User Guide

R1500

Industrial Cellular Iot Gateway

robustOS

Guangzhou Robustel LTD
www.robustel.com

About This Document

This document provides hardware and software information of the Robustel R1500, including introduction, installation, configuration and operation.

Trademarks and Permissions

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

Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner. It is the customer's responsibility to review the advice provided in this document and its suitability for the system. Robustel makes no representations about the specific knowledge of the customer's system or the specific performance of the system. The contents of this document are subject to change without notice due to continued progress in methodology, design and manufacturing. Robustel shall have no liability for any error or damage of any kind resulting from the use of this document.

Technical Support 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 gateway is used in a normal manner with a well-constructed network, the gateway 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 gateway, or for failure of the gateway to transmit or receive such data.

Safety Precautions

General

- The gateway generates radio frequency (RF) power. When using the gateway, care must be taken on safety issues related to RF interference as well as regulations of RF equipment.
- Do not use your gateway in aircraft, hospitals, petrol stations or in places where using cellular products is prohibited.
- Be sure that the gateway will not be interfering with nearby equipment. For example: pacemakers or medical equipment. The antenna of the gateway should be away from computers, office equipment, home appliance, etc.
- An external antenna must be connected to the gateway for proper operation. Only uses approved antenna with the gateway. 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. Gateway may be used at this time.

Using the gateway in Vehicle

- Check for any regulation or law authorizing the use of cellular devices in vehicle in your country before installing the gateway.
- The driver or operator of any vehicle should not operate the gateway while driving.
- Install the gateway by qualified personnel. Consult your vehicle distributor for any possible interference of electronic parts by the gateway.
- The gateway 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 gateway is powered by the vehicle’s main battery. The battery may be drained after extended period.

Protecting Your Gateway

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

- Do not expose the gateway 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 gateway. There is no user serviceable part inside and the warranty would be void.
- Do not drop, hit or shake the gateway. Do not use the gateway under extreme vibrating conditions.
- Do not pull the antenna or power supply cable. Attach/detach by holding the connector.
- Connect the gateway 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

<table>
<tr><td rowspan="2">Name of the Part</td><td colspan="10">Hazardous Substances</td></tr>
<tr><td>(Pb)</td><td>(Hg)</td><td>(Cd)</td><td>(Cr(VI))</td><td>(PBB)</td><td>(PBDE)</td><td>(DEHP)</td><td>(BBP)</td><td>(DBP)</td><td>(DIBP)</td></tr>
<tr><td>Metal parts</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td></tr>
<tr><td>Circuit modules</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td></tr>
<tr><td>Cables and cable assemblies</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td></tr>
<tr><td>Plastic and polymeric parts</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td><td>o</td></tr>
<tr><td colspan="11">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 <i>might exceed</i> the limit requirement in RoHS2.0.</td></tr>
</table>

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
29 Apr., 2019	1.0.0	v.1.0.0	Initial release
10 Jun., 2019	1.0.0	v.1.0.1	• Revised the status of UER in chapter 2.2 LED Indicators. • Revised the screenshot of RobustOS main interface about the device version number in chapter 3.4 and 4.1.1. • Revised the Screenshot of the Cellular frequency in chapter 4.2.4. • Revised the screenshot of firewall function and added the Enable VPN NAT Traversal function and related description in chapter 4.3.2. • Revised the screenshot of IPsec_General and add Optimize DH Exponent Size function and related description in chapter 4.4.1. • Revised the description of input power in chapter 1.1.1. • Revised the description of Power consumption in chapter 1.1.3. • Revised the Product name.
12 Sep., 2019	1.0.0	v.1.0.2	• Revised the Front panel interface • Revised the Regulatory and Type Approval Information

Contents

Chapter 1 Product Overview

1.1 Key Features

The Robustel Industrial Cellular Iot gateway R1500 supports GSM/GPRS/EDGE 2G networks, 3G networks such as WCDMA, HSPA+ 3.5G and LTE 4G networks, providing high-speed wireless network bandwidth for devices over wireless connections, and it has dual SIM backups to ensure a stable connection to the wireless network.

The R1500 uses Robustel self-developed operating system RobustOS. RobustOS is developed on Linux-based systems and is suitable for most of router devices of Robustel. In addition to basic network functions and protocols, the system gives customers a more customized, more convenient and more practical customization experience. At the same time, Robustel will provide SDKs for partners and customers, allowing users to develop their own functions of using C, Python or Java software languages. In addition, we will provide a wealth of App applications running on RobustOS to meet the needs of fragmented IoT applications.

Robustel is one of the world's leading manufacturers of industrial quality solutions for the IoT and M2M market. Robustel's portfolio of award-winning solutions are comprised of: Wireless Modems, Routers, Gateways, EDGE Computing, Cloud Software and End-to-End IoT solutions.

Founded in 2010 in Guangzhou, China – Robustel has been concentrating on producing the highest quality IoT products possible. As a supplier of wireless IoT hardware Robustel works with over 50 distribution partners servicing more than 120 countries and maintains a dedicated local presence in: Germany, Australia, Japan, UK, US, the Netherlands and Hong Kong. Robustel can respond quickly to users' needs, provide fast, professional services and more targeted R&D and technical support to meet the needs of user customization and individualization. Up to now, Robustel's products and services have been radiated to more than 100 countries and regions around the world. Products are widely used in smart cities, power, oil and gas, finance, environmental protection, security, industrial automation, medical and other fields. The company's business continues to be healthy, stable and rapid growth. After years of continuous efforts, Robustel has become a pioneer in the Internet of Things industry.

- RobustOS + SDK + App
- Supports multiple VPNs such as IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN
- Supports dual card link backup and ICMP detection
- Supports SMS, Email, SNMP Trap and RobustLink
- Event alarm
- Supports Modbus RTU to TCP、Modbus Master
- Supports TCP client/server, UDP, virtual serial port

- Supports DHCP server
- Supports IP Pass-through
- Supports RobustVPN cloud platform, providing simple and secure remote access for industrial equipment such as PLC
- Supports RobustLink M2M centralized management platform to monitor device network status and statistics device traffic in real time
- Supports for firmware upgrades for Web, CLI, USB, SMS and RobustLink
- Robust industrial design (9-36V DC input voltage for horizontal desktop placement, Din rail mounting)

1.2 Package Contents

Before installing your R1500, verify the kit contents as following.

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

- 1 x Robustel Cellular lot gateway R1500

- Terminal block (3.5mm, for power connector)

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

robustel

产品快速指南

感谢您选择鲁邦通！

安装快捷，配置简单

玩转鲁邦通网关，只需四步！

1 材料准备

使用前请确认您的包装设备是否完整。如有任何缺失或损坏，请及时联系您的区域销售代表。

标配设备

选购配件

2 安装硬件

网关连接到电源通电，RUN灯或PWR灯被点亮；再用一根DB9串口线或USB转换线将网关连接到一台电脑上。

3 连接软件配置工具

在电脑上打开网关的软件配置工具（工具通常被命名为"Configurator"），选择正确的COM口，点击工具上的"√"按钮。

4 配置网关

当电脑屏幕上弹出"Operation Succeed!"窗口，恭喜您！软件配置工具已成功连接上网关！赶紧开始配置网关吧。

相关下载

登录以下网址，获取更多产品文档或工具。
www.robustel.com.cn/support/download

技术支持联系方式

座机：020-29019902
邮箱：support@robustel.com

意见反馈

对本指南有任何建议或意见，请直接发送邮件至support@robustel.com，以助我们进一步完善，感谢您的支持。

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

Optional Accessories (sold separately)

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

Stubby antenna 1

Magnet antenna 2

- 35 mm DIN rail mounting kit

- 1x serial cable

- Cable

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

1.3 Specifications

Cellular Interface

- Number of antennas: 2 (MAIN + AUX)
- Connector: SMA, female
- SIM slot: 2 (3.0 V & 1.8 V)
- Standards: GSM/WCDMA/FDD LTE/TDD LTE

Ethernet Interface

- Number of ports: 1 x 10/100 ports

Serial Interface

- Number of ports: 2 x RS-232

- Connector: DB9
- Signal: TxD、RxD、GND、CTS、RTS、DSR、DTR
- Baud rate: 300 bps to 115200 bps

Others

- LED indicators: 1 x RUN, 1 x MDM, 1 x USR, 3 x RSSI
- Built-in: RTC, Watchdog, Timer

Software (Basic features of RobustOS)

- Network protocols: ：PPP、PPPoE、TCP、UDP、DHCP、ICMP、NAT、HTTP、HTTPs、DNS、ARP、NTP、SMTP、Telnet、SSH2、DDNS, etc.
- VPN tunnel: IPsec, OpenVPN, GRE
- Management: Web, CLI, SMS
- Serial port: Transparent, TCP Client/Server, UDP, Modbus RTU Gateway

App Center (Available Apps for RobustOS)

- Apps*: Language, RobustLink

**Request on demand. For more Apps please visit www.robustel.com.*

Power Supply and Consumption

- Connector: 2-pin 3.5 mm female socket
- Input voltage: 9 to 36V DC
- Power consumption: Idle: 80 mA@12 V
  Data link: 450 mA (peak) @12 V

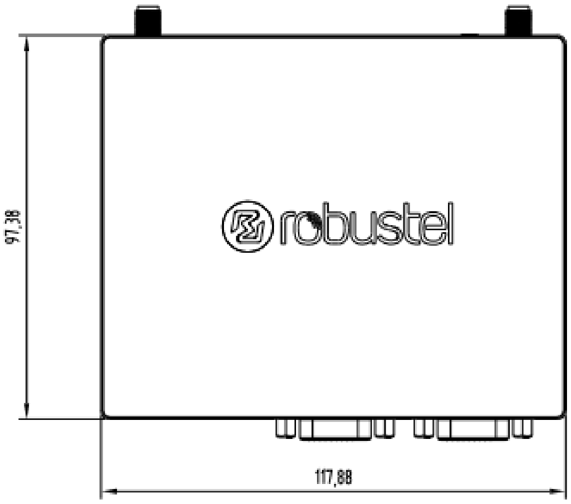
Physical Characteristics

- Ingress protection: IP30
- Housing & Weight: Plastic
- Dimensions: 118 x 97.5 x 28.5 mm
- Installations: Desktop, and 35 mm DIN rail mounting
  (DIN rail mounting requires additional installation accessories)

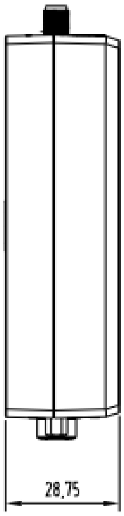
Approvals

- Environmental: RoHS2.0, WEEE

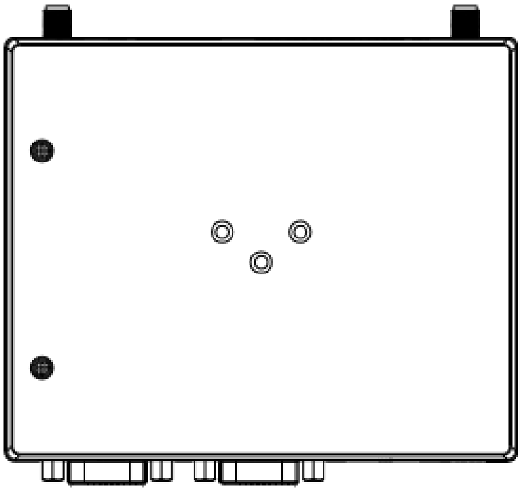
1.4 Dimensions



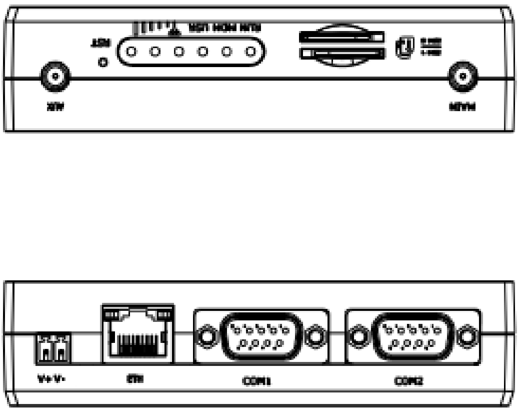
Front view



side view



Rear view



Top & Bottom view

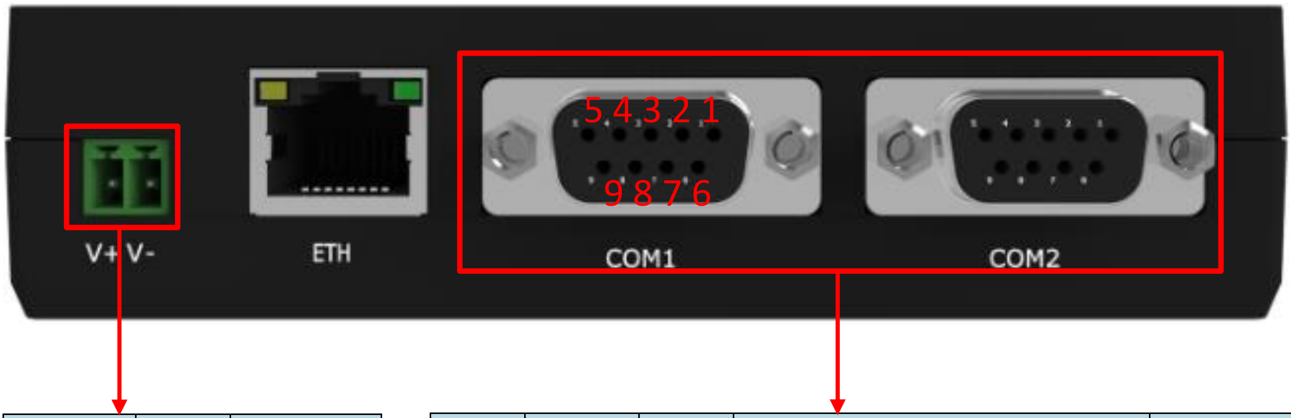
1.5 Ordering Information

Model	R1500-4L
Router Type	LTE Gataway
Air Interface	GSM/WCDMA/FDD LTE/TDD LTE
Frequency Bands	LTE
4G*	
3G	WCDMA/HSPA/DC-HSPA+
2G	GPRS/EDGE
Operating Environment	-40 to +75 °C 5 to 95% RH

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

Chapter 2 Hardware Installation

2.1 Front panel interface

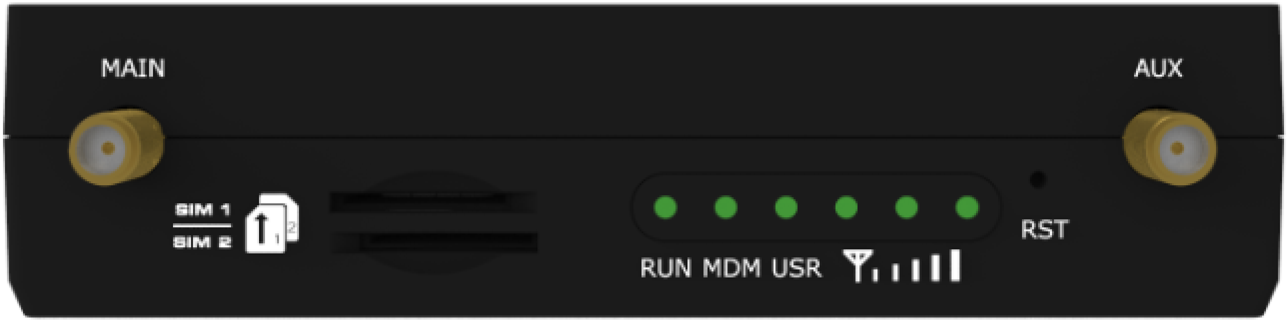


Name	Mark	Function
Power interface	V+	Power input positive, 9-36VDC
Power interface	V-	Power input negative

Label	Name	Mark	Function	Direction
1	--	--		
2	RXD		Receive Data, Signal input	R1500 ←Device
3	TXD		Transmit Data, Signal output	R1500 →Device
4	DTR		Data Terminal Ready, Signal output	R1500 →Device
4	GND		System Ground	--
6	DSR		Data Set Ready, Signal input	R1500 ←Device
7	RTS		Request to Send, Signal output	R1500 →Device
8	CTS		Clear to Send, Signal input	R1500 ←Device
9	--	--	--	--

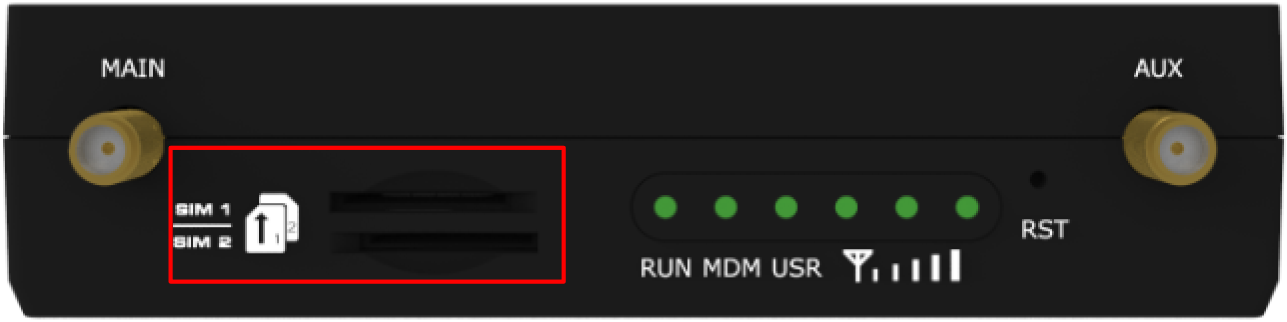
Notes： Pin definitions for COM1 and COM2 are the same.

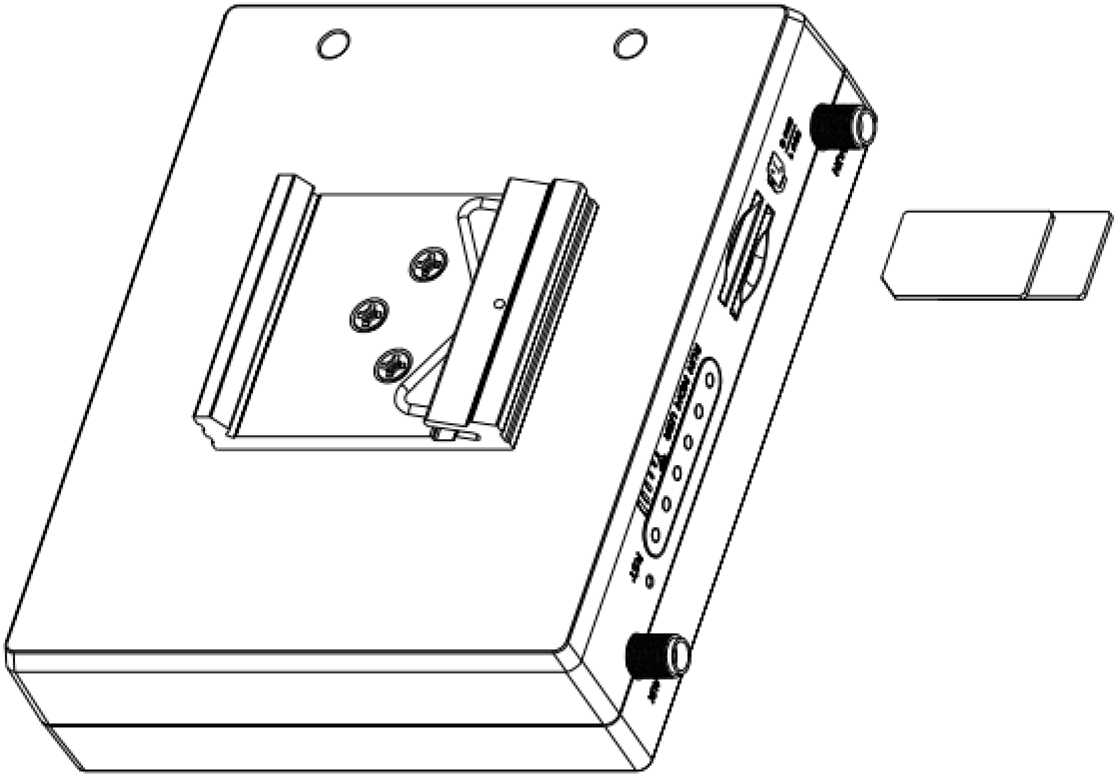
2.2 LED Indicators



Name	Color	Status	Description
RUN	Green	On, solid	Power on
	Green	Fast blinking (2Hz)	System initializing
	Green	On, blinking (1Hz)	Initialization completed, device operating normally
MDM	Green	On, solid	Link connection is working
	Green	On, blinking	Link connection is communicating
	Green	Off	Link connection is not working
USR	Green	On, blinking	Backup card is being used
	Green	On, solid	Main card is being used
📶	None	All off (three lights)	CSQ value 0 or 99, not registered on the network
	Green	On, solid(one light)	CSQ 1-10, poor signal
	Green	On, solid(two light)	CSQ 11-20, normal signal
	Green	On, solid(three light)	CSQ 21-31, good signal

2.3 Insert or Remove SIM Card





Please confirm before inserting the SIM card. When the SIM card is turned on and the device is configured without the correct PIN, the SIM card is unavailable.

- **Insert SIM card**

1. Make sure gateway is powered off.
2. To insert SIM card, press the card with finger until you hear a click

- **Remove SIM card**

1. Make sure gateway is powered off.
2. To remove SIM card, press the card with finger until it pops out and then take out the card.

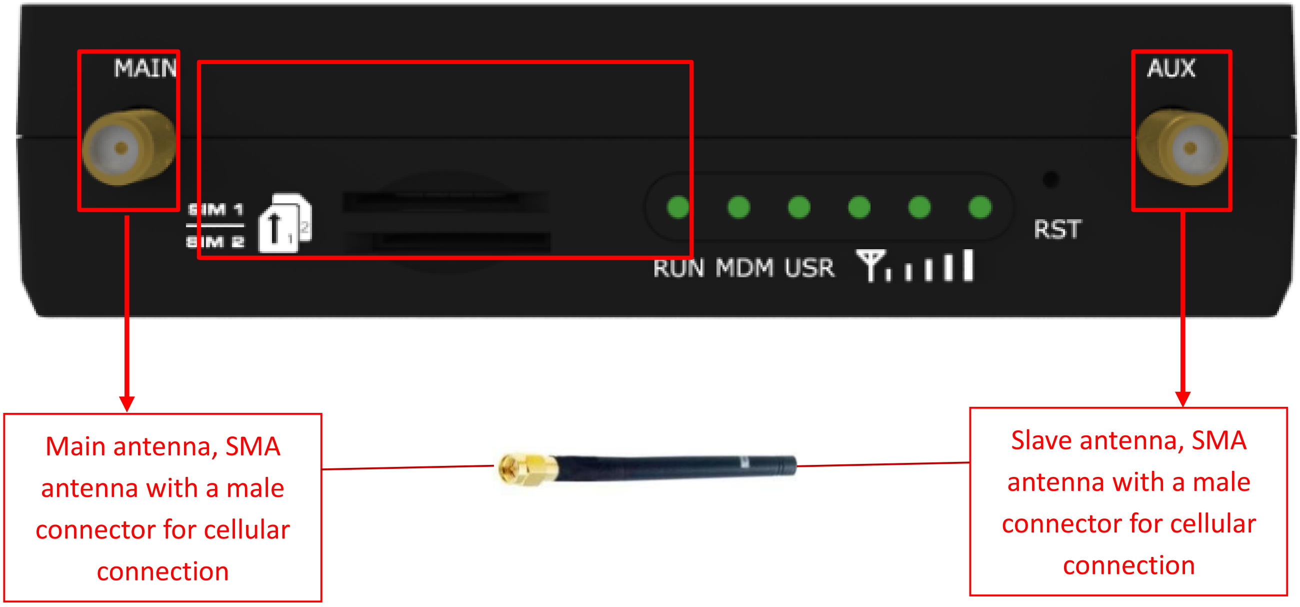
Note:

1. Recommended torque for inserting is 0.5 N.m, and the maximum allowed is 0.7 N.m.
2. Use the specific M2M SIM card when the device is working in extreme temperature, because the regular card for long-time working in harsh environment will be disconnected frequently.
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 gateway is powered off before inserting or removing the card.

2.4 Attach External Antenna (SMA Type)

Attach an external SMA antenna to the gateway'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.

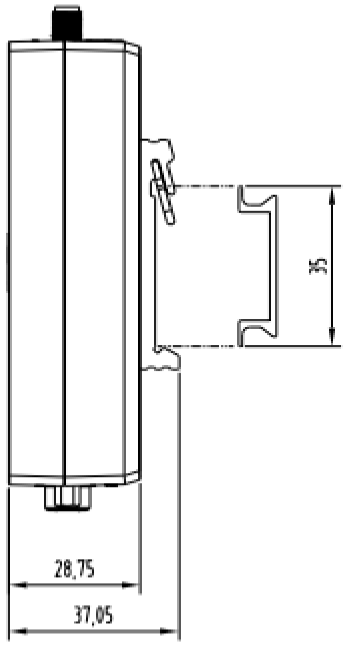

MAIN
AUX
SIM 1
SIM 2
RUN MDM USR
RST
Main antenna, SMA antenna with a male connector for cellular connection
Slave antenna, SMA antenna with a male connector for cellular connection

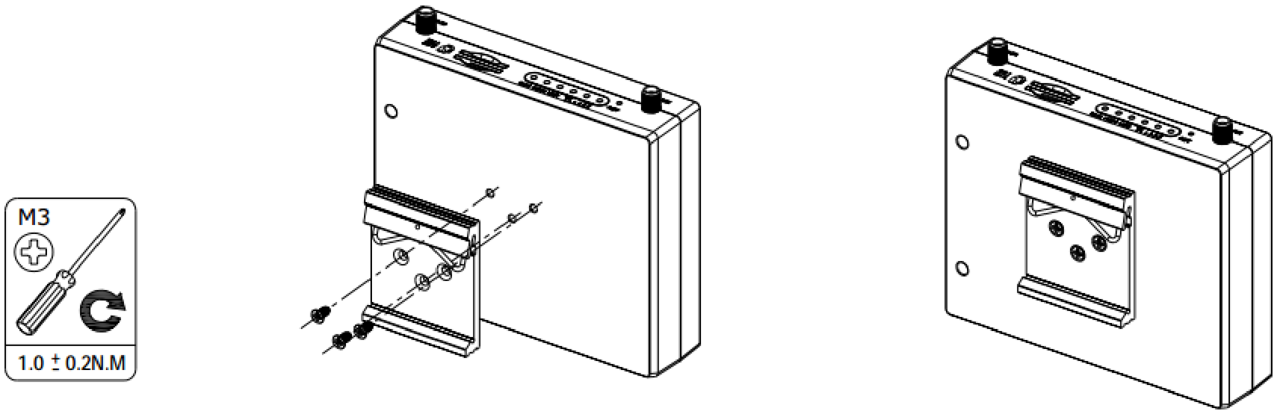
2.5 Mount the Gateway

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

Installation method

- DIN rail mounting (measured in mm)



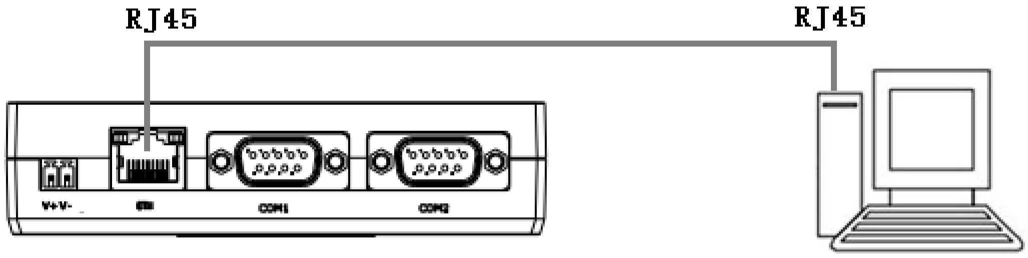


Use 3 pcs of ST3*8 flat head self-tapping Phillips screws to fix the DIN rail to the gateway, and then hang the DIN rail on the mounting bracket. It is necessary to choose a standard bracket.

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

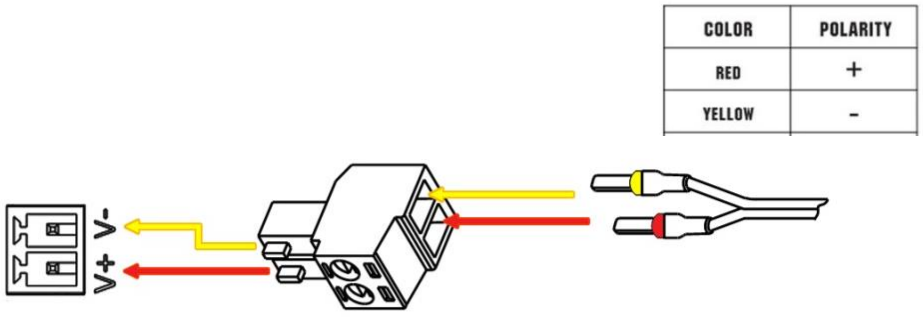
2.6 Connect the Gateway to a Computer

Connect a Category 5 cable to the gateway
network port (ETH) to an external controller or computer's network port



2.7 Power Supply

Power connection diagram



COLOR	POLARITY
RED	+
YELLOW	-

R1500 supports reverse polarity protection, but always refers to the figure above to connect the power adapter correctly. There are two cables associated with the power adapter. Following to the color of the head, connect the cable marked red to the positive pole through a terminal block, and connect the yellow one to the negative in the same way.

Note: The range of power voltage is 9 to 36V DC.

Chapter 3 Initial Configuration

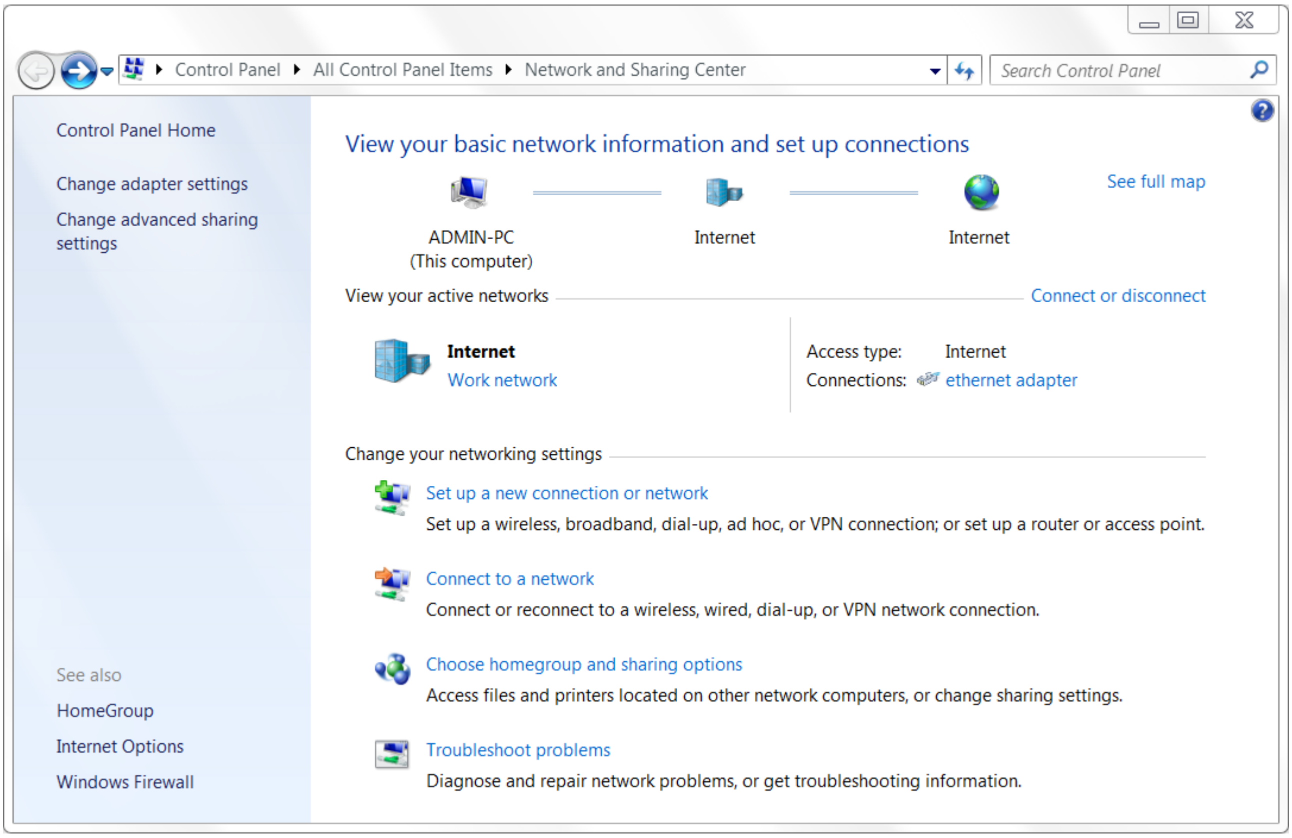
The DTU supports webpage configuration. The supported browsers are IE8.0 or above, Google Chrome, Firefox, etc. The supported operating system is Linux， Mac OS， Windows 98/NT/2000/XP/Me/Vista/7/8 and so on. For R1500, There are several ways to connect to the gateway, either through an external repeater/hub connection or directly to a computer. When the gateway is directly connected to the Ethernet port of the computer, if the router acts as a DHCP server, the computer can obtain the IP directly from the router; the computer can also set the static IP with the router in the same network segment, so that the computer and the router constitute 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 browser to enter the WEB login interface of the router.

3.1 Configure the PC

On the PC side, there are two ways to configure its IP address; one is to automatically obtain an IP address on the local connection of the PC, and the other is to configure a static IP address on the same subnet as the router on the local connection of the PC.

This part takes **the Windows 7** as the example; the configuration of Windows system is similar.

1. Click “Start > Control Panel > Network and sharing center” and double-click Local Area Connection in the window that opens.



View your basic network information and set up connections

View your active networks

Connect or disconnect

Internet
Work network

Access type: Internet
Connections: ethernet adapter

Change your networking settings

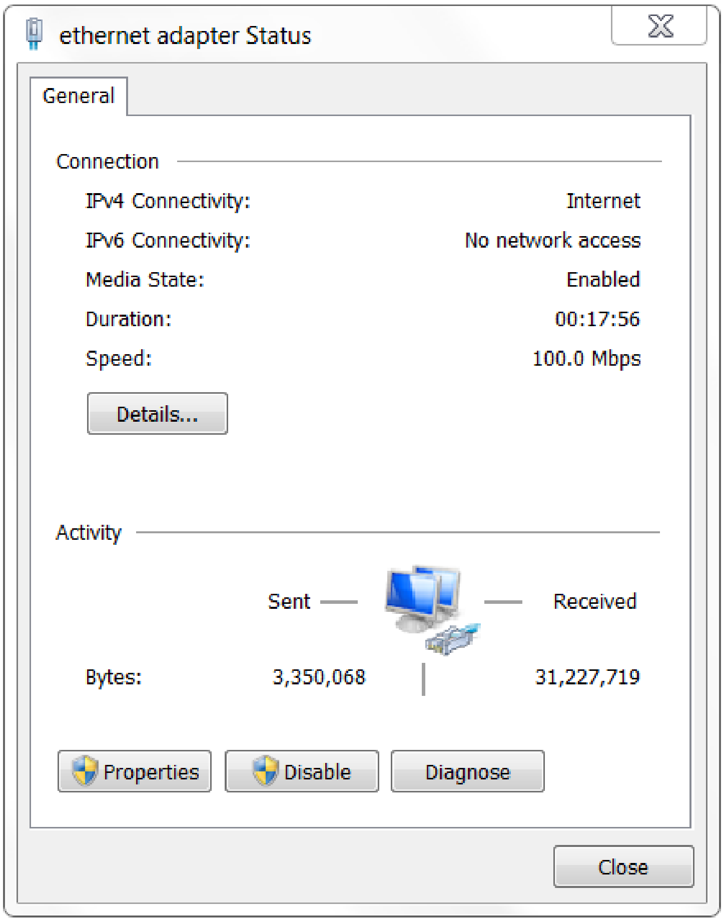
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

2. In the Local Area Connection Status window, click Properties.



ethernet adapter Status

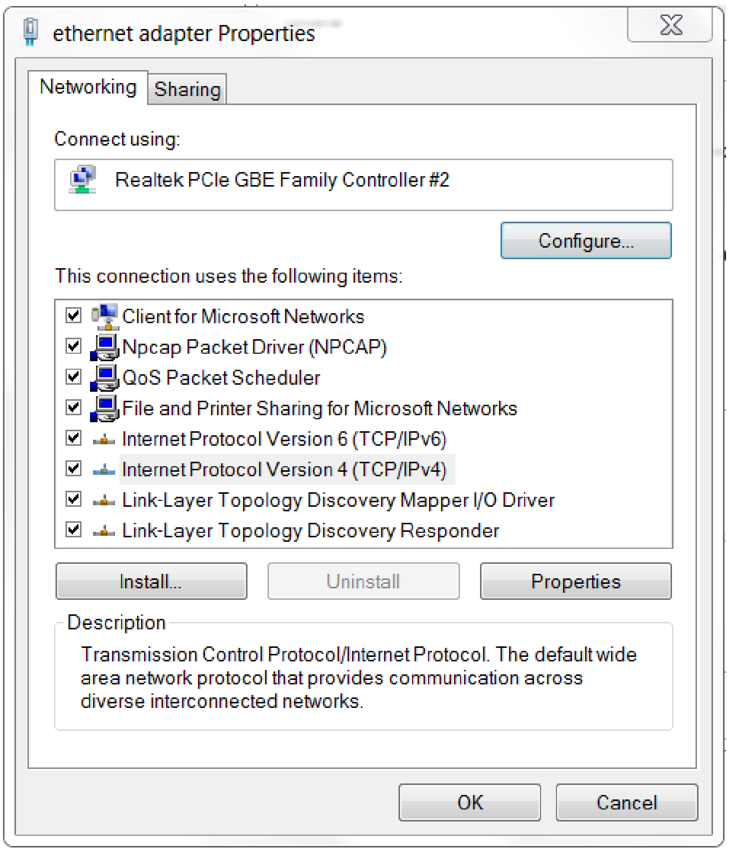
Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	00:17:56
Speed:	100.0 Mbps

Activity

	Sent	Received
Bytes:	3,350,068	31,227,719

3. Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties".



ethernet adapter Properties

Connect using:

Realtek PCIe GBE Family Controller #2

This connection uses the following items:

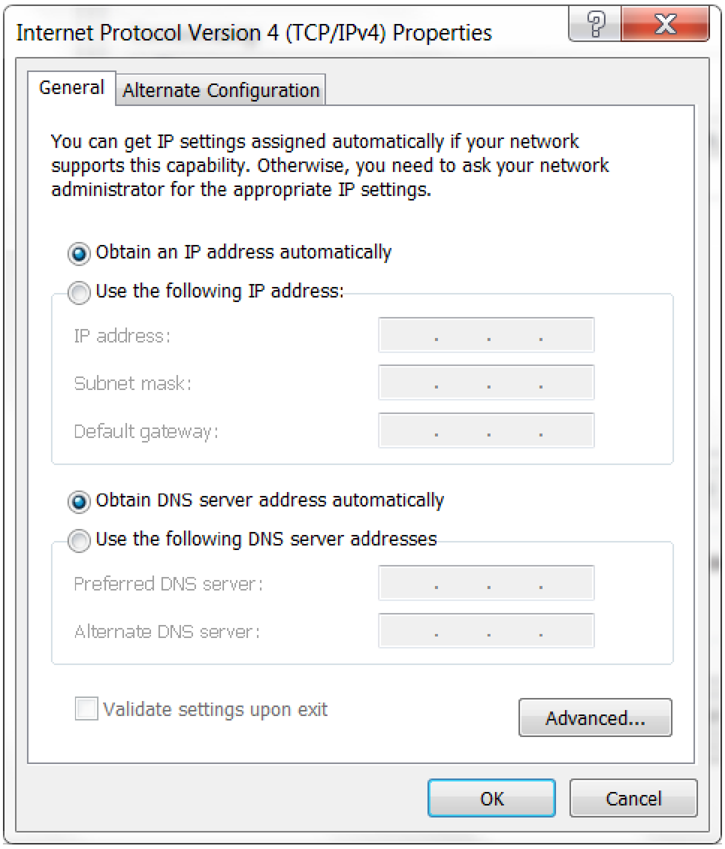
- ☑ Client for Microsoft Networks
- ☑ Npcap Packet Driver (NPCAP)
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

4. There are two ways to configure the IP address of the PC:

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

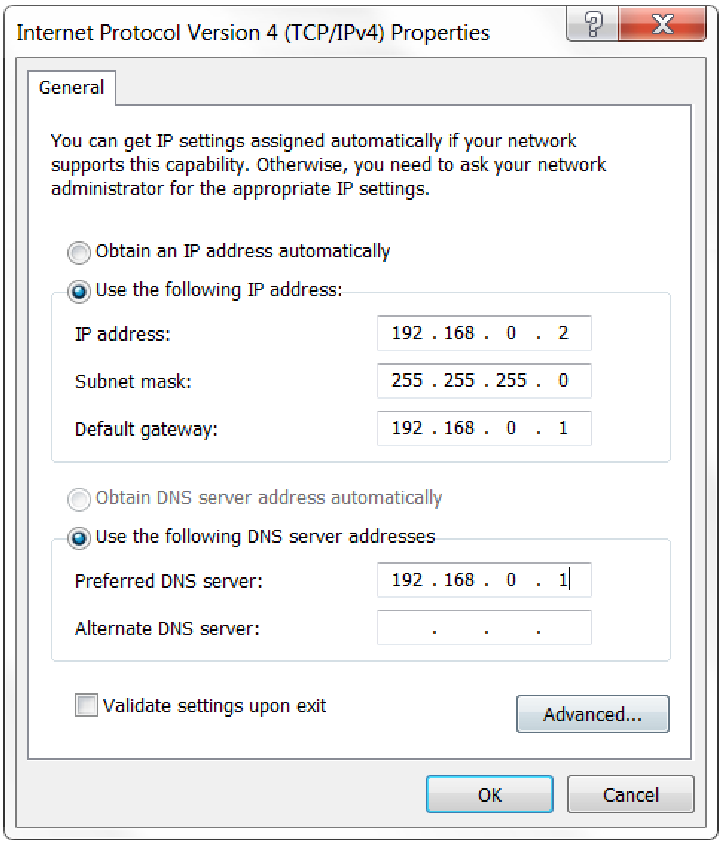
○ Use the following DNS server addresses

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses

Preferred DNS server: 192 . 168 . 0 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

5. Click OK to complete the configuration.

3.2 Factory Default Settings

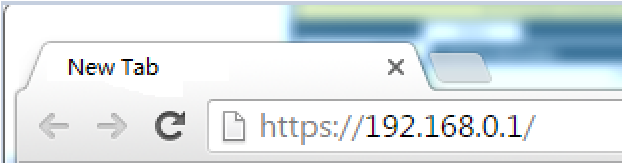
Before configuring your gateway, you need to know the following default settings.

