



# User Guide

## R2000

Industrial Dual SIM Cellular VPN Router  
2 Eth + 2 SIM



robustOS

Guangzhou Robustel LTD  
[www.robustel.com](http://www.robustel.com)


## About This Document

This document provides hardware and software information of the Robustel R2000 Router, including introduction, installation, configuration and operation.

**Copyright©2020 Guangzhou Robustel LTD.**

**All rights reserved.**

## 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. The contents of this document are subject to change without notice due to continued progress in methodology, design and manufacturing. Robustel shall have no liability for any error or damage of any kind resulting from the use of this document.

## Technical Support

Tel: +86-20-29019902

Fax: +86-20-82321505

Email: [support@robustel.com](mailto:support@robustel.com)

Web: [www.robustel.com](http://www.robustel.com)

## Important Notice

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

## Safety Precautions

### General

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

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

### Using the Router in Vehicle

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

## Protecting Your Router

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

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

## Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:



- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

### FCC Caution:


- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## 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	<p>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.</p> <p>Please see <b>Table 3</b> 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.</p>	
SJ/T 11364-2014	<p>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.</p> <p>The orange logo below is used for Robustel products:</p>  <p>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.</p> <p>*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.</p>	

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

Name of the Part	Hazardous Substances									
	(Pb)	(Hg)	(Cd)	(Cr(VI))	(PBB)	(PBDE)	(DEHP)	(BBP)	(DBP)	(DIBP)
Metal parts	o	o	o	o	-	-	-	-	-	-
Circuit modules	o	o	o	o	o	o	o	o	o	o
Cables and cable assemblies	o	o	o	o	o	o	o	o	o	o
Plastic and polymeric parts	o	o	o	o	o	o	o	o	o	o
<p>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.</p> <p>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.</p> <p>:- Indicates that it does not contain the toxic or hazardous substance.</p>										

## 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
24 Aug., 2016	1.2.2	V2.0.0	Initial release
31 Aug., 2016	1.2.2	V2.0.1	<ul style="list-style-type: none"> <li>Modified the frequency range of FDD LTE and TDD LTE</li> <li>Modified the EMC details</li> <li>Modified the Tel &amp; Fax No.</li> </ul>
8 Oct., 2016	1.2.2	V2.0.2	Updated frequency band info in Chapter 1.5 Other minor changes
11 Nov., 2016	1.2.2	V2.0.3	Updated section about 2.9 Power Supply
18 Nov., 2016	1.2.2	v.2.0.4	Updated information about input voltage
29 Nov., 2016	1.2.2	v.2.0.5	Updated section about 1.5 Selection and Ordering Data
19 Jan., 2017	1.2.2	v.2.0.6	<ul style="list-style-type: none"> <li>Changed Tel number to +86-20-29019902</li> <li>Changed CD information in Chapter 1.2</li> <li>Updated section about 1.5 Selection and Ordering Data</li> </ul>
23 Feb., 2017	1.2.2	v.2.0.7	Added note about PD connection
24 Jul., 2017	3.0.0	v.3.0.0	Firmware Update
21 Oct., 2017	3.0.0	v.3.0.1	<ul style="list-style-type: none"> <li>Added "RF output power" information for WiFi interface</li> <li>Added new certificate: EAC</li> <li>Added new product model: R2000-NU</li> <li>Updated router's image</li> <li>Updated network protocol and app</li> <li>Other minor changes</li> </ul>
17 Jan., 2018	3.0.0	v.3.0.2	Updated frequency bands for 3G model
28 Jun., 2018	3.0.0	v.3.0.3	Revised the company name
12 Dec., 2018	3.0.0	v.3.0.4	Added the description of the BG96 module
22 Jan., 2019	3.0.0	v.3.0.5	<ul style="list-style-type: none"> <li>Added the description of the R2000-4M</li> <li>Revised the Certification information</li> <li>Revised the Frequency bands of WIFI</li> </ul>
14 Feb., 2019	3.0.0	v.3.0.6	<ul style="list-style-type: none"> <li>Added the FCC Interference Statement</li> </ul>
28 May., 2019	3.0.0	v.3.0.7	<ul style="list-style-type: none"> <li>Revised the approvals</li> <li>Revised the Regulatory and Type Approval Information</li> </ul>
17 Sep., 2019	3.0.0	v.3.0.8	<ul style="list-style-type: none"> <li>Revised the approvals</li> <li>Revised the Regulatory and Type Approval Information</li> </ul>
25 Nov., 2019	3.0.0	v.3.0.9	<ul style="list-style-type: none"> <li>Revised the description of Update firmware via tftp</li> </ul>
Mar. 4, 2020	3.0.5	v.3.1.0	<ul style="list-style-type: none"> <li>Added the related information of IPv6;</li> </ul>



			<ul style="list-style-type: none"><li>• Revised the screenshot of ROS interface;</li><li>• Revised the parameter description;</li><li>• Revised the Regulatory and Type Approval Information</li><li>• Revised the information of IPsec VPN gateway address</li><li>• Revised the maximum count of filtering</li><li>• Deleted some redundant descriptions in product specifications</li></ul>
--	--	--	--

## Contents

<b>Chapter 1</b>	<b>Product Overview .....</b>	<b>12</b>
1.1	Key Features .....	12
1.2	Package Contents .....	12
1.3	Specifications .....	14
1.4	Dimensions.....	15
<b>Chapter 2</b>	<b>Hardware Installation.....</b>	<b>16</b>
2.1	PIN Assignment .....	16
2.2	LED Indicators.....	16
2.3	Reset Button.....	17
2.4	Ethernet Port.....	18
2.5	Insert or Remove SIM Card .....	18
2.6	Attach External Antenna (SMA Type) .....	19
2.7	Mount the Router .....	20
2.8	Ground the Router .....	21
2.9	Connect the Router to a Computer.....	21
2.10	Power Supply.....	21
2.11	PD Connection (Optional) .....	22
<b>Chapter 3</b>	<b>Initial Configuration .....</b>	<b>23</b>
3.1	Configure the PC.....	23
3.2	Factory Default Settings .....	27
3.3	Log in the Router .....	27
3.4	Control Panel .....	28
3.5	Status.....	29
3.6	Interface > Link Manager .....	32
3.7	Interface > LAN .....	45
3.8	Interface > Ethernet .....	49
3.9	Interface > Cellular .....	50
3.10	Interface > WiFi (Optional).....	55
3.11	Network > Route .....	63
3.12	Network > Firewall .....	65
3.13	Network > IP Passthrough .....	71
3.14	VPN > IPsec.....	71
3.15	VPN > OpenVPN .....	80
3.16	VPN > GRE .....	93
3.17	Services > Syslog.....	95
3.18	Services > Event.....	96
3.19	Services > NTP .....	99
3.20	Services > SMS.....	100
3.21	Services > Email.....	101
3.22	Services > DDNS .....	102
3.23	Services > SSH.....	103
3.24	Services > Web Server .....	104
3.25	Services > Advanced .....	105
3.26	System > Debug.....	106

3.27	System > Update .....	107
3.28	System > App Center .....	108
3.29	System > Tools .....	109
3.30	System > Profile.....	111
3.31	System > User Management .....	113
<b>Chapter 4</b>	<b>Configuration Examples.....</b>	<b>115</b>
4.1	Cellular .....	115
4.1.1	Cellular Dial-Up.....	115
4.1.2	SMS Remote Control.....	117
4.2	Network.....	120
4.2.1	IPsec VPN .....	120
4.2.2	OpenVPN .....	124
4.2.3	GRE VPN.....	126
<b>Chapter 5</b>	<b>Introductions for CLI.....</b>	<b>129</b>
5.1	What Is CLI.....	129
5.2	How to Configure the CLI .....	130
5.3	Commands Reference .....	131
5.4	Quick Start with Configuration Examples.....	131
<b>Glossary</b> .....		<b>138</b>

# Chapter 1 Product Overview

## 1.1 Key Features

The Robustel Industrial Dual SIM Cellular VPN Router (R2000) is a rugged cellular router offering state-of-the-art mobile connectivity for machine to machine (M2M) applications.

R2000 is a powerful router developed from RobustOS, a Robustel self-developed and Linux-based operating system which is designed to be used in Robustel devices. The RobustOS includes basic networking features and protocols providing customers with a very good user experience. Meanwhile, Robustel offers a Software Development Kit (SDK) for partners and customers to allow additional customization by using C, Python or Java. It also provides rich Apps to meet fragmented IoT market demands.

## 1.2 Package Contents

Before installing your R2000 Router, verify the kit contents as following.

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

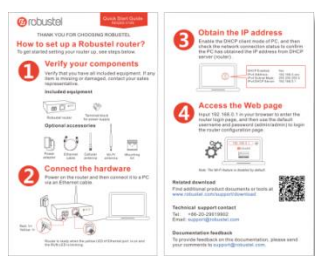
- 1 x Robustel R2000 Industrial Dual SIM Cellular VPN Router



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



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



**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



Magnet antenna



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

Stubby antenna



Magnet antenna



- Wall mounting kit



- 35 mm DIN rail mounting kit



- Ethernet cable



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



## 1.3 Specifications

### Cellular Interface

- Number of antennas: 2 (MAIN + AUX)
- Connector: SMA-K
- SIM: 2 (3.0 V & 1.8 V)
- Standards: GSM/GPRS/EDGE/WCDMA/HSDPA/HSUPA/HSPA+/DC-HSPA+/TD-SCDMA/CDMA (CDMA 1X/EVDO)/FDD LTE/TDD LTE

### Ethernet Interface

- Number of ports: 2 x 10/100 ports, 2 x LAN or 1 x LAN + 1 x WAN
- WAN port: Supporting 802.3 at PD feature (optional)
- Magnet isolation protection: 1.5 KV

### WiFi Interface (Optional)

- Number of antennas: 2 (WiFi1 + WiFi2)
- Connector: RP-SMA-K
- Standards: 802.11b/g/n, supporting AP and Client modes
- Frequency bands: 2.4 GHz
- Security: WEP, WPA, WPA2
- Encryption: 68/124 AES, TKIP

- Data speed: 2\*2 MIMO, 300 Mbps

#### Others

- 1 x RST button
- LED indicators - 1 x RUN, 1 x PPP, 1 x USR, 3 x RSSI
- Built-in Watchdog, Timer

#### Power Supply and Consumption

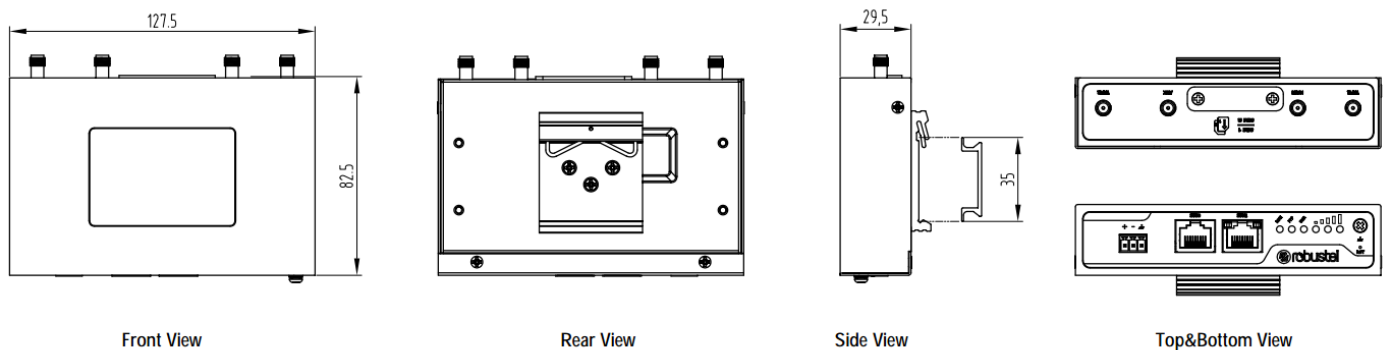
- Connector: 3-pin 3.5 mm female socket
- Input voltage: 9 to 36V DC
- Power consumption: Idle: 100 mA@12 V  
Data link: 500 mA (peak) @12 V
- PD feature\* (optional): WAN port supported  
Input voltage: 48~57V DC

*\*It is not recommended to use DC power supply and PD power supply simultaneously.*

#### Physical Characteristics

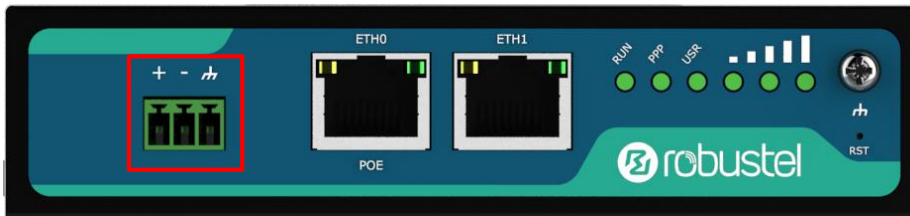
- Ingress protection: IP30
- Housing & Weight: Metal, 305 g
- Dimensions: 127.5 x 82.5 x 29.5 mm
- Installations: Desktop, wall mounting and 35 mm DIN rail mounting

## 1.4 Dimensions



## Chapter 2 Hardware Installation

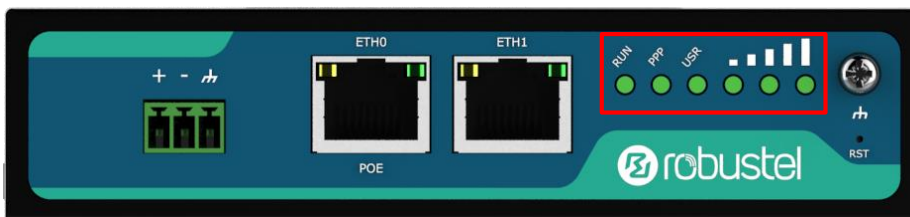
### 2.1 PIN Assignment



PIN	Polarity
1	Positive
2	Negative
3	GND


### 2.2 LED Indicators

The R2000 Router has been designed to be placed on a desktop. Below is the bottom view of the R2000.



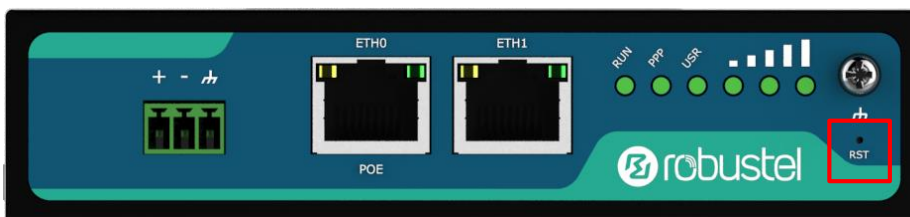
Name	Color	Status	Description
RUN	Green	On, fast blinking (250 mSec blink time)	Router is powered on (System is initializing)
		On, blinking (500 mSec blink time)	Router starts operating
		Off	Router is powered off
PPP	Green	On, solid	Link connection is working
		Off	Link connection is not working
USR-SIM	Green	On, blinking	Backup card is being used
		Off	Main card is being used
USR-NET	Green	On, solid	Network is joined successfully and worked in an optimum one
		On, blinking	Network is joined successfully but worked in a lower-level than standard
		Off	Network is not joined or joining



USR-OpenVPN	Green	On, solid	OpenVPN connection is established
		Off	OpenVPN connection is not established
USR-IPsec	Green	On, solid	IPsec connection is established
		Off	IPsec connection is not established
USR-WiFi	Green	On, solid	WiFi is enabled and working properly
		Off	WiFi is disabled or not working properly
	Green	On, 3 solid lights	High Signal strength (21-31) is available
		On, 2 solid lights	Medium Signal strength (11-20) is available
		On, 1 solid light	Low Signal strength (1-10) is available
		Off	No signal
		On, blinking	When the network is disconnected, those three signal LEDs are designed as a binary combination code to indicate a series of error report. Blinking: 1    Off: 0
			001    AT command failed 010    no SIM card detected 011    need to enter the PIN code 100    need to enter the PUK code 101    registration failed 110    module error 111    not support the module

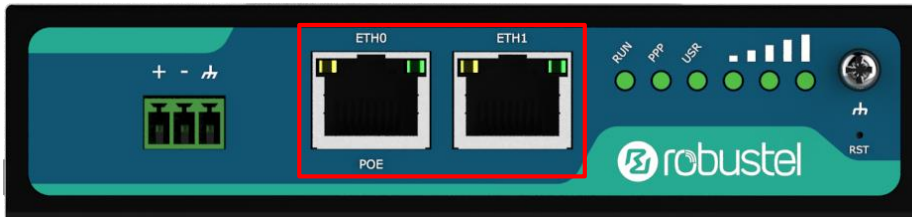
**Note:** You can choose the display type of USR LED. For more details, please refer to **3.25 Service > Advanced**.

## 2.3 Reset Button



Function	Operation
Reboot	Press and hold the RST button for 2 to 7 seconds under the operating status.
Restore to factory default settings	Wait for 3 seconds after powering up the router, press and hold the RST button until all six LEDs start blinking one by one, and release the button to return the router to factory defaults.

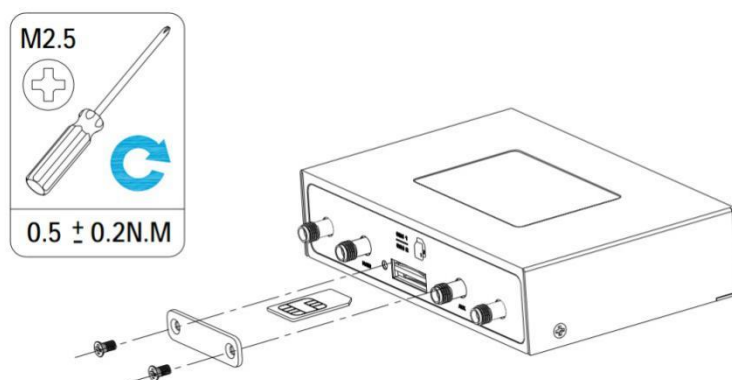
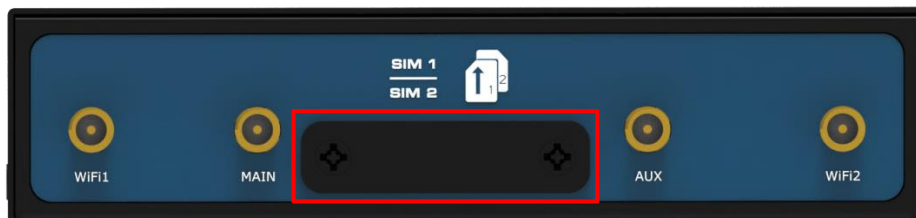
## 2.4 Ethernet Port



There are two Ethernet ports on R2000 Router, including ETH0 and ETH1. Each has two LED indicators. The yellow one is a link indicator but the green one doesn't mean anything. For details about status, see the table below.

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

## 2.5 Insert or Remove SIM Card



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

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

the cover by using a screwdriver.

4. To put back the cover and tighten the screws associated with the cover by using a screwdriver.

- **Remove SIM card**

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

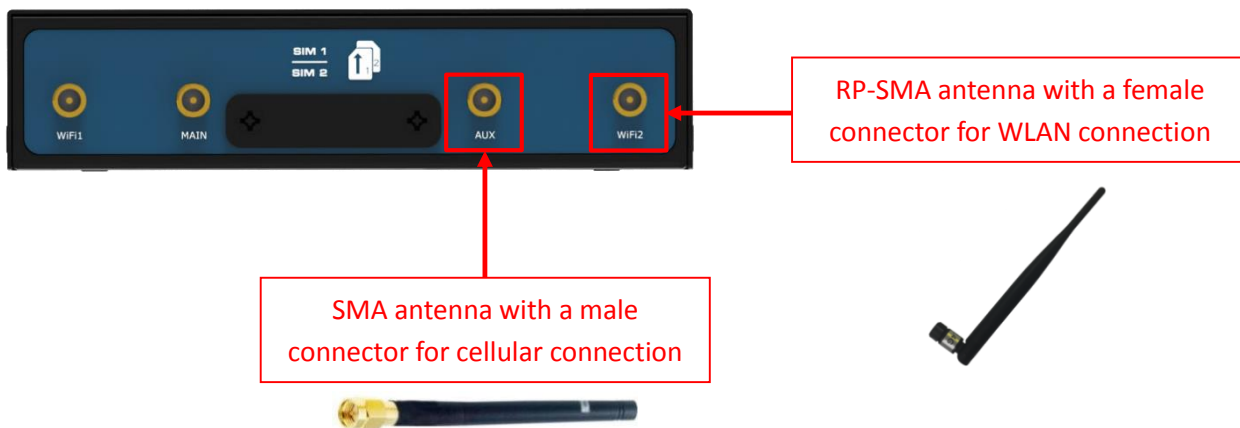
**Note:**

1. Recommended torque for inserting is 0.5 N.m, and the maximum allowed is 0.7 N.m.
2. Use the specific card when the device is working in extreme temperature (temperature exceeding 40 °C), because the regular card for long-time working in harsh environment will be disconnected frequently.
3. Do not forget to twist the cover tightly to avoid being stolen.
4. Do not touch the metal of the card surface in case information in the card will lose or be destroyed.
5. Do not bend or scratch the card.
6. Keep the card away from electricity and magnetism.
7. Make sure router is powered off before inserting or removing the card.

## 2.6 Attach External Antenna (SMA Type)

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

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

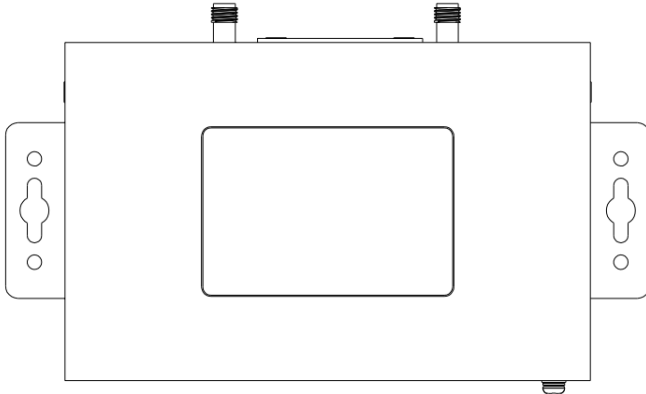


## 2.7 Mount the Router

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

### Two methods for mounting the router

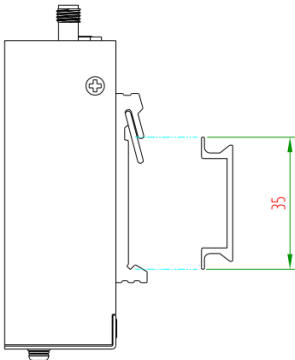
- Wall mounting (measured in mm)



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

**Note:** Recommended torque for mounting is 0.5 N.m, and the maximum allowed is 0.7 N.m.

- DIN rail mounting (measured in mm)



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

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

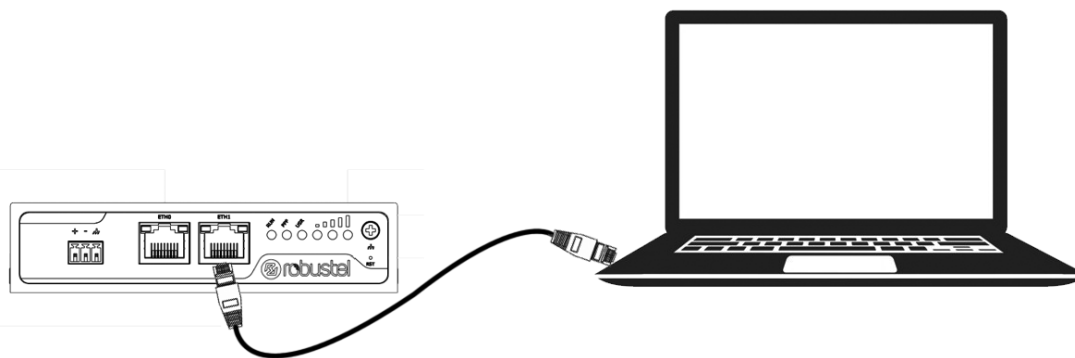
## 2.8 Ground the Router



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

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

## 2.9 Connect the Router to a Computer

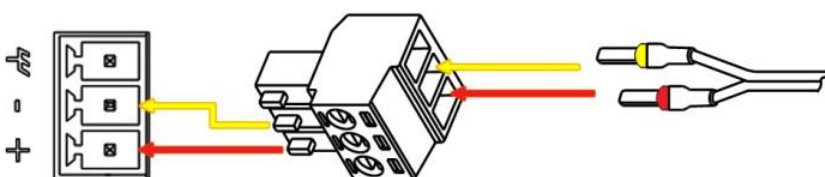


Connect an Ethernet cable to the port marked ETH0 or ETH1 at the bottom of the router, and connect the other end of the cable to your computer.

