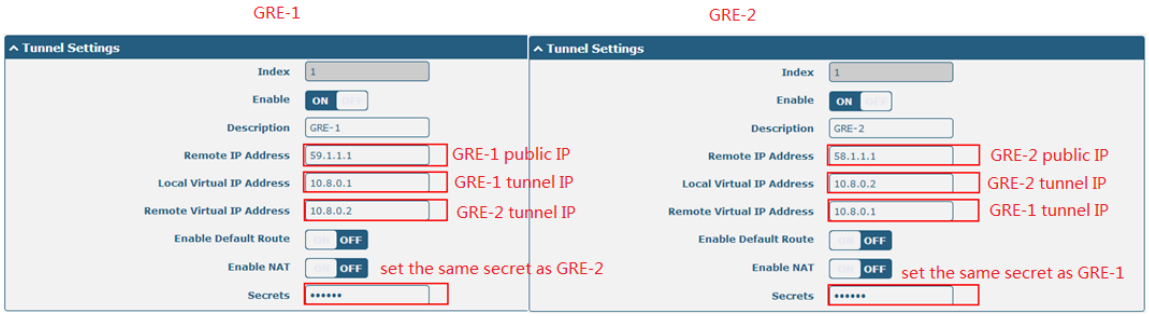
GRE-2:

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



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

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



Chapter 6 Introductions for CLI

6.1 What Is CLI

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

```
router login: admin
Password:
#
  !              Comments
  add            Add a list entry of configuration
  clear          Clear statistics
  config         Configuration operation
  debug          Output debug information to the console
  del            Delete a list entry of configuration
  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

# 
```

Route login:

Router login: admin

Password: admin

#

CLI commands:

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

#

!	Comments
add	Add a list entry of configuration
clear	Clear statistics
config	Configuration operation
debug	Output debug information to the console
del	Delete a list entry of configuration
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

The following list is a description of the help information commands and the error commands encountered during configuration.

Commands /tips	Description
?	Typing a question mark "?" will show you the help information. Example: # config（tick '?'） config Configuration operation # config（tick space key+ +'?'） commit Save the configuration changes and take effect changed configuration save_and_apply Save the configuration changes and take effect changed configuration loaddefault Restore Factory Configuration
Ctrl+c	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	When your setting finished, you should enter those commands to make

# config save_and_apply	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
Set	Set *parameters*	All the function parameters are set by commands set and add, the difference is that set is for the single parameter and add is for the list parameter
Add	Add *parameters*	

Note: More detail about CLI command, please refer to "Command Line Interface Guide".

6.4 Quick Start with Configuration Examples

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

Example 1: Show current version

```
# status system
firmware_version = 3.1.0
firmware_version_full = "3.1.0 (Rev 3527)"
kernel_version = 3.18.92
device_model = R5020-5G
serial_number = 20113056894526
uptime = "0 days, 00:37:26"
system_time = "Sun Jan    1 00:37:09 2017 (NTP not updated)"
ram_usage = "386M Free/448M Total"
#
```

Example 2: Update firmware via tftp

```
# tftpupdate （space+?）
  firmware    New firmware
# tftpupdate firmware （space+?）
  String    Firmware name
# tftpupdate firmware R5020-firmware-sysupgrade-unknown.ruf host 192.168.100.99 //enter a new firmware name
  Downloading
R5020-firmware-s 100% |*******************************|   5018k   0：00：00 ETA
Flashing
```

```
Checking 100%
Decrypting 100%
Flashing 100%
Verifying 100%
Verfify Success
upgrade success                          //update success
# config save_and_apply
OK                                       //save and apply current configuration, make you configuration effect
```

Example 3: Set link-manager

```
# set
   ai                   AI
   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 Port
   sms                  SMS
   ssh                  SSH
   syslog               Syslog
   system               System
   usb                  USB
   user_management      User Management
   web_server           Web Server
   wifi                 WiFi AP

# set link_manager
   primary_link         Primary Link
   backup_link          Backup Link
   backup_mode          Backup Mode
   revert_interval      Revert Interval
   emergency_reboot     Emergency Reboot
   link                 Link Settings
```

```
# set link_management primary_link（space+?）
Enum    Primary Link （wwan1/wwan2/wan/wlan）
# set link_management primary_link wwan1                    //select “wwan1” as primary_link
OK                                                          //setting succeed
set link_manager link 1
   type                 Type
   desc                 Description
   connection_type      Connection Type
   wwan                 WWAN Settings
   static_addr          Static Address Settings
   pppoe                PPPoE Settings
   ping                 Ping Settings
   mtu                  MTU
   dns1_overrided       Overrided Primary DNS
   dns2_overrided       Overrided Secondary DNS
# set link_manager link 1 type wwan1
OK
# set link_manager link 1 wwan
   auto_apn                     Automatic APN Selection
   apn                           APN
   username                      Username
   password                     Password
   dialup_numBer                 Dialup NumBer
   auth_type                Authentication Type
   aggressive_reset              Aggressive Reset
   switch_By_data_allowance   Switch SIM By Data Allowance
   data_allowance                Data Allowance
   Billing_day                  Billing Day
# set link_manager link 1 wwan switch_By_data_allowance true
OK
#
# set link_manager link 1 wwan data_allowance 100           //open cellular switch_by_data_traffic
OK                                                          //setting succeed
# set link_manager link 1 wwan billing_day 1                //setting specifies the day of month for billing
OK                                                          // setting succeed
…
# config save_and_apply
OK                                      // save and apply current configuration, make you configuration effect
```