Item	Description
Username	admin
Password	admin
ETH0	192.168.0.1/255.255.255.0, LAN mode
DHCP server	Open

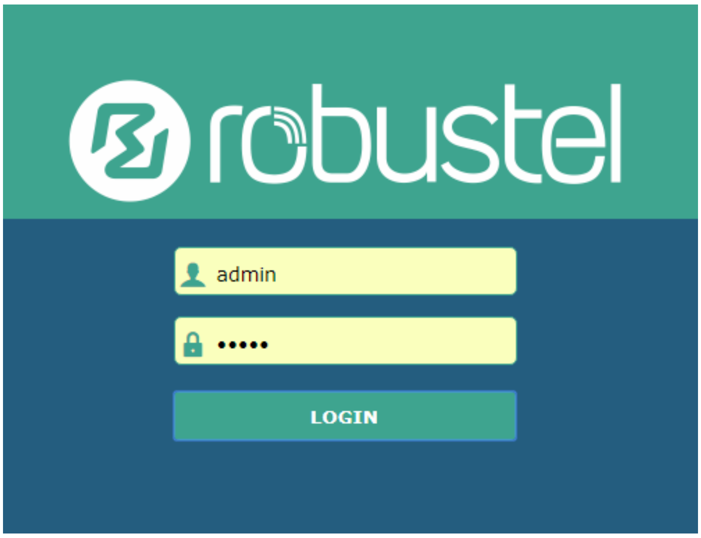
3.3 Login the Gateway

To log in to the management page and view the configuration status of your gateway, 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 gateway into the address bar and press enter. The default IP address of the gateway is 192.168.0.1, though the actual address may vary.
   Note: If a SIM card with a public IP address is inserted in the gateway, enter this corresponding public IP address in the browser's address bar to access the gateway wirelessly.

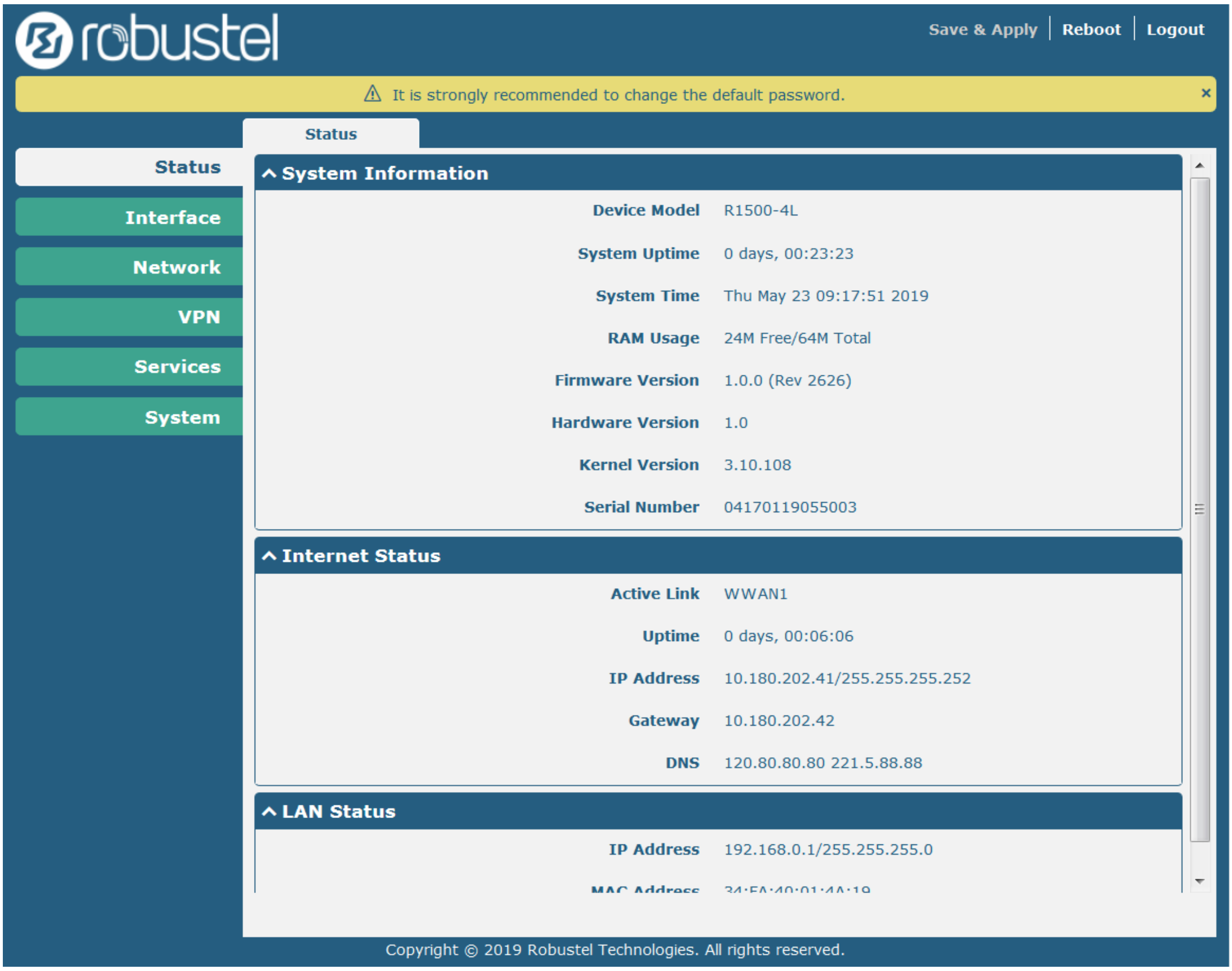


3. In the login page, enter the username and password, choose language and then click **LOGIN**. The default username and password are "admin".
   Note: If enter the wrong username or password over six times, the login web will be locked for 5 minutes.



3.4 Control Panel

After logging in, the home page of the R1500's web interface is displayed as below:



⚠ It is strongly recommended to change the default password. ×

System Information

Device Model R1500-4L
System Uptime 0 days, 00:23:23
System Time Thu May 23 09:17:51 2019
RAM Usage 24M Free/64M Total
Firmware Version 1.0.0 (Rev 2626)
Hardware Version 1.0
Kernel Version 3.10.108
Serial Number 04170119055003

Internet Status

Active Link WWAN1
Uptime 0 days, 00:06:06
IP Address 10.180.202.41/255.255.255.252
Gateway 10.180.202.42
DNS 120.80.80.80 221.5.88.88

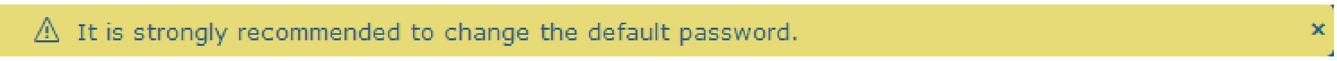
LAN Status

IP Address 192.168.0.1/255.255.255.0
MAC Address 34:FA:40:01:4A:19

Copyright © 2019 Robustel Technologies. All rights reserved.

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 gateway, the page will pop up the following tab



⚠ It is strongly recommended to change the default password. ×

Click × 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 **System > User Management**.

Control Panel		
Item	**Description**	**Button**
Save & Apply	Click to save the current configuration into gateway's flash and apply the modification on every configuration page, to make the modification taking effect.	Save & Apply
Reboot	Click to restart the gateway.	Reboot
Logout	Click to log the current user out safely.	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:

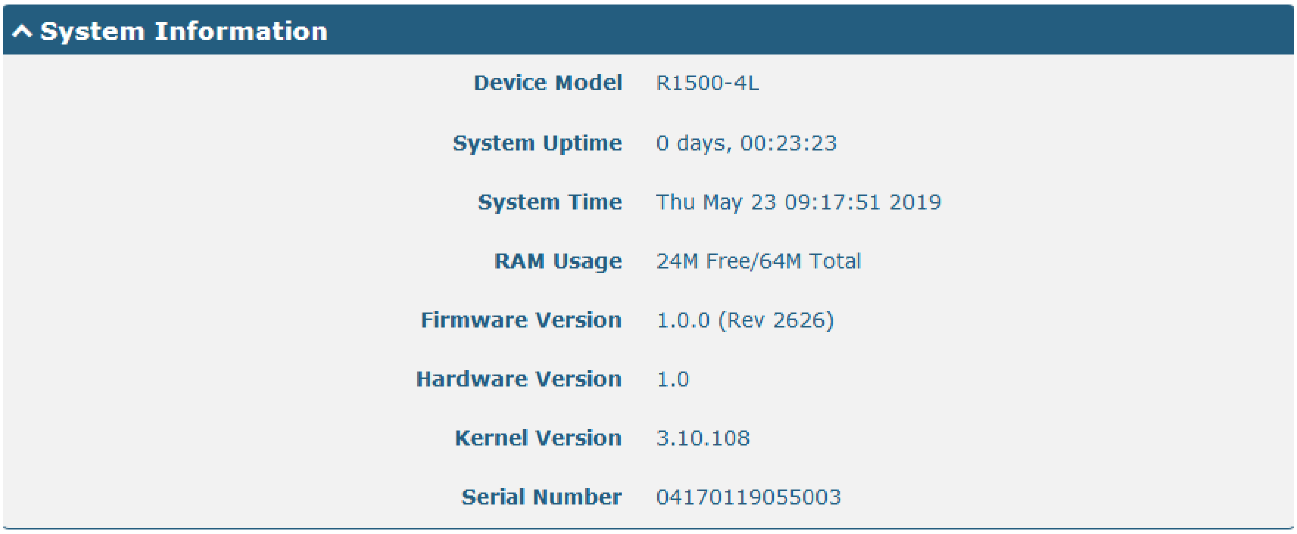
1. Modify in one page;
2. Click Submit under this page;
3. Modify in another page;
4. Click Submit under this page;
5. Complete all modification;
6. Click Save & Apply.

Chapter 4 Gateway Configuration

4.1 System

4.1.1 System Information

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



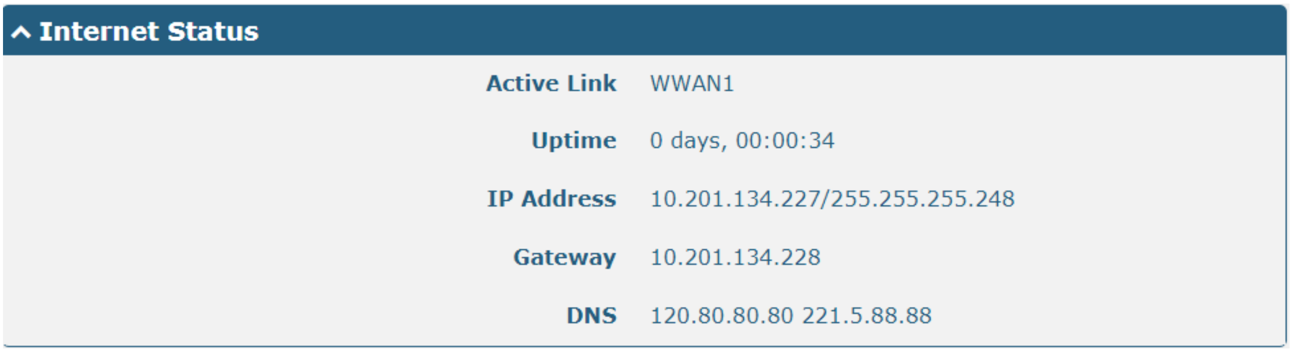
^ System Information

Device Model	R1500-4L
System Uptime	0 days, 00:23:23
System Time	Thu May 23 09:17:51 2019
RAM Usage	24M Free/64M Total
Firmware Version	1.0.0 (Rev 2626)
Hardware Version	1.0
Kernel Version	3.10.108
Serial Number	04170119055003

System Information	
Item	**Description**
Device Model	Show the model name of your device.
System Uptime	Show the current amount of time the gateway 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 gateway.
Hardware Version	Show the current hardware version.
Kernel Version	Show the current kernel version.
Serial Number	Show the serial number of your device. From the serial number, you can get information about the router's factory time and so on.

4.1.2 Cellular Status

This section shows the cellular status information of the router.



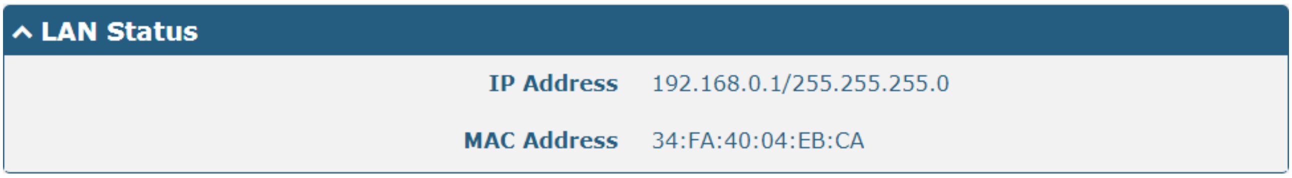
Internet Status

Active Link	WWAN1
Uptime	0 days, 00:00:34
IP Address	10.201.134.227/255.255.255.248
Gateway	10.201.134.228
DNS	120.80.80.80 221.5.88.88

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

4.1.3 Internet Status

This section shows the Internet status information of the router.



LAN Status

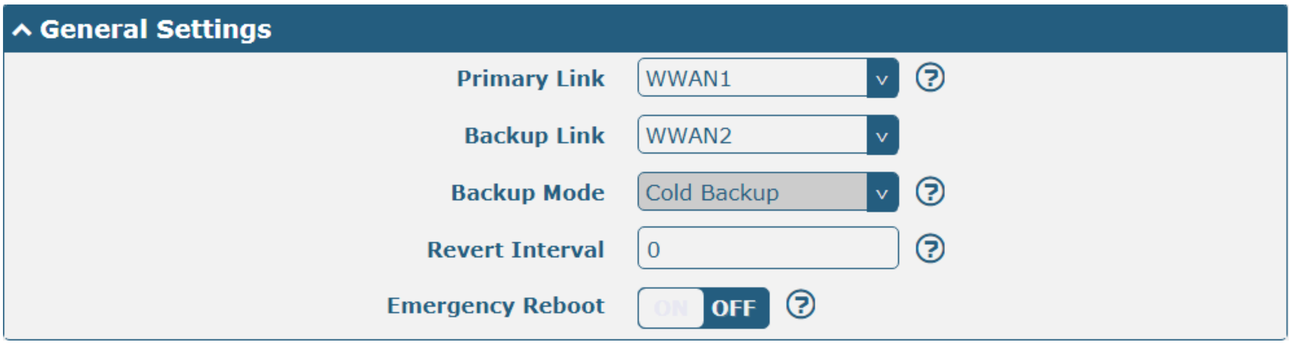
IP Address	192.168.0.1/255.255.255.0
MAC Address	34:FA:40:04:EB:CA

Internet Status	
Item	**Description**
IP Address	Show the IP address and mask of the router on the current LAN.
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

Primary Link: WWAN1

Backup Link: WWAN2

Backup Mode: Cold Backup

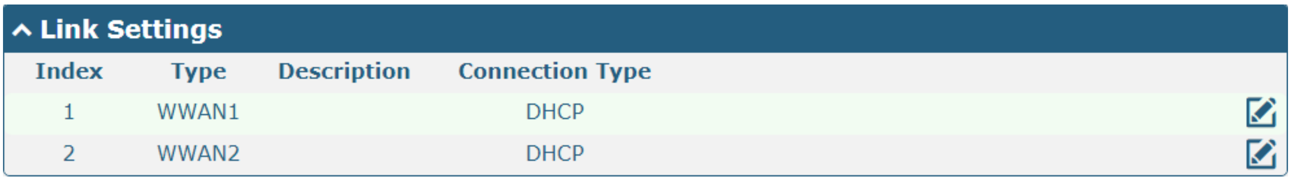
Revert Interval: 0

Emergency Reboot: ON OFF

General Settings @ Link Manager		
Item	**Description**	**Default**
Primary Link	Select from “WWAN1” or “WWAN2”. • WWAN1: Select to make SIM1 as the primary wireless link • WWAN2: Select to make SIM2 as the primary wireless link	WWAN1
Backup Link	Select from “WWAN1”, “WWAN2”, or “None”. • WWAN1: Select to make SIM1 as backup wireless link • WWAN2: Select to make SIM2 as backup wireless link • None: Do not select any backup link	WWAN2
Backup Mode	Can only select from “Cold Backup”. • Cold Backup: The inactive link is offline on standby	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.	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 gateway always online. The Ping detection increases the reliability and also costs the data traffic.

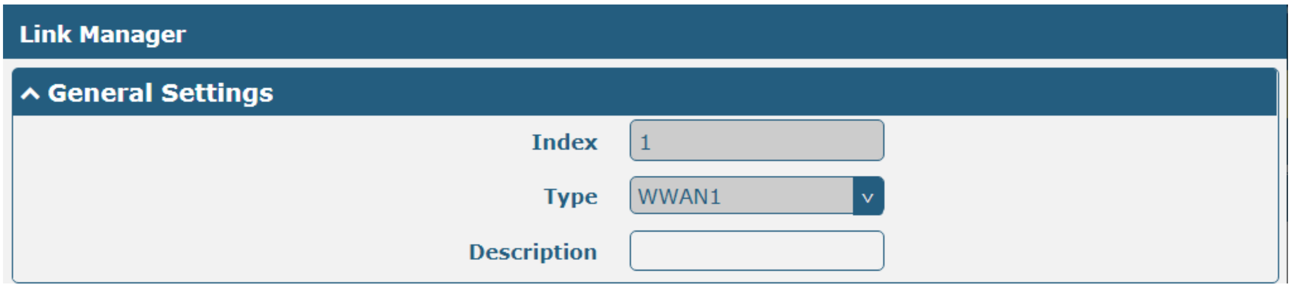


^ Link Settings

Index	Type	Description	Connection Type
1	WWAN1		DHCP
2	WWAN2		DHCP

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

WWAN1/WWAN2

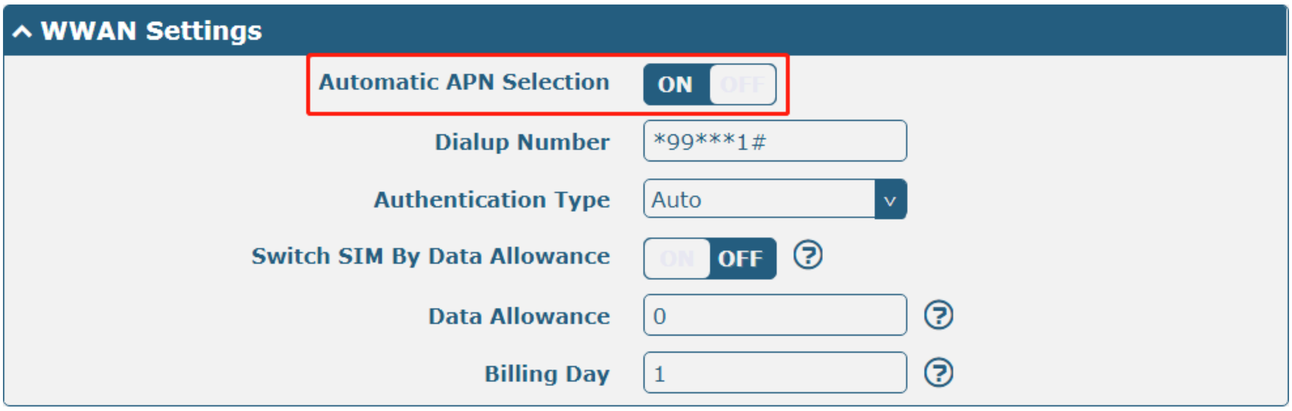


Link Manager

^ General Settings

Index	1
Type	WWAN1
Description	

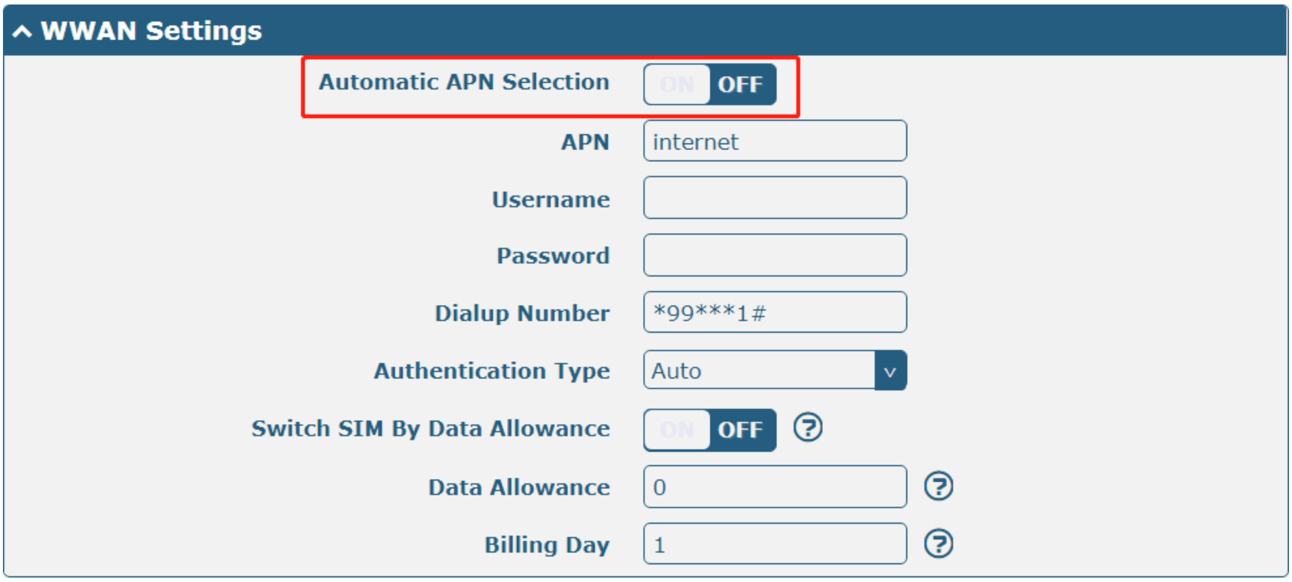
The window is displayed as below when enabling the "Automatic APN Selection" option.



^ WWAN Settings

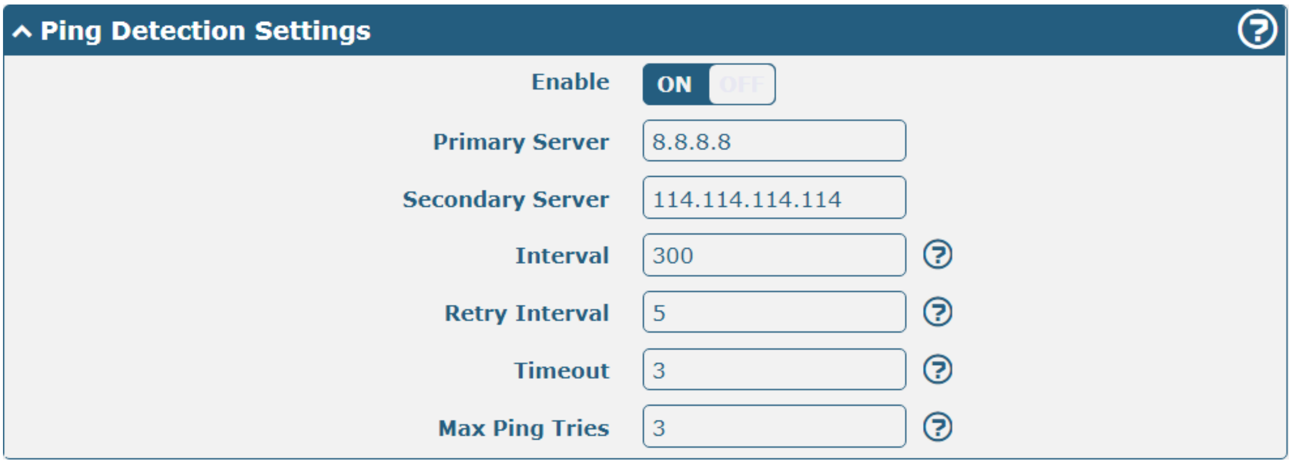
Automatic APN Selection	ON
Dialup Number	*99***1#
Authentication Type	Auto
Switch SIM By Data Allowance	OFF
Data Allowance	0
Billing Day	1

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



^ WWAN Settings

Automatic APN Selection	OFF
APN	internet
Username	
Password	
Dialup Number	*99***1#
Authentication Type	Auto
Switch SIM By Data Allowance	OFF
Data Allowance	0
Billing Day	1



Enable: ON

Primary Server: 8.8.8.8

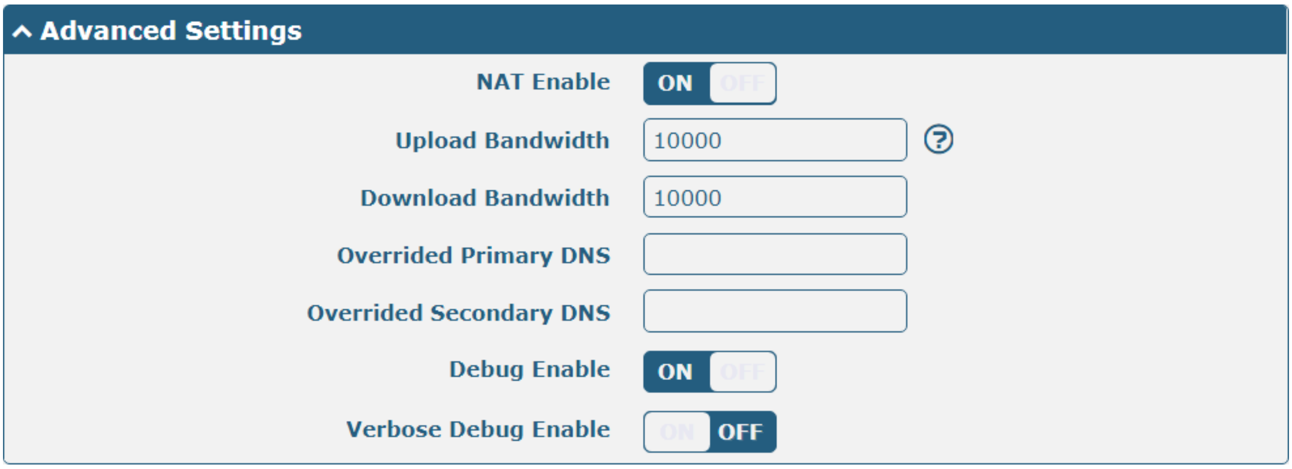
Secondary Server: 114.114.114.114

Interval: 300

Retry Interval: 5

Timeout: 3

Max Ping Tries: 3



NAT Enable: ON

Upload Bandwidth: 10000

Download Bandwidth: 10000

Overrided Primary DNS:

Overrided Secondary DNS:

Debug Enable: ON

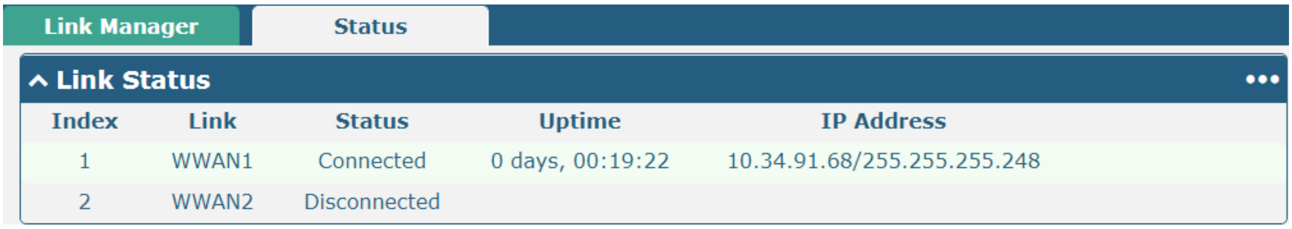
Verbose Debug Enable: OFF

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		
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

Link Settings (WWAN)		
Item	**Description**	**Default**
Data Allowance	Set the monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will be displayed in **Interface > Link Manager > Status > WWAN Data Usage Statistics**. 0 means disable data traffic record.	0
Billing Day	Specify the monthly billing day. The data traffic statistics will be recalculated from that day.	1
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the gateway.	ON
Primary Server	Gateway will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Gateway 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 gateway 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		
Enable NAT	Click the toggle button to enable/disable the NAT feature. NAT is Network Address Translation, which is network address translation.	ON
Upload bandwidth	Set the upload bandwidth for QoS in kbps.	10000
Download bandwidth	Set the download bandwidth for QoS 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

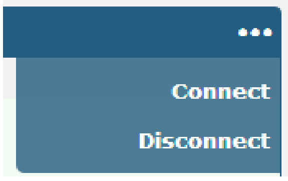
Status

This page allows you to view the status of link connection.

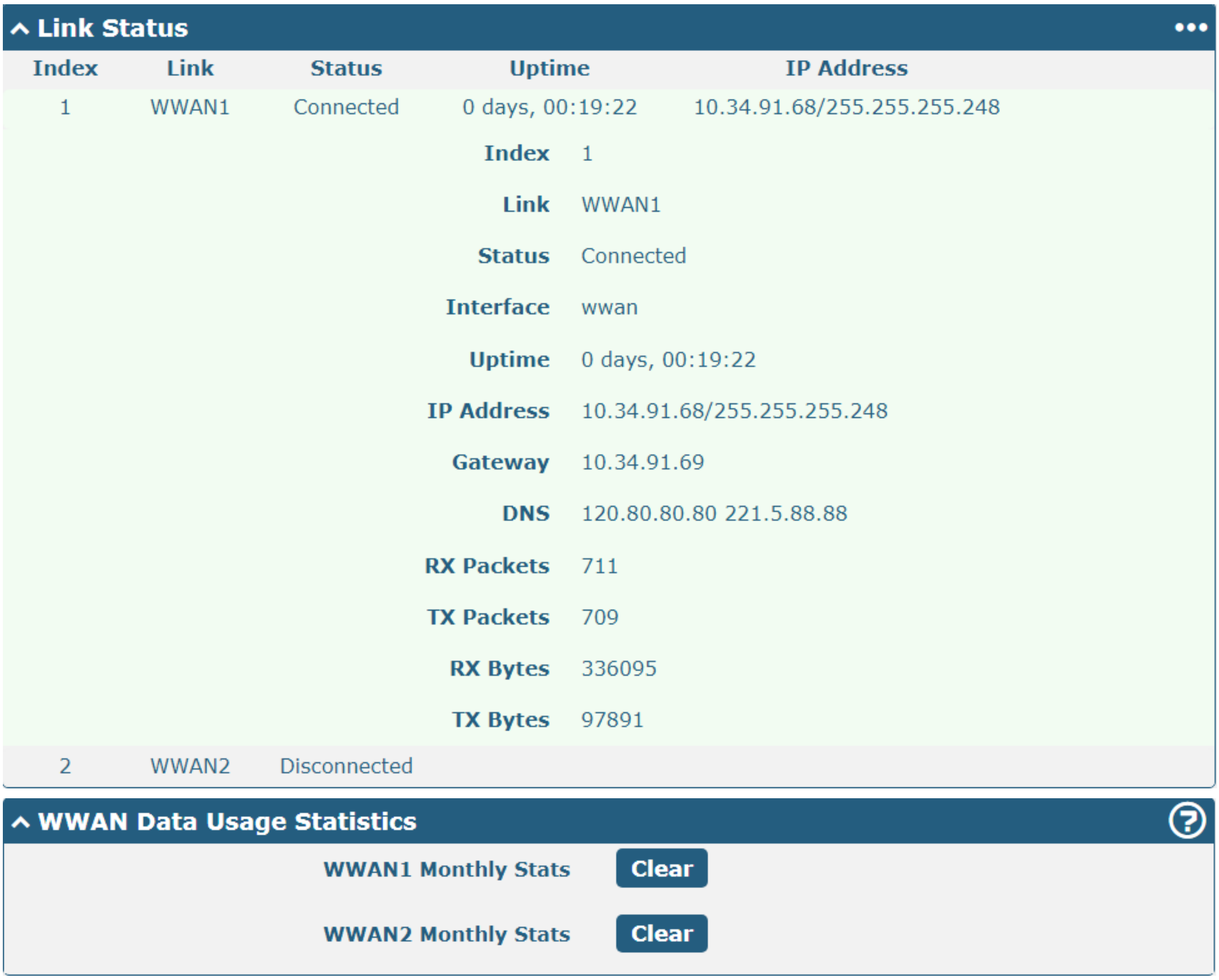


Index	Link	Status	Uptime	IP Address
1	WWAN1	Connected	0 days, 00:19:22	10.34.91.68/255.255.255.248
2	WWAN2	Disconnected		

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.



Index	Link	Status	Uptime	IP Address
1	WWAN1	Connected	0 days, 00:19:22	10.34.91.68/255.255.255.248

Index	1
Link	WWAN1
Status	Connected
Interface	wwan
Uptime	0 days, 00:19:22
IP Address	10.34.91.68/255.255.255.248
Gateway	10.34.91.69
DNS	120.80.80.80 221.5.88.88
RX Packets	711
TX Packets	709
RX Bytes	336095
TX Bytes	97891

Index	Link	Status	Uptime	IP Address
2	WWAN2	Disconnected		

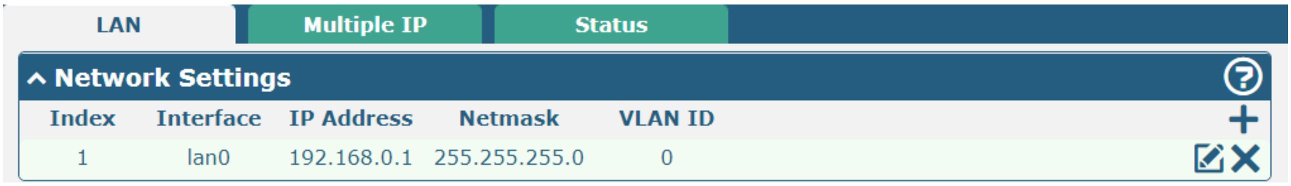
Click the Clear button to clear SIM1 or SIM2 monthly data traffic usage statistics. Data statistics will be displayed only if enable the Data Allowance function in **Interface > Link Manager > Link Settings > WWAN Settings > Data**

Allowance.

4.2.2 LAN

This section allows you to set the related parameters of local area network. R1500 has only one LAN network connection ETH0. After ETH0 is restored to factory settings, the default IP is 192.168.0.1/255.255.255.0.