## 2.10 Power Supply

### CONNECTING THE POWER CABLE

COLOR	POLARITY
RED	+
YELLOW	-



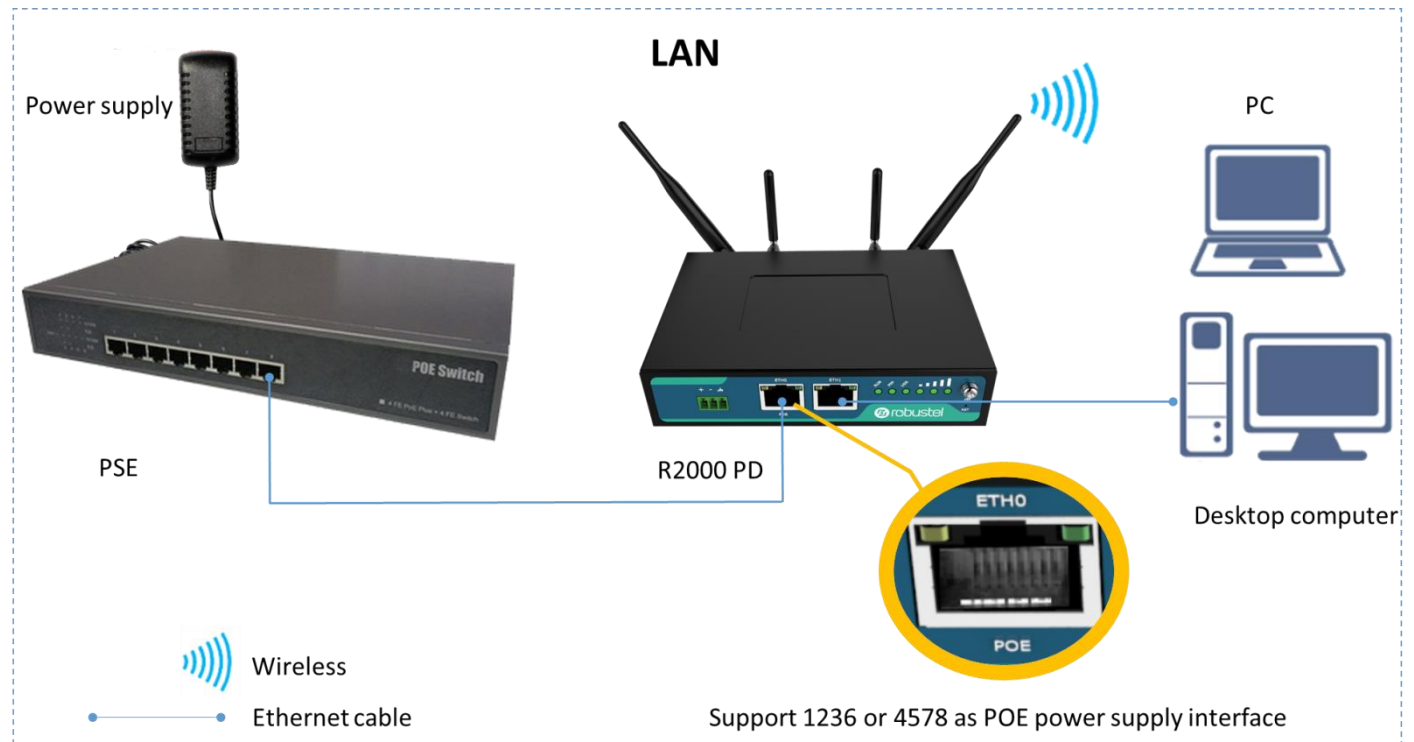
R2000 router supports reverse polarity protection, but always refers to the figure above to connect the power adapter correctly. There are two cables associated with the power adapter. Following to the color of the head, connect the cable marked red to the positive pole through a terminal block, and connect the yellow one to the negative in the same way.

**Note:** The range of power voltage is 9 to 26V DC (A014401, A014402, A014403, A014404, A014405, A014406, A014701, A014702, A014703, A014704, A014705, A014706) or 9 to 36V DC.

## 2.11 PD Connection (Optional)

If you would like to power the R2000 Router through the Ethernet port, please refer to the following topology to connect the R2000 to a PSE (Power Sourcing Equipment). The range of PoE power voltage is 48~57V DC.

**Note:** It is not recommended to use DC power supply and PD power supply simultaneously.



## Chapter 3 Initial Configuration

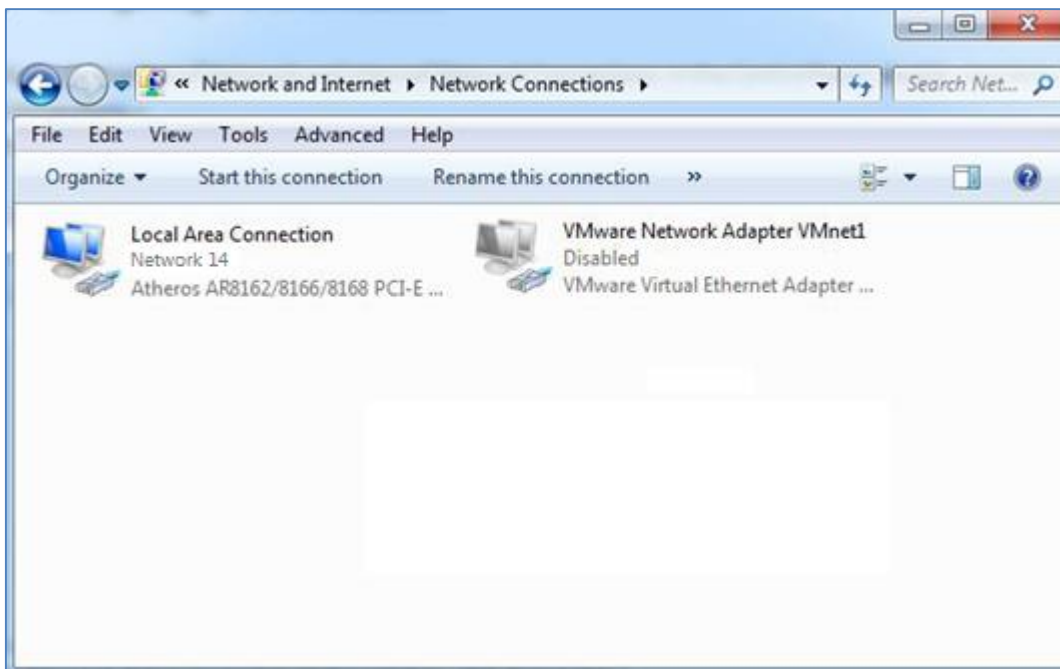
The router can be configured through your web browser that including IE 8.0 or above, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. It provides an easy and user-friendly interface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

### 3.1 Configure the PC

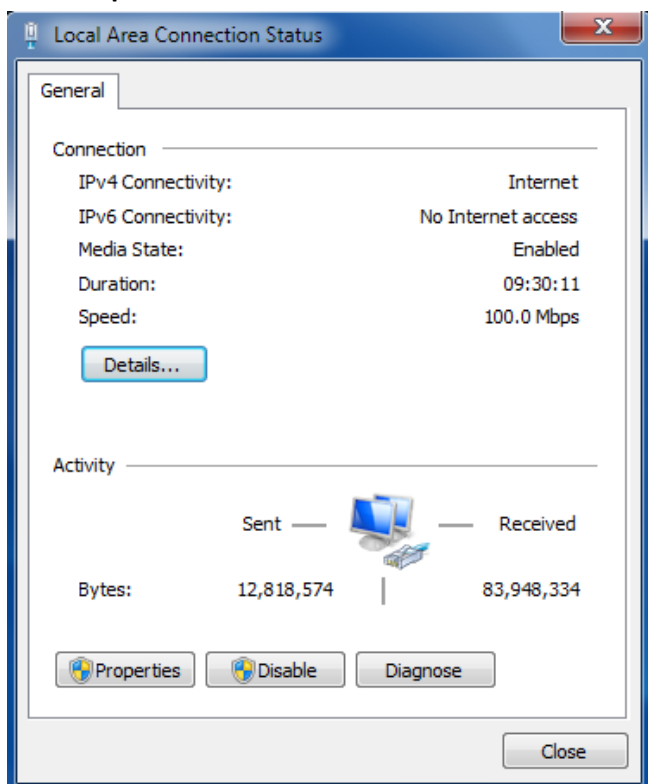
There are two methods to get IP address for the PC. One is to obtain an IP address automatically from “Local Area Connection”, and another is to configure a static IP address manually within the same subnet of the router. Please refer to the steps below.

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

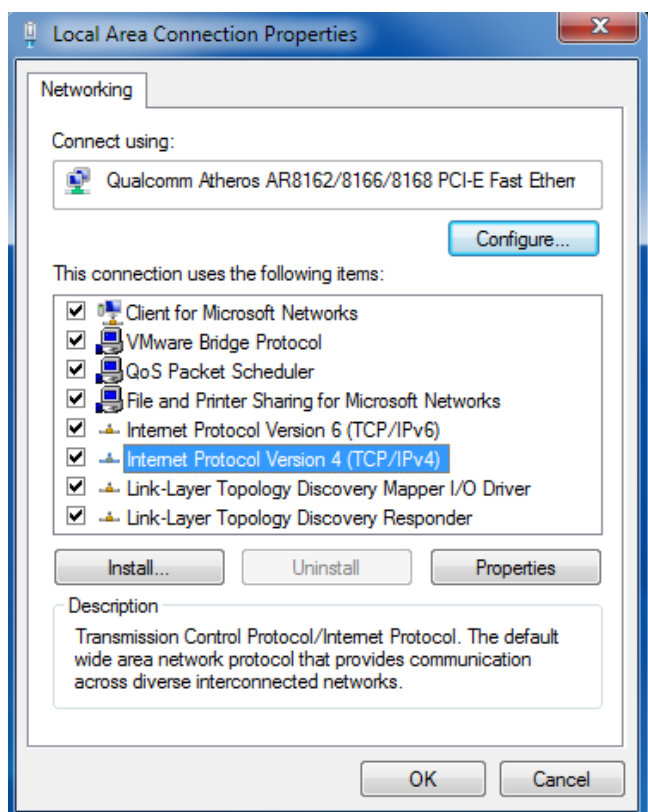
1. Click **Start > Control panel**, double-click **Network and Sharing Center**, and then double-click **Local Area Connection**.



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

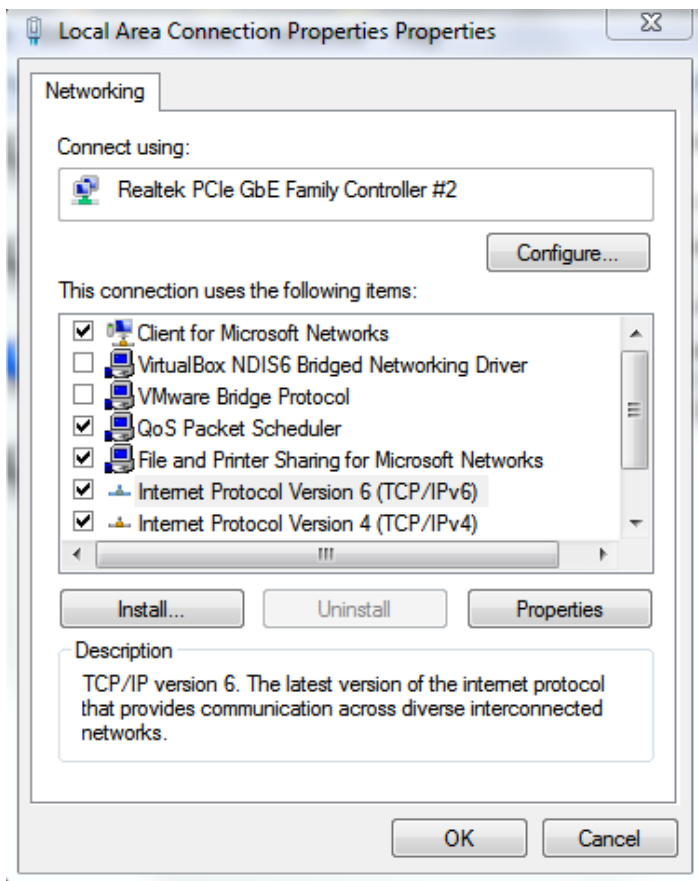


3. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



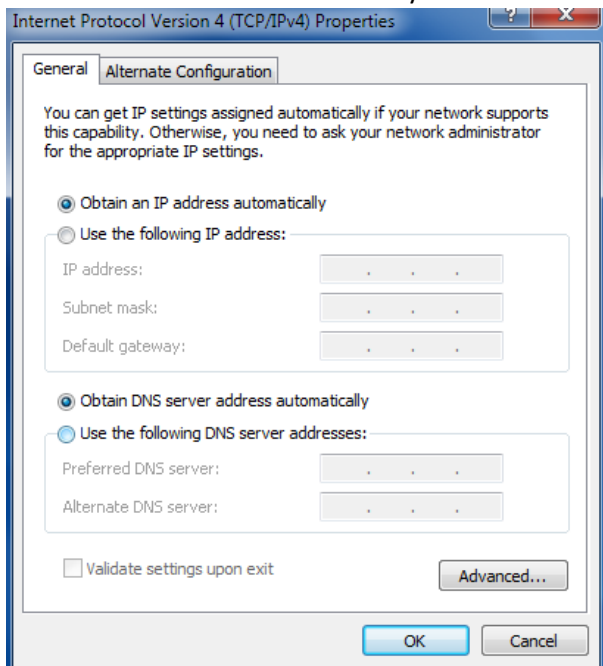


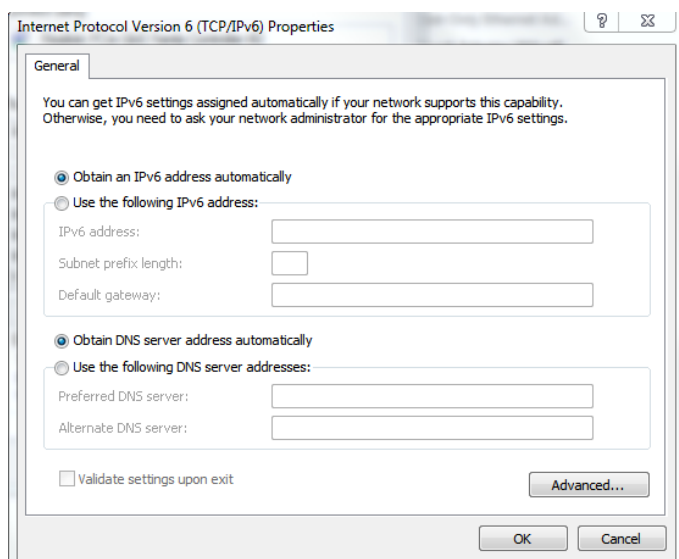
4. Choose **Internet Protocol Version 6 (TCP/IPv6)** and click **Properties**.



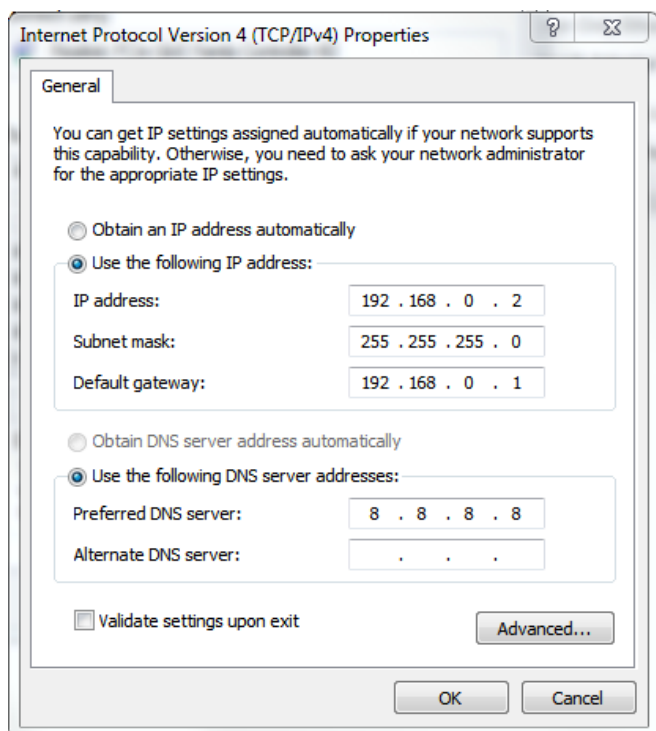
5. Two ways for configuring the IP address of PC.

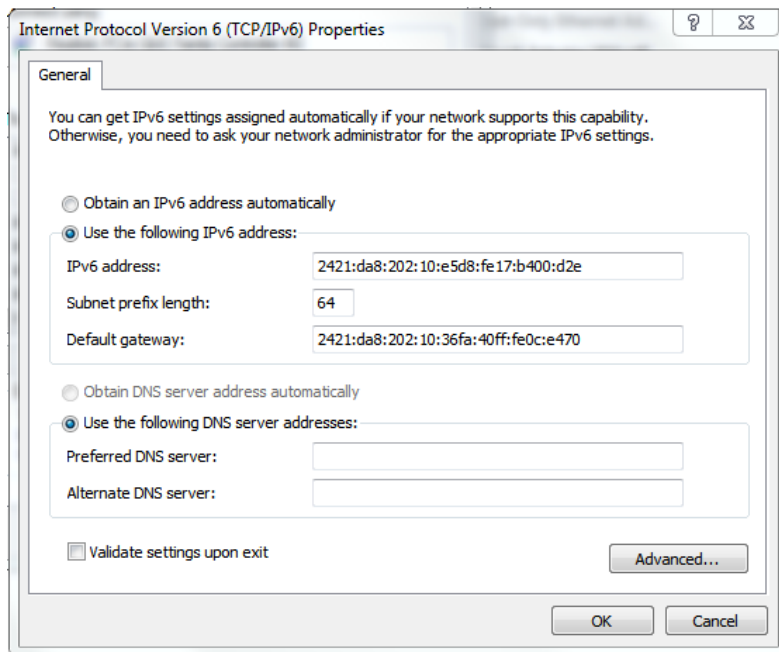
Obtain an IP address automatically from the DHCP server, click "**Obtain an IP address automatically**";





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





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

## 3.2 Factory Default Settings

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

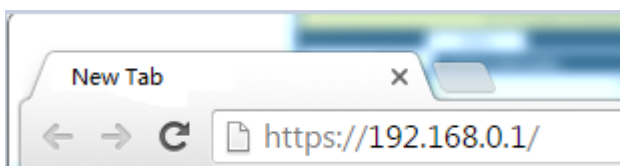
Item	Description
Username	admin
Password	admin
ETH0	192.168.0.1/255.255.255.0, LAN mode
ETH1	192.168.0.1/255.255.255.0, LAN mode
DHCP Server	Enabled

## 3.3 Log in the Router

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

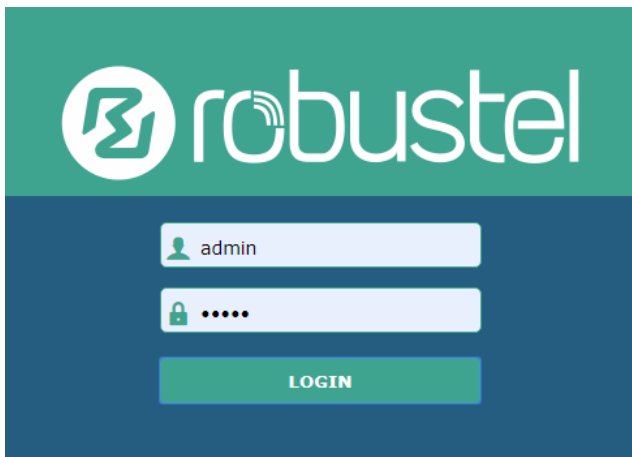
1. On your PC, open a web browser such as Internet Explorer, Google or Firefox, etc.
2. From your web browser, type the IP address of the router into the address bar and press enter. The default IP address of the router is <http://192.168.0.1/>, though the actual address may vary.

**Note:** If a SIM card with a public IP address is inserted in the router, enter this corresponding public IP address in the browser's address bar to access the router wirelessly.



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

**Note:** If enter the wrong username or password over 6 times, the login web will be locked for 5 minutes.



### 3.4 Control Panel

After logging in, the home page of the R2000 Router's web interface is displayed, for example.



The screenshot displays the Robustel R2000 Router's web interface home page. The page features a sidebar with navigation options: Status, Interface (Link Manager, LAN, Ethernet, Cellular, WiFi), Network, VPN, Services, and System. The main content area is divided into two sections: System Information and Internet Status.

**System Information:**

Device Model	R2000-L4LA
System Uptime	0 days, 00:06:57
System Time	Fri Nov 29 11:12:40 2019
RAM Usage	15M Free/64M Total
Firmware Version	3.3.0 (Rev 2888)
Hardware Version	1.0
Kernel Version	3.10.49
Serial Number	01270819110002

**Internet Status:**

Uptime	0 days, 00:00:40
Active IPv4 Link	WWAN1
IPv4 Address	10.161.3.12/255.0.0.0
IPv4 Gateway	10.0.0.1
IPv4 DNS	120.80.80.80 221.5.88.88
Active IPv6 Link	WWAN1
IPv6 Address	2408:84f3:2d:9e2c:1e:10ff:fe1f:0/64
IPv6 Gateway	fe80::4e54:99ff:fe45:e5d5
IPv6 DNS	2408:805d:8:: 2408:805c:4008::


Copyright © 2019 Robustel Technologies. All rights reserved.






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

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




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

It is strongly recommended for security purposes that you change the default username and/or password. Click the

 button to close the popup. To change your username and/or password, see **3.31 System > User Management**.

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

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

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

## 3.5 Status

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

## System Information

^ System Information		
Device Model	R2000	
System Uptime	0 days, 06:17:32	
System Time	Thu Jul 6 17:28:51 2017	
RAM Usage	17M Free/64M Total	
Firmware Version	3.0.0	
Hardware Version	1.0	
Kernel Version	3.10.49	
Serial Number	111111111	

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

## Internet Status

^ Internet Status	
Uptime	0 days, 00:00:40
Active IPv4 Link	WWAN1
IPv4 Address	10.161.3.12/255.0.0.0
IPv4 Gateway	10.0.0.1
IPv4 DNS	120.80.80.80 221.5.88.88
Active IPv6 Link	WWAN1
IPv6 Address	2408:84f3:2d:9e2c:1e:10ff:fe1f:0/64
IPv6 Gateway	fe80::4e54:99ff:fe45:e5d5
IPv6 DNS	2408:805d:8:: 2408:805c:4008::

Internet Status	
Item	Description
Uptime	Show the current amount of time the link has been connected.
IPv4 Link Description	Show the currently online link: WWAN1, WWAN2, WAN or WLAN.
IPv4 Address	Show the IPv4 address of current link.
IPv4 Gateway	Show the IPv4 gateway address of the current link.
IPv4 DNS	Show the current primary IPv4 DNS server and secondary server.
IPv6 Link Description	Show the currently online link: WWAN1, WWAN2, WAN or WLAN.
IPv6 Address	Show the IPv6 address of current link.
IPv6 Gateway	Show the IPv6 gateway address of the current link.
IPv6 DNS	Show the current primary IPv6 DNS server and secondary server.