Example 4: Set LAN IP address

```
# set Ethernet port_setting 2 port_assignment lan0          // Set Table 2 (eth1) to lan0
OK
# config save_and_apply                                     // Make the configuration take effect
OK
```

Example 5: Set LAN IP address

```
# show lan all
network {
id = 1
interface = lan0
ip = 192.168.0.1
netmask = 255.255.255.0
mtu = 1500
dhcp {
        umber = true
        mode = server
        relay_server = “”
        pool_start = 192.168.0.2
        pool_end = 192.168.0.100
        netmask = 255.255.255.0
        gateway = “”
        primary_dns = “”
        secondary_dns = “”
        wins_server = “”
        lease_time = 120
        expert_options = “”
        umbe_enaBle = false
}
vlan_id = 0
}
multi_ip {
id = 1
interface = lan0
ip = 172.16.24.24
netmask = 255.255.0.0
}
#
# set lan
   network        Network Settings
   multi_ip    Multiple IP Address Settings
   vlan            VLAN
# set lan network 1(space+?)
   interface   Interface
   ip              IP Address
   netmask   Netmask
   mtu        MTU
   dhcp       DHCP Settings
# set lan network 1 interface lan0
OK
```

```
# set lan network 1 ip 172.16.24.24                    //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_band11 = false
        lte_band12 = false
        lte_band13 = false
        lte_band14 = false
```

```
        lte_band17 = false
        lte_band18 = false
        lte_band19 = false
        lte_band20 = false
        lte_band21 = false
        lte_band24 = false
        lte_band25 = false
        lte_band26 = false
        lte_band28 = false
        lte_band30 = false
        lte_band31 = false
        lte_band34 = false
        lte_band37 = false
        lte_band38 = false
        lte_band39 = false
        lte_band40 = false
        lte_band41 = false
        nsa_nr5g_band38 = false
        nsa_nr5g_band41 = false
        nsa_nr5g_band77 = false
        nsa_nr5g_band78 = false
        nsa_nr5g_band79 = false
        nr5g_band1 = false
        nr5g_band2 = false
        nr5g_band3 = false
        nr5g_band5 = false
        nr5g_band7 = false
        nr5g_band8 = false
        nr5g_band12 = false
        nr5g_band20 = false
        nr5g_band28 = false
        nr5g_band38 = false
        nr5g_band40 = false
        nr5g_band41 = false
        nr5g_band66 = false
        nr5g_band71 = false
        nr5g_band77 = false
        nr5g_band78 = false
        nr5g_band79 = false
    }
    telit_band_settings {
        gsm_band = 900_and_1800
        wcdma_band = 1900
    }
    debug_enable = true
    verbose_debug_enable = false
```

```
        creg_timeout = 0
}
sim {
        id = 2
        card = sim2
        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_band11 = false
                lte_band12 = false
                lte_band13 = false
                lte_band14 = false
                lte_band17 = false
                lte_band18 = false
                lte_band19 = false
                lte_band20 = false
                lte_band21 = false
                lte_band24 = false
                lte_band25 = false
                lte_band26 = false
                lte_band28 = false
                lte_band30 = false
                lte_band31 = false
                lte_band34 = false
```

```
            lte_band37 = false
            lte_band38 = false
            lte_band39 = false
            lte_band40 = false
            lte_band41 = false
            nsa_nr5g_band38 = false
            nsa_nr5g_band41 = false
            nsa_nr5g_band77 = false
            nsa_nr5g_band78 = false
            nsa_nr5g_band79 = false
            nr5g_band1 = false
            nr5g_band2 = false
            nr5g_band3 = false
            nr5g_band5 = false
            nr5g_band7 = false
            nr5g_band8 = false
            nr5g_band12 = false
            nr5g_band20 = false
            nr5g_band28 = false
            nr5g_band38 = false
            nr5g_band40 = false
            nr5g_band41 = false
            nr5g_band66 = false
            nr5g_band71 = false
            nr5g_band77 = false
            nr5g_band78 = false
            nr5g_band79 = false

        }
        telit_band_settings {
            gsm_band = 900_and_1800
            wcdma_band = 1900
        }
        debug_enable = true
        verbose_debug_enable = false
        creg_timeout = 0
}
# set
    ai                      AI
    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 Port
   sms                    SMS
   ssh                    SSH
   syslog                 Syslog
   system                 System
   usb                    USB
   user_management    User Management
   web_server         Web Server
   wifi                   WiFi AP
# set cellular(space+?)
      sim    SIM Settings
# set cellular sim(space+?)
      Integer    Index (1..2)

# set cellular sim 1(space+?)
   card                       SIM Card
   phone_number               Phone Number
   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
…
# config save_and_apply
OK                                    // save and apply current configuration, make you configuration effect
```

Glossary

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

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

Abbr.	Description
WAN	Wide Area Network
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network

Guangzhou Robustel LTD

Address: 3rd Floor, Building F, Kehui Park, No.95 Daguan Road, Guangzhou, China 510660

Tel: 86-20-29019902

Email: info@robustel.com