LAN

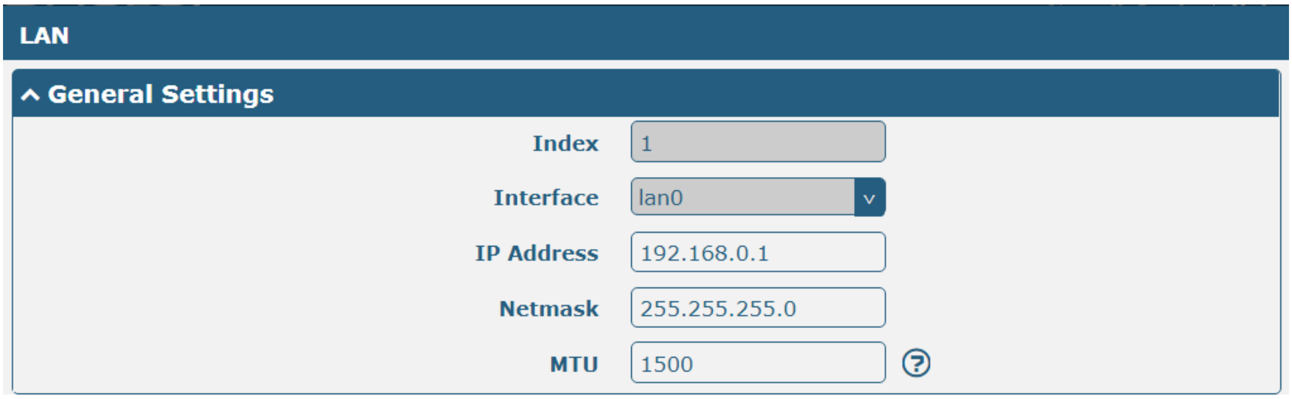


Network Settings

Index	Interface	IP Address	Netmask	VLAN ID
1	lan0	192.168.0.1	255.255.255.0	0

Note: Lan0 cannot be deleted.

Click ✎ to edit the parameters of the current LAN port.



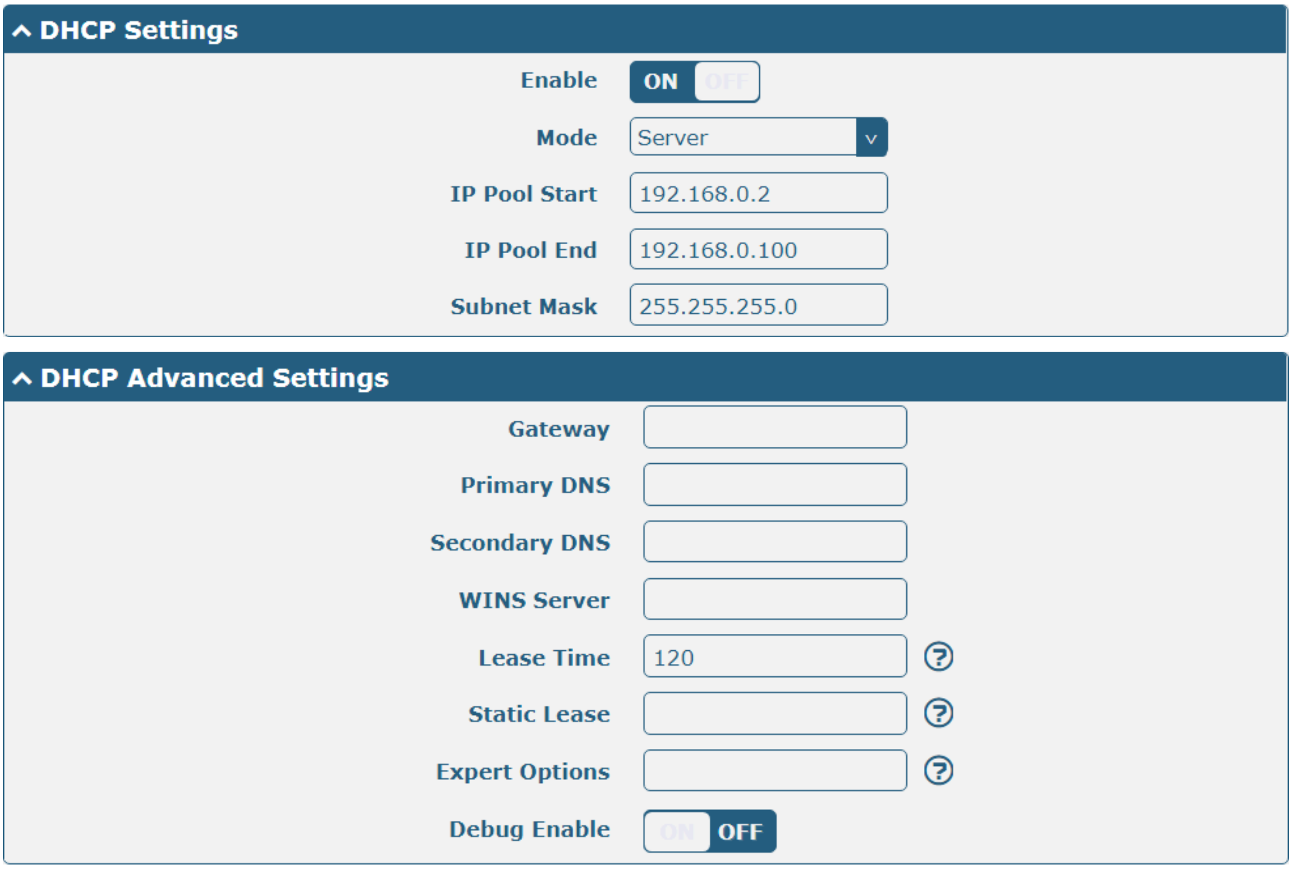
LAN

General Settings

Index	1
Interface	lan0
IP Address	192.168.0.1
Netmask	255.255.255.0
MTU	1500

LAN		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Interface	Show the currently edited interface. **Note**: Only when one of ETH0 or ETH1 is selected as lan1 in Ethernet > Port > Port Settings, lan1 can be configured.	lan0
IPv4 address	Set the IP address of the LAN port.	192.168.0.1
Subnet mask	Set the subnet mask of the LAN port.	255.255.255.0
MAN	Set the maximum transmission unit.	1500

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



DHCP Settings

Enable: ON

Mode: Server

IP Pool Start: 192.168.0.2

IP Pool End: 192.168.0.100

Subnet Mask: 255.255.255.0

DHCP Advanced Settings

Gateway:

Primary DNS:

Secondary DNS:

WINS Server:

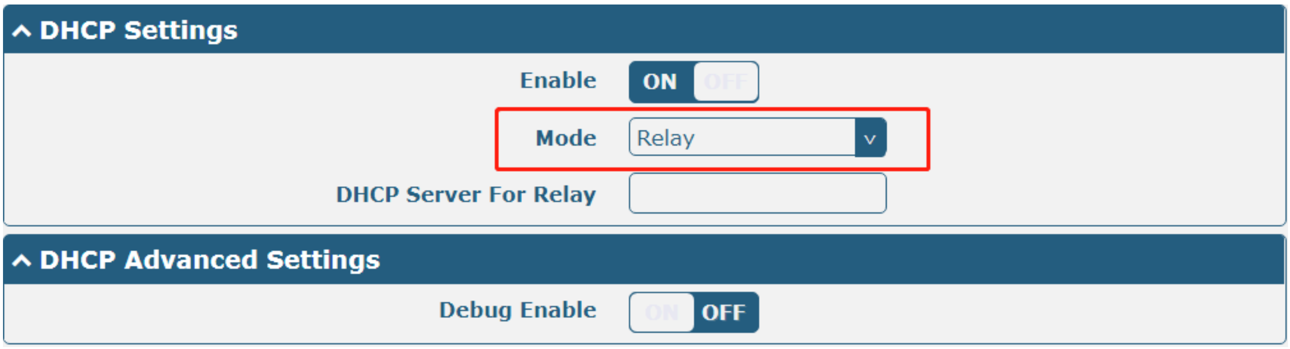
Lease Time: 120

Static Lease:

Expert Options:

Debug Enable: OFF

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



DHCP Settings

Enable: ON

Mode: Relay

DHCP Server For Relay:

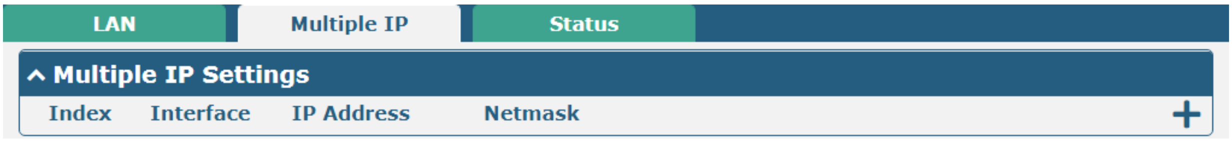
DHCP Advanced Settings

Debug Enable: OFF

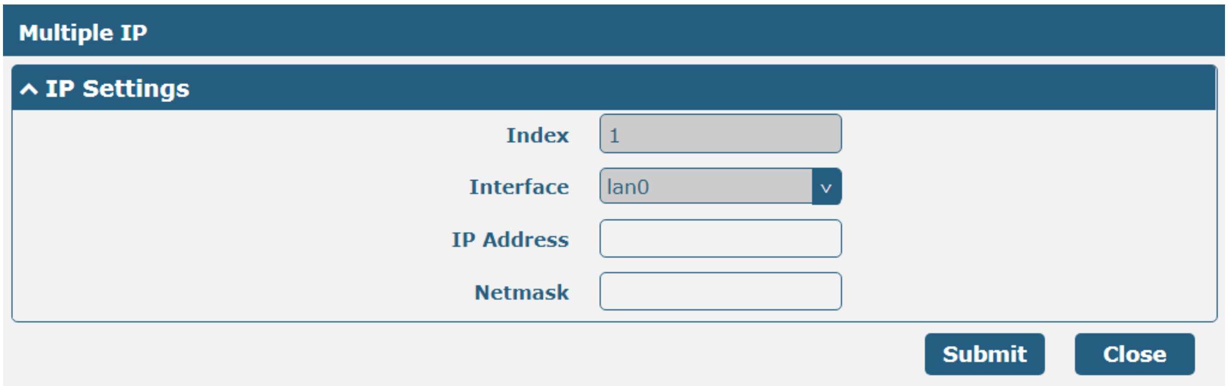
LAN		
Item	**Description**	**Default**
DHCP Settings		
Enable	Click the toggle button to enable/disable the DHCP feature.	ON

LAN		
Item	**Description**	**Default**
mode	Select the mode of DHCP from "Server" or "Relay". • Server: lease IP address to the DHCP client connected to the LAN port • Relay: The router can become a DHCP relay, which will provide a relay tunnel for solving the problem that the DHCP client is not in the same subnet as the DHCP server.	server
Starting IPv4 address pool	Define the IP address pool start to assign addresses to DHCP clients.	192.168.0.2
End the IPv4 address pool	Defines the end of the IP address pool that assigns addresses to DHCP clients.	192.168.0.100
Subnet mask	Define the subnet mask of the IP address obtained by the DHCP client from the DHCP server.	null
DHCP relay agent	Enter the IP address of the DHCP relay server.	null
DHCP Advanced Settings		
Gateway	The gateway assigned to the client by the DHCP server must be on the same network segment as the DHCP address pool.	null
Overrided Primary DNS	Override primary DNS will override the automatically obtained DNS	null
Overrided Secondary DNS	Override secondary DNS will override the automatically obtained D NS.	null
WINS server	Enter the address of the WINS server. The Windows System Internet Naming Service (WINS) manages all devices on the LAN and can be empty.	null
Lease time	Set the lease time in minutes. Lease time refers to the lease period in which the network user of the dynamic IP address occupies the IP address.	120
Static lease	The lease is bound by a MAC address to correspond to an IP address. The format is mac, ip; mac, ip;..., e.g. FF:ED:CB:A0:98:01,192.168.0.200	null
Expert option	Enter dnsmasq advanced options for DHCP. The format is config-desc; config-desc, such as log-dhcp; quiet-dhcp.	null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	OFF

Multiple IP



Click ✎ To edit multiple IP addresses of the LAN port; click ✕ to delete multiple IP addresses of the LAN port; click + To add a new multi-IP.



Multiple IP

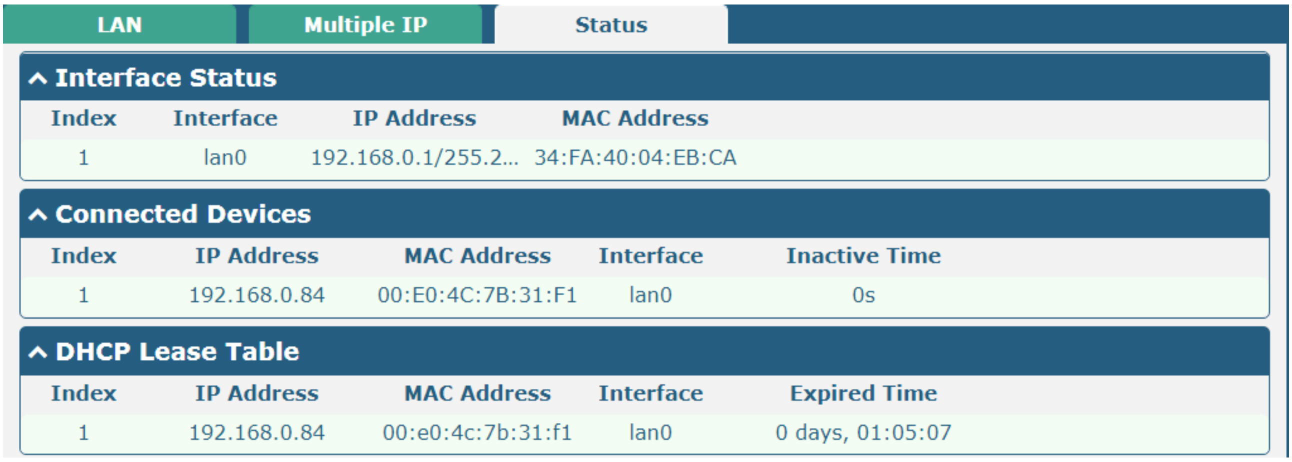
^ IP Settings

Index	1
Interface	lan0
IP Address	
Netmask	

IP address setting		
project	**Description**	**default**
Index	Indicate the ordinal of the list.	--
Interface	Show the currently edited interface.	--
IP address	Set the IP address of the LAN port.	null
Subnet mask	Set the subnet mask of the LAN port.	null

Status

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



^ Interface Status

Index	Interface	IP Address	MAC Address
1	lan0	192.168.0.1/255.2...	34:FA:40:04:EB:CA

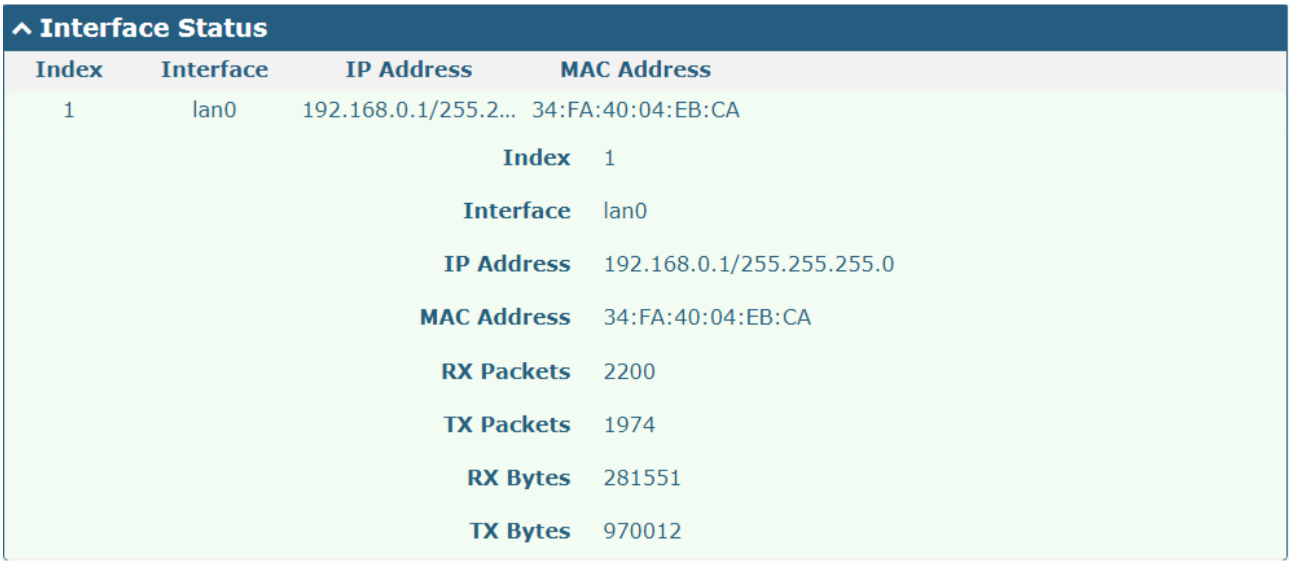
^ Connected Devices

Index	IP Address	MAC Address	Interface	Inactive Time
1	192.168.0.84	00:E0:4C:7B:31:F1	lan0	0s

^ DHCP Lease Table

Index	IP Address	MAC Address	Interface	Expired Time
1	192.168.0.84	00:e0:4c:7b:31:f1	lan0	0 days, 01:05:07

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



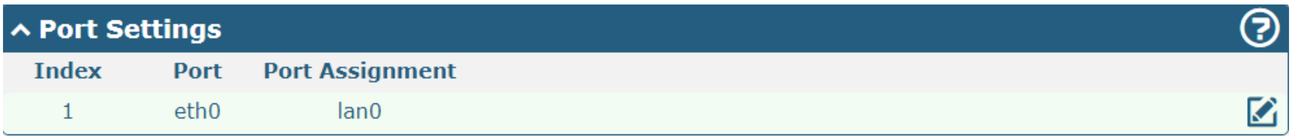
^ Interface Status

Index	Interface	IP Address	MAC Address
1	lan0	192.168.0.1/255.2...	34:FA:40:04:EB:CA

Index	1
Interface	lan0
IP Address	192.168.0.1/255.255.255.0
MAC Address	34:FA:40:04:EB:CA
RX Packets	2200
TX Packets	1974
RX Bytes	281551
TX Bytes	970012

4.2.3 Ethernet

This section is used to configure Ethernet and related parameters. The R1500 gateway has one Ethernet port ETH0. ETH0 is used as the LAN port to which the lower device is connected to the router. The ETH0 factory default is lan0, and the default IP is 192.168.0.1./255.255.255.0.

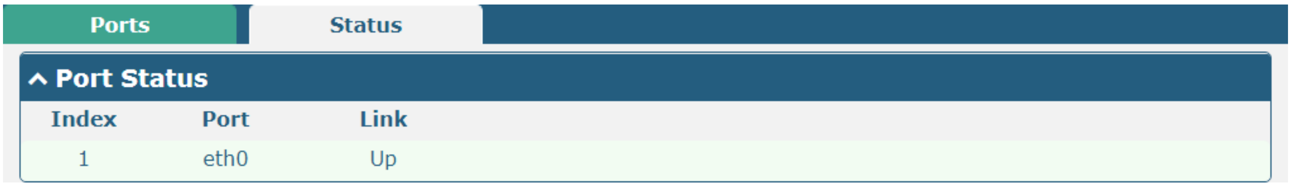


^ Port Settings

Index	Port	Port Assignment
1	eth0	lan0

Port setting		
Option	**Description**	**defa ult**
index	Indicate the ordinal of the list.	--
port	The currently edited port is displayed and cannot be edited.	--
Port assignme nt	Select the type of network port and only select lan0.	lan0

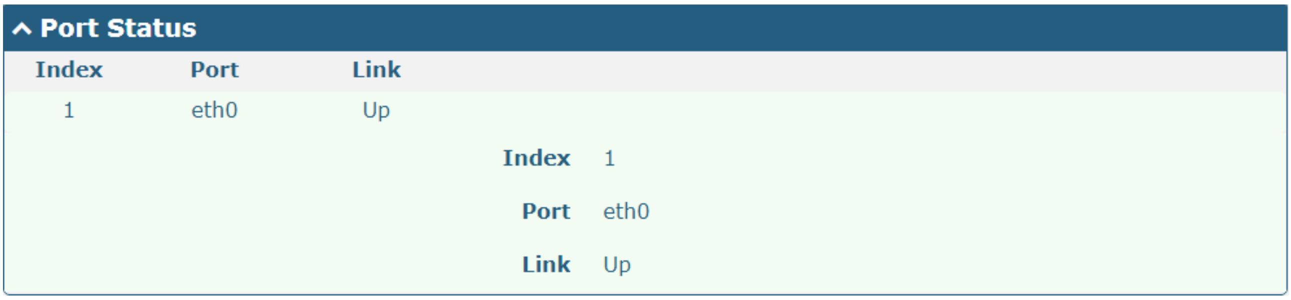
. Click the Status bar to see the connection status of all Ethernet ports.



^ Port Status

Index	Port	Link
1	eth0	Up

Click on one of the lines and its detailed status information will be displayed below the current line.



^ Port Status

Index	Port	Link
1	eth0	Up

Index 1

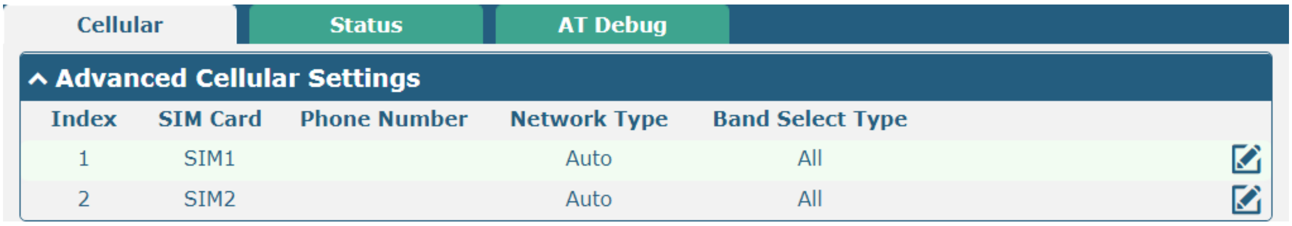
Port eth0

Link Up

This section allows you to set the related parameters of local area network. R1500 has only one LAN network connection ETH0. After ETH0 is srestored to factory settings, the default IP is 192.168.0.1/255.255.255.0.

4.2.4 Cellular

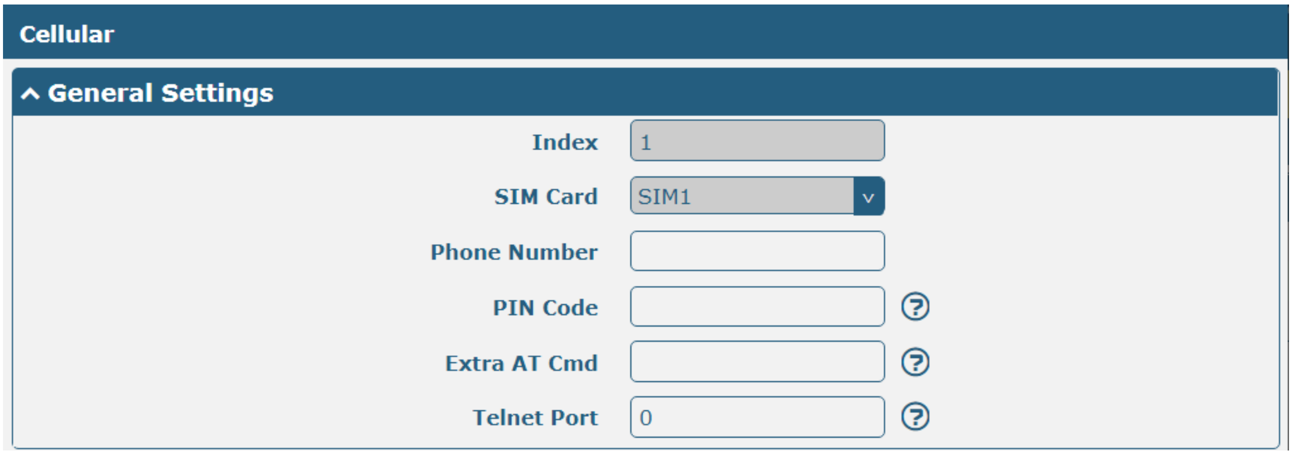
This section allows you to set up the cellular network and related parameters. The R1500 has two SIM card slots, but since it is a single module, it does not support two SIM cards working at the same time. Both the SIM1 card slot and the SIM2 card slot are available when the single SIM card is inserted for the first time.



Advanced Cellular Settings

Index	SIM Card	Phone Number	Network Type	Band Select Type
1	SIM1		Auto	All
2	SIM2		Auto	All

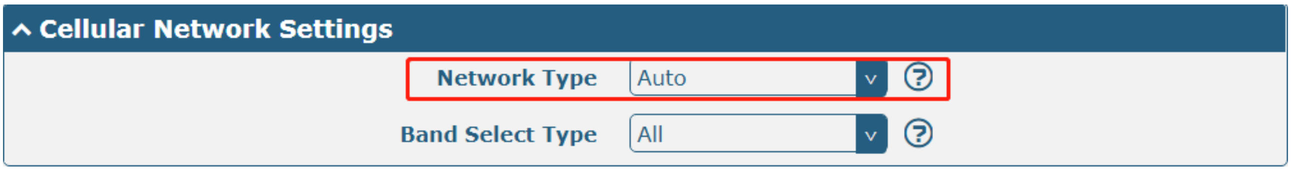
Click on the far right of SIM1 ✎ To edit the parameters:


Cellular

General Settings

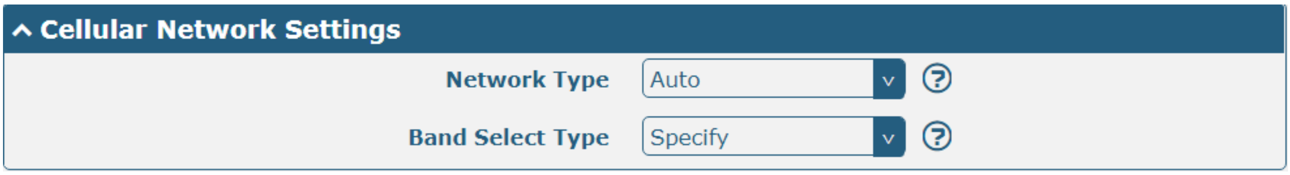
Index	1
SIM Card	SIM1
Phone Number	
PIN Code	
Extra AT Cmd	
Telnet Port	0

When "Automatic" is selected for "Network Type", the window looks like this:

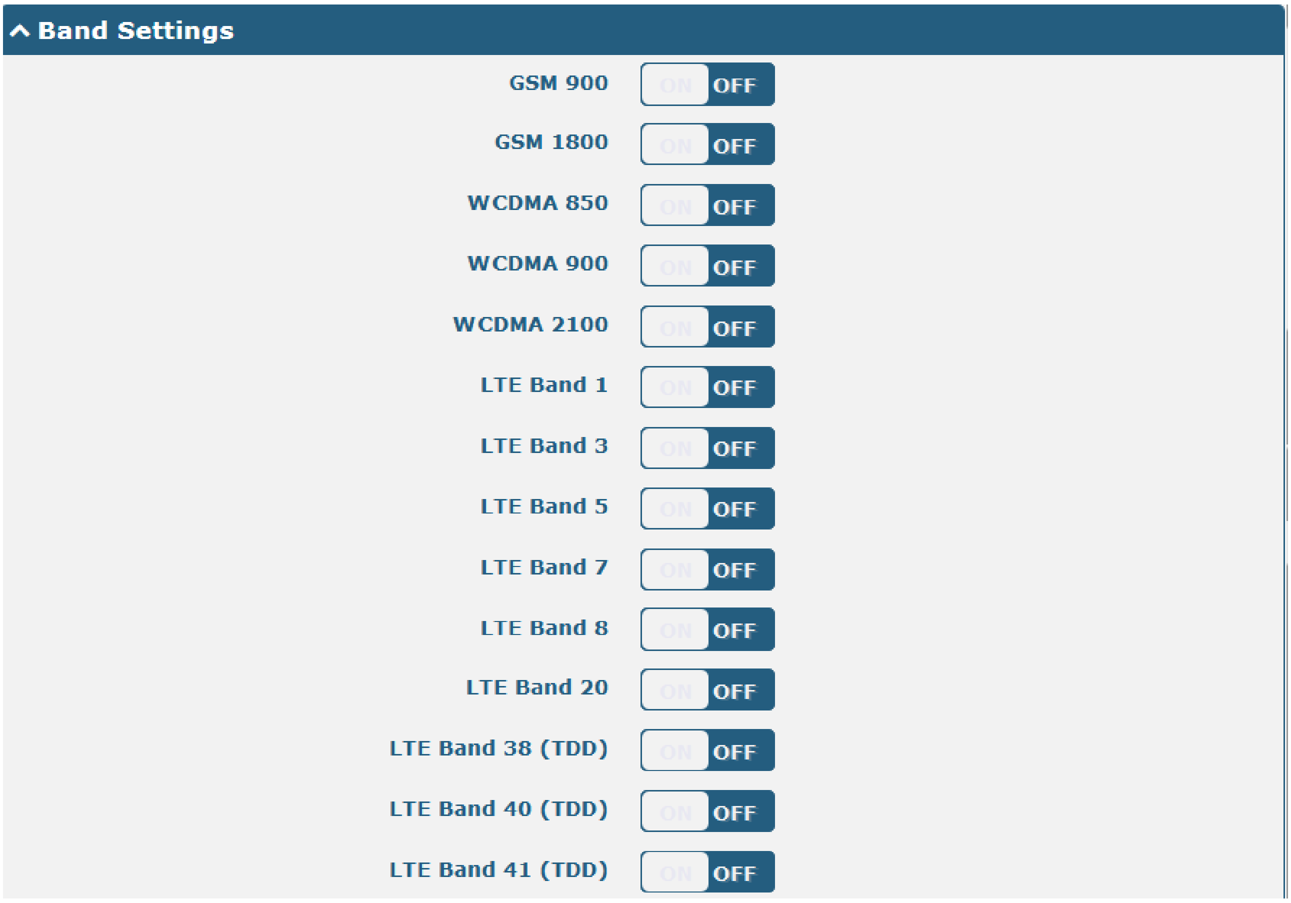

Cellular Network Settings

Network Type	Auto
Band Select Type	All

When "Specify" is selected for "Band Selection", the window looks like this:


Cellular Network Settings

Network Type	Auto
Band Select Type	Specify



^ Band Settings

GSM 900 ON [✓ OFF]

GSM 1800 ON [✓ OFF]

WCDMA 850 ON [✓ OFF]

WCDMA 900 ON [✓ OFF]

WCDMA 2100 ON [✓ OFF]

LTE Band 1 ON [✓ OFF]

LTE Band 3 ON [✓ OFF]

LTE Band 5 ON [✓ OFF]

LTE Band 7 ON [✓ OFF]

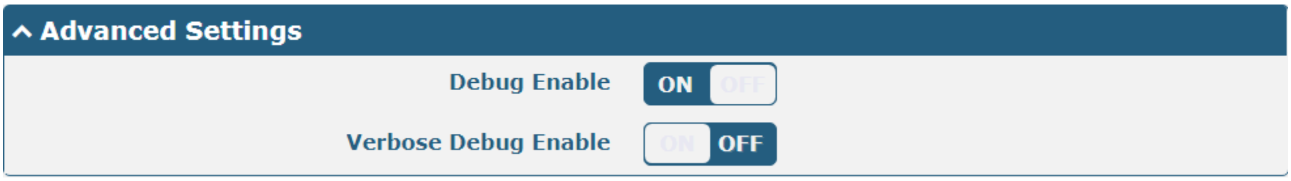
LTE Band 8 ON [✓ OFF]

LTE Band 20 ON [✓ OFF]

LTE Band 38 (TDD) ON [✓ OFF]

LTE Band 40 (TDD) ON [✓ OFF]

LTE Band 41 (TDD) ON [✓ OFF]



^ Advanced Settings

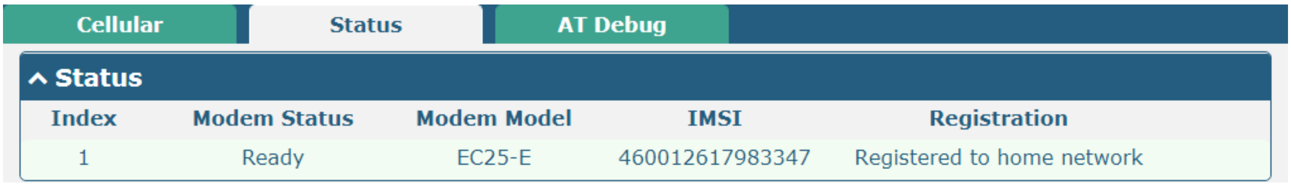
Debug Enable [✓ ON] OFF

Verbose Debug Enable ON [✓ OFF]

Cellular		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
SIM card	Show the currently edited SIM card	SIM1
telephone number	Define the phone number of the SIM card.	Null
PIN code	Enter the PIN code used to unlock the SIM card, 4-8 digits.	Null
Extra AT command	Enter additional AT commands for wireless module initialization for expert use only.	Null
Telnet port	Specify a port. The user Telnet connection router sends an AT command through this port.	Nul
Cellular Settings		
Network Type	Select the cellular network type, which is the network access order. Select from "Automatic", "Only 2G", "Priority 2G", "Only 3G", "Priority 3G", "Only 4G", "Priority 4G".	auto
Band selection	Select from "All" or "Specified". When "Specify" is selected, the user can select certain frequency bands.	All

Cellular		
Item	**Description**	**Default**
Advanced Settings		
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Detailed Debug Enable	Click the toggle button to enable/disable the detailed debug options. Enable link management detailed debugging information output.	OFF

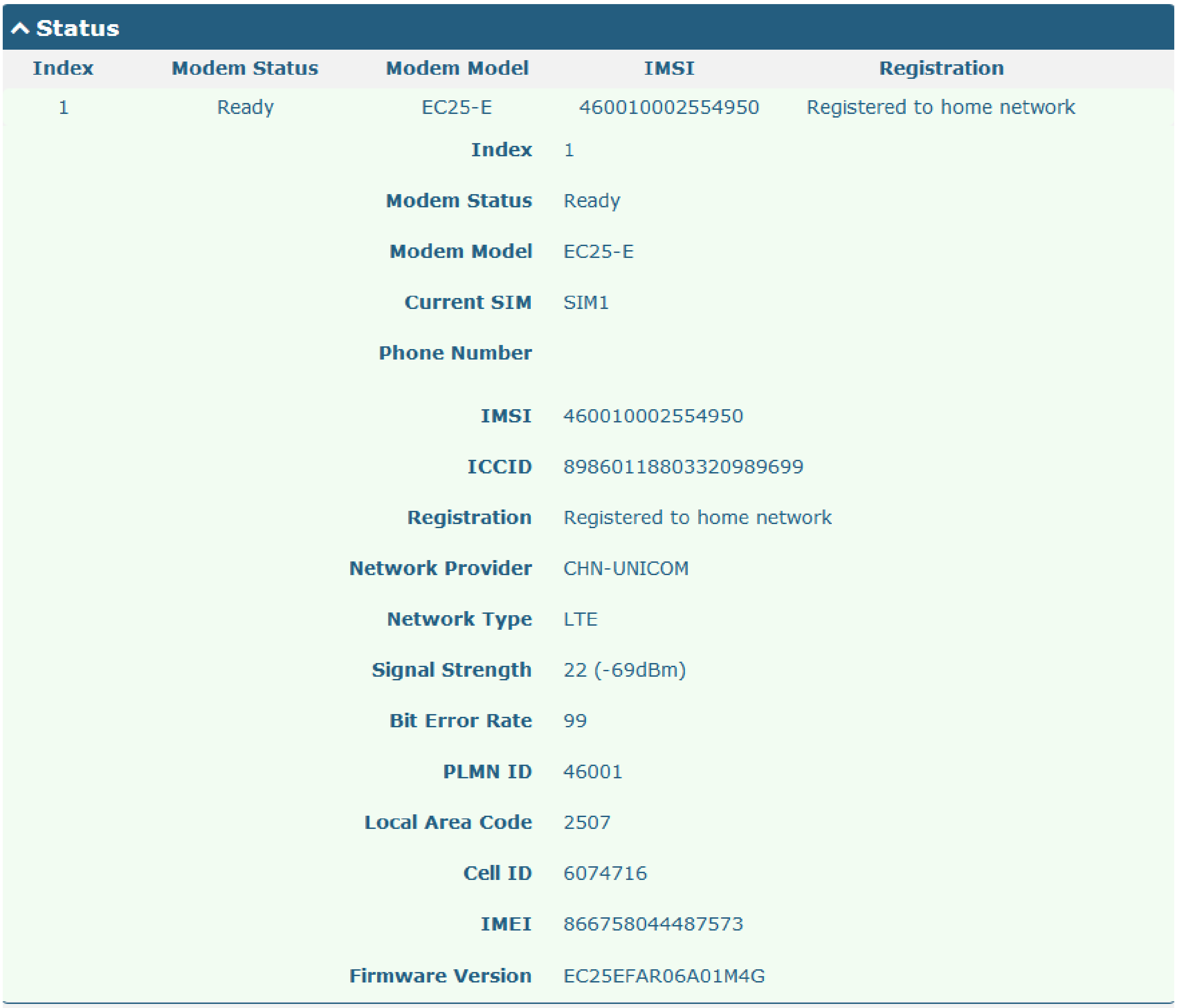
Click the Status bar to view status information for the cellular network.



^ Status

Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	EC25-E	460012617983347	Registered to home network

Click on one of the lines and its detailed status information will be displayed below the current line.