## LAN Status

^ LAN Status	
IP Address	192.168.0.1/255.255.255.0
Active IPv6 Address	2121:da8:202:10:36fa:40ff:fe18:68e3/64
Inactive IPv6 Address	
MAC Address	34:FA:40:18:68:E3

LAN Status	
Item	Description
IP Address	Show the IP address and the Netmask of the router.
IPv6 Address	Show the IPv6 address and prefix length obtained by the router along with the current online link.
Inactive IPv6 Address	Show the IPv6 address and prefix length obtained by the router along with the current backup link.
MAC Address	Show the MAC address of the router.

## 3.6 Interface > Link Manager

This section allows you to setup the link connection.

Link Manager

Status

^ 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", "WWAN2", "WAN" or "WLAN". <ul style="list-style-type: none"> <li>WWAN1: Select to make SIM1 as the primary wireless link</li> <li>WWAN2: Select to make SIM2 as the primary wireless link</li> <li>WAN: Select to make WAN Ethernet port as the primary wired link <b>Note:</b> WAN link is available only if enable eth0 as WAN port in <b>Interface &gt; Ethernet &gt; Ports &gt; Port Settings</b>.</li> <li>WLAN: Select to make WLAN as the primary wireless link <b>Note:</b> WLAN link is available only if enable WiFi as Client mode, please refer to <b>3.10 Interface &gt; WiFi</b>.</li> </ul>	WWAN1
Backup Link	Select from "WWAN1", "WWAN2", "WAN", "WLAN" or "None". <ul style="list-style-type: none"> <li>WWAN1: Select to make SIM1 as backup wireless link</li> <li>WWAN2: Select to make SIM2 as backup wireless link</li> <li>WAN: Select to make WAN Ethernet port as the primary wired link <b>Note:</b> WAN link is available only if enable eth0 as WAN port in <b>Interface &gt; Ethernet &gt; Ports &gt; Port Settings</b>.</li> <li>WLAN: Select to make WLAN as the primary wireless link <b>Note:</b> WLAN link is available only if enable WiFi as Client mode, please refer to <b>3.10 Interface &gt; WiFi</b>.</li> <li>None: Do not select any backup link</li> </ul>	WWAN2
Backup Mode	Select from "Cold Backup", "Warm Backup" or "Load Balancing". <ul style="list-style-type: none"> <li>Cold Backup: The inactive link is offline on standby</li> <li>Warm Backup: The inactive link is online on standby</li> <li>Load Balancing: Use two links simultaneously</li> </ul> <b>Note:</b> R2000 do not support warm backup and load balancing in the situation of two WWAN links.	Cold Backup
Revert Interval	Specify the number of minutes that elapses before the primary link is checked if a backup link is being used in cold backup mode. 0 means disable checking. <b>Note:</b> Revert interval is available only under the cold backup mode.	0
Emergency Reboot	Click the toggle button to enable/disable this option. Enable to reboot the whole system if no links available.	OFF

**Note:** Click  for help.



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

^ Link Settings					
Index	Type	Description	IPv4 Connection Type	IPv6 Connection Type	
1	WWAN1	admin	DHCP	SLAAC	
2	WWAN2		DHCP	SLAAC	
3	WAN		DHCP	SLAAC	
4	WLAN		DHCP	SLAAC	

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

## WWAN1/WWAN2

Link Manager

^ General Settings

Index

1

Type

WWAN1

Description

admin

IPv6 Enable

ON OFF

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

^ WWAN Settings

Automatic APN Selection

ON OFF

Dialup Number

\*99\*\*\*1#

Authentication Type

Auto

Switch SIM By Data Allowance

ON 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

☐ ON ☒ OFF

APN

internet

Username

Password

\*\*\*\*\*

Dialup Number

\*99\*\*\*1#

Authentication Type

Auto

PPP Preferred

☐ ON ☒ OFF

Switch SIM By Data Allowance

☐ ON ☒ OFF

Data Allowance

0



Billing Day

1



### ^ IPv6 LAN Settings

Connection Type

Static

IPv6 Prefix

2521:da8:202:10::/64

IPv6 NAT Enable

☒ ON ☐ OFF

### ^ Ping Detection Settings



Enable

☒ ON ☐ OFF

IPv4 Primary Server

8.8.8.8

IPv4 Secondary Server

114.114.114.114

IPv6 Primary Server

2001:4860:4860::8888

IPv6 Secondary Server

2400:da00:2::29

Interval

300



Retry Interval

5



Timeout

3



Max Ping Tries

3



^ Advanced Settings

IPv4 NAT Enable

ON OFF

Upload Bandwidth

10000

?

Download Bandwidth

10000

Overridden Primary DNS

Overridden Secondary DNS

Overridden IPv6 Primary DNS

Overridden IPv6 Secondary DNS

Debug Enable

ON OFF

Verbose Debug Enable

ON OFF

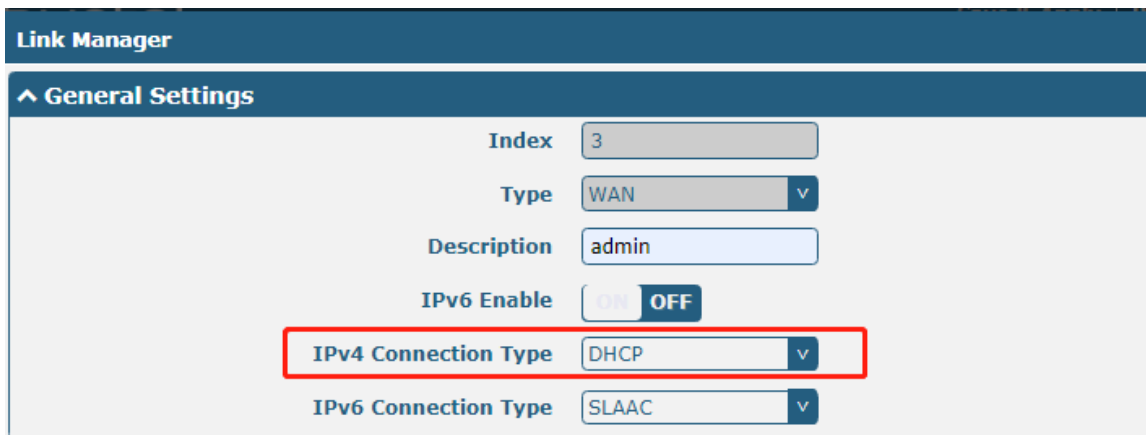
Link Settings (WWAN)		
Item	Description	Default
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WWAN1
Description	Enter a description for this link.	Null
IPv6	Click the toggle button to enable/disable IPv6.	OFF
WWAN Settings		
Automatic APN Selection	Click the toggle button to enable/disable the “Automatic APN Selection” option. After enabling, the device will recognize the access point name automatically. Alternatively, you can disable this option and manually add the access point name.	ON
APN	Enter the Access Point Name for cellular dial-up connection, provided by local ISP.	internet
Username	Enter the username for cellular dial-up connection, provided by local ISP.	Null
Password	Enter the password for cellular dial-up connection, provided by local ISP.	Null
Dialup Number	Enter the dialup number for cellular dial-up connection, provided by local ISP.	*99***1#
Authentication Type	Select from “Auto”, “PAP” or “CHAP” as the local ISP required.	Auto
PPP Preferred	The PPP dial-up method is preferred.	OFF
Switch SIM By Data Allowance	Click the toggle button to enable/disable this option. After enabling, it will switch to another SIM when the data limit reached. <b>Note:</b> Only used for dual-SIM backup.	OFF
Data Allowance	Set the monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will be displayed in <b>Interface &gt; Link Manager &gt; Status &gt; WWAN Data Usage Statistics</b> . 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
IPv6 LAN Settings		
Connection Type	Select the link to assign an IPv6 prefix to the local area network.	Delegated

Link Settings (WWAN)		
Item	Description	Default
IPv6 prefix	Set the static IPv6 prefix assigned by the link to the LAN.	Null
Enable IPv6 NAT	Set the link to enable IPv6 NAT.	OFF
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
IPv4 Primary Server	Router will ping this primary address/domain name to check that if the current IPv4 connectivity is active.	8.8.8.8
IPv4 Secondary Server	Router will ping this secondary address/domain name to check that if the current IPv4 connectivity is active.	114.114.114.114
IPv6 Primary Server	Router will ping this primary address/domain name to check that if the current IPv6 connectivity is active.	2001:4860:4860::8888
IPv6 Secondary Server	Router will ping this secondary address/domain name to check that if the current IPv6 connectivity is active.	2400:da00:2::29
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advanced Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
Upload Bandwidth	Set the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Set the download bandwidth used for QoS, measured in kbps.	10000
Specify Primary DNS	Defines the primary IPv4 DNS server used by the link.	Null
Specify Secondary DNS	Defines the secondary IPv4 DNS server used by the link.	Null
Specify IPv6 Primary DNS	Defines the primary IPv6 DNS server used by the link.	Null
Specify IPv6 Secondary DNS	Defines the secondary IPv6 DNS server used by the link.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

## WAN

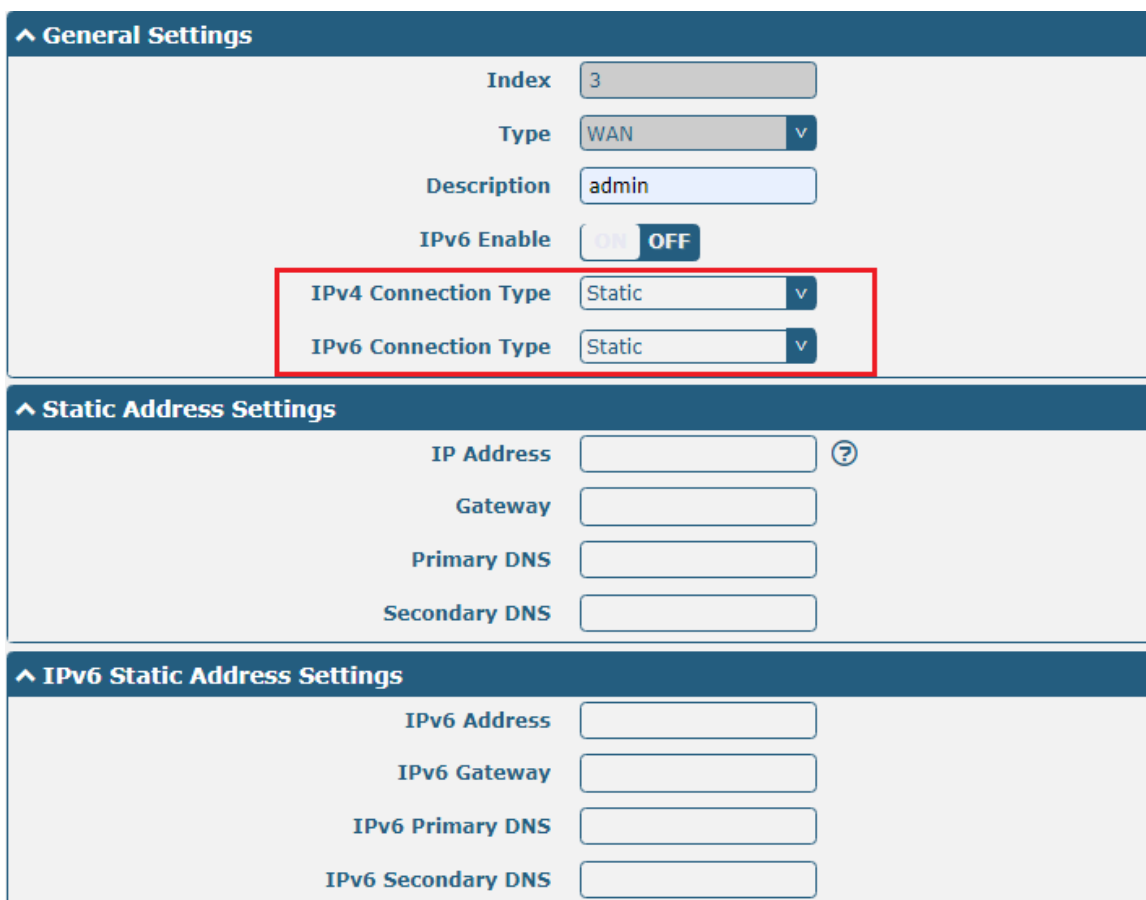
Router will obtain IP automatically from DHCP server if choosing “**DHCP**” as **IPv4 connection type**. The window is displayed as below.

The router will automatically obtain an IPv6 prefix from the DHCP server When SLAAC is selected for **IPv6 Connection Type**.



The screenshot shows the 'Link Manager' window with the 'General Settings' tab selected. The 'Index' is 3, 'Type' is WAN, and 'Description' is admin. The 'IPv6 Enable' toggle is set to OFF. The 'IPv4 Connection Type' is set to DHCP, and the 'IPv6 Connection Type' is set to SLAAC. A red rectangle highlights the 'IPv4 Connection Type' dropdown menu.

The window is displayed as below when choosing “**Static**” as the **IPv4 connection type** and **IPv6 connection type**.



The screenshot shows the 'Link Manager' window with the 'General Settings' tab selected. The 'Index' is 3, 'Type' is WAN, and 'Description' is admin. The 'IPv6 Enable' toggle is set to OFF. The 'IPv4 Connection Type' is set to Static, and the 'IPv6 Connection Type' is set to Static. A red rectangle highlights both dropdown menus. Below the 'General Settings' tab, the 'Static Address Settings' tab is visible, showing fields for IP Address, Gateway, Primary DNS, and Secondary DNS. The 'IPv6 Static Address Settings' tab is also visible, showing fields for IPv6 Address, IPv6 Gateway, IPv6 Primary DNS, and IPv6 Secondary DNS.

The window is displayed as below when choosing “**PPPoE**” as the **IPv4 connection type** and **IPv6 connection type**

### ^ General Settings

Index Type Description IPv6 Enable ☐ ON ☒ OFFIPv4 Connection Type IPv6 Connection Type Address Mode 

### ^ PPPoE Settings

Username Password Authentication Type PPP Expert Options  ?

### ^ Ping Detection Settings

Enable ☒ ON ☐ OFFIPv4 Primary Server IPv4 Secondary Server IPv6 Primary Server IPv6 Secondary Server Interval  ?Retry Interval  ?Timeout  ?Max Ping Tries  ?

### ^ Advanced Settings

IPv4 NAT Enable ☒ ON ☐ OFFMTU  ?Upload Bandwidth  ?Download Bandwidth Overridden Primary DNS Overridden Secondary DNS Overridden IPv6 Primary DNS Overridden IPv6 Secondary DNS Debug Enable ☒ ON ☐ OFFVerbose Debug Enable ☐ ON ☒ OFF

Link Settings (WAN)		
Item	Description	Default
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WAN
Description	Enter a description for this link.	Null
Enable IPv6	Click the toggle button to enable / disable IPv6.	OFF
IPv4 Connection Type	Select from "DHCP", "Static" or "PPPoE".	DHCP
IPv6 Connection Type	Select from "SLAAC", "DHCPv6", "Static" or "PPPoE".	SLAAC
Address Type	Select from "SLAAC" or "DHCPv6".	SLAAC
IPv4 Static Address Settings		
IP Address	Set the IP address with Netmask which can access the Internet. IP address with Netmask, e.g. 192.168.1.1/24	Null
Gateway	Set the gateway of the IP address in WAN port.	Null
Primary DNS	Set the primary DNS.	Null
Secondary DNS	Set the secondary DNS.	Null
IPv6 Static Address Settings		
IPv6 Address	Set the IP address with Netmask which can access the Internet. IP address with Netmask, e.g. 2521:da8:202:10::20/64.	Null
Gateway	Set the gateway of the IPv6 address in WAN port.	Null
IPv6 Primary DNS	Defines the primary IPv6 DNS server used by the link.	Null
IPv6 Secondary DNS	Defines an alternative IPv6 DNS server for the link.	Null
PPPoE Settings		
Username	Enter the username provided by your Internet Service Provider.	Null
Password	Enter the password provided by your Internet Service Provider.	Null
Authentication Type	Select from "Auto", "PAP" or "CHAP" as the local ISP required.	Auto
PPP Expert Options	Enter the PPP Expert options used for PPPoE dialup. You can enter some other PPP dial strings in this field. Each string can be separated by a semicolon.	Null
IPv6 LAN Ping Settings		
Connection Type	Select the link to assign an IPv6 prefix to the local area network.	Delegated
IPv6 Prefix	Set the static IPv6 prefix assigned by the link to the LAN.	Null
Enable IPv6 NAT	Set the link to enable IPv6 NAT.	OFF
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.114.114
IPv6 Primary Server	The router pings the primary address / domain name to detect whether the current IPv6 connection is always present.	2001:4860:4860::8888

IPv6 Secondary Server	The router pings the alternate address / domain name to detect whether the current IPv6 connection is always present.	2400:da00:2::29
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
<b>Advanced Settings</b>		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Specify Primary DNS	Defines the primary IPv4 DNS server used by the link.	Null
Specify Secondary DNS	Defines the secondary IPv4 DNS server for the link.	Null
Specify IPv6 Primary DNS server	Defines the primary IPv6 DNS server used by the link.	Null
Specify IPv6 secondary DNS server	Defines the secondary IPv6 DNS server for the link.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

## WLAN

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

Link Manager

^ General Settings

Index

3

Type

WLAN

Description

IPv6 Enable

ON OFF

IPv4 Connection Type

DHCP

^ WLAN Settings

SSID

router

Connect to Hidden SSID

ON OFF

Password



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

^ General Settings

Index

3

Type

WLAN

v

Description

IPv6 Enable

ON

OFF

IPv4 Connection Type

Static

v

v WLAN Settings

^ Static Address Settings

IP Address

?

Gateway

Primary DNS

Secondary DNS

R2000 Router does not support the **PPPoE** WLAN Connection Type.

^ IPv6 LAN Settings

Connection Type

Static

v

IPv6 Prefix

IPv6 NAT Enable

ON

OFF

^ Ping Detection Settings

?

Enable

ON

OFF

IPV4 Primary Server

8.8.8.8

IPv4 Secondary Server

114.114.114.114

IPv6 Primary Server

2001:4860:4860::8888

IPv6 Secondary Server

2400:da00:2::29

Interval

300

?

Retry Interval

5

?

Timeout

3

?

Max Ping Tries

3

?

**Advanced Settings**

IPv4 NAT Enable

ON OFF

MTU

1500

?

Upload Bandwidth

10000

?

Download Bandwidth

10000

Overridden Primary DNS

Overridden Secondary DNS

Overridden IPv6 Primary DNS

Overridden IPv6 Secondary DNS

Debug Enable

ON OFF

Verbose Debug Enable

ON OFF

Link Settings (WLAN)		
Item	Description	Default
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WLAN
Description	Enter a description for this link.	Null
Enable Ipv6	Click the toggle button to enable/disable IPv6.	OFF
Connection Type	Select from "DHCP" or "Static".	DHCP
WLAN Settings		
SSID	Enter a 1-32 characters SSID which your router wants to connect. SSID (Service Set Identifier) is the name of your wireless network.	router
Connect to Hidden SSID	Click the toggle button to enable/disable this option. When router works as Client mode and needs to connect any access point which has hidden SSID, you need to enable this option.	OFF
Password	Enter an 8-63 characters password of the access point which your router wants to connect.	Null
Static Address Settings		
IP Address	Enter the IP address with Netmask which can access the Internet, e.g. 192.168.1.1/24	Null
Gateway	Enter the IP address of WiFi AP.	Null
Primary DNS	Set the primary DNS.	Null
Secondary DNS	Set the secondary DNS.	Null
IPv6 LAN Settings		
Connection Type	Select link to assign IPv6 prefix to LAN	Delegated
IPv6 Prefix	Set the static IPv6 prefix assigned by the link to the LAN	Null
Enable IPv6 NAT	Set the link to enable IPv6 NAT	OFF
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
Primary Server	Router will ping this primary address/domain name to check that if the	8.8.8.8

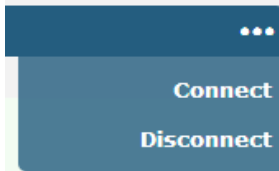
	current connectivity is active.	
Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.114.114
IPv6 Primary Server	Router will ping this primary address/domain name to check that if the current IPv6 connectivity is active.	2001:4860:4860::8888
IPv6 Secondary Server	Router will ping this secondary address/domain name to check that if the current IPv6 connectivity is active.	2400:da00:2::29
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
<b>Advance Settings</b>		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Specify Primary DNS	Defines the primary IPv4 DNS server used by the link.	Null
Specify Secondary DNS	Defines the secondary IPv4 DNS server for the link.	Null
Specify IPv6 Primary DNS server	Defines the primary IPv6 DNS server used by the link.	Null
Specify IPv6 secondary DNS server	Defines the secondary IPv6 DNS server for the link.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

## Status

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

Link Manager		Status		
^ Link Status				
Index	IPv4 Link	IPv6 Link	Status	Uptime
1	WWAN1	WWAN1	Connected	0 days, 00:01:12
2	WWAN2	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.

^ Link Status

Index	IPv4 Link	IPv6 Link	Status	Uptime
1	WWAN1	WWAN1	Connected	0 days, 06:54...

Index 1

IPv4 Link WWAN1

IPv6 Link WWAN1

Status Connected

IPv4 Interface wwan

IPv6 Interface wwan

Uptime 0 days, 06:54:37

IPv4 Address 10.37.98.229/255.255.255.252

IPv4 Gateway 10.37.98.230

IPv4 DNS 120.80.80.80 221.5.88.88

IPv6 Address 2408:84f3:1034:96f9:1e:10ff:fe1f:0/64

IPv6 Gateway fe80::4e54:99ff:fe45:e5d5

IPv6 DNS 2408:805d:8:: 2408:805c:4008::

RX Packets 712

TX Packets 979

RX Bytes 47530

TX Bytes 80258

^ WWAN Data Usage Statistics

WWAN1 Monthly Stats

Clear

WWAN2 Monthly Stats

Clear



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

### 3.7 Interface > LAN




This section allows you to set the related parameters for LAN port. There are two LAN ports on R2000 Router, including ETH0 and ETH1. The ETH0 and ETH1 can freely choose from lan0 and lan1, but at least one LAN port must be assigned as lan0. The default settings of ETH0 and ETH1 are lan0 and their default IP are 192.168.0.1/255.255.255.0.

#### LAN

By default, there is a LAN port (lan0) in the list. To begin adding a new LAN port (lan1), please configure ETH0 or ETH1 as lan1 first in **Ethernet > Ports > Port Settings**. Otherwise, the operation will be prompted as “List is full”.

LAN	Multiple IP	Status			
^ Network Settings					
Index	Interface	IPv4 Address...	Netmask	VLAN ID	
1	lan0	192.168.0.1	255.255.255.0	0	 

**Note:** Lan0 cannot be deleted.

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

LAN	
^ General Settings	
Index	<input type="text" value="1"/>
Interface	<input type="text" value="lan0"/> v
IPv4 Address	<input type="text" value="192.168.2.1"/>
Netmask	<input type="text" value="255.255.255.0"/>
IPv6 Address Allocation Type	<input type="text" value="SLAAC"/> v
MTU	<input type="text" value="1500"/> ?

General Settings @ LAN		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Interface	Show the editing port. Lan1 is available only if it was selected by one of ETH0~ETH1 in <b>Ethernet &gt; Ports &gt; Port Settings</b> .	--
IP Address	Set the IP address of the LAN port.	192.168.0.1
Netmask	Set the Netmask of the LAN port.	255.255.255.0
IPv6 Address Assignment Type	Set the method of assigning IPv6 addresses on the LAN side.	SLAAC
MTU	Enter the Maximum Transmission Unit.	1500

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

^ DHCP Settings

Enable ☒ ON ☐ OFF

Mode Server v

IP Pool Start

IP Pool End

Subnet Mask

^ DHCP Advanced Settings

Gateway

Primary DNS

Secondary DNS

WINS Server

Lease Time  ?

Static Lease  ?

Expert Options  ?

Debug Enable ☐ ON ☒ OFF

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

^ DHCP Settings

Enable ☒ ON ☐ OFF

Mode Relay v

DHCP Server For Relay

^ DHCP Advanced Settings

Debug Enable ☐ ON ☒ OFF

LAN		
Item	Description	Default
DHCP Settings		
Enable	Click the toggle button to enable/disable the DHCP function.	ON
Mode	Select from “Server” or “Relay”. <ul style="list-style-type: none"> <li>Server: Lease IP address to DHCP clients which have been connected to LAN port</li> <li>Relay: Router can be a DHCP Relay, which will provide a relay tunnel to solve the problem that DHCP Client and DHCP Server are not in a same subnet</li> </ul>	Server
IP Pool Start	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.0.2
IP Pool End	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.0.100

LAN		
Item	Description	Default
Subnet Mask	Define the subnet mask of IP address obtained by DHCP clients from DHCP server.	255.255.255.0
DHCP Server for Relay	Enter the IP address of DHCP relay server.	Null
DHCP Advanced Settings		
Gateway	Define the gateway assigned by the DHCP server to the clients, which must be on the same network segment with DHCP address pool.	Null
Primary DNS	Define the primary DNS server assigned by the DHCP server to the clients.	Null
Secondary DNS	Define the secondary DNS server assigned by the DHCP server to the clients.	Null
WINS Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever.	Null
Lease Time	Set the lease time which the client can use the IP address obtained from DHCP server, measured in seconds.	120
Static lease	Bind a lease to correspond an IP address via a MAC address. format: mac,ip;mac,ip;..., e.g. FF:ED:CB:A0:98:01,192.168.0.200	Null
Expert Options	Enter some other options of DHCP server in this field. format: config-desc;config-desc, e.g. log-dhcp;quiet-dhcp	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for DHCP information output.	OFF




## Multiple IP

LAN
Multiple IP
Status

^ Multiple IP Settings

Index	Interface	IP Address	Netmask
-------	-----------	------------	---------

+

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

Multiple IP

^ IP Settings

Index	<input type="text" value="1"/>
Interface	<input type="text" value="lan0"/> v
IP Address	<input type="text"/>
Netmask	<input type="text"/>

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

## VLAN Trunk

LAN	Multiple IP	VLAN Trunk	Status	
^ VLAN Settings				
Index	Enable	Interface	VID	IP Address
				Netmask

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

VLAN Trunk	
^ VLAN Settings	
Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Interface	<input type="text" value="lan0"/> v
VID	<input type="text" value="100"/>
IP Address	<input type="text"/>
Netmask	<input type="text"/>

VLAN Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this VLAN. Enable to make router can encapsulate and de-encapsulate the VLAN tag.	ON
Interface	Choose the interface which wants to enable VLAN trunk function. Select from "lan0" or "lan1" depends on your ETH0 and ETH1's corresponding LAN ports.	lan0
VID	Set the tag ID of VLAN and digits from 1 to 4094.	100
IP Address	Set the IP address of VLAN port.	Null
Netmask	Set the Netmask of VLAN port.	Null



## Status

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

LAN	Multiple IP	Status		
^ Interface Status				
Index	Interface	IP Address	Active IPv6 Address	
1	lan0	192.168.0.1/255.2...	2221:da8:202:10:36fa:4...	
^ Connected Devices				
Index	IPv4/IPv6 Address	MAC Address	Interface	Inactive Time
1	192.168.0.59	D0:50:99:A9:2B:80	lan0	0s
^ DHCP Lease Table				
Index	IPv4/IPv6 Address	MAC Address or IAID	Interface	Expired Time
1	192.168.0.59	d0:50:99:a9:2b:80	lan0	0 days, 01:51:38

^ DHCP Lease Table				
Index	IP Address	MAC Address	Interface	Expired Time

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

^ Connected Devices				
Index	IPv4/IPv6 Address	MAC Address	Interface	Inactive Time
1	192.168.0.59	D0:50:99:A9:2B:80	lan0	0s
<div> <div>Index</div> <div>1</div> </div>				
<div> <div>IPv4/IPv6 Address</div> <div>192.168.0.59</div> </div>				
<div> <div>MAC Address</div> <div>D0:50:99:A9:2B:80</div> </div>				
<div> <div>Interface</div> <div>lan0</div> </div>				
<div> <div>Inactive Time</div> <div>0s</div> </div>				

## 3.8 Interface > Ethernet

This section allows you to set the related parameters for Ethernet. There are two Ethernet ports on R2000 Router, including ETH0 and ETH1. The ETH0 on the router can be configured as either a WAN port or LAN port, also can be assigned as a PoE port, while ETH1 can only be configured as a LAN port. The default settings of ETH0 and ETH1 are lan0 and their default IP are 192.168.0.1/255.255.255.0.

Ports	Status	
^ Port Settings		
Index	Port	Port Assignment
1	eth0	lan0
2	eth1	lan0

Click  button of eth0 to configure its parameters, and modify the port assignment parameters of eth0 in the

pop-up window.

**Ports**

**^ Port Settings**

Index

Port

Port Assignment

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

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



Ports	Status	
^ Port Status		
Index	Port	Link
1	eth0	Down
2	eth1	Up


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

^ Port Status		
Index	Port	Link
1	eth0	Down
2	eth1	Up
Index 2 Port eth1 Link Up		

### 3.9 Interface > Cellular

This section allows you to set the related parameters of Cellular. The R2000 Router has two SIM card slots, but do not support two SIM cards online simultaneously due to its single-module design. If insert single SIM card at the first time, SIM1 slot and SIM2 slots are available.

Cellular					Status	AT Debug
^ Advanced Cellular Settings						
Index	SIM Card	Phone Number	Network Type	Band Select Type		
1	SIM1		Auto	All		
2	SIM2		Auto	All		

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

**Cellular**

**^ General Settings**

Index	<input type="text" value="1"/>
SIM Card	<input type="text" value="SIM1"/> v
Phone Number	<input type="text"/>
PIN Code	<input type="text"/> ?
Extra AT Cmd	<input type="text"/> ?
Telnet Port	<input type="text" value="0"/> ?

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

**^ Cellular Network Settings**

Network Type	<input type="text" value="Auto"/> v ?
Band Select Type	<input type="text" value="All"/> v ?

**^ Advanced Settings**

Debug Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Verbose Debug Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

Note: When it is a BG96 module, the options in "Network Type" are as follows:

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

^ 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

**Note:** When the device selection module is BG96, the options in "Network Type" are as follows.

^ Cellular Network Settings

Network Type
Auto
?

Band Select Type
Auto
2G Only
M1 Only
NB Only
?

^ Advanced Settings

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

Cellular		
Item	Description	Default
Cellular Network Settings		
Network Type	<p>Select the cellular network type, which is the network access order. Select from “Auto”, “2G Only”, “2G First”, “3G Only”, “3G First”, “4G Only”, “4G First”.</p> <ul style="list-style-type: none"> <li>Auto: Connect to the best signal network automatically</li> <li>2G Only: Only the 2G network is connected</li> <li>2G First: Connect to the 2G Network preferentially</li> <li>3G Only: Only the 3G network is connected</li> <li>3G First: Connect to the 3G Network preferentially</li> <li>4G Only: Only the 4G network is connected</li> <li>4G First: Connect to the 4G Network preferentially</li> </ul> <p><b>Note:</b> When the device selection module is BG96, select from “Auto”, “2G Only”, “M1 Only”, “NB Only”.</p> <ul style="list-style-type: none"> <li>Auto: Connect to the best signal network automatically</li> <li>2G Only: Only the 2G network is connected</li> <li>M1 Only: Only the CAT M1 network is connected</li> <li>NB Only: Only the NB-IOT network is connected</li> </ul>	Auto
Band Select Type	Select from “All” or “Specify”. You may choose certain bands if choosing “Specify”.	All
Advanced Settings		
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

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

Cellular	Status	AT Debug		
^ Status				
Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	EC25-E	460015687108599	Registered to home network

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

^ Status				
Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	EC25-E	460015687108599	Registered to home network
Index 1				
Modem Status Ready				
Modem Model EC25-E				
Current SIM SIM1				
Phone Number				
IMSI 460015687108599				
ICCID 89860119801073537094				
Registration Registered to home network				
Network Provider CHN-UNICOM				
Network Type LTE				
Signal Strength 27 (-59dBm)				
Bit Error Rate 99				
PLMN ID 46001				
Local Area Code 2507				
Cell ID 6074716				
IMEI 866758047488842				
Firmware Version EC25EFAR06A03M4G				

Status	
Item	Description
Index	Indicate the ordinal of the list.
Modem Status	Show the status of the radio module.
Modem Model	Show the model of the radio module.
Current SIM	Show the SIM card that your router is using.
Phone Number	Show the phone number of the current SIM. <b>Note:</b> This option will be displayed if enter manually in <b>Cellular &gt; Advanced Cellular Settings &gt; SIM1/SIM2 &gt; General Settings &gt; Phone Number</b> .
IMSI	Show the IMSI number of the current SIM.
ICCID	Show the ICCID number of the current SIM.
Registration	Show the current network status.
Network Provider	Show the name of Network Provider.
Network Type	Show the current network service type, e.g. GPRS.
Signal Strength	Show the signal strength detected by the mobile.
Bit Error Rate	Show the current bit error rate.
PLMN ID	Show the current PLMN ID.
Local Area Code	Show the current local area code used for identifying different area.
Cell ID	Show the current cell ID used for locating the router.

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

This page allows you to check the AT Debug.

Cellular
Status
AT Debug

^ AT Debug

Command

Result

Send

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

## 3.10 Interface > WiFi (Optional)

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

### WiFi AP

#### Configure Router as WiFi AP

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

WiFi
Access Point
Advanced
ACL
Status

^ General Settings

Mode AP ?

Region SE ?

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

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

WiFi	Access Point	Advanced	ACL	Status
<b>^ General Settings</b>				
Enable <input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF				
Wireless Mode 11bgn Mixed v				
Channel Auto v ?				
SSID router				
Broadcast SSID <input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF				
Security Mode Disabled v ?				

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

<b>^ General Settings</b>				
Enable <input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF				
Wireless Mode 11bgn Mixed v				
Channel Auto v ?				
SSID router				
Broadcast SSID <input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF				
Security Mode WPA-Personal v ?				
WPA Version Auto v				
Encryption Auto v ?				
PSK Password v ?				
Group Key Update Interval 3600				

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

<b>^ General Settings</b>				
Enable <input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF				
Wireless Mode 11bgn Mixed v				
Channel Auto v ?				
SSID router				
Broadcast SSID <input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF				
Security Mode WPA-Enterprise v ?				
WPA Version Auto v				
Encryption Auto v ?				
Radius Authentication Server Address v				
Radius Authentication Server Port 1812				
Radius Server Share Secret v				
Group Key Update Interval 3600				



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

^ General Settings

Enable

ON OFF

Wireless Mode

11bgn Mixed

v

Channel

Auto

v

?

SSID

router

Broadcast SSID

ON OFF

Security Mode

WEP

v

?

WEP Key

?

General Settings @ Access Point		
Item	Description	Default
Enable	Click the toggle button to enable/disable the WiFi access point option.	OFF
Wireless Mode	Select from “11bgn Mixed”, “11b Only”, “11g Only” or “11n Only”. <ul style="list-style-type: none"> <li>11bgn Mixed: Mix three agreements, for backward compatibility</li> <li>11b only: IEEE 802.11b, 11Mbit/s~2.4GHz</li> <li>11g only: IEEE 802.11g, 54Mbit/s~2.4GHz</li> <li>11n only: IEEE 802.11n, 300Mbps~600Mbps</li> </ul>	11bgn Mixed
Channel	Select the frequency channel, including “Auto”, “1”, “2” ..... “13”. <ul style="list-style-type: none"> <li>Auto: Router will scan all frequency channels until the best one is found</li> <li>1~13 Router will be fixed to work with this channel Following are the frequency of 1~13 channel: 1: 2412 MHz 2: 2417 MHz 3: 2422 MHz 4: 2427 MHz 5: 2432 MHz 6: 2437 MHz 7: 2442 MHz 8: 2447 MHz 9: 2452 MHz 10: 2457 MHz 11: 2462 MHz 12: 2467 MHz 13: 2472 MHz</li> </ul>	Auto

General Settings @ Access Point		
Item	Description	Default
SSID	Enter the Service Set Identifier, the name of your wireless network. The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other. Enter 1 to 32 characters.	router
Broadcast SSID	Click the toggle button to enable/disable the SSID being broadcast. When enabled, the client can scan your SSID. When disabled, the client cannot scan your SSID. If you want to connect to the router AP, you need to manually enter the SSID of router AP at WiFi client side.	ON
Security Mode	<p>Select from “Disabled”, “WPA-Personal”, “WPA-Enterprise” or “WEP”.</p> <ul style="list-style-type: none"> <li>Disabled: User can access the WiFi without password</li> </ul> <p><b>Note:</b> It is strongly recommended for security purposes that you do not choose this kind of mode.</p> <ul style="list-style-type: none"> <li>WPA-Personal: WiFi Protected Access only provides one password used for Identity Authentication</li> <li>WPA-Enterprise: Provides an authentication interface for EAP which can be authenticated via Radius Authentication Server or other Extended Authentication</li> <li>WEP: Wired Equivalent Privacy provides encryption for wireless device’s data transmission</li> </ul>	Disabled
WPA Version	<p>Select from “Auto”, “WPA” or “WPA2”.</p> <ul style="list-style-type: none"> <li>Auto: Router will choose automatically the most suitable WPA version</li> <li>WPA2 is a stronger security feature than WPA</li> </ul>	Auto
Encryption	<p>Select from “Auto”, “TKIP” or “AES”.</p> <ul style="list-style-type: none"> <li>Auto: Router will choose automatically the most suitable encryption</li> <li>TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication</li> </ul> <p><b>Note:</b> It's not recommended to use TKIP encryption in 802.11n mode.</p> <ul style="list-style-type: none"> <li>AES: AES encryption uses a wireless connection. AES can be used for CCMP WPA-PSK and WPA 802.1x authentication. AES is a stronger encryption algorithm than TKIP</li> </ul>	Auto
PSK Password	Enter the Pre share key password. When router works as AP mode, enter Master key to generate keys for encryption. A PSK Password is used as a basis for encryption methods (or cipher types) in a WLAN connection. The PSK Password should be complicated and as long as possible. For security reasons, this PSK Password should only be disclosed to users who need it, and it should be changed regularly. Enter 8 to 63 characters.	Null

General Settings @ Access Point		
Item	Description	Default
Radius Authentication Server Address	Enter the address of radius authentication server.	Null
Radius Authentication Server Port	Enter the port of radius authentication server.	1812
Radius Server Share Secret	Enter the shared secret of radius authentication server.	Null
Group Key Update Interval	Enter the time period of group key renewal.	3600
WEP Key	Enter the WEP key. The key length should be 10 or 26 hexadecimal digits depending on which WEP key is used, 64 digits or 128 digits.	Null

WiFi

Access Point

Advanced

ACL

Status

^ Advanced Settings

Max Associated Stations

64

Beacon Interval

100

?

DTIM Period

2

?

RTS Threshold

2347

?

Fragmentation Threshold

2346

?

Transmit Rate

Auto

v

11N Transmit Rate

Auto

v

Transmit Power

Max

v

Channel Width

Auto

v

?

Enable WMM

ON

OFF

Enable Short GI

ON

OFF

?

Enable AP Isolation

ON

OFF

?

Debug Level

none

v

Advanced Settings		
Item	Description	Default
Max Associated Stations	Set the max number of clients allowed to access the router's AP.	64
Beacon Interval	Set the interval of time in which the router AP broadcasts a beacon which is used for wireless network authentication.	100
DTIM Period	Set the delivery traffic indication message period and the router AP will multicast the data according to this period.	2
RTS Threshold	Set the "request to send" threshold. When the threshold set as 2347, the router AP will not send detection signal before sending data. And when the threshold set as 0, the router AP will send detection signal before sending data.	2347
Fragmentation Threshold	Set the fragmentation threshold of a WiFi AP. It is recommended that you use the default value 2346.	2346
Transmit Rate	Set the transmit rate. You can choose Auto or specify a Transmit	Auto

Advanced Settings		
Item	Description	Default
	Rate, including 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps, MCS0, MCS1, MCS2, MCS3, MCS4, MCS5, MCS6 and MCS7.	
11N Transmit Rate	Specify the transmit rate under the IEEE 802.11n mode or let is default to "Auto".	Auto
Transmit Power	Select from "Max", "High", "Medium" or "Low".	Max
Channel Width	Select from "Auto", "20MHz" or "40MHz". <b>Note:</b> 40 MHz channel width provides higher available data rate, twice as many as 20 MHz channel width.	Auto
Enable WMM	Click the toggle button to enable/disable the WMM option.	ON
Enable Short GI	Click the toggle button to enable/disable the Short Guard Interval option. Short GI is a blank time between two symbols, providing a long buffer time for signal delay. Using the Short GI would increase 11% in data rates, but also result in higher packet error rates.	ON
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option. When enabled, the router will isolate all connected wireless devices. The wireless device cannot access the router directly via WLAN.	OFF
Debug Level	Select from "verbose", "debug", "info", "notice", "warning" or "none".	none

WiFi

Access Point

Advanced

ACL

Status

^ General Settings

Enable ACL

ON OFF

ACL Mode

Accept

?

^ Access Control List

Index	Description	MAC Address
+		

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

ACL

^ Access Control List

Index

1

Description

MAC Address

ACL		
Item	Description	Default
General Settings		
Enable ACL	Click the toggle button to enable/disable this option.	OFF
ACL Mode	Select from "Accept" or "Deny". <ul style="list-style-type: none"> <li>Accept: Only the packets fitting the entities of the "Access Control List" can be allowed</li> </ul>	Accept

ACL		
Item	Description	Default
	<ul style="list-style-type: none"> <li>Deny: All the packets fitting the entities of the “Access Control List” will be denied</li> </ul> <p><b>Note:</b> Router can only allow or deny devices which are included in “Access Control List” at one time.</p>	
Access Control List		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this access control list.	Null
MAC Address	Add a MAC address here.	Null

This section allows you to view the status of AP.

WiFi	Access Point	Advanced	ACL	Status	
^ AP Status					
		Status	COMPLETED		
		Channel	6		
		Channel Width	20 MHz		
		MAC Address	34:FA:40:01:DE:02		
^ Associated Stations					
Index	MAC Address	IP Address	Name	Connected Time	Signal

## WiFi Client

### Configure Router as WiFi Client

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

WiFi
^ General Settings
<div>Mode</div> <div>Client</div> <div>?</div>
<div>Region</div> <div>SE</div> <div>?</div>

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

WiFi
^ General Settings
<div>Mode</div> <div>Client</div> <div>?</div>
<div>Region</div> <div>SE</div> <div>?</div>

Status

Interface

Link Manager

LAN

Ethernet

Cellular

WiFi

WLAN

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


^ WLAN Settings	
SSID	<input type="text" value="Robustel"/>
Connect to Hidden SSID	<input type="button" value="ON"/> <input checked="" type="button" value="OFF"/>
Password	<input type="password" value="••••••••"/>

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

Status	
^ WLAN Status	
IPv4 Status	Connected
IPv6 Status	Connected
Uptime	0 days, 00:00:12
IPv4 Address	192.168.10.106/255.255.255.0
IPv4 Gateway	192.168.10.1
IPv4 DNS	192.168.10.1
IPv6 Address	2001:1221::36fa:40ff:fe03:b311/64
IPv6 Gateway	fe80::36fa:40ff:fe18:68be
IPv6 DNS	fe80::c06:1dff:fea1:f0ab
MAC Address	34:fa:40:03:b3:11

^ Link Status	
Signal	-70 dBm
Noise	-95 dBm
Width	20 MHz
TX Bitrate	6.5 MBit/s MCS 0
TX	3166 bytes (27 packets)
RX	21277 bytes (189 packets)

^ WPA Status	
WPA State	COMPLETED
Frequency	2422
BSSID	88:da:1a:2a:69:bc
SSID	routerIpv63000
Mode	station
Key Management	WPA2-PSK
Pairwise Cipher	CCMP
Group Cipher	TKIP

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


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

### 3.11 Network > Route

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

#### Static Route

Static Route		Status				
^ Static Route Table						
Index	Description	Destination	Netmask/Prefix Length	Gateway	Interface	+

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

**Static Route**

^ Static Route

Index

Description

Destination

Netmask/Prefix Length

?

Gateway

Interface

wlan0
v

Static Route		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this static route.	Null
Destination	Enter the IP address of destination host or destination network.	Null
Netmask/ Ipv6 Address Prefix Length	Enter the Netmask of destination host or destination network.	Null
Gateway	Define the gateway of the destination.	Null
Interface	Choose the corresponding port of the link that you want to configure.	wwan

## Status

This window allows you to view the status of route.



Static Route		Status			
^ Route Table					
Index	Destination	Netmask/Prefix Length	Gateway	Interface	Metric
1	0.0.0.0	0.0.0.0	192.168.10.1	wlan0	0
2	192.168.0.0	255.255.255.0	0.0.0.0	lan0	0
3	192.168.10.0	255.255.255.0	0.0.0.0	wlan0	0
4	2001:1221::	64	::	wlan0	256
5	2001:4860:4860::...	128	fe80::36fa:40ff:fe...	wlan0	0
6	2400:da00:2::29	128	fe80::36fa:40ff:fe...	wlan0	0
7	2421:da8:202:10::	64	::	lan0	256
8	fe80::	64	::	lan0	256
9	fe80::	64	::	eth1	256
10	fe80::	64	::	wwan	256
11	fe80::	64	::	wlan0	256
12	::	0	fe80::36fa:40ff:fe...	wlan0	1024
13	ff02::1	128	::	lan0	0
14	ff02::1	128	::	wlan0	0
15	ff02::2	128	::	wlan0	0
16	ff02::16	128	::	lan0	0
17	ff02::1:2	128	::	wlan0	0
18	ff02::1:3	128	::	lan0	0
19	ff02::1:ff14:4f32	128	::	lan0	0
20	ff00::	8	::	lan0	256
21	ff00::	8	::	eth1	256
22	ff00::	8	::	wwan	256
23	ff00::	8	::	wlan0	256

## 3.12 Network > Firewall

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

### Filtering

The filtering rules can be used to either accept or block certain users or ports from accessing your router. Click Network> Firewall> Filter. The following information is displayed:

Filtering	Port Mapping	Custom Rules	DMZ	Status
<b>General Settings</b>				
Enable Filtering <input type="checkbox"/> ON <input type="checkbox"/> OFF				
Default Filtering Policy <input type="text" value="Accept"/> <input type="button" value="v"/> <input type="button" value="?"/>				
<b>Access Control Settings</b>				
Enable Remote SSH Access <input type="checkbox"/> ON <input type="checkbox"/> OFF				
Enable Local SSH Access <input type="checkbox"/> ON <input type="checkbox"/> OFF				
Enable Remote Telnet Access <input type="checkbox"/> ON <input type="checkbox"/> OFF				
Enable Local Telnet Access <input type="checkbox"/> ON <input type="checkbox"/> OFF				
Enable Remote HTTP Access <input type="checkbox"/> ON <input type="checkbox"/> OFF				
Enable Local HTTP Access <input type="checkbox"/> ON <input type="checkbox"/> OFF				
Enable Remote HTTPS Access <input type="checkbox"/> ON <input type="checkbox"/> OFF				
Enable Remote Ping Respond <input type="checkbox"/> ON <input type="checkbox"/> OFF <input type="button" value="?"/>				
Enable DOS Defending <input type="checkbox"/> ON <input type="checkbox"/> OFF				
Enable Console <input type="checkbox"/> ON <input type="checkbox"/> OFF <input type="button" value="?"/>				
Enable VPN NAT Traversal <input type="checkbox"/> ON <input type="checkbox"/> OFF <input type="button" value="?"/>				
<b>Whitelist Rules</b> <input type="button" value="?"/>				
Index	Description	Source Address		
<input type="button" value="+"/>				
<b>Filtering Rules</b>				
Index	Source Address	Source Port	Source MAC	Target Address
				Target Port
				Protocol
<input type="button" value="+"/>				

Click  to add the whitelist rules.