^ Status

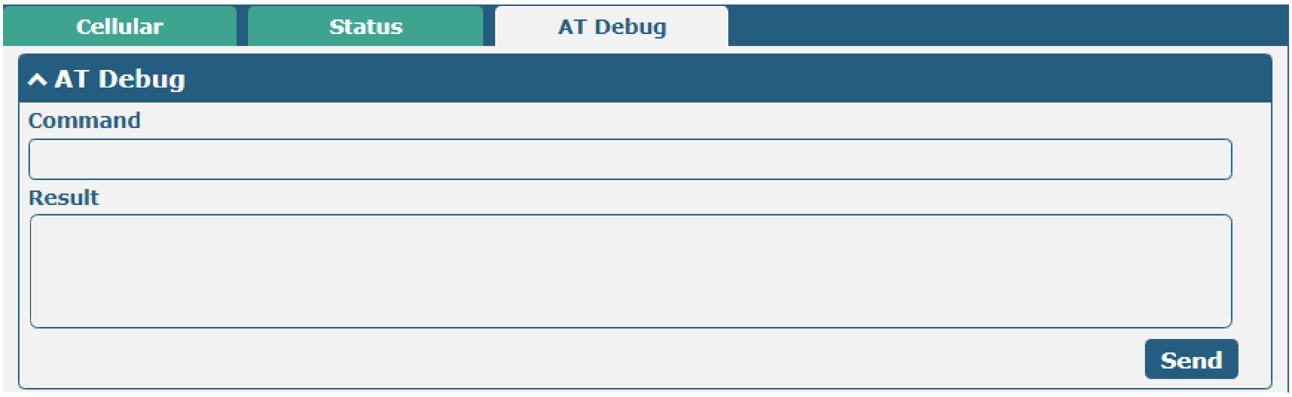
Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	EC25-E	460010002554950	Registered to home network

Index	1
Modem Status	Ready
Modem Model	EC25-E
Current SIM	SIM1
Phone Number	
IMSI	460010002554950
ICCID	89860118803320989699
Registration	Registered to home network
Network Provider	CHN-UNICOM
Network Type	LTE
Signal Strength	22 (-69dBm)
Bit Error Rate	99
PLMN ID	46001
Local Area Code	2507
Cell ID	6074716
IMEI	866758044487573
Firmware Version	EC25EFAR06A01M4G

Cellular	
Item	**Description**

Cellular	
Item	**Description**
Index	Indicate the ordinal of the list.
Modem status	Show the operating status of the wireless module.
Modem model	Show the model number of the wireless module.
Current SIM card	Show the SIM card currently used by the gateway: SIM1 or SIM2.
telephone number	Show the phone number of the current SIM card. **Note**: This option should be manually filled in "Cellular > Advanced Cell Settings > SIM1/SIM2 > Phone Number".
IMSI	Show the IMSI code of the current SIM card.
Registration status	Show the current network status.
Operator	Show the operator of the currently registered network.
Network Type	Show the current type of network service, such as WCDMA.
Signal strength	Show the current signal strength.
Bit error rate	Show the current bit error rate.
Carrier identification number	Show the current carrier identification number.
Location area code	Show the current location area code to identify different location areas.
Cell number	Show the current cell number and is used to locate the router.
IMEI	Show the IMEI code of the wireless module.
Firmware version	Show the firmware version of the current wireless module.

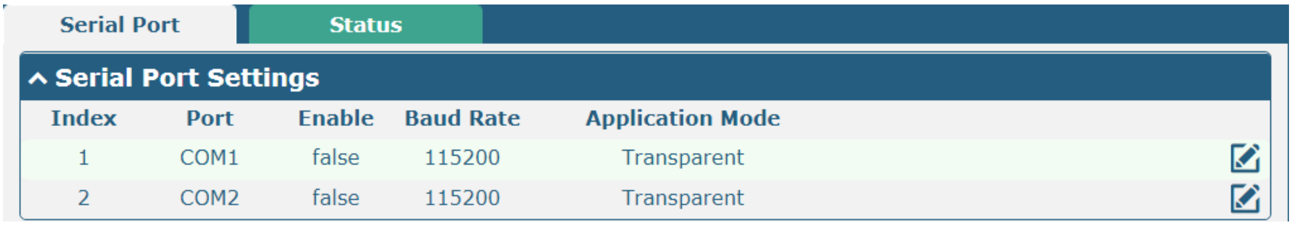
Click the "AT Debugging" field to detect the AT command.



AT command debugging		
project	**Description**	**default**
command	Enter the AT command you want to send to the mobile communication module in the text box.	Null
result	The router displays the AT command responded by the mobile communication module in this text box.	null
Send	Click the button to send AT command.	--

4.2.5 Serial Port

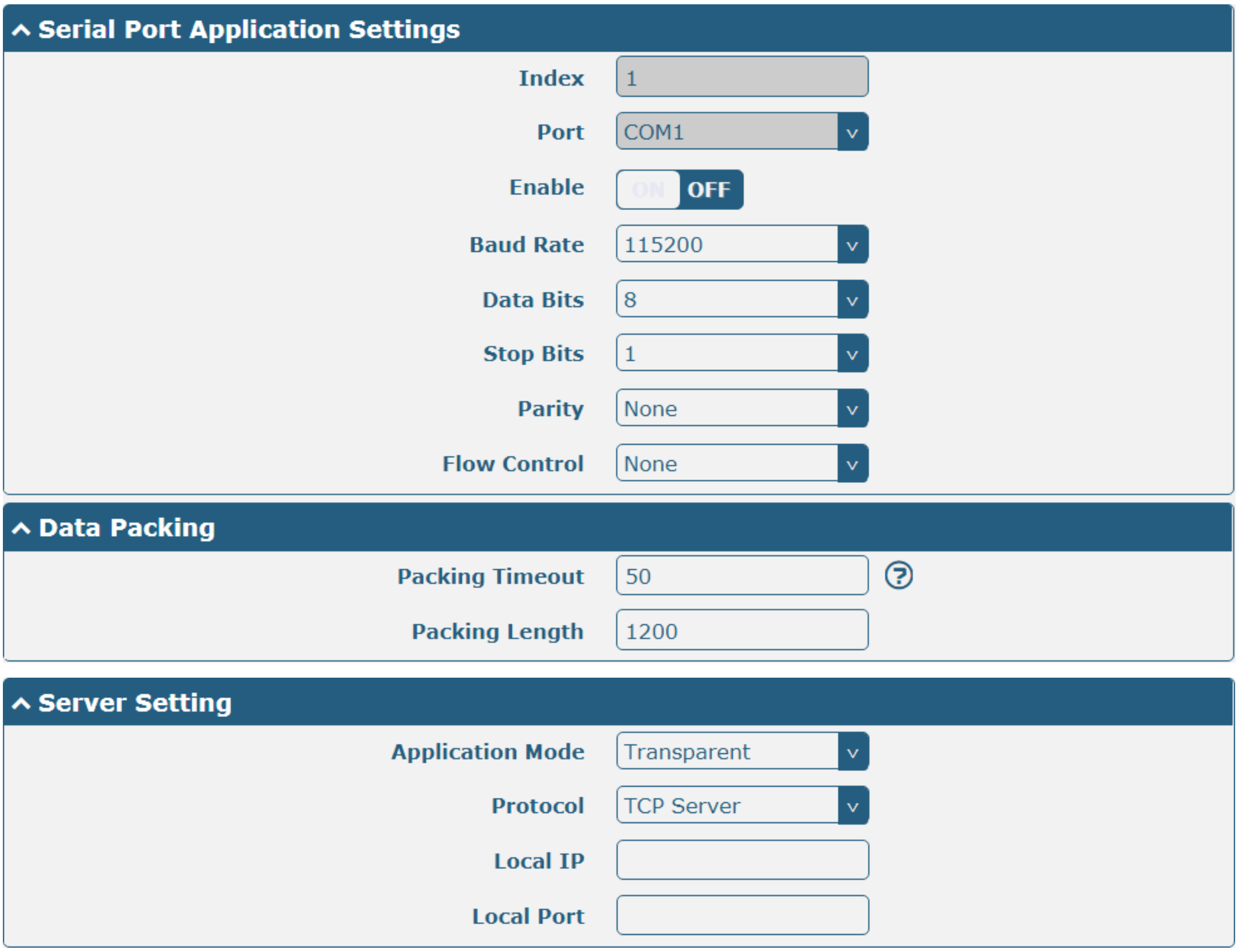
This section allows you to set the serial port parameters. R1500 supports two RS-232, and both COM1 and COM2 are RS-232. Serial port provides a way to transfer serial data to IP data, or vice versa, and transmit these data via wired or wireless network to achieve data transparent transmission.



Serial Port Settings

Index	Port	Enable	Baud Rate	Application Mode
1	COM1	false	115200	Transparent
2	COM2	false	115200	Transparent

Click on the far right of COM1 ✎ Button, pop-up window is as follows:



Serial Port Application Settings

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

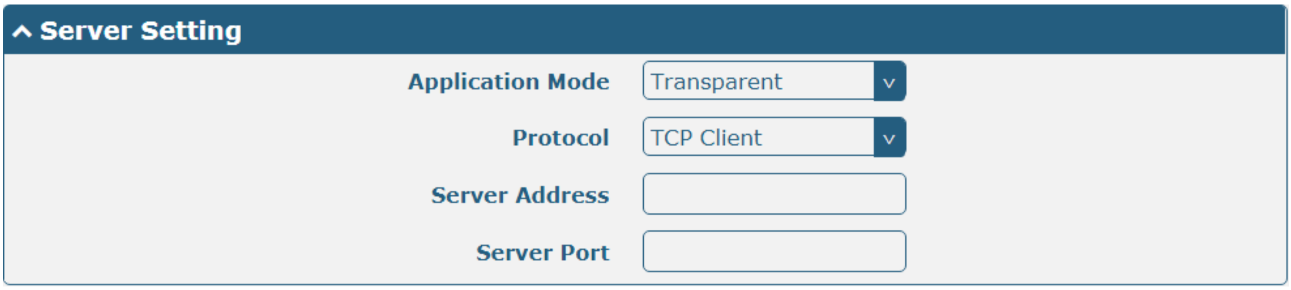
Data Packing

Packing Timeout	50
Packing Length	1200

Server Setting

Application Mode	Transparent
Protocol	TCP Server
Local IP	
Local Port	

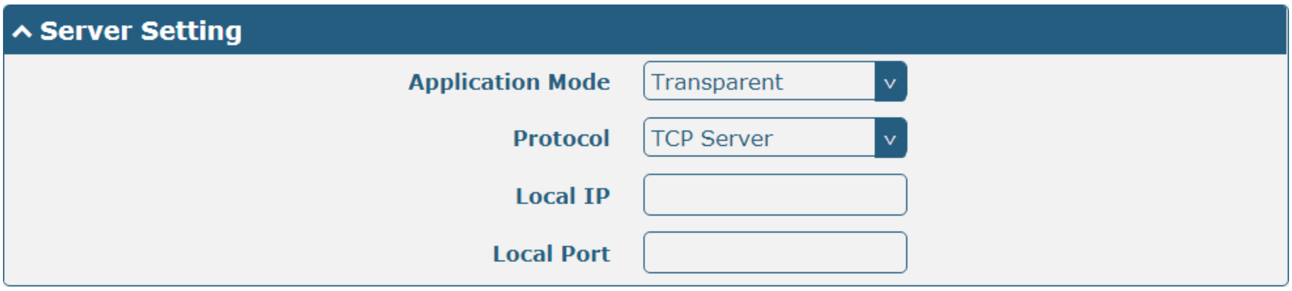
- The window is displayed as below when choosing “Transparent” as the application mode and “TCP Client” as the protocol.



Server Setting

Application Mode	Transparent
Protocol	TCP Client
Server Address	
Server Port	

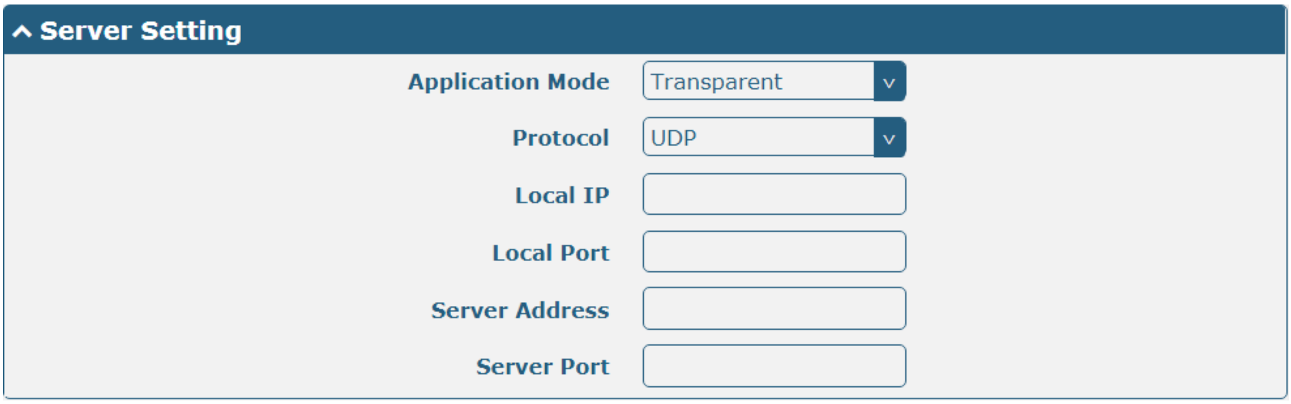
The window is displayed as below when choosing "Transparent" as the application mode and "TCP Server" as the protocol.



Server Setting

Application Mode	Transparent
Protocol	TCP Server
Local IP	
Local Port	

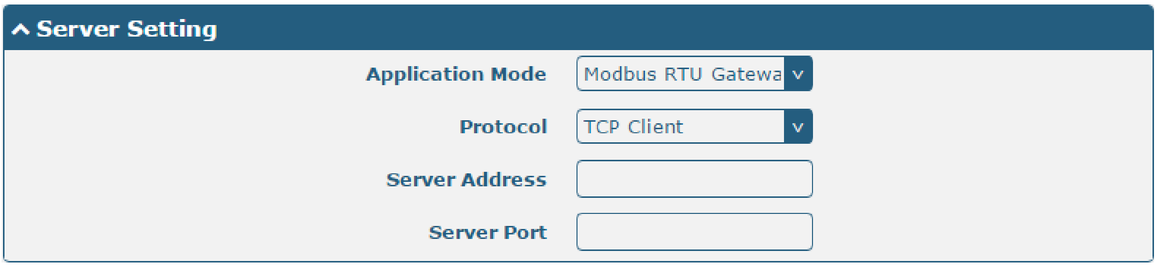
The window is displayed as below when choosing "Transparent" as the application mode and "UDP" as the protocol.



Server Setting

Application Mode	Transparent
Protocol	UDP
Local IP	
Local Port	
Server Address	
Server Port	

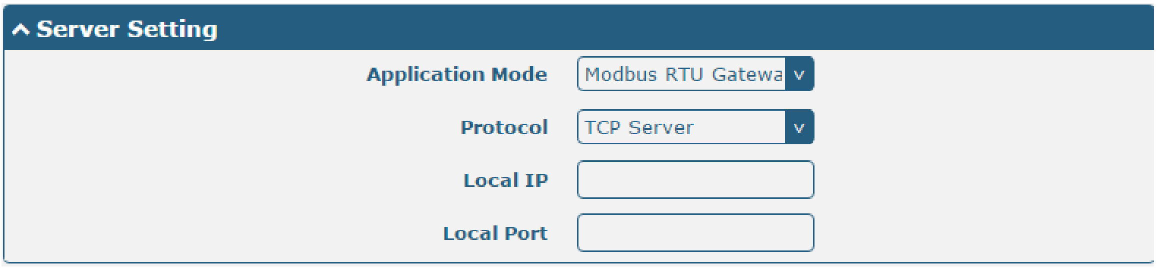
- The window is displayed as below when choosing "Modbus RTU Gateway" as the application mode and "TCP Client" as the protocol.



Server Setting

Application Mode	Modbus RTU Gatewa
Protocol	TCP Client
Server Address	
Server Port	

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



Server Setting

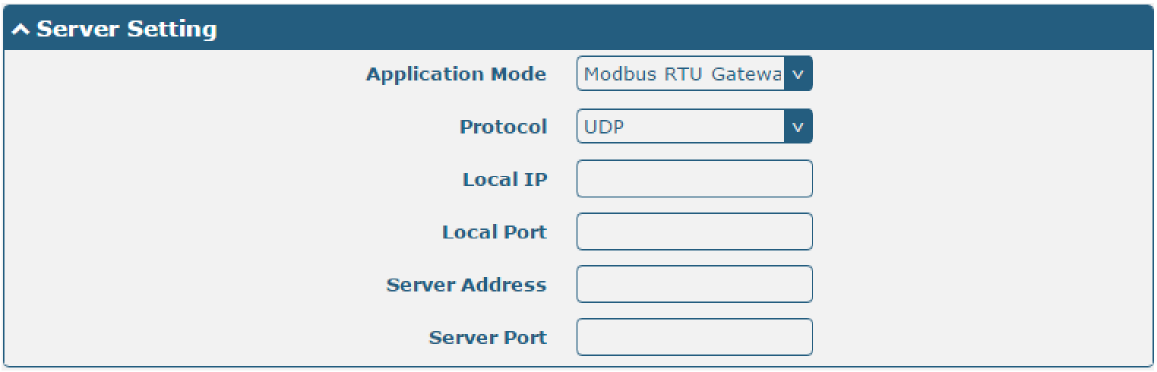
Application Mode: Modbus RTU Gatewa

Protocol: TCP Server

Local IP:

Local Port:

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



Server Setting

Application Mode: Modbus RTU Gatewa

Protocol: UDP

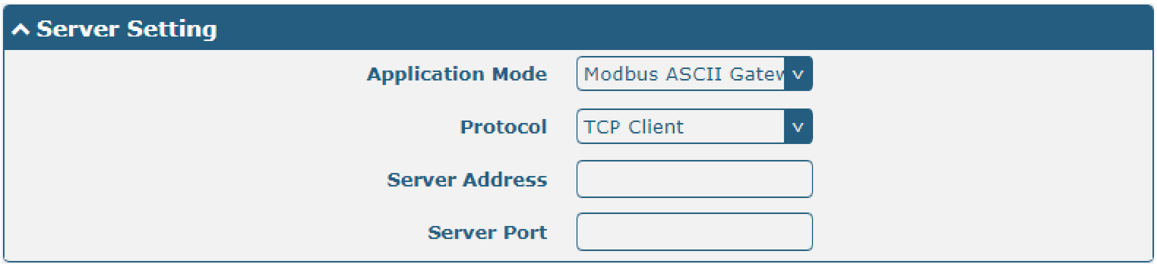
Local IP:

Local Port:

Server Address:

Server Port:

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



Server Setting

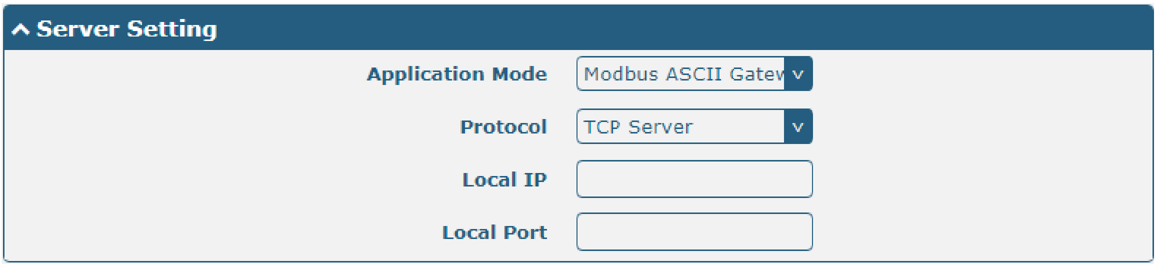
Application Mode: Modbus ASCII Gatev

Protocol: TCP Client

Server Address:

Server Port:

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



Server Setting

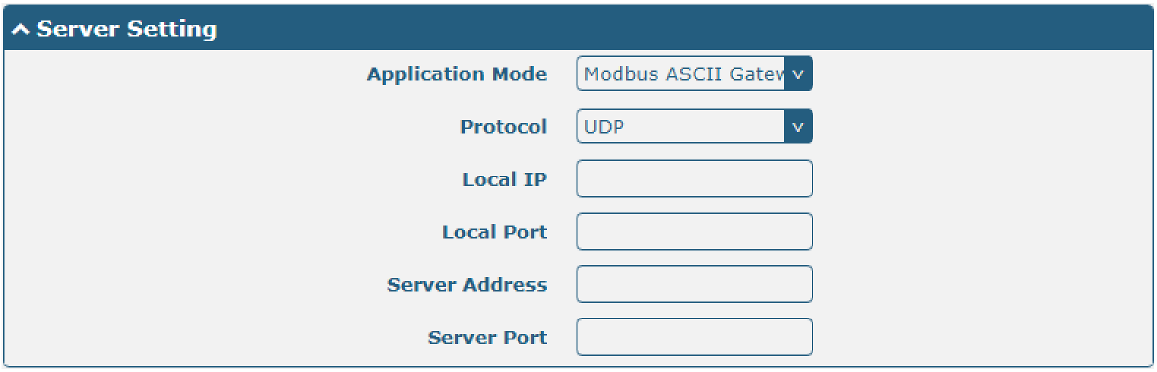
Application Mode: Modbus ASCII Gatev

Protocol: TCP Server

Local IP:

Local Port:

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



Server Setting

Application Mode: Modbus ASCII Gatev

Protocol: UDP

Local IP

Local Port

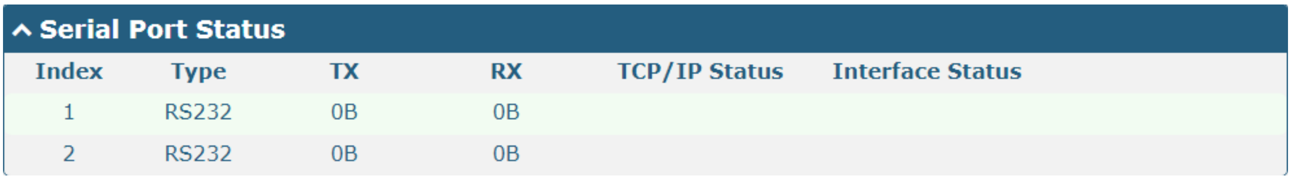
Server Address

Server Port

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.	--
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
Check Digit	Select from "None", "Odd Check" and "Even Check".	None
Flow control	Select from "None", "Software" and "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 Setting		
Application Mode	Select from "Transparent", "Modbus RTU Gateway" or "Modbus ASCII Gateway". • Transparent: gateway will transmit the serial data transparently • Modbus RTU Gateway: gateway will translate the Modbus RTU data to Modbus TCP data and sent out, and vice versa • Modbus ASCII Gateway: gateway will translate the Modbus ASCII data to Modbus TCP data and sent out, and vice versa	Transparent
Protocol	Select from "TCP Client", "TCP Server" or "UDP". • TCP Client: Gateway works as TCP client, initiate TCP connection to TCP server. Server address supports both IP	TCP Client

Serial Port		
Item	**Description**	**Default**
	and domain name • TCP Server: Gateway works as TCP server, listening for connection request from TCP client • UDP: Gateway works as UDP client	
Server Address	Enter the address of server which will receive the data sent from gateway'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	Enter the IP of TCP or UDP.	Null
Local Port	Enter the port of TCP or UDP.	Null

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



Serial Port Status

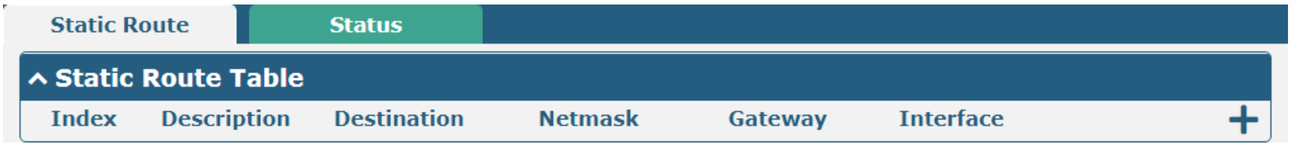
Index	Type	TX	RX	TCP/IP Status	Interface Status
1	RS232	0B	0B		
2	RS232	0B	0B		

4.3 The internet

4.3.1 Routing

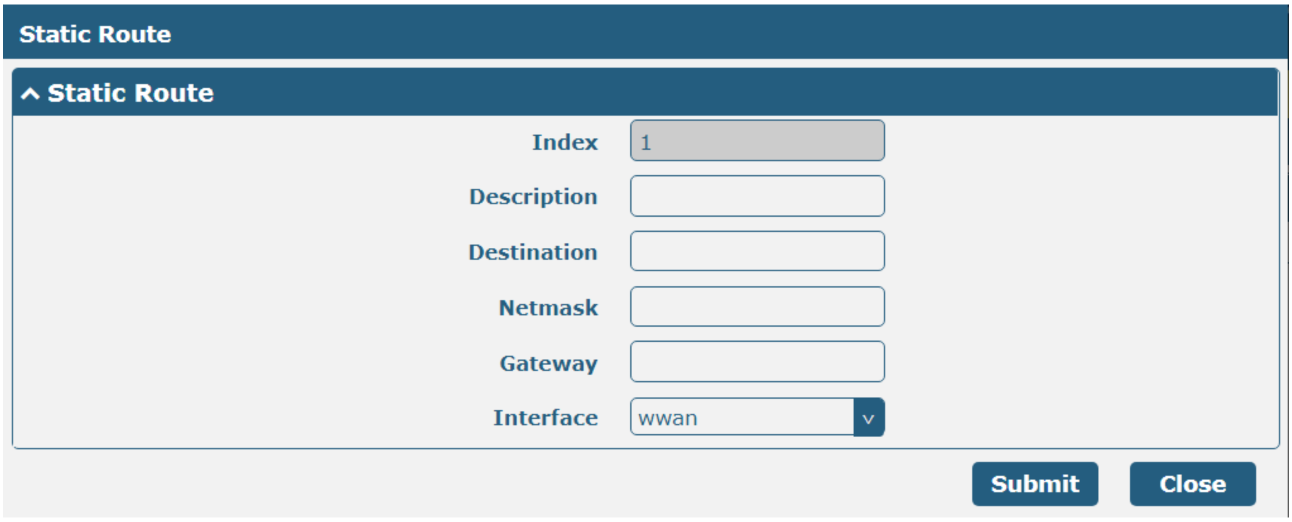
A static route is a route based on the destination address. Up to 20 static routes can be added to the router. The routing information protocol, RIP (Route Information Protocol), is widely used in small networks with stable rate changes. OSPF (Open Shortest Path First) protocol is used for decision routing in a single autonomous system and is suitable for large networks.

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



Index	Description	Destination	Netmask	Gateway	Interface

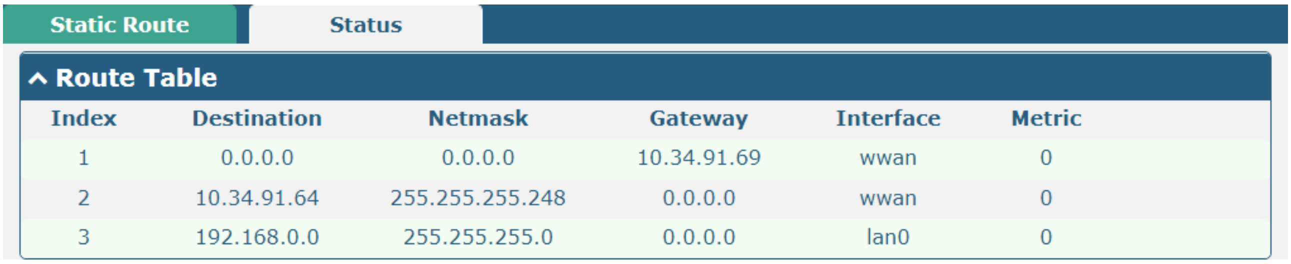
Click +, add a static route in the pop-up window. You can add up to 20 items.



Index	1
Description	
Destination	
Netmask	
Gateway	
Interface	wwan

Static route		
Option	**Description**	**default**
index	Indicate the ordinal of the list.	--
description	Enter a description for the static route.	null
Destination point	Enter the IP address of the destination host or destination network.	null
Subnet mask	Enter the subnet mask of the destination host or destination network.	null
Gateway	Enter the IP address of the static routing rule gateway. The router will forward all data matching the destination address and subnet mask to the gateway.	null
interface	Select the interface of the link you are currently configuring.	wwan1

Click on the "Status" bar to view the routing table status of the device.

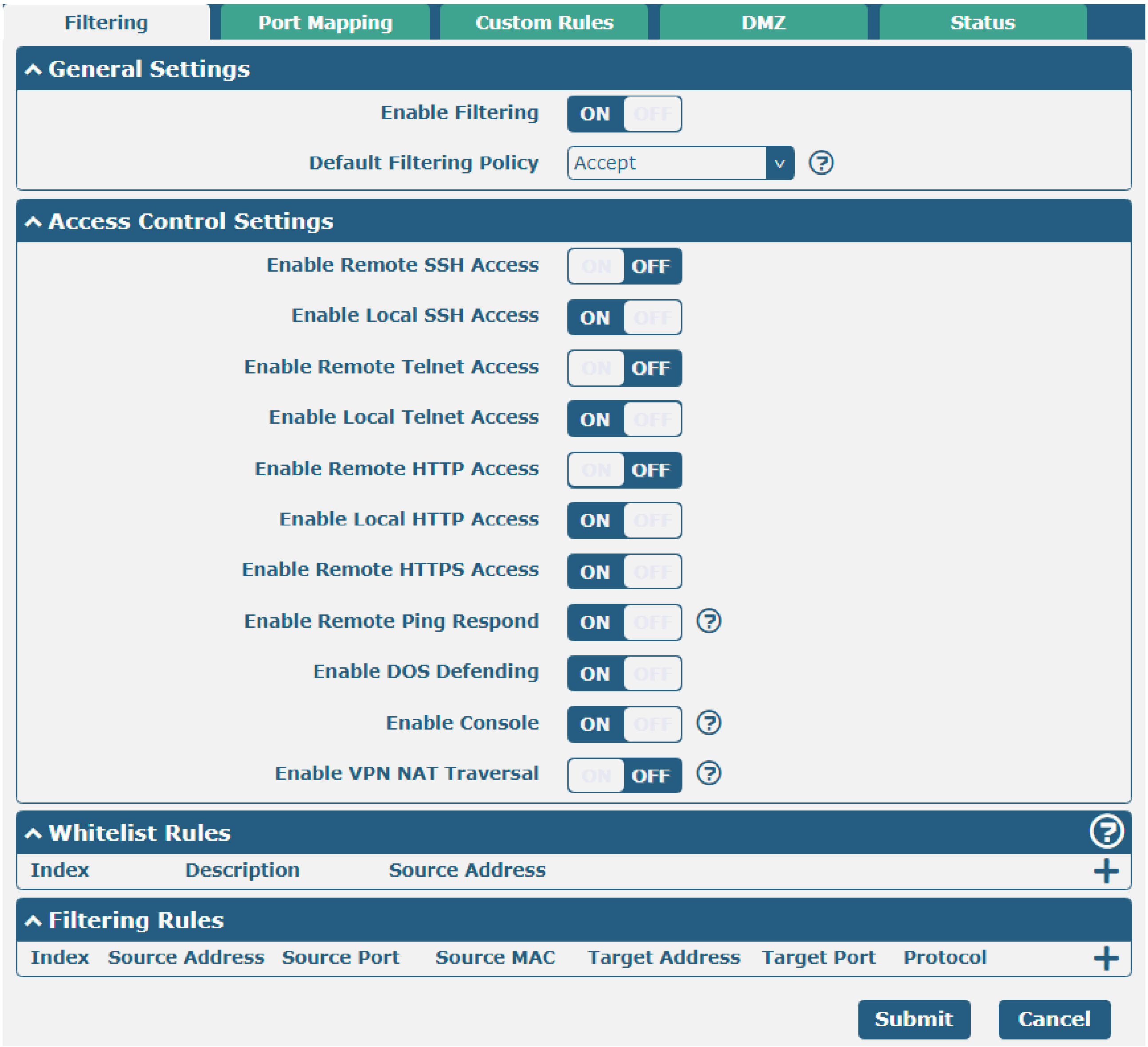


Route Table

Index	Destination	Netmask	Gateway	Interface	Metric
1	0.0.0.0	0.0.0.0	10.34.91.69	wwan	0
2	10.34.91.64	255.255.255.248	0.0.0.0	wwan	0
3	192.168.0.0	255.255.255.0	0.0.0.0	lan0	0

4.3.2 Firewall

This section is used to set firewall parameters, including setting access controls and adding filtering rules. Filtering rules allow users to customize the acceptance or discard of specified access sources and filter their IP addresses or MAC addresses. Click Network > Firewall > Filter to display the following:



General Settings

Enable Filtering	ON
Default Filtering Policy	Accept

Access Control Settings

Enable Remote SSH Access	OFF
Enable Local SSH Access	ON
Enable Remote Telnet Access	OFF
Enable Local Telnet Access	ON
Enable Remote HTTP Access	OFF
Enable Local HTTP Access	ON
Enable Remote HTTPS Access	ON
Enable Remote Ping Respond	ON
Enable DOS Defending	ON
Enable Console	ON
Enable VPN NAT Traversal	OFF

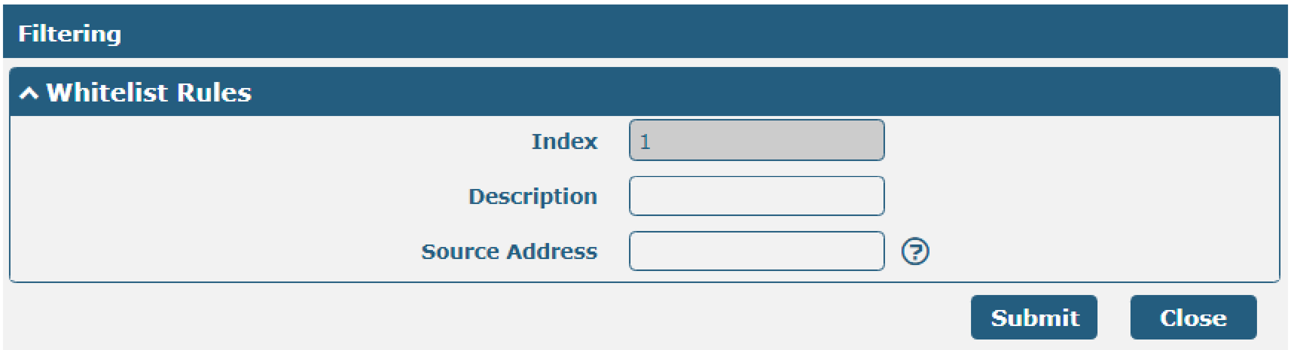
Whitelist Rules

Index	Description	Source Address

Filtering Rules

Index	Source Address	Source Port	Source MAC	Target Address	Target Port	Protocol

Click + to add a whitelist rule and add up to 50.

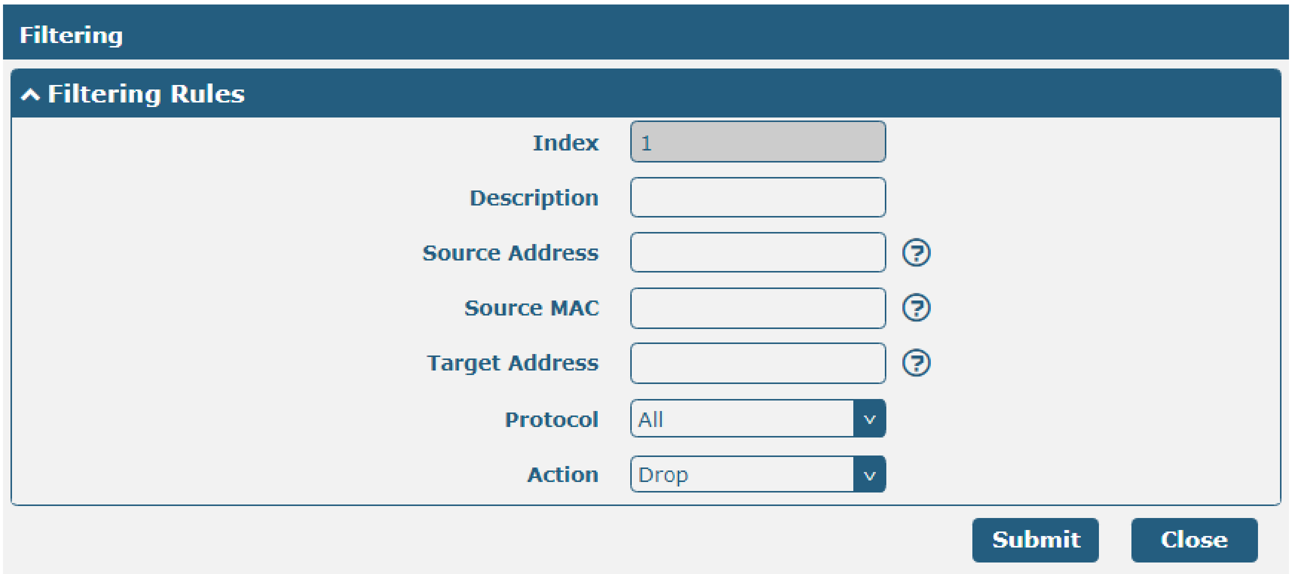


Filtering

^ Whitelist Rules

Index	1
Description	
Source Address	

Click + Add filter rules and add up to 50. When the protocol defaults to "All" or selects "ICMP", the window displays as follows (take the "All" protocol as an example):

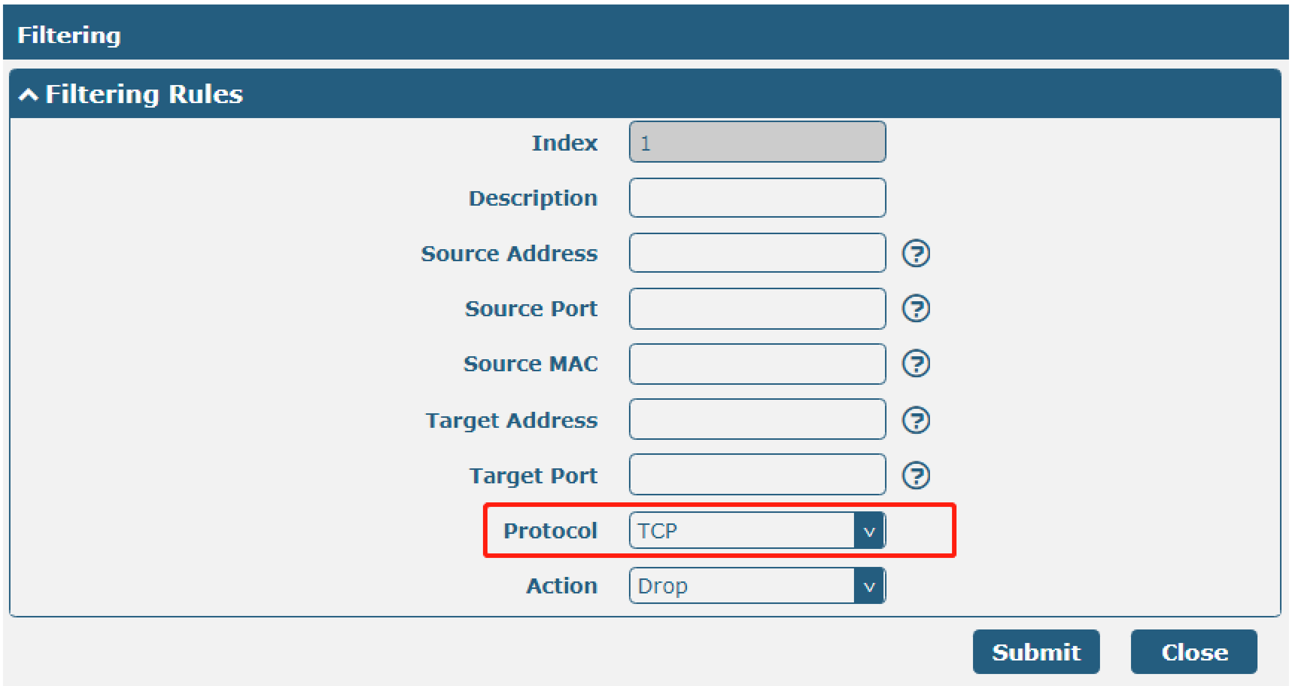


Filtering

^ Filtering Rules

Index	1
Description	
Source Address	
Source MAC	
Target Address	
Protocol	All
Action	Drop

When "TCP", "UDP" or "TCP-UDP" is selected as the protocol, the window is displayed as follows (take the "TCP" protocol as an example):



Filtering

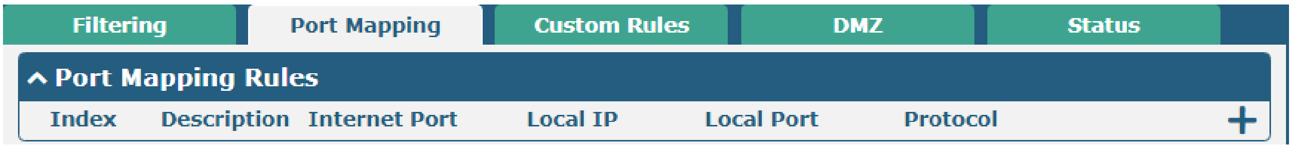
^ Filtering Rules

Index	1
Description	
Source Address	
Source Port	
Source MAC	
Target Address	
Target Port	
Protocol	TCP
Action	Drop

filter		
Option	**Description**	**default**
General settings		
Enable	Click the toggle button to enable/disable the default filter rule.	ON
Default filtering policy	You can choose to accept or discard. • Accept: Other accesses are allowed except the filter rule table is set to drop access connection requests. • Discard: All accesses are denied except that the filter rule table is set to accept access requests.	accept
Access control		
Enable remote SSH access	Click the toggle button to enable/disable this option. Allowed, enabledUsers on the internetRemotely access the router via SSH.	OFF
Enable local SSH access	Click the toggle button to enable/disable this option. When enabled, allows users on the LAN to access the router locally via SSH.	ON
Enable remote Telnet access	Click the toggle button to enable/disable this option. When enabled, allows users on the Internet to remotely access the router through Telnet.	OFF
Enable local Telnet access	Click the toggle button to enable/disable this option. When enabled, allows users on the LAN to access the router locally through Telnet.	ON
Enable remote HTTP access	Click the toggle button to enable/disable this option. When enabled, allows users on the Internet to remotely access the router via HTTP.	OFF
Enable local HTTP access	Click the toggle button to enable/disable this option. When enabled, allows users on the LAN to access the router locally via HTTP.	ON
Enable remote HTTPS access	Click the toggle button to enable/disable this option. When enabled, allows users on the Internet to remotely access the router via HTTPS.	ON
Respond to a remote ping request	Click the toggle button to enable/disable this option. When enabled, the router will reply to ping requests from other hosts on the Internet.	ON
Enable anti-denial of service attacks	Click the toggle button to enable/disable this option. When enabled, the router denies the service attack. The purpose of a denial of service attack is to attempt to prevent the intended user from using a machine or network resource.	ON
Enable WAN side IP forwarding	Click the toggle button to enable/disable this option. When enabled, the router allows packets from the WAN port to be forwarded to the LAN port gateway.	ON
Enable debug port	Click the toggle button to enable/disable this option.	ON
Enable VPN NAT Traversal	Click the toggle button to enable/disable this option.	OFF

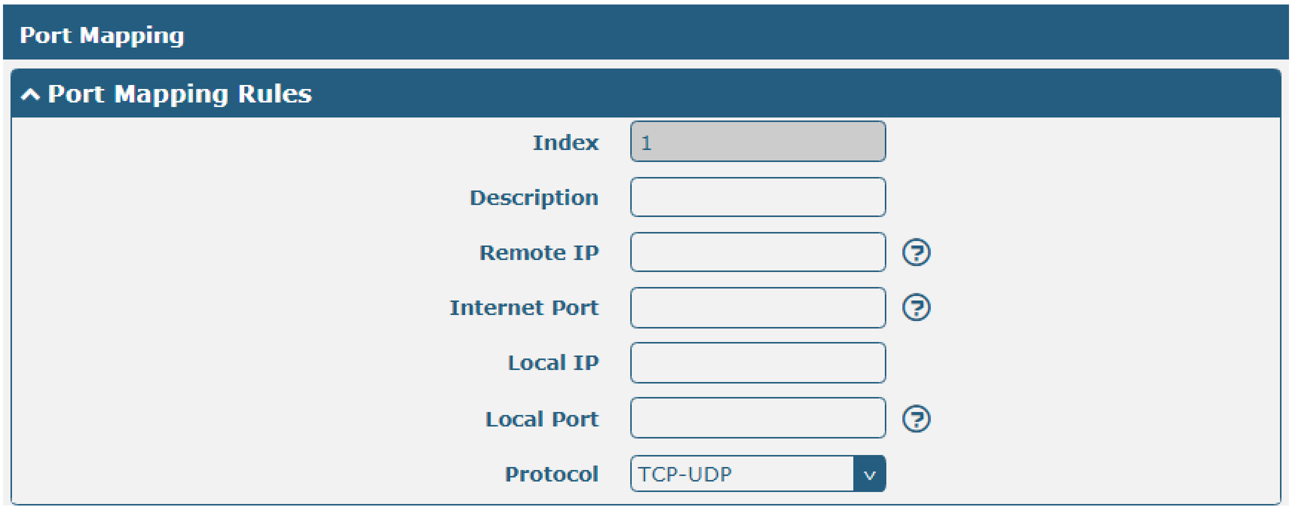
filter		
Option	**Description**	**default**
whitelist		
index	Indicate the ordinal of the list.	--
description	Enter a description of this filter rule or MAC binding rule.	null
source address	Specify an access source and enter itsource address. Note: The whitelist is used for HTTPS/HTTP/SSH/Telnet management and has a higher priority than access control HTTPS/HTTP/SSH/Telnet.	null
Filtering rules		
index	Indicate the ordinal of the list.	--
description	Enter a description of this filter rule or MAC binding rule.	null
source address	Specify an access source and enter itsource address.	null
Source port	Specify an access source and enter itSource port.	null
Source MAC address	Specify an access source and enter itSource MAC address.	null
target address	Enter the destination address to be accessed by the access source, which can be the IP device connected to the router.	null
Target port	Enter the target port to be accessed by the access source, which can be the IP device connected to the router.	null
protocol	Select the protocol used for access, including "All", "TCP", "UDP", "ICMP" or "TCP-UDP". **Note:**If you are not sure about the current access protocol, it is recommended to select "All".	All
action	Set the filtering rules for access, optionally accept or discard.	throw away

Port mapping meansManually defined in the router, all data received from certain ports on the public network are forwarded to a certain port of an IP on the internal network. Click Network > Firewall > Port Mapping to display the following:



Index	Description	Internet Port	Local IP	Local Port	Protocol

Click + Add up to 50 port mapping rules.



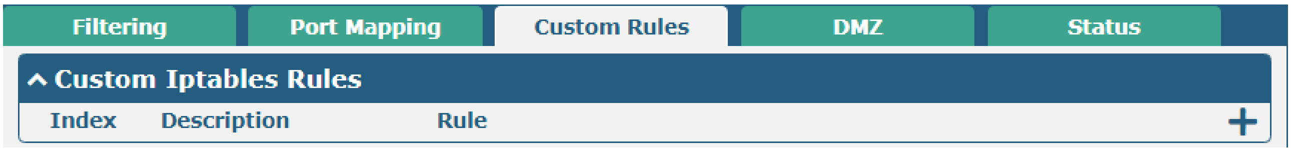
Port Mapping

^ Port Mapping Rules

Index	1
Description	
Remote IP	
Internet Port	
Local IP	
Local Port	
Protocol	TCP-UDP

Port mapping rule		
project	**Description**	**default**
index	Indicate the ordinal of the list.	--
description	Enter a description of this port mapping.	null
Remote IP address	Define a host or network that allows access to the local IP address, which is unlimited. For example: 10.10.10.10/255.255.255.255 or 192.168.1.0/24	null
network port	Enter the external port of the external network access router.	null
Local IP	Enter the IP address of the device you want to forward data to the intranet.	null
Local port	Enter the port number of the device you want to forward data to the intranet.	null
protocol	Select from "TCP", "UDP" or "TCP-UDP" depending on the application.	TCP-UDP

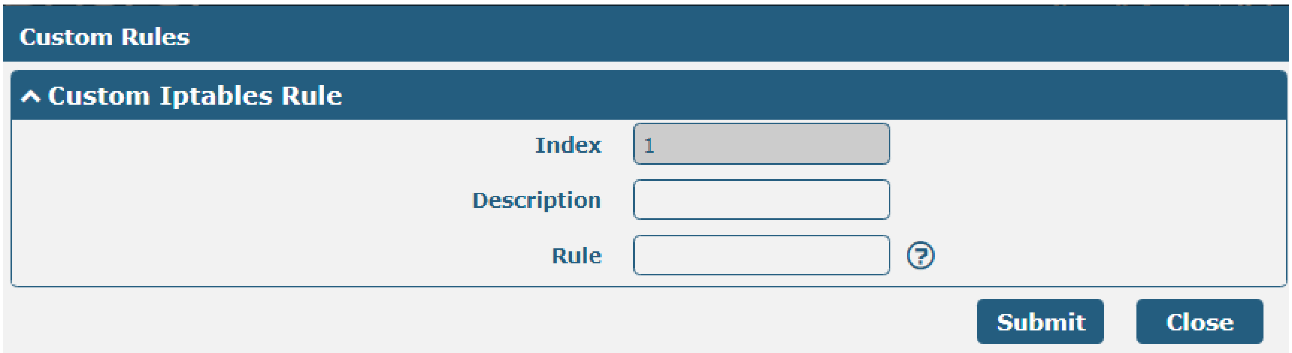
User accessible″Custom Rules″ add itselfAdd firewall rules.



^ Custom Iptables Rules

Index	Description	Rule

Click + Add a rule.



Custom Rules

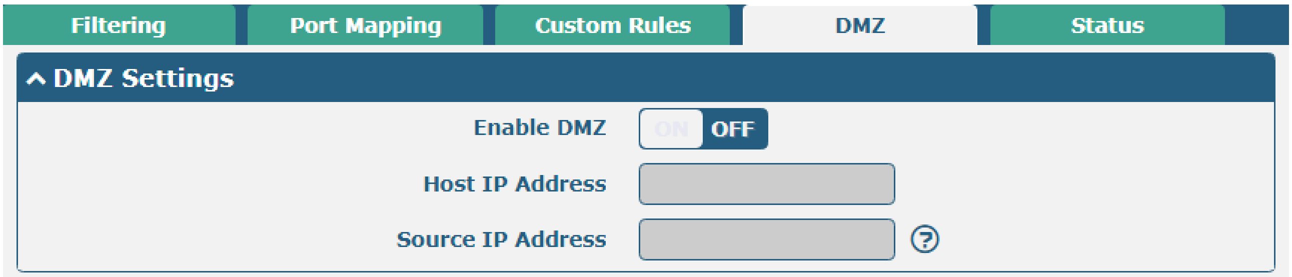
^ Custom Iptables Rule

Index	1
Description	
Rule	

Custom rule		
Option	**Description**	**default**
index	Indicate the ordinal of the list.	1
description	Show rule description.	null
rule	Display firewall rules.	null

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

Click Network > Firewall > DMZ to display the following:



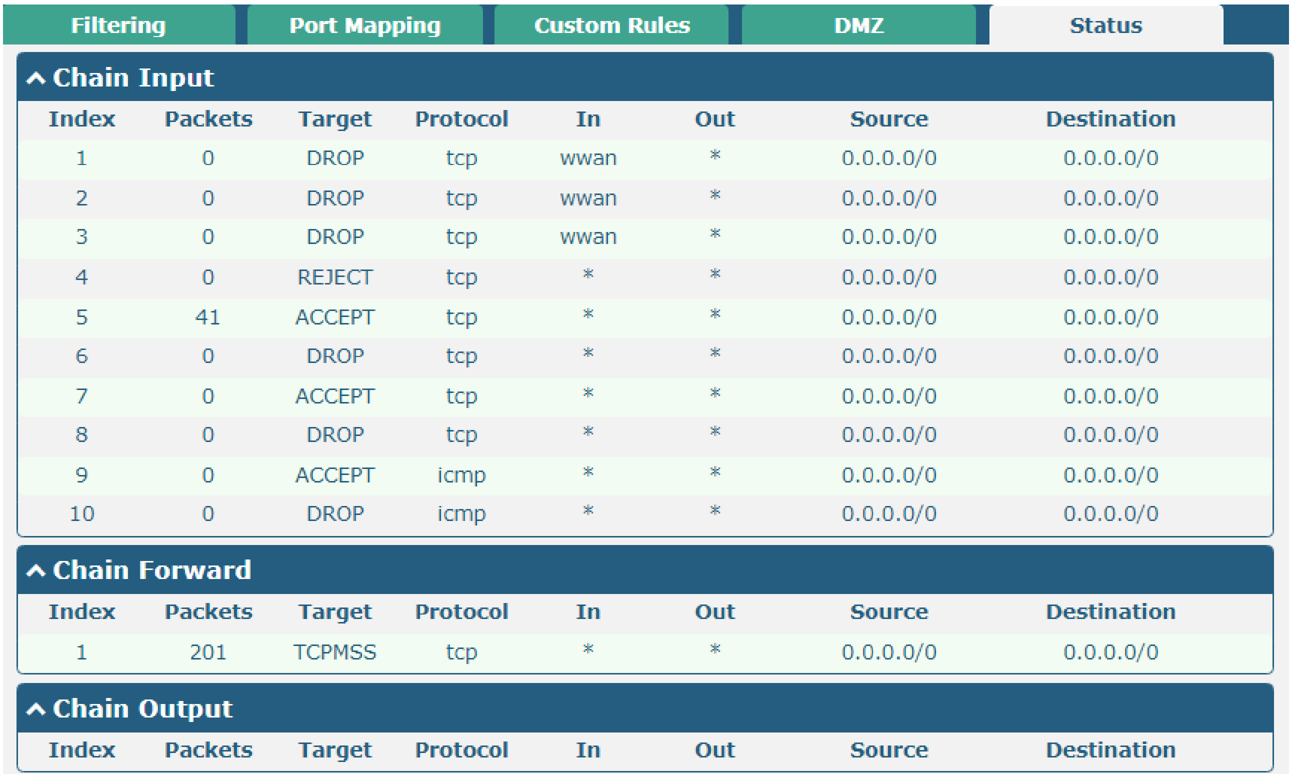
Enable DMZ ON OFF

Host IP Address

Source IP Address

DMZ settings		
Option	**Description**	**default**
Enable	Click the toggle button to enable/disable the DMZ feature.	OFF
Host IP address	Enter the IP address of the host in the internal network quarantine.	null
Source IP address	Set up a host that can talk to the DMZ host. 0.0.0.0 means that all addresses can talk to the DMZ.	nul

Click "Status" to see all the rules.



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	41	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

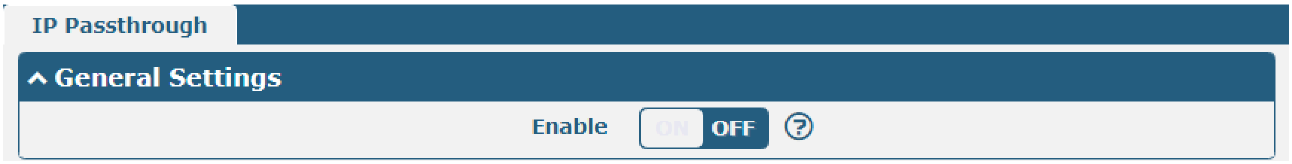
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	201	TCPMSS	tcp	*	*	0.0.0.0/0	0.0.0.0/0

Chain Output

Index	Packets	Target	Protocol	In	Out	Source	Destination

4.3.3 IP Passthrough

Click Network > IP Passthrough > IP Passthrough, and then click the toggle button to enable or disable the IP Passthrough feature.



General Settings

Enable ON OFF

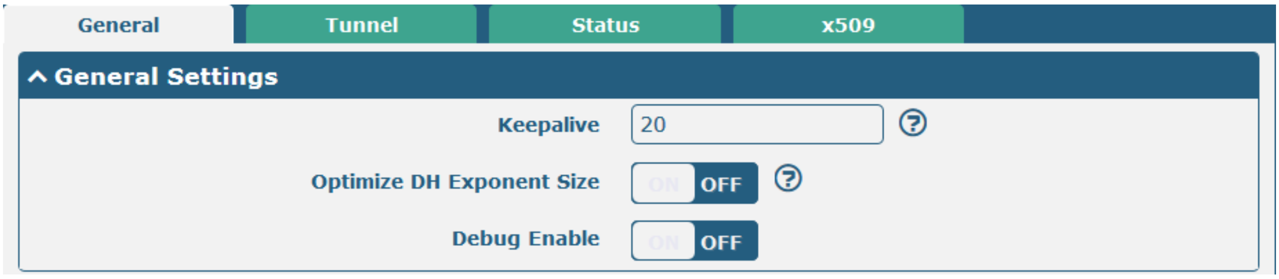
When the router turns on the IP Passthrough function, the terminal device (such as a PC) will open the DHCP Client mode and then connect to the LAN port of the router. After the router successfully dials the number, the PC will automatically obtain the IP address and DNS server address assigned by the operator.

4.4 Virtual private network

4.4.1 IPsec

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

Click Virtual Private Network > IPsec > GeneralTo set the IPsec parameters.



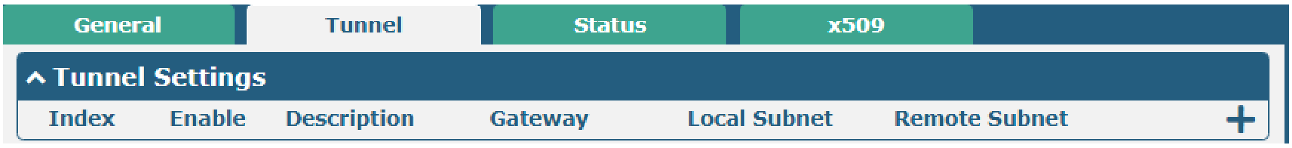
General Settings

Keepalive: 20

Optimize DH Exponent Size: ON OFF

Debug Enable: ON OFF

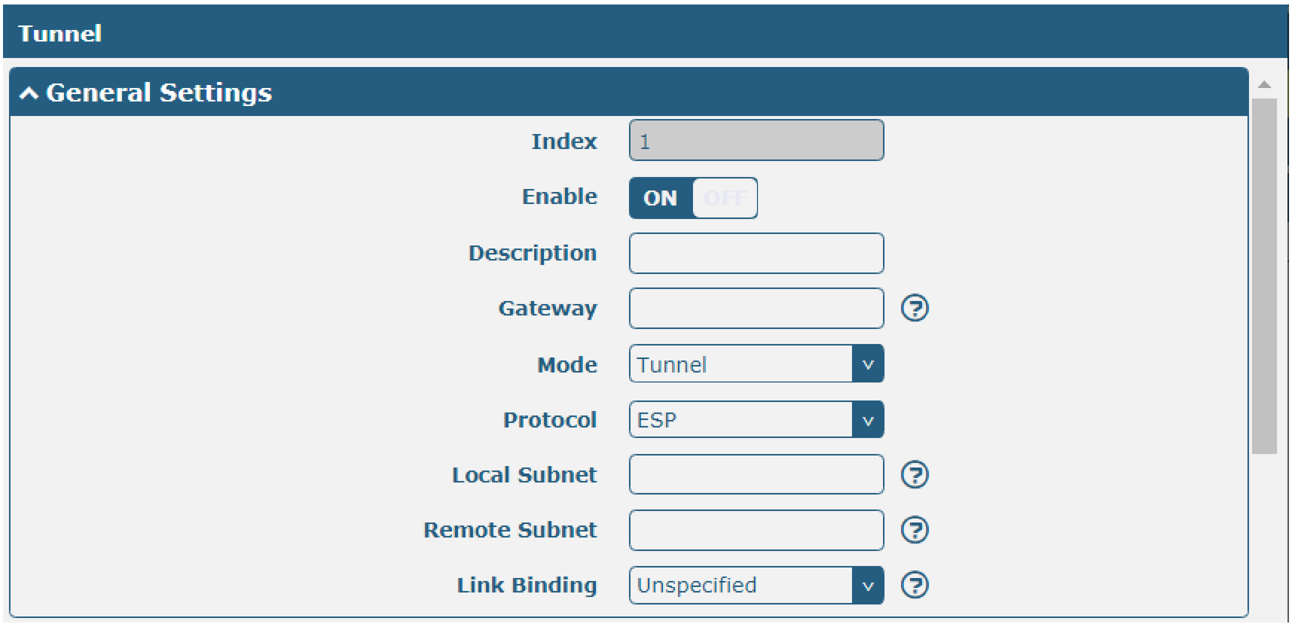
General Settings @General		
project	**Description**	**default**
Survival time	Set the time to live in seconds. The router sends keep-alive packets to the NAT (Network Address Translation) server at regular intervals to prevent the records on the NAT table from disappearing.	20
Optimize DH Exponent Size	Click the toggle button to enable/disable this option. When using DHgroup17 or DHgroup18, enabling this option can help shorten the time it takes to generate DH keys.	OFF
Output debugging information	Click the toggle button to enable/disable this option. Enable the debugging of IPsec VPN and output it to the debugging port.	OFF



Tunnel Settings

Index	Enable	Description	Gateway	Local Subnet	Remote Subnet

Click ➕ Add an IPsec tunnel and add up to six.



Tunnel

General Settings

Index: 1

Enable: ON OFF

Description:

Gateway:

Mode: Tunnel

Protocol: ESP

Local Subnet:

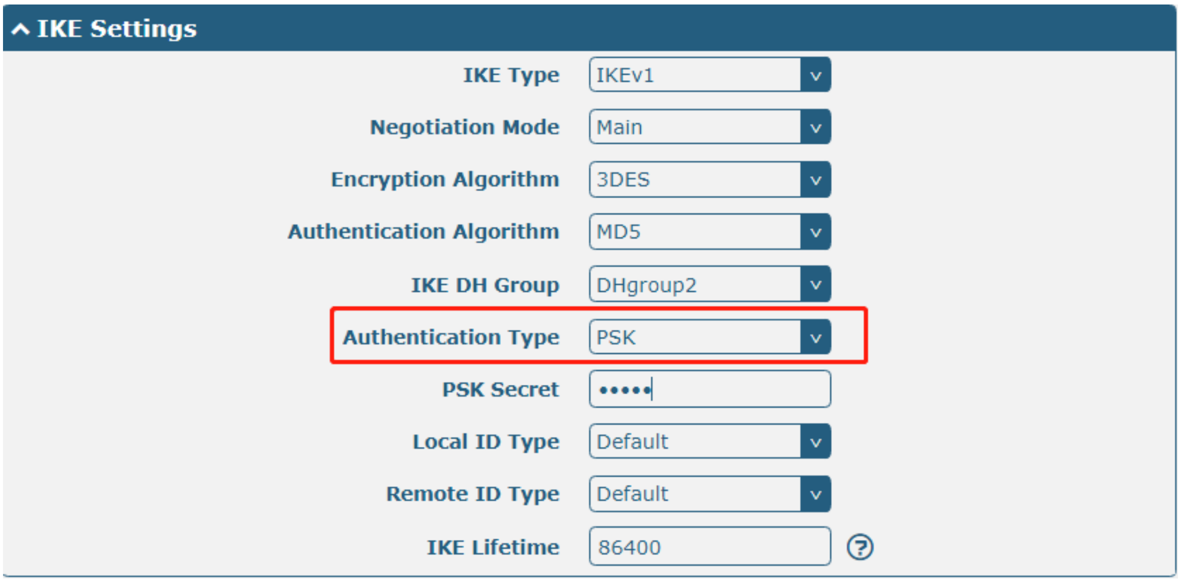
Remote Subnet:

Link Binding: Unspecified

General setting @隧道		
project	**Description**	**default**

General setting @隧道		
project	**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 of this IPsec tunnel.	null
Gateway	Enter the remote IPsec VPN server address. 0.0.0.0 means any address.	null
mode	Optional "tunnel" or "transfer". • Tunnel: Generally used between gateways or between terminals and gateways. The gateway acts as a proxy for the host behind it. • Transmission: used for communication between terminals or between terminals and gateways, such as establishing an encrypted Telnet connection between workstations and routers.	tunnel
protocol	Optional "ESP" or "AH" as a security protocol. • ESP: Using the ESP protocol • AH: Use the AH protocol	ESP
Local subnet	Enter the local subnet address and mask protected by IPsec. Local subnet mask, for example 192.168.1.0/24.	null
Remote subnet	Enter the remote subnet address and mask protected by IPsec. Remote subnet mask, for example 10.8.0.0/24.	null

In the IKE settings window, when the authentication type selects "PSK", the window is displayed as follows:



^ IKE Settings

IKE Type: IKEv1

Negotiation Mode: Main

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

IKE DH Group: DHgroup2

Authentication Type: PSK

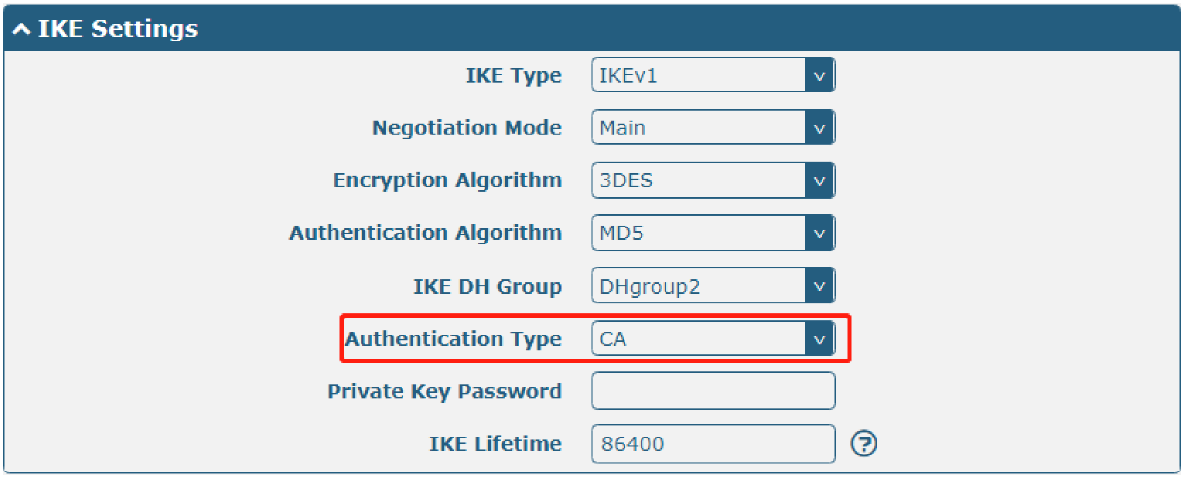
PSK Secret: •••••

Local ID Type: Default

Remote ID Type: Default

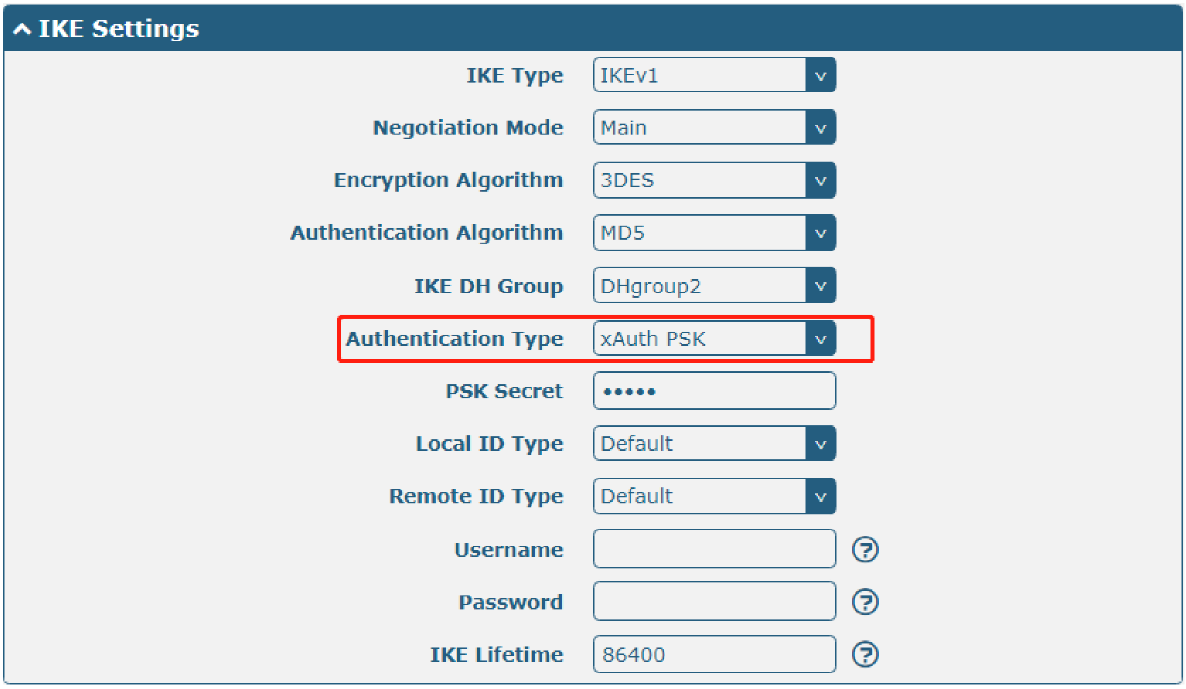
IKE Lifetime: 86400

When the authentication type selects "CA", the window is displayed as follows:



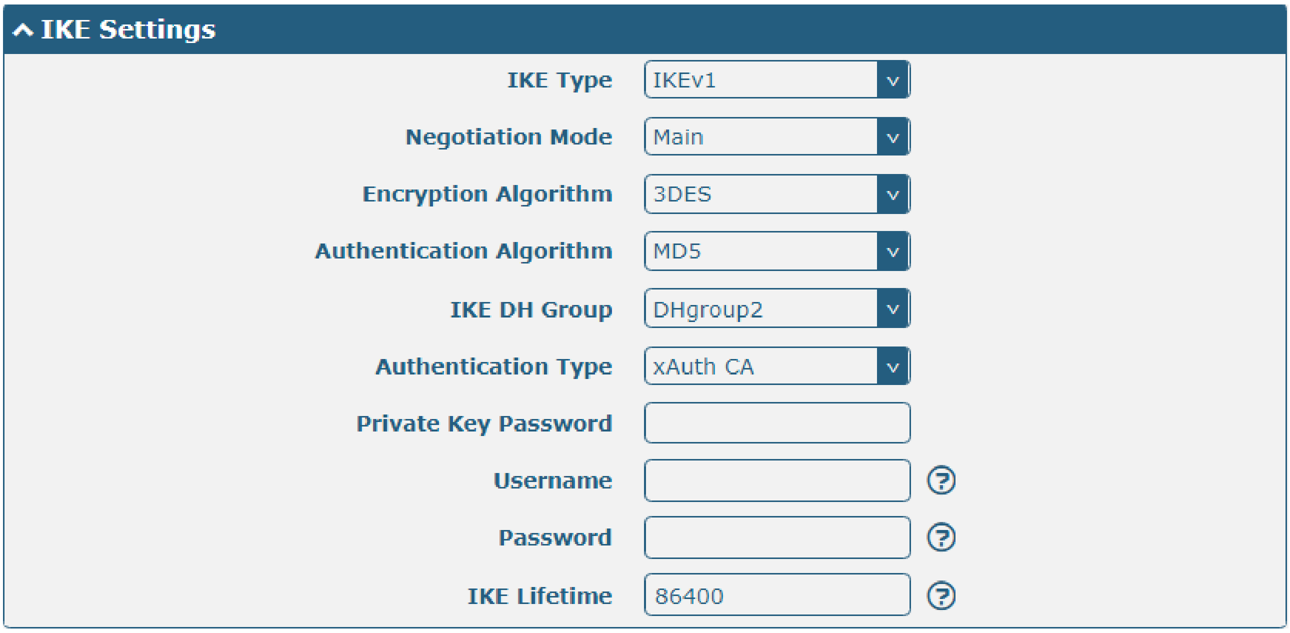
IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	MD5
IKE DH Group	DHgroup2
Authentication Type	CA
Private Key Password	
IKE Lifetime	86400

When the authentication type selects "xAuth PSK", the window is displayed as follows:



IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	MD5
IKE DH Group	DHgroup2
Authentication Type	xAuth PSK
PSK Secret	•••••
Local ID Type	Default
Remote ID Type	Default
Username	
Password	
IKE Lifetime	86400

When the authentication type is selected "xAuth CAWhen the window is displayed as follows:



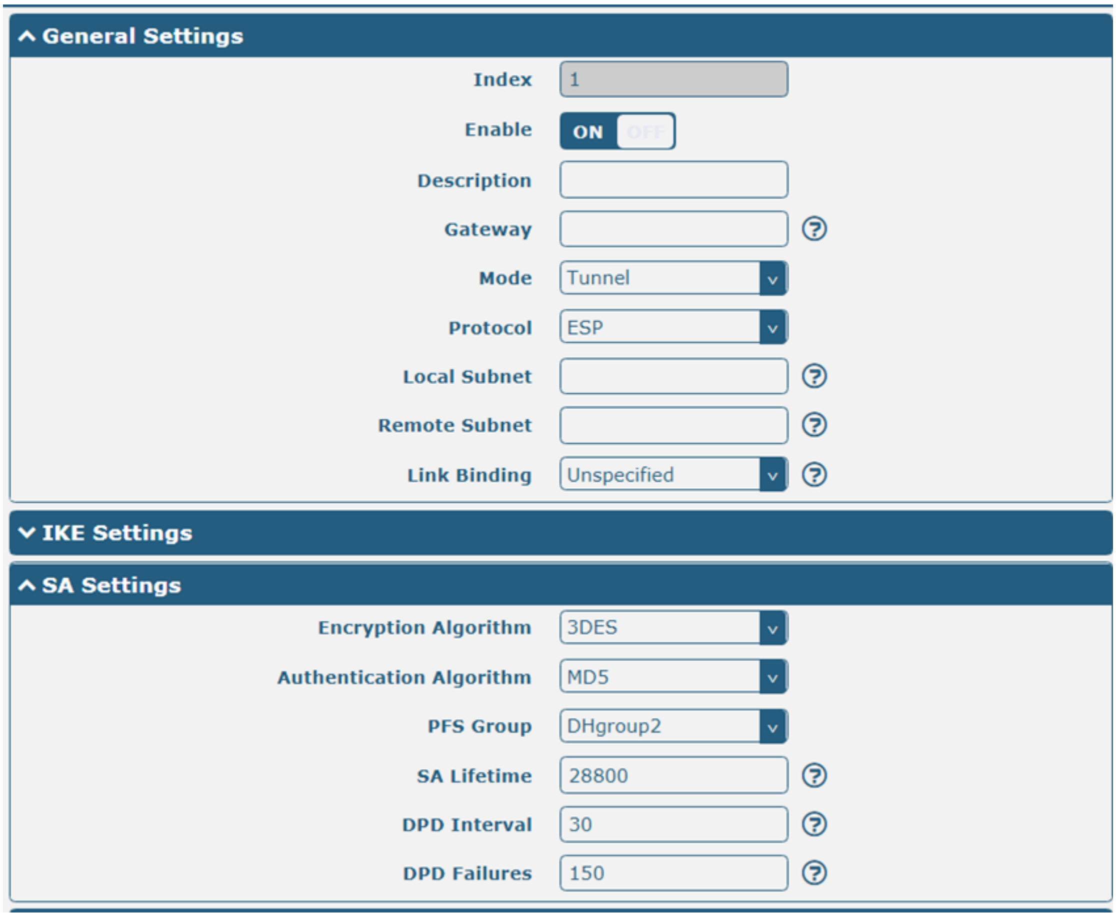
^ IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	MD5
IKE DH Group	DHgroup2
Authentication Type	xAuth CA
Private Key Password	
Username	
Password	
IKE Lifetime	86400

IKE settings		
project	**Description**	**default**
IKE type	You can select "IKEv1" and "IKEv2".	IKEv1
Negotiation mode	Select the negotiation mode of IKE (Network Key Exchange) from "Main Mode" and "Savage Mode". If the IP address of an IPsec tunnel is obtained automatically, you must select the aggressive mode as the IKE (Network Key Exchange) negotiation mode. In this case, the SA negotiation can be established as long as the username and password are correct.	Main mode
Authentication method	The authentication algorithm is selected from "MD5", "SHA1", "SHA2 256", and "SHA2 512" to be applied to IKE (Network Key Exchange) negotiation.	MD5
Encryption Algorithm	The encryption algorithm selected from "3DES", "AES128", "AES192", and "AES256" is applied in IKE (Network Key Exchange) negotiation. • 3DES: Using 168-bit 3DES encryption algorithm • AES128: Using 128-bit AES encryption algorithm • AES192: Using 192-bit AES encryption algorithm • AES256: Using 256-bit AES encryption algorithm	3DES
IKE DH grouping	The DH packet is selected for IKE (Network Key Exchange) negotiation. You can select DHgroup1, DHgroup2, DHgroup5, DHgroup14, DHgroup15, DHgroup16, DHgroup17, or DHgroup18.	DHgroup2
Authentication type	The authentication type is selected from "PSK", "CA", "xAuth PSK" and "xAuth CA" to be applied to IKE negotiation. • PSK: Pre-shared key • CA: x509 certificate authentication • xAuth: Extended authentication for AAA servers	PSK

IKE settings		
project	**Description**	**default**
PSK key	Enter the PSK key.	null
Local ID type	Select from "Default", "FQDN" or "User FQDN". • Default: IP address is selected by default • FQDN: Fully Qualified Domain Name, which is the official domain name. In the IKE negotiation, the FQDN is used as the local ID. If you select this option, you need to remove the domain name and then enter it, such as test.robustel.com. • User FQDN: Use the user FQDN as the local ID in IKE negotiation; if you select this option, you must bring @, such as test@robustel.com	default
Remote ID type	Select from "Default", "FQDN" or "User FQDN". • Default: IP address is selected by default • FQDN: Fully Qualified Domain Name, which is the official domain name. In the IKE negotiation, the FQDN is used as the remote ID. If you select this option, you need to remove the domain name and then enter it, such as test.robustel.com. • User FQDN: Use the user FQDN as the remote ID in IKE negotiation; if you select this option, you must bring @, such as test@robustel.com	default
IKE survival time	Set the lifetime in IKE negotiation. Before the SA expires, IKE negotiates a new SA; once the new SA is established, it will take effect immediately; the old one will be cleared immediately after expiration.	86400
Key password	Enter CA andxAuth CAThe key password under authentication.	null
username	InputxAuth PSK and xAuth CAUsername under authentication.	null
password	Enter the password for xAuth PSK and xAuth CA authentication.	null