Filtering
<b>Whitelist Rules</b>
Index <input type="text" value="1"/>
Description <input type="text"/>
Source Address <input type="text"/> <input type="button" value="?"/>

Click  to add a filtering rule. The maximum count is 50. The window is displayed as below when defaulting "All", "ICMP" or choosing "ICMPv6" as the protocol. Here take "All" as an example.

Filtering

^ Filtering Rules

Index

1

Description

Source Address

?

Source MAC

?

Target Address

?

Protocol

All

v

Action

Drop

v

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

^ Filtering Rules

Index

1

Description

Source Address

?

Source Port

?

Source MAC

?

Target Address

?

Target Port

?

Protocol

TCP

v

Action

Drop

v

Filtering		
Item	Description	Default
General Settings		
Enable Filtering	Click the toggle button to enable/disable the filtering option.	ON
Default Filtering Policy	Select from “Accept” or “Drop”. Cannot be changed when filtering rules table is not empty. <ul style="list-style-type: none"> <li>Accept: Router will accept all the connecting requests except the hosts which fit the drop filter list</li> <li>Drop: Router will drop all the connecting requests except the hosts which fit the accept filter list</li> </ul>	Accept
Access Control Settings		
Enable Remote SSH Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via SSH.	OFF
Enable Local SSH Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via SSH.	ON
Enable Remote Telnet Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via Telnet.	OFF

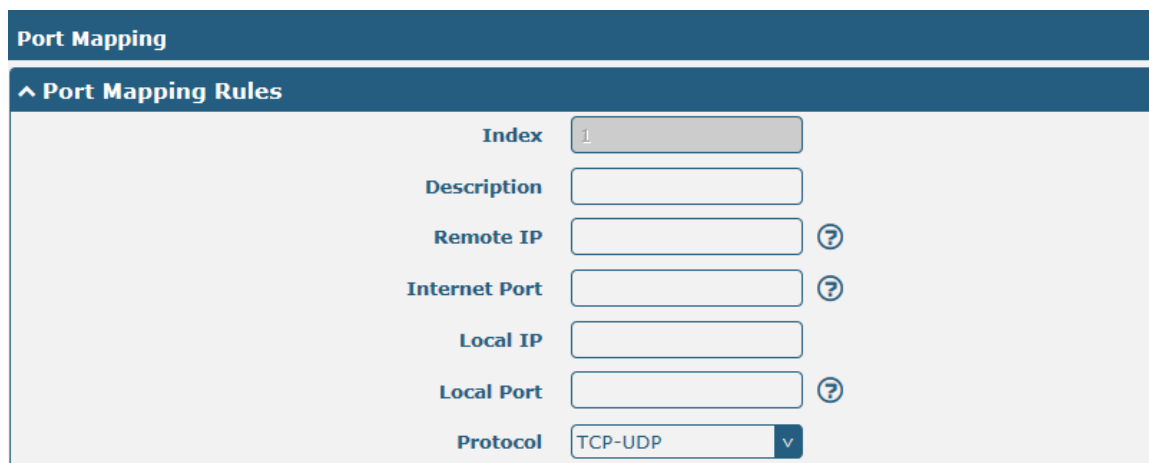
Filtering		
Item	Description	Default
Enable Local Telnet Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via Telnet.	ON
Enable Remote HTTP Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via HTTP.	OFF
Enable Local HTTP Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via HTTP.	ON
Enable Remote HTTPS Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via HTTPS.	ON
Enable Remote Ping Respond	Click the toggle button to enable/disable this option. When enabled, the router will reply to the Ping requests from other hosts on the Internet.	ON
Enable DOS Defending	Click the toggle button to enable/disable this option. When enabled, the router will defend the DOS. Dos attack is an attempt to make a machine or network resource unavailable to its intended users.	ON
Enable debug port	Click the toggle button to enable / disable this option.	ON
Enable vpn nat traversal	Click the toggle button to enable / disable this option. When enabled, enable NAT traversal for GRE / L2TP / PPTP VPN packets.	OFF
Whitelist Rules		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this whitelist rule.	Null
Source Address	Specify an access originator and enter its source address.	Null
Filtering Rules		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this filtering rule.	Null
Source Address	Specify an access originator and enter its source address.	Null
Source Port	Specify an access originator and enter its source port.	Null
Source MAC	Specify an access originator and enter its source MAC address.	Null
Target Address	Enter the target address which the access originator wants to access.	Null
Target Port	Enter the target port which the access originator wants to access.	Null
Protocol	Select from "All", "TCP", "UDP", "ICMP", "ICMPv6" or "TCP-UDP". <b>Note:</b> It is recommended that you choose "All" if you don't know which protocol of your application to use.	All
Action	Select from "Accept" or "Drop". <ul style="list-style-type: none"> <li>Accept: When Default Filtering Policy is drop, router will drop all the connecting requests except the hosts which fit this accept filtering list</li> <li>Drop: When Default Filtering Policy is accept, router will accept all the connecting requests except the hosts which fit this drop filtering list</li> </ul>	Drop

## Port Mapping

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



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



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

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



Click  to add an IPv4 or IPv6 custom rule, the window is displayed as follows (take "IPv4" as an example):

## Custom Rules

### ^ Custom Iptables Rule

Index

Description

Rule  ?

### Custom Firewall Rules

Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this Custom Firewall Rules.	Null
Rule	Enter custom rules.	Null

## DMZ

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

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

Filtering
Port Mapping
DMZ

### ^ DMZ Settings

Enable DMZ

Host IP Address

Source IP Address  ?

### DMZ Settings

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

Click the Status bar to view the firewall status of the device.

Filtering	Port Mapping	Custom Rules	DMZ	Status			
^ Chain Input							
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	DROP	tcp	wlan0	*	0.0.0.0/0	0.0.0.0/0
2	0	DROP	tcp	wlan0	*	0.0.0.0/0	0.0.0.0/0
3	0	DROP	tcp	wlan0	*	0.0.0.0/0	0.0.0.0/0
4	0	REJECT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
5	6	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
6	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
7	5	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
8	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
9	0	ACCEPT	icmp	*	*	0.0.0.0/0	0.0.0.0/0
10	0	DROP	icmp	*	*	0.0.0.0/0	0.0.0.0/0
11	0	DROP	tcp	wlan0	*	::/0	::/0
12	0	DROP	tcp	wlan0	*	::/0	::/0
13	0	DROP	tcp	wlan0	*	::/0	::/0
14	0	REJECT	tcp	*	*	::/0	::/0
15	0	ACCEPT	tcp	*	*	::/0	::/0
16	0	DROP	tcp	*	*	::/0	::/0
17	0	ACCEPT	tcp	*	*	::/0	::/0
18	0	DROP	tcp	*	*	::/0	::/0
19	0	ACCEPT	icmpv6	*	*	::/0	::/0
20	0	DROP	icmpv6	*	*	::/0	::/0
^ Chain Forward							
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	TCPMSS	tcp	*	*	0.0.0.0/0	0.0.0.0/0
2	0	TCPMSS	tcp	*	*	::/0	::/0
^ Chain Output							
Index	Packets	Target	Protocol	In	Out	Source	Destination

### 3.13 Network > IP Passthrough

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

IP Passthrough

^ General Settings

Enable
☐ OFF

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

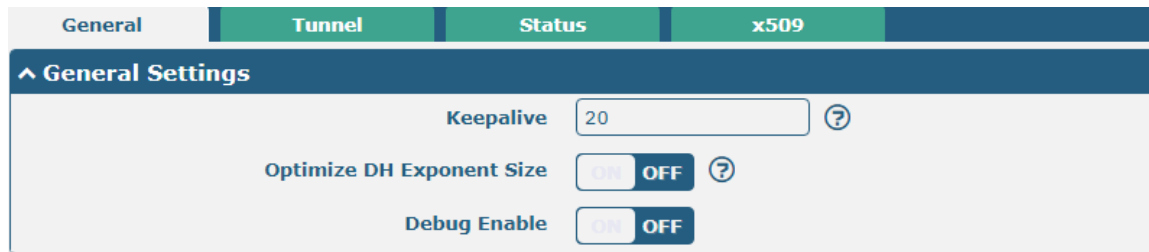
### 3.14 VPN > IPsec

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

a communication session.

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

## General

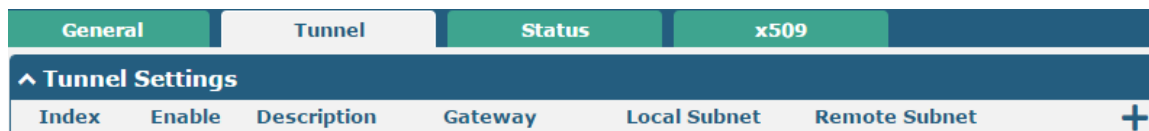


The General Settings interface shows tabs for General, Tunnel, Status, and x509. The General tab is active. It contains the following settings:

- Keepalive:** A text input field with the value 20 and a help icon.
- Optimize DH Exponent Size:** A toggle switch currently set to OFF with a help icon.
- Debug Enable:** A toggle switch currently set to OFF with a help icon.

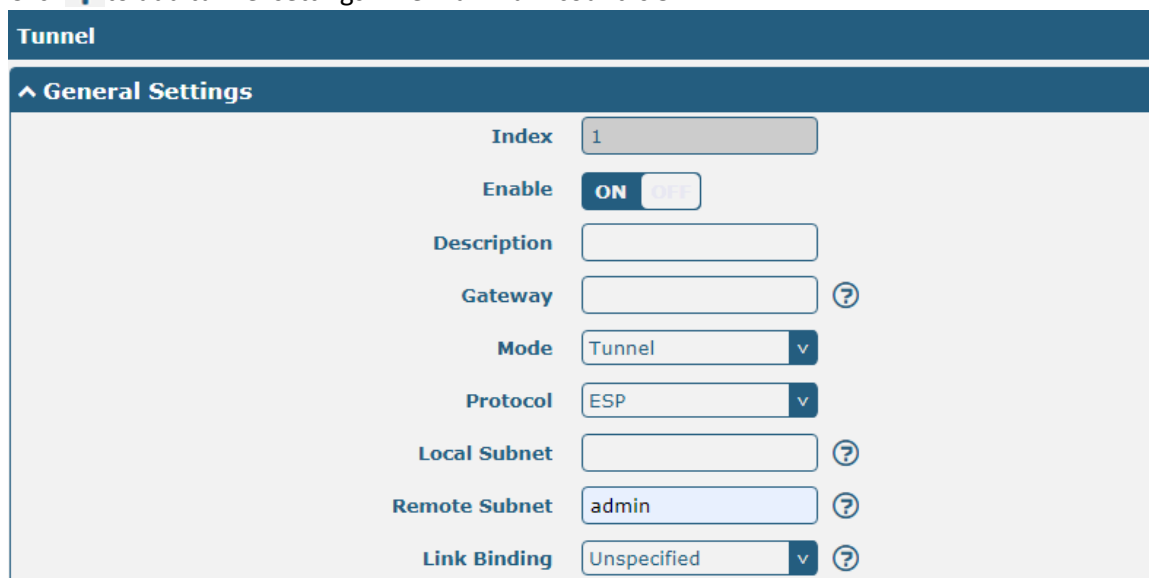
General Settings @ General		
Item	Description	Default
Enable NAT Traversal	Click the toggle button to enable/disable the NAT Traversal function. This option must be enabled when router under NAT environment.	ON
Keepalive	Set the keepalive time, measured in seconds. The router will send packets to NAT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

## Tunnel



The Tunnel Settings interface shows tabs for General, Tunnel, Status, and x509. The Tunnel tab is active. It displays a table with columns: Index, Enable, Description, Gateway, Local Subnet, Remote Subnet, and a plus icon (+) to add new settings.

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



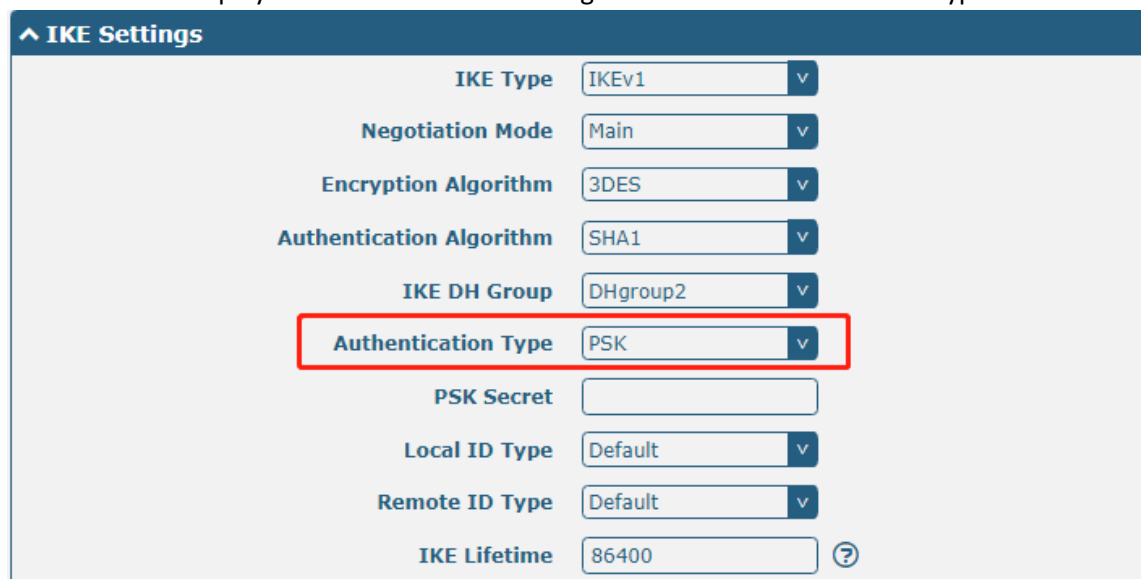
The Tunnel General Settings interface shows the configuration for a specific tunnel (Index 1). The settings are as follows:

- Index:** 1
- Enable:** A toggle switch currently set to ON.
- Description:** An empty text input field.
- Gateway:** An empty text input field with a help icon.
- Mode:** A dropdown menu currently set to Tunnel.
- Protocol:** A dropdown menu currently set to ESP.
- Local Subnet:** An empty text input field with a help icon.
- Remote Subnet:** A text input field with the value 'admin' and a help icon.
- Link Binding:** A dropdown menu currently set to Unspecified with a help icon.



General Settings @ Tunnel		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this IPsec tunnel.	ON
Description	Enter a description for this IPsec tunnel.	Null
Gateway	Enter the address or domain name of remote side IPsec VPN server. 0.0.0.0 represents for any address.	Null
Mode	Select from "Tunnel" and "Transport". <ul style="list-style-type: none"> <li>Tunnel: Commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it</li> <li>Transport: Used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host-for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination</li> </ul>	Tunnel
Protocol	Select the security protocols from "ESP" and "AH". <ul style="list-style-type: none"> <li>ESP: Use the ESP protocol</li> <li>AH: Use the AH protocol</li> </ul>	ESP
Local Subnet	Enter the local subnet's address with mask protected by IPsec, e.g. 192.168.1.0/24	Null
Remote Subnet	Enter the remote subnet's address with mask protected by IPsec, e.g. 10.8.0.0/24	Null
Link binding	Select from WWAN1, WWAN2, WAN, or WLAN.	Not bound

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



The screenshot shows the 'IKE Settings' window. The 'Authentication Type' dropdown is highlighted with a red box and set to 'PSK'. Other settings include: IKE Type (IKEv1), Negotiation Mode (Main), Encryption Algorithm (3DES), Authentication Algorithm (SHA1), IKE DH Group (DHgroup2), PSK Secret (empty), Local ID Type (Default), Remote ID Type (Default), and IKE Lifetime (86400).

Setting	Value
IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	PSK
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400

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



The screenshot shows the 'IKE Settings' window. The 'Authentication Type' dropdown is highlighted with a red box and set to 'CA'. Other settings include: IKE Type (IKEv1), Negotiation Mode (Main), Encryption Algorithm (3DES), Authentication Algorithm (SHA1), IKE DH Group (DHgroup2), Private Key Password (empty), and IKE Lifetime (86400).

Setting	Value
IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	CA
Private Key Password	
IKE Lifetime	86400

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



The screenshot shows the 'IKE Settings' window. The 'Authentication Type' dropdown is highlighted with a red box and set to 'PKCS#12'. Other settings include: IKE Type (IKEv1), Negotiation Mode (Main), Encryption Algorithm (3DES), Authentication Algorithm (SHA1), IKE DH Group (DHgroup2), Private Key Password (empty), and IKE Lifetime (86400).

Setting	Value
IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	PKCS#12
Private Key Password	
IKE Lifetime	86400

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

^ IKE Settings

IKE Type

IKEv1

v

Negotiation Mode

Main

v

Encryption Algorithm

3DES

v

Authentication Algorithm

SHA1

v

IKE DH Group

DHgroup2

v

Authentication Type

xAuth PSK

v

PSK Secret

Local ID Type

Default

v

Remote ID Type

Default

v

Username

?

Password

?

IKE Lifetime

86400

?

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

^ IKE Settings

IKE Type

IKEv1

v

Negotiation Mode

Main

v

Encryption Algorithm

3DES

v

Authentication Algorithm

SHA1

v

IKE DH Group

DHgroup2

v

Authentication Type

xAuth CA

v

Private Key Password

Username

?

Password

?

IKE Lifetime

86400

?

IKE Settings		
Item	Description	Default
IKE Type	Select from "IKEv1" and "IKEv2".	IKEv1
Negotiation Mode	Select from “Main” and “Aggressive” for the IKE negotiation mode in phase 1. If the IP address of one end of an IPsec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main
Authentication Algorithm	Select from “MD5”, “SHA1”, “SHA2 256” or “SHA2 512” to be used in IKE negotiation.	SHA1
Encrypt Algorithm	Select from “3DES”, “AES128”, “AES192” and “AES256” to be used in IKE negotiation.	3DES

IKE Settings		
Item	Description	Default
	<ul style="list-style-type: none"> <li>3DES: Use 168-bit 3DES encryption algorithm in CBC mode</li> <li>AES128: Use 128-bit AES encryption algorithm in CBC mode</li> <li>AES256: Use 256-bit AES encryption algorithm in CBC mode</li> </ul>	
IKE DH Group	Select from "DHgroup1", "DHgroup2", "DHgroup5", "DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17" or "DHgroup18" to be used in key negotiation phase 1.	DHgroup2
Authentication Type	Select from "PSK", "CA", "PKCS#12", "xAuth PSK" and "xAuth CA" to be used in IKE negotiation. <ul style="list-style-type: none"> <li>PSK: Pre-shared Key</li> <li>CA: x509 Certificate Authority</li> <li>xAuth: Extended Authentication to AAA server</li> </ul>	PSK
PSK Secret	Enter the pre-shared key.	Null
Local ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. <ul style="list-style-type: none"> <li>Default: Use an IP address as the ID in IKE negotiation</li> <li>FQDN: Use an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com.</li> <li>User FQDN: Use a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security gateway, e.g., test@robustel.com.</li> </ul>	Default
Remote ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. <ul style="list-style-type: none"> <li>Default: Use an IP address as the ID in IKE negotiation</li> <li>FQDN: Use an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com.</li> <li>User FQDN: Use a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security gateway, e.g., test@robustel.com.</li> </ul>	Default
IKE Lifetime	Set the lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as the new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.	86400
Private Key Password	Enter the private key under the "CA" and "xAuth CA" authentication types.	Null
Username	Enter the username used for the "xAuth PSK" and "xAuth CA" authentication types.	Null
Password	Enter the password used for the "xAuth PSK" and "xAuth CA" authentication types.	Null

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

**^ General Settings**

Index	1
Enable	<b>ON</b> OFF
Description	
Gateway	
Mode	Tunnel v
Protocol	ESP v
Local Subnet	
Remote Subnet	
Link Binding	Unspecified v

**^ IKE Settings**

**^ SA Settings**

Encryption Algorithm	3DES v
Authentication Algorithm	SHA1 v
PFS Group	DHgroup2 v
SA Lifetime	28800 ?
DPD Interval	30 ?
DPD Failures	150 ?

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

**^ General Settings**

Index	1
Enable	<b>ON</b> OFF
Description	
Gateway	
Mode	Tunnel v
Protocol	AH v
Local Subnet	
Remote Subnet	
Link Binding	Unspecified v

**^ IKE Settings**

**^ SA Settings**

Authentication Algorithm

PFS Group

SA Lifetime

DPD Interval

DPD Failures

**^ Advanced Settings**

Enable Compression ☐ OFF

Enable Forceencaps ☐ OFF

Expert Options

SA Settings		
Item	Description	Default
Encrypt Algorithm	Select from "3DES", "AES128" or "AES256" when you select "ESP" in "Protocol". Higher security means more complex implementation and lower speed. DES is enough to meet general requirements. Use 3DES when high confidentiality and security are required.	3DES
Authentication Algorithm	Select from "MD5", "SHA1", "SHA2 256" or "SHA2 512" to be used in SA negotiation.	MD5
PFS Group	Select from "DHgroup1", "DHgroup2", "DHgroup5", "DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17" or "DHgroup18" to be used in SA negotiation.	DHgroup2
SA Lifetime	Set the IPsec SA lifetime. When negotiating set up IPsec SAs, IKE uses the smaller one between the lifetime set locally and the lifetime proposed by the peer.	28800
DPD Interval	Set the interval after which DPD is triggered if no IPsec protected packets is received from the peer. DPD is Dead peer detection. DPD irregularly detects dead IKE peers. When the local end sends an IPsec packet, DPD checks the time the last IPsec packet was received from the peer. If the time exceeds the DPD interval, it sends a DPD hello to the peer. If the local end receives no DPD acknowledgment within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgment after having made the maximum number of retransmission attempts, it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.	60
DPD Failures	Set the timeout of DPD (Dead Peer Detection) packets.	180
Advanced Settings		
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the inner headers of IP packets.	OFF
Enable Forced Encapsulation	Click the toggle button to enable / disable this option. After it is enabled, even if no NAT condition is detected, the UDP encapsulation of esp packets is forced. This may help overcome restrictive firewalls.	OFF

SA Settings		
Item	Description	Default
Expert Options	Add more PPP configuration options here, format: config-desc;config-desc, e.g. protostack=netkey;plutodebug=none	Null

## Status

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

General	Tunnel	Status	x509
^ IPsec Tunnel Status			
Index	Description	Status	Uptime

## x509

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

General	Tunnel	Status	x509
^ X509 Settings			
<div> <div>Tunnel Name</div> <div>Tunnel 1 v</div> </div> <div> <div>Local Certificate</div> <div>Choose File No file chosen</div> <div>⬆</div> </div> <div> <div>Remote Certificate</div> <div>Choose File No file chosen</div> <div>⬆</div> </div> <div> <div>Private Key</div> <div>Choose File No file chosen</div> <div>⬆</div> </div> <div> <div>CA Certificate</div> <div>Choose File No file chosen</div> <div>⬆</div> </div> <div> <div>PKCS#12 Certificate</div> <div>Choose File No file chosen</div> <div>⬆</div> </div>			
^ Certificate Files			
Index	File Name	File Size	Modification Time

x509		
Item	Description	Default
X509 Settings		
Tunnel Name	Choose a valid tunnel.	Tunnel 1
Certificate Files	Click on "Choose File" to locate the certificate file from your computer, and then import this file into your router. The correct file format is displayed as follows: @ca.crt @remote.crt @local.crt @private.key @crl.pem	--
Peer Certificate	Select the peer certificate to import to the router.	--
Private Key	Select the correct private key file to import into the router.	--
Root Certificate	Select the root certificate file to import into the router.	--

x509		
Item	Description	Default
PKCS # 12 Certificate	Select the PKCS # 12 certificate file to import into the route	--
Certificate Files		
Index	Indicate the ordinal of the list.	--
Filename	Show the imported certificate's name.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null


### 3.15 VPN > OpenVPN

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

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

#### OpenVPN

OpenVPN	Status	x509					
^ Tunnel Settings							
Index	Enable	Description	Mode	Protocol	Server Address	Interface Type	+

Click  to add tunnel settings. The maximum count is 3. The window is displayed as below when choosing "None" as the authentication type. By default, the mode is "P2P".