When the protocol in "Virtual Private Network > IPsec > Tunnel > General Settings" selects "ESP", the SA settings are displayed as follows:



General Settings

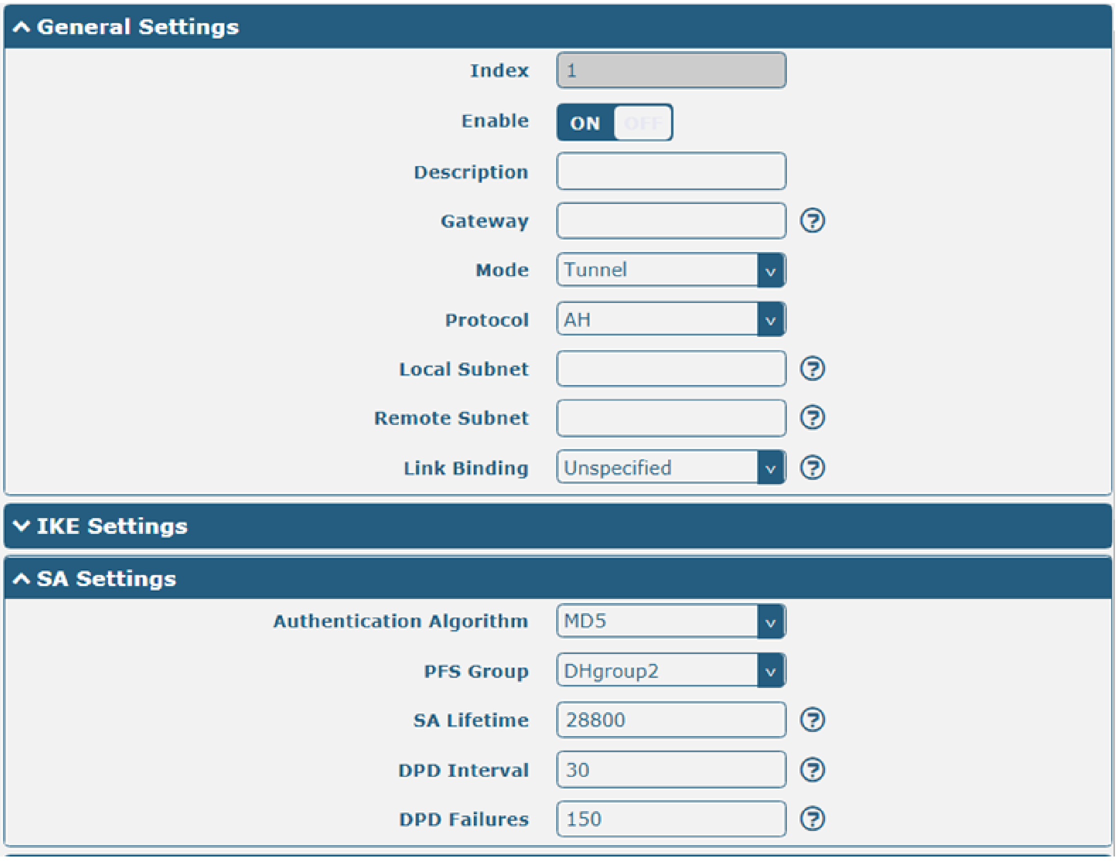
Index	1
Enable	ON OFF
Description	
Gateway	
Mode	Tunnel
Protocol	ESP
Local Subnet	
Remote Subnet	
Link Binding	Unspecified

IKE Settings

SA Settings

Encryption Algorithm	3DES
Authentication Algorithm	MD5
PFS Group	DHgroup2
SA Lifetime	28800
DPD Interval	30
DPD Failures	150

When the protocol in "Virtual Private Network > IPsec > Tunnel > General Settings" selects "AH", the SA settings are displayed as follows:



General Settings

Index	1
Enable	ON OFF
Description	
Gateway	
Mode	Tunnel
Protocol	AH
Local Subnet	
Remote Subnet	
Link Binding	Unspecified

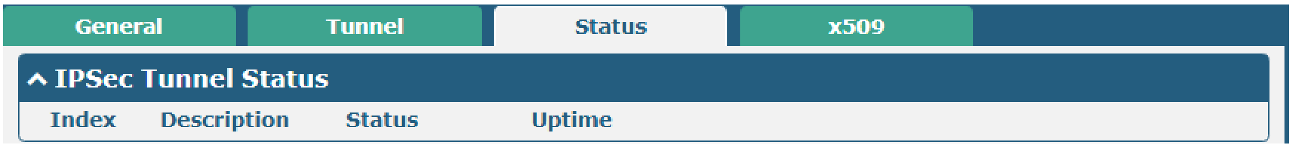
IKE Settings

SA Settings

Authentication Algorithm	MD5
PFS Group	DHgroup2
SA Lifetime	28800
DPD Interval	30
DPD Failures	150

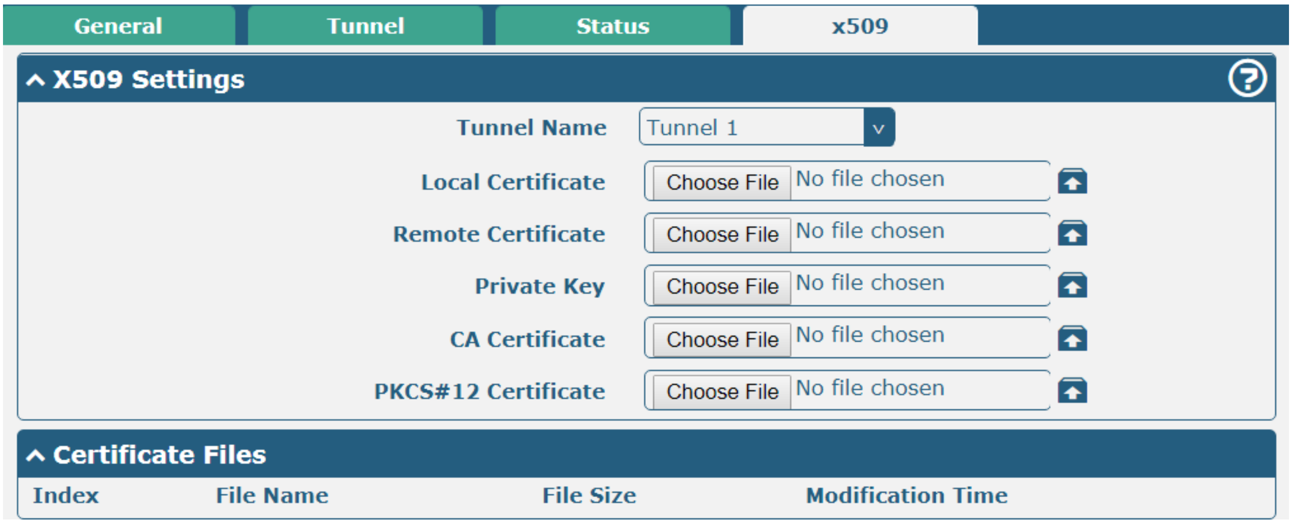
SA settings		
project	**Description**	**default**
Encryption Algorithm	When "ESP" is selected in "Protocol", "3DES", "AES192", "AES128" or "AES256" can be selected. Higher security means more complex implementations and lower rates. DES can meet general needs, and 3DES is chosen for higher security and confidentiality requirements.	3DES
Authentication method	The authentication algorithm selected from "MD5", "SHA1", "SHA2 256", and "SHA2 512" is applied to the SA negotiation phase.	MD5
PFS group	Select from PFS (N/A), DHgroup1, DHgroup2, DHgroup5, DHgroup14, DHgroup15, DHgroup16, DHgroup17, or DHgroup18.	DHgroup2
DPD interval	Set the interval time. If the IPsec protection packet is not received from the peer end, the DPD will be triggered after the interval has elapsed. DPD is a failed peer detection that irregularly detects whether the peer of IKE (Internet Key Exchange) has failed. When the local terminal receives the IPsec packet, the DPD detects the last time the IPsec packet was received from the peer. If the time exceeds the DPD interval, it will send a DPD hello packet to the peer. If the local terminal does not receive a DPD acknowledgment within the DPD packet return time, it will retransmit the DPD hello packet. If the local terminal sends a DPD hello packet that exceeds the maximum number of retransmission attempts and does not receive the DPD acknowledgment, the peer is considered invalid. The IKE SA and IKE SA-based IPsec SAs are cleared.	30
DPD failures	Set the timeout period for the DPD (Failed Peer Detection) packet.	150
advanced settings		
Enable compression	Click the toggle button to enable/disable this option. When enabled, this feature compresses the header of the IP packet.	OFF
Expert option	Add more configuration options for PPP. Format: config-desc; config-desc, such as protostack=netkey;plutodebug=none	Null

This section is used to view the connection status of IPsec.



Index	Description	Status	Uptime

This section is used to import certificates such as CA.

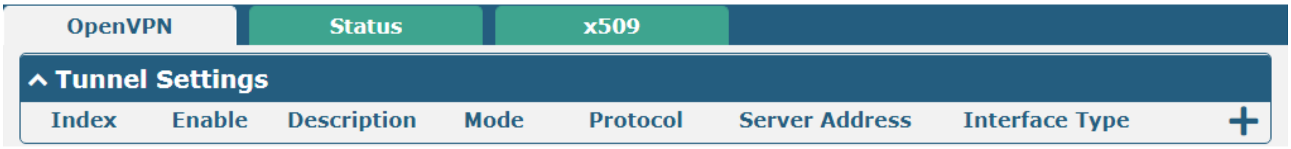


x509		
Option	**Description**	**default**
X509 settings		
Tunnel name	Choose a valid tunnel.	Tunnel 1
Local certificate	Import the certificate file from the local to the router. The correct certificate file format is as follows: @ ca.crt @remote.crt @local.crt @private.key @ crl.pem	--
Peer certificate	Select the peer certificate to import to the router.	--
Private key	Select the private key to import to the router.	--
CA Certificate	Select the CA certificate to import to the router.	--
Certificate file		
index	Indicate the ordinal of the list.	--
file name	Displays the certificate name of the imported router.	null
File size	Displays the size of the current file.	null
Last Modified	Displays the timestamp of the last modified certificate.	null

4.4.2 OpenVPN

This section is used to set the parameters of Open VPN. OpenVPN is an open source SSL-based VPN system. The router's OpenVPN feature supports point-to-point and point-to-multipoint (client) VPN tunnels.

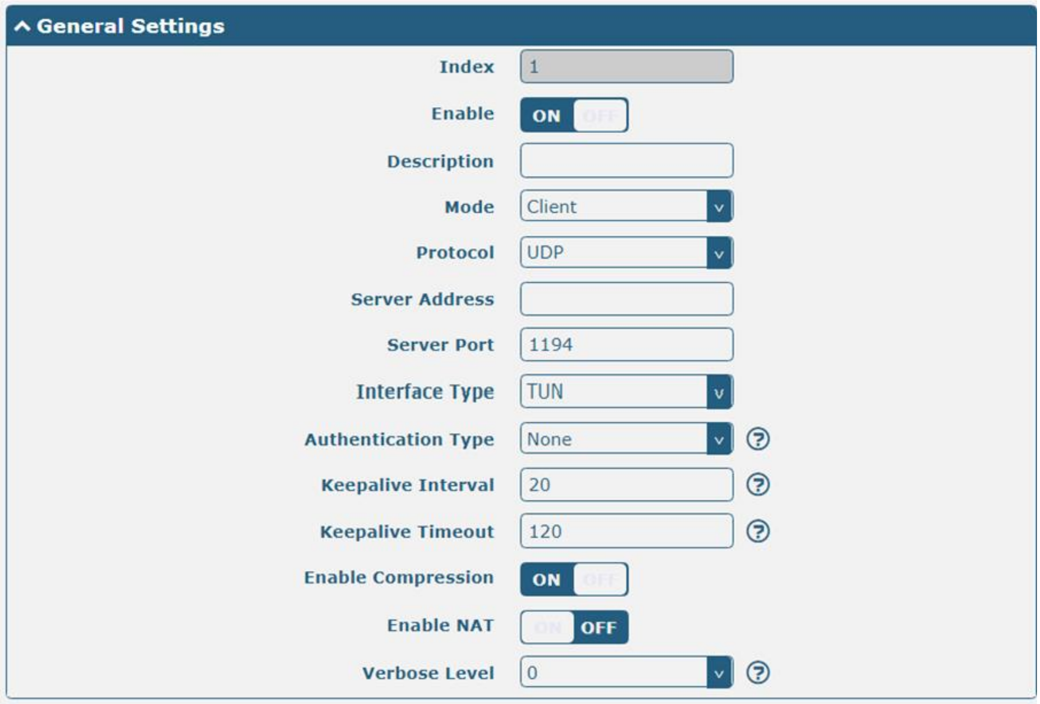
Click Virtual Private Network > OpenVPN > OpenVPN to display the following:



Tunnel Settings

Index	Enable	Description	Mode	Protocol	Server Address	Interface Type	+

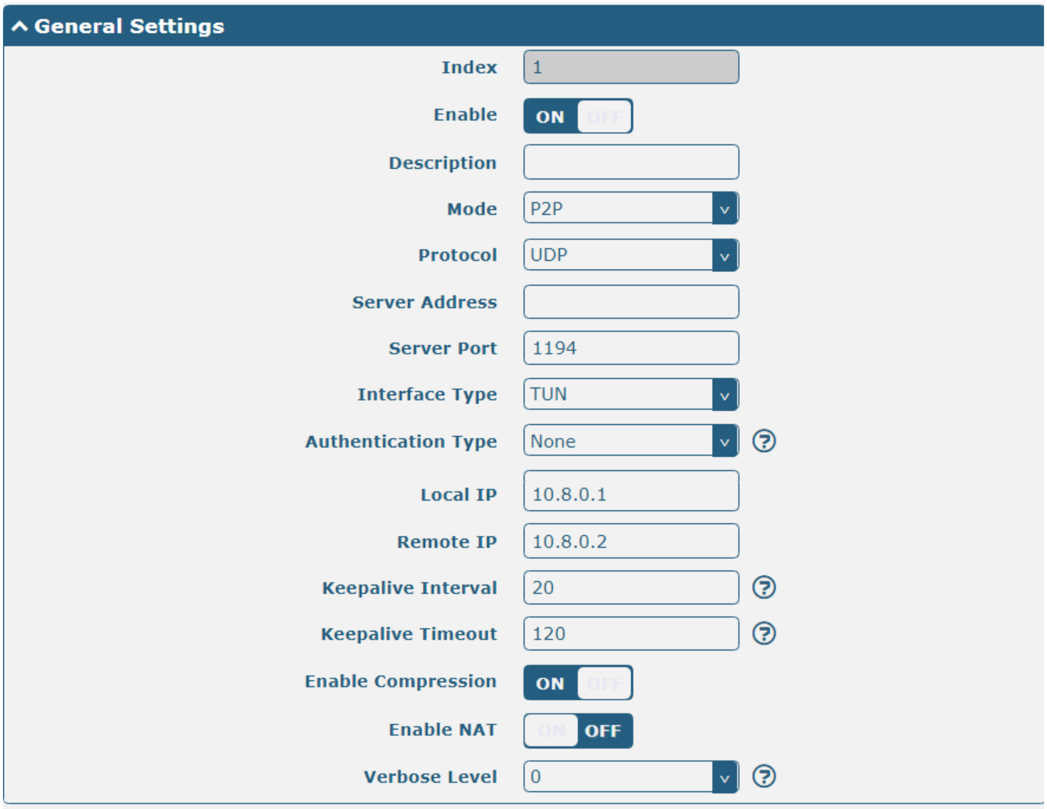
Click + To add an OpenVPN tunnel, you can add up to five. The mode defaults to "client" and looks like this:



General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	None
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

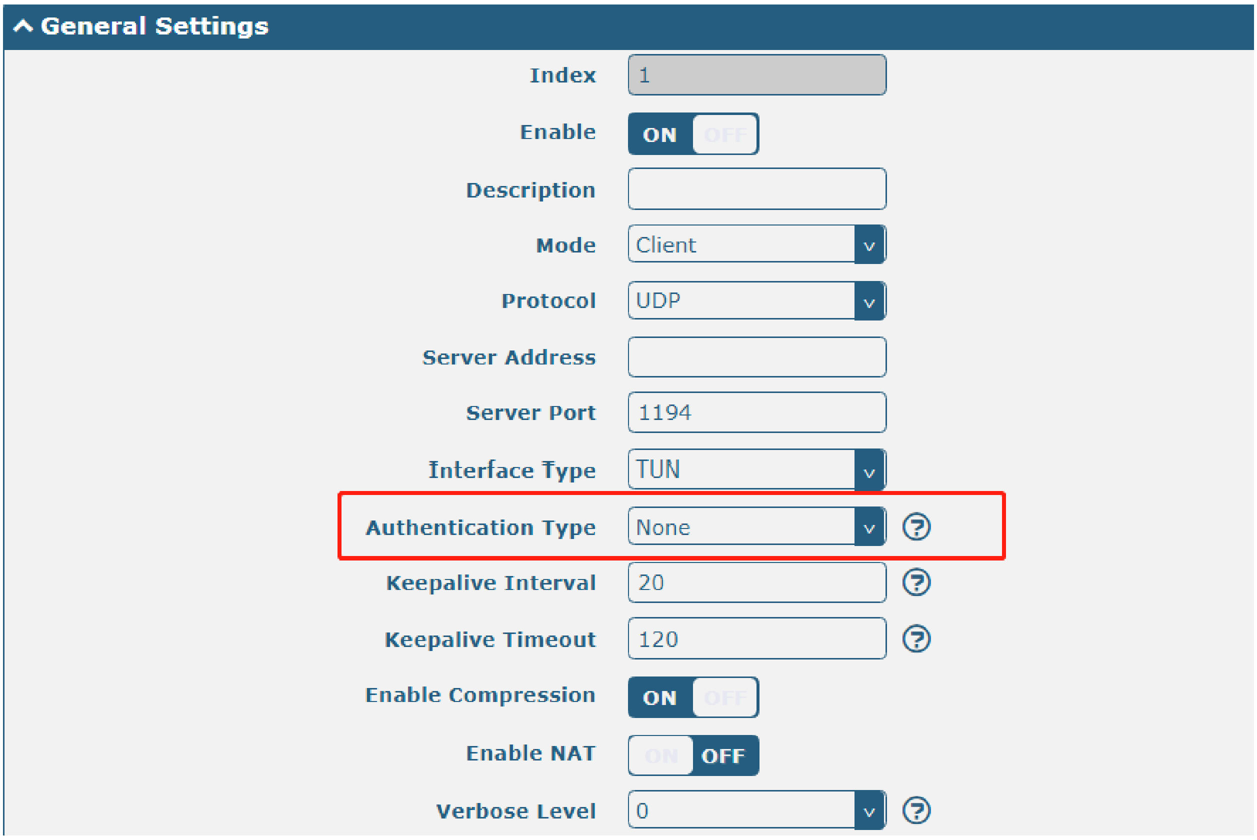
When the mode selects "P2P", the window is displayed as follows:



General Settings

Index	1
Enable	ON
Description	
Mode	P2P
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	None
Local IP	10.8.0.1
Remote IP	10.8.0.2
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

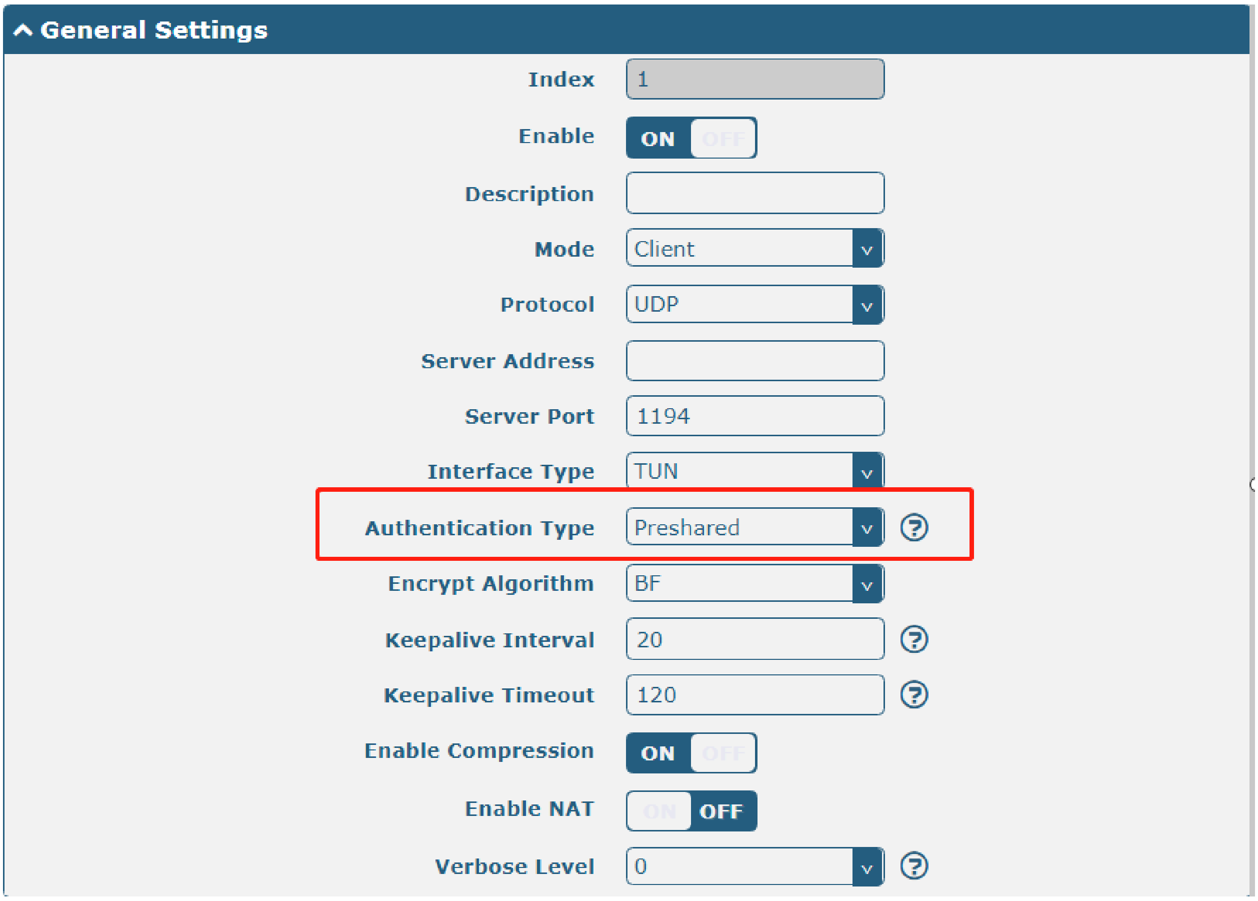
When the verification mode is "None", the window is displayed as follows:



General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	None
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

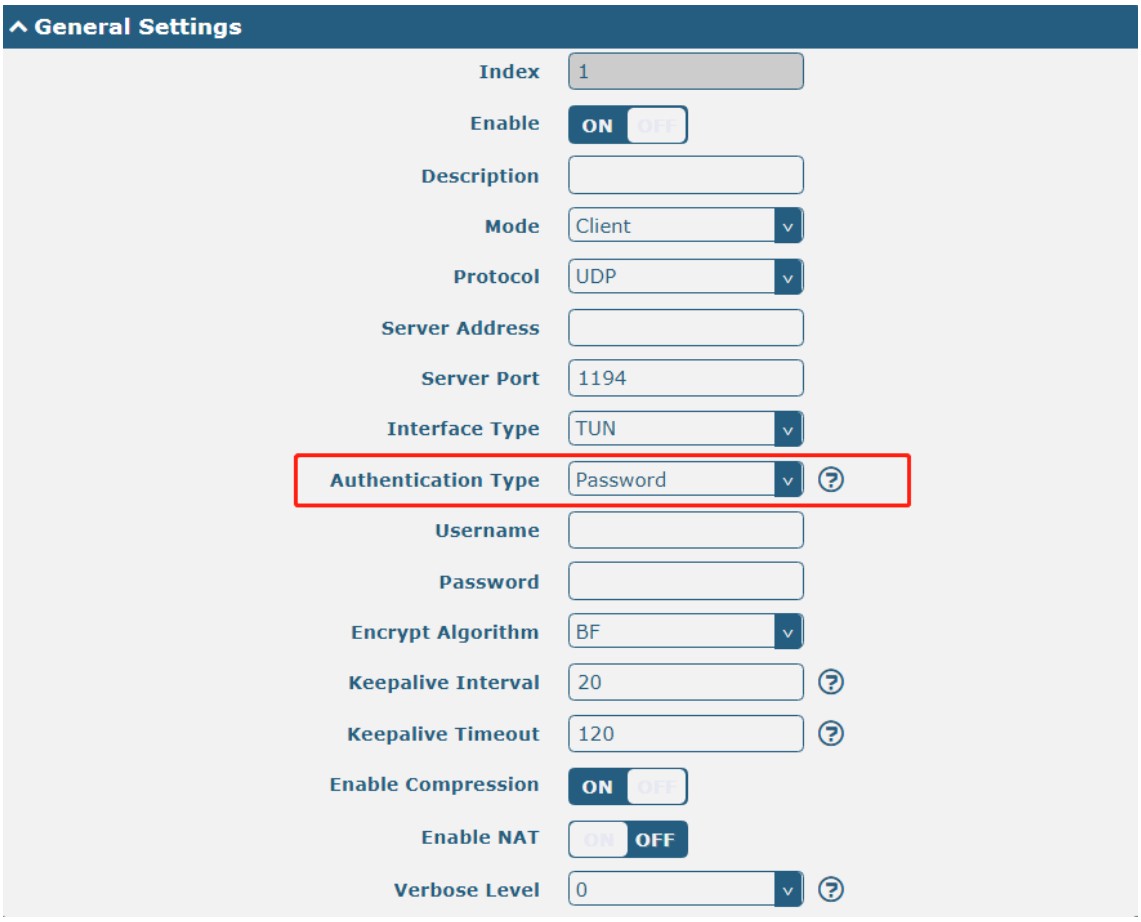
When "Authentication Mode" selects "Pre-Share Key", the window displays as follows:



General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	Preshared
Encrypt Algorithm	BF
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

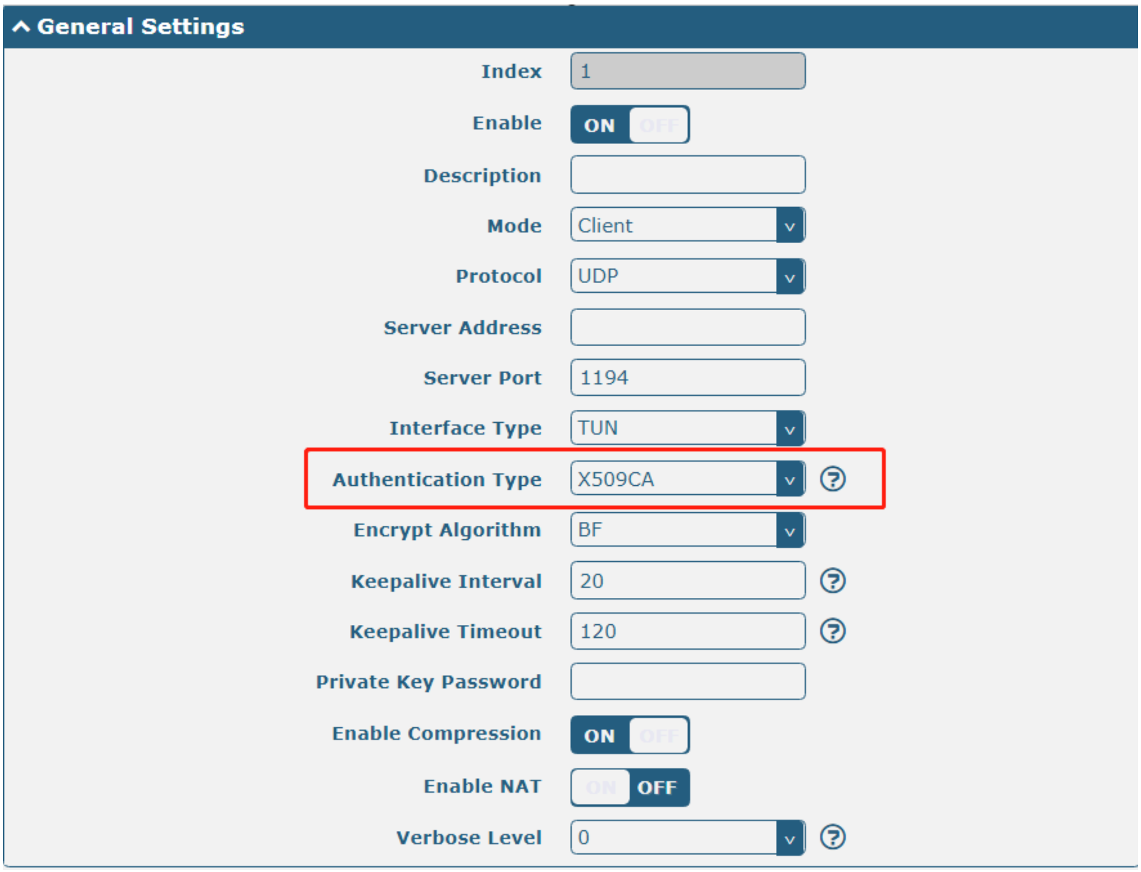
When the authentication method selects "Password", the window displays as follows:



^ General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	Password
Username	
Password	
Encrypt Algorithm	BF
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

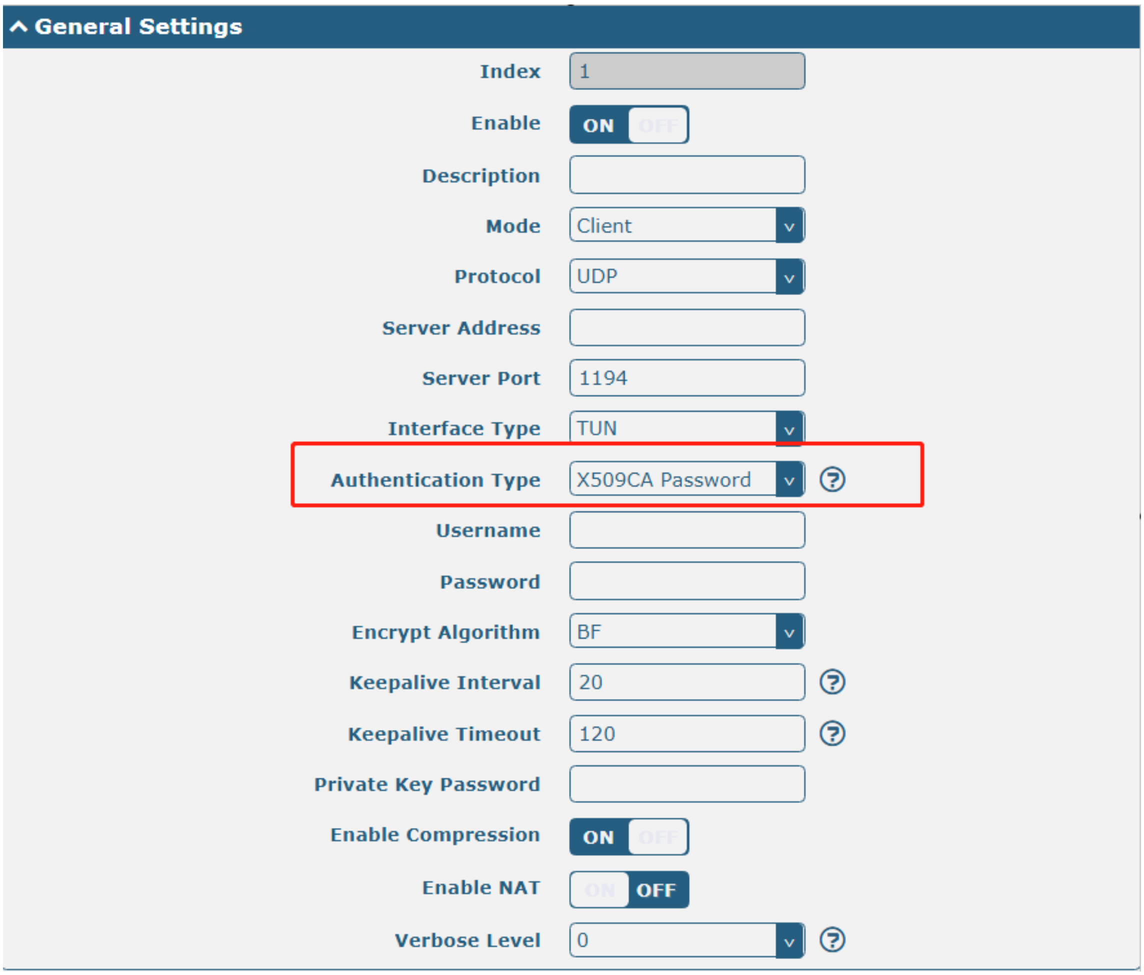
When "X509CA" is selected for "Authentication Method", the window is displayed as follows:



^ General Settings

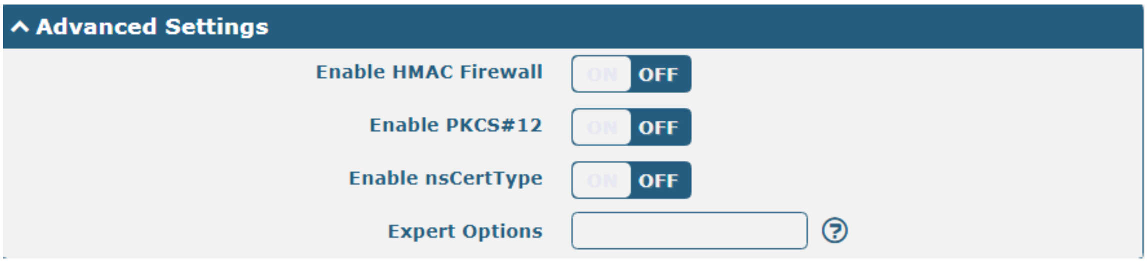
Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	X509CA
Encrypt Algorithm	BF
Keepalive Interval	20
Keepalive Timeout	120
Private Key Password	
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

When "Authentication Method" selects "X509CA Password", the window displays as follows:



General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	X509CA Password
Username	
Password	
Encrypt Algorithm	BF
Keepalive Interval	20
Keepalive Timeout	120
Private Key Password	
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0



Advanced Settings

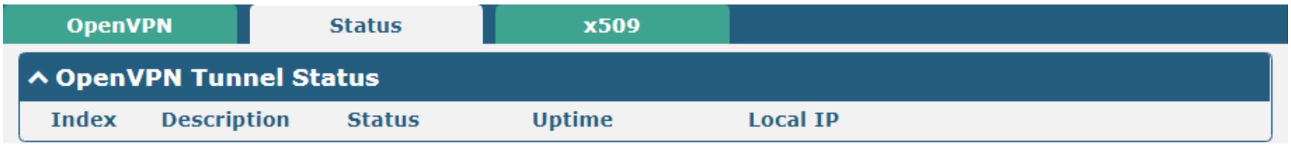
Enable HMAC Firewall	OFF
Enable PKCS#12	OFF
Enable nsCertType	OFF
Expert Options	

OpenVPN		
project	**Description**	**default**
General settings		
index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable the OpenVPN client.	ON
description	Enter a description of the OpenVPN.	null
mode	Select "P2P" or "Client".	Client
protocol	Select from "UDP", "TCP Client" or "TCP Server" depending on the application requirements.	UDP
server address	Enter the peer IP address or the domain name of the remote OpenVPN server.	null

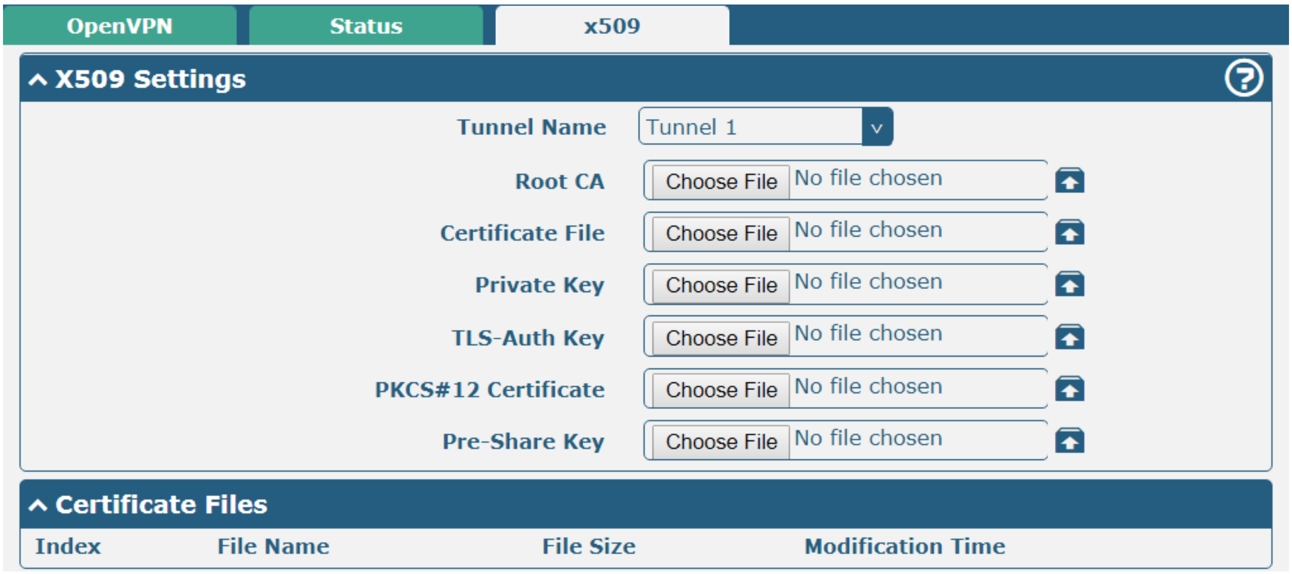
OpenVPN		
project	**Description**	**default**
Server port	Enter the listening port of the peer or OpenVPN server.	1194
Interface Type	Select "TUN" or "TAP". The difference between TUN and TAP is that the TUN device is a point-to-point virtual device at the network layer, and the TAP is a virtual device at the Ethernet link layer.	DO
Ways of identifying	Select from None, Pre-Share Key, Password, X509CA, and X509CA Password. **Note**: "None" and "Pre-shared Key" are only available in P2P mode.	no
username	Enter the username for the "Password" or "X509CA Password" authentication method.	null
password	Enter the password for both the "password" or "X509CA password" authentication method.	null
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
Encryption Algorithm	Optional "BF", "DES", "DES-EDE3", "AES128", "AES192" and "AES256". • BF: 128-bit encryption algorithm using BF in CBC mode • DES: 64-bit encryption algorithm using DES in CBC mode • DES-EDE3: 192-bit encryption algorithm using 3DES in CBC mode • AES128: 128-bit encryption algorithm using AES in CBC mode • AES192: AES's 192-bit encryption algorithm in CBC mode • AES256: AES 256-bit encryption algorithm in CBC mode	BF
Keep alive interval	Set the ping interval for checking whether the tunnel is disconnected.	20
Keep alive timeout	Set the keep alive timeout. If the connection is timed out during this time, the OpenVPN tunnel will be re-established.	120
Private key password	Enter the private key password in the "X509CA" and "X509CA Password" authentication mode.	null
Enable compression	Click the toggle button to enable/disable this option. When enabled, this feature compresses the header of the IP packet.	ON
Enable NAT	Click the toggle button to enable/disable the NAT (Network Address Translation) feature. When turned on, the host IP behind the router will be encapsulated.	OFF
Detailed level	Select the output log information level, the value is 0.~11. • 0: only output fatal error message • 1~4: normal use range • 5: Output data packet transmission and reception information • 6~11: Debug information range	0
advanced settings		
Enable HMAC firewall	Click the toggle button to enable/disable this option. Add additional HMAC (Hash Message AuthEntication Code) authentication at the	OFF

OpenVPN		
project	Description	default
	top of the TLS control channel to protect the link against DoS attacks.	
Enable PKS#12	Click the toggle button to enable/disable the PKCS#12 certificate. PKS#12, a digital certificate encryption standard used to identify personally identifiable information.	OFF
EnablensCertType	Click the toggle button to enable/disablensCertType, which specifies the server verification mode. Server opennsCertType, the OpenVPN client also needs to be configured consistently.	OFF
Expert option	Enter some other PPP-initiated strings in this field. Each string is separated by a space.	null

In the status bar, you can view the connection status of OpenVPN.