**OpenVPN**

**^ General Settings**

Index

1

Enable

ON

OFF

Enable IPv6

ON

OFF

Description

Mode

P2P

?

TLS Mode

None

?

Protocol

UDP

Peer Address

Peer Port

1194

Listen IP Address

Listen Port

1194

Interface Type

TUN

Authentication Type

None

?

Local IP

10.8.0.1

Remote IP

10.8.0.2

Encrypt Algorithm

BF

Authentication Algorithm

SHA1

Keepalive Interval

20

?

Keepalive Timeout

120

?

TUN MTU

1500

Max Frame Size

Enable Compression

ON

OFF

Enable NAT

ON

OFF

Verbose Level

0

?

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

**General Settings**

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	
Mode	Client <input type="button" value="v"/> <input type="button" value="?"/>
Protocol	UDP <input type="button" value="v"/>
Peer Address	
Peer Port	1194
Interface Type	TUN <input type="button" value="v"/>
Authentication Type	None <input type="button" value="v"/> <input type="button" value="?"/>
Encrypt Algorithm	BF <input type="button" value="v"/>
Authentication Algorithm	SHA1 <input type="button" value="v"/>
Renegotiation Interval	86400 <input type="button" value="?"/>
Keepalive Interval	20 <input type="button" value="?"/>
Keepalive Timeout	120 <input type="button" value="?"/>
TUN MTU	1500
Max Frame Size	
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable DNS overrid	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF <input type="button" value="?"/>
Verbose Level	0 <input type="button" value="v"/> <input type="button" value="?"/>

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

## ^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable IPv6	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="Server"/> v ?
Protocol	<input type="text" value="UDP"/> v
Listen IP Address	<input type="text"/>
Listen Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> v
Authentication Type	<input type="text" value="None"/> v ?
Enable IP Pool	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Client Subnet	<input type="text" value="10.8.0.0"/>
Client Subnet Netmask	<input type="text" value="255.255.255.0"/>
Encrypt Algorithm	<input type="text" value="BF"/> v
Authentication Algorithm	<input type="text" value="SHA1"/> v
Renegotiation Interval	<input type="text" value="86400"/> ?
Max Clients	<input type="text" value="10"/>
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
TUN MTU	<input type="text" value="1500"/>
Max Frame Size	<input type="text"/>
Private Key Password	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable Default Gateway	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	<input type="text" value="0"/> v ?

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

**General Settings**

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable IPv6	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Description	
Mode	P2P <input type="button" value="v"/> ⓘ
TLS Mode	None <input type="button" value="v"/> ⓘ
Protocol	UDP <input type="button" value="v"/>
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN <input type="button" value="v"/>
Authentication Type	None <input type="button" value="v"/> ⓘ
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF <input type="button" value="v"/>
Authentication Algorithm	SHA1 <input type="button" value="v"/>
Keepalive Interval	20 ⓘ
Keepalive Timeout	120 ⓘ
TUN MTU	1500
Max Frame Size	
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	0 <input type="button" value="v"/> ⓘ

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

**^ General Settings**

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable IPv6	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Description	
Mode	P2P <input type="button" value="v"/> ?
TLS Mode	None <input type="button" value="v"/> ?
Protocol	UDP <input type="button" value="v"/>
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN <input type="button" value="v"/>
Authentication Type	Preshared <input type="button" value="v"/> ?
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF <input type="button" value="v"/>
Authentication Algorithm	SHA1 <input type="button" value="v"/>
Keepalive Interval	20 ?
Keepalive Timeout	120 ?
TUN MTU	1500
Max Frame Size	
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	0 <input type="button" value="v"/> ?

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

**^ General Settings**

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable IPv6	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Description	
Mode	P2P <input type="button" value="v"/> ?
TLS Mode	None <input type="button" value="v"/> ?
Protocol	UDP <input type="button" value="v"/>
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN <input type="button" value="v"/>
Authentication Type	Password <input type="button" value="v"/> ?
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF <input type="button" value="v"/>
Authentication Algorithm	SHA1 <input type="button" value="v"/>
Keepalive Interval	20 ?
Keepalive Timeout	120 ?
TUN MTU	1500
Max Frame Size	
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	0 <input type="button" value="v"/> ?

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

**^ General Settings**

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable IPv6	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Description	
Mode	P2P <input type="button" value="v"/> ?
TLS Mode	None <input type="button" value="v"/> ?
Protocol	UDP <input type="button" value="v"/>
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN <input type="button" value="v"/>
Authentication Type	X509CA <input type="button" value="v"/> ?
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF <input type="button" value="v"/>
Authentication Algorithm	SHA1 <input type="button" value="v"/>
Keepalive Interval	20 ?
Keepalive Timeout	120 ?
TUN MTU	1500
Max Frame Size	
Private Key Password	
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	0 <input type="button" value="v"/> ?

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

**General Settings**

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable IPv6	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Description	
Mode	P2P <input type="button" value="v"/> <input data-bbox="925 492 949 526" type="button" value="?"/>
TLS Mode	None <input type="button" value="v"/> <input data-bbox="925 548 949 582" type="button" value="?"/>
Protocol	UDP <input type="button" value="v"/>
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN <input type="button" value="v"/>
Authentication Type	X509CA Password <input type="button" value="v"/> <input data-bbox="925 907 949 940" type="button" value="?"/>
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF <input type="button" value="v"/>
Authentication Algorithm	SHA1 <input type="button" value="v"/>
Keepalive Interval	20 <input data-bbox="925 1176 949 1209" type="button" value="?"/>
Keepalive Timeout	120 <input data-bbox="925 1232 949 1265" type="button" value="?"/>
TUN MTU	1500
Max Frame Size	
Private Key Password	
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	0 <input type="button" value="v"/> <input data-bbox="925 1545 949 1579" type="button" value="?"/>

**Advanced Settings**

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

**Advanced Settings**

Enable HMAC Firewall	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable PKCS#12	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable nsCertType	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Expert Options	<input type="button" value="v"/> <input data-bbox="925 1937 949 1971" type="button" value="?"/>

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



^ Advanced Settings

Enable HMAC Firewall

ON OFF

Enable Ctrl

ON OFF

Enable Client To Client

ON OFF

Enable Dup Client

ON OFF

Enable IP Persist

ON OFF ?

Expert Options

?

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

OpenVPN
Status
x509

^ Tunnel Settings


Index	Enable	Description	Mode	Protocol	Peer Address	Interface Type	+
-------	--------	-------------	------	----------	--------------	----------------	---

^ Password Manage

Index	Username	+
-------	----------	---

^ Client Manage

Index	Enable	Common Name	Client IP Address	+
-------	--------	-------------	-------------------	---

Click User Password Management  to add username and password, as shown below:

OpenVPN


^ General Settings

Index

1

Username

Password

Click Client Management  to add client information, as shown below:

OpenVPN

^ General Settings

Index

1

Enable

ON OFF

Common Name

?

Client IP Address

General Settings @ OpenVPN		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this OpenVPN tunnel.	ON
Enable Ipv6	Click the toggle button to enable / disable OpenVPN using IPv6.	OFF
Description	Enter a description for this OpenVPN tunnel.	Null

General Settings @ OpenVPN		
Item	Description	Default
Mode	Select from "P2P" or "Client".	Client
TLS Mode	Select from "None", "Client" or "Server".	None
Protocol	Select from "UDP", "TCP-Client" or "TCP-Server".	UDP
Server Address	Enter the end-to-end IP address or the domain of the remote OpenVPN server.	Null
Server Port	Enter the end-to-end listener port or the listening port of the OpenVPN server.	1194
Listening Address	Local server address.	Null
Listening Port	Local server port.	1194
Interface Type	Select from "TUN" or "TAP" which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.	TUN
Authentication Type	Select from "None", "Preshared", "Password", "X509CA" and "X509CA Password". <b>Note:</b> "None" and "Preshared" authentication type are only working with P2P mode.	None
Enable IP Address Pool	Click the toggle button to enable / disable the IP address pool allocation function.	OFF
Starting Address	Defines the beginning of an IP address pool that assigns addresses to OpenVPN clients.	10.8.0.5
End Address	Defines the end of the IP address pool for assigning addresses to OpenVPN clients.	10.8.0.254
Client Network	Enter the client network IP.	10.8.0.0
Client Netmask	Enter the client netmask.	255.255.255.0
Username	Enter the username used for "Password" or "X509CA Password" authentication type.	Null
Password	Enter the password used for "Password" or "X509CA Password" authentication type.	Null
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
Encrypt Algorithm	Select from "BF", "DES", "DES-EDE3", "AES128", "AES192" and "AES256". <ul style="list-style-type: none"> <li>BF: Use 128-bit BF encryption algorithm in CBC mode</li> <li>DES: Use 64-bit DES encryption algorithm in CBC mode</li> <li>DES-EDE3: Use 192-bit 3DES encryption algorithm in CBC mode</li> <li>AES128: Use 128-bit AES encryption algorithm in CBC mode</li> <li>AES192: Use 192-bit AES encryption algorithm in CBC mode</li> <li>AES256: Use 256-bit AES encryption algorithm in CBC mode</li> </ul>	BF
Renegotiation Interval	Set the renegotiation interval. If connection failed, OpenVPN will renegotiate when the renegotiation interval reached.	86400
Maximum Number of Clients	Set the maximum number of clients allowed to access the OpenVPN server.	10

General Settings @ OpenVPN		
Item	Description	Default
Keepalive Interval	Set keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Set the keepalive timeout. Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120
MTU	Set the maximum transmission unit.	1500
Data Fragmentation	Set the maximum frame length.	Null
Private Key Password	Enter the private key password under the "X509CA" and "X509CA Password" authentication type.	Null
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the data stream of the header.	ON
Enable Default Gateway	Standalone switch button to enable / disable the default gateway function. After enabling, push the local tunnel address as the default gateway of the peer device.	OFF
Receive DNS Push	Standalone switch button to enable / disable receiving DNS push function. After enabling, it is allowed to receive DNS information pushed by the peer.	OFF
Enable NAT	Click the toggle button to enable/disable the NAT option. When enabled, the source IP address of host behind router will be disguised before accessing the remote OpenVPN client.	OFF
Verbose Level	Select the level of the output log and values from 0 to 11. <ul style="list-style-type: none"> <li>0: No output except fatal errors</li> <li>1~4: Normal usage range</li> <li>5: Output R and W characters to the console for each packet read and write</li> <li>6~11: Debug info range</li> </ul>	0
Advanced Settings @ OpenVPN		
Enable HMAC Firewall	Click the toggle button to enable/disable this option. Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.	OFF
Enable PKCS#12	Click the toggle button to enable/disable the PKCS#12 certificate. It is an exchange of digital certificate encryption standard, used to describe personal identity information.	OFF
Enable nsCertType	Click the toggle button to enable/disable nsCertType. Require that peer certificate was signed with an explicit nsCertType designation of "server".	OFF
Enable Crl	Click the toggle button to enable / disable the option. When enabled, client certificates can be revoked.	OFF
Enable Client to Client	Click the toggle button to enable / disable the option. When enabled, clients can communicate with each other.	OFF
Enable Dup Client	Click the toggle button to enable / disable the option. After being enabled, the tunnel IPs obtained by multiple clients are different, and the tunnel IP of the client and the tunnel IP of the server are interoperable.	OFF

General Settings @ OpenVPN		
Item	Description	Default
Enable IP Address Hold	Click the toggle button to enable / disable the option. When enabled, the IP in the address pool is obtained automatically.	ON
Expert Options	Enter some other options of OpenVPN in this field. Each expression can be separated by a ';'.	Null
Advanced Settings @ User Password Management		
Username	Custom tunnel connection username.	Null
Password	Custom tunnel connection password.	Null
Client Management		
Enable	Click the toggle button to enable / disable this option. When enabled, the client IP address can be managed.	OFF
Common Name	Set the certificate name.	Null
Client IP Address	Set a fixed client virtual IP.	Null

## Status

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

OpenVPN	Status	x509				
^ OpenVPN Tunnel Status						
Index	Description	Status	Mode	Uptime	Local IP	Local IPv6
^ OpenVPN Client List						
Index	Common Name		Real IP	Port	Virtual IP	Virtual IPv6

## x509

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

OpenVPN	Status	x509
---------	--------	------

^ X509 Settings

Tunnel Name

Tunnel 1

Mode

Client

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

^ Certificate Files

Index	File Name	File Size	Modification Time
-------	-----------	-----------	-------------------

x509		
Item	Description	Default
X509 Settings		
Tunnel Name	Choose a valid tunnel. Select from "Tunnel 1", "Tunnel 2", "Tunnel 3", "Tunnel 4", "Tunnel 5" or "Tunnel 6".	Tunnel 1
Tunnel mode	Select "P2P Mode", "Client Mode" or "Server Mode".	Client mode
Root certificate	Select the root certificate file to import into the router.	--
Certificate Files	Click on "Choose File" to locate the certificate file from your computer, and then import this file into your router.	--
Private Key	Select the private key file to import into the router.	--
TLS-Auth Key	Select the TLS-Auth key file to import into the router.	--
PKCS # 12 Certificate	Select the PKCS # 12 certificate file to import into the router.	--
Certificate Files		
Index	Indicate the ordinal of the list.	--
Filename	Show the imported certificate's name.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

### 3.16 VPN > GRE

This section allows you to set the GRE and the related parameters. Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. There are two main uses of the GRE protocol: enterprise internal protocol encapsulation and private address encapsulation.

#### GRE

GRE	Status			
^ Tunnel Settings				
Index	Enable	Description	Remote IP Address	

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

## GRE

### ^ Tunnel Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Remote IP Address	<input type="text"/>
Local Virtual IP Address	<input type="text"/>
Local Virtual Netmask/Prefix Length	<input type="text"/>
Remote Virtual IP Address	<input type="text"/>
Enable Default Route	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Secrets	<input type="text"/>
Link Binding	<input type="text" value="Unspecified"/> <input type="button" value="v"/> <input data-bbox="906 824 930 848" type="button" value="?"/>

### Tunnel Settings @ GRE

Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this GRE tunnel.	ON
Description	Enter a description for this GRE tunnel.	Null
Remote IP Address	Set the remote real IP address of the GRE tunnel.	Null
Local Virtual IP Address	Set the local virtual IP address of the GRE tunnel.	Null
Local Virtual Netmask/ IPv6 prefix length	Set the local virtual Netmask of the GRE tunnel.	Null
Remote Virtual IP Address	Set the remote virtual IP Address of the GRE tunnel.	Null
Enable Default Route	Click the toggle button to enable/disable this option. When enabled, all the traffics of the router will go through the GRE VPN.	OFF
Enable NAT	Click the toggle button to enable/disable this option. This option must be enabled when router under NAT environment.	OFF
Secrets	Set the key of the GRE tunnel.	Null
Link Binding	Select from "WWAN1", "WWAN2", "WAN", or "WLAN".	Not bound

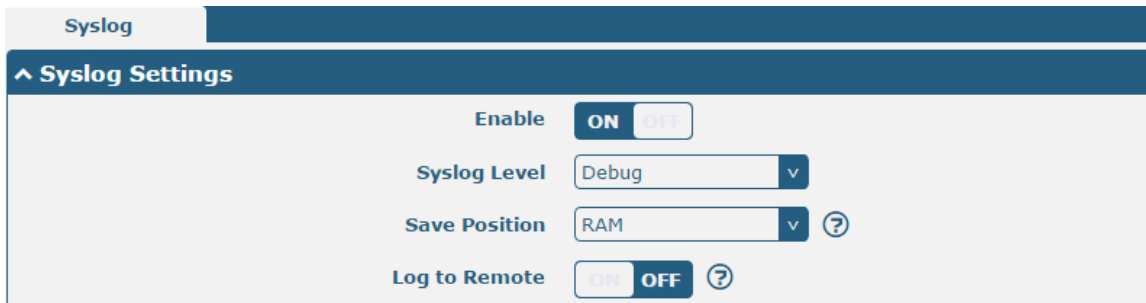
## Status

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

GRE	Status				
^ GRE tunnel status					
Index	Description	Status	Local IP Address	Remote IP Address	Uptime

### 3.17 Services > Syslog

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



The screenshot shows the 'Syslog Settings' window. The 'Enable' toggle is set to 'ON'. 'Syslog Level' is set to 'Debug'. 'Save Position' is set to 'RAM'. 'Log to Remote' is set to 'OFF'. There is a help icon (?) next to the 'Log to Remote' toggle.

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



The screenshot shows the 'Syslog Settings' window with 'Log to Remote' enabled. The 'Enable' toggle is 'ON'. 'Syslog Level' is 'Debug'. 'Save Position' is 'RAM'. 'Log to Remote' is 'ON'. 'Add Identifier' is 'OFF'. 'Remote IP Address' is an empty text field. 'Remote Port' is set to '514'. Help icons (?) are present next to 'Log to Remote' and 'Add Identifier'.

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

### 3.18 Services > Event

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

Event

Notification

Query

^ General Settings

Signal Quality Threshold
?

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


Event

Notification

Query

^ Event Notification Group Settings

Index
Description
Send SMS
Send Email
DO Control
Save to NVM
+

Click  button to add an Event parameters.

Notification

^ General Settings

Index

Description

Send SMS

ON OFF

Send Email

ON OFF

DO Control

ON OFF

Save to NVM

ON OFF

?



^ Event Selection
?

System Startup

ON OFF

System Reboot

ON OFF

System Time Update

ON OFF

Configuration Change

ON OFF

Cellular Network Type Change

ON OFF

Cellular Data Stats Clear

ON OFF

Cellular Data Traffic Overflow

ON OFF

Poor Signal Quality

ON OFF

Link Switching

ON OFF

WAN Up

ON OFF

WAN Down

ON OFF

WLAN Up

ON OFF

WLAN Down

ON OFF

WWAN Up

ON OFF

WWAN Down

ON OFF

IPSec Connection Up

ON OFF

IPSec Connection Down

ON OFF

OpenVPN Connection Up

ON OFF

OpenVPN Connection Down

ON OFF

LAN Port Link Up

ON OFF

LAN Port Link Down

ON OFF

DDNS Update Success

ON OFF

DDNS Update Fail

ON OFF

Received SMS

ON OFF

SMS Command Execute

ON 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 router will send notification to the specified phone numbers via SMS if event occurs. Set the related phone number in "3.21 Services > Email", and use ';' to separate each number.	OFF
Send Email	Click the toggle button to enable/disable this option. When enabled, the router will send notification to the specified email box via Email if event occurs. Set the related email address in "3.21 Services > Email".	OFF

DO Control	Click the toggle button to enable / disable this option. After it is turned on, the event router will send it to the corresponding DO in the form of Low / High level.	OFF
Save to NVM	Click the toggle button to enable/disable this option. Enable to save event to nonvolatile memory.	OFF

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

Event

Notification

Query

Event Details

Save Position

RAM

Filtering

```

Sep 11 19:00:53, system startup
Sep 11 19:00:55, LAN port link down, eth0
Sep 11 19:00:55, LAN port link up, eth1
Sep 11 19:01:06, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 19:01:16, system time update
Sep 11 19:47:25, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:25, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:25, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:26, configuration change, via web manager
Sep 11 19:47:41, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:42, configuration change, via web manager
Sep 11 19:47:42, WWAN (cellular) down, WWAN1
Sep 11 19:47:44, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 19:48:50, configuration change, via web manager
Sep 11 19:48:51, WWAN (cellular) down, WWAN1
Sep 11 19:48:52, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 19:49:04, configuration change, via web manager
Sep 11 19:49:05, WWAN (cellular) down, WWAN1
Sep 11 19:49:10, WLAN up
Sep 11 19:59:33, configuration change, link_manager restored to default after firmware updating
Sep 11 19:59:34, configuration change, via web manager
Sep 11 19:59:36, WLAN down
Sep 11 19:59:38, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 20:29:00, LAN port link down, eth1
Sep 11 20:34:06, LAN port link up, eth1

```

Clear

Refresh

Event Details		
Item	Description	Default
Save Position	Select the events' save position from "RAM" or "NVM". <ul style="list-style-type: none"> <li>RAM: Random-access memory</li> <li>NVM: Non-Volatile Memory</li> </ul>	RAM
Filter Message	Enter the filtering message based on the keywords set by users. Click the "Refresh" button, the filtered event will be displayed in the follow box. Use "&" to separate more than one filter message, such as message1&message2.	Null

### 3.19 Services > NTP

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

NTP

Status

^ Timezone Settings

Time Zone

UTC+08:00

Expert Setting

^ NTP Client Settings

Enable

ON

OFF

Primary NTP Server

pool.ntp.org

Secondary NTP Server

NTP Update Interval

0

^ NTP Server Settings

Enable

ON

OFF

NTP		
Item	Description	Default
<b>Timezone Settings</b>		
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
<b>NTP Client Settings</b>		
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
<b>NTP Server Settings</b>		
Enable	Click the toggle button to enable/disable the NTP server option.	OFF

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

NTP

Status

^ Time

System Time

2019-12-31 10:48:42

PC Time

2019-12-31 10:48:44

Sync

Last Update Time

2019-12-31 09:52:08

## 3.20 Services > SMS

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

SMS

SMS Testing

^ SMS Management Settings

Enable

ON OFF

Authentication Type

Password

v

?

Phone Number

?

SMS Management Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable the SMS Management option. <b>Note:</b> If this option is disabled, the SMS configuration is invalid.	ON
Authentication Type	Select Authentication Type from "Password", "Phonenum" or "Both". <ul style="list-style-type: none"> <li>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; ..."</li> <li><b>Note:</b> Set the WEB manager password in <b>System &gt; User Management</b> section.</li> <li>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; ..."</li> <li>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; ..."</li> </ul>	Password
Phone Number	Set the phone number used for SMS management, and use ';' to separate each number. <b>Note:</b> 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

SMS Testing

^ SMS Testing

Phone Number

Message

Result

Send

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

## 3.21 Services > Email

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

Email

^ Email Settings

Enable

ON OFF

Enable TLS/SSL

ON OFF ?

Enable STARTTLS

ON OFF

Outgoing Server

Server Port

Timeout

?

Auth Login

ON OFF ?

Username

Password

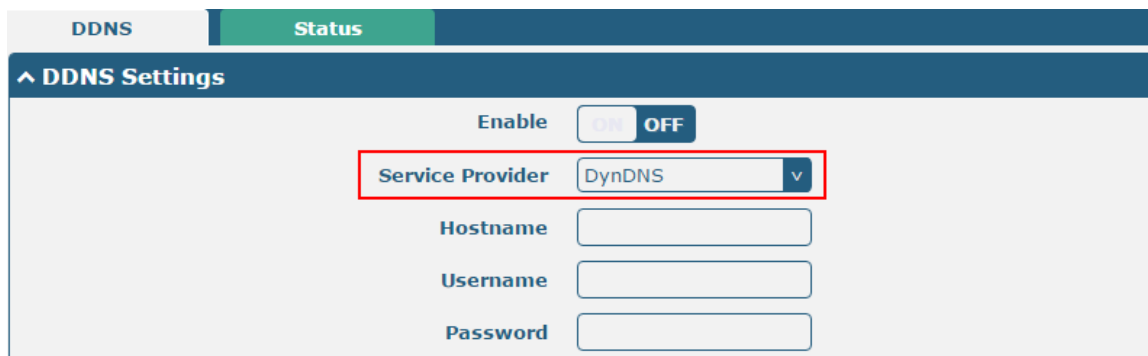
From

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
Enable STARTTLS	Click the toggle button to enable / disable STARTTLS encryption.	OFF
Outgoing server	Enter the SMTP server IP Address or domain name.	Null
Server port	Enter the SMTP server port.	25
Timeout	Set the max time for sending email to SMTP server. When the server doesn't receive the email over this time, it will try to resend.	10
Auth Login	If the mail server supports AUTH login, you must enable this button and set a username and password.	OFF
Username	Enter the username which has been registered from SMTP server.	Null
Password	Enter the password of the username above.	Null
From	Enter the source address of the email.	Null
Subject	Enter the subject of this email.	Null

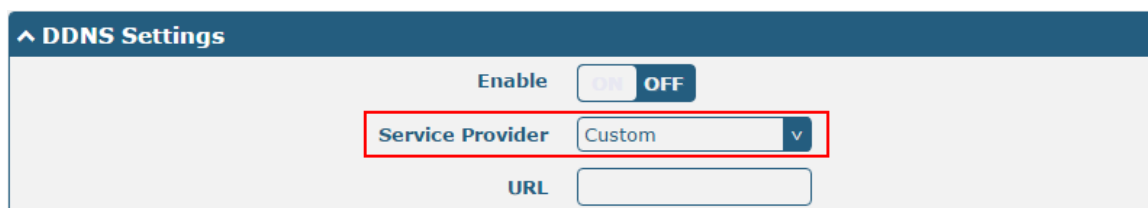
## 3.22 Services > DDNS

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



The screenshot shows the 'DDNS' tab selected in the top navigation bar. Below it, the 'Status' tab is active. The 'DDNS Settings' section is expanded, showing an 'Enable' toggle set to 'OFF'. A red box highlights the 'Service Provider' dropdown menu, which is currently set to 'DynDNS'. Below this, there are input fields for 'Hostname', 'Username', and 'Password', all of which are currently empty.

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



The screenshot shows the 'DDNS Settings' section with the 'Service Provider' dropdown menu set to 'Custom', highlighted by a red box. Below this, there is an input field for 'URL', which is currently empty. The 'Enable' toggle remains set to 'OFF'.

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”. <b>Note:</b> The DDNS service only can be used after registered by Corresponding service provider.	DynDNS
Hostname	Enter the hostname provided by the DDNS server.	Null
Username	Enter the username provided by the DDNS server.	Null
Password	Enter the password provided by the DDNS server.	Null
URL	Enter the URL customized by user.	Null

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

DDNS
Status

^ DDNS Status

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.

## 3.23 Services > SSH

Router supports SSH password access and secret-key access.

SSH
Keys Management

^ SSH Settings

Enable ☒ ON ☐ OFF

Port

Disable Password Logins ☐ ON ☒ OFF

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

	case, only the key can be used for login.	
--	---	--

SSH
Keys Management

^ Import Authorized Keys

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 router. <b>Note:</b> This option is valid when enabling the password logins option.

## 3.24 Services > Web Server

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

Web Server
Certificate Management

^ General Settings

HTTP Port

?

HTTPS Port

?

General Settings @ Web Server		
Item	Description	Default
HTTP Port	Enter the HTTP port number you want to change in router's Web Server. On a Web server, port 80 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTP Port number except 80, only adding that port number then you can login router's Web Server.	80
HTTPS Port	Enter the HTTPS port number you want to change in router's Web Server. On a Web server, port 443 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTPS Port number except 443, only adding that port number then you can login router's Web Server.  <b>Note:</b> HTTPS is more secure than HTTP. In many cases, clients may be exchanging confidential information with a server, which needs to be secured in order to prevent unauthorized access. For this reason, HTTP was developed by Netscape corporation to allow authorization and secured transactions.	443

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



Web Server

Certificate Management

^ Import Certificate

Import Type

CA

HTTPS Certificate

Choose File

No file chosen

Import

Import Certificate		
Item	Description	Default
Import Type	Select from "CA" and "Private Key". <ul style="list-style-type: none"> <li>CA: a digital certificate issued by CA center</li> <li>Private Key: a private key file</li> </ul>	CA
HTTPS Certificate	Click on "Choose File" to locate the certificate file from your computer, and then click "Import" to import this file into your router.	--

## 3.25 Services > Advanced

This section allows you to set the Advanced and parameters.

System

Reboot

^ System Settings

Device Name

router

?

User LED Type

None

?

System

Reboot

^ System Settings

Device Name

router

?

User LED Type

None

None

SIM

NET

OpenVPN

IPSec

WiFi

?

System Settings		
Item	Description	Default
Device Name	Set the device name to distinguish different devices you have installed; valid characters are a-z, A-Z, 0-9, @, ., -, #, \$, and *.	router
User LED Type	Specify the display type of your USR LED. Select from "None", "SIM", "NET", "OpenVPN", "IPSec" or "WiFi". <ul style="list-style-type: none"> <li>None: Meaningless indication, and the LED is off</li> <li>SIM: USR indicator showing the SIM status</li> <li>NET: USR indicator showing the NET status</li> <li>OpenVPN: USR indicator showing the OpenVPN status</li> <li>IPSec: USR indicator showing the IPsec status</li> </ul>	None

- WiFi: USR indicator showing the WiFi status
- Note:** For more details about USR indicator, see “2.2 LED Indicators”.

System	Reboot
<b>^ Periodic Reboot Settings</b>	
Periodic Reboot	<input type="text" value="0"/> ?
Daily Reboot Time	<input type="text"/> ?

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

## 3.26 System > Debug

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

Syslog								
<b>^ Syslog Details</b>								
<div> Log Level: <input type="text" value="Debug"/> </div> <div> Filtering: <input type="text"/> </div> <div> <pre> Sep 11 21:00:58 router user.debug rping[4655]: round-trip min/avg/max = 141.447/141.447/141.447 ms Sep 11 21:00:58 router user.debug link_manager[3986]: rcv action ping_success from rping Sep 11 21:00:58 router user.debug link_manager[3986]: target link WWAN1, state Connected Sep 11 21:00:58 router user.info link_manager[3986]: WWAN1 ping test success Sep 11 21:05:58 router user.debug link_manager[3986]: WWAN1 (wwan) start ping test Sep 11 21:05:58 router user.debug rping[4718]: start ping 8.8.8.8 (wwan) Sep 11 21:05:59 router user.debug rping[4718]: PING 8.8.8.8 (8.8.8.8) from 10.18.11.133: 16 data bytes Sep 11 21:05:59 router user.debug rping[4718]: 24 bytes from 8.8.8.8: seq=0 ttl=51 time=139.263 ms Sep 11 21:05:59 router user.debug rping[4718]: Sep 11 21:05:59 router user.debug rping[4718]: --- 8.8.8.8 ping statistics --- Sep 11 21:05:59 router user.debug rping[4718]: 1 packets transmitted, 1 packets received, 0% packet loss Sep 11 21:05:59 router user.debug rping[4718]: round-trip min/avg/max = 139.263/139.263/139.263 ms Sep 11 21:05:59 router user.debug link_manager[3986]: rcv action ping_success from rping Sep 11 21:05:59 router user.debug link_manager[3986]: target link WWAN1, state Connected Sep 11 21:05:59 router user.info link_manager[3986]: WWAN1 ping test success </pre> </div> <div> Manual Refresh Clear Refresh </div>								
<b>^ Syslog Files</b>								
<table border="1"> <thead> <tr> <th>Index</th> <th>File Name</th> <th>File Size</th> <th>Modification Time</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>messages</td> <td>77945</td> <td>Wed Sep 11 21:05:59 2019</td> </tr> </tbody> </table>	Index	File Name	File Size	Modification Time	1	messages	77945	Wed Sep 11 21:05:59 2019
Index	File Name	File Size	Modification Time					
1	messages	77945	Wed Sep 11 21:05:59 2019					
<b>^ System Diagnostic Data</b>								
System Diagnostic Data <b>Generate</b>								

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

### 3.27 System > Update

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

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

Update

^ System Update

File

Choose File

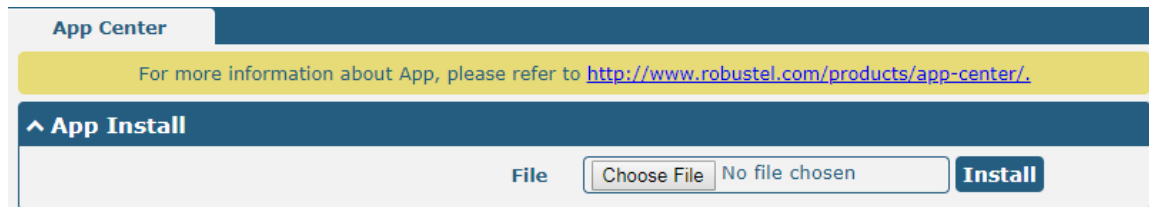
No file chosen

Update

## 3.28 System > App Center

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

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




App Center

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


^ App Install

File  No file chosen

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

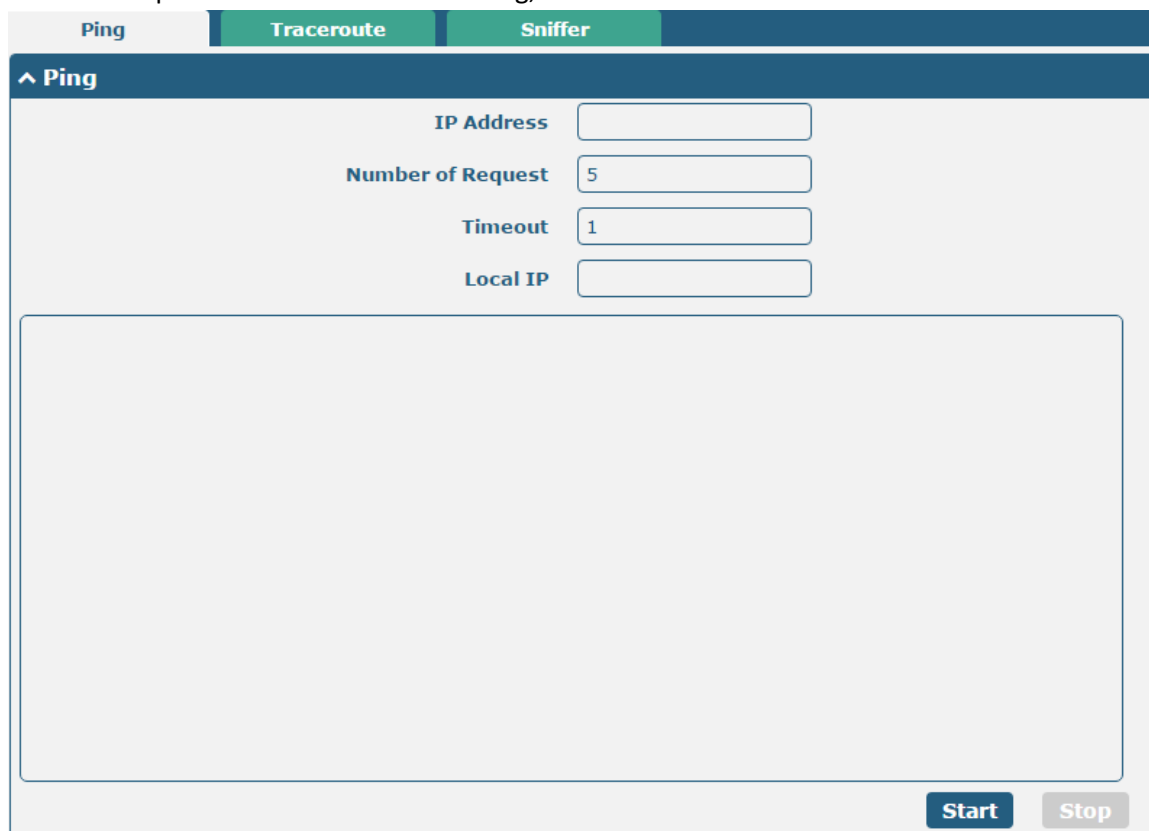


^ Installed Apps				
Index	Name	Version	Status	Description
1	language_chinese	3.1.0	Stopped	Chinese language 

App Center		
Item	Description	Default
App Install		
File	Click on “Choose File” to locate the App file from your computer, and then click  to import this file into your router. <b>Note:</b> File format should be xxx.rpk, e.g. R2000-robustlink-1.0.0.rpk.	--
Installed Apps		
Index	Indicate the ordinal of the list.	--
Name	Show the name of the App.	Null
Version	Show the version of the App.	Null
Status	Show the status of the App.	Null
Description	Show the description for this App.	Null

## 3.29 System > Tools



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



The screenshot shows the 'Ping' tool interface. It features a header with three tabs: 'Ping', 'Traceroute', and 'Sniffer'. The 'Ping' tab is selected. Below the tabs, there is a form with the following fields:

- IP Address**: A text input field.
- Number of Request**: A text input field with the value '5'.
- Timeout**: A text input field with the value '1'.
- Local IP**: A text input field.

Below the form is a large, empty rectangular box intended for displaying the ping results log. At the bottom right of the interface are two buttons: 'Start' (in blue) and 'Stop' (in grey).

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

Ping
Traceroute
Sniffer

### Traceroute

Trace Address

Trace Hops

Trace Timeout

Start Stop

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

Ping
Traceroute
Sniffer


### Sniffer

Interface

Host



Packets Request





Protocol

Status 

Start Stop

### Capture Files

Index	File Name	File Size	Modification Time	
1	19-09-11_21-18-43.cap	52420	Wed Sep 11 21:18:54 2019	 

Sniffer		
Item	Description	Default
Interface	Choose the interface according to your Ethernet configuration.	All
Host	Filter the packet that contain the specify IP address.	Null
Packets Request	Set the packet number that the router can sniffer at a time.	1000
Protocol	Select from "All", "IP", "TCP", "UDP" and "ARP".	All
Status	Show the current status of sniffer.	--
	Click this button to start the sniffer.	--
	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.	--

### 3.30 System > Profile

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

Profile

Rollback

^ Import Configuration File

Reset Other Settings to Default ☐ OFF ?  
Ignore Invalid Settings ☐ OFF ?  
XML Configuration File  No file chosen

^ Export Configuration File

Ignore Disabled Features ☐ OFF ?  
Add Detailed Information ☐ OFF ?  
Encrypt Secret Data ☐ OFF ?  
XML Configuration File   
XML Configuration File

^ Default Configuration

Save Running Configuration as Default  ?  
Restore to Default Configuration

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 <input type="text" value="Choose File"/> to locate the XML configuration file from your computer, and then click <input type="button" value="Import"/> to import this file into your router.	--

Export Configuration File		
Ignore Disabled Features	Click the toggle button as “OFF” to ignore the disabled features.	OFF
Add Detailed Information	Click the toggle button as “On” to add detailed information.	OFF
Encrypt Secret Data	Click the toggle button as “ON” to encrypt the secret data.	OFF
XML Configuration File	Click <b>Generate</b> button to generate the XML configuration file, and click <b>Export</b> to export the XML configuration file.	--
Default Configuration		
Save Running Configuration as Default	Click <b>Save</b> button to save the current running parameters as default configuration.	--
Restore to Default Configuration	Click <b>Restore</b> button to restore the factory defaults.	--

**Profile**
**Rollback**

**Configuration Rollback**

Save as a Rollbackable Archive
**Save**
?

**Configuration Archive Files**

Index	File Name	File Size	Modification Time	
1	config1.tgz	2741	Sun Jan 1 00:00:05 2017	↺
2	config2.tgz	2886	Sun Jan 1 00:00:05 2017	↺
3	config3.tgz	2886	Sun Jan 1 00:00:05 2017	↺
4	config4.tgz	2886	Thu Dec 26 00:00:02 2019	↺

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



### 3.31 System > User Management

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

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

Super User

Common User

^ Super User Settings

New Username

?

Old Password

?

New Password

?

Confirm Password

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

Super User

Common User

^ Common User Settings

Index

Role

Username

+

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

Common User

^ Common Users Settings

Index

Role

v

Username

?

Password

?

Common User Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Role	Select from "Visitor" and "Editor". <ul style="list-style-type: none"> <li>Visitor: Users only can view the configuration of router under this level</li> </ul>	Visitor

	<ul style="list-style-type: none"><li>• Editor: Users can view and set the configuration of router under this level</li></ul>	
Username	Set the Username; valid characters are a-z, A-Z, 0-9, @, ., -, #, \$, and *.	Null
Password	Set the password which at least contains 5 characters; valid characters are a-z, A-Z, 0-9, @, ., -, #, \$, and *.	Null

## Chapter 4 Configuration Examples

### 4.1 Cellular

#### 4.1.1 Cellular Dial-Up

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

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

Link Manager

Status

^ General Settings

Primary Link

WWAN1

?

Backup Link

WWAN2

Backup Mode

Cold Backup

?

Revert Interval

0

?





Emergency Reboot


ON

OFF

?

^ Link Settings

Index	Type	Description	IPv4 Connection Type	IPv6 Connection Type	
1	WWAN1	admin	DHCP	SLAAC	
2	WWAN2		DHCP	SLAAC	
3	WAN		DHCP	SLAAC	
4	WLAN		DHCP	SLAAC	

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

Link Manager

^ General Settings

Index

1

Type

WWAN1

Description

admin

IPv6 Enable

ON

OFF

### ^ WWAN Settings

Automatic APN Selection	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Dialup Number	<input type="text" value="*99***1#"/>
Authentication Type	<input type="text" value="Auto"/> v
PPP Preferred	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
Switch SIM By Data Allowance	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
Data Allowance	<input type="text" value="0"/> ?
Billing Day	<input type="text" value="1"/> ?

### ^ IPv6 LAN Settings

Connection Type	<input type="text" value="Static"/> v
IPv6 Prefix	<input type="text" value="2521:da8:202:10::/64"/>
IPv6 NAT Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF

### ^ Ping Detection Settings ?



Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
IPv4 Primary Server	<input type="text" value="8.8.8.8"/>
IPv4 Secondary Server	<input type="text" value="114.114.114.114"/>
IPv6 Primary Server	<input type="text" value="2001:4860:4860::8888"/>
IPv6 Secondary Server	<input type="text" value="2400:da00:2::29"/>
Interval	<input type="text" value="300"/> ?
Retry Interval	<input type="text" value="5"/> ?
Timeout	<input type="text" value="3"/> ?
Max Ping Tries	<input type="text" value="3"/> ?

### ^ Advanced Settings

IPv4 NAT Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Upload Bandwidth	<input type="text" value="10000"/> ?
Download Bandwidth	<input type="text" value="10000"/>
Overridden Primary DNS	<input type="text"/>
Overridden Secondary DNS	<input type="text"/>
Overridden IPv6 Primary DNS	<input type="text"/>
Overridden IPv6 Secondary DNS	<input type="text"/>
Debug Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Verbose Debug Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

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

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

Cellular	Status	AT Debug			
^ Advanced Cellular Settings					
Index	SIM Card	Phone Number	Network Type	Band Select Type	
1	SIM1		Auto	All	
2	SIM2		Auto	All	

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

^ General Settings

Index: 
SIM Card:  v
Phone Number: 
PIN Code:  ?
Extra AT Cmd:  ?
Telnet Port:  ?

^ Cellular Network Settings

Network Type:  v ?
Band Select Type:  v ?

^ Advanced Settings

Debug Enable: ☐ ON ☐ OFF
Verbose Debug Enable: ☐ ON ☐ OFF

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

## 4.1.2 SMS Remote Control

R2000 supports remote control via SMS. You can use following commands to get the status of the router, and set all the parameters of the router. There are three authentication types for SMS control. You can select from “Password”, “Phonenum” or “Both”.

**An SMS command has the following structure:**

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

**SMS command Explanation:**

1. User name and Password: Use the same username and password as WEB manager for authentication.

2. **cmd1, cmd2, cmd3 to Cmdn**, the command format is the same as the CLI command, more details about CLI cmd please refer to **Chapter 5 Introductions for CLI**.

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

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



The screenshot shows the 'Export Configuration File' section of the Robustel R2000 web interface. It includes three sections: 'Import Configuration File', 'Export Configuration File', and 'Default Configuration'. In the 'Export Configuration File' section, there are three toggle switches for 'Ignore Disabled Features', 'Add Detailed Information', and 'Encrypt Secret Data', all currently set to 'OFF'. Below these are two buttons: 'Generate' and 'Export'. The 'Default Configuration' section has a 'Save' button and a 'Restore' button.

**XML command:**

```
<lan >
<network max_entry_num="2" >
<id > 1</id >
<interface > lan0</interface >
<ip > 172.16.10.67</ip >
<netmask > 255.255.0.0</netmask >
<mtu > 1500</mtu >
```

**SMS cmd:**

```
set lan network 1 interface lan0
set lan network 1 ip 172.16.10.67
set lan network 1 netmask 255.255.0.0
set lan network 1 mtu 1500
```

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

**admin:admin;status system**

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

**SMS received:**

```
hardware_version = 1.0
```

```
firmware_version = "3.0.0"  
kernel_version = 3.10.49  
device_model = R2000  
serial_number = 111111111  
system_uptime = "0 days, 06:17:32"  
system_time = "Thu Jul 6 17:28:51 2017"
```

**admin:admin;reboot**

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

**SMS received:**

OK

**admin:admin;set firewall remote\_ssh\_access false;set firewall remote\_telnet\_access false**

In this command, username is "admin", password is "admin", and the command is to disable the remote\_ssh and remote\_telnet access.

**SMS received:**

OK

OK

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

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

**SMS received:**

OK

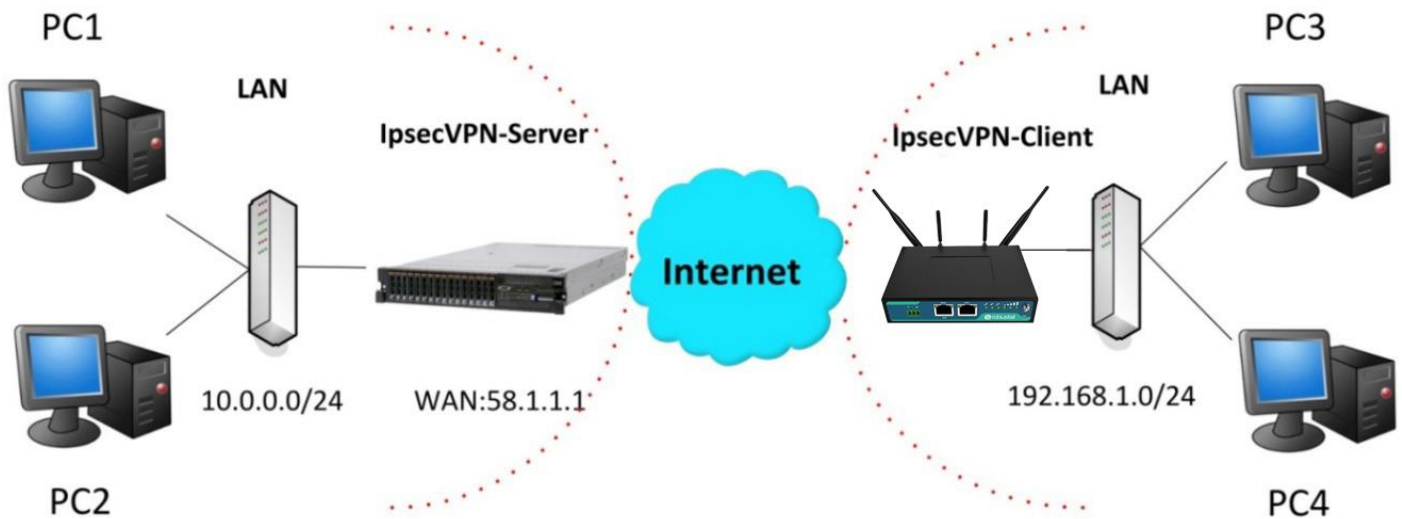
OK

OK

OK

## 4.2 Network

### 4.2.1 IPsec VPN



The configuration of server and client is as follows.