This section is used to import certificates such as CA.



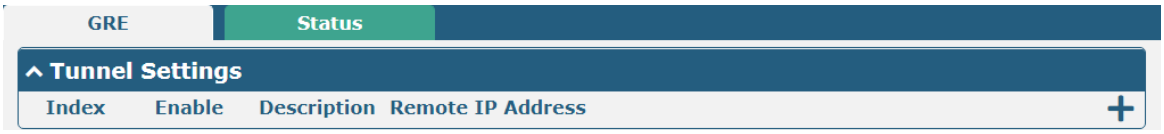
Tunnel Name: Tunnel 1
Root CA: Choose File No file chosen
Certificate File: Choose File No file chosen
Private Key: Choose File No file chosen
TLS-Auth Key: Choose File No file chosen
PKCS#12 Certificate: Choose File No file chosen
Pre-Share Key: Choose File No file chosen

x509		
project	Description	default
X509 settings		
Tunnel name	Choose a valid tunnel.	Tunnel 1
Root certificate	Select the correct root certificate to import into the router. The correct certificate file format is as follows: @ ca.crt @remote.crt	null

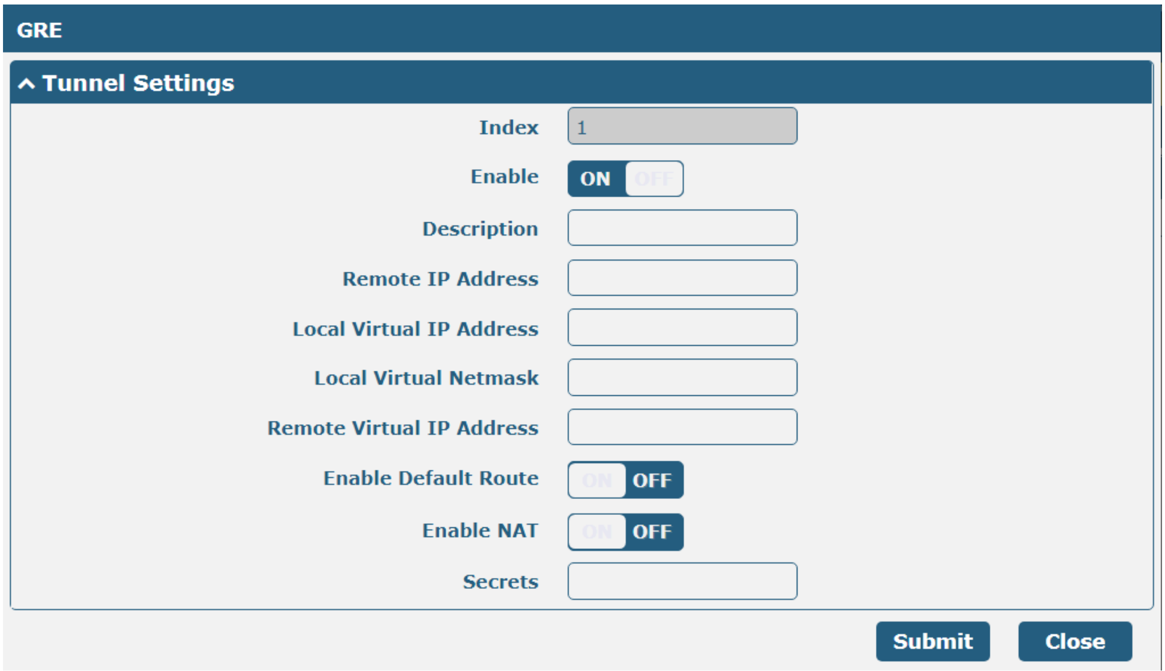
	@local.crt @private.key @ crl.pem @ client.p12	
Certificate file	Select the certificate file to import to the router.	null
Private key	Select the key to import to the router.	null
TLS-Auth key	selectThe TLS-Auth key is imported to the router.	null
PKCS#12 certificate	selectThe PKCS#12 certificate is imported to the router.	null
Pre-shared key	Select the pre-shared key to import to the router.	null
Certificate file		
index	Indicate the ordinal of the list.	--
file name	Show the certificate name of the imported router.	null
File size	Show the size of the current file.	null
Last Modified	Show the timestamp of the last modified certificate.	null

4.4.3 GRE

This section is used to set the GRE parameters. GRE (Generic Routing Encapsulation), a general routing protocol encapsulation, specifies how to encapsulate another network protocol with one network protocol. The main uses of the GRE protocol are two: enterprise internal protocol encapsulation and private address encapsulation.



Click + To add a GRE tunnel, you can add up to five.



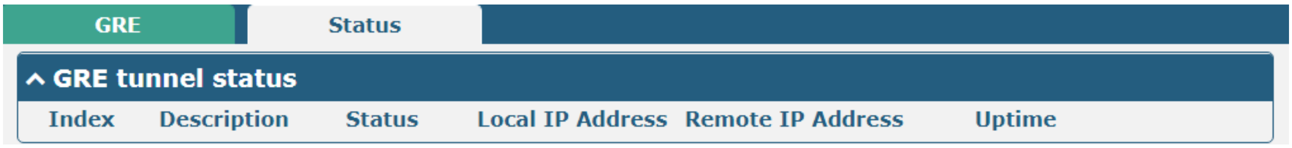
GRE

^ Tunnel Settings

Index	1
Enable	ON
Description	
Remote IP Address	
Local Virtual IP Address	
Local Virtual Netmask	
Remote Virtual IP Address	
Enable Default Route	OFF
Enable NAT	OFF
Secrets	

Tunnel setting @GRE		
project	**Description**	**default**
index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable GRE. GRE (Generic Routing Encapsulation) is a packaged packet protocol to enableIPRouting packets from other protocols in the network.	ON
description	Enter a description of 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 subnet mask	Set the local virtual subnet mask of the GRE tunnel.	null
Remote virtual IP address	Set the virtual IP address of the remote end of the GRE tunnel.	null
Enable default route	Click the toggle button to enable/disable this option. When enabled, all data traffic is sent through the GRE tunnel.	OFF
Enable NAT	Click the toggle button to enable/disable NAT (Network Address Translation) traversal. This option must be enabled in a NAT (Network Address Translation) environment.	OFF
password	Set the GRE tunnel key.	null

Click the Status bar to view the connection status of the GRE VPN.



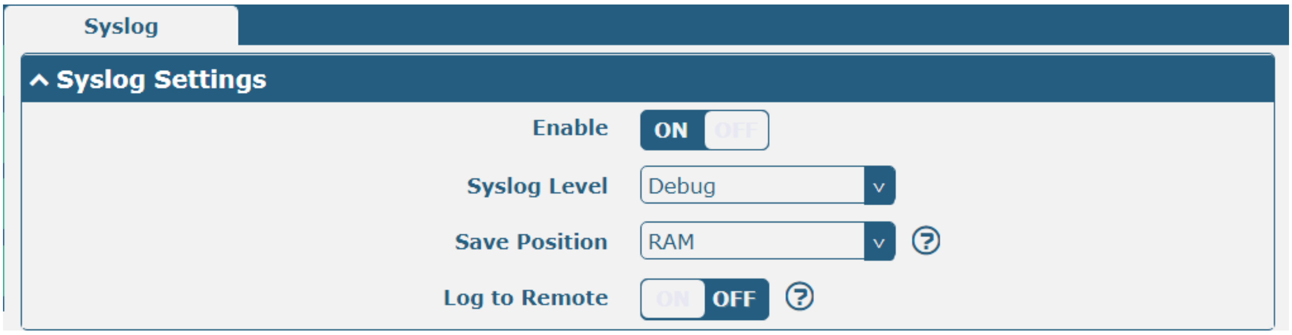
^ GRE tunnel status

Index	Description	Status	Local IP Address	Remote IP Address	Uptime

4.5 Service

4.5.1 Syslog

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



Syslog Settings

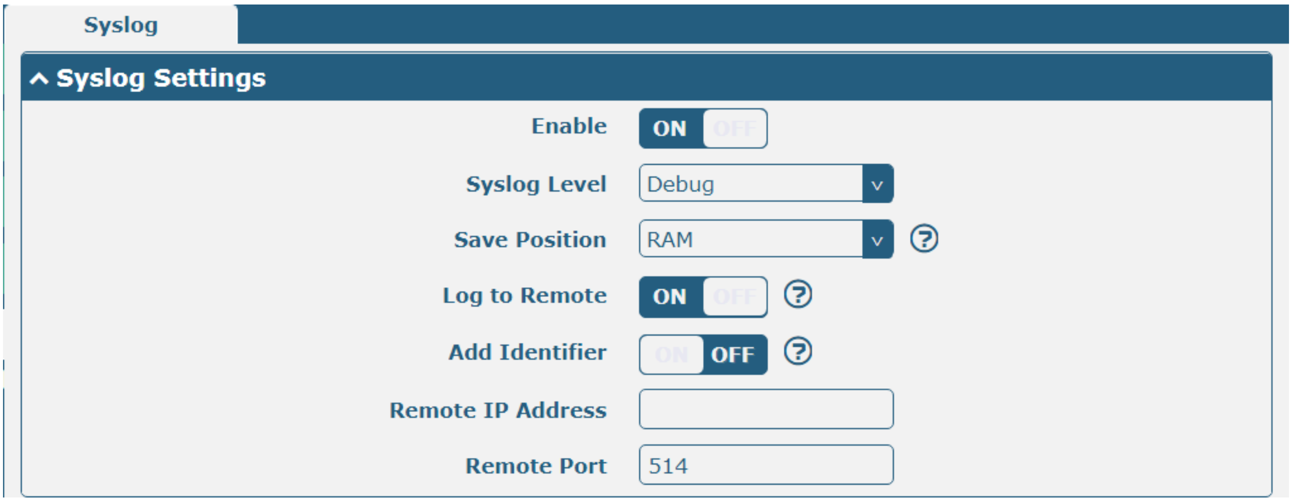
Enable: ON

Syslog Level: Debug

Save Position: RAM

Log to Remote: OFF

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



Syslog Settings

Enable: ON

Syslog Level: Debug

Save Position: RAM

Log to Remote: ON

Add Identifier: OFF

Remote IP Address:

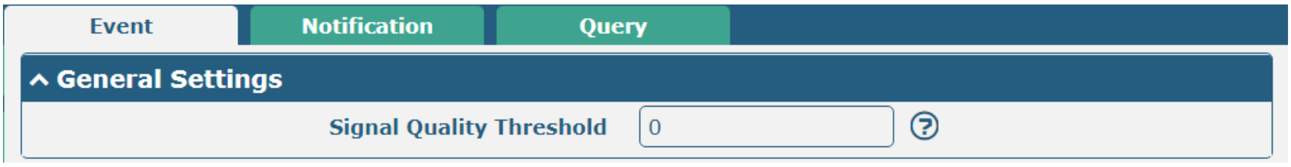
Remote Port: 514

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. **Note:** The lower level will output more syslog in details.	Debug
Save Position	Select the save position from "RAM", "NVM" or "Console". Choose "RAM". The data will be cleared after reboot. **Note**: It's not recommended that you save syslog to NVM for a long time.	RAM
Log to Remote	Click the toggle button to enable/disable this option. Enable to allow gateway sending syslog to the remote syslog server. You need to enter the IP and Port of the syslog server.	OFF
Remote IP Address	Enter the IP address of syslog server when enabling the "Log to Remote" option.	Null

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

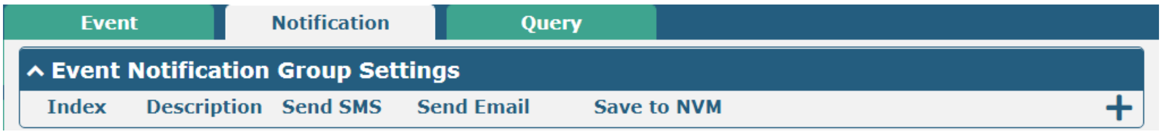
4.5.2 Event

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

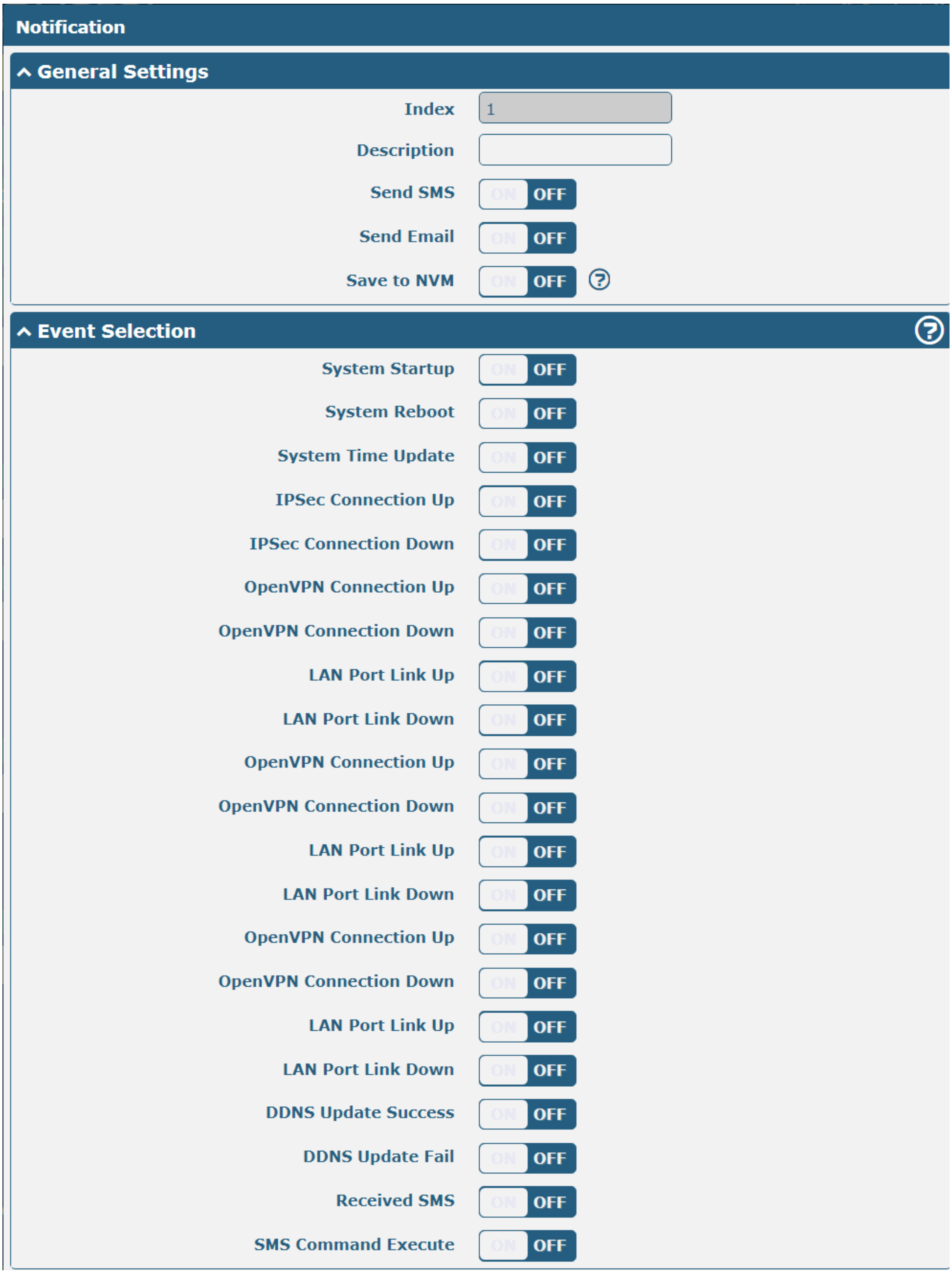


Signal Quality Threshold: 0

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



Click + button to add an Event parameters.



Notification

General Settings

Index: 1

Description:

Send SMS: OFF

Send Email: OFF

Save to NVM: OFF

Event Selection

System Startup: OFF

System Reboot: OFF

System Time Update: OFF

IPSec Connection Up: OFF

IPSec Connection Down: OFF

OpenVPN Connection Up: OFF

OpenVPN Connection Down: OFF

LAN Port Link Up: OFF

LAN Port Link Down: OFF

OpenVPN Connection Up: OFF

OpenVPN Connection Down: OFF

LAN Port Link Up: OFF

LAN Port Link Down: OFF

OpenVPN Connection Up: OFF

OpenVPN Connection Down: OFF

LAN Port Link Up: OFF

LAN Port Link Down: OFF

DDNS Update Success: OFF

DDNS Update Fail: OFF

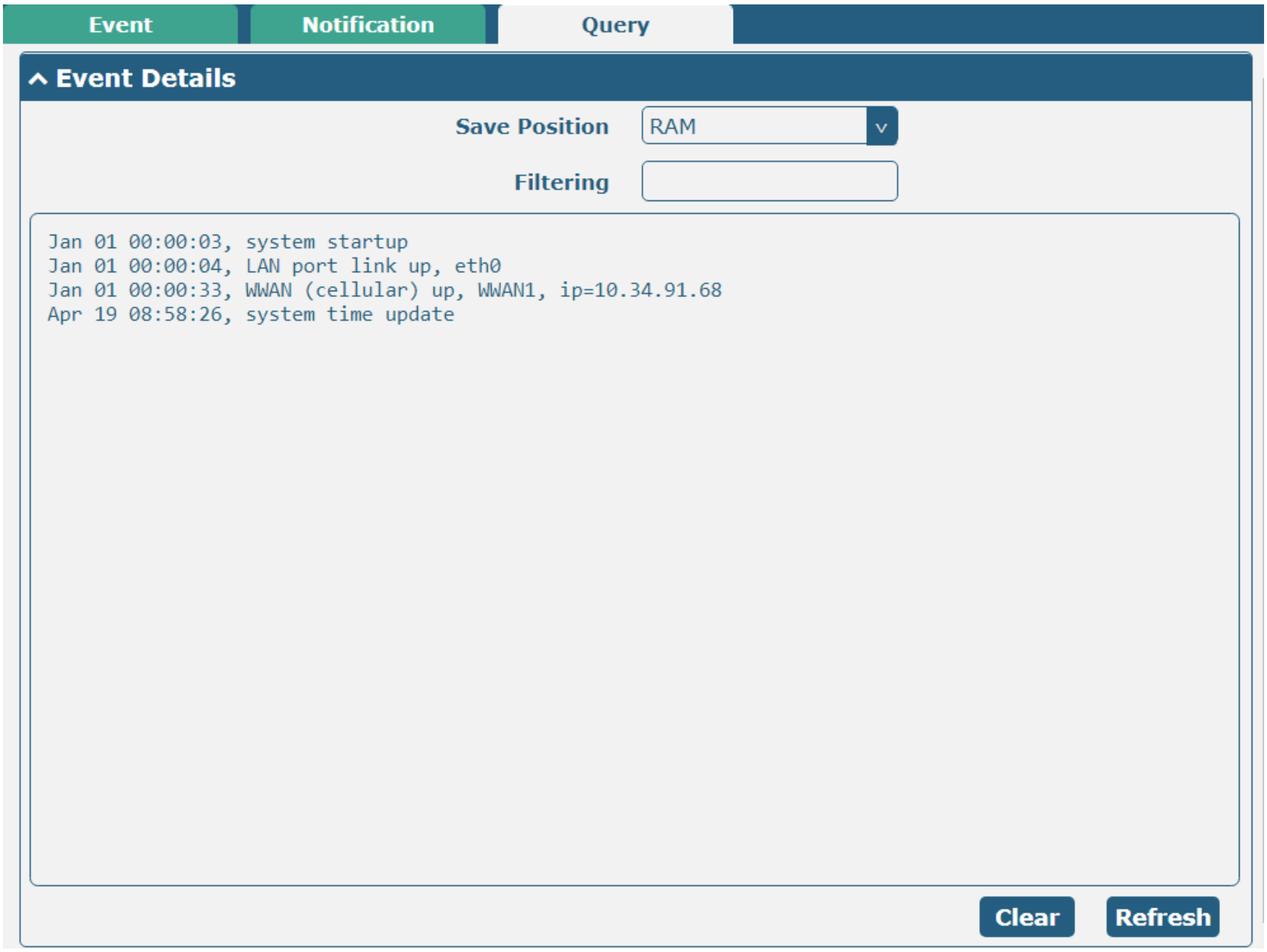
Received SMS: OFF

SMS Command Execute: OFF

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 gateway will send notification to the specified phone numbers via SMS if event occurs. Set	OFF

	the related phone number in "3.14 Services > Email", and use ';'to separate each number.	
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 gateway will send notification to the specified email box via Email if event occurs. Set the related email address in "3.14 Services > Email".	OFF
Email Address	Enter the email addresses used for receiving event notification. Use a space to separate each address.	Null
Save to NVM	Click the toggle button to enable/disable this option. Enable to save event to nonvolatile memory.	OFF

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



Save Position: RAM

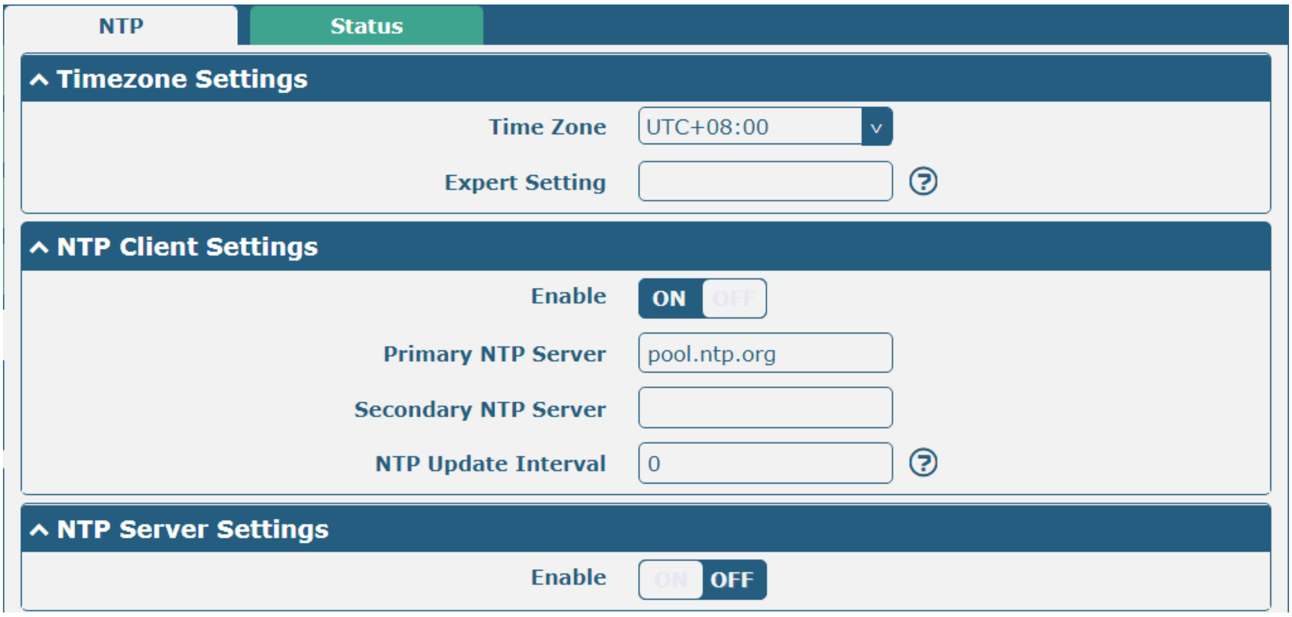
Filtering:

```
Jan 01 00:00:03, system startup
Jan 01 00:00:04, LAN port link up, eth0
Jan 01 00:00:33, WWAN (cellular) up, WWAN1, ip=10.34.91.68
Apr 19 08:58:26, system time update
```

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

4.5.3 NTP

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



Timezone Settings

Time Zone: UTC+08:00

Expert Setting:

NTP Client Settings

Enable: ON

Primary NTP Server: pool.ntp.org

Secondary NTP Server:

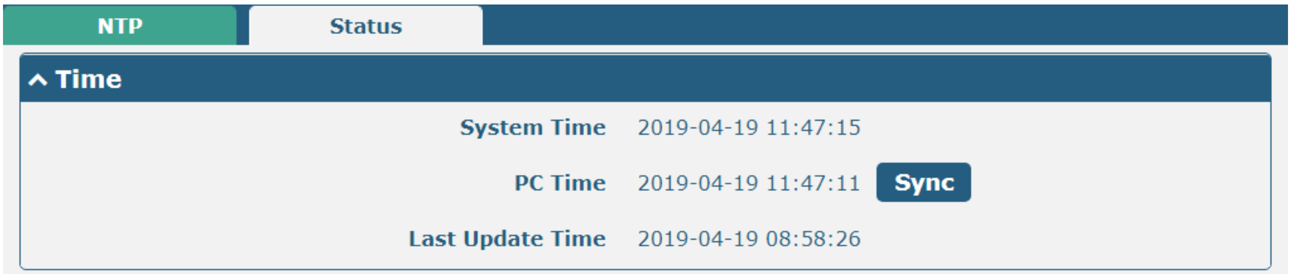
NTP Update Interval: 0

NTP Server Settings

Enable: OFF

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

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



Time

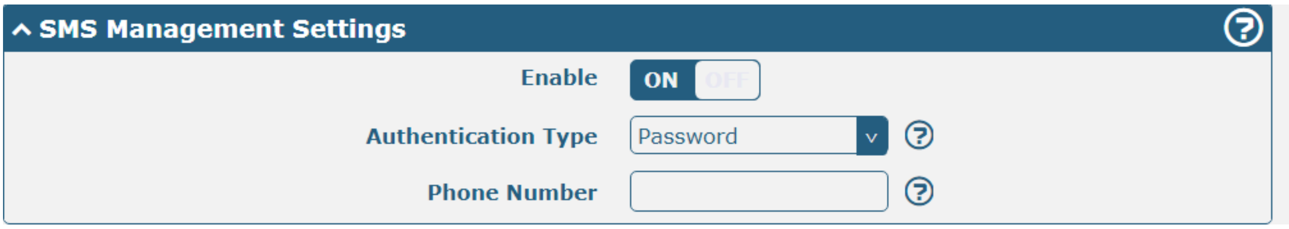
System Time: 2019-04-19 11:47:15

PC Time: 2019-04-19 11:47:11

Last Update Time: 2019-04-19 08:58:26

4.5.4 SMS

This section allows you to set SMS parameters. Gateway supports SMS management, and user can control and configure their gateways by sending SMS.



SMS Management Settings

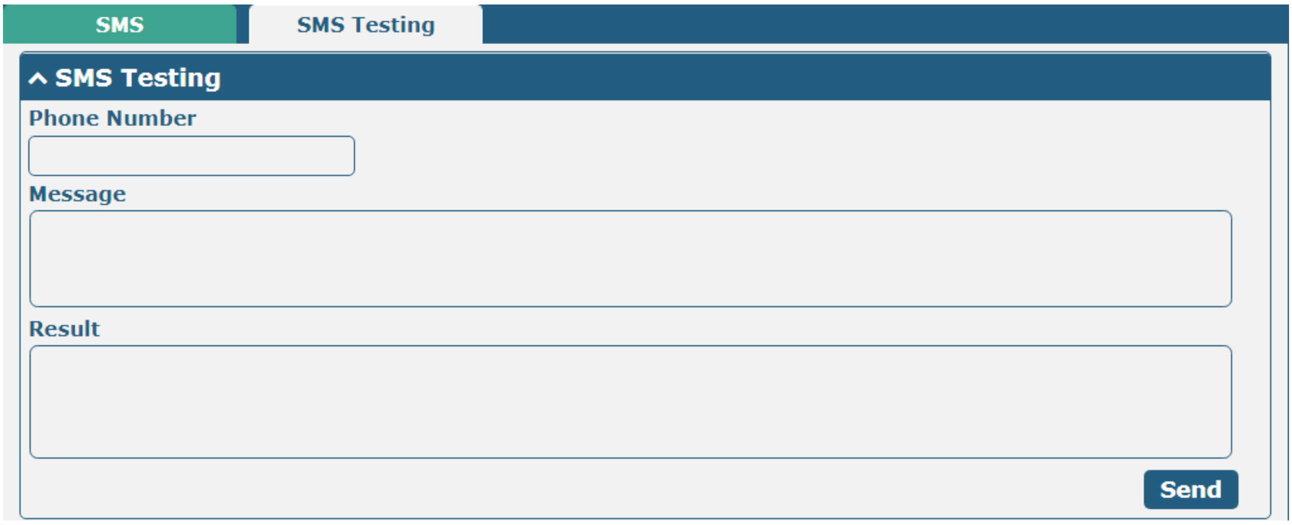
Enable: ON

Authentication Type: Password

Phone Number:

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

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



SMS Testing

Phone Number:

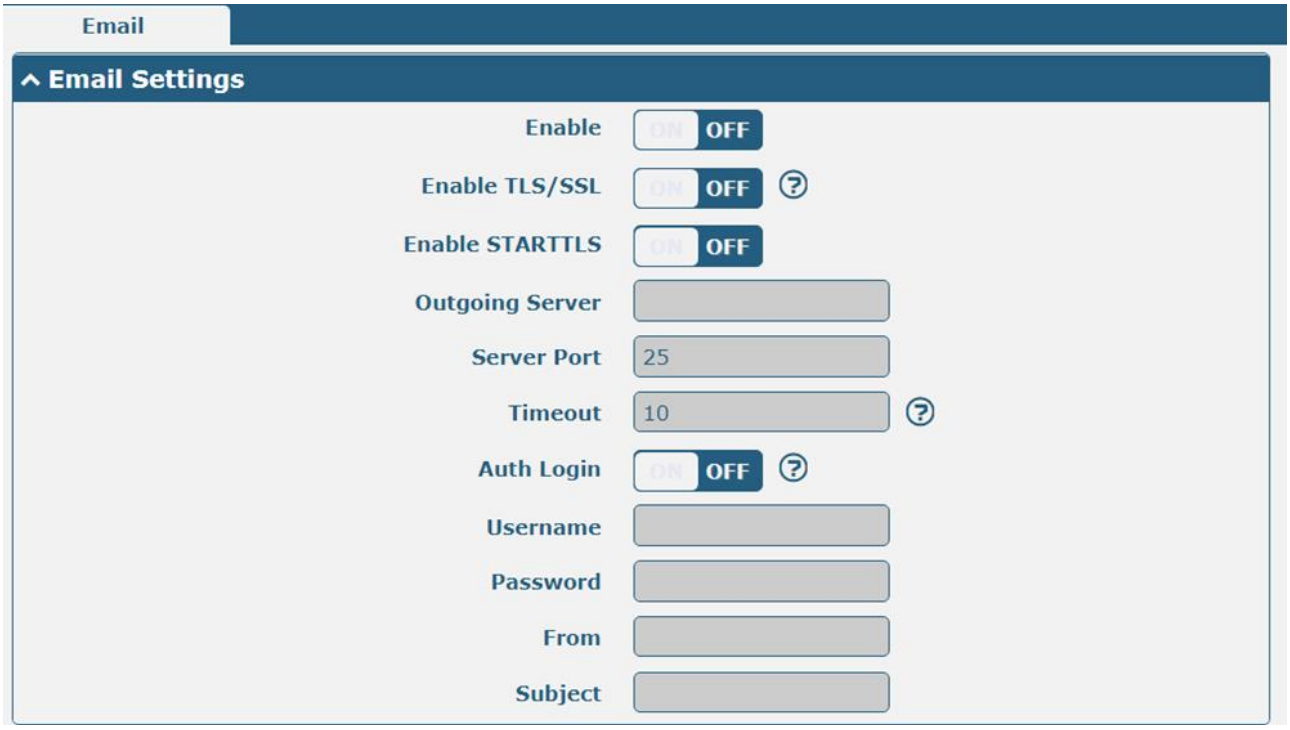
Message:

Result:

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

4.5.5 Email

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


Email

Email Settings

Enable: OFF

Enable TLS/SSL: OFF

Enable STARTTLS: OFF

Outgoing Server:

Server Port: 25

Timeout: 10

Auth Login: OFF

Username:

Password:

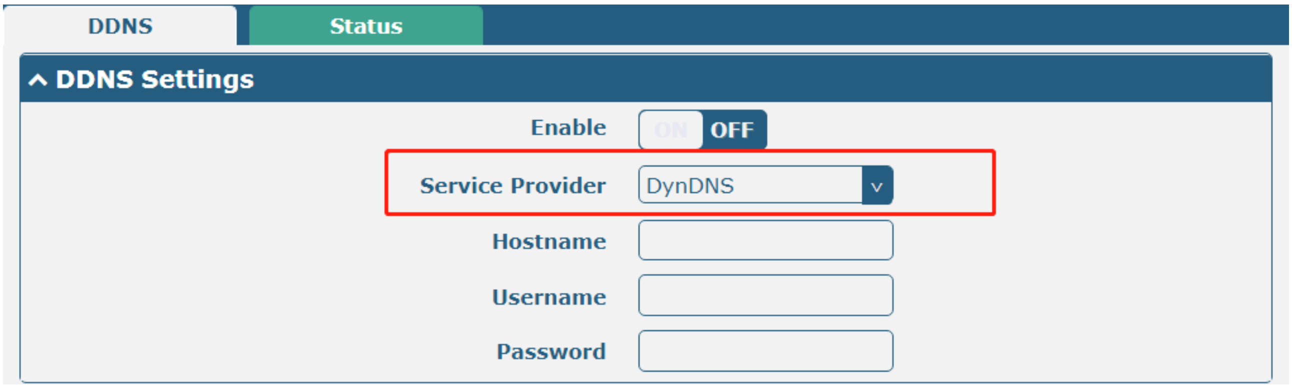
From:

Subject:

Email Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Email option.	OFF
Enable TLS/SSL	Click the toggle button to enable/disable the TLS/SSL option.	OFF
Outgoing server	Enter the SMTP server IP Address or domain name.	Null
Server port	Enter the SMTP server port.	25
Username	Enter the username which has been registered from SMTP server.	Null
Password	Enter the password of the username above.	Null
From	Enter the source address of the email.	Null
Subject	Enter the subject of this email.	Null

4.5.6 DDNS

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



Enable: OFF

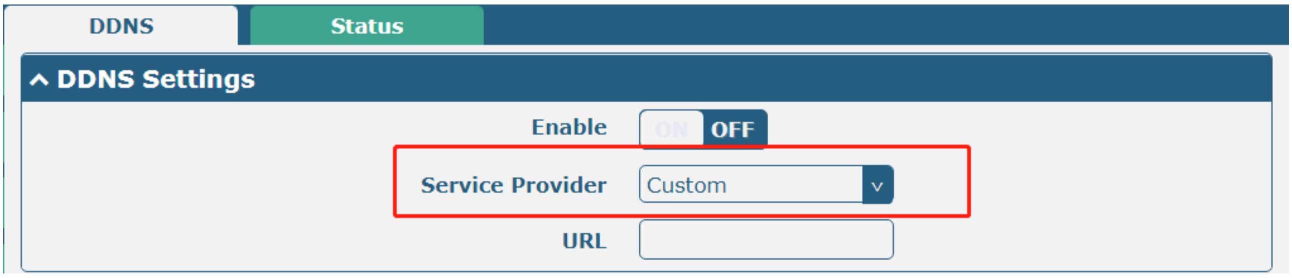
Service Provider: DynDNS

Hostname:

Username:

Password:

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



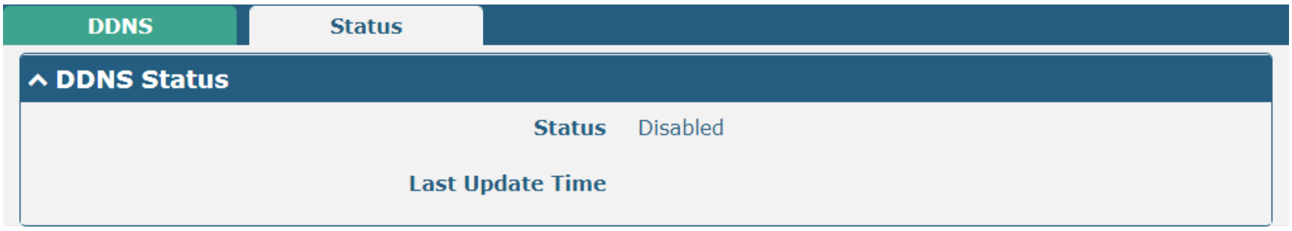
Enable: OFF

Service Provider: Custom

URL:

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

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



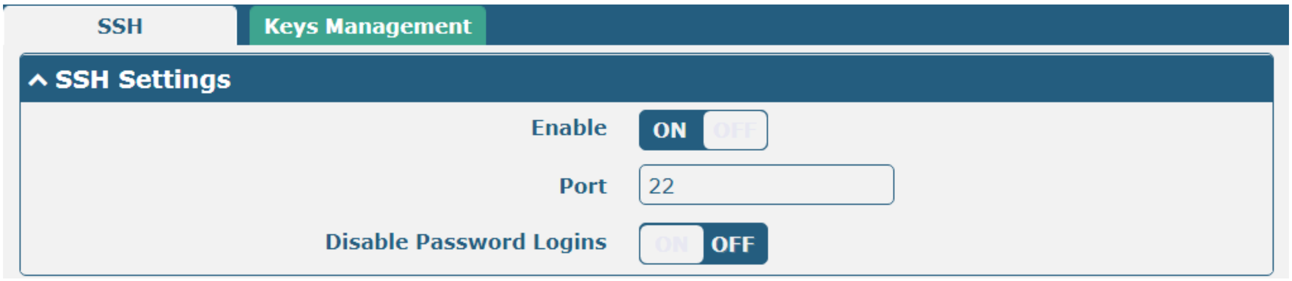
Status Disabled

Last Update Time

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

Gateway supports SSH password access and secret-key access.