#### IPsec VPN\_Server:

##### Cisco 2811:



```

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

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

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

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

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

```

## IPsec VPN\_Client:

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

General		Tunnel	Status	x509		
^ Tunnel Settings						
Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+

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

**Tunnel**

**General Settings**

Index   
Enable ☒ ON ☐ OFF  
Description   
Gateway  ?  
Mode  v  
Protocol  v  
Local Subnet  ?  
Remote Subnet  ?  
Link Binding  v ?

**IKE Settings**

IKE Type  v  
Negotiation Mode  v  
Encryption Algorithm  v  
Authentication Algorithm  v  
IKE DH Group  v  
Authentication Type  v  
PSK Secret   
Local ID Type  v  
Remote ID Type  v  
IKE Lifetime  ?

**SA Settings**

Encryption Algorithm  v  
Authentication Algorithm  v  
PFS Group  v  
SA Lifetime  ?  
DPD Interval  ?  
DPD Failures  ?

### Advanced Settings

Enable Compression
☐ ON ☒ OFF

Enable Forceencaps
☐ ON ☒ OFF ?

Expert Options
 ?

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

The comparison between server and client is as below.

### Server (Cisco 2811)

```

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

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

Router(config)#crypto ipsec ?
security-association Security association parameters
transform-set Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
ah-md5-hmac AH-MD5-HMAC transform
ah-sha-hmac AH-SHA-HMAC transform
esp-3des ESP transform using 3DES(EDE) cipher (168 bits)
esp-aes ESP transform using AES cipher (128 bits)
esp-des ESP transform using DES cipher (64 bits)
esp-md5-hmac ESP transform using HMAC-MD5 auth
esp-md5-hmac ESP transform using HMAC-MD5 auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac

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

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

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

```

### General Settings

Index: 1

Enable: ☒ ON

Description:

Gateway: 58.1.1.1 ?

Mode: Tunnel v

Protocol: ESP v

Local Subnet: 192.168.1.0/24 ?

Remote Subnet: 0.0.0.0/24 ?

Link Binding: Unspecified v ?

### IKE Settings

IKE Type: IKEv1 v

Negotiation Mode: Main v

Encryption Algorithm: 3DES v

Authentication Algorithm: MD5 v

IKE DH Group: DHgroup2 v

Authentication Type: PSK v

PSK Secret: \*\*\*\*\*

Local ID Type: Default v

Remote ID Type: Default v

IKE Lifetime: 86400 ?

### SA Settings

Encryption Algorithm: 3DES v

Authentication Algorithm: MD5 v

PFS Group: DHgroup2 v

SA Lifetime: 28800 ?

DPD Interval: 30 ?

DPD Failures: 150 ?

### Advanced Settings

Enable Compression: ☐ ON ☒ OFF

Enable Forceencaps: ☐ ON ☒ OFF ?

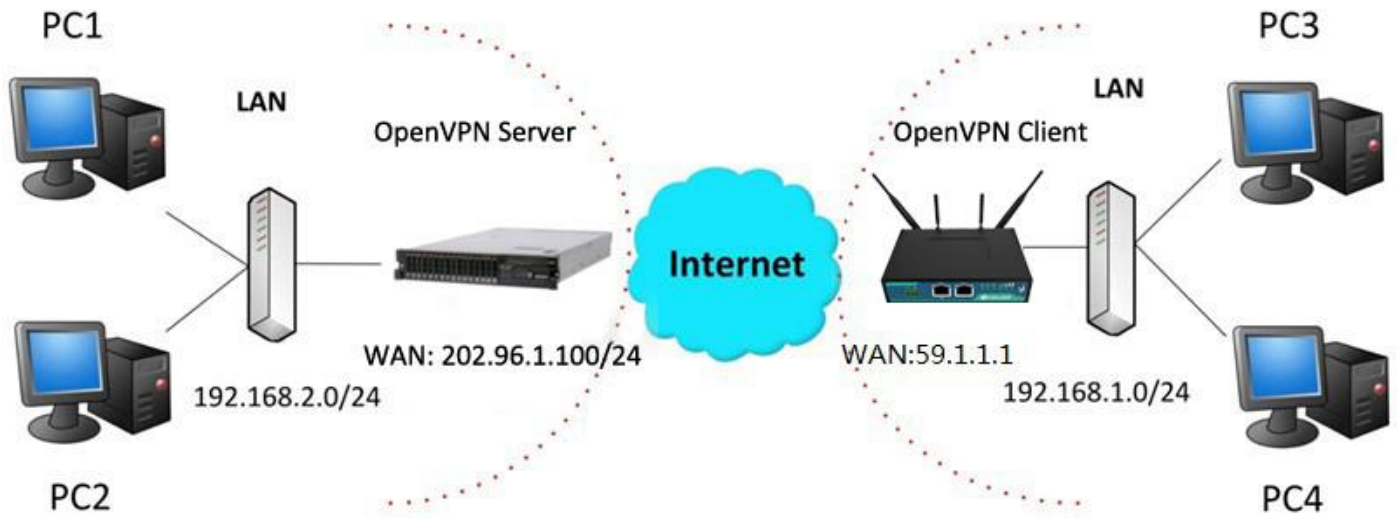
Expert Options:  ?

Router IKE Settings should be consistent with service fees.

Router SA Settings should be consistent with service fees.

## 4.2.2 OpenVPN

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



### OpenVPN\_Server:

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

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

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

## OpenVPN\_Client:

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

OpenVPN	Status	x509					
^ Tunnel Settings							
Index	Enable	Description	Mode	Protocol	Peer Address	Interface Type	+

OpenVPN	Status	x509					
^ Tunnel Settings							
Index	Enable	Description	Mode	Protocol	Server Address	Interface Type	+

Click **+** to configure the Client01 as below.

OpenVPN	
^ General Settings	
Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	client01
Mode	Client <input type="button" value="v"/> <input data-bbox="925 1008 949 1041" type="button" value="?"/>
Protocol	UDP <input type="button" value="v"/>
Peer Address	202.96.1.100
Peer Port	1194
Interface Type	TUN <input type="button" value="v"/>
Authentication Type	X509CA <input type="button" value="v"/> <input data-bbox="925 1265 949 1299" type="button" value="?"/>
Encrypt Algorithm	BF <input type="button" value="v"/>
Authentication Algorithm	SHA1 <input type="button" value="v"/>
Renegotiation Interval	86400 <input data-bbox="925 1422 949 1456" type="button" value="?"/>
Keepalive Interval	20 <input data-bbox="925 1467 949 1500" type="button" value="?"/>
Keepalive Timeout	120 <input data-bbox="925 1523 949 1556" type="button" value="?"/>
TUN MTU	1500
Max Frame Size	1400
Private Key Password	•••••
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable DNS overrid	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF <input data-bbox="805 1836 829 1870" type="button" value="?"/>
Verbose Level	3 <input type="button" value="v"/> <input data-bbox="925 1892 949 1926" type="button" value="?"/>

^ Advanced Settings

Enable HMAC Firewall

ON OFF

Enable PKCS#12

ON OFF

Enable nsCertType

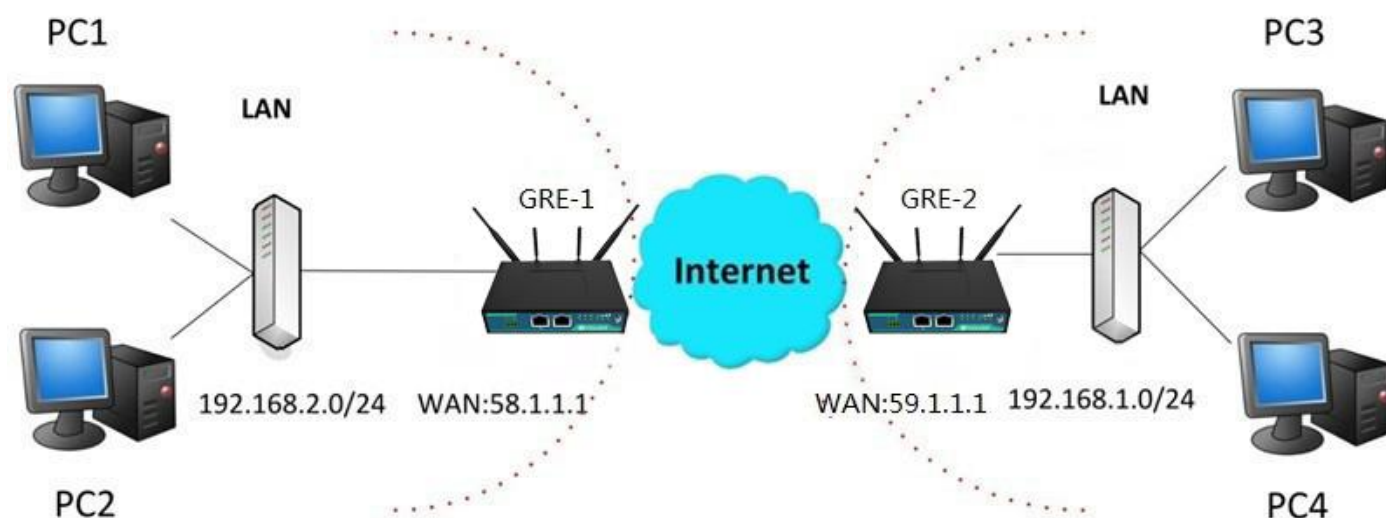
ON OFF

Expert Options

?

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

## 4.2.3 GRE VPN




The configuration of two points is as follows.

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

GRE	Status			
^ Tunnel Settings				
Index	Enable	Description	Remote IP Address	

### GRE-1:

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

**^ Tunnel Settings**

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	
Remote IP Address	59.1.1.1
Local Virtual IP Address	10.8.0.1
Local Virtual Netmask/Prefix Length	255.255.255.0 ?
Remote Virtual IP Address	10.8.0.2
Enable Default Route	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Secrets	.....
Link Binding	Unspecified v ?

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

## GRE-2:

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

**GRE**

**^ Tunnel Settings**

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	GRE-2
Remote IP Address	58.1.1.1
Local Virtual IP Address	10.8.0.2
Local Virtual Netmask/Prefix Length	255.255.255.0 ?
Remote Virtual IP Address	10.8.0.1
Enable Default Route	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Secrets	.....
Link Binding	Unspecified v ?

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

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

GRE		GRE	
^ Tunnel Settings		^ Tunnel Settings	
Index	1	Index	1
Enable	<input checked="" type="checkbox"/> ON	Enable	<input checked="" type="checkbox"/> ON
Description	GRE-1	Description	GRE-2
Remote IP Address	58.1.1.1	Remote IP Address	59.1.1.1
Local Virtual IP Address	10.8.0.1	Local Virtual IP Address	10.8.0.2
Local Virtual Netmask/Prefix Length	255.255.255.0	Local Virtual Netmask/Prefix Length	255.255.255.0
Remote Virtual IP Address	10.8.0.2	Remote Virtual IP Address	10.8.0.1
Enable Default Route	<input type="checkbox"/> OFF	Enable Default Route	<input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> OFF	Enable NAT	<input type="checkbox"/> OFF
Secrets	*****	Secrets	*****
Link Binding	Unspecified	Link Binding	Unspecified

GRE-1 real public network IP address

GRE-1 real tunnl IP address

GRE-2 real tunnl IP address

GRE-2 real public network IP address

GRE-2 real tunnl IP address

GRE-1 real tunnl IP address

USE the same password for GRE-1 and GRE-2

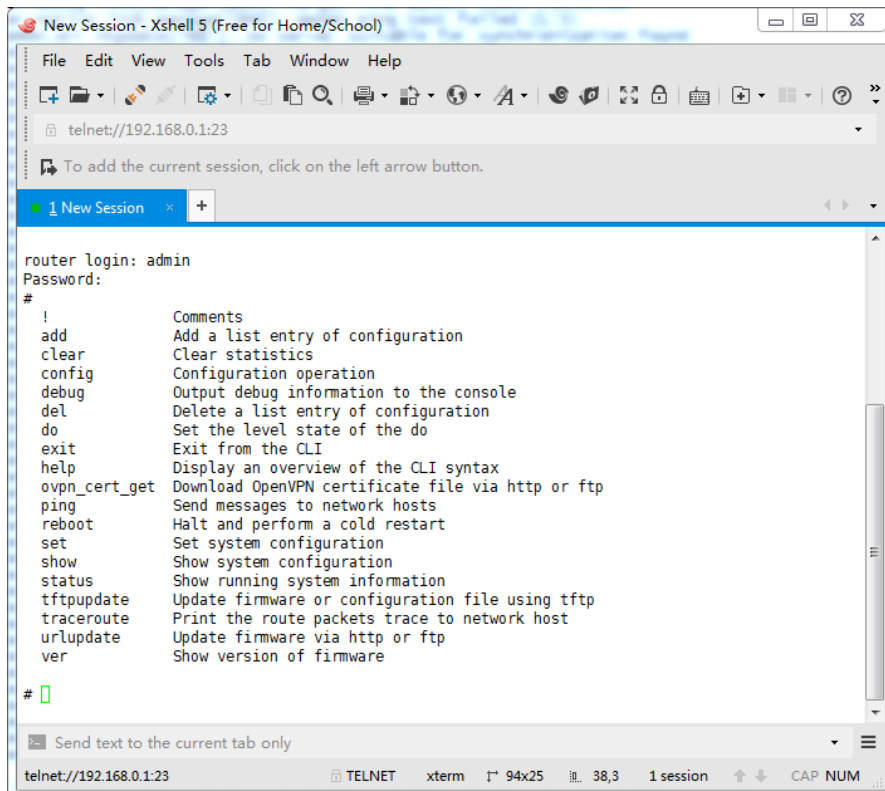
USE the same password for GRE-1 and GRE-2



## Chapter 5 Introductions for CLI

### 5.1 What Is CLI

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



#### Route login:

Router login: admin

Password: admin

#

#### CLI commands:

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

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

help	Display an overview of the CLI syntax
ovpn_cert_get	Download OpenVPN certificate file via http or ftp
ping	Send messages to network hosts
reboot	Halt and perform a cold restart
route	Static route modify dynamically, this setting will not be saved
set	Set system configuration
show	Show system configuration
status	Show running system information
tftpupdate	Update firmware using tftp
traceroute	Print the route packets trace to network host
urlupdate	Update firmware using http or ftp
ver	Show version of firmware

## 5.2 How to Configure the CLI

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

Commands /tips	Description
?	<p>Typing a question mark “?” will show you the help information. eg.</p> <p># config ( Press ‘?’ ) config Configuration operation</p> <p># config ( Press spacebar + ‘?’ ) commit Save the configuration changes and take effect changed configuration save_and_apply Save the configuration changes and take effect changed configuration loaddefault Restore Factory Configuration</p>
Ctrl+c	Press these two keys at the same time, except its “copy” function but also can be used for “break” out of the setting program.
Syntax error: The command is not completed	Command is not completed.
Tick space key+ Tab key	<p>It can help you finish you command. Example:</p> <p># config (tick enter key) Syntax error: The command is not completed # config (tick space key+ Tab key) commit save_and_apply loaddefault</p>
#config commit	When your setting finished, you should enter those commands to make

# config save_and_apply	your setting take effect on the device. <b>Note:</b> Commit and save_and_apply plays the same role.
-------------------------	--

## 5.3 Commands Reference

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

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

## 5.4 Quick Start with Configuration Examples

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

### Example 1: Show current version

```
# status system
hardware_version = 1.0
firmware_version = "3.0.0"
kernel_version = 3.10.49
device_model = R2000
serial_number = 111111111
system_uptime = "0 days, 06:17:32"
system_time = "Thu Jul 6 17:28:51 2017"
```

### Example 2: Update firmware via tftp

```
# tftpupdate (space+?)
firmware New firmware
# tftpupdate firmware (space+?)
String Firmware name
# tftpupdate firmware filename R2000-firmware-sysupgrade-unknown.bin host 192.168.100.99 //enter a new
firmware name
Downloading
R2000-firmware-s 100% | ***** | 5018k 0:00:00 ETA
```

```

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

```

### Example 3: Set link-manager

```

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

```

```

OK                                     //setting succeed
# set link_manager link 1
    type                Type
    desc                Description
    connection_type     Connection Type
    wwan                WWAN Settings
    static_addr         Static Address Settings
    pppoe               PPPoE Settings
    ping               Ping Settings
    mtu                 MTU
    dns1_overridden     Overridden Primary DNS
    dns2_overridden     Overridden Secondary DNS
# set link_manager link 1 type wwan1
OK
# set link_manager link 1 wwan
    auto_apn            Automatic APN Selection
    apn                 APN
    username            Username
    password            Password
    dialup_number       Dialup Number
    auth_type           Authentication Type
    aggressive_reset     Aggressive Reset
    switch_by_data_allowance Switch SIM By Data Allowance
    data_allowance      Data Allowance
    billing_day          Billing Day
# set link_manager link 1 wwan switch_by_data_allowance true
OK
#
# set link_manager link 1 wwan data_allowance 100           //open cellular switch_by_data_traffic
OK                                                         //setting succeed
# set link_manager link 1 wwan billing_day 1                //setting specifies the day of month for billing
OK                                                         // setting succeed
...
# config save_and_apply
OK                                                         // save and apply current configuration, make you configuration effect

```

### Example 4: Set Ethernet

```

# set Ethernet port_setting 2 port_assignmEnt lan0         //Set Table 2 (eth1) to lan0
OK
# config save_and_apply                                     //setting succeed
OK

```

## Example 5: Set LAN IP address

```
# show lan all
network {
    id = 1
    interface = lan0
    ip = 192.168.0.1
    netmask = 255.255.255.0
    mtu = 1500
    dhcp {
        enable = true
        mode = server
        relay_server = ""
        pool_start = 192.168.0.2
        pool_end = 192.168.0.100
        netmask = 255.255.255.0
        gateway = ""
        primary_dns = ""
        secondary_dns = ""
        wins_server = ""
        lease_time = 120
        expert_options = ""
        debug_enable = false
    }
}

multi_ip {
    id = 1
    interface = lan0
    ip = 172.16.10.67
    netmask = 255.255.0.0
}

#
# set lan
network      Network Settings
multi_ip     Multiple IP Address Settings
vlan         VLAN
# set lan network 1(space+?)
interface    Interface
ip           IP Address
netmask      Netmask
mtu          MTU
dhcp         DHCP Settings
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.10.67      //set IP address for lan
OK                                       //setting succeed
```

```
# set lan network 1 netmask 255.255.0.0
```

```
OK
```

```
#
```

```
...
```

```
# config save_and_apply
```

```
OK // save and apply current configuration, make you configuration effect
```

## Example 6: CLI for setting Cellular

```
# show cellular all
```

```
sim {
```

```
    id = 1
```

```
    card = sim1
```

```
    phone_number = ""
```

```
    extra_at_cmd = ""
```

```
    network_type = auto
```

```
    band_select_type = all
```

```
    band_gsm_850 = false
```

```
    band_gsm_900 = false
```

```
    band_gsm_1800 = false
```

```
    band_gsm_1900 = false
```

```
    band_wcdma_850 = false
```

```
    band_wcdma_900 = false
```

```
    band_wcdma_1900 = false
```

```
    band_wcdma_2100 = false
```

```
    band_lte_800 = false
```

```
    band_lte_850 = false
```

```
    band_lte_900 = false
```

```
    band_lte_1800 = false
```

```
    band_lte_1900 = false
```

```
    band_lte_2100 = false
```

```
    band_lte_2600 = false
```

```
    band_lte_1700 = false
```

```
    band_lte_700 = false
```

```
    band_tdd_lte_2600 = false
```

```
    band_tdd_lte_1900 = false
```

```
    band_tdd_lte_2300 = false
```

```
    band_tdd_lte_2500 = false
```

```
}
```

```
sim {
```

```
    id = 2
```

```
    card = sim2
```

```
    phone_number = ""
```

```
    extra_at_cmd = ""
```

```
    network_type = auto
```

```
    band_select_type = all
```

```
    band_gsm_850 = false
```

```

band_gsm_900 = false
band_gsm_1800 = false
band_gsm_1900 = false
band_wcdma_850 = false
band_wcdma_900 = false
band_wcdma_1900 = false
band_wcdma_2100 = false
band_lte_800 = false
band_lte_850 = false
band_lte_900 = false
band_lte_1800 = false
band_lte_1900 = false
band_lte_2100 = false
band_lte_2600 = false
band_lte_1700 = false
band_lte_700 = false
band_tdd_lte_2600 = false
band_tdd_lte_1900 = false
band_tdd_lte_2300 = false
band_tdd_lte_2500 = false
}
# set(space+?)
at_over_telnet      cellular      ddns          dhcp          dns
event              firewall    ipsec         lan           link_manager
ntp                openvpn    reboot       route        serial_port
sms                snmp       syslog       system       user_management
vrrp

# set cellular(space+?)
  sim    SIM Settings
# set cellular sim(space+?)
  Integer  Index (1..2)

# set cellular sim 1(space+?)
  card          SIM Card
  phone_number  Phone Number
  extra_at_cmd  Extra AT Cmd
  network_type  Network Type
  band_select_type  Band Select Type
  band_gsm_850  GSM 850
  band_gsm_900  GSM 900
  band_gsm_1800 GSM 1800
  band_gsm_1900 GSM 1900
  band_wcdma_850 WCDMA 850
  band_wcdma_900 WCDMA 900
  band_wcdma_1900 WCDMA 1900
  band_wcdma_2100 WCDMA 2100

```



```
band_lte_800      LTE 800 (band 20)
band_lte_850      LTE 850 (band 5)
band_lte_900      LTE 900 (band 8)
band_lte_1800     LTE 1800 (band 3)
band_lte_1900     LTE 1900 (band 2)
band_lte_2100     LTE 2100 (band 1)
band_lte_2600     LTE 2600 (band 7)
band_lte_1700     LTE 1700 (band 4)
band_lte_700      LTE 700 (band 17)
band_tdd_lte_2600 TDD LTE 2600 (band 38)
band_tdd_lte_1900 TDD LTE 1900 (band 39)
band_tdd_lte_2300 TDD LTE 2300 (band 40)
band_tdd_lte_2500 TDD LTE 2500 (band 41)
# set cellular sim 1 phone_number 18620435279
OK
...
# config save_and_apply
OK                                     // save and apply current configuration, make you configuration effect
```

# Glossary

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

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

Abbr.	Description
WAN	Wide Area Network

## **Guangzhou Robustel LTD**

**Add:** 3rd Floor, Building F, Kehui Park, No.95 Dagan Road,  
Guangzhou, China 510660

**Tel:** 86-20-29019902

**Email:** [info@robustel.com](mailto:info@robustel.com)

**Web:** [www.robustel.com](http://www.robustel.com)