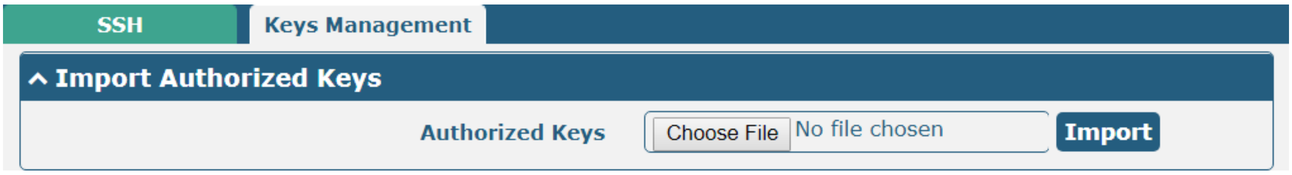


Enable ON

Port 22

Disable Password Logins OFF

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

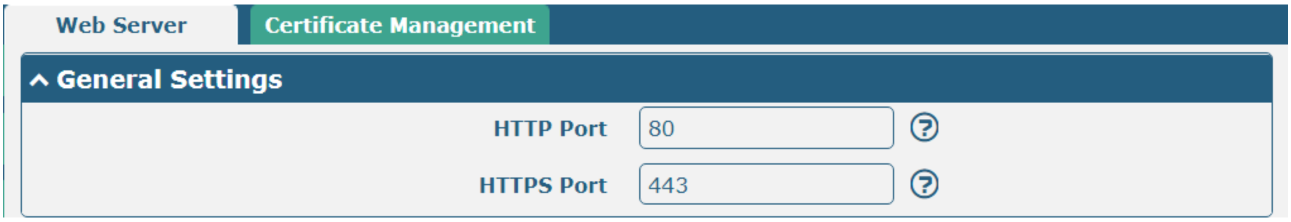


Authorized Keys No file chosen

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

4.5.8 Web Server

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

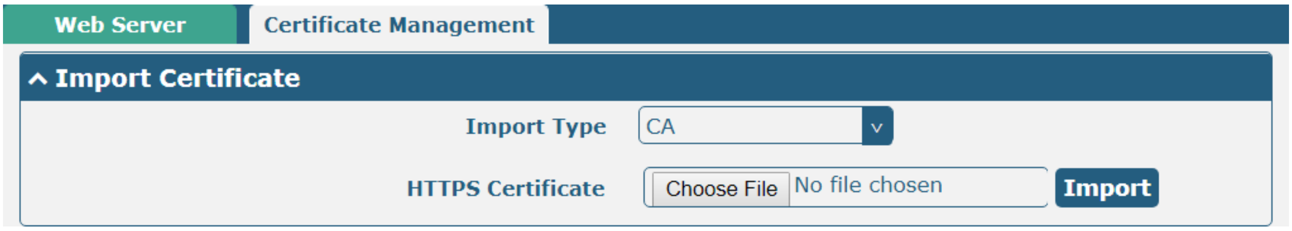


HTTP Port 80

HTTPS Port 443

General Settings @ Web Server		
Item	**Description**	**Default**
HTTP Port	Enter the HTTP port number you want to change in gateway'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 gateway with other HTTP Port number except 80, only adding that port number then you can login gateway's Web Server.	80
HTTPS Port	Enter the HTTPS port number you want to change in gateway'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 gateway with other HTTPS Port number except 443, only adding that port number then you can login gateway'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 gateway.



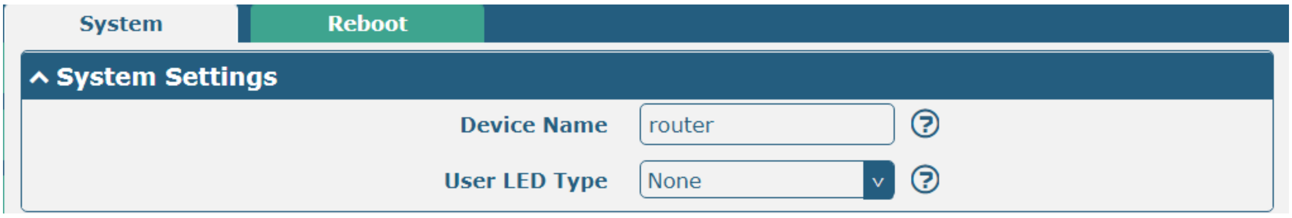
Import Type CA

HTTPS Certificate

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 gateway.	--

4.5.9 Advanced

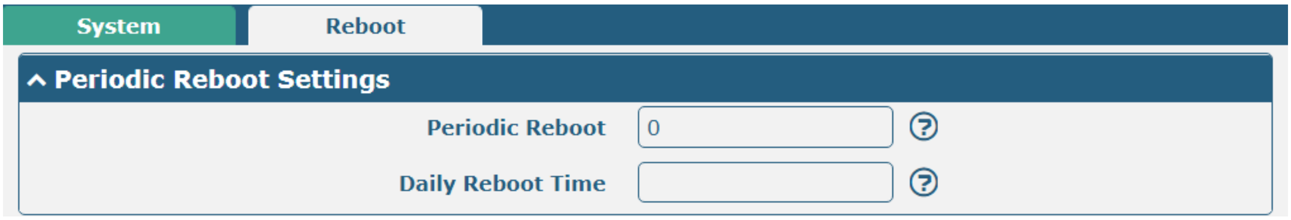
This section allows you to set the reboot.



Device Name: router

User LED Type: None

Periodic Reboot Settings		
Item	**Description**	**Default**
Device name	Set the name of the router to distinguish other installed devices.	router
Custom LED light type	Select from “None, SIM, NET, OpenVPN, or IPsec.” • None: After selecting this option, the USR indicator is off, meaningless. • SIM: After selecting this type, the USR indicator of the router shows the status of the SIM. • NET: After selecting this type, the USR indicator of the router shows the status of NET. • OpenVPN: After selecting this type, the USR indicator of the router shows the status of OpenVPN. • IPsec: After selecting this type, the USR indicator of the router shows the status of IPsec. **Note:**See "2.2 LED Indicators" for specific status information.	None



Periodic Reboot: 0

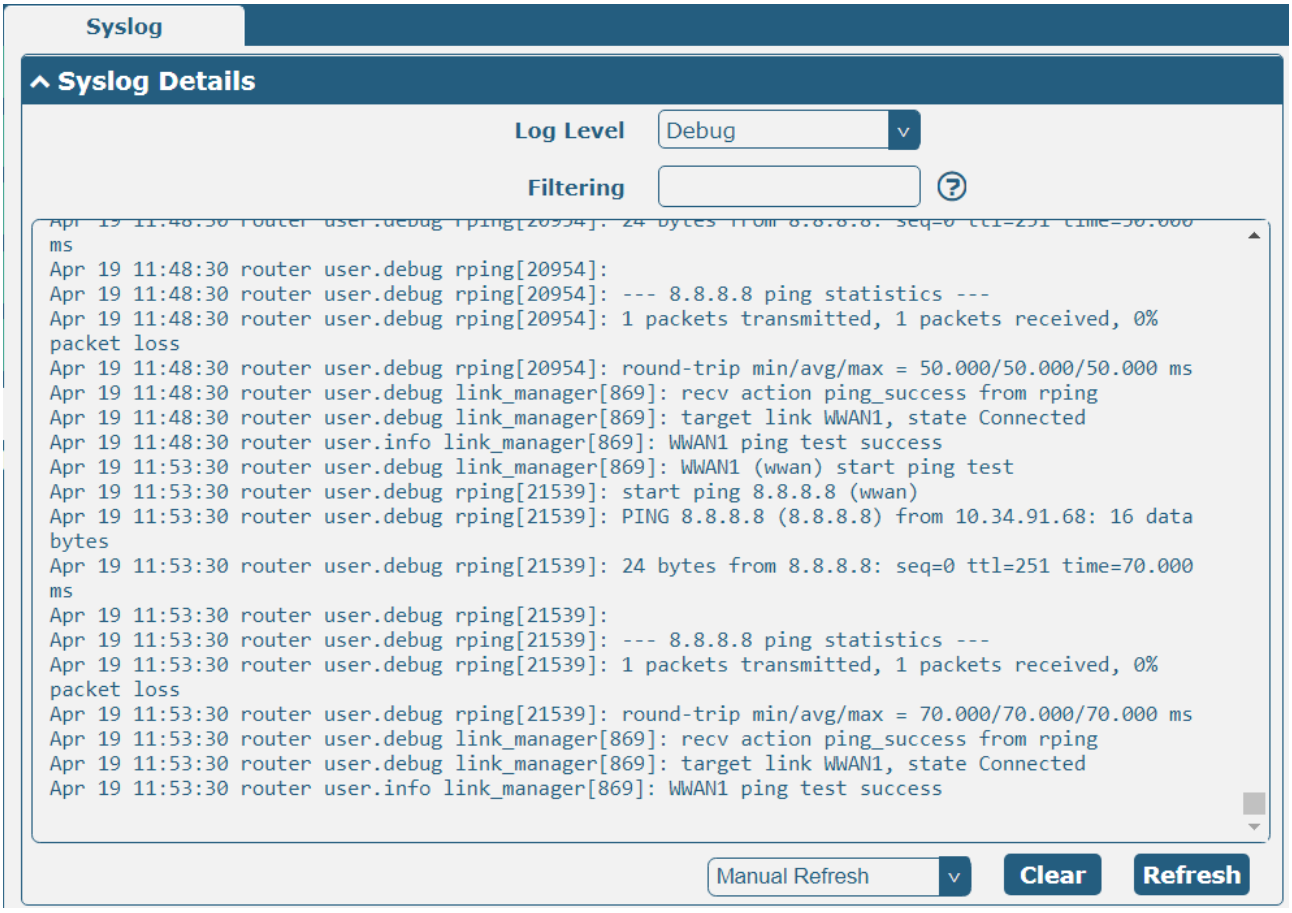
Daily Reboot Time:

Restart settings regularly		
project	**Description**	**default**
Restart regularly	Set the period for the router to restart. 0 means that regular restarts are not enabled.	0
Daily restart time	Set the time point for restarting the router every day, in the formatHH: MM (24-hour system). When this item is empty, it means to close the scheduled restart.	null

4.6 System

4.6.1 Debug

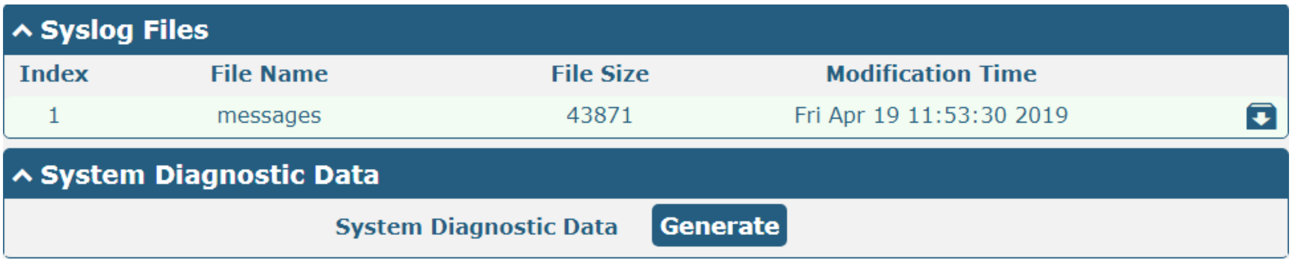
This section allows you to check and download the syslog details. Click Service > System Log > System Log Settings to open the system log.



Log Level: Debug

Filtering:

```
Apr 19 11:48:30 router user.debug rping[20954]: 24 bytes from 8.8.8.8: seq=0 ttl=251 time=50.000
ms
Apr 19 11:48:30 router user.debug rping[20954]:
Apr 19 11:48:30 router user.debug rping[20954]: --- 8.8.8.8 ping statistics ---
Apr 19 11:48:30 router user.debug rping[20954]: 1 packets transmitted, 1 packets received, 0%
packet loss
Apr 19 11:48:30 router user.debug rping[20954]: round-trip min/avg/max = 50.000/50.000/50.000 ms
Apr 19 11:48:30 router user.debug link_manager[869]: recv action ping_success from rping
Apr 19 11:48:30 router user.debug link_manager[869]: target link WWAN1, state Connected
Apr 19 11:48:30 router user.info link_manager[869]: WWAN1 ping test success
Apr 19 11:53:30 router user.debug link_manager[869]: WWAN1 (wwan) start ping test
Apr 19 11:53:30 router user.debug rping[21539]: start ping 8.8.8.8 (wwan)
Apr 19 11:53:30 router user.debug rping[21539]: PING 8.8.8.8 (8.8.8.8) from 10.34.91.68: 16 data
bytes
Apr 19 11:53:30 router user.debug rping[21539]: 24 bytes from 8.8.8.8: seq=0 ttl=251 time=70.000
ms
Apr 19 11:53:30 router user.debug rping[21539]:
Apr 19 11:53:30 router user.debug rping[21539]: --- 8.8.8.8 ping statistics ---
Apr 19 11:53:30 router user.debug rping[21539]: 1 packets transmitted, 1 packets received, 0%
packet loss
Apr 19 11:53:30 router user.debug rping[21539]: round-trip min/avg/max = 70.000/70.000/70.000 ms
Apr 19 11:53:30 router user.debug link_manager[869]: recv action ping_success from rping
Apr 19 11:53:30 router user.debug link_manager[869]: target link WWAN1, state Connected
Apr 19 11:53:30 router user.info link_manager[869]: WWAN1 ping test success
```



Index	File Name	File Size	Modification Time
1	messages	43871	Fri Apr 19 11:53:30 2019

System Diagnostic Data: Generate

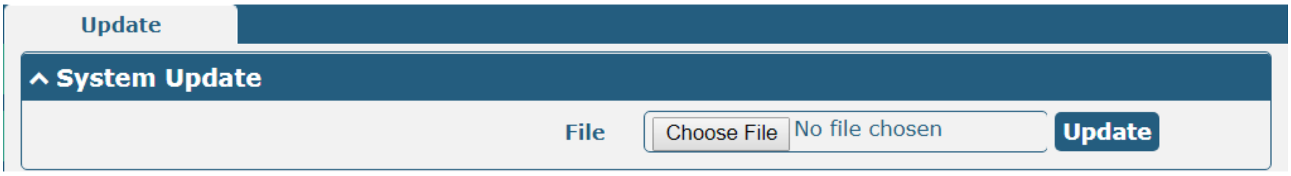
Syslog	
Item	**Description**
Syslog Details	
Log Level	Select from "Debug", "Info", "Notice", "Warn", "Error" which from low to high. The lower level will output more syslog in detail.
Filtering	Enter the filtering message based on the keywords. Use "&" to separate more than one filter message, such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

Refresh	Select from “Manual Refresh”, “5 Seconds”, “10 Seconds”, “20 Seconds” or “30 Seconds”. You can select these intervals to refresh the log information displayed in the follow box. If selecting “manual refresh”, you should click the refresh button to refresh the syslog.
Clear	Click the button to clear the syslog.
Refresh	Click the button to refresh the syslog.
Syslog Files	
Syslog Files List	It can show at most 5 syslog files in the list, the files’ name range from message0 to message 4. And the newest syslog file will be placed on the top of the list.
System Diagnosing Data	
Generate	Click to generate the syslog diagnosing file.

4.6.2 Update

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

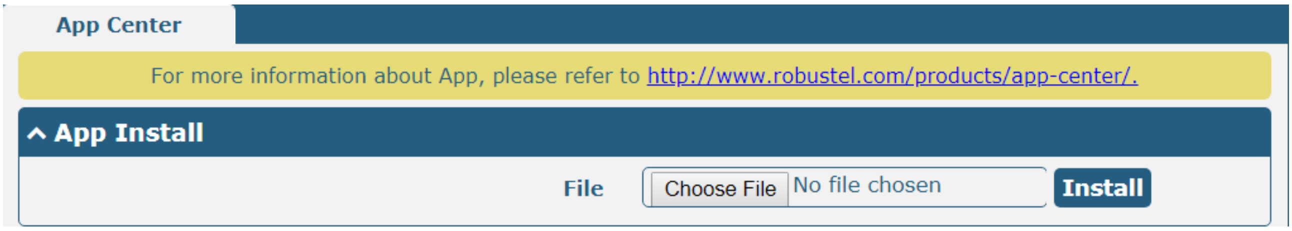
Note: To access the latest firmware file, please contact your technical support engineer.



4.6.3 App Center

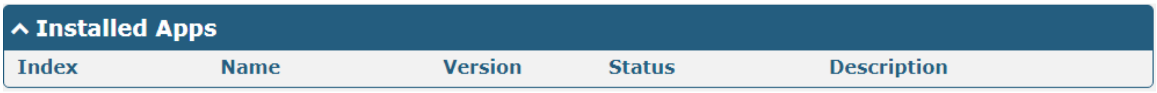
This section allows you to add some required or customized applications to the gateway. Import and install your applications to the App Center, and reboot the device according to the system prompts. Each installed application will be displayed under the “Services” menu.

Note: After importing the applications to the gateway, 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 gateway again.



For more information about App, please refer to http://www.robustel.com/products/app-center/.

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

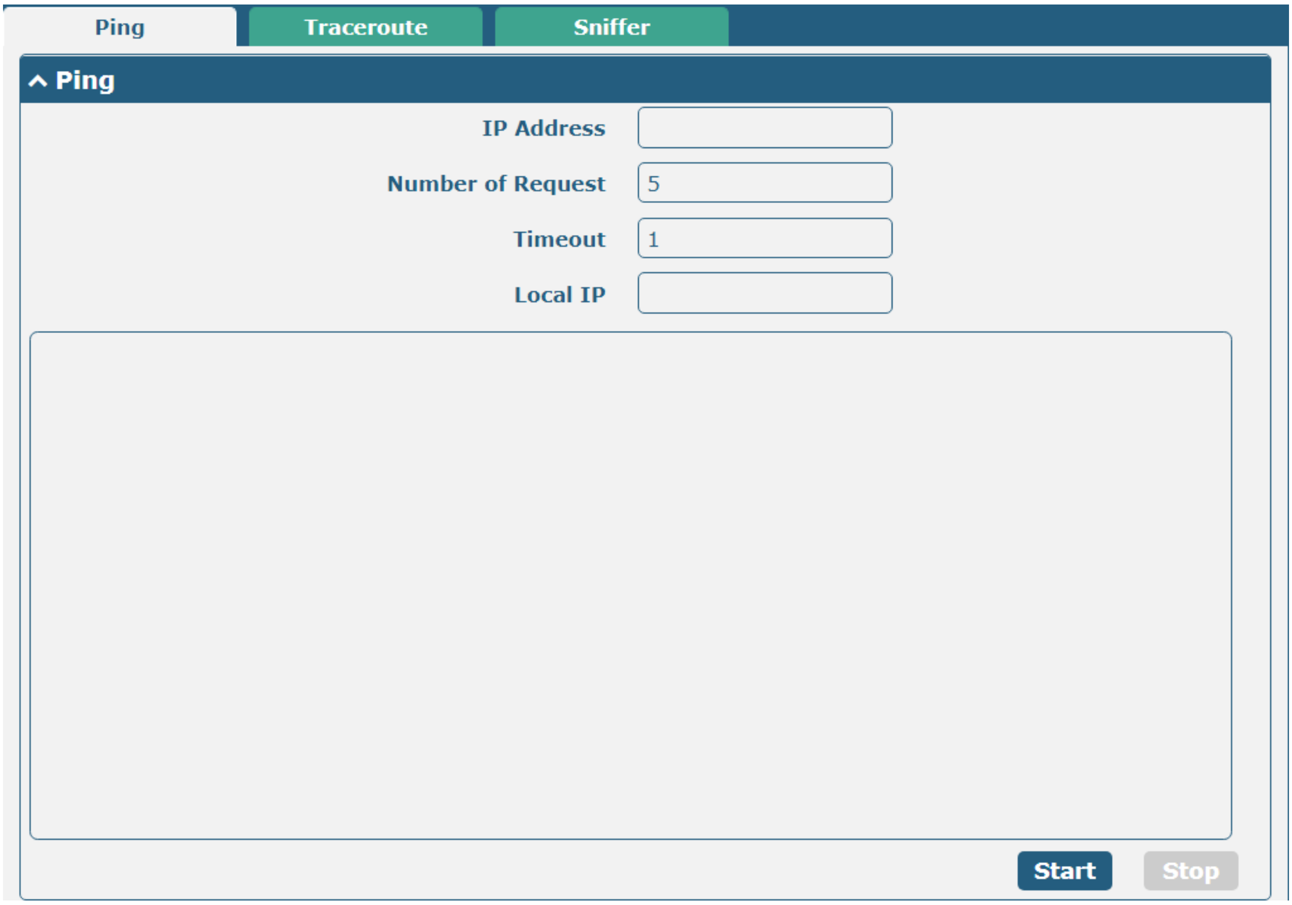


Index	Name	Version	Status	Description

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 gateway. **Note**: File format should be *xxx.rpk*, e.g. *M1200-robustlink-1.0.0.rpk*.	--
Installed Apps		
Index	Indicate the ordinal of the list.	--
Name	Show the name of the App.	Null
Version	Show the version of the App.	Null
Status	Show the status of the App.	Null
Description	Show the description for this App.	Null

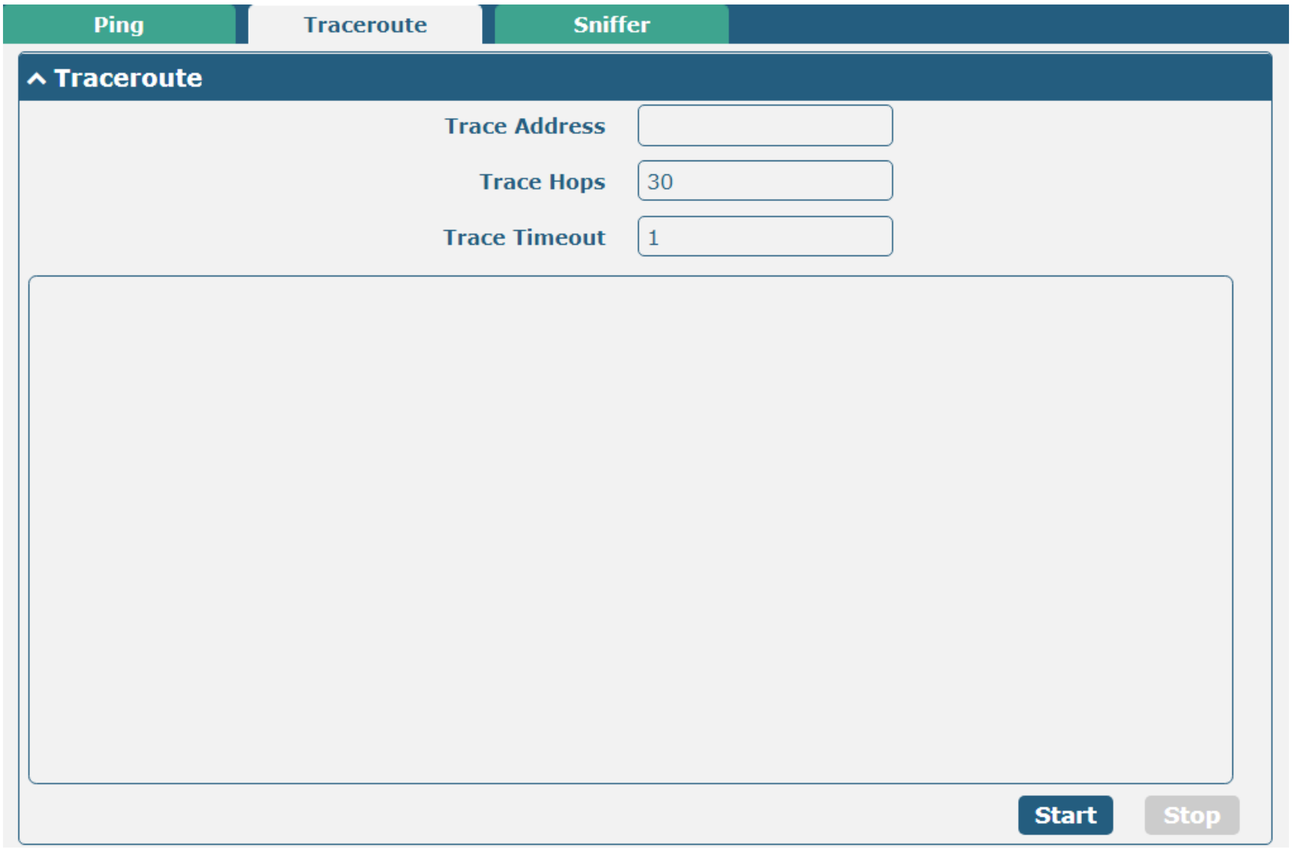
4.6.4 Tools

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 requests.	1
Local IP	Specify the local IP from cellular WAN, Ethernet WAN or Ethernet LAN. Null stands for selecting local IP address from these three automatically.	Null
Start	Click this button to start ping request, and the log will be displayed in the follow box.	Null
Stop	Click this button to stop ping request.	--

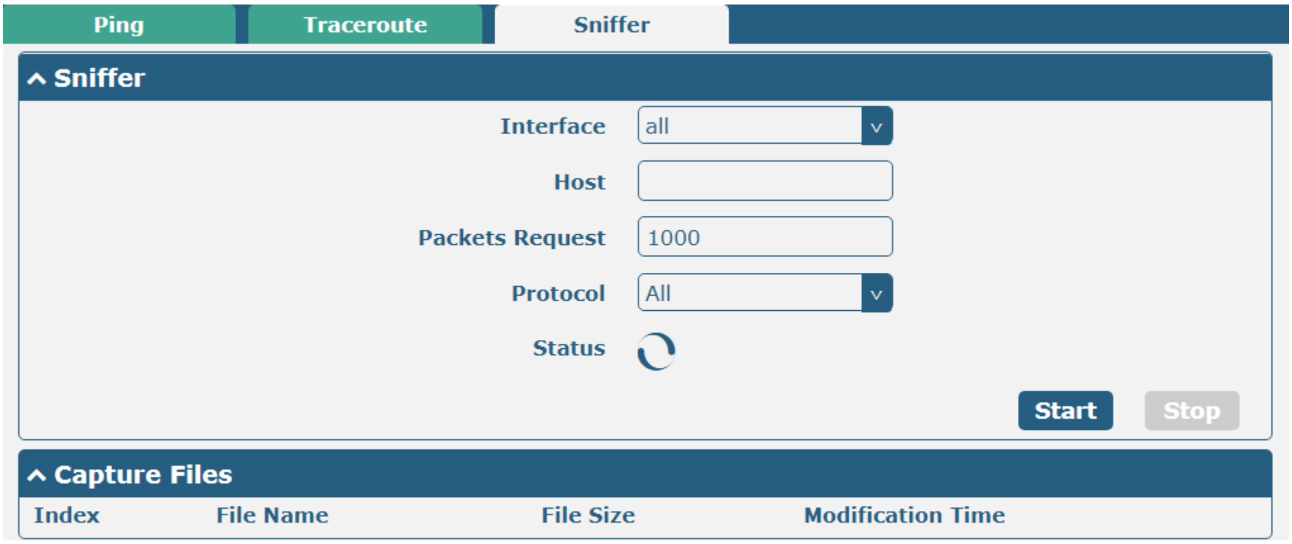


Trace Address

Trace Hops 30

Trace Timeout 1

Traceroute		
Item	**Description**	**Default**
Trace Address	Enter the trace's destination IP address or destination domain.	Null
Trace Hops	Specify the max trace hops. gateway 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

Interface: all

Host:

Packets Request: 1000

Protocol: All

Status:

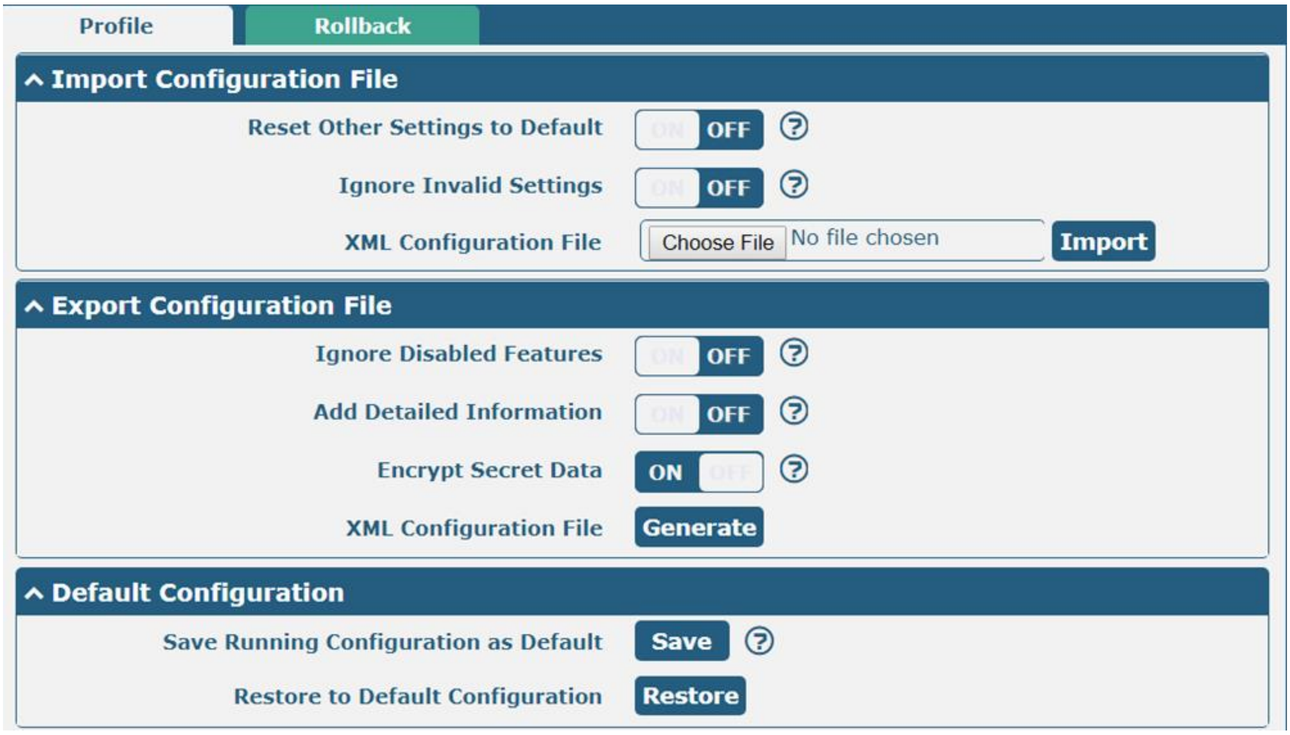
Capture Files

Index	File Name	File Size	Modification Time

Sniffer		
Item	**Description**	**Default**
Interface	Select the interface according to the "Ethernet" configuration and select from "All", "PPP1", "WWAN" and "IO".	All
Host	Filter the packet that contain the specify IP address.	Null
Packets Request	Set the packet number that the gateway 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 gateway to factory default setting.



Import Configuration File

Reset Other Settings to Default: OFF

Ignore Invalid Settings: OFF

XML Configuration File: Choose File No file chosen Import

Export Configuration File

Ignore Disabled Features: OFF

Add Detailed Information: OFF

Encrypt Secret Data: ON

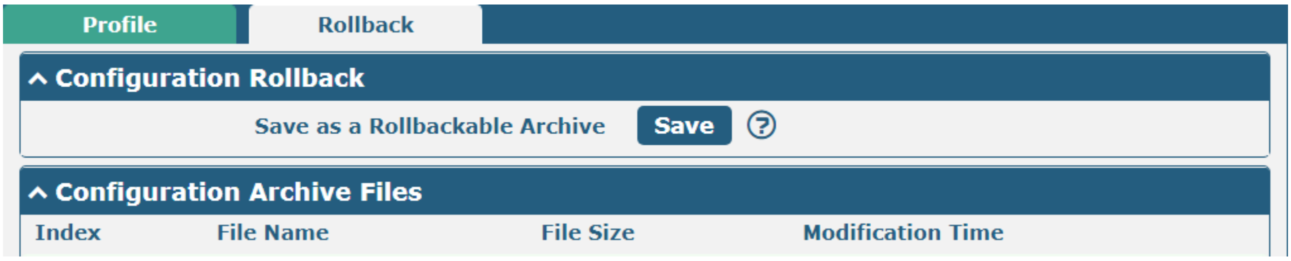
XML Configuration File: Generate

Default Configuration

Save Running Configuration as Default: Save

Restore to Default Configuration: Restore

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

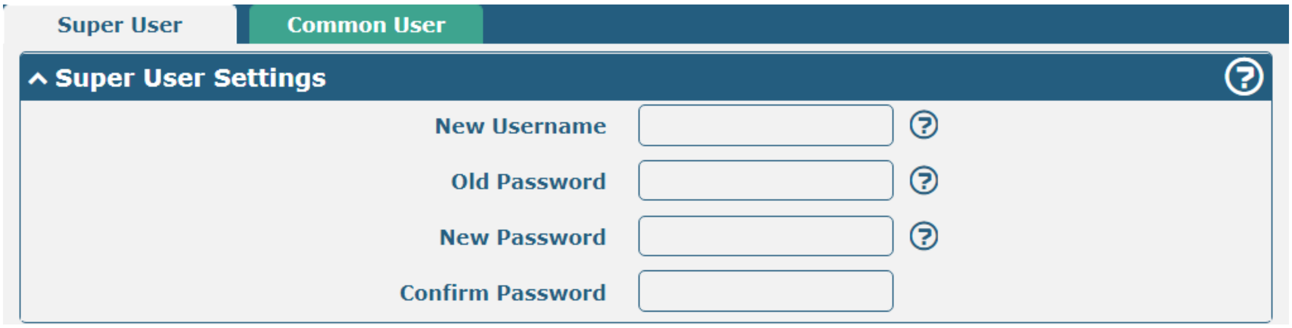


Rollback		
Item	**Description**	**Default**
Configuration Rollback		
Save as a Rollbackable Archive	Create a save point manually. Additionally, the system will create a save point every day automatically if configuration changes.	--
Configuration Archive Files		
Configuration Archive Files	View the related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

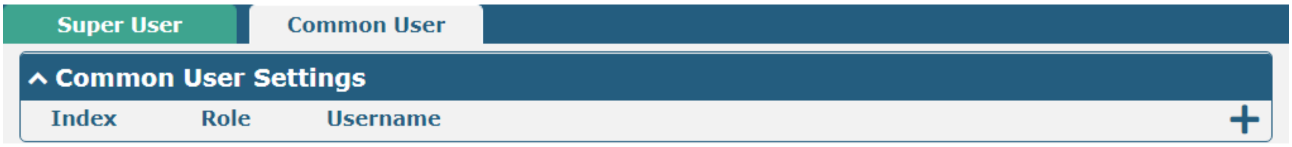
4.6.6 User Management

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

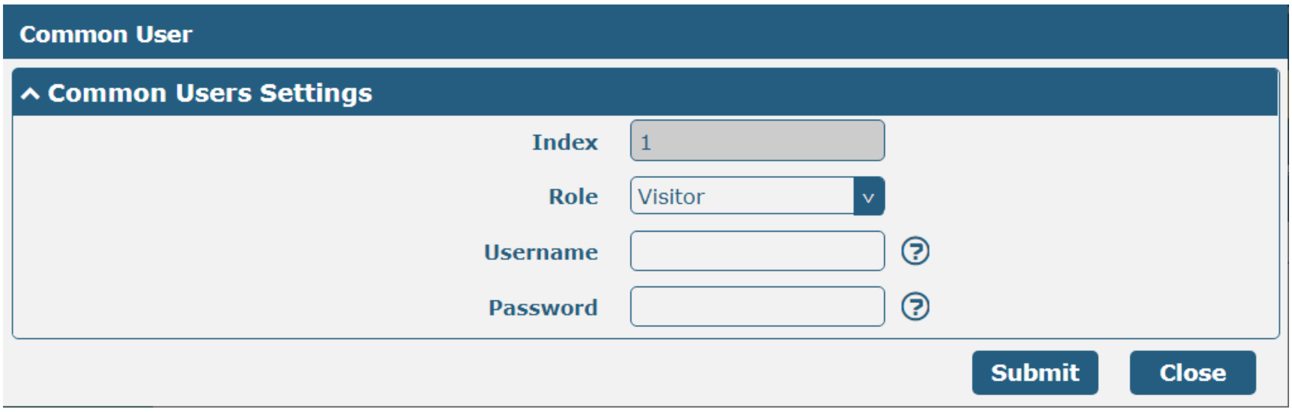
Note: Your new password must be more than 5 character and less than 32 characters and may contain numbers, upper and lowercase letters, and standard symbols.



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



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



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

Glossary

Abbr.	Description
AC	Alternating Current
APN	Access Point Name of GPRS Service Provider Network
CE	Conformité Européene (European Conformity)
CHAP	Challenge Handshake Authentication Protocol
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
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
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharges
ETSI	European Telecommunications Standards Institute
GND	Ground
GPRS	General Package Radio Service
GSM	Global Standard for Mobile Communications
IMEI	International Mobile Equipment Identification
kbps	kbits per second
LED	Light Emitting Diode
MAX	Maximum
Min	Minimum
MO	Mobile Originated
MS	Mobile Station
MT	Mobile Terminated
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

Abbr.	Description
PPP	Point-to-point Protocol
PIN	Personal Identity Number
PSU	Power Supply Unit
PUK	Personal Unblocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTS	Request to Send
Rx	Receive Direction
SIM	Subscriber Identification Module
SMA	Subminiature Version A RF Connector
SMS	Short Message Service
TCP/IP	Transmission Control Protocol / Internet Protocol
TE	Terminal Equipment, also referred to as DTE
Tx	Transmit Direction
UART	Universal Asynchronous Receiver-transmitter
USSD	Unstructured Supplementary Service Data
VSWR	Voltage Stationary Wave Ratio

Guangzhou Robustel LTD

Add:	3rd Floor, Building F, Kehui Park, No.95 Daguan Road, Guangzhou, China 510660
Tel:	86-20-29019902
Email:	info@robustel.com
Web:	www.robustel.com